

Configuring SS7, SCTP

OPERATING INSTRUCTION

Copyright

© Ericsson AB 2006-2007, 2010-2011, 2013, 2015-2016. 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.



Contents

1	Overview	1
1.1	Description	1
1.2	Prerequisites	1
2	Procedure	3
2.1	Creating SCTP Layer	3
2.2	Configuring SCTP	3
3	Recommended SS7 Parameters	7
3.1	SCTP Managed Object	7
3.2	SCTP End Point Profile Managed Object	8
3.3	Estimations of Userdata Transmit Buffer Size and Threshold of Userdata Transmit Buffer Size	9
	Glossary	11
	Reference List	11





1 Overview

1.1 Description

This instruction describes, using an example, how to configure Stream Control Transmission Protocol (SCTP). The procedure in this example shows a complete configuration with usable values. For a specific customer configuration, other relevant values may be used.

1.2 Prerequisites

1.2.1 Documents

Not applicable

1.2.2 Tools

TelORB Manager and Signaling Manager.

1.2.3 Conditions

- The IP addresses must be known. The Local IP Address is the assigned both Evolved Virtual IP (eVIP) and IP address for the SCTP FE.





2 Procedure

This procedure describes how to create an Sctp Front End and its Local IP Address table or Sctp Front End with Distributed End Point property.

2.1 Creating Sctp Layer

In the **Signaling Manager** perform the following steps:

1. Expand **Signaling System** to view the underlying structure, if it is not already expanded.
2. Add element on **SCTPs**. An instance of Sctp with **Instance ID 0** will be added. The value of the **Instance ID** is automatically calculated and set depending on the previously added Front End instances. It is the instance ID of the previous Front End instance plus one. See Figure 1.

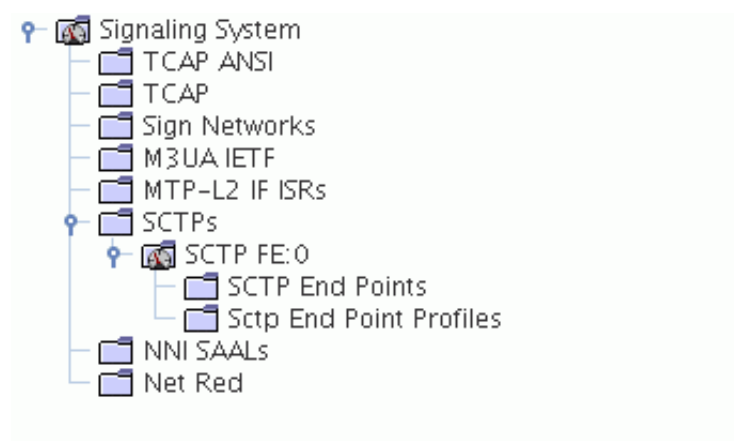


Figure 1 Added an Instance of Sctp

No Sctp End Point instance is added by default.

2.2 Configuring Sctp

2.2.1 Sctp Properties

All properties are using default values. If some properties are not visible in the Sctp property sheet, it is due to that **Expert mode** has not been selected in **Tools** menu.

Note: Local and remote IP addresses should be set in IPv6 format in case of IPv6 configuration.



2.2.2 Creating Local IP Address Table

In order to create Local IP Address Table/SCTP End Point element you may need to:

1. Add an element on **SCTP End Points**. An instance of IP Address Table , called **IP Address Table #1**, is added. See Figure 2.

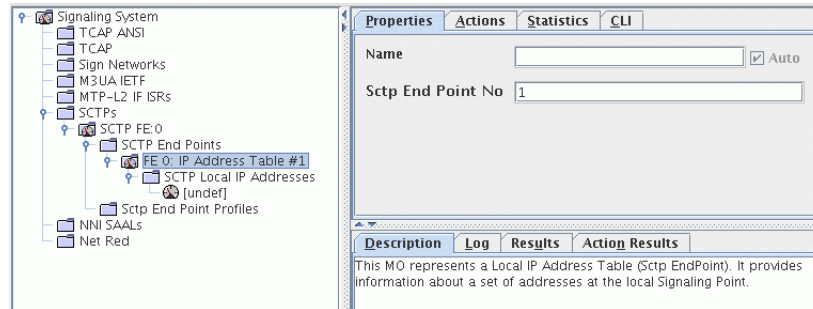


Figure 2 Added an Instance of SCTP Local IP Address Table

Note: By default an instance of an SCTP Local IP address, called **[undef]** is added in the **SCTP Local IP Addresses** element. In order to make this IP address valid, its **Address** property must be set. The **Port Number** property, that is visible in **Expert Mode** only, is not exported to the SCTP protocol layer when configuring pure SCTP (Signaling Manager configuration parameter **imc.names** set to "**signalingssystem,sctp**").

Note: Value of **Port Number** property of Local address table is needed only if this End Point is used in **M3UA**. If **M3UA** isn't used, then **Port Number** can be left with default value

2. Set the **Address** property of the added SCTP Local IP Address, **[undef]**. The IP Address element will be updated with its set IP address. See Figure 3

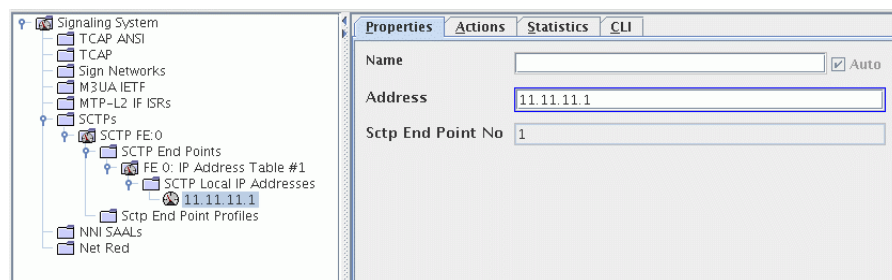


Figure 3 Address Field Which is Set with a Valid IP Address

2.2.3 Creating More Local IP Address

One Local IP Address was added during the steps in “Creating Local IP Address Table” in Section 2.2.2 on page 4. In order to add more Local IP Address for a certain Local IP Address Table, for instance **IP Address Table #1**, perform the following steps:



1. Add element on **SCTP Local IP Addresses**. An instance of SCTP Local IP Address, called **[undef]** is added in the **SCTP Local IP Addresses** element.
2. Set the **Address** property of the added SCTP Local IP Address, **[undef]**. The Local IP Address element will be updated with the set IP address, see Figure 3.

Note: You can also create a Local IP Address by making a copy of one already created instance. Its **Address** property must be updated. Duplicate IP Addresses are not allowed.

2.2.4 Creating More Sctp End Points

1. Select the previously added **FE 0: IP Address Table #1** and press the insert key or right click and select add. A second instance called **FE 0: IP Address Table #2** is added.
2. Set the **Address** property of the added SCTP Local IP Address. The Local IP Address element will be updated with the set IP address.

Note: New End Points creation is necessary only if they are used in M3UA

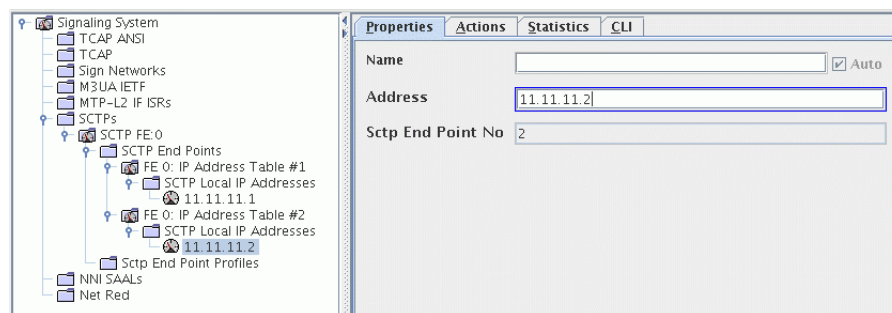


Figure 4 Added a second SCTP End Point.

2.2.5 Validate SCTP

In order to validate, you select **Validate** from the **Edit** menu. The result will be displayed in the Results field below the Property sheet. If the configuration is not valid the incorrect properties will be listed in different lines. By Selecting a line, Signaling Manager will prompt to the location to edit the property with proper values to make the configuration valid.





3 Recommended SS7 Parameters

This section contains information about specific SS7 parameters or options. When performing a complete configuration procedure or using a template configuration, Signaling Manager provides default values. Most of these values will work for an SS7 stack in a running network and are not described specifically here. In some case though, parameters will have to be modified.

3.1 SCTP Managed Object

Table 1 Properties of the SCTP Managed Object

Property Name	Recommended value	Comments
No of Associations	512	Defines the maximum number of associations to be handled by a SCTP instance in this configuration.
Size of outgoing IP buffer	65 535	Sets the maximum number of bytes which SCTP can write to IP socket. The parameter is validated for compliance to possible range. If the outgoing SCTP packet is bigger than this buffer size the packet will be lost.
Size of incoming IP buffer	0	Sets the maximum number of bytes which is used by IP layer when receive packets from the network. If the incoming packet is bigger than this parameter, IP layer will not be able to receive this packet and it will be rejected. If 0 is specified, the operating system default value is used. The max value is OS specific.
CRC Calculation Activated	Yes	Defines whether CRC calculation is active or not. No - value 0 of CRC-Calculation Status Yes - value 1 of CRC-Calculation Status
ICMP Activated	Yes	Defines whether ICMP is active or not. No - value 0 [Bit 0 (activation)] Yes - value 1 [Bit 0 (activation)]



Table 1 Properties of the SCTP Managed Object

Property Name	Recommended value	Comments
ULM Buffer Size	2 000 000	Defines the limitation for buffer that is assigned for the upper layer messages. SCTP will not save confirmations and indications if the buffer is overflowed.
Multihome Robustness	Enable	Defines whether Multihome Robustness is disabled or enable. Disable - value 0 of Multi-home Robustness Enable - value 1 of Multi-home Robustness

3.2 SCTP End Point Profile Managed Object

Table 2 Properties of the SCTP End Point Profile Managed Object

Property Name	Recommended value	Comments
Min RTO	200	The minimum value that RTO is allowed to have. If when computing the RTO the result is less than the minimum, RTO is rounded up to the value of this parameter.
Max RTO	1000	The maximum value that RTO is allowed to have. If when computing RTO the result is greater than the maximum, RTO shall be rounded down to Max RTO .
Init RTO	400	This is the initial value that the RTO takes, prior to the first RTT measure.
Bundling Activated	Enable	Defines whether Bundling is enable or disable. Disable - value 0 of Bundling Status Enable - value 1 of Bundling Status
PMTU	1480 (without eVIP) 1452 (with eVIP)	Path Maximum Transmission Unit, the maximum number of bytes of an IP datagram that can be transferred in a single unit over a specific path in an IPv4 network. If an IP datagram exceeds the PMTU , normally it will be either fragmented or dropped by IP layer.
IPv6 PMTU	1480 (without eVIP) 1452 (with eVIP)	Defines PMTU on IPv6 paths.



Table 2 Properties of the SCTP End Point Profile Managed Object

Property Name	Recommended value	Comments
Block CrossPaths Flag	do not block cross-paths , see Remark 1	Defines if SCTP should block cross-paths for traffic do not block cross-paths - matches value 0 block cross-paths - matches value 1
DSCP	64	This value represents the "Differentiated Service Code Point" related to the Quality of Service. Only values 0 - 63 will be used, value 64 means that SCTP should take this parameter from user requests or, if it is absent in such requests, use the value 0.

Notes:

1. Parameter **Block Cross-paths Flag** must be **True** if we have Multihoming association with IP addresses from different networks

3.3 Estimations of Userdata Transmit Buffer Size and Threshold of Userdata Transmit Buffer Size

For each association in SCTP there is a special buffer for transmitting, named as the **M** buffer, see Remark. User messages that are completely ready for transfer through IP network are stored in this buffer until SCTP is not be able to pass these messages to IP network. The main purpose of this buffer is to smoothen unexpected events like disturbances in IP network and possible difference in performance of SCTP and SCTP user. In normal situation (no problems with IP network and performance of SCTP and SCTP user are approximately equal) this buffer should be almost empty. The value for this buffer is defined with the help of the **Userdata Transmit Buffer Size** parameter from SCTP configuration. Based on this information and taking into account possible events within TSP cluster we can estimate the necessary value for this buffer. We suggest to use the following algorithm for the estimation of the **Userdata Transmit Buffer Size** value:

- To describe the algorithm the following definitions are used: **S** - TCAP user message size (in bytes); **I** – traffic intensity on one association (in messages / seconds); **Time_o** – time of IP layer outage (during this time SCTP shouldn't take a decision about "Down" state of association); **N** – N threshold size (in bytes); **M** – M buffer size (in bytes); **Header** - size of all headers that will be added to User's message by SS7 layers or Diameter Base protocol.
- The following parameters should be defined before further estimations: **S**, **I**. Product of **S + Header** and **I** results in the value that can be called as expected traffic flow through one association. If SCTP front end is shared between SIGTRAN and Diameter then the largest of expected traffic flow on SCTP association should be chosen for buffer estimation.



- The possible time of the outage on IP layer during an unplanned or planned reconfiguration within the cluster (like reload or disable of processor) should be checked according to "TSP System Characteristics" (3/15502-ANA90105/1 Uen) document. Because of quite similar nature of SCTP and TCP we suggest to choose the maximum time of outage for TCP protocol. For example, in our estimations we take **Time_o** equal to 3 seconds.
- The **N** threshold size should be greater or equal to the product of the expected traffic flow on the one association and the time of the outage on IP layer. The following condition should be fulfilled: $I \times (S + \text{Header}) \times \text{Time}_o \leq N$. All estimations performed for the **N** threshold first and only after that the **M** buffer value is calculated, this condition will prevent from receiving unwanted "SCTP congestion" alarms during the reload of processors.
- **M** buffer size should be specified taking into account that the recommended **N** threshold equals to 75% of the **M** buffer, that is $M = 4 / 3 \times N$.

The described algorithm is illustrated in the examples below.

Note: In spite of the separate buffer for each SCTP association existing, the value that can be configured with the help of Signaling Manager is specified for the whole SCTP front end and will be applied for all associations that belong to the exact SCTP front end.

The following values are used for estimations:

S = 150 bytes (TCAP user message size)

Additional header will be added to message from SS7 stack layers (TCAP, SCCP, M3UA) ~128 bytes + 32 bytes from SCTP layer.

I = 5000 messages per seconds for one SCTP association. This message size corresponds to ~12 Mbps throughput.

Time_o = 3 seconds

$(5000 \times (150 + 128 + 32) \times 3) = 4650000 \text{ bytes} = 4.4 \text{ MB}$

In this case **N** should be greater or equal to 4650000

So, we got **N** buffer size - 4.4 MB and should calculate the size of **M** buffer as 4/3 of **N** threshold

M buffer size in this case will be equal to $(4650000 \times 4 / 3) = 6200000 \text{ bytes} = 5.9 \text{ MB}$

Example 1 M buffer size estimation for SIGTRAN traffic



Glossary

SCTP

Stream Control Transmission Protocol

VIP

Virtual IP address

M3UA

MTPL3 User Adaptation layer

SS7

Signaling System Number 7

FE

Front End