# Oracle® COMMUNICATIONS
## Diameter Signaling Router
DSR Network Impact Report

Release 8.5.0.2

F35176-04

September 2021

# Oracle Diameter Signaling Router DSR Network Impact Report,

# Release 8.5.0.2



F35176-04, September 2021

# Contents


**1 INTRODUCTION ..... 11**

1.1 PURPOSE AND SCOPE ..... 11
1.2 COMPATIBILITY ..... 11
1.2.1 DSR 8.5.0.X PRODUCT COMPATIBILITY ..... 11
1.3 DSR 8.5.X INCOMPATIBILITY FEATURES ..... 11
1.4 DISCLAIMERS ..... 12

**2 OVERVIEW OF DSR 8.5.X FEATURES ..... 13**

2.1 ENHANCEMENTS TO DSR 8.5.0.2.0 ..... 13
*2.1.1 vSTP IPv6 Support ..... 13*
*2.1.2 Segregation of OAM and Replication Traffic Support ..... 13*
*2.1.3 IPFE and Service Mp Scale from Sizing 0 ..... 14*
*2.1.4 vSTP Service MP deployment ..... 14*
*2.1.5 Support of External Group ID for NIDD ..... 14*
*2.1.6 Support of External Group ID for ME ..... 14*
2.2 ENHANCEMENTS TO DSR 8.5.0.1.0 ..... 14
*2.2.1 Mobile Private Network (MPN) vDRA ..... 16*
*2.2.2 Diameter Security Application (DSA) with Session Integrity Validation Check (SIVC) ..... 16*
*2.2.3 Mission Critical Push to Talk (MCPTT) Rx Gateway ..... 17*
*2.2.4 Operate VNF ..... 17*
*2.2.5 Heal VNFM ..... 17*
*2.2.6 Custom Size vDSR Instantiation ..... 18*
*2.2.7 Dual IP stack support for Diameter+SBR flavor through VNFM ..... 18*
*2.2.8 vSTP eLynx TDM card support ..... 18*
*2.2.9 vSTP Home SMS Routing ..... 18*
*2.2.10 vSTP Max and Reserved Link TPS ..... 19*
*2.2.11 vSTP Multi-component TCAP message security ..... 19*
*2.2.12 vSTP Reassembly error for SCCP XUDT message ..... 19*
*2.2.13 vSTP SCTP Firewall Enhancements ..... 20*
*2.2.14 vSTP TCAP Decoding Enhancement ..... 20*
*2.2.15 vSTP Test Mode for GTT actions ..... 20*
*2.2.16 vSTP TIF Enhancements ..... 22*
2.3 ENHANCEMENTS TO DSR 8.5.0 ..... 23
*2.3.1 var Partition size increased by 1GB ..... 24*
*2.3.2 DSR Support of Large vDAMP profile (35K MPS) on OL7 and KVM ..... 24*
*2.3.3 DSA Support for Visualization with Common Security Dashboard ..... 24*
*2.3.4 DSR ZBA and SOR application enhancements to support UDR ..... 24*
*2.3.5 DSR support for Service Based Interface ..... 25*
*2.3.6 VNFM supports modify vnf information ..... 25*
*2.3.7 VNFM Enhancements for VDSR Scaling ..... 25*
*2.3.8 Cloud-init to ensure that DA-MP is not instantiated before SOAM ..... 25*
*2.3.9 VNFM to Support APIGW with the new DB VMs ..... 26*
*2.3.10 SCEF Monitoring Location area Range Configuration for RAC/TAC ..... 26*
*2.3.11 SCEF debugs based on IMSI/External-ID /MSISDN/TltrId ..... 26*
*2.3.12 IDIH support for SCEF ..... 26*
*2.3.13 vSTP Accounting Measurements ..... 27*
*2.3.14 vSTP ELK Integration with Security Dashboard ..... 27*
*2.3.15 vSTP Multiple Linksets and route support ..... 27*
2.4 HARDWARE CHANGES ..... 28
*2.4.1 Hardware Supported ..... 28*
*2.4.2 Hardware Upgrade ..... 28*
2.5 SOFTWARE DETAILS ..... 28
*2.5.1 Software Platform Components in 8.5.X ..... 28*
*2.5.2 iDIH 8.2.3 ..... 29*
*2.5.3 SDS 8.5 ..... 29*
2.6 FIRMWARE CHANGES ..... 30
2.7 UPGRADE OVERVIEW ..... 30
*2.7.1 DSR Upgrade Path ..... 30*

*2.7.2 SDS upgrade path* ..... *30*
*2.7.3 IDIH upgrade path* ..... *31*
*2.7.4 Upgrade Execution* ..... *31*
*2.7.5 Limitations* ..... *31*
2.8 MIGRATION OF DSR DATA ..... 32

**3 RELEASE 8.5 FEATURE OAM CHANGES ..... 33**

3.1 SLS ROTATION ..... 33
*3.1.1 Purpose and Solution* ..... *33*
**3.1.2** *meals* ..... *34*
3.2 SFAPP DYNAMIC LEARNING ..... 36
*3.2.1 purpose and solution* ..... *36*
*3.2.2 meals* ..... *36*
3.3 TIF SUPPORT ..... 38
*3.3.1 purpose and solution* ..... *38*
*3.3.2 meals* ..... *39*
3.4 SEGMENTED XUDT ..... 40
*3.4.1 purpose and solution* ..... *40*
*3.4.2 meals* ..... *41*
3.5 DUPLICATE POINT CODE SUPPORT ..... 44
*3.5.1 purpose and solution* ..... *44*
*3.5.2 meals* ..... *45*
3.6 VSTP IR21 BULK UPLOAD FOR SS7 SECURITY ..... 46
*3.6.1 purpose and solution* ..... *46*
*3.6.2 meals* ..... *47*
3.7 DSA WITH UDR ..... 49
*3.7.1 Upgrade* ..... *50*
*3.7.2 Common security* ..... *50*

**4 MEAL INSERTS ..... 51**

4.1 DSR/SDS 8.5.0.2.0 MEAL SNAPSHOT ..... 51
*4.1.1 MEAL Delta between 8.1.0.0.0 and 8.5.0.2.0* ..... *51*
*4.1.2 MEAL Delta between 8.2.1.0.0 and 8.5.0.2.0* ..... *51*
*4.1.3 MEAL Delta between 8.3.0.0.0 and 8.5.0.2.0* ..... *51*
*4.1.4 MEAL Delta between 8.4.0.0.0 and 8.5.0.2.0* ..... *51*
*4.1.5 MEAL Delta between 8.4.0.3.0 and 8.5.0.2.0* ..... *52*
*4.1.6 MEAL Delta between 8.4.0.5.0 and 8.5.0.2.0* ..... *52*
*4.1.7 MEAL Delta between 8.5.0.0.0 and 8.5.0.2.0* ..... *52*
*4.1.8 MEAL Delta between 8.5.0.1.0 and 8.5.0.2.0* ..... *52*
4.2 DSR/SDS 8.5.0.1.0 MEAL SNAPSHOT ..... 52
*4.2.1 MEAL Delta between 8.1.2.0.0 and 8.5.0.1.0* ..... *52*
*4.2.2 MEAL Delta between 8.2.1.0.0 and 8.5.0.1.0.* ..... *53*
*4.2.3 MEAL Delta between 8.3.0.0.0 and 8.5.0.1.0* ..... *53*
*4.2.4 MEAL Delta between 8.4.0.0.0 and 8.5.0.1.0* ..... *53*
*4.2.5 MEAL Delta between 8.4.0.3.0 and 8.5.0.1.0* ..... *53*
*4.2.6 MEAL Delta between 8.4.0.5.0 to 8.5.0.1.0* ..... *53*
*4.2.7 MEAL Delta between 8.5.0.0.0 to 8.5.0.1.0* ..... *53*
4.3 DSR/SDS 8.5.0.0.0 MEAL SNAPSHOT ..... 54
*4.3.1 MEAL Delta between 8.1.2.0.0 and 8.5.0.0.0* ..... *54*
*4.3.2 MEAL Delta between 8.2.1.0.0 and 8.5.0.0.* ..... *54*
*4.3.3 MEAL Delta between 8.3.0.0.0 and 8.5.0.0.0* ..... *54*
*4.3.4 MEAL Delta between 8.4.0.0.0 and 8.5.0.0.0* ..... *54*
*4.3.5 MEAL Delta between 8.4.0.3.0 and 8.5.0.0.0* ..... *54*
*4.3.6 MEAL Delta between 8.4.0.5.0 to 8.5.0.0.0* ..... *54*

**5 REFERENCE LIST ..... 55**

**List of Figures**

***Figure 1 – DSR Upgrade Paths***.....30
***Figure 2 – SDS Upgrade Paths*** .....31
***Figure 3 – IDIH Upgrade Paths***.....31

**List of Tables**

Table 1: DSR 8.5.0.2.0 New Features/Enhancements ....13
Table 2: vSTP IPv6 Support Feature Description....13
Table 3: Segregation of OAM and Replication Traffic Support Feature Description....13
Table 4 - IPFE and Service Mp Scale from Sizing 0 Feature Description....14
Table 5: vSTP Service MP deployment Feature Description ....14
Table 6 - Support of External Group ID for NIDD Feature Description ....14
Table 7: Support of External Group ID for ME Feature Description ....14
Table 8 - DSR 8.5.0.1.0 New Features/Enhancements ....15
Table 9 – Mobile Private Network (MPN) vDRA Feature Description....16
Table 10 – Diameter Security Application (DSA) with Session Integrity Validation Check (SIVC) Feature Description ....16
Table 11 - Mission Critical Push to Talk (MCPTT) Rx Gateway ....17
Table 12 – Operate VNF Feature Description ....17
Table 13 – Heal VNFM Feature Description....18
Table 14 – Custom Size vDSR Instantiation Feature Description ....18
Table 15 –Dual IP stack support for Diameter+SBR flavor through VNFM Feature Description ....18
Table 16 – vSTP eLynx TDM card support Feature Description ....18
Table 17 – vSTP Home SMS Routing Feature Description....18
Table 18 - vSTP Max and Reserved Link TPS Feature Description....19
Table 19 – vSTP Multi-component TCAP message security Feature Description ....19
Table 20 – vSTP Reassembly error for SCCP XUDT message Feature Description ....20
Table 21 – vSTP SCTP Firewall Enhancements Feature Description ....20
Table 22 – vSTP TCAP Decoding Enhancement Description....20
Table 23 – vSTP Test Mode for GTT actions Feature Description ....20
Table 24 – vSTP TIF Enhancements Feature Description....22
Table 25 - DSR 8.5.0 New Features/Enhancements ....23
Table 26 – var Partition Size Increased Feature Description ....24
Table 27 – Large VDAMP Profile on OL7 and KVM Feature Description ....24
Table 28 - Visualization Server Feature Description....24
Table 29 – ZBA and SOR Support for UDR Feature Description....24
Table 30 – Service-Based Interface Feature Description....25
Table 31 – Modify VNF Information Feature Description....25
Table 32 – vDSR Scaling Feature Description ....25
Table 33 – DA-MP to Instantiate Configuration When SOAM is up Feature Description....25
Table 34 – SCEF Deployment Through MySQL DB Feature Description ....26
Table 35 - Routing Area Code (RAC) and Tracking Area Code (TAC) Range Feature Description....26
Table 36 – SCEF Collects Debugs Based on MSISDN/TltrId/IMSI/External-ID ....26
Table 37 – IDIH Support for SCEF Feature Description....26
Table 38 – vSTP Accounting Measurements Feature Description ....27
Table 39 – vSTP ELK Integration with Security Dashboard Description ....27
Table 40 – vSTP Multiple Linksets and Route Support Feature Description ....27
Table 41 - Hardware Details....28
Table 42 - Software Platform Component Details - 8.5.0.2....28
Table 43 – Software Platform Component Details – 8.5.0.1 ....29
Table 44 - IDIH Details ....29
Table 45 - SDS Details ....29
Table 46 – Measurements....36
Table 47 – Alarms & Events....37
Table 48 – Measurements....39
Table 49 – Alarms & Events....40
Table 50 – Measurements....41
Table 51 – Alarms & Events....42
Table 52 – Measurements....47

# GLOSSARY

| Acronym/Term | Definition |
|---|---|
| APIGW | API Gateway |
| ASGU | Automated Server Group Upgrade |
| AS | Application Server |
| ASU | Automated Site Upgrade |
| AVP | Attribute Value Pair |
| BSBR | Binding SBR |
| CA | Communication Agent |
| CAF | Customized Application Framework |
| CLI | Command Line Interface |
| CLR | Cancel Local Request |
| DA-MP | Diameter Agent Message Processor |
| DAL | Diameter Application Layer |
| DCA | Diameter Custom Application Framework |
| DCL | Diameter Connection Layer |
| DEA | Diameter Edge Agent |
| DPC | Destination Point Code |
| DPL | Data Processor Library |
| DRMP | Diameter Routing Message Priority |
| DPI | Diameter Plug-in |
| DSA | Diameter Security Application |
| DoS | Denial of Service |
| EXGSTACK | Eagle Next Generation Stack |
| vEIR | Virtual Equipment Identity Register |
| ECR | Mobile Equipment-Identity-Check-Request |
| ECA | Mobile Equipment-Identity-Check-Answer |
| FLOBR | Flexible Link set Optional Based Routing |
| GUI | Graphical User Interface |
| GTT | Global title translation |
| GTA | Global title Address |
| HSS | Home Subscriber Server |
| HLR | Home Location register |
| iLO | Integrated Lights Out |
| IMI | Internal Management Interface |
| IPv4 | IPv4 address of the subscriber |
| IPv6 | IPv6 address of the subscriber |
| IMSI | International Mobile Subscriber Identity |
| IMPU | IP Multimedia Public Identity |
| IMPI | IP Multimedia Private Identity |
| IOT | Interoperability Tests |
| KPI | Key Performance Indicator |
| LAI | Location Area Identity |

| Acronym/Term | Definition |
|---|---|
| LTE | Long Term Evolution |
| MAP | Mobile Application Part |
| MBR | Map Based Routing |
| MCC | Mobile Country Code |
| MEAL | Measurements, Events, Alarms, and Logging |
| MME | Mobility Management Entity |
| MMI | Man Machine Interface |
| MP | Message Processor |
| MPS | Messages per Second |
| MS | Mobile Station/Handset |
| MSU | Message signal Unit |
| MSISDN | Mobile Station International Subscriber Directory Number |
| MTC | Machine type communication |
| MTP | Message Transfer Part |
| MO | Managed Object |
| NE | Network Element |
| NGN | Next Generation Networks |
| NGN-PS | NGN Priority Services |
| NIDD | Non-IP data delivery [directly through MME/SGSN] |
| NMS | Network Management System |
| NOAM | Network Operations Administration and Maintenance |
| NF | Network Function |
| NRF | NF Repository Function |
| OAG | Oracle Accessibility Guidelines |
| OAM | Operations, Administration, Maintenance |
| OAM&P | Operations, Administration, Maintenance and Provisioning |
| OCUDR | Oracle Communications User Data Repository |
| OPC | Origin Point Code |
| PDRA | Policy Diameter Relay Agent |
| PCRF | Policy Control and Charging Rules Function |
| PCIMC | Per Connection Ingress Message Control |
| PDU | Protocol Data Unit |
| PDN | Packet Data Network |
| PM&C | Platform, Management and Control |
| POR | Plan of Record |
| PS | Priority Service (NGN-PS) |
| RAN | Radio Access Network |
| ROS | Routing Option Set |
| RSA | Reset Answer |
| RSR | Reset Request |
| SBR | Session Binding Repository |
| SSBR | Session SBR |
| SCEF | Service Capability Exposure Function |
| ScsAsId | String provided by SCS to identify itself in non-3GPP world |

| Acronym/Term | Definition |
|---|---|
| SCEF-MP | Message processing server that will run business login of SCEF/MTC-IWF. (for DSR , it is DA-MP server) |
| SCEF-DB | U-SBR (database server that stores context of SCEF calls) |
| SCS | Service Control Server |
| SOAM | Site Operations Administration and Maintenance |
| SS7 | Signaling System No. 7 |
| STP-MP | Signaling Transfer Point Message Processor |
| SV | Software Version |
| TPD | ORACLE Platform Distribution |
| TCAP | Transaction Capability Part |
| TLTRI | T8 Long Term Transaction Reference ID |
| TTRI | T8 Transaction Reference ID |
| TOBR | TCAP Opcode Based Routing |
| UE | User Equipment |
| USBR | Universal SBR |
| VIP | Virtual IP Address |
| VNF | Virtual Network Functions |
| VNFM | Virtual Network Functions Manager |
| VPLMN | Virtual Public Land Mobile Network |
| VSTP | Virtual SS7 Signal Transfer Point |
| VEDSR | Virtualized Engineered DSR |
| XMI | External Management Interface |
| XSI | External Signaling Interface |

# 1 INTRODUCTION

## 1.1 PURPOSE AND SCOPE

The 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.

## 1.2 COMPATIBILITY

### 1.2.1 DSR 8.5.0.X PRODUCT COMPATIBILITY

- DSR 8.5.0.X is compatible with IDIH 8.2.3
- DSR 8.5.0.X is compatible with VNFM 5.1
- DSR 8.5.0.X is compatible with SDS 8.2, 8.3, 8.3.X, 8.4, 8.4.0.X.Y, and 8.5.
- DSR 8.5.0.X is compatible with APIGW 8.5.0.X
- DSR 8.5.0.X is compatible with TPD 7.7, ComCOL 7.5, AppWorks 9.1, EXGSTACK 9.1, TVOE 3.6, PM&C 6.6, APIGW 8.5 and UDR 12.6.1
- SDS 8.5.0.X is compatible with TPD 7.7, ComCOL 7.5, AppWorks 9.1, EXGSTACK 9.1, TVOE 3.6, and PM&C 6.6.

  **X = PI End Cycle**
  **Y = Patches within the PI Cycle.**

## 1.3 DSR 8.5.X INCOMPATIBILITY FEATURES

The following features have been made incompatible with DSR 8.3 and later.

- Active/Standby DA-MP server architecture (1+1) redundancy model
- MAP-IWF
- GLA
- The "Diameter Security Application (DSA) with Universal-SBR (USBR)" is an obsolete application. Alternatively, the "Diameter Security Application (DSA) with UDR is introduced in DSR 8.4.0.5.0. For information, refer to the Diameter Security Application with UDR User's Guide. Customers using this application must not upgrade DSR software to DSR 8.4.0.5.0 release and must migrate to "DSA with UDR" based application.
- Virtualized Engineered DSR (VEDSR) deployment, which is also known as TVOE based Fully Virtualized Rack Mount Server (FV RMS) Signaling node, is not supported from DSR 8.3 and later. The non-supported network elements of VEDSR are as follows:

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

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

Virtualized Engineered DSR (VEDSR) networks and associated elements need to be migrated to virtual DSR implementation based on KVM with or without OpenStack or VMware prior to DSR 8.3 or 8.4.x upgrade or install.

## 1.4 DISCLAIMERS

This document summarizes Diameter Signaling Router Release 8.5 new and enhancement features as compared to Release 8.4.x, and the operations impact of these features at a high level. The Feature Requirements Specification (FRS) documents remain the defining source for the expected behavior of these features.

# 2 OVERVIEW OF DSR 8.5.X FEATURES

This section provides a high-level overview of the DSR 8.5 release features that may impact OAM interfaces and activities.

For a list of all features, please see Release Notes for DSR 8.5 found at the following link:
**http://docs.oracle.com/en/industries/communications/diameter-signaling-router/index.html**

For additional details of the various features, please refer to the "DSR 8.5 Feature Guide" found at the following link:
**http://docs.oracle.com/en/industries/communications/diameter-signaling-router/index.html**

## 2.1 ENHANCEMENTS TO DSR 8.5.0.2.0

Note: For information about upgrade planning and required steps before the upgrade, refer to the DSR 8.5.0.1.0 Software Upgrade Guide.

***Table 1: DSR 8.5.0.2.0 New Features/Enhancements***

| DSR 8.5.0.2 Feature/Enhancement Name |
|---|
| vSTP IPv6 Support |
| Segregation of OAM and Replication Traffic Support |
| IPFE and Service Mp Scale from Sizing 0 |
| vSTP Service MP deployment |
| Support of External Group ID for NIDD |
| Support of External Group ID for ME |

### 2.1.1 VSTP IPV6 SUPPORT

***Table 2: vSTP IPv6 Support Feature Description***

| Name | Description | Scope |
|---|---|---|
| POR 32406460 | Both IPv4 and IPv6 addresses are supported in IP configuration of local and remote hosts for Signaling links. For more information, see Oracle Communications Diameter Signaling Router Virtual Signaling Transfer Point User's Guide | Enhancement Request |

### 2.1.2 SEGREGATION OF OAM AND REPLICATION TRAFFIC SUPPORT

***Table 3: Segregation of OAM and Replication Traffic Support Feature Description***

| Name | Description | Scope |
|---|---|---|
| | This feature supports separate network for OAM and Replication traffic. For more information, see Oracle Communications Virtual Network Functions Manager Installation and User Guide. | Enhancement Request |

### 2.1.3 *IPFE AND SERVICE MP SCALE FROM SIZING 0*

***Table 4 - IPFE and Service Mp Scale from Sizing 0 Feature Description***

| Name | Description | Scope |
|---|---|---|
| | This feature supports scale from sizing 0 for IPFE and Service Mp VMs. For more information, see Oracle Communications Virtual Network Functions Manager Installation and User Guide. | Enhancement Request |

### 2.1.4 *VSTP SERVICE MP DEPLOYMENT*

***Table 5: vSTP Service MP deployment Feature Description***

| Name | Description | Scope |
|---|---|---|
| | VNFM deploys the Service MP along with vSTP-MP only. This is an optional feature. For more information, see Oracle Communications Virtual Network Functions Manager Installation and User Guide. | Enhancement Request |

### 2.1.5 *SUPPORT OF EXTERNAL GROUP ID FOR NIDD*

***Table 6 - Support of External Group ID for NIDD Feature Description***

| Name | Description | Scope |
|---|---|---|
| POR 30002100 | The group Message Delivery feature allows an SCS/AS to deliver a payload to a group of UEs. SCEF supports group message delivery for a group of UEs which are part of the same External Group ID. For more information, see Oracle Communications Diameter Signaling Router Service Capability Exposure Function User's Guide. | Enhancement Request |

### 2.1.6 *SUPPORT OF EXTERNAL GROUP ID FOR ME*

***Table 7: Support of External Group ID for ME Feature Description***

| Name | Description | Scope |
|---|---|---|
| POR 30002100 | SCEF supports Monitoring Events using External Group Identifier. SCEF also support monitoring of multiple/group of UE's procedures. For more information, see Oracle Communications Diameter Signaling Router Service Capability Exposure Function User's Guide. | Enhancement Request |

## *2.2 ENHANCEMENTS TO DSR 8.5.0.1.0*

Note: For information about upgrade planning and required steps before the upgrade, refer to the DSR 8.5.0.1.0 Software Upgrade Guide.

***Table 8*** **- DSR 8.5.0.1.0 New Features/Enhancements**

| DSR 8.5.0.1 Feature/Enhancement Name |
|---|
| Mobile Private Network (MPN) vDRA |
| Diameter Security Application (DSA) with Session Integrity Validation Check (SIVC) |
| Mission Critical Push to Talk (MCPTT) Rx Gateway |
| Operate VNF |
| Heal VNFM |
| Custom Size vDSR Instantiation |
| Dual IP stack support for Diameter+SBR flavor through VNFM |
| vSTP eLynx TDM card support |
| vSTP Home SMS Routing |
| vSTP Max and Reserved Link TPS |
| vSTP Multi-component TCAP message security |
| vSTP Reassembly error for SCCP XUDT message |
| vSTP SCTP Firewall Enhancements |
| vSTP TCAP Decoding Enhancement |
| vSTP Test Mode for GTT actions |
| vSTP TIF Enhancements |

### 2.2.1 *MOBILE PRIVATE NETWORK (MPN) VDRA*

***Table 9 –*** *Mobile Private Network (MPN) vDRA Feature Description*

| Name | Description | Scope |
|---|---|---|
| POR 31946079 | This feature aggregates Diameter and RADIUS traffic from external gateways towards appropriate Diameter and RADIUS peers. External gateways are palced on an automated process through provisioning portals.<br>For more information, see the following guides:<br>• Oracle Communications Diameter Signaling Router Feature Guide<br>• Oracle Communications Diameter Signaling Router Diameter User's Guide<br>• Oracle Communications Diameter Signaling Router RADIUS User's Guide<br>• Oracle Communications Diameter Signaling Router Alarms and KPIs Reference<br>• Oracle Communications Diameter Signaling Router Measurements Reference | Enhancement Request |

### 2.2.2 *DIAMETER SECURITY APPLICATION (DSA) WITH SESSION INTEGRITY VALIDATION CHECK (SIVC)*

***Table 10 –*** **Diameter Security Application (DSA) with Session Integrity Validation Check (SIVC)** *Feature Description*

| Name | Description | Scope |
|---|---|---|

| | | |
|---|---|---|
| POR 31679600 | This feature facilitates GPRS Tunnelling Protocol - Core (GTP - C) signaling fraud detection based on the subscriber location information for an outbound roaming subscriber. It scans the 3GPP-Gx-CCR-I message of outbound roaming subscribers to check whether a Update Location Request (ULR) message corresponding to the Credit Control Request - Initial (CCR-I) message is present in UDR DB or not. For more information, see the following guides:<br>• Oracle Communications Diameter Signaling Router Feature Guide<br>• Oracle Communications Diameter Security Application User's Guide with UDR | Enhancement Request |

### 2.2.3 *MISSION CRITICAL PUSH TO TALK (MCPTT) RX GATEWAY*

***Table 11 -*** **Mission Critical Push to Talk (MCPTT) Rx Gateway**

| Name | Description | Scope |
|---|---|---|
| POR 31946094 | The Rx ShUDR (Rx Gateway MCPTT) application enables the Push to Talk service using the DCA framework. For more information, see the following guides:<br>• Oracle Communications Diameter Signaling Router Feature Guide<br>• Oracle Communications Diameter Signaling Router Rx ShUDR Application User Guide. | Enhancement Request |

### 2.2.4 *OPERATE VNF*

***Table 12 –*** **Operate VNF** *Feature Description*

| Name | Description | Scope |
|---|---|---|
| POR 31992999 | This feature changes the operational state of a VNF instance, including starting and stopping the VNF instance. For more information, see *Oracle Communications Virtual Network Functions Manager Installation and User Guide.* | Enhancement Request |

### 2.2.5 *HEAL VNFM*

***Table 13 –*** *Heal VNFM Feature Description*

| Name | Description | Scope |
|---|---|---|
| POR 32092399 | This feature is a resource for healing a VNFc instance. For more information, see Oracle Communications Virtual Network Functions Manager Installation and User Guide. | Enhancement Request |

### 2.2.6 *CUSTOM SIZE VDSR INSTANTIATION*

***Table 14 –*** **Custom Size vDSR Instantiation Feature Description**

| Name | Description | Scope |
|---|---|---|
| POR: 32447086 | This feature enables instantiation of custom number of VNFc for DSR signaling and SDS signaling VNFs. For more information, see Oracle Communications Virtual Network Functions Manager Installation and User Guide. | Enhancement Request |

### 2.2.7 *DUAL IP STACK SUPPORT FOR DIAMETER+SBR FLAVOR THROUGH VNFM*

***Table 15 –*** **Dual IP stack support for Diameter+SBR flavor through VNFM Feature Description**

| Name | Description | Scope |
|---|---|---|
| POR: 32447038 | This feature supports Dual IP Stack deployment and the existing single IP deployment model. For more information, see Oracle Communications Virtual Network Functions Manager Installation and User Guide. | Enhancement Request |

### 2.2.8 *VSTP ELYNX TDM CARD SUPPORT*

***Table 16 –*** *vSTP eLynx TDM card support* Feature Description

| Name | Description | Scope |
|---|---|---|
| POR 31976156 | Starting with this release, the Time Division Multiplexing (TDM) over vSTP supports signal transmission over the eLynx Card. For more information, see Oracle Communications Diameter Signaling Router Virtual Signaling Transfer Point User's Guide. | Enhancement Request |

### 2.2.9 *VSTP HOME SMS ROUTING*

***Table 17 –*** **vSTP Home SMS Routing Feature Description**

| Name | Description | Scope |
|---|---|---|

| | | |
|---|---|---|
| POR 31641920 | With this release, vSTP provides an enhanced capability to address spoofing and spamming issues using the Home SMS Routing. This functionality enables operators to route all the MO and MT SMs through an SMS proxy service located in the HPLMN of the receiving MS. The service provides an SMS signaling FW that analyzes MO and MT packets before submitting or delivering them. For more information, see Oracle Communications Diameter Signaling Router vSTP SS7 Security User's Guide. | Enhancement Request |

### 2.2.10 *VSTP MAX AND RESERVED LINK TPS*

***Table 18 -*** **vSTP Max and Reserved Link TPS *Feature Des*cription**

| Name | Description | Scope |
|---|---|---|
| POR 31681055 | vSTP supports Reserved link TPS and Maximum link TPS parameters. The Reserved link TPS is a reserved bandwidth for specific link and the Max link TPS is MAX limit for the link. For more information, see *Oracle Communications Diameter Signaling Router Virtual Signaling Transfer Point User's Guide.* | Enhancement Request |

### 2.2.11 *VSTP MULTI-COMPONENT TCAP MESSAGE SECURITY*

***Table 19 – vSTP Multi-component TCAP message security Feature Description***

| Name | Description | Scope |
|---|---|---|
| POR 31437763 | The Multi-component TCAP message security feature provides additional capability to the existing TCAP Opcode Based Routing (TOBR) functionality. This feature enables the MSU being processed under the GTT Set of type OPCODE to check for the presence of multiple MAP operations in the same message. For more information, see *Oracle Communications Diameter Signaling Router vSTP SS7 Security User's Guide.* | Enhancement Request |

### 2.2.12 *VSTP REASSEMBLY ERROR FOR SCCP XUDT MESSAGE*

***Table 20 –*** *vSTP Reassembly error for SCCP XUDT message Feature Description*

| Name | Description | Scope |
|---|---|---|
| POR 31437763 | This feature enhances the vSTP screening capability of SCCP XUDT segmented messages by checking the length of the first segment and based on it a decision can be made to drop or allow the packet into the network. vSTP can discard reassembly procedure if the length of the first segmented MSU is less than configured length. For more information, see Oracle Communications Diameter Signaling Router vSTP SS7 Security User's Guide. | Enhancement Request |

### 2.2.13 *VSTP SCTP FIREWALL ENHANCEMENTS*

***Table 21 –*** *vSTP SCTP Firewall Enhancements Feature Description*

| Name | Description | Scope |
|---|---|---|
| POR 31437763 | With this release, vSTP enables operators to configure the Linux firewall to allow desired signaling network traffic on vSTP-MPs. This feature provides capability to dynamically update the Linux firewall configuration on vSTP-MPs to allow or restrict signaling traffic. For more information, see Oracle Communications Diameter Signaling Router vSTP SS7 Security User's Guide. | Enhancement Request |

### 2.2.14 *VSTP TCAP DECODING ENHANCEMENT*

***Table 22 –*** *vSTP TCAP Decoding Enhancement Description*

| Name | Description | Scope |
|---|---|---|
| POR 31983758 | vSTP provides the functionality to filter the ITU messages in case of any additional octets present in the TCAP layer. For more information, see Oracle Communications Diameter Signaling Router Virtual Signaling Transfer Point User's Guide. | Enhancement Request |

### 2.2.15 *VSTP TEST MODE FOR GTT ACTIONS*

***Table 23 –*** *vSTP Test Mode for GTT actions Feature Description*

| Name | Description | Scope |
|---|---|---|

| | | |
|---|---|---|
| POR 31641942 | vSTP provides the functionality to test the set of rules applied in SS7 network to block unauthorized traffic. This feature provides a detection mode, which raises an event for the MSU that encounters the GTT action and skips all the GTT actions included in that set. This helps identify all traffic that is discarded/copied/forwarded while the rule is active. For more information, see Oracle Communications Diameter Signaling Router Virtual Signaling Transfer Point User's Guide. | Enhancement Request |

### 2.2.16 *VSTP TIF ENHANCEMENTS*

***Table 24 –*** *vSTP TIF Enhancements Feature Description*

| Name | Description | Scope |
|---|---|---|
| POR 31641934 | The TIF functionality has been enhanced with the support for Linkset, Generic Number, and Redirecting Number based Blocklisting in vSTP for ISUP traffic. For more information, see *Oracle Communications Diameter Signalling Router TIF User's Guide.* | Enhancement Request |

## 2.3 ENHANCEMENTS TO DSR 8.5.0

Note: For information about upgrade planning and required steps before the upgrade, refer to the DSR 8.5 Software Upgrade Guide.

***Table 25 -*** **DSR 8.5.0 New Features/Enhancements**

| DSR 8.5 Feature/Enhancement Name |
|---|
| var Partition size increased by 1GB |
| DSR Support of Large vDAMP profile on OL7 and KVM |
| DSA Support for Visualization with Common Security Dashboard |
| DSR ZBA and SOR application enhancements to support UDR |
| DSR support for Service Based Interface |
| VNFM supports modify vnf information |
| VNFM Enhancements for VDSR Scaling |
| Cloud-init to ensure that DA-MP is not instantiated before SOAM |
| VNFM to Support SCEF deployment through mysql db |
| SCEF Monitoring Location Area Configuration for RAC/TAC |
| SCEF Debugs Based on IMSI or External-ID |
| IDIH Support for SCEF |
| vSTP Accounting Measurements |
| vSTP ELK Integration with Security Dashboard |
| vSTP Multiple Linksets and route support |

### 2.3.1 *VAR PARTITION SIZE INCREASED BY 1GB*

***Table 26 –*** *var Partition Size Increased Feature Description*

| Name | Description | Scope |
|---|---|---|
| POR 31559296 | This feature is introduced to increase the var partition size from 1 GB to 2 GB and decrease the filemgmt size by 1 GB, that is, from 17 GB to 16 GB only on DSR systems. | Enhancement Request |

### 2.3.2 *DSR SUPPORT OF LARGE VDAMP PROFILE (35K MPS) ON OL7 AND KVM*

***Table 27 –*** *Large VDAMP Profile on OL7 and KVM Feature Description*

| Name | Description | Scope |
|---|---|---|
| POR 30133498 | This feature enables VM and BareMetal DA-MP on the same SOAM. Large VMs to support Gen 10. | Enhancement Request |

### 2.3.3 *DSA SUPPORT FOR VISUALIZATION WITH COMMON SECURITY DASHBOARD*

***Table 28 -*** *Visualization Server Feature Description*

| Name | Description | Scope |
|---|---|---|
| POR 31444698 | Visualization Server displays all the logs in a graphical format. It logs vulnerable messages into a log file on MPs. The Active SO collects these log files from MPs and exports them in the configured path of Visualization Server. | Enhancement Request |

### 2.3.4 *DSR ZBA AND SOR APPLICATION ENHANCEMENTS TO SUPPORT UDR*

***Table 29 –*** *ZBA and SOR Support for UDR Feature Description*

| Name | Description | Scope |
|---|---|---|
| POR 31900247 | This feature enables Zero Balance Application (ZBA) and Steering of Roaming (SoR) to support UDR instead of USBR. For more information, refer to the following guides:<br>• DSR Roaming Steering Guide<br>• DSR Zero Balance Application User's Guide | Enhancement Request |

### 2.3.5 *DSR SUPPORT FOR SERVICE BASED INTERFACE*

***Table 30 –*** *Service-Based Interface Feature Description*

| Name | Description | Scope |
|---|---|---|
| POR 30759142 | In the Policy DRA configuration, **Enable Reroute** and **Reroute Peer Route Table Name** fields are introduced to configure Reroute. | Enhancement Request |

### 2.3.6 *VNFM SUPPORTS MODIFY VNF INFORMATION*

***Table 31 –*** **Modify VNF Information Feature Description**

| Name | Description | Scope |
|---|---|---|
| POR: 30394289 | VNFM supports the API to Modify VNF operation to modify created VNF Identifier resources. For information about this feature, refer to the Virtual Network Functions Manager Installation and User Guide. | Enhancement Request |

### 2.3.7 *VNFM ENHANCEMENTS FOR VDSR SCALING*

***Table 32 –*** **vDSR Scaling Feature Description**

| Name | Description | Scope |
|---|---|---|
| POR: 31351885 | Currently, both VNFM operations to Scale vDSR (Scale to Level and Scale out) have the following limitations:<br>• The software release to be used for the new VNFCs to be deployed will be retrieved from the VNFM storage and will be the software release used to instantiate the VNF.<br>• The active NOAM used by cloud-config and cloud-init will be retrieved from the VNFM storage and will be the active NOAM used to instantiate the VNF.<br>These limitations cause VNF malfunctioning while upgrading the VNF after instantiating and the cloud-config and cloud-init MMI commands to fail.<br>With this new feature, the VNFM Scale form/template will include two additional parameters: SW Release and Active NOAM. | Enhancement Request |

### 2.3.8 *CLOUD-INIT TO ENSURE THAT DA-MP IS NOT INSTANTIATED BEFORE SOAM*

***Table 33 –*** **DA-MP to Instantiate Configuration When SOAM is up Feature Description**

| Name | Description | Scope |
|---|---|---|
| POR 31693871 | This features states that DA-MP cloud-init should initiate configuration only after SOAM is up. | Enhancement Request |

### 2.3.9 *VNFM TO SUPPORT APIGW WITH THE NEW DB VMS*

***Table 34 –*** **SCEF Deployment Through MySQL DB Feature Description**

| Name | Description | Scope |
|---|---|---|
| POR 31768098 | This feature enables VNFM to support SCEF deployment through MySQL DB as DB for OCSG. | Enhancement Request |

### 2.3.10 *SCEF MONITORING LOCATION AREA RANGE CONFIGURATION FOR RAC/TAC*

***Table 35 -*** *Routing Area Code (RAC) and Tracking Area Code (TAC) Range Feature Des***cription**

| Name | Description | Scope |
|---|---|---|
| POR 30002040 | SCEF Monitoring Location Area configuration includes the TRACKING AREA ID and ROUTING AREA ID information to support the RAC/TAC range.<br>**Note**:<br>When a DSR with SCEF application enabled is upgraded from any earlier version to DSR 8.5 or later, then the existing MMI configuration records for `/scef/monitoringlocationareas/` is deleted after the upgrade due to the change in the schema information. | Enhancement Request |

### 2.3.11 *SCEF DEBUGS BASED ON IMSI/EXTERNAL-ID /MSISDN/TLTRID*

***Table 36 –*** *SCEF Collects Debugs Based on MSISDN/TltrId/IMSI/External-ID*

| Name | Description | Scope |
|---|---|---|
| POR 30214915 | This feature enables SCEF to collect debugs based on MSISDN/TltrId/IMSI/External-ID filtering and Diameter/T8 logic. Diagnostics information must contain internal logic, Diameter, and T8. | Enhancement Request |

### 2.3.12 *IDIH SUPPORT FOR SCEF*

***Table 37 –*** *IDIH Support for SCEF Feature Description*

| Name | Description | Scope |
|---|---|---|
| POR 30994039 | Using this feature, users can:<br>• Create and manage trace filters on SCEF related Diameter interfaces to capture messages required for troubleshooting service issues.<br>• View traces in graphical formats.<br>• Filter, view and store the results in IDIH. | Enhancement Request |

### 2.3.13 *VSTP ACCOUNTING MEASUREMENTS*

***Table 38 –*** *vSTP Accounting Measurements Feature Description*

| Name | Description | Scope |
|---|---|---|
| POR 29518686 | vSTP supports Accounting Measurement for different combinations to track the send/received MSUs on any linkset of vSTP. Users can enable any of the accounting measurement combinations as per their requirements. This feature allows users to<br>• Generating CSV report for any combination for any given time period.<br>• Check pegging for any record or entry. | Enhancement Request |

### 2.3.14 *VSTP ELK INTEGRATION WITH SECURITY DASHBOARD*

***Table 39 –*** *vSTP ELK Integration with Security Dashboard Description*

| Name | Description | Scope |
|---|---|---|
| POR 31053233 | vSTP Logging and Visualization feature generates and sends log messages from SCCP and SFAPP to an external visualization server. The log messages are converted into the JSON format with data enrichment for enhanced visualization.<br>With this feature, advanced data analysis and visualization is performed in a variety of charts, tables, and maps. | Enhancement Request |

### 2.3.15 *VSTP MULTIPLE LINKSETS AND ROUTE SUPPORT*

***Table 40 –*** *vSTP Multiple Linksets and Route Support Feature Description*

| Name | Description | Scope |
|---|---|---|

| | | |
|---|---|---|
| POR 31053131 | Using this feature, users can:<br>• vSTP provides support for multiple routes to a destination of ANSI/ITU-I/ITU-N/ITUN24<br>• vSTP provides support for establishing multiple linksets to Adjacent Point Code (APC). | Enhancement Request |

## 2.4 HARDWARE CHANGES

### 2.4.1 HARDWARE SUPPORTED

***Table 41 -*** **Hardware Details**

| Hardware | Comment |
|---|---|
| HP BL460c Gen8, Gen8_v2 | c-Class |
| HP BL460c Gen9, Gen9_v2 | c-Class |
| HP DL360/380 Gen8, Gen8_v2 | Rack Mount Server |
| HP DL380 Gen9, Gen9_v2 | Rack Mount Server |
| Oracle Server X5-2 | Rack Mount Server |
| Oracle Server X6-2 | Rack Mount Server |
| Oracle Server X7-2 | Rack Mount Server |
| Netra X5-2 | Rack Mount Server |
| HP 6125XLG, 6125G, 6120XG | Enclosure Switch |
| Cisco 3020 | Enclosure Switch |
| Cisco 4948E-F | Rack Switch |
| Cisco 4948E | Rack Switch |

Note:
Gen9, Gen9 v2, and Gen 8 v2 hardware are also supported when purchased by a customer. Mixed Sun/HP deployments are not generally supported.

### 2.4.2 HARDWARE UPGRADE

The VEDSR 8.5 release builds on top of the RMS and supports the newer and higher capacity X7-2 RMS hardware.

## 2.5 SOFTWARE DETAILS

### 2.5.1 SOFTWARE PLATFORM COMPONENTS IN 8.5.X

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

***Table 42 - Software Platform Component Details - 8.5.0.2***

| Component | Release |
|---|---|
| TPD | 7.8.0.0.0-89.8.1 |
| COMCOL | 7.5.0.34.0-14121 |
| APIGW | 8.5.0.2.0_92.8.0 |
| PM&C | 6.6.1.0.0-66.9.0 |
| TVOE | 3.6.2.0.0-88.58.0 |
| AppWorks | 9.3.0-93.8.0 |
| EXGSTACK | 9.3.0-93.8.0 |

| | |
|---|---|
| HP Firmware FUP | 2.2.13 (Minimum1) |
| Oracle Firmware | 3.1.8 (Minimum2) |

***Table 43 –*** **Software Platform Component Details – 8.5.0.1**

| Component | Release |
|---|---|
| TPD | 7.7.1.0.0-88.75.0 |
| COMCOL | 7.5.0.30.0-14117 |
| APIGW | 8.5.0.1.0_91.17.0 |
| PM&C | 6.6.1.0.0-66.9.0 |
| TVOE | 3.6.2.0.0-88.58.0 |
| AppWorks | 9.2.0-92.12.0 |
| EXGSTACK | 9.2.0-92.13.0 |
| HP Firmware FUP | 2.2.13 (Minimum3) |
| Oracle Firmware | 3.1.8 (Minimum4) |

### 2.5.2 *IDIH 8.2.3*

***Table 44 -*** **IDIH Details**

| Component | Release |
|---|---|
| IDIH Release | 8.2.3.0.0_82.40.0 |

DSR 8.5 is compatible with IDIH 8.2.3

### 2.5.3 *SDS 8.5*

***Table 45 -*** **SDS Details**

| Component | Release |
|---|---|
| SDS Release | 8.5.0.2.0_92.7.0 |

DSR 8.5 is compatible with SDS 8.1.2, 8.2.1, 8.3, 8.3.X, 8.4, and 8.4.0.X.Y.

NOTE**:** It is recommended for SDS to be upgraded before the DSR. SDS release 8.5 is compatible with DSR releases 8.1.2, 8.2.1, 8.3, 8.3.X, 8.4, and 8.4.0.X.Y.

X = PI End Cycle
Y = Patches within the PI Cycle.

1 - This represents the minimum release of the HP FUP 2.2.x series to support all content in the Platform 74 release. It is recommended that the latest firmware release always be used in order to address known security issues.

2 - This represents the minimum release of the Oracle firmware series to support all content in the Platform 74 release. It is recommended that the latest firmware release always be used in order to address known security issues.

3 - This represents the minimum release of the HP FUP 2.2.x series to support all content in the Platform 74 release. It is recommended that the latest firmware release always be used in order to address known security issues.

4 - This represents the minimum release of the Oracle firmware series to support all content in the Platform 74 release. It is recommended that the latest firmware release always be used in order to address known security issues.

## 2.6 FIRMWARE CHANGES

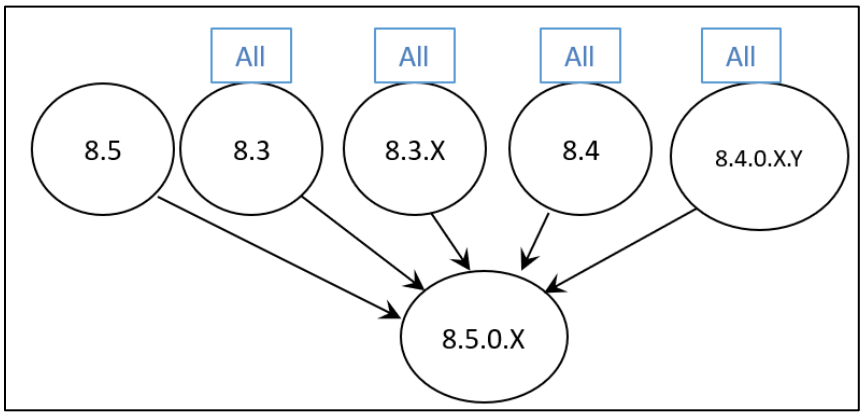
Firmware release guidance is provided through DSR 8.5 Release Notice which can be found at the following link:
http://docs.oracle.com/en/industries/communications/diameter-signaling-router/index.html
and then navigating to the Release 8.5 link.

## 2.7 UPGRADE OVERVIEW

This section provides an overview of the Upgrade activities for Release 8.5.

### 2.7.1 DSR UPGRADE PATH

The supported upgrade paths for DSR 8.5 are:



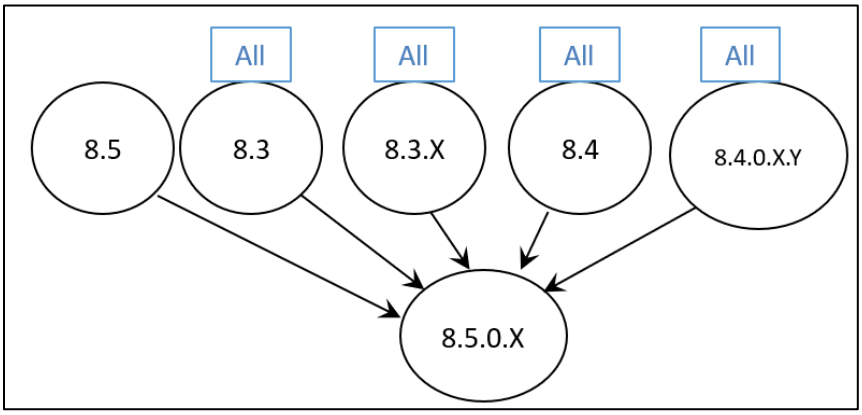

**X = PI End Cycle**
**Y = Patches within the PI Cycle.**

***The figure above refers to the available releases and all of its maintenance releases.***

***Figure 1 – DSR Upgrade Paths***

### 2.7.2 SDS UPGRADE PATH

The supported upgrade paths for SDS 8.5 are:




**X = PI End Cycle**
**Y = Patches within the PI Cycle.**

***The figure above refers to the available releases and all of its maintenance releases.***

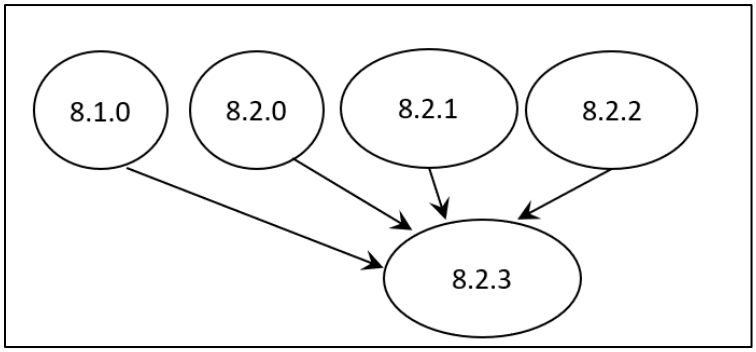
***Figure 2 – SDS Upgrade Paths***

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

.

### 2.7.3 *IDIH UPGRADE PATH*

The supported upgrade paths for IDIH 8.2.3 are:




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

***Figure 3 – IDIH Upgrade Paths***

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

### 2.7.4 *UPGRADE EXECUTION*

With DSR 8.5, there are multiple methods available for upgrading a site. The newest and most efficient way to upgrade a site is the Automated Site Upgrade feature. As the name implies, this feature will upgrade an entire site (SOAMs and all C-level servers) with a minimum of user interaction. Once the upgrade is initiated, the upgrade will automatically prepare the server(s), perform the upgrade, and then sequence to the next server or group of servers until all servers in the site are upgraded. The server upgrades are sequenced in a manner that preserves data integrity and processing capacity.

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

Additionally, there are separate procedures described in the upgrade procedures to support either a manual or automated approach to upgrading any particular server group. When planning upgrades the "Site Upgrade Methodology Selection" section of the upgrade procedure should be carefully reviewed. ***The use of the automated methods (Auto Site or Auto Server Group) for DA-MP server groups should be carefully considered regarding potential negative traffic impacts***. The ASU enhancement in DSR 8.5 resolves this issue. The user is now instructed to rearrange/add cycles to create a suitable upgrade plan.

### 2.7.5 *LIMITATIONS*

When AppEventLog file is full then SOAM/NOAM becomes unstable and shown undefined behavior like:
1. Replication and merging stopped.
2. GUI access stops working.

Also, note that upgrade will fail if utilization of /var/TKLC/rundb partition is more than 70% which may be true in case of larger AppEventLog file size (~5.5 GB in size). To prevent the above listed issues, we need to assign/allocate

/var/TKLC/rundb size and AppEventLog file size in sync i.e. AppEventLog file size (plus some delta for other files like MeasStat) should be always less than 70 % of /var/TKLC/rundb partition size.

## 2.8 MIGRATION OF DSR DATA

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

# 3 RELEASE 8.5 FEATURE OAM CHANGES

At the time of upgrade to DSR 8.5, a number of features and enhancements will become visible on the interfaces to the DSR and may change certain existing OAM behaviors of the system.
OAM changes includes: User Interfaces (NO GUI, SO GUI), Measurements Reports, Alarms, and KPIs.

## *3.1 SLS ROTATION*

### 3.1.1 *PURPOSE AND SOLUTION*

**Purpose**

- In many cases, MSCs switches and other originating nodes do not send an adequate distribution of SLS values. For example, in case of ITU ISUP messages, SLS is obtained from the lower 4 bits of the CIC field representing the circuit being used. CIC selection can be determined based on an odd/even method where a SSP uses either all odd CICs or all even CICs to help prevent glaring. This causes the LSB of the SLS to be fixed (0 or 1) which means SSP sends either odd or even SLS. Thus, the transit nodes (STPs), do not achieve a good distribution of traffic across links.
- For combined linkset, in ANSI and ITU MTP protocols, the LSB of the SLS is used to load share between linksets of a combined linkset and the remaining SLS bits are used to distribute traffic across different links within a linkset. Since STP receives improper distribution of SLS value (either LSB as 0 or 1), hence the STPs cannot perform proper loading sharing across the linkset and the links of a linkset.
- For single linkset, since STP receives improper distribution of SLS value (either LSB as 0 or 1), the STPs cannot perform proper loading sharing across all the links of a linkset.

**Solution**

SLS Rotation feature allows the user to use the below options for addressing the problem.

- Outgoing Bit Rotation
- Use of Other CIC Bit
- Incoming Bit Rotation
- Random SLS
- ANSI 5-bit to ANSI 8-bit SLS Conversion
- ITU to ANSI SLS Conversion
- ANSI to ITU SLS Conversion

**Note:** The SLS modified using the above-mentioned solutions is only used for internal linkset and link selection. The actual SLS field of the message (i.e. the SLS value received by the vSTP is the SLS value sent out by the vSTP) is not modified.

**Feature Overview**

- **Outgoing Bit Rotation**
    - The User can have the vSTP to rotate the 4 bits of SLS, according to outgoing Linkset, thus changing the LSB of the SLS.
    - If configured, this option is applied and **SLS will be converted from 5-bit to 8-bit.**
- **ITU to ANSI SLS Conversion**
    - If the ITU 4-bit SLS is “ABCD” then the ANSI 5-bit SLS will be “D (~D) ABC”, which is already implemented as a part of ANSI<->ITU Conversion feature.
    - Secondly, this conversion “ITU 4-bit to ANSI 5-bit” may be followed by 5-bit ANSI to 8-bit ANSI SLS conversion to achieve more randomization for linkset/link selection during the network conversion.
- **ANSI to ITU SLS Conversion**

- Firstly, 5 or 8 bit ANSI SLS value is converted to the 4-bit ITU SLS value by doing MOD 16.
- Secondly, this conversion may be followed by 4-bit ITU to 8-bit ITU SLS conversion to achieve more randomization for linkset/link selection during the network conversion.

- **ANSI 5-bit to ANSI 8-bit SLS Conversion**
  - The User can have the vSTP to perform the 5-bit ANSI conversion to 8-bit ANSI.
  - If configured, this option is applied and SLS will be converted from 5-bit to 8-bit.
- **ITU to ANSI SLS Conversion**
  - If the ITU 4-bit SLS is "ABCD" then the ANSI 5-bit SLS will be "D (~D) ABC", which is already implemented as a part of ANSI<->ITU Conversion feature.
  - Secondly, this conversion "ITU 4-bit to ANSI 5-bit" may be followed by 5-bit ANSI to 8-bit ANSI SLS conversion to achieve more randomization for linkset/link selection during the network conversion.
- **ANSI to ITU SLS Conversion**
  - Firstly, 5 or 8 bit ANSI SLS value is converted to the 4-bit ITU SLS value by doing MOD 16.
  - Secondly, this conversion may be followed by 4-bit ITU to 8-bit ITU SLS conversion to achieve more randomization for linkset/link selection during the network conversion.

**Note: All algorithms are applicable to both MTP Routed and GT Routed MSUs.**

---

3.1.2 MEALS

## Measurements

1. No new Measurements are being implemented as part of this feature.
2. Appropriate Logging will be done accordingly to print the Rotated SLS value used for Linkset and Link selection. The logs should be optional only. User need to turn on the M3RL SLS INFO (13th bit) to see the logs.

Note: The traces are not supposed to be enabled for TPS rate>100 as it might cause undesired behavior.

### Alarms & Events

No new Events are being implemented as part of this feature.

No new Alarms are being implemented as part of this feature.

**Limitation**

1. Usage of 5th bit as LSB for incoming bit rotation is to be avoided if all the nodes are GR compliant. This is due to the fact that ANSI mandated outgoing 5 bit rotation causes the 5th bit to not have a uniform distribution of 0's and 1's.
2. If 5 to 8 Bit Conversion is applied on incoming 5 bit SLS, then 3 new SLS bits (calculated based on the OPC) will be prefixed to the 5-bit SLS. If all 8 SLS bits are considered for applying ISLSBR, the 3 new sls bits will become sticky bits and will cause un-even distribution. In this scenario, ISLSRSB value 6-8 will cause even more un-even distribution.
3. If 5-bits SLS is received on incoming linkset, 5-to-8 bit conversion is 'OFF' on outgoing linkset and 8-bits SLS are to be considered for applying ISLSBR, then no rotation shall happen. The "5-to-8 Bit Conversion" option should be turned ON to perform ISLSBR.
4. When two linksets are used as a combined linkset, they should have the same settings for all SLS algorithms (Example "Other CIC Bit", "Rotated SLS Bit"), else there can be random behavior.. This is not enforced in the vSTP, and there is no warning mechanism for incorrectly provisioned linksets and routes

5. Different RANDSLS configurations on two linksets, which happen to be a part of combined linkset for the routes defined for a destination node, may result in undesired SLS distribution. vSTP shall not prompt or reject the linkset provisioning command, if provisioning is done contrary to the above.
6. For different segments of the same MSU, randsls will generate different SLS and hence different link selection. For other SLS algorithms, we assume that the Incoming linkId/SLS is same for different segments of the same MSU, hence the outgoing linkId/linkset id will be same for different segments of the same MSU.

**Dependencies**

The SLS Rotation feature for vSTP has no dependency on any other vSTP operation. The following points must be

considered for SLS Rotation functionality:

- Usage of 5th bit as LSB for incoming bit rotation must be avoided if all the nodes are GR compliant. This is due to the fact that ANSI mandated outgoing 5 bit rotation causes the 5th bit to not have a uniform distribution of 0's and 1's.
- If 5 to 8 Bit Conversion is applied on incoming 5 bit SLS, then 3 new SLS bits (calculated based on the OPC) are prefixed to the 5-bit SLS. If all 8 SLS bits are considered for applying ISLSBR, the 3 new SLS bits become sticky bits and cause uneven distribution. In this scenario, ISLSRSB value 6-8 cause even more uneven distribution.
- If 5 bits SLS is received on incoming linkset, 5 to 8 bit conversion is OFF on outgoing linkset, and 8 bits SLS are considered for applying ISLSBR, then no rotation happens. The 5 to 8 Bit Conversion option must be turned ON to perform ISLSBR.
- When two linksets are used as a combined linkset, they should have the same settings for all SLS algorithms (For example, Other CIC Bit, Rotated SLS Bit), otherwise there can be a random behavior. This is not enforced in vSTP , and there is no warning mechanism for incorrectly provisioned linksets and routes.
- Different RANDSLS configurations on two linksets , which happen to be a part of combined linkset for the routes defined for a destination node may result in undesired SLS distribution. vSTP does not prompt or reject the linkset provisioning command if the provisioning is done contrary to the above.
- For different segments of the same MSU, randsls generates different SLS and different link selection. For other SLS algorithms, it is assumed that the Incoming linkId or SLS is same for different segments of the same MSU, hence the outgoing linkId or linkset id will be same for different segments of the same MSU.

**Troubleshooting Steps**

The troubleshooting scenarios for SLS Rotation:

- If no SLS Rotation algorithm is applied.
    - Ensure that correct parameters are set on ingress and egress Linkset connected to vSTP MP as per SLS Rotation Algorithm.
    - Ensure that appropriate m3rloptions MO parameters are set.
    - SLS Rotation algorithms are specific to domain and type of message such as, SCCP or ISUP. Therefore, the configurations must be done accordingly. For example, Algorithm Use of Other CIC bit is applicable only for ITU ISUP messages.
- If ANSI SLS in Egress Message is not correct as per the SLS Rotation Algorithm applied:
    - Apart from SLS Rotation algorithms, for ANSI domain only Standard 5th Bit Rotation is always applied and is modified in Egress Message.
- If SLS Rotation on Domain Conversion is not working properly:
    - Few parameters can be set on Linksets, so while performing Domain Conversion make sure correct parameter values are specified to get desired output.
    - Slide 33 – 40 must be referred for these scenarios.
    - For ANSI, check value of parameter ASLS8 in Incoming Linkset.

- Also, Interaction between different algorithms of SLS Rotation during Domain Conversion has certain exceptions, refer to slide 38 and 40 for it.
- If certain SLS Algorithm does not get applied.
  - When multiple algorithms are applied to a particular domain message type, the SLS Rotation algorithms are applied as per points mentioned in slide 31 and 32. Combining SLS Rotation Options.
  - Modifying SLS Rotation related parameter values can render one of SLS Rotation Algorithm as inapplicable. Revert the modified parameter values to return to the previous manner of load sharing.

If issue still exists, then contact Oracle for support.

## 3.2 SFAPP DYNAMIC LEARNING

### 3.2.1 PURPOSE AND SOLUTION

**Purpose**

vSTP to create a whitelist of VLRs it interacts with by learning from the results of the validation methods.

**Solution**

This use case will provide protection against all messages coming from VLRs that fail the validation and are not part of the whitelists created. A grey list and black list shall also be created for the VLRs that fail the validation.

**Feature Overview**

The Stateful Security Dynamic Learning feature enables vSTP to create and use a whitelist that is created as part of learning from the validation attempts defined in VLR Validation. This feature is independent of the category of messages, but it provides protection against all the messages coming from VLRs that fail the validation and are not part of the created whitelists. A grey list and black list is also created for the VLRs that fail the validation.

Learning is controlled by these modes using a mode parameter in the SFAPPOPTS table:

- **Learn Mode**: This mode allows to learn about new VLRs and no validations are performed. The newly learnt VLRs are considered as whitelisted.

  Note: The user can configure the amount of time for which the vSTP operates in Learn mode. The time is configured in SFAPPOPTS table. Hence, the switch from Learn to Test mode can happen either by configuring the timer, or manual switch.
- **Test Mode**: This mode validates all the learned VLRs. In case the VLR is not validated, the learnt VLRs remains greylisted and measurements and alarms are generated.
- **Active Mode**: This mode allows validations based on the learned white lists in the system. New VLRs are also learned in this mode. The status of dynamically learnt VLRs are changed to whitelist or blacklist as per their status.
- **OFF Mode**: When none of the above modes is active, it is considered as OFF mode. In this mode, if VLR entry is in whitelist, then no validation is performed for that VLR. By default, the OFF mode remains enabled. That means the SFAPP dynamic learning functionality is disabled.

  Note: In any mode, if VLR is in whitlist table, then it is considered as whitelisted, and the message is forwarded to HLR. If user has changed the mode from Learn/Test/Active mode to OFF mode, then the user has to wait for at least 10 mins before switching the mode again to Active/Learn/Test mode.

### 3.2.2 MEALS

**Measurements**

***Table 46 – Measurements***

| MeasID | Measurement Name | Description | Group | Interval | Type |
|---|---|---|---|---|---|
| 21937 | VstpDynNewVLR | Total number of New Dynamic VLRs Learned. | SFAPP Exception | 5 min | Single |
| 21938 | VstpDynNewRoamEntry | Total number of New Dynamic VLR Roaming entries Learned. | SFAPP Exception | 5 min | Single |
| 21939 | VstpDynVLRBL | Total number of VLRs moved to Blacklist | SFAPP Exception | 5 min | Single |
| 21940 | VstpDynVLRWL | Total number of VLRs moved to Whitelist | SFAPP Exception | 5 min | Single |
| 21941 | VstpDynVLRGL | Total number of VLRs moved to Graylist | SFAPP Exception | 5 min | Single |
| 21942 | VstpDynVelCrossed | Total number of entries for which Velocity check threshold crossed | SFAPP Exception | 5 min | Single |
| 21943 | VstpDynVLRProfAging | Total number of VLRs Profile entries aged out | SFAPP Exception | 5 min | Single |
| 21944 | VstpDynVLRRoamAging | Total number of VLRs Roaming entries aged out | SFAPP Exception | 5 min | Single |

## Alarms & Events

***Table 47 – Alarms & Events***

| ID | Event Name | Type | Raise Condition | Severity | Throttle Sec |
|---|---|---|---|---|---|
| 70429 | VstpDynVlrStatusChanged | Event | When Dynamic VLR Status Changed from Graylist to Blacklist/Whitelist | Info | 10 |
| 70430 | VstpDynVeloThreshCrossed | Event | VLR crossed the Velocity Threshold limit | Info | 10 |
| 70431 | VstpDynVLRProfAging | Event | When VLR is aged out | Info | 10 |
| 70432 | VstpDynVLRRoamAging | Event | When any VLR relation is aged out | Info | 10 |
| 70433 | VstpVlrDynLearningOFF | Event | When Dynamic Learning is turned OFF | Info | 10 |
| 70434 | VstpVlrDynLearningLearntimer | Event | When Learn Timer is expired | Info | 10 |
| 70435 | VstpVlrDynProfileTableFull | Alarm | When Sfapp Dynamic Profile is full (50000 entries) | Major | |
| 70436 | VstpVlrDynProfileTableFull | Alarm | When Sfapp Dynamic Roaming is full (50000 entries) | Major | |

**Limitation**

Wait for latest 10 min before switching OFF mode to any other mode.

## 3.3 TIF SUPPORT

### 3.3.1 PURPOSE AND SOLUTION

**Feature Overview**

For TIF features, TIF provides an overall structure that allows the vSTP to intercept ISUP messages that would normally be through-switched and apply special processing to them. For example, an IAM message could be intercepted and have the called number prefix replaced based on portability information.

TIF processing consists of two main sections:

- TIF uses MTP to select an ISUP MSU for processing and forwards the MSU to Service Module cards for processing.
- TIF decodes the MSU, invokes the Numbering Plan Processor (NPP), and encodes the results.
  TIF features provide NPP with Service Action Handlers to perform database access, data evaluation, and any feature-specific handling for the MSU.

### 3.3.2 MEALS

**Measurements**

***Table 48 – Measurements***

| MeasID | Measurement Name | Description | Group | Interval | Type |
|---|---|---|---|---|---|
| 21921 | VstpTinpMsgRcv | Number of IAM messages received that require TIF processing | VSTP ISUP Performance | 5 min | Single |
| 21922 | VstpTinpMsgGen | Number of IAM messages received that required TIF processing and resulted in the modification of the IAM message or the generation of a REL message. | VSTP ISUP Performance | 5 min | Single |
| 21923 | VstpTinpErr | Number of IAM messages received that required TIF processing but resulted in execution of an error case. | VSTP ISUP Exception | 5 min | Single |
| 21924 | VstpTifRelease | Number of IAM messages received that were processed by TIF and found to be blacklisted by BLRLS Service Action. | VSTP ISUP Exception | 5 min | Single |
| 21925 | VstpTifNotFoundDnRelease | Number of IAM messages received that were processed by TIF and found to be blacklisted by BLNFNDRLS Service Action. | VSTP ISUP Exception | 5 min | Single |
| 21926 | VstpTifFpfxRelease | Number of IAM messages received that were processed by TIF and found to be blacklisted by FPFXRLS Service Action. | VSTP ISUP Exception | 5 min | Single |
| 21927 | VstpTifNoCgpnRelease | Number of IAM messages received that were processed by TIF and found to be blacklisted by NOCGPNRLS Service Action. | VSTP ISUP Exception | 5 min | Single |
| 21928 | VstpTifSelscrRelease | Number of MSUs processed by TIF and found to be blacklisted by SELSCR Service Action. | VSTP ISUP Exception | 5 min | Single |
| 21929 | VstpTifSelscrRelay | Number of MSUs processed by TIF and relayed by SELSCR Service Action. | VSTP ISUP Performance | 5 min | Single |
| 21930 | VstpIsupCAAvgProcessTime | Average time by CA to send query and receive the response from UDR. | VSTP ISUP Performance | 5 min | Single |
| 21931 | VstpIsupCAMaxProcessTime | Peak time by CA to send query and receive the response from UDR | VSTP ISUP Performance | 5 min | Single |
| 21932 | VstpIsupInternalError | Number of messages discarded due to internal processing error. | VSTP ISUP Exception | 5 min | Single |

| | | | | | |
|---|---|---|---|---|---|
| 21933 | VstpIsupCADecodeFail | Number of messages discarded by ISUP due to decode failed of CA response message. | VSTP ISUP Exception | 5 min | Single |
| 21934 | VstpIsupCATimeOut | Number of messages for which CA query to UDR timed out. | VSTP ISUP Exception | 5 min | Single |
| 21936 | VstpIsupCAProcessTime | Time required by CA to send query and receive the response from UDR. | VSTP ISUP Performance | 5 min | Arrayed |

### Alarms & Events

***Table 49 –*** Alarms & Events

| ID | Event Name | Type | Trigger Condition | Throttle Sec |
|---|---|---|---|---|
| 70423 | VstpTifUnexpectedSi | Event | Only TUP and ISUP messages can be processed. | 10 |
| 70424 | VstpTifRouteFailed | Event | Message is too big (modification made it too large). | 10 |
| 70425 | VstpIsupDcdFailed | Event | ISUP Clg Party Decode Failed or ISUP Decode Failure Error. | 10 |
| 70426 | VstpIsupDcdCdpaFailed | Event | ISUP Cld Party Decode Failed. | 10 |
| 70427 | VstpIsupEcdFailed | Event | ISUP Cld Pty Encode Failed or ISUP Clg Pty Encode Failed or ISUP REL encoding failure. | 10 |
| 70428 | VstpTifCcMismatchDn | Event | CC mismatch in DN | 10 |

**Limitation**

The TIF feature has no dependency on any other vSTP operation.

## *3.4 SEGMENTED XUDT*

### 3.4.1 *PURPOSE AND SOLUTION*

**Purpose**

- When the destination for an XUDT message is determined by SCCP and MTP parameters then they will be routed properly by vSTP towards same destination. However, vSTP can route different segments of the same SCCP large XUDT message to different destinations when features like TOBR, MBR are applied on them.
    - First segment (XUDT) usually contains TCAP/MAP layer parameters (Opcode, MSISDN, VLR, IMSI) are routed properly when TOBR/MBR feature is applied.
    - Subsequent segments (XUDT) do not contain TCAP/MAP parameters needed for TOBR/MBR and hence these messages are routed differently without applying TOBR/MBR.
- Routing different segment of the same message to different destination is incorrect behavior.

**Solution**

- vSTP must implement a solution to ensure that all segments of the SCCP Class 1 XUDT messages are routed to the same destination irrespective of the service used for translation.
- To address this problem, vSTP need to support Segmentation and Reassembly of XUDT Class 1 SCCP Messages.
    - vSTP shall perform Reassembly on the incoming segmented XUDT messages
    - vSTP will then perform the services/translation on the Reassembled Message.
    - vSTP shall perform Segmentation on the Outgoing XUDT Reassembled Message to generate segments and perform routing.

**Feature Overview**

The Segmented XUDT feature allows vSTP to perform the following operations:

- Reassembly of incoming XUDT Class 1 SCCP segmented messages
- Segmentation of the outgoing XUDT Class 1 SCCP reassembled messages

This functionality ensures that all segments of the SCCP Class 1 XUDT messages are routed to same destination, irrespective of the service used for translation.

vSTP performs reassembly on the incoming segmented XUDT messages. After the reassembly, the required services or translation is performed on the reassembled message.

The segmentation is performed on the outgoing XUDT reassembled message to generate segments and perform routing.

### 3.4.2 MEALS

**Measurements**

***Table 50 – Measurements***

| Measurement Id | Measurement Name | Dimension | Description | Interval in Mins | Group | Type |
|---|---|---|---|---|---|---|
| 21901 | VstpRxSccpReassProcSucc | Single | Number of times reassembly procedure completed successfully | 30 | VSTP SCCP Performance | Simple |
| 21902 | VstpRxSccpReassProcFail | Single | Number of times reassembly procedure failed | 30 | VSTP SCCP Exception | Simple |
| 21903 | VstpRxSccpXUDTSgmnts | Single | Number of ingress segmented XUDT messages received from network | 30 | VSTP SCCP Performance | Simple |
| 21904 | VstpRxSccpSgmntsDisc | Single | Number of segmented XUDT messages Discarded due to reassembly failure. | 30 | VSTP SCCP | Simple |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Exception | |
| 21905 | VstpRxSccpSgmntsReassFail | Single | Number of segmented XUDT messages that encountered Reassembly failure due to any errors | 30 | VSTP SCCP Exception | Simple |
| 21906 | VstpTxSccpSegProcSucc | Single | Number of times segmentation procedure completed successfully | 30 | VSTP SCCP Performance | Simple |
| 21907 | VstpTxSccpSegProcFail | Single | Number of times segmentation procedure failed | 30 | VSTP SCCP Exception | Simple |
| 21908 | VstpTxSccpLargeMsgs | Single | Number of reassembled large messages received for segmentation | 30 | VSTP SCCP Performance | Simple |
| 21909 | VstpRxSccpReassSegSucc | Single | Number of Segmented XUDT Messages reassembled successfully | 30 | VSTP SCCP Performance | Single |

## Alarms & Events

***Table 51 –*** Alarms & Events

| Event Name | Event Id | Raise Condition |
|---|---|---|
| SCCP XUDT Reassembly Failure | 70331 | When reassembly is failed due to any of the below conditions- out of sequence segments received, Internal Error, reassembly Timer Expired. Note: The specific condition will be mentioned in the event reason. |
| SCCP XUDT Segmentation Failure | 70332 | If number of required segments is greater than the maximum number of segments, Maximum number of segments is 16. |

**Limitation**

- Segments of the same message received on different VSTP MPs (as result of CO or CB or any other scenario) will not be handled properly, and as a result reassembly error procedure will be initiated.
- Reassembly is performed for only segmented XUDT Class 1 messages. Segmentation functionality will be performed only on the reassembled messages (performed by vSTP)
- XUDT Reassembly functionality shall not be supported for Route on SSN messages.

**Troubleshooting Steps**

The troubleshooting steps for vSTP XUDT Segmentation feature are as follows:

- If a Segmented Class 1 XUDT message is received for reassembly, then the measurement **VstpRxSccpXUDTSgmnts** is pegged to count the Number of ingress segmented XUDT messages received from network.
- If the reassembly procedure is successful, then the measurement **VstpRxSccpReassProcSucc** is pegged to count the Number of times reassembly procedure completed successfully.
- If the reassembly procedure is successful, then the measurement **VstpRxSccpReassSegSucc** is pegged to count the Number of Segmented XUDT Messages reassembled successfully.
- If the reassembly procedure fails, then the measurement **VstpRxSccpReassProcFail** is pegged to count the number of times reassembly procedure failed.
- If the reassembly procedure fails, then the measurement **VstpRxSccpSgmntsReassFail** is pegged to count the Number of segmented XUDT messages that encountered Reassembly failure due to any errors.
- If the reassembly procedure fails, then the measurement **VstpRxSccpSgmntsDisc** is pegged to count the Number of segmented XUDT messages Discarded, this measurement is pegged if **alwMsgDuringRsmblyErr** in the sccpoptions MO is **False**.
- If a reassembled message is received for segmentation, then the measurement **VstpTxSccpLargeMsg**s is pegged to count the number of reassembled large messages received for segmentation.
- If the segmentation procedure is successful, then the measurement **VstpTxSccpSegProcSucc** is pegged to count the number of times segmentation procedure completed successfully.
- If the segmentation procedure fails, then the measurement **VstpTxSccpSegProcFail** is pegged to count the number of times segmentation procedure failed.
- If reassembly procedure fails, then check the event **SCCP XUDT Reassembly Failure** is raised in the vSTP GUI with the following reasons:
  - **out of sequence segments received**
  - **reassembly Timer Expired**
  - **Internal Error**

    If the reassembly failure occurs due to reassembly Timer Expiry, then user may need to adjust the value of the parameter **reassemblyTimerDurationAnsi** or **reassemblyTimerDurationItu** defined in sccpoptions MO.
- If segmentation procedure fails, then check the event SCCP XUDT Segmentation Failure raised in the vSTP GUI. The event is raised with the reason **number of required segments is greater than the maximum number of segments**. In case of this error, adjust the value of **segmentedMSULength** parameter in sccpoptions MO.

  Contact My Oracle Support in case the problem persists.

**Dependencies**

The XUDT Segmentation feature has no dependency on any other vSTP operation.

The following points must be considered for XUDT Segmentation functionality:

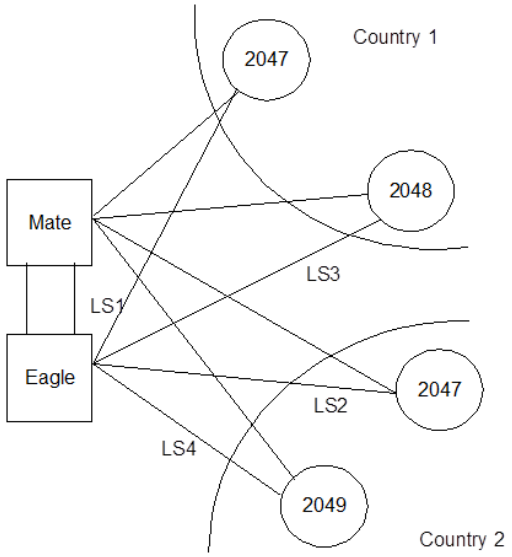
- Segments of the same message received on different vSTP MPs (as result of CO or CB or any other scenario) are not completely supported. The reassembly error procedure will be initiated for such messages.
- Reassembly is performed for only segmented XUDT Class 1 messages. Segmentation functionality will be performed only on the reassembled messages (performed by vSTP).
- XUDT Reassembly functionality is not supported for Route on SSN messages.

## 3.5 *DUPLICATE POINT CODE SUPPORT*

### 3.5.1 *PURPOSE AND SOLUTION*

**Purpose**

This feature will allow an vSTP to route traffic for two or more destinations/countries that may have overlapping point code values. For example, in the network shown in below figure, both Country 1 and Country 2 have SSPs with a PC value of 2047.




**Solution**

- The user must divide their ITU-National/Spare destinations into groups. These groups would likely be based on Country. However, 1 group could have multiple countries within it, or a single country could be divided into multiple groups. The requirement for these groups would be:
    - No duplicate point codes are allowed within a group
    - ITU-National/Spare traffic from a group must be destined for a PC within the same group.
    - The user must assign a unique two letter group code to each group.
- Each group will be identified with a group code and user will provide group code information while adding point code information.
- Group code will be two letter alphabet in the range ‘aa’ to ‘zz’

**Feature Overview**

The Duplicate Point Code support functionality allows vSTP to route traffic for two or more countries that may have overlapping point code values.

The users divide their ITU-National or Spare destinations into groups. These groups are based on the country. When the user enters an ITU National or Spare point code, they must also enter the group code to associate point code with groups. A group code is unique two letter code to identify a group.

**ITU Point Code Support Functionality**

When an ITU-N message arrives at vSTP, an internal point code based on the 14 bit PC is created in the message. Also, the group code gets assigned to the incoming linkset. The following points must be considered while configuring the Duplicate Point Code functionality:

- If the user does not assign any group code while adding ITU-N nodes (Local Signalling Point or Remote Signalling Points), then by default the aa group code is assigned.
- For every group that is used, either a True PC or secondary point code must be provided using the Local Signalling Point command.
- When a message is received from M3UA, then the group code is determined by the network appearance present in the message.

**Operations for MTP3 and SCCP Management Messages**

When vSTP receives a network management message concerning an ITU-National or Spare destination, the routeset to apply the message is determined based on the concerned point code and the group code of the message.

When vSTP generates MTP and SCCP management messages that concern an ITU- National or Spare destination, then only the messages with the same group code are sent to point codes.

When M3UA receives a management message (DAVA, DUNA), then the group code is determined by the **NA** present in the message.

**Interaction**

ITU-International linksets do not have a group code. ITU-National or Spare MSUs received on ITU-International linksets are assigned a group code of **aa**.

Gateway Screening has no impact of group codes support. However, the user can effectively screen on group codes by assigning a different screenset to linksets that have different group codes.

Each ITU-N destination and group code can have it’s own ITU-I or ANSI alias PC. Each ITU-I or ANSI node can be assigned one ITU-N destination. For conversion from ITU-I or ANSI to ITU-N to succeed, the ITU-N alias of the sending node must have the same group code as the destination group code. So each ITU-I or ANSI node can only send and receive messages from one ITU-N group.

## 3.5.2 MEALS

### Measurements

No measurement changes for Duplicate Point Code.

### Alarms & Events

No new event or alarm added for this feature.

**Troubleshooting Steps**

In case of the error scenarios, different vSTP alarms and measurements are pegged.

**Dependencies**

The Duplicate Point Code support feature has no dependency on any other vSTP operation.

The following points must be considered while configuring Duplicate Point Code functionality:

- The Duplicate Point Code support is applicable only for ITU-National/ITU-Spare Destinations.
- The ITU-National traffic from a group must be destined for a PC within the same group.
- No duplicate point codes are allowed within a group
    - It is not possible to change the group code for a destination. To move a destination from one group to another, user must provision a new destination that uses the new group code and delete the old destination.
    - If conversion between ITU-N and ITU-I or ANSI is used, then only one ITU-N group can send traffic to a specific ANSI or ITU-I node.

## 3.6 VSTP IR21 BULK UPLOAD FOR SS7 SECURITY

### 3.6.1 PURPOSE AND SOLUTION

**Purpose**

Certain GSM MAP messages requires validation of information present at MAP and SCCP portion, based on that validation packets are either allowed or discarded. There are approx. 800 mobile network operators across world and information pertaining to their network resides in GSMA IR.21 document. Operator wise Network information data viz. MCC-MNC, Node GT (HLR/VLR/MSC) and CC-NDC becomes huge and cumbersome for operator to maintain and upload that in vSTP to implement security check for CAT2 messages.

**Solution**

This feature allows a vSTP to provides security to detect anomalies on inbound packets through bulk upload of customer IR.21 documents.

**Feature Overview**

The goal is to develop a utility that will read and record all information present in GSMA IR.21 into a configuration file. This configuration file will be uploaded in vSTP directly from this Utility. The file (.csv) will have network node details for Operators Roaming Partner. This utility shall be external to vSTP node which can be installed on Linux machine.

SCPVAL GTT Action on EAGLE shall be enhanced to address SS7 CAT2 security checks. This GTT action will ensure MSU details viz. CGPA and IMSI belongs to same Operator after validating it with the newly generated table.

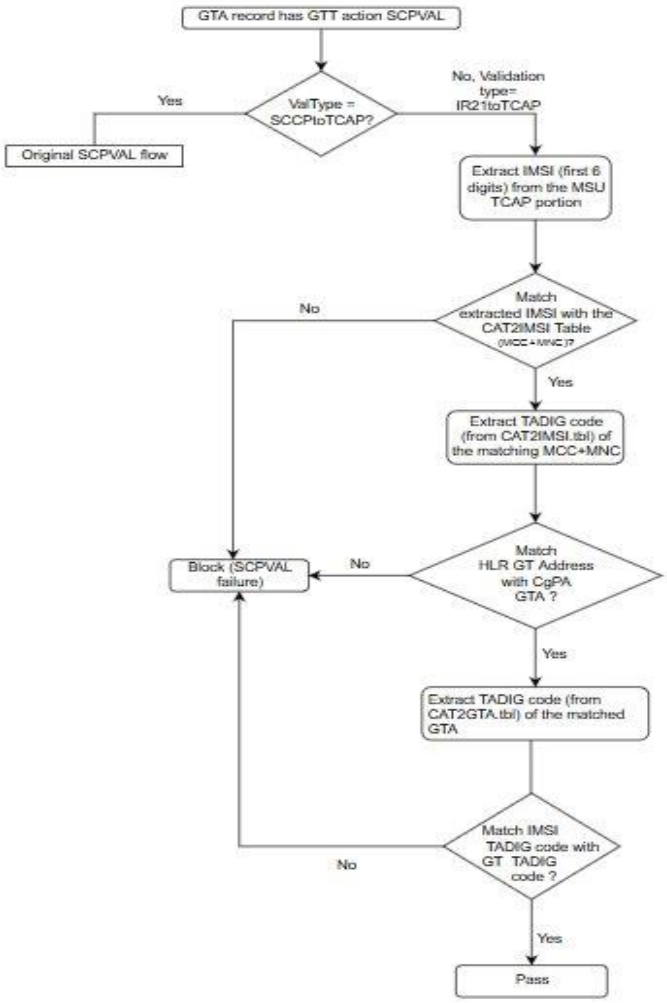
This feature will allow an vSTP to read the IR.21 document and store that in tabular form which can then be referred by EAGLE for CAT2 security implementation.

There are three part of CAT2 feature.

- First part will parses IR.21 xml file on the Linux machine, extract the information needed from the IR.21 file for validation of the message and convert its data in .csv format.

- Load this .csv file into vSTP through bulk upload. This data will be stored on SO's and MP's IR21RoutingInfo and IR21NetworkElement table. Note: We can use MMI also to populate individual entry in IR21RoutingInfo and IR21NetworkElement table, but the individual configuration is not the preferred way.
- Configure GTT to enforce CAT2 validation on received MSU. Validation shall be done through data available in IR21RoutingInfo and IR21NetworkElement table.

Following is the CAT2 flow diagram:




## 3.6.2 MEALS

### Measurements

***Table 52 – Measurements***

| Measurement Name | Dimension | Description | Interval in Mins | Group | Type |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| VstpGttActScpvalCat2Total | Arrayed | The total number of messages received by SCPVAL CAT2 GTT Action. | 30 | Performance | Simple |
| VstpGttActScpvalCat2Discard | Arrayed | The total number of messages discarded by SCPVAL CAT2 GTT Action. | 30 | Performance | Simple |
| VstpGttActScpvalCat2NotApplied | Arrayed | The total number of messages where SCPVAL CAT2 GTT Action was not applied. | 30 | Performance | Simple |
| VstpCgpaGttActScpvalCat2Total | Arrayed | The total number of messages received by SCPVAL CAT2 GTT Action per CGTT. | 30 | Performance | Simple |
| VstpCgpaGttActScpvalCat2Discard | Arrayed | The total number of messages discarded by SCPVAL CAT2 GTT Action per CGTT. | 30 | Performance | Simple |
| VstpCgpaGttActScpvalCat2NotApplied | Arrayed | The total number of messages where SCPVAL CAT2 GTT Action was not applied per CGTT. | 30 | Performance | Simple |

## Alarms & Events

No new event or alarm added for this feature.

**Limitation**

- Only Opcodes listed below shall be decoded to apply IMSI & CgPA check.

provideRoamingNumber 4

provideSubscriberInfo70

provideSubscriberLocation 83

cancelLocation 3

insertSubscriberData 7

deleteSubscriberData 8

getPassword 18

reset 37

activateTraceMode 50

unstructuredSS-Request 60

unstructuredSS-Notify 61

informServiceCentre 63

alertServiceCentre 64

setReportingState 73

remoteUserFree 75

istCommand 88

- Only First 5-6 digits from IMSI is considered for matching.

| <- 3 Digits -> | <- 2 or 3 Digits -> | |
|---|---|---|
| **MCC** | **MNC** | **MSIN** |
| **< ---------- Not more than 15 Digit ---------- >** | | |

- IMSI is composed of three parts:

Mobile Country Code (MCC)

Mobile Network Code (MNC)

Mobile Subscriber Identification Number (MSIN)

- MCC and MNC determines the Operator ID. This will be used for CAT2 validation.
- First match shall be performed with 6 digit and if match not found then it shall be performed with 5 digit else fail.

## 3.7 DSA WITH UDR

Diameter Security Application (DSA) has implemented various Countermeasures to detect vulnerability in an ingress diameter message from a foreign network.

The Countermeasures can be divided into two categories.

- Stateful Countermeasure
- Stateless Countermeasure

Stateful Countermeasures are those Countermeasures which require to maintain State Data for validating vulnerability of the ingress diameter messages. These State-Data will be maintained in the UDR.

Stateless Countermeasures are those Countermeasure which do not require data from earlier diameter message for checking vulnerability of a given incoming diameter message. Message is screened for vulnerability by using DSA configuration data.

The Stateless Countermeasures are executed in the below sequence [if configured and enabled]:

- Application-Id Whitelist Screening
- Application-Id and Command-Code Consistency Check
- Origin Realm and Destination Realm Whitelist Screening
- Origin host and Origin Realm Consistency Check
- Destination-Realm and Origin-Realm Match Check
- Visited-PLMN-ID and Origin-Realm Consistency Check
- Realm and IMSI Consistency Check
- Subscriber Identity Validation

- Specific AVP Screening
- AVP Multiple Instance Check

The Stateful Countermeasures are executed in the below sequence [if configured and enabled] :

- Message Rate Monitoring
- Time-Distance Check
- Previous Location Check
- Source Host Validation HSS
- Source Host Validation MME

### 3.7.1 *UPGRADE*

DSA with UDR in Release 8.5.0.0.0 does not support the upgrade.

### 3.7.2 *COMMON SECURITY*

Time distance check counter measure is common for DSA and VSTP applications and both the applications use UDR as a common DB for security across protocol use cases.

This Countermeasure is applicable across 4G network and also for Cross Protocol Security Use Case.

Time Distance Check validate the movement from 2G/3G location to 4G Location against configured min transit time between two location using IMSI as key value.

For example: First subscriber is roaming into 2G network, update location comes to 2G home location though vSTP application ( vSTP will update the subscriber details in UDR with IMSI as key. Then subscriber move to 4G network within min transition time , update location comes to 4G Home network through DSA Application , DSA application read the data from UDR if already there and apply Business login and marked the message as vulnerable if transition from 2G location to 4G location is within min transition time.

This counter measure provides common configuration for both vSTP & UDR for TimeDistChk_Country_Config table. This table is not recommended to edit when vSTP and DSA is running under same SOAM server for Common Security feature.

# 4 MEAL INSERTS

This section summarizes the changes to Alarms, Measurements, KPIs and MIBs. In the following inserts pertain to DSR Release 8.5 MEAL snapshot and deltas to earlier releases 8.3.0.0.0, 8.4.0.0.0, 8.4.0.3.0, and 8.4.0.5.0.

- The DSR/SDS 8.1.2.0.0 GA Release is DSR/SDS 8.1.2.0.0-81.25.0
- The DSR/SDS 8.2.1.0.0 GA Release is DSR/SDS 8.2.1.0.0_82.17.0
- The DSR/SDS 8.3.0.0.0 GA Release is DSR/SDS 8.3.0.0.0-83.15.0
- The DSR/SDS 8.4.0.0.0 GA Release is DSR/SDS 8.4.0.0.0-84.15.0
- The DSR/SDS 8.4.0.3.0 GA Release is DSR/SDS 8.4.0.3.0-85.17.0
- The DSR/SDS 8.4.0.5.0 GA Release is DSR/SDS 8.4.0.5.0-88.9.1
- The DSR/SDS 8.5.0.0.0 GA Release is DSR/SDS 8.5.0.0.0-90.11.0
- The DSR/SDS 8.5.0.2.0 GA Release is DSR/SDS 8.5.0.2.0_92.7.0

## *4.1 DSR/SDS 8.5.0.2.0 MEAL SNAPSHOT*

MEAL_dsr-8.5.0.2.0-92.3.0.xlsx

MEAL_sds-8.5.0.2.0-92.3.0.xlsx

### 4.1.1 *MEAL DELTA BETWEEN 8.1.0.0.0 AND 8.5.0.2.0*

MEAL_dsr-8.1.0.0.0-81.20.0-dsr-8.5.0.2.0-92

MEAL_sds-8.1.0.0.0-81.20.0-sds-8.5.0.2.0-9

### 4.1.2 *MEAL DELTA BETWEEN 8.2.1.0.0 AND 8.5.0.2.0*

MEAL_dsr-8.2.1.0.0_82.19.0-dsr-8.5.0.2.0-92

MEAL_sds-8.2.1.0.0-82.17.0-sds-8.5.0.2.0-9

### 4.1.3 *MEAL DELTA BETWEEN 8.3.0.0.0 AND 8.5.0.2.0*

MEAL_dsr-8.3.0.0.0-83.15.0-dsr-8.5.0.2.0-92

MEAL_sds-8.3.0.0.0-83.15.0-sds-8.5.0.2.0-9

### 4.1.4 *MEAL DELTA BETWEEN 8.4.0.0.0 AND 8.5.0.2.0*

MEAL_dsr-8.4.0.0.0-84.15.0-dsr-8.5.0.2.0-92

MEAL_sds-8.4.0.0.0-84.15.0-sds-8.5.0.2.0-9

### 4.1.5 *MEAL DELTA BETWEEN 8.4.0.3.0 AND 8.5.0.2.0*

MEAL_dsr-8.4.0.3.0-8
5.17.0-dsr-8.5.0.2.0-9

MEAL_sds-8.4.0.3.0-8
5.17.0-sds-8.5.0.2.0-9

### 4.1.6 *MEAL DELTA BETWEEN 8.4.0.5.0 AND 8.5.0.2.0*

MEAL_dsr-8.4.0.5.0-8
8.9.1-dsr-8.5.0.2.0-92

MEAL_sds-8.4.0.5.0-8
8.9.1-sds-8.5.0.2.0-92

### 4.1.7 *MEAL DELTA BETWEEN 8.5.0.0.0 AND 8.5.0.2.0*

MEAL_dsr-8.5.0.0.0-9
0.11.0-dsr-8.5.0.2.0-9

MEAL_sds-8.5.0.0.0-9
0.11.0-sds-8.5.0.2.0-9

### 4.1.8 *MEAL DELTA BETWEEN 8.5.0.1.0 AND 8.5.0.2.0*

MEAL_dsr-8.5.0.1.0-9
1.17.0-dsr-8.5.0.2.0-9

MEAL_sds-8.5.0.1.0-9
1.17.0-sds-8.5.0.2.0-9

## *4.2 DSR/SDS 8.5.0.1.0 MEAL SNAPSHOT*

MEAL_dsr-8.5.0.1.0-9
1.17.0.xlsx

MEAL_sds-8.5.0.1.0-9
1.17.0.xlsx

### 4.2.1 *MEAL DELTA BETWEEN 8.1.2.0.0 AND 8.5.0.1.0*

MEAL_dsr-8.1.0.0.0-8
1.20.0-dsr-8.5.0.1.0-9

MEAL_sds-8.1.0.0.0-8
1.20.0-sds-8.5.0.1.0-9

### 4.2.2 *MEAL DELTA BETWEEN 8.2.1.0.0 AND 8.5.0.1.0.*


MEAL_dsr-8.2.1.0.0_8
2.19.0-dsr-8.5.0.1.0-9


MEAL_sds-8.2.1.0.0-8
2.17.0-sds-8.5.0.1.0-9

### 4.2.3 *MEAL DELTA BETWEEN 8.3.0.0.0 AND 8.5.0.1.0*


MEAL_dsr-8.3.0.0.0-8
3.15.0-dsr-8.5.0.1.0-9


MEAL_sds-8.3.0.0.0-8
3.15.0-sds-8.5.0.1.0-9

### 4.2.4 *MEAL DELTA BETWEEN 8.4.0.0.0 AND 8.5.0.1.0*


MEAL_dsr-8.4.0.0.0-8
4.15.0-dsr-8.5.0.1.0-9


MEAL_sds-8.4.0.0.0-8
4.15.0-sds-8.5.0.1.0-9

### 4.2.5 *MEAL DELTA BETWEEN 8.4.0.3.0 AND 8.5.0.1.0*


MEAL_dsr-8.4.0.3.0-8
5.17.0-dsr-8.5.0.1.0-9


MEAL_sds-8.4.0.3.0-8
5.17.0-sds-8.5.0.1.0-9

### 4.2.6 *MEAL DELTA BETWEEN 8.4.0.5.0 TO 8.5.0.1.0*


MEAL_dsr-8.4.0.5.0-8
8.9.1-dsr-8.5.0.1.0-91.


MEAL_sds-8.4.0.5.0-8
8.9.1-sds-8.5.0.1.0-91.

### 4.2.7 *MEAL DELTA BETWEEN 8.5.0.0.0 TO 8.5.0.1.0*


MEAL_dsr-8.5.0.0.0-9
0.11.0-dsr-8.5.0.1.0-9


MEAL_sds-8.5.0.0.0-9
0.11.0-sds-8.5.0.1.0-9

## 4.3 DSR/SDS 8.5.0.0.0 MEAL SNAPSHOT

MEAL_dsr-8.5.0.0.0-9
0.8.0.xlsx

MEAL_sds-8.5.0.0.0-9
0.8.0.xlsx

### 4.3.1 MEAL DELTA BETWEEN 8.1.2.0.0 AND 8.5.0.0.0

MEAL_dsr-8.1.0.0.0-8
1.20.0-dsr-8.5.0.0.0-9(

MEAL_sds-8.1.0.0.0-8
1.20.0-sds-8.5.0.0.0-9(

### 4.3.2 MEAL DELTA BETWEEN 8.2.1.0.0 AND 8.5.0.0.

MEAL_dsr-8.2.1.0.0_8
2.19.0-dsr-8.5.0.0.0-9(

MEAL_sds-8.2.1.0.0-8
2.17.0-sds-8.5.0.0.0-9(

### 4.3.3 MEAL DELTA BETWEEN 8.3.0.0.0 AND 8.5.0.0.0

MEAL_dsr-8.3.0.0.0-8
3.15.0-dsr-8.5.0.0.0-9(

MEAL_sds-8.3.0.0.0-8
3.15.0-sds-8.5.0.0.0-9(

### 4.3.4 MEAL DELTA BETWEEN 8.4.0.0.0 AND 8.5.0.0.0

MEAL_dsr-8.4.0.0.0-8
4.15.0-dsr-8.5.0.0.0-9(

MEAL_sds-8.4.0.0.0-8
4.15.0-sds-8.5.0.0.0-9(

### 4.3.5 MEAL DELTA BETWEEN 8.4.0.3.0 AND 8.5.0.0.0

MEAL_dsr-8.4.0.3.0-8
5.17.0-dsr-8.5.0.0.0-9(

MEAL_sds-8.4.0.3.0-8
5.17.0-sds-8.5.0.0.0-9(

### 4.3.6 MEAL DELTA BETWEEN 8.4.0.5.0 TO 8.5.0.0.0

MEAL_dsr-8.4.0.5.0-8
8.9.1-dsr-8.5.0.0.0-90.

MEAL_sds-8.4.0.5.0-8
8.9.1-sds-8.5.0.0.0-90.

# 5 REFERENCE LIST

The DSR 8.5 Release Notice and Customer Documentation can be found at the following OTN link.
http://docs.oracle.com/en/industries/communications/diameter-signaling-router/index.html

DSR IP Flow Document: CGBU_019284 (ORACLE Internal Document)

Platform IP Flow Document: CGBU_PM_1112 (ORACLE Internal Document)