Oracle® COMMUNICATIONS

Diameter Signaling Router
DSR Network Impact Report

Release 8.4

F12342 Revision 02
June 2020

Oracle Diameter Signaling Router DSR Network Impact Report,

Release 8.4

Contents

ORACLE® COMMUNICATIONS 1

DIAMETER SIGNALING ROUTER DSR NETWORK IMPACT REPORT 1

1 INTRODUCTION 11

1.1 PURPOSE/SCOPE 11
1.2 COMPATIBILITY 11
1.2.1 8.4.0.0.0 PRODUCT COMPATIBILITY 11
1.3 DSR 8.4.X INCOMPATIBILITY FEATURES 11
1.3.1 8.4.0.3.0 INCOMPATIBILITY FEATURES 11
1.3.2 8.4.0.5.0 INCOMPATIBILITY FEATURES 11
1.4 DISCLAIMERS 12

2 OVERVIEW OF DSR 8.4.X FEATURES 13

2.1 ENHANCEMENTS TO DSR 8.4.0.0.0 14
2.1.1 Alarm Group Feature 15
2.1.2 Time distance CHECK ENHANCEMENT FEATURE 15
2.1.3 VNFM 16
2.1.4 MMI UPDATES 17
2.1.5 VSTP SPARE POINT CODE SUPPORT 18
2.1.6 VSTP MNP SUPPORT OVER SS7 19
2.1.7 VSTP MTP SCREENING SUPPORT 19
2.1.8 VSTP Multiple point code support 19
2.1.9 VSTP flow control ENHANCEMENTS 19
2.1.10 VSTP ANSI-ITU Conversion SUPPORT 20
2.1.11 VSTP GTT Modifications 20
2.1.12 VSTP SCCP loop DETECTION 20
2.1.13 VSTP MBR enhancement 20
2.1.14 SCEF 20
2.2 ENHANCEMENTS TO DSR 8.4.0.3.0 22
2.2.1 vstp GTT Throttle action 23
2.2.2 vstp GTT scpval action 23
2.2.3 vstp MTP based gtt 23
2.2.4 vstp sfapp stateful security 23
2.2.5 vstp TDm support 24
2.2.6 vstp M3UA Client support 24
2.2.7 VSTP IDPR MOSMS 24
2.2.8 vstp eir enhancements 24
2.3 ENHANCEMENTS TO DSR 8.4.0.5.0 25
2.3.1 VSTP sls rotation 25
2.3.2 VSTP sfapp dynamic learning 25
2.3.3 VSTP tif support 25
2.3.4 VSTP segmented xudt 26
2.3.5 VSTP duplicate point code support 26
2.3.6 vSTP GUI configuration 26
2.3.7 vstp ir21 bulk upload for ss7 security 26
2.3.8 dsa with udr 26
2.4 HARDWARE CHANGES 27
2.4.1 Hardware Supported 27
2.4.2 Hardware Upgrade 27
2.5 SOFTWARE DETAILS 27
2.5.1 Software Platform Components in 8.4.0.0.0 27
2.5.2 Software Platform Components in 8.4.0.3.0 28
2.5.3 Software Platform Components in 8.4.0.5.0 28
2.5.4 DSR Release 8.4 29
2.5.5 iDIH 8.2.1 and 8.2.2 29

2.5.6 SDS 8.4 29
2.6 FIRMWARE CHANGES 29
2.7 UPGRADE OVERVIEW 30
2.7.1 DSR Upgrade Path 30
2.7.2 The supported upgrade paths for SDS 8.4 30
2.7.3 The supported upgrade paths for iDIH 8.2.1 31
2.7.4 Upgrade Execution 31
2.7.5 Limitations 31
2.8 MIGRATION OF DSR DATA 32
3 RELEASE 8.4.0.0.0 FEATURE OAM CHANGES 33
3.1 ALARM GROUP FEATURE 33
3.1.5 Alarm Aggregation interworking with Alarm Group feature 36
3.2 TIME DISTANCE CHECK 36
3.3 VNFM 38
3.4 SCEF 42
3.5 VSTP SPARE POINT CODE SUPPORT 50
3.6 VSTP MNP GPORT 54
3.7 VSTP MNP ATI NP 63
3.8 VSTP MNP INP 66
3.9 VSTP MTP SCREENING SUPPORT 68
3.10 VSTP MULTIPLE POINT CODE SUPPORT 74
3.11 VSTP FLOW CONTROL ENHANCEMENTS 80
3.12 VSTP ANSI-ITU CONVERSION 80
4 RELEASE 8.4.0.3.0 FEATURE OAM CHANGES 82
4.1 GTT THROTTLE ACTION 82
4.2 GTT SCPVAL ACTION 86
4.3 MTP BASED GTT 89
4.4 SFAPP STATEFUL SECURITY 90
4.5 TDM SUPPORT 95
4.6 M3UA CLIENT SUPPORT 99
4.7 VSTP IDPR MOSMS 102
4.8 VSTP EIR ENHANCEMENTS 106
5 RELEASE 8.4.0.5.0 FEATURE OAM CHANGES 112
5.1 SLS ROTATION 112
5.2 SFAPP DYNAMIC LEARNING 115
5.3 TIF SUPPORT 117
5.4 SEGMENTED XUDT 119
5.5 DUPLICATE POINT CODE SUPPORT 123
5.6 VSTP IR21 BULK UPLOAD FOR SS7 SECURITY 125
5.7 DSA WITH UDR 129
6 MEAL INSERTS 131
6.1 DSR/SDS 8.4.0.5.0 MEAL SNAPSHOT 131
6.1.1 MEAL Delta between 8.4.0.0.0 and 8.4.0.5.0 131
6.1.2 MEAL Delta between 8.4.0.3.0 and 8.4.0.5.0 131
6.2 DSR/SDS 8.4.0.3.0 MEAL SNAPSHOT 131
6.2.1 MEAL Delta between 7.0.1.0.0 and 8.4.0.3.0 131
6.3 DSR/SDS 8.4.0.0.0 MEAL SNAPSHOT 132
6.3.1 MEAL Delta between 8.0.0.0.0 and 8.4.0.0.0 132
6.3.2 MEAL Delta between 8.1.0.0.0 and 8.4.0.0.0 132
6.3.3 MEAL Delta between 8.2.1.0.0 and 8.4.0.0.0 132
6.3.4 MEAL Delta between 8.3.0.0.0 and 8.4.0.0.0 132
7 REFERENCE LIST 133

List of Figures

Figure 1 – DSR Upgrade Paths..........30
Figure 2 – SDS Upgrade Paths..........30
Figure 3 – IDIH Upgrade Paths..........31
Figure 4 - Alarm Group Feature Design..........33
Figure 5 – Peer Node Alarm Group GUI..........34
Figure 6 – Connection Alarm Group GUI..........35
Figure 7 – DCA Framework Screen..........37
Figure 8 – VNF Scaling..........39
Figure 9 – VNF LCM Operation..........40
Figure 10 – VNF Forceful Termination..........41
Figure 11 – VNF Graceful Termination..........42
Figure 12 – LWM2M Registration Process..........43
Figure 13 – Subscription and Observe..........43
Figure 14 – Event Notification..........44
Figure 15 – Subscription and cancel..........44
Figure 16 – Action on DL data transfer..........44
Figure 17 – T8 Event..........45
Figure 18 – DELETE Subscription..........46
Figure 19 – T8 Request and Response..........46
Figure 20 – PUT Operation..........47
Figure 21 – DELETE Operation..........47
Figure 22 – T8 POST Operation..........48
Figure 23 – API based charging for Invocation events..........49
Figure 24 – Notify and Uplink Request..........49
Figure 25 – SLTM Operation accept..........52
Figure 26 – SLTM Operation discard..........52
Figure 27 – MMI API Guide reference..........53
Figure 28 – ATINP message flow..........64
Figure 29 – INQP message flow..........67
Figure 30 – MTP screening design diagram..........69
Figure 31 – Process Flow of GTT Throttle Action..........84
Figure 32 – Flow Diagram for SCPVAL..........87

List of Tables

Table 1 - DSR 8.4.0.0.0 New Features/Enhancements 14
Table 2 - Alarm Group Feature Description 15
Table 3 - Time Distance Check Feature Description 15
Table 4 - VNFM Feature Description 16
Table 5 - MMI Updates Feature Description 17
Table 6 - VSTP Spare point code Feature Description 18
Table 7 - VSTP MNP support over SS7 Feature Description 19
Table 8 - VSTP mtp screening support Feature Description 19
Table 9 - VSTP multiple point code support Feature Description 19
Table 10 - VSTP Flow Control Enhancements Feature Description 19
Table 11 - VSTP ANSI-ITU Conversion support Feature Description 20
Table 12 - VSTP GTT Modifications Feature Description 20
Table 13 - VSTP sccp loop detection Feature Description 20
Table 14 - VSDTP MBR enhancement Feature Description 20
Table 15 - SCEF Feature Description 20
Table 16 - DSR 8.4.0.3.0 New Features/Enhancements 22
Table 17 – VSTP GTT Throttle Action Feature Description 23
Table 18 – VSTP GTT SCPVAL Action Feature Description 23
Table 19 – VSTP GTT SCPVAL Action Feature Description 23
Table 20 –VSTP MTP Based GTT Feature Description 23
Table 21 – VSTP SFAPP Stateful Security Feature Description 23
Table 22 – VSTP TDM Support Feature Description 24
Table 23 – VSTP M3UA Client Support Feature Description 24
Table 24 – VSTP IDPR MOSMS Feature Description 24
Table 25 – VSTP EIR Enhancements Feature Description 24
Table 26 - DSR 8.4.0.5.0 New Features/Enhancements 25
Table 27 – VSTP SLS Rotation Feature Description 25
Table 28 – VSTP SFAPP Dynamic Learning Feature Description 25
Table 29 – VSTP TIF Support Feature Description 25
Table 30 – VSTP Segmented XUDT Feature Description 26
Table 31 – VSTP Duplicate Point Code Feature Description 26
Table 32 – VSTP GUI Configuration Feature Description 26
Table 33 – VSTP IR21 Bulk Upload for SS7 Security 26
Table 34 – VSTP GUI Configuration Feature Description 26
Table 35 - Hardware Details 27
Table 36 – Software Platform Component Details – 8.4.0.0.0 27
Table 37 – Software Platform Component Details – 8.4.0.0.0 28
Table 38 – Software Platform Component Details – 8.4.0.5.0 28
Table 39 - Release Details 29
Table 40 - IDIH Details 29
Table 41 - SDS Details 29
Table 42 – Security Countermeasure Config 36
Table 43 -System Config Options Table 36
Table 44 -TimeDistChk_Config Table 36
Table 45 – TimeDistChk Continent Config 37
Table 46 – TimeDistChk MCC Config 37
Table 47 - NI and Name 50
Table 48 - Configuration details1 51
Table 49 - Configuration details2 51
Table 50 – MO Details 1 53
Table 51 – MO Details 2 53
Table 52 – MO details 3 59
Table 53 – Measurements details1 59
Table 54 – Measurement details2 60
Table 55 – Events & Alarms 1 61
Table 56 – MO’s for ATI NP Feature 65
Table 57 – ATI NP Measurements details 65
Table 58 – Alarms & Events for ATI NP feature 66

Table 59 – Measurements for INPQ feature 67
Table 60 – Alarms & Events for INPQ feature........68
Table 61 - Message processing with mtpScrEventLog and mtpScrTestMode option when NSFI is FAIL........71
Table 62 – MO details for MTP screening feature 72
Table 63 – Alarms and Events for MTP screening feature........73
Table 64 – SCCP message routing behavior........75
Table 65 – Point Code provisioning 77
Table 66 – Isp Name with reference........78
Table 67 – Field name with Description........78
Table 68 – AppType with Ssn id 78
Table 69 – Alarms & Description........79
Table 70 – Events & Description........79
Table 71 – MO details for GTT action feature 80
Table 72 – Measurements........84
Table 73 – Alarms for GTT Throttle Action Feature........85
Table 74 – GTT Action SCPVAL – Parameters........86
Table 75 – Alarms for GTT SCPVAL Action Feature 88
Table 76 – Measurements........90
-Table 77 – Measurements........91
Table 78 – Alarms for SFAPP Stateful Security Feature........93
Table 79 – Measurements........95
Table 80 – Events for TDM Support Feature 97
Table 81 – Alarms for TDM Support Feature........97
Table 82 – Measurements........100
Table 83 – Measurements........103
Table 84 – Events for vSTP IDPR MOSMS Feature 105
Table 85 – Measurements........107
Table 86 – Alarms & Events for vSTP EIR Feature........108
Table 87 – Measurements........116
Table 88 – Alarms & Events 117
Table 89 – Measurements........118
Table 90 – Alarms & Events........119
Table 91 – Measurements........120
Table 92 – Alarms & Events........121
Table 93 – Measurements........127

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
LTE	Long Term Evolution

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

Acronym/Term	Definition
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/SCOPE

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

1.2 COMPATIBILITY

1.2.1 8.4.0.0.0 PRODUCT COMPATIBILITY

DSR 8.4.0.0.0 is compatible with IDIH 8.0, 8.1, 8.2, 8.2.1 and 8.2.2

DSR 8.4.0.0.0 is compatible with SDS 8.0.1, 8.1.2, 8.2.1, 8.3 and 8.4.0

DSR 8.4.0.0.0 is compatible with APIGW 8.4.0

DSR 8.4.0.0.0 is compatible with TPD 7.6, ComCOL 7.5, AppWorks 8.4, EXGSTACK 8.4, TVOE 3.6, PM&C 6.6, APIGW 8.4 and UDR 12.5.1

SDS 8.4 is compatible with TPD 7.6, ComCOL 7.5, AppWorks 8.4, EXGSTACK 8.4, TVOE 3.6 and PM&C 6.6.

1.3 DSR 8.4.X INCOMPATIBILITY FEATURES

The following features has been made incompatible from DSR 8.3 and remain incompatible in 8.4

- Active/Standby DA-MP server architecture (1+1) redundancy model
- MAP-IWF
- Radius
- GLA

1.3.1 8.4.0.3.0 INCOMPATIBILITY FEATURES

Virtualized Engineered DSR (VEDSR) deployment also known as TVOE based Fully Virtualized Rack Mount Server (FV RMS) Signaling node is not supported from DSR Release 8.3 onwards.
Following are the non-supported network elements of Virtualized Engineered DSR (VEDSR):

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

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

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

1.3.2 8.4.0.5.0 INCOMPATIBILITY FEATURES

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. Refer to NIR document and Diameter Security Application with UDR User’s Guide for details.

Customers using this application must not upgrade DSR software to DSR 8.4.0.5.0 release and should migrate to "DSA with UDR" based application.

1.4 DISCLAIMERS

This document summarizes Release Diameter Signaling Router Release 8.4 new and enhancement features as compared to Release 8.3, and the operations impacts 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 8.4.X FEATURES

This section provides a high-level overview of the DSR 8.4.x release features that may impact OAM interfaces and activities.

For a list of all features, please see Release Notes for DSR 8.4.x 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 8.4 Feature Guide" found at the following link:
http://docs.oracle.com/en/industries/communications/diameter-signaling-router/index.html

2.1 ENHANCEMENTS TO DSR 8.4.0.0.0

Note: For information on upgrade planning and required steps before upgrade, please refer to the DSR 8.4 Software Upgrade Guide on the public Oracle Documentation Site:

Docs.oracle.com → Industries → Oracle Communications → Diameter Signaling Router → Release 8.4.

***Table 1* - DSR 8.4.0.0.0 New Features/Enhancements**

DSR 8.4 Feature/Enhancement Name
Alarm Group Feature
Time Distance Check Enhancement Feature
VNFM
MMI Updates
vSTP Spare Point Code Support
vSTP MNP support over SS7 using vSTP
vSTP MTP Screening Support
vSTP Multiple Point Code Support for virtual STP
vSTP Flow control enhancements
vSTP ANSI-ITU Conversion support
vSTP GTT Modifications
vSTP SCCP loop detection
vSTP MBR enhancements
SCEF

2.1.1 *ALARM GROUP FEATURE*

Table 2 - **Alarm Group Feature Description**

Name	**Description**	**Scope**
POR: 27797933	DSR displays all relevant individual and aggregated alarms for Connection/Peer as per functionality captured by Alarm Aggregation feature. However due to the large size of the network, volume of connection and peer initiating alarms can be high. This limits operator view to monitor the state of crucial managed objects. Operators have requested the Alarm Group feature that allows them to suppress similar type of alarms, after a given threshold. Alarm Group feature allows operator to do the following: ➢ Define group of peers/connections for which alarm throttling is required ➢ Define throttling level for each group This is named as Alarm Group feature. This feature is administratively managed by the operator through GUI, Configuration and alarm monitoring is also on Active SOAM Note: Alarm Aggregation feature and Alarm Group feature are mutually exclusive for Peer Nodes and Connections.	Alarm Group feature shall work for Peer Node Alarm Group and Connection Alarm Group, Alarm monitoring is limited to Peer Nodes and Connections that are added in Alarm Group

2.1.2 *TIME DISTANCE CHECK ENHANCEMENT FEATURE*

Table 3 - **Time Distance Check Feature Description**

Name	Description	Scope

POR: 28108321 28899149 27737337	This feature provides the following enhancement: Enhance DSA logic to detect whether the IMSI is vulnerable or not when subscriber is an outbound roamer. Update DSR OAM GUI to configure MCC_Based, VPLMN_Based and Continent - Changed allowed even if diameter connection is enabled. • This feature is intended for security countermeasure which detects if subscriber is indeed physically able to move roam from one network/country to another network/country within the given transit time. Ex: If the mobile subscriber is roaming from USA to India within 1 hour which is physically impossible to commute in 1 hour. Such scenarios can be the hacker induced security attacks on the MNO's network. • This countermeasure is applicable to outbound roaming subscriber and compares the current location with previous location of the subscriber and analyze if it is physically possible to move from the previous location to this new one. This can be achieved by maintaining the minimum transit time between each of the VPLMN Id's or MCC's of VLPMN Id's. • If subscriber moves from one country to another country, and the time difference between last update location and current update location procedure (i.e. time difference between last ULR and current AIR/ULR) is not greater than the configured transit time between corresponding countries(MCC's) then ingress AIR/ULR shall be marked as vulnerable by DEA	Enhancement Request

2.1.3 *VNFM*

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

Table 4 - **VNFM Feature Description**

Name	Description	Scope

POR: 28104363	DSR VNFM is an application that helps to deploy virtual DSRs quickly by automating the entire deployment process and making it ready to use in the shortest possible time. The VNFM is responsible for the lifecycle management of virtual network functions (VNFs) under the control of the network function virtualization orchestrator (NFVO). The VNFM would be helpful in • Instantiate Network OAM VNFs with fixed IPs • Instantiate Signaling VNFs with Multiple XSIs for fixed IPs • Instantiating DSR DR NOAM • Instantiating SDS DR NOAM • Scale VNF -Scale VNF to Level (Scale Out C Level servers of Signaling VNF) -Scale VNF to Arbitrary size (Scale Out C Level servers of Signaling VNF) • Query Individual / All LCM Operation(s) Terminating VNF • Discover VNF • Terminate VNF	Enhancement Request

2.1.4 *MMI UPDATES*

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

Table 5 - **MMI Updates Feature Description**

Name	Description	Scope

POR 27096415 Machine-to-Machine interface updates	MMIs have been enabled for the following: • SBR Configuration o SBR Databases o SBR Database Resizing Plans o SBR Data Migration Plans o Database Options • Dynamic Peer Discovery - Configuration o Realms o DNS Sets o Discovery Attributes • Diameter Common - MPs o DA-MP o SS7-MP • Topology Hiding – Configuration o Trusted Network Lists o Path Topology Hiding Configuration Sets o S6a/S6d HSS Topology Hiding Configuration Sets o MME/SGSN Topology Hiding Configuration Sets o S9 PCRF Topology Hiding Configuration Sets Options o S9 AF/pCSCF Topology Hiding Configuration Sets o Protected Networks • User Configuration - Appworks -Software Management o Versions • User Configuration - Appworks - Access Control o Users o Groups o Sessions o Authorized Ips • User Configuration - Appworks - Remote Server o LDAP Authentication o Data Export • User Configuration - Appworks - Alarms o Alarm History o Trap Logs • User Configuration - Appworks - Administration o General Options	Enhancement Request User Configuration – Appworks – Remote Server o Data Export User Configuration – Appworks - Alarms o Place and Place Association in Alarm History o Export in Alarm History

2.1.5 *VSTP SPARE POINT CODE SUPPORT*

The DSR 8.4 provides support for ITUI spare domain and ITUN spare.

***Table 6* - VSTP Spare point code Feature Description**

Name	Description	Scope
POR 28219409	This feature provides support for ITUI spare domain and ITUN spare domain.	Enhancement Request

2.1.6 VSTP MNP SUPPORT OVER SS7

The DSR 8.4 vSTP provides support for MNP over SS7. It covers GPORT, ATINPQ and IDPQ.

Table 7 - VSTP MNP support over SS7 Feature Description

Name	Description	Scope
POR 27355487 & 28829325 – {28648154, 28648192}	This feature provides support for GPORT, ATINPQ and IDPQ. Also, it includes support for HEX digits for GTA.	Enhancement Request

2.1.7 VSTP MTP SCREENING SUPPORT

The DSR 8.4 vSTP provides MTP screening features, which allows screening of messages based on the parameters of MTP3 layer.

Table 8 - VSTP mtp screening support Feature Description

Name	Description	Scope
POR 25973064	MTP screening feature provides solution to screen the messages based on MTP3 layer parameters of the messages.	Enhancement Request

2.1.8 VSTP MULTIPLE POINT CODE SUPPORT

The DSR 8.4 vSTP provides support for multiple local point codes of a particular domain. This feature provides support for SPC and CPC.

Table 9 - VSTP multiple point code support Feature Description

Name	Description	Scope
POR 28126356	This feature supports assigning multiple point codes to VSTP i.e. SPC (Secondary Point Codes) and CPC (Capability Point Codes). Earlier, vSTP was used to support only one local signaling point for a domain, which is now known as TPC (True point code). CPC also optionally permits attaching service/application with hosted CPC. SPC in turn enables collapsing/merging of multiple STPs into one vSTP.	Enhancement Request

2.1.9 VSTP FLOW CONTROL ENHANCEMENTS

The DSR 8.4 vSTP supports with the egress and ingress flow control

Table 10 - VSTP Flow Control Enhancements Feature Description

Name	Description	Scope
POR 28609300	Flow Control is essential to prevent it from sending bursty traffic in the egress path and receiving bursty traffic in ingress path. This maintains a balanced message processing rate in the ingress path based on capacity at run time.	Enhancement Request

2.1.10 *VSTP ANSI-ITU CONVERSION SUPPORT*

The DSR 8.4 vSTP supports ANSI/ITU SCCP Conversion

Table 11 - **VSTP ANSI-ITU Conversion support Feature Description**

Name	Description	Scope
POR 25973034	ANSI/ITU SCCP Conversion feature provides the vSTP the ability to support a generic ANSI/ITU SCCP Conversion. ANSI/ITU SCCP Conversion is supported for UDT, UDTS, XUDT and XUDTS messages.	Enhancement Request

2.1.11 *VSTP GTT MODIFICATIONS*

The DSR 8.4 vSTP supports GTT modifications feature

Table 12 - **VSTP GTT Modifications Feature Description**

Name	Description	Scope
POR 25972692	This request is to allow the support of GTT Modification as per EAGLE code in vSTP (equivalent to Advanced GTT Modification in EAGLE World)	Enhancement Request

2.1.12 *VSTP SCCP LOOP DETECTION*

The DSR 8.4 vSTP supports SCCP looping issues.

Table 13 - **VSTP sccp loop detection Feature Description**

Name	Description	Scope
POR 29136281	Loop Detection feature allows user to solve the SCCP looping issue without the need for network-wide implementation of a protocol.	Enhancement Request

2.1.13 *VSTP MBR ENHANCEMENT*

The DSR 8.4 vSTP MBR Enhancement enabled GTT routing based on three new parameters (VLRNP, SMRPOA and SMRPDA)

Table 14 - **VSDTP MBR enhancement Feature Description**

Name	Description	Scope
POR 27393516	This feature allows GTT routing based on MAP component (i.e. IMSI, MSISDN, VLRNB, SMRPOA, SMRPDA). MBR Enhancement enabled GTT routing based on three new parameters (VLRNP, SMRPOA and SMRPDA).	Enhancement Request

2.1.14 *SCEF*

Table 15 - **SCEF Feature Description**

Name	Description	Scope
POR 28111851 LWM2M Gateway	LWM2M Gateway(LG) shall act as cross proxy converting the CoAP messages to HTTP messages and vice versa to enable IP device communication between IoT devices and SCS/AS (Note: CoAP protocol is used as transport protocol to carry the LWM2M payload.) LG shall enable LWM2M protocol based IoT device communication for following use cases: – Access Control – Device Management – Connectivity – Firmware Update – Location – Connectivity Statistics LG shall enabled SCEF to be used for following transport bindings: – TCP, UDP, TLS and DLTS (covered by this feature) (***Note: Scope of the current release will be UDP transport only***) – Non IP Data Delivery (existing SCEF functionality) LG shall provide unified T8 interface for both IP and Non IP device communication enabling MO, MT and monitoring event MTC call flows.	Enhancement Request
POR 28111828 MQTT Broker	MQTT Broker(MB) shall act as cross proxy converting the MQTT messages to HTTP messages and vice versa to enable IP device communication between IoT devices and SCS/AS. MB shall enable IoT device communication for following use case: – MO messages MB shall enable SCEF to be used for following transport bindings: – TCP and TLS (covered by this feature) MB shall provide unified T8 interface for IP device communication enabling monitoring event call flows	Enhancement Request

POR 28629586 QoS Control	According to 3GPP specifications, there are two main Network Attach options to support IOT connectivity. 1. Attach with PDN (Packet Data Network) connection. 2. Attach without PDN connection. For IOT connectivity attach with PDN scenario, The 3rd party SCS/AS may request that a data session to a UE that is served by the 3rd party service provider is set up with a specific QoS (e.g. low latency or jitter) and priority handling. This section defines requirements for supporting the functionality where Oracle SCEF can enable PCRF setting up of the QoS via Rx Interface as requested from SCS/AS.	Enhancement Request
POR 28124801 API Based Charging Solution	SCEF shall support API based charging for the following procedures that operate across the T8 reference point. In addition, charging shall be implemented based on Offline event based charging mechanism. Moreover, the event are. – NIDD Events – Monitoring Events – Device Triggering Events – Enhanced coverage Restriction Events.	Enhancement Request
POR 28113780 SCEF T8 Compliance Changes	SCEF Compliance changes as per 3GPP TS 29.122 latest specification i.e.,v15	Enhancement Request

2.2 ENHANCEMENTS TO DSR 8.4.0.3.0

Note: For information on upgrade planning and required steps before upgrade, please refer to the DSR 8.4 Software Upgrade Guide on the public Oracle Documentation Site:

Docs.oracle.com → Industries → Oracle Communications → Diameter Signaling Router → Release 8.4.0.3.0.

***Table 16* - DSR 8.4.0.3.0 New Features/Enhancements**

DSR 8.4.0.3.0 Feature/Enhancement Name
vSTP Gtt Throttle Action
vSTP _GTT_SCPval
vSTP MTP Based GTT
vSTP Sfapp Stateful Security
vSTP_TDM_Support
vSTP M3UA Client Support
vSTP IDPR MOSMS

vSTP EIR Enhancements

2.2.1 VSTP GTT THROTTLE ACTION

Table 17 **– VSTP GTT Throttle Action Feature Description**

Name	Description	Scope
POR: 29152322	The GTT Throttle action is part of SS7 security firewall. It provides support for Egress throttling of GTT messages in vSTP	Enhancement Request

2.2.2 VSTP GTT SCPVAL ACTION

Table 18 **– VSTP GTT SCPVAL Action Feature Description**

Name	Description	Scope
POR: 29152322	The SCPVAL GTT action along with relevant parameters performs the validation on MAP parameters by comparing the SCCP and MAP digits.	Enhancement Request

Table 19 **– VSTP GTT SCPVAL Action Feature Description**

Name	Description	Scope
POR: 29152322	The SCPVAL GTT action along with relevant parameters performs the validation on MAP parameters by comparing the SCCP and MAP digits.	Enhancement Request

2.2.3 VSTP MTP BASED GTT

Table 20 **–VSTP MTP Based GTT Feature Description**

Name	Description	Scope
POR: 29115539	This feature provides the capability of performing SCCP services on MTP-routed messages. Therefore, allows the operator to perform GTT and GTT Actions on MTP Routed MSUs, similar to GTT handling for GT Routed MSUs.	Enhancement Request

2.2.4 VSTP SFAPP STATEFUL SECURITY

Table 21 **– VSTP SFAPP Stateful Security Feature Description**

Name	Description	Scope
POR:	SS7 Firewall - Stateful Applications (SFAPP) allows vSTP to validate the messages coming in for a subscriber by validating them against the Visitor Location Register (VLR). The last seen details of the subscriber can be fetched from the Home Location Register (HLR). Once the HLR provides a validity of the new VLR, vSTP then allows the message into the network. If the message is not validated, it is handled as per configuration (either silent discard, fallback, or respond with error).	Enhancement Request

2.2.5 VSTP TDM SUPPORT

***Table 22* – VSTP TDM Support Feature Description**

Name	Description	Scope
POR:	This feature was introduced in 8.4.0.3.1 patch release. The feature provides access to E1/T1 links based ADAX HDC3 PCIe TDM Card using PCIe Pass-through.	Enhancement Request

2.2.6 VSTP M3UA CLIENT SUPPORT

***Table 23* – VSTP M3UA Client Support Feature Description**

Name	Description	Scope
POR: 29113802	The MTP3-User Adaptation (M3UA) Client support allows vSTP to trigger the M3UA connection initiation. For information related to M3UA Protocol	Enhancement Request

2.2.7 VSTP IDPR MOSMS

***Table 24* – VSTP IDPR MOSMS Feature Description**

Name	Description	Scope
POR: 29265575, 29302872, 29302882, 29302888, 29302902, 29265587, 29152427	The Prepaid IDP Query Relay feature (IDP Relay) provides a mechanism to ensure the correct charging for calls from prepaid subscribers in a portability environment. The Mobile Originated Short Message Service (MO SMS) features address the number portability requirements of wireless network operators for delivery of Mobile Originated SMS messages. The vSTP 5 ISS MO SMS features apply number portability database lookup to SMS messages for GSM networks, validates subscriber use of the correct Short Message Service Center, and delivers messages to Prepaid Servers if either the Calling Party Number or Called Party Number is associated with a prepaid subscriber.	Enhancement Request

2.2.8 VSTP EIR ENHANCEMENTS

***Table 25* – VSTP EIR Enhancements Feature Description**

Name	Description	Scope
POR: 29651069, 29651081	This feature allows using EirOptoins MO to enable white listed IMSI/IMEI logging. Instead of IP, vSTP logs the OPC in the logs. Instead of IP, DEIR logs the Origin Host and Origin Realm in the logs. OPC/Origin Host and Origin Realm is logged by default. There are no options to enable/disable logging OPC/Origin Host and Origin Realm. Total 100K IMSI white listing is supported on vSTP and DEIR (Diameter EIR)	Enhancement Request

2.3 ENHANCEMENTS TO DSR 8.4.0.5.0

Note: For information on upgrade planning and required steps before upgrade, please refer to the DSR 8.4 Software Upgrade Guide on the public Oracle Documentation Site:

Docs.oracle.com → Industries → Oracle Communications → Diameter Signaling Router → Release 8.4.0.5.0.

Table 26 - DSR 8.4.0.5.0 New Features/Enhancements

DSR 8.4.0.5.0 Feature/Enhancement Name
vSTP SLS Rotation
vSTP_SFAPP_Dynamic
vSTP Tif Support
vSTP Segmented XUDT
vSTP Duplicate Point Code Support
vSTP GUI Configuration
vSTP IR21 Bulk Upload for SS7 Security
DSA with UDR

2.3.1 VSTP SLS ROTATION

Table 27 – VSTP SLS Rotation Feature Description

Name	Description	Scope
POR: 29153597	The Signaling Link Selection(SLS) Rotation feature facilitates a proper distribution of SLS values to provide a good distribution of traffic and load sharing across links and linksets.	Enhancement Request

2.3.2 VSTP SFAPP DYNAMIC LEARNING

Table 28 – VSTP SFAPP Dynamic Learning Feature Description

Name	Description	Scope
POR: 30087663	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.	Enhancement Request

2.3.3 VSTP TIF SUPPORT

Table 29 – VSTP TIF Support Feature Description

Name	Description	Scope
POR: 30087787	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.	Enhancement Request

2.3.4 VSTP SEGMENTED XUDT

Table 30 **– VSTP Segmented XUDT Feature Description**

Name	Description	Scope
POR: 29265596	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	Enhancement Request

2.3.5 VSTP DUPLICATE POINT CODE SUPPORT

Table 31 **– VSTP Duplicate Point Code Feature Description**

Name	Description	Scope
POA: 30087756	The Duplicate Point Code support functionality allows vSTP to route traffic for two or more countries that may have overlapping point code values.	Enhancement Request

2.3.6 VSTP GUI CONFIGURATION

Table 32 **– VSTP GUI Configuration Feature Description**

Name	Description	Scope
POR:	The vSTP configurations and Maintenance operations can be performed using VSTP GUI on Active System OAM (SOAM). vSTP configuration GUI allows you to manage vSTP configuration. You can perform different tasks on an Active System OAM (SOAM). The VSTP > Configuration folder contains the tables used in vSTP operations. To configure a specific table, select the table name from the list to display the table details. vSTP maintenance pages display status information for Links, RSPs, Connections, Linksets, and SCCP applications.	Enhancement Request

2.3.7 VSTP IR21 BULK UPLOAD FOR SS7 SECURITY

Table 33 **– VSTP IR21 Bulk Upload for SS7 Security**

Name	Description	Scope
POR:	This feature allows a vSTP to provides security to detect anomalies on inbound packets through bulk upload of customer IR.21 documents.	Enhancement Request

2.3.8 DSA WITH UDR

Table 34 **– VSTP GUI Configuration Feature Description**

Name	Description	Scope

POR:	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	Enhancement Request

2.4 HARDWARE CHANGES

2.4.1 HARDWARE SUPPORTED

Table 35 - **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 8.4 release builds on top of the RMS and provides the support for the newer and higher capacity X7-2 RMS hardware.

2.5 SOFTWARE DETAILS

2.5.1 SOFTWARE PLATFORM COMPONENTS IN 8.4.0.0.0

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

Table 36 – **Software Platform Component Details – 8.4.0.0.0**

Component	Release
TPD 64 Bit	7.6.1.0.0-88.55.0
COMCOL	7.5.0.14.0-14027
APIGW	8.4.0.0.0_84.15.0
PM&C	6.6.1.0.0-66.9.0
TVOE	3.6.1.0.0-88.55.0
AppWorks	8.4.0-84.11.0

EXGSTACK	8.4.0-84.12.0
HP Firmware FUP	2.2.13 (Minimum[1])
Oracle Firmware	3.1.8 (Minimum[2])

2.5.2 *SOFTWARE PLATFORM COMPONENTS IN 8.4.0.3.0*

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

***Table 37* – Software Platform Component Details – 8.4.0.0.0**

Component	Release
TPD 64 Bit	
COMCOL	
APIGW	
PM&C	
TVOE	
AppWorks	
EXGSTACK	
HP Firmware FUP	2.2.13 (Minimum[3])
Oracle Firmware	3.1.8 (Minimum[4])

2.5.3 *SOFTWARE PLATFORM COMPONENTS IN 8.4.0.5.0*

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

***Table 38* – Software Platform Component Details – 8.4.0.5.0**

Component	Release
TPD 64 Bit	
COMCOL	
APIGW	
PM&C	
TVOE	
AppWorks	
EXGSTACK	
HP Firmware FUP	2.2.13 (Minimum[5])

[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.

[5] - 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.

Oracle Firmware	3.1.8 (Minimum[6])

2.5.4 *DSR RELEASE 8.4*

DSR Release 8.4 inherits all functionality from DSR 8.3

***Table 39* - Release Details**

Component	Release
DSR Release	8.4

2.5.5 *IDIH 8.2.1 AND 8.2.2*

***Table 40* - IDIH Details**

Component	Release
IDH Release	8.2.1, 8.2.2

DSR 8.4 is compatible with IDIH 7.3, 8.0, 8.1, 8.2, 8.2.1 and 8.2.2

2.5.6 *SDS 8.4*

***Table 41* - SDS Details**

Component	Release
SDS Release	8.4

DSR 8.4 is compatible with SDS 8.0.1, 8.2.1, 8.2.1, 8.3 and 8.4

NOTE**:** It is recommended for SDS to be upgraded before the DSR. SDS release 8.4 is compatible with DSR releases 8.0.1, 8.1.1, 8.2.1 and 8.3

2.6 *FIRMWARE CHANGES*

Firmware release guidance is provided via DSR 8.4 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 8.4.x link.

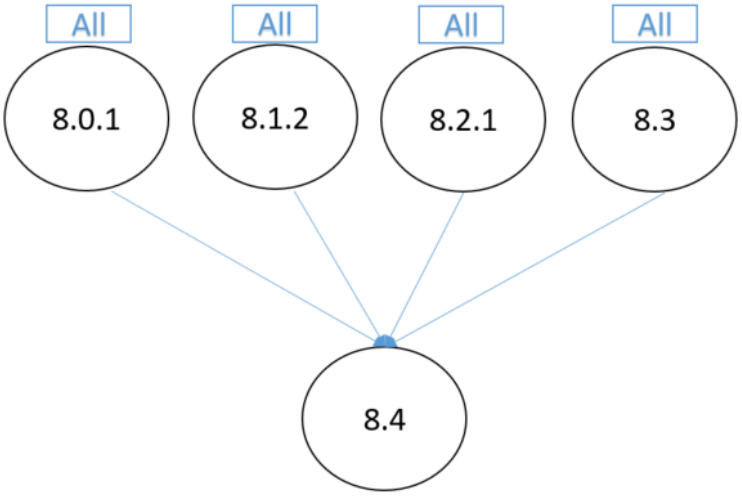
[6] - This represents the minimum release of the Oracle firmware series to support all content in the Platform 74 release. It is recommended that the latest firmware release always be used in order to address known security issues.

2.7 UPGRADE OVERVIEW

This section provides an overview of the Upgrade activities for Release 8.4.

2.7.1 DSR UPGRADE PATH

The supported upgrade paths for DSR 8.4 are:

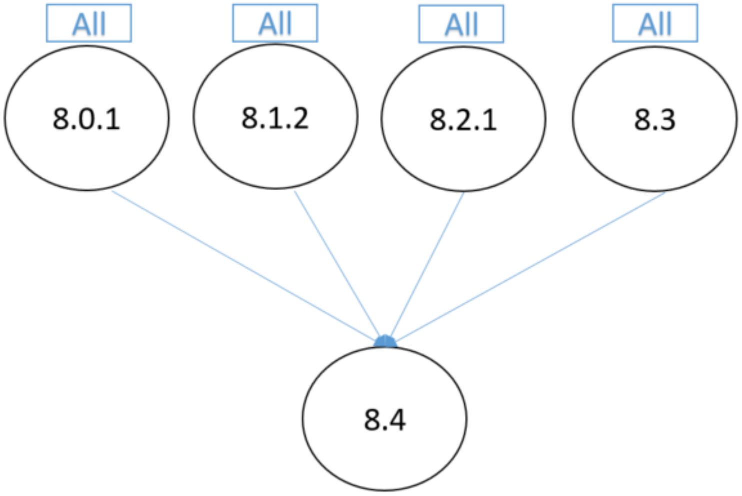


All in the figure above refers to the available releases and all of its maintenance releases

Figure 1 – DSR Upgrade Paths

2.7.2 THE SUPPORTED UPGRADE PATHS FOR SDS 8.4

The supported upgrade paths for SDS 8.4 are



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

Figure 2 – SDS Upgrade Paths

!!Caution!!

SDS Upgrade

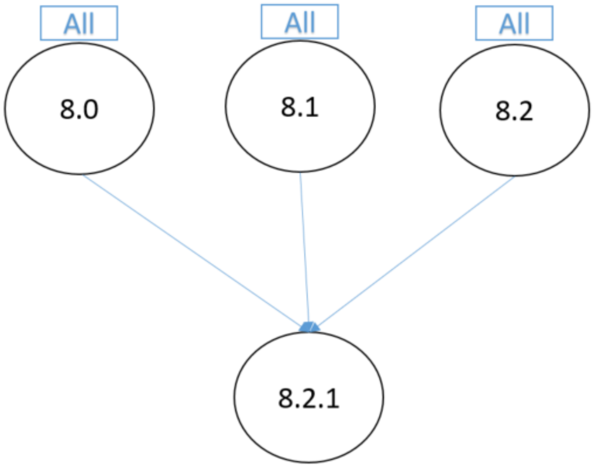
If the customer deployment has only FABR features enabled, it is recommended to upgrade the SDS nodes first before upgrading the DSR nodes.

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

.

2.7.3 *THE SUPPORTED UPGRADE PATHS FOR IDIH 8.2.1*

The supported upgrade paths for iDIH 8.2.1 are



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

Figure 3 – IDIH Upgrade Paths

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

2.7.4 *UPGRADE EXECUTION*

With DSR 8.4, 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 8.4 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 please note that upgrade will fail if utilization of /var/TKLC/rundb partition is more than 70% which may be true in case of larger AppEventLog file size (~5.5 GB in size). To prevent the above listed issues, we need to assign/allocate /var/TKLC/rundb size and AppEventLog file size in sync i.e. AppEventLog file size (plus some delta for other files like MeasStat) should be always less than 70 % of /var/TKLC/rundb partition size.

2.8 MIGRATION OF DSR DATA

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

3 RELEASE 8.4.0.0.0 FEATURE OAM CHANGES

At the time of upgrade to DSR 8.4.0.0.0 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.

Note: this section covers OAM changes that will be visible after upgrade to the 8.4.0.0.0 release and does not include changes that will be seen only as new Optional Features are activated on the system (post-upgrade activity, and customer specific).

3.1 ALARM GROUP FEATURE

3.1.1 PROBLEM STATEMENT

DSR displays all relevant individual and aggregated alarms for Connection/Peer as per functionality captured by Alarm Aggregation feature. However due to the large size of the network, volume of connection and peer initiating alarms can be high. This limits operator view to monitor the state of crucial managed objects. Operators have requested the feature that allows them to suppress similar type of alarms, after a given threshold.

3.1.2 OVERVIEW

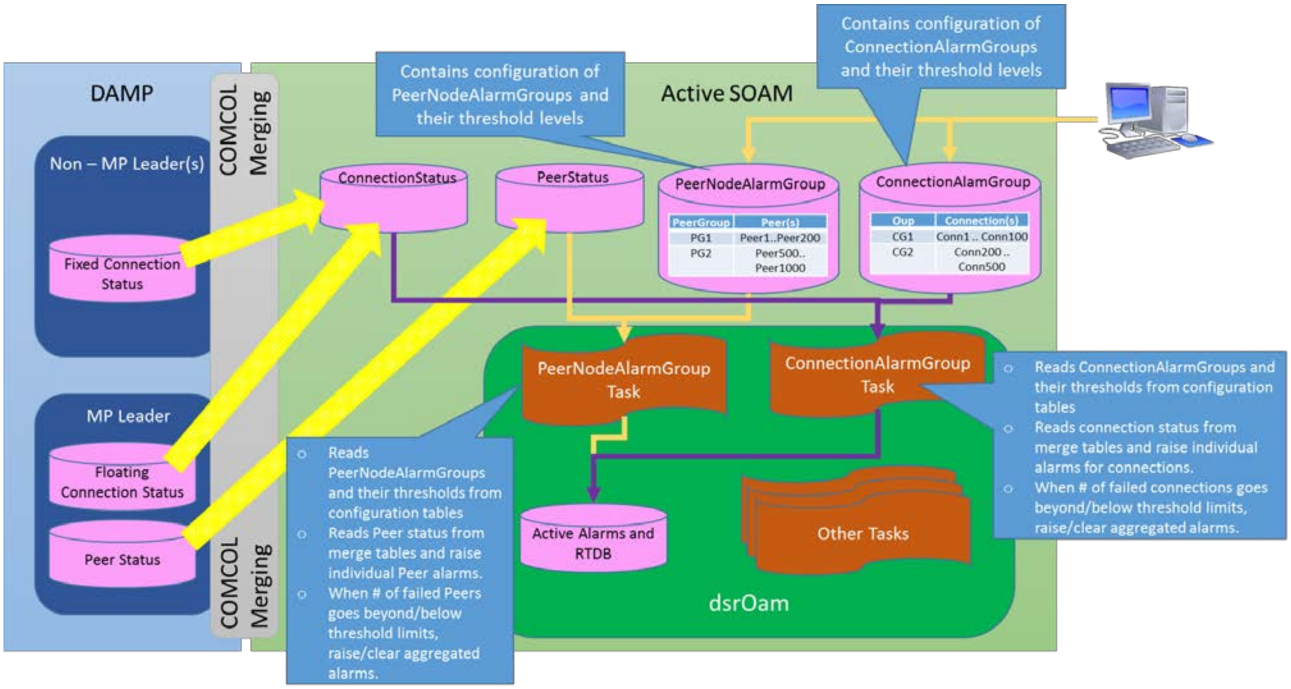
This feature allows operator to do the following:

- ➢ Define group of peers/connections for which alarm throttling is required
- ➢ Define throttling level for each group

This is named as Alarm Group feature. This feature is administratively managed by the operator through GUI.

Note: Alarm Aggregation feature and Alarm Group feature are mutually exclusive for Peer Nodes and Connections.

Overall working design on this feature is as follows:



Contains configuration of PeerNodeAlarmGroups and their threshold levels

Contains configuration of ConnectionAlarmGroups and their threshold levels

PeerGroup	Peer(s)
PG1	Peer1..Peer200
PG2	Peer500.. Peer1000

Oup	Connection(s)
CG1	Conn1 .. Conn100
CG2	Conn200 .. Conn500

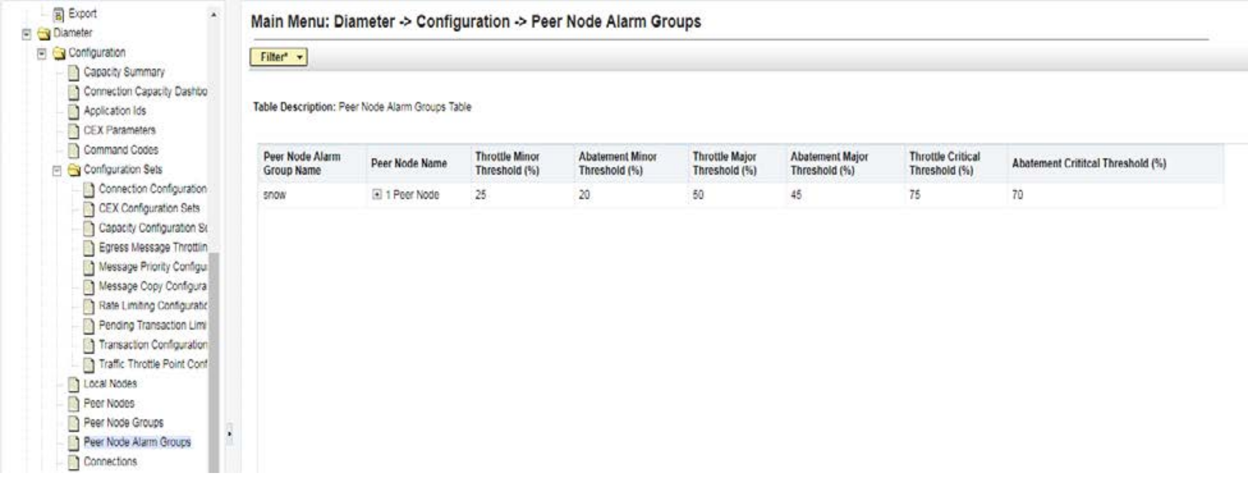
- ○ Reads PeerNodeAlarmGroups and their thresholds from configuration tables
- ○ Reads Peer status from merge tables and raise individual Peer alarms.
- ○ When # of failed Peers goes beyond/below threshold limits, raise/clear aggregated alarms.

- ○ Reads ConnectionAlarmGroups and their thresholds from configuration tables
- ○ Reads connection status from merge tables and raise individual alarms for connections.
- ○ When # of failed connections goes beyond/below threshold limits, raise/clear aggregated alarms.

Figure 4 - Alarm Group Feature Design

3.1.3 PEER NODE ALARM GROUP

A new GUI screen “Peer Node Alarm Groups” allows user to create Peer Node Alarm Groups, associate the peer nodes to a Peer Node Alarm Group and define throttle and abatement threshold (Minor, Major and Critical) level for each Alarm Group. Threshold level of a Peer Node Alarm Group has no impact on the thresholds of other Peer Node Alarm Group,



Main Menu: Diameter -> Configuration -> Peer Node Alarm Groups

Table Description: Peer Node Alarm Groups Table

Peer Node Alarm Group Name	Peer Node Name	Throttle Minor Threshold (%)	Abatement Minor Threshold (%)	Throttle Major Threshold (%)	Abatement Major Threshold (%)	Throttle Critical Threshold (%)	Abatement Crititcal Threshold (%)
snow	⊞ 1 Peer Node	25	20	50	45	75	70

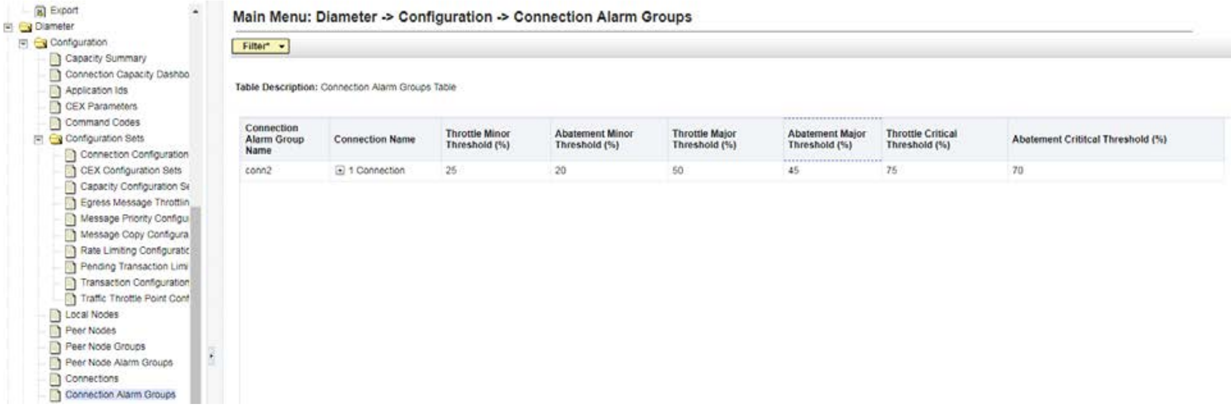
Figure 5 **– Peer Node Alarm Group GUI**

Given below is the high level working of Peer Node Alarm Group:

1. New task “PeerNodeAlarmGroup” is added in dsroam process. This task is running on Active SOAM.
2. This task checks the administrative state of Alarm Group feature in every 10 seconds.
3. If Alarm Group feature is enabled, then the task proceeds further for the processing. If Alarm Group feature is disabled, there is no alarm reporting for peer node failures or threshold condition by “PeerNodeAlarmGroup” task.
4. Underlying steps are performed if Alarm Group feature is enabled:
    a) Read the configuration data of Peer Node Alarm Group(s). This includes peer nodes in a Peer Node Alarm Group and the threshold level of that alarm group. It also reads the Peer Node status table to see if peer node alarm is set by DA-MP.
    Please note that peer node status is only reported by MP Leader. In case of no MP leader detection or multi-MP leaders condition, (No / Multi) MP leader alarm is raised. There is no reporting of individual peer alarms or group threshold alarm.
    b) Raise the alarm for every failed peer node in an alarm group until throttling level of that Peer Node Alarm Group is not reached.
    c) Once throttle condition is met for a Peer Node Alarm Group, peer node failure alarms for the peers in that alarm group are cleared. This also raises a group alarm to signify that throttle threshold condition for the Peer Node Alarm Group has been reached. Threshold level of a Peer Node Alarm Group is unaffected by threshold of other Peer Node Alarm Group.
    d) There are no alarms raised for individual peer node failures in a Peer Node Alarm Group until group threshold alarm of Minor or Major or Critical severity is present.
    e) When number of failed peer nodes in a Peer Node Alarm Group drops below the abatement minor threshold, then threshold alarm for a Peer Node Alarm Group is cleared. Further, individual alarms for peer node failures in that Peer Node Alarm Group are asserted.
    f) DSROAM process does not have alarm reporting for a peer not added in any Peer Node Alarm Group.
    g) If peer node is associated to a Peer Node Alarm Group, then Peer Node Status screen displays its associated Peer Node Alarm Group Name and the id of the alarm raised by DA-MP against the peer node.
5. Underlying steps are performed if Alarm Group feature is disabled:
    a) Clear the Peer Node Alarm Group threshold alarm if it had been raised before.
    b) Individual peer node failure alarms remain unaffected.

3.1.4 CONNECTION ALARM GROUP

A new GUI screen “Connection Alarm Groups” allows user to create Connection Alarm Groups, associate the connections to a Connection Alarm Group and define throttle and abatement threshold (Minor, Major and Critical) level for each Alarm Group. Threshold level of a Connection Alarm Group has no impact on the thresholds of other Connection Alarm Group,



Main Menu: Diameter -> Configuration -> Connection Alarm Groups

Table Description: Connection Alarm Groups Table

Connection Alarm Group Name	Connection Name	Throttle Minor Threshold (%)	Abatement Minor Threshold (%)	Throttle Major Threshold (%)	Abatement Major Threshold (%)	Throttle Critical Threshold (%)	Abatement Critical Threshold (%)
conn2	⊞ 1 Connection	25	20	50	45	75	70

Figure 6 – Connection Alarm Group GUI

Given below is the high level working of Connection Alarm Group:

1. New task “ConnectionAlarmGroup” is added in dsroam process. This task is running on Active SOAM.
2. This task checks the administrative state of Alarm Group feature in every 10 seconds.
3. If Alarm Group feature is enabled, then the task proceeds further for the processing. If Alarm Group feature is disabled, there is no alarm reporting for connection failures or threshold condition by “ConnectionAlarmGroup” task.
4. Underlying steps are performed if Alarm Group feature is enabled:
    a) Read the configuration data of Connection Alarm Group(s). This includes connections in a Connection Alarm Group and the threshold level of that alarm group. It also reads the Connection status table to see if connection alarm is set by DA-MP.
       Please note that floating connection status is only reported by MP Leader. In case of no MP leader detection or multi-MP leaders condition, (No / Multi) MP leader alarm is raised. Consequently, there is no reporting of floating connections.
       Fixed connection status is reported by the MP owning the connection. Fixed connection status is not affected by No MP leader or multi-MP leader conditions. Consequently, there is reporting of fixed connection status.
    b) Raise the alarm for every failed connection in an alarm group until throttling level of that Connection Alarm Group is not reached.
    c) Once throttle condition is met for a Connection Alarm Group, connection failure alarms for the connections in that alarm group are cleared. This also raises a group alarm to signify that throttle threshold condition for the Connection Alarm Group has been reached. Threshold level of a Connection Alarm Group is unaffected by threshold of other Connection Alarm Group.
    d) There are no alarms raised for individual connection failures in a Connection Alarm Group until group threshold alarm of Minor or Major or Critical severity is present.
    e) When number of failed connections in a Connection Alarm Group drops below the abatement minor threshold, then threshold alarm for a Connection Alarm Group is cleared. Further, individual alarms for connection failures in that Connection Alarm Group are asserted.
    f) DSROAM process does not have alarm reporting for a connection not added in any Connection Alarm Group.
    g) If connection is associated to a Connection Alarm Group, then Connection Status screen displays its associated Connection Alarm Group Name and the id of the alarm raised by DA-MP against the connection.
5. Underlying steps are performed if Alarm Group feature is disabled:
    a) Clear the Connection Alarm Group threshold alarm if it had been raised before.
    b) Individual connection failure alarms remain unaffected.

3.1.5 ALARM AGGREGATION INTERWORKING WITH ALARM GROUP FEATURE

3.2 TIME DISTANCE CHECK

3.2.1 DESCRIPTION

if a S6a/d ULR/AIR is received for an Outbound Roamer and an earlier ULR has already been received for this Roamer and the time difference between the previously received ULR's VPLMN-Id/MCC and the current ULR/AIR's VPLMN-Id/MCC is less than the minimum transition time configured in Time Distance Check Config Table then current received ULR/AIR will be considered as Vulnerable by Time-Distance-Check CounterMeasure and configured action will be performed as defined

3.2.2 OVERVIEW

The feature enhance DSA logic to find whether Outbound Roamer is Vulnerable or not. Following tables has to be configured.

Table 42 – Security Countermeasure Config

Admin Status	Admin_Status defines the current Admin State of the countermeasure. If the Admin_Status is configured as **Enable**, then only the countermeasure business logic is executed. If the Admin_Status is configured as **Disable**, then the countermeasure business logic is not executed.
Operating Mode	Defines the action taken if a message is found to be vulnerable by the countermeasure. If the Operating_Mode is configured as **Detection_Only**, then the countermeasure works on monitoring mode. The vulnerable message is only reported to the user. DSA further processes the message (depending upon Continue If vulnerable configuration) for executing the next available countermeasure. If the Operating_Mode is configured as **Detection_And_Correction_By_Drop**, then the vulnerable diameter message is discarded at DSR and is not processed/relayed any further. If the Operating_Mode is configured as **Detection_And_Correction_By_Send_Answer**, then the vulnerable diameter message is rejected by DSR by sending an Error Answer and is not processed/relayed any further.

***Table 43 -**System Config Options Table*

MCC or VPLMN-ID	Indicates the source and destination node IDs configured in **Error! Reference source not found.** are MCCs or VPLMN-IDs. If MCC_Or_VPLMNID is configured as **MCC_Based**, then the source and destination node IDs are treated as MCC values. If MCC_Or_VPLMNID is configured as **VPLMNID_Based**, then the source and destination node IDs are treated as VPLMN-ID values.

***Table 44 -**TimeDistChk_Config Table*

Source and Destination Node-IDs	Defines the two Node-ID values. Node-ID can be MCC or VPLMN-ID of any given network. Value of MCC_Or_VPLMNID configured in *Error! Reference source not found.* determines that the configured Node-IDs is MCCs or VPLMN-IDs. If MCC_Or_VPLMNID is configured as **MCC_Based**, then the Node_ID_1 and Node_ID_2 are treated as MCC values.

	If MCC_Or_VPLMNID is configured as **VPLMNID_Based**, then the Node_ID_1 and Node_ID_2 are treated as VPLMN-ID values.
Minimum Transition Time	Defines the minimum transition time (in minutes) required to move between Node_ID_1 and Node_ID_2.

Table 45 – TimeDistChk Continent Config

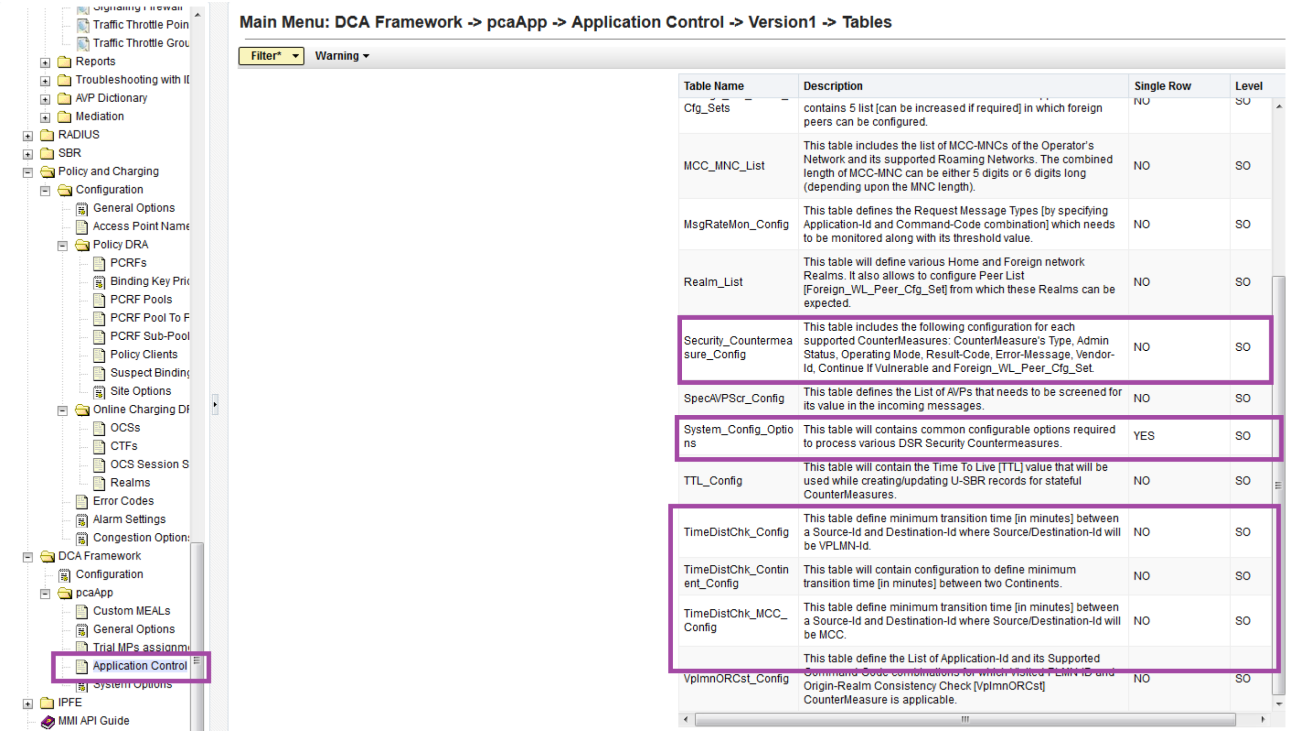
Continent_1 and Continent_2	List of Various supported continents.
Minimum Transition Time	Minimum Transition time [in Minutes] between the Continent_1 and Continent_2.[Range = 0 - 720]

Table 46 – TimeDistChk MCC Config

Node_Id_1 and Node_Id_2	Node_Id is MCC .[Range = 3digits Integer]
Minimum Transition Time	Minimum Transition time [in Minutes] between the Node_Id_1 and Node_Id_2.[Range = 1 - 4320]

3.2.3 GUI CHANGES

DCA Framework Screen (Main Menu > DCA Framework > Application Control > Version > [Click on "Config"])



Main Menu: DCA Framework -> pcaApp -> Application Control -> Version1 -> Tables

Table Name	Description	Single Row	Level
Cfg_Sets	contains 5 list [can be increased if required] in which foreign peers can be configured.	NO	SO
MCC_MNC_List	This table includes the list of MCC-MNCs of the Operator's Network and its supported Roaming Networks. The combined length of MCC-MNC can be either 5 digits or 6 digits long (depending upon the MNC length).	NO	SO
MsgRateMon_Config	This table defines the Request Message Types [by specifying Application-Id and Command-Code combination] which needs to be monitored along with its threshold value.	NO	SO
Realm_List	This table will define various Home and Foreign network Realms. It also allows to configure Peer List [Foreign_WL_Peer_Cfg_Set] from which these Realms can be expected.	NO	SO
Security_Countermeasure_Config	This table includes the following configuration for each supported CounterMeasures: CounterMeasure's Type, Admin Status, Operating Mode, Result-Code, Error-Message, Vendor-Id, Continue If Vulnerable and Foreign_WL_Peer_Cfg_Set.	NO	SO
SpecAVPScr_Config	This table defines the List of AVPs that needs to be screened for its value in the incoming messages.	NO	SO
System_Config_Options	This table will contains common configurable options required to process various DSR Security Countermeasures.	YES	SO
TTL_Config	This table will contain the Time To Live [TTL] value that will be used while creating/updating U-SBR records for stateful CounterMeasures.	NO	SO
TimeDistChk_Config	This table define minimum transition time [in minutes] between a Source-Id and Destination-Id where Source/Destination-Id will be VPLMN-Id.	NO	SO
TimeDistChk_Continent_Config	This table will contain configuration to define minimum transition time [in minutes] between two Continents.	NO	SO
TimeDistChk_MCC_Config	This table define minimum transition time [in minutes] between a Source-Id and Destination-Id where Source/Destination-Id will be MCC.	NO	SO
VplmnORCst_Config	This table define the List of Application-Id and its Supported Command-Code combinations for which Visited PLMN-ID and Origin-Realm Consistency Check [VplmnORCst] CounterMeasure is applicable.	NO	SO

Figure 7 **– DCA Framework Screen**

3.2.4 BEHAVIOR

Minimum Transit Time between country X and Y is preconfigured as 'd' time units at DSA into Minimum Transit Time Table. This configuration shall be used to perform time distance check.

1. Mobile subscriber is in home network X and performs updated location procedure with home network HSS

2. Mobile subscribers now roams into visited network Y outside home network. Visited network MME/SGSN initiates the AIR/ULR as the part of authentication and update location procedure.
3. DSA receives the AIR/ULR from the visited network MME/SGSN and saves the timestamp Y = a for later timestamp comparison. DEA shall initiate the Send Routing Information Request for LCS on SLh interface towards home network HSS to know the last know serving node (i.e. MME/SGSN) information back in the home network.

HSS responds back with last serving node i.e. MME/SGSN identity of home network. Here DEA acts as an GLMC node for communicating with HSS.

4. DEA sends the S6a/d interface IDR message to last serving MME/SGSN network element of home network to retrieve the last update location timestamp. Home network serving node identity is retrieved in Step 3 from HSS. DEA requests the location information(which also includes the last unknown attach timestamp) from last home network MME/SGSN by setting '**EPS Location Information Request'** IDR Flag bit in IDR request sent to MME/SGSN. Home network MME/SGSN shall include the last unknown update location timestamp using **Age-Of-Location-Information** AVP embedded into **MME-Location-Information/SGSN-Location-Information** AVP of IDA response. DEA shall store the home network last update location timestamp X = b.

3.3 VNFM

3.3.1 DESCRIPTION

The DSR VNFM 3.0 provides support for following operations:

- Instantiate Network OAM VNFs with fixed IPs
- Instantiate Signaling VNFs with Multiple XSIs for fixed IPs
- Instantiating DSR DR NOAM
- Instantiating SDS DR NOAM
- Scale VNF
  -Scale VNF to Level (Scale Out C Level servers of Signaling VNF)
  -Scale VNF to Arbitrary size (Scale Out C Level servers of Signaling VNF)
- Query Individual / All LCM Operation(s) Terminating VNF
- Discover VNF
- Terminate VNF

3.3.2 INSTANTIATE NETWORK OAM VNFS WITH FIXED IPS

VNFM supports both the fixed and dynamic IP support. In order to bring up the new VNFM with the same IP as the existing one, the user can use FIXED IP deployment model.

3.3.3 INSTANTIATE SIGNALING VNFS WITH MULTIPLE XSIS FOR FIXED IPS

Signaling VNF supports both dynamic and fixed IP deployment with multiple XSIs support for both.

3.3.3.1 DSR Signaling VNF with Multiple XSI support (1,2 & 4 xsi interface only)

- Multiple XSI support only DSR Signaling node.
- DAMP vnf will support 1 ,2 & 4 xsi interface.
- STPMP vnf will support 1, 2, & 4 xsi interface.
- IPFE vnf will support 1, 2, & 4 xsi interface.
- UDR vnf will support only 1 & 2 xsi interface.
- While passing the xsiNetwork through request body. Add list of network in the xsiNetwork.

3.3.4 SCALE VNF

It is a N/B LCM scale_to_level Rest I/F which helps in Scaling already created VNF's .

Following are the two options while scaling using "scale to VNF level" N/B Interface.

1. Scale VNF to Level based on pre-defined sizes (using Instantiation level Id) .

2. Scale VNF to Level with arbitrary sizes (using scaleInfo).

Note:

- This feature is only supported for Scaling out C-level servers of Signaling Stack.
- The stack must have been instantiated prior to performing scale to level operation.
- Before Scaling the VNF to level, VnfInstance Id of the stack must be available.
- The instantiation level for Signaling stack is available under Instantiating the first signaling VNF section.
- Currently, we do not support the cloud-init (appworks configurations) for the scaled out VMs. It will supported shortly.
- Scale To Level Request accepts either instantiationLevelId or scaleInfo
- Cross deployment scaling is not supported by VNFM - if the user instantiated the VNF in fixed IP deployment model, then he must scale to level using FIXED IP deployment model only and vice versa.

The following image illustrates the VNF Scaling:

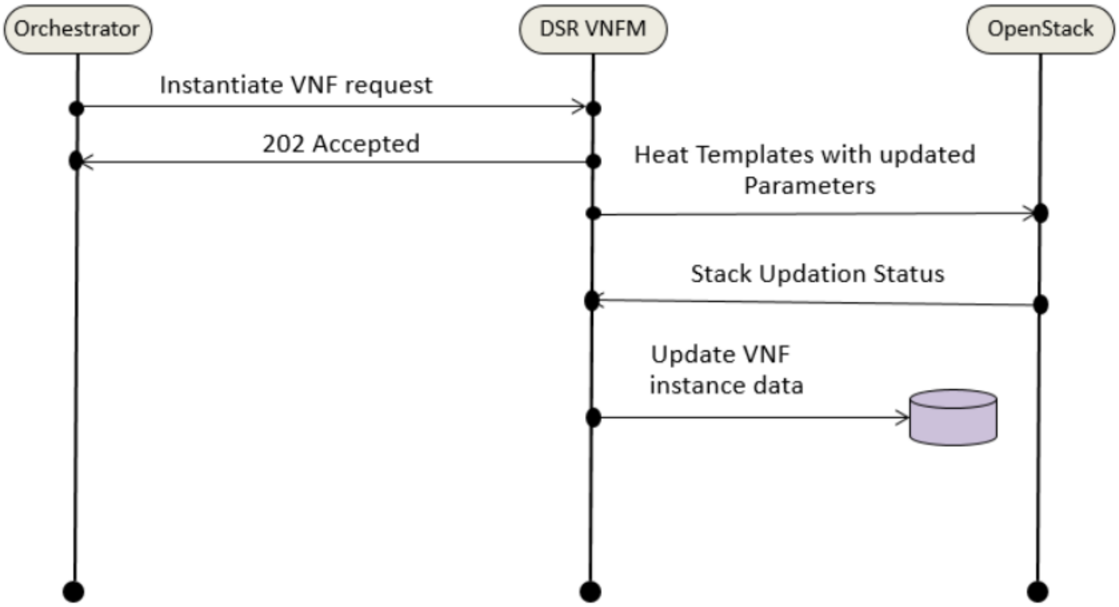


Figure 8 **– VNF Scaling**

3.3.5 QUERY INDIVIDUAL / ALL LCM OPERATION(S) TERMINATING VNF

This resource represents VNF lifecycle management operation occurrences. This resource can be used to query status information about multiple VNF lifecycle management operation occurrences.

The diagram describes a sequence for querying/reading information about a VNF LCM Operation.

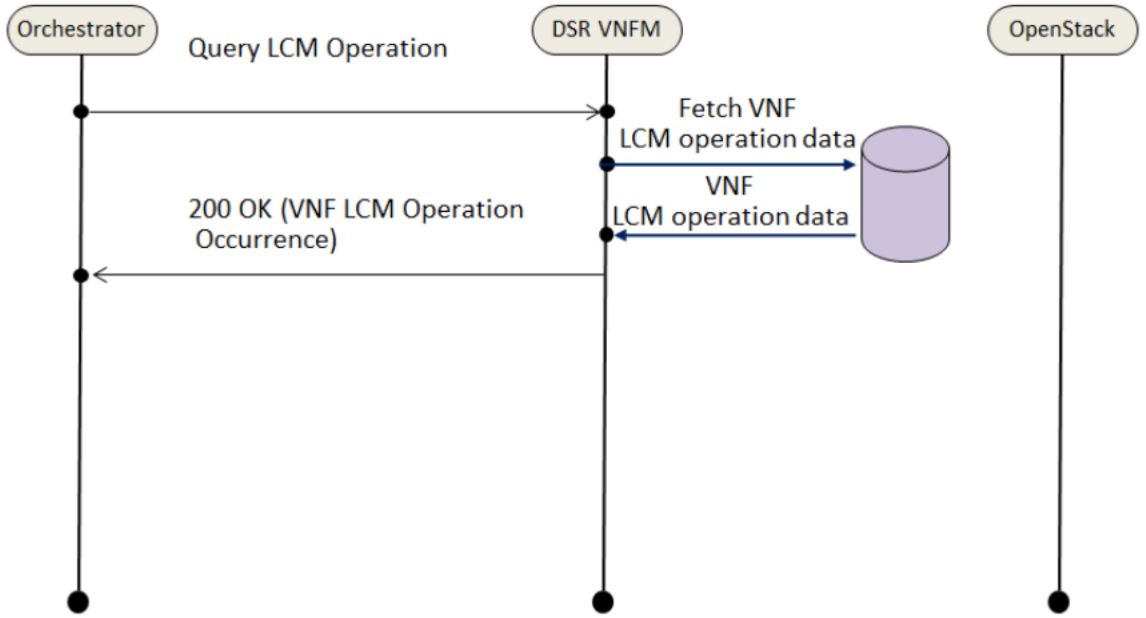


Figure 9 **– VNF LCM Operation**

Below are the two ways to query LCM Operation

1) Query individual LCM Operation

2) Query All LCM Operation

3.3.6 DISCOVER VNF

1. It is an LCM Discover Rest I/F.

2. It is used to discover the created stack in OpenStack and save the stack information (parameter file and VNF instance) in the VNFM persistent directory. This information can be used for further requests by the orchestrator. For example, to scale out the stack. This information can be used to further request by the orchestrator . e.x :- To scale out the stack.

3. Before Discovering the Stack, the following information must be available:

- The **Stack ID** for a previously created stack.
- Information about the OpenStack instance on which the Stack must be discovered:
  - OpenStack Controller URI
  - Domain name
  - Username
  - Password
  - Tenant name

4. The Interface discovers the stack and performs below operations:

1. Download the Parameter file of discover stack
2. Create the Instance file of discover stack.
3. These two files will be save in "/var/vnfm/instances/<autoDiscovery InstanceId>/" directory

3.3.7 TERMINATING VNF

This resource represents the "Terminate VNF" operation. The client can use this resource to terminate a VNF instance. The POST method terminates a VNF instance.

Two types of TerminateVnfRequest that represents request parameters for the "Terminate VNF" operation:

1. FORCEFUL: The VNFM will delete the VNF and release the resources immediately after accepting the request.
2. GRACEFUL: After accepting the request, VNFM will first validate if the VNF configuration is cleaned up . Once the validation is successful, VNFM will delete the VNF and release the resources.

3.3.7.1 Forceful Termination

The VNFM will delete the VNF immediately after accepting the request. The instance file is updated with VNF Operational State set to "STOPPED",

Note: If the VNF is still in service, requesting forceful termination can adversely impact the network service.

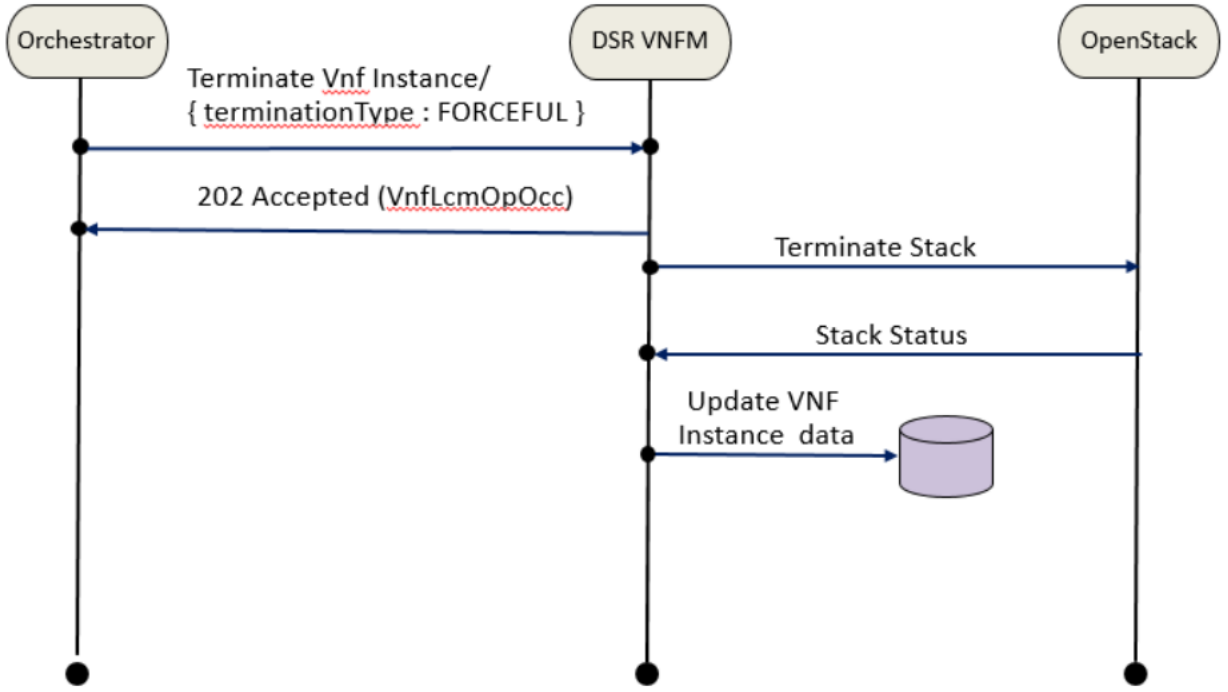


Figure 10 **– VNF Forceful Termination**

3.3.7.2 Graceful Termination

The VNFM will first validate if the VNF configuration is cleaned up after accepting the request. If the configuration is cleaned up , the VNFM will delete the VNF. Then the instance file is updated with VNF Operational State set to "STOPPED".

If appworks configurations not cleaned up manually and orchestrator tries to do gracefull termination for that VNF, then termination of VNF will fail.

Note: User must manually clean up the AppWorks configurations before doing Graceful Termination.

Steps for cleaning up the AppWorks Configuration for Signaling Stack of DSR and SDS:

1. Open corresponding Active NOAM GUI of the Signaling instance.
2. In Status & Manage Tab, under HA - edit the **Max Allowed HA Role** of instances of the Signaling stack as **OOS**.
3. In Configuration Tab, under Server Groups, edit the corresponding server groups of the instances and uncheck **SG Inclusion** for the Server, and press OK. After this step, the excluded Servers must disappear in Status & Manage -> Server section.
4. Finally, go to Configuration -> Servers section, select the servers that are to be deleted and press the delete button.
   Note: 'GRACEFUL' termination is not supported for DR NOAM and SDS DR NOAM. Although, tried to perform then this scenario will be treated as 'FORCEFUL' termination and the stack will be deleted.

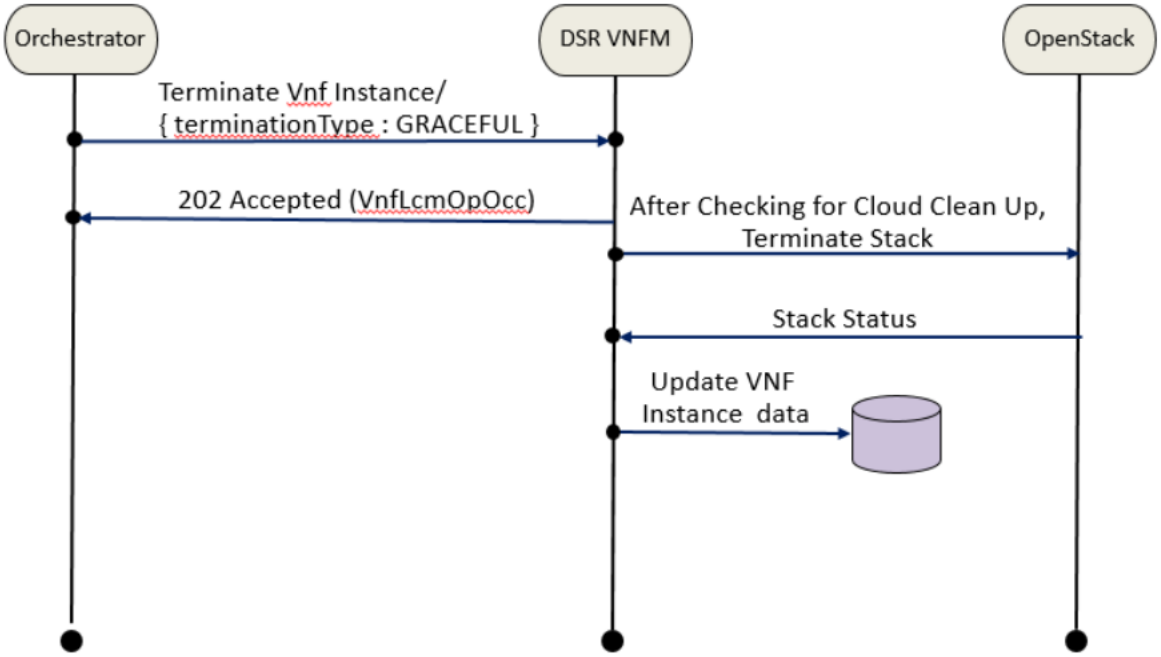


Figure 11 **– VNF Graceful Termination**

3.4 SCEF

LWM2M Gateway:

LwM2M server is intended to handle IP device connectivity of IoT network via LwM2M protocol over CoAP. The server provides a unified interface T8 towards SCS A/S to handle communication with LwM2M devices.Lwm2M server is developed using communication service framework in OCSG.

LWM2M Device registration process
When LwM2M device is registered, LwM2MServer will send a notification to configured SCS/AS Url.
SCS/AS Url can be configured to receive registration notification for a specified device id or based on domain.
If no SCS/AS Url is configured for the device registration messages received then the device will be registered with LWM2MServer and will not be notified to SCS/AS.

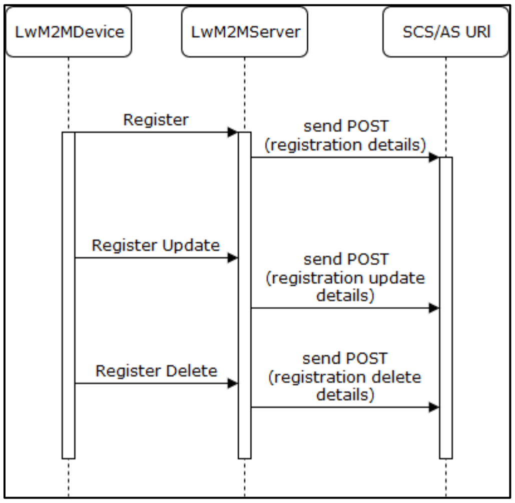

LwM2MDevice
LwM2MServer
SCS/AS URl
Register
send POST (registration details)
Register Update
send POST (registration update details)
Register Delete
send POST (registration delete details)

Figure 12 – **LWM2M Registration Process**

LwM2M device registration process

Monitoring Event
Create event subscription to monitor a LwM2M device resource (using T8 Monitoring Event API)
SCS/AS can send monitoring event subscription message to API Gateway to monitor a device resource.
If the device is not registered for which the subscription request is received, HTTP 404 Device not found error will be returned.
If the device is registered in LwM2M server, then LwM2M observe message will be created sent to Device. A unique subscription identifier will be generated by server and returned in response.
The subscription will be active in LwM2M server until SCS/AS delete the request.

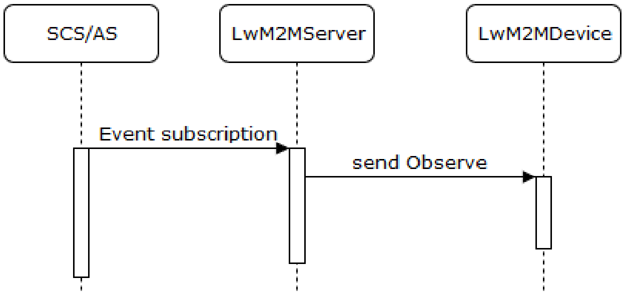


Figure 13 – **Subscription and Observe**

LwM2M event subscription process

Subscription event notification:
When device send notification to the observe request, the stored subscription request will be fetched and notification request will be generated and sent to the callback Url sent in subscription request.

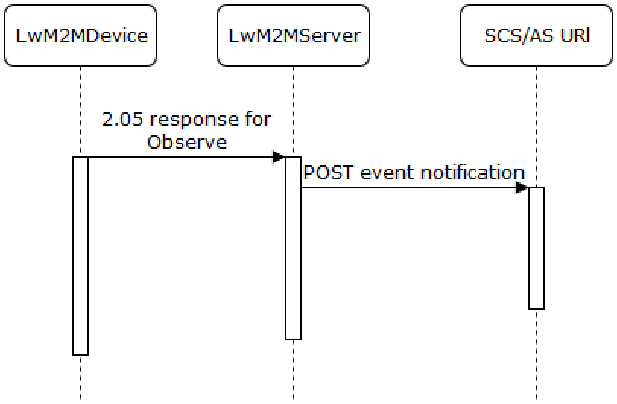


Figure 14 **– Event Notification**

LwM2M event subscription notification process

Delete subscription request (using T8 Monitoring event API)
SCS/AS can send HTTP Delete message to stop monitoring of the device resource.
If the subscription id sent is wrong then HTTP 404 error code should be returned.
If the subscription id sent is correct then LwM2M cancel request should be sent to Device to stop the observation.

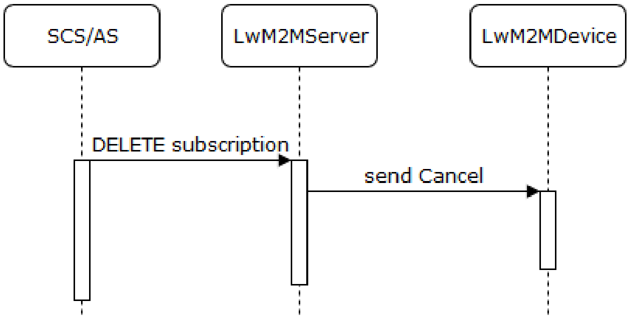


Figure 15 **– Subscription and cancel**

LwM2M event subscription delete process

NIDD Downlink Data Transfer
Sending data to device (MT Data using T8 Nidd API)
SCS/AS can send data to LwM2M device using Nidd Downlink Data transfer request.
When the Downlink data transfer request is sent LwM2M server will send corresponding LwM2M message to the device.
If the device is not registered with the server then HTTP 404 message should be returned.

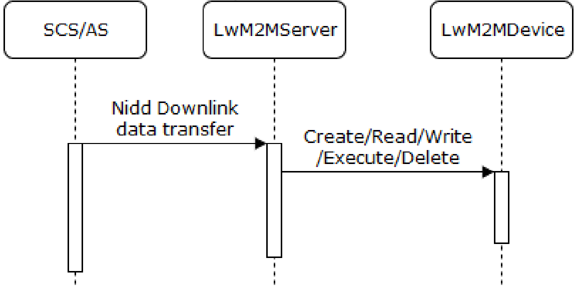

SCS/AS
LwM2MServer
LwM2MDevice
Nidd Downlink data transfer
Create/Read/Write /Execute/Delete

Figure 16 **– Action on DL data transfer**

LwM2M MT Data delivery process

MQTT Broker:

High-level functional requirements of SCEF MQTT Broker includes MQTT IP Device Monitoring event procedure that includes Unified T8 interface for IP devices.
MQTT Broker is intended to handle IP device connectivity of IoT network via MQTT protocol. The broker provides a unified interface T8 towards SCS A/S to handle communication with MQTT devices.
MQTT Broker is developed using communication service framework in OCSG.

Create event subscription to monitor a MQTT device (using T8 Monitoring Event API)
If the device is not connected for which the subscription request is received, HTTP 404 Device not found error would be returned.

If the device is connected to MQTT Broker, then a unique subscription identifier will be generated by broker and returned in response.

The subscription will be active in MQTT Broker until delete request is sent.

Subscription event notification:

When SCS/AS publish the data, the stored subscription request will be fetched and notification request will be generated and sent to the callback Url sent in subscription request.

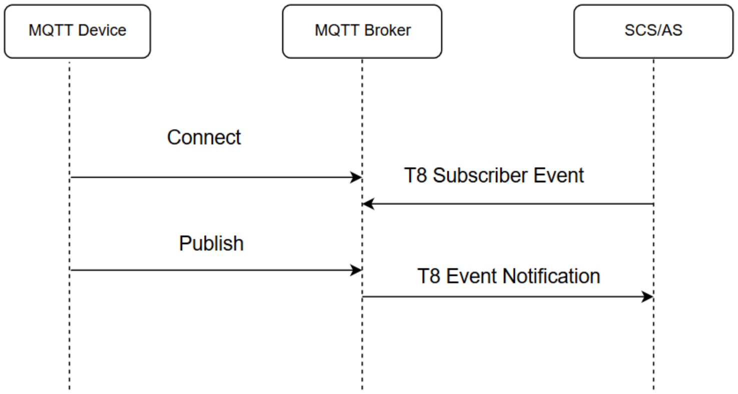


Figure 17 **– T8 Event**

MQTT Monitoring data call flow

Delete subscription request (using T8 Monitoring event API):

MQTT Device can send HTTP Delete message to MQTT Broker to delete subscription of the device.

If the subscription id sent is wrong then HTTP 404 error code should be returned.

If the subscription id sent is correct then subscription of the MQTT device will be deleted and response ok is returned.

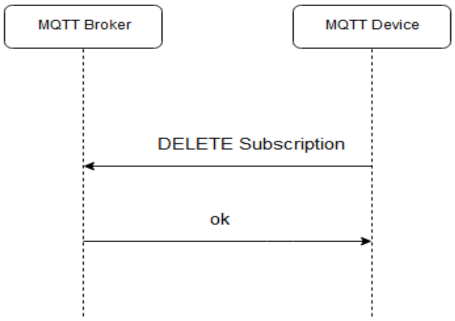


Figure 18 **– DELETE Subscription**

MQTT Event subscription delete process

<u>QoS Control</u>

The QoS Control feature in SCEF allows SCS/AS to setup an AS session with required QoS and priority handling. In order to achieve this SCEF will act as AF to PCRF and setup the session over Rx interface.

AS Session Setup

Below diagram illustrates the procedure of AS session setup initiated by SCS/AS to a given user as identified using the IPv4 or IPv6 address.

SCS/AS sends AS Session setup request with required QoS subscription to SCEF over T8 interface. SCEF processes the request and sends a Rx AAR message towards PCRF to create AS session with requested QoS and priority signaling.

When PCRF sends a success response in Rx-AAA. Then a session record is created in the database and a resource location (URI) is sent to SCS/AS in the response.

The SCS/AS shall use the URI received in the Location header in subsequent requests to the SCEF to refer to this AS session. Otherwise, the SCEF shall send an HTTP response to the SCS/AS with a corresponding status code and include the result in the body of the HTTP response.

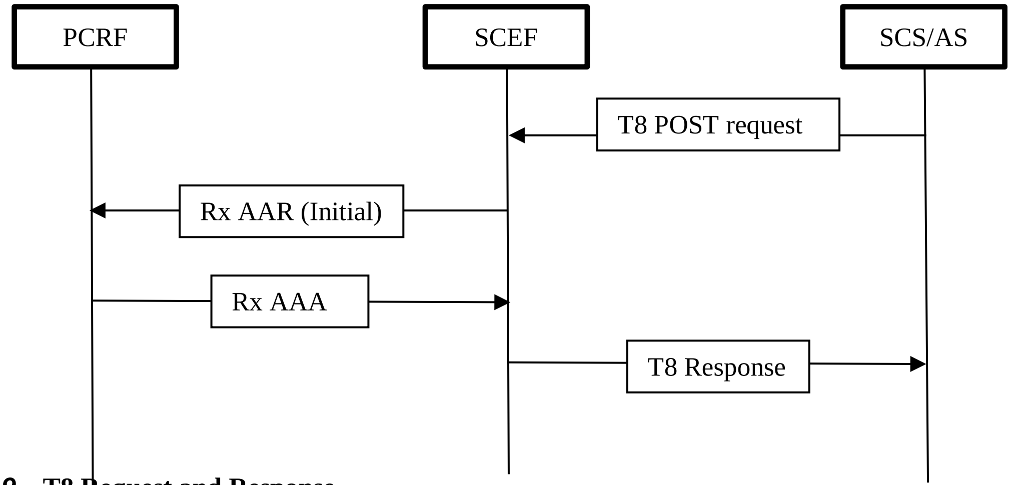


Figure 19 **– T8 Request and Response**

AS Session Setup

3.4.1 AS SESSION MODIFY

The below figure illustrates AS Session modify procedure to replace existing QoS properties. In order to update the established AS session, the SCS/AS sends an HTTP PUT message to the resource "Individual AS Session with Required QoS Subscription" requesting to replace all properties in the existing resource, addressed by the URI received in the response to the request that has created the resource. The UE IP address has to remain unchanged from previously provided values. After receiving such message, SCEF will make the change and interact with the PCRF to modify the Rx session by triggering an Rx-AAR.

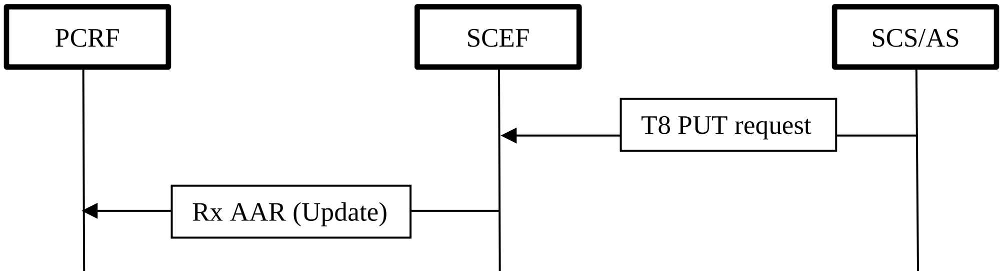


Figure 20 **– PUT Operation**

AS Session modify

3.4.2 AS SESSION REMOVE

Figure illustrates AS Session remove initiated by SCS/AS. To remove the AS session SCS/AS sends an HTTP DELETE message to the resource "Individual AS Session with Required QoS Subscription". After receiving the HTTP DELETE message, the SCEF interacts with the PCRF to terminate the Rx session by sending an Rx-STR.

After success response from PCRF, the AS session data stored in database is cleared. After this a success response is sent back to SCS/AS stating that the AS session is removed successfully.

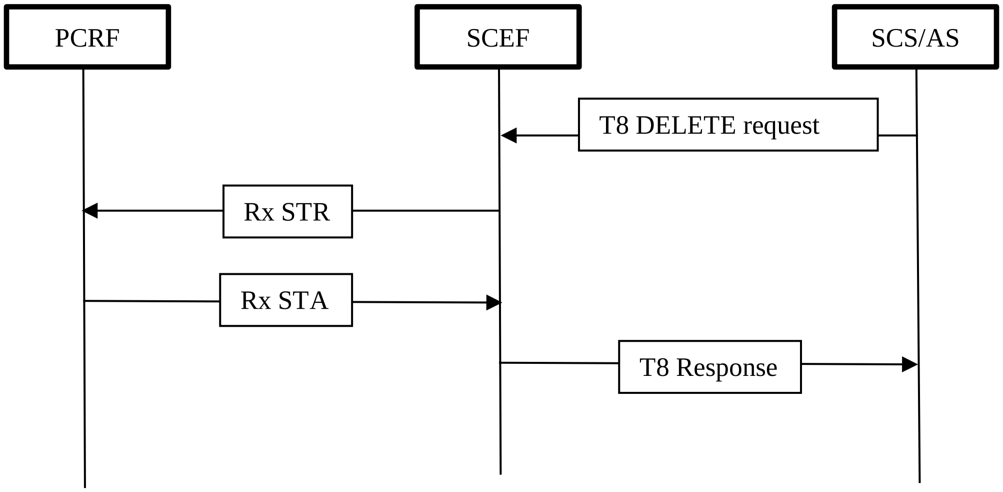


Figure 21 **– DELETE Operation**

3.4.3 AS SESSION QOS NOTIFICATION

When SCEF receives Rx ASR from PCRF, it gets informed that the Rx session is terminated (e.g. due to a release of PDN connection). SCEF sends STR towards PCRF and then it will send an HTTP POST message including the notified event (session terminated) and the accumulated usage (if received from the PCRF) to the callback URI "notificationUri" provided by the SCS/AS during the creation of individual AS Session with Required QoS Subscription. The SCS/AS shall respond with an HTTP response to confirm the received notification.

The event notification generated when PCRF terminates the Rx session. In this case PCRF sends Rx-ASR to SCEF, it verifies if the session exists in the database. Once the session data is fetched from the database a notification is sent to SCS/AS with details of the event. After a response is received from SCS/AS the session data in the database will be cleared.

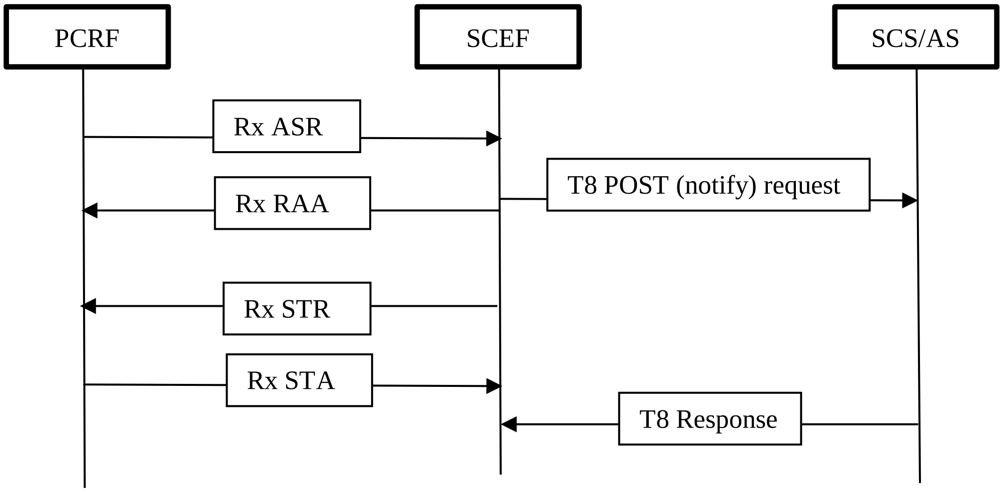


Figure 22 **– T8 POST Operation**

AS Session termination event notification

3.4.4 API BASED CHARGING

SCEF shall support API based charging for the following procedures that operate across the T8 reference point. In addition, charging shall be implemented based on Offline event based charging mechanism. Moreover, the event are.

- NIDD Events
- Monitoring Events
- Device Triggering Events
- Enhanced coverage Restriction Events.

The SCEF shall support Offline charging for API based charging. On the other hand, in offline charging, an user is charged for the network resources that is already used. That is, the network reports the resource usage by the particular user by forwarding the CDR (Charging Data Record) to its billing domain.

SCEF shall support Event based charging function (EBCF). EBCF is based on their occurrence rather than their duration or volume used in the event. Typical SCEF events are Nidd/Monitor/Device Trigger/ECR.

SCEF shall create an exposure function API CDR in real time (up to 1 second) for each event when the API invocation or notification encountered.

Invocation:

SCS/AS shall send T8 request (Nidd/Monitor/Device Trigger/ECR) to OCSG, which is part of SCEF.

OCSG forwards the incoming T8 request to serving SCEF-MP.

SCEF-MP will act on the message and send back response message to OCSG.

Now OCSG will generate a CDR with available data and write into a file in binary format. Then forward that response to SCS/AS.

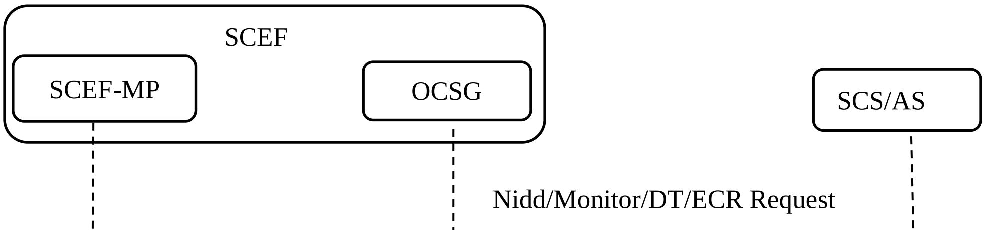


Figure 23 – API based charging for Invocation events

Notification:

SCEF-MP may receive notification message from MME/HSS if SCEF subscribed for certain events.

SCEF-MP shall send that notification request (Nidd/Monitor/Device Trigger) to OCSG.

Now OCSG will generate a CDR with available data and write into a file in binary format. Then forwards the request to SCS/AS.

Moreover, the subsequent SCS/AS response will be forward to SCES-MP via OCSG.

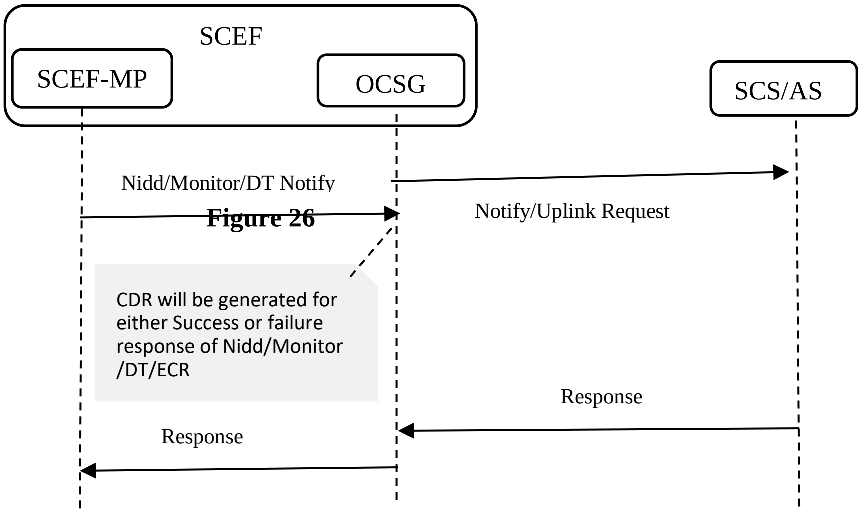


Figure 24 **– Notify and Uplink Request**

SCEF T8 Compliance Changes

Changes were made to the existing APIs (NIDD (Non-IP Data Delivery), Device Triggering, Monitoring Events, Enhanced Coverage Restriction (ECR) Control) to comply with specifications **3GPP TS 29.122 T8 Reference Point for Northbound APIs**

3.5 VSTP SPARE POINT CODE SUPPORT

3.5.1 *PURPOSE AND SOLUTION*

Purpose

1. At present vSTP supports only 4 domain PCs of ANSI/ITU-I/ITU-N/ITU-N24.
2. This limits operators from hosting more no. of point codes for ITUI and ITUN domain which triggers the need for more no of nodes in the network and associated provisioning & maintenance.

Solution

Spare PC solution resolves the above limitations by enabling vSTP to new domain PC ITUN Spare and ITUI Spare in addition to the point codes used by the vSTP domains ITU-N (14-bit or 24-bit) and ITU-I.

Feature Overview

- The vSTP to fully support ITU National Spare and ITU International Spare by providing a new PC sub type named Spare.
- ITUN_S and ITUI_S indicates a Spare point code. Spare point codes only apply to ITU-I and ITU-N point code types.
- The subservice field contains the network indicator and two spare bits. The network indicator is used by signaling message handling functions.

Table 47 - NI and Name

NI	NAME
00(03)	International
01(43)	International-Spare
10(83)	National
11(c3)	National-Spare

- The vSTP currently provides full support for four types of point codes (PC) – ANSI, ITU-National (NI=10binary), ITU-National 24-bit, and ITU-International (NI=00 binary). ITU National Spare PCs (NI=11 binary) and ITU International Spare(NI= 01 binary) PCs can be primarily supported :
- If the Spare PC feature is enabled then vSTP will validate the NI value of incoming message on designated linkset . If NI value matches then link will be mark available otherwise message will be discarded.
- For example, any incoming message with DPC = 1-1-1 (NI=11binary) on link set equal to configured ITUN spare DPC = 1-1-1 (NI=11binary) shall be accepted.
- If the Spare PC feature is disabled then vSTP will allow to accept the In coming messages with NI value ITUI spare on configured ITUI linkset.
- Incoming messages with the Spare bit set will be treated as Non-Spare point codes.
- For example, vSTP will accept a message with DPC = 1-1-1 (NI=11_{binary}) the same way as a message with DPC = 1-1-1 (NI=10_{binary}).

MTP Message Routing

- **Message destined for DPC When Spare PC feature turned on and No MTP conversion.**

- The NI Value of an outgoing MTP-routed MSU must match the domain type of the APC/SAPC on the corresponding link set over which the MSU is received otherwise error is thrown “MTP3 Routing Error - Invalid NI”.
- During MTP routing with no MTP conversion, the MSU is simply routed without modification, so the outgoing NI will be the same as the incoming NI.
- All route selection and MSU processing shall be done using a combination of the DPC and the Network Indicator fields in incoming messages.

Table 48 - Configuration details1

Spare Feature	**Spare Bit on**	**Configured Domain/NI for APC**	**Domain /Received NI in MSU**	**Message Routing**
Yes	Yes	ITUN_S(11)	ITUN_S(11)	MSU routed
Yes	Yes	ITUN(10)	ITUN_S(11)	MSU Discarded
Yes	Yes	ITUI_S(01)	ITUI_S(01)	MSU routed
Yes	Yes	ITUI(00)	ITUI_S(01)	MSU Discarded

- If a message is MTP-routed with conversion, the outgoing NI value will be set to the provisioned value of the outgoing DPC. The incoming NI will only be used to define the incoming DPC as Spare or Non-Spare, in order to determine the correct conversion.

Table 49 - Configuration details2

Spare Feature	**Spare Bit on**	**Configured Domain/NI for APC**	**Domain /Received NI in MSU**	**Message Routing**
Off	Yes	ITUN_S(11)	ITUN_S(11)	MSU Discarded
Off	Yes	ITUN(10)	ITUN_S(11)	MSU routed
Off	Yes	ITUI_S(01)	ITUI_S(01)	MSU Discarded
Off	Yes	ITUI(00)	ITUI_S(01)	MSU routed

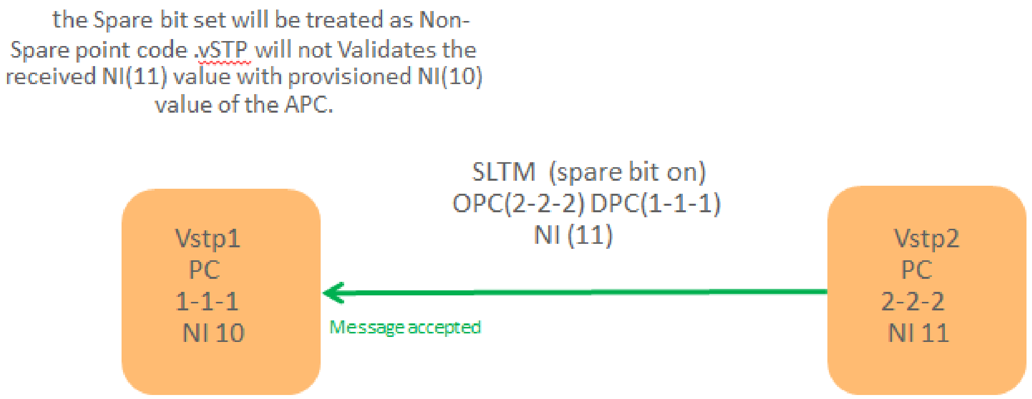
SCCP Message GTT Routing:

- During SCCP Translation via GTT, the outgoing NI will match the GTT-database value for the DPC associated with the CdPA digits to be translated.
- The incoming NI does not affect the digits used for SCCP translation, and thus does not affect the outgoing NI.
    - **NOTE**: Based on GTT configuration, the Network Conversion feature may convert spare point code into other supported domain.

Signaling Link Test Messages (SLTM/SLTA)

- SLTM/SLTA messages will be performed with the linkset APC, and the NI will match the provisioned value of the APC.
- vSTP shall validate that the DPC of the message matches with the DPC provisioned against the OPC of the message.
- When Spare PC feature is on, The NI Value of an received message must match the domain type of the APC on the corresponding link set over which the MSU is transmitted.
- When Spare feature is off, Incoming messages with the Spare bit set will be treated as Non-Spare point codes.
- For example , vSTP will route a message with DPC = 1-1-1 (NI=11binary) the same way as a message with DPC = 1-1-1 (NI=10binary).

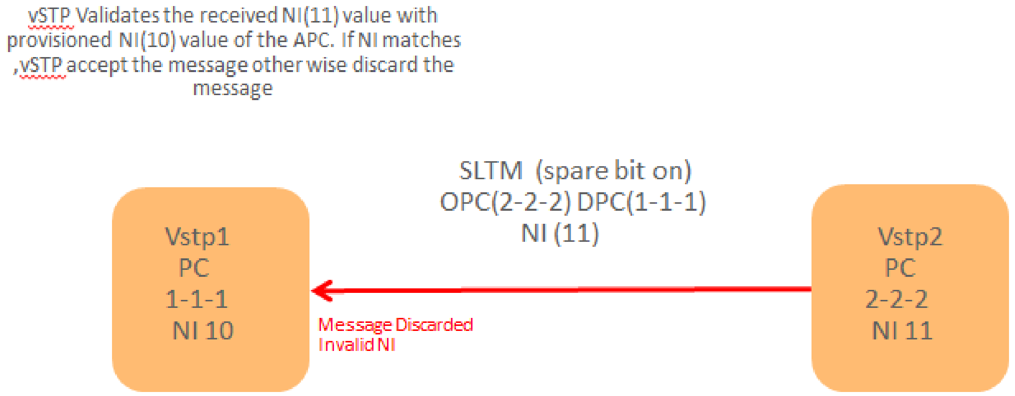
Signaling Link Test Messages (SLTM/SLTA) Spare PC Off



the Spare bit set will be treated as Non-Spare point code .vSTP will not Validates the received NI(11) value with provisioned NI(10) value of the APC.

Figure 25 – SLTM Operation accept

Signaling Link Test Messages (SLTM/SLTA) Spare PC On



vSTP Validates the received NI(11) value with provisioned NI(10) value of the APC. If NI matches ,vSTP accept the message other wise discard the message

Figure 26 – SLTM Operation discard

MO’s and operations supported:

- Following is the list of MO’s and operation supported for Spare PC feature :
- ss7DomainType supports ITUN_S and ITUI_S domain.

***Table 50 – MO Details** 1*

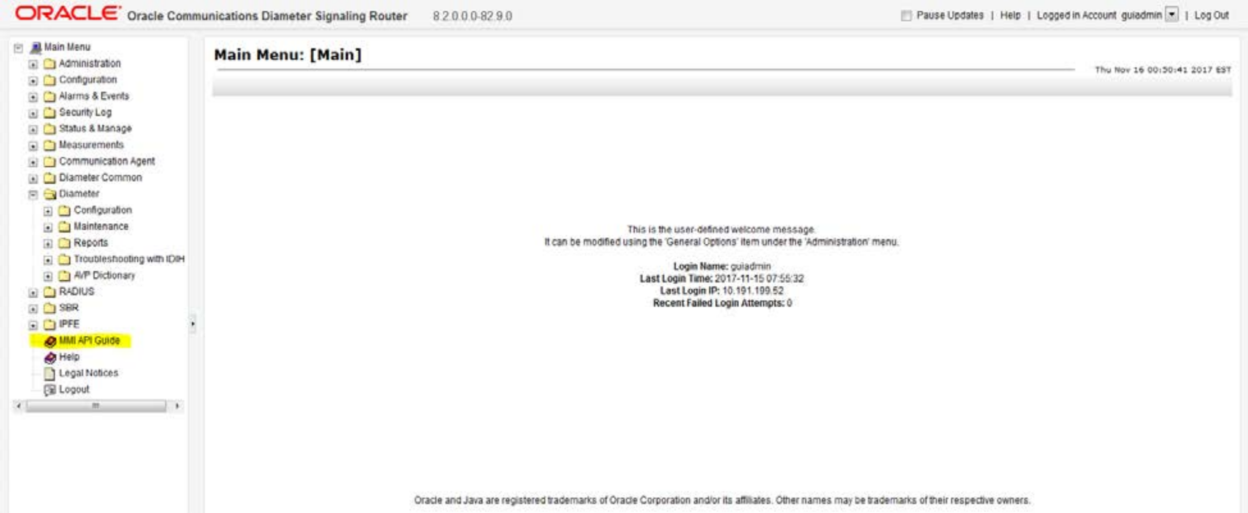
MO Name	Operations supported	URI
VstpLocalSP	Insert, Update, Delete	/vstp/localsignalingpoints
VstpRemoteSP	Insert, Update, Delete	/vstp/remotesignalingpoints
VstpSccpGTTSel	Insert, Update, Delete	/vstp/gttselectors

- SparePCSupportEnabled flag should be Enable to support ITUN_S and ITUI_S domain.

Table 51 – MO Details 2

MO Name	Operations supported	URI
m3rloptions	update	/vstp/m3rloptions

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



Main Menu: [Main]

Thu Nov 16 00:30:41 2017 EST

This is the user-defined welcome message.
It can be modified using the 'General Options' item under the 'Administration' menu.

Login Name: guiadmin
Last Login Time: 2017-11-15 07:55:32
Last Login IP: 10.191.199.52
Recent Failed Login Attempts: 0

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

Figure 27 – MMI API Guide reference

3.6 VSTP MNP GPORT

3.6.1 *PURPOSE AND SOLUTION*

- **Purpose**
- Support for GSM Mobile Number Portability (a.k.a. G-Port) feature in vSTP.
- Mobile Number Portability (MNP) allows mobile subscribers to retaining their original MSISDN when changing the network to which they subscribe.
- This feature is an optional feature and can be turned on/off via configurable option in the VstpMnpOptions.
- **Solution**
- G-Port shall perform the following actions based on the message received and number status:
    - If the number is ported-out or not known to be ported and the message received is call-related SRI (not-SOR), G-Port shall send the SRI Ack message to the MSC with the Routing Number information in the MAP portion of the message.
    - If the number is ported-out and the message received is non-call related (non-SRI), G-Port shall perform message relay and forward the translated message based on the Routing Number information.
    - If the number is non-ported or ported-in then G-Port shall perform HLR translation and forward the translated message to the HLR.
- An additional user option will allow the user to configure the G-Port to modify the above processing in the following way:
    - If the number is not found in the UDR NPDB (individual or range) then the G-Port shall return a negative acknowledgement in response to an SRI.

G-PORT INVOLVES FOLLOWING MAIN FUNCTIONS:

Message discrimination: Since G-Port is currently only used for translation of ported numbers, it provides a method to identify which messages should receive G-Port vs. GTT. This is provided via a service selector table where one can define G-Port service for a combination of selectors. If a selector match is not found then G-Port shall fall-through to GTT.

Number conditioning: Since the UDR NPDB stores International MSISDNs only, G-Port provides the capability to condition incoming numbers to be international MSISDNs (i.e. Delete Routing Number Prefix or Insert CC or/and NDC) for the database look up. Also, messages with ported-in number in SCCP CdPA or MAP MSISDN might have RN prefix. G-Port shall strip off the RN prefix and then condition the non-international numbers to international numbers, if needed, before performing any database lookup.

SRI Response : When the incoming SRI message does not already contain a RN in the SCCP portion, or if the VstpMnpOption:MNPCRP is off, G-Port shall generate a SRI Ack message for a SRI message when the number is foreign number, and a RN is associated with the DN in the database. When neither a RN nor a SP is associated with a MSISDN in the database, G-Port shall formulate a SRI Ack message ONLY for “null” PT or “foreign number” PT. For all other cases the SRI shall fall through to GTT. When formulating a SRI Ack message, G-Port shall use the RN prefix associated with the MSISDN entry to build the MSRN number or based on the VstpMnpOption:MSRNDIG to not prefix shall return the RN only. G-Port shall generate negative SRI Ack message upon encountering any MAP SRI problems. If VstpMnpOption:MNPCRP is on and the SRI message already contains a RN in the SCCP portion or MAP MSISDN, then G-Port will issue Event # 70304 and the message will fall through to GTT. Since the CdPA / MAP MSISDN contains RN+DN, this should result in a GTT failure, which will cause a UDTS to be returned to the originator if the Return Message on Error flag was set in the incoming UDT. If MSISDN is provisioned in UDR NPDB with PT values of 0/1/2 (foreign number), the SRI response will have NPS value of 0/1/2. When PT value of “null” is defined, it will be mapped to NPS value of (0) in the SRI response.

G-Port Message Relay: G-Port shall perform message relay on non-SRI or SRI-SOR (SRI messages with OR Interrogation Indicator present) messages when the MSISDN number is ported. Message relay shall provide an ability to prefix the Routing number to the CdPA digits or replace the CdPA digits by RN prefix based on the Digit Actions. If VstpMnpOptions:SRISMGTTRTG is ON, then the SRI_SM and ReportSMDeliveryStatus messages shall not be relayed. Instead the CdPA GTA in the message shall be modified in CC+RN+DN format (or RN+IDN format if CC match is not found in leading digits). The NAI of CdPA GTA shall be set to International and the message shall Fall-Through to GTT.

Message relay on ported-in numbers : G-Port shall automatically perform SCCP relay on SRI and non-SRI messages for Own Numbers (i.e. a SP is associated with the DN in the database). However, the non-ported (PT=4) or ported-in (PT=5) entries should be present in the UDR NPDB and SP entity should have been defined for this entry. This applies even in the case when VstpMnpOptions:MNPCRP is on and the message contained an RN in the incoming SCCP. If GRN is also associated (along with SP entity) with the DN and the GRN is not present in the HomeRN table and VstpMnpOptions:SRISMGTTRTG is ON, then the SRI_SM and ReportSMDeliveryStatus messages shall not be relayed. Instead the CdPA GTA in the message shall be modified in CC+GRN+DN format (or GRN+IDN format if CC match is not found in leading digits). The NAI of CdPA GTA shall be set to International and the message shall Fall-Through to GTT.

- **G-Port Message Handling:**

    1. The message arrives at vSTP route-on-gt. vSTP decodes the SCCP portion and uses the data to perform G-Port Selection based on the CdPA GT fields other than the ES and GTAI. The result of this selection provides service indicator. The service indicator will be G-Port if MNP-SRF is required. If a service selector does not match the incoming GT fields, then GTT selection is attempted.

    2. If step 1 indicates MNP-SRF is required and the message is not a UDTS generated by vSTP, vSTP then performs SSN-based discrimination. If the message is a UDTS generated by the vSTP then regular GTT is performed on the message.

    3. MNP-SRF will first decode the Operation Code of the MAP message to distinguish SRI/SRI_SM message with the rest. If the Operation Code is SRI and the OR Interrogation indicator is absent, and the VstpMnpOptions:SRIDN = "TCAP", then the MSISDN parameter is decoded from the MAP portion of the message. If the Operation Code is SRI_SM, and the VstpMnpOptions parameter SRISMDN = "TCAP", then the MSISDN parameter is decoded from the MAP portion of the message. If the VstpMnpOptions parameter SRIDN (for SRI message) / SRISMDN (for SRI_SM message) = "SCCP", or if the message is not SRI or not SRI_SM, then digits available in the SCCP CdPA GTAI are used for database lookup.

    4. The decoded DN (either from MAP MSISDN or from SCCP CdPA) is then conditioned to an international number before performing the UDR NPDB lookup. The conditioning is different based on whether the digits are obtained from TCAP or MAP part of the message.

        - If the digits are from the SCCP part then number conditioning is based on SNAI value. RN prefix deletion is performed first and then conversion to International based on its value. Conversion to international format is based on DefCC and DefNDC, as required. If the incoming number is CCRNDN, DefCC and MultCC will be used to determine the Best Match CC to locate the RN digits for RN prefix deletion.

        - If the digits are from the MAP part then number conditioning is based on NAI of MSISDN Parameter. Home RN Prefix deletion is performed if VstpMnpOptions:MNPCRP is on. The number is converted to International if needed. Conversion to international format is based on DefCC and DefNDC, as required. If the incoming number is international, DefCC and MultCC will be used to determine if the format is CCRNDN or RNIDN. If a Best Match CC is located, then it will be used to locate the RN digits for RN prefix deletion.

    5. The UDR NPDB database lookup involves 2 steps:

        - First the exception or individual number database is searched for a match. If the match is found then the data associated with this entry is considered.

        - If the conditioned number is absent in the exception (individual) database, then the number range database is searched. If the match is found then the data associated with this range entry is considered. If the search is unsuccessful then the result is no match.

    6. If the number is found, and a RN prefix is present for this entry, then:

- If the message is SRI, and VstpMnpOptions:MNPCRP is off, or if VstpMnpOptions:MNPCRP is on and a HomeRN was not present in the incoming DN (i.e. a HomeRN was not deleted from the SCCP CdPA/MAP MSISDN), then G-Port shall generate a SRI Ack message with the RN prefix in the Routing Number parameter.
- If the message is non-SRI, and VstpMnpOptions:MNPCRP is off, or if VstpMnpOptions:MNPCRP is on and a HomeRN was not present in the incoming DN (i.e. a HomeRN was not deleted from the SCCP CdPA), then G-Port shall use the translation data for the number to alter the CdPA digits and route the message to the destination.
- If the message is SRI or non-SRI, and VstpMnpOptions:MNPCRP is on, and a HomeRN was present in the incoming DN (i.e. a HomeRN was deleted from the SCCP CdPA/MAP MSISDN), then G-Port shall generate Event #70304, and the message shall fall through to GTT. In most network implementations, since the message contains RN+DN, this should cause a GTT failure, which will result in the vSTP sending a UDTS to the originator if the Return Message on Error flag was set in the incoming UDT.
- If VstpMnpOptions:SRISMGTTRTG is ON, then the SRI_SM and ReportSMDeliveryStatus messages shall not be relayed. Instead the CdPA GTA in the message shall be modified in CC+RN+DN format (or RN+IDN format if CC match is not found in leading digits). The NAI of CdPA GTA shall be set to International and the message shall Fall-Through to GTT.

7. If the number is found and a SP entity is present for this entry, then G-Port shall use the SP translation data for the number to route the message to the destination. This is true whether or not VstpMnpOptions:MNPCRP option is on. However, if GRN is also associated (along with SP entity) with the DN and the GRN is not present in the HomeRN table and VstpMnpOptions:SRISMGTTRTG is ON, then the SRI_SM and ReportSMDeliveryStatus messages shall not be relayed. Instead the CdPA GTA in the message shall be modified in CC+GRN+DN format (or GRN+IDN format if CC match is not found in leading digits). The NAI of CdPA GTA shall be set to International and the message shall Fall-Through to GTT.
8. If the number is found and neither SP nor RN data is associated with it (this is a direct routing case with number not known to be ported or not identified to be ported), then

   - If the message is is SRI, and VstpMnpOptions:MNPCRP is off, or if VstpMnpOptions:MNPCRP is on and no HomeRN was present in the incoming DN (i.e. a HomeRN was not deleted from the SCCP CdPA/MAP MSISDN), and if the portability type associated with the DN entry is other than 3-35 , then G-Port shall generate a SRI Ack message with the MSISDN in the Routing Number parameter. If the message is SRI, and VstpMnpOptions:MNPCRP is off, or if VstpMnpOptions:MNPCRP is on and no HomeRN was present in the incoming DN (i.e. a HomeRN was not deleted from the SCCP CdPA/MAP MSISDN), and the portability type associated with the DN entry is 3-35, then the SRI shall fall through to GTT (i.e. no SRI Ack message is generated).
   - If NPS parameter will be encoded in the SRI Ack message if :

     VstpMnpOptions : ENCODENPS=ON and DN is associated with PT =0, 1, 2 (foreign number)

     VstpMnpOptions : ENCDNPSPTNONE=ON and DN is associated with PT = null (deemed foreign number)
   - If the message is non-SRI, and VstpMnpOptions:MNPCRP is off, or if VstpMnpOptions:MNPCRP is on and no HomeRN was present in the incoming DN (i.e. a HomeRN was not deleted from the SCCP CdPA), then the message shall fall through to GTT.
   - If the message is SRI or non-SRI, and VstpMnpOptions:MNPCRP is on, and a HomeRN was present in the incoming DN (i.e. a HomeRN was deleted from the SCCP CdPA/MAP MSISDN), then G-Port shall generate Event #70304, and the message shall fall through to GTT. In most network implementations, since the message contains RN+DN, this should cause a GTT failure, which will result in the vSTP sending a UDTS to the originator if the Return Message on Error flag was set in the incoming UDT.

9. If the number is not found in the UDR NPDB then the VstpMnpOptions:SRIDNNOTFOUND option is consulted if query is not SRI prepaid. If the query is identified to be an SRI prepaid then SRI Ack message shall be sent back. NPS will be encoded in the SRI Ack message if VstpMnpOptions:ENCDNPSDNNOTFOUND is ON.
10. If the VstpMnpOptions:SRIDNNOTFOUND option is set to SRINACK then a negative acknowledgement is generated in response to the given message.
11. If the VstpMnpOptions:SRIDNNOTFOUND option is set to GTT then GTT is performed on the message.

- **Message Verification/Decode:**
  - **MTP/SCCP Verification:** vSTP shall not perform any additional MTP/SCCP verification for G-Port. G-Port shall use the information decoded by SCRC.
  - **General TCAP/MAP verification:** TCAP/MAP verification is performed on all messages.

    Any error found in the message verification process will not generate any error responses. G-Port will abort verification and perform message relay on the message using the decoded SCCP information. The Event information shall be printed to report the error.
  - **MAP Verification:** G-Port performs no MAP verification like validation of ACN or decoding of User Information. G-Port shall look at the operation code of the message to distinguish SRI messages with all other messages. After determining the operation code to be SRI, G-Port shall look for the presence of OR Interrogation Parameter to further distinguish SRI from SRI for Optimal routing (SRI-SOR) message. If the OR Interrogation is present or if operation code is not SRI then G-Port message relay is performed. Otherwise, SRI Specific verification is performed.
  - **SRI specific Verification:** This verification shall be performed only for SRI messages. G-Port shall only look for MSISDN parameter only. It shall not look for the existence of any other parameter even if they are mandatory.

    Any error found in this part of the verification process would cause the following to occur:
    - SRI message will be discarded, appropriate SRI negative response message is sent back.

- **Message Handling:**
  - **RN Prefix deletion:**
    - **<u>SRIDN = ‘SCCP’</u>**

      The decoded SCCP CdPA digits may have a RN concatenated with the MSISDN number in two forms 1). RN+DN 2). CC+RN+DN.. So when the SNAI is either RNIDN or RNNDN or RNLDN, G-Port compares the decoded MSISDN number with the list of provisioned home RN prefixes defined in the NPDB. If a match is found, then G-Port shall strip off the RN digits from the number. Number conditioning (if required) is performed after deleting the RN. When SNAI is CCRNDN, G-Port shall first compare the CC to DEFCC/MultCC list. If CC≠ DEFCC/MultCC then no prefix deletion is performed and G-Port processing continues. If CC=DEFCC/MultCC then, G-Port shall compare the digits after CC with the list of provisioned home RN prefixes defined in the NPDB. If a match is found, then G-Port shall strip off the RN digits from the number. If no match then the no prefix deletion is performed and G-Port processing continues.
    - **<u>SRIDN = ‘TCAP’</u>**

      The decoded MAP MSISDN digits may have a RN concatenated with the MSISDN number in two forms. 1) RN + DN 2) CC+RN+DN. The MAP NAI will be used to determine the type: International, National or Subscriber. If VstpMnpOptions:MNPCRP is off, RN prefix deletion will not be attempted. If VstpMnpOptions:MNPCRP is on, then RN prefix deletion will be attempted on all MSISDNs. If the MAP NAI indicates International, then a check shall be performed for DEFCC/MultCC prefix on the MSISDN. If DEFCC/MultCC is detected, then HomeRN deletion shall be attempted using the CC+RN+DN format. All other MSISDNs will use the RN+DN format. G-Port shall compare the decoded MSISDN number with the list of provisioned home RN prefixes defined in the NPDB. If a match is found, the G-Port shall strip off the RN digits from the number. Number conditioning (if required) is performed after deleting the RN. If CC+RN+DN search is performed, G-Port shall compare the digits after CC with the list of provisioned home RN prefixes defined in the NPDB. If a match is found the G-Port shall strip off the RN digits from the number. If no match is found, then no prefix deletion is performed and G-Port processing continues.

The RN Prefix deletion for SRI_SM, when SRISMDN= SCCP or TCAP, will work in the same manner as it works for SRI message when SRIDN=SCCP or TCAP respectively.

- **Number Conditioning:**

  UDR NPDB shall store international MSISDNs only. The received MSISDN number or SCCP CdPA digits may need to be converted to an international number in order to do a database lookup. When G-Port is required to be performed on a message and the number is not international (i.e. NAI of MSISDN number is “National (Significant) Number” or “Subscriber Number” or SNAI is NATL or SUB or RNNDN or RNLDN), then the National/Local to International number is triggered. For a National (Significant) Number, the received CdPA/MAP MSISDN digits will be prepended with the default country code and for a Subscriber number the CdPA/MAP MSISDN digits will be prepended with the default country code and the default network code.

- **Database Lookup:**

  G-Port performs the UDR NPDB database lookup using the international MSISDN. The individual number database is searched first and if the number is not found, then the number range database is searched. If a match is not found in individual and range based database then GTT is performed on the message. In case of MSISDN numbers in the UDR NPDB database being odd and CdPA GTI of the incoming being 2 and the last digit of the number is ‘zero’, G-Port shall first perform database lookup once using the even number. If no match is found then G-Port shall again perform the database lookup now using the odd number (without last digit).

- **Mobile terminated GSM SMS NP:**

  MT-SMS messaging involves the SMSC or MMSC querying the HLR for destination subscriber for SMS delivery. For GSM network, these query messages are called SRI_SM. The HLR response to these messages includes routing information that can be used by the query generator (SMSC) to deliver the SMS message. The G-Port service intercepts these MT-SMS messages destined to the HLR and replies with routing information for out of network destination subscribers.

  The MT-SMS NP feature will:

  - Intercept SMS routing information request from SMSC/MMSC before it reaches the HLR.
  - Extract message destination address (MAP MSISDN or SCCP Called Party GTA based on SRISMDN parameter value in VstpMnpOptions table), condition the digits and perform lookup in NPDB.
  - For destination address/subscribers belonging to foreign networks, sends reply message to the SMSC/MMSC with routing information. This information can be used by the SMSC to route the message to their recipient networks using protocols like SMPP.
  - For in-network destination addresses, the SMS routing information request is relayed to the HLR.

- **MT-SMS NP Processing :**

  The SMSC (or MMSC) will send the SRI_SM message to the vSTP (with a destination of the HLR) with SCCP CdPA GTA (or MAP MSISDN based on SRISMDN parameter value in VstpMnpOptions table) as the DN of the destination subscriber to be GT routed to the HLR.

  The service selector configured to channel MSUs to the G-Port service has an “SNAI” or service NAI parameter as described earlier.

  - **Processing Step:**

- Existing handling of SRI_SM for GT-routed, ANSI/ITU MTP/SCCP, ITU TCAP/MAP, encapsulated in either non-segmented XUDT or UDT SCCP message type, matching G-Port service Selector involves the following steps (detailed MSU decode/encode information provided later).

- **Limitations**
  - MNP G-Port feature is designed with a basic concept: Own-network subscribers are provisioned with an SP Entity type, and other network subscribers are provisioned with RN Entity type or No Entity type

MOs and Operation Supported:

- Following is the list of MO's and operation supported for vSTP MNP G-Port features

Table 52 – MO details 3

MO Name	Operations Supported
VstpSccpMnpOptions	Update
VstpSccpSrvcSel	Insert, Update, Delete
VstpSccpHomeEntity	Insert, Delete

Table 3

- Refer MMI API Guide on Active NOAM/SOAM: "Main Menu ->MMI API Guide" on any DSR 8.4 GA release setup for details about the URI, example and parameters about each MO.

3.6.2 MEALS

3.6.2.1 Measurements:

Following measurements are added by G-Port feature and all are B scoped

Table 53 – Measurements details1

Measurement Name	Dimension	Description	Interval in Mins	Group	Type
vstpMnpCrd	Single	Number of times circuler route detected by MNP CRP	5	Performance	Simple
vstpGportSriRecv	Single	Number of call related SRI message received.	5	Performance	Simple
vstpGportSriReply	Single	Number of call related SRI messages that fell through to GPORT service.	5	Performance	Simple

vstpGportSriGtt	Single	Number of call related SRI message that fell through to GTT due to no match.	5	Performance	Simple
vstpGportSriErr	Single	Number of call related messages that cause an error response message.	5	Performance	Simple
vstpGportSriSmRcv	Single	Number of SRI_SM message received.	5	Performance	Simple
vstpGportSriSmRep	Single	Number of SRI_SM messages resulting in SRI_SM_ACK or SRI_SM_NACK.	5	Performance	Simple
vstpGportSriSmErr	Single	Number of SRI_SM messages resulting in error.	5	Performance	Simple
vstpGportNonCallRelay	Single	Number of non-call related messages relayed by G-Port.	5	Exception	Simple
vstpGportNonCallGtt	Single	Number of on-call related messages that fell through to GTT.	5	Performance	Simple
VstpUdrDbDiscCATxFail	Single	Number of messages discarded by Lss because of send fail to CA layer.	5	Exception	Simple
VstpMnpCAQueryProcessMax	Single	Peak time by CA to send query and receive the response from UDR	5	Performance	Peak
VstpMnpCAQueryProcessAvg	Single	Average time by CA to send query and receive the response from UDR	5	Performance	Average
VstpMnpCAQueryProcesTime	Array	Time required by CA to send query and receive the response from UDR	5	Performance	Simple
VstpMnpCATimeOut	Single	Number of messages for which CA query to UDR timed out	5	Exception	Simple

Table 54 – Measurement details2

Measurement Name	Dimension	Description	Interval in Mins	Group	Type

VstpUdrDbDiscCADcdFail	Single	Number of messages discarded by LSS due to decode failed of CA response message	5	Exception	Simple
VstpUdrDbDiscPduFul	Single	Number of messages discarded when PDU pool is exhausted	5	Exception	Simple
VstpUdrDbDiscIntErr	Single	Number of messages discarded due to internal processing error	5	Exception	Simple
VstpMnpRxRatePeak	Single	The peak Rx messages by MNP Application	5	Performance	Peak
VstpMnpRxRateAvg	Single	The average Rx messages by MNP Application	5	Performance	Average
VstpMnpMsgRecv	Single	Number of messages received MNP Application	5	Performance	Simple
VstpUdrDbSubsNotFound	Single	Number of subscriber record not in UDR DB	5	Exception	Simple
VstpUdrDbQueryFailUDRConnDown	Single	Number of UDR DB Queries not initiated due to UDR connectivity down	5	Exception	Simple

3.6.2.2 Events & Alarms

Following new events & alarms are added by GPORT feature:

Table 55 – Events & Alarms 1

Alarm/Event Name	Type	Description	Raise condition	Clear condition	Throttle sec	Instance	Additional Information	Severity

Invalid length of conditioned digits (70301)	Event	MNP length of the conditioned digit is invalid	1. If the length of the international MSISDN is less than 5 or greater than 15 digits.	NA	1	None	SIO, OPC, DPC, SCCP MSG Type	NA
Conv to intl num - Dflt CC not found (70302)	Event	Dflt CC not defined	1. If the default CC is not found	NA	1	None	SIO, OPC, DPC, SCCP MSG Type	NA
Conv to intl num - Dflt NC not found (70303)	Event	Default NC not defined	1. If the NDC is not found during the conversion of the MSISDN to an international MSISDN	NA	1	None	SIO, OPC, DPC, SCCP MSG Type	NA
MNP Circular Route detected (70304)	Event	NP Circular Route detected	1. If a RN is found, or if neither a RN nor a SP are found, in the database for a DN when a HomeRN was present in the incoming DN of the message	NA	1	None	SIO, OPC, DPC, SCCP MSG Type	NA
Translation PC type is ANSI (70305)	Event	MNP translated PC type is ANSI		NA	1	None	SIO, OPC, DPC, SCCP MSG Type	NA
Invalid digits in MAP MSISDN parameter (70306)	Event	GPORT inv map msisdn for sri/srism	1. If number of digit (MSISDN address digits) is '0' or greater than '21'	NA	1	None	SIO, OPC, DPC, SCCP MSG Type	NA
Invalid prefix/suffix digit length (70307)	Event	Too many digits	1. If SRI_SM or ReportSMDeliveryStatus Digit modification fails for modified DN > 21 digits	NA	1	None	SIO, OPC, DPC, SCCP MSG Type	NA

3.7 VSTP MNP ATI NP

3.7.1 *PURPOSE AND SOLUTION*

Purpose

- Support for ATI Number Portability (a.k.a. ATI NP) feature in vSTP.
- Number Portability (MNP) allows mobile subscribers to retaining their original MSISDN when changing the network to which they subscribe.
- This feature is an optional feature and can be turned on/off via configurable option in the VstpMnpOptions.

Solution

- ATI NP shall perform the following actions based on the message received :
- If the incoming ATI query message requested MNP information, ATI NP shall send the ATI Ack message to the MSC with the Routing Number and number portability status information in the MAP portion of the message.
- If the incoming ATI query message requested Location information, ATI NP shall send the ATI Ack message to the MSC with the Location information of the VLR.

Message flow for ATINP Solution on vSTP

1. MSC will send ATI request to vSTP-MP over SS7 links.
   - vSTP-MP will decode and verify the ATI Message
   - Check whether ATI message has valid request (the requestedInfo parameter must be MNPRequestedInfo and/or Location Information).
   - Decode the MSISDN parameter from the Subscriber Identity parameter.
   - Condition the MSISDN to the international format
2. vSTP-MP will query the UDR NOAM for conditional MSISDN DB.
3. UDR NOAM will look up MSISDN DB and will send response to the vSTP-MP.
4. Determine whether the lookup is considered to be successful based on provisioned options. If yes, use entity information to encode ATI ACK response and route the response to the originator. If no, send ATI NACK response with appropriate error code.

- **Message flow for ATINP Solution on vSTP**

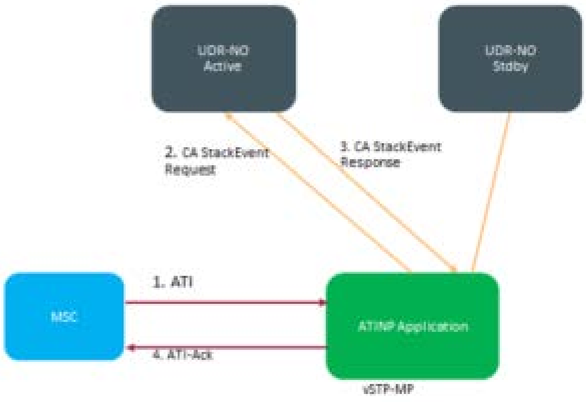


Figure 28 – ATINP message flow

- **ATI NP Message Handling:**

1. The ATI query message arrives at vSTP with routing determined by either route-on-gt or route-on-SSN.
    - If the message is route-on-SSN and the SSN number in Called Party Subsystem field in the matches to the ATINP SSN provisioned on vSTP, the message is sent to ATINP subsystem for further processing.
    - If the message is route-on-GT, vSTP decodes the SCCP portion and uses the data to perform ATINP Selection based on the CdPA GT fields. The result of this selection provides service indicator. If the service selector is ATINP, the message is sent to ATINP subsystem for further processing.
2. The message is decoded to verify the opcode and mandatory parameters. fF the MAP message opcode is ATI, the MSISDN and requested info parameters are decoded. If MSISDN is valid and either MNPinfo or LocationInfo or both parameters are present, further number conditioning is performed. Otherwise, error message is sent back to originator.
3. The decoded DN is conditioned to international number before performing UDR NPDB lookup.

The DN is considered to be in international format if either of the following conditions are true.

- VstpMnpOptions:ATISNAI = INTL OR
- VstpMnpOptions:ATISNAI = NAI and NAI field from MSISDN is INTL (0x1) or Network Specific Number (0x3).

If the incoming DN is in national format, VstpMnpOptions:DefCC will be prepended to the DN to condition it in international format.

4. The UDR NPDB database lookup involves 2 steps:
    - First the exception or individual number database is searched for a match. If the match is found then the data associated with this entry is considered.
    - If the conditioned number is absent in the exception (individual) database, then the number range database is searched. If the match is found then the data associated with this range entry is considered. If the search is unsuccessful then the result is no match.
5. UDR NPDB lookup is considered successful if
    - VstpMnpOptions:ATINPTYPE = ANY and MSISDN is found in the NPDB with entity type = RN, SP or GRN. or
    - VstpMnpOptions:ATINPTYPE = ALWAYS and MSISDN is not found in individual or range entries.

6. If UDR NPDB lookup is successful and if the ATI query contains MNP request info parameter ATINP will send ATI ACK response message with the following fields in the message
   - Routing Number : Formatting will be determined by VstpMnpOptions:ATIACKRN option
   - IMSI : Formatting will be determined by VstpMnpOptions:ATIACKIMSI option
   - MSISDN : Formatting will be determined by VstpMnpOptions:ATIACKMSISDN option
   - Number portability Status

     Not Known To Be Ported (0)

     Own Number Ported Out (1)

     Foreign Number Ported To Foreign Network (2)

     Own Number Not Ported Out (4)

     Foreign Number Ported In (5)
7. If UDR NPDB lookup is successful and if the ATI query contains Location Information request info parameter ATINP will send ATI ACK response message with the following fields in the message
   - VLR Number: Formatting will be determined by VstpMnpOptions:ATIACKVLRNUM option
8. If UDR NPDB lookup is unsuccessful ATINP will send ATI NACK response message with the error code = "UnknownSubscriber"

MOs and Operation Supported:

Table 56 – MO's for ATI NP Feature

MO Name	Operations Supported
VstpSccpMnpOptions	Update
VstpSccpSrvcSel	Insert, Update, Delete

Refer MMI API Guide on Active NOAM/SOAM: "Main Menu ->MMI API Guide" on any DSR 8.4 GA release setup for details about the URI, example and parameters about each MO.

3.7.2 MEALS

3.7.2.1 Measurements

Table 57 – ATI NP Measurements details

Meas Id #	Measurement Name	Description	Dimension	Type	Interval Mins	Measurement Group
21678	vSTPAtiNpRcv	Total MSUs received by SCCP with opcode of ATI.	Single	Simple	5	vSTP MNP Performance
21679	vSTPAtiNpAck	Total ATI-ACK response messages sent by SCCP	Single	Simple	5	vSTP MNP Performance

Meas Id #	Measurement Name	Description	Dimension	Type	Interval Mins	Measurement Group
21680	vSTPAtiNpErr	Total MSUs received by SCCP with opcode of ATI that did not result in either ATI-ACK or ATI-NACK response message.	Single	Simple	5	vSTP MNP Exception
21689	VstpAtiNpRxRate Peak	The peak Rx messages by ATINP Application	Single	Max	5	vSTP MNP Performance
21690	VstpAtiNpRxRate Avg	The average Rx messages by ATINP Application	Single	Average	5	vSTP MNP Performance

3.7.2.2 Alarms & Events

Table 58 – Alarms & Events for ATI NP feature

Event Id #	Event Text	Event Description	Throttle (Sec)	Additional Info
70091	Missing Mandatory Parameter	Subscriber Identity parameter or Requested Info parameter is missing in the received message	10	SIO, OPC, DPC, CgPA, CdPA, SSN
70092	Malformed Subscriber Id	The subscriber Identity parameter in ATI NP query was found to be mistyped.	10	SIO, OPC, DPC, CgPA, CdPA, SSN
70093	Unexpected value for Subscriber Id	The Choice for Subscriber Identity in ATI NP query is not MSISDN.	10	SIO, OPC, DPC, CgPA, CdPA, SSN
70094	Invalid MSISDN length	The MSISDN length in Subscriber Information was 0, or the MSISDN length was 1 (byte) and the MSISDN had only one 0xF (filler) digit.	10	SIO, OPC, DPC, CgPA, CdPA, SSN
70095	ATINP Invalid Requested Info	The Requested Info parameter in incoming ATI NP query was invalid. Either, length of Requested Info parameter < 2, or the Requested Info parameter does not contain MNP Requested Info and/or Location Information , or the parameter is badly formatted	10	SIO, OPC, DPC, CgPA, CdPA, SSN
70096	Digits truncated in encoded parameter	One or more encoded digits parameters in ATI ACK response had to be truncated to fit maximum allowed encoded digits.	10	SIO, OPC, DPC, CgPA, CdPA, SSN

3.8 VSTP MNP INP

3.8.1 PURPOSE AND SOLUTION

Purpose

- Support for INPQ Number Portability feature in vSTP.
- Number Portability (MNP) allows mobile subscribers to retaining their original MSISDN when changing the network to which they subscribe.
- This feature is an optional feature and can be turned on/off via configurable option in the VstpMnpOptions.

Solution

- INPQ shall perform the following actions based on the message received :
    - If the incoming INPQ query message requested MNP information, INPQ shall send the INPQ Ack message to the MSC with the Routing Number and number portability status information in the MAP portion of the message.
    - If the incoming INPQ query message requested Location information, INPQ shall send the INPQ Ack message to the MSC with the Location information of the VLR.

Message flow for INPQ Solution on vSTP

1. MSC will send INPQ request to vSTP-MP over SS7 links.
    - vSTP-MP will decode and verify the INPQ Message
    - Check whether INPQ message has valid request (the requestedInfo parameter must be MNPRequestedInfo and/or Location Information).
    - Decode the MSISDN parameter from the Subscriber Identity parameter.
    - Condition the MSISDN to the international format
2. vSTP-MP will query the UDR NOAM for conditional MSISDN DB.
3. UDR NOAM will look up MSISDN DB and will send response to the vSTP-MP.
4. Determine whether the lookup is considered to be successful based on provisioned options. If yes, use entity information to encode INPQ ACK response and route the response to the originator. If no, send INPQ NACK response with appropriate error code.

Message flow for INQP Solution on vSTP

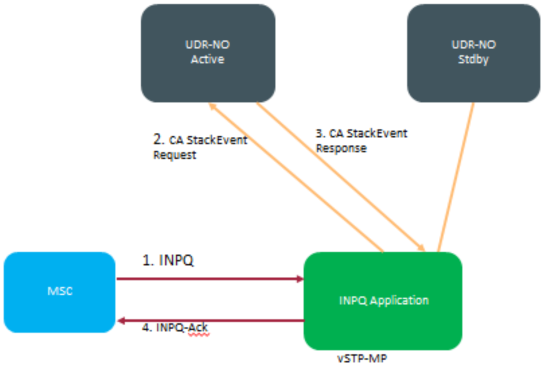


Figure 29 – INQP message flow

3.8.2 MEALS

3.8.2.1 Measurements

Table 59 – Measurements for INPQ feature

Measurement Name	Dimension	Description	Interval in Mins	Group	Type
VstpInpCirrouteDetected	Single	No. of circular route detected by INPQS	5	Performance	Simple
VstpInpSuccessReply	Single	Number of INP successful replies	5	Performance	Simple
VstpInpErrReplies	Single	Number of INP error replies with TCAP error code	5	Performance	Simple
VstpInpDiscardedQuerieNoReply	Single	Number of INP discarded queries as no reply is generated	5	Performance	Simple
VstpInpQueryReceived	Single	Inp Query received			

3.8.2.2 Alarms & Events

Table 60 – Alarms & Events for INPQ feature

Alarm/Event Name	Type	Description	Raise condition	Clear condition	Throttle sec	Instance	Additional Information	Severity
Unsupported ACN object ID length.(70420)	Event	Unsupported ACN object ID length.	ACN object Identifier length > 32	NA	10	None	SIO, OPC, DPC, SCCP MSG Type	NA
Failed to Decode TCAP parameters.(70421)	Event	Failed to Decode TCAP parameters.	Invalid INAP CalledPartyNumber len,No parameter sequence	NA	10	None	SIO, OPC, DPC, SCCP MSG Type	NA
INAP Called Party Number is missing.(70422)	Event	INAP Called Party Number is missing.	No INAP CalledPartyNumber parameter	NA	10	None	SIO, OPC, DPC, SCCP MSG Type	NA

3.9 VSTP MTP SCREENING SUPPORT

3.9.1 *PURPOSE AND SOLUTION*

Purpose

At present VSTP allows all MSUs to enter for processing which will be received on a link set. This will be a security issue for VSTP because any message can enter into VSTP for processing and can be part of crashing the software or interrupt the processing of other messages.

Solution

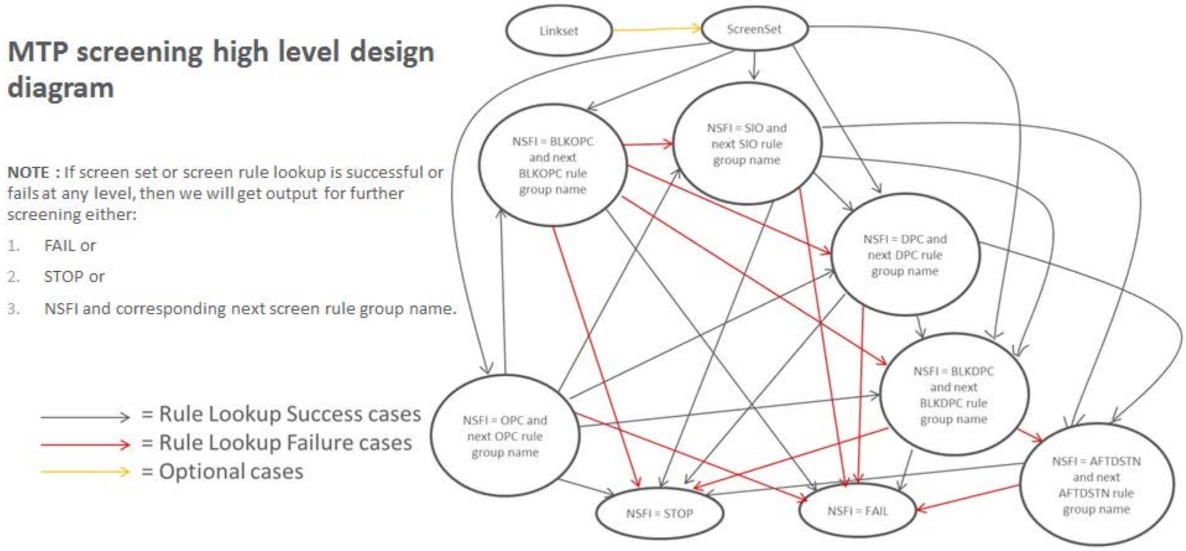
MTP screening feature provides solution to screen the message based on MTP3 layer parameters of the messages. The feature achieves it by :

1. Creating screening rule and keeping rules of same type in a group.
2. Creating a screen set and referring rule group created above in that screen set.
3. Attaching that screen set to incoming linkset.

Feature Overview

- MTP Screening feature provides a first level of security check for VSTP.
- The MTP Screening feature examines the contents of a Message Signaling Unit (MSU) attempting to enter the VSTP against predefined criteria in the VSTP database to determine if the MSU should be allowed to enter.
- When a message comes on a linkset, the associated screen set will be looked up. Based on the NSFI and rule group name associated with screen set, the rule in the corresponding rule group will be looked up.
- If rule lookup is successful, then message will go for further screening level based on NSFI and the next screen rule group name associated with it.
- If rule lookup does not find a match, then
    - In case of BLKOPC/BLKDPC rule type, default rule for that rule group will be looked up and based on NSFI and next screen rule group name associated with default rule further screening performed.
    - In case of OPC/SIO/DPC/AFTDSTN rule type, FAIL NSFI will be performed.
- The final result of MTP screening should always be either FAIL or STOP.
    - In case of FAIL, the message will be discarded.
    - In case of STOP, the message will go for further processing in VSTP.

MTP screening high level design diagram



MTP screening high level design diagram
Linkset
ScreenSet
NSFI = BLKOPC and next BLKOPC rule group name
NSFI = SIO and next SIO rule group name
NSFI = DPC and next DPC rule group name
NSFI = BLKDPC and next BLKDPC rule group name
NSFI = OPC and next OPC rule group name
NSFI = AFTDSTN and next AFTDSTN rule group name
NSFI = STOP
NSFI = FAIL
= Rule Lookup Success cases
= Rule Lookup Failure cases
= Optional cases

NOTE : If screen set or screen rule lookup is successful or fails at any level, then we will get output for further screening either:

1. FAIL or
2. STOP or
3. NSFI and corresponding next screen rule group name.

Figure 30 – MTP screening design diagram

Types of MTP Screening "NSFI":

- OPC

- BLKOPC
- SIO
- DPC
- BLKDPC
- AFTDSTN

Types of MTP Screening "NSFI" - OPC:

- OPC NSFI and next OPC rule group name defines rules that have all the Originating Point Codes that are allowed to send any message to the recipient network.
- The possible values for rule type OPC are BLKOPC, SIO, DPC, BLKDPC, STOP, FAIL.
- When a message comes on a linkset, the corresponding screen set will be looked up. Based on the NSFI and next screening rule group name associated with screen set (i.e. OPC as first NSFI and next OPC rule group name in that case), the rule lookup will be performed.
- If OPC screening rule lookup is successful, then message should go for further screening level.
- If OPC screening rule lookup does not find a match, then message should be discarded if mtpScrTestMode is OFF in VstpLinkset table.

Types of MTP Screening "NSFI" - BLKOPC:

- BLKOPC NSFI and next BLKOPC rule group name defines rules that have all the Originating Point Codes that are prohibited to send any message to the recipient network.
- The possible values for rule type BLKOPC are SIO, DPC, BLKDPC, STOP, FAIL.
- When a message comes on a linkset, the screen set associated with that linkset will be looked up and based on the NSFI and next screening rule group name associated with screen set (i.e. BLKOPC as first NSFI and next BLKOPC rule group name in that case), the rule lookup will be performed.
- If BLKOPC screening rule lookup is successful, then message should be discarded if mtpScrTestMode is OFF in VstpLinkset table.
- If BLKOPC rule lookup does not find a match in BLKOPC rule group, then message should go for further screening level based on default rule in BLKOPC rule group.

Types of MTP Screening "NSFI" - SIO:

- SIO NSFI and next SIO rule group name defines rules that have all the SIO values that are allowed/prohibited to send any message to the recipient network.
- The possible values for rule type SIO are DPC, BLKDPC, AFTDSTN, STOP, FAIL.
- When a message comes on a linkset, the corresponding screen set will be looked up. Based on the NSFI and next screening rule gr screening rule group name associated with screen set (i.e. SIO as first NSFI and next SIO rule group name in that case), the rule lookup will be performed.
- If SIO screening rule lookup is successful, then message should go for further screening level.
- If SIO rule lookup does not find a match, then message should be discarded if mtpScrTestMode is OFF in VstpLinkset table.
- The NSFI "AFTDSTN" only applicable for messages which has service indicator value < 3.

Types of MTP Screening "NSFI" - DPC:

- DPC NSFI and next DPC screening rule group name defines rules that have all the Destination Point Codes that are allowed to send any message to the recipient network.
- The possible values for rule type DPC are BLKDPC, AFTDSTN, STOP, FAIL.
- When a message comes on a linkset, the corresponding screen set will be looked up. Based on the NSFI and next screening rule gr screening rule group name associated with screen set (i.e. DPC as first NSFI and next DPC rule group name in that case), the rule lookup will be performed.
- If DPC screening rule lookup is successful, then message should go for further screening level.

- If DPC rule lookup does not find a match, then message should be discarded if mtpScrTestMode is OFF in VstpLinkset table.

Types of MTP Screening "NSFI" - BLKDPC:

- BLKDPC NSFI and next BLKDPC rule group name defines rules that have all the Destination Point Codes that are prohibited to send any message to the recipient network.
- The possible values for rule type BLKDPC are AFTDSTN, STOP, FAIL.
- When a message comes on a linkset, the corresponding screen set will be looked up. Based on the NSFI and next screening rule gr screening rule group name associated with screen set (i.e. BLKDPC as first NSFI and next BLKDPC rule group name in that case), the rule lookup will be performed.
- If BLKDPC screening rule lookup is successful, then message should be discarded if mtpScrTestMode is OFF in VstpLinkset table.
- If BLKDPC rule lookup does not find a match in BLKDPC rule group, then message should go for further screening level based on default rule in BLKDPC rule group.

Types of MTP Screening "NSFI" - AFTDSTN:

- AFTDSTN NSFI and next AFTDSTN rule group name defines rules that have all the Affected Destination values for network management messages that are allowed to send any message to the recipient network.
- The possible values for rule type AFTDSTN are STOP and FAIL.
- During screening if NSFI is AFTDSTN then either STOP or FAIL action will be performed based of AFTDSTN screening success or failure.
- The AFTDSTN NSFI can't be configured as first NSFI in Screen Set.
- Only messages which have Affected Destination (i.e. SNM message) will be screened.
- The message which doesn't have Affected Destination will be continue processed and not discarded. Event 70393 (Invalid MSU received for AFTDSTN NSFI) will be generated if mtpScrEventLog flag is ON for that incoming linkset.

Table 61 - Message processing with mtpScrEventLog and mtpScrTestMode option when NSFI is FAIL

mtpScrEventLog (ON/OFF)	mtpScrTestMode (ON/OFF)	Message discarded/Message continue processed for further routing	Event 70392 (MSU discarded due to MTP Screening) Generated (Yes/No)
OFF	OFF	Message will be discarded	No
ON	OFF	Message will be discarded	Yes
OFF	ON	Message will be continue processed for further routing	No
ON	ON	Message will be continue processed for further routing	Yes

NOTE:

When mtpScrEventLog is OFF and mtpScrTestMode is ON then screening rule processing will not take place.

NSFI STOP doesn't have any effect with these options.

Table 62 – MO details for MTP screening feature

MO Name	Operations supported	URI
MTP Screening Rule	POST/PUT/DELETE/GET	/vstp/mtpscreeningrules
MTP Screen Set	POST/PUT/DELETE/GET	/vstp/mtpscreensets
Linkset	POST/PUT/DELETE/GET	/vstp/linksets

- Refer MMI API Guide on Active NOAM/SOAM: "Main Menu ->MMI API Guide" on any DSR 8.4 GA release setup for details about the URI, example and parameters about each MO.

Screening Examples:

1. If a message is coming with the values:
   - Service Indicator = 5
   - Network Indicator Code = 3
   - Priority = 0

- In order to **discard** this message, please configure the SIO screening rule through MMI as shown in Slide #29 with NSFI = FAIL.

2. If a message is coming with the values:
   - Service Indicator = 0
   - Priority = Any Value (0-3)
   - Network Indicator Code = Any Value (0-3)
   - H0 code = 4
   - H1 Code = 1

- In order for the message to be **continued to process**, please configure the SIO screening rule through MMI as shown in Slide #29 with NSFI = STOP.

3.9.2 MEALS

3.9.2.1 Measurements

Following is the List of measurements supported by MTP Screening Feature:

- VstpRxScrPerformed: The total number of MSUs on which MTP Screening is performed.
- VstpRxLnksetScrPerformed: The total number of MSUs on which MTP screening performed on Linkset.
- VstpRxMSUScrDiscard: The total number of MSUs discarded due to MTP Screening.

- VstpRxLnksetMSUScrDiscard: The total number of received MSUs discarded due to MTP screening on Linkset.

3.9.2.2 Alarms & Events

Following is the list of events supported by MTP Screening Feature:

Table 63 – Alarms and Events for MTP screening feature

Alarm/Event Name	Type	Description	Raise Condition
MSU Failed MTP Screening (70392)	Event	MSU Failed MTP Screening	When incoming MSU is discarded on a linkset due to MTP screening and mtpEventLogging flag is turned on for that linkset.
Invalid MSU received for AFTDSTN NSFI (70393)	Event	Invalid MSU received for AFTDSTN NSFI	When NSFI is AFTDSTN and a non-network management message received which does not have affected destination and mtpEventLogging flag is turned on for that linkset.

Limitations:

1. This feature does not implement screening based on SCCP layer parameters. The feature scope is limited to screening based on MTP3 layer parameters.
2. Point code support for the following is not tested in this release and advised not to configure the same:
   - ITUN16
   - ITUN24
   - ITUN_S
   - ITUI_S

Troubleshooting Steps

- If MTP Screening executes successfully on an incoming MSU, then **VstpRxScrPerformed** measurement will be pegged on a system basis.
- If MTP Screening executes successfully on an incoming MSU, then VstpRxLnksetScrPerformed measurement will be pegged on a per Linkset basis.
- If incoming MSU is discarded due to MTP Screening, then VstpRxMSUScrDiscard measurement will be pegged on a system basis.
- If incoming MSU is discarded due to MTP Screening, then VstpRxLnksetMSUScrDiscard measurement will be pegged on a per Linkset basis.
- When incoming MSU is discarded on a linkset due to MTP screening and mtpEventLogging flag is turned on for that linkset, then event 70392 MSU Failed MTP Screening will be generated and contains reason with MTP3 layer parameters (i.e. OPC, DPC, SIO) information and incoming Linkset Name.
- When NSFI is AFTDSTN and a non-network management message received which does not have affected destination and mtpEventLogging flag is turned on for that linkset, then event 70393 Invalid MSU received

for AFTDSTN NSFI will be generated and contains reason with MTP3 layer parameters (i.e. OPC, DPC, SIO) information and incoming Linkset Name.

If any of the above statement fails as per given scenarios, then verify configuration.

If issue still exists, then contact Oracle for support.

3.10 VSTP MULTIPLE POINT CODE SUPPORT

3.10.1 *PURPOSE AND SOLUTION*

Purpose:

- At present vSTP supports only 4 True Point Codes(TPCs) of ANSI/ITU-I/ITU-N/ITU-N24 domain and 1 Capability Point Code(CPC).
  - This limits operators from hosting more no. of point codes which triggers the need for more no of nodes in the network and associated provisioning & maintenance.
  - Since only for each domain only one TPC can be configured, it limits operators from using same Signaling Transfer Point(STP) to handle multiple national networks.
  - It also limits provisioning of additional links between two nodes beyond the number of links permitted by the protocol.
  - Moreover, vSTP does not support associating CPC with a hosted application/service.
- MPC solution resolves the above limitations by enabling vSTP to host Secondary Point Codes (SPCs) in addition to the true point codes used by the vSTP in any of the three domains ANSI, ITU-N (14-bit or 24-bit) and ITU-I.
- It also optionally permits attaching service/application with hosted CPC.
- This in turn enables collapsing/merging of multiple STPs into one vSTP.

Solution:

1. VstpLocalSP table stores all the self point codes hosted by vSTP. This table schema shall be changed to allow provisioning of SPC and CPC.
2. Support shall be provided to associate CPC with a service/application hosted by vSTP.
3. Adjacent Remote Signaling Point(RSP) can be associated with LocalSP (configured as TPC or SPC) via Linkset configuration (in VstpLinkset table).
4. SRM message encoding shall be modified to set TPC/SPC as the Origin Point Code(OPC) as configured for the recipient RSP.
5. Upgrade changes required to ensure old entries of VstpLocalSP table is copied properly into the new VstpLocalSP table.

Feature Overview:

- This feature proposes to start support for Secondary Point Codes and increase the number of supported Capability point codes.
- Multiple Point Code (MPC) feature shall allow the vSTP to add the support of Secondary Point Codes (SPCs) in addition to the true point codes used by the vSTP in any of the three domains ANSI, ITUN/ITUN-Spare (14-bit or 24-bit) and ITUI/ITUI-Spare.
- This is a different concept from capability point codes. The provisioning and routing will use secondary point codes as if they were the actual point code of the vSTP. SPCs are supported for any type of link (A, B, C, D, etc.).
- In addition to the one True Point Code (TPC) already supported for each of the ANSI, ITU-N (14-bit or 24-bit) and ITU-I domains, the vSTP support a pool of Secondary Point Codes (SPC), each of which may be assigned as either ANSI, ITUI/ITUI-Spare, 14-bit ITUN/ITUN-Spare, or 24-bit ITUN.
- In addition to the SPCs this feature also recommends increasing the number of CPCs supported by the vSTP.

- Currently only 1 CPC is supported. This number shall be increased to 100. The increase CPC would allow the vSTP to support more applications on the same node and allow route-on-gt functionality for routing to various applications.
- MPC feature creates the framework to allow provisioning and usage of SPCs in vSTP. This change shall primary affect the provisioning and routing algorithms. In addition to the SPC's the CPC shall also be increased.

Sccp Message Routing:

Message destined for TPC

- Existing vSTP SCCP layer signaling data message processing order can route the message to either of the following components:
  - SCMG
  - LSS
  - GTT
- SCMG
  - Message with CDPA SSN as SCMG and CDPA RI as "Route On SSN" is sent to SCMG for processing.
- LSS
  - CDPA SSN matches with SSN configured in VstpSccpApplications table.
  - Application's Admin state is Enabled.
- GTT
  - When above 2 criteria fails.
  - With MPC support
    - ▪ Handling of message destined for TPC remains unchanged.
    - ▪ Message destined for SPC is treated the same way as it is done for TPC.
    - ▪ Message destined for CPC handled in the following way :
      - VstpLocalSP table must have this CPC for the message to reach SCCP.
      - Check for routing Indicator whether it is GT or SSN.
      - If RI is GT, message goes for GTT. Otherwise message goes for application.
      - Check VstpSccpApplications table and verify whether the CDPA SSN value is provisioned & admin state is enabled.
      - If above condition satisfies message goes to LSS for further processing. Otherwise message is discarded and an event is raised.

Table 64 – SCCP message routing behavior

Routing Change		Rt-On-Gt	Rt-On-Ssn
DPC=TPC		No Change	No Change
DPC=SPC		Same handling as TPC	
DPC=CPC	cpcType = STP	Handling takes usual path of DPC being set to TPC/SPC	

	cpcType != STP	Application specific handling triggers

Application Handling : (DPC = CPC)	cpcType = EIR	cpcType = Others (Future)
	• Check whether application is provisioned in VstpSccpApplication • If yes, check whether admin state is set to Enabled • Send to LSS EIR	• Implementation specific • As new applications gets added message routing path shall be decided accordingly to send the message respective application

- OPC of the message generated by vSTP
  - Any message generated by vSTP shall set the OPC to the TPC/SPC used by the message's destination. Following is a list of messages generated by vSTP
    - Signaling Link Test Messages
    - MTP Network Management Messages
    - SCCP Messages post GTT
    - Message generated by local subsystem
- DPC of the message generated by vSTP
  - There is no change.
- Affected Point Codes
  - TFx and TCx messages may include vSTP's secondary point code depending on scenario(s)
- Message Specific Handling
  - Signaling Link Test Messages (SLTM/SLTA)
    - vSTP shall validate that the DPC of the message matches with the TPC/SPC provisioned against the OPC of the message.
    - Even if DPC matches with any other provisioned TPC/SPC, the message shall be rejected.
    - This check is enforced to detect provisioning errors which may interfere with network management.
  - Transfer Prohibited/Restricted/Allowed Messages
    - vSTP shall never generate a TFP, TFR with a Affected Point Code set to vSTP's True Point Code or one of vSTP's Secondary Point Codes.
    - If vSTP receives a Route Set Test message (RST or RSR) concerning a Secondary Point Code, vSTP shall respond with a TFA concerning the Secondary Point Code.
  - Route Set Test Messages
    - Affected Point Code in vSTP generated routeset test messages shall always be a Remote Point Code
  - Transfer Control Messages
    - For TFC messages, the Affected Point Code is always the DPC of the message that encountered congestion. For vSTP, the Affected Point Code of the TFC is always a remote point code.
  - Subsystem Test (SST)

    - When vSTP receives a Subsystem Test (SST) message for a local subsystem that is online, vSTP sends an SSA back.
    - If the SST’s Affected Point Code is either the True Point Code or a Secondary Point Code, vSTP shall respond with an SSA with the Affected Point Code set to the SST’s Affected Point Code.
  - GTT Messages
    - In present implementation, when vSTP performs GTT, and the result of translation is a remote point code, vSTP replaces the OPC of the message with it’s True Point Code.
    - With this feature, vSTP shall replace the OPC of the message with the TPC/SPC used by the translated point code.
  - Local Subsystem Messages
    - When vSTP receives a Subsystem Test (SST) message on TPC/SPC for a local subsystem that is online, vSTP sends an SSA back.
    - In case the subsystem is not online, no response is sent back.

Limitations:

1. This feature does not implement Multiple Linkset towards same RSP.
2. This feature does not implement Local subsystem routing i.e. “messages coming with routing indicator as route on GT to be routed locally to application hosted on the vSTP” , wont be supported.

MO’s and operations supported

Point Code Provisioning

- VstpLocalSP Table schema is changed to accommodate provisioning of SPC(s) and CPC(s).
  - Upto 40 SPCs is supported.
  - Upto 100 CPCs is supported.
  - Capability Point Code can be associated with Service/Application.

Table 65 – Point Code provisioning

Field Name	**Description**	**Mandatory (M)/Optional(O)**	**Default Value**	**Value Range**	**Modification Supported**
lspName	LSP Name	M	NA	UNCHANGED	No
lspId	LSP ID				No
Domain	PC Domain				No
mtpPc	Point Code (Integer)				Yes only if point code type is "CPC"

mtpPcStr	Point Code String				
pcType	Defines Point Code Type	M	NA	TPC/ SPC/ CPC	No
cpcType	Defines Service/Application	O	STP	STP/ EIR	No

- “pcType” field is used to identify the type of point code whether it is TPC or SPC or CPC.
- “cpcType” field is used to identify the type of service/application hosted by that point code.
- If “pcType” field is set to "CPC", user has to supply "cpcType" value, in other cases default value "STP" shall be applied.
- Below is a sample entry with the new table structure.

Table 66 – lsp Name with reference

lspName	LspID	Domain	mtpPC	mtpPcStr	pcType	cpcType
LSP1	1	ITUI	14503	7-20-7	TPC	STP
LSP2	2	ITUI	4114	2-2-2	CPC	EIR

- VstpSccpApplications Table schema is changed to include “appType” field which indicates application/service associated with the SSN.
- The only value supported for now would be EIR, INPQ, ATINP.
- When new application / service is added , this type shall include the same.

Table 67 – Field name with Description

Field Name	Description	Default Value	Value Range	Modification Supported
appId	Application ID No	NA	0-65535	No
appType	Application or Service Type	NA	EIR (For Now)	No
Ssn	Subsystem Number	NA	0-255	No
appAdminState	Application admin state	Disabled	Enabled/Disabled	Yes

- ed in place of “appName” to indicate a service / application provided by vSTP

Table 68 – AppType with Ssn id

appId	appType	Ssn	appAdminState
1	EIR	9	Disabled

Provisioning Dependencies/Restrictions

- VstpLocalSP

- While provisioning CPC, if service provided in "cpcType" field is other than "STP", ensure it is provisioned in VstpSccpApplications table.
- If same service type is not present in VstpSccpApplications table, first an entry has to be made there.
- Allow deletion of SPC only if it is not referenced in any other tables like VstpLinkset.

– VstpLinkset

- Allow SPC to be selected as LSP ID while configuring Linkset.
- CPC ID is not allowed to configure as LSP ID in VstpLinkset MO.

– VstpSccpApplications

- Restrict deletion of tuple if matching "appType" entry exists in VstpLocalSP MO.
- Allow deletion only if no matching entry exists in VstpLocalSP MO.

3.10.2 MEALS

3.10.2.1 Measurements

NO MEASUREMENT ADDED/MODIFIED FOR THIS FEATURE.

3.10.2.2 Alarms & Events

Following Event is reused by this feature, with a new reason code.

Table 69 – Alarms & Description

Alarm/Event Name	Type	Description	Raise Condition	Clear Condition	Throttle Sec	Instance	Additional Information	Severity
SLTC failure (70378)	Event	Signaling Link Test Failure	While handling SLTM/SLTA message if DPC of the message doesn’t match with the TPC/SPC provisioned against the OPC	NA	NA	None	Message Type, DPC & OPC of the message	NA

Table 70 – Events & Description

Alarm/Event Name	Type	Description	Raise Condition	Clear Condition	Throttle Sec	Instance	Additional Information
SCCP Application MSU Discarded (70416)	Event	SCCP Application MSU Discarded	Data message having DPC=CPC with cpctype as “EIR” but message SSN does not match with the one provisioned in VstpSccpApplications table or the application admin state is “disabled”	NA	10	None	Contains rejection reason is either SSN mismatch or admin state being “disable

3.11 VSTP FLOW CONTROL ENHANCEMENTS

DETAILS OF FEATURE ARE NOT APPLICABLE AS, IT IS AN ENGINEERING FEATURE.

3.12 VSTP ANSI-ITU CONVERSION

3.12.1 *PURPOSE AND SOLUTION*

Purpose:

- During cross domain signaling some ANSI and ITU SCCP and/or MTP3 user message parameters are incompatible in format.
- Hence there is a need for conversion capability that will correctly format and decode/encode SCCP parameters.
- There is a need for conversion capability to support UDT(S) and XUDT(S) across inter-network traffic.

Solution:

vSTP ANSI ITU Conversion Feature have been developed to perform cross domain conversion over inter-network traffic(UDT(S) and XUDT(S) messages, MTP routed, GT routed).

Feature Overview:

- Cross domain (ANSI/ITU) signaling can be MTP routed or GT routed.
- Cross domain conversion combination supported across domains are
    - ANSI, ITU-I(S) ,ITU-N(S)
    - ITU-N24, ITU-I(S)
- Based on message type, ANSI/ITU Conversion supports UDT, XUDT, UDTS and XUDTS messages.
- The feature also provides SCCP management (SCMG) across network type boundaries
- This feature also provide support of China Point Code SCCP conversions to ITU-International.

SCCP Conversion Overview:

- MTP Routed UDT(S)/XUDT(S) Conversion
- MTP Routed UDT(S)/XUDT(S) SCMG Conversion
- GT Routed UDT(S)/XUDT(S) Conversion
- SCCP Conversion Details
    - Conversion of MTP Routing labels
    - Conversion of SCCP parameters
    - SCCP Conversion through GTT Action

- MTP routed SCCP messages (UDT(S)/XUDT(S)) are converted in the following steps:
    - MTP conversion
    - SCCP Conversion
- GT routed SCCP messages (UDT(S)/XUDT(S)) are converted in the following steps:
    - MTP conversion
    - SCCP Conversion

Table 71 – MO details for GTT action feature

MO Name	Operations supported	URI
Remote Signaling Points	Insert, Update, Delete	/vstp/remotesignalingpoints
GTT Sets	Insert, Update, Delete	/vstp/gttsets
GTT Selectors	Insert, Update, Delete	/vstp/gttselectors
Global Title Addresses	Insert, Update, Delete	/vstp/globaltitleaddresses
GTT Modifications	Insert, Update, Delete	/vstp/gttmods
Default Conversions	Insert, Update, Delete	/vstp/defaultconversions

- Refer MMI API Guide on Active NOAM/SOAM: “Main Menu ->MMI API Guide” on any DSR 8.4 GA release setup for details about the URI, example and parameters about each MO.

4 RELEASE 8.4.0.3.0 FEATURE OAM CHANGES

At the time of upgrade to DSR 8.4.0.3.0 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.

4.1 GTT THROTTLE ACTION

4.1.1 *PURPOSE AND SOLUTION*

Purpose

- This feature is a part of SS7 Security Firewall.
- More attention is being given to the security aspects in SS7 networks.
- Mobile Interconnects is generally used for SS7 network security attacks. Specifically spam and DoS attacks.
- To prevent these attacks Interconnect level (SCCP level) traffic flow control is needed.
- On Sigtran linkset, vSTP provides ingress throttling by using the per link data rate.
- However, there is no support for Egress throttling (traffic control) of GTT messages in vSTP.
- GTT Throttle feature provides the support for Egress throttling of GTT messages in vSTP.

Solution

- The GTT Throttle Feature design is both simple and flexible by adding a new type of GTT Action SFTHROT.
- For each GTT Action, user will provision threshold as maximum number of MSUs hitting the GTT action per second.
- SMS framework is used to accumulate the total number of MSU count per SFTHROT action.
- When a MSU hits a GTT action of the type SFTHROT, the MSU count of that action is updated.
- SMS framework accumulates the total number of messages per SFTHROT action on MP Leader and sends cumulative count to all MPs across site.
- If the cumulative count of messages has crossed the provisioned threshold, MPs will start throttling that messages.
- Any MSU hitting that GTT action will get discarded and the MSU count of that messages is not increased due to throttling, due to which cumulative value will decreased in next sliding window. Once the cumulative value drops below configured threshold it will allow messages.

Feature Overview

The GTT Throttle action works based on the following rules:

1. When an MSU hits a GTT action of the type SFTHROT, the MSU count of that action gets updated.

   Note: The Shared Metric Service (SMS) framework is used to accumulate the total number of MSU count per SFTHROT action.

2. The MSU count is updated only on the Message Processor (MP) on which the message is received for that action. On the other hand, the Threshold configuration for SFTHROT action is across the MPs.

   Note: For each GTT Action, user provisions a threshold value that is the maximum number of MSUs hitting the GTT action per second.

3. Two sysmetrics are registered. The first is for MSU count per MP and second one for cumulative MSU count across the site.

4. Aggregation of the MSU count from all the MPs is done by the MP Leader. There is only one MP leader across the site. It performs the aggregation of MSU counts. Rest of the MPs across the site are

known as followers.

5. Whenever a message comes to any MP, it will increment the sysmetric count of that MP known as local sysmetric count. All the follower MPs will send the local sysmetric count data to the MP Leader to get the aggregated value of that action.

6. The MP Leader will receive the data from all the other MPs including it's own local sysmetric count. It will do the aggregation and broadcast the cumulative count to all the MPs.

7. The SMS framework is used to send local sysmetric count to MP leader and receive the aggregated sysmetric count from it. The aggregation of the count is taken care by SMS framework hence, any degradation in SMS service will impact the feature.

8. When GTT message is received for SFTHROT action, then the aggregated sysmetric count is compared with the configured threshold value for that action:

   If the aggregated sysmetric count value is lesser than the configured threshold value, then the message is allowed and the local sysmetric count value is increased by 1.

   If the aggregated sysmetric count value is more than the configured threshold value, then the local sysmetric count value does not get increased due to throttling. The GTT message is discarded, discard measurement is pegged for that action, and an alarm is raised.

   a. The alarm will get cleared once the aggregated sysmetric count drops below 90% of the configured threshold value.

   b. As there is no local sysmetric is pegged, the aggregated count will be decreased in next sliding window. Convergence time is 2 sec.

   c. Once the cumulative value drops below the configured threshold, it will allow the GTT messages for that action and the local sysmetric count will be increased.

      Note: For GTT Throttle action, an error margin of +2% to -2% of the provisioned threshold value must be considered. The error margin depends on the cloud infrastructure load & burst pattern of incoming traffic.

The following figure shows the process flow for GTT Throttle action:

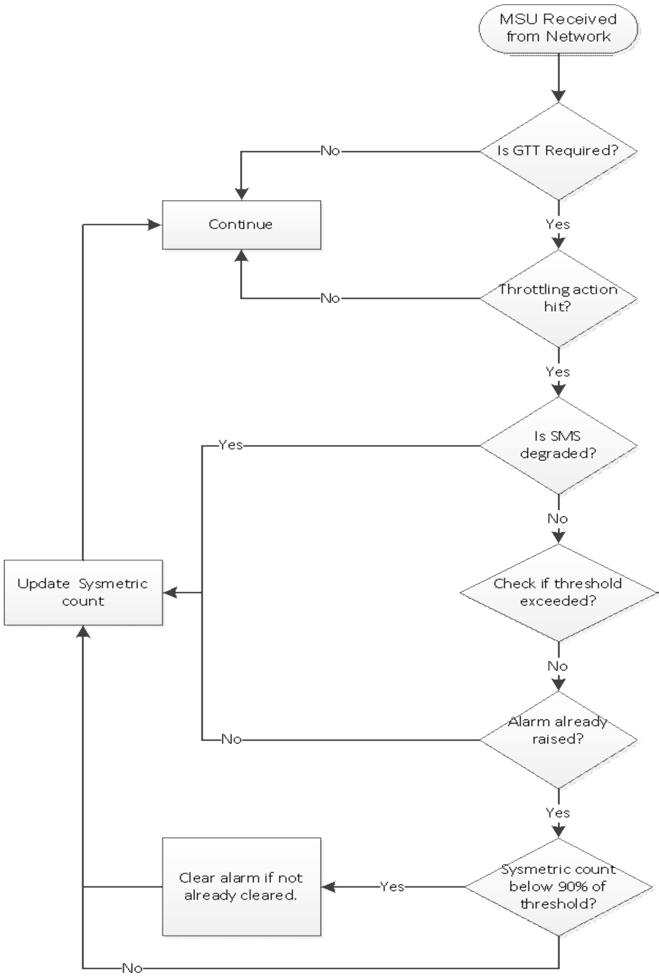

MSU Received from Network
Is GTT Required?
No
Yes
Continue
Throttling action hit?
No
Yes
Is SMS degraded?
Yes
No
Discard MSU
Update Sysmetric count
Check if threshold exceeded?
Yes
Raise alarm if not already raised.
No
Alarm already raised?
No
Yes
Clear alarm if not already cleared.
Yes
Sysmetric count below 90% of threshold?
No

Figure 31 – Process Flow of GTT Throttle Action

4.1.2 MEALS

4.1.2.1 Measurements

Table 72 – Measurements

Measurement Name	Dimension	Description	Interval in Mins	Group	Type
VstpThrottleActionMsgRatePeak	Arrayed	The peak number of messages Aggregated per GTT Throttle Action.	5	Performance	Max

VstpThrottleActionMsgRateAvg	Arrayed	The Average number of messages Aggregated per GTT Throttle Action.	5	Performance	Average
VstpThrottleActionMsgDiscard	Arrayed	The number of messages discarded per GTT Throttle Action.	5	Exception	Simple

4.1.2.2 Alarms & Events

No event is added/modified for this feature.

Following is the alarm supported by GTT Throttle Action Feature:

Table 73 – Alarms for GTT Throttle Action Feature

Alarm/Event Name	Type	Description	Raise Condition	Clear Condition	Throttle Sec	Instance	Additional information	Severity
Sccp Egress Tps Threshold Crossed(70418)	Alarm	Sccp Egress Tps Threshold Crossed.	When incoming message rate for actid SFTHROT is 100% of the provisioned threshold.	When incoming message rate for actid SFTHROT is reduced to 90% or less of the provisioned threshold.	86400	GTTAction	Ta index	Major

Limitation

There is error margin of +2% to -2% of the provisioned threshold value depending on the cloud infrastructure load & burst pattern of incoming traffic.

Dependencies

The GTT Throttle action support for vSTP has no dependency on any other vSTP operation.

Troubleshooting Steps

In case of error scenario, check the incoming traffic. The incoming traffic must be 100% or above the provisioned threshold value for respective actid with SFTHROT action.

4.2 GTT SCPVAL ACTION

4.2.1 *PURPOSE AND SOLUTION*

Purpose

In certain MAP operations, some of the MAP parameters are expected to be same as either the SCCP CdPA or CgPA. At present, vSTP has no validation checks for the same.

Solution

With SS7 Firewall, a new GTT Action will be added to perform validation on MAP parameters. It makes comparison of the SCCP and MAP digits. The feature achieves it by adding a new GTT Action, SCPVAL, along with relevant parameters.

Feature Overview

- In certain MAP operations, some of the MAP parameters are expected to be same as either the SCCP CdPA or CgPA.
- A new GTT Action will be added to do such validation.
- This validation will be done only on MO-FSM and MT-FSM messages coming to vSTP.
- A new GTT Action “SCPVAL” is introduced for this task, which will have the following parameters:
    - SPRM
    - TPRM
    - NDGT
    - USEICMSG
    - UIMREQD
    - DEFACTID

Table 74 – GTT Action SCPVAL – Parameters

Field Name	Description	Default Value
ACT	GTT Action Existing Values: Disc, Dup, Fwd, Srvc, Tcaperr, Udts New Value: SCPVAL	Mandatory Enum
SPRM	SCCP Parameter	Mandatory Values: CGGTA/CDGTA
TPRM	TCAP Parameter	Mandatory Values: SMRPOA/SMRPDA
NDGT	Number of digits to be matched. Specifies the number of digits that needs to be matched between SCCP parameter and MAP parameter.	Optional Values: 1-21, All Default value: All
USEICMSG	Use Incoming Message. Specifies whether to retrieve the data for comparison from the original or post GTT message.	Values: ON/OFF OFF: Use original, i.e. as the message was received by SCCP ON: Use post-GTT, i.e. after possible EPAP/GTT

		translation/modification data has been applied
UIMREQD	UIM Required. Specifies whether to generate event in case GTT Action failure.	Values: ON/OFF
DEFACTID	Default Action ID. The default action that is performed when SCPVAL GTT Action fails.	String

The flowchart depicts the implementation of MAP SCCP validation.

Figure 32 – Flow Diagram for SCPVAL

4.2.2 MEALS

4.2.2.1 Measurements

Following is the list of measurements supported by SCPVAL Feature:

- VstpCdpaGttActScpvalTotal: The number of messages that successfully pass SCPVAL CdPA GTT action.
- VstpCdpaGttActScpvalDiscard: The number of messages discarded by SCPVAL CdPA GTT action.

- VstpCdpaGttActScpvalNotApplied: The number of messages where validation was not applied by SCPVAL CdPA GTT action.
- VstpCgpaGttActScpvalTotal: The number of messages that successfully pass SCPVAL CgPA GTT action.
- VstpCgpaGttActScpvalDiscard: The number of messages discarded by SCPVAL CgPA GTT action.
- VstpCgpaGttActScpvalNotApplied: The number of messages where validation was not applied by SCPVAL CgPA GTT action.

4.2.2.2 Alarms & Events

Following is the list of events supported by SCPVAL Feature:

Table 75 – Alarms for GTT SCPVAL Action Feature

Alarm/Event Name	Type	Description	Raise Condition
GTT Action Failed (70278)	Event	GTT Action Failed	When any one of the GTT Action (i.e. DUPLICATE, FORWARD, TCAP ERROR, SCPVAL) fails and UIMREQD is set to ON.

Limitation

This feature supports the validation only on the following messages coming to the vSTP:

- MO-FSM (MAP version 2 or 3)
- MT-FSM (MAP version 3)

Dependencies

The SCPVAL action has no dependency on any other vSTP operation.

Troubleshooting Steps

The following are the troubleshooting scenarios for SCPVAL action:

- If an incoming MSU successfully passes SCPVAL CdPA GTT action, then VstpCdpaGttActScpvalTotal measurement will be pegged on a per Linkset basis.
- If validation was not applied by SCPVAL CdPA GTT action on an incoming message, VstpCdpaGttActScpvalNotApplied will be pegged on a per Linkset basis.
- If incoming MSU is discarded by SCPVAL CdPA GTT action, then VstpCdpaGttActScpvalDiscard measurement will be pegged on a per Linkset basis.
- If validation was not applied by SCPVAL CgPA GTT action on an incoming message, VstpCgpaGttActScpvalNotApplied will be pegged on a per Linkset basis.
- If an incoming MSU successfully passes SCPVAL CgPA GTT action, then VstpCgpaGttActScpvalTotal measurement will be pegged on a per Linkset basis.
- If incoming MSU is discarded by SCPVAL CgPA GTT action, then VstpCgpaGttActScpvalDiscard measurement will be pegged on a per Linkset basis.
- When anyone of the GTT Action (i.e. DUPLICATE, FORWARD, TCAP ERROR, SCPVAL) fails and UIMREQD is set to ON, then event 70278 GTT Action Failed will be generated. It contains error cause with SCCP and TCAP details, GTT Action set name and linkset ID.

If any of the above statement fails as per given scenarios, then verify configuration.

If issue still exists, then contact Oracle for support.

4.3 MTP BASED GTT

4.3.1 *PURPOSE AND SOLUTION*

Purpose

- Support for MTP based GTT with Screening Action feature in vSTP.
- GTT and GTT Actions were not performed on MTP Routed MSU's prior to implementation of this feature in vSTP.

Solution

- The MTP based GTT with Screening Action feature enhanced vSTP's capability of performing SCCP services on MTP-routed messages.
- This vSTP feature allows the operator to perform GTT and GTT Actions on MTP Routed MSUs similar to existing GTT handling for GT Routed MSU's.

Feature Overview

The MTP based GTT with Screening Action is performed if the service handling results in Fall through to GTT or if **GTT Required** option is **ON** for Service Relayed MSU.

The following system-wide options are used to configure this functionality:

- **MTP Routed GTT**

  The MTP Routed GTT (mtprgtt) option is used for MTP Routed GTT functionality as follows:

  - If option = **OFF**, then GTT shall not be performed on MTP Routed MSUs.
  - If option = **Use MTP Point codes**, then GTT shall be performed on MTP Routed MSU, SCCP Portion shall be updated based on translation entry but MSU shall be sent to Original DPC (and not to translated DPC).
  - If option = **Full GTT**, then GTT shall be performed on MTP Routed MSU, SCCP Portion as well as MTP Portion shall be updated based on translation results.

- **MTP Routed GTT fallback**

  The MTP Routed GTT fallback (mtprgttfallbk) option is used for error handling to be performed in case of GTT failure for MTP routed MSUs. It has the following values:

  - If option = **GTT failure**, then MSU will be discarded with appropriate UIM. UDTS will be sent to originator and measurements shall be pegged as done for GT routed messages.
  - If option = **Fall back to MTP routing**, then MSU (with translation/modification/ routing data from UDR-related service) shall be MTP routed.

The support for the following features is required for the functionality of MTP based GTT:

- SCCP Stop Action: provide a means for the operator to specify SCCP Stop Action in the MTP Screening Rules, to allow the MTP processing to fall through to GTT on non-discarded MSUs.
- XLAT = NONE: provide a means for the operator to specify GTT Translation Type
- = NONE**.**
- GTT SET = DPC: A new GTT set, DPC (with set type dpc) shall be supported. The provisioning and behavior of the DPC Translations shall be same as OPC Translations. However, DPC GTT set cannot be used as secondary optional set (i.e. DPC GTT set cannot be assigned to OPCSN parameter in translation entry). The DPC GTT set type can be searched only when the GTT hierarchy is FLOBR specific.

4.3.2 MEALS

4.3.2.1 Measurements

Table 76 – Measurements

Meas ID	Name	Report Group	Collection Interval	Dimension
21304	VstpRxMSUMtpRoutedSccp	VSTP MTP3 Performance	5 min	Single

4.3.2.2 Alarms & Events

No specific Alarms and Events are generated for MTP based GTT.

Limitation

1. This feature does not implement screening based on SCCP layer parameters. The feature scope is limited to screening based on MTP3 layer parameters.

Dependencies

The MTP based GTT support for vSTP has no dependency on any other vSTP operation.

Troubleshooting Steps

In case of the error scenarios, the measurements specific to MTP based GTT feature are pegged. For information related to MTP based GTT measurements, see MTP Based GTT Alarms and Measurements.

4.4 SFAPP STATEFUL SECURITY

4.4.1 *PURPOSE AND SOLUTION*

Purpose

- Categories of messages that need to be monitored and handled to provide security to home networks from messages coming in from spurious sources with identification information of the subscribers roaming out. The messages coming in for a subscriber, roaming out of the network are in a sequence and to truly validate the veracity of the subscriber, a state information is required. This state information can be about the last message, last location, last activity time.
- Following category of messages has been identified to be protected against in the SS7 networks

Category 3: Outbound roaming MAP messages.

Category 3.1: VLR Check MAP messages

Category 3.2: Time, Location Check messages

The following Category 3 packets are worthy of monitoring and analysis on this basis:

- UpdateLocation
- UpdateGPRSLocation

- PurgeMS
- RegisterSS
- EraseSS5
- ActivateSS5
- DeactivateSS5
- InterrogateSS5
- ProcessUnstructuredSSRequest5
- SendAuthenticationInfo
- RestoreData
- NoteMMEvent
- SendParameters5

Solution

This feature would allow the vSTP to validate the messages coming in for a subscriber roaming out by validating them against the VLR the subscriber was last seen by the HLR. If the HLR provides a validity of the new VLR the vSTP would let the message into the network if not, the message would be handled per configuration (either silent discard or respond with error).

Feature Overview

Stateful Applications (SFAPP) allows vSTP to validate the messages coming in for a subscriber by validating them against the Visitor Location Register (VLR). The last seen details of the subscriber can be fetched from the Home Location Register (HLR). Once the HLR provides a validity of the new VLR, vSTP then allows the message into the network. If the message is not validated, it is handled as per configuration (either silent discard, fallback, or respond with error).

4.4.2 MEALS

4.4.2.1 Measurements

-Table 77 – Measurements

Meas ID	Name	Description	Group	Inter val	Dimension
21702	VstpSfappMsgSuccess	Total number of messages that passed VLR validation.	Vstp SFAPP Performance	5 min	Array
21703	VstpSfappMsgFailed	Total number of messages failed VLR validation	Vstp SFAPP Performance	5 min	Array
21704	VstpSfappMsgError1	Total number of Vstp generated SFAPP messages with validation errors	Vstp SFAPP Performance	5 min	Array
21705	VstpSfappMsgError2	Total number of Vstp generated SFAPP messages with validation errors	Vstp SFAPP Performance	5 min	Array
21706	VstpRxSfappMsg	The total number of messages received to SFAPP.	Vstp SFAPP Performance	5 min	Single

21707	VstpRxSfappMsgDiscard	The number of SFAPP messages that have been received and discarded	Vstp SFAPP Exception	5 min	Single
21708	VstpSfappInternalError	Number of messages discarded due to internal processing error	Vstp SFAPP Exception	5 min	Single
21709	VstpSfappCADecodeFail	Number of SfApp CA response discarded due to decode failed	Vstp SFAPP Exception	5 min	Single
21710	VstpSfappCATimeOut	Number of messages for which CA query to UDR timed out	Vstp SFAPP Exception	5 min	Single
21711	VstpSfappCAAvgProcessTime	Average Sfapp CA query response time from UDR.	Vstp SFAPP Performance	5 min	Single
21712	VstpSfappCAMaxProcessTime	Peak time by CA to send query and receive the response from UDR for Sfapp Messages	Vstp SFAPP Performance	5 min	Single
21713	VstpSfappSubsNotFound	Number of subscriber record not in UDR DB	Vstp SFAPP Exception	5 mn	Single
21714	VstpSfappCATx	Number of DB request sent by vSTP	Vstp SFAPP Performance	5 min	Single
21715	VstpSfappCATxFail	Number of messages discarded by SFAPP because of send fail to CA layer.	Vstp SFAPP Exception	5 min	Single
21716	VstpSfappPduFull	Number of messages discarded when PDU pool is exhausted	Vstp SFAPP Exception	5 min	Single
21717	VstpSfappCAProcesTime	Time required by CA to send query and receive the response from UDR	Vstp SFAPP Performance	5 min	Single
21718	VstpSFAPPStackQueuePeak	The peak VSTP SFAPP Stack Event Queue utilization measured during the collection interval.	VSTP SFAPP Performance	30 min	Arrayed

21719	VstpSFAPPStackQueueAvg	The average VSTP SFAPP Stack Event Queue utilization measured during the collection interval.	VSTP SFAPP Performance	30 min	Arrayed
21720	VstpSFAPPStackQueueFull	The number of ingress SFAPP messages that were discarded because the VSTP SFAPP Stack Event Queue was full.	VSTP SFAPP Exception	30 min	Arrayed
21782	VstpTxSfappMsg	The total number of messages transmitted from SFAPP.	VSTP SFAPP Performance	5 miin	Single
21783	VstpTxSfappMsgPeak	The peak number of messages transmitted from SFAPP	VSTP SFAPP Performance	5 min	Single
21784	VstpTxSfappMsgAvg	The average number of messages transmitted from SFAPP	VSTP SFAPP Performance	5 min	Single

4.4.2.2 Alarms & Events

Following is the list of events/alarms supported by MTP Screening Feature:

Table 78 – Alarms for SFAPP Stateful Security Feature

Alarm/Event Name	**Type**	**Description**	**Raise Condition**	**Clear Condition**	**Throttle sec**	**Instance**	**Severity**
SFAPP Validation Error	Event	When SFAPP decode fails	When SFAPP message decodeing fails		10	None	Info
SFAPP Validation Matching State not found	Event	SFAPP Validation Matching State not found	When SFAPP Validation Matching State not found.		10	None	info
SFAPP Validation Encoding Error	Event	SFAPP Validation Encoding Error.	When Sfapp message encoding fails.		10	None	info

SFAPP Validation Response Timeout Error.	Event	SFAPP Validation Response Timeout Error.	When SFAPP Validation Response Timeout Error.		10	None	info
SFAPP Validation Velocity Chk Failed.	Event	SFAPP Validation Velocity Chk Failed.	When SFAPP Validation Velocity Chk Failed.		10	None	info
SFAPP Validation Failed	Event	SFAPP Validation Failed	When SFAPP message Validation Failed		10	None	info
SFAPP Invalid CC/NDC received	Event	SFAPP Invalid CC/NDC received	When invalid CC/NDC received in VLR of Sfapp message		10	None	info
Updation failed in UDR	Event	Updation failed in UDR	When updation is failed on UDR for IMSI record.		10	None	Info
VSTP SFAPP Stack Event Queue Utilization	Alarm	The percent utilization of the VSTP MP's SFAPP Event Queue is approaching its maximum capacity	When the percent utilization of the VSTP MP's SFAPP Event Queue is approaching its maximum capacity	The percent utilization of the VSTP MP's SFAPP Event Queue comes back to normal	10	None	Major

Troubleshooting Steps

vSTP Sfapp messages will be discarded in following scenarios :

Check whether Sfapp Thread CPU utilization exceeded Congestion Level 2

1. This check is performed at the beginning of message processing cycle and if set vSTP immediately responds with default response

Check whether Sfapp Application operational state is “Unavailable”

1. Check whether Sfapp operational state in VstpSccpAppStatus table is set to “Unavailable”
2. vSTP performs this check before sending the message to UDR and if the state “Unavailable” it sends default response; the query is not sent to UDR anymore
3. VstpSfappCATimeOut meas is pegged in this case

4.5 TDM SUPPORT

4.5.1 *PURPOSE AND SOLUTION*

Purpose

At present, VSTP provides IP connectivity for SS7 network. However, the legacy TDM links are still running on the legacy platform. The replacement of legacy (typically old) systems with VSTP becomes infeasible for transition because of lack of TDM support in VSTP.

Solution

vSTP TDM Support feature provides access to E1/T1 links based ADAX HDC3 PCIe TDM Card using PCIe Pass Through. This solution involves following components :

- TDM Hardware: ADAX HDC3 PCIe card with physical TDM connectivity supporting Virtual IO. This card shall have built-in processor to process the MTP2 layer on hardware itself.
- VSTP MP with MTP NIF functionality: An additional (MTP Network Interworking Function - NIF) layer will be added to existing VSTP MP so that the MTP3 Layer can communicate with the MTP2 layer running on the TDM PCIe Card.
- The MTP2 Adapter (NIF) layer on VSTP MP shall communicate with MTP2 layer using Virtual-IO calls.
- The Host machine shall allow PCI Pass-through Access to the VSTP MP virtual machines.

Feature Overview

The TDM support functionality includes the following components

- **TDM Hardware:** The hardware involves Adax HDC3 PCIe card with physical TDM connectivity supporting Virtual IO. This card contains built-in processor to process the MTP2 layer on hardware itself.

  Adax HDC3 PCIe card supports direct access using PCIe Pass-through. Therefore, a single Adax 4-port or 8-Port HDC3 PCIe card can be accessed only from a single VM at a time.

- **MTP Network Interworking Function (NIF):** An additional MTP NIF layer is added to existing vSTP MP so that the MTP3 Layer can communicate with the MTP2 layer running on the TDM PCIe Card.

  The M3RL layer in vSTP MP VM communicates with the MTP2 layer running on the Adax HDC3 card via the MTP2 Adapter layer.

- **MTP2 Adapter:** The MTP2 Adapter NIF layer on vSTP MP communicates with MTP2 layer using Virtual-IO calls. It uses the libraries and APIs provided by Adax to communicate with Adax HDC3 Card.
- **Host machine:** The Host machine allows PCI Pass-through access to the vSTP MP virtual machines.

4.5.2 MEALS

4.5.2.1 Measurements

Table 79 – Measurements

Meas ID	Name	Report Group	Collection Interval	Dimension
21800	VstpMtp2LnkOutageDuration	VSTP MTP2 Exception	5 min	Arrayed (Link Id)
21804	VstpMtp2LnkAvailableDuration	VSTP MTP2 Performance	5 min	Arrayed (Link Id)

21805	VstpMtp2RxLnkMSUOctets	VSTP MTP2 Performance	5 min	Arrayed (Link Id)
21806	VstpMtp2RxLnkMSUOctetsForGTT	VSTP MTP2 Performance	5 min	Arrayed (Link Id)
21807	VstpMtp2TxLnkMSUOctets	VSTP MTP2 Performance	5 min	Arrayed (Link Id)
21808	VstpMtp2Priority0MsuDiscarded	VSTP MTP2 Exception	5 min	Arrayed (Link Id)
21809	VstpMtp2Priority1MsuDiscarded	VSTP MTP2 Exception	5 min	Arrayed (Link Id)
21810	VstpMtp2Priority2MsuDiscarded	VSTP MTP2 Exception	5 min	Arrayed (Link Id)
21811	VstpMtp2Priority3MsuDiscarded	VSTP MTP2 Exception	5 min	Arrayed (Link Id)
21812	VstpMtp2RxLnkMSU	VSTP MTP2 Performance	5 min	Arrayed (Link Id)
21813	VstpMtp2RxLnkMSUForGTT	VSTP MTP2 Performance	5 min	Arrayed (Link Id)
21814	VstpMtp2TxLnkMSU	VSTP MTP2 Performance	5 min	Arrayed (Link Id)
21816	VstpMtp2LnkMaintUsage	VSTP MTP2 Performance	5 min	Arrayed (Link Id)
21821	VstpMtp2LnkCO	VSTP MTP2 Performance	5 min	Arrayed (Link Id)
21823	VstpMtp2OOSDuration	VSTP MTP2 Exception	5 min	Single
21826	VstpMtp2LnkCumlInhibitDuration	VSTP MTP2 Exception	5 min	Arrayed (Link Id)
21827	VstpMtp2LnkRemoteInhibitDuration	VSTP MTP2 Exception	5 min	Arrayed (Link Id)
21828	VstpMtp2RxLnkMSUError	VSTP MTP2 Exception	5 min	Arrayed (Link Id)
21833	VstpMtp2LnkLocalInhibit	VSTP MTP2 Exception	5 min	Arrayed (Link Id)
21835	VstpMtp2LnkTotalOutage	VSTP MTP2 Exception	5 min	Single
21839	VstpMtp2RxLnkMSUInError	VSTP MTP2 Exception	5 min	Arrayed (Link Id)
21840	VstpMtp2LnkTotalActiveDuration	VSTP MTP2 Exception	5 min	Arrayed (Link Id)

21841	VstpMtp2LnkTotalUnAvailableDuration	VSTP MTP2 Exception	5 min	Single

4.5.2.2 Alarms & Events

Following is the list of events supported by MTP2 Links:

Table 80 – Events for TDM Support Feature

Event Name	**ID**	**Raise Condition**
MTP2 Link admin state change	70220	The MTP2 link administrative state is manually changed from one administrative state to another (e.g. Disabled to Enabled and vice versa)
Failed to send message to TDM driver	70221	This event is generated when sending message to TDM driver fails.
Failed to receive message from TDM driver	70222	This event is generated when read message from TDM driver fails.
MTP2 link operational state changed	70223	This event is generated when MTP2 link operational state is changed
MTP2 link failed	70224	This event is generated when MTP2 link is failed due to Link Out Of Service Message Received from peer or MTP2 Link Stop Request Received
MTP2 Ingress message discarded	70225	This event is generated when MTP2 Ingress message is discarded
MTP2 Egress message discarded	70226	This event is generated when MTP2 Egress message is discarded
Received Remote Out Of Service on MTP2 link	70227	This event is generated when Remote Out Of Service is received from peer on MTP2 link.

Following is the list of alarms supported by MTP2 Links:

Table 81 – Alarms for TDM Support Feature

Alarm ID	**Alarm Name**	**Raise Condition**
70001	Link Down	New Link Added or Link manually Disabled.
70005	Link Unavailable	MTP2 has reported to MTP3 that a link is out of service.
70009	Link Congested	Link Congestion alarm is derived from link buffer utilization.

		Minor (>= 60%), Major (>=80%), Critical (>=90%), % level of link buffer capacity.
70102	MTP3 Ingress Link MSU TPS Crossed	Ingress MTP3 signaling traffic rate is above Minor (>= 60%), Major (>=80%), Critical (>=90%), % level of Max = VstpLinkset table: linkTps
70103	MTP3 Egress Link MSU TPS Crossed	Egress MTP3 signaling traffic rate is above Minor (>= 60%), Major (>=80%), Critical (>=90%), % level of Max = VstpLinkset table: linkTps
70104	MTP3 Ingress Link Management TPS Crossed	Ingress MTP3 SNM rate is above Critical (>=20%), % level of Max = VstpLinkset table: linkTps
70084	VSTP MTP2 Transmission and Retransmission Buffer Utilization	MTP2 Link Buffer Utilization is above Minor (>= 60%), Major (>=80%), Critical (>=95%)

Limitation

- Current implementation doesn't support J1 and ATM interfaces.
- One VSTP MP VM can support only one 4-Port ADAX HDC3 Card.
- Single ADAX HDC3 card cannot be accessed from Multiple VSTP MP VMs.
- The ADAX HDC3 driver and required components are not packaged with Standard DSR ISO in current release. These components and RPMs have to be installed separately.

Dependencies

The TDM support for vSTP has no dependency on any other vSTP operation.

Troubleshooting Steps

The following are the troubleshooting scenarios for TDM support:

- **The E1/T1 links do not align properly**

  Do the following to troubleshoot:

  - Verify that the cable is not faulty.
  - Verify the cable connections.
  - Verify that the Adax HDC3 card configuration (in QCXfile) is as per the Interface Mapping configuration.
  - Ensure that the Adax HDC3 card timing source configuration is correct. In case of SUERM errors, modify the timing source.

- **Frequent toggling of the E1/T1 Links**

  Do the following to troubleshoot:

  - Verify that the point codes associated with the linkset are correct.
  - Verify that the link alignment and SLTM timers are correct.

- **Adax HDC3 Card is not detected on a vSTP MP VM**

  Do the following to troubleshoot:

  - Check that the vSTP MP VM and the Adax HDC3 card are co-located on same host machine.

- Check the Adax HDC3 RPMs.
  The following RPMs are required on vSTP MP VM for configuring Adax HDC3 Card:
- Adax-LiS-2.21.8-1-RedHat-6.10-x86-64bit.rpm
- Adax-hdc-1.79-1-RedHat-6.10-x86-64bit-LiS2.21.8-MAJ234.rpm
- Adax-qcx-1.25-1-Linux-x86-64bit.rpm

Points to Consider

The following points must be considered while configuring TDM:

- The J1 and ATM interfaces are not supported.
- Single vSTP MP VM can support only one 4-Port Adax HDC3 Card.
- An Adax HDC3 card cannot be accessed from Multiple VSTP MP VMs .
- The Adax HDC3 driver components and RPMs needs to be installed separately.

4.6 M3UA CLIENT SUPPORT

4.6.1 *PURPOSE AND SOLUTION*

Purpose

- Initially vSTP can work only as M3UA SGP but with introduction of this feature now vSTP can work as M3UA ASP/AS.
- Support for M3UA Client mode feature in vSTP.
- M3UA client support allow the vSTP to trigger the M3UA connection initiation.

Solution

M3UA client support provide following functionality :

- Configuration of M3UA as client through connections mmi configuration.
- Initiation of ASP State Maintenance messages (ASP-UP, ASP-Active …) .
- Receiving and processing of SS7 Signaling Network Management messages (DAVA,DUNA ,DUPU, DRST, DAUD and SCON). messages.

Feature Overview

The MTP3-User Adaptation (M3UA) Client support allows vSTP to trigger the M3UA connection initiation. For information related to M3UA Protocol, refer to RFC 4666.

The M3UA client support over vSTP enables a user to achieve the following functionalities:

- Initiation of SCTP connection to send INIT message to the server.
- Initiation of ASP state maintenance messages such as, ASP-UP, ASP-Active etc.
- Receiving and processing of SS7 Signaling Network Management messages such as, DAVA, DUNA, DUPU, DRST, DAUD and SCON.
- Receiving and processing of M3UA notify messages (NTFY).
- M3UA peer receiving the DATA message sends an MTP-TRANSFER indication primitive to the upper layer.
- On receiving an MTP-TRANSFER request primitive from an upper layer at an ASP the M3UA layer sends a corresponding DATA message to its M3UA peer.
- The M3UA message distribution function determines the Application Server (AS) by comparing the information in the MTP-TRANSFER request primitive with a provisioned Routing Key.

Message Flow

The following figure shows the message flow for M3UA client server functionality, where, SGP acts as the M3UA server and ASP is the M3UA client:

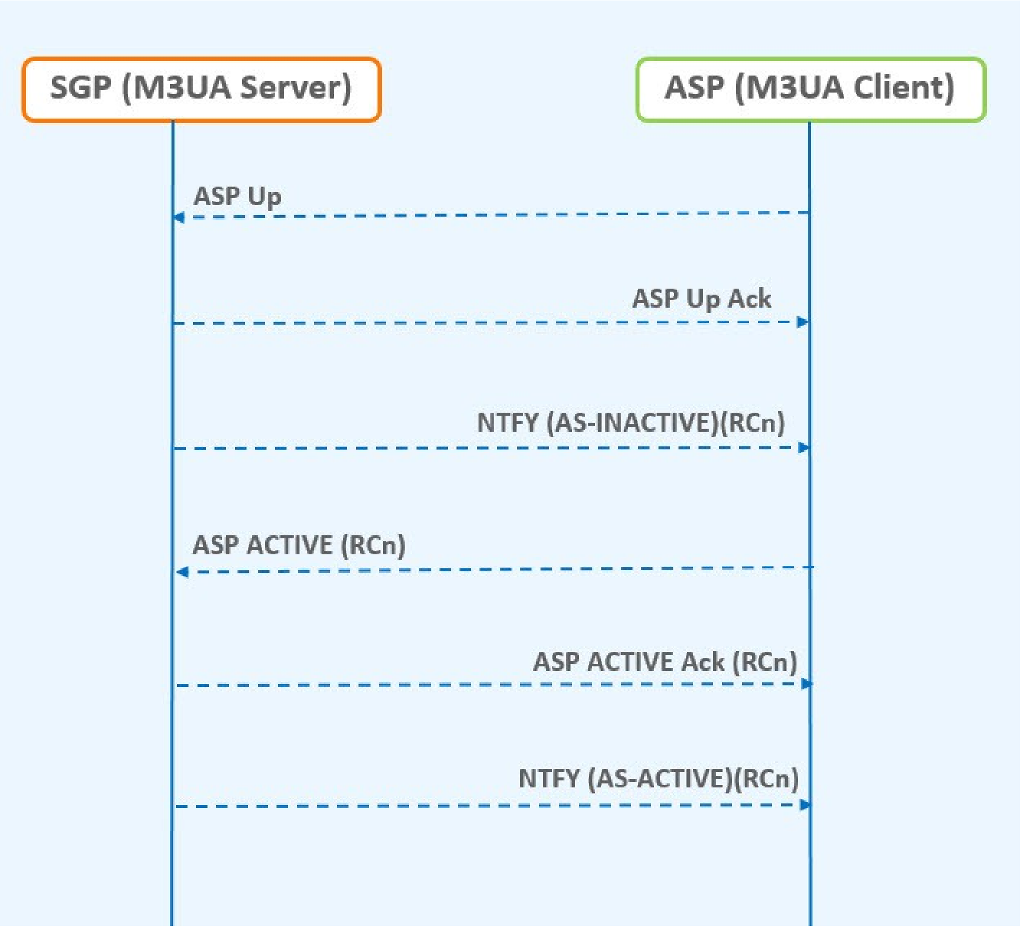


Figure 2-22 Message Flow for ASP - M3UA Client

4.6.2 MEALS

4.6.2.1 Measurements

Table 82 – Measurements

Measurement Name	Dimension	Description	Interval in Mins	Group	Type
VstpTxM3uaDataMsg	Single	M3UA User DATA messages sent by VSTP server	30	Performance	Simple
VstpRxM3uaDataMsg	Single	M3UA User DATA messages received by VSTP server	30	Performance	Simple
VstpTxM3uaDataOctets	Single	M3UA DATA octets sent by the VSTP server	30	Performance	Simple
VstpRxM3uaDataOctets	Single	M3UA DATA octets received by the VSTP server	30	Performance	Simple

vSTPTxAsnOctets	Single	The number of octets sent on an association	30	Performance	Simple
vSTPRxAsnOctets	Single	The number of octets received on an association	30	Performance	Simple
VstpTxASPUp	Single	The number of ASP Up messages sent by the VSTP M3ua client.	30	Performance	Simple
VstpTxASPDown	Single	The number of ASP Down messages sent by the VSTP M3ua client.	30	Performance	Simple
VstpTxHeartbeat	Single	The number of Heartbeat messages sent by the VSTP M3ua client.	30	Performance	Simple
VstpTxASPActive	Single	The number of ASP Active messages sent by the VSTP M3ua client.	30	Performance	Simple
VstpTxASPInactive	Single	The number of ASP Inactive messages sent by the VSTP M3ua client.	30	Performance	Simple
VstpRxDUNA	Single	The number of DUNA messages received by the VSTP M3ua Client.	30	Performance	Simple
VstpRxDAVA	Single	The number of DAVA messages received by the VSTP M3ua Client.	30	Performance	Simple
VstpRxDAVA	Single	The number of DAVA messages received by the VSTP M3ua Client.	30	Performance	Simple
VstpRxDUPU	Single	The number of DUPU messages received by the VSTP M3ua Client.	30	Performance	Simple
VstpRxDRST	Single	The number of DRST messages received by the VSTP M3ua Client.	30	Performance	Simple
VstpTxDAUD	Single	The number of DAUD messages sent by the VSTP M3ua Client.	30	Performance	Simple
VstpRxASPUpAck	Single	The number of ASP Up Ack messages received by the VSTP client.	30	Performance	Simple
VstpRxASPDownAck	Single	The number of ASP Down Ack messages received by the VSTP client.	30	Performance	Simple

VstpRxASPActiveAck	Single	The number of ASP Active Ack messages received by the VSTP client.	30	Performance	Simple
VstpRxASPInactiveAck	Single	The number of ASP Inactive Ack messages received by the VSTP client.	30	Performance	Simple
VstpRxM3uaNotify	Single	The number of M3UA NOTIFY messages recevied by the VSTP client.	30	Performance	Simple

4.6.2.2 Alarms & Events

No new event or alarm added for this feature.

Dependencies

The M3UA Client support for vSTP has no dependency on any other vSTP operation.

Troubleshooting Steps

In case of the error scenarios, the measurements specific to M3UA client support feature are pegged. For information related to M3UA measurements, see M3UA Client Support Alarms and Measurements.

4.7 VSTP IDPR MOSMS

4.7.1 *PURPOSE AND SOLUTION*

Purpose

- Support for Prepaid IDP Query Relay (IDPR) feature in vSTP.
- Support for Mobile Originated Short Message Service (MOSMS) feature in vSTP.

Solution

- Mobile Switching Centers (MSCs) in the network are configured to send IDP prepaid query messages through vSTP, the vSTP intercepts the IDP query based on a set of configurable criteria, performs a number portability (UDR) lookup on the called number, inserts the portability information (Routing Number or HLR Address), and forwards the IDP query to a prepaid SCP for processing. When a respective entry is found in the UDR, any processing is controlled by NPP Service Actions and configuration option provisioning in the IDPROPTS table. The CdPN can be modified with the portability information (Routing Number or HLR address) and the CgPN.
- The Mobile Originated Short Message Service (MOSMS) feature address the number portability requirements of wireless network operators for delivery of Mobile Originated SMS messages. The vSTP MOSMS features apply number portability database lookup to SMS messages for GSM networks, validates subscriber use of the correct Short Message Service Center, and delivers messages to Prepaid Servers if either the Calling Party Number or Called Party Number is associated with a prepaid subscriber.

Feature Overview

The Prepaid IDP Query Relay feature (IDP Relay) provides a mechanism to ensure the correct charging for calls from prepaid subscribers in a portability environment.

IDP Relay processes GT-routed INAP or CAP messages with ITU MTP/SCCP/TCAP parts and Opcode=IDP.

IDP Relay provides functions that handle complex numbering schemes and number conditioning, such as the following examples:

- The Nature of Address Indicator (NAI) could be used in a non-compliant manner (the NAI is set to International and the number format is not international).

- The Local Area Code (LAC) 2- byte field of the Local Area Identification (LAI) information element is used in one of the following ways: – As the Area Code in cases where the AC is needed but not provided in the CdPN – To determine how to format the outgoing CdPN in the IDP query.
- The collect call Escape Codes 90 and 90909 might need to be stripped and re-inserted after the RN.
- The Carrier Selection Point (CSP) can be removed from the incoming number and sometimes re-inserted (as when the LAC is not equal to the AC).
- The RN for the CgPN might be needed when the call is identified as a collect call.
- Service Key selection could vary, and could require a change in the number of bytes present the Service Key.
- Unsegmented XUDT messages might be required.
- Sometimes the RN but not the SP, or the SP but not the RN, or both the RN and SP are required in the outgoing number format.

The Mobile Originated Short Message Service (MO SMS) features address the number portability requirements of wireless network operators for delivery of Mobile Originated SMS messages. The vSTP 5 ISS MO SMS features apply number portability database lookup to SMS messages for GSM networks, validates subscriber use of the correct Short Message Service Center, and delivers messages to Prepaid Servers if either the Calling Party Number or Called Party Number is associated with a prepaid subscriber.

These features include:

- Mobile Originated Based GSM SMS Number Portability (MO-Based GSM SMS NP)
- Portability Check for Mobile Originated SMS (MNP SMS)
- Prepaid Short Message Service Intercept (PPSMS)
- Mobile Originated SMS Additional Subscriber Data (MO SMS ASD)
- Mobile Originated SMS Generic Routing Number (MO SMS GRN)

The MO SMS features are based on the vSTP platform with UDR. Numbering Plan Processor (NPP) is used by the MO SMS features for number conditioning and service logic execution.

4.7.2 MEALS

4.7.2.1 Measurements

Table 83 – Measurements

Meas ID	Name	Report Group	Collection Interval	Dimension
21739	VstpSccpIdprCdpn	Vstp IDPR Performance	30 min	Single
21740	VstpSccpIdprCdpn2	Vstp IDPR Performance	30 min	Single
21741	VstpSccpIdprCdpn3	Vstp IDPR Performance	30 min	Single
21742	VstpSccpIdprCdpn4	Vstp IDPR Performance	30 min	Single
21743	VstpSccpIdprMsrcv	Vstp IDPR Performance	30 min	Single

21744	VstpSccpIdprMsErr	Vstp IDPR Performance	5 min	Single
21745	VstpSccpIdpSkgtart	Vstp IDPR Performance	30 min	Single
21746	VstpSccpIdpSkgtart2	Vstp IDPR Performance	30 min	Single
21747	VstpSccpIdpSkgtart3	Vstp IDPR Performance	30 min	Single
21748	VstpSccpIdpSkgtart4	Vstp IDPR Performance	30 min	Single
21749	VstpSccpIdpInpConn	Vstp IDPR Performance	30 min	Single
21750	VstpSccpIdpInpConn2	Vstp IDPR Performance	30 min	Single
21751	VstpSccpIdpInpConn3	Vstp IDPR Performance	30 min	Single
21752	VstpSccpIdpInpConn4	Vstp IDPR Performance	30 min	Single
21753	VstpSccpIdpInpCont	Vstp IDPR Performance	30 min	Single
21754	VstpSccpIdpInpCont2	Vstp IDPR Performance	30 min	Single
21755	VstpSccpIdpInpCont3	Vstp IDPR Performance	30 min	Single
21756	VstpSccpIdpInpCont4	Vstp IDPR Performance	30 min	Single
21757	VstpSccpIdpAPtyRtd	Vstp IDPR Performance	30 min	Single
21758	VstpSccpIdpAPtyGtt	Vstp IDPR Performance	30 min	Single
21759	VstpSccpIdpSkrtd	Vstp IDPR Performance	30 min	Single
21760	VstpSccpIdpAPtySkr	Vstp IDPR Performance	30 min	Single

21761	VstpSccpIdpInpRlc	Vstp IDPR Performance	30 min	Single
21762	VstpSccpIdpInpRlc2	Vstp IDPR Performance	30 min	Single
21763	VstpSccpIdpInpRlc3	Vstp IDPR Performance	30 min	Single
21764	VstpSccpIdpInpRlc4	Vstp IDPR Performance	30 min	Single
21765	VstpSccpIdpInpRtg	Vstp IDPR Performance	30 min	Single
21766	VstpSccpIdpInpRtg2	Vstp IDPR Performance	30 min	Single
21767	VstpSccpIdpInpRtg3	Vstp IDPR Performance	30 min	Single
21768	VstpSccpIdpInpRtg4	Vstp IDPR Performance	30 min	Single
21769	VstpSccpMsGwsAGt	Vstp IDPR Performance	5 min	Single
21770	VstpSccpIdprMsSucc	Vstp IDPR Performance	30 min	Single
21771	VstpSccpIdprMsFail	Vstp IDPR Performance	5 min	Single
21772	VstpSmsMogRecv	Vstp MOSMS Performance	5 min	Single
21773	VstpSmsMogErr	Vstp MOSMS Performance	5 min	Single
21774	VstpSccpMoSmsSegOk	Vstp MOSMS Performance	30 min	Single
21775	VstpSccpMoSmsSegErr	Vstp MOSMS Performance	30 min	Single
21788	VstpSccpIdpBlkConn	Vstp IDPR Performance	30 min	Single
21789	VstpSccpIdpBlkCont	Vstp IDPR Performance	30 min	Single
21659	vstpGportNonCallRelay	Vstp MNP Exception	5 min	Single
21660	vstpGportNonCallGtt	Vstp MNP Performance	5 min	Single

4.7.2.2 Alarms & Events

Table 84 – Events for vSTP IDPR MOSMS Feature

ID	Event Name	Raise Condition
70310	VstpTooManyDigitDRA	DRA digits have exceeded INAP_MAX_CDPN_DIGITS (32)
70311	VstpIdprCgpnEcdError	IDPR CGPN encoding failed

70312	VstpIdprCdpnEcdError	IDPR CDPN encoding failed
70313	VstpIdprCdpnNppServiceOff	IDPRCDPN(X) NPP SERVICE is OFF
70314	VstpIdprCgpnNppServiceOff	IDPRCGPN NPP SERVICE is OFF
70315	VstpDestAddrDcdFail	DESTINATION ADDRESS DECODING is FAIL
70316	VstpTcapEncFail	TCAP ENCODING is FAIL
70317	VstpOutBoundDigit	OUT OF BOUND DIGIT
70318	VstpSMSMandParamMiss	SMS MANDATORY PARAMETER MISSING
70319	VstpAddrDcdFail	ADDRESS DECODING is FAIL
70320	VstpMnpCdpaMatchHomeSmsc	MNPCDPA MATCHES HOME SMSC

Limitation

Flow control and Congestion control mechanisms are not fully implemented in DSR release 8.4.0.3.0.

4.8 VSTP EIR ENHANCEMENTS

4.8.1 *PURPOSE AND SOLUTION*

Purpose

- Support Equipment Identity Register functionality in vSTP
- Help network operators to reduce GSM mobile handset thefts by providing a mechanism that allows the network operators to prevent stolen or disallowed handsets from accessing the network.

Solution

- vEIR IMSI whitelist expansion: Total 100K IMSI white listing are now supported on vSTP and DEIR (Diameter EIR)
- vEIR Logging enhancements:
  White listed IMEI/IMSI logging is already available. Use the Eir Options MO to enable white listed IMSI/IMEI logging.
    - Instead of IP, vSTP will log the OPC in the logs.
    - Instead of IP, DEIR will log the Origin Host and Origin Realm in the logs
    - OPC/Origin Host and Origin Realm will be logged by default. There will not be any options to enable/disable logging OPC/Origin Host and Origin Realm.

Feature Overview

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

4.8.2 MEALS

4.8.2.1 Measurements

Table 85 – Measurements

Measurement Name	Dimension	Description	Interval in Mins	Group	Type
VstpEirMsgRecv	Single	Number of messages successfully received by EIR application	5	Performance	Simple
VstpEirMsgTrans	Single	Number of messages successfully transmitted by EIR application to SCCP layer	5	Performance	Simple
VstpEirBlackImei	Single	Number of IMEI that are black listed	5	Performance	Simple
VstpEirGrayImei	Single	Number of IMEI that are Gray listed	5	Performance	Simple
VstpEirWhiteImei	Single	Number of IMEI that are White listed	5	Performance	Simple
VstpEirUnkImei	Single	Number of IMEI that are Unknown	5	Performance	Simple
VstpEirImeiNotFound	Single	Number IMEI that are not found in DB	5	Performance	Simple
VstpEirBlackAllwImei	Single	Number of IMEI that are black listed but allowed due to IMSI over-rider	5	Performance	Simple
VstpEirBlackImsiFail	Single	Number of IMEI black listed which has IMSI match failed	5	Exception	Simple
VstpEirImsiRangeSucc	Single	Number of Response sent using IMSi range match. Response can be White, Black, Gray or Unknown.	5	Performance	Simple
VstpEirDiscLssFul	Single	Number of messages discarded due to Lss stack queue was full.	5	Exception	Simple
VstpEirDiscSccpTxFail	Single	Number of messages discarded by Lss because of send fail to SCCP Layer	5	Exception	Simple
VstpEirDiscCATxFail	Single	Number of messages discarded by Lss because of send fail to CA layer.	5	Exception	Simple
VstpEirDiscUnkSsn	Single	Number of messages discarded due to unknown SSN	5	Exception	Simple

VstpEirDiscIMEIMis	Single	Number of messages discarded to missing IMEI	5	Exception	Simple
VstpEirProcessMax	Single	Max time for processing of EIR message received from SCCP layer and sending back the response	5	Performance	Peak
VstpEirProcessAvg	Single	Avg time for processing of EIR message received from SCCP layer and sending back the response	5	Performance	Average
VstpEirProcesTime	Array	Processing time of EIR message received from SCCP layer and sending back the response. (Bucketed at 10ms intv)	5	Performance	Arrayed
VstpEirCAQurProcessMax	Single	Max time for CA query response time to UDR	5	Performance	Peak
VstpEirCAQueProcessAvg	Single	Avg time for CA query response time to UDR	5	Performance	Average
VstpEirCAQueProcesTime	Array	Processing time required for time for CA query response time to UDR. (Bucketed at 10ms intv)	5	Performance	Arrayed
VstpEirQueTimeOut	Single	Number of messages for which CA query to UDR timed out.	5	Exception	Simple
VstpEirDiscCADcdFail	Single	Number of messages discarded by LSS due to decode failed of CA response message	5	Exception	Simple
VstpEirDiscPduFul	Single	Number of messages discarded when PDU pool is exhausted	5	Exception	Simple
VstpEirDiscIntErr	Single	Number of messages discarded due to internal processing error.	5	Exception	Simple
VstpBadMessageFormat	Single	Number of badly formatted messages	5	Exception	Simple
VstpEirDbQueryFailUDRConnDown	Single	Number of EIR DB Queries not initiated due to UDR connectivity down	5	Exception	Simple

4.8.2.2 Alarms & Events

Table 86 – Alarms & Events for vSTP EIR Feature

Alarm/Event Name	Type	Description	Raise Condition	Clear Condition	Throttle Sec	Instance	Additional Information	Severity
EIR Application Status Changed (70068)	Alarm	CA Service unavailable or Congested	When UDR connection is down. When CA service is down or degraded.	When UDR connection is up. CA service is available.	300	None	Reason for degrade status	Critical
TCAP Invalid Parameter or Decode failure (70069)	Event	Failed to decode TCAP parameter	Invalid len in transaction portion Invalid len in dialogue portion Invalid len in component portion No originating transaction ID Invalid transaction ID len Dest transaction ID in Begin No External element No External Object Identifier Not Structured Dialogue No External ASN1-Type No External element No External Object Identifier Not Structured Dialogue No Dialogue Request No Application Context Name No ACN Object Identifier No component portion No Invoke ID	NA	10	None	CdPA PC, SSN and RI CgPA PC, SSN and RI TCAP data	NA

			No operation code Unsupported network type Unsupported operation code					
Message Encode failed (70070)	Event	Failed to encode message	Error in encoding of messages due to incorrect CGPA parameter.	NA	30	None	CdPA PC, SSN and RI CgPA PC, SSN and RI	NA
Missing IMEI (70071)	Alarm	IMEI is missing in the received message	IMEI is missing in the received message	Auto clear after 5 mins	300	None	CdPA PC, SSN and RI	Minor
Invalid IMEI length (70072)	Event	Invalid Length for Map IMEI Parameter	IMEI invalid length	NA	10	None	CdPA PC, SSN and RI CgPA PC, SSN and RI	NA
Unknown Message (70073)	Event	Unsupported TCAP message type	Unsupported TCAP message type	NA	10	None	CdPA PC, SSN and RI CgPA PC, SSN and RI	NA
Logging Error in MP (70078)	Alarm	Log write Error in MP	LogDirCreateError LogFileCreateError LogFileOpenError LogFileWriteError LogLowDiskSpace LogHighEventRate LogMetaFileCreateError LogMetaFileWriteError LogHighEventRate	Logging resumes in MP	86400	None	Cause of Error	Minor
Log fetch Error from SOAM (70077)	Alarm	Eir Log copy from MP to SOAM failure	SOAM fails to copy EIR log from SOAM	SOAM is able to copy the Eir Logs from SOAM	86400	None	Cause of failure	Minor
Lss Stack Event Queue Utilization (70075)	Alarm	The percent utilization of the VSTP MP's LSS Stack Event Queue is approaching	Stack Queue utilization crosses 60/80/95 percent	Stack Queue utilization comes back to 50/70/90 percent	86400	None	NA	Minor

		its maximum capacity						
Logging Stack Event Queue Utilization (70076)	Alarm	The percent utilization of the VSTP MP's Logging Stack Event Queue is approaching its maximum capacity	Stack Queue utilization crosses 60/80/95 percent	Stack Queue utilization comes back to 50/70/90 percent	86400	None	NA	Minor

Limitation

- Assumption is UDR NO’s replication will be in good health always.
- If for any reason replication is down between Active NO and Standby or Spare NO’s for longer duration there can be inconsistency of data between NO’s and can lead to different equipment status for same IMEI number.

5 RELEASE 8.4.0.5.0 FEATURE OAM CHANGES

At the time of upgrade to DSR 8.4.0.5.0 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.

5.1 SLS ROTATION

5.1.1 *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.

5.1.2 MEALS

5.1.2.1 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.

5.1.2.2 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 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.

5.2 SFAPP DYNAMIC LEARNING

5.2.1 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.

5.2.2 MEALS

5.2.2.1 Measurements

Table 87 – 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

5.2.2.2 Alarms & Events

Table 88 – 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.

5.3 TIF SUPPORT

5.3.1 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.

5.3.2 MEALS

5.3.2.1 Measurements

Table 89 – 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

5.3.2.2 Alarms & Events

Table 90 – 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.

5.4 SEGMENTED XUDT

5.4.1 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.

5.4.2 MEALS

5.4.2.1 Measurements

Table 91 – 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 Exception	Simple
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

5.4.2.2 Alarms & Events

Table 92 – 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:

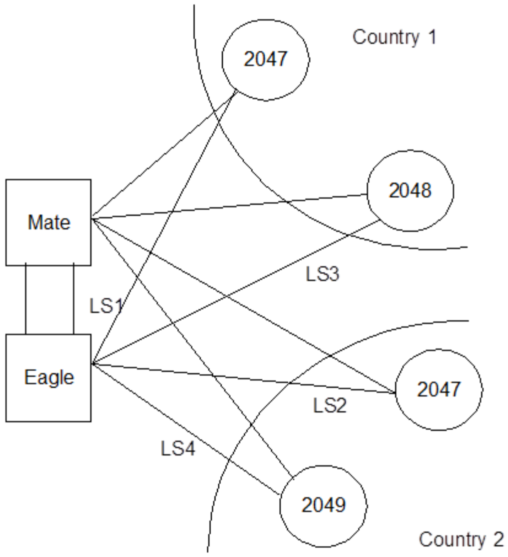
- Segments of the same message received on different vSTP MPs (as result of CO or CB or any other scenario) are not completely supported. The reassembly error procedure will be initiated for such messages.
- Reassembly is performed for only segmented XUDT Class 1 messages. Segmentation functionality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

5.5 DUPLICATE POINT CODE SUPPORT

5.5.1 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.

5.5.2 MEALS

5.5.2.1 Measurements

No measurement changes for Duplicate Point Code.

5.5.2.2 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.

5.6 VSTP IR21 BULK UPLOAD FOR SS7 SECURITY

5.6.1 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.

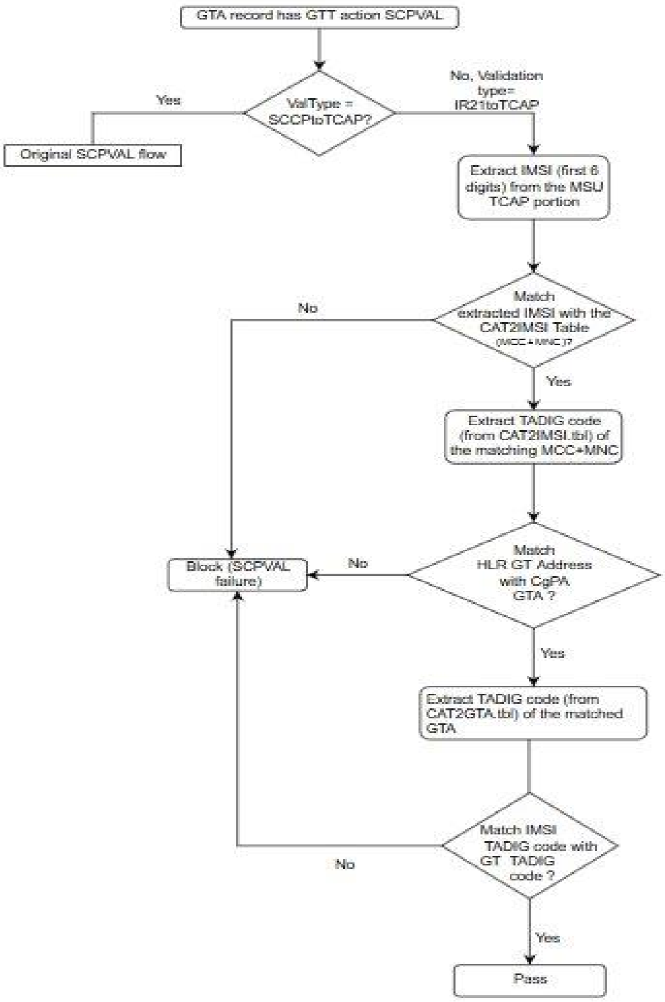
SCPVAL GTT Action on EAGLE shall be enhanced to address SS7 CAT2 security checks. This GTT action will ensure MSU details viz. CGPA and IMSI belongs to same Operator after validating it with the newly generated table.

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:


GTA record has GTT action SCPVAL
Yes
ValType = SCCPtoTCAP?
No, Validation type= IR21toTCAP
Original SCPVAL flow
Extract IMSI (first 6 digits) from the MSU TCAP portion
No
Match extracted IMSI with the CAT2IMSI Table (MCC+MNC)?
Yes
Extract TADIG code (from CAT2IMSI.tbl) of the matching MCC+MNC
Block (SCPVAL failure)
No
Match HLR GT Address with CgPA GTA ?
Yes
Extract TADIG code (from CAT2GTA.tbl) of the matched GTA
No
Match IMSI TADIG code with GT TADIG code ?
Yes
Pass

5.6.2 MEALS

5.6.2.1 Measurements

Table 93 – 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

5.6.2.2 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
provideSubscriberInfo	70
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.

5.7 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

5.7.1 UPGRADE

DSA with UDR in Release 8.4.0.0.5 does not support the upgrade.

5.7.2 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.

6 MEAL INSERTS

This section will summarize the changes to Alarms, Measurements, KPIs and MIBs. In the following inserts pertain to DSR Release 8.4 MEAL snapshot and deltas to earlier releases 8.0.0, 8.1.0 and 8.2.1 and 8.3

- 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

6.1 DSR/SDS 8.4.0.5.0 MEAL SNAPSHOT

MEAL_dsr-8.4.0.5.0-88.9.1.xlsx

MEAL_sds-8.4.0.5.0-88.9.1.xlsx

`

6.1.1 *MEAL DELTA BETWEEN 8.4.0.0.0 AND 8.4.0.5.0*

MEAL_dsr-8.4.0.0.0-84.15.0-dsr-8.4.0.5.0

MEAL_sds-8.4.0.0.0-84.15.0-sds-8.4.0.5.0

6.1.2 *MEAL DELTA BETWEEN 8.4.0.3.0 AND 8.4.0.5.0*

MEAL_dsr-8.4.0.3.0-85.17.0-dsr-8.4.0.5.0

MEAL_sds-8.4.0.3.0-85.17.0-sds-8.4.0.5.0

6.2 DSR/SDS 8.4.0.3.0 MEAL SNAPSHOT

MEAL_dsr-8.4.0.3.0-85.17.0.xlsx

6.2.1 *MEAL DELTA BETWEEN 7.0.1.0.0 AND 8.4.0.3.0*

MEAL_dsr-7.0.1.0.0-70.28.0-dsr-8.4.0.3.0

6.3 DSR/SDS 8.4.0.0.0 MEAL SNAPSHOT

MEAL_dsr-8.4.0.0.0-84.15.0.xlsx

MEAL_sds-8.4.0.0.0-84.15.0.xlsx

6.3.1 *MEAL DELTA BETWEEN 8.0.0.0.0 AND 8.4.0.0.0*

MEAL_dsr-8.0.0.0.0-80.25.0-dsr-8.4.0.0.0

MEAL_sds-8.0.0.0.0-80.25.0-sds-8.4.0.0.0

6.3.2 *MEAL DELTA BETWEEN 8.1.0.0.0 AND 8.4.0.0.0*

MEAL_dsr-8.1.0.0.0-81.20.0-dsr-8.4.0.0.0

MEAL_sds-8.1.0.0.0-81.20.0-sds-8.4.0.0.0

6.3.3 *MEAL DELTA BETWEEN 8.2.1.0.0 AND 8.4.0.0.0*

MEAL_dsr-8.2.1.0.0_82.19.0-dsr-8.4.0.0.0

MEAL_sds-8.2.1.0.0-82.17.0-sds-8.4.0.0.0

6.3.4 *MEAL DELTA BETWEEN 8.3.0.0.0 AND 8.4.0.0.0*

MEAL_dsr-8.3.0.0.0-83.15.0-dsr-8.4.0.0.0

MEAL_sds-8.3.0.0.0-83.15.0-sds-8.4.0.0.0

7 REFERENCE LIST

The DSR 8.4 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)