Oracle® COMMUNICATIONS

Diameter Signaling Router
DSR Network Impact Report

Release 8.0

E69037-01
March 2017

Oracle Diameter Signaling Router DSR Network Impact Report, Release 8.0

TABLE OF CONTENTS

List of Terms

ASGU ..... Automated Server Group Upgrade
AVP ..... Attribute Value Pair
CLI..... Command Line Interface
GUI..... Graphical User Interface
HSS..... Home Subscriber Server
iLO..... Integrated Lights Out
IMI..... Internal Management Interface
IOT ..... Interoperability Tests
KPI..... Key Performance Indicator
LTE..... Long Term Evolution
MEAL..... Measurements, Events, Alarms, and Logging
MME ..... Mobility Management Entity
MP ..... Message Processor
MPS..... Messages per Second
NE..... Network Element
NMS ..... Network Management System
OAM..... Operations, Administration, Maintenance
OAM&P ..... Operations, Administration, Maintenance, and Provisioning
PDRA ..... Policy Diameter Relay Agent
PCRF ..... DSR Control and Charging Rules Function
PCIMC..... Per Connection Ingress Message Control
PDU ..... Protocol Data Unit
PM&C ..... Platform, Management, and Control
PS..... Priority Service (NGN-PS)
ROS ..... Routing Option Set
TPD ..... ORACLE Platform Distribution
VIP..... Virtual IP Address
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 Product Compatibility

DSR 8.0 is compatible with IDIH 6.0, 7.0, 7.1, 7.2, and 8.0
DSR 8.0 is compatible with SDS 5.0, 7.1, 7.2, and 8.0
DSR 8.0 is compatible with Platform 7.4

1.3 Disclaimers

This document summarizes Release 8.0 new and enhancement features as compared to Release 7.3, and the operations impacts of these features, at a high level. The Feature Requirements (FRS) documents remain the defining source for the expected behavior of these features.

Note: Feature implementations may change slightly during product test.

2. Overview of DSR 8.0 Features

This section provides an overview of the DSR 8.0 release features that may impact OAM interfaces and activities.

For a list of all features, please see Release Notes for DSR 8.0 found at the following link:

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

2.1 Enhancements to DSR 8.0 Functionality by Category

Note: For information on upgrade planning and required steps before upgrade, please refer to the DSR 8.0 Software Upgrade Guide on the public Oracle Documentation Site:

Docs.oracle.com → Industries → Oracle Communications documentation → Diameter Signaling Router → Release 8.0.

Table 1 DSR 8.0 New Features/Enhancements

DSR 8.0 Feature/Enhancement Name
Diameter Custom Application (DCA)
Machine-to-Machine Interface (MMI)
Automated Site Upgrade (ASU)
Oracle VM Cloud Support
Firewall Feature
Independent SBR DB Support for DCA
16 Signaling VLAN Support & VE-DSR Automated VM Creation
FABR and RBAR Enhancements

DSR 8.0 Feature/Enhancement Name
IP Address of the Connection in the SCTP Connection Impaired Trap
Listen Port Updates for Peer Node
Mediation Support for 2000 Counters
Multi Server Export
Nested Routing and Screening
PCRF Pooling Modes
SDS Provisioning Log Export
SDS Connection System ID Field Enhancements
Supporting More than 20 Routing Option Sets
Excessive Request Reroute Alarm
NetBackup 7.7

2.2 Diameter Custom Application (DCA) Framework

This feature enables R&D teams both inside and outside Oracle to build applications that can run on top of the DSR.

Name	Description	Scope
PR 19689230 Diameter Custom Applications Framework	This feature defines an application development for developers to build applications that will run & interface with the DSR in a manner similar to native DSR applications.	Enhancement Request

2.3 MMI

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

Name	Description	Scope
PR 21113457 Machine to Machine Interface	This feature provides an MMI (Machine to Machine Interface) to the DSR product to support all operations needed to manage and configure DSR system. Implements a RESTful MMI interface to the DSR product to expose supported operations on the DSR object model.	GUI

2.4 Automated Site Upgrade

A single button selection will initiate the upgrade of an entire DSR site.

Name	Description	Scope
PR 22169766 Automated Site Upgrade	Automated Site Upgrade is an enhancement in which an entire DSR site upgrade can be initiated with just a few initial selections. For the purpose of this feature, a topological site (TSite) is defined as a SOAM server group plus all subtending servers of that server group, regardless of physical location. To demonstrate this definition, the figure in the below section 3.3.1.1 shows two physical locations, labeled “Site 1” and “Site 2”. Each site contains a SOAM server group and an MP server group. Each SOAM server group has a spare SOAM that, although physically located at the other site, is a member of the site that owns the server group. With Site Upgrade, SOA-sp will be upgraded with the Site 1 SOA server group, and SOB-sp will be upgraded with the Site 2 SOB server group. The MP server groups will be upgraded in the same maintenance window as their respective TSite SOAMs. Auto Site Upgrade will manage: preparing the Server for upgrade, upgrading the Server to the selected ISO, sequencing of remaining Servers while maintaining the required Server redundancy	Enhancement Request

2.5 Oracle VM Cloud Support

DSR will support deployment via OVM-S hypervisor..

Name	Description	Scope
PR 19107463 Oracle VM Cloud Support	This feature design to productize the ability of the DSR to be cloud deployable	Enhancement Request

2.6 Firewall Feature

The DSR firewall feature supports dynamic management and/or automation of Linux firewall rules on the solution servers.

Name	Description	Scope
PR 20834837 DSR Diameter Signaling Firewall	This feature allows users to restrict traffic on the signaling network to expected Diameter traffic in accordance with the configured Diameter peers.	Enhancement Request

2.7 Independent SBR DB Support for DCA

The Independent SBR (I-SBR) provides a common database framework to host database solutions for various applications including DSR native applications developed by Oracle and applications developed by third party developers.

Name	Description	Scope
PR 19689230 & PR 21960600 Custom application development infrastructure & Independent SBR infrastructure for DCA	This feature introduced a common application development environment to enable development teams inside and outside Oracle to develop applications on DSR via provided APIs and service enablers with fast development cycles. As part of the common application development environment, the Independent SBR (I-SBR) was designed to provide generic database services to a variety of native and custom applications. Universal-SBR is a database solution on top of the I-SBR infrastructure used by DCA applications and/or native applications	Enhancement Request

2.8 16 Signaling VLAN Support and VE-DSR Automated VM Creation

The number of supported DSR signaling vlan's is increasing from 4 to 16 for this release. The VE-DSR automated VM creation feature will reduce errors and the time necessary to deploy VE-DSR systems.

Name	Description	Scope
PR 20570039 Support for 16 Signaling VLANs & PR 22925356 VE-DSR Automated VM creation	This features introduces automated guest Creation in the VE-DSR environment	Enhancement Request

2.9 FABR and RBAR Enhancements

FABR & RBAR support for extracting IMSI and MSISDN from User-Identifier grouped AVP

3GPP rel 13 has introduced a couple of new Diameter interfaces: S6m/S6n.. These interfaces carry the IMSI and MSISDN within a newly defined grouped AVP called "User-Identifier" AVP. Within the User-Identifier AVP, the IMSI itself is contained within the "user-name" AVP and the MSISDN is contained within the "MSISDN" AVP. The user-identifier AVP is defined in 29.336 (rel 13).

Support for decoding MSISDN from User-Name AVP in FABR & RBAR

The MSISDN can appear in any of the following formats in the user Name AVP.

```
19195551212
19195551212@abc.com  (there is no sip: in front)
Sip:19195551212@abc.com
Tel:19195551212
```

FABR & RBAR will be enhanced to be able to decode MSISDN when any of the above formats are used.

Support for MSISDN AVP at the base level in FABR & RBAR

Prior to DSR 8.0 FABR & RBAR supports extracting the MSISDN from the MSISDN AVP if it is present under the User-Identity Grouped AVP but does not support extracting the MSISDN if it is present at the base level in the message. FABR & RBAR will be enhanced to supported extraction of MSISDN from the MSISDN AVP when present at the base level in the message.

Name	Description	Scope
PR 22749119 RBAR support for extracting IMSI and MSISDN from User-Identifier grouped AVP PR 22749126 FABR support for extracting IMSI and MSISDN from User-Identifier grouped AVP PR 20293128 Support for MSISDN AVP at the base level in RBAR PR 20293129 Support for MSISDN AVP at the base level in FABR PR 19113206 - [236698] Support for Decoding MSISDN from User Name AVP in RBAR 19113207 - [236699] Support for Decoding MSISDN from User Name AVP in FABR	FABR & RBAR enhancements 4 new Primary AVP and Routing Entity combinations	GUI & Enhancement Request

2.10 IP Address of the Connection in the SCTP Connection Impaired Trap

Name	Description	Scope
PR 22522359 Availability of the IP address in the SCTP Connection Impaired trap	Prior to DSR 8.0, minor alarm 22103 'SCTP Connection Impaired' did not contain the ip address associated with the connection. This information will be included from DSR 8.0 onward.	Enhancement Request

2.11 Listen Port Updates for Peer Node

Provisioning screens modified to no longer require the user to specify a listening port for Peer Nodes/Connections when provisioning the DSR as "Responder".

Name	Description	Scope
PR 19090512 listen port updates for peer node	This feature allows configuration of Peer Nodes without Listen Ports -Allowed when associated Connections are in Responder mode only -This is not allowed for Initiator and Initiator & Responder mode	GUI

2.12 Mediation Support for 2000 Counters

Name	Description	Scope
PR 23594176 Increase counters supported in mediation to 2000	The mediation framework in DSR currently supports 200 counters that can be used for measurements based upon message content. This limit will be increased to 2000. In addition, the number of rules supported in each rule set (or for each rule template) will be increased from 250 to 2000 to support the inclusion of potentially all 2000 counters within the rule set or template. Due to performance impacts there is a necessary constraint which limits the total number of rules across all rule sets combined to not exceed 3750.	Enhancement Request

2.13 Multi Server Export

Name	Description	Scope
PR 20354454 Multiple Export Server Destinations	The DSR currently supports the configuration of one export server per NE that can be used as the target for automatic export of reports, backup, etc. This feature will add support for up to 5 target servers per NE that can be used to support sending different types of data files.	Enhancement Request

2.14 Nested Routing and Screening

Name	Description	Scope
PR 23147209 Nested Routing and Screening	This feature improves the flexibility of ART configuration by allowing the action component of ART rules to additionally reference an ART or PRT. The action component of PRT rules can now also reference a PRT. This additional flexibility reduces overall configuration complexity and improves DSR operating efficiency by simplifying processing required for message route selection.	Enhancement Request

2.15 PCRF Pooling Modes

In short, customers currently running DSR 6.0 or 7.0 who have pooling disabled due to AF/APN issue will have to :

- Apply a mediation work around to include the APN at the ingress leg of Rx message processing and then remove it at the egress leg
- Enable PCRF Pooling
- Allow the Binding Migration to complete
- Upgrade to DSR 8.0 or later (i.e. upgrade to a release having the Pooling Modes feature)
- Manually Switch to “Single Pool Mode” (Network-Wide OAM Configuration)
- Remove the mediation workaround

Name	Description	Scope
PR 23264107 Behavior of PDRA is changed once after enabled PCRF Pooling	This feature enhances the pre-existing PCRF Pooling feature to allow the choice of operating with either a single PCRF pool or to instead use multiple PCRF pools. Operators who would like the DSR to determine PCRF correlation based upon IMSI instead of IMSI+APN can now select the use of single pool mode.	Enhancement Request

2.16 SDS Provisioning Log Export

Name	Description	Scope
PR 19727450 Provisioning Log Export via either APDE or syslog	This feature provides the ability to export the SDS provisioning log to a remote server other than remote servers provided by the DSR APDE (Automatic Performance Data Export).	Enhancement Request

2.17 SDS Connection System ID Field Enhancements

Name	Description	Scope
PR 22185058 SDS Connection System ID Field Enhancements	Prior to this release, the connection System ID field within the SDS Provisioning GUI supported only 8 characters. Since actual connection endpoints are often expressed in terms of DNS FQDN format this 8 character limitation can result in overly truncated and ambiguous connection naming. This release addresses this issue by supporting 1-256 alphanumeric characters within the connection System ID field.	GUI & Enhancement Request

2.18 Supporting More Than 20 Routing Option Sets

Name	Description	Scope
PR 21067704 Supporting more than 20 Routing Option Sets	This feature will increase the number of supported Routing Option Sets from 20 to 50.	Enhancement Request

2.19 Excessive Request Reroute Alarm

Name	Description	Scope
PR 20323447 Excessive Request Re-routing Alarm	This feature introduces as new alarm indicating excessive Request Re-routing. This alarm is raised when the (current average # of reroutes due to Answer timeout + current average # of reroutes due to Answer response) exceeds a configurable threshold. This threshold is expressed as a percentage of the current average # of requests being processed by the DA-MP.	Enhancement Request

2.20 NetBackup 7.7

Name	Description	Scope
PR 24499683 NetBackup 7.7 Support	NetBackup upgrade requires 5GB. This feature is to address fresh installs and to increase dnetbackup_lv to 5GB.	Bug fix

2.21 Hardware Changes

2.21.1 Hardware Supported

Hardware	Comment
HP BL460c Gen8, Gen8_v2	c-Class
HP BL460c Gen9, Gen9_v2	c-Class
HP DL360/380 Gen8, Gen8_v2	Rack Mount Server
HP DL380 Gen9, Gen9_v2	Rack Mount Server
Oracle Server X5-2	Rack Mount Server
Netra X5-2	Rack Mount Server
HP 6125XLG, 6125G, 6120XG	Enclosure Switch

Hardware	Comment
Cisco 3020	Enclosure Switch
Cisco 4948E-F	Rack Switch
Cisco 4948E	Rack Switch

Note: Gen9 and Gen 8 v2 hardware (with upgraded processors) are also supported, when purchased by a customer.

Note Mixed Sun/HP deployments are not generally supported.

2.21.2 Hardware Upgrade

Due to the enhanced processing capabilities and requirements of DSR Release 8.0, HP Gen6 and Gen7 hardware are NOT supported. All Gen6 and Gen7 servers must be replaced with supported hardware before upgrading to release 8.0. Deployment of certain Optional features may require additional hardware.

2.22 Software Changes

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

Component	Release
TPD 64 Bit	7.4.0.0.0-88.37.0
COMCOL	7.3.0.36.0-13500
PM&C	6.4.0.0.0-64.8.0
TVOE	3.4.0.0.0-88.37.0
AppWorks	7.2.0-72.58.0
Exgs	8.0.0-80.25.0
HP Firmware FUP	2.2.10 (Minimum[1])
Oracle Firmware	3.1.7 (Minimum[2])

2.22.1 DSR Release 8.0

DSR Release 8.0 inherits all functionality from DSR 7.4.

Component	Release
DSR Release	8.0

DSR 8.0 is compatible with Platform 7.4.

2.22.2 iDIH 8.0

Component	Release
IDH Release	8.0

DSR 8.0 is compatible with IDIH 7.0, 7.1, 7.2, 7.3 and 7.4.

1 This represents the minimum release of the Tekelec HP FUP 2.2.x series to support all content in the Platform 7.3 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 7.3 release. It is recommended that the latest firmware release always be used in order to address known security issues.

2.22.3 SDS 8.0

Component	Release
SDS Release	8.0

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

2.23 Firmware Changes

Firmware release guidance is provided via DSR 8.0 Release Notice which can be found at the following link:

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

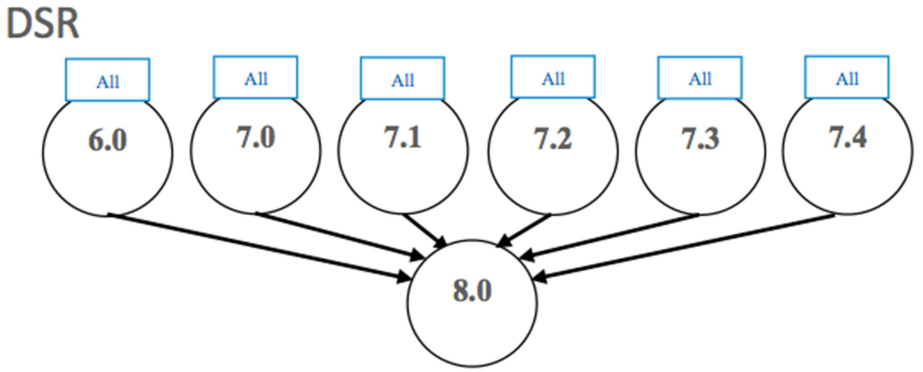
and then navigating to the Release 8.0.x link.

2.24 Upgrade Overview

This section provides an overview of the Upgrade activities for Release 8.0.

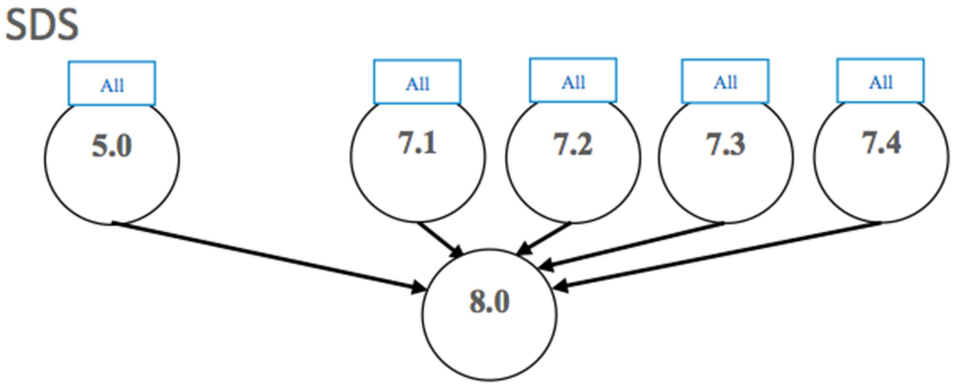
2.24.1 Upgrade Path

The supported upgrade paths for DSR 8.0 are:



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

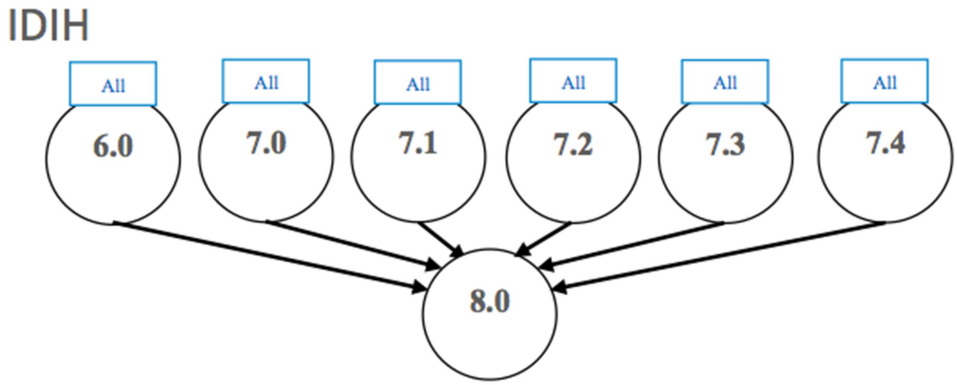
The supported upgrade paths for SDS 8.0 are:



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

Recommendation is to upgrade SDS prior to DSR upgrades. 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.

The supported upgrade paths for iDIH 8.0 are:



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

2.24.2 Upgrade Execution

The procedures for site upgrades have been significantly modified for DSR 8.0 to emphasize parallel upgrades of C-level server groups (DA-MP's, IPFE's, SS7-MP's, and SBR's). Additionally, there are separate procedures described to support either a manual or automated approach to upgrading any particular server group. The use of automated server group upgrade for DA-MP server groups should be carefully considered regarding potential negative traffic impacts. If there are any traffic flows which are limited to a sub-set of DA-MP's then it is recommended to use the manual upgrade procedures.

Previous DSR releases would not allow use of SG upgrade if any server within the SG has already been upgraded. This restriction no longer applies. It is possible to initiate SG or Site upgrade on a partially upgraded SG or site.

2.24.3 Active/Standby DA-MP Redundancy Model Supported

Active/Standby DA-MP server architecture (1+1) continues to be supported in DSR 8.0.

Migration to Multi-active (N+0) DA-MP server architecture is recommended for all customers, and required for activating PDRA functionality.

2.25 Migration of DSR Data

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

3. Feature OAM Changes

At the time of upgrade to DSR 8.0, 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 include: User Interfaces (NO GUI, SO GUI), Measurements Reports, Alarms, and KPIs.

Note: This section covers OAM changes that will be visible after upgrade to the 8.0 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 Diameter Custom Application (DCA)

3.1.1 Description

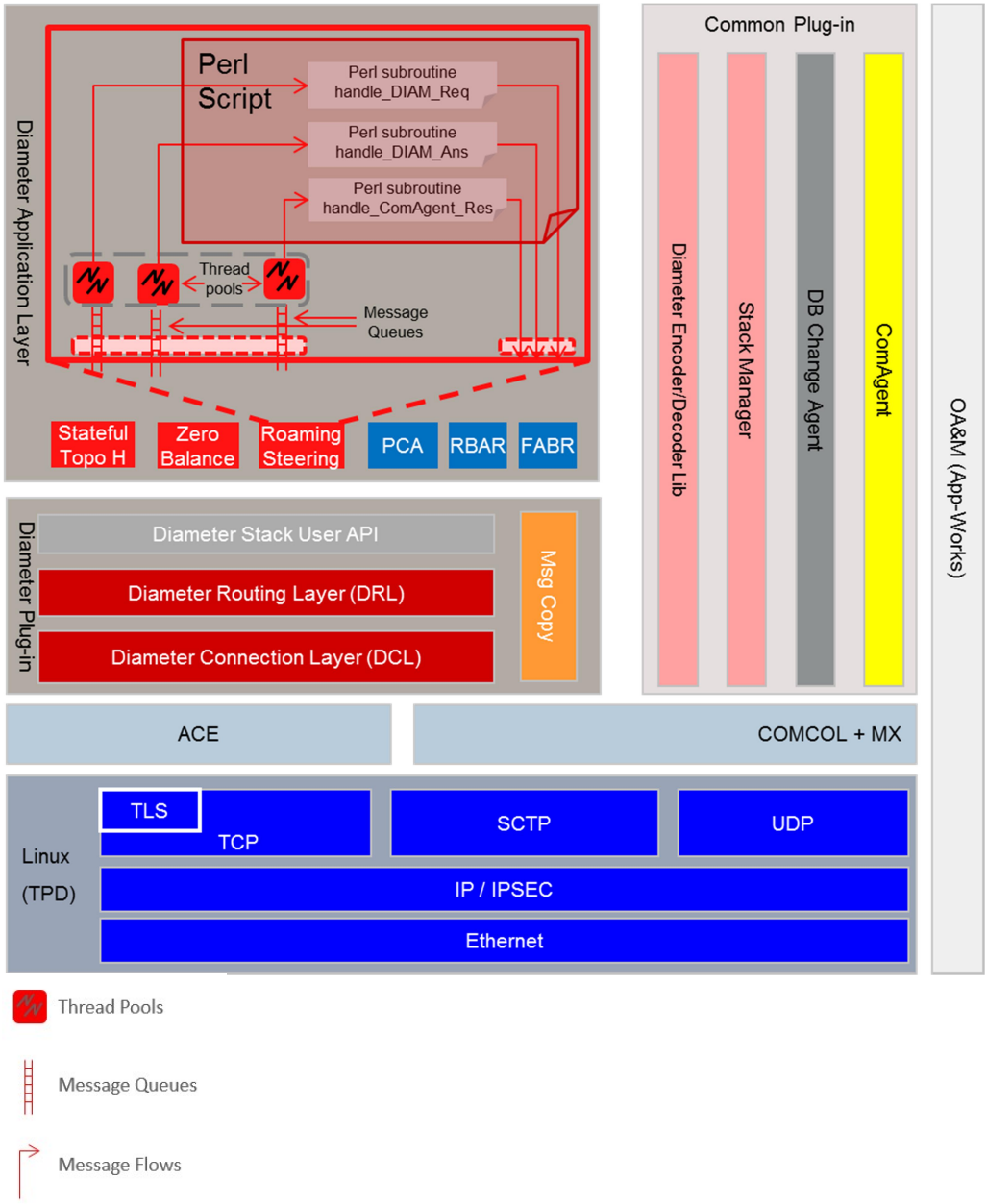
- The DCA framework consists of APIs and services that will allow developers to create applications on the DSR.
- There can be multiple versions of each Diameter Custom Application in various states (Archived, Production, Trial, and Development).
- Each of the versions of the Diameter Custom Application will include their own copy of the business logic, database schema and NO & SO level configuration data.
- The framework supports the ability to export and import Diameter Custom Applications including schema and configuration data from the NO and SO.
- DCA framework will support iDIH.
- DCA framework will support backup and restore of application logic and schema
- DCA framework will support backup and restore of application configuration data at the NO and SO.
- The framework facilitates activation/de-activation of Diameter Customer Applications.
- The framework will ensure that Diameter Custom Applications will not be allowed to consume resources beyond what they are allocated.

Feature – Data Model

The DCA Framework introduces new NO managed objects:

Managed Object	Description
Configuration	Allows configuring DCA Framework parameters
Custom MEALs	Allows definition of all custom defined measurements & events. Read-only on SO.
General Options	Enables specifying the Perl Subroutine for Diameter Request & Answer.
System Options (SOAM Only)	Enables the configuration of the DCA App parameters that are relevant to the operational status “unavailable”, resources exhaustion, run-time errors, & Realm/FQDN that are placed in Answer message generated by the DCA
Trial MPs	Allows specifying which MPs will run the trial version of an application.
Application Control	Allows insert, deletion & listing of application versions, copying and modifying an existing app version, importing/exporting of an app & provisioned data, allows access to the app version configuration tables, access to flowchart and Changing the status of an application version.
SBR Database Name Mapping	Allows viewing and configuring the mapping between U-SBR DB logical names (as used in perl script) and U-SBR DB physical names

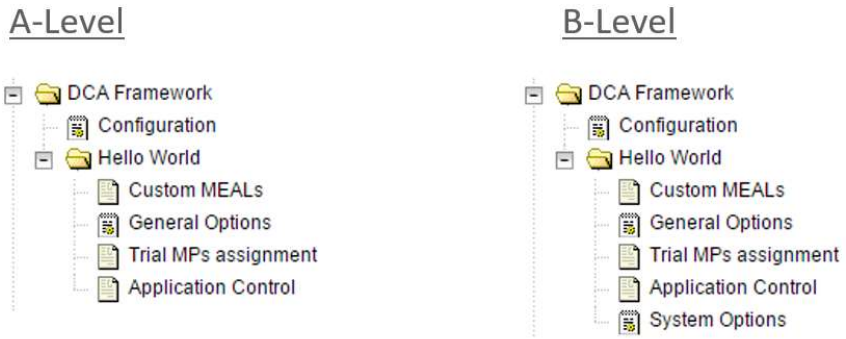
3.1.2 Architecture



3.1.3 Activating a New DCA Application

- User provides an Application short name and long name
- New Subfolder (using long name) is added under DCA Framework folder
- Application short name (DCA_<short name>) becomes available to the list of Applications that ART rules can select
- Application is Operationally Disabled/Shutdown

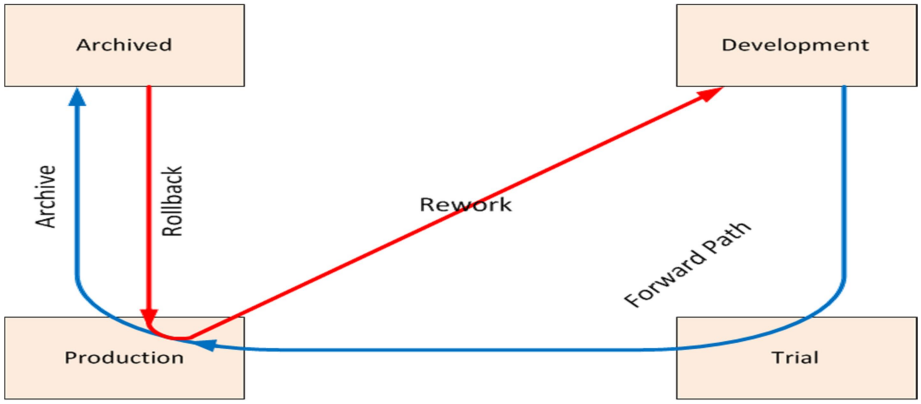
A-level versus B-Level Menu Items



System Options defines behavior when a custom application is unavailable, degraded, overloaded, etc.

DCA App Lifecycle

The DCA Framework allows you to manage the state of the DCA apps between four states: Development, Trial, Production and Archived. By placing different versions of an Application in various states, developers can bring a system to a previous state with minimum service interruption.

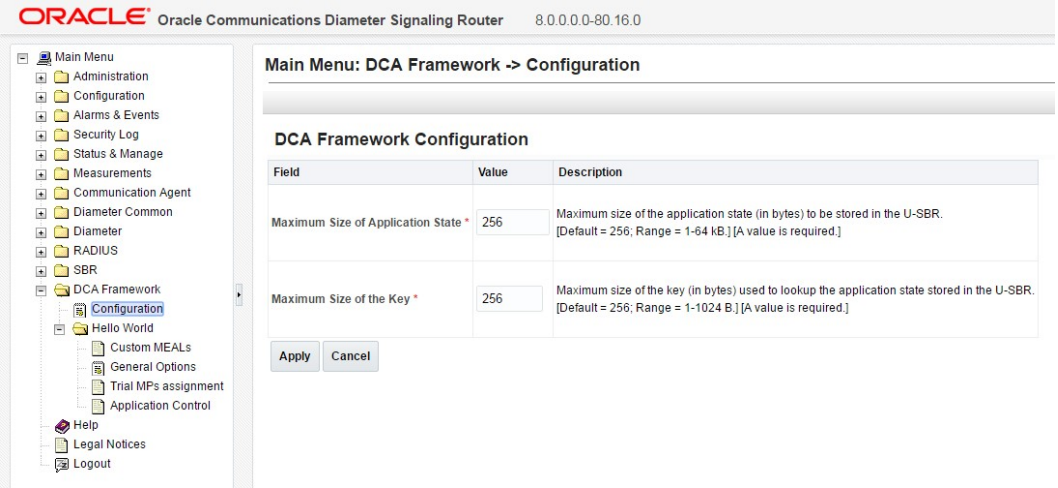


3.1.4 DCA GUI

DCA Framework: Configuration

Once the DCA Framework has been activated a single LHM option will be available, Configuration.

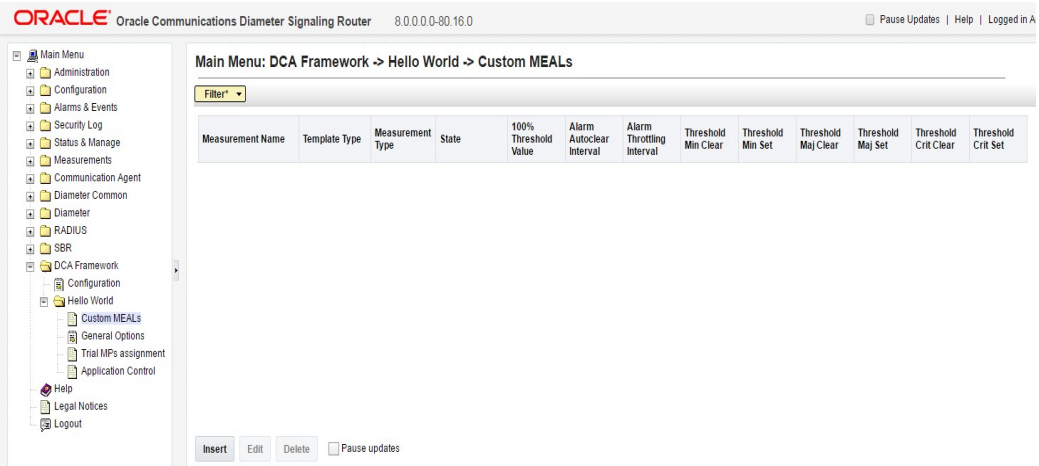
The below configuration screen has only 2 options and both are related to SBR. Max Size of app state & size of the key



Custom MEALs

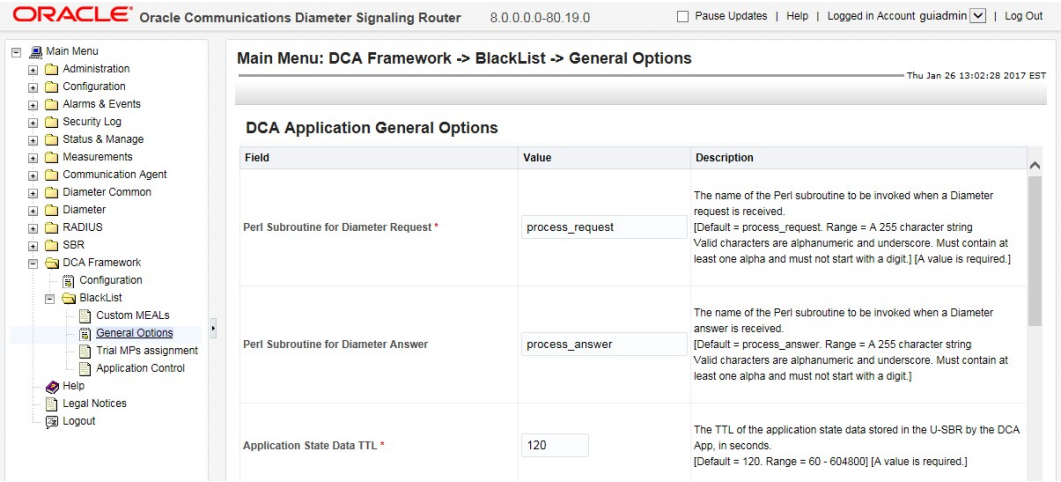
After our Blacklist application has been activated from the NO CLI, it will appear with its own sub menu the given short name under the "DCA Framework"

The first menu item is Custom MEALs…. Here we can create new Custom MEAL templates to be used in our App.



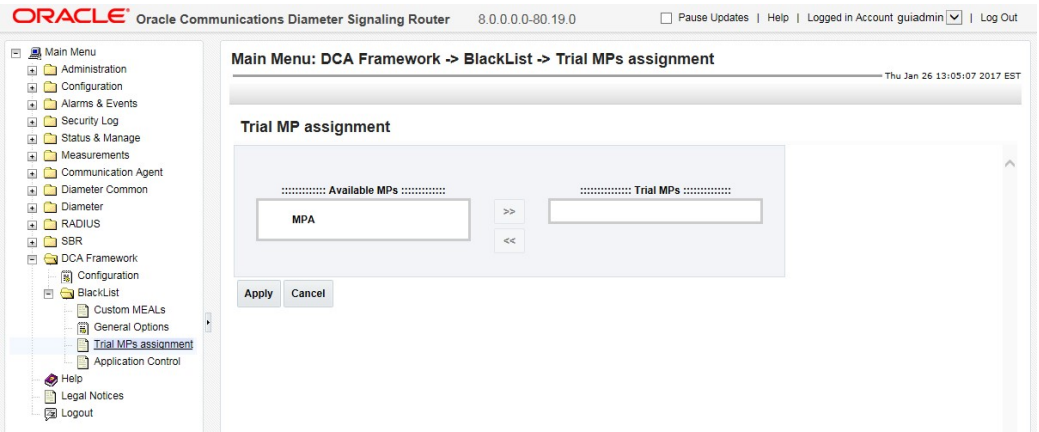
General Options

The General Options screen allows users to specify the name of the subroutines for handling Diameter Request and Application

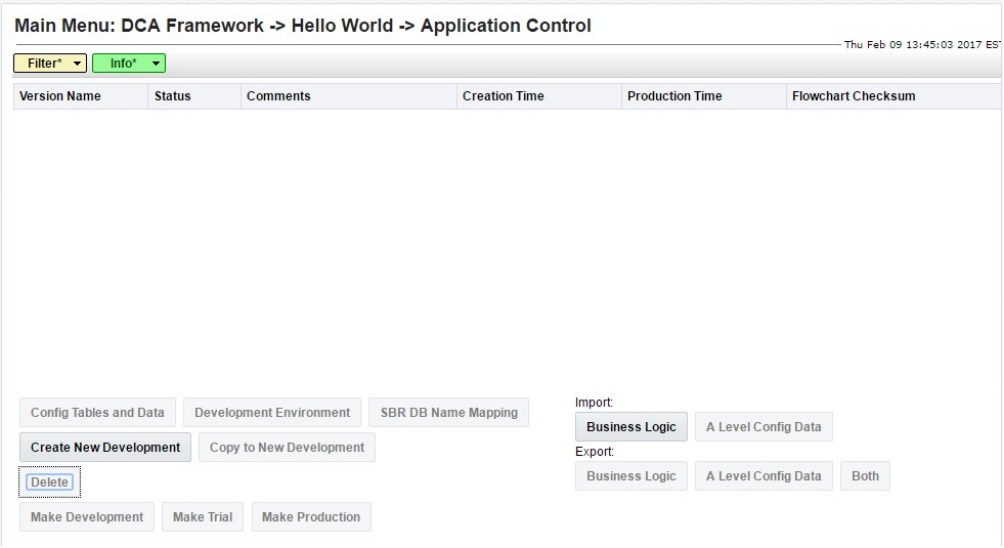


Trial MPs Assignment

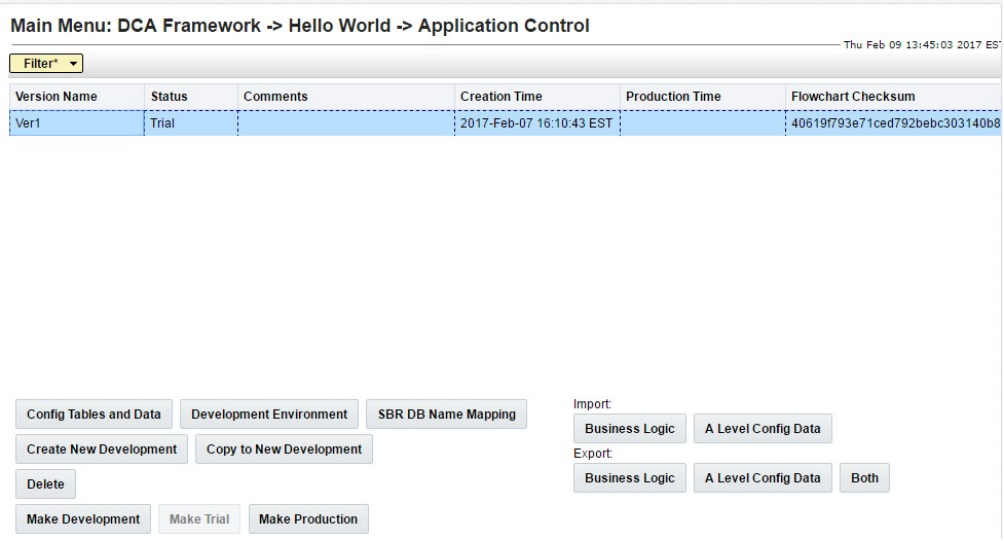
This screen allows users to specify which DA-MPs will run the Trial version of the DCA App



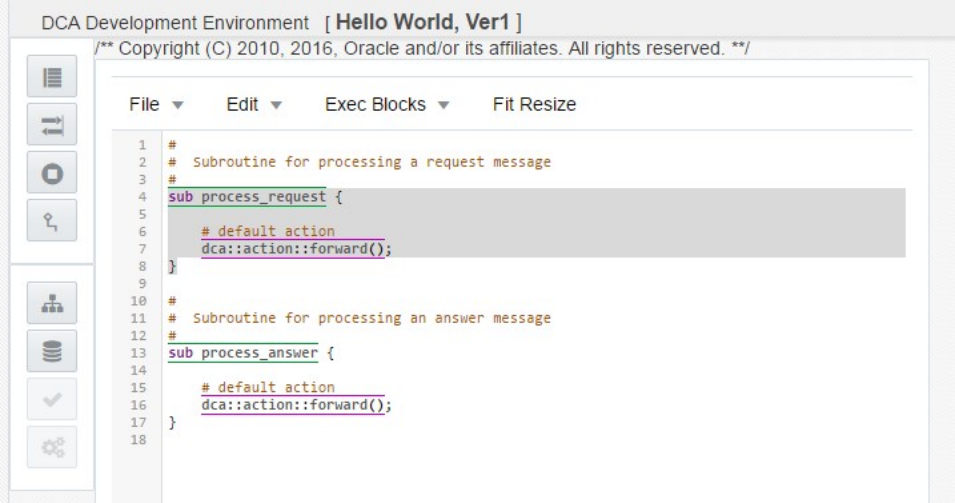
Application Control – Initial Screen



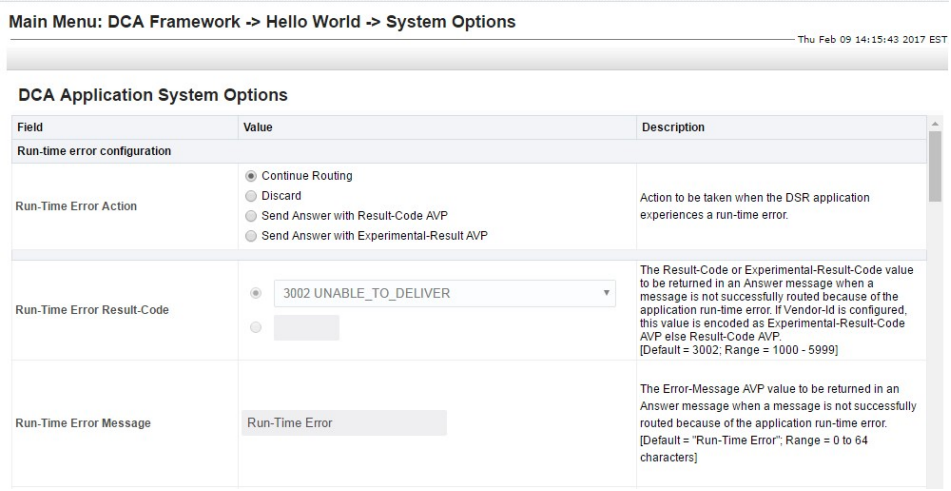
Application Control – Action Buttons



Development Environment



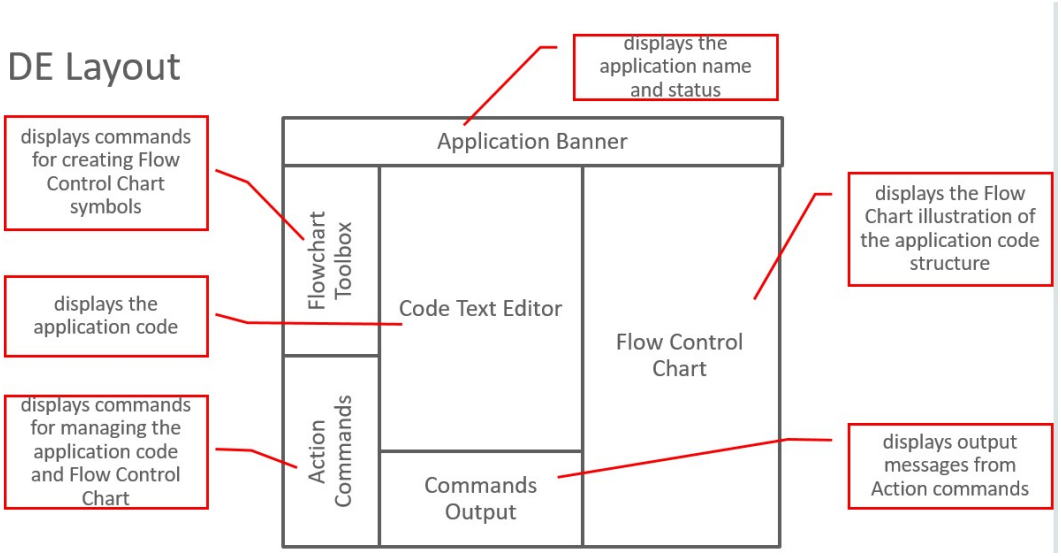
B-Level – System Options



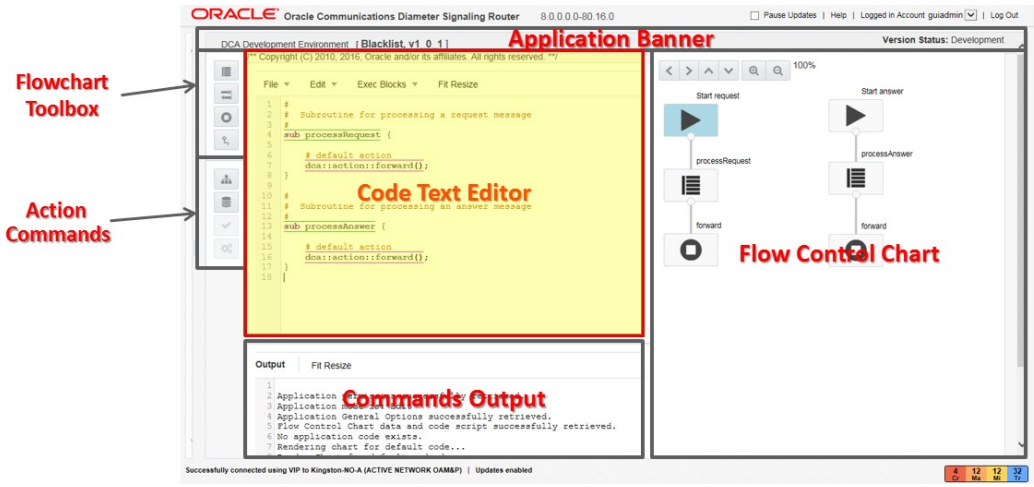
3.1.5 DCA Development Environment

- The DCA-Development Environment (DCA-DE) is the crux of the DCA framework
- The DCA-DE allows the developers to:
- Create, edit and save
- Check syntax and Compile the application code
- Generate an interactive Flow Control chart
- The Flow Control chart is saved together with the application code

DE Layout

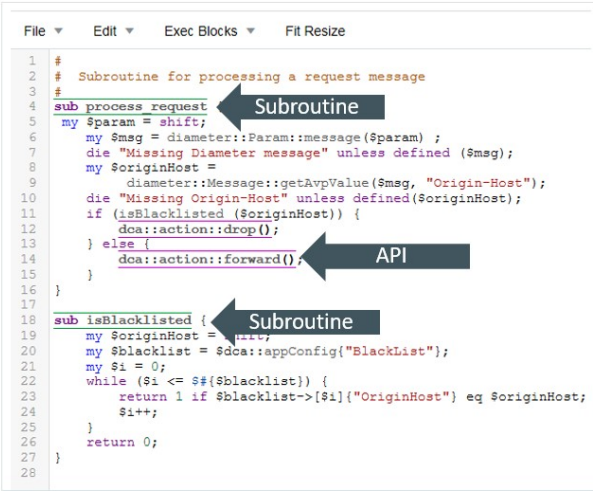


Code Text Editor

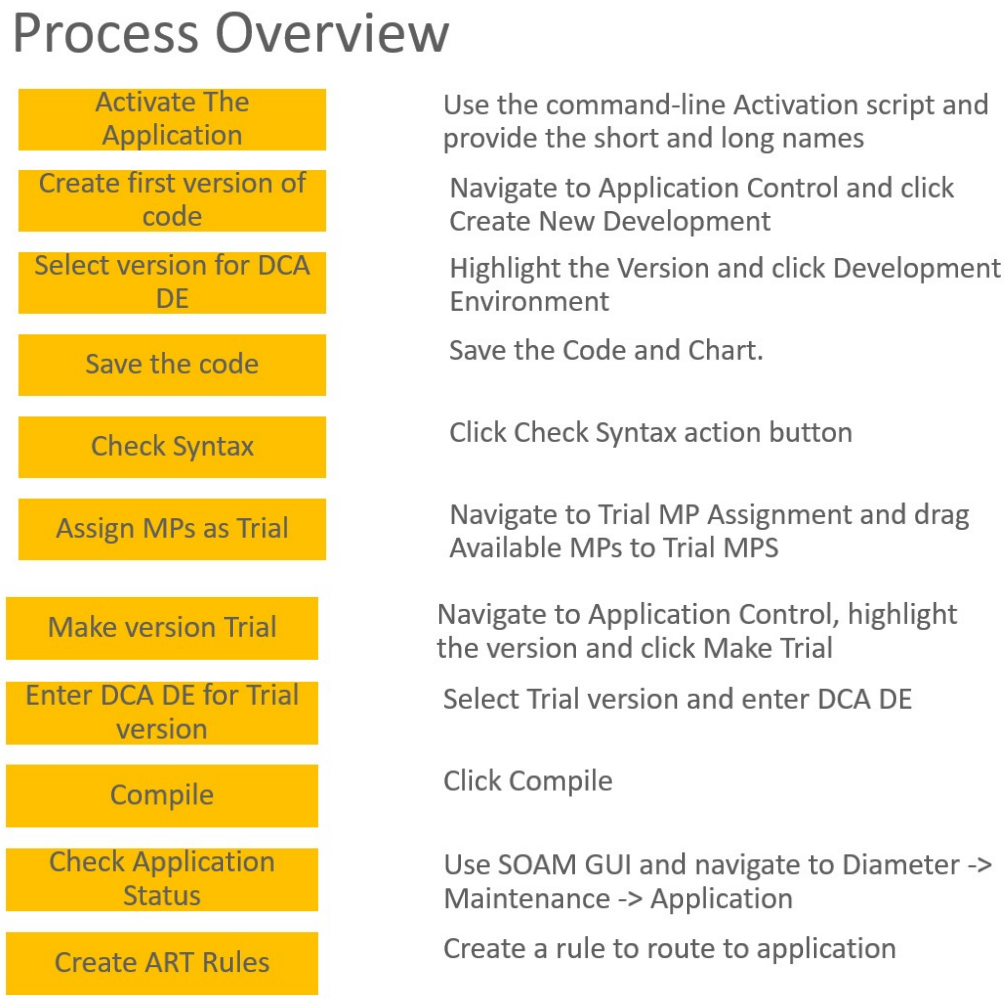


Code Text Editor Description

- Presents an editable view of the DCA Application code (Perl).
- Automatic line numbering
- File menu bar
- Text markup for subroutines, API, comments, etc.
- Supports editor short cut commands (^c, ^x, ^p, ^f, ^z)



Process- Flow

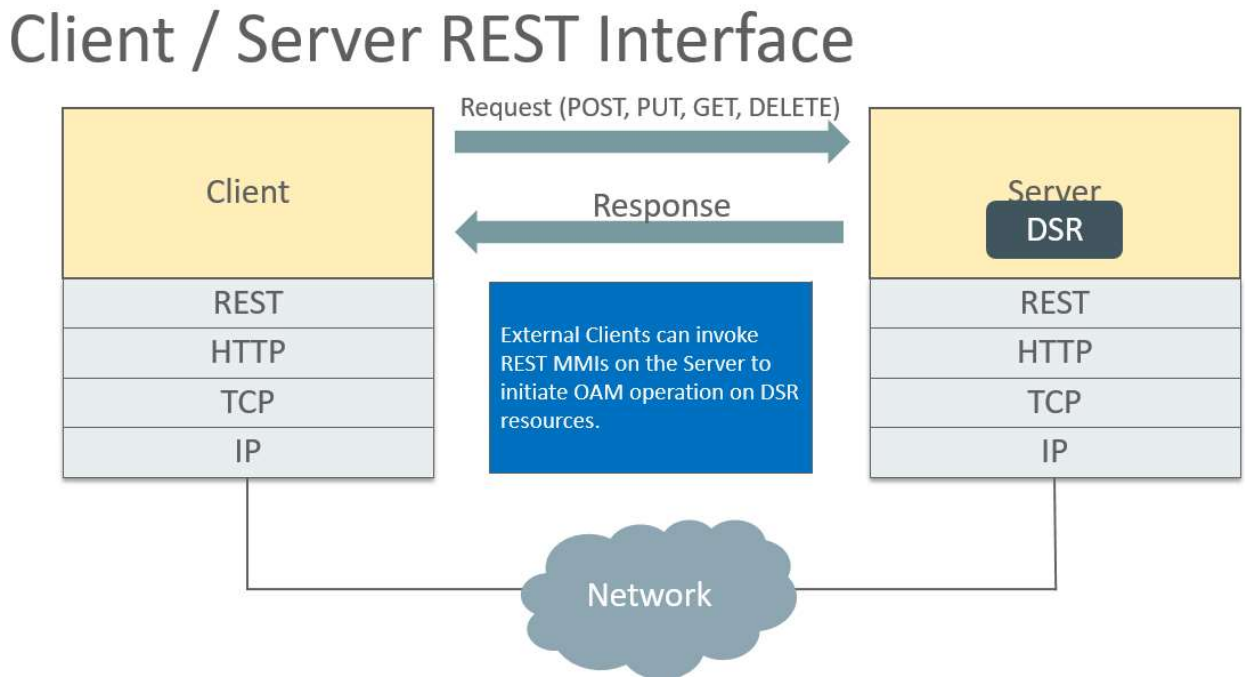


3.2 Machine-to-Machine Interface (MMI)

3.2.1 Description

- The DSR MMI supports the operations, maintenance and configuration actions that are required to deploy, maintain or undeploy the DSR.
- MMI supports the import/export of all configuration data including a filterable subset as well.
- MMI is a secure interface employing encryption and ensuring that only authorized users will be allowed access to system resources.
- DSR configuration items which are comprised of potentially large data sets i.e. APN's, can be efficiently configured via the MMI interface through the use of list operations.
- The DSR MMI feature will include performance management aspects to ensure controlled and reportable command processing with respect to resource consumption of CPU, Memory, IOPs, and network bandwidth on MMI interfaces.
- To assist with after-the-fact troubleshooting the MMI feature supports the logging of both commands and command results.

Implements a RESTful MMI interface to the DSR product to expose supported operations on the DSR object model. In many cases parallels the GUI



DSR objects are mapped to REST "Resources", Resources are named using a URI

Example URI:

1. https: URI scheme. DSR only support https
2. 10.240.70.141: target fqdn or IP address.
3. mmi: constant used in the URI to represent an MMI request.
4. dsr: Product name.
5. v1.0: MMI version. This is used for backward compatibility
6. diameter: Area of the resource
7. routegroups: Name of the resource collection

3.2.2 MMI Authentication

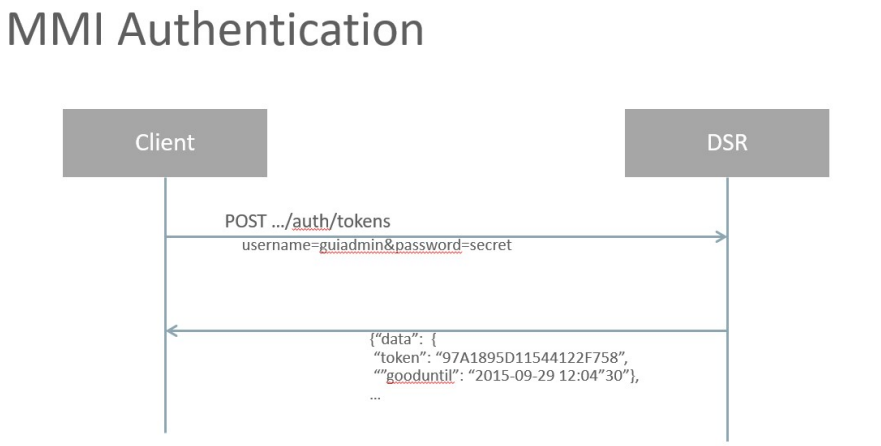
A key requirement for the DSR MMI is that all requests must be:

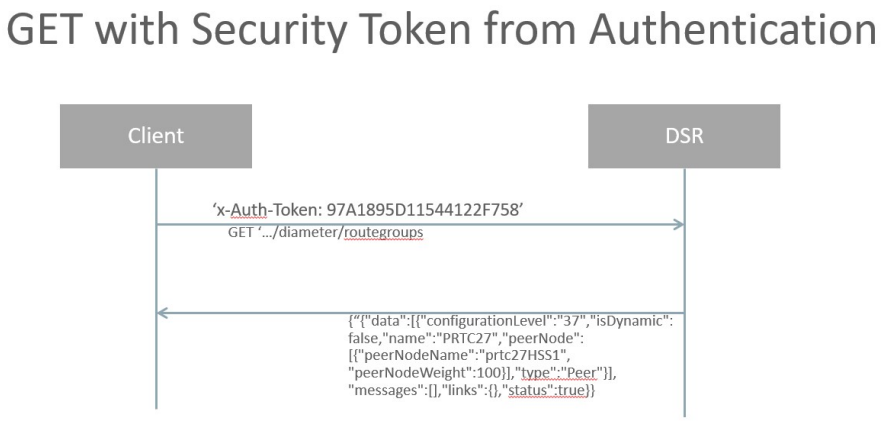
- Authenticated
- Authorized
- Logged

The technique used in DSR is modeled after the authentication scheme found in OpenStack.

In token based authentication, the user must always provide a token along with every request. Clients use a special authentication REST interface to request a new token using a set of credentials.

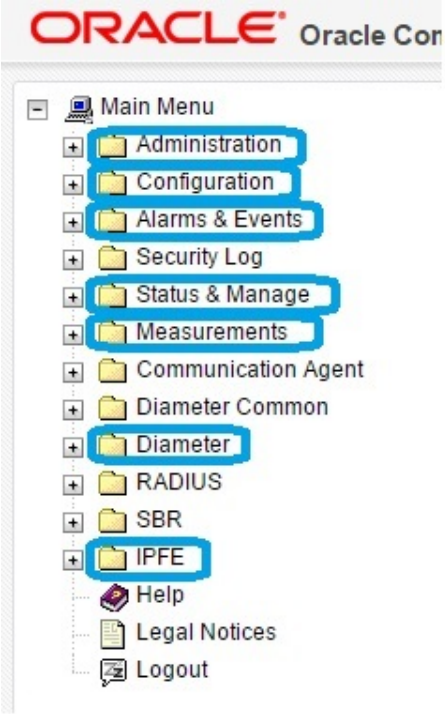
By default Tokens have a 2hr life



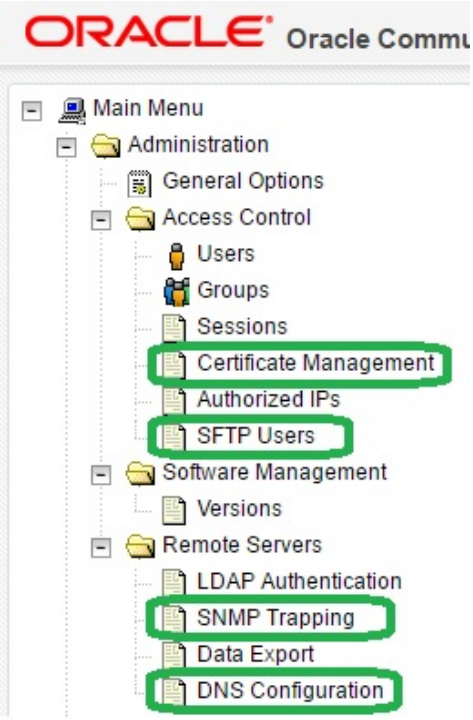


3.2.3 MMI Coverage of DSR Objects

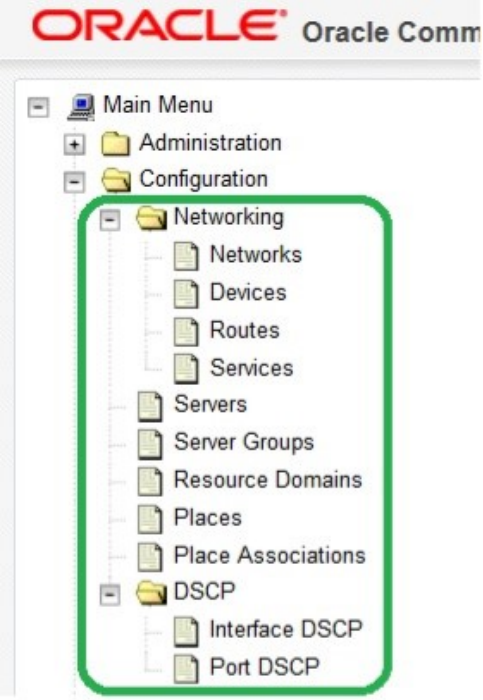
- DSR Core Diameter MMIs



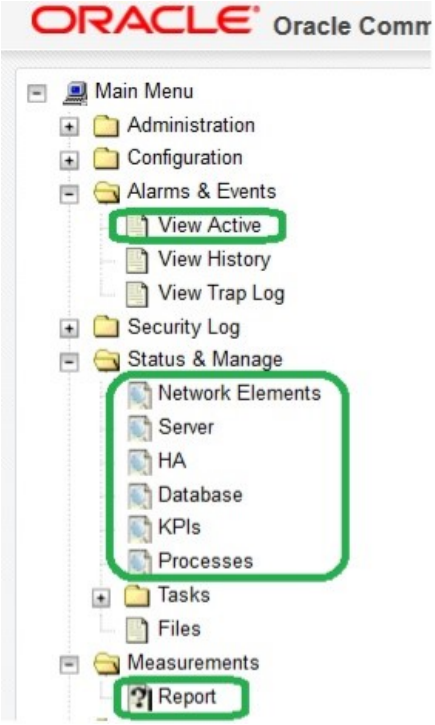
- **MMI coverage-Administration -** DSR MMIs are currently supported in the indicated areas under Administration.



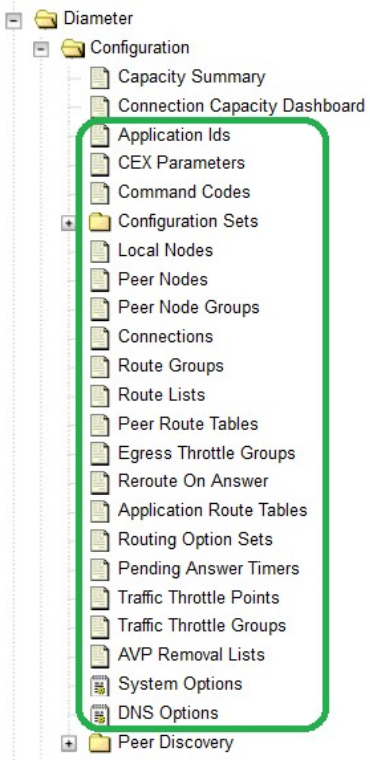
- **MMI coverage-Configuration -** DSR MMIs are currently supported in the indicated areas under Configuration.



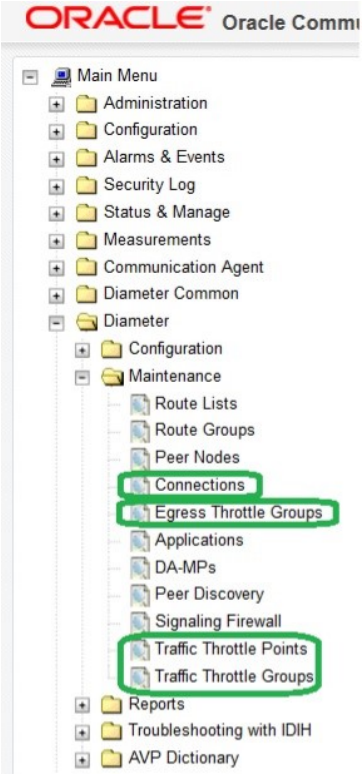
- **Alarms, Status & Manage, Measurements-** DSR MMIs are currently supported in the indicated areas under Alarms & Events, Status & Manage, and Measurements.



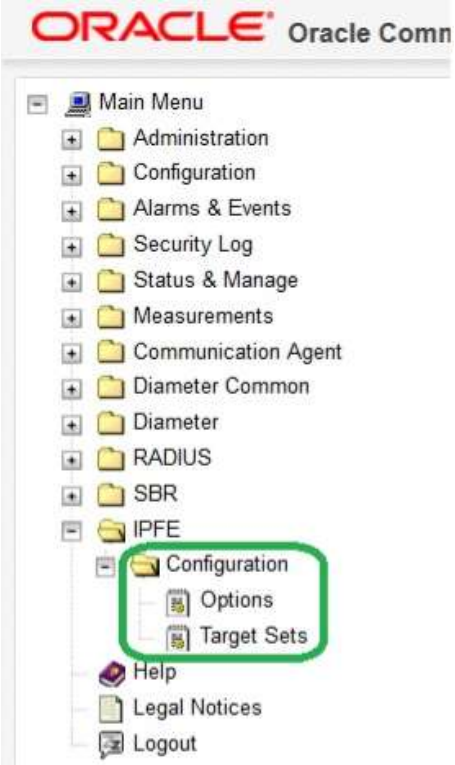
- **Diameter/Configuration-** DSR MMIs are currently supported in the indicated areas under Diameter Configuration



- **Diameter/Maintenance-** DSR MMIs are currently supported in the indicated areas under Diameter Maintenance.

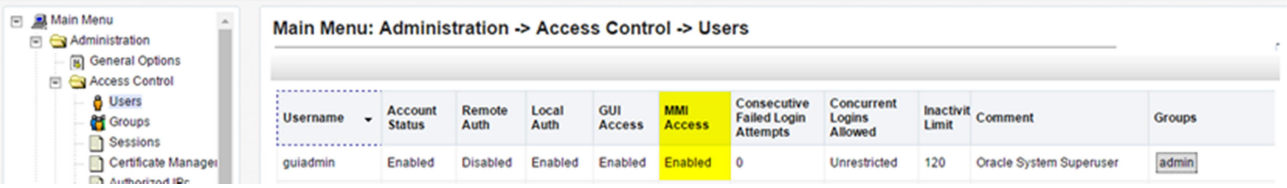


- **MMI Coverage - IPFE-** DSR MMIs are currently supported in the indicated areas under IPFE.



3.2.4 MMI User Authorization

Authorization to MMI can be controlled on a per-username basis.



Note: By default, MMI access will be enabled for the guiadmin user on new install **and** upgrades.

3.2.5 MMI Overload Control

The intent of the Overload Control is to minimize the opportunity for resource (CPU and RAM) starvation due to MMI requests on an OAM server in the presence of high processing loads.

The following SysMetrics are selected for calculating the overload condition:

Metric ID	Metric Name	Metric Description	Threshold
31000	System.CPU_UtilPct	System CPU Utilization Percentage	80%
31001	System.RAM_UtilPct	System RAM Utilization Percentage	80%

3.2.6 MMI Bulk Configuration

Complete Configuration Data can be retrieved with the bulk Configurator Resource /bulk/configurator

- Supports GET and POST
- DELETE and PUT are not supported in DSR 8.0
- GET Is Asynchronous
- Generates a file in the file management path (/var/TKLC/db/filemgmt) of the server the GET was performed
- The Bulk Configurator Resource Accepts these Query Parameters:
- Area //Comma separated list of areas to include
- Filename //allows the specification of a filename for the export XML file generated in File Management. If the parameter is not provided a default name of 'bulkexport_{timestamp}.xml is used.

Example:

The below curl command retrieves the topology information. The information is written to the file management directory in the file named test.xml.

curl --insecure --header 'X-Auth-Token:F95C05781D61803595F6'
'https://localhost/mmi/dsr/v0.23/bulk/configurator?area=topo&filename=test.xml‘

MMI Response:

{"data":[],"messages":[],"links":{"task status":{"type":"status","href":"\/mmi\/dsr\/v0.23\/mon\/tasks\/NO1:67","action":"TASK STATUS","description":"Query task status."}},"status":true}

3.3 Automated Site Upgrade (ASU)

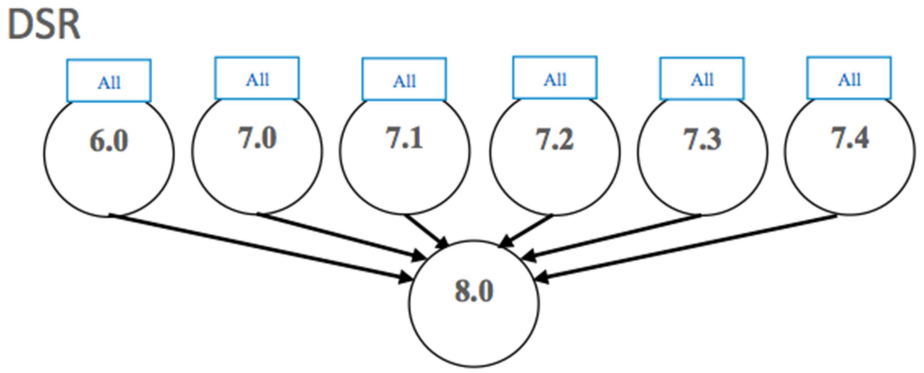
3.3.1 Description

Automated Site Upgrade (ASU) is an enhancement in which an entire DSR site upgrade (SOAMs and C-level servers) can be initiated with just a few initial selections. Once ASU is initiated, automation will handle a) prepare server b) server upgrade c) sequencing of remaining servers.

- ASU provides only partial support for SDS in release 8.0.
- Although SDS SOAMs must still be upgraded using the pre-existing Auto Server Group upgrade feature (ASG), the upgrade of all subtending DP servers may still be automated using the ASU feature.

3.3.2 Compatibility and Topology

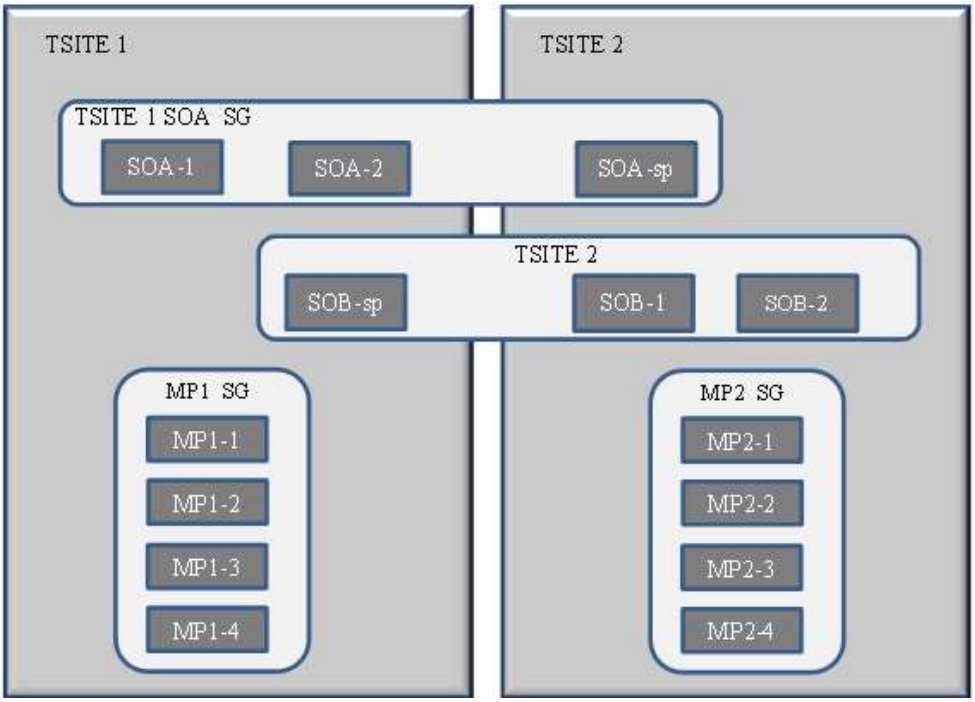
DSR 8.0 Supported Upgrade Paths



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

- DSR 8.0 is compatible with IDIH 7.0, 7.1, 7.2, 7.3 and 7.4.
- DSR 8.0 is compatible with SDS 5.0, 7.1, 7.2, 7.3 and 7.4.
- DSR 8.0 is compatible with Platform 7.4

The below figure depicts a 2 site DSR system with each site containing SOAM and DA-MP Server Groups. Each site's SOAM Server Group defines a spare SOAM server that is physically located at the other site. When a site is upgraded via the Automated Site Upgrade (ASU) feature, the upgrade includes the SOAM spare server even though it is physically located at the other site.



A site upgrade can be initiated on SOA_SG and all of its children using a minimum of GUI selections. The upgrade will perform the following actions:

- Upgrade soa-1, soa-2, and soa-sp
- Upgrade the servers in MP_SG based on an availability setting and HA roles
- In parallel with step 2, upgrade any other Server Groups which are also children of SOA_SG.

- Server Groups that span sites (e.g., SOAMs and SBRs) will be upgraded according to the T-Site to which the server belongs. This will result in upgrading Spare servers that physically reside at another site, but belong to a Server Group in the SOAM that is targeted for site upgrade.

Note: Auto Site Upgrade (ASU) will not automatically initiate the upgrade of TSite 2 in parallel with TSite 1. However, the feature will allow the user to manually initiate Auto Site Upgrade of multiple Tsites in parallel. Some deployments a DSR mated site architecture whereby each site serves as a signaling redundancy point for the other site. In such cases, parallel site upgrades could jeopardize customer signaling traffic.

3.3.3 Scope

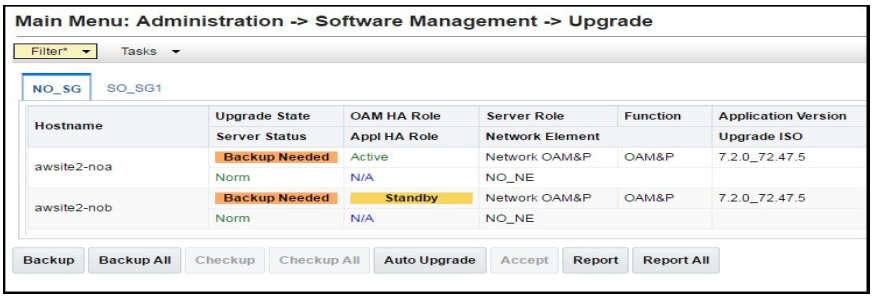
The scope of this feature is a DSR SOAM Site which may include the following DSR components:

- SOAMS
- DA-MP's
- IPFE's
- SBR's
- SS7-MP's

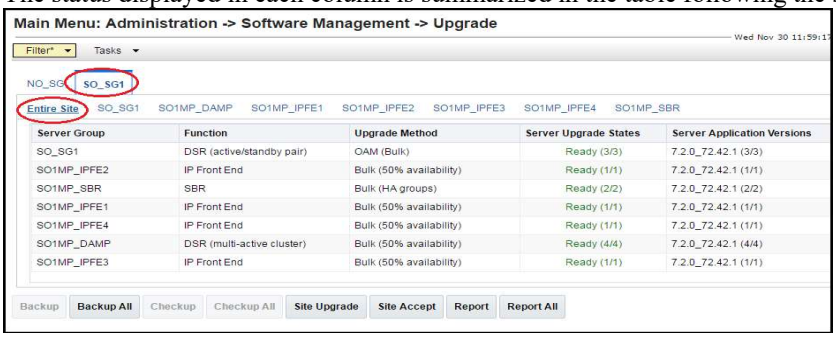
- The scope of DSR Site upgrade does not include firmware. Firmware is hardware dependent and has its own set of upgrade procedures. Similarly, platform components (PM&C and TVOE) have their own upgrade procedures. These components are required to have been completed prior to initiating a DSR Site Upgrade.
- NOAM and DRNOAM upgrades are executed separately and prior to an Automated Site Upgrade. The upgrade procedures for these components remain identical to previous releases. In addition, ASU provides partial support for SDS in release 8.0.

3.3.4 ASU Execution Upgrade

DSR Upgrade is still initiated from the NOAM Administration > Software Management > Upgrade GUI. On initial entry to this screen, the user is presented with a tabbed display of NO and SO Server Groups. With the NO Server Group tab selected, this screen is largely unchanged from the upgrade screen of previous releases. The NO Server Group servers are displayed with the usual assortment of buttons. On this screen, the Auto Upgrade button refers to Automated Server Group upgrade, not Automated Site Upgrade. The site upgrade features become available once an SO Server Group is tab is selected.



When an SO Server Group tab is selected, a second row appears that displays selectable links to the entire site, as well as to each Server Group in this site. By selecting the Entire Site link, the table rows are populated with upgrade details of the site's Server Groups. Each table row provides a summary of the servers belonging to the Server Group. The status displayed in each column is summarized in the table following the screen shot on the next slide.

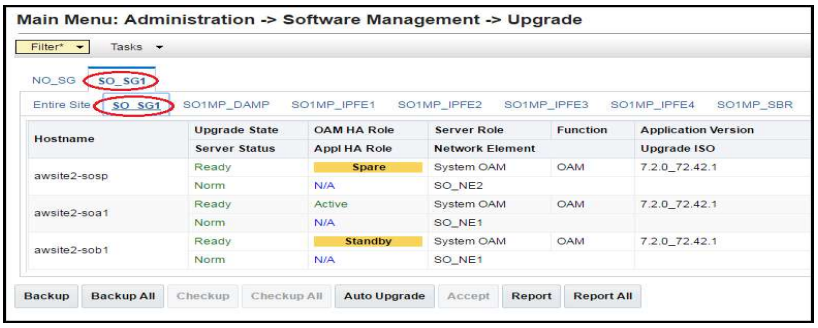


Server Group	Function	Upgrade Method	Server Upgrade States	Server Application Versions
SO_SG1	DSR (active/standby pair)	OAM (Bulk)	Ready (3/3)	7.2.0_72.42.1 (3/3)
SO1MP_IPFE2	IP Front End	Bulk (50% availability)	Ready (1/1)	7.2.0_72.42.1 (1/1)
SO1MP_SBR	SBR	Bulk (HA groups)	Ready (2/2)	7.2.0_72.42.1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

It is from this screen that a site upgrade is initiated by selecting the Site Upgrade button.

Column Name	Purpose	Values
Server Group	Displays the Server Group name	Various
Function	Displays the Server Group function. The function partially determines how a server/Server Group is upgraded	DSR (active/standby pair) DSR (multi-active cluster) IP Front End SBR SS7-IWF SDS
Upgrade Method	Displays the method by which the servers in the Server Group are upgraded	OAM (Bulk) OAM (Serial) Serial Bulk (50% availability) Bulk (66% availability) Bulk (75% availability) Bulk (HA groups) All
Server Upgrade States	Displays the number of servers in the Server Group that are in each upgrade state	Pending (x/y) Success (x/y) Ready (x/y) Failed (x/y) Not Ready (x/y)
Server Application Versions	Displays the number of servers in the Server Group that are on the source and target releases	Various

When a Server Group link is selected, the table rows are populated with the upgrade details of the individual servers within that Server Group. From this screen, the Automated Server Group upgrade and individual server upgrade functions are initiated. The functionality and behavior of this screen is unchanged from previous releases.

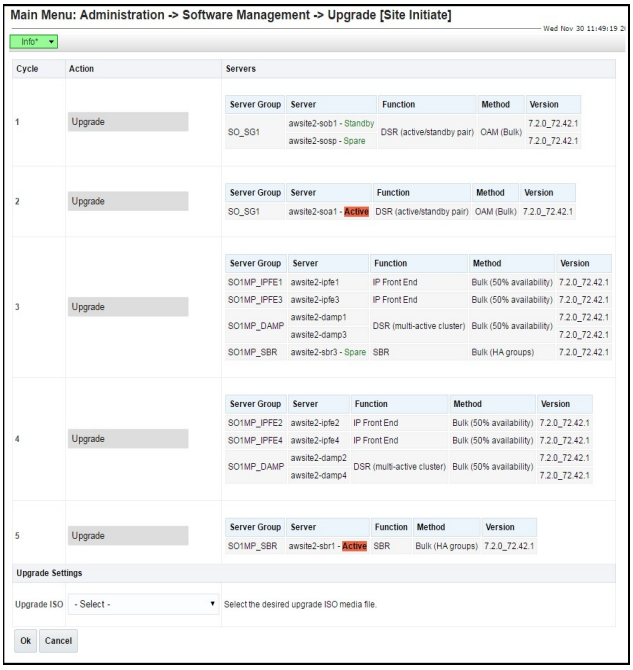


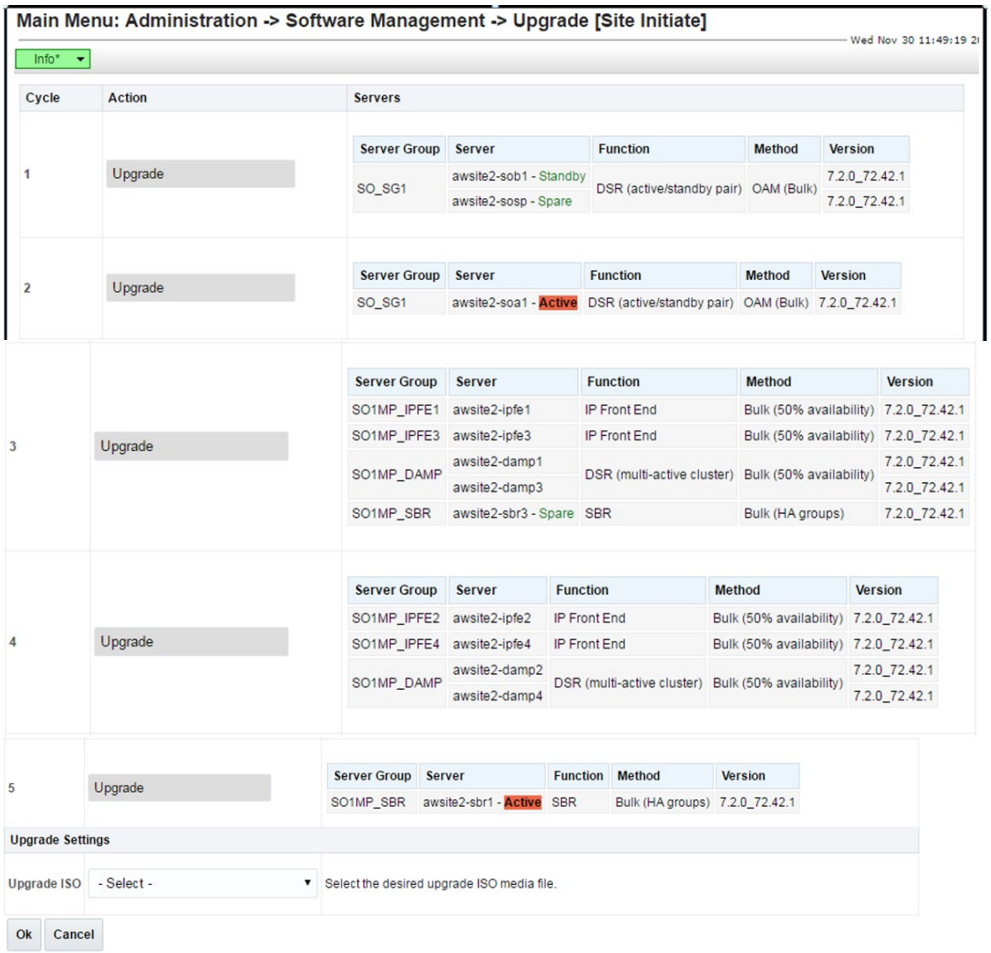
Hostname	Upgrade State / Server Status	OAM HA Role / Appl HA Role	Server Role / Network Element	Function	Application Version / Upgrade ISO
awsite2-sosp	Ready	Spare	System OAM	OAM	7.2.0_72.42.1
	Norm	N/A	SO_NE2		
awsite2-soa1	Ready	Active	System OAM	OAM	7.2.0_72.42.1
	Norm	N/A	SO_NE1		
awsite2-sob1	Ready	Standby	System OAM	OAM	7.2.0_72.42.1
	Norm	N/A	SO_NE1		

3.3.5 ASU Execution-Site Upgrade

When the Site Upgrade button is selected, the Upgrade [Site Initiate] screen displays a summary of the servers and Server Groups that will be upgraded, and provides a dropdown list of target ISO files. Once an ISO is selected, clicking the Ok button initiates the upgrade.

- The Upgrade [Site Initiate] screen displays the number of Cycles it will take to upgrade the entire site (B-level and C-level), the Action to be taken for each cycle, and the Servers that will be upgraded in each cycle.
- The cycles shown are sequential. That is, each cycle is dependent on the successful completion of the previous cycle.
- The following screenshots show an upgrade requiring 5-cycles. Any particular DSR deployment may involve a different number of cycles.
- In Upgrade [Site Initiate] screen, Cycle 1 shows that the Spare and Standby SOAMs will be upgraded in parallel.
- Cycle 2 shows the upgrade of the Active SOAM.
- Cycle 3 shows the upgrade of two IPFEs, one-half of the DA-MPs, and the Spare SBR.
- Cycle 4 shows the upgrade of the other two IPFEs, the other one-half of the DA-MPs, and the Standby SBR.
- Cycle 5 shows the upgrade of the Active SBR.
- The upgrade ISO is selected in the Upgrade Settings section.
- While the site upgrade is in progress, the upgrade status of all of the servers and Server Groups is displayed on the Administration > Software Management > Upgrade screen.





3.3.6 ASU Upgrade Failure Handling

In the event that a server fails to successfully upgrade during the execution of an Auto Site Upgrade, failure events will be generated for the server, for the associated Server Group, and for the associated site. A server upgrade failure alarm will also be raised for each server that failed. These events and alarms are summarized in the following table.

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

3.4 Oracle VM Cloud Support

3.4.1 Description

Customers want to deploy DSR in their cloud environments, where resources like virtual CPUs, memory, and disk space are specified by a cloud manager rather than dictated by the hardware on which the DSR is installed. Earlier DSR design had assumed known hardware configurations. Now we need to determine how well the DSR will perform in a cloud environment and make recommendations to cloud administrators on the resources to provide DSR VMs.

DSR 8.0 introduces support of DSR deployment in the Oracle Virtual Machine (OVM) cloud environment.

Oracle Virtual Application (OVA) continues to support Cloud DSR deployment. In addition to the two previously available hypervisors (KVM and VMware), OVA in DSR 8.0 is enhanced to install an additional choice of hypervisor: Oracle Virtual Machine (OVM).

3.4.2 DSR Cloud Install

- Cloud DSR Install requires less procedural interaction than Engineered DSR

Engineered DSR requires execution of these procedures	Installation Procedures	Cloud DSR does not require these procedures
Yes	TPD Installation	No, TPD is included in the OVA
Yes	TVOE & PMAC	No, not needed
Yes	NetBackup	No, not available

- There are five (5) different Cloud OVAs available for download, through the normal customer channels.

DSR application software
- NOAMP
- SOAM
- MP

iDIH
- Application
- Mediation
- Database

SDS application software
- SDS NOAMP
- SDS SOAM
- SDS DP

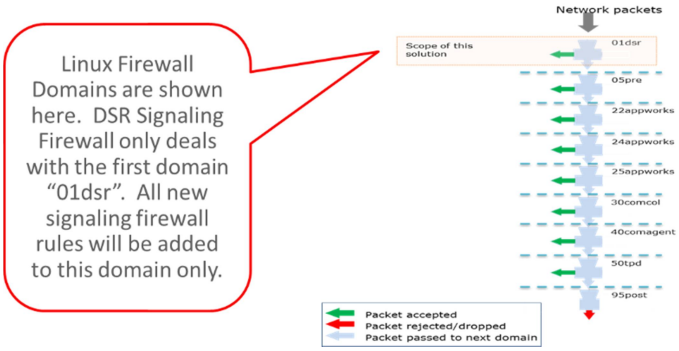
- Basic steps to install DSR 8.0 on OVM include:
  - Upload OVA image
  - Create VMs and edit number of CPUs, disk space, and memory according to the values in the “Resource Profiles” appendix in the doc.
  - Edit existing or add VNICs
  - Set IP addresses
  - Continue with application configuration, which is common for all hypervisors.
- OVM Manager Command Line Interface, example procedure step

1 ☐	**Preperation**	Refer to Appendix E. Common OVM-Manager tasks (CLI) for setting up the platform. **Note**: Logon to the OVM-M CLI for executing all the OVM commands. Refer step 1 of Appendix E. Common OVM-Manager tasks (CLI)
2 ☐	**OVM-M CLI:** Import the OVA	1. Import the VirtualAppliance / OVA OVM>`importVirtualAppliance Repository name=MyRepository url="http://///example.com//myvirtualappliance.ova"` Example: OVM> importVirtualAppliance Repository name=Vms01Repo url=http:////10.240.191.134//DSR-8.0.0.0.0_80.11.0.ova

3.5 Firewall Feature

3.5.1 Description

Prior to DSR Release 8.0, the DA-MP servers do not restrict any network traffic which means the signaling networks are defenseless to any security threat. The Figure shows how the DSR Linux firewalls are configured on DA-MP servers in DSR prior to Release 8.0 software. Notice that the network traffic arriving on the DA-MP servers is readily accepted by the very first firewall rule in 01dsr "domain" without even inspecting the network packet



This feature brings the flexibility and capability in DSR to dynamically determine and customize the Linux firewall on each DA-MP server in the DSR Signaling node to allow only the essential network traffic pertaining to the active signaling configuration. The in-bound signaling traffic is accepted by the DSR application over the configured and enabled Diameter and Radius connections only. By monitoring the active Diameter configuration, this feature determines which configured connections are enabled. It then configures the Linux Firewall on the DA-MP servers to allow the signaling network traffic for those connections only, thus providing added security to the signaling networks.

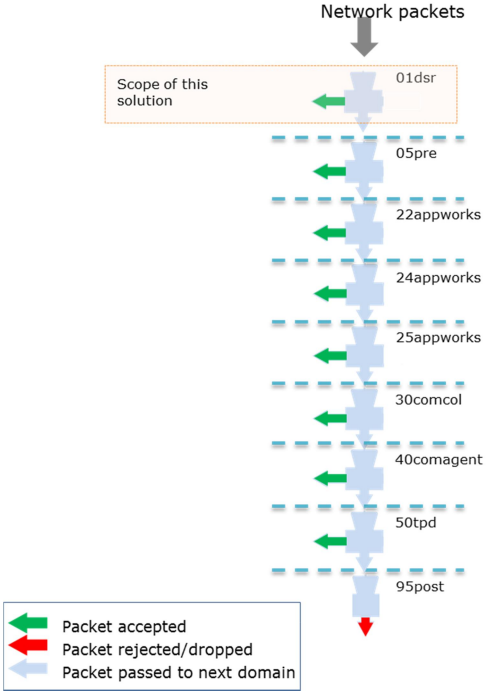
This solution added following capabilities in the DSR Release 8.0 software –

- Capability to automatically configure the Linux firewall to allow desired signaling network traffic on DA-MPs.
- Capability to dynamically update the Linux firewall configuration on DA-MPs to allow or disallow signaling traffic.
- Capability to administer (Enable and Disable) the DSR Signaling Firewall on the Signaling Node via System OAM configuration user interfaces.

3.5.2 Linux Firewall

This solution will install and organize the rules in “01dsr” firewall domain in following order

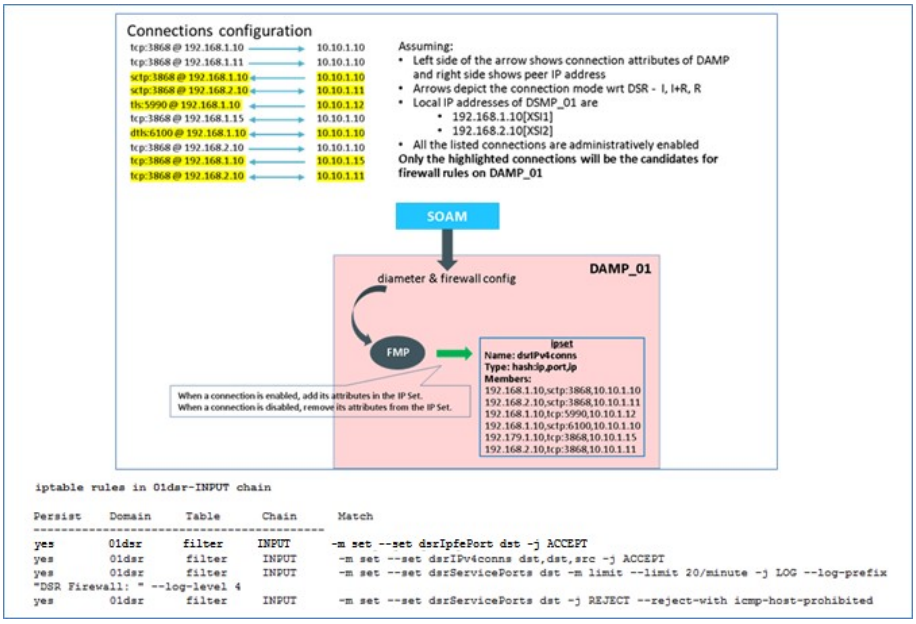
- The rule that allows all the in-bound network traffic. This is a static rule.
- The rule that allows the in-bound traffic corresponding to the enabled Diameter and Radius connections. It will reference an IP Set which will contain the list of connection quadruples.
- The rule that logs the in-bound traffic that has destination port as one of the Diameter or Radius service ports. This traffic will get rejected by the next rule.
- The rule that rejects the in-bound traffic that has destination port as one of the Diameter or Radius service ports.



The first rule will be removed when the DSR Signaling Firewall is enabled and inserted back when it is disabled.

IP Sets: The solution utilizes the “ipset” and “iptablesAdm” Linux utilities to make the dynamic updates in the Linux firewall. This solution doesn’t configure firewall rules for each connection; rather it creates IP Sets once and references them in firewall rules. This way, the firewall rules do not change when there is a change in the active signaling configuration.

The following examples demonstrate the Linux firewall configuration when DSR Signaling firewall is enabled and disabled.



Linux Firewall configuration when signaling Firewall is disabled

```
iptables rules in 01dsr-INPUT chain

Persist    Domain     Table      Chain      Match
----------------------------------------
yes        01dsr      filter     INPUT      -j ACCEPT
yes        01dsr      filter     INPUT      -m set --set dsrIPv4IpfePort dst,dst -j ACCEPT
yes        01dsr      filter     INPUT      -m set --set dsrIPv4conns dst,dst,src -j ACCEPT
yes        01dsr      filter     INPUT      -m set --set dsrIPv4ServicePorts dst,dst -m limit --limit
20/minute -j LOG --log-prefix "DSR Firewall: " --log-level 4
yes        01dsr      filter     INPUT      -m set --set dsrIPv4ServicePorts dst,dst -j REJECT --reject-
with icmp-host-prohibited
```

3.6 Independent SBR DB Support for DCA

3.6.1 Description

Prior to DSR release 7.2, the Session Binding Repository (SBR) has provided a dedicated Database solution to the Policy and Charging Application (PCA) and Gateway Location Application (GLA) on DSR. The PCA SBR is designed for PCA as a built-for-purpose Database solution with dedicated DB types, application specific interface to SBR Database, application specific database schema and audit procedure, application specific data replication policy and High Availability (HA) policies. An example of policy SBR database is demonstrated in the following diagram:

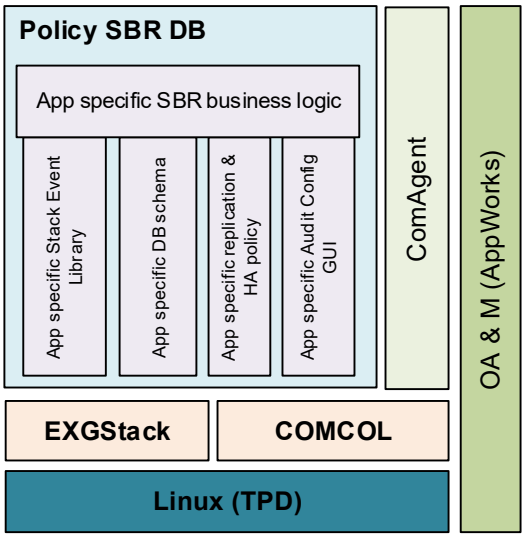


Figure: Policy SBR Database Architecture

While the built-for-purpose database approach is optimized for providing high performance database solution to PCA, it will be very difficult, if possible, and not cost effective to use the same approach to provide database solutions to a large number of applications to be developed by possibly non-Oracle development teams.

Aiming at solving the problem mentioned above, a feature is developed in DSR 8.0 to provide a common application development environment to enable the development teams inside and outside Oracle to develop applications on DSR via provided APIs and service enablers with fast development cycles. As part of the common application development environment, the Independent SBR (I-SBR) is designed to provide database services to a variety of applications to meet various application and business needs.

3.6.2 Independent SBR (I-SBR) Infrastructure

The Independent SBR (I-SBR) provides a common database framework to host database solutions for various applications including DSR native applications developed by Oracle engineers and applications developed by third party developers. The major functionalities of the I-SBR infrastructure include:

- A common framework to host a generic database, that can be used by multiple and different applications such as DCA applications, as well as many built-for-purpose databases for some other applications such as PCA or GLA,
- A common configuration and maintenance system to enable users to configure and manage databases for various types of applications, and a common control for database audit,
- A common communication mechanism to allow various applications to communicate with different databases, generic or built-for-purpose, via the DSR ComAgent routing services and a common stack event library,
- A common Comcol HA policy management and Resource/Sub-resource management for various database,
- A common set of Alarms, Events, KPIs and Measurements for database usages that are applicable for all applications.

The Figure below illustrates the I-SBR infrastructure with its components and the SBR database built on top of it.

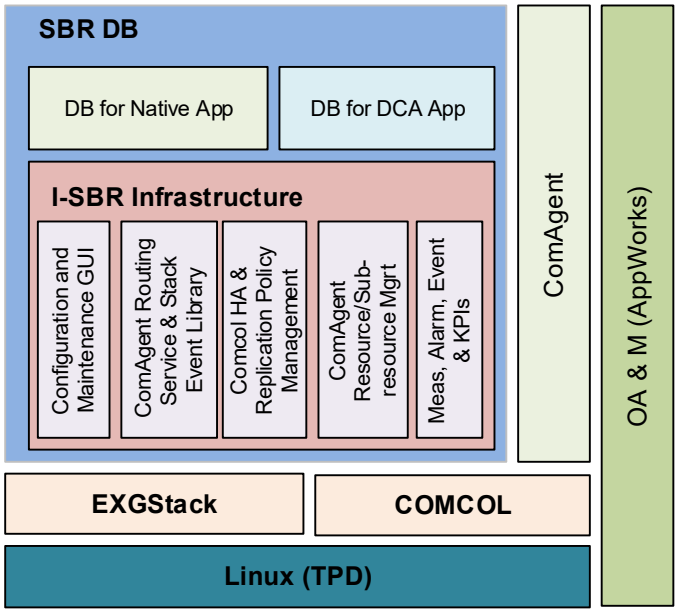


Figure: Independent SBR Infrastructure

The I-SBR infrastructure provides a common framework on which various database solutions can be formed to meet different applications' needs. The databases can be built up by using the common I-SBR infrastructure, that is unchanged and independent from any application, plus the application specific SBR business logic and, if applicable, other application specific components. The database constructed on top of I-SBR infrastructure can be a special purpose database for one particular application such as Binding or Session SBR for PCA application, or a generic database with common stack events and database schema for a variety of applications such as Universal SBR for DCA applications and/or some other DSR native applications. The following figures display these two examples respectively.

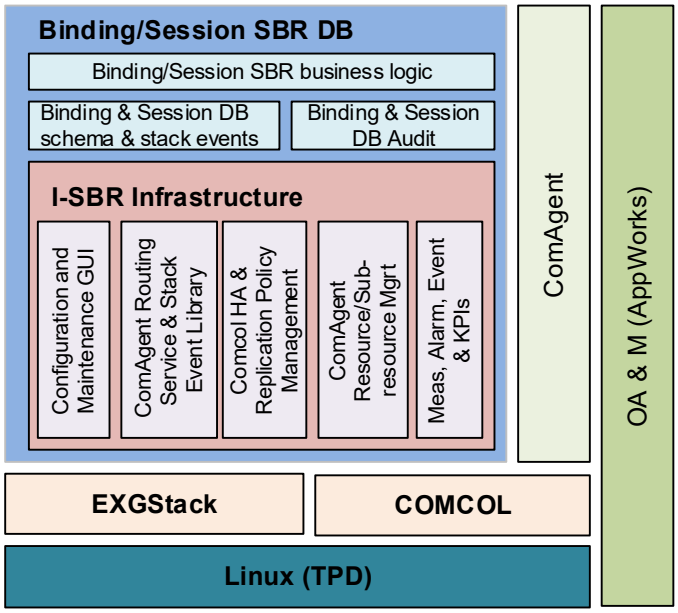


Figure: Binding/Session SBR DB for PCA

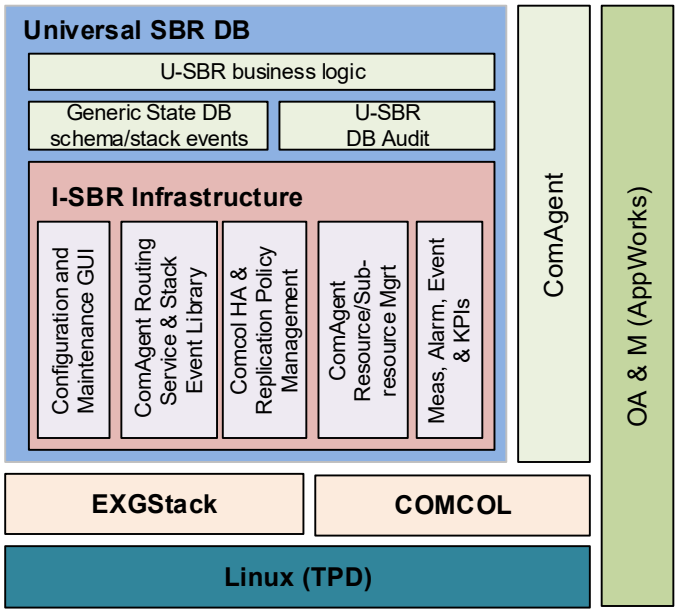


Figure: Universal SBR DB for DCA Apps

SBR infrastructure can be used in a variety of ways to build database solutions for various applications. A generic database may be used by multiple applications. In this case, all applications can access to the same database via common generic stack events. An example of this database is the Universal SBR DB for all DCA applications and/or some other DSR native applications as shown in

Figure. On the other hand, I-SBR infrastructure can host multiple database solutions on the same SBR server that different applications can use their own databases respectively. For example, Session SBR database and Universal SBR database can be hosted on the same SBR server on top of I-SBR infrastructure serving PCA application and DCA applications respectively as illustrated in Figure:

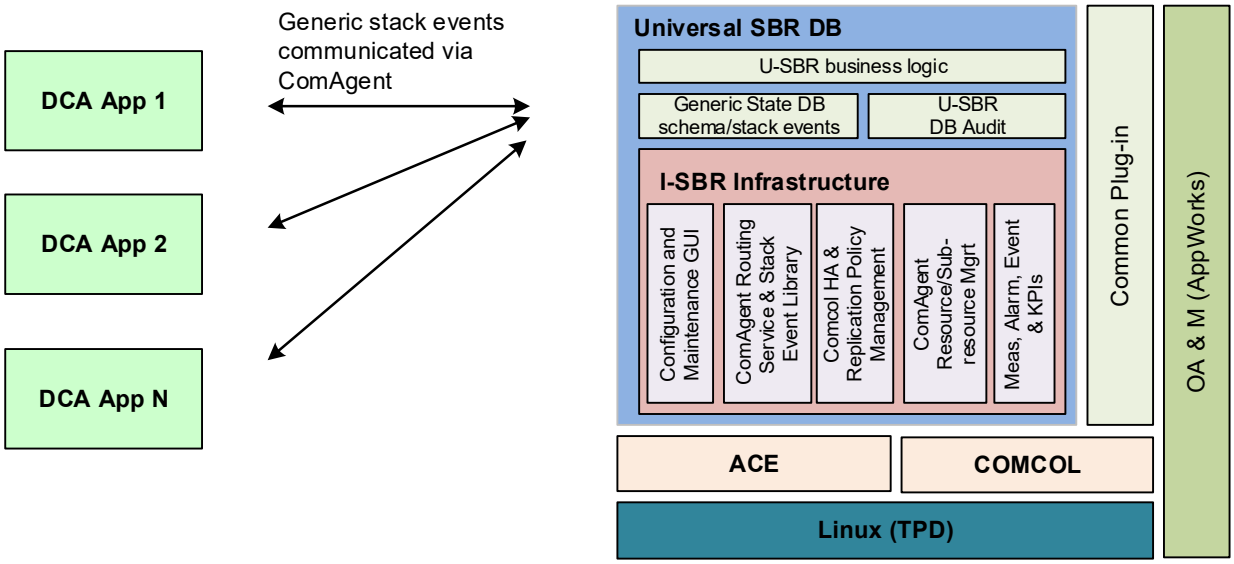


Figure: Universal SBR DB Used by Multiple DCA Apps

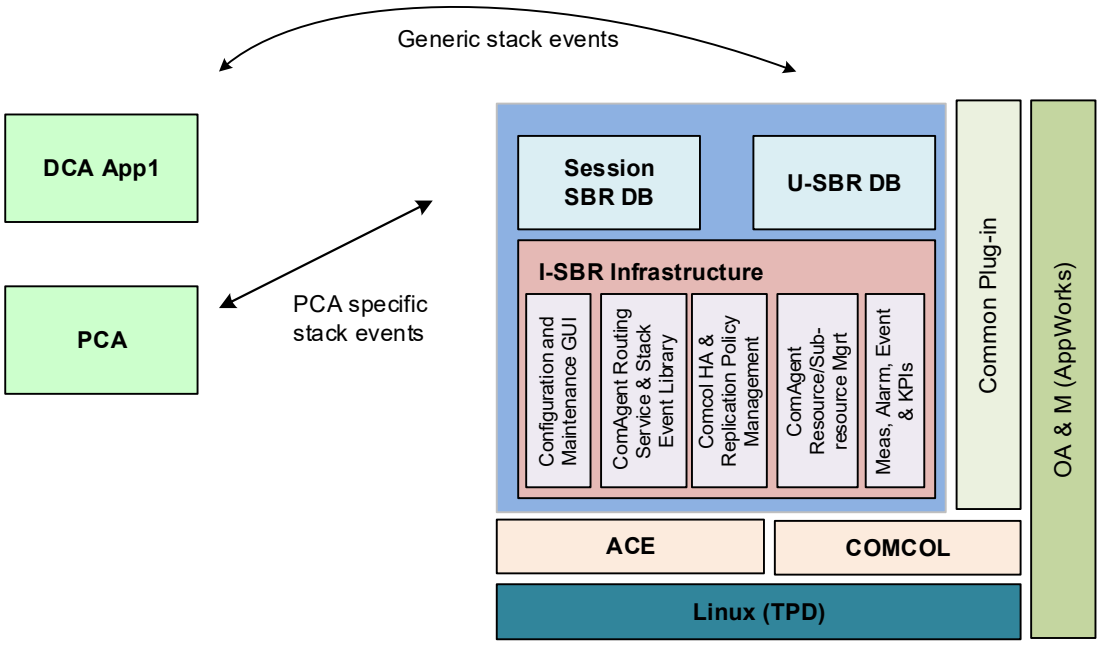


Figure: Session SBR DB and Universal SBR DB on Same SBR Server

3.7 16 Signaling VLAN Support & VE-DSR Automated VM Creation

3.7.1 Description

Prior to DSR 8.0, VEDSR guest Creation was manual and required the user to create each DSR guest individually. This feature automates the Creation of the VEDSR guests.

3.7.2 Data Model

An overall installation requirement is decided upon among the data that should be collected:

- The Total number of Rack Mount Servers
- The number of VMs and servers on each Rack Mount Server and their role(s)
- What time zone should be used across the entire collection of DSR sites?
- Will SNMP traps be viewed at the NOAM, or will an external NMS be used? (Or both?)
- PCI cards installed? (HP DL380 Gen 9 (10Gbps) Only) – Segregated Signaling Only

3.7.3 VEDSR 8.0 Installation

- VEDSR is a fully virtualized DSR, all DSR server functions are virtual: (NOAMP, SOAM, MP, IPFE, SBR, iDIH, SDS)
- Requires PMAC to install DSR guests
- The VEDSR solution continues to be based on PMAC/TVOE and runs on Oracle X5-2/X6-2 or HP G9 servers.
- A VEDSR signaling node may consist of up to 8 physical servers and is targeted to support, at a minimum, 100K Diameter MPS.
- The actual number of servers used in a deployment may vary and depends on the MPS and HA requirements.
- Up to eight (8) different ISOs are required for VEDSR. These are available for download through OSDC.

Platform	iDIH	DSR	SDS
• TVOE	• Application	• DSR NOAMP	• SDS NOAMP
• TPD	• Mediation	• DSR SOAM	• SDS SOAM
• PMAC	• Database	• DSR MPP	• SDS DP

3.8 FABR and RBAR Enhancements

3.8.1 Description

Range Based Address Resolution (RBAR) is an enhanced routing application that allows the routing of Diameter end-to-end transactions based on Diameter Application ID, Command Code, Routing Entity Type, and Routing Entity Addresses (range and individual) as a Diameter Proxy Agent.

Full Address Based Resolution (FABR) is a routing application that enables network operators to resolve the designated Diameter server (IMS HSS, LTE HSS, PCRF, OCS, OFCS, and AAA) addresses based on Diameter Application ID, Command Code, Routing Entity Type, and Routing Entity Addresses, then routes the Diameter Request to the resolved destination.

DSR 8.0 has added feature enhancements for RBAR and FABR by adding support for 4 new Primary AVP and Routing Entity combinations.

They include:

1) User-Identifier with an embedded UserName AVP.

2) User-Identifier with an embedded MSISDN AVP.

3) UserName AVP with no embedded AVP.

4) MSISDN AVP with no embedded AVP.

Top Level AVP	Embedded AVP	Routing Entity	for RBAR & FABR
User-Identifier	UserName	IMSI, IMPI	yes
User-Identifier	MSISDN	MSISDN, IMPU	yes
UserName		MSISDN, IMPU	yes
MSISDN		MSISDN, IMPU	yes

Figure: New Primary AVP and Routing Entity combinations

Its support new Diameter interface like S6m & S6n. The first two new AVPs can be utilized with the S6m and S6n Diameter interfaces. In DSR 8.0, these interfaces can now carry the IMSI in the embedded UserName AVP inside the top level User-Identifier AVP. When carrying a MSISDN, it is also carried in the embedded MSISDN AVP inside the top level User-Identifier AVP.

UserName AVPs can be utilized with the Gy and Ro Diameter interfaces. In DSR 8.0, these interfaces can now carry the MSISDN in the top level UserName AVP.

MSISDN AVPs can be utilized with the SLg Diameter interfaces. In DSR 8.0, this interfaces can now carry the MSISDN in the top level MSISDN AVP.

3.8.2 SOAM GUI

Main Menu: RBAR -> Configuration -> Address Resolutions -> [Insert]

Tue Aug 07 10:05:05 2012 U

Attribute	Value	Description
Application ID	- Select - *	Application ID in Diameter message.
Command Code	- Select - *	Command Code value in Diameter message.
Primary Routing Entity		
Routing Entity	- Select - *	Type of Routing Entity. A Routing Entity can be a User Identity (IMSI, MSISDN, IMPI or IMPU) or an IP Address associated with the User Equipment (IPv4, IPv6-prefix or UNSIGNED16 address).
Primary AVP	- Select - *	Primary AVP which will be used for extracting the Routing Entity address.
Secondary AVP	- Select -	Secondary AVP which will be used for extracting the Routing Entity address.
Address Table Name	- Select - *	Address Table for this Routing Entity Type.
Secondary Routing Entity		
Routing Entity	- Select -	Type of Routing Entity. A Routing Entity can be a User Identity (IMSI, MSISDN, IMPI or IMPU) or an IP Address associated with the User Equipment (IPv4, IPv6-prefix or UNSIGNED16 address).
Primary AVP	- Select -	Primary AVP which will be used for extracting the Routing Entity address.
Secondary AVP	- Select -	Secondary AVP which will be used for extracting the Routing Entity address.
Address Table Name	- Select -	Address Table for this Routing Entity Type.

Ok Apply Cancel

Figure: Address Resolutions Insert Screen

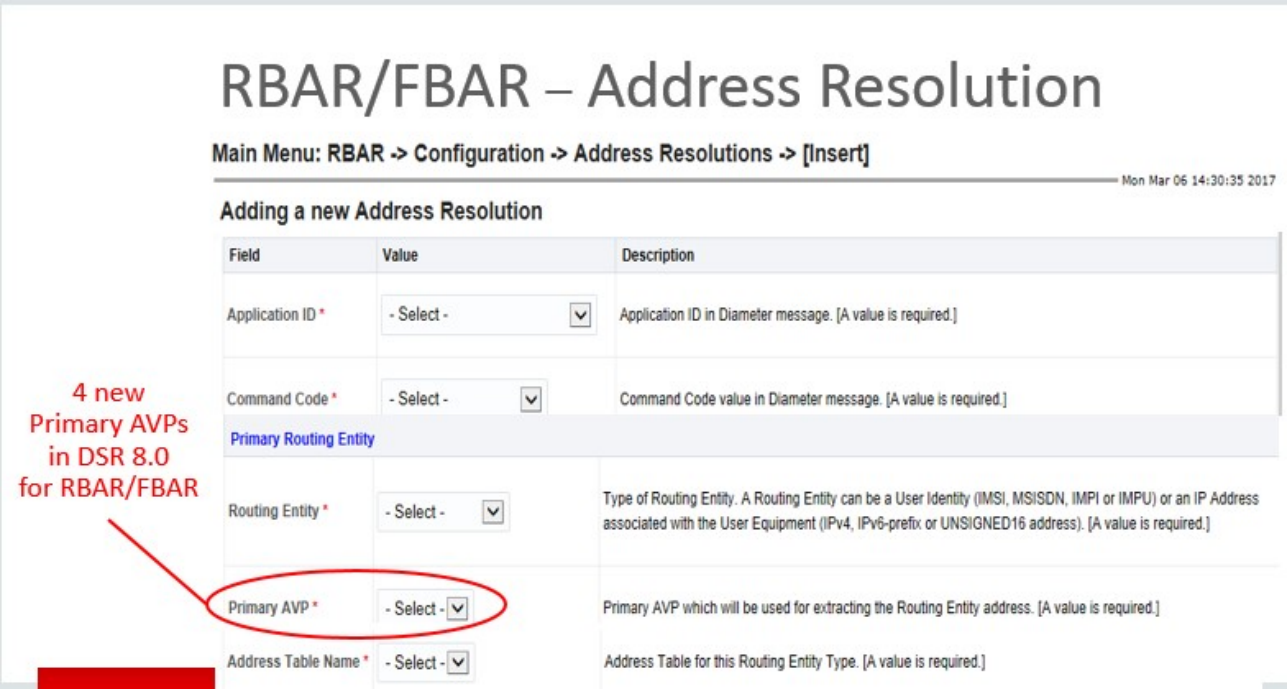


Figure: RBAR /FBAR> the Configuration > and then Address Resolutions.

- For RBAR/FBAR Routing Entity: IMSI or IMPI
  - 1 new Primary AVP was added in DSR 8.0: UserIdentifier.UserName

Primary Routing Entity		
Routing Entity *	-- Select -- **IMSI** **IMPI**	Type of Routing Entity. A Routing Entity can be a User Identity (IMSI, MSISDN, IMPI or IMPU). [A value is required.]
Primary AVP *	-- Select -- Public Identity ServiceInfo.Subscription-Id(1) ServiceInfo.Subscription-Id(2) ServiceInfo.Subscription-Id(3) ServiceInfo.Subscription-Id(4) Subscription-Id(1) Subscription-Id(2) Subscription-Id(3) Subscription-Id(3) ✓ **UserIdentifier.UserName** UserIdentity.Public-Identity UserName	Primary AVP which will be used for extracting the Routing Entity address. [A value is required.]

Figure: The User Identifier AVP Highlighted with the Green Checks

- For RBAR/FBAR Routing Entity: MSISDN or IMPU
  - 3 new Primary AVPs were added: MSISDN, UserIdentifier.MSISDN, & UserName

Primary Routing Entity		
Routing Entity *	-- Select -- **MSISDN** **IMPU**	Type of Routing Entity. A Routing Entity can be a User Identity (IMSI, MSISDN, IMPI or IMPU). [A value is required.]
Primary AVP *	-- Select -- ✓ **MSISDN** Public Identity ServiceInfo.Subscription-Id(0) ServiceInfo.Subscription-Id(2) ServiceInfo.Subscription-Id(3) ServiceInfo.Subscription-Id(4) Subscription-Id(0) Subscription-Id(2) Subscription-Id(3) Subscription-Id(4) ✓ **UserIdentifier.MSISDN** UserIdentity.MSISDN UserIdentity.Public-Identity ✓ **UserName**	Primary AVP which will be used for extracting the Routing Entity address. [A value is required.]

Figure: The 3 new AVPs are Highlighted with the Green Checks

3.9 IP Address of the Connection in the SCTP Connection Impaired Trap

3.9.1 Description

Prior to DSR 8.0, minor alarm 22103 'SCTP Connection Impaired' did not contain the ip address associated with the connection. This information will be included from DSR 8.0 onward.

SctpPathUnavailable (22103) Alarm will occurs when SCTP multi-homed connection has operationally unavailable path. The potential cause for alarm are host IP interface is down or host IP interface is unreachable from the peer or peer IP interface is down or peer IP interface is unreachable from the host. In previous version, 2103 Minor alarm will not have ip address associated with the connection. In DSR 8.0 Rel, ip address associated with the connection was included.

The alarm will be clear, when connection is operationally unavailable or all paths are operationally available.

3.10 Listen Port Updates for Peer Node

3.10.1 Description

This feature allows configuration of Peer Nodes without Listen Ports.

This will be allowed when associated Connections are in Responder mode only.

This is not allowed for Initiator and Initiator & Responder mode

If, during the insertion or updating of any Diameter connection, the Connection Mode is Initiator or Initiator & Responder and Peer Node selected don't have any Listen port (TCP, SCTP, TLS or DTLS) associated with it then error code [19890] shall be generated

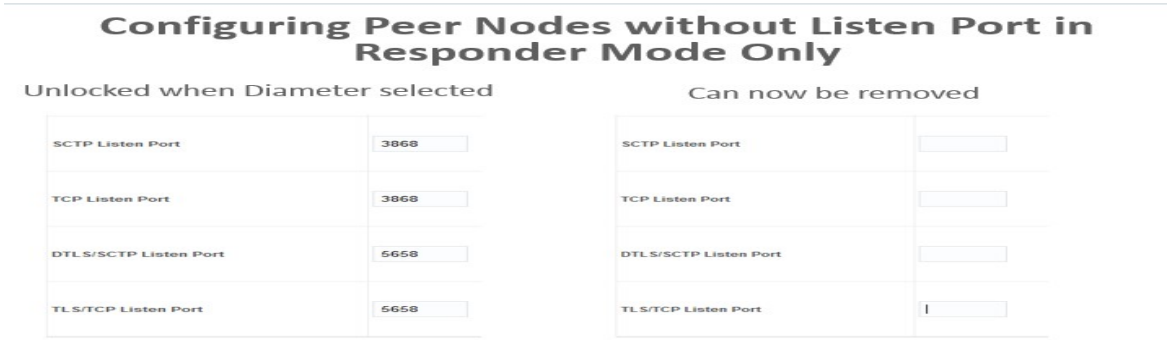


Figure: Listen Port is not configured in "Responder" Mode

3.11 Mediation Support for 2000 Counters

3.11.1 Description

In DSR 8.0, the maximum number of measurements that can be defined on the "Diameter-> Mediation-> Measurements" screen has been increased to 2000. In earlier version it was around 200.

The maximum number of mediation rules provisioned in the system at a time has been increased to 50000.

Maximum number of provisioned rules per template/rule set will depend on the template type. For a slow-search template (where at least one condition is a slow search) the maximum number of provisioned rules is 250. For a fast-search template the maximum number of provisioned rules is 2000.

3.12 Multi Server Export

3.12.1 Description

In Previous release, user allowed to securely export data to a single remote Linux based server. Collection of DSR KPI data, performance, Log Collection and others that depend on the ability to export that data from the DSR platform. Currently only one export server can be data-filled on the DSR. This data export configuration is clumsy and prone to erratic operation as the external systems try to get their intended files.

In Release 8.0 user allowed to securely export data to multiple (up to five) remote Linux based server. Five Remote Servers per NOAM and/or SOAM pair are supported. Appworks data model is increased to collect and store data for multiple remote servers

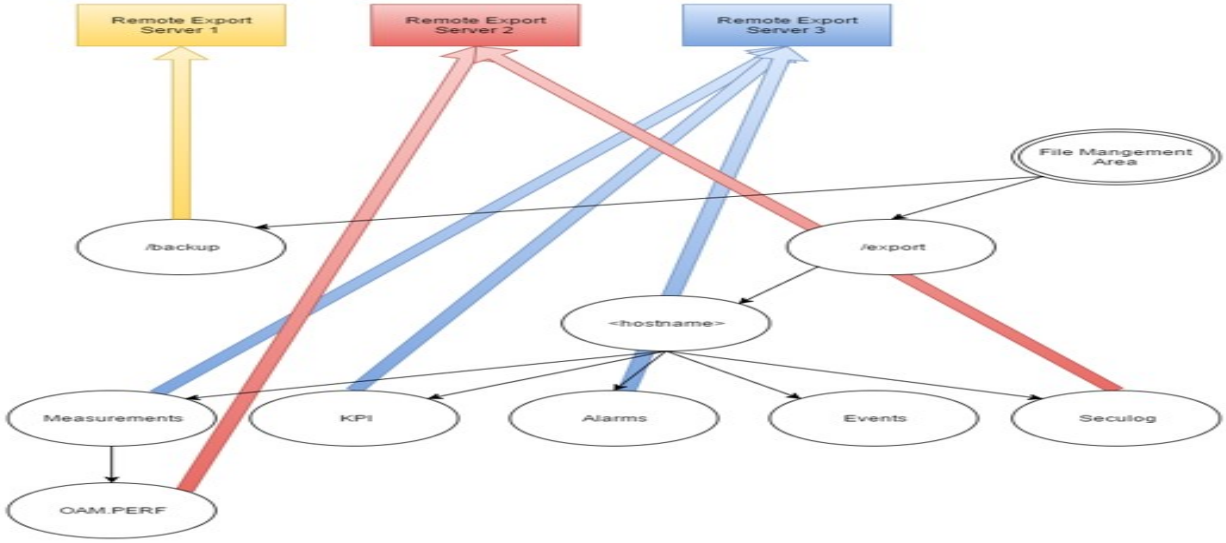


Figure: Multiple Export Servers

Types of data exported in DSR are Backups, Alarm and event history, Measurement, security logs and application data.

Export Data

- Files stored under this path: **/var/TKLC/db/filemgmt/**
- Files created by System Processes
- Files transferred according to time/day and server destination

APDE is the term to describe the automated system collection of performance data and the ability to export that data

Secure Shell is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

RSYNC is the process that copies the files from the DSR's /var/TKLC/db/filemgmt/export and /var/TKLC/db/filemgmt/backup directories to the remote servers configured.

Files are transferred by the RSYNC process - Periodically, at time/day configured per remote server. RSYNC will create directory structure on remote server. If files removed from remote server, RSYNC does not replace.

The RSYNC process only copies files from the active NOAM and SOAM servers to the remote export server.

If the NOAM or SOAM changes HA states to the standby server. All Export files will remain on the previously active server and will not be available for RSYNC to transfer. Wait for new Export files to be created on the new active server and then RSYNC will transfer those files.

3.12.2 NOAM/SOAM GUI

– Administration → Remote Servers → Data Export

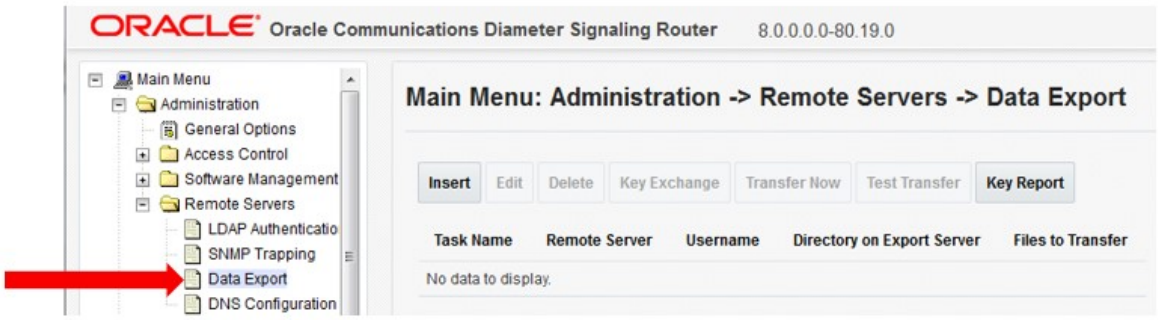


Figure: Data Export GUI

3.13 Nested Routing and Screening

3.13.1 Description

This feature improves the flexibility of ART configuration by allowing the action component of ART rules to additionally reference an ART or PRT. The action component of PRT rules can now also reference a PRT. This additional flexibility reduces overall configuration complexity and improves DSR operating efficiency by simplifying processing required for message route selection.

This feature has ability to select an ART or PRT within an ART rule and ability to select an PRT within a PRT rule. **In Routing Rules – new "Action" (Forward) has been added**. ART Rules Can Forward to both ART tables or PRT tables. But the PRT Rules can only forward to other PRT tables not ART.

This Feature Improved routing rule creation and maintenance. It Improves the ability to screen request on a per Mobile Network Operator (MNO).

Nested Routing and Screening does not require an Activate/Deactivate procedure. No administration required to Enable / Disable this Feature. The Max forward limit for this feature is 5.

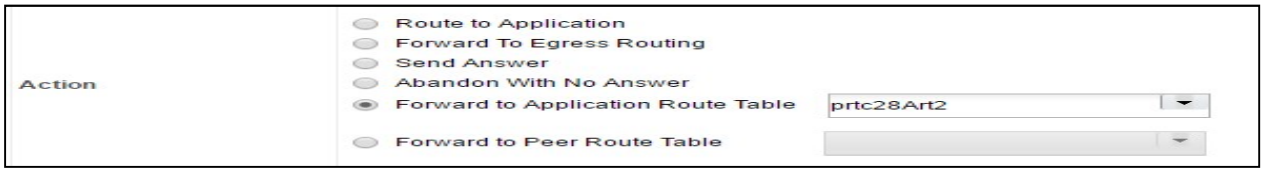


Figure: New Action Added as "Forward"

3.14 PCRF Pooling Modes

3.14.1 Description

The PCRF Pooling feature is an evolution of the Policy DRA DSR application first introduced in DSR 4.1.5. The initial version of Policy DRA supported a single pool of PCRFs at each P-DRA site over which policy Diameter signaling was distributed using the subscriber's IMSI. The PCRF Pooling feature allows for creation of multiple pools of PCRFs, which are selected using the combination of IMSI and Access Point Name (APN). This capability allows the customer to route policy Diameter signaling initiating from a given APN to a designated subset of the PCRFs that may provide specialized policy treatment using knowledge of the APN. This option that retains the functionality implemented in DSR Release 5.1.

Creating multiple Pools of PCRFs which are selected using combination of IMSI and Access Point Names (APN) provides the option of creating multiple bindings for a subscriber based on the APN of the P-GW that creates the binding capable session. Therefore, for binding dependent interface correlation, the anchor key (IMSI) and MSISDN alternate key are not sufficient to find a binding. Such interfaces when trying to find a binding using one of these keys must also include the APN using which the binding was created. This is a limitation for some customers whose binding dependent interface equipment (for e.g., the AF) does not have knowledge of the APN. The PCRF Pooling feature presents a limitation to such customers, that they cannot use IMSI or MSISDN as subscriber keys to perform binding correlation.

To overcome this limitation, the PCRF Pooling Modes feature is introduced in DSR Release 8.0 that presents the customer a choice to retain the P-DRA behavior of APN independent subscriber binding that is to route all policy Diameter signaling initiating from a given subscriber (IMSI) to a single Pool of PCRFs regardless of the APN of the P-GW. This mode (the Single Pool Mode) can be selected by customers who are limited to or otherwise desire to bind all subscriber sessions to a single PCRF and thereby correlate binding dependent sessions solely on IMSI or MSISDN. For DSR 8.0+ customers using IPv4 or IPv6 addresses for binding correlation, the Multi Pool Mode should be used.

DSR Release 8.0 presents the customer with two configuration options called – **'Single Pool Mode' and 'Multi Pool Mode'**

In Single Pool Mode, all binding capable session initiation request messages are routed to the 'Default' PCRF Pool regardless of the PCRF Pool mapped to the APN received in the request. The 'Default' PCRF Pool is created automatically. This PCRF Pool can be mapped to a PRT at every DSR site and thus, in Single Pool Mode, all new binding capable session creation requests are routed to a single pool of PCRFs defined by a PRT at each DSR site

In Multi Pool Mode, binding dependent session creation request messages if required to correlate using MSISDN or IMSI keys must include an APN. If some network operator's AF equipment does not include APN in the requests, a **Default APN** can be configured to be used to lookup up bindings using MSISDN or IMSI. The Default APN can be used by network operators who want to operate PCRF Pooling in Multi Pool Mode but have a specific set of binding dependent interface equipment that initiate policy Diameter messages, for subscribers for which the binding capable sessions were created using a single APN, without including that APN in the binding dependent request message

An example of use of the Default APN is shown in the figure below.

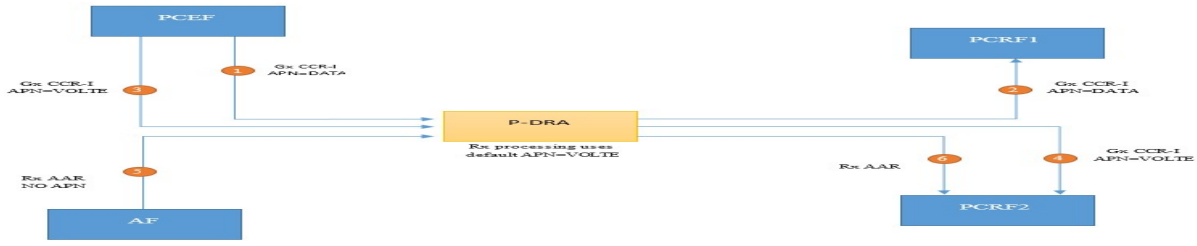


Figure: Using the Default APN

Once on the Network Wide Options GUI Screen, you will see the PCRF Pooling Mode parameter. You will select either Single Pool Mode or Multi Pool Mode. The default setting is Multi Pool Mode.

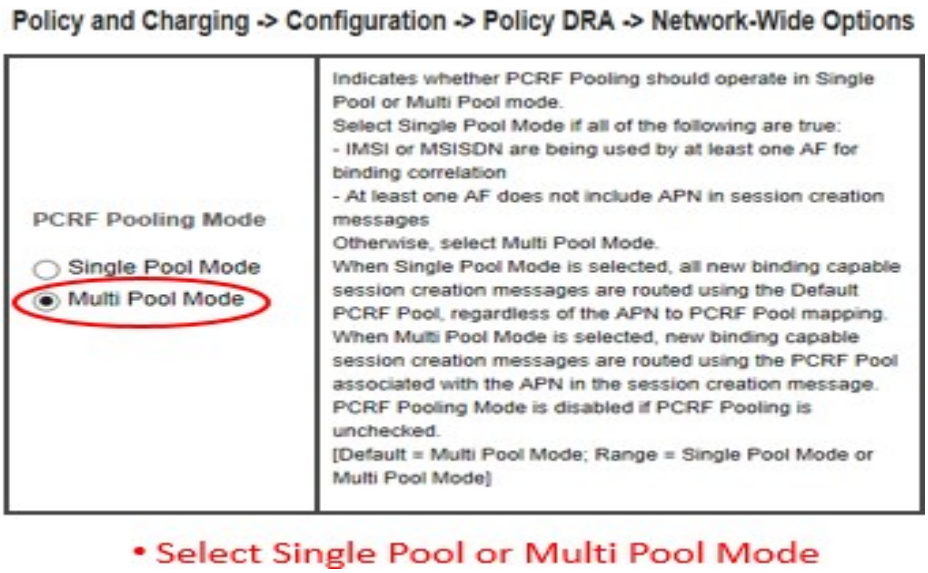


Figure: Two Radio Buttons on NOAM GUI

3.15 SDS Provisioning Log Export

3.15.1 Description

SDS provisioning is typically done from an external feed in the customer network. Some of the provisioned information in SDS may also be inserted, updated or deleted from the GUI. At present, command logging is an optional feature only available from the GUI and there is no ability to export it.

In SDS 7.1, users can view the provisioning logs of SDS data being provisioned from various sources including the GUI, Import and SOAP/XML.

Users however cannot export these provisioning logs in SDS 7.1. In This Release covers the requirements to enable the export of these provisioning logs.

The SDS provisioning log export shall not require any steps to activate or enable this feature when it is made available either via a fresh install or via upgrade.

3.16 SDS Connection System ID Field Enhancements

3.16.1 Description

One of the fields in the command log is the System ID field. This field is 8 characters wide in SDS 7.1. Eight characters tend to leave the user constrained when attempting to enter an FQDN which could be as long as 255 characters. Hence in order to provide more clarity, this field width is being increased to 255 characters.

There is a business requirement to increase the size of the System ID field to accommodate a full FQDN, which could go up to 255 characters. Since the System ID is part of the command log, this may influence the sizing of the circular table but changes to that table are considered to be implementation details. It is however expected to affect the frequency with which the export will be performed.

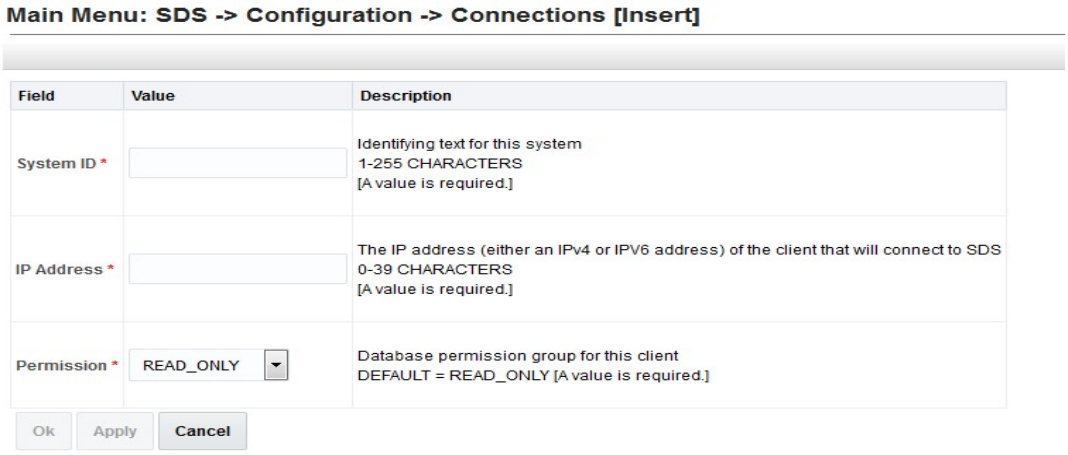


Figure - Enhancement of System Field.

3.17 Supporting More than 20 Routing Option Sets

3.17.1 Description

Routing Option Sets have been supported by DSR since release 4.0. Up to 20 Routing Option Sets were able to be provisioned.

Release 8.0 has expanded the provisioning count from 20 to 50. Routing Option Sets are collections of parameters, which influence the processing of Diameter transactions sent by Diameter Peers.

A Provisioned ROS can be assigned while configuring Peer Nodes directly or also indirectly via Transaction Configuration Sets (TCS). A TCS can be provisioned to specify a particular ROS and then the TCS can be selected during Peer Node configuration.

Routing Option Sets are provisioned within the DSR using the SOAM GUI

3.18 Excessive Request Reroute Alarm

3.18.1 Description

This Alarm alerts the Customer when excessive reroutes are occurring. This alarm is raised when the percentage of total request, that are being rerouted, is greater than the provisioned threshold for Alarm Onset.

The percentage of traffic being rerouted is scoped/calculated per DA-MP. The Alarm is cleared when the percentage falls below the Abatement threshold value

The percentage is compared to the provisioned Onset Threshold. When the current percentage is ≥ Onset, the alarm is raised

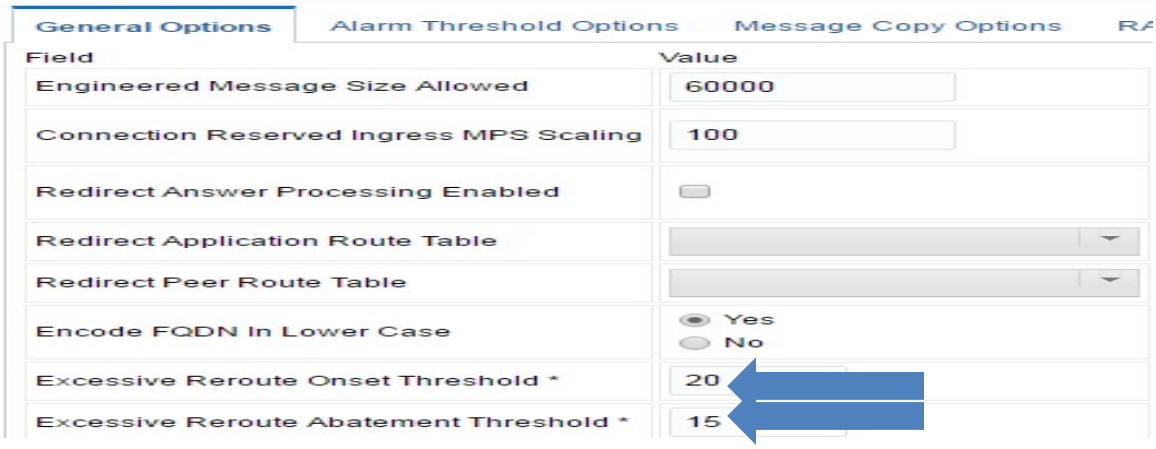


Figure: Enabling the Threshold Alarm Configuration.

4. Meal Inserts

This section summarizes the changes to Alarms, Measurements, and KPIs. The following inserts pertain to DSR release 8.0 and deltas with releases 5.1, 6.0, 7.0, 7.1, & 7.2 Alarms, Measurements, KPIs, and MIBs.

4.1 Alarms Delta (Release 8.0)

NGN-PS Feature

Alarm Name	Description	Group
MpRxNgnPsOfferedRate	DA-MP ingress NGN-PS message rate threshold crossed.	Diameter
MpNgnPsStateMismatch	DA-MP NGN-PS administrative and operational state mismatch.	Diameter
MpNgnPsDrop	DA-MP NGN-PS message discarded or rejected.	Diameter
NgnPsMsgMisrouted	NGN-PS message routed to peer DSR lacking NGN-PS support.	Diameter
NgnPsOfferedRate	Connection ingress NGN-PS request rate threshold crossed.	Diameter

<See section 4.5 and the embedded spreadsheets>

4.2 Measurements Delta (Release 8.0)

NGN-PS Feature

Measurement Name	Description
MpRxNgnPsOffered	DA-MP ingress NGN-PS messages offered.
MpRxNgnPsOfferedRateAvg	DA-MP ingress NGN-PS messages offered rate average.
MpRxNgnPsOfferedRatePeak	DA-MP ingress NGN-PS messages offered rate peak.
MpRxNgnPsAccepted	DA-MP ingress NGN-PS messages accepted.
MpRxNgnPsAcceptedRateAvg	DA-MP ingress NGN-PS messages accepted rate average.
MpRxNgnPsAcceptedRatePeak	DA-MP ingress NGN-PS messages accepted rate peak.
RxNgnPsOffered	Connection ingress NGN-PS messages offered.
RxNgnPsAccepted	Connection ingress NGN-PS messages accepted.
RxNgnPsRequestsOffered	Connection ingress NGN-PS requests offered.
MpNgnPsXactionPassAvg	DA-MP NGN-PS transaction success rate average.
MpNgnPsXactionFailPeersAvg	DA-MP NGN-PS transaction failure rate by peers average.

<See section 4.5 and the embedded spreadsheets>

4.3 KPIs (Release 8.0)

PCIMC Enhancement Feature

Priority based message ingress rate and discard via ingress control has new associated KPI metrics.

KPI Name	Description
IcRateP0	Connection ingress message rate with Priority 0
IcRateP1	Connection ingress message rate with Priority 1
IcRateP2	Connection ingress message rate with Priority 2
IcRateP3	Connection ingress message rate with Priority 3
IcRateP4	Connection ingress message rate with Priority 4

KPI Name	Description
IcDropP0	P0 ingress messages dropped for exceeding connection max MPS
IcDropP1	P1 ingress messages dropped for exceeding connection max MPS
IcDropP2	P2 ingress messages dropped for exceeding connection max MPS
IcDropP3	P3 ingress messages dropped for exceeding connection max MPS
IcDropP4	P4 ingress messages dropped for exceeding connection max MPS

NGN-PS Feature

Metric Name	Description
MpRxNgnPsOfferedRate	DA-MP ingress NGN-PS messages offered rate.

<See section 4.5 and the embedded spreadsheets>

4.4 MIB Notifications (Release 8.0)

<See section 4.5 and the embedded spreadsheets>

4.5 MEAL Snapshot for DSR 8.0

MEAL_dsr-8.0.0.0.0-80.25.0.xlsx

4.6 Meal Deltas (8.0)

MEAL_dsr-6.0.0-60.24.0-dsr-8.0.0.0.0-80.2

MEAL_dsr-7.3.0.0.0-73.18.0-dsr-8.0.0.0.0

MEAL_sds-5.0.1-50.23.0-sds-8.0.0.0.0-80

MEAL_sds-7.3.0.0.0-73.18.0-sds-8.0.0.0.0

5. Reference List

DSR 8.0 User Guides for DSR (see customer documentation)

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

Release Notices and Licensing Information User Manuals

DSR 8.0 Release Notice

DSR 8.0 Licensing Information User Manual

DSR Planning, Installation, Upgrade, and Disaster Recovery

DSR 8.0 Feature Guide

DSR 8.0 Planning Guide

DSR Hardware and Software Installation Procedure

DSR Software Installation and Configuration Procedure

DSR Software Upgrade Guide

DSR Rack Mount Server Installation Guide

DSR Rack Mount Server Disaster Recovery Guide

DSR Disaster Recovery Guide

Policy and Charging DRA Feature Activation Procedure

GLA Feature Activation Procedure

Mediation Feature Activation Procedure

FABR Feature Activation Procedure

RBAR Feature Activation Procedure

MAP-Diameter Feature Activation Procedure

DTLS Feature Activation Procedure

IPv6 Migration Guide

DSR Network Impact Report Word

DSR Security Guide

Cloud Installation and Upgrade

DSR Cloud Installation Guide
DSR Cloud Software Upgrade Guide
DSR Cloud Benchmarking Guide
DSR Cloud Disaster Recovery Guide
SDS Cloud Installation Guide
SDS Cloud Disaster Recovery Guide

Diameter Signaling Router Core Document Set

Operation, Administration, and Maintenance (OAM) Guide
Communication Agent User's Guide
Hardware Documentation Roadmap Reference
Policy and Charging Application User's Guide
Diameter User's Guide
Mediation User's Guide
Range Based Address Resolution (RBAR) User's Guide
Full Address Based Resolution (FABR) User's Guide
Session Binding Repository (SBR) User's Guide
IP Front End (IPFE) User's Guide
Alarms and KPIs Reference
Measurements Reference
Diameter Common User's Guide
MAP-Diameter IWF User's Guide
RADIUS User's Guide
SS7/SIGTRAN User's Guide
Transport Manager User's Guide
Gateway Location Application (GLA) User's Guide
Related Publications Reference PDF
DSR VM Placement and CPU Socket Pinning Tool XLSX
DSR Compliance Matrix

Integrated Diameter Intelligence Hub (IDIH) Document Set

IDIH User's Guide
IDIH Audit Viewer Administrator's Guide
IDIH Alarm Forwarding Administrator's Guide
IDIH Operations, Administration, and Maintenance Guide
IDIH ProTrace User's Guide
IDIH System Alarms User's Guide
IDIH Log Viewer Administration's Guide