

MTAS SS7 Management Guide

MTAS

USER GUIDE

Copyright

© Ericsson AB 2016, 2018–2019. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
1.1	Prerequisites	1
2	Overview	3
3	H.248 over SCTP	5
4	Diameter over SCTP	7
5	M3UA over SCTP	13
6	MTP3-User Configuration	19
6.1	Signaling Network Configuration	19
6.2	Configure TCAP	21
6.3	CAP and MAP Configuration	22
6.4	Configure SCTPs, PMTU, and IPv6 PMTU	24
7	Activate the Configuration Changes	25





1 Introduction

This document describes how to enable and configure Signaling System 7 (SS7) stack for the MTAS.

1.1 Prerequisites

It is assumed that the user of this document is familiar with the Operation and Maintenance (O&M) area, in general.

1.1.1 Licenses

Not applicable.

1.1.2 Documents

Before starting any procedure in this document, ensure that the following documents are available:

- MTAS Internal and External Connectivity
- Ericsson Command-Line Interface User Guide
- Managed Object Model (MOM)
- Signaling Manager User Guide
- MTAS Media Control Management Guide
- Diameter Management
- MTAS Subscriber Data Management Guide
- MTAS Charging Management Guide
- MTAS IMS Centralized Services Management Guide
- MTAS CAPv2 Management Guide

1.1.3 Conditions

The following conditions must apply:

- The MTAS non-VIP and VIP external connectivity is established
- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.



— The Signaling Manager is connected.



2 Overview

MTAS includes several functions that are providing services to external network entities over such logical interfaces that are using SCTP for transport. To these services (Diameter, H.248, and M3UA), as “SCTP User Application”, the system embedded SS7 component is providing “SCTP transport service”.

In addition, some other functions use transfer of CAMEL Application Part (CAP) and ETSI Mobile Application Part (MAP) operations through Signaling Transport over IP (SIGTRAN), that is, SS7 together with Stream Control Transmission Protocol (SCTP). Therefore, MTAS can be configured with the SS7 stack using SCTP, Message Transfer Part User Adapt Layer (M3UA), Signaling Connection Control Part (SCCP), Transaction Capabilities Application Part (TCAP), IN Application Part (INAP) to enable CAP traffic, and ETSI Mobile Application Part (MAP) to enable ETSI MAP traffic. Throughout the document when “MAP” is used, it implies “ETSI MAP”.

This document provides guidelines and instructions how to influence the behavior of the SS7 provided “SCTP Transport Service” for “SCTP User Applications” of different kind (Diameter, MRFC, M3UA), and also gives some guidelines how the SIGTRAN full-stack is supposed to be configured in MTAS.





3 H.248 over SCTP

Plain SCTP, that is, without SS7, is used as the transport protocol in the H.248-based Mp interface. The interface is used between the integrated Media Resource Function Controller (MRFC) distributed function in MTAS and external Multimedia Resource Function Processors (MRFP) whenever multimedia session manipulation is needed. The Service Access Point (SAP) to the distributed MRFC function is provided by an SCTP socket.

The high-availability of the SAP is assured in a way that the SCTP socket (SCTP EndPoint) is created on a shared IP (Virtual IP; VIP) address by as many service instances as many PLs are contained in the MTAS VNF. That is: the VNF is ready to terminate any of the MRFP-initiated H.248 over SCTP control link association on any of the available PLs; the underlying VIP layer decides to which available service instance an SCTP association is distributed.

A service instance is determining the SCTP EndPoint, the socket parameters as follows:

— IP

- The `tasvip4` and `tasvip6` hostnames are resolved, resulting a pair of IP addresses in the IPv4/IPv6 dual-stack scenario. IPv4-only and IPv6-only use cases are also supported (either of the IP to hostname association is absent).
- The IP to hostname associations are made VNF internally, cluster-wise available in a persistent way by defining the rules in `/cluster/etc/cluster.conf`.
- The used IPv4 and IPv6 addresses in these rules must be VIP addresses that are assigned to the `mtas_sig` network (distributor) device.

— Port

- The ITU-T recommended well-known port (2944) is hard-coded into the MRFC function

Once these inputs are all collected, the SAP is opened on every PL instance by the MRFC service instances.

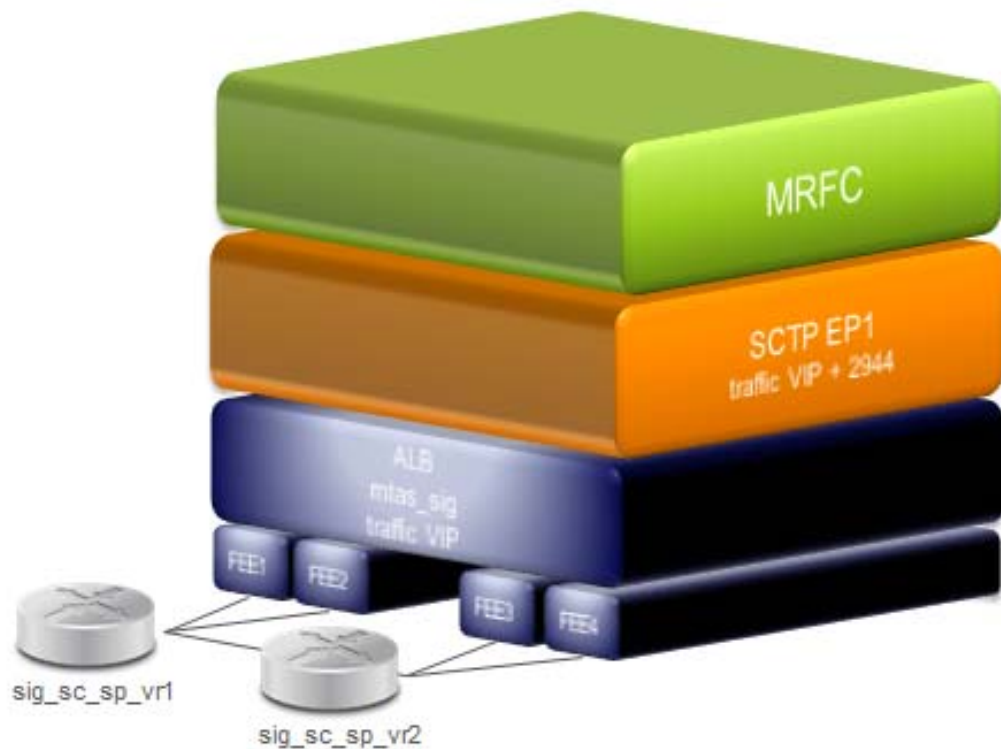


Figure 1 Mp in MTAS, The Interface Is Bound to a Single-Homed Local SCTP EndPoint

Note:

- The SAP for the distributed MRFC function is created if the ManagedElement=1, MtasFunction=MtasFunction, MtasMrfc=0, mtasMrfcServiceLocation configuration attribute is set to INTERNAL.
- In contrary to the general misconception, the distributed MRFC function does not attempt to retrieve SCTP socket parameters (IP, port) from SS7 OAM. In turn, the function does not require any configuration change in the MTAS VNF embedded SS7 component. The MTAS VNF image contains such SS7 component-specific default settings that enable the described, MRFC function-specific way of opening its SAP for the remote MRFPs.
- The behavior of the MRFC SCTP EndPoint and its terminated SCTP associations (the SCTP transport service) can be influenced by tuning the parameters of SCTP End Point Profile = 0 through the SS7 Signaling Manager that can be started either in CLI (**ss7smcli**) or GUI mode (**ss7smgui**). In the latter case, the X-forwarding through SSH must be enabled.



4 Diameter over SCTP

Plain SCTP, that is, without SS7, can be used as the transport protocol in the Diameter-based external logical interfaces, in Rf/Ro/CDS and also Sh/Dh.

- The Dh interface between the MTAS and the Subscriber Location Function (SLF) is used to retrieve the address of the HSS, which holds the subscription for a given user.
- The Sh interface, which is between the MTAS and the HSS, is used for transferring user profile information such as user service-related information, user identities, or charging function addresses.
- The Rf interface is used between the MTAS and the Charging Data Function (CDF) for transferring MMTel offline charging information.
- The Ro interface (Diameter Credit Control Application) is used between the MTAS and the Online Charging Function (OCF) for transferring MMTel online charging information. The Ro interface is also used by the Advice of Charge (AoC) Supplementary Service for accessing the AoC information related to a communication to be provided to the served user.
- The Communication Details Servers (CDS) interface is used between the MTAS and the CDS by the Malicious Communication Identification (MCID) service to transfer communication details for Malicious Communication Identification purposes. It is also used by other Supplementary Services that allow the user to request actions that are based on earlier calls (that is, Dynamic Black List).

Between MTAS and the adjacent Diameter Peer Node, it is possible to set up either a single connection or multiple connections. By the use of multiple connections the load is spread among the available PL instances and the throughput is increased. TCP and SCTP transport are both supported for these connections. Each connection is handled by a Diameter service instance. When SCTP is chosen for the transport protocol, a service instance is exposing the local endpoint of a Diameter connection as an SCTP EndPoint on an arbitrary chosen PL. If the PL is scaled in, the corresponding SCTP EndPoint is created on another PL and the Diameter over SCTP connection is reestablished.

The socket parameters of an SCTP EndPoint are taken from the [Diameter configuration](#). In-line with the verified reference configurations, the local SCTP EndPoint of a Diameter connection can be created in two ways:

The Local SCTP EndPoint of a Diameter Connection Is Single-Homed

A single IP address (per INET flavor) is configured for the local SCTP EndPoint under the `ManagedElement=1,MtasFunction=MtasFunction,MtasSupportFunctions=0,DIA-CFG-Application=DIA` configuration management fragment.

- Dh/Sh: the configured IP address is the “Traffic VIP” address that is provided by the `mtas_sig` network device (ALB).

- Rf/Ro/CDS: the configured IP address is the “OM VIP” address that is provided by the `mtas_om` network device (ALB).



Figure 2 Dh/Sh in MTAS, The Interface Is Bound to a Single-Homed Local SCTP EndPoint



Figure 3 Rf/Ro/CDS in MTAS, The Interface Is Bound to a Single-Homed Local SCTP EndPoint

The Local SCTP EndPoint of a Diameter Connection Is Multihomed

Multiple IP addresses (per INET flavor) are configured for the local SCTP EndPoint under the ManagedElement=1,MtasFunction=MtasFunction,MtasSupportFunctions=0,DIA-CFG-Application=DIA configuration management fragment.

- Dh/Sh: the configured IP addresses are the “Traffic VIP MH1” and “Traffic VIP MH2” addresses that are provided by the `mtas_sig_pdl` and `mtas_sig_pdr` network devices (ALBs).
- Rf/Ro/CDS: the configured IP addresses are the “Ro/Rf/CDS VIP MH1” and “Ro/Rf/CDS VIP MH2” addresses that are provided by the `mtas_om_pdl` and `mtas_om_pdr` network devices (ALBs).

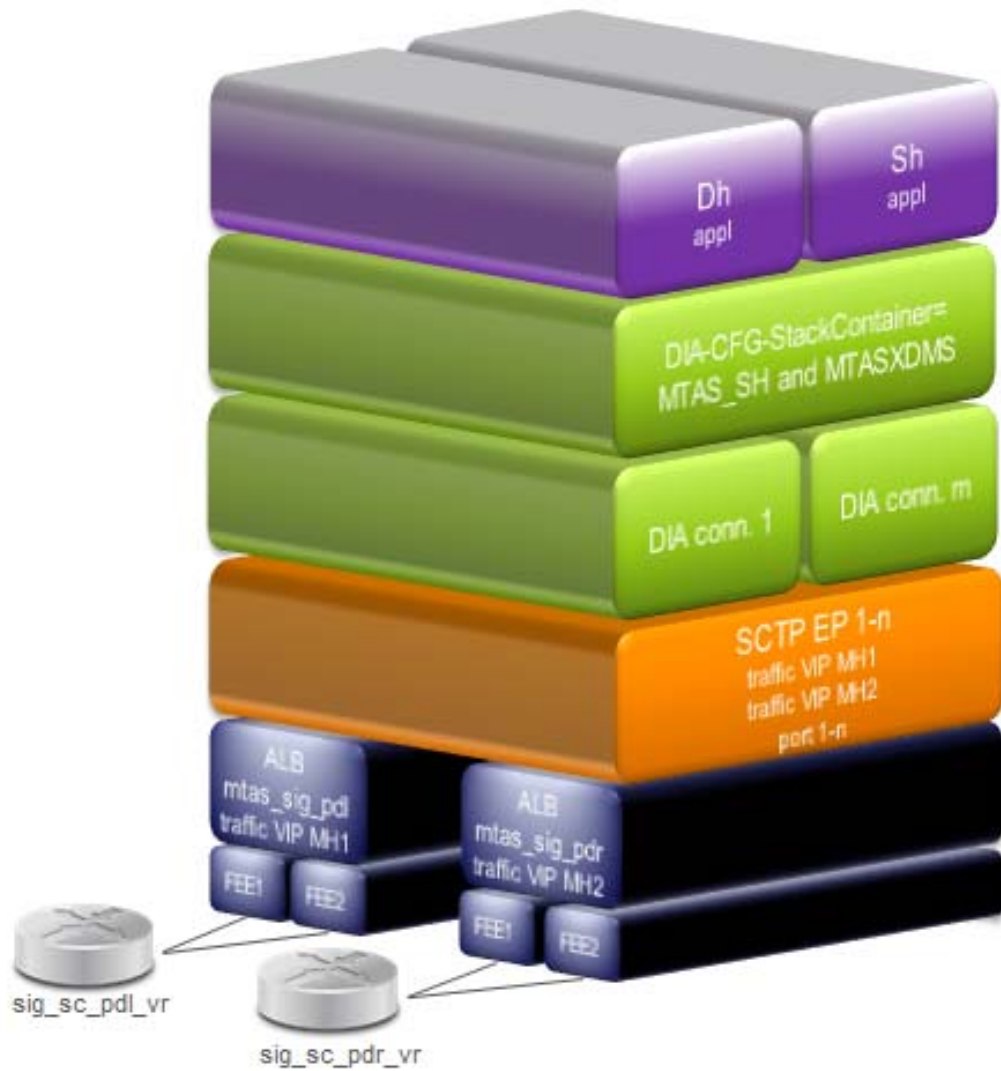


Figure 4 Dh/Sh in MTAS, The Interface Is Bound to a Multihomed Local SCTP EndPoint

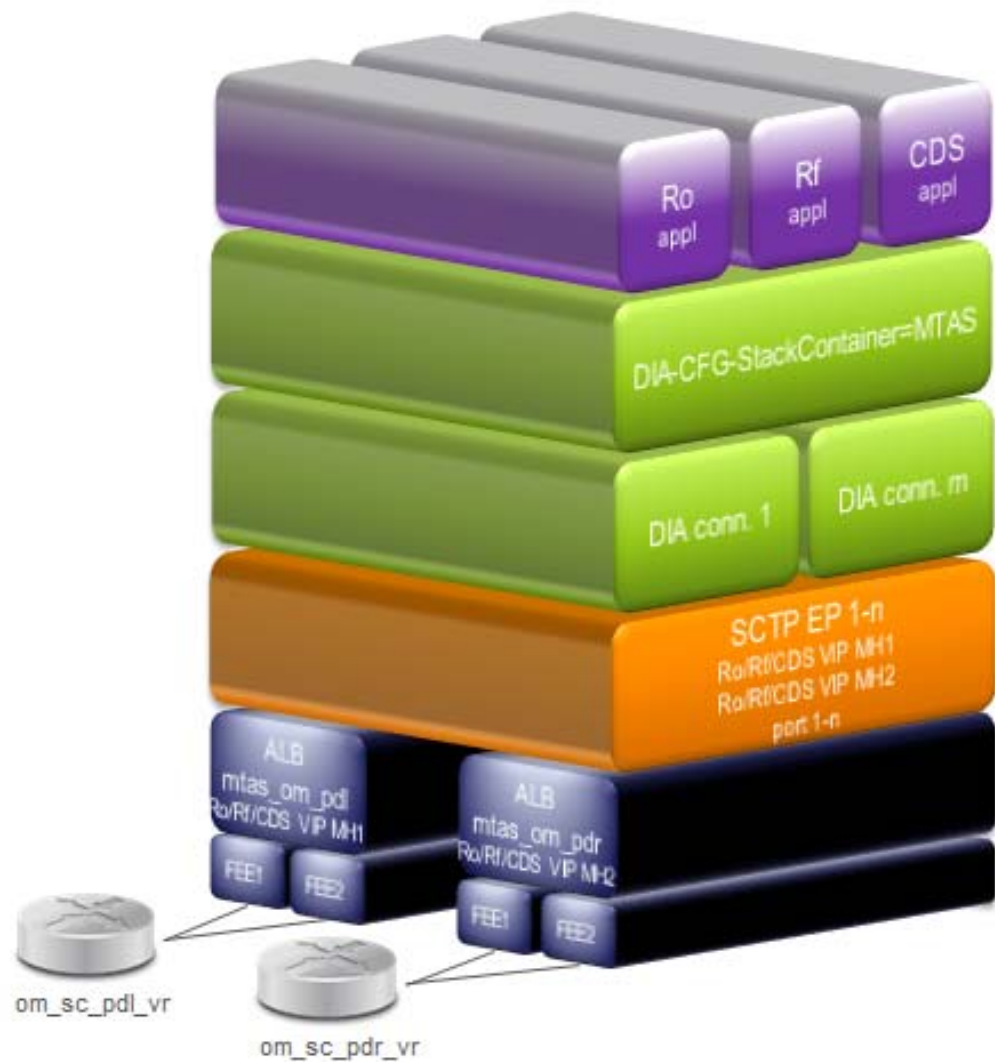


Figure 5 Rf/Ro/CDS in MTAS, The Interface Is Bound to a Multihomed Local SCTP EndPoint

See the MTAS Subscriber Data Management Guide for further details regarding how to configure the Diameter stack for the Sh/Dh interfaces. See the MTAS Charging Management Guide for further details regarding how to configure the Diameter stack for the Rf, Ro, and CDS interfaces.

**Note:**

- In contrary to the general misconception, the distributed Diameter stack does not attempt to retrieve SCTP socket parameters (IP, port) from SS7 OAM. In turn, its provided functions for the users (Dh/Sh, Rf/Ro/CDS) do not require any configuration change in the MTAS VNF embedded SS7 component. The MTAS VNF image contains such SS7 component-specific default settings that enable the summarized mechanism.
- The behavior of the Diameter SCTP EndPoint and its terminated SCTP associations (the SCTP transport service) can be influenced by tuning the parameters of SCTP End Point Profile = <x> through the SS7 Signaling Manager, where <x> equals to the value of the sctpEndPointProfile parameter that is set under a DIA-CFG-StackContainer, DIA-CFG-OwnNodeConfig Managed Object Instance. The SS7 Signaling Manager can be started either in CLI (**ss7smcli**) or GUI mode (**ss7smgui**). In the latter case, the X-forwarding through SSH must be enabled.



5 M3UA over SCTP

SCTP is used as the transport protocol in the M3UA based external logical interfaces. In the verified reference configurations – see the described in more detail in [MTAS Internal and External Connectivity](#) – the MTAS VNF is exposed as an M3UA Application Server with a pair of redundant ASPs/IPSPs associated with a specific Routing Key in the signaling network. The pairs of ASPs/IPSPs are bound to their unique local SCTP EndPoint. Unlike for other SCTP users (H.248, Diameter), the socket parameters of these SCTP EndPoint must be defined through the SS7 Signaling Manager ([Configuring SS7, SCTP](#)).

There are as many M3UA service instances running inside the VNF as many PLs are contained in the elastic segment. It is a VNF internal decision on which service instance the ASP/IPSP specific signaling links are handled. If a PL is scaled in for example, so an M3UA service instance that is handling an M3UA signaling link disappears, the signaling link is going to be handled by another one. The service instance is chosen based on VNF internal load balancing mechanism.

Note: Although an M3UA signaling link is handled by a selected M3UA service instance, the workload that is imposed on the VNF because of interworking with other SS7 signaling network entities is distributed among the available PLs on MTP3-User, on TCAP dialogue level.

The M3UA service instances are working from a common set of configuration objects that are defined in SS7 OAM through the SS7 Signaling Manager. For them, in-line with the verified reference configurations, the local SCTP EndPoints of the ASP/IPSPs can be created in two ways:

The Local SCTP EndPoint of an M3UA Signaling Link Is Single-Homed

A single IP address (per INET flavor) is configured for the local SCTP EndPoints:

— ASP/IPSP1

- IP: “SIGTRAN VIP SH1”, provided by the `mtas_sig` network device (ALB).
- Port: 2905

— ASP/IPSP2

- IP: “SIGTRAN VIP SH2”, provided by the `mtas_sig` network device (ALB).
- Port: 2905

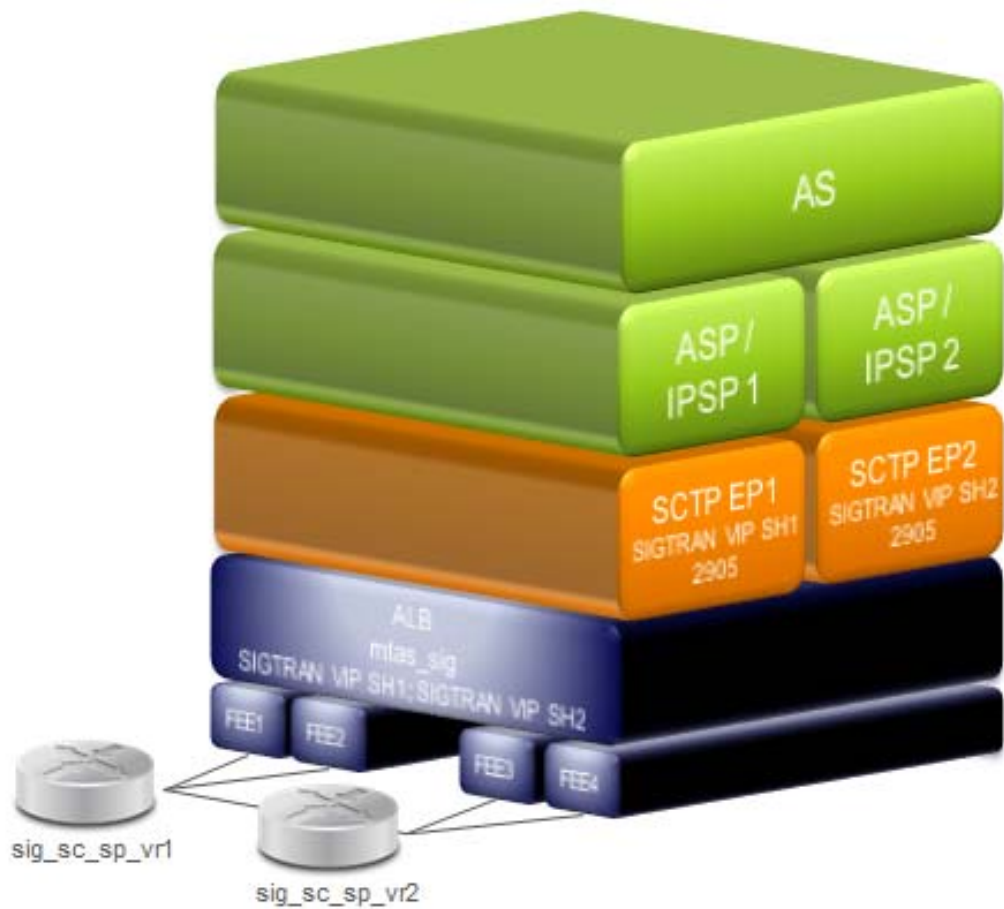


Figure 6 M3UA in MTAS, The Interface Is Bound to a Single-Homed Local SCTP EndPoint

To configure local SCTP EndPoints for the pair of ASP/IPSPs, in line with traffic separation profile1:

1. Open a Signaling Manager GUI.
2. Choose the **Tools** menu and select **Configuration Mode > Initial** in **Expert** mode.
3. Go to **Signaling System**.
4. Right-click **SCTP FE:256 > SCTP End Points**, select **Add**. A new **SCTP EP** with a **Local Address Table** is added.
5. In the newly added **SCTP EP**, set the **Port Number** to 2905, set the **Used by M3UA** to Yes, set the **Sctp End Point Profile** to SCTP End Point Profile #0, or create a new profile specific for M3UA and refer to that one.
6. In the newly added **Local Address Table**, per INET flavor, add **SIGTRAN VIP SH1**, set **Use Extended Format** to VPN name extension, set **VPN Name** to **mtas_sig**.



7. Right-click **SCTP FE:256 > SCTP End Points**, select **Add**. A new **SCTP EP** with a **Local Address Table** is added.
8. In the newly added **SCTP EP**, set the **Port Number** to 2905, set the **Used by M3UA** to Yes, set the **Sctp End Point Profile** to **SCTP End Point Profile #0**, or create a new profile specific for M3UA and refer to that one.
9. In the newly added **Local Address Table**, per INET flavor, add **SIGTRAN VIP SH2**, set **Use Extended Format** to **VPN name extension**, set **VPN Name** to **mtas_sig**.
10. In **M3UA IETF**, set **Distributed End Point Support** to **On** and create two **Local SP** Managed Object Instances (ASP or IPSP). Associate these with the local **SCTP EndPoints** that are created in the previous steps 4–6 and 7–9 (**SCTP End Point** attribute of the **Local SP** object instance).

The Local SCTP EndPoint of an M3UA Signaling Link Is Multihomed

Multiple IP addresses (per INET flavor) are configured for the local SCTP EndPoints:

— ASP/IPSP1

- IP: “SIGTRAN VIP MH1”, provided by the **mtas_sig_pdl** network device (ALB) and “SIGTRAN VIP MH2”, provided by the **mtas_sig_pdr** network device (ALB).
- Port: 2905

— ASP/IPSP2

- IP: “SIGTRAN VIP MH1”, provided by the **mtas_sig_pdl** network device (ALB) and “SIGTRAN VIP MH2”, provided by the **mtas_sig_pdr** network device (ALB).
- Port: 2906

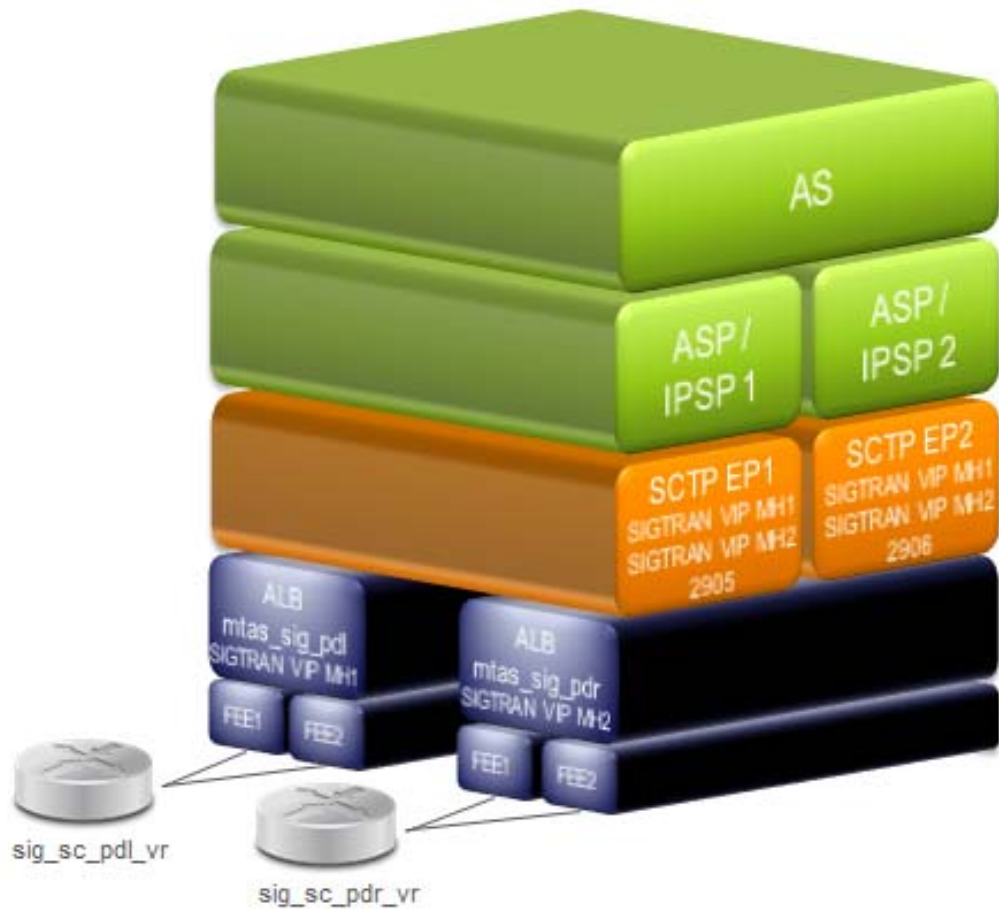


Figure 7 M3UA in MTAS, the Interface Is Bound to a Multihomed Local SCTP EndPoint

To configure local SCTP EndPoints for the pair of ASP/IPSPs, in line with traffic separation profile2:

1. Open a Signaling Manager GUI.
2. Choose the **Tools** menu and select **Configuration Mode > Initial** in **Expert** mode.
3. Go to **Signaling System**.
4. Right-click **SCTP FE:256 > SCTP End Points**, select **Add**. A new **SCTP EP** with a **Local Address Table** is added.
5. In the newly added **SCTP EP**, set the **Port Number** to 2905, set the **Used by M3UA** to Yes, set the **Sctp End Point Profile** to SCTP End Point Profile #0, or create a new profile specific for M3UA and refer to that one.
6. In the newly added **Local Address Table**, per INET flavor, add **SIGTRAN VIP MH1**, set **Use Extended Format** to VPN name extension, set **VPN Name** to **mtas_sig_pdl**.



7. In the same **Local Address Table**, per INET flavor, add SIGTRAN VIP MH2 , set **Use Extended Format** to VPN name extension, set **VPN Name** to mtas_sig_pdr.
8. Right-click **SCTP FE:256 > SCTP End Points**, select **Add**. A new **SCTP EP** with a **Local Address Table** is added.
9. In the newly added **SCTP EP**, set the **Port Number** to **2906**, set the **Used by M3UA** to Yes, set the **Sctp End Point Profile** to SCTP End Point Profile #0, or create a new profile specific for M3UA and refer to that one.
10. In the newly added **Local Address Table**, per INET flavor, add SIGTRAN VIP MH1 , set **Use Extended Format** to VPN name extension, set **VPN Name** to mtas_sig_pdr.
11. In the same **Local Address Table**, per INET flavor, add SIGTRAN VIP MH2 , set **Use Extended Format** to VPN name extension, set **VPN Name** to mtas_sig_pdr.
12. In **M3UA IETF** , set **Distributed End Point Support** to On and create two **Local SP** Managed Object Instances (ASP or IPSP). Associate these with the local SCTP EndPoints that are created in the previous steps 4–6 and 7–9 (**SCTP End Point** attribute of the **Local SP** object instance).





6 MTP3-User Configuration

The following scenarios are to be considered:

- Configure CAP/INAP when the MTAS node is deployed as an SCC AS and acts as a gsmSCF for Service Domain Selection (SDS), to assist MSC to select IMS as service domain for ICS users.
- Configure ETSI MAP when the MTAS node is deployed as an SCC AS without interface to HSS (IMS) and acts as a GMSC to interwork with HLR to retrieve MSRN routing number.
- Configure CAP/INAP when the MTAS node is deployed as an MMTel Telephony AS and it acts as a gsmSSF when interworking with IN services.

6.1 Signaling Network Configuration

A prerequisite is that the SS7 signaling network is configured before performing the tasks in the following sections. This configuration includes the following stack layers:

- M3UA
- SCCP

How to connect M3UA and SCTP is described briefly in Section 5 on page 13.

The MTAS specifics to be considered when configuring the SS7 signaling network is listed in the following subsections:

SCCP Layer

The Subsystem Number (SSN) selected for gsmSSF user in the local SCCP SAP must match with the configured SSN in MTAS, `mtasCsiSsfSubsystemNumber`.

The Subsystem Number (SSN) selected for the remote SCCP SAP must match with the configured SSN in MTAS, `mtasCsiRemoteScfSubsystemNumber`.

The Subsystem Number (SSN) selected for gsmSCF user in the local SCCP SAP must match with the configured SSN in MTAS, `mtasCsiScfSubsystemNumber`.

Based on the configuration description in this document, it is assumed that `mtasCsiSsfSubsystemNumber` and `mtasCsiScfSubsystemNumber` are not configured to same subsystem number.

The Subsystem Number (SSN) selected for GMSC user in the local SCCP SAP must match with the configured SSN in MTAS, `mtasCsiMapGmscSubsystemNumber` and `mtasCsiCapGmscSubsystemNumber`.

A GT Translator for MAP called party, CAP calling party, and CAP called party must be configured for the Local SPC that matches with the global title encoding for called party and calling party that are used in the MTAS CSI subsystem.

This process means the following:

- When `mtasCsiMapCdGti=1`: `mtasCsiMapCdNai` must match with configured Nature of Address.
- When `mtasCsiMapCdGti=2`: `mtasCsiMapCdTt` must match with configured Translation Type.
- When `mtasCsiMapCdGti=3`: `mtasCsiMapCdTt` and `mtasCsiMapCdNp` must match with configured Translation Type and Numbering Plan.
- When `mtasCsiMapCdGti=4`: `mtasCsiMapCdTt`, `mtasCsiMapCdNp`, and `mtasCsiMapCdNai` must match with configured Translation Type, Numbering Plan, and Nature of Address.
- When `mtasCsiCapCdGti=1`: `mtasCsiCapCdNai` must match with configured Nature of Address.
- When `mtasCsiCapCdGti=2`: `mtasCsiCapCdTt` must match with configured Translation Type.
- When `mtasCsiCapCdGti=3`: `mtasCsiCapCdTt`, `mtasCsiCapCdNp`, and `mtasCsiCapCdEs` must match with configured Translation Type, Numbering Plan, and Encoding scheme.
- When `mtasCsiCapCdGti=4`: `mtasCsiCapCdTt`, `mtasCsiCapCdNp`, `mtasCsiCapCdNai`, and `mtasCsiCapCdEs` must match with configured Translation Type, Numbering Plan, Nature of Address, and Encoding scheme.
- When `mtasCsiCapCgGti=1`: `mtasCsiCapCgNai` must match with configured Nature of Address.
- When `mtasCsiCapCgGti=2`: `mtasCsiCapCgTt` must match with configured Translation Type.
- When `mtasCsiCapCgGti=3`: `mtasCsiCapCgTt`, `mtasCsiCapCgNp`, and `mtasCsiCapCgEs` must match with configured Translation Type, Numbering Plan, and Encoding scheme.
- When `mtasCsiCapCgGti=4`: `mtasCsiCapCgTt`, `mtasCsiCapCgNp`, `mtasCsiCapCgNai`, and `mtasCsiCapCgEs` must match with configured Translation Type, Numbering Plan, Nature of Address, and Encoding scheme.

When creating a Signaling Network for ETSI MAP, set the Network Standard same as selected in MTAS CSI subsystem, `mtasCsiMapSccpStandard` and `mtasCsiCapSccpStandard` (ITU or ANSI).



6.2 Configure TCAP

To configure TCAP layer in the SS7 stack:

1. Open a Signaling Manager GUI.
2. Choose the **Tools** menu and select **Configuration Mode > Initial** in Expert mode.
3. Go to **Signaling System**, select **TCAP**.
4. Check that the recommended values are set for TCAP:

Set **Max Number Of Subsystems** to 5.

Three subsystems are currently supported in MTAS and two are used as reserve, that is, this parameter is set to 5.

The **Max Number of TC users per Subsystem** depends the platform size. For a platform with five Payloads, set **Max Number Of TC-users per Subsystem** to 10.

There are five TC users per SSN since there is one TC user per SSN per Payload. There are five connections, since each TC user connects to each BE, and there is one BE per Payload. There are five BEs since there is one BE per Payload, and five in reserve. The calculation is as follows for node with five Payloads: $5 \times 5 / 5 + 5 = 10$. Follow the same logic when calculating this value for other configurations.

Example

For node with 26 Payloads, set **Max Number of TC users per Subsystem** to 32.
 26 TC users per SSN, since there is one TC user per SSN per Payload.
 26 Connections, since each TC user connects to each BE, and there is one BE per Payload.
 26 BEs since there is one BE per Payload.
 Five in reserve
 $26 \times 26 / 26 + 5 = 31$ and round up to 32 for memory alignment.

The **Max Number of Dialogues per Subsystem** depends on the use of CAP and MAP. The following examples for how to calculate this value are based on engineered call capacity per Payload and average call setup time + 25% reserve or engineered call capacity per Payload and average call length + 25% reserve. CAP or MAP signaling is for some use cases only done during call setup but can, for example, for IN/CAMEL prepaid scenario, be done during the complete call and then same TCAP dialogue ID is kept until the call is ended. The operator needs to configure the number of dialogues based on the scenario is used by their system.

Set **Max Number Of Dialogues per Subsystem** to n.

The number n depends on the scenario used by the system and is to be calculated in a similar way as in the following examples.

In the created TCAP Subsystem, set **Max Number Of Dialogues** based on engineered call capacity per TP and the average call setup time + 25% reserve as follows:

- TCAP Subsystem for SCC AS SCF application, $SSN=mtasCsiScfSubsystemNumber$ the call setup time is the time between incoming CAP IDP request and outgoing CAP CON response, for example:
 $150calls/s * 15ms + 25\% = 3$ or $150calls/s * 30ms + 25\% = 6$
- TCAP Subsystem for SCC AS GMSC application, $SSN=mtasCsiMapGmscSubsystemNumber$ the call setup time is the time to get a response on MAP SRI request from SCC AS to HLR, for example: $150calls/s * 0,5s + 25\% = 94$ or $150calls/s * 2s + 25\% = 375$
- TCAP Subsystem for MMTel Telephony AS and IN/CAMEL prepaid scenario, $SSN=mtasCsiSsfSubsystemNumber$, the average call length used here is 195 s, 60 calls/s assumes to give 60% CPU load for CAMEL Prepaid, for example $60calls/s * 195s + 25\% = 14625$
- TCAP Subsystem for MMTel Telephony AS and IN/CAMEL VPN scenario, $SSN=mtasCsiSsfSubsystemNumber$, the average call setup used here is 5 s, 60 calls/s assumes to give 60% CPU load for CAMEL VPN, for example $60calls/s * 5s + 25\% = 375$
- TCAP Subsystem for MMTel Telephony AS and IN/CAMEL Play Announcement (PA) scenario, $SSN=mtasCsiSsfSubsystemNumber$, the average call setup used here is 10 s, a 10-s long announcement is assumed, 60 calls/s assumes to give 60% CPU load for CAMEL PA, for example, $60calls/s * 10s + 25\% = 750$

Set **Max Number of Concurrent Operations per Dialogue** to 1000.

Set **Timer Dialogue** to 0 meaning that this timer is not used.

5. Go to **TCAP Subsystems**.
6. Right-click **TCAP Subsystems**, select **Add**.

Create a TCAP Subsystem for each application to be configured.

For example, if SCC AS CAP and MAP and MMTel Telephony AS CAP is to be used in the system, then three TCAP subsystems must be added with the same configured values in the CMs as mentioned in SCCP Layer, Page 19.

7. Validate the configuration with **Edit** menu, select **Validate**.

6.3 CAP and MAP Configuration

This section describes how to configure CAP/INAP and ETSI MAP in the SS7 stack.



6.3.1 Configure INAP

This section describes how to add INAP and connect it to a TCAP subsystem, to bind a CSI subsystem.

To add INAP and connect it to a TCAP subsystem:

1. Open a Signaling Manager GUI.
2. Choose the **Tools** menu and select **Configuration Mode > Initial** in Expert mode.
3. Go to **Signaling System**, select **INAP**.
4. Check that the recommended values are set for INAP:

Set **Max Subsystems** to 3.

Two INAP/CAP applications are currently supported in MTAS and one is added in reserve.

Set **Max Dialogues** in the same way as described in Section 6.2 on page 20 for **Max Number of Dialogues**.

Set **Unbind At Broken Connection** to No, to be able to resume CAP traffic after restart and sudden crash of the SS7DistributorProcess. This configuration must be changed to Yes before running upgrade and changed back to No after upgrade.

5. Right-click **INAP > INAP > INAP Subsystem** and select **Add**. Set the same subsystems applicable for INAP, as set in SCCP Layer, Page 19 and if both INAP and CAP in SCC AS, that is, the SCF role and INAP/CAP in MMTel Telephony AS, that is, the SSF role are used in the system, then two INAP subsystems must be added.
6. Validate the configuration with **Edit** menu and select **Validate**.

6.3.2 Configure ETSI MAP

This section describes how to add ETSI MAP subsystem and connect it to a TCAP subsystem, to bind a CSI subsystem.

To add ETSI MAP and connect it to a TCAP subsystem:

1. Open a Signaling Manager GUI.
2. Choose the **Tools** menu and select **Configuration Mode > Initial** in Expert mode.
3. Go to **Signaling System**, select **ETSI MAP**.
4. Check that the recommended values are set for **ETSI MAP**.



Set **Max Subsystems** to 2.

One ETSI MAP application is supported in MTAS and one is used as reserve.

Set the **Max Dialogues** in the same way as described in Section 6.2 on page 20 for **Max Number of Dialogues**.

Set **Unbind At Broken Connection** to Yes, to be able to resume MAP traffic after restart, upgrade, and sudden crash of the SS7MapDistributorProcess.

5. Right-click **ETSI MAP > ETSIMAP > ETSIMAP Subsystems** and select **Add**. Set the same Subsystems applicable for MAP as set in SCCP Layer, Page 19. Only MAP in SCC AS is supported in MTAS, so only one can be configured.
6. Validate the configuration with **Edit** menu and select **Validate**.

6.4 Configure SCTPs, PMTU, and IPv6 PMTU

MTU value is configurable, so if there is a change in MTU value in `/cluster/etc/cluster.conf` from default 1500 to another value, then in SS7 stack PMTU and IPv6 PMTU should be equal 0. These parameters get the values from vMTAS interfaces.

To configure MTU in the SS7 stack:

1. Open the Signaling Manager GUI.
2. Choose the **Tools** menu and select **Configuration Mode > Initial in Expert mode**.
3. Go to **Signaling System**, select **SCTPs**
4. Select **SCTP End Point Profile#N** (N=0,1...)
5. Set PMTU and IPv6 PMTU value equal to 0



7 Activate the Configuration Changes

To activate the configuration changes:

1. In Signaling Manager GUI, go to **Tools** and select **Process view**.
2. Select **Configure > Initial configuration** and click **OK**.
3. Select **Restart the stack**.

Wait until active indication is shown in the bottom left corner of the Signaling Manger.

4. Make a normal backup to back up the updated cnf files.