# Oracle® Communications Policy Management

Network Impact Report

Release 12.2

**E82607-01**

December 2016

ORACLE®

Oracle Communications Policy Management Network Impact Report, Release 12.2

E82607-01

## TABLE OF CONTENTS

# 1.0 INTRODUCTION

## 1.1 PURPOSE AND SCOPE

This document highlights the change(s) in this Release 12.2 of the product that may have impact on the customer network, and should be considered by the customer during planning for this release.

## 1.2 DISCLAIMERS

This document summarizes Oracle Communication Policy Management Release 12.2 new and enhancement features as compared to previous release of 9.9.2/11.5.x/12.1.x and the operations impacts of these features, at a high level. The Feature Requirements (FRS) documents remain the defining source for the expected behavior of these features.

*Note that feature implementations may change slightly during product test.*

## 1.3 GLOSSARY

This section lists terms and acronyms specific to this document.

***Table 1: Acronyms***

| | |
|---|---|
| 3GPP | Third-Generation Partnership Project |
| AAA | Authorize-Authenticate-Answer |
| AAR | Authorize-Authenticate-Request |
| ADC | Application Detection and Control |
| AF | Application Function |
| AMBR | Aggregate Maximum Bit Rate |
| ARP | Allocation Retention Priority |
| AVP | Attribute Value Pair |
| BBERF | Bearer Binding and Event Reporting Function |
| BoD-AM | Bandwidth On Demand Application Manager |
| BSS | Business Support System |
| CALEA | Communications Assistance for Law Enforcement Act. |
| CCA | Credit-Control-Answer (CC-Answer) |
| CCR | Credit-Control-Request (CC-Request) |
| CMP | Configuration Management Platform |
| CMTS | Cable Modem Termination System |
| CSCF | Call Session Control Function |
| DCC | Diameter Credit Control |
| DPA | Disconnect-Peer-Answer |
| DPI | Deep Packet Inspection |
| DPR | Disconnect-Peer-Request |
| DRA | Diameter Routing Agent |
| DRMP | Diameter Routing Message Priority |
| DSR | Diameter Signaling Router |
| DTMF | Dual Tone Multi Frequency |
| eMPS | Enhanced Multimedia Priority Service |
| EVS | Enhanced Voice Services |

| | |
|---|---|
| FRS | Feature Requirements Specification |
| GBR | Guaranteed Bit Rate |
| Gen-6, Gen-7, Gen-8 | Refers to the generation of HP server hardware. |
| GUI | Graphical User Interface |
| HA | High Availability |
| H-PCRF | Home PCRF or Home MPE |
| HSS | Home Subscriber Server |
| HTTP | Hypertext Transfer Protocol |
| HW | Hardware |
| IE | Internet Explorer |
| IMS | IP Multimedia Subsystem |
| IP | Internet Protocol |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| JSON | JavaScript Object Notation |
| KPI | Key Performance Indicator |
| LAN | Local Area Network |
| LDAP | Lightweight Directory Access Protocol |
| LI | Lawful Intercept |
| LIMF | Lawful Intercept Mediation Function |
| LVM | Logical Volume Manager |
| MA | Management Agent |
| MCD | Media Component Description |
| MC-PTT | Mission Critical Push-To-Talk |
| MDF | Message Distribution Function |
| MP | Message Processor |
| MPE | Oracle Multimedia Policy Engine |
| MPE-R | Oracle Multimedia Policy Engine – Routing Mode |
| MPE-S | Oracle Multimedia Policy Engine – Serving Mode |
| MRA | Oracle Multiprotocol Routing Agent |
| MS | Mediation Server |
| NFVO | Network Functions Virtualization Orchestrator |
| NOAM | Network OAM |

| | |
|---|---|
| NW-CMP | Network-Level Configuration Management Platform |
| OAM | Operations Administration Maintenance |
| OCS | Online Charging Service |
| OM | Operational Measurement |
| OSSI | Operation Support System Interface |
| PCC | Policy and Charging Control |
| PCD | Policy Connection Director |
| PCEF | Policy and Charging Enforcement Function (GGSN, PGW, DPI) |
| PCMM | Packet Cable Multimedia |
| PCRF | Policy Control Resource Function (Oracle MPE) |
| P-CSCF | Proxy CSCF |
| PDN | Packet Data Network |
| PGW | Packet Data Network Gateway |
| PNR | Push-Notification-Request |
| PS_TO_CS_HANDOVER | Packet Switched to Circuit Switched Handover |
| PTT | Push-To-Talk |
| PUR | Profile-Update-Request |
| QCI | QoS Class Identifier |
| QoS | Quality of Service |
| RAR | Re-Auth-Request (RA-Request)SUPL |
| REST | Representational State Transfer |
| ROB | Release of Bearer |
| S-CMP | Site-Level Configuration Management Platform |
| S-CSCF | Serving CSCF |
| SGW | Serving Gateway |
| Sh | Diameter Sh Interface |
| SMPP | Short Message Peer-to-Peer |
| SMS | Short Message Service |
| SNR | Subscribe-Notification-Request |
| SPR | Subscriber Profile Repository |
| STA | Session-Termination-Answer |
| STR | Session-Termination-Request |
| SRA | Successful Resource Allocation |
| TDF | Traffic Detection Function |

| | |
|---|---|
| TPS | Transactions Per Second |
| UD | Upgrade Director |
| UDR | User Data Repository |
| UE | User Equipment |
| UM | Upgrade Manager |
| UMCH | Usage Monitoring Congestion Handling |
| VIM | Virtual Infrastructure Manager |
| VM | Virtual Machine |
| VNF | Virtual Network Function |
| VO | Verification Office |
| XML | Extensible Markup Language |

# 2.0 OVERVIEW OF ORACLE COMMUNICATIONS POLICY MANAGEMENT RELEASE 12.2 FEATURES

This section provides an overview list of the Oracle Communications Policy Management Release 12.2 new features.

## *2.1 POLICY MANAGEMENT RELEASE 12.2 NEW FEATURES SUPPORT*

| Feature PR# | Feature Name |
|---|---|
| 19720700 | 3GPP ENHANCEMENT: USAGE MONITORING CONGESTION HANDLING (UPDATED TIME-TARIFF SPEC) |
| 20224100 | 3GPP ENHANCEMENT: SUPPORT 3GPP TIME-BASED USAGE MANAGEMENT/TIMEBASED UPGRADE MANAGER |
| 21322637 | 3GPP ENHANCEMENT: APPLICATION BASED CHARGING |
| 21322663 | 3GPP ENHANCEMENT: GROUP COMMUNICATION – QCI RELATED |
| 19720429 | 3GPP ENHANCEMENT: SUPPORT OF QCI VALUES OUTSIDE OF 1-9 |
| 21322590 | 3GPP ENHANCEMENT: MISSION CRITICAL QCIs |
| 19113866 | TRACK MAXIMUM TPS IN KPI INTERVAL |
| 20319847 | ADD AUDIT LOG TO CMP SAVELOG |
| 20325595 | EXPOSE ENGINEERING LOG LEVEL CONFIGURATION IN CMP |
| 22536198 | SUPPORT FOR SECURING PCRF NETWORK INTERFACES (FIREWALL ENABLED SUPPORT) |
| 24304274 | GX PENDING TRANSACTION RACE CONDITION |
| 20632502 | SELECTIVE TRIGGERING OF POLICY EVALUATION ON STR AND CCR-T |
| 20632554 | SETTING GX SESSION LEVEL PARAMETERS VIA POLICY ACTION ON RX REQUEST |
| 19482300 | VIRTUALIZED POLICY TABLES |
| 22315457 | MRA SENDS SDR THROUGH DRA |
| 22121678 | 7.105: ENHANCED MULTIMEDIA PRIORITY SERVICE PHASE 1 |

| | |
|---|---|
| 22135682 | 7.404: EVS CODEC SUPPORT |
| 19720429 | 7.119: OPERATOR SPECIFIC QCI |
| 22264564 | 7.104: INCLUSION OF MSISDN IN SUBSCRIPTION ID AVP OF GX:CCR-I INTERFACE |
| 21322590 | 7.122: QCI FOR NON-CRITICAL PUSH TO TALK+ USER PLANE (QCI - 66) |
| 19646305 | CONFIGURATION TEMPLATES FOR CABLE FEATURES |
| 20162894 | PCMM PER MPE SUMMARY AND PER CMTS STATISTICS THROUGH OSSI/XML |
| 20286860 | DISCOVER CMTS SUBNETS WHEN SAVING A NEWLY CREATED NETWORK ELEMENT |
| 21153115 | GENERIC POLICY NOTIFICATION INTERFACE - CONVERT FOR CABLE MODE |
| 21348748 | UNIFIED EXPORT/IMPORT FEATURE SUPPORT FOR CABLE MODE |
| 22186376 | IPV6 SUPPORT FOR OAM AND REPLICATION NETWORKS FOR CABLE |
| 20162817 | PROVIDE THE NUMBER OF ACTIVE GATES PER AMID PER MPE THROUGH OSSI/XML |
| 20287350 | EXPORT BOD SESSION DATABASE |
| 22114178 | INCLUDE MORE OPTIONS FOR RESET FREQUENCY FOR PLANS |
| 22258207 | NOTIFICATION TRIGGERS FOR AGGREGATE QUOTA |
| 19358129 | CABLE POLICY VMWARE SUPPORT ON MULTIPLE HW PLATFORMS |
| 22293420 | POLICY CONNECTION DIRECTOR ( PCD ) |
| 19359794 | ENTRY LEVEL POLICY SOLUTION ON RACK MOUNT SERVERS (RMS) |
| 20837199 | POLICY MANAGEMENT VNF MANAGEMENT |
| 20271401 /224376 | SUPPORT TO CONFIGURE BEARER LEVEL ARP IN POLICY ACTION |
| 20271416 /224391 | RESULT CODE 5143 RETURNED IF REQUESTED QOS CONFLICTS WITH AUTHORIZED QOS |

| | |
|---|---|
| 20271430 /224512 | NOTIFICATION DURING THE CONFIGURED INTERVAL |
| 20271438 /225037 | UE SUBSCRIPTION REASON RETURNED IN SESSION RELEASE CAUSE AVP |
| 20271448 /224443 | MPE CANNOT SEND DPR MESSAGE TO DISCONNECT DIAMETER CONNECTION ACTIVELY |
| 238974 | ADD SIGC ADDRESS SUPPORT |
| 240023 | ADC RULE SUPPORT FOR PCC RULE LEVEL |
| 239241 | ADD THE POLICY SUPPORT TO DO THE JUDGMENT ACCORDING TO PCEF'S DOMAIN |
| 21305529 | POLICY MANAGEMENT SUPPORT FOR ORACLE NETRA SERVER X5-2 |
| 19488243 | SPECIFY GX AND RX RESULT CODE WHILE NO BINDING INFO |

### 2.1.1 Policy Releases Software Merge into Policy 12.2

This Policy release 12.2 includes features of Policy 9.9.2, 11.5.x, and 12.1.x

## 2.2 POLICY MANAGEMENT HARDWARE REQUIREMENTS

### 2.2.1 Supported Hardware

The Policy Management Policy Release 12.2 software can be applied on the following list of hardware that previously supported under Release 9.9.2 / 11.5.x / 12.1.x

- Oracle NETRA Server X5-2.
- Oracle Server X5-2 on Rack Mount Server (RMS).
- Compatible with HP Gen-6, Gen-8 and Gen-9 Rack Mount Server ( RMS) and C-class Servers
- HP 6120XG and HP 6125XLG enclosure switches.

**NOTE:** *PP-5160 server is NOT supported*

### 2.2.2 Policy Management Support for Oracle NETRA Server X5-2 ( PR# 21305529 )

It will be initially implemented in Tekelec Platform Distribution Release 7.0.3 which is part Release 12.2. The Netra X5-2 can be AC or DC powered. Other than processor and memory changes, here is a brief listing of the hardware changes for the Netra X5-2 from the Oracle Server X5-2.

- The server is NEBS certified.
- To meet NEBS requirements, the CPU Power Limit option is used to effectively lower the Thermal Design Power (TDP) such that the CPU will always run just below the 55°C (131°F) throttle point. This function reduces the CPU power to 120 watts from the maximum 145 watts to prevent CPU throttling. In this mode, performance at lower ambient temperature is reduced, however, the CPU cores will not throttle at or below 55°C (131°F). When disabled, the system will operate normally and the default TDP of 145 watts will be maintained. In this mode, the CPU cores should throttle as needed when ambient temperatures and load cause the die temperature to exceed maximum.
- The server is 2-U in height.
- The server has six PCI slots, one of which is dedicated to the disk controller.
- Six USB ports: two on front panel (USB 2.0), two on rear panel (USB3.0) and two internal on motherboard (USB 2.0).

### 2.2.3 Entry level Policy Solution on Rack Mount Servers (RMS) ( PR# 19359794 )

Policy in a box Solution for OVM/KVM on RMS system with benchmarked only on OVM/Enterprise Manager X5-2 (CMP, MPE, MRA/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 i.e. one CMP cluster, one MRA cluster, and two MPE clusters, on a single physical RMS server with another set of Policy system running on the second physical RMS server as a Standby system. Thus, the minimum basic Policy system configuration requires only a single physical RMS server and a High Availability (HA) Policy system would require two RMS servers.

## 2.3 POLICY MANAGEMENT SOFTWARE CHANGES

### 2.3.1 Software Components

| Components | Releases |
|---|---|
| TPD 64 Bit | 7.0.3 |
| COMCOL | 6.4 |
| PM&C | 6.0.3 |
| TVoE | 3.0.3 |
| HP Firmware FUP | 2.2.9 (Minimum) |
| Oracle Firmware | 3.1.5 (Minimum) |

### 2.3.2 UDR & SPR Product Compatibility

| Products | Releases | Compatibility |
|---|---|---|
| Oracle SDM SPR | 9.3.1 | Profile V2, Profile V3 and Profile V4 schemas |
| Oracle Communication UDR | 10.2<br>12.1<br>12.2 | Profile V2, Profile V3 and Profile V4 schemas |

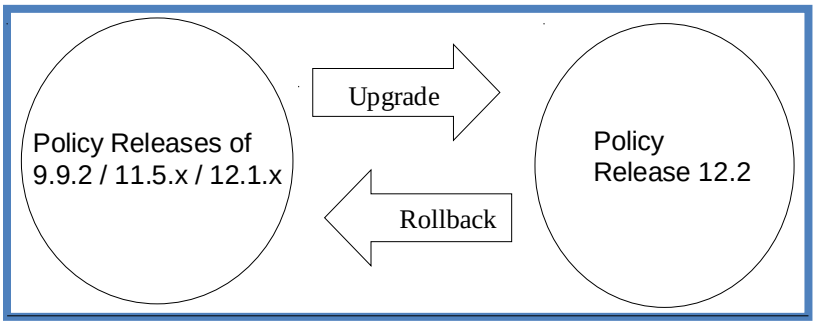
## 2.4 POLICY MANAGEMENT SOFTWARE UPGRADE/BACKOUT OVERVIEW ( PR# 233969 )

During the execution of Policy software upgrade/rollback (backout) procedures, it is expected that the CMP clusters, MRA clusters and MPE clusters will be running in different software releases.

In Release 11.5.x, both Cable and Fixed/Wireline deployments are using the same software release for the first time in distinct "modes". As with this Release 12.2, Fixed/Wireline mode is no longer supported, so it is expected that upgrade will result in Cable mode only.

### 2.4.1 Supported Software Upgrade/Rollback ( Backout) Paths for Release 12.2

The Figure below shows the supported upgrade Path for Release 12.2




As with the past releases, both Geo-Redundancy and non Geo-Redundancy Policy system deployment will need separate Policy software upgrade/rollback ( backout) procedures.

### 2.4.2 Supported Software Releases Upgrade Sequence

#### 2.4.2.1 Upgrade Sequence

The CMP clusters ( CMP/NW-CMP and DR-CMP/NW-CMP ) shall be upgraded first from Release N to Release N+1 prior to executing upgrade on any other server clusters ( MPE, MRA/PFE, MA, and BoD ) of the system.

In the case that cluster-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 sequence may be spread through multiple maintenance windows over an extended time period, with periods of steady state operation in mixed-mode between windows.*

The upgrade of Policy Management system from Release N to Release N+1 shall generally be executed in the following sequence:

**NOTE:** *Refer to the separately available related upgrade/rollback upgrade paths for more detail procedures.*

***Release 12.1.x to Release 12.2 ( Wireless mode)***

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

***Release 11.5.x to Release 12.2 ( Wireless mode)***

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

***Release 11.5.x to Release 12.2 ( Cable mode)***

1. Standalone Primary CMP cluster and Disaster Recovery (DR) CMP cluster.
2. MA.
3. MPE-R clusters
4. MPE-S clusters, including spare server if geo-redundancy is deployed.
5. BoD-AM clusters, including spare server if geo-redundancy is deployed.

***Release 9.9.2 to Release 12.2 ( Wireless mode)***

1. Standalone Primary CMP cluster and Disaster Recovery (DR) CMP cluster
2. MPE clusters, including spare server if geo-redundancy is deployed.
3. MRA clusters, including spare server if geo-redundancy is deployed
4. Oracle Communications UDR (UDR) server(s)
5. MDF/MS server(s)

### *2.4.3 Mixed Version Policy Management system expectations*

The system that is running Release 9.9.2 / 11.5.x / 12.1.x mixed configuration supports the performance and capacity of Release 9.9.2 / 11.5.x / 12.1.x respectively. The mixed version Policy Management configuration supports Release 9.9.2 / 11.5.x / 12.1.x features respectively.

In the mixed version Policy Management configuration Release 12.2 CMP has the following general limitations -

- New features must not be enabled until the upgrades of all servers managed by that CMP are completed. This also applies to using policy rules that include new conditions and actions introduced in the release.

- 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 -

  (a) Network Elements can be added.

  (b) Advanced Configuration settings that were valid for 9.9.2 / 11.5.x / 12.1.x may be changed.

**NOTE:** *Replication between CMP and DR-CMP is automatically disabled during upgrade of CMP and DR-CMP from Release 9.9.2 / 11.5.x / 12.1.x to Release 12.2. The replication is automatically enabled once both active CMP and DR-CMP are upgraded to Release 12.2.*

***Mixed-version Configurations Supported between Release 12.1.x and Release 12.2 ( Wireless mode)***

| Policy Management Components | CMP Release 12.2 | MRA Release 12.2 | MPE Release 12.2 |
|---|---|---|---|
| CMP release 12.1.x | No | No | No |
| MRA release 12.1.x | Yes | Yes | Yes |
| MPE release 12.1.x | Yes | Yes | N/A |

***Mixed-version Configurations Supported between Release 11.5.x and Release 12.2 ( Wireless & Cable modes)***

| Policy Management Components | CMP Release 12.2 | MPE/MPE-R Release 12.2 | MPE-S Release 12.2 | BoD Release 12.2 | MRA/MA Release 12.2 |
|---|---|---|---|---|---|
| CMP release 11.5.x | No | No | No | N/A | Yes |
| MPE/MPE-R release 11.5.x | Yes | N/A | Yes | N/A | Yes |
| MPE-S release 11.5.x | Yes | Yes | N/A | N/A | Yes |
| BoD release 11.5.x | Yes | Yes | Yes | N/A | N/A |
| MRA/MA release 11.5.x | Yes | Yes | Yes | N/A | N/A |

***Mixed-version Configurations Supported between Release 9.9.2 and Release 12.2 ( Wireless mode)***

| Policy Management Components | CMP Release 12.2 | MRA Release 12.2 | MPE Release 12.2 | MDF/MS Release 12.2 |
|---|---|---|---|---|
| CMP release 9.9.2 | No | No | No | Yes |
| MRA release 9.9.2 | Yes | Yes | Yes | Yes |
| MPE release 9.9.2 | Yes | Yes | N/A | Yes |
| MDF/MS release 9.9.2 | Yes | Yes | Yes | N/A |

### *2.4.4 Supported Software Releases Rollback (Backout) Support & Limitation*

- Once the whole Policy Management system is upgraded to Release 12.2, customer(s) may decide that a backout to the previous release is required. In that case, each individual server/cluster 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 all the related component servers are rolled back first before the active CMP/NW-CMP and DR-CMP/NW-CMP can be rolled back to the previous version.

- 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 for example, if all of the servers in the Policy Management system were backed out from Release 12.2 to Release 9.9.2 / 11.5.x / 12.1.x, these servers could subsequently be upgraded to Release 12.2-Build_A etc.

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

- 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 minor release(s) of Release 12.2.

#### 2.4.4.1 *Rollback ( Backout) Sequence*

The Rollback of Policy Management system from Release N+1 to Release N shall generally be executed in the following sequence ( reverse of the Upgrade sequence):

**NOTE:** *Refer to the separately available related upgrade/rollback upgrade paths for more detail procedures.*

***Release 12.2 to Release 12.1.x ( Wireless mode)***

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

***Release 12.2 to Release 11.5.x ( Wireless mode)***

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

***Release 12.2 to Release 11.5.x ( Cable mode)***

1. BoD-AM clusters, including spare server if geo-redundancy is deployed
2. MPE-S clusters, including spare server if geo-redundancy is deployed
3. MPE-R clusters
4. MA.
5. Standalone Primary CMP cluster and Disaster Recovery (DR) CMP cluster.

***Release 12.2 to Release 9.9.2 ( Wireless mode)***

1. MDF/MS server(s)
2. UDR server(s)
3. MRA clusters, including spare server if geo-redundancy is deployed
4. MPE clusters, including spare server if geo-redundancy is deployed.
5. Standalone Primary CMP cluster and Disaster Recovery (DR) CMP cluster

### *2.4.5 Upgrade Director ( UD)*

For upgrade paths from Release 9.9.2/11.5.x to Release 12.2, there will be an initial upgrade procedure of the pre-Release 12.2 CMP using pre-Upgrade Director methods, and thereafter, the upgrade of all other components will be using the Upgrade Director from just upgraded Release 12.2 CMP.

As for upgrade path from Release 12.1.x to Release 12.2, the Upgrade Director functionality already existed in both releases, so just strictly follow the relevant Upgrade/Rollback procedures.

## *2.5 MIGRATION OF POLICIES AND SUPPORTING POLICY DATA*

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

# 3.0 CHANGES BY FEATURE

## *3.1 MRA ROUTING SDR THROUGH DRA (PR# 22315457)*

### *3.1.1 Pre-Requisite*

Oracle currently implements a proprietary Session Recovery feature ( PR# 229630 & PR# 232952 ), which allows the network to recover lost Gx session(s) on MPE, or Binding(s) previously created on either Primary or Backup MRA. This functionality is implemented in conjunction support from specific PCEF (PGW). This Session Recovery feature has to be enabled/implemented first prior to applying the following new feature enhancement.

### *3.1.2 Introduction*

This feature enhancement allows MRA sent SDR message to be routed over DRA. It does not impact the current implementation of SDR message sent from MPE.

### *3.1.3 Detailed Description*

In the current Session Recovery implementation, the MRA initiates a proprietary SDR message to directly connected PCEF ( PGW) as shown below in Figure 1. if it receives Rx:AAR-I from the P-CSCF, and does not find the associated binding.

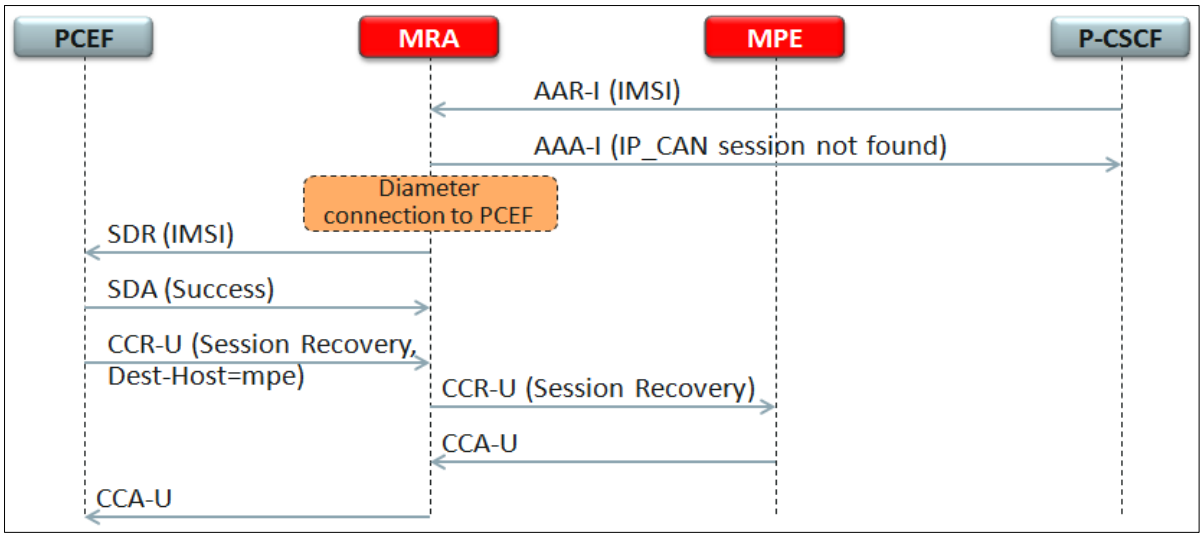



***Figure 1: Current Session Recovery Implementation with direct Diameter connection between MRA and PCEF ( PGW).***

This implementation has it's limit i.e if there is a DRA or any Diameter Peer device between the MRA and PCEF ( PGW), then the MRA will interpret as the direct Diameter connection to the PCEF is down, thus no SDR message is sent out, as shown below in Figure 2.

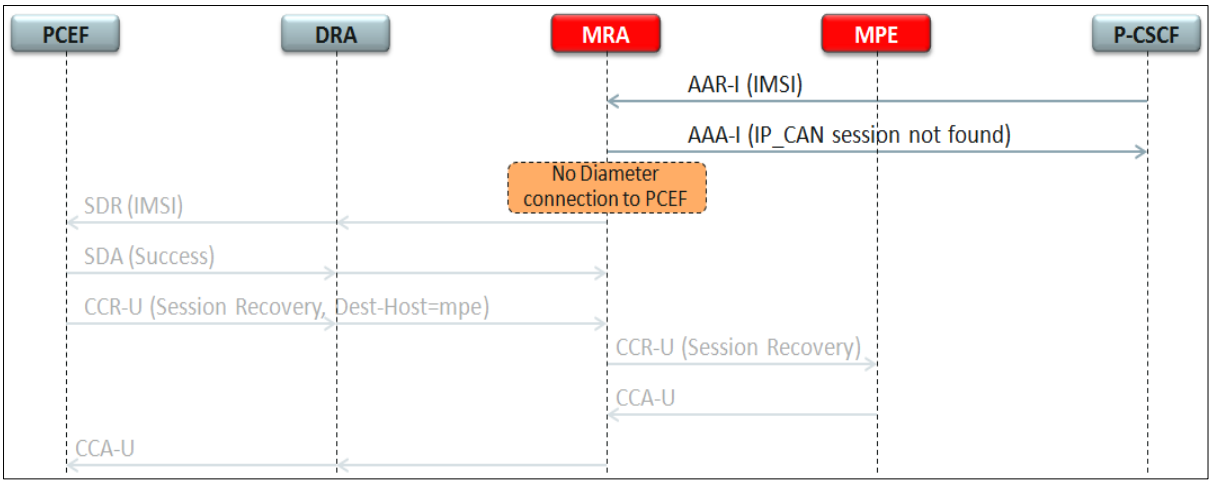



***Figure 2: Session Recovery Fails due to DRA installed between MRA and PCEF ( PGW)***

The high level solution is to have known MRA Diameter Peers routing configured for the PCEF ( PGW) with DRA as it's peer.

**NOTE:** *Diameter error message of " IP-CAN session not found" is now changed to "IP-CAN_SESSION_NOT_AVAILABLE"*

There are three setup scenarios that this feature enhancement can be implemented –

## a) DIRECT CONNECTION TO PCEF ON MRA

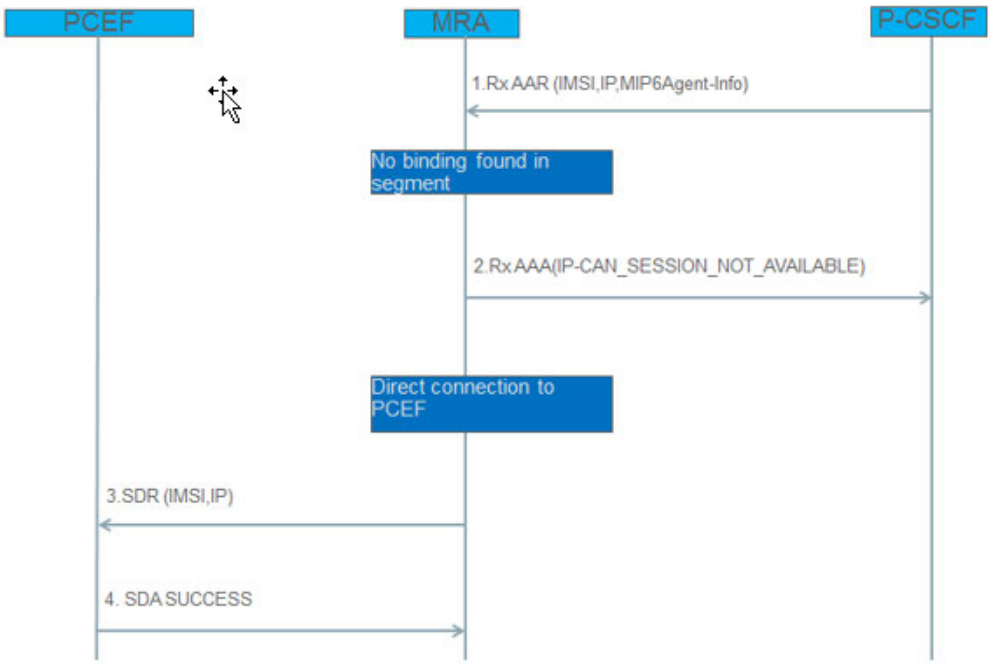



**Figure 1: Direct connection to PCEF**

1. When an AAR message is coming to MRA in which there is no MRA binding info found by the indexed user id.

2. MRA rejects Rx:AAR message when session is not found with diameter error message of " IP-CAN_SESSION_NOT_AVAILABLE"

3. An identity of PCEF with connection to MRA will be selected by MIP6AgentInfo in Rx message in a round robin balanced way when the connection for this PCEF identity is found in the current PCEF connections in MRA. A SDR message will be created according to the AAR message and sent to the destination peer by this selected destination identity.

4. PCEF replied with successful SDA message.

### b) ROUTE TO PCEF ON MRA WHEN THERE IS NO DIRECT CONNECTION TO PCEF

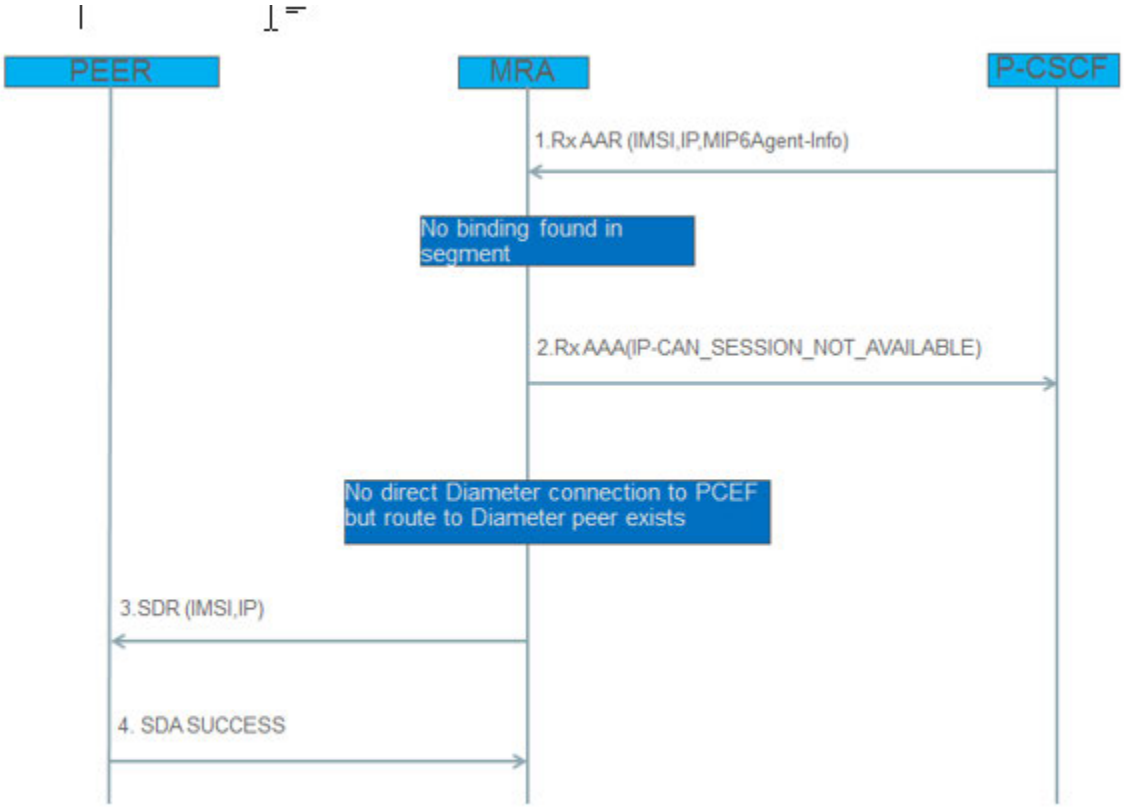



**Figure 2: Diameter peer to PCEF on MRA when there is no direct connection to PCEF**

1. When an AAR message is coming to MRA in which there is no MRA binding info found by the indexed user id.

2. MRA rejects Rx:AAR message when session is not found with diameter error message of " IP-CAN_SESSION_NOT_AVAILABLE"

3. The PCEF Diameter identity is chosen in a round robin way and there are no direct connections to PGW but a matching route exists to the diameter peer. A SDR message will be created according to the AAR message and forwarded to this diameter peer.

4. The peer replied with successful SDA message.

### c) CONNECTION TO BACKUP MRA WHEN THERE ARE NO DIRECT CONNECTIONS TO PCEF AND DIAMETER PEER

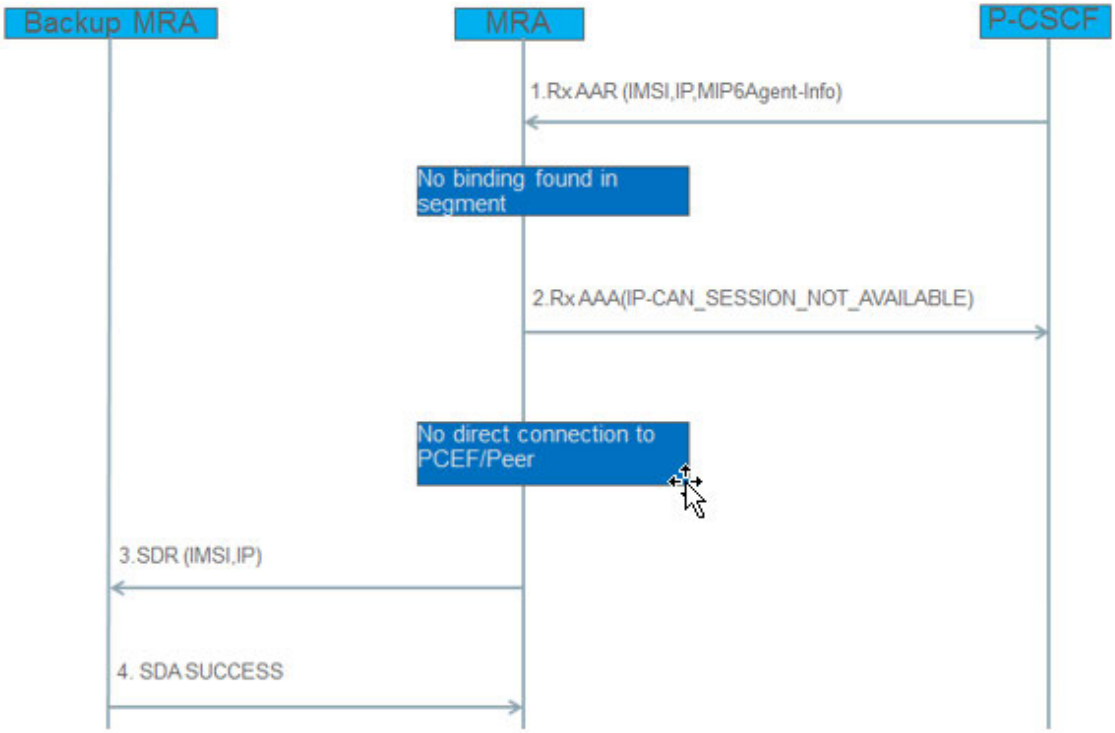



**Figure 3: Connection to Backup MRA when there are no direct connections to PCEF and Peer**

1. When an AAR message is coming to MRA in which there is no MRA binding info found by the indexed user id.

2. MRA rejects Rx:AAR message when session is not found with diameter error message of "IP-CAN_SESSION_NOT_AVAILABLE"

3. The PCEF Diameter identity is chosen in a round robin way but all direct connections to PGW is down. There are no connections to peer. A backup MRA which is the associated as backup MRA in the MRA association configuration is connected to this MRA. A SDR message is created according to the AAR message and sent to this backup MRA only once. In the backup MRA, a diameter error message of

"DIAMETER_UNABLE_TO_DELIVER " will happen if the Backup MRA cannot find the direction connection with PCEF or matched peer in the routing table.

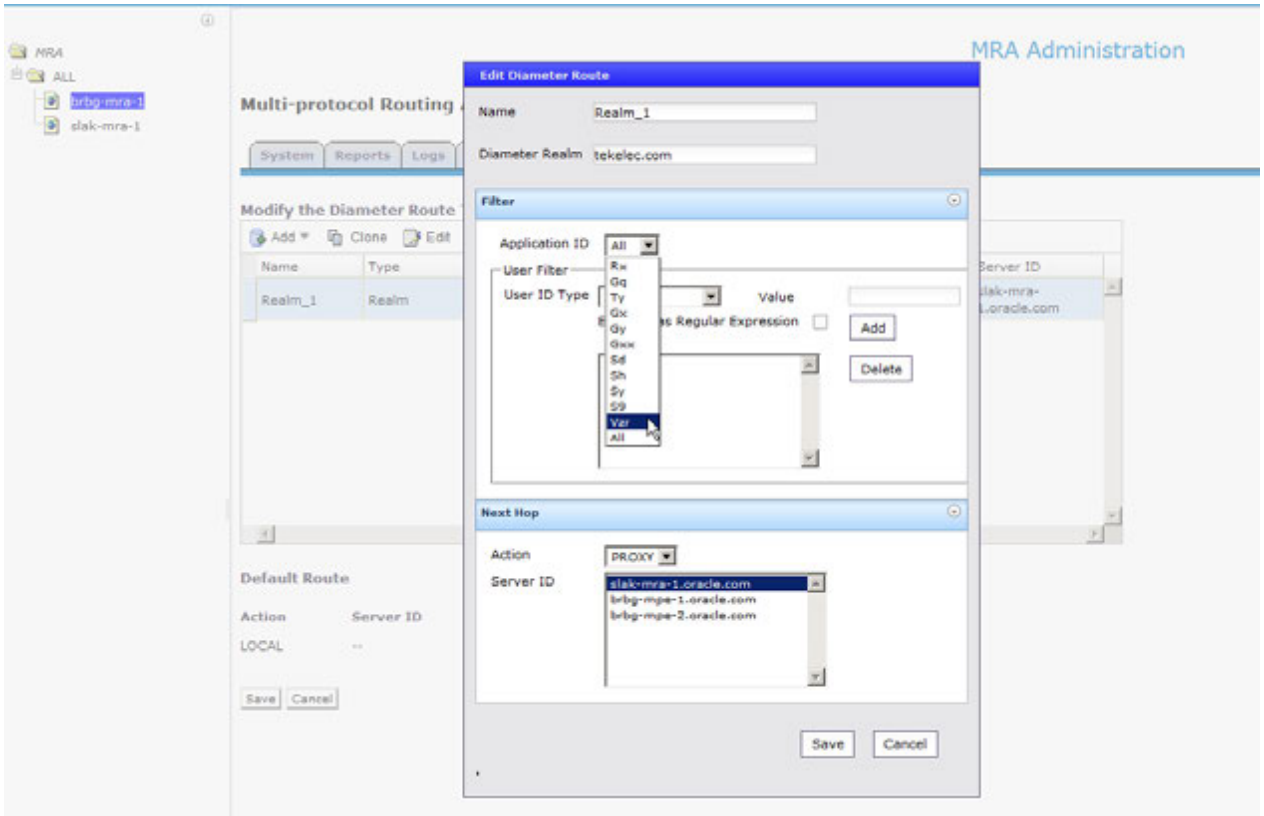
4. Backup MRA replied with successful SDA message.

### *3.1.4 User Interface Changes*

Additional "**Vzr**" Application ID included under the Host and Realm Based Route configuration as shown in the CMP screenshot below – it's only available on the MRA for this feature enhancement.

The SDR message will be forwarded if the "**Vzr**" and a Next Hop server is connected to this MRA.

**CMP GUI:** *MRA → Configuration → ( Select MRA cluster name ) → Diameter Routing → Modify Routes → ( Add Realm Based Route, or Add Host Based Route option menu )*



## 3.2 3GPP QCI AND GROUP COMMUNICATION ENHANCEMENTS ( PR# 19720429 , 21322590, 20271401 & 21322633 )

### 3.2.1 Introduction

These feature enhancements describe the functions and requirements as specified in the following –

**PR# 19720429** – Support of QCI values 1 to 254

**PR# 21322590 –** Mission Critical QCI

**PR# 20271401 –** Support to configure bearer level ARP in policy action

**PR# 21322633 –** Group Communications Services

### 3.2.2 Detailed Description

**PR# 19720429** – Support of 3GPP for QCI values from 1 to 254 set via policy configuration. This includes allowing QCI values up to 254 specified in the Traffic Profiles and Roaming Profiles.

Currently, Policy Management supports QCI values range only from 1 to 9.

**PR# 21322590** – Support of 3GGP Mission Critical QCI values of 65, 66, 69 and 70 with 'MissionCriticalQCI' indicator set in the received Gx:CCR-I message –

| bit | Feature name | M/O | Vendor-Id |
|---|---|---|---|
| 25 | **MissionCriticalQCIs** | O | 3GPP<br><br>(10415) |

Those QCI values could be used for Mission Critical Services as specified in the following –

- QCI-65 ( GBR) for Mission Critical PTT (user plane voice)
- QCI-66 ( GBR) for non-Mission Critical PTT (user plane voice)
- QCI-69 ( non-GBR) for Mission Critical PTT (signaling plan)
- QCI-70 ( non-GBR) for Mission Critical Data

**PR# 20271401 -** Override default eMPS/GCS ARP value

**PR# 21322633 -** Support to recognize new 3GPP of Group Communication Service Application Server ( GCS AS) as negotiated between Policy Management and PCEF in the received Gx:CCR-I message,

| bit | Feature name | M/O | Vendor-Id |
|---|---|---|---|
| 10 | **GroupComService**<br><br>**( GCS)** | O | 3GPP<br><br>(10415) |

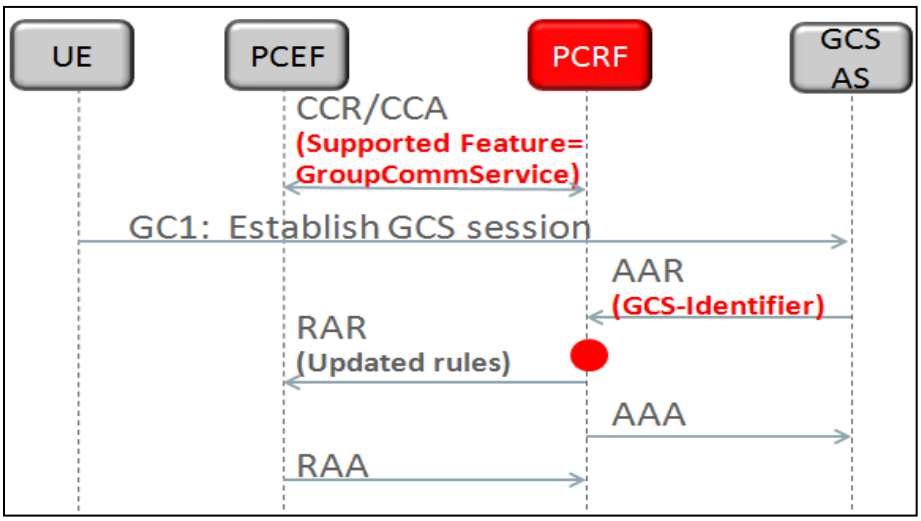
and specified in the “Supported Features” Identifier AVP of received Rx:AAR message.

| **Attribute Name** | **AVP Code** |
|---|---|
| GCS-Identifier | 538 |

<AA-Request> ::= < Diameter Header: 265, REQ, PXY >
< Session-Id >
{ Auth-Application-Id }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
[ Destination-Host ]
[ IP-Domain-Id ]
[ AF-Application-Identifier ]
*[ Media-Component-Description ]
[ Service-Info-Status ]
[ AF-Charging-Identifier ]
[ SIP-Forking-Indication ]
*[ Specific-Action ]
*[ Subscription-Id ]
[ OC-Supported-Features ]
*[ Supported-Features ]
[ Reservation-Priority ]
[ Framed-IP-Address ]
[ Framed-Ipv6-Prefix ]
[ Called-Station-Id ]
[ Service-URN ]
[ Sponsored-Connectivity-Data ]
[ MPS-Identifier ]
[ GCS-Identifier ]
[ Rx-Request-Type ]
*[ Required-Access-Info ]
[ Origin-State-Id ]
*[ Proxy-Info ]
*[ Route-Record ]
*[ AVP ]

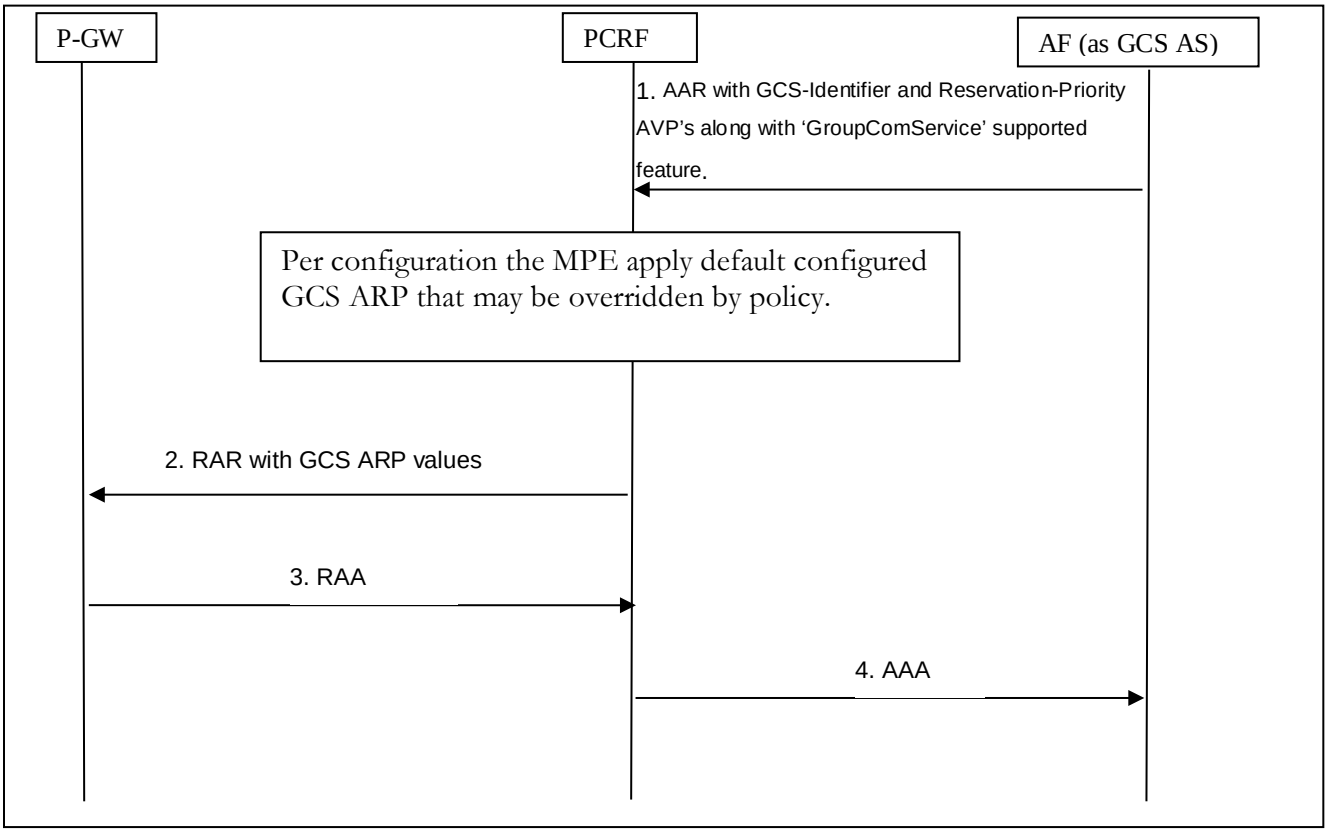
– Support to setting up QoS ( QCI and ARP) values via configured policy, for both Uplink and Downlink UE unicast resources.

This could result in sending a new or updating the PCC rule to PCEF ( PGW) as typical call flow described in the following –




One important application of GCS session is emergency services. It is useful to create policies which take different actions based upon whether the PCEF supports Mission critical QCIs.

- **Group Communication Service – Rx session Establishment**

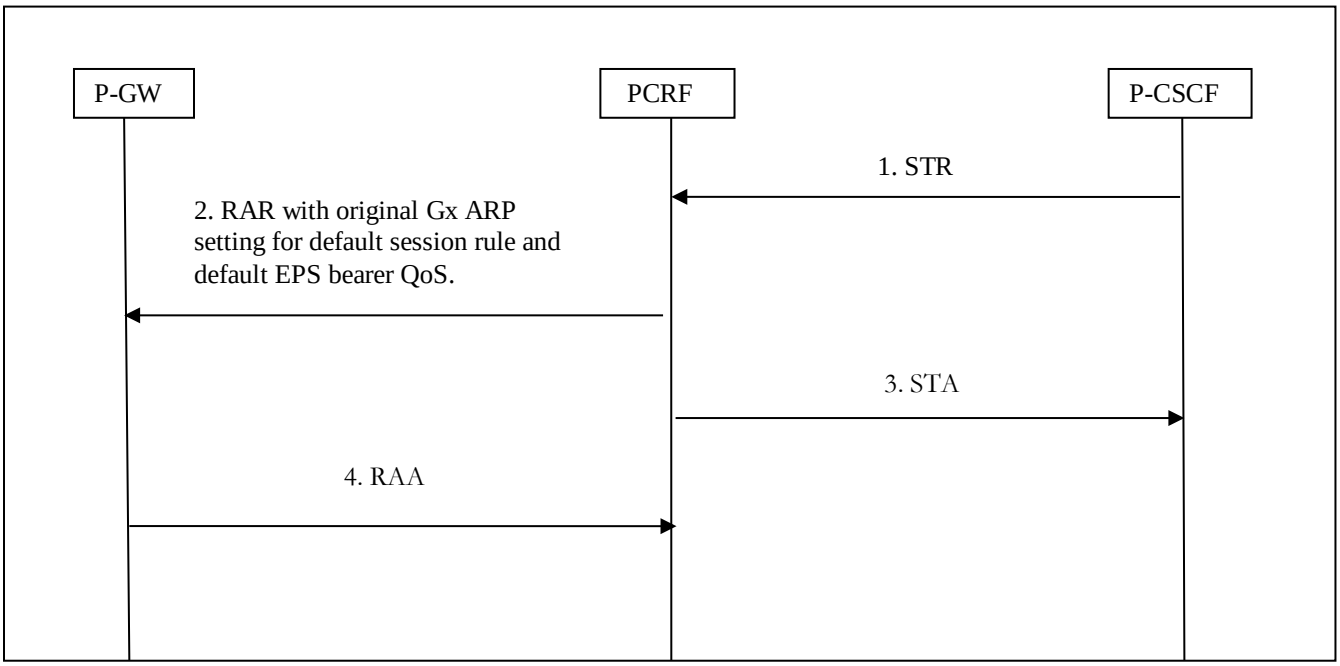


**Pre-requisite** - There is an existing Gx session for a specific PDN connection.

1. The AF sends an AAR-I to the PCRF with GCS-Identifier AVP and Reservation-Priority AVP's along with 'GroupComService' supported feature.
2. In case the Reservation-Priority AVP is received within the command(session) level, the PCRF applies the configured GCS ARP values to the session default rule, to all session application rules as well as to the default-eps-bearer-QoS. In case the Reservation-Priority AVP is received within particular media, the PCRF applies the configured GCS ARP values to the application rules corresponding to that media only.
3. MPE evaluates the received GCS-Identifier value and may set new ARP values.
4. MPE sends Gx:RAR to the P-GW for the new Rx session being established.
5. The PGW responds with a RAA over Gx to the PCRF.
6. The PCRF sends AAA successful back to the AF.

**NOTE:** For the MPE to apply the default configured GCS ARP, AAR must include both GCS-Identifier and Reservation-Priority AVP's.

- **Group Communication Service – Rx session Termination**




**Pre-requisite** - There are existing Gx and Rx sessions for a specific PDN connection.

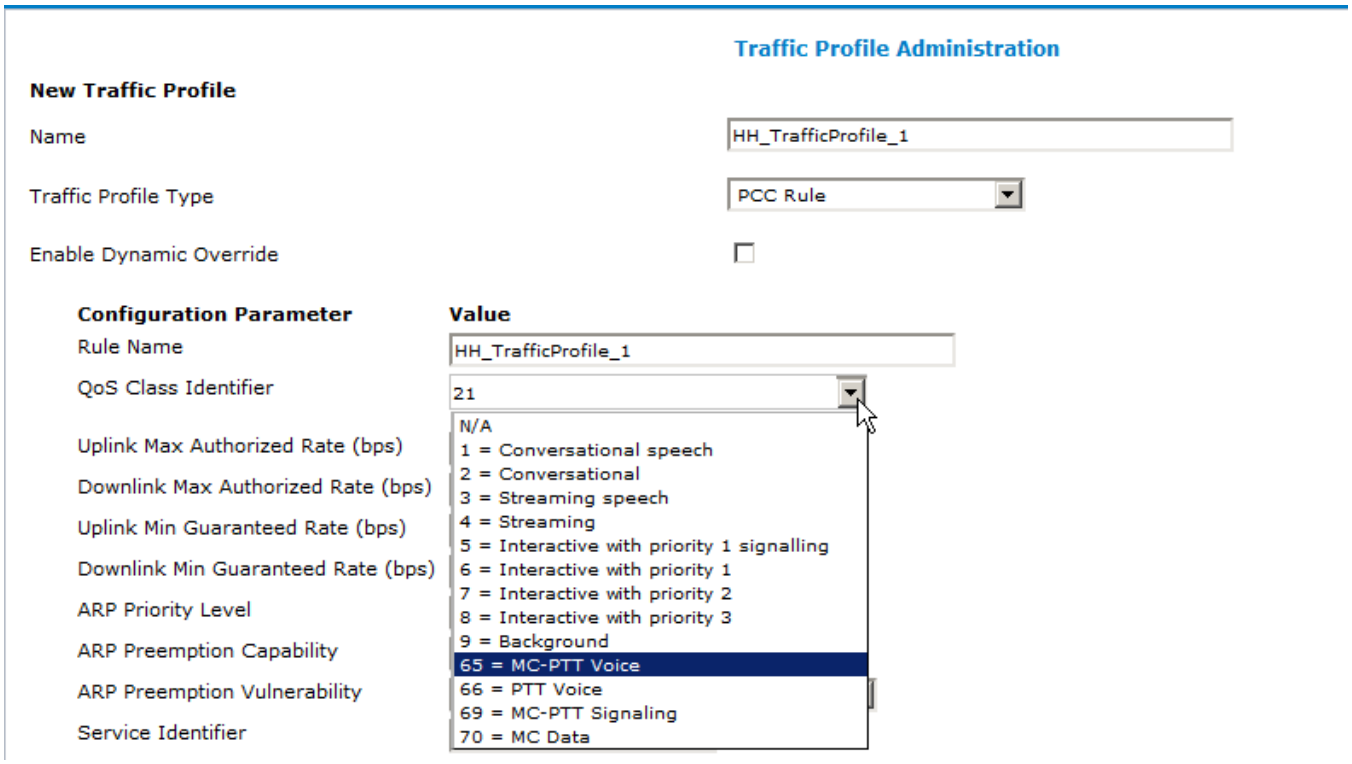
1. The P-CSCF sends an STR to the PCRF to terminate the Rx session.

2. MPE deletes the Rx session. MPE sends RAR to GW to remove application rules. RAR includes Charging-Rule-Install with the default session rule and default-EPS-Bearer-QoS contain the original ARP values that were installed at the time when Gx session was established.
3. MPE sends STA to P-CSCF.
4. MPE receives RAA back from the P-GW.

### 3.2.3 User Interface Changes

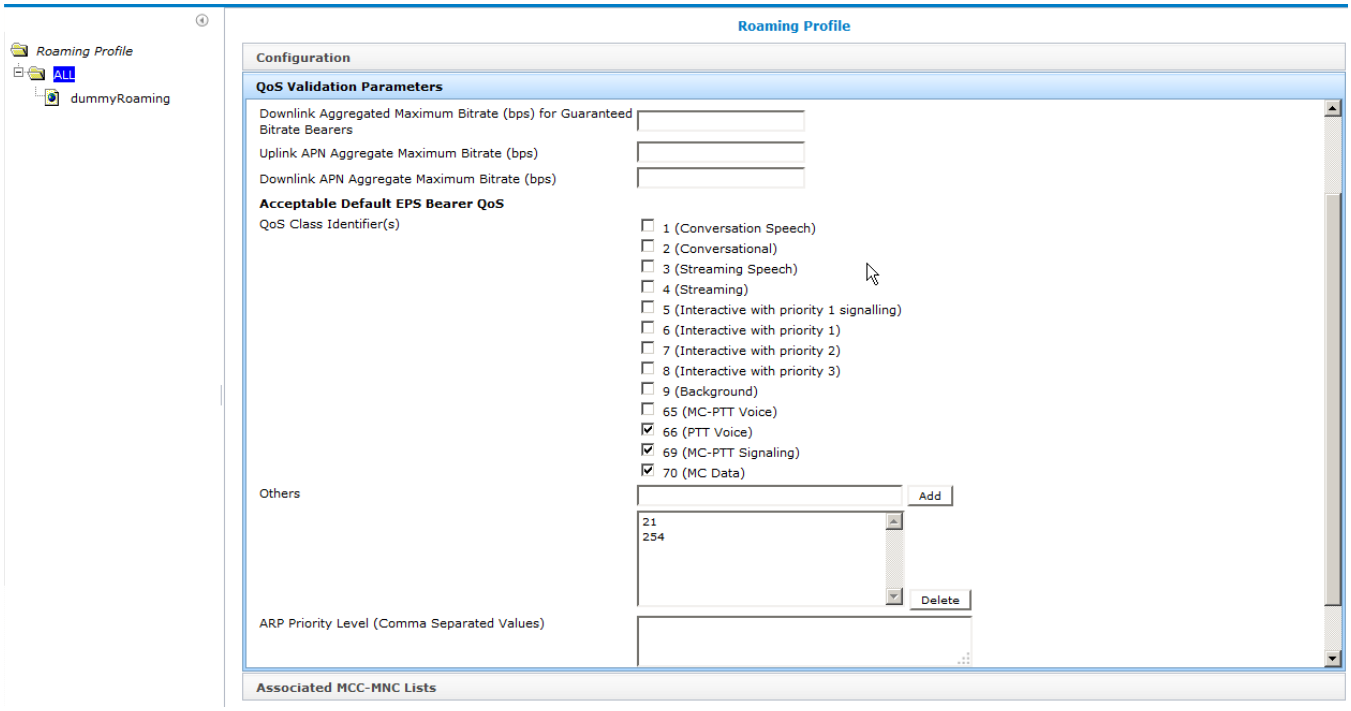
Additional QCI values supported up to 254 in the following traffic profiles: Diameter QoS, PCC Profile and PCC Rule.

**CMP GUI:** *Policy Server → Traffic Profiles*



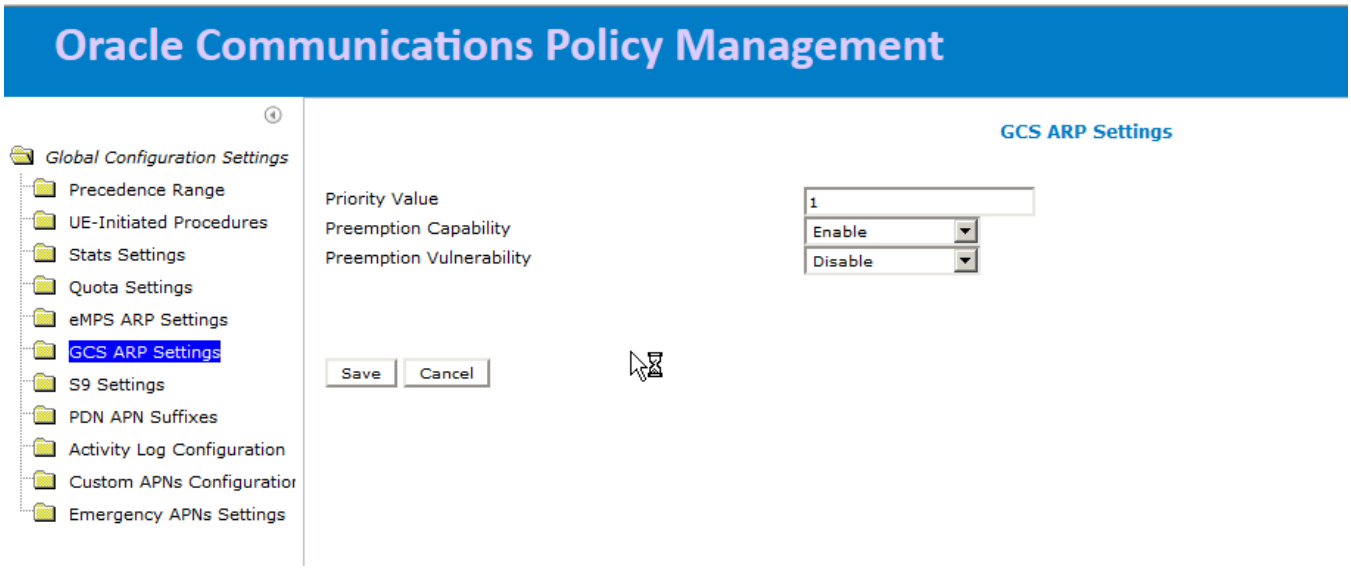

**NOTE:** *Either QCI values from 1 through 254 can be entered in "**QoS Class Identifier**" parameter, or the pre-defined QCI dropdown values as shown above.*

**CMP GUI:** *Policy Server → Roaming Profiles*




A new "**GCS ARP Global Settings"** is added and will be applied by default to PCC rules as well as to the default bearer per receiving of GCS-Identifier and Reservation-priority AVP's.

**CMP GUI:** *Global Configuration → Global Configuration Settings → GCS ARP Settings*




## Priority Level

Valid values: *1 through 15*
Default value: *1*

**Preemption Capability**

Valid values: *Preemption_Capability_Enabled ; Preemption_capability_Disabled*
Default value: *Preemption_Capability_Enabled*

**Preemption Vulnerability**

Valid values: *Preemption_Vulnerabilty_Enabled ; Preemption_Vulnerabilty_Disabled*
Default value: *Preemption_Vulnerabilty_Disabled*

When the Reservation-priority AVP is received within the command level, GCS ARP is applied to the default session rule, the application rules as well as to the DEBQ.

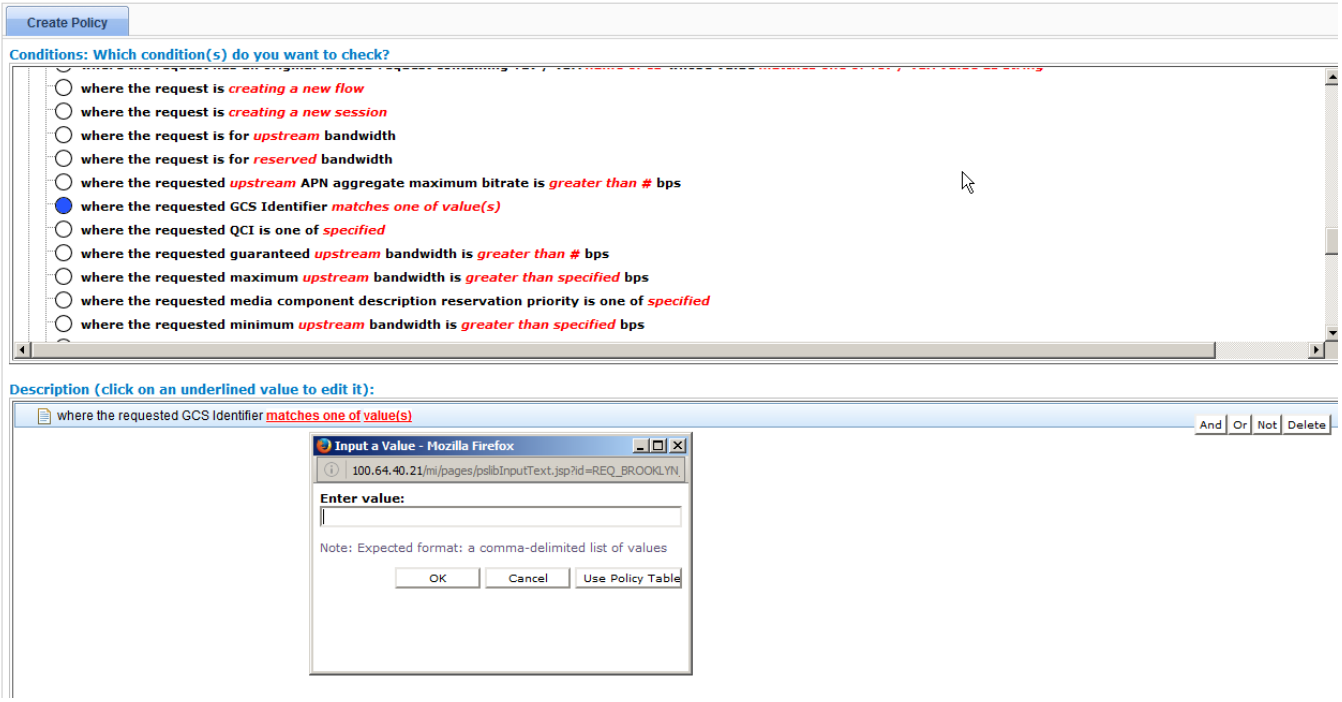
When the Reservation-priority ls received within the media, the GCS ARP will be applied only to the application rules that corresponding to this media.

**Policy Changes Table**

| Policy Condition Group | Policy Condition or Action | Description |
|---|---|---|
| **"Request" Conditions** | Where the requested GCS Identifier matches one of value(s) | Checks the value of the received Rx GCS-Identifier AVP. |
| **"Request" Conditions** | Where the corresponding enforcement session supports feature name | Evaluates the supported feature name taken from the enforcement session that correlates to this application (Rx )request. |
| **"Request" Conditions** | Where the requested QCI is one of specified | Allows QCI values to be within the range of 1-9 or 65, 66, 69 70. |
| **"Request" Conditions** | Where the select type is contained in Match List(s) select list(s) | Adding new Match List Type 'Requested QCI'. |
| **"Action"** | Set specified ARP to value | Override default eMPS/GCS ARP value |

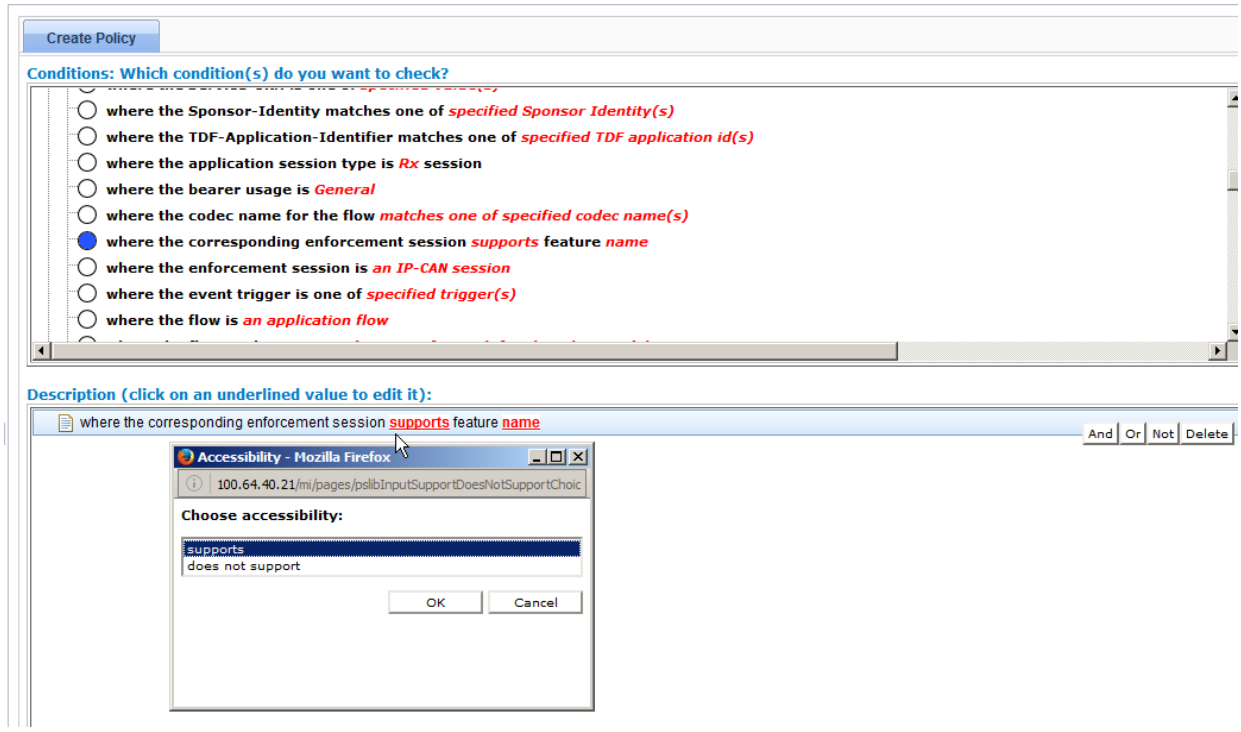
### 3.2.3.1 *Where the requested GCS Identifier matches one of value(s)*

**CMP GUI:** *Policy Managemenr → Policy Library → Policies*



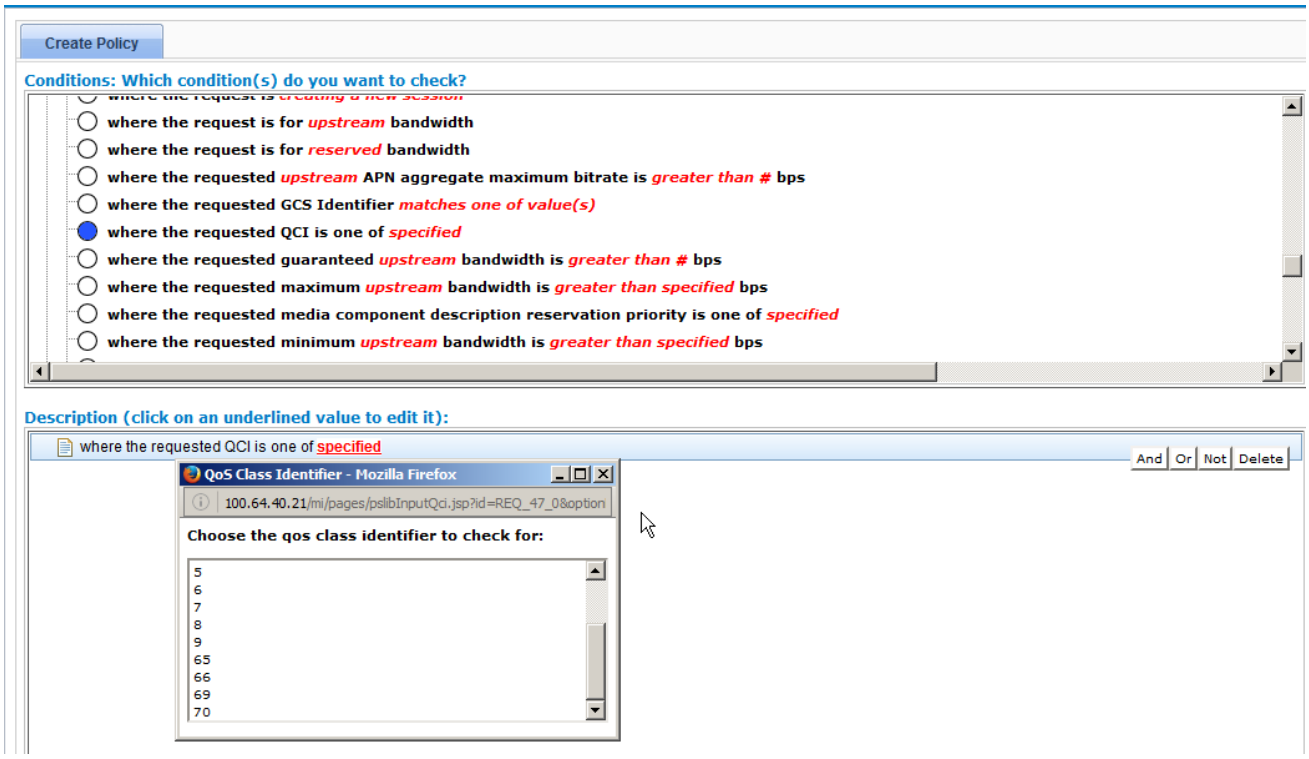

### 3.2.3.2 *Where the corresponding enforcement session supports feature name*

**CMP GUI:** *Policy Managemenr → Policy Library → Policies*



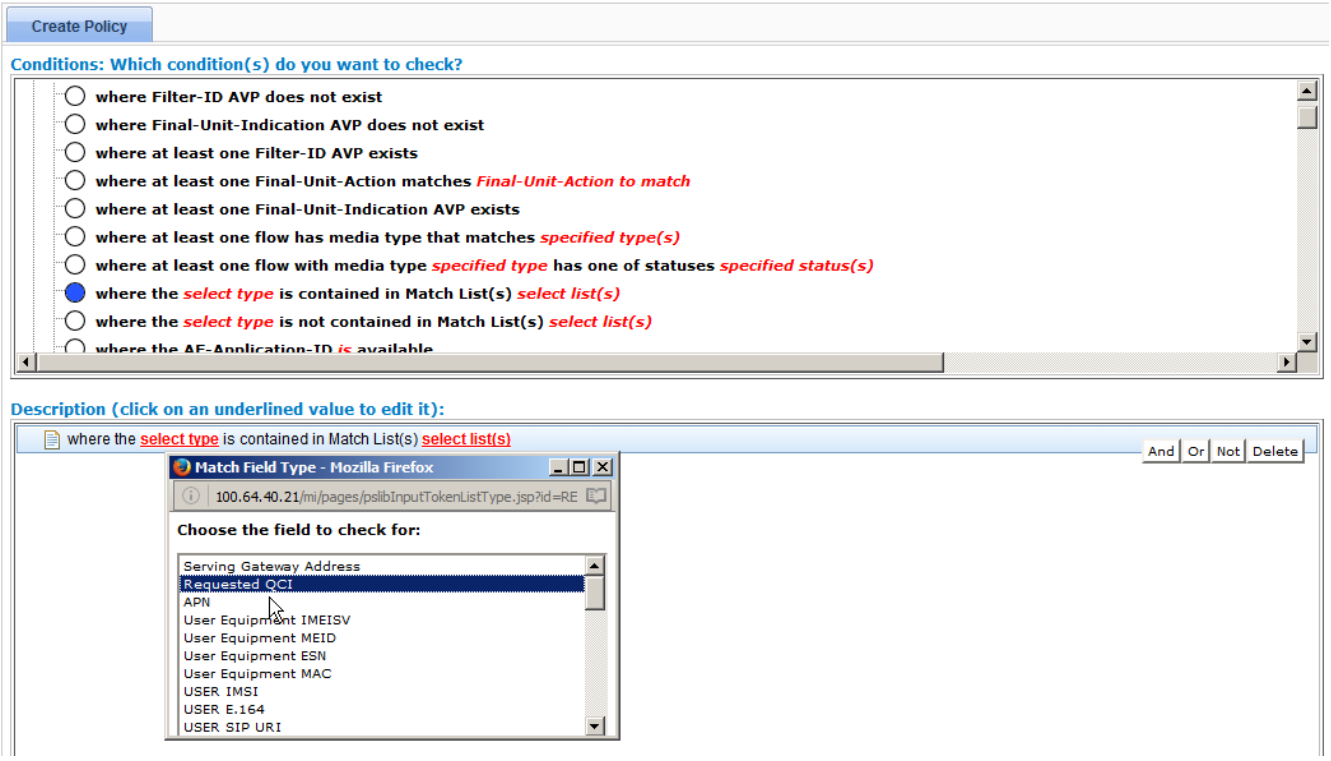
### 3.2.3.3 *Where the requested QCI is one of specified*

**CMP GUI:** *Policy Managemenr → Policy Library → Policies*




### 3.2.3.4 *Where the select type is contained in Match List(s) select list(s)*

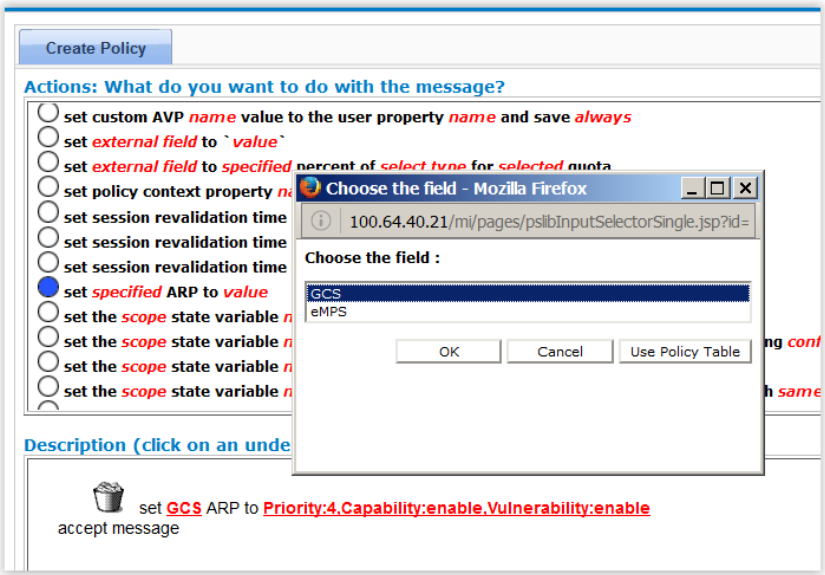
**CMP GUI:** *Policy Managemenr → Policy Library → Policies*




### 3.2.3.5 *Set specified ARP to value*

The GCS ARP value can also be overridden via the new policy action to be applied by default to PCC rules as well as to the default bearer per received GCS-Identifier and Reservation-priority AVP's

**CMP GUI:** *Policy Managemenr → Policy Library → Policies*



## 3.3 OPTIONS TO RESET PLAN FREQUENCY ( PR# 22114178 )

### 3.3.1 Introduction

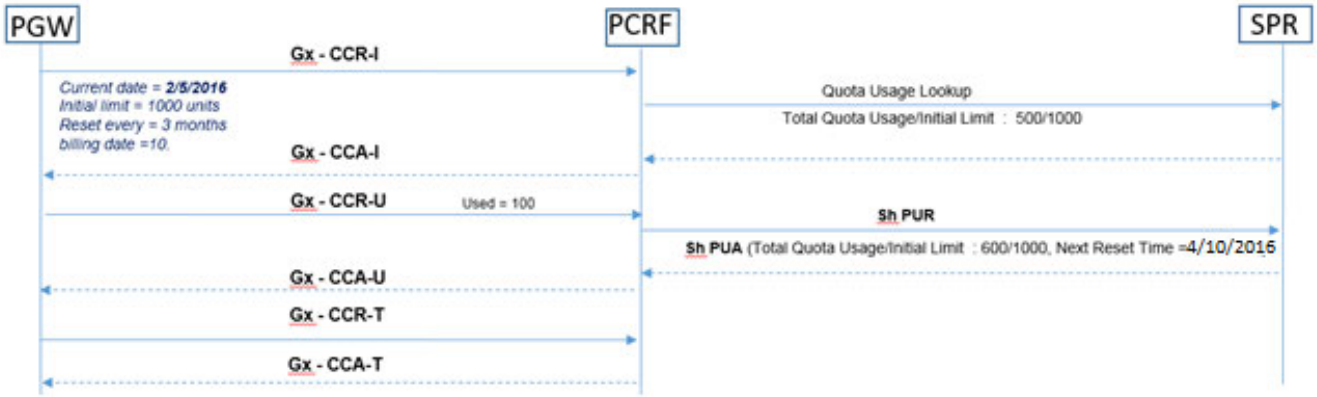
Currently, when defining a plan, the Policy Management Quota Profile Plan only provides daily/weekly/monthly options to reset the plan. Operators cannot specify 'n' number of days/weeks/months for which a plan can be reset.

### 3.3.2 Detailed Description

This new feature enhancement adding more flexibility with more granular for the period of time options. For example, it can be reset for every 'n' number of days, weeks or months such as every 4 days, 2 weeks, or 3 months etc.

As in the example shown below, the Billing Date is set at every 10th day of the month, and with the current date of 02/05/2016, therefore the Next Reset time will be of 04/10/2016. It's the third of 10th from the current date i.e.

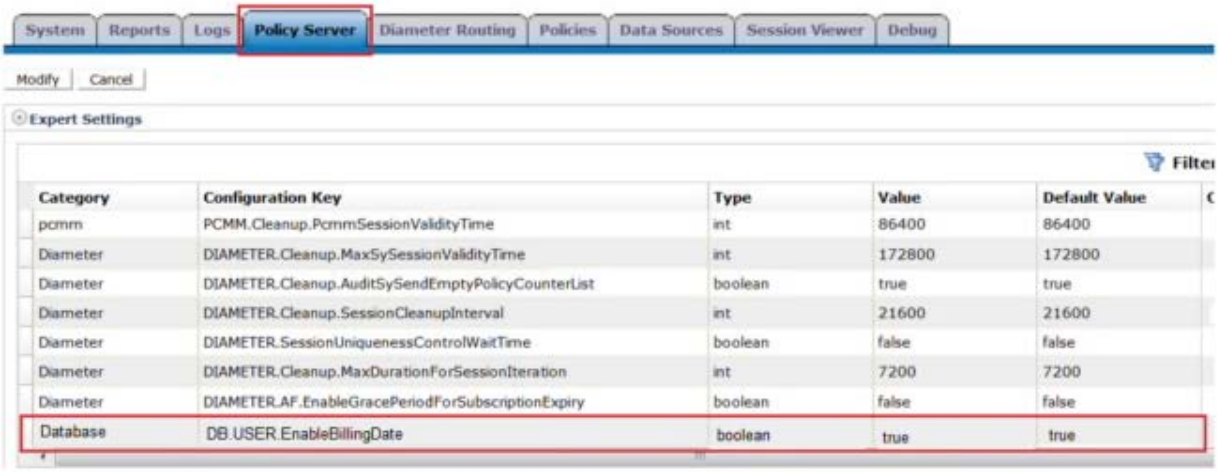
**1st** – 02/10/2016
**2nd** – 03/10/2016
**3rd** – 04/10/2016




### 3.3.3 User Interface Changes

A new Expert Setting Configuration Key of " **DB.USER.EnableBillingDate** " needs to be added in order to enable/disable this feature enhancement. It is set to "**true**" by default. This will result of that the 'Billing Date Effective Name' entered in the Subscriber's profile, will be used as a Plan Start Date to calculate the next reset time.

**CMP GUI:** Policy Server → Configuration → *( MPE cluster name )* → Policy Server → Advanced → Modify → Expert Settings




| Category | Configuration Key | Type | Value | Default Value |
|---|---|---|---|---|
| pcmm | PCMM.Cleanup.PcmmSessionValidityTime | int | 86400 | 86400 |
| Diameter | DIAMETER.Cleanup.MaxSySessionValidityTime | int | 172800 | 172800 |
| Diameter | DIAMETER.Cleanup.AuditSySendEmptyPolicyCounterList | boolean | true | true |
| Diameter | DIAMETER.Cleanup.SessionCleanupInterval | int | 21600 | 21600 |
| Diameter | DIAMETER.SessionUniquenessControlWaitTime | boolean | false | false |
| Diameter | DIAMETER.Cleanup.MaxDurationForSessionIteration | int | 7200 | 7200 |
| Diameter | DIAMETER.AF.EnableGracePeriodForSubscriptionExpiry | boolean | false | false |
| Database | DB.USER.EnableBillingDate | boolean | true | true |

It is recommended to enter a valid date for Billing Date Effective Name, so it can be used as Plan Start Date. If valid date is not entered, or the new Expert Setting Configuration key of '**DB.USER.EnableBillingDate**' is not set to "**true**", the time at which CCR-I is sent will be used to calculate as a basis for the next reset time.

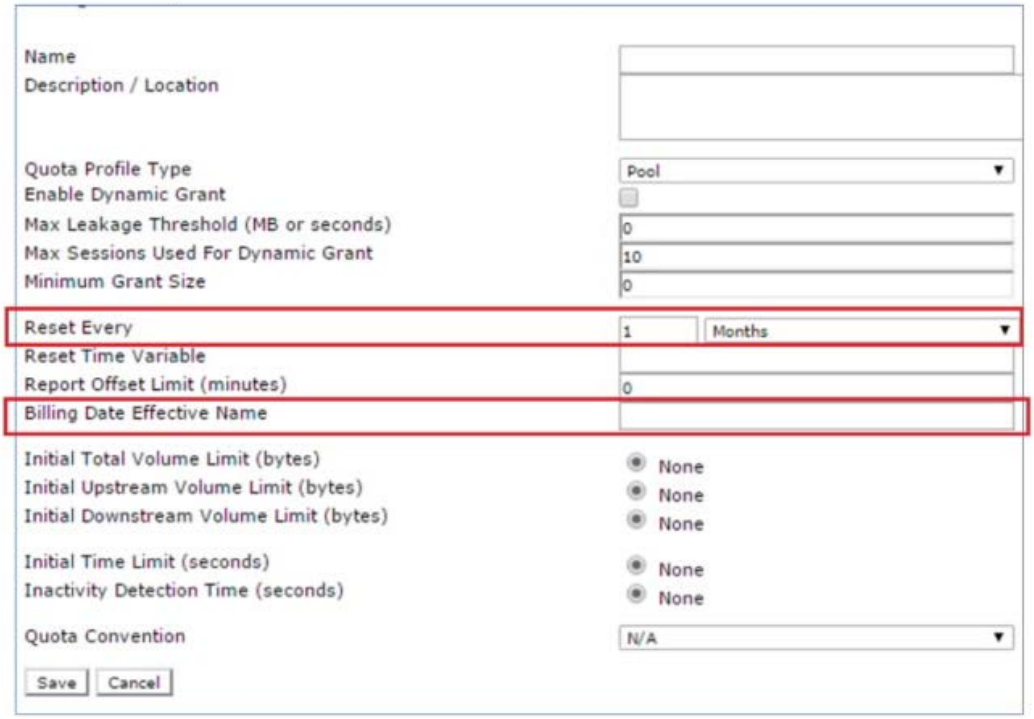
In addition, the '**Reset Frequency**' field label under Quota Profile Plan configuration is changed to '**Reset Every**', and a new input field is added where value input will indicate the 'number' of days/weeks/months that the plan will be reset. As for the yearly plan reset, multiple of '12' value for this new field of 'Months' can be entered accordingly. This new field is available for both Pool and Subscriber Quota Profile Type.

The new '**Reset Every**' parameter is initially set to value of "1" upon Policy Management system upgraded to Release 12.2.

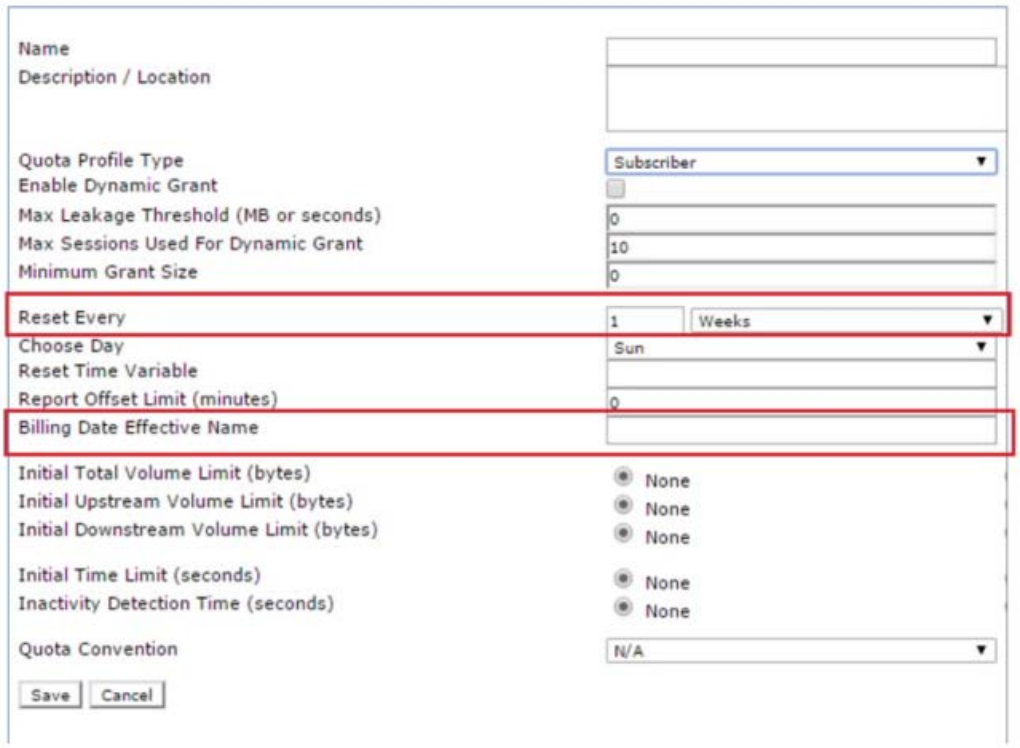
**CMP GUI:** Policy Server → Quota Profiles → Plans → *( plan name )* → Modify

As shown in the following examples –

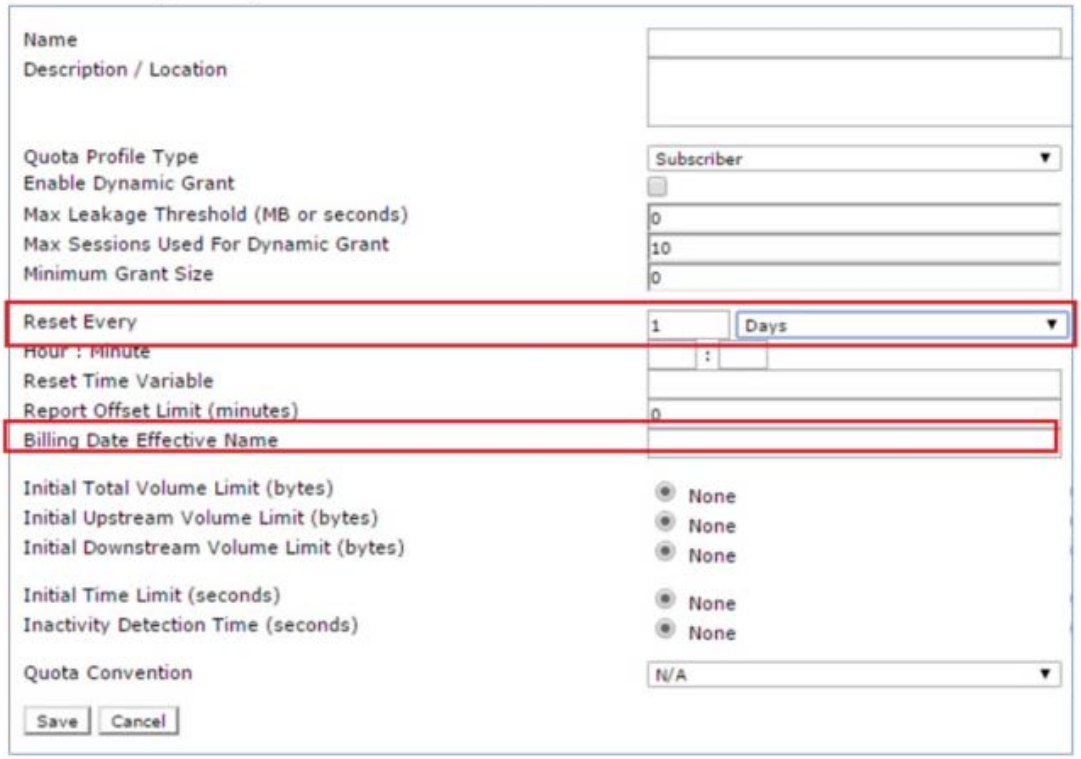
1. Reset Every - Months




2. Reset Every – Weeks



## 3. Reset Every – Day




Furthermore, Policy OSSI is updated to support the configuration of "Reset Frequency" parameter as shown below –


```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ConfigurationData version="12.2.0.0.0">
    <Quota>
        <Name>QuotaAfterCkpoint</Name>
        <Description></Description>
        <DynamicQuotaType>0</DynamicQuotaType>
        <Priority>0</Priority>
        <LimitTotalVolume>false</LimitTotalVolume>
        <LimitUpVolume>false</LimitUpVolume>
        <LimitDownVolume>false</LimitDownVolume>
        <TotalVolumeLimit>0</TotalVolumeLimit>
        <UpVolumeLimit>0</UpVolumeLimit>
        <DownVolumeLimit>0</DownVolumeLimit>
        <LimitTime>false</LimitTime>
        <TimeLimit>0</TimeLimit>
        <LimitTimeInactivity>false</LimitTimeInactivity>
        <TimeInactivity>0</TimeInactivity>
        <LimitEvent>false</LimitEvent>
        <EventLimit>0</EventLimit>
        <ReplenishingFrequency>0</ReplenishingFrequency>
        <VolumeThresholdPercentage>0.0</VolumeThresholdPercentage>
        <TimeThresholdPercentage>0.0</TimeThresholdPercentage>
        <EventThresholdPercentage>0.0</EventThresholdPercentage>
        <EnableInterimReporting>false</EnableInterimReporting>
        <InterimReportingInterval>0</InterimReportingInterval>
        <QuotaExhaustionAction>0</QuotaExhaustionAction>
        <RedirectServerType>1</RedirectServerType>
        <QuotaResetIntervalType>1</QuotaResetIntervalType>
        <ResetFreqMultiplier>58</ResetFreqMultiplier>
        <QuotaResetDayOfWeek>0</QuotaResetDayOfWeek>
        <QuotaResetTimeOfDay></QuotaResetTimeOfDay>
        <QuotaResetTimeVariable></QuotaResetTimeVariable>
        <QuotaReportOffsetLimit>0</QuotaReportOffsetLimit>
        <BillingDateEff></BillingDateEff>
        <QuotaType>0</QuotaType>
        <MaxLeakageThreshold>0</MaxLeakageThreshold>
        <EnableDynamicGrant>false</EnableDynamicGrant>
        <MaxSessionsUsedForDynamicGrant>10</MaxSessionsUsedForDynamicGrant>
        <MinGrantSize>0</MinGrantSize>
        <DurationUnitType>2</DurationUnitType>
        <DurationUnit>0</DurationUnit>
        <ActiveTimePeriod></ActiveTimePeriod>
        <ExpirationDateExtensionMethod>0</ExpirationDateExtensionMethod>
        <GroupName></GroupName>
    </Quota>
</ConfigurationData>
```

## 3.4 NOTIFICATION TRIGGERS FOR AGGREGATE QUOTA ( PR# 22258207 )

### 3.4.1 Introduction

Currently, policy conditions such as "**where the user is using greater than # percent of select type for selected quota**" do NOT take into account of any Top-up or Rollover limit setup in the quota plan. In other words, Subscriber usage percentage calculation only uses the base quota plan limit. Any usage notification triggers setup based on these calculations, may be triggered incorrectly from the Subscriber's point of view

This feature changes the outcome of those policy conditions to include all Top-ups and Rollovers usage and limits for the percentage calculation.. However, it will not alter existing Granting calculation for a subscriber session, thus the Grant values will be the same. Expired/Exhausted top-ups and Subscriber's Passes are not used in the calculation.

The policy conditions and actions which are impacted if this feature is enabled -

| Policy Condition Group | Policy Condition or Action |
|---|---|
| User Conditions | Where the user is using greater than specified percent of select type for selected quota |
| User Conditions | Where the user is using greater than specified percent and less than specified percent of select type for selected quota |
| User Conditions | Where the user is using greater than # units of total volume (bytes) for selected quota. |
| Policy Context Properties | The policy variable for User Quota usage:<br><br>*{User.Quota.<quotaname>.**Volume**}* looks at the usage for that particular quota. This is now enhanced to specify whether "**aggregated quota**" is requested or not.<br><br>*{User.Quota.<quotaname>.**Volume.aggregate**}* - Will fetch the aggregated usage value for that quota (included usage against top-ups and rollover).<br><br>*{User.Quota.<quotaname>.**Volume.noaggregate**}* - Will fetch only the usage against the basic quota limit and not aggregated i.e. the same behavior as it's existing basic context property and reserve for future usage.<br><br>The above implementation is also applicable for the policy variable of *{ User.Quota.<quotaname>.**Time** }*, so there will be the following enhanced variables:<br><br>*{ User.Quota.<quotaname>.**Time.aggregate** }, and*<br><br>*{ User.Quota.<quotaname>.**Time.noaggregate** }* |
| Policy Context Properties | The policy variable for Quota Profile limits:<br><br>*{Quota.Limit.<quotaname>.**Volume**}* looks at the quota limit for the quota profile with <quotaname>. This is now enhanced to specify whether "**aggregated quota**" is requested or not for the subscriber or pool quota.<br><br>*{Quota.Limit.<quotaname>.**Volume.aggregate**}*- Will fetch the aggregated limit for that quota profile and includes limits from top-ups and rollover defined for that Subscriber or Pool.<br><br>*{Quota.Limit.<quotaname>.**Volume.noaggregate**}*- Will fetch only the limit defined in the the basic quota and not aggregated i.e. the same behavior as it's existing basic |

| | |
|---|---|
| | context property and reserve for future usage.<br><br>The above implementation is also applicable for the policy variable of *{ Quota.Limit.<quotaname>.**Time** }* , so there will be the following enhanced variables:<br><br>*{ Quota.Limit.<quotaname>.**Time.aggregate** }*, *and*<br><br>*{ Quota.Limit.<quotaname>.**Time.noaggregate** }* |

In order to preserve backward compatibility, the current behavior can be preserved with a new checkbox field for "**Aggregate Quota**" left unchecked or set to false by default. Otherwise, then all Quota plans that use that Quota convention will have the new impelmentation.

The Export/Import of the Policies will include this new field.

The new field is also added to the OSSI output.

### 3.4.2 Detailed Description

Those above-mentioned policy conditions allow the Operator to specify percentage of usage to limit to be calculated and trigger the policy based on those.

*Example of use case-1 with the new feature -*

Let's say the policy condition is set as

*where the user is using greater than 80 percent and less than 90 percent of total volume for PoolQuota1 quota send SMS `80 percent quota reached.` to user. Request delivery receipt `default`.*

The *PoolQuota1* is defined as a Quota Plan with Initial Volume Limit 10MB. Now, the Subscriber purchased and activated two 5MB topups.

With existing implementation, it would send SMS when the usage reaches 8MB, which is 80% of the plan limit of 10MB.

With this feature enhancement, it would only send SMS when the usage reaches 16 MB, since the calculation for the 80% based on quota plan which now include the recently purchased topups i.e. (10MB + 5MB + 5MB=20MB ).

*Example of use case-2 with the new feature –*

Using the same policy conditions as outlined in use case-1. The PoolQuota1 is defined as a Quota Plan with Initial Volume Limit 10MB.

The Subscriber purchased two 5MB top-ups, but one of which is not activated yet and will be in a future date.

The Operator has *roll-over* enabled before top-ups, and has a roll-over of 2MB from the previous cycle.

The Subscriber has used up 10MB of basic plan quota before the next reset time, so is granted the 2MB from the roll-over. The Subscriber then used up 1MB from this rollover, so the total usage (basic plan usage + rollover usage) is 11MB.

The aggregate limit is ( basic plan limit + top-ups limit + roll-over limit) 10MB + 10MB + 2MB = 22MB. So, the usage percentage is calculated as (11MB / 22MB) * 100 = 50%.

Without "**Aggregate quota**" being enabled/checked, this would be computed as 100% as the user has used up the basic quota for the cycle.

*Example of use case-3 with the new feature –*

With the pro-rate is enabled, and user quota was pro-rated by a factor of 0.4. In this case, the Subscriber was not allotted the full quota grant of 10MB but only the pro-rated quota plan limit of 4MB.

The Subscriber has purchased and activated two 5MB top-ups. So, the new limit usage is now total of 14 MB ( the pro-rated quota plan limit of 4MB + top-ups limit of 10 MB )

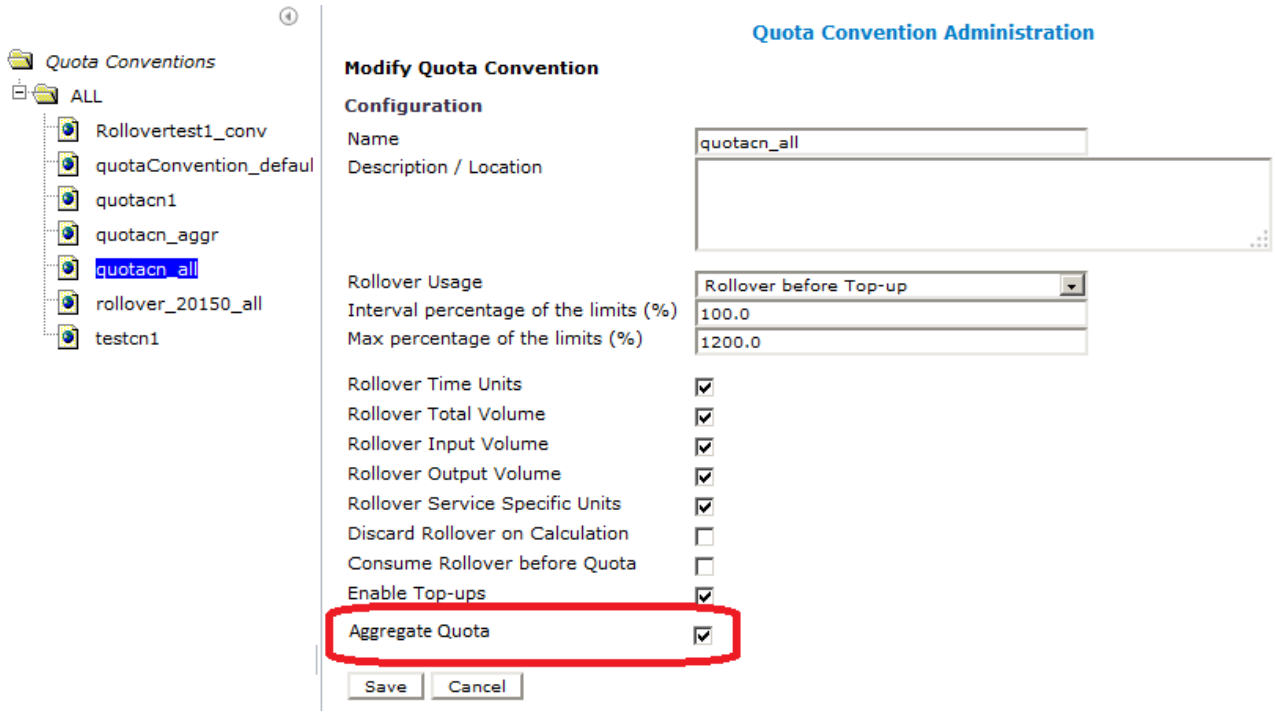
The Subscriber has used up 2MB. With the feature enabled, the percentage calcualtion is ( 2 MB / 14 MB ) = 14.28571%

**NOTE:** Top-ups and rollovers are not subject to pro-rating factor.

### *3.4.3 User Interface Changes*

A new checkbox field is added to CMP of Quota Conventions menu calls "**Aggregate Quota**". It is set disabled or unchecked, by default. So, the behavior of the two existing policy conditions is the same as is.

To enable this new feature enhancement, check on the "Aggregate Quota" box as shown in CMP GUI below -


Quota Convention Administration
Quota Conventions
ALL
Rollovertest1_conv
quotaConvention_defaul
quotacn1
quotacn_aggr
quotacn_all
rollover_20150_all
testcn1
Modify Quota Convention
Configuration
Name
quotacn_all
Description / Location
Rollover Usage
Rollover before Top-up
Interval percentage of the limits (%)
100.0
Max percentage of the limits (%)
1200.0
Rollover Time Units
Rollover Total Volume
Rollover Input Volume
Rollover Output Volume
Rollover Service Specific Units
Discard Rollover on Calculation
Consume Rollover before Quota
Enable Top-ups
Aggregate Quota
Save
Cancel

## 3.5 POLICY SUPPORT ON NETWORK ELEMENT'S IDENTITY ( PR# 20271484 )

### 3.5.1 Introduction

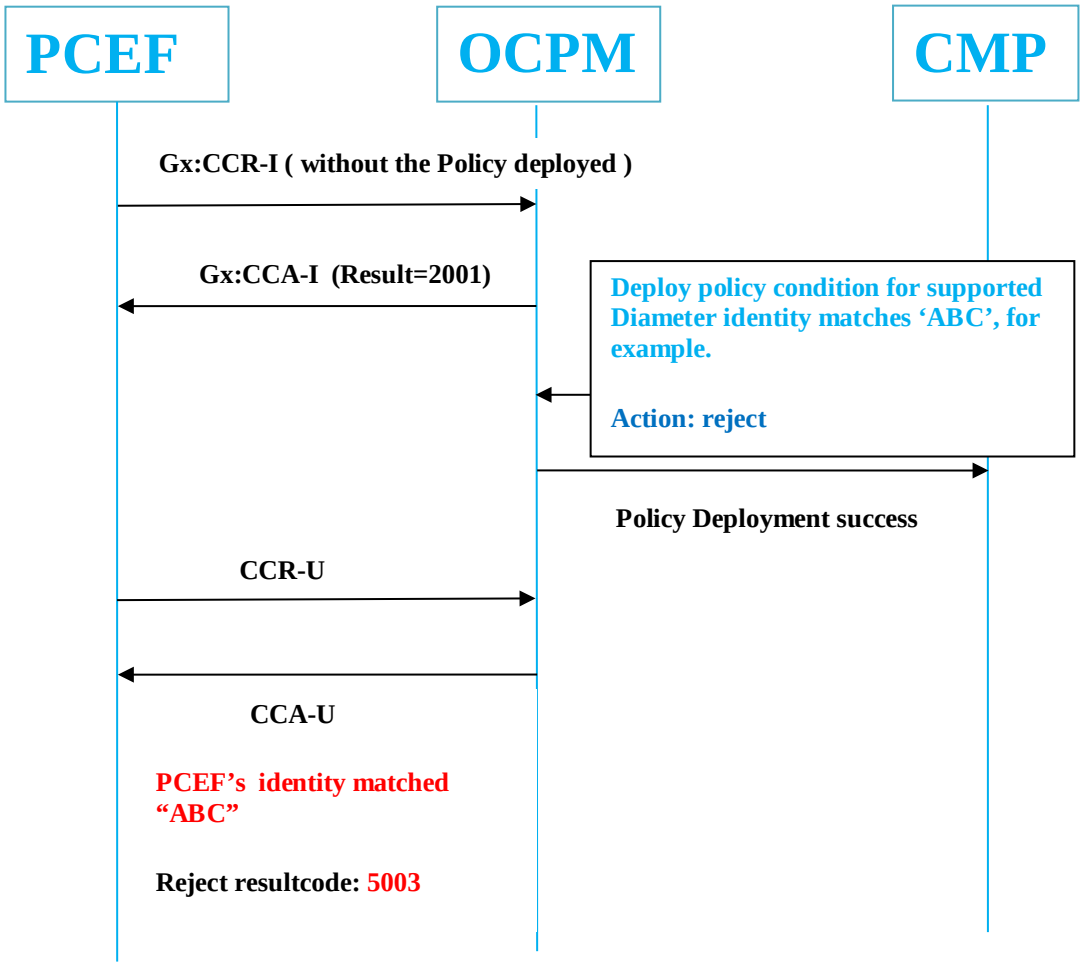
This feature introduces two new policy conditions to check for Diameter identity stated in "Origin Host" AVP of received Gx:CCR , Rx:AAR and Sd:CCR messages. Diameter Notification and Update messages are not supported.

### 3.5.2 Detailed Description

Here are the new Policy conditions –

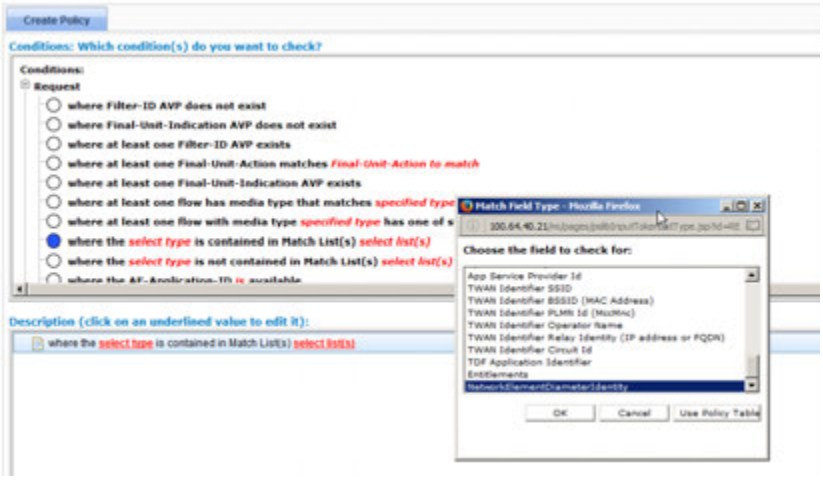
| Policy Condition | Description |
|---|---|
| where the ***select type*** is contained in Match List(s)<br>***select list(s)*** | *select type* = NE_IDENTITY<br>*select list(s)* = pre-defined Match List<br><br>This is to check whether the Network Element's Diameter Identity **matches** the one in pre-defined Match List. |
| where the ***select type*** is *not* contained in Match List(s)<br>***select list(s)*** | *select type* = NE_IDENTITY<br>*select list(s)* = pre-defined Match List<br><br>This is to check whether the Network Element's Diameter Identity **doesn't match** the one in pre-defined Match List. |
| where the network element's diameter identity<br>***matches one of specified name(s) /***<br>***does not match any of specified name(s)*** | This is to check whether the Network Element's Diameter Identity matches or not, to one of specified name(s), which can be comma separated string containing wildcards such as " * ", or " ? " |

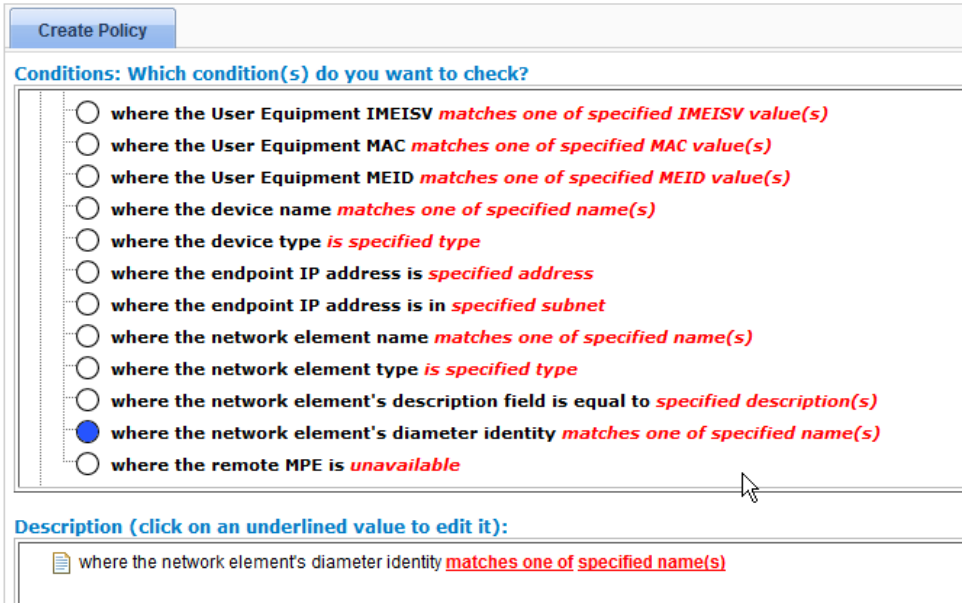
This can be illustrated in the following Call Flow –




### *3.5.3 User Interface Changes*

As can be seen in the Figure below, a new option named " **NetworkElementDiameterIdentity**" is added to the *select type* in the Policy Condition.


Create Policy
Conditions: Which condition(s) do you want to check?
Conditions:
Request
where Filter-ID AVP does not exist
where Final-Unit-Indication AVP does not exist
where at least one Filter-ID AVP exists
where at least one Final-Unit-Action matches Final-Unit-Action to match
where at least one Final-Unit-Indication AVP exists
where at least one flow has media type that matches specified type
where at least one flow with media type specified type has one of s
where the select type is contained in Match List(s) select list(s)
where the select type is not contained in Match List(s) select list(s)
Match Field Type - Mozilla Firefox
Choose the field to check for:
App Service Provider Id
TWAN Identifier SSID
TWAN Identifier BSSID (MAC Address)
TWAN Identifier PLMN Id (MccMnc)
TWAN Identifier Operator Name
TWAN Identifier Relay Identity (IP address or FQDN)
TWAN Identifier Circuit Id
TDF Application Identifier
Entitlements
NetworkElementDiameterIdentity
OK
Cancel
Use Policy Table
Description (click on an underlined value to edit it):
where the select type is contained in Match List(s) select list(s)


Create Policy
Conditions: Which condition(s) do you want to check?
where the User Equipment IMEISV matches one of specified IMEISV value(s)
where the User Equipment MAC matches one of specified MAC value(s)
where the User Equipment MEID matches one of specified MEID value(s)
where the device name matches one of specified name(s)
where the device type is specified type
where the endpoint IP address is specified address
where the endpoint IP address is in specified subnet
where the network element name matches one of specified name(s)
where the network element type is specified type
where the network element's description field is equal to specified description(s)
where the network element's diameter identity matches one of specified name(s)
where the remote MPE is unavailable
Description (click on an underlined value to edit it):
where the network element's diameter identity matches one of specified name(s)

## 3.6 SPECIFY GX AND RX RESULT CODES FOR MRA WHILE NO BINDING INFO ( PR# 19488243 & 20271501 )

### 3.6.1 Introduction

This feature allows MRA to return as configured Result-Codes (could be different from the default values ) when the MRA receives the supported Gx:CCR-U/CCR-T ; Rx:AAR-I/AAR-U/STR messages but can't find corresponded DRA binding information.

### 3.6.2 Detailed Description

Currently without the DRA binding information, the MRA is returning the following default Result-Codes –

Gx:CCA: Result-Code 0:5002 DIAMETER_UNKNOWN_SESSION_ID

Gx:CCA: Result-Code 0:5012 DIAMETER_UNABLE_TO_COMPLY

Gx:CCA:Result-Code 0:3002_DIAMETER_UNABLE TO DELIVER

Rx:AAA: Result-Code 10415:5065 IP_CAN SESSION_NOT_AVAILABLE

Rx:STA: Result-Code 0:5012 DIAMETER_UNABLE_TO_COMPLY

Furthermore, use **Reference [10]** and **[11]** for valid applicable configured Result Codes and CC/Rx-Request-Type respectively.

The following MRA Configuration keys should first set to enable the feature -

(1) **DIAMETERDRA.TopologyHiding.Enabled** should be set to "**true**",

**NOTE:** *This configuration key doesn't affect Rx:AAR-I message*

(2) And, **DIAMETERDRA.TopologyHiding.Apps** could contain values of "**Gx,Rx**", OR either "**Gx**" or "**Rx**", OR "*****" for all

Next, in order to override the above-mentioned default returned Result-Codes, configure the following MRA Configuration Keys:

(1) **DIAMETERDRA.NoBindingInfo.ResultCodeRuleIndexLimit** – *default value is 10. The value of this configuration is to limit the maximum number of Rules' index as shown in the next Configuration Key in (2) below. Any Rule index number exceeds the RuleIndexLimit value, will NOT be executed. In other words, if the default limit value of 10 is configured, the RuleIndexNumber of 11 and beyond, won't have any effect.*

(2) **DIAMETERDRA.NoBindingInfo.ResultCodeRulePrefix** – *applicable for all received Gx and Rx:STR messages. The value of this is the prefix of configuration's key which is used to specify the Result Code rules containing one **Filter** prefix and one **Action** prefix with the following formats –*

– *[Prefix][IndexNumber].filter=App/MessageType/AVPList. Use Reference [11] and [12], Section 8.3 and Section 5.6.5 respectively.*

– *[Prefix][IndexNumber].action=VendorId:DiameterResultCode.. Use Reference [10], Section 7.1*

As shown in the following configuration example –

DIAMETERDRA.NoBindingInfo.**ResultCodeRule1.Filter**=Gx/CCR/CC-Request-Type=2
DIAMETERDRA.NoBindingInfo.**ResultCodeRule1.Action**=0:5007
DIAMETERDRA.NoBindingInfo.**ResultCodeRule2.Filter**=Gx/CCR/CC-Request-Type=3
DIAMETERDRA.NoBindingInfo.**ResultCodeRule2.Action**=10415:5141
DIAMETERDRA.NoBindingInfo.**ResultCodeRule3.Filter**=Rx/AAR/Rx-Request-Type=0
DIAMETERDRA.NoBindingInfo.**ResultCodeRule3.Action**=10415:5064
DIAMETERDRA.NoBindingInfo.**ResultCodeRule4.Filter**=Rx/AAR/Rx-Request-Type=1
DIAMETERDRA.NoBindingInfo.**ResultCodeRule4.Action**=99999:9999
DIAMETERDRA.NoBindingInfo.**ResultCodeRule5.Filter**=Rx/STR[1]
DIAMETERDRA.NoBindingInfo.**ResultCodeRule5.Action**=98765:1234

[1]*Exception for App/MessageType format.*
*Refer RFC-4006, Section 8.3 for CC-Request-Types AVP*
*Refer ETSI TS 129.214 V11.6.0, Section 5.3.31 for Rx-Request-Types AVP*

(3) **DIAMETERDRA.NoBindingInfo.ResultCodeForRxAARWithDestinationHost** – *applicable for received Rx:AAR with Destination-Host AVP from AF ( P-CSCF) without Rx-Request-Type AVP.*

(4) **DIAMETERDRA.NoBindingInfo.ResultCodeForRxAARWithoutDestinationHost -** *applicable for received Rx:AAR without Destination-Host AVP from AF ( P-CSCF) and without Rx-Request-Type AVP.*

### 3.6.3 User Interface Changes

**CMP GUI:** *MRA → Configuration → ( Select MRA cluster name ) → MRA → Advanced → Modify → Service Overrides → Add*

As shown in the example below -

Service Overrides

| Category | Configuration Key | Type | Value | Default Value |
|---|---|---|---|---|
| DIAMETERDRA.NoBin | DIAMETERDRA.NoBindingInfo.ResultCodeRuleIndexL | int | **5** | 10 |
| DIAMETERDRA.Topol | DIAMETERDRA.TopologyHiding.Apps | String | Gx,Rx | Gx,Rx |
| DIAMETERDRA.Topol | DIAMETERDRA.TopologyHiding.Enabled | boolean | **true** | false |

Service Overrides

Filter

| Category | Configuration Key | Type | Value | Default Value | C |
|---|---|---|---|---|---|
| | DIAMETERDRA.NoBindingInfo.ResultCodeRule2.Actio | | *0:5012* | *Undefined* | |
| | DIAMETERDRA.NoBindingInfo.ResultCodeRule2.Filter | | *Rx/AAR/Rx-Request-Type=0* | *Undefined* | |
| | DIAMETERDRA.NoBindingInfo.ResultCodeRule1.Actio | | *0:5002* | *Undefined* | |
| | DIAMETERDRA.NoBindingInfo.ResultCodeRule1.Filter | | *Gx/CCR /CC-Request-Type=1* | *Undefined* | |

This is no

## 3.7 INCLUSION OF MSISDN IN SUBSCRIPTION-ID AVP OF GX:CCR-I INTERFACE FOR OCS LOOKUP ( PR# 22264564 )

### 3.7.1 Introduction

This feature enhancement allows Policy Management to use the MSISDN value received in Gx:CCR-I message to query the OCS for Policy Counter information, when the Policy Management does NOT receive an MSISDN value from the following scenarios either –

1. UDA/SNA response from HSS/SPR.; or
2. HSS/SPR does not send UDA/SNA response, and Sy Data Source is defined as "on-demand" and "Validate User" set to false .

### 3.7.2 Detailed Description

Currently, when Policy Management retrieves Policy Counter information from an OCS based of the MSISDN value received from the SPR/HSS, as shown below in Figure 3 with the following assumption of either -

- The OCS is provisioned as a secondary data source using MSISDN as the Subscriber key; or
- OCS lookup is triggered by policy execution.

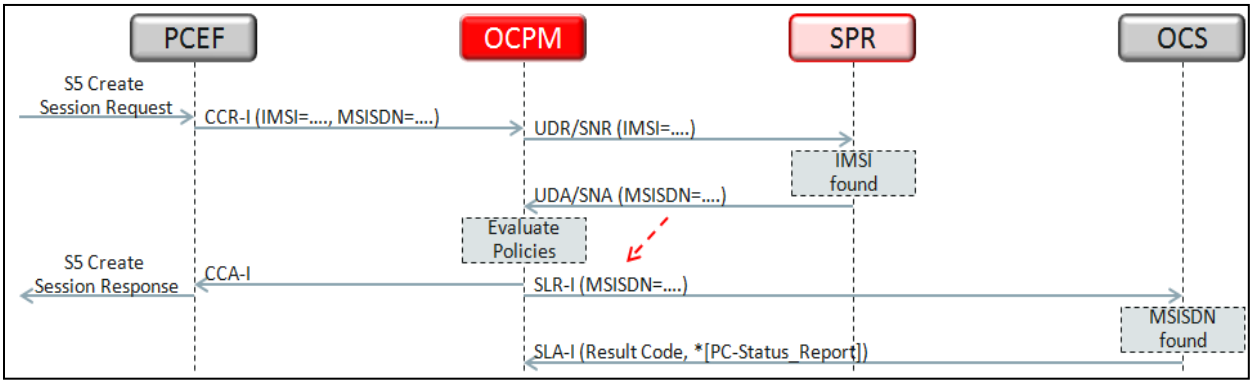



*Figure 3: OCS Query Based on MSISDN Received in Sh:UDA/SNA (SPR Response)*

Otherwise, the Policy Management will not attempt to retrieve Policy Counter information from the OCS.

So, this feature enhancement allows Policy Management to use the MSISDN in the received Gx:CCR-I message to query the OCS as shown below in Figure 4.

In a typical Gx:CCR-I message, the IMSI and MSISDN values can be included via separate instances of the Subscription-ID AVP as described in RFC-4006.

```
Subscription-Id ::= < AVP Header: 443 >
                    { Subscription-Id-Type }
                    { Subscription-Id-Data }
```

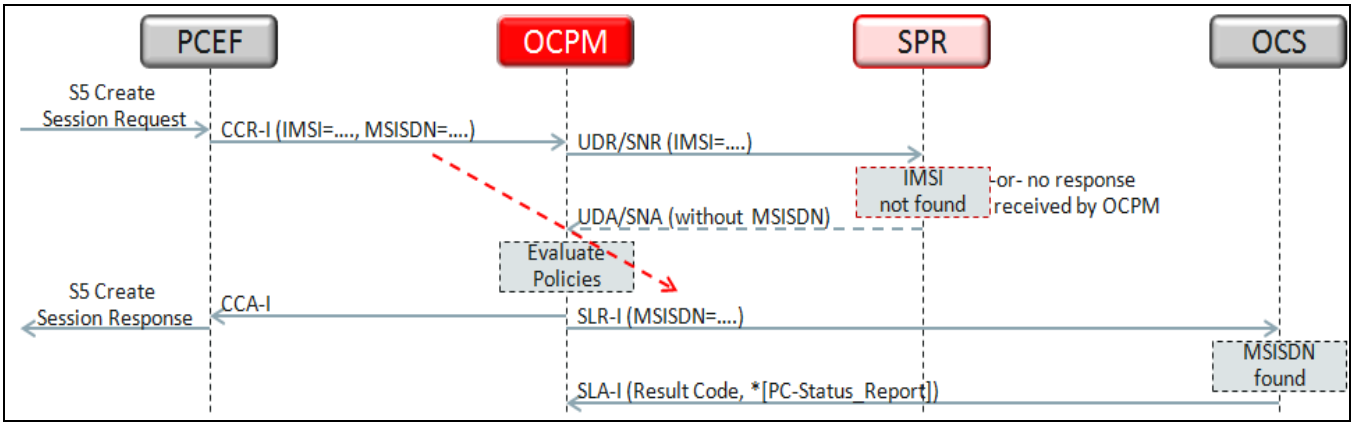



***Figure 4: OCS Query Based on MSISDN Received in Gx:CCR-I***

If the MSISDN value does not exist in the OCS from either case, then the Subscriber session must be established without the Policy Counter information, as shown below. This is the same behaviour as current implementation.

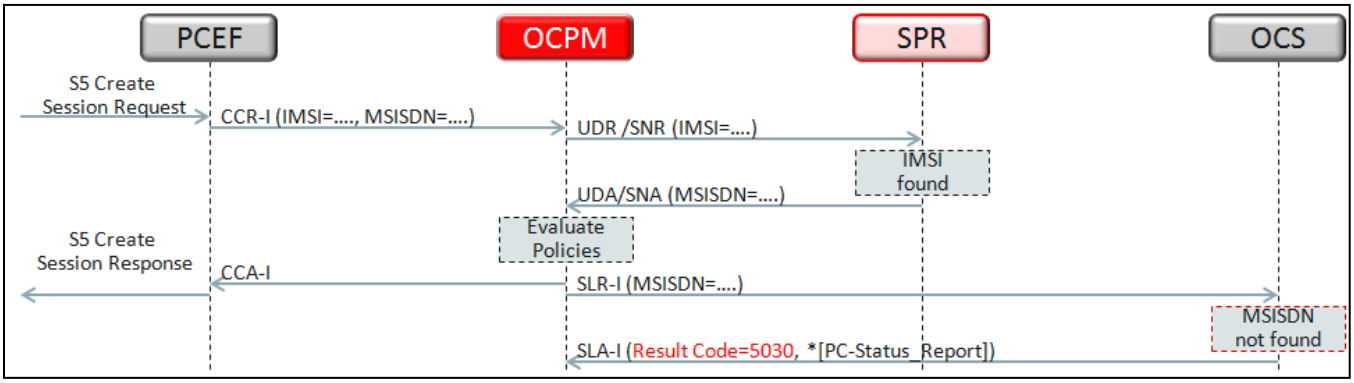



***Figure 5: OCS Query ( in this example is based on HSS/SPR response) with Unknown MSISDN. The SLA-I response from OCS will be the same as with MSISDN value retrieved from Gx:CCR-I message.***

### *3.7.3 User Interface Changes*

NONE

## 3.8 PCMM MESSAGES PER MPE AND PER CMTS STATISTICS VIA OSSI/XML ( PR# 20162894 )

### 3.8.1 Introduction

Currently, there are multiple PCMM sessions related statistics displayed in CMP GUI like Gate set/info/delete messages counts and errors counters. These counters are presented on configured MPE level as well as CMTS level.

This new feature further provides the capability of extracting these statistics fed through OSSI/XML.

### 3.8.2 Detailed Description

A new OSSI interface "**PcmmCmtsGateStats**" is created as part of this feature release to collect the messages count for each of the following messages kinds per CMTS:

1) Gate set
2) Gate info
3) Gate delete

The "**OssiXmlOm.xsd**" XML schema definition file used by OSSI is modified to cater for these statistics collection.

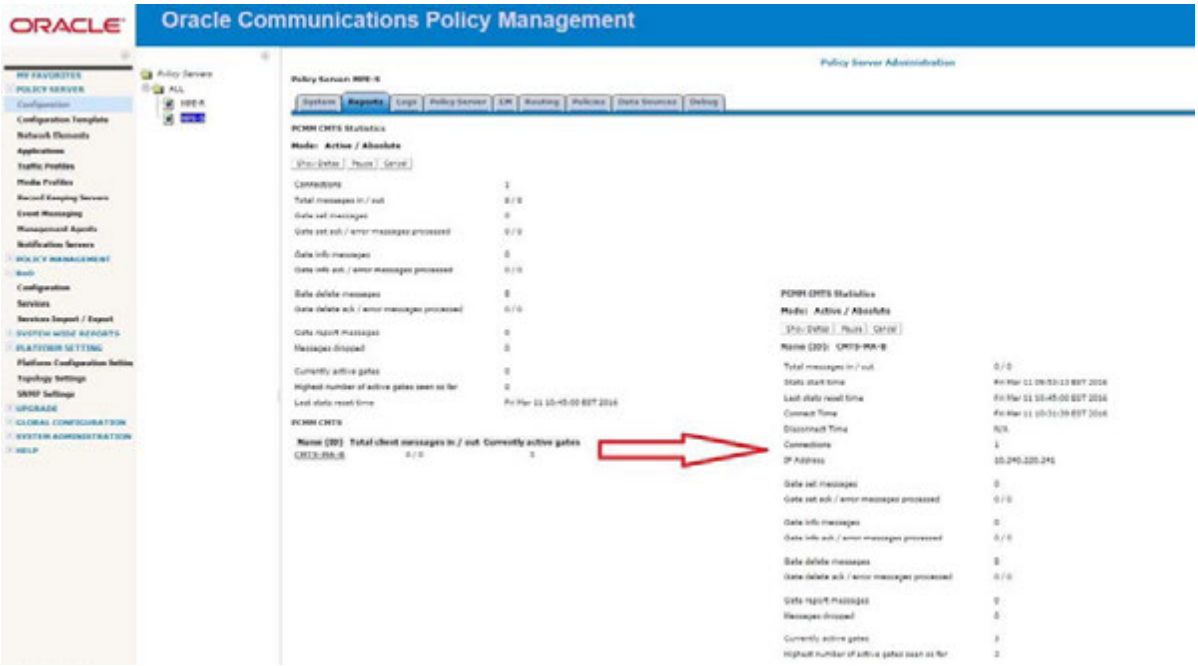
An example request for PCMM Gates stats for 'CMTS-12-2' network element as shown -

```
<?xml version="1.0" encoding="UTF-8"?>
<XmlInterfaceRequest>
<QueryOmStats>
<StartTime>2015-08-03T00:01:00</StartTime>
<EndTime>2015-08-08T23:59:00</EndTime>
< PcmmCmtsGateStats >
<PolicyServer>MPE1</PolicyServer>
<Name>CMTS-12-2</Name>
</ PcmmCmtsGateStats >
</QueryOmStats>
</XmlInterfaceRequest>
```

### 3.8.3 User Interface Changes

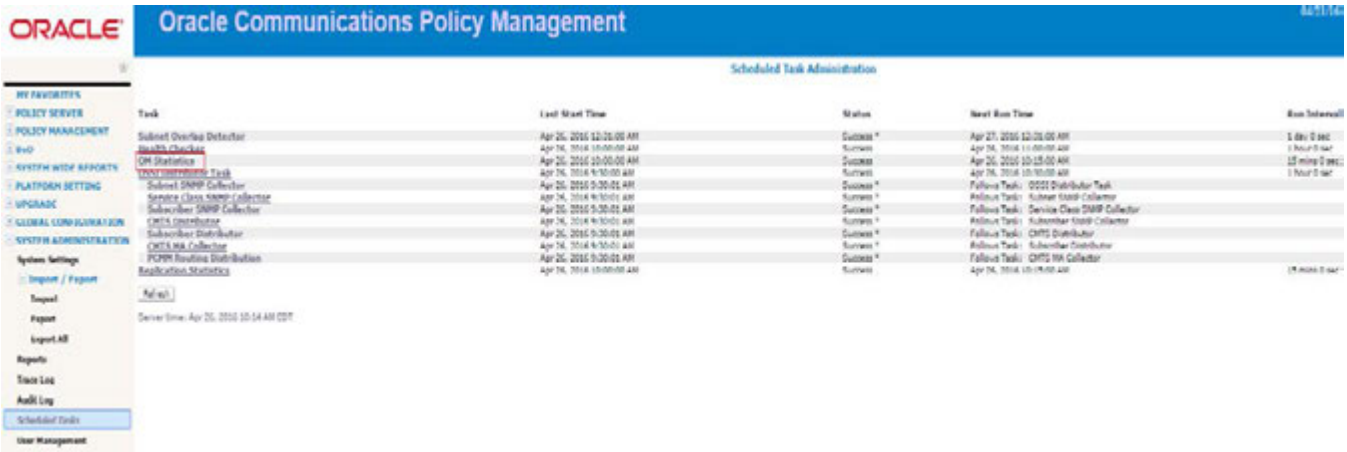
The data provided will be equivalent to what is presented in the following GUI:

**CMP GUI:** *Policy Server → Configuration → <Configured MPE> → Reports → PCMM CMTS Statistics → PCMM CMTS*




These statistical data are collected as part of all Operational and measure statistics collected by "**OM Statistics**" scheduled task under the following GUI:

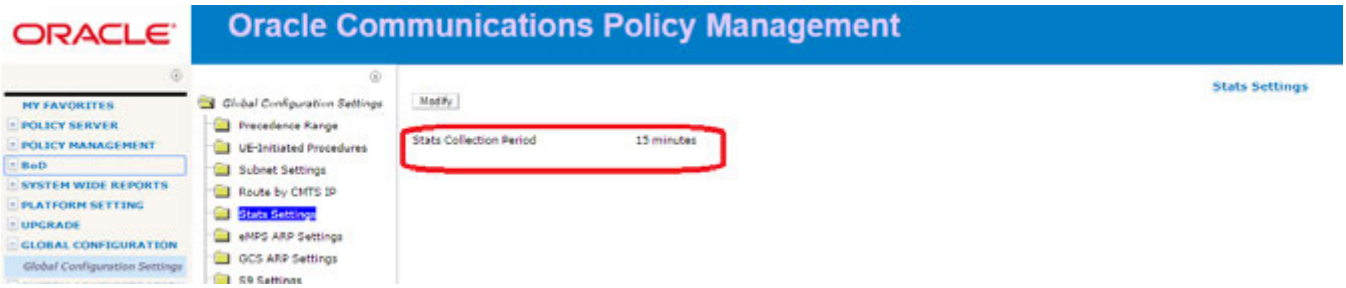
**CMP GUI:** *System Administration → Scheduled Tasks*



The reports data counters are collected throughout an interval of time as configured in the following GUI:

**CMP GUI:** *global configuration → global configuration settings → stats settings*

- default value is 15 minutes



## 3.9 PROVIDE NUMBER OF ACTIVE GATES PER AMID AND PER MPE VIA OSSI/XML ( PR# 20162817 )

### 3.9.1 Introduction

Currently, the MP GUI displays statistics on PCMM active gates per AMID, these counters are presented on configured MPE level.

This feature extends the capability of extracting these statistics to be fed through OSSI/XML.

### 3.9.1 Detailed Description

A new OSSI interface "**PcmmAmGateStats**" is created as part of this feature release to collect the messages count for each of the following messages kinds per CMTS:

1) Gate set
2) Gate info
3) Gate delete

The "**OssiXmlOm.xsd**" XML schema definition file used by OSSI is modified to cater for these statistics collection.

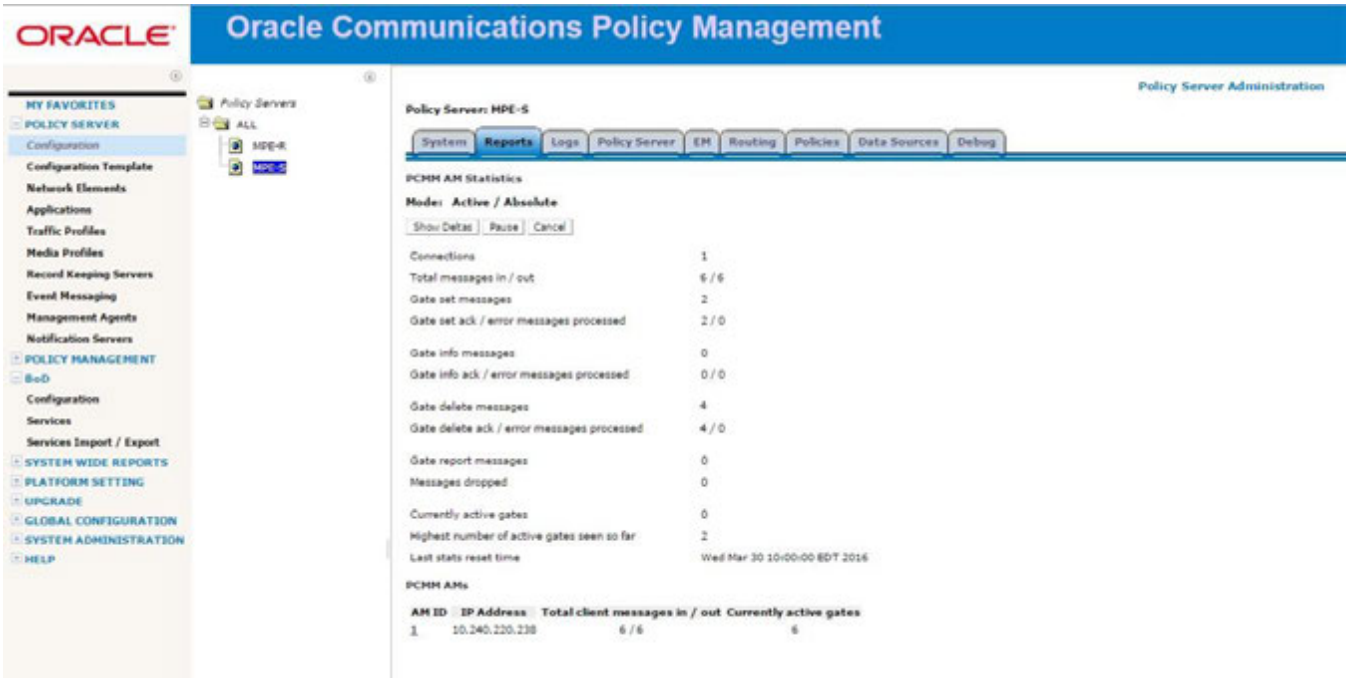
An example request for PCMM AM Gates stats for 'Atlanta105' policy Server as shown -

```
<?xml version="1.0" encoding="UTF-8"?>
<XmlInterfaceRequest>
 <QueryOmStats>
 <StartTime>2015-08-03T00:01:00</StartTime>
 <EndTime>2015-08-08T23:59:00</EndTime>
 < PcmmAmGateStats >
 <PolicyServer>Atlanta105</PolicyServer>
 <Name>1</Name>
 </ PcmmAmGateStats >
 </QueryOmStats>
</XmlInterfaceRequest>
```

### 3.9.2 User Interface Changes

The data provided will be equivalent to what is presented in the following GUI:

**CMP GUI:** *Policy Server → Configuration → <Configured MPE> → Reports → PCMM AM Statistics → PCMM AM*

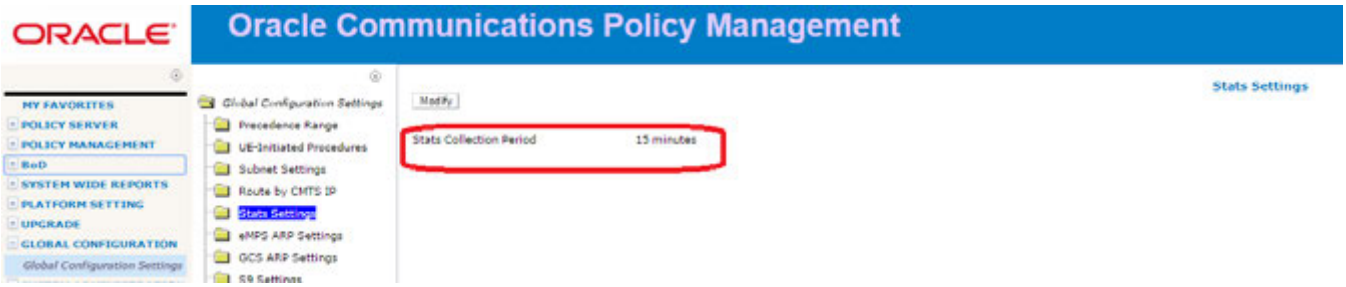



These statistical data are collected as part of all Operational and Measure ( OM) statistics collected by "**OM Statistics**" scheduled task in CMP GUI: *System Administration → Scheduled Tasks*


The reports data counters are collected throughout an interval of time configured in the following –

**CMP GUI:** *Global Configuration → Global Configuration Settings → Stats Settings*

Default value is 15 minutes.


ORACLE
Oracle Communications Policy Management
MY FAVORITES
POLICY SERVER
POLICY MANAGEMENT
BoD
SYSTEM WIDE REPORTS
PLATFORM SETTING
UPGRADE
GLOBAL CONFIGURATION
Global Configuration Settings
Global Configuration Settings
Precedence Range
UE-Initiated Procedures
Subnet Settings
Route by CMTS IP
Stats Settings
eMPS ARP Settings
GCS ARP Settings
Modify
Stats Collection Period
15 minutes
Stats Settings

## 3.10 DISCOVER CMTS SUBNETS WHEN SAVING A NEWLY CREATED NETWORK ELEMENT ( PR# 20286860)

### 3.10.1 Introduction

This feature enhance the functionality of creating new CMTS network elements via OSSI/XML to additionally discover the subnets associated to this new CMTS and push the new and modified subnets to the relevant MPE(s).

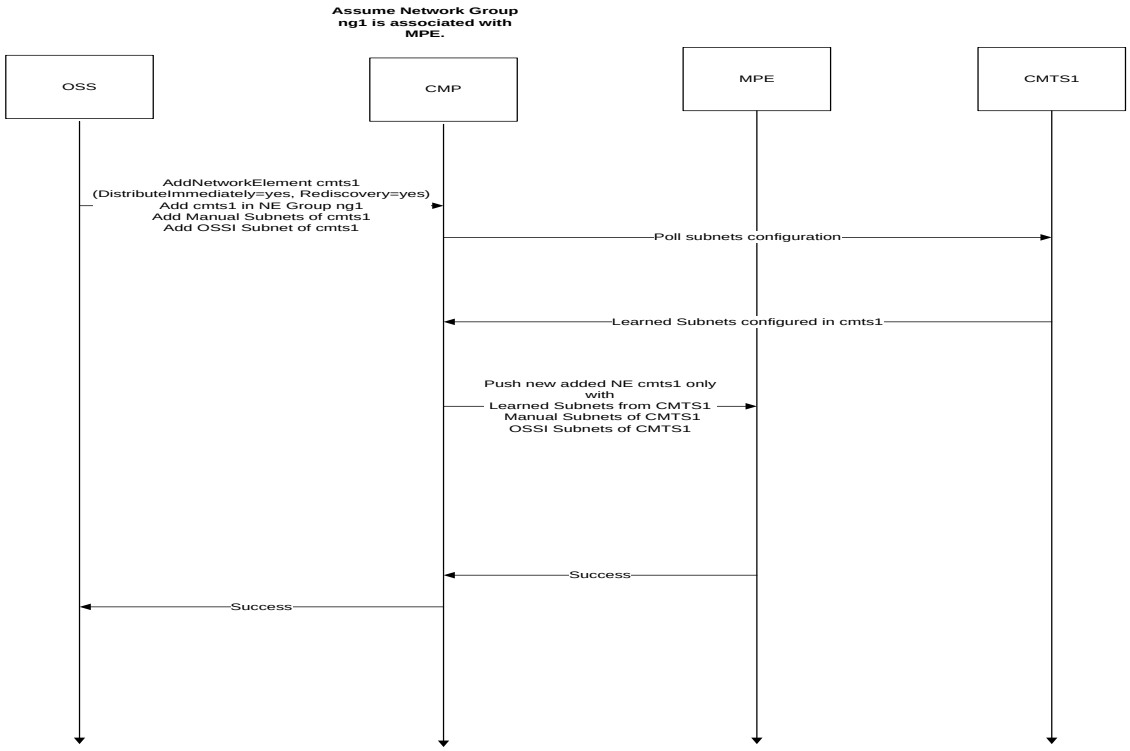
When provisioning a new CMTS via OSSI/XML interface command, CMP will learn CMTS's subnet configuration via SNMP service and push them to associated MPE cluster(s).

### 3.10.2 Detailed Description

To support OSSI trigger re-discovery CMTS subnet via SNMP, The new attributes 'Rediscovery' and 'DistributeImmediately' will be supported in QueryNetworkElement, AddNetworkElement and UpdateNetworkElement OSSI requests.

If Rediscovery attribute value is set to 'yes', AddNetworkElement and UpdateNetworkElement request will also trigger CMP re-discovery after CMP create or modify CMTS requests.

After the re-discovery of the subnets associated with the new CMTS, CMP trigger subnet information push to MPE via SNMP interface and return back CMTS subnets information in OSSI response. Following an illustrative flow showing the process of discovering the subnets associated with a newly added CMTS (CMTS1) and CMP pushing only the new learned subnets to MPE:



### *3.10.3 User Interface Changes*

NONE

## 3.11 STATISTICS RESET MODE UNIFICATION ( PR# 22534128)

### 3.11.1 Introduction

Previously Oracle Communications Policy Manager used to provide 2 reset modes for statistics and counters displayed in CMP GUI:

1. Manual Reset
2. Interval Reset

This feature phase out the manual reset technique for statistics and counters leaving only the interval reset technique.

This applies to both modes Cable and Wireless

### 3.11.2 Detailed Description

With manual reset technique, all the statistics and counters were reset only by customer manually or with system restart or upgrade.

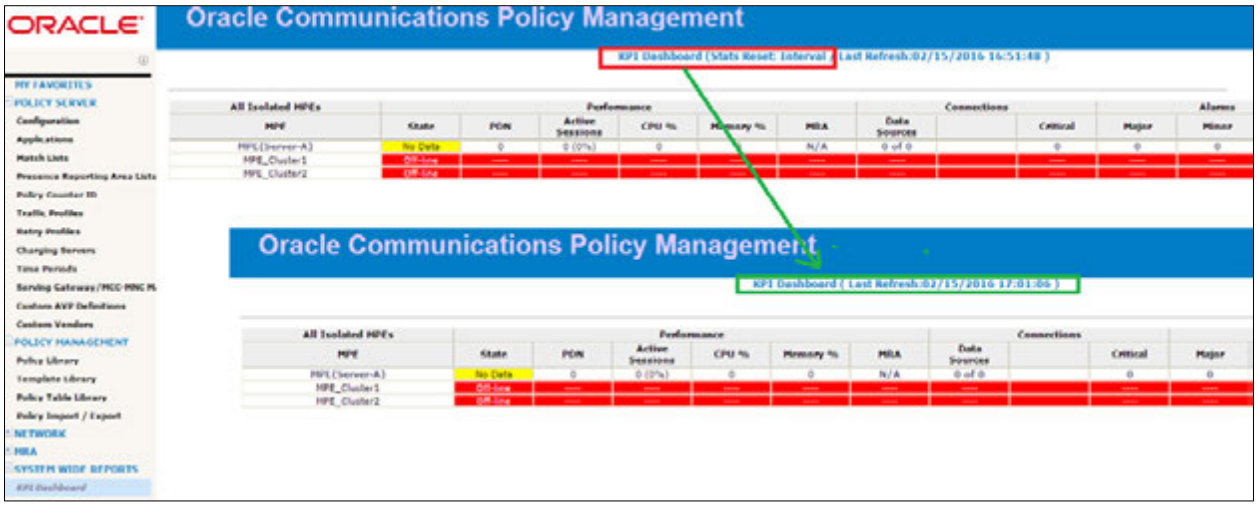
CMP GUI is updated by removing “Reset Counts” and “Reset All Counts” buttons of multiple reports and statistics pages so as to enable statistics reset by interval only.

At the beginning of each interval, all counters and statistics will reset automatically to Zero and start counting thereafter. In the mean time , all previous/historical interval data will be stored in COMCOL database.

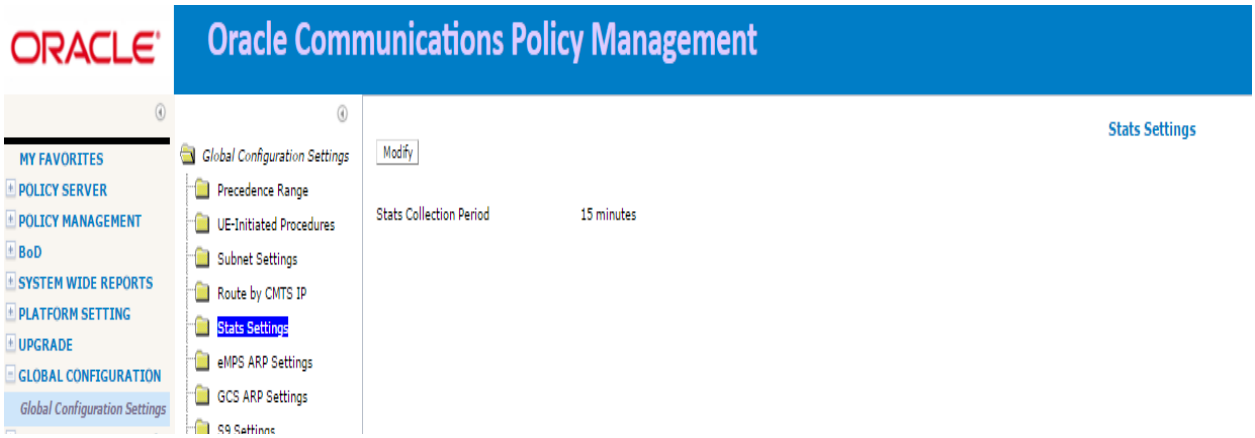
CMP will then retrieve these historical interval date from COMCOL and store it in MySql database table. These historical data is kept for 24 hours.

### 3.11.3 User Interface Changes

As a reason of this feature, CMP screens headings will not include statistics reset mode used any more:




Statistics settings is also removed from global configuration to enable only interval statistics collection by default: Global Configuration -> Global Configuration Settings -> Stats Settings



## 3.12 BOD ENHANCEMENTS ( PR# 20287350)

### 3.12.1 Introduction

This feature provides the ability of extracting multiple BOD related counters and statistics that are displayed in CMP GUI via OSSI/XML interface.

In addittion, BOD will introduce new statistics counting PCMM error messages categorized by error code that is displayed in the reports tab of configured BOD cluster in CMp GUI.

Also, as part of BOD enhancements in this release, BOD notification is enhanced in case of session early termination to send more details as part of the notification message sent out, early termination applies to sessions which expires before its entire assigned duration at session creation.

### 3.12.2 Detailed Description

As part of this feature, a set of existing BOD reports that are in CMP GUI will be available to be exported and fed into other customer's reporting or management systems via OSSI/XML including:

1. BOD PCMM gates stats
2. BOD PCMM gates stats by AMID
3. BOD PCMM sessions stats by AMID
4. BOD failed sessions stats by failure reason
5. BOD PCMM gates report stats
6. BOD HTTP requests and responses stats
7. BOD SOAP requests and responses stats

A BoD session may encounter several errors during its life cycle. In such cases, BoD uses its state machine mechanism to determine if the error can be recovered. Sessions that CANNOT be recovered are counted in "Failed Sessions". And the error which brings the session into an unrecoverable state is the "Failed Reason" of the session.

If a session involves both upstream and downstream Gates, and the two Gates fail on different reasons, the failed reason of the session is summarized by following priorities:

- The un-recoverable error takes the highest priority, if the two errors has the same priority
- The error of upstream Gate takes higher priority

A BoD session may encounter several errors during its life cycle. In such cases, BoD uses its state machine mechanism to determine if the error can be recovered. Sessions that CANNOT be recovered are counted in "Failed Sessions". And the error which brings the session into an unrecoverable state is the "Failed Reason" of the session.

Early Termination occurs when BoD receives a GateReport from CMTS and decides to terminate the session before the actual time assigned to this session is exhausted.

The details of GateReport message that triggers early terminations are valid Session ID and valid Gate ID and either one of the following conditions:

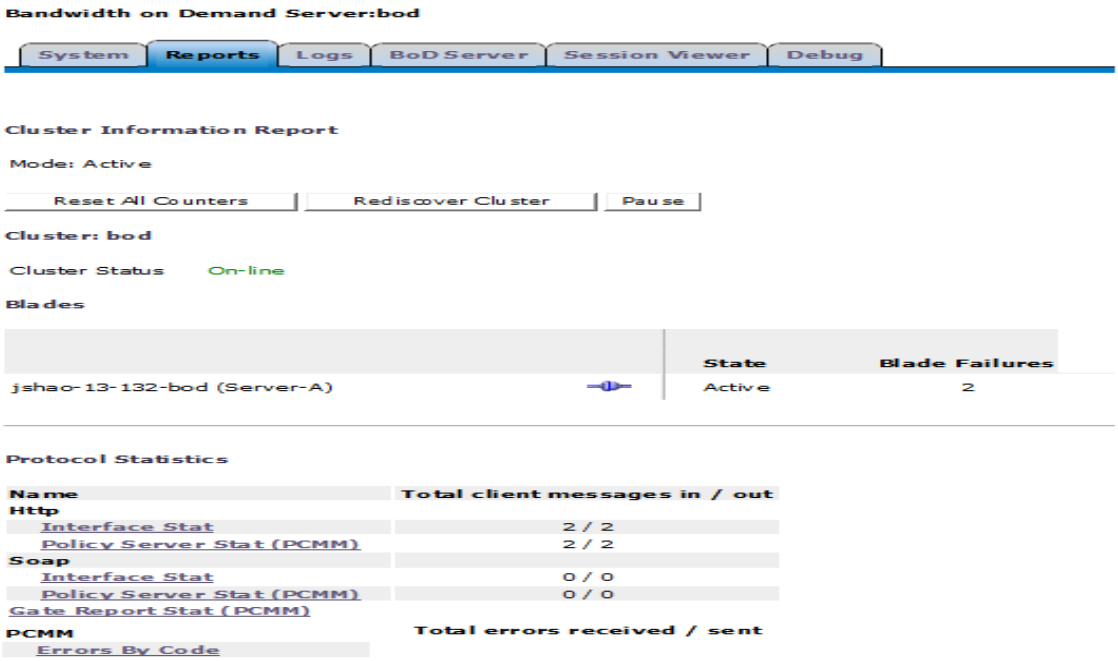
- State=4 “Committed” and reason=7 “Gate state unchanged, but volume limit reached”
- State=1 “idle/closed” and reason!=5 “Inactivity timer expired”

Following the details appended to the notification messages as part of this feature enhancement:

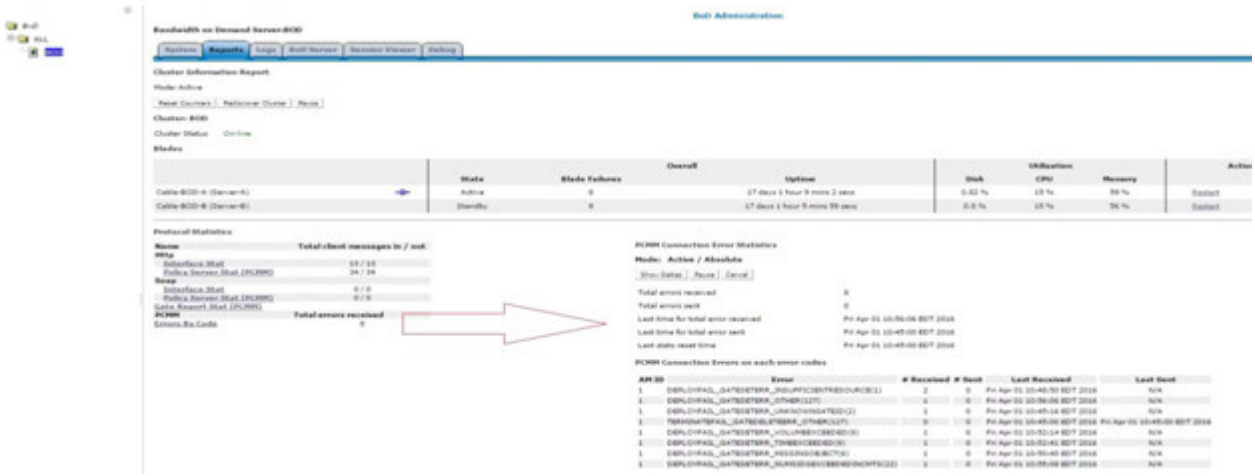
- SUBIP – the SUBIP of the BoD session
- AMID – the AMID of the BoD session
- DUR – the duration configured of the BoD session
- ACTUALDUR – the actual duration of the BoD session

### *3.12.3 User Interface Changes*

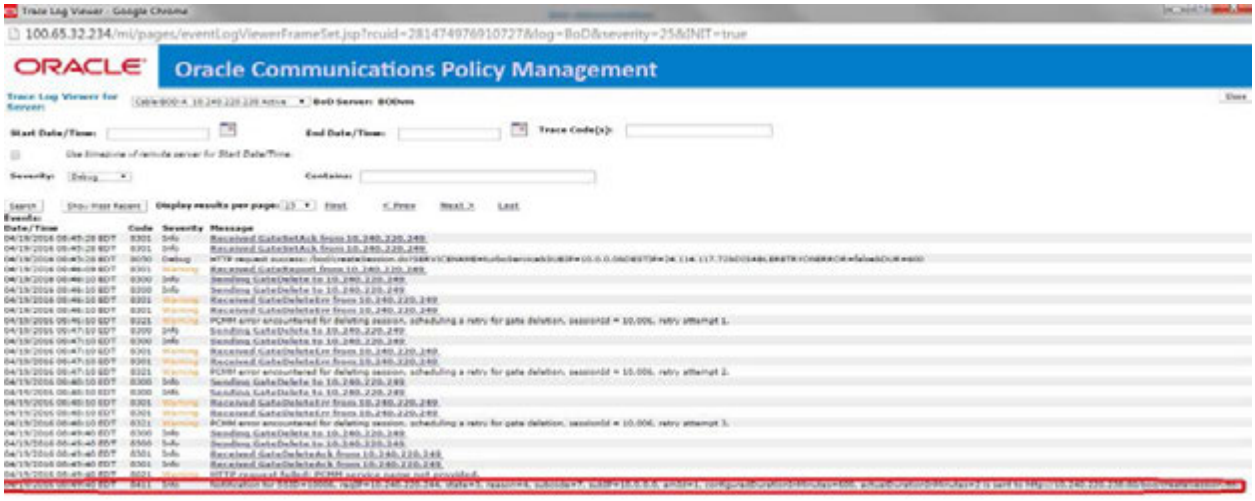
All BOD reports statistics data will be available through OSSI/XML: BOD -> Configuration -> <Configured BOD> -> Reports




New statistics data provides the number of PCMM error messages is presented in the GUI under: BOD -> Configuration -> <Configured BOD> -> Reports -> PCMM -> Errors by code



Sample trace log entry showing the notification sent with the new details



## 3.13 UNIFIED EXPORT/IMPORT ENHANCEMENTS FOR CABLE MODE( PR# 21348748)

### 3.13.1 Introduction

This feature enables customers to export several CMP GUI objects into one file and in one export request instead of the previous export support technique of exporting one object at a time. In addittion, export added more granularity to choose specific configurations under certain object to export rather than the whole configurations under that object..

Bulk export also added the ability to include dependency objects in the export process by setting a flag in the CMP GUI export screen.

While importing or exporting, user will have the ability to choose what to do with conflicts between existing and imported objects either by deleting or overwriting existing objects or reject importing objects that already exists or stop the import in case of conflicts or just run a validation without actual import.

### 3.13.2 Detailed Description

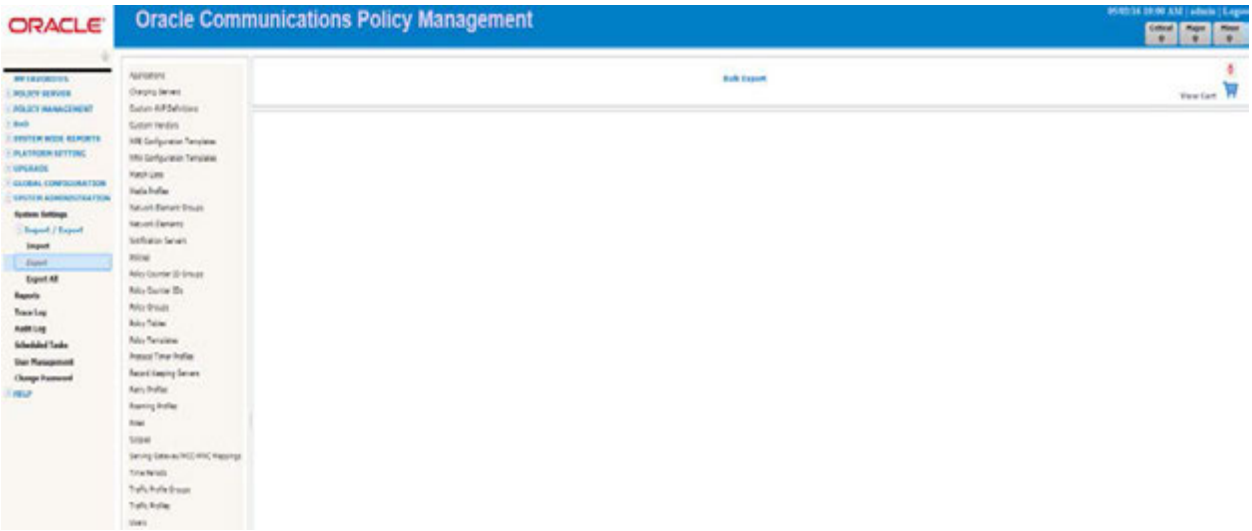
In the export screen, when an object type is selected from the horizontal tree list, the configured items in that type are displayed to support the granularity to choose the configured items to be exported. The results of the export is produced in the form of a zip file incuding an MD5 checksum file that is used afterwards when this file is imported as a verification mechanism to check if it has been modified/altered.

The objects to be exported can be selected and added to shopping cart then the shopping cart objects can be exported at the end.

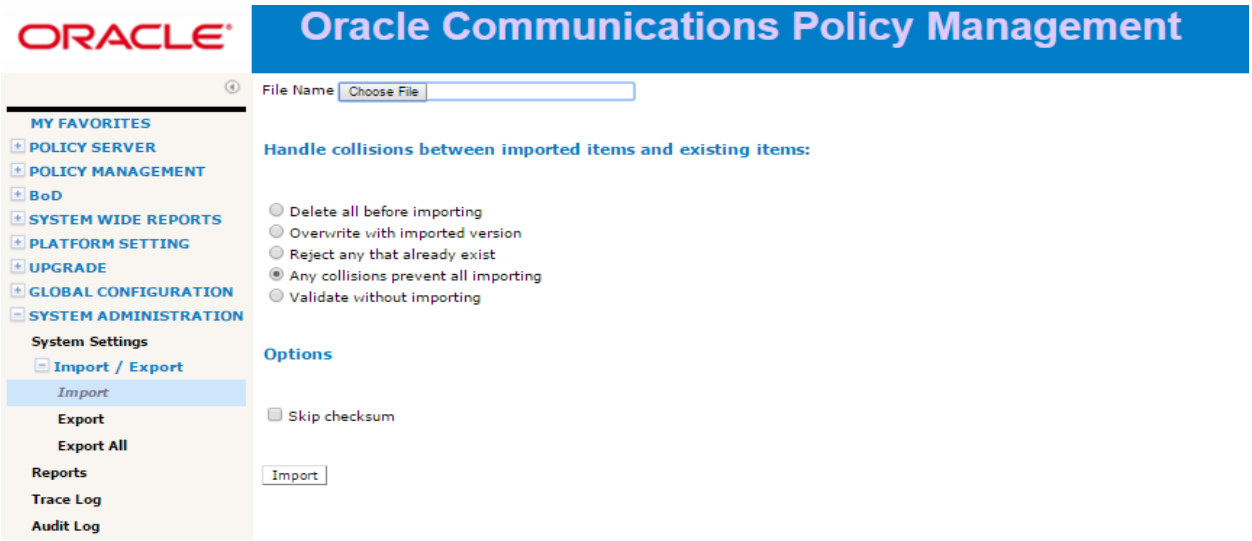
If an account has dependency on Network Element or Tier, then it will be exported or imported with that object in case the option of exporting dependencies is chosen before the export process. This dependency will be included automatically with all items dependent with any object selected for export.

### 3.13.3 User Interface Changes

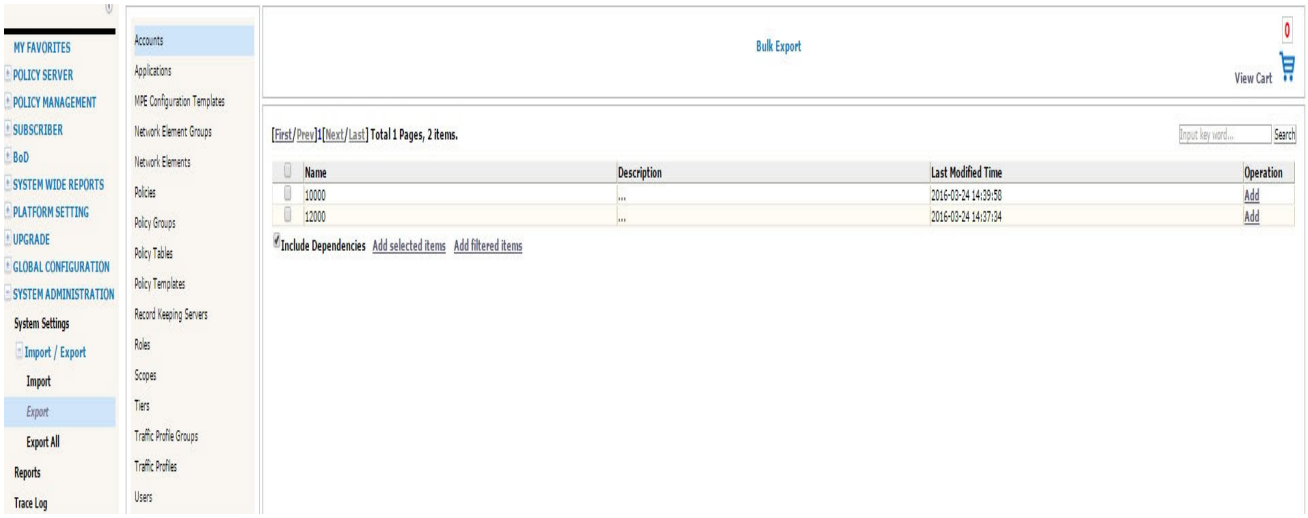
Bulk export main screen:




Bulk Import main screen:



Include dependencies option while exporting:



## 3.14 GENERIC POLICY NOTIFICATION INTERFACE - CONVERT FOR CABLE ( PR# 21153115 )

### 3.14.1 Introduction

The intent of this feature is to provide generic, highly configurable external event notification functions beyond the previously existing SMS, Email, and logging functions.

The existing methods in the current product to send either end-user notifications (SMS, Email) or operator notifications (logging, Syslog, LDAP Write) are specific to the interface on which they work and not flexible enough to provide generic notifications.

The eventual usage of these messages could be either end-user notifications (after processing by an external gateway), or event-specific messages as triggers to other operator systems (B/OSS).

The 'Generic Notifications from Policy System' feature provides necessary framework based on HTTP/web services interface to provide highly configurable/flexible notifications. The methods, destinations, and contents of the messages are flexible at the time of message generation by Policy Actions.

### 3.14.2 Detailed Description

| Policy Condition Group | Policy Condition or Action | Description |
|---|---|---|
| **Action** | **Send http "POST" notification to url "URL" with headers "headers" and content "content"** | Send a HTTP request to specified destination. The fields 'destination', 'headers', 'content' are all free-flowing text fields to be configured by operator. |
| **Action** | **Send http "POST" notification to "select notification destination" with headers "headers" and content "content"** | Send a HTTP request to pre-defined destination.<br><br>The fields 'headers', 'content' are all free-flowing text fields to be configured by operator. |

The '**URL**' 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 '**POST**' is the default notification delivery technique, this field is 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 is a pop-up box with 2 fields: 'Header' and 'Value'. Both fields shall be free-flowing text fields. There is no validation whether particular header type is a valid HTTP header. Similarly, there is no validation whether the 'value' corresponds to 'header type'. Operator shall be able to add up to 20 such rows of 'header' and 'value' in a single policy. Once the user clicks OK, header and value will be separated by a colon and multiple headers will come as a comma separated list of values. The content shown on the policy screen will display the escape characters as well, / in this case.

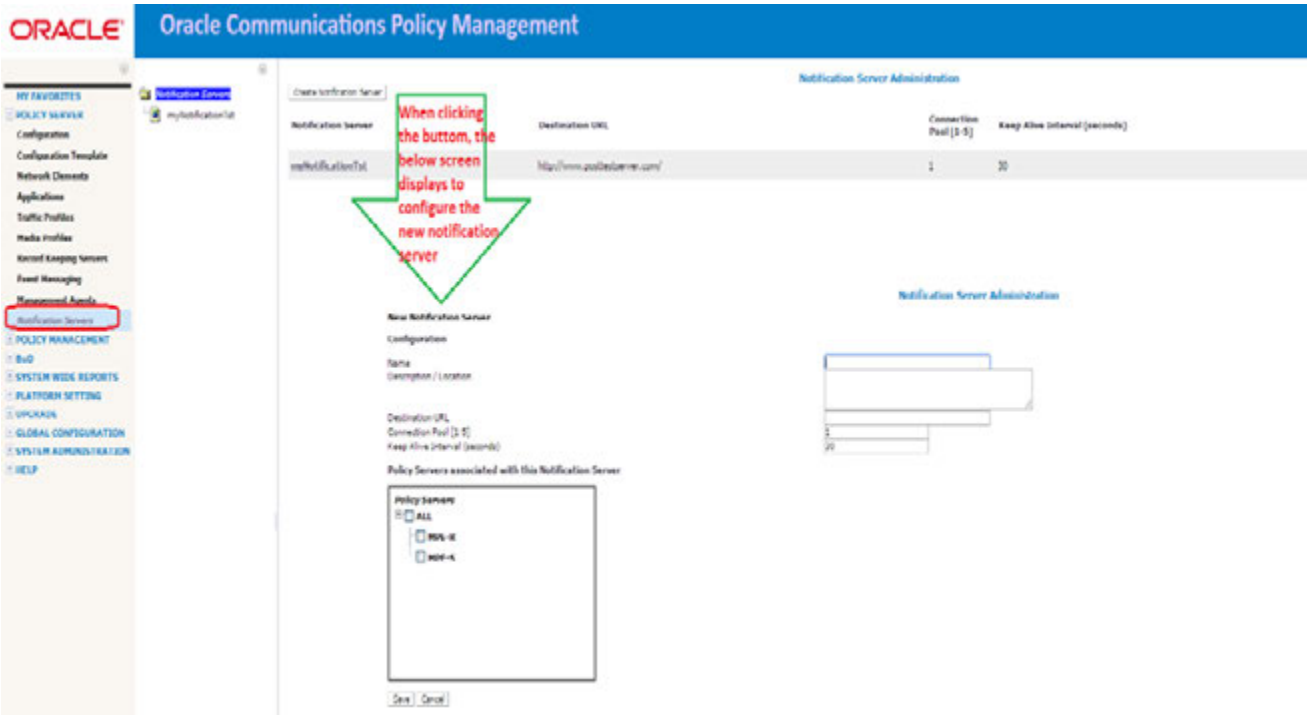
**NOTE:** In order for MPE to read the headers correctly if there are colons and/or commas in the header or value they will be escaped with forward slash (/). Also, Forward slash is not allowed as the last character in either the header or value and header name cannot be empty.

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 also allow for policy variable substitution. MPE shall not validate whether the 'header' value corresponds to particular 'content'.

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

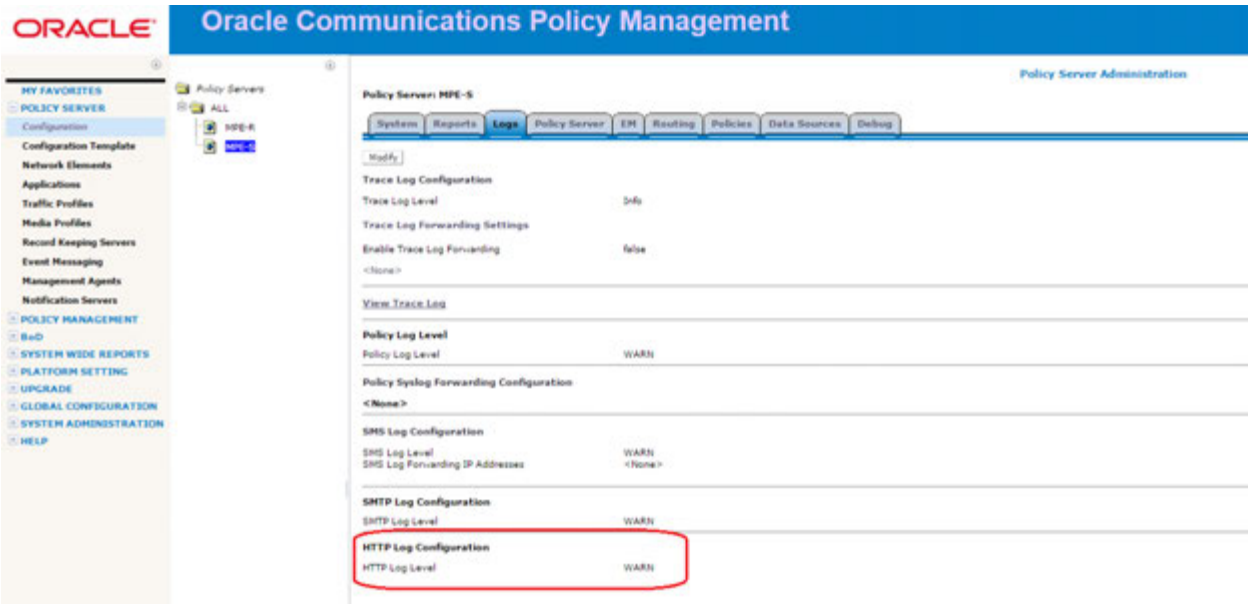
### *3.14.3 User Interface Changes*

New menu item "**Notification Server**" is added under "Policy Server" to configure static based Notification servers:




New Logs

A new log called "**HTTP log**" is introduced to track the HTTP notification messages sent from Oracle Communications Policy Management to external Notification servers. Log level can be set from CMP GUI as follows:




The actual log file is located on MPE servers under **/var/camiant/log**:

```
[root@Cable-MPE-S-A log]# cd /var/camiant/log
[root@Cable-MPE-S-A log]# ls -ltr
total 1114468
drwx------ 2 root root    16384 Mar  9 18:56 lost+found
drwxr-x--- 2 root root     4096 Mar  9 19:11 firewall
-rw-r----- 1 root root        0 Mar  9 19:11 rc.stats.daily
-rw-r----- 1 root root        0 Mar  9 19:11 policy.log
-rw-r----- 1 root root        0 Mar  9 19:11 dynamic_quota.log
-rw-r----- 1 root root        0 Mar  9 19:11 quota_rollover.log
-rw-r--r-- 1 root root        0 Mar  9 19:12 huge_core.log
-rw-r----- 1 root root        0 Mar  9 19:12 smsr.log
-rw-r----- 1 root root        0 Mar  9 19:12 smsclient.log
-rw-r----- 1 root root        0 Mar  9 19:12 SMPP.log
-rw-r----- 1 root root        0 Mar  9 19:12 SMTP.log
-rw-r----- 1 root root        0 Mar  9 19:12 HTTP.log
-rw-r----- 1 root root      990 Mar  9 19:16 qpLayout.log
```

Persistent Notification servers Connection Configurations

A new configuration file "**NotificationCfg.properties**" is introduced to handle the settings of establishing persistent connection to the configured Notification Servers in CMP GUI.

The file would be in MPE server under the following path: **/opt/camiant/smsr/smscfg/**

Should a connection attempt fail Oracle Communications Policy Management will continuously retry at constant intervals as per the configured connection retry value in this properties file till the connection is restored.

```
[admusr@Cable-MPE-S-A smscfg]$ more NotificationCfg.properties
#Generated at Tue Apr 12 17:42:27 EDT 2016
#Tue Apr 12 17:42:27 EDT 2016
http.cfg.connectionTimeout=3
http.cfg.enabled=true
http.cfg.numConnectionDynamic=1
http.cfg.requestTimeout=3
http.cfg.retry.enabled=true
http.cfg.retry.interval=60
http.queue.clearsize=1600
http.queue.size=2000
http.queue.threads=10
[admusr@Cable-MPE-S-A smscfg]$
```

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.

| | | | |
|---|---|---|---|
| 04/13/2016 19:54:04 EDT | 2567 | Warning | SMTP:Error attempting to establish a new connection to . Error: Could not connect to SMTP host: localhost, port: 25 |
| 04/13/2016 19:54:06 EDT | 2565 | Warning | SMTP:Connection to MTA was closed. |

## 3.15 MPE SENDS DPR TO DISCONNECT DIAMETER CONNECTION ( PR# 224443 & 20271448 )

### 3.15.1 Introduction

When a Diameter peer needs to disconnect due to some internal reasons, Policy Management can actively send the DPR (Disconnect-Peer-Request) to the Diameter peers.

### 3.15.2 Detailed Description

The **Disconnect-Peer-Request (DPR)**, indicated by the **Command-Code set to 282** and the Command Flags' **'R' bit ( Request)** is cleared. The AVP flag '**M' bit** is set for all 3 AVPs in the message, is sent to a peer to inform its intentions to shut down the transport connection.

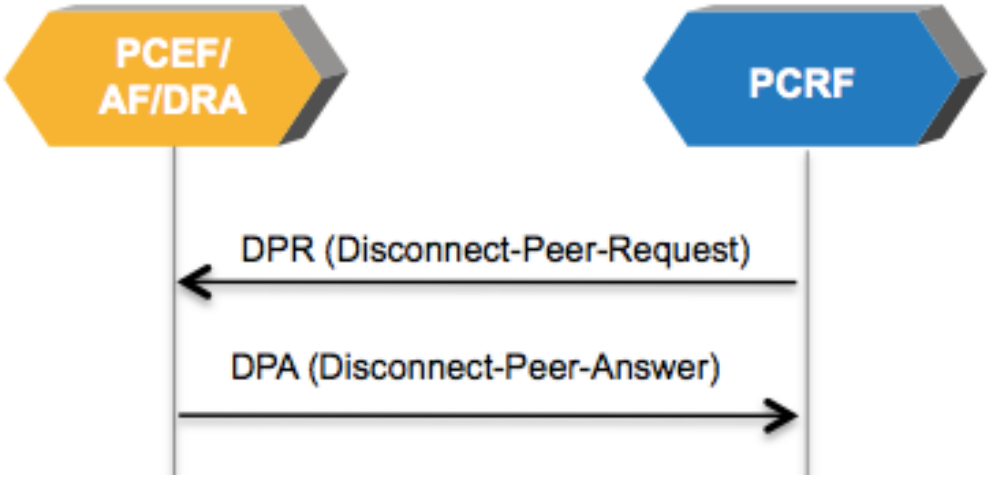
Message syntax:

```
<DPR>::= < Diameter Header: 282, REQ >
{ Origin-Host }
{ Origin-Realm }
{ Disconnect-Cause }
```

The **Disconnect-Peer-Answer (DPA)**, indicated by the **Command-Code set to 282** and the Command Flags' **'R'** (Request) is cleared. The AVP flag **'M' bit** is set for all 3 AVPs in the message, is sent as a response to the Disconnect-Peer-Request message.

Message syntax:

```
<DPA>::= < Diameter Header: 282 >
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
[ Error-Message ]
[ Failed-AVP ]
```



**DPR( PCRF →PCEF)**

| | | |
|---|---|---|
| Origin-Host AVP | M | PCRF host name |
| Origin-Realm AVP | M | PCRF domain name |
| Disconnect-Cause AVP | M | Cause value |
| **DPA( PCEF→PCRF)** | | |
| Result-Code AVP | M | Result |
| Origin-Host AVP | M | PCRF host name |
| Origin-Realm AVP | M | PCRF domain name |

Here is the list of '**Disconnect-Cause'** as defined in RFC6733, to disconnect diameter peers (Policy Management/AF/DRA) -

- REBOOTING (0)
- BUSY (1)
- DO_NOT_WANT_TO_TALK_TO_YOU (2)

### *3.15.3 User Interface Changes*

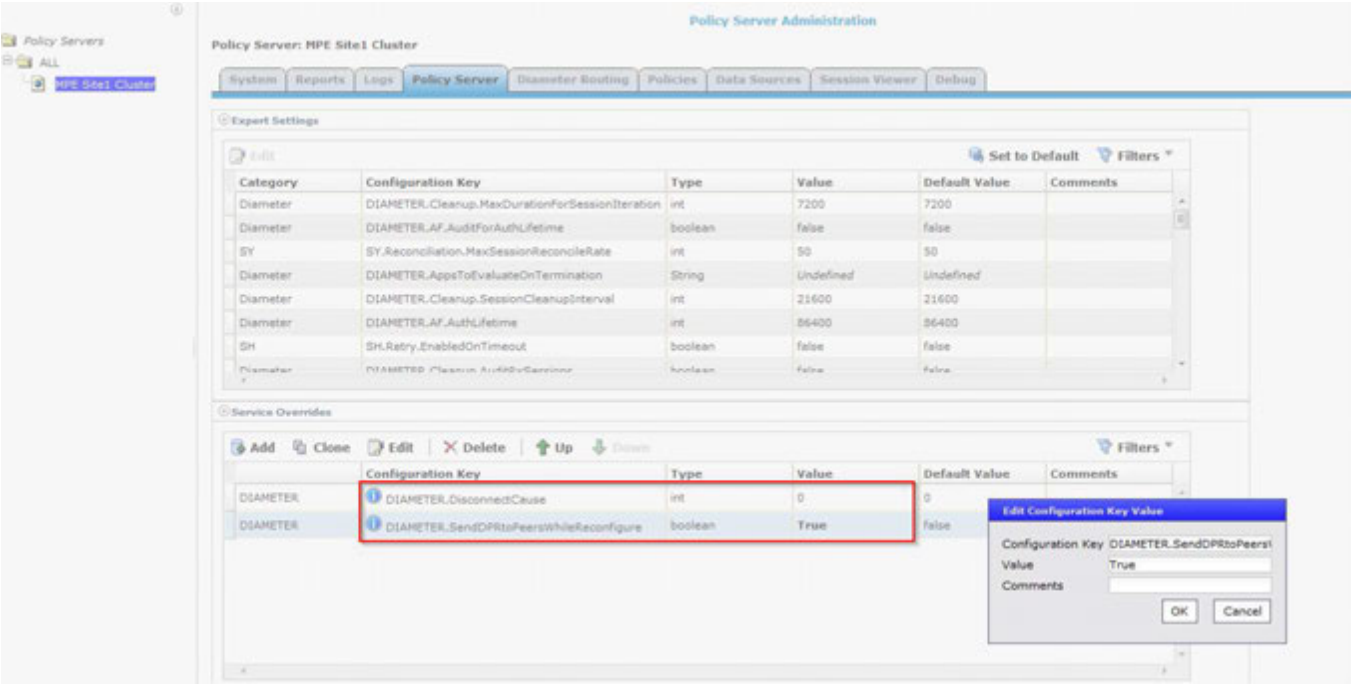
There are two new Advance Setting of Configuration keys, as shown below, applicable to both MPE and MRA in the Policy Management Service Overrides which need to be enabled for the feature -

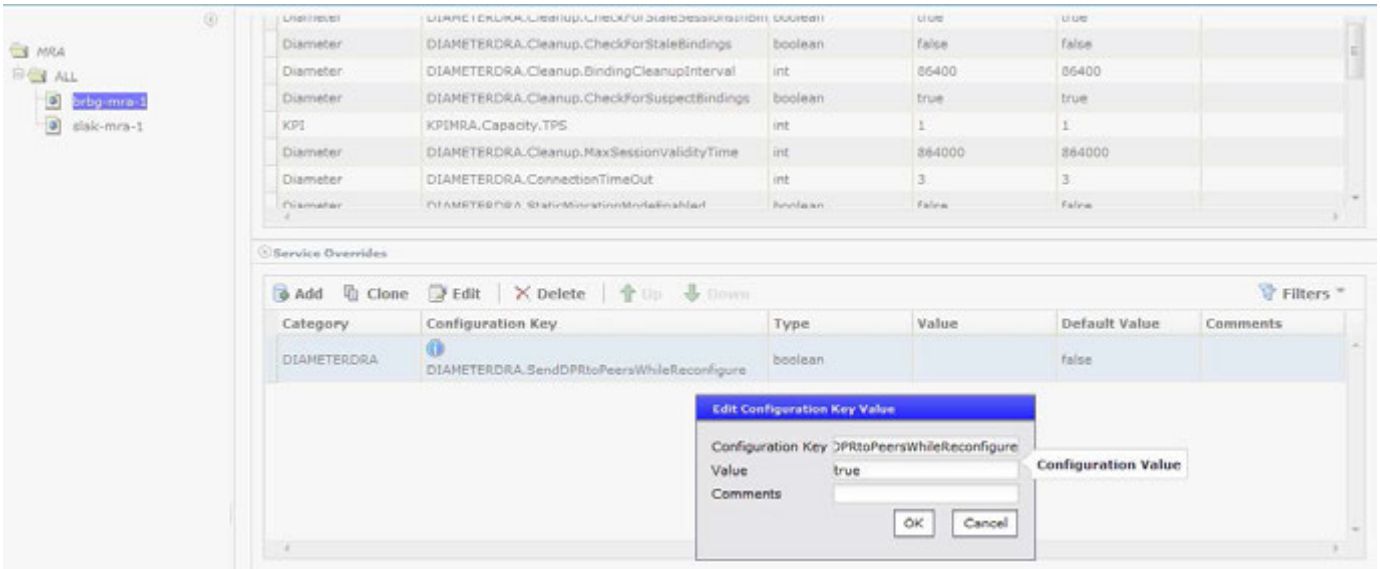
1) **DIAMETER.SendDPRtoPeersWhileReconfigure ( MPE)** and **DIAMETERDRA.SendDPRtoPeersWhileReconfigure ( MRA)**. Default value is "false". If it's set to "true" and there is a change in Realm/Identity/Port ( not case sensitive) configuration, DPR will be sent to every diameter peer before disconnecting the peer(s).
2) **DIAMETER.DisconnectCause ( MPE)** and **DIAMETERDRA.DisconnectCause ( MRA)**. Default value is "0". The DPR sent to every diameter peers with specified Disconnect-Cause which can be one of the following -

   - REBOOTING (0)
   - BUSY (1)
   - DO_NOT_WANT_TO_TALK_TO_YOU (2)

**CMP GUI:** Policy Server → Configuration → All → *( MPE cluster name )* → Policy Server → Advanced → Modify → Service Overrides

**CMP GUI:** MRA → Configuration → All → *( MRA cluster name )* → MRA → Advanced → Modify → Service Overrides


Policy Servers
ALL
HPE Site1 Cluster
Policy Server Administration
Policy Server: HPE Site1 Cluster
System
Reports
Logs
Policy Server
Diameter Routing
Policies
Data Sources
Session Viewer
Debug
Expert Settings
Set to Default
Filters
Category
Configuration Key
Type
Value
Default Value
Comments
Diameter
DIAMETER.Cleanup.MaxDurationForSessionIteration
int
7200
7200
DIAMETER.AF.AuditForAuthLifetime
boolean
false
false
SY
SY.Reconciliation.MaxSessionReconcileRate
int
50
50
DIAMETER.AppsToEvaluateOnTermination
String
Undefined
Undefined
DIAMETER.Cleanup.SessionCleanupInterval
int
21600
21600
DIAMETER.AF.AuthLifetime
int
86400
86400
SH
SH.Retry.EnabledOnTimeout
boolean
false
false
Service Overrides
Add
Clone
Edit
Delete
Up
Down
DIAMETER
DIAMETER.DisconnectCause
int
0
0
DIAMETER.SendDPRtoPeersWhileReconfigure
boolean
True
false
Edit Configuration Key Value
Configuration Key
DIAMETER.SendDPRtoPeers
Value
True
Comments
OK
Cancel


MRA
ALL
orbg-mra-1
slak-mra-1
Diameter
DIAMETERDRA.Cleanup.CheckForStaleBindings
boolean
false
false
DIAMETERDRA.Cleanup.BindingCleanupInterval
int
86400
86400
DIAMETERDRA.Cleanup.CheckForSuspectBindings
true
true
KPI
KPIMRA.Capacity.TPS
1
1
DIAMETERDRA.Cleanup.MaxSessionValidityTime
864000
864000
DIAMETERDRA.ConnectionTimeOut
3
3
Service Overrides
Add
Clone
Edit
Delete
Up
Down
Filters
Category
Configuration Key
Type
Value
Default Value
Comments
DIAMETERDRA
DIAMETERDRA.SendDPRtoPeersWhileReconfigure
boolean
false
Edit Configuration Key Value
Configuration Key
DPRtoPeersWhileReconfigure
Value
true
Comments
OK
Cancel
Configuration Value

## 3.16 NOTIFICATIONS DURING THE CONFIGURED INTERVAL ( PR# 224512 & 20271430 )

### 3.16.1 Introduction

This feature allows Policy Management ( MPE) to send SMS notification, via policy action, to the end user only during the configured interval in SMPP. This enable Operator to limit the end user notification frequency and to avoid the potential “notification storm” in some special cases like location based notification policy control.

### 3.16.2 Detailed Description

The Policy Management ( MPE) writes the current SMS notification sent date into the State filed in subscription profile in SPR when the first SMS notification is sent if the subs is located in the Cell ID match list which is configured In the CMP.

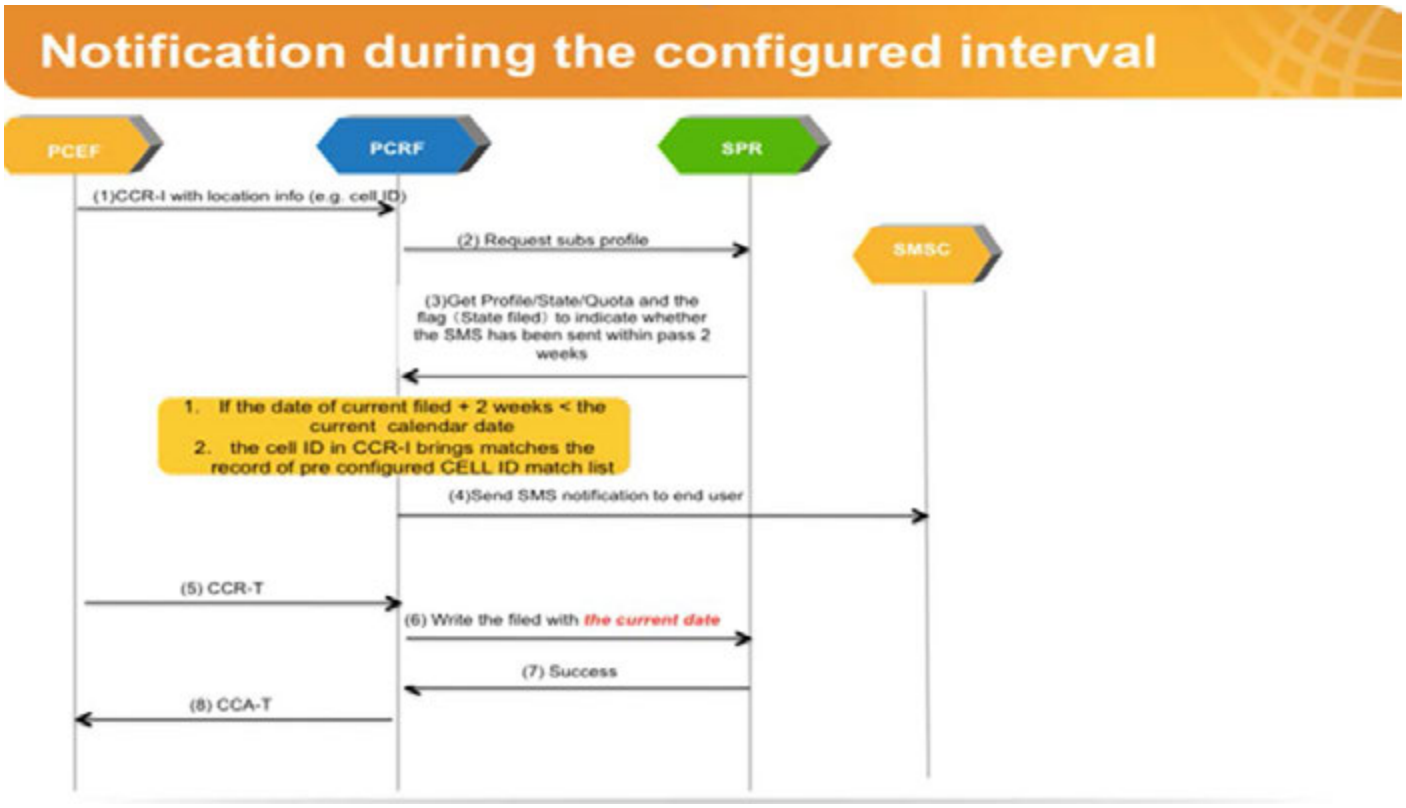
***Example:***

The Policy Management ( MPE) would compare the result of recorded date in State field + 2 weeks (*a configuration example*) with the Current Calendar Date

If Recorded date+ 2 weeks > Current Calendar Date
Action: Continue ( *Do Not send the SMS*)

If Recorded date+ 2 weeks < Current Calendar Date and If use location info is in the Cell ID match list
Action: Send the SMS notification ( *Write the State filed with current Calendar date* )

The location string in the SMS content should be able to linked with the hit Cell ID




### 3.16.3 User Interface Changes

Here is the Policy changes with the feature:

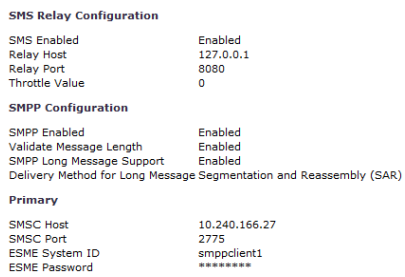
- CMP Mode settings set to “Wireless Quote Gx” and ‘SMS:SMPP’

Mode Settings

Change Mode

| | |
|---|---|
| Mode | Wireless:Diameter 3GPP, Wireless:Diameter 3GPP2, Wireless:Quotas Gx, Wireless:Quotas Gy, Wireless:Gx-Lite, SMS:SMPP |
| Manage Policy Servers | true |
| Manage MA Servers | false |
| Manage Policies | true |
| Manage MSAs | true |
| Manage BoDs | false |
| Manage SPR Subscriber Data | true |
| Manage Geo-Redundant MPE/MRA/DOC | false |
| Manager is HA (clustered) | true |
| Manage Analytic Data | false |
| Manage Direct Link | false |
| Manager is NW-CMP | false |
| Manager is SI-CMP | false |

- MPE Policy Server Tab configured for SMS Relay and SMPP configuration



**SMS Relay Configuration**

| | |
|---|---|
| SMS Enabled | Enabled |
| Relay Host | 127.0.0.1 |
| Relay Port | 8080 |
| Throttle Value | 0 |

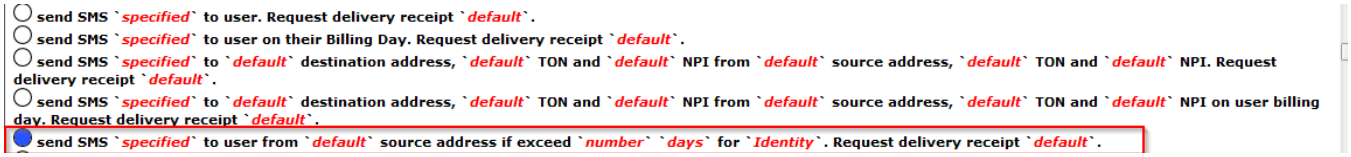
**SMPP Configuration**

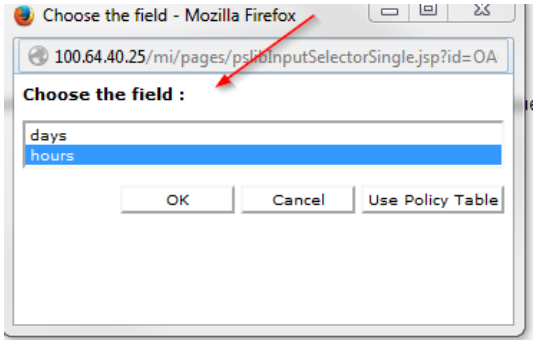
| | |
|---|---|
| SMPP Enabled | Enabled |
| Validate Message Length | Enabled |
| SMPP Long Message Support | Enabled |
| Delivery Method for Long Message | Segmentation and Reassembly (SAR) |

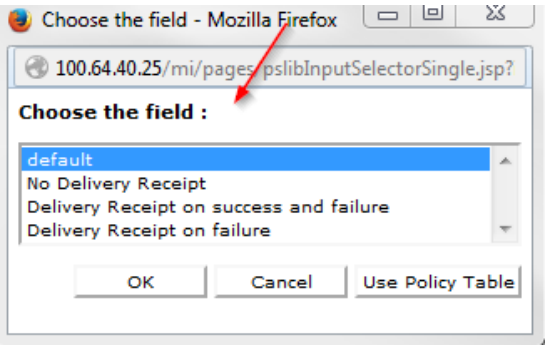
**Primary**

| | |
|---|---|
| SMSC Host | 10.240.166.27 |
| SMSC Port | 2775 |
| ESME System ID | smppclient1 |
| ESME Password | ******** |

| Policy Condition Group | Policy Condition or Action | Description |
|---|---|---|
| “Optional” actions | send SMS `specified` to user from `default` source address if exceed `number` `days` for `Identity`. Request delivery receipt `default`. | This policy action can send notification to end user, and only once during the configured interval. |




- **SMS 'specified'**

SMS message content.

- **destination address**

Dest_terminal_Id(The destination phone number) in SMS SUBMIT message, if 'default' it will be replaced by User.MSISDN. It supports multi destination addresses, each address separated by comma. Note the multi destination addresses will cause to generate multi SMS messages including one destination address..

- **source address**

Src_Id(The source phone number) in SMS SUBMIT message, if 'default' it will be replaced by smpp.protocol.srcId configured in SMPP.properties.

- **delivery receipt**

The policy variable 'default' can be replaced with a user specified value which choices are default, No Delivery Receipt, or Delivery Receipt. When choosing the 'default' field, it will be replaced by "Registered Delivery" which configured in SMS profile configuration under the Policy Server tab. If choose 'Delivery Receipt' field will ask for delivery receipt while submitting SMS, and choose 'No Delivery Receipt' field will not request it.

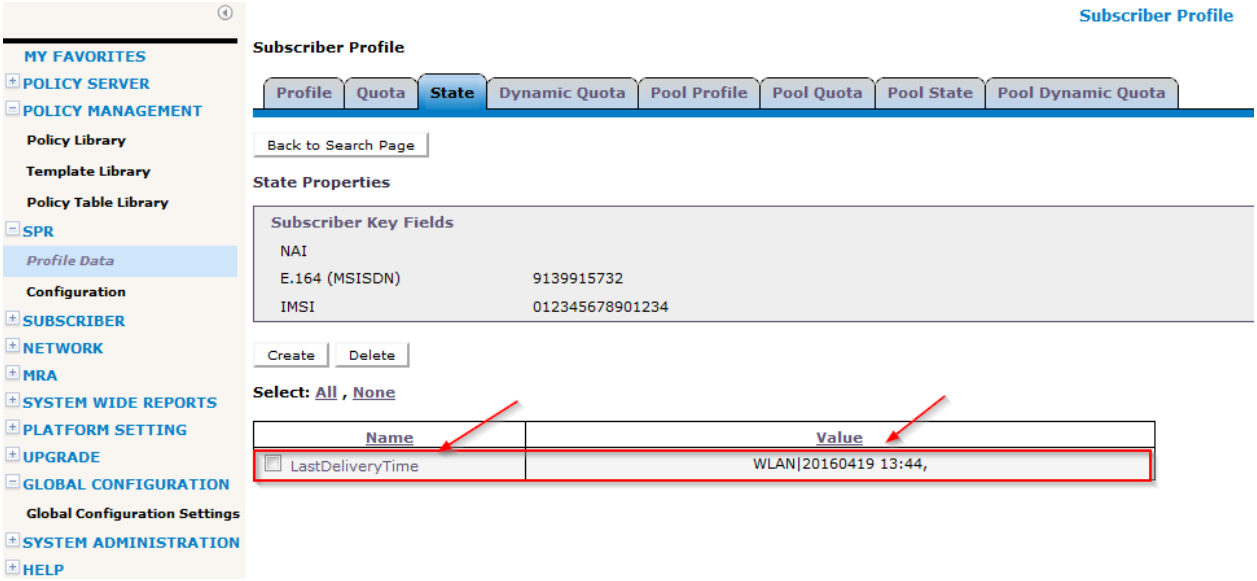
- **if exceed `number` `days` for `Identity`**

We use "Identity" to identify different kinds of SMS, "number days" means a time period, This policy action will control to send this kind SMS only once during specific time period. We have two units for interval: days and hours, default value is day.

Service Overrides –

1) SMPP.NotifyDuringIntervalUserStateKey
2) SMPP.NotifyDuringIntervalDelimiter
3) SMPP.NotifyDuringIntervalDetailDelimiter

The Notification Interval configuration is as of the following -




- The "LastDeliveryTime" string contains all information for every identity which defined in policy action. The format is as: Identity01|LastDeliveryTime01,Identity02|LastDeliveryTime02,… The symbol to separate every item here is “,”.

- The Entity state "LastDeliveryTime" is saved to SPR/UDR with correct identity eg.“WLAN" and correct delivery time information.

## 3.17 RESULT-CODE 5143 RETURNED IF REQUESTED QoS CONFLICTS WITH AUTHORIZED QoS ( PR# 224391 & 20271416 )

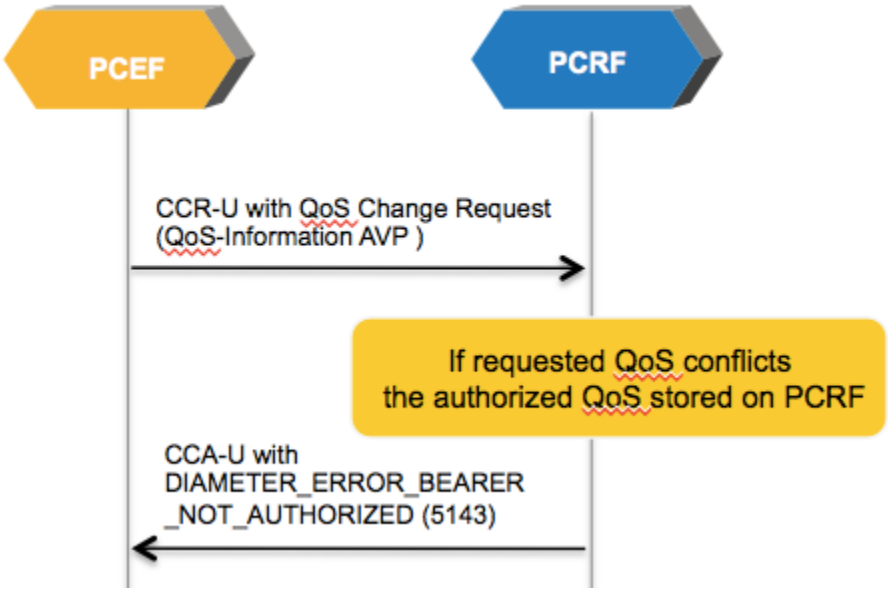
### 3.17.1 Introduction

This feature allows Policy Management to provide Experimental-Result-Code AVP of " **DIAMETER_ERROR_BEARER_NOT_AUTHORIZED (5143)**" together with the bearer-identifier AVP in the CCA as an indication to PCEF that the authorized QoS exceeds the subscribed QoS.

Besides support for Gx interface, the Sd and Gxx interfaces are also supported. The support for Rx interface already supported in the pre-Release 12.2.

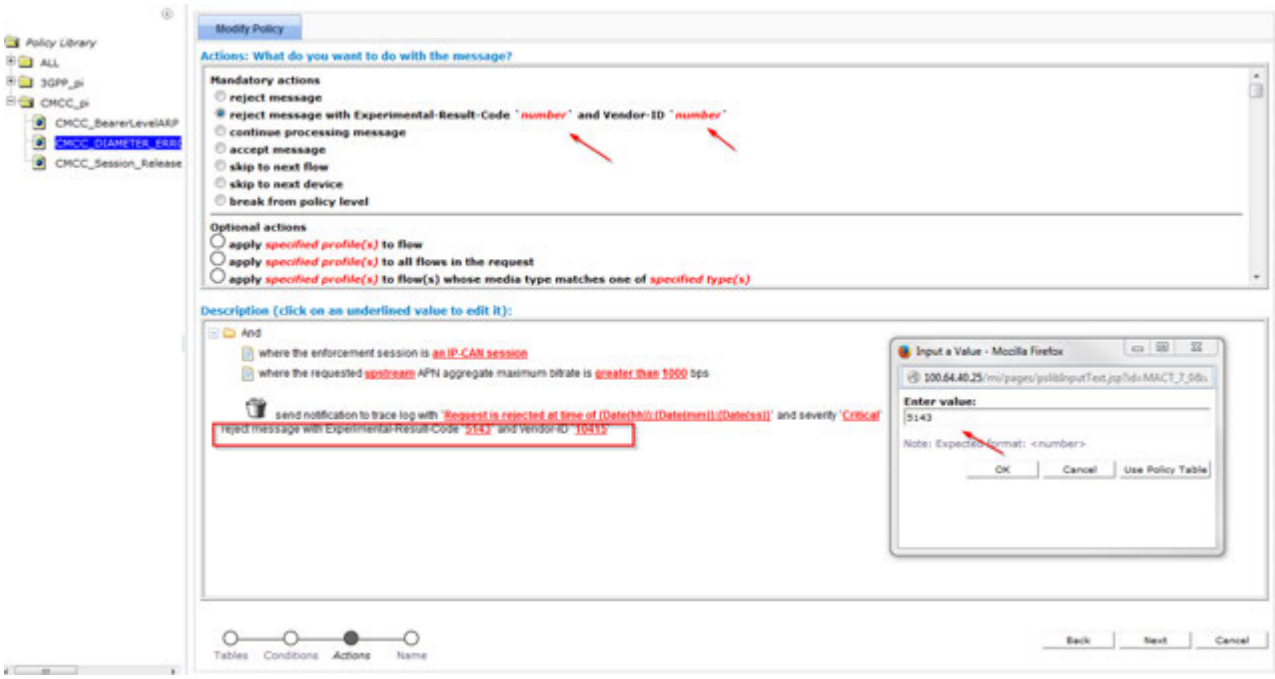
### 3.17.2 Detailed Description

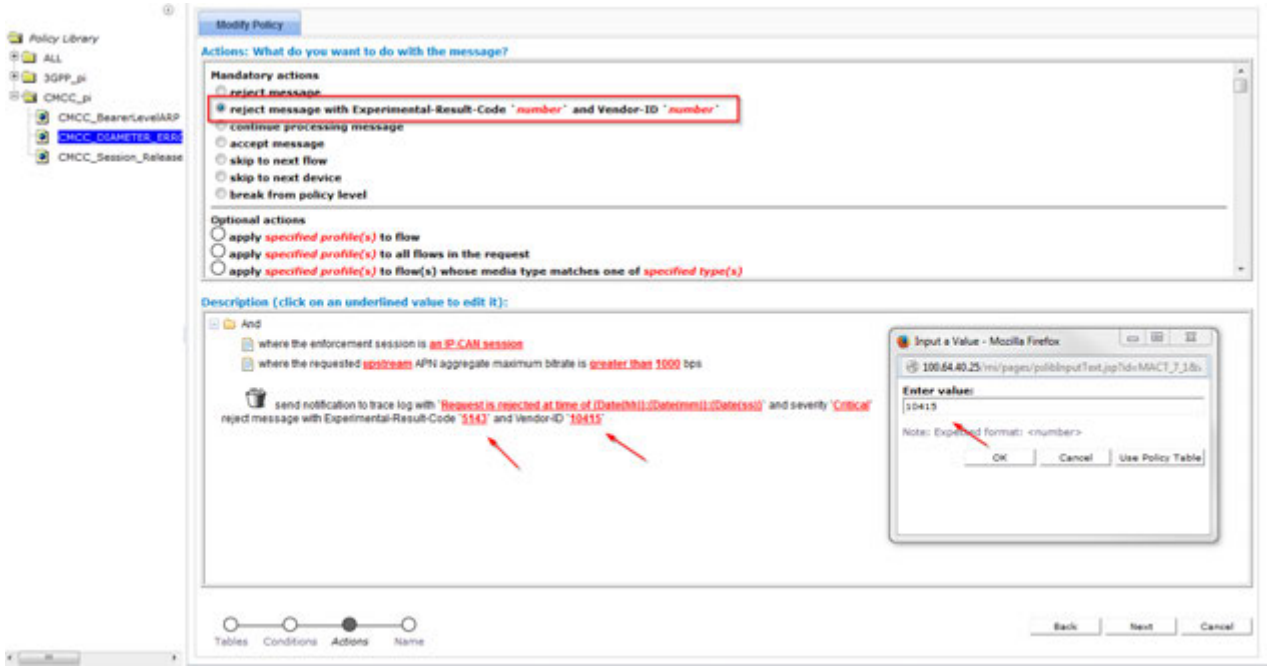
This error shall be used when the Policy Management cannot authorize an IP-CAN bearer (e.g. the authorized QoS would exceed the subscribed QoS) upon the reception of an IP-CAN bearer authorization request coming from the PCEF. The affected IP-CAN bearer is the one that triggered the corresponding CCR. The PCEF shall reject the attempt to initiate or modify the bearer indicated in the related CCR command



### 3.17.3 User Interface Changes

| Policy Condition Group | Policy Condition or Action | Description |
|---|---|---|
| **"Mandatory" actions** | Reject message with Experimental-Result-code 'number' and Vendor-ID 'number' | Configure the Experimental-Result-code, the Diameter_Error_Bearer_Not_Authorized(**5143**) and Vendor-Id **10415** |



Sample usecase screenshot: Reject with Experimental-Result and Vendor-Id (PCRF respond with Gx CCA-U)

```
2016-04-05 15:31:31.516
received a reply :
Diameter Message: CCA
Version: 1
Msg Length: 168
Cmd Flags: PXY
Cmd Code: 272
App-Id: 16777238
Hop-By-Hop-Id: 866908834
End-To-End-Id: 2962257759
  Session-Id (263,M,l=28) = diamcliGx.9136870251
  Experimental-Result (297,M,l=32) = DIAMETER_ERROR_BEARER_NOT_AUTHORIZED (3GPP,5143)
    Vendor-Id (266,M,l=12) = 10415
    Experimental-Result-Code (298,M,l=12) = 5143
  Origin-Host (264,M,l=29) = ohio-mpe-1.oracle.com
  Origin-Realm (296,M,l=18) = oracle.com
  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
```

## 3.18 UE SUBSCRIPTION REASON RETURNED IN SESSION-RELEASE-CAUSE AVP ( PR# 225037 & 20271438 )

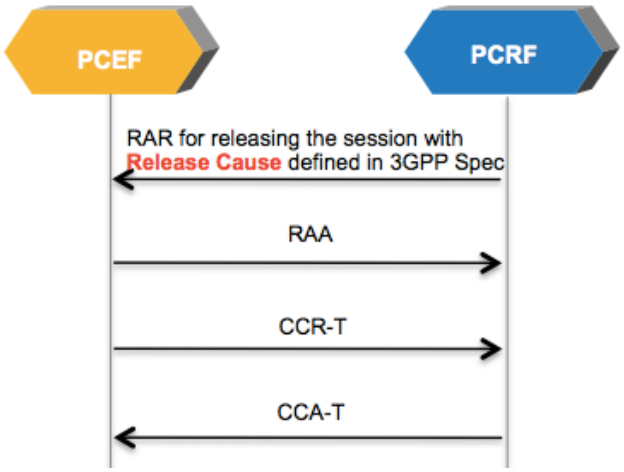
### 3.18.1 Introduction

Currently Policy Management can only fill “UNSPECIFIED_REASON(0)” in Session-Release-Cause AVP ( code: 1045) when using the policy condition “Release the session”. This feature only supports Gx, Gxx, s9 and sd Interfaces

This feature enables Policy Management to send RAR containing the following Session-Release-Cause AVPs to the PCEF -

1) UNSPECIFIED_REASON:0
2) UE_SUBSCRIPTION_REASON:1
3) INSUFFICIENT_SERVER_RESOURCES:2
4) IP_CAN_SESSION_TERMINATION:3
5) UE_IP_ADDRESS_RELEASE：4

### 3.18.2 Detailed Description



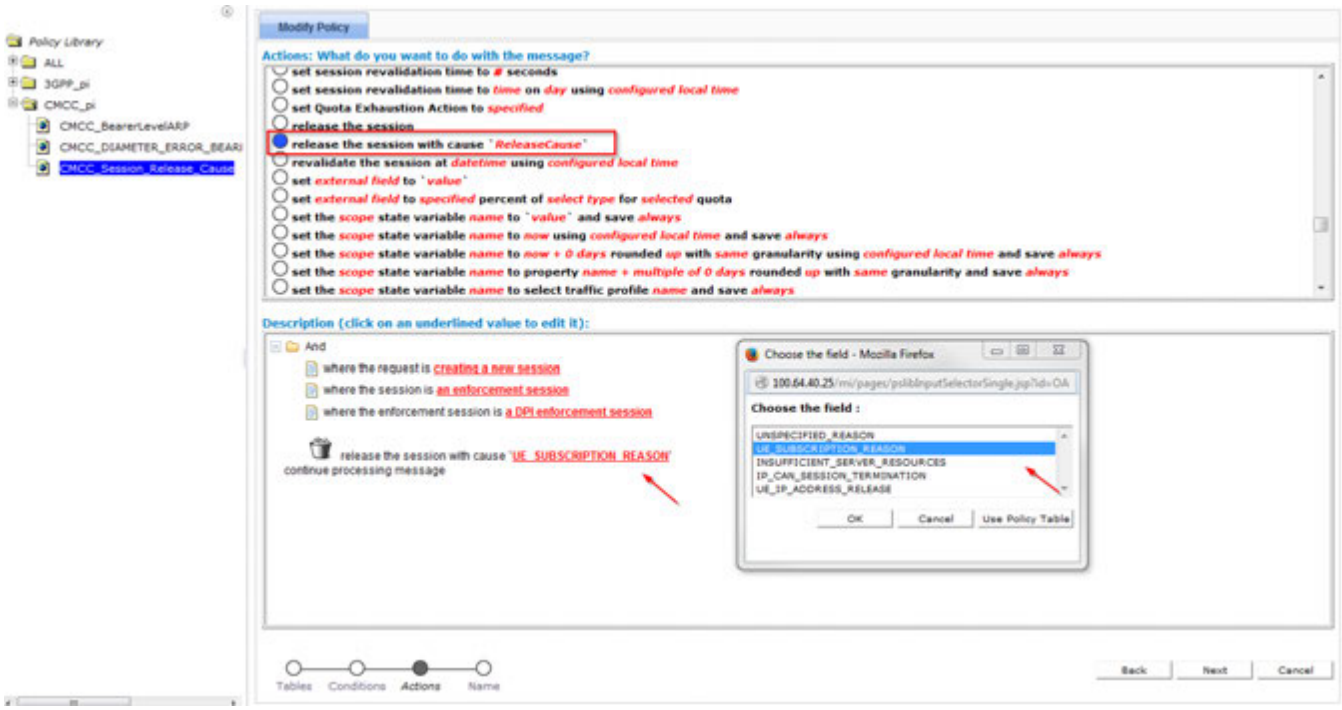

PCRF able to send RAR (per 3GPP Techical Spec 29.212 c70, Section:5.3.44) containing Session-Release-Cause AVP to the PCEF.

### 3.18.3 User Interface Changes

| Policy Condition Group | Policy Condition or Action | Description |
|---|---|---|
| **“Optional” actions** | release the session with cause ‘Release Cause’ | Configure by choosing the Release Cause: UNSPECIFIED_REASON(0), UE_SUBSCRIPTION_REASON(1), INSUFFICIENT_SERVER_RESOURCES(2), IP_CAN_SESSION_TERMINATION(3), UE_IP_ADDRESS_RELEASE(4) |

**Session-Release-Cause AVP**

| Name | Description |
|---|---|
| UNSPECIFIED_REASON | This value is used for unspecified reasons. |
| UE_SUBSCRIPTION_REASON | This value is used to indicate that the subscription of UE has changed (e.g. removed) and the session needs to be terminated. |
| INSUFFICIENT_SERVER_RESOURCES | This value is used to indicate that the server is overloaded and needs to abort the session. |
| IP_CAN_SESSION_TERMINATION | This value is used to indicate that the corresponding IP-CAN session is terminated. The IP_CAN_SESSION_TERMINATION value is introduced in order to be used by Sd only, when PCRF initiates the TDF session termination within IP-CAN session termination. |
| UE_IP_ADDRESS_RELEASE | This value is used to indicate that the IPv4 address of a dual stack IP-CAN session is released. The UE_IP_ADDRESS_RELEASE value is introduced in order to be used by Sd only, when PCRF initiates the TDF session termination if the IPv4 address of a dual stack IP-CAN session is released and if there is an active IPv4 address related TDF session for that IP-CAN session. |



## 3.19 SUPPORT TO CONFIGURE BEARER LEVEL ARP IN POLICY ACTION ( PR# 224376 & 20271401 )

### 3.19.1 Introduction

This feature extends the capability of Policy Management Policy Action to set '**bearer level ARP Preemption Capability** " and " **bearer level ARP Preemption Vulnerability**", in addition to the current of " **priority level of bearer level ARP**"

### 3.19.2 Detailed Description

These two parameters in CCA message will be set as the values brought by CCR message from PCEF. To optimize the current system limitation and support the policy parameters setting in a flexible way, these two parameters are required to be set by CMP and send to PCEF via the Gx interface.

If these parameters are NOT configured, the system should be able to use the default value in CCA message.

The **Allocation-Retention-Priority AVP (AVP code 1034)** is of type Grouped, and it is used to indicate the priority of allocation and retention, the pre-emption capability and pre-emption vulnerability for the SDF if provided within the QoS-Information-AVP or for the EPS default bearer if provided within the Default-EPS-Bearer-QoS AVP.

The **Priority-Level AVP** of the default bearer should be set to a sufficiently high level of priority and the ARP pre-emption vulnerability of the default bearer should be set appropriately to minimize the risk for unexpected PDN disconnection or UE detach from the network according to operator specific policies.

**AVP Format:**

Allocation-Retention-Priority ::= < **AVP Header: 1034** >
{ Priority-Level }
[ Pre-emption-Capability ]
[ Pre-emption-Vulnerability ]

**The description of the "bearer level ARP Preemption Capability" and "bearer level ARP Preemption Vulnerability" as follow table:**

| Name | description |
|---|---|
| PREEMPTION_CAPABILITY_ENABLED | This value indicates that the service data flow or bearer is allowed to get resources that were already assigned to another service data flow or bearer with a lower priority level. |
| PREEMPTION_CAPABILITY_DISABLED | This value indicates that the service data flow or bearer is not allowed to get resources that were already assigned to another service data flow or bearer with a lower priority level. This is the default value applicable if this AVP is not supplied. |
| PREEMPTION_VULNERABILITY_ENABLED | This value indicates that the resources assigned to the service data flow or bearer can be pre-empted and allocated to a service data flow or bearer with a higher priority level. This is the default value applicable if this AVP is not supplied. |
| PREEMPTION_VULNERABILITY_DISABLED | This value indicates that the resources assigned to the service data flow |

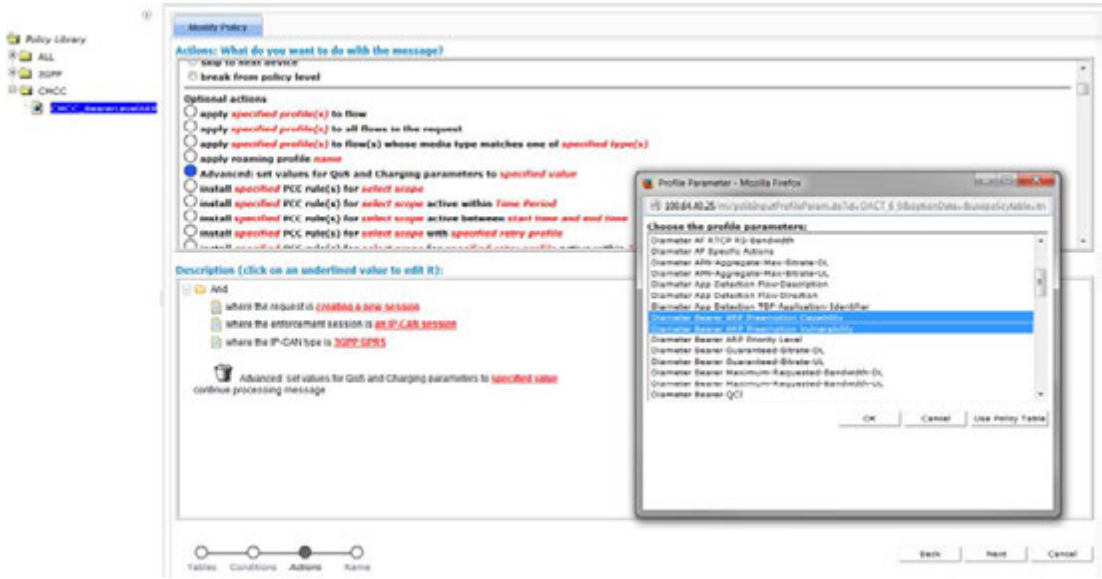
| | |
|---|---|
| | or bearer shall not be pre-empted and allocated to a service data flow or bearer with a higher priority level. |

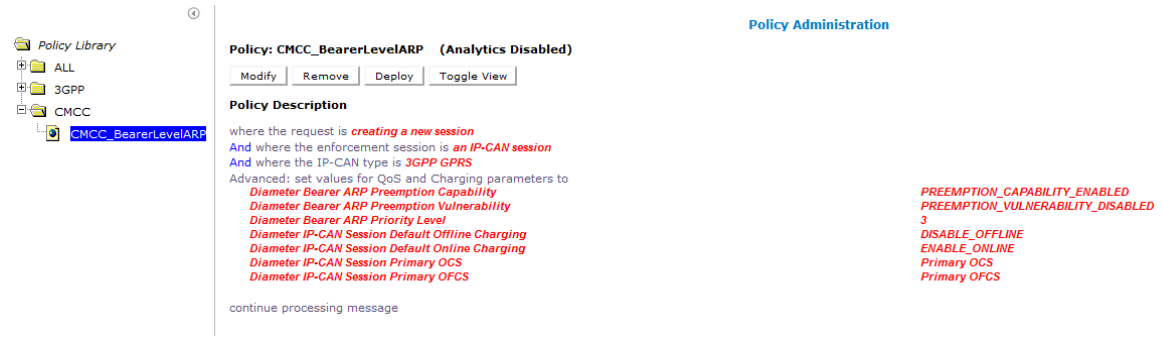
**Sample use case:** Bearer Level ARP in Policy action with Policy Management responds with Gx:CCA-I

```
      QoS-Information (1016,VM,v=10415,l=152) =
        QoS-Class-Identifier (1028,VM,v=10415,l=16) = 3
        Guaranteed-Bitrate-UL (1026,VM,v=10415,l=16) = 10000
        Guaranteed-Bitrate-DL (1025,VM,v=10415,l=16) = 30000
        Max-Requested-Bandwidth-UL (516,VM,v=10415,l=16) = 20000
        Max-Requested-Bandwidth-DL (515,VM,v=10415,l=16) = 50000
        Allocation-Retention-Priority (1034,V,v=10415,l=60) =
          Priority-Level (1046,V,v=10415,l=16) = 15
          Preemption-Capability (1047,V,v=10415,l=16) = PREEMPTION_CAPABILITY_DISABLED (1)
          Preemption-Vulnerability (1048,V,v=10415,l=16) = PREEMPTION_VULNERABILITY_ENABLED (0)
      Precedence (1010,VM,v=10415,l=16) = 1999
    Bearer-Identifier (1020,VM,v=10415,l=15) = 102
```

### *3.19.3 User Interface Changes*

| Policy Condition Group | Policy Condition or Action | Description |
|---|---|---|
| **“Optional” actions** | Advanced: set values for QoS and Charging parameters to ‘specified value’ | Configure "bearer level ARP Preemption Capability" and "bearer level ARP Preemption Vulnerability" in the action. |






## 3.20 3GPP USAGE MONITORING CONGESTION HANDLING (UPDATED TIME-TARIFF SPEC) ( PR# 19720700 )

### 3.20.1 Introduction

This feature introduces support for Usage Monitoring Congestion Handling ( UMCH) as defined by 3GPP 29.212 [5]. V12.9. It allows usage reporting at end of billing cycles to be further distributed to prevent message storm and usage leakage.

### 3.20.2 Detailed Description

The PCRF will support this functionality when the PCEF provides the UMCH supported feature upon session establishment. This only applies to quota plans for both subscribers and pools, since they occur on a set cycle such as daily, weekly, and monthly.

Dynamic quota such as passes, top-ups, and roll-over will behave as they currently do prior to UMCH.

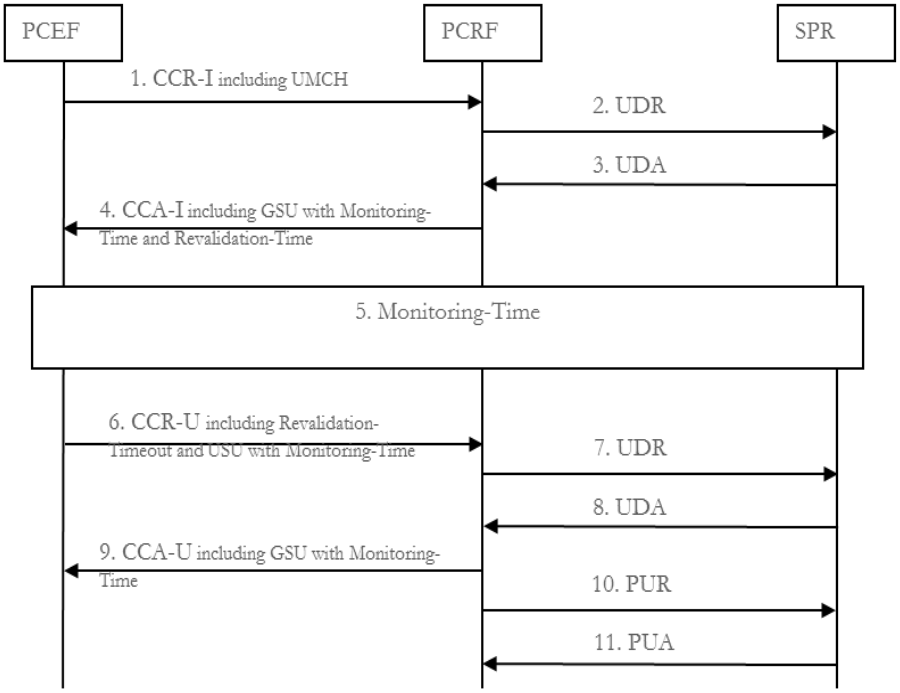
The PCRF, upon receiving a CCR-I with the UMCH supported feature, will have the capability to send 2 Granted-Service-Units, with one of them containing a Monitoring-Time AVP in the CCA.

Upon receiving a CCR-u after the Monitoring-Time, that contains 2 Used-Service-Units, and one of them also has the Monitoring-Time AVP, will record this usage to the SPR.

The octets in the Granted-Service-Unit along with the Monitoring-Time AVP, will be calculated by pro-rating the units based off of this formula.

(Max-Possible-Grant-From-Policy) * ((Revalidation-Time – Monitoring-Time)/Plan Cycle)

where the Max-Possible-Grant-From-Policy = Percentage in policy * Volume Limit defined in quota profile




The call flow explains scenario of Revalidation Timeout with usage report included in the same message.

1. The PCEF sends a CCR-initial to the PCRF which includes the UMCH supported feature.

2. The PCRF sends a UDR to the SPR to lookup the user's profile and quota records.

3. The SPR sends a UDA containing the user's profile and quota records.

4. The PCRF sends a CCA-initial to the PCEF containing the computed Revalidation-Time and 2 Granted-Service-Unit AVPs, where 1 of them contains the Monitoring-Time AVP.

5. The user continues to use usage as the monitoring time is passed.

6. The PCEF sends a CCR-update to the PCRF upon the Revalidation-Time occurring. This message includes the Revalidation-Timeout event trigger and 2 Used-Service-Unit AVPs, where 1 of them contains the Monitoring-Time AVP.

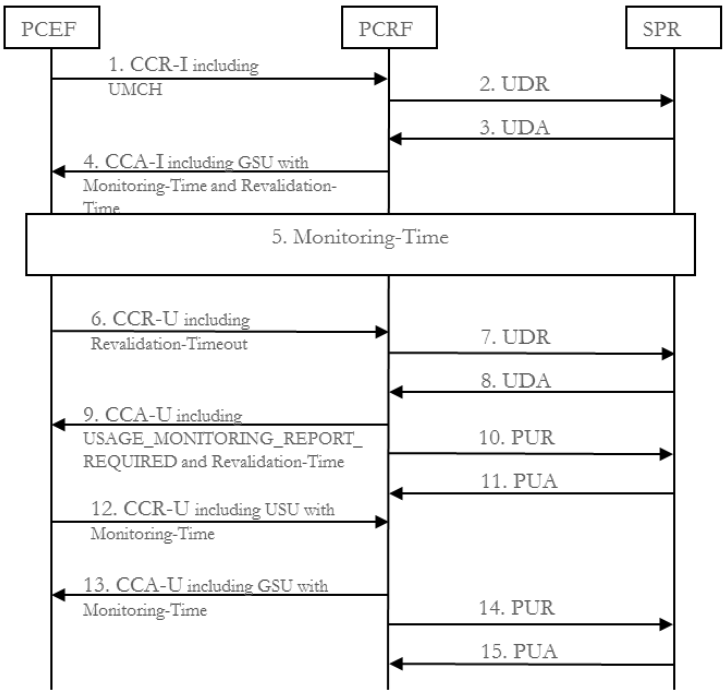
7. The PCRF sends a UDR to the SPR to lookup the user's quota records.

8. The SPR sends a UDA containing the user's quota records.

9. The PCRF calculates a new grant based off of a new cycle beginning and sends a CCA-update to the PCEF containing a newly computed Revalidation-Time and 2 Granted-Service-Unit AVPs, where 1 of them contains the Monitoring-Time AVP.

10. This step occurs asynchronously along with the previous step. The PCRF updates the quota records of the user from the Used-Service-Unit AVP that contained the Monitoring-Time and reports this to the SPR in a PUR.

11. The SPR responds with a PUA.




The call flow explains scenario of Revalidation Timeout with usage report included in the separate message(s).

1. The PCEF sends a CCR-initial to the PCRF which includes the UMCH supported feature.
2. The PCRF sends a UDR to the SPR to lookup the user's profile and quota records.
3. The SPR sends a UDA containing the user's profile and quota records.
4. The PCRF sends a CCA-initial to the PCEF containing the computed Revalidation-Time and 2 Granted-Service-Unit AVPs, where 1 of them contains the Monitoring-Time AVP.
5. The user continues to use usage as the monitoring time is passed.
6. The PCEF sends a CCR-update to the PCRF upon the Revalidation-Time occurring. This message includes the Revalidation-Timeout event trigger and does not contain any usage reports.
7. The PCRF sends a UDR to the SPR to lookup the user's quota records.
8. The SPR sends a UDA containing the user's quota records.
9. The PCRF calculates a new grant based off of a new cycle beginning and sends a CCA-update to the PCEF containing a newly computed Revalidation-Time and 2 Granted-Service-Unit AVPs, where 1 of them contains the Monitoring-Time AVP. The PCRF also includes USAGE_MONITORING_REPORT_REQUIRED in a Usage-Monitoring-Information AVP.

10. This step occurs asynchronously along with the previous step. The PCRF updates the quota records of the user indicating the quota has reset by sending a PUR to the SPR.

| Name | Default Value | Description |
|---|---|---|
| DB.User.BillingRevalidationTimeInterval | 1800 | Range in seconds from the end billing date that a random revalidation time will be chosen. |

11. The SPR responds with a PUA.

12. The PCEF sends a CCR-update to the PCRF in response to receiving the USAGE_MONITORING_REPORT_REQUIRED. This message includes 2 Used-Service-Unit AVPs, where 1 of them contains the Monitoring-Time AVP.

13. The PCRF calculates a new grant based off of a new cycle beginning and sends a CCA-update to the PCEF containing 2 Granted-Service-Unit AVPs, where 1 of them contains the Monitoring-Time AVP.

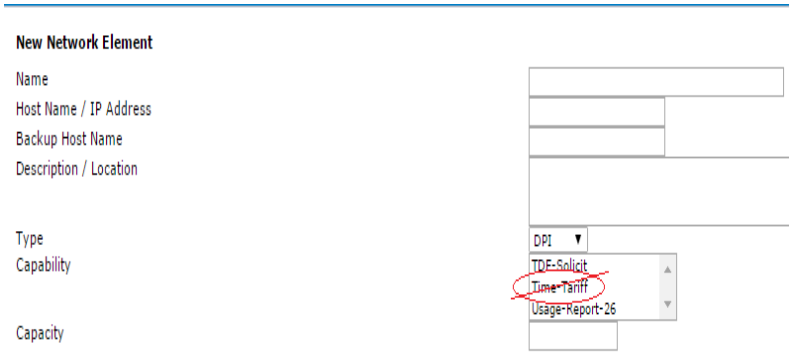
14. This step occurs asynchronously along with the previous step. The PCRF updates the quota records of the user from the Used-Service-Unit AVP that contained the Monitoring-Time and reports this to the SPR in a PUR.

15. The SPR responds with a PUA.

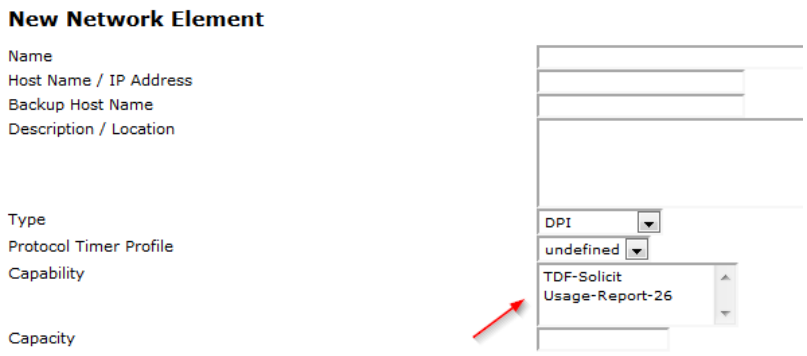
### *3.20.3 User Interface Changes*

Functionality related to the proprietary version of Time-Tariff support is being removed. This includes the network capability called “Time-Tariff” for DPI and PGW network elements.

The figure below show the former value “Time-Tariff” for the network capability is being removed




The figure below show the Policy Management R12.2.0 with values only TDF-Solicit and Usage-Report-26




Configuration Changes: The below configuration key that are configured as overrides on the Advanced Settings tab in CMP

This service override can be used to increase the range that the PCEF will report usage at the end of a billing cycle. By default this is set to a window of 1800 seconds (half-hour) after the billing cycle ends.

## 3.21 3GPP SUPPORT TIME-BASED USAGE MANAGEMENT/TIMEBASEDUM (PR# 20224100)

### 3.21.1 Introduction

This feature introduces support for Time-Based Usage Management as defined by 3GPP 29.212 [5]. V12.9. The PCRF will support this functionality when the PCEF provides the TimeBasedUM supported feature upon session establishment for Gx or Sd protocol applications.

### 3.21.2 Detailed Description

The PCRF will now support Time-Based Usage Management for both the Gx and Sd protocol applications. For Gx this feature is enabled if the TimeBasedUM and REL9 supported features are included on a CCR-initial message. It is enabled for Sd if the TimeBasedUM supported feature is included in both the TSR and TSA messages. The PCRF will send the TimeBasedUM supported feature on the TSR if it receives this supported feature over the Gx interface.

From the PCRF point of view, the TimeBasedUM supported feature indicates that CC-Time can be used to grant units to the PCEF within the Granted-Services-Unit AVP. In order to support this, a number of policies, as shown in 2.2.1, are updated to support time based grants. The PCEF will then begin usage tracking and report any usage for CC-Time in a Used-Service-Unit AVP. The PCRF will then record this usage to the SPR.

In addition, 29.212 defines a new Quota-Consumption-Time AVP which specifies the Inactivity Detection Time. The inactivity detection time is configurable per quota plan, pass, or top-up as shown in section 2.2.2. If this is configured it would then be included within the Usage-Monitoring-Information AVP anytime a policy to grant time units is applied and sent on the CCA. This value indicates the time interval in seconds after which the time measurement shall stop for the Monitoring Key, if no packets are received belonging to the corresponding Monitoring Key.

The new supported features and AVPs are shown below: TimeBasedUM Feature of Feature-List-ID used in Gx/Sd

| .Feature bit | Feature | M*andatory*/O*ptional* | Description |
|---|---|---|---|
| 15 (Gx)/ 2 (Sd) | TimeBasedUM | O | This feature indicates support for Time based Usage Monitoring Control. If the PCEF supports this feature, the behaviour shall be as specified in corresponding sub clauses in the 3GPP specification. |

Quota-Consumption-Time AVP

| AVP Name | AVP Code | Used in | | | | Value Type | AVP Flag rules | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ACR | ACA | CCR | CCA | | Must | May | Should not | Must not | May Encr. |
| Quota-Consumption-Time | 881 | - | - | - | X | Unsigned32 | V,M | P | | | N |

**AVP Formats:**

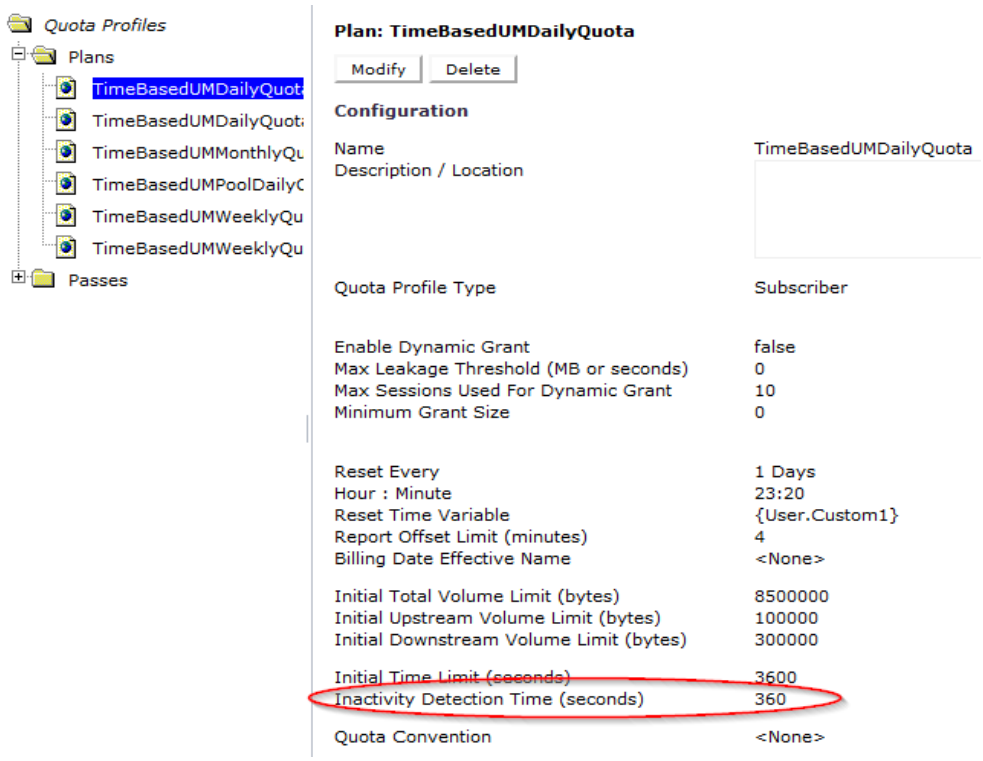
```
Usage-Monitoring-Information::= < AVP Header: 1067 >
                                [ Monitoring-Key ]
                              0*2[ Granted-Service-Unit ]
                              0*2[ Used-Service-Unit ]
                                [ Quota-Consumption-Time ]
                                [ Usage-Monitoring-Level ]
                                [ Usage-Monitoring-Report ]
                                [ Usage-Monitoring-Support ]

                             *[ AVP ]
```

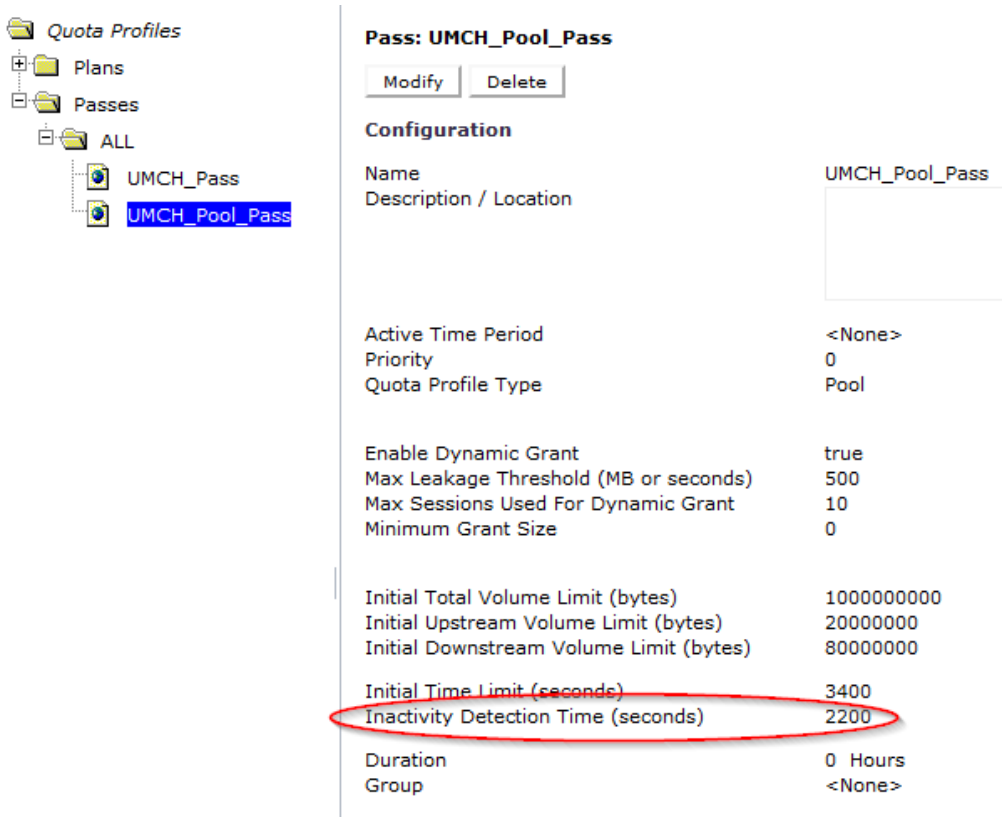
***Quota-Consumption-Time included in Usage-Monitoring-Information AVP***

```
Granted-Service-Unit ::= < AVP Header: 431 >
                                 [ CC-Time ]
                                 [ CC-Total-Octets ]
                                 [ CC-Input-Octets ]
                                 [ CC-Output-Octets ]
                                *[ AVP ]
```

### *3.21.3 User Interface Changes*

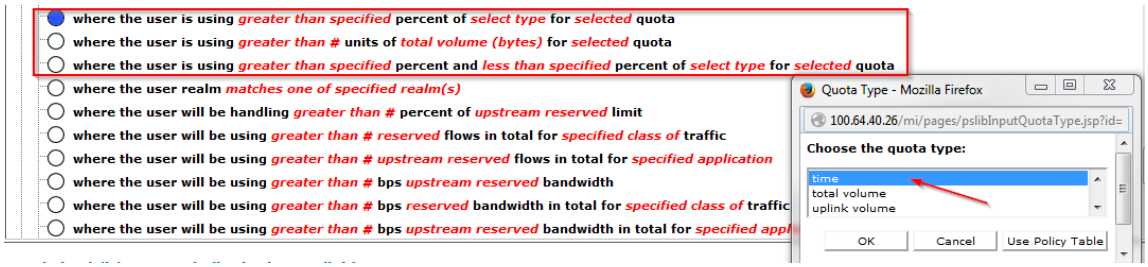
- In order to support the Quota-Consumption-Time AVP, a new configurable field "Inactivity Detection Time" is added. This field only becomes editable when the Initial Time Limit is specified**.**



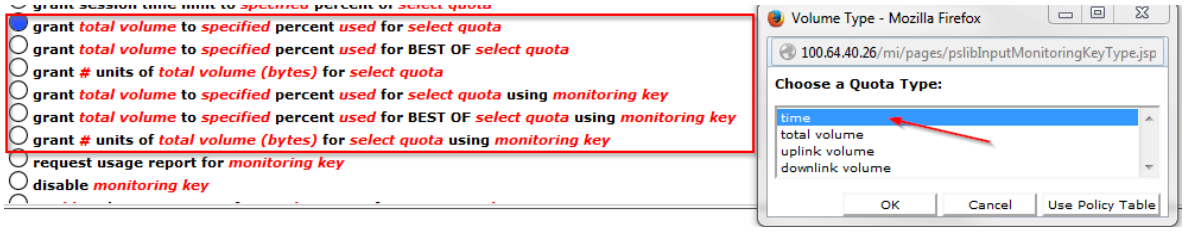



**Policy condition/action changes:**

- There are policy conditions that check or specify the type of quota. Previously most of these only included the option for ***the volume types: total, uplink, and downlink***. Now this will include the option to pick the ***quota type of "time".***
- The new option Quota Type "***time***" and the policies affected by this are shown in the figure below




- There are many policy actions and conditions that check or specify the type of quota. Previously most of these only included the option for the **volume types**: ***total, uplink, and downlink***. Now this will include the option to pick the quota type of "***time***".
- The new option Quota Type "***time***" and the policies affected by this are shown in the figure below




- The below policy condition group summarizes policies affected with description

| Policy Condition Group | Policy Condition or Action | Description |
|---|---|---|
| "grant" Actions | **grant *total volume* to *#* percent *used* for *select quota*** | ➢ Grant the specified quota type[1] for the selected quota with a percentage |
| | **grant *total volume* to *#* percent *used* for BEST OF *select quota*** | ➢ Grant the specified quota type[1] for the selected quota(s) using the best of algorithm from FD007618 with a percentage |
| | **grant *total volume* to *#* bytes for *select quota*** | ➢ Grant the specified quota type[1] for the selected quota with absolute bytes |
| | **grant *total volume* to *#* percent *used* for *select quota* using *monitoring key*** | ➢ Grant the specified quota type[1] for the selected quota using a monitoring key with a percentage |
| | **grant *total volume* to *#* percent *used* for BEST OF *select quota* using *monitoring key*** | ➢ Grant the specified quota type[1] for the selected quota(s) using the best of algorithm from FD007618 with a percentage using a monitoring key |
| | **grant *total volume* to *#* bytes of *select quota* using *monitoring key*** | ➢ Grant the specified quota type[1] for the selected quota with absolute bytes using a monitoring key |
| | **grant *#* percent of *select type* for BEST OF *select quota*** | ➢ Grant the specified quota type[1] for the selected quota(s) using the best of algorithm from FD007618 with a percentage |
| Quota Conditions | **where the user is using *greater than* *#* percent of *select type* for *selected* quota** | Check to see how much quota the user has consumed based on percentage and quota type[1] |
| | **where the user is using *greater than* *#* bytes in *total volume* for *selected* quota** | Check to see how much quota the user has consumed based on absolute bytes and quota type[1] |
| | **where the user is using *greater than* *#* percent and *less than* *#* percent of *select type* for *selected* quota** | Check to see how much quota the user has consumed based on percentage and quota type[1] with multiple conditions |

[1] The quota type will now include the following choices: Time, Total Volume, Uplink Volume, and Downlink Volume

## 3.22 3GPP APPLICATION BASED CHARGING (PR# 21322637)

### 3.22.1 Introduction

This feature adds support for the Application-Based Charging functionality to Gx and Sd interfaces as it is described in 3GPP TS 29.212 Rel 12 to PCRF. This functionality includes support of the new and re-used related AVPs as well as new "ABC" Supported-Feature for Gx and Sd protocols and procedures accordingly.

### 3.22.2 Detailed Description

To Support the ABC feature, PCRF and TDF have to negotiate a new supported feature

| Feature bit | Feature | Mandatory/Optional (M/O) | Description |
|---|---|---|---|
| 17 (Gx) / 4 (Sd) | ABC | O | This feature indicates support for Application Based Charging. |

Gx / Sd AVPs for ABC Support*:*

New Gx AVP
*Credit-Management-Status AVP*
*PCEF Gx interface CCR-I contains Diameter Gx re-used existing AVPs to support ABC feature:*
*Charging-Characteristics-3GPP → 3GPP-Charging-Characteristics as 4 hex digits (e.g. "0800"),*
*GGSN-Address-3GPP → 3GPP GGSN Address, ABC Feature*
*GGSN-IPv6-Address-3GPP → 3GPP GGSN IPv6 Address, ABC Feature*
*Dynamic-Address-Flag → 3GPP , 0- static, 1- dynamic, ABC Feature*
*Dynamic-Address-Flag-Extension AVP → 3GPP , 0- static, 1- dynamic, ABC Feature*
*Selection-Mode-3GPP AVP → The 3GPP-Selection-Mode, ABC Feature*
*PDN-Connection-Charging-ID AVP → The PDN-Connection-Charging-ID, ABC Feature*
*User-CSG-Information Grouped AVP*
CSG-Access-Mode avp
CSG-Membership-Indication avp
CSG-Id avp

The above AVPs are propagated to the TDF Sd interface in the TSR message. The only difference is the Supported Feature Bit is set to 16 (bit 4) for Sd interface, and for Gx CCR-I this value is 131072 (bit 17).

User-CSG-Information AVP and Credit-Management-Status AVP are only applicable when ABC feature is supported.

To support ABC feature functionality a new event trigger is added to Gx:

CREDIT_MANAGEMENT_SESSION_FAILURE (46).

The following event triggers values are applicable when ABC feature is supported:

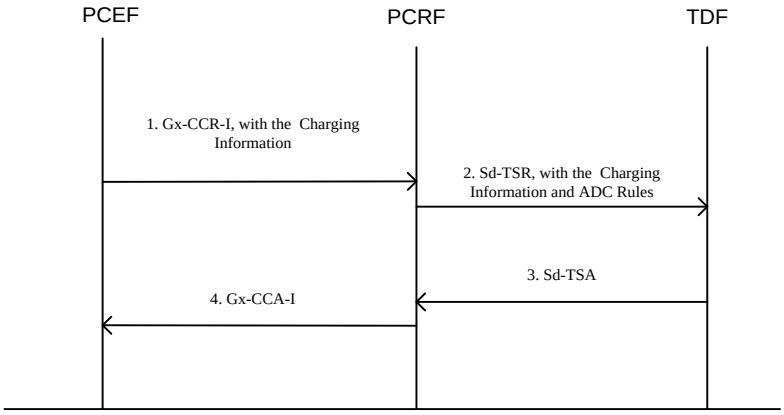
OUT_OF_CREDIT (15),
REALLOCATION_OF_CREDIT (16),
USER_CSG_INFORMATION_CHANGE (30),

USER_CSG_HYBRID_SUBSCRIBED_INFORMATION_CHANGE (35),
USER_CSG_ HYBRID_UNSUBSCRIBED_INFORMATION_CHANGE (36),
CREDIT_MANAGEMENT_SESSION_FAILURE (46).

**NOTE:** CREDIT_MANAGEMENT_SESSION_FAILURE(46) - When used in a CCR command, this value indicates that a transient/permanent failure has been detected in the OCS. If the failure does not apply to all PCC Rules, the affected PCC Rules are indicated within the Charging-Rule-Report AVP, with the PCC-Rule-Status set to value ACTIVE and the Rule-Failure-Code AVP set to the corresponding value as reported by the OCS. If the failure applies to the session, the Credit-Management-Status shall be set to the corresponding value as reported by the OCS

Note: For the PCEF, CREDIT_MANAGEMENT_SESSION_FAILURE event trigger only applies to the situation that the IP-CAN session is not terminated by the PCEF due to the credit management session failure.

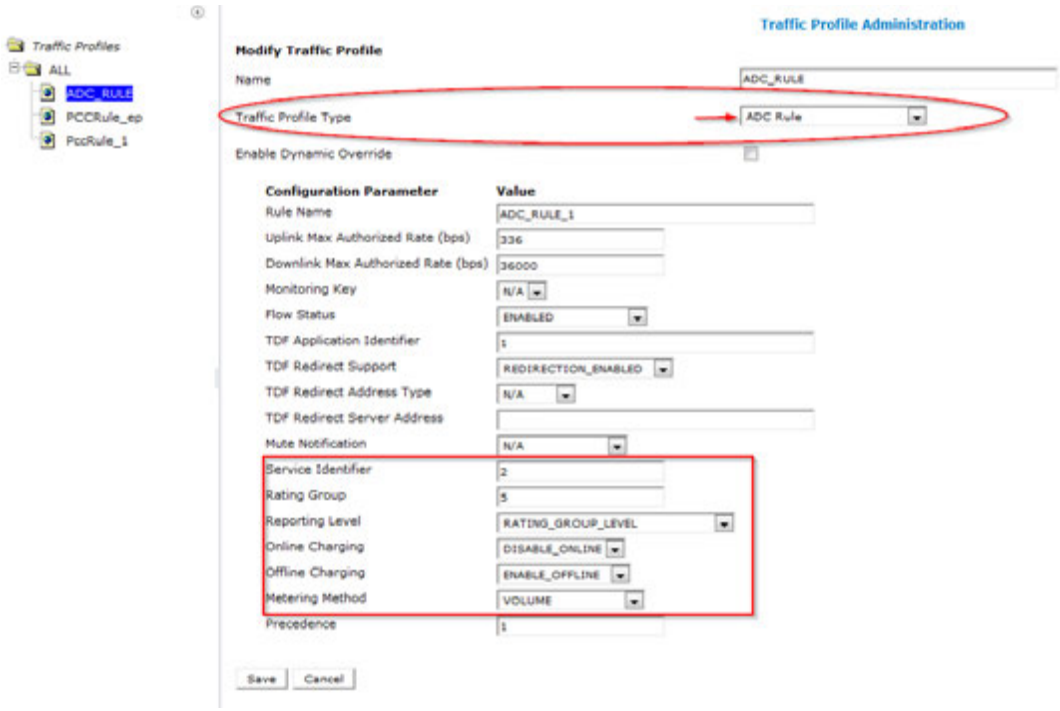
Call Flow: Propagation of the Charging Information to TDF




### *3.22.3 User Interface Changes*

CMP GUI – 'Traffic Profiles' UI changes

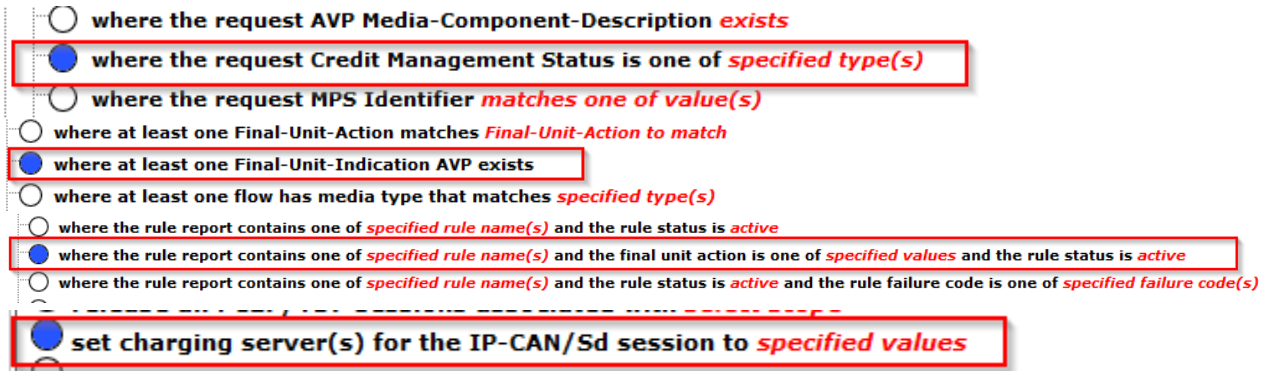
- To accommodate the new AVPs the definition of '***ADC Rule***' Traffic Profile Type has been ***extended*** by this feature to contain the Charging Information used for the Application Based Charging.




CMP GUI – 'Policy' UI changes

- There is a new policy condition introduced to support ABC feature by a policy server. Two existing conditions and an action that can be applicable to Sd protocol.

| Policy Condition Group | Policy Condition or Action | Description |
|---|---|---|
| "Request" Conditions(New) | where the request Credit Management Status is one of {1} | Identifies Credit Management status reported by TDF |
| "Request" Conditions (Extended) | where at least one Final-Unit-Indication AVP exists | This condition can be used in conjunction with the ADC rule report to identify final unit indication state over Sd protocol |
| "Request" Conditions (Extended) | where the rule report contains one of {0} and the final unit action is one of {1} and the rule status is {2} | This condition can be used in conjunction with the ADC rule report to identify final unit indication state over Sd protocol |
| Action (Extended) | set charging server(s) for the IP-CAN/Sd session to specified values | This action can be applied to Sd protocol when ABC feature is enabled; For example: set charging server(s) for the IP-CAN/Sd session to Primary Online Server:OCS1, Primary Offline OFCS |



## 3.23 7.404: EVS CODEC SUPPORT (PR# 22135682)

### 3.23.1 Introduction

EVS is a codec which has been adopted by 3GPP, defined in 3GPP TS 26.114. The PCRF NATIVELY supports the EVS (Enhanced Voice Services) Codec. The EVS codec provides the same audio quality with lower capacity requirements or higher audio quality with same capacity requirement as today's AMR-WB codec.

### 3.23.2 Detailed Description

This feature support the bandwidth computation based on the codec data offered in the SDP messages. The EVS codec includes two operational modes:

- EVS Primary mode: Includes 11 bit-rates for fixed-rate or multi-rate operation; 1 average bit-rate for variable bit-rate operation; and 1 bit-rate for SID (3GPP TS 26.441).
- EVS AMR-WB IO mode: Includes 9 codec modes and SID. All are bitstream interoperable with the AMR-WB codec (3GPP TS 26.171).

The mode (EVS Primary mode/ EVS AMR-WB IO mode), br/br-send/br-recv, ptime, channels count, IPv4/IPv6 are the keys to decide the bandwidth of audio flow with EVS codec.

PCRF can give the desired bandwidth according to the Coded parameters.

### 3.23.3 EVS Codec Support Use case Example

This use case is to verify that the PCRF derives the correct bandwidth for Codec "EVS" in diameter message. In this case EVS is "primary mode" and whose *ptime is 20ms, bitrate is 7.2 kbps*

- From PGW establish a Gx session with IPv4 framed IP and other Required AVPs
- Establish Rx session over IPv4 flow and other Required EVS parameter AVPs
- Check Maximum Bandwidth in RAR sent to PGW
  - Based on below Bandwidth Computation of b=AS for EVS Primary mode (IPv4, ptime=20)

| Mode | 7.2 | 8 | 9.6 | 13.2 | 16.4 | 24.4 | 32 | 48 | 64 | 96 | 128 | SID |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AS (kbps) | **25** | 25 | 27 | 30 | 34 | 42 | 49 | 65 | 81 | 113 | 145 | N/A |

- Maximum Rate bandwidth of Uplink and down link RTP flow of Rx set to 25Kbytes/sec
- Rule installed on Gx session from Rx session has Maximum-Requested bandwidth (UL/DL) of 25Kbytes/sec

*Screenshots:*

- *From PGW establish a Gx session with IPv4 framed IP*

```
Diameter Message: CCR
Version: 1
Msg Length: 764
Cmd Flags: REQ,PXY
Cmd Code: 272
App-Id: 16777238
Hop-By-Hop-Id: 0
End-To-End-Id: 1618920827
  Session-Id (263,M,l=20) = diamcliGx.01
  Origin-Host (264,M,l=22) = pgw.oracle.com
  Origin-Realm (296,M,l=18) = oracle.com
  Auth-Application-Id (258,M,l=12) = 16777238
  Destination-Realm (283,M,l=18) = oracle.com
  CC-Request-Type (416,M,l=12) = INITIAL_REQUEST (1)
  CC-Request-Number (415,M,l=12) = 0
  User-Equipment-Info (458,,l=44) =
    User-Equipment-Info-Type (459,,l=12) = IMEISV (0)
    User-Equipment-Info-Value (460,,l=23) = 012345678901234
  Subscription-Id (443,M,l=44) =
    Subscription-Id-Type (450,M,l=12) = END_USER_IMSI (1)
    Subscription-Id-Data (444,M,l=23) = 012345678901234
  Subscription-Id (443,M,l=40) =
    Subscription-Id-Type (450,M,l=12) = END_USER_E164 (0)
    Subscription-Id-Data (444,M,l=18) = 9139915732
  Origin-State-Id (278,M,l=12) = 0x12345607
  Framed-IP-Address (8,M,l=12) = 10.254.10.1
  SGSN-Address-3GPP (6,VM,v=10415,l=16) = 202.73.195.28
  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=44) =
    APN-Aggregate-Max-Bitrate-DL (1040,V,v=10415,l=16) = 8640000
    APN-Aggregate-Max-Bitrate-UL (1041,V,v=10415,l=16) = 32000000
  RAI (909,VM,v=10415,l=23) = MCCMNC=10100 LAC=53 RAC=0
  User-Location-Info-3GPP (22,VM,v=10415,l=20) = Type=CGI(0) MCCMNC=10100 LAC=35 CI=50521
  Called-Station-Id (30,M,l=19) = testapn.com
  Bearer-Control-Mode (1023,VM,v=10415,l=16) = UE_NW (2)
  SGSN-MCC-MNC-3GPP (18,VM,v=10415,l=17) = 10100
  Default-EPS-Bearer-QoS (1049,V,v=10415,l=88) =
    QoS-Class-Identifier (1028,VM,v=10415,l=16) = 7
    Allocation-Retention-Priority (1034,V,v=10415,l=60) =
      Priority-Level (1046,V,v=10415,l=16) = 4
      Preemption-Capability (1047,V,v=10415,l=16) = PREEMPTION_CAPABILITY_DISABLED (1)
      Preemption-Vulnerability (1048,V,v=10415,l=16) = PREEMPTION_VULNERABILITY_ENABLED (0)
```

The AF/Rx session correlates to the Gx session based on Framed-IP-Address

- *Establish Rx session over IPv4 flow*

```
processing Rx AAR message for session: diamcliRx.01
Message Sent:

Diameter Message: AAR
Version: 1
Msg Length: 652
Cmd Flags: REQ,PXY
Cmd Code: 265
App-Id: 16777236
Hop-By-Hop-Id: 0
End-To-End-Id: 3630177949
  Session-Id (263,M,l=20) = diamcliRx.01
  Origin-Host (264,M,l=21) = af.oracle.com
  Origin-Realm (296,M,l=18) = oracle.com
  Auth-Application-Id (258,M,l=12) = 16777236
  Destination-Realm (283,M,l=18) = oracle.com
  Media-Component-Description (517,VM,v=10415,l=524) =
    Media-Component-Number (518,VM,v=10415,l=16) = 1
    Media-Sub-Component (519,VM,v=10415,l=164) =
      Flow-Number (509,VM,v=10415,l=16) = 1
      Flow-Description (507,VM,v=10415,l=66) = permit out 17 from 10.0.1.229 11112 to 10.0.1.228 1240
      Flow-Description (507,VM,v=10415,l=65) = permit in 17 from 10.0.1.228 1240 to 10.0.1.229 11112
    AF-Application-Identifier (504,VM,v=10415,l=14) = vp
    Media-Type (520,VM,v=10415,l=16) = AUDIO (0)
    Max-Requested-Bandwidth-UL (516,VM,v=10415,l=16) = 60000
    Max-Requested-Bandwidth-DL (515,VM,v=10415,l=16) = 60000
    Flow-Status (511,VM,v=10415,l=16) = ENABLED (2)
    Codec-Data (524,VM,v=10415,l=129) =
      uplink
      offer
      m=audio 1240 RTP/AVP 97
      a=rtpmap:97 EVS/16000
      a=fmtp:97 br=7.2; bw=nb; max-red=220
      a=ptime:20
    Codec-Data (524,VM,v=10415,l=127) =
      downlink
      answer
      m=audio 11112 RTP/AVP 97
      a=rtpmap:97 EVS/16000
      a=fmtp:97 br=7.2; bw=nb; max-red=220
      a=ptime:20
  Framed-IP-Address (8,M,l=12) = 10.254.10.1
```

The EVS Codec-Data with uplink and downlink parameters

Framed-IP-Address

- *Rule installed on Gx session from Rx session has Maximum-Requested bandwidth (UL/DL) of 25Kbytes/sec*
- *Maximum Rate bandwidth of Uplink and down link RTP flow of Rx set to 25Kbytes/sec*

```
Diameter Message: RAR
Version: 1
Msg Length: 608
Cmd Flags: REQ,PXY
Cmd Code: 258
App-Id: 16777238
Hop-By-Hop-Id: 1628589390
End-To-End-Id: 611876557
  Session-Id (263,M,l=20) = diamcliGx.01
  Origin-Host (264,M,l=29) = ohio-mpe-1.oracle.com
  Origin-Realm (296,M,l=18) = oracle.com
  Destination-Realm (283,M,l=18) = oracle.com
  Destination-Host (293,M,l=22) = pgw.oracle.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=416) =
    Charging-Rule-Definition (1003,VM,v=10415,l=404) =
      Charging-Rule-Name (1005,VM,v=10415,l=15) = 0_1
      Flow-Information (1058,V,v=10415,l=96) =
        Flow-Direction (1080,V,v=10415,l=16) = UPLINK (2)
        Flow-Description (507,VM,v=10415,l=65) = permit in 17 from 10.0.1.228 1240 to 10.0.1.229 11112
      Flow-Information (1058,V,v=10415,l=96) =
        Flow-Direction (1080,V,v=10415,l=16) = DOWNLINK (1)
        Flow-Description (507,VM,v=10415,l=66) = permit out 17 from 10.0.1.229 11112 to 10.0.1.228 1240
      Flow-Status (511,VM,v=10415,l=16) = ENABLED (2)
      QoS-Information (1016,VM,v=10415,l=152) =
        QoS-Class-Identifier (1028,VM,v=10415,l=16) = 1
        Guaranteed-Bitrate-UL (1026,VM,v=10415,l=16) = 25000
        Guaranteed-Bitrate-DL (1025,VM,v=10415,l=16) = 25000
        Max-Requested-Bandwidth-UL (516,VM,v=10415,l=16) = 25000
        Max-Requested-Bandwidth-DL (515,VM,v=10415,l=16) = 25000
        Allocation-Retention-Priority (1034,V,v=10415,l=60) =
          Priority-Level (1046,V,v=10415,l=16) = 15
          Preemption-Capability (1047,V,v=10415,l=16) = PREEMPTION_CAPABILITY_DISABLED (1)
          Preemption-Vulnerability (1048,V,v=10415,l=16) = PREEMPTION_VULNERABILITY_ENABLED (0)
      Precedence (1010,VM,v=10415,l=16) = 400
  Route-Record (282,M,l=29) = ohio-mpe-1.oracle.com
```

bandwidth computation of EVS Codec Primary mode (IPV4, ptime=20)
Rule installed on Gx session from Rx session has Maximum-Requested bandwidth (UL/DL) of 25Kbytes/sec

## 3.24 TRACK MAXIMUM TPS IN KPI INTERVAL (PR# 19113866 )

### 3.24.1 Introduction

Currently, as part of KPI Stats, TPS stats are captured in sum total and do not include TPS per message type. This feature shall add TPS stats per message type for various interface like Gx, Rx, Sh etc. This will help in exactly determining TPS behavior for each interface/each message and will help in solving related issues.

### 3.24.2 Detailed Description

During upgrade from previous release to a release containing these enhancements, the default value of Stats Reset Configuration is changed from 'Manual' to 'Interval'. For other TPS stats, there is no impact as they are not displayed on CMP

Currently TPS is calculated in system as:

Total number of Transaction initiating messages received (since last count)/ Time difference (since last count; in seconds)

As part of this feature, the TPS shall be tracked for each message type on each interface. So, for ex, TPS related to CCR-I messages on Gx interface shall be calculated as:
PCEF_CCRI_MAX_TPS = Number of CCR-I received on Gx (since last count) /
Time difference (since last count; in seconds)

- All Diameter interfaces are supported and tracked separately
- A timestamp of when the maximum TPS was reached for each message type (for each interface) will be included.
- TPS Stats (per message type) related to the Cable interface (Rx/PCMM) is not part of this feature (Rx in Wireless environment is supported).
- These Stats are stored on both MPE & MRA. None of the these stats are displayed on CMP
- These Stats are available to be queried via the OSSI Interface

**Maximum TPS Stats for PCEF (Gx) Interface**

| Reference Name | MPE/MRA Counter Name |
|---|---|
| PCEF_CCRI_CURRENT_TPS | PcefCCRICurrentTPS |
| PCEF_CCRI_MAX_TPS | PcefCCRIMaxTPS |
| PCEF_CCRI_TIME_MAX_TPS | PcefCCRITimeOfMaxTPS |
| | |
| PCEF_CCRU_CURRENT_TPS | PcefCCRUCurrentTPS |
| PCEF_CCRU_MAX_TPS | PcefCCRUMaxTPS |
| PCEF_CCRU_TIME_MAX_TPS | PcefCCRUTimeOfMaxTPS |
| | |
| PCEF_CCRT_CURRENT_TPS | PcefCCRTCurrentTPS |
| PCEF_CCRT_MAX_TPS | PcefCCRTMaxTPS |
| PCEF_CCRT_TIME_MAX_TPS | PcefCCRTTimeOfMaxTPS |
| | |
| PCEF_RAR_CURRENT_TPS | PcefRARCurrentTPS |
| PCEF_RAR_MAX_TPS | PcefRARMaxTPS |
| PCEF_RAR_TIME_MAX_TPS | PcefRARTimeOfMaxTPS |
| | |

## OSSI

A new query will be added to the existing commands to allow users to request TPS statistics for a specified time range. A query request can contain a number of parameters that allow the user to request a specific set of data and format how that data is returned. Here are example request and response to help demonstrate the changes that will be made to this interface:

```
<?xml version="1.0" encoding="UTF-8"?>
<XmlInterfaceRequest>
  <QueryOmStats DeltaCount="false">
   <StartTime>2010-07-23T18:35:00Z</StartTime>
    <TpsStats>
      <PolicyServer>kiran-anchorage-mpe</PolicyServer>
      <MRA></MRA>
    </TpsStats>
  </QueryOmStats>
</XmlInterfaceRequest>
```

This is the example response:

```
<?xml version='1.0' ?>
<Statistics>
  <TpsStats>
    <Sample>
      <StartTime>2015-08-31T19:43:39Z</StartTime>
      <EndTime>2015-08-31T20:21:52Z</EndTime>
      <PolicyServer>kiran-anchorage-mpe</PolicyServer>
      <AfAARICurrentTPS>1306</AfAARICurrentTPS>
      <AfAARIMaxTPS>306</AfAARIMaxTPS>
      <AfAARITimeOfMaxTPS>2015-08-31T20:21:52Z</AfAARITimeOfMaxTPS>
      <AfAARMCurrentTPS>13</AfAARMCurrentTPS>
      <AfAARMMaxTPS>5</AfAARMMaxTPS>
      <AfAARMTimeOfMaxTPS>2015-08-31T20:21:52Z</AfAARMTimeOfMaxTPS>
      <AfASRCurrentTPS>13</AfASRCurrentTPS>
      <AfASRMaxTPS>5</AfASRMaxTPS>
      <AfASRTimeOfMaxTPS>2015-08-31T20:21:52Z</AfASRTimeOfMaxTPS>
      <AfSTRCurrentTPS>13</AfSTRCurrentTPS>
      <AfSTRMaxTPS>5</AfSTRMaxTPS>
      <AfSTRTimeOfMaxTPS>2015-08-31T20:21:52Z</AfSTRTimeOfMaxTPS>
...
      <RadiusAccountingOffCurrentTPS >0</RadiusAccountingOffCurrentTPS >
      <RadiusAccountingOffMaxTPS>0</RadiusAccountingOffMaxTPS>
      <RadiusAccountingOffTimeOfMaxTPS>2015-08-31T20:21:52Z</RadiusAccountingOffTimeOfMaxTPS>
      <RadiusAccountingOffCurrentTPS>
    </Sample>
  </TpsStats>
</Statistics>
```

New command (in mramgr and rcmgr) ‘show counters tpsstats’ will list new TPS stats

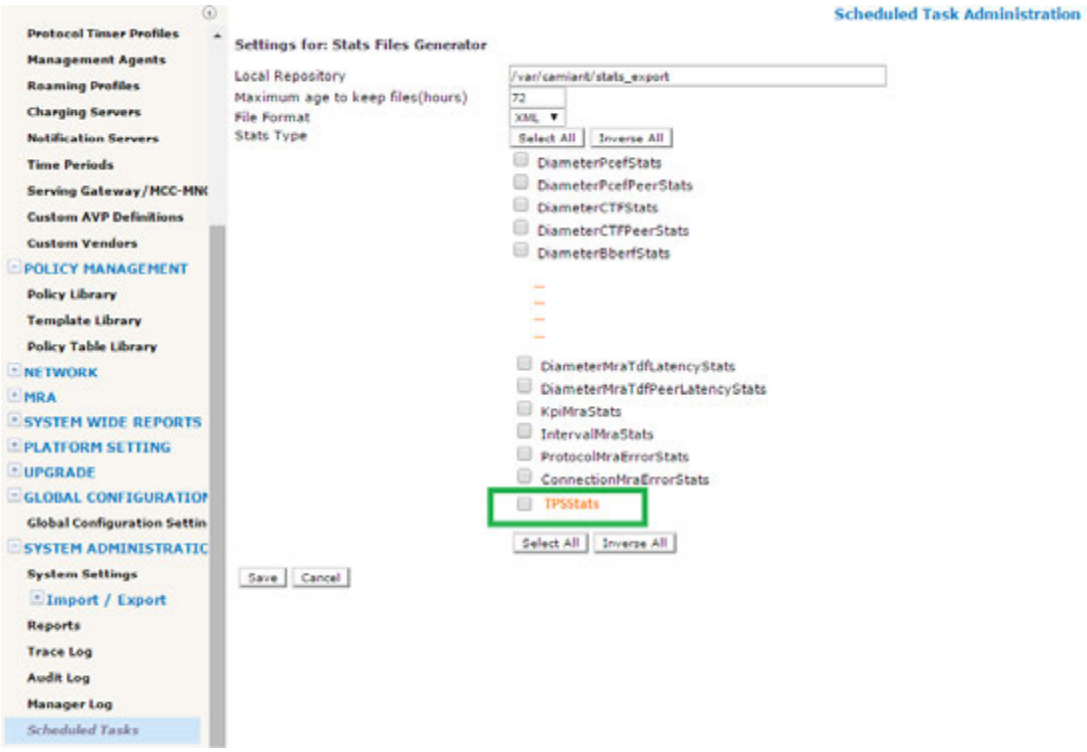
**Performance Impacts**

Addition of new stats will not have any performance impact on MPE/MRA.

### *3.24.3 User Interface Changes*

A new category of stats named “TPSStats” is created to track TPS per message type under each interface.

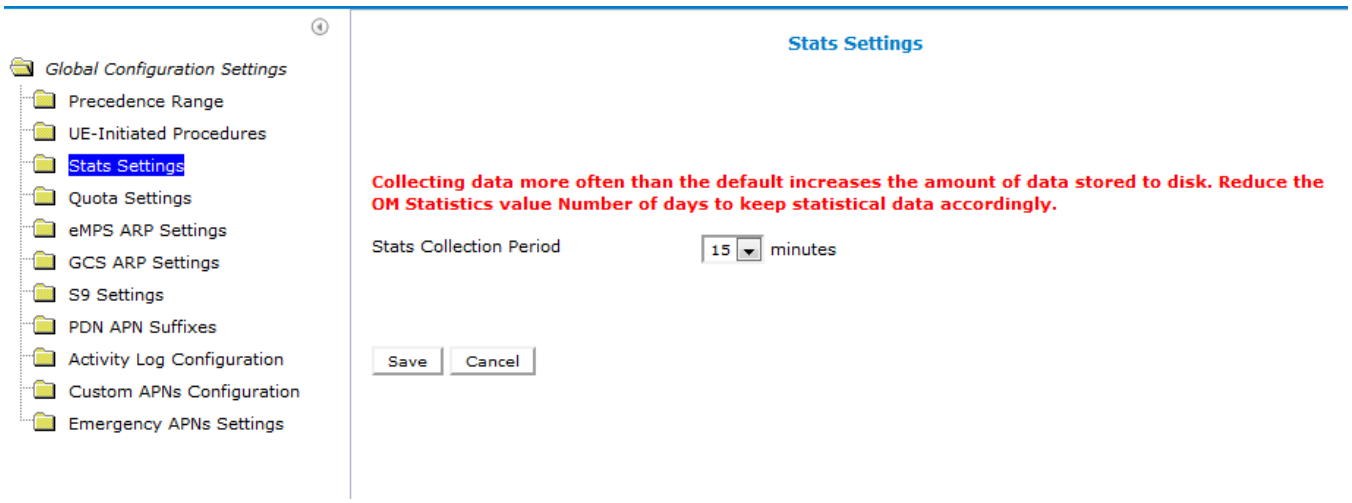
The new category is added under Statistics Generator files



## Default Interval Mode for Stats

The Stats settings under ‘Global Configuration Settings’ will now show Stats Collection Period of ‘15’ minutes.

***KPI Interval Stats as default***



## 3.25 ADD AUDIT LOG TO CMP SAVELOG ( PR# 20319847 )

### 3.25.1 Introduction

This enhancement adds the audit logs to the CMP savelog.

### 3.25.2 Detailed Description

As part of this feature, CMP savelog shall now include CMP Audit logs (as displayed under System Administration -> Audit logs) for last 2 months.

The procedure to take savelog is same as before: from platcfg menu; Policy Configuration -> Save Platform Debug Logs. All other options under this remain as before

There are 2 options to capture auditlog data: either in .xml file OR in .txt file. Sample output of both is captured:

Sample output of auditlog.txt:

```
281474976711135	2015-08-04 05:19:22	admin	10.176.255.9	user	login	MPE Manager	admin	2015-08-04 05:19:22
1	\N	\N
281474976711136	2015-08-04 05:19:46	admin	10.176.255.9	user	changePassword	admin	2015-08-04 05:19:46
1	\N	\N
281474976711137	2015-08-04 05:50:49	admin	10.176.255.9	user	logout	admin	2015-08-04 05:50:49
1	\N	\N
281474976810657	2015-08-05 01:29:49	admin	10.176.255.9	user	login	MPE Manager	admin	2015-08-05 01:29:49
1	\N	\N
```

Sample output of auditlog.xml:


```
<?xml version="1.0"?>

 <row>
	<field name="uid">281474976711134</field>
	<field name="timestamp">2015-08-04 05:19:07</field>
	<field name="username"></field>
	<field name="hostname"></field>
	<field name="auditclass">manager</field>
	<field name="auditaction">modify</field>
	<field name="key1"></field>
	<field name="key2"></field>
	<field name="mscname"></field>
	<field name="mschostname"></field>
	<field name="details">Architecture&lt;br&gt;&amp;nbsp;&amp;nbsp;&amp;nbsp; {auditLog.valueOld}
standalone&lt;br&gt;&amp;nbsp;&amp;nbsp;&amp;nbsp; {auditLog.valueNew}
distributed&lt;br&gt;MiMode&lt;br&gt;&amp;nbsp;&amp;nbsp;&amp;nbsp; {auditLog.valueNew}
DiamAF,Diam3gppPCEF,gxquota&lt;br&gt;</field>
	<field name="createtimestamp">2015-08-04 05:19:07</field>
	<field name="createuser" xsi:nil="true" />
	<field name="modifytimestamp" xsi:nil="true" />
	<field name="modifyuser" xsi:nil="true" />
 </row>
```

### *3.25.3 User Interface Changes*

None.

## 3.26 EXPOSE ENGINEERING LOG LEVEL CONFIGURATION IN CMP ( PR# 20325595 )

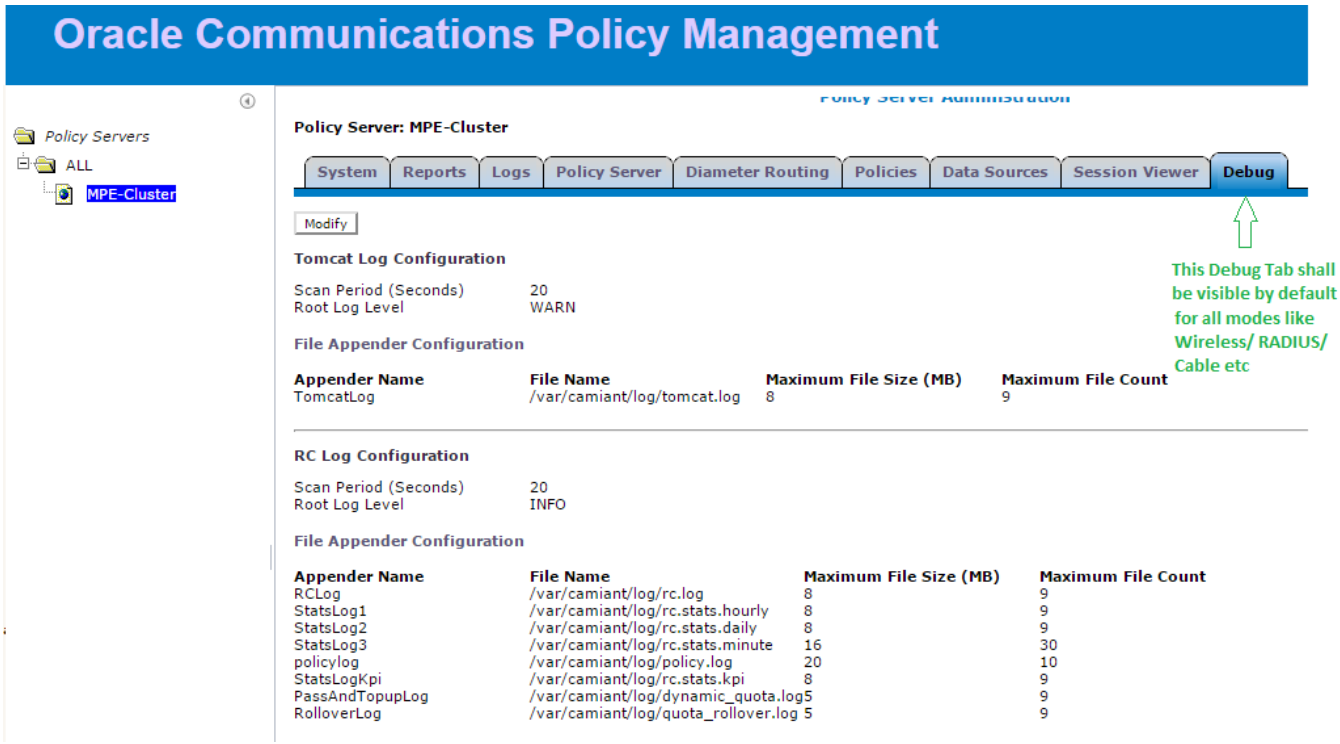
### 3.26.1 Introduction

Currently, in order to debug customer issues, files logback-tomcat.log, logback-rc.xml, logback-mra.xml, and logback-bod.xml have to be modified at each target MPE/MRA/BoD to enable specific component level logging. This consumes a lot of time. This enhancement allows the operator to easily enable debug-level logging from CMP for the specific component as required.

### 3.26.2 Detailed Description

Currently, the Debug tab on CMP is visible only if 'Debug mode' is enabled. As part of enhancement 'Enable Debug Logging via CMP', debug tab on CMP shall be enabled by default for any mode (Wireless/Cable/ SPC, RADIUS, BoD etc) irrespective of Debug mode – on MPE / MRA/BoD. This includes for any option selected under these modes.

By default, modify in this tab shall be allowed only for Role: 'Administrator'. For all other roles, this tab will by default be 'Read-Only'




***Debug page on CMP***

**NOTE**: The debug tab will not be available via Configuration Template.

**Enhancements to Debug page for supporting class log level - MPE**

Currently, as shown above, the Debug page on CMP does not support configuring log level per class for any component. For ex, if someone wants to enable DEBUG log level for particular class for RC component, then the same can't be done. This has to be done manually by logging into MPE & changing the corresponding logback-rc.xml file respectively.

As part of enhancement 'Enable Debug Logging via CMP', the Debug page has been enhanced to support class log level for different components in the MPE

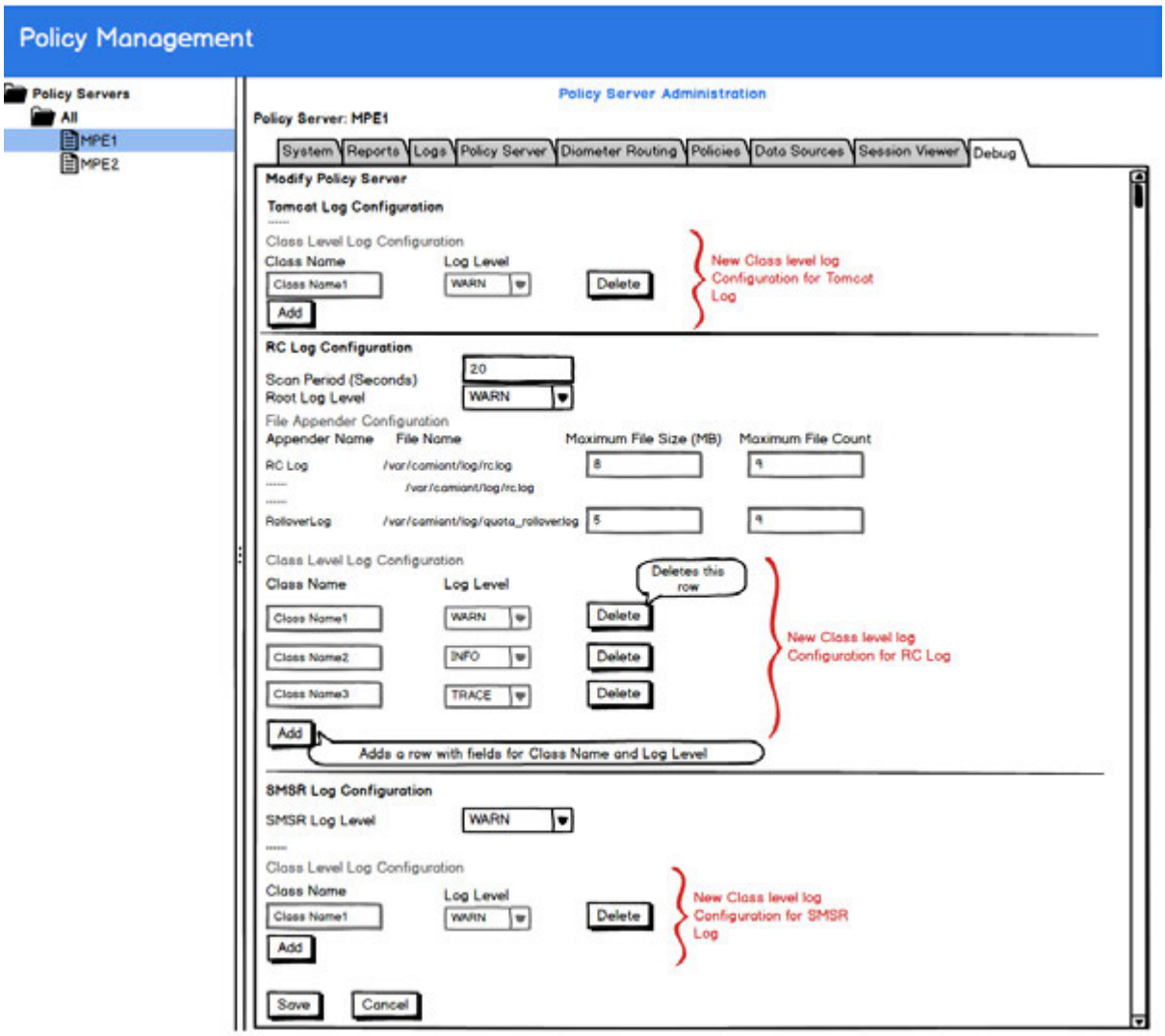
The class level log configuration shall be provided for all loggers like Tomcat log, RC log, SMSR log

For these class level log configuration, operator shall be able to specify the exact class name (for which logging is to be enabled) (as a string) & select the particular log level (from dropdown list), the same shall be set in corresponding logger file. For ex, if operator specifies class name as 'msc.rc.PolicyEngine' under RC log class level log configuration & select log level as 'Debug', following will be written in logback-rc.xml file:

```
<logger name="msc.rc.PolicyEngine" level="DEBUG" additivity="false">
   <appender-ref ref="RCLog"/>
</logger>
```

The .xml files corresponding to each logger is specified below:

Tomcat log -> /etc/camiant/logconfig/logback-tomcat.xml
RC log -> /etc/camiant/logconfig/logback-rc.xml
SMSR log -> /etc/camiant/logconfig/logback-tomcat-rc.xml




***Debug Page enhancements for MPE***

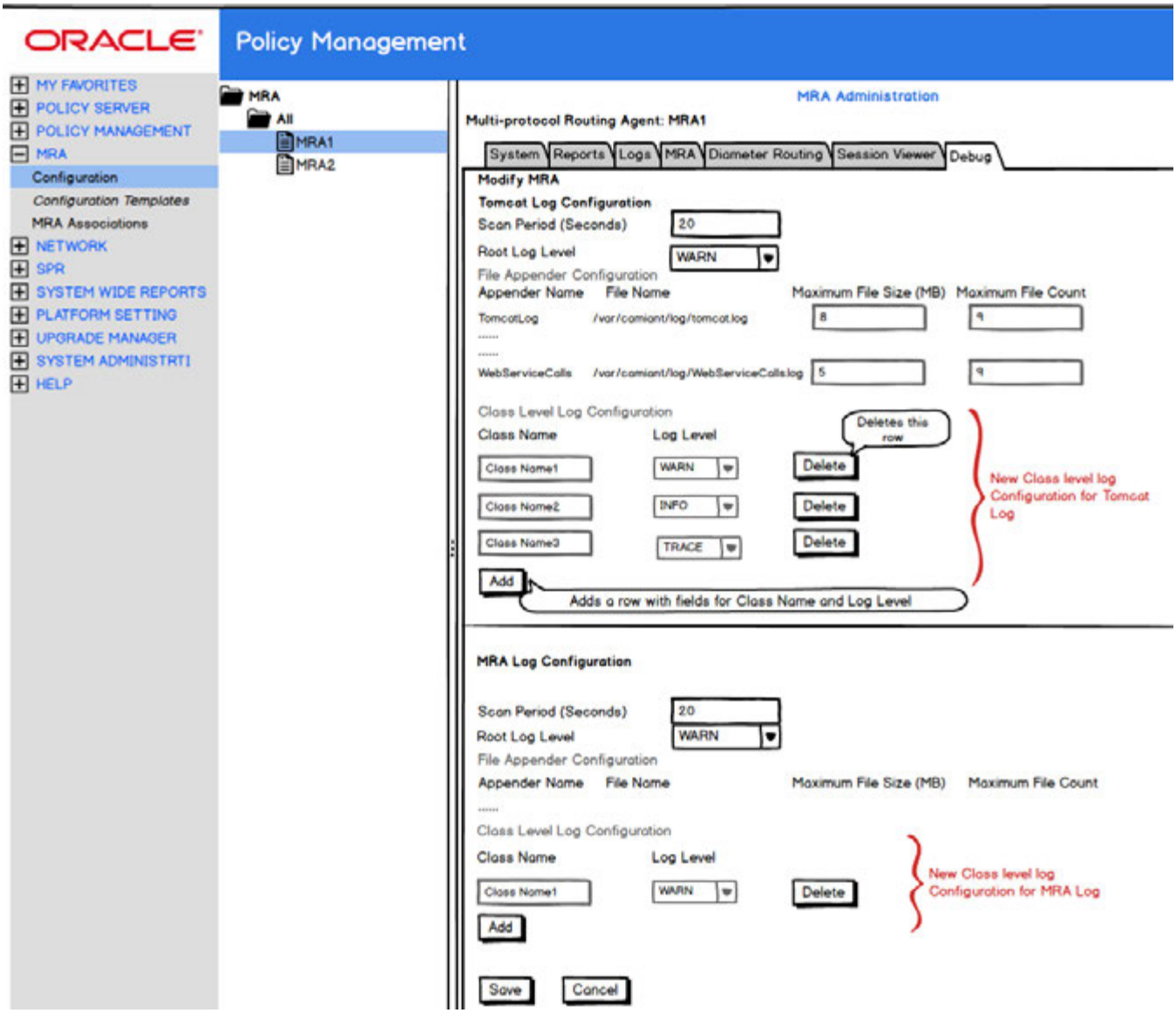
### *Enhancements to Debug page for supporting class log level - MRA*

As part of enhancement 'Enable Debug Logging via CMP', the Debug page shall be enhanced to support class log level for different components in MRA

The class level log configuration shall be provided for all loggers like Tomcat log, RC log

The .xml files corresponding to each logger is specified below:

Tomcat log -> /etc/camiant/logconfig/logback-tomcat.xml
RC log -> /etc/camiant/logconfig/logback-mra.xml




***Debug Page enhancement for MRA***

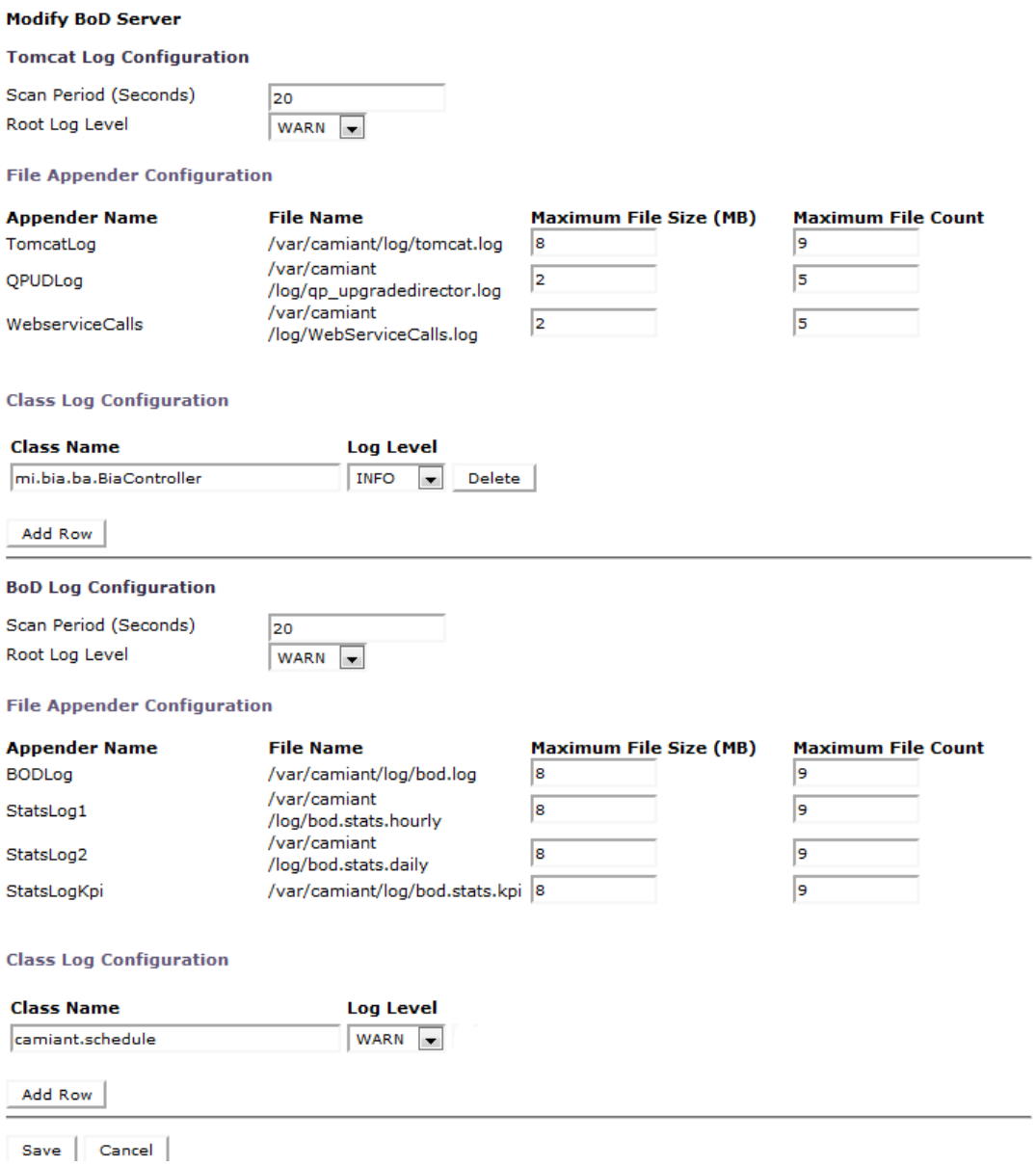
***Enhancements to Debug page for supporting class log level - BoD***

As part of enhancement 'Enable Debug Logging via CMP', the Debug page shall be enhanced to support class log level for different components in BoD

The class level log configuration shall be provided for all loggers like Tomcat log, BoD log

The .xml files corresponding to each logger is specified below:

Tomcat log -> /etc/camiant/logconfig/logback-tomcat.xml
BoD log -> /etc/camiant/logconfig/logback-bod.xml

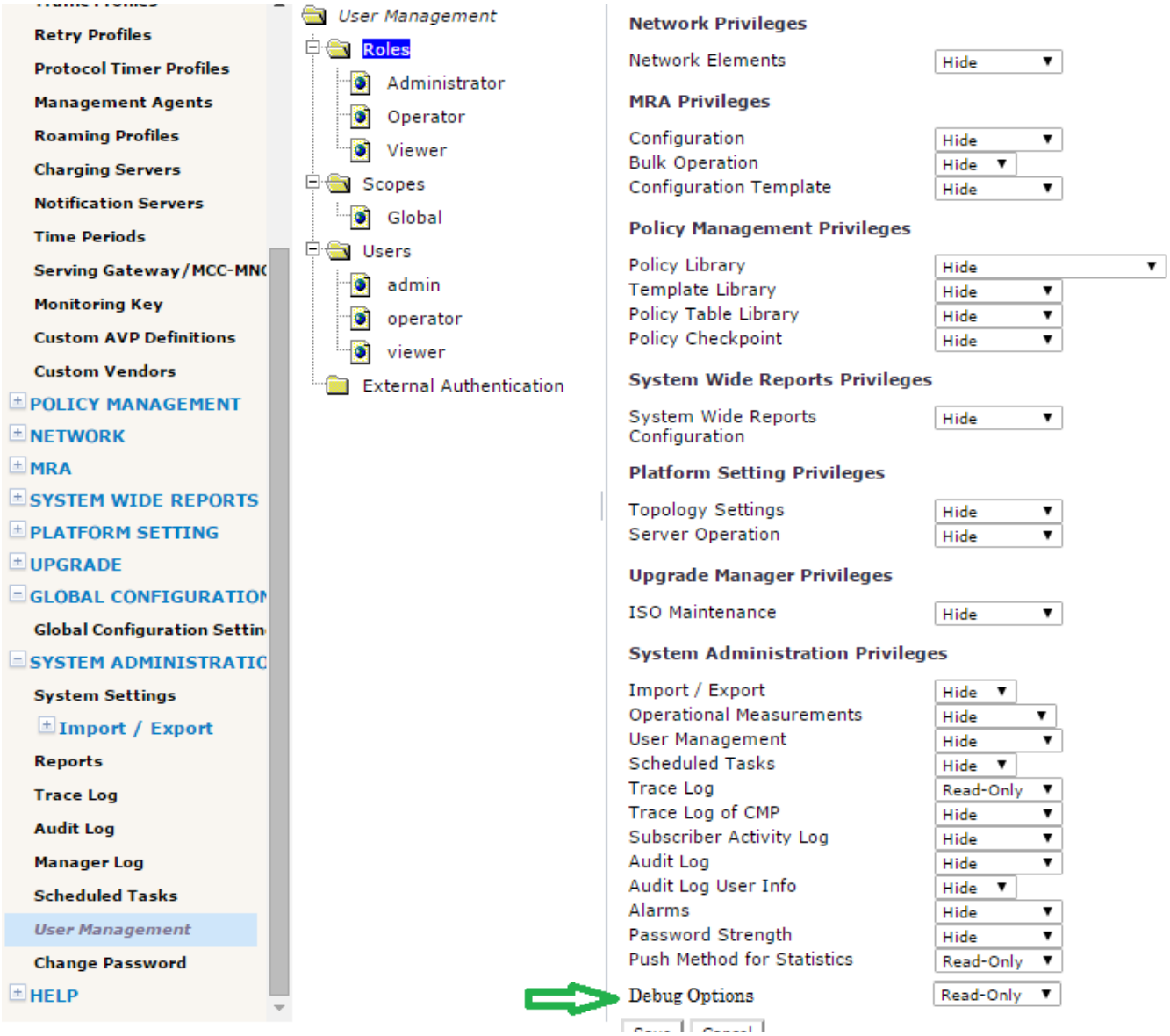



***Debug Page enhancement for BoD***

### *3.26.3 User Interface Changes*

***System Administration***

There will be a new row 'Debug Options' under User management -> Roles -> System Administration Privileges. This will have access control for debug tab: Read-Write or Read-only




***Role based authorization for Debug Page***

## 3.27 ADD SUPPORT FOR ADC ON GX ( PR# 240023 / 20271473 )

### 3.27.1 Introduction

In 3GPP TS 29.212 V12.4.0, PCRF needs to support application detection information and redirect function over the Gx interface. The PCRF may instruct the PCEF to detect application (s) by providing the Charging-Rule-Install AVP (s) with the corresponding parameters and provide the redirect instruction for a dynamic PCC rule to the PCEF enhanced with ADC (Application Detection Control). The MPE and CMP need to enhance the Gx reference point, traffic profiles, and policies to support this feature.

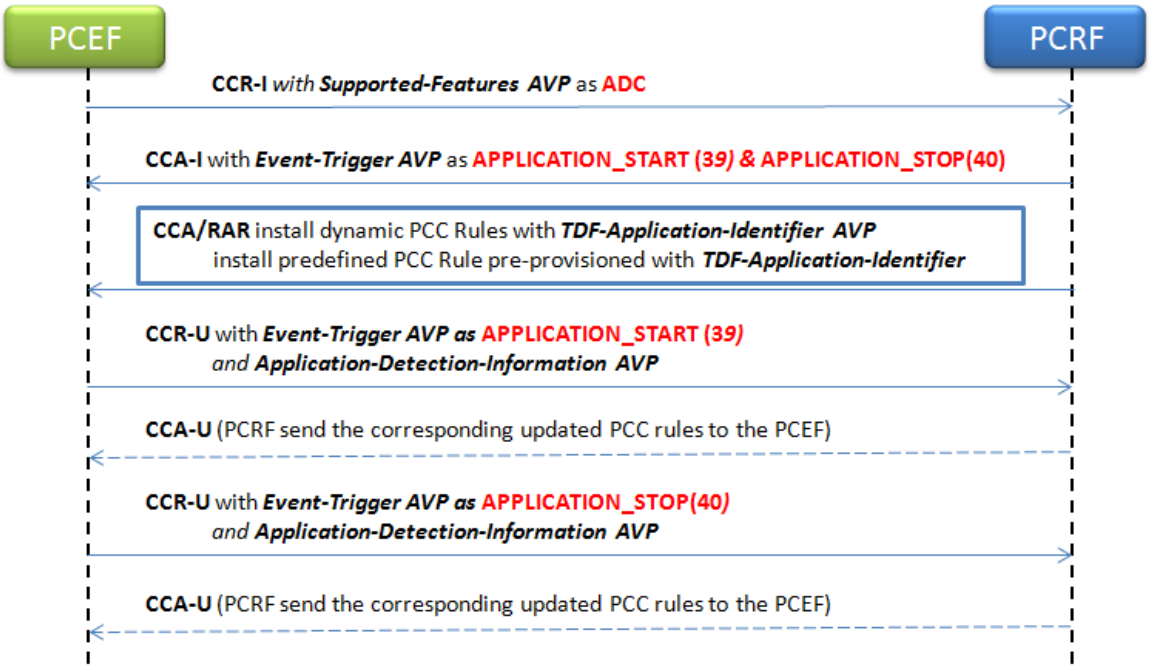
The TDF-Application-Instance-Identifier AVP and Flow-Information AVP is also supported under Application-Detection-Information AVP on the Sd interface.

**Feature Activation**

For Gx interface, this feature is only applicable if the ADC feature was advertised in Supported-Features AVP by the PCEF or the PCRF will not send TDF-Application-Identifier/ Mute-Notification / Redirect-Information AVP in Charging-Rule-Definition AVP in CCA or RAR to PCEF. If PCEF advertises ADC feature in CCR-I, PCRF shall subscribes to the APPLICATION_START/APPLICATION_STOP Event-Triggers in CCA-I.

### 3.27.2 Detailed Description

- **Gx interface:**



The PCRF shall instruct the PCEF enhanced with ADC to detect application (s) and provide redirect function by dynamic PCC rules or predefined PCC Rule/predefined PCC Rule base in CCA or RAR.

For predefined PCC Rule/ predefined PCC Rule base which pre-provisioned with corresponding ADC information, only Charging-Rule-Name/Charging-Rule-Base-Name need to be provided in Charging-Rule-Install AVP.

For dynamic PCC rule, PCRF shall provide the Charging-Rule-Install AVP (s) in dynamic PCC rules with the corresponding parameters as follows:

```
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 ]
Redirect-Information ::= < AVP Header: 1085 >
                                [ Redirect-Support ]
                                [ Redirect-Address-Type ]
                                [ Redirect-Server-Address ]
                          *[ AVP ]
```

The application to be detected is identified by the TDF-Application-Identifier AVP. If the PCRF requires to be reported about when the application start/stop is detected, it shall also subscribe to the APPLICATION_START and APPLICATION_STOP Event-Triggers. The PCRF may also mute such a notification about a specific detected application by providing Mute-Notification AVP within the PCC Rule.

The redirect instruction shall be encoded using a Redirect-Information AVP within the Charging-Rule-Definition AVP of the dynamic PCC rule.

```
Redirect-Information ::= < AVP Header: 1085 >
                              [ Redirect-Support ]
                              [ Redirect-Address-Type ]
                              [ Redirect-Server-Address ]
                         *[ AVP ]
```

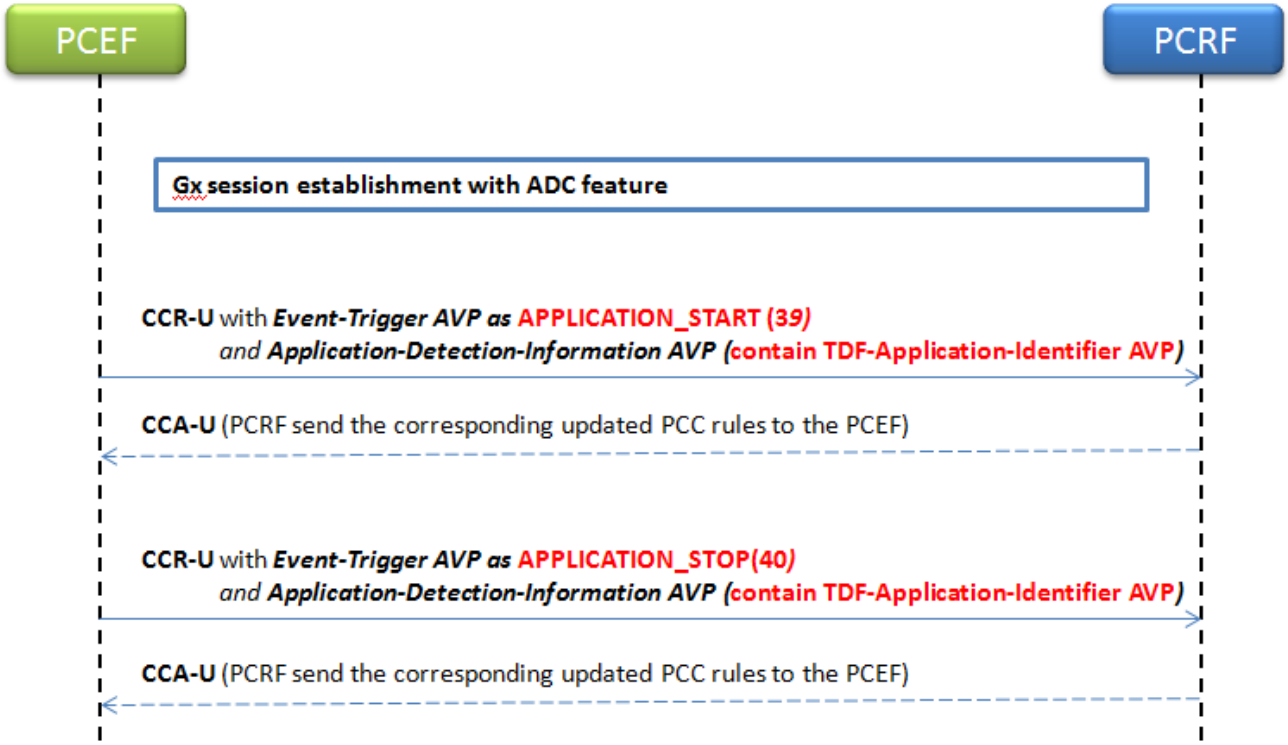
- **PCEF report the information regarding the detected application's traffic to PCRF**

When PCEF reports the information regarding the detected application's traffic to PCRF, PCRF makes policy decisions based on the information received and sends the corresponding updated PCC rules to the PCEF.

The Application-Detection-Information AVP is now supported in PCRF.

```
Application-Detection-Information ::=    < AVP Header: 1098 >
                                              { TDF-Application-Identifier }
                                              [ TDF-Application-Instance-Identifier ]
                                             *[ Flow-Information ]
                                             *[ AVP ]
```

**Use Case-1: PCEF reports for APPLICATION_START only with TDF-Application-Identifier in Application-Detection-Information**




- PCRF can install specified PCC rule/predefined PCC Rule/ predefined PCC Rule base for different TDF-Application-Identifier by policy engine in CCA-U when PCEF report for APPLICATION_START.

- PCRF can remove specified PCC rule/ predefined PCC Rule/ predefined PCC Rule base for different TDF-Application-Identifier by policy engine in CCA-U when PCEF report for APPLICATION_STOP.

For example:

**App_Start**

where the request is ***modifying an existing session***
And where the event trigger is one of ***APPLICATION_START***
And where the TDF-Application-Identifier matches one of ***TDFID01,TDFID02***
install ***pcc_rule1*** PCC rule(s) for ***session***
continue processing message

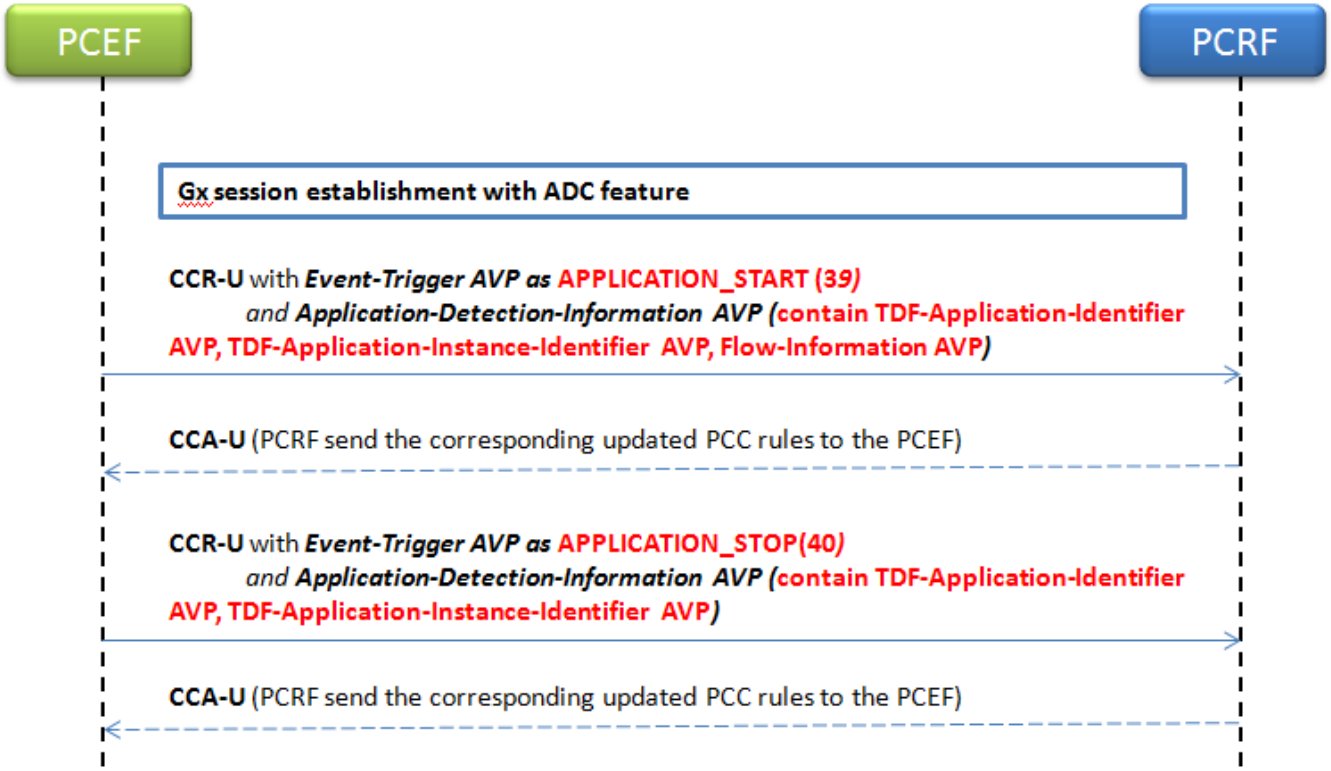
---

**App_Stop**

where the request is ***modifying an existing session***
And where the event trigger is one of ***APPLICATION_STOP***
And where the TDF-Application-Identifier matches one of ***TDFID01,TDFID02***
remove ***pcc_rule1*** PCC rule(s)
continue processing message

**Use Case-2: PCEF reports for APPLICATION_START with TDF-Application-Instance-Identifier *and* Flow-Information in Application-Detection-Information**

When the Event trigger indicates APPLICATION_START, the Flow-Information AVP for the detected application may be included under Application-Detection-Information AVP, if deducible. The TDF-Application-Instance-Identifier, which is dynamically assigned by the PCEF in order to allow correlation of APPLICATION_START and APPLICATION_STOP Event-Triggers to the specific Flow-Information AVP, if service data flow descriptions are deducible, shall also be provided when the Flow-Information AVP is included. Also, the corresponding Event-Trigger (APPLICATION_START or APPLICATION_STOP) shall be provided to PCRF. When the TDF-Application-Instance-Identifier is provided along with the APPLICATION_START, it shall also be provided along with the corresponding APPLICATION_STOP.




When PCEF reports for APPLICATION_START with TDF-Application-Identifier and TDF-Application-Instance-Identifier and Flow-Information AVP, PCRF can install specified PCC rule/ predefined PCC Rule/ predefined PCC Rule base for different reported flows by policy engine in CCA-U.

If PCEF report for APPLICATION_START, TDF-Application-Instance-Identifier AVP and Flow-Information AVPs must be included under Application-Detection-Information AVP at the same time or both not present. If only one of them present, PCRF shall generate a warning level trace log and continue with the session processing.

**New Trace Logs**

4551-Policy_Warning **scenario one for policy action**: remove default PCC/ADC rule(s) of default TDF application id(s) for APPLICATION_STOP

**Description:** If PCRF can't find associated PCC/ADC rules(s) with this TDF-Application-Identifier and TDF-Application-Instance-Identifier info, then PCRF shall generate a warning level trace log and continue with the session processing.

| | | | |
|---|---|---|---|
| CST | 4566 | Info | Policy Action Trace: remove Pcc rules when App-Stop |
| CST | 4551 | Warning | Policy Trace remove Pcc rules when App-Stop: Could not execute 'remove PCC rule(s) of TDF application id(s) for APPLICATION_STOP' because there is no TDF-Application-Instance-Ider |
| CST | 1412 | Info | Diameter:Sent CCA [317643130:3219489681 / ggsn;1407402506;0] DIAMETER_SUCCESS (2001) to ggsn(10.60.33.17:48484) in 21 ms |

**Log: Policy Trace policy name:** Could not execute 'remove PCC rule(s) of TDF application id(s) for APPLICATION_STOP' because there is no TDF-Application-Instance-Identifier in Application-Detection-Information AVP

4551-Policy_WARNing **scenario two for policy action**: remove default PCC/ADC rule(s) of default TDF application id(s) for APPLICATION_STOP

**Description:** If no TDF-Application-Instance-Identifier is in the Application-Detection-Information AVP, but some installed PCC rule(s) contain binding info for the same TDF-Application-Identifier, then PCRF shall generate a warning level trace log and continue with the session processing.

```
CST 4566 Info    Policy Action Trace: remove Pcc rules when App-Stop
CST 4551 Warning Policy Trace remove Pcc rules when App-Stop: Could not execute 'remove PCC rule(s) of TDF application id(s) for APPLICATION_STOP' because can not find related PCC rule to remove
CST 1412 Info    Diameter:Sent CCA [317643129:3219489680 / ggsn;1407402506;0] DIAMETER_SUCCESS (2001) to ggsn(10.60.33.17:48484) in 17 ms
```

**Log: Policy Trace policy name:** Could not execute 'remove PCC/ADC rule(s) of TDF application id(s) for APPLICATION_STOP' because can not find related PCC/ADC rule to remove

**Policy Changes**

Policy wizard changes of the type “request conditions”.

| Policy Condition Group | Policy Condition or Action | Description |
|---|---|---|
| **“request” conditions** | **where the flow is *an application flow*** | **Enhance** the existing policy condition by adding a new flow type – **an application detection flow** |
| **“request” conditions** | **where the QoS parameters in the flow are equal to *specified value*** | **Enhance** the existing policy condition, so that it can support:<br>➢ *Diameter App Detection TDF-Application-Identifier*<br>➢ *Diameter App Detection Flow-Description*<br>➢ *Diameter App Detection Flow-Direction* |
| **“request” conditions** | **where the *select type* is contained in Match List(s) *select list(s)*** | **Enhance** the existing policy condition, add new select type: **TDFApplicationIdentifier** |
| **“request” conditions** | **where the *select type* is not contained in Match List(s) *select list(s)*** | **Enhance** the existing policy condition, add new select type: **TDFApplicationIdentifier** |

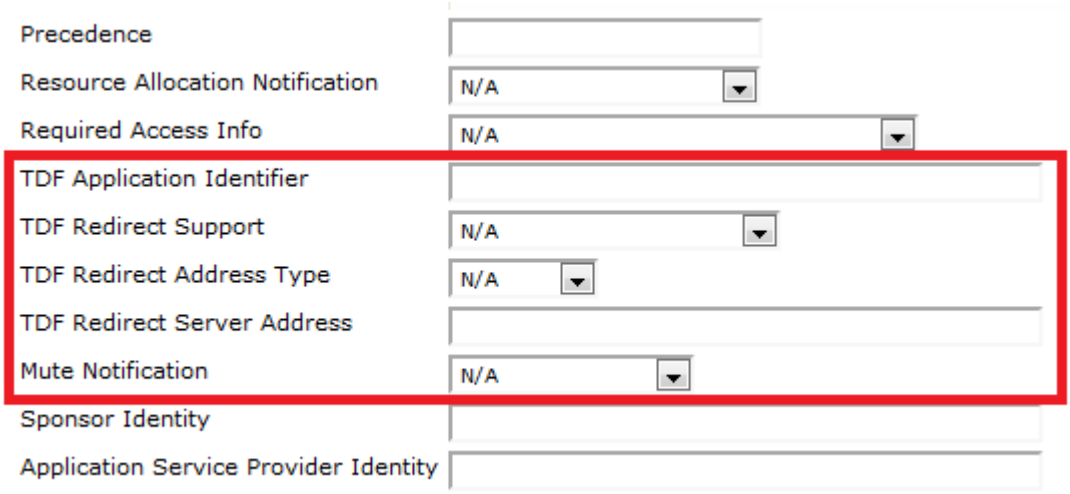
Policy wizard changes of the type “optional actions”.

| Policy Condition Group | Policy Condition or Action | Description |
|---|---|---|
| "optional" actions<br><br>"optional" actions<br><br>"optional" actions | add the APP Detection Flow *select scope* to *specified* PCC/ADC rule(s)<br><br>remove *default* PCC/ADC rule(s) of *default* TDF application id(s) for APPLICATION_STOP<br><br>apply *specified profile(s)* to request | It can bind TDF-Application-Identifier and TDF-Application-Instance-Identifier info of current application detection flow to PCC/ADC rule( s)<br>It can remove associated PCC/ADC rule(s) while PCEF/TDF is reporting for APLICATION_STOP<br><br>**Enhance** the existing policy action, so that it can change "TDF Application Identifier/TDF Redirect Support/TDF Redirect Address Type/TDF Redirect Server Address/Mute Notification" information in dynamic PCC rule |
| "optional" actions | apply *specified profile(s)* to all flows in the request | **Enhance** the existing policy action, so that it can change "TDF Application Identifier/TDF Redirect Support/TDF Redirect Address Type/TDF Redirect Server Address/Mute Notification" information in dynamic PCC rule |
| "optional" actions | apply *specified profile(s)* to flow(s) whose media type matches one of *specified type(s)* | **Enhance** the existing policy action, so that it can change "TDF Application Identifier/TDF Redirect Support/TDF Redirect Address Type/TDF Redirect Server Address/Mute Notification" information in dynamic PCC |
| "optional" actions | apply *specified profile(s)* to selected *specified type(s)* flows in the request | **Enhance** the existed policy action, so that it can change "TDF Application Identifier/TDF Redirect Support/TDF Redirect Address Type/TDF Redirect Server Address/Mute Notification" information in dynamic PCC rule |

### *3.27.3 User Interface Changes*

**PCC profile enhancement**

Operator can define PCC Profile on "Traffic Profiles" on CMP. "TDF Application Identifier/TDF Redirect Support/TDF Redirect Address Type/TDF Redirect Server Address/Mute Notification" are added for this feature.



| Display on Traffic Profiles | AVP in Charging-Rule-Definition AVP |
|---|---|
| TDF Application Identifier | TDF-Application-Identifier |
| Mute Notification | Mute-Notification |
| TDF Redirect Support | Redirect-Support in Redirect-Information AVP |
| TDF Redirect Address Type | Redirect-Address-Type in Redirect-Information AVP |
| TDF Redirect Server Address | Redirect-Server-Address in Redirect-Information AVP |

## 3.28 [RX COUNTER] ADD SEVERAL RAW COUNTERS FOR RX RELATED MESSAGES SUPPORT FOR ADC ON GX ( PR# 20271492 )

### 3.28.1 Introduction

Currently, on the PCRF, there are existing counters "AAASendSuccessCount / AAASendFailureCount" which represent the successful/failure AAA which is sent from PCRF to AF, responding to an AAR. PCRF will now add finer grain counters to divide the AAA to AAA initial or AAA update ones.

### 3.28.2 Detailed Description

Four new counters will be added as "AAAInitialSendSuccessCount / AAAInitialSendFailureCount", "AAAModificationSendSuccessCount / AAAModificationSendFailureCount" which are respectively for AAA initial response and update response. These counters are only provided on MPE, while not provided on MRA in the current stage. The reason of not supporting these counters on MRA is that the initial or modification of AF session is decided by the existence of AF session in MPE.

Also, there are existing counters "ASRSendCount / ASRTimeoutCount" which represent the send/timeout ASR which is sent from PCRF to AF. There is a need to summarize the number of ASR triggered by handover. The handover scenario is that the ASR included with Abort-Cause as PS_TO_CS_HANDOVER[6]. Then it will need to add the corresponding counters as "ASRHOSendCount / ASRHOTimeoutCount". These counters can be provided both on MPE and MRA.

Prior to 12.2, the PCRF tracks counters for "AAASendSuccessCount /AAASendFailureCount". This feature adds finer grain counters to distinguish between "AAA initial" and "AAA update" Rx interface messages.

**Prior to 12.2**

| Counter Name |
|---|
| AAA success messages received / sent |
| AAA failure messages received / sent |

**Introduced in 12.2**

| Counter Name |
|---|
| AAA initial success messages received / sent |
| AAA initial failure messages received / sent |
| AAA modify success messages received / sent |
| AAA modify failure messages received / sent |

**NOTE:** These counters are only provided on MPE

Prior to 12.2 , the PCRF tracks counters on the Rx Interface for “ASRSendCount & ASRTimeoutCount”. This feature also adds counters to summarize the number of ASR messages triggered by a handover. The handover scenario is when the ASR includes the Abort-Cause as PS_TO_CS_HANDOVER[6].

**Introduced in 12.2**

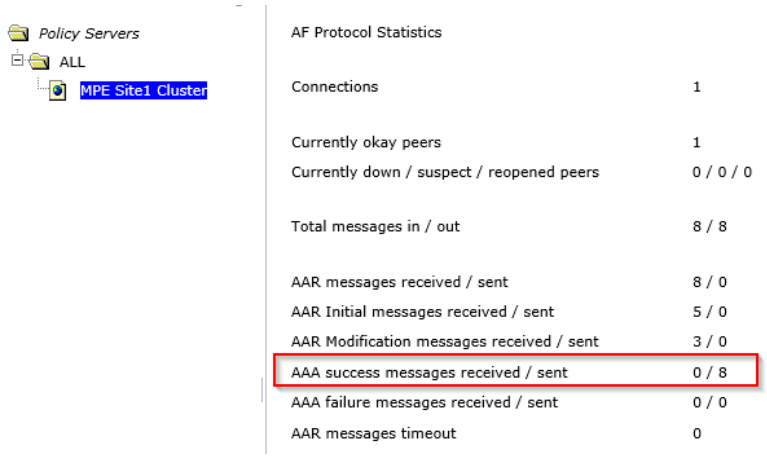
| Counter Name |
| --- |
| ASR HO messages received / sent |
| ASR HO timeout |

### *3.28.3 User Interface Changes*

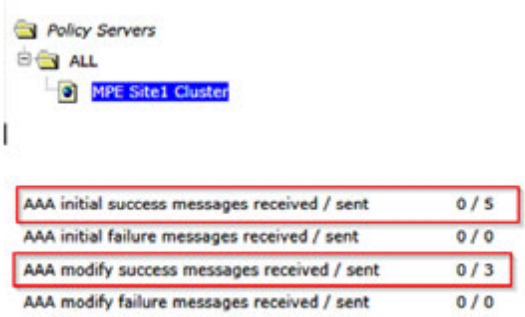
Open AF Protocol Statistics on the reports tab of the MPE and confirm the new counters are incrementing that distinguish between AAA “initial” and “update” (or modify) received/sent messages. These messages will equal the total of AAA messages received/sent. In previous releases this level of granularity did not exist.

**For example:**

Total AAA success messages sent




Total AAA success initial and modify (update) messages sent


Policy Servers
ALL
MPE Site1 Cluster
AAA initial success messages received / sent 0 / 5
AAA initial failure messages received / sent 0 / 0
AAA modify success messages received / sent 0 / 3
AAA modify failure messages received / sent 0 / 0

## 3.29 ENHANCED PRIORITY FOR EMPS BASED WIRELESS PRIORITY SERVICES ( PR# 22121678 )

### 3.29.1 Introduction

This feature enhancement allows Policy Management to:

- Recognize that an incoming Rx request is for an emergency service (e.g., 911 in the US)
- Notify the PGW (and any intermediary nodes) that this is a high priority message by setting and sending a new optional AVP called DRMP (Diameter Routing Message Priority) in a RAR
- Ensure that messages associated with priority calls are not shed on either the MPE or the MRA unless absolutely necessary, with new load shedding rules
- When all priority sessions are terminated, instruct the PGW to revert to the behaviors defined before the priority session as established (current functionality)

#### Feature Activation

After fresh install or upgrade, the new AVP is defined in Diameter dictionary. But the AVP won't be added to Diameter messages by default unless a Policy action described in section is triggered.

### 3.29.2 Detailed Description

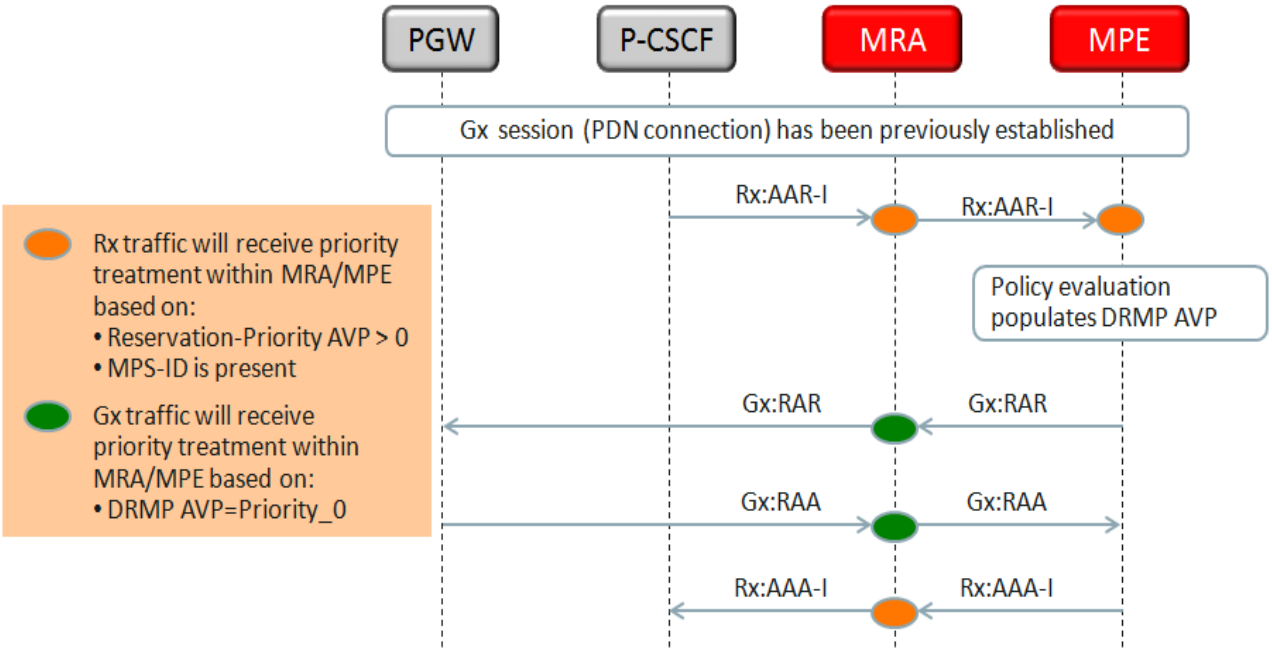
The feature "Enhanced Priority for eMPS Based Wireless Priority Services" enables Oracle PCRF Release 12.2.0.0 products to support Multimedia Priority Support as defined in 3GPP 29.212 and the Diameter message priority mechanism defined in Annex J of 3GPP TS 29.213.

To be specific, PCRF performs the following actions when it receives Rx: AAR requests whose service information including an MPS session indication and the service priority level from P-CSCF:

Grants highest priority to the messages;

May include a DRMP AVP indicating a priority level in the requests to the PCEF and also grants highest priority to them.

The message flow is summarized below:




**Policy Changes**

New policy actions are defined to set DRMP AVP to specified value. The action is exposed to user when "Diameter 3GPP" mode is enabled.

User can use the existing policy conditions combining with the new policy action to add the DRMP AVP and assign a priority level to messages.

| Policy Condition Group | Policy Condition or Action | Description |
|---|---|---|
| **NA** | **Optional actions: set DRMP AVP to DRMP Level in Re-Authorized Request** | This action is exposed to user when mode "Diameter 3GPP" is enabled.<br>It is used to set the DRMP AVP to specified priority level in Gx: RAR messages. Only one value can be specified.<br>The **DRMP Level** can be one of:<br>• *PRIORITY_0 value 0*<br>• *PRIORITY_1 value 1*<br>• *PRIORITY_2 value 2*<br>• *PRIORITY_3 value 3*<br>• *PRIORITY_4 value 4*<br>• *PRIORITY_5 value 5*<br>• *PRIORITY_6 value 6*<br>• *PRIORITY_7 value 7*<br>• *PRIORITY_8 value 8*<br>• *PRIORITY_9 value 9*<br>• *PRIORITY_10 value 10*<br>• *PRIORITY_11 value 11*<br>• *PRIORITY_12 value 12*<br>• *PRIORITY_13 value 13* |

| | | |
|---|---|---|
| | | • *PRIORITY_14 value 14*<br>• *PRIORITY_15 value 15* |

## Configuration Changes

A group of new rules are added into default load shedding configuration, to proceed MPS messages when there is congestion

- For an upgrade of Policy Management from previous releases, the new load shedding rules need to be added manually.
- For a fresh install, no manual operations are needed because these rules are pre-defined automatically on CMP.

**MPE**

| Name | level | App | Message | avpName | initial | upgrade | terminate | apnName | apnValue | drmpName | drmpValue | mpsIdAndRpName | mpsIdAndRpExist | Action |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DefaultRule1 | 1 | Gx | CCR | CC-Request-Type | 1 | -999 | -999 | Called-Station-Id | | DRMP | | | false | DIAMETER_TOO_BUSY |
| DefaultRule14 | 1 | Gx | CCR | CC-Request-Type | 1 | -999 | -999 | Called-Station-Id | | DRMP | 0 | | false | ACCEPT |
| DefaultRule4 | 1 | Gxx | CCR | CC-Request-Type | 1 | -999 | -999 | Called-Station-Id | | | | | false | DIAMETER_TOO_BUSY |

| Name | level | App | Message | avpName | initial | upgrade | terminate | apnName | apnValue | drmpName | drmpValue | mpsIdAndRpName | mpsIdAndRpExist | Action |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DefaultRule17 | 2 | Rx | AAR | Rx-Request-Type | 0 | -999 | -999 | Called-Station-Id | | | | MPS-Identifier_Reservation-Priority | true | ACCEPT |
| DefaultRule2 | 2 | Gx | CCR | CC-Request-Type | 1 | -999 | -999 | Called-Station-Id | | DRMP | | | false | DIAMETER_TOO_BUSY |
| DefaultRule15 | 2 | Gx | CCR | CC-Request-Type | 1 | -999 | -999 | Called-Station-Id | | DRMP | 0 | | false | ACCEPT |
| DefaultRule5 | 2 | Gxx | CCR | CC-Request-Type | 1 | -999 | -999 | Called-Station-Id | | | | | false | DIAMETER_TOO_BUSY |
| DefaultRule7 | 2 | Rx | AAR | Rx-Request-Type | 0 | -999 | -999 | Called-Station-Id | | | | MPS-Identifier_Reservation-Priority | false | DIAMETER_TOO_BUSY |

| Name | level | App | Message | avpName | initial | upgrade | terminate | apnName | apnValue | drmpName | drmpValue | mpsIdAndRpName | mpsIdAndRpExist | Action |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DefaultRule3 | 3 | Gx | CCR | CC-Request-Type | 1 | 2 | -999 | Called-Station-Id | | DRMP | | | false | DIAMETER_TOO_BUSY |
| DefaultRule16 | 3 | Gx | CCR | CC-Request-Type | 1 | 2 | -999 | Called-Station-Id | | DRMP | 0 | | false | ACCEPT |
| DefaultRule6 | 3 | Gxx | CCR | CC-Request-Type | 1 | 2 | -999 | Called-Station-Id | | | | | false | DIAMETER_TOO_BUSY |
| DefaultRule8 | 3 | Rx | AAR | Rx-Request-Type | 0 | 1 | -999 | Called-Station-Id | | | | MPS-Identifier_Reservation-Priority | false | DIAMETER_TOO_BUSY |
| DefaultRule18 | 3 | Rx | AAR | Rx-Request-Type | 0 | 1 | -999 | Called-Station-Id | | | | MPS-Identifier_Reservation-Priority | true | ACCEPT |
| DefaultRule9 | 3 | Sh | PNR | | -999 | -999 | -999 | Called-Station-Id | | | | | false | DIAMETER_TOO_BUSY |
| DefaultRule10 | 3 | Sy | SNR | | -999 | -999 | -999 | Called-Station-Id | | | | | false | DIAMETER_TOO_BUSY |

| Name | level | App | Message | avpName | initial | upgrade | terminate | apnName | apnValue | drmpName | drmpValue | mpsIdAndRpName | mpsIdAndRpExist | Action |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DefaultRule11 | 4 | Drma | LNR | | -999 | -999 | -999 | | | | | | false | ACCEPT |
| DefaultRule12 | 4 | Drma | LSR | | -999 | -999 | -999 | | | | | | false | ACCEPT |
| DefaultRule13 | 4 | Drma | RUR | | -999 | -999 | -999 | | | | | | false | ACCEPT |

**MRA**

| Name | level | App | Message | avpName | initial | upgrade | terminate | apnName | apnValue | drmpName | drmpValue | mpsIdAndRpName | mpsIdAndRpExist | Action |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DefaultRule1 | 1 | Gx | CCR | CC-Request-Type | 1 | -999 | -999 | Called-Station-Id | | DRMP | | | false | DIAMETER_TOO_BUSY |
| DefaultRule2 | 1 | Gxx | CCR | CC-Request-Type | 1 | -999 | -999 | Called-Station-Id | | DRMP | | | false | DIAMETER_TOO_BUSY |
| DefaultRule6 | 1 | Gx | CCR | CC-Request-Type | 1 | -999 | -999 | Called-Station-Id | | DRMP | 0 | | false | ACCEPT |

| Name | level | App | Message | avpName | initial | upgrade | terminate | apnName | apnValue | drmpName | drmpValue | mpsIdAndRpName | mpsIdAndRpExist | Action |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DefaultRule2 | 2 | Gx | CCR | CC-Request-Type | 1 | -999 | -999 | Called-Station-Id | | DRMP | | | false | DIAMETER_UNABLE_TO_COMPLY |
| DefaultRule5 | 2 | Gxx | CCR | CC-Request-Type | 1 | -999 | -999 | Called-Station-Id | | | | | false | DIAMETER_UNABLE_TO_COMPLY |
| DefaultRule7 | 2 | Rx | AAR | Rx-Request-Type | 0 | -999 | -999 | Called-Station-Id | | | | MPS-Identifier_Reservation-Priority | false | DIAMETER_UNABLE_TO_COMPLY |

| Name | level | App | Message | avpName | initial | upgrade | terminate | apnName | apnValue | drmpName | drmpValue | mpsIdAndRpName | mpsIdAndRpExist | Action |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DefaultRule3 | 3 | Gx | CCR | CC-Request-Type | 1 | 2 | -999 | Called-Station-Id | | DRMP | | | false | DIAMETER_UNABLE_TO_COMPLY |
| DefaultRule6 | 3 | Gxx | CCR | CC-Request-Type | 1 | 2 | -999 | Called-Station-Id | | | | | false | DIAMETER_UNABLE_TO_COMPLY |
| DefaultRule8 | 3 | Rx | AAR | Rx-Request-Type | 1 | 2 | -999 | Called-Station-Id | | | | MPS-Identifier_Reservation-Priority | false | DIAMETER_UNABLE_TO_COMPLY |
| DefaultRule9 | 3 | Sh | PNR | | -999 | -999 | -999 | Called-Station-Id | | | | | false | DIAMETER_UNABLE_TO_COMPLY |
| DefaultRule10 | 3 | Sy | SNR | | -999 | -999 | -999 | Called-Station-Id | | | | | false | DIAMETER_UNABLE_TO_COMPLY |

| Name | level | App | Message | avpName | initial | upgrade | terminate | apnName | apnValue | drmpName | drmpValue | mpsIdAndRpName | mpsIdAndRpExist | Action |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DefaultRule11 | 4 | Drma | LNR | | -999 | -999 | -999 | | | | | | false | ACCEPT |
| DefaultRule12 | 4 | Drma | LSR | | -999 | -999 | -999 | | | | | | false | ACCEPT |
| DefaultRule13 | 4 | Drma | RUR | | -999 | -999 | -999 | | | | | | false | ACCEPT |

**Performance Impacts**

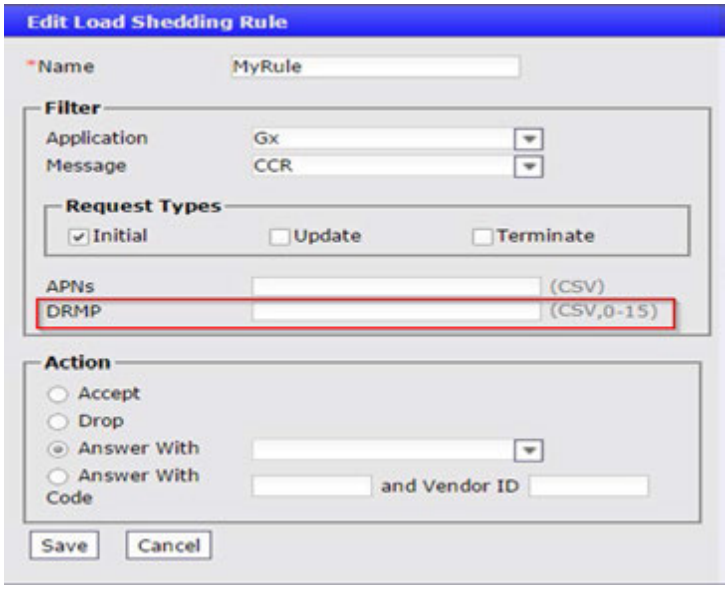
The new default group of load shedding rules will allow more messages to be process in MPE and MRA, when system is over loaded. This behavior will cause system more quickly into higher level of busy state.

### *3.29.3 User Interface Changes*

The configuration changes are in Diameter 3GPP mode only.

In MPE and MRA Load Shedding Rule edit page, when Application is Gx and Message is CCR, add one parameter: DRMP.

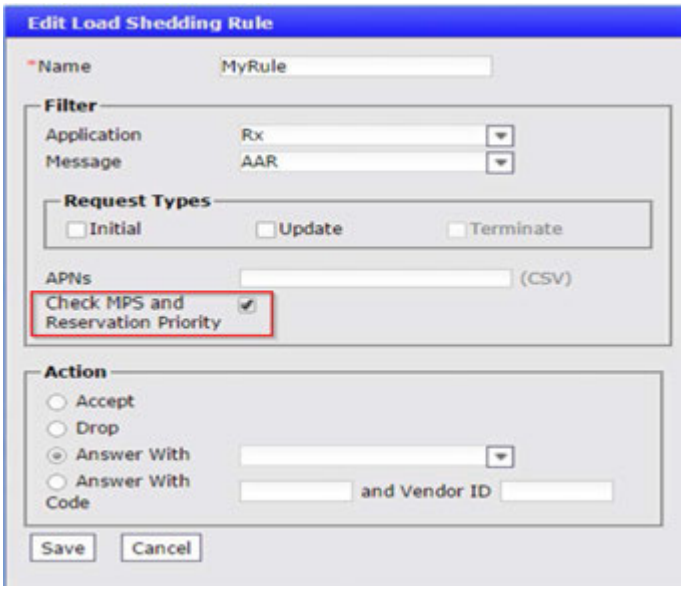
**Load Shedding Rule Edit Page: Gx CCR**




**Parameter:**
DRMP: value from 0 to 15, if there is more than one values, use comma separated values. Such as: 1,2,3. The parameter is used to check the DRMP AVP value in messages.

In MPE and MRA Load Shedding Rule edit page, when Application is Rx and Message is AAR add one parameter: Check MPS and Reservation Priority.

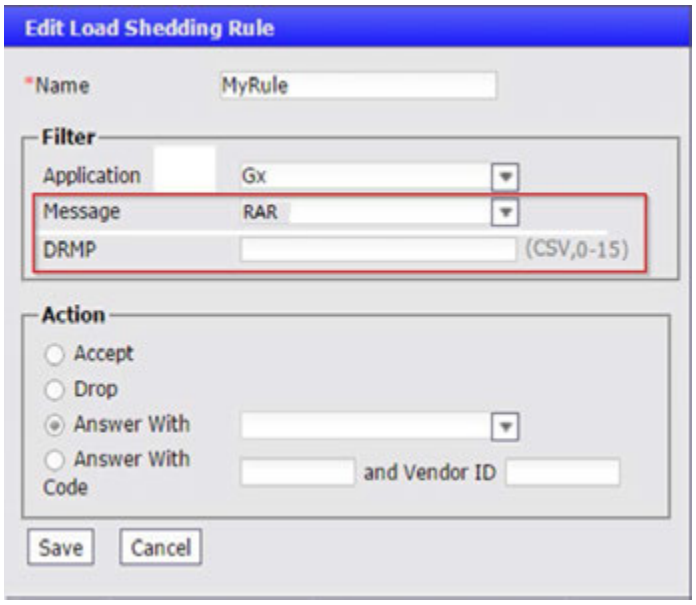
**Load Shedding Rule Edit Page: Rx AAR**




**Parameter:**
Check MPS and Reservation Priority: Check the existence of AVPs: MPS-Identifier and Reservation-Priority or not.

In MRA Load Shedding Rule edit page, when Application is Gx, RAR message type is added. And parameter [DRMP] is also added.

**Load Shedding Rule Edit Page: Gx RAR**



**Parameter:**
DRMP: value from 0 to 15, if there is more than one value, use comma separated values such as: 1,2,3.
The parameter is used to check the DRMP AVP value in messages.

## 3.30 SELECTIVE TRIGGERING OF POLICY EVALUATION ON STR AND CCR-T (PR# 20632502)

### 3.30.1 Introduction

This feature allows the operator to select which terminate messages (Rx:STR and/or Gx:CCR-T) will trigger policy evaluation on their reception. Currently the selection applies to both Rx:STR and Gx:CCR-T.

### 3.30.2 Detailed Description

Two configuration parameters control the behavior of the feature:

- Existing parameter 'DIAMETER.PolicyExecutionOnSessionTermination'. 'True' means that **all** termination messages trigger policy evaluation; 'false' means only the applications listed in the next parameter will trigger policy evaluation.
- New parameter 'DIAMETER.AppsToEvaluateOnTermination'. Only the applications listed here ('Rx' / 'Gx' / 'Rx,Gx') will trigger policy evaluation.

### 3.30.3 User Interface Changes

POLICY SERVER > Configuration > [MPE] > Policy Server > Advanced

Expert Settings

| | Category | Configuration Key | Type | Value | Default Value |
|---|---|---|---|---|---|
| L | Diameter | DIAMETER.AppsToEvaluateOnTermination | String | **Rx** | *Undefined* |

Service Overrides

| | Category | Configuration Key | Type | Value | Default Value |
|---|---|---|---|---|---|
| L | DIAMETER | DIAMETER.PolicyExecutionOnSessionTermination | boolean | **false** | true |

The settings in the example above mean that not all the termination messages will trigger policy evaluation and that only Rx:STR will.

## 3.31 SETTING GX PARAMETERS VIA POLICY ACTION BASED ON RX REQUEST (PR# 20632554)

### 3.31.1 Introduction

The feature "Enable Setting Gx Session-Level Parameters on Rx Request" allows Gx session-level parameters to be set during policy execution of an Rx:AAR message.

This allows the AAR to maintain its data and be processed, while simultaneously allowing for Gx parameters to be set without impact on the AAR data.

### 3.31.2 Detailed Description

The Gx parameters will be set via the policy action:

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

That is, a policy can be written containing the above action and, upon reception of an Rx:AAR, the Gx:RAR message will be sent back with the required Gx session-level parameters set as per the policy action.

### 3.31.3 User Interface Changes

The following policy example will be executed upon reception of an Rx:AAR and the indicated parameters will be sent in a Gx:RAR.

**Policy Description**

where the flow is ***an application flow***
Advanced: set values for QoS and Charging parameters to

| | |
|---|---|
| ***Diameter APN-Aggregate-Max-Bitrate-DL*** | ***512000*** |
| ***Diameter APN-Aggregate-Max-Bitrate-UL*** | ***128000*** |

continue processing message

## 3.32 VIRTUAL POLICY TABLES (PR# 19482300)

### 3.32.1 Introduction

Virtual policy tables are representations of existing policy tables with no data of their own that can be used to test table changes without affecting existing tables and policies.

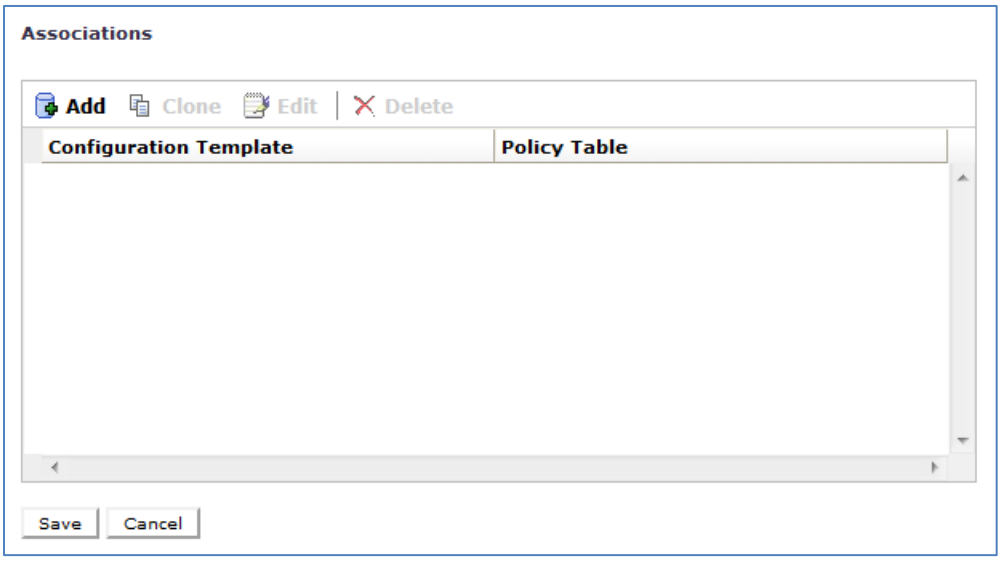
### 3.32.2 Detailed Description

Policies that use virtual policy tables can be made to point to different tables with different values with no changes to the policies themselves.

### 3.32.3 User Interface Changes

Virtual policy tables are created at POLICY MANAGEMENT > Policy Table Library > Virtual Policy Tables


In the same window while creating a virtual policy table, the virtual policy table can be associated with one or several configuration templates and different policy tables:



## 3.33 SUPPORT FOR CONFIGURATION TEMPLATES FOR CABLE (PR# 19646305)

### 3.33.1 Introduction

A configuration template is an object that contains configuration information common to two or more MPEs.

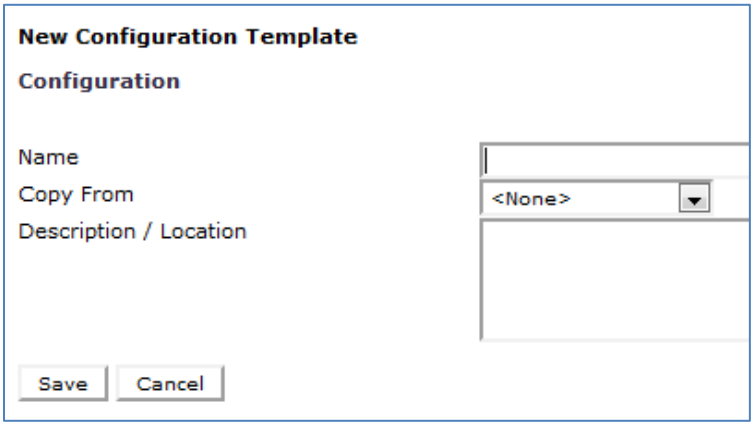
### 3.33.2 Detailed Description

They can be created and configured to include different kinds of parameters that apply to several MPEs such as:

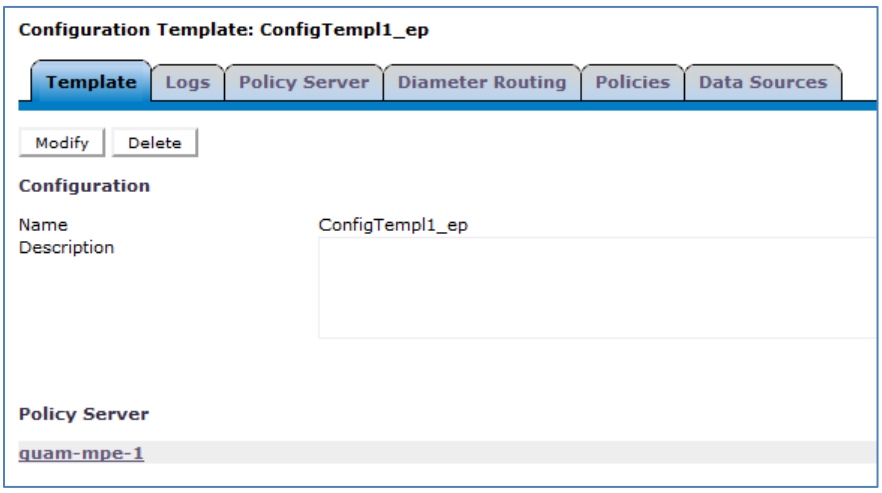
- Logging level
- Policy server settings
- Event messaging
- Routing
- Diameter AF configuration
- Load-shedding rules

### 3.33.3 User Interface Changes

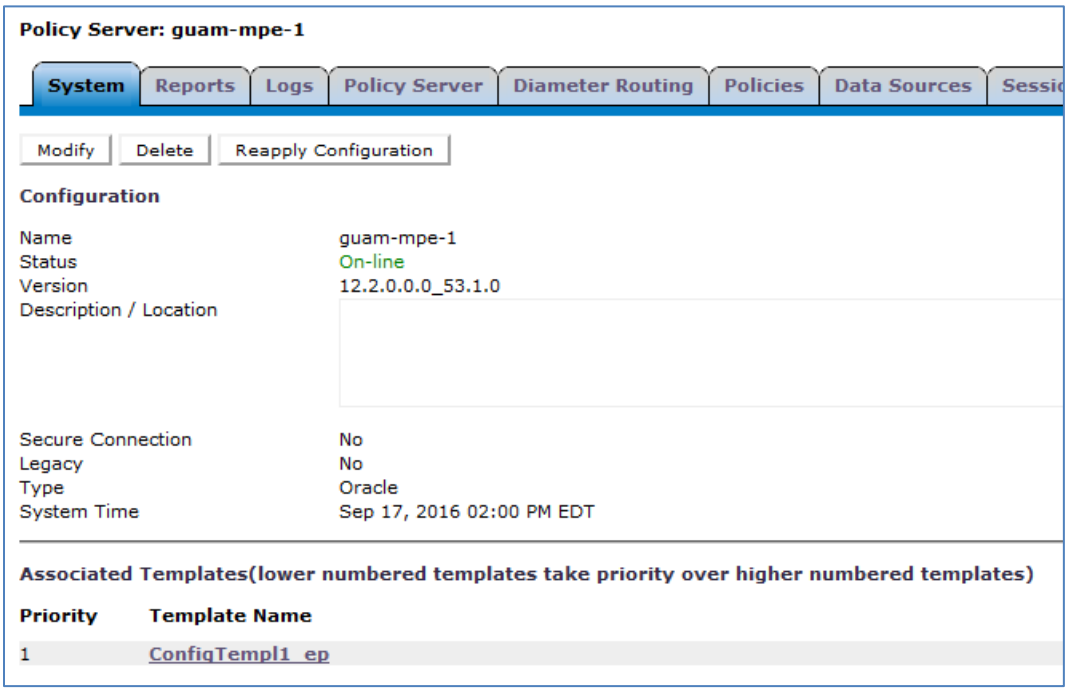
They are created at POLICY SERVER > Configuration Template



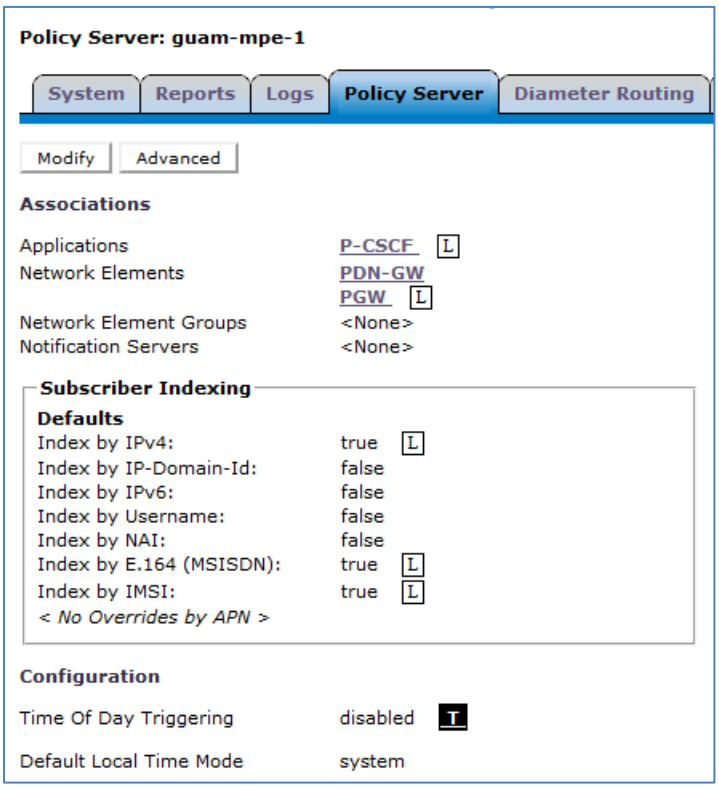
And once created they can be configured with the desired configuration information and associated with an MPE:




Once associated they appear under the corresponding MPE:



And indications are added whenever the information locally configured in the MPE differs from that in the template:




In the example above “L” indicates Local information, i.e., not set by the template and “T” indicates Template information, i.e., information that has overridden the original local settings.

## 3.34 SIG-C ADDRESS SUPPORT (PR# 238974)

### 3.34.1 Introduction

This feature introduces support for a third signaling interface, SIG-C, in addition to SIG-A and SIG-B for both MPEs and MRAs.

### 3.34.2 Detailed Description

SIG-C can be used just like SIG-A/SIG-B and has the same capabilities as those interfaces.

SIG-C support can be observed:

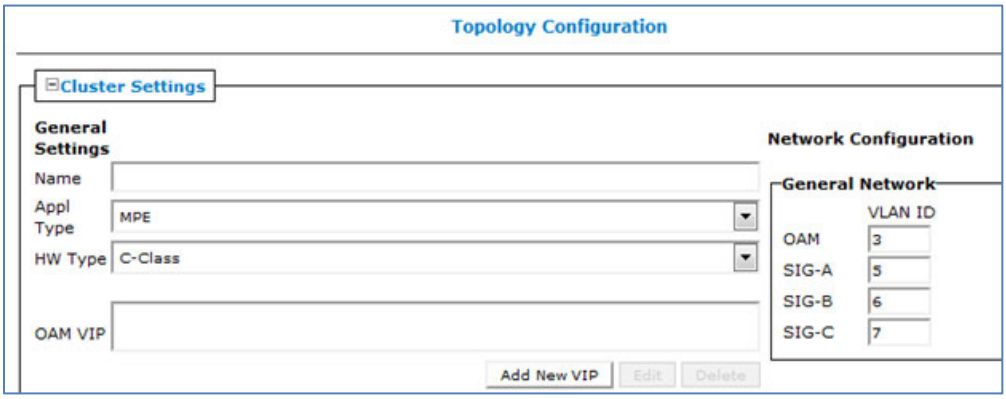
- During platform initial configuration
- During cluster/server configuration in the CMP GUI
- Through the use of the two configuration keys that filter the availability of SIG-A/SIG-B/SIG-C for SCTP in both MPEs and MRAs. The following configuration keys determine which signaling interfaces are allowed to be used with SCTP:
    - For MPEs: *DIAMETER.Sctp.SIGDeviceFilter*. The default value is 'SIGA;SIGB;SIGC' meaning that all three interfaces can be used with SCTP.
    - For MRAs: *DIAMETERDRA.Sctp.SIGDeviceFilter* (notice the different name). The default value is also 'SIGA;SIGB;SIGC' meaning that all three interfaces can be used with SCTP.

### 3.34.3 User Interface Changes

These are some of the instances where support for SIG-C can be found:

#### 3.34.3.1 SIG-C in VLAN IDs

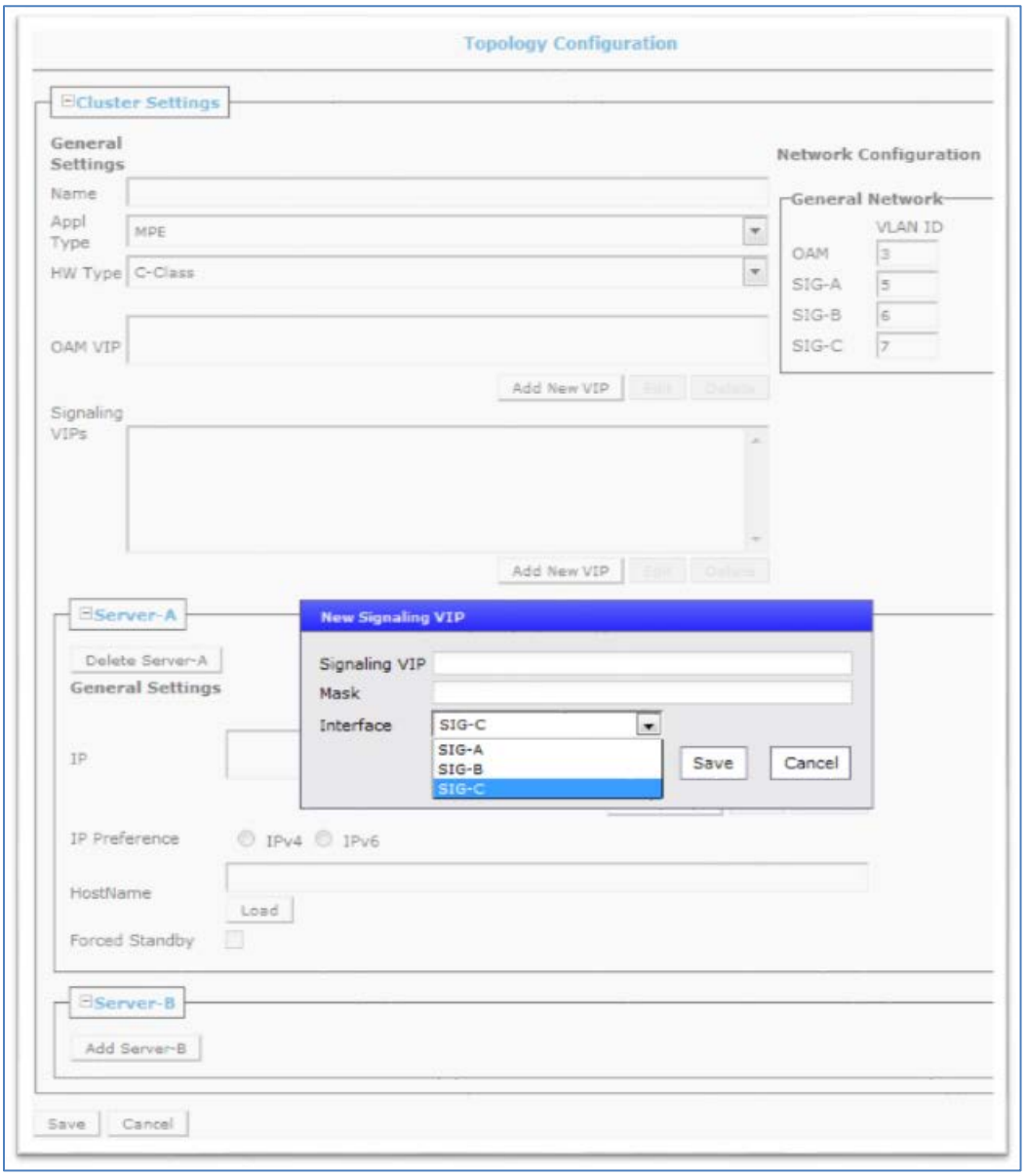
PLATFORM SETTING > Topology Settings > ... > Add MPE/MRA Cluster




On the right under Network Configuration it can be seen that SIG-C is available for VLAN ID use.

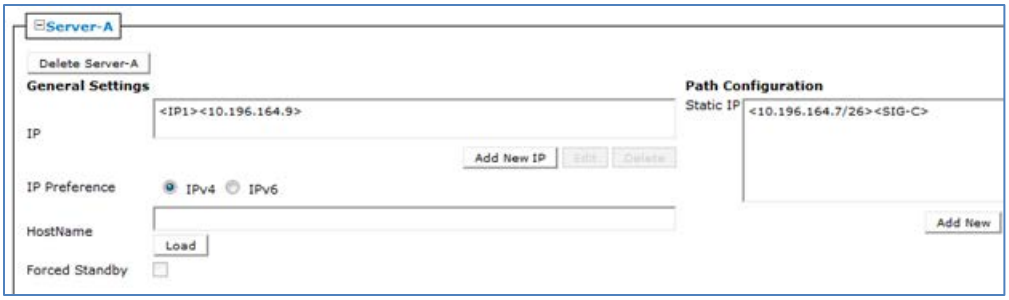
#### 3.34.3.2 *SIG-C for Signaling VIP*

PLATFORM SETTING > Topology Settings > ... > Add MPE/MRA Cluster > Add New VIP




#### 3.34.3.3 *Static IPs can use SIG-C*

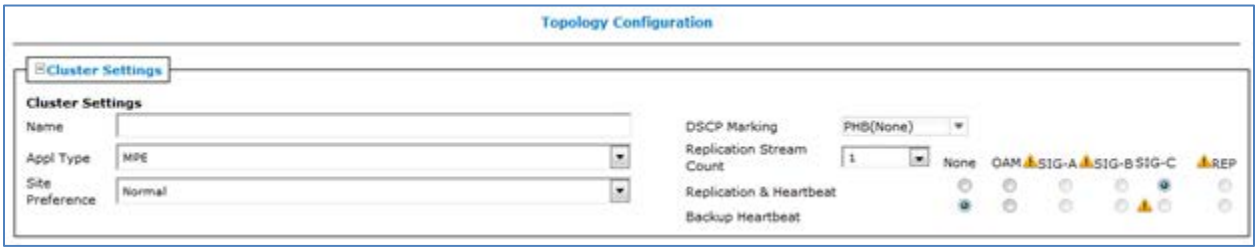
PLATFORM SETTING > Topology Settings > ... > Add MPE/MRA Cluster




As can be seen on the right under Path Configuration, the Static IP assigned to this server uses the SIG-C interface.

#### 3.34.3.4 *SIG-C in Georedundant Settings*

PLATFORM SETTING > Topology Settings > ... > Add MPE/MRA Cluster




Replication & Heartbeat and Backup Heartbeat can now use SIG-C as well.

#### 3.34.3.5 *Platform Configuration*

SIG-C is also available during platform initial configuration:

```
lqqqqqqqqqqqqqqqqqqqqqqqqu Initial Configuration tqqqqqqqqqqqqqqqqqqqqqqqqk
x                                                                        x
x                 HostName: guam-mpe-1a                                  x
x   OAM Real IPv4 Address: 10.240.152.79/26                             x
x OAM IPv4 Default Route:  10.240.152.66                                 x
x   OAM Real IPv6 Address:                                               x
x OAM IPv6 Default Route:                                                x
x              NTP Servers: 10.250.54.75                                 x
x            DNS Server A:                                               x
x            DNS Server B:                                               x
x              DNS Search:                                               x
x              OAM Device: bond0                                         x
x                OAM VLAN: 85                                            x
x               SIGA VLAN: 86                                            x
x               SIGB VLAN: 87                                            x
x               SIGC VLAN: 89                                            x
x                                                                        x
x                            lqqqqk   lqqqqqqqqk                         x
x                            x OK x   x Cancel x                         x
x                            mqqqqj   mqqqqqqqqj                         x
x                                                                        x
x                                                                        x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

As well as in:

```
lqqqqqqqqqqqqqqqqqqqqqqqqu Add Route tqqqqqqqqqqqqqqqqqqqqqqqqk
x                                                          x
x                 IP Type:  (*) IPv4  ( ) IPv6             x
x              Route Type:  ( ) host  (*) net  ( ) default x
x                 Network:  ( ) OAM  ( ) SIGA  ( ) SIGB  (*) SIGC x
x  Preferred Source Addr:  (*) None  ( ) VIP  ( ) STATIC   x
x             Destination:                                 x
x         Gateway Address:                                 x
x                                                          x
x                  lqqqqk   lqqqqqqqqk                     x
x                  x OK x   x Cancel x                     x
x                  mqqqqj   mqqqqqqqqj                     x
x                                                          x
x                                                          x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

## 3.35 POLICY CONNECTION DIRECTOR (PR# 22293420)

### 3.35.1 Introduction

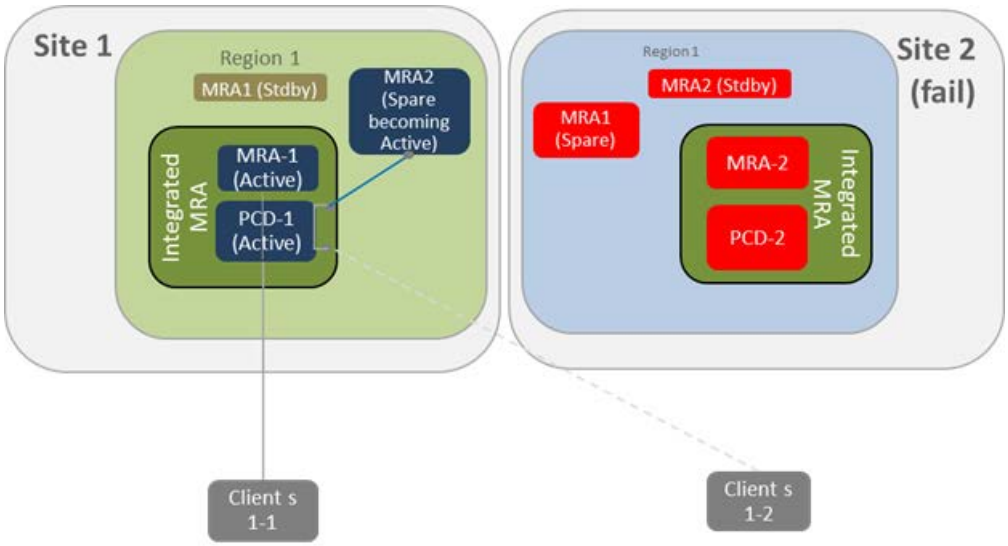
The Policy Connection Director (PCD) feature adds connection-level routing capabilities to an MRA in addition to the existing Diameter-level routing (using realm or hostname) and binding-level routing (using DRA binding information).

### 3.35.2 Detailed Description

PCD allows a specific client (a network element) to specify a primary and a secondary MRA connection.

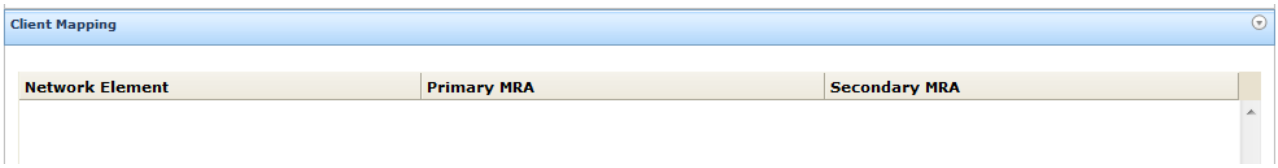
When the PCD functionality is added to an MRA, inter-MRA connections are established between the designated primary and secondary MRAs for the indicated network element only.

When a site failure occurs with PCD configured, messages from the indicated network element and intended for the failed MRA site are sent instead to the secondary site where the backup MRA will send them directly to the spare MRA site without parsing the messages for Diameter or Binding routing. The impact on processing on the backup MRA is minimal as the redirection is done at the connection level.

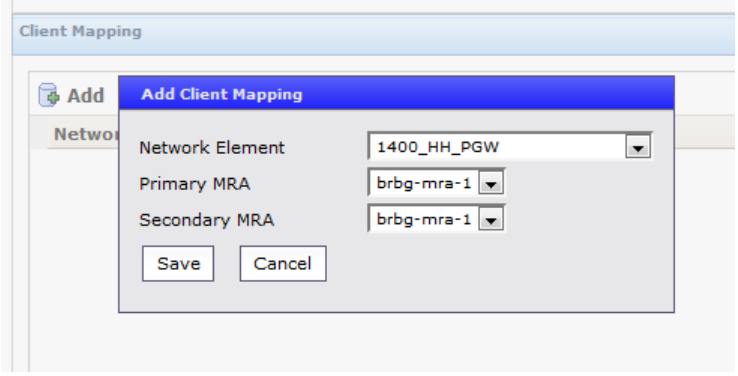



### 3.35.3 User Interface Changes

Under the existing MRA Associations window and **only** when an association has already been created) the new Client Mapping panel now appears:



The Client Mapping panel allows for the creation of a PCD connection between the primary and the secondary MRAs and associated with the indicated network element:




Once a client mapping association has been created, the inter-MRA PCD connection between the network element and the MRA can be seen at MRA > Reports > Diameter AF Statistics:

Diameter AF peers

| ID | IP Address : Port | Currently active connections | Connect Time | Disconnect Time |
|---|---|---|---|---|
| AF1 | 10.148.233.88 : 34101 | 1 | Tue May 03 07:29:22 EDT 2016 | N/A |
| pcd-mpe-vq.com | 10.196.132.155 : 3868 | 1 | Tue May 03 06:09:05 EDT 2016 | N/A |
| pcd_mra2.oracle.com | 10.148.234.214 : 51636 | 2 | Tue May 03 06:09:06 EDT 2016 | N/A |

Diameter AF PCD Peers

| ID | IP Address : Port | Currently active connections | Connect Time | Disconnect Time |
|---|---|---|---|---|
| af1-pcd-pcd_mra2.oracle.com | 10.148.234.214 : 3868 | 1 | Tue May 03 07:29:22 EDT 2016 | N/A |

In the above example the network element AF1 has a PCD connection to the MRA mra2.oracle.com

## 3.36 POLICY VNF MANAGEMENT (PR# 20837199)

### 3.36.1 Introduction

The VNF Management feature introduces into Policy Management a new application called NF Agent.

The NF Agent provides VNF Management services and acts as the integration point for orchestration software (NFVO) and Virtual Infrastructure Manager (VIM) interfaces via APIs.

VNF Management services provide the functionality that allows the virtual instance of an application (a VNF) to be instantiated, managed, and destroyed.

### 3.36.2 Detailed Description

The NF Agent is a hidden web service application that provides the logical interface and mappings between virtual deployments and Policy Management objects and logic.

It is accessed via the CMP application during MPE/MRA cluster and server configuration.

It keeps mappings between logical MPE/MRA and virtual instances.

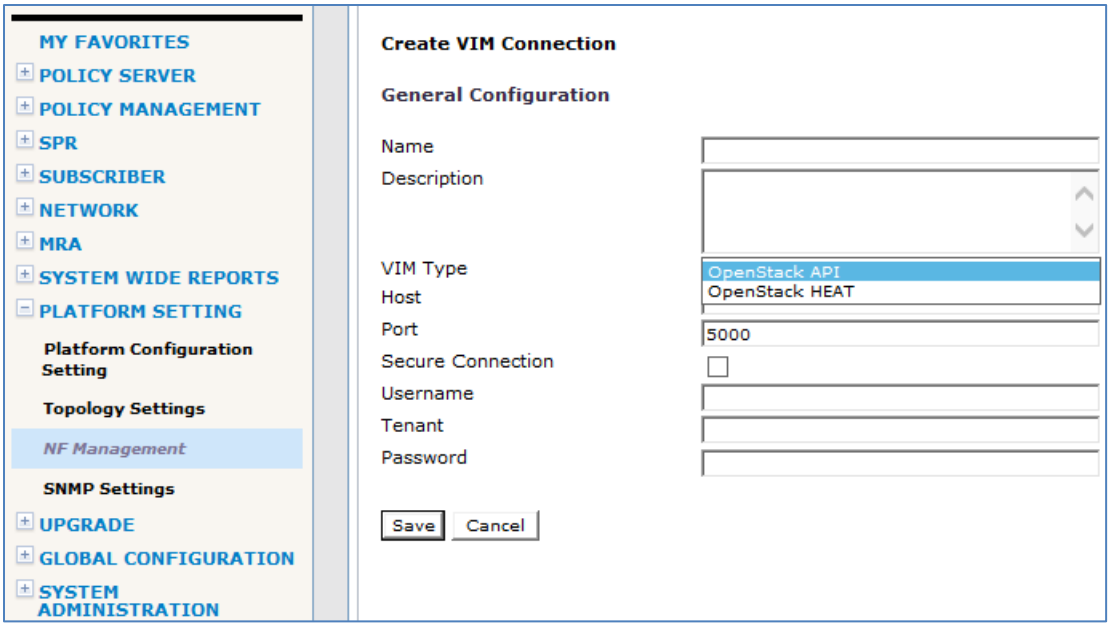
It currently supports two VIM connection types called OpenStack API and OpenStack Heat API.

### 3.36.3 User Interface Changes

Two new interface changes are introduced due to this feature.

#### 3.36.3.1 VIM Connections

A new object is introduced, a VIM Connection:

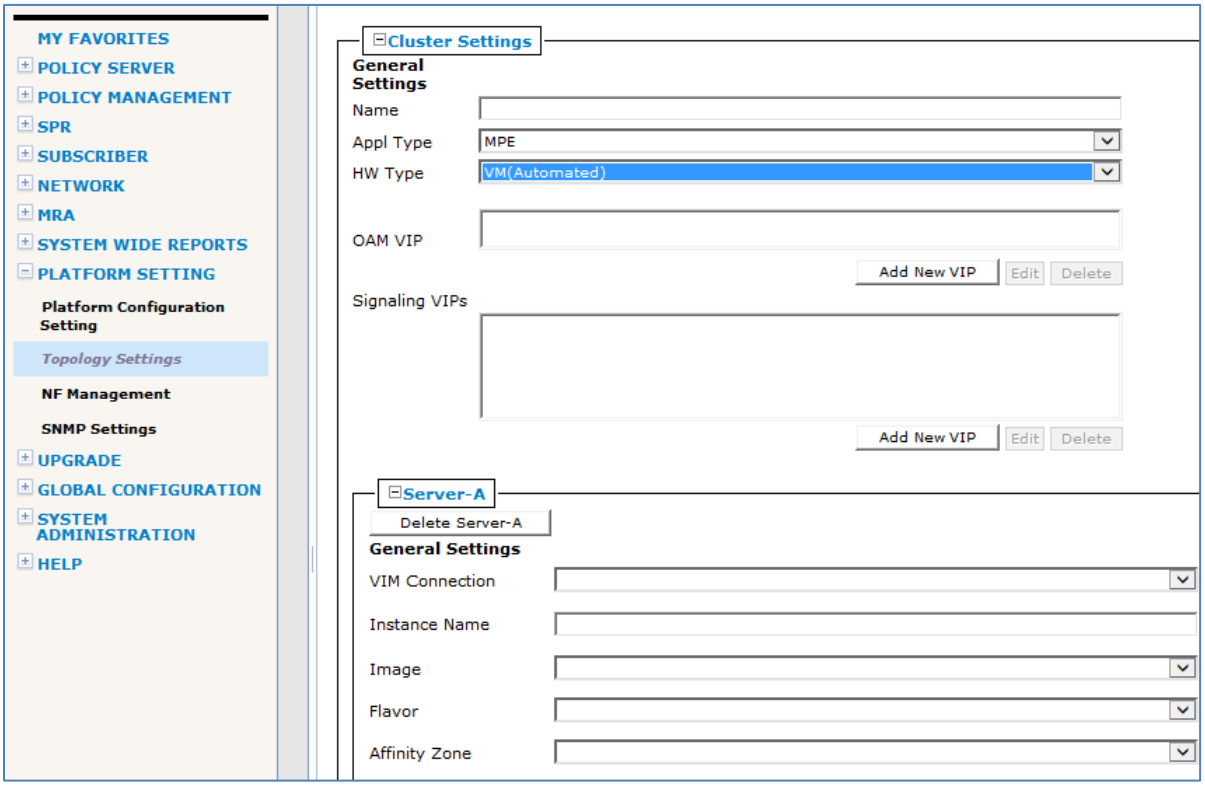



Two VIM types are supported, OpenStack API and OpenStack HEAT.

This object allows the establishment of connections to the different Virtual Infrastructure Managers (VIMs) responsible for creating/reading/updating/deleting the necessary virtual instances of MPE/MRA.

### 3.36.3.2 *Topology*

A new hardware type option for creating an MPE/MRA cluster:




The VM (Automated) hardware type allows the creation of MPE/MRA clusters as virtual instances.

When VM (Automated) is selected as hardware type, it prompts the display of a new set of options for the servers making up the new cluster.

The VIM Connection used provides additional instructions (Image, Flavor, etc.) can be passed to the VIM to specify the type of virtual instance needed to be created.

When the Save button is clicked and data has been collected, the CMP does a REST POST to the NF Agent which in turn instructs the VIM to create the new VM with the indicated parameters.

## 3.37 GX PENDING TRANSACTION RACE CONDITION (PR# 24304274)

### 3.37.1 Introduction

This enhancement allows successful Rx session establishment when Policy Management receives a second AAR message within a short time.

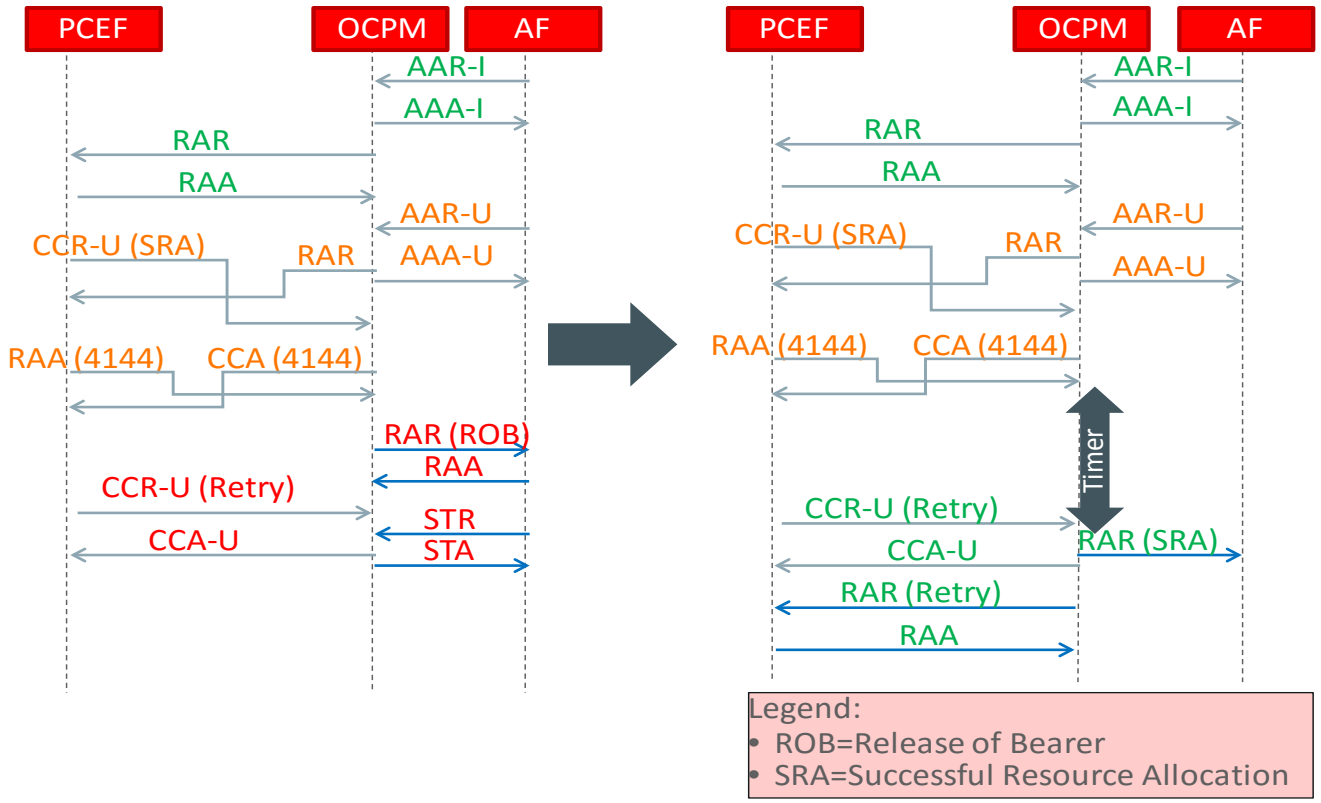
### 3.37.2 Detailed Description

Policy Management will no longer immediately send an Rx:RAR with Release of Bearer. Instead, Policy Management shall initiate a timer, and take the following actions:

- If Policy Management receives a Gx:CCR-U (presumably a retry of the previous failed CCR-U) for this subscriber before the timer expires, it shall respond with a Gx:CCA-U indicating success, and perform subsequent actions as needed to process the CCR-U (including, in the use case discussed, sending an RAR with the Specific-Action AVP indicating Successful Resource Allocation).. This behavior is illustrated on the right side of Figure 1.

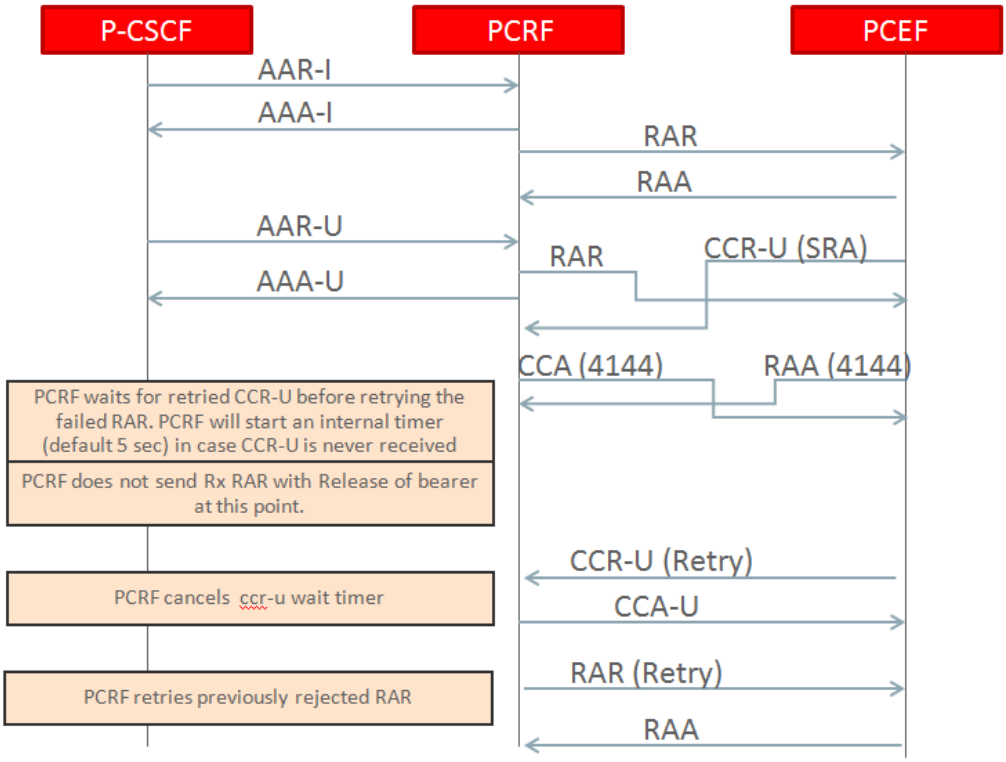
- If the timer expires before a Gx:CCR-U is received, Policy Management shall perform the appropriate failure processing as was previously done.

The message flow is summarized below:




**NOTE:** Left side of above figure is current behavior. Right side is the behavior enhanced

The detailed message flow is summarized below:




### *3.37.3 GUI Configuration Changes*

The below two new configurations are introduced in conjunction with *DIAMETER.Gx.RaceModeratorEnabled=true*

| Variable Name (Default) | Required/ Optional | Type | Description |
|---|---|---|---|
| DIAMETER.Gx. RarRetryOnCcrRace (disabled by default) | Required | Boolean | This property controls whether to resend Gx:RAR when the diameter message is not received by the destination host, as still on the way. |
| DIAMETER.Gx. CcrRetryWaitTime | Optional | Integer | The time in millisecond which PCRF server will wait for client request retry before retry server pending request. This configuration is applied when RarRetryOnCcrRace is true. |

## 4.0 PROTOCOL FLOW/PORT CHANGE

Additional 1813/UDP port support for default factory Firewall rules specifically for CMCC deployment.

## 5.0 OSSI XML/ SNMP MIB CHANGE

In the following table, the Added, changed and Deleted MIBs are listed, for the Delta of Policy Releases 9.9.2/11.5.x/12.1.x to 12.2.

**NOTE:**

### Policy Management MIBs

**Release 9.9.2 → 12.2**
**Release 11.5.x → 12.2**

| |
|---|
| pcrfMIBNotificationsTransportClosedNotify |
| pcrfMIBNotificationsTransportDisconnectedNotify |

**Issue**: Notifications removed from MIB.

**Impact**: If this new MIB is compiled to the central NMS and Release 9.9.2 or 11.5.x system emits these notifications, the operator will not be able to translate these notifications. NO impact to Release 12.1.x system.

**Recommendation**: No Action, documentation only.

**Release 12.1.x → 12.2**

| |
|---|
| pcrfMIBNotificationsQPFailedToExecuteRecaptureIpv4Notify |
| pcrfMIBNotificationsQPFailedToPrepareRecaptureIpv4Notify |
| pcrfMIBNotificationsQPFailedToRollbackRecaptureIpv4Notify |

**Issue**: Notifications removed from MIB.

**Impact**: If this new MIB is compiled to the central NMS and Release 9.9.2, 11.5.x, or 12.1.x system emits these notifications, the operator will not be able to translate these notifications.

**Recommendation**: No Action, documentation only.

### Policy Platform ( TPD) Changes from 6.7.0.x and 6.7.2.x to 7.0.3.x

| Change Type | MIB Module | Notification Name |
|---|---|---|
| Changed | TEKELEC-TPD-ALARMS-MIB | tpdDeviceIfWarn |

#### Old

```
[trapSequenceNumber, alarmLocation, alarmState, alarmId, alarmSeverity, alarmText, alarmTime,
bindVarNamesValuesStr, hrDeviceDescr, hrDeviceErrors, alarmNumber, alarmEventType, alarmProbableCause,
alarmAdditionalInfoStr]
```

**New**

```
[trapSequenceNumber, alarmLocation, alarmState, alarmId, alarmSeverity, alarmText, alarmTime,
hrDeviceDescr, hrDeviceErrors, bindVarNamesValuesStr, alarmNumber, alarmEventType, alarmProbableCause,
alarmAdditionalInfoStr]
```

**Issue**: Notification VarBinds have changed order.

**Impact**: Operator will get wrong values in a mixed version environment between Releases of 9.9.2 or 11.5.x with Release 12.2

**Recommendation**: Contact Oracle Technical Support

## *5.1 DELTA CHANGES FROM POLICY 9.9.2 ( TPD 6.7.0.X )*

| Change Type | MIB Module | OID | Notification Name |
|---|---|---|---|
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.31301 | comcolHaTopologyNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32540 | comcolTpdCpuPowerLimitMismatchNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32348 | comcolTpdFipsSubsystemProblemNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32537 | comcolTpdFipsSubsystemWarningNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32337 | comcolTpdFlashProgramFailureNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32347 | comcolTpdHWMGMTCLIProblemNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32701 | comcolTpdHidsBaselineCreatedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32702 | comcolTpdHidsBaselineDeletedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32707 | comcolTpdHidsBaselineUpdatedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32704 | comcolTpdHidsDisabledNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32703 | comcolTpdHidsEnabledNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32349 | comcolTpdHidsFileTamperingNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32706 | comcolTpdHidsResumedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32705 | comcolTpdHidsSuspendedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32346 | comcolTpdOEMHardwareProblemNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32350 | comcolTpdSecurityProcessDownNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32338 | comcolTpdSerialMezzUnseatedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.86306 | pcrfMIBNotificationsCMPApplyFailedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70501 | pcrfMIBNotificationsClusterMixedVersionNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70502 | pcrfMIBNotificationsClusterReplicationInhibitedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.71403 | pcrfMIBNotificationsConnectivityDegradedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.71402 | pcrfMIBNotificationsConnectivityLostNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70505 | pcrfMIBNotificationsISOMismatchNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.86308 | pcrfMIBNotificationsNCMPReferdObjMissNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.86303 | pcrfMIBNotificationsNWCMPApplyFailedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.74103 | pcrfMIBNotificationsNeWithoutCmtsIpNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.71003 | pcrfMIBNotificationsOmStatsExceptionErrorNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.71002 | pcrfMIBNotificationsOmStatsParseErrorNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.71005 | pcrfMIBNotificationsOmStatsValueExceedErrorNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70045 | pcrfMIBNotificationsQPDNSServerIsNotAvailableNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70041 | pcrfMIBNotificationsQPFailedToBlockAllIPv4Notify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70040 | pcrfMIBNotificationsQPFailedToBlockOAMIPv4Notify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70043 | pcrfMIBNotificationsQPFailedToRemoveAllIPv4Notify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70042 | pcrfMIBNotificationsQPFailedToRemoveOAMIPv4Notify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70044 | pcrfMIBNotificationsQPFailedToRollbackrecaptureIpv4Notify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70039 | pcrfMIBNotificationsQPHasBlockedIPv4Notify |

| | | | |
|---|---|---|---|
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70038 | pcrfMIBNotificationsQPHasBlockedOAMIPv4Notify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70017 | pcrfMIBNotificationsQPNoStaticIPForRouteNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70016 | pcrfMIBNotificationsQPNoVipForRouteNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70007 | pcrfMIBNotificationsQPReaourceNotReadyNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.71001 | pcrfMIBNotificationsRemoteDiversionNotPossibleNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.86307 | pcrfMIBNotificationsSCMPSYNCFAILSNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.86305 | pcrfMIBNotificationsSCMPSplitBrainNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.86304 | pcrfMIBNotificationsSCMPUNREACHABLENotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70503 | pcrfMIBNotificationsServerForcedStandbyNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70508 | pcrfMIBNotificationsServerIsZombieNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70500 | pcrfMIBNotificationsSystemMixedVersionNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70507 | pcrfMIBNotificationsUpgradeInProgressNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70506 | pcrfMIBNotificationsUpgradeOperationFailedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.78850 | pcrfMIBNotificationsVNFOperationErrorNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.79995 | pcrfMIBNotificationsX1ConnectionLostNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.79996 | pcrfMIBNotificationsX2ConnectionLostNotify |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.3.41 | tpdCpuPowerLimitMismatch |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.2.49 | tpdFipsSubsystemProblem |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.3.38 | tpdFipsSubsystemWarning |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.2.38 | tpdFlashProgramFailure |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.4.2 | tpdHidsBaselineCreated |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.4.3 | tpdHidsBaselineDeleted |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.4.8 | tpdHidsBaselineUpdated |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.4.5 | tpdHidsDisabled |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.4.4 | tpdHidsEnabled |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.2.50 | tpdHidsFileTampering |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.4.7 | tpdHidsResumed |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.4.6 | tpdHidsSuspended |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.2.51 | tpdSecurityProcessDown |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.2.39 | tpdSerialMezzUnseated |
| Changed **[OBSOLETE]**[1] | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.31223 | comcolHaHbTransmitFailureNotify |
| Changed **[OBSOLETE]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.31222 | comcolHaNotConfiguredNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.31287 | comcolHaSbrCompleteNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.31285 | comcolHaSbrEntryNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.31286 | comcolHaSbrPlanNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.31225 | comcolHaSvcStartFailureNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32300 | comcolTpdFanErrorNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32306 | comcolTpdRamShortageErrorNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32503 | comcolTpdRamShortageWarningNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32307 | comcolTpdSwapSpaceShortageErrorNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32505 | comcolTpdSwapSpaceShortageWarningNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70015 | pcrfMIBNotificationsQPAddRouteFailedNotify |
| Changed **[VarBinds]** | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.3.14 | tpdDeviceIfWarn |
| Deleted | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.71402 | pcrfMIBNotificationsTransportClosedNotify |
| Deleted | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.71403 | pcrfMIBNotificationsTransportDisconnectedNotify |

## 5.2 DELTA CHANGES FROM POLICY 11.5.X ( TPD 6.7.2.X )

| Change Type | MIB Module | OID | Notification Name |
|---|---|---|---|
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.31301 | comcolHaTopologyNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32540 | comcolTpdCpuPowerLimitMismatchNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32348 | comcolTpdFipsSubsystemProblemNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32537 | comcolTpdFipsSubsystemWarningNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32337 | comcolTpdFlashProgramFailureNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32347 | comcolTpdHWMGMTCLIProblemNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32701 | comcolTpdHidsBaselineCreatedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32702 | comcolTpdHidsBaselineDeletedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32707 | comcolTpdHidsBaselineUpdatedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32704 | comcolTpdHidsDisabledNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32703 | comcolTpdHidsEnabledNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32349 | comcolTpdHidsFileTamperingNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32706 | comcolTpdHidsResumedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32705 | comcolTpdHidsSuspendedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32346 | comcolTpdOEMHardwareProblemNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32350 | comcolTpdSecurityProcessDownNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32338 | comcolTpdSerialMezzUnseatedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.79120 | pcrfMIBNotificationsBatchDiskQuotaExceedsNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.86306 | pcrfMIBNotificationsCMPApplyFailedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70501 | pcrfMIBNotificationsClusterMixedVersionNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70502 | pcrfMIBNotificationsClusterReplicationInhibitedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.71403 | pcrfMIBNotificationsConnectivityDegradedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.71402 | pcrfMIBNotificationsConnectivityLostNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.79110 | pcrfMIBNotificationsFilesUploadingFailureNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70505 | pcrfMIBNotificationsISOMismatchNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.79108 | pcrfMIBNotificationsMSDiskNoSpaceNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.79107 | pcrfMIBNotificationsMSDiskQuotaExceedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.79105 | pcrfMIBNotificationsMediationSOAPTooBusyNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.86308 | pcrfMIBNotificationsNCMPReferdObjMissNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.86303 | pcrfMIBNotificationsNWCMPApplyFailedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.74103 | pcrfMIBNotificationsNeWithoutCmtsIpNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.71003 | pcrfMIBNotificationsOmStatsExceptionErrorNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.71002 | pcrfMIBNotificationsOmStatsParseErrorNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.71005 | pcrfMIBNotificationsOmStatsValueExceedErrorNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70045 | pcrfMIBNotificationsQPDNSServerIsNotAvailableNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70041 | pcrfMIBNotificationsQPFailedToBlockAllIPv4Notify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70040 | pcrfMIBNotificationsQPFailedToBlockOAMIPv4Notify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70043 | pcrfMIBNotificationsQPFailedToRemoveAllIPv4Notify |

| | | | |
|---|---|---|---|
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70042 | pcrfMIBNotificationsQPFailedToRemoveOAMIPv4Notify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70044 | pcrfMIBNotificationsQPFailedToRollbackrecaptureIpv4Notify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70039 | pcrfMIBNotificationsQPHasBlockedIPv4Notify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70038 | pcrfMIBNotificationsQPHasBlockedOAMIPv4Notify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70017 | pcrfMIBNotificationsQPNoStaticIPForRouteNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70016 | pcrfMIBNotificationsQPNoVipForRouteNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70007 | pcrfMIBNotificationsQPReaourceNotReadyNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.71001 | pcrfMIBNotificationsRemoteDiversionNotPossibleNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.86307 | pcrfMIBNotificationsSCMPSYNCFAILSNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.86305 | pcrfMIBNotificationsSCMPSplitBrainNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.86304 | pcrfMIBNotificationsSCMPUNREACHABLENotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.72575 | pcrfMIBNotificationsSMSRHTTPConnectionClosedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.79106 | pcrfMIBNotificationsSPRConnectionFailedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.79109 | pcrfMIBNotificationsSPRLicenselimitNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70503 | pcrfMIBNotificationsServerForcedStandbyNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70508 | pcrfMIBNotificationsServerIsZombieNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70500 | pcrfMIBNotificationsSystemMixedVersionNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70507 | pcrfMIBNotificationsUpgradeInProgressNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70506 | pcrfMIBNotificationsUpgradeOperationFailedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.78850 | pcrfMIBNotificationsVNFOperationErrorNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.79995 | pcrfMIBNotificationsX1ConnectionLostNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.79996 | pcrfMIBNotificationsX2ConnectionLostNotify |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.3.41 | tpdCpuPowerLimitMismatch |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.2.49 | tpdFipsSubsystemProblem |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.3.38 | tpdFipsSubsystemWarning |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.2.38 | tpdFlashProgramFailure |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.4.2 | tpdHidsBaselineCreated |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.4.3 | tpdHidsBaselineDeleted |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.4.8 | tpdHidsBaselineUpdated |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.4.5 | tpdHidsDisabled |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.4.4 | tpdHidsEnabled |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.2.50 | tpdHidsFileTampering |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.4.7 | tpdHidsResumed |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.4.6 | tpdHidsSuspended |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.2.51 | tpdSecurityProcessDown |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.2.39 | tpdSerialMezzUnseated |
| Changed **[OBSOLETE]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.31223 | comcolHaHbTransmitFailureNotify |
| Changed **[OBSOLETE]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.31222 | comcolHaNotConfiguredNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.31287 | comcolHaSbrCompleteNotify |

| | | | |
|---|---|---|---|
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.31285 | comcolHaSbrEntryNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.31286 | comcolHaSbrPlanNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.31225 | comcolHaSvcStartFailureNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32300 | comcolTpdFanErrorNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32306 | comcolTpdRamShortageErrorNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32503 | comcolTpdRamShortageWarningNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32307 | comcolTpdSwapSpaceShortageErrorNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32505 | comcolTpdSwapSpaceShortageWarningNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70015 | pcrfMIBNotificationsQPAddRouteFailedNotify |
| Changed **[VarBinds]** | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.3.14 | tpdDeviceIfWarn |
| Deleted | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.71402 | pcrfMIBNotificationsTransportClosedNotify |
| Deleted | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.71403 | pcrfMIBNotificationsTransportDisconnectedNotify |

## *5.3 DELTA CHANGES FROM POLICY 12.1.X ( TPD 7.0.2.X )*

| Change Type | MIB Module | OID | Notification Name |
|---|---|---|---|
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32540 | comcolTpdCpuPowerLimitMismatchNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32348 | comcolTpdFipsSubsystemProblemNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32537 | comcolTpdFipsSubsystemWarningNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32337 | comcolTpdFlashProgramFailureNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32701 | comcolTpdHidsBaselineCreatedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32702 | comcolTpdHidsBaselineDeletedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32707 | comcolTpdHidsBaselineUpdatedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32704 | comcolTpdHidsDisabledNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32703 | comcolTpdHidsEnabledNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32349 | comcolTpdHidsFileTamperingNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32706 | comcolTpdHidsResumedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32705 | comcolTpdHidsSuspendedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32350 | comcolTpdSecurityProcessDownNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32338 | comcolTpdSerialMezzUnseatedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.79120 | pcrfMIBNotificationsBatchDiskQuotaExceedsNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.79110 | pcrfMIBNotificationsFilesUploadingFailureNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.79108 | pcrfMIBNotificationsMSDiskNoSpaceNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.79107 | pcrfMIBNotificationsMSDiskQuotaExceedNotify |

| | | | |
|---|---|---|---|
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.79105 | pcrfMIBNotificationsMediationSOAPTooBusyNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.74103 | pcrfMIBNotificationsNeWithoutCmtsIpNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70045 | pcrfMIBNotificationsQPDNSServerIsNotAvailableNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70041 | pcrfMIBNotificationsQPFailedToBlockAllIPv4Notify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70040 | pcrfMIBNotificationsQPFailedToBlockOAMIPv4Notify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70043 | pcrfMIBNotificationsQPFailedToRemoveAllIPv4Notify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70042 | pcrfMIBNotificationsQPFailedToRemoveOAMIPv4Notify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70044 | pcrfMIBNotificationsQPFailedToRollbackrecaptureIpv4Notify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70038 | pcrfMIBNotificationsQPHasBlockedOAMIPv4Notify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70017 | pcrfMIBNotificationsQPNoStaticIPForRouteNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70016 | pcrfMIBNotificationsQPNoVipForRouteNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70007 | pcrfMIBNotificationsQPReaourceNotReadyNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.79106 | pcrfMIBNotificationsSPRConnectionFailedNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.79109 | pcrfMIBNotificationsSPRLicenselimitNotify |
| Added | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.78850 | pcrfMIBNotificationsVNFOperationErrorNotify |
| Added | TEKELEC-TPD-ALARMS-MIB | 1.3.6.1.4.1.323.5.3.18.3.1.3.41 | tpdCpuPowerLimitMismatch |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.31287 | comcolHaSbrCompleteNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.31285 | comcolHaSbrEntryNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.31286 | comcolHaSbrPlanNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32300 | comcolTpdFanErrorNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32347 | comcolTpdHWMGMTCLIProblemNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32346 | comcolTpdOEMHardwareProblemNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32306 | comcolTpdRamShortageErrorNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32503 | comcolTpdRamShortageWarningNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32307 | comcolTpdSwapSpaceShortageErrorNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.32505 | comcolTpdSwapSpaceShortageWarningNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70015 | pcrfMIBNotificationsQPAddRouteFailedNotify |
| Changed **[DESCRIPTION]** | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70039 | pcrfMIBNotificationsQPHasBlockedIPv4Notify |
| Deleted | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70041 | pcrfMIBNotificationsQPFailedToExecuteRecaptureIpv4Notify |
| Deleted | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70040 | pcrfMIBNotificationsQPFailedToPrepareRecaptureIpv4Notify |
| Deleted | PCRF-ALARM-MIB | 1.3.6.1.4.1.323.5.3.29.1.2.70042 | pcrfMIBNotificationsQPFailedToRollbackRecaptureIpv4Notify |