Oracle® Communications

DSR Cloud Benchmarking Guide

Release 9.3.0.0.0

G56439-01

May 2026

ORACLE

Oracle Communications DSR Cloud Benchmarking Guide, Release 9.3.0.0.0

G56439-01

Contents

Preface

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

My Oracle Support

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

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request.
2. Select **3** for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:
   - For Technical issues such as creating a new Service Request (SR), select **1**.
   - For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

What's New in This Guide

This section introduces the documentation updates for Release 9.3.0.0.0.

Release 9.3.0.0.0 - G56439-01, May 2026

- Updated value of CPU and RAM utilization peak for "Relay" in the Table G-1.
- Updated value of CPU peak and RAM utilization peak for "Radius+Diameter" in the Table 3-23.
- Updated values of CPU and RAM utilization peak for "All stateful" and "All Stateful + All Stateless (total 20 countermeasures)" in the Topology of diameter security application (DSA) benchmarking section.
- Updated values of CPU and RAM utilization peak for "single server group (1 SBR(s)", 1 SBR(b)) and "four server groups (4 SBR(s), 4 SBR(b))" in the Message Flow of policy DRA benchmarking section.
- Updated values of CPU and RAM utilization peak for "DA-MP CPU Peak", "DA-MP RAM Utilization Peak", "DP CPU Peak", and "DP RAM Peak" in the Message Flow of full address based resolution (FABR - SDS) capacity section.
- Updated value of CPU Peak for "RBAR" in the Message Flow of RBAR benchmark section.
- Updated values of CPU and RAM utilization peak for "Relay" in the Message Flow of DA-MP Relay Benchmark section.
- Added DSR and vSTP VMs in the Table D-1.
- Added the IPFE and following sections:
  - Topology
  - Indicative Alarms/Events
- Added the vSTP MP HLR-Router Benchmarking and following sections:
  - #unique_29
  - Message Flow
  - Indicative Alarms/Events
- Added the vSTP MTP Routing and GTT and following sections:
  - Message Flow
  - Indicative Alarms/Events
- Added the vSTP MTP Routing and GTT Routing with MTP Screening and following sections:
  - #unique_36
  - Message Flow
  - Indicative Alarms/Events
- Added the vSTP MP Benchmarking GTT with Other Features and following sections:
  - Topology
  - Indicative Alarms/Events

Acronyms

The following tables provide information about the acronyms and the terminology used in this document.

Table Acronyms

Acronym	Description
API	Application Programming Interface
ARR	Application Route Rule
ART	Application Route Table
CM	Counter Measure
COTS	Commercial Off the Shelf
CPU	Central Processing Unit
DA-MP	Diameter Agent Message Processor
DB	Database
DP	Database Processor
DSA	Diameter Security Application
DSR	Diameter Signaling Router
EIR	Equipment Identity Register
ETG	Egress Throttle Group
FABR	Full Address Based Resolution
FQDN	Fully Qualified Domain Name
GB	Gigabyte
HDD	Hard Disk Drive
HP	Hewlett Packard
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
ID	Identification
IDIH	Integrated Diameter Intelligence Hub
IMI	Internal Message Interface
IMSI	International Mobile Subscriber Identity
I/O	Input/Output
IOP	Interoperability
IoT	Internet of Things
IP	Internet Protocol
IPCAN	Internet Protocol Connectivity Access Network
IPFE	IP Front End
KPI	Key Performance Indicator
KSM	Kernel Same-page Merging
KVM	Kernel-based virtual machine
LSI	Large Scale Integration
LTE	Long Term Evolution
MME	Mobility Management Entity
MNO	Mobile Network Operator
MP	Message Processor

Table (Cont.) Acronyms

Acronym	Description
MPS	Messages Per Second
MSISDN	Mobile Station International Subscriber Directory Number
MTC	Machine Type Communication
NIC	Network Interface Card
NOAM	Network Operations, Alarms, Measurements
NE	Network Element
OAM	Operations, Administration, and Maintenance
OCDSR	Oracle Communications Diameter Signaling Router
OCSG	Oracle Communications Services Gatekeeper
OHC	Oracle Help Center
PCRF	Policy and Charging Rules Function
PDRA	Policy Diameter Routing Agent
PRR	Peer Route Rule
PVSCSI	Paravirtual SCSI
RAM	Random Access Memory
RBAR	Range Based Address Resolution
SAS	Serial Attached SCSC
SBR	Session Binding Repository
SBR(b)	SBR – Binding database
SBR(s)	SBR – Session database
SBR(u)	SBR – Universal database
SCS/AS	Service Centralization and Continuity Application Server
SCSI	Small Computer System Interface
SDS	Subscriber Database Server
SFF	Small Form Factor
SGSN	Serving GPRS Support Node
SMS	Short Message Service
SOAM	System (nodal) Operations, Alarms, Measurements
SS7	Signaling System #7
SSD	Solid State Drive
THP	Transparent Huge Pages
TSA	Target Set Address
TTP	Troubleshooting Trigger Point
vSTP	virtual Signaling Transfer Point
UDR-NO	User Data Repository Network OAM & Provisioning
VM	Virtual Machine
VNF	Virtual Network Function
VoLTE	Voice over LTE
WAN	Wide Area Network
XMI	External Management Interface
XSI	External Signaling Interface

Table Terminology

Term	Description
1+1 Redundancy	For every 1, an additional 1 is needed to support redundant capacity. The specific redundancy scheme is not inferred. For example, active-active and active-standby.
Geo-Diverse	Refers to DSR equipment located at geographically separated sites/datacenters.
Geo-Redundant	A node at a geo-diverse location which can assume the processing load for another DSR signaling node(s).
Ingress Message Rate	A measure of the total Diameter messages per second ingressing the DSR. For this measure, a message is defined as any Diameter message that DSR reads from a Diameter peer connection independent of how the message is processed by the DSR.
Messages Per Second	A measure of the DSR Diameter message processing volume in messages per second. For this measure, a message is defined as: • DSR processing of an ingress Diameter message and either transmitting a single outgoing Diameter message or discarding the ingress message. The outgoing message may be a variant of, or a response to, the ingress message. • DSR transmission of any Diameter message, as required by DSR configuration, that is associated with incremental actions/events associated with #1 above. For example, the re-routing of a Request upon connection failure or the copying of a Request. Messages excluded from this measure are: • Diameter peer-to-peer messages: CER/CEA, DWR/DWA, and DPR/DPA • Ingress Diameter messages discarded by the DSR due to Overload controls • Answers received in response to Message Copy For the vSTP MP the MPS excludes the equivalent SSNM status management messages.
N+K Redundancy	For every N, an additional K is needed to support redundant capacity. The specific redundancy scheme is not inferred. For example, active-active, active-standby.
Node	A DSR node is a DSR signaling node (SOAM and subtending topology), an NOAM node or an SDS node. A node is synonymous with the network element (NE).
Site	A specific geographic location or datacenter where DSR application is installed.

1

Introduction

The Oracle Communications Diameter Signaling Router (OCDSR or DSR) is deployable in the cloud as a Virtual Network Function (VNF). With DSR's added flexibility of being cloud deployable, operators must be able to manage the capacity and performance of the DSR in the cloud.

This document provides:

- Recommendations on performance tuning the DSR.
- Benchmark data from our labs.
- Information on the key metrics used to manage DSR performance and capacity.

1.1 References

The following reference documents are available on Oracle Help Center (OHC):

- *Oracle Communications Diameter Signaling Router Alarms and KPIs Guide*
- *Oracle Communications Diameter Signaling Router Measurement Reference Guide*
- *Oracle Communications Diameter Signaling Router Cloud Installation Guide*
- *Oracle Communications Diameter Signaling Router Policy and Charging Application User Guide*
- *Subscriber Data Server Installation and Configuration Guide*

2

Cloud Deployable DSR

DSR can be deployed on the following platforms:

- **OpenStack based Cloud**: It provides virtualization of DSR, but does not use a cloud manager and does not co-reside with other applications. This deployment is compact and cost-effective.
- **KVM based environment**: It provides full virtualization. It assumes the DSR resources are managed by a Commercial Off-the-Shelf (COTS) cloud manager and that the DSR can be one of many applications in the cloud.

3

Benchmarking Cloud Deployable DSR

This chapter is divided into the following sections:

- Infrastructure Environment
  This section provides details of the infrastructures used for the benchmark testing, including the hardware and software. It also describes key settings and attributes, and some recommendations on configuration.
- Benchmark section for each DSR server type
  Each DSR server type is treated independently for benchmarking. Each section describes the traffic setup, and the observed results. It also provides metrics and guidelines for assessing performance on any infrastructure.

Data Usage

This data is intended to provide guidance. Recommendations may need to be adapted to the conditions in a given operator's network. Each of the following sections include metrics that provide feedback on the running performance of the application.

When planning to deploy a DSR into any cloud environment, a few steps are recommended:

- Understand the initial deployment scenario for the DSR.
  - Which features are planned?
  - How much of what type of traffic?
    This may change once deployed, and the DSR can be grown or shrunk to meet the changing needs.
- Use the **DSR Cloud Dimensioning** tool to get an estimate of the types of DSR virtual servers needed and an initial estimate of the quantity of the virtual machines and resources. Oracle Sales Consultant can run this tool based on DSR requirements:
  - The tool allows for a very detailed model to be built of your DSR requirements, including:
    - Required MPS by Diameter Application ID (S6a, Sd, Gx, Rx, so on).
    - Required DSR applications such as Full Address Based Resolution (FABR), Range Based Address Resolution (RBAR), Policy DRA (PDRA), and any required sizing information such as the number of subscribers supported for each application.
    - Any required DSR features such as Topology Hiding, Message Copy, IPSEC, or Mediation that can affect performance.
    - Network-level redundancy requirements, such as mated pair DSR deployments, where one DSR needs to support full traffic, when one of the DSRs is unavailable.
    - Infrastructure information, such as OpenStack or KVM, and Server parameters.
  - The tool then generates a recommended number of VMs for each of the required VM types.

> **Note**
>
> These recommendations are just guidelines. Since the actual performance of the DSR can vary significantly based on the details of the infrastructure.

- Based on the initial deployment scenario, determine if additional benchmarking is warranted:
  - For labs and trials, there is no need to benchmark performance and capacity if the goal of the lab is to test DSR functionality.
  - If the server hardware is different from the hardware used in this document then the performance differences can likely be estimated using industry standard metrics. This is done by comparing single-threaded processor performance of the CPUs used in this document with respect to the CPUs used in the customer's infrastructure. This approach is most accurate for small differences in hardware (for instance, different clock speeds for the same generation of Intel processors) and least accurate across processor generations where other architectural differences such as networking interfaces could also affect the comparison.
  - It is the operator's decision to determine if additional benchmarking in the operator's infrastructure is desired. Here is a few things to consider when deciding:
    - Benchmark infrastructure is similar to the operator's infrastructure, and the operator is satisfied with the benchmark data provided by Oracle.
    - Initial turn-up of the DSR is handling a relatively small amount of traffic and the operator prefers to measure and adjust once deployed.
    - Operator is satisfied with the high-availability and geo-diversity of the DSR, and is willing to risk initial overload conditions, and adjusts once the DSR is in production.
- If required, perform benchmark testing on the target cloud infrastructure. Perform benchmark only on those types of DSR servers required for the deployment.
  For example, if full address resolution is not planned, do not waste time benchmarking the SDS, SDS SOAM, or DPs.
  - When the benchmark testing is complete, observe the data for each server type, and compare it with the baseline used for the estimate from the **DSR Cloud Dimensioning** tool.
    - If the performance estimate for a given DSR function is X and the observed performance is Y, then adjust the performance for that DSR function to Y.
    - Re-calculate the resources needed for deployment based on the updated values.
- Deploy the DSR.
- Monitor the DSR performance and capacity as described later in the document. As the network changes additional resources may be required. If needed, increase the DSR resources as described later in this document.

3.1 Infrastructure Environment

This section describes the infrastructure that was used for benchmarking. In general, the defaults or recommendations for hypervisor settings are available from the infrastructure vendors.

Whenever possible the DSR recommendations align with vendor defaults and recommendations. Benchmarking was performed with the settings described in this section. Operators may choose different values, better or worse performance compared to the benchmarks might be observed. When recommendations other than vendor defaults or recommendations are made, additional explanations are included in the applicable section.

There is a sub-section included for each infrastructure environment used in benchmarking.

3.1.1 General Rules for All Infrastructures

3.1.1.1 Hyper-Threading and CPU Over-Subscription

All of the tests were conducted with Hyper-Threading enabled, and with a 1:1 subscription ratio for vCPUs in the hypervisor. The hardware used for the testing were dual-processor servers with 32 physical cores each (Oracle X9-2). Thus, each server had:

```
(2 CPUs) x (32 cores per CPU) x (2 threads per core) = 128 vCPUs
```

It is not recommended to use over-subscribed vCPUs (for instance 4:1) in the hypervisor. Not only is the performance lower, but it makes the performance more dependent on the other loads running on each physical server.

Turning off Hyper-Threading is also not recommended. There is a small increase in performance of a given VM without Hyper-Threading for a given number of vCPUs. But since the number of vCPUs for each processor drops in half without Hyper-Threading, the overall throughput for each server also drops almost by half.

The vCPU sizing for each VM is provided in the DSR VM Configurations section.

> **Note**
>
> The recommended configuration is: Hyper-Threading is enabled with 1:1 CPU subscription ratio.

CPU Technology

The CPUs in the servers used for the benchmarking were the Oracle X9-2. Servers with different processors does give different results. In general there are the following issues when mapping the results of the benchmarking data in this document to other CPUs:

- The per-thread performance of a CPU is the main attribute that determines VM performance. The number of threads is fixed in the VM sizing as shown in DSR VM Configurations section. A good metric for comparing the per-thread performance of different CPUs is the integer performance measured by the **SPECint2006 (CINT2006)** defined by SPEC.ORG.
  The mapping of **SPECint2006ratios** to DSR VM performance ratios isn't exact, but it's a good measure to determine whether a different CPU is likely to run the VMs faster or slower than the benchmark results in this document.

  Conversely CPU clock speeds are a relatively poor indicator of relative CPU performance. Within a given Intel CPU generation (v2, v3, v4, so on) there are other factors that affect per-thread performance, such as potential turbo speeds of the CPU in comparison with the cooling solution in a given server.

  Comparing between Intel CPU generations, there is a generation over generation improvement of CPU throughput in comparison with the clock speed. This means that even a newer generation chip with a slower clock speed may run a DSR VM faster.

- The processors must have enough cores that a given VM can fit entirely into a NUMA node. Splitting a VM across NUMA nodes greatly reduces the performance of that VM. The largest VM size (refer DSR VM Configurations section) is 18 vCPUs. Thus, the smallest processor that should be used is a 9-core processor. Using processors with more cores typically makes it easier to pack VMs more efficiently into NUMA nodes but should not affect individual VM CPU-related performance otherwise.
- One caveat about CPUs with very high core counts is that the user must be aware of potential bottlenecks caused by many VMs contending for shared resources such as network interfaces and ephemeral storage on the server. These tests were run on relatively large CPUs (32 physical cores for each chip), and no such bottlenecks were encountered while running strictly DSR VMs. In clouds with VMs from other applications potentially running on the same physical server as DSR VMs, or in future processor generations with much higher core counts. This potential contention for shared server resources has to be watched closely.

> **Note**
>
> The selected VM sizes should fit within a single NUMA node, for instance 9 physical cores for the VMs that required 18 vCPUs. Check the performance of the target CPU type against the benchmarked CPU using per-thread integer performance metrics.

3.1.1.2 VM Packing Rate

The DSR doesn't require or use CPU pinning. Thus, the packing of the DSR VMs onto the physical servers is under the control of OpenStack using the affinity or anti-affinity rules given in DSR VM Configurations. Typically, the VMs do not fit exactly into the number of vCPUs available in each NUMA node, leaving some un-allocated vCPUs. The ratio of the allocated to the unallocated vCPUs is the VMPacking Ratio. For instance, on a given server if 102 out of 128 vCPUs on a server were allocated by the OpenStack, that server would have a packing ratio of ~80%. The achieved packing in a deployment depends on a lot of factors, including the mix of large VMs (DA-MPs, SBRs) with the smaller VMs, and whether the DSR is sharing the servers with other applications that have a lot or large or small VMs.

When planning the number of physical servers required for an DRS a target packing ratio of 80% is a good planning number. A packing ratio of 100% is hard to achieve and may affect the performance numbers shown in the benchmarks. Some amount of server capacity is necessary to run the Host OS for the VMs. While performing functions such as interrupt handling, a packing ratio of 95% or lower is desirable.

> **Note**
>
> When planning for physical server capacity a packing ratio of 80% is a good guideline. Packing ratios of greater than 95% might affect the benchmark numbers since there aren't sufficient server resources to handle the overhead of Host OSs.

3.1.1.3 Infrastructure Tuning

The following parameters should be set in the infrastructure to improve DSR VM performance. The instructions for setting them for a given infrastructure is including the *DSR Cloud Installation Guide*.

- Txqueuelen: The default of 500 is too small. Recommendation is to set this parameter to 120000.

  - Tuned on the compute hosts.
  - Default value of 500 is too small. Our recommendation is to set to 120000. This increases the network throughput of a VM.
- Ring buffer increase on the physical Ethernet interfaces: The default is too small. The recommendation is to set both receive and transmit values to 4096.
- Multiqueue: Multiqueue should be enabled on any IPFE VMs to improve performance.

> **Note**
>
> Refer to instructions in the *DSR Cloud Installation Guide*.

3.1.2 KVM (QEMU)/Oracle X9-2 – Infrastructure Environment

There are a number of settings that affect performance of the hosted virtual machines. A number of tests were performed to maximize the performance of the underlying virtual machines for the DSR application.

Host Hardware

- Oracle Server X9-2
  - CPU Model: Intel(R) Xeon(R) Platinum 8358 CPU @ 2.60GHz
  - 2 CPUs
  - 32 physical cores per CPU
  - RAM: 768 GB
  - HDD: 3.8 TB of NVMe storage (with Software RAID-1 configured)
  - NIC
  - Oracle Quad Port 10G Base-T Adapter

Hypervisor

- QEMU-KVM Version: QEMU 6.2.0, libvirt 8.0.0, API QEMU 8.0.0

3.1.2.1 Device Drivers

VirtIO is a virtualizing standard for network and disk device drivers where just the guest's device driver knows it is running in a virtual environment and cooperates with the hypervisor. This enables guests to get high performance network and disk operations and gives most of the performance benefits of para-virtualization.

Vhost-net provides improved network performance over Virtio-net by totally by passing QEMU as a fast path for interruptions. The vhost-net runs as a kernel thread and interrupts with less overhead providing near native performance. The advantages of using the vhost-net approach are reduced copy operations, lower latency, and lower CPU usage.

> **Note**
>
> The VirtIO driver was used for Test Bed setting.

3.1.2.2 BIOS Power Settings

Typical BIOS power settings (hardware vendor dependent, see relevant infrastructure hardware vendor documentation for details) provide three options for power settings:

- Power Supply Maximum: The maximum power the available PSUs can draw.
- Allocated Power: The power is allocated for installed and hot pluggable components.
- Peak Permitted: The maximum power the system is permitted to consume.

> **Note**
>
> Set to **Allocated Power** or equivalent for your Hardware vendor.

Disk Image Formats

The preferred disk image file formats available when deploying a KVM virtual machine:

- QCOW2: Disk format supported by the QEMU emulator that can expand dynamically and supports Copy-on-write.

QCOW2 provides a number of benefits, such as:

- Smaller file size, even on file systems which don’t support holes (such as, sparse files)
- Copy-on-write support, where the image only represents changes made to an underlying disk image
- Snapshot support, where the image can contain multiple snapshots of the images history

Test Bed Setting: QCOW2

3.1.2.3 Guest Caching Modes

The operating system maintains a page cache to improve the storage I/O performance. With the page cache, write operations to the storage system are considered completed after the data has been copied to the page cache. Read operations can be satisfied from the page cache if the data requested is in the cache. The page cache is copied to permanent storage using fsync. Direct I/O requests bypass the page cache. In the KVM environment, both the host and guest operating systems can maintain their own page caches, resulting in two copies of data in memory.

The following caching modes are supported for KVM guests:

- Writethrough: I/O from the guest is cached on the host but written through to the physical medium. This mode is slower and prone to scaling problems. Best used for a small number of guests with lower I/O requirements. Suggested for guests that do not support a writeback cache (such as, Red Hat Enterprise Linux 5.5 and earlier), where migration is not needed.
- Writeback (Selected): With caching set to writeback mode, both the host page cache and the disk write cache are enabled for the guest. Due to this, the I/O performance for applications running in the guest is good, but the data is not protected in a power failure. As a result, this caching mode is recommended only for temporary data where potential data loss is not a concern.
- None: With caching mode set to none, the host page cache is disabled, but the disk write cache is enabled for the guest. In this mode, the write performance in the guest is optimal

because write operations bypass the host page cache and go directly to the disk write cache. If the disk write cache is battery-backed, or if the applications or storage stack in the guest transfer data properly (either through fsync operations or file system barriers), then data integrity can be ensured. However, because the host page cache is disabled, the read performance in the guest would not be as good as in the modes where the host page cache is enabled, such as write through mode.

- Unsafe: The host may cache all disk I/O, and sync requests from guest are ignored.

Caching mode None is recommended for remote NFS storage, because direct I/O operations (O_DIRECT) perform better than synchronous I/O operations (with O_SYNC). Caching mode None effectively turns all guest I/O operations into direct I/O operations on the host, which is the NFS client in this environment. Moreover, it is the only option to support migration.

> **Note**
>
> For Test Bed Setting, set Caching Mode to Writeback.

3.1.2.4 Memory Tuning Parameters

Swappiness

The swappiness parameter controls the tendency of the kernel to move processes out of physical memory and onto the swap disk. Since disks are much slower than RAM, this can lead to slower response times for system and applications if processes are too aggressively moved out of memory.

- vm.swappiness = 0: The kernel swaps only to avoid an out of memory condition.
- vm.swappiness = 1: Kernel version 3.5 and over, as well as kernel version 2.6.32-303 and over; Minimum amount of swapping without disabling it entirely.
- vm.swappiness = 10: This value is recommended to improve performance when sufficient memory exists in a system.
- vm.swappiness = 60: Default
- vm.swappiness = 100: The kernel swaps aggressively

> **Note**
>
> For Test Bed Setting, set `vm.swappiness` to 10.

Kernel Same Page Merging

Kernel Same-page Merging (KSM), used by the KVM hypervisor, allows KVM guests to share identical memory pages. These shared pages are usually common libraries or other identical, high-use data. KSM allows for greater guest density of identical or similar guest operating systems by avoiding memory duplication. KSM enables the kernel to examine two or more already running programs and compare their memory. If any memory regions or pages are identical, KSM reduces multiple identical memory pages to a single page. This page is then marked copy-on-write. If the contents of the page is modified by a guest virtual machine, a new page is created for that guest.

This is useful for virtualization with KVM. When a guest virtual machine is started, it only inherits the memory from the host qemu-kvm process. Once the guest is running, the contents of the guest operating system image can be shared when guests are running the same operating system or applications. KSM allows KVM to request that these identical guest memory regions be shared.

KSM provides enhanced memory speed and utilization. With KSM, common process data is stored in cache or in main memory. This reduces cache misses for the KVM guests, which can improve performance for some applications and operating systems. Secondly, sharing memory reduces the overall memory usage of guests, which allows for higher densities and greater utilization of resources.

The following 2 services controls KSM:

- KSM Service: When the KSM service is started, KSM shares up to half of the host system's main memory. Start the KSM service to enable KSM to share more memory.
- KSM Tuning Service: The ksmtuned service loops and adjusts KSM. The ksmtuned service is notified by libvirt, when a guest virtual machine is created or destroyed

> **Note**
>
> For Test Bed Setting, set KSM service to active and ensure ksmtuned service running on KVM hosts.

Zone Reclaim Mode

When an operating system allocates memory to a NUMA node, but the NUMA node is full, the operating system reclaims memory for the local NUMA node rather than immediately allocating the memory to a remote NUMA node. The performance benefit of allocating memory to the local node outweighs the performance drawback of reclaiming the memory. However, in some situations reclaiming memory decreases performance to the extent that the opposite is true. In other words, in these situations, allocating memory to a remote NUMA node generates better performance than reclaiming memory for the local node.

A guest operating system causes zone to reclaim in the following situations:

- When you configure the guest operating system to use huge pages.
- When you use KSM to share memory pages between guest operating systems.

Configuring huge pages and running KSM are both best practices for KVM environments. Therefore, to optimize performance in KVM environments, it is recommended to disable zone reclaim.

> **Note**
>
> For Test Bed Setting, disable zone reclaim.

Transparent Huge Pages

Transparent huge pages (THP) automatically optimize system settings for performance. By allowing all free memory to be used as cache, performance is increased.

> **Note**
>
> For Test Bed Setting, enable THP.

3.2 Benchmark Testing

The way the testing was performed and the benchmark test set-up is the same for each benchmark infrastructure. Each section describes the common set-up and procedures used to benchmark, and then the specific results for the benchmarks are provided for each benchmark infrastructure.

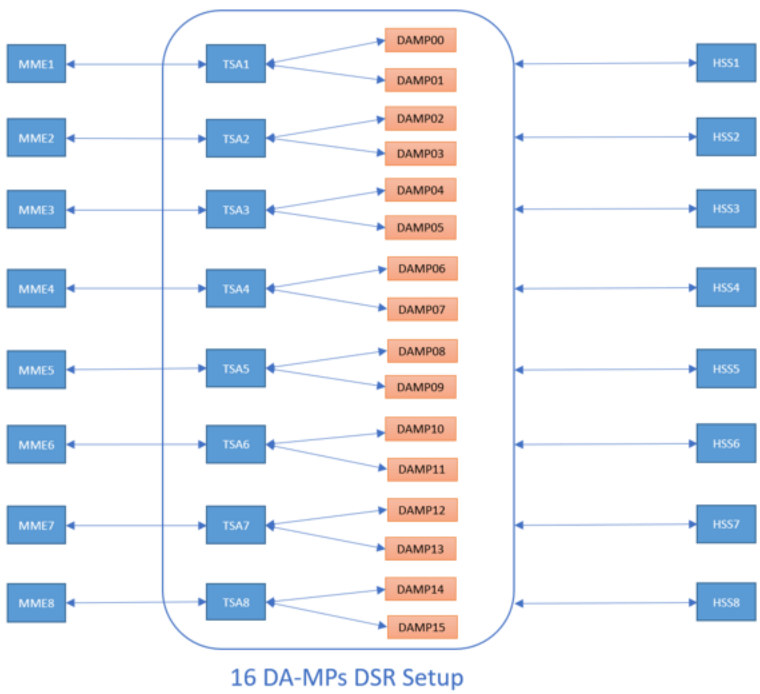
3.2.1 DA-MP Relay Benchmark

This benchmarking case illustrates conditions for an overload of a DSR DA MP.

3.2.1.1 Topology

The below figure illustrates the logical topology used for this testing. Diameter traffic is generated by an MME simulator and sent to an HSS simulator.

Figure 3-1 DA-MP Relay Testing Topology

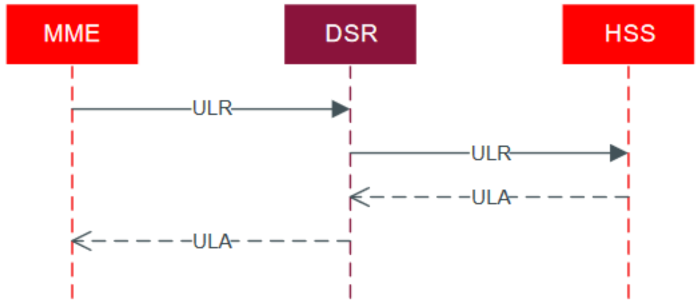


The `dsr.cpu` utilization can be further increased to higher levels by means of configuration changes with DOC/CL1/CL2 discards set to 0 and multi-queuing enabled on all hosts. With this configuration, it must be noted that all the discards are at one step CL3 for all incoming and outgoing messages.

3.2.1.2 Message Flow

The following image illustrates the Message sequence for the benchmark case.

Figure 3-2 DA-MP Relay Message Sequence



The following table summarizes the DSR relay benchmarking results:

Table 3-1 Relay Performance Benchmarking on 16 DA-MPs DSR Setup

Scenario	Call Flow Model	DSR MPS Achieved	DA-MP Flavor	DA-MP Profile	Avg Msg Size	CPU Peak	RAM Utilization Peak
Relay	100% Relay	288K	12 vCPU (Regular)	30K_MPS	2.0 K	17%	26%
Relay (with Multique enable, configuration set to DOC/CL1/CL2 discards set to 0 and multi queuing enabled on all hosts)	100% Relay	576K	12 vCPU (Regular)	40K_MPS_FABR	2.0 K	36%	32%
Relay	100% Relay	560K	18 vCPU (Large)	35K_MPS	2.0 K	19%	23%

3.2.1.3 Indicative Alarms or Events

During benchmark testing the following alarms or events were observed when it reaches congestion.

Table 3-2 DA-MP Relay Alarms or Events

Number	Severity	Server	Name	Description
22008	Info	DA-MP	Orphan Answer Response Received	An answer response was received for which no pending request transaction existed resulting in the Answer message being discarded.
22201	Minor	DA-MP	MpRxAllRate	DA-MP ingress message rate threshold crossed.
22221	Minor	DA-MP	Routing MPS Rate	Message processing rate for this DA-MP is approaching or exceeding its engineered traffic handling capacity.

Table 3-2 (Cont.) DA-MP Relay Alarms or Events

Number	Severity	Server	Name	Description
22225	Minor	DA-MP	MpRxDiamAllLen	DA-MP diameter average ingress message length threshold crossed.

3.2.2 RBAR Benchmark

Range Based Address Resolution (RBAR) is a DSR-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.

A Routing Entity can be:

- A User Identity:
  - International Mobile Subscriber Identity (IMSI)
  - Mobile Subscriber Integrated Services Digital Network (Number) (MSISDN)
  - IP Multimedia Private Identity (IMPI)
  - IP Multimedia Public Identity (IMPU)
- An IP Address associated with the User Equipment:
  - IPv4 (based upon the full 32-bit value in the range of 0x00000000 to 0xFFFFFFFF)
  - IPv6-prefix (1 to 128 bits)
- A general-purpose data type: UNSIGNED16 (16-bit unsigned value)

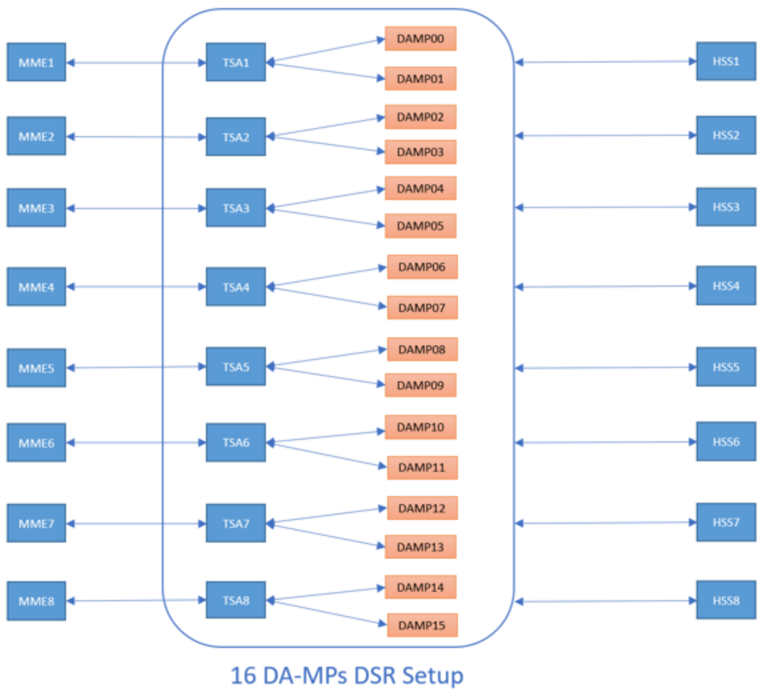
Routing resolves to a Destination that can be configured with any combination of a Realm and Fully Qualified Domain Name (FQDN); Realm-only, FQDN-only, or Realm and FQDN.

When a message successfully resolves to a destination, RBAR replaces the destination information (Destination-Host and/or Destination-Realm) in the ingress message with the corresponding values assigned to the resolved destination and forwards the message to the (integrated) Diameter Relay Agent for egress routing into the network.

3.2.2.1 Topology

The following figure illustrates the logical topology used for this testing. Diameter traffic is generated by an MME simulator and sent to an HSS simulator.

Figure 3-3 RBAR Testing Topology



3.2.2.2 Message Flow

The following image illustrates the Message sequence for this benchmark case.

Figure 3-4 DA-MP RBAR Message Sequence

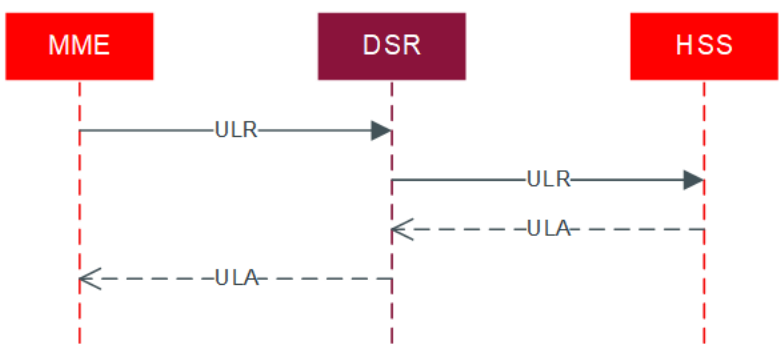


Table 3-3 RBAR Performance Benchmarking on 16 DA-MPs DSR Setup

Scenario	Call Flow Model	DSR MPS Achieved	DA-MP Flavor	DA-MP Profile	Avg Msg Size	CPU Peak	RAM Utilization Peak
RBAR	100% RBAR	16K/MP	12 vCPU (Regular)	30K_MPS	2.0 K	20%	25%

Table 3-3 (Cont.) RBAR Performance Benchmarking on 16 DA-MPs DSR Setup

Scenario	Call Flow Model	DSR MPS Achieved	DA-MP Flavor	DA-MP Profile	Avg Msg Size	CPU Peak	RAM Utilization Peak
RBAR Enhancement (Total Rules Configured are 2500 and Total Rules Matching are 320)	100% RBAR Enhancement	224 (14K/MP)	12 vCPU (Regular)	30K_MPS	2.0K	20%	26%

3.2.2.3 Indicative Alarms or Events

During benchmark testing, the following alarms or events are observed when congestion occurs.

Table 3-4 DA-MP RBAR Alarms or Events

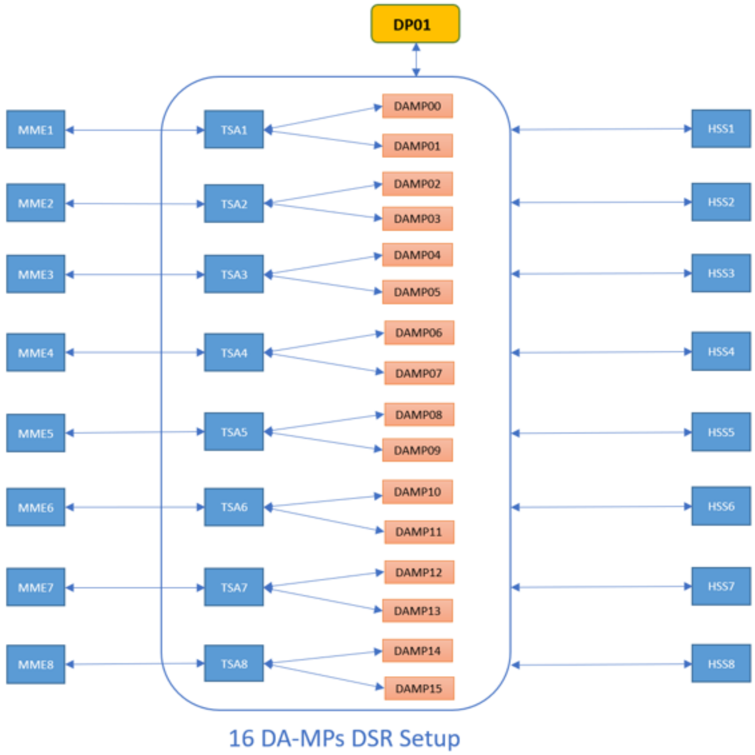
Number	Severity	Server	Name	Description
22004	Info	DA-MP	Maximum pending transactions allowed exceeded	Routing attempted to select an egress transport connection to forward a message but the maximum number of allowed pending transactions queued on the connection has been reached.
22008	Info	DA-MP	Orphan Answer Response Received	An answer response was received for which no pending request transaction existed resulting in the Answer message being discarded.
22225	Minor	DA-MP	MpRxDiamAllLen	DA-MP diameter average ingress message length threshold crossed.

3.2.3 Full Address Based Resolution (FABR - SDS) Capacity

The FABR application adds a Database Processor (DP) server to perform database lookups with a user defined key (IMSI, MSISDN, or Account ID and MSISDN or IMSI). If the key is contained in the database, the DP returns the realm and FQDN associated with that key. The returned realm and FQDN can be used by the DSR Routing layer to route the connection to the desired endpoint. Since there is additional work done on the DA-MP to query the DP, running the FABR application has an impact on the DA-MP performance. This section contains the performance of the DA-MP while running FABR as well as benchmark measurements on the DP itself.

3.2.3.1 Topology

Figure 3-5 SDS DP Testing Topology



SDS DB Details

The SDS database was first populated with subscribers. This population simulates real-world scenarios likely encountered in a production environment and ensure the database is of substantial size to be queried against.

- SDS DB Size: 300 million routing entities (150 million MSISDNs or 150 million IMSIs)
- AVP Decoded: User-Name for IMSI

SDS profile (Large) enhances the capacity of SDS FABR database to 780 million routing entities. The Large profile is defined in DSR VM Configurations based on the below 780 million entry configuration:

- 260 million subscribers having 2 IMSI, 1 MSISDN = 780 million routing entities
- IMSI = 15 bytes
- MSISDN = 10 bytes

3.2.3.2 Message Flow

Figure 3-6 SDS DP Message Sequence

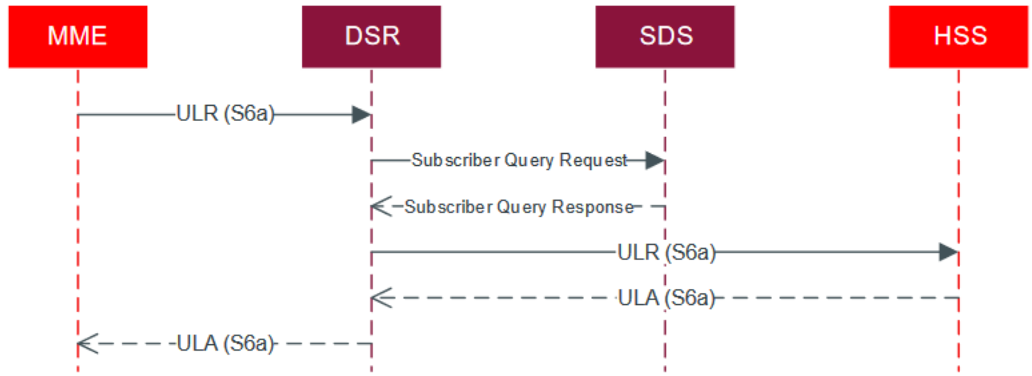


Table 3-5 SDS DP Performance Benchmarking using one SDS DP

Scenario	Call Flow Model	DP MPS Achieved	DA-MP MPS Achieved	DA-MP Flavor	DA-MP Profile	Avg Msg Size	DA-MP CPU Peak	DA-MP RAM Utilization Peak	DP CPU Peak	DP RAM Peak
FABR	100% FABR	80K	160K	12 vCPU (Regular)	30K_MPS	2.0K	23%	24%	33%	38%

3.2.3.3 Indicative Alarms or Events

Table 3-6 SDS DP Alarms or Events

Number	Severity	Server	Name	Description
22225	Minor	DA-MP	MpRxDiamAllLen	DA-MP diameter average ingress message length threshold crossed.

3.2.4 Full Address Based Resolution (FABR-UDR) Capacity

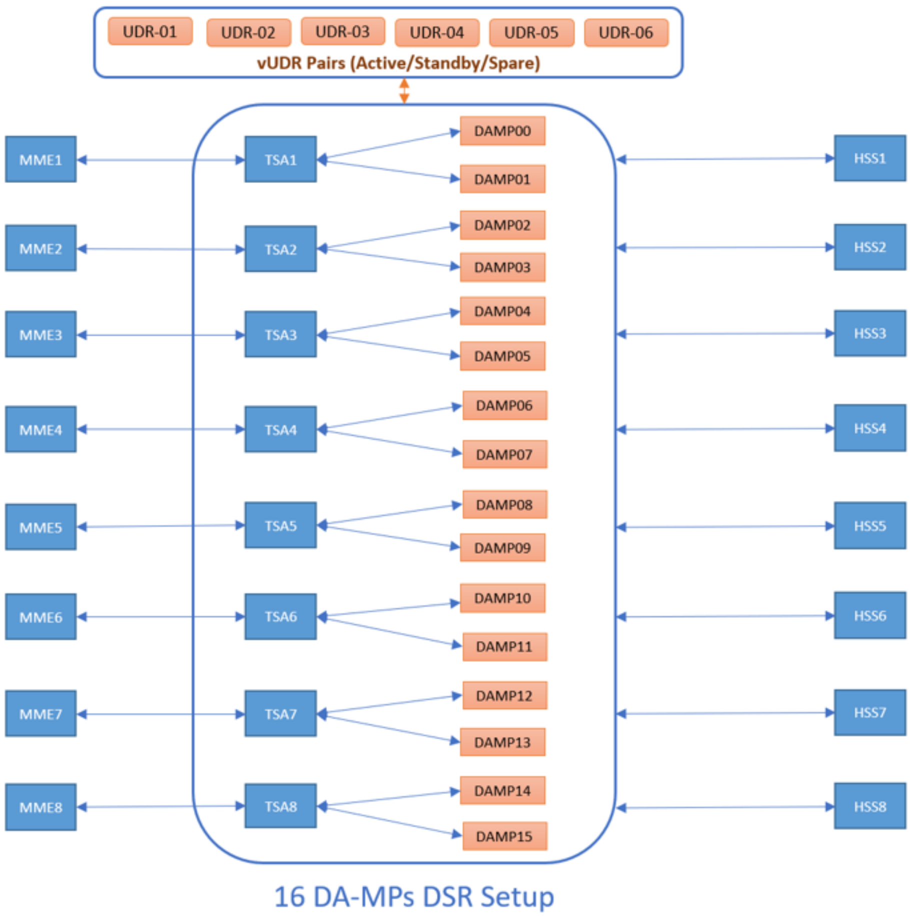
The FABR is a DSR application that provides an enhanced DSR routing capability to enable network operators to resolve the designated Diameter server (IMS HSS, LTE HSS PCRF, OCS, OFCS, and AAA) addresses based on individual user identity addresses in the incoming Diameter request messages. It offers enhanced functionalities with User Data Repository (UDR), which is used to store subscriber data. FABR routes the message as a Diameter Proxy Agent based on request message parameter content.

FABR use the services of the Diameter Plug-In for sending and receiving Diameter messages from or to the network. It uses Communication Agent to interact with off-board data repository

(UDR) for address resolution. This section contains the performance of the DA-MP while running FABR.

3.2.4.1 Topology

Figure 3-7 FABR with UDR Testing Topology



UDR DB Details

The UDR database was first populated with subscribers. This population simulates real-world scenarios likely encountered in a production environment and ensure the database is of substantial size to be queried against.

- UDR DB Size: Tested with 40 Million records
- AVP Decoded: User-Name for IMSI

Following UDR profile is used for benchmarking.

Table 3-7 UDR Profile

vCPU	RAM (GB)	HDD (GB)
18	70	450

3.2.4.2 Message Flow

Figure 3-8 FABR with UDR Message Sequence

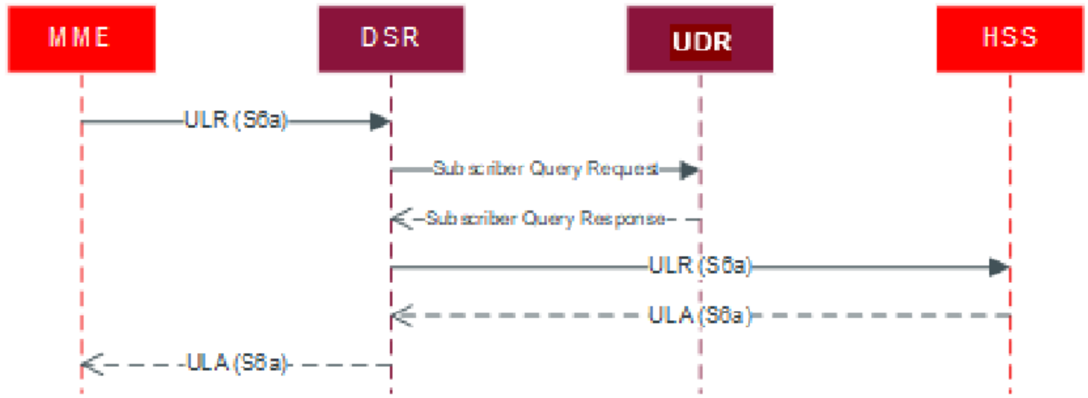


Table 3-8 FABR with UDR Performance Benchmarking on 16 DA-MPs DSR Setup

Scenario	Call Flow Model	DSR MPS Achieved	DA-MP Flavor	DA-MP Profile	Avg Msg Size	CPU Peak	RAM Utilization Peak
FABR + Relay	70% FABR + 30% Relay	288K (18K/MP)	12 vCPU (Regular)	30K_MPS	2.0 K	39%	27%

3.2.4.3 Indicative Alarms or Events

Table 3-9 FABR with UDR Alarms or Events

Number	Severity	Server	Name	Description
19825	Minor/Major/ Critical	DA-MP	Communication Agent Transaction Failure Rate	The number of failed transactions during the sampling period has exceeded the configured thresholds.
19832	Info	DA-MP	Communication Agent Reliable Transaction Failed	Failed transaction between servers result in normal maintenance actions, overload conditions, software failures, or equipment failures.
22201	Minor	DA-MP	MpRxAllRate	DA-MP ingress message rate threshold crossed.
22221	Minor	DA-MP	Routing MPS Rate	Message processing rate for this DA-MP is approaching or exceeding its engineered traffic handling capacity.
22606	Info	DA-MP	Database or DB connection error	FABR application received service notification indicating Database (DP) or DB connection (COM Agent) Errors (DP timeout, errors or COM Agent internal errors) for the sent database query.

3.2.5 Policy DRA (PDRA) Benchmarking

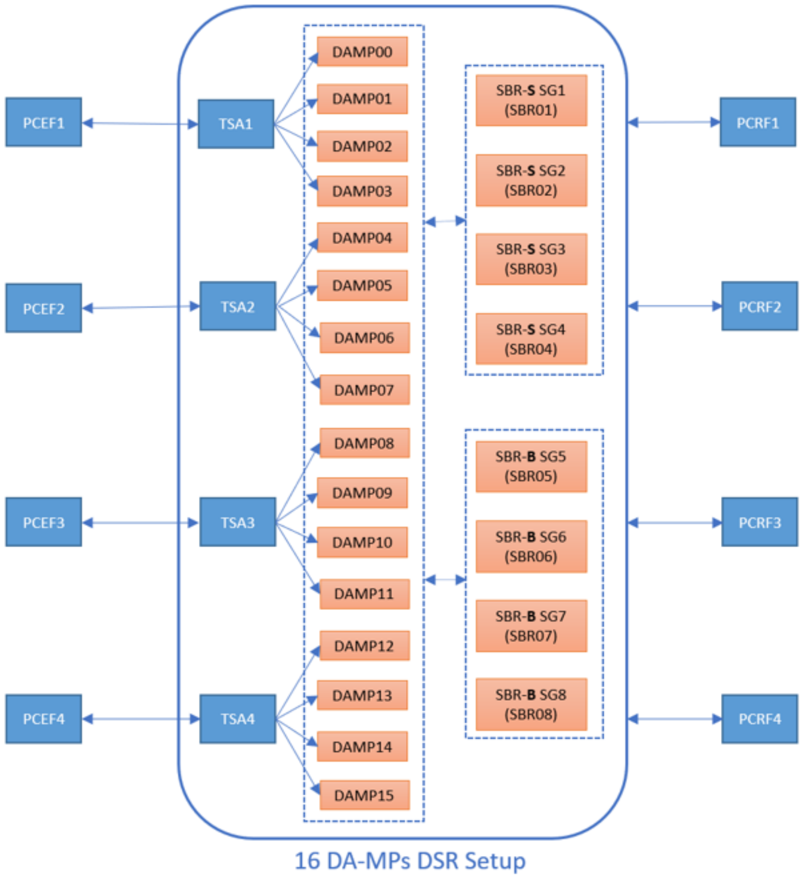
The Policy DRA (PDRA) application adds two additional database components, the SBR(session) (SBR-s) and the SBR (binding) (SBR-b). The DA-MP performance was also measured since the PDRA application puts a different load on the DA-MP than either running Relay or FABR traffic. There are two sizing metrics when determining how many SBR-s or SBR-g server groups (for example, horizontal scaling units) are required. The first is the MPS traffic rate seen at the DA-MPs. This is the metric that is benchmarked in this document. The second factor is the number of bindings (SBR-b) or sessions (SBR-s) that can be supported. This session or binding capacity is set primarily by the memory sizing of the VM and is fixed at a maximum of 16 million per SBR from the DSR 8.3 release. The number of bindings and sessions required for a given network are customer dependent. But a good starting place for engineering is to assume:

- The number of bindings is equal to the number of subscribers supported by the PCRFs.
- The number of sessions is equal to number of subscribers times the number of IPCAN sessions required on average for each subscriber. For instance, a subscriber might have one IPCAN session for LTE, and one for VoLTE.

> **Note**
>
> The number of sessions is equal to or greater than the number of bindings.

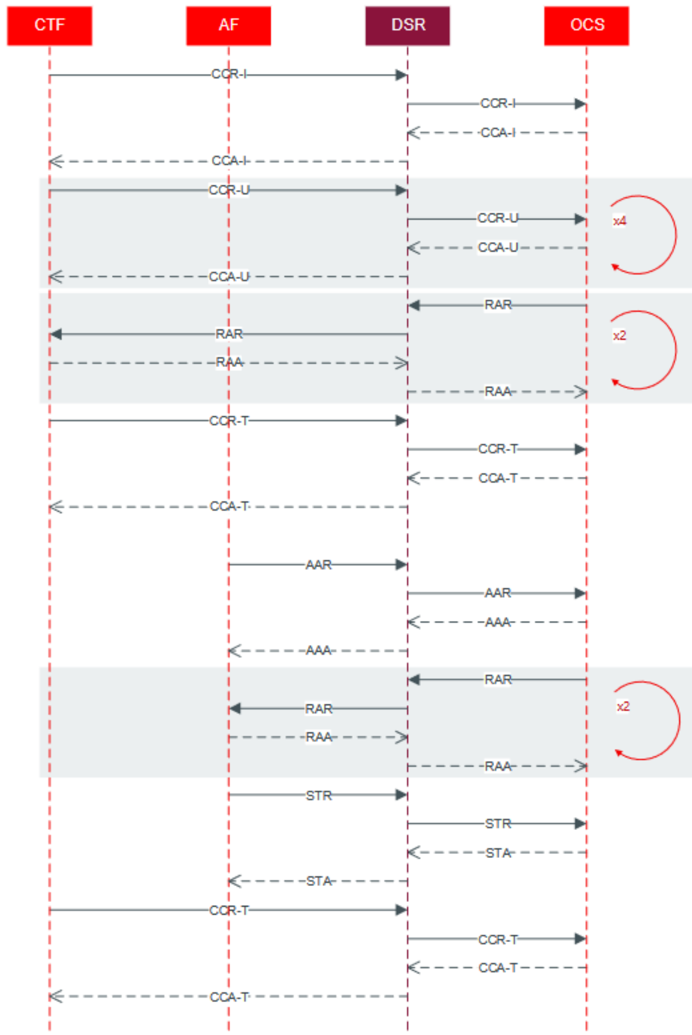
3.2.5.1 Topology

Figure 3-9 SBR Testing Topology



3.2.5.2 Message Flow

Figure 3-10 PDRA Message Sequence



The following table shows the call model used for the testing. The message distribution is Oracle's baseline benchmarking may differ significantly from customer distributions based on factors such as the penetration of LTE support in comparison with VoLTE support. The traffic details shows the configured PDRA options. For more details on these options, see *Oracle Communications Diameter Signaling Router Policy and Charging Application User Guide*.

Table 3-10 PDRA Test Call Model

Messages			Traffic Details	
Message	**Count**	**Distribution**	**Message**	**Distribution**
CCR-I, CCA-I	1	7.14%	Gx with MSISDN Alternative Key, Gx Topology Hiding	100%

Table 3-10 (Cont.) PDRA Test Call Model

Messages			Traffic Details	
Message	**Count**	**Distribution**	**Message**	**Distribution**
CCR-U, CCA-U	3	21.42%	Gx Topology Hiding	100%
CCR-T, CCA-T	1	7.14%	Gx Topology Hiding	100%
Gx RAR, RAA	3	21.42%	Gx Topology Hiding	100%
AAR, AAA Initial	2	14.29%	Rx Topology Hiding	100%
STR, STA	2	14.29%	Rx Topology Hiding	100%
Rx RAR, RAA	2	14.29%	Rx Topology Hiding	100%

Table 3-11 PDRA Performance Benchmarking on 16 DA-MPs DSR Setup

Scenario	Call Flow Model	SBR MPS Achieved	DA-MP Flavor	DA-MP Profile	Avg Msg Size	DA-MP CPU Peak	RAM Utilization Peak
Single Server group (1 SBR(s), 1 SBR(b))	100% PDRA	50K	12 vCPU (Regular)	30K_MPS	600	21%	24%
Two Server groups(2 SBR(s), 2 SBR(b))	100% PDRA	100K	12 vCPU (Regular)	30K_MPS	600	22%	25%
Four Server groups (4 SBR(s), 4 SBR(b))	100% PDRA	200K	12 vCPU (Regular)	30K_MPS	600	23%	23%

Note

The PDRA is tested with 100K MPS traffic using 4 DAMPs (Regular Profile), with each session or binding SBRs configured for 2 server groups (1 set). To reach 400K MPS traffic, an infrastructure setup consisting of 4 sets of the specified 2-server group SBR configuration is required.

3.2.5.3 Indicative Alarms or Events

Table 3-12 PDRA Alarms or Events

Number	Severity	Server	Name	Description
22716	Info	SBR	SBR Audit Statistics Report	SBR Audit Statistics Report

3.2.6 Diameter Security Application (DSA) Benchmarking

Counter measures are applied for benchmarking, for ingress messages received from external foreign network and for egress messages sent to external foreign network. Different counter measure profiles can be created for different IPX or roaming partners by enabling or disabling counter measures individually for different IPX provider or roaming partner Diameter Peers.

Enabling DSA Application (DSA) Benchmarking

DSA application is enabled on DA-MP and it uses vUDR to store context information.

3.2.6.1 Topology

Figure 3-11 DSA Testing Topology

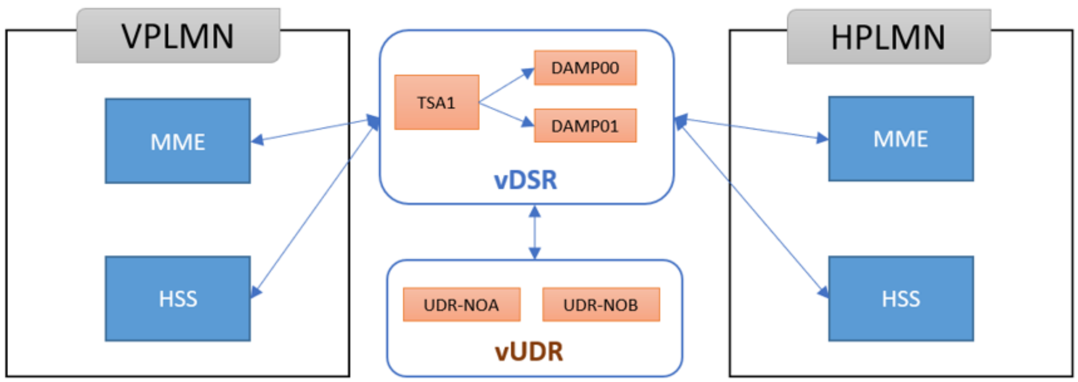
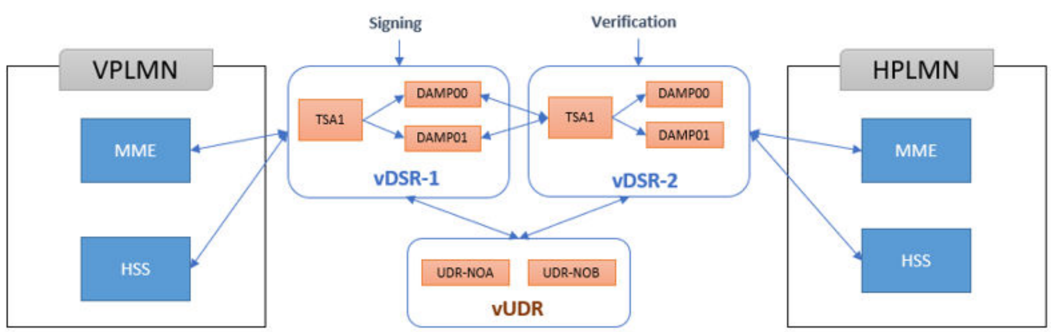


Figure 3-12 DSA Testing Topology with DESS Feature



The following stateful and stateless counter measure application configuration and the modes of operations used in benchmarking tests.

Table 3-13 Stateful and Statelss Counter Measures

Application Configuration Data		General Options Settings	
Table Name	**Count of Configured Entries**	**Options**	**Values**
AppCmdCst_Config	2	Opcodes Accounting	Disabled
AppIdWL_Config	1	Max. UDR Queries per Message	5

Table 3-13 (Cont.) Stateful and Statelss Counter Measures

Application Configuration Data		**General Options Settings**	
Table Name	**Count of Configured Entries**	**Options**	**Values**
AVPInstChk_Config	48	Max. Size of Application State	4800
Foreign_WL_Peers_Cfg_Sets	14	Logging of Vulnerable Messages	Enabled
MCC_MNC_List	11		
MsgRateMon_Config	1		
Realm_List	6		
Security_Countermeasure_Config	19		
SpecAVPScr_Config	1	**Application Threads**	
System_Config_Options	1	Request	6
TimeDistChk_Config	2000	Answer	4
TTL_Config	5	SbrEvent	4
VplmnORCst_Config	1	AsyncEvent	2
TimeDistChk_Country_Config	2		
TimeDistChk_Exception_List	0		
TimeDistChk_Continent_Config	15		
VplmnORCst_Config	1		
RealmIMSICst_Config	210		
Exception_Rule_Config	0		
All Exception Types Table • IMSI_Exception_Config • MCC_MNC_Exception_Config • Origin_Host_Exception_Config • Realm_Exception_Config • VPLMN_ID_Exception_Config	0		

> **Note**
>
> The following error is received during performance run, if the call rate is more than 1.7k in each MP DSA:
>
> ```
> UDR Internal Error: Create record failed. Error Code = SendError
> ```
>
> This is caused due to comagent connection getting timeout due to ttl expired.
>
> ```
> Communication Agent Reliable Transaction Failed}  .. GN_INFO/INF
> Failure reason = Time to live limit exceeded
> ```
>
> To avoid this scenario, run the following commands from Active DSR NOAM before running performance traffic:
>
> ```
> iset -fvalue=400 ComAgtConfigParams where "name='IntraNe Maximum
> Timeout Value'"
> iset -fvalue=3 ComAgtConfigParams where "name='Maximum Number Of
> Retries'"
> ```
>
> - The following error is encountered, when the traffic is around 5.3k on each MP during the performance run:
>   - Communication Agent Reliable Transaction Failed: Communication Agent Reliable Transaction Failed.
>   - DCA to UDR ComAgent Error: DCA failed to send query to UDR due to ComAgent Error.
>   - Communication Agent Transaction Failure Rate: The number of failed transactions over the sampling period exceeded the configured thresholds.
>
>   To improve efficiency and to avoid the above issue, use the xsi2 interface for comagent connections between DSR and UDR.

Table 3-14 DSA Performance Benchmarking on 2 DA-MPs DSR Setup

Counter Measure (CM)	With and Without UDR Encryption	Call Flow Model	DSR MPS Achieved (Per DA-MP)	DA-MP Flavor	UDR Flavor	DA-MP Profile	Avg Msg Size	CPU Peak	RAM Utilization Peak
Previous Location Check	Without UDR Encryption	15% Vulnerable and 85% Non Vulnerable traffic	9.2K	12 vCPU (Regular)	18vCPU	30K_MPS	2.0 K	19%	24%
	With UDR Encryption	15% Vulnerable and 85% Non Vulnerable traffic	9.2K	12 vCPU (Regular)	12 vCPU (Regular)	30K_MPS	2.0 K	26%	29%

Table 3-14 (Cont.) DSA Performance Benchmarking on 2 DA-MPs DSR Setup

Counter Measure (CM)	With and Without UDR Encryption	Call Flow Model	DSR MPS Achieved (Per DA-MP)	DA-MP Flavor	UDR Flavor	DA-MP Profile	Avg Msg Size	CPU Peak	RAM Utilization Peak
Time Distance Check	Without UDR Encryption	15% Vulnerable and 85% Non Vulnerable traffic	9.8K	12 vCPU (Regular)	18vCPU	30K_MPS	2.0 K	22%	25%
	With UDR Encryption	15% Vulnerable and 85% Non Vulnerable traffic	9.8K	12 vCPU (Regular)	18vCPU	30K_MPS	2.0 K	22%	25%
Source Host Validation Hss	Without UDR Encryption	15% Vulnerable and 85% Non Vulnerable traffic	9.6K	12 vCPU (Regular)	18vCPU	30K_MPS	2.0 K	20%	25%
	With UDR Encryption	15% Vulnerable and 85% Non Vulnerable traffic	9.6K	12 vCPU (Regular)	18vCPU	30K_MPS	2.0 K	21%	25%
Message Monitoring Rate	N/A	15% Vulnerable and 85% Non Vulnerable traffic	10K	12 vCPU (Regular)	18vCPU	30K_MPS	2.0 K	20%	26%
Session Integrity Validation Chk	Without UDR Encryption	15% Vulnerable and 85% Non Vulnerable traffic	10K	12 vCPU (Regular)	18vCPU	30K_MPS	2.0 K	20%	25%
	With UDR Encryption	15% Vulnerable and 85% Non Vulnerable traffic	10K	12 vCPU (Regular)	18vCPU	30K_MPS	2.0 K	29%	25%
All Stateful	Without UDR Encryption	15% Vulnerable and 85% Non Vulnerable traffic	7.02K	12 vCPU (Regular)	18vCPU	30K_MPS	2.0 K	29%	25%

Table 3-14 (Cont.) DSA Performance Benchmarking on 2 DA-MPs DSR Setup

Counter Measure (CM)	With and Without UDR Encryption	Call Flow Model	DSR MPS Achieved (Per DA-MP)	DA-MP Flavor	UDR Flavor	DA-MP Profile	Avg Msg Size	CPU Peak	RAM Utilization Peak
	With UDR Encryption	15% Vulnerable and 85% Non Vulnerable traffic	7.02K	12 vCPU (Regular)	18vCPU	30K_MPS	2.0 K	23%	23%
All Stateful + All Stateless (Total 20 Countermeasures)	Without UDR Encryption	15% Vulnerable and 85% Non Vulnerable traffic	5.25K	12 vCPU (Regular)	18vCPU	30K_MPS	2.0 K	18%	25%
	With UDR Encryption	15% Vulnerable and 85% Non Vulnerable traffic	5.25K	12 vCPU (Regular)	18vCPU	30K_MPS	2.0 K	17%	23%
All Stateful with DESS Enabled	Without UDR Encryption	15% Vulnerable and 85% Non Vulnerable traffic	2.5K	12 vCPU (Regular)	18vCPU	30K_MPS	2.0 K	25%	26%
	With UDR Encryption	15% Vulnerable and 85% Non Vulnerable traffic	2.5K	12 vCPU (Regular)	18vCPU	30K_MPS	2.0 K	25%	26%
All Stateful + All Stateless with DESS Enabled (Total 20 Countermeasures)	Without UDR Encryption	15% Vulnerable and 85% Non Vulnerable traffic	2.5K	12 vCPU (Regular)	18vCPU	30K_MPS	2.0 K	40%	24%
	With UDR Encryption	15% Vulnerable and 85% Non Vulnerable traffic	2.5K	12 vCPU (Regular)	18vCPU	30K_MPS	2.0 K	40%	24%

> **Note**
>
> The DESS (Diameter End-to-End Security) feature also supports two other algorithms (ECDSA and DSA), which marginally delivers better performance.

Indicative Alarms/Events

Table 3-15 Indicative Alarms/Events

Number	Severity	server	Name	Description
19825	Minor/ Major/ Critical	DA-MP	Communication Agent Transaction Failure Rate	The number of failed transactions during the sampling period has exceeded configured thresholds.
19832	Info	DA-MP	Communication Agent Reliable Transaction Failed	Failed transaction between servers result from normal maintenance actions, overload conditions, software failures, or equipment failures.
33308	Info	DA-MP	DCA to UDR Comagent Error	DCA failed to send query to UDR due to ComAgent Error.
33446	Major	DA-MP	SrcHostValHssExecFailedAlrm	Failed executing *Source-Host-Validation-HSS* business logic. Disable the `CounterMeasure` until the problem is resolved.
33449	Major	DA-MP	TimeDistChkExecFailedAlrm	Failed executing *Time-Distance Check* business logic. Disable the `CounterMeasure` until the problem is resolved.

3.2.7 Rx-ShUDR-Application (RSA) Benchmarking

Rx-ShUDR Application (RSA) is implemented using DCA framework and will be deployed at the Oracle Roaming DRA which is a virtual DSR. Oracle Roaming DRA (R-DRA) Virtual DSR establishes Diameter Rx connection with Oracle PCRF segments.

When deciding on whether a request should be processed, the Rx-ShUDR Application takes a number of aspects into consideration:

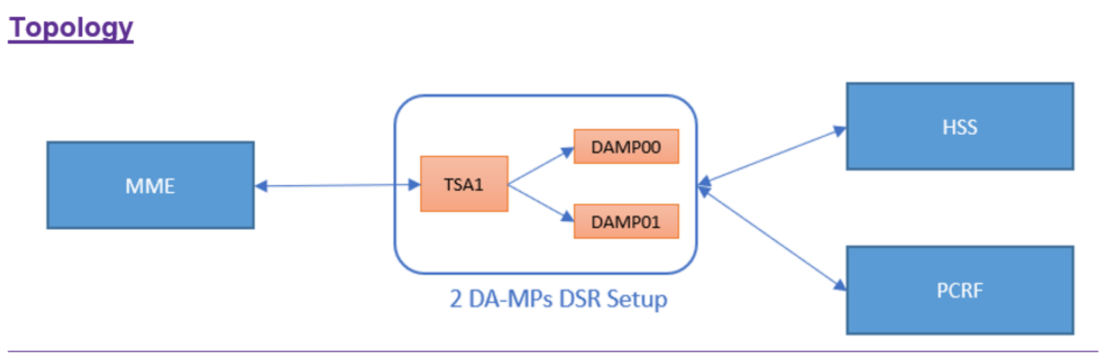
- Sh Lookup parameter must be enabled for received Rx Client FQDN. It can be checked in the Rx_Client Table.
- Sh UDR message should be created as per the content received in the Rx AAR message from MCPTT client and send it to the dedicated HSS through Core DRA.

> **Note**
>
> If Sh Lookup parameter is disabled, AAR message should be forwarded to the RBAR dip for PCRF segment address resolution using the IPv6 prefixes from the received Rx AAR message.

- RBAR (Range Based Address Resolution) activated on R-DRA (Roaming DRA), populated with IPv6 Prefixes mapped to PCRF segment FQDNs.

Topology

Figure 3-13 Topology



Message Flow

Figure 3-14 Message Flow

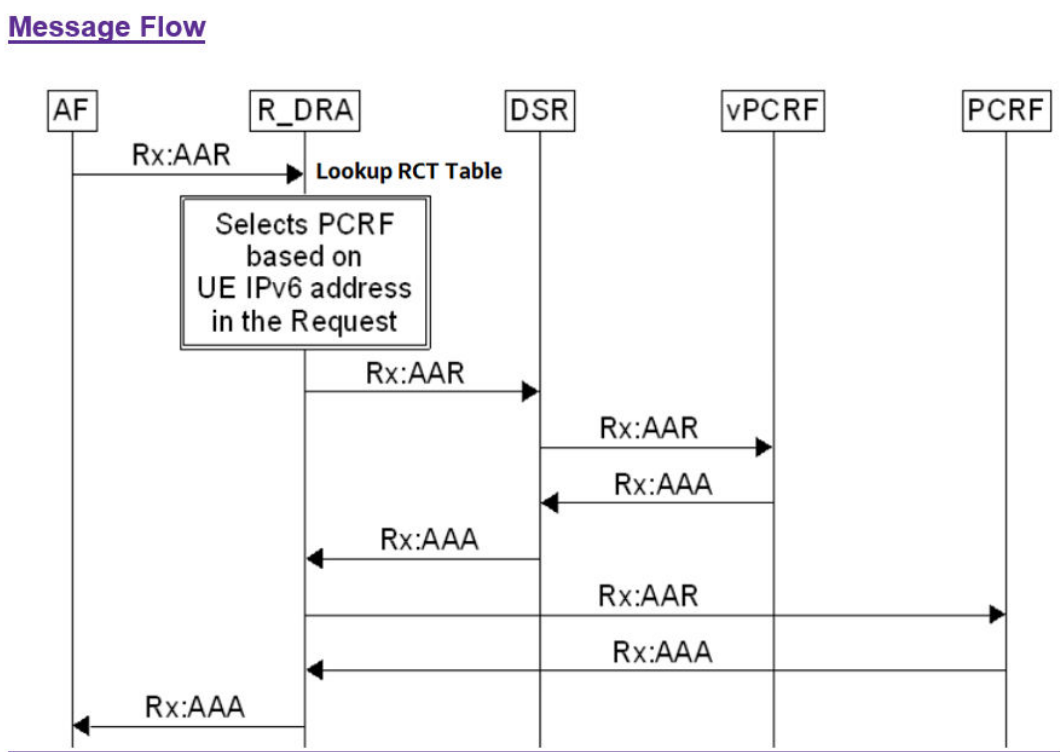
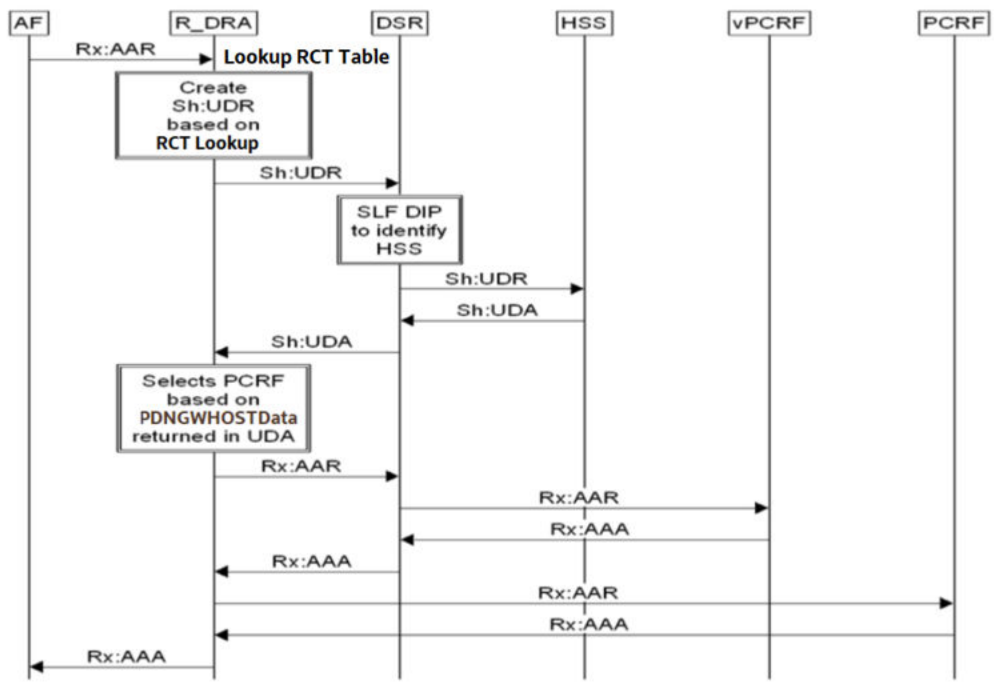


Figure 3-15 Sh lookup



Configuration

The following table describes the application configurations and the modes of operations used in benchmarking tests.

RSA Test Cal Model

Table 3-16 DSR common configuration

DSR Common Configuration parameters	No of Records	Rx Message originator	Supported Diameter Message
No of DAMP's	2	MCPTT Client	AAR-I/U, STR
No of Local Nodes	2	PCRF	ASR, RAR
No of Peer Nodes	40	-	-
No of MCPTT Client Connections	16	Rx Message originator	Supported Message Type
No of PCRF connections	16	Rx ShUDR application	Sh-UDR
No of HSS Connections	8	-	-
Total No of connections	40	-	-

Table 3-17 Application configuration

Table Name	Counts	Messages	Distribution
Error_Action_Config	41	Rx AAR, AAA Initial	40%
PDNGWHost_PCRF_Mapping	7	Rx AAR, AAA Update	4%
Rx_Client	10	Rx STR, STA	13%

Table 3-17 (Cont.) Application configuration

Table Name	Counts	Messages	Distribution
System_Config_Options	1	Rx ASR, ASA	13%
Topology_Hiding	3	Rx RAR, RAA	3%
-	-	Sh-UDR, Sh-UDA	27%

RSA Performance Benchmarking on 2 DA-MPs DSR Setup

Table 3-18 RSA Performance Benchmarking

Scenario	Call Flow Model	DSR MPS Achieved	DA-MP Flavor	DA-MP Profile	Avg Msg Size	CPU Peak	RAM Utilization Peak
Use Case (A+B) scenario with 27% of the traffic having Sh_lookup	Use Case (A + B)	30K (15K/MP)	12 vCPU (Regular)	30K_MPS	400	19%	22%

Indicative Alarms/Events

Table 3-19 Indicative Alarms/Events

Number	Severity	Server	Name	Description
22008	Info	DA-MP	Orphan Answer Response Received	An Answer response was received for which no pending request transaction existed resulting in the Answer message being discarded.
33318	Major	DA-MP	DCA `CreateAndSend` Request Message Send Failed	Failed while sending a `CreateAndSend` request message.
33430	Major	DA-MP	RxShUDRAppExecFailedAlrm	Failed executing Rx-ShUDR application business logic.
5002	Critical	IPFE	IPFE address configuration error	An address pertaining to inter-IPFE state synchronization is configured incorrectly.
5003	Critical	IPFE	IPFE state sync run error	Error syncing state data between IPFEs.
5011	Critical	IPFE	System or platform error prohibiting operation	Error related to system misbehavior or platform misconfiguration, check traces for more information.
5012	Critical	IPFE	Signaling interface heartbeat timeout	Heartbeats to monitor the liveness of a signaling interface is timed out.

3.2.8 Radius Benchmarking

Radius (Remote Authentication Dial In User Service) is an Authentication, Authorization and Accounting (AAA) protocol that is a predecessor to diameter. Radius is frequently used, specially in WLAN networks and 3G mobile data applications. DSR will be deployed in networks requiring support for both Diameter and Radius nodes as well in Radius only networks.

Radius has similarities to Diameter but is significantly different in many ways. Radius is primarily supported on DSR by a new connection layer called the Radius Connection Layer, while using the existing routing services of the Diameter Routing Layer (DRL) and the existing Diameter based message interface to or from the DRL.

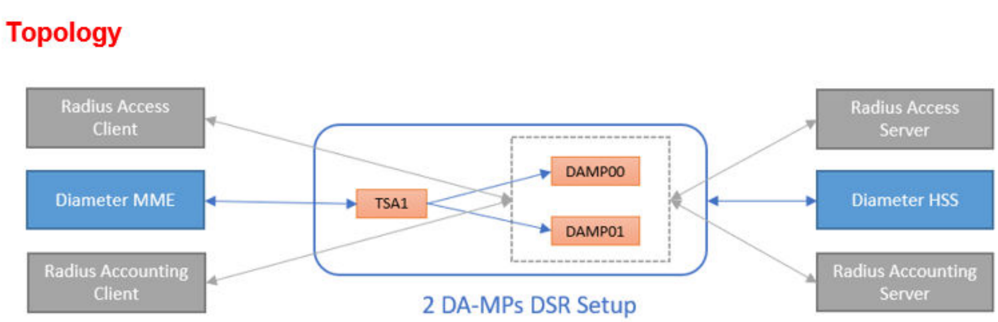
Ingress radius request or response messages are encapsulated in Diameter Request or Answer messages respectively. Diameter Request message content is created by Radius Connection Layer based on a set of predefined rules using both configuration data and radius message content. Diameter answer message content is created by Radius Connection Layer based on a set of predefined rules using mostly the Diameter Request message content associated with the transaction.

Radius request message routing is based upon the associated Diameter Request message which encapsulates the Radius message, the user must be familiar with how the Diameter Request capsule is created so they can configure the DRL to route Radius request messages.

Diameter Routing Layer provides required information to Radius Connection Layer to enable forwarding of Radius messages to the peer.

The Radius Connection Layer prevents accidental routing of non Radius messages to a Radius connection due to misconfiguration.

Figure 3-16 Topology



Configuration

Following table describes the configurations used in benchmarking tests:

Table 3-20 Radius Configuration

Parameters	Counts
Number of DAMP's	2
Number of Radius Client Connections for Access-Accept	16
Number of Radius Server Connections Access-Request	45
Number of Radius Client Connections Accounting-Accept	8
Number of Radius Server Connections Accounting-Request	45
Total Number of Connections	114
Number of Local Nodes	9
Number of Peer Nodes	114

Table 3-21 Diameter Configuration

Parameters	Counts
Number of DAMP's	2
Number of DAMPs with fixed or floating connections	2
Number of IFEE	2
Number of TSA Defined	1
Number of DAMP in TSA Groups	2
Number of Initiator Connections	120
Number of Responder Connections	40
Total Number of Diameter Connections	160
Number of Local Nodes	2
Number of Peer Nodes	10

Table 3-22 Traffic Call Model

Traffic Type	Distribution
Radius Access Traffic	5%
Radius Accounting Traffic	25%
Diameter Relay Traffic	70%

Table 3-23 Radius + Diameter Performance Benchmarking on 2 DA-MPs DSR Setup

Scenario	Call Flow Model	DSR MPS Achieved	DA-MP Flavor	DA-MP Profile	Avg Msg Size	CPU Peak	RAM Utilization Peak
Radius + Diameter	30% Radius + 70% Diameter	36K (18K/MP)	12 vCPU (Regular)	30K_MPS	400	23%	25%

Table 3-24 Indicative Alarms/Events

Number	Severity	Server	Name	Description
22008	Info	DA-MP	Orphan Answer Response Received	An Answer response was received for which no pending request transaction existed resulting in the Answer message being discarded.
22201	Minor	DA-MP	MpRxAllRate	DA-MP ingress message rate threshold crossed.
22221	Minor	DA-MP	Routing MPS Rate	Message processing rate for this DA-MP is approaching or exceeding its engineered traffic handling capacity.

3.2.9 IDIH (Integrated Diameter Intelligence Hub) Benchmarking

Oracle Communications IDIH (Integrated Diameter Intelligent Hub) is a signaling troubleshooting and analysis tool. IDIH captures and stores network trace data from Diameter Signaling Router (DSR) which is network signalling or routing node for visualization and troubleshooting purposes.

IDIH provides a web-based UI, with graphical view of network messages along with ladder diagram and full decode of network trace data which is easy to understand. It captures and stores additional metadata related to network traffic which provides information about the internal processing applied within the routing nodes to the network traffic. The configuration data from network routing nodes is pulled and converted into human-readable format.

In addition to visualization of signaling data, IDIH allows you to manage and run queries on captured network traffic, each query can have advanced filtering on individual protocol attributes or combination of attributes aligned with various logical operators. User can also save or update these queries for later usage. It also allows you to export individual network transactions or a complete trace in HTML and PCAP format.

IDIH provides statistical data about each captured trace, which displays the success and failures of a trace. It also provides a response code wise distribution for each trace.

3.2.9.1 Message Flow

Figure 3-17 Topology

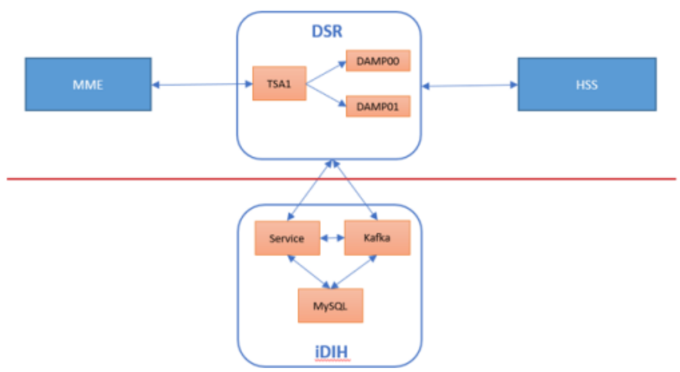


Table 3-25 iDIH Performance Benchmarking using DSR Setup

S.No	Scenario	Call Flow Model	DSR MPS Achieved	DA-MP Flavor	DA-MP Profile	Avg Msg Length	CPU Peak	RAM Utilization Peak CPU	CPU (IDIH)	RAM (IDIH)
1	Relay	100% Relay	18K(9K per MP)	12 vCPU (Regular)	30K_MPS	2.0K	10%	24%	3.97%	57.75%

> **Note**
>
> On the IDIH platform, a total of 6 traces are active and enabled every five minutes.

3.2.9.2 Indicative Alarms/Events

During benchmark testing, the following alarms or events were observed as the system entered congestion.

Table 3-26 DA-MP Relay Alarms/Events

Number	Severity	Server	Name	Description
22008	Info	DA-MP	Orphan Answer Response Received	An Answer response was received for which no pending request transaction existed resulting in the Answer message being discarded.

3.2.10 IPFE

The IPFE operates in both VMware and KVM environments. The following table presents the measured IPFE capacity. The following three main factors determine the throughput limits:

- The number of TSAs (one or more) on the IPFE.
- If there are more than 2,000 connections.
- If the average message size is less than the MTU size. Default MTU size is 1500 bytes.

In the most conditions the throughput of the IPFE is 2 Gbit/sec. However, when all three of the above conditions occur simultaneously, the throughput of the IPFE drops to 1.6 Gb/sec. When monitoring IPFE capacity, both the guest and host CPU utilization must be monitored. Much of the IPFE work is done at the host kernel level so the CPU utilization numbers returned by the IPFE application level dont fully reflect all of the IPFE overhead on the system.

Table 3-27 IPFE Throughput

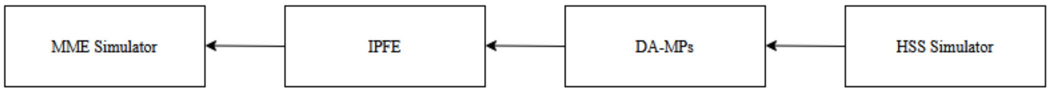
	Single TSA on IPFE Pair		**Two or more TSAs on IPFE Pair (Total on both TSAs)**	
	Avg Msg Size < 1 MTU	Avg Msg Size >= 1 MTU	Avg Msg Size < 1 MTU	Avg Msg Size >= 1 MTU
2,000 Connections or less	2 Gbit/sec	2 Gbit/sec	2 Gbit/sec	2 Gbit/sec
More than 2,000 Connections	2 Gbit/sec	1.6 Gbits/sec	2 Gbit/sec	2 Gbit/sec

3.2.10.1 Topology

The following image illustrates a typical IPFE configuration, where IPFEs are deployed for ingress-side traffic between Diameter clients. This configuration is commonly used because the number of Diameter clients, such as MMEs, is typically much higher than the number of

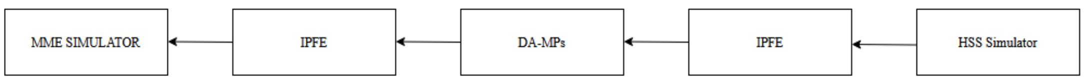
Diameter servers, such as HSSs. The bandwidth values provided in Table 31 correspond to the traffic flowing between the clients (MME in the figure above) and the DSR DA-MPs.

Figure 3-18 IPFE on Ingress Side Only



The following image illustrates another possible IPFE configuration, in which the IPFE uses connection initiator functionality to establish connections between the DA-MPs and the Diameter servers, shown here as the HSS simulator. The IPFE bandwidth requirements for the egress side must be calculated separately. If all DSR traffic passes through an IPFE on both the ingress and egress sides, the required IPFE bandwidth is: (2 * MPS) * (average Diameter message size including IP overhead)).

Figure 3-19 IPFE on both Ingress and Egress Sides



3.2.10.2 Indicative Alarms/Events

The following table shows the key recommended metrics for managing IPFE performance. For additional IPFE measurements, see *Oracle Communications Measurements Guide*.

Table 3-28 IPFE Metrics

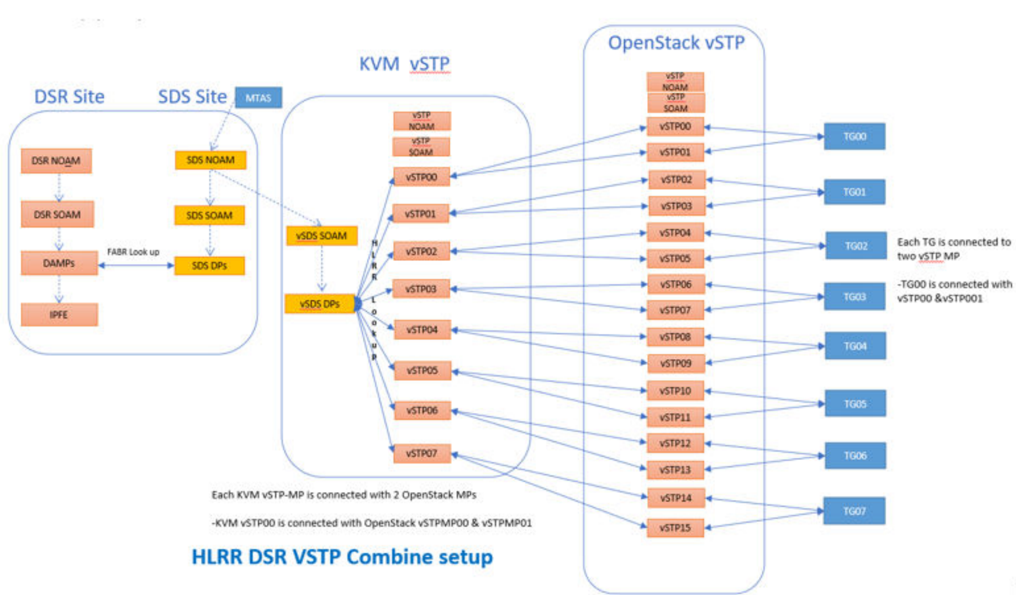
Measurement ID	Name	Group	Scope	Description	Recommended Usage Conditions	Recommended Usage Actions
5203	RxIpfeBytes	IPFE Performance	Server Group	Bytes received by the IPFE	If the number of (bytes * 8 bits/byte) or (time interval in s) is > benchmarked capacity (Gbps)	If the traffic is expected to grow then, consider adding an additional IPFE pair.

Table 3-28 (Cont.) IPFE Metrics

Measurement ID	Name	Group	Scope	Description	Recommended Usage Conditions	Recommended Usage Actions
1052	CPU_UtilPct_Average	System	System (IPFE)	The average CPU usage from 0 to 100% (100% indicates that all cores are completely busy)	When running in normal operation with a mate in normal operation, and this measurement exceeds 30% occupancy, or exceeds 60% occupancy when running without an active mate.	Contact Oracle support.
1056	RAM_UtilPct_Average	System	System (IPFE)	The average committed RAM usage as a percentage of the total physical RAM	If the average RAM utilization exceeds 80% utilization..	Contact Oracle support.

3.2.11 vSTP MP HLR-Router Benchmarking

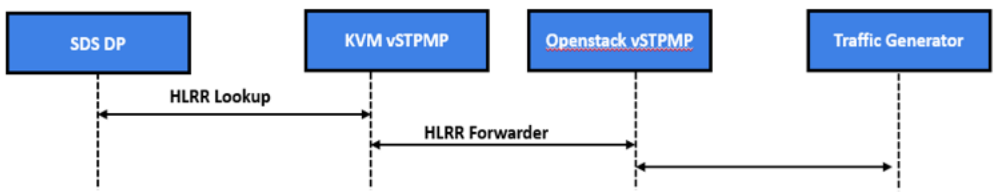
The following image shows benchmarking results for the HLR Router feature on vSTP MPs. Testing was performed using an 8 KVM vSTP MP setup connected to SDS Site 2 DPs. OpenStack vSTP-MPs forward HLRR queries to the KVM vSTP-MPs for SDS database queries. SDS Site 1 is connected to the DSR DA-MPs.



3.2.11.1 Message Flow

The following image shows HLRR traffic forwarded from OpenStack MP (Message Processor) to KVM vSTPMP. KVM vSTPMP looks up SDS DP:

Figure 3-20   vSTP MP HLRR Message Flow



The following table summarizes HLR Router feature benchmarking results:

Table 3-29   HLRR vSTP MP and SDS DP Benchmarking

Scenario	Call Flow Model	vSTP MPS Achieved	vSTP MP Flavor	vSTP MP CPU Peak	vSTP MP RAM Utilization Peak	SSSS DDDD SSSS DDDD PPPP MFCR PI PA SaUM AvPP coee hr(aa i Skk ei vt ee d- 2)
KVM vSTP MP performing HLRR lookup on SDS & routing to SS7 peer	10K HLR Routing	80K MPS (10K/MP)	8 vCPU	28%	42%	8211 0444 Kv%% MC PP SU ((8L 0a Kr / g De P))

Table 3-30 DSR DA-MP and SDS DP Benchmarking

Scenario	Call Flow Model	DP MPS Achieved	DA-MP MPS Achieved	DA-MP Flavor	DA-MP Profile	ADDSDD vAADPP g--SCR MMMDPA sPPPUM gCRFPP SPAl ee i UMaaa zPUVkk eet o ai r(kl S i i zt ae t - i 1 o) n P e a k
FABR	100% FABR	80K MPS (80K/DP)	160K (10K/DA-MP)	18 vCPU (Large)	30K_MPS	292211 . %0413 0 %%% K C P U (L a r g e)

3.2.11.2 Indicative Alarms/Events

During benchmark testing the following alarms/events were observed as it crossed threshold.

Table 3-31 vSTP MP HLR Router Traffic Alarms/Events

Number	Severity	Server	Name	Description
70357	MINOR	vSTP MP	Ingress max Mp MSU TPS Crossed	vSTP ingress max Mp MSU TPS threshold crossed
70358	MINOR	vSTP MP	Egress max Mp MSU TPS Crossed	vSTP egress Max Mp MSU TPS threshold crossed.
70102	MINOR	vSTP MP	MTP3 Ingress Link MSU TPS Crossed	vSTP ingress link MSU TPS threshold crossed

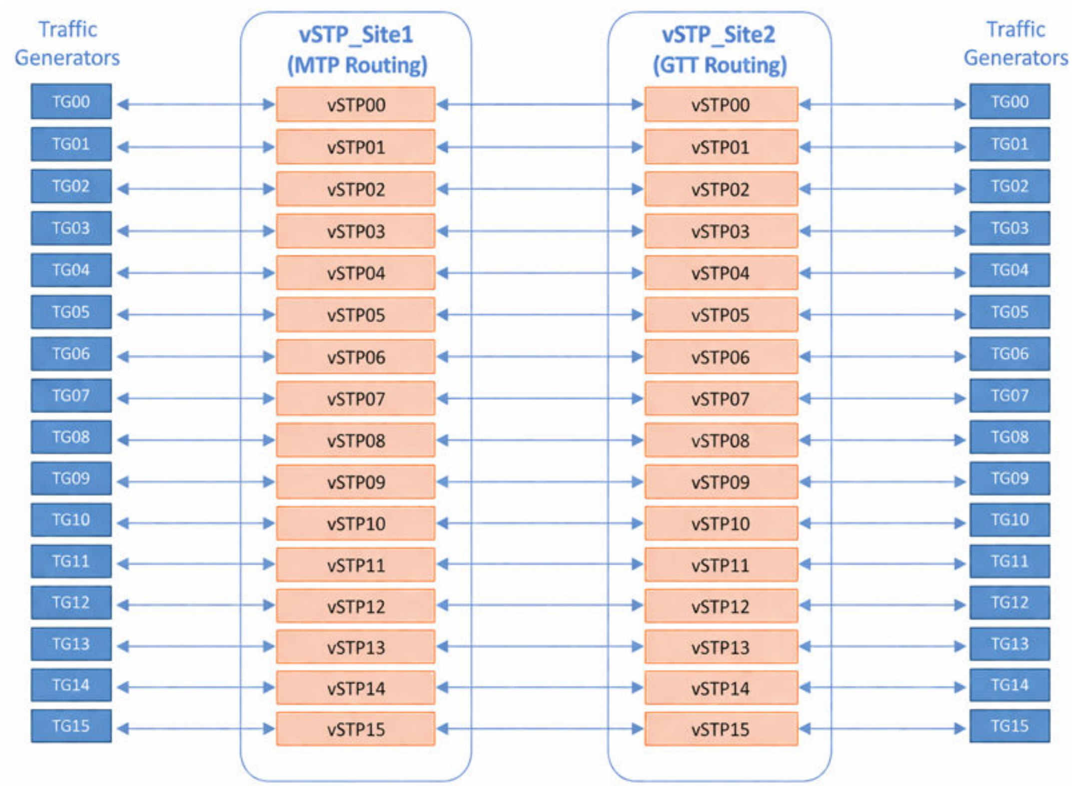
Table 3-31 (Cont.) vSTP MP HLR Router Traffic Alarms/Events

Number	Severity	Server	Name	Description
70103	MINOR	vSTP MP	MTP3 Egress Link MSU TPS Crossed	vSTP egress link MSU TPS threshold crossed.

3.2.12 vSTP MTP Routing and GTT

The vSTP MP server type is a virtualized STP that supports M2PA, M3UA, and TDM. It can be deployed either with other DSR functionality as a combined DSR and vSTP, or as a standalone virtualized STP without any DSR functionality. Following scenario test MTP and GTT routing running on test bed for 16 vSTP MP scenario.

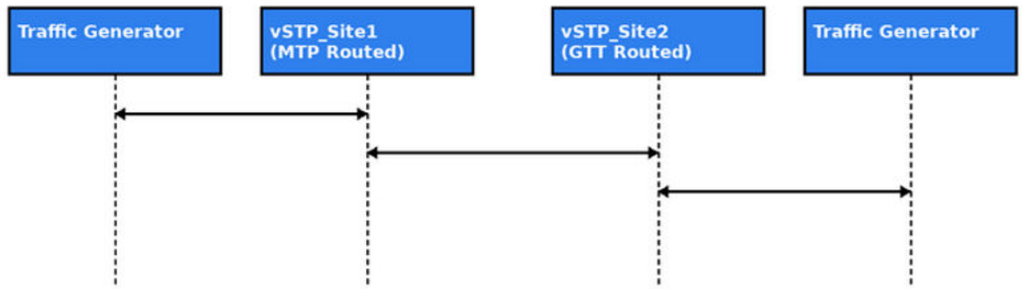
Figure 3-21 16 vSTPs MP Test Setup.png



3.2.12.1 Message Flow

The following image shows the vSTP MTP and GTT message flow between Site1 and Site2 during performance benchmarking:

Figure 3-22 vSTP MTP and GTT Message Flow



The following table summarizes the GTT and MTP routing benchmarking results for the 16 vSTP MP setup:

Table 3-32 GTT and MTP routing for 16 VSTP MPs Benchmarking

Scenario	Call Flow Model	vSTP MPS Achieved	vSTP MP Flavor	CPU Peak	RAM Utilization Peak
GTT + MTP Routing	100% MTP Routing on Site1 100% GTT Routing on Site2	320K (20K/MP)	8 vCPU	Site1=34% Site2=42%	Site1=55% Site2=55%

3.2.12.2 Indicative Alarms/Events

During benchmark testing the following alarms/events were observed as it crossed threshold.

Table 3-33 GTT and MTP Routing

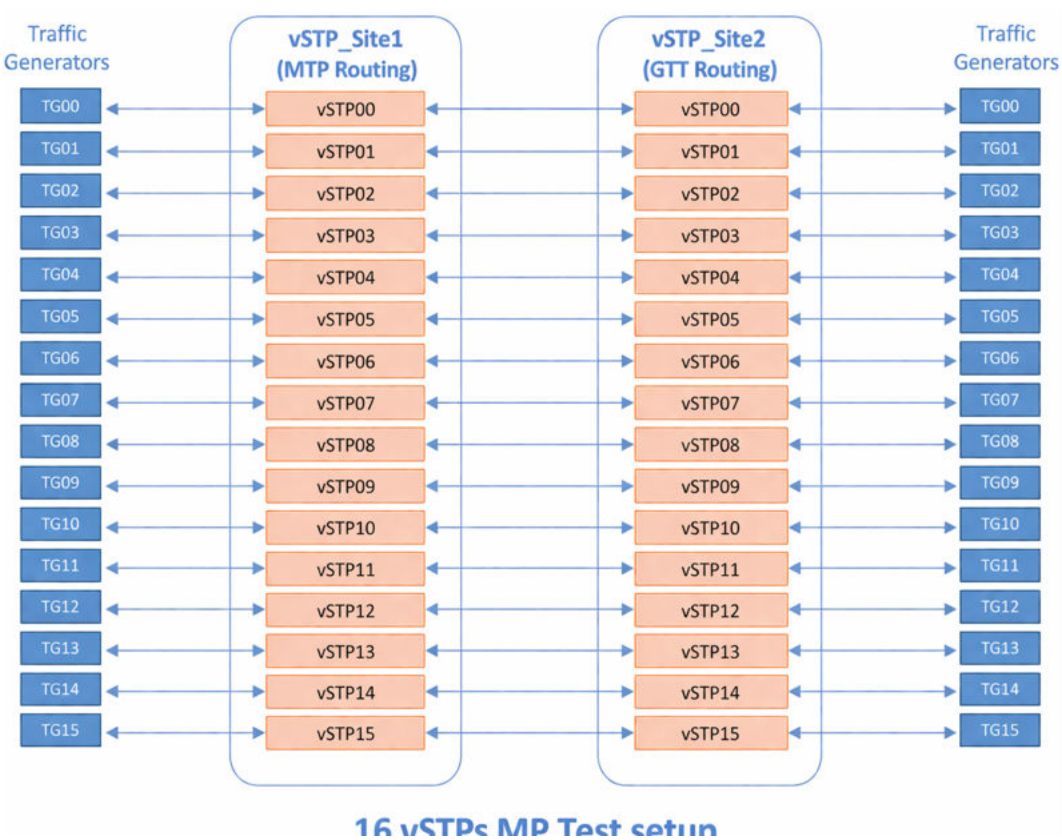
Number	Severity	Server	Name	Description
70357	MINOR MAJOR	vSTP MP	Ingress max Mp MSU TPS Crossed	vSTP ingress max Mp MSU TPS threshold crossed.
70358	MINOR MAJOR	vSTP MP	Egress max Mp MSU TPS Crossed	vSTP egress Max Mp MSU TPS threshold crossed.
70102	MINOR	vSTP MP	MTP3 Ingress Link MSU TPS Crossed	vSTP ingress link MSU TPS threshold crossed.
70103	MINOR	vSTP MP	MTP3 Egress Link MSU TPS Crossed	vSTP egress link MSU TPS threshold crossed.

3.2.13 vSTP MTP Routing and GTT Routing with MTP Screening

The vSTP-MP server type is a virtualized STP that supports M2PA, M3UA, and TDM. It can be deployed either with other DSR functionality as a combined DSR and vSTP, or as a standalone virtualized STP without any DSR functionality. Following scenario tests MTP and GTT routing where MTP screening is applied on inter vSTP M2PA links.

Topology

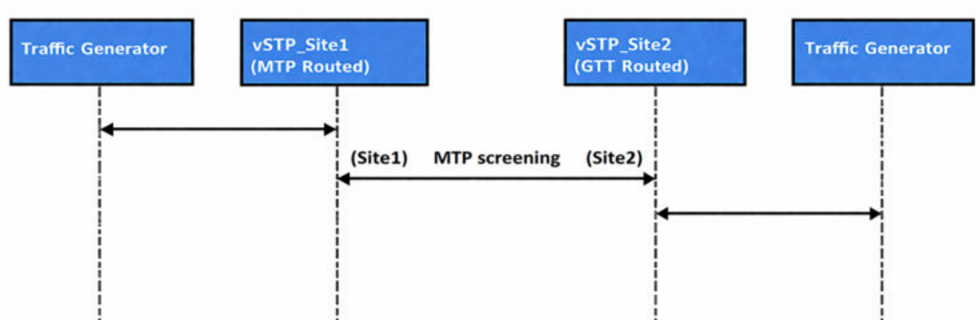
The following image shows the 16 vSTP MP test setup used for MTP screening performance benchmarking, including traffic generator connectivity and message routing between Site1 and Site2:



3.2.13.1 Message Flow

The following image shows the vSTP MTP and GTT message flow with MTP screening between Site1 and Site2 during performance benchmarking:

Figure 3-23 vSTP MTP and GTT with MTP Screening Message Flow



The following table provides the MTP screening performance benchmarking results for the 16 MP vSTP and 16 SS7-MP vSTP setup configuration:

Table 3-34 MTP Screening Performance Benchmarking on 16 MPVSTP MPs vSTP Setup

Scenario	Call Flow Model	vSTP MPS Achieved	vSTP MP Flavor	CPU Peak	RAM Utilization Peak
GTT + MTP Routing with MTP screening (M2PA & M3UA)	100% MTP Routing on Site1 with Screening 100% GTT Routing on Site2	256K (16K/MP)	8 vCPU	Site1=40 % Site2=47 %	Site1=42 % Site2=42 %

3.2.13.2 Indicative Alarms/Events

During benchmark testing the following alarms/events were observed as it crossed threshold.

Table 3-35 VSTP MP Screening Traffic Alarms/Events

Number	Severity	Server	Name	Description
70357	MINOR MAJOR	vSTP MP	Ingress max Mp MSU TPS Crossed	vSTP ingress max Mp MSU TPS threshold crossed.
70358	MINOR MAJOR	vSTP MP	Egress max Mp MSU TPS Crossed	vSTP egress Max Mp MSU TPS threshold crossed.
70102	MINOR	vSTP MP	MTP3 Ingress Link MSU TPS Crossed	vSTP ingress link MSU TPS threshold crossed.
70103	MINOR	vSTP MP	MTP3 Egress Link MSU TPS Crossed	vSTP egress link MSU TPS threshold crossed.

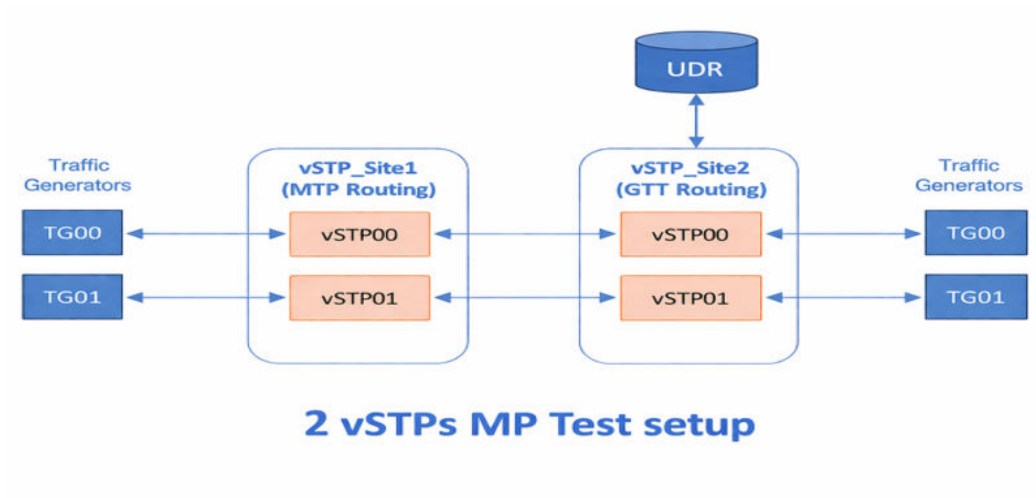
3.2.14 vSTP MP Benchmarking GTT with Other Features

The following table describes the feature wise vSTP MP benchmarking where the testing has been performed on a small two vSTP MP test setup with one pair of UDR connected.

3.2.14.1 Topology

The below image shows the feature-wise vSTP MP benchmarking where the testing has been performed on a small two VSTP MP test setup with one pair of UDR connected:

Figure 3-24 2 vSTPs MP Test Setup



The following table describes feature-wise vSTP MP Benchmarking:

Table 3-36 Feature-wise vSTP MP Benchmarking

Scenario	Call Flow Model	vSTP MPS Achieved per MP	vSTP MP	CPU Peak	RAM Peak
SFAPP+MNP + GTT	2K MNP + 2K SFAPP + 6K GTT	10K/MP	8 vCPU	33%	52%
SFAPP + MNP + GFLEX + GTT	2K MNP + 2K SFAPP + 1K GFLEX + 4K GTT	9K/MP	8 vCPU	25%	49%
SFAPP + GTT (UDR encryption off)	4kSFAPP + 4k GTT	8K/MP	8 vCPU	40%	43%
SFAPP + GTT (UDR encryption on)	4kSFAPP + 4k GTT	8K/MP	8 vCPU	39%	43%
TIF + GTT	5K MNP + 10K GTT	15K/MP	8 vCPU	28%	39%
vMNP + GTT	5K MNP + 10K GTT	15K/MP	8 vCPU	31%	42%
GFLEX + GTT	5K MNP + 10K GTT	15K/MP	8 vCPU	41%	42%
INPQ + GTT	5K MNP + 10K GTT	15K/MP	8 vCPU	37%	43%
vEIR	5K	5K/MP	8 vCPU	17%	49%
Elynx (E1/T1 Card) – GTT Relay	10K TDM + 10K GTT	20K /MP	8 vCPU	44%	41%
ENUM	5K	5K /MP	8 vCPU	10%	47%
DNS	10K	10K/MP	8 vCPU	3%	42%
vSTP – Home SMS	MO-FSM AllowList + BlockList Traffic (10K + 10K)	10K vSTP MP (2 MPs) 20K / Proxy MP	8 vCPU	46%	45%

Table 3-36 (Cont.) Feature-wise vSTP MP Benchmarking

Scenario	Call Flow Model	vSTP MPS Achieved per MP	vSTP MP	CPU Peak	RAM Peak
Tracing (GTT)	9K (Tracing)	9K/MP	8 vCPU	45%	48%
Tracing (GTT) + Non-Tracing (GTT)	6K (Tracing) + 6K (GTT)	12K/MP	8 vCPU	40%	44%

> **Note**
>
> - For ENUM, a new vENUM-MP is introduced. vENUM sends messages to the UDR (Unified Data Repository) over the ComAgent interface.
> - Default timer values are supported when vSTP is configured to operate at 10K MPS (Messages Per Second) per message processor.
> - When vSTP is configured to operate at 20K MPS, the t1Timer through t5Timer values must be updated. Refer to the *MMI API Specification* for the updated timer values. MNP (Mobile Number Portability) processing is equivalent to two messages, and SFAPP (Service Function Application) processing is equivalent to four messages.
> - For the tracing feature, tracing is applied to all GTT (Global Title Translation) traffic.
> - ENUM message processor supports 5K DNS traffic with load balancing (CPU Peak=3, Ram Peak=47).

3.2.14.2 Indicative Alarms/Events

During benchmark testing the following alarms/events were observed as it crossed threshold.

Table 3-37 VSTP MP Feature Traffic Alarms/Events

Number	Severity	Server	Name	Description
70357	Minor	vSTP MP	Ingress max Mp MSU TPS Crossed	vSTP ingress max Mp MSU TPS threshold crossed.
70358	Minor	vSTP MP	Egress max Mp MSU TPS Crossed	vSTP egress Max Mp MSU TPS threshold crossed.
70102	Minor Major Critical	vSTP MP	MTP3 Ingress Link MSU TPS Crossed	vSTP ingress link MSU TPS threshold crossed.
70103	Minor Major Critical	vSTP MP	MTP3 Egress Link MSU TPS Crossed	vSTP egress link MSU TPS threshold crossed.

Appendix

This section provides information about the following:

- Summary of VM configurations
- Networking characteristics of different VMs
- DSR Benchmarking values on KVM/Oracle X9-2 server

A

DSR VM Configurations

The following table provides a summary of the VM configurations used for the benchmarking data and the affinity rules for deploying those VMs. Using VM sizes different from these tested values may give unexpected results because the application profiles are tuned to this number of vCPUs and memory sizes.

Table A-1 VM Configurations and Affinity Rules

VM Name	vCPU	RAM (GB)	Disk (GB)	Max Config	Redundancy Models	Affinity/Placement Rules (Per Site)	Notes
DSR NOAM (Regular)	4	14	120	1 Pair	Active/ Standby	2 VMs per DSR network in any site. VMs to be deployed on separate servers.	NA
DSR NOAM (Large)	8	14	120	1 Pair	Active/ Standby	2 VMs per DSR network in any site. VMs to be deployed on separate servers.	It is recommended to use large NOAM profile if the deployment is more than 24 C level servers. If SOAM profile is large, NOAM profile must be large. In large profiles, the scheduled two measurement exports run in parallel.
DSR SOAM (Regular)	4	14	120	1 Pair per DSR NF	Active/ Standby or Active/ Standby/ Spare	2 VMs per site. VMs to be deployed on separate servers.	Redundancy model Active/Standby/Spare model is used for PCA mated-pair deployments. For all other deployments Active or Standby model is used.

Table A-1 (Cont.) VM Configurations and Affinity Rules

VM Name	vCPU	RAM (GB)	Disk (GB)	Max Config	Redundancy Models	Affinity/Placement Rules (Per Site)	Notes
DSR SOAM (Large)	8	14	120	1 Pair per DSR NF	Active/ Standby or Active/ Standby/ Spare	2 VMs per site. VMs to be deployed on separate servers.	Redundancy model Active/Standby/Spare model is used for PCA mated-pair deployments. For all other deployments Active/Standby model is used. If the diameter connections are higher than 4K, it is recommended to use SOAM large profile. If NOAM profile is large, SOAM profile must be large. In large profiles, the scheduled two measurement exports will run in parallel.
DA-MP (Regular)	12	16	120	32 per DSR NF	Active Cluster (N+0)	Should be spread over as many servers as possible to minimize capacity loss on server loss.	The limit of 24 is the combined total of DA-MPs, DA-MP with EIR cannot max out all types in one DSR (for instance 24 DA-MPs AND 32 vSTPs). The vSTP MPs do not count against this 32.
DA-MP (Large)	18	24	120	32 per DSR NF	Active Cluster (N+0)	Should be spread over as many servers as possible to minimize capacity loss on server loss.	The limit of 24 is the combined total of DA-MPs, DA-MPs with IWF, DA-MP with EIR cannot max out all types in one DSR (for instance 24 DA-MPs AND 32 vSTPs).
vSTP MP	8	12	120	32 per DSR NF	Active Cluster (N+0)	Should be spread over as many servers as possible to minimize capacity loss on server loss.	The vSTP MPs do not count against the 32 DA-MP limits in a single OCDSR node, hence a DSR can have up to 32vSTP MPs.
HomeSMSC Service MP	8	12	120	32 per DSR NF	Active Cluster (N+0)	Should be spread over as many servers as possible to minimize capacity loss on server loss.	The Service MPs do not count against the 32 DA-MP limits in a single OCDSR node, hence DSR can have up to 32 service MPs.

Table A-1 (Cont.) VM Configurations and Affinity Rules

VM Name	vCPU	RAM (GB)	Disk (GB)	Max Config	Redundancy Models	Affinity/Placement Rules (Per Site)	Notes
vENUM Service MP	8	12	150	32 per DSR NF	Active Cluster (N+0)	Should be spread over as many servers as possible to minimize capacity loss on server loss.	The vENUM MPs do not count against the 32 DA-MP limits in a single OCDSR node, hence DSR can have up to 32 ENUM MPs.
IPFE	6	16	120	2 pairs per DSR NF	Active/ Standby	Each VM in a pair must be deployed on separate server.	Deployed in pairs. Max 2 pairs (4VMs).
SBR(s)	12	25	120	8 Server Groups per SBR(b)	Active/ Standby/ Spare	Active/Standby VMs to be deployed on separate servers,Spare is typically at another geographic location for geo-redundancy.	Can be either Active/ Standby/Spare or Active/Standby depending on customer geo-redundancy requirements.
SBR(b)	12	32	120	8 Server Groups per SBR(b)	Active/ Standby/ Spare	Active/Standby VMs to be deployed on separate servers,Spare is typically at another geographic location for geo-redundancy.	Can be either Active/ Standby/Spare or Active/Standby depending on customer geo-redundancy requirements.
SBR(u)	12	24	120	64 Server Groups per SBR(b	Active/ Standby/ Spare	Active/Standby VMs to be deployed on separate servers,Spare is typically at another geographic location for geo-redundancy.	Can be either Active/ Standby/Spare or Active/Standby depending on customer geo-redundancy requirements.
SDS NOAM (Regular)	4	32	350	1 Pair per Network	Active/ Standby	Anti-affinity between the Active/Standby VMs	Active/Standby. An optional "Disaster Recovery" SDS is supported that would typically be located at a different data center to provide geo-redundancy.
Query Server (Regular)	4	32	350	1 per SDS NOAM	N/A since non-redundant	Non, non-redundant	Optional 1 per site. Can have one for the primary SDS-NOAM and one for the Disaster Recovery SDS-NOAM
SDS SOAM (Regular)	4	12	175	1Pair per DSR NF	Active/ Standby	2 VMs per site. VMs to be deployed on separate servers.	NA
SDS DP (Regular)	6	10	175	10 per DSR NF	Active Cluster (N+0)	Should be spread over as many servers as possible to minimize capacity loss on server loss.	To be evenly distributed across servers to minimize capacity loss.

Table A-1 (Cont.) VM Configurations and Affinity Rules

VM Name	vCPU	RAM (GB)	Disk (GB)	Max Config	Redundancy Models	Affinity/Placement Rules (Per Site)	Notes
SDS NOAM (Large)	4	128	890	1 Pair per Network	Active/ Standby	Anti-affinity between the Active/Standby VMs	Active/Standby. An optional "Disaster Recovery" SDS is supported that would typically be located at a different data center to provide geo-redundancy.
Query Server (Large)	4	128	890	1 per SDS NOAM	N/A since non-redundant	Non, non-redundant	Optional 1 per site. Can have one for the primary SDS-NOAM and one for the Disaster Recovery SDS-NOAM.
SDS SOAM (Large)	4	64	450	1 Pair per DSR NF	Active/ Standby	2 VMs per site. VMs to be deployed on separate server.	Supports
SDS DP (Large)	24	64	450	10 per DSR NF	Active Cluster (N+0)	Should be spread over as many servers as possible to minimize capacity loss on server loss.	To be evenly distributed across servers to minimize capacity loss.
UDR NO (Small)	6	16	270	n (Active,Standby)	Active/ Standby/ Spare	Active/Standby/Spare VMs to be deployed on separate servers, Spare is typically at another geographic location for geo-redundancy	Redundancy model Active/Standby/Spare model is used. Active/ Standby on Site 1 and Spare on Site 2. UDR is scaled by adding UDR NOs. The Standby UDR NO also receives query traffic from STP-MP and DA-MP.
UDR NO (Medium)	12	32	450	n (Active,Standby)	Active/ Standby/ Spare	Active/Standby/Spare VMs to be deployed on separate servers, Spare is typically at another geographic location for geo-redundancy	Redundancy model Active/Standby/Spare model is used. Active/ Standby on Site 1 and Spare on Site 2. UDR is scaled by adding UDR NOs. The Standby UDR NO also receives query traffic from STP-MP and DA-MP.

Table A-1 (Cont.) VM Configurations and Affinity Rules

VM Name	vCPU	RAM (GB)	Disk (GB)	Max Config	Redundancy Models	Affinity/Placement Rules (Per Site)	Notes
UDR NO (Regular)	18	70	450	n (Active,Standby)	Active/ Standby/ Spare	Active/Standby/Spare VMs to be deployed on separate servers, Spare is typically at another geographic location for geo-redundancy	Redundancy model Active/Standby/Spare model is used. Active/ Standby on Site 1 and Spare on Site 2. UDR is scaled by adding UDR NOs. The Standby UDR NO also receives query traffic from STP-MP and DA-MP.
UDR NO (Large)	32	128	850	n (Active,Standby)	Active/ Standby/ Spare	Active/Standby/Spare VMs to be deployed on separate servers, Spare is typically at another geographic location for geo-redundancy	Redundancy model Active/Standby/Spare model is used. Active/ Standby on Site 1 and Spare on Site 2. UDR is scaled by adding UDR NOs. The Standby UDR NO also receives query traffic from STP-MP and DA-MP.
UDR NO (Extra Large)	56	256	850	n (Active,Standby)	Active/ Standby/ Spare	Active/Standby/Spare VMs to be deployed on separate servers, Spare is typically at another geographic location for geo-redundancy	Redundancy model Active/Standby/Spare model is used. Active/ Standby on Site 1 and Spare on Site 2. UDR is scaled by adding UDR NOs. The Standby UDR NO also receives query traffic from STP-MP and DA-MP.
IDIH Service	6	16	120	1 per site	N/A since non-redundant	None, non-redundant	Optional component for Diameter traffic monitoring
IDIH Kafka	6	16	170	1 per Site	N/A since non-redundant	None, non-redundant	Optional component for Diameter traffic monitoring
IDIH MySql	6	16	220	1 per Site	N/A since non-redundant	None, non-redundant	Optional component for Diameter traffic monitoring
VNFM	8	10	80	NA	N/A since non-redundant	None, non-redundant	VNF Manager deployment
ATS	8	16	120	NA	N/A since non-redundant	None, non-redundant	Automated Test Suite Tool

> **Note**
>
> The minimum requirement for IDIH Service, IDIH Kafka, and IDIH MySQL is 6 vCPUs. For optimal performance, 12 vCPUs are recommended.

B

DSR VM Disk Requirements

This section provides guidance on the disk requirements for the OCDSR VMs. Characterizing disk requirements can be tricky since there are many variables that can affect disk usage, such as how many reports are being run on the OAM systems, or how often backups are run. Peak disk utilization can also be different from average disk utilization, for instance during backups or restore operations. While these guidelines are provided for the disk usage of the different VM types, customers should verify their disk usage under their own conditions since they are more driven by how the customer uses their system than by easier to calculate factors such as CPU utilization per MPS.

The OCDSR has been designed as a low disk utilization application, with all critical call processing applications performed in memory. There is also no swap disk utilization in any of the VMs. As a background for all of these numbers, the OCDSR has been run for years on "bare metal" deployments with a single pair of industry standard 10k RPM, 2½ inch disk drives in Raid 1. So even maximum sized OCDSR configurations run successfully on the approximately 120 IOPs provided by those disks. When run on higher performance disk subsystems such as SSDs, high disk utilization tasks such as background report generation just complete faster. The notes for each VM type give some of the factors that can drive different disk utilization levels. For instance, the primary traffic handling VMs, the IPFEs and the different types of MPs, have a fairly constant disk utilization independent of the traffic level. This is because the primary disk utilization is for saving statistics, then forwarding them to the SOAM.

Table B-1 VM Disk Utilization Characteristics

VM Name	Disk (GB)	Routine Disk Utilization (IOPs)1	Peak Disk Utilization (IOPs)2	Disk Usage Modes	Notes
DSR NOAM	120	100	800	Periodic (30 second) small writes to collect statistics. Large block reads to run reports and backups.	Background disk utilization is mostly statistics collection from managed DSRs. Peak disk utilization driven by customer report generation and maintenance activities such backups.
DSR SOAM	120	100	800		
DAMP	120	50	500	Writes statistics to disk at 30 second intervals, reads them at 5-minute intervals to send to SOAM	Disk utilization is independent to traffic levels. Is affected by the size of the DSR configuration (number of connections for instance) and the utilization of features that create measurements such as ETGs and TTPs.
vSTP	120	50	500		Disk utilization is independent to traffic levels. Is affected by the size of the vSTP configuration such as the number of local and remote peers.
SS7 MP	120	50	500		Disk utilization is independent to traffic levels. Is affected by the size of the DSR configuration

Table B-1 (Cont.) VM Disk Utilization Characteristics

VM Name	Disk (GB)	Routine Disk Utilization (IOPs)1	Peak Disk Utilization (IOPs)2	Disk Usage Modes	Notes
IPFE	120	20	100		IPFE has relatively few configuration items and statistics, and very low disk utilization.
SBR(s)	120	50	800	Disk writes mostly short bursts for statistics storage	Peak disk utilization driven by recovery activities between active/ standby servers.
SBR(b)	120	50	800		
SDS NOAM	350	100	800	Synchronizes changes to in-memory database to disk. Mostly write application	SDS can maintain multiple copies of large subscriber database. Peak disk utilization is mostly driven by creating new backups.
SDS SOAM	175	50	800		
SDS DP	175	80	500		
SDS Query Server	350	100	800	Synchronizes changes to in-memory database to disk. Reads are driven by customer queries	The query server is not a real-time system. The amount of disk reads is driven entirely by manual customer database queries.

The "routine" disk utilization is the minimum engineered IOPs for the proper functioning of the VM. Average disk utilization is typically lower.

The "Peak" disk utilization is number of IOPs the VM is capable of using given sufficient resources.

C

VM Networking Requirements

This section gives information on the networking characteristics of the different VMs. The traffic is broken down into signaling traffic handled on the XMI network, and OAM traffic carried on the IMI and XMI networks.

The Diameter Traffic requirements on the XSI networks can be calculated from the MPS. Treating the OCDSR as black box, this network traffic is simply the average Diameter message size (for requests and answers) times the MPS rate for the OCDSR node. The complication is that some Diameter traffic is likely to go through both an ingress DA-MP and an egress DA-MP. The most conservative consumption is that any ingress message is equally likely to go out any of the DA-MPs. Thus, if a DSR has X DA-MPs,and Y total MPS per DA-MP, the average Diameter signaling traffic through a DA-MP is:

```
((Average Diameter message size including IP overhead) * Y) * (1+ ((2X-1)/X))
```

As an example, if the average Diameter message size is 2,000 bytes including overhead, the overall DSRMPS is 10000 MPS, and the number of DA-MPs is three, the calculation would be:

```
(2,000 bytes * 8 bits/byte *10,000 MPS) * (1+ (2*3 DA-MPs) -1)/(3 DA-MPs)) =
(160,000 kb/s) * (2.66) = 426,666 kb/s per DA-MP
```

For the MP types other than the DA-MPs simply substitute the average size of signaling types, for instance SS7 messages for the vSTP MP. Since typically SS7 messages are much smaller than Diameter messages (for instance ~200 bytes for SMS), the vSTP MP bandwidth is much smaller than the DA-MP bandwidth.

The OAM traffic on the VMs can be much more variable since it's dependent to customer-specific usage patterns such as the number of reports requested and the number of periodic activities (backups and restores). The notes for each VM type give some background on the network impacts of these customer-driven activities.

Table C-1 VM Networking Utilization Characteristics

VM Name	Networks Supported	Management Networks (Gb/s)	Traffic Networks (Gb/s)	Notes
DSR NOAM	XMI IMI	2	N/A	Activities such as backups can generate higher network utilization but runs at the rate of the bandwidth available since they are not real-time activities.
DSR SOAM		1		
DA MP	XMI IMI XSI	0.2	MPS Dependent	See explanation above for how to calculate the signaling network traffic.
DA MP w/IWF				
vSTP MP				

Table C-1 (Cont.) VM Networking Utilization Characteristics

VM Name	Networks Supported	Management Networks (Gb/s)	Traffic Networks (Gb/s)	Notes
IPFE	XMI IMI XSI	2.0	MPS Dependent	The peak networking capacity supported by the IPFE is 3.2 Gb/s. Typically, the IPFE is deployed only on the ingress (towards clients such as MMEs) side of the DA-MP, so the total traffic through the IPFE is ½ the total bandwidth of the DA-MPs.
SBR(s) SBR(b) SBR(u)	XMI IMI	1.0	N/A	The given OAM bandwidth is for routine operations. Some recovery operations such as synchronizing the database between the active and standby servers after a prolonged disconnection can consume an order of magnitude or more of network bandwidth. The required amount of bandwidth for these recovery operations is very dependent on customer-factors such as number of subscribers, the MPS rate, and the amount of networking downtime.
SDS NOAM	XMI IMI	1.0	N/A	The maximum bandwidth required by the SDS NOAM is determined primarily by the provisioning rate from external customer systems along with the size of the customer records.
DP SOAM	XMI IMI	1.0	N/A	All of the subscriber data provisioned at the SDSNOAM is passed down to each DP SOAM, which then distributes the data to any attached DPs.
DP	XMI IMI	1.0	N/A	The DP receives writes of new subscriber records from the SOAM, and database queries from the DA-MPs.
Query Server	XMI IMI	1.0	N/A	The Query Server is synchronized to the changes in the SDS NOAM. In addition, there is some network traffic due to customer search requests, but this traffic is small compared to the synchronization traffic.
UDR NO	XMI IMI XSI	1.0	N/A	UDR NO receives internal query from STP MP and DAMP.

The following table shows some guidelines for mapping the logical OCDSR networks (XMI, IMI, so on) to interfaces. There is nothing fixed about these assignments in the application, so they can be assigned as desired if the customer has other requirements driving interface assignment.

Table C-2 Typical OCDSR Network to Device Assignments

VM Name	OAM (XMI)	Local (IMI)	Signaling A (XSI1)	Signaling B (XSI2)	Signaling C (XSI3)	Signaling (...)	Signaling D (XSI6)	Replication (SBR Rep)	DIH Internal
DSR NOAM	eth0	eth1							

Table C-2 (Cont.) Typical OCDSR Network to Device Assignments

VM Name	OAM (XMI)	Local (IMI)	Signaling A (XSI1)	Signaling B (XSI2)	Signaling C (XSI3)	Signaling (...)	Signaling D (XSI6)	Replication (SBR Rep)	DIH Internal
DSR SOAM	eth0	eth1							
DA-MP	eth0	eth1	eth2	eth3	eth4		eth17	eth18	
IPFE	eth0	eth1	eth2	eth3	eth4		eth17		
SBRB	eth0	eth1						eth2	
SBRS	eth0	eth1						eth2	
vSTP	eth0	eth1	eth2	eth3	eth4		eth17		
UDRNO	eth0	eth1	eth2	eth3	eth4		eth17		
SDS NOAM	eth0	eth1							
DP	eth0	eth1							
Query Server	eth0	eth1							

D

Summary of Benchmark Data Recommendations

The information shown in the following table is a summary of the benchmark data described throughout the document. This data is intended to provide guidance and is based solely on the observed results from the test setups described in this document. Recommendations may need to be adapted to the conditions in a given operator's cloud, such as differences in traffic patterns, feature utilization patterns, and infrastructure differences.

Table D-1 Benchmark Data Summary

Benchmark Run	Openstack/KVM
Application Software	DSR 9.x (running Oracle Linux 8.x)
Host VM	OpenStack Wallaby, KVM
HW	Oracle Server X9-2
VM Profiles/Flavors	DSR VM Configurations

Table D-2 Recommended Maximum Engineering Targets

VM Name	VM Purpose	Recommended Maximum Engineering Targets	
		Unit	Quantity
DSR NOAM	Network Operation,Administration, Maintenance (and Provisioning)	VM	1+1
DSR SOAM	Site (node/Network Element) Operation,Administration,Maintenance (and Provisioning)	VM	1+1
DA MP (Relay) (Regular Profile)	Diameter Agent Message Processor	MPS	18,000
DA MP (Relay) (Regular Profile) configuration set to DOC/CL1/CL2discards set to 0 and multi queuing enabled on all hosts	Diameter Agent Message Processor	MPS	36,000
DA MP (Relay) (Large Profile)	Diameter Agent Message Processor	MPS	35,000
DA MP (RBAR)	Diameter Agent Message Processor	MPS	16,000
DA MP (FABR with UDR)	Diameter Agent Message Processor	MPS	18,000 (70% FABR and 30% Relay)
DSA (All Stateful)	Diameter Agent Message Processor	MPS	7.02K
DSA (All Stateful + All Stateless)	Diameter Agent Message Processor	MPS	5.25K
vSTP MP	Virtual STP for M3UA and M2PA message Processing	MPS	20,000
vSTP w/ EIR	Virtual STP Message processor with EIR application	MPS	10000

Table D-2 (Cont.) Recommended Maximum Engineering Targets

VM Name	VM Purpose	Recommended Maximum Engineering Targets	
		Unit	Quantity
EIR + GTT	Virtual STP Message processor with EIR application and GTT	MPS	5000 EIR + 8000 GTT
SBR(s) (Single Server Group)	Subscriber Binding Repository (session) for Policy DRA	Diameter sessions	16,000,000
		MPS	50,000
SBR(s) (4 Server Groups)	Subscriber Binding Repository (session) for Policy DRA	Diameter sessions	64,000,000
		MPS	200,000
SBR(b) (Single Server Group)	Subscriber Binding Repository (binding) for Policy DRA	Diameter sessions	16,000,000
		MPS	50,000
SBR(b) (4 Server Groups)	Subscriber Binding Repository (binding) for Policy DRA	Diameter sessions	64,000,000
		MPS	200,000
SDS SOAM	Database Processor Site (node) Operation, Administration, Maintenance for address resolution and subscriber location functions	VM	1+1
SDS DP	Database Processor for address resolution and subscriber location functions	MPS requiring DP lookups (usually 50% of FABR traffic)	80,000
SDS (NOAM)	Subscriber Database Processor for address resolution and subscriber location functions	Routing Entities (SDS Large Profile)	780 million (260 million subscribers having 2 IMSI, 1 MSISDN)
		Routing Entities (SDS Regular Profile)	300 million Routing Entities (150 M MSISDNs/150 M IMSIs)
		Provisioning TPS	800
SDS Query Server	Allows customers to query FABR subscriber data via a MySQL interface	N/A	N/A
DSR	Diameter Agent Message Processor	Nodal Capacity	576K MPS
vSTP	Virtual STP for M3UA and M2PA message Processing for MTP & GTT routing	Nodal Capacity	512K MPS

E

Detailed Infrastructure Settings

Table E-1 Detailed Infrastructure Settings

Attribute	KVM/Oracle X9-2
Model	Oracle Server X9-2
Processor Type	Intel(R) Xeon(R) Platinum 8358 CPU @ 2.60GHz
vCPUs	2 CPUs (32 physical cores per CPU)
RAM	768 G
CPU Cache Memory	L1d Cache: 48K L1i Cache: 32K L2 Cache: 1280K L3 Cache: 49152K
Number and Type of NICs	Oracle Quad Port 10G Base-T Adapter
BIOS Power Settings	Power Supply Maximum: Maximum power the available PSUs can draw Allocated Power: Power allocated for installed and hot pluggable components Peak Permitted: Maximum power the system is permitted to consume (set to Allocated Power)
HDD	3.8 TB of NVMe storage (with Software RAID-1 configured)

F

Small DSR VM Configuration

Many customers do not need the capacity provided by even a single pair of standard size DSR DA-MP VMs. The fixed configuration in this section is for customers who need the following configuration:

- Relay or RBAR applications
- 6k MPS or less (assuming an infrastructure equal to or better than the X5-2 processors used for the benchmark tests)
- 5K or less RBAR entries
- No IPFE

This configuration should be run with the 6k DA-MP profile.

Table F-1 Minimal System VM Configurations and Affinity Rules

VM Name	vCPU	RAM (GB)	Disk (GB)	Max Config	Redundancy Models	Affinity/Placement Rules (Per Site)	Notes
DSR NOAM	4	8	120	1 Pair	Active/ Standby	2 VMs for each DSR network in any site. VMs to be deployed on separate servers if possible.	Two NOAMs are always required to support upgrades, but they can be on the same server if only one server is available.
DSR SOAM	4	8	120	1 Pair per DSR NF	Active/ Standby		
DA-MP	4	8	120	1 or 2 per DSR NF	1 or 1+1	The 1+1 configuration should have the DA-MPs on different servers.	There is a little value in having redundant DA-MPs (1+1) if they are on the same server, since the server is the thing that is most likely to fail.

Topology

Figure F-1 vDSR Setup

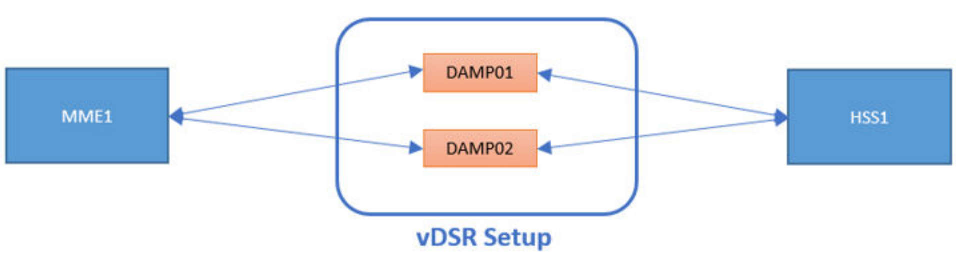


Table F-2 Performance Benchmarking Figures (Small DSR VM Profile)

Scenario	Call Flow Model	DSR MPS Achieved	DA-MP Flavor	DA-MP Profile	Avg Msg Size	CPU Peak	RAM Utilization Peak
Relay	100% Relay	12K (6K/MP)	4 vCPU	6K_MPS	2.0 K	25%	42%
RBAR	100% RBAR	12K (6K/MP)	4 vCPU	6K_MPS	2.0 K	35%	35%

G

24 vCPU Profile Testing on Oracle X9-2

This section provides DSR Benchmarking results for the KVM/Oracle X9-2 server using a 24 vCPU profile.

Topology

Figure G-1 Topology for KVM/Oracle X9-2 server with 24 vCPU Profile

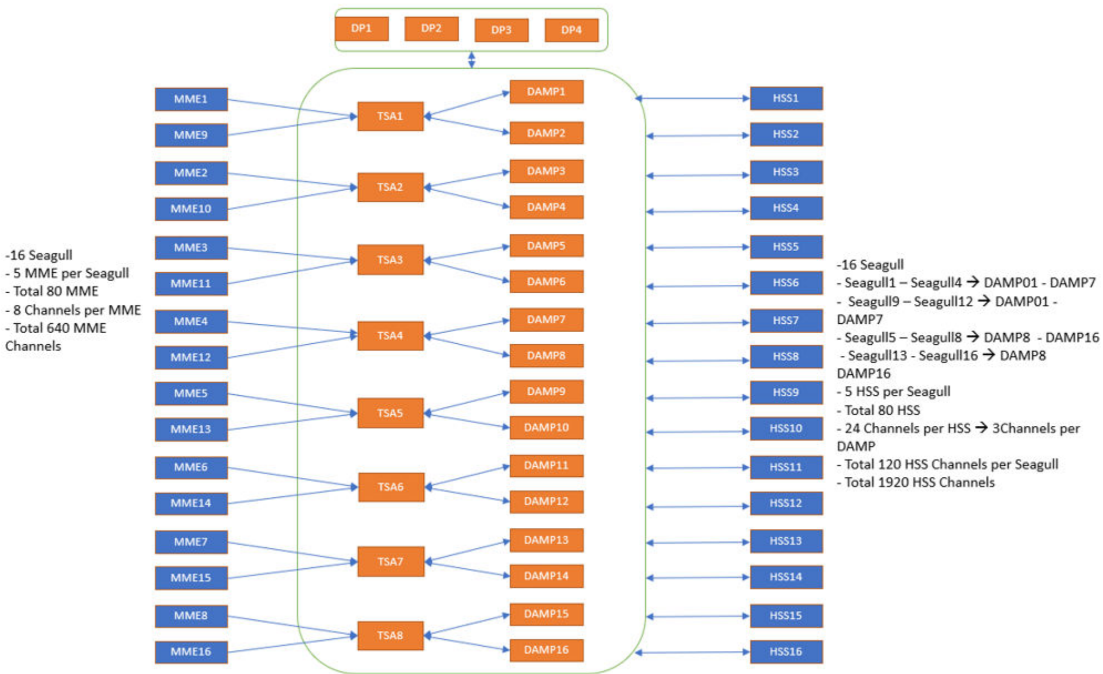


Table G-1 Performance Benchmarking on Oracle X9-2

Scenario	Call Flow Model	DSR MPS Achieved	DA-MP Flavor	SDS DP Flavor	DA-MP Profile	Avg Msg Size	CPU Peak	RAM Utilization Peak
Relay	100% Relay	720K (45K/MP)	24 vCPU	24 vCPU	40K_MPS_FABR	2.0 K	21%	20%
FABR + Relay	70% FABR + 30% Relay	664K (41.5K/MP)	24 vCPU	24 vCPU	40K_MPS_FABR	2.0 K	36%	23%