****

**Oracle® COMMUNICATIONS**

Diameter Signaling Router   
DSR Network Impact Report

Release 8.3

E93239 Revision 02

July 2020

Oracle Diameter Signaling Router DSR Network Impact Report,

Release 8.3

Copyright © 2020 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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

**TABLE OF CONTENTS**

[Oracle® COMMUNICATIONS 1](#_Toc44498625)

[Diameter Signaling Router DSR Network Impact Report 1](#_Toc44498626)

[1.0 Introduction 8](#_Toc44498627)

[1.1 Purpose/Scope 8](#_Toc44498628)

[1.2 Compatibility 8](#_Toc44498629)

[1.3 Disclaimers 8](#_Toc44498630)

[2.0 Overview of DSR 8.3 Features 10](#_Toc44498631)

[2.1 enhancements to DSR 8.3 functionality by category 11](#_Toc44498634)

[2.2 AVP Removal feature 12](#_Toc44498635)

[2.3 vEIR (DIAMETER & vSTP) 12](#_Toc44498636)

[2.4 MTC-IWF and SCEF Solution 12](#_Toc44498637)

[2.5 5G Service proxy 13](#_Toc44498638)

[2.6 VNFM 13](#_Toc44498639)

[2.7 HA Switchover safeguards 14](#_Toc44498640)

[2.8 diameter security application (RSR message support) 14](#_Toc44498641)

[2.9 MMI UPDATES 15](#_Toc44498642)

[2.10 vSTP Congestion and flow control 17](#_Toc44498643)

[2.11 vstp Licence measurement feature 17](#_Toc44498644)

[2.12 vstp event/alarm logging enhancement 17](#_Toc44498645)

[2.13 CAPACITY INCREASE FEATURE 17](#_Toc44498646)

[2.15 hardware Changes 18](#_Toc44498660)

[2.16 software Changes 18](#_Toc44498661)

[2.17 firmware Changes 19](#_Toc44498662)

[2.18 upgrade Overview 20](#_Toc44498663)

[2.19 migration of DSR Data 22](#_Toc44498664)

[3.0 Feature OAM Changes 23](#_Toc44498665)

[3.1 AVP Removal FEATURE 23](#_Toc44498666)

[3.2 vEIR (Diameter & VSTP) 25](#_Toc44498667)

[3.3 SCEF 36](#_Toc44498668)

[3.4 5G SPF + NRF (PoC) 41](#_Toc44498669)

[3.5 vNFM 44](#_Toc44498670)

[3.6 CAPACITY INCREASE FEATURE 50](#_Toc44498671)

[3.7 DIAMETER SECURITY APPLICATION (RSR MESSAGE support) 50](#_Toc44498672)

[3.8 VSTP license measurement 53](#_Toc44498673)

[3.9 vstp Congestion Control Enhancements 54](#_Toc44498674)

[3.10 vstp Event/alarm Logging Enhancements 55](#_Toc44498675)

[3.11 MMI Updates 55](#_Toc44498676)

[4.0 MEAL INSERTS 57](#_Toc44498677)

[4.1 DSR/SDS 8.3 MEAL Snapshot 57](#_Toc44498678)

[4.2 Meal Deltas (8.2.1) 57](#_Toc44498679)

[4.3 Meal Deltas (8.1.1) 57](#_Toc44498680)

[4.4 Meal Deltas (8.0) 57](#_Toc44498681)

[4.5 Meal Deltas (7.3) & SDS (7.3.1) 57](#_Toc44498682)

[5.0 reference list 58](#_Toc44498683)

[***Figure 1 – DSR Upgrade Paths*** 20](#_Toc44498684)

[***Figure 2 – SDS Upgrade Paths*** 20](#_Toc44498685)

[***Figure 3 – IDIH Upgrade Paths*** 21](#_Toc44498686)

**GLOSSARY**

| **Acronym/Term** | **Definition** |
| --- | --- |
| APIGW | API Gateway |
| ASGU | Automated Server Group Upgrade |
| AS | Application Server |
| ASU | Automated Site Upgrade |
| AVP | Attribute Value Pair |
| BSBR | Binding SBR |
| CA | Communication Agent |
| CAF | Customized Application Framework |
| CLI | Command Line Interface |
| CLR | Cancel Local Request |
| DA-MP | Diameter Agent Message Processor |
| DAL | Diameter Application Layer |
| DCA | Diameter Custom Application Framework |
| DCL | Diameter Connection Layer |
| DEA | Diameter Edge Agent |
| DPC | Destination Point Code |
| DPL | Data Processor Library |
| DRMP | Diameter Routing Message Priority |
| DPI | Diameter Plug-in |
| DSA | Diameter Security Application |
| DoS | Denial of Service |
| EXGSTACK | Eagle Next Generation Stack |
| ECR | Mobile Equipment-Identity-Check-Request |
| ECA | Mobile Equipment-Identity-Check-Answer |
| FLOBR | Flexible Link set Optional Based Routing |
| GUI | Graphical User Interface |
| GTT | Global title translation |
| GTA | Global title Address |
| HSS | Home Subscriber Server |
| HLR | Home Location register |
| iLO | Integrated Lights Out |
| IMI | Internal Management Interface |
| IPv4 | IPv4 address of the subscriber |
| IPv6 | IPv6 address of the subscriber |
| IMSI | International Mobile Subscriber Identity |
| IMPU | IP Multimedia Public Identity |
| IMPI | IP Multimedia Private Identity |
| IOT | Interoperability Tests |
| KPI | Key Performance Indicator |
| LAI | Location Area Identity |
| LTE | Long Term Evolution |
| MAP | Mobile Application Part |
| MBR | Map Based Routing |
| MCC | Mobile Country Code |
| MEAL | Measurements, Events, Alarms, and Logging |
| MME | Mobility Management Entity |
| MMI | Man Machine Interface |
| MP | Message Processor |
| MPS | Messages per Second |
| MS | Mobile Station/Handset |
| MSU | Message signal Unit |
| MSISDN | Mobile Station International Subscriber Directory Number |
| MTC | Machine type communication |
| MTP | Message Transfer Part |
| MO | Managed Object |
| NE | Network Element |
| NGN | Next Generation Networks |
| NGN-PS | NGN Priority Services |
| NIDD | Non-IP data delivery [directly through MME/SGSN] |
| NMS | Network Management System |
| NOAM | Network Operations Administration and Maintenance |
| NF | Network Function |
| NRF | NF Repository Function |
| OAG | Oracle Accessibility Guidelines |
| OAM | Operations, Administration, Maintenance |
| OAM&P | Operations, Administration, Maintenance and Provisioning |
| OCUDR | Oracle Communications User Data Repository |
| OPC | Origin Point Code |
| PDRA | Policy Diameter Relay Agent |
| PCRF | Policy Control and Charging Rules Function |
| PCIMC | Per Connection Ingress Message Control |
| PDU | Protocol Data Unit |
| PDN | Packet Data Network |
| PM&C | Platform, Management and Control |
| POR | Plan of Record |
| PS | Priority Service (NGN-PS) |
| RAN | Radio Access Network |
| ROS | Routing Option Set |
| RSA | Reset Answer |
| RSR | Reset Request |
| SBR | Session Binding Repository |
| SSBR | Session SBR |
| SCEF | Service Capability Exposure Function |
| ScsAsId | String provided by SCS to identify itself in non-3GPP world |
| SCEF-MP | Message processing server that will run business login of SCEF/MTC-IWF. (for DSR , it is DA-MP server) |
| SCEF-DB | U-SBR (database server that stores context of SCEF calls) |
| SCS | Service Control Server |
| SOAM | Site Operations Administration and Maintenance |
| SPF | Service Proxy Function |
| SS7 | Signaling System No. 7 |
| STP-MP | Signaling Transfer Point Message Processor |
| SV | Software Version |
| TPD | ORACLE Platform Distribution |
| TCAP | Transaction Capability Part |
| TLTRI | T8 Long Term Transaction Reference ID |
| TTRI | T8 Transaction Reference ID |
| TOBR | TCAP Opcode Based Routing |
| UE | User Equipment |
| USBR | Universal SBR |
| vEIR | Virtual Equipment Identity Register |
| VIP | Virtual IP Address |
| VNF | Virtual Network Functions |
| VNFM | Virtual Network Functions Manager |
| VPLMN | Virtual Public Land Mobile Network |
| VSTP | Virtual SS7 Signal Transfer Point |
| VEDSR | Virtualized Engineered DSR |
| XMI | External Management Interface |
| XSI | External Signaling Interface |

# Introduction

## Purpose/Scope

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

## Compatibility

### Product Compatibility

DSR 8.3 is compatible with IDIH 7.3, 8.0, 8.1, 8.2 and 8.2.1

DSR 8.3 is compatible with SDS 7.3, 8.0, 8.1, 8.2 and 8.3

DSR 8.3 is compatible with APIGW 8.3

DSR 8.3 is compatible with TPD 7.6, ComCOL 7.5, AppWorks 8.3, EXGSTACK 8.3, TVOE 3.6, PM&C 6.6, APIGW 8.3 and UDR 12.5.x

SDS 8.3 is compatible with TPD 7.6, ComCOL 7.5, AppWorks 8.3, EXGSTACK 8.3, TVOE 3.6 and PM&C 6.6.

### DSR 8.3 Incompatibility Software

The following software elements are not compatible with DSR 8.3:

* DAMP Active-Standby Configuration
* GLA
* MAP Diameter Interworking
* RADIUS

Virtualized Engineered DSR (VEDSR) deployment, which is also known as TVOE based Fully Virtualized Rack Mount Server (FV RMS) Signaling node, is not supported from DSR 8.3 onwards.

Following are the non-supported network elements of Virtualized Engineered DSR (VEDSR):

* DSR NOAM,
* DSR SOAM,
* DSR Message Processors (MP),
* SS7 MP,
* DSR IPFE,
* DSR SBR (Session/Binding/Universal),
* SDS NOAM,
* SDS SOAM,
* SDS QS,
* SDS DP

Note: DSR and SDS Baremetal Installations with TVOE based NOAM/SOAM will continue to be supported.

VEDSR networks and associated elements must be migrated to virtual DSR implementation based on KVM with/without OpenStack or VMware prior to DSR 8.3 upgrade or install.

## Disclaimers

This document summarizes Release Diameter Signaling Router 8.3 new and enhancement features as compared to Release 8.2, 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.

This document summarizes Diameter Signaling Router 8.3 **5G Service Proxy** enhancement feature. It is a standalone VM and is intended for demonstration purpose only. This feature has no impact whatsoever to DSR 8.3 release.

# Overview of DSR 8.3 Features

This section provides a high-level overview of the DSR 8.3 release features that may impact OAM interfaces and activities.

For a list of all features, please see Release Notes for DSR 8.3 found at the following link:

**<http://docs.oracle.com/en/industries/communications/diameter-signaling-router/index.html>**

For additional details of the various features, please refer to the “DSR 8.3 Feature Guide” found at the following link:

[**http://docs.oracle.com/en/industries/communications/diameter-signaling-router/index.html**](http://docs.oracle.com/en/industries/communications/diameter-signaling-router/index.html)



## enhancements to DSR 8.3 functionality by category

Note: For information on upgrade planning and required steps before upgrade, please refer to the DSR 8.3 Software Upgrade Guide on the public Oracle Documentation Site:

Docs.oracle.com 🡪 Industries 🡪 Oracle Communications documentation🡪 Diameter Signaling Router 🡪 Release 8.3.

Table 1 DSR 8.3 New Features/Enhancements

|  |
| --- |
| **DSR 8.3 Feature/Enhancement Name** |
|
| [AVP Removal Feature](#_Automatic_Site_Upgrade_1)**Error! Hyperlink reference not valid.** |
| [vEIR (Diameter & vSTP)](#_mmi_1) |
| [MTC-IWF and SCEF Solution](#_DSR_HP_C-Class/Cloud/VEDSR)**Error! Hyperlink reference not valid.** |
| [5G Service Proxy](#_DSR_Route_Group)**Error! Hyperlink reference not valid.** |
| [VNFM](#_Feature_MMI_Updates)**Error! Hyperlink reference not valid.** |
| [HA Switchover Safeguards](#_Gen9_V2_Performance)**Error! Hyperlink reference not valid.** |
| [Diameter Security Application (RSR message support)](#_SDS_Add_Functionality)**Error! Hyperlink reference not valid.** |
| [MMI Updates](#_SSST)**Error! Hyperlink reference not valid.** |
| [vSTP Congestion and Flow Control](#_fabr_and_rbar) |
| [vSTP License Measurement Feature](#_Stallion_data_collector) |
| [vSTP Event/Alarm Logging Enhancement](#_Accessibility) |
| [Capacity Increase Feature](#_Availability_Group_enhancement) |

## AVP Removal feature

This feature is intended to avoid the message priority assignment using DRMP and NGN-PS AVP’s which are used internally to throttle messages during congestion and also to avoid the DoS attacks using DRMP and NGN-PS AVPs when either NGN-PS or DRMP Admin State is enabled and “Ignore Priority From Peer” is enabled for a given peer.

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| POR 24970121  AVP Removal Feature | This feature provides the following enhancement:  Enhance DCL logic to avoid the message priority assignment using DRMP and NGN-PS AVP’s based on the new configuration provided from GUI.  Update DSR OAM GUI to allow user to enable/disable the field “Ignore Priority From Peer” in following condition:   * When either NGN-PS Admin or DRMP Admin state is enabled. * Changed allowed even if diameter connection is enabled. | Enhancement Request |

## vEIR (DIAMETER & vSTP)

This enhancement will support Equipment Identity Register (vEIR) Diameter & vSTP functionality.

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| POR 27355466  vEIR | EIR solution helps network operators to reduce mobile handset thefts by providing a mechanism that allows the network operators to prevent stolen or disallowed handsets from accessing the network. | Enhancement Request |

## MTC-IWF and SCEF Solution

This enhancement will provide access to network capabilities through homogenous network application programming interfaces (e.g. Network APIs) defined over T8 interface towards SCS/AS.

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| POR 24441275 | The SCEF solution provide the following functionality.   * Non IP data delivery for low power devices * Monitoring a devices state * SCS/AS AAA (Application Server authorization, accounting and SLAs) * Device Trigger Delivery through SMS acting as an MTC-IWF * Receiving reports about the network congestion condition of the RAN | Enhancement Request |

## 5G Service proxy

This feature is intended to provide the deployment of 5G SPF+NRF using VNFM

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| Bug 27123299  DSR 5G SPF\_NRF VNF | This enhancement support  SPF establishes a 5G service proxy (signaling) portal.  SPF integrates with internal NRF.  SPF routes messages between external NFs.  Includes active NRF by default.  NRF provides all standard NRF services:   * NF registration * NF discovery. Only discovery by service name is supported. * NF de-registration   NRF receives messages via SPF function and sends messages via SPF function.  SPF and NRF store valuable data in persistent cloud storage.  Automated Deployment/Configuration of SPF+NRF VNF via DSR VNFM on OpenStack clouds.  VM snapshot (CINDER block) disaster recovery is supported.  Only HTTP supported (no TLS support). | Enhancement Request |

## VNFM

The objective of the DSR VNFM is to provide an ETSI-compliant VNF manager.

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
|  | The VNFM would be helpful in   * Automate lifecycle management (LCM) operations for DSR VNFs. * Automation of these operations can reduce their execution time by up to 90 percent. * Provide a standardized interface for ease of integration with automation clients. | Enhancement Request |

## HA Switchover safeguards

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| POR 27031274  ENH 27031274: HA switchover safeguards  BUG 26998761: Upgrade Complete displayed before replication active | Applications implemented the new hooks(validators) to verify the Health of the mate servers before switchover  Health of mate server implies the Replication Status  Replication link status will either be "Active" or "ActivePostAudit"  Application code will check the replication link status here.  HA Status GUI will display the warning if mate server in that server group is not healthy. Also an alarm shall be raised and user shall take the appropriate action.  As an early check (In Prepare/Ready state) Upgrade module shall check mate server health and shall display warning.  ASU shall also call these validators APIs if this check is required for B/C level servers during switchover.  Assumption: solution for the feature based on Comcol APIs which provide health status of local/remote servers | Bug Fix |

## diameter security application (RSR message support)

The RSR message support has been added for statefull counter measures in DSR Rel.8.3

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| POR 27155790 | This feature will support RSR message for the following statefull counter measures in DSA   * Previous Location Check * Source Host Validation HSS * Source Host Validation MME | Enhancement Request |

## MMI UPDATES

DSR supports a RESTful machine-to-machine interface to support OAM requests from external clients Oracle provided or from 3rd parties.

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| POR 27096415  Machine-to-Machine interface updates | MMIs have been enabled for the following:   * FABR * Applications * Exceptions * Destinations * Address Resolutions * System Options * ComAgent * Remote Servers * Common Application Options * Connection Status * Routed Services Status * HA Services Status * Diameter * Common Application Options * Shared Traffic Throttle Groups * Capacity Summary * Connection Capacity * Route List * Route Group * Peer Nodes * DAMPs (Peer, Connectivity, and Server Host Name Status Tables) * Signaling Firewall * Application Maintenance * SDS * Connections * Destinations * Destination Map * NAI Host * DRMP * Domain Identifiers * Options * Blacklist * Subscribers * Routing Entities | Enhancement Request |

## vSTP Congestion and flow control

The DSR 8.3 vSTP function support with the following congestion and flow control including

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| POR 26678690 | PDU Pool tuning.  Usage tracking of RSP and Linkset buffers and related MEALs. | Enhancement Request |

## vstp Licence measurement feature

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| POR 27729578 | This feature is intended to provide the means to user to run automated or on-demand reports for licensing utilization for vSTP MPS. | Enhancement Request |

## vstp event/alarm logging enhancement

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| POR 27393516 | The DSR 8.3 vSTP function implemented various Event/Alarm, Logging, measurements | Enhancement Request |

## CAPACITY INCREASE FEATURE

|  |  |  |
| --- | --- | --- |
| Name | Description | Scope |
| POR/ebug: 27140375  ebug: 27579837, 27723029 and 22152700 | * This feature support for more than 32 DA-MPs or vSTP MPs per SOAM   Note: Testing of increased system capacities (such as 500k MPS DSR) will be a later feature.   * ARR has been increased to 50K and ART has been increased to 1.5K. * PRT rules within the NE have been increased to 50000. * Diameter Connection per System support 32000. | Bug Fix & Enhancement Request |



## hardware Changes

* + 1. **Hardware Supported**

|  |  |
| --- | --- |
| **Hardware** | **Comment** |
| HP BL460c Gen8, Gen8\_v2 | c-Class |
| HP BL460c Gen9, Gen9\_v2 | c-Class |
| HP DL360/380 Gen8, Gen8\_v2 | Rack Mount Server |
| HP DL380 Gen9, Gen9\_v2 | Rack Mount Server |
| Oracle Server X5-2 | Rack Mount Server |
| Oracle Server X6-2 | Rack Mount Server |
| Oracle Server X7-2 | Rack Mount Server |
| Netra X5-2 | Rack Mount Server |
| HP 6125XLG, 6125G, 6120XG | Enclosure Switch |
| Cisco 3020 | Enclosure Switch |
| Cisco 4948E-F | Rack Switch |
| Cisco 4948E | Rack Switch |

Note:

Gen9, Gen9 v2 and Gen 8 v2 hardware are also supported, when purchased by a customer.

Mixed Sun/HP deployments are not generally supported.

## software Changes

Software changes include a new release of the software Platform components, and new DSR release.

|  |  |
| --- | --- |
| Component | Release |
| TPD 64 Bit | 7.6.0.0.0-88.54.0 |
| COMCOL | 7.5.0.3.0-14027 |
| PM&C | **6.6.0.0.0-66.8.0** |
| TVOE | 3.6.0.0.0-88.54.0 |
| AppWorks | 8.3.0-83.15.0 |
| EXGSTACK | 8.3.0-83.14.0 |
| HP Firmware FUP | 2.2.12 (Minimum[[1]](#footnote-1)) |
| Oracle Firmware | 3.1.8 (Minimum[[2]](#footnote-2)) |

* + 1. **DSR Release 8.3**

DSR Release 8.3 inherits all functionality from DSR 8.2

|  |  |
| --- | --- |
| Component | Release |
| DSR Release | 8.3 |

DSR 8.3 is compatible with TPD 7.6, ComCOL 7.5, AppWorks 8.3, EXGSTACK 8.3, TVOE 3.6 and PM&C 6.6.

* + 1. **iDIH 8.2.1**

|  |  |
| --- | --- |
| Component | Release |
| IDH Release | 8.2.1 |

DSR 8.3 is compatible with IDIH 7.3, 8.0, 8.1, 8.2 and 8.2.1

* + 1. **SDS 8.3**

|  |  |
| --- | --- |
| Component | Release |
| SDS Release | 8.3 |

DSR 8.3 is compatible with SDS 7.3, 8.0, 8.1, 8.2 and 8.3

NOTE**:** It is recommended for SDS to be upgraded before the DSR. SDS release 8.3 is compatible with DSR releases 7.3, 8.0, 8.1, 8.2 and 8.3

## firmware Changes

Firmware release guidance is provided via DSR 8.3 Release Notice which can be found at the following link:

<http://docs.oracle.com/en/industries/communications/diameter-signaling-router/index.html>

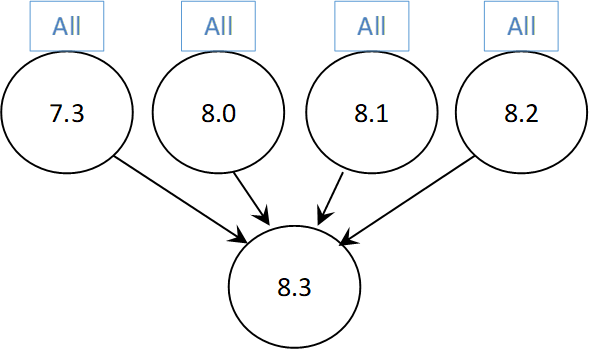
and then navigating to the Release 8.3.x link.

## upgrade Overview

This section provides an overview of the Upgrade activities for Release 8.3.

* + 1. **DSR Upgrade Path**

The supported upgrade paths for DSR 8.3 are:

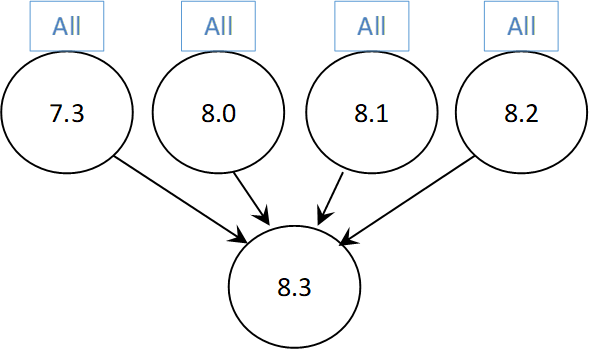


***All in the figure above refers to the available releases and all of its maintenance releases***

***Figure 1 – DSR Upgrade Paths***

* + 1. **The supported upgrade paths for SDS 8.3 are:**

The supported upgrade paths for SDS 8.3 are



***All in the figure above refers to the available releases and all of its maintenance releases***

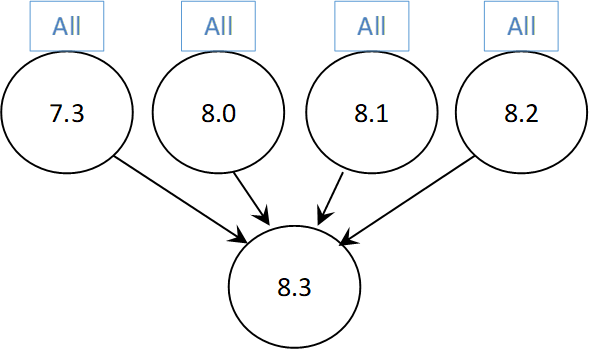
***Figure 2 – SDS Upgrade Paths***

|  |  |  |
| --- | --- | --- |
| MCj04113060000[1] | **!!Caution!!** | SDS Upgrade  If the customer deployment has only FABR features enabled, it is recommended to upgrade the SDS nodes first before upgrading the DSR nodes.  If the customer deployment has both the FABR and PCA features enabled, then upgrade the DSR nodes first before upgrading the SDS nodes. |

.

* + 1. **The supported upgrade paths for iDIH 8.2.1 are:**

The supported upgrade paths for iDIH 8.2.1 are



***All in the figure above refers to the available releases and all of its maintenance releases***

***Figure 3 – IDIH Upgrade Paths***

iDIH upgrade can be scheduled prior to or following the DSR upgrade. If iDIH upgrade is deferred until after DSR upgrades, then any newly captured elements existing within the upgraded DSR will not be decoded by iDIH until after the iDIH upgrade.

* + 1. **Upgrade Execution**

With DSR 8.3, there are multiple methods available for upgrading a site. The newest and most efficient way to upgrade a site is the Automated Site Upgrade feature. As the name implies, this feature will upgrade an entire site (SOAMs and all C-level servers) with a minimum of user interaction. Once the upgrade is initiated, the upgrade will automatically prepare the server(s), perform the upgrade, and then sequence to the next server or group of servers until all servers in the site are upgraded. The server upgrades are sequenced in a manner that preserves data integrity and processing capacity. Release 8.3 now delivers Auto Site Upgrade for the SDS.

Automated Site Upgrade can be used to upgrade the DSR/SDS servers. However, Auto Site Upgrade cannot be used to upgrade PMAC, TVOE, or IDIH servers at a site.

Additionally, there are separate procedures described in the upgrade procedures to support either a manual or automated approach to upgrading any particular server group. When planning upgrades the “Site Upgrade Methodology Selection” section of the upgrade procedure should be carefully reviewed. ***The use of the automated methods (Auto Site or Auto Server Group) for DA-MP server groups should be carefully considered regarding potential negative traffic impacts***. The ASU enhancement in DSR 8.3 resolves this issue. The user is now instructed to rearrange/add cycles to create a suitable upgrade plan.

* + 1. **Limitations**

When AppEventLog file is full then SOAM/NOAM becomes unstable and shown undefined behavior like:

1. Replication and merging stopped.

2. GUI access stops working.

Also please note that upgrade will fail if utilization of /var/TKLC/rundb partition is more than 70% which may be true in case of larger AppEventLog file size (~5.5 GB in size). To prevent the above listed issues, we need to assign/allocate /var/TKLC/rundb size and AppEventLog file size in sync i.e. AppEventLog file size (plus some delta for other files like MeasStat) should be always less than 70 % of /var/TKLC/rundb partition size.

## migration of DSR Data

As in prior releases, the existing DSR Data will be preserved during the upgrade.

# Feature OAM Changes

At the time of upgrade to DSR 8.3, a number of features and enhancements will become visible on the interfaces to the DSR and may change certain existing OAM behaviors of the system.

OAM changes include: User Interfaces (NO GUI, SO GUI), Measurements Reports, Alarms, and KPIs.

Note: this section covers OAM changes that will be visible after upgrade to the 8.3 release and does not include changes that will be seen only as new Optional Features are activated on the system (post-upgrade activity, and customer specific).

## AVP Removal FEATURE

#### Description

The purpose of this feature is to avoid

* DoS attacks using DRMP and NGN-PS AVPs when either NGN-PS or DRMP Admin State is enabled and “*Ignore Priority From Peer*” is enabled for given peer.
* Message priority assignment using DRMP and NGN-PS AVP’s which are used internally to throttle messages during congestion.

#### Overview

The feature enhances DCL logic to avoid the message priority assignment using DRMP and NGN-PS AVP’s based on the new configuration provided from GUI.

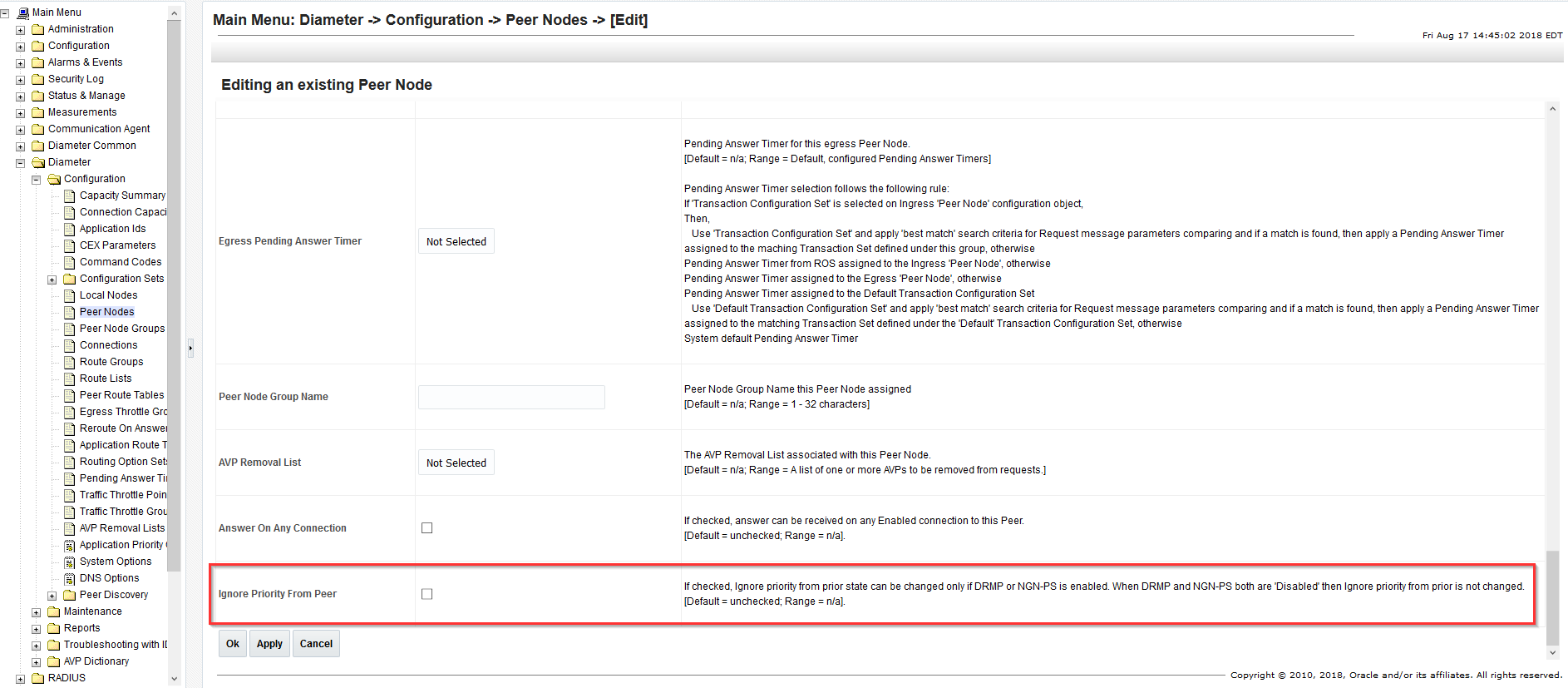
#### GUI Changes

**3.1.3.1 Diameter Peer Nodes Screen** *(Main Menu > Diameter > Configuration > Peer Nodes > [Edit])*

DSR GUI allow user to enable/disable the field “*Ignore Priority From Peer*” on Site/SOAM level (the default behavior is “Disabled”)

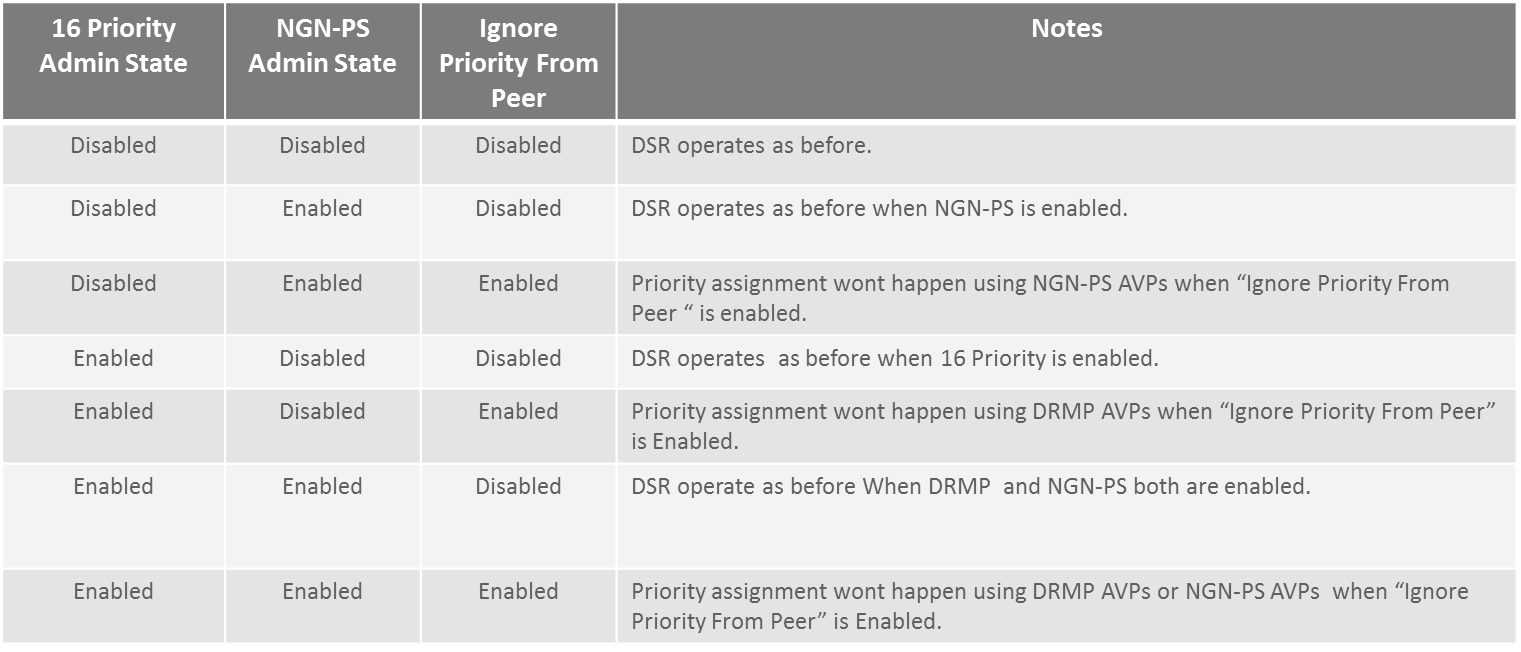
Note: To enable this new field “*Ignore Priority From Peer* “either DRMP Admin or NGN-PS admin state should be enabled (Main Menu: Diameter -> Configuration -> System Options -> Priority Options -> NGN-PS Admin State or 16 Priority Admin State) .

DSR GUI will throw error when user try to enable the field “*Ignore Priority From Peer*” without either DRMP or NGN-PS Admin state enabled. [Error Code 19051] - Ignore priority from peer cannot be changed as DRMP & NGN-PS features are both disabled.



#### Behavior

Based on new field configuration, the following table show how the DSR operates using 16 Priority and NGN-PS feature.

****

## vEIR (Diameter & VSTP)

* + 1. Diameter EIR

This feature support Equipment Identity Register functionality in DSR 8.3 (Diameter & vSTP) based.

**3.3.1.1 Solution**

EIR solution enables comparing of the IMEI provided during handset registration against a set of lists provided by the network operator. There will be three lists Black, Gray and White. User Equipment (UE) on the White & Grey list shall be allowed access to the network. UEs on the black list shall be denied to access the network.

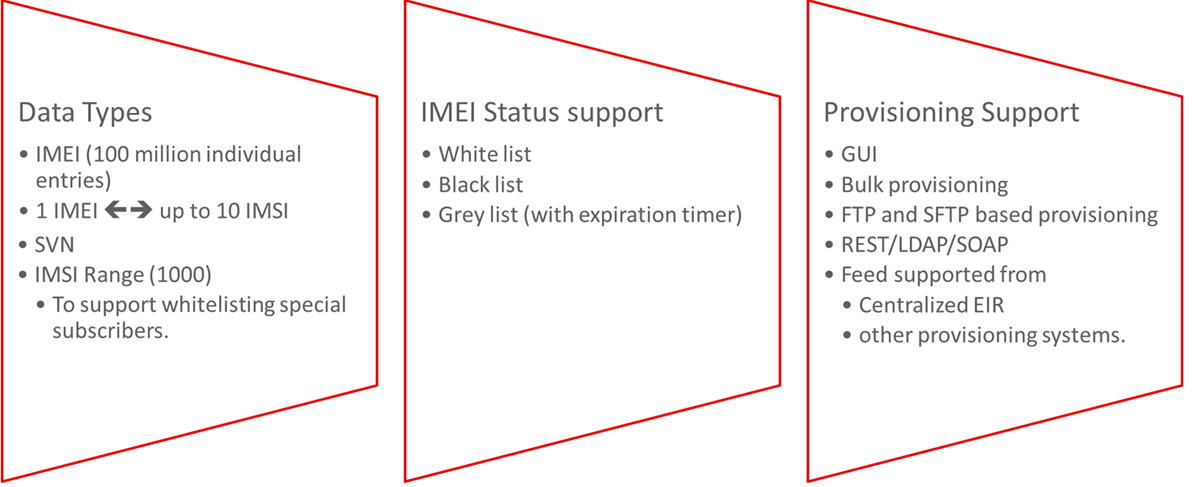
The Solution also allows the operator to enable IMSI based screening prior to the IMEI lookup. If IMSI in ECR message matches with one of the configured IMSI, special handling is performed for corresponding IMEIs.

**3.3.1.2 Feature Overview**

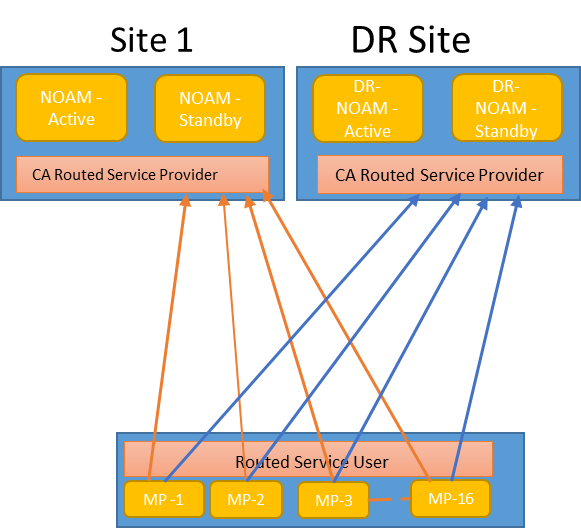
*Equipment Identity Database:*

EIR uses OCUDR as off board database to store equipment identity. OCUDR NOAM shall be deployed as A level server. DSR NOAM and OCUDR NOAM shall be deployed in different topology.

IMEI and IMSI user database provisioning shall be done on the OCUDR. SOAP, REST, Bulk Import interface shall be used for provisioning. Multiple sites DAMP of DSR can connect to OCUDR NOAM to query the equipment status.



DA-MP will establish ComAgent (CA) connections with both Active and Standby UDR NOAM. OCUDR NOAM’s will be configured as routed service providers. DA-MP’s will act as routed service users.

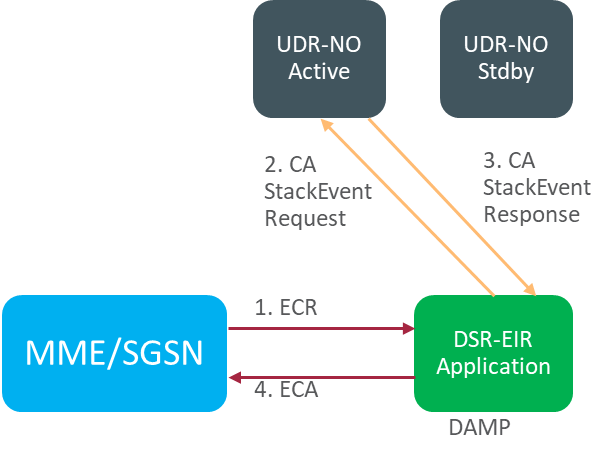


Note:

The Customer need to add ComAgent connections to connection group manually. DAMP’s in Site-1 shall route the traffic in round robin manner to all the connections in “UDRSvcGroup”.

If due to any reason connection to 1 NOAM goes down or gets congested CA will route the messages to other NOAMs.

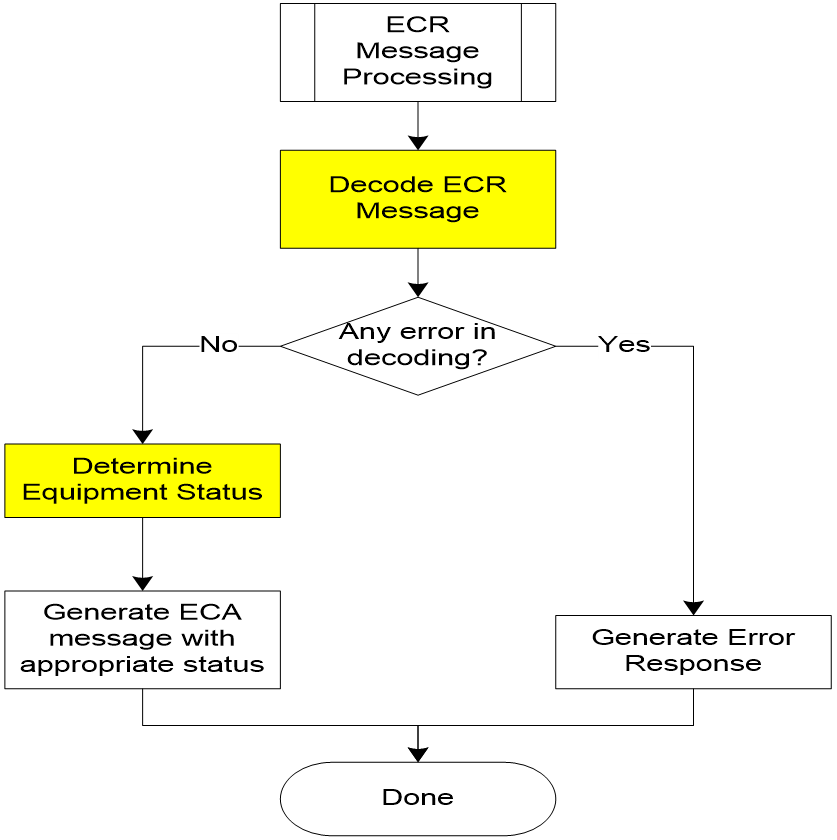
*Equipment Identity Message Handling:*

1. MME/SGSN will send ECR message to DSR over diameter connection. 

2. DAMP will query the UDR Active and standby NOAM in round-robin fashion for IMEI status. DAMP will use CA for querying the UDR DB.

3. UDR NOAM will look up IMEI DB and will send response to the DAMP. Response to DAMP will be sent using CA.

4. EIR application on DAMP will receive the response from UDR and create ECA message, encode it and send to MME/SGSN.

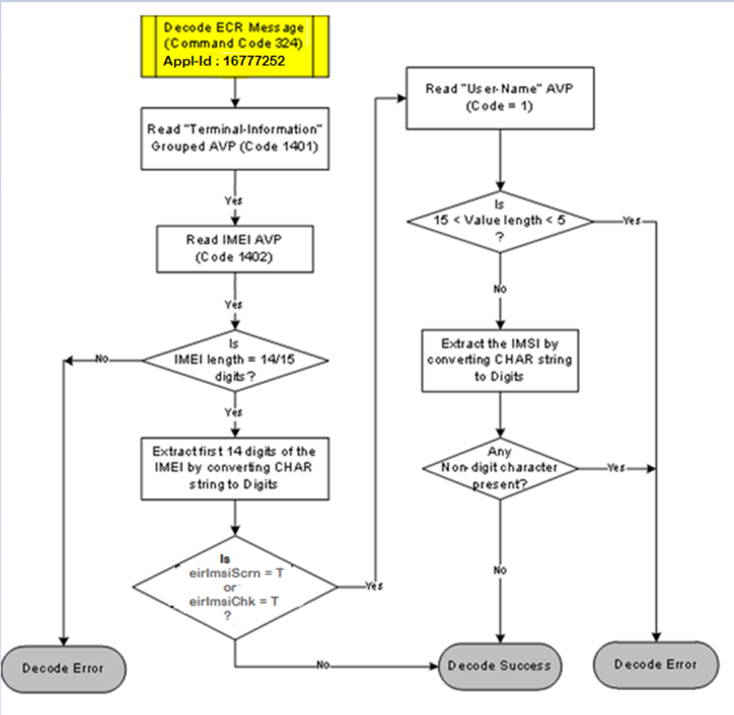


1. EIR will receive ECR message.

2. EIR will decode the message. If decoding is successful, then EIR try to determine the equipment status

3. If decoding fails, based on the decode error, response is determined and sent.

4. If equipment status is successfully determined then EIR will send ECA

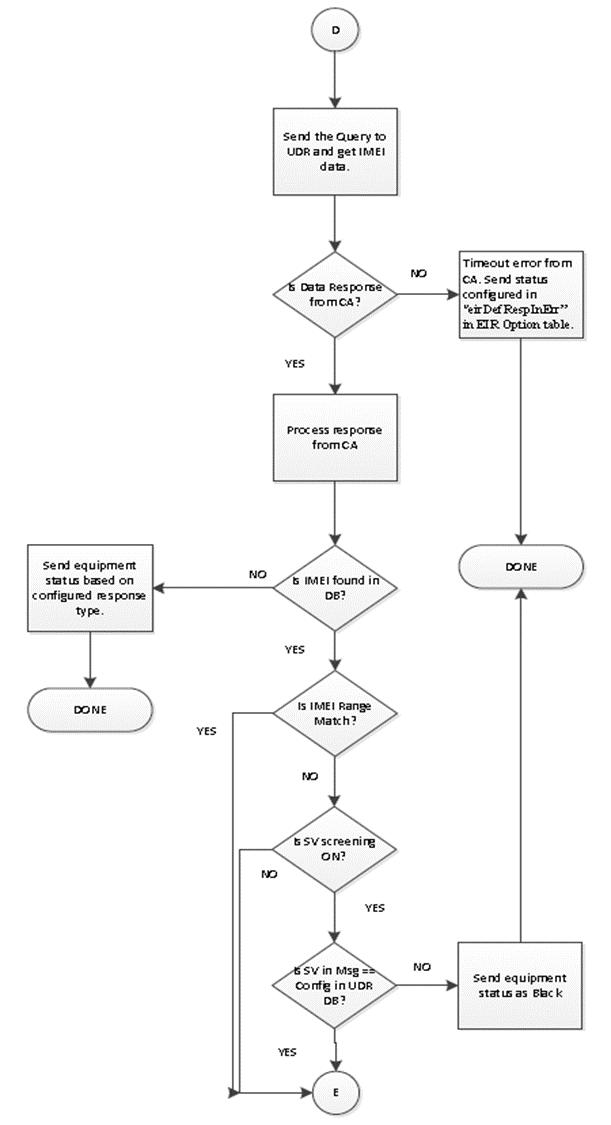


*Decoding IMEI and IMSI*

EIR will check the application ID in the received message. It should be 16777252. If not, processing of ECR message is stopped, ECA with error result code 3007 will be sent out and measurement DeirInvalidAppId will be pegged.

EIR doesn’t validate the vendor id for the incoming message (ECR).

For decode error, ECA with corresponding error code will be sent out. EIR will comply with error codes mentioned in RFC 6733.

*UDR query response handling:*

1. IMEI look up request event will be sent to UDR. UDR will look up the received IMEI for exact match, if not found UDR will look up for range match.

2. If UDR sends successful data event response then IMEI equipment status will be used from response stack event.

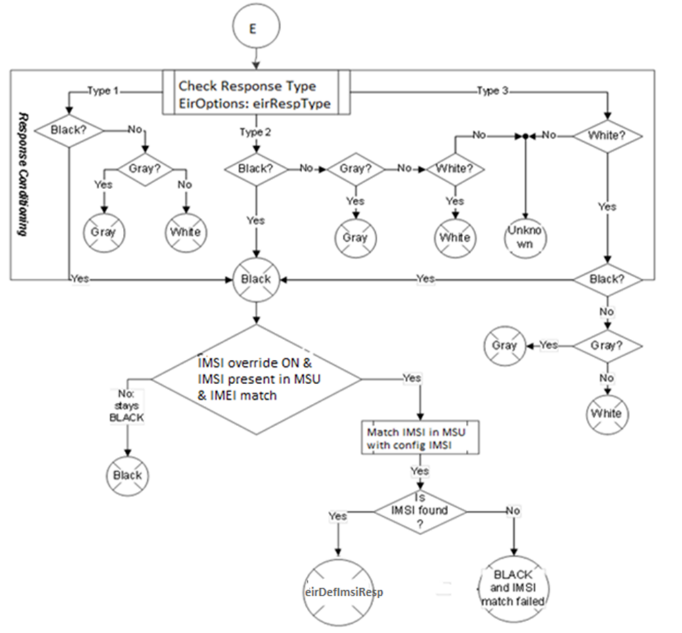
3. In case of stack event timeout default response option (eirDefRespInErr) value from EirOptions table will be used as equipment status.

4. If IMEI in ECR doesn’t found by UDR in IMEI exact match and IMEI Range match, send the equipment status based on the response type. Response type will decide the equipment status needs to be sent in case of unknown IMEI.

5. If IMEI in ECR found in UDR through IMEI exact match and SV check is enabled, then SV is checked.

6. UDR will send default SV 99 in case of IMEI range match. If IMEI in ECR found in UDR through IMEI range match, then SV check will be skipped at DSR.

7. In case of SV check, if SV received in message does not match with configured in DB then ECA will be sent with equipment status as Black. If SV matches equipment status will be determined after response conditioning.



*IMSI override check:*

For every IMEI table we will have max 10 IMSI mapped in UDR DB.

In response to the UDR DB query we will get all the IMSI mapped to IMEI.

If eirImsiChk (IMSI override check) is enabled, and IMEI is Black listed,

IMSI lookup will happen.

If IMSI in msg found in IMSI list from UDR. Status will be changed

to white list from black list. Otherwise status will not be changed.

IMSI override functionality will be skipped in case of IMEI range match at UDR.

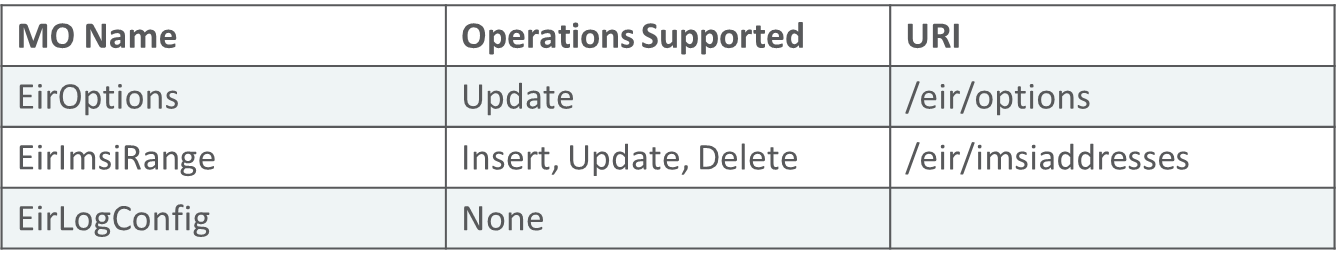
*Equipment status determination logic based on Response Type:*

Equipment status determination logic based on Response Type

* This table shows the equipment status result based on response type and status flags.
* In case of IMEI is not found in the UDR DB. We will send the status in EIR based of response type.

**3.3.1.3 MOs and Operation Supported**

Following is the list of MO’s and operation supported for EIR features.

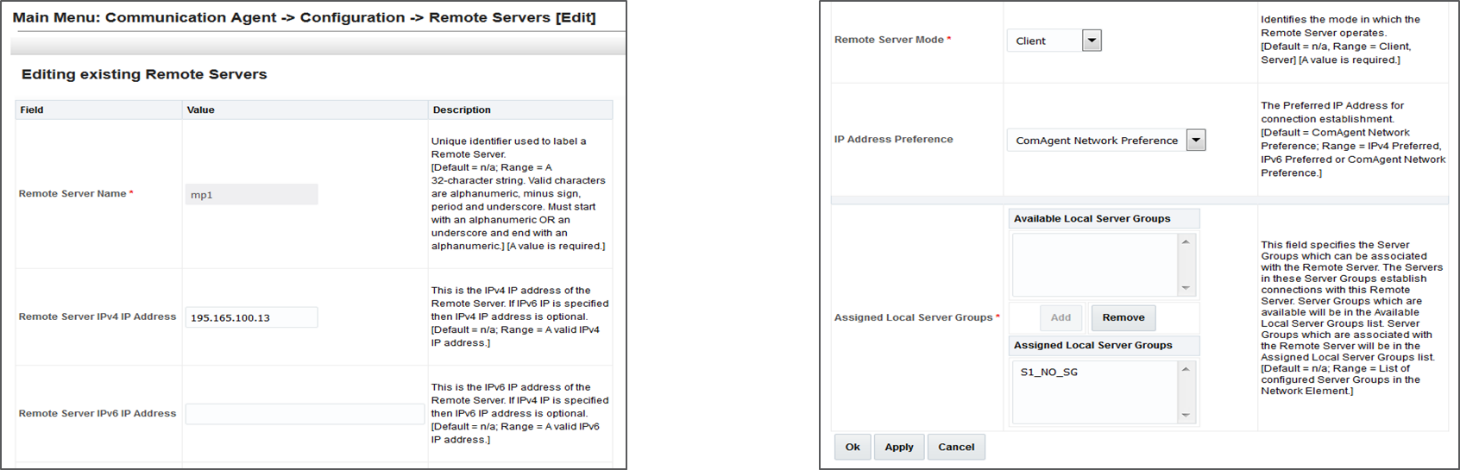


Refer MMI API Guide on Active NOAM/SOAM: “Main Menu ->MMI API Guide” on any DSR 8.3 GA release setup for details about the URI, example and parameters about each MO.

**3.3.1.4 Configuration: GUI Changes**

***Configuration: OCUDR – Add DAMP(s) on OCUDR***

Add details of DAMP in the ComAgent Remote Servers screen as client at " Main Menu: Communication Agent 🡪 Configuration 🡪 Remote Servers [Insert] " on Active OCUDR NOAMP. Select OCUDR server group from “Available Local Server Groups” which needs to communicate with DAMP.

******

On Active OCUDR GUI "Main Menu: Communication Agent 🡪 Maintenance 🡪 Connection Status" screen, verify that connections are "InService".

On Active OCUDR GUI "Main Menu: Communication Agent 🡪 Maintenance 🡪 Routed Services Status" screen, verify that DRADbSvc status is "Normal“

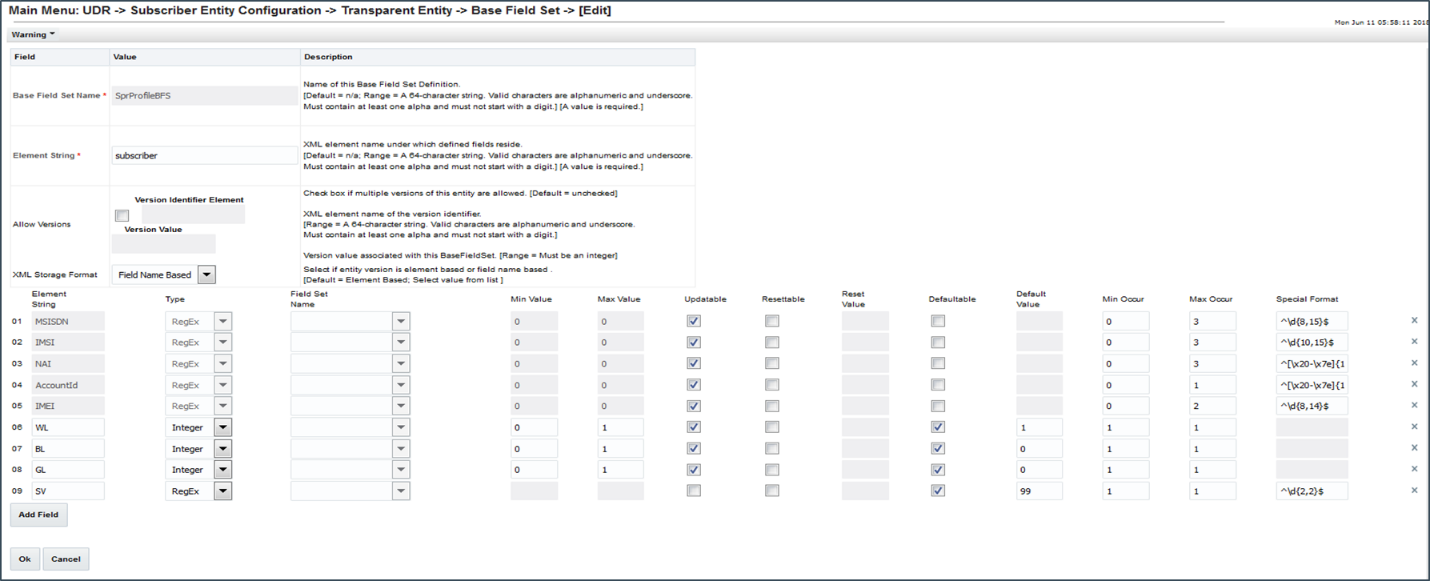
***Configuration: How to create subscribers on OCUDR?***

On Active NOAMP GUI, delete the non-required fields and add the required fields for EIR subscriber profile.

The values of the different options for profile fields should be configured as follows:

* WL stands for White List, which is of type INT with min value of 0 and max value of 1. Min occurrence of 1 and Max occurrence of 1.The default value is 1.
* GL stands for Grey List, which is of type INT with min value of 0 and max value of 1. Min occurrence of 1 and Max occurrence of 1. The default value is 0.
* BL stands for Black List, which is of type INT with min value of 0 and max value of 1. Min occurrence of 1 and Max occurrence of 1. The default value is 0.
* SV stands for Software Version. Which is a numeric string of length 2 - Min occurrence of 1 and Max occurrence of 1. default value is '99'

EIR profile fields should look like as shown in the snapshot below:



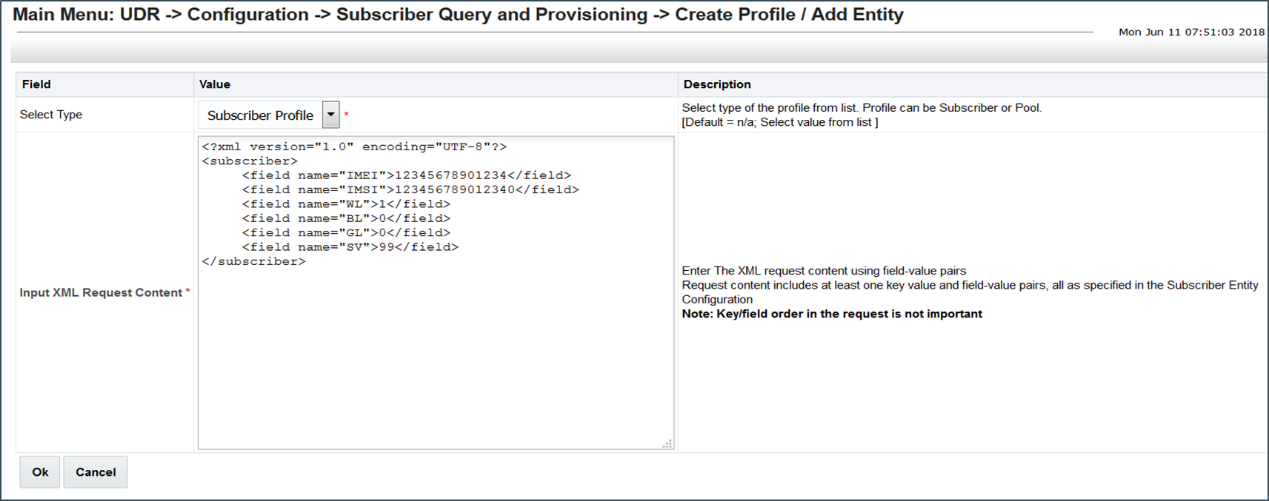
By default, provisioning is disabled on OCUDR. We need to browse “Main Menu: UDR 🡪 Configuration 🡪 Provisioning Options” on NOAMP GUI and:

Check “Allow SOAP Connections”.

Check “Allow REST Connections”

Click on “Apply” button.

A sample request for “create subscriber” can be executed from active NOAMP GUI: Main Menu: UDR 🡪 Configuration 🡪 Subscriber Query and Provisioning.

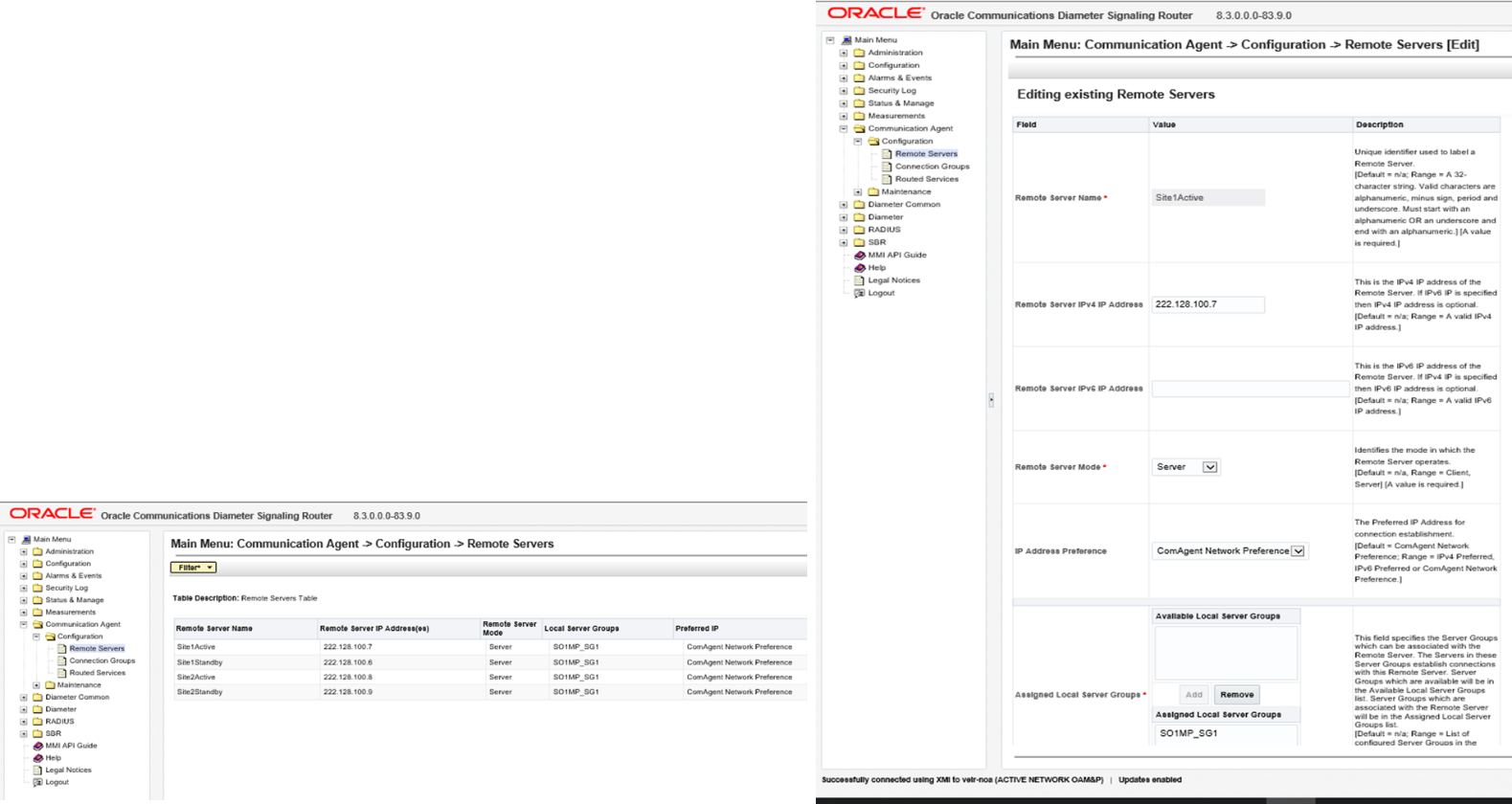


***Configuration: UDR Configuration in DSR***

*Assumption*:

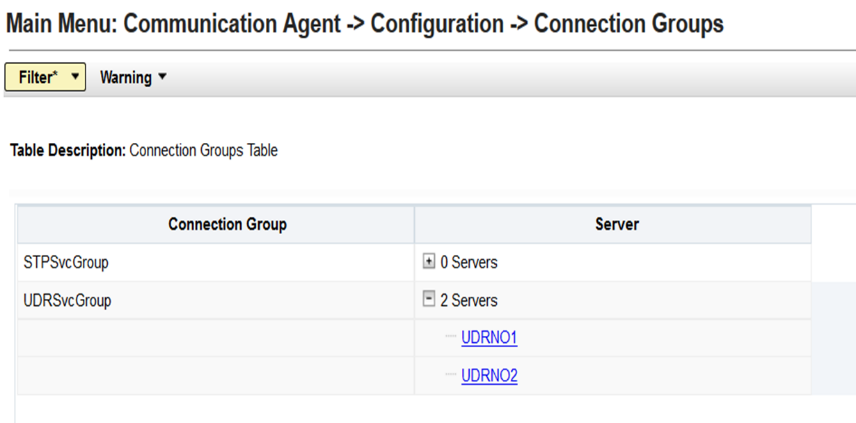
User is aware of UDR and ComAgent functionality

UDR is already installed and UDR topology is already configured.

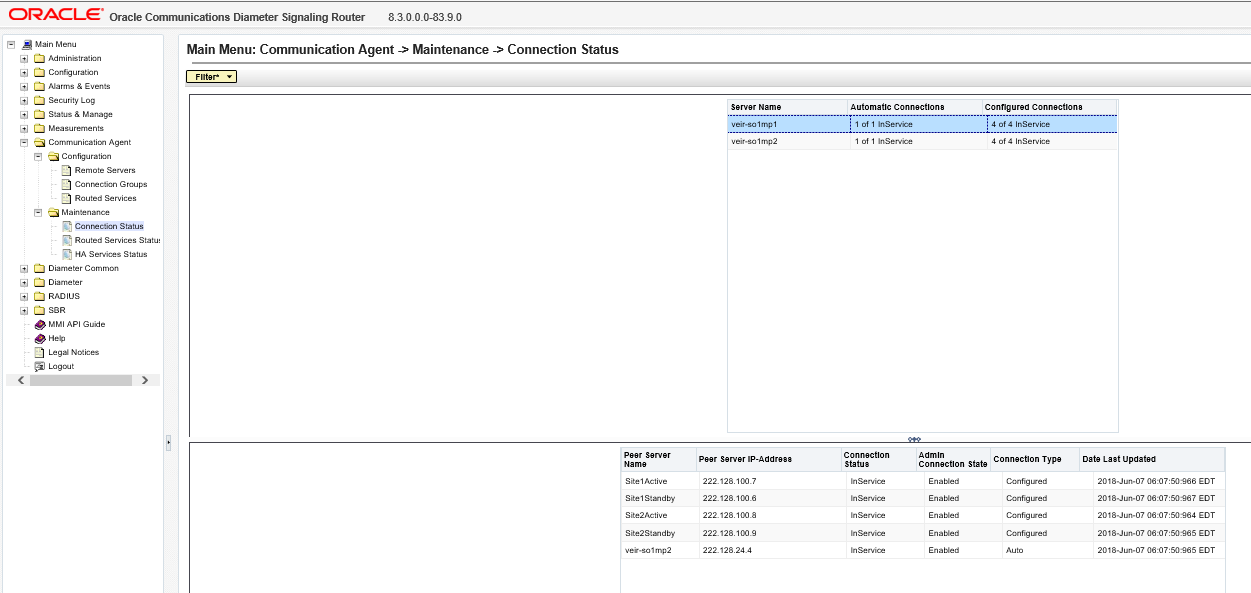


***Steps*:**

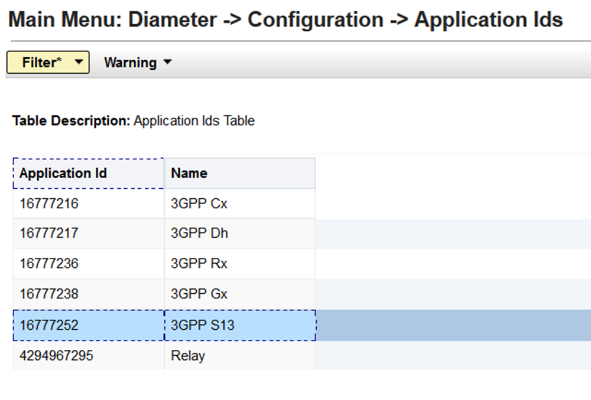
1. On Active DSR NOAM, Go to " Main Menu: Communication Agent 🡪 Configuration 🡪 Remote Servers [Insert] "
2. Add UDR NO IP in the ComAgent Remote Server screen as Server. Select DAMP server group in Local SG which needs to communicate with UDR
3. Add similarly Stdby, DRNO's
4. Go to "Main Menu: Communication Agent -> Configuration -> Connection Groups" screen. Select “UDRSvcGroup" and click on "Edit".
5. Add all available UDR NO servers.



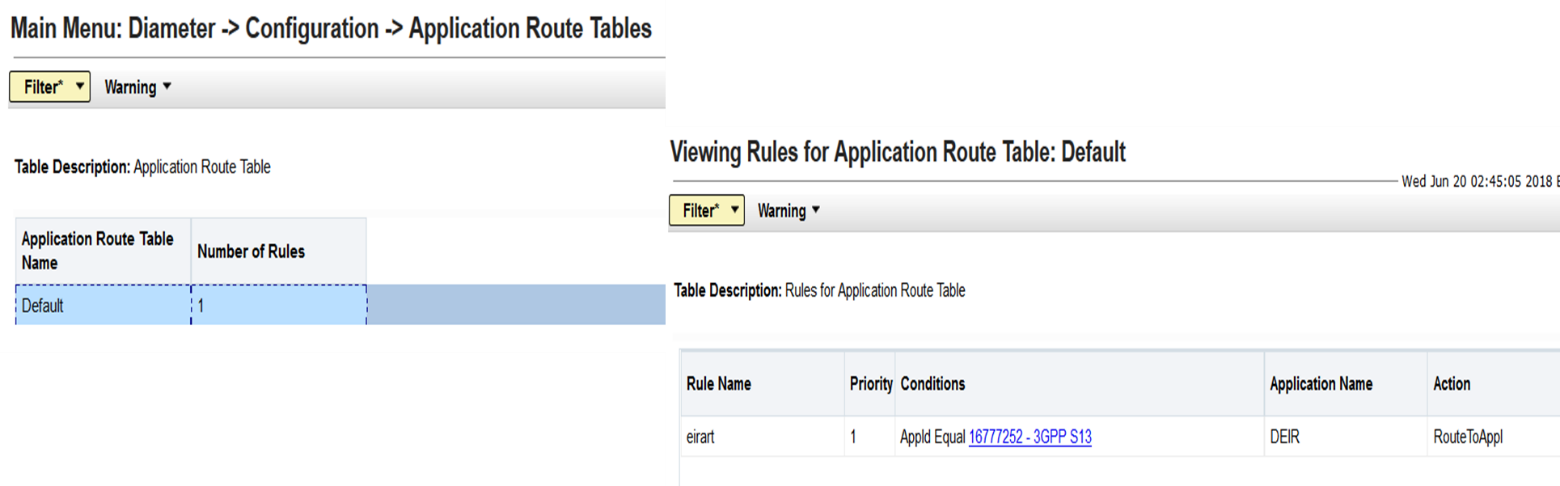
1. Go to "Main Menu: Communication Agent 🡪 Maintenance 🡪 Connection Status" screen. Select Server name to check the connection status



1. Go to " Main Menu: Diameter 🡪 Configuration 🡪 Application Ids" screen on active SOAM. Click insert and add S13 interface application id.



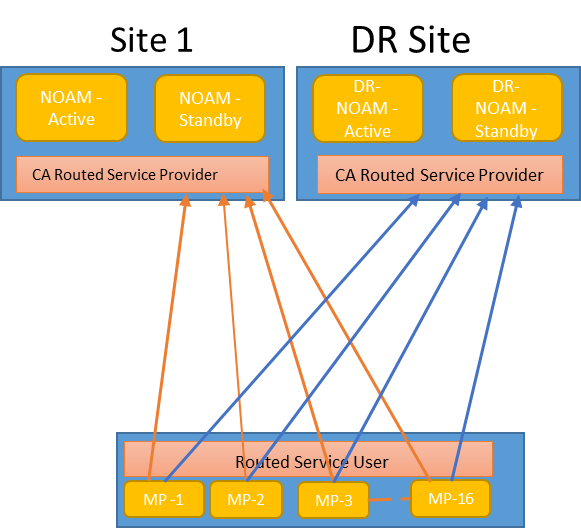
1. Go to " Main Menu: Diameter -> Configuration -> Application Route Tables" screen and insert the new ART or add a rule in existing ART.



#### vSTP EIR

This EIR provides vSTP the ability to query Mobile Station’s Identity from a designated repository provisioned by the network operator. This enables the operator to block stolen Mobile Stations from accessing the network. Querying the Mobile Station Identity and methods to decide final equipment status are configurable.

**3.3.3.1 Feature Overview**

**vSTP MP Connectivity with Equipment Identity Database: **

vSTP-MP shall establish ComAgent (CA) connections with both Active and Standby UDR NOAM.

OCUDR NOAM’s shall be configured as routed service providers.

vSTP-MP’s shall act as routed service users.

Pre-configured connection groups “STPSvcGroup” shall be used for Routed Service.

Connection Group “STPSvcGroup” shall have connections to both Primary and Secondary site NOAM’s.

Note: Customer need to add ComAgent connections to connection group manually.

vSTP-MP’s in Site-1 shall route the traffic in round robin manner to all the connections in “STPSvcGroup”.

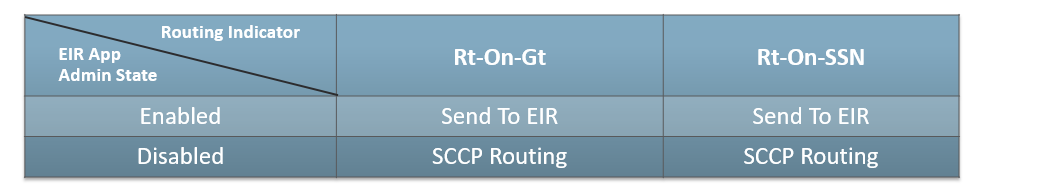
If due to any reason connection to 1 NOAM goes down or gets congested CA will route the messages to other NOAMs.

**vSTP EIR Application Administration:**

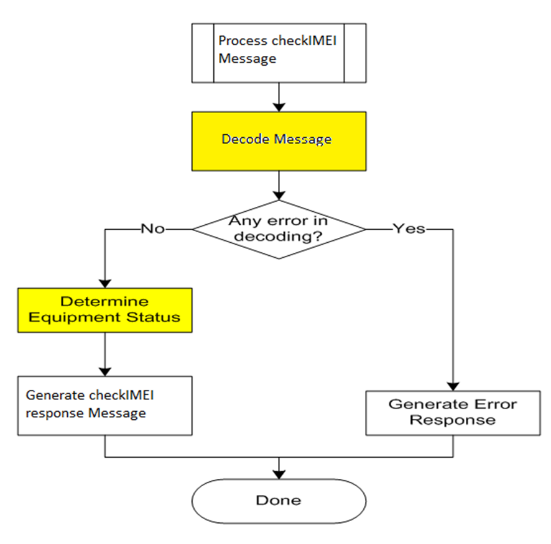
* EIR application is disabled by default and assigned SSN value as “9”.
* User/Customer will not be able to directly add/modify or perform admin action on this table.
* In order to allow customers to enable EIR Application, a command line tool is provided to modify application Admin state
* This tool can be executed only from Active SOAM
* Customer can additionally modify the SSN value also (if required)
* Customer need to change the application state to “Enabled” to run EIR service on vSTP

**vSTP EIR Message Handling:**

* New Local subsystem Stack Layer (LSS) is developed to host EIR application
* MSC sends CheckIMEI request to vSTP-MP over SS7 links. SCCP layer decodes the message and sends to EIR Application if the following conditions are met
  + Message CdPA SSN matches with configured EIR SSN
  + EIR Application is Enabled
* If CdPA SSN does not match with configured EIR SSN or EIR Application is disabled, the message is sent to SCCP for GTT
* Following table explains message handling for RI set to Rt-On-Gt & Rt-On-SSN with following considerations
  + configured EIR SSN value in vSTP = 9
  + Ingress Message CDPA SSN is 9



* EIR application will support only following signaling standards
  + ANSI
  + ITU-I
  + ITU-N
* TCAP message must be of TC-BEGIN with invoke component, and the MAP Op-Code must be CheckIMEI.
  + Return Result – If IMEI look up result(black/gray/white) in success
  + Return Error – If decoding of some parameter fails or look up fails
  + Reject – If component decoding fails.
  + U-Abort – If decoding Transaction portion fails.
  + P-Abort – If decoding fails for certain decode errors in the dialog or component portion.
* MAP version will be decoded from Dialog portion’s ACN. vSTP will support MAP version 1, 2 and 3.
* If Dialog portion is not present the Default MAP version will be used to decode TCAP parameters.
* Default MAP version will be configurable through MMI.



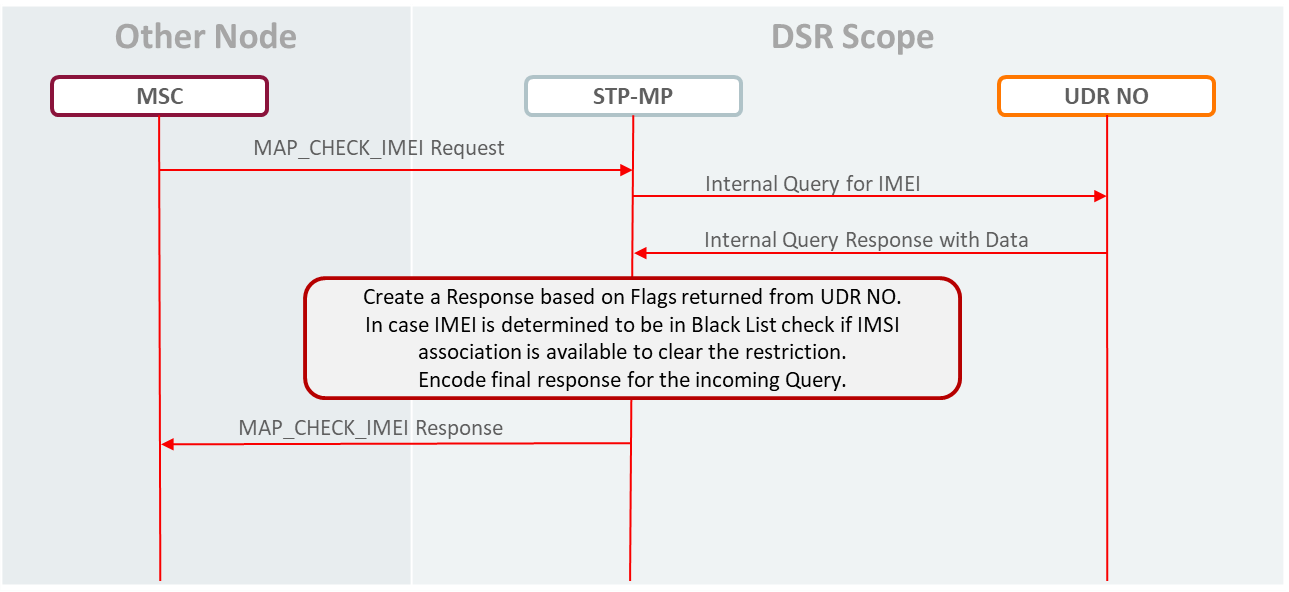
EIR will receive checkIMEI message.

EIR will decode the message. If decoding is successful, then EIR try to determine the equipment status

If decoding fails, based on the decode error, response is determined and sent.

If equipment status is successfully determined, then EIR will send checkIMEI response.

**SS7 EIR Call Flow:**

****

**EIR IMSI Decoding:**

* IMSI is not part of checkIMEI message but to provide support for IMSI check different vendors have opted for different IMSI encoding scheme.
* Following MSC vendor IMSI encoding scheme will be supported by
  + Ericson
  + Alcatel
  + Vimplecom

**Ericsson IMSI Encoding:**

* In order to include the IMSI in the message, Ericsson has modified the message from the standard format in [6]. Instead of a single parameter, there is a parameter sequence with IMEI and optional IMSI.
* The ASN.1 format Ericsson uses is:
* IMEI OCTET STRING (8)
* IMSI OCTET STRING (3..8)

PARAMETER SEQUENCE {

imei IMEI

imsi (PRIVATE 1) IMSI OPTIONAL

}

* This format will be identified by checking for the presence of the Parameter Set tag stored by the generic decoder. If the Parameter Set Tag is detected, then IMEI is identified by Tag ID h’4 and IMSI (optional) is identified by Tag h’1. The IMEI is 8 bytes in length. The first 7 bytes compose the value that will be searched in the database, and the last byte is software version.
* The IMSI is 3 to 8 bytes in length. The entire data will be used. It will be assumed to be International E.212 format.

**Alcatel IMSI Encoding:**

* Alcatel encodes the IMSI in the dialog portion destination reference field. The destination reference field is a generic information location that can carry implementation dependent data. There no other specified use for destination reference in a CheckIMEI message, so the storage of the IMSI is acceptable.
* If the IMEI is a located as a single parameter in the component portion (thus, not the Ericsson/Vimplecom format), the dialog portion will be searched for IMSI. Since Phase 1 does not contain a Dialog portion, this only applies to Phase 2 and Phase 2+ messages. The IMSI, based on the decoded NAI, will be conditioned to International format. If the NP is not 6 (E.212), then the digit information will be ignored.

**VimpleCom IMSI Encoding:**

* In order to include the IMSI in the message, Vimplecom has modified the message from the standard format. Instead of a single parameter, there is a parameter sequence with IMEI and optional IMSI.
* The ASN.1 format Ericsson uses is:
* IMEI OCTET STRING (8)
* IMSI OCTET STRING (3..8)

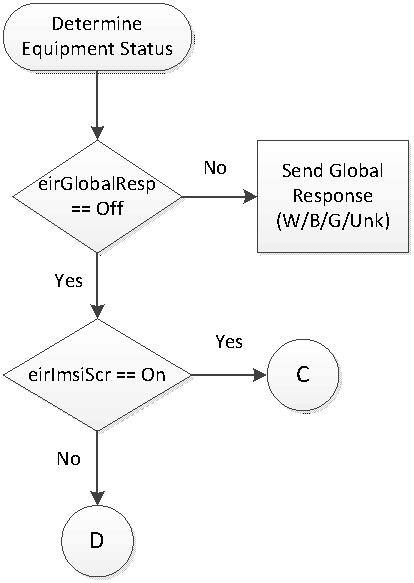
PARAMETER SEQUENCE {

imei IMEI

imsi (PRIVATE 1) IMSI OPTIONAL

}

* This format will be identified by checking for the presence of the Parameter Set tag stored by the generic decoder. If the Parameter Set Tag is detected, then IMEI is identified by Tag ID h’4 and IMSI (optional) is identified by Tag h’0. The IMEI is 8 bytes in length. The first 7 bytes compose the value that will be searched in the database, and the last byte is software version.
* The IMSI is 3 to 8 bytes in length. The entire data will be used. It will be assumed to be International E.212 format.

**EIR Determination of Equipment Status:**

🡪EIR will provide option in EirOptions table to configure global response type (eirGlobalResp). If this option is set, then based on value set in this option checkIMEI response is sent to the MSC.

🡪By default, global response will be set to Off.

🡪If Global response set to Off following Order will be used to determine the equipment status

IMSI range screening

IMEI and IMEI Range screening

SV Screening – Last 2 digits of IMEI will be used for software version

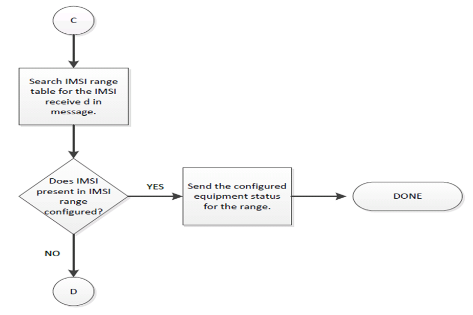
IMSI exact match

🡪If “IMSI Screening” option is set to “On” in EirOptions table then IMSI will be decoded and searched in the IMSI range table.

🡪By default, “IMSI Screening” will be set to On.

🡪If match is found in the IMSI range table then response will be sent based on the configured IMSI status.

🡪Wild card ranges will not be supported in this release.



**Note**: Please refer to the above Page # 28 - Section # 3.3.1.2 for the details on the following topics

*UDR query response handling:*

*IMSI override check:*

*&*

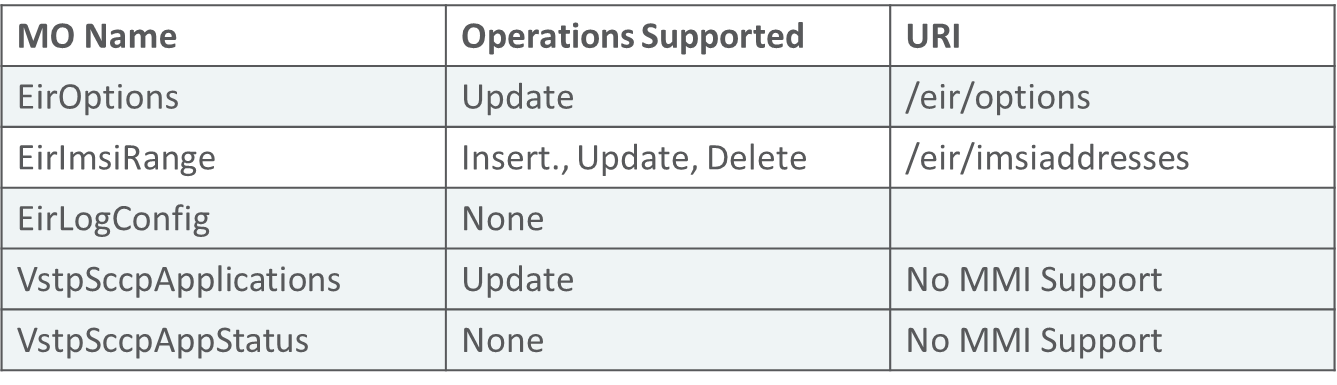
*Equipment status determination logic based on Response Type:*

**EIR Limitations:**

* EIR application will not be invoked as part of SCCP GTT translation
* SSN Management will not be implemented in this release. e.g. When process is up SSA broad cast will not be performed

#### MOs and Operation Supported

Following is the list of MO’s and operation supported for vSTP EIR feature



Refer MMI API Guide on Active NOAM/SOAM: “Main Menu 🡪 MMI API Guide” on any DSR 8.3 GA release setup for details about the URI, example and parameters about each MO.

**VstpSccpApplications:**

* This table holds entry for SCCP Applications.
* One default entry is present in this table for EIR Application as shown below:

#!/bin/sh

iload -ha -xU -fappId -fappName -fssn -fappAdminState VstpSccpApplications \

<<'!!!!'

1|Eir|9|Disabled

!!!!

* In this release no MMI support is there for this table, hence a script named “applicationAdmin” is provided to user to enable edit operation

[admusr@ravieir-soa1 bin]$ applicationAdmin

application name is mandatory

applicationAdmin [application\_name] [new\_admin\_state] <new\_ssn>

application\_name: Eir 🡪 Mandatory Parameter

new\_admin\_state: Enabled, Disabled 🡪 Mandatory Parameter

new\_ssn: 2-254. It is optional Parameter.🡪 Optional Parameter

* User needs to enable “appAdminState” to “Enabled” to activate EIR functionality
* Execute following command to do the same:

applicationAdmin Eir Enabled

The output of the above command is shown below:

ravieir-soa1 has Role defined as [1]

Current status is [ Active ] and Role [ 1 ]

Application admin state is updated successfully

[admusr@ravieir-soa1 bin]$ iqt VstpSccpApplications

appId appName ssn appAdminState

1 Eir 9 Enabled

* Similarly, user can change the SSN as well, but that is only allowed when “appAdminState” is set to “Disabled”

**VstpSccpAppStatus:**

* This is a status table maintained per MP to keep the operational state of the EIR Application
* The operational state is decided based on connectivity status between MP and UDR NOAM. ComAgent keeps sending service notification based on connection state and accordingly operational state is updated.
* Three operations states are supported

Available 🡨 Eir Query is sent to UDR NOAM

Unavailable 🡨 Eir Query is not sent, instead default response is sent as configured in EirOptons Table

Degraded 🡨 Eir Query is sent to UDR NOAM

* No MMI support since it is an internal Status table.
* Sample content of this table:

[admusr@ravieir-so1mp2 KD]$ iqt VstpSccpAppStatus

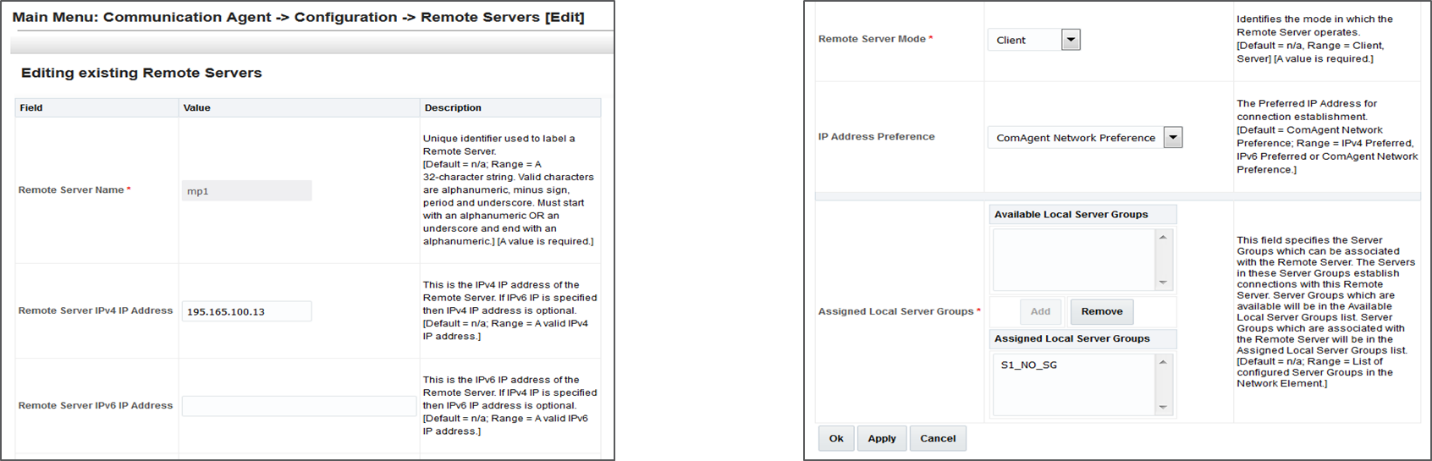
appId appName ssn appAdminState appOperState

1 Eir 9 Enabled Available

* This table can be referred for internal debugging purpose

#### Configuration: GUI (Add vSTP MP(s) on OCUDR)

Add details of vSTP MP in the ComAgent Remote Servers screen as client at " Main Menu: Communication Agent 🡪 Configuration 🡪 Remote Servers [Insert] " on Active OCUDR NOAMP. Select OCUDR server group from “Available Local Server Groups” which needs to communicate with vSTP MP.



On Active OCUDR GUI "Main Menu: Communication Agent -> Maintenance -> Connection Status" screen, verify that connections are "InService".

On Active OCUDR GUI "Main Menu: Communication Agent -> Maintenance -> Routed Services Status" screen, verify that STPDbSvc status is "Normal”

**Note**: Please refer to the above Page # 30 - Section # 3.3.1.4 for the details on the following topics

*Configuration: How to create subscribers on OCUDR?*

## SCEF

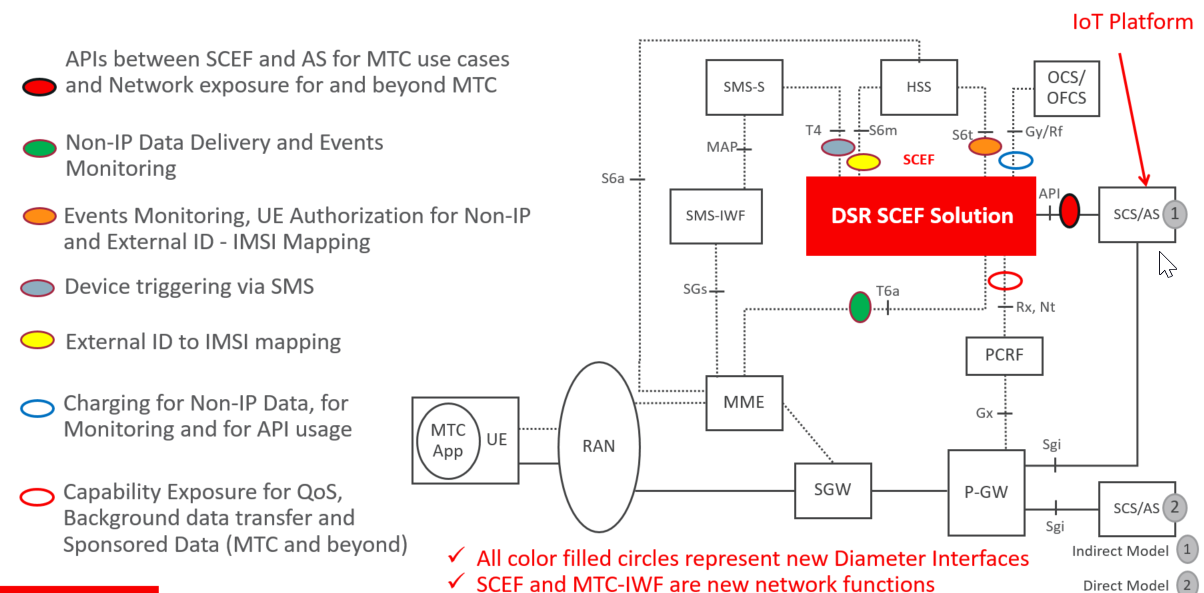
* + 1. Description

The Service Capability Exposure Function (SCEF) provides a means for the discovery of the exposed services and capabilities. The SCEF provides access to network capabilities through homogenous network application programming interfaces (e.g. Network APIs) defined over T8 interface towards SCS/AS

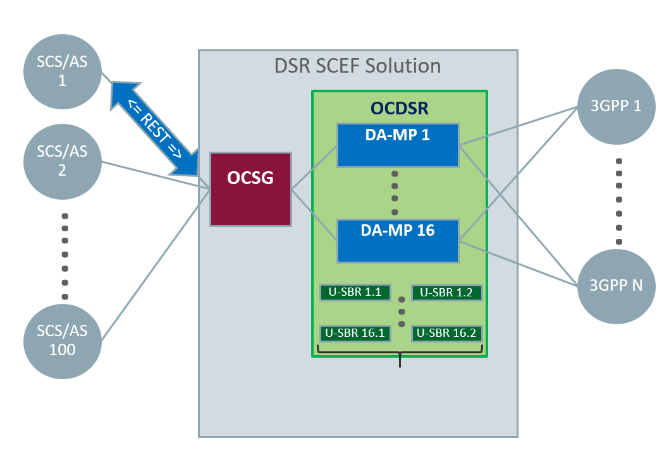
The functionalities of SCEF include:

* Non-IP data delivery for low power devices
* Monitoring a devices state
* SCS/AS AAA (Application Server authorization, accounting and SLAs)
* Device Trigger Delivery through SMS acting as an MTC-IWF
* Receiving reports about the network congestion condition of the RAN

**3GPP MTC Architecture (Oracle View):**



**DSR SCEF Solution Components:**

OCSG: Oracle Communications Services Gatekeeper (DSR API Gateway). Provides REST API to external servers, perform the following functions:

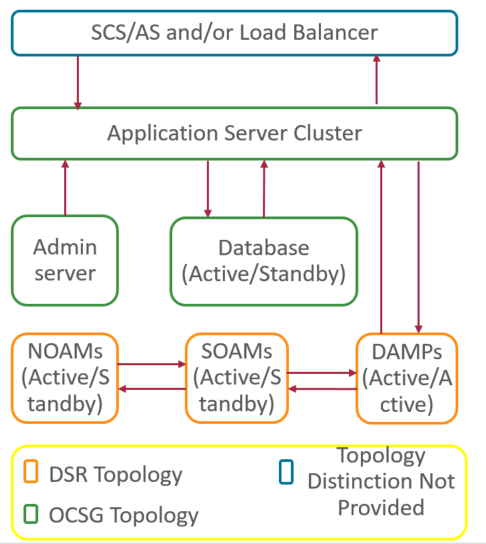
Authentication of SCS application servers

Support for API life cycle

Profile management

Quota and Rate management

Load balance HTTP traffic among the DA-MP servers

**General Architecture:**

Application Servers expose REST APIs externally to Load Balancer (if present) or group of SCS/AS

Application Server cluster is one or more separate application servers handling traffic

Admin Server allows configuration and maintenance of OCSG nodes

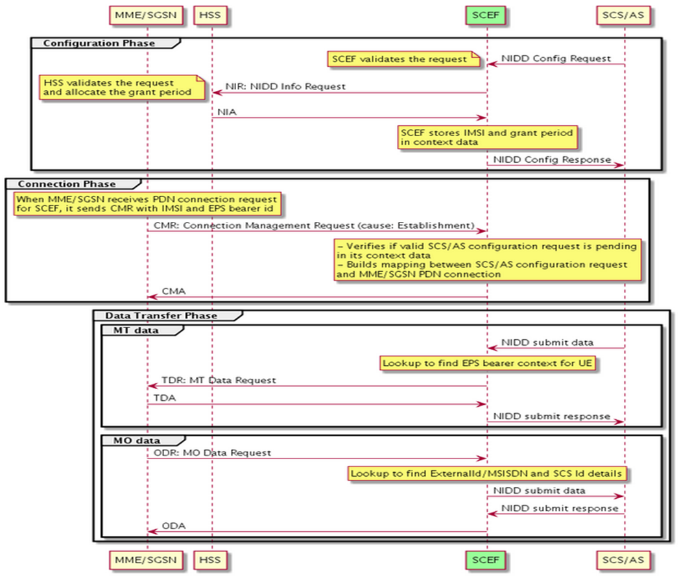
Database uses a separate DSR Active/Standby cluster running COMCOL IDB/MySQL for exclusive OCSG purposes

OCSG (DSR API Gateway) uses a separate ISO (OVA) than regular DSR

DSR DA-MPs communicate with OCSG Application Servers via REST

#### Use Cases Supported in DSR 8.3

**NIDD (Non-IP Data Delivery):** Used to handle MO and MT communication with UEs. This managed object allows the customer to create instance of NIDD configuration sets as needed. Support MT message delivery by buffering up to 5 MT NIDD messages per PDN connection in case UE is not reachable or no PDN connection is established. Messages will be buffered up to configurable maximum message latency time at DSR. Support APN rate control for both MO and MT



Configuration Phase:

* + SCS/AS send NIDD config request.
  + SCEF validates it with HSS.

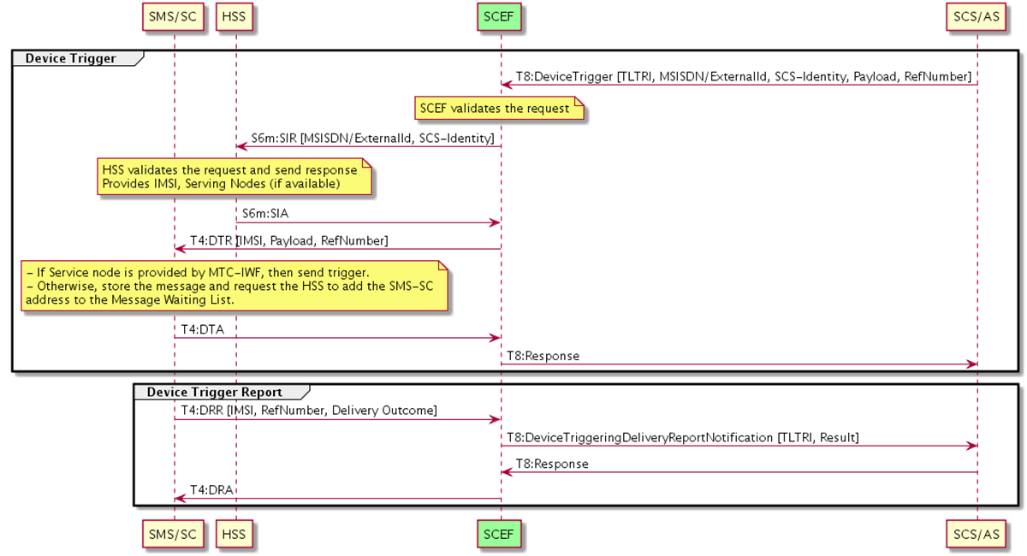
Connection Phase:

* + MME/SGSN initiates PDN connection setup messaging with SCEF.
  + SCEF validates the request.

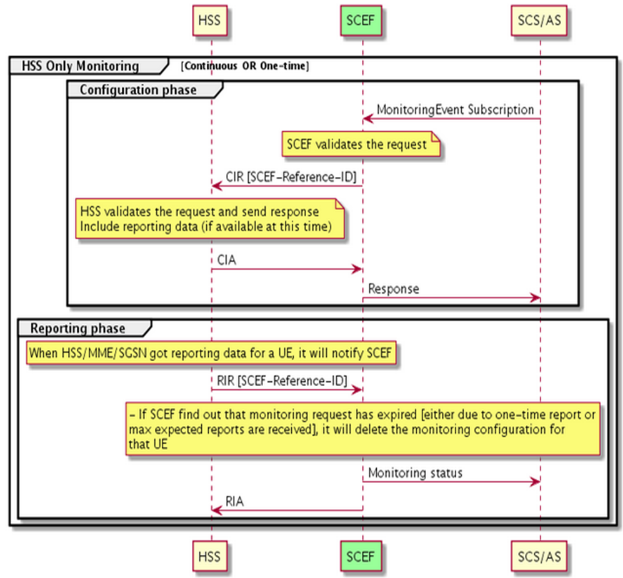
Data Transfer Phase:

* + SCS/AS can initiate data transfer towards UE. SCEF finds MME/SGSN that has PDN connection setup and sends data for delivery.
  + UE can initiate data transfer towards SCS/AS. SCEF finds details of UE and send message to corresponding SCS/AS.

**Device Triggering:** Used by an SCS/AS to send information for the UE to perform a specific action. Allow device triggers initiated from SCS/AS through T8 RESTful interface. Authorization of device trigger requests through HSS using S6m interface. Supports Device Trigger delivery through SMS-SC using T4 interface. Supports Device Trigger delivery status back to SCS/AS.



**Monitoring Events:** Intended for monitoring 3GPP system events for statistics, logging, or other purposes. Events such as UE\_REACHABILITY(1), LOSS\_OF\_CONNECTIVITY(0), LOCATION\_REPORTING(2), CHANGE\_OF\_IMSI\_IMEI(SV)\_ASSOCIATION(3), ROAMING\_STATUS(4). This managed object allows the customer to create instances of monitoring configuration sets as needed.



HSS only monitoring:

* Configuration Phase:

SCS/AS send monitoring subscription request to SCEF

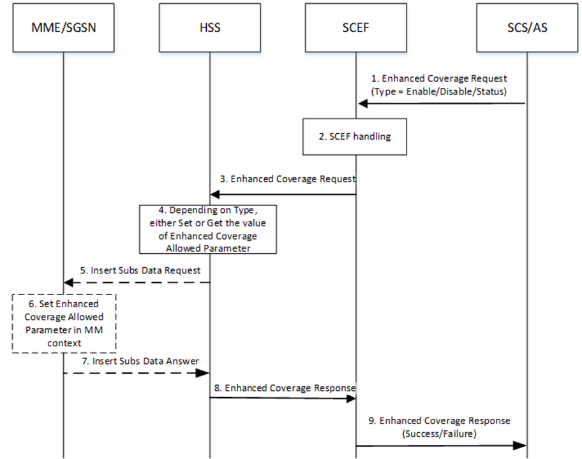
SCEF validates it and send it to HSS for configuration and monitoring

* Reporting Phase:

When monitoring data is available for UE, HSS will send RIR to SCEF

SCEF validates the request and notifies SCS/AS

**Enhanced Coverage Restriction (ECR) Control:**Enhanced Coverage may require use of extensive resources (e.g., radio and signalling resources) from the network. This feature enables an SCS/AS to control the usage of Enhanced Coverage by specific UEs

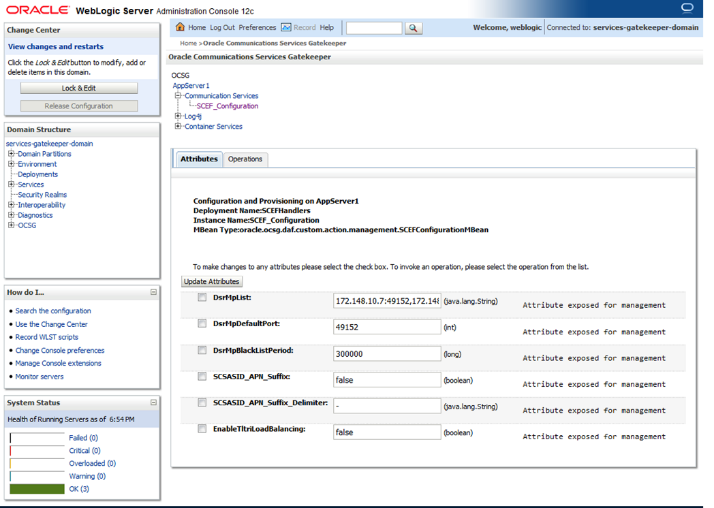
* Enables 3rd party service providers to query status of enhanced coverage restriction or enable/disable enhanced coverage restriction per individual UEs

**3.4.2.1 MEAL**

The SCEF application has added the following new Measurement Report Groups.

* SCEF Performance Measurement Group
* SCEF Exception Measurement Group
* SCEF NIDD Performance Measurement Group
* SCEF NIDD Exception Measurement Group
* SCEF Monitoring Performance Group
* SCEF Monitoring Exception Group

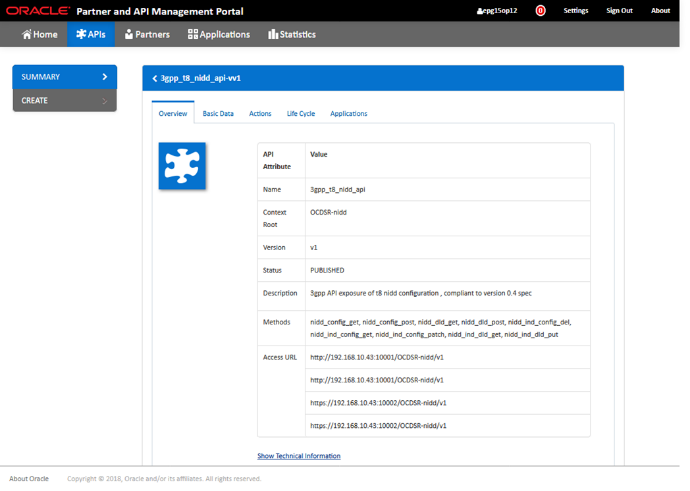
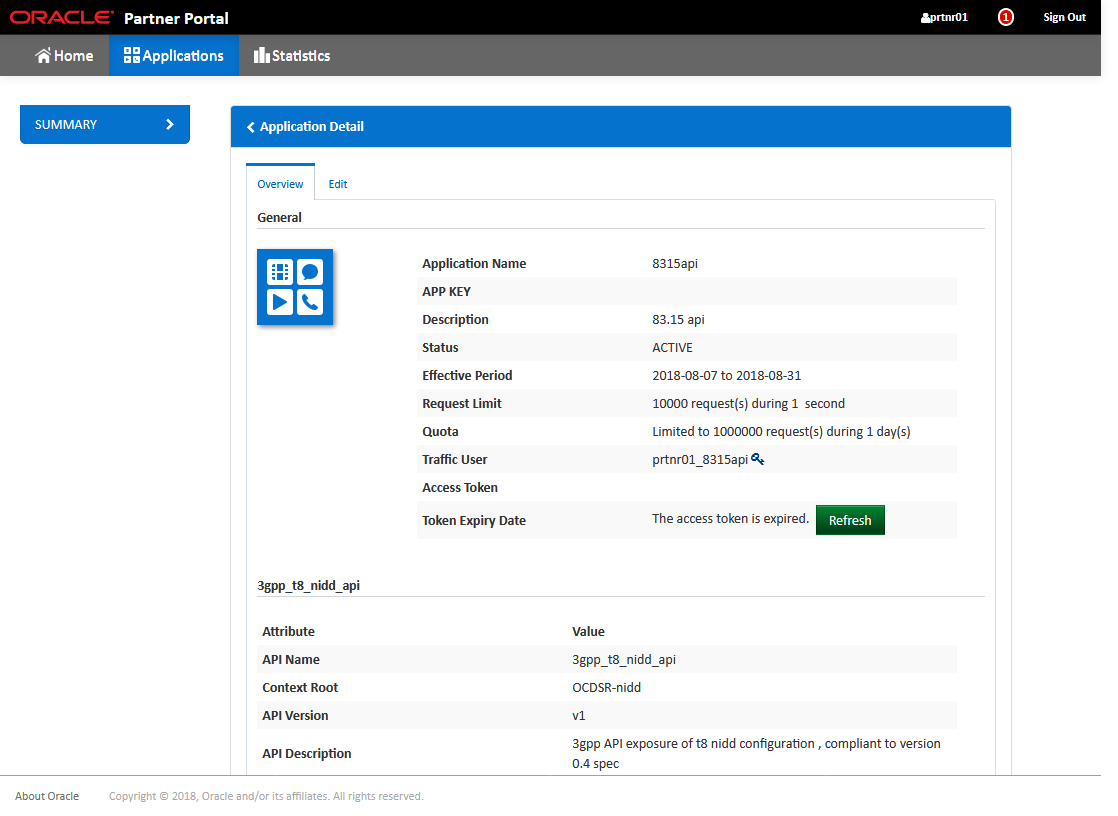
**3.4.2.2 OCSG GUI Console:**

* Resides in the Admin server
* Shows the status of the system
* Configures DSR MP IP addresses and other settings
* Displays message statistics

**OCSG: API & Partner Portal:**

* Resides in the application servers
* “Application,” i.e., API packaging for customer use
* Defines SLA (i.e., traffic limits) per API
* Defines traffic authorization credentials (only messages with proper authorization are allowed)

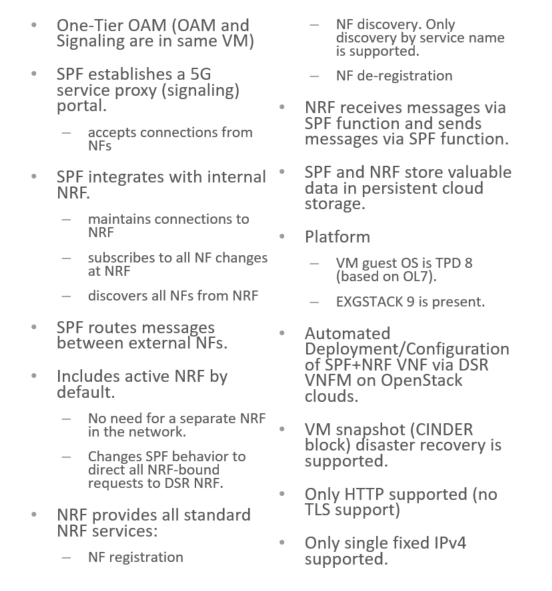
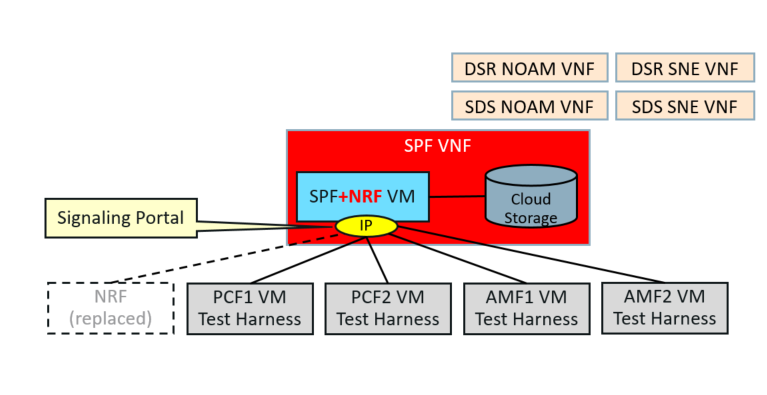
**OCSG API & Partner Portal**



## 5G SPF + NRF (PoC)

* + 1. Description

This feature is intended to provide the means to user to run “on demand”/automated reports for licensing utilization for

****

#### Deployment of SPF+NRF VNF

SPF+NRF is a single VM solution which is deployed and configured using VNFM (VNFM steps are explained in further slides).

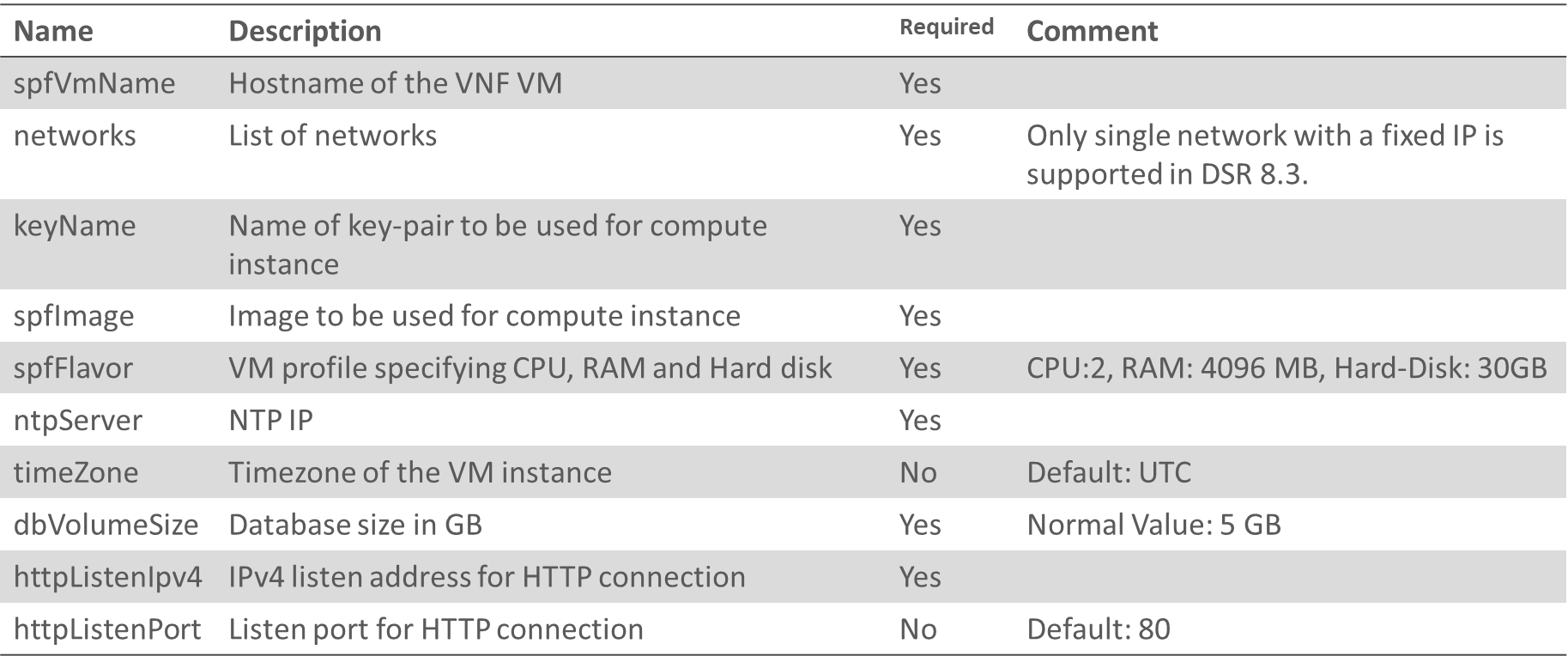
Only supported configuration is via VNFM interface. Configurable attributes are shown on the next slide.

SPF+NRF VM uses OpenStack CINDER block for database which means that the database is always available even when VM is destroyed (DR scenario).

httpListenIpv4:httpListenPort shall be provided in the HTTP/2 authority for NRF messages i.e. NF registration, NF de-registration and NF discovery. The attribute httpListenIpv4 and httpListenPort are defined on the next slide.

Any non-NRF message which needs to be routed through the SPF+NRF shall have the :authority header set to the destination service IP and port.

**Supported Configuration:**

****

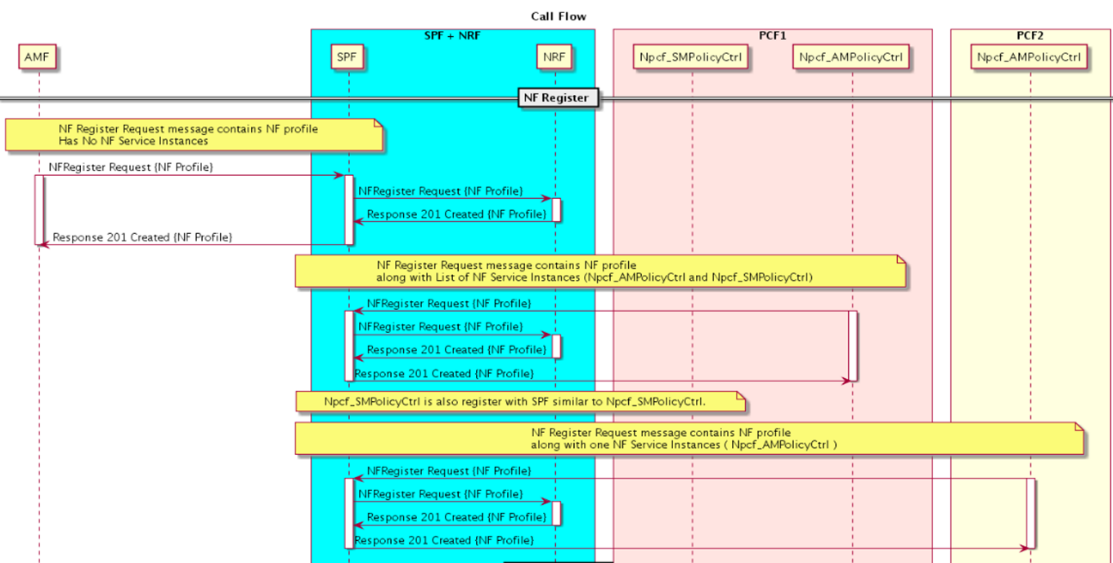
**VNFM Steps:**

VNF deployment is a two-step process

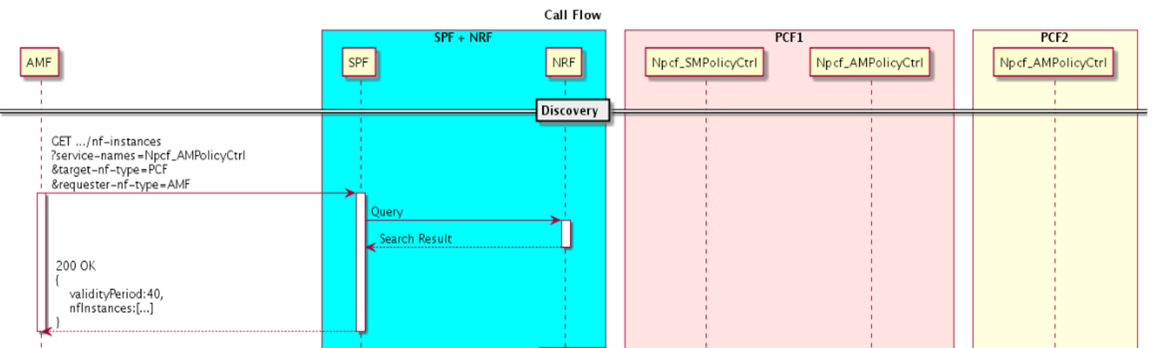
Step1: Creating a VNF instance

Step2: Instantiating the SPF VNF

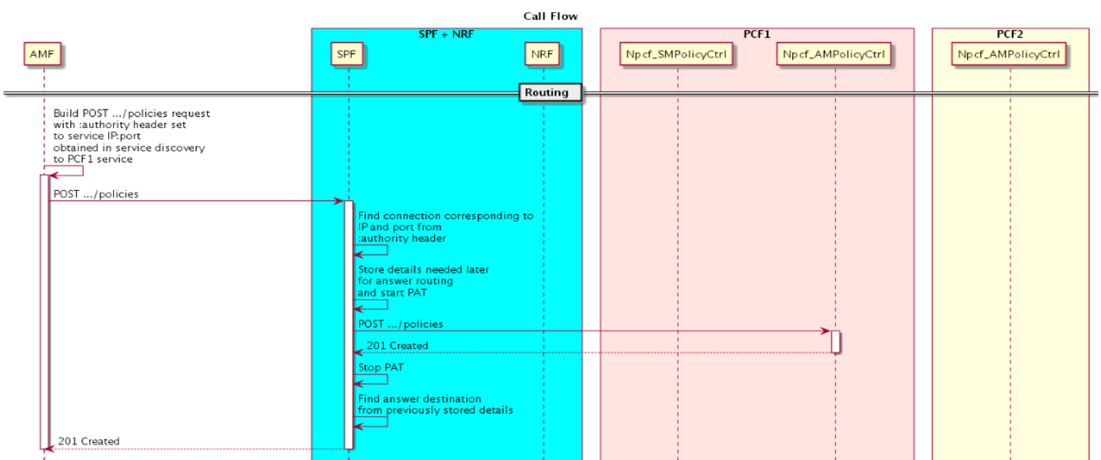
**Call Flow – NF Registration**

****

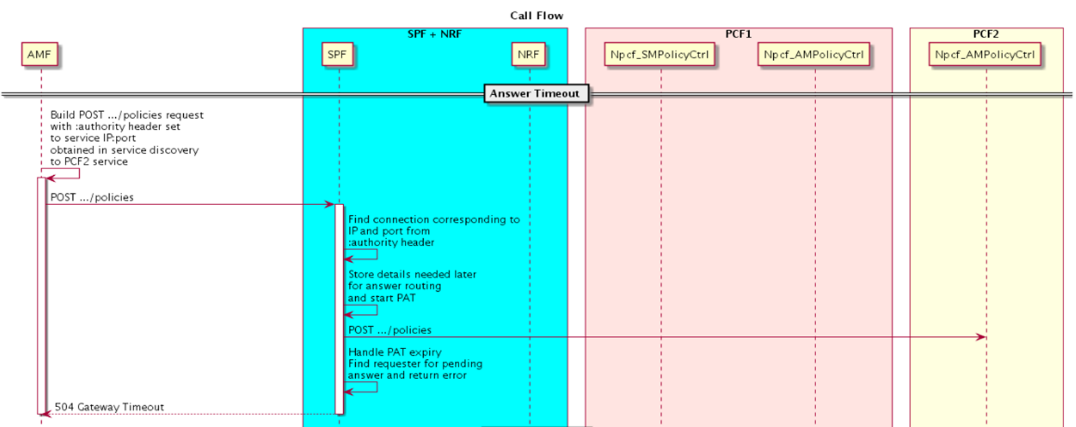
**Call Flow – NF Discovery**

****

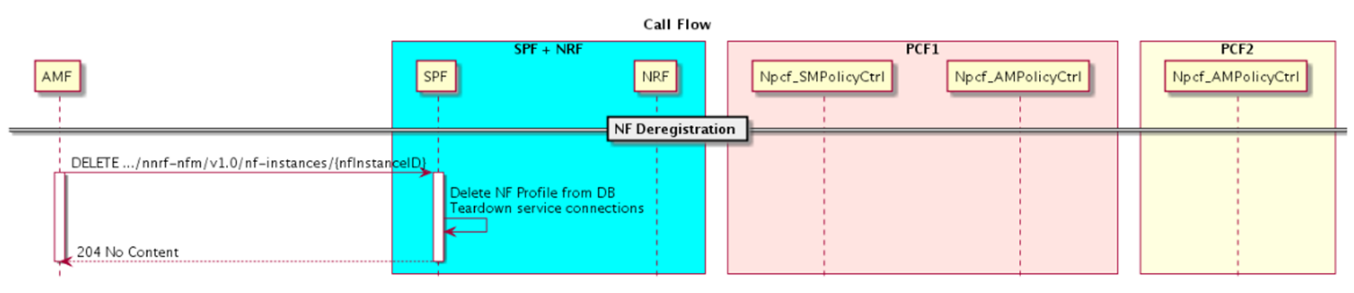
**Call Flow – Routing**

****

**Call Flow – Answer Timeout**

****

**Call Flow – Deregistration**

****

## vNFM

* + 1. Description

The main objective of the DSR VNFM is to provide an ETSI-compliant VNF manager. The VNFM would be helpful in the following ways:

* Automate lifecycle management (LCM) operations for DSR VNFs. Automation of these operations can reduce their execution time by up to 90 percent.
* Provide a standardized interface for ease of integration with automation clients, especially ETSI-compliant NFV Orchestrators. The DSR VNFM will provide a REST API that complies with ETSI NFV-SOL 003.
* The VNFM is also helpful in responding quickly to changing customer requirements, and to deliver solutions for those requirements in a very short time.

**Prerequisites:**

DSR-specific flavors. DSR VNFM assumes that the following flavors are defined on each OpenStack tenant that DSR VMs will be deployed on

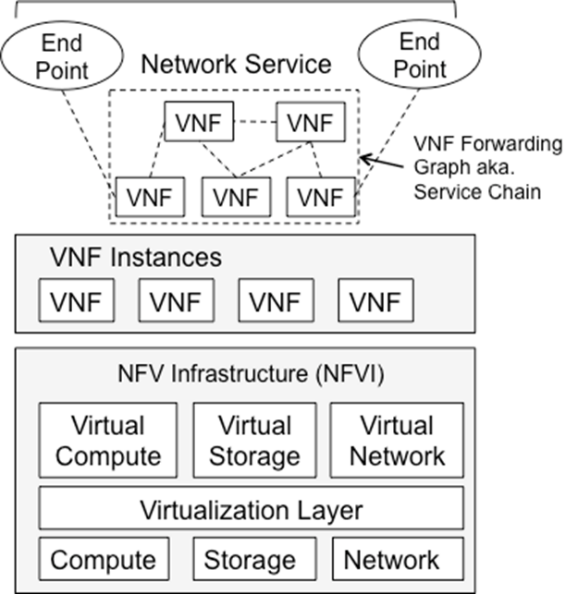
****

**Advantages of using VNFM:**

Deployment of Virtual DSR (vDSR) was performed through the following methods that required manual processing:

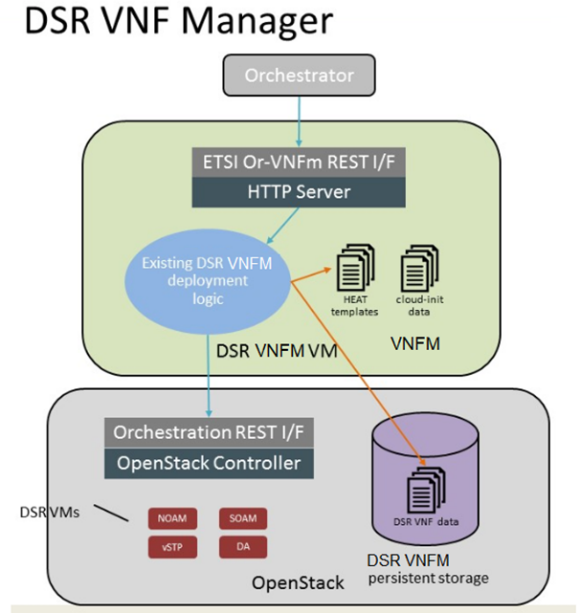
* VM creation and installation process
* HEAT Template based installation (Heat template requires manual update)
* The manual deployment consumes multiple hours to deploy a fully operational DSR and the HEAT template-based method needed more caution as it required more manual work.
* Using DSR VNFM, the users can now deploy a fully operational DSR on OpenStack in less than 15 minutes!
* This application benefits both the internal and external customers by reducing the operating expenses with the implementation of automation and by reducing human errors with the eliminating of manual intervention.

#### VNF Management Functions and Responsibilities



* Manage Virtual Network Function (VNF) templates dictating resource requirements for the specific NF
* Manage the life cycle of the VNFs
* Maintain and manage the VNF local capacity requests
* Implement local policies / business rules for VNF configuration

#### Accessing VNFN via REST Interface

The DSR VNFM is accessible via a REST interface. There is no provision to access the REST interface through CLI, or GUI, however it can be accessed through a Swagger specification provided for the REST interface (http://<VNFM IP>:8080/docs/vnfm/). There are many other compatible interfaces that can be used with popular REST testing tools.

Some of the most widely used tools that can be used with the REST testing tool are:

*Swagger UI*

With the Swagger UI, a GUI can be generated from the Swagger specification.

*Postman*

Another popular tool for creating REST requests is the Postman tool. It is available as a standalone app and as a Chrome browser plugin. You can import a Swagger specification to allow Postman to understand the VNFM REST API in detail, which will allow it to assist you when creating requests and interpreting responses.

Currently DSR VNFM support the following operations.

* Create VNF Identifier
* Instantiate VNF

#### Create VNF Identifier (sample)

The following procedure is a part of feature activation preparation and is used to verify the system topology of the DSR network and servers:

Before a DSR VNF is instantiated, the user must issue a request to create a VNF instance by using the command "create VNF instance".

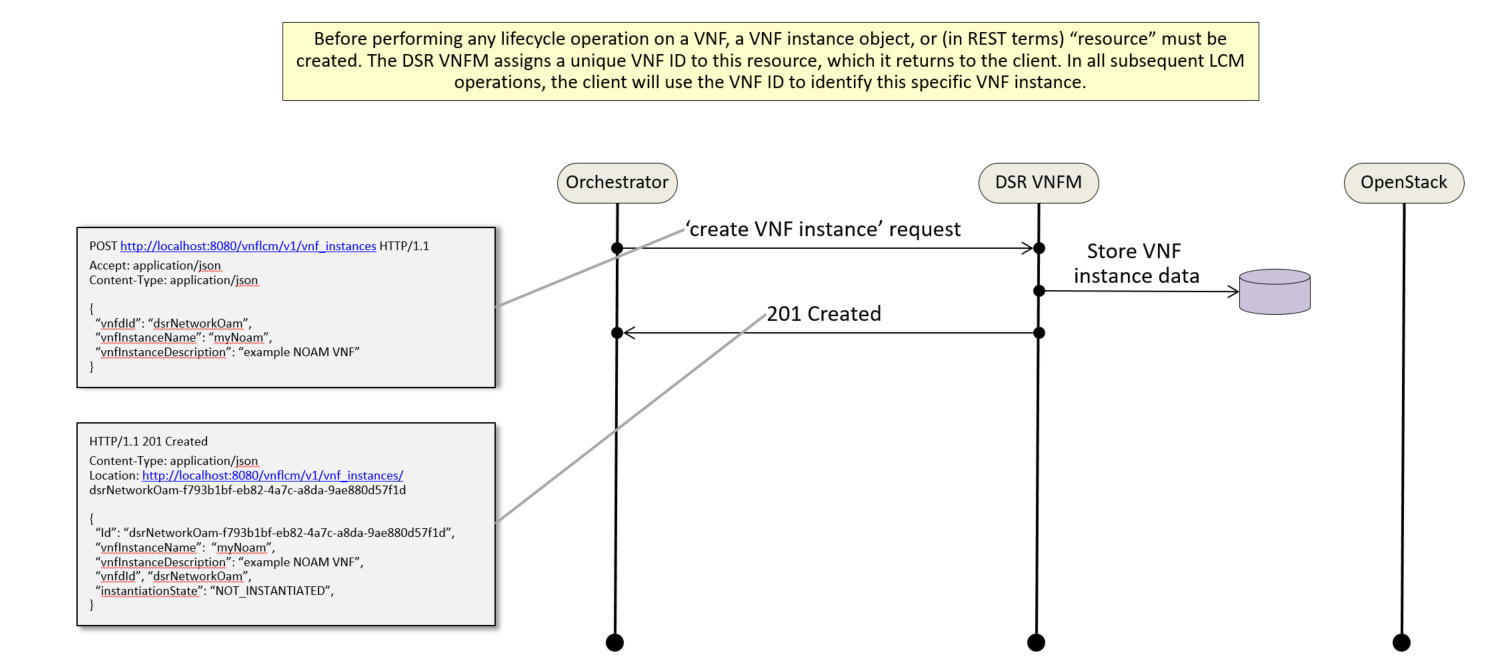
Creating a VNF instance simply informs the VNFM that a user has requested to instantiate a VNF at some point of time in the future.

The VNFM returns a VNF ID that must be saved, as it is required later while performing operations on the same VNF.

      Note: Each VNF has its own VNF ID, so if it is required to create a DSR with Two signaling VNFs, the user must issue the request to create a VNF instance three times, one for the network OAM VNF and one each for both the signaling VNFs.

For more information about the full listing of all inputs and possible outputs of the command "create VNF instance”, see ETSI NFV-SOL 003, section 5.4.2.3.1, or the DSR VNFM Swagger specification

**Create VNF Instance Call Flow –**



**Create VNF instance request generated (Create Rest Request for the VNF NOAM)**

URL: [http://<<VNFM HOST IP>>:8080/vnfm/v1/vnf\_instances](http://myhost:8080/vnfm/v1/vnf_instances)  
Accept: application/json  
Content-Type: application/json

Example for NOAM:

   {

"vnfdId": "dsrNetworkOam",

"vnfInstanceName": "DemoNoam",

"vnfInstanceDescription": "DemoNoam "

}

**Create VNF Instance Response (Create Rest Response for the VNF NOAM)**

201 Created  
Content-Type: application/json  
URL: [http://<<VNFM HOST IP>>:8080/vnfm/v1/vnf\_instances](http://myhost:8080/vnfm/v1/vnf_instances)/dsrNetworkOam-38e2c734-2e1f-4ed8-b18b-08d6c30c60d2

 { "id": "dsrNetworkOam-cdf2d110-ac13-4c54-b87e-c49935cd8b33",  
 "vnfdId": "dsrNetworkOam",  
 "instantiationState": "NOT\_INSTANTIATED",  
 "vnfInstanceName": "DemoNoam"  
}

**Create VNF instance request generated (Create Rest Request for the VNF Signaling)**

URL: [http://<<VNFM HOST IP>>:8080/vnfm/v1/vnf\_instances](http://myhost:8080/vnfm/v1/vnf_instances)  
Accept: application/json  
Content-Type: application/json

Example for Signaling:

   {

"vnfdId": "dsrSignaling",

"vnfInstanceName": "DemoSignaling",

"vnfInstanceDescription": "DemoSignaling "

}

**Create VNF Instance Response (Create Rest Response for the VNF Signaling)**

201 Created  
Content-Type: application/json  
URL: [http://<<VNFM HOST IP>>:8080/vnfm/v1/vnf\_instances](http://myhost:8080/vnfm/v1/vnf_instances)/dsrSignaling-38e2c734-2e1f-4ed8-b18b-08d6c30c60d2

 { "id": "dsrSignaling-cdf2d110-ac13-4c54-b87e-c49935cd8b33",  
 "vnfdId": "dsrSignaling",  
 "instantiationState": "NOT\_INSTANTIATED",  
 "vnfInstanceName": "DemoSignaling"  
}

**Create VNF instance request generated (Create Rest Request for the VNF SPF)**

URL: [http://<<VNFM HOST IP>>:8080/vnfm/v1/vnf\_instances](http://myhost:8080/vnfm/v1/vnf_instances)  
Accept: application/json  
Content-Type: application/json

**Example for SPF:**

   {

"**vnfdId": “SPF",**

"vnfInstanceName": "DemoSPF",

"vnfInstanceDescription": "DemoSPF"

}

**Create VNF Instance Response (Create Rest Response for the VNF SPF)**

201 Created  
Content-Type: application/json  
URL: [http://<<VNFM HOST IP>>:8080/vnfm/v1/vnf\_instances](http://myhost:8080/vnfm/v1/vnf_instances)/SPF-38e2c734-2e1f-4ed8-b18b-08d6c30c60d2

 { "id": "SPF-cdf2d110-ac13-4c54-b87e-c49935cd8b33",  
 "vnfdId": "dsrSPF",  
 "instantiationState": "NOT\_INSTANTIATED",  
 "vnfInstanceName": "DemoSPF"  
}

#### Instantiating VNF (sample)

In order to start a DSR deployment, it is required to instantiate a DSR Network OAM VNF. Before deploying the VNF, the following information must be available:

The VNF ID for a previously created DSR network OAM VNF instance.

Information about the OpenStack instance on which the VNF must be deployed:

OpenStack Controller URI

Domain name

Username

Password

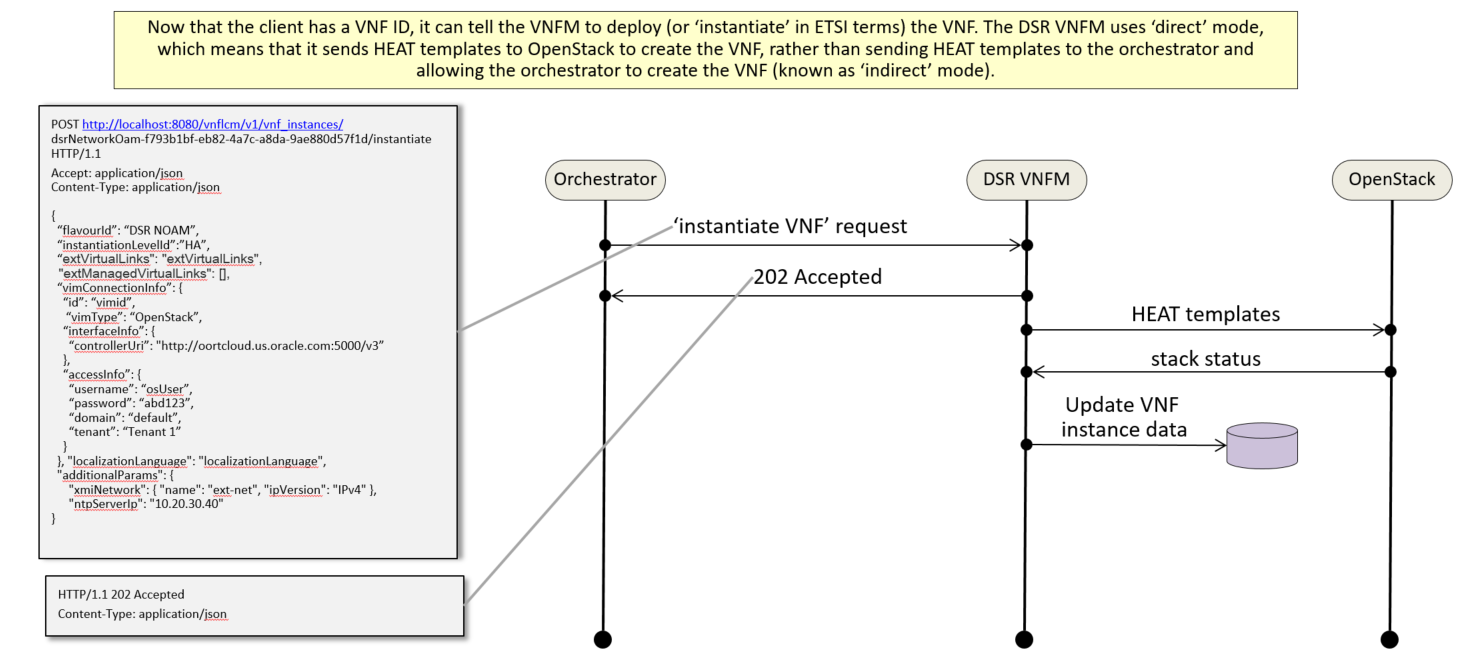
Tenant name

The name of a public network in the selected OpenStack instance that will carry the OAM traffic.

The IP of an NTP server accessible by VMs within the selected OpenStack instance. The OpenStack controller that controls the selected OpenStack instance normally hosts an NTP server and is often a good choice.

For more information about the full listing of all inputs and possible outputs of the command "instantiate VNF", see ETSI NFV-SOL 003, section 5.4.4.3.1, or the DSR VNFM Swagger specification.

**Instantiating VNF Instance Call Flow –**

****

**Instantiating NOAM Request generated (Instantiate Rest Request for the VNF NOAM)**

URL: [http://<<VNFM HOST IP>>:8080/vnfm/v1/vnf\_instances/](http://myhost:8080/vnfm/v1/vnf_instances/)< VNF ID received from create request>/instantiate

Accept: application/json  
Content-Type: application/json

 {

"flavourId": "DSR NOAM",

"instantiationLevelId": "HA",

"extVirtualLinks": "extVirtualLinks",

"extManagedVirtualLinks": [],

"vimConnectionInfo":[ {

"id": "vimid",

"vimType": "OpenStack",

"interfaceInfo": {

"controllerUri": "http://oortcloud.us.oracle.com:5000/v3"

},

"accessInfo": {

"username": "dsrci.user",

"password": "cisanity",

"domain": "default",

"tenant": "DSR CI"

}

}],

"localizationLanguage": "localizationLanguage",

"additionalParams": {

"xmiNetwork": {

"name": "ext-net3",

"ipVersion": "IPv4"

},

"ntpServerIp": "10.250.32.10"

}

}

**Instantiate VNF Instance Response**

202 Accepted

Content-Type: application/json

The 202 response means that the request was accepted for processing. The VNF might take up to 15 minutes to become fully operational. Use the DSR GUI to determine when the VNF is operational.

If the VNFM creates a VNF that is operational, but has no signaling VNFs, then it is required to deploy one or more signaling VNF, and create the DIAMETER configuration data (peers, connections, etc.) for those VNFs to perform DIAMETER routing.

The supported NOAM Flavor is DSR NOAM.

**Instantiating Signaling Request generated (Instantiate Rest Request for the VNF Signaling)**

URL: [http://<<VNFM HOST IP>>:8080/vnfm/v1/vnf\_instances/](http://myhost:8080/vnfm/v1/vnf_instances/)< VNF ID received from create request>/instantiate

Accept: application/json  
Content-Type: application/json

 {{

"flavourId": "DIAMETER+SS7",

"instantiationLevelId": "HA",

"extVirtualLinks": "extVirtualLinks",

"extManagedVirtualLinks": [{

"id": "",

"virtualLinkDescId": "",

"resourceId": "8a4d1ec6-367a-4b1a-978d-2c4eae3daec3"

},

{

"id": "",

"virtualLinkDescId": "",

"resourceId": "2bed5886-8c97-4623-8da3-9c500cce71e3"

}

],

"vimConnectionInfo":[ {

"id": "vimid",

"vimType": "OpenStack",

"interfaceInfo": {

"controllerUri": "http://oortcloud.us.oracle.com:5000/v3"

},

"accessInfo": {

"username": "dsrci.user",

"password": "cisanity",

"domain": "default",

"tenant": "DSR CI"

}

}],

"localizationLanguage": "localizationLanguage",

"additionalParams": { "xmiNetwork": { "name": "ext-net3", "ipVersion": "IPv4" },

"xsiNetwork": { "name": "ext-net2", "ipVersion": "IPv4" },

"ntpServerIp": "10.250.32.10",

"primaryNoamVmName": "NOAM00-32cd6138",

"noamSgName": "dsrNetworkOam\_NOAM\_32cd6138\_SG"

}

}}

**Instantiating SPF Request generated**

URL: [http://<<VNFM HOST IP>>:8080/vnfm/v1/vnf\_instances/](http://myhost:8080/vnfm/v1/vnf_instances/)< VNF ID received from create request>/instantiate

Accept: application/json  
Content-Type: application/json

 {{

"flavourId": "SPF",

"instantiationLevelId": "HA",

"extVirtualLinks": "extVirtualLinks",

"extManagedVirtualLinks": [],

"vimConnectionInfo":[ {

"id": "vimid",

"vimType": "OpenStack",

"interfaceInfo": {

"controllerUri": "http://oortcloud.us.oracle.com:5000/v3"

},

"accessInfo": {

"username": "xxxx.user",

"password": "xxxx",

"domain": "default",

"tenant": "<Tenant Name>"

}

}],

"localizationLanguage": "localizationLanguage",

"additionalParams": {

"networks": [{

"network": "ext-net3",

"fixed\_ip": "10.196.12.248"

}],

"ntpServerIp": "10.250.32.10",

"keyName": "spf",

"httpListenIpv4": "10.196.12.248",

"httpListenPort": 9999,

"timeZone": "GMT",

"dbVolumeSize": 5

}

}}

**Instantiate VNF Instance Response**

202 Accepted

Content-Type: application/json

The 202 response means that the request was accepted for processing. The VNF might take up to 15 minutes to become fully operational. Use the DSR GUI to determine when the VNF is operational.

* The supported Flavor is **SPF.**

## CAPACITY INCREASE FEATURE

* + 1. Problem statement / Solution

The current testing limit for a given type of MP is 16 (DA-MP, vSTP). This feature is to increase the testing limits for CONFIGURING more of a given MP type within the existing hard configuration limits. Multiple drivers for increasing the limit

* Virtualized MPs have lower capacity than “bare metal” MPs, need more of them to hit a given DSR MPS
* For vSTP need more vSTP MPs to allow for easier mapping to SLIC cards for Eagle replacement

#### New Configuration Limits

The 8.3 configuration limits (within the 48 server limit):

* 0-32 DA-MPs
* 0-32 vSTP MPs

#### Capacity Increase

The 8.3 increased the limit on system connections

* ARR has been increased to 50K and ART has been increased to 1.5K.
* PRT rules within the NE have been increased to 50000.
* Diameter Connection per System support 32000.

## DIAMETER SECURITY APPLICATION (RSR MESSAGE support)

* + 1. Description

RSR Message support is added for the following statefull counter measures in DSA:

1. Previous Location Check

2. Source Host Validation HSS

3. Source Host Validation MME

**1. Previous Location Check [PreLocChk]:**

This Countermeasure screens S6a/d PUR and NOR message of Outbound Roaming Subscribers to check if the MME from which the PUR/NOR message received is the same MME or not, on which the subscriber is currently registered.

The Outbound Roaming Subscriber is considered as successfully registered to a Foreign Network MME when an Ingress S6a/d ULR/A (ULA with Result-Code as 2xxx) is processed by DSA.

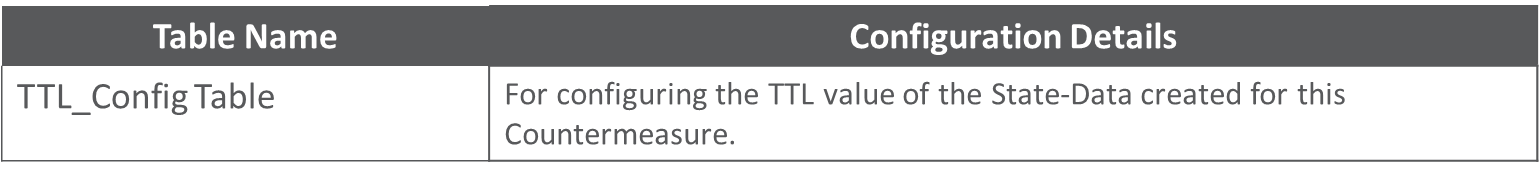
The Outbound Roaming Subscriber is considered de-registered from the Foreign Network MME when

* An Egress S6a/d CLR is processed by DSA. Or
* An Egress S6a/d RSR with valid user-id range is processed by DSA. Or
* A non-vulnerable Ingress PUR message is processed by DSA.

This Countermeasure considers the ingress S6a/d PUR and NOR message as vulnerable if any of the below condition is true

* The subscriber has not registered to any MME.
* The MME from which the PUR/NOR message is received is different from the MME on which the subscriber is registered.

Below is the list of table that needs to be configured for this Countermeasure



**2. Source Host Validation [SrcHostValHss]:**

This Countermeasure screens S6a/d IDR, DSR, RSR and CLR message of Inbound Roaming Subscribers to check if the HSS from which the IDR/DSR/RSR/CLR message is received is the same HSS or not to which earlier registration request has been sent successfully.

The Inbound Roaming Subscriber is considered as successfully registered with the Home Network when an Egress S6a/d ULR/A (ULA with Result-Code as 2xxx) is processed by DSA.

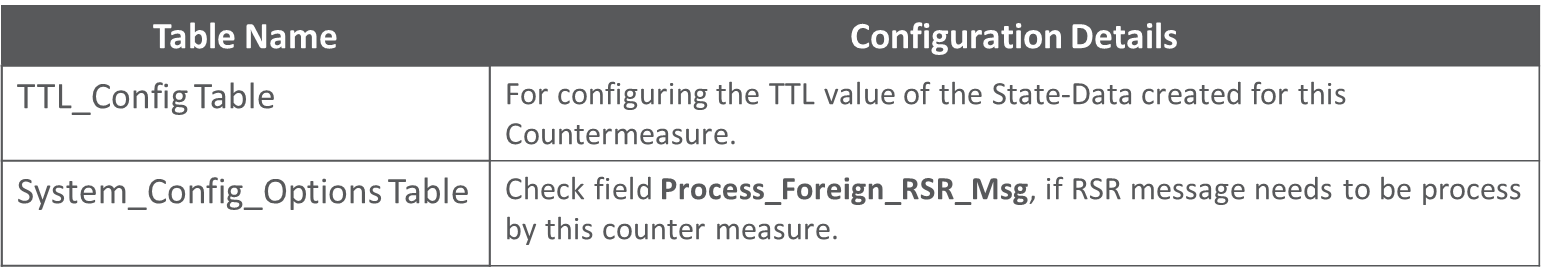
The Inbound Roaming Subscriber is considered de-registered from the Home Network when

* An Egress S6a/d PUR is processed by DSA. Or
* A non-vulnerable Ingress CLR message is processed by DSA.
* A Ingress RSR message containing the valid User-Id is processed by DSA.

This Countermeasure considers the ingress S6a/d IDR, DSR and CLR message as vulnerable if any of the below condition is true

* The subscriber has not registered with the Home Network.
* The HSS from which the IDR/DSR/CLR message is received is different from the HSS to which earlier registration request has been sent.

Below is the list of table that needs to be configured for this Countermeasure



**3. Source Host Validation MME [SrcHostValMme]:**

This Countermeasure screens S6a/d ULR and PUR message of Outbound Roaming Subscribers to check if the MME from which these messages are received is valid or not. This Countermeasure also validates the sequential ordering of authentication and registration process when the subscriber moves from one foreign network to another foreign network.

The Outbound Roaming Subscriber is considered as successfully authenticated by the Home Network when a Ingress S6a/d AIR/A (AIA with Result-Code as 2xxx) is processed by DSA

The Outbound Roaming Subscriber is considered as successfully registered to a Foreign Network when a non-Vulnerable Ingress S6a/d ULR/A (ULA with Result-Code as 2xxx) is processed by DSA

The subscriber is considered de-registered from the Foreign Network when

* An Egress S6a/d CLR is processed by DSA. Or
* An Egress S6a/d RSR with User-Ids of valid range is processed by DSA. Or
* A non-vulnerable Ingress PUR message is processed by DSA.

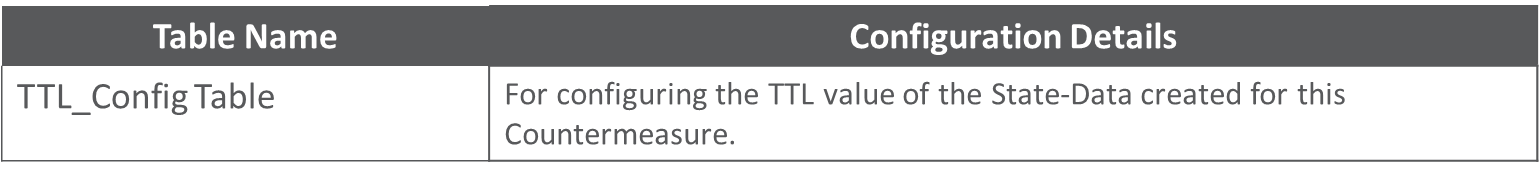
This Countermeasure considers the ingress S6a/d ULR message as vulnerable if any of the below condition is true

* The subscriber has not authenticated by the Home Network.
* The Visited-PLMN-Id from which the subscriber has authenticated is not matching with the Visited-PLMN-Id from which registration request is received.

This Countermeasure considers the ingress S6a/d PUR message as vulnerable if any of the below condition is true

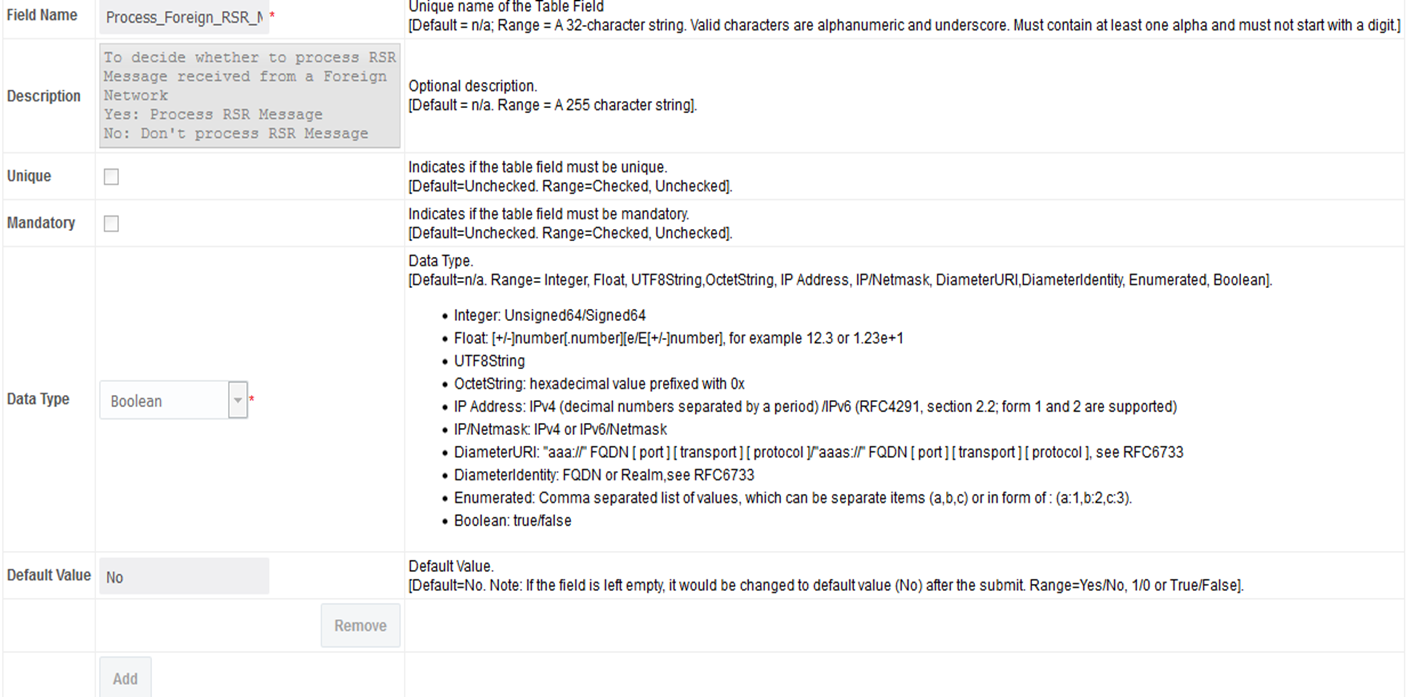
* The subscriber has not authenticated by the Home Network.
* The subscriber has not registered with the Home Network.
* The MME from which the PUR message is received is different from the MME on which the subscriber is registered.

Below is the list of table that needs to be configured for this Countermeasure



#### DSA Tables

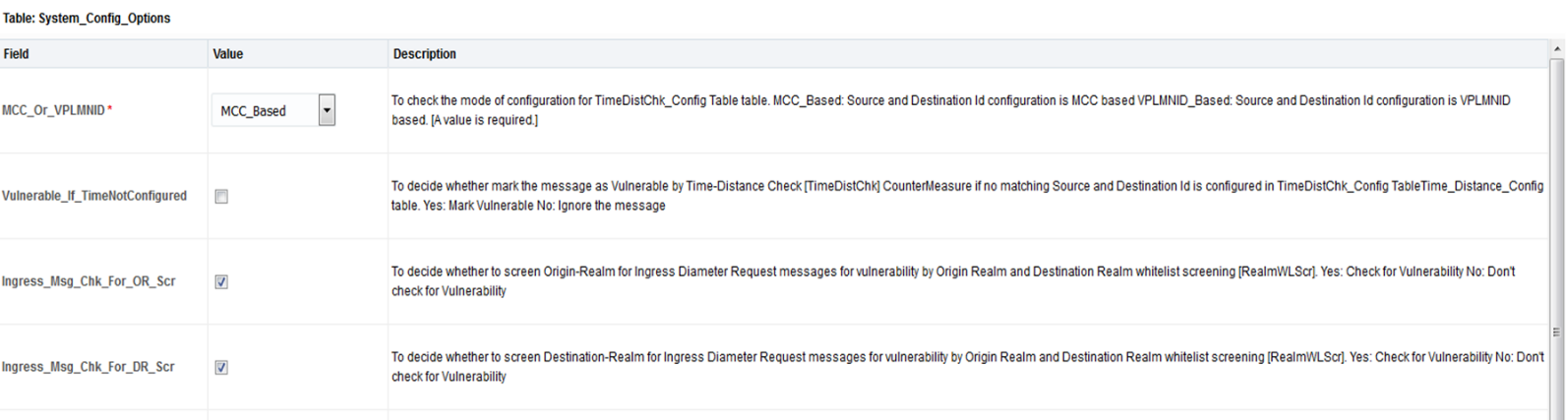
A new field (Process\_Foreign\_RSR\_Msg) is added into the System\_Config\_Options table.

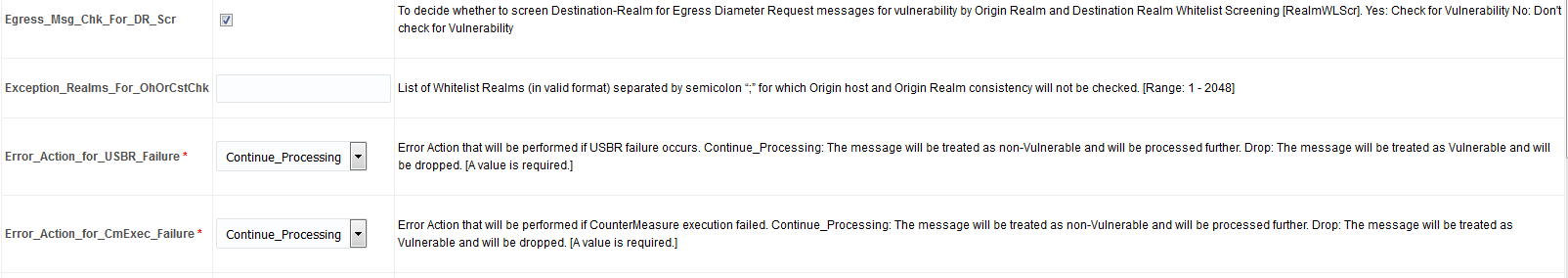


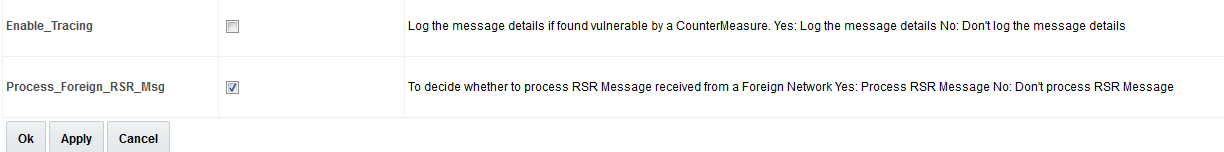
#### GUI Changes

**System\_Config\_Options Table View Screen**

(SOAM GUI 🡪 Main Menu 🡪 DCA Framework 🡪 Diameter Security Application 🡪 Application Control 🡪 Version 🡪 Config Data 🡪 System\_Config\_Options 🡪 Provision Table 🡪 Insert)







## VSTP license measurement

#### Description

This feature is intended to provide Peak traffic information integrated inside historical reports for a given user defined period for licensed capacity inside new measurement report group for vSTP

A measurement implemented for the MPS measurement per network element as follows:

* *VstpLicNERxMSU (Measurement ID 21130):* Ingress traffic rate at given Network Element.

The measurement VstpLicNERxMSU calculated at end of each 5 min interval as sum of Message rate of SysMetric ID 21019 (VstpTxM3RLDataMsgs) for each MP on given Network Element.

* *VstpLicNETxMSU (Measurement ID 21132):* Egress traffic rate at given Network Element.

The measurement VstpLicNETxMSU calculated as sum of Message rate of SysMetric ID 21020 (VstpRxM3RLDataMsgs) for each MP on given Network Element.

Both the above measurements will be pegged at 5 minute intervals.

A measurement implemented for the network wide MPS for the entire network as follows:

* *VstpLicRxTPS (Measurement ID 21134):* Network wide Ingress traffic rate.

The measurement VstpLicRxTPS calculated as sum of Message rate (MPS) each Network Element in Network (Measurement ID 21130).

* *VstpLicTxTPS (Measurement ID 21135):* Network wide Egress traffic rate.

The measurement VstpLicTxTPS calculated as sum of Message rate (MPS) each Network Element in Network (Measurement ID 21132).

Both the above measurements will be pegged at 5 minute intervals.

A measurement shall be implemented for the daily peak MPS for entire network as follows:

* VstpLicRxTPSPeak (Measurement ID 21131): Network MPS Peak for ingress traffic.
* VstpLicTxTPSPeak (Measurement ID 21133): Network MPS Peak for egress traffic.

The Network MPS Peak measurement (both ingress & egress ) will be measured at end of 5 minute intervals. The MPS value pegged (in the Measurement ID 21134 / 21135) will be used to calculate the new corresponding (ingress / egress) daily peak. A new peak will be pegged only if the current MPS value is greater than the last recorded daily peak (applies to both ingress and egress peaks).

Note: At the start of each new day, the “License Measurements” thread will reset the current in-memory value for the Peak Network MPS (ingress & egress) back to zero.

|  |  |
| --- | --- |
|  | When a measurement report is requested for user specified duration and interval, report will contain the Network Peak MPS values (ingress & egress) for the interval when peak value was changed. For other intervals, 0 reported. |

## vstp Congestion Control Enhancements

The DSR 8.3 support vSTP congestion and flow control including

* PDU Pool tuning
* Usage tracking of RSP and Linkset buffers and related MEALs

#### Description

* + - 1. **PDU Pool**

PDU Pool size Increased to 27 K.

2 K PDUs from 27 K PDU Pool should be reserved for Link Status messages.

* + - 1. **Usage tracking of RSP and Linkset buffers**

M2PA link retransmission buffer size be equal to configured TPS \* T7 timer value.

M2PA link congestion level be max (CL of retransmission buffer, CL of connection queue)

M2PA link connection queue size be equal to retransmission buffer size.

M3UA link connection queue size be equal to configured TPS.

#### MEALS

* + - 1. **Alarm Enhancements**

New alarms are to track the usage of various buffers:

* Alarm “Link Retransmission Buffer Utilization Threshold Exceeded” to track the usage of link retransmission buffer.
* Alarm “Linkset Buffer Utilization Threshold Exceeded” to track the usage of linkset buffer. Linkset Buffer is used for buffering traffic during changeover/change back procedures.
* Alarm “RSP Buffer Utilization Threshold Exceeded” to track the usage of RPS buffer. RPS Buffer is used for buffering traffic during forced/controlled rerouting procedures.

Alarm “Transmission Association Queue Congestion Crossed” already exists for connection queue usage tracking.

Use of Comcol Sysmetric framework is for the usage tracking.

New alarm “PDU Pool exhausted for data messages” is proposed to report event of PDU pool exhaustion for data messages.

* + - 1. **Measurement Enhancements**

The new measurements indicate that message is dropped because link retransmission buffer full.

* Arrayed measurement *VstpMsuDiscardedLinkBufferFull* is to account number of messages dropped on particular link after retransmission buffer getting full.
* Similarly, measurement, *VstpMsuDiscardedLinksetBufferFull* (arrayed on linkset) is for Linkset buffer and arrayed VstpMsuDiscardedRspBufferFull (arrayed on RSP) is proposed RSP buffer. respectively.
* Existing measurement *VstpTxM3RLBufOverflow* is pegged for all types of buffers and is not arrayed. So new arrayed measurements specific to Linkset and RSP buffers are proposed.

New measurements *VstpPriority0MsuDiscarded, VstpPriority1MsuDiscarded, VstpPriority2MsuDiscarded, VstpPriority3MsuDiscarded* are to account discard of different type of priority messages during congestion. These measurements are valid for ANSI only.

## vstp Event/alarm Logging Enhancements

The DSR 8.3 supported vSTP the event/alarm list and logging mechanism. The section 4.0 MEAL Inserts summarize.

## MMI Updates

MMI provides the ability for EMS, OSS or NMS systems at customer’s network to interface directly with the DSR. Use of the MMI will allow real time changes in the DSR that is initiated by a configuration change in north-bound customer management systems.

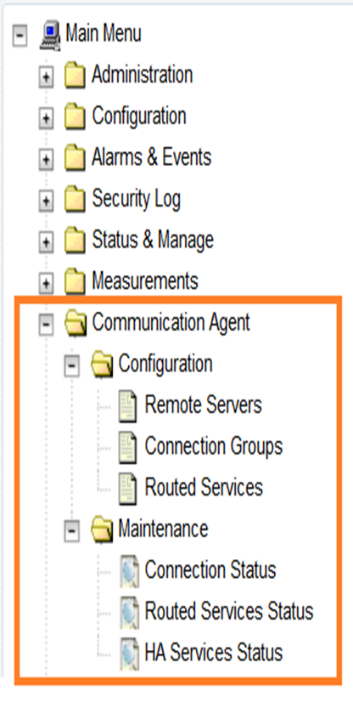
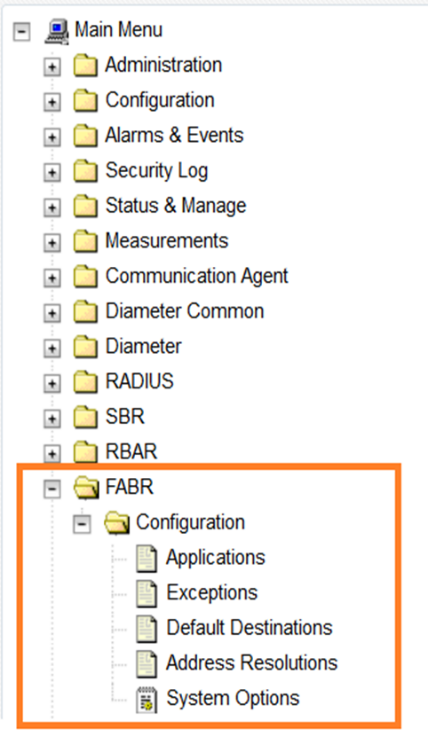
REST MMI chosen because “defacto industry standard and extensible and customizable to meet all the DSR interfaces.

#### Description

In the initial release of MMI, the following DSR applications can be managed via RESTful API

* Applications (RBAR, FABR, SCEF, vEIR)

**MMIs supported on DSR8.3: (DSR-NO & DSR-SO)**

****

**REST Operations:**

REST Operations can Create (POST), Request (GET), Update (PUT) or Delete (DELETE):

* GET: URI may be item (/servers/NOA) or collection (/servers) or query parameters
* POST and PUT also require a JSON Payload that fully defines object to create or edit
* DELETE: only one item

DSR objects are mapped to REST “Resources” (using URI)

* Eg: https://10.240.70.141/mmi/dsr/v1.0/diameter/routegroups
* Most common encodings of REST data are XML and JSON

As part of the build process the RAML specification is parsed and transformed to human readable documentation

# MEAL INSERTS

This section will summarize the changes to Alarms, Measurements, KPIs and MIBs. In the following inserts pertain to DSR Release 8.3 MEAL snapshot and deltas to earlier releases 7.3, 8.0, 8.1.1 and 8.2.1

The DSR/SDS 8.3 GA Release is 8.3.0.0.0-83.15.0

## DSR/SDS 8.3 MEAL Snapshot

## Meal Deltas (8.2.1)

## Meal Deltas (8.1.1)

## Meal Deltas (8.0)

## Meal Deltas (7.3) & SDS (7.3.1)

# reference list

The DSR 8.3 Release Notice and Customer Documentation can be found at the following OTN link.

<http://docs.oracle.com/en/industries/communications/diameter-signaling-router/index.html>

(Navigate to the Release 8.3.x link)

1. - This represents the minimum release of the HP FUP 2.2.x series to support all content in the Platform 74 release. It is recommended that the latest firmware release always be used in order to address known security issues. [↑](#footnote-ref-1)
2. - This represents the minimum release of the Oracle firmware series to support all content in the Platform 74 release. It is recommended that the latest firmware release always be used in order to address known security issues. [↑](#footnote-ref-2)