

SS7 CAF

Operating Manual

OPERATING MANUAL

Copyright

© Ericsson AB 2012 - 2017. 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 SS7 CAF Trademark Information.

Abstract

This guide is a walkthrough of Operation and Maintenance of the Ericsson SS7 with distributed architecture in CBA environment.

Product Support

Tieto

Customer Support Center

Phone: +46104817400 (08:00 – 17:00 CET)

Fax: +46104817201

E-mail: signalingsupport@tieto.com



Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 1 |
| 1.1 | Typographic Conventions | 1 |
| 2 | General | 3 |
| 2.1 | SS7 CAF in CBA Environment | 3 |
| 2.2 | SS7 Stack System Overview | 3 |
| 2.3 | Control of SS7 CAF Component | 5 |
| 2.4 | Control of Processes within the SS7 CAF Component | 5 |
| 2.5 | SS7 CAF Packages | 10 |
| 3 | Backup and Restore operations | 15 |
| 3.1 | SS7 CAF and BRF | 15 |
| 4 | SS7 CAF and Scaling Operations | 17 |
| 4.1 | Scale-Out | 17 |
| 4.2 | Scale-In | 17 |
| 4.3 | Error Handling | 17 |
| 5 | SS7 CAF Configuration Interfaces | 19 |
| 5.1 | Signaling Manager | 19 |
| 6 | Configuring SS7 CAF | 23 |
| 6.1 | Defining New SS7 CAF Configuration | 23 |
| 6.2 | Multiple SCTP Processes per Blade | 26 |
| 6.3 | SCTP Only stack | 27 |
| 6.4 | SS7 CAF Configuration for Scaling Operations | 28 |
| 6.5 | Setup Parameters | 28 |
| 6.6 | ECM Active Host | 29 |
| 6.7 | Usage of IPv6 | 31 |
| 6.8 | CP trace and logging facilities | 31 |
| 6.9 | ECM logging | 31 |
| 6.10 | SCTP Distributed End Points | 32 |
| 6.11 | eVIP Address as Common Parts Manager Address | 34 |
| 6.12 | LDE MIP Address as Common Parts Manager Address | 36 |
| 6.13 | NTF Alarms Configuration | 37 |



| | | |
|-----------|---|-----------|
| 6.14 | General Configuration Recommendations | 39 |
| 6.15 | Save SS7 CAF Configuration | 42 |
| 6.16 | Generate (Export) SS7 CAF Configuration Files | 43 |
| 6.17 | Setting parameters for large eVIP configuration | 43 |
| 7 | SS7 CAF Performance Management | 45 |
| 8 | Network Examples | 47 |
| 9 | Software Development Kit | 49 |
| 9.1 | SDK Installation | 49 |
| 10 | SS7 CAF Troubleshooting | 51 |
| | Reference List | 53 |



1 Introduction

This guide is a walkthrough of Operation and Maintenance of the Ericsson SS7 with distributed architecture in CBA environment.

1.1 Typographic Conventions

Commands to type in console or terminal, file and folder names are written in the following style: `rpm -qa | grep EAB`

Output of commands is written in the following style: `No files are found`

Variables that needs to be changed with corresponding value are written in the following style: `<Package name>`

File contents or code snippets are written in the following style:
`MSGINTERACT = Sctp01, SS7_BASE`





2 General

2.1 SS7 CAF in CBA Environment

SS7 CAF is an SA-aware CBA application component that supports the following SAF services:

| | |
|-------------|---|
| SMF: | SS7 CAF packages are provided as CoreMW RPMs and campaigns |
| AMF: | SS7 CAF component availability is controlled via AMF service |
| NTF: | SS7 CAF provides Fault Management model to CoreMW and COM/COM SA |
| PM: | SS7 CAF provides Performance Management model to CoreMW, see Section 7 on page 45 |

SS7 CAF configuration is stored in LDE PSO storage as files and is available on PLs via /opt/sign/etc link.

SS7 CAF processes can not start and restart without LDE PSO storage available because they require configuration files for stating up.

2.2 SS7 Stack System Overview

Page 4 shows the Ericsson Signaling system in an HD environment system. Each box within the figure is a separate module. Several modules are linked together into processes with a certain function in the HD system.

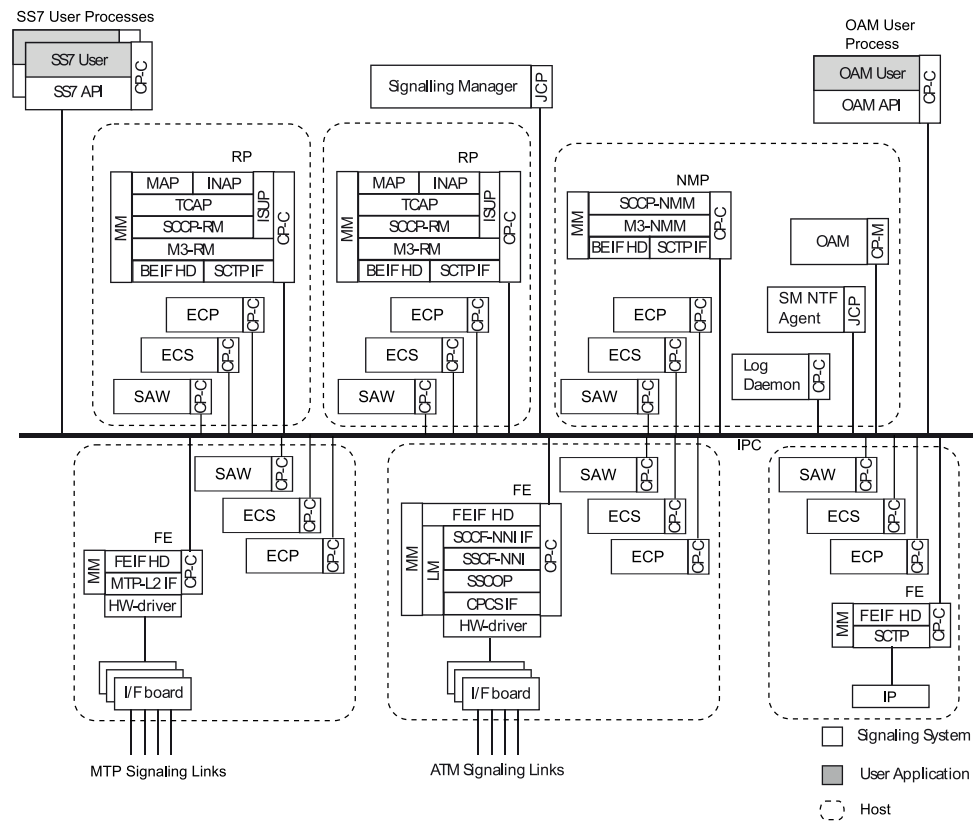


Figure 1 Example of a SS7 system



The processes included in an HD system are:

| | |
|-----------------------------------|---|
| RP process: | Handles SS7–user traffic |
| NMP process: | Handles network management |
| FE Process: | Handles SCTP IP traffic via SCTP FE |
| OAM Process: | Serves as the interface for management applications and also supervises different processes within a SS7 system |
| LOG DAEMON (LOGD) Process: | Provides logging of system information to log files |
| SAW process: | Acts together with the SS7 processes as an SAF AMF specified component, it can be referred as an AMF proxy towards SS7 processes. SAW handles start and stop of the SS7 processes |
| ECP process: | Supervises the execution of SS7 processes. It starts all SS7 processes and restarts them if necessary |
| ECS process: | Supervises the execution of ECP process |
| SM process: | Is used for configuration and operation of the SS7 Ericsson Signaling stack |
| SM NTF Agent process: | Maps SS7 alarms/notifications according to the SAF NTF specification |

2.3 Control of SS7 CAF Component

SS7 CAF is installed as a CBA component on a cluster and is controlled by AMF. The AMF modeling of SS7 CAF consists of one type of SU executing on each node where SS7 processes are present. The SU includes only one component.

To check SS7 CAF component and service unit status see Reference [14].

For more information on how to operate on nodes, SS7 CAF component, SS7 CAF service units refer to CoreMW documentation.

Note: The AMF controlled component in SS7 CAF will spawn several internal SS7 processes that are configured and supervised using the methods provided by SS7, see Section 2.4 on page 5 for details. Different SS7 CAF service units may have a different set of SS7 processes running.

2.4 Control of Processes within the SS7 CAF Component

The internal Process Management function within SS7 subsystem is called Execution Control. EC is started automatically when the SS7 CAF component is



unlocked. EC starts, supervises and stops processes in different use cases, for example:

- Initial start of the SS7 subsystem
- Recovery after failure
- Add process
- Remove process
- Termination of the SS7 subsystem
- Control of the SS7 SM NTF Agent

2.4.1 Process Arguments

Using the example configuration templates provided in the Signalling Manager package there is no need to change the process arguments described in this chapter, but in some cases it could be necessary to adjust the SS7 stack process arguments for user needs. This chapter describes the different arguments for the SS7 stack processes. For ECM arguments please refer to Reference [4]. For arguments to the SS7 AMF Wrapper and the SM NTF Agent, please refer to Reference [10] and Reference [9].

2.4.1.1 RP and NMP arguments

RP or NMP is started by ECM using the “be” binary. Available arguments are:

Table 1 Arguments for “be” binary.

| Argument | Description | Default |
|----------|--|---------------|
| -t | Trace on. | FALSE |
| -v | Show the versions of the software within this binary. | |
| -l | CP Manager location, use when process serves as CP Client. | Unspecified |
| -i | Instance number for this process. | 0 |
| -e | maxEntries, only applicable if not in cp.cnf. | 3000 |
| -u | userId of CP Manager. | CP_MANAGER_ID |
| -m | isManager, use when process serves as CP Manager. | FALSE |
| -s | isStandAlone, use when process serves as CP Stand Alone. | FALSE |



| | | |
|----|---|---|
| -r | restartCounter, only applicable for IET TCAP and SCCP. Ignored otherwise. | 255 |
| -c | Configuration file name for IMM. | imm.cnf |
| -a | Number of seconds to wait, only applicable if the process serves as CP Client. | 3 |
| -o | Number of times to try initiating CP, only applicable if the process serves as CP Client. | Infinitely |
| -d | Message Port Owner, default value depends on which module runs in the process. | BE IF HD: SS7_BASE_ID FE IF HD: EINSS7_FEIFHD_ID OAM: CP_MANAGER_ID |
| -b | Specify the type of BE: Monolithic - 1 NMM - 2 RM - 3 | |
| -w | ConnTimeWait. Used to activate asynchronous connection feature and defines time to wait in MsgConn or any functions of this family. | 5 |

2.4.1.2

OAM arguments

OAM is started by ECM using the “oam” binary. Available arguments are:

Table 2 Arguments for the “oam” binary.

| Argument | Description | Default |
|----------|--|---------------|
| -t | Trace on. | FALSE |
| -v | Show the versions of the software within this binary. | |
| -l | CP Manager location, use when process serves as CP Client. | Unspecified |
| -i | Instance number for this process. | 0 |
| -e | maxEntries, only applicable if not in cp.cnf. | 3000 |
| -u | userId of CP Manager. | CP_MANAGER_ID |



| | | |
|----|---|---|
| -m | isManager, use when process serves as CP Manager. | FALSE |
| -s | isStandAlone, use when process serves as CP Stand Alone. | FALSE |
| -r | restartCounter, only applicable for IET TCAP and SCCP. Ignored otherwise. | 255 |
| -c | Configuration file name for OAM. | oam.cnf |
| -a | Number of seconds to wait, only applicable if the process serves as CP Client. | 3 |
| -o | Number of times to try initiating CP, only applicable if the process serves as CP Client. | Infinitely |
| -d | Message Port Owner, default value depends on which module runs in the process. | BE IF HD: SS7_BASE_ID FE IF HD: EINSS7_FEIFHD_ID OAM: CP_MANAGER_ID |
| -w | ConnTimeWait. Used to activate asynchronous connection feature and defines time to wait in MsgConn or any functions of this family. | 5 |

2.4.1.3

FEs arguments

Available arguments for the different “fe” binaries are:

Table 3 Arguments for the different “fe” binaries.

| Argument | Description | Default |
|----------|--|---------------|
| -t | Trace on. | FALSE |
| -v | Show the versions of the software within this binary. | |
| -l | CP Manager location, use when process serves as CP Client. | Unspecified |
| -i | Instance number for this process. | 0 |
| -e | maxEntries, only applicable if not in cp.cnf. | 3000 |
| -u | userId of CP Manager. | CP_MANAGER_ID |



| | | |
|----|---|---|
| -m | isManager, use when process serves as CP Manager. | FALSE |
| -s | isStandAlone, use when process serves as CP Stand Alone. | FALSE |
| -r | restartCounter, only applicable for IET TCAP and SCCP. Ignored otherwise. | 255 |
| -c | Configuration file name for IMM. | imm.cnf |
| -a | Number of seconds to wait, only applicable if the process serves as CP Client. | 3 |
| -o | Number of times to try initiating CP, only applicable if the process serves as CP Client. | Infinitely |
| -d | Message Port Owner, default value depends on which module runs in the process. | BE IF HD: SS7_BASE_ID FE IF HD: EINSS7_FEIFHD_ID OAM: CP_MANAGER_ID |
| -w | ConnTimeWait. Used to activate asynchronous connection feature and defines time to wait in MsgConn or any functions of this family. | 5 |

2.4.2 Process Handling in Signaling Manager

SS7 processes (RP, FE) specified in the EC configuration can be added and removed by the Signaling Manager in runtime, see Reference [5]

Add and remove process

By using the Signaling Manager, processes can be added and removed

OAM, NMP, SAW, NTF-agent and Log daemon processes can not be added or removed

Restart process

SS7 processes can be restarted with Signaling Manager command

Set active ECM

A slave host can be switched to be master by activating the ECM running on that machine. The OAM and NMP processes will be moved to the host where the new active EC manager process executes. Any processes with followActive enabled will also be moved



Restart stack The whole SS7 system including supervised user applications can be restarted

See Reference [5], Signaling Manager User Guide for further information.

2.5 SS7 CAF Packages

The SS7 CAF software consists of:

- SDP campaigns, CSM fragment, plugin and scripts delivered in the deployment template package. Campaigns and scripts are used to install, upgrade and remove SS7 CAF software. CSM fragment, plugin and scripts are used to install and upgrade SS7 CAF using CSM way.
- RPM packages in the runtime package. These packages are used on the CBA cluster
- RPM package in the SDK package.

Each RPM package creates a directory `/opt/sign/EABss70<number>` on each cluster node where the package is installed.

2.5.1 RPM Packages in the Runtime Package

Table 4 Software bundle RPM packages included in the delivery

| Package Name | Target cluster node(s) | (O) Optional/ (M) Mandatory | Description | Comments |
|--------------------------|------------------------------|-----------------------------|--|----------|
| EABss7038: SS7 NTF Agent | Nodes where SS7 CAF operates | M | SM NTF Agent interface towards NTF in middleware | |



| | | | | |
|----------------------------------|------------------------------|---|--|---|
| EABss7039: SS7 Preinstall | Nodes where SS7 CAF operates | M | AMF startup /termination scripts for the SS7 CAF. The startup script creates soft-links to the cluster persistent file system to allow the SS7 CAF software to locate the SS7 CAF configuration and write log files. SS7 CAF C API libraries | |
| EABss7041: SS7 Alarm Model | Service Controllers | M | Alarm model | |
| EABss7044: SS7 AMF Wrapper | Nodes where SS7 CAF operates | M | saw binary. Process saw responsible for supervising SS7CAF and reporting its status to AMF in middleware. | |
| EABss7049: SS7 Common Package | Nodes where SS7 CAF operates | M | ecp, ecs, logd, oam, shoff, showver, tv and tvtool binaries | |
| EABss7050: SS7 Signaling Manager | Nodes where SS7 CAF operates | M | Signaling Manager software and documentati on. SS7 CAF configuration templates. SS7CAF JAVA API libraries | |
| | Service Controllers | M | | The package on SCs delivers scaling support in SS7 CAF and also allows Users to use SM on SCs for Configuratiuon Managment. . |



| | | | | |
|-------------------------------------|--|---|---|---|
| EABss7052: SS7 FE SCTP | Nodes where SS7 CAF operates | O | fe_sctp binary. PM model for FE. | The package can be excluded from installation if SCTP is not used If this package is used, then LKSCTP must not be used at the same time |
| EABss7053: SS7 BE IETF | Nodes where SS7 CAF operates | O | be binary which is used both as RP and NMP process. PM model for BE. | The package can be excluded from installation if RP and NMP are not used (for example in SCTP only configuration) |
| EABss7069: Java Runtime Environment | Nodes where SS7 CAF operates | M | Java Runtime Environment (JRE) for the SS7 CAF java based software | |
| | Service Controllers | M | | The package on SCs needed for scaling support in SS7 CAF and also allows Users to use SM on SCs for Configuratiuon Managmen |
| EABss7072: SCTPd | All nodes where eVIP LBE to handle SCTP traffic are deployed | O | SCTP Distribut or | |
| EABss7077: Scaling | Service Controllers | O | Scaling scripts | The package can be excluded from installation if scaling is not used |
| EABss7078: BISU | Service Controllers | M | Plugin for BISU | |

Note: The optional packages can be excluded or included by modifying the SS7 CAF Installation Campaign (in case of campaign installation) or the CSM system fragment (in case of CSM installation)



2.5.2 Campaigns in Deployment Template

Table 5 Campaign SDP included in the delivery

| Name | Description |
|---|---|
| ERIC-SS7CAF_I-TEMPLATE-CXP9020969: SS7 Install Campaign | Default install campaign for 2 SCs + 2 PLs installation |
| ERIC-SS7CAF_R-TEMPLATE-CXP9020969 : SS7 Remove Campaign | Remove campaign |
| ERIC-SS7CAF_U-TEMPLATE-CXP9020969: SS7 Upgrade Campaign | Upgrade (BFU) campaign |

2.5.3 CSM Fragment in Deployment Template

CSM fragment in the deployment package is used both for SS7 CAF installation and upgrade. If the system has been installed or upgraded using CSM, software removal is not supported.

2.5.4 RPM in SDK

The following RPM package exists for the SS7 software. This package are used when using SS7 applications in a development environment.

— EABss7051: SS7 Boot Package

2.5.5 vDicos IIDP package

The vDicos APIs are packed in tarball named **ERIC-SS7CAF_EABss7073-CXP9020969-*<revision>*.tgz**. Details on how to use the vDicos APIs can be found in Application Programmer's Guide for SS7 CAF.

Note: For information on how to prepare and install vDicos with vDicos applications see vDicos installation instruction.





3 Backup and Restore operations

SS7 CAF configuration is stored in `/opt/sign/etc` folder on nodes where SS7 CAF was installed. This folder is a target for backup and restore operations.

SS7 CAF logs are stored in `/opt/sign/log` folder on nodes where SS7 CAF was installed. This folder is not a target for any backup or restore operations.

It is possible to use the following functionality in CBA environment for backup and restore operations:

- BRF backup when BRF component is installed

3.1 SS7 CAF and BRF

Only SS7 CAF configuration files and SS7 Software are backed up/restored during a BRF System backup/restore.

Note: Only the configuration files in `/opt/sign/etc` are backed up as SS7 CAF configuration. If the SS7 CAF configuration is opened and edited in Signaling Manager but not yet saved to disk or activated, it will not be part of the backup. It is strongly recommended to finish SS7 CAF configuration and close Signaling Manager before any BRF backup or restore operation is executed to avoid inconsistency of SS7 CAF configuration data opened in Signaling Manager and the actual SS7 CAF configuration stored in BRF backup or data restored from BRF backup.

`/opt/sign/etc` is a link to cluster PSO configuration area which is part of BRF System backup and restore operations. This link recreated during each start of SS7 CAF component.

`/opt/sign/log` is a link to cluster PSO no-backup area which is not part of BRF System backup and restore operations. This link recreated during each start of SS7 CAF component.

All SS7 CAF software is installed to PSO software area which is part of BRF System backup and restore operations.





4 SS7 CAF and Scaling Operations

To allow SS7 CAF participation in Scaling Operations it shall be configured according to Section 6.4 on page 27.

SM CLI/GUI must be closed before start of Scaling Operations, manual updates of configuration during Scaling Operations are not allowed.

Note: In case SM is not closed then displayed configuration will be outdated. Export of the outdated configuration can lead to a faulty state of SS7 CAF.

EABss7077 installs C2 scaling plugin on Service Controllers, Signaling Manager and JRE required for scaling also installed on SCs by EABss7050 and EABss7069 respectively. In case SS7CAF should not participate in Scaling Operations then EABss7077 package should be excluded either from installation campaign using **Campaign_generator_without_DX.sh** or from CSM system model, see Reference [16] for details.

4.1 Scale-Out

During Scale-Out operation the following changes are applied to SS7 CAF configuration automatically:

- ECM configuration for Scaled-Out node(s) is cloned from configuration of ECM host with the lowest priority
- SCTP FE configuration for SCTP FE instance(s) for Scaled-Out node(s) is cloned from existing SCTP FE configuration

4.2 Scale-In

During Scale-In operation CAP sessions will be moved from the hosts which are affected by Scale-In. Traffic will be evenly distributed between all BEs which are not affected by Scale-In. Then the following changes are applied to SS7 CAF configuration automatically:

- ECM configuration for Scaled-In node(s) is removed from ECM configuration
- SCTP FE configuration for SCTP FE instance(s) for Scaled-In node(s) is removed

4.3 Error Handling

In case of unsuccessful scaling operation an error is reported to CoreMW. SS7CAF does not control CoreMW behavior in error cases.



Before performing scaling operation SS7 CAF validates configuration. If any errors are found then configuration will not be changed and the error is reported to CoreMW.



5 SS7 CAF Configuration Interfaces

SS7 CAF provides the following configuration interfaces:

- Signaling Manager. This is a common configuration interface for SS7 CAF which can be used in both GUI and CLI modes

5.1 Signaling Manager

Signaling Manager is a Java-based tool for the configuration and operation of Ericsson Signaling stacks including SS7 CAF. The tool can be used to create, modify and save SS7 CAF configuration, get SS7 CAF components status and to control it using actions.

Signaling Manager provides the following interfaces:

- Graphical User Interface. It is mostly used for manual interaction. This mode requires X-server to be available
- Command Line Interface. It is mostly used for issuing configuration changes in script files. CLI can be used when X-server is not available, for CLI usage details see Reference [6]
- Signaling Manager API. This interface can be used inside an application
- Java web applet

All Signaling Manager interfaces provide similar configuration capabilities.

The complete Signaling Manager user guide is available in Reference [5].

5.1.1 Signaling Manager Configuration File

Signaling Manager has its own configuration file allowing to configure Signaling Manager behavior.

After SS7CAF installation the configuration file is stored as **/opt/sign/etc/signmgr.cnf**.

The following template for the Signaling Manager configuration file exists:

- **/opt/sign/cnf_template/example_signmgr.cnf** to be used if COM NBI interfaces wasn't activated in SS7 CAF

Note: The SM NTF (SAF OAM) process which includes Signaling Manager API in SS7 CAF is also using **/opt/sign/etc/signmgr.cnf**. Make sure that SM NTF launch string in ECM configuration is changed accordingly before replacing or renaming **/opt/sign/etc/signmgr.cnf** file

5.1.2 Local Usage of Signaling Manager

The X-server should be installed on the same cluster host where Signaling Manager is going to be used in order to use SM GUI. For details on how to install X-server on a host see Reference [14].

5.1.3 Remote Usage of Singaling Manager

Signaling Manager can be used remotely in the following ways:

- as a Java applet, see chapter Section 5.1.4 on page 20
- without the applet, see Reference [5].

5.1.4 Signaling Manager as a Java Applet

This chapter provides information on how to setup Signaling Manager as a Java applet.

Note: To get a meaningful usage of this feature a web-server is required, how to install and configure ditto is not explained here.

If Signaling Manager is going to be used as an “ordinary” application as well as an applet it is possible to override parameters in **System Components/Signaling Manager** through command line parameters. This enables “applet-specific” settings to be passed via the HTML-file. Consider the following scenario; If Signaling Manager is used locally as an application, the settings for **Rio**, which is used for remote filesystems using FTP, should not be used. These **Rio** settings are however vital for the applet to function. By leaving the **Rio** settings blank in the configuration for **System Components/Signaling Manager** and editing the HTML-file to override these settings, Signaling Manager can both be run locally as an “ordinary” application and remotely as an applet.

Signaling Manager executed from an applet behaves similar as running it locally. It is started from a web-page, which means that a HTML-file needs to specify how to start it. An example HTML-file is bundled with this installation and located in **/opt/sign/etc/signmgr_applet.html**. All jar-files needed to run the Signaling Manager as an applet has been signed using certificate should be accepted the first time the applet has been started.

When running as an applet any settings can be overridden in the HTML-file which correspond to the command-line for the applet. Please notice that **<signmgr config file>** must be placed in the class path to make it possible for the applet to open it, or use the command line parameter **own.conf** to specify a path. The example HTML-file shows the usage of command line parameters, such as **own.conf**, and how to “link” to the jar-packages. For more command line parameters, see Reference [7].



The following lines has to be added to the `java.policy` file in order to give the Signaling Manager the necessary access rights:

```
// Give Signaling Manager some permissions

grant {

    permission java.net.SocketPermission "*", "connect, resolve";

    permission java.util.PropertyPermission "*", "read";

    permission java.util.PropertyPermission "*", "write";

};
```

This file is typically located in the “lib/security” directory of the JRE. Alternatively, place it in the `.java.policy` in the home directory to affect only a single user.

Note: Using Signaling Manager as an applet remote access to the filesystem where the SS7 configuration is located should be configured.

Using Signaling Manager as an applet, the web-page where it was executed must not be closed otherwise Signaling Manager will be closed as well.





6 Configuring SS7 CAF

SS7 CAF configuration is stored in `/opt/sign/etc` folder as collection of configuration files for particular SS7 modules.

For details on particular configuration file see corresponding Configuration File Descriptions (see References on page Reference List on page 53). Additional details about SS7 configuration and characteristics can be found in the Dimensioning Guide (Reference [1]), the Signaling Manager User Guide (Reference [5]).

6.1 Defining New SS7 CAF Configuration

Depending on initial preconditions there are might be a few options how to define new SS7 CAF configuration:

- Blank configuration. Creating new configuration from scratch
- Creating the configuration from provided template files
 - Note:** Recommended way because adapted to existing SS7CAF features.
- Migration of existing HD configuration
- Migration of existing non-HD configuration

6.1.1 Create a new SS7 CAF configuration

Follow these steps in Signaling Manager to create a new configuration. A new configuration can be created from scratch (a blank configuration or from a template). In both cases start by opening the New Configuration dialog: **File** -> **New**.

The dialog consists of three tabs, select:

- **Blank** to start the configuration from scratch
- **Template** to make an initial configuration based on the example templates, **example_single.cim**, **example_double.cim**, **example_double_sctp.cim**
 - **example_single.cim** is an example file containing SS7 CAF configuration with SCTP bearer and four SSN:s (one used by A41MAP and three for INAP, ETSI MAP and EMAP Local Service Center) deployed on a single host. It contains the same configuration for System Components as **singlehost.cim**
 - **example_double.cim** is an example file containing SS7 CAF configuration with SCTP bearer and four SSNs (one used by A41MAP and three for



INAP, ETSI MAP and EMAP Local Service Center) deployed on two hosts. It contains the same configuration for System Components as **doublehost.cim**

Note: This SS7 CAF configuration has Common Parts parameter **EVIP** is set to **ON** which enables and requires VIP functionality for SCTP distributed EP

- **example_double_sctp.cim** is a double host SS7 CAF configuration for SCTP Only stack. It contains one SCTP FE on each host and has no RP processes

Note: This SS7 CAF configuration has Common Parts parameter **EVIP** is set to **ON** which enables and requires VIP functionality for SCTP distributed EP

6.1.2 Import of an existing HD configuration

The following steps should be executed to import existing HD configuration.

Collect all the old configuration files in one directory, so that all files can be imported at the same time.

Open the existing cim-file (usually active.om.cim): **File -> Open**. When Signaling Manager has loaded the file, open the New Configuration dialog: **File -> New**.

The dialog consists of three tabs, select **Import CNF**. Select the configuration files for System Components (cp.cnf, oam.cnf, ecm.xml and possibly ECMclasses.xml) and set the **Select template** drop down menu to **Keep current model**.

If an expert mode is enabled, **Tools->Expert Mode**, the imported configuration can be seen in the System Components MO.

The ECM configuration must be extended with a process class and a process instance for the NTF Agent. Two new properties that controls the process restart alarm must also be set.

While in expert mode, expand the System Components MO and locate the ECM MO. Set the **Timer Process Alarm** and **Max Process Alarm** properties to their recommended values. Add a new Process Class and set the properties to the following values:

| | |
|----------------------|--------|
| ClassID | SAFOAM |
| Instance Type | AP |



Command

```
/opt/sign/EABss7069/jre/bin/java -ea
-Dinstall.root=/opt/sign/EABss7038/ -classpath
/opt/sign/EABss7038/lib/smntf.jar:/opt/
sign/EABss7050/lib/signmgr.jar:/opt/sig
n/EABss7050/lib/jcp.jar:/opt/sign/etc/
-Djava.library.path=/opt/sign/EABss7038/lib/
smntf.SmntfMain -handlers=signmgr.core.L
ogFileHandler -cp.localuser.uid=SAF_OAM
-cp.server.enabled=yes -own.conf=<signmgr
config file> -returntorunning.timeout=2000
-audit.log.quantity=0 -alarm.log.quantity=0
```

Supervise User ID

SAF_OAM

Add a process to one of the hosts with the following settings:

Instance ID 0

Follow Active ECM

Yes (Must be set after the process class has been set)

Process Class SAFOAM

Process Group Earliest possible group, that is the one with the lowest possible number.

Add a user and message interact entries for the AMF Wrapper. Expand the CP MO on the System Components MO.

1. Add one **User** for each host, set the **User ID** to **SAF_AMF**, set **Instance ID** to the same value as the ECM user has for the same host. Set the **Hosts** property to **<hostname>: <port>**. Port can for example be 6672.
2. Add one **User Pair** for each host, set both **First** and **Second User ID** to **SAF_AMF** and set the **Instance ID** in the same way as for the users. Set the **Msg Interact** property to 0n.

6.1.3 Import of an existing non-HD configuration

The following steps should be executed to import existing non-HD configuration.

Collect all the old configuration files in one directory, so that all files can be imported at the same time.

Open the New Configuration dialog: **File -> New**.

The dialog consists of three tabs, select **Import CNF**. To get a configuration for System Components together with import, select one of the following templates from the drop down menu, **Select template**, at the bottom of the dialog:

- **singlehost.cim** - Single Host template with only System Components configured, suitable for import of non-HD stack configurations.
- **doublehost.cim** - Double Host template with only System Components configured, suitable for import of non-HD stack configurations.

Select the configuration files from the old configuration.

Note: Do not include **cp.cnf** in the import, configuration for Common Parts is already prepared in the templates.

Be sure to select the correct system **Standard** or the import may fail.

Signaling Manager imports configuration files from older versions and converts them to the used version. The only restriction is that the configuration must be LPY111384 R2 or later. To view the total set of supported stack module revisions start Signaling Manager and open the **About** dialog in Help menu. The information is displayed if the **More Info** button is pressed.

Note: If imported configuration is older than LPY111384 R2 it cannot be imported and should be modified manually to fit the LPY111384 R2 version and imported then.

Be sure to add the NTF Agent process and the AMF Wrapper entries in the same manner that is described in Section 6.1.2 on page 24.

6.2 Multiple SCTP Processes per Blade

Default configuration of SCTP FE processes doesn't allow to use the same IP address by several SCTP FE on the same host. In case this functionality is needed the following updates should be performed in configuration:

1. Enable an expert mode in **Tools->Expert Mode**.
2. Add process class **SCTP_CONTROL FEP** to **Signaling System/System Components/ECM/Process Classes** with the following parameters:
 - **Class ID:** SCTP_CONTROL FEP
 - **Instance Type:** SCTP_CONTROL
 - **Command:** should be copied from **SCTP FEP** process class, parameter **-f 1** should be added to start-up arguments
 - **Supervise User ID:** SCTP
3. Add process class **SCTP_SERVER FEP** to **Signaling System/System Components/ECM/Process Classes** with the following parameters:
 - **Class ID:** SCTP_SERVER FEP
 - **Instance Type:** SCTP_SERVER



- **Command:** should be copied from **SCTP FEP** process class, parameter **-f 2** should be added to start-up arguments
 - **Supervise User ID:** SCTP
4. Add process with process class **SCTP_CONTROL FEP** to host **Active** in **Signaling System/System Components/ECM/Hosts**. This process must have Instance ID 0.
 5. Replace **SCTP FEP** processes with **SCTP_SERVER FEP** processes on every host. Instance ID for these processes must not be equal to 0.

Additional process classes define SCTP FE processes with new roles: **Control** and **Server**. SCTP FE without **-f** parameter and Instance Type **FEP** have a role **Single** which represents old SCTP behavior. Description of each role can be found in Reference [18].

If **SCTP FEP** process class is used **SCTP_CONTROL FEP** with **SCTP_SERVER FEP** process classes cannot be used. I.e. any host has SCTP FE with a **Single** role then **Control** and **Server** roles cannot be used and vice versa.

Processes with **SCTP_SERVER FEP** class cannot be used without **SCTP_CONTROL FEP** class.

6.3 SCTP Only stack

SCTP Only stack is a stack where only SCTP FE are used as traffic bearers and no BEs are used.

The following processes are present in SCTP Only stack:

- SAW
- SAF OAM
- OAM
- SCTP FE
- ECP
- ECS
- LOGD

SCTP Only stack is configured in the same way as the SS7 stack using Signaling Manager.

6.4 SS7 CAF Configuration for Scaling Operations

SS7 CAF configuration shall comply to the following rules in order to participate in Scale-Out and Scale-In operations:

- "Follow active ECM" processes (e.g. SAF_OAM, LOGD) must be configured under special ECM-host "Active". For configuration see Section 6.6 on page 29
- LDE MIP shall be used as Common Parts manager address. For configuration of LDE MIP as Common Parts manager address see Section 6.12 on page 36
- Only one SCTP FE shall be configured per host. All SCTP FE shall have the same startup parameters
- One or none SS7 BEs can be defined per host. All SS7 BE shall have the same startup parameters
- Only Distributed EP(s) can be defined in SCTP configuration. The same SCTP Distributed EP(s) shall be defined across all FEs, see Section 6.10 on page 32 for configuration procedure
- SCTP FE configuration including SCTP Distributed EP(s) shall be the same for all SCTP FE(s), see Section 6.10 on page 32
- If M3 configuration is used, it shall use only SCTP Distributed EP(s), see Section 6.10 on page 32 for configuration options
- At least one host with installed SS7 CAF should be included into scaling domain, otherwise update of configuration will be skipped during scaling. See Reference [23] for information about configuration of scaling domains.
- ECM parameter **Connection Time Wait** must be set to **25**
- Asynchronous connection should be enabled for BE, FE and NMP processes. It can be activated using the following ways:
 - **-w 5** should be added to BE, FE, NMP launching command
 - Parameter **Msg Conn Time Wait** should be set to **25** in CP settings

Whenever SS7 CAF configuration is updated the rules shall be followed in updated configuration. For example, if some SCTP FE parameter is changed, it also has to be changed for all other SCTP FE(s).

6.5 Setup Parameters

Enable expert mode in Signaling Manager; **Tools->Expert Mode**, which is necessary to be able open the System Components MO. Also enable initial configuration; **Tools->Configuration Mode->Initial**, to be able to modify all parameters.

CP Manager Address is located directly under **System Components**.



The ECM and CP parameters are located under **System Components/ECM** and **System Components/CP**.

The M3UA and SCTP parameters are located under **M3UA IETF** and **SCTPs**, respectively.

All address parameters must contain all hosts involved in the signaling stack installation.

Update, if necessary, the CP Manager Address for Signaling Manager own configuration:

- **CP Manager Address** must be set to a comma separated list of alternative IP-address or host names and port-number pairs that the CP Manager is configured to listen to.

Update, if necessary, the Max Instance ID for Signaling Manager own configuration:

- **Max Instance ID** must be equal to value of the macro MAX_NUMBER_OF_INSTANCES. For details about MAX_NUMBER_OF_INSTANCES see Reference [15]

CP parameter **Msg Buff Size** should have value **10000** or more.

Update, if necessary, the following values for ECM and CP:

- **Hostnames of the EC processes (EINSS7_ECM)**
- **Hostname of the EC supervisor (EINSS7_ECS)**
- **Hostname of the AMF Wrapper (SAF_AMF)**

Note: **Instance Id** of the EC Users in CP must be the same as for corresponding host's priority number in ECM. See Reference [4] and Reference [2].

Update, if necessary, the following values for M3UA and SCTP:

- **M3UA remote SPs**
- **SCTP local IP Addresses for SCTP end-points**

Note: To add/remove hosts or user processes, see Reference [8].

Update, if necessary, ECM logging settings, for more information see Section 6.9 on page 31.

6.6 ECM Active Host

Special host with hostname **Active** should be defined in ECM for processes which should follow active ECM:

— LOGD

— SAFOAM

If it is not defined in ECM configuration it should be created and “Follow active ECM” processes should be configured under this host. This can be done in Signaling Manager GUI or to do this via CLI use following commands:

1. Define Active host:

```
ECHSI: ADDR="Active";
```

```
ECHSC: ADDR="Active", PRI0="";
```

2. Remove processes SAFOAM and LOGD which were defined outside the Active host:

```
ECPSE: CID=SAFOAM, IID=0;
```

```
ECPSE: CID=LOGD, IID=0;
```

3. Create processes SAFOAM and LOGD under the Active host:

```
ECPSI: ADDR="Active", CID=SAFOAM, IID=0, ON0=1;
```

```
ECPSC: CID=SAFOAM, IID=0, TimerConnect=30000;
```

```
ECPSI: ADDR="Active", CID=LOGD, IID=0, ON0=1;
```

4. Perform initial reconfiguration and restart stack to apply new value of the parameters:

```
configure: INITIAL;
```

```
procr: ALL;
```

Note: If you are updating configuration via GUI make sure SAF_OAM and LOGD Instance IDs have not been changed.

Note: TimerConnect might need higher value dependent on HW and if it too low SAF_OAM will not be started.

The "Process Down" alarm will appear for LOGD after step 4. This alarms will not be cleared automatically and this is expected behavior. To clean it up manually perform the following command:

```
ntfsend -s 0 -c 193,24209,513 -n '3GPPSystemComponents.Name=System
Components,Ecm.Name=ECM,Host.Address=PL-X,ClassID=11,InstanceType=
7,Process.InstanceID=0'
```

Where **PL-X** is a name of host where LOGD was configured before, for example PL-4.



6.7 Usage of IPv6

The IPv6 stack configuration is similar to IPv4, but IPv6 addresses are used instead of IPv4 addresses. Information about configuration of address parameters can be found at Section 6.5 on page 28

Note: If IPv6 is used for IPC then IPv6 network should be configured on the cluster, see Reference [22] and Reference [21] for details.

6.8 CP trace and logging facilities

/opt/sign/log is a default SS7 log storage, alteration of the log folder is highly not recommended.

For detailed information about advanced trace and logging facilities see Reference [14] .

6.9 ECM logging

ECM logging to log file in NFS folder can be used. But there might be a case when both Service Controllers are shut down. Then NFS will be unavailable and ECM will hang trying to write the log. To avoid this case it is recommended to configure ECM to send the log messages to the system log.

6.9.1 Configuring ECM logging to syslogd with SM GUI

1. Launch Signaling Manager GUI and switch the initial configuration mode on.
2. Turn the expert mode on.
3. Change the value of 'Log' parameter on ECM tab of System Components to "syslogd".
4. Perform initial reconfiguration and restart stack to apply new value of the parameter.

6.9.2 Configuring ECM logging to syslogd with SM CLI

1. Launch Signaling Manager CLI.
2. Choose the initial configuration mode.

`confmode:mode="init";`
3. Change ECM logging:

`ECECC:Log=syslogd;`
4. Perform initial reconfiguration and restart stack to apply new value of the parameter.

configure:INITIAL;

procr:ALL;

6.10 SCTP Distributed End Points

SCTP distributed End Point is an SCTP End Point shared between several SCTP Front End instances.

This feature requires both eVIP and SS7 CAF SCTP Distributor functionality.

6.10.1 SS7 CAF Configuration for SCTP Distributed End Points

To enable usage of eVIP functionality in SS7 CAF the **EVIP** option at **CP** tab of System Components in Signaling Manager GUI must be set to **ON**.

Note: It is not possible to use SS7 CAF without installed eVIP if **EVIP** option set to **ON**.

For all SCTP End Points the **Used By M3** option should be set to **No**.

If M3 is used:

- For every SCTP FE **Is Used By M3** option should be set to **Yes**

Note: **Used By M3** option for End Point should be still set to **No**

- For every Distributed End Point should be created Local SP which refers to End Point on the first SCTP FE
- M3 option **Distributed End Point Support** on M3UA tab of M3UA IETF in Signaling Manager GUI must be set to **ON** to allow usage of SCTP Distributed End Points feature

With such SS7 configuration only one ALB can be used for SCTP traffic distribution since ALB selection is based on a process name (see Section 6.10.3 on page 34). To allow usage of VIP addresses from several ALBs by one SCTP FE the ALB name should be specified for every EP address in addition to configuration above:

- If SCTP API is used ALB name should be specified during EP initialization, more information can be found in function specification for used API.
- If SS7 protocols are used the following attributes should be updated in SM for the **Signaling System/SCTPs/SCTP End Points/SCTP Local Address**:
 - **Use Extended Format** - Parameter defines if Local IP Address is configured with or without extension.
 - **VPN Name** - VPN Name string defines network in which this IP Address will be placed. VPN Name can contain not more than 13 symbols: [A-Za-z0-9_-].



To specify ALB name parameter **Use Extended Format** should be set to **VPN Name extension**. In this case parameter **VPN Name** must contain the name of ALB which should be used for the address.

6.10.2

Examples of SCTP Distributed End Point Configuration

Below the examples of SCTP Distributed End Point stack configuration can be found.

Page 33 shows the simplest configuration, user initialized EP has the same IP address and port on every SCTP FE:



Figure 2 1 SCTP FE per payload with 1 Distributed EP

If it is intended to use several Distributed EPs then additional EPs can be initialized on the same SCTP FE, but IP addresses or ports for new EPs should be different from existing EPs, see Page 33.

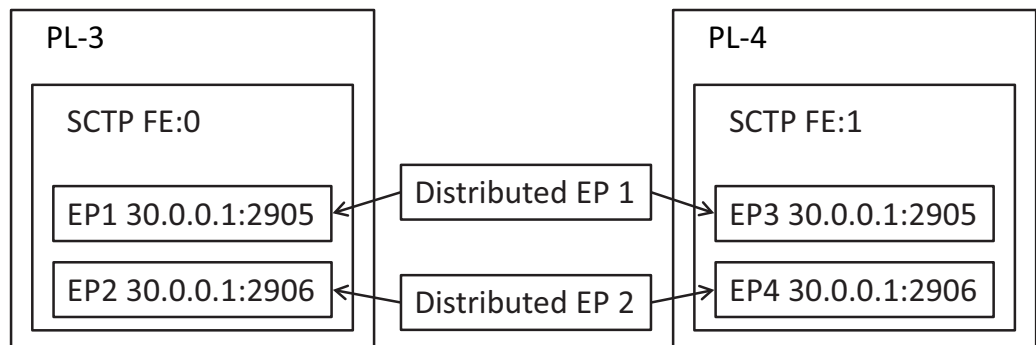


Figure 3 1 SCTP FE per payload with 2 Distributed EPs

SCTP FE process is a single threaded, so on hosts with multicore CPUs several SCTP FEs should be running to use more cores. In this case the same IP addresses cannot be used in the several SCTP FEs on the same host due to limitation in SCTPd. So if user wants to use several SCTP FEs on the same host then IP addresses used by these SCTP FEs should be different. See Page 34.

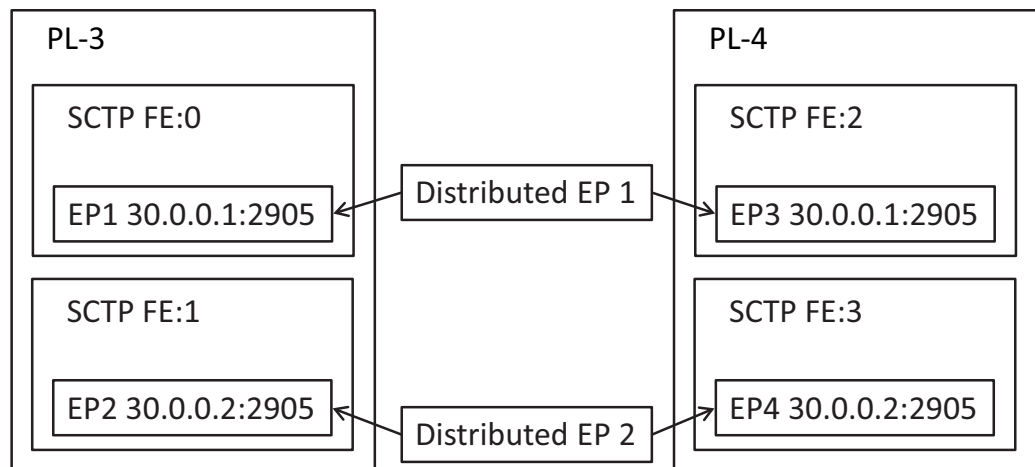


Figure 4 2 SCTP FEs per payload with 2 Distributed EPs

6.10.3

eVIP Configuration for SCTP Distributed End Points

SCTP distributor package shall be installed and available on nodes which are serving as eVIP LBE.

eVIP shall be installed and available in the cluster to allow SCTP traffic distribution. Configure the following in eVIP to allow SCTP traffic distribution via SCTP Distributed EP(s):

- For each VIP address to be used in SCTP distributed EP: define eVIP flow policy with SCTP protocol and set **SO_GRP** parameter to **1011250**
- For each ALB which handles SCTP traffic: in the ALB selection policy set parameter **process** to **fe_sctp**

See Reference [21] for details on eVIP configuration procedures.

Note: SCTP Distributor is an implementation of eVIP Adjunct Helper.

6.11

eVIP Address as Common Parts Manager Address

It is possible to use eVIP address as a single common IP address for Common Parts manager address.

This feature requires both eVIP and SS7 CAF functionality.

6.11.1

eVIP Configuration

eVIP shall be installed and available in the cluster. Configure the following in eVIP to allow usage of eVIP address as Common Parts manager address:



- For the VIP address to be used as Common Parts Manager address: define eVIP flow policy with TCP protocol and TCP port used for Common Parts manager
- For the ALB which handles traffic towards Common Parts manager: in the ALB selection policy set parameter **process** to **oam**

See Reference [21] for details on eVIP configuration procedures.

6.11.2 SS7 CAF Configuration

Launch either Signaling Manager GUI or CLI, switch it to initial configuration mode.

Set Common Parts manager address to eVIP address:

- If using Signaling Manager GUI, then on CP tab of System Components
- If using Signaling Manager CLI, then using the following command:

```
SSSCC:CPMA="<eVIP CPM addres>:<CPM Port>";
```

<CPM port> is Common Parts manager listen port, by default its value is 6669

<eVIP CPM addres> is eVIP address intended to be used as Common Parts manager address

Set **If Aliased** option to **Yes**:

- If using Signaling Manager GUI, then on CP tab of System Components
- If using Signaling Manager CLI, then using the following command:

```
CPCPC:IfAlias=0;
```

It is recommended to separate traffic between Common Parts manager and Common Parts clients from traffic between FE and BE processes by using different subnets for different type of traffic. For configuration see Section 6.14.4 on page 40

Note: If the traffic is not separated, then all SCTP and Signaling traffic will go through a single eVIP address which might not handle an intense traffic

If Common Parts manager address is changed while SS7 CAF is up and running, then in order to apply the change SS7 CAF AMF Service Group **safSg=NWay-Traffic, safApp=ERIC-SS7CAF** has to be locked, instance locked, instance unlocked and unlocked to allow SAW process acknowledge the change. For procedure see CoreMW guides. For CoreMW 3.6 and prior it can be done using the following commands on any of the Service Controllers in the cluster:

```
amf-adm lock safSg=NWay-Traffic,safApp=ERIC-SS7CAF
amf-adm lock-in safSg=NWay-Traffic,safApp=ERIC-SS7CAF
```



```
amf-adm unlock-in safSg=NWay-Traffic,safApp=ERIC-SS7CAF  
amf-adm unlock safSg=NWay-Traffic,safApp=ERIC-SS7CAF
```

6.12 LDE MIP Address as Common Parts Manager Address

It is possible to use LDE MIP address as a single common IP address for Common Parts manager address.

This feature requires both LDE and SS7 CAF functionality.

6.12.1 LDE Configuration

Define MIP address with **ss7cafcpmaddress** name in LDE cluster configuration.

See LDE User Guide for details on MIP configuration procedures.

Note: Do not activate MIP manually, activation will be done by SS7 CAF processes automatically once SS7 CAF is configured for MIP usage

6.12.2 SS7 CAF Configuration

Launch either Signaling Manager GUI or CLI, switch it to initial configuration mode.

Set Common Parts manager address to LDE MIP address:

- If using Signaling Manager GUI, then on **CP** tab of System Components
- If using Signaling Manager CLI, then using the following command:

```
SSSCC:CPMA="ss7cafcpmaddress:<CPM Port>";
```

<CPM port> is Common Parts manager listen port, by default its value is 6669

Set **If Aliased** option to **Yes**:

- If using Signaling Manager GUI, then on **CP** tab of System Components
- If using Signaling Manager CLI, then using the following command:

```
CPCPC:IfAlias=0;
```

For each ECM host pre and post scripts have to be set:

- If using Signaling Manager GUI, then in configuration for each ECM host:
 - **Pre Script** to **/opt/sign/instance/cpm_mip_activation.sh**
--activate



- Post Script to `/opt/sign/instance/cpm_mip_activation.sh`
`--deactivate`

Note: Different parameters are passed to the scripts

- If using Signaling Manager CLI, then repeat the following two commands for each ECM host:

```
ECHSC:ADDR=<ECM HOST NAME>,PRESCRIPT="/opt/sign/instance/cpm_mip_activation.sh --activate";
```

```
ECHSC:ADDR=<ECM HOST NAME>,POSTSCRIPT="/opt/sign/instance/cpm_mip_activation.sh --deactivate";
```

<ECM HOST NAME> is the ECM host name

Note: Different parameters are passed to the scripts

If Common Parts manager address is changed while SS7 CAF is up and running, then in order to apply the change SS7 CAF AMF Service Group **safSg=NWay-Traffic**, **safApp=ERIC-SS7CAF** has to be locked, instance locked, instance unlocked and unlocked to allow SAW process acknowledge the change. For procedure see CoreMW guides. For CoreMW 3.6 and prior it can be done using the following commands on any of the Service Controllers in the cluster:

```
amf-adm lock safSg=NWay-Traffic,safApp=ERIC-SS7CAF
amf-adm lock-in safSg=NWay-Traffic,safApp=ERIC-SS7CAF
amf-adm unlock-in safSg=NWay-Traffic,safApp=ERIC-SS7CAF
amf-adm unlock safSg=NWay-Traffic,safApp=ERIC-SS7CAF
```

6.13 NTF Alarms Configuration

The following alarm masks must be set to let SM NTF Agent pass the alarms to middleware NTF service:

Table 6 Alarms

| Alarm | SS7 module and required alarm mask | OPI reference |
|--|------------------------------------|-----------------------|
| SS7 CAF Dialogue Threshold High Watermark Exceeded | TCAP: 93 | 1/1543-ANA 901 37 Uen |
| SS7 CAF OAM Connection Lost | N/A | 2/1543-ANA 901 37 Uen |
| SS7 CAF Link out of service | MTPL3: 4 | 3/1543-ANA 901 37 Uen |
| SS7 CAF Remote Processor Outage | MTPL3: 5 | 4/1543-ANA 901 37 Uen |



| | | |
|---|------------|------------------------|
| SS7 CAF Low Link Availability | MTPL3: 94 | 5/1543-ANA 901 377 Uen |
| SS7 CAF Connections Exceed High Threshold | SCCP: 49 | 6/1543-ANA 901 37 Uen |
| SS7 CAF Remote SSN Status Change | SCCP: 42 | 7/1543-ANA 901 37 Uen |
| SS7 CAF SCCP Bind Request | SCCP: 46 | 8/1543-ANA 901 37 Uen |
| SS7 CAF SSC Received | SCCP: 58 | 9/1543-ANA 901 37 Uen |
| SS7 CAF Process Down | N/A | 10/1543-ANA 901 37 Uen |
| SS7 CAF ECM Goes Down | N/A | 11/1543-ANA 901 37 Uen |
| SS7 CAF ECM Goes Active | N/A | 12/1543-ANA 901 37 Uen |
| SS7 CAF AS State Change | MTPL3: 126 | 13/1543-ANA 901 37 Uen |
| SS7 CAF SP State Change | MTPL3: 124 | 14/1543-ANA 901 37 Uen |
| SS7 CAF Route Set Failure | MTPL3: 111 | 15/1543-ANA 901 37 Uen |
| SS7 CAF Congestion Status Change | MTPL3: 170 | 16/1543-ANA 901 37 Uen |
| SS7 CAF Link Deactivated | MTPL3: 8 | 17/1543-ANA 901 37 Uen |
| SS7 CAF Local Link Congestion | MTPL3: 30 | 18/1543-ANA 901 37 Uen |
| SS7 CAF Call Control Replaced | ISUP: 84 | 19/1543-ANA 901 37 Uen |
| SS7 CAF Resource Group State Change | ISUP: 44 | 20/1543-ANA 901 37 Uen |
| SS7 CAF Number of Circuits Exceed High Water Mark | ISUP: 88 | 21/1543-ANA 901 37 Uen |
| SS7 CAF DPC State Change | ISUP: 43 | 22/1543-ANA 901 37 Uen |
| SS7 CAF Start Process Failed | N/A | 23/1543-ANA 901 37 Uen |
| SS7 CAF SCTP IP Path is Down | SCTP: 12 | 24/1543-ANA 901 37 Uen |



| | | |
|--|---------------|------------------------|
| SS7 CAF SCCP Unbind Request | SCCP: 47 | 25/1543-ANA 901 37 Uen |
| SS7 CAF Link Unavailable for UP | MTPL3: 91 | 26/1543-ANA 901 37 Uen |
| SS7 CAF Dialogue Threshold High Watermark Exceeded ANSI TCAP | ANSI TCAP: 40 | 27/1543-ANA 901 37 Uen |

For details on each alarm see corresponding OPI.

For details on how to configure and subscribe to SS7 Stack alarms see Reference [8]

Note: All these are alarms are set by default in example templates configurations.

6.13.1 Default Names for Signaling Porotocol Layers and "\$" Sign in the SS7 Stack Alarms

In Signaling Manager the Signaling protocol layers can have either a:

- Custom name. It can be set by writing a name in the **Property** tab
- Default value. It can be set by checking **Auto** checkbox in the **Property** tab

All example template cim files provided with SS7 CAF are having Signaling protocol layers have checked **Auto** checkbox in the **Property** tab.

If a Signaling protocol layer has checked **Auto** checkbox in the **Property** tab, then the "\$" sign appears before the layer name in the SS7 CAF alarms.

6.14 General Configuration Recommendations

This chapter contains general configuration recommendations that need to be kept to avoid potential problems with the SS7 CAF component.

6.14.1 ECM and CP configuration dependencies

To avoid unexpected behavior when one of the configured hosts in a system becomes unavailable it's recommended to follow the rules for ECM and CP timers as described in Reference [1].

The example configuration is configured for two hosts.

Note: Host priority change is not applied during ECM reconfiguration. In order to apply the changes all service units should be locked and unlocked. For details on service unit operations see Reference [14].

6.14.2 Log Write Mode

It is **not** recommended to set **Log Write Mode** Common Parts configuration parameter to **SEQ** because in that mode LOGD process writes logs without controlling amount of consumed disk space. With such log writing enabled it is possible that logs take all available free disk space which might result in unpredictable behavior of the system in overall.

Instead it is recommended to set **Log Write Mode** Common Parts configuration parameter to **CIR** to control amount of disk space used by SS7 CAF logs.

6.14.3 Recommended parameter values for vDicos applications

Recommended following values for parameters in Common Parts:

MSGBUFSIZE = 5000

MSGMAXENTRIES = 50

Note: Default values of MSGBUFSIZE and MSGMAXENTRIES can raise "Out of user heap" error on vDicos system.

6.14.4 Network Definition for Common Parts (MSGPREFERDNET, MSGALLOWEDNETS and MSGDISALLOWEDNETS)

It's often useful to specify which IP-network the internal signaling traffic (Common Parts) shall use. Usually it's not possible to use all available networks on a server since all networks are not connected. Thus the network selected and used by Common Part must be a network which is reachable from all hosts in the signaling cluster, including the application and OAM hosts.

Having many network interfaces can also affect the time it takes until all Common Parts processes get connected. Each network will be tried until a connection is successfully established. Another problem is that the IP traffic can sometimes find other ways to connect; it's not always the shortest and fastest route that is chosen.

To be able to define a preferred network that Common Parts shall use, configuration parameter named MSGPREFERDNET in Common Parts configuration could be used. This parameter allows to set a net mask identifying which IP subnet that shall be used. All Common Parts processes will then use this subnet to connect.

MSGPREFERDNET = <net mask>

The net mask may have the following formats:

- 123.* (class A)
- 123.123.* (class B)
- 123.123.123.* (class C)



— 123.123.123.123 (Unique address, not commonly used)

Addresses to Common Parts processes specified with MSGIPA do not have to be inside the sub-net.

MSGPREFERDNET is not implemented for JCP, therefore in order to use a specific network while using JCP JVM start parameter should be used:

–Dcom.ericsson.jcp_ip_aliases=[<IP-addresses to filter out, separated by semicolon>]

To be able to restrict the allowed network that Common Part shall use, configuration parameters named MSGALLOWEDNETS and MSGDISALLOWEDNETS in Common Parts configuration should be used.

MSGALLOWEDNETS allows to set net masks identifying IP networks for Common Parts IPC.

The syntax of MSGALLOWEDNETS is a list of IP subnets separated by comma, for example:

MSGALLOWEDNETS = 10.41.45.*, fe80::214:4fff:fe70:a 01a/10

MSGALLOWEDNETS may contain message port owner (Common Parts client) ID set first before the addresses. In this case common settings will not be applicable to this message port owner:

MSGALLOWEDNETS = CP_MANAGER, 13.1.27.0/24, fe80::214:4fff:fe70:a01a/10

If MSGALLOWEDNETS is configured, the Common Parts processes will only bind to those IP addresses which satisfy the allowed subnet list.

Note: IP addresses specified with MSGIPA parameter in Common Parts configuration can be outside the subnets defined in MSGALLOWEDNETS parameter.

MSGDISALLOWEDNETS is used to specify IP networks which should not be used for IPC. The syntax of this parameter is similar to MSGALLOWEDNETS.

If MSGDISALLOWEDNETS is configured, the Common Parts processes will only bind to those IP addresses which do not satisfy the disallowed subnet list.

Note: IP addresses specified with MSGIPA parameter in Common Parts configuration can be inside the subnets defined in MSGDISALLOWEDNETS parameter.

To get more information about MSGPREFERDNET, MSGALLOWEDNETS and MSGDISALLOWEDNETS parameters see Reference [2].



6.14.5 Port Number Definition for Common Parts

To restrict the interval of used port numbers the parameter MSGALLOWEDPORTS can be used. The syntax of MSGALLOWEDPORTS is a list of ports and ranges of ports separated by comma. All ports specified by this parameter must be in range 1024 - 65535

The parameter may contain message port owner (Common Parts client) ID, and message port owner ID with instance. The message port owner ID should be specified first before the port list. If message port owner ID is specified without instance, such a parameter will be considered common for all instances of the specified message port owner:

MSGALLOWEDPORTS = FEIFHD, 36000, 36100, 36200

Note: SS7 CAF processes can not open ports outside the defined in MSGALLOWEDPORTS. If all ports in the range are already in use, a process will fail to open its port.

Port set in MSGIPA parameter may be not specified in MSGALLOWEDPORTS.

To get more information about MSGALLOWEDPORTS parameters see Reference [2].

6.14.6 Bundling in SCTP Configuration

BundlingTimer should be set to non-zero value when Bundling is activated.

BundlingTimer set to 0 when Bundling is activated might cause problems to bring up association.

6.14.7 Deploying with SIGTRAN

When deploying with SIGTRAN there could be a situation where ping of remote addresses is OK, but associations are not getting up. Check with operator that there are no firewall settings that restricts any ports for the used IP addresses. The firewall must allow the entire IP address, all ports.

6.15 Save SS7 CAF Configuration

The configuration should be validated before saving: select **Edit->Validate** from the menu.

Save the configuration to **/opt/sign/etc**, and close Signaling Manager.



6.16 Generate (Export) SS7 CAF Configuration Files

- Start the Signaling Manager in online mode:

```
/opt/sign/EABss7050/bin/signmgr -own.conf=<signmgr config file> &
```

- Open the SS7 CAF configuration previously created as a template .

Note: Any changes made on the configuration at this point will not affect the template.

- At **Process view...** the dialog box which is opened when the Process View Option in the Tools menu is selected, choose operations **Configure** and **Initial Configuration** to generate a number of CNF format files from the configuration has been just completed. CNF files are the files being used by the signaling modules during initiation/reinitiation. The number of configuration files depends on the configured signaling protocol modules.

Note: The CNF files are exported to the specified **Export location**, which by default is **/opt/sign/etc**.

If the ECM IMC is loaded and an **ECMclasses.xml** file exists in the **Export location** it will be renamed to **ECMclasses.old.xml** because it is obsolete and replaced by **ecm.xml**

6.17 Setting parameters for large eVIP configuration

In case configuring any setup, larger than the small configuration of 4 ALBs, with 2 LBEs, 2 FEEs, and 2 SEs configured for each ALB, values for sysctrl parameters should be changed (see reference Reference [14]).





7 SS7 CAF Performance Management

SS7 CAF supports common for all components official CBA interface Core MW ECIM PM, see Reference [24].

PM Groups and Measurement Types in SS7 CAF are described in Reference [19] and Reference [20].



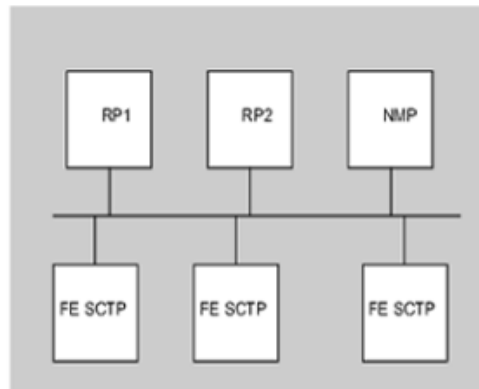


8 Network Examples

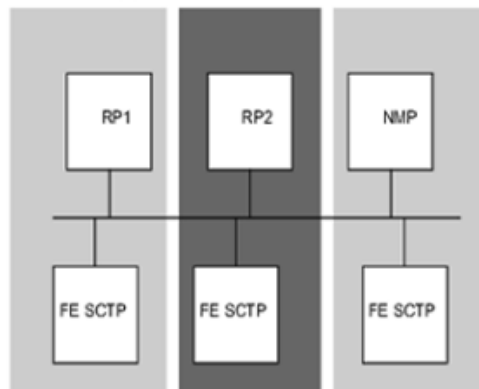
The BE and FE processes can be installed and executed in different machines.

Page 47 shows a few examples of different networks and process distribution.

Architecture (1)



Architecture (2)



Architecture (3)

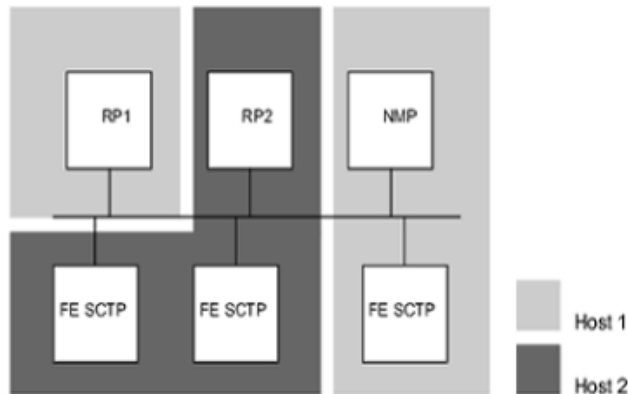


Figure 5 Examples of different networks and process distribution.



Architecture 1

- Description:** One host architecture.
- Distribution:** RP1, RP2, NMP, and SCTP FE are running at host 1.

Architecture 2

- Description:** Two hosts architecture.
- Distribution:** RP1, NMP, and SCTP FE are running at host1. SCTP FE and RP2 are running at host 2.

Architecture 3

- Description:** Two hosts architecture.
- Distribution:** RP1 and SCTP FE are running at host1. SCTP FE and RP2 are running at host 2.

The distribution of the processes are outlined in the EC configuration file which should be modified by user.

All templates and configuration files included in the installation (and CNF files exported by the Signaling Manager) are stored at **/opt/sign/etc/** which must be accessible by all hosts involved in the installation.



9 Software Development Kit

SS7 CAF provides the SDK package with the following contents:

- SS7 CAF API (headers and libraries)
- SS7 CAF API for vDicos environment
- SS7 CAF documentation
- Developer environment script

9.1 SDK Installation

In order to install SDK use the following steps:

1. Login to the host where SDK is to be installed if not already done:

```
ssh -l <User> <hostname or IP>
```

2. Create a folder where SDK contents should be installed to:

```
mkdir -p <folder to install SDK to>
```

3. Upload the following zip-archive with the SDK SS7 CAF package to the SDK folder using `scp` or `sftp`:

```
— CXP9022702-<revision>.zip
```

Note: <revision> is the revision of downloaded SS7 CAF package

4. Go to the SDK install folder:

```
cd <folder to install SDK to>
```

5. Unzip the archive:

```
unzip CXP9022702-<revision>.zip
```

6. Extract the SDK contents:

```
tar xf ss7caf-<revision>-<build number>-sdk-sle-cxp9022702.tar.gz
```





10 SS7 CAF Troubleshooting

For SS7 CAF troubleshooting details see Reference [14]





Reference List

SS7 CAF documentation

- [1] SS7 CAF Dimensioning Guide, 2/1551-ANA 901 37 Uen
- [2] Common Parts Configuration File Description, 3/190 73-CAA 201 29 Uen
- [3] OAM Configuration File Description, 190 73-CAA 901 791Uen
- [4] Execution Control Module Functional Specification, 15517-CAA 901 1672 Uen
- [5] Signaling Manager User Guide , 1553-CNA 403 0874/1 Uen
- [6] Signaling Manager Command Line Interface User Guide, 1/1553-CNA 403 0874 Uen
- [7] Signaling Manager Configuration, 19073-CNA 403 0874/1 Uen
- [8] Configuring SS7 System Components, 7/1543-CNA 403 0874/1 Uen
- [9] SM NTF Agent Function Specification, 155 17-CAA 901 2467 Uen
- [10] SS7 AMF Wrapper Function Specification, 155 17-CAA 901 2465 Uen
- [11] Application Programmer's Guide for SS7 CAF, 1/1551-ANA 901 37 Uen
- [12] Product Revision Information, 109 21-ANA 901 37 Uen
- [13] Common Parts Functional Specification, 15517-CAA 201 29 Uen
- [14] SS7 CAF Troubleshooting Guide, 3/1553-ANA 901 37 Uen
- [15] SS7 CAF Deviation Description, 1/170 05-ANA 901 37 Uen
- [16] SS7 CAF Installation Instructions, 1/1531-ANA 901 37 Uen
- [17] Glossary of Terms and Acronyms
- [18] SCTP, FUNCTIONAL SPECIFICATION, 155 17-CAA 901 548 Uen
- [19] SCTP Performance Measurements, 1/155 19-ANA 901 37 Uen
- [20] SS7 Performance Measurements, 2/155 19-ANA 901 37 Uen

CBA documentation

- [21] eVIP Management Guide, User Guide, 1/1553-APR 901 0467/1 Uen



- [22] LDE Management Guide, User Guide, 1/1553-CAA 901 2978/1 Uen
- [23] Core MW Cluster Manager Description, Function Description, 2/155 16-CAA 901 2624/1 Uen
- [24] Core MW Performance Management Description, 1/155 16-CAA 901 2624/4 Uen