Signaling Delivery Controller

Product Description

4.4

Catalog Number: GD-015-44-45 Ver. 2

Publication Date: May 2015

Legal Information

Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

AskF5, F5, F5 [DESIGN], F5 Networks, OpenBloX, OpenBloX (design), Rosetta Diameter Gateway, Signaling Delivery Controller, SDC, Traffix, and Traffix [DESIGN] are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents indicated at: *http://www.f5.com/about/guidelines-policies/patents*

Confidential and Proprietary

The information contained in this document is confidential and proprietary to F5 Networks. The information in this document may be changed at any time without notice.

About F5 Networks

F5 Networks (NASDAQ: FFIV) makes the connected world run better. F5 helps organizations meet the demands and embrace the opportunities that come with the relentless growth of voice, data, and video traffic, mobile workers, and applications—in the data center, the network, and the cloud. The world's largest businesses, service providers, government entities, and consumer brands rely on F5's intelligent services framework to deliver and protect their applications and services while ensuring people stay connected. For more information, visit *www.F5.com* or contact us at *Tfx_info@f5.com*.

About this Document

Document Name: F5 Signaling Delivery Controller Product Description

Catalog Number: GD-015-44-45 Ver. 2

Publication Date: May 2015

Document Objectives

This document provides an overview and a high level functionality description of the F5 Signaling Deliver Controller (SDC).

The target audience of this document includes Network and Solution Architects and Program and Product Managers.

Document History

Revision Number	Change Description	Change Location
May 2015 – Ver. 2	Updated trademark text.	

Conventions

The style conventions used in this document are detailed in Table 1.

Table 1: Conventions

Convention	Use
Normal Text Bold	Names of menus, commands, buttons, user-initiated CLI commands and other elements of the user interface
Normal Text Italic	Links to figures, tables, and sections in the document, as well as references to other documents
`Script`	Language scripts
`Courier`	File names
Note:	Notes which offer an additional explanation or a hint on how to overcome a common problem

Convention	Use
Warning:	Warnings which indicate potentially damaging user operations and explain how to avoid them

Table of Contents

List of Figures

List of Tables

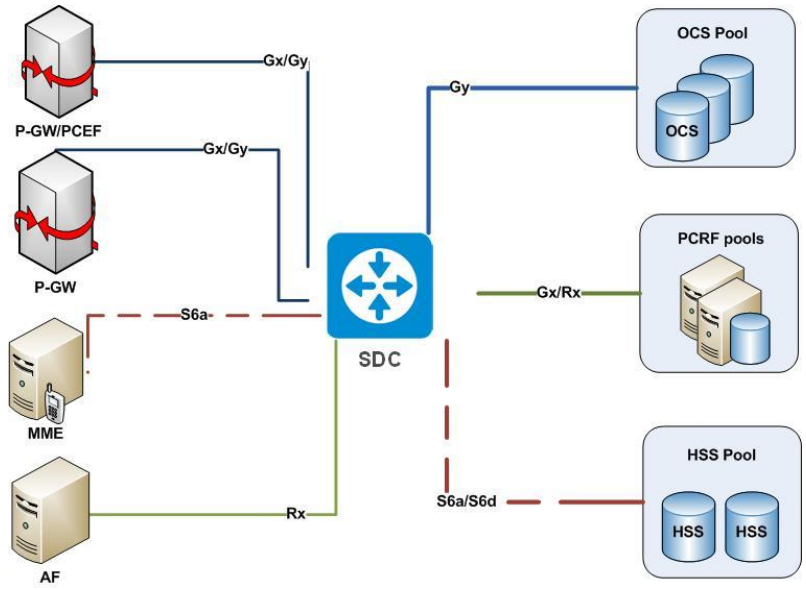
1. Introduction to SDC

The F5® Traffix® Signaling Delivery Controller™ (SDC) is a modular signaling platform that provides a flexible and robust solution for the emerging control plane connectivity challenges. The SDC is shown in *Figure 1*.

The SDC was designed to meet the demanding requirements posed by the growing volume of signaling traffic and the complexity of connectivity and signaling in LTE and IMS networks with advanced Diameter Gateway, Diameter Load Balancer, and Diameter Router solutions, consolidated on a single, unified platform.

The SDC enables service providers to scale and manage services and applications in LTE and IMS networks, supporting millions of concurrent sessions and hundreds of millions of subscribers. The SDC solution centralizes signaling and Diameter routing, traffic management, and load balancing tasks to scale and grow IMS and LTE networks incrementally and cost effectively, while increasing resiliency and reliability to support the subscriber's ever increasing service and broadband demands.

Figure 1: Signaling Delivery Controller



The core functionality of SDC is based on a powerful contextual routing engine which allows definition and execution of different routing policies that simplify the control plane network management. The routing engine, together with advanced load balancing algorithms, fast failback detection, failover mechanisms, and congestion control, provide unprecedented scalability and high-availability of Diameter and other nodes.

When deploying the SDC between LTE, IMS, and legacy network elements, service providers gain multiple added-value benefits such as:

- **Simple and transparent** Diameter network configuration, administration, and maintenance. Easy installation procedures with a user friendly GUI makes SDC fast to deploy and easy to maintain. Its capabilities are extremely powerful, yet simple to configure and modify. Automatic cluster detection and a secure configuration replication among parallel cluster nodes reduce the administrator's efforts to minimum.
- **Comprehensive network management** using Diameter contextual routing engine that reduces and centralizes the routing logic and reliefs Diameter nodes from handling this logic.
- **Congestion control** for Diameter servers using advanced in-band health monitoring, overload detection and throttling mechanisms. Using the health monitoring mechanisms, SDC manages back-end failures and reduces the risk of unintentionally sending traffic to overloaded or unavailable servers.
- **Scalability** of Diameter server nodes (such as PCRF, HSS, OCS) using Layer 4-7 load balancing algorithms, and fast failover detection and failback mechanisms. Combined with congestion control mechanisms, SDC assures that signaling traffic is sent to healthy servers and that after unhealthy server recovery, it is automatically and gradually reintroduced to the network.
- SDC provides **flexibility, scripting and customization**. SDC provides full user control for definition for routing and transformation script rules using the Java-based

Groovy scripting language. Using this flexible scripting, SDC can detect errors in messages or perform interaction with external systems while executing routing decision. When interaction with external systems is required, SDC can be integrated with 3rd party, Java-based libraries.

- **LTE to legacy interoperability interconnectivity** between new Diameter-based functionalities and legacy infrastructure using legacy signaling protocols.
- Service level **security** and **authorization** for Diameter. To avoid Denial of Service and Distributed Denial of Service attacks, SDC runs different heuristics to protect the system from overrun attempts and invalid requests. It also controls and fine-tunes Denial of Service protection through ACLs.
- **Visibility** into Diameter level performance. The management console allows real time performance visualization and monitoring of SDC internals and back-end servers. The performance counters are also available through multiple methods that allow import to external monitoring systems.
- **Carrier grade** product using off the shelf hardware. SDC supports **front-end failover** using multiple **Virtual IPs**. Using multi-threading and internal load balancing, the SDC performance scales linearly with the number of cores/processors and the number of SDC blades. The scale out ability protects SDC and the signaling network from multiple compound failures.
- **Centralized Management**. In multi-site deployments, the **Element Management** System (EMS) receives data (counters, states, alarms) from each SDC site, and enables global configuration of many aspects of the SDC sites in the deployment.

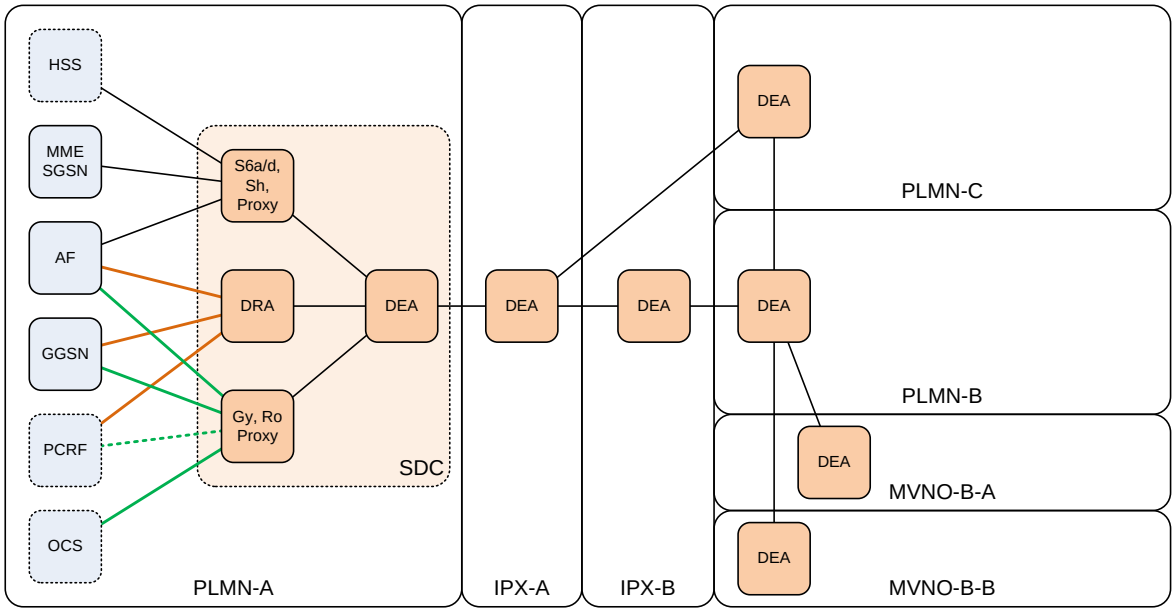
The SDC provides Diameter protocol routing, mediation and interworking functions, allowing service providers to manage legacy to LTE and LTE to LTE roaming seamlessly. By avoiding the need of complex integration and customization projects, SDC provides a simple, reliable, and easy to deploy solution to the most challenging control plane connectivity issues.

The SDC is the market's only fully native Diameter solution and can be deployed as an IETF Diameter Agent (relay, proxy, redirect and translation), 3GPP Diameter Routing Agent (DRA), GSMA Diameter Edge Agent (DEA) and 3GPP Interworking Function (IWF).

2. Supported Implementations

SDC's deployment modes are depicted in *Figure 2*.

Figure 2: End to end Diameter Architecture



Multiple types of service and network providers can benefit from the SDC's capabilities. The specific SDC implementation will depend on the provider's needs, and can be one of the following:

- **Core Network:** SDC is deployed in the PLMN and enables management and scaling of the internal network. *Figure 2* depicts an internal network deployment for PLMN-A. In this deployment, SDC is used (1) S6a/d and Sh Proxy for HSS; (2) Gy/Ro Proxy for OCS; (3) Gx/Rx DRA between GGSN/AF and PCRF. SDC in PLMN-A provides the routing and load-balancing functionalities for Diameter nodes, and gateway/mediation functionalities with non-Diameter nodes. The functionality split is logical and all the functionalities are served by a single SDC deployment.
- **Edge:** The SDC is deployed at the edge of administrative domains, e.g. PLMN or IPX, and enables secure and interoperable roaming and single point of attachment between the partners. In *Figure 2*, edge network deployment is shown. In this

deployment, SDC is used (1) between PLMN and IPX; (2) IPX to IPX (3) PLMN to PLMN (4) PLMN to MVNO/ISP/OTT service provider.

SDC provides the security enforcement and border control functionalities between the domains. It hides the internal PLMN topology of Diameter nodes and provides interworking function with non-Diameter nodes.

In this mode SDC incorporates an IWF function as defined by 3GPP and supports DEA (Diameter Edge Agent) guidelines recommended by GSMA.

- **IPX:** SDC is deployed in IPX provider and performs traffic steering between domains based on the supported roaming agreements. When deployed in IPX carrier/wholesale carrier/roaming hubs, it provides a secure platform to protect the network and properly route Diameter traffic at ingress and egress points.

2.1 SDC in a Core Network

The SDC can be deployed in the core network of the service provider. When deployed in the core network, it reduces the operational burden posed by the peer-to-peer connectivity architecture defined between the different Diameter based network elements. In core network deployment, the SDC provides:

- Centralized management of Diameter signaling routing and flexibility in network configuration
- Native means for scaling up of the Diameter based servers by using Diameter based, message oriented load-balancing mechanisms
- Native methods for overload and failover management by using Diameter based, message oriented, congestion control mechanisms
- Mechanisms for message normalization and adaptation between Diameter variants and between Diameter and legacy protocols

In core network deployment, SDC can serve as a Proxy (*Figure 3*) or Redirect (*Figure 4*) routing agent:

- In proxy mode, all Diameter transactions between two Diameter nodes are transferred through SDC.
- In redirect mode, SDC participates in session establishment between two Diameter nodes, but it does not handle the Diameter transactions.

To leverage the benefit of Diameter message normalization or modification, the SDC should be deployed in proxy mode.

Figure 3: SDC Deployment as Proxy in Local Mode

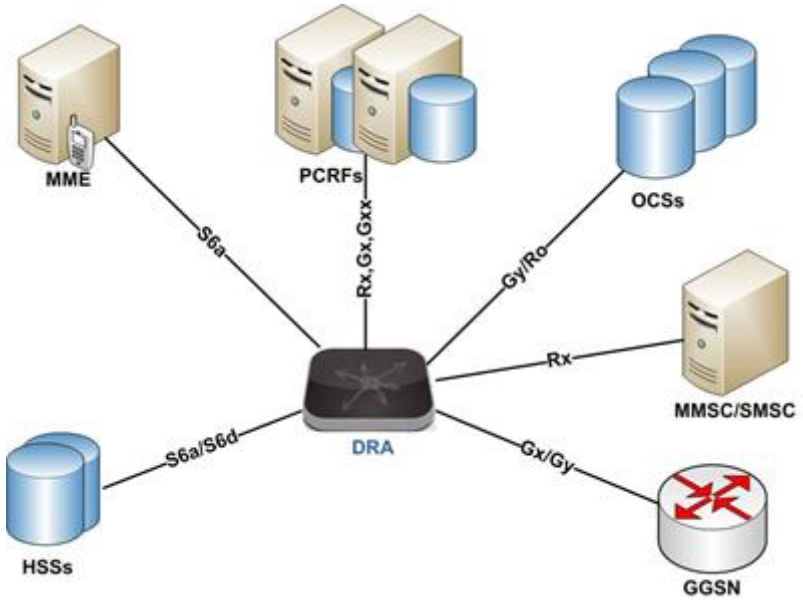
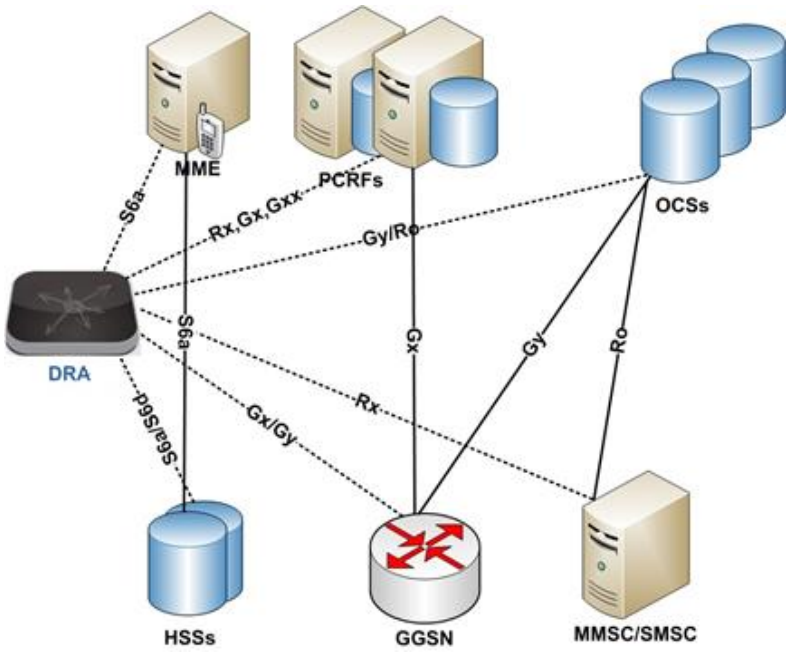


Figure 4: SDC deployment in Local Mode Using Redirect



2.2 SDC at the Edge of the Network

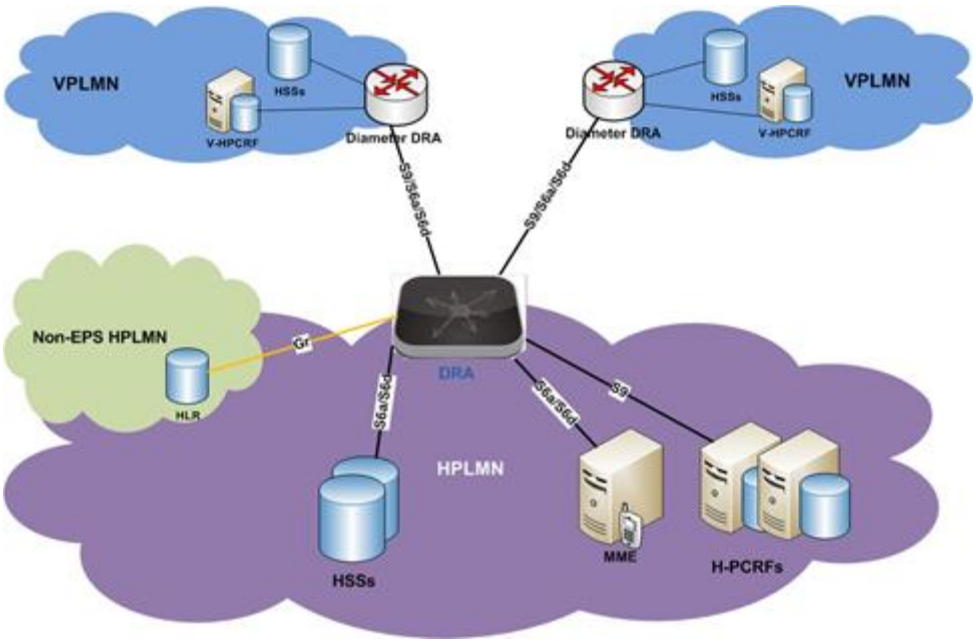
SDC can be deployed at the border of the service provider or IPX network. When deployed at the edge of the network, SDC serves as single point of attachment for roaming partners, other service providers or IPX network. Edge deployment of SDC is shown in *Figure 5*. In this deployment, SDC:

- Hides the Diameter network topology and performs Diameter traffic steering and routing based on predefined rules and roaming policies;
- Enforces Diameter security policies incoming Diameter connection and applies message normalization and adaptation.
- Does message normalization and adaptation between Diameter variants and between Diameter and legacy protocols.

SDC serves as an IWF function defined by 3GPP standards (29.805 and 29.305).

In edge deployment, SDC works as Diameter Proxy agent.

Figure 5: SDC Roaming Deployment

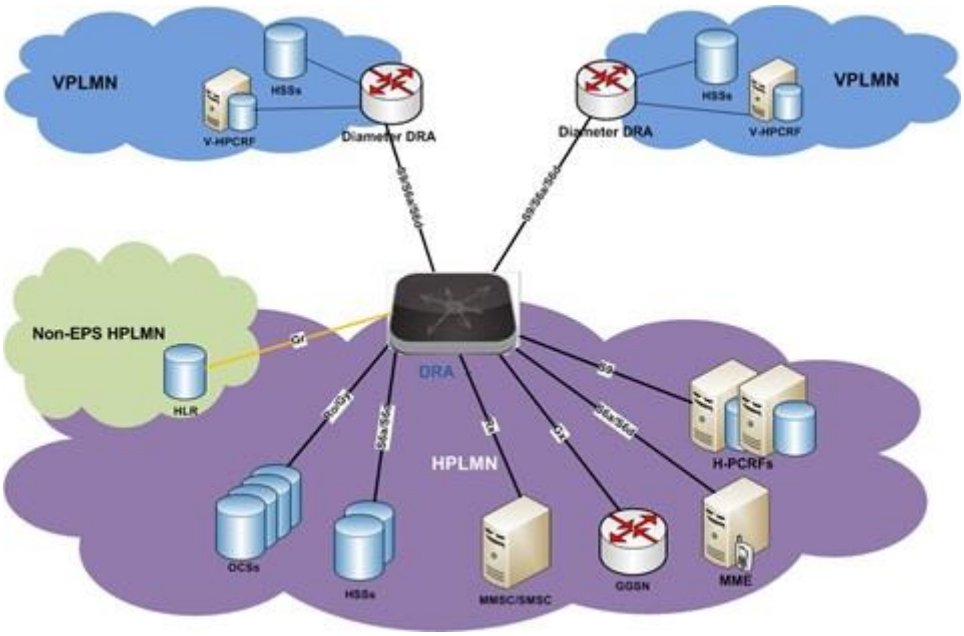


2.3 SDC in Dual Mode

In dual mode deployment, SDC serves as an internal network router and load-balancer. Dual mode deployment of SDC is shown in *Figure 6*. SDC routes traffic between different Diameter-enabled network nodes within the operator's network and provides roaming connectivity with partner service provider networks and MVNO/ISP networks using Diameter, SS7 and other protocols.

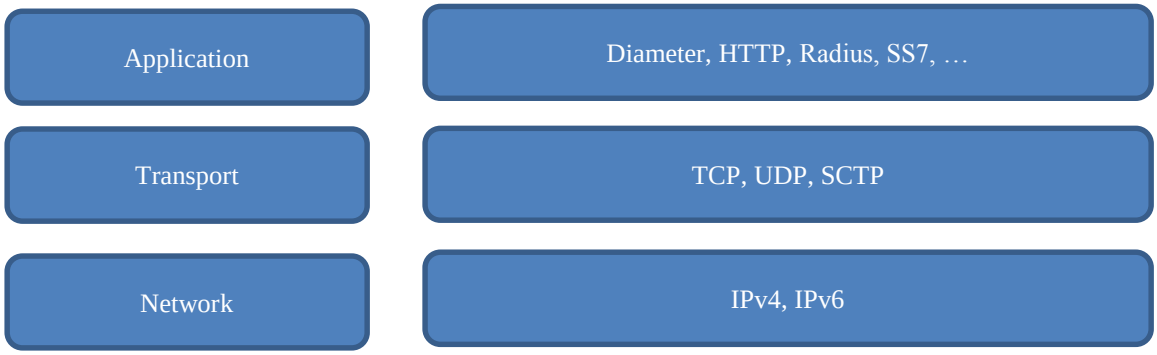
The SDC can work in dual mode, **Proxy** for roaming connection and **Relay** for the local PLMN.

Figure 6: SDC Dual Mode



3. Diameter and Legacy Protocols Support

The SDC solution provides support for the protocols described in this section



3.1 Diameter and 3GPP reference points support

SDC provides native Diameter support for IETF RFCs 3588, 6733, and related IETF RFC and for all reference points defined by 3GPP, e.g. Gx, Gxx, Rx, S6a, S6d, S9, S13, Sh, Ro, Rf, Gy, SWx. SDC also complies with GSMA and MSF guidelines.

SDC provides a flexible and simple mechanism for adding support for new Diameter interfaces, which is achieved by uploading the relevant Diameter data dictionaries. Uploading new data dictionaries is done in runtime and does not require software upgrade or maintenance downtime. The dictionaries are XML based.

The SDC solution provides seamless and transparent support for any vendor specific AVP. Multiple different versions of the same AVP, optionally, encoded differently, are transparently handled by the system. If AVP modification is required, the AVPs are added to the dictionary file with different names, allowing user access and modification.

3.2 Legacy Protocols Support

The solution supports simultaneous usage of multiple dictionaries, enabling SDC to interconnect with multiple Diameter nodes over multiple different reference points.

For the roaming or legacy connectivity, the SDC supports the following protocols:

- Telecom protocols, like RADIUS, SS7: MAP

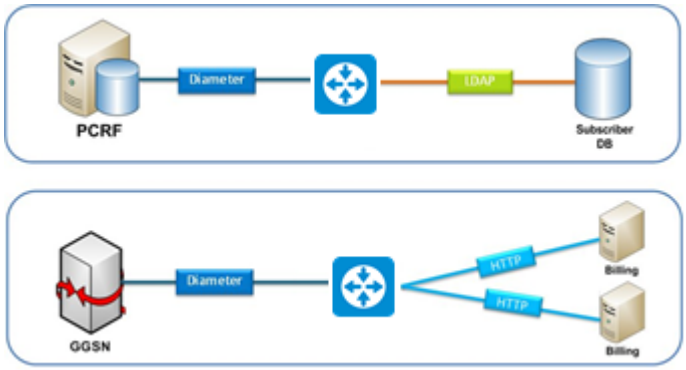
- Support for the SS7 MAP is provided by the SDC in a few ways. The implementation of the SDC as an IWF provides a variety of support scenarios between Diameter and MAP, including the following:
  - **Mobility management – an S6a/S6d - Rel8 Gr interworking scenario**

    In this interworking scenario, the SDC acts as an IWF directly connecting between a Diameter based MME or SGSN using S6a/S6d and a MAP based Rel8 HLR using Gr.
  - **Mobility management – an S6a/S6d - S6a/S6d interworking scenario with two IWFs**

    In this interworking scenario, the Traffic SDC acts as an IWF that works with an additional 3rd party IWF to connect between a Diameter based MME or SGSN using S6a/S6d, a Diameter based Rel8 HSS-MME or Rel8 HSS-SGSN using S6a/S6d, and an SS7/MAP based roaming agreement.
  - **IMEI check – an S13/S13' - Gf interworking scenario with one IWF**

    In this interworking scenario, the SDC acts as an IWF directly connecting between a Diameter based MME or SGSN using S13/S13’ and a MAP based Pre Rel8 EIR using Gf.
- IT protocols, like LDAP, HTTP, JMS, SQL (as shown in *Figure 7*)

Figure 7: Protocol Interconnectivity



3.3 Network and Transport Support

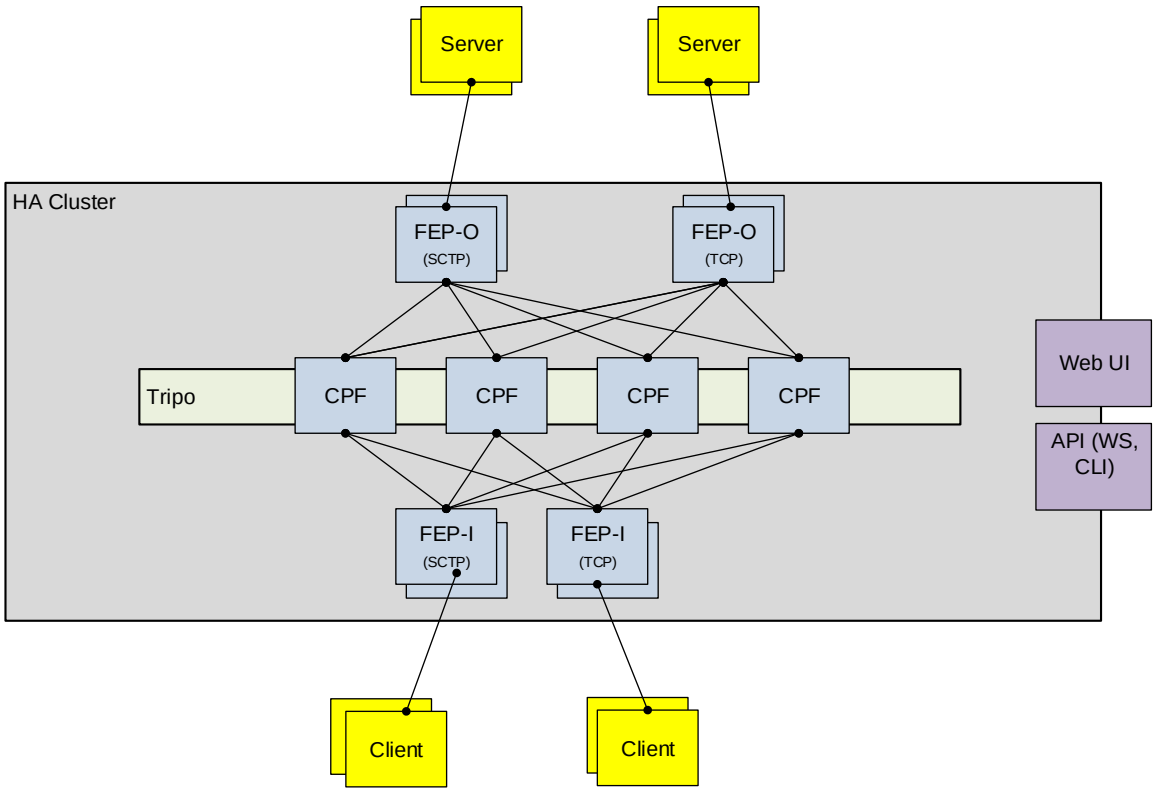
At the network layer, SDC provides support for IPv6 and IPv4. At the transport layer TCP, UDP and SCTP are supported.

SDC supports simultaneous use of SCTP and TCP transport protocols. It allows interconnecting between two peers that use different transport protocols; one peer can use SCTP, while the other is using TCP. It also supports interconnecting between two peers that use different network protocols, IPv4 and IPv6 protocols.

4. SDC Architecture

SDC is a modular platform that allows easy integration of new services, providing flexible mechanisms for adding new external components. As shown in *Figure 8*, external components can easily be added to the SDC by creating one point of contact between the component and a FEP or the component and a CPF. The architecture also allows CPFs to be added without affecting other system components.

Figure 8: SDC Platform Architecture



4.1 Central Management for Multiple SDC sites

The SDC Element Management System (EMS) supports multi-site deployments by providing a centralized point of control. When using EMS, each site is installed with an EMS agent and Splunk Forwarder components. These components, respectively, forward information to and receive information from the EMS manager and Splunk components in

the management site to create an overview of the deployment's performance and support shared global configuration parameters across multiple sites.

4.2 High Availability and Scalability

Standard SDC deployments provide high availability through local and/or geo-redundancy models. For example, for a DRA/DEA deployment, the following models are available:

- high availability-local redundancy
- high availability-local and geo-redundancy
- high availability-geo redundancy

4.2.1 Scalability

The SDC solution provides a vertical and horizontal scalability. Both options are standard, and provided out-of-the-box.

- **For vertical scalability**, it implements a message driven component, optimized for low latency processing and multi-core architecture and relies heavily on multithreading and asynchronous network I/O processing.
- **For horizontal scalability**, it allows use of multiple servers in two modes; "hot standby deployment" and "scalable deployment".

Horizontal scalability in SDC is achieved using built-in cluster management software. Typical "scalable deployment" is shown in *Figure 9,*

The clustering software:

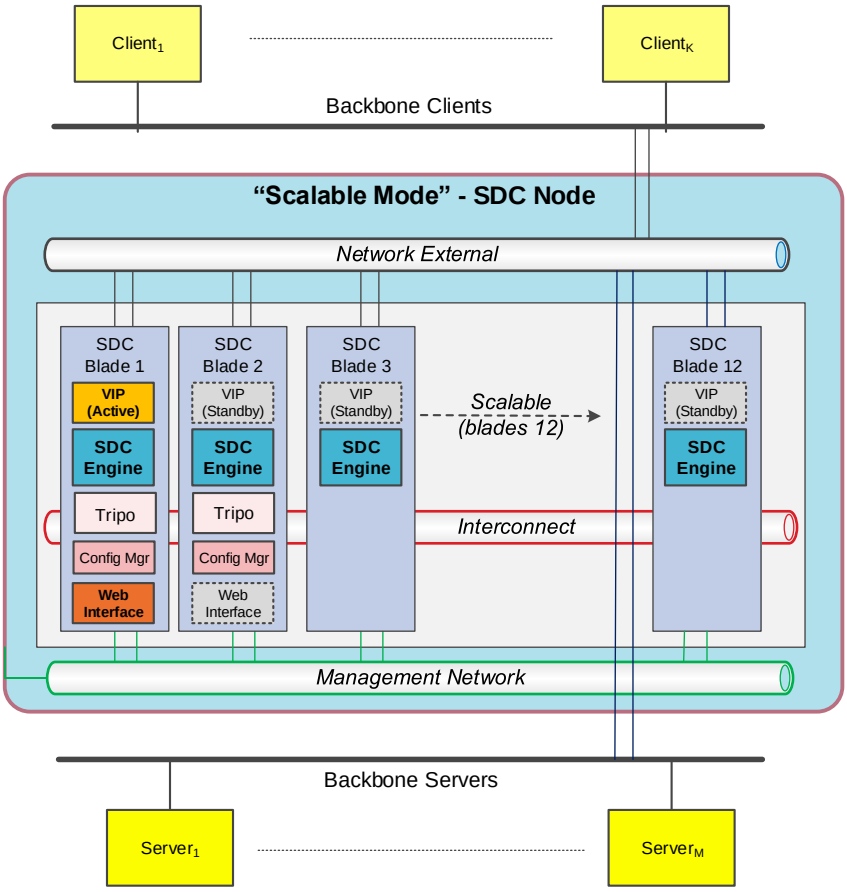
- Hides the internal structure of the node
- Presents VIP(s) for clients and servers
- Distributes the load between the blades
- Aggregates blade connections to Diameter peers

- Manages the different processes and services

For each of the deployed blades, the main software processes are:

- VIP is responsible for externalizing a single IP to ensure failover to another node in case of an active node failure
- SDC core process is responsible for processing of Diameter or other message oriented protocols, e.g. security, routing, load balancing and message transformation;
- Config Manager Process is responsible for configuration, distribution and storage;
- Tripo is the session data repository that stores all the sessions and user tables;
- The Web Console process provides a WEB interface for interactive system configuration and communicates with the Config Manager processes.
- The NMS agent process communicates with the EMS system and performs OAM tasks.

Figure 9: Scalable Deployment, Physical View



4.2.2 Local Redundancy and Scalability

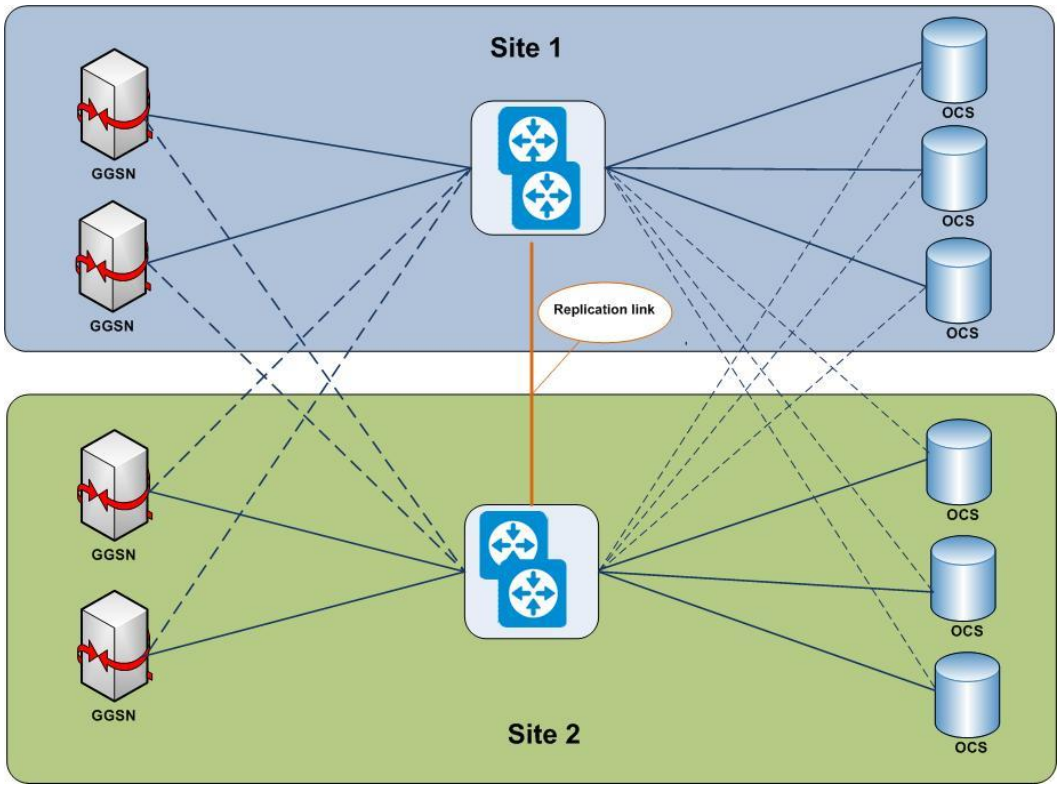
The SDC solution supports N+1 redundancy models. Any failure on the SDC side is transparent to both client and server peers and does not require any manual intervention or reconfiguration of the nodes.

Note: In Active/Active mode, the load is distributed among all available system nodes.

4.2.3 Geographical Redundancy

SDC supports geographical redundancy by deploying locally redundant SDC clusters in each geographical location site. Each of the locally redundant SDC clusters exposes one or more VIP address(es), as depicted in the following figure.

Figure 10: Geographical Redundancy, Active-Standby Deployment Mode



The solution supports multiple geo-redundancy deployment configurations, such as Active-Active or Active-Standby. Replication of routing and session tables is supported in both modes. Active-Standby and Active-Active deployments are shown in *Figure 11*, *Figure 12*, respectively.

Figure 11: Geographical Redundancy, Active-Standby Deployment Mode

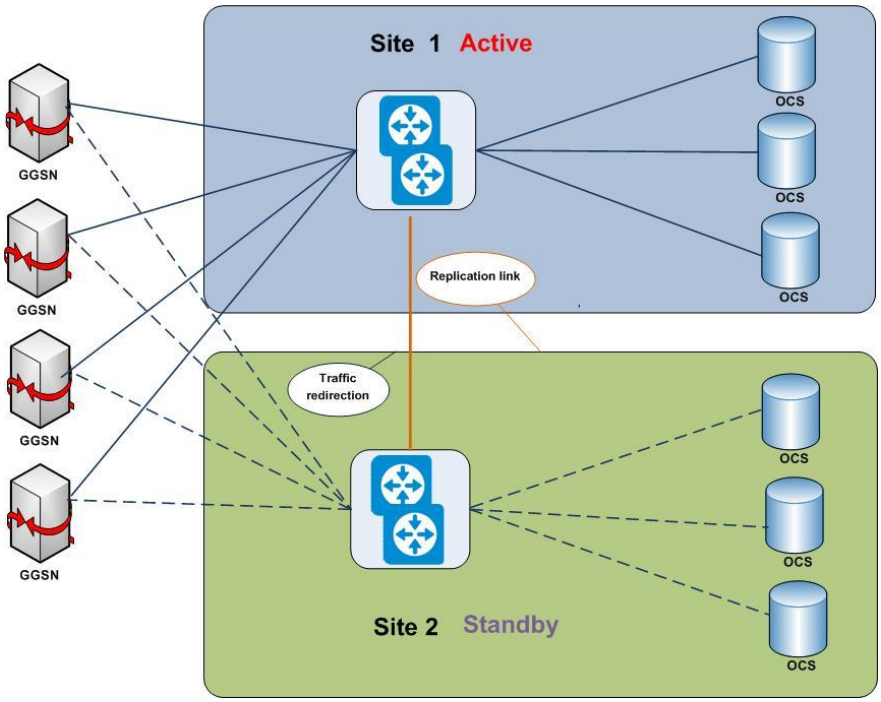
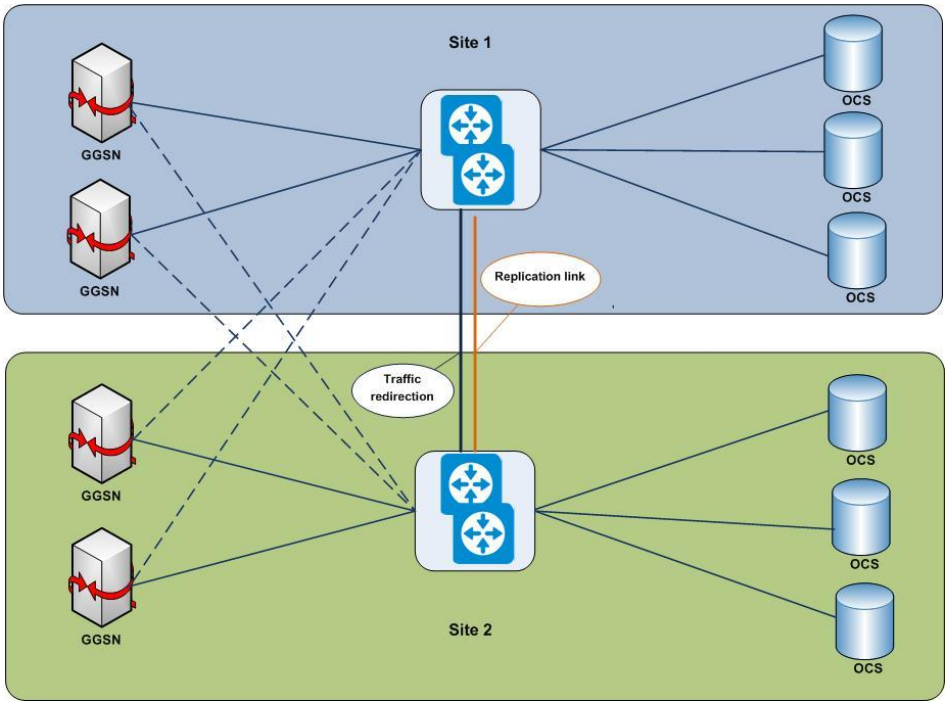


Figure 12: Geographical Redundancy, Active-Active Deployment Mode



4.2.3.1 Site Replication

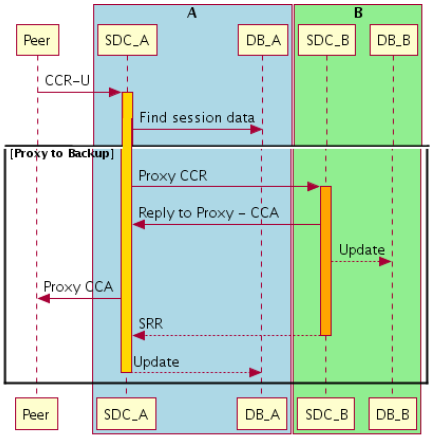
Site replication allows geographically distributed SDC clusters to synchronize Diameter session data amongst sites. Diameter session data includes the following:

- Destination Peer
- Pool name
- Origin Peer
- Session Binding data

Session data is distributed by one SDC node (the origin node) to Remote Servers (the target nodes) configured to receive and handle the replicated data.

An SDC node which receives a request may handle the request or proxy the request to a remote site. Proxying the request is performed when the session is unknown to the local site and the remote site has the required data to handle the incoming request, as depicted below:

Figure 13: Site Replication



This functionality is activated using a new proxy API in a pre-routing script. The network used for replication between sites must have sufficient capacity to carry the replication data traffic. Updates are streamed to the receiving system without expecting acknowledgment. In asynchronous mode, the replication latency has no impact on the system latency, but it

does affect the eventual consistency. For example: when the replication latency is 10ms, and each site handles 30K TPS where 5K TPS is a new session, and there are up to 100 TPS of routing updates, the following calculation is performed: "Lost updates"= 10/1000 * (5000 + 500) =~ 55 updates.

4.2.4 Hardware Support for High Availability

In order to support high availability, a system is required to utilize reliable processes and hardware, that is, to extend the mean time between failures (MTBF) and shorten the recovery time (MTTR). Extending MTBF is achieved by duplicating SDC nodes and using redundant hardware. SDC nodes can assume each other's load. These duplicate nodes are also called redundant components. The following tables detail different types of failure, their detection methods and remedy actions.

Table 2: Hardware Redundancy

Failure Type	Failure Detection Method	Automatic Remedy Action
Machine shutdown (Server motherboard)	Cluster heartbeat	Node failover / Traffic shift to other node
PSU (Power Supply Unit)	Built-in Hardware Monitoring	Failover to Redundant PSU
Disk failure	Hardware – RAID controller	RAID failover to 2nd disk
Network switch	Switch Redundancy mechanisms Network Link monitoring (OS)	Network Switch Failover Node traffic failover to secondary NIC

Table 3: Node Redundancy

Failure Type	FailurelDetection Method	Automatic Remedy Action
Scheduled shutdown / Reboot	Cluster resource mgmt and/or Service Monitor	Node failover / Traffic shift to other node

Failure Type	FailurelDetection Method	Automatic Remedy Action
Critical hardware failure	Cluster heartbeat	Node failover / Traffic shift to other node
Irreversible hardware failure	Cluster heartbeat	Node failover / Traffic shift to other node
OS Crash	Cluster resource mgmt and/or Service Monitor	Node failover / Traffic shift to other node
Low Memory	Resource Monitor utility or SNMP Monitor from external system	Send Notification to Operator (Low Memory)
Low Free Disk Space	Resource Monitor utility or SNMP Monitor from external system	Send Notification to Operator (Low Free Disk space)
CPU Overload	Resource Monitor utility	(in scalable architecture) Lower percentage of requests directed to system node

Table 4: Process Redundancy

Failure Type	Failure Detection Method	Automatic Remedy Action
Crash	Process watchdog “is running” check service monitor	Automatic Persistent data store recovery Process start
Lockup	Service monitor	Process forced termination Automatic Persistent data store recovery Process start
Partial lockup	Service monitor	Process forced termination Automatic Persistent data store recovery Process start
Cannot start	Cluster resource mgmt and/or Service Monitor	Node failover / Traffic shift to other node

Failure Type	Failure Detection Method	Automatic Remedy Action
SDC Overload	Service monitor	(in scalable architecture) Lower percentage of requests directed to system node

4.3 Networking

This section describes the SDC related network physical interfaces and addressing schemes, as well as, the supported network redundancy schemes.

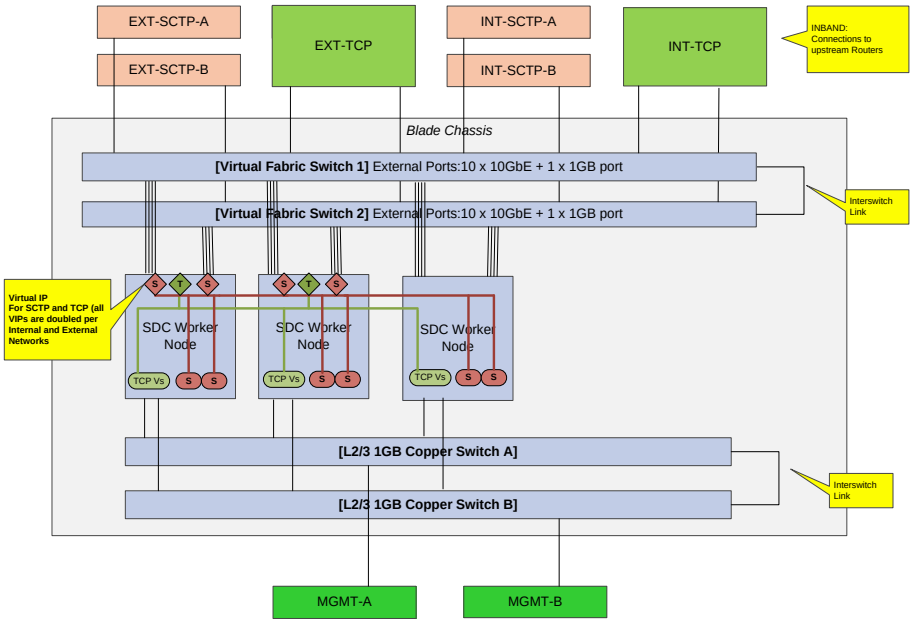
4.3.1 Network Redundancy

SDC applies the networking redundancy scheme for both TCP and SCTP transport protocols. The network redundancy is achieved using redundant pairs of Switch modules (one pair for Signaling traffic and another pair for OAM) and NIC bonding for TCP or multi-homing SCTP.

The local redundancy architecture, as shown in *Figure 14* is achieved in the following way:

- TCP VIP and SCTP VIP can be resident on the same or different SDC blades.
- The traffic is distributed to all available SDC nodes within the cluster
- The TCP and SCTP traffic distribution will be done based on Diameter messages using round-robin or other load balancing algorithm
- TCP and SCTP VIP's will not be dependent on each other

Figure 14: Local Network Redundancy Architecture



4.3.2 Physical Interfaces

The default physical interfaces and cabling of the SDC for HP and IBM infrastructures are detailed in the following tables:

Table 5: Physical Interfaces and Cabling

HP BladeSystem c7000 Chassis					
Network	**Switch**	**Interface Speed**	**Port Count**	**Connector type**	**Description**
Data Signaling	HP Virtual Connect Flex-10 Module	10GbE (or 1GbE)	6	10GbE Fiber 850mns or 1GbE Copper (RJ45) Ethernet	Data Signaling (Diameter, SIP, etc.)
			2	N/A	HP VC Flex-10 Stacking Links (no cables required)

HP BladeSystem c7000 Chassis					
	HP Virtual Connect Flex-10 Module	10GbE (or 1GbE)	6	10GbE Fiber 850mns or 1GbE Copper (RJ45) Ethernet	Data Signaling (Diameter, SIP, etc.)
			2	N/A	HP VC Flex-10 Stacking Links (no cables required)
OAM-OS: Management and Backup Network Connection	HP/BNT GbE2c L2/3 Switch 1	1GbE	5	Ethernet Copper RJ45	Connection to Management and/or Backup Networks
	HP/BNT GbE2c L2/3 Switch 1	1GbE	5	Ethernet Copper RJ45	Connection to Management and/or Backup Networks
OAM-LOM: Chassis Hardware and Switch (“Lights-Out”) Management and Monitoring	HP Onboard Administrator Module 1	1GbE	1	Ethernet Copper RJ45	Connection to Management Network, for Chassis Hardware and Switch (“Lights-Out”) Management and Monitoring
	HP Onboard Administrator Module 2	1GbE	1	Ethernet Copper RJ45	Connection to Management Network, for Chassis Hardware and Switch (“Lights-Out”) Management and Monitoring

4.3.3 Addressing Scheme

SDC supports the following default scheme of IP addressing. Detailed networking design is done after Site Survey and Customer Workshop.

Table 6: Scheme of IP Addressing

Failure Type	Automatic Remedy Action
Data Signaling	4 IP Addresses per Signaling Interface (e.g.: Diameter). Note: ▪ Additional addresses per signaling interfaces are supported ▪ Multiple signaling interfaces are supported ▪ Multiple Networks and/or VLANs supported ▪ IPv4 and IPv6 are supported ▪ SCTP Multi-Homing Supported ▪ If Solution is required to perform L3 routing 3 addresses per subnet will be required for (for VRRP Switch Redundancy)
OAM: Management and Backup Network Connection	One IP Address per hardware blade, plus one Management VIP (4 addresses in the baseline chassis configuration) ▪ Additional Management VIPs are supported ▪ Multiple addresses per blade are supported ▪ Multiple Networks and/or VLANs supported, e.g.: dedicated Management and Backup Interface ▪ Additional addresses will be required for a dedicated Backup Network connection
OAM-LOM: Chassis Hardware and Switch (“Lights-Out”) Management and Monitoring	Six (6) IP Addresses: ▪ 2 for Advanced Management Modules ▪ 4 for Switch Management

4.4 SDC Components

This section describes the SDC components and their roles.

4.4.1 Configuration Manager

The Configuration Manager serves as the system configuration repository, enabling configuration management and distribution between the SDC components. This module manages the configuration of the connected remote peers, and their status, protocol dictionaries, and deployed business rules.

The Element Management System (EMS), an optional add-on for multi-site deployments, manages the configuration information for certain components of the installed SDC sites.

4.4.1.1 Peer State Distribution

Peer state distribution is synchronized using JSON over UDP.

4.4.1.2 Web Services API

Managing the configuration of the remote peers, as well as routing, can also be performed with the SDC Web Service (WS) provisioning interface. The SDC Web Service (WS) provisioning interface is based on SOAP API and is integrated as part of SDC Management Console. The WS provisioning interface enables a user to use a limited set of commands of the SDC Management Console to configure, monitor the system, and for flow management.

4.4.1.3 Command Line Interface (CLI) Application

The CLI application interface enables a system administrator to use a predefined set of commands to define and manage SDC peers and pools.

4.4.2 Web Services UI

The SDC provides a web-based interactive UI management console for system configuration. It is also responsible for performance statistics collection and presentation.

4.4.3 Control Plane Function (CPF)

The Control Plane function is the core component in the SDC architecture, providing Session management, Routing, Load Balancing, and messages manipulation services.

CPF provides replication, alarms, and logging support, as well as basic functionalities required for integrating new services and modules that are not part of the standard deployment, enabling customization of the solution.

An example of such customization is adding support for SLF (Service Location Function) as an external application loaded by the solution. This SLF function is called within the solution rules management, and on its backplane it communicates with proprietary interfaces as supported by the Java application.

4.4.4 Front-End Proxy (FEP)

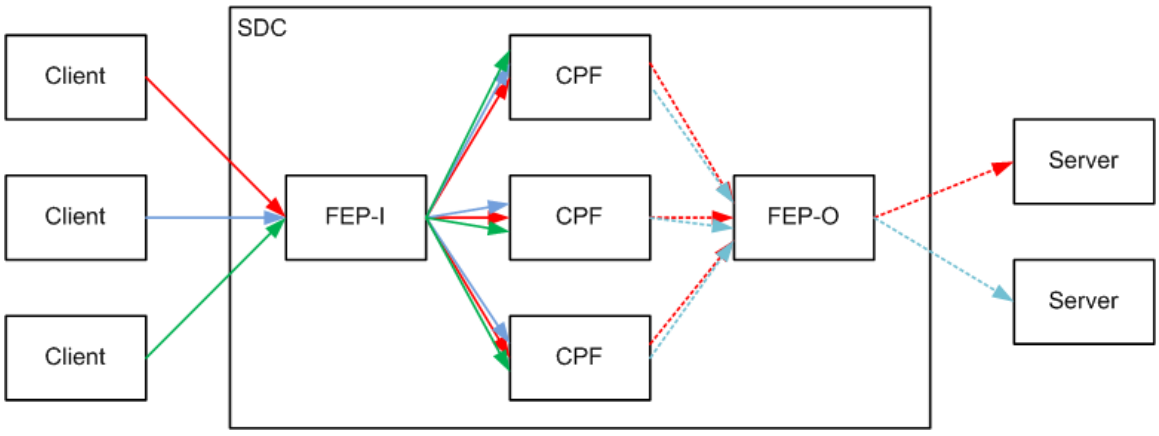
The Front-End Proxy is a network distribution point in SDC. It is built on top of the CPF framework to take advantage of the CPF management, pipeline and other infrastructures. FEP maintains a steady single connection of TCP with the multiple CPF nodes. For each Remote Node, it manages the connection and state machine, providing statistics and management capabilities for the connections and the traffic.

The FEP and CPF nodes, as aforesaid, share the same framework. Both nodes construct a transport pipeline with each of its peers. The FEP node is responsible for managing the peers' state machines, maintain and configure the connections.

As FEP is the connection point, and there usually is a single FEP in SDC, all Remote Servers are connecting to a single connection point, therefore the requirement to maintain a complex network with multiple links becomes redundant. Each Remote Server is now connected to the FEP while the FEP is automatically connected to all CPF nodes. Moreover, and as a byproduct, the topology is transparent to the user.

The following image depicts the basic network architecture:

Figure 15: FEP Network Architecture



The FEP nodes are bi-directional:

- FEP-I: A single network distribution point, hides the internal network architecture from external clients and performs Peer management
- FEP-O: A single network aggregation, hides the internal network architecture from external servers and performs Peer management

All FEP nodes are connected to all CPF nodes. When a new CPF node joins the cluster, all FEP nodes connect to it. When a new FEP node joins the cluster it automatically connects to all CPF nodes. The system supports a connectivity mechanism that ensures a stable connection between the FEP and CPF components.

4.4.5 Tripo

SDC supports dynamic routing based on stateful session management. The SDC session repository – the Tripo – manages the destination of the ongoing transactions per session. The session repository includes session replication between mated SDC sites.

4.4.6 File Server

In some routing scenarios when the online transaction processing cannot be performed, the not routed transactions should be persisted for later offline processing. The SDC File server is used to persist those messages.

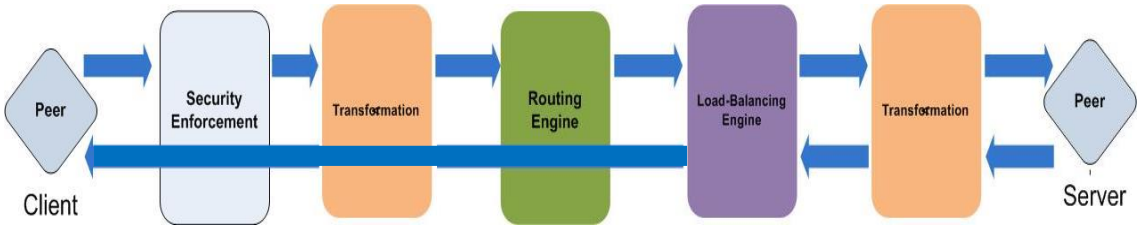
4.4.7 NMS Agent

The NMS Agent is an SDC site central component that collects information about system performance and forwards it to the EMS. The NMS Agent is also used to inform the northbound about unusual SDC system behavior.

5. The SDC Pipeline

The following pipeline is applied to traffic that is processed by the SDC.

Figure 16: SDC Pipeline Flow



The pipeline consists of the following processing elements:

- **Security Enforcement** manages access permissions with the client peers. Validation is done at the IP and Diameter (Application) levels.
- **Pre-Routing Transformation** adapts the incoming message to the SDC format needed to perform effective routing
- **Session Management** manages routing decisions on a session level and replicates session data between SDC sites.
- **Routing** makes a routing decision based on the message content. The Routing decision results in the selection of a destination pool for the transaction. A pool must contain at least one server peer.
- **Load Balancing** chooses the peer from the pool to handle the transaction.
- **Post-Routing Transformation** adapts the outgoing messages to match the destination's format.

5.1 Security Enforcement

SDC enables service providers to apply policy control and different security methods on the peer nodes. This allows control of roaming connections with multiple roaming partners and protection of the signaling network from unexpected traffic.

The security enforcement is done by setting and applying security rules on both the IP and the application levels.

The Security rules at the IP level are defined in ACL format.

5.2 Pre-Routing Transformation

The message transformation mechanism implemented by SDC overcomes interoperability issues between different Diameter vendors and allows the translation from one Diameter protocol to another signaling protocol and vice versa. SDC provides full support for adding, modifying and/or removing AVPs based on user configurable rules. The rules are implemented using smart decision grids and Groovy scripting language, which provides configuration flexibility and simple management.

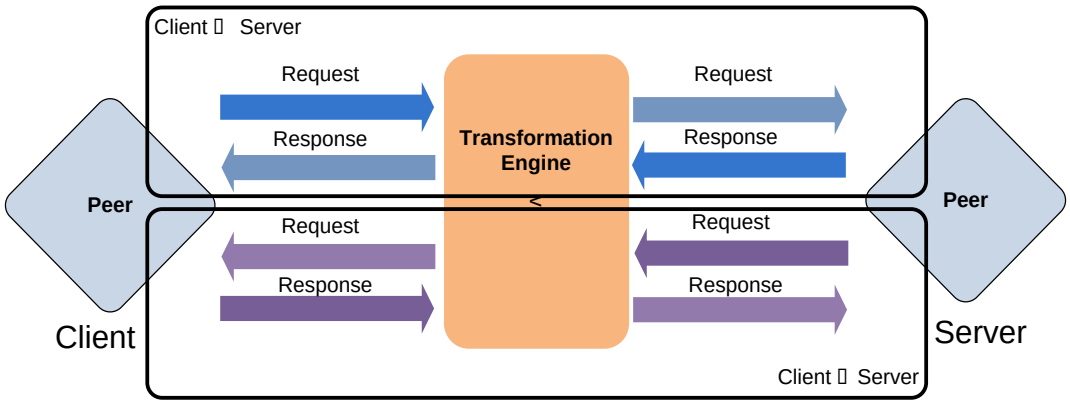
The solution enables bi-directional Diameter message modification and provides the ability to create different rules of message modification according to the direction of the message flow and/or message type, for example:

Modification of Client initiated messages

- Client->Server Request (such as CCR)
- Client->Server Answer (such as RAA)

The message transformation process is shown in *Figure 17*.

Figure 17: A 4 Way Message Transformation



As seen in the above figure, SDC provides the flexibility by defining transformations of **Client Requests** and **Client Responses**.

SDC supports message transformation between Diameter, LDAP, RADIUS, and HTTP nodes, and between nodes of the same type.

5.3 Routing

SDC implements an advanced routing management engine which provides service providers with flexibility to implement different routing rules and policies required to satisfy their business requirements.

Routing rules apply different criteria using combinations of Diameter AVP's, request source, and other properties to make decisions. The routing engine is fully integrated with load balancing policies and the transformation engines to provide a harmonized solution for the most demanding and highly complex deployments.

The SDC routing management also supports routing resolution using external systems or service location functions such as SLF, DNS, LDAP or SQL. These routing scenarios can be applied separately or together.

5.3.1 Basic Routing

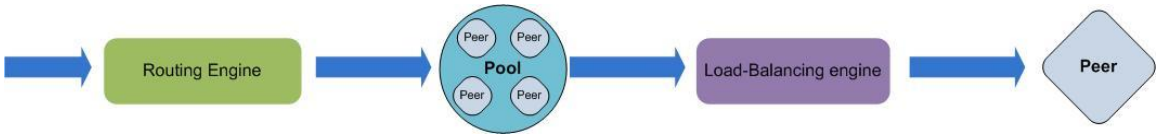
Basic routing decisions result in the selection of a destination pool for the established Diameter session. Pool selection is done using a combination of different AVPs such as Subscription-Id, APN from Called-Station-ID, Application-ID, Source-Peer, etc. The values of the AVPs of the incoming requests are matched with condition sets defined for SDC routing rules or by resolution against external service location functions.

After the basic routing decisions are completed, the load balancing algorithm is applied.

The flow of actions is shown in *Figure 18*. After the destination peer is selected, all messages for the appropriate Diameter session are sent to the selected node.

For failover scenarios, where errors are detected in the remote nodes or they are disconnected, please see *Overload and Congestion Control*.

Figure 18: Routing Flow Using Defined Criteria in the SDC



5.3.2 Routing Using External Location Functions

In some deployments, routing decisions should be retrieved from an external system.

SDC supports several methods of retrieving the routing decisions.

1. **Using internally provisioned routing rules**, the routing rules are provisioned using SOAP API to the SDC internal provisioning database. When a new Diameter session is established, SDC fetches the destination from its provisioning database. When provisioning routing entries, expiry time can be set for the provisioned entries, or they can be kept on a permanent basis.

   In addition to provisioning, SDC can calculate routing decisions, or apply default decisions if routing decisions can be fetched from the internal database.

2. **Using the retrieval function, which implements LDAP, SQL or SOAP**. After a new Diameter session's establishment, SDC will send a request to the location function. The request will include the query parameters, and the response will contain the appropriate pool for the specific request. The query parameters are extracted from the Diameter request's AVPs or calculated by the routing engine.

3. **Using a 3rd party library integrated with SDC**. The following method implements the same logic as described above, but instead of sending requests to an external system, SDC performs programmatic call to an external library integrated within it.

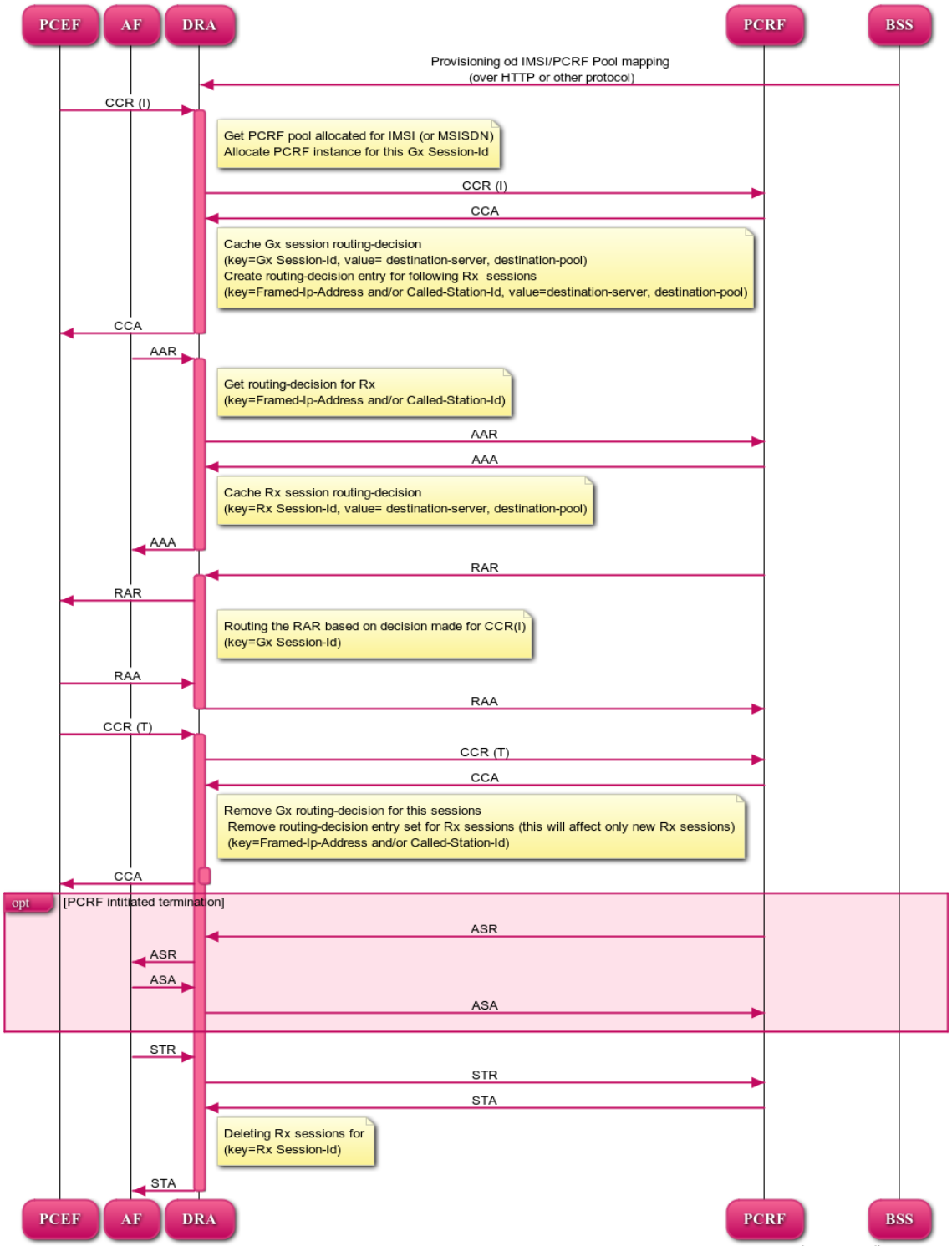
The rules can be broad, e.g. using MCC/MNC, or fine-grained, using IMSI, or other combination of values.

SDC provides a caching functionality for the routing policies. The use of internal caching for routing decisions reduces the overall response time for the Diameter transactions.

5.3.3 Routing Decision Binding between Different Diameter Reference Points

For some Diameter reference points, there is a need to bind sessions originating from different network elements and share common attributes. Bound sessions are handled as a session bundle composed of several sub-sessions. One of such scenarios is IP-CAN session binding, as described in 3GPP 29.213. IP-CAN session binding is required to associate between Rx and Gx session for the same UE. After PCEF establishes a Gx session with the selected PCRF for some UE, all Rx sessions associated with the same UE should be routed to the same PCRF. The process of IP-CAN session binding is shown in *Figure 20*. SDC supports this binding functionality using sets of common AVPs that are available for both reference points. The functionality is available out-of-the-box. For example, for Gx and Rx it can be "Framed-IP-Address" or a combination of "Called-Station-ID" and "Framed-IP-Address".

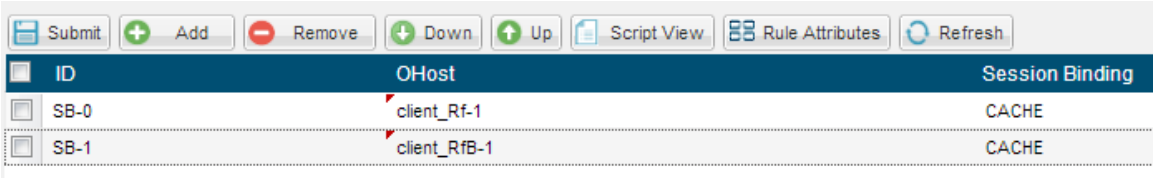
Figure 19: GX and RX Session Binding



Bound sessions are related to as Slave Sessions subject to their Master Sessions. The Master Session is the session for which the routing selection is performed based on the routing rules. Slave Sessions are applied with routing rules inherited from the Master Session.

The session binding is done using one of several session binding methods and based on binding keys. Binding Keys are sets of values extracted from different attributes (e.g. AVPs or XML attributes) of the Master Session and used to bind several session identities.

Figure 20: Session Binding in the SDC Management Console

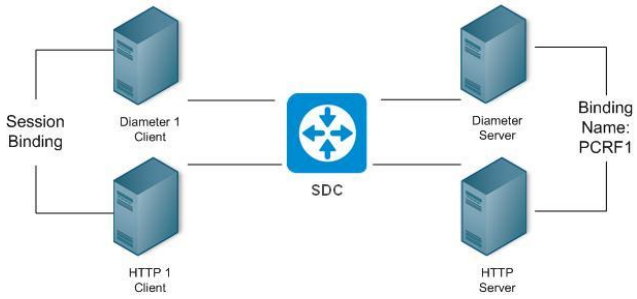


5.3.4 Multi-Protocol Session Binding

Multiple-protocol session binding is applied by linking Destination Server Peers, in addition to the routine client session binding. When two destination servers share a Binding Name they act as a cluster of servers in which each server handles its corresponding sessions, when handling sessions originating from multiple-protocol Clients.

For example, when a Slave Session originates from an HTTP Client Peer and the Master Session originates from a Diameter Client Peer, two Destination Server Peers are required to handle the bound sessions: an HTTP Server and a Diameter Server, respectively. Each time the Diameter Server is selected to handle a Diameter Master session, the Master Session's Slave Sessions are directed to the HTTP Server subjected to the Diameter Server, as depicted in the following image:

Figure 21: Multi-Protocol Session Binding



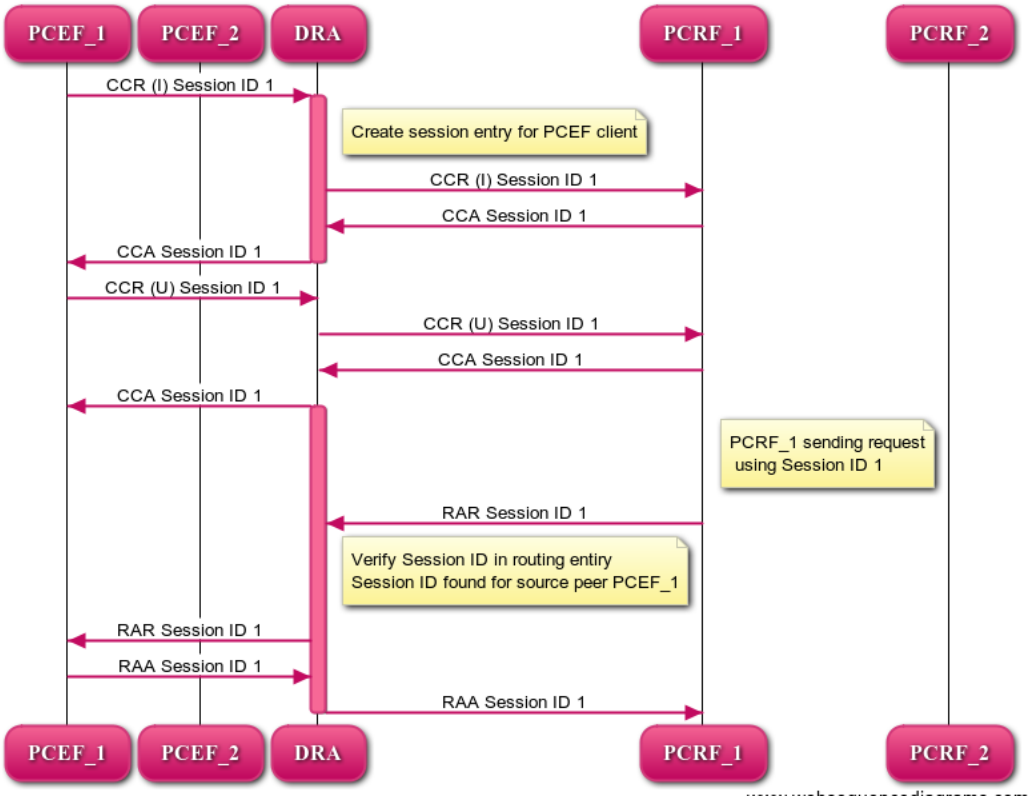
5.3.5 Bi-directional Routing

Bi-Directional routing is natively supported by SDC. Two scenarios of bi-directional routing are handled by the system,

1. **In session routing**

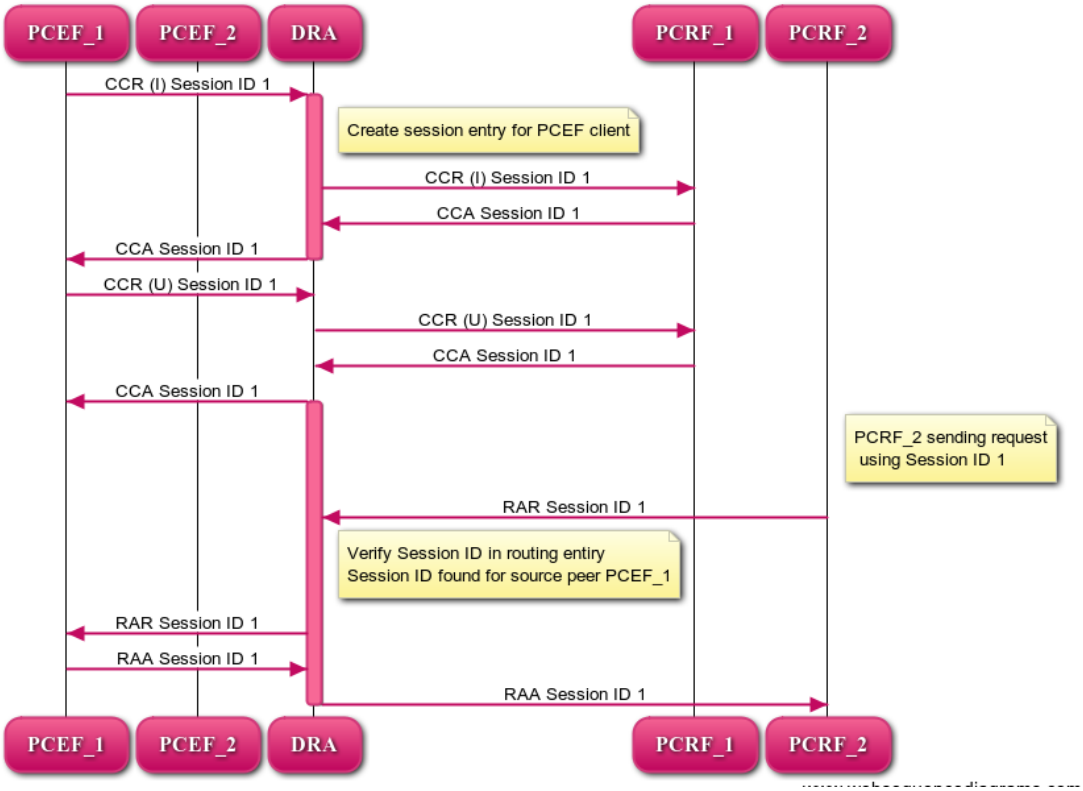
   In this scenario, the Diameter server peer sends the request (e.g. RAR) to the Diameter client peer using the same Diameter Session-ID that was previously established by the Diameter client side. SDC routes the request to the client that established the session as shown in the call flow depicted in *Figure 22*.

Figure 22: In session Call Flow of Server Initiated Diameter Request



SDC accepts requests from different server peers as long as the requests share a Session-ID that was established by the client peer, as shown in the call flow depicted in *Figure 23*.

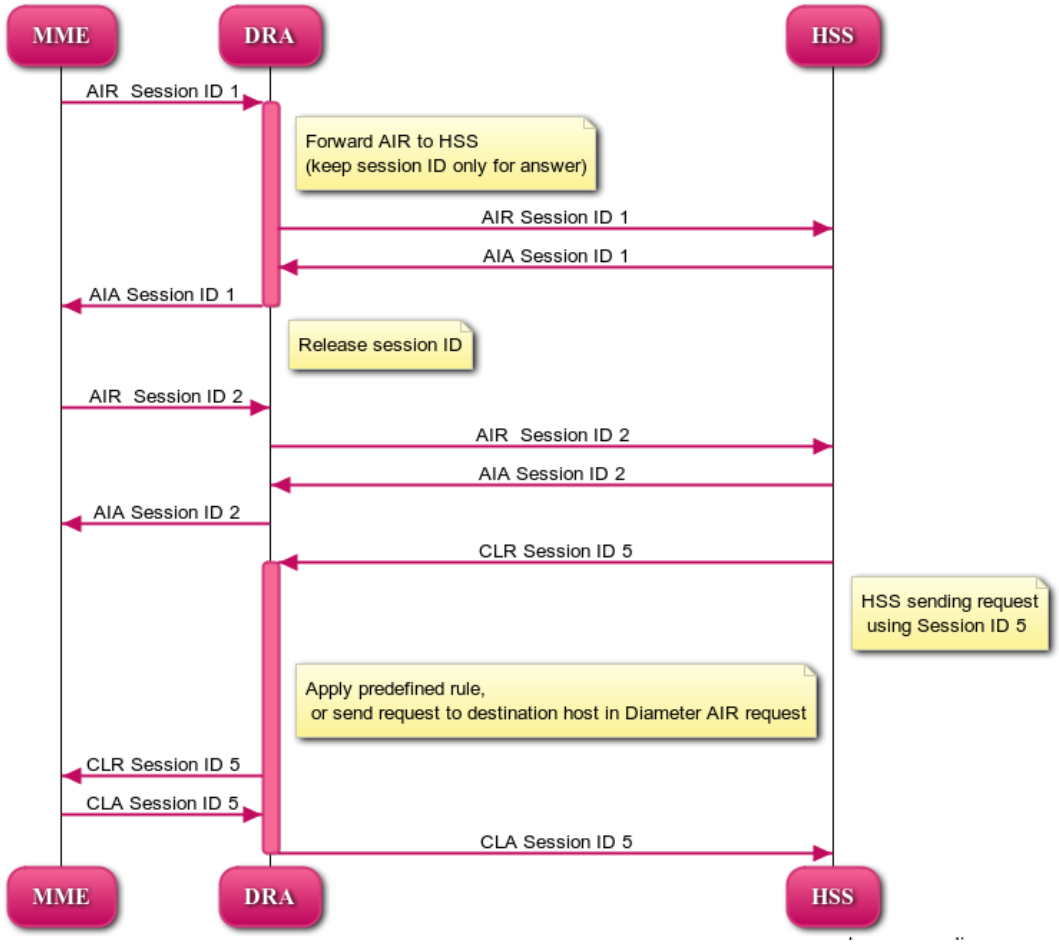
Figure 23: Call flow of Diameter Server Request, Where the Server Peer Is Changed



2. **Out of session routing**

In some cases the communication between the Diameter client and server peers is stateless, meaning that SDC does not maintain a reverse path for the Session-ID. To allow proper handling of out of session server initiated Diameter request, SDC implements advanced routing rules that can be used by the user to define the required behavior. In case no rule is set, SDC sends the request to a client based on the request's "Destination-Host" AVP. This behavior is shown in *Figure 24*.

Figure 24: Out of Session Call Flow of Server Initiated Diameter Request



5.3.6 Redirection

The SDC routing engine supports working in redirect mode. In this mode SDC acts as a Diameter DNS and leases routing decisions to the clients for a predefined and configurable amount of time.

5.3.7 Routing Example

An example of a complex routing rule that can be implemented in SDC is shown in the following figures:

Figure 25: Routing Rule Attributes

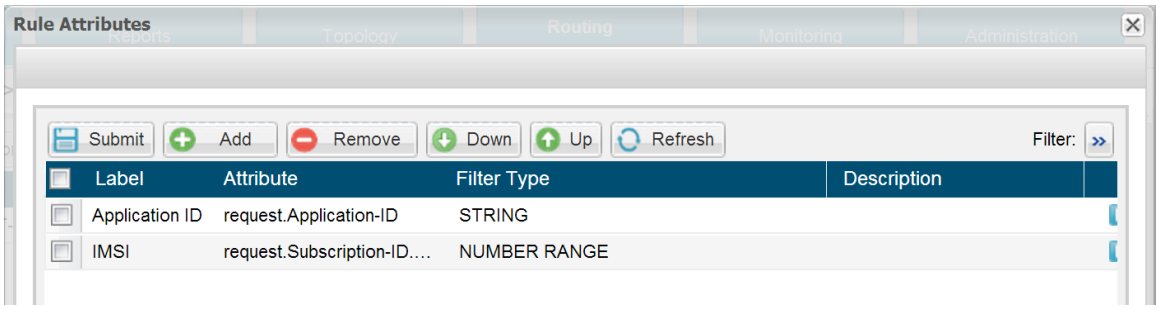
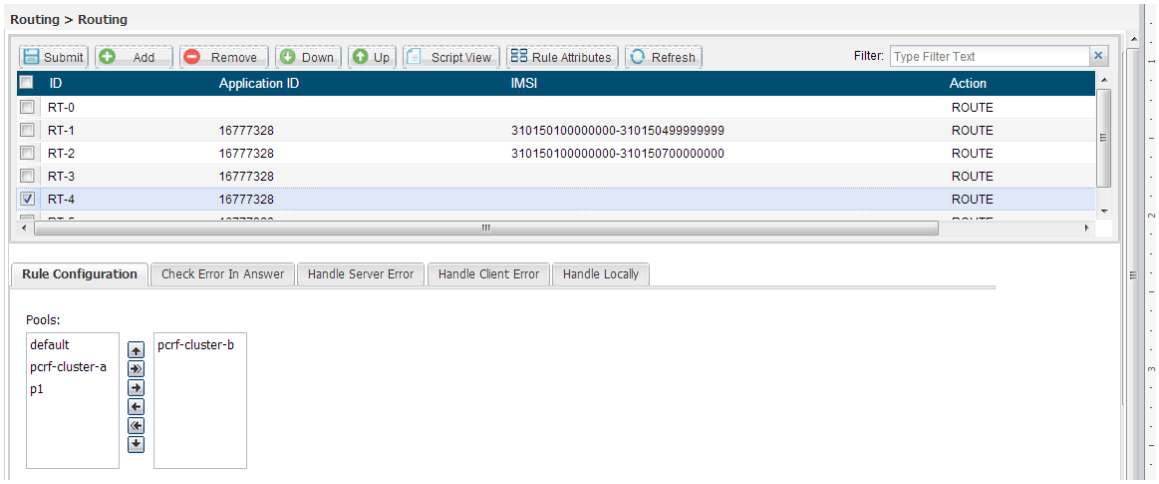


Figure 26: Routing Rule

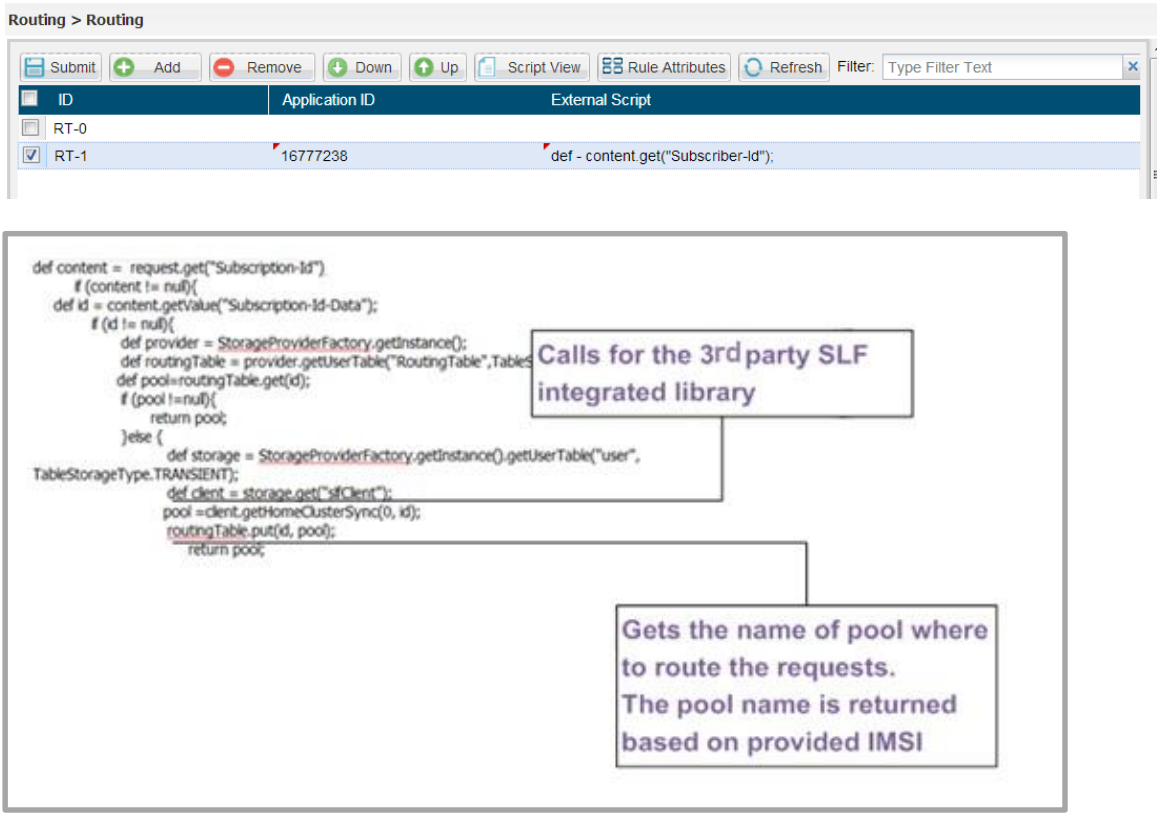


The routing rule shown in *Figure 26* is applied on the Gx Interface. The rules selects which PCRF pool to route a particular session,

- The selection is based on IMSI range.
- The IMSI value is retrieved from "Subscription-ID-Data" AVP, which is part of grouped AVP called "Subscription-ID" and compared to two ranges of IMSIs.
  - The first range is routed to “pcrf-cluster-a”,
  - The second range is routed to “pcrf-cluster-b”.
- If the Subscription-ID-Data AVP is missing or IMSI is not in range, the system routes the traffic to the “default” pool.

Alternatively, the Routing Rule can query an external data source – as shown in *Figure 27* - to obtain the routing decision.

Figure 27: Sample Routing Script Using External Data Source



The routing decision is made upon Diameter Session establishment. The decision persists for the duration of the Diameter session.

5.4 Load Balancing Policies

Load Balancing policies are used when messages are routed to a pool of server peers. The peer selection is based on the pool's defined load balancing policy. The load balancing policies provided by the SDC are described in *Appendix D: Appendix D: Load Balancing Policies.*

5.5 Outgoing Message Transformation

The message transformation mechanism implemented by SDC overcomes interoperability issues between different Diameter vendors and allows the translation from one Diameter protocol to another signaling protocol and vice versa. SDC provides full support for adding, modifying and/or removing AVPs based on user configurable rules. The rules are implemented using smart decision grids and Groovy scripting language, which provides configuration flexibility and simple management.

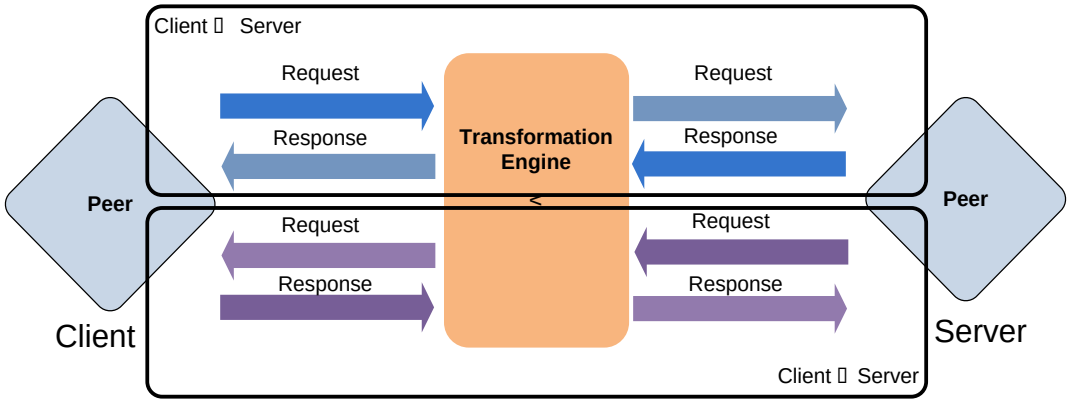
The solution enables bi-directional Diameter message modification and provides the ability to create different rules of message modification according to the direction of the message flow and/or message type, for example:

Modification of Server initiated messages

- Server->Client Request (such as RAR)
- Server->Client Answer (such as CCA)

The message transformation process is shown in *Figure 28*.

Figure 28: A 4 Way Message Transformation

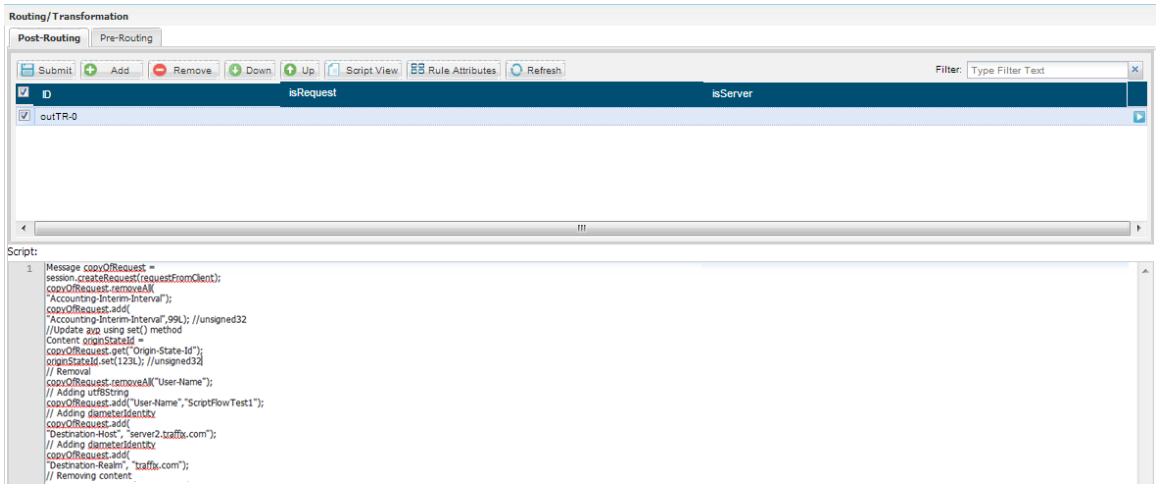


As seen in the above figure, SDC provides the flexibility by defining **Server Responses and Server Requests**.

SDC supports message transformation between Diameter, LDAP, RADIUS, and HTTP nodes, and between nodes of the same type.

A sample modification script is shown in *Figure 29*.

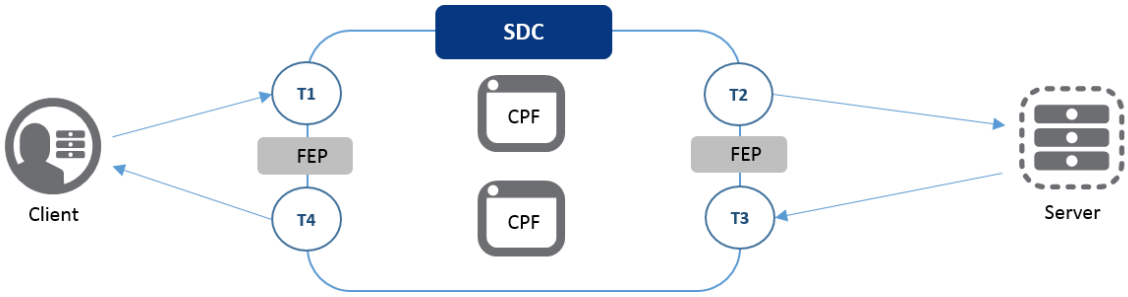
Figure 29: Sample Transformation Grid



6. Overload and Congestion Control

The basic traffic flow between the SDC and the network elements is illustrated in *Figure 30*. In this flow, message requests are sent from clients, received by the SDC, and then sent by the SDC to a server. Message answers are then sent from the server back to the SDC, and then sent by the SDC to the client.

Figure 30: Basic Traffic Flow between the SDC and Networks



This flow includes two types of traffic– incoming (from the client/server to the SDC) and outgoing (from the SDC to the client/server). The volume of traffic received by the SDC at an entry point (T1, T3) or sent by the SDC at an exit point (T2, T4) is monitored and can be limited. These limits ensure that the overall traffic flow performance is constantly under control, and that in the event of an overload, mechanisms can immediately be applied. These mechanisms control and limit the resource usage and allocation, by controlling the number of incoming/outgoing message requests and traffic rates per destination peer. Applying these mechanisms in cases of overload ensures that traffic processing continues with minimal disruption.

7. Application Security

F5 realizes that security is vital to assure availability, integrity and confidentiality of the operator's signaling network. SDC provides multi-level security features that are described in the following sections.

7.1 Diameter Topology Hiding

The SDC solution supports topology hiding by exposing one or more VIP (Virtual IP) in the direction of the peers. The VIP is used as a single point of attachment for all peers connected to the SDC node.

To prevent DOS attack, the solution limit external networks' access to port 3868 and other agreed ports. The solution uses IPTABLES to protect the network from intrusion attempts.

7.2 Diameter Connection Security

The SDC solution limits the number of incoming clients and network sources. The SDC solution provides Diameter level access control lists (ACLs) to ACCEPT or REJECT peers by their IP address, host name/subnet, application-id, product-type, etc. Additionally, the solution provides the user with the ability to implement a custom access policy. The user can inspect any combination of AVPs in a CER message and ACCEPT or REJECT the connection establishment based on custom policy criteria.

SDC ensures idle connection termination after a user configurable timeout period, for both Diameter and management traffic.

The solution uses IPSEC, TLS and DTLS to implement transport level security.

7.3 Diameter Message Security

SDC limits and enforces maximal Diameter message length and for Diameter message screening. The SDC solution allows:

- Removing certain AVP(s) than can unveil the internal structure of the network
- Rewriting AVP(s) using certain anonymization techniques to protect data and mitigate privacy and security concerns to comply with legal requirements of the network and to avoid exposing of information contained in the AVP(s) like Session-Id, Origin-Host, Origin-Realm, etc.
- Using encryption mechanism for encoding/decoding of payload of AVP(s)

8. OAM Support

The SDC's Operations, Administration, and Maintenance (OAM) capabilities are provided using the OAM module. An OAM module is included on each SDC site and a central OAM module is located on Element Management System (EMS) sites.

Key OAM capabilities provided by the SDC include:

- A management console for SDC site configuration and monitoring
- Maintaining the SDC site configuration
- Exposing the SNMP northbound interface to operations support systems for fault management
- Providing a user management mechanism that allows the definition of multiple users with various access levels
- Maintaining log files

EMS OAM module expands on the SDC OAM capabilities with the following:

- Central configuration and monitoring access for a deployment containing multiple SDC sites that are managed by the EMS
- Generated aggregated reports for analysis of signaling traffic and SDC health using a central Reporting Engine

Appendix A: Supported HW

SDC runs on standard off-the-shelf HW such as:

- HP Blade System with Bl460c Gen8 Blades
- HP DL380p Gen8 Rackmount Servers
- IBM BladeCenter with HS23 Blades

Note: IBM BladeCenter with HS22 Blades is only supported for legacy customers upgrading to Release 4.4.

For a scalable deployment, it is recommended to use a blade-based solution that provides chassis-based high capacity HW architecture with inherent manageability, reliability, and redundancy.

Appendix B: Access Level Security

System management is done using secure protocols. The access security supported in the system is summarized in the table below.

Table 7: Supported Access Security

Solution Element	Access Control Model	Access Method	Role/Permission	Permission Description
SDC Management	Permission-based model	Web Management Console, Web Services	Read-Only User	Read-Only Access
			Operator	Manage Diameter Peers and Pools, Enable/Disable links to Peers, Backup and Restore Configuration, etc.
			Super-User (Administrator)	Full Access
Operating System	Permission and Group-based model	SSH, SFTP	Read-Only User	Read-only access to logs, system files and information
			Operator	(Configurable) In addition to User permissions, may be enabled to perform selected administration tasks (e.g.: capture network traffic samples).
			Super-User (Administrator)	Full access

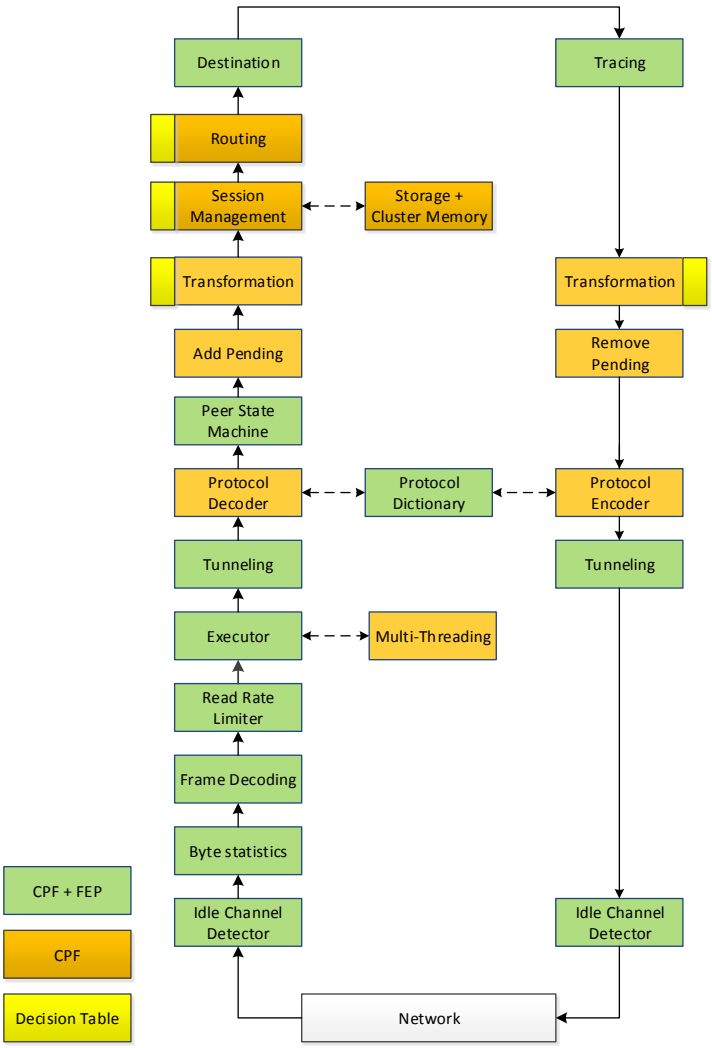
Solution Element	Access Control Model	Access Method	Role/Permission	Permission Description
Chassis Hardware Management	Role and Permission-based model	Web Management Console, SNMP, SSH	Read-Only User Super-User (Administrator) Custom Role set	Read-only access Full access (Configurable) Custom set, selected from a wide list of roles, with option to restrict access to specific sub-elements
Networking Hardware Management	Permission-based model	SSH	Read-Only User	Read-only access
			Operator	Read-Only access and permission to make temporary operational configuration changes to selected options, and reset ports.
			Super-User (Administrator)	Full access
SNMP Monitoring and Management	USM (User-based security model)	SNMP	USM user	Per-user configured Read/Write/Notify permissions to specified SNMP objects(OIDs)

In addition to that, SDC records of all user interactions in its auditing logs and all idle OAM sessions are terminated.

Appendix C: Low Level SDC Pipeline

The detailed message flow through the SDC pipeline is shown in *Figure 31*[1].

Figure 31: Detailed System Flow



[1] More details are available in Pipeline.xlsx and PeerFSM.xlsx

Appendix D: Load Balancing Policies

Table 8: Load Balancing Policies

Load Balancing Policy	Description
By Precedence	Messages are sent to the first peer in the pool, as long as it is open for traffic. When the first peer goes out of service, messages are sent to the next peer in the pool, and so on. When the first peer gets back to service and reopens, messages are again sent to that first peer.
Round Robin	Messages are evenly distributed across the pool's available peers, in the order that the peers appear in the pool settings.
Weighted Round Robin	Messages are distributed across the pool's available server peers according to a predefined proportion. The weight of each server peer is set during peer configuration, and should be based upon its ability to handle incoming requests. Weighted Round Robin is a static algorithm. No external parameters are taken under account upon request distribution. With Weighted Round Robin, new requests are distributed in a round robin pattern, but instead of sending the request to the next available server peer in line, requests are sent to the server peer that has not yet reached its quota.
Fastest Response Time	Messages are sent to the server peers according to the peer's response time. The response time is used as the weight of the server peer. Fastest Response Time is a dynamic algorithm since it takes external parameters (response time) into account upon request distribution.

Load Balancing Policy	Description
Queue Size Ratio	Messages are sent to the servers peers according to the pending requests size. If Server A's weight is higher than Server B's weight, the policy assumes Server A has a higher traffic handling capacity and maintains a longer queue of pending requests, compared to other servers in the Pool. That is, the higher the server's weight, the greater the number of pending requests it will handle. After getting the performance figures from the active peers (RTT or the number of pending requests), they are normalized between the value 1 and the maximal ratio (the default value is 100): The highest value is 1 while the lowest value is the max ratio value. Queue Size Ratio policy is a dynamic algorithm and responds to external fluctuations upon request distribution.
Load Based	Messages are distributed between servers based on the real-time performance and load experienced by the servers in the pool. Servers with the least load will be the first to receive requests.
Contextual	The Contextual load balancing policy maps the clients' session ID's to a list of available server peers. This way messages are sent to a specific server peer, according to their session ID.
Weighted Contextual	The Weighted Contextual load balancing policy maps the clients' session ID's to a list of available server peers. This way messages are sent to a specific server peer according to their

Load Balancing Policy	Description
	session ID. In addition to the session ID parameter, traffic distribution is also controlled by a predefined proportion. The weight of each server peer is set during the peer configuration and should be based upon its ability to handle incoming requests.
External	The peer is selected according to an external script's rule.

Glossary

The following table lists the terms and abbreviations used in this document.

Table 9: Terms and Abbreviations

Term	Definition
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AF	Application Function
Answer	A message sent from one Client/Server Peer to the other following a request message
API	Application Programming Interface
AVP	Attribute Value Pair
CLI	Command Line Interface
Client Peer	A physical or virtual addressable entity which consumes AAA services
CPF	Control Plane Function
Data Dictionary	Defines the format of a protocol's message and its validation parameters: structure, number of fields, data format, etc.
DEA	Diameter Edge Agent
Destination Peer	The Client/Server peer to which the message is sent
DRA	Diameter Routing Agent
EMS Site	Element Management System Site
FEP-In	In-Front End Proxy
FEP-Out	Out-Front End Proxy
Geo Redundancy	A mode of operation in which more than one geographical location is used in case one site fails

Term	Definition
HA	High Availability
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IMS	IP Multimedia Subsystem
JMS	Java Message Service
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
LTE	Long Term Evolution
Master Session	The session for which the routing selection is performed based on the routing rules (Slave Sessions are applied with routing rules inherited from the Master Session)
MME	Mobility Management Entity
NGN	Next Generation Networking
Node	Physical or virtual addressable entity
OAM	Operation, Administration and Maintenance
OCS	Online Charging System
Origin Peer	The peer from which the message is received
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
PLMN	Public Land Mobile Network
Pool	A group of Server Peers
RADIUS	Remote Authentication Dial In User Service
Request	A message sent from one Client/Server peer to the other, followed by an answer message

Term	Definition
SCCP	Signaling Connection Control Part
SCTP	Stream Control Transmission Protocol
SDC	Signaling Delivery Controller
SDC Site	The entire list of entities working in a single site
Server Peer	A physical or virtual addressable entity which provides AAA services
Session	An interactive information interchange between entities
Slave (Bound) Session	A session which inherits properties from a master session
SNMP	Simple Network Management Protocol
SS7	Signaling System No. 7
TCP	Transmission Control Protocol
TLS	Transport Layer Security
Transaction	A request message followed by an answer message
Tripo	Session data repository
UDP	User Datagram Protocol
UE	User Equipment
URI	Universal Resource Identification.
Virtual Server	A binding point used by SDC to communicate with the Remote Peers (Clients and Servers)
VPLMN	Visited Public Land Mobile Network
Web UI	Web User Interface
WS	Web Service

