

# **Oracle® Communications Diameter Signaling Router**

Network Impact Report

Release 8.2

**E88983-02**

July 2020

## Oracle ® Communication Diameter Signaling Router Network Impact Report, Release 8.2

Copyright © 2017, 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, then the following notice is applicable:

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

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

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

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

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

My Oracle Support (MOS) (<https://support.oracle.com>) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

## Table of Contents

<b>1. Introduction.....</b>	<b>6</b>
1.1 Product Compatibility.....	6
1.1.2 DSR 8.2 Incompatibility Software .....	6
1.2 Disclaimer.....	6
1.3 References .....	6
1.4 Acronyms.....	8
<b>2. Overview of DSR 8.2 Features.....</b>	<b>9</b>
2.1 Diameter Security Application .....	10
2.2 Display Mediation Performance Metrics .....	11
2.3 FABR Support for NBloT .....	12
2.4 DSR HP C-Class/Cloud/ Deployment Uses Tekelec Platform Based on OL6.9 .....	12
2.5 License Measurements Feature .....	12
2.6 RBAR Support for NBloT.....	12
2.7 DSR Deployment Using OpenStack Heat DSR VNFDs.....	13
2.8 DSR Merge Table Updates to Limit Merge Scope up to SOAM .....	13
2.9 MMI Updates .....	14
2.10 vSTP (Virtual Signaling Transfer Point) Features .....	14
2.11 Stallion Data Collector Productization .....	15
2.12 Accessibility .....	15
2.13 VE-DSR supports x7-2 .....	15
2.14 Availability Group Enhancement for DSR Site Upgrade .....	16
2.15 Hardware Changes.....	16
2.15.1 Hardware Supported.....	16
2.16 Software Changes .....	17
2.16.1 DSR Release 8.2 .....	17
2.16.2 iDIH 8.2 .....	17
2.16.3 SDS 8.2.....	17
2.17 Firmware Changes .....	17
2.18 Upgrade Overview .....	18
2.18.1 DSR Upgrade Path .....	18
2.18.2 SDS Upgrade Path .....	18
2.18.3 iDIH Upgrade Path.....	19
2.18.4 Upgrade Execution .....	19
2.18.5 Limitations.....	19
2.19 Migration of DSR Data.....	20
<b>3. Feature OAM Changes .....</b>	<b>20</b>
3.1 RBAR support for NBloT .....	20
3.1.1 Description .....	20
3.1.2 Alarm and Event Changes.....	20
3.1.3 GUI Changes .....	21
3.1.4 Added Measurements.....	23
3.2 FABR Support for NBloT .....	23
3.2.1 Description .....	23

3.2.2	Alarm and Event Changes .....	24
3.2.3	GUI Changes .....	24
3.2.4	Added Measurements .....	29
3.3	Machine-to-machine (MMI) Updates .....	30
3.3.1	Description .....	30
3.3.2	Alarm and Event Changes .....	30
3.3.3	GUI Changes .....	30
3.4	Display Mediation Performance Metrics Per Template Using the GUI (Mediation + Signaling) .....	30
3.4.1	Description .....	30
3.4.2	Alarm and Event Changes .....	32
3.4.3	GUI Changes .....	32
3.5	Network Wide Measurements for Licensed Capabilities .....	34
3.5.1	Description .....	34
3.5.2	Alarm and Event Changes .....	35
3.5.3	License Measurements .....	35
3.5.4	GUI Changes .....	37
3.6	vSTP GTT Actions Support .....	40
3.6.1	Description .....	40
3.6.2	MOs and Operations Supported .....	40
3.6.3	Alarm and Event Changes .....	44
3.6.4	Measurements .....	45
3.6.5	GUI Changes .....	45
3.7	vSTP GTT Features (FLOBR, TOBR, MBR) .....	45
3.7.1	Description .....	45
3.7.2	Filters .....	48
3.7.3	MOs and Operations Supported .....	48
3.7.4	vSTP Limitations in DSR 8.2 .....	48
3.7.5	Alarm and Event Changes .....	49
3.7.6	GUI Changes .....	49
3.8	vSTP Scalability .....	50
3.8.1	Description .....	50
3.8.2	Alarm and Event Changes .....	53
3.8.3	GUI Changes .....	53
3.9	Customized Application Framework .....	54
3.9.1	Description .....	54
3.9.2	Alarm and Event Changes .....	54
3.9.3	DSA Vulnerable Message Logging .....	55
3.10	Auto Site Upgrade (ASU) Enhancements .....	56
3.10.1	Description .....	56
3.10.2	Alarm and Event Changes .....	58
3.10.3	GUI Changes .....	58
<b>4.</b>	<b>MEAL Inserts .....</b>	<b>61</b>
4.1	DSR/SDS Release 8.2 MEAL Snapshot .....	62
4.2	MEAL Deltas (8.1.1) .....	62

4.3	MEAL Deltas (8.1)	62
4.4	MEAL Deltas (8.0)	62
4.5	MEAL Deltas (7.3)	62
4.6	MEAL Deltas (7.2)	62
4.7	MEAL Deltas (7.1.1)	62
4.8	MEAL Deltas (7.1)	63
4.9	MEAL Deltas (7.0.1)	63

## List of Tables

Table 1.	Acronyms	8
Table 2.	DSR 8.2 New Features/Enhancements	10
Table 3.	MOs and Support Operations for GTT Actions	40
Table 4.	Supported GTT Modes for TOBR/FLOBR/MBR	47
Table 5.	GTT Selector Key for TOBR/FLOBR/MBR	47
Table 6.	GTT Set Types for TOBR/FLOBR/MBR	48
Table 7.	MOs and Support Operations for GTT Actions	48
Table 8.	ASU Site Upgrade Failure Alarms/Events	58

## List of Figures

Figure 1.	DSR Upgrade Paths	18
Figure 2.	SDS Upgrade Paths	18
Figure 3.	iDIH Upgrade Paths	19
Figure 4.	Call Flow: OpCode, CgPAGT	48
Figure 5.	Supported Topologies	50
Figure 6.	Multiple STP Server in One Server Group	51
Figure 7.	HA Role Shown as Active for All STP Servers	51
Figure 8.	Link and LinkSet	52
Figure 9.	Route, RouteSet, and Destination (RSP)	52
Figure 10.	Sample of Log File	56
Figure 11.	Specialized Fixed Diameter Connections	57
Figure 12.	Specialized Floating Diameter Connections	57
Figure 13.	Specialized Distribution of DSR Features	58
Figure 14.	Site Upgrade Bulk Availability Setting	59
Figure 15.	Site Upgrade SOAM Method Setting	59
Figure 16.	NOAM Upgrade Screen	60
Figure 17.	SOAM Upgrade Screen	60
Figure 18.	Rearrange Cycles Button	61
Figure 19.	Rearrange Cycles Screen	61

## 1. Introduction

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.

### 1.1 Product Compatibility

- DSR 8.2 is compatible with IDIH 7.1, 7.2, 7.3, 7.4, 8.0, and 8.1
- DSR 8.2 is compatible with SDS 7.1, 7.2, 7.3, 7.4, 8.0, and 8.1
- DSR 8.2 is compatible with Platform 7.5

#### 1.1.2 DSR 8.2 Incompatibility Software

The following software elements are not compatible with DSR 8.2 onwards:

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

Note: DAMP Active-Standby Configuration needs to be migrated to DAMP Multi-Active Cluster Configuration prior to DSR 8.2.x or later upgrade or install.

### 1.2 Disclaimer

This document summarizes DSR release 8.2 new and enhancement features as compared to DSR release 8.1, and the operations impacts of these features at a high level. The Feature Requirements Specification (FRS) document remains the defining source for the expected behavior of these features.

Note that feature implementations may change slightly during product testing.

### 1.3 References

DSR Release 8.2 Release Notes and Licensing Information; DSR Planning, Installation, Upgrade, and Disaster Recovery Guides; Cloud Installation and Upgrade Guides; DSR User Guides; SDS User Guides; and IDIH User Guides can be located at:

[https://docs.oracle.com/cd/E88991\\_01/index.htm](https://docs.oracle.com/cd/E88991_01/index.htm)

They include the following:

#### Release Notices and Licensing Information User Manuals

- [1] DSR 8.2.x Release Notice
- [2] DSR 8.2 Licensing Information User Manual

#### DSR Planning, Installation, Upgrade, and Disaster Recovery

- [3] DSR 8.2 Feature Guide
- [4] DSR 8.2 Planning Guide
- [5] DSR C-Class Hardware and Software Installation Procedure 1/2
- [6] DSR C-Class Software Installation and Configuration Procedure 2/2
- [7] DSR Software Upgrade Guide
- [8] DSR Rack Mount Server Installation Guide
- [9] DSR Rack Mount Server Disaster Recovery Guide
- [10] DSR Network Interconnect: Rack Mount Server
- [11] DSR C-Class Disaster Recovery Guide

- [12] DSR/SDS NOAM Failover Guide
- [13] DSR/SDS VM Placement and CPU Socket Pinning Tool
- [14] Diameter Custom Application (DCA) Feature Activation Procedure
- [15] DTLS Feature Activation Procedure
- [16] FABR Feature Activation Procedure
- [17] GLA Feature Activation Procedure
- [18] MAP-Diameter Feature Activation Procedure
- [19] Mediation Feature Activation Procedure
- [20] Policy and Charging DRA Feature Activation Procedure
- [21] RBAR Feature Activation Procedure
- [22] DSR Network Impact Report
- [23] DSR Security Guide
- [24] DSR Security App Using Mediation Example Procedure
- [25] Zero Balance Application User's Guide
- [26] Virtual Network Function Whitepaper

### **Cloud Installation and Upgrade**

- [27] DSR Cloud Installation Guide
- [28] DSR Cloud Software Upgrade Guide
- [29] DSR Cloud Benchmarking Guide
- [30] HEAT Templates
- [31] DSR Cloud Disaster Recovery Guide
- [32] SDS Cloud Installation Guide
- [33] SDS Cloud Disaster Recovery Guide

### **Diameter Signaling Router Core Document Set**

- [34] DSR Getting Started
- [35] Hardware Documentation Roadmap Reference
- [36] Operation, Administration, and Maintenance (OAM) Guide
- [37] Diameter User's Guide
- [38] Communication Agent User's Guide
- [39] Policy and Charging Application User's Guide
- [40] Mediation User's Guide
- [41] Range Based Address Resolution (RBAR) User's Guide
- [42] Full Address Based Resolution (FABR) User's Guide
- [43] Session Binding Repository (SBR) User's Guide
- [44] IP Front End (IPFE) User's Guide
- [45] Diameter Common User's Guide
- [46] MAP-Diameter IWF User's Guide
- [47] RADIUS User's Guide
- [48] SS7/SIGTRAN User's Guide
- [49] Transport Manager User's Guide
- [50] Gateway Location Application (GLA) User's Guide
- [51] Diameter Custom Application (DCA) User's Guide
- [52] Diameter Custom Application (DCA) Programmer's Guide
- [53] Diameter Custom Application (DCA) Steering of Roaming User's Guide

- [54] Diameter Security Application User's Guide
- [55] Alarms and KPIs Reference
- [56] Measurements Reference
- [57] MMI API Specification
- [58] Virtual Signaling Transfer Point (vSTP) User's Guide
- [59] Related Publications Reference
- [60] DSR Compliance Matrix

#### **SDS Database Server Document Set**

- [61] SDS Getting Started
- [62] SDS User's Guide
- [63] SDS Provisioning Interface
- [64] SDS Initial Installation and Configuration Guide
- [65] SDS Software Upgrade Procedure
- [66] SDS Disaster Recovery User's Guide

#### **Integrated Diameter Intelligence Hub (IDIH) Document Set**

- [67] IDIH User's Guide
- [68] IDIH Alarm Forwarding Administrator's Guide
- [69] IDIH Audit Viewer Administrator's Guide
- [70] IDIH Operations, Administration and Maintenance Guide
- [71] IDIH ProTrace User's Guide
- [72] IDIH Log Viewer Administration's Guide

## **1.4 Acronyms**

An alphabetized list of acronyms used in the document

**Table 1. Acronyms**

<b>Acronym</b>	<b>Definition</b>
ASU	Automated Site Upgrade
AVP	Attribute Value Pair
CLI	Command Line Interface
DA-MP	Diameter Agent Message Processor
DEA	Diameter Edge Agent
DRMP	Diameter Routing Message Priority
DSA	Diameter Security Application
EXGSTACK	Eagle Next Generation Stack
FLOBR	Flexible Linkset Optional Based Routing
FRS	Feature Requirements Specification
GTA	Global Title Address
GTT	Global Title Translation
GUI	Graphical User Interface
HSS	Home Subscriber Server
IMI	Internal Management Interface

Acronym	Definition
IOT	Interoperability Tests
KPI	Key Performance Indicator
LTE	Long Term Evolution
MAP	Mobile Application Part
MBR	Map Based Routing
MEAL	Measurements, Events, Alarms, and Logging
MME	Mobility Management Entity
MMI	Man Machine Interface
MO	Managed Object
MP	Message Processor
MPS	Messages Per Second
MSU	Message SIGNAL UNIT
MTC	Machine Type Communication
MTP	Message Transfer Part
NE	Network Element
OAM	Operations, Administration, and Maintenance
OAM&P	Operations, Administration, Maintenance, and Provisioning
PCRF	Policy Control and Charging Rules Function
PDRA	Policy Diameter Relay Agent
PDU	Protocol Data Unit
PMAC	Platform, Management, and Control
PS	Priority Service (NGN-PS)
SOAM	Site OAM
SS7	Signaling System No. 7
TCAP	Transaction Capability Part
TOBR	TCAP Opcode Based Routing
TPD	ORACLE Platform Distribution
VEDSR	Virtualized Engineered DSR
vSTP	Virtual SS7 Signal Transfer Point

## 2. Overview of DSR 8.2 Features

This section provides a high-level overview of the DSR 8.2 release features that may impact OAM interfaces and activities. All documentation can be accessed by going to documentation site at:

[https://docs.oracle.com/cd/E88991\\_01/index.htm](https://docs.oracle.com/cd/E88991_01/index.htm)

or

**docs.oracle.com > Industries > Oracle Communications documentation > Diameter Signaling Router > Release 8.2**

For a list of all features, refer to the **Release Notes** for DSR 8.2 found at the following link:

For additional details on the various features, refer to the **DSR Feature Guide** found at the same link.

For information on upgrade planning and required steps before upgrade, refer to the **DSR Software Upgrade Guide**.

Table 2 lists the features and enhancements that are summarized in the following subsections.

**Table 2. DSR 8.2 New Features/Enhancements**

<b>DSR 8.2 Feature/Enhancement Name</b>
Diameter Security Application
Display Mediation Performance Metrics
FABR Support for NBIoT
DSR HP C-Class/Cloud/ Deployment Uses Tekelec Platform Based on OL6.9
License Measurements Feature
RBAR Support for NBIoT
DSR Deployment Using OpenStack Heat DSR VNFDs
DSR Merge Table Updates to Limit Merge Scope up to SOAM
MMI Updates
vSTP (Virtual Signaling Transfer Point) Features
Stallion Data Collector Productization
Accessibility
VE-DSR supports x7-2
Availability Group Enhancement for DSR Site Upgrade
Hardware Changes
Software Changes
Firmware Changes
Upgrade Overview
Migration of DSR Data

## 2.1 Diameter Security Application

DSR Diameter Security Application (DSA) allows the operator to screen various diameter messages received from roaming partners for possible vulnerabilities.

Name	Description	Scope
POR 23740146 Diameter Security Application (DSA) vulnerable message logging	The application is deployed at DSR acting as DEA for Ingress Messages received from external foreign network and for Egress Messages sent to external foreign network. DSA has implemented various Countermeasures to detect vulnerability in an ingress diameter message from a foreign network. All the Countermeasures are executed in a predefined sequence for detecting vulnerability of the message.	Enhancement request

## 2.2 Display Mediation Performance Metrics

This enhancement displays mediation performance related metrics using the GUI.

Name	Description	Scope
POR 25203514, POR 25866323 Display mediation performance related metrics using the GUI	This enhancement supports mechanism to provide performance related guidance to operators with respect to deploying templates. Specifically, provide an ability to monitor the usage of the processes associated with executing mediation templates.	Enhancement request

## 2.3 FABR Support for NBloT

This enhancement supports extracting external-identifier from user-identifier grouped and device-action AVP.

Name	Description	Scope
POR 23642377, POR 25409460 Able to route Diameter messages based on any of routing entities using FABR	This feature enhances FABR and SDS to understand external-Identifier (alphanumeric) and route messages based on complete match (complete external-ID) or partial match (only domain-ID) based on configuration.	Enhancement request

## 2.4 DSR HP C-Class/Cloud/ Deployment Uses Tekelec Platform Based on OL6.9

Name	Description	Scope
POR 25883974, POR 25884004, POR 25784468	Enhance DSR HP c-class deployments to use a Tekelec Platform (TPD, TVOE, PMAC) based on OL6.9. Enhance DSR cloud deployment to use a Tekelec platform based on OL6.9. This includes DSR guests hosted in OpenStack/KVM and VMware cloud environments.	Enhancement request

## 2.5 License Measurements Feature

This feature lets the user to run on demand and automated reports for licensing utilization for MPS, simultaneous sessions for stateful applications, and for the number of subscribers for FABR.

Name	Description	Scope
POR 19104288 Network wide measurements for licensed capacities	This feature is intended to provide peak information integrated inside historical reports for a given user defined period for licensed capacity inside new measurement report groups for: MPS license, PCA license, number of routing entities in the SDS database.	Enhancement request

## 2.6 RBAR Support for NBloT

RBAR support for extracting external-identifier from user-identifier and device-action grouped AVPs.

Name	Description	Scope
POR 26286901 RBAR — Address resolution based on exact match of external ID POR 23642388 RBAR support for extracting external-identifier from user-identifier grouped AVP POR 26573812 MTC-IWF address resolution for device triggering IOT use case – RBAR support POR 25409468 Tertiary routing entity support in RBAR	With the support for external-identifier in address resolution configuration, RBAR decodes the external-identifier AVP and makes routing decisions by matching the decoded value (comprising of the local identifier and domain identifier) with the configuration. RBAR can be configured to perform an exact match or a longest sub-domain match on the domain identifier. It can also be configured to perform a second level match on the local identifier, which in turn may be exact or range based.	Enhancement request

## 2.7 DSR Deployment Using OpenStack Heat DSR VNFDs

Name	Description	Scope
POR 26050662 DSR deployment procedure using OpenStack Heat DSR VNFDs	<p>This feature adds the following capability to DSR:</p> <ul style="list-style-type: none"> <li>Can be deployed in OpenStack cloud using Heat templates (instruction for generate manual Heat templates are in the Cloud Installation Guide) DSR VNFDs.</li> <li>Bootstrap the NOAM with a bulk XML that does not contain the IP addresses of any other VM, that is, configure servers without IP addresses, server groups without servers, etc.</li> <li>Each VM has an IP address and makes MMI calls to the NOAM to add its IP addresses in the server configuration; has the initial configuration (TKLCCConfigData.sh) from NOAM; and configures and adds itself into the appropriate server group using another MMI call to NOAM.</li> </ul> <p>The feature includes single- and multi-site deployment testing.</p> <p><b>Limitations:</b></p> <ul style="list-style-type: none"> <li>Deployment in DSR 8.2 is supported on OpenStack Mitaka release only.</li> <li>The only VM types supported in DSR 8.2 are the NOAM, SOAM, DA-MP, IPFE, and vSTP-MP.</li> <li>Deployment of spare servers in DSR topology is not supported in DSR 8.2.</li> <li>Deployment of only one pair of IPFE is supported in a signaling node.</li> <li>Only one IPFE TSA (public IP) address is supported. This means SCTP multi-homed connections are not supported through IPFE.</li> <li>The TSA address must be known and included in the DSR signaling node HEAT template before the deployment.</li> <li>No OpenStack security is supported for IPFE and DAMP VMs.</li> </ul>	Enhancement request

## 2.8 DSR Merge Table Updates to Limit Merge Scope up to SOAM

The DSR table merge feature identifies certain merge tables with status data scoped only until the B level.

Name	Description	Scope
POR 19118167 Support merge scope at table level to merge the status data up to NO/SO. POR 19117177 (bug fix) LRGSYS:Status data is being merged to the NO	This feature reduces the total network bandwidth required to merge DSR tables, thereby improving DSR's efficiency in the network.	Enhancement request

## 2.9 MMI Updates

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

Name	Description	Scope
POR 26134326 Machine-to-Machine interface updates	These features continue to enhance/grow the capabilities of the MMI (Machine-to-Machine Interface) feature introduced in DSR release 8.0&8.1. Feature: Support MMI for RBAR Feature: Diameter MMI Updates	Enhancement request

## 2.10 vSTP (Virtual Signaling Transfer Point) Features

The DSR vSTP function supports these features.

Name	Description	Scope
POR 25925997 vSTP minimum 100K MPS per vSTP site capacity POR 25972649 vSTP GTT actions support POR 25972623, POR 25972614 vSTP TCAP opcode-based routing (TOBR) vSTP flexible linkset origin based routing (FLOBR) vSTP MAP Based Routing (MBR)	<p>This feature supports higher traffic capacity requirements, redundancy/diversity at the signaling interfaces, scalable DSR vSTP, and a vSTP comprising more than one active STP-MP servers.</p> <p>This enhancement is about the support of GTT actions in vSTP. The feature covers both signaling and MMI related developments.</p> <p>The supported GTT actions (by priority order) include:</p> <ul style="list-style-type: none"> <li>• Discard (silent)</li> <li>• UDTs</li> <li>• TCAP Error</li> <li>• Forward</li> <li>• Duplicate (vSTP only supports 1 duplicate action in an action set)</li> </ul> <p>vSTP GTT features (TOBR, FLOBR, MBR)</p> <ul style="list-style-type: none"> <li>• TOBR provides vSTP with the ability to route messages based on their operation codes. With TOBR feature, vSTP considers the following information contained in TCAP portion of messages for performing GTT. <ul style="list-style-type: none"> <li>• ITU Messages <ul style="list-style-type: none"> <li>• Message Type/Package Type</li> <li>• Application Context Name</li> <li>• Operation Code</li> </ul> </li> <li>• ANSI Messages <ul style="list-style-type: none"> <li>• Package Type</li> <li>• Operation Code Family</li> <li>• Operation Code Specifier</li> </ul> </li> </ul> </li> <li>• FLOBR supports these two types of routing: <ul style="list-style-type: none"> <li>• <b>Link set based routing:</b> ability to route GTT traffic</li> </ul> </li> </ul>	Enhancement request

Name	Description	Scope
	<p>based on the incoming link set.</p> <ul style="list-style-type: none"> <li>• <b>Flexible routing:</b> ability to route GTT traffic based on a variety of parameters (MTP, SCCP, and TCAP depending on features that are active) in a flexible order on a per-translation basis.</li> </ul> <p>With FLOBR, the user can change default CdPA GTTSET to point to any GTT set type and find the translation flexibly.</p> <ul style="list-style-type: none"> <li>• MBR provides vSTP with the ability to route messages based on their <b>MAP Components</b>. This can be done by adding two new GTT set types. These new GTT set types are linked by OPCODE set type or any of them.</li> <li>• IMSI</li> <li>• MSISDN</li> </ul>	

## 2.11 Stallion Data Collector Productization

Enhance DSR to include the stallion collection tool.

Name	Description	Scope
POR 26181457	Script provides a framework to allow other users to drop a file (at a certain location with pre-defined format) with the set of data to be collected by this script.	Enhancement request

## 2.12 Accessibility

DSR Accessibility feature tracking bugs

Name	Description	Scope
26303016	<b>RBAR &gt; Address Resolutions:</b> Accessibility issues.	Bug fixes
26301746	<b>RBAR &gt; Addresses:</b> Accessibility issues.	
25387034	<b>AVP Dictionary:</b> Confusing use of color for custom dictionary	
25262568	<b>WCAG 1.4.4:</b> MP statistics (SCTP) scroll bars not visible at 100%.	

## 2.13 VE-DSR supports x7-2

VE-DSR supports deployment and operation on Oracle X7-2 RMS. This feature is the maturation of the current rack mount server virtualized DSR solution.

Name	Description	Scope
POR 26358702	<p>This feature is for the RMS and provides support for the newer and higher capacity X7-2 RMS hardware.</p> <p>Ability to activate the DSR Policy and Online Charging Proxy application (PCA) and Full Address Based Resolution (FABR) application in addition to the Relay, RBAR, and SS7 MD-IWF.</p> <p>Footprint reduction taking advantage of the higher capacity of the Oracle X7-2 hardware.</p>	Enhancement request

## 2.14 Availability Group Enhancement for DSR Site Upgrade

Name	Description	Scope
POR 25065437 Availability group enhancement for DSR site upgrade	<p>This feature benefits from the addition of availability groups to identify which servers can, and cannot, be upgraded together. Each available group created by the customer ensures only the servers with that group are upgraded together.</p> <p>This helps eliminate or minimize upgrade-induced traffic outages.</p> <p>The availability groups are based on the place and place association concepts that already exist.</p>	Enhancement request

## 2.15 Hardware Changes

### 2.15.1 Hardware Supported

Hardware	Comment
HP BL460c Gen 8, Gen 8_v2	c-Class
HP BL460c Gen 9, Gen 9_v2	c-Class
HP DL360/380 Gen 8, Gen 8_v2	Rack Mount Server
HP DL380 Gen 9, Gen 9_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

**Notes:**

- Gen 9, Gen 9 v2, and Gen 8 v2 hardware are also supported, when purchased by a customer.
- Mixed Sun/HP deployments are not generally supported.

## 2.16 Software Changes

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

Component	Release
TPD 64 Bit	7.5.0.0.0-88.45.0
COMCOL	7.4.0.16.0-13795
PMAC	6.5.0.0.0-65.10.0
TVOE	3.5.0.0.0-88.45.0
AppWorks	8.2.0-82.16.0
EXGSTACK	8.2.0-82.15.0
HP Firmware FUP	2.2.12 (minimum <sup>1</sup> )
Oracle Firmware	3.1.8 (minimum <sup>2</sup> )

### 2.16.1 DSR Release 8.2

DSR release 8.2 inherits all functionality from DSR 8.1.

Component	Release
DSR Release	8.2

DSR 8.2 is compatible with platform 7.5.

### 2.16.2 IDIH 8.2

Component	Release
IDH Release	8.2

DSR 8.2 is compatible with IDIH 7.1, 7.2, 7.3., 7.4, 8.0, and 8.1

### 2.16.3 SDS 8.2

Component	Release
SDS Release	8.2

DSR 8.2 is compatible with SDS 7.1, 7.2, 7.3, 7.4, 8.0, and 8.1.

**Note:** Upgrade SDS before the DSR. SDS release 8.2 is compatible with DSR releases 7.1, 7.2, 7.3, 7.4, 8.0, 8.1, and 8.2.

## 2.17 Firmware Changes

Firmware release guidance is provided in the DSR 8.2 Release Notice, which can be found at the following link:

[https://docs.oracle.com/cd/E88991\\_01/index.htm](https://docs.oracle.com/cd/E88991_01/index.htm)

---

<sup>1</sup> This represents the minimum release of the HP FUP 2.2.x series to support all content in the platform 7.4 release. The latest firmware release should always be used to address known security issues.

<sup>2</sup> This represents the minimum release of the Oracle firmware series to support all content in the platform 7.4 release. The latest firmware release should always be used to address known security issues.

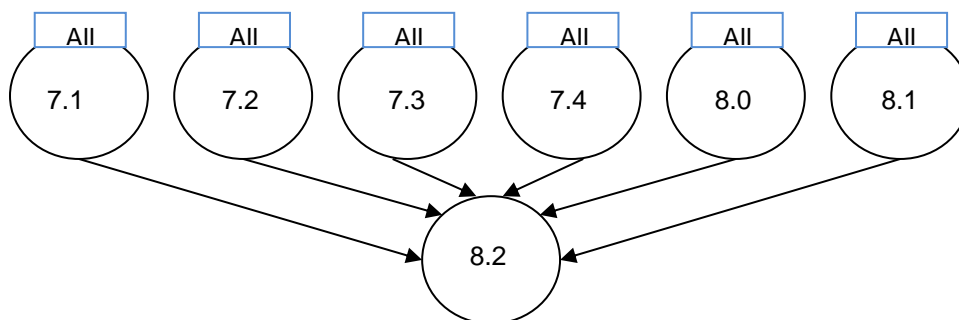
## 2.18 Upgrade Overview

This section provides an overview of the upgrade activities for release 8.2.

Upgrade DSR before SDS. iDIH upgrades can be scheduled before or following the DSR upgrade. If the iDIH upgrade is deferred until after DSR upgrades, then any newly captured elements existing within the upgraded DSR are be decoded by iDIH until after the iDIH upgrade.

### 2.18.1 DSR Upgrade Path

The supported upgrade paths for DSR release 8.2 are:



**Figure 1. DSR Upgrade Paths**

All paths refer to the available releases and all of the associated maintenance releases.



### CAUTION

If the customer deployment has both the FABR and PCA features enabled, then DSR nodes must be upgraded first before upgrading the SDS nodes.



### CAUTION

#### Possible firewall modification required

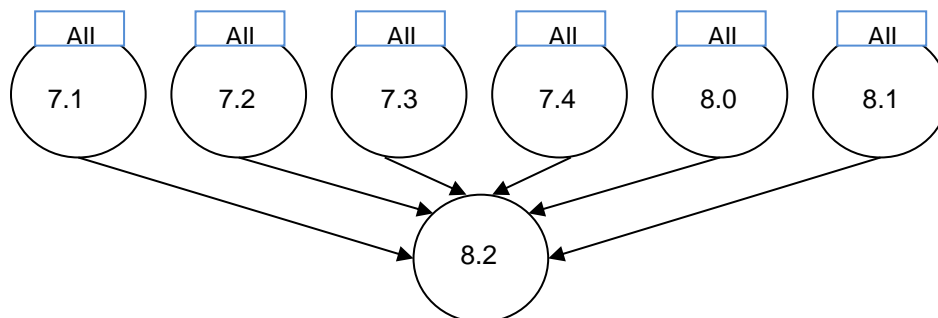
The DSR products have implemented an internal Domain Name System (DNS) to manage name resolution of all servers in the topology.

When upgrading from pre-7.1 releases, ensure firewalls are properly configured for continued system functionality.

Refer to the **DSR Release Upgrade Guide** for specific guidance.

### 2.18.2 SDS Upgrade Path

The supported upgrade paths for SDS 8.2 are:



**Figure 2. SDS Upgrade Paths**

All paths refer to the available releases and all of the associated maintenance releases.



## CAUTION

### Possible firewall modification required

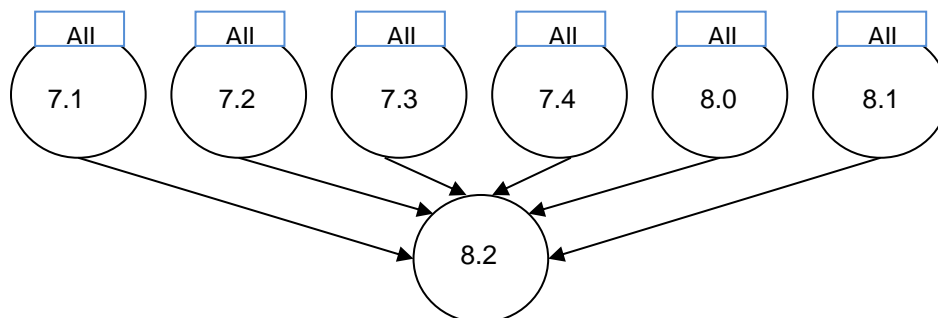
The SDS products have implemented an internal Domain Name System (DNS) to manage name resolution of all servers in the topology.

When upgrading from pre-7.1 releases, ensure firewalls are properly configured for continued system functionality.

Refer to the **SDS Release Upgrade Guide** for specific guidance.

## 2.18.3 iDIH Upgrade Path

The supported upgrade paths for iDIH 8.2 are:



**Figure 3. iDIH Upgrade Paths**

All paths refer to the available releases and all of the associated maintenance releases.

## 2.18.4 Upgrade Execution

With DSR 8.2, there are multiple methods available for upgrading a site. The newest and most efficient way is by using the Automated Site Upgrade feature. As the name implies, this feature upgrades an entire site (SOAMs and all C-level servers) with a minimum of user interaction. Once the upgrade is initiated, the upgrade automatically prepares the server(s), performs the upgrade, and sequences 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 8.2 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 release 8.2 resolves this issue. The user is now instructed to rearrange/add cycles to create a suitable upgrade plan.

## 2.18.5 Limitations

When the AppEventLog file is full, then SOAM/NOAM becomes unstable and undesirable behavior may exist, for example:

- Replication and merging may stop
- GUI access may stop working

Also, upgrades may fail if utilization of the `/var/TKLC/rundb` partition is more than 70%, which may be true in the case of larger an AppEventLog file size (~5.5 GB in size). To prevent these issues,

assign/allocate `/var/TKLC/rundb` size and **AppEventLog** file size in sync, that is, AppEventLog file size (plus some delta for other files like MeasStat) should be always less than 70% of `/var/TKLC/rundb` partition size.

## 2.19 Migration of DSR Data

As in prior releases, the existing DSR data is preserved during the upgrade.

## 3. Feature OAM Changes

At the time of upgrade to DSR 8.2, a number of features and enhancements display 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, and alarms and KPIs.

**Note:** This section covers OAM changes that display after upgrading to the 8.2 release, and does not include changes that display only as new optional features are activated on the system (post-upgrade activity and customer specific).

### 3.1 RBAR support for NBloT

#### 3.1.1 Description

In the 3GPP MTC architecture, there are use cases where the user-identifier or device-action AVP carry an external-identifier instead of an IMSI or MSISDN. To route such messages, there is a business need to be able to perform an external-identifier lookup in RBAR to find the destination and make routing decisions.

The address resolution can be performed based on:

- An exact match on the entire external identifier, or,
- An exact or longest sub-domain match on the domain identifier component of the external identifier, or,
- An exact or longest sub-domain match on the domain identifier component followed by a range match on the local identifier component of the external identifier.
- Tertiary routing entity support in RBAR.

#### 3.1.2 Alarm and Event Changes

New alarms 22411 (Address Range Lookup for Local Identifier skipped) is defined.

### 3.1.3 GUI Changes

#### 3.1.3.1 Address Table

Main Menu > RBAR > Configuration > Address Tables > Insert.

##### Adding a new Address Table

Field	Value	Description
Name *	ext_id_domain_id_table	Unique name of the Address Table. [Default = n/a; Range = A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.] [A value is required.]
Comment	For Domain Resolution	Purpose of the Address Table. [Default = n/a; Range = A 64-character string]
Routing Entity Type *	External Identifier	Type of Routing Entity. A Routing Entity can be a User Identity (IMSI, MSISDN, IMPI, IMPU or External Identifier) or an IP Address associated with the User Equipment (IPv4 or IPv6 Prefix) or UNSIGNED16. [A value is required.]
Routing Entity Component	Domain Identifier	Routing Entity Component of the Address. Entity Type External Identifier: [Default = n/a; Range = Domain Identifier, Local Identifier]

Ok Apply Cancel

#### 3.1.3.2 Addresses

Main Menu > RBAR > Configuration > Addresses > Insert.

##### Adding a new Address

Field	Value	Description
Routing Entity Type *	External Identifier	Routing Entity Type of the Address. [Default = n/a; Range = IMSI, MSISDN, IMPI, IMPU, IPv4, IPv6 Prefix, UNSIGNED16, External Identifier] [A value is required.]
Routing Entity Component	Domain Identifier	Routing Entity Component of the Address. Entity Type External Identifier: [Default = n/a; Range = Domain Identifier, Local Identifier]
Table Name *	ext_id_domain_id_table	Address table of the Address. [Default = n/a; Range = List of configured Table Names] [A value is required.]
Address Type	<input type="radio"/> Range <input type="radio"/> Individual <input checked="" type="radio"/> Domain Name	An address range, an individual address or a domain name. [Default = Range; Range = Range, Individual, Domain Name]
Start Address		Start Address of the range. [Default = n/a; Range = Same range as the Address field except: Entity type External Identifier: Default=n/a; Range = A 1 - 20 digit string. Valid digits are 0 - 9]

End Address	<input type="text"/>	End Address of the range. [Default = n/a; Range = Same range as the Address field except: Entity type External Identifier: Default=n/a, Range = A 1 - 20 digit string. Valid digits are 0 - 9]
Address	<input type="text" value="example.com"/>	<p>Routing Entity Address.</p> <p>Entity type IMSI: [Default=n/a; Range = A 15 digit string. Valid digits are 0 - 9].</p> <p>Entity type MSISDN: [Default=n/a; Range = A 3 - 15 digit string. Valid digits are 0 - 9].</p> <p>Entity type IMPI: [Default=n/a; Range = A 15 digit string. Valid digits are 0 - 9].</p> <p>Entity type MPU: [Default=n/a; Range = A 3 - 15 digit string. Valid digits are 0 - 9].</p> <p>Entity type IPv4: [Default=n/a; Range = A 15 character string in quad-dotted format. Valid characters are numeric (0-9) and dot (.)]</p> <p>Entity type IPv6 Prefix: [Default=n/a; Range = A valid IPv6 address of 39 characters consisting of hexadecimal (0-9, A-F, a-f) and colon (:)]</p> <p>Entity type UNSIGNED16: [Default=n/a; Range = 0 - FFFF]</p> <p>Entity type External Identifier: Domain Identifier: [Default=n/a; Range = A 1 - 128 character string to identify the subscriber's domain. Valid characters are non-blank printable ASCII characters (0x21 - 0x7F)]</p> <p>Entity type External Identifier: Local Identifier: [Default=n/a; Range = A 1 - 128 character string to identify the subscriber within the domain. Valid characters are non-blank printable ASCII characters (0x21 - 0x7F) except ";,:&lt;&gt;@[()\]</p> <p>Note1: This is the IPv6 address part of the IPv6 prefix address.</p> <p>Note2: If the IPv6 address part of the IPv6 prefix is expressed in binary form (converting hexadecimal digits to bits), no bit which is set (value=1), can be at an index that is greater than the configured IPv6 Prefix Length. For example: '0001:0001::' for prefix length 28 is invalid as the 32nd bit is set.</p> <p>Note3: Trailing zeros can be dropped in IPv6 address part of the IPv6 prefix but not leading zeros. For example: '8::' for prefix length 1 is invalid as '8::' is treated as '0008::'.</p>
IPv6 Prefix length	<input type="text"/>	Prefix length of IPv6-prefix address. [Default = n/a; Range = 1 - 128]
Destination *	<input type="text" value="dest1"/> <input type="button" value="v"/>	Destination of the Address. [Default = n/a; Range = List of RBAR Destinations] [A value is required.]
Nested Table Name	<input type="text" value="ext_id_local_id_table"/> <input type="button" value="v"/>	Address Table for next level search using the local Identifier of External Identifier AVP. [Default = n/a; Range = List of Address Table Names of Routing Entity Type External Identifier with sub type Local Identifier]
<input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

### 3.1.3.3 Address Resolutions

Main Menu > RBAR > Configuration > Address Resolutions > Insert.

Tertiary Routing Entity		
Routing Entity	<input type="text" value="- Select -"/> <input type="button" value="v"/>	Type of Routing Entity. A Routing Entity can be a User Identity (MSI, MSISDN, IMPI, MPU or External Identifier) or an IP Address associated with the User Equipment (IPv4, IPv6-prefix or UNSIGNED16 address). [Default = n/a; Range = MSI, MSISDN, IMPI, MPU, IPv4, IPv6 Prefix, UNSIGNED 16, External Identifier]
Primary AVP	<input type="text" value="- Select -"/> <input type="button" value="v"/>	<p>Primary AVP which will be used for extracting the Routing Entity address.</p> <p>Entity types MSI, MSISDN, IMPI, MPU: [Default = n/a; Range = Public Identity, Serviceinfo Subscription-Id(0), Serviceinfo Subscription-Id(1), Serviceinfo Subscription-Id(2), Serviceinfo Subscription-Id(3), Serviceinfo Subscription-Id(4), Subscription-Id(0), Subscription-Id(1), Subscription-Id(2), Subscription-Id(3), Subscription-Id(4), UserIdentity MSISDN, UserIdentity Public Identity, UserName]</p> <p>Entity type IPv4: [Default = n/a; Range = Framed IP Address]</p> <p>Entity type IPv6 Prefix: [Default = n/a; Range = Framed IPv6 Prefix]</p> <p>Entity type UNSIGNED16: [Default = n/a; Range = Serviceinfo PSN to 3GPP-CC]</p> <p>Entity type External Identifier: [Default = n/a; Range = UserIdentifier External-Identifier]</p>
Secondary AVP	<input type="text" value="- Select -"/> <input type="button" value="v"/>	<p>Secondary AVP which will be used for extracting the Routing Entity address.</p> <p>Entity types MSI, MSISDN, IMPI, MPU: [Default = n/a; Range = Public Identity, Serviceinfo Subscription-Id(0), Serviceinfo Subscription-Id(1), Serviceinfo Subscription-Id(2), Serviceinfo Subscription-Id(3), Serviceinfo Subscription-Id(4), Subscription-Id(0), Subscription-Id(1), Subscription-Id(2), Subscription-Id(3), Subscription-Id(4), UserIdentity MSISDN, UserIdentity Public Identity, UserName]</p>
Address Table Name	<input type="text" value="- Select -"/> <input type="button" value="v"/>	Address Table for this Routing Entity Type. [Default = n/a; Range = List of Available configured Address Table names]
<input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

### 3.1.3.4 System Options

Main Menu > RBAR > Configuration > System Options.

Allow Longest Sub-Domain Match	<input type="checkbox"/>	This configuration is used for searching domain addresses. If checked, RBAR will look for the longest matching sub-domain when an exact match is not found using the Domain Identifier component of the External Identifier received in the ingress Diameter message. [Default = No (Unchecked); Range = Yes (Checked), No (Unchecked)]
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

### 3.1.4 Added Measurements

Number	Name	Interval	Description
10325	RxRbarResolExternalIdentifier	5min	Number of request message successfully resolved with routing entity type <b>External Identifier</b> .
10326	RxRbarResolFailExternalIdentifierMatch	5min	Number of request messages received with a valid external-identifier AVP value that did not match a provisioned address.
10327	RxRbarInvalidExternalIdentifierAvp	5min	Number of request messages received with external-identifier AVP that contained an invalid format.
10344	RxRbarResolLocalIdentifier	5min	Number of addresses successfully resolved with routing entity type external identifier using the local identifier component.
10345	RxRbarResolDomainFallback	5min	Number of addresses resolutions that used a destination that was found by the domain identifier search because a subsequent local identifier search was unsuccessful.
10346	RxRbarResolDomainFallback	5min	Number of addresses successfully resolved with routing entity type external identifier because of a longest sub-domain match.
10347	RxRbarLocalIdNotNumeric	5min	Number of request messages for which a range based local identifier resolution could not be attempted because the local identifier value was not numeric.
10348	RxRbarLocalIdExcessLength	5min	Number of request messages for which a range based local identifier resolution could not be attempted because the local identifier value exceeded the max allowed length for range lookup.

## 3.2 FABR Support for NBIoT

### 3.2.1 Description

This feature enhances FABR and SDS to understand and route based on alphanumeric external-identifier.

- Current 3GPP architecture uses identifiers such as IMSI/MSISDN to address the end user devices. With the emergence of MTC architecture, current identifiers (for example, IMSI/ MSISDN) are found to be insufficient to address billions of MTC devices.
- 3GPP specifications have introduced an external-identifier to address the above problem and to resolve addressing limitation in MTC architecture because of the huge penetration of IoT devices.
- For MTC use cases, user-identifier AVP can carry external-identifier value instead of IMSI/ MSISDN on Diameter based MTC interfaces, that is, Tsp, T4, S6m, and Gi/Sgi.

- This feature enhances FABR and SDS to understand external-identifier (alphanumeric) and route messages based on complete match (complete external-ID) or partial match (only domain-ID) based on configuration.

## 3.2.2 Alarm and Event Changes

N/A

## 3.2.3 GUI Changes

FABR related GUIs include:

### 3.2.3.1 Address Resolutions

Main Menu > FABR > Configuration > Address Resolutions > Insert.

- New Tertiary Routing Entity (RE) Configuration section, in addition to existing 2 REs.
- Added AVP UserIdentifier.External-Id under dropdown options Primary AVP, Secondary AVP.
- Added **MTC-HSS** destination type to **Type** options.
- Added selectable checkbox **FallBackSearch**.
- FallBackSearch** when checked (enable) allows routing based on partial match.

Main Menu: FABR > Configuration > Address Resolutions > [Insert]

Adding a new Address Resolution

Blacklist Search Enabled ☐ If checked, IMS/MSISDN blacklist lookup will be performed prior to the full address lookup. If the System Options 'BlackList Search Enabled' is not checked, then this attribute is ignored. [Default = No, Range = n/a]

FallBack Search Enabled ☐ If checked Domain-identifier lookup will be performed, when external identifier lookup did not find an exact match. If the System Options 'Fallback Search Enabled' is not checked, then this attribute is ignored. [Default = No, Range = n/a]

Tertiary Routing Entity

Routing Entity External Identifier ▼ Type of Routing Entity. A Routing Entity can be a User Identity (MSI, MSISDN, IMPI, IMPU) or External Identifier.

Primary AVP UserIdentifier.External-Id ▼ Primary AVP which will be used for extracting the Routing Entity address. Entity types (MSI, MSISDN, IMPI, IMPU) [Default = n/a, Range = Public Identity, ServiceInfo Subscription-Id(0), ServiceInfo Subscription-Id(1), ServiceInfo Subscription-Id(2), ServiceInfo Subscription-Id(3), ServiceInfo Subscription-Id(4), Subscription-Id(0), Subscription-Id(1), Subscription-Id(2), Subscription-Id(3), Subscription-Id(4), UserIdentity MSISDN, UserIdentity Public-identity, UserName] Entity type IPv4 [Default = n/a, Range = Framed IP Address] Entity type IPv6 Prefix [Default = n/a, Range = Framed IPv6 Prefix] Entity type UNSIGNED16 [Default = n/a, Range = ServiceInfo PSInfo 3GPP-CC] Entity type External Identifier [Default = n/a, Range = UserIdentifier.External-Id]

Secondary AVP --Select-- ▼ Secondary AVP which will be used for extracting the Routing Entity address. Entity types (MSI, MSISDN, IMPI, IMPU) [Default = n/a, Range = Public Identity, ServiceInfo Subscription-Id(0), ServiceInfo Subscription-Id(1), ServiceInfo Subscription-Id(2), ServiceInfo Subscription-Id(3), ServiceInfo Subscription-Id(4), Subscription-Id(0), Subscription-Id(1), Subscription-Id(2), Subscription-Id(3), Subscription-Id(4), UserIdentity MSISDN, UserIdentity Public-identity, UserName]

Destination Type MTC-HSS ▼ Type of Destination for this Routing Entity Type. Destination Entity can be IMS-HSS, LTE-HSS, MTC-HSS, PCRF, OCS, OFCS, AAA, USERDEF1 or USERDEF2.

Prefix Search Enabled ☐ If checked, IMS/MSISDN prefix based lookup will be performed, if the full address lookup did not find a match. If the System Options 'Prefix Search Enabled' is not checked, then this attribute is ignored. [Default = No, Range = n/a]

Blacklist Search Enabled ☐ If checked, IMS/MSISDN blacklist lookup will be performed prior to the full address lookup. If the System Options 'BlackList Search Enabled' is not checked, then this attribute is ignored. [Default = No, Range = n/a]

FallBack Search Enabled ☒ If checked Domain-identifier lookup will be performed, when external identifier lookup did not find an exact match. If the System Options 'Fallback Search Enabled' is not checked, then this attribute is ignored. [Default = No, Range = n/a]

OK Apply Cancel

### 3.2.3.2 System Options

Main Menu > FABR > Configuration > System Options.

- Added selectable checkbox FallBackSearch.
- FallBackSearch is enabled when the **FallBackSearch** global option is selected (on FABR's System Option screen) and for the specific AVP and destination type in FABR address resolution screen.

Main Menu: FABR -> Configuration -> System Options

Thu Mar 16 06:04:47 2017

Configuration Options		
Application Unavailable Vendor-Id	<input type="text" value=""/>	successfully routed because of FABR application being unavailable. [Default = n/a; Range = 1 - 4294967295]
Bundling Enabled	<input type="checkbox"/>	If checked, FABR will bundle DP query Events to form a DP Bundled query Event, which will be send to DP Server. [Default= No; Range=n/a]
Maximum Bundle Size	<input type="text" value="5"/>	Maximum number of individual DP query Events that can be bundled. [Default= 5; Range= 2-20]
Prefix Search Enabled	<input type="checkbox"/>	If checked, IMS/MSISDN prefix based lookup will be performed if the full address lookup did not find a match. [Default= No; Range=n/a]
Blacklist Search Enabled	<input type="checkbox"/>	If checked then IMS/MSISDN blacklist lookup will be performed prior to the full address lookup. [Default= No; Range=n/a]
fallback Search Enabled	<input type="checkbox"/>	If checked then Domain-identifier lookup will be performed, when external identifier lookup did not find a exact match [Default= No; Range=n/a]

### 3.2.3.3 Destinations

Main Menu > SDS > Configuration > Destinations > Insert.

Added **MTC-HSS** destination type to **Type** options.

Main Menu

- Administration
- Configuration
  - Options
  - DRMP
  - Connections
  - NAI Hosts
  - Destinations
  - Domain Identifier
  - Destination Map
  - Routing Entities
  - Subscribers
  - Blacklist
- Maintenance
- Help
- Legal Notices
- Logout

Main Menu: SDS -> Configuration -> Destinations [Insert]

Field	Value	Description
Name *	<input type="text"/>	Destination Identifier 1-32 CHARACTERS [A value is required.]
Type	MTC-HSS	Type of destination
FQDN	<input type="text"/>	Fully-Qualified Domain Name 0-255 CHARACTERS
Realm	<input type="text"/>	Realm 0-255 CHARACTERS

Ok Apply Cancel

### 3.2.3.4 Domain Identifier

**Main Menu > SDS > Configuration > Domain Identifier > Insert.**

- This screen is used to insert, delete, and filter domain identifier.
- Domain Identifier name and its default destinations to be provisioned here.
- Domain Identifier can be associated to any destination type. User must specify at-least 1 destination.
- This screen provisions all nine destination types: IMS HSS, LTE HSS, PCRF, OCS, OFCS, AAA, user defined 1, user defined 2, and MTC-HSS.
- Destinations types are automatically populated from Destinations screen inputs.
- Length of domain identifier is 1-128 characters.

Main Menu
Administration
Configuration
Alarms & Events
Security Log
Status & Manage
Measurements
Communication Agent
SDS
Configuration
Options
DRMP
Connections
NAI Hosts
Destinations
Domain Identifier
Destination Map
Routing Entities
Subscribers
Blacklist
Maintenance
Help
Legal Notices
Logout

Main Menu: SDS -> Configuration -> Domain Identifier [Insert]

Field	Value	Description
Domain Identifier *	<input type="text"/>	Domain Identifier hostname 1-128 CHARACTERS [A value is required.]
IMS HSS	None ▼	IMS HSS destination
LTE HSS	None ▼	LTE HSS destination
PCRF	None ▼	PCRF destination
OCS	None ▼	OCS destination
OfCS	None ▼	OfCS destination
AAA	None ▼	AAA destination
User defined 1	None ▼	User defined 1 destination
User defined 2	None ▼	User defined 2 destination
MTC-HSS	None ▼	MTC-HSS

Ok
Apply
Cancel

### 3.2.3.5 Routing Entities

**Main Menu > SDS > Configuration > Routing Entities > Insert/Update.**

- Added **External-Identifier** routing entity type **Type** options.
- Address length of Local Identifier can be 1-128 characters.
- Domain identifier is automatically populated from Domain Identifier screen inputs.
- Inserted label and new **MTC-HSS** destination type to **Type** options.

**Main Menu: SDS -> Configuration -> Routing Entities[Insert/Update]** Tue Jan 09 01:10:47 2018 EST

Field	Value	Description
Type *	External Identifier ▼	The type of routing entity [A value is required.]
Local Identifier *		The routing entity address 1-128 CHARACTERS
Domain Identifier		Address length is 1-128 characters
NAI Host	▼	NAI Host
IMS HSS	None ▼	IMS HSS destination
LTE HSS	None ▼	LTE HSS destination
MTC HSS	None ▼	MTC HSS destination
PCRF	None ▼	PCRF destination
OCS	None ▼	OCS destination
OFCS	None ▼	OFCS destination
AAA	None ▼	AAA destination

### 3.2.3.6 Subscribers

**Main Menu > SDS > Configuration > Subscribers > Insert.**

- Added a new External Identifiers label.
- Added support to allow insertion of up to 10 'External-Identifier's up to a length of 257 characters each per subscriber.
- Inserted label and new **MTC-HSS** destination type to **Type** options.
- MTC-HSS value is automatically populated from Destinations screen inputs, similar to the way LTE-HSS/IMS-HSS is auto populated.
- One subscriber can be associated with six IMSIs, six MSISDNs, and ten external-identifiers.

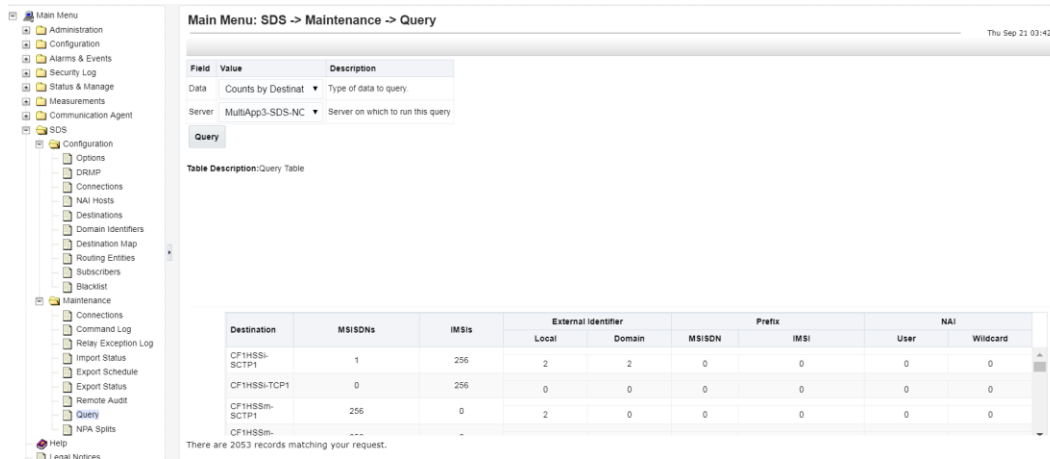
**Main Menu: SDS -> Configuration -> Subscribers [Insert]**

Field	Value	Description
Account ID	<input type="text"/>	Unique identification number associated with this subscriber's account OPTIONAL; 1-26 DIGITS
MSISDNs	<input type="text"/> <div> <input type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="Clear All"/> </div>	MSISDNs associated with this subscriber (maximum of 6) OPTIONAL; 8-15 DIGITS
IMSI	<input type="text"/> <div> <input type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="Clear All"/> </div>	IMSI associated with this subscriber (maximum of 6) OPTIONAL; 10-15 DIGITS
External Identifiers	<input type="text"/> <div> <input type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="Clear All"/> </div>	Allow insertion of 10 External-Identifier's up to a length of 257 character
Inherit Destinations	<input type="checkbox"/>	Whether or not to inherit destinations from the specified routing entities DEFAULT = UNCHECKED
IMS HSS	None <input type="button" value="v"/>	IMS HSS destination
LTE HSS	None <input type="button" value="v"/>	LTE HSS destination
MTC HSS	None <input type="button" value="v"/>	MTC HSS destination

### 3.2.3.7 Query

**Main Menu > SDS > Maintenance > Query.**

- Added new column to display count of external identifiers next to IMSI column.
- Counts query displays the total number of External Identifiers provisioned.



### 3.2.4 Added Measurements

Following measurements are added in FABR:

Number	Name	Interval	Description
10673	RxFabrResolExtId	5min	Number of addresses successfully resolved with full external identifier.
10674	RxFabrResolExtIdDomainId	5min	Number of addresses successfully resolved with the domain identifier received in an external identifier.
10675	RxFabrResolFailExtIdMatch	5min	Number of request messages received with a valid external-identifier avp value that did not match a provisioned address.
10676	TxFabrDbQueryExtId	5min	Number of DB queries sent to DP based on decoded external identifier.

Following measurements are added in SDS:

Number	Name	Interval	Description
4237	DpsExtIdQueriesReceived	5min	Number of external identifier queries received.
4238	DpsExtIdQueriesFailed	5min	Number of external identifier queries with fail response.
4239	DpsExtIdSuccessResponses	5min	Number of external identifier queries with success response.
4240	DpsExtIdDomainIdSuccessResponses	5min	Number of domain identifier part of external identifier queries with success response
4241	DpsExtIdNotFoundResponses	5min	Number of external identifier queries with NotFound response.

### 3.3 Machine-to-machine (MMI) Updates

#### 3.3.1 Description

The feature adds MMI support for the following features:

- MOs included in RBAR: Applications, Exceptions, Destinations, Address Tables, Individual Addresses, Range Addresses, Address Resolution, System Options, Domain Addresses
- MOs included in Diameter: MCCMNC, MCCMNC Mapping, MCC Ranges, Common Application Options

#### 3.3.2 Alarm and Event Changes

N/A

#### 3.3.3 GUI Changes

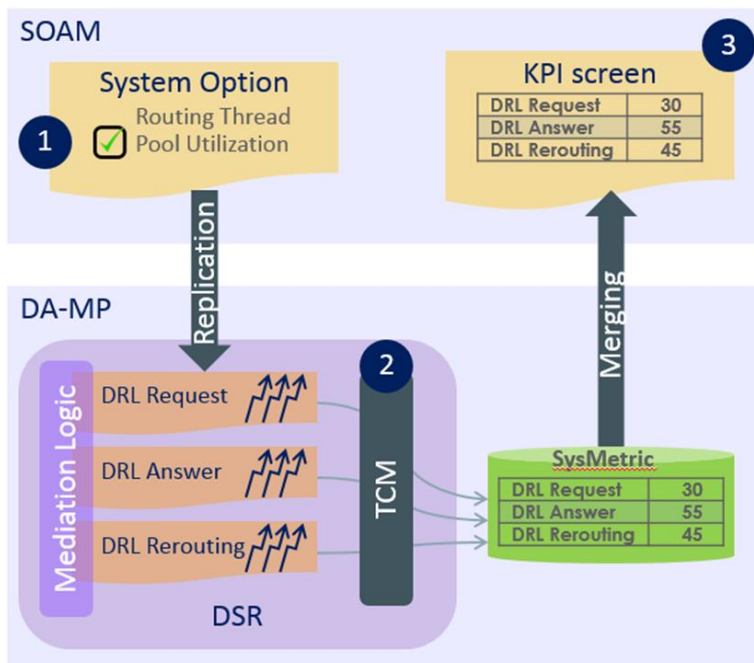
N/A

### 3.4 Display Mediation Performance Metrics Per Template Using the GUI (Mediation + Signaling)

#### 3.4.1 Description

This feature provides the following enhancements:

- Allow user to enable/disable of publishing **Routing Thread Pool Utilization** metrics on GUI.
- Enhance DPI logic to capture the CPU utilization of following thread pools:
  - DRL Request pool
  - DRL Answer pool
  - DRL Rerouting pool
- Display the CPU utilization of these thread pools on GUI (as KPI).
- Display the Average Processing Time per Template on GUI (as KPI).

**Overview of the feature:**

- User can enable this feature through GUI and restart **dsr** application on all DA-MPs (in that site).
- TCM reports CPU utilization of DPI threads that run mediation logic on routable messages.
- GUI displays the CPU utilization on GUI as KPIs.

**EXGSTACK Implementation:**

In this feature, the following enhancements have been made to the EXGSTACK framework to publish the CPU utilization of thread(s) that runs mediation logic:

- Segregate CPU monitoring vs, overload control
  - For example, the user can request CPU monitoring of DPI thread pools without considering it for overload control.
- User can register more than one metric to capture CPU utilization of thread pool.
  - All registered metrics are updated to publish the normalized thread CPU Utilization of that thread pool.
    - This allows user to have individual threshold for each metric (for reporting purpose).
  - However, only one metric can set threshold value for overload control (to keep it backward compatible).

**DPI:**

With DRMP feature (16 priority), DPI registers its DRL tasks (or thread pools) with TCM framework to monitor thread CPU utilization and apply overload control to ensure QoS for high priority messages.

As part of this enhancement, DPI captures the CPU utilization of the following DRL thread pools and publishes them on GUI:

- DRL Request Task
- DRL Answer Task
- DRL Reroute Task

### 3.4.2 Alarm and Event Changes

The **MpRoutingThreadPoolStateMismatch (8020)** alarm is introduced as part of this enhancement. This alarm is raised by DA-MP on which application restart is pending after changing the **Routing Thread Pool Utilization** flag on the **Main Menu > Diameter -> Configuration -> System Options** screen.

Alarm clears when either of following is true:

- User restart DSR application on that DAMP
- User revert back feature state from GUI.

### 3.4.3 GUI Changes

DPI GUI allows user to enable **Routing Thread Pool Utilization** functionality on Site/SOAM level.

- **Main Menu > Diameter -> Configuration -> System Options** screen allows user to enable/disable this functionality.

Default behavior is **Disabled**.

- Application impact: For any change in **Routing Thread Pool Utilization** feature, application restart on all DA-MPs (in that site) is required.
- KPI screen displays **Routing Thread Pool Utilization** as tab under the ThreadUtil group.

#### 3.4.3.1 Diameter System Options Screen

**Main Menu > Diameter > Configuration > System Options.**

Main Menu: Diameter -> Configuration -> System Options

Wed Sep 13 06:28:

Redirect Application Route Table	<input type="text"/>	Application Route Table instance used to process a Redirected Request. [Default = n/a; Range = Any Application Route Table configured on the system.]
Redirect Peer Route Table	<input type="text"/>	Peer Route Table instance used to process a Redirected Request. [Default = n/a; Range = Any Peer Route Table configured on the system.]
Encode FQDN In Lower Case	<input checked="" type="radio"/> Yes <input type="radio"/> No	Whether or not FQDNs should be encoded as configured or in all lower-case. [Default = Yes; Range = Yes, No]
Excessive Reroute Onset Threshold *	<input type="text" value="20"/>	Excessive Reroute Onset Threshold per DA-MP. Excessive Reroute Alarm will be raised when percentage of sum of rerouted messages due to Answer Response and/or Answer Timeout to the total requests forwarded exceeds the Onset Threshold value. [Default = 20%; Range=1%-100%]
Excessive Reroute Abatement Threshold *	<input type="text" value="15"/>	Excessive Reroute Abatement Threshold per DA-MP. Excessive Reroute Alarm will be cleared when percentage of sum of rerouted messages due to Answer Response and/or Answer Timeout to the total requests forwarded is less than this Abatement Threshold for configured Abatement Time. [Default = 15%; Range=0%-99%]
Discard Policy	<input type="text" value="Priority Only"/>	The order of priority and/or color-based traffic segments to consider when determining discard candidates for the application of treatment during Congestion processing. [Default=Priority Only; Range=Color Within Priority, Priority Within Color, Priority Only]
ETG Mode	<input type="text" value="Threshold"/>	Defines the type of message throttling that the system will support for all ETGs. Threshold - Threshold Mode is legacy mode, which configures the congestion level for ETGs and enforce the Requests based on congestion level of ETG. Limit - Limit Mode shapes the egress message rate according to the maximum message and pending transaction rate, the system discard policy, and the current mix of requests by message color and priority. [Default=Threshold; Range=Threshold, Limit]
Routing Thread Pool Utilization Enabled	<input type="checkbox"/>	If checked, Routing Thread Pool Utilization functionality is enabled, which calculates the CPU utilization of thread pools that runs mediation logic on routable messages. If unchecked, Routing Thread Pool Utilization functionality is disabled. Non-operational thread pool performance Alarm will be raised if DA-MP not restarted after enabling the functionality. [Default = Disabled]

### 3.4.3.2 KPI Screen

Main Menu > Status & Manage > KPIs [Group: ThreadUtil].

Main Menu: Status & Manage -> KPIs [Group: ThreadUtil]

Entire-Network

MP1

Routing Thread Pool Util Status

Name	Average	Max	Min	Median	Sum	Desc
DrlRequestTask	0.00	0.00	0.00	0.00	0.00	The percentage of CPU utilization while p...
DrlAnswerTask	0.00	0.00	0.00	0.00	0.00	The percentage of CPU utilization while p...
DrlRerouteTask	0.00	0.00	0.00	0.00	0.00	The percentage of CPU utilization while p...

### 3.4.3.3 Mediation (KPI GUI Screen)

Main Menu > Status & Manage > KPIs [Group: CAPM].

As part of this enhancement, the processing time of each Rule template is shown on the KPI screen as arrayed metrics.

This allows retrieval of the average processing time of each rule template using MMI.

Main Menu: Status & Manage -> KPIs [Group: CAPM]

Mon Sep 04 09:1

Entire-Network

MP1

SO1

Non Arrayed

Processing time [us]

Name	Average	Max	Min	Median	Sum	Desc
Test_Template_Fast	0.00	0.00	0.00	0.00	0.00	Indicates the average processing time of R...
Test_Template_Empty	0.00	0.00	0.00	0.00	0.00	Indicates the average processing time of R...
Test_Template_Empty_Sleep	0.00	0.00	0.00	0.00	0.00	Indicates the average processing time of R...
Test_Template_Slow	0.00	0.00	0.00	0.00	0.00	Indicates the average processing time of R...
Test_Template_Fast_Sleep	0.00	0.00	0.00	0.00	0.00	Indicates the average processing time of R...
Test_Template_Slow_Sleep	0.00	0.00	0.00	0.00	0.00	Indicates the average processing time of R...
test17	0.00	0.00	0.00	0.00	0.00	Indicates the average processing time of R...

## 3.5 Network Wide Measurements for Licensed Capabilities

### 3.5.1 Description

This feature provides the means to run on demand/automated reports for licensing utilization for MPS, simultaneous sessions for stateful applications, and for the number of subscribers for FABR. This feature provides peak information integrated inside historical reports for a given user defined period for licensed capacity inside new measurement report groups for:

- MPS license: MPS Peak information and MPS utilization reporting at a network wide level and for each signaling node of the DSR network
- PCA license: Concurrent session Peaks for PDRA and OC-DRA for the entire DSR network and for each PCA mated site place association of the DSR network. In addition Concurrent session's utilization reporting at a network wide level and mated site place association of the DSR network.
- Number of routing entities in the SDS database

#### Network-Wide MPS License

This license determines the maximum number of network-wide Messages per Second (MPS) allowed by Oracle Communications Diameter Signaling Router. Messages excluded from this measure are:

- Diameter peer-to-peer messages: CER/CEA, DWR/DWA, and DPR/DPA
- Ingress Diameter messages discarded by the DSR due to Overload controls
- Answers received in response to Message Copy

Network-wide MPS is calculated as the peak 5-minute interval of the sum of all signaling nodes managed by a single NOAM node

#### PCA Policy Proxy License

- Network-wide concurrent sessions
  - This license determines the number of concurrent Diameter sessions allowed by Oracle Communications Diameter Signaling Router for policy proxy. Licensing for concurrent sessions is provided on a network-wide basis.
  - Network-wide concurrent sessions are calculated as the peak 5- minute interval of the sum (sum of the averages) of all signaling nodes managed by a single NOAM.
- Concurrent sessions per PCA mated sites place association
  - This license determines the number of concurrent Diameter sessions allowed by Oracle Communications Diameter Signaling Router for policy proxy. Licensing for concurrent sessions is provided per PCA Mated Sites Place Association basis.
  - PCA mated sites concurrent sessions are calculated as the peak 5- minute interval of the signaling node managed by system operations, administration and maintenance per mated site.
  - Note: On-line charging feature has been released after the policy-proxy and while defining the licensing model for that feature the decision was made not to extend this license definition to the on-line charging proxy feature

#### Subscriber Metric License

This license determines the number of subscribers or entities allowed by Oracle Communications Diameter Signaling Router for full address resolution. Licensing for Subscribers is provided on a network-wide basis. Each entry (entity) in the provisioned subscriber database server (SDS) counts as one subscriber.

## 3.5.2 Alarm and Event Changes

N/A

## 3.5.3 License Measurements

This section describes new measurements added as part of the new measurements report, which include historical and peak utilization of the MPS, stateful applications, and subscriber metric licenses.

### MPS Measurements – Network Wide

<b>Id</b>	<b>14097</b>
<b>Name</b>	NetworkMps
<b>Description</b>	Network wide messages per second for the entire network
<b>Dimension</b>	Non Arrayed

<b>Id</b>	<b>14097</b>
<b>Name</b>	NetworkMps
<b>Description</b>	Network wide messages per second for the entire network
<b>Dimension</b>	Non Arrayed

### MPS Measurements – Single Node

<b>Id</b>	<b>14091</b>
<b>Name</b>	NetworkElementMps
<b>Description</b>	Network element messages per second
<b>Dimension</b>	Arrayed on Network Element

### PCA Policy Proxy Measurements – Network Wide

<b>Id</b>	<b>14098</b>
<b>Name</b>	NetworkPdraSessions
<b>Description</b>	Network wide average number of active sessions for P-DRA
<b>Dimension</b>	Non Arrayed

<b>Id</b>	<b>14094</b>
<b>Name</b>	NetworkPeakPdraSessions
<b>Description</b>	Network wide Peak for the average number of sessions for P-DRA
<b>Dimension</b>	Non Arrayed

**PCA Policy Proxy Measurements – Mated Site**

<b>Id</b>	<b>14093</b>
<b>Name</b>	PlaceAssociationPdraSessions
<b>Description</b>	Average number of active sessions per place association for P-DRA
<b>Dimension</b>	Arrayed on Place Association

**PCA Online Charging Proxy Measurements – Network Wide**

<b>Id</b>	<b>14099</b>
<b>Name</b>	NetworkOcdraSessions
<b>Description</b>	Network wide average number of active sessions for OC-DRA
<b>Dimension</b>	Non Arrayed

<b>Id</b>	<b>14096</b>
<b>Name</b>	NetworkPeakOcdraSessions
<b>Description</b>	Network wide Peak for the average number of sessions for OC-DRA
<b>Dimension</b>	Non Arrayed

**PCA Online Charging Proxy Measurements – Mated Site**

<b>Id</b>	<b>14095</b>
<b>Name</b>	PlaceAssociationOcdraSessions
<b>Description</b>	Average number of active sessions per place association for OC-DRA
<b>Dimension</b>	Arrayed on Place Association

**SDS Subscriber Metric Measurement**

<b>Id</b>	<b>4199</b>
<b>Name</b>	ProvRoutingEntityPeak
<b>Description</b>	Peak value calculated by adding count of following Routing entities: <ul style="list-style-type: none"> <li>• IMSI</li> <li>• MSISDN</li> <li>• NAI User</li> <li>• Wildcard NAI User Prefix</li> <li>• IMSI Prefix</li> <li>• MSISDN Prefix</li> </ul>
<b>Dimension</b>	Non-Arrayed

### 3.5.4 GUI Changes

The following screens show how the measurement report looks with DSR release 8.2. These measurements can be pulled by selecting the **License Measurements** group on the Measurements filter screen.

The screenshot shows a web interface for filtering measurements. It is divided into two main sections: 'Measurement' and 'Scope'. In the 'Measurement' section, there are two dropdown menus: the first is set to 'License Measurements' and the second is set to 'Five Minute'. A red rectangular box highlights these two dropdowns. To the right of these dropdowns is a 'Reset' button. In the 'Scope' section below, there are two more dropdown menus: the first is set to 'Network Element' and the second is set to 'Server Group'. To the right of these is another 'Reset' button.

**Note:** With license measurements, the interval should always be set to **Five Minute**.

#### 3.5.4.1 Network-Wide Measurements Report

All the network-wide measurements display on the Non-Arrayed tab of the Measurement Report screen.

- NetworkMps
- NetworkPeakMps
- NetworkPdraSessions
- NetworkPeakPdraSessions
- NetworkOcdraSessions
- NetworkPeakOcdraSessions

<div> <span>Entire-Network</span> <span>E1B11LICDAMP1</span> <span>E1B12LICDAMP2</span> <span>E1B16LICSSBR4</span> <span>E2B1LICNOAM</span> <span>E2B1LICNOAM2</span> <span>E2B2LIC</span> </div>							
<div> <span>NetworkElementMps</span> <span>PlaceAssociationOcdraSessions</span> <span>PlaceAssociationPdraSessions</span> <span>Non-Arrayed</span> </div>							
Timestamp	Percent Complete	NetworkMps	NetworkOcdraSessions	NetworkPdraSessions	NetworkPeakMps	NetworkPeakOcdraSessions	NetworkPeakPdraSessions
2017-08-29 04:05:00 EDT	100	398	9619	6968	0	0	0
2017-08-29 04:10:00 EDT	100	399	9619	6968	0	0	0
2017-08-29 04:15:00 EDT	100	398	9619	6968	0	0	0
2017-08-29 04:20:00 EDT	100	400	9619	6968	400	0	0
2017-08-29 04:25:00 EDT	100	400	9619	6968	0	0	0
2017-08-29 04:30:00 EDT	100	399	9619	6968	0	0	0
2017-08-29 04:35:00 EDT	100	399	9619	6968	0	0	0
2017-08-29 04:40:00 EDT	100	399	9619	6968	0	0	0
2017-08-29 04:45:00 EDT	100	798	9619	6968	0	0	0
2017-08-29 04:50:00 EDT	100	800	9619	6968	800	0	0
2017-08-29 04:55:00 EDT	100	800	9619	6968	800	0	0
2017-08-29 05:00:00 EDT	40	0	0	0	0	0	0

### 3.5.4.2 Network Element MPS Measurement Report

The network element MPS measurement report is on the NetworkElementMPS tab. There is a column for each of the network elements in the DSR topology.

④ **Entire-Network** E1B11LICDAMP1 E1B12LICDAMP2 E1B16LICSSBR4 E2B1LICNOAM E2B1LICNOA

**NetworkElementMps** PlaceAssociationOcdraSessions PlaceAssociationPdcaSessions Non-Arrayed

Timestamp	Percent Complete	LICENSING LAB NOAM	LICENSING SOAM Site1	LICENSING SOAM Site2	LICENSING SOAM Site3	LICENSING LAB DRNOAM
2017-08-29 03:55:00 EDT	100	0	200	199	0	0
2017-08-29 04:00:00 EDT	100	0	200	198	0	0
2017-08-29 04:05:00 EDT	100	0	199	199	0	0
2017-08-29 04:10:00 EDT	100	0	200	199	0	0
2017-08-29 04:15:00 EDT	100	0	199	198	0	0
2017-08-29 04:20:00 EDT	100	0	200	200	0	0
2017-08-29 04:25:00 EDT	100	0	200	199	0	0
2017-08-29 04:30:00 EDT	100	0	199	200	0	0
2017-08-29 04:35:00 EDT	100	0	200	199	0	0
2017-08-29 04:40:00 EDT	100	0	199	200	0	0
2017-08-29 04:45:00 EDT	100	0	399	399	0	0
2017-08-29 04:50:00 EDT	100	0	400	399	0	0

### 3.5.4.3 Place Association Wise Concurrent Policy DRA sessions Measurement Report

The Place Association wise Policy DRA concurrent sessions measurement report is on the PlaceAssociationPdcaSessions tab. There is a column for each of the place associations for Policy and Charging Mated Sites type in the DSR topology.

④ **Entire-Network** E1B11LICDAMP1 E1B12LICDAMP2 E1B16LICSSBR4 E1B7LICSOAM3 E1B8LICDA

**NetworkElementMps** PlaceAssociationOcdraSessions **PlaceAssociationPdcaSessions** Non-Arrayed

Timestamp	Percent Complete	PA SESSION1	PA SESSION2
2017-08-07 06:30:00 EDT	100	4677	4087
2017-08-07 06:35:00 EDT	100	4677	4087
2017-08-07 06:40:00 EDT	100	4677	4087
2017-08-07 06:45:00 EDT	100	6904	6546
2017-08-07 06:50:00 EDT	100	6904	6546
2017-08-07 06:55:00 EDT	100	6904	6546
2017-08-07 07:00:00 EDT	100	6904	6546
2017-08-07 07:05:00 EDT	100	6904	6546

### 3.5.4.4 Place Association Wise Concurrent Online Charging DRA Sessions Measurement Report

The Place Association wise Online Charging DRA concurrent sessions measurement report is on the PlaceAssociationPdraSessions tab. There is a column for each of the place associations for the Policy and Charging Mated Sites type in the DSR topology.

<div> <div>Entire-Network</div> <div>E1B11LICDAMP1</div> <div>E1B12LICDAMP2</div> <div>E1B16LICSSBR4</div> <div>E1B7LICSOAM3</div> <div>E1B8L</div> </div>				
NetworkElementMps	PlaceAssociationOcdraSessions	PlaceAssociationPdraSessions	Non-Arrayed	
Timestamp	Percent Complete	PA SESSION1	PA SESSION2	
2017-08-07 06:30:00 EDT	100	3960	3962	
2017-08-07 06:35:00 EDT	100	3960	3962	
2017-08-07 06:40:00 EDT	100	3960	3962	
2017-08-07 06:45:00 EDT	100	3960	3962	
2017-08-07 06:50:00 EDT	100	5591	5594	
2017-08-07 06:55:00 EDT	100	5591	5594	
2017-08-07 07:00:00 EDT	100	5591	5594	
2017-08-07 07:05:00 EDT	100	5591	5594	

### 3.5.4.5 Subscriber Metric Measurement Report

The SDS License Measurement ProvRoutingEntityPeak displays on an SDS 8.2 (Oracle Communications Diameter Signal Router Full Address Resolution) system on the Non-Arrayed tab of the Measurement screen.

<div> <div>Entire-Network</div> <div>SDS-DP1</div> <div>SDS-DP2</div> <div>SDS-DP3</div> <div>SDS-DP4</div> </div>			
Non-Arrayed			
Timestamp	Percent Complete	ProvRoutingE	
2017-08-28 07:35:00 EDT	100	0	
2017-08-28 07:40:00 EDT	100	86	
2017-08-28 07:45:00 EDT	100	0	
2017-08-28 07:50:00 EDT	100	175	
2017-08-28 07:55:00 EDT	100	0	
2017-08-28 08:00:00 EDT	100	0	
2017-08-28 08:05:00 EDT	100	0	
2017-08-28 08:10:00 EDT	100	0	
2017-08-28 08:15:00 EDT	100	0	
2017-08-28 08:20:00 EDT	100	0	
2017-08-28 08:25:00 EDT	100	219	
2017-08-28 08:30:00 EDT	50	0	

## 3.6 vSTP GTT Actions Support

### 3.6.1 Description

The GTT action feature is used to perform some additional actions on the incoming/translated MSU for the global title translation.

Some GTT actions (for example, UDTs, TCAP Error) inform that a message has been discarded by vSTP.

This is an optional feature and can be used by configuring GTT action, GTT action set, and GTA MO.

There are five types of GTT actions:

- **Discard:** The discard GTT action discards incoming MSU.
- **UDTS:** UDTs GTT action informs that an incoming MSU has been discarded and an error response is sent back with an UDTs error code.
- **TCAP Error:** TCAP error GTT action informs that an incoming MSU has been discarded and an error response is sent back with a TCAP error code.
- **Duplicate:** The duplicate GTT action sends a copy of an incoming/translated MSU to a specified point code as per configuration. The MSU is sent to a translated and a duplicate point code.
- **Forward:** The forward GTT action forwards an incoming/translated MSU to a specified point code as per configuration. The MSU is not forwarded to the translated point code.

If forward GTT action failed, then these default actions are performed as per configurations:

- **Fallback:** Forwards the MSU to a translated point code.
- **Discard:** Discards incoming MSU.
- **UDTS:** Sends a UDTs response with an UDTs error code as per configuration.
- **TCAP Error:** Sends a TCAP error response with a TCAP error code as per configuration.

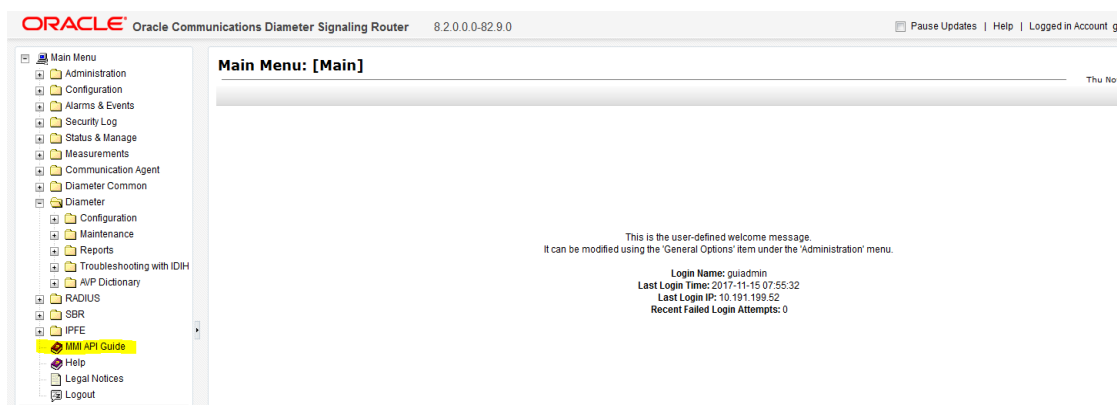
### 3.6.2 MOs and Operations Supported

Table 3 lists the MOs and operations supported for the GTT actions feature.

**Table 3. MOs and Support Operations for GTT Actions**

MO Name	Operations Supported	URI
GTT Action	Insert, update, delete	/vstp/gttactions
GTT Action Set	Insert, update, delete	/vstp/gttactionsets
GTA	Insert, update, delete	/vstp/globaltitleaddresses

Refer to the **MMI API Guide** on active NOAM/SOAM by navigating to **Main Menu >MMI API Guide** on DSR release 8.2 GUI for details about the URI, examples, and parameters about each MO.



### 3.6.2.1 MMI: Discard Action – Insert

Create a file with following content file1:

```
{
  "act": "Disc",
  "actid": "discAct",
  "uimreqd": true
}
```

Execute following command on Active SOAM to insert Discard GTT action (discAct):

```
mmiclient.py /vstp/gttactions -v POST -r /<Absolute path>/<File Name>
```

Example output for insert:

```
[admusr@AD-soa1 ~]$ mmiclient.py /vstp/gttactions -v POST -r /tmp/discard
{
  "data": true,
  "links": {},
  "messages": [],
  "status": true
}
```

### 3.6.2.2 MMI: Discard Action – Display

Execute following command on Active SOAM to display Discard GTT action (discAct):

```
mmiclient.py /vstp/gttactions
```

Example output for display:

```
[admusr@AD-soa1 ~]$ mmiclient.py /vstp/gttactions
{
  "data": [
    {
      "act": "Disc",
      "actid": "discAct",
      "uimreqd": true
    }
  ]
}
```

```

    }
  ],
  "links": {},
  "messages": [],
  "status": true
}

```

### 3.6.2.3 MMI: Discard Action – Update

Create a file with following content file1:

```

{
  "act": "Disc",
  "actid": "discAct",
  "uimreqd": false
}

```

Execute following command on active SOAM to update discard GTT action (discAct):

```
mmiclient.py /vstp/gttactions/<Action Name> -v PUT -r /<Absolute
path>/<File Name>
```

Example output for update:

```

[admusr@AD-soal ~]$ mmiclient.py /vstp/gttactions/discAct -v PUT -r
/tmp/discard
{
  "data": true,
  "links": {},
  "messages": [],
  "status": true
}

```

### 3.6.2.4 MMI: Discard Action – Delete

Execute following command on active SOAM to delete discard GTT action (discAct):

```
mmiclient.py /vstp/gttactions/<Action Name> -v DELETE
```

Example output for delete:

```

[admusr@AD-soal ~]$ mmiclient.py /vstp/gttactions/discAct -v DELETE
No output returned by URI:
https://localhost/mmi/dsr/v2.0/vstp/gttactions/discAct? for 'DELETE'
operation

```

### 3.6.2.5 MMI: GTT Action Set – Insert

Create a file with following content file1:

```

{
  "actid1": "discAct",

```

```
"actsn": "actSet1"
}
```

Execute following command on active SOAM to insert action set (actSet1):

```
mmiclient.py /vstp/gttactionsets -v POST -r /<Absolute path>/<File Name>
```

Example output for insert:

```
[admusr@AD-soa1 ~]$ mmiclient.py /vstp/gttactionsets -v POST -r /tmp/as
{
  "data": true,
  "links": {},
  "messages": [],
  "status": true
}
```

### 3.6.2.6 MMI: GTT Action Set – Display

Execute following command on active SOAM to display GTT action set (actSet1):

```
mmiclient.py /vstp/gttactionsets/<Action Set Name>
```

Example output for display:

```
[admusr@AD-soa1 ~]$ mmiclient.py /vstp/gttactionsets
{
  "data": [
    {
      "actid1": "discAct",
      "actsn": "actSet1"
    }
  ],
  "links": {},
  "messages": [],
  "status": true
}
```

### 3.6.2.7 MMI: GTT Action Set – Update

Insert a new GTT action discAct1 and create a file with following content file1:

```
{
  "actid1": "discAct1",
  "actsn": "actSet1"
}
```

Execute following command on active SOAM to insert discard GTT action (discAct):

```
mmiclient.py /vstp/gttactionsets/<Action Set Name> -v PUT -r /<Absolute
path>/file1
```

Example output for update:

```
[admusr@AD-soa1 ~]$ mmiclient.py /vstp/gttactionsets/actSet1 -v PUT -r /tmp/as
{
    "data": true,
    "links": {},
    "messages": [],
    "status": true
}
```

### 3.6.2.8 MMI: GTT Action Set – Update

Execute following command on Active SOAM to delete GTT Action Set (actSet1):

```
mmiclient.py /vstp/gttactionsets/<Action Set Name> -v DELETE
```

Example output for Delete :

```
[admusr@AD-soa1 ~]$ mmiclient.py /vstp/gttactionsets/actSet1 -v DELETE
No output returned by URI:
https://localhost/mmi/dsr/v2.0/vstp/gttactionsets/actSet1? for 'DELETE'
operation
```

### 3.6.3 Alarm and Event Changes

This alarm supports the GTT action feature.

- Event ID 70286 GTT Duplicate Action processing stopped.
  - This alarm is raised when SCCP thread CPU utilization reaches above configured threshold value and duplicate action processing stopped.
  - This alarm clears when SCCP thread CPU utilization comes to normal state and duplicate action processing resumes.

These events support the GTT action feature.

- Event ID 70277 GTT Action Discarded MSU. This event displays with any one of these reasons:
  - GTT action discard discarded MSU
  - GTT action UDTs discarded MSU
  - GTT action TCAP error discarded MSU
- Event ID 70278 GTT Action Failed. This event displays with any one of these reasons:
  - GTT action duplicate failed
  - GTT action forward failed
  - 3. GTT action failed to send TCAP error

### 3.6.4 Measurements

- Following is the List of per TT measurement supported by GTT Action Feature :
  - ☐ VstpCgpaGTTActionSet - The total number of messages receiving any CgPA GTT action.
  - ☐ VstpCdpaGTTActionSet - The total number of messages receiving any CdPA GTT action.
  - ☐ VstpCgpaDiscardGTTAction - The total number of messages discarded by the DISCARD CgPA GTT Action.
  - ☐ VstpCdpaDiscardGTTAction - The total number of messages discarded by the DISCARD CdPA GTT Action.
  - ☐ VstpCgpaUdtsGTTAction - The total number of messages discarded by the UDTs CgPA GTT Action.
  - ☐ VstpCdpaUdtsGTTAction - The total number of messages discarded by the UDTs CdPA GTT Action.
  - ☐ VstpCgpaTcapErrGTTAction - The total number of messages discarded by the TCAP Error CgPA GTT Action.
  - ☐ VstpCdpaTcapErrGTTAction - The total number of messages discarded by the TCAP Error CdPA GTT Action.
  - ☐ VstpCgpaForwardGTTAction - The total number of messages forwarded by Forward CgPA GTT Action.
  - ☐ VstpCdpaForwardGTTAction - The total number of messages forwarded by Forward CdPA GTT Action.
  - ☐ VstpCgpaDuplicateGTTAction - The total number of messages Duplicated by Duplicate CgPA GTT Action.
  - ☐ VstpCdpaDuplicateGTTAction - The total number of messages Duplicated by Duplicate CdPA GTT Action.

### 3.6.5 GUI Changes

Refer to the **MMI API Guide** on active NOAM/SOAM by navigating to **Main Menu >MMI API Guide** on DSR release 8.2 GUI.

## 3.7 vSTP GTT Features (FLOBR, TOBR, MBR)

### 3.7.1 Description

TOBR, FLOBR, MBR, and 7-Level search for the GTT feature was developed to allow GTT routing based on an incoming linkset, CdPA, and CgPA parameters, on TCAP opcode MAP components (that is, IMSI, MSISDN).

#### 3.7.1.1 FLOBR (Flexible Linkset Operational Based Routing)

FLOBR supports the following two types of routing:

- **Link set based routing:** ability to route GTT traffic based on the incoming link set.
- **Flexible routing:** ability to route GTT traffic based on a variety of parameters (MTP, SCCP, and TCAP, depending on active features) in a flexible order on a per-translation basis.

With the FLOBR feature, the user can change default CdPA GTTSET to point to any GTT set type and find the translation flexibly.

- When GTT mode is **FLOBR CDPA**, CDPA fields in the MSU shall be used for GTT selector search and GTT set shall be taken from “CDPA GTT SET Name” configured in the selector entry.
- When GTT mode is **FLOBR CGPA**, CGPA fields in the MSU shall be used for GTT selector search and GTT set shall be taken from “CGPA GTT SET Name” configured in the selector entry.
- When GTT hierarchy is **FLOBR CDPA and FLOBR CGPA**, GTT selectors shall be searched as defined in 1. If no selector match is found or CDPA GTTSET is not provisioned, GTT selectors shall be searched as defined in 2.

- When GTT hierarchy is **FLOBR CGPA and FLOBR CDPA**, GTT selectors shall be searched as defined in 2. If no selector match is found or CGPA GTTSET is not provisioned, GTT selectors shall be searched as defined in 1.
- If GTT selectors are not found as specified in 1, 2, 3, or 4, then vSTP considers this as translation failure.

With FLOBR, the user can provision a fallback option for each translation that tells the system how to route an MSU under the following conditions:

- Routing when subsequent search failed in FLOBR.
- Routing when same GTT set name is referred more than once.
- Limiting the number of database searches to 7 for FLOBR.

Under the above conditions

- When fallback option in last matched translation is set to **No**, the GTT fails and the MSU is discarded.
- When fallback option in last matched translation is set to **Yes**, the GTT is performed based on that matched entry.

### 3.7.1.2 TOBR (TCAP Opcode Based Routing)

TOBR provides vSTP with the ability to route messages based on their operation codes. With the TOBR feature, vSTP considers the following information contained in TCAP portion of messages for performing GTT.

- ITU Messages
  - Message Type / Package Type
  - Application Context Name
  - Operation Code
- ANSI Messages
  - Package Type
  - Operation Code Family
  - Operation Code Specifier

TOBR supports the following messages:

- ITU TCAP
  - Begin
  - Continue
  - End
  - Abort
  - Unidirectional
- ANSI TCAP
  - Unidirectional
  - QueryWithPermission
  - QueryWithoutPermission
  - Response

- ConversationWithPermission
- ConversationWithoutPermission
- Abort

**Note:** If the message/package type is NOT one of those mentioned in the above list, vSTP treats it as an unknown message type and does not proceed with the decoding.

As part of TOBR feature, vSTP attempts to decode the TCAP portion of all UDT/UDTS/Unsegmented XUDT/Unsegmented XUDTS queries coming to the SCCP layer for GTT. If decoding fails, the message still undergoes GTT using some default values for the TCAP data that denote their absence in the message.

ACN is used for all supported ITU TCAP messages except ABORT. No attempt to retrieve ACN is made for Abort messages. All other supported messages may have a Dialog portion containing Dialogue Request/Unidirectional Dialogue/Dialogue Response PDU, from which the ACN is retrieved. If no Dialog portion is detected, then ACN is assumed to be NONE.

TOBR attempts to find Operation Code (Opcode) in all supported ITU TCAP messages except ABORT. These messages must contain Invoke or Return Result (Last or Not Last) as the first component. If not, Opcode is assumed to be NONE.

TOBR attempts to find Operation Family and Specifier in all supported ANSI TCAP messages (except ABORT) containing an INVOKE component. For all other messages, Family and Opcode are assumed to be NONE.

### 3.7.1.3 MBR (MAP Based Routing)

MBR provides vSTP with the ability to route messages based on their **MAP Components**. This can be done by adding two new GTT set types. These new GTT settypes are linked by OPCODE settype or any of them.

- IMSI
- MSISDN

The GTTsets of the types mentioned above are allowed to be provisioned ONLY in GTA entries from a GTTSet of the type OPCODE or one of the other GTT Set types supported by this feature.

Supported GTT modes selector keys, and set types for TOBR/FLOBR/MBR are listed in the following tables.

**Table 4. Supported GTT Modes for TOBR/FLOBR/MBR**

Feature Name	Modes
TOBR/FLOBR/MBR	FLOBR_CDPA FLOBR_CGPA FLOBR_CDCG FLOBR_CGCD

**Table 5. GTT Selector Key for TOBR/FLOBR/MBR**

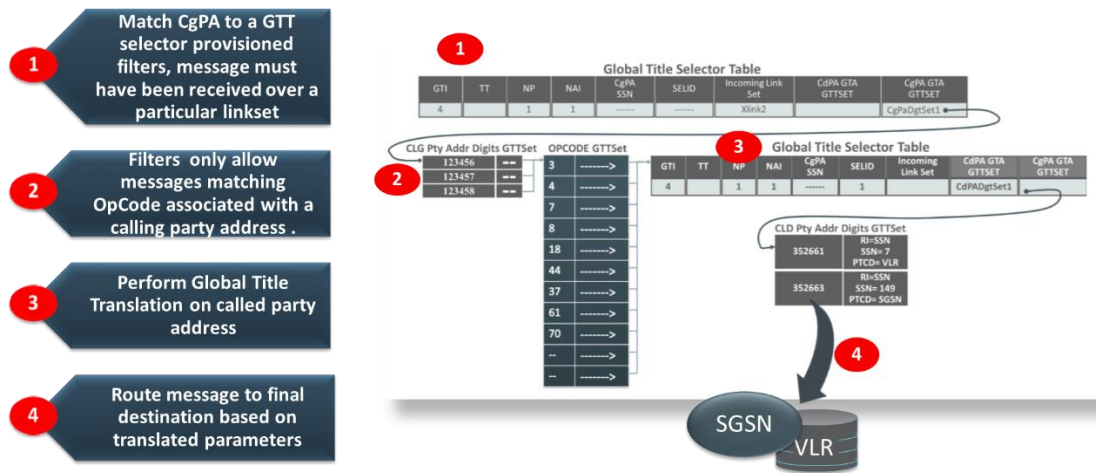
Feature Name	Selector Type	GTI, Domain, TT, (NO and NAI if GTII/GTIN/GTIN24=4)	CgPA SSN	SELID	Link Set ID
TOBR/FLOBR/MBR	CdPA	Yes	No	Yes	Yes
	CgPA	Yes	Yes	Yes	Yes

**Table 6. GTT Set Types for TOBR/FLOBR/MBR**

Feature Name	Available GTT Set Types for:	
	CdPA GTT Selectors	CgPA GTT Selectors
TOBR	Opcode	Same as CdPA GTT selectors
FLOBR	CdPA GTA, CdPA SSN, CgPA GTA, CgPA SSN, Cg PA PC, OPC	Same as CdPA GTT selectors
MBR	Opcode, IMSI, MSISDN	Same as CdPA GTT selectors

### 3.7.2 Filters

Filters MAP messages identified by OpCode coming from a particular origin (calling party address).

**Figure 4. Call Flow: OpCode, CgPAGT**

### 3.7.3 MOs and Operations Supported

Table 7 lists the MOs and operations supported for the TOBR/FLOBR/MBR features.

**Table 7. MOs and Support Operations for GTT Actions**

MO Name	Operations Supported	URI
Linkset	Insert, update, delete	/vstp/linksets
GTT Set	Insert, update, delete	/vstp/gttsets
GTT Selector	Insert, update, delete	/vstp/gttselectors
GTA	Insert, update, delete	/vstp/globaltitleaddresses

### 3.7.4 vSTP Limitations in DSR 8.2

- Default MAPSET and MRNSET are not supported; hence, default MAPSET and MRNSET should not be configured.
- GTT Load Sharing features — FGTTLS, IGTTLS, and WGTTLs are enabled by default.
  - In DSR 8.2, Load Sharing features — FGTTLS, IGTTLS, and WGTTLs are enabled by default. After upgrade there is no impact.
  - In release 8.2, on configuring a GTA rule, if MRNSET is not specified with RI=GT, default value of MRNSET gets taken as 0. In other words, MRNSET is not a mandatory attribute to specify for configuring a GTA rule.

- In DSR8.1, MRNSET was mandatory to be specified for GTA rule configuration when FGTTLS, IGTTLS, and WGTTLs were enabled using MMI.
- Allowed records: Maximum tuple (mapSetId + RSP + SSN) allowed for mapset and mrnset (mrnSetId + RSP) is reduced to 6000 and 3000, respectively.
  - Upgrade from 8.1 to 8.2, customers are requested to delete records which are above the specified limits of MAPSET (6000) and MRNSet (3000).
- Allowed IDs: Allowed range value for mapSetId and mrnSetId is reduced to 6000 and 1500, respectively. This is applicable for /vstp/mapsets, /vstp/mrnsets, /vstp/gttaddresses, and /vstp/gttactions.
  - Release 8.2 has valid MRNSET ID as 0 to 1500 (considering minimum 2 RSPs per MRNSET ID). For MAPSET, valid IDs are 0 to 6000; therefore, before the upgrade, customers are requested to delete MRNSET IDs and MAPSSET IDs that are greater than above limits if they already exist on the setup.
 

**Note:** If not deleted, non-supported MRNSET IDs and MAPSSET IDs cannot be deleted or updated after upgrading to DSR release 8.2.
- DSR 8.2 vSTP does not have any flow control so any event where traffic is put on hold, spike is generated when the traffic is put off hold. Exact traffic spike depends upon the traffic rate and hold duration. Considering these scenarios where traffic is put on hold (Changeover, Changeback, Forced Rerouting, Controlled Rerouting), link TPS should be configured high enough to accommodate the spike.
- Release 8.1 does not allow TPS control at the MP level for configuring links on MP. Whereas, release 8.2 does have an MMI check where the provisioned linkTPS cannot go beyond 10000 per MP.
 

Therefore, a note for users doing an upgrade from release 8.1 to release 8.2: Manually verify the total TPS of links hosted on a MP is not more than 10000 TPS. If it is more than 10000k, reduce it to 10000 TPS, which is required for release 8.2.
- If combined routing is used (that is, two routes with same routing cost are configured for an RSP), then traffic may not be equally distributed when both routes comes available at the same time.
- A maximum of two routes per RSP is supported.

### 3.7.5 Alarm and Event Changes

Several MEAL updates are introduced using the vSTP feature. Refer to section **4.1 DSR/SDS Release 8.2 MEAL Snapshot** for additional details.

### 3.7.6 GUI Changes

N/A

### 3.8 vSTP Scalability

This feature enhancement supports higher traffic capacity requirement (support of 100K+ MPS SS7 traffic at the system level) and redundancy/diversity at the signaling interfaces, and scalable DSR vSTP comprising more than one active STP-MP server.

#### 3.8.1 Description

##### 3.8.1.1 Scalable DSR vSTP Support

- Support N+K active-active scalability model for STP MP servers.
- Support distributed MTP3 and SCCP layer.
- Routing configuration (configured using MMI on SOAM) is shared among all the MP servers.
- Links associated with a given LinkSet can be provisioned across multiple MP servers.
- Link, Linkset, Route, Remote PC, and Remote SSN status are the same on all MP servers.
- Message can ingress on any MP and can egress from same or different MP servers.
- No messages loss occurs when a given MP server is gracefully shut down. Ingress and egress traffic is gracefully re-routed.
- Cross vSTP delay is less than 25ms in case of intra-MP routing.
- Cross vSTP delay is less then 75ms in case of inter-MP routing.

##### 3.8.1.2 Topology Supported

- Only STP-MP servers in a site.
- STP-MP and DA-MP servers in a site.

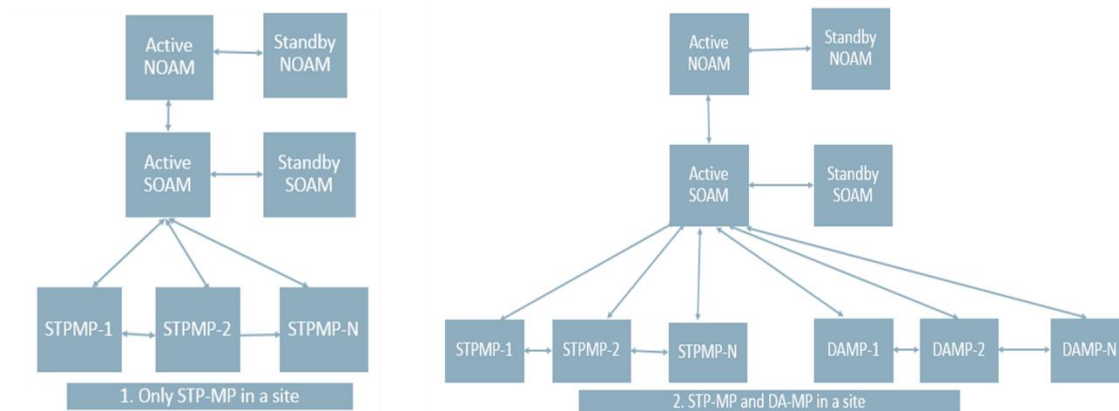


Figure 5. Supported Topologies

### 3.8.1.3 Multiple STP Servers

Multiple STP servers are in one server group configuration as shown in Figure 6.

Main Menu: Configuration -> Server Groups

Filter\* Warning

Server Group Name	Level	Parent	Function	Connection Count	Servers															
NO_SG	A	NONE	DSR (active/standby pair)	1	<div>Network Element: NO_NE</div> <table><tr><th>Server</th><th>Node HA Pref</th><th>VIPs</th></tr><tr><td>pvsd2-noa</td><td></td><td></td></tr></table>	Server	Node HA Pref	VIPs	pvsd2-noa											
Server	Node HA Pref	VIPs																		
pvsd2-noa																				
SO1MP_SG1	C	SO_SG1	STP	1	<div>Network Element: SO_NE1</div> <table><tr><th>Server</th><th>Node HA Pref</th><th>VIPs</th></tr><tr><td>pvsd2-so1mp1</td><td></td><td></td></tr><tr><td>pvsd2-so1mp2</td><td></td><td></td></tr><tr><td>pvsd2-so1mp3</td><td></td><td></td></tr><tr><td>pvsd2-so1mp4</td><td></td><td></td></tr></table>	Server	Node HA Pref	VIPs	pvsd2-so1mp1			pvsd2-so1mp2			pvsd2-so1mp3			pvsd2-so1mp4		
Server	Node HA Pref	VIPs																		
pvsd2-so1mp1																				
pvsd2-so1mp2																				
pvsd2-so1mp3																				
pvsd2-so1mp4																				
SO_SG1	B	NO_SG	DSR (active/standby pair)	1	<div>Network Element: SO_NE1</div> <table><tr><th>Server</th><th>Node HA Pref</th><th>VIPs</th></tr><tr><td>pvsd2-soa1</td><td></td><td></td></tr></table>	Server	Node HA Pref	VIPs	pvsd2-soa1											
Server	Node HA Pref	VIPs																		
pvsd2-soa1																				

Figure 6. Multiple STP Server in One Server Group

### 3.8.1.4 HA Status

The HA role should be active for all STP servers as shown in Figure 7.

Main Menu: Status & Manage -> HA

Filter* Mon Nov 20 02:17:21 2017 EST							
Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role	Mate Hostname List	Network Element	Server Role	Active VIPs
pvsd2-soa1	Active	N/A	Active		SO_NE1	System OAM	
pvsd2-so1mp2	Spare	Active	Active	pvsd2-so1mp3 pvsd2-so1mp1 pvsd2-so1mp4	SO_NE1	MP	
pvsd2-so1mp3	Active	Active	Active	pvsd2-so1mp2 pvsd2-so1mp1 pvsd2-so1mp4	SO_NE1	MP	
pvsd2-so1mp1	Standby	Active	Active	pvsd2-so1mp2 pvsd2-so1mp3 pvsd2-so1mp4	SO_NE1	MP	
pvsd2-so1mp4	Spare	Active	Active	pvsd2-so1mp2 pvsd2-so1mp3 pvsd2-so1mp1	SO_NE1	MP	

Figure 7. HA Role Shown as Active for All STP Servers

### 3.8.1.5 Main Routing Configuration

The main routing configuration includes:

- Links (shown in Figure 8)
- Linksets (shown in Figure 8)
- Routes (shown in Figure 9)
- Destination (RSP) and Remote SSN (shown in Figure 9)
- Routing configuration done at SOAM is replicated to all MP servers.
- All MP servers update their RT-DB based on routing configuration as per DBCA notifications.
- All MP servers of the cluster have the same view of routing configuration at any time.

**Note:** There may be some replication/propagation delay (in ms).

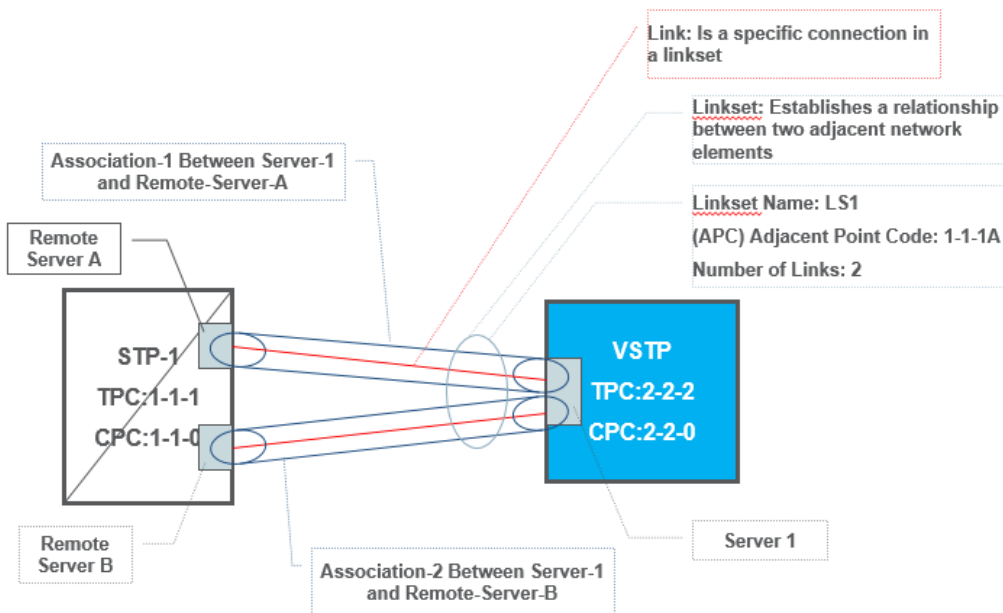
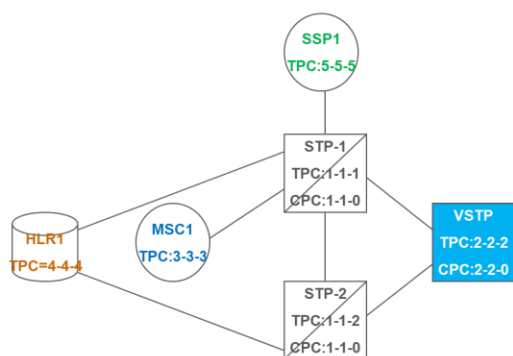


Figure 8. Link and LinkSet



- A Route is a path to a destination (RSP)
- A RouteSet is a collection of routes to a destination (RSP)
- Note: a path is an informal word for a linkset
- Note: a destination is an informal word for an RSP

For this example we define...

1. RSP: name=MSC1, PC=3-3-3
2. RSP: name=HLR1, PC=4-4-4
3. RSP: name=SSP1, PC=5-5-5
4. RSP: name=STP-1, PC=1-1-1
5. RSP: name=STP-2, PC=1-1-2
6. LS: name=LS1, APC=1-1-1
7. LS: name=LS2, APC=1-1-2
8. ROUTE: RSP=MSC1, LS=LS1, cost=10
9. ROUTE: RSP=MSC1, LS=LS2, cost=20
10. ROUTE: RSP=HLR1, LS=LS1, cost=5
11. ROUTE: RSP=HLR1, LS=LS2, cost=5
12. ROUTE: RSP=SSP1, LS=LS1, cost=99
13. ROUTE: RSP=STP-1, LS=LS1, cost=5
14. ROUTE: RSP=STP-1, LS=LS2, cost=15
15. ROUTE: RSP=STP-2, LS=LS1, cost=5
16. ROUTE: RSP=STP-2, LS=LS2, cost=5

Figure 9. Route, RouteSet, and Destination (RSP)

### 3.8.1.6 Scalability MMI

MO Name	URI	Operations Supported
vSTP MP leader	/vstp/mpleader	GET
vSTP capacity	/vstp/capacity	GET
vSTP MP peer status	/vstp/mppeers/status — All MPs /vstp/mppeers/{mp}status — Per MP	GET
vSTP alarm aggregation options	/vstp/alarmaggregationoptions	GET, PUT

**MMI – MP Leader**

- A new MMI API is added to know the active MP leader.
- An MP leader is an MP designated as a leader in an MP server group (/topo/servergroups).
- If no MP leader is present or there are multiple MP leaders, then an error message displays in the HTTP response.
- MMI API — /vstp/mpleader

**MMI – Capacity**

- MMI API gathers the following statistics of vSTP resources:
  - Resource Name
  - Scope is used to define if the given capacity for a given resource is system-wide or per STP-MP.
  - ScopeName defines the MP server hostname.
  - Maximum number of records that can be configured for a given resource name.
  - Used capacity by publishing the number of entries already configured for a given resource name.
  - Available capacity is the count that can be additionally configured for a given resource name.
- MMI API — /vstp/capacity

**MMI – MP Peer Status**

- Returns operational status of all MPs and its corresponding peer MPs. Response data contains the following information for MP status:
  - Name of the vSTP-MP server name reporting the status.
  - Name of the peer vSTP-MP server name.
  - Status can be Available/Unavailable/Degraded/Unknown.
  - CPL (Connection Priority Level) of vSTP-MP server.
  - CPL reason.
- MMI APIs:
  - /vstp/mppeers/status
  - /vstp/mppeers/{mp}/status

**MMI – Alarm Aggregation Options**

- vSTP Alarm Aggregation Options are those configurable threshold values that manage aggregation of vSTP alarms.
- There is a single instance of this resource that contains each of the individual options that can be retrieved and updated.
- MMI API — /vstp/alarmaggregationoptions

**3.8.2 Alarm and Event Changes**

Several MEAL updates are introduced using the vSTP scalability feature. Refer to section 4.1 DSR/SDS Release 8.2 MEAL Snapshot for additional details.

**3.8.3 GUI Changes**

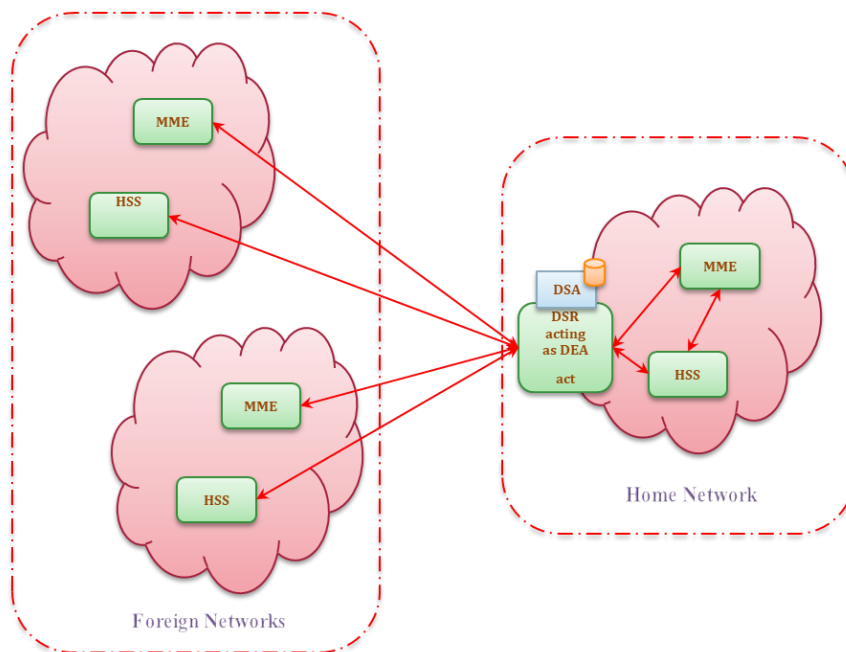
N/A

### 3.9 Customized Application Framework

Customized Application Framework/DSR Security Application (DSA) allows the operator to screen various diameter messages received from roaming partners for possible vulnerabilities.

#### 3.9.1 Description

The application is deployed at DSR acting as DEA for ingress messages received from external foreign network and for egress messages sent to external foreign network.



DSA has implemented various countermeasures to detect vulnerability in an ingress diameter message from a foreign network. All the countermeasures are executed in a predefined sequence for detecting vulnerability of the message.

If a message is found to be vulnerable by a countermeasure, action is performed depending upon the countermeasure's operating mode. Supported operating modes are **Detection Only**, **Detection and Correction by Drop**, and **Detection and Correction by Send Answer**.

The countermeasures can be divided into two categories.

- **Stateful Countermeasure:** Stateful countermeasures require maintaining state data for validating vulnerability of the ingress diameter messages. This state data is maintained in the U-SBR.
- **Stateless Countermeasure:** Stateless countermeasures do not require maintaining state data for validating vulnerability of the ingress diameter message.

Each countermeasure can be enabled or disabled independently for screening the message for vulnerability.

#### 3.9.2 Alarm and Event Changes

Several DSA custom MEALS (Measurements, SysMetric, Alarms) updates are introduced using the vSTP scalability feature. Refer to section 4.1 DSR/SDS Release 8.2 MEAL Snapshot for additional details.

### 3.9.3 DSA Vulnerable Message Logging

#### 3.9.3.1 Configuring Vulnerable message Logging

By default, logging a vulnerable message is disabled (Enable Tracing option of System\_Config\_Options Table).

Before enabling logging, perform these steps on all servers under the SO server group (active/standby/spare) where DSA is running.

1. Log into the SO server using SSH as **admusr**.

2. Create a directory and copy the below list of files to it.

```
> fetchLogDsa.sh    fetchLogDsa.ini    configureScriptAndCronJob.sh
dsa_application.cron    dsa_application_log_rotate
```

3. Change the permission of the file as below

```
chmod 744 configureScriptAndCronJob.sh dsa_application.cron
dsa_application_log_rotate fetchLogDsa.ini fetchLogDsa.sh
```

4. Execute the **configureScriptAndCronJob.sh** script.

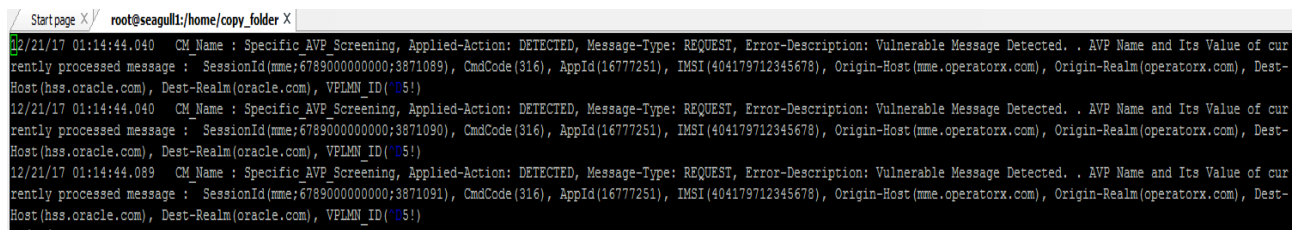
```
sh configureScriptAndCronJob.sh
```

This script sets up a cron job task that runs periodically to fetch the log files from MPs and dumps it at the SO.

Execute step 1 to 4 on the active, standby, and spare SO where the DSA application is running.

#### 3.9.3.2 Logging

- Option has been provided to log vulnerable message details into a log file on MPs. The active SO collects these log files from the MPs and dumps it to the configured path.
- MPs create the file containing vulnerable message details on **/var/TKLC/db/filemgmt/dca\_logs**.
- Each log file may contain a maximum of 30000 vulnerable message details. Also, each log file is open for a maximum of one hour for logging. Once the maximum number of entries is logged into a log file or on the expiry of the 1 hour timeout, the file is closed for logging and a new log file is created for subsequent logs.
- MPs suspend logging if the available disk space of **/var/TKLC/db/filemgmt/dca\_logs** on MP is less than 30%. The logging resumes again once the available disk space increases.
- MPs also suspend logging if the vulnerable message logging rate is above 25000 per second. The logging resumes again once the vulnerable message logging rate decreases.
- Alarm #33316 is raised to notify the user if the logging is suspended on the MP(s). The alarm is cleared once the logging resumes.
- The active SO collects the closed log file from the MP and saves them on **/var/TKLC/db/filemgmt/export/dsa**.
- The active SOAM suspends collecting the logs from MP if the available disk space of **/var/TKLC/db/filemgmt/dsa** on active SO is less than **30%**. The collection resumes again once the available disk space increases.
- The active SOAM also suspends collecting the logs from MP if any error occurs during the log collection process. The collection resumes again once the error is resolved.
- Alarm #33317 is raised to notify the user if log collection is suspended on SO due to any error. The alarm is cleared once the error is resolved.
- Figure 10 shows a snippet of a sample log file.



```

12/21/17 01:14:44.040 CM_Name : Specific_AVP_Screening, Applied-Action: DETECTED, Message-Type: REQUEST, Error-Description: Vulnerable Message Detected. . AVP Name and Its Value of currently processed message : SessionId(mme;6789000000000;3871089), CmdCode(316), AppId(16777251), IMSI(404179712345678), Origin-Host(mme.operatorx.com), Origin-Realm(operatorx.com), Dest-Host(hss.oracle.com), Dest-Realm(oracle.com), VPLMN_ID('US!')
12/21/17 01:14:44.040 CM_Name : Specific_AVP_Screening, Applied-Action: DETECTED, Message-Type: REQUEST, Error-Description: Vulnerable Message Detected. . AVP Name and Its Value of currently processed message : SessionId(mme;6789000000000;3871090), CmdCode(316), AppId(16777251), IMSI(404179712345678), Origin-Host(mme.operatorx.com), Origin-Realm(operatorx.com), Dest-Host(hss.oracle.com), Dest-Realm(oracle.com), VPLMN_ID('US!')
12/21/17 01:14:44.089 CM_Name : Specific_AVP_Screening, Applied-Action: DETECTED, Message-Type: REQUEST, Error-Description: Vulnerable Message Detected. . AVP Name and Its Value of currently processed message : SessionId(mme;6789000000000;3871091), CmdCode(316), AppId(16777251), IMSI(404179712345678), Origin-Host(mme.operatorx.com), Origin-Realm(operatorx.com), Dest-Host(hss.oracle.com), Dest-Realm(oracle.com), VPLMN_ID('US!')

```

Figure 10. Sample of Log File

## 3.10 Auto Site Upgrade (ASU) Enhancements

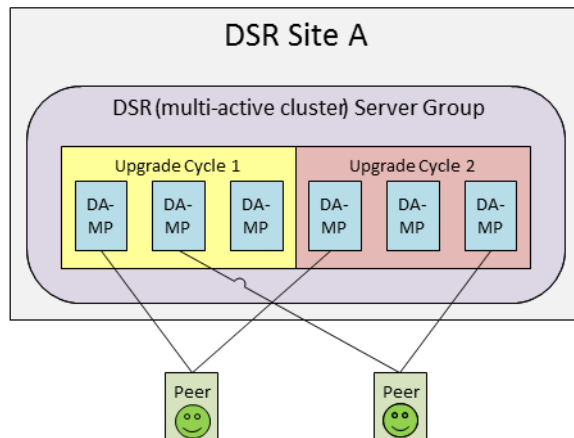
### 3.10.1 Description

- In DSR 8.1, automated upgrades assumed an even distribution of traffic across all DA-MPs within a site's DA-MP server group.
- In DSR 8.1, DSR configuration flexibility allows segmentation of diameter traffic among subsets of DA-MPs within the server group; however, the automated upgrade process is not able to adjust its server selection algorithm to account for these traffic/DA-MP segmentation scenarios. To avoid risk of traffic loss, manual upgrades are recommended for such deployments.
- DSR/SDS 8.2 onwards, additional flexibility is provided to operator to rearrange the servers before sending cycles for the upgrade.
- Automated site upgrade (ASU) provides a **Rearrange Cycles** button to reassign the MP servers between different cycles.
- A **Rearrange Cycles** form provides the capability to remove the MP servers from a cycle to a free pool and add the server to a cycle from free pool.
- SOAM, SBRs, and IPFE servers are not available for selection in the **Rearrange Cycles** form. Upgrades for SOAMs, SBRs, IPFE servers are already handled and they do not need to be rearranged.
- ASU restricts upgrade of servers belonging to same type but present in different cycle until all the servers belonging to same type in a cycle are upgraded.
- The **Rearrange Cycles** form provides the capability to add more cycles to the form using an **Add Cycle** button.
- When you click **Add Cycle**, a new empty select box representing a new cycle is created and the newly added cycle is added to the end of existing cycle. For example, if there are already eight cycles, then **Add Cycle** adds a new select box as ninth cycle.
- ASU provides a **Report** button to print, download, and save the server distribution among the cycles.

DSR 8.2 ASU enhancements solve the upgrade related traffic outage potential due to:

- Specialized fixed diameter connections

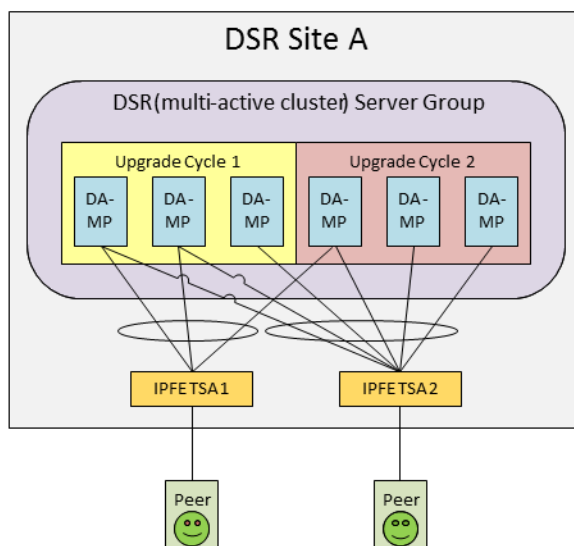
Use the **Rearrange Cycle** option to swap servers between upgrade cycle 1 and cycle 2. An unhappy peer now has redundant connections spawning between two cycles and it is happy again. This peer is NOT isolated now for the duration of the upgrade as shown in Figure 11.



**Figure 11. Specialized Fixed Diameter Connections**

- Specialized floating diameter connections

Swap the servers between two cycles so that not all servers in the subset fall into the same cycle. An unhappy peer now has redundant connections spawning between two cycles and thus it is happy again. This peer is NOT isolated now for the duration of the upgrade as shown in Figure 12.



**Figure 12. Specialized Floating Diameter Connections**

- Specialized distribution of DSR features

Create a new cycle and rearrange the servers to maintain a minimum 50% availability for all applications and so that there is no traffic outage as shown in Figure 13.

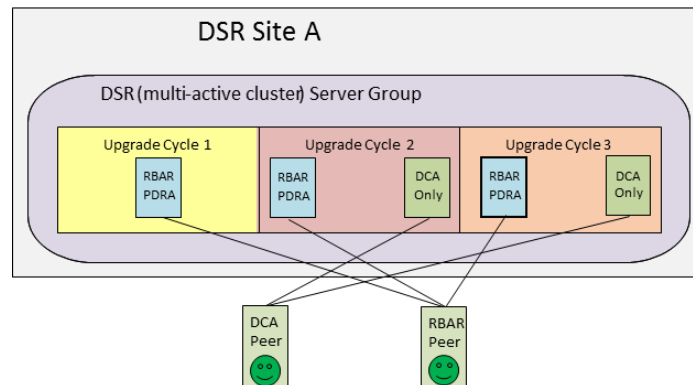


Figure 13. Specialized Distribution of DSR Features

### 3.10.2 Alarm and Event Changes

**Operations – ASU Site Upgrade Failure Handling** — In the event that a server fails to successfully upgrade during the execution of an auto site upgrade, failure events are generated for the server for the associated server group and for the associated site. A server upgrade failure alarm is also raised for each server that failed. These events and alarms are summarized in Table 8.

Table 8. ASU Site Upgrade Failure Alarms/Events

Event/Alarm	Event/Alarm ID	Event/Alarm Text
Server upgrade failure alarm	10134	Server upgrade operation failed
Server upgrade failed event	10133	Server upgrade operation failed
SG upgrade failed event	10123	Server group upgrade operation failed
Site upgrade failed event	10143	Site upgrade operation failed

### 3.10.3 GUI Changes

ASU is designed to upgrade an entire topological site with a minimum of GUI selections with the goal of completing the upgrade within a single four-hour maintenance window. By selecting only a site along with a target ISO, DSR can upgrade the entire site, including SOAMs and all C-level servers, without requiring further user intervention.

#### 3.10.3.1 ASU Pre-Set Options

There are two pre-set options that influence the sequencing of the upgrade automation. These options are located on the General Options screen under **NOAM > Administration**.

- Site Upgrade Bulk Availability
- Site Upgrade SOAM Method

On the **Administration > General Options** screen, **Site Upgrade Bulk Availability** (shown in Figure 14) sets the minimum server availability to values of 0%, 50%, 66%, and 75% for server groups that use the bulk upgrade method. **Minimum availability** means that **at least** the specified percentage of servers, within a server group (like DA-MP) or over a given server group function (like SS7-IWF), remain in service during the upgrade.

Site Upgrade Bulk Availability *	1	Site based upgrade availability for bulk upgrade of MP groups. (0 = none, 1 = 50%, 2 = 66%, 3 = 75%). <b>** Cannot be changed while any site upgrade is running. **</b> [Default = 1; Range = 0-3] [A value is required.]
----------------------------------	---	--

Figure 14. Site Upgrade Bulk Availability Setting

Figure 15 shows another portion of the **Administration > General Options** screen that relates to site upgrade. The **Site Upgrade SOAM Method** controls how the SOAM server group is upgraded, either serial or bulk. If serial mode is selected, all of the servers in the SOAM server group are upgraded serially, in HA order. With this mode, the SOAM upgrade could take as many as four upgrade cycles to complete: Spare > Spare > Standby > Active. Three upgrade cycles are required if there is only a single spare SOAM; and two cycles if there are no spares.

Site Upgrade SOAM Method *	1	Site based upgrade SOAM method. (0 = serial, 1 = bulk). <u>Note:</u> Bulk upgrade will upgrade all non-active SOAM servers together. <b>** Cannot be changed while any site upgrade is running. **</b> [Default = 1; Range = 0-1] [A value is required.]
----------------------------	---	---

Figure 15. Site Upgrade SOAM Method Setting

**Notes:**

- If bulk mode is selected, all of the non-active SOAM servers are upgraded first, followed by the active SOAM. This mode requires at most two upgrade cycles to upgrade all of the SOAMs, regardless of how many spares are present.
- The primary determining factor for a customer to select serial or bulk mode is the desire/requirement to maximize redundancy (serial mode) or minimize upgrade time (bulk mode). The default setting for this option is 1 (bulk).

### 3.10.3.2 ASU Execution

- NOAM upgrade screen
  - One tab level visible for NOAM SG and two tab levels visible for SOAM SG
  - Button options differ between the NOAM and SOAM SG tabs.
  - With the NO server group tab selected, this screen is largely unchanged from the upgrade screen of previous releases. The NO server group servers are displayed with the usual assortment of buttons. Shown in Figure 16, the **Auto Upgrade** button refers to Automated Server Group upgrade, not Automated Site Upgrade. The site upgrade features become available once an SO server group tab is selected

Main Menu: Administration -> Software Management -> Upgrade

Filter\* Tasks

NO\_SG SO\_SG1

Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
awsite2-noa	Backup Needed	Active	Network OAM&P	OAM&P	7.2.0_72.47.5
	Norm	N/A	NO_NE		
awsite2-nob	Backup Needed	Standby	Network OAM&P	OAM&P	7.2.0_72.47.5
	Norm	N/A	NO_NE		

Backup Backup All Checkup Checkup All Auto Upgrade Accept Report Report All

Figure 16. NOAM Upgrade Screen

- Upgrade (site initiate) screen

Figure 17 shows the secondary screen with the **Site Upgrade** button on the SOAM server group tab.

Main Menu: Administration -> Software Management -> Upgrade

Filter\* Tasks

NO\_SG SO\_SG1

Entire Site SO\_SG1 SO1MP\_DAMP SO1MP\_IPFE1 SO1MP\_IPFE2 SO1MP\_IPFE3 SO1MP\_IPFE4 SO1MP\_SBR

Server Group	Function	Upgrade Method	Server Upgrade States	Server Application Versions
SO_SG1	DSR (active/standby pair)	OAM (Bulk)	Ready (3/3)	7.2.0_72.42.1 (3/3)
SO1MP_IPFE2	IP Front End	Bulk (50% availability)	Ready (1/1)	7.2.0_72.42.1 (1/1)
SO1MP_SBR	SBR	Bulk (HA groups)	Ready (2/2)	7.2.0_72.42.1 (2/2)
SO1MP_IPFE1	IP Front End	Bulk (50% availability)	Ready (1/1)	7.2.0_72.42.1 (1/1)
SO1MP_IPFE4	IP Front End	Bulk (50% availability)	Ready (1/1)	7.2.0_72.42.1 (1/1)
SO1MP_DAMP	DSR (multi-active cluster)	Bulk (50% availability)	Ready (4/4)	7.2.0_72.42.1 (4/4)
SO1MP_IPFE3	IP Front End	Bulk (50% availability)	Ready (1/1)	7.2.0_72.42.1 (1/1)

Backup Backup All Checkup Checkup All Site Upgrade Site Accept Report Report All

Figure 17. SOAM Upgrade Screen

- Upgrade (rearrange cycles) screen

Click **Rearrange Cycles** (shown in Figure 18) to rearrange the servers in a cycle and avoid any potential traffic disruptions.

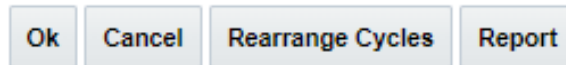


Figure 18. Rearrange Cycles Button

Servers in the upgrade cycle can be rearranged from **NOAM Administration > Software Management > Upgrade [Rearrange Cycles]** (shown in Figure 19).

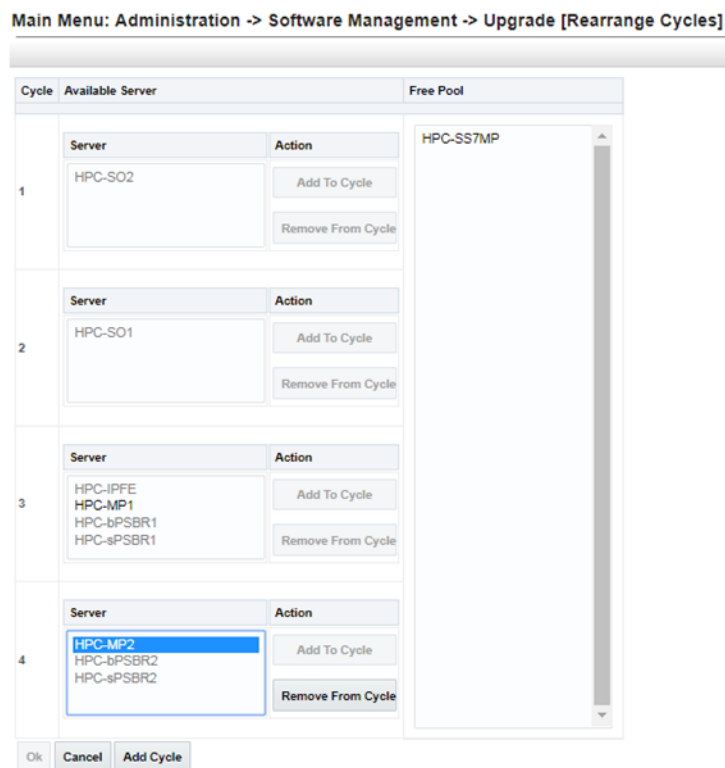


Figure 19. Rearrange Cycles Screen

#### Notes:

- Servers can be removed from the existing cycles and moved to **Free Pool** by selecting the server in a cycle and clicking **Remove From Cycle**.
- Servers can be added to the existing or new cycle by selecting the server from **Free Pool** and clicking **Add To Cycle**.
- While rearranging the servers, the operator can take into consideration the traffic pattern and the deployment scenarios that affect the traffic.

## 4. MEAL Inserts

This section summarizes the changes to alarms, measurements, KPIs, and MIBs. The following inserts pertain to DSR release 8.2 MEAL snapshots and deltas to earlier releases 7.1, 7.1.1, 7.2, 7.3, 8.0, 8.1, and 8.1.1.

The DSR/SDS 8.2 GA release is 8.2.1.0.0-82.17.0.

**Note:** The DSR/SDS 8.2 MEAL snapshot is the same for both GA release 8.2.1.0.0-82.17.0 and for the release build 8.2.0.0.0-82.15.0.

## 4.1 DSR/SDS Release 8.2 MEAL Snapshot



MEAL\_dsr-8.2.0.0.0-8  
2.15.0.xlsx



MEAL\_sds-8.2.0.0.0-8  
2.15.0.xlsx

## 4.2 MEAL Deltas (8.1.1)



MEAL\_dsr-8.1.1.0.0-8  
1.22.0-dsr-8.2.0.0.0-8;



MEAL\_sds-8.1.1.0.0-8  
1.22.0-sds-8.2.0.0.0-8;

## 4.3 MEAL Deltas (8.1)



MEAL\_dsr-8.1.0.0.0-8  
1.20.0-dsr-8.2.0.0.0-8;



MEAL\_sds-8.1.0.0.0-8  
1.20.0-sds-8.2.0.0.0-8;

## 4.4 MEAL Deltas (8.0)



MEAL\_dsr-8.0.0.0.0-8  
0.25.0-dsr-8.2.0.0.0-8;



MEAL\_sds-8.0.0.0.0-8  
0.25.0-sds-8.2.0.0.0-8;

## 4.5 MEAL Deltas (7.3)



MEAL\_dsr-7.3.0.0.0-7  
3.18.0-dsr-8.2.0.0.0-8;



MEAL\_sds-7.3.0.0.0-7  
3.18.0-sds-8.2.0.0.0-8;

## 4.6 MEAL Deltas (7.2)



MEAL\_dsr-7.2.0.0.0-7  
2.25.0-dsr-8.2.0.0.0-8;

## 4.7 MEAL Deltas (7.1.1)



MEAL\_dsr-7.1.1.0.0-7  
1.31.0-dsr-8.2.0.0.0-8;

## 4.8 MEAL Deltas (7.1)



MEAL\_dsr-7.1.0.0-7  
1.24.0-dsr-8.2.0.0-8;

## 4.9 MEAL Deltas (7.0.1)



MEAL\_dsr-7.0.1.0.0-7  
0.28.0-dsr-8.2.0.0-8;