A MITEL
PRODUCT
GUIDE

OpenScape CAP V3

Common Application Platform

Service Documentation

09/2024

A31003-G9330-I100-18-7620

Notices

Trademarks

Contents

1 Preface

This chapter contains a short summary of the contents of this document and a list of the various formats in which this and additional documents are available. The layout conventions used in this document are also explained.

1.1 Structure of this documentation

This document is structured as follows:

? **Chapter 2** contains an overview of the architecture of OpenScape CAP, as well as typical configurations and installation scenarios.

? **Chapter 3** outlines the system requirements for OpenScape CAP.

? **Chapter 4** describes how to install OpenScape CAP components. This chapter describes the server components "CAP Management", "Call Control Services (SCC/SCCP)" and the connectivity adapters CA4000 and as well as the client components "CAP Service Starter", "CAP TAPI Service Provider (TCSP)", and "Virtual Wave Driver". You will also find details on migration (in particular the migration of configuration and user data from earlier versions of CAP and TELAS) and importing data (in particular the synchronization of data with HiPath / OpenScape 4000).

? **Chapter 5** introduces the CAP Management interface.

? **Chapter 6** describes how to configure the OpenScape CAP components using OpenScape CAP Management. This chapter explains how OpenScape CAP is connected to HiPath / OpenScape 4000, HiPath 3000, OpenScape Voice and other switching systems. It also describes how to configure the XML Phone Service.

? **Chapter 7**contains an overview of the OpenScape CAP Management functions.

? **Chapter 8** deals with diagnostics and error handling in the event of installation and runtime problems.

? **Chapter 9** explains the operating modes supported by OpenScape CAP, namely "single domain native mode" and "multi domain harmonized mode".

? **Appendix A** contains implementation details in relation to both the structure of the OpenScape CAP software and the layout of configuration files and parameters.

? **Appendix B** describes how the server PC is connected to a HiPath 4000 communication system that has no built in CSTA interface.

The documentation also contains a **Glossary** and an **Index**.

1.2 Versions of this document

? **PDF format**

This version of the document is named *manual.pdf*.

The English version is saved in the directory
`<InstDir>`*\WebSpace\Admin\webapps\mgmnt\lang\en\admManual*\.

The German version is saved in the directory
`<InstDir>`*\WebSpace\Admin\webapps\mgmnt\lang\de\admManual*\.

The PDF format is particularly suitable for printing and is available online via the OpenScape CAP Management user interface.

? **HTML format**

This version of the document is named *manual.html.*

The German and English versions are stored in the same directories as specified above.

The HTML version of the manual is also available as online help.

? **Release notes**

Release notes with important information on last-minute changes to products are stored on the CD in the file *<xxx>Readme.txt*.

They are available in English only.

1.3 Additional documentation

The following documentation contains further topics relating to OpenScape CAP:

? OpenScape CAP Application Developers’ Guide
Vol.1 - Basics
Vol.2 - TAPI
Vol.3 - JTAPI
Vol.4 - CSTA XML
Vol.5 - CSTA III ASN.1
Vol.6 - XML Phone Server
Vol.7 - Fault Management
Vol.9 - Management

? OpenScape CAP TAPI Service Provider, Service Manual

1.4 Layout conventions

... **OK** button.	**Buttons** and **menus** appear in **bold print**.
... file `global.cfg` ...	`Files` or `directories` are displayed in `courier` font.
<*some text*>	Entries or output that may vary according to the situation are shown within angle brackets.

Table 1:

> This symbol indicates notes or recommendations.

7 This symbol indicates important information that you must read.

1.5 Feedback on documentation

If you would like to report a problem with this document, please contact the next support level.

? Unify employees should contact the support center responsible for their region.

? Customers are advised to contact the Unify Customer Support Center.

Please have the following information to hand so that the support center can quickly pinpoint the document you have a problem with:

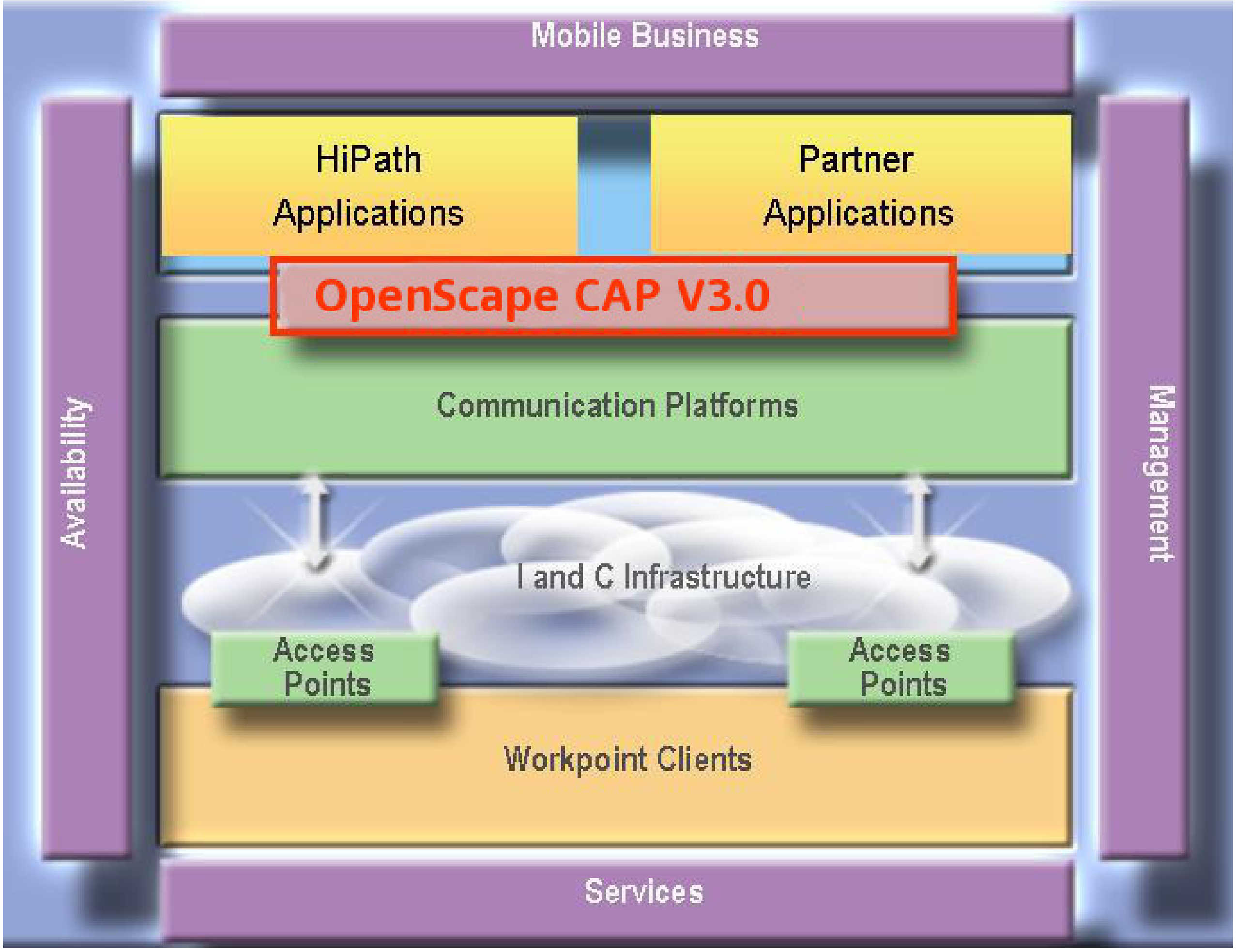
? **Title:** OpenScape CAP V3, Common Application Platform, Service Documentation

? **Part number:** A31003-G9330-I100-18-7620

2 Overview

This chapter describes the Common Application Platform within the OpenScape architecture. The synonyms CAP and OpenScape CAP are used interchangeably in the following.

2.1 General role of OpenScape CAP in the HiPath / OpenScape architecture



OpenScape CAP is a central element in the HiPath / OpenScape architecture. It serves as a powerful middleware connecting applications based on standard protocols, both with HiPath / OpenScape systems and third-party PBXs.

Licensing is required for every device (phone, trunk, etc.) that is controlled by the applications. The features supported are grouped into five different license packages. These packages do not make any distinction between protocols, encoding variants, or connection types.

Services

? Flexible use of applications based on standards.

? CTI application support for clients in different infrastructures.

? Support for media streaming without expensive hardware.

? Integration of OpenScape CAP and applications into the OpenScape Management system.

? Seamless support for applications while migrating the infrastructure from a classic telephone network to an IP network.

? Integration of XML based applications

? CTI extensions to existing applications

Services for application partners

? Develop applications only once - OpenScape CAP guarantees compatibility with numerous telephone infrastructures using different technologies.

? Enhancement of individual applications with management, serviceability, and security features by using services provided by OpenScape CAP.

? Acceleration of application development by linking individual applications to HiPath / OpenScape applications. This transforms them into an integral part of the HiPath / OpenScape portfolio.

? Reduced training effort by using XML.

? Programming API with interactive development support for XML Phone Services.

? Harmonization of interfaces reduces development and sustaining effort.

? Additional business opportunities by leveraging large installed base.

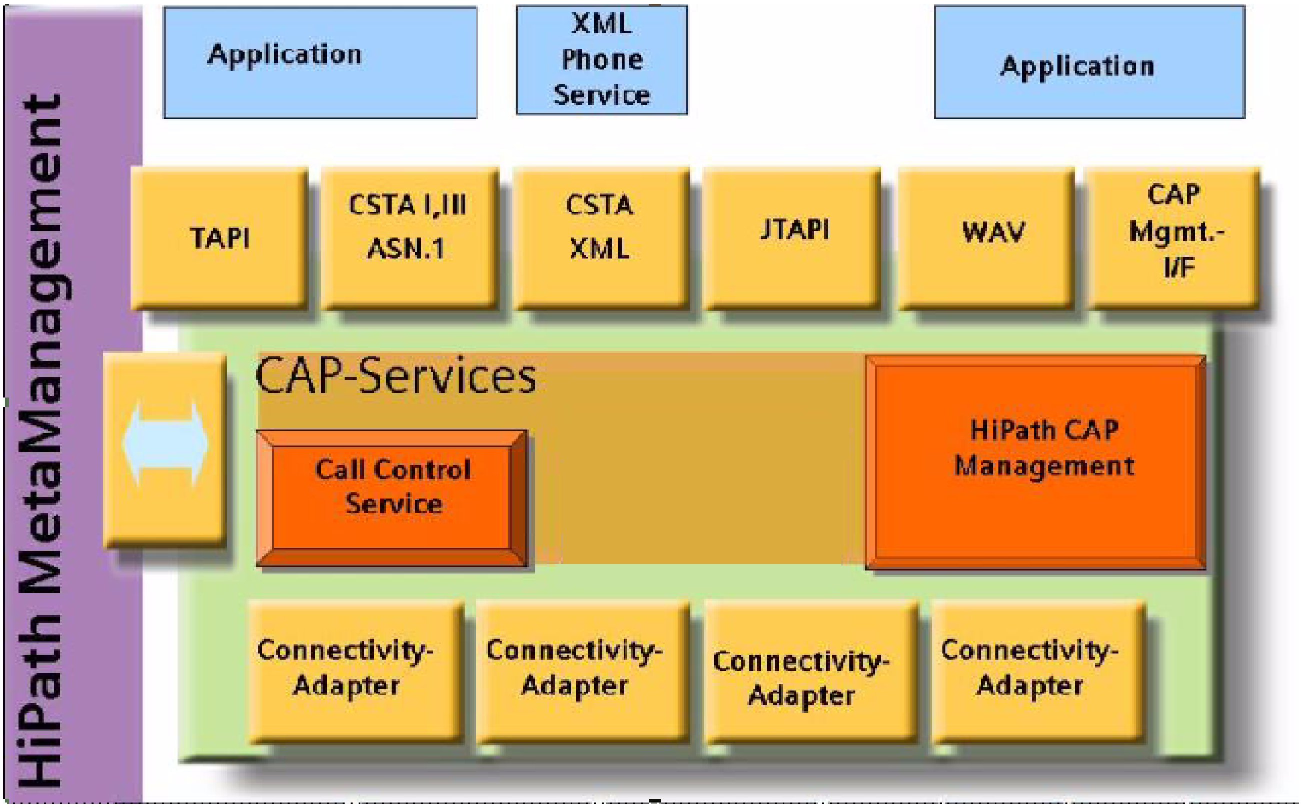
2.2 Features and overview of services

OpenScape CAP is a powerful middleware that offers modular scalability. It promotes effective improvements and reduces costs by supporting:

? standard APIs for application developers,

? application development through providing services for CTI, management, and licensing, available in an SDK (software development kit),

The following diagram shows the basic structure of OpenScape CAP with detailed information on protocols and encoding variants supported, CAP internal services, and a number of supported PBXs. **CSTA I is out of support**.



Highlights

? Standard protocols and APIs: Microsoft TAPI 2.2/3.1, JTAPI, CSTA III ASN.1, CSTA XML, Microsoft Wave API

? Call Control Service (SCC) for CTI

- Multi domain features

  – Harmonization of call models for HiPath 3000, HiPath 4000, OpenScape 4000, HiPath 5000, HiPath 8000, OpenScape Voice for TAPI and CSTA based applications

? Fault Management Service

  – Integration in OpenScape Management (independent of CAP Management)

? License, User, and Configuration Management services

  – Uniform license structure

  – Integrated license and user management

  – LM as a service for licensing OpenScape CAP and applications alike

? Support for special features

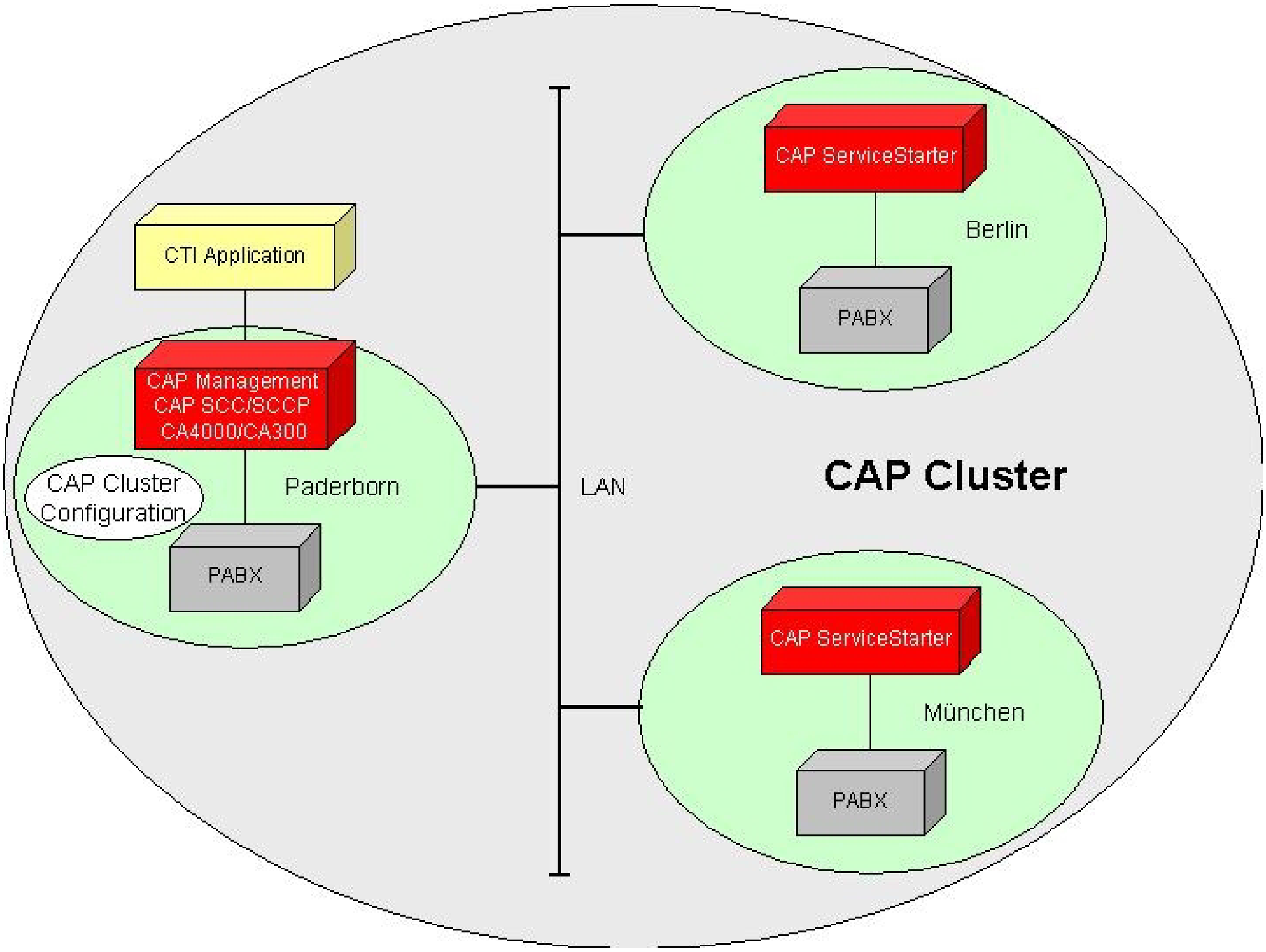
  – AP emergency (HiPath / OpenScape 4000)

  – XML PhoneServices (HiPath 4000)

2.3 OpenScape CAP Management

CAP Management is the central component in a CAP cluster. It administers and controls all processes and services in a local or distributed OpenScape CAP installation. The cluster ID is a unique identifier for CAP components in the same CAP cluster.

The following diagram illustrates the location and configuration of individual CAP components in a distributed installation.



CAP Management is started by the Windows service **OpenScape CTI** and provides a Web-based interface for administration. Under Linux it is started as /etc/init.d/cti process.

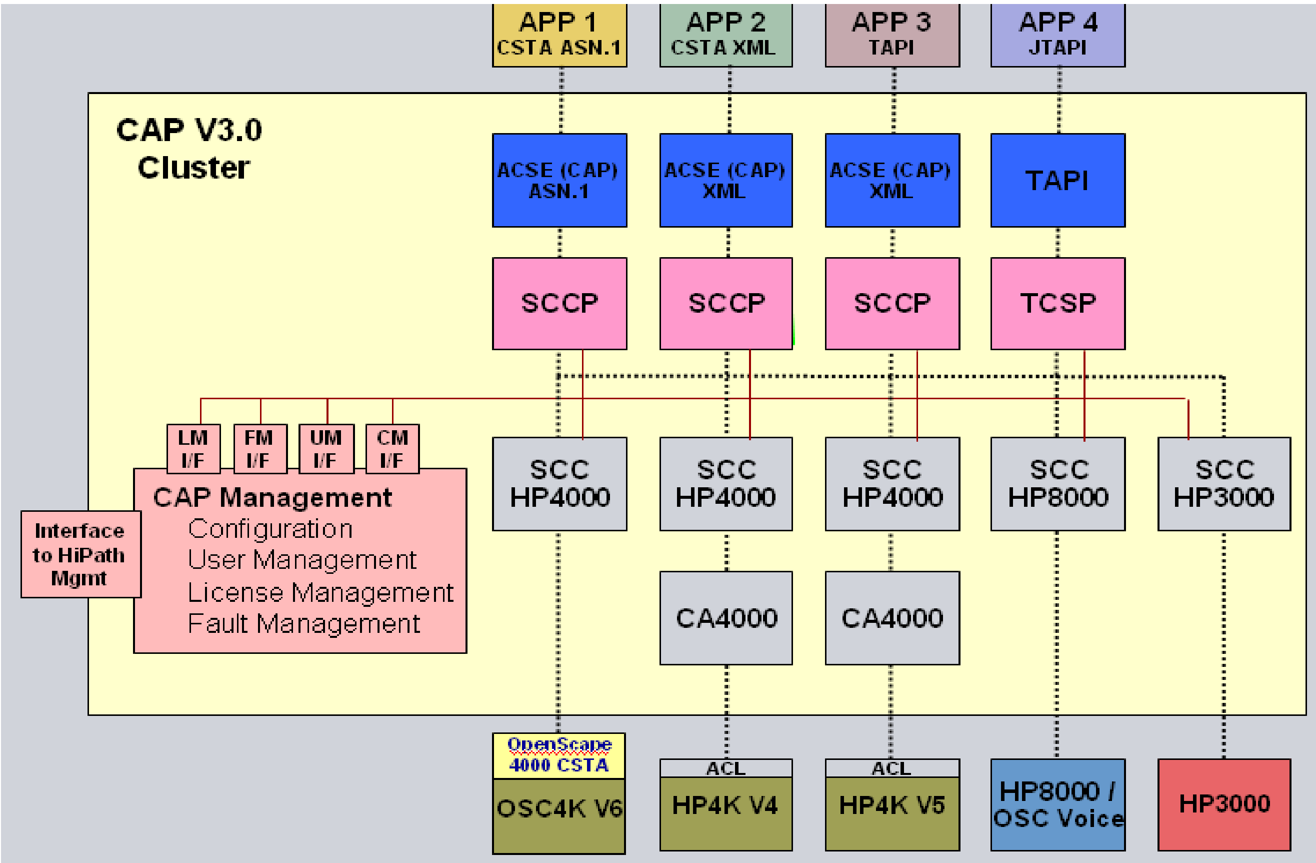
CAP Management tasks

- Administration of central and distributed components
- Administration of users
- Administration of devices
- Administration of licenses
- License verification and access control for users and devices
- Administration of status information associated with the various processes and services

OpenScape CAP Management services

CAP Management can be split into various services that have different tasks:

- Configuration Management (SCM)
- User Management (SUM)
- License Management (SLM)
- Address Translation Service (SAT)
- PBX Interface (SPI)
- CallIdRepository
- Open LDAP Server
- Fault Management (SFM) (independent of CAP Management)



These services are not installed separately but rather automatically using the **CAP Management** setup menu item. The only exception is OpenScape CAP Fault Management. This service will be dealt with later in greater detail.

Important OpenScape CAP Management services, such as SCM, SUM, and SLM can be addressed by HTTP requests. These are first used internally by other services (SCC, SCCP, CAP TCSP) without being directly visible to an application. Nevertheless, they can also be used by external applications so that the relevant features can be integrated there quickly and easily.

> To guarantee backward-compatibility, HTTP requests are still supported but are being phased out and gradually replaced by appropriate XML requests.

2.3.1 OpenScape CAP Configuration Management (SCM)

The various PBXs that are connected to the CAP are administered in OpenScape CAP Configuration Management. This is done by configuring a Call Control Service (SCC) for each individual PBX. This SCC is unique for each PBX type. To every SCC a unique service node ID is assigned that can be selected freely, except in cases where user data is imported from an external source which requires a specific ID for consistency. Similarly, a Call Control Service Proxy (SCCP) is configured and administered with a unique service node ID for applications in **multi domain mode**. For information on how to configure the components SCC and SCCP, and for description of additional OpenScape CAP Configuration Management facilities, see Chapter 6, "Configuration with OpenScape CAP Management", and Chapter 7, "Additional OpenScape CAP Management Functions".

An application can use the HTTP request
`http://<fqdn>:8170/mgmnt/admin/req?getPBXSvcAddr=<service node ID>`
to request the IP address and port number of an SCC based on the service node ID.

Extensions, hunt groups, ACD (RCG) groups of different PBXs are assigned different SCCs based on their device ID. The device ID is the long call number in canonical format (for example, +49(5251)8-27486). Trunks are configured in the same way. To administer them, they are also configured as devices with a device ID only known to the SCM. As the HiPath / OpenScape 4000 needs "LODEN" numbers for addressing purposes in hunt groups, trunks, and, RCG groups, the "Address Translation Service" (SAT) converts the device ID into a "LODEN" number.

An application can use the HTTP request
`http://<fqdn>:8170/mgmnt/admin/req?getServiceForDevice=<Device ID>`
to request the IP address and port number of an SCC to which a CSTA request should be sent for a certain device.

The components SCCP and CAP TCSP actively use this Configuration Management function. The Phone Controller in ComAssistant also uses the XML equivalent of this function as an external application.

2.3.2 OpenScape CAP User Management (SUM)

User Management is the main component of OpenScape CAP. Every CTI user must be configured in CAP User Management. Each user is administered using a unique user ID and assigned a password. You can also allocate users to devices/switching systems and assign access rights/ licenses to devices/users as described in Section 7.3, "User" and Section 7.5, "License Management".

CAP User Management can be linked to Windows User Management.

An application can use the HTTP request
`http://<fqdn>:8170/mgmnt/auth/req?authenticate=<user Id>&passwd=<Password>&encoding=B64`
to authenticate a user and the associated password.

The components SCCP, SCC, and CAP TCSP actively use this User Management function. The Phone Controller in ComAssistant also uses the XML equivalent of this function as an external application.

2.3.3 OpenScape CAP License Management (SLM)

License Management is used by OpenScape CAP components and applications based on OpenScape CAP.

License keys can be installed by selecting the appropriate menu options. These license keys include an application ID and the number of client licenses available.

Demo licenses are available.

The license keys CAP-E (Entry), CAP-S (Standard), and CAP-A (Advanced) enable associated client features. Additionally, application-specific licenses can be used as well. These are equivalent to CAP-A licenses. They are used e.g. by OpenScape CTI applications SimplyPhone for Outlook (SimplyPhone O), SimplyPhone for Lotus Notes (SimplyPhone N), and ComAssistant. "XPhone" (c4b) is the first external application to use CAP License Management.

A license is assigned to a device. Licenses can be assigned in the course of device configuration or through automatic assignment during license verification; they remain assigned to the device afterwards.

License variants

Entry client (CAP-E)	Only the "MakeCall" feature is supported.
Standard client (CAP-S)	All features are supported with the exception of ACD features.
Advanced client (CAP-A)	All features are supported including ACD features.
Linux client (CAP-L)	In addition to a CAP-E / CAP-S / CAP-A or application-specific license, a CAP-L license is required in case the CAP installation is hosted on a Linux server.

The following table provides an overview of the various marketing packages.

License	**per channel**	**1**	**10**	**25**	**100**	**site >500**
Entry / CAP-E			X			
Standard / CAP-S			X	X	X	X
Advanced / CAP-A			X	X	X	X
Linux / CAP-L		X	X	X	X	X
Media FAX / CAP-FM	X					
Application License	for internal applications - HiPath ProCenter / OpenScape Call Canter Application - HiPath SimplyPhone family - HiPath Com Assistant - etc. and for selected OEM applications Application license implicitly includes CAP client license					

Initially, an application must register itself to CAP (authentication) by providing an application ID. This application ID must match one of the installed licenses. License verification is performed for every request sent by this application to the CAP for a specific device. If the relevant client license has been assigned to this device, the request is forwarded to the PBX.

Please note that CAP-L licenses are claimed implicitly by CAP software depending on the installation environment; an explicit registration for CAP-L is not required nor reasonable.

The CAP components use the HTTP request
`http://<fqdn>:8170/mgmnt/admin/req?registerLicense=<ApplicationID>&userId=<DeviceID>`
to check if a device has been assigned the required license before they can forward a request. External applications can also use the same request or its XML equivalent to check if a device configured in the specific application has been assigned an appropriate license.

Conclusion: License verification is always performed.

Exceeding the number of client licenses

If the number of client licenses installed for an application is exceeded, temporary licenses with two-month validity are assigned. At the same time, notification is sent via e-mail to a specific e-mail address. All temporary licenses are marked by a "*". When the period of validity expires, requests for these devices are rejected.

2.3.4 Address Translation Service (SAT)

The "Address Translation Service (SAT)" is responsible for always managing the phone numbers in international or canonical format in communication between an application and the SCCP or the SCC. Canonical and international formats have been specified in the ECMA CSTA III Standard.

? It converts a dialed number from international or canonical format into a diallable number. The "Overlapping" between extension and a part of the LDC (Local Destination Code) is considered.

? It converts the phone number of the monitored device from an international / canonical format to a format the PBX can handle. Here, "Overlapping" is considered too.

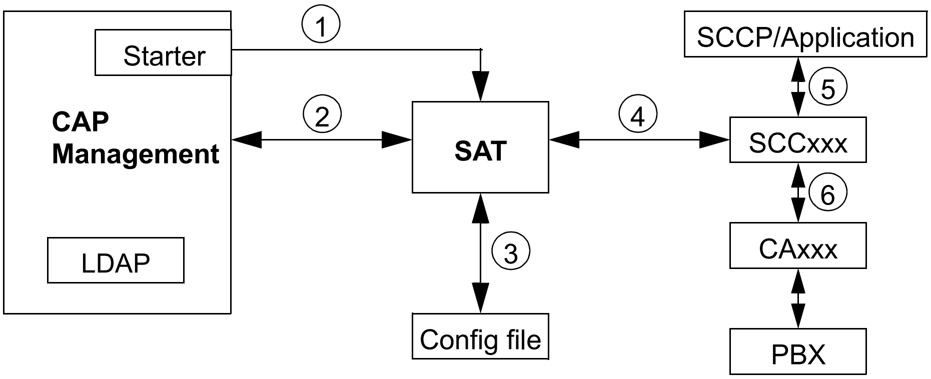
? It converts the phone number transmitted in an event or in a response from the formats "extension", "NAC number" (Node Access Code precedes number), "PNP number" into canonical format so that an application can always uniquely assign this event to a device, can search in a corporate directory or can perform a call.

? For addressing non-station devices (trunks, hunt groups, route control groups) on HiPath / OpenScape 4000, it converts the switch internal identification ("LODEN") to the number configured in CAP.

? For a succesful SAT conversion all of the devices must be configured in CAP database. There's only one exception to this rule: devices with VNR number which do not appear in canonical form in any C->S direction CSTA message and the required setting is activated. (For a detailed description see CAP ADG Vol. 1 Chapter 4.1 SAT and Chapter 5.6 Non-unique numbering plan.)

For downward compatibility, a legacy mode has been introduced. In legacy mode address conversion is switched off, so CAP3.0 behavior concerning devideIDs is the same as in CAP2.0. Legacy mode can be set for the whole CAP installation or for specific SCCs. It cannot be set for specific applications, however. Activation / deactivation is controlled by configuration files (see Section A.2.15). Changed configuration settings become effective only after restarting the service.

The following diagram shows the integration of SAT in CAP V3.0 (interfaces 1, 2, 3, 4) as well as additional interfaces affected by SAT (5, 6).



IF1: SAT is started by the CAP Management Starter service and cannot be stopped and restarted using the Diagnose Agent, only can be restarted by restarting the whole OpenScape CTI service.

IF2: On startup, SAT retrieves the list of SCC data from CAP Management. In case of modifications, CAP Management notifies SAT and passes the modified data (push). SAT retrieves device data as well from CAP Management in specific situations.

IF3: On startup, SAT gets configuration data like TCP port, log level or "Legacy Mode" from the SatServer.cfg config file.

IF4: Conversion orders and conversion results are exchanged between SAT and SCC via this XML interface. By default, port 8999 is used for this communication; a different port can be set in the config file (see Section A.2.15, "SAT configuration files").

XML commands may contain tags as follows:

? ConvertToDiallable:
convert international / canonical number to PBX diallable format

? ConvertToSFR
convert international / canonical number to PBX SFR format

? ConvertToSwitchFormat
convert international / canonical number or trunk to respective PBX format (like the LODEN for trunks)

? ConvertToPbxDeviceNumber
convert a trunk identified by network wide canonical number to the respective PBX format (like LODEN)

? ConvertToCanonical
convert PBX specific number or trunk identifier (like LODEN) to international / canonical number or trunk identifier

- SatEntry - embracing subsequent tags
- DeviceID
  number in CSTA III format, including all sub tags like typeOfNumber
- CallingCalledInfo
  call control characterization of number; possible values are CallingIncoming, CallingOutgoing, CalledIncoming, CalledOutgoing
- CallingPbxId
  identification of respective PBX in CAP Management (termed SccId there)
- PerformedInfo
  feedback for conversion; possible values are OKCanonicalNo, OKDialingNo, OKSFR, OK-DeviceNumber, NoTransMgmt, NoTransParam, OKAlreadyFormatted

IF5: This interface has been available in CAP V2.0 already. In case "Legacy Mode" has been switched off, CSTA device IDs will be modified here by SAT invocation.

Coming **from** an application, CSTA III deviceID formats are supported as follows:

- Dialing number, canonical format (e.g. +49(89)722-1234)
- Dialing number, international format (e.g. +49897221234)
- SFR number, canonical format (e.g. N+49(89)722-1234)
- SFR number, international format (e.g. N+49897221234)
- SFR number with name, canonical format (e.g. N<+49(89)722-1234>John Doe)
- SFR number with name, international format (e.g. N<+49897221234>John Doe)
- Other formats without preceding + sign are not converted by SAT but passed on to the PBX without modification.

Going **to** an application, CSTA III deviceID formats are supported as follows:

- SFR number, canonical format (e.g. N+49(89)722-1234)
- SFR number, international format (e.g. N+49897221234)
- SFR number with name, canonical format (e.g. N<+49(89)722-1234>John Doe)
- SFR number with name, international format (e.g. N<+49897221234>John Doe)
- In case a number received from the PBX cannot be converted, it is passed on to the application without modification. In this case, "typeOfNumber" is set to "dialingNumber" or "other" depending on whether a dial string has been detected or not.

IF6: This interface has been available in CAP V2.0 already. It is not affected by SAT operation - no adaptations are required in CAs or PBXes.

Please note that for successful address conversion in SAT it is indispensable to have PBX / SCC data (like country codes of communicating PBXes) properly configured in CAP Management.

A CallingIncoming number originated in a foreign PBX can be converted

– if it is a public number (like 0030..., incoming call from Berlin)

– if it is mapped in a PBX specific numbering plan, a private numbering plan (PNP) or as an extension in case the respective device has been configured in CAP Management (e.g. 991234, with 99 as inter-PBX dialing code)

In case you need address conversion throughout a PBX network even for devices / PBXes that are not managed through CAP, it is required to configure "virtual SCCs" and import all of the devices for these PBXes. See Section 6.5 for details.

For successful translation from diallable number to international or canonical format, it is important that the exit code for national/international calls configured for a switch must not be used as leading part of any device number on that same switch (e.g. for a switch using "20" as exit code, no device with a number starting with "20..." is allowed in that switch).

2.3.5 PBX Information

The PBX information service (SPI) is a new service to facilitate data synchronization between CAP and PBX. Complementing the import facility which is based on import *files* to be provided by external sources, SPI establishes a direct connection to the PBX administration to retrieve user and device data without need for intermediate files.

SPI can be invoked from the CAP Management GUI; it is currently supported for HiPath / OpenScape 4000 connectivity only (see Section 6.2.3).

2.3.6 CallIdRepository

The internal "CallIdRepository" service is not directly visible for any application. Its task is to administer the call ID originally assigned throughout its existence (from start to finish) and to forward it to an application over the SCC.

This service has been provided for HiPath / OpenScape 4000 connectivity only; it is not required except for very specific application scenarios. Accordingly, it is switched off by default.

2.3.7 Open LDAP Server

The "Open LDAP Server" manages all configuration data for the CAP.

2.3.8 OpenScape CAP Fault Management (SFM)

Although OpenScape CAP Fault Management is provided on the OpenScape CAP CD for strategic and sales reasons, it should still be considered fully separate from the other OpenScape CAP services. Information on OpenScape CAP Fault Management is contained in a separate manual, the "OpenScape CAP Fault Management Developer’s Guide"; installation and configuration are also dealt with there.

OpenScape CAP Fault Management consists of six DLLs. Rather than a stand-alone service, it is connected to the Windows SNMP service. Windows-based programs can be managed by OpenScape Fault Management by integrating these DLLs. An ADG is provided for this.

CAP FM supports the following features:

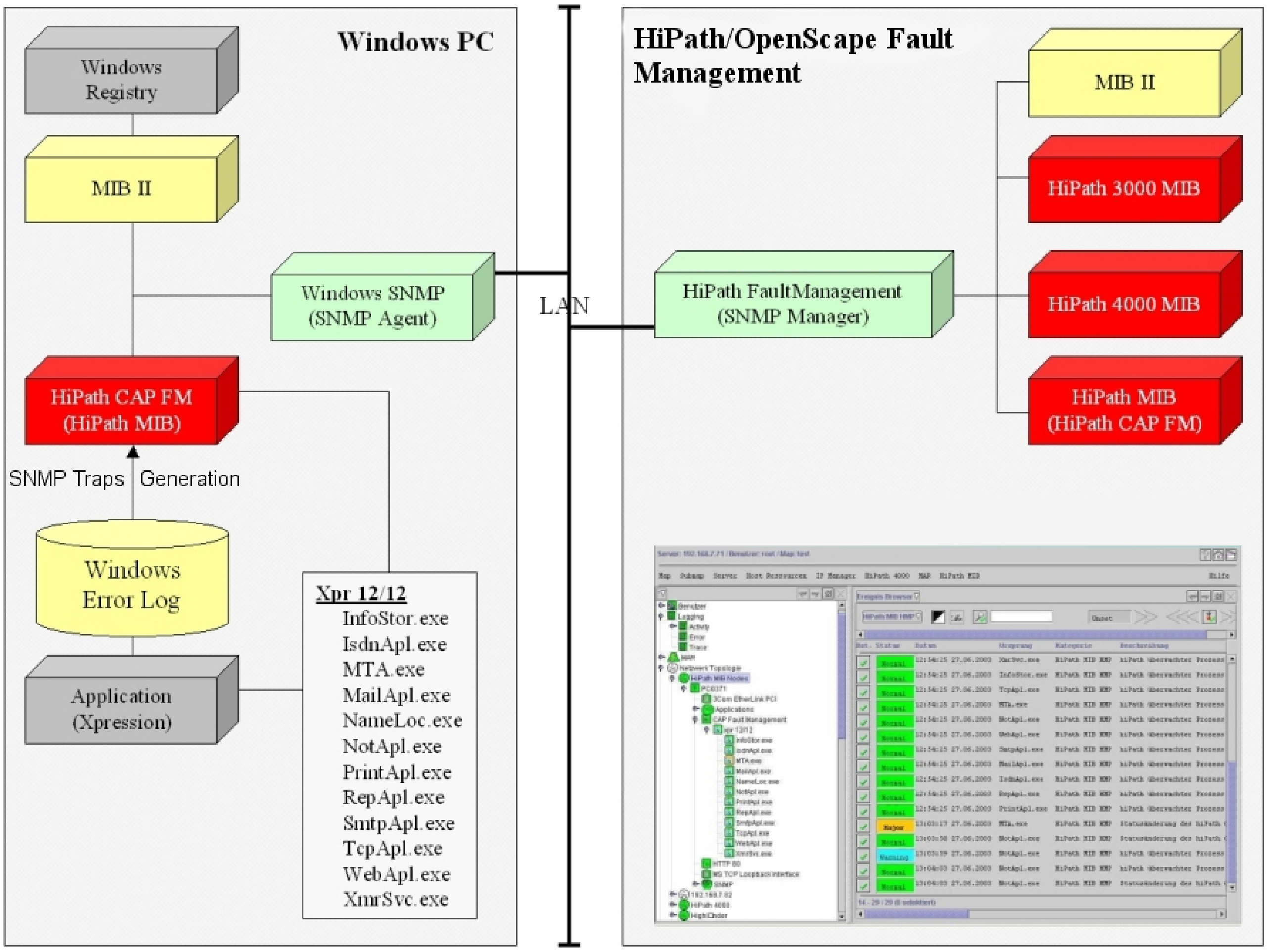
? Auto Discovery

? OpenScape MIB-based information

? Trap notification

In addition to the information available via MIB II, OpenScape Fault Management contains information on the CAP FM applications supported and the processes to be monitored. In the OpenScape Fault Management direction, traps are either forwarded over the CAP FM SNMP agent or the CAP FM agent creates them based on specially marked messages in the Event Log window.

The following diagram provides an illustration of Auto Discovery initiated by OpenScape Fault Management for a Windows PC with an active SNMP agent, Xpressions 450 installed, and integrated OpenScape CAP FM.



Administration of CAP with OpenScape Fault Management

CAP provides an XML interface that is automatically recognized by OpenScape Fault Management. A connection to the OpenScape CAP Diagnostic Manager is set up over this interface. Information on the statuses of the various CAP processes are cyclically retrieved by OpenScape Fault Management and displayed on the FM desktop. There is also a direct link to the Diagnostic Agent in OpenScape Fault Management.

2.4 OpenScape CAP operating modes

OpenScape CAP supports two different operating modes:

Single domain native mode

HiPath / OpenScape 4000 with CSTA III ASN.1 interface only

Multi domain harmonized mode

CSTA III ASN.1, CSTA XML, Microsoft TAPI, JTAPI, Microsoft WAVE API (HiPath 3000 and HiPath / OpenScape 4000 only), XML Phone Service (HiPath 4000 only)

The PBXs, protocols, and encoding variants supported differ depending on the operating mode. For details on the individual operating modes, see Chapter 9, "Operating Modes".

For detailed information on the services supported, refer to the OpenScape CAP Prospect, the OpenScape CAP Technical Information, or the OpenScape CAP ADG. These documents provide an explicit list of all services supported for the individual PBXs in "native mode" and "harmonized mode" for the various protocols and encoding variants.

2.4.1 Explanation of terms

Single domain	Only one PBX, SCC connection.
Multi domain	One or more PBXs, SCCP connection, different types of PBXs possible
Native mode	Proprietary protocol elements of CSTA, standard and private services are supported.
Harmonized mode	Only standard CSTA services are supported.

Single domain native mode is used for the CTI connection of existing applications without the need for changes in the application software. The application is unable to detect the presence of OpenScape CAP.

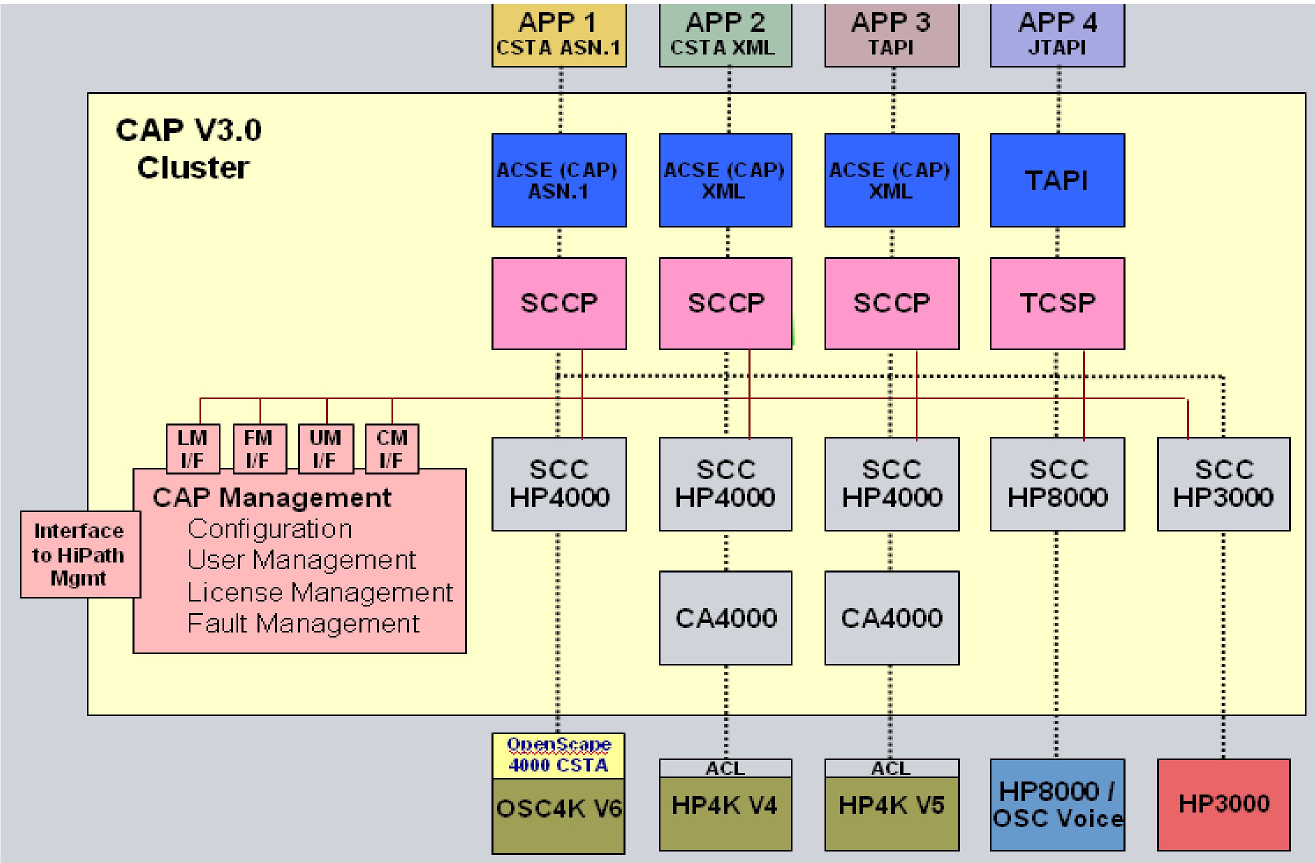
Multi domain harmonized mode is used in modified form by the Phone Controller in ComAssistant. CAP TCSP uses it too. Additional applications are currently being developed. An application must support CAP’s new ACSE_AARQ, extensions in long canonical format, and call IDs containing eight bytes.

2.5 OpenScape CAP components

The components SCC, SCCP, CA4000 and CAP TCSP offer a number of combination options for setting up connections between an application and various PBXs.

The following diagram is a structural illustration of CAP in "multi domain harmonized mode".

H300 is out of support.



2.5.1 Call Control Service Proxy (SCCP)

SCCP is a CAP component that supports "multi domain mode". SCCP provides a TCP/IP connection port for applications. The first request to the SCCP after connection setup must be ACSE_AARQ.

This includes:

- User name
- Password
- Application ID
- CSTA version
- Native mode = true/false

An application must authenticate itself at SCCP with a valid CAP user name/password. The SCCP uses CAP Management's SUM component for this.
SCCP saves the application ID for client licensing of subsequent requests; it uses CAP Management SLM for this. The SCCP saves successful CTI user license verification actions for 3600 seconds.
The CSTA version defines the type of CSTA III encoding in which the following requests are transmitted.
The CSTA XML protocol is used for communication with the JTAPI application. The JAR files supplied by CAP must have been imported by these applications for this.
Native mode = true/false defines whether the following requests contain proprietary protocol elements and if extended scope and "private services" should be supported.

SCCP configuration parameters

An SCCP is not set to "native mode" or "harmonized mode" by configuration. Instead, the various operating modes are activated by the identifier "native mode = true/false" in ACSE_AARQ.

Different SCCP positions are defined with configuration parameters:

For the application	An application connects to an SCCP over an IP address and a port opened by SCCP.
Local position	The name of the CAP cluster PC on which the SCCP should run.
To the PBX	The direction cannot be configured. An SCCP only connects to SCC instances. It determines the IP address and the associated port of an SCC through the CAP Management SCM. To do this, the extension must be transmitted in long canonical format for every initial request.

2.5.2 The Call Control Service (SCC)

The SCC is a CAP component with a connection to a PBX. An appropriate SCC variant is used for each of the PBX types supported by CAP.
Every SCC is managed by a configured service node ID. This ID must be unique and can be random except in cases where user data is imported at a later point. Additionally, every SCC is assigned the call numbers of the PBX connected.

SSC configuration parameters

In **multi domain mode**, the protocols and the encoding variants CSTA III ASN.1, CSTA XML are supported in the SCCP direction while NetTSPI is supported in the CAP TCSP direction.

In **single domain native mode**, applications are linked directly to an SCC (HiPath / OpenScape 4000 only). The SCC4000 is permanently configured in one of the protocol variants "CSTA III ASN.1" or "ACSE (CSTA III ASN.1)".

Different SCC positions are defined with **configuration parameters**:

For the application	An SCCP, CAP TCSP or an application connects to an SCC over an IP address and a port opened by the SCC.
Local position	The name of the CAP cluster PC on which the SCC should run.
To the PBX	The direction to a PBX is defined on the basis of an IP address and port number connected to SCC. SCCHiPath3000 connects directly to the HiPath 3000. HiPath 3000 can also be connected over S_0 and V.24. SCCHiPath4000 connects to CA4000.

2.5.3 The Connectivity Adapter 4000 (CA4000)

CA4000 converts the proprietary HiPath 4000 CTI protocol (ACL-C+) into a standardized protocol (CSTA). The connection to HiPath 4000 can be set up over ATL, the WAML and the SL100/200. CA4000 supports CSTA III or ACSE (CSTA III) links in ASN.1 encoding. CA4000 is always configured together with the associated SCC in CAP Management.

CA4000 configuration parameters

The IP address of HiPath 4000, a PBX link number, and a sub-application number are configured for communication with HiPath 4000. For SCC - CA4000 communication, an IP address as well as a port (1025 - 5000) is configured.

> PROBLEMS WITH CA4000 AND WINDOWS SERVICES:
> Note that Windows Task Scheduler and the Windows logon service seize ports in the range 1025 - 1299 which can change every time the relevant service is restarted.

2.5.4 The CAP TAPI Service Provider (CAP TCSP)

CAP TCSP is a CAP component that supports "multi domain harmonized mode". It provides the TAPI Service Provider Interface (TSPI) to applications based on Windows TAPI. Its multi domain capability is based on the use of CAP SCM; it communicates directly with the SCC over a proprietary protocol (NetTSPI). Simultaneous connection with multiple SCCs is supported.

CAP TCSP configuration parameters

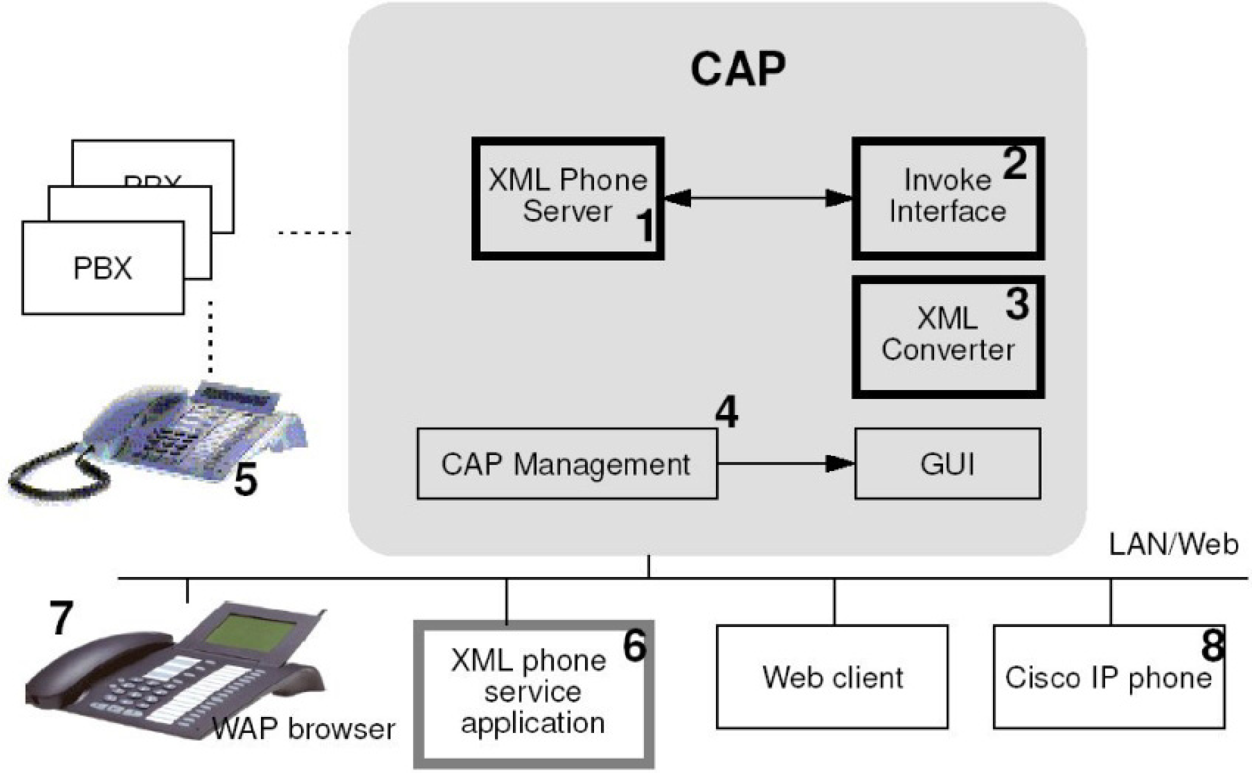
CAP TCSP is installed via a separate setup facility (setupTapi.exe). After installation, it appears in the Advanced tab under "Phone and Modem Options" and is started via the Windows "Telephony" service.

Configuration parameters include the IP address or the PC name of the CAP Management computer and the CAP Management port number (default 8170). The various lines are configured with the device ID (long call number in canonical format). They must be configured in the SUM. Automatic synchronization is possible between CAP TCSP lines and all CTI users configured in CAP. However, this is only advisable if required by a corresponding application. Like an external application, CAP TCSP uses the SUM for authenticating users (devices). Default passwords must be modified during initial login. A connection is not set up with SCC until after successful authentication. Client licensing is automatically performed by an internal SCC routine. This starts linear with the application ID "CAP-A", "CAP-S" and ends with "CAP-E". TAPI applications can supply individual application IDs for licensing.

2.5.5 The XML Phone Service (XMLPS)

"XML Phone Service (XMLPS)" is an application based on an SCCP configured in CAP. It provides a new XML interface for external applications. XML applications use the standard HTTP/HTTPS protocol for communication with the XMLPS. XMLPS applications can use terminals associated with a HiPath 4000 or HiPath 3000 as input/output devices (e.g. OpenScape uses XMLPS). WAP terminals (for example, optiPoint 600) or mobile phones can use an optional WML adapter to access these applications. The XML Phone Service consists of three main components:

- **OpenScape CAP XMLPS Phone Server Process** (sxmlps.exe)
  This process is the component that connects to SCCP
- **OpenScape CAP XMLPS Invoke Interface**
  This interface is used to operate the terminals (display, key LEDs)
- **OpenScape CAP XMLPS Converter Servlets**
  The converter consists of Java servlets that convert XML into WML. Cisco WAP Phone conversion is also supported (CAPPhone Syntax to CiscoPhone Syntax, CiscoPhone Syntax to CAPPhone Syntax).



The XML Phone Server operates as a browser and treats the terminals as endpoints with:

? a two-line display,

? audio indicator (beep),

? application keys with associated LED,

? menu item selection keys,

? OK key,

? the normal keypad as an alphanumeric keypad.

If an application key is pressed at the terminal, the XML phone application starts by calling the configured URL that is associated with this button in the CAP. In response, the application uses the invoke interface to send a CAPPhone object (as a HTTP response with the MIME type: XML) that should be processed for the terminal where the button was pressed.

The application can

? show a text message on the display,

? generate a signal tone,

? set the LED status.

The XML Phone Service comes with a number of simple but useful applications named "**On A Button Suite"**:

? **EasyLookup**
Allows searching in an LDAP directory without using a PC. In a call, the function retrieves available information on all parties involved in the call from the LDAP directory. Otherwise, a manual search for names or phone numbers in the LDAP directory is possible. Names and, where applicable, additional information is presented on the phone display. Available information may be used for dialling an outgoing call as well.

? **Easy See**
At the push of a button, data on all parties involved in a call is retrieved from the LDAP directory and is presented as a "phone card" on the PC.

? **EasyShare**
Starts NetMeeting on all PCs assigned to the parties connected via the call (over SysTray).

? **EasyMail**
Opens a new e-mail for all parties connected via a call.

? **EasyConference**
Allows for creating / joining conferences via your phone; for proper operation, it requires an MMCS board to be installed in your HP4000. It operates with MMCS "Master Conference Rooms" only, providing the conference master with a convenient interface for controlling the conference. Other parties involved in the conference do not need the EasyCon-

ference application. The master gets a notification on his/her phone by display, sound and a flashing EasyConference key as soon as the first party has entered the conference room. The master has the option to
- enter the conference room
- display parties currently present in the conference room
- remove single parties from the conference.

Additional information on the XML Phone Service is available in the XMLPS Application Developers' Guide which comes with the CAP documentation; after CAP installation, it is available online as well via the URL `http://<CAP host>:8172`.

3 System Requirements

This chapter describes all hardware and software requirements for installing OpenScape CAP. Some CAP components may be installed both on the central server PC and on remote or client PCs. The complete installation procedure is described in Chapter 4, "Installation".

3.1 Hardware requirements

The following is a list of the hardware requirements for the server PC and for the remote PCs (if any). All affected PCs must be connected to a common network.

3.1.1 Central server PC (for CAP Management)

All OpenScape CAP server components must be installed on the central server PC (for example, OpenScape CAP Management or the CAP Call Control Services).

Minimum requirements

? processor with at least 2GHz

? At least 1 GB main memory

? Approx. 1 GB free hard disk place (10 GB is recommended for an adequate logging)

NOTE: If VM-Ware is used, then the minimum requirement of CAP is not 1GB, but 2GB memory.

Depending on the structure of your system, we recommend opting for over-equipped PCs rather than under-equipped ones that fall short of the minimum requirements. The following table outlines which PCs should be used for which configuration levels:

Configuration	**PC type**
Call Control	
no	A
small	A
medium	A
large	B
very large	C

Call Control

? small up to 100 users

? mediumup to 500 users

? large up to 2,000 users

? very largeup to 20,000 users

PC type

? A 2 GHz / 1 GB RAM / 40 GB HD (minimum requirement)

? B 2 GHz / 4 GB RAM / 60 GB HD (minimum requirement)

? C Distributed system consisting of PC types B or multiprocessor power PC with at least 8 GB RAM

3.1.2 Client PCs (for CAP ServiceStarter)

Client PCs are additional network-based PCs on which CAP ServiceStarter is installed in distributed installation scenarios. They can include OpenScape CAP components, such as call control services or connectivity adapters. Requirements depend on the number and type of components to be supported. Thus the following data is only provided as a guide. In addition, CTI applications also run on the client PCs.

Minimum requirements

? at least 1,6 GHz CPU

? At least 1 GBmain memory

? Approximately 800 MB of disk space

3.1.3 Communication system

Ensure that the communication system (e.g. HiPath / OpenScape 4000, HiPath 3000, etc.) with which OpenScape CAP is to operate is fully functional. One of the connection options supported by the communication system and OpenScape CAP must be available (for example, over a TCP/IP connection).

3.1.4 VMware requirements

The following tables summarizes the VMware requirements for CAP 3.0 SMR13 and SMR14 release in case the system is set up in a virtual environment.

OpenScape CAP Management V3.0 SMR13 and SMR14		
General Product Info	Operating System	Please see the Release Notes for the current supported Windows versions.
	Native Redundancy Support	No
	Redundancy Strategy	-
	Voice/Video Media Terminating	No
	Voice/Video Signalling Traffic	No
	Other Real-Time critical requirements	No

Table 3-1 Supported VMware features

OpenScape CAP Management V3.0 SMR13 and SMR14		
VM Feature Compatiblity	vMotion Support	Yes **Restrictions / Limitations:** vMotion should not be used during business hours on high load system.
	High Availability (HA) Support	Yes
	Fault Tolerance (FT) Support	No
	Site Recovery Manager (SRM) Support	Yes **Note:** All VMware requirements (incl. Hardware) and best practices have to be fulfilled. The network between the data center sites has to be a transparent layer 2 network which provides identical enviroments in both locations.
	Backup with vStorage-APIs for Data Protection	Yes **Note:** vStoreage APIs can be used as an additional backup layer for image level backups that allow to restore vitual disk contents after a disk failure fast.The standard backup mechanism normally used in physical deployments have to be applied in addition.
	VMware Tools Support	Yes **Note:** Installation of VMware Tools is recommended.
	Virtual Appliance (vApp) Support	No

Table 3-1 Supported VMware features

OpenScape CAP Management V3.0 SMR13 and SMR14									
		Smallest	**Depl. 1**	**Depl. 2**	**Depl. 2**	**Depl. 3**	**Depl. 3**	**Depl. 4**	**Depl 4.**
Depl. Scenarios	Depl. Scenario	Single Node	Single Node	Multi Node	Multi Node	Multi Node	Multi Node	Multi Node	Multi Node
	Number of Nodes	1	1	Frontend Server	Backend Server	Frontend Server	Backend Server	Frontend Server	Backend Server
	Max Users	500 Users	5.000 Users	10.000 Users	10.000 Users	30.000 Users	30.000 Users	50.000 Users	50.000 Users
vCPU	vCPU	1	2	1	2	1	2	1	2
	vCPU Freq. (min)	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz
	vCPU Shares	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal
	vCPU Reserv.	0	0	0	0	0	0	0	0
		Issues resulting from CPU contention cannot be addressed towards the application.							
	vCPU Limit	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
vRAM	vRAM	2 GB	2 GB	2 GB	2 GB	4 GB	4 GB	4 GB	4 GB
	vRam Shares	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal
	vRam Reserv.	2 GB	2 GB	2 GB	2 GB	4 GB	4 GB	4 GB	4 GB
	vRAM Limit	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited

Table 3-2 VMware requirements for different deployments

OpenScape CAP Management V3.0 SMR13 and SMR14									
		Smallest	**Depl. 1**	**Depl. 2**	**Depl. 2**	**Depl. 3**	**Depl. 3**	**Depl. 4**	**Depl 4.**
vNIC	vNIC (No. Req‘d)	1	1	1	1	1	1	1	1
	vNIC Type	VMX-NET3	VMX-NET3	VMX-NET3	VMX-NET3	VMX-NET3	VMX-NET3	VMX-NET3	VMX-NET3
	vNIC Manual MAC (See note)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Network Bandwitdth (estimated reqm‘t)	400 Kbsp	400 Kbsp	400 Kbsp	400 Kbsp	400 Kbsp	400 Kbsp	400 Kbsp	400 Kbsp

Table 3-2 VMware requirements for different deployments

OpenScape CAP Management V3.0 SMR13 and SMR14									
		Smallest	**Depl. 1**	**Depl. 2**	**Depl. 2**	**Depl. 3**	**Depl. 3**	**Depl. 4**	**Depl 4.**
Storeage (vDisk)	vDisk (No. Req‘d)	1	1	1	1	1	1	1	1
	vDisk Size	60 GB	60 GB	60 GB	80 GB	135 GB	265 GB	135 GB	265 GB
		vDisk Size is the total amount of storeage needed for the operating system, the application, and the application data.							
	vDisk Mode	Snapshot	Snapshot	Snapshot	Snapshot	Snapshot	Snapshot	Snapshot	Snapshot
	vDisk Format	thick layz-zeroed	thick layz-zeroed	thick layz-zeroed	thick layz-zeroed	thick layz-zeroed	thick layz-zeroed	thick layz-zeroed	thick layz-zeroed
	Addt‘l Storage	NO	NO	NO	NO	NO	NO	NO	NO
	Storeage Throughput (estimated reqm‘t)	~200KB/s per SCC	~200KB/s per SCC	~200KB/s per SCC	~50KB/s per SCC	~200KB/s per SCC	~50KB/s per SCC	~200KB/s per SCC	~200KB/s per SCC
	Storeage throughput depends on log level and load.								
	Storeage IOPS (estimated regm‘t)	2 per SCC	2 per SCC	2 per SCC	2 per SCC	2 per SCC	2 per SCC	2 per SCC	2 per SCC
	Maximum 10 SCCs are allowed per Frontend server.								

Table 3-2 VMware requirements for different deployments

3.2 Software requirements

The following is a list of the software requirements for the server PC and for the client PCs (if any).

3.2.1 Central server PC / client PC

Operating system

? Please see the Release Notes for the current supported Windows versions.

? SuSE Linux Enterprise Server (SLES) 10

? SuSE Linux enterprise Server (SLES) 11

Web browsers

It is recommended that a Web browser be available on the server PC for tests and configuration tasks after initial installation.

3.2.2 WEB client PC

> PCs that set up a connection to OpenScape CAP Management are known as WEB client PCs. These are **not** the PCs on which the CAP ServiceStarter is installed!

Operating system

The operating system on the client PC is not subject to any restrictions. As well as Windows operating systems, you can also use UNIX, Linux, MacOS, etc.

Web browsers

? Internet Explorer 8.0 and above

? Firefox 10.x and higher

? Chrome 24.x and higher

REMARK: Problems might occur with the newest versions of Internet Explorer (version 10 or 11). It is recommended to use the Compatibility mode.

The Web browser must support and permit JavaScript and cookies. Internet Explorer must be set so that every time a page is loaded it checks whether a new version of this page exists (can be set under **Tools | Internet Options | Temporary Internet files | Settings | Check for newer versions of stored pages: Every visit to the page**).

> > CAP Management operation is only guaranteed with the named browser versions. Please note that Netscape is no longer supported.

3.3 Additional installation prerequisites

? The host name mustn't include any non-standard characters. Standard characters include letters(A-Z, a-z), digits(0-9), and hyphens(-).

? The host must have a fixed and valid IP address and be entered in the DNS.
Check that name resolution is correct using the DOS command `nslookup` and the input `<PC name>` or `<IP address>.`

? If there is more than one NIC installed on the PC, the first NIC must be connected to the customer LAN.
Check that the NIC binding is correct by sending a `PING` to the actual PC name. The IP address of the customer LAN should be sent back in response to this PING.

The NIC binding can be altered by selecting the menu item **Control Panel | Network and Dial-up Connections | Advanced | Advanced Settings | Connections**.

? If CAP Management is not installed on a server operating system, you must modify the system performance options via **My Computer | Properties | Advanced | Performance Options | Application response | Optimize performance for: Background services**.

? Please ensure that the cluster ID assigned to CAP Management is not used by another CAP Management server in the same IP network.

? For SMR13 and above Java requirements have changed significanlty. Due to licensing reasons there is no built in Java in CAP anymore. For the installation Java 7 is required to be preinstalled on the sytem.

? For an installation on a pretty recent Windows (latest security patches activated), problems with starting the CAP Management GUI may result as by default the Internet Explorer is set up with security setting “Allow META REFRESH” disabled. Please make sure to enable this setting.

? For an installation on Windows 2003 in case the available firewall has been activated, , the firewall blocks the multicast communication used within CAP.
Alternatives for proceeding:

  ? Deactivate the firewall (undesirable in most cases)

  ? Configuration of the firewall explicitly for CAP (see Section 4.9.3, "Firewall configuration for CAP"

  ? Add the name, the fullname and the IP address of the PC to the trusted sites of the Internet Explorer via **Tools | Internet Options| Security | Trusted Sites | Add.**

4 Installation

This chapter explains the entire installation of OpenScape CAP. Unlike earlier versions, the current version for Windows comes with an MSI installer package that allows for a standard installation as well as for an installation customized according to customer requirements.

The standard ("Complete") installation takes care of installing all available CAP components on the CAP server machine. Please refer to **Section 4.1**.

The customized ("Server") installation is targeted at the CAP server machine as well; it allows for individually selecting packages for installation. Details are described in **Section 4.2**.

For a distributed setup, remote CAP hosts must have the "Starter" installation. Details are described in **Section 4.3**.

The installation on Linux is described separately in **Section 4.4**.

Additional information presented in this chapter include:

? **Section 4.6** describes the general proceeding common to all installation tasks

? **Section 4.7** provides details of a distributed installation

? **Section 4.8** describes the start sequence for CAP processes in non-distributed and distributed installations

? Installation of additional components is described in **Section 4.5** (CAP TAPI Service Provider)

? **Section 4.9** covers special features during installation or maintenance

? **Section 4.10** describes how to uninstall OpenScape CAP

To increase transparency, only the "usual" installation tasks are explained here. There are cross-references to other chapters in this manual and to other manuals dealing with special aspects and troubleshooting in the event of problems during installation and configuration. Many of these aspects are covered in Chapter 8 and Appendix A.

7 Typical installation scenarios, including the relationship between SCCP and SCC are described in Chapter 2, "Overview".
Ensure to select an adequate scenario for the case in hand with an appropriate combination of SCCP and SCC variants.
The current version of OpenScape CAP Configuration Management cannot fully prevent a configuration of SCC instances that technically does not make sense.

Installation sequence

To configure OpenScape CAP correctly, you must follow a precise sequence of steps:

1. Obtain licenses for OpenScape CAP and applications.
2. Install OpenScape CAP following the procedures described below.
3. Configure switch connectivities as required, each of them including Call Control Services (SCCs) with suitable Connectivity Adapters (CAs) connected to the switching host.
4. You may have to configure SCCPs, depending on the application to be installed.
5. Install licenses via CAP Management.
6. Configure or import devices.
7. Configure or import users and assign devices.

In case an application is to be installed directly afterwards:

8. Install applications.

Requirements

Before starting the installation, you should check that the following requirements have been met:

? Do you have all licenses for OpenScape CAP?

? Has a Web browser been installed and configured correctly (Internet Explorer, FireFox, Chrome)?

? Does this browser support cookies and JavaScript? Are cookies allowed and is JavaScript enabled?

? Does the PC have a valid IP address, and is it administrated correctly in the DNS?

? The person performing the installation must have administrator rights on the PC.

4.1 "Complete" installation

This installation is targeted at the central CAP server; it requires the most disk space but basically runs easily without any additional interaction.

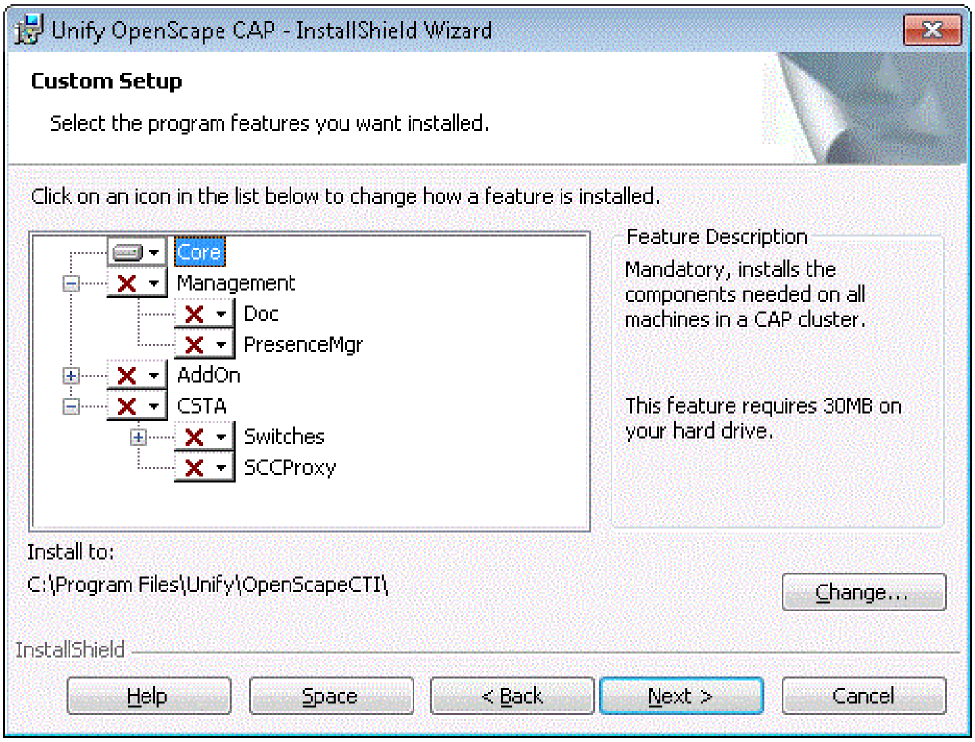
From the software directory on the CAP CD, invoke `setup.bat` to start the installation. When prompted for Setup Type, select "Complete" - all program features including optional features will be installed.

4.2 "Server" installation

This installation is targeted at the central CAP server; it allows for specific selection of required components.

From the software directory on the CAP CD, invoke `setup.bat` to start the installation. When prompted for Setup Type, select "Server" to install CAP Management and CSTA services as required.

During the installation process, a selection view is presented to determine components to be installed.



Unify OpenScape CAP - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

Feature Description

Mandatory, installs the components needed on all machines in a CAP cluster.

This feature requires 30MB on your hard drive.

Install to:
C:\Program Files\Unify\OpenScapeCTI\

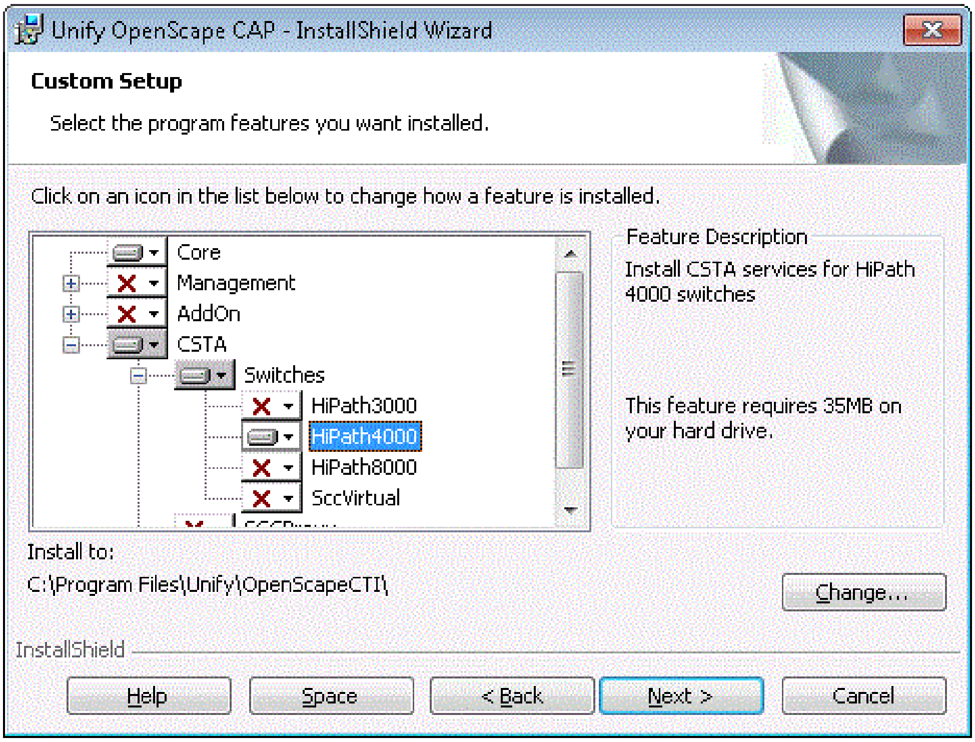
The **Core** package contains CAP Management services; it is indispensable and must not be deselected.

The **Management** package contains online documentation which is optional.

The **AddOn** package contains PhoneServices which is optional (see Section 2.5.5) as well as UMIntegration which is irrelevant as of today.

The **CSTA** package contains the selection of available switch connectivities as well as SCCP (see Chapter 6 for a detailed description of these components). Please note that by selecting one of the switches, all CAP parts required for connecting to that switch will be installed automatically. Separate handling of e.g. SCC4000 and CA4000 for connecting to the HiPath 4000 is no longer required.

A possible selection for connecting to HiPath 4000 only is shown in the diagram below.



Unify OpenScape CAP - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- Core
- ☒ Management
- ☒ AddOn
- CSTA
  - Switches
    - ☒ HiPath3000
    - HiPath4000
    - ☒ HiPath8000
    - ☒ SccVirtual

Feature Description
Install CSTA services for HiPath 4000 switches

This feature requires 35MB on your hard drive.

Install to:
C:\Program Files\Unify\OpenScapeCTI\

4.3 "Starter" installation

This installation is targeted at a remote host in a distributed CAP installation; it provides no selection facilities.

From the software directory on the CAP CD, invoke `setup.bat` as administrator to start the installation on the remote host. When prompted for Setup Type, select "Starter" - a CAP process starter instance will be installed.

4.4 Linux installation

> 7 Please note that CAP components must be installed completely on Linux or completely on Windows. "Mixed" Linux+Windows installations are not supported.
> The description below covers particularities of the Linux installation only. Unless stated differently here, descriptions for Windows apply to Linux as well.
>
> Remaining chapters of this service manual do contain application hints specific to the Windows platform in several places (e.g. when describing how to start the "OpenScape CTI" service); for improved readability, a description of the Linux variant has not been added to all of these places. Please refer to the subsequent section for Linux particularities.

For installation of OpenScape CAP V3.0 on SuSE Linux Enterprise Server 10, a set of rpm packages is provided (xx depending on the final release number):

? Basic package
CAP-V3.0-R14.0xx.0.i386.rpm

? CAP management package
CAP-mgmt-V3.0-R14.0xx.0.i386.rpm

? Documentation package
CAP-doc-V3.0-R14.0xx.0.i386.rpm

? CSTA packages for switch connectivity
CAP-Scc<system name>-V3.0-R14.0xx.0.i386.rpm
CAP-SccP-V3.0-R14.0xx.0.i386.rpm
CAP-SccVirtual-V3.0-75.0xx.0.i386.rpm

For a "Starter" installation (analogous to Section 4.3) only the basic package must be installed.

For a "Server" installation (analogous to Section 4.2) the basic and CAP management packages must be installed. Additionally, install CSTA packages as required plus the optional documentation packages.

A "Complete" installation (analogous to Section 4.1) results from installing all available packages.

4.4.1 Proceeding for installation on Linux

1. Login as "root" on the Linux system
2. Install rpm packages as required
   ```
   rpm -U -h -v <package_1> [ <package_2> ...]
   ```
   (-h to display a progress bar, -v for verbose information)

It is possible to install multiple packages together; in case packages are installed one after the other, make sure to observe the correct sequence: start with the basic package, then install the CAP management package and finally remaining packages in any sequence. In case the correct sequence is not observed, rpm will issue respective error messages.

3. Change to the installation directory - it is in "/opt/” and called “HiPathCTI"
4. Delete the following entry in `/etc/hosts`:I
   ```
   127.0.0.2 servername.domain.com servername
   ```
5. Invoke the configuration tool
   ```
   ./bin/tools/configure.sh
   ```
   or explicitly
   ```
   /<install_path>/bin/tools/configure.sh
   ```
   The `configure.sh` configuration tool stores the host name and the IP address of the PC on which installation is performed in configuration files.
   Depending on the Linux system configuration and the root user environment, this will open either a graphical interface (if an X server is running that can be accessed by the user) which is identical to the Windows installation GUI, or a text based interface. This allows to install and configure CAP as well remotely like via an ssh connection.
6. Check configuration by pressing Verify button.

The graphical user interface has already been described for Windows. Subsequently only differences between the text based and graphical configuration interfaces are described.

7 The console for text based configuration must have a minimum size of 80x25 characters; otherwise some presentation problems might result.

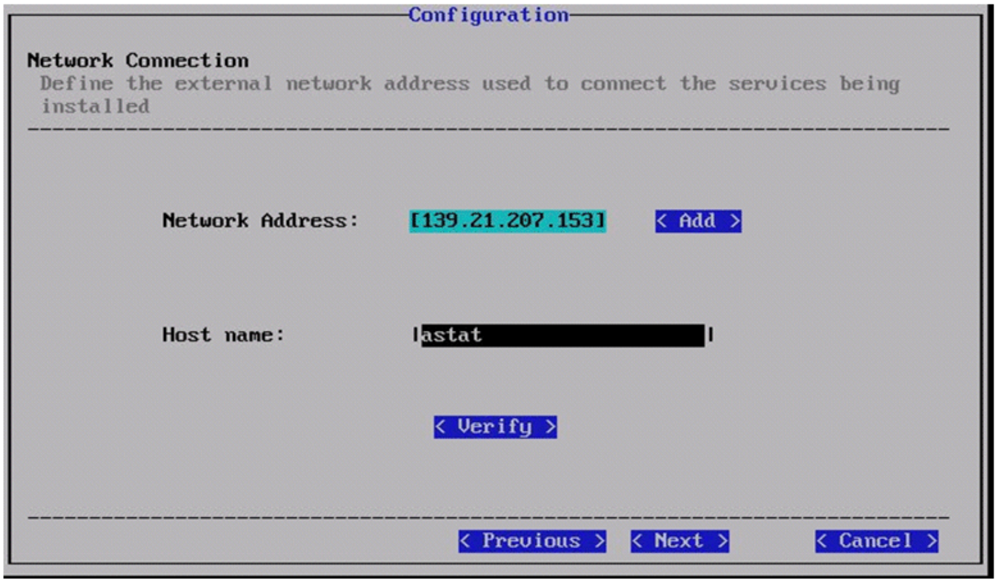
Text based configuration has been designed similar to the graphical configuration; due to limited presentation facilities, some restrictions apply:

? Navigation is controlled by cursor keys; there is no support for mouse controls.

? Selecting a check box ([ ]) is possible via space key; buttons (blue) can be pressed using the return / enter key.

? The sequence of configuration dialogs is identical in text based and graphical user interfaces.

Network connection dialog



Configuration

Network Connection
Define the external network address used to connect the services being installed

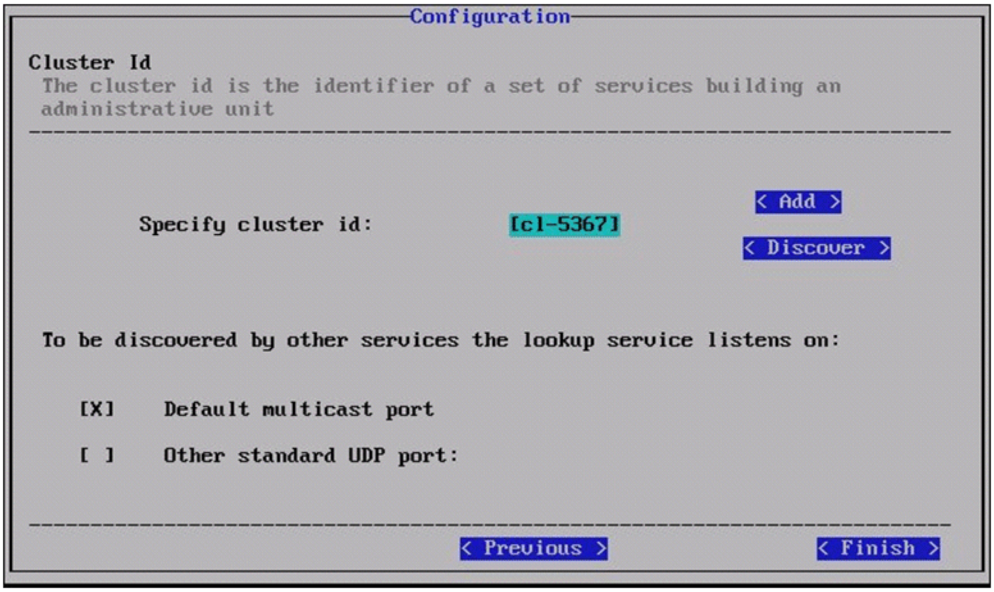
Network Address: [139.21.207.153]

Host name: astat

The "Network Address" field provides a pull-down menu that can be opened via Return / Enter. Selection is possible via cursor keys, using Return / Enter for confirmation.

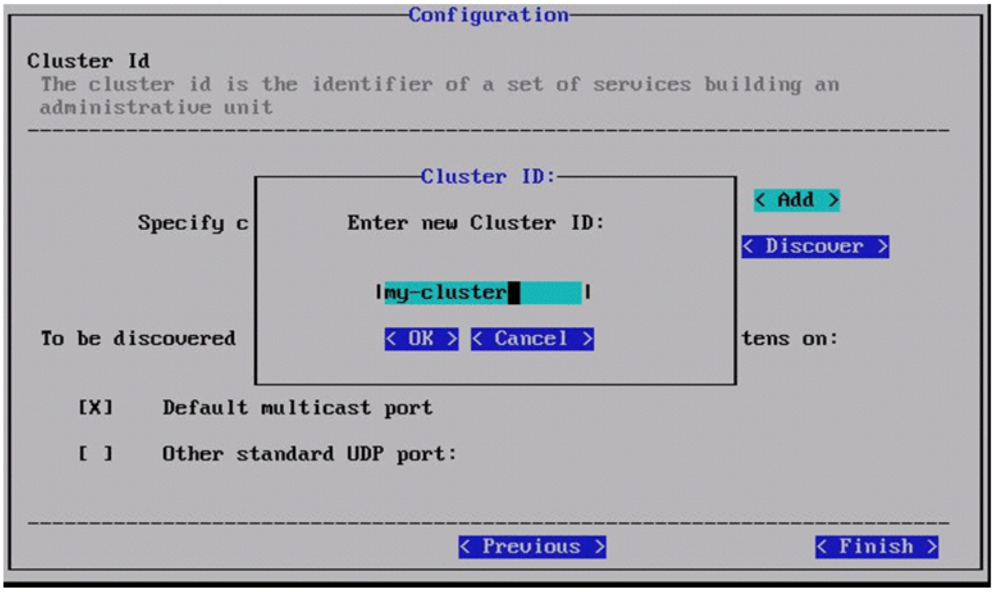
In case the respective IP address is not available in the list, use the <Add> button to enter a new address. If a correct IP address has been entered, it is shown in the pull-down menu subsequently.

Cluster dialog



```
Cluster Id
  The cluster id is the identifier of a set of services building an
  administrative unit

        Specify cluster id:          [cl-5367]

  To be discovered by other services the lookup service listens on:

     [X]    Default multicast port

     [ ]    Other standard UDP port:
```

The "Cluster Id" field provides another pull-down menu. Once again use the <Add> button to define a cluster id of your own.



```
Cluster Id
  The cluster id is the identifier of a set of services building an
  administrative unit

        Specify c        Enter new Cluster ID:

                         |my-cluster        |

  To be discovered                                    tens on:

     [X]    Default multicast port

     [ ]    Other standard UDP port:
```

The entry subsequently is shown in the pull-down menu.

All other functions are presented identical to the graphical configuration dialog.

4.4.2 Starting and stopping CAP services on Linux systems

CAP services on Linux systems are controlled by the init daemon as usual:

```
/<install_path>/bin/tools/cti.rc [start|stop|forced_stop|status|restart]
```

for CAP services on the server PC

```
/<install_path>/bin/tools/cti.rc [start|stop|forced_stop|status|restart]
```

for CAP services on the starter PC

`start` - start the service

`stop` - stop the service via "soft shutdown"

`forced_stop` - stop the service via "kill"

`status` - status query

`restart` - is identical to a stop - start sequence

4.4.3 Upgrade installation on Linux systems

Upgrading is similar to installing. (See previous sections.)

4.4.4 Uninstallation on Linux systems

As general rule, rpm uninstallation can be done in reverse order of the installation process.

1. Login as "root" on the Linux system
2. Create an overview of installed CAP packages
   ```
   rpm -q -a | grep CAP
   ```
   (-q for query, -a for all)
3. Uninstall rpm packages, first the Doc and SCC-s rpms, than the “mgmt” package and basic package last.
   ```
   rpm -e -v <package_1> [ <package_2> ...]
   ```
   (-v for verbose information)

Important

Because of the dependency chain the CAP-mgmnt rpm must be the last one to be uninstalled.

4.4.5 Additional issues on Linux systems

When using the web-based CAP Management user interface in a browser on Linux systems, there are no differences compared to Windows systems.

It’s only the operation of the diagnostic agent that might require special attention: For the diagnostic agent to be brought up correctly in a browser, a plugin for the installed JRE must have been installed on the respective system / browser. On Linux systems, this installation regularly will be handled by an administrator due to security reasons; it will not be done "on-the-fly" if during start-up of the diagnostic agent it becomes evident that the plugin is missing.

Accordingly, if problems are encountered during start-up of the diagnostic agent on a Linux system, have your administrator check that the appropriate plugin is available.

4.5 Additional packages

There are additional installation packages that due to operational and technical constraints have not been included in the CAP MSI installer.

OpenScape CAP TAPI Service Provider

For clients connecting to CAP via the TAPI interface, the TAPI Service Provider must be installed locally on the client machine.

From the software directory on the CAP CD, invoke `setupTapi.exe` to start the installation. For details on TAPI installation and configuration, please refer to the specific TAPI Service Provider documentation included on the CAP CD.

4.6 General installation proceeding

For all installation variants via CAP.msi installer, please proceed as follows:

1. Insert the installation CD in the CD/DVD drive of the relevant PC and invoke the setup by double-clicking the following file:

   ```
   <CD/DVD drive>:\software\setup.bat
   ```

2. Confirm the welcome dialog with **Next** and agree the licensing conditions by clicking **Next**.
3. Select the appropriate Setup Type and follow the instructions.
4. You can change the installation directory if necessary during installation.

   If you wish to use a different directory, please note that `CTI` is always automatically added at the end of the path.

   The installation directory will be referred to as <***InstDir***> from this point on.

5. Components will now be installed and old data will be migrated as appropriate.

   Leave the setting "All services run on this host" unchanged.

   The <PC name> can be subsequently set as a unique CAP cluster ID in the following file:

   ```
   <InstDir>\config\Start\startNT.cfg
   ```

   The entry is:

   ```
      args: "<PC name>/TelasWebStarter"
   ```

   This entry can be manually modified after installation and is activated when the "OpenScape CTI" service is restarted.

6. If several network cards are installed in your PC (for example, one for accessing the network and one for accessing the communication system), you must select the IP address on which the CAP processes are started. In this case, select the IP address of the customer LAN. If only one network card is installed, no selection is required.

   The <PC name> and the <IP address> of the CAP processes to be started can be subsequently set in the following files:

   `<InstDir>\config\Start\startNT.cfg`

   The entries are:

   ```
   args: -localAddr
   args: "<PC name>/<IP address>"
   ```

   `<InstDir>\config\common\global.cfg`

   The entries are:

   ```
   <?x set INST_HOST = "<PC name>" ?>
   <?x set INST_IP = "<IP address>" ?>
   ```

   `<InstDir>\startMenu\startPageAdmin`
   Adapt the URL behind the link as underlined
   `http://<PC-Name>:8170/`

   These entries can be manually modified after installation and are activated when the "OpenScape CTI" service is restarted.

7. Finalize installation by following the final instructions on the screen.

8. Restart the PC.

The server components **OpenScape CAP Management**, **Call Control Proxy** (SCCP), and **Call Control Service** (SCC) as selected are now available on the PC. Chapter 6, "Up to 32 characters (letters, numbers, underscore) are permitted, but hyphen is supported only under Windows. Configuration with OpenScape CAP Management" explains how to configure these components.

Check that installation has been successful

Once the "OpenScape CTI" service has been started successfully, you can set up a connection over a Web browser with CAP Management.

You can check if installation was successful by performing the following steps.

1. Select **Control Panel | Administrative Tools | Services** to check if the new Windows service "OpenScape CTI" has been added. Following the server restart, this service will have been started automatically. In case you check the services without prior restart, you might as well now start the "OpenScape CTI" service manually.

2. Set up a connection to OpenScape CAP Management in a Web browser by selecting **Start | Programs | OpenScape CAP | Management** or set up a direct connection to the following address: `http://<CAP Management PC>:8170/`

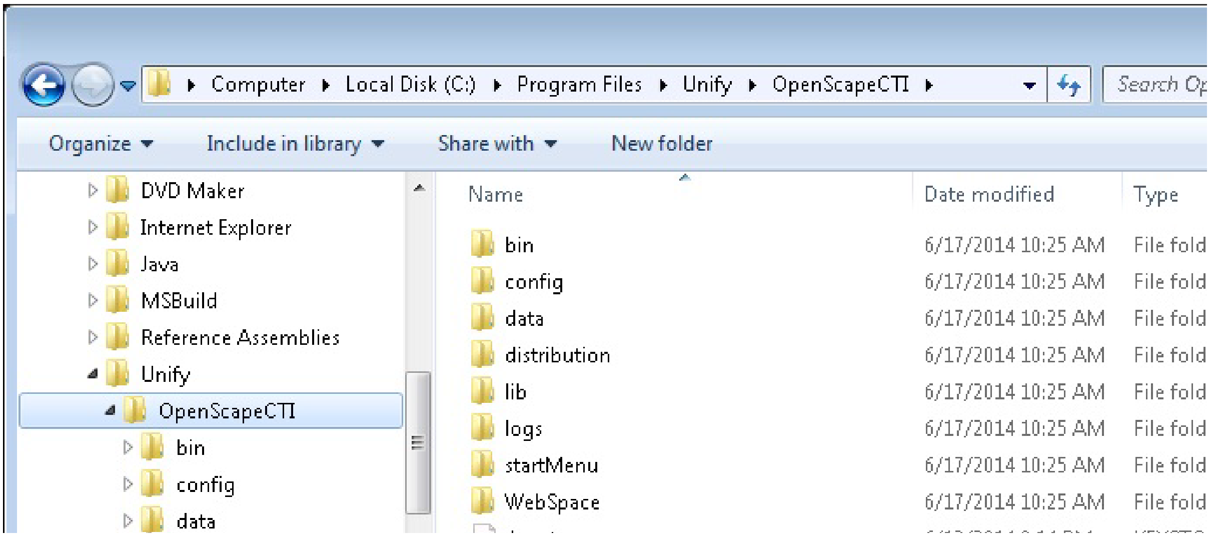
   > The connection between Web browser and CAP Management can also be operated in SSL mode. For this, select
   > `<InstDir>\config\common\ports.cfg`
   > and change the parameter `<?x set CAP_SEC_MODE = "OFF" ?>` to
   > `<?x set CAP_SEC_MODE = "FULL" ?>`.
   > You must then restart the "OpenScape CTI" service. CAP Management can now be addressed over the default port `8470`:
   > `https://<CAP Management PC>:8470/`.

   Log on to OpenScape CAP Management entering **`Admin`** as the user name and **`Admin`** as the password. Please note that these are case-sensitive. The user name and password should be changed later. If data from a previous version has been migrated, the password for the old version will, of course, still apply.

   The CAP Management interface appears following successful authentication of the "Admin" user ID (see Chapter 5, "Getting Familiar with OpenScape CAP Management"). For example, select **Help** in the main menu and click **CAP Service Manual (HTML)** in the list displayed. The online / HTML version of the CAP Service Manual appears.

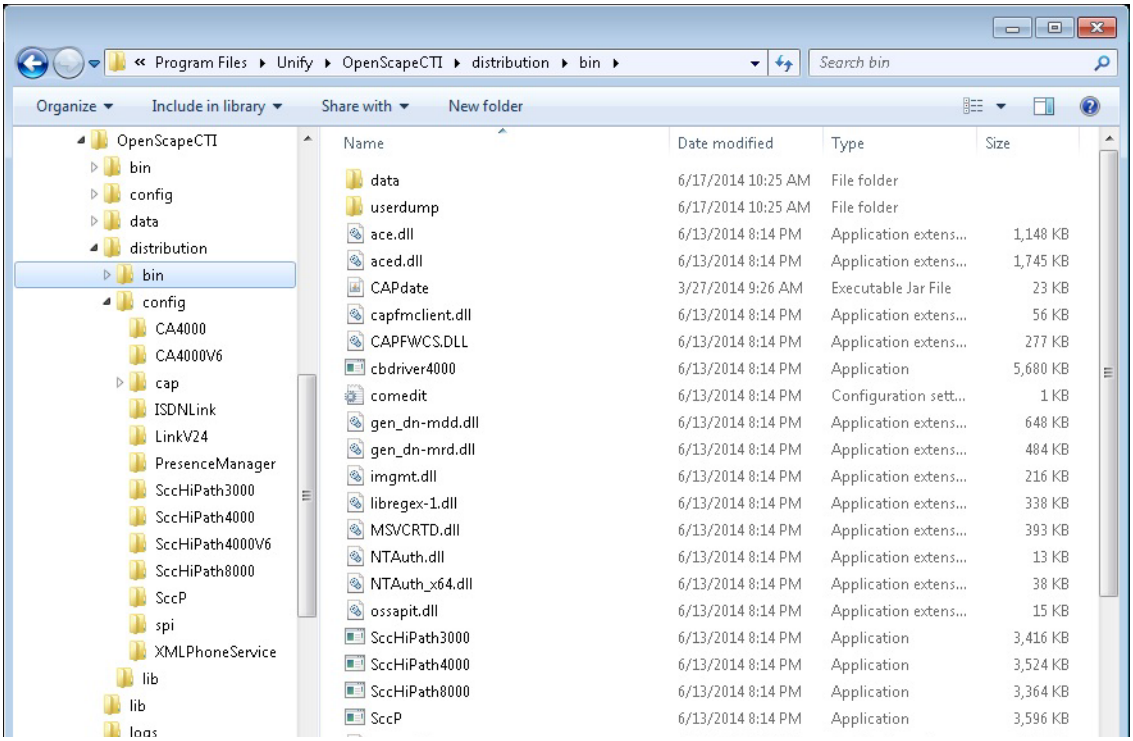
3. You may now check the installation in the file system; please note that subsequent screen shots provide an example installation only - details may vary for different "real life" installations.

   The default installation directory for the CAP Management core is
   `C:\<install_path>\`



Name	Date modified	Type
bin	6/17/2014 10:25 AM	File fold
config	6/17/2014 10:25 AM	File fold
data	6/17/2014 10:25 AM	File fold
distribution	6/17/2014 10:25 AM	File fold
lib	6/17/2014 10:25 AM	File fold
logs	6/17/2014 10:25 AM	File fold
startMenu	6/17/2014 10:25 AM	File fold
WebSpace	6/17/2014 10:25 AM	File fold

The default installation directory for CAP Call Control Service components is `C:\<install_path>\distribution\`

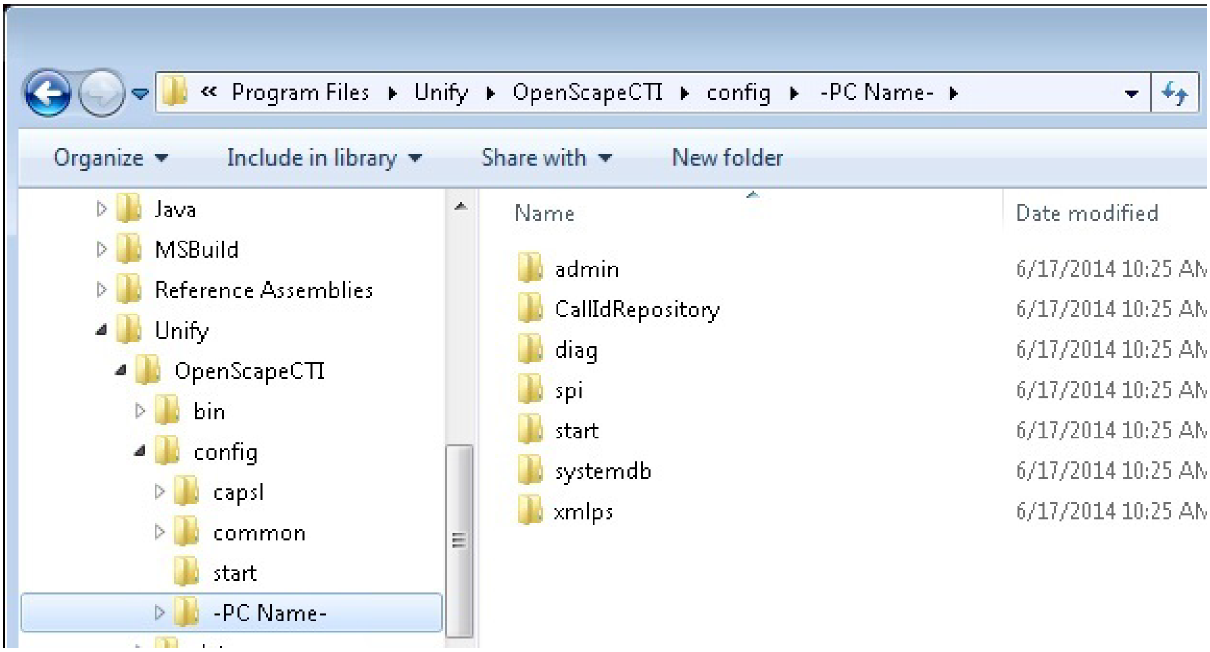


Name	Date modified	Type	Size
data	6/17/2014 10:25 AM	File folder	
userdump	6/17/2014 10:25 AM	File folder	
ace.dll	6/13/2014 8:14 PM	Application extens...	1,148 KB
aced.dll	6/13/2014 8:14 PM	Application extens...	1,745 KB
CAPdate	3/27/2014 9:26 AM	Executable Jar File	23 KB
capfmclient.dll	6/13/2014 8:14 PM	Application extens...	56 KB
CAPFWCS.DLL	6/13/2014 8:14 PM	Application extens...	277 KB
cbdriver4000	6/13/2014 8:14 PM	Application	5,680 KB
comedit	6/13/2014 8:14 PM	Configuration sett...	1 KB
gen_dn-mdd.dll	6/13/2014 8:14 PM	Application extens...	648 KB
gen_dn-mrd.dll	6/13/2014 8:14 PM	Application extens...	484 KB
imgmt.dll	6/13/2014 8:14 PM	Application extens...	216 KB
libregex-1.dll	6/13/2014 8:14 PM	Application extens...	338 KB
MSVCRTD.dll	6/13/2014 8:14 PM	Application extens...	393 KB
NTAuth.dll	6/13/2014 8:14 PM	Application extens...	13 KB
NTAuth_x64.dll	6/13/2014 8:14 PM	Application extens...	38 KB
ossapit.dll	6/13/2014 8:14 PM	Application extens...	15 KB
SccHiPath3000	6/13/2014 8:14 PM	Application	3,416 KB
SccHiPath4000	6/13/2014 8:14 PM	Application	3,524 KB
SccHiPath8000	6/13/2014 8:14 PM	Application	3,364 KB
SccP	6/13/2014 8:14 PM	Application	3,596 KB

The `distribution` directory contains additional subdirectories. `distribution\bin` contains the executable programs SCC/SCCP. `distribution\config` contains `tel-as.cfg` configuration files for SCC/SCCP, split into individual subdirectories.

From here, the SCC/SCCP is distributed among the entire CAP cluster depending on the configuration. That is, each of the selected SCC/SCCP components is installed once on the CAP Management PC, irrespective of whether or not one of these components is later active. If you need to replace specific SCC/SCCP executables later for error correction / patching, this must be done in the `distribution\bin` directory. After this, all services in the CAP cluster are restarted and the new program versions are automatically distributed. This is also the case if the entire configuration is located on a single PC. CAP structure is not important here. The same structure and the same relationship also apply for the XML Phone Service (XMLPS).

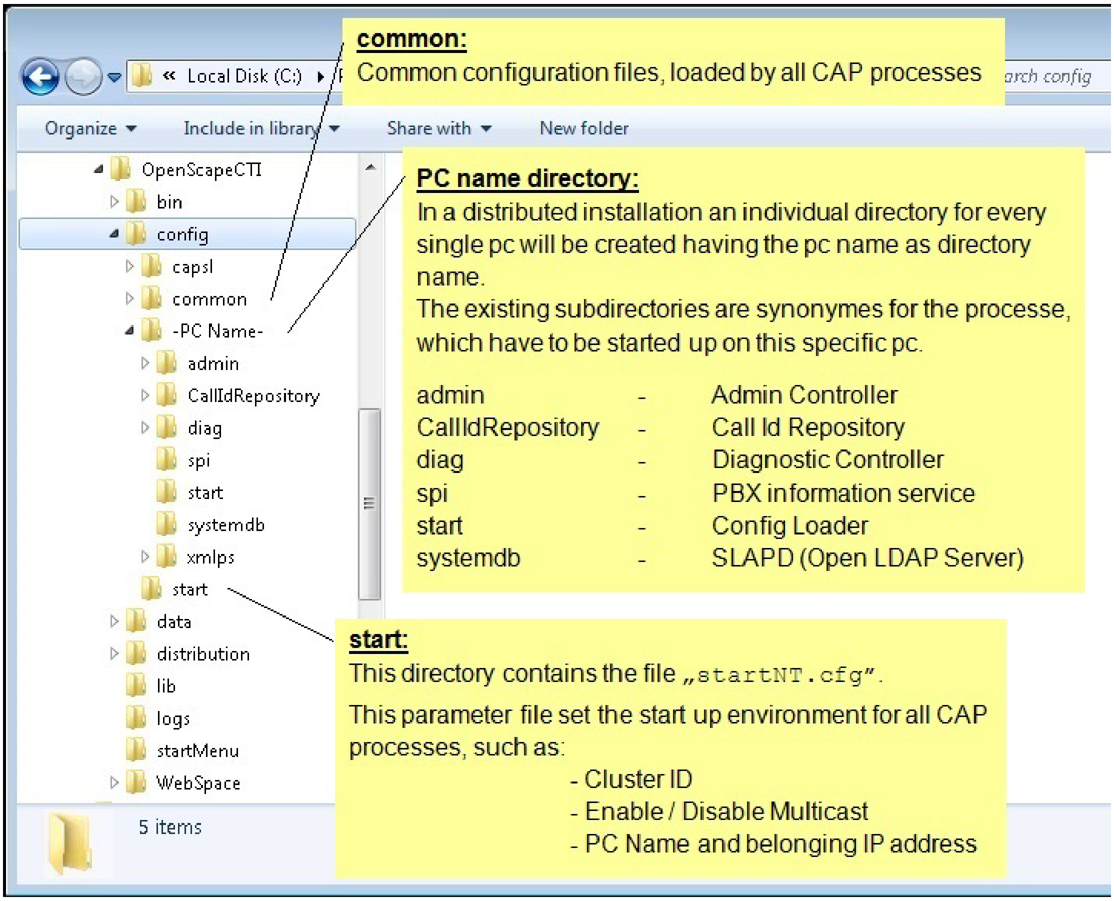
Configuration files for all components in a CAP cluster can be found in the directory `<InstDir>\config\`



Name	Date modified
admin	6/17/2014 10:25 A
CallIdRepository	6/17/2014 10:25 A
diag	6/17/2014 10:25 A
spi	6/17/2014 10:25 A
start	6/17/2014 10:25 A
systemdb	6/17/2014 10:25 A
xmlps	6/17/2014 10:25 A

All of the configuration files are stored once on the CAP Management PC - even in case of a distributed installation.

You can assign defined categories to the subdirectories in the `config` configuration directory.



common:
Common configuration files, loaded by all CAP processes

PC name directory:
In a distributed installation an individual directory for every single pc will be created having the pc name as directory name.
The existing subdirectories are synonymes for the processe, which have to be started up on this specific pc.

admin	-	Admin Controller
CallIdRepository	-	Call Id Repository
diag	-	Diagnostic Controller
spi	-	PBX information service
start	-	Config Loader
systemdb	-	SLAPD (Open LDAP Server)

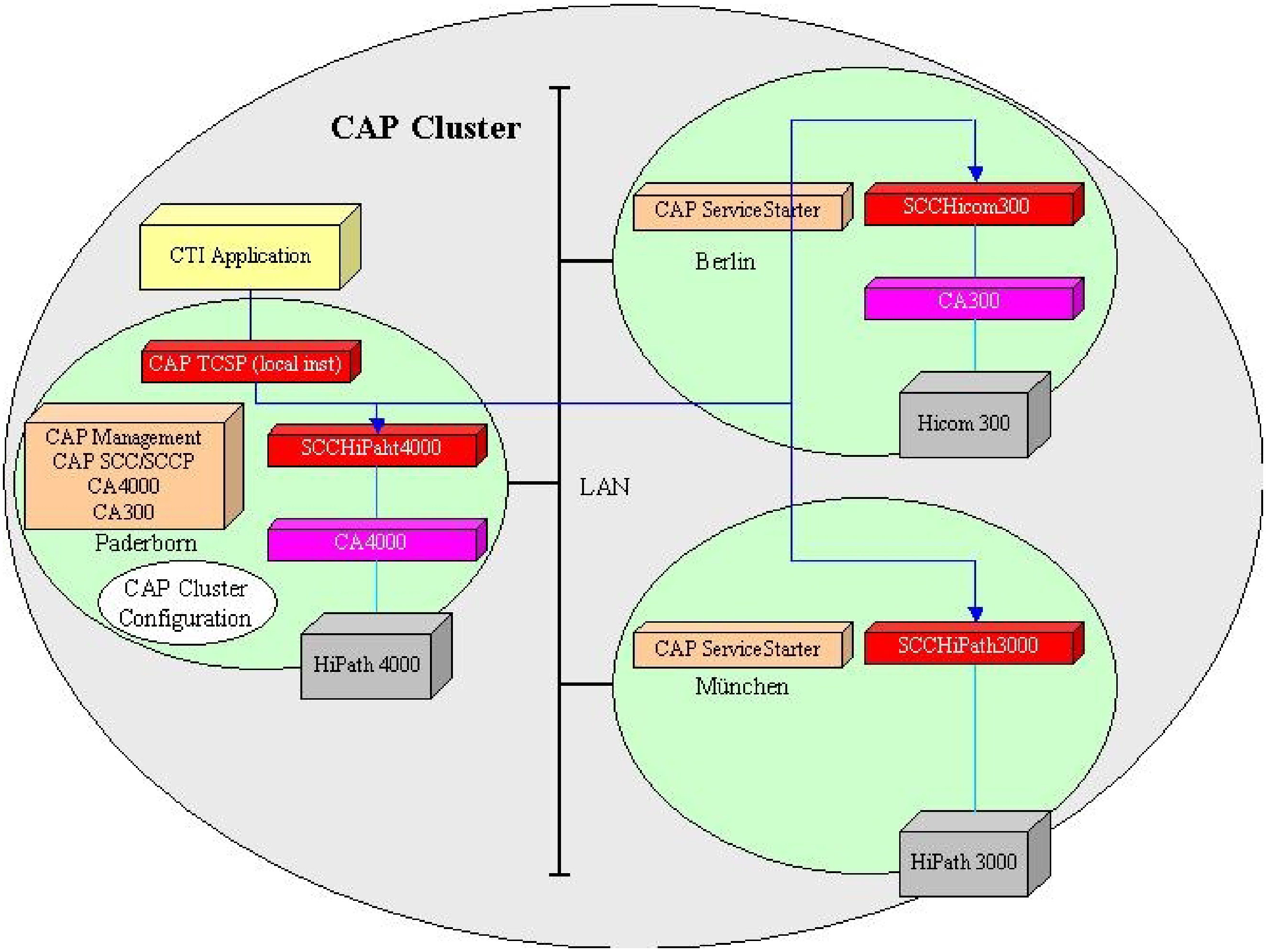
start:
This directory contains the file „`startNT.cfg`".

This parameter file set the start up environment for all CAP processes, such as:

- Cluster ID
- Enable / Disable Multicast
- PC Name and belonging IP address

4.7 Distributed installation

In case you want to connect an application over one CAP with multiple PBXs in a number of different locations, you can set up a distributed installation to optimize network load. In this case, CAP Management as well as CAP Call Control Services (SCC/SCCP) and CA4000 (if needed) will be installed at a single location ("CAP Management PC") only. This is irrespective of whether you plan to have SCCP/SCC (and CA) or XMLPS instances started later on the CAP Management PC. For every frontend PC the recommended maximum SCC that can run on a sngle machine is 10.



The remote PCs configured to host SCCP/SCC (and CA) or XMLPS instances must be prepared for that by installing the Service Starter component (cf. Section 4.3 and Section 4.6).

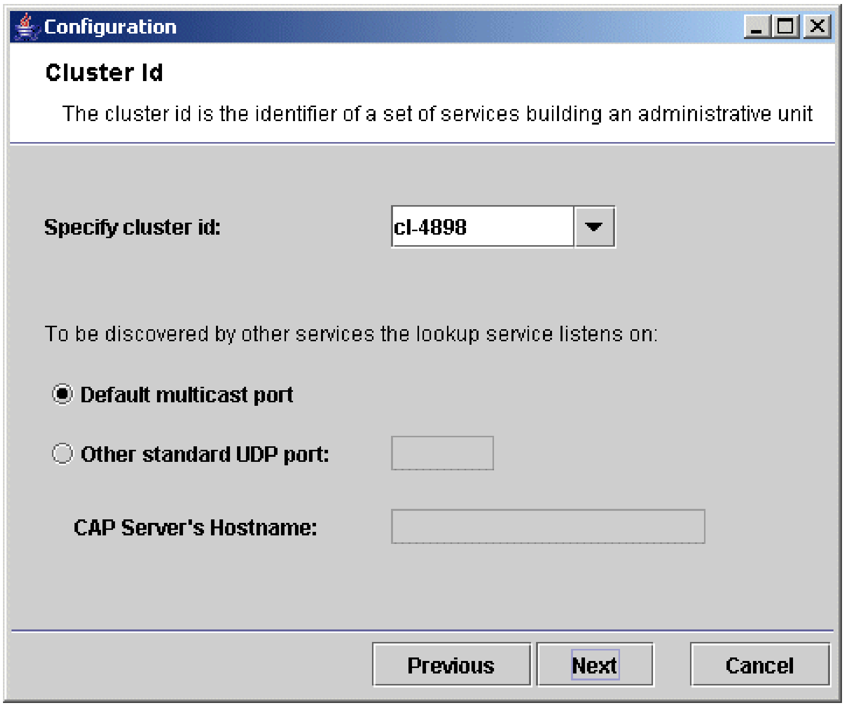
At the end of the installation, the Service Starter must be tied to an existing CAP Management host by identifying the respective CAP cluster.

The user is prompted to identify the network interface to be used for external connections of the Service Starter (like described in Section 4.6, step 7). Afterwards, this interface is used to initiate a discovery of existing clusters in the network. A "Lookup Client“ service sends a multicast through the LAN and tries to find any CAP Management lookup services present.

Discovering existing clusters ...

All lookup services found are offered for selection with their cluster IDs. Select the cluster ID for the associated CAP Management or enter it manually.

> If the cluster ID of the associated CAP Management is not listed, then the communication between CAP Management and CAP ServiceStarter must be changed from multicast to a fixed IP address:UDP port. To do this, follow the instructions in the Section "Deactivating Multicast".



Cluster Id

The cluster id is the identifier of a set of services building an administrative unit

Specify cluster id: cl-4898

To be discovered by other services the lookup service listens on:

● Default multicast port

○ Other standard UDP port:

CAP Server's Hostname:

The CAP cluster ID can be subsequently modified in the following file:

```
<InstDir>\config\Start\startNT.cfg
```

The entry is:

```
args: "<PC name>/TelasWebStarter"
```

using <PC name> as a synonym for the cluster id. This entry can be manually modified after installation and is active when the **CAP ServiceStarter** service is restarted.

To finalize the ServiceStarter installation, now start the service with

– **Control Panel | Administrative Tools | Services**

Installation on the remote PC is now complete.

The Service Starter process is automatically started every time you start the PC. It connects with the OpenScape CAP Management PC, determines all data for the components configured for the remote PC, loads the current software versions and required configuration data and starts the relevant processes.

> Start the **CAP ServiceStarter** service only after completely configuring the CAP components (SCC, CA, SCCP, XMLPS) for this PC!

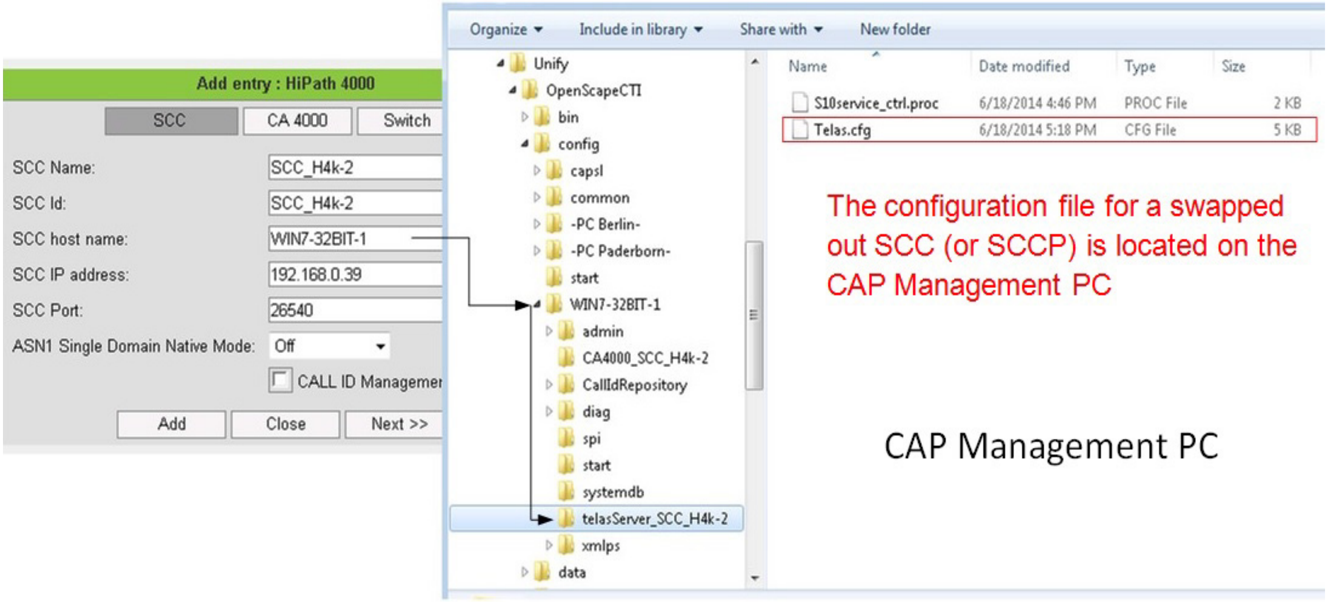
After installation

Please note that unlike the central CAP Management host, after installation no SCC / SCCP / CA4000 etc. executables are available in the `<InstDir>\bin` directory on the remote host.

Configuration of components for the remote host is done on the CAP Management PC.

> During the configuration of SCC or SCCP the remote host's IP address must be given. Therefore in the diagnoses, these tasks will be shown only when the remote host with starter pack is configured well and running.

A new subdirectory corresponding to the PC name of the remote host will be created automatically in the `<InstDir>\config\` directory on the CAP Management PC.



SCC Name:	SCC_H4k-2
SCC Id:	SCC_H4k-2
SCC host name:	WIN7-32BIT-1
SCC IP address:	192.168.0.39
SCC Port:	26540
ASN1 Single Domain Native Mode:	Off

☐ CALL ID Managemer

Name	Date modified	Type	Size
S10service_ctrl.proc	6/18/2014 4:46 PM	PROC File	2 KB
Telas.cfg	6/18/2014 5:18 PM	CFG File	5 KB

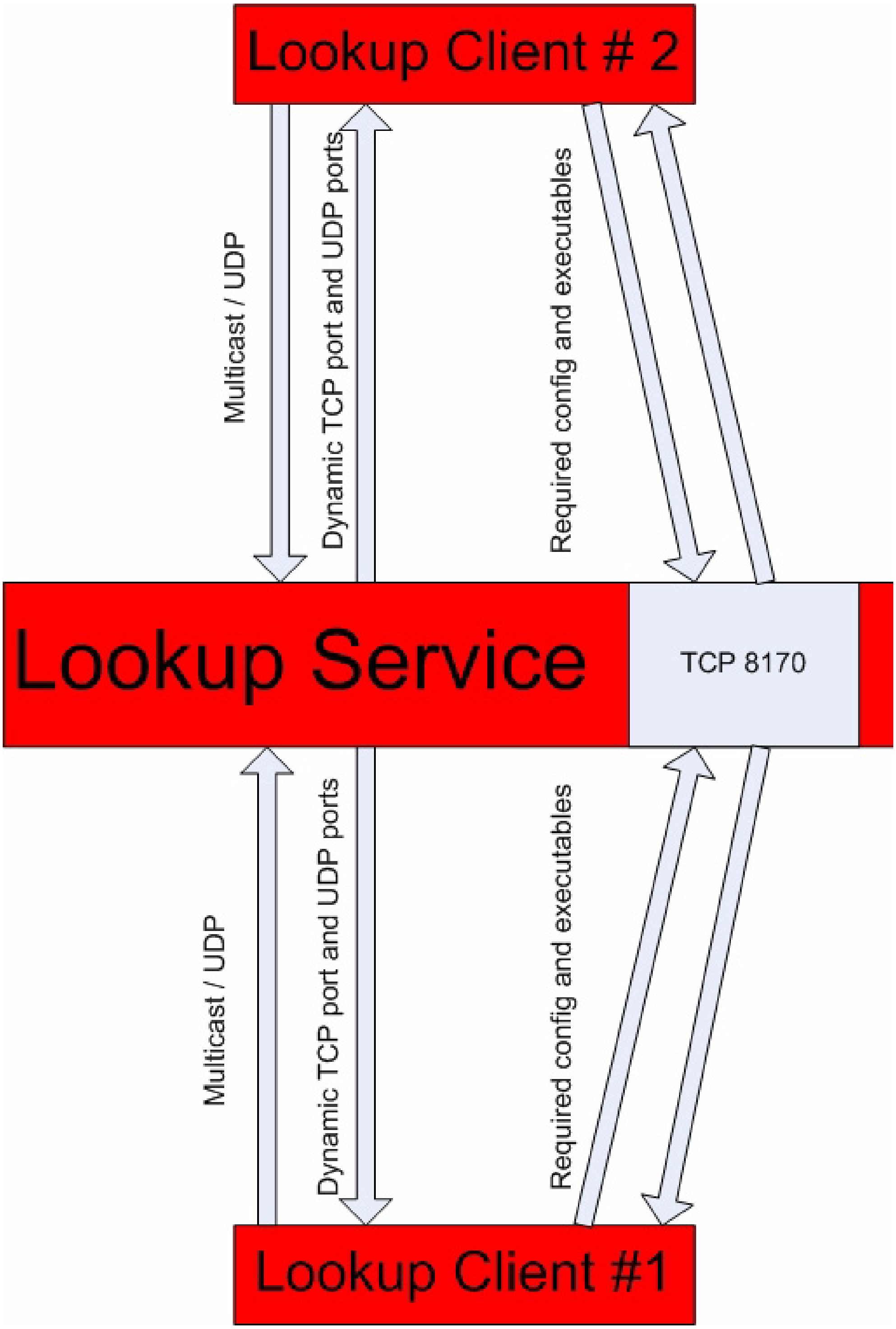
The configuration file for a swapped out SCC (or SCCP) is located on the CAP Management PC

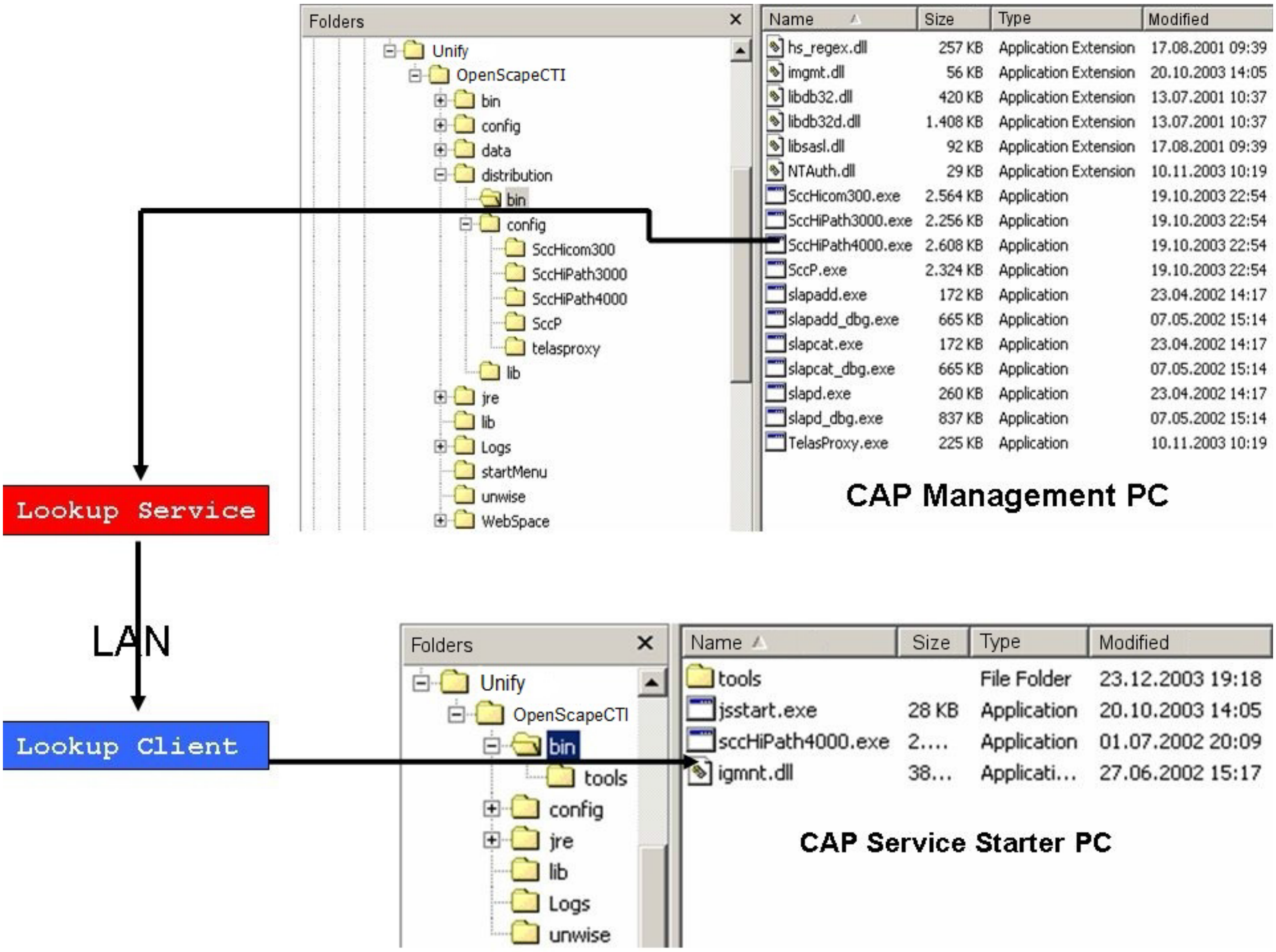
CAP Management PC

As a result, configuration files for "remote" services remain on the CAP Management PC in the directory `<InstDir>\config\<PC name>\`.

According to the configuration, executables (residing in `<InstDir>\distribution\bin\` on the CAP Management PC) are transferred from this source directory to the remote host during startup of the Service Starter there.

The transfer of these executables goes through the 8170 TCP port of CAP Management PC, as you can see the next page.


Lookup Client # 2
Multicast / UDP
Dynamic TCP port and UDP ports
Required config and executables
Lookup Service
TCP 8170
Multicast / UDP
Dynamic TCP port and UDP ports
Required config and executables
Lookup Client #1



Name	Size	Type	Modified
hs_regex.dll	257 KB	Application Extension	17.08.2001 09:39
imgmt.dll	56 KB	Application Extension	20.10.2003 14:05
libdb32.dll	420 KB	Application Extension	13.07.2001 10:37
libdb32d.dll	1.408 KB	Application Extension	13.07.2001 10:37
libsasl.dll	92 KB	Application Extension	17.08.2001 09:39
NTAuth.dll	29 KB	Application Extension	10.11.2003 10:19
SccHicom300.exe	2.564 KB	Application	19.10.2003 22:54
SccHiPath3000.exe	2.256 KB	Application	19.10.2003 22:54
SccHiPath4000.exe	2.608 KB	Application	19.10.2003 22:54
SccP.exe	2.324 KB	Application	19.10.2003 22:54
slapadd.exe	172 KB	Application	23.04.2002 14:17
slapadd_dbg.exe	665 KB	Application	07.05.2002 15:14
slapcat.exe	172 KB	Application	23.04.2002 14:17
slapcat_dbg.exe	665 KB	Application	07.05.2002 15:14
slapd.exe	260 KB	Application	23.04.2002 14:17
slapd_dbg.exe	837 KB	Application	07.05.2002 15:14
TelasProxy.exe	225 KB	Application	10.11.2003 10:19

Name	Size	Type	Modified
tools		File Folder	23.12.2003 19:18
jsstart.exe	28 KB	Application	20.10.2003 14:05
sccHiPath4000.exe	2....	Application	01.07.2002 20:09
igmnt.dll	38...	Applicati...	27.06.2002 15:17

4.8 CAP process start sequence

In this section, a distinction is made between whether the CAP processes run on a distributed installation or a non-distributed installation.

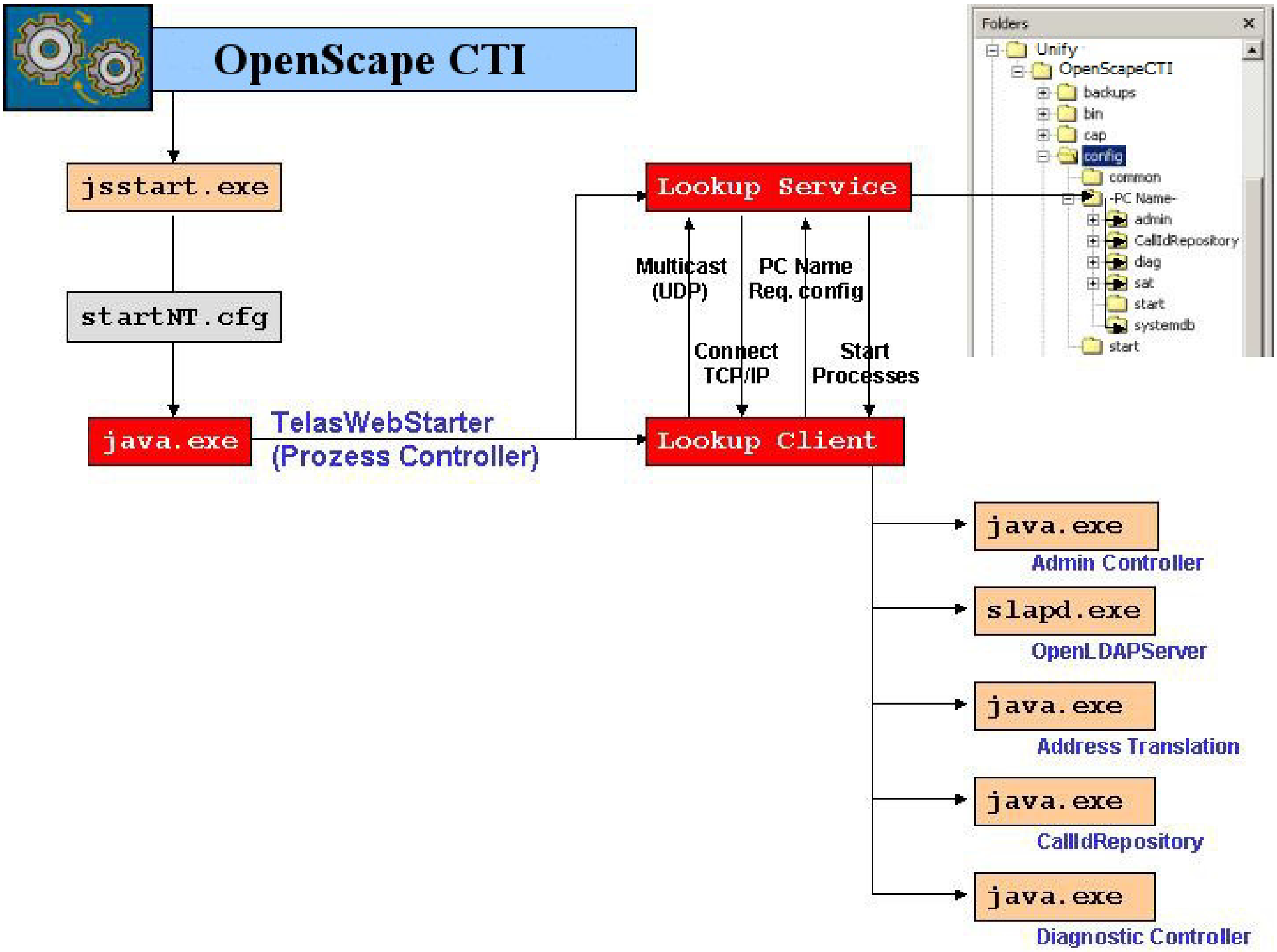
Please note that the screen shots shown subsequently are to be taken with a grain of salt - they may vary for different real-life installations and different CAP versions.

4.8.1 Non-distributed installation

As indicated by the file structure, specific processes are started on the CAP Management PC. The **OpenScape CTI** Windows service is linked to the `jsstart.exe` program (Java Service Starter).

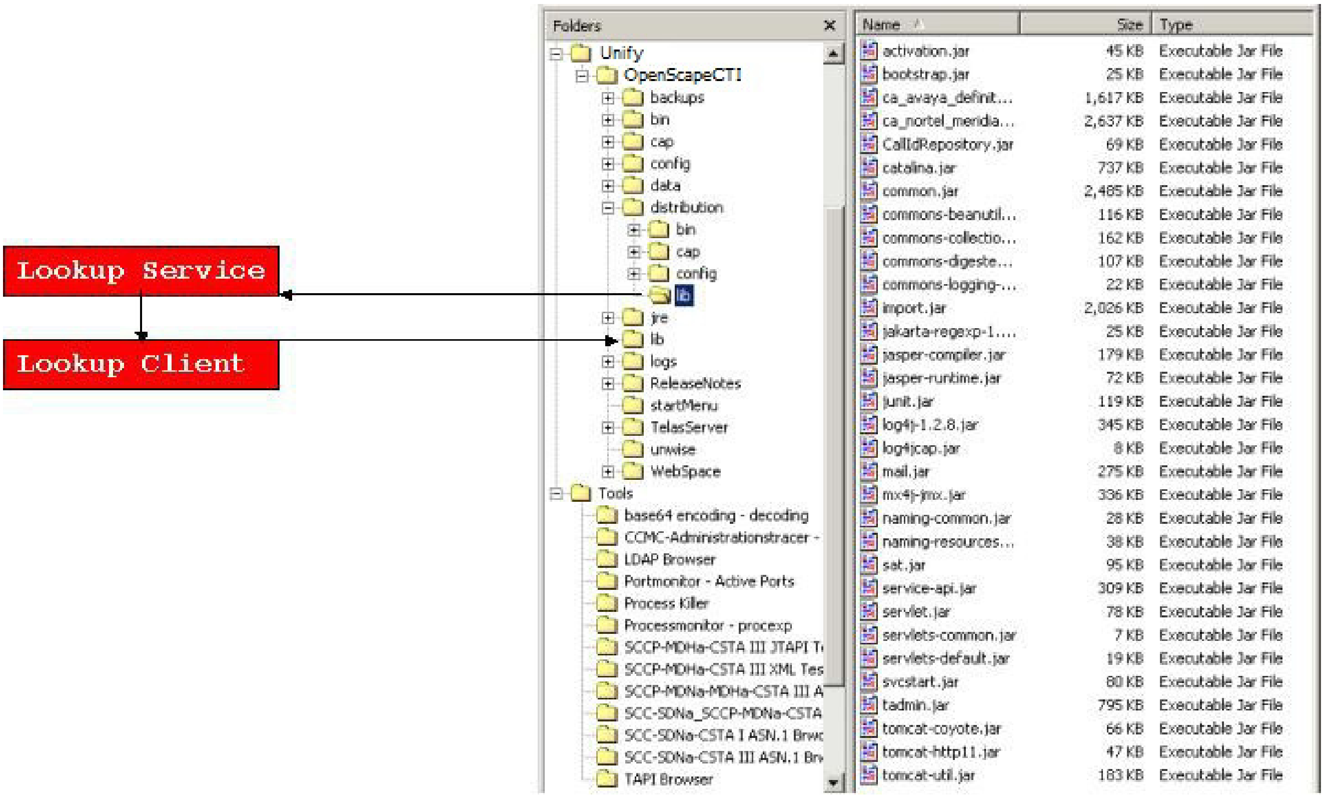
The CAP process start procedure

The following diagram illustrates the internal structure and connectivity of the CAP processes that are started with the "OpenScape CTI" Windows service.



The "OpenScape CTI" Windows service starts the `jsstart` process (Java Service Starter); this in turn starts the first Java process. This Java process is named "TelasWebStarter" and is the process controller for the internal CAP Lookup Service and Lookup Client services.
Neither of the internal services "know" each other at first. The "Lookup Client" issues a "multicast" (similar to a broadcast, but addressed to a class D IP address) to first find the "Lookup Service" in the same CAP cluster.
Following successful connection setup, the "Lookup Client" forwards its local PC name to the "Lookup Service". This action issues a request for information on the processes to be started. The "Lookup Service" then responds by transferring this data. All executable programs are transferred and the corresponding processes are started.

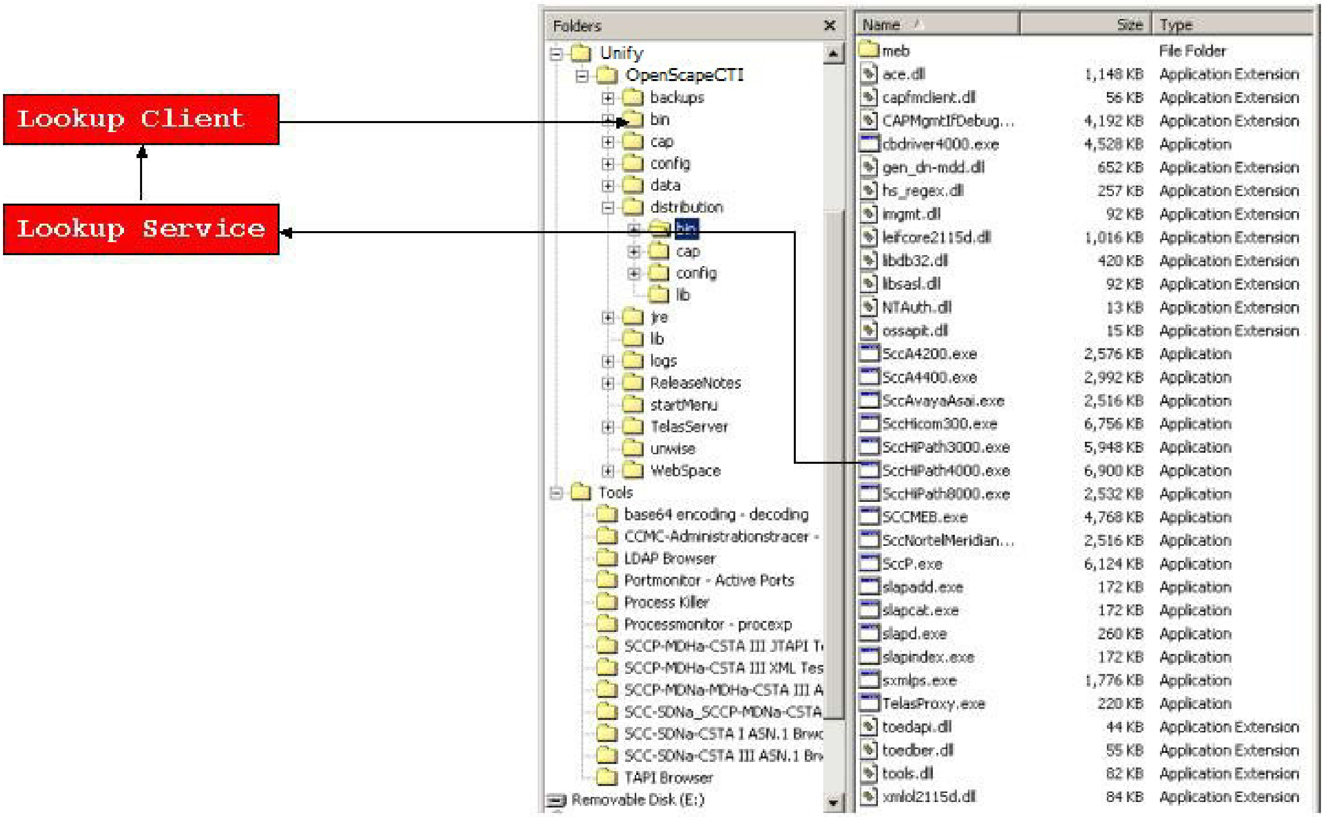
The distribution principle for executable programs indicates the success of a transfer operation.



Name	Size	Type
activation.jar	45 KB	Executable Jar File
bootstrap.jar	25 KB	Executable Jar File
ca_avaya_definit...	1,617 KB	Executable Jar File
ca_nortel_meridia...	2,637 KB	Executable Jar File
CallIdRepository.jar	69 KB	Executable Jar File
catalina.jar	737 KB	Executable Jar File
common.jar	2,485 KB	Executable Jar File
commons-beanutil...	116 KB	Executable Jar File
commons-collectio...	162 KB	Executable Jar File
commons-digeste...	107 KB	Executable Jar File
commons-logging-...	22 KB	Executable Jar File
import.jar	2,026 KB	Executable Jar File
jakarta-regexp-1....	25 KB	Executable Jar File
jasper-compiler.jar	179 KB	Executable Jar File
jasper-runtime.jar	72 KB	Executable Jar File
junit.jar	119 KB	Executable Jar File
log4j-1.2.8.jar	345 KB	Executable Jar File
log4jcap.jar	8 KB	Executable Jar File
mail.jar	275 KB	Executable Jar File
mx4j-jmx.jar	336 KB	Executable Jar File
naming-common.jar	28 KB	Executable Jar File
naming-resources...	38 KB	Executable Jar File
sat.jar	95 KB	Executable Jar File
service-api.jar	309 KB	Executable Jar File
servlet.jar	78 KB	Executable Jar File
servlets-common.jar	7 KB	Executable Jar File
servlets-default.jar	19 KB	Executable Jar File
svcstart.jar	80 KB	Executable Jar File
tadmin.jar	795 KB	Executable Jar File
tomcat-coyote.jar	66 KB	Executable Jar File
tomcat-http11.jar	47 KB	Executable Jar File
tomcat-util.jar	183 KB	Executable Jar File

This mechanism copies the "jar" files from the directory
`<InstDir>\distribution\lib\`
to the destination directory
`<InstDir>\lib.`
This directory contains the versions of the "jar" files currently in use.

The same principle is also used for the SCC/SCCP distribution.



Name	Size	Type
meb		File Folder
ace.dll	1,148 KB	Application Extension
capfmclient.dll	56 KB	Application Extension
CAPMgmtIFDebug...	4,192 KB	Application Extension
cbdriver4000.exe	4,528 KB	Application
gen_dn-mdd.dll	652 KB	Application Extension
hs_regex.dll	257 KB	Application Extension
imgmt.dll	92 KB	Application Extension
leifcore2115d.dll	1,016 KB	Application Extension
libdb32.dll	420 KB	Application Extension
libsasl.dll	92 KB	Application Extension
NTAuth.dll	13 KB	Application Extension
ossapit.dll	15 KB	Application Extension
SccA4200.exe	2,576 KB	Application
SccA4400.exe	2,992 KB	Application
SccAvayaAsai.exe	2,516 KB	Application
SccHicom300.exe	6,756 KB	Application
SccHiPath3000.exe	5,948 KB	Application
SccHiPath4000.exe	6,900 KB	Application
SccHiPath8000.exe	2,532 KB	Application
SCCMEB.exe	4,768 KB	Application
SccNortelMeridian...	2,516 KB	Application
SccP.exe	6,124 KB	Application
slapadd.exe	172 KB	Application
slapcat.exe	172 KB	Application
slapd.exe	260 KB	Application
slapindex.exe	172 KB	Application
sxmlps.exe	1,776 KB	Application
TelasProxy.exe	220 KB	Application
toedapi.dll	44 KB	Application Extension
toedber.dll	55 KB	Application Extension
tools.dll	82 KB	Application Extension
xmlol2115d.dll	84 KB	Application Extension

This mechanism copies the "exe" files from the directory
`<InstDir>\distribution\bin\`
to the destination directory
`<InstDir>\bin.`
This directory contains the versions of the "exe" files currently in use.

CAP process overview on the CAP Management PC in the Windows Task Manager

As a result, the CAP processes on the CAP Management PC should appear in the Windows Task Manager without any additional configuration (e.g. SCC, CA).
Accordingly, after stopping the **OpenScape CTI** service, you should not see these processes anymore! If they are still displayed, these processes must be terminated manually.

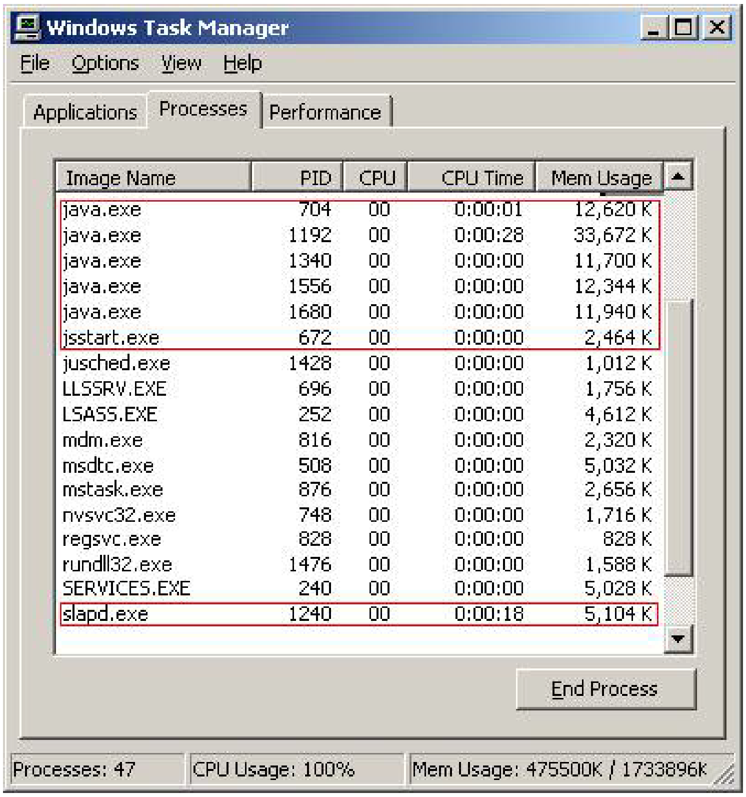


Image Name	PID	CPU	CPU Time	Mem Usage
java.exe	704	00	0:00:01	12,620 K
java.exe	1192	00	0:00:28	33,672 K
java.exe	1340	00	0:00:00	11,700 K
java.exe	1556	00	0:00:00	12,344 K
java.exe	1680	00	0:00:00	11,940 K
jsstart.exe	672	00	0:00:00	2,464 K
jusched.exe	1428	00	0:00:00	1,012 K
LLSSRV.EXE	696	00	0:00:00	1,756 K
LSASS.EXE	252	00	0:00:00	4,612 K
mdm.exe	816	00	0:00:00	2,320 K
msdtc.exe	508	00	0:00:00	5,032 K
mstask.exe	876	00	0:00:00	2,656 K
nvsvc32.exe	748	00	0:00:00	1,716 K
regsvc.exe	828	00	0:00:00	828 K
rundll32.exe	1476	00	0:00:00	1,588 K
SERVICES.EXE	240	00	0:00:00	5,028 K
slapd.exe	1240	00	0:00:18	5,104 K

Processes: 47 | CPU Usage: 100% | Mem Usage: 475500K / 1733896K

Ending CAP processes manually

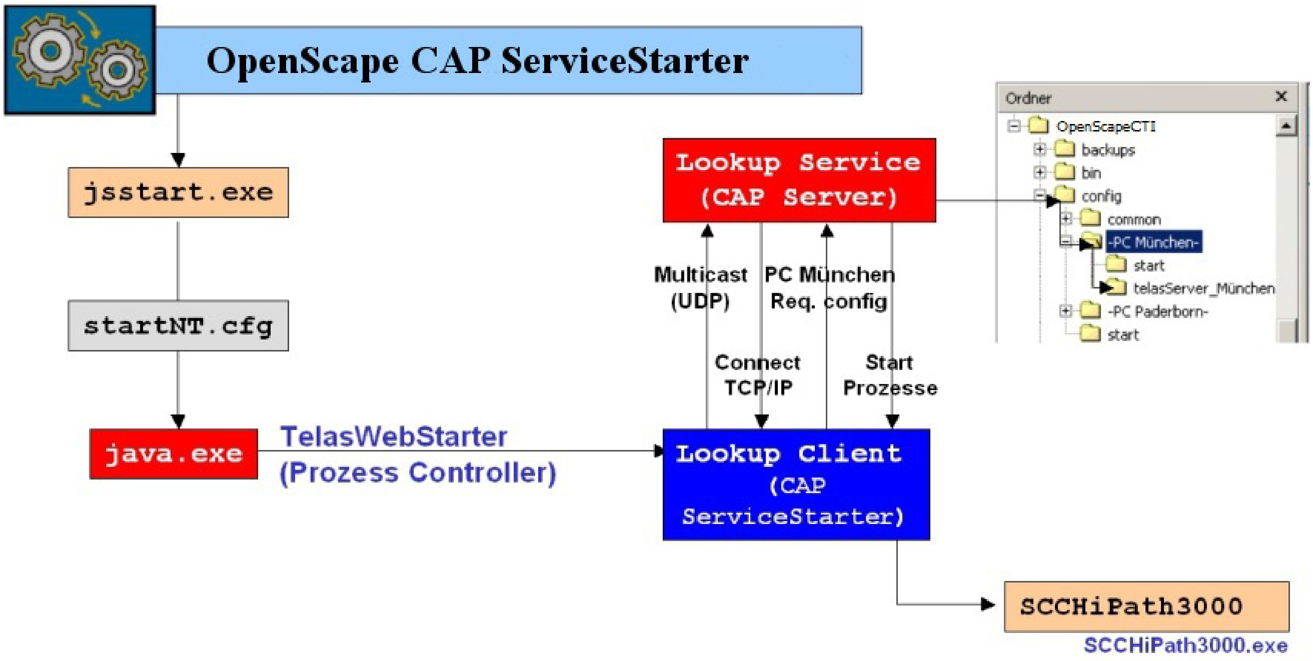
You cannot end CAP processes with the "End Process" function. During the installation phase, you must ensure that all processes end when the "OpenScape CTI" service is ended. If necessary, we recommend stopping the service and then checking if all processes were ended, and ensuring that this is the case before restarting the service.

You must restart the PC if there are CAP processes still running after you ended the "OpenScape CTI" service.

> These processes can be ended with the "kill.exe" program. You do not have to restart the PC if you choose this option.

4.8.2 Distributed installation

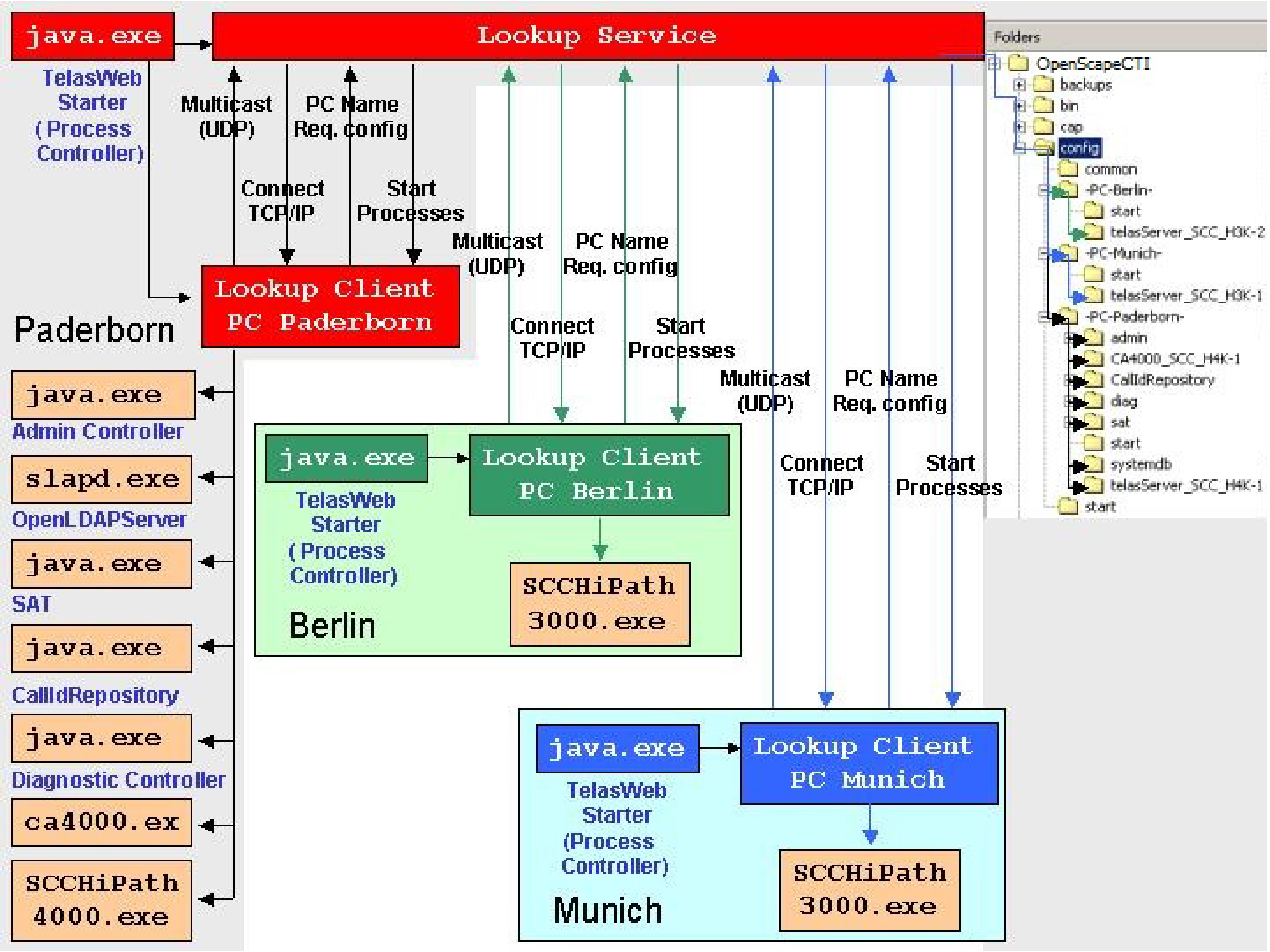
As indicated by the file structure, specific processes are started on the CAP Management PC and the CAP Service Starter PC. The **OpenScape CTI** Windows service is linked to the `jsstart.exe` program (Java Service Starter).



7	The "OpenScape CTI" service must not be started before distributed components are configured. If the " OpenScape CTI" Windows service is started before a configuration is available on the CAP Management PC, the Lookup Client (`java.exe`) on the CAP Service Starter PC connects to the Lookup Service on the CAP Management PC, transfers its PC name, and requests the remote processes to be started. In case no configuration is available at this time, the Lookup Client (`java.exe`) is terminated on the CAP Service Starter PC and can only be restarted by restarting the " OpenScape CTI" Windows service.

The CAP process start procedure

The following diagram illustrates the internal structure and connectivity of the CAP processes that are started on the CAP Management PC as well as on the CAP Service Starter PC with the " OpenScape CTI" Windows service each.



The " OpenScape CTI" Windows service starts the "jsstart" process (Java Service Starter); this, in turn, starts the first "java" process. This "java" process is named "TelasWebStarter" and is the process controller for the internal CAP "Lookup Service" and "Lookup Client" services.

Neither of the internal services "know" each other at first. The "Lookup Client" issues a "multicast" (similar to a broadcast, but addressed to a class D IP address) to first find the "Lookup Service" in the same CAP cluster.

Following successful connection setup, the "Lookup Client" forwards its local PC name to the "Lookup Service". This action issues a request for information on the processes to be started. The "Lookup Service" then responds by transferring this data.

All executable programs are transferred and the corresponding processes are started.

The "Lookup Clients" on the CAP Service Starter PC use the same principle to search for the "Lookup Service". If this is found, the same procedure is started as internally on the CAP Management PC.

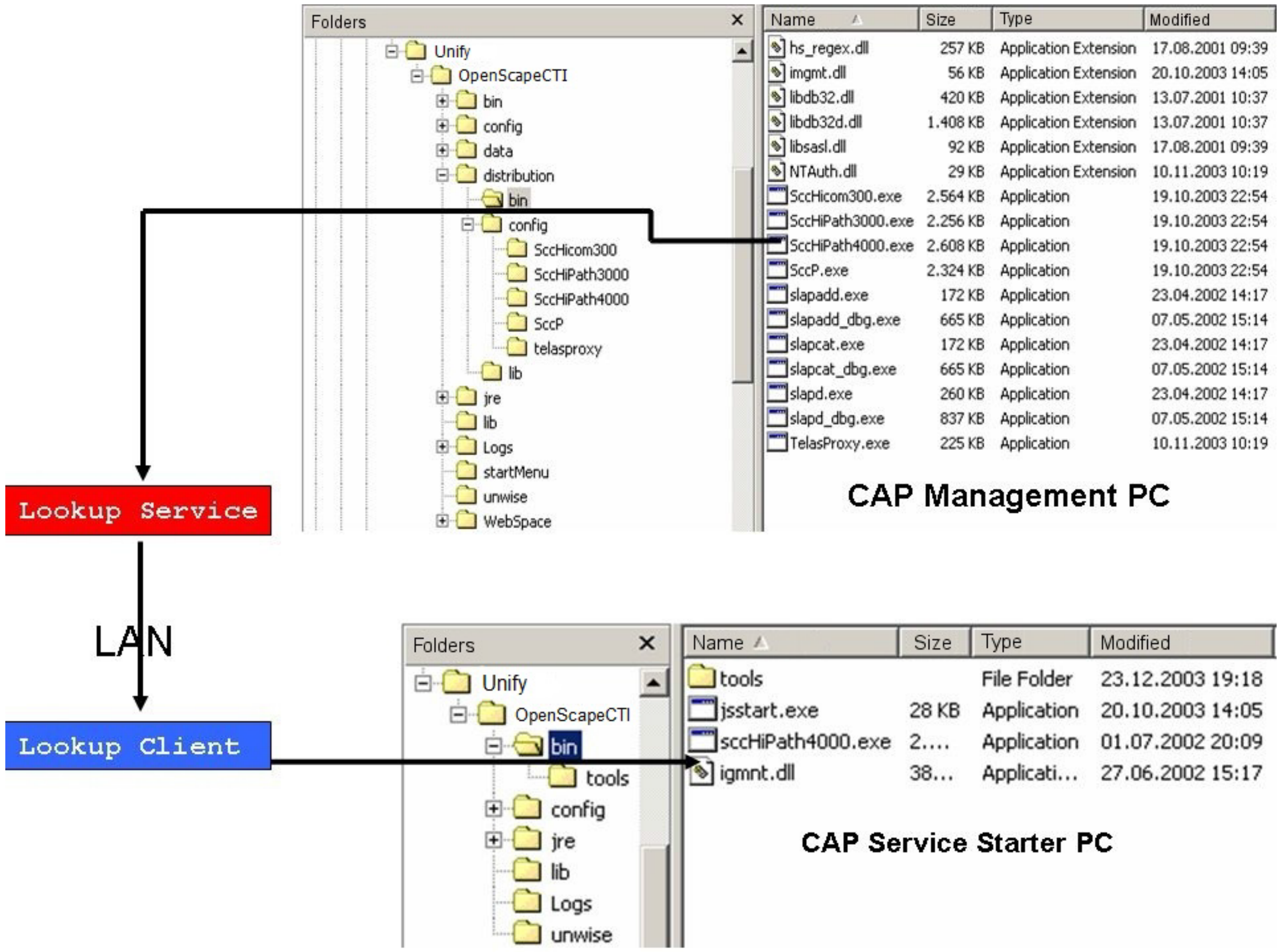
Automatic distribution of the CAP SCC or SCCP component

The `distribution` directory contains the additional subdirectories `distribution\bin` and `distribution\config`.

The `bin` directory contains the executable programs SCC/SCCP. The `config` directory contains the "telas.cfg" configuration files for SCC/SCCP, split into individual subdirectories.

From here, the SCC/SCCP is distributed among the entire CAP cluster depending on the configuration. That is, the SCC/SCCP component is only ever installed once on the CAP Management PC, irrespective of whether or not one of these components is later active. The executable SCC/SCCP program can be replaced at a later stage as part of fault clearance, but only in the directory `distribution\bin`. After this, all services in the CAP cluster are restarted and the new program versions are automatically distributed. This is also the case if the entire configuration is located on a single PC. CAP structure is not important here.

The destination directory for the selected "CAP Call Control Service" component is `<InstDir>\distribution\bin`. The programs are transferred from this source directory to the PC where the configuration should then be started.



CAP Management PC

Name	Size	Type	Modified
hs_regex.dll	257 KB	Application Extension	17.08.2001 09:39
imgmt.dll	56 KB	Application Extension	20.10.2003 14:05
libdb32.dll	420 KB	Application Extension	13.07.2001 10:37
libdb32d.dll	1.408 KB	Application Extension	13.07.2001 10:37
libsasl.dll	92 KB	Application Extension	17.08.2001 09:39
NTAuth.dll	29 KB	Application Extension	10.11.2003 10:19
SccHicom300.exe	2.564 KB	Application	19.10.2003 22:54
SccHiPath3000.exe	2.256 KB	Application	19.10.2003 22:54
SccHiPath4000.exe	2.608 KB	Application	19.10.2003 22:54
SccP.exe	2.324 KB	Application	19.10.2003 22:54
slapadd.exe	172 KB	Application	23.04.2002 14:17
slapadd_dbg.exe	665 KB	Application	07.05.2002 15:14
slapcat.exe	172 KB	Application	23.04.2002 14:17
slapcat_dbg.exe	665 KB	Application	07.05.2002 15:14
slapd.exe	260 KB	Application	23.04.2002 14:17
slapd_dbg.exe	837 KB	Application	07.05.2002 15:14
TelasProxy.exe	225 KB	Application	10.11.2003 10:19

CAP Service Starter PC

Name	Size	Type	Modified
tools		File Folder	23.12.2003 19:18
jsstart.exe	28 KB	Application	20.10.2003 14:05
sccHiPath4000.exe	2....	Application	01.07.2002 20:09
igmnt.dll	38...	Applicati...	27.06.2002 15:17

CAP Service Starter process overview in Windows Task Manager

The CAP Service Starter processes should be listed as follows in Windows Task Manager. After the **OpenScape CTI** service was started, the `SCCHiPath3000.exe` was transferred by a configuration on the CAP Management PC. Accordingly, after stopping the **OpenScape CTI** service, you should not see these processes anymore! If they are still displayed, these processes must be terminated manually.

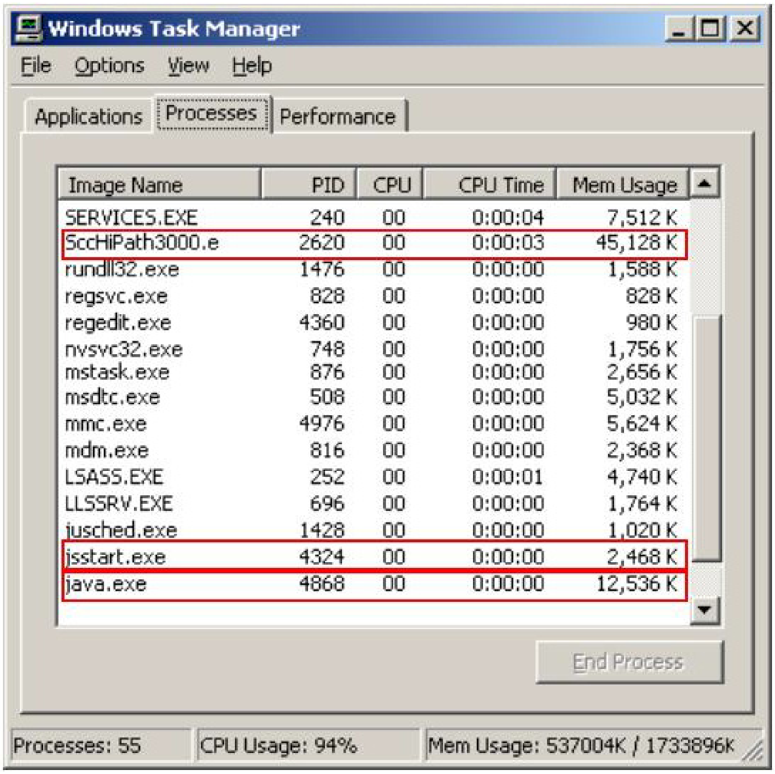


Image Name	PID	CPU	CPU Time	Mem Usage
SERVICES.EXE	240	00	0:00:04	7,512 K
SccHiPath3000.e	2620	00	0:00:03	45,128 K
rundll32.exe	1476	00	0:00:00	1,588 K
regsvc.exe	828	00	0:00:00	828 K
regedit.exe	4360	00	0:00:00	980 K
nvsvc32.exe	748	00	0:00:00	1,756 K
mstask.exe	876	00	0:00:00	2,656 K
msdtc.exe	508	00	0:00:00	5,032 K
mmc.exe	4976	00	0:00:00	5,624 K
mdm.exe	816	00	0:00:00	2,368 K
LSASS.EXE	252	00	0:00:01	4,740 K
LLSSRV.EXE	696	00	0:00:00	1,764 K
jusched.exe	1428	00	0:00:00	1,020 K
jsstart.exe	4324	00	0:00:00	2,468 K
java.exe	4868	00	0:00:00	12,536 K

Processes: 55 | CPU Usage: 94% | Mem Usage: 537004K / 1733896K

Ending processes manually

You cannot end CAP Service Starter processes with the "End Process" function. During the installation phase, you must ensure that all processes end when the " OpenScape CTI" service is ended.

If necessary, we recommend stopping the service, then checking if all processes were ended, and ensuring that this is the case before restarting the service.

You must restart the PC if there are CAP processes still running after you ended the " OpenScape CTI" service.

> These processes can be ended with the "kill.exe" program. You do not have to restart the PC if you choose this option.

4.9 Specific installation issues

4.9.1 Multiple network cards

If several network cards/NICs are configured in a CAP PC (for example, one for connection to in the customer LAN, one for connection to the HiPath / OpenScape switching host), it is important during configuration to identify the network card through which the OpenScape CAP is to be connected to the customer LAN. This is not automatically possible in all cases; for this reason a checkbox appears during installation to enable the corresponding NIC card to be identified. This checkbox also appears when only one card is configured - simply select this card and continue with the installation.

The <PC name> and the <IP address> of the CAP processes to be started can be subsequently set in the following files:

`<InstDir>\config\Start\startNT.cfg`

The entries are:

```
args: -localAddr
args: "<PC name>/<IP address>"
```

`<InstDir>\config\common\global.cfg`

The entries are:

```
<?x set INST_HOST = "PC name" ?>
<?x set INST_IP = "IP address" ?>
```

These entries can be manually modified after installation and are active when the **OpenScape CTI** or **CAP ServiceStarter** service is restarted.

4.9.2 Configuring several clusters

In a distributed installation (that is, OpenScape CAP components such as, SCC, CA4000, XMLPS or SCCP run on different PCs from OpenScape CAP Management), associated components identify themselves by means of a lookup service on the basis of a `cluster ID`.

If you want to install OpenScape CAP Management several times in your network environment (e.g. to enable the independent operation of different OpenScape CAP installations), a separate cluster ID is required to identify each of these installations uniquely.

In the case of a distributed installation (CAP ServiceStarter installation, select "Some services will run on other hosts" in the window shown below), you will be prompted to enter a cluster ID. To assist you, cluster IDs found by multicast are displayed for your selection. Select the Cluster ID specified by the associated CAP Management. In general, the displayed cluster IDs correspond to the PC names of the associated CAP Management PCs. If no cluster ID appears, either CAP Management is not yet installed or not started, or network components are blocking multicast. Then you need to enter the cluster ID directly. It always has to correspond to the cluster ID of the associated CAP Management.

The <PC name> can be subsequently set as a unique CAP cluster ID on the CAP Management PC and on the CAP ServiceStarter PC in the following file:

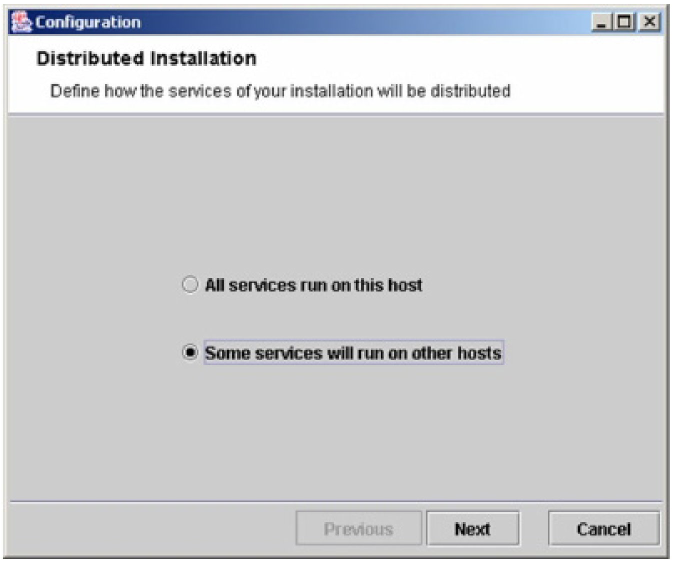
```
<InstDir>\config\Start\startNT.cfg
```

The entry is:

```
    args: "<PC name>/TelasWebStarter"
```

This entry can be manually modified after installation and is active when the " OpenScape CTI" service is restarted.

If multicast is blocked, proceed according to the instructions in the next section.



Configuration

Distributed Installation

Define how the services of your installation will be distributed

○ All services run on this host

● Some services will run on other hosts

4.9.3 Firewall configuration for CAP

In order to protect your CAP server against external attacks, it is recommended to set up a firewall that blocks all but the necessary ports from external access.

The ports that must be kept open for proper CAP operation are described subsequently. Most of them are generally valid, but some are dependant on the current installation environment; proper action must be taken especially in case of a distributed installation (i.e. CAP components being distributed across multiple servers). The firewall configuration applies to the "central" CAP server.

- ? port 8169
  CAP management interface, XML via TCP/IP
  - to be kept open in any case

- ? port 8170
  CAP management interface, http via TCP/IP
  - to be kept open in any case

- ? port 8470
  CAP management interface, https via TCP/IP
  - to be kept open in case https communication is used

- ? client ports for SCC and / or SCCP services
  as configured for the customer installation (default values in range 26535… and 27535)
  - to be kept open in any case

- ? port for DiagnosisService
  regularly assigned dynamically, see below for explicit assignment
  - to be kept open in any case

- ? port for LookupService
  regularly a UDP port for multicast, see below for switching off multicast
  - multicast to be switched off, with explicit definition of port,
  required in case of distributed installation only

4.9.3.1 Explicit assignment of port for DiagnosisService

Make sure the service OpenScape CTI has been stopped.

Go to the installation directory, and open the config file

```
<InstDir>/config/<CAPHost>/diag/diag_svc/DiagnoseServer.cfg
```

You may want to save the current version of this file for backup.

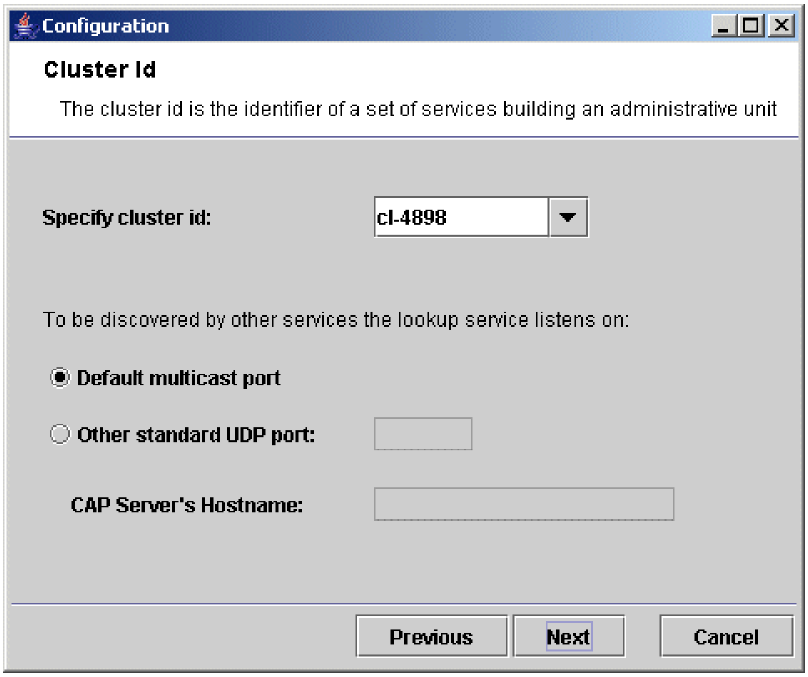
Now add the line

```
Diagnose.MsgServer.Port = <xxxx>
```

with <xxxx> representing any valid and free port number, and save the file. <xxxx> will be the port used for access to the DiagnosisService, which must be kept open in the firewall configuration.

4.9.3.2 Explicit configuration of LookupService without Multicast

This configuration can already be set up properly during the installation. In case you select "Some services run on other hosts" at the end of the installation process, you will be prompted with a screen as below:



Configuration

Cluster Id

The cluster id is the identifier of a set of services building an administrative unit

Specify cluster id: cl-4898

To be discovered by other services the lookup service listens on:

● **Default multicast port**

○ **Other standard UDP port:**

CAP Server's Hostname:

You may want to enter a specific name for cluster id (or keep the proposed default). In any case make sure to deselect "Default multicast port" but select "Other standard UDP port" and define a valid, free UDP port here.

The values defined here will be stored in a config file. In case you have an existing installation, it is possible to modify this file afterwards.

Make sure the service OpenScape CTI has been stopped.

Go to the installation directory, and open the config file

```
<InstDir>/config/start/startNT.cfg
```

You may want to save the current version of this file for backup.

Now modify the entry

```
args:   -svcId
args:   "<CAPHost>/TelasWebStarter"
```

to read

```
args:  -svcId
args:  "<ClusterId>@<CAPHost>:<UDPPort>/TelasWebStarter"
```

with <ClusterId> and <UDPPort> representing the values as described in the installation dialog above, and save the file. <UDPPort> will be the port used for access to the LookupService, which must be kept open in the firewall configuration.

It is absolutely essential that this entry is identical on all PCs in the CAP cluster, on remote CAP PCs as well as on the central CAP Management host.

Please note that modifications to the configuration files as described above become effective as soon as the OpenScape CTI service has been restarted.

4.9.4 Adaptation of the IP address on the OpenScape CAP PC

While the OpenScape CAP software is being installed, information about the PC - in particular the host name and the IP address of the PC on which installation is being performed - are determined and stored (in configuration files and in the form of directory and file names). This is why subsequent changes to the host name or IP address render the installation inconsistent and unusable without a corresponding adaptation.

This section describes the changes required to adapt to changes in host name or IP addresses. The same procedure can also be used when OpenScape CAP is installed in the form of a *ghost image* in order to adapt the configuration of the production environment to the installation environment.

Initial situation

OpenScape CAP Management was installed as described in Section 4.1. The OpenScape CAP Call Control Service or Connectivity Adapter CA 4000 components can also be installed.

Modifications

All required modifications relate to the content of the <***InstDir***> installation directory as defined above.

> 7 The full path name for the installation directory is also stored at various locations in the installation; that is why, when performing an installation via ghost image, it is important to make sure that the installation path used when creating the ghost image also exists on the target host.

1. File `<InstDir>/config/start/startNT.cfg`
   Modify the two underscored definitions
   ```
   args: -localAddr
   args: "mypc.area.xxxxxx.yy/142.33.22.11"
   ```

2. File `<InstDir>/config/common/global.cfg`
   Modify the three underscored definitions
   ```
   <?x set INST_HOST = "mypc.area.xxxxxx.yy" ?>
   <?x set INST_IP = "142.33.22.11" ?>
   <?x set CONFIG_URL = "http://mypc.area.xxxxxx.yy:
                                    <?x $CAP_STD_PORT ?>" ?>
   ```

3. Directory `<InstDir>/Config/`
   The `<host name>` subdirectory should be modified in accordance with the altered host name.

4. File `<InstDir>/config/<host name>/systemdb/S02service_ctrl.proc`
   Modify the underscored definition
   ```
   args: <InstDir>/config/mypc/systemdb/slapd_cap.conf
   ```

5. File `<InstDir>/config/<host name>/systemdb/slapd_cap.conf`
   Modify the underscored definitions
   ```
   include <InstDir>/config/mypc/systemdb/core_30.schema
   include <InstDir>/config/mypc/systemdb/cap.schema
   pidfile <InstDir>/config/mypc/systemdb/slapd_cap.pid
   argsfile <InstDir>/config/mypc/systemdb/slapd_cap.args
   ```

6. Link `<InstDir>/startMenu/startPageAdmin`
   Modify the URL following the link as underlined
   ```
   HTTP://mypc.area.xxxxxx.yy:8170/   or
   HTTP://mypc.area.xxxxxx.yy:8170/
   ```

7. Directory `<InstDir>/bin/tools/`
   This directory contains a number of tools/batch files for administrative purposes (cf. Section 8.6.3). The batch files may also need to be modified.

If HiPath ComAssistant has also been installed in addition to OpenScape CAP, four more items should be modified.

8. File `<InstDir>/config/<host name>/addrbkdb/S02service_ctrl.proc`
   Modify the underscored definition
   ```
   <?x include "/mypc/journal_access/backup.cfg" ?>
   args: <InstDir>/config/mypc/addrbkdb/slapd_twpabs.conf
   ```

9. File `<InstDir>/config/<host name>/addrbkdb/slapd_twpabs.conf`
   Modify the underscored definitions
   ```
   include <InstDir>/config/mypc/addrbkdb/core.schema
   ```

```
include <InstDir>/config/mypc/addrbkdb/twpabs.schema
pidfile <InstDir>/config/mypc/addrbkdb/slapd_twpabs.pid
argsfile <InstDir>/config/mypc/addrbkdb/slapd_twpabs.args
```

10. File `<InstDir>/config/<host name>/twebdb/S02service_ctrl.proc`
    Modify the underscored definition
    ```
    <?x include "/mypc/journal_access/backup.cfg" ?>
    args: <InstDir>/config/mypc/twebdb/slapd_tweb.conf
    ```

11. File `<InstDir>/config/<host name>/twebdb/slapd_tweb.conf`
    Modify the underscored definitions
    ```
    include <InstDir>/config/mypc/twebdb/core.schema
    include <InstDir>/config/mypc/systemdb/user_prefs.schema
    pidfile <InstDir>/config/mypc/twebdb/slapd_tweb.pid
    argsfile <InstDir>/config/mypc/twebdb/slapd_tweb.args
    ```

12. File `<InstDir>/config/<host name>/journal_access/S40service_ctrl.proc`
    Modify the underscored definition
    ```
    <?x include "/mypc/journal_access/backup.cfg" ?>
    ```

13. Link `<InstDir>/startMenu/startPageUser`
    Modify the URL following the link as underlined
    `http://mypc.area.xxxxxx.yy:8180/` or
    `https://mypc.area.xxxxxx.yy:8180/`

4.9.5 Conflicting port assignments

During CAP installation, most of the ports used for internal communication are assigned automatically; some of them will in fact be assigned dynamically in cooperation with the operating system. For components to be configured by the administrator, port assignment is part of the configuration.

Any port assignment bears the risk of port conflicts.

For ports assigned dynamically, the operating system makes sure to prevent conflicts.

For ports assigned during configuration, it is up to the administrator to prevent conflicts; there is some assistance from CAP Management, as default ports are proposed for assignment with automatically incrementing the port numbers.

For ports assigned during installation, there is always the risk of conflicts. These port numbers regularly are stored in configuration files. In case of a conflict, you might try to modify the respective configuration files to avoid the conflict.
A conflict that has been observed during system test is with the Common Web Service installed in a HiPath 3000 / 5000 network. It uses port 8280 which is used by the OpenScape CAP Process Controller as well. Adapt `startNT.cfg` to use another port in that case.

> For proceeding the port assignments please compare the hints in Section 4.9.3, "Firewall configuration for CAP"

4.9.6 Disabling services

Sometimes it can be useful to disable certain services (SCC or SCCP) temporarily without losing the configuration data.

1. To do this, select **Service** in the main menu and enable **Switch connections** or **SCC Proxy** in the navigation area. Select the relevant service from the list and click the **Modify** icon.
2. Activate **Disable PBX** and click **Modify**.
   The relevant service now appears in the overview list with a red dot. Disabled services can be re-enabled by removing the checkmark in **Disable PBX**. These services will then reappear in the overview list with a green dot.

> Please note that disabling a service will not affect current SCC processes. For this you need to stop the **OpenScape CTI** system service on the relevant PC and restart it; only then will the change take effect!

4.10 Maintenance installation

Maintenance of the OpenScape CTI system is controlled by the `CAP.msi` installer facility as well.

Use **Start | Settings | Control Panel | Software | Modify or Remove Program** and select the component **OpenScape CAP** for modification / removing. This opens the MSI installer for "Maintenance Installation".

The installer provides selections "Modify", "Repair", and "Remove". "Modify" can be used to have components added that were excluded from an earlier installation, and "Repair" can be used to fix problems with an existing installation.

Select "Remove" to have the installation removed. It takes care of removing all affected components without requiring any additional user interaction. Please note that specific uninstallation of single CAP components is neither necessary nor desirable.

> Once the uninstall procedure is completed, please check the installation directory: some files may be left there that either contain configuration data that have been kept deliberately or that could not be deleted as they are perceived as being still in use. In case you want the installation directory to be completely purged, please do that manually.

4.11 Upgrading from SMR3 to SMR5 or a newer version

Before you start upgrading:

? Check if you have a license file, with your licenses!
When you want to use your OpenScape CAP, a license is required. You should buy this only at the first time and after that you can import it into all version of OpenScape / HiPath CTI independently of the version number. But do not forget to check de expire date, because after it is expired you must buy another one. We usually provide it with a *.lic extension. The licenses are valid for that computer which MAC address was given at the beginning of the license enquiring procedure. It means that the license is only valid for a fix MAC address.

? Collect all the data form your configured SCCs and SCCPs!
After upgrading procedure the properties of SCC and SCCP will be shown by the OpenScape management but it will not be there physically, therefore it is suggested to note these data, before you start the upgrading. If you have a lot of SCC and SCCP configured in your management, it will take a long time, but you really must to do this before the upgrading. After upgrading delete the SCCs and SCCPs and re-create them using data as noted before.

? Check if your old version of HiPath CTI is sill running!
First of all you must stop the HiPath CTI service form the Control Panel. To do this, run the Services (Start|Settings|Contorll Panel|Administrative tool) and select HiPath CTI. Click the right button on it and chose stop.

How to run upgrade:

You cannot do the update form SMR3 to SMR5 directly. First you must upgrade your system from SMR3 to SMR4 and after that you can continue the upgrading to SMR5. Because of the reasons described above you need an installation pack of HiPath CTI V3.0 in a version of SMR4 and SMR5. **You can upgrade from SMR5 to a newer version directly.**

Steps of upgrading:

1. Stop the current running version of HiPath CTI. (Stop the service from administrative tools.)
2. Start the installation of the newer version of OpenScape CTI by run the setup.bat.

3. The installer will recognize a previously installed version of HiPath CTI, therefore it will offer you an upgrade. If you don’t use the default directory, you must install the upgrade into the same different directory like the original one.
4. After you finished the installation you must continue with the data migration. These steps are described in chapter 4.11.4. (Look at step 9.)
5. After finished data migration, start the OpenScape CTI service (from administrative tools|service).
6. Run the management and check all described property at step 14. of chapter 4.11.4. For addition do the same with SCCP like with SCC for finalize installation.

At the end of the migration from SMR3 to SMR4 you should continue with migration from SMR4 to SMR5. The procedure of this upgrading same as it was in case of upgrade from SMR3 to SMR4. There is only difference in data migrating. The data migration is described in chapter 4.11.4. (Look at step 11.).

4.12 Upgrade/update Instructions

> > After upgrading or updating components of OpenScape CAP the tecnician has to make sure that CAP is using the new .exe and .jar files in order to avoid inconsistencies.

You can check .exe files via **DiagnoseAgent** (Processes -> Process -> Snapshot -> (Status) -> version)

You can check .jar files in CAP Management (Help -> Product information)

5 Getting Familiar with OpenScape CAP Management

This chapter explains the log on and off procedure for CAP Management and describes the CAP Management user interface.

5.1 Starting CAP Management

> You should select a screen resolution of 1024 x 768 pixels or higher for the best possible display of CAP Management.

1. Start OpenScape CAP Management with **Start | Programs | OpenScape CAP | Management**.
2. Your HTML browser will open and the login dialog will appear.

5.1.1 Logging on

Access to the functions of CAP Management is only provided after successful login. An ID and password are required to login to CAP Management. The default administrator ID provided with the installation for this purpose is "Admin" with default password "Admin". This password should be changed by the administrator as soon as possible (see below).

1. For login, enter the standard administrator ID "Admin" and the standard administrator password "Admin" in the relevant input fields. For security purposes, the password entered will be represented by a series of asterisks.

   > The ID and password entries are case-sensitive.

2. Click **OK**. The data is checked and CAP Management is started.

   > After 30 minutes of inactivity, the browser and system are automatically disconnected. To carry out further actions with CAP Management, you must log in again.

To change the default password "Admin", proceed as follows:

1. In the main menu, activate **User**.
2. In the navigation area, select **Search/Modify**.
3. Enter **Admin** as a search keyword under User ID and click **Search**.
4. In the next dialog that opens, change the password.

To define a new user with administrator rights, configure a user as described in Section 7.3.1 and select **Admin** as the user’s role.

Please note that starting with HiPath CAP V3.0 SMR4 in addition to an administrator with unlimited admin rights it is possible to define "business group administrators" (BGAdmin). These are confined to administration of the respective business group; for details, please refer to Section 7.1. As the same user id may be defined in different business groups, possibly only the combination of business group + user id is unique within the CAP installation.

In that case, login requires "<business group>/<user id>" or (for authentication via Windows login) "<domain>\<windows login>" to be specified.

5.1.2 Logging off

Normally, you do not need to log off separately to close CAP Management. It is enough to close the CAP Management window.

In case you want to terminate the CAP Management session without closing the window, you can do so by explicitly selecting **Logout** from the main menu. You are prompted for confirmation, and the session is closed subsequently. To continue working with CAP Management, you must log in again (see Section 5.1.1, "Logging on").

5.2 CAP Management interface

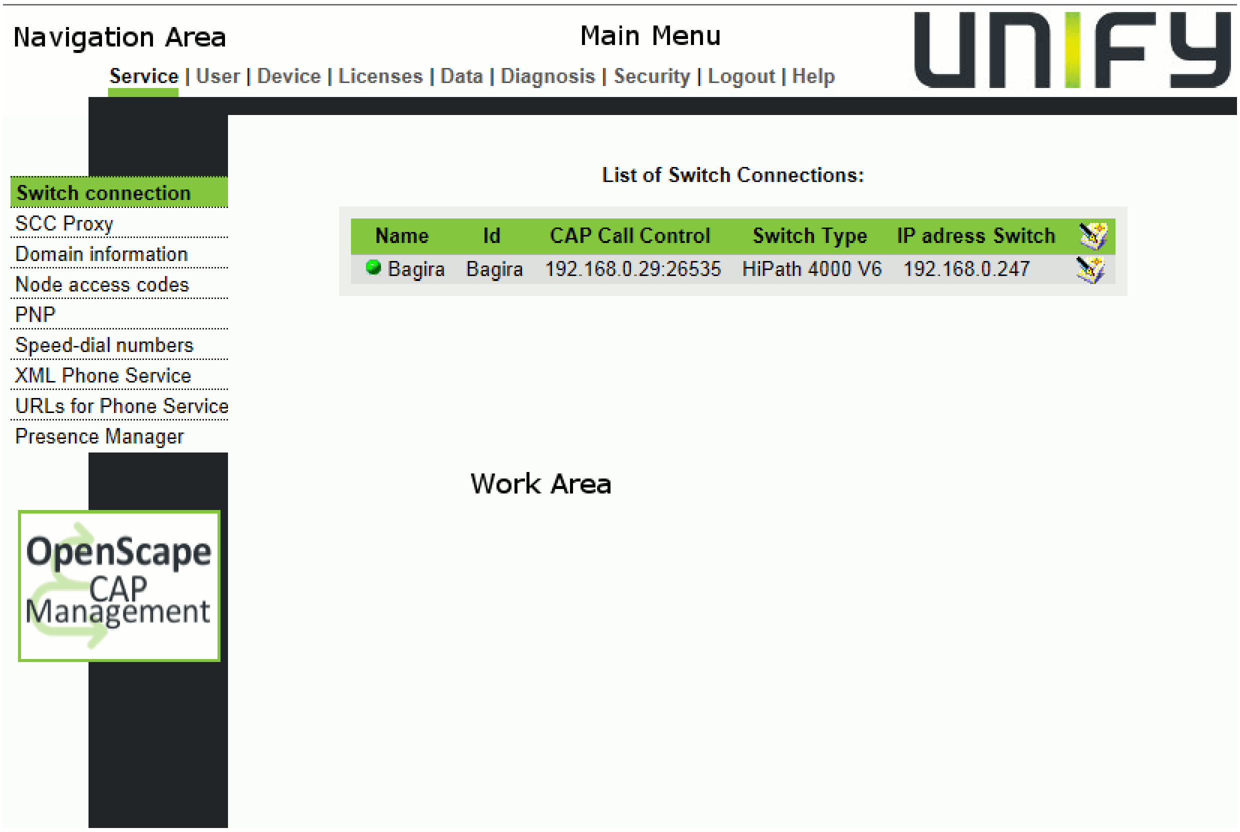
The CAP Management interface consists of HTML pages that can be opened with an HTML browser. This allows for CAP Management to be operated platform-independently on all commonly used operating systems.

Each of the HTML pages consists of the following three areas:

? Main menu

? Navigation area

? Work area



List of Switch Connections:

Name	Id	CAP Call Control	Switch Type	IP adress Switch
● Bagira	Bagira	192.168.0.29:26535	HiPath 4000 V6	192.168.0.247

> If the size of the browser window prevents navigation and work areas from being displayed completely, horizontal or vertical scroll bars appear at the edges, enabling you to scroll the section displayed.

> CAP management is using URL rewriting. If the size of the URL exceeds the limit of the browser, it would not work. The use of a different browser or a newer version isrecommended in such cases.

5.2.1 Main menu

The main menu contains the various CAP Management menu items. When you click a menu item, the selection list in the navigation area and the display in the work area change accordingly.

5.2.2 Navigation area

The navigation area contains the various submenu items for the main menu. When you click one of the submenu items, the associated page in the work area appears.

5.2.3 Work area

The data for configuring OpenScape CAP can be entered or selected in the work area. The available information and action options depend on the choice of menu item in the navigation area. You will find a description of the information and actions under the relevant menu item.

6 Configuration with OpenScape CAP Management

You can connect various communication systems to OpenScape CAP V3.0:

? HiPath 8000 / OpenScape Voice

? HiPath / OpenScape 4000

? HiPath 3000 / 5000

For each switch to be connected to OpenScape CAP, a corresponding SCC instance must be configured, like:

? SCC8000 for HiPath 8000 / OpenScape Voice

? SCC4000 for HiPath / OpenScape 4000

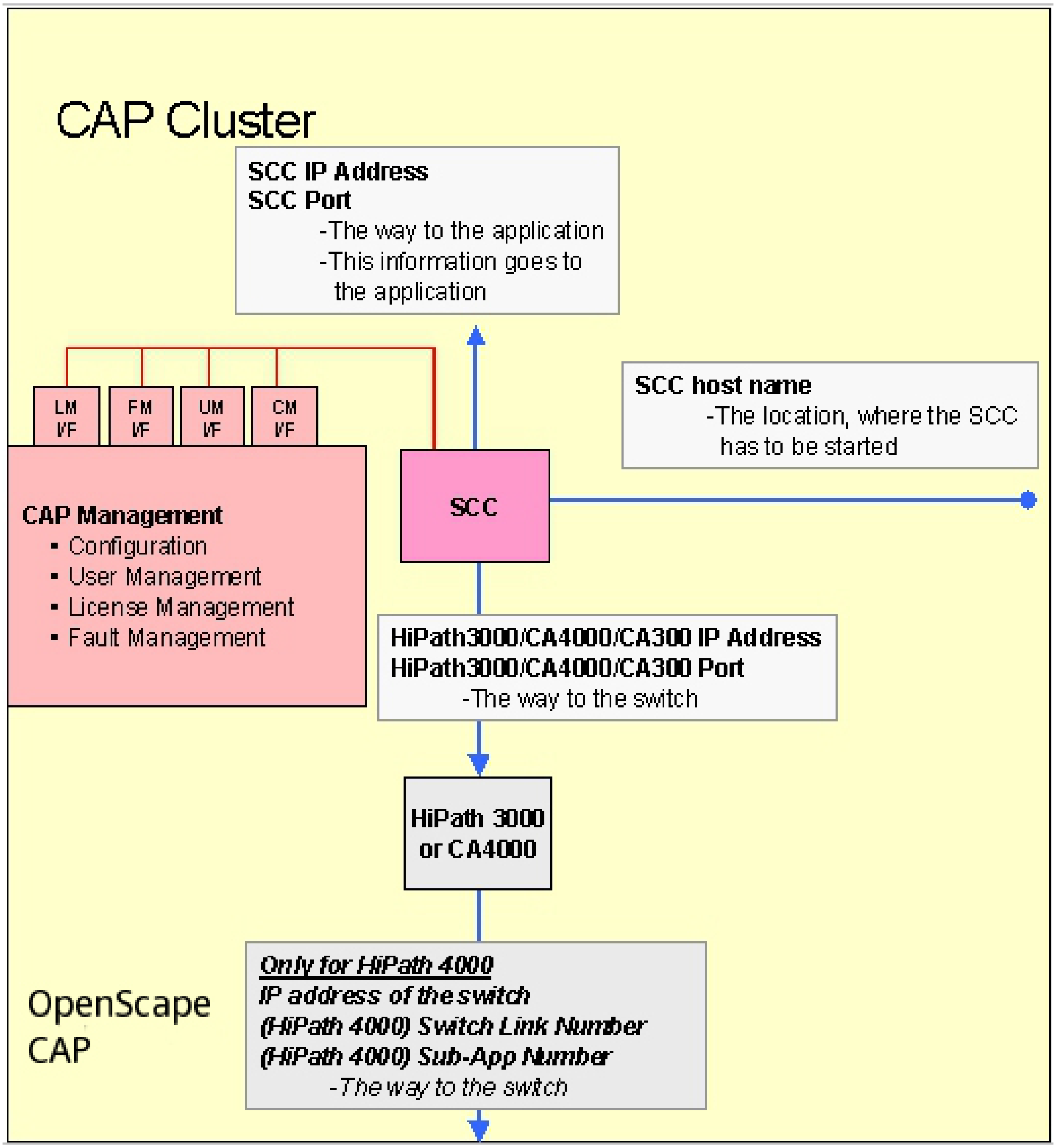
? SCC3000 for HiPath 3000

To create and configure a new SCC instance, select **Service** in the main menu and enable **Switch connection** in the navigation area. Click in the work area to create a new entry and select the appropriate SCC variant in the pop-up selection box.

Use of an SCCP is necessary to facilitate multi domain capability for CSTA XML and CSTA ASN.1 protocols (also for JTAPI and XMLPS applications). The SCCP can communicate with several SCCs simultaneously.

This chapter explains the settings you must make in OpenScape CAP Management to connect the communication systems listed above to OpenScape CAP. In addition, it explains how to configure an SCCP.

The following diagram shows the positioning of an SCC in the CAP with explanations of the fundamental configuration points.


CAP Cluster
SCC IP Address
SCC Port
-The way to the application
-This information goes to the application
LM VF
FM VF
UM VF
CM VF
SCC host name
-The location, where the SCC has to be started
CAP Management
▪ Configuration
▪ User Management
▪ License Management
▪ Fault Management
SCC
HiPath3000/CA4000/CA300 IP Address
HiPath3000/CA4000/CA300 Port
-The way to the switch
HiPath 3000 or CA4000
Only for HiPath 4000
IP address of the switch
(HiPath 4000) Switch Link Number
(HiPath 4000) Sub-App Number
-The way to the switch
OpenScape CAP

6.1 HiPath 8000 / OpenScape Voice connectivity

6.1.1 Overview

CSTA is a standard for computer-supported telephony (CTI) that was established by the international standardization organization ECMA (European Computer Manufacturers Association). The physical connection between the HiPath 8000 / OpenScape Voice and a PC that is running SCCHiPath8000 is set up with the help of a TCP/IP LAN connection.

6.1.2 Preparation

To enable HiPath 8000 connectivity, a CSTA link must be set up as described in the HiPath 8000 / OpenScape Voice documentation.

6.1.3 Configuration

To connect a HiPath 8000 / OpenScape Voice for the first time or to reconfigure an existing connection, proceed as follows:

1. Click the **Switch connection** menu item in the navigation area.
   a) A connection has not yet been configured. Continue with 2a.
   b) One or more connections are already configured. These are displayed in a list. Continue with 2b.
2. Configure the connection.
   a) If a connection has not yet been configured, click the **Add new entry** icon and select **HiPath 8000** as the server version.
   b) If one or more connections are already configured, these are displayed in a list. Select a connection by clicking the **Modify** icon for the relevant connection.

   The HiPath 8000 configuration dialog now is displayed in the work area, comprising parts SCC and Switch.

"SCC" dialog

Field	Description
SCC Name	Enter a mnemonic name for the SCC here, e.g. "SCC-HP8000". This name can be assigned at the administrator’s discretion. It must be unique within the entire CAP installation. Up to 32 characters (letters, numbers, underscore and hyphen) are permitted. Accentuated letters are supported only under Windows.
SCC Id (optional)	Enter an Id for the SCC here; the identifier must be unique within the entire OpenScape CAP installation; it cannot be changed after configuration has been completed. In the Diagnostic Agent, the "SCC Id" is used to display the SCC in the list of processes. The HiPath / OpenScape node number (for example, 10-60-200, 30-70-600, etc.) is usually used here. must be unique within the entire CAP installation. Up to 32 characters (letters, numbers, underscore and hyphen) are permitted. Accentuated letters are supported only under Windows. **Note**: When importing user data, the SCC Id must match the PBX Id in the import file.
SCC host name	The name of the host on which the SCC process is running must be specified here. A PC name directory is created in the directory `<InstDir>\config\` using the "host name". A subdirectory called `telas-server_<SCC ID>` is added for the SCC. This subdirectory contains all configuration files for these processes that are to be started. **Note:** For distributed installation (which means that the SCC PC is not your own PC/local host), you must install OpenScape CAP Service Starter on the specified SCC PC (cf. Section 4.3).
SCC IP address (cannot be edited)	Here the IP address of the PC on which the SCC process should run is displayed. The address is determined via the host name; it is shown just to allow for a sanity check.

Field	Description
SCC Port (optional)	The port assigned to the SCC process may be specified here. Port **26535** is used by default. If this port was already assigned to a different SCC by the CAP configuration, the system automatically offers the next free port (for example, 26537).

"Switch" dialog

Field	Description
IP address of the Switch	Enter the HiPath 8000 IP address via which the CSTA interface of the HiPath 8000 can be reached.
Port of the Switch (optional)	Enter the switch port here.
IP address of the Backup Switch	Enter the HiPath 8000 IP address via which the CSTA interface of the backup HiPath 8000 / OpenScape Voice can be reached.
Port of the BAckup Switch (optional)	Enter the backup switch port here.
Speed-dial numbers	Only the ComAssistant Phone Controller uses speed-dial numbers. If the application initiates the dialing, the system checks whether the external call number dialed has been configured in the assigned speed-dial list. If the number is found in the list, the SCC sends the configured speed-dial number to the HiPath 8000 for dialing, instead of the long call number. Speed-dial lists are only used if the CTI users do not have unrestricted trunk access, and would like to dial using an LDAP search result, even though they only have access to system speed-dialing. As a rule, call numbers for people are stored on an LDAP server as long call numbers in canonical format.
Domain numbers	The left part shows a list of configured domain numbers (see Section 7.2.3); use the arrow key to move selected entries relevant for this switch to the right hand side.
NAC	The left part shows a list of configured node access codes (see Section 7.2.4); use the arrow key to move selected entries relevant for this switch to the right hand side.
Private Numbering Plan	The left part shows a list of configured PNPs (see Section 7.2.5); use the arrow key to move selected entries relevant for this switch to the right hand side.

Actions

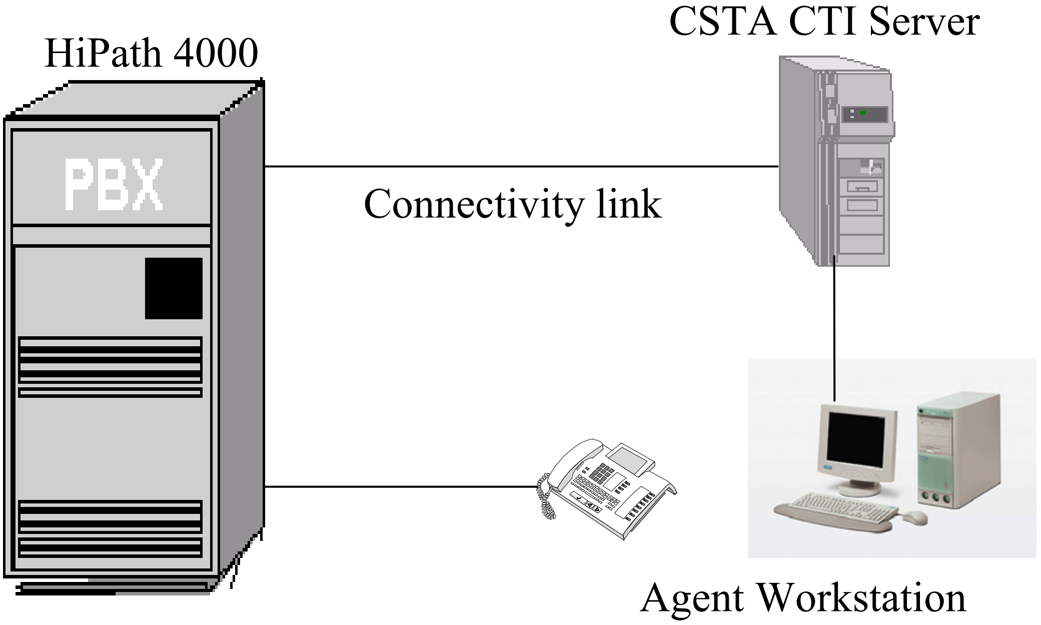
Action	Description
Add	Checks data for completeness and adds the entry to the switch connections list.
Close	Closes the **Add entry** dialog without saving the entries.
Delete	Deletes an existing switch connection. **Note**: This button only appears if at least one switch connection is already configured.
Next >>	Calls up the next dialog.
<< Previous	Calls up the previous dialog.

> \> When configuring HiPath 8000 connectivity for ComAssistant V2.0, the application will make use of configuration data only but bypass the SCC8000 service. Accordingly the SCC might be disabled (cf. Section 4.9.6) after it has been configured - unless it is used by another application.

6.2 HiPath / OpenScape 4000 connectivity

6.2.1 Overview

HiPath 4000 V4, V5 does not support a standardized protocol for communication with applications. For this reason, it is absolutely necessary to use the "Connectivity Adapter HiPath 4000" (CA4000) protocol converter. The CA4000 converts the HiPath 4000 (ACL-C+) proprietary protocol into a standardized protocol (CSTA III). CSTA is a standard for computer-supported telephony (CTI) that was established by the international standardization organization ECMA (European Computer Manufacturers Association). With OpenScape CAP V3.0, the CA4000 can only be used in conjunction with the SCCHiPath4000. All CA4000 configuration parameters are integrated in the SCCHiPath4000 configuration. The physical connection between the HiPath 4000 and a PC that is running CA4000/SCCHiPath4000 is made with the help of a TCP/IP LAN connection.
The HiPath 4000 supports 32 "ACL-C+" application connections simultaneously. Depending on the software version, it may be that less than 32 "ACL-C+" application connections can be released.



6.2.2 Preparation

Configure the SCCHiPath4000 to connect a HiPath 4000. Its configuration menu also offers the CA4000 configuration parameters. If the connection to the HiPath 4000 is made via the SL100/200, the IP address or the IP network of the SCCHiPath4000/CA4000 PC must be included in the HiPath 4000 firewall list.

REMARK: in case of **HiPath 4000 V6 / OpenScape 4000 V7** the CAP does not start CA4000 process, but connects directly to the HiPath / OpenScape 4000 CSTA interface. In case a HiPath 4000 V6 / OpenScape 4000 V7 switch connection is configured, then according to this no application/subapplication ID is needed to configured via GUI.

This connection to the CSTA is established on port 102. This port is defended by security rules, so by default it is not accessible. In case of SMR13 and after an SCC is created that will try to register itself into CSTA (technically the request's IP address gets reqistered). These entries can be managed manually on CSTA side. However, due to technical reasons deregistering is not yet supported, so in case an SCC gets deleted then it is adviced to delete the corresponding trusted address entry on the CSTA side as well.

In case of HiPath 4000 V4/5 -> HiPath 4000 V6 upgrade, the device/user data of the previous switch connection must be exported, then the export file must be edited (the old SCCId must be replaced to the SCCId of the HiPath 4000 V6 connection, and then an import must be made of this changed device/user file, after the old switch connection and device/user data were deleted.

Also in case of an upgrade from HiPath 4000 Vx (x less then 6) to the V6 the CAP V3.0 needs to adapt this: only the switch connection of the HiPath 4000 Vx must be deleted and then with the same ID a HiPath 4000 V6 connection type must be added. **(Previously it is recommended to backup the database.)** Every special seetings of the previous SCC must be adapted to the Telas.cfg of the new SCC connection (and the CA4000 relevant config settings to the CSTA integrated in V6 as well).

6.2.3 Configuration

To connect a HiPath 4000 for the first time or to reconfigure an existing connection, proceed as follows:

1. Click the **Switch connection** menu item in the navigation area.
   a) A connection has not yet been configured. Continue with 2a.
   b) One or more connections are already configured. These are displayed in a list. Continue with 2b.
2. Configure the connection.
   a) If a connection has not yet been configured, click the **Add new entry** icon and select **HiPath 4000** as the server version.
   b) If one or more connections are already configured, these are displayed in a list. Select a connection by clicking the **Modify** icon for the relevant connection.

   The HiPath 4000 configuration dialog now is displayed in the work area, comprising parts SCC, CA4000, and Switch.

"SCC" dialog

Field	Description
SCC Name	Enter a mnemonic name for the SCC here, e.g. "SCC-HP4000". This name can be assigned at the administrator's discretion. It must be unique within the entire CAP installation. Up to 32 characters (letters, numbers, underscore and hyphen) are permitted. Accentuated letters are supported only under Windows.
SCC Id (optional)	Enter an Id for the SCC here; the identifier must be unique within the entire OpenScape CAP installation; it cannot be changed after configuration has been completed. In the Diagnostic Agent, the "SCC Id" is used to display the SCC in the list of processes. In the same way, the associated CA4000 process is displayed as `CA4000_<SCC Id>`. The HiPath / OpenScape node number (for example, 10-60-200, 30-70-600, etc.) is usually used here. Up to 32 characters (letters, numbers, underscore and hyphen) are permitted. Accentuated letters are supported only under Windows. **Note**: When importing user data, the SCC Id must match the PBX Id in the import file.
SCC host name	The name of the host on which the SCC process is running must be specified here. A PC name directory is created in the directory `<InstDir>\config\` using the "host name". A subdirectory called `telas-server_<SCC Id>` is added for the SCC. A subdirectory called `ca4000_<SCC Id>` is added for the associated CA4000. These subdirectories contain all configuration files for these processes that are to be started. **Note:** For distributed installation (which means that the SCC PC is not your own PC/local host), you must install OpenScape CAP Service Starter on the specified SCC PC (cf. Section 4.3).
SCC IP address (cannot be edited)	Here the IP address of the PC on which the SCC process should run is displayed. The address is determined via the host name; it is shown just to allow for a sanity check.

Field	Description
SCC Port (optional)	The port assigned to the SCC process may be specified here. Port **26535** is used by default. If this port has already been assigned to a different SCC in the CAP configuration, the system automatically offers the next free port (for example, 26536).
ASN1 Single Domain Native Mode	If this SCC is connected to an SCCP or a TCSP (multi domain mode), you should keep the default value **Off**. In "multi domain mode", the SCC supports the CSTA III ASN.1, CSTA XML, and NetTSPI protocols. The SCC state is always "active". If you select a CSTA protocol version, the SCC operating mode changes to "single domain native mode". In this mode, the SCC passes a protocol through on a one-to-one basis, and its status is "not ready" if there is no application connection. Depending on application requirements, select from: ? `CSTA ACSE`: Interface is configured for CSTA Phase III and requires a login to the SCC via ACSE request (version 5) (for more information, see the OpenScape CAP Application Developers’ Guide), ? `CSTA III`: Interface is configured for CSTA Phase III.
CallID Management for TAPI	This box allows to activate the management of Call-IDs via Call-IDRepository which is necessary for selected TAPI applications only (refer to respective application documentation). Regularly the setting should be left **Off** without changes.
E164 number format	It is available only from SMR13. If this option is selected then E164 number formats will be used. This option can be used for HiPath 4000 V6 R2 and upwards switches

"CA4000" dialog

Field	Description
CA4000 IP address (not shown, cannot be edited)	This IP address is used for communication between SCC and CA4000. It is set automatically, equal to the SCC IP address, and will not be shown in the GUI.
CA4000 port (optional)	Optionally, you can specify the port provided by the CA4000 for this connection ("1025-5000"). The SCC addresses this port for communication to the CA4000. Port 4640 is used by default. Because there are occasionally problems with Windows processes that use ports in the range from "1025 - 1299", we recommend a port of "1300" or higher.

Field	Description
Switch Link Number (optional)	This number must be the same in the CA configuration and in the AMO CPTP:APPL. The crucial parameters in the AMO are the ACM number and the APPL number. They are calculated from the default value "50" plus the switch link number. (ACM 50 + switch link number; APPL 50 + switch link number). Example: Switch link number = 5 >>> ACM55;APPL55;
Switch sub-appl number (optional)	This number must be the same in the CA configuration and in the AMO XAPPL. The crucial parameter in the AMO is the sub-application number "Dxx" (D01-D32). Example: Switch sub appl number = 25 >>> D25
Use External DNIS (optional)	Activation of DNIS (Dialed Number Identification Service) is an additional information field in the "Delivered, Queued, Diverted, Established, Connection Cleared Event". Currently, the HiPath 4000 does not support this completely. If DNIS is activated, the HiPath 4000 conveys the number dialed by the external caller in this field. If DNIS is not active, the ANI (Automatic Number Identification) is conveyed in this field; this is the external caller's call number.

"Switch" dialog

Field	Description
IP address of the Switch	Enter the HiPath 4000 IP address here. If the connection is via the SL100/200, make sure that the IP address or the entire IP network of the SCC4000/CA4000 PC is entered in the firewall list.
SPI Account **SPI Password** **Business Group**	For direct access to the HiPath 4000 administration interface via the PBX Interface service (SPI), please enter the "HiPath Expert Access" login data here. Afterwards, the button "**Get device data**" is activated which allows to have device data imported from the switch at any time. Please note that this function allows to have devices created / device data modified - no devices will be removed from the CAP Management database. Devices always will be imported into the specified BG - it is currently not supported to distribute devices provided via SPI across multiple BGs.

Field	Description
Speed-dial numbers	Only the ComAssistant Phone Controller uses speed-dial numbers. If the application initiates the dialing, the system checks whether the external call number dialed has been configured in the assigned speed-dial list. If the number is found in the list, the SCC sends the configured speed-dial number to the HiPath 4000 for dialing, instead of the long call number. Speed-dial lists are only used if the CTI users do not have unrestricted trunk access, and would like to dial using an LDAP search result, even though they only have access to system speed-dialing. As a rule, call numbers for people are stored on an LDAP server as long call numbers in canonical format.
Domain numbers	The left part shows a list of configured domain numbers (see Section 7.2.3); use the arrow key to move selected entries relevant for this switch to the right hand side.
NAC	The left part shows a list of configured node access codes (see Section 7.2.4); use the arrow key to move selected entries relevant for this switch to the right hand side.
Private Numbering Plan	The left part shows a list of configured PNPs (see Section 7.2.5); use the arrow key to move selected entries relevant for this switch to the right hand side.

Actions

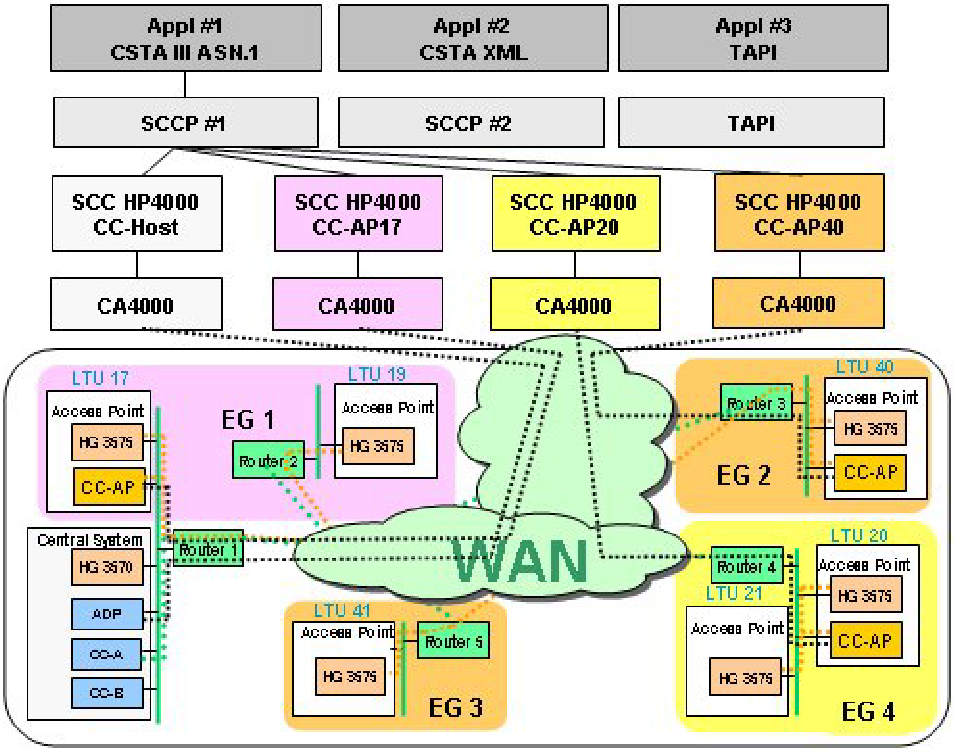
Action	Description
Add	Checks data for completeness and adds the entry to the switch connections list.
Close	Closes the **Add entry** dialog without saving the entries.
Delete	Deletes an existing switch connection. **Note**: This button only appears if at least one switch connection has already been configured.
Next >>	Calls up the next dialog.
<< Previous	Calls up the previous dialog.

6.2.4 Connecting a HiPath / OpenScape 4000 AP Emergency Configuration

With CAP V3.0 additional configuration features specific to AP Emergency have been provided to allow for applications to leverage the extended reachability of a HiPath / OpenScape 4000 network (cf. Section B.4).

6.2.4.1 Architecture

From the CAP point of view, any HiPath / OpenScape 4000 CC-AP will be handled like a "mini HiPath / OpenScape 4000", i.e. for connecting a HiPath / OpenScape 4000 CC-AP SCC4000 and CA4000 or SCC for 4000-embedded CSTA must be configured as usual.



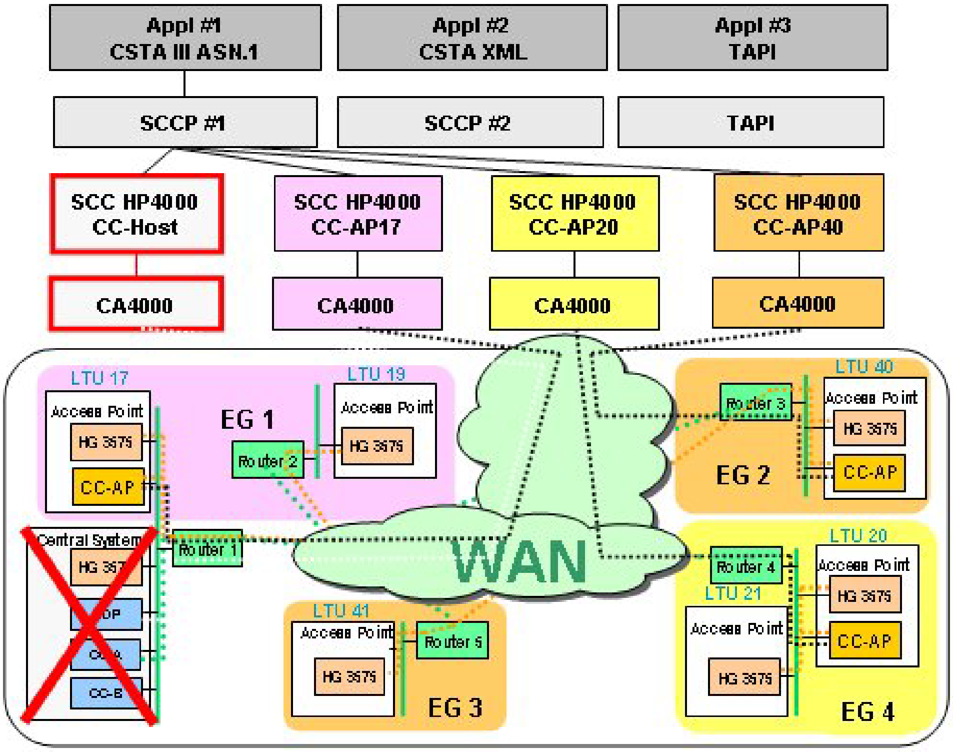
For each application an SCC Proxy is mandatory, coordinating and deciding which subscriber can be reached on which way.

Finally, for each device supporting AP Emergency the "emergency path" (i.e. the SCC4000 connecting to the respective HiPath / OpenScape 4000 CC-AP) must be configured in addition to the primary path (i.e. the SCC4000 connecting to the HiPath 4000 Server).

> Please note that the CAP AP Emergency support is provided for applications connecting via SCCP only.
> For direct access to single SCCs as well as for access via TAPI no AP Emergency support is available!

6.2.4.2 Failure Scenarios

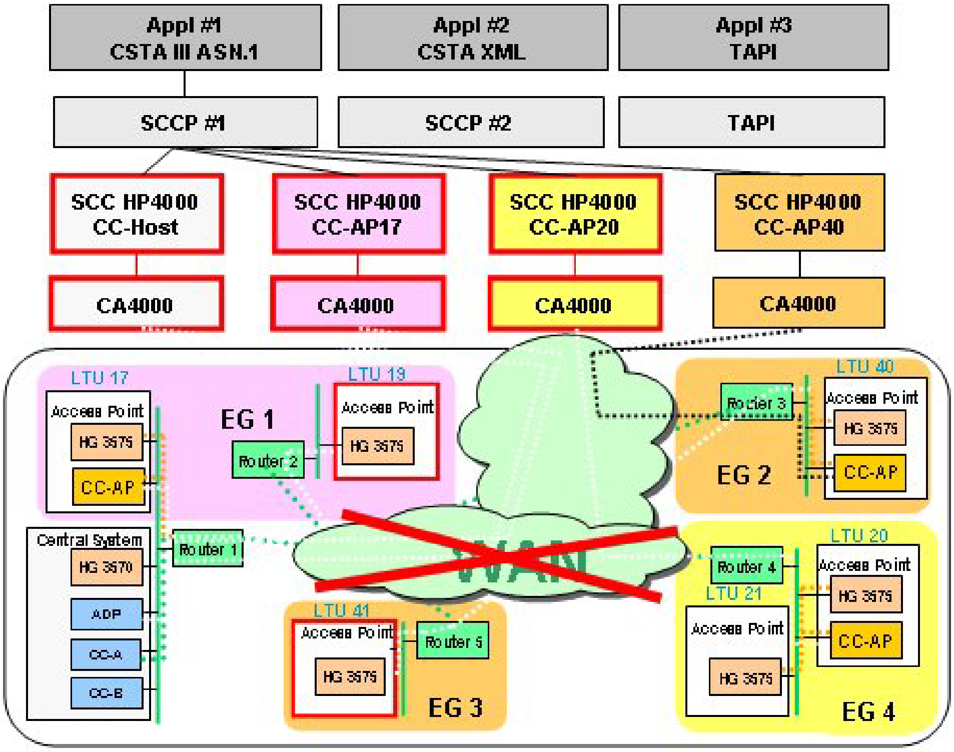
HiPath / OpenScape 4000 server failure



On HiPath / OpenScape 4000 level, all of the devices connected **locally** (i.e. to shelves within the server) are not reachable any more. All of the **Access Points** will survive the failure, as any AP is able to reach its own CC-AP.

On CAP level, only the connection between SCC4000 ("CC-Host") and HiPath 4000 server is interrupted, i.e. all devices connected locally are not reachable any more.

(Complete or partial) WAN failure



On HiPath / OpenScape 4000 level, all of the devices connected **locally** (i.e. to shelves within the server) will survive the failure. The same is true for **Access Points** that still can reach the assigned CC-AP (AP20, AP21, AP40 in the example) or that are directly connected to the HiPath / OpenScape 4000 server (AP17 in the example). Remaining Access Points experience a total failure (AP19, AP41 in the example).

On CAP level, in the example above almost all of the SCC4000 connections are broken; only devices connected to AP40 are still reachable because the SCC4000 "CC-AP40" is not affected by the partial WAN failure.

6.2.4.3 Configuration

As sketched above, components must be configured as follows:

? Switch connection
SCC4000 towards each HiPath 4000 CC-AP

? SCC Proxy
SCCP per application as coordinating instance

? Device
Entry for alternative SCC4000 to CC-AP for any AP-enabled device

For configuration of the switch connection, basically proceed as described in Section 6.2.3; subsequently, only specific deviations will be described.

1. Click the **Switch connection** menu item in the navigation area.
   The SCC4000 connected to the HiPath / OpenScape 4000 server should be visible already
2. Configure the connection: click the **Add new entry** icon and select **HiPath 4000** as the server version.

   The HiPath 4000 configuration dialog now is displayed in the work area, comprising parts SCC, CA4000, and Switch.

Basically, any HiPath 4000 CC-AP has administration data identical to the HiPath 4000 server (except for some minor deviations, but in particular subscriber numbers and dialling plan are identical).

Based on the identical HiPath 4000 data we recommend to use the SCC4000 configuration settings for the HiPath 4000 server as a blueprint for subsequent configuration of the additional SCC4000 instances.

"SCC" dialog

Field	Description
SCC Name	A new string must be defined as SCC Name. It may be helpful if the string is defined to contain info about ? being an SCC connected to a HiPath / OpenScape 4000 CC-AP (not to a HiPath / OpenScape 4000 server) ? which HiPath / OpenScape 4000 server the CC-AP is assigned to ? which of several CC-APs is the one addressed here Naming rules apply as specified in Section 6.2.3.
SCC Id (optional)	A new string must be defined as SCC Id. It may be helpful if the string is defined to contain info about ? being an SCC connected to a HiPath / OpenScape 4000 CC-AP (not to a HiPath / OpenScape 4000 server) ? which HiPath / OpenScape 4000 server the CC-AP is assigned to ? which of several CC-APs is the one addressed here Naming rules apply as specified in Section 6.2.3.

Field	Description
SCC host name	The name of the host on which the SCC process is running must be specified here. This need not be the same host as specified for the HiPath 4000 server connection! Naming rules apply as specified in Section 6.2.3.
remaining fields	as specified in Section 6.2.3.

"CA4000" dialog

Field	Description
CA4000 IP address (not shown, cannot be edited)	as specified in Section 6.2.3.
CA4000 port (optional)	Define a new, as of yet unused port here. Rules apply as specified in Section 6.2.3.
Switch Link Number (optional)	Define a new, as of yet unused combination (like 6 / 26 etc.) here. This combination must have been configured accordingly on HiPath / OpenScape 4000 side (AMOs as described in Section 6.2.3).
Switch sub-appl number (optional)	
Use External DNIS (optional)	as specified in Section 6.2.3.

"Switch" dialog

Field	Description
IP address of the Switch	Please specify the IP address of the HiPath / OpenScape 4000 CC-AP LAN interface here. If the connection is via the SL100/ 200, make sure that the IP address or the entire IP network of the SCC4000/CA4000 PC is entered in the firewall list of every CC-AP.
remaining fields	as specified in Section 6.2.3.

For configuring the SCC Proxy, proceed as specified in Section 6.5.2.
Please pay special attention to the description of the "Disable AP Emergency" field.

For configuring devices, proceed as specified in Section 7.4.2.
Please pay special attention to the description of the "Emergency" field.

6.3 HiPath 3000 connectivity

6.3.1 Overview

HiPath 3000 supports the CSTA III standardized protocol for communication with applications (subject to prior ACSE login). CSTA is a standard for computer-supported telephony (CTI) that was established by the international standardization organization ECMA (European Computer Manufacturers Association). The physical connection between the HiPath 3000 and a PC that is running SCCHiPath3000 is set up with the help of a TCP/IP LAN connection or an ISDN S_0 connection.
HiPath 3000 supports a maximum of eight CSTA III connections at one time. Depending on the HiPath 3000 software version used, the number CSTA III connections released may be less than eight.

> > The TCP/IP connection to the HiPath 3000 is released only via the HG1500. The TCP/IP connection via the **LIM module** is **not** supported!
> HiPath 3000 configurations using the **CSP component** are **not** supported either; the "CSP flag" must be deactivated in the H3000 configuration; otherwise a CSTA event flow may result that creates problems in the SCC3000.

6.3.2 Preparation

To enable HiPath 3000 connectivity, a CSTA link must be set up as described in the HiPath 3000 documentation. The HiPath 3000 CSTA interface can be reached from all IP addresses by default. Using the application firewall list, however, it is possible to release or block separate IP addresses or entire IP networks.

6.3.3 Configuration

To connect a HiPath 3000 for the first time or to reconfigure an existing connection, proceed as follows:

1. Click the **Switch connection** menu item in the navigation area.
   a) A connection has not yet been configured. Continue with 2a.
   b) One or more connections are already configured. These are displayed in a list. Continue with 2b.
2. Configure the connection.

a) If a connection has not yet been configured, click the **Add new entry** icon and select **HiPath 3000** as the server version.

b) If one or more connections are already configured, these are displayed in a list. Select a connection by clicking the **Modify** icon for the relevant connection.

The HiPath 3000 configuration dialog now is displayed in the work area, comprising parts SCC and Switch.

"SCC" dialog

Field	Description
SCC Name	Enter a mnemonic name for the SCC here, e.g. "SCC-HP3000". This name can be assigned at the administrator's discretion. It must be unique within the entire CAP installation. Up to 32 characters (letters, numbers, underscore and hyphen) are permitted. Accentuated letters are supported only under Windows.
SCC Id (optional)	Enter an Id for the SCC here; the identifier must be unique within the entire OpenScape CAP installation; it cannot be changed after configuration has been completed. In the Diagnostic Agent, the "SCC Id" is used to display the SCC in the list of processes. The HiPath node number (for example, 10-60-200, 30-70-600, etc.) is usually used here. Up to 32 characters (letters, numbers, underscore and hyphen) are permitted. Accentuated letters are supported only under Windows. **Note**: When importing user data, the SCC Id must match the PBX Id in the import file.
SCC host name	The name of the host on which the SCC process is running must be specified here. A PC name directory is created in the directory `<InstDir>\config\` using the "host name". A subdirectory called `telas-server_<SCC ID>` is added for the SCC. This subdirectory contains all configuration files for these processes that are to be started. **Note:** For distributed installation (which means that the SCC PC is not your own PC/local host), you must install OpenScape CAP Service Starter on the specified SCC PC (cf. Section 4.3).

Field	Description
SCC IP address (cannot be edited)	Here the IP address of the PC on which the SCC process should run is displayed. The address is determined via the host name; it is shown just to allow for a sanity check.
SCC Port (optional)	The port assigned to the SCC process may be specified here. Port **26535** is used by default. If this port was already assigned to a different SCC by the CAP configuration, the system automatically offers the next free port (for example, 26537).

"Switch" dialog

Field	Description
Switch Connectivity	Select to have the switch connected via **LAN**, via **ISDN Link,** or via **V24**. Subsequent contents of the Switch dialog depend on the selection here. We describe the LAN connection first. For connection via ISDN, see Section 6.3.4. For connection via V.24, see Section 6.3.5.
IP address of the Switch	Enter the HiPath 3000 IP address via which the CSTA interface of the HiPath 3000 switching PC can be reached.
Port of the Switch (optional)	Enter the port **7001** here. HiPath 3000 does not support any other connection ports.
Speed-dial numbers	Only the ComAssistant Phone Controller uses speed-dial numbers. If the application initiates the dialing, the system checks whether the external call number dialed has been configured in the assigned speed-dial list. If the number is found in the list, the SCC sends the configured speed-dial number to the HiPath 3000 for dialing, instead of the long call number. Speed-dial lists are only used if the CTI users do not have unrestricted trunk access, and would like to dial using an LDAP search result, even though they only have access to system speed-dialing. As a rule, call numbers for people are stored on an LDAP server as long call numbers in canonical format.
Domain numbers	The left part shows a list of configured domain numbers (see Section 7.2.3); use the arrow key to move selected entries relevant for this switch to the right hand side.
NAC	The left part shows a list of configured node access codes (see Section 7.2.4); use the arrow key to move selected entries relevant for this switch to the right hand side.

Field	Description
Private Numbering Plan	The left part shows a list of configured PNPs (see Section 7.2.5); use the arrow key to move selected entries relevant for this switch to the right hand side.

Actions

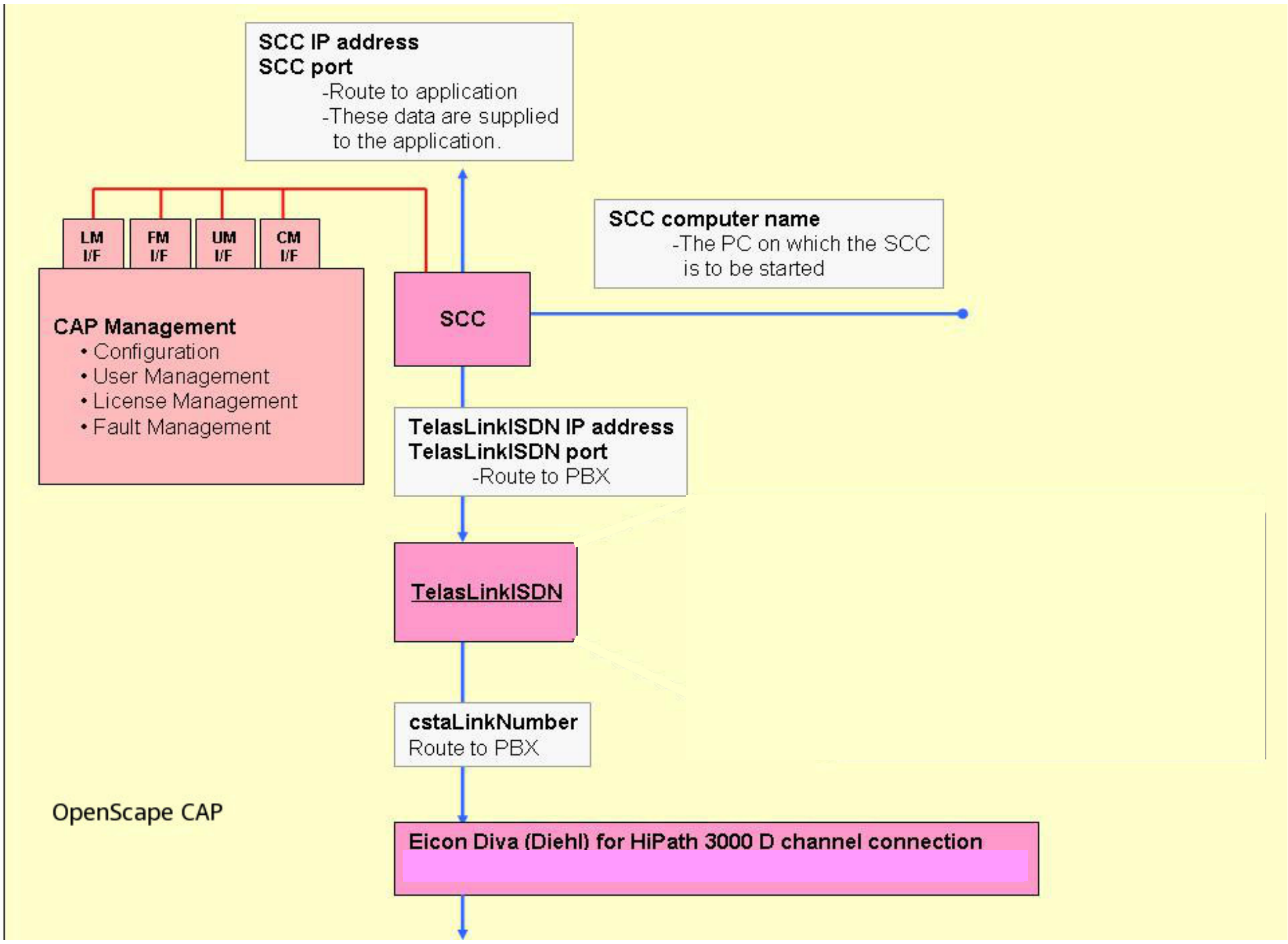
Action	Description
Add	Checks data for completeness and adds the entry to the switch connections list.
Close	Closes the **Add entry** dialog without saving the entries.
Delete	Deletes an existing switch connection. **Note**: This button only appears if at least one switch connection is already configured.
Next >>	Calls up the next dialog.
<< Previous	Calls up the previous dialog.

6.3.4 HiPath 3000 connectivity via ISDN link

As an option for HiPath 3000, SCC connectivity may be done via ISDN. For that purpose, the `TelasLinkISDN.exe` component has been provided as a TCP/IP-ISDN converter. This program may be started only once on each PC; accordingly, a separate PC must be used for each HiPath 3000 ISDN connection.

The program opens a TCP port to which the SCC can connect on one side. The first ISDN card in the PC is accessed on the other side.

> The ISDN connection to the HiPath 3000 is established via D channel; it is supported by the Eicon Diva (Diehl) ISDN card only



Just like the SCC components, `TelasLinkISDN.exe` is installed automatically as part of the CAP Call Control Service. It is configured during creation of a HiPath 3000 connectivity.

Please note that corresponding components SCC, LinkISDN, and ISDN card must be hosted on the same PC.

Configuration is as described in Section 6.3.3; only the "Switch" dialog changes as follows:

"Switch" dialog

Field	Description
Switch Connectivity	Select **ISDN Link** here.
Link IP Address (not shown, cannot be edited)	This IP address is used for SCC to LinkISDN communication. It is set automatically equal to the SCC Host IP address and is not displayed in the GUI.
Link Port	Define the port to be used for SCC to LinkISDN communication.
Link Number	Define the number (ISDN phone number) to be used for ISDN access to the HiPath 3000 switch
Speed-dial numbers	... remaining fields as described in Section 6.3.3.

Tabelle 6-1

6.3.5 HiPath 3000 connectivity via V.24

As an option for HiPath 3000, SCC connectivity may be done via V.24. For that purpose, the `TelasLinkV24.exe` component has been provided. This program may be started only once on each PC; accordingly, a separate PC must be used for each HiPath 3000 V.24 connection.

The program opens a TCP port to which the SCC can connect on one side. The V.24 interface of the PC is accessed on the other side.

Just like the SCC components, `TelasLinkV24.exe` is installed automatically as part of the CAP Call Control Service. It is configured during creation of a HiPath 3000 connectivity. Please note that corresponding components SCC, and LinkV24 must be hosted on the same PC.

Configuration is as described in Section 6.3.3; only the "Switch" dialog changes as follows:

"Switch" dialog

Field	Description
Switch Connectivity	Select **V24** here.
Link IP Address (not shown, cannot be edited)	This IP address is used for SCC to LinkV24 communication. It is set automatically equal to the SCC Host IP address and is not displayed in the GUI.

Field	Description
Link Port	Define the port to be used for SCC to LinkV24 communication.
Speed-dial numbers	... remaining fields as described in Section 6.3.3.

6.4 "Virtual" Connectivity

6.4.1 Overview

There are certain scenarios where applications want to make use of the CAP phone number handling facilities (SAT, see Section 2.3.4) without the need for really controlling the respective devices. For that purpose, all of the configuration data tied to a switch numbering plan must be available but no SCC or Connectivity Adapter service needs to be installed.

This specific configuration is provided by means of a "virtual" connectivity. It allows subsequently devices to be imported / defined which are assigned to that "virtual" connectivity, and which are processed correspondingly in SAT.

6.4.2 Configuration

To establish a virtual connectivity for the first time or to reconfigure an existing one, proceed as follows:

1. Click the **Switch connection** menu item in the navigation area.
   a) A connection has not yet been configured. Continue with 2a.
   b) One or more connections are already configured. These are displayed in a list. Continue with 2b.
2. Configure the connection.
   a) If a connection has not yet been configured, click the **Add new entry** icon and select **Virtual** as the switch type.
   b) If one or more connections are already configured, these are displayed in a list. Select a connection by clicking the **Modify** icon for the relevant connection.

   The Virtual configuration dialog now is displayed in the work area, comprising parts SCC and Switch.

"SCC" dialog

Field	Description
SCC Name	Enter a mnemonic name for the SCC here, e.g. "Virtual1". This name can be assigned at the administrator’s discretion. It must be unique within the entire CAP installation. Up to 32 characters (letters, numbers, underscore and hyphen) are permitted. Accentuated letters are supported only under Windows.
SCC Id (optional)	Enter an Id for the SCC here; the identifier must be unique within the entire OpenScape CAP installation; it cannot be changed after configuration has been completed. The HiPath node number (for example, 10-60-200, 30-70-600, etc.) is usually used here. Up to 32 characters (letters, numbers, underscore and hyphen) are permitted. Accentuated letters are supported only under Windows. **Note**: When importing user data, the SCC Id must match the PBX Id in the import file.
SCC host name **SCC IP address** **SCC Port**	As no SCC will be running for a virtual connectivity, these fields will be ignored.

"Switch" dialog

Field	Description
IP address of the Switch **Port of the Switch**	As no switch connection will be established for a virtual connectivity, these fields will be ignored.
Speed-dial numbers	Only the ComAssistant Phone Controller uses speed-dial numbers. If the application initiates the dialing, the system checks whether the external call number dialed has been configured in the assigned speed-dial list. If the number is found in the list, the SCC sends the configured speed-dial number to the HiPath 3000 for dialing, instead of the long call number. Speed-dial lists are only used if the CTI users do not have unrestricted trunk access, and would like to dial using an LDAP search result, even though they only have access to system speed-dialing. As a rule, call numbers for people are stored on an LDAP server as long call numbers in canonical format.

Field	Description
Domain numbers	The left part shows a list of configured domain numbers (see Section 7.2.3); use the arrow key to move selected entries relevant for this switch to the right hand side.
NAC	The left part shows a list of configured node access codes (see Section 7.2.4); use the arrow key to move selected entries relevant for this switch to the right hand side.
Private Numbering Plan	The left part shows a list of configured PNPs (see Section 7.2.5); use the arrow key to move selected entries relevant for this switch to the right hand side.

Actions

Action	Description
Add	Checks data for completeness and adds the entry to the switch connections list.
Close	Closes the **Add entry** dialog without saving the entries.
Delete	Deletes an existing switch connection. **Note**: This button only appears if at least one switch connection is already configured.
Next >>	Calls up the next dialog.
<< Previous	Calls up the previous dialog.

6.5 Configuring an OpenScape CAP Call Control Proxy (SCCP)

6.5.1 Overview

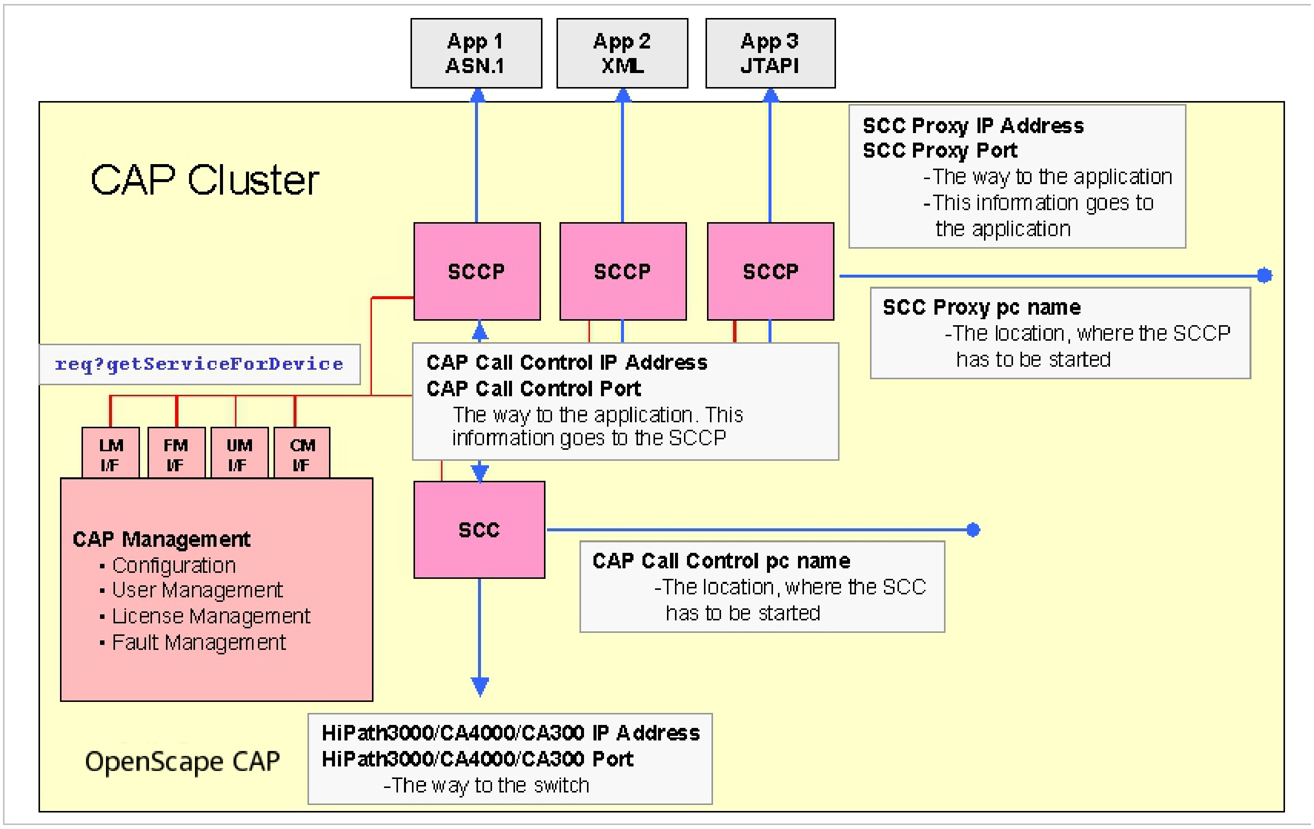
An SCCP instance should be configured for every application that is to use OpenScape CAP in a CSTA or JTAPI multi domain configuration and for every XML Phone Service.

SCC proxies are only used in "multi domain mode". An SCCP supports the CSTA III ASN.1 and CSTA XML protocols. An SCCP always supports only one connection to an application. Several SCCPs can set up a connection to the same SCC at the same time. The SCCP handles application authentication, user licensing, and determination of the SCCs belonging to the CAP devices. It uses the CAP Management services for these jobs.

When setting up a connection to an SCCP, an application must first send an ACSE_AARQ. This request contains:

- User
- Password
- CSTA version
- Application ID
- Native (mode), true or false (default)

After successful authentication, the SCCP saves the application ID for this existing connection and uses it for subsequent user licensing. With each additional CSTA request (for a device), the SCCP uses a connection to CAP License Management (SLM) to check whether a license (according to the application ID) has been assigned for this device (or for the associated user). If automatic license assignment has been activated, an appropriate client license is automatically assigned to a device/user, if such a license is not already available. If the license check is successful, the SCCP saves this for 3600 seconds and forwards the request to the SCC associated with the device.



6.5.2 Configuration

To configure an SCCP instance for the first time or to reconfigure an existing SCCP instance, proceed as follows:

1. Click the **SCC Proxy** menu item in the navigation area.

   a) An SCCP instance has not yet been configured. Continue with 2a.

   b) One or more SCCP instances are already configured. These are displayed in a list. Continue with 2b.

2. Configure the SCCP instance.

   a) If an SCCP instance has not yet been configured, click the **Add new entry** icon.

   b) If one or more SCCP instances are already configured, these will be displayed in a list. Select an SCCP instance by clicking the **Modify** icon for the selected SCCP instance.

Dialog

Field	Description
SCC Proxy Name	Enter a mnemonic name for the SCC Proxy here. This name can be assigned at the administrator’s discretion. It must be unique within the entire CAP installation. Up to 32 characters (letters, numbers, underscore and hyphen) are permitted. Accentuated letters are supported only under Windows.
SCC Proxy Identifier (optional)	Enter an Id for the SCC proxy here. The identifier must be unique within the entire OpenScape CAP installation and cannot be modified after creation. In the Diagnostic Agent, this "SCCP Id" is used to display the SCCP in the list of processes. Up to 32 characters (letters, numbers, underscore and hyphen) are permitted. Accentuated letters are supported only under Windows. Blanks are not allowed!
SCC Proxy host name	Enter the host name of the PC on which the SCCP process is to run. A PC name directory is created in the directory `<InstDir>\config\` using the "host name". A subdirectory called "sccp_<SCCP ID>" is added for the SCCP. These subdirectories contain all configuration files for this process that is to be started. **Note**: For distributed installation (i.e. the SCCP PC is not your own PC/local host) ensure that you install OpenScape CAP Service Starter on the specified SCCP PC (cf. Section 4.3).
SCC Proxy IP address (cannot be edited)	Here the IP address of the PC on which the SCCP process should run is displayed. The address is determined via the host name; it is shown just to allow for a sanity check.
SCC Proxy port (optional)	As an option, you can enter the port to which the SCCP process is to be assigned. Port **27535** is used by default. If this port was already assigned to a different SCCP by the CAP configuration, the system automatically offers the next free port (for example, 27536).

Field	Description
Disable AP Emergency	You can deactivate the AP Emergency feature on CAP level (and on application level) here; it will still be active on HiPath / OpenScape 4000 level, however: With a HiPath / OpenScape 4000 AP Emergency configuration a device connected to a remote AP shelf still can only be reached by SCCP via the "primary" SCC4000 ("SCC ID"). Even in case an additional SCC4000 ("emergency") path has been created for this device, it would not be used in case of emergency (which means the device is unreachable for the application during the emergency period). Deactivating AP Emergency on CAP level can be reasonable ? in case the SCCP is connected to non-HiPath / OpenScape 4000 switches only (AP Emergency is a HiPath / OpenScape 4000 only feature) ? in case the SCCP is connected to HiPath / OpenScape 4000 switches (via SCC4000), but none of these switches will make use of the AP Emergency feature ? in case the application using SCCP and SCC4000 with connections to HiPath / OpenScape 4000 switches with AP Emergency enabled does not want to have a "seamless" APE switch-over without being notified. **ATTENTION**: It is not possible to restrict this feature to specific devices or HiPath / OpenScape 4000 switches - de-/activation always is valid for an SCCP with all its connected HiPath / OpenScape 4000 switches!

Actions

Action	Description
Add	Adds the entry to the list of SCCP services.
Close	Closes the **Add entry** dialog without saving the entries.
Delete	Deletes an existing SCCP Instance. **Note**: This button only appears if at least one SCCP instance is already configured.

7 Additional OpenScape CAP Management Functions

You can use OpenScape CAP Management to configure all of the OpenScape CAP. OpenScape CAP Management provides the following functions for this purpose:

? **Service**
This function allows you to configure the switch connections (SCC) and SCCP instances. You can also configure the XML Phone Service and assign speed-dial numbers here.

? **User**
This menu encompasses user management, enabling you to add, change or remove users and bring users together to form user groups. Common settings like default passwords can be defined here as well.

? **Device**
This is where you configure and modify the devices (phones, trunks, hunt groups, etc.) attached to the various PBXes. Licenses are assigned to devices here.

? **Licenses**
This menu allows you to install and uninstall licenses. It provides an overview of license usage and control mechanisms for license assignment.

? **Data**
Here you can make the settings for exporting or importing the OpenScape CAP database.

? **Diagnosis**
This menu is used to start the CAP Management Diagnostic Agent. It provides monitoring, configuration and problem diagnostics functions for all components in the system: logging information, display and modification of configuration data, service and process states, show participating hosts, restart processes. Moreover, the Download Data function allows to store selected diagnostic data in a file for offline analysis.

? **Logout**
This menu supports terminating the CAP Management session; no sub-menus are available here.

? **Help**
You can display the OpenScape CAP documentation in the various formats and languages here.

The functions listed here can be found as menu items in the OpenScape CAP Management main menu. When you click a menu item, the selection list in the navigation area and the display in the work area change accordingly.

7.1 Business Groups

For the first time, HiPath CAP V3.0 SMR4 provides support for business groups (BG); these are meant to divide the administrative area into separate regions of visibility and responsibility. The administrator can define business groups and assigned business group administrators (BGAdmin). Each BGAdmin is limited to viewing and administrating data of the attached BG only.

Objects assigned to a BG are

? users

? devices

? licenses

? user groups

? URLs for XML Phone Service

In order to also get hold of objects that are not assigned to a specific BG, a "pseudo" business group "Standard" or "none" is created automatically during installation.

Functions available to a BGAdmin (in the assigned BG) are

? create and manage users (CTI user role only) and devices

? import / export data, confined to users and devices of the BG

? create and manage user groups

? manage BG attributes

? define URLs for XML Phone Service

? manage assigned licenses

? as well as unlimited access to diagnostic functions

Functions confined to the "super" administrator only are

? configure services (SCC, SCCP, XML Phone Service)

? create domains / PNPs / NACs

? create and delete BGs

? create and manage Admin as well as BGAdmin users

? install / uninstall licenses

? assign installed licenses to BGs

? manage security settings for communication links

Subsequent descriptions always cover the complete admin functionality; parts that are not accessible to BGAdmins are marked as "**not for BGAdmin**".

7.2 Service

The Call Control Services and Call Control Proxies are configured in **Service**. You can also configure the XML Phone Service and assign speed-dial numbers here.

7.2.1 Switch connection (not for BGAdmin)

Information on how to configure the Call Control Services with OpenScape CAP Management is described in Section 6.2 to Section 6.3.5.

7.2.2 SCC proxy (not for BGAdmin)

Information on how to configure the Call Control Proxies with OpenScape CAP Management is described in Section 6.5.

7.2.3 Domain information (not for BGAdmin)

Domain information is used as part of the dialling information in a switch configuration; here they can be defined and be assigned with an identifier, to be re-used when configuring switch connectivities.

1. Click **Service** in the main menu and select the **Domain information** menu item in the navigation area. A list of available domain info entries is presented for selection / modification.
2. To configure a new domain info, click the button in the header line.

   A table opens to enter data for a new domain information as follows:

Field	Description
Name of domain	Enter a useful name here.
Id of domain (optional)	You may enter an Id here which must be unique in the entire system. In case you don’t, it will be assigned automatically.
Country code	Country code (e.g. "49" for Germany). This is used to derive a country’s standard outdial rule. It defines the first part of a device ID in the canonical format that is assigned to the respective SCC instances. To avoid inconsistent settings, no direct data entry is possible here; instead, select one of the supported countries from the pull-down menu - the value will be transferred automatically.

Field	Description
National prefix	Prefix for a national E.164 call number. It is automatically derived from a country’s outdial rule and only needs to be configured if it does not comply with the national standard. The SAT uses the "National prefix" (implicit/ explicit) for unambiguous identification of a device if a call number is transmitted with the "National prefix" in an event.
International prefix	Prefix for an international E.164 call number. It is automatically derived from a country’s outdial rule and only needs to be configured if it does not comply with the national standard. The SAT uses the "International prefix" (implicit/explicit) for unambiguous identification of a device if a call number is transmitted with the "International prefix" in an event.
PBX format	can be one of "international" or "national" (meaning US format) as configured in the PBX.
Outside line access **International outside line access**	Access code (for example, "0"). The SAT uses "Outside line access" for unambiguous identification of a device if a call number is transmitted with "outside line access" in an event. ComAssistant continues to use this code for each outgoing external call.
Area code (optional)	Enter the area code (e.g. "89" for Munich) here. It defines the second part of a device ID in the canonical format that is assigned to the respective SCC instances.
Main number	Enter the number of the main connection within a local network (e.g. "722" for Unify, Munich, Hofmannstraße). It defines the third part of a device ID in the canonical format that is assigned to the respective SCC instances.
Overlap (optional)	The number of overlapping numbers in the "Main number" and the extension, for example, for 49(89)722:1, which means that if the overlap=1, the PBX format for device +49(89)722-345 is 2345, which means the last digit of the main number (in this case: 2) precedes the extension (in this case: 345) and the resulting call number 2345 is configured in the PBX. It is not allowed to set 0 into this field!

Field	Description
Virtual node Code	It can be used special in case of the HiPath / OpenScape 4000 feature, called 'Non-unique numbering plan' (NUNP). Please configure this number only for Domain information, which will be assigned to SCC connection of a HiPath / OpenScape 4000 with NUNP. For more information, see chapter '5.6 Non-unique numbering plan (NUNP)' the OpenScape CAP Application Developers' Guide Vol. 1

3. Enter data as required, and confirm with **Add**.
4. The new domain information is shown in the list view.

   The domain information has been stored and can now be used when configuring or modifying PBX access data.

   Remark: In case of any domain modification, the OpenScape CTI service must be restarted!

7.2.4 Node Access Codes (not for BGAdmin)

Node Access Codes (NAC) are used as part of the dialling information in a switch configuration; here they can be defined and be assigned with an identifier, to be re-used when configuring switch connectivities.

1. Click **Service** in the main menu and select the **Node access codes** menu item in the navigation area. A list of available NAC entries is presented for selection / modification.
2. To configure a new NAC, click the button in the header line.

   A table opens to enter data for a new NAC as follows:

Field	Description
NAC Name	Enter a useful name here.
NAC Id (optional)	You may enter an Id here which must be unique in the entire system. In case you don't, it will be assigned automatically.

Field	Description
NAC	In the case of HiPath / OpenScape networks with open numbering, the NAC (Node Access Code) is the node code, which means the call number of a PBX node. This node code precedes the extension when dialing (for example, 96-2345 if the NAC=96 and 99-2345 if the NAC=99). This enables the same extension (in this case: 2345) to be configured in several PBX nodes (in this case: 96 and 99); the number becomes unique when the NAC precedes it. The SAT uses the NAC for unambiguous identification of a device if a call number is transmitted with the "NAC" in an event.
Overlap	The number of overlapping numbers in the NAC and extension, for example, for 962:1, which means that if the overlap=1, the PBX format for device 962-345 is 2345, which means that the last digit of the NAC (in this case: 2) precedes the extension (in this case: 345) and the resulting call number 2345 is configured in the PBX.

3. Enter data as required, and confirm with **Add**.

4. The new NAC entry is shown in the list view.
   The NAC has been stored and can now be used when configuring or modifying PBX access data.

7.2.5 PNP (not for BGAdmin)

Private numbering plans (PNP) are used as part of the dialling information in a switch configuration; here they can be defined and be assigned with an identifier, to be re-used when configuring switch connectivities.

1. Click **Service** in the main menu and select the **PNP** menu item in the navigation area. A list of available PNP entries is presented for selection / modification.
2. To configure a new PNP, click the button in the header line.

   A table opens to enter data for a new PNP as follows:

Field	Description
PNP Name	Enter a useful name here.
PNP Id (optional)	You may enter an Id here which must be unique in the entire system. In case you don’t, it will be assigned automatically.
PNP Outside line access	Code for accessing a private number network. These networks are configured according to ECMA-155 PNP (Private Network Numbering Plan). The SAT uses "PNP Outside line access" for unambiguous identification of a device if this access number is transmitted along with a call number in an event.
Prefix level 2 code	Prefix for a level 2 PNP call number. The SAT uses "Prefix level 2 code" for unambiguous identification of a device if this prefix is transmitted along with a call number in an event.
Prefix level 1 code	Prefix for a level 1 PNP call number. The SAT uses "Prefix level 1 code" for unambiguous identification of a device if this prefix is transmitted along with a call number in an event.
Level 2 code (optional)	PNP Level 2 code (corresponds to country code in E.164) The "Level 2 code" defines the first part of a device ID in the canonical format that is assigned to respective SCC instances.
Level 1 code (optional)	PNP Level 1 code (corresponds to the area code in E.164) The "Level 1 code" defines the second part of a device ID in the canonical format that is assigned to respective SCC instances.

Field	Description
Local code	PNP Level 0 code (corresponds to the main number in E.164) The "Local code" defines the third part of a device ID in the canonical format that is assigned to respective SCC instances.
Overlap (optional)	The number of overlapping numbers in the "Local code" and the extension, for example, for 33-44-552:1, which means that if the overlap=1, the PBX format for device 3344552-345 is 2345, which means the last digit of the local code (in this case: 2) precedes the extension (in this case: 345) and the resulting call number 2345 is configured in the PBX.

3. Enter data as required, and confirm with **Add**.
4. The new PNP entry is shown in the list view.

   The PNP has been stored and can now be used when configuring or modifying PBX access data.

7.2.6 Speed-dial numbers (not for BGAdmin)

Speed-dial numbers are used by the ComAssistant CTI application to optimize the dialing process. However, they are not necessarily required. Configuration is therefore optional. Speed-dial numbers are useful for ComAssistant users who only have speed-dial authorization for the system but would like to set up a connection with an LDAP search result even though the LDAP server only supports the existing call numbers in canonical format (standard). The ComAssistant converts canonical call numbers into speed-dial numbers.
Speed-dial numbers are administered in freely configurable lists. Only one list can be assigned to each SCC in the SCC configuration.

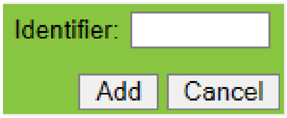
1. Click **Service** in the main menu and select the **Speed-Dial Numbers** menu item in the navigation area.

   Define a name for the location by using a **Speed-dial number identifier** which is used as the speed-dial number list. For each selected entry in the first window, **Speed-dial number identifier**, the entries that have already been assigned are displayed in the second window, **Speed-dial number/Long number**. The speed-dial number identifier must be unique throughout the entire system. If possible, enter a mnemonic ID (such as the exact designation of the location); this will be displayed in a selection dialog when configuring a PBX.

To configure a new speed-dial number, proceed as follows:

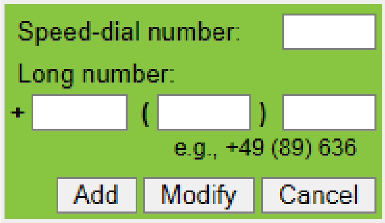
2. Click the button next to the **Speed-dial number ID** selection window.

   The window for entering the speed-dial number identifier is opened:



3. Enter the text in the input field and click **Add** to confirm. The window is closed and your entry appears in the **Speed-Dial Numbers Identifier** window.

   The window for entering the number combination is opened:



4. Enter the speed-dial number and the long number.

   The long number consists of three parts: country code without leading **+**; area code without leading **0**; and main number of extension.

> Make sure the correct number format is used.

5. Confirm with **Add** and your entry will appear in the **Speed-Dial Number/Long Number** window.
6. Click **Cancel** to close the window.
7. Click **Submit** in the main dialog to finally enter the configuration.

   The speed-dial number is now configured and can be used when configuring or modifying PBX access data.

7.2.7 XML Phone Service (not for BGAdmin)

General Overview

XML Phone Services for HiPath CAP is a component that allows XML developers to create or integrate a wide array of applications for HiPath 4000 and HiPath 3000 devices.

Using the (optional) WML adaptor, WAP-enabled devices, such as optiPoint 600 units or even mobile phones, can access XML applications. Future enhancements of the CAP XML Phone Services will also support voice-controlled access.

CAP users can therefore develop new applications with which the device (circuit-switched or IP-based) is used as an input/output device. In addition, office applications can be enhanced so that they can also be accessed by telephone. The XML applications are deployed using the standard HTTP/HTTPS protocol supported by standard Web servers (such as, Microsoft IIS, Apache, EJB server, and Servlet Engine). The programming language that is used for the XML application is consequently irrelevant, that is, it does not matter whether the XML applications are developed using script languages like PHP, Perl or standard programming languages like C# in the .Net environment, Java, or other programming languages.

Some examples of relevant XML applications are:

? Information systems (for example, stock market quotes, travel information, customer information etc.)

? Personal or group address books

? Management applications (for example, for PIN administration)

? Changing presence contexts

? Activating call forwarding from a list of possible destinations

? Instant messaging

Additional information on the XML Phone Service is available in the XMLPS Application Developers' Guide which comes with the CAP documentation; after CAP installation, it is available on-line as well via the URL `http://<CAP host>:8172`.

XML Phone Service

The XML Phone Service (XMLPS) is a CSTA XML application that is always installed on top of SCCP. An XMLPS can operate different XML applications simultaneously. If you want to use more than one XML Phone Service, you must configure a new SCCP for each XMLPS. In addition, each XMLPS must have a separate TDD application number (default = 999).

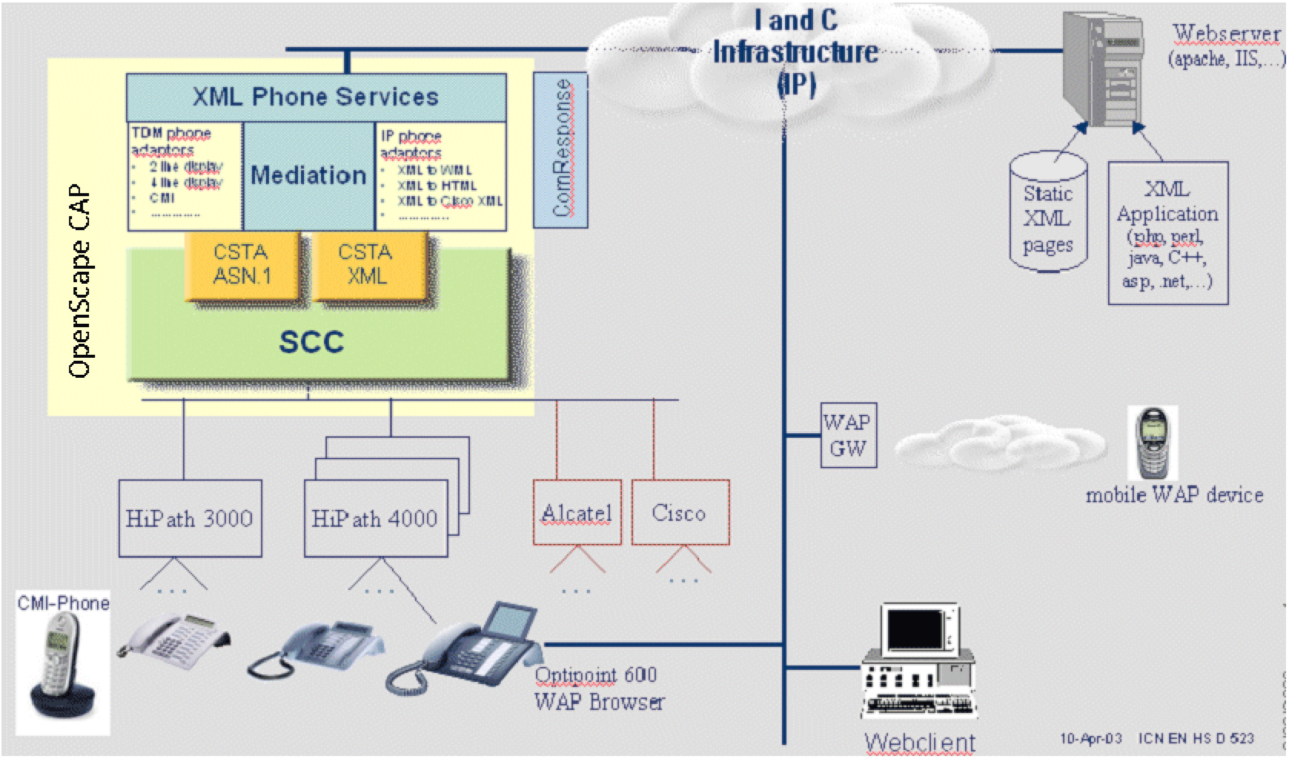
This change is made in the configuration file `<InstDir>\XMLPSSvc_<XMLPS ID>\telas.cfg` with the parameter "`globalAppId = ...`" for each XMLPS that is configured.

XMLPS service start: When the service starts, it logs on to SCCP with a default user/password and the application ID "XMLPS". This application ID must have been assigned to a user as a license in CAP Management. In contrast, the application installed on XMLPS is not explicitly licensed.

XMLPS features: The CAPPhone XML objects are used by the XMLPS for displaying menus and input formats and for pure text displays on optiset or optiPoint devices on a HiPath 4000 or HiPath 3000. The XML Phone Server operates as a browser and treats the Siemens devices as output devices. The device communicates with the XMLPS application using the telephone data service.
The following features are supported:

- Two-line or four-line display with 16 or 24 characters per line (as configured via the XMLPS device type).
- All automatically generated terms (EXIT, BACK, SUBMIT) are available in English, German, and French. Additional languages for command terms must be explicitly defined by the application itself.
- Audio indicator (BEEP, SILENT).
- Application buttons with associated lamps, where the lamp status can be changed (STEADY, WINK, FLUTTER, OFF).
- "OK" button.
- The normal keyboard is supported in numerical and text mode.

XMLPS application example: The following diagram shows a possible scenario where a device initiates communication with an XMLPS application. **Alcatel and Cisco is out of support**.



XMLPS invoke interface: The invoke interface is addressed by an application for operating telephones (CAPPhone Execute) using a case-sensitive URL. This operation can be performed on a telephone at any time. XML Phone Server behavior depends on the telephone connection status.

? No XMLPS application has started: in this case, all XML PhoneExecute messages are executed immediately:

  ? if activated, a text title is displayed for five seconds.

  ? If activated, a signal tone (BEEP) is output.

  ? if activated, the button lamp is activated; this is the one that was configured in the CAP configuration with the corresponding URL. This lamp status is maintained as long as it is not overwritten or the assigned XMLPS application is not started.

? An XMLPS application is started: in this case, the lamp status is set for the button that is assigned to this application URL.

? This status depends on the configuration parameter `"lampModeActiv"` in the file `"telas.cfg"` in an XMLPS.

? Each additional invoke message overwrites the lamp status.

? For this reason, all CAPPhoneExecute jobs are not executed until after the active application has ended.

To configure an XML phone service for the first time or to reconfigure an existing XML phone service you should proceed as follows:

1. Click **Service** in the main menu and select the **XML Phone Service** menu item in the navigation area.
   a) No XML phone service is configured as of yet. Continue with 2a.
   b) An XML phone service has already been configured. You will see this in the "XML Phone Service list". Continue with 2b.
2. Configure the XML phone service.
   a) If no XML phone service is yet configured, click the **Add new entry** icon.
   b) If an XML phone service is already configured, you will see it in the "XML Phone Service list". Select an XML phone service by clicking the **Edit** icon for the XML phone service.
3. Complete the fields described below:

Field	Description
Phone Service Name	Enter a symbolic name for the XML Phone Service here. This name can be assigned and used at the administrator’s discretion. It is not used internally. Up to 32 characters (letters, numbers, underscore, and hyphen) are permitted.
Phone Service Id (optional)	Enter an ID for the XML Phone Service here. These identifiers must be unique within the entire OpenScape CAP installation. They are needed later when you are assigning HiPath 4000 terminals to an XMLPS and therefore to a particular XMLPS application and when displaying the XMLPS process unambiguously in the Diagnostic Agent. Up to 32 characters (letters, numbers, underscore, and hyphen) are permitted.
SCC Proxy Id	Select the SCCP that will be used by this specific XMLPS alone.

Field	Description
Phone Service Host name	The name of the host on which the "sxmlps" process is running must be entered here. A PC name directory is created in the directory `<InstDir>\config\` using the "host name". A subdirectory called `XMLPhoneSvc_<XMLPS ID>` is added for the XMLPS. These subdirectories contain all configuration files for this process that is to be started.
Phone Service IP address (optional)	The IP address of the host on which the "sxmlps" process is running must be entered here. The IP address is determined automatically from the host name if no input is made here.
Invoke interface port	The invoke interface servlet can be addressed via the port number that you can define here. The default port number is "3102". The invoke interface is used for operating the telephone displays.
Disable XML Phone Service	Activate this option to prevent an already configured XML phone service from starting when OpenScape CAP is started.

4. Complete your entries with one of the following actions:

Action	Description
Add or **Modify**	Adds the entry to the "XML Phone Service list".
Cancel or **Close**	Closes the dialog without saving the entries.
Delete	Deletes the existing XML Phone Service. **Note**: This button only appears if an XML phone service is already configured.

7.2.8 URLs for XML Phone Service

You can call up an XML application and start a dialog with it by pressing a specially configured key on a HiPath 4000 device. To do this, you must configure one button per XMLPS application URL on the device as the name button with the destination "TDD application number and the accompanying button number" in the HiPath 4000. Next, assign the URLs of the device buttons that were configured here to a "phone device" (see Section 7.4.1, "Adding devices"). All XMLPS application URLs are administered in a list in CAP Management. This list of URLs applies to all configured XML phone services within OpenScape CAP.

Add the URLs of the XML Phone Service applications here; these can be assigned to the "phone devices" later. The XMLPhone Service standard applications have already been configured.

1. Click **Service** in the main menu and select the **URLs for Phone Service** menu item in the navigation area.
2. Complete the fields as described in the table below.

Field	Description
Business Group (preselected for BGAdmin)	The default selection is "Standard" or "none". Additional BGs are presented for selection as soon as BGs have been defined. URLs are created in the BG defined; this assignment cannot be modified later on (no moving between BGs).
URL	Enter the URL of an XML phone service application, including all parameters. The parameters are the same for all users.
URL Name	Enter a symbolic name for the URL of the XML phone service here. This name can be assigned and used at the administrator’s discretion. It is not used internally. Up to 32 characters (letters, numbers, underscore, and hyphen) are permitted.
URL Description	If necessary you should enter a more detailed description of the URL here.

3. Click the **Add** button and your entry will be saved; it appears in the lower window.

   You can use the **Modify** button to change an existing entry for a URL, while the **Delete** button allows you to delete the entry.

7.2.9 Presence Manager

The direct call button functionality of the HiPath / OpenScape 4000 is limited for one system and the switch itself is not able to handle network wide direct call button configurations.

Presence Manager is a CAP modul (similar to the XMLPS) and it is able to handle the network wide direct call button, which means that if a direct call button of device is set to another device in another HiPath / OpenScape 4000 switch, and the led next by the direct call button shows the status of the destination.

Detailed: in case the external device (direct call button destination) is ringing then the led next by the direct call button is flashing and if the the external party is busy then the direct call button is red (without flashing).

If the direct call button of the device is pressed, then a call will be initiated to the destination (to the external device).

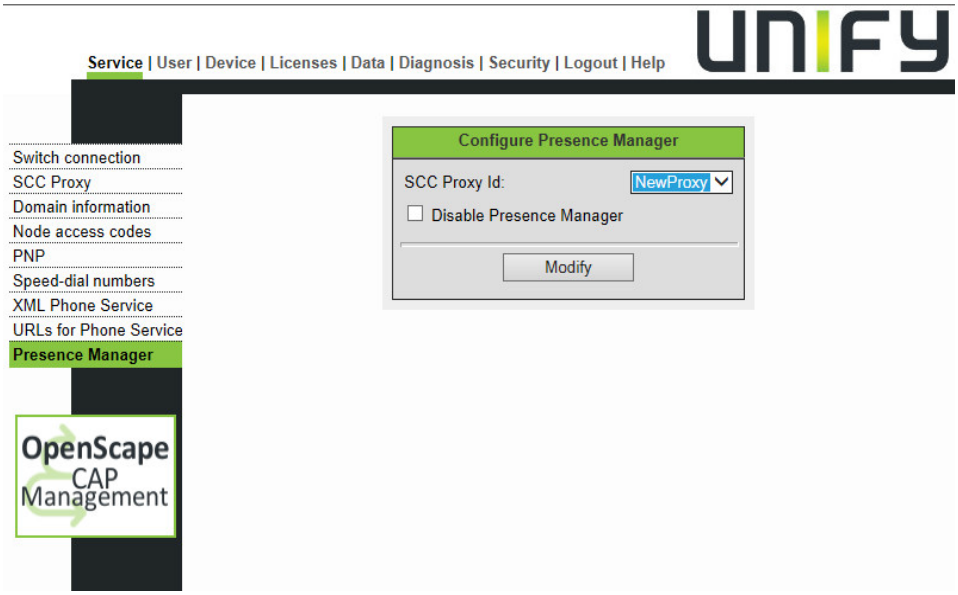
The Presence Manager is able to handle also such scenarios, when the direct call destination is in the same HiPath / OpenScape 4000. In this case only the AMO commands listed in the AMO configuration section (, and no additional setting is needed in switch).

CAP management user interface is expanded in order to allow the user to configure direct call button(s) on a device. The user interface will enable unlimited button-device associations which will be stored in CAP’s LDAP database.

Setting up on the user interface

1. First a proxy must be created, which is used only by Presence Manager. It can be done from Service / SCC Proxy menu, add new entry button.

2. After proxy created it must be assigned to the Presence Manager (underService menu):



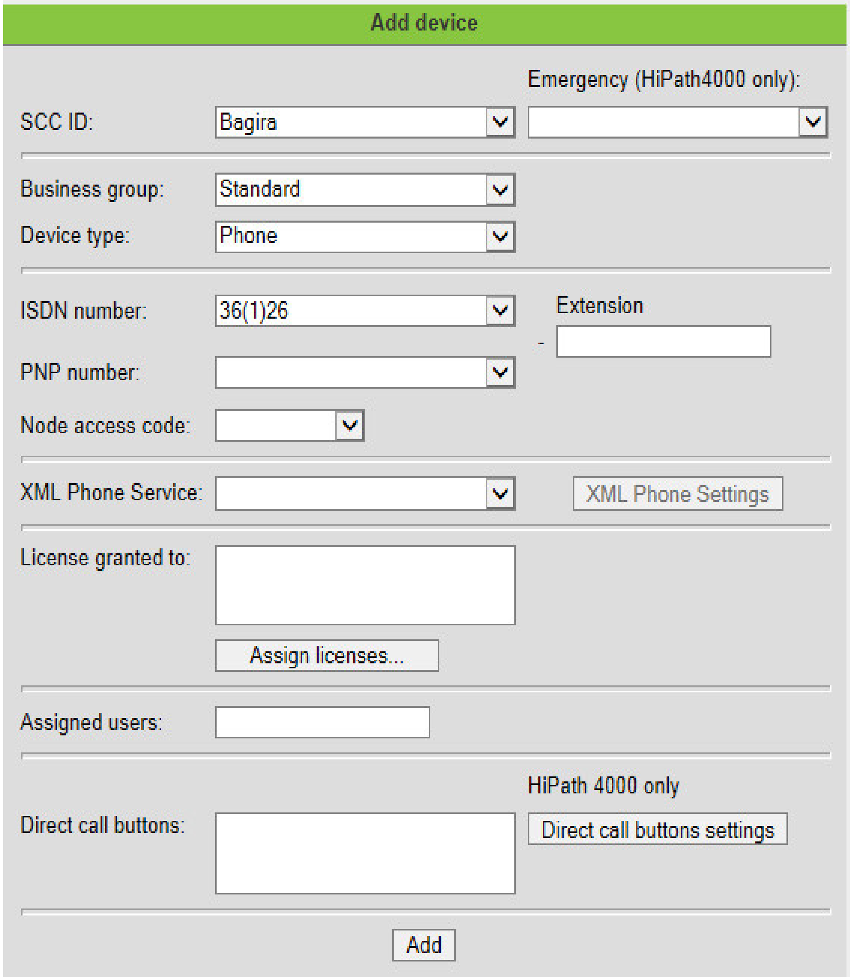
Configure Presence Manager

SCC Proxy Id: NewProxy

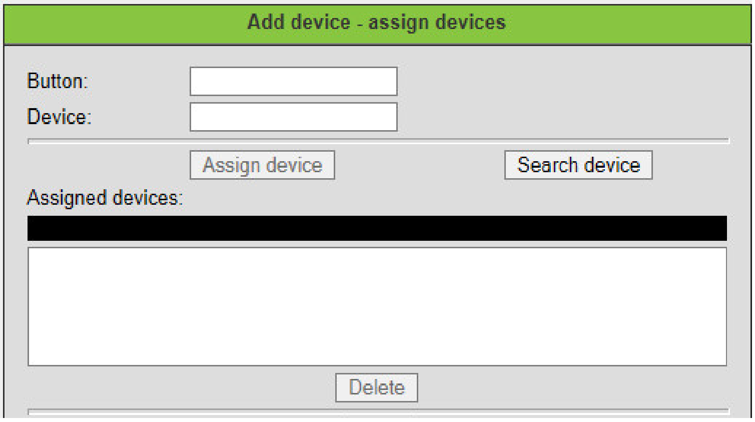
☐ Disable Presence Manager

Modify

3. Direct call configuration will be placed on the device dialog. If you add a new device or modify an existing one, you will be able to create, modify and deletebutton-device associations in the Direct call button part of the device dialog.



4. The Direct call button Settings brings up the following dialog:



Here you can create button – device assignments or delete existing ones. Destination device can only be selected from database, it means all of the devices must be configured in CAP management database. The button number must be configured in AMO TAPRO (see next section).

AMO configuration

For the devices, which are assigned to Presence Manager, must be configured the Name key in the AMO TAPRO. E.g. the device 3256 has assigned on the button 10 the device 3257, then the following AMO must be executed:

```
CHANGE-TAPRO:3256,,OPTISET,,,,,,,,,,NAME;
```

For function calling assigned device via pressing button the following AMO shold be configured – in this example the device 2356 has configured on the button 10, that by pressing it the 3257 will be called:

```
ADD-ZIEL:NAME,3256,10,3257,BD,,,SLKSTNO;
```

Restrictions

Presence Manager is only supported on HiPath / OpenScape 4000 systems.

7.3 User

The functions for administering users of the OpenScape CTI system are contained in the main menu under **User**. For example, you can:

? Add users

? Search for users

? Modify user data

? Create user groups

? Manage security settings (e.g. password setup and authentication modes)

Application authentication

An application always has to send an ACSE_AARQ request once a connection has been set up to an SCCP. The user/password (for example, CAP/123) contained in this request must match a CAP CTI or CAP Application user. The SCCP sends a corresponding HTTP request `(http://<fqdn>:8170/mgmnt/auth/req?authenticate=<User ID>&passwd=<Password>&encoding=b64)` to CAP User Management. If the user is successfully authenticated, the TCP/IP connection to the application is maintained. If the authentication is unsuccessful, the TCP/IP connection to the application is interrupted.

The ApplicationID transmitted in the ACSE_AARQ is not used at that time. The SCCP stores the ApplicationID and uses it later for CTI client licensing of CSTA requests (using the telephone number in canonical format). In the same way, the SCC works with the ApplicationID that is transmitted as an option by the CAP TCSP in TAPI `"lineDevSpecificFeature"`. SCCP/SCC send a corresponding HTTP request `(http://<fqdn>:8170/mgmnt/admin/req?registerLicense=<ApplicationID>&userId=<DeviceID>)` to CAP License Management. If the license check was successful, the SCCP/SCC saves this information for 3600 seconds.

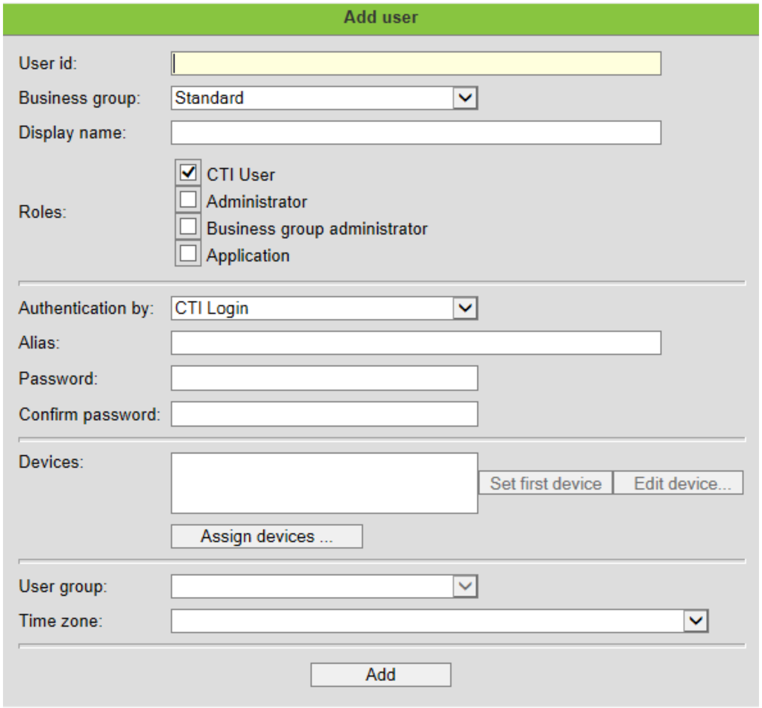
ComAssistant: The ComAssistant application uses CAP User Management to authenticate its users. For unambiguous identification of a CAP CTI user, ComAssistant may provide a user ID, an alias (-name), or a device ID (telephone number in canonical format).

SimplyPhone For Outlook/Notes: These TAPI-based applications support only the device ID (telephone number in canonical format) for unambiguous identification of a CAP CTI user.

7.3.1 Adding users

In this dialog, users with different roles or rights can be configured. Authentication can be performed by OpenScape CAP Management.

Click **User** in the main menu and select the **Add** menu item in the navigation area.



Add user

User id:

Business group: Standard

Display name:

Roles:
☑ CTI User
□ Administrator
□ Business group administrator
□ Application

Authentication by: CTI Login

Alias:

Password:

Confirm password:

Devices:

User group:

Time zone:

5. Enter the data for the new user in the relevant fields. The fields are described in the table below.

"Add user" dialog

Field	Description
User ID	The user ID uniquely identifies the user and is a mandatory entry. If a user with this ID already exists, you will receive an error message. The user can log on using this user ID. User authentication can also be performed on the basis of the "alias" or the telephone number. ATTENTION! If CTI users have already been manually configured before a user data import, the user IDs MUST match the corresponding number of the phone device assigned without special characters. If this is not the case, the user data import will cause serious database errors. Furthermore, the user data cannot be exported first and then re-imported.
Display name	The display name is used for messages and prompts which pertain to the respective user (for example, *The journal for <display name> contains no entries*). The display name is currently only used by the ComAssistant application.
Roles	The user can be created as ? CTI user; "normal" user with devices assigned ? administrator, with access to OpenScape CAP Management functions (not for BGAdmin) ? Business group administrator, with limited administration rights fro the BG defined below (not for BGAdmin) ? application user, for generic application use without devices assigned (not for BGAdmin). An application can be authenticated generally with its application user or individually with single CTI users.
Authentication by	You can choose two different types of authentication via the drop-down menu: ? **CTI Login** The login is handled by OpenScape CAP Management. You must assign an alias name and password for this purpose. ? **Windows Login** In this case, a CTI user is linked to a Windows user (a domain or the local user management). During CAP authentication, a CTI user must enter the user ID or device ID and the password of the Windows user. The advantage in this case is that the CTI user only has to keep the Windows password.

Field	Description
Alias (for authentication with CTI Login only)	Along with the user ID, which is unique in the system and which cannot be modified by the user, an alias can be assigned; this must also be unique. The user can change this alias at any time. The alias (-name) was introduced because the user ID in a user data import is only a number string and users like to support an individual user name after a successful import. A user can then use this alias for authentication.
Password (for authentication with CTI Login only)	This defines the individual password that does **NOT** have to be changed during initial authentication. The password entry is hidden (converted to asterisks) automatically. If no password is entered, the default password is entered for this user. The user is then prompted to change this password when logging on for the first time. The default password is defined under **User** | **Business Groups| Default Password**. See Section 7.3.3 for details.
Confirm Password (for authentication with CTI Login only)	Re-enter the password entered above to confirm / check the entry; once again the entry is hidden automatically.
Username (for authentication with Windows Login only)	Enter the Windows user name here that exists in a domain or the local user management. During CAP authentication, a CTI user must enter the user ID or device ID and the password of the assigned Windows user.
Domain (for authentication with Windows Login only)	Enter the domain in which the assigned Windows user is configured here. This can be a real domain ID or the local user management. In this case, you must enter the local PC name. Authentication over the operating system has the advantage that the CAP user and the domain user use the same password (the domain user password). This password only has to be administered in the domain.

Field	Description
Devices	Select devices to be assigned to this user from the list of phone devices that have already been configured. Please note that multiple devices may be assigned to one user. The **Assign devices** button opens a separate dialog for device definition / selection; **Close**ing this dialog brings you back to the Add user dialog. Devices that have already been assigned are displayed in the Devices area; they can be modified individually by selecting one of them and pressing **Edit device**. For applications that rely on a one-to-one mapping between users and devices (like ComAssistant), it is possible to identify one of the devices assigned as the user’s "**first device**". This enables the application to ignore additional devices. The initial device assigned to the user is assumed to be the user’s "first device". You may change that assignment subsequently by selecting another one and pressing **Set first device**. The first device is outlined in blue
Business group (preselected for BGAdmin)	The default selection is "Standard" or "none". Additional BGs are presented for selection as soon as BGs have been defined. Assignment of users to a business group should be done based on data imported from the PBX. This assignment cannot be modified later on (no moving between BGs).
User group	Select a user group here to assign the user to a user group. Application examples: ComAssistant uses the user groups to display a user’s buddy list. The CAP TCSP can automatically include the users and devices assigned to a specific user group as TAPI lines. **Notes:** ? To enable a user group to be selected, it must first be configured under **User | Manage User Groups**.
Time zone	Select a time zone to be assigned to the user from the pull-down menu.

6. Click the Add button. A new set of user data is created and the following message appears:

   ```
   User entered: <User ID> (for example, 495251827486)
   ```

   If a user with the same ID already exists, then the following error message appears:

   ```
   User already exists: <User ID> (for example, 495251827486)
   ```

7.3.2 Searching and changing users

1. Click **User** in the main menu and select the **Search/Modify** menu item in the navigation area. A window opens enabling you to specify data for a more precise search:
2. Enter your search keyword in one of the fields. The fields are described in the table below.

"Search user" dialog

Field	Description
User id, **Display name**, **Alias**, **User Group**, **License**, **SCC ID**, **Device,** **User role,** **Business Group**	These input fields can be used to conduct a more precise search for the required user data. The asterisk can be used as a wild card character in any of these fields: `*` finds all entries, C`*` all entries beginning with C, `*`n all entries that end in n, etc. The selection menus available under "User Group", "License", "SCC ID", "User role", and "Business Group" always show only entries that have been configured in CAP.
Max. number of results	This limits the number of entries displayed as a search result. This makes it possible to restrict the search before finally displaying the result.
Number of results per page	The search result may cover several pages.
Mark search result for delete	As described below, the search result may be used to mark specific users for deletion. In case the search is targeted to find a complete set of users for deletion, this field allows to have all retrieved users pre-marked for deletion.
Mark search result for export	As described below, the search result may be used to mark specific users for export. In case the search is targeted to find a complete set of users for export, this field allows to have all retrieved users pre-marked for export.

Actions

Field	Description
Clear fields	Field contents are deleted (except for User role and Business Group which keep default entries "CTI User" and "Standard Business Group"), and the **Max. number of results** and **Number of results per page** fields in the `adminIf.cfg` configuration file are redefined.
Search	Starts the search process.

Field	Description
Last search	All fields contain the values used in the last search query. "Last Search" does not yield any more data after a browser session is complete. **Note:** The result of the last search can also be obtained directly by selecting the **Last Search Result** menu item in the navigation area.

3. Click the **Search** button. The result of the search query (if more than one) appears in a list.

   Use the cursor control keys to navigate through several pages (first - previous - next - last page).

   The printer icon can be used to obtain a print preview of the results list in a separate window.

   The "delete" column of the result list provides deletion marks; by ticking a deletion mark, the respective line can be selected for deletion. By clicking the deletion symbol (cross in the head line), all lines selected are finally deleted.

   The "export" column of the result list provides export marks; by ticking an export mark, the respective line can be selected for export. By clicking the export symbol (disc icon in the head line), all lines selected are exported to a file, using the Excel csv (comma separated values) format.
4. Use the ✎ icon to select a user from the list who’s data you wish to modify.
5. The current data for the selected user is displayed for modification purposes.
6. Modify the user data as described in Section 7.3.1.

7	The user ID cannot be modified because it acts as a unique ID for the user. Alike, license information which is tied to devices is displayed for information purposes only - it cannot be modified either. Please note that as a user may have several devices assigned which in turn may carry the same license, it is possible for a user to indirectly consume e.g. three CAP-S licenses

Various options are offered in the **Password** drop-down menu for modifying the password. You can change the password, keep it or reset it to the default password.

>	The default password is defined under **User | Business groups| Default Password**. See Section 7.3.3 for details.

7. Confirm your input with the **Modify** button. A message is issued to confirm that the changes have been applied:

`User data has been modified for: <User ID>` (e.g. `hm007`)

You may use the **Close** button to leave the dialog without executing any modifications.

7.3.3 Configuration of business groups

1. Click **User** in the main menu and select the **Business groups** menu item in the navigation area. A list of available business groups is presented for selection / modification. BGAdmins only can see assigned BGs.
2. To create a new BG (not for BGAdmin), click the button in the header line.

   A table opens to enter data for a new BG.
3. Enter the required data in the input fields.

   "Configuration of business group" dialog

Field	Description
Business group id, name (preselected for BGAdmin)	The default selection is "Standard" or "none". Additional BGs are presented for selection as soon as BGs have been defined.
Default password	Define the default password. This password is valid if you do not specify a password when you create a new user entry or if you reset the password using **Reset** when you change a user entry (see Section 7.3.2). If the default password is assigned when new users are added or when user data is modified, the user is prompted to change this password during initial login. The default password is "**`123456`**".
Password expiration period (in days)	Here you enter the validity period for passwords in number of days. When this period has expired, the user is automatically prompted to change or confirm the password.

Field	Description
Mode of authentication	Use the drop-down menu to set the type of authentication: ? **All available logins**: When configuring a CTI or Admin user, both authentication options are always available for selection for each separate user. ? **CTI Login** The authentication is completely handled by OpenScape CAP Management. Authentication is performed in CAP Management by using the user ID, the alias, or the device ID and the associated password. ? **Windows Login:** A CAP user must always be linked to a Windows user for authentication. Authentication is performed by using the user ID or the device ID and the password of the Windows user assigned.
Voice box phone (HQ8000 only)	Irrelevant for the current release.

4. Click the **Submit** button to confirm the change.

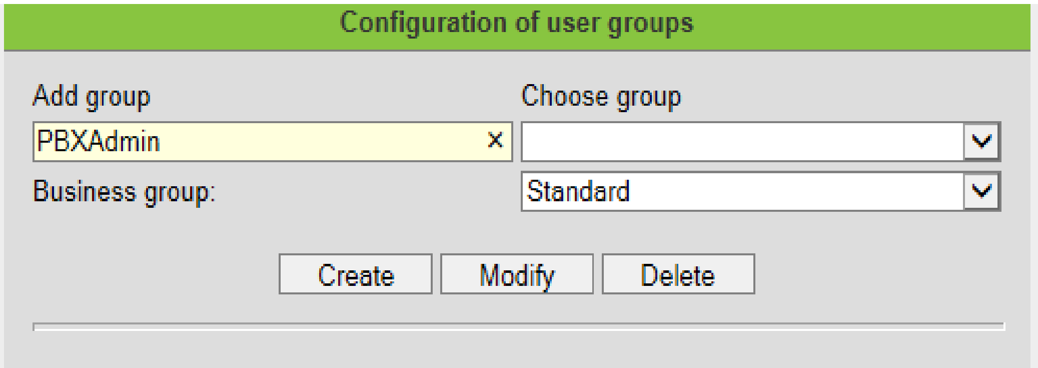
   Basically the same proceeding applies when modifying data of an existing BG (as far as possible) or deleting a BG.

> Deleting a BG is not allowed for BGAdmin; deleting a BG requires the BG to be "empty". In case a BG to be deleted still contains some objects (users, devices), a warning is issued to the administrator.

7.3.4 User groups

You can define user groups and change existing user groups here.
The ComAssistant currently uses user groups for displaying the buddy list. CAP TCSP uses user groups for automatically including a defined user group as a TAPI line device.

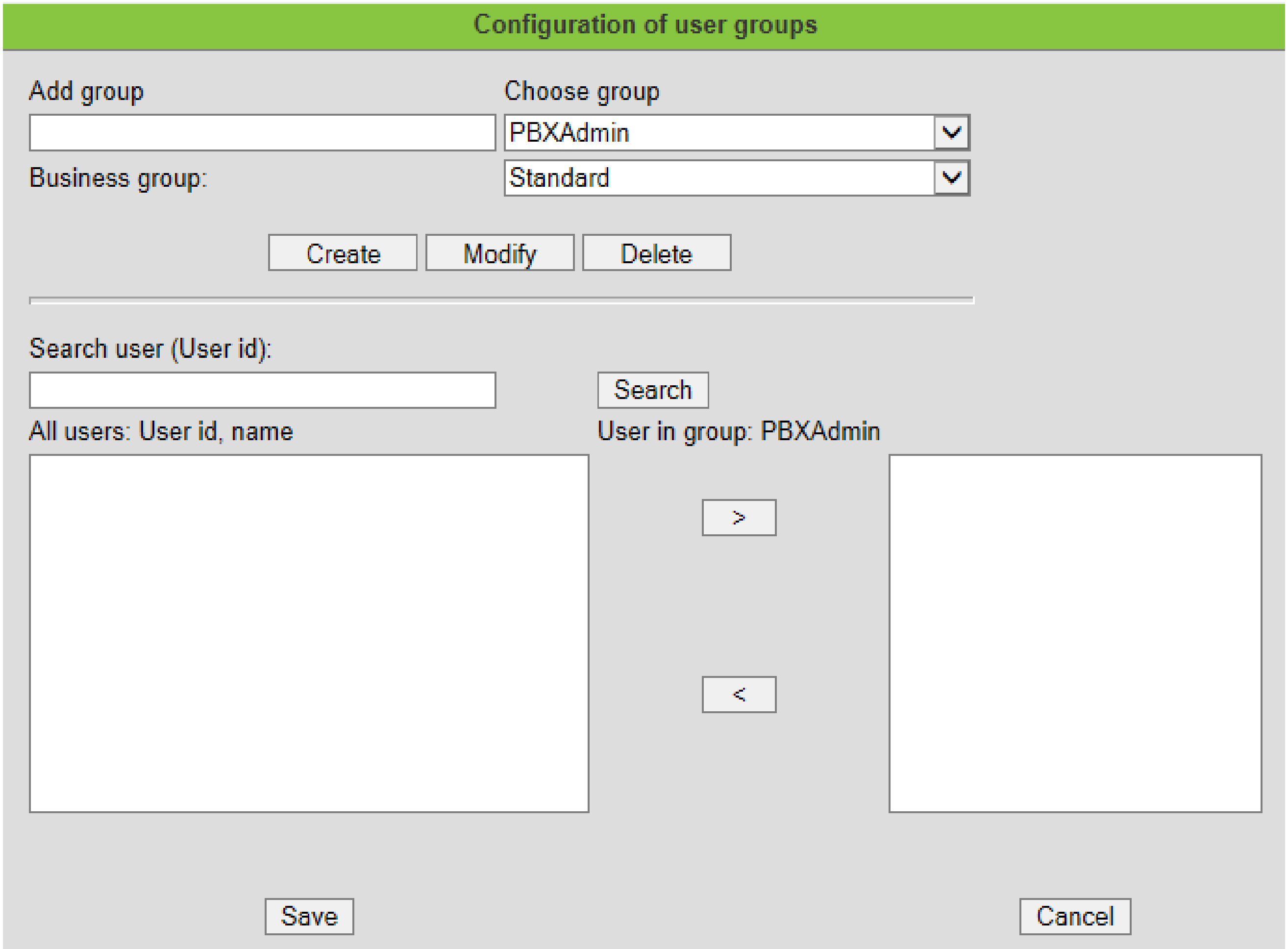
1. Click **User** in the main menu and select the **Manage user groups** menu item in the navigation area. The following window appears:



Add group: PBXAdmin

Business group: Standard

2. To define a new group, enter the name of the group to be created under **Add group** and click **Create**.
   To edit or delete an existing group, select the relevant group under **Choose group** and click **Edit** or **Delete**.
   When a group is deleted, links to this group are also deleted for all users belonging to this group.
3. A new window appears in which you can create or modify a group.



Configuration of user groups

Add group:

Choose group: PBXAdmin

Business group: Standard

Search user (User id):

All users: User id, name

User in group: PBXAdmin

The right hand window shows the users currently assigned to the group, while the left hand window shows all other users. You can move user entries between the windows, either by double-clicking on individual entries or using the cursor control keys (after user entries have been selected). It is possible to make multiple entry selections.

4. You can conclude the definition with **Submit** as soon as the group's composition has been defined/modified. **Cancel** takes you back to step 2 without saving any changes.

7.3.5 Integration with HiPath / OpenScape User Management (not for BGAdmin)

The current version of OpenScape CAP V3.0 provides a facility for integrating CAP and User Management to allow for an almost automatic synchronization of user data.

Please note that currently in User Management only user data for HiPath / OpenScape 4000 systems are administrated. Users assigned to other switches still need to be managed in CAP.

7.3.5.1 Connecting CAP to User Management

Support for User Management is activated by means of the following entry in `<InstDir>/config/<host>/admin/mgmnt/admin.cfg:`

```
ProgramMode = HiPathUserManager
```

This entry activates a configuration file with the same name:

```
<InstDir>/config/<host>/admin/mgmnt/modes/HiPathUserManager.cfg
```

This file serves to configure the behavior of user and device dialogs. Reasonable settings have been preselected here - e.g. all fields for data entry in the user dialog have been blocked, but password and license assignment fields are kept open for entry. For more details, please refer to the file. If the ProgramMode is kept as "CAP" (default value), the connection to User Management is still possible, but without any specific adaptations to the user and device dialogs.

For the CAP to User Management connection to work properly, please make sure the following configuration files are correct after the CAP installation:

`<InstDir>/config/<host>/admin/semi/config/LocalConfigHiPathCAP.xml` should be as follows - no modification required:

```
<HPM ver="1.0">
   <ENVIRONMENT>
      <LOCAL_SERVER_IP>127.0.0.1</LOCAL_SERVER_IP>
      <LOCAL_SERVER_PORT>4448</LOCAL_SERVER_PORT>
   </ENVIRONMENT>
</HPM>
```

`<InstDir>/config/<host>/admin/semi/config/SdkConfig4448.xml` is created automatically as soon as the CAP to User Management connection has been established - no modification required:

```
<HPM ver="2.0">
   <ENVIRONMENT>
      <HPM-UM_SERVER_IP>192.168.111.228</HPM-UM_SERVER_IP>
      <HPM-UM_SERVER_PORT>4443</HPM-UM_SERVER_PORT>
      <HPM-DS_SERVER_IP>192.168.111.228</HPM-DS_SERVER_IP>
      <HPM-DS_SERVER_PORT>2600</HPM-DS_SERVER_PORT>
      <EM_ID>192.168.111.129-4448</EM_ID>
   </ENVIRONMENT>
</HPM>
```

`<InstDir>/config/<host>/admin/semi/config/traceconfig.xml` should be as follows - no modification required. This file is used to define the trace directory (<TRACE_PATH>). For testing purposes, the trace level (XML,DEBUG,INFO,WARN,ERROR,FATAL) can be modified via setting "<TRACER_LEVEL>". This file changes the trace behavior at the User Management Interface.

```
<!--Tracer Configuration File
OPERATION specifies whether the trace is active
   (supported values: ACTIVATE, DEACTIVATE)
TRACER_LEVEL specifies the trace level
   (supported levels: XML,DEBUG,INFO,WARN,ERROR,FATAL)
TRACER_MODE specifies the trace modus
   (supported modes: OVERWRITE, APPEND)
TRACE_PATH specifies the path where the trace file is stored.
   This value is optional. If it is not specified, the trace file
   is stored to the default directory (see EM-SDK description).
-->
<HPM ver="1.0">
   <TRACER>
      <OPERATION>ACTIVATE</OPERATION>
      <TRACER_LEVEL>DEBUG</TRACER_LEVEL>
      <TRACER_MODE>OVERWRITE</TRACER_MODE>
      <TRACE_PATH>C:/HiPathCTI_CAP30_I803a/logs</TRACE_PATH>
   </TRACER>
   <DETAILS>

   </DETAILS>
</HPM>
```

7.3.5.2 Proceeding for the administrator

For cooperation of CAP and User Management, we recommend to proceed as follows. Four scenarios need to be distinguished:

? Scenario 1: No users created in any of the systems

? Scenario 2: Users created in CAP, none in User Management

? Scenario 3: Users created in User Management, none in CAP

? Scenario 4: Users created in both systems

For all of the scenarios holds:

? SCC configurations for the respective PBXes must have been completed in CAP. Please make sure the names of configured SCC instances match the names of the PBXes as used in User Management.

? Set up the CAP element manager in User Management. Make sure the port configuration matches the entry in `LocalConfigHiPathCAP.xml` (default is 4448).

Scenario 1: No users created in any of the systems

? Users should be created in User Management, together with their phone resources; of course, this requires integration of HiPath / OpenScape 4000 as well.

? Upload CAP data to User Management. This serves to inform User Management about relevant CAP data, like which licenses have been installed in CAP and which messages CAP is expecting to receive from User Management.

? Execute "Download Users" in User Management. Make sure to select the third option ("Download Users for Element Manager initial setup").

? After successful download, all users with phone numbers have been created in CAP.

? From now on, user data will be synchronized automatically as far as possible. For instance, for a user that gets assigned a ComAssistant license in CAP by logon, the license assignment is reported to User Management. This works as well the other way around. Additional user attributes, which are termed CAP attributes in User Management (to be found in "HiPathApplications"), should be modified in User Management only - these are synchronized in the direction from User Management to CAP only. Licenses are synchronized in both directions.

? It’s possible as well to manually synchronize user data (see below).

Scenario 2: Users created in CAP, none in User Management

? Select "Tools/Element Manager Sync" in User Management

? Upload user data - Button "Upload Data".

? Import the users to User Management - Button: "Match&Merge Users")

? Assign phone resources to users in User Management

? Execute "Download Users" in User Management.
Make sure to select the second option ("Synchronize phone numbers").

? Upload user data once again; this serves to upload license assignments as well.

? Import users to User Management.

? From now on, user data will be synchronized automatically as far as possible.

Scenario 3: Users created in User Management, none in CAP

? To be handled like scenario 1 - it’s only that users with assigned phone resources exist

Scenario 4: Users created in both systems

? Execute "Download Users" in User Management. Make sure to select the third option ("Download Users for Element Manager initial setup").

? Upload user data (to be started from User Management).

? Import users to User Management.

? From now on, user data will be synchronized automatically as far as possible.

> 7 As described above (cf. Section 7.3.1, "Adding users") users belonging to a user group must not have assigned more than one device; this is enforced in the CAP Management configuration GUI as far as possible but currently cannot be enforced for user data synchronization between CAP and User Management.
> So the administrators need to make sure this condition is met in User Management before starting data synchronization.

7.4 Device

CAP manages devices of different types:

? extensions (type “Phone”)

? virtual extensions (type “Virtual Device”)

? trunks (type “Trunk”)

? hunt groups (type “HuntGroup”)

? route control groups (type “RCG”)

? SIP devices (type “SIP”)

? MGCP devices (type “MGCP”)

? Fax devices (type “FaxNumber”)

? mail addresses (type “MailAddress”)

? routing devices (type “RoutingDevice”)

Devices, users, and licensing

So called **Station Devices** (extensions, virtual extensions, SIP or MGCP devices etc.) regularly are assigned to a CAP user. Please note that only type “Phone” and “Virtual Device” devices may be configured via the CAP administration GUI. Other station types may only be created via import only through SPI. From release SMR9 it is now possible to assign the type SIP device to SIP-phones, thus distinguishing it from other device types.

Non-Station Devices (trunks, hunt groups, route control groups, routing devices) which are also known as "logical devices" are not assigned to a CAP user. Non-Station devices are created only via import facility (see Section 7.6.1) or HiPath / OpenScape 4000 SPI interface (see Section 6.2.3).

Based on the device ID, each device is assigned to exactly one SCC / the PBX behind that SCC. The device ID is either a dialable number in the long "canonical" format (e.g. +49(5251)8-27486) or, for trunks, an unambiguous administration number in CAP management created in the import process by combining the SCC ID and the hardware location of the respective module / channel (e.g. +SCC-H4K-1+1-67-1+0 = +<SCC-ID>+<location>+<channel>).

Licenses for various types are always assigned to devices. License assignment can be either "implicitly during register license" or "at device administration" (see Section 7.5.3). As for device types != "Phone" or "Virtual Device" editing in the CAP management GUI is not possible, these can get licenses assigned only implicitly; therefore, make sure to set the respective licenses to assignment mode “implicitly during register license” (see Section 7.5.3). This causes licenses to be assigned automatically as soon as the device is used.

Licenses assigned either way (explicitly or implicitly) are displayed in the device dialog and can be searched for in the device search dialog (see Section 7.4.2).

Accordingly, it is crucial for license ordering to cover not only the number of phone (station device) users but also the number of logical devices (non-station devices) that shall be controlled via CAP CTI interfaces.

Devices and applications

Using "Address Translation Service" (SAT) features, an application can always use the associated number in canonical format to address a device. Conversion into a number that the SCC can use for addressing is done using the display in the "PBX format" field of a device. If an overlap is configured, it is taken into account here. The relevant LODEN number is displayed in this field for HiPath / OpenScape 4000 "RCG groups", "hunt groups", and "trunks".

The long number in canonical format is also always transmitted to the application in events. To guarantee this function, the PNP number and the node access code are administered in the device configuration, corresponding to an SCC configuration belonging to a device. If an event contains a number corresponding to the configuration (for example: extension, PNP number, node access code+extension, ISDN number), the number is converted into the device ID before it is forwarded by the SAT.

Accordingly, for an application that needs to monitor logical devices it’s indispensable to

1. have the logical device data created in CAP Management via import / SPI;
2. have SAT activated for the respective SCC / SCCP instances (see Section A.2.15);
3. have licenses available and marked for implicit assignment.

Restriction: In case an application does not use the canoncical format (but the extension/PBX format) in the CSTA Requests, then the extensions/PBX formats must be unique in the CAP Management database.

You can add and configure devices in the **Device** main menu ("extension" (type: phone), "virtual extension" (type: virtual device)). The following functions are available to you:

? Add device

? Search device

? Edit device

7.4.1 Adding devices

1. Click **Device** in the main menu and select the **Add** menu item in the navigation area.
2. Enter the data for the new device in the relevant fields. The fields are described in the table below.

"Add device" dialog

Field	Description
SCC ID	Select the switch connection that is used here. Based on this selection, an extension or virtual extension is permanently assigned to a PBX. Furthermore, the ISDN number(s), PNP number(s), and node access code(s) are displayed in accordance with the associated SCC configuration.
Emergency (HiPath / OpenScape 4000 only)	Select the alternative connection to be used in case of AP Emergency. This allows the device to be reached even in case the primary SCC4000 / CA4000 connection specified via SCC ID fails. **ATTENTION** This requires the device to be AP Emergency enabled: ? the device has been configured at an AP shelf (by HiPath / OpenScape 4000 administration) ? the device has been assigned to an AP Emergency group (by HiPath / OpenScape 4000 Administration) ? the AP Emergency group has been assigned to a CC-AP ("Common Control for Access Point Emergency" - HW component in an AP shelf required to provide local survivability) (by HiPath / OpenScape 4000 administration) ? an SCC4000/CA4000 has been configured to connect to this CC-AP (by CAP administration) **ATTENTION** In case the AP Emergency feature has been deactivated on CAP level in the controlling SCCP ("Disable AP Emergency", cf. Section 6.5.2), the SCCP will not make use of alternate paths whatsoever! Although the device can be used manually on HiPath / OpenScape 4000 level, it will remain unreachable for applications until the primary connection to SCC4000 / CA4000 defined under "SCC ID" has been re-established.

Field	Description
Business group (preselected for BGAdmin)	The default selection is "Standard" or "none". Additional BGs are presented for selection as soon as BGs have been defined. Assignment of devices to a business group should be done based on data imported from the PBX. This assignment cannot be modified later on (no moving between BGs).
Device type	Select the device type here. The supported types are "Phone" and "VirtualDevice". Any other types of devices can only be imported.
ISDN number	Pull-down menu with available domain info entries (see Section 7.2.3); select the entry appropriate for this device.
PNP number	Pull-down menu with available PNP entries (see Section 7.2.5); select the entry appropriate for this device.
Node access code	Pull-down menu with available NAC entries (see Section 7.2.4); select the entry appropriate for this device.
Extension	Number of the extension, which means the device number. This number is usually configured in the PBX in exactly the same way. **Exception:** If overlap has been selected, the extension number must be entered without the overlap number. Consequently, this extension number is only a fragment of the number configured in the PBX (for example, if the main station/extension = 722-1234 and overlap = 1, the extension 21234 is configured in the PBX).
PBX format (output only as result of "Search Device")	This field cannot be administered. This displays the call numbers configured in the PBX for all devices that are addressed in the CSTA via a dialable number. Any overlap configuration is also taken into account here (for example, if the main station/extension = 722-1234 and overlap=1, then extension 21234 appears in the PBX format field). For HiPath / OpenScape 4000 devices that are addressed in the CSTA via a CSTA device ID (RCG, trunk, hunt group), the associated LODEN number appears. The SAT needs this data for conversion.
XML Phone Service (device type "phone" only)	Select an XML Phone Service you wish to enable for the device from the drop-down list. **XML Phone Settings** is then enabled (see below).

Field	Description
XML Phone Settings (device type "phone" only)	If you click the **XML Phone Settings** button, you will be offered the following setting options: ? **Device information** Selection from a list of supported device types ? **Language** Selection from a list of supported languages ? **Button number** The number of the button on the device that is to be assigned to the URL of the XML application. Pressing the button starts the XML application and displays it on the device. ? **URL parameters** Additional parameters can expand a URL call. This configuration depends on the XML application.
License granted to	If assignment of licenses by the administrator is set for applications (see Section 7.5.3, option **at device administration** enabled), then licenses must be explicitly assigned here. Select the application from the list. Multiple licenses can be assigned simultaneously. Licenses assigned before can also be deleted. Licenses assigned implicitly are also shown here.
Assigned users	This is an output-only field; assignment of users and devices is done via "Add user" or "Modify user" (Section 7.3.1, Section 7.3.2)

3. Click the **Add** button. The entries are saved as a new data record.

> No device can be added until domain does not exist.

7.4.2 Searching and changing devices

1. Click **Device** in the main menu and select the **Search/Modify** menu item in the navigation area. The following window enabling you to conduct a more precise search:
2. Enter your search keyword in one of the fields. The fields are described in the table below.

"Search device" dialog

Field	Description
Device, **Device type**, **SCC ID**, **SCC Emergency,** **XML Phone Service,** **License** **Assigned users** **Business Group**	These input fields can be used to conduct a more precise search for the required user data. The asterisk can be used as a wild card character in any of these fields: `*` finds all entries, C`*` all entries beginning with C, `*`n all entries that end in n, etc. The selection menus available under "Device type", "SCC ID", "SCC Emergency", "XML Phone Service", "License", and "Business Group" always show only entries that have been configured in CAP. Note, that from SMR9 you can also list SIP devices separately.
Max. number of results	This limits the number of entries displayed as a search result. This makes it possible to restrict the search before finally displaying the result.
Number of results per page	The search result may cover several pages.
Mark search result for delete	As described below, the search result may be used to mark specific devices for deletion. In case the search is targeted to find a complete set of devices for deletion, this field allows to have all retrieved devices pre-marked for deletion.
Mark search result for export	As described below, the search result may be used to mark specific devices for export. In case the search is targeted to find a complete set of devices for export, this field allows to have all retrieved devices pre-marked for export.

Actions

Field	Description
Clear fields	All field content is deleted and the "Max. number of results" and "Number of results per page" fields in the `admin-If.cfg` configuration file are redefined.
Search	Starts the search process.
Last search	Click "Last search" to complete all fields with the values used in the last search inquiry. "Last Search" does not yield any more data after a browser session is complete. **Note:** The result of the last search can also be obtained directly by selecting the **Last Search Result** menu item in the navigation area.

3. Click the **Search** button. The result of the search query (if more than one) appears in a list.

Use the cursor control keys to navigate through several pages (first - previous - next - last page).

The printer icon can be used to obtain a print preview of the results list in a separate window.

The "delete" column of the result list provides deletion marks; by ticking a deletion mark, the respective line can be selected for deletion. By clicking the deletion symbol (cross in the head line), all lines selected are finally deleted.

The "export" column of the result list provides export marks; by ticking an export mark, the respective line can be selected for export. By clicking the export symbol (disc icon in the head line), all lines selected are exported to a file, using the Excel csv (comma separated values) format.

4. Use the ✎ icon to select a device from the list whose data you wish to modify.
5. The current data for the selected device is displayed for editing purposes.
6. Edit the device data as described in Section 7.4.1.
7. Confirm your input with **Modify**. A message is issued to confirm that the changes have been applied:

```
Device data has been modified for: <device> (for example optiPoint 410)
```

7.5 License Management

> 7 CAVEAT: Please note that as an important change against CAP V2.0 and previous SMRs of CAP V3.0, licenses are no longer tied to users but now will be assigned to devices. As current installations regularly have a one-to-one mapping between users and devices, this means no new handling approach for the customer; yet it's conceptually clearer and brings some modifications for the Management GUI.
> Of course licenses currently assigned to users will be migrated accordingly when upgrading to a CAP V3.0 SMR3 installation.

CAP License Management administers the number of client licenses available for an application. A license is always bound to a MAC address of an active NIC in CAP Management and is checked each time the service is restarted and each time a license is installed.

Each application must identify itself to the CAP with an application ID. This application ID is passed in the ACSE_AARQ. All additional requests for users are licensed using this application ID. The license check takes place in interaction between the SCCP/SCC and SLM. Applications can also ask for a license check by sending an HTTP request to the SLM.

The **Licenses** main menu offers functions for administering licenses for using the OpenScape CTI system. You can:

- ? View licenses,
- ? Assign licenses,
- ? Install licenses,
- ? Uninstall licenses,
- ? Split up licenses

The SCC/SCCP checks the license. After a successful check, the SCC/SCCP stores the license information for 3600 seconds. The license is checked for a device during the first CSTA or NetTSPI request.
If the "implicitly during register license" feature is activated, a license is implicitly assigned to a device in the license checking procedure. For that purpose, the application ID transmitted from the application in the ACSE_AARQ (for CSTA request) is taken as the necessary license; of course, the procedure only succeeds if that license has been installed before.
For TAPI applications (CAP TAPI Service Provider/NetTSPI), an internal routine sequentially asks for licenses CAP-A, then CAP-S, and CAP-E, - unless a specific application ID has been handed over by a TAPI "lineDevSpecificFeature" within 10 seconds after a TAPI "lineOpen".

> The HiPath CAP V1.0 license "UNKNOWN" which was used to license the number of monitor points to be set in a CA4000 is not needed any more in HiPath CAP V2.0 and higher. CA4000 version 6.0.0.0 and higher does not support a separate link to the CAP SLM, so there is no need for a separate license.

Demo licenses / exceeding assigned licenses

Demo license keys are already pre-installed (MAC address FF-FF-FF-FF-FF-FF). After initial assignment of a client license, the associated demo license key is valid for an additional two months and is marked with an "expiration date". Once this date expires, devices with demo licenses can no longer be controlled by the corresponding application.

The same proceeding applies for regular license keys as soon as the number of available clients has been reached. Additional devices applying for licenses are given a temporary license that is valid for two months (marked with a "*" in device management), and the corresponding license key is marked with an "expiration date". Once this date expires, devices with temporary licenses can no longer be controlled by the corresponding application.

In order to convert temporary licenses back to regular licenses, you must either install additional client licenses with the respective application ID, or reassign available licenses as follows:

- Delete licenses that have already been assigned to devices.
- Search for devices with temporary licences, select them, one after the other, and explicitly confirm these with **"Change"**.

> Please note that in HiPath CAP V3.0 SMR4 and above the licenses are managed considering the business groups; accordingly, the quota assigned to one BG may be exhausted (causing the "license exceeded" mechanisms to be invoked) though when looking at the system as a whole free licenses may be available. In this case, the administrator may decide to realign licenses among BGs.

E-mail message when licenses are exceeded

In case the number of licenses assigned exceeds the number of licenses installed, an e-mail notification (repeating once per day) can be configured. For that purpose, change the following text lines in the `<InstDir>\config\common\global.cfg:`

```
<?x set MAIL_SERVER = "name of SMTP email server"?>
<?x set MAIL_SENDER = "<?x $TelasWebName?> notification
                                               <name of mail sender>"?>
<?x set MAIL_SYSADMIN = "name of mail recipient"?>
```

7.5.1 Installing licenses (not for BGAdmin)

Licenses are installed via license files. These files can be obtained from the same source as the OpenScape CAP software. For Unify customers this is usually Production. Working on the basis of order and delivery data, the administrator is capable of generating licenses for downloading from a special Production web site.

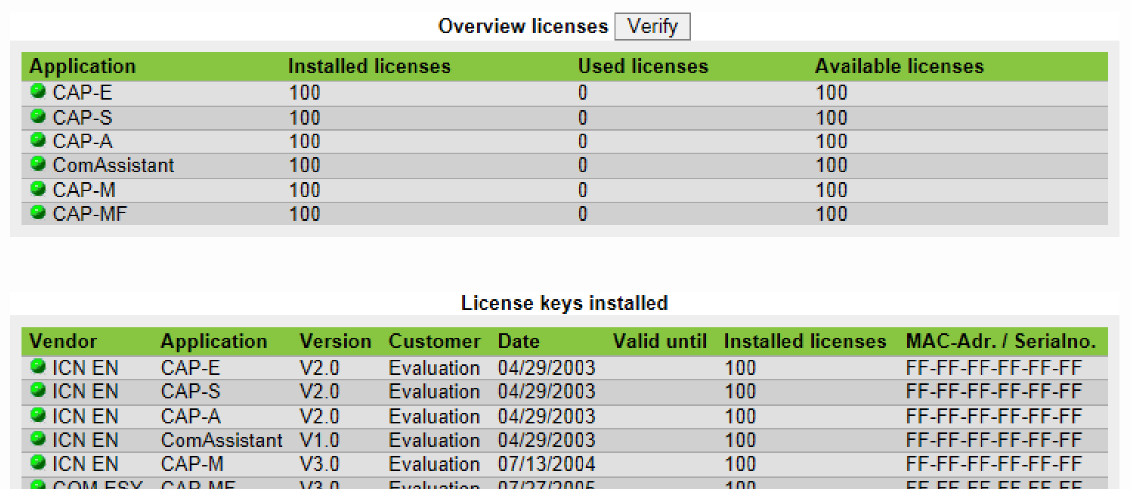
To prevent misuse, license keys are linked to the OpenScape CAP Management PC via the MAC ID. For this reason, the MAC ID for license generation must also be supplied.

> \> Demo licenses are provided when OpenScape CAP is installed; these are not linked to a particular MAC ID and are only valid for a limited period.

1. Obtain the license file and save it locally.
2. Click **Licenses** in the main menu and select the **Install** menu item in the navigation area.
3. Specify the absolute path of the license file here.
4. With **Install**, the license file is processed, and the new licenses are made available.

7.5.2 Showing licenses

1. Click **Licenses** in the main menu and select the **Show** menu item in the navigation area.



Overview licenses

Application	Installed licenses	Used licenses	Available licenses
● CAP-E	100	0	100
● CAP-S	100	0	100
● CAP-A	100	0	100
● ComAssistant	100	0	100
● CAP-M	100	0	100
● CAP-MF	100	0	100

License keys installed

Vendor	Application	Version	Customer	Date	Valid until	Installed licenses	MAC-Adr. / Serialno.
● ICN EN	CAP-E	V2.0	Evaluation	04/29/2003		100	FF-FF-FF-FF-FF-FF
● ICN EN	CAP-S	V2.0	Evaluation	04/29/2003		100	FF-FF-FF-FF-FF-FF
● ICN EN	CAP-A	V2.0	Evaluation	04/29/2003		100	FF-FF-FF-FF-FF-FF
● ICN EN	ComAssistant	V1.0	Evaluation	04/29/2003		100	FF-FF-FF-FF-FF-FF
● ICN EN	CAP-M	V3.0	Evaluation	07/13/2004		100	FF-FF-FF-FF-FF-FF
● COM ESY	CAP-MF	V3.0	Evaluation	07/27/2005		100	FF-FF-FF-FF-FF-FF

The **Overview** table contains information on the licensed applications, the number of installed licenses and the number of licenses per application that have already been used or are still available. The lower table contains detailed information on each installed license key.

The MAC ID "FF-FF-FF-FF-FF-FF" represents the demo license key. The key is valid from the first time a demo version is used; it is therefore shown in brackets behind the number of available licenses in the upper table. Demo licenses are valid for 2 months.

The complete display is available for the administrator only; the overview comprises license usage in all business groups.

For a BGAdmin, only the "Overview" part is shown, confined to data of the own BG. The number of available licenses also is calculated within this BG. Licenses that have been installed in CAP without assigning any quota to this BG are shown with a red bullet.

7.5.3 Assigning licenses

There are two ways to assign licenses to individual devices:

? If you use demo licenses or if **new licenses** are installed, the default is for the **"implicitly during register license"** feature to be active. This means that during each first licensing request (`registerLicense`) to the CAP Management for a CAP device, a corresponding license will be granted if this license is available and the device has not been granted the requested license before. If the number of client licenses available is exceeded, temporary licenses that are valid for two months are automatically granted.
Note for TAPI applications: As many TAPI applications regularly do not transmit an individual application ID for licensing (`lineDevSpecificFeature`), the SCC internally carries out a step-by-step license request in the order "CAP-A", "CAP-S", "CAP-E". These steps are repeated until a license has been checked successfully or until there is no license available. For example, if a customer has purchased a CAP-S license, the allocation of the CAP-A demo license must be set to "at device administration", or the CAP-A demo license key must be uninstalled. This prevents demo licenses from being assigned inadvertently.

? Alternatively, the administrator can *explicitly* assign licenses to a device when configuring the device in OpenScape CAP Device Management (cf. Section 7.4.1). If there are no more available licenses when setting up the device, the administrator receives a corresponding error message.

1. Click **Licenses** in the main menu and select the **Assign** menu item in the navigation area to define the assignment process.
2. Subsequently you must select the BG for which assignment is to be displayed / modified. For an administrator, a free selection of all BGs is available (as well as an "Overview" which creates a list of all assignment modes in all business groups ready for printout). For a BGAdmin, only data of the own BG are presented.
3. For each of the license keys/application IDs available, select assignment "at device administration" (explicit assignment by the administrator) or "implicitly during register license" (first come/first served).
4. Click **Save** to confirm your selection.

Licenses assigned to a device (either way) are always shown in the **Search / Modify Device** dialog. In the **Search / Modify User** dialog, licenses indirectly consumed by the user (via devices assigned to that user) are shown as well. As a user may have several devices assigned which come with the same license each, multiple licenses of the same type may be consumed by one user. These are shown e.g. as "CAP-S[2]" : the user is consuming two CAP-S licenses.

7.5.4 Deleting licenses (not for BGAdmin)

Sometimes it is necessary to delete already installed licenses.

1. Click **Licenses** in the main menu and select the **Uninstall** menu item in the navigation area.
2. Select the application / the license key which is to be deleted.
3. If you also wish to remove the licenses to be deleted for devices to whom these licenses have been assigned, then select "Delete license assignments as well".
4. Click **Uninstall** to execute the action.

> > In previous releases of CAP V3.0, it was not possible to delete demo licenses. This is possible now - particularly useful to prevent situations described in Section 7.5.3, where a demo license is assigned although a product license is available.

7.5.5 Split up licenses (not for BGAdmin)

This is a new function in HiPath CAP V3.0 SMR4; it serves to distribute installed licenses among the separate business groups. After installation (Section 7.5.1) licenses automatically are made available in the standard BG "none"; other BGs (in case some have already been created) stay with a quota of 0. In order to change the distribution,

1. Click **Licenses** in the main menu and select the **Split-up** menu item in the navigation area.
2. Subsequently you must select the BG you want to make licenses available for. A free selection of all BGs is available (as well as an "Overview" which creates a list of the current distribution of licenses across all business groups ready for printout).
3. A table is shown with information
   "Application" - installed license keys / applicationIds
   "Installed" - the total number of licenses provided by the installation
   "Remaining quota" - number of licenses not yet assigned to any BG
   "Quota" - enter a quota for the selected BG here
   "Used" - number of licenses currently in use (i.e. assigned to a device) in the selected BG
   "Available" - number of licenses not yet in use (i.e. not assigned to any device) in the selected BG
4. After entering all quotas, click **Save** to confirm the distribution.

7.6 Data

In the **Data** menu item of the main menu you can import data in various formats from a file into the CAP Management database, which is particularly useful for data synchronization with external sources like a PBX administration. Additionally, a bulk import facility is provided which is operating in batch mode and can be invoked offline.

CAP Management data can be exported to a file which may be helpful to conveniently check database contents in a file format. Please note also the export mechanism directly tied to user and device management described in Section 7.3.2 and Section 7.4.2 which serves a similar purpose.

For scheduled synchronization in predefined time intervals, import (and export) tasks / timers can be defined as well.

> 7 Please note that export / import has not been designed to serve as a replacement for backup / restore. Generally speaking, it is neither possible nor reasonable to use a file created during an export operation as input for an import operation.
> Likewise, the formats of export or import files may change between different software versions; so for every new CAP version make sure that your import files still have a valid format - there is no commitment that an import file valid for CAP version x can still be used without problems for CAP version x+1.
> Please note, that in case of many devices belong to one user, the import/export process works fine only by exporting devices, then exporting user and devices, importing devices, and finally importing user and devices with add/update mode.

Please note that the export / import facility has not been designed for that purpose!

The CAP configuration and user data is administered by an open LDAP server (process "SLAPD"); this data is in the directory:

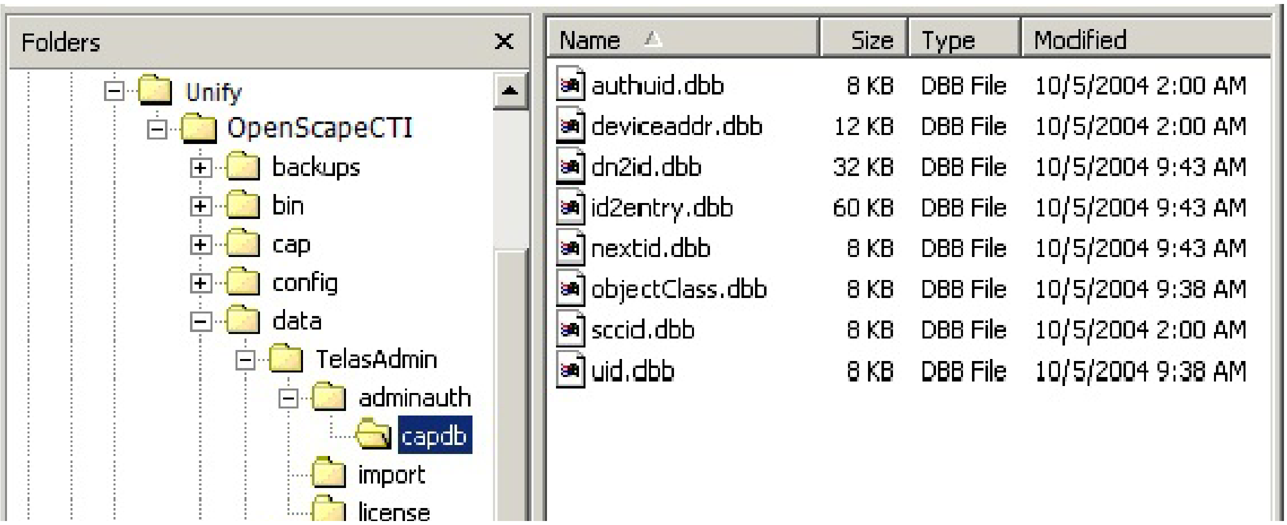
```
<InstDir>\data\TelasAdmin\adminauth\capdb
```

In the case of user and device inconsistency use the following tool:

1. Make sure that CAP service is running

2. Start command <InstDir>\bin\tools\user2device.bat from commandprompt

3. If you have a very large databsase and after running this tool you find "NO Response" text in the output text, then try to increase the value of the parameter soTimeOut.
It is also advisable to carry out the command as followed:
user2device.bat > out.txt
so you can save the result in a convenient way.



Name	Size	Type	Modified
authuid.dbb	8 KB	DBB File	10/5/2004 2:00 AM
deviceaddr.dbb	12 KB	DBB File	10/5/2004 2:00 AM
dn2id.dbb	32 KB	DBB File	10/5/2004 9:43 AM
id2entry.dbb	60 KB	DBB File	10/5/2004 9:43 AM
nextid.dbb	8 KB	DBB File	10/5/2004 9:43 AM
objectClass.dbb	8 KB	DBB File	10/5/2004 9:38 AM
sccid.dbb	8 KB	DBB File	10/5/2004 2:00 AM
uid.dbb	8 KB	DBB File	10/5/2004 9:38 AM

7.6.1 Importing data

Data import is always controlled by an import file containing a header line providing information for interpretation of the remaining file contents, followed by one line per entry / record. For additional details, please see below.

If you want to import data from a particular file, select **Data | Import**.

1. Click **Data** in the main menu and select the **Import** menu item in the navigation area.
2. Enter the data in the relevant fields. The fields are described in the table below.

"Database import" dialog

Field	Description
Data type	Select the objects to be imported: ? User and device data ? Device data ? User data ? User and device data HiPath 8000 Depending on the selection, the data fields that may be present in the import file are different. The last selection has been provided for cooperation with the HiPath 8000 "GEM tool" only.
Import mode	Select one of: ? Create data from import file the respective part of the DB is purged before import, leaving DB contents identical to import file contents ? Add/update entries from import file which means Add+Modify - entries present in the import file will be created / updated in the database, others remain untouched ? Update entries from import file which means entries in the import file are updated according to the defined action (ADD, MOD, DEL); others remain untouched
Import File	Identify the file to be imported, either by directly specifying a path name or by selecting the file in a search dialog

Field	Description
Business group (preselected for BGAdmin)	The default selection is "Standard" or "none". Additional BGs are presented for selection as soon as BGs have been defined. Import data is processed according to the "Business Group" value coming with the data: In case it fits the selected BG, the record is processed, otherwise it is ignored. An empty selection field (not for BGAdmin) is equivalent to all BGs being selected. In this case, all data records are processed and assigned to BGs according to the respective "Business group" value provided. In case a specified BG does not yet exist, it is created implicitly. Records that come without a "Business Group" value are assigned to the standard / "none" BG.

3. Click the **Start transfer** button to start importing.

All of the configuration and schema files described below are located in the directory

```
<InstDir>\data\TelasAdmin\import
```

Import configuration file

The file `impAdmData.cfg` defines parameters for data import.

```
ExecuteAllChanges = 1 (Default unset)
```

This option has been introduced to prevent accidental modification of large parts of the database. If the parameter is unset (commented out), data import is controlled depending on the number of entries existing in the CAP DB and the number of changes to be made. If there are less than 100 CTI users, an import is performed only if the number of the data changes is lower than 10%. If there are 100 or more CTI users, an import is performed only if the number of the data changes is 1% or lower.

In case you don’t want or need this kind of protection, remove the comment sign to enforce execution of all changes in any case.

It is possible to set up customer-specific the limit to another value than 1%.

In this case use the new parameter

```
# Maximum number of objects which can be changed before import stops
(in percent)

#NumOfChangesInPercent = 1
```

Insert the desired customer-specific value (in percent) and remove the comment sign in front of the parameter NumOfChangesInPercent. In this case the value is used as limit (without dtermination for "small" or for "large" databases). This limit can be canceled, when you activate the parameter ExecuteAllChanges = 1.

Please note that all saved changes in the file impAdmData.cfg are activated automatically for the following import-action (initiated with CAP user interface or timer)

It is not necessary to restart the CAP or different CAP services.

Data import files

Depending on data type and import mode selected, different formats apply; you may use the `devices.hdms`, `user.hdms`, or `user.txt` template files as a starter for creating your own import file.

Fields supported in a "Device data" import file

Field	Description
action	for import mode "update entries from import file", this field defines the action for the respective entry / record; supported values are ADD (new entry), MODify, DELete (existing entry)
countryCode	e.g. "49" for Germany, "43" for Austria
areaCode	local area code without leading 0, e.g. "89" for Munich
number	main number without extension, e.g. "722" for Unify MUC
extension	extension, e.g. the "1234" of +49(89)722-1234
sccId	identifier of the service (SCC) controlling the device
sccId2	identifier of the alternative service (SCC) controlling the device (AccessPointEmergency configuration, HiPath / OpenScape 4000 only)
deviceId	device number in canonical format, e.g. "+49(89)722-1234"
devType	values supported for device type are Phone (default), SIP, HuntGroup, VirtualDevice, RoutingDevice, Trunk
deviceInfo	identifier for device description used in XMLPS context; values supported are CMI, Optipoint_410, Optiset_Advanced
pbxFormat	device number in format used towards the PBX +49(89)722-1234 translates e.g. to "897221234" (HiPath 8000) or "1234" (HiPath / OpenScape 4000, overlap 0) or "21234" (HiPath / OpenScape 4000, overlap 1)

Field	Description
pnp	definition of a private numbering plan, format is <L2C>-<L1C>-<LC>:<overlap> (e.g. "49-89-722:2") <L2C> and <L1C> are optional
nac	node access code
XMLPSId	id of an XML Phone Service the device has been configured for
urlAssignList	list of pairs <invoke button>:<URL Id> configured for the device e.g. "2:url1"
licenses	list of licenses assigned to the device, e.g. "CAP-S,ComAssistant"
businessGroup	business group the device is assigned to
deviceCategory **namedDeviceTypes** **routeingDevice** **groupHunt** **groupACD** **groupPick** **groupUser** **deviceModelName** **nidGroup**	these items are used as specified in the CSTA standard

Mandatory fields for Device data import are sccId plus either deviceId or a combination of countryCode, areaCode, number, and extension.

> 7 For the import action to be executed consistently, please note that the SCC identified for a device must have been configured already in CAP Management, using the same countryCode/areaCode/number data as defined for the device.
> Example:
> Importing a device entry "+49(89)722-1234|007" leads to inconsistencies if
> - either an SCC with ID 007 has not yet been configured before
> - or SCC "007" exists but has been configured with, say "+49(89)700".
> SCC "007" must have been configured with "+49(89)722".

Example (minimal Device data import file):

```
countryCode|areaCode|number|extension|sccId
49|89|722|53111|0220
49|89|722|53517|0220
```

which is functionally equivalent to:

```
deviceId|sccId
+49(89)722-53111|0220
+49(89)722-53517|0220
```

Fields supported in a "User data" import file

Field	Description
action	for import mode "update entries from import file", this field defines the action for the respective entry / record; supported values are ADD (new entry), MODify, DELete (existing entry)
name	user name, e.g. "James Bond"
credentials	password in clear text; in case the entry is empty, the user will be assigned the standard password
credStamp	validity period for password (this field is supported in case of export only!)
authUId	unambiguous alias for login (in case of Windows login, use <domain>\<loginName>
uid	unambiguous identifier for the user
roles	user roles; values supported are CTI user (default), Admin, application
authMode	authentication mode; values supported are TELAS (default), NT
userGroups	comma separated list of user groups the user is assigned to
timeZone	time zone the user is assigned to
businessGroup	business group the user is assigned to
removable	flag shows if user may be removed or is protected against removal (this field is supported in case of export only!)

Mandatory fields for User data import are either uid or authUId; in either case, it is reasonable to provide a name as well. In case of authMode=NT (authentication by Windows login) authUId is mandatory.

Example (User data import file):

```
name|credentials|authUId
James Bond||jamie
```

Fields supported in a "User and device data" import file

Fields include all of the entries named above for device import and user import.

Mandatory fields for User and device data import are the same as specified for Device data import. In case neither uid nor authUId are defined, the uid value is taken from the number / deviceId. Please note this may cause problems in case a device is shared among several users!

Example (User and device data import file, update mode):

```
action|countryCode|areaCode|number|extension|sccId|name|credentials|au-
thUId|licenses
ADD|49|89|722|53111|0220|JAHN|myPasswd|janni|
MOD|49|89|722|53517|0220|Gustav Meier||gustl|CAP-A
```

Data import log files

The `"updatePerm.cmd"` can be found in this directory after the import. It contains all import tasks that have been executed. The name of the log file is:

```
<InstDir>\logs\<PC name>\import.log
```

This file is updated permanently to log all of the modifications triggered via import actions.

Import HiPath / OpenScape 4000 non-station devices

When applications address non-station devices (see Section 7.4) of the HiPath / OpenScape 4000, an address type conversion has to be performed. Devices of this type are identified by their LODEN number towards the HiPath / OpenScape 4000, but the application regularly will use a (symbolic) device ID / phone number.

Example:

```
RCG 100      dialing number: +49(5251)2214+7661    LODEN: 33554442
```

The HiPath 4000 Expert Access utility includes a feature for downloading all device data (extensions, hunt groups, RCG groups, trunks as well as the respective LODEN numbers) from the switch to a file.

7 Please note that for successful import the "Canonical Prefix"
[example: +49(5251)2214] as used in OpenScape CAP
must have been configured consistently in HiPath / OpenScape 4000 via AMO KNDEF

Importing device data via the SPI utility as described in Section 6.2.3 is the more convenient way.

7.6.2 Bulk import (not for BGAdmin)

In order to expedite the initial CAP setup for a large number of users / devices, a bulk import facility is provided. This facility works in offline mode only (OpenScape CTI service not running). It takes an import file (regular format as used for online import as well) to create a file in ldif format which then is passed to the database via LDAP slapadd command.

Please proceed as follows:

1. Stop the OpenScapeCTI service
2. Adapt the `impAdmData.cfg` configuration file (see Section 7.6.1); just activate the entry

   ```
   UsingLdif = true
   ```

   by removing the comment character
3. From a command window in the `.../HiPathCTI/bin/tools` directory, invoke the file

   ```
   import.bat <import file name>
   ```

   providing `<import file name>` either as a path name relative to the `.../HiPathCTI/data/TelasAdmin/import` directory, or as an absolute path name

   This creates a file named `objects.ldif` located in the `.../import` directory which in turn is entered into the database using a database tool named slapadd.
4. After the action has been completed, you may want to deactivate the "UsingLdif" entry.
5. Restart the OpenScapeCTI service.

> 7 With the "bulk import" inevitably duplicate entries will be created for those devices which are already inserted with the "normal import method".
>
> Therfore it is recommended to use only one of the offered "import methods".

> 7 During "bulk import", special attention must be paid to password handling.
>
> Bulk import runs in offline mode, i.e. no data can be retrieved from the CAP database which is not running; this holds for the "default password" setting as well. That is why a password ("credentials") must be provided for every user entry in the bulk import file; it may be the (business group specific) default password.
>
> Please note that passwords are to be specified in cleartext here; they must be at least 3 characters.

7.6.3 Exporting data

If you want to export database contents to a file (using the .csv comma-separated-values format), select the **Data | Export** menu item.

1. Click **Data** in the main menu and select the **Export** menu item in the navigation area.
2. Enter the data in the relevant fields. The fields are described in the table below.

"Database export" dialog

Field	Description
Data type	Select one of: ? User and device data ? Device data ? User data ? User and device data HiPath 8000 Depending on the selection, the data fields available for export are different; for details, please refer to the description for import in Section 7.6.1
Business group (preselected for BGAdmin)	The default selection is "Standard" or "none". Additional BGs are presented for selection as soon as BGs have been defined. Only data of the selected BG are exported. An empty selection field (not for BGAdmin) is equivalent to all BGs being selected.

3. Click the **Select fields** button in case you want to restrict the export to specific fields of the user and / or device data. After selection, click **Start transfer**.
4. Alternatively, click the **Export all fields** button in case you want to have all available user / and or device data exported.
5. You are then prompted with a regular Windows dialog to either open the created export file or save it to a destination that can be specified.

> > Please note that for security reasons user export is confined to users with role "CTI user". Neither "admin" nor "application" users will be exported.

7.6.4 Scheduled tasks

You can configure a new task or reconfigure an existing task here. You can use a task (timer) to define the times at which the files are to be automatically imported from a particular directory or at which the CAP CTI users should be exported to a particular directory. You cannot change the name of the export file here - it is "user.txt" or "user.hdms".

To configure a task (timer) for the first time or to reconfigure an existing task, proceed as follows:

1. Click **Data** in the main menu and select the **Scheduled Tasks** menu item in the navigation area.
   a) There are currently no tasks configured. Continue with 2a.
   b) A task has already been configured. You will see this in the "List of running import timer". Continue with 2b.
2. Configure the tasks.
   a) If no task is yet configured, click the **Create new timer** icon.
   b) If a task is already configured, you will see it in the "List of running import timer". Select the task by clicking the **Edit** icon.
3. Complete the fields described below:

"Timer configuration" dialog

Field	Description
Timer name	Enter any name for the task.
Transfer type	Select one of: ? User and device data ? Device data ? User data ? User and device data HiPath 8000 Depending on the selection, the data fields that may be present in the import file are different; for details, please refer to the description for import in Section 7.6.1
Direction	Select import or export.
Import mode (field inactive if export has been selected)	Select one of: ? Create data from import file ? Add/update entries from import file ? Update entries from import file See Section 7.6.1 for details.

Field	Description
Interval	In this field, specify the intervals at which the database is to be imported or exported. You can choose between the following intervals: ? once a day ? once a week ? once a month
Time of activation	Enter the start time for the transfer in hours (hh) and minutes (mm).
Day of activation	Enter the start date for the transfer in DD/MM/YYYY format (e.g. 16/05/2004). You can also select the date from a calendar. To do this, click the calendar icon on the right next to the input field.
Source/Target directory	Specify the location where the export file is stored or the import file is located.
File name	Specify the name of the export or import file.
Business group (preselected for BGAdmin)	The default selection is "Standard" or "none". Additional BGs are presented for selection as soon as BGs have been defined. The scheduled task refers to the selected BG.

4. Complete your entries with one of the following actions:

Action	Description
Save	Saves your entries and adds the task to the "List of running import timer".
Pause	Puts the selected task into standby mode, which means that it will no longer execute until you release it again with this button.
Delete	Deletes the selected task from the "List of running import timer".
Cancel	Closes the dialog without saving the entries.

By clicking on the icon terminating any timer entry in the list of timers, you may obtain detail information on the current state of the respective timer.

7 For scheduled tasks to be processed correctly it is indispensable that specified files be available (read/write) at the scheduled time and (for import) be up to date. In order to prevent one and the same import file from being imported again and again (without noticing that no new import file was provided) every import file will be renamed after successful processing by prepending an underscore "_" to the file name.

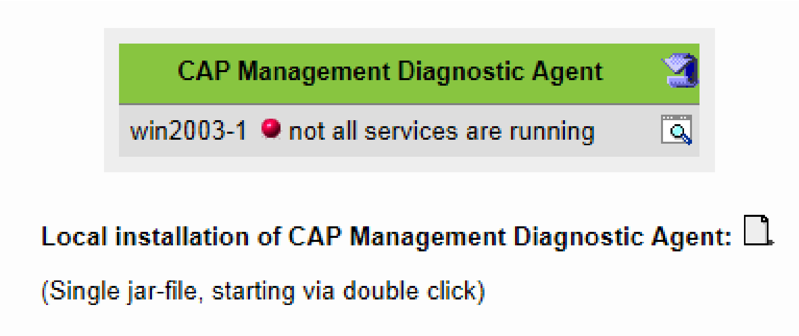
7.7 Diagnostics

The functions for monitoring, configuration and problem diagnostics for all components in the system are handled here. For example, logging information, display and modification of configuration data, service and process states, display of participating hosts, restart processes.

Important note! If CAP SMR13 or SMR14 is installed then Java 7 must be installed and set as default JRE on the client machine from where the Management is accessed otherwise - due to conflicting versions - it won’t be possible to start it.

1. Click **Diagnosis** in the main menu and select the **Diagnostics** menu item in the navigation area:

   A general message indicating the status of the overall system is displayed.



CAP Management Diagnostic Agent

win2003-1 ● not all services are running

Local installation of CAP Management Diagnostic Agent:

(Single jar-file, starting via double click)

2. Click the 🔍 button to the right of the message.

   The **CAP Management Diagnostic Agent** diagnostic applet is started and provides all functions for diagnostics and configuration in a separate window.

The CAP Management Diagnostic Agent can be installed locally. This application then runs locally on the PC, independently of the Web browser.

Local installation of the CAP Management Diagnostic Agent

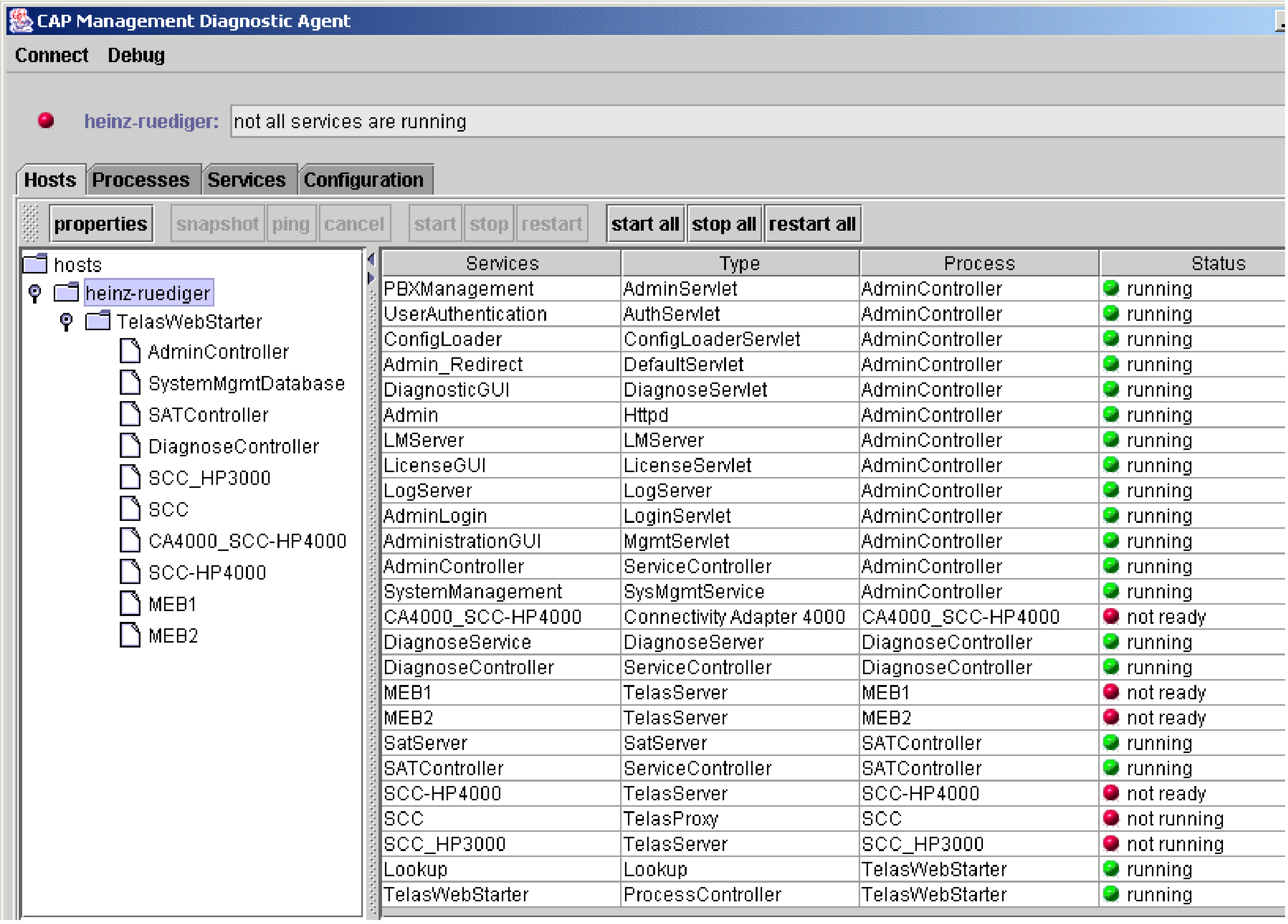
1. Start downloading the `twebDiagAgent.jar` file.
2. Note the location of the downloaded file.
3. In Explorer, go to the folder containing the saved file.
4. Start the CAP Management Diagnostic Agent by double-clicking it.

> If the "Diagnostic Agent" is installed locally, this application must not be installed in a path that contains blanks. If this is the case, the local "Diagnostic Agent" cannot start.
> You can solve this problem by changing the REGISTRY, however.
> In `HKEY_CLASSES_ROOT\jarfile\shell\open\command`, change the entry:
> "`<jre path>\bin\javaw.exe" -jar %1`
> to:
> "`<jre path>\bin\javaw.exe" -jar "%1`".
> `<jre path>` is the path to the locally installed Java Runtime Environment.
> Restriction: the Diagnostoc Agent from the SMR9 requires Java 1.6 installation, from SMR13 requires java 1.7!

If German is selected as the browser language when downloading, then the German version of the CAP Management Diagnostic Agent will be supplied - similarly the English version will be supplied if the language setting is English.

The Diagnostic Agent is always associated with a Diagnostic Controller that runs on the PC with the CAP Management from which it was downloaded.

The following figure shows the user interface of the CAP Management Diagnostic Agent:



🔴 heinz-ruediger: not all services are running

Services	Type	Process	Status
PBXManagement	AdminServlet	AdminController	🟢 running
UserAuthentication	AuthServlet	AdminController	🟢 running
ConfigLoader	ConfigLoaderServlet	AdminController	🟢 running
Admin_Redirect	DefaultServlet	AdminController	🟢 running
DiagnosticGUI	DiagnoseServlet	AdminController	🟢 running
Admin	Httpd	AdminController	🟢 running
LMServer	LMServer	AdminController	🟢 running
LicenseGUI	LicenseServlet	AdminController	🟢 running
LogServer	LogServer	AdminController	🟢 running
AdminLogin	LoginServlet	AdminController	🟢 running
AdministrationGUI	MgmtServlet	AdminController	🟢 running
AdminController	ServiceController	AdminController	🟢 running
SystemManagement	SysMgmtService	AdminController	🟢 running
CA4000_SCC-HP4000	Connectivity Adapter 4000	CA4000_SCC-HP4000	🔴 not ready
DiagnoseService	DiagnoseServer	DiagnoseController	🟢 running
DiagnoseController	ServiceController	DiagnoseController	🟢 running
MEB1	TelasServer	MEB1	🔴 not ready
MEB2	TelasServer	MEB2	🔴 not ready
SatServer	SatServer	SATController	🟢 running
SATController	ServiceController	SATController	🟢 running
SCC-HP4000	TelasServer	SCC-HP4000	🔴 not ready
SCC	TelasProxy	SCC	🔴 not running
SCC_HP3000	TelasServer	SCC_HP3000	🔴 not running
Lookup	Lookup	TelasWebStarter	🟢 running
TelasWebStarter	ProcessController	TelasWebStarter	🟢 running

To navigate in this window, simple select the relevant tab. The significance of the various tabs is explained below.

Diagnostic information

The following information is important and helpful when analyzing problems:

- **Product information**: provides an overview of the installed product. The version and build states are important points here. This information should always be supplied when contacting the hotline.
- **Process information**: shows the table of currently active processes. It is important that the status of all displayed processes be correct. This gives the administrator an initial overview of the problems.
- **Service information**: this table contains precise information about the services active in the system as well as their status. The status also indicates potential problems. The process/service allocation is also displayed.

– **Configuration information**: the configuration files can be viewed, analyzed and changed. Once configuration files have been changed, the corresponding components (possibly even the entire system) must be shut down and restarted.

– **Logging information**: logging information is constantly written to files during operation. All log files are saved in the directory <InstDir>\Logs. The errors.log file plays an important role. Errors related to all services are saved in this file together with the appropriate service ID. It is advisable to check this file at regular intervals and to reset it if necessary so that problems can be identified more quickly in the event of an error. To enable precise analysis of a specific, reproducible problem, you must first delete the logging history (Logging Reset) and then reproduce the error. This removes outdated log information and reduces the amount of log data to be analyzed.
When the system is restarted, any existing log files are renamed as < name>_last.log in accordance with the logging configuration so that information is not lost. Varying amounts of information are saved depending on the log level set. Log levels for active processes are displayed with Show Logging. If a problem is discovered in one of these processes, its level can be raised specifically to obtain more precise information.

– **Save Diagnostic Data**: with this option, the diagnostic information can be saved to a file for analysis and forwarding. The data is packed in a zip archive and can be downloaded by development or the hotline.

> > The status info presented in the diagnostic agent will be synchronized with the processes / services in regular intervals; yet it may not be accurate in case of status changes between synchronization points. You may enforce synchronization at any point in time by invoking Connect -> Refresh.
> More information on diagnostics is contained in Chapter 8, "Troubleshooting".

7.7.1 Hosts

If the **Hosts** tab is selected, all hosts in a network where a OpenScape CTI service is running are shown in a tree structure in the left window. If a host is selected, all services running on that PC are shown with their state and process allocation.

? **Properties**
In general **Properties** can be used to display additional information in a separate window as soon as a host or a line has been selected in the list of services. This information can be evaluated in Development for diagnostic purposes.

? **Start all, stop all, restart all**
This function enables all CAP/CTI processes on particular hosts (select the required hosts in the tree structure) or on all hosts in the network (uppermost entry **hosts** to be started, stopped or stopped and directly restarted.

7.7.2 Processes

If the **Processes** tab is selected, all processes running in the entire system are listed. If a process is selected, various functions can be executed for this process.

? **Properties**
Same as above (Section 7.7.1), depending on the process selected.

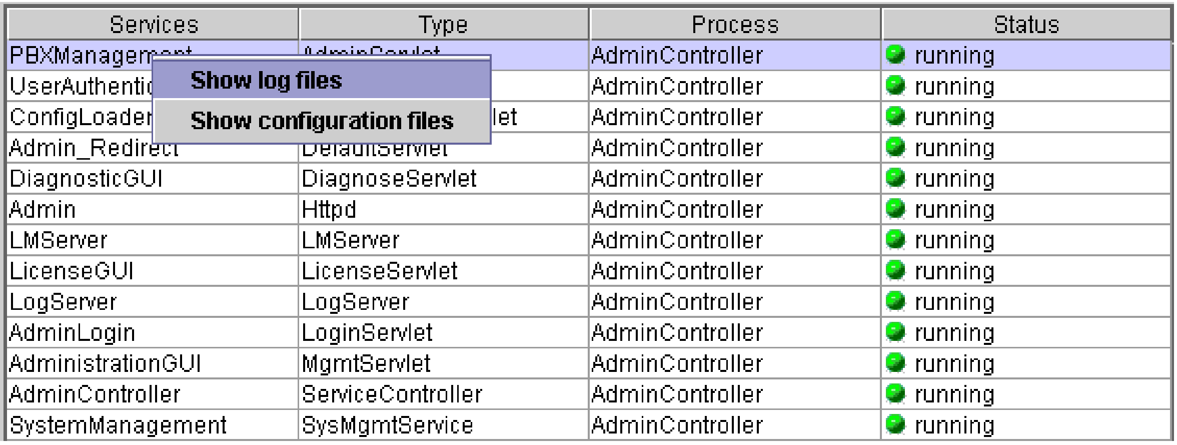
? **snapshot**
If a process is selected, you can call up information on the process environment, logging and thread state via **snapshot** You can also query the parameters currently loaded (for example, query the port of an SCC).

? **ping**
If a process is selected, you can check the current receive status using **ping**.

? **start, stop, restart**
These functions can be used for all processes with the exception of the special **TelasWebStarter** process.

? **start all, stop all, restart all**
All other processes are started using the **TelasWebStarter** process. In this way the system can be shut down completely and then restarted after this process is selected.

? **Show log files, Show configuration files**



Services	Type	Process	Status
PBXManagem	AdminServlet	AdminController	● running
UserAuthentic		AdminController	● running
ConfigLoader	let	AdminController	● running
Admin_Redirect	DefaultServlet	AdminController	● running
DiagnosticGUI	DiagnoseServlet	AdminController	● running
Admin	Httpd	AdminController	● running
LMServer	LMServer	AdminController	● running
LicenseGUI	LicenseServlet	AdminController	● running
LogServer	LogServer	AdminController	● running
AdminLogin	LoginServlet	AdminController	● running
AdministrationGUI	MgmtServlet	AdminController	● running
AdminController	ServiceController	AdminController	● running
SystemManagement	SysMgmtService	AdminController	● running

These functions are available via a context-sensitive menu: Select a process, open the context-sensitive menu with the right mouse button and select the function. The list of log/configuration files is displayed. Double-click the relevant file to display the content.

7.7.3 Services

A complete list of the services available in the system together with their process allocation and current state are displayed when you click the **Services** tab. The following functions are also available in this tab after a service has been selected:

? **properties, snapshot** and **ping**
Same as above (Section 7.7.1, Section 7.7.2), depending on the selected service.

? **Show log files, Show configuration files**
As above (Section 7.7.2), these are available via a context-sensitive menu for the selected service.

? **Reload config**
This facility allows to have the selected service reload its configuration data without being restarted. It has not yet been made available for all types of CAP services, so depending on the type of service selected the button is rendered active or inactive in a context-sensitive way.

7.7.4 Configuration

The complete system configuration can be viewed and edited via the **Configuration** tab. The `<`*`InstDir`*`>\config\` configuration directory is displayed in the left window in a tree structure with the usual Explorer navigation option. The configuration files contained in the selected directory are shown to the right. The following functions are possible in this view:

? **Properties**
The amount of existing data, the last change date and the name of the directory for existing files are displayed for the selected directory.

? **Display**
The content of the selected configuration file is displayed in an edit window. A special feature of this display is that the variables or "include" statements used in the file can be resolved accordingly using the **Replace variables** function and filled with completely new information. Changes can only be saved in the *Not replaced* state.

7.7.5 Logging

During runtime, runtime information is saved to files for all services in the system. This includes information, warnings and faults. The scope of recorded data depends on the set log level.

All log files are generally saved in the `<`*`InstDir`*`>\Logs directory`. In the case of distributed installations, a separate subdirectory with the host name (no domain suffix) is created for each participating PC.

Logging is controlled and log files are displayed in the CAP Management Agent either by means of the **Logging** tab or via the **Debug** menu item.

Once the **Logging** tab has been selected, all file loggers who save information to files are displayed. These can easily be allocated to the corresponding process/service based on their names. For this, the current logging level is displayed in the right hand column as the most important information for all loggers. Once a line in this table has been selected, the level for the selected logger can be modified.

? **Properties**
By clicking "properties", additional information on the selected logger is shown in a separate window. This information is only intended for service technicians or development.

? **Reset Logging**
This function permits the deletion of old logging information which may disrupt fault analysis. Older logging files are deleted and the logging file currently in use is emptied.

? **Change Logging Level**
Select the required level from the drop-down menu next to **Set Level**. The selection applies to the currently selected logger. To activate the setting, it must be confirmed using **set level**. The change in logging level only applies temporarily until the relevant service is next restarted. The changes are not written to the configuration files.

> Please note that modifications of the logging level apply to the selected logger only. Settings for the ErrorLog, which is used globally by all loggers, cannot be modified here - they must be done directly in the `LogServer.cfg` configuration file.

? **Set the Log Filter**
You can set <u>one</u> log filter inclusively or exclusively here. It can expand or restrict the logging operation. This filter applies to the entire contents of the log file for a selected CAP process. It is comparable to a search term in a text or Word document.

To view the content of the logging files, select a file logger from the list of file loggers. The context-sensitive menu (right mouse button) **Show Log Files** displays the list of all log files created by this logger. To view the content of the file, double-click the file name.

7.7.6 "Process Controller" and Services

Every running Windows CAP Java process has its own startup script, located in the <PC_name> subdirectories. The configuration file extension is `*.proc` and the leading **Sxx** number specifies the process startup order number.

```
Example: <InstDir>\config\pc-name\admin\S01service_ctrl.proc
```

The processes are: TelasWebStarter, Admin Controller, Diagnostic Controller, SAT Controller and CallIdRepository. They act as "process controller" and "service controller". After a successful process start, every single java.exe will startup additional internal services. The service configuration file extension is `*.svc` and the leading **Sxx** number specifies the service startup order number.

The Admin "service controller" also starts up and controls the CAP HTTP server. The Web server configuration file is `"http-server.props"`.

Admin Controller

The Admin Controller services are:

- PBXManagement
- UserAuthentication
- ConfigLoader
- Admin_Redirect
- DiagnosticGUI
- Admin (HTTP server)
- LMServer
- LicenseGUI
- LogServer
- AdminLogin
- AdministrationGUI
- CallIdRepository
- SATServer
- AdminController (as service controller)

Diagnostic Controller

The Diagnostic Controller services are:

- DiagnosticService
- DiagnosticController (as service controller)

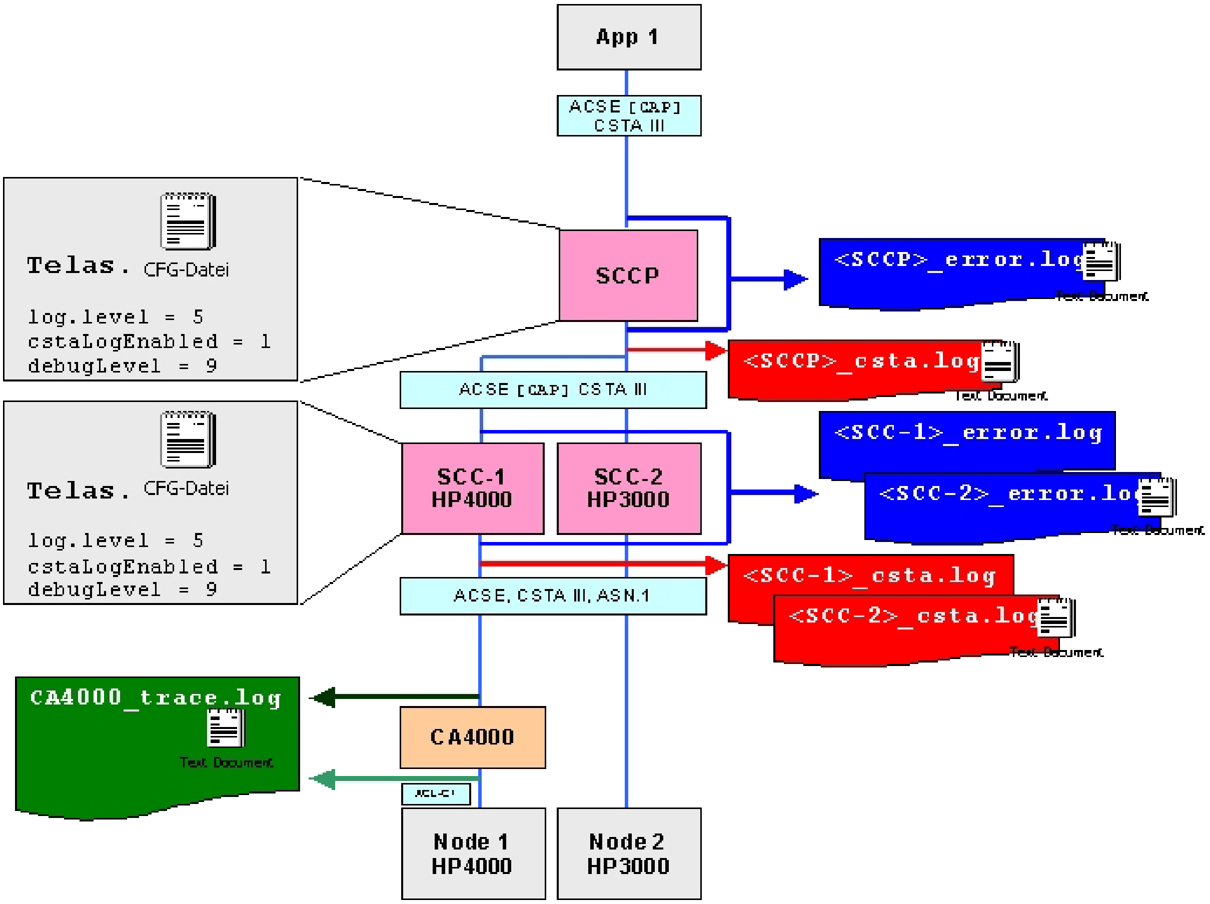
TelasWebStarter

The TelasWebStarter services are:

- Lookup
- TelasWebStarter (as "process controller") (It is the lookup client!!!)

7.7.7 CSTA Communication Trace

Depending on the different interfaces, a complete CSTA communication trace from the application to a switch can be enabled.



7.7.7.1 SCCP Logging

The SCCP is a "multi domain" component and supports the CSTA III protocol in the encoding types ASN.1 and XML. One SCCP supports only one connection to one application at a time.

<SCCP>_error.log

If the log level setting is correct, the <SCCP>_error.log file contains the messages in the encoding types CSTA III ASN.1, CSTA XML and much more! The communication between the application and the SCCP as well as to CAP Management (SUM, SCM, SLM) is displayed.

<SCCP>_csta.log

If the log level setting is correct, the <SCCP>_csta.log file contains the conversation to all SCCs in CSTA III ASN.1. CSTA XML is converted to ASCII.

7.7.7.2 SCC Logging

The SCC is a "single domain/multi domain" component and supports the CSTA III protocol in the encoding types ASN.1 and XML. Depending on the operational mode, one SCC supports only one connection to one application at a time, or multiple connections to SCCP and TCSP at the same time.

<SCC>_error.log

If the log level setting is correct, the <SCC>_error.log file contains the messages in the encoding types CSTA III ASN.1, CSTA XML, NetTSPI (to TCSP) and much more! The application or SCCP conversation, the conversation with the switch or CA4000 and the conversation with the CAP Management (SUM, SCM, SLM) are displayed.

<SCC>_csta.log

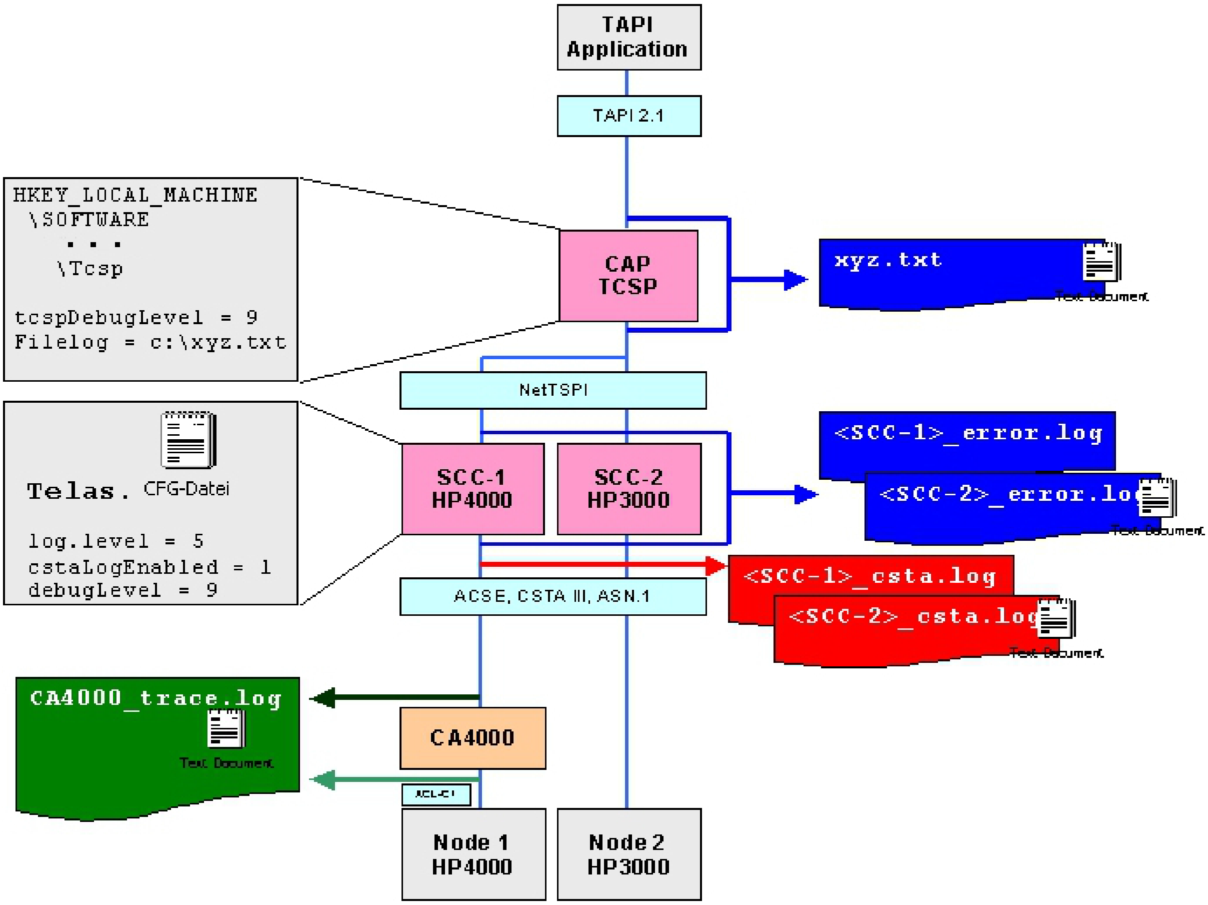
If the log level setting is correct, the <SCC>_csta.log file contains the conversation with the switch or CA4000 in CSTA III ASN.1.

7.7.7.3 CA4000 Logging

The CA4000 trace is part of the CAP standard logging feature. The log file "xxx_-CA4000_trace.log" contains the ACL conversation with the HiPath 4000 and the CSTA III ASN.1 conversation with the SCC.

7.7.8 TAPI Communication Trace

Depending on the different interfaces, a complete TAPI/CSTA communication trace from the application to a switch can be enabled.



```
HKEY_LOCAL_MACHINE
 \SOFTWARE
   . . .
   \Tcsp

tcspDebugLevel = 9
Filelog = c:\xyz.txt
```

```
Telas. CFG-Datei

log.level = 5
cstaLogEnabled = 1
debugLevel = 9
```

In this mode of communication, the CAP TCSP replaces the SCCP. Registry settings define the CAP TCSP log level and the file location. HFind registry entry for "Tcsp"

```
tcspDebugLevel = 9

filelog = "C:\tcsp_log.txt"
```

7.7.9 Saving diagnostic data

This function is useful if direct remote system diagnostics is not possible due to restrictions in network authorization. All logging information, configuration data and other system data relevant for diagnostics is packed in a zip file for downloading.

1. Click **Diagnosis** in the main menu and select the **Download Data** menu item in the navigation area.
2. You may now identify the amount of data to be stored:
   - Log files from all log directories or for selected servers only
   - Configuration files
   - Snapshot of states of running services
3. Click **Download**.
4. You are then prompted with a regular Windows dialog to either open the created file (which normally is not necessary) or save it to a destination that can be specified.

7.8 Security

It is possible to defend the management's web login page from brute force attacks by locking out clients that failed authentication for a while. If this feature is turned on then after every failed login attempt the new login requests from the same IP address are suspended for a couple of seconds. This suspension increases after every failed login attempt. Durring a suspension there is no possible way to log in from the suspended IP, even if the right user name and password have been entered.

7.8.1 List of Suspensions

In this submenu there is a list of the currently suspended IP addresses. If a client manages to log in after one or more failed tries then it will get removed from this list.

- **IP address:** the ipv4 or ipv6 address of the client that failed to login.
- **Last try:** date of the last failed attampt.
- **Attempts:** how many times have the client continuosly failed to log in.
- **Expiration:** date and time when the suspension will end.
- **Remove:** with this function it is possible to remove an entry from this list, so loggin in can be tried again from that client before the original suspension is up.

7.8.2 Suspension Settings

This feature has a couple of settings that can be modified in this submenu.

- **Enable suspensions for failed authentications** (OFF by default) - this flag turns this feature on and off.
- **Skip suspension checking for localhost** (OFF by default) - this flag indicates that in case the login request is coming from the host computer then the whole suspension checking will be skipped.
- **Log the suspensions** (ON by default) - if this flag is on then every suspension procedure will be logged (even the ones when authentication passes).
- **Trusted IP Addresses** - ip addresses in the list are considered safe, so no suspension check will be done for requests coming from any of these addresses.
- **Remove** - removes an address from the Trusted IP Addresses list
- **Add** - adds an addres to the Trusted IP Addresses list (WARNING! No validity check is done here. If the request's ip address doesn't match any of the addresses in the list-then the suspension checking procedure will be launced).

– **Timeframe to save the suspensions in minutes** (60 by default) - due to performance issues the suspensions are not saved in CAP Management’s own database, but kept in the memory. This approach is to prevent the brute force attack escalating to Denial of Sevice attack, and rendering the CAP management database useless by overloading it with failed authentication request. However since suspensions need to be saved a single file will be created in CAP’s config directory, namely suspensions.txt. This file will be read only at the start up, and going to get updated according to the given timeframe.

7.9 Help

The documentation for OpenScape CAP and all installed OpenScape CTI components is available under this menu item.

1. Select **Help** in the main menu.

   All available documentation is listed in the navigation area.

2. Select documentation from the list. You will either see a table listing the relevant documentation or the information will be displayed directly.

Manuals are usually available in both PDF and HTML formats in German and English. Release notes are provided as text files in English only.

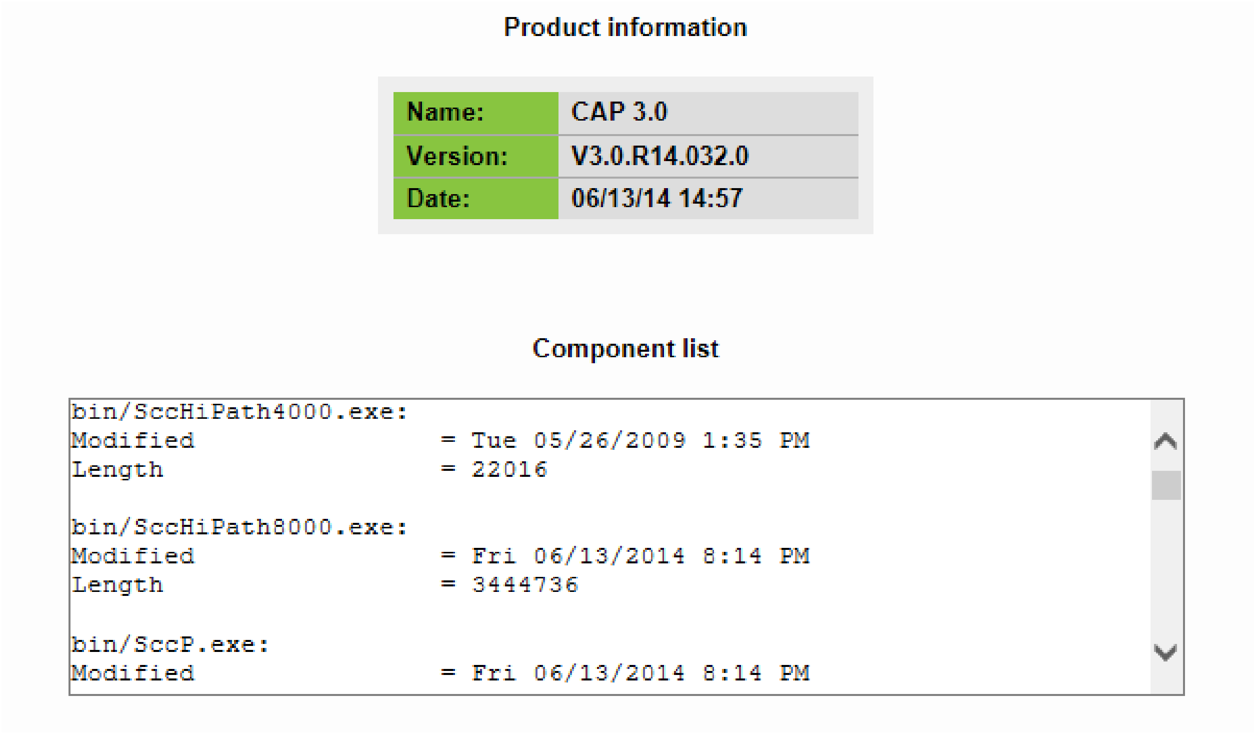
The HTML version is recommended for online consultation; if you wish to print out the documentation you should use the PDF file.

Product information

Product information can also be reached via the **Help** menu item in the main menu. If you select **Product information** in the navigation area, you will see important product information as well as information about licensing conditions and copyright.

In case of faults or problems, the software version and date of manufacture, etc. can be obtained from the product information.

Example of product information:



Product information

Name:	CAP 3.0
Version:	V3.0.R14.032.0
Date:	06/13/14 14:57

Component list

```
bin/SccHiPath4000.exe:
Modified                = Tue 05/26/2009 1:35 PM
Length                  = 22016

bin/SccHiPath8000.exe:
Modified                = Fri 06/13/2014 8:14 PM
Length                  = 3444736

bin/SccP.exe:
Modified                = Fri 06/13/2014 8:14 PM
```

8 Troubleshooting

This chapter covers the following points:

? how to isolate problems,

? how to handle errors,

? how to find technical help.

8.1 Responsibilities in the event of problems

Problems can arise when operating the hardware or software. There are basically four bodies that can be held responsible for a problem:

? the LAN operator,

? Microsoft,

? Unify or

? the application vendor.

Using the following table you can determine who is responsible in each different scenario.

Problem area	Description	Responsibility
LAN	Physical connections, bridge, router, NIC (Network Interface Card)	LAN operator
Windows 2003, 2008, 2012, 7,8	Operating system	Microsoft
SUSE Linux Enterprise Server 10, 11	Operating system	Novell
PC and server hardware	Servers, clients	Customer
OpenScape CAP	CA4000, SCCHiPath4000, SCCHiPath4000V6, SCCP, CAP TCSP, XMLPS	Unify
Application	Installation, configuration	Application vendor

8.2 General procedure for problem definition

To resolve problems when operating the system, proceed as follows:

1. Reproduce the problem to determine if it persists. Make note of all symptoms.
2. Ensure that the client/server application is working properly. If it is not, contact the application vendor or the department responsible for error correction.
3. Follow the instructions for problem definition. Perform the recommended actions one by one until the problem is resolved.
4. If you are unable to resolve the problem on your own, read Section 8.8, "Technical support" for information on how to get technical help.

8.3 Problems during installation

Check the following points if you experience problems after installation:

? Have all installation requirements been fulfilled?

? Has the network configuration of the PC been properly completed?

? Are the host name, IP address and domain name known and configured correctly?

? Is the PC entered in the DNS and does it have a valid name?

? Is the **OpenScapeCTI Service** running (check e.g. via **Control Panel | Services**)?

? Has a Web browser been installed and configured?

? Have you entered the user and password correctly (**`Admin, Admin`**)?

? Was the PC rebooted after installation?

> If you have made any changes to the configuration, the active CTI service must be stopped and restarted, as certain configuration changes only become effective after a program restart. Other problems and information on how to resolve them can be found in the next section.

8.3.1 General problems

? Did you perform a reboot following installation? If not, you should do so now.

? Check if Log Files (in the *logs* directory) contain messages such **as ... port 8170 in use ...**
If this is the case, the port required by OpenScape CAP Management on the system is already in use.

The default is **port 8170**. The port can be reconfigured if necessary:
Search the `config` directory for all files (`*.*`) with the content **8170.** Replace the port number **8170** with a new port number which is not used by the system. You can use any text editor (such as **Notepad**) to edit the files.

? Perform a reboot after making the changes.

8.3.2 Problems with inconsistent IP addresses

If the PC on which a OpenScape CAP component is installed and on which the CTI service is running has several network cards (e.g. one for connecting to the customer LAN and one for connecting to the switching host) then it possible that the wrong IP address is being used to communicate via LAN. This question is usually dealt with during installation (see Section 4.9). To resolve this problem, edit the *InstDir>*`\config\start\startNT.cfg` file by entering the correct IP address for accessing the customer LAN at the following point:

```
args: -localAddr
args: <HostNameOfServer>/<IPAddrOfServer>
```

Example:

```
args: -localAddr
args: PC08154711/139.21.25.245
```

> After this change has been made, the CTI service should be stopped and restarted.

8.3.3 Login not working

On entering a **user name** and **password** for authentication, the Web browser issues an error message such as **Login failed, try again later.**

? Check that the **OpenScapeCTI** service is running.

? Check that the login data has been entered correctly
(note use of uppercase/lowercase).

8.3.4 Administrator home page is not opened

In this case, the browser outputs an error messages, such as

```
Netscape is unable to locate the server localhost:8170.
Please check the server name and try again.
```

? Check that the **OpenScapeCTI service** is running (e.g. via **Control Panel | Services**).

8.3.5 CAP Management is not working on all PCs in the intranet

OpenScape CAP Management operates correctly on the installation host but the pages are not being displayed correctly on some PCs in the Intranet.

1. Check whether the name of the server PC is known.

   For test purposes, the proxy for this PC can be disabled in the browser settings.

2. If this action helps, administer the PC in the DNS.

8.3.6 CAP Management diagnostics applet is not working correctly

After the diagnostic applet has been launched (as described in Section 7.7), the applet fails to start or comes to a stop with a message such as "Wait for Diagnose Server".

This may be due to the fact that the OpenScape CAP Management PC has two network cards. If one of the two corresponding IP addresses is used to access the OpenScape CAP Management interface, but the other IP address is used to start the diagnostic applet, an error occurs in the Java runtime system (security violation).

The only workaround in this case is to explicitly specify IP addresses:

1. As described in Section 8.3.2 above, ensure that the host name and IP address are specified correctly in the file `startNT.cfg`
2. After OpenScape CAP Management has been launched with **Start | Programs | OpenScape CAP | Management**, you should replace the symbolic host name in the CAP Management URL shown in your browser with the IP address.

This ensures the consistent use of the set IP address (at least for the current OpenScape CAP Management session).

8.3.7 Authentication is requested whenever the browser is restarted

Check whether the relevant browser supports cookies and, if so, whether these are enabled.

8.4 Problems with Connectivity Adapter HiPath 4000

In the case of problems limited to Connectivity Adapter HiPath 4000, proceed as follows to discover the precise errors in Connectivity Adapter HiPath 4000.

1. Evaluate the Unify system and error logs.
2. Contact the relevant Unify service department.

Unify system and error logs

Check the Unify system and error logs and check if there are activities or error messages that point to a malfunction in the Connectivity Adapter HiPath 4000.

8.5 Problems with the connection to HiPath 3000

If error analysis points to problems in the connection to the HiPath 3000 switching system that are not dealt with above, please refer to the HiPath 3000 documentation, which provides more detailed information on the topic.

8.6 System diagnostics functions

HiPath CAP Management provides system diagnostics functions to ensure that diagnostics can be performed as simply and efficiently as possible. See Section 7.7, "Diagnostics" for details on the user interface.

With this Web-based user interface, diagnostics can be performed not only on the configuration server, but also from every other host in the intranet host network.

To prevent this data being viewed or changed by every user, the diagnostics area is reserved for the administrator and is protected by an administrator name and password.

8.6.1 General

This section contains information about how to use the functions described in Section 7.7. Diagnostics provides information that is not always intended for the administrator, but which may also have to be sent to the hotline and Service/Development for detailed analysis, for example.

8.6.1.1 Diagnostic information

The following information is important and helpful when analyzing problems.

? **Product information**

Provides an overview of the installed product. The version and build states are important points here. This information should always be supplied when contacting the hotline.

? **Process information**

Shows the table of currently active processes. It is important that the status of all displayed processes be correct. This gives the administrator an initial overview of the problems.

? **Service information**

This table contains precise information about the services active in the system as well as their status. The status also indicates a potential problem in this case. The process/service allocation is also displayed.

? **Configuration information**

The configuration files described in Appendix A.2, "Description of the configuration files" can be viewed, analyzed and changed. Once configuration files have been changed, the corresponding components (possibly even the entire system) must be shut down and restarted.

? **Logging information**

Logging information is constantly written to files during operation. All log files are saved in the directory `<InstDir>\Logs`.

The **`errors.log`** file plays an important role. Errors relating to all services are saved in this file together with the appropriate service ID. It is advisable to check this file at regular intervals and to reset it if necessary so that problems can be identified more quickly in the event of an error.

To enable precise analysis of a specific, reproducible problem, you must first delete the logging history (**Reset Logging**) and then reproduce the error. This removes outdated log information and reduces the amount of log data to be analyzed.

When the system is restarted, any existing log files are renamed as `<name>_last.log` in accordance with the logging configuration so that information is not lost.

Varying amounts of information are saved depending on the log level set. Log levels for active processes are displayed with **Show Logging**. If a problem is discovered in one of these processes, its level can be raised specifically to obtain more precise information.

? **Save Diagnostic Data**

Save Diagnostic Data offers a useful option for combining the diagnostic information and saving it to a file for analysis and forwarding. The data is packed in a zip archive and can be downloaded by Development or the hotline.

8.6.1.2 Start/Restart

In cases where the system configuration is changed (editing of configuration files) or where there are runtime problems with OpenScape CTI system processes/services, the affected components must be restarted. OpenScape CAP Management diagnostics interface (Section 7.7) makes this possible from any PC with network access, even in the case of a distributed installation of the OpenScape CTI system.

In many cases it is not necessary to restart the whole system. It may be enough to stop and restart individual processes. You should also use the diagnostics interface for this purpose as this enables you can to monitor the status of the associated processes at the same time.

8.6.2 Troubleshooting runtime problems

This example is intended to show how the administrator analyzes a service with status *not running* (red LED on).

First, call up the status of all services via the **Services** tab.

If the **Phone** service in the **PhoneController** process shows the status **not running***:*

? Switch to the **Logging** tab. If it is still not displayed, it must be activated via the menu **Debug | Show Logging**.

? The list that appears includes the **Phone** logger together with the configured trace level. Once the relevant line has been selected, the level can also be increased if required.

? The corresponding logging information is obtained with **Show Log Files** by means of the context-sensitive menu (right mouse button) when the line is selected. The contents of the relevant log file can be displayed by double-clicking.

? If configuration data is also required, select **Show Configuration Files** from the same context-sensitive menu.

8.6.3 Diagnosing startup problems

Under normal circumstances, the OpenScape CTI system services are started in sequence by a central service called the Start Service. This is displayed in Windows as the **OpenScape CTI** service.

Log information is generated during a normal startup to enable startup problems to be analyzed. If this log information is not sufficient to pinpoint the problem, it is possible to start each system service separately.

Batch files are provided for this purpose in the `<InstDir>\bin\tools` directory.

1. **`startNT.bat`**

   Start file for the OpenScape CAP Service Starter (OpenScape CTI)

2. **`admin_ctrl.bat`**

   Start file for the administration functions (AdminServiceController)

3. **`diag_ctrl.bat`**

   Start file for the diagnostic functions (DiagnoseController)

4. **`phone_ctrl.bat`**

   If ComAssistant is installed, this is the start file for telephony functions (PhoneController)

5. **`jaccess_ctrl.bat`**

   If ComAssistant is installed, this is the start file for journal functions (JournalAccessController)

To localize errors, proceed as follows:

? Open a shell window and call up `startNT.bat`.
This is the same as starting the **OpenScape CTI** service. However, this has the advantage that all startup errors for the other services are written as **standard error**. These messages should be output to a single file.

e.g.: `startNT 2>startNT.txt`

The entire system is now started, and startup problems are logged in `start.txt`.

If only one of the processes named above is causing problems, you should remove it from the automatic startup. To do this, proceed as follows:

? Installation directory `<InstDir>\config\<HostName>\<ProcessName>`, which is assigned to the <ProcessName> process on the <HostName> PC contains a `S<xx>service_ctrl.proc` file (<xx> stands for a number that can vary for each process).

? Disable this file by renaming the extension `.proc`.

? Start the system via `startNT.bat` or the NT service.
This starts all components apart from the process where the start file has been renamed.

? Open a shell window for starting this process via the corresponding .bat file.

? Once again you should output the **standard error** messages to a single file.

e. g. `admin_ctlr 2>adminStart.txt`

You can proceed in the same way for the other processes. Since the services communicate with one another during operation, other messages are output continuously to the associated shell windows which can be analyzed. Generally, however, a problem can be detected as soon as one of the services starts.

7	Note that when the problem has been rectified, the disabled process start file should be re-enabled (restore `Extension.proc`.

8.7 Special diagnostic information

This chapter describes how should the CAP be proactively configured to have enough diagnostic information in case an error happens.

There are preparations which are suggested to be setup before the whole system started and there are specific settings for specific problems.

8.7.1 General preparations

In case any error happens please always provide the **sysdiag.zip** file which contains the configuration settings and all CAP logs!

8.7.1.1 Standard logging

The standard logging should be enabled. It should be adjusted for all

- SCC (3000,4000,8000)
- SCCP

LogLevel settings

Please edit

<installdir>\HiPathCTI\config\<Server Name>\sccp_<SCCP Id>**Telas.cfg** !

The following entries and values should be set:

```
log.level = 5
debugLevel = 9
cstaLogEnabled = 1
```

For CA4000 please edit

<installdir>\HiPathCTI\config\<Server Name>\ca4000_<ca4000 Id>**ca4000.cfg**

```
log.level = 4
```

For SAT please edit

<installdir>\HiPathCTI\config\<Server Name>\sat\sat_svc\SatServer.cfg

```
LOG_LEVEL = 5
```

For SPI please edit:

<installDir>\HiPathCTI\config\<Server Name>\spi\Telas.cfg

log.level = 5

debugLevel = 9

traceLevel = 5

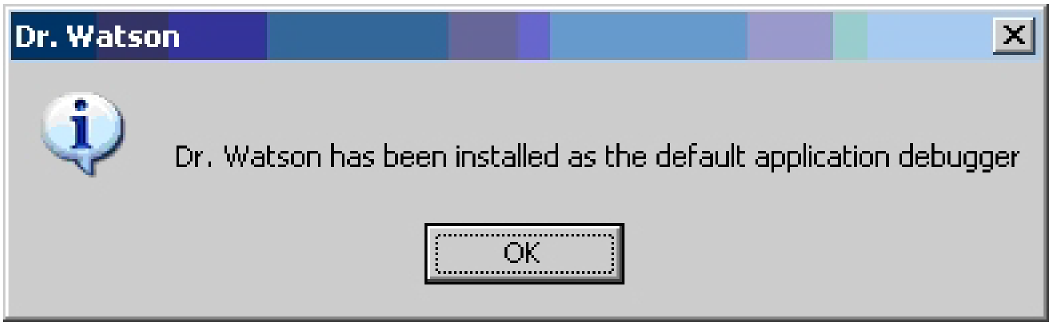
8.7.1.2 Setup DrWatson

The DrWatson should be installed and activated on the CAP server. It will generate diagnostic information in case a CAP component crashes.

Activate DrWatson:

Use cmd line and type „drwtsn32 -I“

You will receive:


Dr. Watson

Dr. Watson has been installed as the default application debugger

In order to verify whether the DrWatson-setup was successful please use cmd line and type „regedit“.

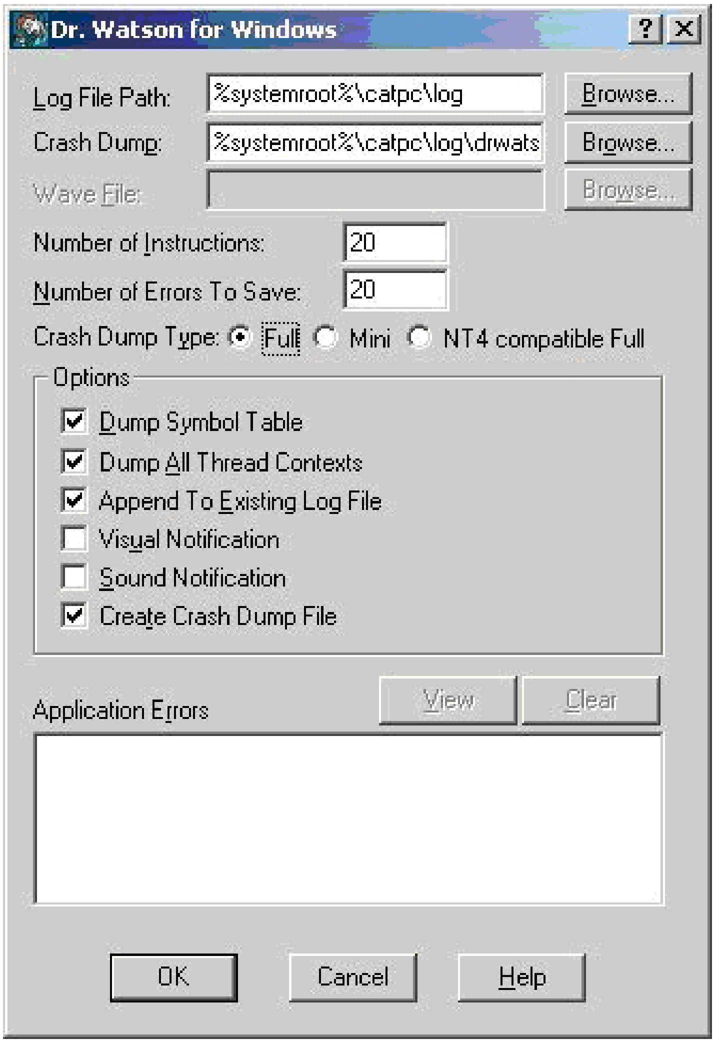
In the path

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug

The value of ***Debugger*** should be *drwtsn32 -p %ld -e %ld -g*

Set DrWatson options:

Use cmd line, type „drwtsn32“. Set the options to the followings.



Log File Path: %systemroot%\catpc\log

Crash Dump: %systemroot%\catpc\log\drwats

Wave File:

Number of Instructions: 20

Number of Errors To Save: 20

Crash Dump Type: ● Full ○ Mini ○ NT4 compatible Full

Options

- ☑ Dump Symbol Table
- ☑ Dump All Thread Contexts
- ☑ Append To Existing Log File
- □ Visual Notification
- □ Sound Notification
- ☑ Create Crash Dump File

Application Errors

The log file name will be ***drwtsn32.log*** and it will be generated in the given path (Log File Path). The file name and path of crash dump can be edited (Core Dump).

In case a crash occurs please save as soon as possible

- sysdiag.zip (log files of the CAP components)
- drwtsn32.log (DrWatson-log) and dump file
- Windows Event Log

8.7.2 Error specific log settings

8.7.2.1 Crash situations

In case of crash of SCC or SCCP components it may be useful to have an additional trace file. It can be activated the following way.

- Stop SCCP in Diagnostic Agent on the "Processes" tab
- In the directory

  <installdir>\OpenScapeCTI\config\<Server Name>\telasServer_<SCC or SCCP Id>

  copy the following lines into ***S10service_ctrl.proc***:

  args: -l

  args: 6

  args: -f

  args: <?x $INST ?>/logs/<SCC or SCCP Id>Trace.txt

  The name of the txt could be for example:

  args: <?x $INST ?>/logs/SCC4000**Trace.txt**
- Start SCCP in Diagnostic Agent

8.7.2.2 Performance problems

It is possible that there are performance problems if any of the following symptom can be observed:

- here are delays in the message processing of CAP
- a CAP component uses 100% CPU for more than 1-2 seconds
- the memory usage of a component increases continuously (without end)

In this case the further analysis needs performance logs. It takes longer and more CAP logs and performance monitor log files.

For more and longer CAP logs please edit

<installdir>\OpenScapeCTI\config\<Server Name>\admin\log\LogServer.cfg

Here are the entries which has to be modified (for all affected SCC/P):

log.maxLines.<SCCP Id>_Error = 500000 (size of the log in lines)

log.maxFiles.<SCCP Id>_Error = 20 (number of log files)

log.maxLines.<SCC4000 Id>_Error = 500000

log.maxFiles.<SCC4000 Id>_Error = 20

E.g.:

log.maxLines.SCCP_Error = 500000

log.maxFiles.SCCP_Error = 20

log.maxLines.HP4000_Error = 500000

log.maxFiles.HP4000_Error = 20

In order to have performance monitor logs please start performance monitor!

(perfmon.exe)

Choose "Counter Logs", then "New Log settings..." by right clicking.

Add a name and add counters to the measurement for every affected process (SCCP):

- Process -> SCCP -> %Processor time -> Add
- Process -> SCCP -> Private Bytes -> Add

Add the overall processor time, too:

- Processor -> Total -> %Processor time -> Add

Set the interval to 1 seconds.

Set the Log File to a "Text file (Comma delimited)" and set "End file names with: mmddhhmm"

Finally schedule the measurement that it will be started and stopped manually.

By right clicking on the name of the measurment it can be started and stopped.

The log file will be generated in the given directory.

8.7.2.3 Problems with SPI service

In case you experience problems with Service for Pbx Information component please adjust the following settings.

In case there are many devices configured on the specific Hipath 4000 then the timeout should be adjusted to let CAP management query all devices from the switch.

In <install_path>\config\<Server name>\admin\mgmnt\admin.cfg

```
SysMgmtTimeout = 600000
```

If you experience further problems please activate SPI tracing.

```
# XML-Trace for SPI Service
    SPI.traceDir = <?x $INST_DIR ?>/logs
    SPI.traceHeader = true
```

These modifications require a CAP service restart.

The additional SPI traces will be generated here:

```
<intsall_path>\logs\SPITraceFile.txt
<intsal_path>\logs\SPI_XML.trc
```

8.8 Technical support

If you are unable to resolve problems encountered when operating the system, please contact the following departments:

? In the event of problems with the application program on the computer system, contact the application vendor.

? In the event of problems with the communication server or the server software, contact the appropriate Unify service department.

? In the event of problems with the CTI server, contact the CSTA application supplier.

9 Operating Modes

OpenScape CAP supports two different operating modes. The PBXs, protocols, and encoding variants supported differ depending on the operating mode.

Single Domain Native Mode

HiPath / OpenScape 4000, CSTA III ASN.1 only

Multi Domain Harmonized Mode

CSTA III ASN.1, CSTA XML, TAPI, JTAPI, XMLPS

> Please note that availability of different operating modes on different switches is subject to being tested and released for the respective CAP release.
> As the final source for definitive information on modes supported, please refer to the ReleaseNotes provided with the CAP release.

9.1 Single domain native mode

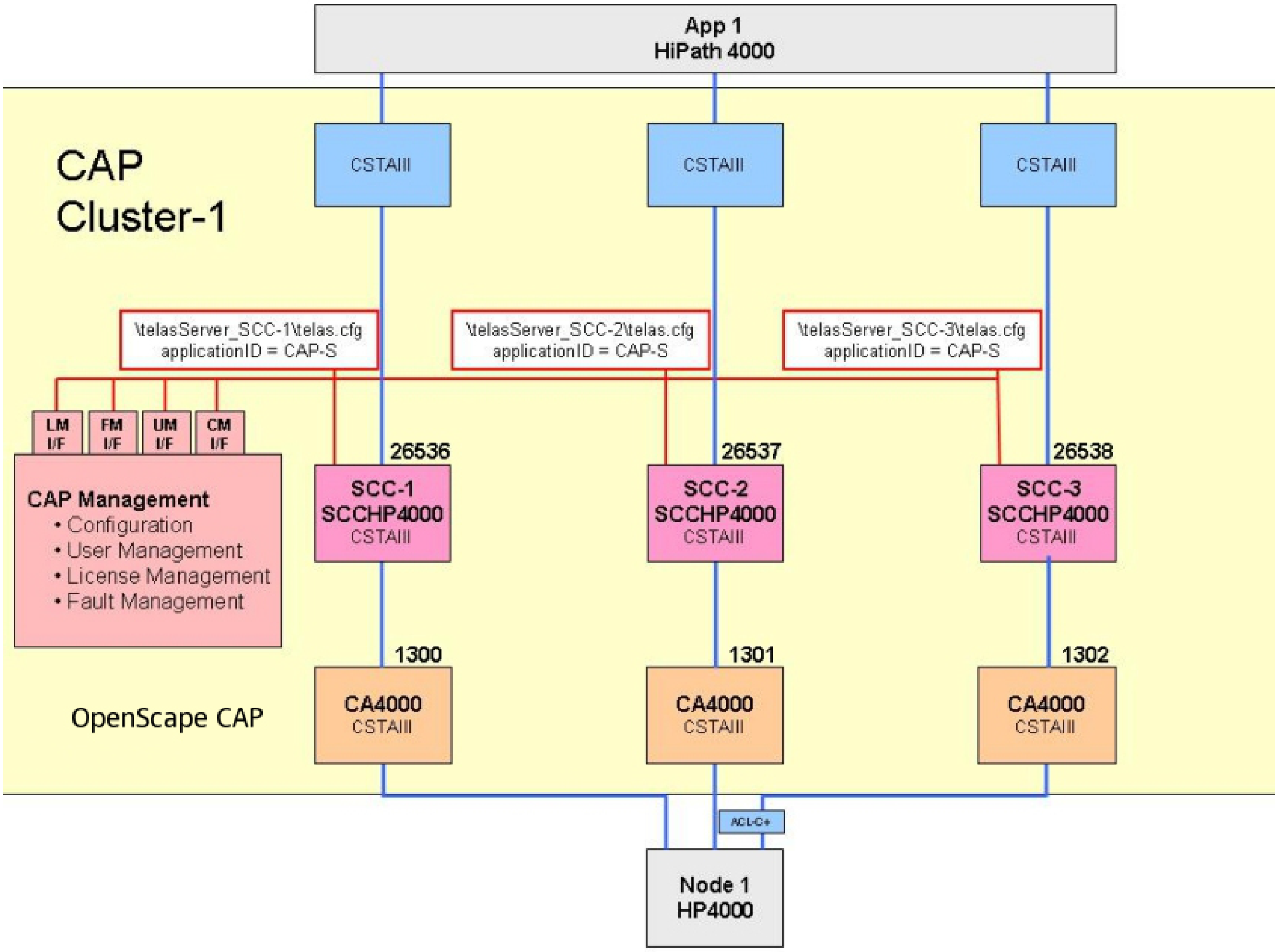
In "single domain native mode", one application is connected to one PBX via one CAP. Proprietary protocol elements, private services, and extended features are supported. The number of SCCs used here is irrelevant, but the **ApplicationID** that is set must be identical for all SCCs.

Single domain native mode is used to provide CTI support to CSTA applications that have already been developed. No application software changes are necessary for this. The application is not aware of the existence of an SCC.

9.1.1 Installation examples

The SCC used for connecting HiPath 4000 to CAP is permanently configured for a defined protocol.

Another installation option involves connecting an application to a PBX using several links for load balancing. In the following example, concrete values (PBX, protocols, and port numbers) are used.



9.1.2 HiPath 4000 SCC configuration in single domain native mode

The HiPath 4000 supports the ACL-C+ proprietary protocol and must have the CA4000 protocol converter. This supports the CSTA III ASN.1 encoded protocol (to ECMA 285), also with additional identification by ACSE. **(CSTA phase I is not supported anymore.)**

Some protocol elements of ACL-C+ are not used.

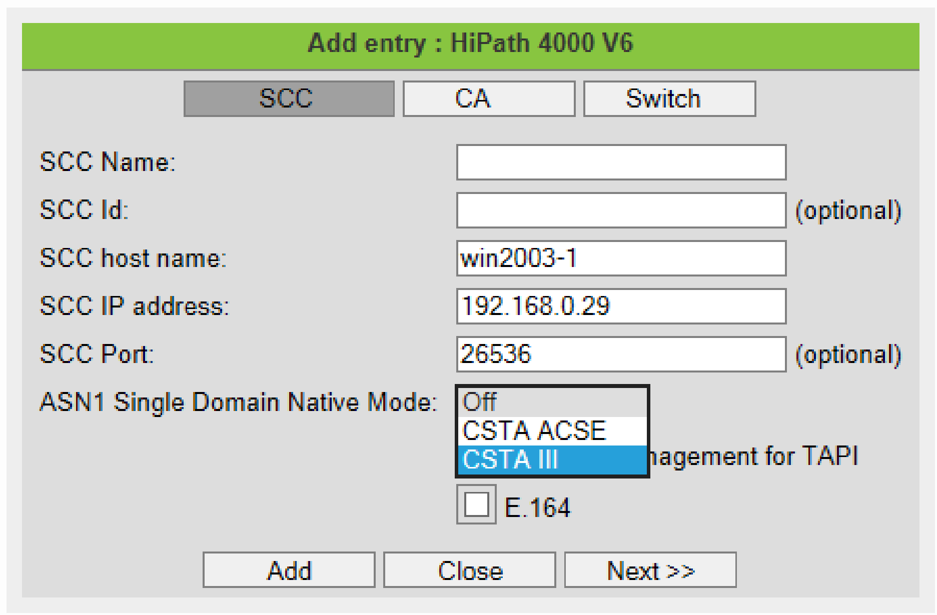
Use the **Service - Switch Connection** menu item to add an "SCCHiPath4000".

"ASN.1 Single Domain Native Mode" is changed to:

? **CSTA ACSE**, and the corresponding CA4000 port is also configured in "CSTA ACSE" mode.

? **CSTA III,** and the corresponding CA4000 port is also configured in "CSTA III" mode.

This configuration always depends on the application used.



Add entry : HiPath 4000 V6

SCC | CA | Switch

SCC Name:
SCC Id: (optional)
SCC host name: win2003-1
SCC IP address: 192.168.0.29
SCC Port: 26536 (optional)
ASN1 Single Domain Native Mode: Off / CSTA ACSE / CSTA III
agement for TAPI
☐ E.164

Add | Close | Next >>

9.1.2.1 CTI users in "single domain native mode"

All CTI users must be configured under User Management.

9.1.2.2 Licensing in "single domain native mode"

The license to be assigned to a CTI user is determined by configuring the parameter "ApplicationID = ???" in the SCC configuration file `telas.cfg`.

With the first CSTA request, the SCC contacts CAP License Management and asks whether the "ApplicationID" assigned in the file `telas.cfg` is assigned to the CTI user as a license. If license assignment in "At user login" (default) mode is active, a license is always assigned. If a license was successfully checked for a user, the SCC saves this information for 3600 seconds. Likewise, this information is deleted when the SCC restarts.

9.1.3 Testing the HiPath 4000 "single domain native mode" for the CSTA III configuration

CSTA test program for CSTA III

To test this configuration, use the program `CSTA3Host.exe.` The connection destination that is configured is the CAP Call Control IP address and the CAP Control port.

SCC status

Without an application connection, the SCC status is "**not ready**".

Operating Modes
Single domain native mode

Application login (ACSE_AARQ)

Not used.

Application ID

The application ID is defined by the "ApplicationID" parameter in the SCC configuration file `tel-as.cfg`.

Native mode = true/false

It is not necessary to mark native mode explicitly because this is configured directly for each SCC.

Extensions

Extensions are addressed via their short extension number in each request.

Call ID

The "Call ID" is two bytes long.

9.1.4 Testing the HiPath 4000 "single domain native mode" for the ACSE configuration

CSTA test program

To test this configuration, use the program `CSTA3Host.exe`. The connection destination that is configured is the CAP Call Control IP address and the CAP Control port.

SCC status

Without an application connection, the SCC status is "**not ready**".

Application login (ACSE_AARQ)

The CSTA version (version five) is indicated.

Application ID

The application ID is defined by the "ApplicationID" parameter in the SCC configuration file `tel-as.cfg`.

Native mode = true/false

It is not necessary to mark native mode explicitly because this is configured directly for each SCC.

Extensions

Extensions are addressed via their short extension number in each request.

Call ID

The "Call ID" is two bytes long.

9.2 Multi domain harmonized mode

In "multi domain harmonized mode", one or more applications are connected to one or more PBXs of the same or differing type via one CAP. Standard CSTA services are supported, but proprietary protocol elements and private services are not supported. In this way, an application is independent of the infrastructure on which it is installed. The number of SCCs/SCCPs used here is irrelevant. Each application to be used uses an individual application ID which is transmitted by the ACSE_AARQ.

The following protocols and coding methods are supported in "harmonized mode":

? CSTA III ASN.1

? CSTA XML

? TAPI 2.2/3.1

? JTAPI

NOTE ON DISTINGUISHING "HARMONIZED MODE" FROM "NATIVE MODE"

The only difference between "harmonized mode" and "native mode" is that "Native = false" (default) is set for the former in the ACSE_AARQ.

NOTE ON CONNECTING AN APPLICATION TO THE CAP

An application is only ever connected to a single SCCP.

NOTE ON CONFIGURING AN SCC IN "MULTI domain HARMONIZED MODE"

An SCC’s "multi domain harmonized mode" is activated with the configuration point: "ASN.1 Single Domain Native Mode = Off".

NOTE ON THE "APPLICATION ID" IN THE SCC CONFIGURATION FILE "TELAS.CFG"

The "ApplicationID" parameter in the SCC configuration file "telas.cfg" is automatically deactivated in "multi domain mode".

Multi domain harmonized mode is used to provide CTI support to new CSTA applications that want to use the CAP "multi domain" feature and that need standard CSTA services but that want to be independent of PBXs.

9.2.1 Application-specific protocol requirements

For "multi domain harmonized mode", applications must meet the following requirements:

1. Login via ACSE

The ACSE_AARQ must contain the following information:

- User name (CAP CTI or CAP admin user)
- Password (of the CAP CTI or CAP admin user)
- Application ID (needed for licensing)
- The CSTA version (version five, version six)
- Native = false (default)

2. Extensions in long canonical format.

The extension numbers must be sent in long canonical format (for example, +49(5251)8-27486) for certain requests (such as, MakeCall, SnapshotDevice, MonitorStart). This format is needed for correct licensing and for forwarding a request from an SCCP to an SCC.

3. The Call ID is a maximum of nine bytes long.

9.2.2 Authentication and licensing

Application authentication

An application always has to send an ACSE_AARQ once a connection has been set up to an SCCP. The user/password (for example, CAP/123) contained in this request must match a CAP CTI or CAP Admin user. The SCCP sends a corresponding HTTP request `(http://<fqdn>:8170/mgmnt/auth/req?authenticate=<User ID>&passwd=<Password>&encoding=b64)` to CAP User Management. If the user is successfully authenticated, the TCP/IP connection to the application is maintained. If the authentication is unsuccessful, the TCP/IP connection to the application is interrupted. The "Application ID" in the ACSE_AARQ must be valid here. For successful authentication, the corresponding license must be installed in the CAP.

CTI client licensing

The SCCP stores the "Application ID" transmitted in the ACSE_AARQ and uses it later for CTI client licensing of CSTA requests (using the telephone number in canonical format). The SCCP sends a corresponding HTTP request (`http://<fqdn>:8170/mgmnt/admin/req?registerLicense= <ApplicationID>&userId=<DeviceID>`) to CAP License Management. If the license check was successful, the SCCP saves this information for 3600 seconds.

9.2.3 Testing the CAP "multi domain harmonized mode" for the CSTA III ASN.1 configuration

CSTA III ASN.1 test program

To test this configuration, use the program `CAPHost.exe`.

The connection destination that is configured is the CAP SCCP IP address and the CAP SCCP port.

In the ACSE_AARQ, "Native = false" is sent and dropped because the default is "Native = false." Different PBX types can only be tested during a connection session in "harmonized mode".

SCCP status

Without an application connection, the SCCP status is "running".

SCC status

Without an application connection, the SCC status is "running".

Application login (ACSE_AARQ)

An application must authenticate itself with a CAP CTI or Admin user (for example, CAP) and the associated password (for example, 123). CAP Management carries out this authentication via the SCCP. The CSTA version (version five) is also indicated.

Application ID

The application ID is passed in the ACSE_AARQ.

Native mode = true/false

It is not necessary to mark native mode explicitly because "Native = false" is the default.

Extensions

Extensions are addressed via their long call numbers if none of the corresponding requests contains an additional reference ID (for example, Call ID).

Call ID

The "Call ID" is a maximum of nine bytes long.

9.2.4 JTAPI

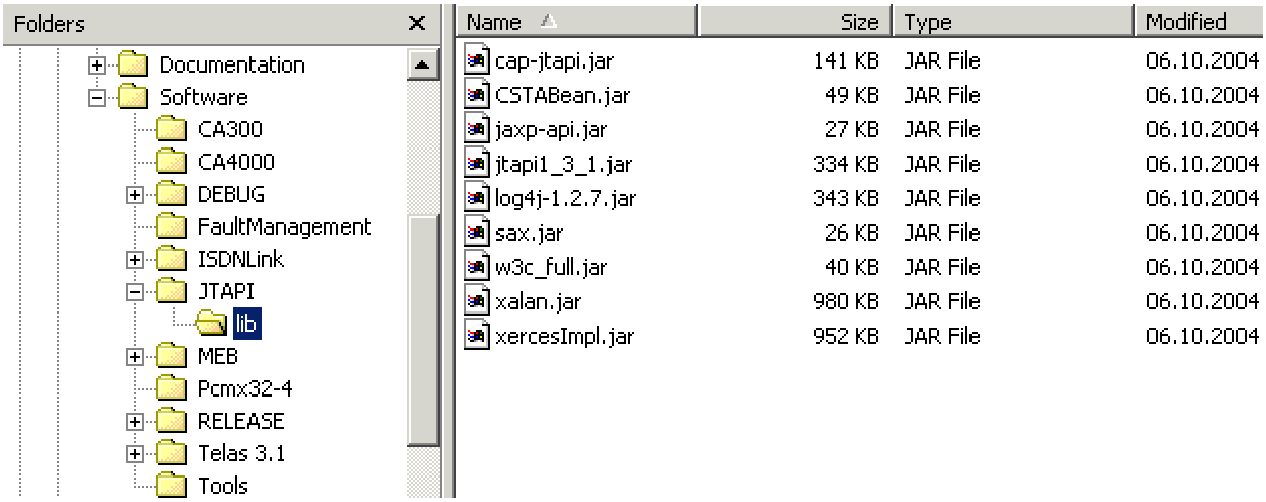
The JTAPI protocol is only supported in "multi domain harmonized mode".

OpenScape CAP V3.0 provides the corresponding Java classes.

The advantage of JTAPI/JATPI is that it is independent of the operating system.

Communication with an SCCP takes place via CSTA XML.

The Java classes are located on the OpenScape CAP V3.0 CD in the directory `Software\JTAPI\lib`.

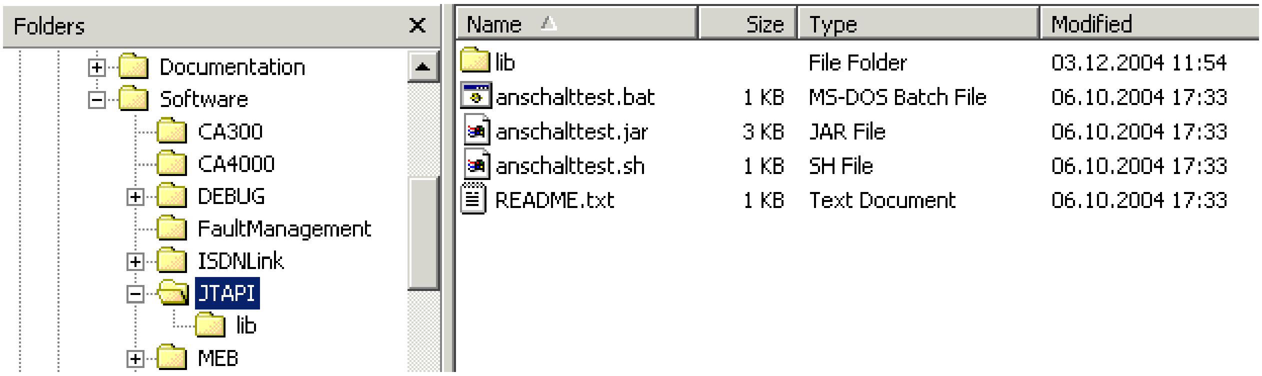


Name	Size	Type	Modified
cap-jtapi.jar	141 KB	JAR File	06.10.2004
CSTABean.jar	49 KB	JAR File	06.10.2004
jaxp-api.jar	27 KB	JAR File	06.10.2004
jtapi1_3_1.jar	334 KB	JAR File	06.10.2004
log4j-1.2.7.jar	343 KB	JAR File	06.10.2004
sax.jar	26 KB	JAR File	06.10.2004
w3c_full.jar	40 KB	JAR File	06.10.2004
xalan.jar	980 KB	JAR File	06.10.2004
xercesImpl.jar	952 KB	JAR File	06.10.2004

9.2.4.1 JTAPI test

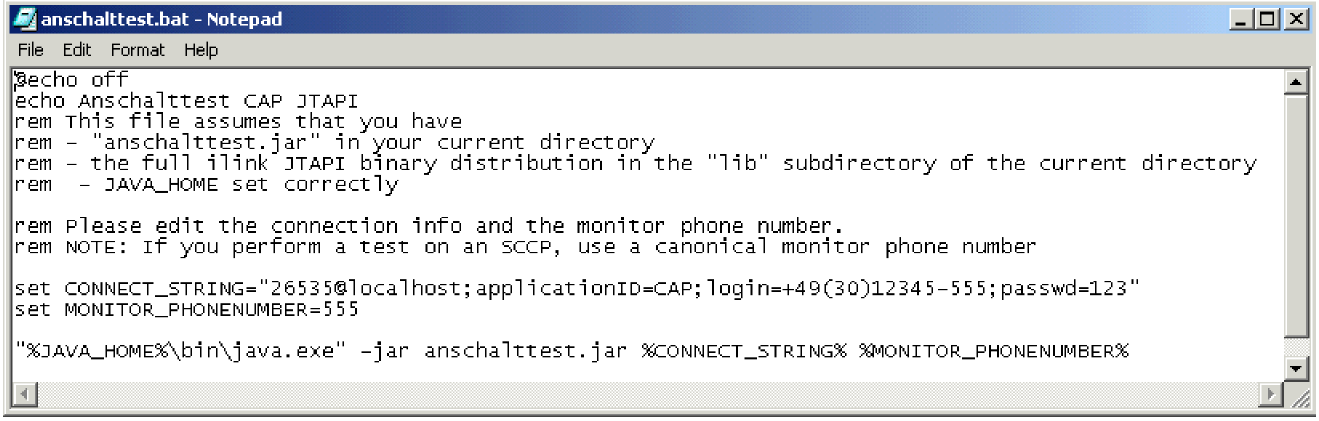
"Java Runtime Environments 1.3.1" or later must be installed to test JTAPI.

The `anschalttest.bat` test program is located on the OpenScape CAP V3.0 CD in the directory `Software\JTAPI`.



Name	Size	Type	Modified
lib		File Folder	03.12.2004 11:54
anschalttest.bat	1 KB	MS-DOS Batch File	06.10.2004 17:33
anschalttest.jar	3 KB	JAR File	06.10.2004 17:33
anschalttest.sh	1 KB	SH File	06.10.2004 17:33
README.txt	1 KB	Text Document	06.10.2004 17:33

The file contents must be adapted as appropriate during installation.



```
@echo off
echo Anschalttest CAP JTAPI
rem This file assumes that you have
rem - "anschalttest.jar" in your current directory
rem - the full ilink JTAPI binary distribution in the "lib" subdirectory of the current directory
rem  - JAVA_HOME set correctly

rem Please edit the connection info and the monitor phone number.
rem NOTE: If you perform a test on an SCCP, use a canonical monitor phone number

set CONNECT_STRING="26535@localhost;applicationID=CAP;login=+49(30)12345-555;passwd=123"
set MONITOR_PHONENUMBER=555

"%JAVA_HOME%\bin\java.exe" -jar anschalttest.jar %CONNECT_STRING% %MONITOR_PHONENUMBER%
```

`26535@localhost`

Input of the port number and IP address (or PC name) on which the SCCP is running.

`applicationID=CAP`

Input of the "Application ID". It must correspond to a license that has been installed.

`login=+49(30)12345-555`

Input of the CAP CTI or admin user for application authentication.

`MONITOR_PHONENUMBER=555`

Input of the call number in canonical format (for example, +49(5251)2421-27486) for checking the "MonitorStart" feature.

`%JAVA_HOME%`

The variable that is set to the Java installation directory. If this variable is not set, this variable must be replaced (for example, C:\Program Files\Java\j2re1.4.2_06\).

Starting the batch file `anschalttest.bat`

1. Copy the "\Software\JTAPI\lib" directory which contains the CAP Java classes to any directory (for example, C:\temp\) on the hard disk and modify the contents of the file according to your configuration.
2. Open a CMD window
3. Change to the chosen directory (for example, C:\temp\) and start the batch file "anschalttest.bat". An attempt is now made to set a monitor point on this device. If this is not possible, the corresponding error messages are output in the CMD window.

9.2.5 TAPI

The OpenScape CAP TAPI Service Provider (CAP TCSP) can be used by all Windows TAPI-based programs.

9.2.5.1 Licensing

With the first NetTSPI request, the SCC contacts CAP License Management and asks whether the corresponding "ApplicationID" is assigned to the CTI user as a license. If license assignment in "At user login" (default) mode is active, a license is always assigned. If a license was successfully checked for a user, the SCC saves this information for 3600 seconds. Likewise, this information is deleted when the SCC restarts.

Standard TAPI applications do not use any individual "Application ID" and are licensed by an SCC using an internal routine.

After receiving the first CAP TCSP NetTSPI request, the addressed SCC starts the license check for a CTI user in the following order:

1. CAP-A
2. CAP-S
3. CAP-E

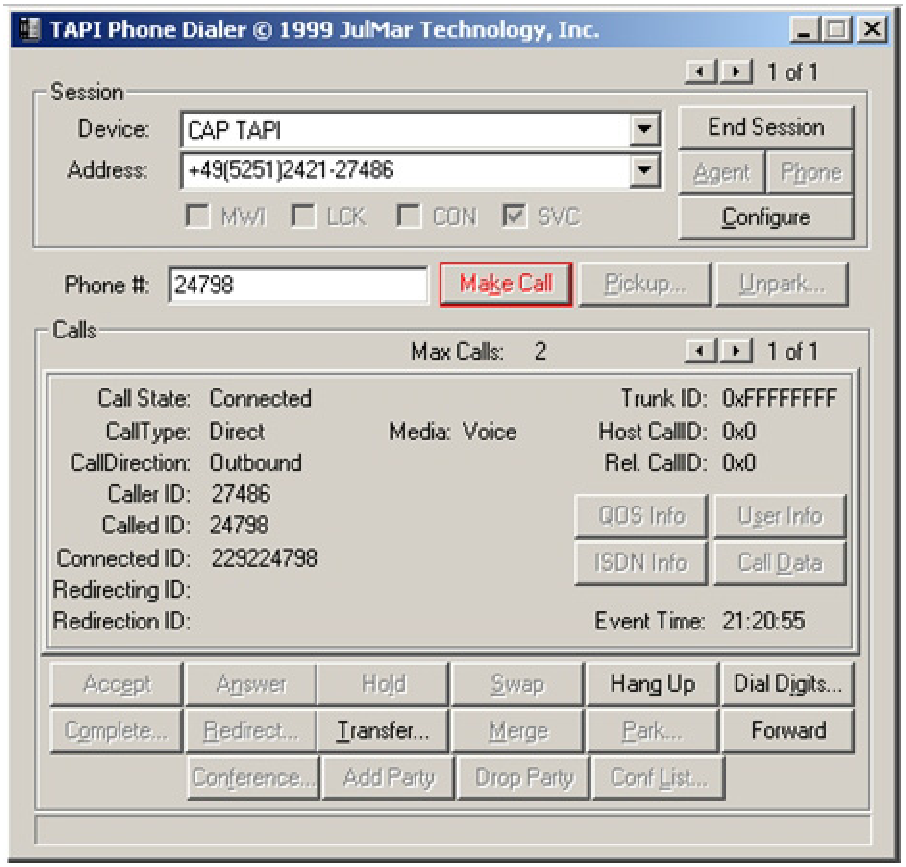
The connection to the CAP TCSP is interrupted if none of the requested licenses has been assigned. The CAP TCSP reacts by displaying an error message on the monitor.

New TAPI applications (such as xPhone) use an individual "Application ID" by setting a parameter in the "LineDevSpecificFeature".

9.2.5.2 TAPI test

TAPI test program `Phone.exe`

Each Windows TAPI-based program (Outlook, Phone Dialer) can be used to test the configuration for the TAPI. You must make sure that the Windows TAPI server automatically sets a monitor point on the device that does not actually support the "CAP-E" license as soon as the line is opened. Only later does the "CAP-E" license prevent an event from spreading from the Windows TAPI server to the TAPI application.



TAPI Phone Dialer © 1999 JulMar Technology, Inc.

Session

Device: CAP TAPI

Address: +49(5251)2421-27486

□ MWI □ LCK □ CON ☑ SVC

Phone #: 24798

Calls

Max Calls: 2

Call State: Connected
CallType: Direct
CallDirection: Outbound
Caller ID: 27486
Called ID: 24798
Connected ID: 229224798
Redirecting ID:
Redirection ID:

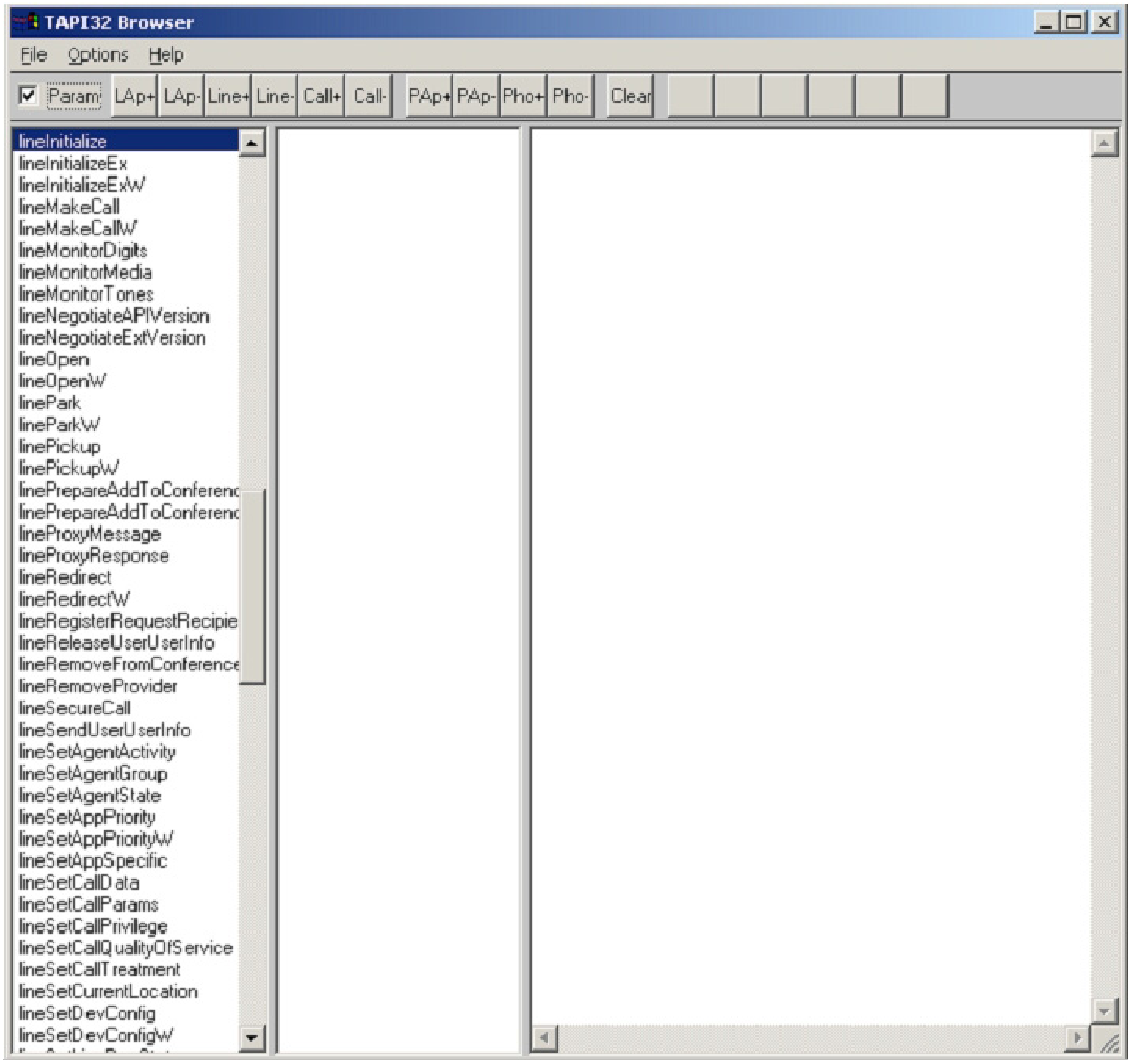
Media: Voice

Trunk ID: 0xFFFFFFFF
Host CallID: 0x0
Rel. CallID: 0x0

Event Time: 21:20:55

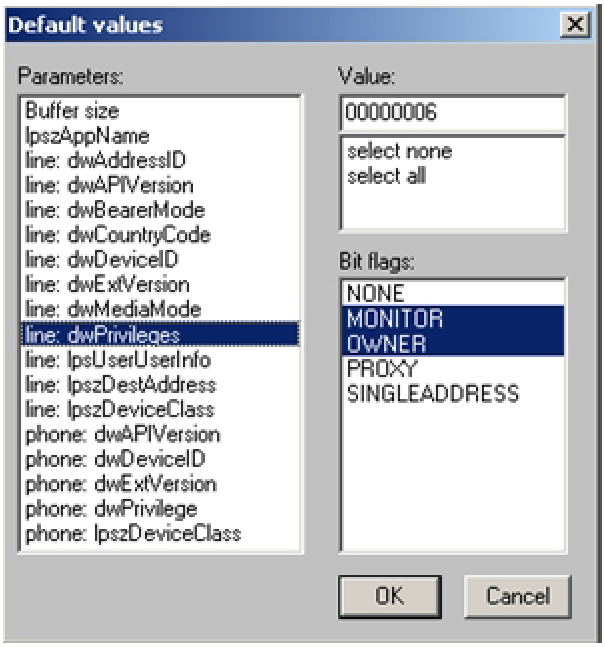
TAPI test program `tb20.exe`

With the TAPI test program `tb20.exe`, you can configure basic TAPI requests. For any request, all available parameters can be set.



First select "**Options - Default values**".

Set **line dwPrivileges** to **Monitor** and **Owner**.



Parameters:

Buffer size
lpszAppName
line: dwAddressID
line: dwAPIVersion
line: dwBearerMode
line: dwCountryCode
line: dwDeviceID
line: dwExtVersion
line: dwMediaMode
line: dwPrivileges
line: lpsUserUserInfo
line: lpszDestAddress
line: lpszDeviceClass
phone: dwAPIVersion
phone: dwDeviceID
phone: dwExtVersion
phone: dwPrivilege
phone: lpszDeviceClass

Value: 00000006

select none
select all

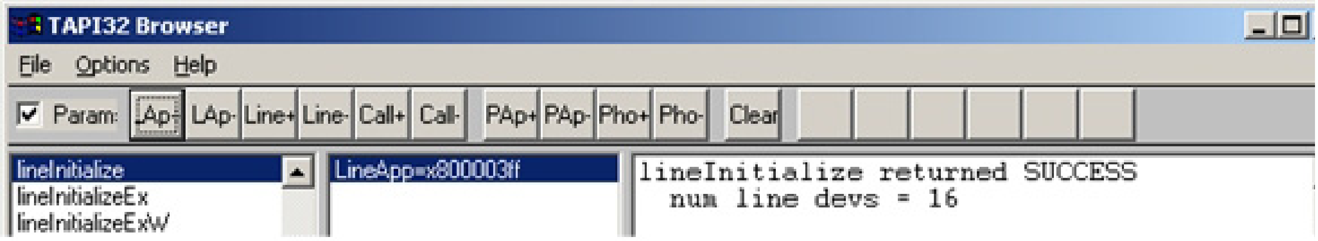
Bit flags:

NONE
MONITOR
OWNER
PROXY
SINGLEADDRESS

Establishing the link to the Windows TAPI server

```
"lineInitialize"
```

In response, you get the **LineApp** handler and the number of available line devices (provided by all installed TAPI service providers).



lineInitialize
lineInitializeEx
lineInitializeExW

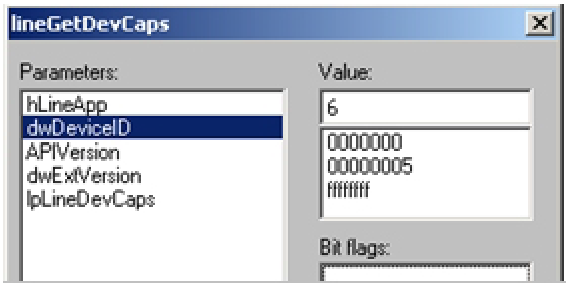
LineApp=x800003ff

```
lineInitialize returned SUCCESS
  num line devs = 16
```

Finding a suitable TAPI line device

```
"lineGetDevCaps"
```

Enter the device IDs (one after the other) to find the related line devices.



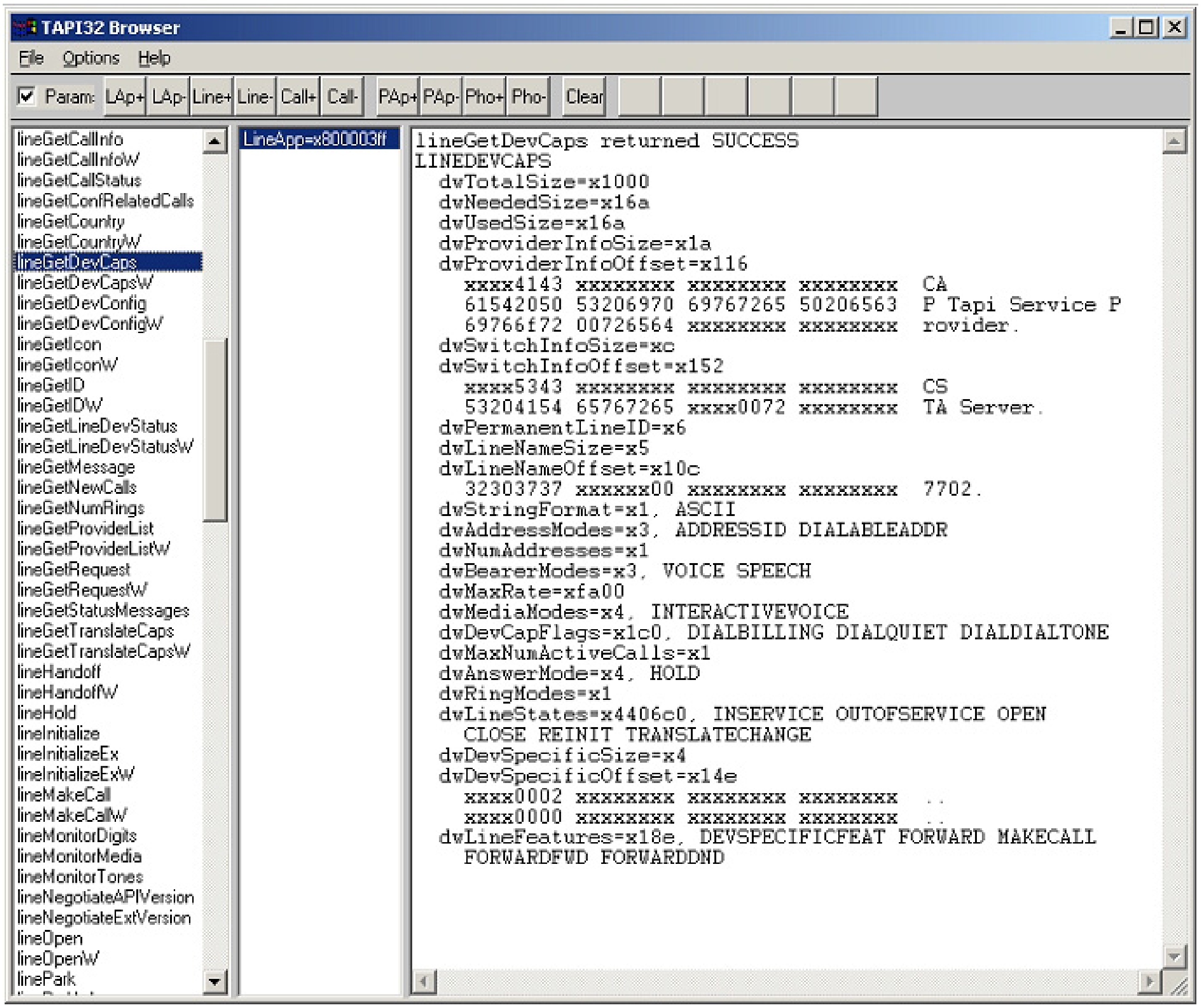
Parameters:

- hLineApp
- dwDeviceID
- APIVersion
- dwExtVersion
- lpLineDevCaps

Value: 6

```
0000000
00000005
ffffffff
```

In response, you get detailed information about every available line device.



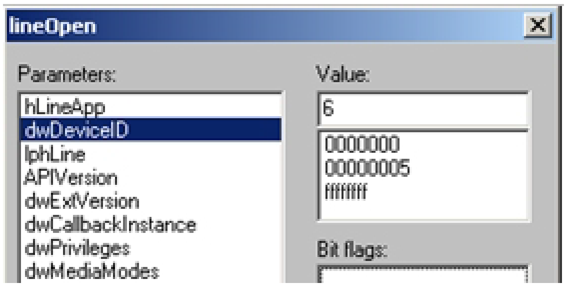
☑ Param:

```
lineGetDevCaps returned SUCCESS
LINEDEVCAPS
  dwTotalSize=x1000
  dwNeededSize=x16a
  dwUsedSize=x16a
  dwProviderInfoSize=x1a
  dwProviderInfoOffset=x116
    xxxx4143 xxxxxxxx xxxxxxxx xxxxxxxx  CA
    61542050 53206970 69767265 50206563  P Tapi Service P
    69766f72 00726564 xxxxxxxx xxxxxxxx  rovider.
  dwSwitchInfoSize=xc
  dwSwitchInfoOffset=x152
    xxxx5343 xxxxxxxx xxxxxxxx xxxxxxxx  CS
    53204154 65767265 xxxx0072 xxxxxxxx  TA Server.
  dwPermanentLineID=x6
  dwLineNameSize=x5
  dwLineNameOffset=x10c
    32303737 xxxxxx00 xxxxxxxx xxxxxxxx  7702.
  dwStringFormat=x1, ASCII
  dwAddressModes=x3, ADDRESSID DIALABLEADDR
  dwNumAddresses=x1
  dwBearerModes=x3, VOICE SPEECH
  dwMaxRate=xfa00
  dwMediaModes=x4, INTERACTIVEVOICE
  dwDevCapFlags=x1c0, DIALBILLING DIALQUIET DIALDIALTONE
  dwMaxNumActiveCalls=x1
  dwAnswerMode=x4, HOLD
  dwRingModes=x1
  dwLineStates=x4406c0, INSERVICE OUTOFSERVICE OPEN
    CLOSE REINIT TRANSLATECHANGE
  dwDevSpecificSize=x4
  dwDevSpecificOffset=x14e
    xxxx0002 xxxxxxxx xxxxxxxx xxxxxxxx  ..
    xxxx0000 xxxxxxxx xxxxxxxx xxxxxxxx  ..
  dwLineFeatures=x18e, DEVSPECIFICFEAT FORWARD MAKECALL
    FORWARDFWD FORWARDDND
```

Opening a TAPI line device

"lineOpen"

Enter the line device’s ID.

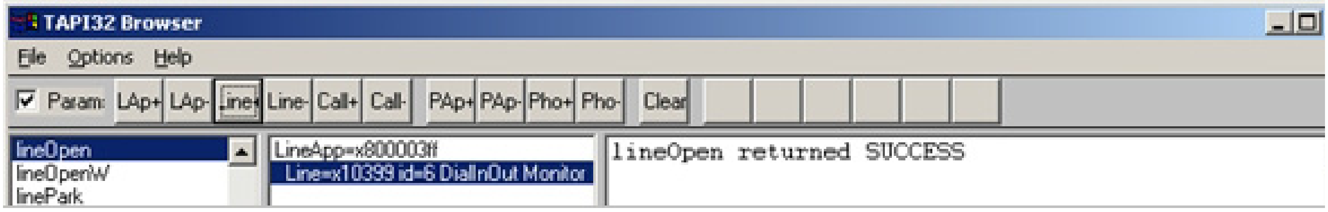


hLineApp
dwDeviceID
lphLine
APIVersion
dwExtVersion
dwCallbackInstance
dwPrivileges
dwMediaModes

6

0000000
00000005
ffffffff

In response, you get information about the line session ID.



lineOpen
lineOpenW
linePark

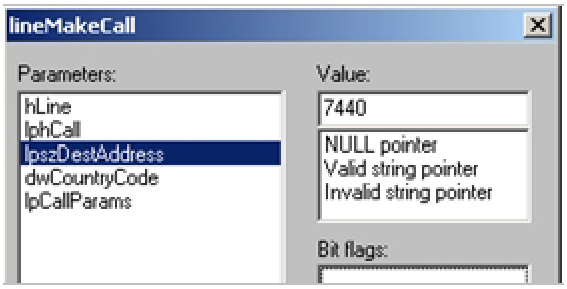
LineApp=x800003ff
Line=x10399 id=6 DialInOut Monitor

```
lineOpen returned SUCCESS
```

Making a call

"lineMakeCall"

Enter the destination number at **IpszDestAddress**.

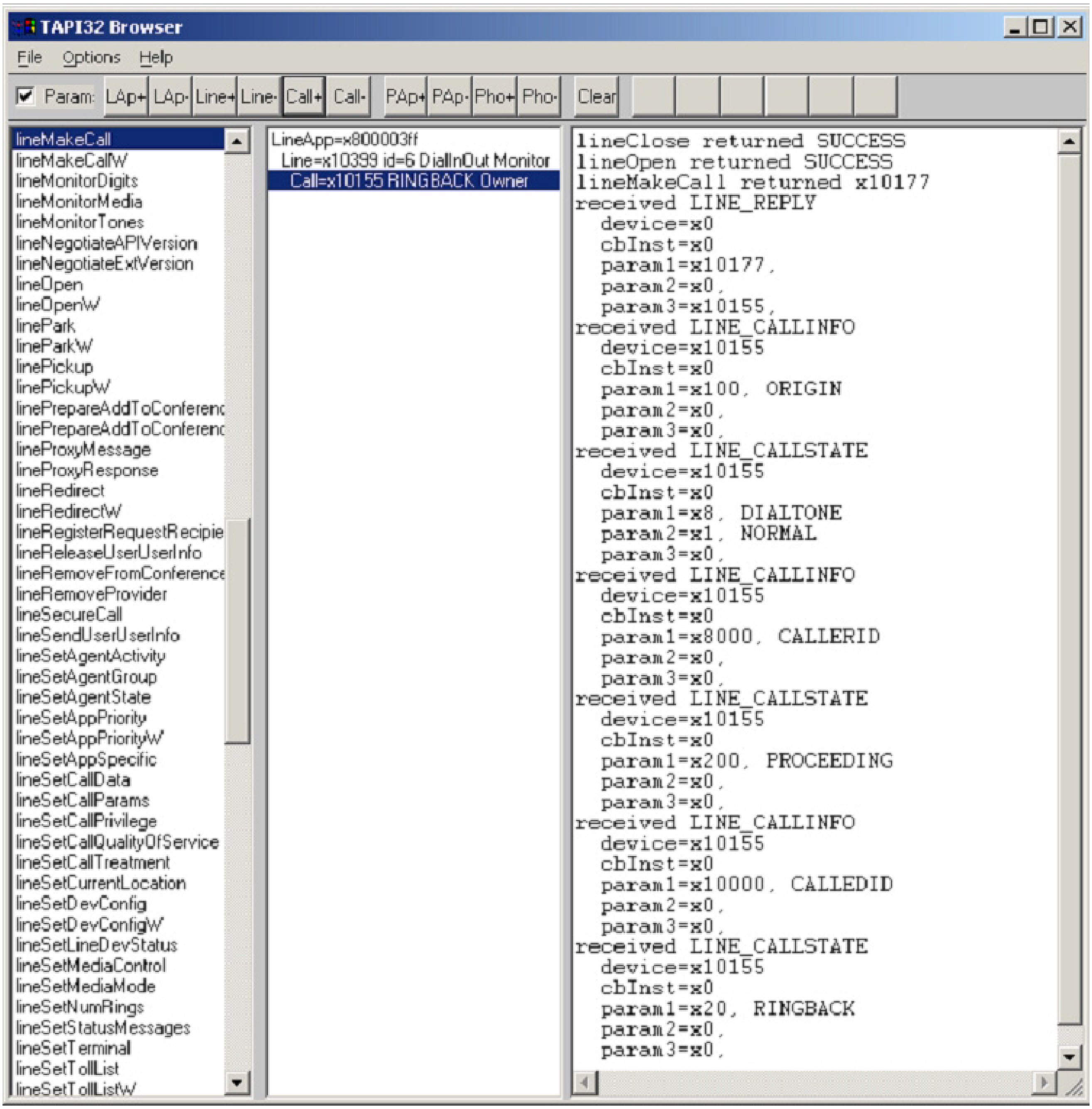


hLine
lphCall
lpszDestAddress
dwCountryCode
lpCallParams

7440

NULL pointer
Valid string pointer
Invalid string pointer

In response, you get information about the call ID.



```
lineMakeCall
lineMakeCallW
lineMonitorDigits
lineMonitorMedia
lineMonitorTones
lineNegotiateAPIVersion
lineNegotiateExtVersion
lineOpen
lineOpenW
linePark
lineParkW
linePickup
linePickupW
linePrepareAddToConferenc
linePrepareAddToConferenc
lineProxyMessage
lineProxyResponse
lineRedirect
lineRedirectW
lineRegisterRequestRecipie
lineReleaseUserUserInfo
lineRemoveFromConference
lineRemoveProvider
lineSecureCall
lineSendUserUserInfo
lineSetAgentActivity
lineSetAgentGroup
lineSetAgentState
lineSetAppPriority
lineSetAppPriorityW
lineSetAppSpecific
lineSetCallData
lineSetCallParams
lineSetCallPrivilege
lineSetCallQualityOfService
lineSetCallTreatment
lineSetCurrentLocation
lineSetDevConfig
lineSetDevConfigW
lineSetLineDevStatus
lineSetMediaControl
lineSetMediaMode
lineSetNumRings
lineSetStatusMessages
lineSetTerminal
lineSetTollList
lineSetTollListW
```

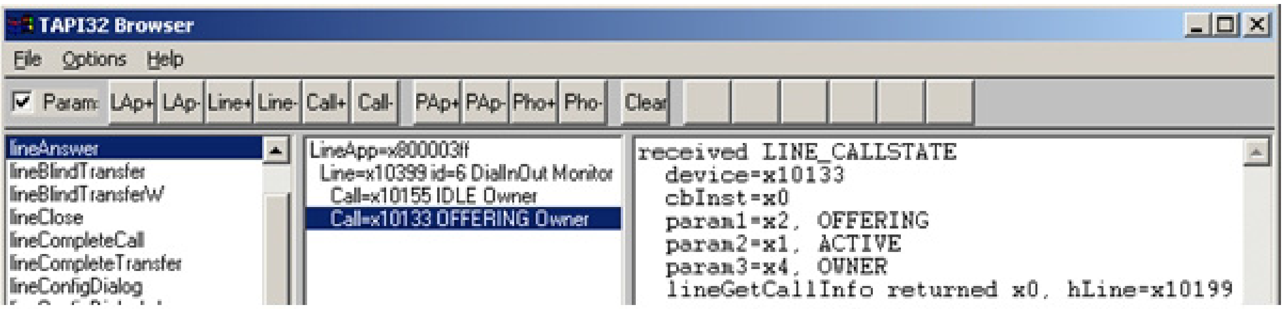
```
LineApp=x800003ff
  Line=x10399 id=6 DialInOut Monitor
    Call=x10155 RINGBACK Owner
```

```
lineClose returned SUCCESS
lineOpen returned SUCCESS
lineMakeCall returned x10177
received LINE_REPLY
  device=x0
  cbInst=x0
  param1=x10177,
  param2=x0,
  param3=x10155,
received LINE_CALLINFO
  device=x10155
  cbInst=x0
  param1=x100, ORIGIN
  param2=x0,
  param3=x0,
received LINE_CALLSTATE
  device=x10155
  cbInst=x0
  param1=x8, DIALTONE
  param2=x1, NORMAL
  param3=x0,
received LINE_CALLINFO
  device=x10155
  cbInst=x0
  param1=x8000, CALLERID
  param2=x0,
  param3=x0,
received LINE_CALLSTATE
  device=x10155
  cbInst=x0
  param1=x200, PROCEEDING
  param2=x0,
  param3=x0,
received LINE_CALLINFO
  device=x10155
  cbInst=x0
  param1=x10000, CALLEDID
  param2=x0,
  param3=x0,
received LINE_CALLSTATE
  device=x10155
  cbInst=x0
  param1=x20, RINGBACK
  param2=x0,
  param3=x0,
```

Answering a call

`"lineAnswer"`

An incoming call is offered to the line owner.

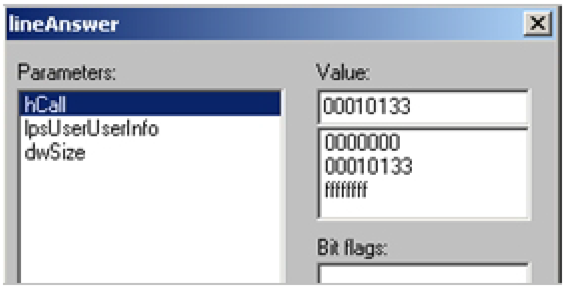

TAPI32 Browser
File Options Help
☑ Param: LAp+ LAp- Line+ Line- Call+ Call- PAp+ PAp- Pho+ Pho- Clear

```
lineAnswer
lineBlindTransfer
lineBlindTransferW
lineClose
lineCompleteCall
lineCompleteTransfer
lineConfigDialog
```

```
LineApp=x800003ff
  Line=x10399 id=6 DialInOut Monitor
    Call=x10155 IDLE Owner
    Call=x10133 OFFERING Owner
```

```
received LINE_CALLSTATE
  device=x10133
  cbInst=x0
  param1=x2, OFFERING
  param2=x1, ACTIVE
  param3=x4, OWNER
  lineGetCallInfo returned x0, hLine=x10199
```

Enter the **hcall** number of the offered call.



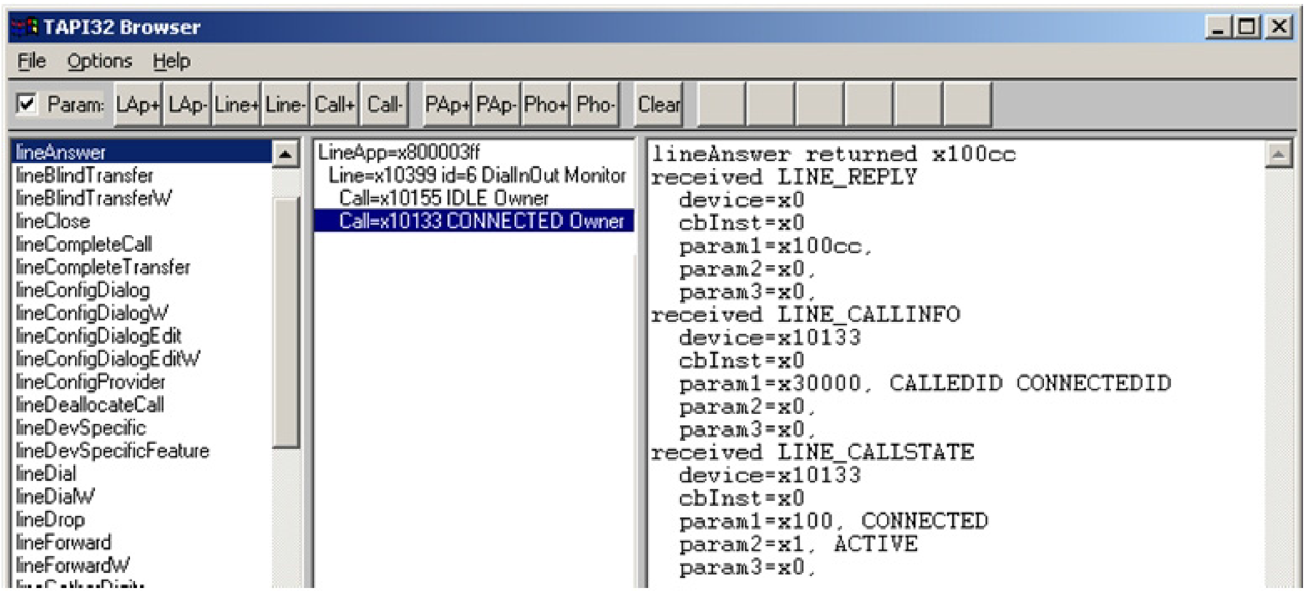
Parameters:

```
hCall
lpsUserUserInfo
dwSize
```

Value: 00010133

```
0000000
00010133
ffffffff
```

In response, you get information about the connected call.


TAPI32 Browser
File Options Help
☑ Param: LAp+ LAp- Line+ Line- Call+ Call- PAp+ PAp- Pho+ Pho- Clear

```
lineAnswer
lineBlindTransfer
lineBlindTransferW
lineClose
lineCompleteCall
lineCompleteTransfer
lineConfigDialog
lineConfigDialogW
lineConfigDialogEdit
lineConfigDialogEditW
lineConfigProvider
lineDeallocateCall
lineDevSpecific
lineDevSpecificFeature
lineDial
lineDialW
lineDrop
lineForward
lineForwardW
```

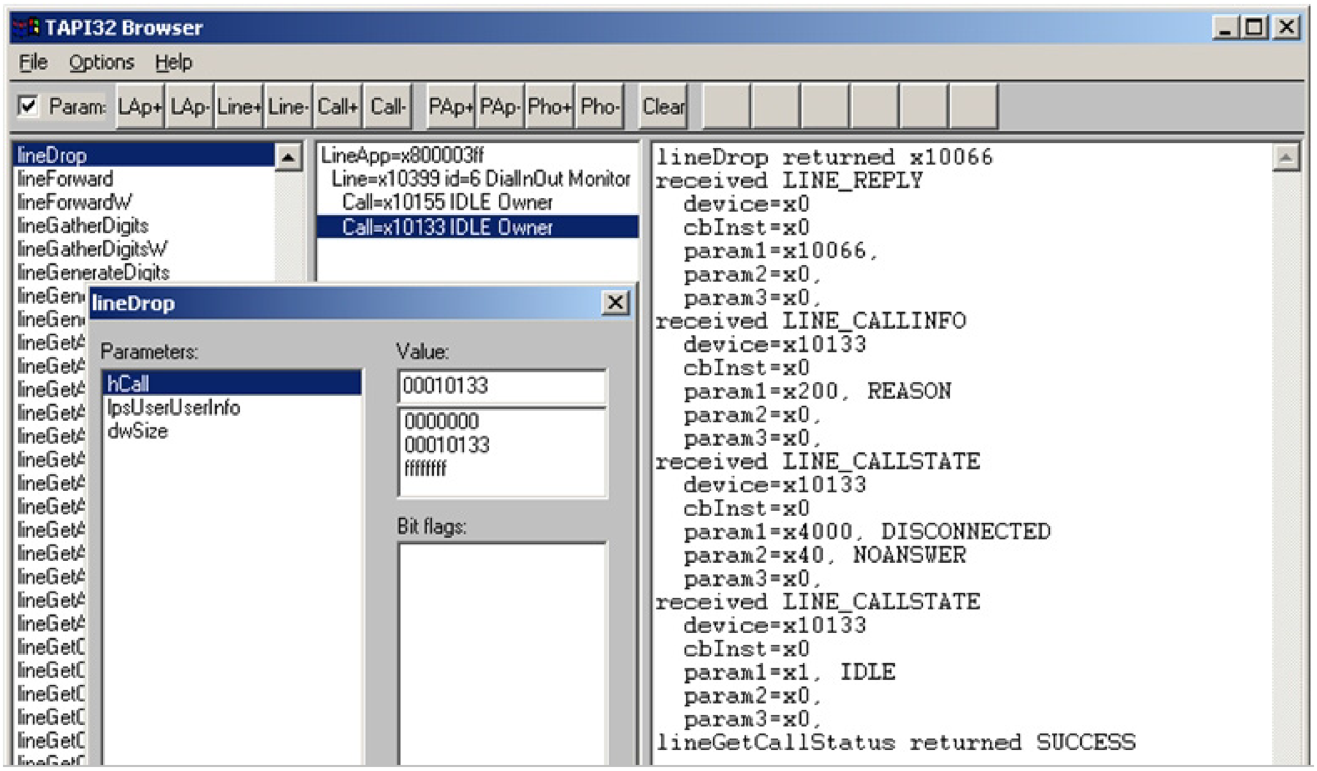
```
LineApp=x800003ff
  Line=x10399 id=6 DialInOut Monitor
    Call=x10155 IDLE Owner
    Call=x10133 CONNECTED Owner
```

```
lineAnswer returned x100cc
received LINE_REPLY
  device=x0
  cbInst=x0
  param1=x100cc,
  param2=x0,
  param3=x0,
received LINE_CALLINFO
  device=x10133
  cbInst=x0
  param1=x30000, CALLEDID CONNECTEDID
  param2=x0,
  param3=x0,
received LINE_CALLSTATE
  device=x10133
  cbInst=x0
  param1=x100, CONNECTED
  param2=x1, ACTIVE
  param3=x0,
```

Hanging up a call

```
"lineDrop"
```

Enter the **hcall** number of the connected call.



Value: 00010133

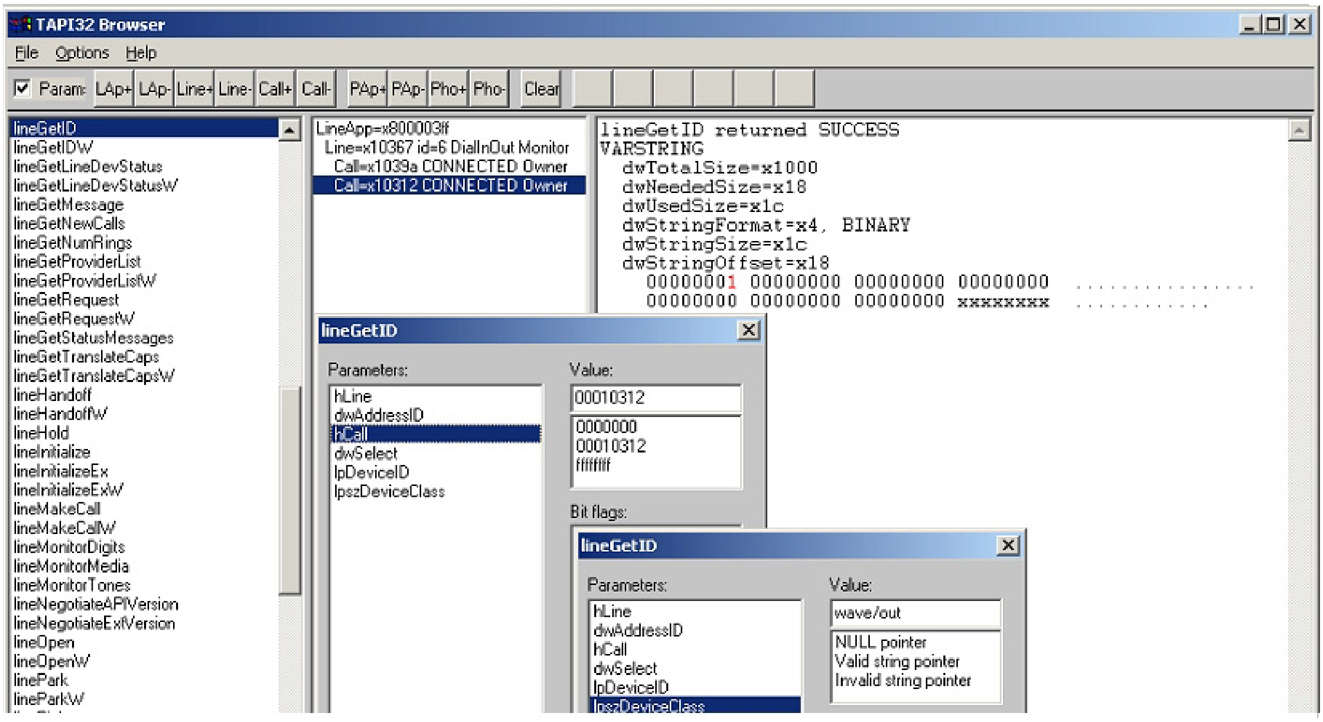
0000000
00010133
ffffffff

```
lineDrop returned x10066
received LINE_REPLY
  device=x0
  cbInst=x0
  param1=x10066,
  param2=x0,
  param3=x0,
received LINE_CALLINFO
  device=x10133
  cbInst=x0
  param1=x200, REASON
  param2=x0,
  param3=x0,
received LINE_CALLSTATE
  device=x10133
  cbInst=x0
  param1=x4000, DISCONNECTED
  param2=x40, NOANSWER
  param3=x0,
received LINE_CALLSTATE
  device=x10133
  cbInst=x0
  param1=x1, IDLE
  param2=x0,
  param3=x0,
lineGetCallStatus returned SUCCESS
```

Getting media device ID

`"lineGetID"`

Enter the **hcall** number of the connected call and **wave/out** or **wave/in** for **IpzDeviceClass**.



```
LineApp=x800003ff
  Line=x10367 id=6 DialInOut Monitor
    Call=x1039a CONNECTED Owner
    Call=x10312 CONNECTED Owner
```

```
lineGetID returned SUCCESS
VARSTRING
  dwTotalSize=x1000
  dwNeededSize=x18
  dwUsedSize=x1c
  dwStringFormat=x4, BINARY
  dwStringSize=x1c
  dwStringOffset=x18
    00000001 00000000 00000000 00000000  ................
    00000000 00000000 00000000 xxxxxxxx  ............
```

lineGetID

Parameters: hLine, dwAddressID, hCall, dwSelect, lpDeviceID, lpszDeviceClass

Value: 00010312

0000000
00010312
ffffffff

Bit flags:

lineGetID

Parameters: hLine, dwAddressID, hCall, dwSelect, lpDeviceID, lpszDeviceClass

Value: wave/out

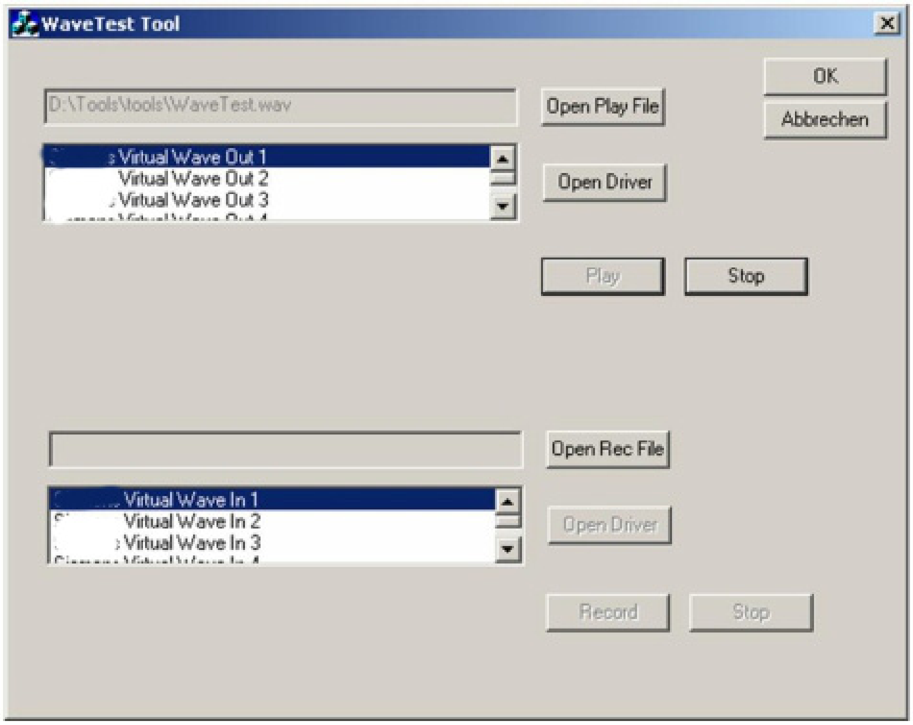
NULL pointer
Valid string pointer
Invalid string pointer

Playing a wave file with “WaveTest.exe”

Start program:

C:\<install_path>\bin\tools\WaveTest.exe

1. Open a wave file to be played.
2. Select the received “dvStringOffset” channel number (dvStringOffset 0 = channel 1, dvStringOffset 1 = channel 2,…).
3. Click “Open Driver”.
4. Play the wave file.
5. Click “Stop” once to pause, twice to stop.



9.2.6 XML Phone Service

The test application **"TEFEX"** for testing the XML Phone Service is automatically installed at the same time as the actual application. In conjunction with a HiPath 4000 telephone, it lets you test input and output functions and XMLPS signaling.

To perform a test, you must carry out the following steps:

1. Under "URL List for XML PhoneService", configure the URL **"http://localhost/tefex/tefex"** with the URL identifier "TEFEX".
2. Configure a name button on a device with the destination **"C13999xx"**, where "xx" stands for the button number.
3. Start the device configuration for this device and assign the URL of the "TEFEX" application to the button "xx" under "XML Phone settings".

Now you can test the configuration of the XML Phone Service.

9.2.6.1 TEFEX

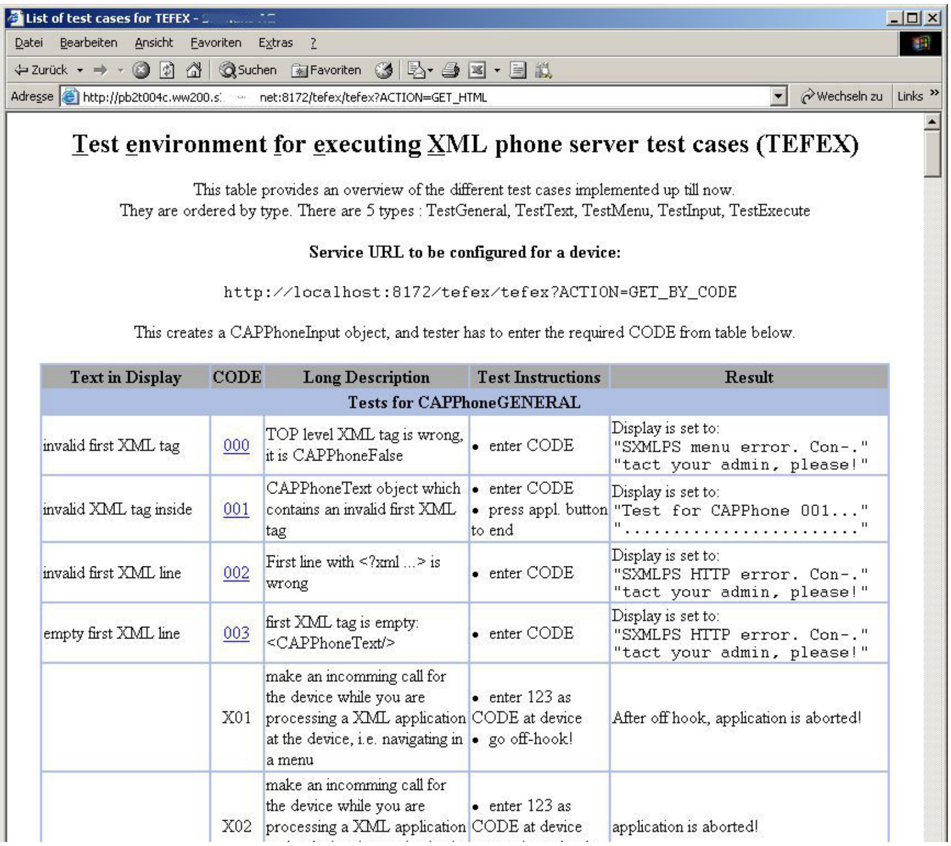
"TEFEX" is a test application that supports three different functions:

? telephone-based input by code,

? telephone-based input by type,

? "CAPPhoneEXECUTE" execution from a browser.

A complete description of all functions available is provided on the following html page: "**http://localhost:8172/tefex/tefex?ACTION=GET_HTML**".


List of test cases for TEFEX -
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten
Adresse http://pb2t004c.ww200.s net:8172/tefex/tefex?ACTION=GET_HTML
Wechseln zu Links

Test environment for executing XML phone server test cases (TEFEX)

This table provides an overview of the different test cases implemented up till now.
They are ordered by type. There are 5 types : TestGeneral, TestText, TestMenu, TestInput, TestExecute

Service URL to be configured for a device:

```
http://localhost:8172/tefex/tefex?ACTION=GET_BY_CODE
```

This creates a CAPPhoneInput object, and tester has to enter the required CODE from table below.

Text in Display	CODE	Long Description	Test Instructions	Result
		Tests for CAPPhoneGENERAL		
invalid first XML tag	000	TOP level XML tag is wrong, it is CAPPhoneFalse	• enter CODE	Display is set to: "SXMLPS menu error. Con-." "tact your admin, please!"
invalid XML tag inside	001	CAPPhoneText object which contains an invalid first XML tag	• enter CODE • press appl. button to end	Display is set to: "Test for CAPPhone 001..." "........................"
invalid first XML line	002	First line with <?xml ...> is wrong	• enter CODE	Display is set to: "SXMLPS HTTP error. Con-." "tact your admin, please!"
empty first XML line	003	first XML tag is empty: <CAPPhoneText/>	• enter CODE	Display is set to: "SXMLPS HTTP error. Con-." "tact your admin, please!"
	X01	make an incomming call for the device while you are processing a XML application at the device, i.e. navigating in a menu	• enter 123 as CODE at device • go off-hook!	After off hook, application is aborted!
	X02	make an incomming call for the device while you are processing a XML application	• enter 123 as CODE at device	application is aborted!

All test functions supported are divided into the following groups:

? Tests for CAPPhoneGENERAL

? Tests for CAPPhoneTEXT

? Tests for CAPPhoneMENU

? Tests for CAPPhoneINPUT

? Tests for CAPPhoneEXECUTE (can only be used from the browser)

All test functions supported are sorted according to:

? Text on the display (during the test: "get test by type"),

? Code (during the test: "get test by code"),

? Long description (detailed description),

? Test instructions (description of the inputs on the telephone or in the browser),

? Result (test result, what is really tested).

Telephone-based input by code (Test by Code)

The following messages appears on the telephone’s display when a TEFEX session is started and the test mode "get test by code" is selected:

Test Environment for CAP
CODE:

A code that is listed in the "CODE" column can now be entered. Whether further input is necessary on the device (Test Instructions) depends on the code that is entered. If the test is successful, the messages in the Result column (Display is set to:) should be displayed on the device display according to the code.
If you are working in a browser and you click a code, the browser will display the XML message that is sent from TEFEX to the XMLPS during a test for this code.

Telephone-based input by type (Test by Type)

Another menu appears on the telephone’s display when a TEFEX session is started and the test mode "get test by type" is selected:

Test Environment for CAP
Test for CAPPhone:

You can now browse this menu with "**<**" and "**>**" and select the following type groups with the "**OK**" button:

? Test for CAPPhone Text:

? Test for CAPPhone Menu:

? Test for CAPPhone Input:

? Test for CAPPhone Exec: (although this is offered here, this test is **not supported** when operating from a telephone)

Select a test group.

The text from the "Text in Display" column is now offered to you in menu form, step by step, according to the selected test group. To select a test, press the "OK" button. Whether further input is necessary on the device (Test Instructions) depends on the test that is selected. If the test is successful, the message in the Result column (Display is set to:) should be displayed on the device display according to the test call.
If you are working in a browser and you click a code, the browser will display the XML message that is sent from TEFEX to the XMLPS during a test for this code.

Executing "CAPPhoneEXECUTE" from a browser

A new html page is shown if you click a CODE from the "Test for CAPPhoneExecute" group (for example, CODE 404) on the TEFEX html page.

In the XML string, change the value for the <phone> tag and enter the device ID of the device that is being used for this test. Now press the **Send to Invoke Interface Servlet** button. If the test is successful, the message in the Result column (Display is set to:) should be displayed on the device display according to the test call.

A Implementation details

A.1 Installation structure

A.1.1 Configuration files

During installation, the configuration files for all OpenScape CTI components are saved in different subdirectories of the `<InstDir>` installation directory.

When installing OpenScape CAP Management, the directory structure is set up as follows. Individual directories are gradually filled with the installation and configuration data for other components.

```
<InstDir>\config\

   common\

      cap.cfg
      global.cfg
      http-server.zip
      ports.cfg
      proc.cfg
      ROOT.war

   start\

      StartNT.cfg

   <hostI>\

      start\
         JStarter.cfg

      <process1>\
         S<x>service_ctrl.proc
         <service1>\
            S<x><service1>.svc
            <service1>.cfg
            http-server.props
         ...
         <serviceN>\
            S<x><serviceN>.svc
            <serviceN>.cfg
            http-server.props

      ...

      <processN>\
        ...
```

? <InstDir>\config\common\
This contains important configuration files for all OpenScape CTI components.

? <InstDir>\config\start\
This contains the configuration file for the start service used to start the entire system.

? <InstDir>\config\localhost\
All configurations for the processes and services which are to run on the installation host are saved here. The content of this directory plays a significant role in the network distribution of the system.

? <InstDir>\config\<host>\
A directory like this is created for every host configured in the system and is named according to the host name (without domain extension). This directory contains all information and configuration data for the processes and services which should run on this host. In the case of a standard installation, exactly one directory of this type is provided (for the local host).

? <InstDir>\config\<hostI>\<processN>\
A directory of this type is provided for each process which should run on <hostI> . This directory always contains a file S<x>service_ctrl.proc, which contains the information on how the process should be started. The name prefix S<x> is used to determine the process start sequence. <x> stands for a number (e.g. S47service_ctrl.proc. This process is started by the system before S49service_ctrl.proc). The file name therefore defines the process start sequence.
If several services are to run as threads within a process, a separate subdirectory is created for each service with the service name <serviceN>. If only one service is running in a process, a subdirectory is not provided.

? <InstDir>\config\<hostI>\<processN>\<serviceN>\
This directory exists for every service thread within a process. This directory always contains a file named S<x><serviceN>.svc containing the information on how the service is to be started. The process start sequence is defined based on the file name. The subdirectory also contains all configuration files specific to the service. If the service is a servlet engine, the configuration file http-server.props must also be provided.

? <InstDir>\data\TelasAdmin\
This is where OpenScape CAP Management stores the data for Security Service, Administration Service and the Import tool.

This flexible architecture enables system processes to be easily distributed across several hosts. A new <hostl> directory is automatically created on the master server for each new computer node when configuring a distributed component for a computer. The process subdirectories that are to run on <hostI> are then transferred to this directory.

The **Service Starter** must now be installed on `<hostI>`. When started for the first time, this automatically obtains the required data and processes from the master server (see also Section 4.7, "Distributed installation").

A.1.2 Program files

During installation, the program files, together with the Java class libraries, batch files and DLLs belonging to the product, are stored in subdirectories of the *<InstDir>\distribution* directory.

During startup, these components are copied to the directories *<InstDir>*`\bin`, *<InstDir>*`\bin\tools` and `<InstDir>\lib`. A check is performed in this case to determine whether or not a copy is needed. A copy is always needed when the components from *<InstDir>*`\distribution` are from different versions.

? `<InstDir>\bin`
This contains the `jsstart.exe` program (Start service for WinNT) and the `tools` subdirectory contains various batch files for data import and for starting individual system components.

? `<InstDir>\jre`
This contains the Java runtime system.

? `<InstDir>\lib`
This contains the Java class libraries for the product.

A.1.3 Log files

Log files are created in the directory *<InstDir>*`\Logs` during operation and filled with information, errors and states of Telas components in accordance with the set logging level. There is always a subdirectory here named after the CAP Management PC. In the case of distributed installation, PC name directories are created for all PCs. Every directory contains all log files for the processes running on the host PC.

OpenScape CAP Management creates this directory during installation. It is used by all OpenScape CTI components.

A.1.4 Files for the user interface

All HTML pages belonging to the OpenScape CAP Management and Call Control Service are saved in the `<InstDir>\WebSpace`.

Every OpenScape CTI component creates a local subdirectory here, to which it then saves the non-language-specific HTML pages (`*.html`), while saving the language-specific header files (`*.h`) and program resource files (`*.properties`) to other subdirectories. These include the user interface and the installation and administration manuals.

The language-specific files are always located in a subdirectory called `lang.` The directories contained within this subdirectory are named according to the relevant language; OpenScape CAP Management is supplied in the language variants `de` (German) and `en` (English).

Since the various HTML pages are cross-referenced, their layout can be changed, but they may not be renamed. You should note that any changes you make to the pages will be overwritten if you perform a new installation.

The `css` directory contains the styles used in all HTML pages. The `std_style.css` style file is used by default.

The `Plugin` directory contains the Java Runtime plugin (for the Web browsers Netscape Navigator/Communicator and Microsoft Internet Explorer) required for the diagnostics applet. To ensure that the plugin is available, this installation may have to be carried out before diagnostics are performed for the first time.

A.2 Description of the configuration files

OpenScape CAP management provides configuration files as described in Section A.1.1 in the `<InstDir>\config\` directory. The list below only includes those configuration files where important configuration changes can be made.

A.2.1 Configuration of Logging and Tracing

Several entries in different configuration files are put together to control the CAP logging / tracing facility. Subsequently, the important files affected are described and examples for reasonable settings are given.

1. The **`/config/common/global.cfg`** configuration file contains a number of commonly used configuration settings (cf. Section A.2.2), amongst others log / trace settings. As `global.cfg` is included in numerous other configuration files, modifications here implicitly will affect all dependant components.

   Relevant configuration settings:

   ```
   log.class        = com.xxxxxx.log.ClientLogger
   log.serverUrl    = lookup://LogServer
   log.level        = 3
   log.maxLines     = 2000
   log.maxFiles     = 3
   ```

   `log.class` and`log.serverUrl` must be left unchanged

   `log.level` defines the amount of logging / tracing (higher level -> more data)

   ```
   OFF       = -1
   FATAL     = 0
   ERROR     = 1
   WARNING   = 2
   MESSAGE   = 3
   TRACE     = 4
   DBG_TRACE = 5
   ```

   `log.maxlines` defines the maximum number of lines per LogFile

   `log.maxfiles` defines the maximum number of LogFiles to be created (cf. Section A.1.3); these are named following the scheme

   ```
   <name>.log
   <name>_last.log
   <name>_last1.log
   <name>_last2.log
   ...
   ```

The following settings are not present in the default version of the configuration file; they can be added if required:

`log.daily = <number>`
Number of days for which logging files are to be saved; one directory per day will be created in the `<INST_DR>/logs` directory
`log.daily = 0` means no day-based logging
`log.daily = 7` means logging for a total of seven days; older log files will be deleted

```
log.filter = <string>
log.filterModus = expand | exclusive
```

allow for selective logging according to specific filter criteria; events meeting the filter criteria always will be logged using the highest logging level 5. Please note that this facility is available for CAP Management loggers only.

Examples for application

```
log.filter = 51234
log.filterModus = expand
log.level = 3
```

Logging data are collected on level 3; additionally, information containing the string "51234" is logged on level 5.

```
log.filter = 722,89*4132
log.filterModus = exclusive
log.level = 3
```

Only information containg the strings "722" or "89" followed by an arbitrary string followed by "4132" is logged on level 5; setting log.level = 3 is irrelevant in this case.

All of the log settings apply to all loggers with the associated log files each. An overview of all active loggers is available in the DiagnoseAgent (Section 7.7.5) via Debug -> Show Logging. These include

- central loggers of the management framework like
  - start
  - admin
  - lookup
  - diag
- logger for services / SCC instances like
  - <SCC name>_Sys
  - <SCC name>_Error

  ? <SCC name>_CA4000_Sys   (for HiPath 4000 connectivity)

  ? <SCC name>_CA4000_Trace (for HiPath 4000 connectivity)

? loggers for additional services and applications like ComAssistant

Additionally, settings can be modified explicitly for single loggers. For that purpose, add the logger name to qualify the parameter, like

```
log.maxLines.admin          = 10000
log.maxFiles.admin          = 5
log.maxlines.<SCC name>_Sys = 20000
log.maxFiles.<SCC name>_Sys = 10
```

2. Please note that specific settings apply for the global **`errors.log`** which is used commonly by all components; these don’t follow the scheme described above. Instead, they are defined centrally in the `/config/<host>/admin/log/LogServer.cfg` configuration file:

```
include "/common/global.cfg"
errorsLog.file     = errors.log
errorsLog.maxLevel = 1
errorsLog.maxLines = 10000
errorsLog.maxFiles = 2
```

   You may modify `maxLines` and `maxFiles` here, as described above. Regularly this won’t be necessary.

3. For every Switch connectivity configured, an SCC instance is created coming with its **`telas.cfg`** configuration file:

```
include "/common/global.cfg"
log.class          = com.xxxxxx.log.ClientLogger
log.serverUrl      = lookup://LogServer
log.level          = 3
cstaLogEnabled     = 0
debugLevel         = 0
```

   `log.class` and `log.serverUrl` must be left unchanged

   `log.level` may be redefined here; it would override the value imported from `global.cfg`. In most cases this is not reasonable; instead, we recommend to have logLevel set in `global.cfg` identical for all components, have no logLevel entry in `telas.cfg`, but have service specific deviations set temporarily via the DiagnoseAgent.

   `cstaLogEnabled = 1` can be set to switch on tracing of the CSTA message traffic for this SCC instance on top of the normal logging; output goes to a `<SCC name>_CSTA.log` file; CSTA logging by default is switched off.

`debugLevel` allows for fine-tuning of an SCC specific trace to `<SCC name>_Error.log` on top of the normal logLevel. Values supported range from 0 (switched off - default setting) to 9 (maximum information).

As a new feature coming with CAP V3.0 SMR3, a specific logging facility for SCCs has been implemented that is controlled by additional entries in the telas.cfg config file. Logging outputs can be interpreted by CAP development only; this kind of logging should be activated according to development instructions only.

4. In addition to the settings described above controlled by configuration files, it is possible at any time to view current log settings via the **DiagnoseAgent** (Debug -> Show Logging). The logLevel can be changed here as well. For that, select the respective logger, choose a new logLevel and activate it by "SetLevel". Please note that a modification on this way will not make its way into any configuration file; it will be lost after restart of the system.

A.2.2 `global.cfg`

This file contains global settings for all process and service controllers in the entire system. The variables for the installation environment are predefined as appropriate during installation. This file must therefore not normally be changed.

Global variables and configuration parameters are set at the beginning of the file. These can then be used in all other configuration files. The installation routine enters the correct values automatically.

`INST_HOST`	Contains the host name in the user LAN without a domain suffix
`INST-IP`	Contains the host IP address in the user LAN (not for PBX connection)
`CONFIG_URL`	URL for the OpenScape CAP Management homepage
`CFG`	Path to the directory containing the configuration files

Subsequent variables are used to control logging. For additional details, please refer to Section A.2.1.

7 The `tomcat.log.level` setting (default setting -1 / switched off) is used to control Web server logging. Logging should only be enabled in special cases, as it is extremely detailed and can result in the generation of large data volumes.

`useDaylightTime = true`
This option controls automatic adjustment to daylight saving time. If you have enabled automatic adjustment in your operating system (default), this option must be set to `true` so that the times

used during logging, for example, correspond to the system clock. If this function is disabled in the operating system, this option must be set to `false`.
You can check the operating system settings with **Control Panel | Date/Time | Time Zone**

```
MaxCookieAge = 43200
```
Life of a cookie in **minutes**. The successful authentication of a CAP user for ComAssistant is saved in a cookie. When this timeout expires, the CAP user is forced to repeat the authentication procedure.

```
CustomizedPath =
```
If you want to use local HTML pages, you can specify a path to these files here. You will find more detailed information in the ComAssistant Installation and Administration Manual, "Customized HTML pages".

```
<?x set TelasWebName = "CAP" ?>
```
Definition of the CAP server name for unique identification in a notification mail.

```
<?x set MAIL_SERVER = "mail.org.de" ?>
```
SMTP mail server name entry. The name replaces "mail.org.de".

```
<?x set MAIL_SENDER = "<?x $TelasWebName ?> notifica-
tion<tws@mail.org.de>" ?>
```
Mail sender entry. The entry replaces "tws@mail.org.de".

```
<?x set MAIL_SYSADMIN = "sysadm@mail.org.de" ?>
```
Mail recipient entry. The entry replaces "sysadm@mail.org.de".

```
PasswordMode = ADMIN [ADMIN/AUTO]
```
`ADMIN =` ComAssistant users who forget their password must contact the CAP administrator to obtain a new password.
`AUTO =` ComAssistant users who forget their password can request a new password via e-mail. The CAP user must have been assigned an e-mail address on a specific LDAP server for this. The LDAP server is configured in the `admin.cfg` file.

A.2.3 `ports.cfg`

The ports for the HTTP and HTTPS connection to CAP Management and ComAssistant are defined in this file.

```
<?x set CAP_SSL_PASSWD = "changeit" ?>
```

The password that was assigned when generating the encryption file is defined here.

```
<?x set CAP_SSL_FILE = ".keystore" ?>
```

The name of the encryption file for CAP is defined here. The ".keystore" file with the password "changeit" already exists by default.

```
<?x set CAP_SEC_MODE   = "OFF" ?>
```

The secure connection to CAP Management is set up here (OFF/ON).

```
<?x set CAP_SEC_PORT   = "8470" ?>
```

The port for secure connection to CAP Management is defined here (default = 8470). This port is opened by the CAP’s Web server.

```
<?x set CAP_STD_PORT   = "8170" ?>
```

The port for normal connection to CAP Management is defined here (default = 8470). This port is opened by the CAP’s Web server.

```
<?x set SPW_SSL_PASSWD = "changeit" ?>
```

The name of the encryption file for CAP is defined here. The "`.keystore`" file with the password "`changeit`" already exists by default.

```
<?x set SPW_SSL_FILE   = ".keystore" ?>
```

The secure connection to CAP Management is set up here (OFF/ON).

```
<?x set SPW_SEC_MODE   = "OFF" ?>
```

The secure connection to ComAssistant is set up here (OFF/ON).

```
<?x set SPW_SSL_AUTH = "false" ?>
```

The secure connection to ComAssistant is set up here during the login session (true/false).

```
<?x set SPW_SEC_PORT   = "8480" ?>
```

The port for secure connection to CAP Management is defined here (default = 8470). This port is opened by the ComAssistant Web server (Phone Controller).

```
<?x set SPW_STD_PORT   = "8180" ?>
```

The port for normal connection to CAP Management is defined here (default = 8470). This port is opened by the ComAssistant Web server (Phone Controller).

```
<?x set SPW_MGMT_PORT = "8168" ?>
```

The port for the XML connection from ComAssistant to CAP Management is defined here (default = 8168). This port is opened by the CAP’s Web server.

A.2.4 `TelasWeb.cfg`

The `TelasWeb.cfg` file is extremely important for configuring the entire OpenScape CTI system. No changes need to be made here for the moment for the standard installation.

The following section explains the most important entries in this file:

`ConfigDomain`
Domain name of the host on which the central configuration service was installed.

> 7 This entry is only required when the domain name of the installation host cannot be determined during the installation of OpenScape CAP Management. This is easily recognized by the fact that the following URLs only contain the node name.

`PhoneURL`
URL for accessing the Phone Service

`Journal.AccessUrl`
URL for accessing the Journal Access Service.

`.Journal.AccessUrl`
URL for accessing the Mail Service.

`RequestTimeout = 10`
Maximum time in seconds waited for a response to a request to the Phone Service.

`PBX.PingInterval = 120000`
If no requests were issued over a long period, a ping request is used in the specified interval to check whether the server is still working. The time is specified in milliseconds.

`NoExpireDate = 0`
The expiration date for passwords is administered and defined in the OpenScape CTI system. ComAssistant uses this data by default. If an expiration date is not required for passwords, this option can be set to 1.

`EnableConsultation = YES`
Indicates whether the PBX system supports the special telephone functions of toggling and conference calling. These functions are normally supported (YES). More detailed information can be found in the Installation and Administration Manual for ComAssistant.

`#EnableCMCSupport = YES`
Activate "Client Matter Code" support for ComAssistant. If the feature is enabled, a project code can be selected for explicitly identifying a call data record.

```
#SametimeServer = mhpa48wc.mchp.xxxxxx.yy
```

You can define the Sametime Server (Lotus Domino Server) for ComAssistant here. This is only possible if the SameTime package for ComAssistant is installed on the CAP server. The presence and absence of linked Lotus Notes users can be visualized in ComAssistant with this connection.

```
UserDBAccessParams = NO
```

Instead of ComAssistant PABS, you can activate the WEBDAV interface on the Exchange server for ComAssistant users to permit the optional use of the user's own Outlook Contacts saved on the Exchange server.

A.2.5 `startNT.cfg`

The `StartNT.cfg` file is used by the Start Service (`jsstart.exe`) to start the entire OpenScape CTI system as a system service. The variable data is set accordingly during installation.

Important arguments for the start include:

```
args:     <CAP Management PC name>/TelasWebStarter
```

Each OpenScape CTI system is identified using a cluster ID. This uniquely defines the processes and services which belong to a cluster.
As a rule, the PC's actual name is set as the cluster ID when installing CAP Management. In the case of distributed installation, it can be chosen from a selection menu for LAN-supported multicast. If a customer does not want multicast or if it is not supported in a distributed installation, the entry must be extended as follows on all CAP computers (as well as on the CAP server):
args: **<CAP Management PC name>@<CAP Management PC name>:<Free UDP port>**/TelasWebStarter

```
#args:-v
```

If problems arise at startup, detailed logging can be activated with the commented out **`-v`** option. You should remove the comment character # for this purpose.

```
args:-port
args: 8280
```

This entry defines the port for the diagnostic agents. This port need only be changed if it is already occupied on the host.

A.2.6 `.proc` process control files

Within the CAP framework, the ProcessController can start, stop and control any pre-configured process. Each process is described by a `.proc` configuration file defining location and name of the program as well as arguments to be passed on from the ProcessController to the starting process.

The complete set of processes to be started by a ProcessController instance is defined by the collection of all `.proc` files beneath the directory named like the host where the ProcessController is running.

`.proc` file syntax

`.proc` files are parsed like property files. Each line containing a ":" character is taken as a configuration argument, a "#" character defines a line comment. The first key of a script must define the Service Identifier; the order of the remaining keys has no meaning because all keys and values are collected before they are applied. All keys are case insensitive (not the values!).

Selection of important keys used in delivered `.proc` files:
(Please note that editing / modifying `.proc` files is strongly discouraged because correct system operation can be affected; only the `restart` key family might be useful for adaptations at a customer site)

`service: <service-identifier>`

unique identifier of the process/service

`cmd: <command>`

absolute path of the command to be executed

`args: <argument>`

argument to be passed to the process/service (multiple occurrence possible)

`env: <environment>`

environment variable to be set for the process (multiple occurrence possible)

`wait: <timeout in seconds>`

wait time before executing next command (only for synchronous mode)

`mode: <synchronize mode>`

start process synchronously (mode 0) or asynchronously (mode 1 - default)

`workdir: <working directory>`

path to be set as the process working directory `mkdir: <directory path>`

path to be created if it doesn't exist (multiple occurrence possible)

`restart: <auto restart mode>`

a process can be restarted automatically in case of a crash (stop without request)
restart:0 means no auto restart (default), restart:1means auto restart

`restartexitvalue: <exit value>`

auto restart is executed only if the process has terminated with given exit code

`restartwaittime: <timeout>`

define waiting time (in seconds) to elapse before ProcessController auto-restarts the crashed process

`get: <get command>`

a get command loads any file from the distribution directory to the lib directory (default) or to any other fully specified directory. In case the file is already present in the destination directory, the command compares modification dates and executes the copy only in case the dates are different (multiple occurrence possible)

Note: A get command can come with up to three parameters

```
<relative source path> [<relative dest path>] [<replace argument]
```

A replace argument describes variables for the PageGenerator to be replaced in the retrieved file in a comma separated list like

```
"replace=INST_HOST=<hostname>,INST_DIR=<install path>"
```

If no dest path is defined the file is copied to the lib directory, using the relative source path as destination path relative to the lib directory

`getunzip: <get and unzip command>`

like the get command, but the file to be copied must be zip-formatted and will be unpacked at the destination location.

A.2.7 `admin.cfg`

This file is stored in the directory `<InstDir>\config\<host name>\admin\mgmt`. This command is used to configure the administration services. All settings are made during installation.

```
Ldap.server = scd2ldap.xxxxxx.net:389
```

If you forget your password when using ComAssistant, you can request an e-mail with a new, automatically generated password. To verify a CAP user and an e-mail address entered, the LDAP server checks the relationship between the e-mail address and the "Phone-Device Number" assigned to the user (call number in canonical format). Enter the LDAP server names here or the IP address and the LDAP port.

```
#Ldap.user = cn=Test User,ou=An OU,o=Xxxxxxx
#Ldap.password = myverysecretpasswordthatnobodysees
```

In some cases to access the LDAP service, the LDAP client must authenticate itself to the server. To supply the authentication information in the "bind" (login) operation enter the fully qualified Distinguished Name (DN) of the client and the client’s clear-text password here.

```
#Ldap.ssl = 1
```

The above mechanism has security problems because the password can be read from the network. To avoid exposing the password in this way, you can use the simple authentication mechanism within an encrypted channel, provided that this is supported by the LDAP server.

If the LDAP server you are accessing allows its services to be accessed through SSL, it is recommended to use this option, by uncommenting the above line.

Please check that you are using the correct port in the Ldap.server parameter at which the LDAP server is offering SSL.

You need to ensure that the client trusts the LDAP server that you'll be using. You must install the server's certificate (or its CA's certificate) in your JRE's database of trusted certificates.

```
# cd JAVA_HOME/lib/security
# keytool -import -file server_cert.cer -keystore cacerts
```

Important! Always use the cacerts keystore.

```
#Ldap.phone-number = telephoneNumber
#Ldap.mailaddress = mail
```

If the search field names (mapping) do not match the default in this LDAP server, enter the appropriate search field name. The field name is shown on the left in CAP and on the right in the LDAP server.

```
Ldap.timeLimit = 30
```

Define the length of a search timeout here. The search is ended if a common entry is not found for a call number and an e-mail address within this time. The result of this is that no e-mails with automatically generated passwords are sent to the ComAssistant users.

`Language = de`
Set the language for e-mails with automatically generated password for ComAssistant users: `de = German, en = English`

```
DatabaseServerList = SYSDB,SYSDB.MAP.Users,SYSDB.MAP.User-
groups,SYSDB.MAP.Scc,SYSDB.MAP.SCCProxy,SYSDB.MAP.Devices,
SYSDB.MAP.Snrs, SYSDB.MAP.Licenses, SYSDB.MAP.Businessgroup,
SYSDB.MAP.Urls, SYSDB.MAP.Ca, SYSDB.MAP.Xmlphoneservice
```

Preparation for connecting external LDAP servers instead of internal CAP LDAP servers, SLAPD, for managing all data.

```
xml.logRequests = 1
xml.traceDir = <?x $INST_DIR ?>/logsXML
```

By default, these entries are inactive (commented out). In case you want the XML message traffic from / to CAP Management to be traced, remove the comment sign. This produces a substantial amount of logging data but may be helpful in special cases, e.g. for tracing activities for handling the AccessPointEmergency feature.

`ProgramMode = CAP`
OpenScape CAP V3.0 supports the automatic integration of user data. This eliminates the need for duplicated user management, both in CAP and in an application. The following applications can be exclusively connected:

? `CAP =` Internal CAP User Management component **(default)**

? `HiPath4000Manager =` Integration in HiPath 4000 Manager **(not released)**

? `HiPathUserManager =` Integration in HiPath User Management

? `HQ8000 =` Integration of HQ8000 User Management **(not scheduled)**

? `OpenScape =` Integration of OpenScape User Management **(not scheduled)**

`#ModesListDir = modes`
The default directory `<InstDir>\config\<host name>\admin\mgmnt\modes` contains the configuration files for connecting the various user management systems. The file names correspond to the parameter inputs for "`ProgramMode`". You can select a different directory containing the relevant configuration files. In this case, enter the complete path name.

A.2.8 `adminIf.cfg`

This file is stored in the directory *<**InstDir**>\config\<host name>\admin\mgmt*. This file is used for configuring the AdminInterfaceService. All settings are made during installation.

```
TelasWebInstalled = 1/0
```

If this option is set (1), the CAP GUI features a link to the ComAssistant Help.

```
TelasServerNames
```

(do not change!) This parameter contains a list of the supported PBX connections with the corresponding names for display in the OpenScape CAP Management user interface. Every entry has the following structure: "<directory name> | <selection name>,". The directory `<InstDir>\config\distribution\config\<directory name>` contains templates for all configuration files for this specific SCC. The <selection name> is offered for selection when adding an SCC.

```
Asn1Modes = false|off, acse|CSTA ACSE, 3|CSTA III
```

(do not change!) Mapping is defined here for the SCC configured in "single domain native mode".

```
MaxResult = 300
PageResult = 10
```

Define the default parameters for the search mask that appears when you select "Search for users" here.

```
MaxTeamAgentMembers = 20
```

Define the maximum number of users that belong to a buddy list for ComAssistant here.

```
DeviceTypes = Phone|Phone, VirtualDevice|VirtualDevice
```

(do not change!) Mapping is specified here for the devices that can be added in CAP Management Device Configuration.

A.2.9 `auth.cfg`

This file is used for configuring the Security Service. All settings are made during installation. The most important entries in this file are the expiration date and the default password for CTI users. This data is set via the OpenScape CAP Management user interface in the *Default password* dialog.

```
ExpirePeriod = 40
```

Maximum validity of an individual password in days. This parameter can be modified over the CAP GUI.

```
ExpirePeriodAutoPassword = 60
```

Maximum validity of an individual, automatically generated password in days. This parameter can be modified over the CAP GUI.

`StandardPassword = MTIzNDU2`
The default password for a CAP user in Base64 encoded form.

A.2.10 backup.cfg

This file contains the settings for the automatic backup of CAP and ComAssistant data. Note that in the event of a backup to a network drive, the Windows service "OpenScape CTI" was assigned to a domain user who is authorized to access this network drive and also has local "login as service" authorization. The various backups must be performed at different times.

`NrBackups = 7`
Define the number of backups to be saved here. A backup is created every day. The format of the backup directory name is:
"<Month>-<Day>.<Backup counter>"

`BackupRootDir = C:/<install_path>/backups`
Define the destination directory for all backups.

`<?x set RULES_BACKUP_TIME = "01:55:00" ?>`
The backup time for the ComAssistant rule assistant’s data is defined here.

`<?x set USERS_BACKUP_TIME = "02:00:00" ?>`
The backup time for CAP data is defined here.

`<?x set PABS_BACKUP_TIME = "02:10:00" ?>`
The backup time for the ComAssistant user’s personal address books is defined here.

`<?x set JOURNAL_BACKUP_TIME = "02:30:00" ?>`
The backup time for the ComAssistant user’s call journals is defined here.

`<?x set CAP_LDAP_MODE = "STANDALONE" ?>`
In a Windows installation, the "`standalone`" parameter must be retained. "`Replica`" can only be used to activate replication in the case LINUX-based installation (possible in future).

A.2.11 ConfigLoader.cfg

This file contains the settings for the Configuration Loader Service and generally should not be changed. Configuration directory paths and the names of the templates for the personal journal settings are specified here.

By changing the following entry, the personal journal settings of all users can be saved to another directory. You may want to save to another directory if space on your hard disk is limited, for example, or if you want to back up data.

```
PersonalConfigDir =
               C:/<install_path>/data/TelasWeb/Journals
```

A.2.12 `Diagnose.cfg`

This file contains settings for the diagnostic servlet.

A.2.13 `Login.cfg`

In this file the administrator can preset login domains, which are then offered for selection to CTI users, who have selected authentication by means of "Windows Login", during login.

A.2.14 `DiagnoseServer.cfg`

It is possible to configure ,e-mail notifications for system malfunctions via the `DiagnoseServer.cfg` file. The e-mails are then sent to the specified mail address by the diagnostics service. The configuration of an e-mail server is essential for this. This is defined in the file "`global.cfg`".

`#Diagnose.Timer.PingInterval = 150`
The ping interval time is defined here (default = 150 seconds). When this time expires, the diagnostic server checks the current status of an internal CAP services with a ping.

`#Diagnose.Timer.CheckProcInterval = 128`
The snapshot interval time is defined here (default = 128 seconds). When this timer expires, the diagnostic server checks the current status of a CAP process controller (TelasWebStarter) with a snapshot and at the same time receives additional information on the active processes.

`#Diagnose.Timeout.Request = 20`
The waiting time after a ping or snapshot is defined here (default =20 seconds). When this timer expires, further pings or snapshots are sent until the "Retry Counter" is exceeded.

`#Diagnose.Timeout.Resend = 2`
The time (default =2 seconds) after which another ping or snapshot is sent after a "Timeout.Request" is defined here.

`#Diagnose.Timeout.RetryCount = 3`
The retry counter after "Timeout.Request" is defined here (default =3 retries). The status of a process controller or internal CAP service is modified when this retry counter expires.

`#MailTrap.Receiver-<n>.Address = <?x $MAIL_SYSADMIN ?>`
The e-mail address of the recipient of a diagnostic e-mail is defined here. The variable `<?x $MAIL_SYSADMIN ?>` can be replaced. <n> stands for block number. Each block can contain different configurations.

`#MailTrap.Receiver-<n>.TrapFilter = <id> [|<id>] ...`
The active filters for this block are defined here. <Id> stands for filter number which must be configured later. If a filter matches, an e-mail is generated and sent to the associated block address.

```
#MailTrap.Receiver-<n>.SubjectFile = <subjectTemplateFile>
```

The name of the associated "Subject Template File" is defined here. The "**subjectSample.cfg**" template file is located in the directory of the file "DiagnoseServer.cfg". Please note that file names are case-sensitive.

```
#MailTrap.Receiver-<n>.BodyFile = <bodyTemplateFile>
```

The name of the associated "Body Template File" is defined here. The "**subjectSample.cfg**" template file is located in the directory of the file "bodySample.cfg". Please note that file names are case-sensitive.

```
#MailTrap.Receiver-<n>.Enabled = true
```

You can activate or deactivate this configuration block here.

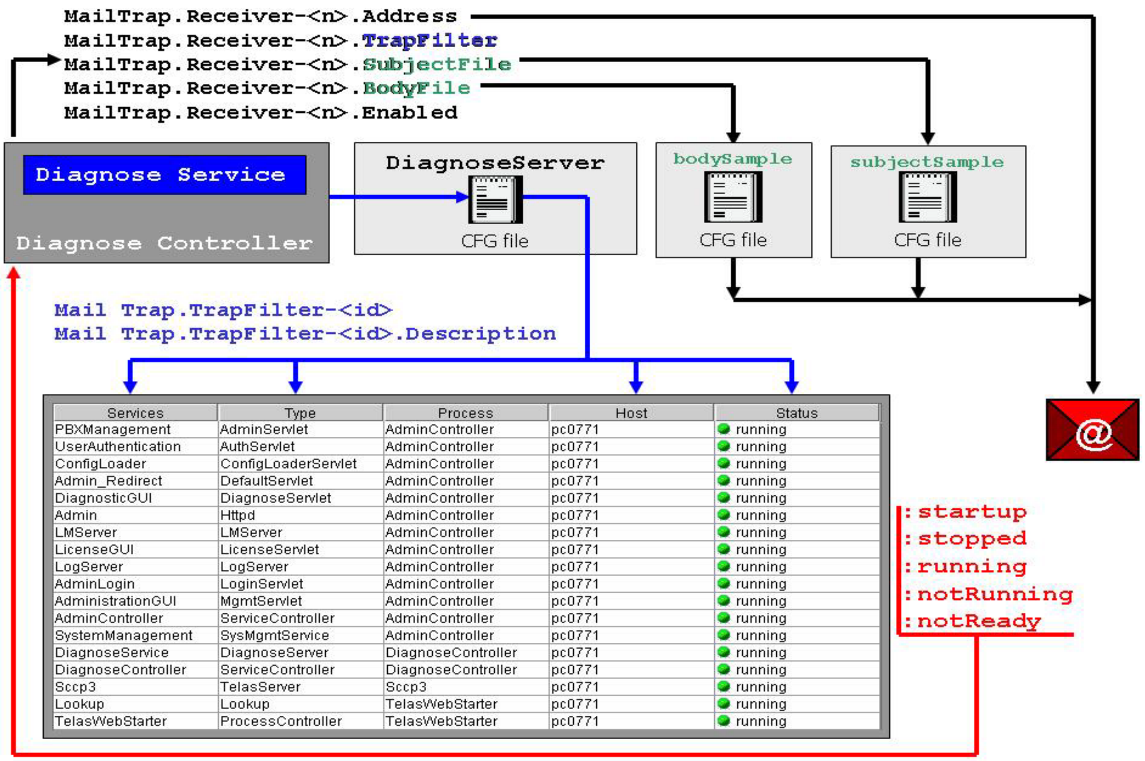
```
MailTrap.TrapFilter-<id> = <host>/[<svcType>/]<svcId>:<threshold>:<state>[|<state>]
MailTrap.TrapFilter-<id>.Description = <id>= filter description
```

You can explicitly define the file here and add a description.

<host> - The PC on which a process or internal CAP service is running.
<svcType> - The internal CAP service name
<svcId> - The service identifier
<threshold> - The threshold
<state> - The state of a process or internal CAP service.
The following statuses are supported:
notReady|notRunning|stopped|startup|running

Example of a trap configuration

```
MailTrap.Receiver-0.Address = DAuser0771@tipb.de
MailTrap.Receiver-0.TrapFilter = 0|1|2|3|4|5|6
MailTrap.Receiver-0.SubjectFile = subjectSample.cfg
MailTrap.Receiver-0.BodyFile = bodySample.cfg

MailTrap.TrapFilter-0 = pc0771/TelasServer/sccp-1:1:notReady|notRunning
MailTrap.TrapFilter-0.Description = 0 = location/Type/Service:amount:status

MailTrap.TrapFilter-1 = */Httpd/*:1:notReady|notRunning
MailTrap.TrapFilter-1.Description = 1 = One Httpd is notReady or notRunning

MailTrap.TrapFilter-2 = */TelasServer/*:1:notReady|notRunning
MailTrap.TrapFilter-2.Description = 2 = One TelasServer is notReady or
notRunning

MailTrap.TrapFilter-3 = *ccp*:1:notReady|notRunning
MailTrap.TrapFilter-3.Description = 3 = *ccp*

MailTrap.TrapFilter-4 = */Httpd/*:1:*
MailTrap.TrapFilter-4.Description = 4 = One Httpd is notReady or notRunning

MailTrap.TrapFilter-5 = *:1:stopped
MailTrap.TrapFilter-5.Description = 5 = One of the processes/services has
stopped

MailTrap.TrapFilter-6 = *:*:running
MailTrap.TrapFilter-6.Description = 6 = All processes/services are running
```


MailTrap.Receiver-<n>.Address
MailTrap.Receiver-<n>.TrapFilter
MailTrap.Receiver-<n>.SubjectFile
MailTrap.Receiver-<n>.BodyFile
MailTrap.Receiver-<n>.Enabled
Diagnose Service
Diagnose Controller
DiagnoseServer
CFG file
bodySample
CFG file
subjectSample
CFG file
Mail Trap.TrapFilter-<id>
Mail Trap.TrapFilter-<id>.Description
@
:startup
:stopped
:running
:notRunning
:notReady

Services	Type	Process	Host	Status
PBXManagement	AdminServlet	AdminController	pc0771	● running
UserAuthentication	AuthServlet	AdminController	pc0771	● running
ConfigLoader	ConfigLoaderServlet	AdminController	pc0771	● running
Admin_Redirect	DefaultServlet	AdminController	pc0771	● running
DiagnosticGUI	DiagnoseServlet	AdminController	pc0771	● running
Admin	Httpd	AdminController	pc0771	● running
LMServer	LMServer	AdminController	pc0771	● running
LicenseGUI	LicenseServlet	AdminController	pc0771	● running
LogServer	LogServer	AdminController	pc0771	● running
AdminLogin	LoginServlet	AdminController	pc0771	● running
AdministrationGUI	MgmtServlet	AdminController	pc0771	● running
AdminController	ServiceController	AdminController	pc0771	● running
SystemManagement	SysMgmtService	AdminController	pc0771	● running
DiagnoseService	DiagnoseServer	DiagnoseController	pc0771	● running
DiagnoseController	ServiceController	DiagnoseController	pc0771	● running
Sccp3	TelasServer	Sccp3	pc0771	● running
Lookup	Lookup	TelasWebStarter	pc0771	● running
TelasWebStarter	ProcessController	TelasWebStarter	pc0771	● running

A.2.15 SAT configuration files

The Address Translation Service (SAT, see Section 2.3.4 for details) is configured only by means of configuration files that must be edited explicitly; no configuration via CAP Management GUI is supported. Affected config files are

SatServer.cfg (directory <InstDir>/config/<host>/admin/sat_svc)

Telas.cfg (directory <InstDir>/config/<host>/sccp_<sccp_name>)

Telas.cfg (directory <InstDir>/config/<host>/telasServer_<scc_name>)

SatServer.cfg is the central SAT configuration file which looks like

```
#--------------------------------------------------------------------------
# Environment for Service Address Translation
#--------------------------------------------------------------------------

<?x include "/common/global.cfg" ?>

...

#
# configuration of SatServer local TCP port
#
LOCAL_PORT = 8999 <-- set TCP port here (8999 used as default)
LOG_LEVEL = 2     <-- set log level here (default 2 means error logging)

#
# legacy mode setting - used to set CAP V3.0 operation in CAP V2.0 mode:
# Applications that don’t want to adapt don’t get canonical or interntl
# format numbers except for PBXes which are newly supported in CAP V3.0
#
# Default setting: SAT bypassed
LEGACY_MODE = true
# Unset legacy mode to activate SAT!
#LEGACY_MODE = false
```

The **Telas.cfg** config files for configured SCC and SCCP contain new entries related to SAT operation which should be modified in sync with activation / deactivation of SAT:

```
# ================================================================
# CAP Management      -      Service Configuration      -     SCCP
# ================================================================
# WARNING: Please don't change values manually, use CAP Management
# ----------------------------------------------------------------
```

```
..
# Flag sets legacy mode operation for the SCCP to SCC direction;
# 1 (legacy mode set) is default value
# Uncomment subsequent entry to activate SAT!
#CFR_SATLegacyMode = 0


# ==================================================================
# CAP Management      -      Service Configuration       -     SCC
# ==================================================================
# WARNING: Please don't change values manually, use CAP Management
# ------------------------------------------------------------------

..

# Flags set legacy mode operation for the SCC - Switch connection;
# 1 (legacy mode set) is default value
# Uncomment subsequent entries to activate SAT!
# Computing Function to Switching Function (SCC to switch)
#CFR_SATLegacyMode = 0
# Switching Function to Computing Function (switch to SCC)
#SFR_SATLegacyMode = 0

# Flag for SAT tuning (populate SAT cache on MonitorStart)
# Regularly it is recommended to keep the default value 1
#noMStartSATMode = 0
```

Remark: special setting (for customer EON) - explanation and desription only in english

The following text need to insert into the **`SatServer.cfg`** (im Verzeichnis `<InstDir>/config/<host>/admin/sat_svc`):

```
 DomainCacheMode = 1

 DBCache = 7
```

DomainCacheMode: the value can be either 1 or 2:
The DomainCacheMode configuration adds special rules to convert

dialing numbers to canonical format even if the number is not in the database. The conversion is based on the VNR prefix.

Mode 1 (DOMAIN_CACHE_PREFIX_BY_SCC) goes through all the SCC's domains and if the number starts with the VNR code of the domain, we have a match and this domain is used for the conversion.

Mode 2 (DOMAIN_CACHE_FIXED_LENGTH_BY_SCC) uses hashmaps. The length of the VNR number is fixed (vncLength) and the domain is looked up in the hashmap by a key pair which holds the scc id and the first vncLength characters of the dialing number.

Mode 1 is more general and faster, mode 2 not recommended.

DBCache: cache CAP management data, possible values:

1 - cache domain entries

2 - cache scc entries

4 - cache scc list

The values can be combined (added) to cache multiple data types.

A.2.16 No accent via CSTA (ASN.1)

Remark: only english description is available

The CAP can deliver accent characters via CSTA II ASN1, but since that is not CSTA conform, tha’s why the following settings can be applied for applications, which want to be ASN1 conform.

It is possible to convert the CallInfo (and ExtendedCallInfo) fields in ACL events to a 7 bit only ASCII string. There are 3 options which affect the conversion and two of them is new and available only from this version. These options must be set

in ca4000.cfg file.

1. USE_ACCENTED_CHARACTERS=0

This option should work on all switch version. It turns on the the conversion to 7bit call info (and extended call info) conversion without that the call info received from swith is sent out on the CSTA side without modification. The default value is 1 (when there's no conversion). To turn it on please set it to 0 as above.

2. CALLINFO_CONVERT_MODE=w1252

This option only affects the callinfo conversion (V3 basically, but the specification allows it on later versions). It can have 3 values:
off - no callinfo conversion
w1252 - windows codepage 1252 mode where the chars above 127 are mapped to a similar lower char. (For example Ü -> U, Á -> A etc.) Unmappable chars (for exmple 0x81 or 0xfe) are changes to the default char (see option 3.)
defaultchar - all chars above 127 mapped to the default char (see option 3.) The default mode is 'defaultchar'

3. CALLINFO_CONVERT_DEFAULT_CHAR=.

Unmappable characters are changed to this one. The default value is _ (underscore).

An example configuration:

```
USE_ACCENTED_CHARACTERS=0
CALLINFO_CONVERT_MODE=w1252
CALLINFO_CONVERT_DEFAULT_CHAR=.
```

These lines can be anywhere in the config file, but if it is at the and please make sure that there's a new line after the last config entry!

Co

A.2.17 Configuration data for CAP Management

All data used exclusively by CAP Management for PBX system connections and for checking authorization is saved in the *<**InstDir**>\data\TelasAdmin\adminauth\capdb* directory.

The `capdb` subdirectory contains the authentication information for the authentication service of CAP Management in an LDAP database. All of the information for authorized users (e.g. user type, password and timestamp) is entered here. It is also used to store the assignments of PBX to IP address and port of the responsible CAP Call Control Service processes.

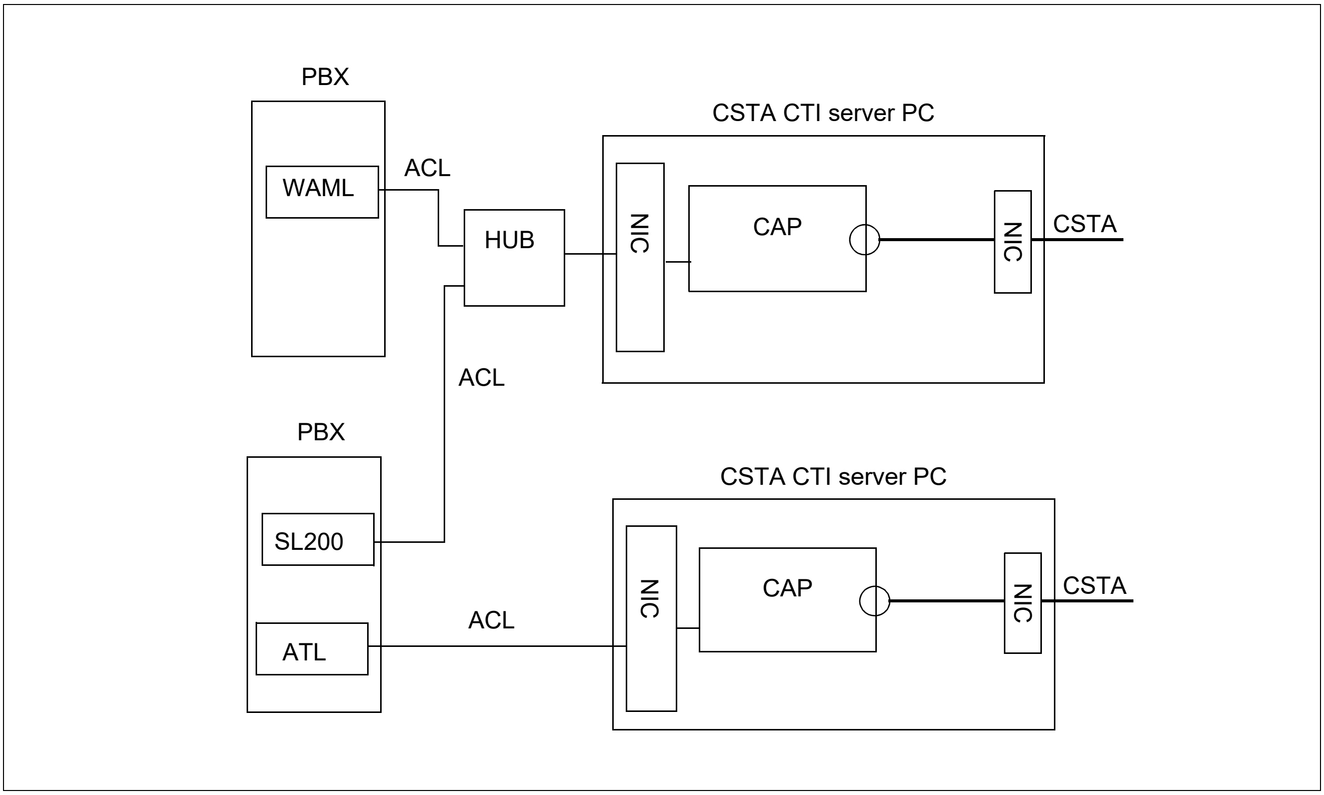
> 7 All files are managed via the OpenScape CAP Management user interface. Modifying of one of this files with an text editor is not authorized.

B Connecting HiPath 4000 with a Server PC

B.1 Server PC connectivity options

HiPath 4000 features integrated Ethernet server bus ports. This means you can connect the OpenScape CAP server PC over an Ethernet TCP/IP connection. A TCP/IP connection is a logical data connection between two addresses which are composed of a port number (for TCP) and a logical IP address. In this configuration, multiple logical destinations can be reached over a physical address (the TCP port number). The TCP protocol ensures that the data packets transmitted reach the logical IP destination address in the correct order and without loss of data. The connection is completely cleared down if an error occurs.

The following diagram shows possible connections to a HiPath 4000.



Basically, the CSTA CTI server can also be configured with a single LAN card, although this is not recommended.

B.1.1 Connection to the Atlantic LAN

An unshielded twisted-pair cable to the internal Ethernet LAN serves as the physical interface between the HiPath 4000 and OpenScape CP. The internal ("Atlantic") LAN provides high data bandwidth and is therefore ideal for data communication between the HiPath 4000 processors and OpenScape CAP. The internal Ethernet LAN can be accessed directly over the ports on the rear panel of the HiPath 4000.

If there are multiple OpenScape CAP servers connected to the same Atlantic LAN, every server must have a unique IP address. An external hub is also required. A standard twisted-pair cable is used for the physical connection to the external hub. Any standard hub with RJ45 ports can be used as the external hub, for example Office Connect Ethernet Hub 4 (4 TP/RJ45 ports) from 3Com (vendor number 3C16704A). The hub ports should always be MDI/MDIX switch ports.

IP addresses

IP addresses (IP network numbers plus server numbers) provide access to the servers connected to the Atlantic LAN. The Atlantic LAN’s IP network number is "192.0.2.0", which defines a class C address. These network numbers use all servers connected to the Atlantic LAN.

The components have fixed IP addresses, for example:

CC-A: 192.0.2.1
CC-B: 192.0.2.2
ADS/ADP: 192.0.2.3

The following address ranges are reserved for external applications:

ext. ACD server: 192.0.2.10 - 192.0.2.19 (default: 192.0.2.16)

OpenScape CAP: 192.0.2.23 - 192.0.2.29 (default: 192.0.2.25)

If there are multiple OpenScape CAP servers connected to the same Atlantic LAN, every server must have a unique IP address. An external hub is also required. The default address of the first CAP server is 192.0.2.25. The address number is incremented by one for each additional server (192.0.2.26, 192.0.2.27, etc.). A total of five servers can be connected.

B.1.2 Connection to the SL200 or WAML board

Fixed IP addresses are defined in the Atlantic LAN for the HiPath components. It is therefore impossible to configure additional PBXs in the same LAN. This restriction can be avoided by using an SL200 board (in HiPath 4000) or a WAML board (in HiPath 4000).

These LAN boards have freely configurable IP addresses and can be used to access the Atlantic LAN.

> 7 You cannot configure a WAML board at the same time as an SL200 board.

B.2 Configuring the HiPath 4000 software

B.2.1 Configuring the connection to the SL200 board (HiPath 4000 only)

The Atlantic LAN must be configured properly before you start to configure the SL200 board.

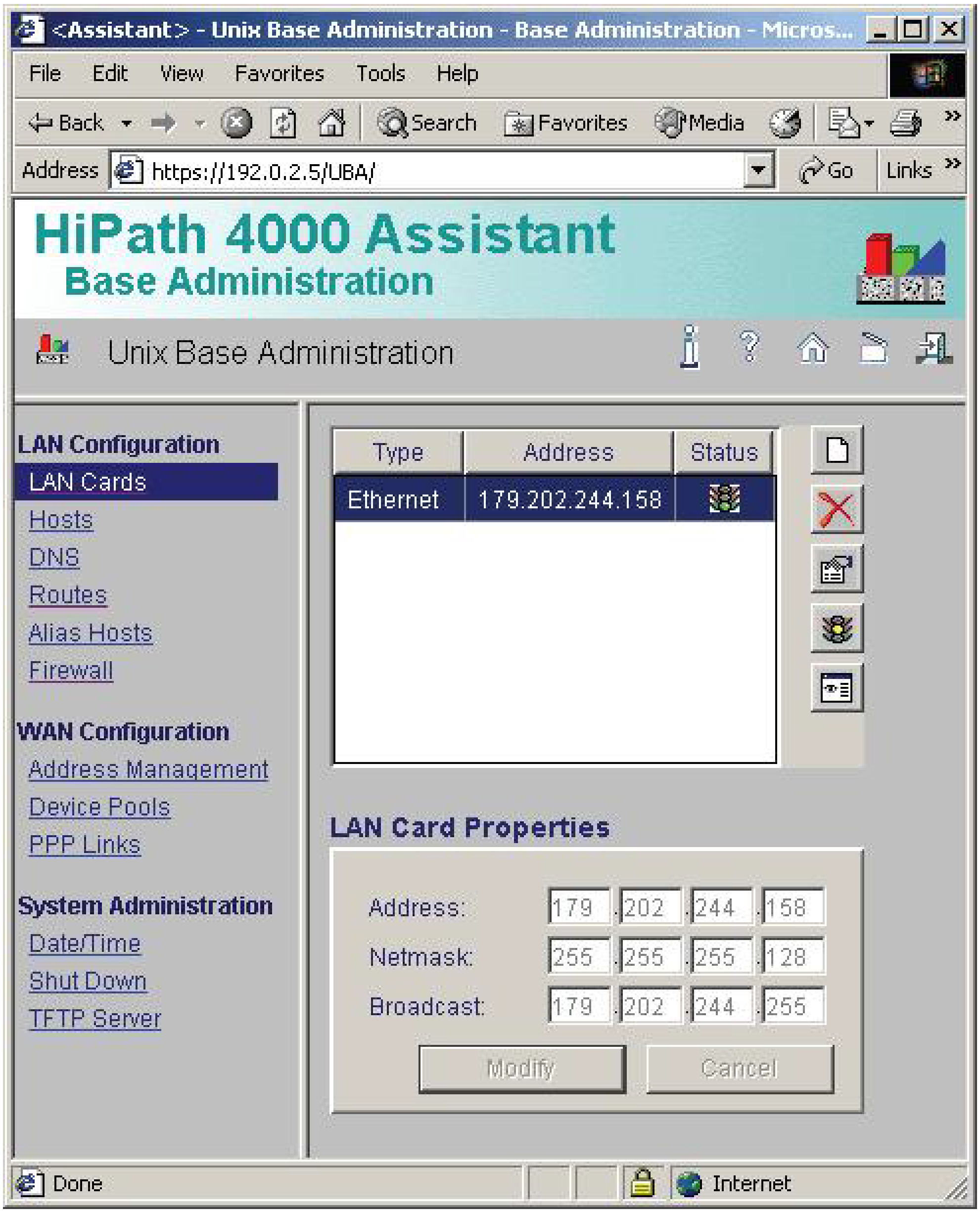
Use the UnixWare service tool ’Unix Base Administrator’ (UBA) to configure the SL200 card for use with CA4000. The UBA service tool can be found under LaunchPad in the ’Base Administration’ folder in HiPath 4000 Assistant.

Once the LAN settings for SL200 have been properly configured in the UBA under ’LAN Cards’ and ’Routes’, proceed with the section ’Firewall settings’.

Configuring with HiPath 4000 Assistant and the UBA

Open a Web browser on a PC with direct access to the Atlantic LAN. Go to the HiPath 4000 Assistant’s public domain under http://192.0.2.5 and follow the instructions under the link ’Client Preparation’. Next, use the browser to access the UBA tool by entering the following link: https://192.0.2.5/UBA

You must now start by configuring the LAN card. Do this by selecting ’LAN Configuration’ and clicking the menu item ’LAN Cards’. The table in the right-hand frame should be blank (if it contains an entry, the LAN card was already configured and does not have to be re-configured). Click the ’New LAN Card Configuration’ icon (above right in the right-hand frame) and enter the IP address, netmask, and broadcast values provided by the system administrator for SL200. Add the card for the entry. The new entry then appears after a few seconds in the table. Then, restart UnixWare as a privileged user in a Unix shell by clicking ’ShutDown’ or by entering ’shutdown -y -g0’.

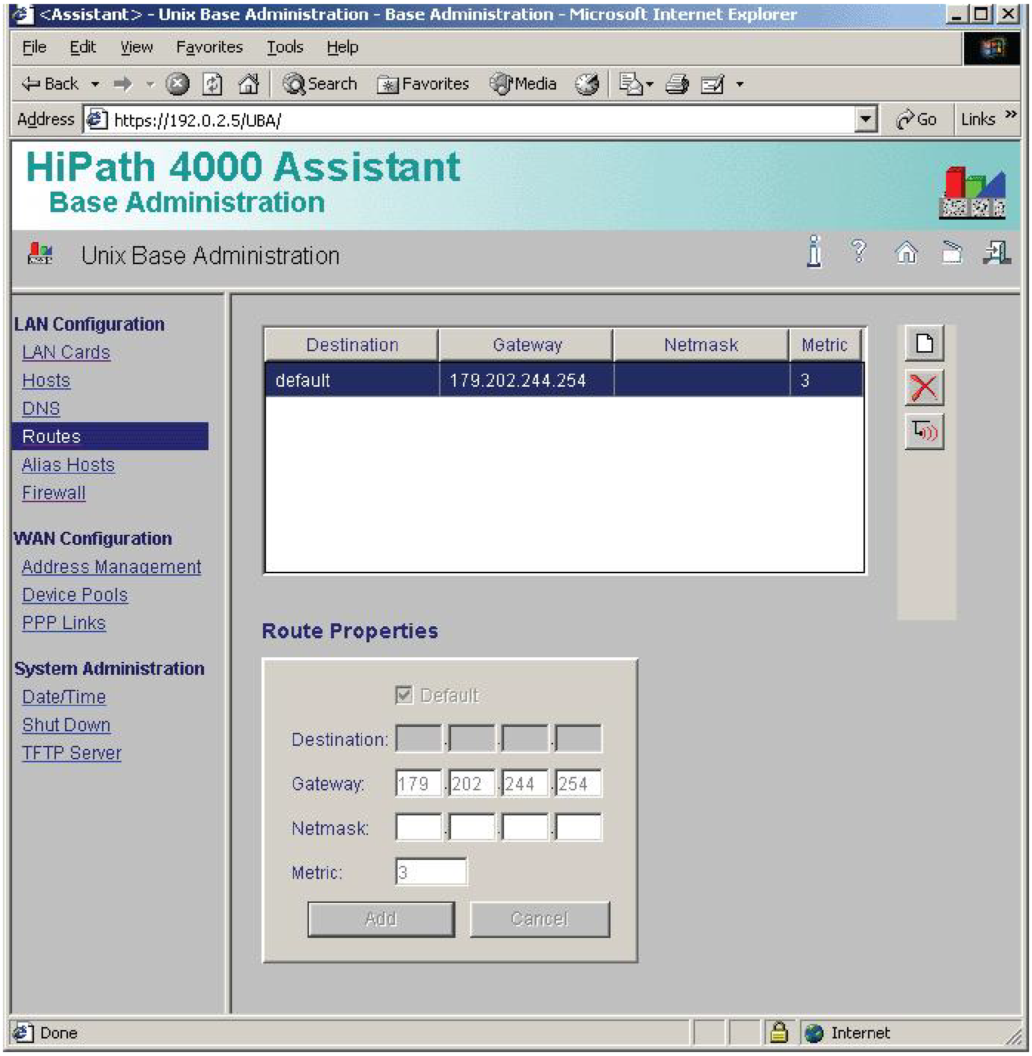


Type	Address	Status
Ethernet	179.202.244.158	

LAN Card Properties

Address: 179 .202 .244 .158
Netmask: 255 .255 .255 .128
Broadcast: 179 .202 .244 .255

Activate the UBA as soon as UnixWare has been restarted and all UnixWare services have been started and select the 'Routes' menu item. Click the 'New Route' icon (above right in the right-hand frame). Select the 'Default' check box, enter the gateway value you received from the system administrator and enter '3' under 'Metric'. Normally, you do not have to enter a value for 'Netmask'. If in doubt, consult your system administrator; click 'Add' for the route, wait until it appears in the table and then restart UnixWare.



Destination	Gateway	Netmask	Metric
default	179.202.244.254		3

Route Properties

☑ Default

Destination: . . .

Gateway: 179 .202 .244 .254

Netmask: . . .

Metric: 3

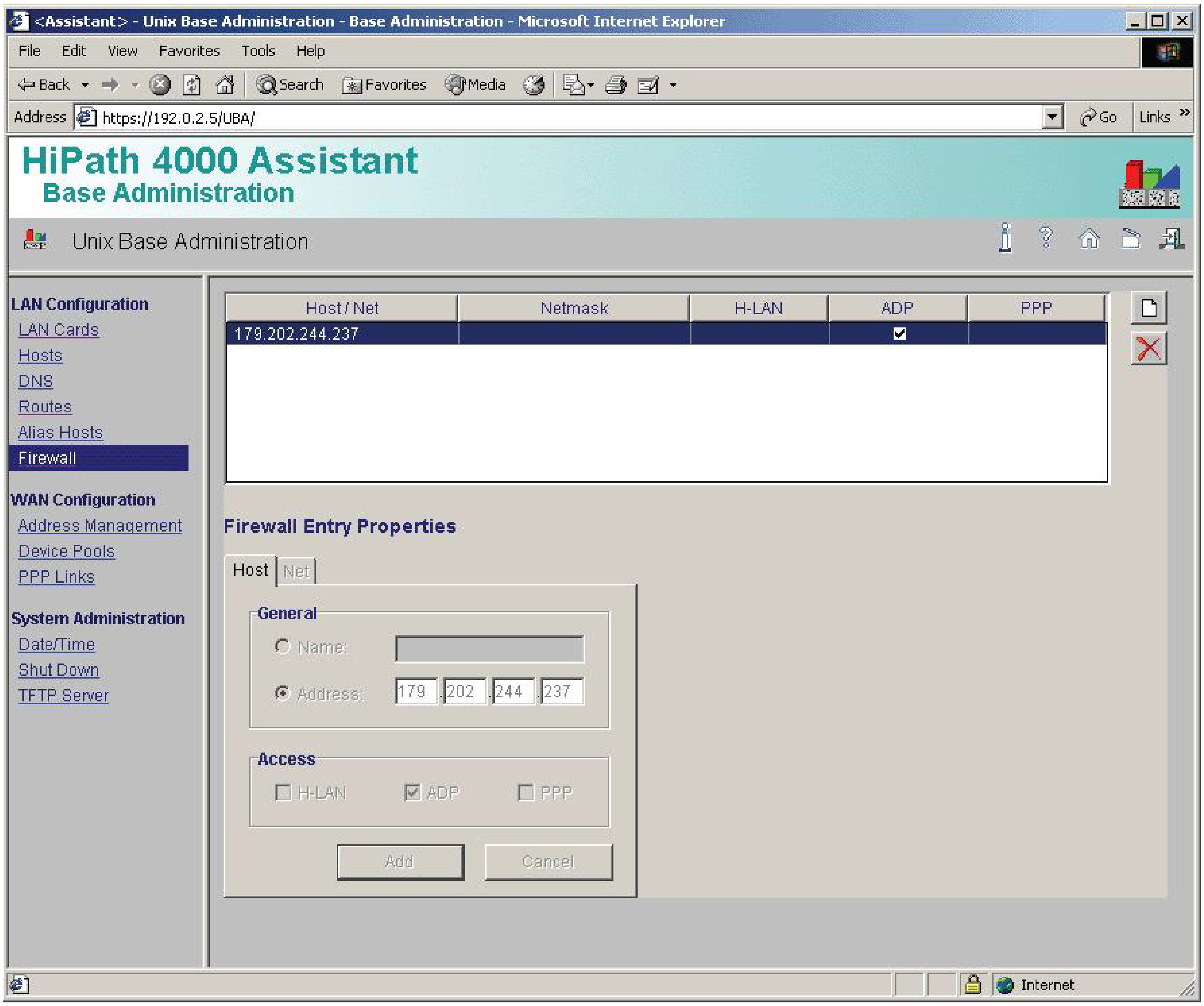
Firewall settings

The following steps must be performed once LAN configuration has been started for SL200 with the options ’LAN Cards’ and ’Routes’ and UnixWare has been restarted:

1. Select the ’Firewall’ option under ’LAN Configuration’. After a few seconds the firewall settings appear in the right-hand frame.
2. ’Host’ is set by default in the ’New Firewall Entry’ field. Click the ’Address’ option.
3. Enter the IP address of the computer you want to use to access the CA4000.
4. You may only select the option ’ADP’ in the ’Access’ field here.
5. Click the ’Add’ button.

6. After a few seconds, a new line appears in the Host / Net table on top in the right-hand frame.

7. If you have to configure additional workstations, click the ’New Firewall Entry’ icon on the upper right and repeat steps 2-6 for each additional workstation. A host should be available for use with CA4000 as soon as it has been added to the list.



Address: https://192.0.2.5/UBA/

Host / Net	Netmask	H-LAN	ADP	PPP
179.202.244.237			☑	

○ Name:
● Address: 179 . 202 . 244 . 237

□ H-LAN ☑ ADP □ PPP

B.2.2 Configuring the connection to the WAML board

Before the WAML board is configured, the Atlantic LAN must be properly configured and connected to the WAML board over a LAN cable.

The AMO LANC can be used to configure the WAML board for LAN communication. A maximum of four WAML boards can be configured in a HiPath system.

B.3 Connecting the CAP PC to HiPath 4000

The procedure includes the attachment of the connection cable and the execution of a ping on the HiPath 4000 Perform the following steps:

1. Connect an RJ45 cable to the adapter card at the back of the CTI server.
2. Connect the other end of the RJ45 cable to the hub C/SL200/WAML card in HiPath 4000.
3. Send a ping to the IP address of the HiPath 4000. Enter the following character string at the input prompt:

   ping 192.0.2.3 (for a connection to the Atlantic LAN)
4. If the connection is successful, you receive a reply from HiPath 4000. Otherwise, check the connections and repeat the ping. If the problem persists, replace the cable and repeat the ping.

B.3.1 Configuring the ACL connection

The system will not work properly until OpenScape CAP and HiPath 4000 are specially configured, that is, certain specific parameters must be set.

HiPath parameterization is performed with the help of MML command batches (AMOs).

If multiple gateways are configured for the same HiPath system, separate ACL-C application parameters must be configured for this in HiPath 4000.

The following steps must be performed for every installation:

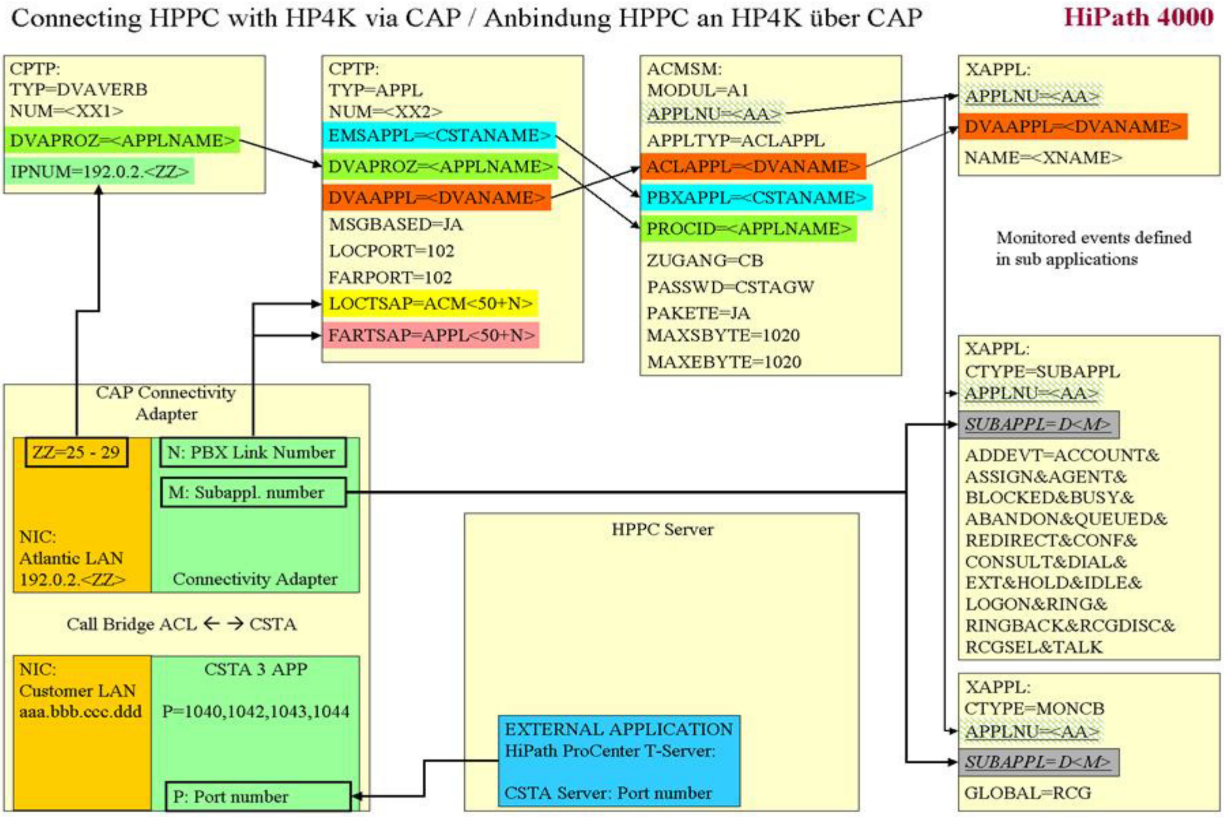
1. Set the maximum number of ACL-C applications
   AMO: DIMSU
   Parameter: ECCS:
2. Set the maximum number of monitored devices
   AMO: DIMSU (DIMensioning of features, Switching Unit)
   Parameter: ACDMONID, number of monitored ID groups (for example, ACD agents - ACD-G only).
   Maximum number of monitored devices permitted. The application is prevented from setting more than the maximum number of monitored devices.

3. Set the call processing timer
   AMO: CTIME, customer-specific CP timer, switching unit
   Administration of the call processing timer evaluated by the "MakeCall" event.
4. Configuration of the physical ports for TCP/IP data communication
   AMO: CPTP, communication parameter for TCP/IP connection
   Type: DPCON
5. Set the interface parameters (transport address)
   AMO: CPTP, communication parameter for TCP/IP connection
   Type: APPL
6. Configuration of ACL Manager parameters
   AMO: ACMSM, ACL Manager communication parameters
   TYPE=ACLAPPL
7. Configuration of parameters for sub-applications
   AMO: XAPPL, DP application ACL
8. AMO application administration
   AMO: APC

Certain parameters set with AMOs must be identical to the values set in the OpenScape CAP configuration.

In particular, these are:

Password	(ACMSM)
Block size for transmission/receipt	(ACMSM)
IP address of the gateway	(CPTP)
Generated ACL-C events	(XAPPL)
ID of the sub-application	(XAPPL)



Connecting HPPC with HP4K via CAP / Anbindung HPPC an HP4K über CAP

HiPath 4000

CPTP:
TYP=DVAVERB
NUM=<XX1>
DVAPROZ=<APPLNAME>
IPNUM=192.0.2.<ZZ>

CPTP:
TYP=APPL
NUM=<XX2>
EMSAPPL=<CSTANAME>
DVAPROZ=<APPLNAME>
DVAAPPL=<DVANAME>
MSGBASED=JA
LOCPORT=102
FARPORT=102
LOCTSAP=ACM<50+N>
FARTSAP=APPL<50+N>

ACMSM:
MODUL=A1
APPLNU=<AA>
APPLTYP=ACLAPPL
ACLAPPL=<DVANAME>
PBXAPPL=<CSTANAME>
PROCID=<APPLNAME>
ZUGANG=CB
PASSWD=CSTAGW
PAKETE=JA
MAXSBYTE=1020
MAXEBYTE=1020

XAPPL:
APPLNU=<AA>
DVAAPPL=<DVANAME>
NAME=<XNAME>

Monitored events defined in sub applications

XAPPL:
CTYPE=SUBAPPL
APPLNU=<AA>
SUBAPPL=D<M>
ADDEVT=ACCOUNT&ASSIGN&AGENT&BLOCKED&BUSY&ABANDON&QUEUED&REDIRECT&CONF&CONSULT&DIAL&EXT&HOLD&IDLE&LOGON&RING&RINGBACK&RCGDISC&RCGSEL&TALK

XAPPL:
CTYPE=MONCB
APPLNU=<AA>
SUBAPPL=D<M>
GLOBAL=RCG

CAP Connectivity Adapter

ZZ=25 - 29

NIC:
Atlantic LAN
192.0.2.<ZZ>

N: PBX Link Number

M: Subappl. number

Connectivity Adapter

Call Bridge ACL ← → CSTA

NIC:
Customer LAN
aaa.bbb.ccc.ddd

CSTA 3 APP
P=1040,1042,1043,1044

P: Port number

HPPC Server

EXTERNAL APPLICATION
HiPath ProCenter T-Server:
CSTA Server: Port number

B.3.2 HiPath 4000 configuration batch for the CA

The configuration batch for HiPath 4000 contains three parameters that are important for communication with the CAP CA server:

? IP address of the CAP CA server PC

? PBX Link Number

? PBX Sub Appl Number

IP address of the CAP CA server PC

If everything is set correctly, the appropriate IP address is entered here. However, this has currently no value in conjunction with CA. It is only used if HiPath 4000 were to set up the TCP/IP connection autonomously.

PBX Link Number

This must match in the CA configuration and in the AMO CPTP:APPL. The crucial parameter in the AMO is the ACM number and the APPL number. It is composed of the default value "50" plus the PBX link number (ACM 50 + PBX link number; APPL 50 + PBX link number).

Example: PBX link number = 5 >>> ACM55;APPL55;

PBX Sub Appl Number

This must match in the CA configuration and in the AMO XAPPL. The crucial parameter in the AMO is the sub-application number "Dxx".

Example: PBX sub appl number = 25 >>> D25

7	Only sub app number in the range of D17 and D32 are allowed to configure to be able to monitor the devices.

B.3.2.1 HiPath 4000 batch for CA4000

```
ADD-CPTP:DPCON,55,"CAPCONN1","<IP-CA4000-PC>";

ADD-CPTP:APPL,55,"CAP1","CAPCONN1","CAPAPP1",YES,102,102,"ACM55","APPL55";

/*

ADD-XAPPL:55,"CAPAPP1","CAP1",,Y;

CHANGE-XAPPL:SUBAPPL,55,D25,ALL;

CHANGE-XAPPL:MONCB,55,D25,RCG,;

/*

ADD-ACMSM:,55,ACLAPPL,"CAPAPP1","CAP1","CAPCONN1",CB,"CSTAGW",Y,1020,1020;

/*

/* Signaling time setting (here 15 seconds) for

/* "MakeCall" at the call-initiating extension for analog

/* terminals

CHANGE-CTIME:TYPESWU=CP1,ECCSSUPV=15;

/*

/* EXEC-UPDAT:BP,ALL;

/* EXEC-UPDAT:A1,ALL

/* EXEC-REST:SYSTEM,RELOAD;
```

B.3.2.2 Configuring a HiPath 4000 terminal for XML Phone Service

To use XML Phone Service, at least one name key must be free on a terminal. If not, the AMO TAPRO can be used to change the function of a key.

Example:

```
CHANGE-TAPRO:STNO=<extension>,TD<key number_xx>=NAME;
```

```
CHANGE-TAPRO:STNO=27486,TD07=NAME;
```

Use the AMO ZIEL to configure an OpenScape CAP XML Phone Service as a "non voice" application.

Example:

```
ADD-ZIEL:TYPE=NAME,SRCNO=<extension>,KYNO=xx,DESTNON=C13999xx;
```

```
ADD-ZIEL:TYPE=NAME,SRCNO=27486,KYNO=07,DESTNON=C1399907;
```

The URL that was previously associated with the preconfigured button is assigned to the device in the CAP Management GUI.

Additional settings in HiPath 4000

The "Repdail Pause Timer" in the "Switching Unit" must be set to the lowest value possible. Use the AMO CTIME for this.

Example:

```
CHANGE-CTIME:TYPESWU=CP2,REPAUSE=1;
```

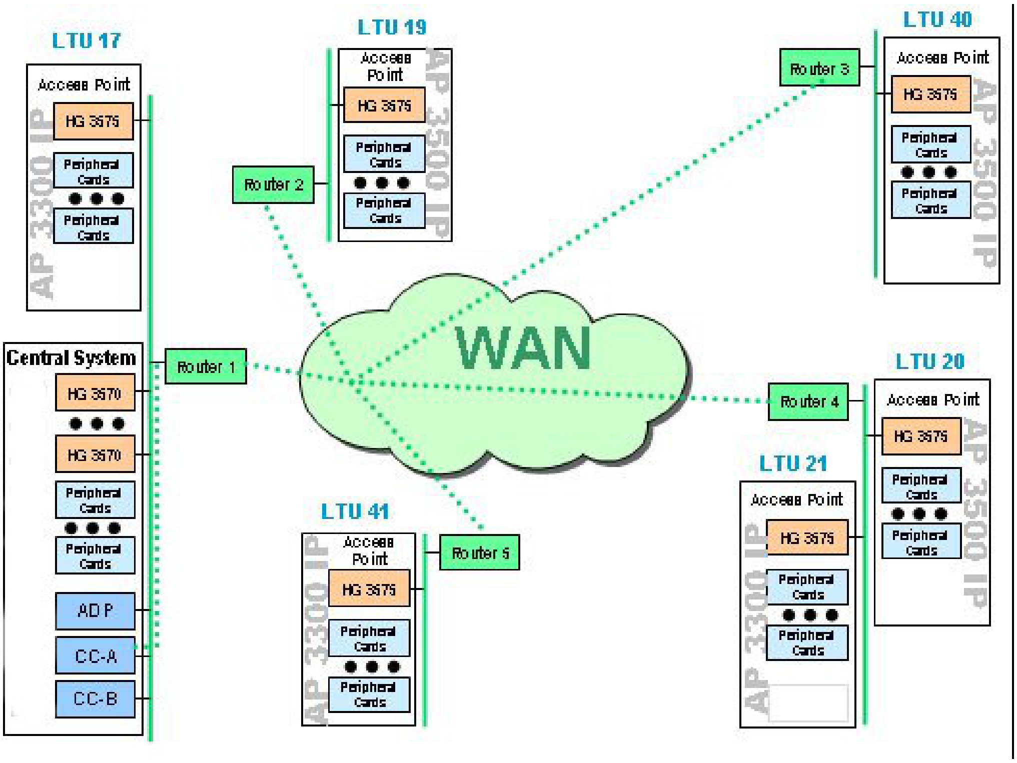
B.4 HiPath / OpenScape 4000 with AP Emergency

This documentation is not intended to cover the AP Emergency feature from HiPath 4000 view in detail (including HW components and SW settings necessary on HiPath 4000 level).

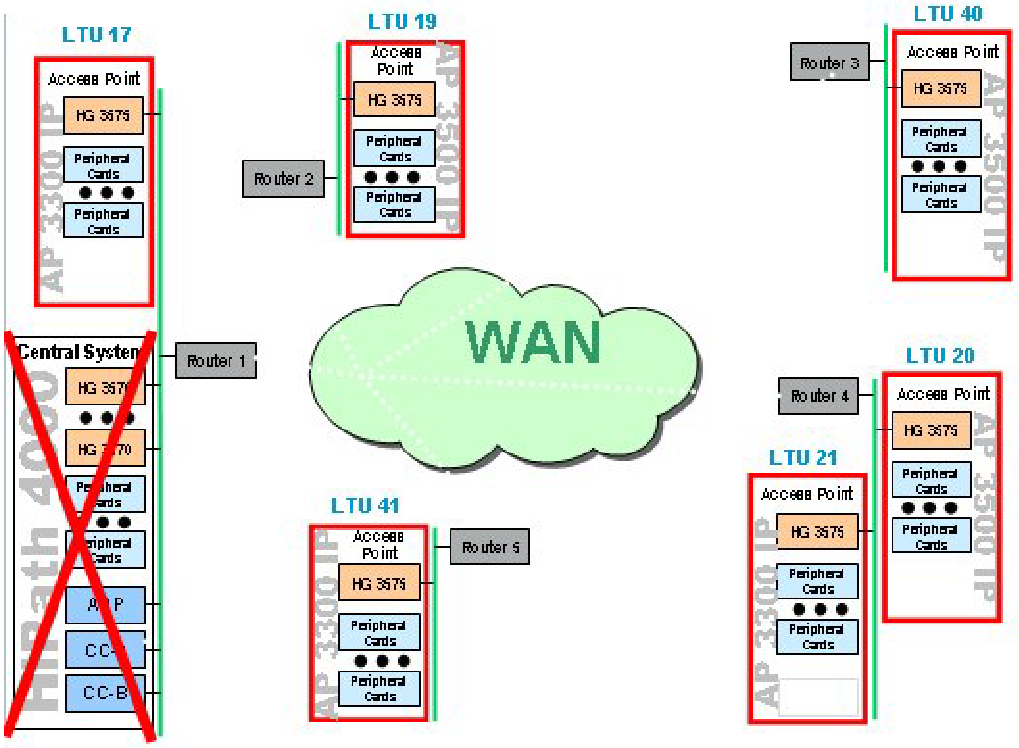
Only a high level description of the functional differences between a HiPath 4000 switch with and without AP Emergency configuration will be provided here. For deeper information, please refer to the very elaborate description in the HiPath 4000 Service Documentation (Complex Solutions - IPDA & APE).

B.4.1 HiPath / OpenScape 4000 w/o AP Emergency

The HiPath 4000 V1.0 IPDA (IP Distributed Architecture) feature allowed for distributing Access Points (frames for HiPath 4000 standard subscriber line modules) across an IP network. Subscriber lines connected to these Access Points are treated as if they were connected directly to the HiPath 4000 server (as usual before). The same holds for the administration of all of the components distributed via IP: there is a common system view with the HiPath 4000 server taken as entry point.



In case of failure of some of the components involved (e.g. failure of HiPath 4000 server, problems in the IP network), up to now it was no longer possible to operate devices connected to remote Access Points (the available workaround based on a modem connection between HiPath 4000 server and access point via PSTN will not be addressed here).



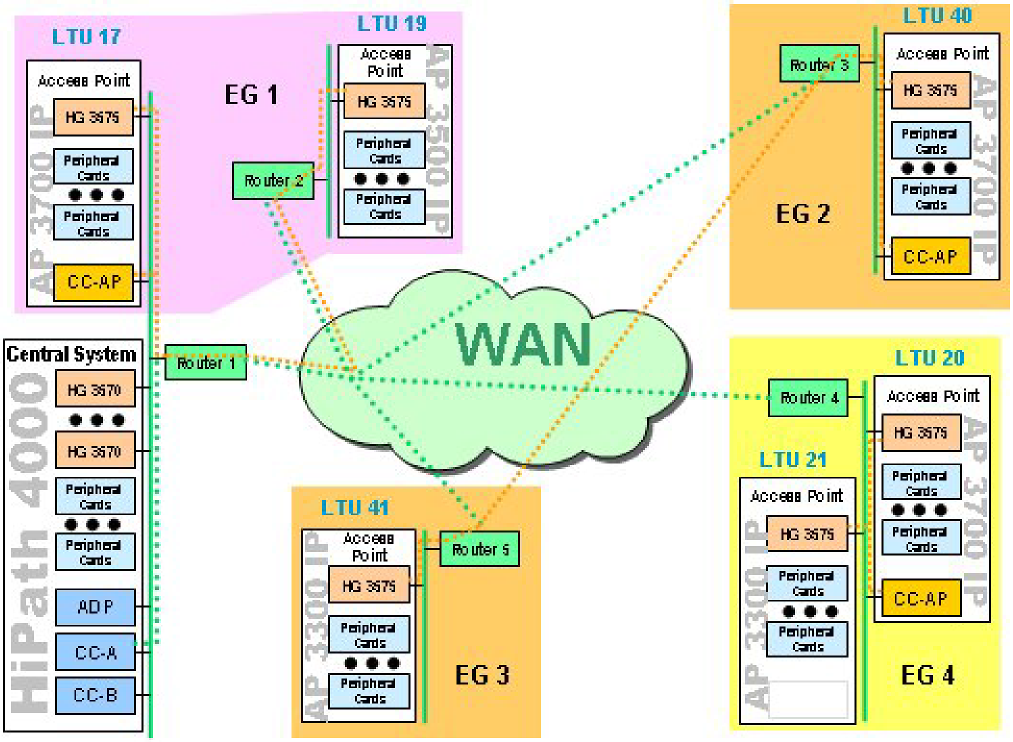
B.4.2 Improvement by AP Emergency

The AP Emergency feature releases with HiPath 4000 V2.0 is meant to help improving the restricted reachability due to component failure as described above.

The intention is to guarantee local reachability of devices connected to the AP shelf after failure of the HiPath 4000 server or the IP network as far as possible (i.e. subscribers connected to the same AP shelf can talk to each other, but can’t talk to subscribers connected to a server host shelf / a non-AP shelf).

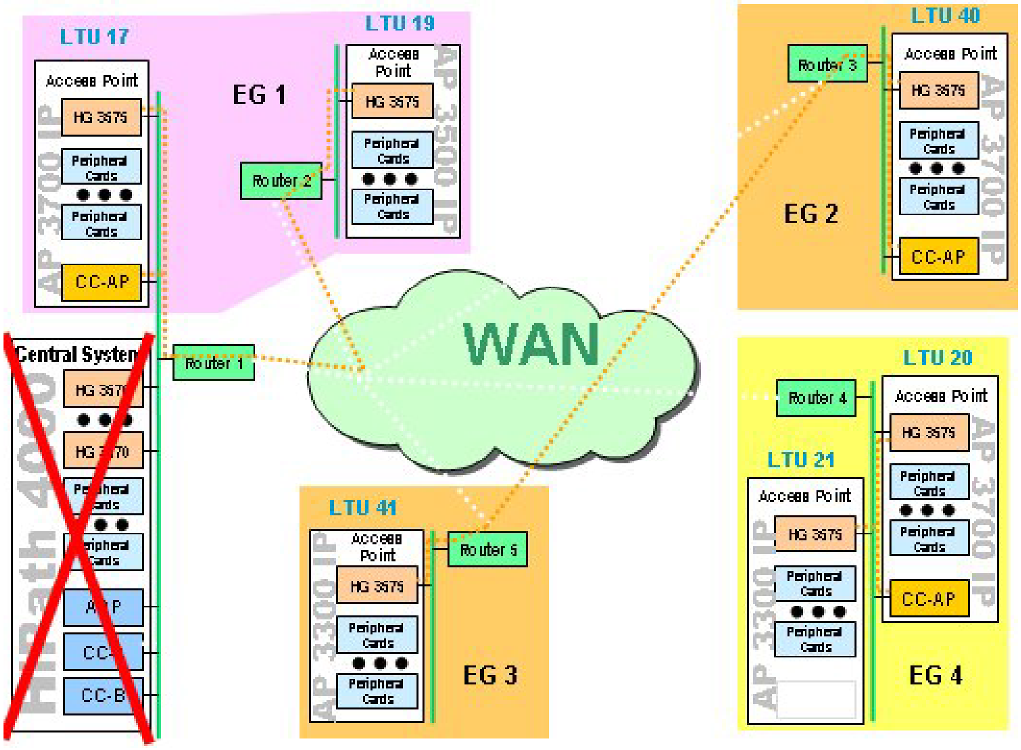
HiPath 4000 AP Emergency configuration

? HiPath 4000 server with IP distributed Access Points as well as HW/SW components required for APE specifically



HiPath 4000 server failure

- devices connected locally (i.e. to shelves within the HIPath 4000 server) are no longer reachable.
- Access Points will survive the failure as any AP is able to reach its assigned CC-AP.

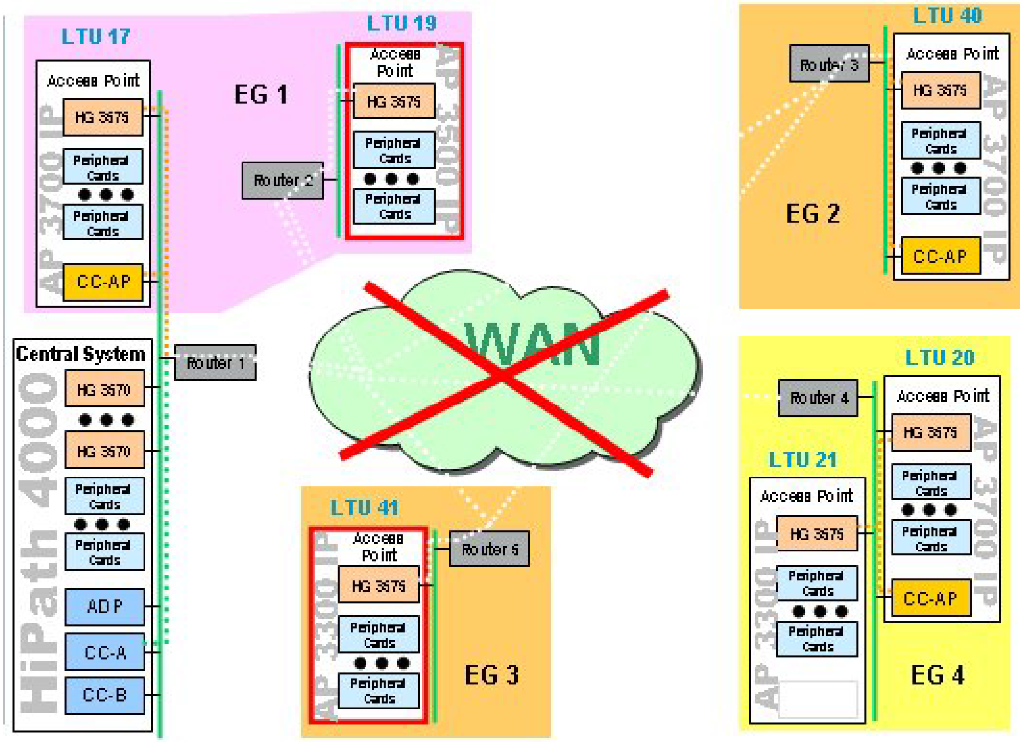


(Total or partial) WAN failure

Only those Access Points will survive that

- ? still can reach their assigned CC-AP (AP20, AP21, AP40 in the example) or
- ? are directly connected to the HiPath 4000 server (AP17 in the example).

Remaining Access Points will experience a total failure (AP19, AP41 in the example).



Glossary

A

ACD

See *Automatic Call Distribution*.

ACD Group

A group of ACD agents that are responsible for processing specific calls (for example, calls to call centers, to credit agencies or to airline booking agencies). See also *Automatic Call Distribution*.

Agent

A customer service employee who initiates or receives customer calls over an agent workstation.

Agent workstation

A workstation with a telephone connected to the HiPath 4000 system and a terminal connected to the LAN.

ANI

See *Automatic Number Identification*.

Answer Call

A service that answers a calling device (for example, when a call is parked) and then connects the party on hold.

Application Supplier

A company that supplies application programs that run in the LAN environment where HiPath 4000 is connected.

AP

Access Point - frame to hold standard HiPath / OpenScape 4000 subscriber line modules.

AP Emergency (APE)

Access Point Emergency (see Section B.4, "HiPath / OpenScape 4000 with AP Emergency").

API

See *Application Program Interface*.

Application Connectivity Link (ACL)

See *Connectivity Adapter HiPath 4000 Application Connectivity Link*.

Application Program Interface (API)

The software used by the LAN to permit HiPath 4000 to perform certain telephony functions (for example, set up or transfer calls).

Automated Outbound Dialing

A feature that lets an agent set up a call to a customer over a telephony application.

Automatic Call Distribution (ACD)

A system feature for the efficient distribution of large volumes of incoming calls received over specially configured lines.

Automatic Number Identification (ANI)

A feature available in the digital telephone network that enables HiPath 4000 users to identify external callers. ANI provides agents connected to HiPath 4000 with information on the caller and allows them to prepare themselves better for the call.

C

Call

All connections between two or more users, for example, a connection between an incoming trunk and an extension or between two or more extensions.

Call Center

A customer service center that is contacted by telephone. Call center staff often use terminals to access information databases.

Call Handling Services

Services that let the agent issue requests, such as Make Call, Clear Connection, Consultation Call, Transfer Call, and Answer Call over the telephony application.

CC-AP

Common Control Access Point - Specific HiPath / OpenScape 4000 hardware in Access Points to take care of local survivability for devices connected to the AP shelf (in case of failure of the HiPath / OpenScape 4000 server or the IP network).

Clear Connection

A service that clears down a call at a particular device.

Connectivity Adapter HiPath 4000 Application Connectivity Link

A synchronous bidirectional communication connection with which HiPath 4000 is connected to the LAN over the telephony server.

Connectivity Adapter HiPath 4000

A Unify product that can be used to integrate a HiPath 4000 system in various LAN environments.

Computer Supported Telephony Application (CSTA)

A standard developed by the ECMA (European Computer Manufacturers Association) for connecting computers to telephone systems.

Computer Telephony Integration (CTI)

An interface used by applications in the LAN to operate and monitor telephony functions in HiPath 4000.

Consultation Call

(1) Consultation connection (a connection where the user places the other party on hold in order to obtain information from a third party). (2) A service that lets a user place a call on soft hold at a device and set up a new call with the same device.

Coordinated Voice and Data Transfer

A feature that transfers voice and data simultaneously when transferring a call from one agent to another.

CSTA

See *Computer Supported Telephony Application*.

CSTA Link

A connection used to connect the HiPath 4000 to the telephony server.

CTI

See *Computer Telephony Integration*.

D

Dialed Number Identification Service (DNIS)

A customer network service in which the telephony application displays data specific to the station number dialed on the agent workstation.

DLS

Deployment and Licensing Server.

E

Enhanced Business Statistics

A feature that lets the application evaluate event stream data from the HiPath 4000 and generate caller statistics.

Event Stream

Information on calls that are generated by the HiPath 4000 system and forwarded to the telephony application. This information is used by the telephony application to determine agent availability and to support features, such as Intelligent Answering and Coordinated Voice and Data Transfer.

I

Intelligent Answering

A feature that causes the telephony application to display transaction or customer-specific data on the agent’s monitor when this agent initiates or receives a call.

IPDA

IP Distributed Architecture - HiPath / OpenScape 4000 architecture which allows for Access Points to be distributed via an IP network; they need not be directly connected to the HiPath 4000 server any more.

ISA

Industry Standard Architecture.

L

Local Area Network (LAN)

A communication network with multiple servers and workstations within a geographically confined area.

M

Make Call

A communication connection from one extension to another.

N

Network Interface Card (NIC)

A board connected to the telephony server and used to exchange data over a network.

P

Performance Data

Diagnostic data saved in a buffer and used to evaluate system performance on the basis of traffic data recorded during a specific period of time.

Port

An interface or access point on a computer or on another data terminal.

Profile

A group of parameter values that can be used to customize the software. The password used to access the system can be set, for example.

S

SCC

Service Call Control

SCI

Session Control Interface

T

TCP/IP

See *Transmission Control Protocol/Internet Protocol*.

Telephony Application

An application program that is executed in a LAN and executes - either directly or indirectly - telephony functions, such as station number dialing, call pickup and transfer or the processing of voice and data connections.

Trace Data

Diagnostic data saved in a buffer and used to trace back messages exchanged between HiPath 4000 and the LAN.

Traffic Data

Diagnostic data saved in a buffer documenting the number of messages exchanged between HiPath 4000 and the LAN within a specific time frame.

Transfer Call

A service that can be used to transfer a held call to another extension in the CBX.

Transmission Control Protocol/Internet Protocol (TCP/IP)

A network protocol that facilitates communication between computers with different hardware architectures and operating systems over interconnected networks.

Index

mitel.com