



Signaling Delivery Controller

SS7 Diameter Interworking Function

4.4

Catalog Number: FD-015-44-35 Ver. 2

Publication Date: May 2015



Legal Information

Copyright

© 2005-2015 F5 Networks, Inc. All rights reserved.

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 SS7 Diameter Interworking Function

Catalog Number: FD-015-44-35 Ver. 2

Publication Date: May 2015

Document Objectives

This document provides an overview of interworking capability scenarios between SS7 protocols – MAP and CAMEL – and Diameter protocols.

Document History

Revision Number	Change Description	Change Location
May 2015 – Ver. 2	Trademark text changed	

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
<i>Normal Text Italic</i>	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
 Warning:	Warnings which indicate potentially damaging user operations and explain how to avoid them



Table of Contents

1. Introduction	1
2. About SS7 and Diameter	2
2.1 Diameter	2
2.2 SS7	2
2.3 SS7 Layers	3
2.3.1 SCTP (Stream Control Transmission Protocol)	3
2.3.2 M3UA, SCCP, and TCAP	4
2.3.2.1 M3UA (MTP3 User Adaptation)	4
2.3.2.2 SCCP (Signaling Connection Control Part)	4
2.3.2.3 TCAP (Transaction Capabilities Application Part)	5
2.3.3 MAP (Mobile Application Part)	5
2.3.4 CAMEL (Customized Application of Mobile Enhanced Logic)	5
3. F5 Solution Deployment	6
3.1 Architecture	6
4. Diameter TCAP Interworking	7
4.1 Terminology	7
4.2 Message Transformation Process	7
4.2.1 Diameter to MAP/SS7 message flow	8
4.2.2 MAP/SS7 to Diameter message flow	9
4.2.3 Routing in SS7	10
4.2.3.1 Configuring the Global Title	10
4.2.4 Dynamic destination Global Title set	11
4.2.4.1 Static configuration of peer	11
4.2.5 Transforming Global Titles, Realms, and Hosts in SCCP	11
4.2.5.1 Messages originating in Diameter-based MMEs to MAP-based HLRs (AIRs, ULRs, NORs, etc.)	11
4.2.5.2 Messages originating in SS7-based HLRs to Diameter-based MMEs (Cancel Location, Delete Subscriber, etc.)	12
4.2.5.3 Messages originating in Diameter-based HSSs to MAP-based SGSNs (CLRs, DLRs, IDRs, etc.)	12
4.2.5.4 Messages originating in SS7-based SGSNs to Diameter-based HSSs (Authenticate Information, Update GPRS Location, etc.)	13
4.3 ASN.1 Support	13
5. Diameter-MAP Interworking Scenarios	14
5.1 S6a/S6d - Rel8 Gr interworking scenario	14
5.1 S6a/S6d - S6a/S6d interworking scenario with two IWFs	14
5.1 S13/S13' - Gf interworking scenario with one IWF	15
6. Working with the SS7 Diameter Interworking Function	16
6.1 Statistics	16
6.2 Performance and Overload Capabilities	16
Appendix A: Diameter CAMEL Interworking	18
A.1 Use Case: Diameter to Gy+ conversion	18
Appendix B: Diameter MAP Interworking (IWF)	20
B.2 Authentication Information Retrieval	20
B.2.1 One IWF Scenario	20



B.2.2 Two IWFs Scenario.....	21
B.3 Update Location.....	22
B.3.1 One IWF Scenario	22
B.3.1.1 Insert Subscriber Data	23
B.3.2 Two IWFs Scenario.....	24
B.4 Cancel Location.....	25
B.4.1 One IWF Scenario	25
B.4.2 Two IWFs Scenario.....	26
B.5 Purge.....	27
B.5.1 One IWF Scenario	27
B.5.2 Two IWFs Scenario.....	28
B.6 Insert Subscriber Data	29
B.6.1 One IWF Scenario	29
B.6.2 Two IWFs Scenario.....	30
B.7 Delete Subscriber Data	31
B.7.1 One IWF Scenario	31
B.7.2 Two IWFs Scenario.....	32
B.8 Reset	33
B.8.1 One IWF Scenario	33
B.8.2 Two IWFs Scenario.....	34
B.9 Notification	35
B.9.1 One IWF Scenario	35
B.9.2 Two IWFs Scenario.....	36
B.10 IMEI Check	37
B.10.1 One IWF Scenario	37
B.11 Trace Activation	38
B.11.1 One IWF Scenario	38
B.11.2 Two IWFs Scenario.....	39
B.12 Trace Deactivation	40
B.12.1 One IWF Scenario	40
B.12.2 Two IWFs Scenario.....	41

List of Figures

Figure 1: OSI and SIGTRAN model layers.....	3
Figure 2: F5 Solution Architecture	6
Figure 3: Diameter to MAP/SS7 message flow.....	8
Figure 4: MAP/SS7 to Diameter message flow	9
Figure 5: S6a/S6d - Rel8 Gr interworking scenario.....	14
Figure 6: S6a/S6d - S6a/S6d interworking scenario with two IWFs	15
Figure 7: S13/S13' - Gf interworking scenario with one IWF.....	15



Figure 8: Use Case: Diameter to Gy+ conversion	18
Figure 9: Use Case: Authentication Information Retrieval – One IWF Scenario	20
Figure 10: Use Case: Authentication Information Retrieval – Two IWFs Scenario	21
Figure 11: Update Location – One IWF Scenario	22
Figure 12: Update Location – Two IWFs Scenario	24
Figure 13: Cancel Location – One IWF Scenario	25
Figure 14: Cancel Location – Two IWFs Scenario	26
Figure 15: Purge – One IWF Scenario	27
Figure 16: Purge – Two IWFs Scenario.....	28
Figure 17: Insert Subscriber Data – One IWF Scenario.....	29
Figure 18: Insert Subscriber Data – Two IWFs Scenario	30
Figure 19: Delete Subscriber Data – One IWF Scenario.....	31
Figure 20: Delete Subscriber Data – Two IWFs Scenario.....	32
Figure 21: Reset – One IWF Scenario.....	33
Figure 22: Reset – Two IWFs Scenario	34
Figure 23: Notification – One IWF Scenario.....	35
Figure 24: Notification – Two IWFs Scenario.....	36
Figure 25: IMEI Check – One IWF Scenario.....	37
Figure 26: Trace Activation – One IWF Scenario	38
Figure 27: Trace Activation – Two IWFs Scenario.....	39
Figure 28: Trace Deactivation – One IWF Scenario	40
Figure 29: Trace Deactivation – Two IWFs Scenario.....	41

List of Tables

Table 1: Conventions	II
Table 2: Interworking Terminology.....	7
Table 3: MAP Support per Version by Command	7
Table 4: Terms and Abbreviations	42



1. Introduction

As you migrate to 4G LTE, it can be too costly or complex to completely replace your existing infrastructure. To make the old infrastructure interoperable with the new, you can capitalize on the interworking function capabilities of the F5[®] Traffix[®] Signaling Delivery Controller[™] (SDC), that enable any-to-any connectivity between Diameter-based and legacy nodes, such as SS7 elements within a mobile network, roaming scenarios that involve legacy network elements, and SS7 elements within Intelligent Networks. In accordance with the IWF scenarios between MAP and Diameter described in the 3GPP TS 29.305 specification (covering mobility and IMEI Check), multiple IWF scenarios are supported, as well as two deployment modes – single IWF deployments and dual IWF deployments. In addition, the F5 solution also includes support for Intelligent Network nodes by offering CAMEL-Diameter interworking.

With support for more than 50 Diameter interfaces, the F5 solution therefore enables you to preserve your existing infrastructure investments and ease your migration to 4G LTE.



2. About SS7 and Diameter

This chapter provides a brief overview of both Signaling System No. 7 (SS7) and Diameter protocols.

2.1 Diameter

The Diameter protocol evolved from the Remote Authentication Dial In User Service (RADIUS) protocol, which was widely used in 3GPP Release 5 onwards, consuming Authentication, Authorization, and Accounting (AAA) services.

As new network technologies were widely adopted, a more comprehensive and extensible access control mechanism was required to process user authentication. Modeling after RADIUS's capabilities and incorporating flexible extension capabilities for future AAA applications, Diameter – an evolution of RADIUS – was designed.

Several additions were required to make Diameter more reliable, including the new Attribute Value Pair (AVPs) and error notification mechanisms. Contrary to its appearance as a client-to-server protocol, the Diameter protocol was designed as a peer-to-peer protocol. It uses the IP network as its mediator and runs on top of TCP or SCTP.

2.2 SS7

The Signaling System No.7 (SS7) protocol was developed to meet call management and service signaling requirements of the digital networks based on full duplex channels.

In SS7 networks, the nodes are called Signaling Points, while the connection between the nodes is called a Signaling Link. Messages are transferred between SPs using Signaling Transfer Points (STPs).

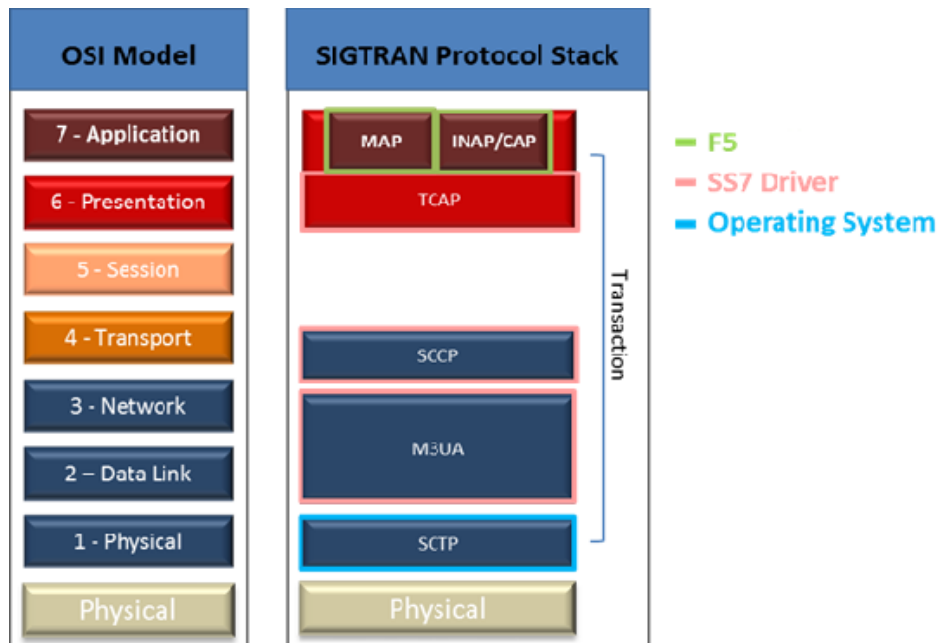
The SIGTRAN protocols are an extension of the SS7 protocol family. It supports the same application and call management paradigms as SS7 but uses an Internet Protocol (IP) transport called Stream Control Transmission Protocol (SCTP).



2.3 SS7 Layers

The SS7 structure was initially developed to be compatible with the Open Systems Interconnection (OSI) model. Figure 1 illustrates the similarities and differences between the two network models and the information following details each protocol layer and how it is accessed and used by the F5 solution.

Figure 1: OSI and SIGTRAN model layers



2.3.1 SCTP (Stream Control Transmission Protocol)

The SCTP transport protocol is used by both Diameter and SS7. The F5 solution is fully compliant with the SCTP layer interworking specified in RFC 4960, providing support for all Diameter Transport Mechanisms – UDP, TCP, and SCTP, and supporting the simultaneous use of SCTP and TCP transport protocols, allowing interconnecting between two peers, each using a different transport protocol. The solution supports commonly used Diameter interfaces - for example S6a, S6d, and S13 – that run on SCTP, as well as SS7 interfaces, such as MAP and CAMEL.



2.3.2 M3UA, SCCP, and TCAP

These layers, responsible - respectively - for establishing the physical connection, defining the Global Title, and establishing the context for the transaction, are implemented by 3rd party software which is used by the F5 solution as a driver towards the SS7 domain.

2.3.2.1 M3UA (MTP3 User Adaptation)

The M3UA layer offers a standard-based interface between MTP3 user parts (ISUP and SCCP running on an application host) and a signaling gateway offering MTP services. The SS7 driver provides a software implementation of the SS7 MTP3 User Adaptation Layer (M3UA) protocol, as defined by the Internet Society in RFC 4666, (which supersedes the previous RFC 3332). The F5 solution currently supports implementations where the M3UA is set in Application Server Process (ASP) mode, which works on the assumption that the IWF connects to Signaling Transport Points (STPs) in the SS7 network. An alternative implementation would be in the M3UA IP Server Process (IPSP) mode that works using direct node connections, not through STPs.

2.3.2.2 SCCP (Signaling Connection Control Part)

The SCCP layer operates parallel to OSI Level 4. SCCP completes the functions of MTP3: end-to-end addressing and routing, connectionless messages (UDTs), and management services for users of the Network Service Part (NSP). The combination of SCCP and MTP3 is called the Network Service Part (NSP). The SCCP layer complies with specifications ITU-T Q.711 through Q.714.

SCCP supports the following network addressing:

- Point Code (PC) routing
- Subsystem Number (SSN) routing
- Global Title (GT) routing



2.3.2.3 TCAP (Transaction Capabilities Application Part)

The TCAP layer is used for transporting transaction-oriented data across the SS7 network. It implements standard Remote Operation Service Element (ROSE) services for applications such as GSM-MAP and IS-41.

TCAP messages are destined for application entities and are transferred end-to-end using the services of SCCP. The TCAP protocol is designed to transfer non-circuit related messages and provide a means for SCP-to-SCP communication via STPs. TCAP is also used to invoke other features from remote switches: its services include free phone, calling card, and wireless roaming. SSP uses TCAP messages to query an SCP (via an STP) and locate their routing numbers in the global title. The response is sent to the SSP via TCAP and STP containing the routing numbers.

For more information about TCAP, see the *TCAP Specifications Q771-Q775*.

2.3.3 MAP (Mobile Application Part)

The MAP protocol is an SS7 TCAP protocol that is used to access the various nodes in mobile networks – including the Mobile Switching Center (MSC)/Mobile Soft Switch (MSS), Home Location Register (HLR), Equipment Identity Register (EIR), Short Message Service Center (SMSC), and Serving GPRS Support Node (SGSN) – to provide mobility and OAM services.

2.3.4 CAMEL (Customized Application of Mobile Enhanced Logic)

The CAMEL protocol runs on top of the SS7 TCAP layer. CAMEL is used to provide extended mobile capabilities, inside mobile networks and especially when roaming between networks, including prepaid charging, unified messaging, fraud control, and Intelligent Network (IN) services like short code translation and other numbering services – for example, VPN.



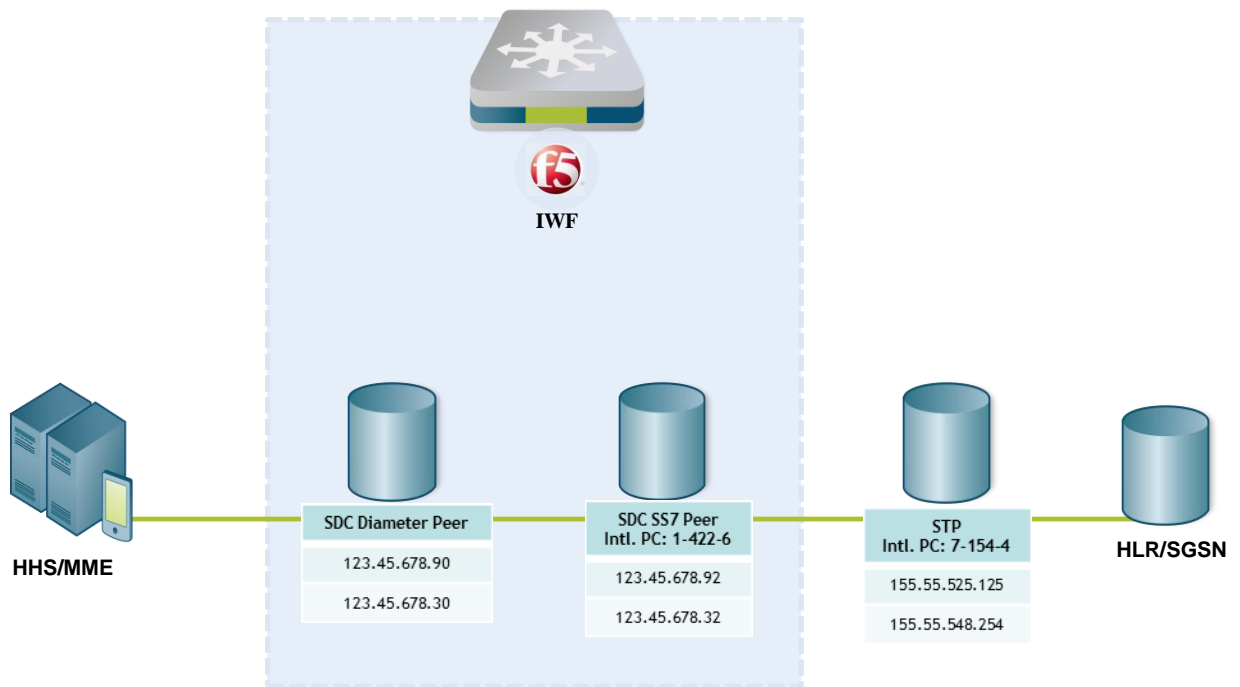
3. F5 Solution Deployment

This chapter describes the suggested deployment architecture to maximize the value gained from the F5 solution.

3.1 Architecture

The figure below illustrates how the F5 solution is implemented between networks, and maps out both the network and solution elements needed to ensure a smooth implementation. For more information about how messages are processed and transformation, see 4.

Figure 2: F5 Solution Architecture





4. Diameter TCAP Interworking

This chapter provides an in depth look at the Diameter SS7 transformation processes.

4.1 Terminology

While interworking between Diameter and SS7, standard Diameter attributes are redefined as their SS7 counterparts (and vice versa), as follows:

Table 2: Interworking Terminology

Diameter term	Context	SS7 term
IP	In an SS7 network	Point Code (PC)
Port	In an SS7 network	Subscriber System Number (SSN)
The <i>Origin-Host</i> AVP	Running on SCCP	<i>Calling Party</i> GT
The <i>Destination-Host</i> AVP	Running on SCCP	<i>Called Party</i> GT
The <i>User-Name</i> AVP	Running on MAP	IMSI
The <i>Session-ID</i> AVP	Running on TCAP	<i>TCAPDialogID</i>
The <i>Hop-ID</i> AVP	Running on TCAP	<i>InvokeID</i>

4.2 Message Transformation Process

Support for SS7 is implemented within the IWF through two message processing pipelines:

- The Diameter to MAP/SS7 pipeline
- The MAP/SS7 to Diameter pipeline

The F5 IWF supports processing of specific commands by MAP version, as described in the following table:

Table 3: MAP Support per Version by Command

Command	MAPv1	MAPv2	MAPv3	Version negotiation supported
gprsUL	No	No	Yes	No

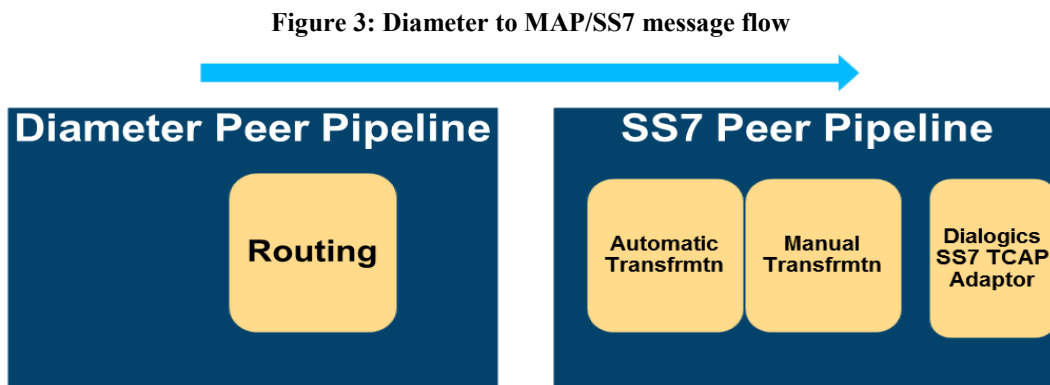


Command	MAPv1	MAPv2	MAPv3	Version negotiation supported
CLR	No	Yes	Yes	No
RSR	No	No	Yes	No
AIR	No	Yes	Yes	Yes
All other	No	No	Yes	No

4.2.1 Diameter to MAP/SS7 message flow

This flow involves two SDC peers – the Diameter peer and the SS7 peer – and is responsible for routing messages originating in Diameter network nodes to SS7 network nodes.

The following figure shows *the Diameter to MAP/SS7 message flow*:



The Diameter to MAP/SS7 message flow includes the following stages:

1. Routing - The Diameter peer receives a message from the Diameter client and routes it to an outgoing SS7 peer. In general, the routing is performed per the message's destination realm AVP. For more information about the routing process, see *Routing in SS7*.
2. Automatic transformation - The message is received in the SS7 peer. The F5 solution then applies a unique mechanism that generates a TCAP message containing a MAP



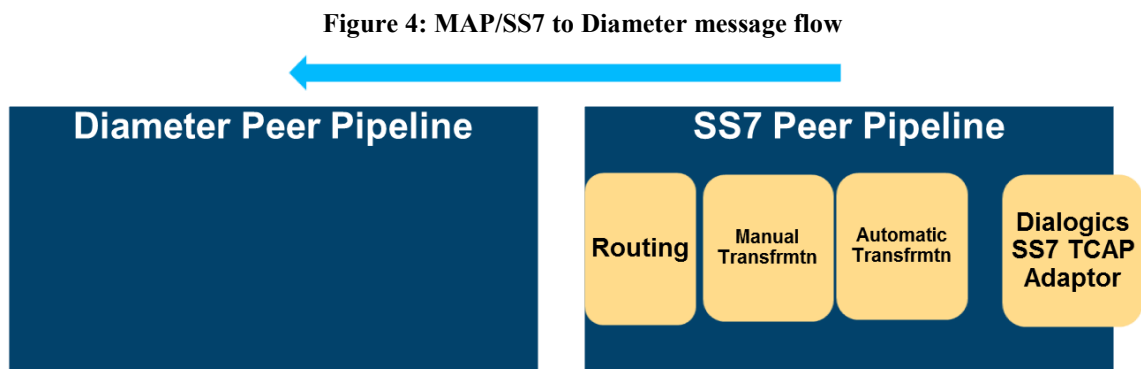
component, based on the incoming Diameter request, as described in *Table 2*. The TCAP Diameter-based attributes are processed into the corresponding MAP message format, as described in the 3GPP TS 29.305 specification. For more information about the F5 mechanism, see *Transforming Global Titles, Realms, and Hosts in SCCP*.

3. Manual transformation - A user script can be activated after the automatic transformation to manually manipulate the generated TCAP message as needed. Both the TCAP and MAP attributes can be manually manipulated.
4. SS7 TCAP Adaptor - Once the transformation is complete, the message is sent to the SS7 TCAP Adaptor driver. The SS7 driver forwards the message to the customer's STP, which then routes the message to the destination based on the Global Title.

4.2.2 MAP/SS7 to Diameter message flow

This flow involves two SDC peers – the SS7 peer and the Diameter peer – and is responsible for routing messages originating in SS7 network nodes to Diameter network nodes.

The following figure shows the MAP/SS7 to Diameter message flow.



The MAP/SS7 to Diameter message flow includes the following stages:

1. SS7 TCAP Adaptor – Messages received from an SS7 network node are routed to an SS7 peer by either the SS7 TCAP Adaptor (based on the message's original Global Title), or according to a default routing decision.



2. Automatic transformation – The message is received in the SS7 peer. The F5 solution then applies a unique mechanism that generates a Diameter message, based on the incoming MAP message, as described in see *Table 2*. The TCAP MAP-based attributes are processed into the corresponding Diameter message format, as described in the 3GPP TS 29.305 specification. For more information about the F5 mechanism, see *Transforming Global Titles, Realms, and Hosts in SCCP*.
3. Manual transformation – A user script can be activated after the automatic transformation to manually manipulate the message as needed.
4. Routing – The SS7 peer then routes the message to a Diameter pool based on user defined scripts. For more information about the routing process, see *Routing in SS7*.

4.2.3 Routing in SS7

4.2.3.1 Configuring the Global Title

The IWF will be connected to the operator’s STP/AS, and not directly to the international SS7 network. The SS7 routing towards and from roaming partners nodes will be done using a Global Title and not a Point Code. The IWF’s Point Code will be used for intra network routing only.

The IWF needs to get a national point code routable in the network, a Global Title for international routing and a pool of GTs for the IWF function, as described later in *Transforming Global Titles, Realms, and Hosts in SCCP*. The GT and GT pool should be registered in the GSMA IR.21.

SS7 routing can be based on an SCCP-based Global Title, which is inserted to the outgoing message by the IWF during the transformation process from Diameter to SS7. In ASP mode, this is the default routing flow. The called global title address can be set dynamically per message, based on the user-name AVP, or statically by configuration of the SS7 peer. The calling global title address can be set dynamically based on the origin-host AVP, or statically by configuration of the SS7 peer. Any automatically produced global title value can be overridden by user script.



4.2.4 Dynamic destination Global Title set

The Global Title can (and sometimes should) be set via a user-defined outgoing transformation script.

4.2.4.1 Static configuration of peer

The SS7 peer can be configured to statically set a configurable pre-defined Global Title address on destination, for every message it sends towards SS7. In this case, an SS7 peer must be configured for every static GT that needs to be sent.



Note: Global Titles set this way can still be overridden by a user script.

4.2.5 Transforming Global Titles, Realms, and Hosts in SCCP

The F5 mechanism provides transformation solutions between Diameter-based AVPs and the Calling and Called Party GTs for the following four scenarios:

- Messages originating in Diameter-based MMEs to MAP-based HLRs (AIRs, ULRs, NORs, etc.)
- Messages originating in SS7-based HLRs to Diameter-based MMEs (Cancel Location, Delete Subscriber, etc.)
- Messages originating in Diameter-based HSSs to MAP-based SGSNs (CLRs, DLRs, IDRs, etc.)
- Messages originating in SS7-based SGSNs to Diameter-based HSSs (Authenticate Information, Update GPRS Location, etc.)

4.2.5.1 Messages originating in Diameter-based MMEs to MAP-based HLRs (AIRs, ULRs, NORs, etc.)

In this scenario, the following attributes are transformed:

- The origin-host AVP is transformed into the Calling Party GT in E164I format.
- The user-name AVP is transformed into the Called Party GT in E214I format.



The transformation is performed based on a dynamic but persistent transformation table located in the IWF, in which each MME is assigned a Global Title. Using this table, the IWF translates the MME's origin-host AVP into a Calling Party GT.

The user can define a specific Global Title for an MME. If a Global Title is not defined for an MME, the IWF automatically defines one from the GT pool reserved for the IWF. The transformation table is then updated with the new definition for future use.

The persistent value definitions enable the following:

- The defined Global Title for an MME stays consistent, even after an IWF restart.
- Consistent Global Titles per MMEs clarify debugging processes and control of message flow. In this scenario, the following attributes are transformed:
- The IWF is initiated with default values that can then be manually altered.

4.2.5.2 Messages originating in SS7-based HLRs to Diameter-based MMEs (Cancel Location, Delete Subscriber, etc.)

In this scenario, the following attributes are transformed:

- The Calling Party GT in E164I format is put on the origin-host AVP. This transformation by default takes the calling GT number, and adds to it a configurable suffix to make it look like IP address.
- The Called Party GT in either E214I or E164I format is transformed into the destination-host AVP.
- This transformation is based on configuration transformation tables.

4.2.5.3 Messages originating in Diameter-based HSSs to MAP-based SGSNs (CLRs, DLRs, IDRs, etc.)

In this scenario, the following attributes are transformed:

- The origin-host AVP is transformed into the Calling Party GT in E164I format.



- In this transformation, the SDC acts as the HLR and its Calling Party GT is used.
- The destination-host AVP is transformed into the Called Party GT in E164I format.
- In this transformation, the Called Party GT is defined based on the transformation table created in Messages originating in SS7-based SGSNs to Diameter-based HSSs (Authenticate Information, Update GPRS Location, etc.).

4.2.5.4 Messages originating in SS7-based SGSNs to Diameter-based HSSs (Authenticate Information, Update GPRS Location, etc.)

In this scenario, the following attributes are transformed:

- The Calling Party GT in E164I format is transformed into the origin-host AVP.
- In this transformation, the origin-host AVP is defined using a transformation table, when the Calling Party Address in E164I format (CCNDCxxxxxx) is translated into the origin-host <CCNDCxxxxxx>.mme.<sdc realm>.
- The Called Party GT is transformed into the destination-host AVP.
- The transformation is performed based on a static but configurable transformation table located in the F5 IWF, in which each Called Party GT is assigned an HSS.

4.3 ASN.1 Support

The F5 solution supports routing and transformation of ASN.1 encoded TCAP messages and parameters to other supported protocols. The support is provided for the ASN.1 Basic Encoding Rules (BER) format, and is configured per customer, based on the specific encoded BER messages they process.



5. Diameter-MAP Interworking Scenarios

This chapter describes the interworking scenarios supported by the F5 solution, as they are described in the 3GPP TS 29.305 specification.

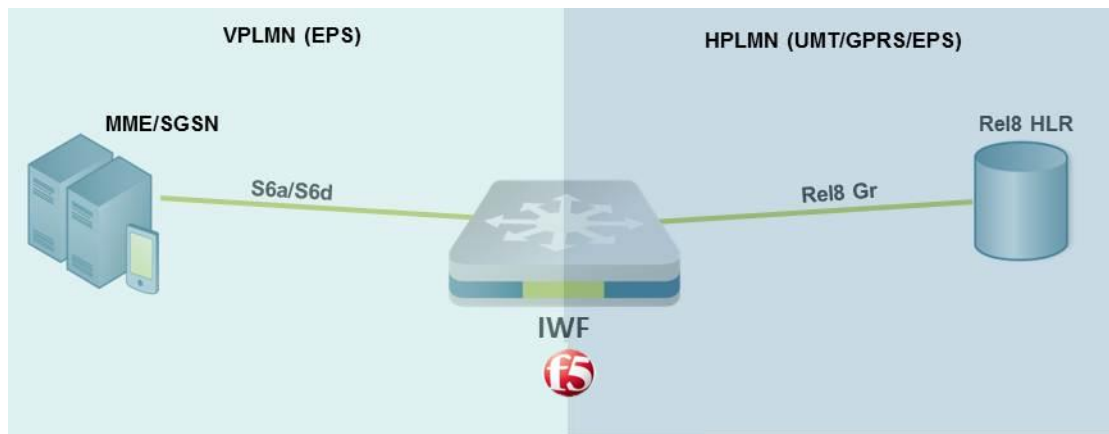
5.1 S6a/S6d - Rel8 Gr interworking scenario

In this interworking scenario, the SDC acts as an IWF directly connecting between a Diameter based HSS and a MAP based SGSN.

This scenario includes:

- Inter PLMN use cases
- Intra PLMN use case, enabling operators to perform a partial update of their legacy network.

Figure 5: S6a/S6d - Rel8 Gr interworking scenario



5.1 S6a/S6d - S6a/S6d interworking scenario with two IWFs

In this interworking scenario, the 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.

This scenario is only applicable for inter PLMN use cases.



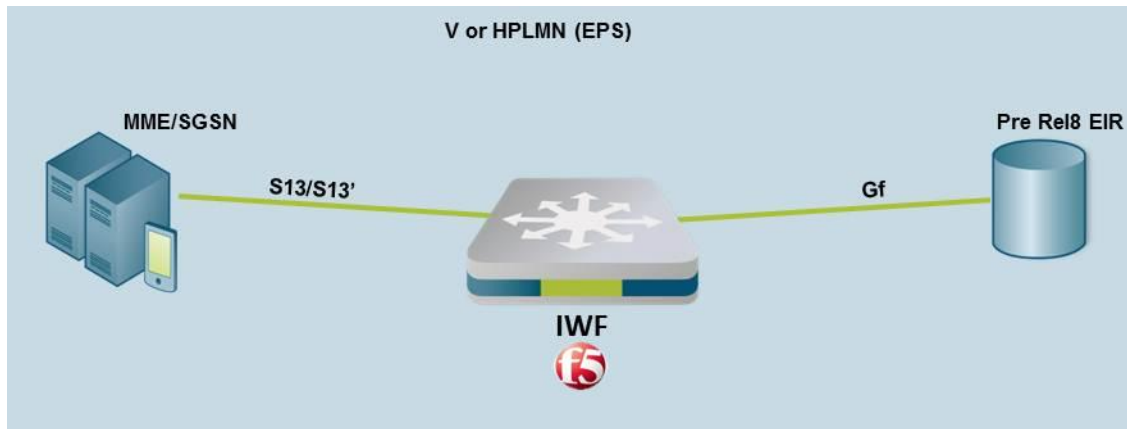
Figure 6: S6a/S6d - S6a/S6d interworking scenario with two IWFs



5.1 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. This scenario is only applicable for intra PLMN use cases, enabling operators to perform a partial update of their legacy network.

Figure 7: S13/S13' - Gf interworking scenario with one IWF





6. Working with the SS7 Diameter Interworking Function

6.1 Statistics

The interworking function generates the following Key Performance Indicators (KPIs):

- Channel Read Limit Message Discards
- Sent Messages
- Received Messages of UpdateGprsLocationRes
- Received Messages of CancelLocationArg
- Received Messages of SendAuthenticationInfoArg
- Received Messages Before Read Discarded
- Sent Message Of CancelLocationRes
- Sent Messages of SendAuthenticationInfoRes
- Sent Messages of UpdateGprsLocationArg
- Pending Requests UpdateGprsLocationArg
- Roundtrip Time UpdateGprsLocationArg
- Peer Average Roundtrip Time
- Received Bytes
- Peer OK Events CLA
- Peer OK Events AIA

6.2 Performance and Overload Capabilities

Processing messages with an average size of 0.5KB, each SS7 link can hold approximately 10 SS7 TPS per link. The basic SS7 license is for the equivalent of 4 SS7 links, providing overall capacity per license for 40 SS7 TPS.



The SS7 driver limits the number of links per implementation at 256 links.



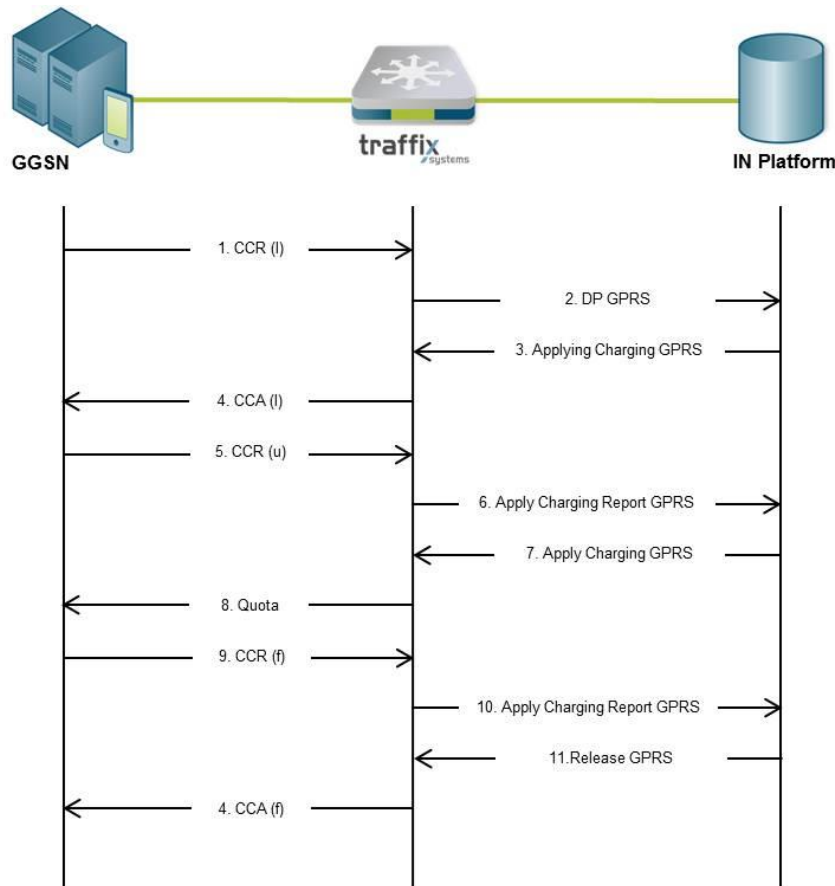
Appendix A: Diameter CAMEL Interworking

This chapter maps out and details a Diameter CAMEL interworking scenario.

Interworking between Diameter-based and CAMEL-based nodes provides a means for mobile networks to communicate with Intelligent Network (IN) platforms, responsible for authorizing static services, such as prepaid calling, unified messaging, and more. All Diameter-CAMEL transformations are user defined by the user through configurable scripts.

A.1 Use Case: Diameter to Gy+ conversion

Figure 8: Use Case: Diameter to Gy+ conversion





The figure above maps out the following Diameter to Gy+ conversion procedure:

1. The GGSN will send a CCR(I) to the Converter to initiate the Credit Control Session.
2. The Converter will send an Initial DP GPRS operation to IN platform.
3. IN platform will respond with an Apply Charging GPRS operation followed by a Continue GPRS operation.
4. CCA(I) is returned from the Converter.
5. The GGSN send a CCR(u) and is translated to a Apply Charging Report GPRS operation which is sent to IN platform.
6. IN platform is responding with an Apply Charging GPRS operation.
7. Quota is returned together with validity timer.
8. GGSN reports the last usage for each rating group to the Converter CCR(f).
9. The CCR(t) is translated to a Apply Charging Report GPRS operation which is sent to IN platform.
10. IN platform is responding with a Release GPRS operation.
11. The Converter returns a response for each reported rating group.

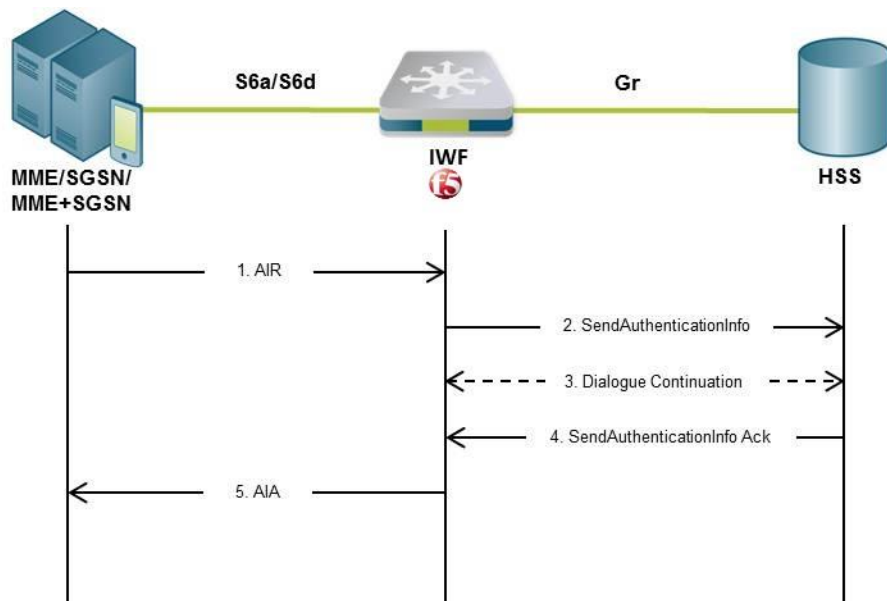
Appendix B: Diameter MAP Interworking (IWF)

This chapter maps out and details the procedures described in the 3GPP TS 29.305 specification that are supported by the F5 solution.

B.2 Authentication Information Retrieval

B.2.1 One IWF Scenario

Figure 9: Use Case: Authentication Information Retrieval – One IWF Scenario



The figure above maps out the following Authentication Info Retrieval procedure in a single IWF deployment:

1. An AIR message is sent from the MME, SGSN, or combined MME/SGSN to the F5 IWF.
2. The F5 IWF creates a MAP (version 3) dialogue towards the HLR by sending a SendAuthenticationInfo request.
3. The HLR may then initiate a MAP version fallback and/or send partial results. The F5 IWF performs the version fallback and/or stores the partial results.

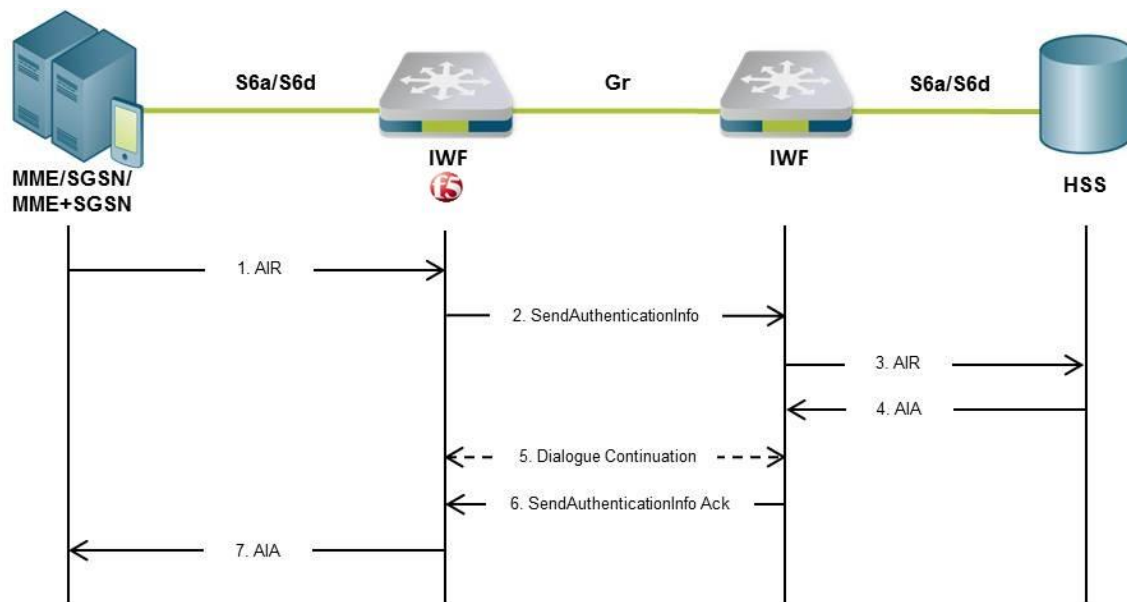


Note: If EPS-Vectors are requested for immediate use, version fallback is not applicable.

- The HLR closes the MAP dialogue by sending the (final) SendAuthenticationInfo Ack to the F5 IWF.
- The F5 IWF uses the information received from the HSS to construct an AIA which is sent to the MME, SGSN, or combined MME/SGSN.

B.2.2 Two IWFs Scenario

Figure 10: Use Case: Authentication Information Retrieval – Two IWFs Scenario



The figure above maps out the following Authentication Info Retrieval procedure in a dual IWF deployment:

- An AIR message is sent from the MME, SGSN, or combined MME/SGSN to the F5 IWF.
- The F5 IWF creates a MAP (version 3) dialogue towards the additional IWF by sending a SendAuthenticationInfo request.
- The IWF constructs an AIR message and sends it to the HSS.

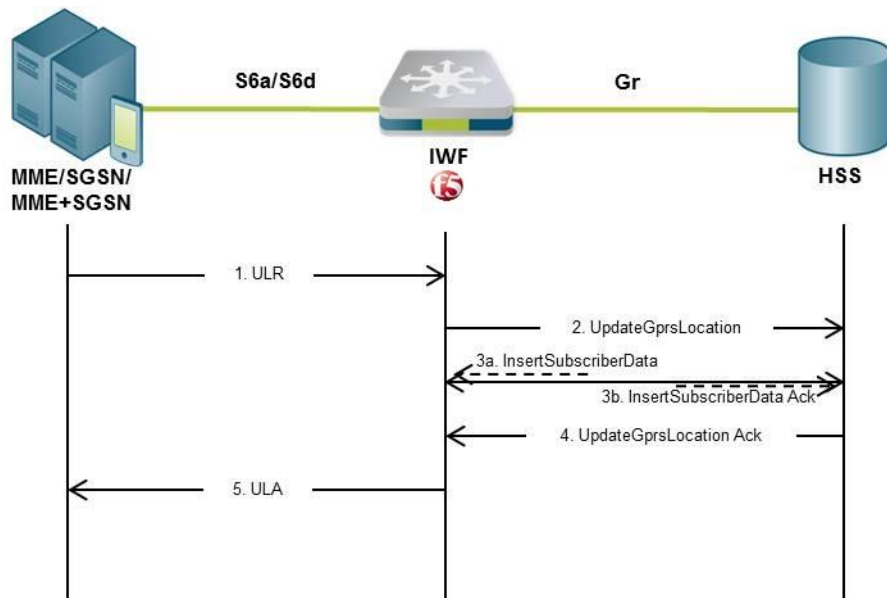


4. The IWF receives an AIA message from the HSS.
5. If segmentation is required, the IWF sends partial results to the F5 IWF which stores the partial results.
6. The IWF closes the MAP dialogue by sending the (final) SendAuthenticationInfo Ack message to the F5 IWF.
7. The F5 IWF uses the information received from the IWF to construct an AIA message which is sent to the MME, SGSN, or combined MME/SGSN.

B.3 Update Location

B.3.1 One IWF Scenario

Figure 11: Update Location – One IWF Scenario



The figure above maps out the Update Location procedure in a single IWF deployment:

1. A ULR message is sent from the MME, SGSN, or combined MME/SGSN to the F5 IWF.



2. The F5 IWF creates a MAP (version 3) dialogue towards the HLR by sending an UpdateGprsLocation request.
3. Depending on the "skip subscriber data" option selected in the ULR message, the HLR may continue the MAP dialogue by sending one or more InsertSubscriberData messages (in acknowledgement or burst mode) to the F5 IWF (3a). The F5 IWF will then temporarily store the received data and send InsertSubscriberData Ack messages back to the HLR (3b).

There are cases in which even when the "skip subscriber data" option is enabled, the HLR may still send InsertSubscriberData messages. In this case the InsertSubscriberData messages received from the HLR shall be acknowledged - but not stored - in the F5 IWF.

When sending InsertSubscriberData Ack messages to the HLR, the F5 IWF will mirror back any services requested by the HLR (within the InsertSubscriberData message) but not supported by the MME, SGSN, or combined MME/SGSN that sent the ULR. The F5 IWF will reject a MAP ActivateTraceMode message received from the HLR by returning an ActivateTraceMode Error (facilityNotSupported).

If the F5 IWF receives a MAP ActivateTraceMode message from the HLR, the F5 IWF needs to store the received trace data. The MME/SGSN returns either a positive or negative result to the HLR depending on whether tracing was enabled in the ULR.

4. The HLR closes the MAP dialogue by sending the UpdateGprsLocation Ack to the F5 IWF.
5. The F5 IWF uses the information received from the HLR to construct an ULA which is sent to the MME, SGSN, or combined MME/SGSN.

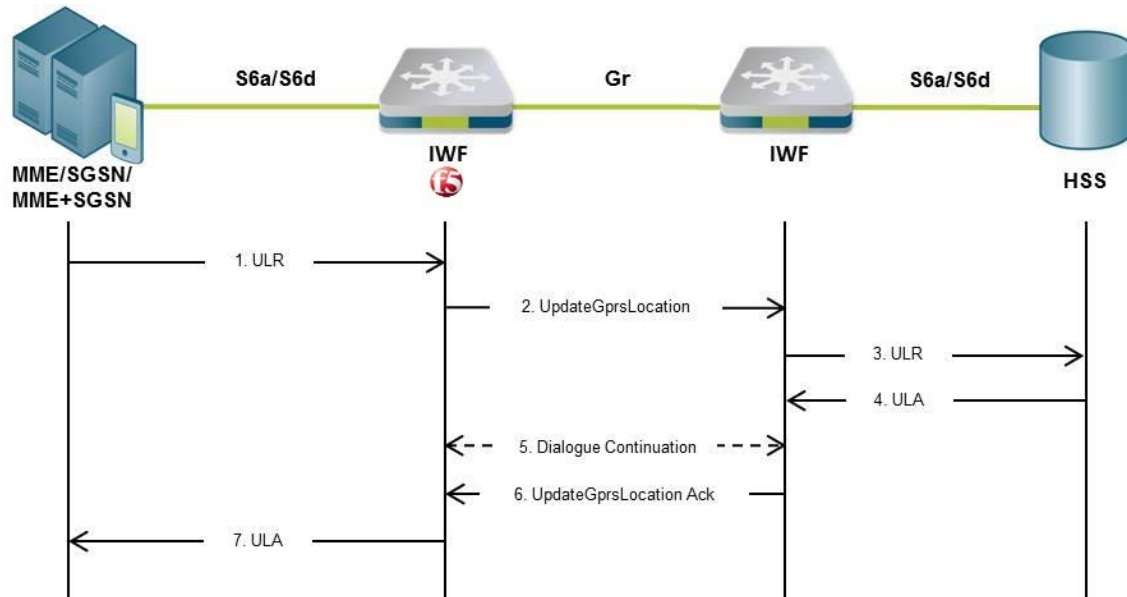
B.3.1.1 Insert Subscriber Data

The Insert Subscriber Data procedure is a sub-procedure within the Update Location procedure, where the HLR sends InsertSubscriberData requests to the IWF, which then

returns an InsertSubscriberData Ack message to the HLR. This continues until all information has been sent from the HLR and received by the IWF.

B.3.2 Two IWFs Scenario

Figure 12: Update Location – Two IWFs Scenario



The figure above maps out the following Update Location procedure in a dual IWF deployment:

1. A ULR message is sent from the MME, SGSN, or combined MME/SGSN to the F5 IWF.
2. The F5 IWF creates a MAP (version 3) dialogue towards the additional IWF by sending an UpdateGprsLocation request.
3. The IWF creates a ULR message and sends it to the HSS.
4. The IWF receives a ULA message back from the HSS.
5. If subscriber data is included in the ULA received by the IWF, it will send one or more InsertSubscriberData messages (in acknowledgement or burst mode) to the F5 IWF. The F5 IWF then temporarily stores the received data and sends

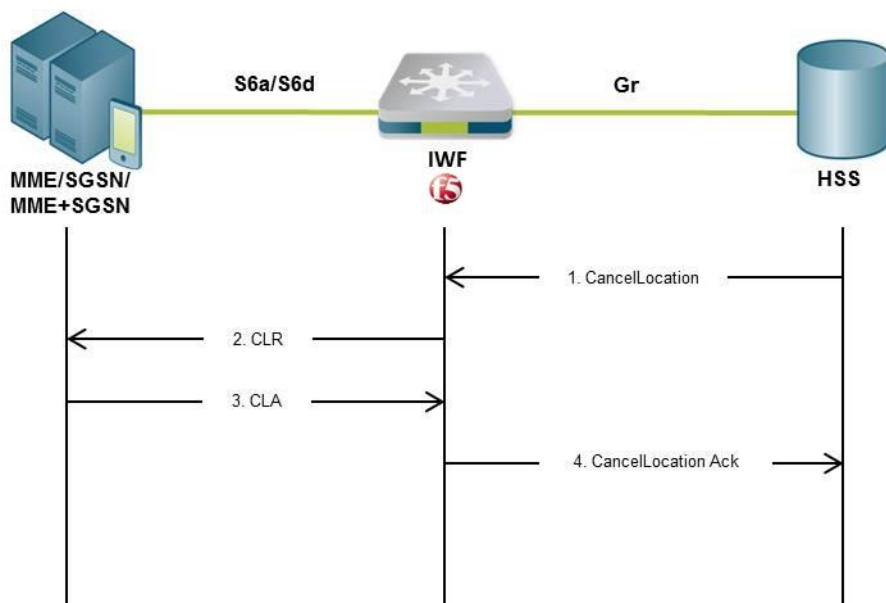


- InsertSubscriberData Ack messages back to the IWF. If the trace data option is enabled in the ULA received by the IWF, it sends an ActivateTraceMode message to the F5 IWF, which then sends an ActivateTraceMode Ack message to the IWF.
6. The IWF closes the MAP dialogue by sending an UpdateGprsLocation Ack to the F5 IWF.
 7. The F5 IWF uses the information received from the IWF to create a ULA message which is sent to the MME, SGSN, or combined MME/SGSN.

B.4 Cancel Location

B.4.1 One IWF Scenario


Figure 13: Cancel Location – One IWF Scenario



The figure above maps out the following Cancel Location procedure in a single IWF deployment:

1. The F5 IWF receives a CancelLocation MAP (version 3) message from the HLR.

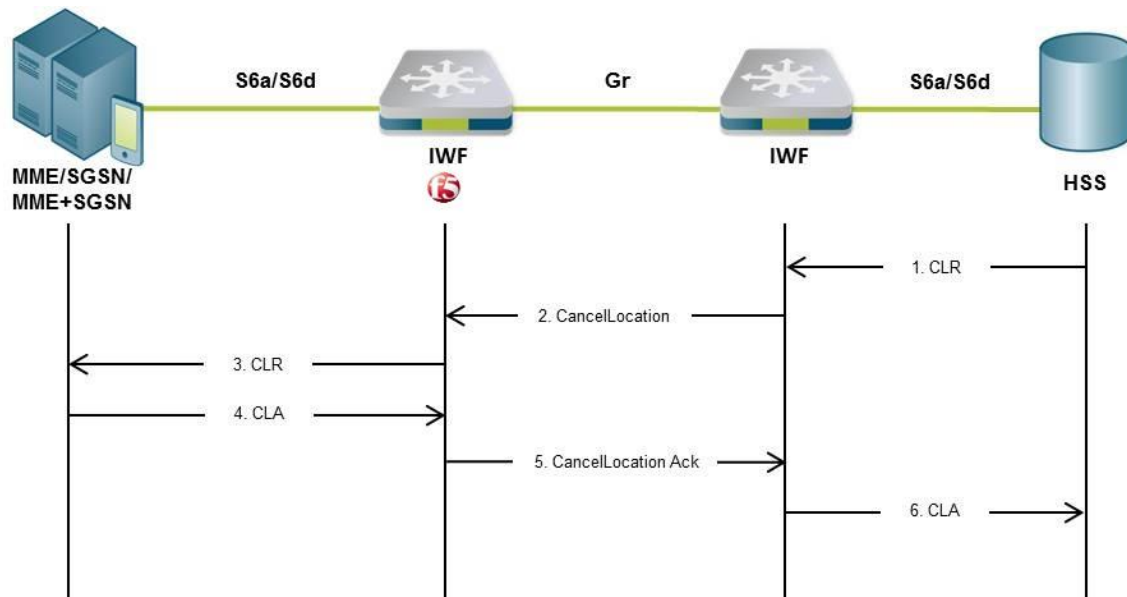


 Note: The F5 IWF will reject CancelLocation messages in MAP versions earlier than version 3, and will initiate version fallback when receiving CancelLocation messages in versions later than version 3.

2. The F5 IWF sends a CLR message to the MME, SGSN, or combined MME/SGSN.
3. The F5 IWF receives a CLA message from the MME, SGSN, or combined MME/SGSN.
4. The F5 IWF closes the MAP dialogue with the HLR by sending a CancelLocation Ack message.

B.4.2 Two IWFs Scenario

Figure 14: Cancel Location – Two IWFs Scenario



The figure above maps out the following Cancel Location procedure in a dual IWF deployment:

1. A CLR message is sent from the HSS to the IWF.
2. The IWF opens a MAP (version 3) dialogue towards the F5 IWF by sending a CancelLocation request.

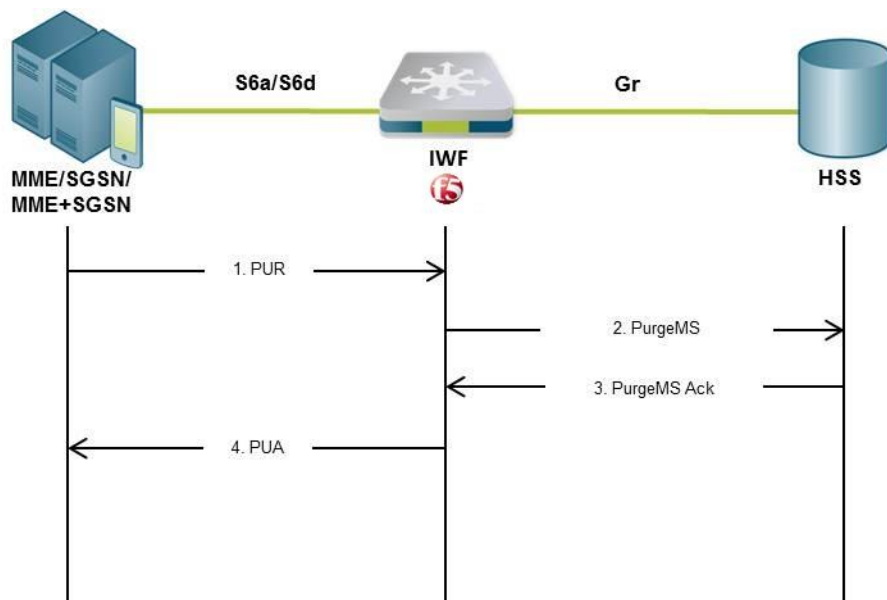


3. The F5 IWF creates a CLR message and sends it to the MME, SGSN, or combined MME/SGSN.
4. A CLA message is sent from the MME, SGSN or combined MME/SGSN to the F5 IWF.
5. The F5 IWF closes the MAP dialogue with the additional IWF by sending a CancelLocation Ack message.
6. A CLA message is sent from the IWF to the HSS.

B.5 Purge

B.5.1 One IWF Scenario

Figure 15: Purge – One IWF Scenario



The figure above maps out the following Purge procedure in a single IWF deployment:

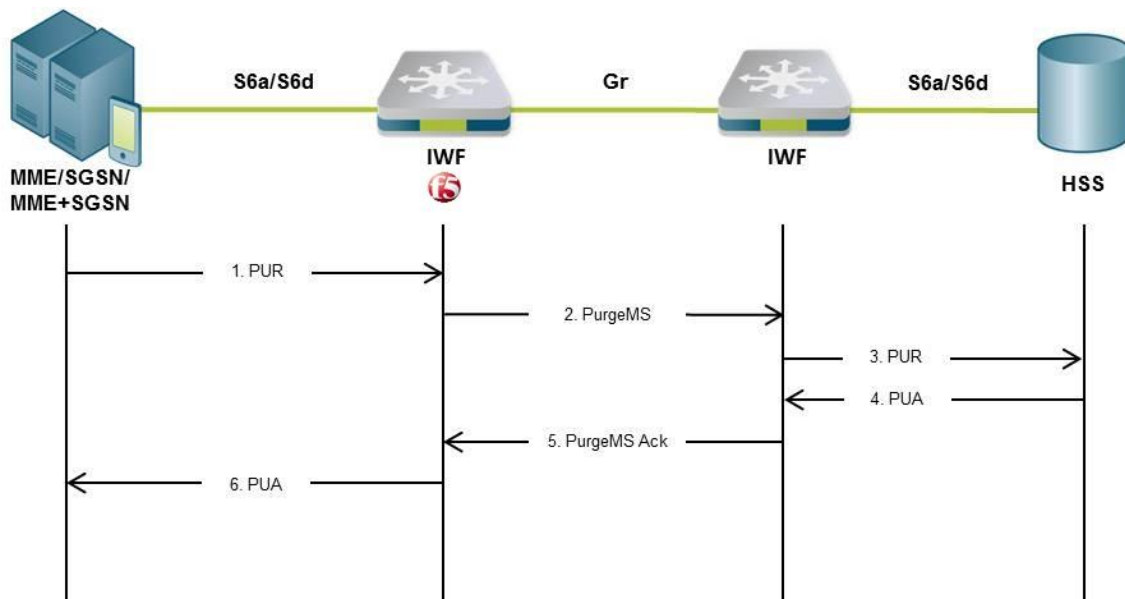
1. A PUR message is sent from the MME, SGSN, or combined MME/SGSN to the F5 IWF.



2. The F5 IWF creates a MAP (version 3) dialogue towards the HLR by sending a PurgeMS request.
3. The F5 IWF receives a PurgeMS Ack response from the HLR.
4. The F5 IWF sends a PUA message to the MME, SGSN, or combined MME/SGSN.

B.5.2 Two IWFs Scenario

Figure 16: Purge – Two IWFs Scenario



The figure above maps out the following Purge procedure in a dual IWF deployment:

1. A PUR message is sent from the MME, SGSN, or combined MME/SGSN to the F5 IWF.
2. The F5 IWF creates a MAP (version 3) dialogue towards the additional IWF by sending a PurgeMS request.
3. The IWF creates a PUR message and sends it to the HSS.
4. The IWF receives a PUA message from the HSS.
5. The IWF closes the MAP dialogue with the F5 IWF by sending a PurgeMS Ack message.

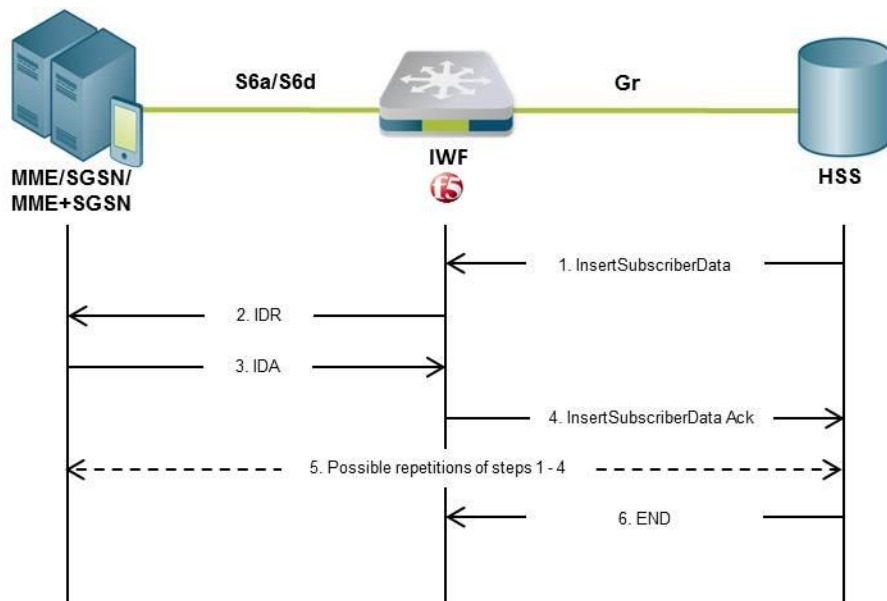


6. The F5 IWF sends a PUA message to the MME, SGSN, or combined MME/SGSN.

B.6 Insert Subscriber Data

B.6.1 One IWF Scenario

Figure 17: Insert Subscriber Data – One IWF Scenario



The figure above maps out following Insert Subscriber Data procedure in a single IWF deployment:

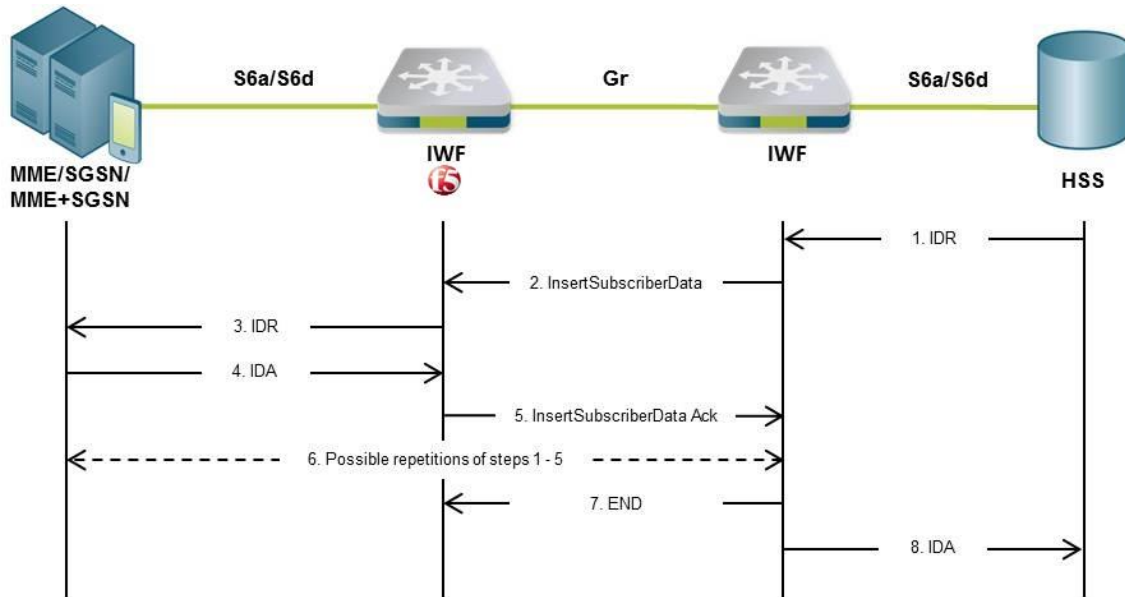
1. A (standalone) InsertSubscriberData message is sent from the HLR to the F5 IWF.
2. The F5 IWF creates an IDR message and sends it to the MME, SGSN, or combined MME/SGSN.
3. The F5 IWF receives an IDA message from the MME, SGSN, or combined MME/SGSN.
4. The F5 IWF sends an InsertSubscriberData Ack message to the HLR.
5. Steps 1 to 4 may be repeated several times. The repetition may be in burst or acknowledge mode.



6. The HLR closes the MAP dialogue.

B.6.2 Two IWFs Scenario

Figure 18: Insert Subscriber Data – Two IWFs Scenario



The figure above maps out the following Insert Subscriber Data procedure in a dual IWF deployment:

1. An IDR message is sent from the HSS to the IWF.
2. The IWF opens a MAP (version 3) dialogue towards the F5 IWF by sending an InsertSubscriberData message.



Note: If segmentation of the data (on MAP level) is required, the IWF temporarily stores the data that could not be sent in this step.

3. The F5 IWF creates an IDR message and sends it to the MME, SGSN, or combined MME/SGSN.
4. The F5 IWF receives an IDA message from the MME, SGSN, or combined MME/SGSN.
5. The F5 IWF sends an InsertSubscriberData Ack message to the IWF.

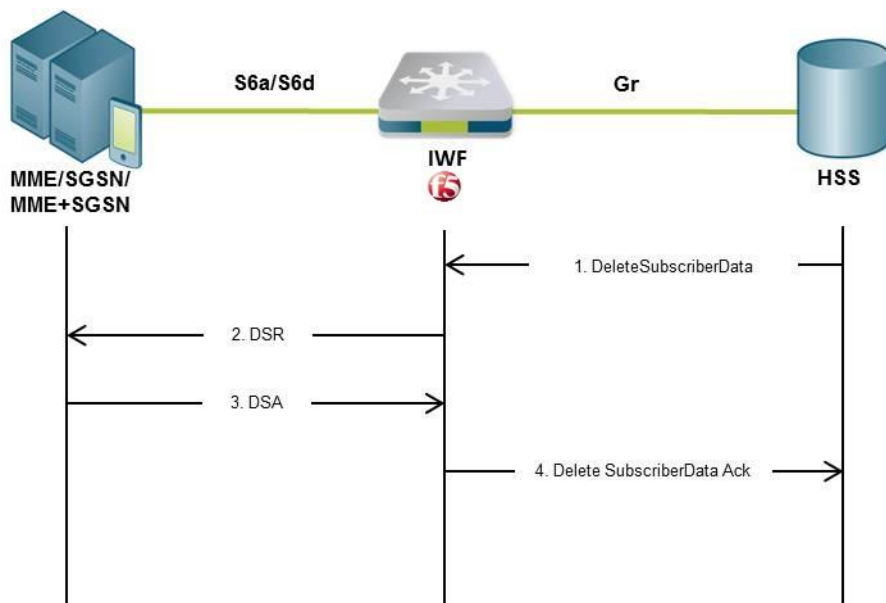


6. If segmentation is required, steps 2 to 5 are repeated until all data is sent. The repetition may be in burst or acknowledge mode.
7. The IWF closes the MAP dialogue with the F5 IWF.
8. The IWF sends an IDA message to the HSS.

B.7 Delete Subscriber Data

B.7.1 One IWF Scenario

Figure 19: Delete Subscriber Data – One IWF Scenario



The figure above maps out the following Delete Subscriber Data procedure in a single IWF deployment:

1. A DeleteSubscriberData MAP (version 3) message is sent from the HLR to the F5 IWF.



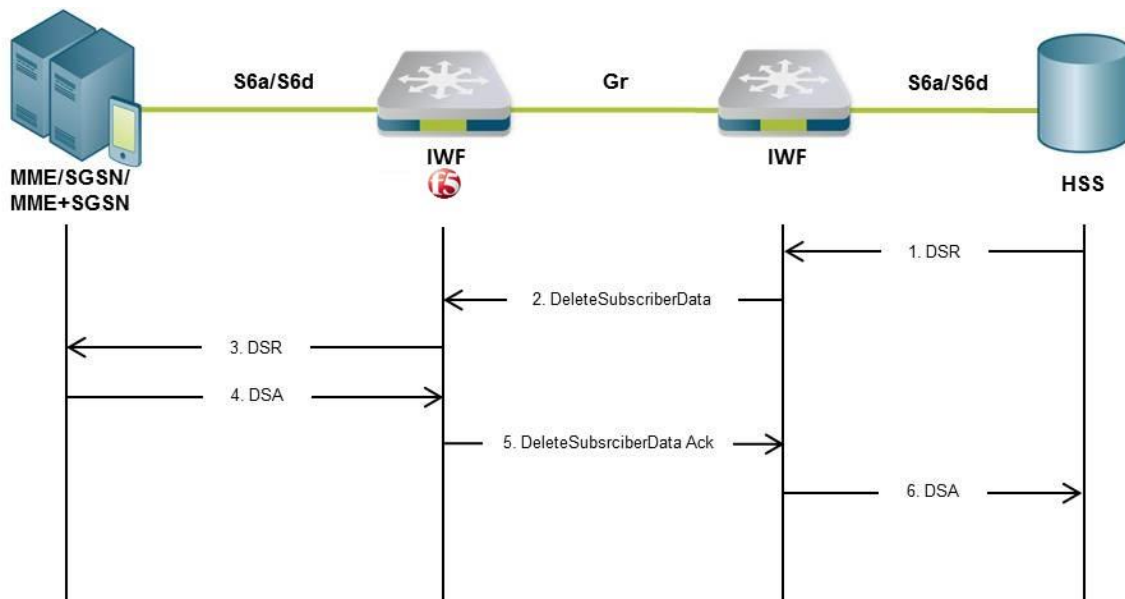
Note: The F5 IWF will reject DeleteSubscriberData messages in MAP versions earlier than version 3, and will initiate version fallback when receiving DeleteSubscriberData messages in versions later than version 3.



2. The F5 IWF sends a DSR message to the MME, SGSN, or combined MME/SGSN.
3. The F5 IWF receives a DSA message.
4. The F5 IWF closes the MAP dialogue with the HLR by sending a DeleteSubscriberData Ack message.

B.7.2 Two IWFs Scenario

Figure 20: Delete Subscriber Data – Two IWFs Scenario



The figure above maps out the following Delete Subscriber Data procedure in a dual IWF deployment:

1. A DSR message is sent from the HSS to the IWF.
2. The IWF creates a MAP (version 3) dialogue towards the F5 IWF by sending a DeleteSubscriberData message.
3. The F5 IWF creates a DSR message and sends it to the MME, SGSN, or combined MME/SGSN.
4. The F5 IWF receives a DSA message from the MME, SGSN, or combined MME/SGSN.

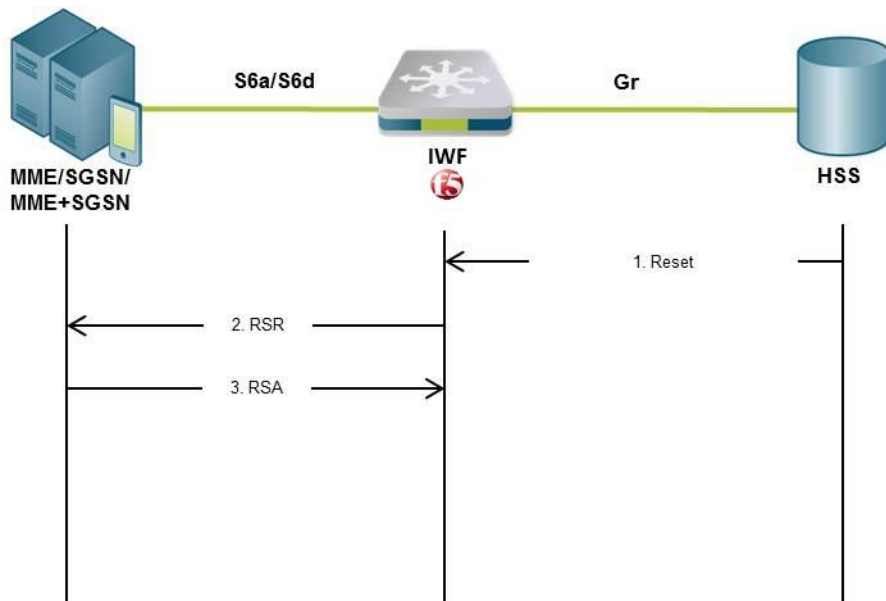


5. The F5 IWF closes the MAP dialogue with the IWF by sending a DeleteSubscriberData Ack message.
6. The IWF sends a DSA message to the HSS.

B.8 Reset

B.8.1 One IWF Scenario

Figure 21: Reset – One IWF Scenario



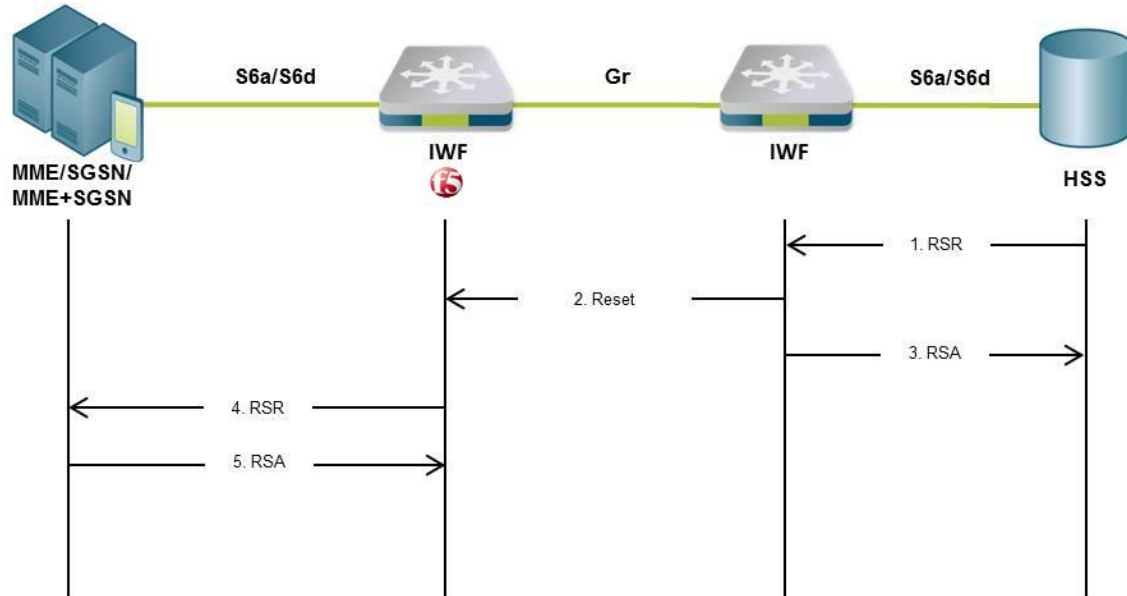
The figure above maps out the following Reset procedure in a single IWF deployment:

1. A Reset MAP (version 1 or version 2) message is sent from the HLR to the F5 IWF.
2. The F5 IWF sends a RSR message to the MME, SGSN, or combined MME/SGSN.
3. The F5 IWF receives a RSA message.



B.8.2 Two IWFs Scenario

Figure 22: Reset – Two IWFs Scenario



The figure above maps out the following Reset procedure in a dual IWF deployment:

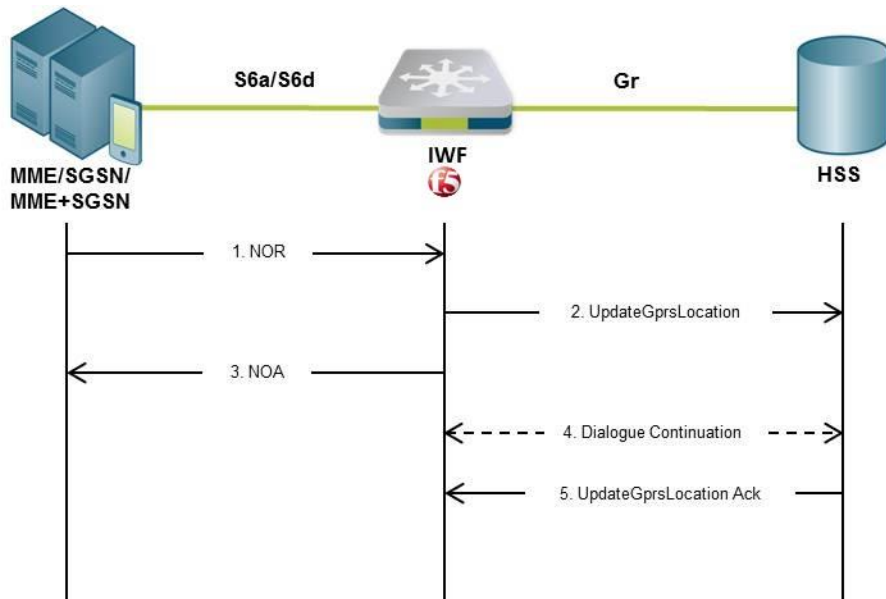
1. An RSR message is sent from the HSS to the IWF.
2. The IWF opens a MAP (version 1 or version 2) dialogue towards the F5 IWF by sending a Reset message.
3. The IWF sends an RSA message to the HSS.
4. The F5 IWF creates a RSR message and sends it to the MME, SGSN, or combined MME/SGSN.
5. The F5 IWF receives an RSA message from the MME, SGSN, or combined MME/SGSN.



B.9 Notification

B.9.1 One IWF Scenario

Figure 23: Notification – One IWF Scenario



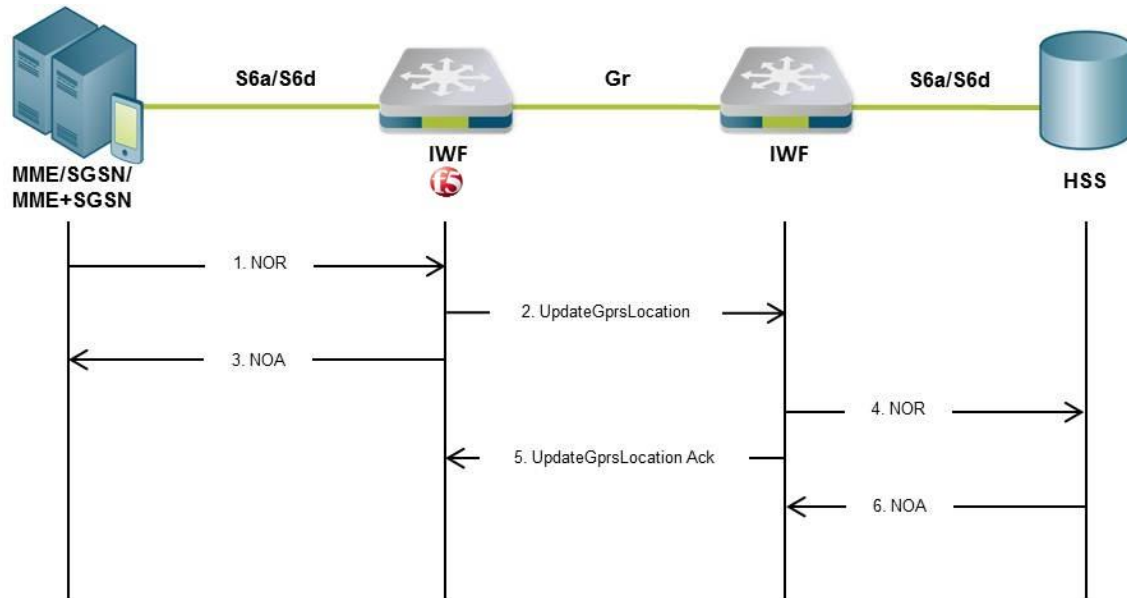
The figure above maps out the following Notification procedure in a single IWF deployment:

1. A NOR message is sent from the MME, SGSN, or combined MME/SGSN to the F5 IWF.
2. The F5 IWF sends an UpdateGprsLocation or ReadyForSM message to the HLR.
3. The F5 IWF sends a NOA message to the MME, SGSN, or combined MME/SGSN.
4. The HLR (if it does not support the "skip subscriber data" ability) may continue the MAP dialogue by sending InsertSubscriberData messages (which are positively acknowledged and discarded) to the F5 IWF.
5. The HLR closes the MAP dialogue by sending an UpdateGprsLocation Ack or ReadyForSM Ack message.



B.9.2 Two IWFs Scenario

Figure 24: Notification – Two IWFs Scenario



The figure above maps out the following Notification procedure in a dual IWF deployment:

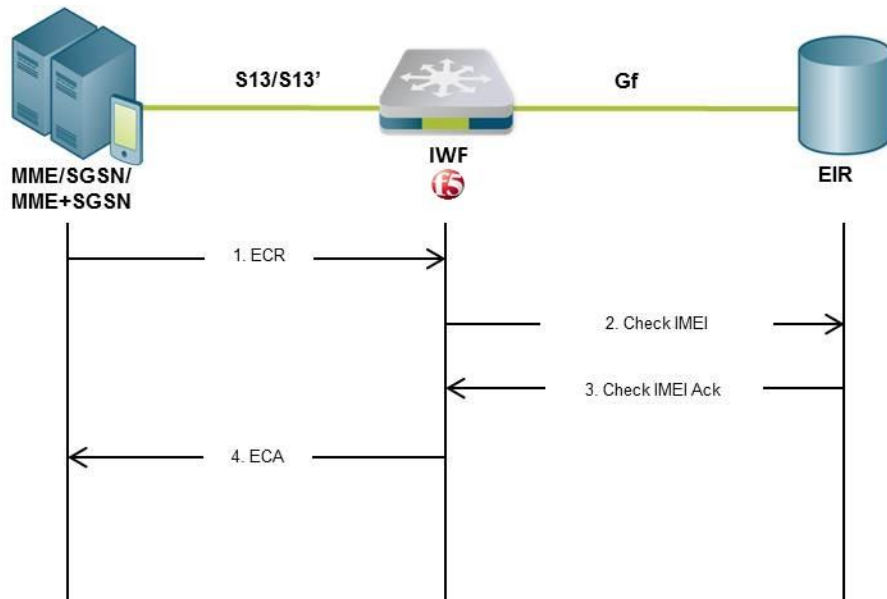
1. A NOR message is sent the MME, SGSN, or combined MME/SGSN to the F5 IWF.
2. The F5 IWF sends an UpdateGprsLocation or ReadyForSM message to the IWF.
3. The F5 IWF sends a NOA message to the MME, SGSN, or combined MME/SGSN.
4. The IWF sends a NOR message to the HSS.
5. The IWF closes the MAP dialogue with the F5 IWF by sending an UpdateGprsLocation Ack or ReadyForSM Ack message.
6. The IWF receives a NOA message from the HSS.



B.10 IMEI Check

B.10.1 One IWF Scenario

Figure 25: IMEI Check – One IWF Scenario



The figure above maps out the following IMEI Check procedure in a single IWF deployment:

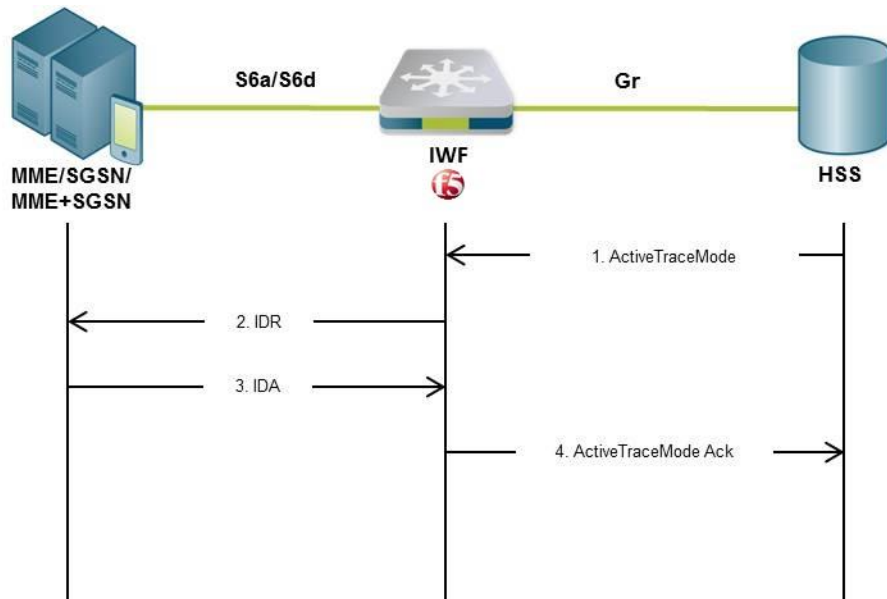
1. An ECR message is sent from the MME, SGSN, or combined MME/SGSN to the F5 IWF.
2. The F5 IWF sends a Check IMEI request to the EIR.
3. The F5 IWF receives a Check IMEI Ack response from the EIR.
4. The F5 IWF sends an ECA message to the MME, SGSN, or combined MME/SGSN.



B.11 Trace Activation

B.11.1 One IWF Scenario

Figure 26: Trace Activation – One IWF Scenario



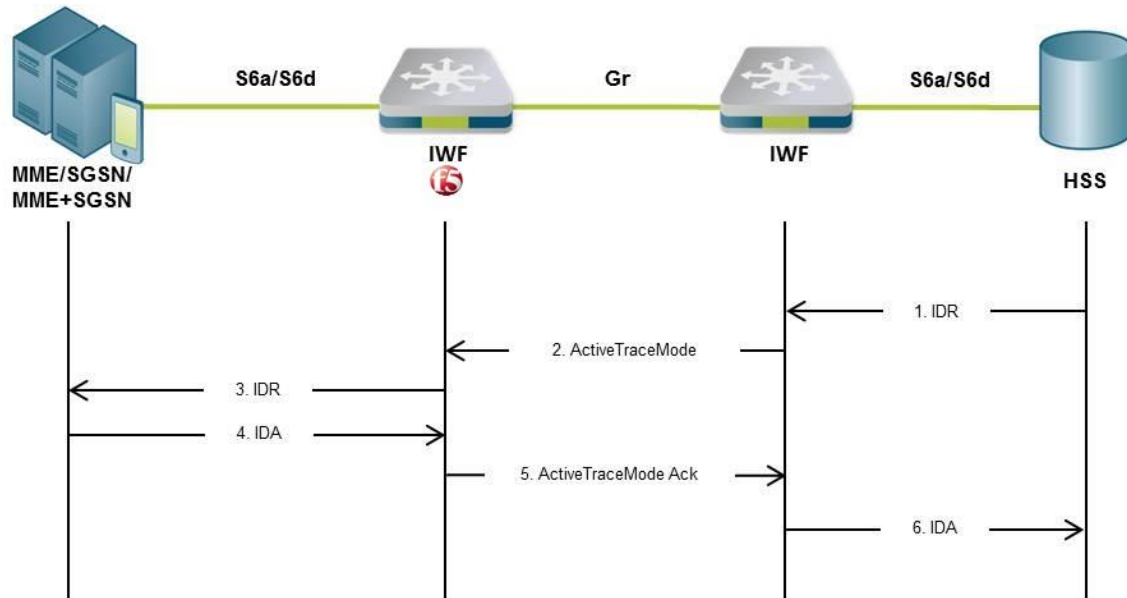
The figure above maps out the following Trace Activation procedure in a single IWF deployment:

1. An ActivateTraceMode message is sent from the HLR to the F5 IWF.
2. The F5 IWF creates an IDR message and sends it to the MME, SGSN, or combined MME/SGSN.
3. The F5 IWF receives an IDA message from the MME, SGSN, or combined MME/SGSN.
4. The F5 IWF sends an ActivateTraceMode Ack message to the HLR.



B.11.2 Two IWFs Scenario

Figure 27: Trace Activation – Two IWFs Scenario



The figure above maps out the following Trace Activation procedure in a dual IWF deployment:

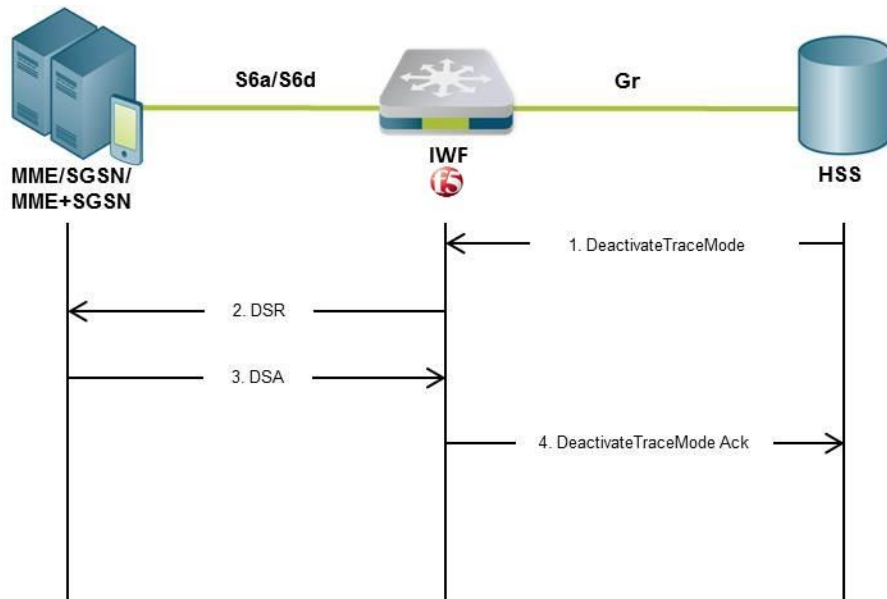
1. An IDR message is sent from the HSS to the IWF.
2. If the IWF finds that “Trace Data” is included in the IDR, it opens a MAP (version 3) dialogue towards the F5 IWF by sending an ActivateTraceMode request.
3. The F5 IWF creates an IDR message and sends it to the MME, SGSN, or combined MME/SGSN.
4. The F5 IWF receives an IDA message from the MME, SGSN, or combined MME/SGSN.
5. The F5 IWF sends an ActivateTraceMode Ack message to IWF.
6. The IWF sends an IDA message to the HSS.



B.12 Trace Deactivation

B.12.1 One IWF Scenario

Figure 28: Trace Deactivation – One IWF Scenario



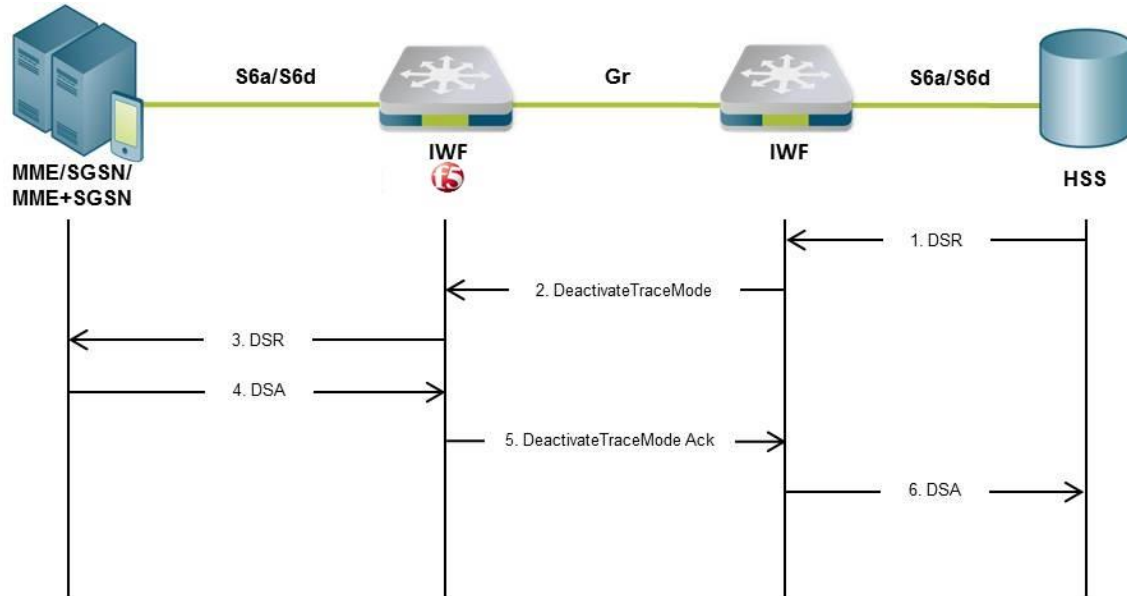
The figure above maps out the following Trace Deactivation procedure in a single IWF deployment:

1. A DeactivateTraceMode message is sent from the HLR to the F5 IWF.
2. The F5 IWF creates a DSR message and sends it to the MME, SGSN, or the combined MME/SGSN.
3. The F5 IWF receives a DSA message from the MME, SGSN, or combined MME/SGSN.
4. The F5 IWF sends a DeactivateTraceMode Ack message to the HLR.



B.12.2 Two IWFs Scenario

Figure 29: Trace Deactivation – Two IWFs Scenario



The figure above maps out the following Trace Deactivation procedure in a dual IWF deployment:

1. A DSR message is sent from the HSS to the IWF.
2. If the IWF finds that “Trace Data Withdrawal” is included in the DSR, it opens a MAP (version 3) dialogue towards the F5 IWF by sending a DeactivateTraceMode request.
3. The F5 IWF creates a DSR message and sends it to the MME, SGSN, or combined MME/SGSN.
4. The F5 IWF receives a DSA message from the MME, SGSN, or combined MME/SGSN.
5. The F5 IWF sends a DeactivateTraceMode Ack request to the IWF.
6. The IWF sends a DSA to the HSS.



Glossary

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

Table 4: 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
SCCP	Signaling Connection Control Part



Term	Definition
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