HiPath CAP
Common Application Platform

Service Manual

SIEMENS

Global network of innovation

Copyright and Trademarks

Hackers who unlawfully gain access to customer telecommunications systems are criminals. Currently, we do not know of any telecommunications system that is immune to this type of criminal activity. Siemens AG will not accept liability for any damages, including long distance charges, which result from unauthorized use. Although Siemens AG has designed security features into its products, it is your sole responsibility to use the security features and to establish security practices within your company, including training, security awareness, and call auditing.

Siemens sales and service personnel, as well as Siemens business partners, are available to work with you to help you guard against this unauthorized use of your telecommunications system.

Request Siemens publications from your Siemens representative or the Siemens branch serving you. Publications are not stocked at the address below.

Siemens AG
Hofmannstr. 51
D-81379 München
Tel.: +49 89 722-0
Fax: +49 89 722-44115

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 HiPath CAP, as well as typical configurations and installation scenarios.
- **Chapter 3** outlines the system requirements for HiPath CAP.
- **Chapter 4** describes how to install HiPath CAP components. This chapter describes the server components "CAP Management", "Call Control Services (SCC/SCCP)" and the two connectivity adapters CA4000 and CA300 as well as the client components "CAP Service Starter", "CAP TAPI Service Provider (TCSP)", and "Siemens 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 4000).
- **Chapter 5** introduces the CAP Management interface.
- **Chapter 6** describes how to configure the HiPath CAP components using HiPath CAP Management. This chapter explains how HiPath CAP is connected to HiPath 4000, HiPath 3000, HiPath 300, and other switching systems. It also describes how to configure the Media Service (MEB) and the XML Phone Service.
- **Chapter 7** contains an overview of the HiPath CAP Management functions.
- **Chapter 8** deals with diagnostics and error handling in the event of installation and runtime problems.
- **Chapter 9** explains the three operating modes supported by HiPath CAP, namely "single-domain/homogeneous/native mode", "multi-domain/homogeneous/native mode", and "multi-domain/heterogeneous/harmonized mode".
- **Appendix A** contains implementation details in relation to both the structure of the HiPath CAP software and the layout of configuration files and parameters.
- **Appendix B** describes how the server PC is connected to a HiPath 4000 or Hicom 300 communication system.

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 HiPath 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 HiPath CAP:

- HiPath CAP Application Developers' Guide Vol. 1-5 (incl. Base, CSTA III, JTAPI, TAPI)
- HiPath CAP Fault Management, Application Developers' Guide
- XML Phone Server V1.0, Application Developers' Guide
- HiPath CAP TAPI Service Provider, Service Manual
- Telas 3.1 Installation and Administration Guide

1.4 Layout conventions

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

This symbol indicates notes or recommendations.

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.

- Siemens employees should contact the support center responsible for their region.
- Customers are advised to contact the Siemens Customer Support Center.

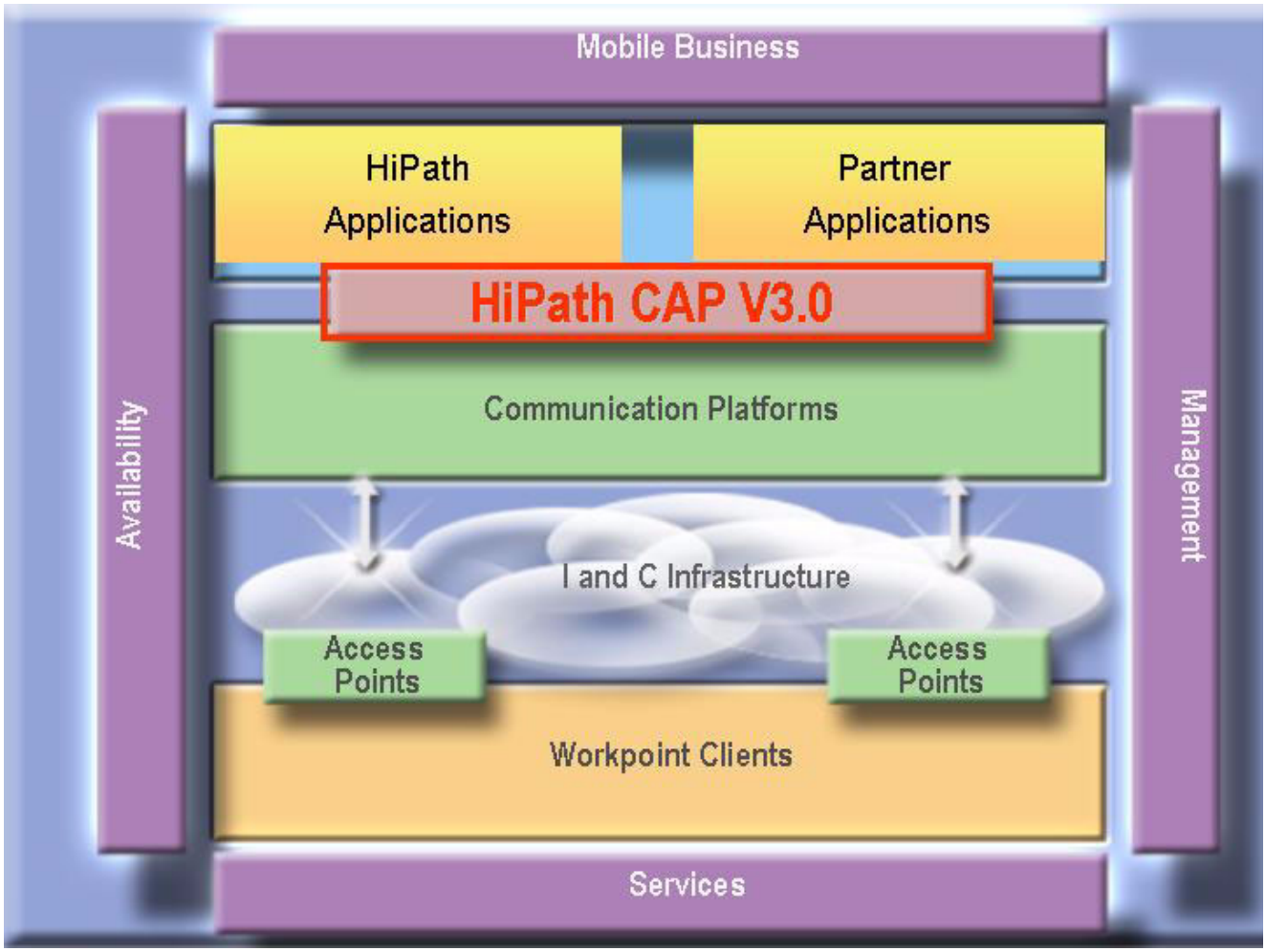
Please have the following information to hand so that the support center can quickly pinpoint the document you have a problem with:

- **Title:** HiPath CAP, Service Manual
- **Part number:** A31003-G9330-I100-2-7620

2 Overview

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

2.1 General role of HiPath CAP in the HiPath architecture



HiPath CAP is a central element in the HiPath architecture. It is a powerful middleware application and connects applications based on standard protocols, both with HiPath systems and third-party PBXs.

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

Services

- Flexible use of applications based on standards.
- CTI application support for clients in different infrastructures.
- Integration of HiPath CAP and applications in the HiPath Management system.
- Migration of infrastructure from the classic telephone network to the IP network that uses the same application.

Services for application partners

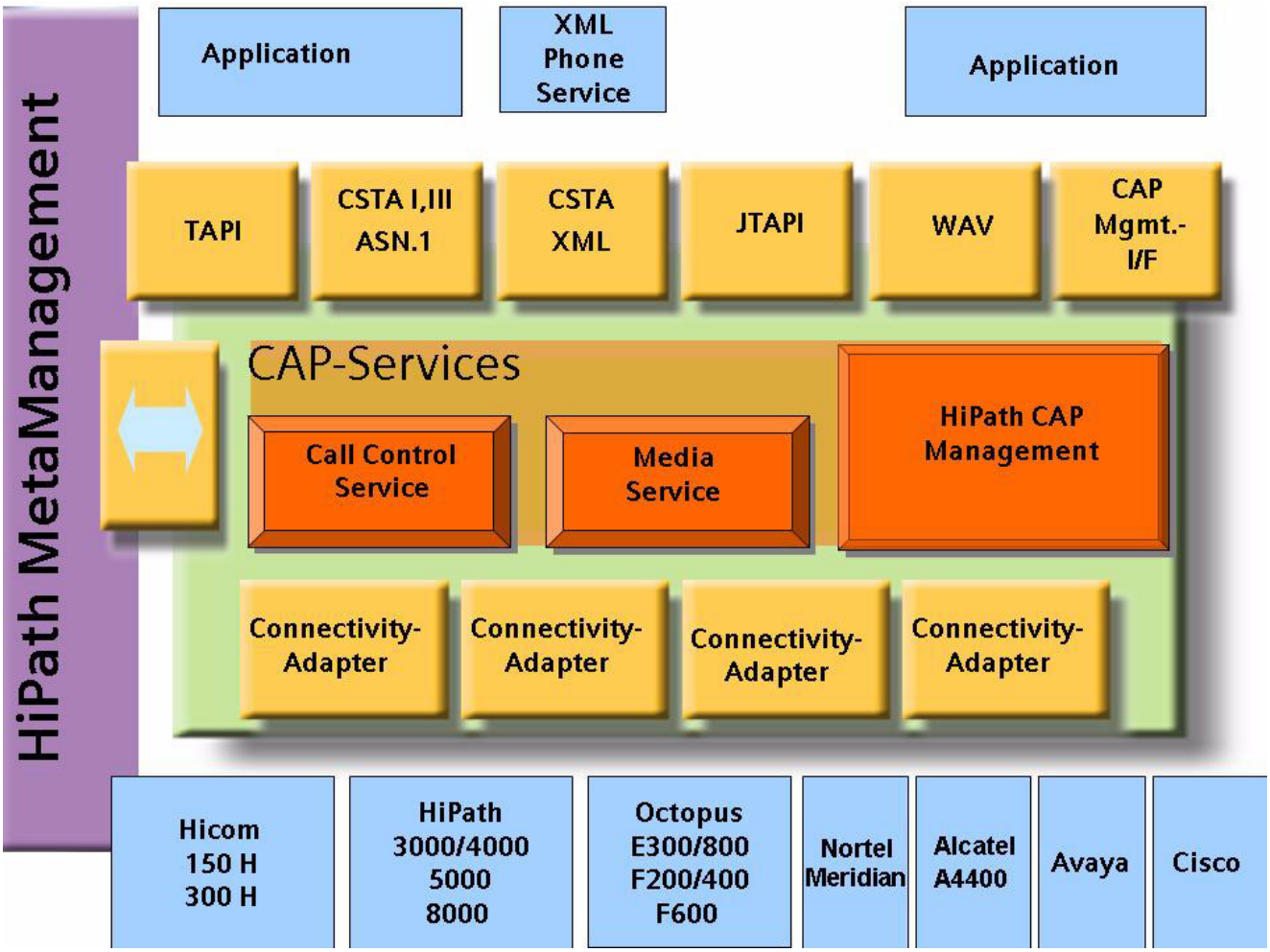
- HiPath CAP guarantees compatibility with a numerous telephone systems that operate using different technologies.
- Enhancement of individual applications with Serviceability Management and security features when using the services supported by HiPath CAP.
- Acceleration of application developments by linking individual applications to HiPath applications. This transforms them into a full component of the HiPath portfolio.

2.2 Features and overview of services

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

- standard APIs for application developers,
- application developments through the provision of services (for CTI), management, and licensing, available in an SDK (software development kit),
- migration from Hicom 300 E/H to HiPath 4000 with multiple connection to different communication platforms that make an application almost independent of the underlying infrastructure.

The following diagram shows the basic structure of HiPath CAP with detailed information on the protocols supported and encoding variants, the CAP-internal services, and a number of supported PBXs.



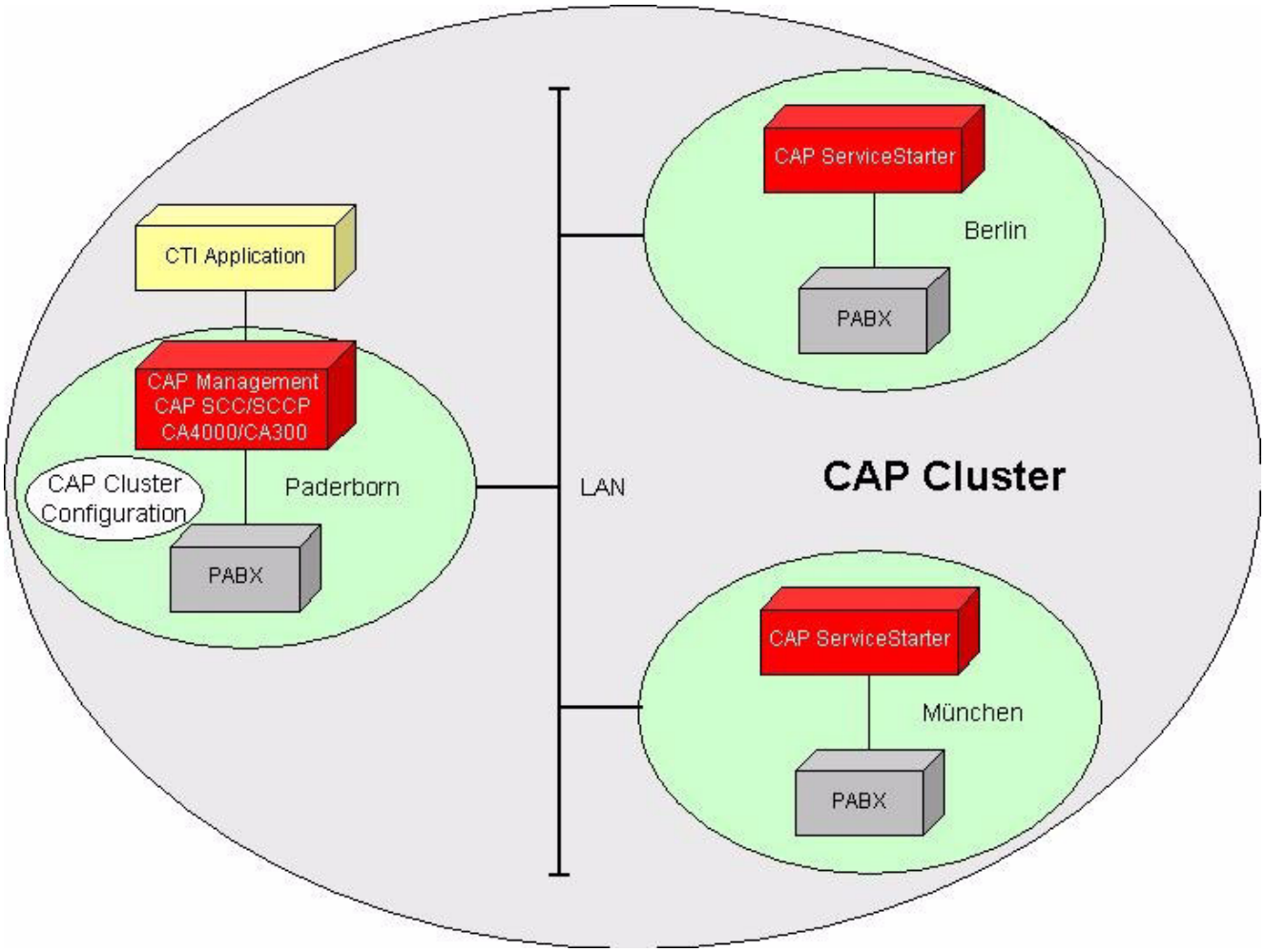
Highlights

- Standard protocols and APIs: Microsoft TAPI 2.x/3.0, Java TAPI, CSTA III ASN.1, CSTA XML, Microsoft Wave API
- Call Control Service (SCC) for CTI
  - Multi-domain features
  - Harmonization of the call model in Hicom 300 E/H, Hicom 150 H, HiPath 3000, HiPath 4000, HiPath 5000 V5.0, HiPath 8000, Octopus E300/800 Rel. 6.5/10, Realitis, Alcatel, Nortel Meridian, Cisco and Avaia - for TAPI- and CSTA-based applications
  - hiQ8000 integration with superior quality (in terms of reliability and number of subscribers configured)
- Media Service (MEB) for CTI
  - Media Streaming as a new HiPath CAP feature for applications
- Fault Management Service
  - Integration in HiPath Management (independent of CAP Management)
- License, User, and Configuration Management services
  - Uniform license structure
  - Integrated license and user management
  - Connection to the HiPath license server (CLS)
  - LM as a service for licensing HiPath CAP and applications in the same manner
- Support for special features
  - LiRus, AP emergency, XML PhoneServices

2.3 HiPath CAP Management

CAP Management is the central component in a CAP cluster. It administers and controls all processes and services in a "stand-alone" or distributed HiPath CAP installation. The cluster ID is a unique marker that identifies CAP components in the same CAP cluster.

The following diagram illustrates the location and configuration of the individual CAP components both in a "stand-alone" installation and in a distributed installation.



CAP Management is started by the Windows service **Siemens HiPath CTI** and provides a Web-based interface for administration.

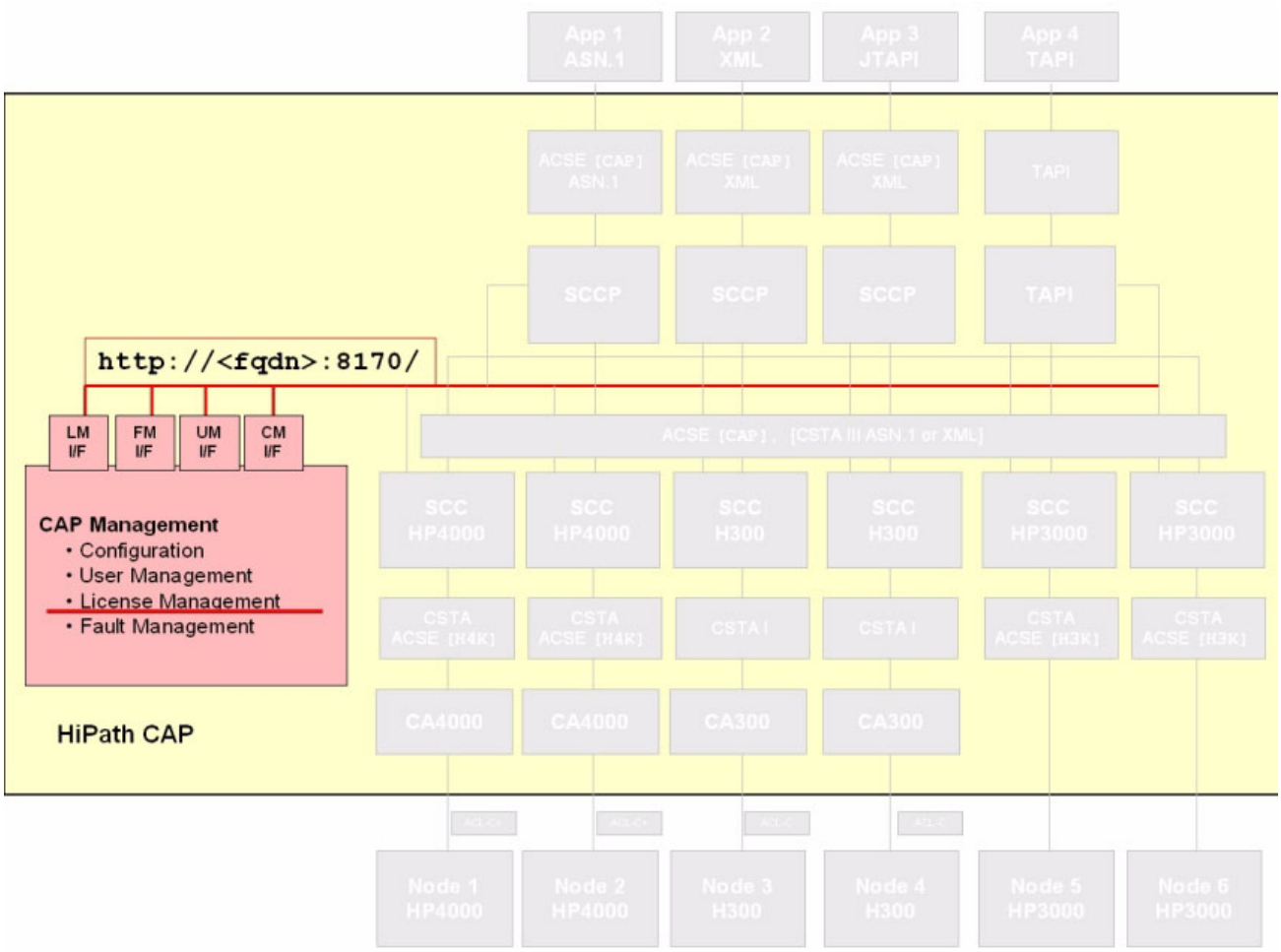
CAP Management tasks

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

HiPath CAP Management services

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

- Configuration Management (SCM)
- User Management (SUM)
- License Management (SLM)
- CallIdRepository
- Address Translation Service (SAT)
- 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 HiPath CAP Fault Management. This service will be dealt with later in greater detail.

Important HiPath CAP Management services, such as, SCM, SUM, and SLM are addressed by HTTP requests. These are first used internally by other services (SCC, SCCP, CAP TCSP) without being directly visible for 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 HiPath CAP Configuration Management (SCM)

The various PBXs that are connected to the CAP are administered in HiPath 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. Every SCC is assigned a unique service node ID that can be random except in cases where user data is imported at a later point where you have to use a specific ID. 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, see Chapter 7, "Further HiPath CAP Management Functions". Further functions of HiPath CAP Configuration Management are described in Chapter 7, "Further HiPath 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 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 SimplyPhone for Web or ComAssistant also uses this function as an external application.

2.3.2 HiPath CAP User Management (SUM)

User Management is the main component of HiPath 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 users as described in Section 7.2, "User" and Section 7.3, "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>&pass-wd=<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 SimplyPhone for Web or ComAssistant also uses this function as an external application.

2.3.3 HiPath CAP License Management (SLM)

License Management is used by HiPath CAP components and applications based on HiPath 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. All other license keys are equivalent to the CAP-A license. Application-specific licenses can consequently be used. These are supported by the HiPath CTI applications SimplyPhone for Web (SimplyPhone W), SimplyPhone for Outlook (SimplyPhone O), SimplyPhone for Lotus Notes (SimplyPhone N), and ComAssistant (ComASS). "XPhone" (c4b) is the first external application to use CAP License Management.

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

The HiPath CAP V1.0 license "UNKNOWN" which licensed the number of monitor points to be set in a CA4000 is not needed 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 and therefore does not require a separate license.

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.
Third-party system (CAP-F):	In addition to the CAP-S and CAP-A licenses, application-specific licenses are required if the device is in a third-party system and a monitor point is to be set. For a CAP-E license, an additional CAP-F license is **not** needed.
Media Streaming (CAP-M):	Media Streaming support for the MEB.

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

CAP Client License		per channel	1	10	25	100	Client Site >500
Entry	*CAP-E*			X	X	X	
Standard	*CAP-S*			X	X	X	X
Advanced	*CAP-A*			X	X	X	X
Media	*CAP-M*	X					
External Switch	*CAP-F*		X				
CAP inside	**for Siemens Com Applications** - HiPath ProCenter - HiPath SimplyPhone Family - HiPath Display Telephone Book - HiPath Hotel - Attendant Supervisor Console - Busy Lamp Field - ... and other planned applications These applications come with their "CAP Client License" included						

An application must register first with CAP (authentication) by specifying an application ID. This application ID must match the installed license's ID. License verification is performed for every request sent by this application to the CAP for a specific CTI user. If the relevant client license is assigned to this CTI user, the request is forwarded to the PBX.

The CAP components use the HTTP request
`http://<fqdn>:8170/mgmnt/Admin/req?registerLicense=<ApplicationID>&userId=<DeviceID>`
to check if a CTI user was assigned a required license before they can forward a request. External applications can also use the same request to check if a user configured in the specific application was 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 this CTI user are rejected.

2.3.4 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.

2.3.5 Address Translation Service (SAT)

The "Address Translation Service (SAT)" is responsible for always administering the call number in canonical format in communication between an application and the SCCP.

- It converts a dialed call number in canonical format into a dialable number.
- It converts a call number in canonical format into a PBX call number in accordance with the overlap configuration and vice versa.
- It converts the call number transmitted in an event from the formats "extension", "NAC number", "PNP number" into canonical format so that an application can always uniquely assign this event to a device.
- The call number configured in CAP is converted into the HiPath 4000 LODEN number for addressing in HiPath 4000 devices (trunks, RCG groups, hunt groups).

2.3.6 Open LDAP Server

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

2.3.7 HiPath CAP Fault Management (SFM)

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

CA4000/CA300 is the only HiPath CAP component that currently uses HiPath CAP Fault Management.

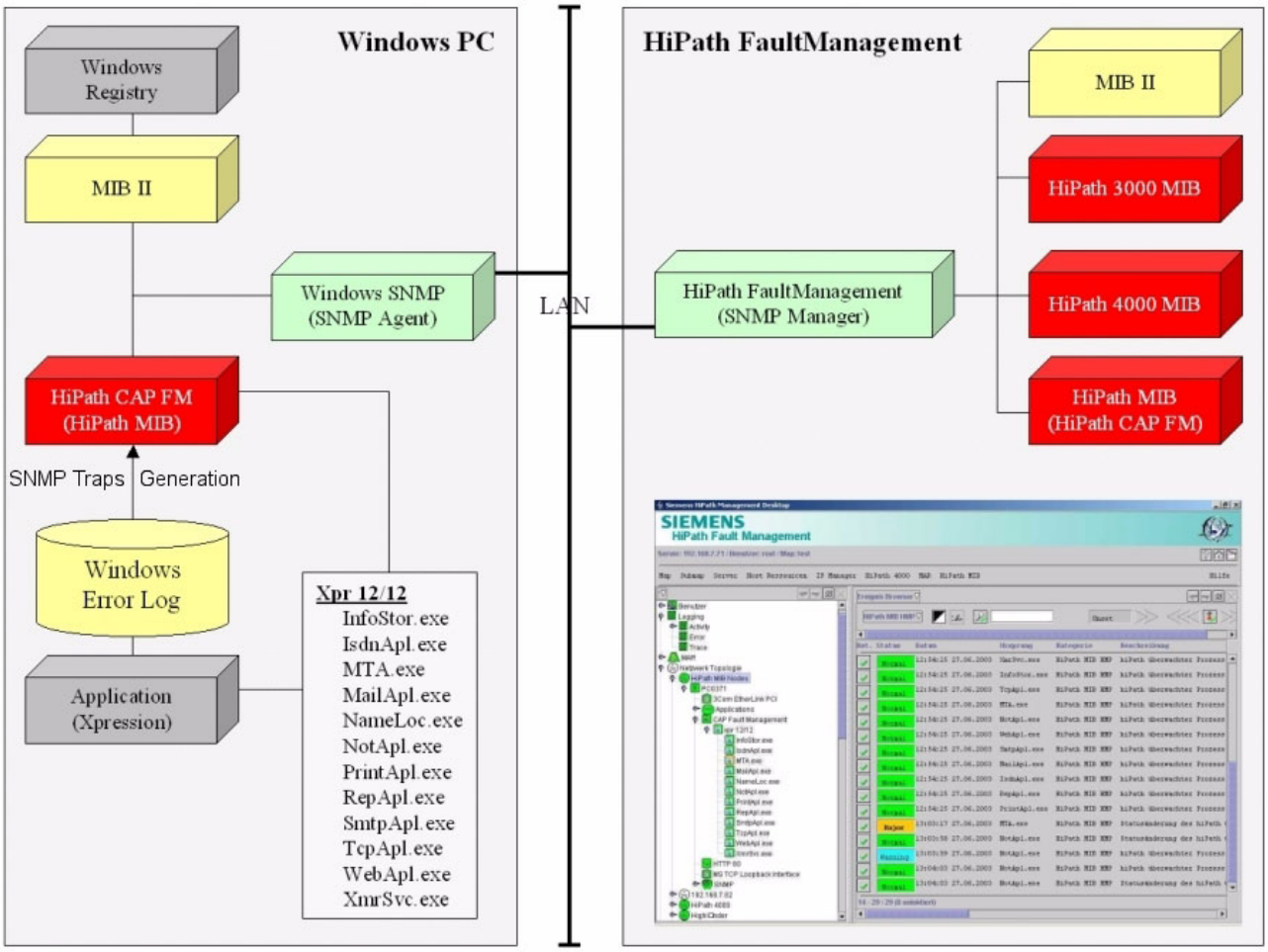
HiPath CAP Fault Management consists of six DLLs. Rather than a stand-alone service, it is connected to the Windows SNMP service. Windows-based programs can be managed by HiPath Fault Management by integrating this DLL. An ADG is provided for this.

CAP FM supports the following features:

- Auto Discovery
- HiPath MIB-based information
- Trap notification

In addition to the information available via MIB II, HiPath Fault Management contains information on the CAP FM applications supported and the processes to be monitored. In the HiPath 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 HiPath Fault Management for a Windows PC with an active SNMP agent, Xpressions 450 installed, and integrated HiPath CAP FM.



Administration of CAP with HiPath Fault Management

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

2.4 HiPath CAP operating modes

HiPath CAP supports three different operating modes. 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".

Single-domain/homogeneous/native mode

Hicom 300: CSTA I ASN.1

HiPath 4000: CSTA I ASN.1, CSTA III ANS.1, ACSE (CSTA III ASN.1)

HiPath 3000: ACSE (CSTA III ASN.1)

Multi-domain/homogeneous/native mode

HiPath 4000/HiPath 3000: ACSE (CSTA III ASN.1)

Multi-domain/heterogeneous/harmonized mode

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

2.4.1 Explanation of terms

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

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

Applications are currently being developed for **multi-domain, homogeneous, native mode**. An application must support CAP's new ACSE_AARQ, extensions in long canonical format, and call IDs containing eight bytes.

Multi-domain heterogeneous harmonized mode is used in modified form by the Phone Controller in SimplyPhone for Web and 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.

2.4.2 Simplification of nomenclature

To simplify complex name assignment (which is certainly advisable), use the following rule:

>> heterogeneous and native mode are mutually exclusive. <<

Native mode which supports proprietary protocol elements as well as standard and private services, is only possible in a CAP configuration with PBXs of the same type (homogeneous). The operating modes can consequently be described as follows:

Single-domain//native mode

Multi-domain//native mode

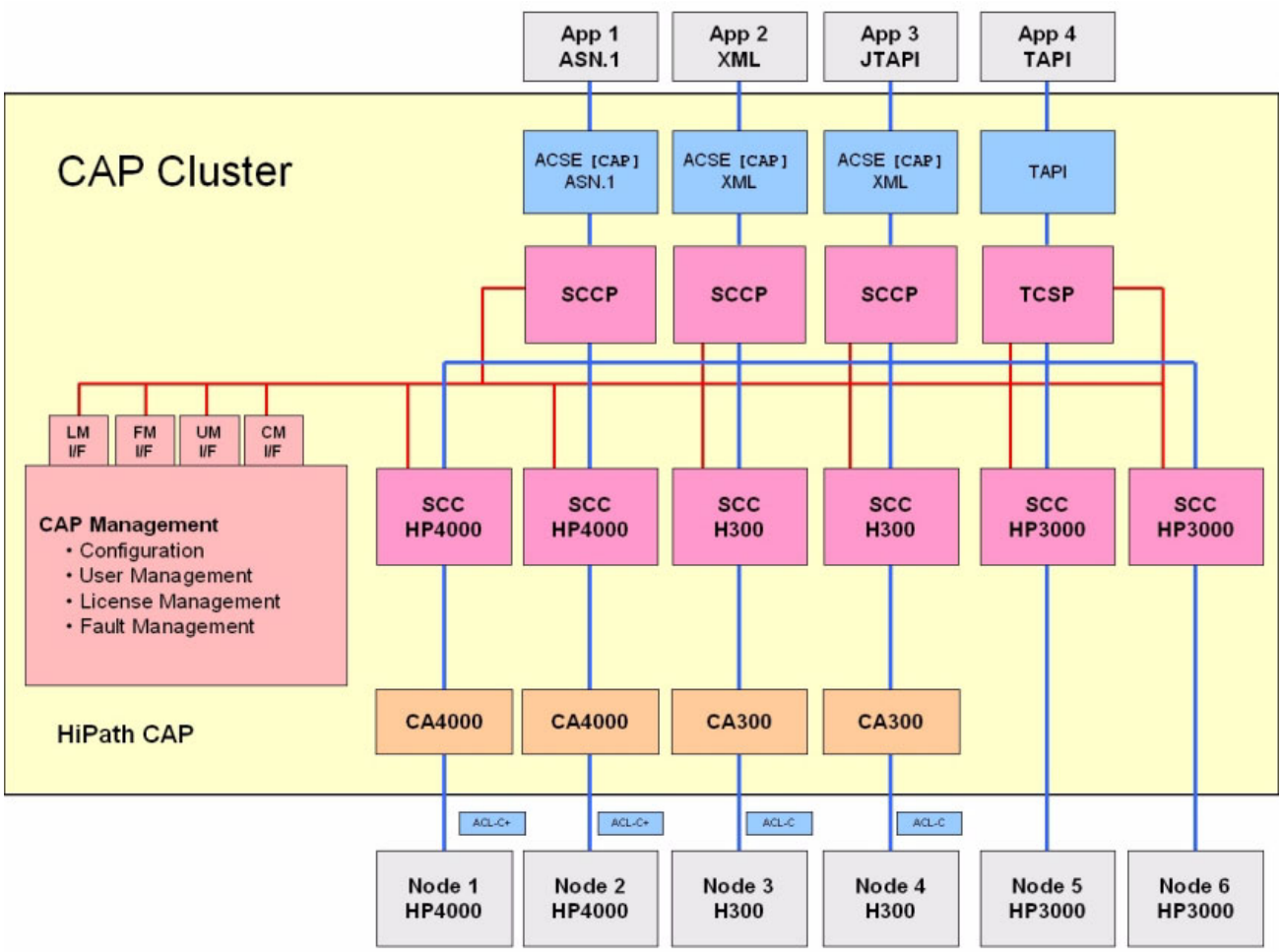
Multi-domain//harmonized mode

For detailed information on the services supported, refer to the HiPath CAP prospectus, the HiPath CAP Technical Information or the HiPath 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.

2.5 HiPath CAP components

The components SCC, SCCP, CA4000, CA300, 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".



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:

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

An application must authenticate itself at SCCP with a valid CAP username/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's SLM for this. The SCCP saves successful CTI user license verification actions every 3600 seconds.
The CSTA version defines the type of CSTA III encoding in which the following requests are transmitted.
The CSTA III XML protocol is used for communication with the JTAPI application. The JAR files supplied by CAP must have been implemented 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 configured in "native mode" or "harmonized mode". 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 with an SCC. 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. Every SCC continues to be assigned the call numbers of the PBX connected.
The CSTA ASN.1 protocol is used for communication with a PBX.

SSC configuration parameters

In **multi-domain//mode**, the protocols and the encoding variants CSTA III ASN.1, CSTA III 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. The protocols supported now depend on the PBX type.

To connect applications to HiPath 3000, an SCC is permanently configured in the "ACSE (CSTA III ASN.1)" protocol.

To connect applications to HiPath 4000, an SCC is permanently configured in one of the three different protocol variants "CSTA I (ASN.1)", "CSTA III (ASN.1)" or "ACSE (CSTA III ASN.1)".

To connect applications to HiPath 300, an SCC is permanently configured in the "CSTA I (ASN.1)" protocol.

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. SCCHicom300 connects to CA300.

2.5.3 The Connectivity Adapter 4000 (CA4000)

CA4000 converts the proprietary HiPath 4000 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 I, 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. The port bandwidth (1025 - 5000) can be used.

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

2.5.4 The Connectivity Adapter 300 (CA300)

CA300 converts the proprietary Hicom 300 protocol (ACL-C) into a standardized protocol (CSTA). The connection to Hicom 300 can be set up over ATL, the WAML and the SL100. CA300 supports CSTA links in ASN.1 encoding.

CA300 configuration parameters

The IP address of Hicom 300 is configured for the connection to Hicom 300. A PBX link number and a sub-application number are configured for communication with HiPath 300. The port bandwidth (1025 - 5000) can be used. CA300 is always configured together with the associated SCC in CAP Management.

PROBLEMS WITH CA300 AND WINDOWS SERVICES:
Note that Windows Task Scheduler and the Windows logon service seize ports that lie in the range 1025 - 1299 and that can vary every time the relevant service is restarted.

2.5.5 The CAP TAPI Service Provider (CAP TCSP)

CAP TCSP is a CAP component that supports "multi-domain//harmonized mode". It supplies the CAP TAPI Service Interface (TSPI) for applications based on Windows TAPI. Its multi-domain capability is based on the use of CAP's SCM and communicates directly with the SCC over a proprietary protocol (NetTSPI). Simultaneous connection with multiple SCCs. Implementation in conjunction with a TAPI server and a terminal server is restricted. As a rule, it is always installed locally on a client.

CAP TCSP configuration parameters

CAP TCSP is installed via the master setup using a separate menu item (Client 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", "CAP-A", "CAP-S" and ends with "CAP-E". TAPI applications can supply individual application IDs for licensing.

2.5.6 HiPath CAP Media Service - The Media Extension Bridge (MEB)

The HiPath CAP 3.0 Media Service is a software component that simulates a PBX with subscriber line interfaces (one subscriber per channel). This must be done by configuring a Cornet-NQ connection between the Media Service component MEB (Media Extension Bridge) and a HiPath 4000 HG3550 V2 or HiPath 3000 HG1500 V2. For Microsoft TAPI-based applications, the "wave/in" and "wave/out" features for playing and recording WAV or AVI files in 8 KHz/16 bit/mono format and the "Receive fax"/"Send fax" features are supported. Accordingly, an application is provided with "incoming call pickup" and "outgoing dialing" features for these functions.

The media service mainly consists of three components:

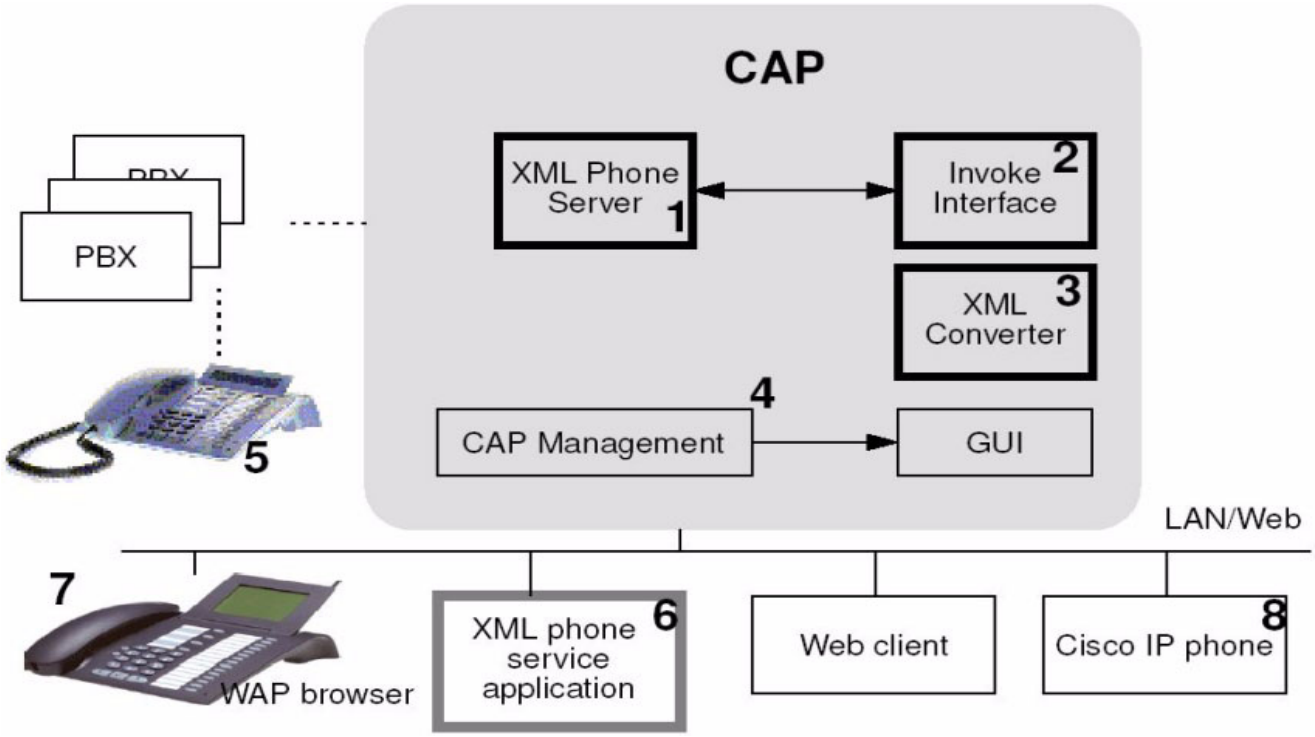
- **Siemens Virtual Wave Driver**
  A virtual driver for outputting or recording IP audio data using the Windows Wave API; similar, for example, to a sound card driver (for driver installation, see Section 4.7, "Installing the Siemens Virtual Wave Driver").
- **MEB (Media Extension Bridge)**
  A central component for controlling the Siemens Virtual Wave Driver and for receiving, evaluating, and forwarding all relevant data between HiPath and applications via SCCMEB and CAP TCSP.
- **SCCMEB**
  A component for connecting CAP TCSP with the MEB.

The "Siemens Virtual Wave Driver" should always be installed locally on the PC where you want to run SCCMEB and MEB. The SCCMEB and MEB components are distributed after the standard routines of the distributed installation, which means that the "CAP ServiceStarter" must also be installed on this PC. Currently, a maximum of 30 simultaneous calls (channels) can be administered per MEB PC, assuming that there are enough CAP-M licenses available.

2.5.7 The XML Phone Service (XMLPS)

As an application, the "XML Phone Service (XMLPS)" is 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 as input/output devices (OpenScape and ComAssistant use 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:

- **HiPath CAP XMLPS Phone Server Process** (sxmlps.exe)
  This process is the component that connects SCCP.
- **HiPath CAP XMLPS Invoke Interface**
  This interface is used to operate the terminals (display, key LEDs)
- **HiPath 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:

- **EasySee**
  Lets you run a search in an LDAP server and shows the names and, where applicable, other information on all parties involved in the call on the telephone's display.
- **Easy Lookup**
  Opens a "phone card" in Internet Explorer and shows all available data to the party connected to a call.
- **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.

3 System Requirements

This chapter describes all hardware and software requirements for installing HiPath CAP. Some CAP component can 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 integrated in a shared network.

3.1.1 Central server PC (for CAP Management)

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

Minimum requirements

- Pentium III processor with at least 800 MHz
- At least 512 MB main memory
- Approx. 500 MB free hard disk memory
  CAP Management and the Call Control Services requires approximately 300 MB of this space. The remaining 200 MB were needed for log files.

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
Media Services	**Call Control**	
no	small	A
no	medium	A
no	large	B
no	very large	C
small	no	A
small	small	A
small	medium	A
small	large	B
medium	small	A
medium	medium	B
medium	large to very large	C

Call Control

- small up to 100 users
- medium up to 500 users
- large up to 2,000 users
- very large up to 20,000 users

Media Services

- small up to 12 channels
- medium up to 30 channels
- large up to 60 channels (two PCs required)
- very large up to 240 channels (multiple PCs required)

PC type

- A Pentium III 800 MHz/512 MB RAM/40 GB HD (minimum requirement)
- B Pentium 4 2.6 GHz/1 GB RAM/60 GB HD or dual processor
- C Distributed system consisting of PC types A or B

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 HiPath 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

- Approximately 50 MB of disk space
- Pentium III processor with at least 800 MHz
- At least 512 MB main memory

3.1.3 Communication system

Ensure that the communication system (e.g. HiPath 4000, HiPath 3000, Hicom 300, etc.), with which HiPath CAP is to operate, is fully functional. One of the connection options supported by the communication system and HiPath CAP must be available (for example, over a TCP/IP connection).

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

- Windows 2000 Professional or Server
- Windows 2003 Server
- Windows XP Professional

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 HiPath 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 5.0 and above
- Netscape Navigator 7.x and higher
- Mozilla 1.x and higher

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 4.7 is no longer supported.

3.3 Additional installation conditions

- 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 one of the cluster IDs assigned to CAP Management is not used by another CAP Management server in the same IP network.

4 Installation

This chapter explains the entire installation of HiPath CAP. The following components can be installed:

Server components

- CAP Management 3.0
- CAP Call Control Service 3.0
- Connectivity Adapter CA4000
- Connectivity Adapter CA300

Client components

- CAP TAPI service providers
- CAP Service Starter 3.0

This chapter is structured as follows:

- **Section 4.1** describes how to install the CAP server components HiPath CAP Management 3.0 (including Configuration, License, and User Management), HiPath Call Control Services 3.0 and the connectivity adapters CA4000/CA300.
- **Section 4.2** describes distributed installation.
- **Section 4.3** describes how to install HiPath CAP Service Starter 3.0.
- **Section 4.4** provides helpful hints about CAP installation.
- **Section 4.5** describes the start sequence for CAP processes in non-distributed and distributed Installation.
- **Section 4.6** describes how to install CAP TAPI Service Provider 3.0.
- **Section 4.7** describes how to install the Siemens Virtual Wave Driver which is a virtual sound card for the Media Service component.
- **Section 4.8** covers the special features during installation, e.g. if you want to modify the IP address at a later date, or need to deactivate services.
- **Section 4.9** explains how to migrate the old TelasAdmin, HiPath CAP V1.0 or CAP V2.0 data to HiPath CAP V3.0.
- **Section 4.10** covers data security, including backup and restore.
- **Section 4.11** describes how to uninstall HiPath 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.

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 HiPath CAP Configuration Management cannot fully prevent technically nonsensical combinations of SCC instances.

The data medium (CD) contains a master installation `setupMaster.exe` for all of the software components contained on the CD. This allows you to select and perform one or more installations simultaneously by simply clicking the required components.

Installation sequence

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

1. Obtain licenses for HiPath CAP and applications.
2. Install HiPath CAP Management and HiPath CAP services - this involves configuring the necessary set of Call Control Services (SCCs) with suitable Connectivity Adapters (CAs) and connecting them to the switching host.
3. You may have to configure SCCPs, depending on the application to be installed.
4. Install licenses via CAP Management.
5. Configure or import devices.
6. Configure or import users and assign devices.

In case an application is to be installed directly afterwards:

7. Install applications.

Requirements

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

- Do you have all licenses for HiPath CAP?
- Has a Web browser been installed and configured correctly (Internet Explorer, Netscape Navigator)?
- Does this browser support cookies and JavaScript? Are cookies allowed and is JavaScript enabled?
- Does the PC have a valid IP address or is it entered in the DNS?
- If a previous version of HiPath CAP Management or TelasAdmin is already installed, proceed as described in Section 4.9, "Migrating from TelasAdmin 4.1 / HiPath CAP 1.0 / HiPath CAP 2.0 Management".
- The person performing the installation must have administrator rights on the PC.

4.1 Installing the server components

The following server components should be installed on the server PC:

- CAP Management 3.0:
  CAP Management can be used to configure HiPath CAP and the HiPath CAP services.
- CAP Call Control Service 3.0:
  Use the CAP Call Control Service to install the components **HiPath Call Control Service** (SCC), **HiPath CAP Call Control Proxies** (SCCP), **HiPath Media Service** (MEB), and **XML Phone Service** (XMLPS). (Chapter 6, "Configuration with HiPath CAP Management" explains how to configure these services.)
- The connectivity adapters for Avaya and Nortel Meridian are automatically installed with HiPath Call Control Services 3.0.
- Connectivity Adapter CA4000 (if a HiPath 4000 is connected):
  Some communication systems require a connectivity adapter to connect to HiPath CAP. Install the **Connectivity Adapter CA4000** component if a HiPath 4000 is connected to HiPath CAP. Section 6.1, "HiPath 4000 connectivity" describes how to configure Connectivity Adapter CA 4000.
- Connectivity Adapter CA300 (if a Hicom 300 is connected):
  Some communication systems require a connectivity adapter to connect to HiPath CAP. Install the **Connectivity Adapter CA300** component if a Hicom 300 is connected to HiPath CAP. Section 6.4, "Hicom 300 connectivity" describes how to configure Connectivity Adapter CA 300.

Performing the installation

1. Insert the installation CD in the CD/DVD drive of the relevant PC. If Setup does not start automatically (i.e. autorun is not enabled), double-click the following file:

   `<CD/DVD drive>:\setupMaster.exe`

2. Confirm the welcome dialog with **Next** and agree the licensing conditions by clicking **Next**.
3. Select **Install Server Components** and checkmark the following list entries:
   - **CAP Management 3.0**
   - **CAP Call Control Service 3.0**
   - **Connectivity Adapter CA4000** (if a HiPath 4000 is connected)
   - **Connectivity Adapter CA300** (if a Hicom 300 is connected):
4. Click **Next**.
5. Follow the instructions.
6. You can change the installation directory if necessary during installation.

   The default installation directory is "`Program Files\Siemens\HiPathCTI`".

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

   The installation directory will be referred to as *<InstDir>* from this point on.
7. An older version of HiPath CAP Management V3.0 will be migrated automatically. Data from HiPath CAP Management V2.0 will also be migrated automatically (siehe Section 4.9.3, "Migrating HiPath CAP V2.0 to HiPath CAP V3.0").
8. The server 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:

   `C:\Program Files\Siemens\HiPathCTI\config\Start\startNT.cfg`

The entry is:

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

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

9. 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, only the IP address of this card is listed.

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

   `C:\Program Files\Siemens\HiPathCTI\config\Start\startNT.cfg`

   The entry is:

   ```
   args: -localAddr

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

   `C :\Program Files\Siemens\HiPathCTI\config\common\global.cfg`

   The entry is:

   ```
   <?x set INST_HOST = "<PC name>" ?>

   <?x set INST_IP = "<IP address>" ?>
   ```

   `C:\Program Files\Siemens\HiPathCTI\/startMenu/startPageAdmin`
   Adapt the URL behind the link as underlined
   `http://<PC-Name>:8170/`

   These entries can be manually modified after installation and are active when the "Siemens HiPath CTI" service is restarted.

10. Conclude installation by following the final instructions on the screen.
11. Restart the PC.

The server components **HiPath CAP Management**, **HiPath Call Control Proxy** (SCCP), and **Call Control Service** (SCC) are now available on the PC. Chapter 6, "Configuration with HiPath CAP Management" explains how to configure these components.

If HiPath CAP is connected to either of the two communication systems HiPath 4000 or Hicom 300, you installed the associated connectivity adapter on the PC. Chapter 6, "Configuration with HiPath CAP Management" explains how to configure the connectivity adapter.

Check that installation has been successful

Once the "Siemens HiPath 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.

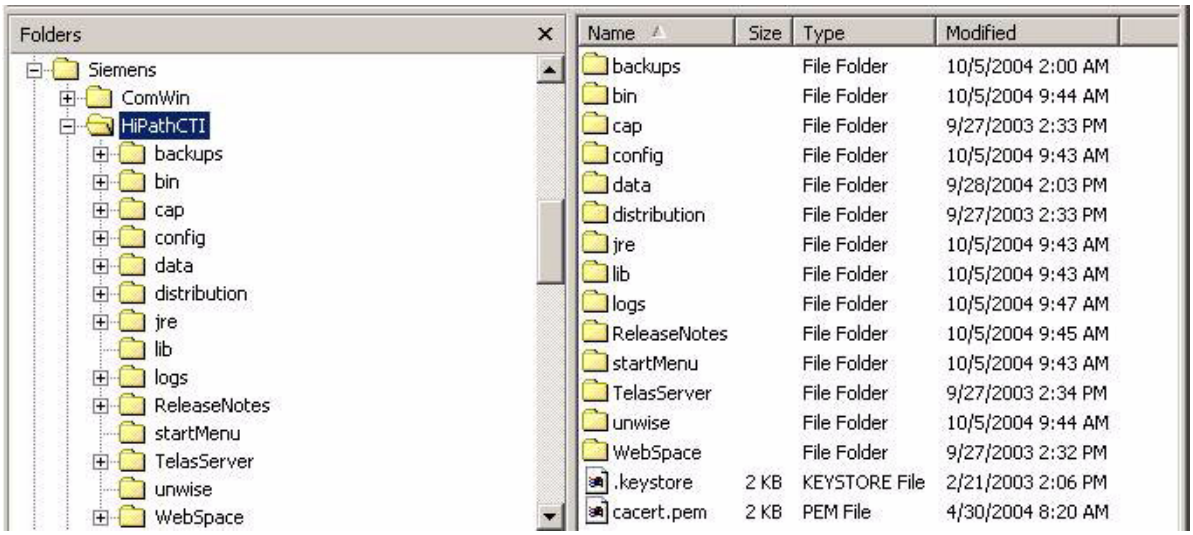
1. Select **Control Panel | Administrative Tools | Services** to check if the new Windows service "Siemens HiPath CTI" was added. Do this by starting the "`Siemens HiPath CTI`" service as follows:
2. Set up a connection to HiPath CAP Management in a Web browser by selecting **Start | Programs | Siemens HiPath CTI | 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 `C:\Program Files\Siemens\HiPathCTI\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 "Siemens HiPath CTI" service. CAP Management can now be addressed over the default port `8470`:
`https://<CAP Management PC>:8470/`.

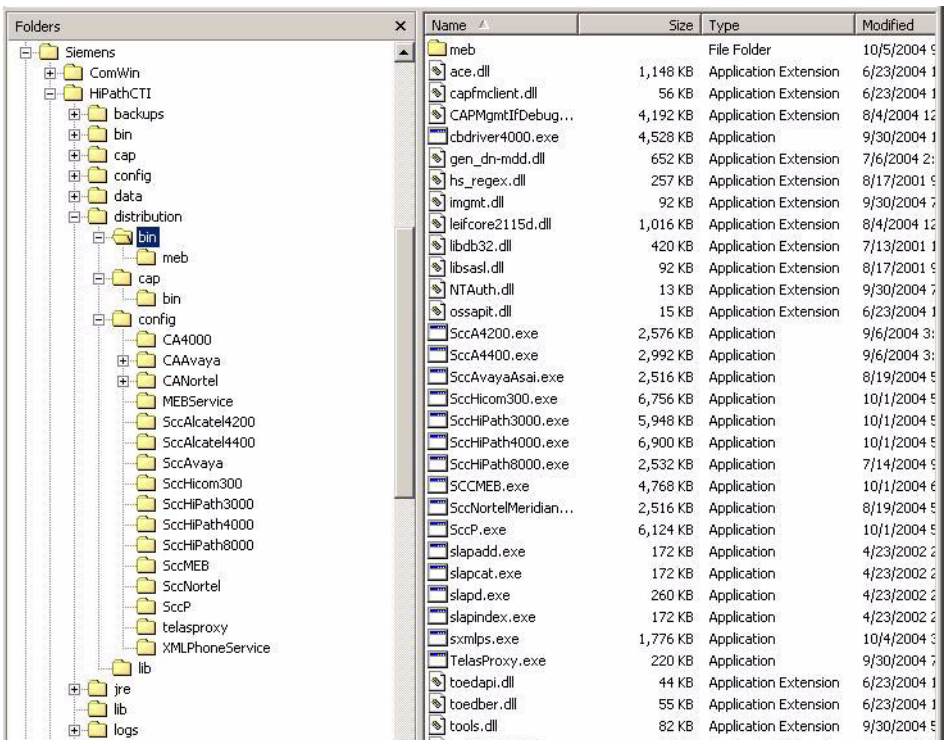
Log on to HiPath CAP Management entering **`Admin`** as the user name and **`Admin`** as the password. Please note that these are case-sensitive. The user name and password should be changed later. If data from a previous version has been migrated, the password for the old version will, of course, still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

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

3. Check the CAP Management installation directory. The default installation directory is `C:\Program Files\Siemens\HiPathCTI\`



4. Check the CAP Call Control Service installation directory. The default installation directory is `C:\Program Files\Siemens\HiPathCTI\distribution\`

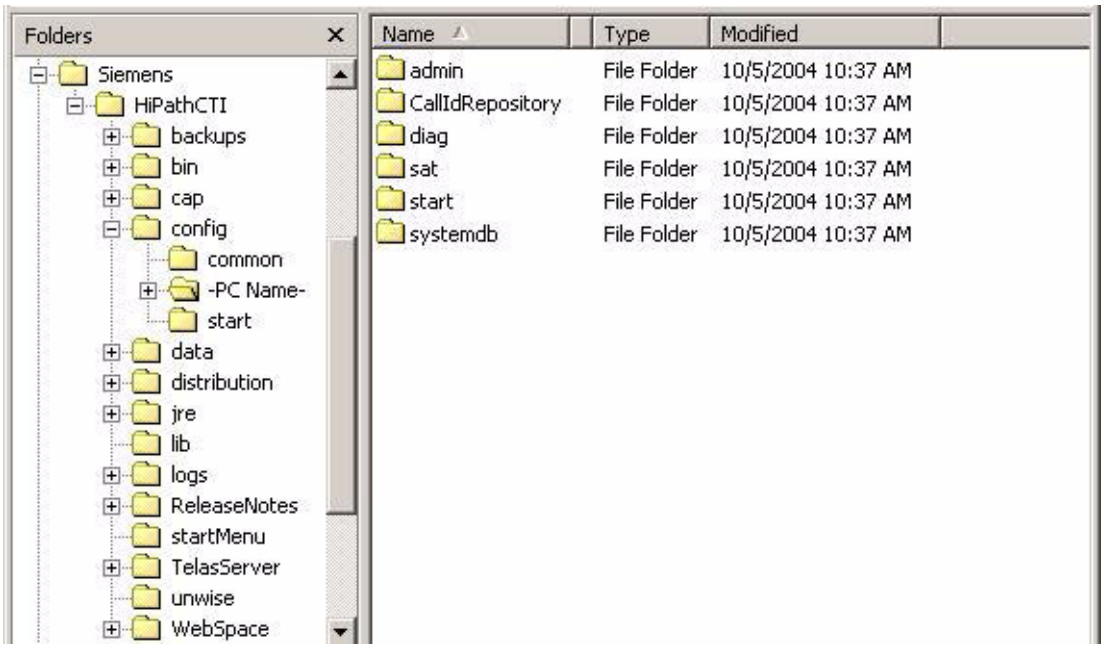


The `distribution` directory contains additional subdirectories, such as, `distribution\bin` and `distribution\config`.

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.

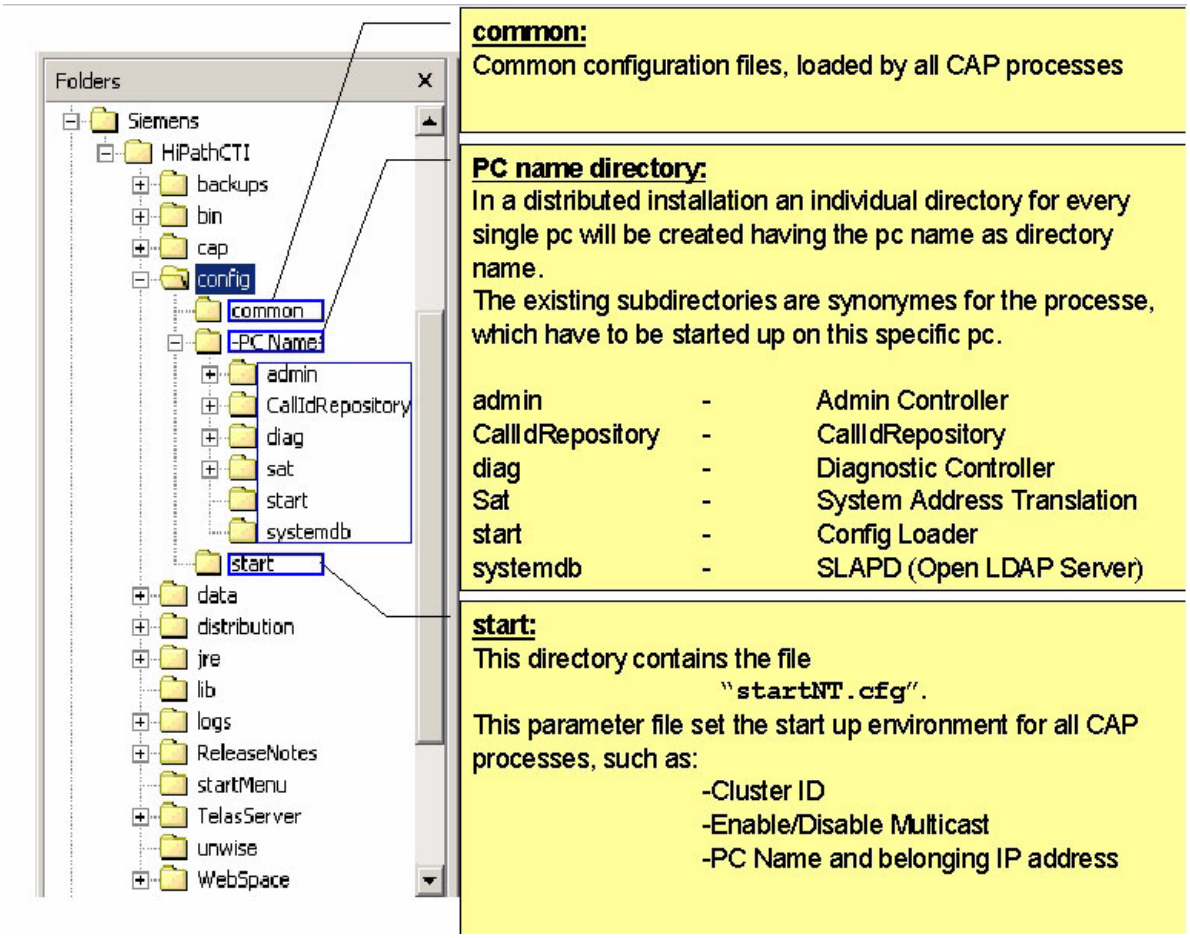
From here, the SCC/SCCP is distributed among the entire CAP cluster depending on the configuration. That is, the SCC/SCCP component is only ever installed once on the CAP Management PC, irrespective of whether or not one of these components is later active. The executable SCC/SCCP program can be replaced 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 same structure and the same relationship also apply for Media Extension Bridge (MEB) and the XML Phone Service (XMLPS).

5. Check the storage location of the configuration files. All configuration files in a CAP cluster can be found in the directory
   `C:\Program Files\Siemens\HiPathCTI\config\`



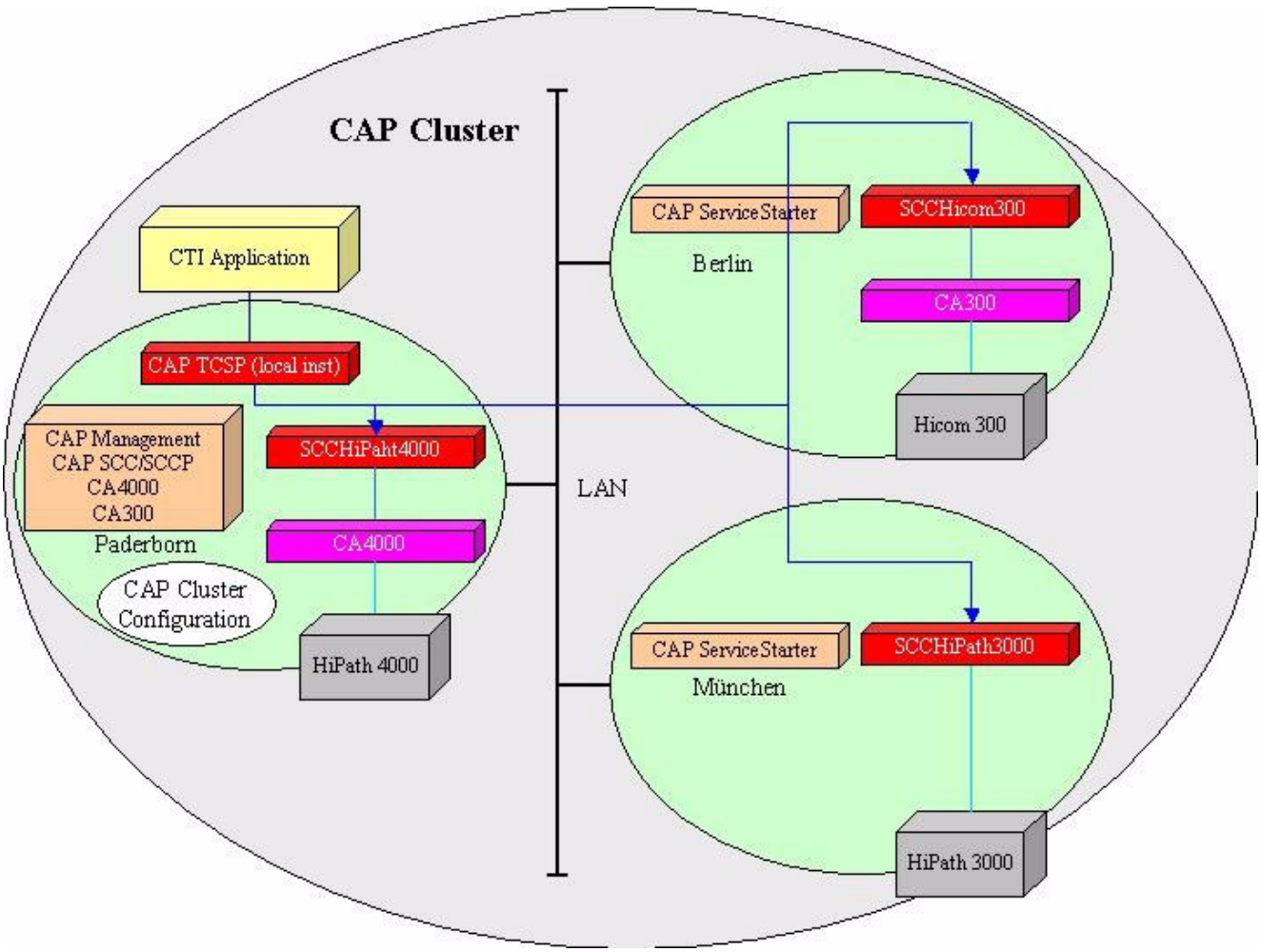
The configuration files are only ever stored on the CAP Management PC - even in the case of distributed installation.

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



4.2 Distributed installation

To satisfy network load requirements, you can set up a distributed installation if you want to connect an application over one CAP with multiple PBXs in a number of different locations. CAP Management is only installed with the CAP Call Control Services (SCC/SCCP) and the CA4000 and CA300 (if needed) at a single location. This is irrespective of whether you to run one or more SCCPs/SCCs (and CA), MEB or XMLPS in future on the CAP Management PC.



4.3 Installing the HiPath CAP Service Starter

To enable the HiPath Call Control Proxies and Call Control Services to be started correctly on the defined PCs, **HiPath CAP Service Starter** should be installed on each of these PCs.

Performing the installation

1. Insert the installation CD in the CD/DVD drive of the relevant PC. If Setup does not start automatically (i.e. autorun is not enabled), double-click the following file:

   `<CD/DVD drive>:\setupMaster.exe`

   > To install the HiPath CAP Service Starter you can also start the `setupStarter.exe` installation program from a subdirectory on the CD.

2. Confirm the welcome dialog with **Next** and agree the licensing conditions by clicking **Next**.
3. Select **Install Client Components** and checkmark the **CAP Service Starter 3.0** entry.

   > You can also select and install additional list entries together with CAP Service Starter. The additional components are installed in the right sequence as described in the chapters dealing with the various components.

4. Click **Next**.
5. Follow the instructions.
6. During installation, you will be prompted to specify the installation location. Select the desired installation directory.

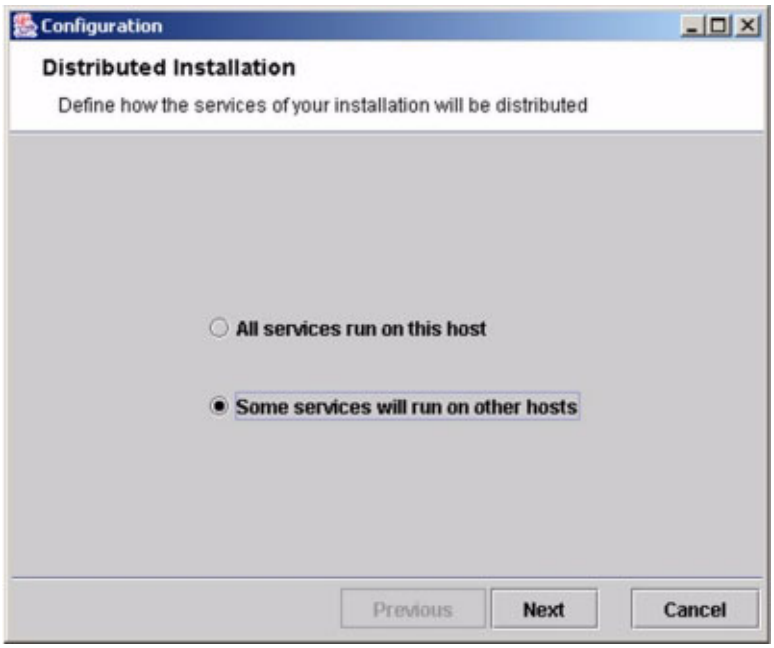
   The default installation directory is "`Program Files\Siemens\HiPathCTI`".

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

7. At the end of the installation, a Java process starts which only supports the "Lookup Client“ service. This "Lookup Client“ sends a multicast through the LAN and tries to find any lookup services that are present there (only on the CAP Management).

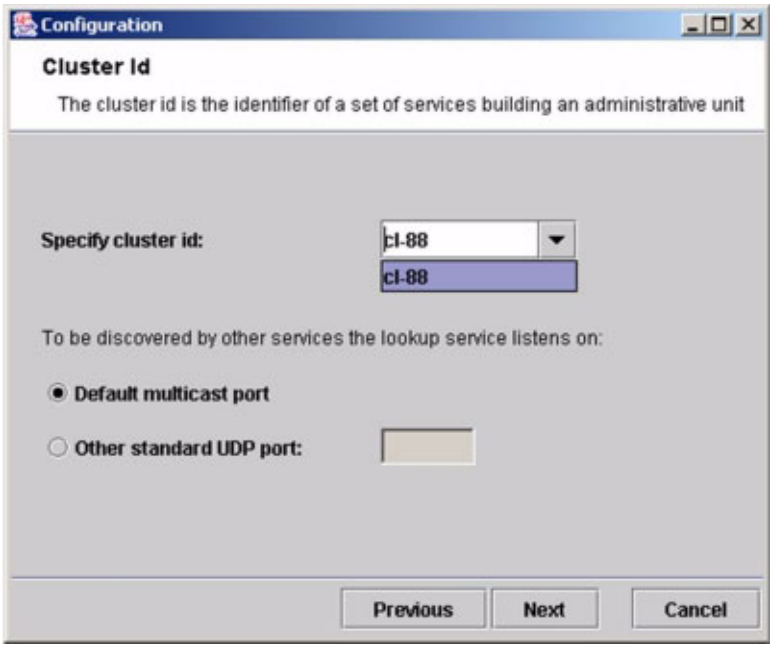
   

8. Depending on the type of installation, a dialog appears to notify you that some services run on other PCs.



Lookup services that are found (only on CAP Management) are offered for selection with their cluster IDs. Select the cluster ID for the associated CAP Managment 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".



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

```
C:\Program Files\Siemens\HiPathCTI\config\Start\startNT.cfg
```

The entry is:

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

This entry can be manually modified after installation and is active when the **Siemens CAP ServiceStarter** service is restarted.

9. 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, only the IP address of this card is listed.

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

   ```
   C:\Program Files\Siemens\HiPathCTI\config\Start\startNT.cfg
   ```

   The entry is:

   ```
   args: -localAddr

   args: "<PC name>/<IP address>"


   C :\Program Files\Siemens\HiPathCTI\config\common\global.cfg
   ```

The entry is:

```
<?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 **Siemens CAP ServiceStarter** service is restarted.

10. Start the "**Siemens CAP ServiceStarter**" service with

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

Installation on the remote PC is now complete.

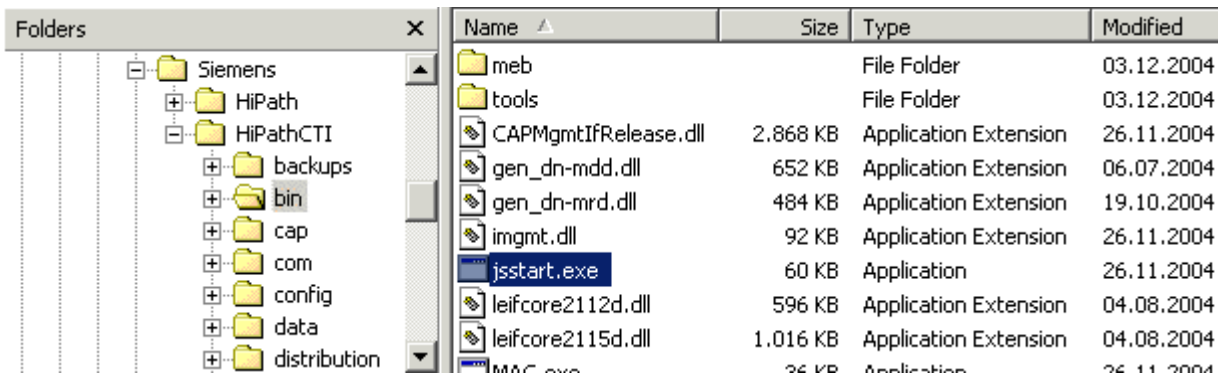
The Service Starter process is automatically started every time you start the PC. It connects with the HiPath CAP Management PC, determines all data for the components configured for the remote PC, loads the current software versions and required configuration data and starts the relevant processes.

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

After installation

After installation, there are no SCC, SCCP, CA4000, CA3000 or other CAP connection components in the directory:

```
C:\program files\Siemens\HiPathCTI\bin
```

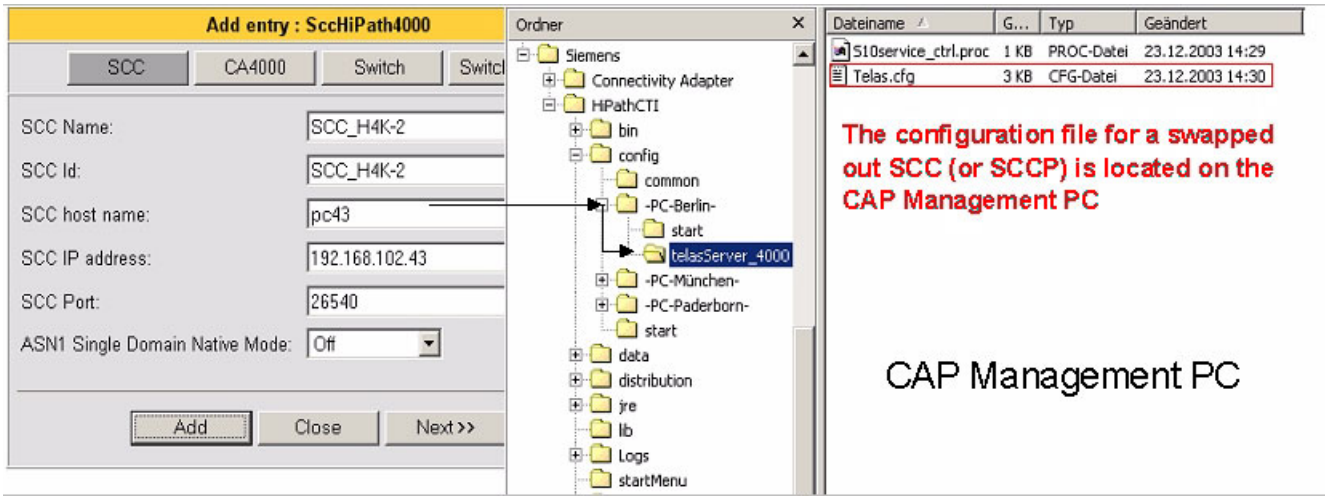


Configuring distributed components on the CAP Management PC

In a distributed installation, a new subdirectory corresponding to the PC name of the CAP ServiceStarter PC will be created automatically in the

`C:\Program Files\Siemens\HiPathCTI\config\`

directory on the CAP Management PC, using (for example) the PC name configured for an SCC.



As a result, all configuration files for all swapped processes stay in a CAP cluster on the CAP Management PC in the directory

`C:\Program Files\Siemens\HiPathCTI\config\<PC name>\`

Automatic distribution of connection components (SCC, SCCP, MEB, XMLPS)

The following subdirectories are present in the `distribution` directory:

- `distribution\bin`
  executable programs SCC, CA, SCCP and XMLPS
- `distribution\bin\meb`
  executable programs for the MEB
- `distribution\config`
  contains the telas.cfg configuration files for SCC, CA, SCCP and XMLPS, split into individual subdirectories.

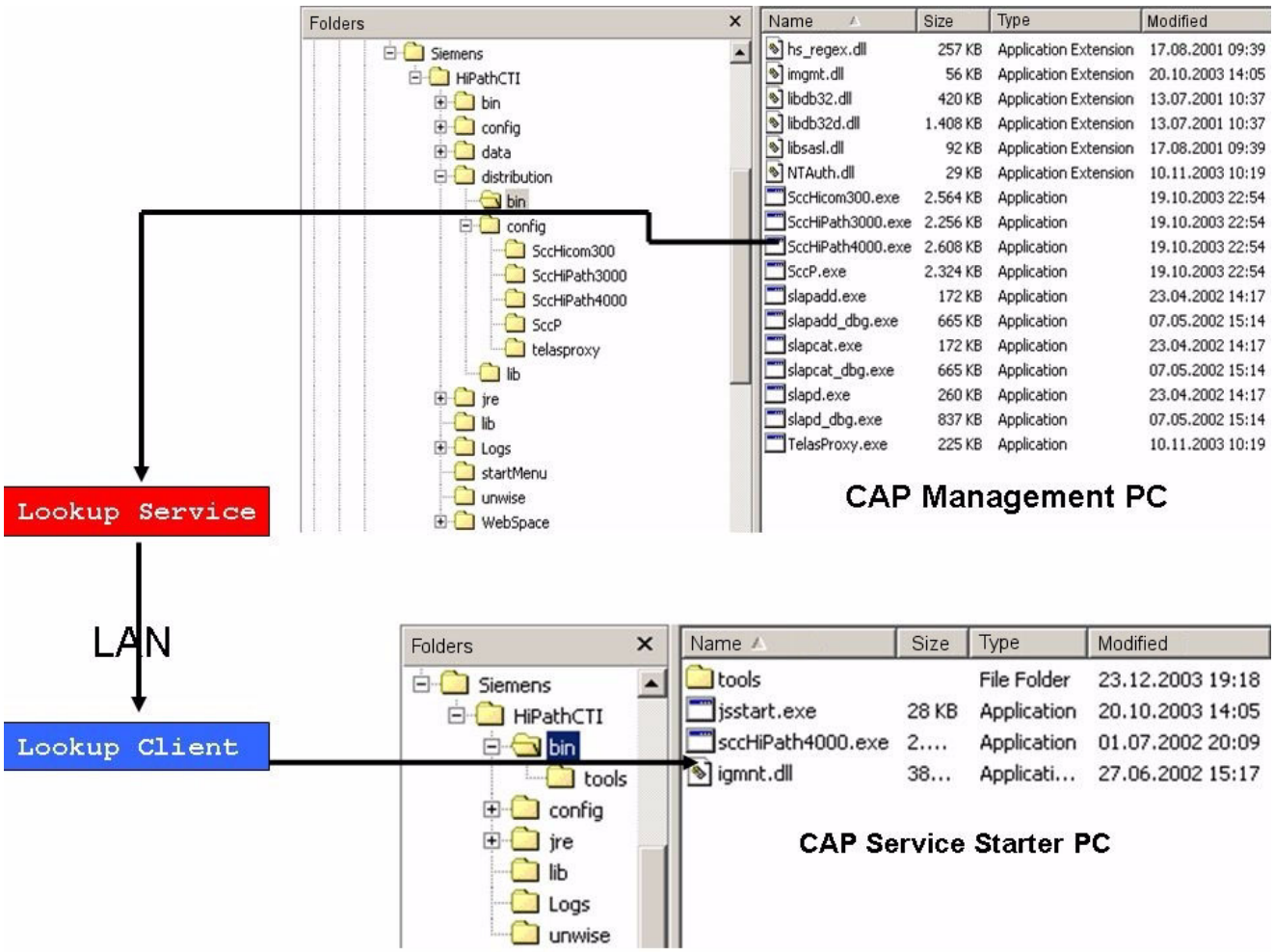
From here, the CAP connection components are distributed throughout the entire CAP cluster depending on the configuration. That is, the SCC/SCCP and CA component installation only occurs once on the CAP Management PC, regardless of whether or not one of these components is later active! If the executable programs for the connection components (e.g.SCC) need to be replaced at a later stage as part of fault clearance, this occurs only in the `distribu-`

`tion\bin` directory or, in the case of the MEB, in the `distribution\bin\meb` 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 destination directory of the selected components "CAP Call Control Service" and "Connectivity Adapter" during installation on the CAP Management PC is:

`C:\Program Files\Siemens\HiPathCTI\distribution\bin`

The programs are transferred from this source directory to the PCs, from which they should be started in accordance with the configuration.



4.4 CAP Installation Hints

4.4.1 Multiple network cards

If several network cards/NICs are configured in a CAP PC (for example, one for incorporation in the customer LAN, one for connection to the Hicom/HiPath switching host), it is important during configuration to identify the network card through which the HiPath 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:

```
C:\Program Files\Siemens\HiPathCTI\config\Start\startNT.cfg
```

The entry is:

```
args: -localAddr

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

```
C :\Program Files\Siemens\HiPathCTI\config\common\global.cfg
```

The entry is:

```
<?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 **Siemens HiPath CTI** or **Siemens CAP ServiceStarter** service is restarted.

4.4.2 Configuring several clusters

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

If you want to install HiPath CAP Management several times in your network environment (e.g. to enable the independent operation of different HiPath 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:

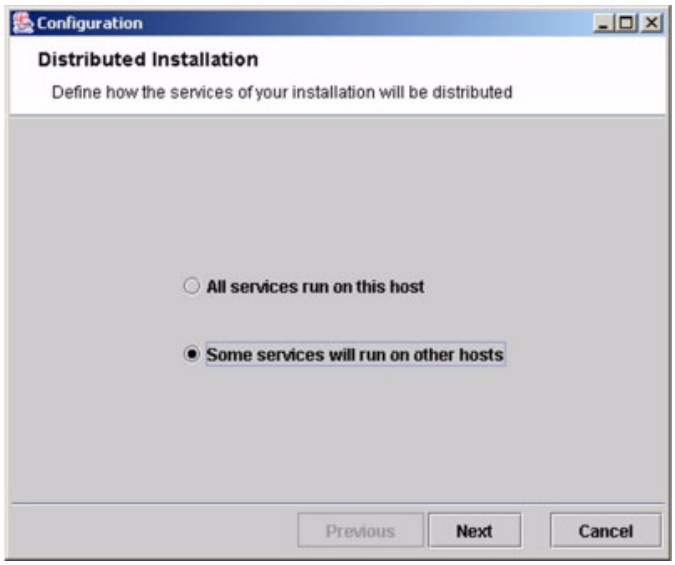
`C:\Program Files\Siemens\HiPathCTI\config\Start\startNT.cfg`

The entry is:

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

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

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



4.4.3 Deactivating Multicast

In a distributed installation, the internal CAP services Lookup Services and Lookup Clients find each other using multicast. Multicast is comparable to a broadcast but is restricted to a network class D address. For CAP components, this IP address is 234.9.8.7. If multicast is blocked by network components, the connection type must be changed and a fixed IP address and UDP port for it must be specified on the **CAP Managment PC** and on all associated **CAP Service-Starter PCs**. The IP address is always the CAP Management PC's IP address. Der UDP port must be a free port on the CAP Management PC (e.g. 5000).

Make the identical change in the `startNT.cfg` file on the CAP Managment PC and on all associated CAP ServiceStarter PCs.

Make the change in this file:

`<instDir>\config\start\startNT.cfg`

Enter the CAP Management PC's PC name or IP address and a free UDP port. The entry is:

```
args: "<Cluster Id>@<CAPManagementPC>:<UDPPort>/TelasWebStarter"
```

This entry can be manually modified after installation and is active when the **Siemens CAP ServiceStarter** or **Siemens HiPath CTI** service is restarted.

4.5 CAP process start sequence

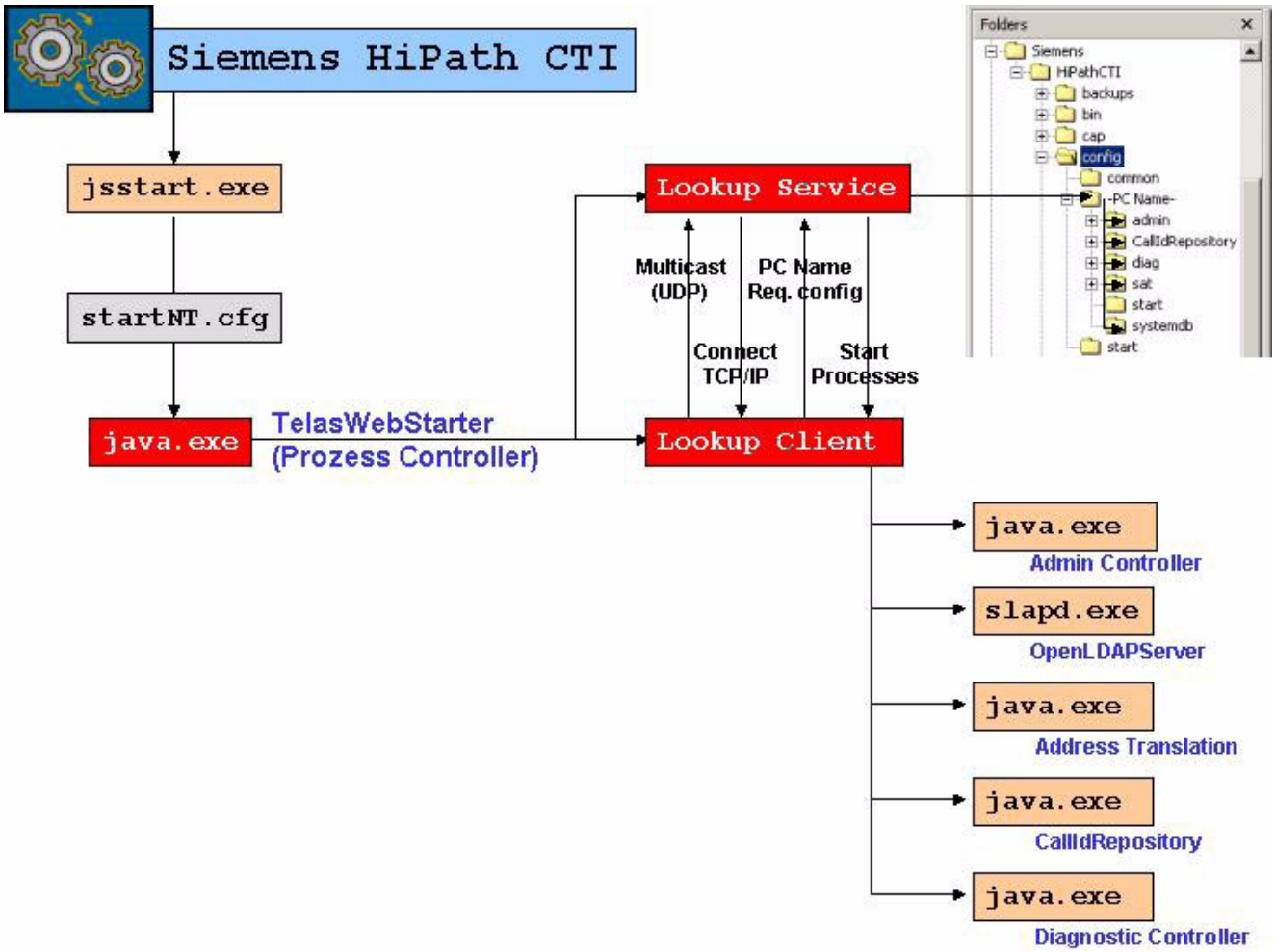
In this section, a distinction is made between whether the CAP processes run on a distributed installation or a non-distributed installation.

4.5.1 Non-distributed installation

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

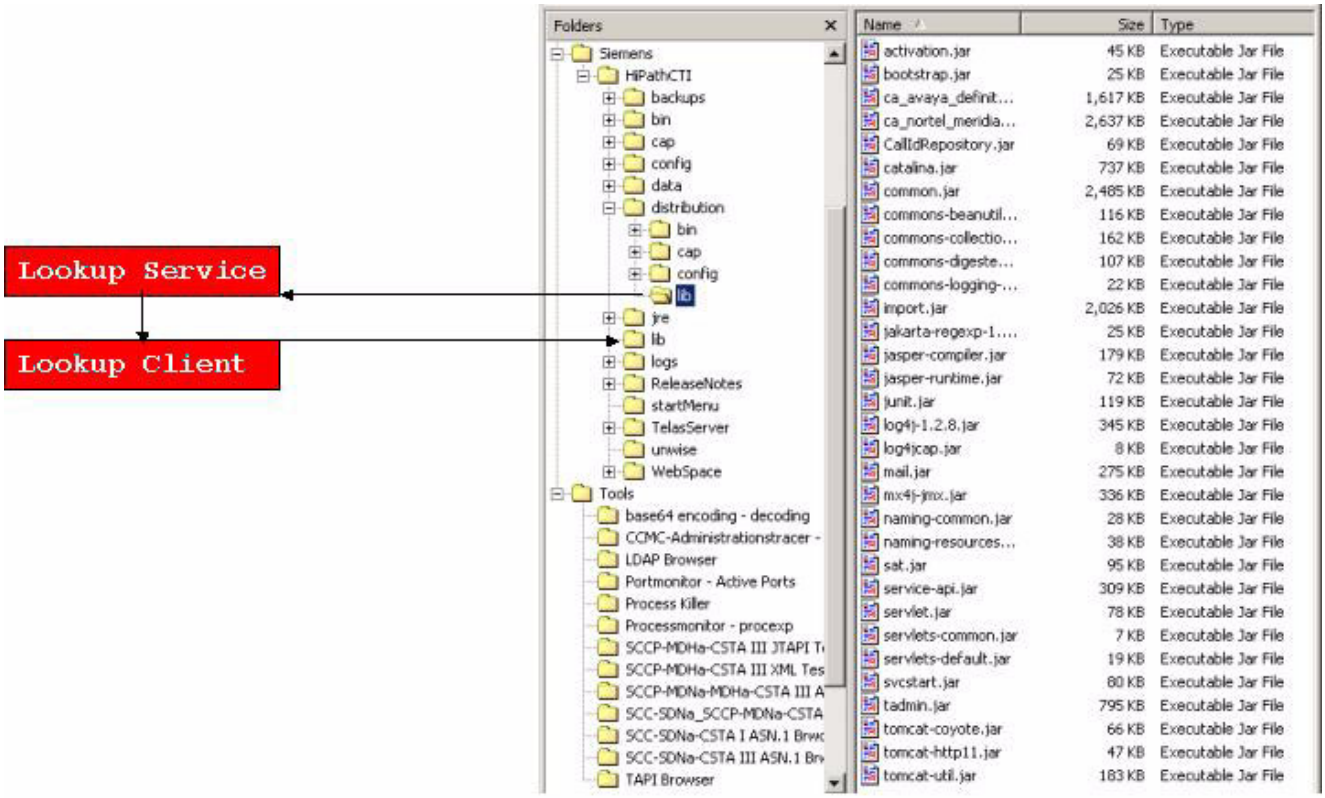
The CAP process start procedure

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



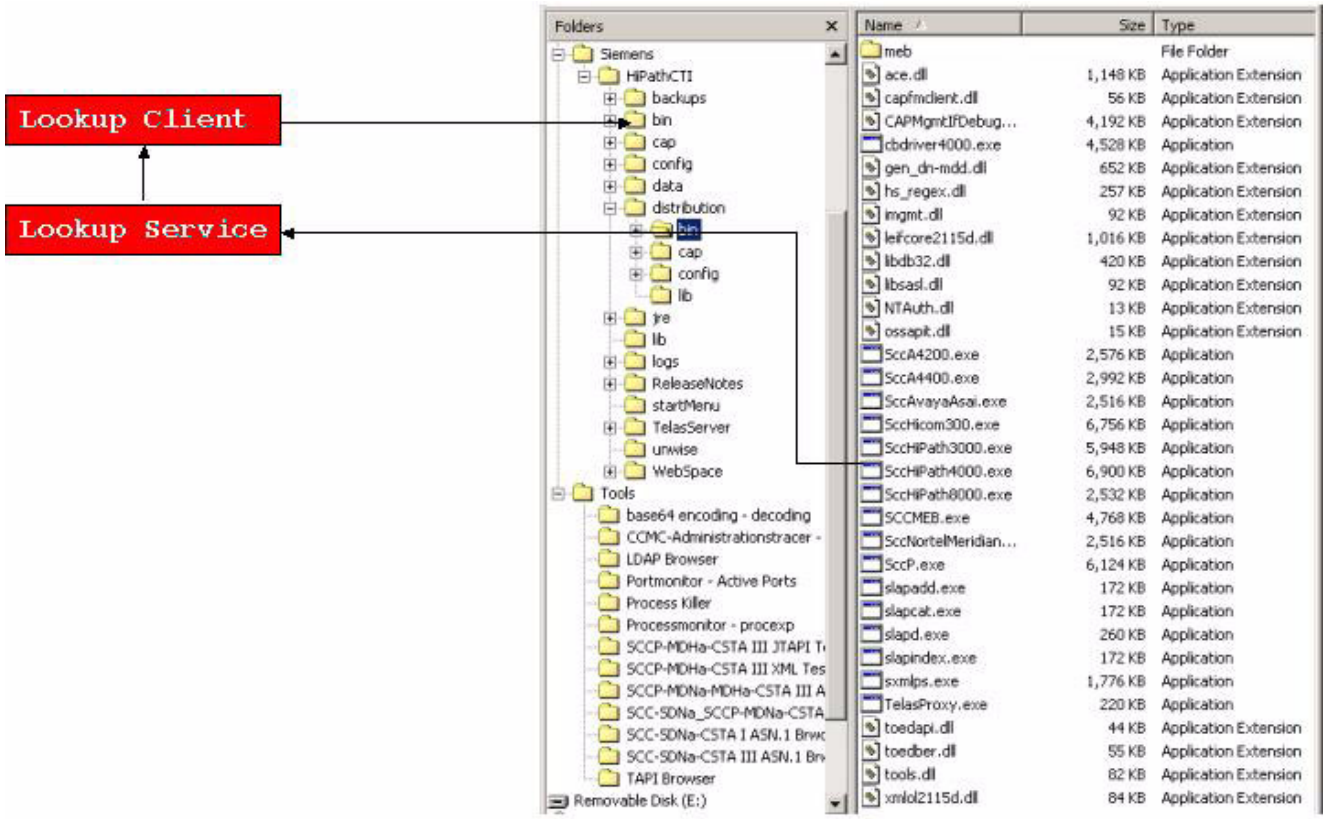
The "Siemens HiPath CTI" Windows service starts the `jsstart` process (Java Service Starter); this in turn starts the first Java process. This Java process is named "TelasWebStarter" and is the process controller for the internal CAP Lookup Service and Lookup Client services. Neither of the internal 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.



This mechanism copies the "jar" files from the directory
`C:\Program Files\Siemens\HiPathCTI\distribution\lib\`
to the destination directory
`C:\Program Files\Siemens\HiPathCTI\lib.`
This directory contains the versions of the "jar" files currently in use.

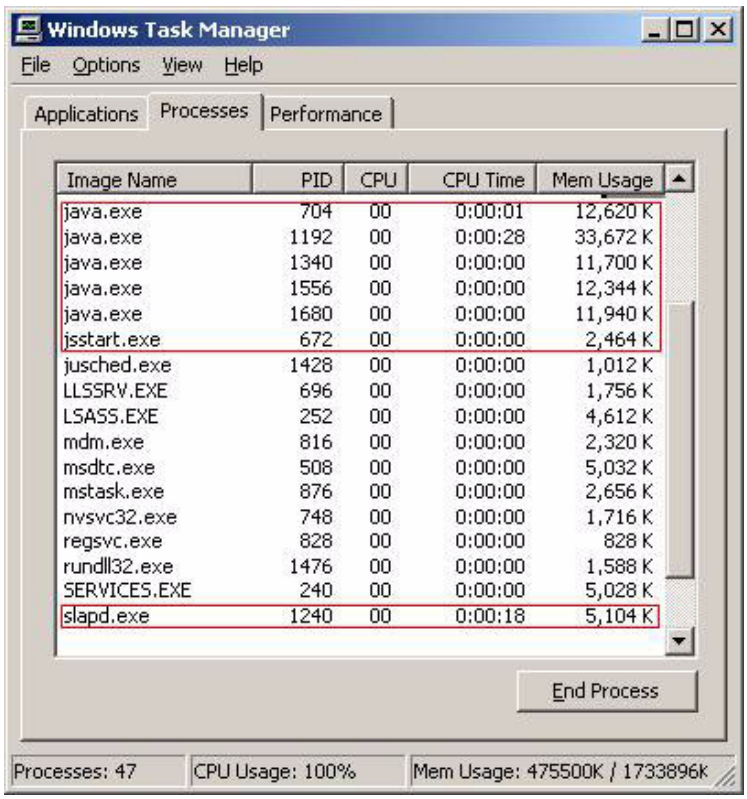
The same principle is also used for the SCC/SCCP distribution.



This mechanism copies the "exe" files from the directory
`C:\Program Files\Siemens\HiPathCTI\distribution\bin\`
to the destination directory
`C:\Program Files\Siemens\HiPathCTI\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 Managment PC should appear in the Windows Task Manager without any additional configuration (e.g. SCC, CA).
Accordingly, after stopping the **Siemens HiPath CTI** service, you should not see these processes anymore! If they are still displayed, these processes must be terminated manually.



Ending CAP processes manually

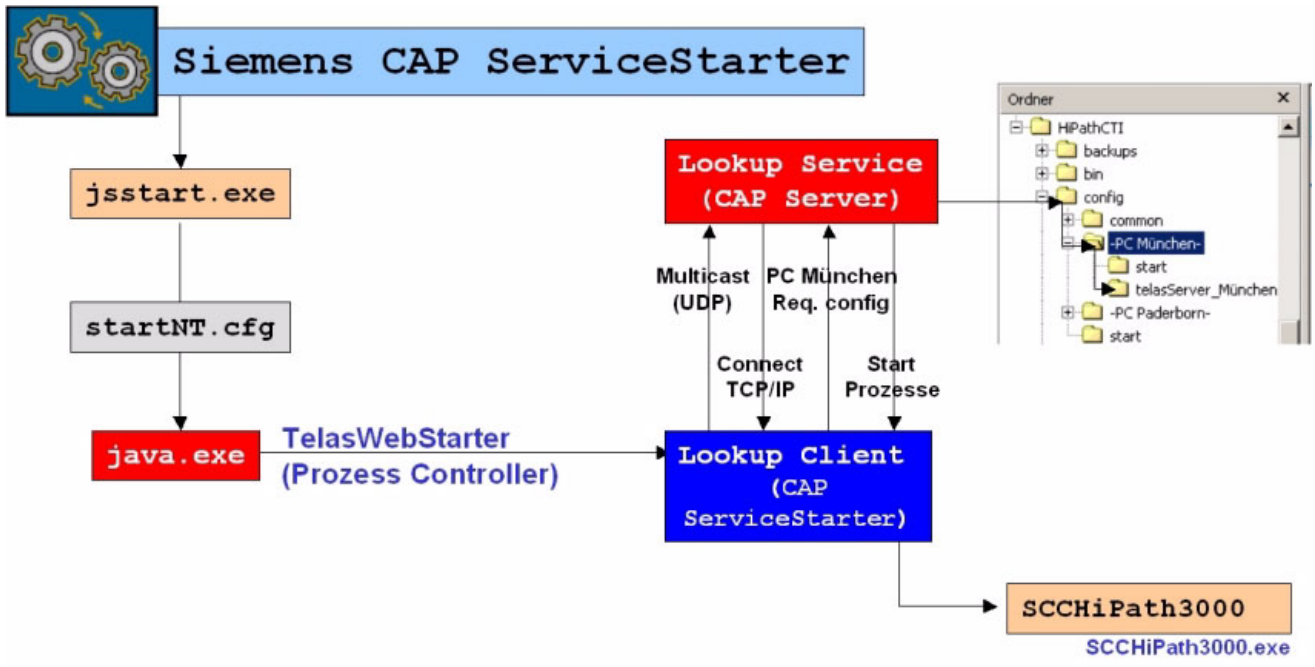
You cannot end CAP processes with the "End Process" function. During the installation phase, you must ensure that all processes end when the "Siemens HiPath CTI" service is ended. If necessary, we recommend stopping the service and then checking if all processes were ended, and ensuring that this is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

You must restart the PC if there are CAP processes still running after you ended the "Siemens HiPath 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.

4.5.2 Distributed installation

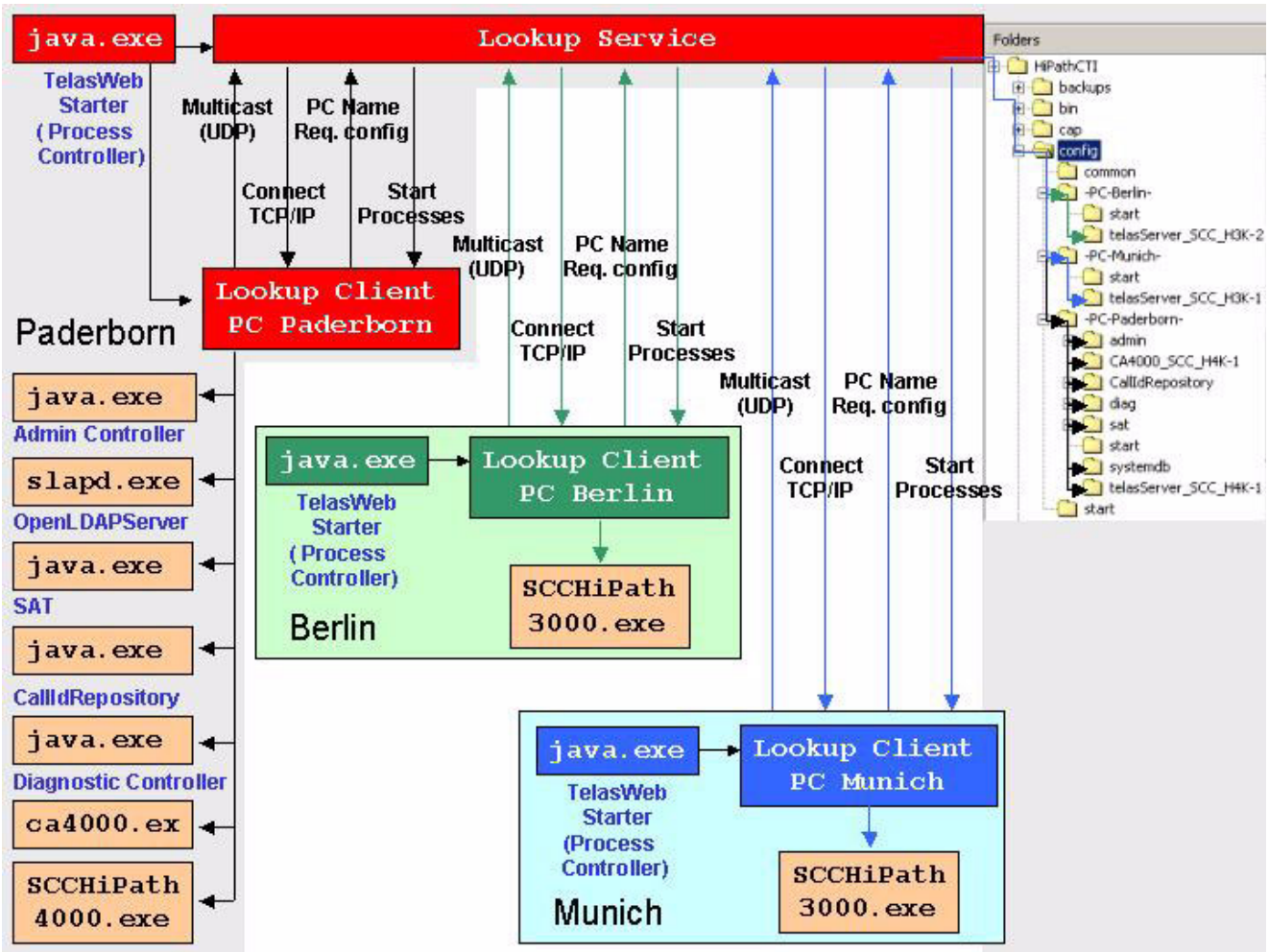
As indicated by the file structure, specific processes are started on the CAP Management PC and the CAP Service Starter PC. The **Siemens HiPath CTI** Windows service is linked to the `jsstart.exe` program (Java Service Starter).



> The "Siemens CAP Service Starter" service may not be started before distributed components are configured.
> If the "Siemens CAP Service Starter" 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 swapped processes to be started. Is there is no configuration 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 "Siemens CAP Service Starter" 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 with the "Siemens HiPath CTI" Windows service and on the CAP Service Starter PC with the "Siemens CAP Service Starter" Windows service.



The "Siemens HiPath 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 CA "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`.

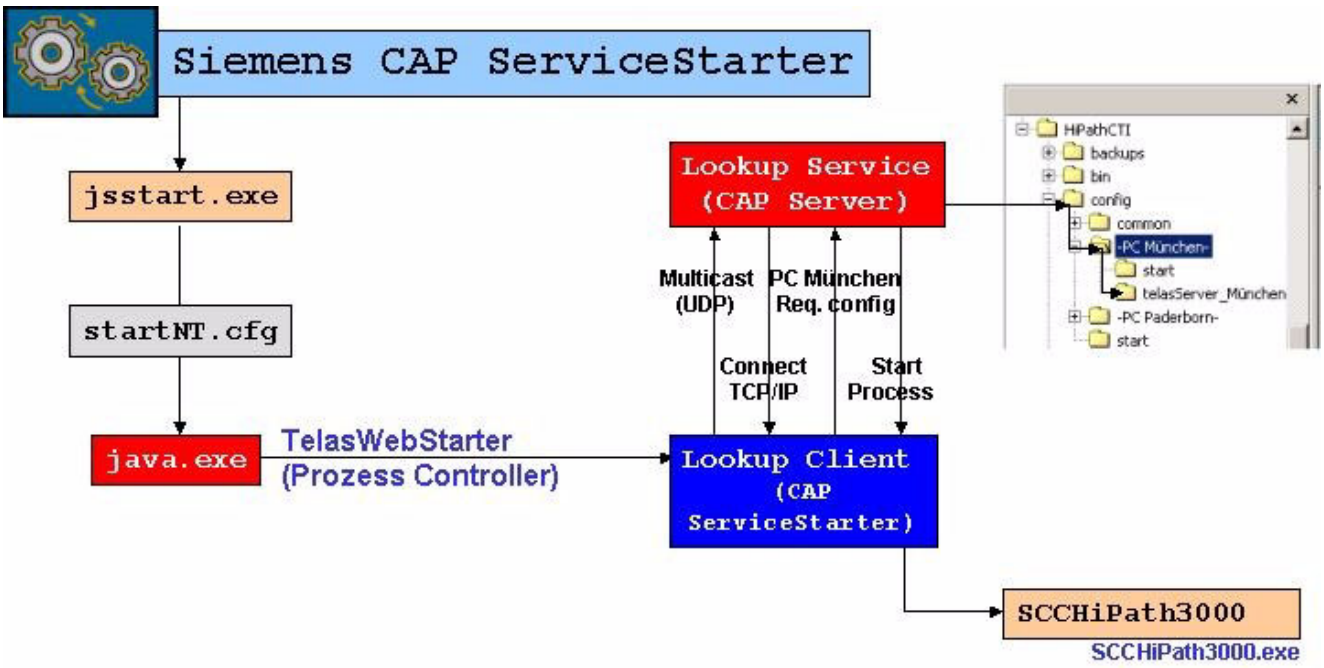
The `bin` directory contains the executable programs SCC/SCCP. The `config` directory contains the "telas.cfg" configuration files for SCC/SCCP, split into individual subdirectories.

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

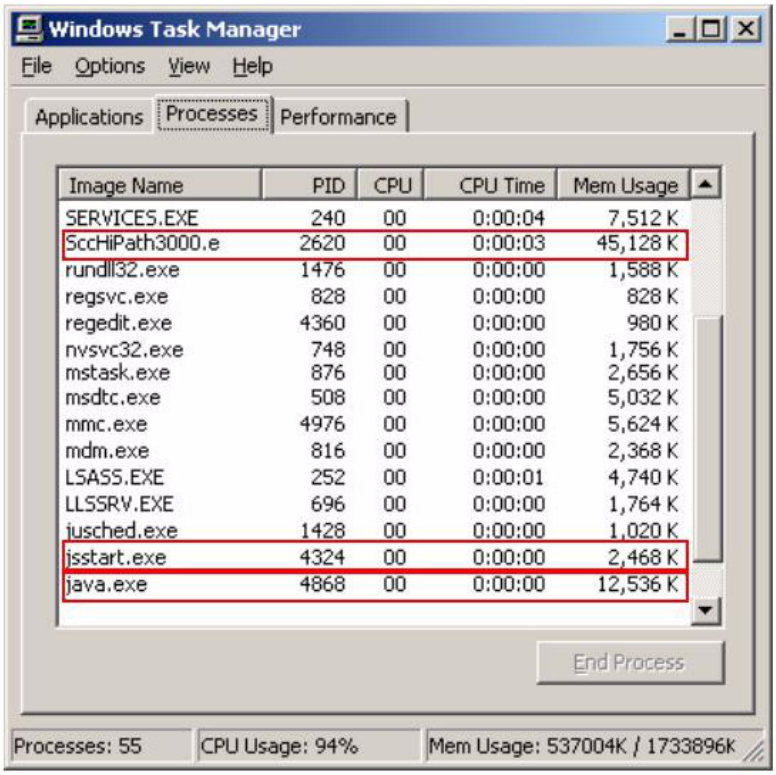
`C:\Program Files\Siemens\HiPathCTI\distribution\bin`

The programs are transferred from this source directory to the PC where the configuration should then be started.


Siemens CAP ServiceStarter
jsstart.exe
startNT.cfg
java.exe
TelasWebStarter
(Prozess Controller)
Lookup Service
(CAP Server)
Multicast
(UDP)
PC München
Req. config
Connect
TCP/IP
Start
Process
Lookup Client
(CAP
ServiceStarter)
SCCHiPath3000
SCCHiPath3000.exe
HPathCTI
backups
bin
config
common
-PC München-
start
telasServer_München
-PC Paderborn-
start

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 **Siemens CAP ServiceStarter** service was started, the `SCCHiPath3000.exe` was transferred by a configuration on the CAP Management PC. Accordingly, after stopping the **Siemens HiPath CTI** service, you should not see these processes anymore! If they are still displayed, these processes must be terminated manually.



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 "Siemens CAP Service Starter" 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 "Siemens CAP Service Starter" service.

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

4.6 Installing CAP TAPI Service Provider 3.0

Some CTI applications use a TAPI Service Provider to provide their functions. The TAPI Service Provider must be installed on the PC on which the CTI application is installed. In this case, there is a TAPI Service Provider on the HiPath CAP Installation CD.

Performing the installation

1. Insert the installation CD in the CD/DVD drive of the relevant PC. If Setup does not start automatically (i.e. autorun is not enabled), double-click the following file:

   `<CD/DVD drive>:\setupMaster.exe`

   To install the HiPath CAP Service Starter you can also start the `setupStarter.exe` installation program from a subdirectory on the CD.

2. Confirm the welcome dialog with **Next** and agree the licensing conditions by clicking **Next**.
3. Select **Install Client Components** and checkmark the **CAP TAPI Service Provider 3.0** entry.

   You can also select and install additional list entries together with CAP TAPI Service Provider. The additional components are installed in the right sequence as described in the chapters dealing with the various components.

4. Click **Next**.
5. Follow the instructions.
6. Further information on the installation and administration of CAP TAPI Service Providers is provided in the individual TAPI Service Provider manuals.

4.7 Installing the Siemens Virtual Wave Driver

In conjunction with the MEB of an application, this driver is similar to a sound card driver and enables the application to output IP audio data using the Windows Wave API. The audio data must be available as wav or avi data in 8 KHz / 16 bit format.

This driver must be installed locally on all MEB PCs. It is installed independently of the CAP Management.

Performing the installation

1. Select **Start | Settings | Control Panel | Hardware**. The hardware wizard is started; click **Next**.
2. Select the hardware option **Add/Troubleshoot a device** and confirm with **Next**.
3. The wizard searches for devices and lists its findings. Select **Add a new device** and confirm with **Next**.
4. Because the Virtual Wave driver is not "real" hardware, select **No, I want to select the hardware from a list**. Confirm again with **Next**.
5. Select the hardware type **Sound, video and game controllers** and click **Next**.
6. To select the device driver, click **Data Carriers**. Insert the installation CD for HiPath CAP. The installation file for virtual wave driver (`oemseup.inf`) is located there in the `\Software\MEB\WaveDriver` folder. After selection, the **Siemens Virtual Wave Driver** model appears. Confirm with **Next**.

   Depending on the currently installed Windows release, a message may appear indicating that a digital signature has not been found. Proceed with the installation by clicking **Yes**.
7. The hardware wizard is ready to install; start by clicking **Next**.
8. The virtual wave driver is installed. Click **Finish** to quit the wizard after installation.
9. The PC only needs to be restarted if a different version of the driver was previously installed.

After installation

Once installation is complete, you can edit the settings for Siemens Virtual Wave Driver under **Start | Settings | Control Panel | System | Hardware | Device Manager | Sound, video and game controllers | Siemens Virtual Wave Driver**.
Thirty new input or output wave devices are available (only in connection with MEB).

4.8 Special features during installation

4.8.1 Adaptation of the IP address on the HiPath CAP PC

While the HiPath 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 HiPath 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

HiPath CAP Management was installed as described in Section 4.1. The HiPath CAP Call Control Service, Connectivity Adapter CA 4000, or Connectivity Adapter CA 300 components can also be installed.

Modifications

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

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.siemens.de/142.33.22.11"
   ```
2. File <*InstDir*>/config/common/global.cfg
   Modify the three underscored definitions
   ```
   <?x set INST_HOST = "mypc.area.siemens.de" ?>
   <?x set INST_IP = "142.33.22.11" ?>
   <?x set CONFIG_URL = "http://mypc.area.siemens.de:<?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.siemens.de:8170/ or
   HTTP://mypc.area.siemens.de: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 SimplyPhone for Web/HiPath ComAssistant has also been installed in addition to HiPath 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.siemens.de:8180/` or
    `https://mypc.area.siemens.de:8180/`

4.8.2 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 reenabled 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 **Siemens HiPath CTI** system service on the relevant PC and restart it; only then will the change take effect!

4.9 Migrating from TelasAdmin 4.1 / HiPath CAP 1.0 / HiPath CAP 2.0 Management

Depending on the version of HiPath CAP or Telas Admin already installed, the following steps must be performed one by one for migration to HiPath CAP V3.0. Migration from a software version < Telas Admin 4.1 is not supported.

If error messages about an incorrect software version are output during a migration (and these messages are known to be inaccurate), delete the following directory in the REGISTRY:
`HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\HiPathCTI`
and repeat migration.

Migration sequence

Step 1: - Upgrade Telas Admin 4.1 to HiPath CAP V1.0

Step 2: - Upgrade HiPath CAP V1.0 HiPath CAP V2.0

(Step 2.1: - Upgrade ComAssistant to SMR 2)

Step 3: - Upgrade HiPath CAP V2.0 to HiPath CAP V3.0

4.9.1 Migrating Telas Admin 4.1 to HiPath CAP V1.0

1. Stop the associated **Siemens HiPath CTI** service.

   This is usually performed in the "Control Panel" window.

2. Install HiPath CAP V1.0 Management (see Section 4.1, "Installing the server components").
   Install HiPath CAP V1.0 Management **in a different directory** to the old version Telas Admin 4.1.

   It is important that you do not uninstall Telas Admin 4.1 at this stage, as automatic migration of the existing data to CAP Management has yet to take place. Wait until HiPath CAP Management V1.0 has been installed before uninstalling Telas Admin 4.1.

   When you install HiPath CAP Management V1.0, the configuration data is automatically migrated from Telas Admin 4.1. The existing data is retained and, if necessary, converted to the new data format.

The following data is automatically transferred from Telas Admin 4.1 (Appendix A, "Implementation details" contains further information about setting up an installation and about the content and structure of configuration files):

- User authentication data, PBX configuration (switching system connections), local line data and speed-dial information are retained automatically. Any new data fields will be completed in line with the existing configuration.
- Apart from the data referred to above, the most important configuration data is also retained, for example:

`global.cfg`	Logging settings
`auth.cfg`	Validity period for passwords, default password
`startNt.cfg`	Cluster information and other settings
`TelasWeb.cfg`	All settings

Data from older TelasAdmin versions (3.1 or 4.0) is not migrated automatically. Migration must be performed manually.

The following restrictions apply in the case of automatic migration:

- Only configurations from the directories `config\common, config\<`*`InstHost`*`>`, and `config\start` are migrated.
- If there are other directories with `config\<PC name>` (if installation is distributed over multiple PCs in the network), this data must be migrated manually. This excludes directories that were used exclusively for the distributed TelasServer 4.1 installation. These directories are regenerated with the required content.
- Modified or local HTML pages (**CustomizedPath** option in the file `TelasWeb.cfg`) must be migrated manually.

3. You can now uninstall Telas Admin 4.1/delete the old installation directory.
4. CallBridgeForWorkGroups (CB4WG 4.1) must be uninstalled and all associated entries in the file `C:\WinNT\system32\drivers\etc\hosts` must be deleted. The separate installation of CA300 or CA4000 is not necessary for the next intermediary step for migration to HiPath CAP V2.0.

4.9.2 Migrating HiPath CAP V1.0 to HiPath CAP V2.0

1. Stop the associated **Siemens HiPath CTI** service.

   This is usually performed in the "Control Panel" window.

2. Install HiPath CAP V2.0 Management (see Section 4.1, "Installing the server components").
   Install HiPath CAP V2.0 Management **in the same directory** as HiPath CAP V1.0 Management.

   When you install HiPath CAP Management V2.0, the configuration data is automatically migrated from HiPath CAP Management V1.0. The existing data is retained and, if necessary, converted to the new data format. **The configuration files for the SCC already configured are not automatically modified. However, the parameters already set will still be supported.** To add additional necessary configuration parameters for an SCC, you can open each individual SCC over CAP V2.0 Management and click the **Change** button. This procedure only needs to be performed during the final stage of migration from HiPath CAP V2.0 to HiPath CAP V3.0 and is not necessary for an intermediary step.

   All licenses installed for HiPath CAP V1.0 are automatically transferred. The HiPath CAP V1.0 license "UNKNOWN" which licensed the number of monitor points to be set in a CA4000 is not needed 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 and therefore does not require a separate license.
   The HiPath CAP V1.0 license "CAP" can be used in HiPath CAP V2.0 instead of the CAP-A, CAP-S, and CAP-S license.
   Example: If a CAP-A license is needed and if a CAP license is installed, this is used instead of the CAP-A.

   The following data is automatically transferred from HiPath CAP V1.0 (Appendix A, "Implementation details" contains further information about setting up an installation and about the content and structure of configuration files):

   - User authentication data, SCC configuration, local line data and speed-dial information are retained automatically. Any new data fields will be completed in line with the existing configuration.

- Apart from the data referred to above, the most important configuration data is also retained, for example:

`global.cfg`	Logging settings
`startNt.cfg`	Cluster information and other settings
`TelasWeb.cfg`	All settings

- Insert the IP address and the PC name of the CAP Management PC in the file `<InstDir>\config\start\startNT.cfg`. The entry is:
"args: "<PC name>/<IP address>"

The following restrictions apply in the case of automatic migration:

- Only configurations from the directories `config\common, config\<`*`InstHost`*`>`, and `config\start` are migrated. This action automatically saves the HiPath CAP V1.0 installation files `"global.cfg"` and `"TelasWeb.cfg"` as `"global.old"` and `"TelasWeb.old"`.
- If there are other directories with `config\<PC name>` (if installation is distributed over multiple PCs in the network), this data must be migrated manually. This is done by "**changing**" the SCC configuration data in CAP V2.0 Management. This is not necessary if HiPath CAP V2.0 is immediately migrated to HiPath CAP V3.0.

3. Modified or local HTML pages (**CustomizedPath** option in the file `TelasWeb.cfg`) must be migrated manually.
4. An older version of Connectivity Adapter HiPath 4000 or Connectivity Adapter Hicom 300 must be uninstalled. CA300 or CA4000 does not have to be installed separately for the final stage of migration to HiPath CAP V3.0.

4.9.3 Migrating HiPath CAP V2.0 to HiPath CAP V3.0

1. Save or make a note of the configuration parameters for all CA4000 and CA300 instances in your CAP cluster.
2. Stop the associated **Connectivity Adapter** Windows service on all PCs on which the CA4000 or CA300 is installed.
3. Uninstall the **Connectivity Adapter** software from all PCs on which the CA4000 or CA300 is installed. This is usually performed in the "Control Panel" window.
4. Stop the associated **Siemens HiPath CTI** service. This is usually performed in the "Control Panel" window.

An existing ComAssistant installation must first be upgraded to SMR2 before HiPath CAP V3.0 may be installed.

5. Install HiPath CAP V3.0 Management, HiPath CAP V3.0 Call Control Service, and, if necessary, Connectivity Adapter HiPath 4000 and/or Connectivity Adapter Hicom 300 (see Section 4.1, "Installing the server components").
   Install HiPath CAP V3.0 components **in the same directory** as HiPath CAP V2.0 Management.

   When you install HiPath CAP Management V3.0, the configuration data is automatically migrated from HiPath CAP Management V2.0. The existing data is retained and, if necessary, converted to the new data format. **The configuration files for the SCC already configured are not automatically modified. However, the parameters already set will still be supported.** To add additional necessary configuration parameters for an SCC, you must open each individual SCC over CAP V3.0 Management, you must edit the IP address related to the HiPath 4000 or Hicom 300, you must edit the PBX link number and the SB applikation number and than click the **Change** button. This action automatically adds another directory to the corresponding PC name directory for the associated CA4000 or CA300 in the case of SCCHiPath4000 or SCCHicom300.

   
   In HiPath CAP V3.0, CA4000 or CA300 can only be configured and administered over HiPath CAP Management. A local separation between SCC and CA is no longer possible. All CAs installed locally must be uninstalled. The default routine for distributed CAP installation distributes CA and the associated SCC.

   
   All licenses installed for HiPath CAP V1.0 are automatically transferred. The HiPath CAP V1.0 license "UNKNOWN" which licensed the number of monitor points to be set in a CA4000 is not needed 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 and therefore does not require a separate license.
   The HiPath CAP V1.0 license "CAP" can be used in HiPath CAP V3.0 instead of the CAP-A, CAP-S, and CAP-S license.
   Example: If a CAP-A license is needed and if a CAP license is installed, this is used instead of the CAP-A.

   The following data is automatically transferred from HiPath CAP V2.0 (Appendix A, "Implementation details" contains further information about setting up an installation and about the content and structure of configuration files):

   - User authentication data, SCC configuration, SCCP configuration, local line data, and speed-dial information are retained automatically. Any new data fields will be completed in line with the existing configuration. This is done in the following steps:
     – The files from the LDAP database directory `<InstDir>\data\TelasAdmin\adminauth\users` are exported to the file `<InstDir>\data\TelasAdmin\adminauth\migrate23\cap20.ldif`.

  - The file `cap20.ldif` is then converted into the file `cap30.ldif` in the same directory
  - and then imported into the new LDAP database directory `<InstDir>\data\TelasAdmin\adminauth\capdb`.

- Apart from the data referred to above, the most important configuration data is also retained, for example:

`global.cfg`	Logging settings
`startNt.cfg`	Cluster information and other settings
`TelasWeb.cfg`	All settings
`admin.cfg`	All settings
`backup.cfg`	All settings

The following restrictions apply in the case of automatic migration:

- Only configurations from the directories `config\common, config\<`*`InstHost`*`>`, and `config\start` are migrated. This action automatically saves the HiPath CAP V2.0 installation files `global.cfg`, `TelasWeb.cfg, admin.cfg`, and `backup.cfg` as `global.old`, `TelasWeb.old`, `admin.old`, and `backup.old`.
- If there are other directories with `config\<PC name>` (if installation is distributed over multiple PCs in the network), this data must be migrated manually. This is done by "**changing**" the SCC configuration data in CAP V3.0 Management.

6. Modified or local HTML pages (**CustomizedPath** option in the file `TelasWeb.cfg`) must be migrated manually.
7. An older version of Connectivity Adapter HiPath 4000 or Connectivity Adapter Hicom 300 must be uninstalled. CA is only installed on the CAP Management PC in HiPath CAP V3.0. It is only every permanently linked to an SCC. In the case of CA distribution (together with the associated SCC), only "Siemens CAP Service Starter" must be installed on the local PC. Distribution is then performed over the standard routine for distributed installation.
8. The CAP TCSP also has to be replaced in a TAPI connection.
9. This data is not transferred if the default password and/or the password validity duration was modified in HiPath CAP V2.0. In this case, you must enter these changes manually later under **User | Settings | Settings for the "Standard Business Group"**.

4.10 Backup & restore

4.10.1 Backup

HiPath CAP Management provides an additional service that backs up critical CAP Management and ComAssistant data.

The directory "<inst dir>\config\<host name>\admin\mgmnt\" contains the file 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 "Siemens HiPath 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:/Programme/Siemens/HiPathCTI/backups`
Specify the destination directory for all backups here.

`<?x set RULES_BACKUP_TIME = "01:55:00" ?>`
Specify the backup time for ComAssistant rules assistant's data here.

`<?x set USERS_BACKUP_TIME = "02:00:00" ?>`
Specify the backup time for CAP data here.

`<?x set PABS_BACKUP_TIME = "02:10:00" ?>`
Specify the backup time for personal address books of ComAssistant users.

`<?x set JOURNAL_BACKUP_TIME = "02:30:00" ?>`
Specify the backup time for the call journals of ComAssistant users here.

`<?x set CAP_LDAP_MODE = "STANDALONE" ?>`
The "standalone" parameter must be retained in a Windows installation. "Replica" can only be used to activate replication in the case of LINUX-based installation (possible in future).

If customer-specific backup services are provided, take care not to save original HiPath CAP data but the contents of the backups directory.

4.10.2 Restore

To restore CAP data from a data backup, you must

- restore configuration files to the file system,
- restore data to the CAP database.

Specify the backup status to be used for the restore operation; this is a subdirectory in "<instDir>HiPathCTI/backups/" (referred to in the following as **<backup>**).

4.10.2.1 Restoring configuration files

- Delete from the <instDir>/HiPathCTI/config/<hostname> directory all subdirectories with the name TelasServer port*.
- Copy all directories from "<Backup>/config/<host name>/TelasServer port*" to "**…HiPathCTI/config/<host name>**".

4.10.2.2 Restoring a database

This can be done either by copying the database files in binary format or by restoring the database contents from an ldif file.

Copying database files

- Stop the **SystemMgmtDatabase** process in the Diagnostic Agent.
- Delete all binary database data in the directory <instDir>/HiPathCTI/data/TelasAdmin/adminauth/users (all files with the extension .dbb).
- Copy all files from <backup>/data/TelasAdmin/adminauth/users /*.dbb to <instDir>/HiPathCTI/data/TelasAdmin/adminauth/users.
- Start the **SystemMgmtDatabase** process in the Diagnostic Agent (this takes a few moments).

Exporting a database to an `ldif` file

- Stop the **SystemMgmtDatabase** process in the Diagnostic Agent.
- Export the database with the `slapcat` command
  (available in `<instDir>/HiPathCTI/distribution/bin`")

  ```
  slapcat

  -f <instDir>/HiPathCTI/config/<hostname>/systemdb/slapd_twusers.conf

  -l <instDir>/data/TelasAdmin/adminauth/users.ldif
  ```

- Start the **SystemMgmtDatabase** process in the Diagnostic Agent (this takes a few moments).

Restoring a database from the `ldif` file

- Stop the **SystemMgmtDatabase** process in the Diagnostic Agent.
- Delete all binary database data in the directory `<instDir>/HiPathCTI/data/TelasAdmin/adminauth/users`(all files with the extension `.dbb`).
- Restore the database with the command `slapadd`
  (available in `<instDir>/HiPathCTI/distribution/bin`")

  ```
  slapadd

  -f <instDir>/HiPathCTI/config/<hostname>/systemdb/slapd_twusers.conf

  -l <backup>/data/TelasAdmin/adminauth/users.ldif
  ```

- Start the **SystemMgmtDatabase** process in the Diagnostic Agent (this takes a few moments).

4.11 Uninstalling HiPath CAP

When uninstalling a HiPath CTI system, the installation procedure sequence should be followed in reverse. HiPath CAP Management should be the last component to be uninstalled. Because HiPath CAP Management forms the basis for an installed HiPath CTI system, none of the other components can work after HiPath CAP Management has been uninstalled.

Performing uninstallation

1. Use **Start | Settings | Control Panel | Software | Modify or Remove Program** to select the component to be uninstalled from the list. You should follow the installation procedure sequence in reverse, that is, HiPath CAP Management must be the last component to be uninstalled in conjunction with HiPath CAP.

Once the uninstall procedure is completed, the installation directory has to be manually removed, as files or user data generated when running the program cannot be removed during uninstallation.

5 Getting Familiar with HiPath 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 HiPath CAP Management with
   Start | Programs | Siemens HiPath CTI | 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 following a successful login. An ID and password are required to login to CAP Management. A distinction is made between an administrator login and a user login. The user must log in as an administrator the first time CAP Management is started. The default administrator ID for this purpose is "Admin", while the default administrator password is also "Admin". The ID and password should be changed by the administrator subsequently (see Section 5.3, "Modifying the administrator password"). The administrator can also configure other users and define their IDs and passwords (see Section 7.2.1, "Add user").

1. 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.

5.1.2 Logging off

You do not need to log off separately to close CAP Management. It is enough to close CAP Management in the normal way.

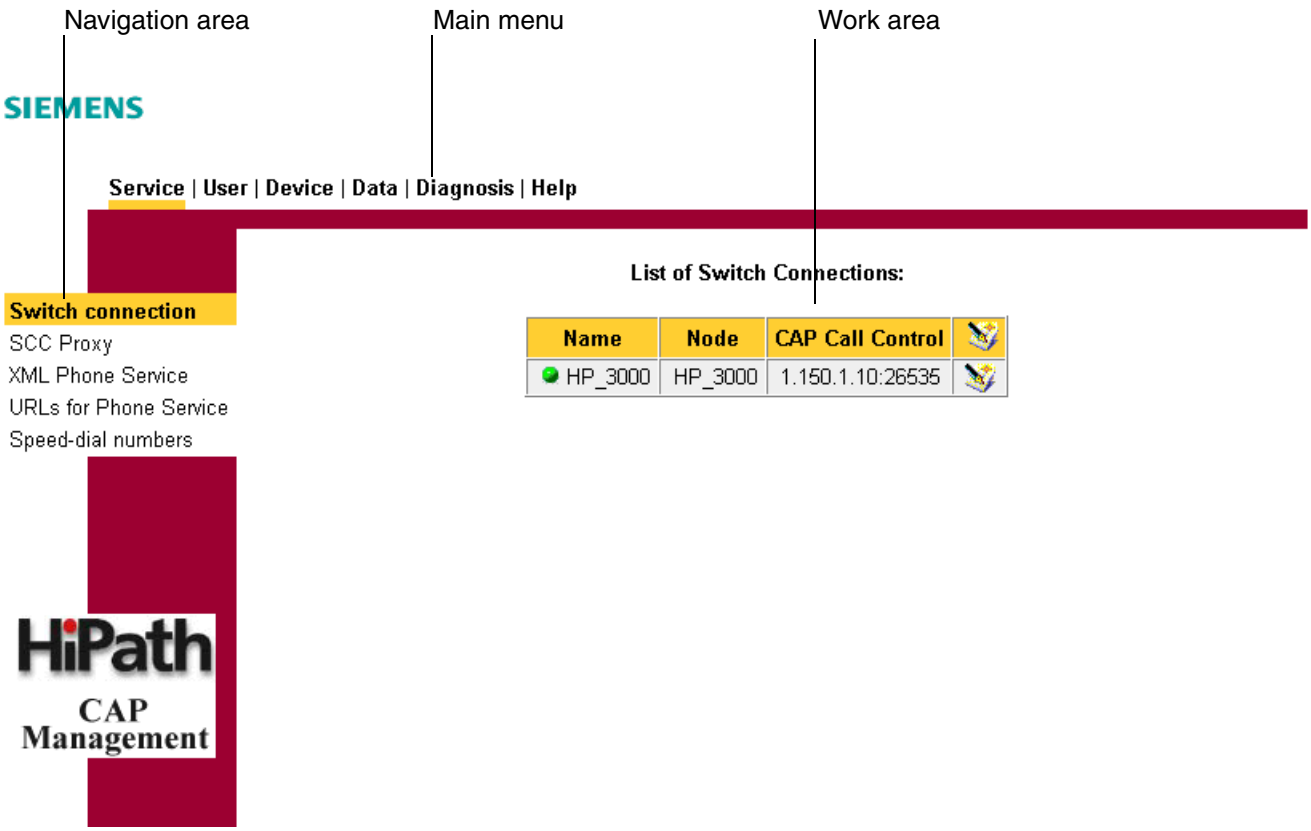
You must log in again to continue working with CAP Management (see Section 5.1.1, "Logging on").

5.2 CAP Management interface

The CAP Management interface consists of HTML pages that can be opened with an HTML browser (Internet Explorer V5.5 SP2 or higher or Netscape Navigator V7.1 or higher). This is why CAP Management runs on a non-platform-specific basis under all commonly used operating systems.

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

- Main menu
- Navigation area
- Work area



If the size of the browser window means that the navigation area and work area cannot be displayed in full, then horizontal or vertical scroll bars appear at the edges, enabling you to scroll the section displayed.

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 HiPath 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.

5.3 Modifying the administrator password

You can change the administrator password or define new users with administrator rights at any time.

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 7.2.1 and select **Admin** as the user's role.

The administrator can adopt the same procedure to modify the password for all other users.

6 Configuration with HiPath CAP Management

You must configure one of the following SCC units for each switching host that is to be connected to HiPath CAP:

- SCC4000 for HiPath 4000
- SCC3000 for HiPath 3000
- SCC300 for Hicom 300
- TelasServer 3.1 - only for old applications that require a connection to Hicom 300 via the ACL-H3 interface. Only TAPI applications connected via the "Telas TSP" and "SimplyPhone for Web" can access the Telas Server 3.1 C interface. Telas Server 3.1 does not support a CSTA interface.

To create and configure a new SCC instance, select **Administration** in the main menu and enable **PBX Services** 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.

You can connect the various communication systems to HiPath CAP V3.0, for example

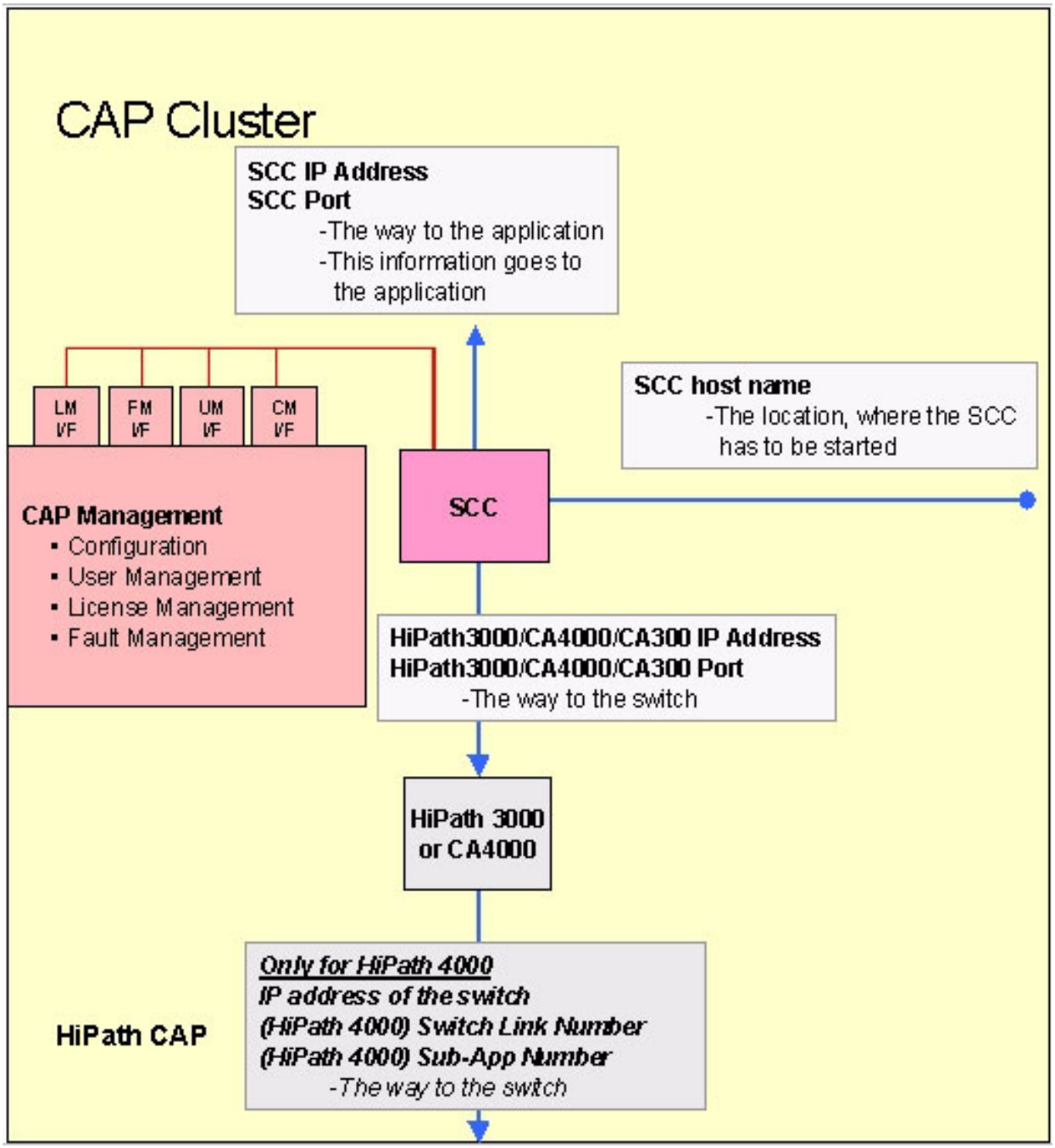
- HiPath 4000
- HiPath 3000
- Hicom 300
- Additional communications systems from Alcatel, Nortel, AVAYA, etc.

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.

Use of the CAP Media Service is necessary for connecting an application to a HiPath 3000 or HiPath 4000 via the Microsoft Wave API. The CAP Media Service comprises several different components. The main components are SCCMEB, MEB, and the Siemens Virtual Wave Driver.

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

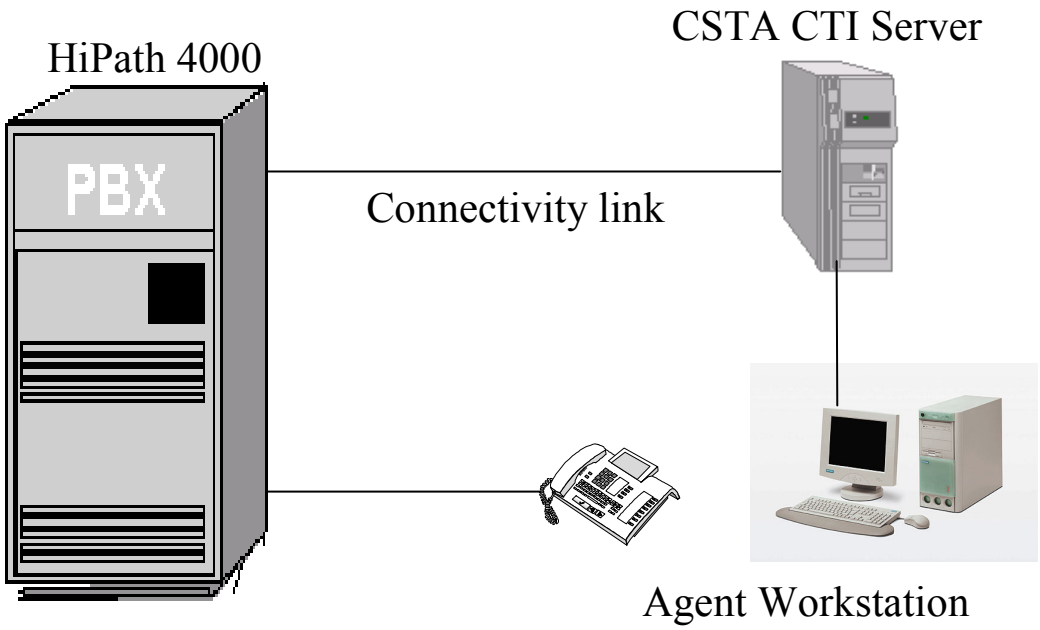
The following diagram shows the positioning of an SCC in the CAP construct with explanations of the fundamental configuration points.


CAP Cluster
SCC IP Address
SCC Port
-The way to the application
-This information goes to the application
SCC host name
-The location, where the SCC has to be started
LM VF
FM VF
UM VF
CM VF
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
HiPath CAP

6.1 HiPath 4000 connectivity

6.1.1 Overview

HiPath 4000 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 I or 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 HiPath 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 HiPath4000 supports 16 "ACL-C+" application connections simultaneously. Depending on the software version, it may be that less than 16 "ACL-C+" application connections can be released.



6.1.2 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.

6.1.3 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.

"SCC" dialog

Field	Description
SCC Name	Enter a mnemonic name for the SCC here, e.g. "SCC-HP4000". 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.
SCC ID (optional)	Enter an ID for the SCC here; these identifiers must be unique within the entire HiPath CAP installation; they cannot be changed after configuration has been completed. They will be used later during device configuration to define a unique assignment of a device (phone, trunk, hunt group, RCG, etc.) to a switching system. In the Diagnostic Agent, this "SCC ID" is used to show the SCC in the list of the processes belonging to the CAP cluster. In the same way, the associated CA4000 process is listed under the name `CA4000_<SCC ID>`. 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. **Note**: When importing user data, the SCC ID must match the PBX ID in the import file.

Field	Description
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 `<Inst-Dir>\config\` using the "host name". A subdirectory called `telasserver_<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 HiPath CAP Service Starter on the specified SCC PC (cf. Section 4.3).
SCC IP address (cannot be edited)	This is where you specify the IP address of the PC on which the SCC process should run.
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, 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 III 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. In the case of old applications in "single-domain native mode", you should set the value required for the relevant application: • `CSTA I`: Interface is configured on CSTA Phase I. • `CSTA ACSE`: Interface is configured to CSTA Phase III and requires a login to the SCC via ACSE request (version 5) (for more information, see the HiPath CAP Application Developers' Guide), • `CSTA III`: Interface is configured on CSTA Phase III.

SCC configuration notes

- Neither the service name nor the service identifier is permitted to contain blanks.
- For distributed installation (which means that the SCC PC is not your own computer or local host), you must install HiPath CAP Service Starter on the specified SCC PC.
- The Diagnostic Controller uses the service node ID to administer an SCC and display it on the Diagnostic Agent GUI.

"CA4000" dialog

Field	Description
CA4000 IP address (cannot be edited)	This specifies the IP address of the PC on which the CAP CA4000 for this PBX connection is running. The SCC addresses this IP address for communication with the CA4000.
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 with the CA4000. Port 1040 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.
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 SCCHiPath4000/CA4000 PC is entered in the firewall list.
Speed-dial numbers	Only the SimplyPhone for Web/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.
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. SimplyPhone for Web/ComAssistant continues to use this code for each outgoing external call.
National prefix (optional)	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 (optional)	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.
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 this SCC.

Field	Description
Area code	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 this SCC. The area code must be transferred to the field on the right together with the main number and the overlap (optional) using the **Add** icon (green arrow).
Main number	Enter the number of the main connection within a local network (e.g. "722" for Siemens, Munich, Hofmannstraße). It defines the third part of a device ID in the canonical format that is assigned to this SCC. The "Main number" must be transferred to the field on the right together with the "Area code" and the "Overlap" (optional) using the **Add** icon (green arrow).
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.
Domain numbers	List of already configured area code/main number combinations.
NAC	In the case of Hicom/HiPath 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 node code (NAC) must be transferred to the field on the right together with the overlap (optional) using the **Add** icon (green arrow). 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.

The input fields, such as, **Speed-dial numbers**, **Outside line access**, and **National and International prefixes**, are provided for use in conjunction with CTI applications, such as, HiPath SimplyPhone for Web/ComAssistant. These are described in the relevant documentation (for example, HiPath SimplyPhone for Web or HiPath ComAssistant documentation).

"Switch PNP" dialog

Field	Description
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	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 this SCC. The "Level 2 code" must be transferred to the field on the right together with the "Level 1 code", the "Local code" and the "Overlap" (optional) with the **Add** icon (green arrow).
Level 1 code	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 this SCC. The "Level 1 code" must be transferred to the field on the right together with the "Level 2 code", the "Local code" and the "Overlap" (optional) with the **Add** icon (green arrow).

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 this SCC. The "Local code" must be transferred to the field on the right together with the "Level 2 code", the "Level 1 code" and the "Overlap" (optional) with the **Add** icon (green arrow).
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.

Actions

Action	Description
Add	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.

6.2 HiPath 3000 connectivity

6.2.1 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 S_0connection.
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!

6.2.2 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.

6.2.3 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.

"SCC" dialog

Field	Description
SCC Name	Enter a mnemonic name for the SCC here, e.g. "SCC-HP3000". 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.
SCC ID (optional)	Enter an ID for the SCC here; these identifiers must be unique within the entire HiPath CAP installation; they cannot be changed after configuration has been completed. They will be used later during device configuration to define a unique assignment of a device (phone, trunk, hunt group, RCG, etc.) to a switching system. In the Diagnostic Agent, this "SCC ID" is used to show the SCC in the list of the processes belonging to the CAP cluster. In the same way, the associated CA4000 process is listed under the name `CA4000_<SCC ID>`. 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. **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 `<Inst-Dir>\config\` using the "host name". A subdirectory called `telasserver_<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 HiPath CAP Service Starter on the specified SCC PC (cf. Section 4.3).
SCC IP address (cannot be edited)	This is where you specify the IP address of the PC on which the SCC process should run.
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).

Field	Description
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 III XML, and NetTSPI protocols. The SCC state is always "active". If you select a CSTA-ASCE protocol version, the SCC operating mode changes to "single-domain native mode". In this mode, the SCCHiPath3000 passes a protocol through on a one-to-one basis, and its status is "not ready" if there is no application connection. In the case of old applications in "single-domain native mode", you should set the value required for the relevant application: • CSTA ACSE: Interface is configured to CSTA Phase III and requires a login to the SCC via ACSE request (version 4, user:"AMHOST", password."77777") (further details can be found in the HiPath CAP Application Developers' Guide).

SCC configuration notes

- Neither the service name nor the service identifier is permitted to contain blanks.
- For distributed installation (which means that the SCC PC is not your own computer or local host), you must install HiPath CAP Service Starter on the specified SCC PC.
- The Diagnostic Controller uses the service node ID to administer an SCC and display it on the Diagnostic Agent GUI.

"Switch" dialog

Field	Description
IP address of the Switch (optional)	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 SimplyPhone for Web/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.
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. SimplyPhone for Web/ComAssistant continues to use this code for each outgoing external call.
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.
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 this SCC.

Field	Description
Area code	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 this SCC. The area code must be transferred to the field on the right together with the main number and the overlap (optional) using the **Add** icon (green arrow).
Main number	Enter the number of the main connection within a local network (e.g. "722" for Siemens, Munich, Hofmannstraße). It defines the third part of a device ID in the canonical format that is assigned to this SCC. The "Main number" must be transferred to the field on the right together with the "Area code" and the "Overlap" (optional) using the **Add** icon (green arrow).
Overlap	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.
Domain numbers	List of already configured area code/main number combinations.
NAC	In the case of Hicom/HiPath 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. The "NAC" (node access code) must be transferred to the field on the right together with the "Overlap" (optional) using the **Add** icon (green arrow).
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.

The input fields, such as, **Speed-dial numbers**, **Outside line access**, and **National and International prefixes**, are provided for use in conjunction with CTI applications, such as, HiPath SimplyPhone for Web/ComAssistant. These are described in the relevant documentation (for example, HiPath SimplyPhone for Web or HiPath ComAssistant documentation).

"Switch PNP" dialog

Field	Description
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	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 this SCC. The "Level 2 code" must be transferred to the field on the right together with the "Level 1 code", the "Local code" and the "Overlap" (optional) with the **Add** icon (green arrow).
Level 1 code	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 this SCC. The "Level 1 code" must be transferred to the field on the right together with the "Level 2 code", the "Local code" and the "Overlap" (optional) with the **Add** icon (green arrow).

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 this SCC. The "Local code" must be transferred to the field on the right together with the "Level 2 code", the "Level 1 code" and the "Overlap" (optional) with the **Add** icon (green arrow).
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.

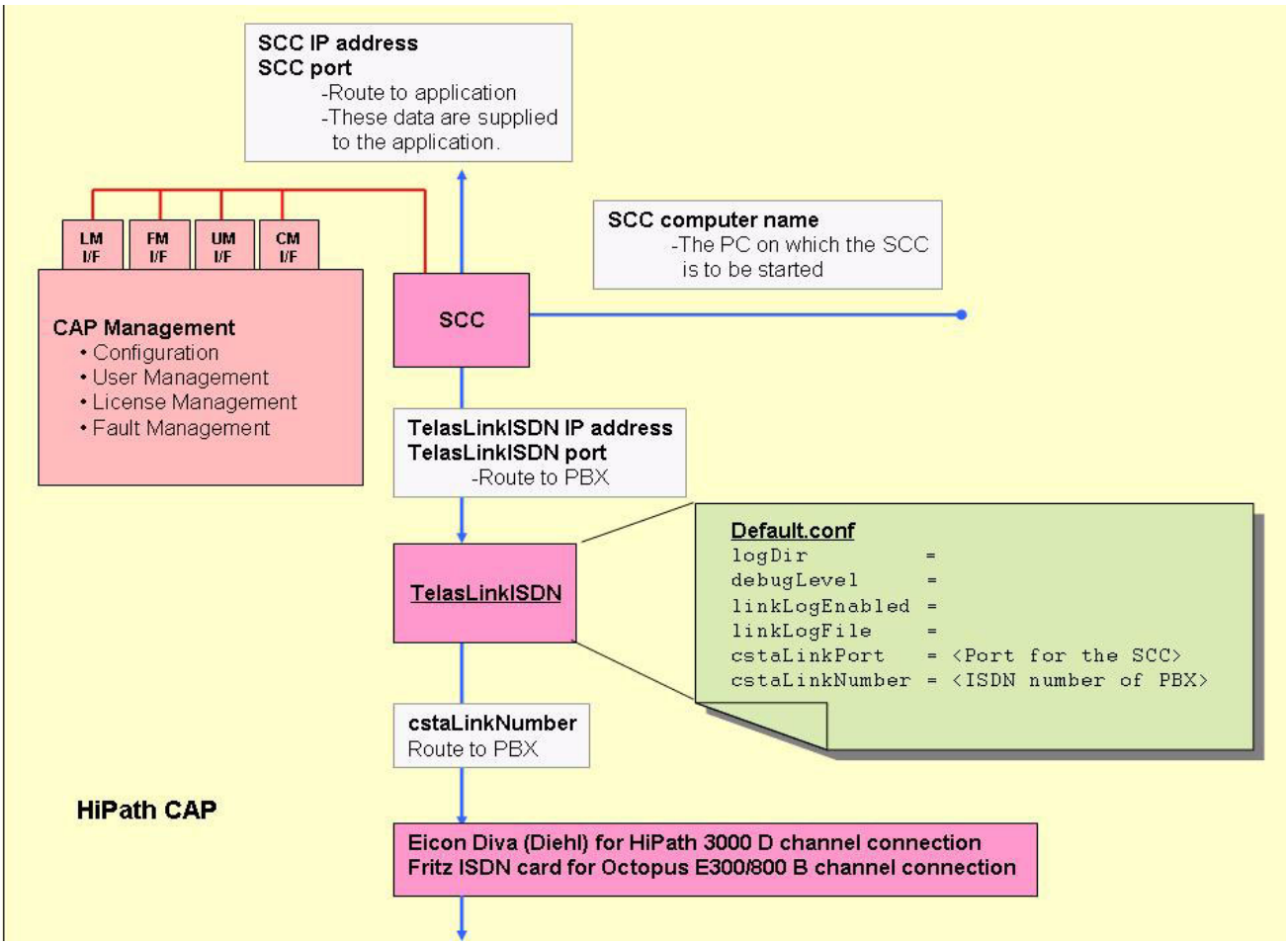
Actions

Action	Description
Add	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 HiPath 3000/Octopus E 300/800 connectivity by ISDN link

An ISDN link one of a number of SCC connectivity options in HiPath 3000 but the only option in Octopus E300/800. You must use a new program `TelasLinkISDN.exe` as a TCP/IP-ISDN converter for this. This program can only be started once on each PC with the result that you must use a separate PC for each HiPath 3000/Octopus E300/800 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 made via the D channel and is only supported by the Eicon Diva (Diehl) ISDN card.
The ISDN connection to the Octopus E300/800 is made via the B channel and is supported by the Fritz ISDN card, for example.
There are two different versions of the `TelasLinkISDN.exe` program: one version for the D channel and one for the B channel connection.



6.3.1 Configuring the program `TelasLinkISDN.exe`

The `TealsLinkISDN.exe` program is not installed automatically. Instead, it must be copied manually from the CAP CD.

- The program for the HiPath 3000 D channel connection is on the CD in the directory "`\Software\ISDNLink`".
- The program for the Octopus E300/800 B channel connection is on the CD in the directory "`\Software\ISDNLink\A6`".

You can copy the program into any directory. Naturally, it makes sense to create a new directory, such as, "`<InstDir>\HiPathCTI\ISDNLink\HiPath3000\`" or "`<InstDir>\HiPathCTI\ISDNLink\OctopusE\`" and copy the program into that path.

Now create a text file with the name `Default.conf` in this directory.
Open this file and add the following configuration parameters to it:

- **logDir**
  defines the directory for outputting log files.
- **debugLevel**
  ISDNLink supports logging with an adjustable degree of detail.
  Select an integer between 0 (logging is switched off) and 9 (logging with maximum detail).
- **linkLogEnabled**
  defines whether data specific to the connection should also be included in the log.
- **linkLogFile**
  defines the name of the log file.
- **cstaLinkPort**
  defines the TCP/IP port over which the SCC can address the ISDNLink.
  Make sure that this value agrees with the configuration value "CAP Link ISDN Port" when configuring the SCC.
- **cstaLinkNumber**
  defines the telephone number with which the Octopus E300/800 can be addressed via ISDN.

Example of a file: `Default.conf`

```
############################################################
#       Configuration File for ISDN <-> TCP router         #
############################################################

logDir     C:\Programme\Siemens\HiPathCTI\Logs\>PC-Name>
debugLevel     9
linkLogEnabled 1
linkLogFile    link.log
cstaLinkPort   2555          # <Connection port for SCC>
cstaLinkNumber 891           # <PBX's ISDN number>


#EOF after this line -- do not remove!
```

6.3.2 "ISDNLink" as a Windows service

A Windows service is automatically configured by the following call to activate the program `TelasLinkISDN.exe` automatically when the PC starts up. This call assumes that the program `TelasLinkISDN.exe` is in the directory that was previously recommended.

The call

`<InstDir>\HiPathCTI\ISDNLink\HiPath3000\TelasLinkISDN.exe -I`

generates the Windows service

`Siemens CAP Call Control Service LinkISDN H150E.`

The call with the "`-u`" switch deletes this Windows service!

The call

`<InstDir>\HiPathCTI\ISDNLink\OctopusE\TelasLinkISDN.exe -I`

generates the Windows service

`Siemens CAP Call Control Service LinkISDN Octopus E300.`

The call with the "`-u`" switch deletes this Windows service!

6.4 Hicom 300 connectivity

6.4.1 Overview

HiPath 300 does not support a standardized protocol for communication with applications. For this reason, it is absolutely necessary to use the "Connectivity Adapter Hicom 300" (CA300) protocol converter. The CA300 converts the Hicom 3000 (ACL-C) proprietary protocol into a standardized protocol (CSTA I). CSTA is a standard for computer-supported telephony (CTI) that was established by the international standardization organization ECMA (European Computer Manufacturers Association). With HiPath CAP V3.0, the CA300 can only be used in conjunction with the SCCHicom300. All CA300 configuration parameters are integrated in the SCCHicom300 configuration. The physical connection between the Hicom 300 and a PC that is running CA300/SCCHicom300 is made with the help of a TCP/IP LAN connection.

Hicom 300 supports 16 "ACL-C" application connections simultaneously. Depending on the software version, the number of "ACL-C" application connections released may be less than 16.

Depending on the Hicom 300 version, it may be necessary to change the accompanying configuration file `telas.cfg` manually.

```
# PBX Switch Version/Release
# ============================================================
# switchVersion = 300 -> Hicom 300 E International 2.0, default if unset
# switchVersion = 310 -> Hicom 300 E + Hicom 300 H 3.0
# switchVersion = 311 -> Hicom 300 E UK 3.1
# switchVersion = 320 -> Hicom 300 E US/Canada 6.6
switchVersion = 310
```

6.4.2 Preparation

Configure the SCCHicom300 to connect a Hicom 300. Its configuration menu also offers the CA300 configuration parameters. If SL100 is used to set up the connection to the Hicom 300, the IP address or the IP network of the
SCCHicom300/CA300 PC must be included in the Hicom 300 firewall list.

6.4.3 Configuration

To connect a Hicom 300 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 300** 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.

"SCC" dialog

Field	Description
SCC Name	Enter a mnemonic name for the SCC here, such as "SCC-H300". 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.
SCC ID (optional)	Enter an ID for the SCC here; these identifiers must be unique within the entire HiPath CAP installation; they cannot be changed after configuration has been completed. They will be used later during device configuration to define a unique assignment of a device (phone, trunk, hunt group, RCG, etc.) to a switching system. In the Diagnostic Agent, this "SCC ID" is used to highlight the SCC in the list of processes belonging to the CAP cluster. In the same way, the associated CA300 process is listed under the name CA300_<SCC ID> . The Hicom node number (for example, 0247, 0091) is usually used here. Up to 32 characters (letters, numbers, underscore, and hyphen) are permitted. **Note**: When importing user data, the "SCC ID" must match the "PBX ID" in the import file.

Field	Description
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 `<Inst-Dir>\config\` using the "host name". A subdirectory called `telasserver_<SCC ID>` is added for the SCC. 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 HiPath CAP Service Starter on the specified SCC PC (cf. Section 4.3).
SCC IP address (cannot be edited)	This is where you specify the IP address of the PC on which the SCC process should run.
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, 26538).
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 III 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. In the case of old applications in "single-domain native mode", you should set the value required for the relevant application: • `CSTA I`: Interface is configured on CSTA Phase I

SCC configuration notes

- Neither the service name nor the service identifier is permitted to contain blanks.
- For distributed installation (which means that the SCC PC is not your own computer or local host), you must install HiPath CAP Service Starter on the specified SCC PC.
- The Diagnostic Controller uses the service node ID to administer an SCC and display it on the Diagnostic Agent GUI.

"CA300" dialog

Field	Description
CAP CA300 IP address (optional)	As an option, you can specify the IP address of the PC on which the CAP CA300 runs for this PBX connection. The SCC addresses this IP address for communication with the CA300. If you do enter a value here, you are assumed to be operating on the local PC (local host 127.0.0.1) because SCC and CA300 are running on the same PC.
CAP CA300 port (optional)	The port provided by CA300 for this connection may be specified here (1025-5000). The SCC addresses this port for communication with the CA300. Port 1040 is used by default. We recommend using port 1300 or higher because there are occasionally problems with Windows processes that use ports in the range 1025 to 1299.
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

"Switch" dialog

Field	Description
IP address of the Switch	Enter the Hicom 300 IP address here. If the connection uses the SL100, make sure that the IP address or the entire IP network of the SCCHicom300/CA300 PC is entered in the firewall list.
Speed-dial numbers	Only the SimplyPhone for Web/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 Hicom 300 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.
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. SimplyPhone for Web/ComAssistant continues to use this code for each outgoing external call.
National prefix (optional)	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 (optional)	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.
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 this SCC.

Field	Description
Area code	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 this SCC. The area code must be transferred to the field on the right together with the main number and the overlap (optional) using the **Add** icon (green arrow).
Main number	Enter the number of the main connection within a local network (e.g. "722" for Siemens, Munich, Hofmannstraße). It defines the third part of a device ID in the canonical format that is assigned to this SCC. The "Main number" must be transferred to the field on the right together with the "Area code" and the "Overlap" (optional) using the **Add** icon (green arrow).
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.
NAC	List of already configured area code/main number combinations.
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.

The input fields, such as, **Speed-dial numbers**, **Outside line access**, and **National and International prefixes**, are provided for use in conjunction with CTI applications, such as, HiPath SimplyPhone for Web/ComAssistant. These are described in the relevant documentation (e.g. for HiPath SimplyPhone for Web).

"Switch PNP" dialog

Field	Description
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	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 this SCC. The "Level 2 code" must be transferred to the field on the right together with the "Level 1 code", the "Local code" and the "Overlap" (optional) with the **Add** icon (green arrow).
Level 1 code	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 this SCC. The "Level 1 code" must be transferred to the field on the right together with the "Level 2 code", the "Local code" and the "Overlap" (optional) with the **Add** icon (green arrow).
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 this SCC. The "Local code" must be transferred to the field on the right together with the "Level 2 code", the "Level 1 code" and the "Overlap" (optional) with the **Add** icon (green arrow).

Field	Description
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.

Actions

Action	Description
Add	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 Connecting TelasServer 3.1/Hicom 300

6.5.1 Overview

For reasons of compatibility, TelasServer 3.1 is also supported for connecting to the ACL-H3 interface of the Hicom 300. It does not support any CSTA interfaces and can only be directly addressed by the SimplyPhone for Web and the ComAssistant applications. A special TAPI Service Provider (Telas TSP) must also be installed for Microsoft TAPI-based applications.

TelasServer 3.1 is usually run on a separate PC and applications access TelasServer 3.1 via a specific TelasProxy; both are incorporated here. By configuring one Telas proxy per TelasServer 3.1, the CAP offers a communication interface for the SimplyPhone for Web and ComAssistant applications. The TelasServer 3.1 component (Software\Telas 3.1\TELAS BAS NT\TelasV31Setup.exe) must be separately installed locally in those places where it should also explicitly run.

6.5.2 Configuration

To connect TelasServer 3.1 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 **TelasServer 3.1** as the server version. This action configures a Telas proxy (instead of a Telas Server 3.1) with a TCP/IP connection to a Telas Server 3.1.
   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.

Dialog

Field	Description
SCC Name	Enter a mnemonic name for the TS3.1 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.
SCC ID (optional)	Enter an ID for the SCC here; these identifiers must be unique within the entire HiPath CAP installation; they cannot be changed after configuration has been completed. They will be used later during device configuration to define a unique assignment of a device (phone, trunk, hunt group, RCG, etc.) to a switching system. In the Diagnostic Agent, this "SCC ID" is used to highlight the SCC in the list of processes belonging to the CAP cluster. The Hicom node number (for example, 0247, 0091) is usually used here. Up to 32 characters (letters, numbers, underscore, and hyphen) are permitted. When importing user data, the "SCC ID" must match the "PBX ID" in the import file.
Telas Proxy host name (optional)	As an option, you can enter the host name of the PC on which the TelasProxy process is to run. A PC name directory is created in the directory `<Inst-Dir>\config\` using the "host name". A subdirectory called `telasproxy_<SCC ID>` is added for the Telas proxy. These subdirectories contain all configuration files for this process that is to be started.
Telas Proxy IP address (optional)	As an option, you can enter the IP address of the PC on which the TelasProxy process is to run. The IP address is determined automatically from the host name if no input is made here.
Telas Proxy port (optional)	As an option, you can enter the port to which the TelasProxy process is to be assigned. Port **8188** is used by default. If this port is occupied, enter another value here. This port is entered in the file `S20TelasProxy.proc`. Unlike the customary standard, the configuration file `TelasProxy.cfg` does not contain any individual configuration parameters whatsoever.
TelasServer IP address	As an option, you can specify the IP address of the PC on which TS3.1 runs for this PBX connection.
TelasServer port	Enter the port provided by the TS3.1 for this connection. The default port is **4711**.

Field	Description
Speed-dial numbers	Only the SimplyPhone for Web/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 Hicom 300 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.
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. SimplyPhone for Web/ComAssistant continues to use this code for each outgoing external call.
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 this SCC.
Main number	Enter the number of the main connection within a local network (e.g. "722" for Siemens, Munich, Hofmannstraße). It defines the third part of a device ID in the canonical format that is assigned to this SCC. The "Main number" must be transferred to the field on the right together with the "Area code" and the "Overlap" (optional) using the **Add** icon (green arrow).
Domain numbers	List of already configured area code/main number combinations.

Make sure that the required component **TelasServer 3.1** (Software\Telas 3.1\TELAS BAS NT\TelasV31Setup.exe) has been installed on the PC specified here.
These components cannot be installed using the HiPath CAP master setup. Please start the appropriate installation routines directly from the CD (details on this can be found in the Telas 3.1 Installation and Administration Manual).

The input fields, **Speed-dial numbers**, **Outside line access**, **Domain numbers**, etc. are provided for use in conjunction with CTI applications such as HiPath SimplyPhone for Web. These are described in the relevant SPW documentation.

Actions

Action	Description
Add	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.

6.6 Media Service connectivity

6.6.1 Overview

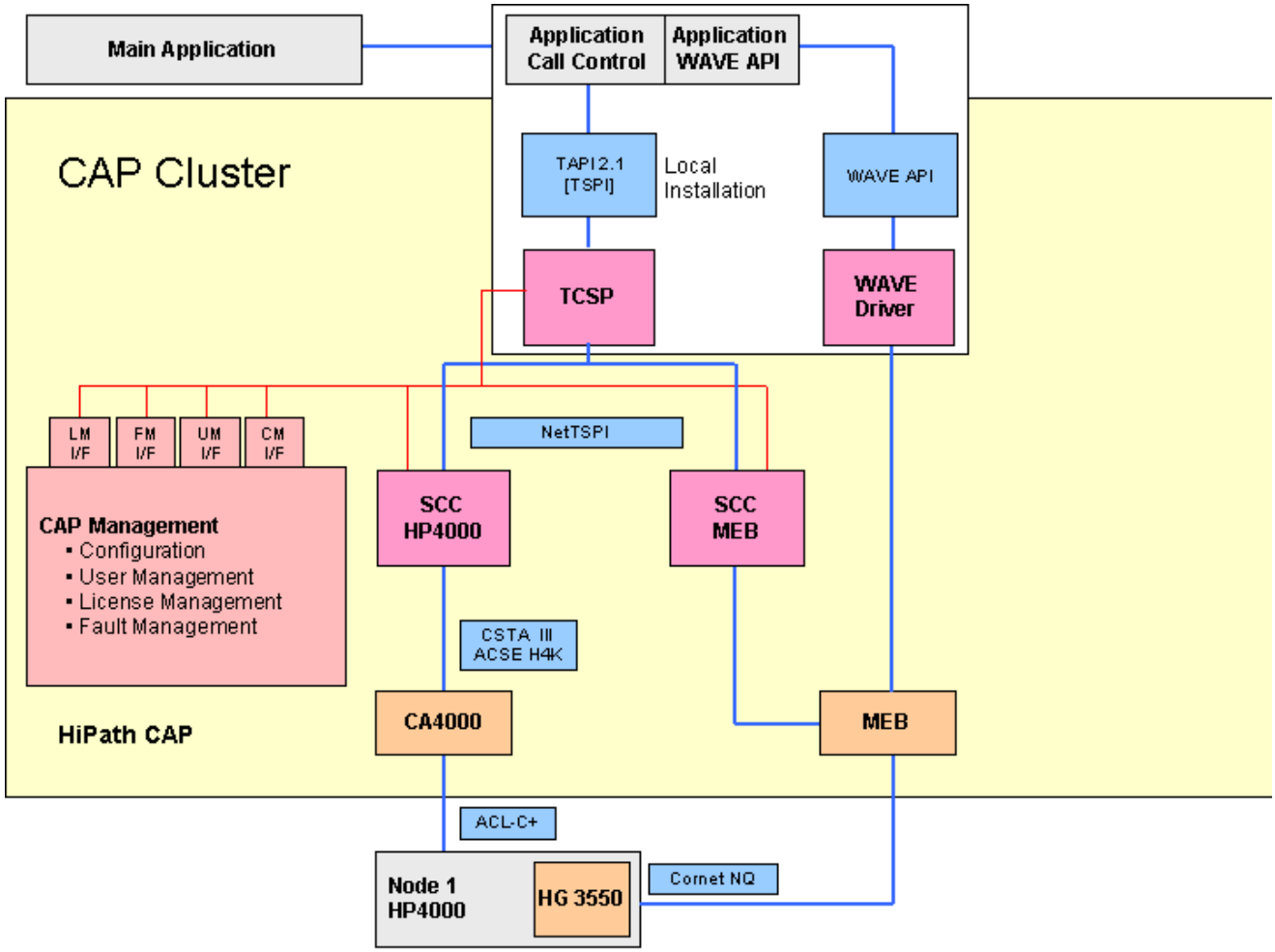
The HiPath CAP 3.0 Media Service is a software component that simulates a PBX with subscriber line interfaces (one subscriber per channel). This must be done by configuring a Cornet-NQ connection between the Media Service component MEB (Media Extension Bridge) and a HiPath 4000 HG3550 V2 or HiPath 3000 HG1500 V2. For Microsoft TAPI-based applications, the "wave/in" and "wave/out" features for playing and recording WAV or AVI files in 8 KHz/16 bit/mono format and the "Receive fax"/"Send fax" features are supported. Accordingly, an application is provided with "incoming call pickup" and "outgoing dialing" features for these functions.

The media service mainly consists of three components:

- **Siemens Virtual Wave Driver**
  A virtual driver for outputting or recording IP audio data using the Windows Wave API; similar, for example, to a sound card driver (for driver installation, see Section 4.7, "Installing the Siemens Virtual Wave Driver").
- **MEB (Media Extension Bridge)**
  A central component for controlling the Siemens Virtual Wave Driver and for receiving, evaluating, and forwarding all relevant data between HiPath and applications via SCCMEB and CAP TCSP.
- **SCCMEB**
  A component for connecting CAP TCSP with the MEB.

The "Siemens Virtual Wave Driver" should always be installed locally on the PC where you want to run SCCMEB and MEB. The SCCMEB and MEB components are distributed after the standard routines of the distributed installation, which means that the "CAP ServiceStarter" must also be installed on this PC. Currently, a maximum of 30 simultaneous calls (channels) can be administered per MEB PC, assuming that there are enough CAP-M licenses available.

The following diagram shows how the Media Service and its components are integrated in CAP 3.0 architecture.



The following must be installed on all MEB PCs:

- the Siemens Virtual Wave Driver

The following must be configured in CAP 3.0 Management for each MEB PC:

- the SCCMEB
- the MEB
- the media application (or its communication adapter) for playing and recording WAV or AVI files (or faxes).

6.6.2 Configuration

To configure Media Service 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) There is no media connection configured yet or you are configuring a new media connection. Continue with 2a.
   b) A media connection is already configured. This will be displayed in a list. Continue with 2b.
2. Configure the media connection.
   a) If a media connection has not yet been configured, click the **Add new entry** icon and select **Media Streaming** as the server version.
   b) To edit the settings for a connection, select the connection by clicking the **Edit** icon for the chosen connection.

"SCC" dialog

Field	Description
Service Name	Enter a mnemonic name for the SCC here, e.g. "SCC-MEB". 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.
Service ID (optional)	Enter an ID for the SCCMEB here; These identifiers must be unique within the entire HiPath CAP installation. The service ID is used to define the assignment of the device to the SCCMEB during the automatic configuration of the accompanying MEB device. Up to 32 characters (letters, numbers, underscore, and hyphen) are permitted.

Field	Description
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 `<Inst-Dir>\config\` using the "host name". A subdirectory called `telasServer_<SCCMEB ID>` is added for the SCCMEB. A subdirectory called `MEBService_<SCC-MEB ID>` is added for the accompanying MEB. These subdirectories contain all configuration files for these processes that are to be started. **Note:** For distributed installation (meaning when the SCC PC is not your own PC/local host), ensure that you install HiPath CAP Service Starter and the "Siemens Virtual Wave Driver" on the specified SCC PC (cf. Section 4.3).
SCC IP address (optional)	The IP address of the PC on which the SCC process is running may be entered here. The IP address is determined automatically from the host name if no input is made here.
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, 26539)

"MEB" dialog

Field	Description
MEB IP address (optional)	Enter the IP address of the PC that is to use this MEB if more than one network card is installed in this PC.
MEB call number (optional)	A CAP user and CAP device are created automatically using this call number; the new device type is "MEBCallnumber" and the device is allocated directly to the CAP user. The media licenses (CAP-M) are assigned to the CAP user immediately, depending on the number of MEB channels configured. TAPI applications use this call number to address all configured MEB channels in order to send requests or receive events.
Max. number of channels	Enter the maximum number of channels for the MEB. Make sure that the corresponding number of CAP-M licenses is available.

Field	Description
Use length check	This option allows you to specify that the MEB is to perform a length check on the dialed call number for incoming calls before a waiting call is answered. The number of digits that HiPath must pass on to the MEB via CornetNQ when there is an incoming call must have been entered under **Call number length** in order for this check to be made. **Note:** If this option is enabled together with the **Use call number list** option, incoming calls are also checked according to both variants. If neither option is enabled, incoming calls are not answered by the MEB.
Call number length	Enter the length of the call number for checking here. **Note:** If transmission of the node access code is configured on the HiPath, you must take the length of the node access code into account when specifying the length of the call number.
Use call number list	The associated call numbers accepted as valid by the MEB can also be identified by the MEB via the call number list. Use this option to specify that the MEB must compare the numbers that HiPath transmitted to the MEB via CornetNQ for incoming calls with the entries in the call number list before answering the calls. For this, the call numbers or call number ranges to be accepted must be entered under**Call number list** (not in canonical format). **Note:** If this option is enabled together with the **Use length check** option, incoming calls are also checked according to both variants. If neither option is enabled, incoming calls are not answered by the MEB. **Note:** If transmission of the node access code is configured on the HiPath, you must take this into account when entering the call numbers.
Call number list	Enter the call numbers/call number ranges to be accepted here. A semicolon ";" is used as the separator for call numbers. Call number ranges are indicated with a dash "-", e.g. "1000-1010;2000;3020-3025".

Field	Description
Media gateway	Enter the IP address of the HG3550 V2 or HG3750 board to which the MEB is connected.
H225 signaling port	Enter the valid H225 signaling port for the MEB. If the PC contains other H.323 applications that use an H.225 port as well as the MEB, the port numbers should match. This includes NetMeeting. Port number "1720" is used by default. Alternatively you could enter port number "11720". Also make sure that the corresponding communications port was set up in the HG3550 V2 or HG1500!
DLS IP address	You can enter the DLS IP address of any existing/used DLS server (optional).

When the documentation was created, it was not possible to determine how to configure the communications port 11720 in the HG3550 V2. The CUSPN parameter, listed in the HG3550 V2 documentation's description of the AMO-STMIB:,,IFDATA, is probably responsible, but is not offered for configuring the change!

Actions

Action	Description
Add	Adds the entry to the Media Services connections list.
Close	Closes the **Add entry** dialog without saving the entries.
Delete	Deletes an existing Media Service connection. **Note**: This button only appears if at least one Media Service connection is already configured.

6.6.3 MEB user

One user is automatically entered for each added MEB. The user name comprises the abbreviation **MEBUser_** and the SCCMEB Service Name, for example `MEBUser_Meb`. The MEB call number is the device for the MEB user.

Page 1 of 1

User Id	Name	Alias	Role	Group	License	SCC	Devices	
Admin	CAP Administrator	Admin	Admin					
MEBUser_MEB1	MEBUser_MEB1	MEBUser_MEB1	Admin TWebUser			MEB1	+49(89)722-22470	
MEBUser_MEB2	MEBUser_MEB2	MEBUser_MEB2	Admin TWebUser			MEB2	+49(2302)98417-70001	
XMLPSUser	XMLPhoneService Account	XMLPSUser	Admin					
telasweb	SPW Account	telasweb	Admin					

6.7 Configuring a HiPath CAP Call Control Proxy (SCCP)

6.7.1 Overview

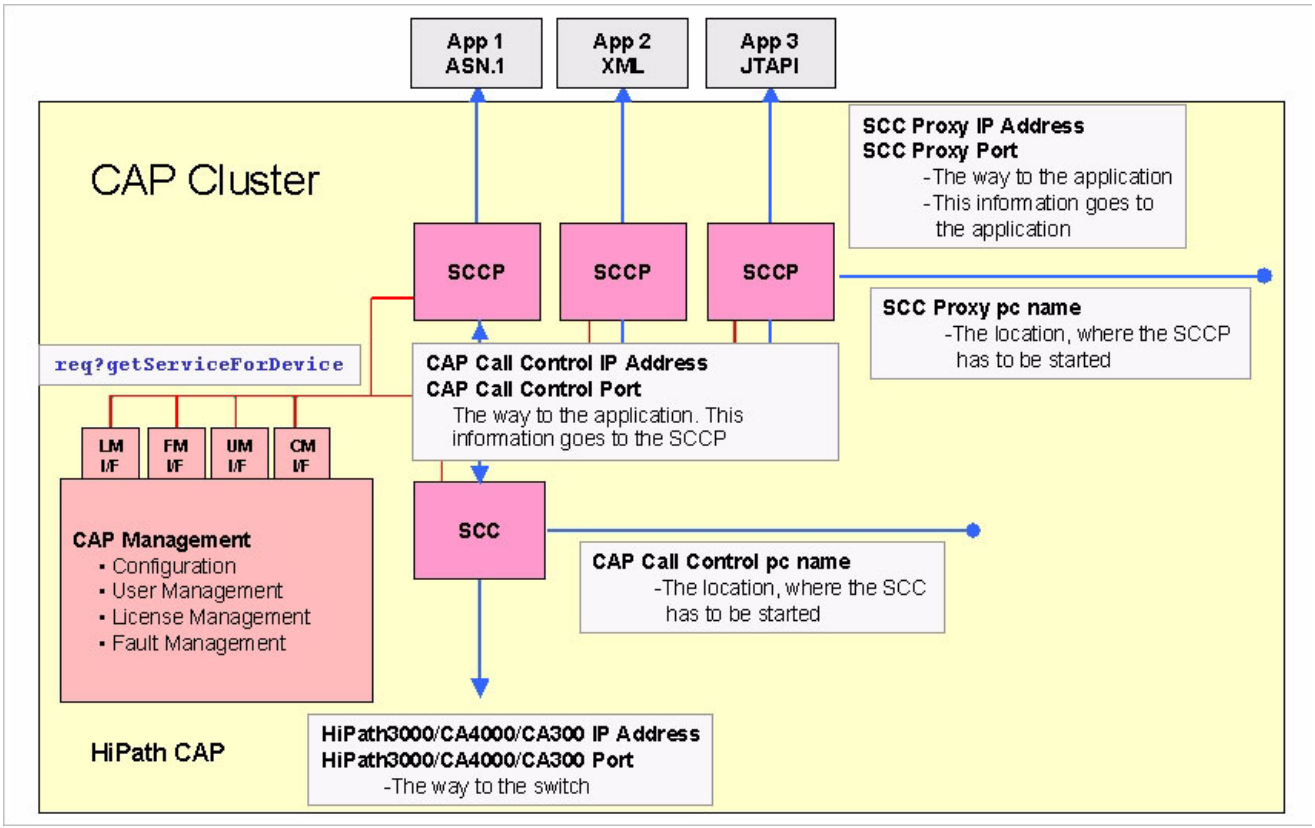
An SCCP instance should be configured for every application that is to use HiPath CAP in a CSTA or JTAPI multi-domain configuration and for every XML Phone Service.

SCC proxies are only used in "multi-domain mode". An SCCP supports the CSTA III ASN.1and CSTA III 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.



6.7.2 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
Service Name	Enter a mnemonic name for the SCC Proxy 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. Blanks are not permitted.
Service Identifier (optional)	Enter an ID for the SCC proxy here. These identifiers must be unique within the entire HiPath CAP installation. In the Diagnostic Agent, this "SCCP ID" is used to highlight the SCCP in the list of processes belonging to the CAP cluster. Up to 32 characters (letters, numbers, underscore, and hyphen) are permitted. Blanks are not permitted.
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 `<Inst-Dir>\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 HiPath CAP Service Starter on the specified SCCP PC (cf. Section 4.3).
SCC Proxy IP address (optional)	As an option, you can enter the IP address of the PC on which the SCCP process is to run. The IP address is determined automatically from the host name if no input is made here.
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).
Disable AP Emergency	You can only deactivate this feature if this SCCP will never set up a connection to an SCCHiPath4000 that is connected to a HiPath 4000 with CC-AP IPDA shelves and an alternative SCCHiPath4000.

SCCP configuration notes

- Neither the service name nor the service identifier is permitted to contain blanks.
- For distributed installation (which means that the SCCP PC is not your own computer/local host), ensure that you install HiPath CAP Service Starter on the specified SCCP PC.
- The Diagnostic Controller uses the service node ID to administer an SCCP and display it in the Diagnostic Agent GUI.

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 Further HiPath CAP Management Functions

You can use HiPath CAP Management to configure all of the HiPath CAP. HiPath 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 set up access to license management, configure the XML Phone Service and assign speed-dial numbers here.
- **User**
  This menu item encompasses user management, enabling you to add, change or remove users and bring users together to form user groups. In addition, this function allows you to install and assign licenses.
- **Device**
  This is where you configure and modify the devices (phones, trunks, hunt groups, etc.) of the various PBXs by assigning them to an SCC.
- **Data**
  Here you can make the settings for exporting or importing the HiPath CAP database. This function can be executed automatically using a timer. You can also back up the HiPath CAP database or reload an existing backup.
- **Diagnostics**
  This menu item is used to start the various diagnostic tools, such as 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.
- **Help**
  You can display the HiPath CAP documentation in the various formats and languages here.

The functions listed here can be found as menu items in the HiPath 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 Service

The Call Control Services and Call Control Proxies are configured in **Service**. You can also set up access to license management, configure the XML Phone Service and assign speed-dial numbers here.

7.1.1 Switch connection

Information on how to configure the Call Control Services with HiPath CAP Management is described in Section 6.1 to Section 6.6.

7.1.2 SCC proxy

Information on how to configure the Call Control Proxies with HiPath CAP Management is described in Section 6.7.

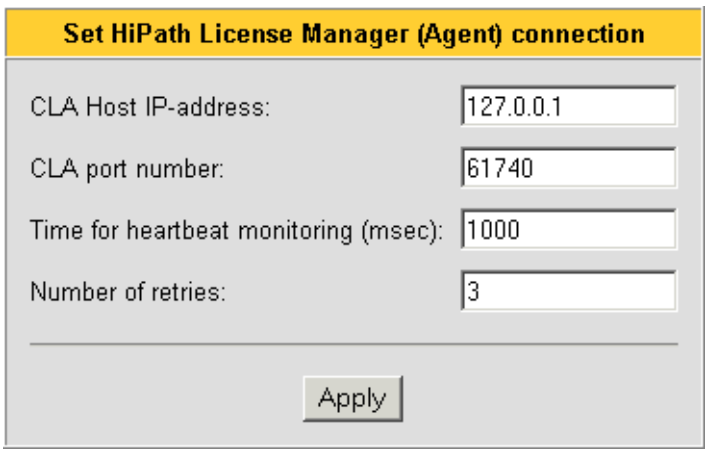
7.1.3 HLM connection (not yet implemented in this version)

> ⚠ Activating licenses via HiPath License Management will not be released until a later version of HiPath CAP.

Licenses are required to enable CTI users to use CTI functions. Depending on the application, these licenses can be activated via HiPath License Management or via the User Administration service implemented in HiPath CAP Management.
If you activate the licenses using HiPath License Management, you will need the License Agent (CLA, Customer License Agent) on a PC in your network and License Management (CLM, Customer License Management) on the same PC or another PC. CLA manages the licenses and License Management presents the user interface with which the licenses can be requested and installed on the CLA Licenses.

The connection to the CLA must be established for this purpose.

1. Click **Service** in the main menu and select the **HLM Connection** menu item in the navigation area.



2. Complete the fields described below:

Field	Description
CLA Host IP address	Not relevant in this version.
CLA port number	Not relevant in this version.
Time for heartbeat monitoring (msec)	Not relevant in this version.
Number of retries	Not relevant in this version.

3. Confirm your input with **Apply**.

7.1.4 XML Phone Service

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 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

XML Phone Service

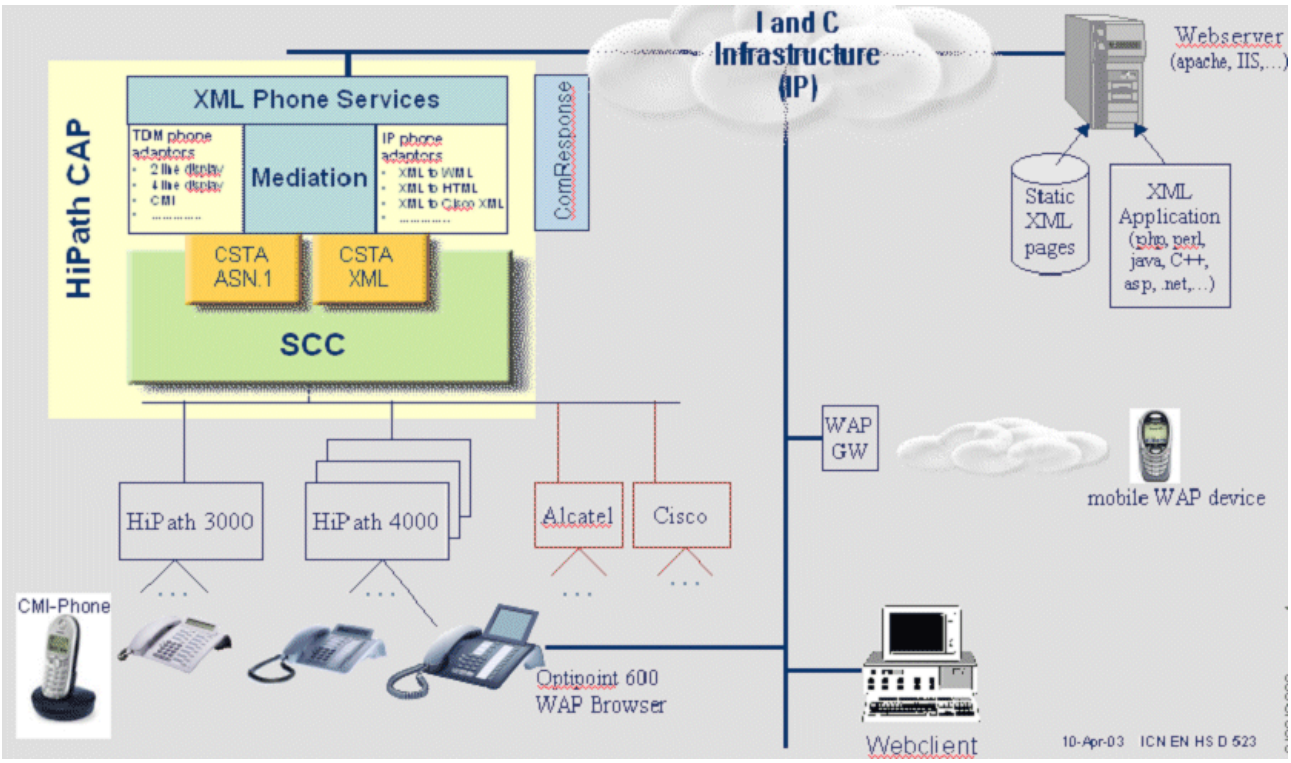
The XML Phone Service (XMLPS) is a CSTA III XML application that is always installed on top of SCCP. An XMLPS can operate different XML applications simultaneously. If you want to use more than one XML Phone Service, you must configure a new SCCP for each XMLPS. In addition, each XMLPS must have a separate 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 Servicestart: 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 Siemens optiset or optiPoint devices on a HiPath 4000. 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 display with 24 characters per line (only the UTF-8 character set is supported).
- All automatically generated terms are in English (EXIT, BACK SUBMIT). 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.



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.

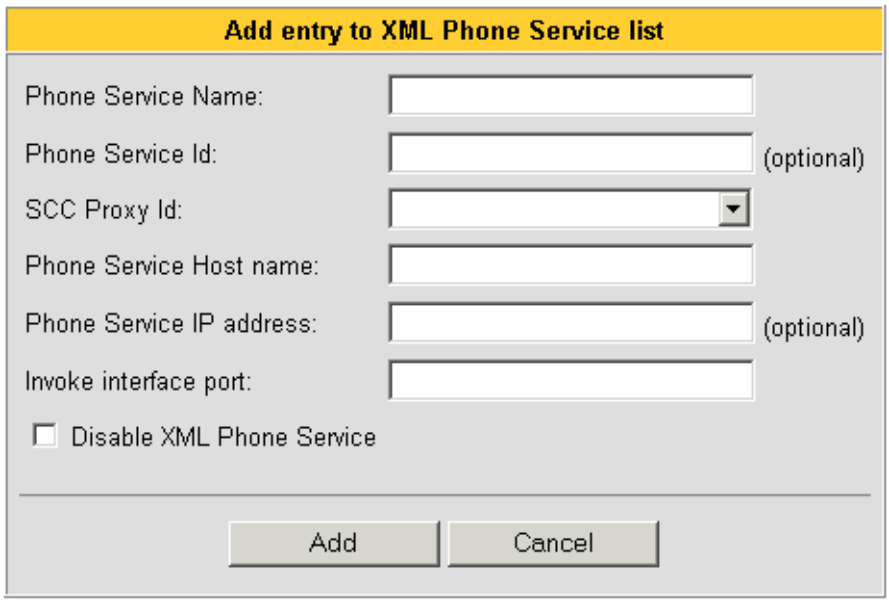
   a) No XML phone service is configured as of yet. Continue with 2a.

   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.

Field	Description
Phone Service Id (optional)	Enter an ID for the XML Phone Service here. These identifiers must be unique within the entire HiPath 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.
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 HiPath CAP is started.

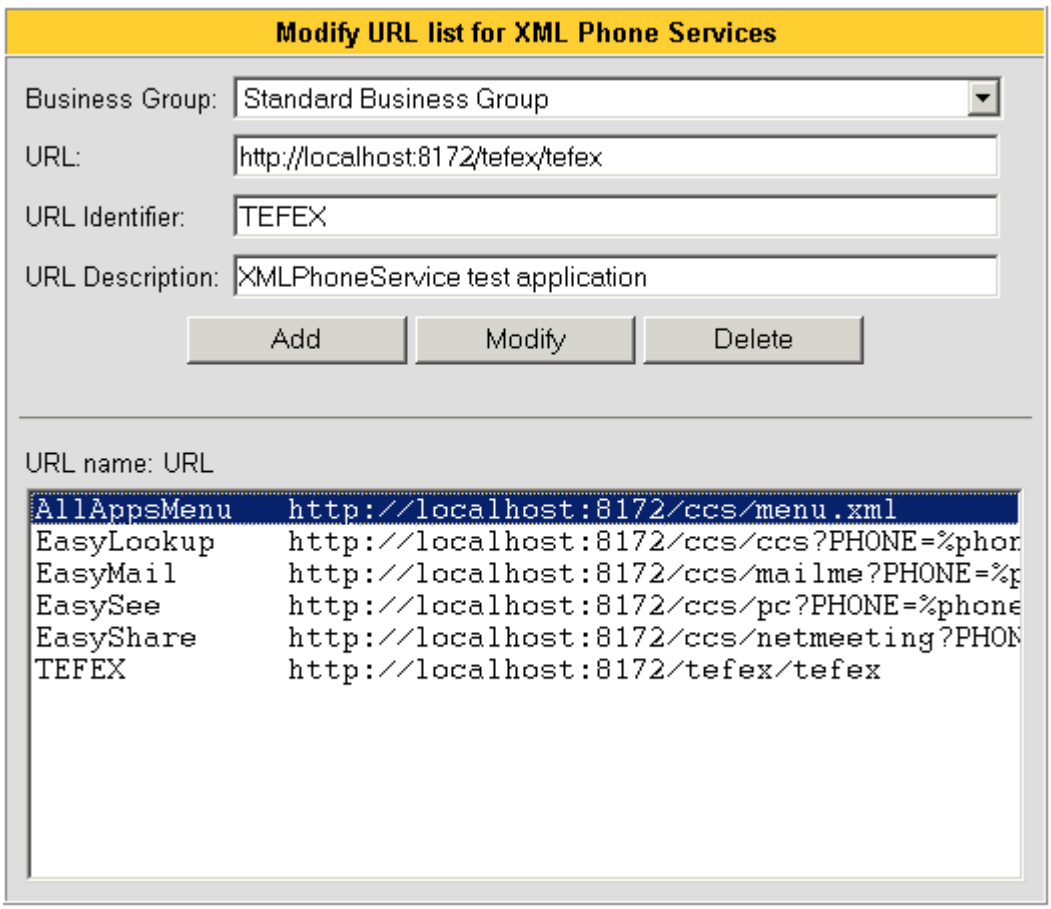
4. Complete your entries with one of the following actions:

Action	Description
Add	Adds the entry to the "XML Phone Service list".
Cancel	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.

7.1.5 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 HiPath CAP.

Add the URLs of the XML Phone Service applications here; these can be assigned to the "phone devices" later. The Siemens 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	The default selection is "Standard Business Group". Additional business groups are displayed if HQ8000 user information has been imported (split up by business groups). Business groups are currently used only in conjunction with HiPath8000/hiQ8000. The assignment of users to a business group is made exclusively on the basis of the data imported from the PBX. It is only displayed in CAP Management; it cannot and may not be changed.
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 appear 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.

4. Click the **Submit** button to save your entries and changes.

7.1.6 Defining speed-dial numbers

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.

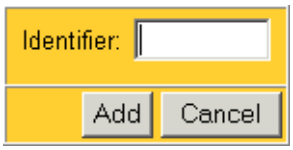
1. Click **Service** in the main menu and select the **Speed-Dial Numbers** menu item in the navigation area.

   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:

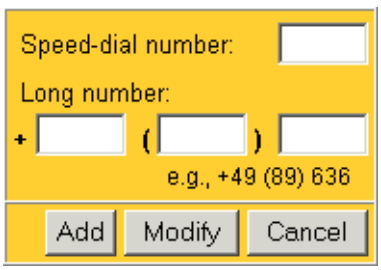
1. Click the  button next to the **Speed-dial number ID** selection window.

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



2. 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:



3. 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.

4. Confirm with **Add** and your entry will appear in the **Speed-Dial Number/Long Number** window.
5. Click **Cancel** to close the window.
6. 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 User

The functions for administering users of the HiPath 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)

In addition to user management, license management is also administered here. You can find a description of license management in Section 7.3, "License Management".

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 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 is meaningless here. For successful authentication, the corresponding license must **not** be installed in the CAP.

ComAssistant: The ComAssistant application uses CAP User Management to authenticate its application users. The following inputs are possible for unambiguous identification of a CAP user:

- User ID
- Alias (-name)
- 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 user.

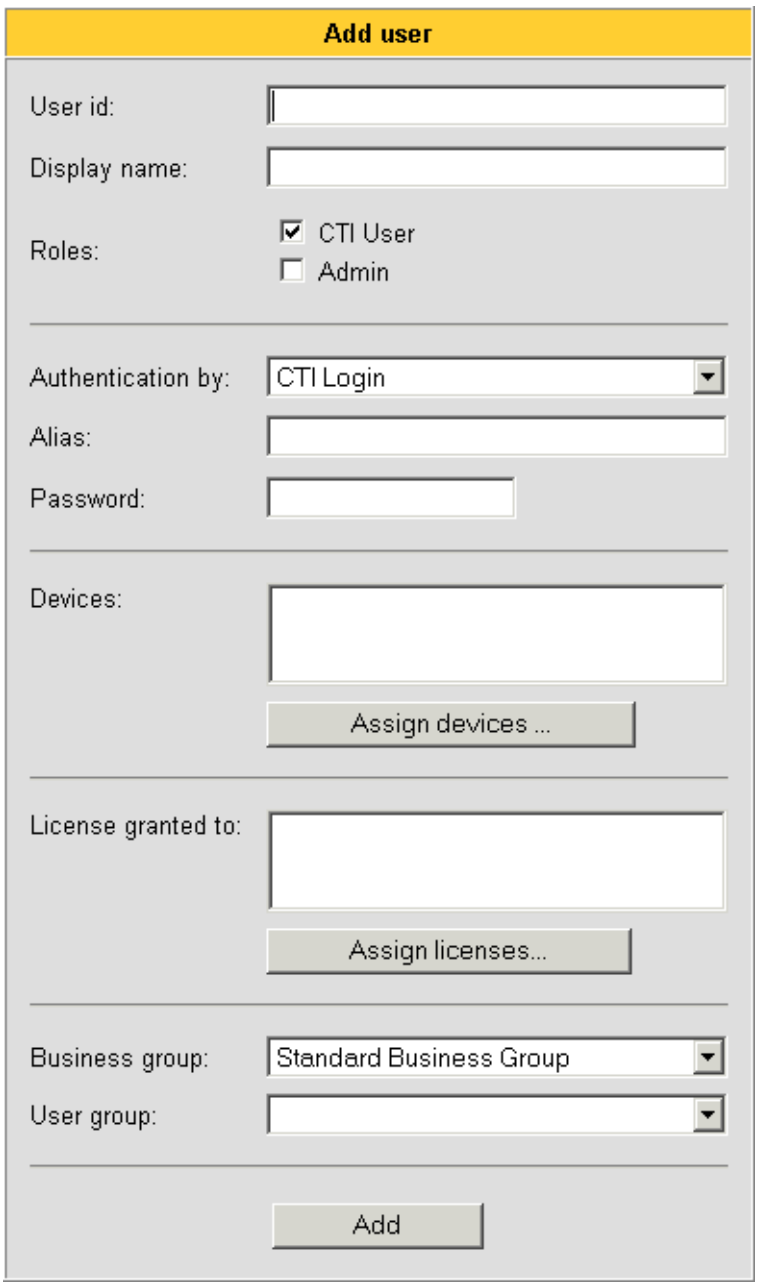
CTI client licensing

The SCCP stores the "Application ID" transmitted in the ACSE_AARQ request 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 application ID that is transmitted as an option by the CAP TCSP in TAPI `"lineDevSpecificFeature"`.
The SCCP/SCC 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/SCC saves this information for 3600 seconds.

7.2.1 Add user

In this dialog, users with different roles or rights can be configured. Authentication can be performed by HiPath CAP Management or the Windows 2000/2003 operating system.

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



2. 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 call 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 authorized as an administrator (with access to HiPath CAP Management functions), as a CTI user ("normal" user without administrator rights) or both. An administration user does not have to have an extension number. To authenticate external applications, the administration user "CAP" is configured by default with the password "123". Use is optional, and can naturally differ depending on the application. An application can also be authenticated with a CTI user.
Authentication by	You can choose two different types of authentication via the dropdown menu: • **CTI Login** The login is handled by HiPath 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. 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** | **Settings** I **Default Password**. See Section 7.2.3 for details.
Username **(**for authentication is 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.
Devices	Select a device that should be assigned to this user from the list of phone devices that have already been configured.

Field	Description
License granted to	If assignment of licenses by the administrator is set for applications (see Section 7.3.3, **User I Assign Licenses,** Option **at user administration** enabled), then the licenses for using the applications must be explicitly assigned here. Select the application from the list (for example, ComAssistant). Licenses can be assigned for several applications simultaneously . User licenses that have already been assigned can also be deleted. If the "Implicitly during license check" feature is active in License Management for a particular license, this is automatically granted and also shown here during the license check. **Temporary licenses** (license overflow) have a "*" as additional identification. To use these to create normal licenses, you must either import more client licenses according to the application ID or perform the following steps: – Delete licenses that have already been assigned to CTI users. – Search for CTI users with temporary licences, select them, one after the other, and explicitly confirm these with **"Change"**.
Business group	The default selection is "Standard Business Group". Additional business groups are displayed if HQ8000 user information has been imported (split up by business groups). Business groups are currently used only in conjunction with HiPath8000/hiQ8000. The assignment of users to a business group is made exclusively on the basis of the data imported from the PBX. It is only displayed in CAP Management; it cannot and may not be changed.
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. **Note:** To enable a user group to be selected, it must first be configured under **User I Manage User Groups**.

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

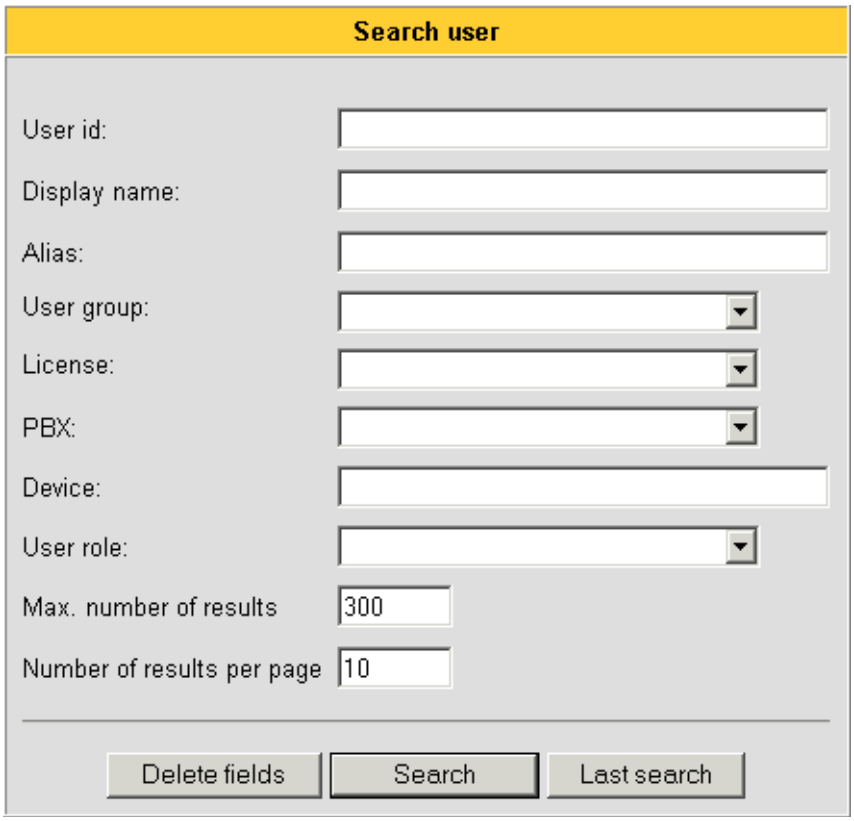
   `User entered: <User ID> (for example, 495251827486)`

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

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

7.2.2 Finding and modifying user entries

1. Click **User** in the main menu and select the **Search/Modify** menu item in the navigation area. The following 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.

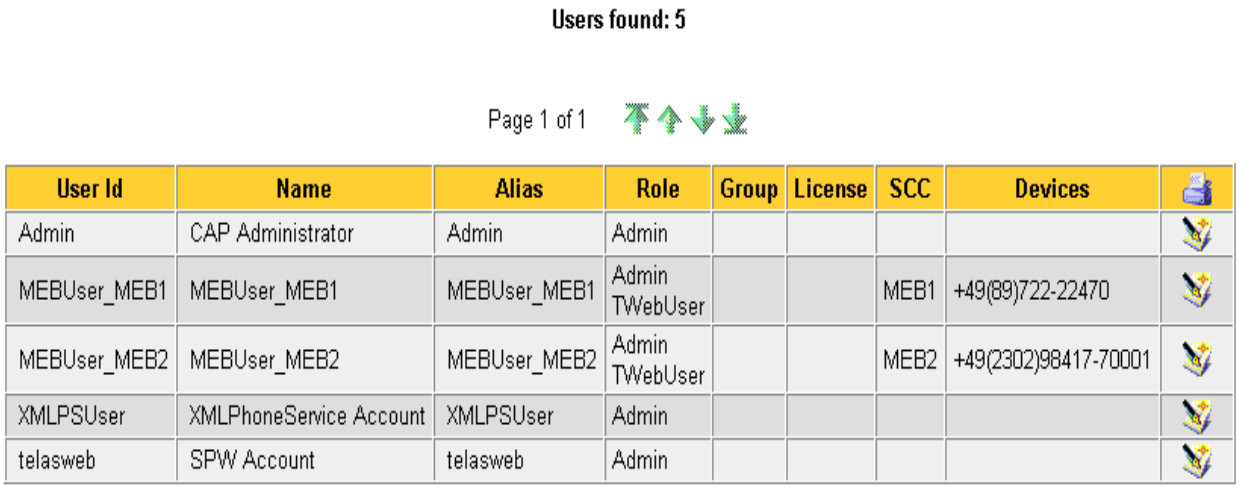
"Search user" dialog

Field	Description
User id, **Display name**, **Alias**, **Group**, **License**, **PBX**, **Device,** **User role**	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 "Group", "License", "PBX" (SCC), and "User role" always show only what has also been configured in the 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.

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.
Last search	All fields contain 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 inquiry appears in a list.

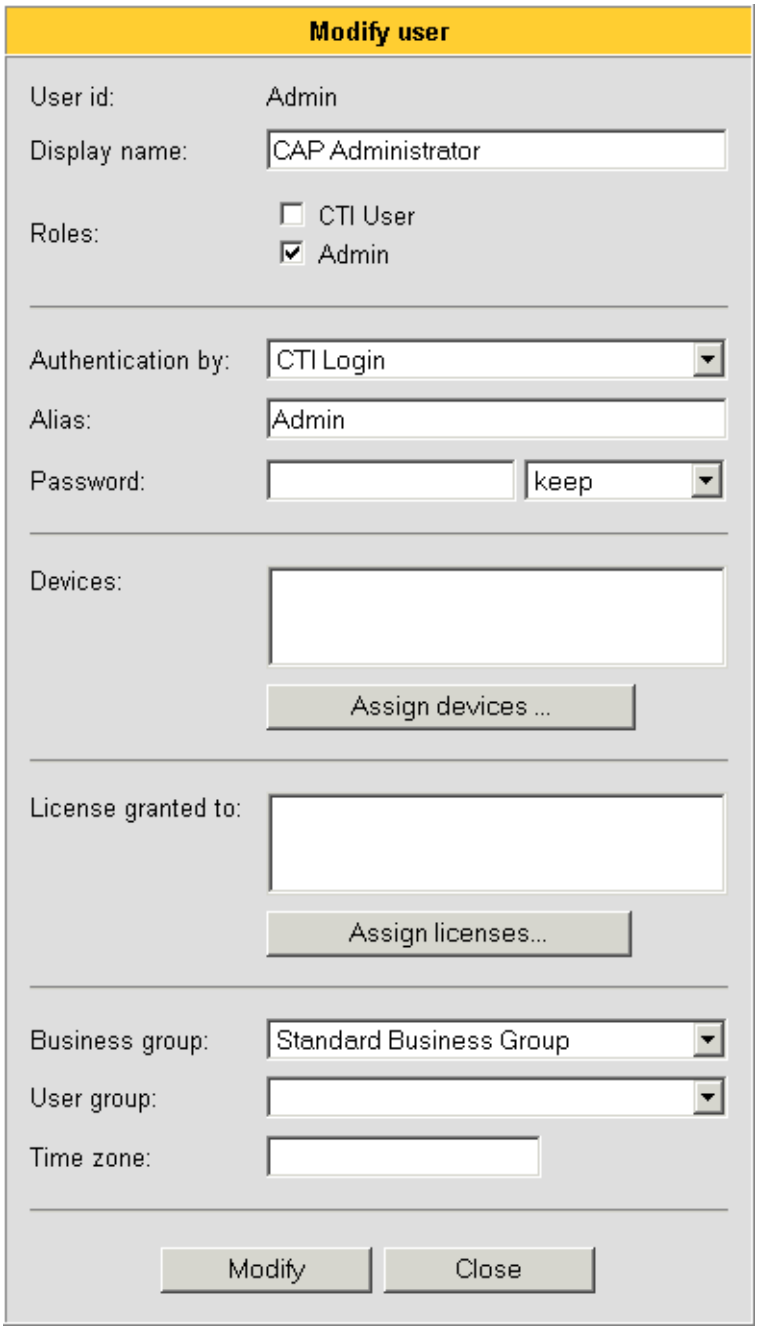


User Id	Name	Alias	Role	Group	License	SCC	Devices	
Admin	CAP Administrator	Admin	Admin					
MEBUser_MEB1	MEBUser_MEB1	MEBUser_MEB1	Admin TWebUser			MEB1	+49(89)722-22470	
MEBUser_MEB2	MEBUser_MEB2	MEBUser_MEB2	Admin TWebUser			MEB2	+49(2302)98417-70001	
XMLPSUser	XMLPhoneService Account	XMLPSUser	Admin					
telasweb	SPW Account	telasweb	Admin					

Use the cursor control keys to navigate through several pages (first - next - previous - last page). The printer icon can be used to obtain a print preview of the results list in a separate window.

If only one result is found, then step 4 is skipped.

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 7.2.1.

> The user ID cannot be modified because it acts as a unique ID for the user.

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

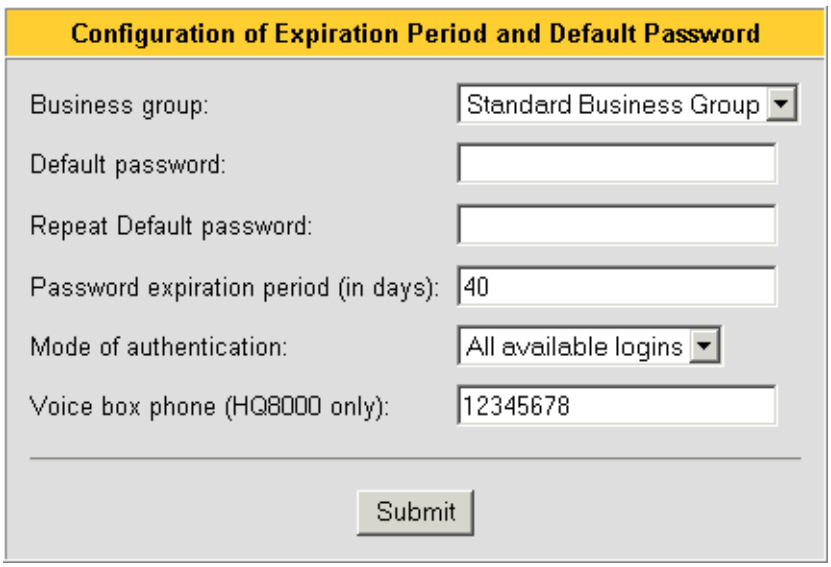
The default password is defined under **User | Settings | Default Password**. See Section 7.2.3 for details.

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`)

7.2.3 Settings for the default password

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



2. Enter the required data in the input fields.

"Configuration of Expiration Period and Default Password" dialog

Field	Description
Business group	The default selection is "Standard Business Group". Additional business groups are displayed if HQ8000 user information has been imported (split up by business groups). Business groups are currently used only in conjunction with HiPath8000/hiQ8000. The assignment of users to a business group is made exclusively on the basis of the data imported from the PBX. It is only displayed in CAP Management; it cannot and may not be changed.

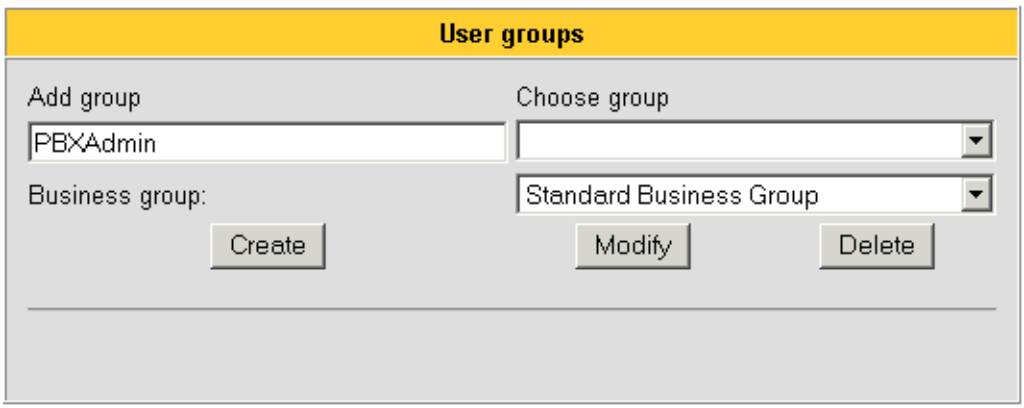
Field	Description
Default password	Define the default password. This password is valid if you do not specify a password when you create a new user entry or if you reset the password using **Reset** when you change a user entry (see Section 7.2.2). If the default password is assigned when new users are added or when user data is modified, the user is prompted to change this password during initial login. The default password is "**123456**".
Repeat Default password	For security purposes repeat the password entered under **Default password**.
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.
Mode of authentication	Use the dropdown 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 HiPath 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.

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

7.2.4 User groups

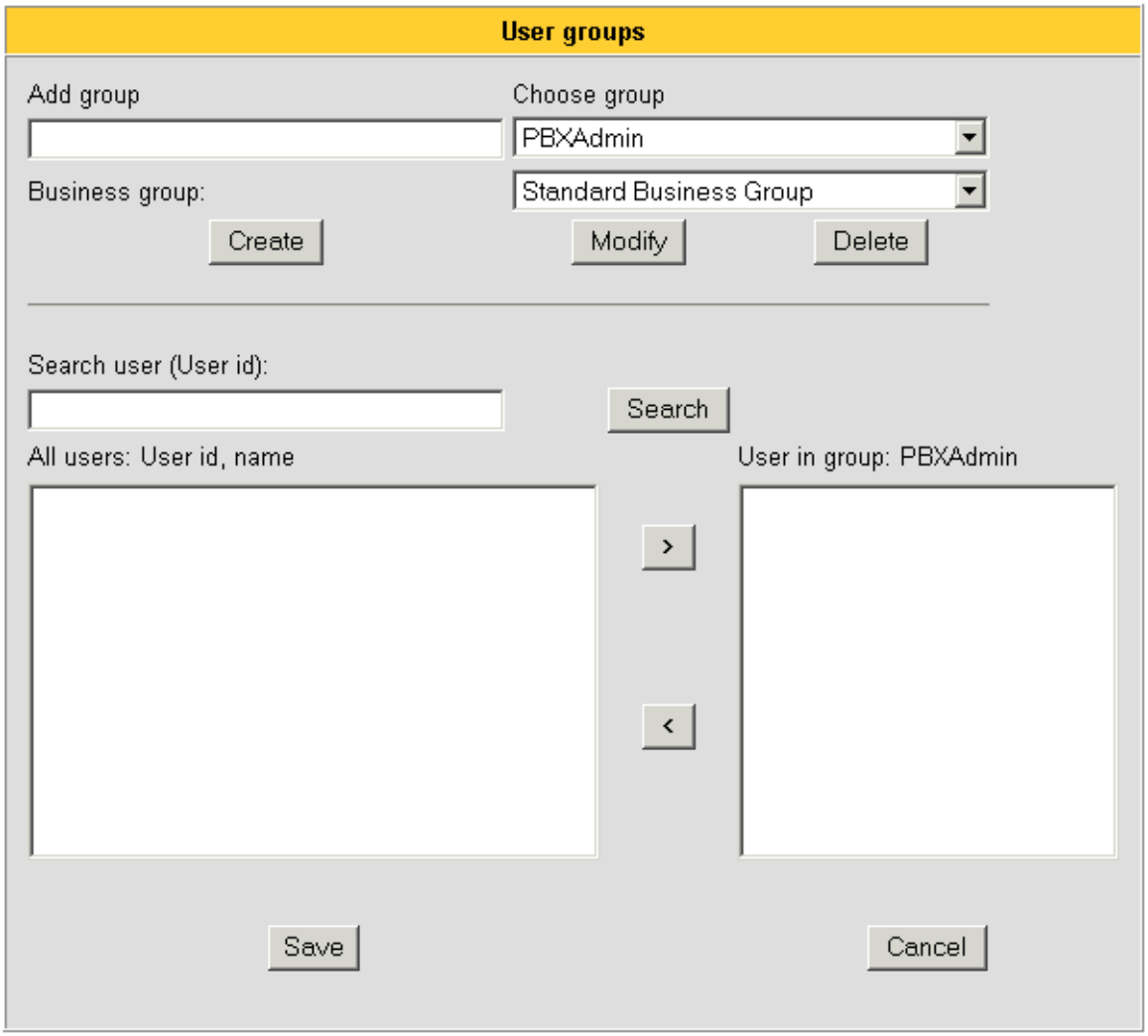
You can define user groups and change existing user groups here.
The ComAssistant currently uses user groups for displaying the buddy list. CAP TCSP uses user groups for automatically including a defined user group as a TAPI line device.

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



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.



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 License Management

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 **User** main menu also offers you functions for administering licenses for using the HiPath CTI system. You can:

- View licenses
- Assign licenses
- Install licenses
- Uninstall 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 CAP user or CAP device during the first CSTA or NetTSPI request.
If the "at user logon" feature is activated, the license that was handed over as the application ID in the ACSE_AARQ (for CSTA request) is implicitly assigned to a user or device.
For TAPI applications (CAP TAPI Service Provider/NetTSPI), an internal routine first requests the license CAP, then CAP-A, CAP-S, and CAP-E, if an individual application ID was not handed over by a TAPI "lineDevSpecificFeature" within 10 seconds after a TAPI "lineOpen".

The HiPath CAP V1.0 license "UNKNOWN" which licensed the number of monitor points to be set in a CA4000 is not needed 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 licenses are already installed (MAC address FF-FF-FF-FF-FF-FF) and cannot be deleted. After initial assignment of a client license, the associated demo license is valid for an additional two months and is marked with an "expiration date". Once this date expires, users can no longer be controlled by the corresponding application. The same applies if there are no more client licenses available. The user is then given a temporary license that is valid for two months (marked with a "*" in user management) and the corresponding license is marked with an "expiration date". Once this date expires, users can no longer be controlled by the corresponding application.

To use these to create normal licenses, you must either import more client licenses according to the application ID or perform the following steps:

- Delete licenses that have already been assigned to CTI users.
- Search for CTI users with temporary licences, select them, one after the other, and explicitly confirm these with **"Change"**.

E-mail message when licenses are exceeded

An e-mail message that repeats daily if the number of licenses assigned exceeds the number of licenses installed can be configured. In the following file:

```
C:\Program Files\Siemens\HiPathCTI\config\common\global.cfg
```

the following text lines must be changed:

```
<?x set MAIL_SERVER = "Name des SMTP fähigen Emailservers"?>
```

```
<?x set MAIL_SENDER = "<?x $TelasWebName?> notification <Name of the mail sender>"?>
```

```
<?x set MAIL_SYSADMIN = "Name des Emailempfängers"?>
```

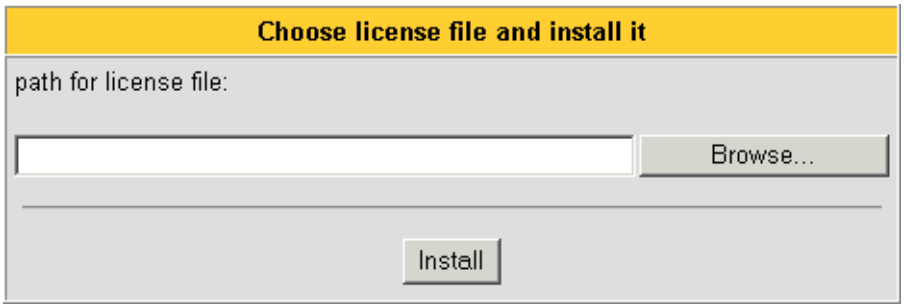
7.3.1 Installing licenses

Licenses are installed via license files. These files can be obtained from the same source as the HiPath CAP software. For Siemens customers this is usually Production. Working on the basis of order and delivery data, the administrator is capable of generating licenses for downloading by means of a special Production web site.

To prevent misuse, license keys are linked to the HiPath 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 HiPath 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 **User** in the main menu and select the **Install Licenses** menu item in the navigation area.



3. Specify the absolute path of the license file here.
4. With **Install**, the license file is analyzed and the new licenses are made available.

7.3.2 Showing licenses

1. Click **User** in the main menu and select the **Show Licenses** 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	6	94 (10/13/2004 10:54)

Details licenses

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

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.

7.3.3 Assigning licenses

There are two ways to assign licenses to individual users:

- If you use demo licenses or if **new licenses** are installed, the default is for the **"implicitly during license check"** feature to be active. This means that during each first licensing request (`registerLicense`) to the CAP Management for a CAP user, a corresponding license will be granted if this license is available and the user was not yet granted the requested license. If the number of client licenses available is exceeded, temporary licenses that are valid for two months are automatically granted.
  Note for TAPI applications: Because the only applications that do not transmit an individual application ID for licensing are almost exclusively TAPI applications (`lineDevSpecificFeature`), the SCC internally carries out a step-by-step license request in the order "CAP", "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 "during user configuration". This ensures that demo licenses are allocated only when this is desired.
- Alternatively, the administrator can *explicitly* assign licenses to a user when configuring the user in HiPath CAP User Management (cf. Section 7.2.1). If there are no more available licenses when setting up the user ID, the administrator receives a corresponding error message.

Licenses can also be granted to a specific user during the data import in "hdms format".

1. Click **User** in the main menu and select the **Assign Licenses** menu item in the navigation area to define the assignment process.

Please, enter when to be assigned a license:

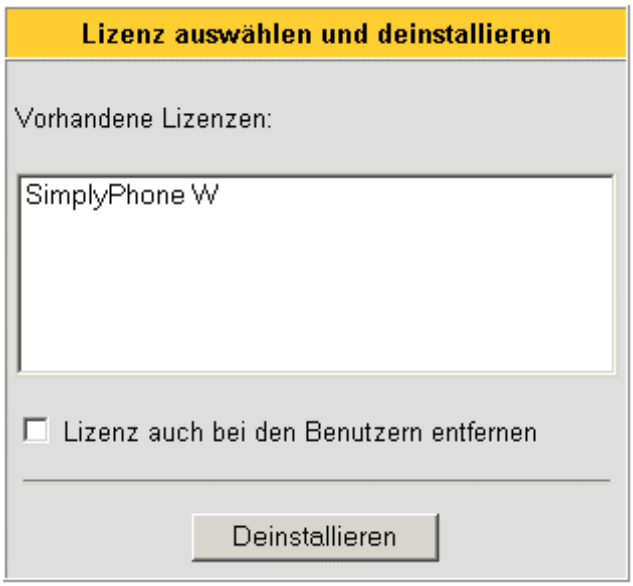
Application	at user administration	at user logon
CAP-E	☐	☑
CAP-S	☐	☑
CAP-A	☐	☑
ComAssistant	☐	☑
	Save	

2. For each of the license keys/application IDs available, select implicit assignment (first come/first served) or "at user administration" (explicit assignment by the administrator).
3. Click **Save** to confirm your selection.

7.3.4 Deleting licenses

Sometimes it is necessary to delete already installed licenses.

1. Click **User** in the main menu and select the **Uninstall Licenses** menu item in the navigation area.



2. Select the application for which the license key is to be deleted.
3. If you also wish to remove the licenses to be deleted for users to whom these licenses have been assigned, then select "Also remove license for users"
4. Click **Uninstall** to execute the action.

7.4 Device

"Extensions" (type: phone), "virtual extensions" (type: virtual device), "RCG groups", "hunt groups", and "lines" associated with the various PBXs are assigned to different SCCs by means of their device IDs. The device ID is either a selectable long call number in canonical format (for example, +49(5251)8-27486) or, for lines, an unambiguous administration number in CAP Management that comprises the SCC ID and the position of the corresponding module or channel (for example, +SCC-H4K-1+1-67-1+0 = +<SCC ID>+<position>+channel). "RCG groups", "hunt groups" and "lines" can only be imported, however. Additional device types are "SIP", "FaxNumber", "MailAddress", "RoutingDevice", and "MGCP". They can also only be imported. The last device type, "MEBCallNumber", is automatically added when a SCCMEB/MEB is configured. If a device type is not "Phone" or "Virtual Device", it cannot be administered.

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. This is the method used by the SCCP, CAP TCSP, and ComAssistant Phone Controller.

Extensions and virtual extensions are assigned to CAP users so that these devices can be controlled or monitored via a CTI application. This is because they can only be licensed by a CAP user. In contrast, RCG groups, hunt groups, and lines can also be licensed without assigned users. At this time, however, this can only be done if the necessary license can be implicitly assigned.

Devices and applications

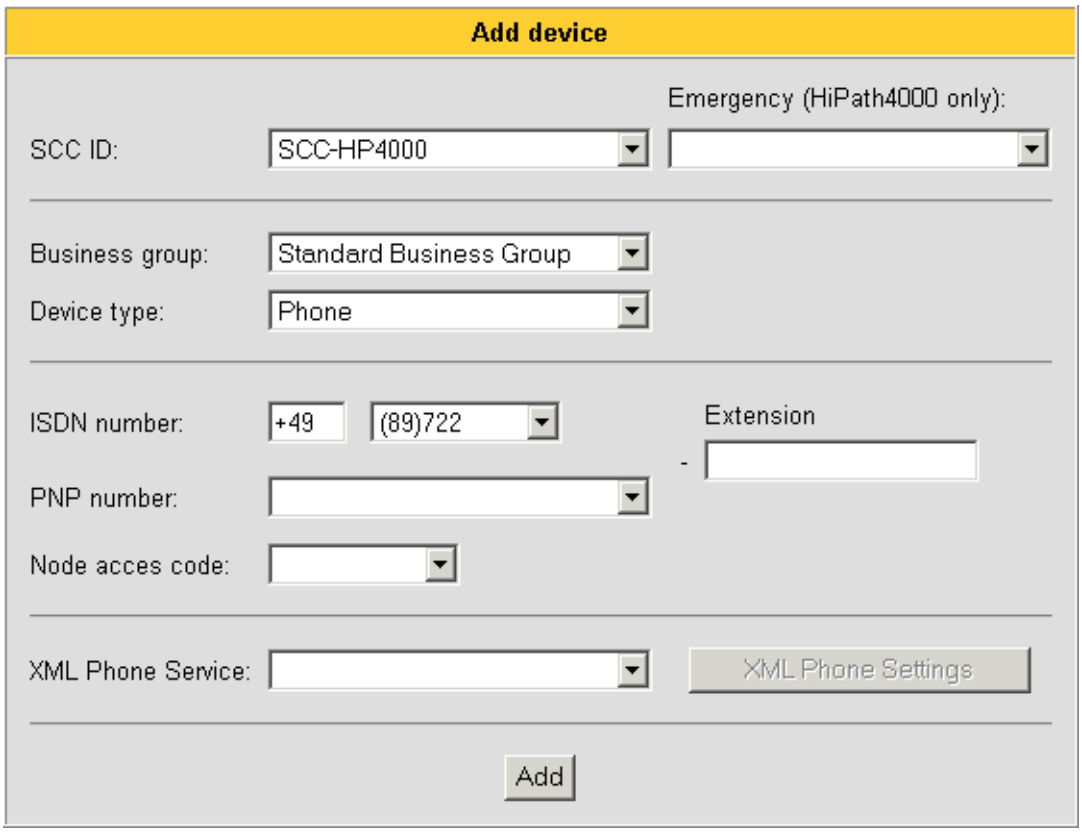
Using "Address Translation Service" (SAT) features, an application can always use the associated call number in canonical format to address a device. Conversion into a number that the SCC can use for addressing is done using the display in the "PBX format" field of a device. If an overlap is configured,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

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.



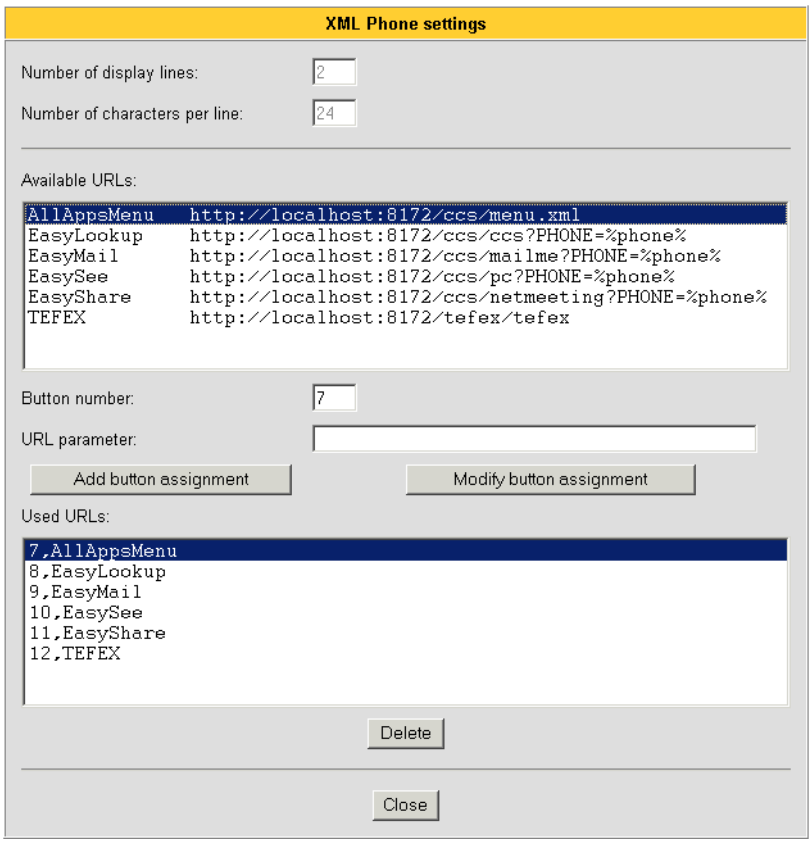
2. Enter the data for the new device in the relevant fields. The fields are described in the table below.

"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 4000 only)	If this device is located in an IPDA shelf in which the new "CC-AP" (Common Control for Access Point SCC Emergency) hardware has been installed and if an additional SCCHiPath4000/CA4000 is configured for this IPDA shelf, select the SCC ID of this alternative SCC here. If the HiPath4000 server (or the SCC/CA connection to this HiPath 4000 server) fails, this device can still be addressed and monitored via the alternative SCC.
Business group	The default selection is "Standard Business Group". Additional business groups are displayed if HQ8000 user information has been imported (split up by business groups). Business groups are currently used only in conjunction with HiPath8000/hiQ8000. The assignment of users to a business group is made exclusively on the basis of the data imported from the PBX. It is only displayed in CAP Management; it cannot and may not be changed.
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	Selection list with ISDN codes (country code/local code/ main number). Together with the extension, this yields an international phone number that is unique worldwide. The ISDN code selection list is created during SCC configuration and can be changed at a later time.
PNP number	Selection list with PNP codes (Level2/Level1/Local code) Together with the extension, this yields a unique PNP number in the private network. The PNP code selection list is created during SCC configuration and can be changed at a later time.

Field	Description
Node access code	Selection list with NACs (Node Access Codes). Together with the extension this yields a unique station number (e.g. 96-1234 / 99-1234) in the open numbered Hicom/HiPath network. The node access code selection list is created during SCC configuration and can be changed at a later time.
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	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 selectable 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 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	Select an XML Phone Service you wish to enable for the device from the dropdown list. **XML Phone Settings** is then enabled (see below).

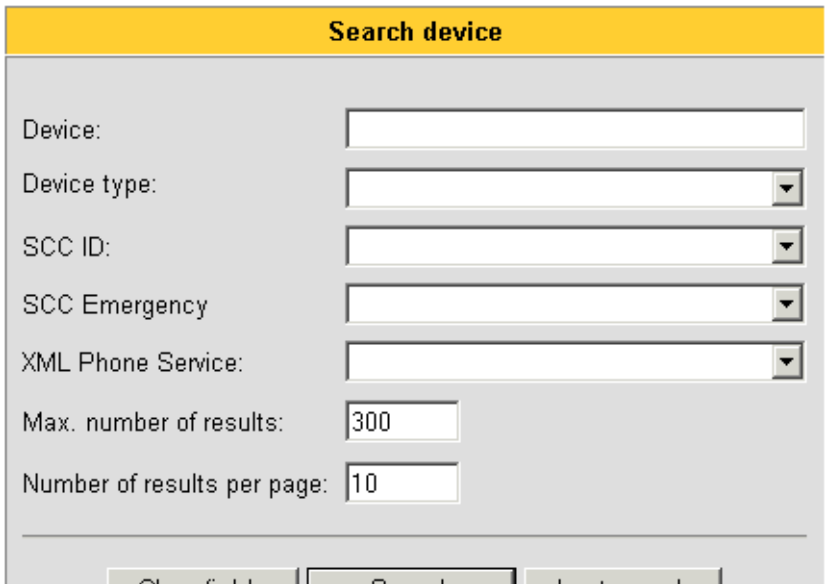
Field	Description
XML Phone Settings	If you click the **XML Phone Settings** button, you will be offered the following setting options: • **Number of display lines** Setting cannot be changed. • **Number of characters per display line** Setting cannot be changed. • **Button number** The number of the 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.



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

7.4.2 Finding 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.

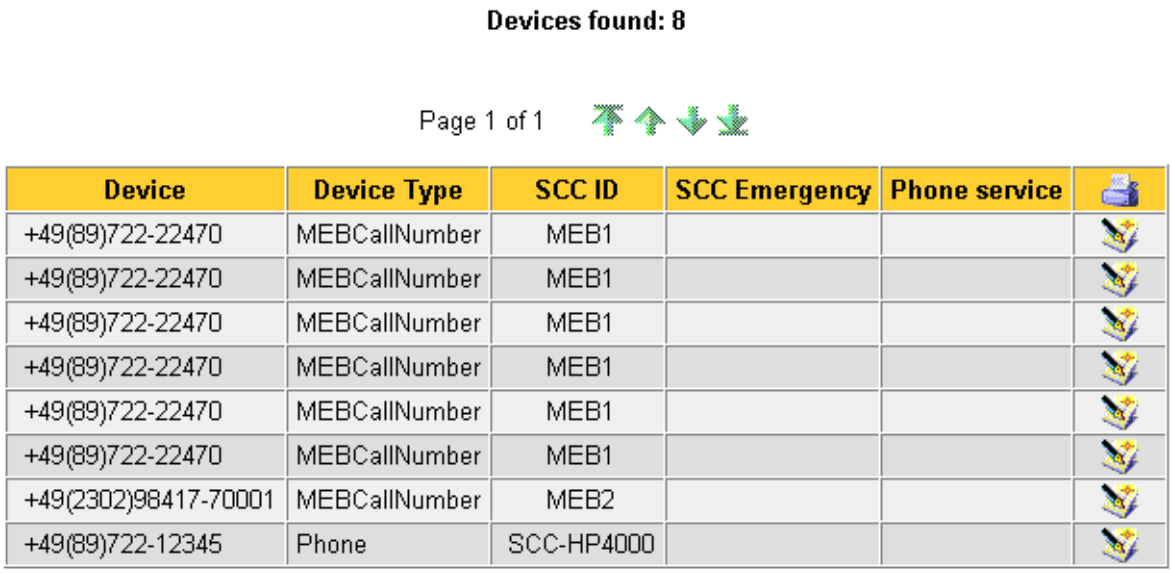
"Search device" dialog

Field	Description
Device	You can search for the name of the device here.
Device type	You can search for the device type here.
SCC ID	You can search for the switch connection used by the device here.
SCC Emergency	You can search for alternative SCCs that are connected to an IPDA shelf with CC-AP hardware installed.
XML Phone Service	In the dropdown list, select an XML Phone Service to which HiPath 4000 phone devices were already assigned.
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.

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.
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 **Search**. The result of the search inquiry appears in a list.

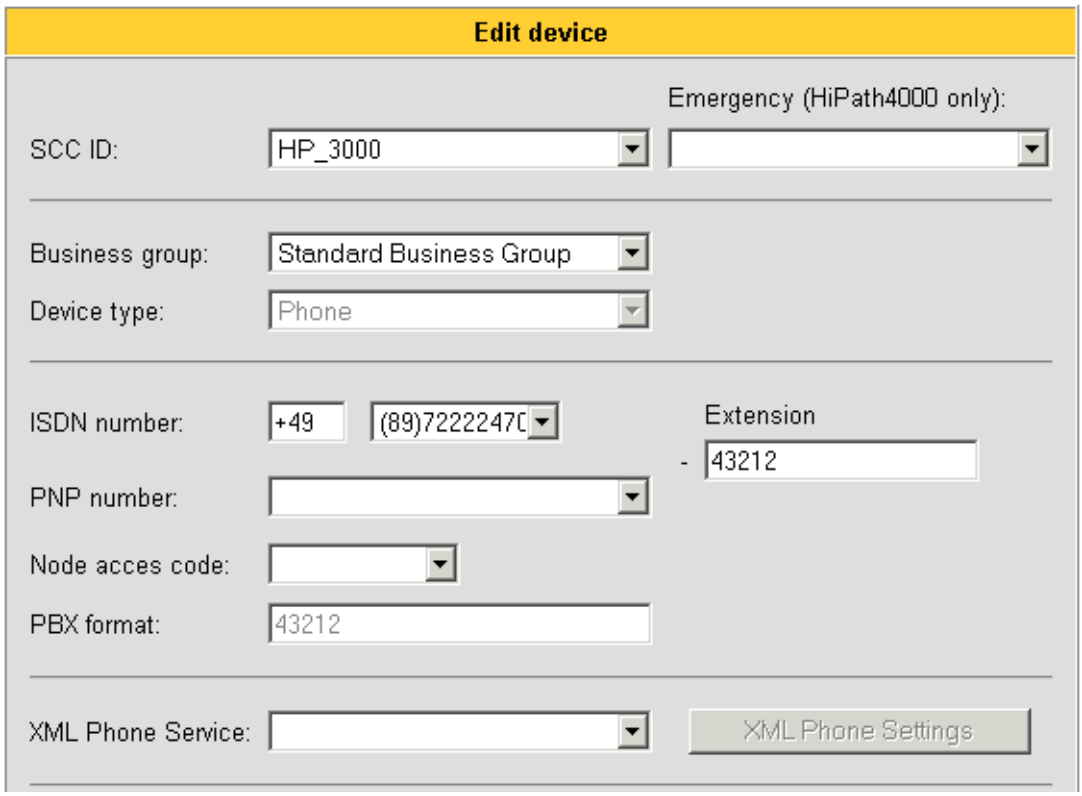


Device	Device Type	SCC ID	SCC Emergency	Phone service	
+49(89)722-22470	MEBCallNumber	MEB1			
+49(89)722-22470	MEBCallNumber	MEB1			
+49(89)722-22470	MEBCallNumber	MEB1			
+49(89)722-22470	MEBCallNumber	MEB1			
+49(89)722-22470	MEBCallNumber	MEB1			
+49(89)722-22470	MEBCallNumber	MEB1			
+49(2302)98417-70001	MEBCallNumber	MEB2			
+49(89)722-12345	Phone	SCC-HP4000			

Use the cursor control keys to navigate through several pages (first - next - previous - last page). The printer icon can be used to obtain a print preview of the results list in a separate window.

If only one result is found, then step 4 is skipped.

4. Use the icon to select a user from the list whose data you wish to modify.
5. The current data for the selected user is displayed for editing purposes.



6. Edit the user 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:

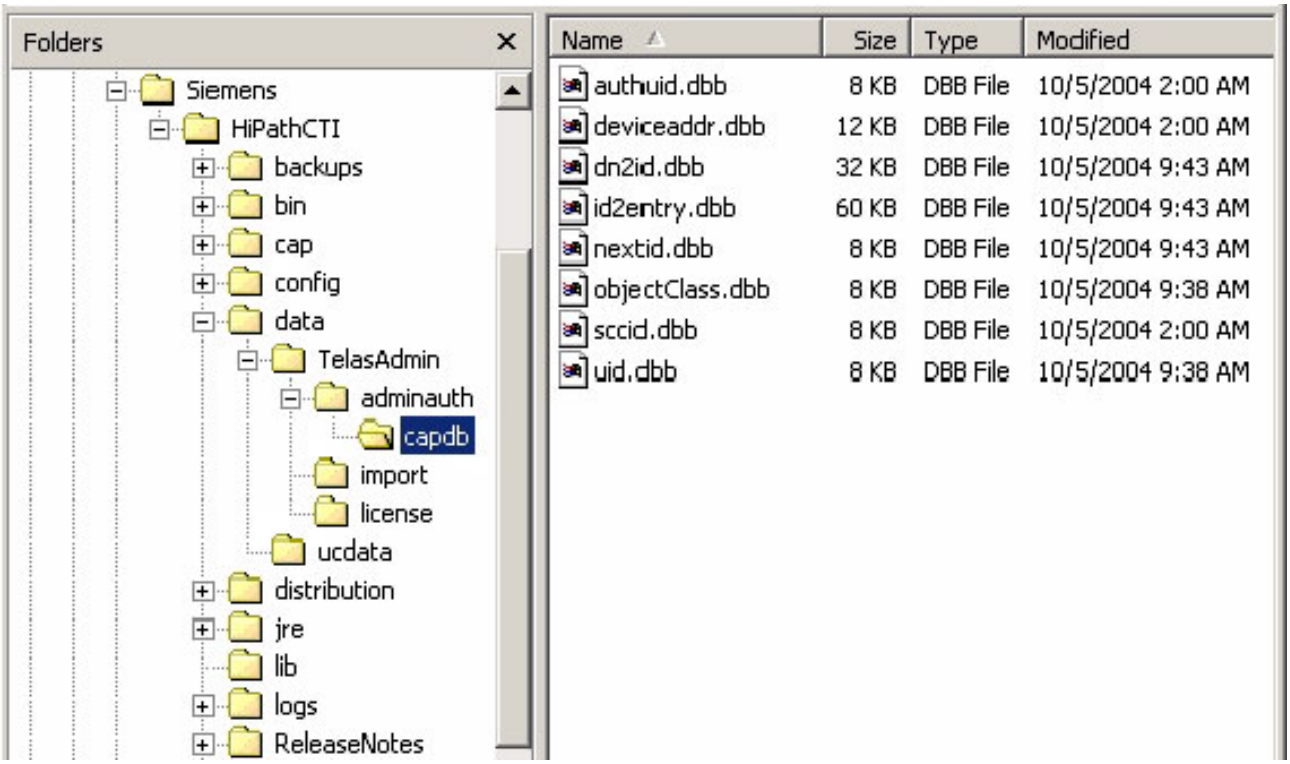
   `Device data has been modified for: <device>` (for example `optiPoint 410`)

7.5 Data

In the **Data** menu item of the main menu you can export the HiPath CAP data contained in a database file to a particular directory and import an already existing database file from a particular directory. If these actions are to be executed automatically at set intervals, then you can set a timer (task) for this purpose.

The CAP configuration and user data is administered by an open LDAP server (process "SLAPD"); this data is in the directory:

```
:\Programs\Siemens\HiPathCTI\data\TelasAdmin\adminauth\capdb
```

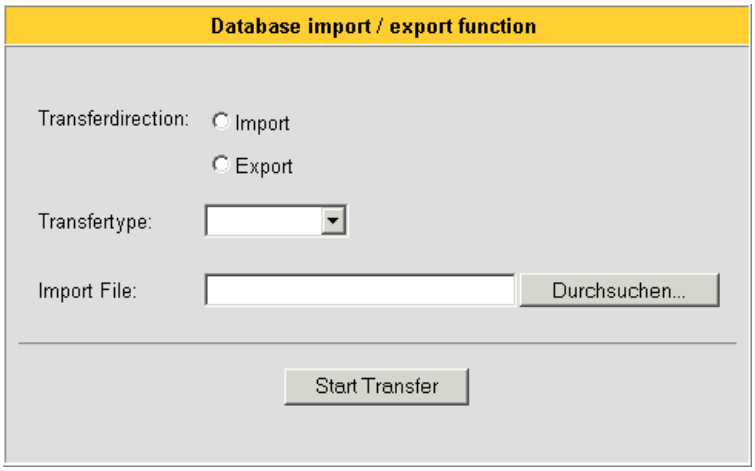


7.5.1 Importing and exporting data

If you want to export the database file to a particular directory, select the **Data | Export** menu item. If you want to import an existing database file from a particular directory, select **Data | Import.**

> ⚠ Error-free data import is only possible if the user IDs of all existing CAP CTI users are the same as the device IDs without special characters.

1. Click **Data** in the main menu and select the **Import** or **Export** menu item in the navigation area.



2. Enter the data in the relevant fields. The fields are described in the table below.

"Database import/export" dialog

Field	Description
Transfer direction	Choose whether you wish to import an existing database or export the database currently in use.
Transfer type	Select the database transfer type: • TXT • HDMS (DMS) • DEV • AllData • HiQ8000
Import File	To import a database, use the **Search** button to go to the directory containing the database to be imported.

3. Click the **Start Transfer** button to start importing or exporting the database.

Import configuration file "impAdmData.cfg"

The file `impAdmData.cfg` defines parameters for data import and export.

```
IgnorePBX = <Service node ID-1>,<Service node ID-2>,…
```

```
Separator = < > (Default "|")
```

Setting these parameters prevents any changes to user data for specific systems (service account ID) during the import and export. This can be very important when importing data in HDMS (DMS) format if all data is not imported for all CTI users. In HDMS format, users are automatically deleted if they are present in the CAP DB but not in the import file.

```
ExecuteAllChanges = 0/1
```

If this parameter is active (1), the data import is controlled depending on the number of users 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 when the number of the data changes is lower than 10%. If there are 100 or more CTI users, an import is performed when the number of the data changes is 1% or lower.

```
Separator = < > (Default "|")
```

The separator no longer has to be explicitly defined.

Data import/export schema files

All import and export schema files are located in the directory:

```
C:\Program Files\Siemens\HiPathCTI\data\TelasAdmin\import
```

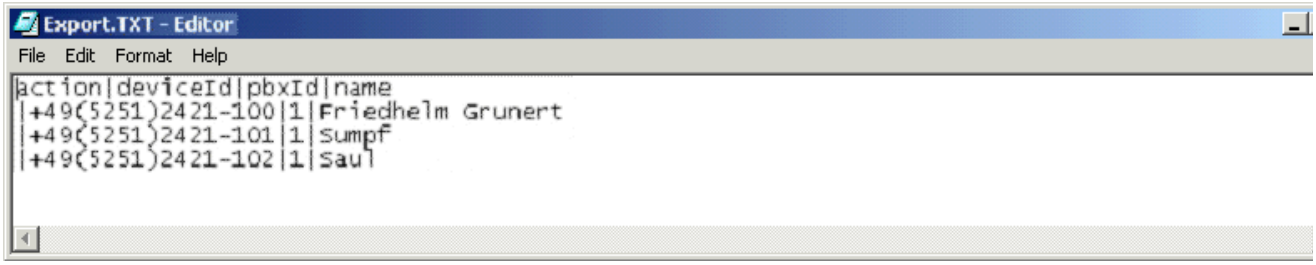
The options available for the imported information and associated field designation is provided in a schema description. If an import file does not contain a header with these field designations, the system automatically assumes the default import (see example files). If the format of the import file does not match the required standard, this file must contain a header in which the field designation is listed according to the information position.

The `"updatePerm.cmd"` can be found in this directory after the import. It contains all import calls that were executed. The import is logged at the same time. The name of the log file is:

```
C:\Program Files\Siemens\HiPathCTI\logs\<PC name>\import.log
```

The TXT import and export format

The `schemeTXT.cfg` template contains the format description for the txt import and export format. Each line in the file contains a command with the following syntax:



txt format examples

```
# Delete user +49(89)636-12345

0;+49(89)636-12345

# Set up Miller for system 0060 with telephone number +49(89)636-12345

# and set the default password.

1;+49(89)636-12345;0060;Miller

# Phone number +49(89)636-12345 is switched to system 0061

2;+49(89)636-12345;0061

# User name for telephone number +49(89)636-12345 is changed to Mellor

2;+49(89)636-12345;;Mellor

# Password for telephone number +49(89)636-12345 is reset to the de-
fault

3;+49(89)636-12345
```

action	Identifies the command to be executed
0	Delete user
1	Add new user
2	Modify password
3	Reset user password to default
deviceId	User telephone number in long canonical format
pbxId	PBX ID for which the phone number is configured. This field is mandatory if action=**1**, optional if action=**2**, and has no significance if action=**0,3**.
name	User name. This field is optional.
pwd	User password. This field is not relevant if action=**0,3**. If it is not specified, the default password is set if action=**1**, and the password is left unchanged if action=**2**.

The HDMS (DMS) import and export format

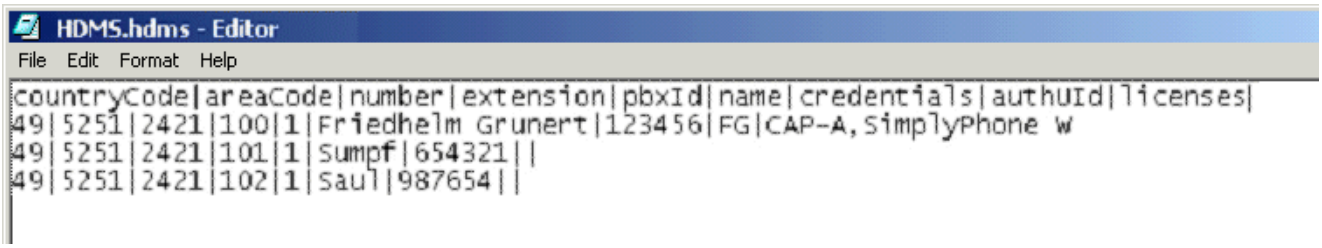
The `schemeHDMS.cfg` template contains the format description for the HDMS import and export format. Unlike the TXT format which contains commands such as **Delete**, **Modify**, and **Add**, this format is evaluated differently. The input file always contains all user data which is synchronized with the current data from the HiPath CAP User Management database.

Add: New users (contained in the .HDMS file but not in the CAP database) are added to the HiPath CAP User Management database. The password is set to the configured default password and the timestamp is set to "0".

Delete: Invalid users (present in the CAP database but not in the .HDMS file) are deleted from the HiPath CAP User Management database.

Modify: The user data is changed as specified in the .HDMS file for users who are contained both in the .HDMS file and in the CAP database. This only applies to the "name" and "pbx" fields.

The password can be changed to HDMS format (credentials) via the import tool; the CTI user must change it during initial login. Each line in the file contains a user data record with the following syntax; Comment lines are prefixed by a # symbol and blank lines are ignored.

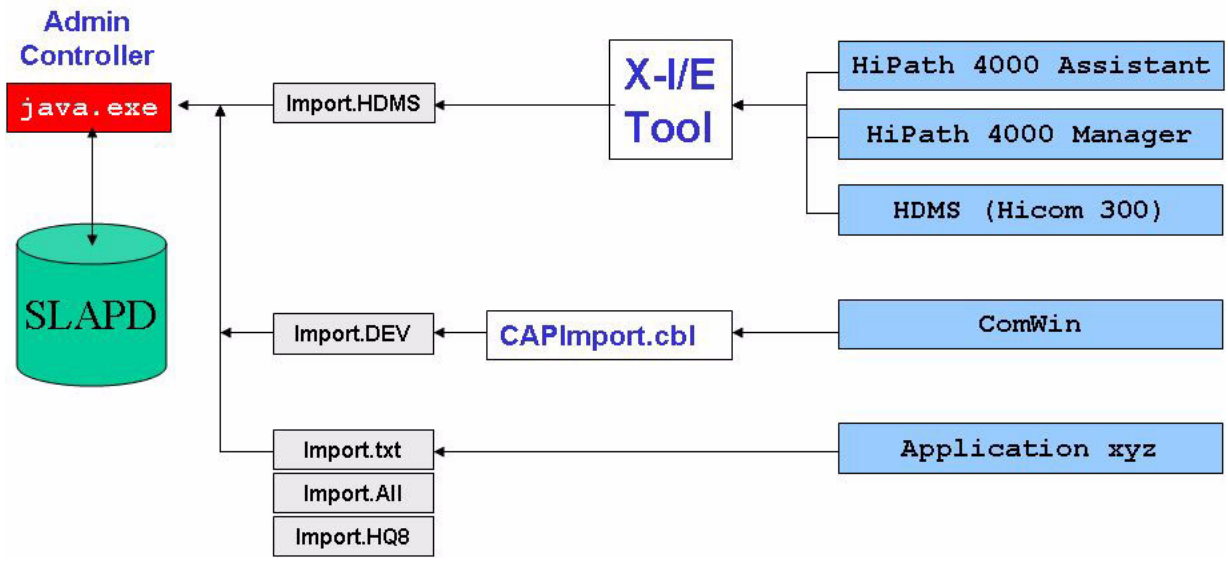


HDMS format examples: Two user data records are transferred in this example. The scheme above is used to check whether these are new or whether the name or PBX has been changed; Otherwise, all other users who are already registered are deleted. As a result of importing, HiPath CAP Management has registered precisely these two users with the details below as valid HiPath CTI users.

```
# John Smith with the telephone number +49(89)636-47111 at PBX 0060

# and Peter Smith with the telephone number +49(89)722-4712 at PBX 0249

49|89|636|47111|0060|John Smith|

49|89|722|4712|0249|Peter Smith|
```

countryCode	Country code for the call number (for example, 49 for Germany)
areaCode	Area code for the call number (for example, 89 for Munich)
number	Call number (for example, 722 for an internal call)
extension	Extension (subscriber extension)
pbxId	PBX ID for which the phone number is configured
name	Subscriber name. This field is optional.
credentials	Individual password; absolutely must be changed during initial login. This field is optional.
authUID	Subscriber alias name. This field is optional.
licenses	Assigned licenses; more than one license can be assigned. This field is optional.

The following chart shows the internal connections during data import.



Import HiPath 4000 non-station devices

When applications address HiPath 4000 logical devices (type RCG, trunk, hunt group) an address type conversion has to be performed. The application usually addresses any device (phone) by its dialing number. But HiPath 4000 logical devices have to be addressed by their LODEN number.

Example:

RCG 100 dialing number: +49(5251)2214-7661 LODEN: 33554442

The HiPath 4000 expert access program "ComWin" includes a feature for downloading all switch device information into a file along with their assigned LODEN numbers.

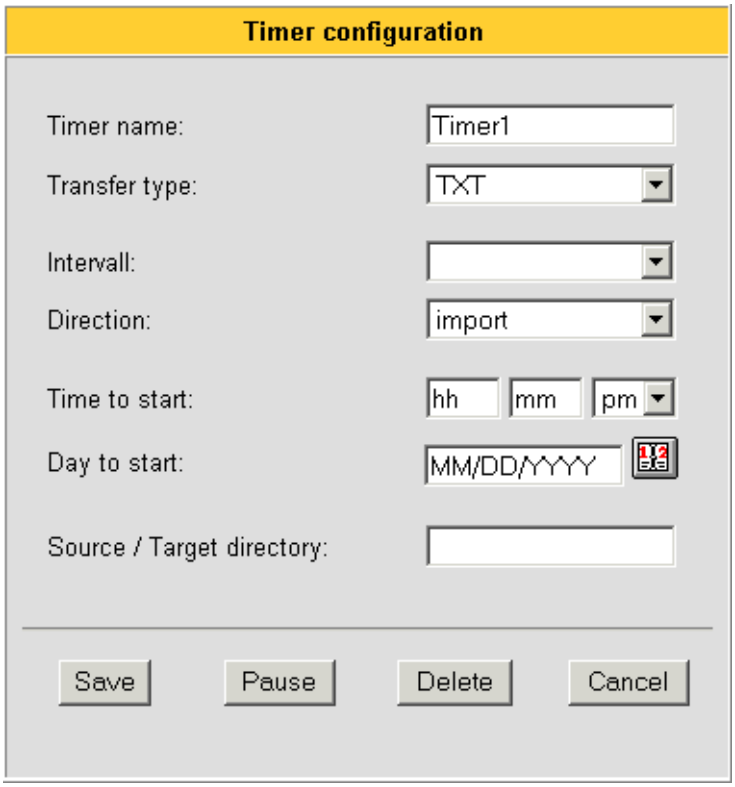
1. Start "ComWin" and establish a connection to a HiPath 4000.
2. Logon to the HiPath 4000.
3. Select Macro - CBL start.
4. Browse for "CAPImport.cbl".
5. Enter the "SCCId" and the "Canonical Prefix" [example: +49(5251)2214].
6. Click "Store".
7. "Read Trunks, RCGs, HuntGroups, Phones"
8. "Save Result to File"
9. Import the resulting file as already described.

7.5.2 Planned 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 the required transfer type from the database: • TXT • HDMS • DEV • AllData • HiQ8000
Interval	In this field, specify the intervals at which the database is to be imported or exported. You can choose between the following intervals: • daily • weekly • monthly
Transfer direction	Choose whether you wish to import an existing database or export the database currently in use.

Field	Description
Time to start	Enter the start time for the transfer in hours (hh) and minutes (mm).
Day to start	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 database to be exported should be stored or where the file to be imported is located. The import files must have the following names: • user.txt • user.hdms • devices.hdams The export files must have the following names: • userExported.txt • userExported.hdms • devicesExported.hdams

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

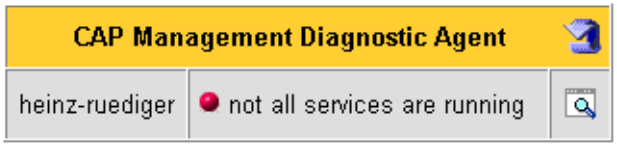
Action	Description
Save	Saves your entries and adds the task to the "List of running import timer".
Pause	Puts the selected task into standby mode, which means that it will no longer execute until you release it again with this button.
Delete	Deletes the selected task from the "List of running import timer". **Note**: This button only appears if a task is already configured.
Cancel	Closes the dialog without saving the entries.

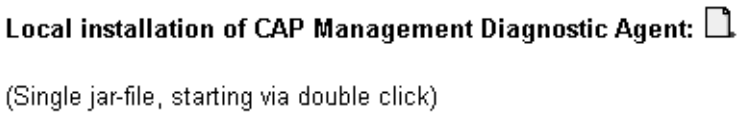
7.6 Diagnostics

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.

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.





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

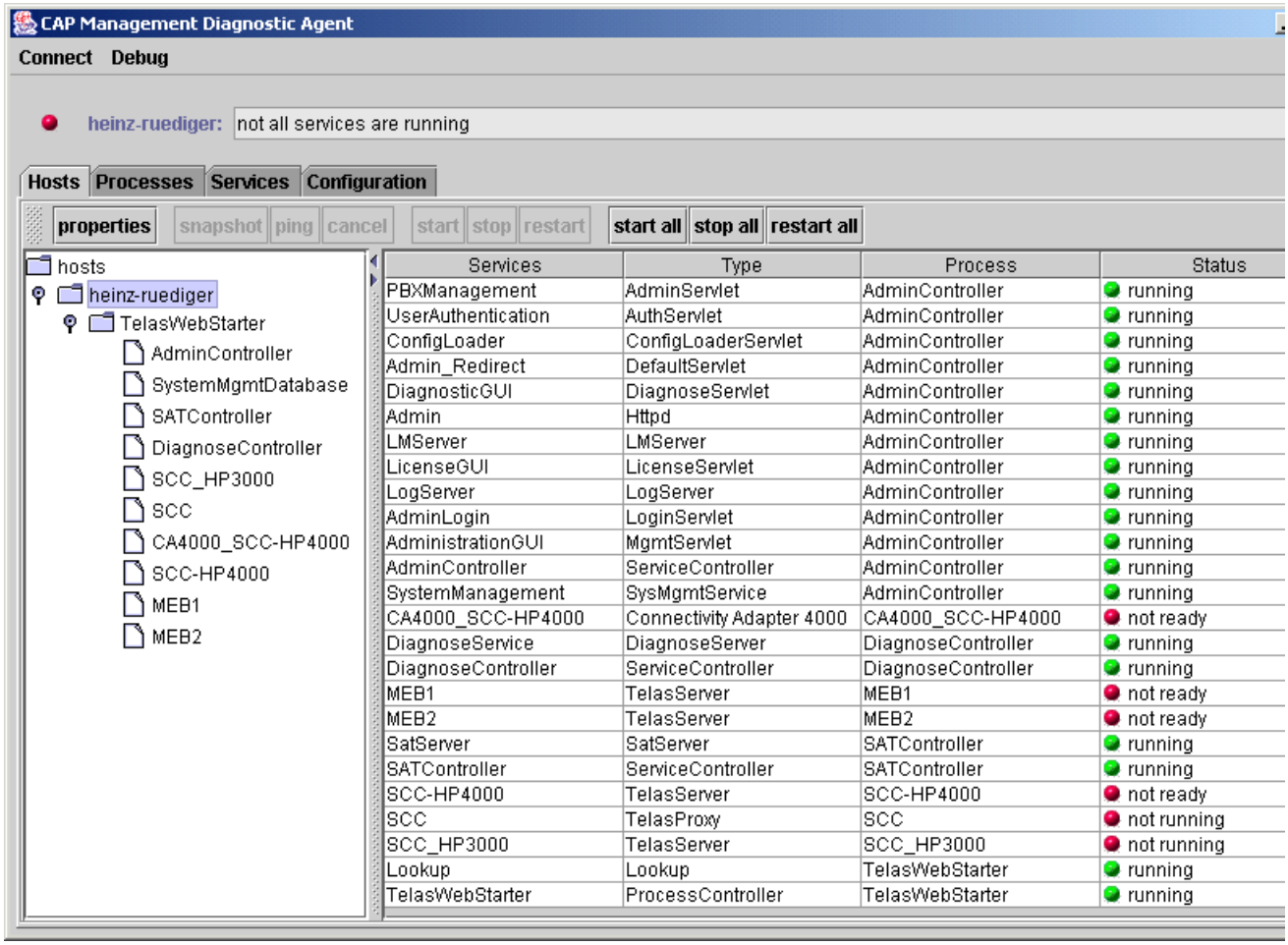
1. Start downloading the `twebDiagAgent.jar` file.
2. Note the location of the downloaded file.
3. In Explorer, go to the folder containing the saved file.
4. Start the CAP Management Diagnostic Agent by double-clicking it.

If the "Diagnostic Agent" is installed locally, this application may 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.

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:



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.

More information on diagnostics is contained in Chapter 8, "Troubleshooting".

7.6.1 Hosts

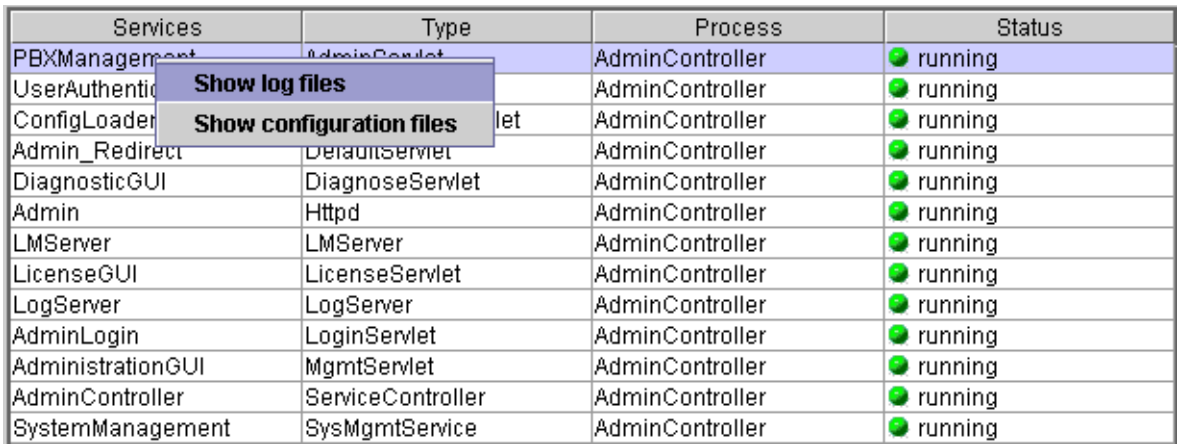
If the **Hosts** tab is selected, all hosts in a network where a HiPath CTI service is running are shown in a tree structure in the left window. If a host is selected, all services running on that PC are shown with their state and process allocation.

- **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.

7.6.2 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 7.6.1), 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**



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.

7.6.3 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 7.6.1, Section 7.6.2), depending on the selected service.
- **Show log files, Show configuration files**
  As above (Section 7.6.2), these are available via a context-sensitive menu for the selected service.

7.6.4 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.

7.6.5 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 dropdown 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.
- **Set the Log Filter**
  You can set one 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.

7.6.6 "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: <inst dir>\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
- AdminController (as service controller)

CallIdRepository

The CallIdRepository services are:

- "unknownService"
- CallIdRepository (as service controller)

Diagnostic Controller

The Diagnostic Controller services are:

- DiagnosticService
- DiagnosticController (as service controller)

SAT Controller

The SAT Controller services are:

- SATServer
- SATController (as service controller)

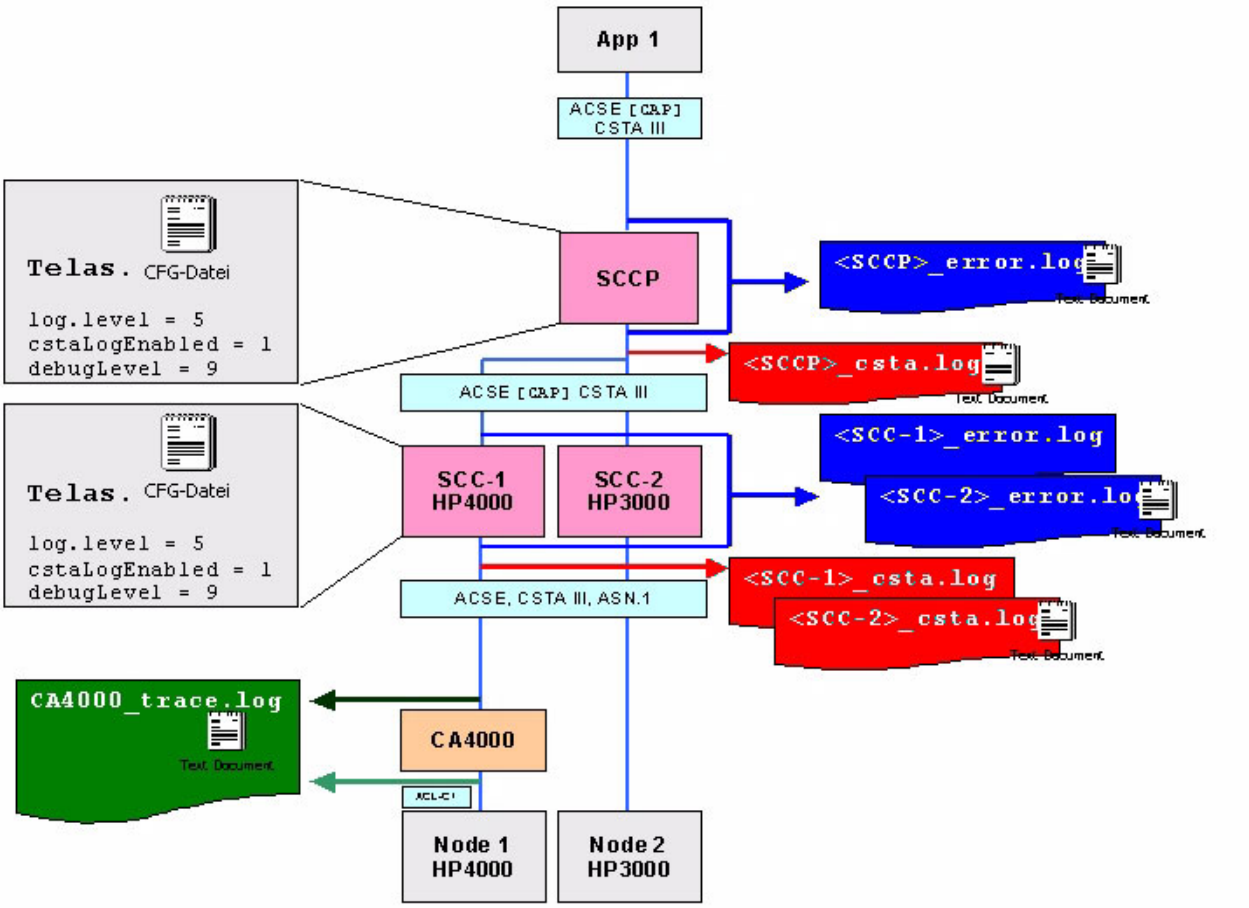
TelasWebStarter

The TelasWebStarter services are:

- Lookup
- TelasWebStarter (as "process controller") (It is the lookup client!!!)

7.6.7 CSTA Communication Trace

Depending on the different interfaces, a complete CSTA communication trace from the application to a switch can be enabled.



7.6.7.1 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 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 ASN.1. CSTA XML is converted to ASCII.

7.6.7.2 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 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

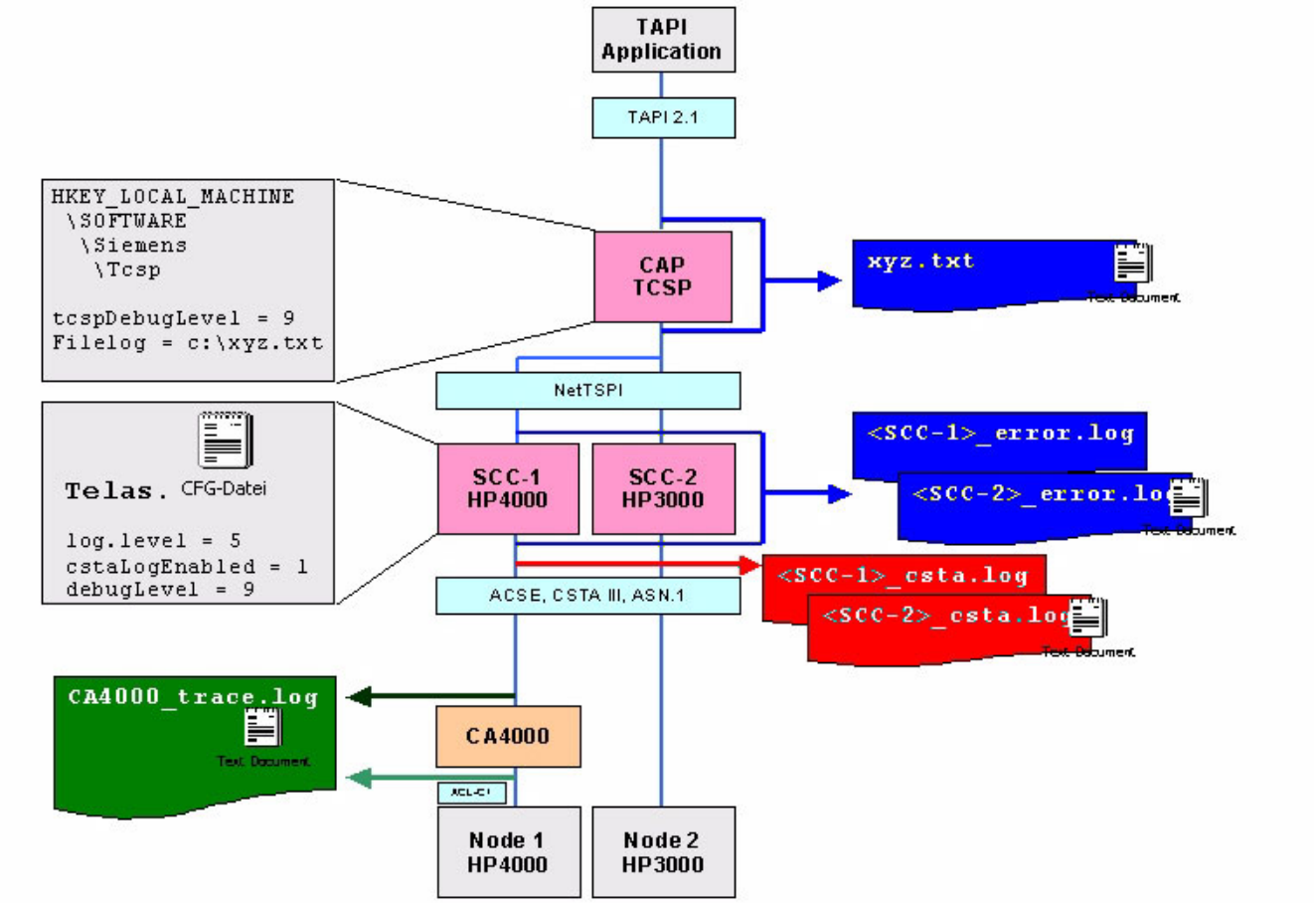
If the log level setting is correct, the <SCC>_csta.log file contains the conversation with the switch or CA4000 in CSTA ASN.1.

7.6.7.3 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 ASN.1 conversation with the SCC.

7.6.8 TAPI Communication Trace

Depending on the different interfaces, a complete TAPI/CSTA communication trace from the application to a switch can be enabled.

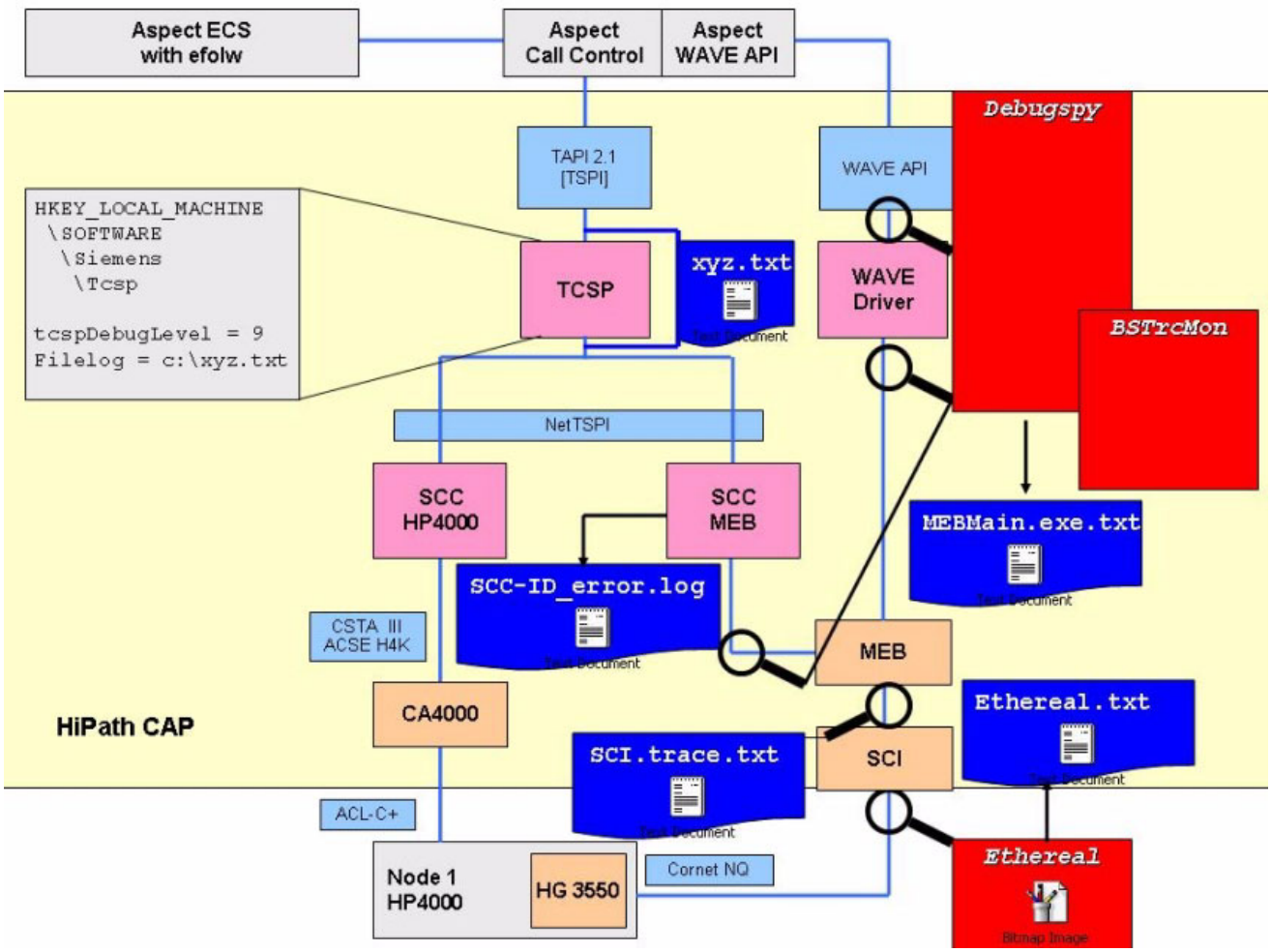


In this mode of communication, the CAP TCSP replaces the SCCP. Registry settings define the CAP TCSP log level and the file location.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\Tcsp

        tcspDebugLevel = 9

        filelog = "C:\tcsp_log.txt"
```

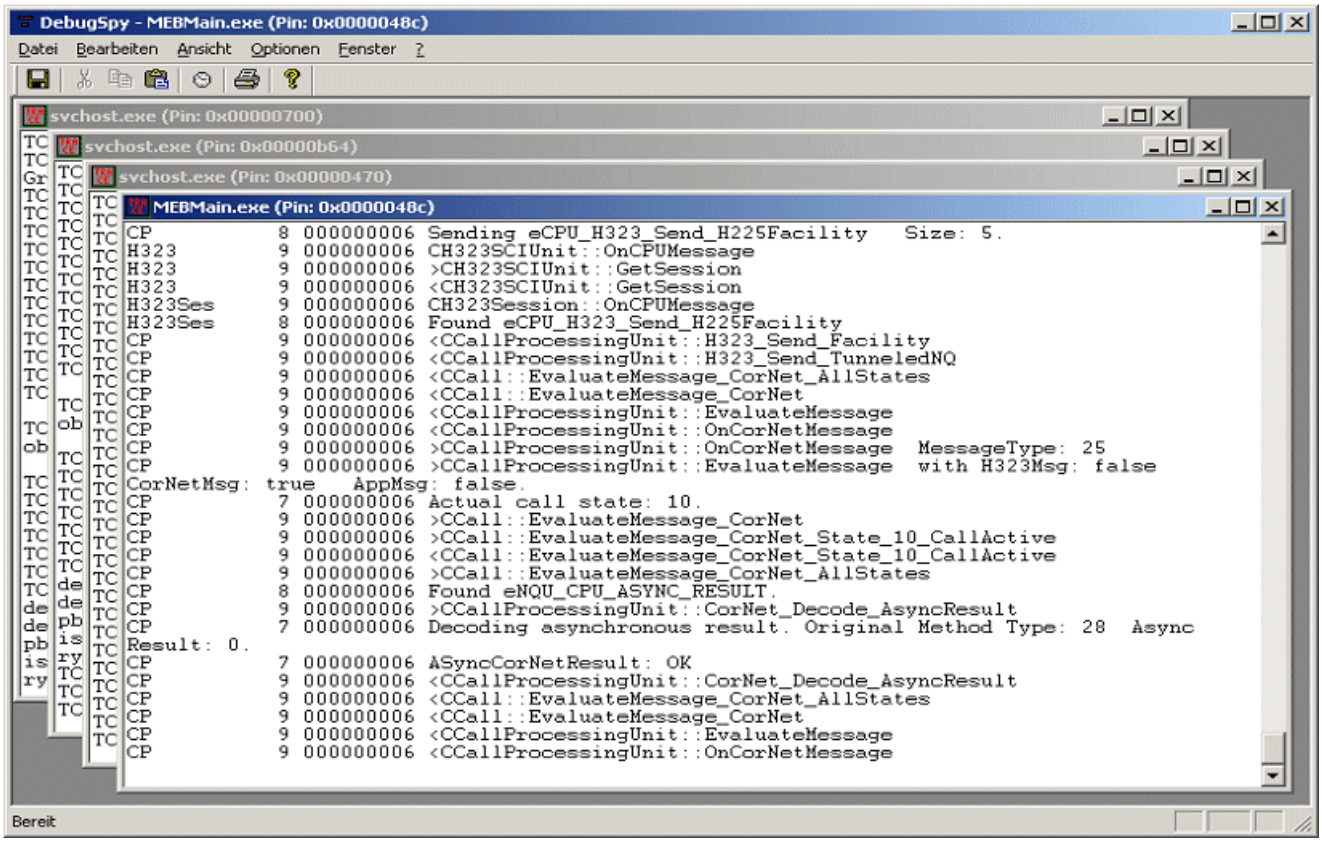
7.6.9 MEB Communication Trace

The following flowchart describes how to enable the SCCMEB and MEB traces.



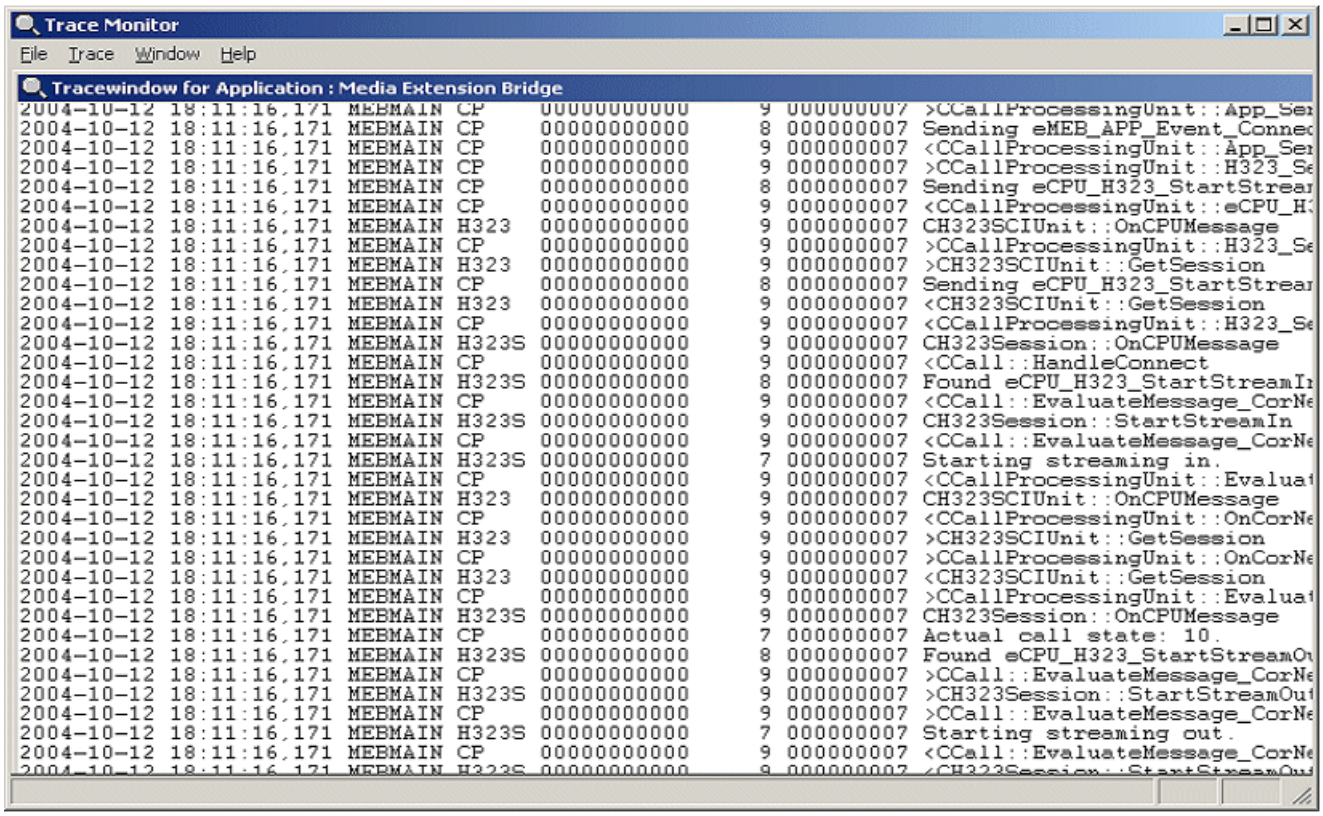
Debugspy

Debugspy is a tool for tracing the complete DLL communication between all running Microsoft components. It opens a window for every process. You can dump the displayed messages to a window-specific file.



BsTrcMon

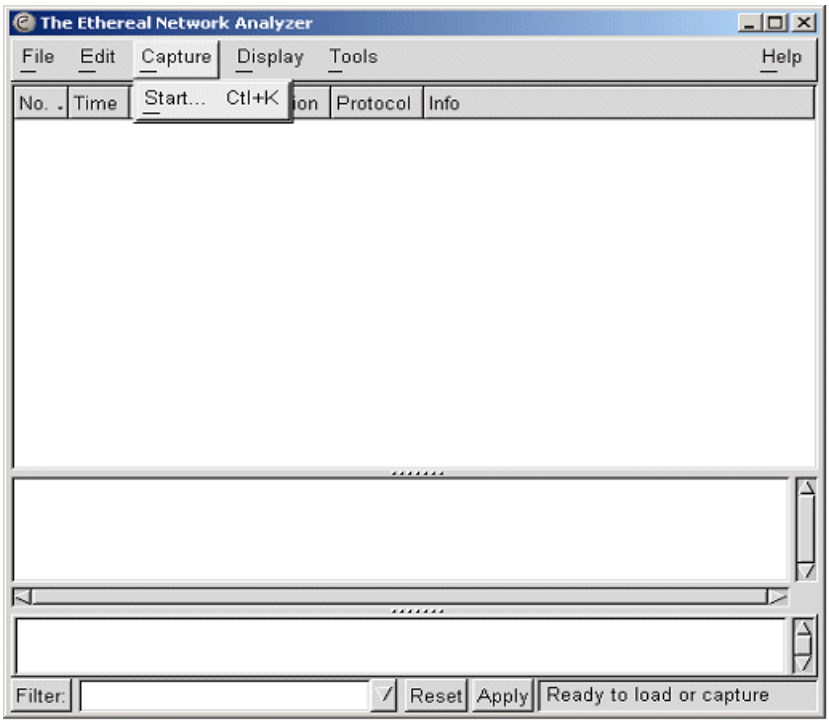
BsTrcMon is a program for tracing the communication of connected programs only. For HiPath CAP, it's only the MEB. If MEB has been started via CAP Management, the feature "Allow service to interact with desktop" for the Windows service "Siemens HiPath CTI" must be enabled for tracing MEB communication. If MEB has been started via MEBAppTester, then tracing always works. You can dump the displayed messages to a file.

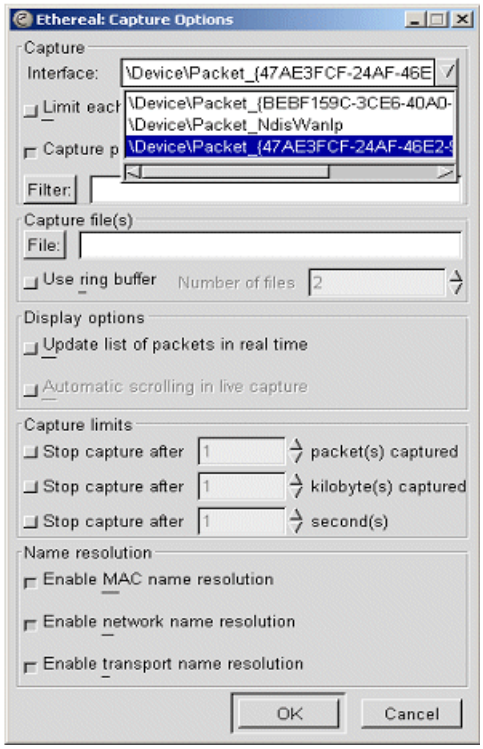


Ethereal

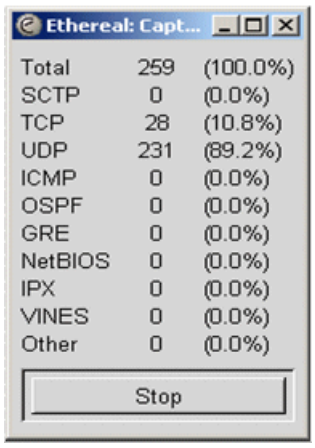
Ethereal is a tool for tracing the TCP/IP conversation of one NIC. Don't set any filters without instructions from development.

Select "Capture - Start" and select the NIC which is being used for the connection to the HG3550 and click "OK".



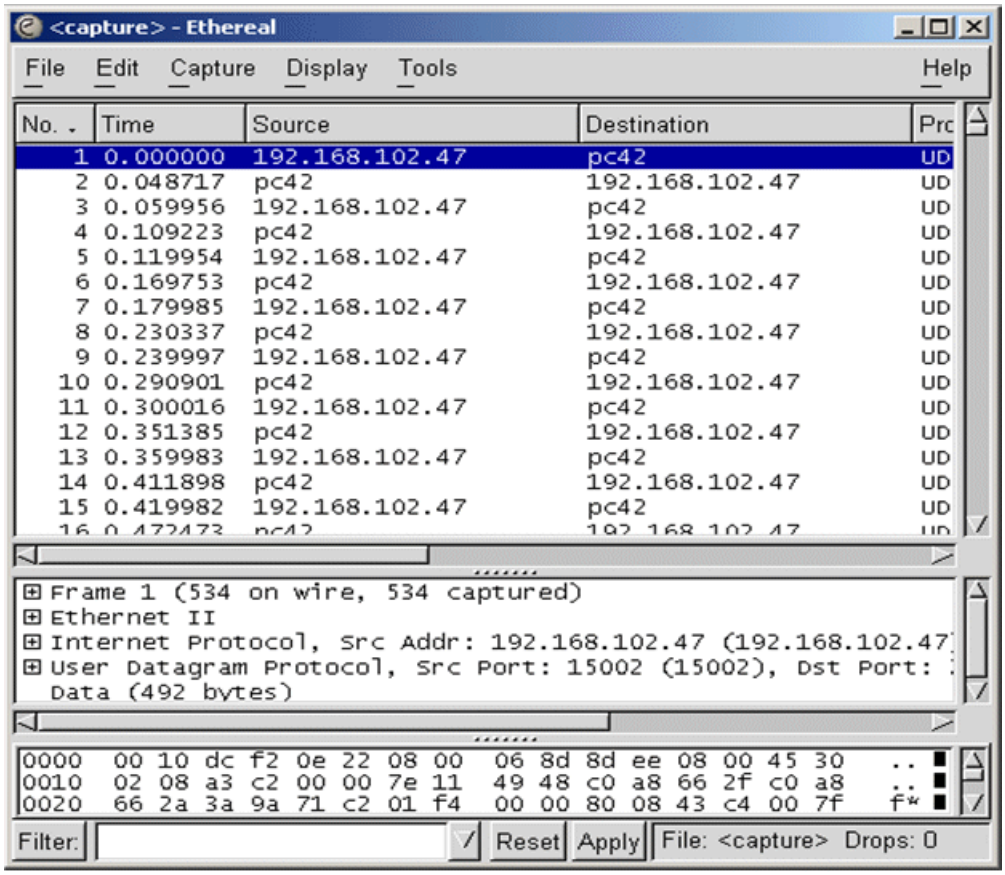


The trace is now active. A counter displays the number of sent and received packages.

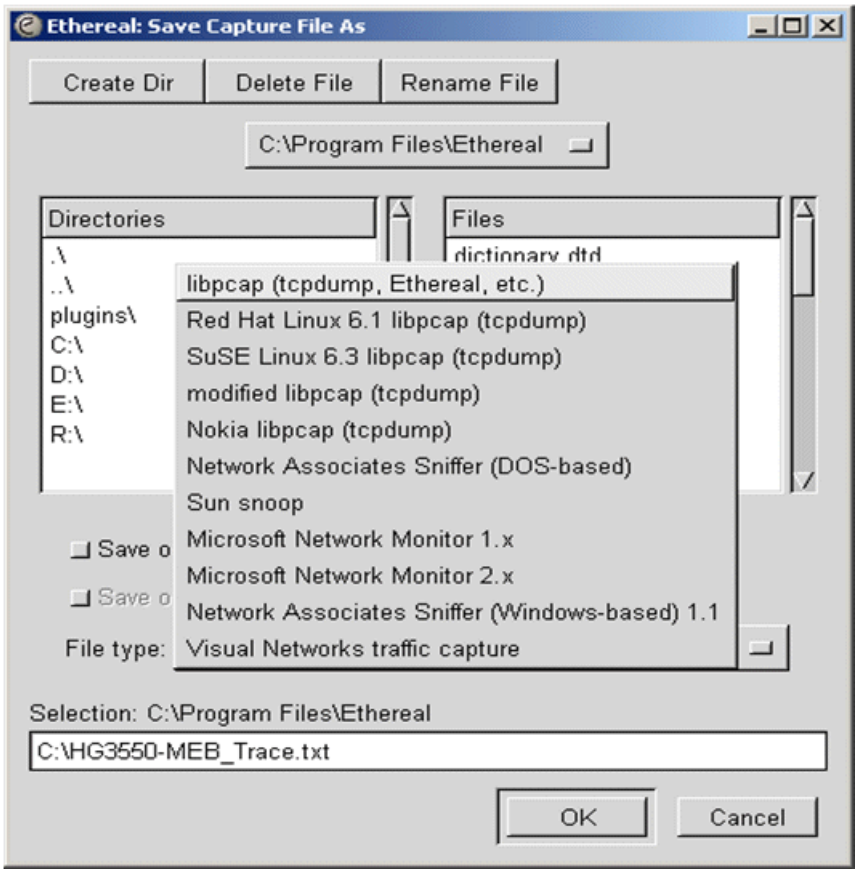


Click "Stop" to stop the trace recording. After the trace recording has been stopped, the buffered information is prepared for output.

Now the recorded trace can be displayed on-screen.



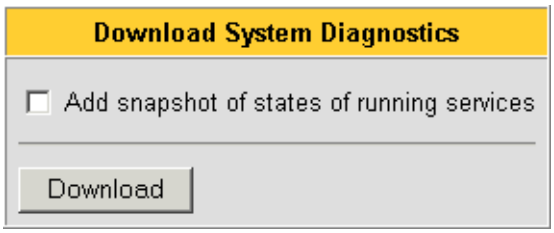
You can save the trace to a file. This file can be opened for analysis with suitable programs.


Ethereal: Save Capture File As
Create Dir
Delete File
Rename File
C:\Program Files\Ethereal
Directories
Files
.\
..\
plugins\
C:\
D:\
E:\
R:\
dictionary.dtd
libpcap (tcpdump, Ethereal, etc.)
Red Hat Linux 6.1 libpcap (tcpdump)
SuSE Linux 6.3 libpcap (tcpdump)
modified libpcap (tcpdump)
Nokia libpcap (tcpdump)
Network Associates Sniffer (DOS-based)
Sun snoop
Microsoft Network Monitor 1.x
Microsoft Network Monitor 2.x
Network Associates Sniffer (Windows-based) 1.1
Visual Networks traffic capture
Save o
Save o
File type:
Selection: C:\Program Files\Ethereal
C:\HG3550-MEB_Trace.txt
OK
Cancel

7.6.10 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:



   All configuration data and log files are saved. Enable the **Add snapshot of states of running services** if you want to save the service environment data.

2. Click **Download**.

7.7 Help

The documentation for HiPath CAP and all installed HiPath 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 the event 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:	CAP03.000-0709
Date:	Mo 09.08.2004 20:22

Component list

```
bin/BSTRC20.dll:
Modified                = Fr 07/30/2004 12:24 PM
Length                  = 32838

bin/NTAuth.dll:
Modified                = Mo 08/09/2004 8:30 PM
Length                  = 12800

bin/NqUnitDll.dll:
Modified                = Fr 07/30/2004 12:24 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,
- Siemens or
- the application vendor.

Using Table 8-1 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 2000	Operating system	Microsoft
PC and server hardware	Servers, clients	Customer
HiPath CAP	CA4000, SCCHiPath4000, SCCP, CAP TCSP, XMLPS, MEB	Siemens
Application	Installation, configuration	Application vendor

Table 8-1 Responsibilities in the event of problems

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 8.7, "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 **Siemens HiPathCTI 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 HiPath 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 HiPath 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 4.4). 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 **`Authorization failed. Retry?.`**

- Check that the **Siemens HiPathCTI** service is running.
- Check that the login data has been entered correctly
  (note use of uppercase/lowercase).

8.3.4 Administrator homepage 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 **Siemens HiPathCTI service** is running (e.g. via **Control Panel | Services**).

8.3.5 CAP Management is not working on all PCs in the intranet

HiPath 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 as been launched (as described in Section 7.6), 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 HiPath CAP Management PC has two network cards. If one of the two corresponding IP addresses is used to access the HiPath 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 HiPath CAP Management has been launched with **Start | Programs | Siemens HiPath CTI | 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 HiPath 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 Siemens system and error logs.
2. Contact the relevant Siemens service department.

Siemens system and error logs

Check the Siemens 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 7.6, "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 7.6. 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 re-started.

- **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 HiPath CTI system processes/services, the affected components must be restarted. HiPath CAP Management diagnostics interface (Section 7.6) makes this possible from any PC with network access, even in the case of a distributed installation of the HiPath 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 HiPath CTI system services are started in sequence by a central service called the Start Service. This is displayed in Windows as the **Siemens HiPath 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 HiPath CAP Service Starter (Siemens HiPath 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 SimplyPhone for Web is installed, this is the start file for telephony functions (PhoneController)

5. **`jaccess_ctrl.bat`**

   If SimplyPhone for Web 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 **Siemens HiPath 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.

Note that when the problem has been rectified, the disabled process start file should be reenabled (restore `Extension.proc`.

8.7 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 Siemens service department.
- In the event of problems with the CTI server, contact the CSTA application supplier.

9 Operating Modes

HiPath CAP supports three different operating modes. The PBXs, protocols, and encoding variants supported differ depending on the operating mode.

Single Domain / Homogeneous / Native Mode

Hicom 300: CSTA I ASN.1

HiPath 4000: CSTA I ASN.1, CSTA III ANS.1, ACSE (CSTA III ASN.1)

HiPath 3000: ACSE (CSTA III ASN.1)

Multi Domain / Homogeneous / Native Mode

HiPath 4000 / HiPath 3000: ACSE (CSTA III ASN.1)

Multi Domain / Heterogeneous / Harmonized Mode

CSTA III ASN.1, CSTA III XML, TAPI, JTAPI, MEB, XMLPS

9.1 Single-domain//native mode

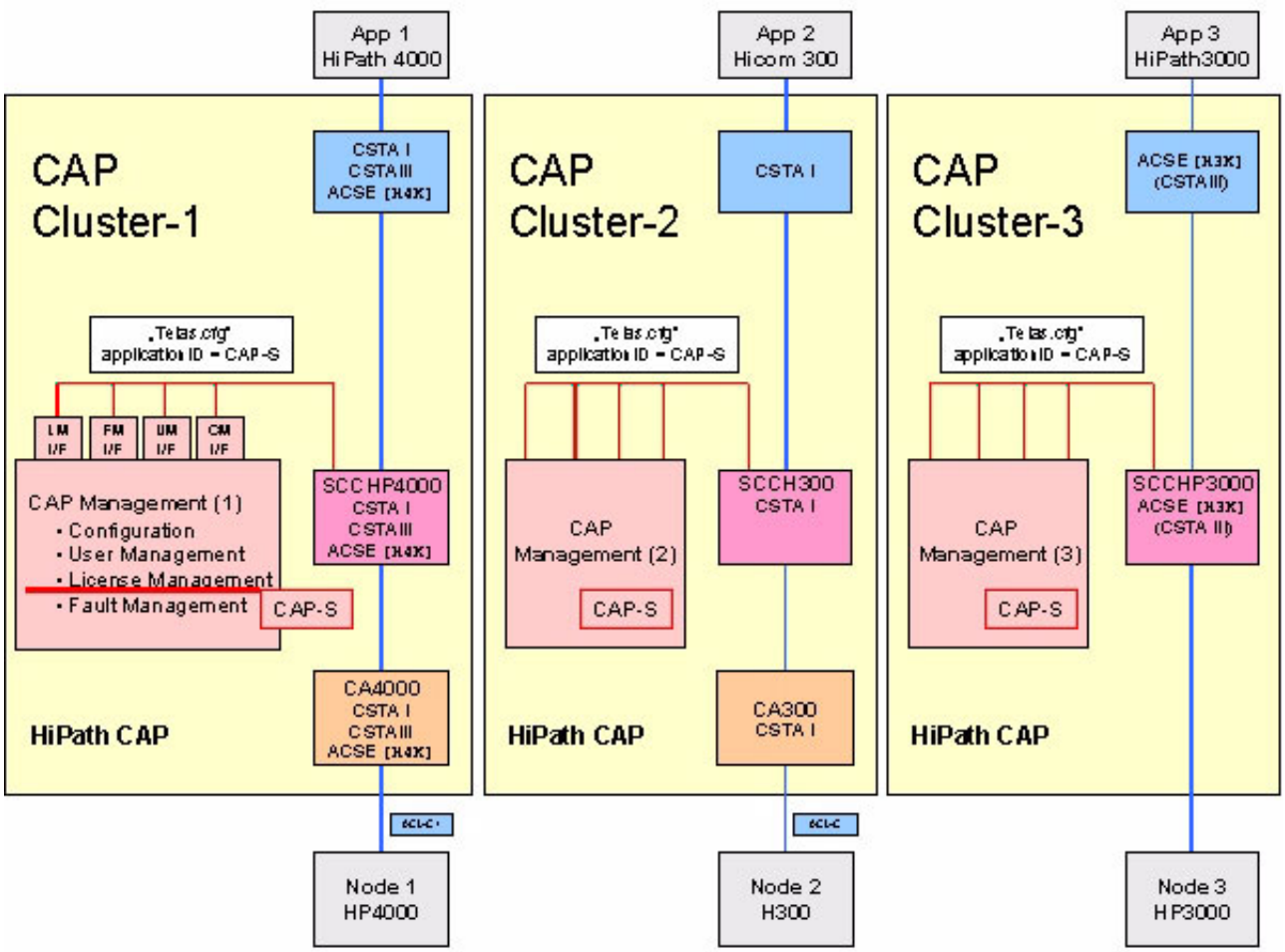
In "single-domain//native mode", one application is connected to one PBX via one CAP. Proprietary protocol elements, private services, and extended features are supported. The number of SCCs used here is irrelevant, but the **ApplicationID** that is set must be identical for all SCCs.

9.1.1 What is the purpose of "single-domain//native mode"?

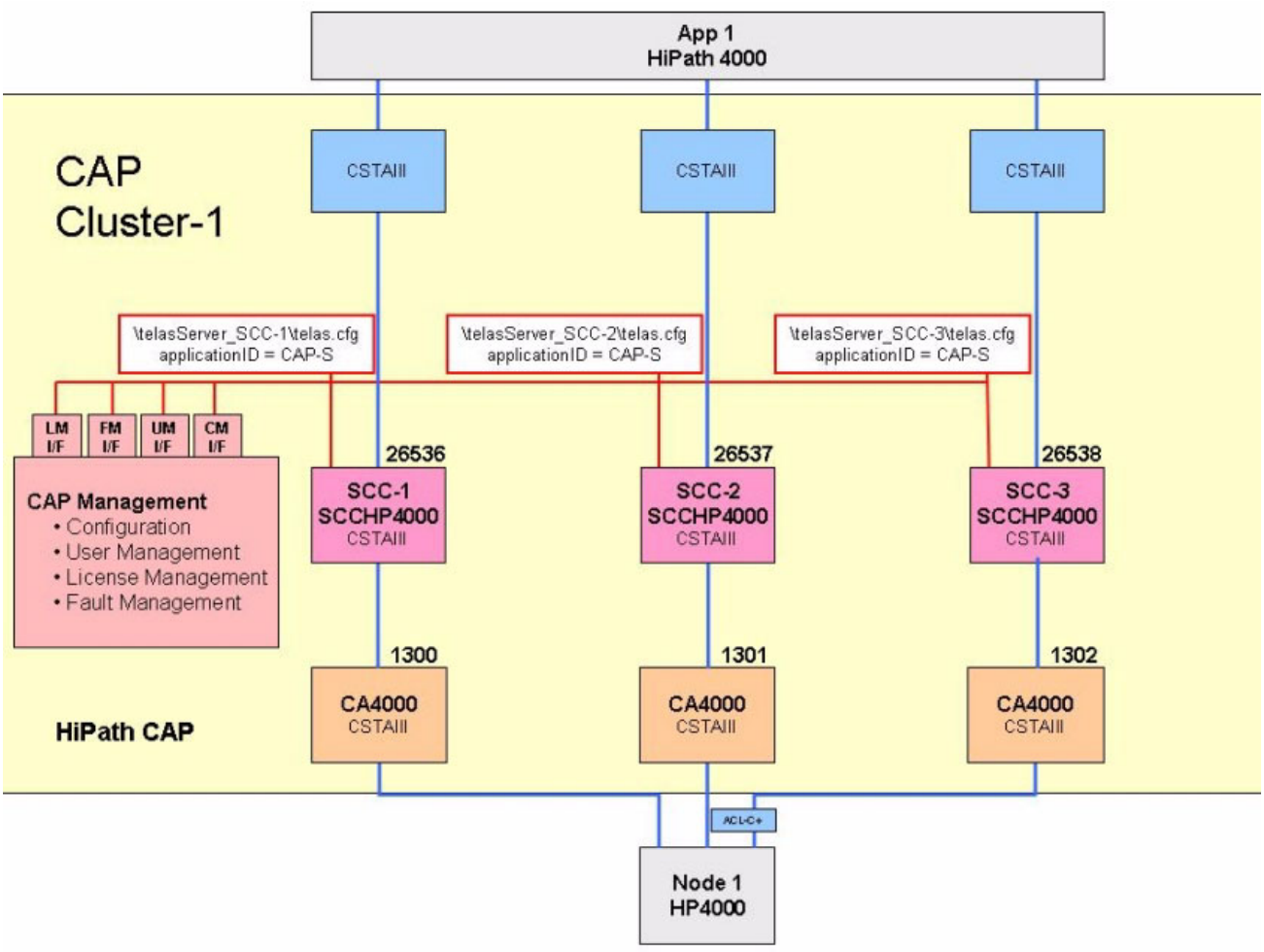
It is used to perform **CTI client licensing** for CSTA applications that have already been developed. No application software changes are necessary for this. The application is not aware of the existence of an SCC.

9.1.2 Installation examples

The SCCs that are to be configured for connecting HiPath 3000/HiPath 4000/Hicom 300 in the CAP are permanently configured for a defined protocol.



Another installation option involves connecting an application to a PBX using several links. In the following example, concrete values (PBX, protocols, and port numbers) are used.



9.1.3 The relationship of the PBX to the SCC

The following describes the relationship between the PBX's supported protocols and the configuration of the different SCCs. The configuration always depends on the application used, however. It determines the protocol version that must be configured.

HiPath 3000 - SCCHiPath3000

The HiPath 3000 supports the CSTA II, ASN.1 encoded protocol (to ECMA 218) and the CSTA III, ASN.1 encoded protocol (to: ISO/IEC 18052).

In contrast, the SCCHiPath3000 supports only the CSTA III, ASN.1 protocol.

The HiPath 3000 sets 0x26 hex in front of each CSTA data record as a proprietary protocol element.

HiPath 4000 - SCCHiPath4000

The HiPath 4000 supports the ACL-C+ proprietary protocol and must have the CA4000 protocol converter. This supports the CSTA I, ASN.1 encoded protocol (to ECMA 179), and the CSTA III, ASN.1 encoded protocol (to ECMA 285), also with additional identification by ACSE.

Proprietary protocol elements are not used.

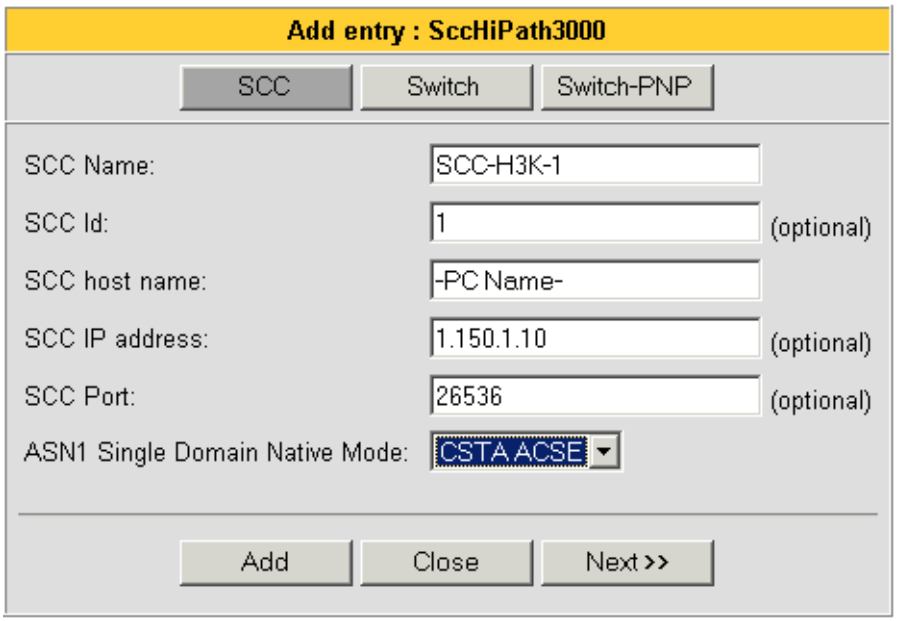
Hicom 300 - SCCHicom300

The Hicom 300 supports the ACL-C proprietary protocol and must have the CA300 protocol converter. This supports the CSTA I, ASN.1 encoded protocol (to ECMA 179).

Proprietary protocol elements are not used.

9.1.4 HiPath3000 SCC configuration in single-domain//native mode

Use the **Service - Switch Connection** menu item to add an "SCCHiPath3000". The option "ASN.1 Single Domain Native mode" is changed to "CSTA ACSE".



9.1.4.1 CTI users in "single-domain//native mode"

All CTI users must be configured under User Management.

9.1.4.2 Licensing in "single-domain//native mode"

Which license must 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.

9.1.4.3 Testing the HiPath 3000 "single-domain//native mode" configuration

CSTA test program

To test this configuration, use the program `CSTA-Browser 3.2.exe`.

The HiPath 3000 proprietary protocol elements are supported in "Phase 3" operating mode.

"Phase 3" is the default operating mode setting. 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)

An application must authenticate itself with the user "AMHOST" and the associated password "77777". This authentication is **not** carried out by CAP Management; instead, it is the HiPath 3000 default login.The CSTA version (version four) is also indicated.

Application ID

The application ID is defined by the "ApplicationID" parameter in the SCC configuration file `telas.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.

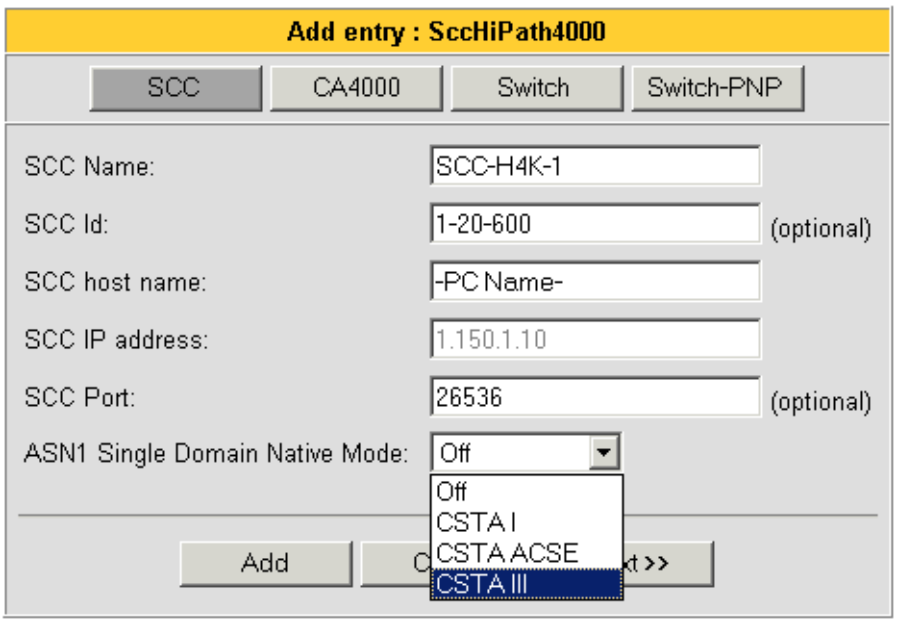
9.1.5 HiPath4000 SCC configuration in single-domain//native mode

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 I**, and the corresponding CA4000 port is also configured in "CSTA I" mode.
- **CSTA III,** and the corresponding CA4000 port is also configured in "CSTA III" mode.

This configuration always depends on the application used.



9.1.5.1 CTI users in "single-domain//native mode"

All CTI users must be configured under User Management.

9.1.5.2 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.

9.1.5.3 Testing the HiPath 4000 "single-domain//native mode" for the CSTA I configuration

CSTA test program for CSTA I

To test this configuration, use the program `CSTA1Host.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)

Not used.

Application ID

The application ID is defined by the "ApplicationID" parameter in the SCC configuration file `telas.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.

9.1.5.4 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**".

Application login (ACSE_AARQ)

Not used.

Application ID

The application ID is defined by the "ApplicationID" parameter in the SCC configuration file `telas.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.

9.1.5.5 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 `telas.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

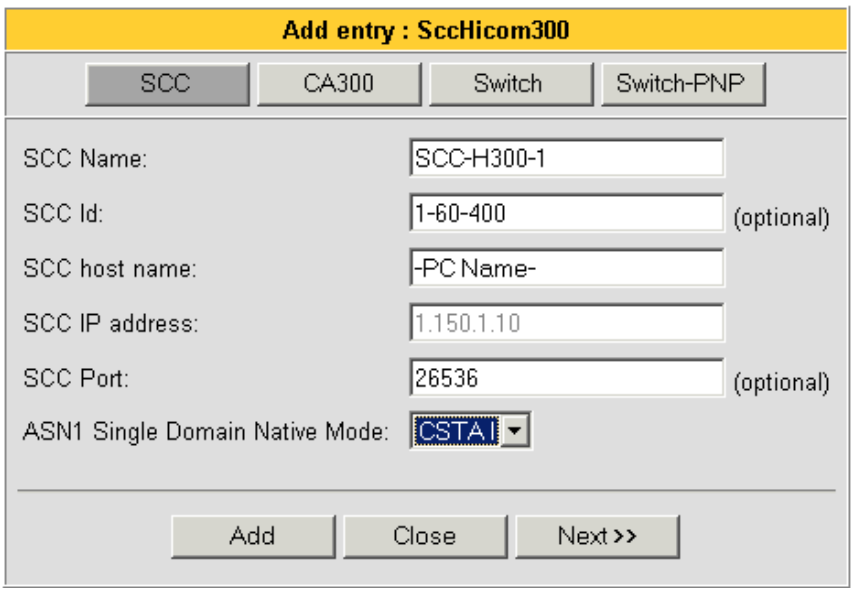
The "Call ID" is two bytes long.

9.1.6 Hicom 300 SCC configuration in single-domain//native mode

Use the **Service - Switch Connection** menu item to add an "SCCHicom300".

"ASN.1 Single Domain Native Mode" is changed to:

- **CSTA I**, because the corresponding CA300 port can only be configured in "CSTA I" mode.



9.1.6.1 CTI users in "single-domain//native mode"

All CTI users must be configured under User Management.

9.1.6.2 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.

9.1.6.3 Testing the Hicom 300 "single-domain//native mode" for the CSTA I configuration

CSTA test program for CSTA I

To test this configuration, use the program `CSTA1Host.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)

Not used.

Application ID

The application ID is defined by the "ApplicationID" parameter in the SCC configuration file `telas.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//native mode

In "multi-domain//native mode", one or more applications are connected to one or more PBXs of the same type via one CAP. Proprietary protocol elements, private services, and extended features are supported. 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.

This mode is only possible for the HiPath 3000 and HiPath 4000. Only the "CSTA III, ASN1" protocol is used.

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//MODE"

An SCC's "multi-domain//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".

9.2.1 What is the purpose of "multi-domain//native mode"?

It is used to license a CTI client for new CSTA applications that want to use the CAP "multi-domain" feature but that simultaneously require private PBX services and extended features.

9.2.2 Application-specific protocol requirements

For "multi-domain//mode", it is imperative that the application 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)
- CSTA version (HiPath 3000 version four, HiPath 4000 version five)
- Native = true

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 eight bytes long.

9.2.3 Authentication - 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 is meaningless here. For successful authentication, the corresponding license must not be installed in the CAP.

CTI client licensing

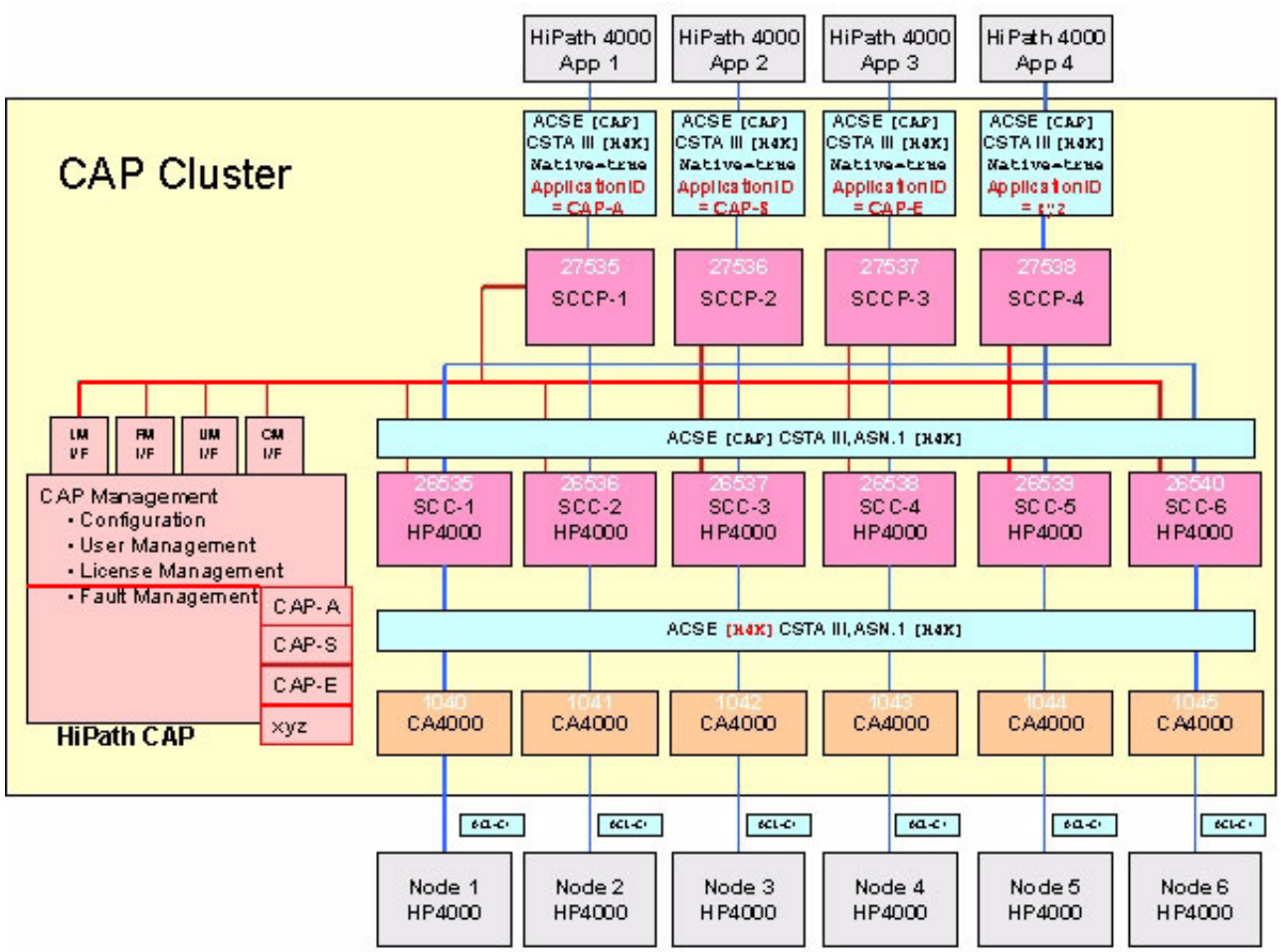
The SCCP stores the "Application ID" transmitted in the ACSE_AARQ and uses it later for CTI client licensing of CSTA requests (using the telephone number in canonical format). The SCCP sends a corresponding HTTP request (`http://<fqdn>:8170/mgmnt/admin/req?registerLicense= <ApplicationID>&userId=<DeviceID>`) to CAP License Management. If the license check was successful, the SCCP saves this information for 3600 seconds.

9.2.4 Installation examples

9.2.4.1 Installation example: HiPath 4000 in "multi-domain//native mode"

NOTE ON THE "APPLICATION ID"

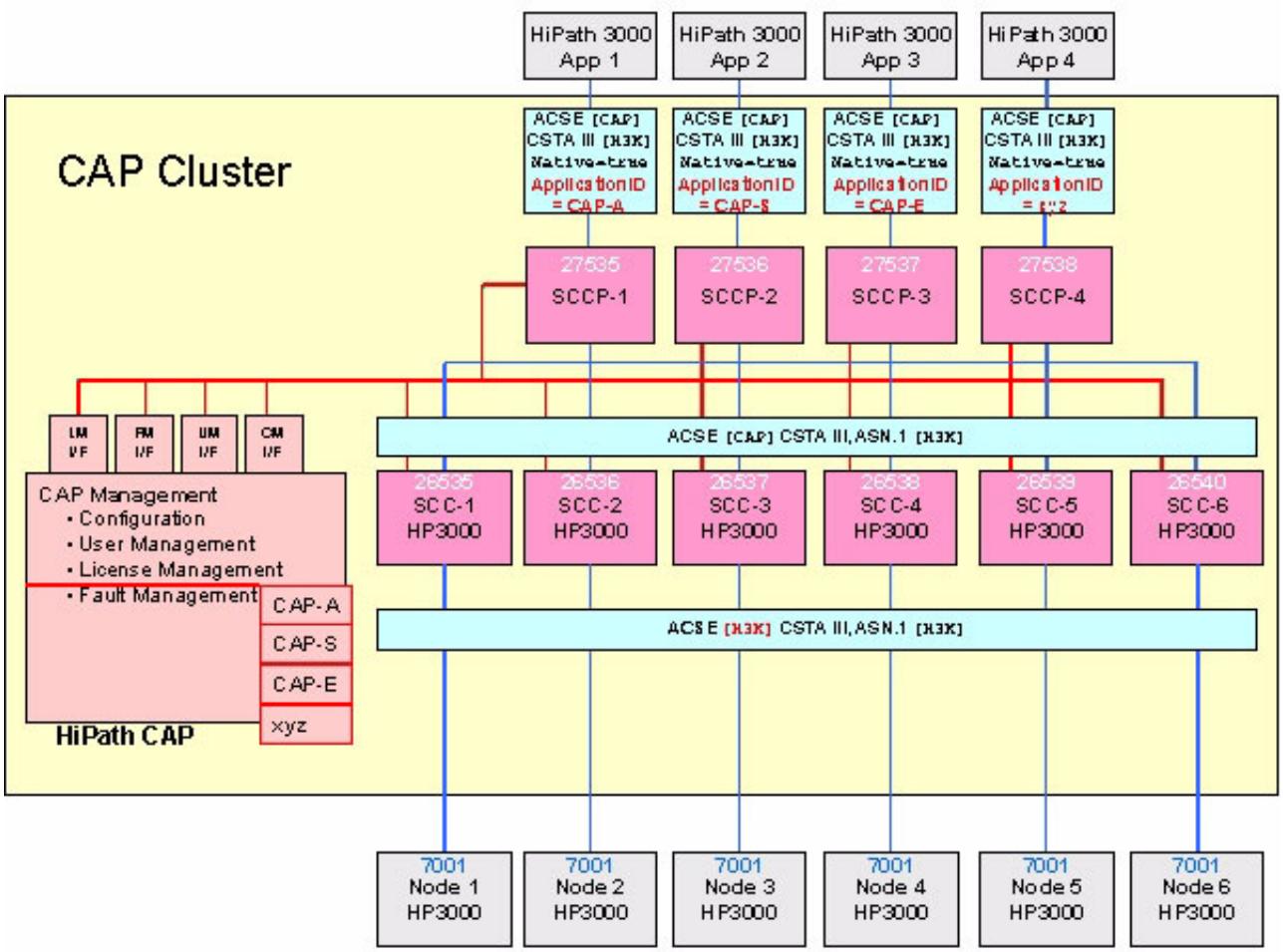
If several different applications are administered via one CAP Management, only one defined application is permitted to use an "Application ID".



9.2.4.2 Installation example: HiPath 3000 in "multi-domain//native mode"

NOTE ON THE "APPLICATION ID"

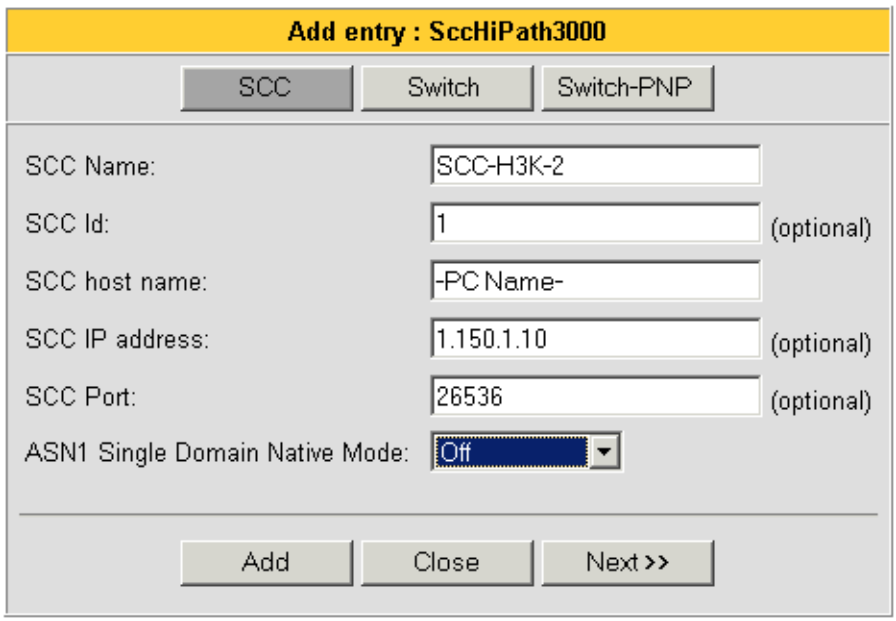
If several different applications are administered via one CAP Management, only one defined application is permitted to use an "Application ID".



9.2.5 HiPath3000 SCC/SCCP configuration in multi-domain//mode

Use the **Service - Switch Connection** menu item to add an "SCCHiPath3000".

"ASN.1 Single Domain Native Mode" is set to "Off".



Use the "Administration - SCCP Proxy" menu item to add one SCCP per application. Make sure that the service node number is also different than that of the SCC. You can "deactivate" the "AP Emergency" configuration parameter because it is only supported for HiPath 4000 systems with IPDA shelves integrated in the "CC-AP".

9.2.5.1 CTI users in "multi-domain//mode"

All CTI users must be configured under User Management.

9.2.5.2 Licensing in "multi-domain//mode"

An application's ACSE_AARQ is used to determine which license must be assigned to a CTI user.

With the first CSTA request, the SCCP 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 SCCP saves this information for 3600 seconds. This information is similarly deleted when the SCCP restarts.

9.2.5.3 Testing the HiPath 3000 "multi-domain//native mode" configuration

CSTA test program

To test this configuration, use the program `CSTA-Browser 3.2.exe`.

The HiPath 3000 proprietary protocol elements are supported in "via SCC3000, native" operating mode. The "CSP" identification facilitates input of a "Call ID" containing eight bytes.

The connection destination that is configured is the CAP SCCP IP address and the CAP SCCP port.

"Native = true" must be sent in the ACSE_AARQ.

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 four) is also indicated.

Application ID

The application ID is passed in the ACSE_AARQ.

Native mode = true/false

It is necessary to mark native mode explicitly ("Native = true").

Extensions

Extensions are addressed via their long call numbers if none of the corresponding requests contains an additional reference ID (for example, Call ID).

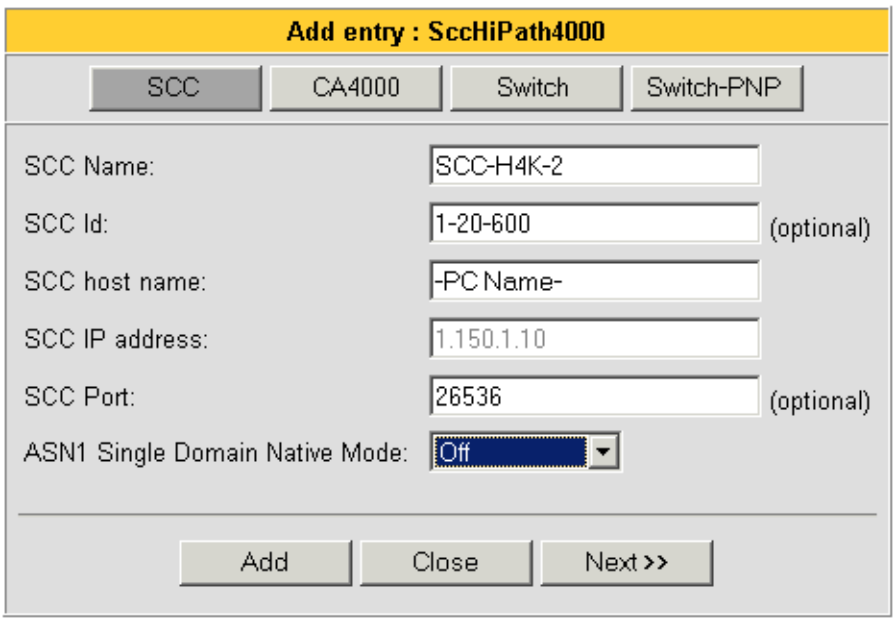
Call ID

The "Call ID" is a maximum of eight bytes long.

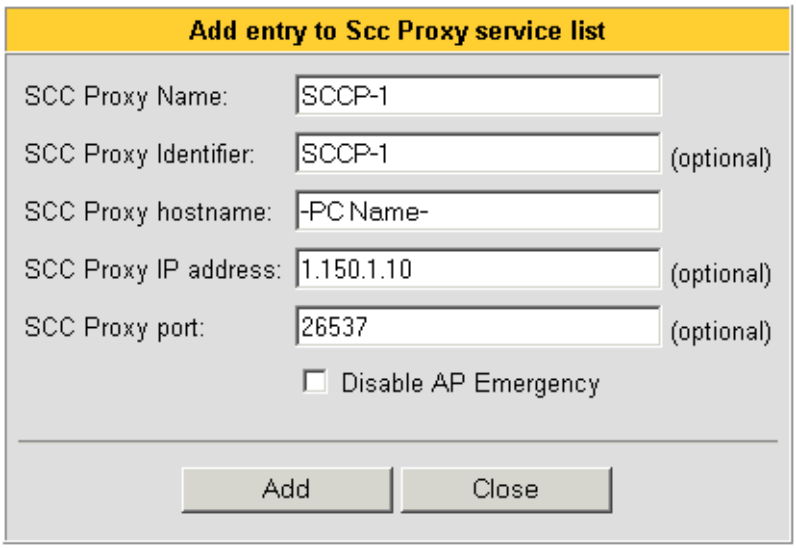
9.2.6 HiPath4000 SCC/SCCP configuration in multi-domain//mode

Use the "Administration - PBX Services" menu item to add an "SCCHiPath4000".

"ASN.1 Single Domain Native Mode" is set to "Off".



Use the "Administration - SCCP Proxy" menu item to add one SCCP per application. Make sure that the service node number is also different than that of the SCC. You can "deactivate" the "AP Emergency" configuration parameter if only HiPath 4000 systems without IPDA shelves integrated in the "CC-AP" are connected.



9.2.6.1 CTI users in "multi-domain//mode"

All CTI users must be configured under User Management.

9.2.6.2 Licensing in "multi-domain//mode"

An application's ACSE_AARQ is used to determine which license must be assigned to a CTI user.

With the first CSTA request, the SCCP 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 SCCP saves this information for 3600 seconds. This information is similarly deleted when the SCCP restarts.

9.2.6.3 Testing the HiPath 4000 "multi-domain//native mode" configuration

CSTA 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.

"Native = true" must be sent in the ACSE_AARQ.

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 necessary to mark native mode explicitly ("Native = true").

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 eight bytes long.

9.3 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, ASN1
- CSTA III, XML
- TAPI 2.1/3.1
- 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//MODE"

An SCC's "multi-domain//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".

9.3.1 What is the purpose of "multi-domain//harmonized mode"?

It is used to license a CTI client for 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.

9.3.2 Application-specific protocol requirements

For "multi-domain//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 eight bytes long.

9.3.3 Authentication - 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 is meaningless here. For successful authentication, the corresponding license must not be installed in the CAP.

CTI client licensing

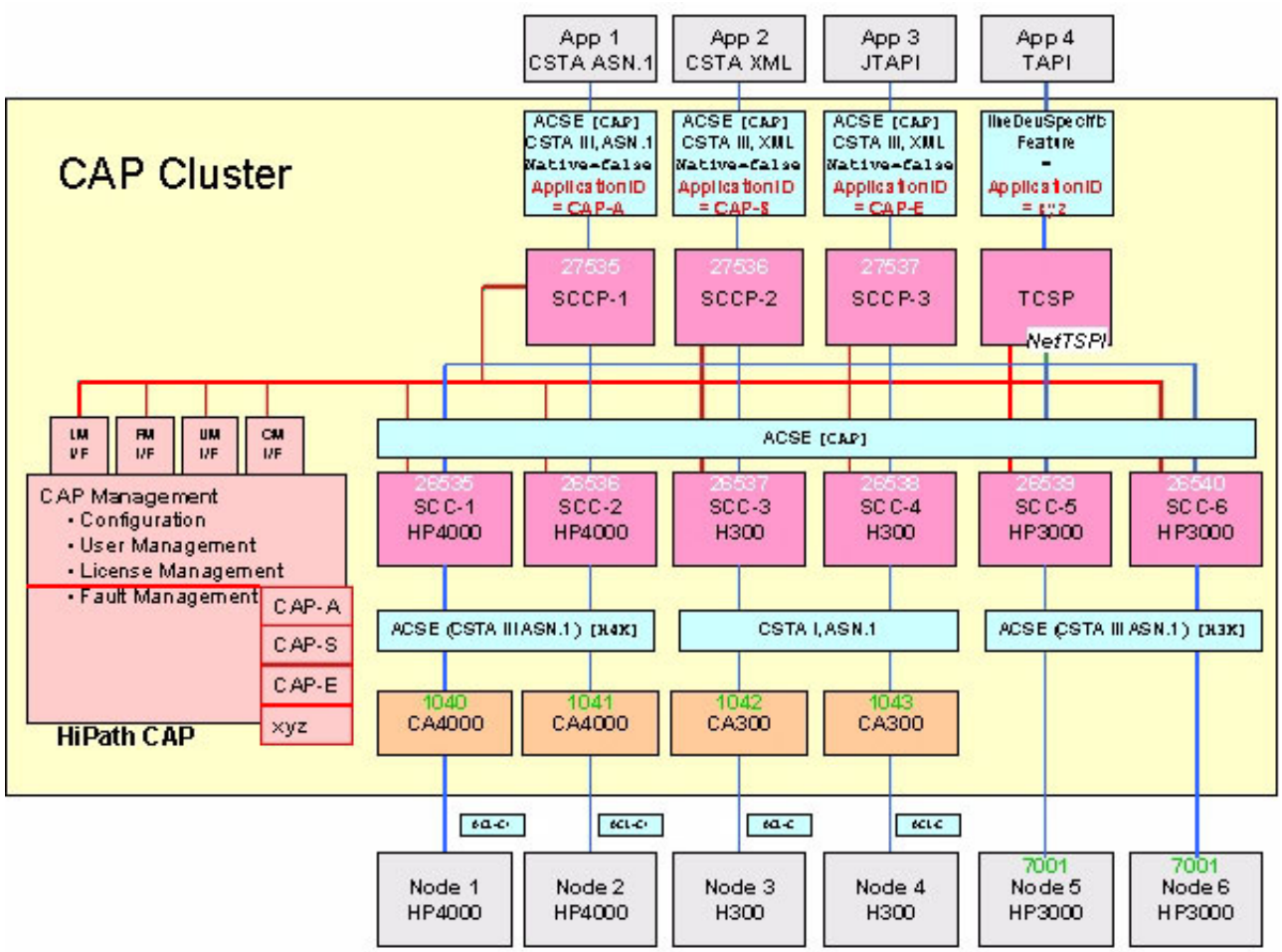
The SCCP stores the "Application ID" transmitted in the ACSE_AARQ and uses it later for CTI client licensing of CSTA requests (using the telephone number in canonical format). The SCCP sends a corresponding HTTP request (`http://<fqdn>:8170/mgmnt/admin/req?registerLicense= <ApplicationID>&userId=<DeviceID>`) to CAP License Management. If the license check was successful, the SCCP saves this information for 3600 seconds.

9.3.4 Installation example

9.3.4.1 Installation example: HiPath CAP V2.0 in "multi-domain//harmonized mode"

NOTE ON THE "APPLICATION ID"

If several different applications are administered via one CAP Management, only one defined application is permitted to use an "Application ID".



9.3.4.2 Configuration and communication model

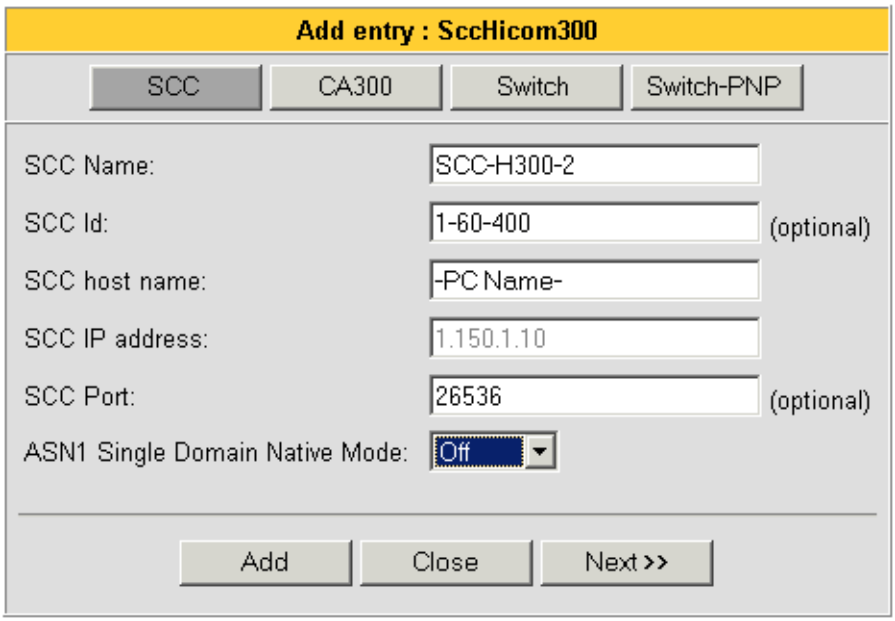
SCCHiPath 3000 and SCCHiPath4000 in "multi-domain mode"

The configuration and communication model is again identical to that of "multi-domain//native mode" and is not explained again here for the HiPath 3000 and HiPath 4000.

SCCHicom300 in "multi-domain mode"

Use the "Administration - PBX Services" menu item to add an "SCCHicom300".

"ASN.1 Single Domain Native Mode" is set to "Off".



9.3.4.3 Testing the CAP "multi-domain//harmonized mode" for the CSTA III, ASN.1 configuration

CSTA III, ASN.1 test program

To test the configuration for the CSTA III, ASN.1, 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 eight bytes long.

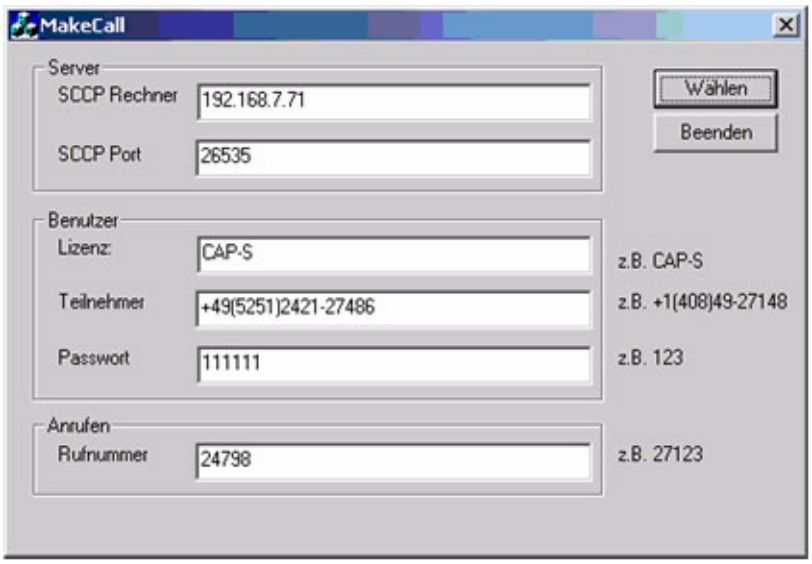
9.3.4.4 Testing the CAP "multi-domain//harmonized mode" for the CSTA III, XML configuration

CSTA III, XML test program

To test the configuration for the CSTA III, XML, use the program "MakeCall.exe."

The connection destination that is configured is the CAP SCCP IP address and the CAP SCCP port.

The station to which the device was assigned one time in the CAP is also used for authentication here. This requires that an individual password be assigned to this CTI user because the default password must absolutely be changed during initial authentication and this program does not support this function.


MakeCall
Server
SCCP Rechner
192.168.7.71
SCCP Port
26535
Wählen
Beenden
Benutzer
Lizenz:
CAP-S
z.B. CAP-S
Teilnehmer
+49(5251)2421-27486
z.B. +1(408)49-27148
Passwort
111111
z.B. 123
Anrufen
Rufnummer
24798
z.B. 27123

9.3.5 JTAPI

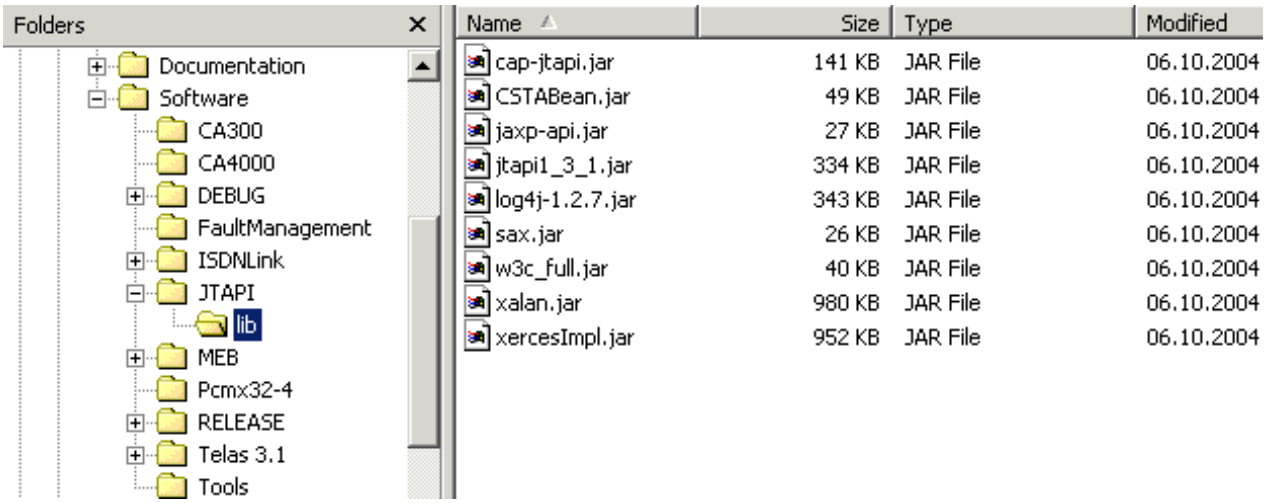
The JTAPI protocol is only supported in "multi-domain//harmonized mode".

HiPath 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 III, XML.

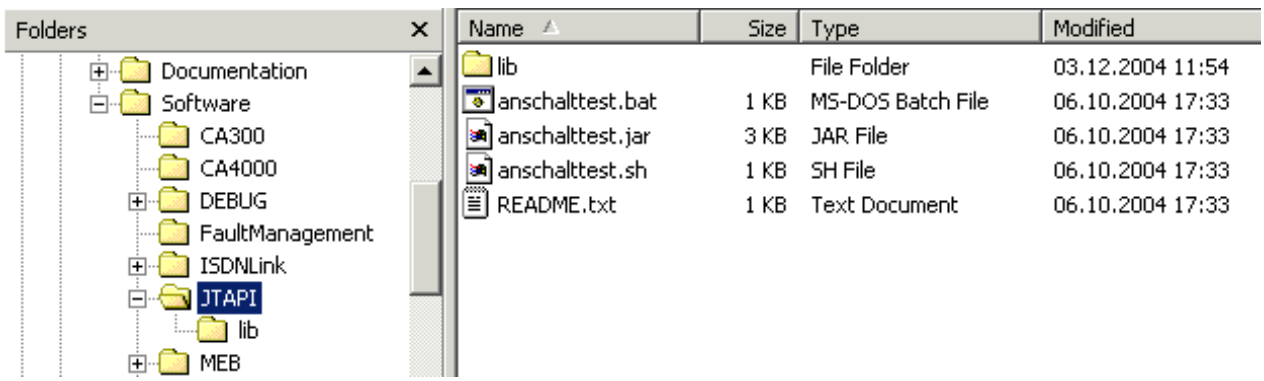
The Java classes are located on the HiPath CAP V3.0 CD in the directory: "Software\JTAPI\lib".



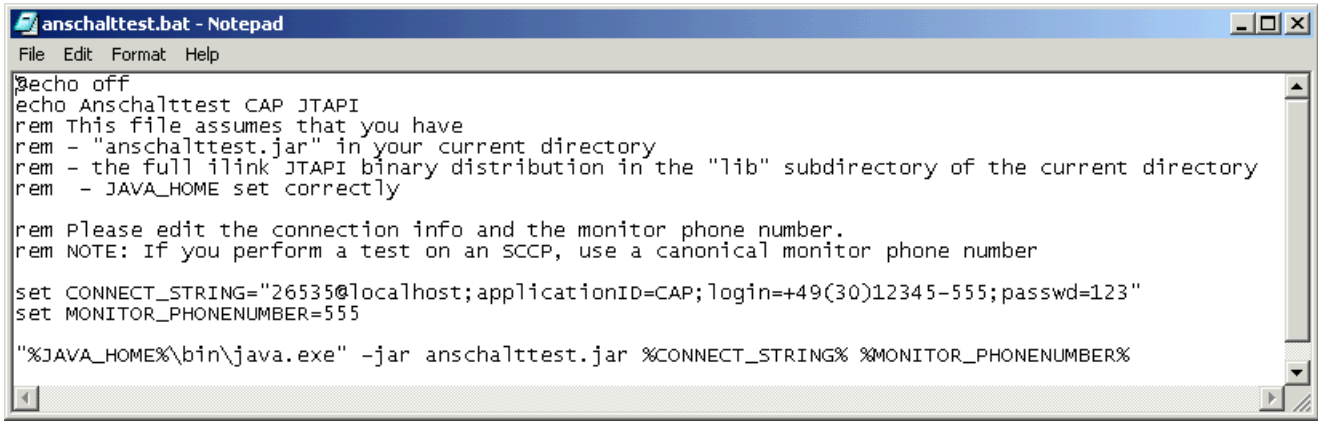
9.3.5.1 JTAPI test

"Java Runtime Environments 1.3.1" or later must be installed to test JTAPI.

The "anschalttest.bat" test program is located on the HiPath CAP V3.0 CD in the directory "Software\JTAPI".



The file contents must be adapted as appropriate during installation.



`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\JavaSoft\JRE\1.3.1\).

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.

9.3.6 TAPI

The HiPath CAP TAPI Service Provider (CAP TCSP) can be used by all Windows TAPI-based programs.

9.3.6.1 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
2. CAP-A
3. CAP-S
4. CAP-E

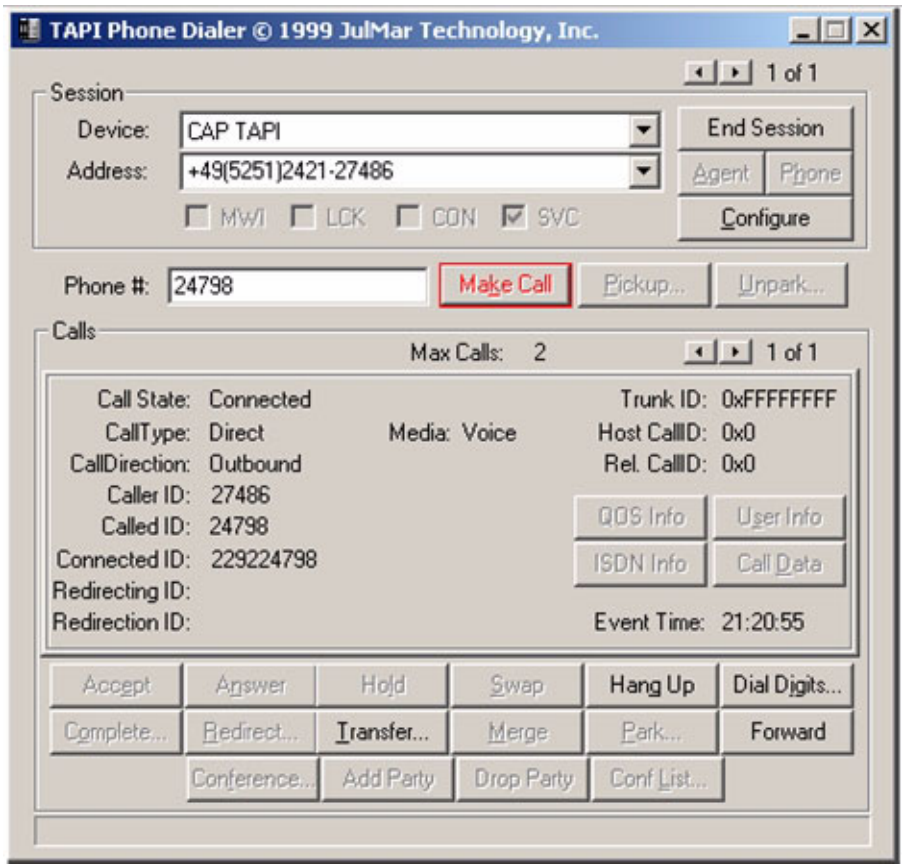
The connection to the CAP TCSP is interrupted if none of the requested licenses has been assigned. The CAP TCSP reacts by displaying an error message on the monitor.

New TAPI applications (such as xPhone) use an individual "Application ID" by setting a parameter in the "LineDevSpecificFeature".

9.3.6.2 Testing the CAP "multi-domain//harmonized mode" for the TAPI configuration

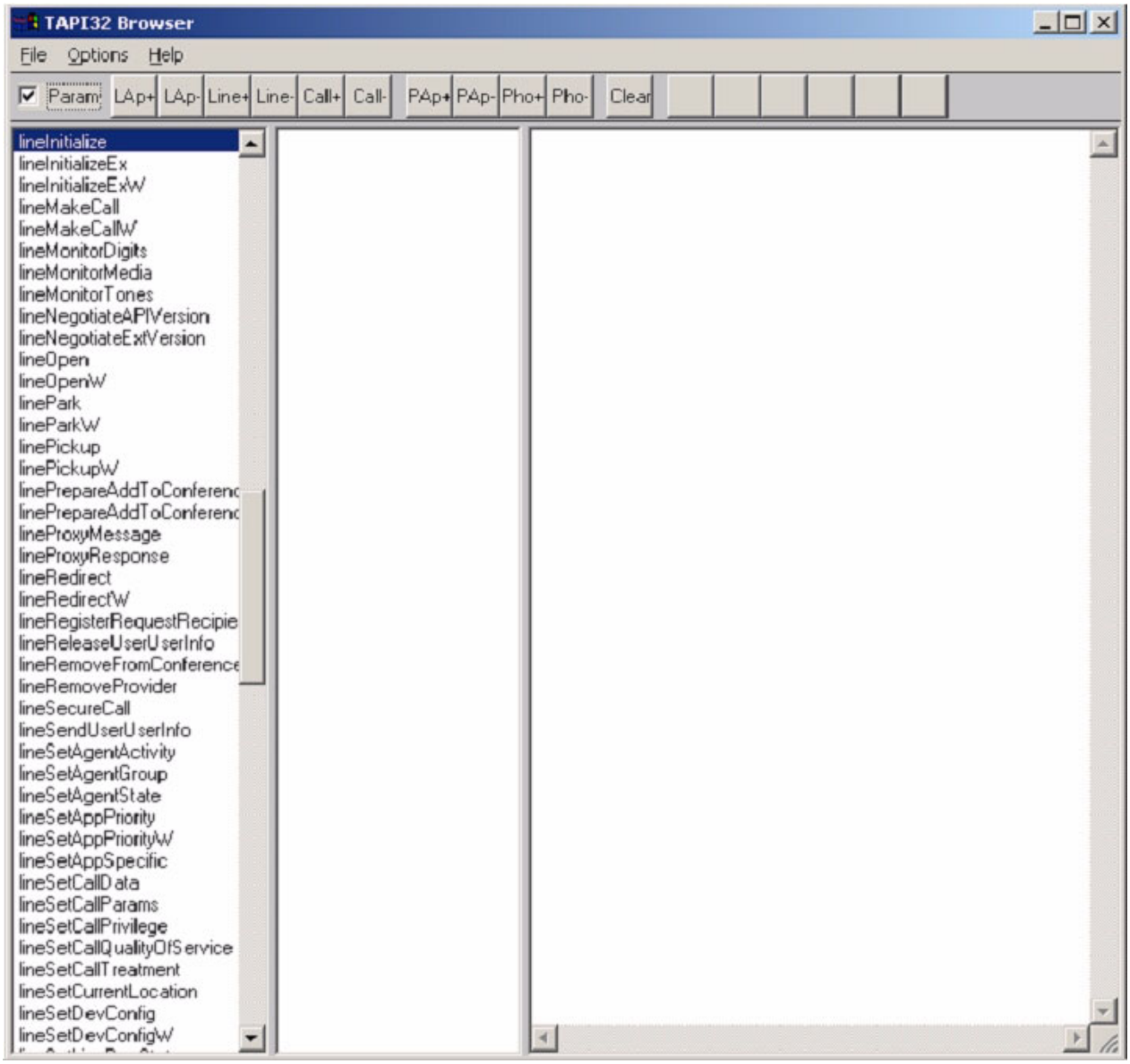
9.3.6.3 TAPI test program `Phone.exe`.

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.



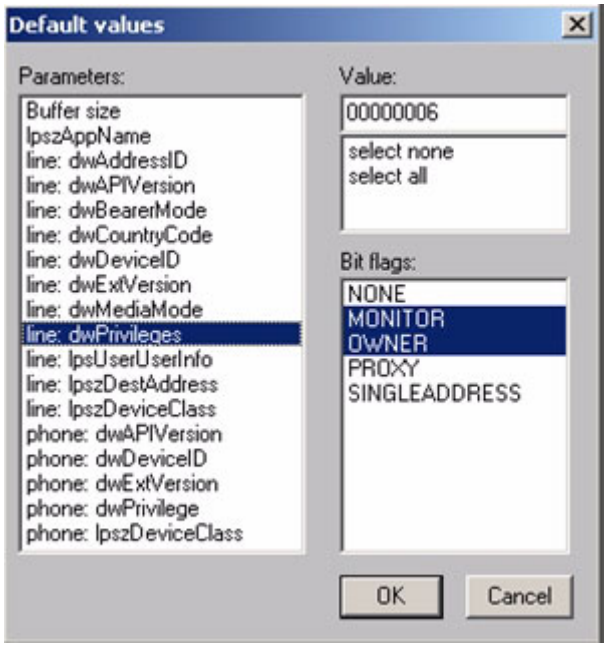
9.3.6.4 TAPI test program `tb20.exe`

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**".

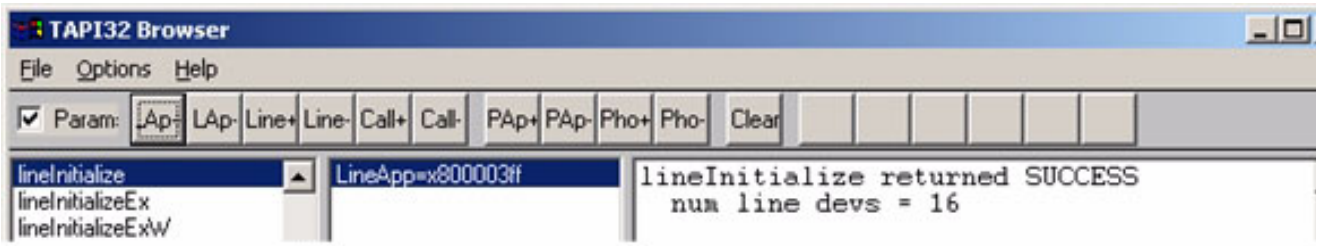
Set "**line dwPrivilege**s" to "**Monitor**" and "**Owner**".



Establishing the link to the Windows TAPI server

```
"lineInitialize"
```

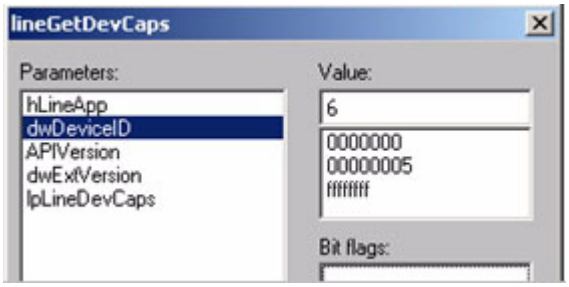
In response, you get the "**LineApp**" handler and the number of available line devices (provided by all installed TAPI service providers).



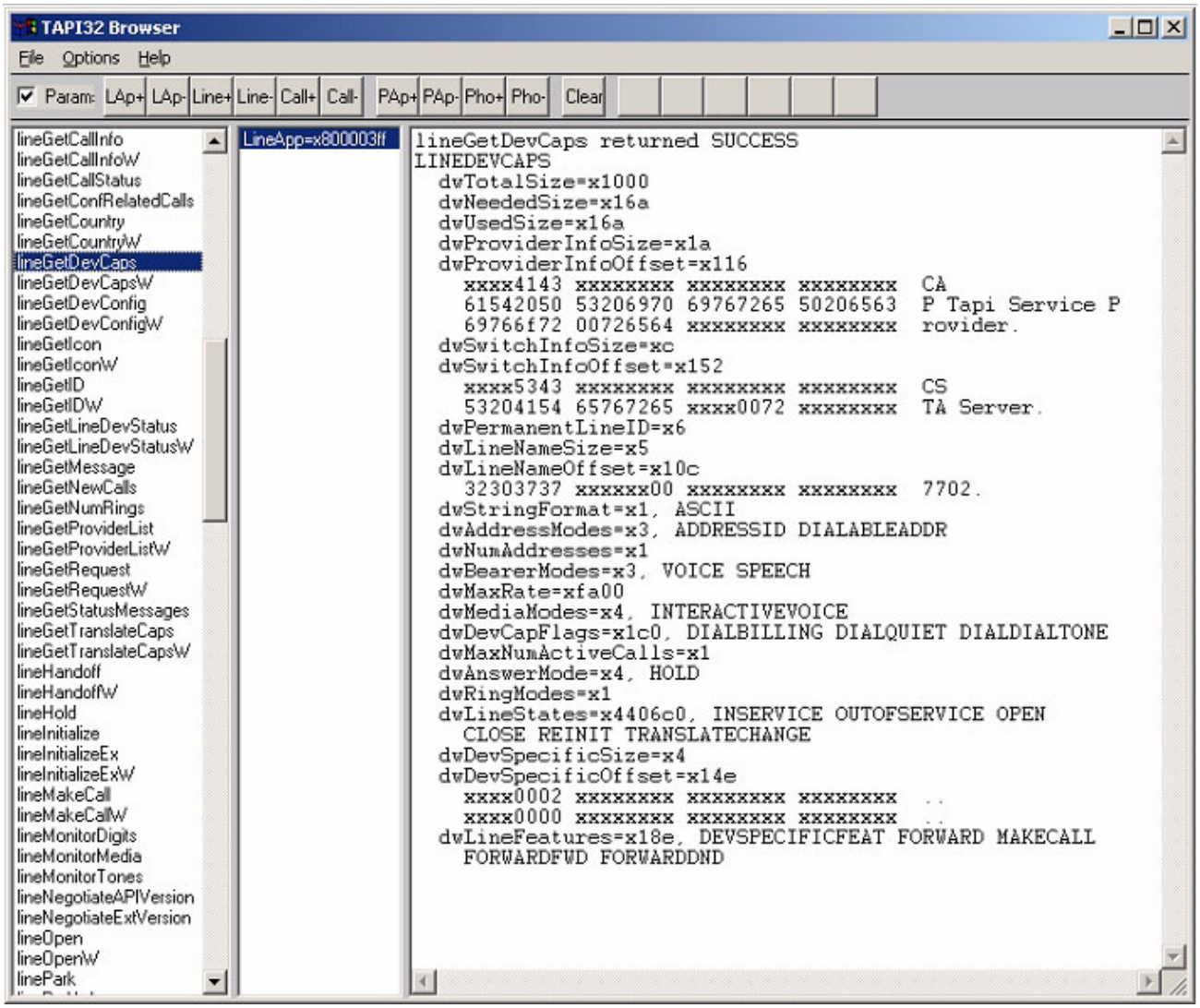
Finding a suitable TAPI line device

```
"lineGetDevCaps"
```

Enter the device IDs (one after the other) to find the related line devices.



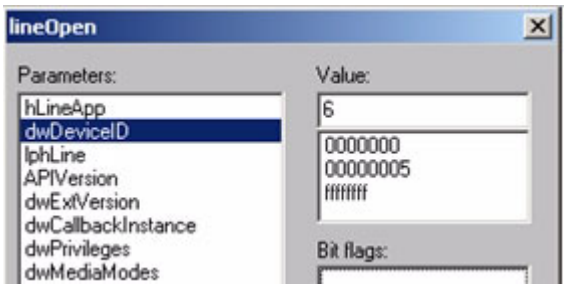
In response, you get detailed information about every available line device.



Opening a TAPI line device

"lineOpen"

Enter the line device's ID.

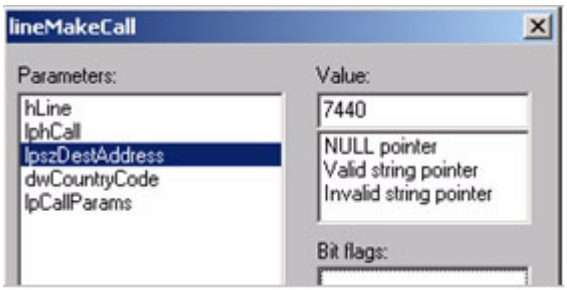


In response, you get information about the line session ID.

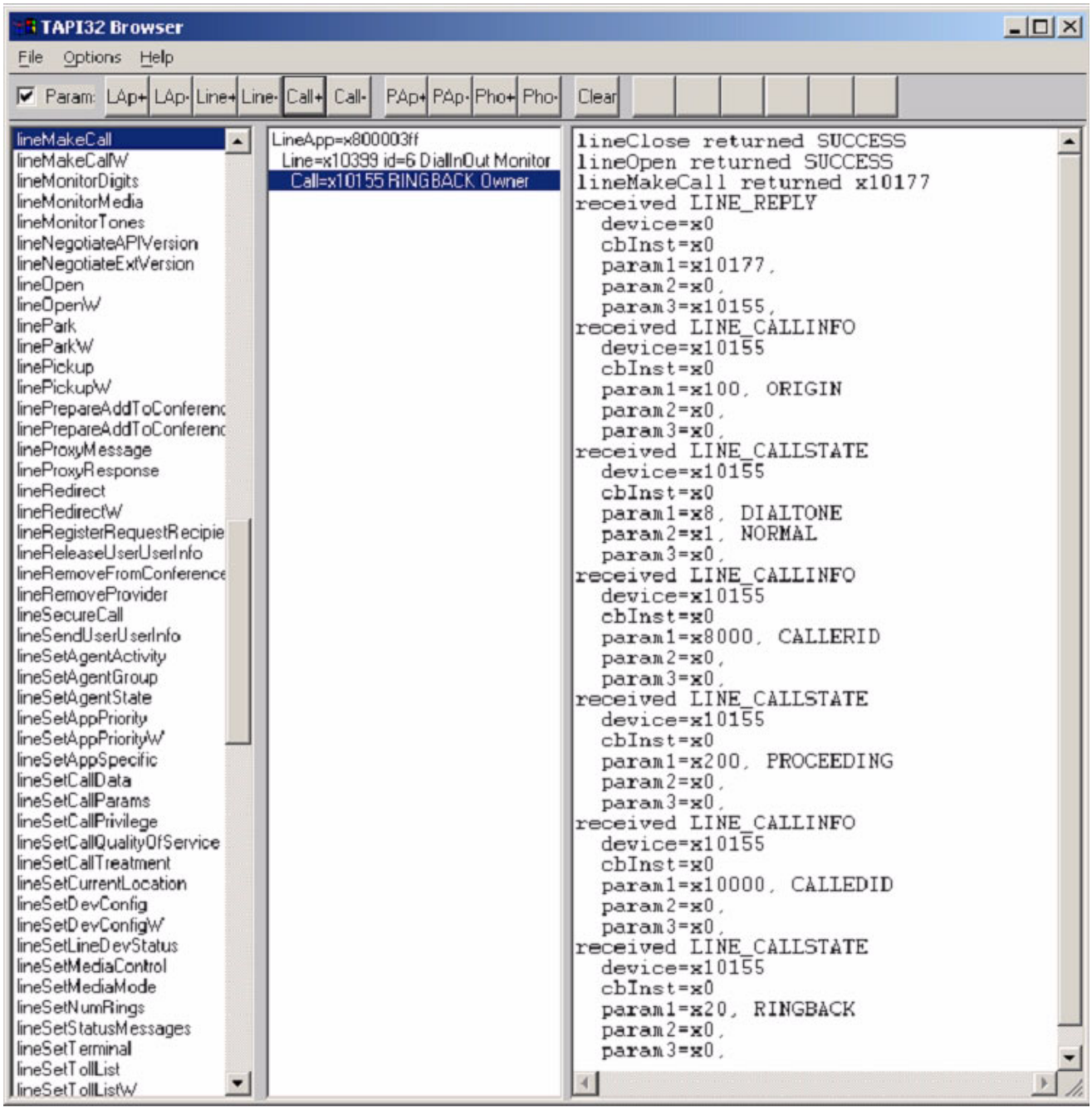
Making a call

"lineMakeCall"

Enter the destination number at "**lpszDestAddress**".



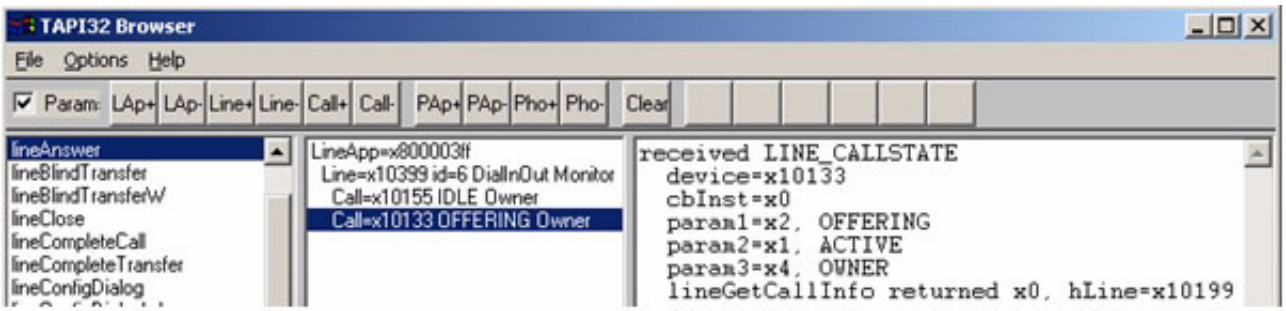
In response, you get information about the call ID.


TAPI32 Browser
File Options Help
Param: LAp+ LAp- Line+ Line- Call+ Call- PAp+ PAp- Pho+ Pho- Clear
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,

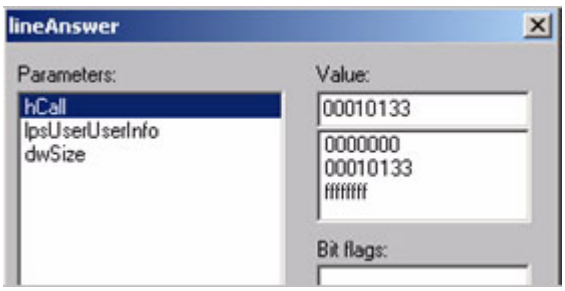
Answering a call

`"lineAnswer"`

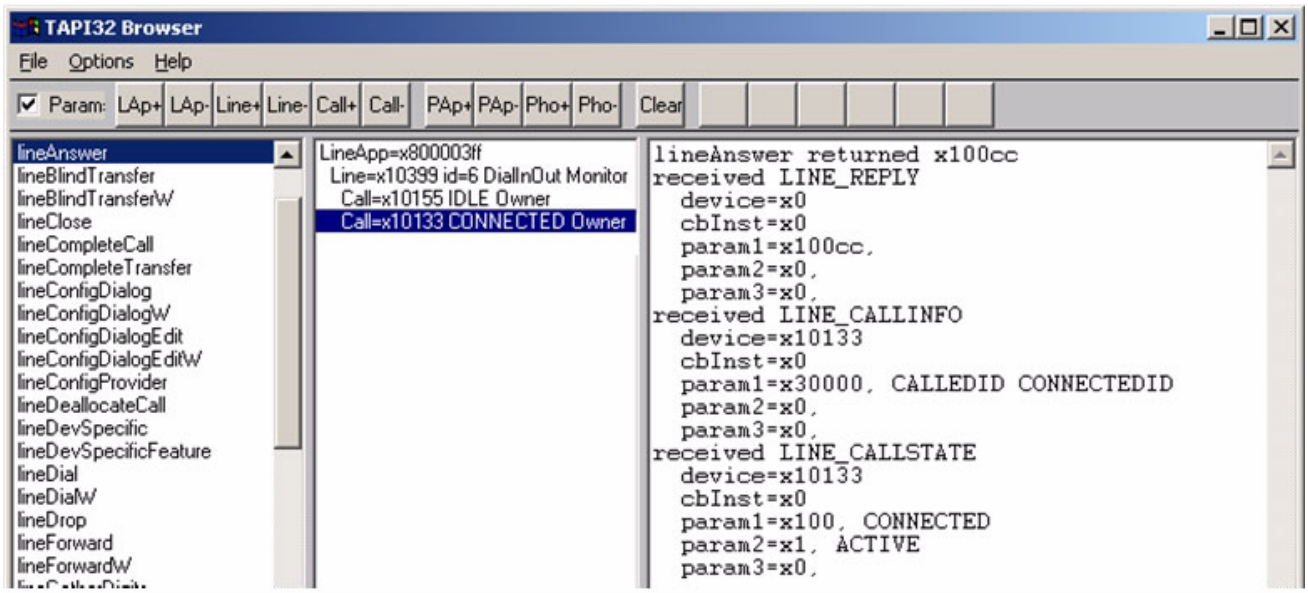
An incoming call is offered to the line owner.



Enter the "**hcall**" number of the offered call.



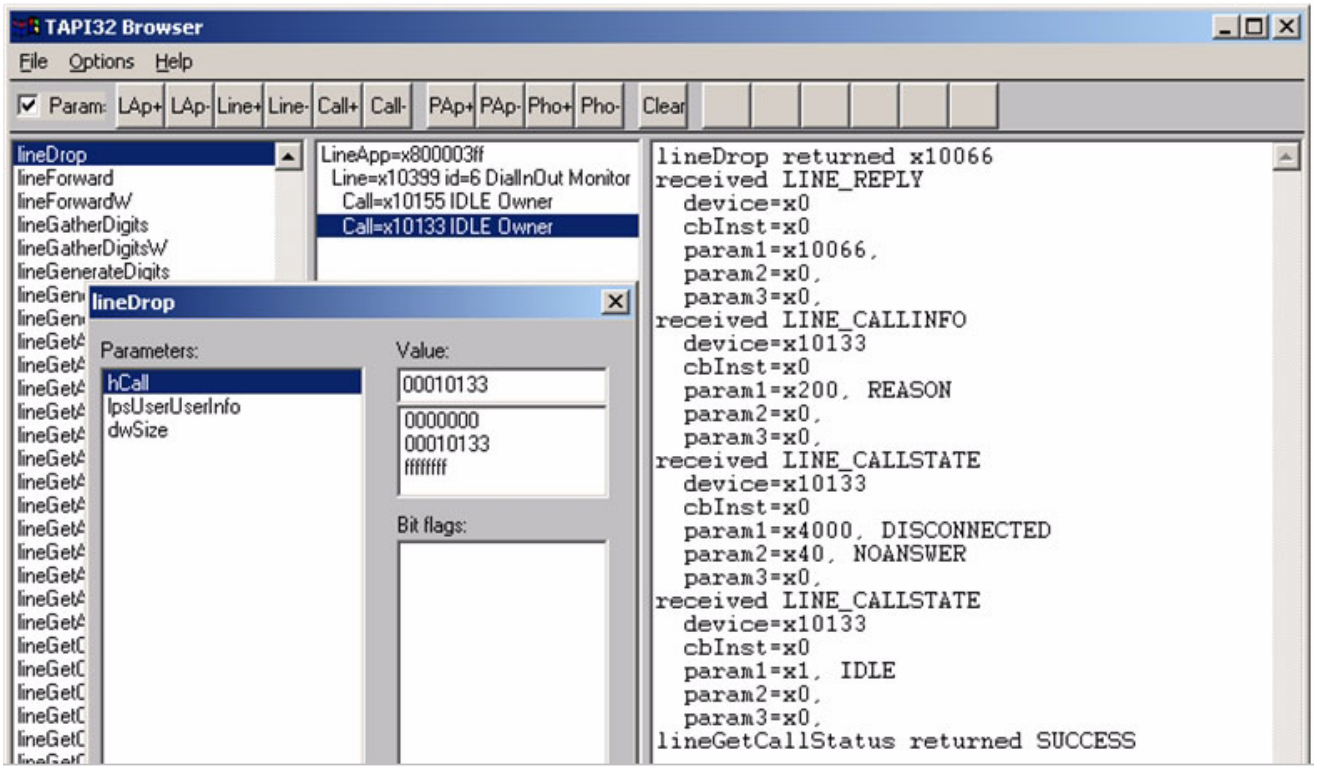
In response, you get information about the connected call.



Hanging up a call

`"lineDrop"`

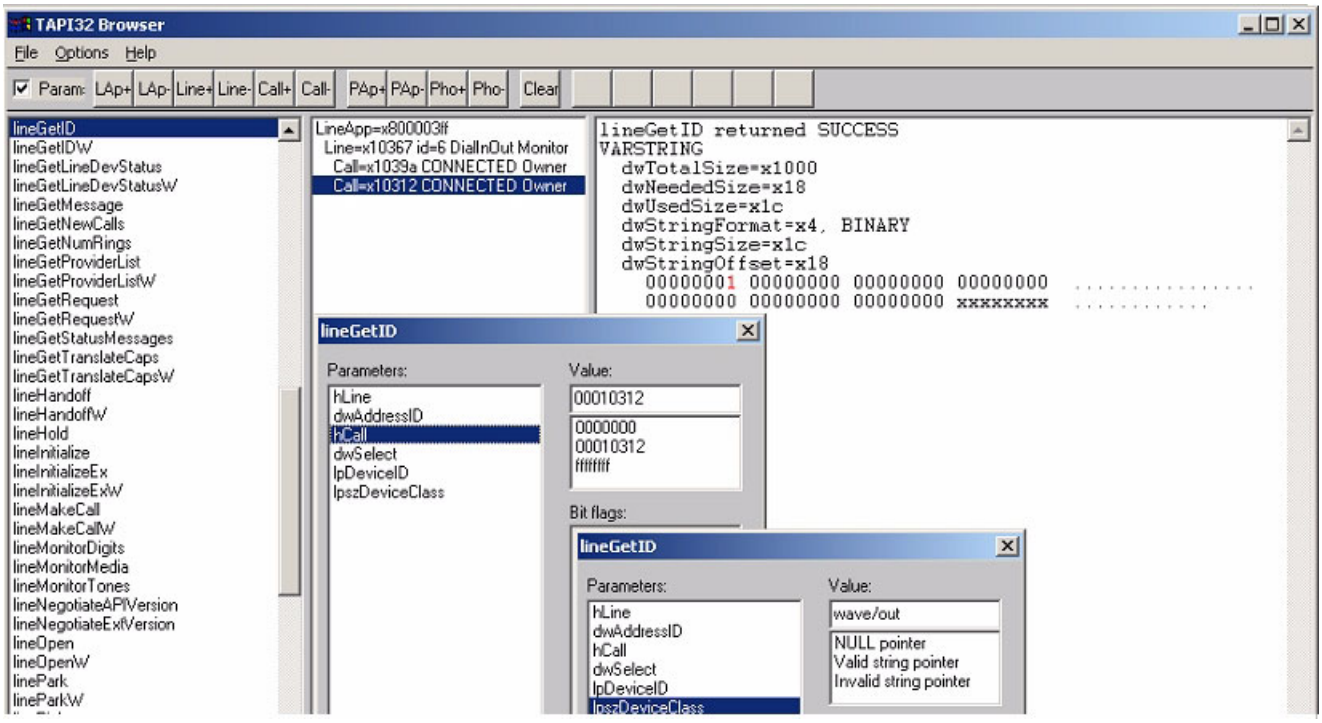
Enter the "**hcall**" number of the connected call.



Getting media device ID

`"lineGetID"`

Enter the "**hcall**" number of the connected call and "**wave/out**" or "**wave/in**" for "**lpzDevice-Class**".

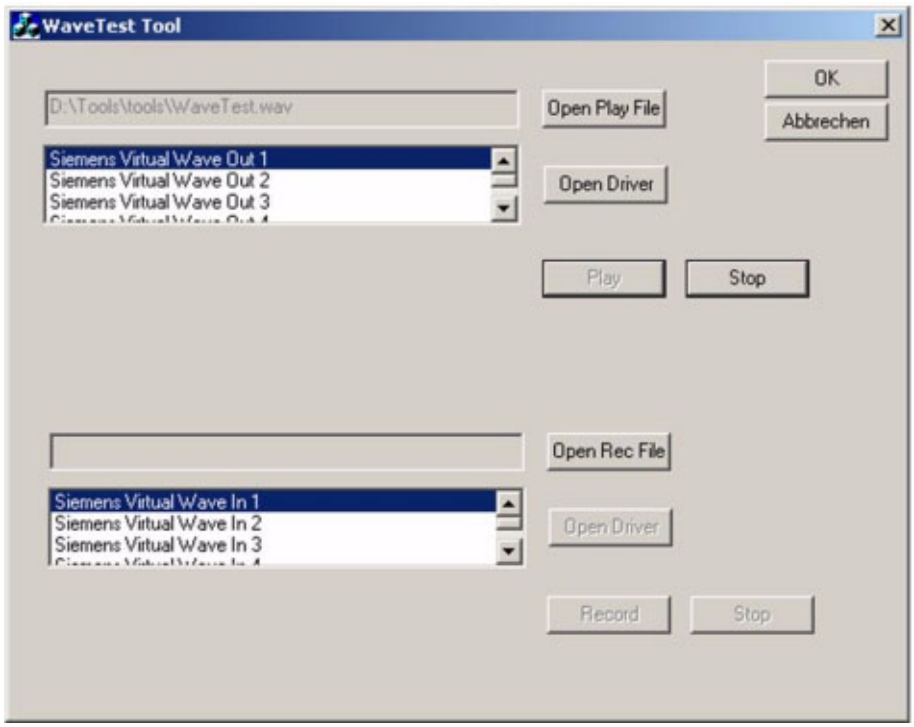


Playing a wave file with “WaveTest.exe”

Start program:

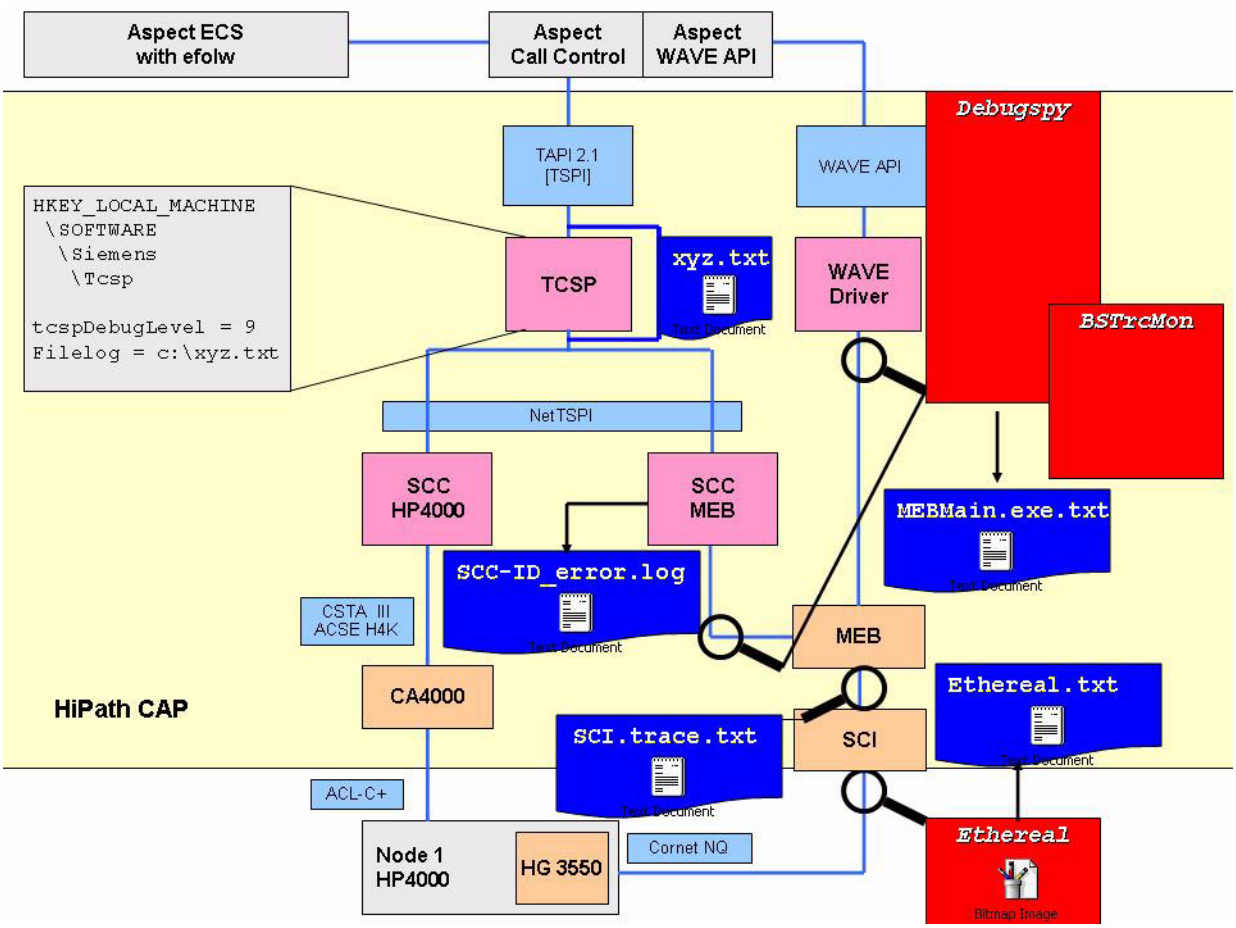
```
C:\Program Files\Siemens\HiPathCTI\binools\WaveTest.exe
```

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.



9.3.7 MEB

The following flowchart describes how to enable the SCCMEB and MEB traces.



9.3.7.1 Testing the communication between HG3550 V2 and CAP MEB PC

To test for proper communication between the HG3550 V2 and the CAP MEB PC, you only need the program called **NetMeeting**. The H.225 communications port must be set to 1720 (default), and the MEB should not be running.

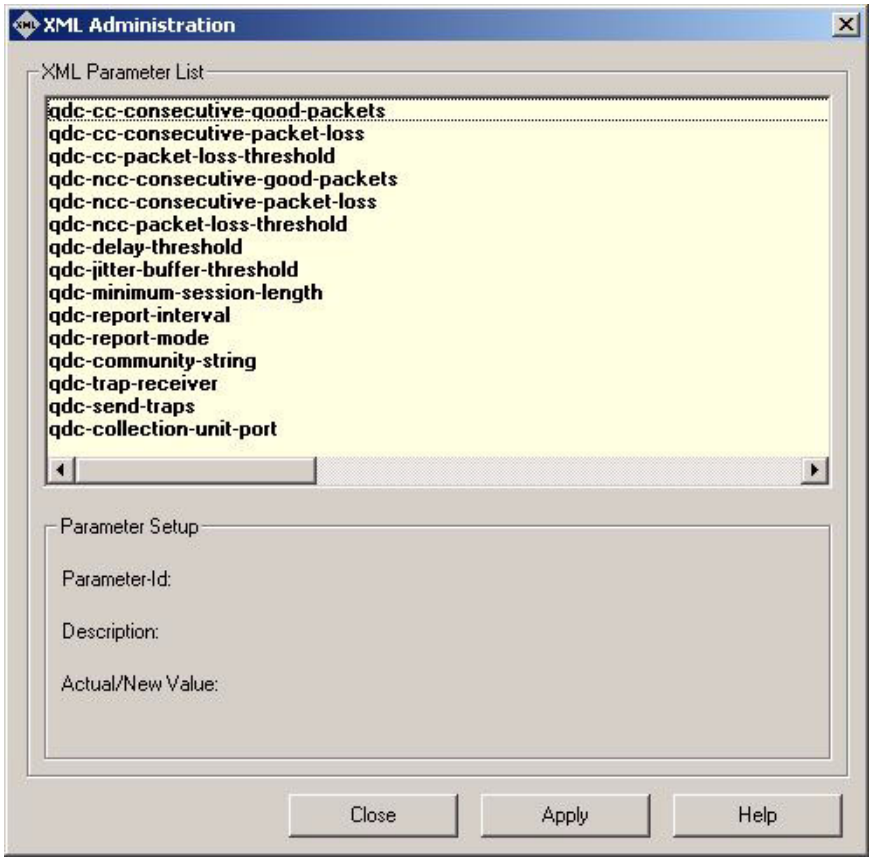
1. Stop the "Siemens HiPath CTI" Windows service on the CAP Managment PC, or the Windows 2000 service "Siemens CAP ServiceStarter" on a CAP ServiceStarter PC.
2. Start NetMeeting.
3. Select the configured node acces code for the MEB with the corresponding number of suffix digits.
4. If a connection can be successfully established, NetMeeting should signal an incoming call. More functions are not supported. That ends this test. The HG3550 V2 is correctly configured and the communication with the CAP MEB PC works.

9.3.7.2 How to check MEB

The program name of the CAP MEB is `MEBMain.exe`. With this and another two test tools (`MEBAppTester.exe` and `WaveTest.exe`), you can perform a complete check of the MEB installation.

You can start without having a connection to CAP Management:

1. Stop the Windows service "Siemens HiPath CTI" or "Siemens CAP ServiceStarter".
2. Copy `C:\Programme\Siemens\HiPathCTI\binools\XMLAdmin.exe` to `C:\Programme\Siemens\HiPathCTI\bin\meb\.`
3. Run `XMLAdmin.exe`.
   During the `MEBMain.exe` startup, some important parameters are required. Without needing a connection to CAP Management, the file `MEBMain.xml` provides these parameters. The program `XMLAdmin.exe` makes it easy to perform the necessary modifications.

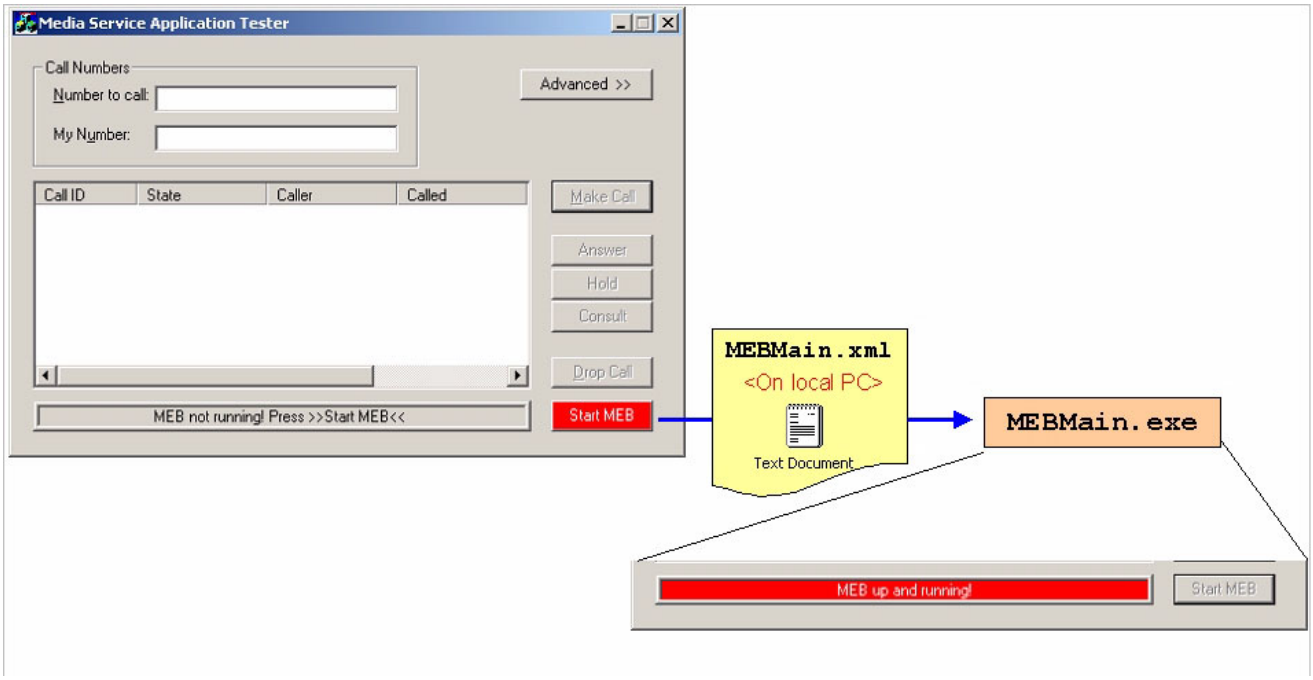


qdc-cc-consecutive-good-packets	Threshold value for consecutive good packets for compressing codecs	8	
qdc-cc-consecutive-packet-loss	Threshold value for consecutive packet loss for compressing codecs	2	
qdc-cc-packet-loss-threshold	Threshold value for packet loss for compressing codecs	10 (0.1%) = 1 %	
qdc-ncc-consecutive-good-packets	Threshold value for consecutive good packets for non-compressing codecs	8	
qdc-ncc-consecutive-packet-loss	Threshold value for consecutive packet loss for non-compressing codecs	2	
qdc-ncc-packet-loss-threshold	Threshold value for packet loss for non-compressing codecs	10 (0.1%) = 1 %	
qdc-delay-threshold	Delay Threshold	100 (millisec)	
qdc-jitter-buffer-threshold	Jitter buffer	15 (millisec)	

qdc-minimum-session-length	Minimum session length	10th part of second = 2 sec	
qdc-report-interval	Report interval	10/20/30/ 40/50/60/ 70/80/90/ 100/110/ 120/130/ 140/150/ 160/170/ 180/	
qdc-report-mode	ReportMode	0/1/2/3/4/ 5/	
qdc-community-string	SNMP Community String	public	
qdc-trap-receiver	IP address of SNMP trap receiver		
qdc-send-traps	QDC reports QCU activation	0 (no)	
qdc-collection-unit-port	QCU IP port	12010	
qdc-collection-unit-addr	QCU IP address		
qdc-send-to-qcu	QDC reports QCU activation	0 (no)	
AUTOACCEPTINCOM-INGCALLS	Auto-accept alert function	1 (on)	
SYSDEVCODECTYPE	System codec setting	1/2/	
CREATINGAREAID3	Creating area ID for global call ID	3	
CREATINGAREAID2	Creating area ID for global call ID	2	
CREATINGAREAID1	Creating area ID for global call ID	1	
CREATINGNODE	Creating node for global call ID	1	
USECAPMNGT	Cap Management integration	0/1	
CREATESCILOG	SCI log activation	0/1	
STATISTICTIMER	Statistics times in ms	900000 (15 min-utes)	
CREATESTATISTICS	MEB statistics	0/1	
GATEWAYCODECTYPE	Codec setting	0-14 3	
H245PORTRANGETO	Port range end for H245 packets	12100	
H245PORTRANGEFROM	Port range start for H245 packets	12000	

RTPPORTRANGETO	Port range end for RTP packets	29131	
RTPPORTRANGEFROM	Port range start for RTP packets	29100	
OUTPUTDEBUGSTRIN-GLEVEL	Trace level for OutputDebugString	1-9-10	
TRACEMONITORLEVEL	Trace level for monitor application	1-9-10	
CALLNUMBERLIST	MEB call number list		CAP
H255SIGNALINGPORT	MEB H225 signaling port	1720	CAP
NUMCHANNELS	Number of licensed channels	1-30-254	CAP
MEDIAGATEWAYIP	HiPath HGxxxx IP address		CAP
OWNMEBIP	IP address for MEB		CAP
DLSIP	IP address for DLS		CAP
CALLNUMBERLENGTH	Calling number length	3-9	CAP
USELIST	MEB uses list of calling numbers	0/1	CAP
USELENGTHCHECK	MEB calling number length check	0/1	CAP
CALLERNUMBERMEB	MEB calling number	+49(5251) 8-27486	CAP

4. Change the value for **USECAPMNGT** to "**0**" and change all required values too.
5. Start `MEBAppTester.exe` and use the feature **Start MEB** to start the `MEBMain.exe`.
6. The message **`MEB up and running`** should appear in the program status line.
7. Now perform your tests.. After a test, do not forget to use the `XMLAdmin.exe` program to set the `USECAPMNGT` parameter in the `MEBMain.xml` file back to `1`.



After a test, do not forget to use the `XMLAdmin.exe` program to set the `USECAPM-NGT` parameter in the `MEBMain.xml` file back to `1`.

If a MEB was started with the `MEBAppTester.exe` test program, it is imperative that the **MEBMain.exe** process be manually terminated with the Task Manager after completion of all tests.

9.3.7.3 MEB test with CAP

If the MEB is started from the CAP, the communications interface for `MEBAppTester.exe` is at first blocked by the SCCMEB.

1. Start the "Siemens HiPath CTI" Windows service on the CAP Managment PC, or the Windows 2000 service "Siemens CAP ServiceStarter" on a CAP ServiceStarter PC.
2. Use the Diagnostics Agent to stop the associated SCCMEB.
3. Run `MEBAppTester.exe`. The message "MEB up and running" should appear in the program status line.
4. Now you can perform your tests.

9.3.7.4 MEB Test with all CAP components

If you want to test a MEB with all CAP components, i.e. you want to perform a test under application conditions, you can only do this together with the CAP TCSP. See Section 9.3.6.4. It provides a basic description of how to use the TAPI test program "tb20". After establishing a connection with a MEB (using the configured phone number in canonical format), you have to find a free `wave/in` or `wave/out` channel with `lineGetID`. This reserves a wave channel on the Siemens Virtual Wave Driver. Only then can you use the WaveTester.exe test program to open this channel and play or record a speech file.

9.3.7.5 MEB test tool "MEBAppTester"

The tool `MEBAppTester.exe` starts `MEBMain.exe` and immediately establishes a connection to the MEB. `MEBAppTester.exe` supports the fundamental Call Control functions, such as, MakeCall, AnswerCall, etc., and the "Play/Stop a wave file" function can be set to automatic or manual control.

You can use this tool to test the all MEB functions (telephony and audio functions). The tool behaves in the same way as an SCCMEB and uses the same methods to communicate with the MEB.

The tool is supplied with HiPath CAP 3.0 and is stored in the directory `C:\Program Files\SIEMENS\HiPath\bin\tools` when CAP 3.0 is installed. No additional installation procedures are needed because the relevant files can be called directly from this directory.

Functions supported

- Make A Call
- Answer A Call
- Hold A Call
- Retrieve A Call
- Consultation
- Transfer A Call
- "Auto-Answer Calls"
- "Auto-Drop on close"

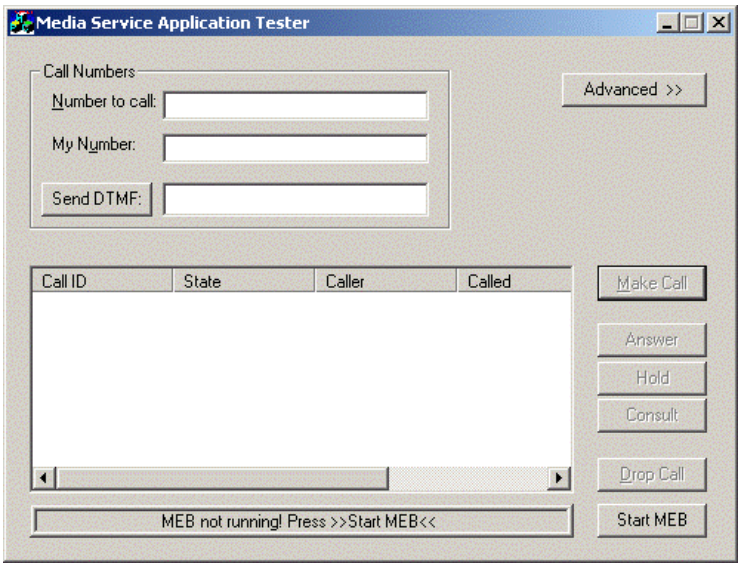
Starting the MEB Application Tester

Start the tool by double-clicking the file `MEBAppTester.exe` in the directory `C:\Program Files\SIEMENS\HiPathCTI\bin\tools`.

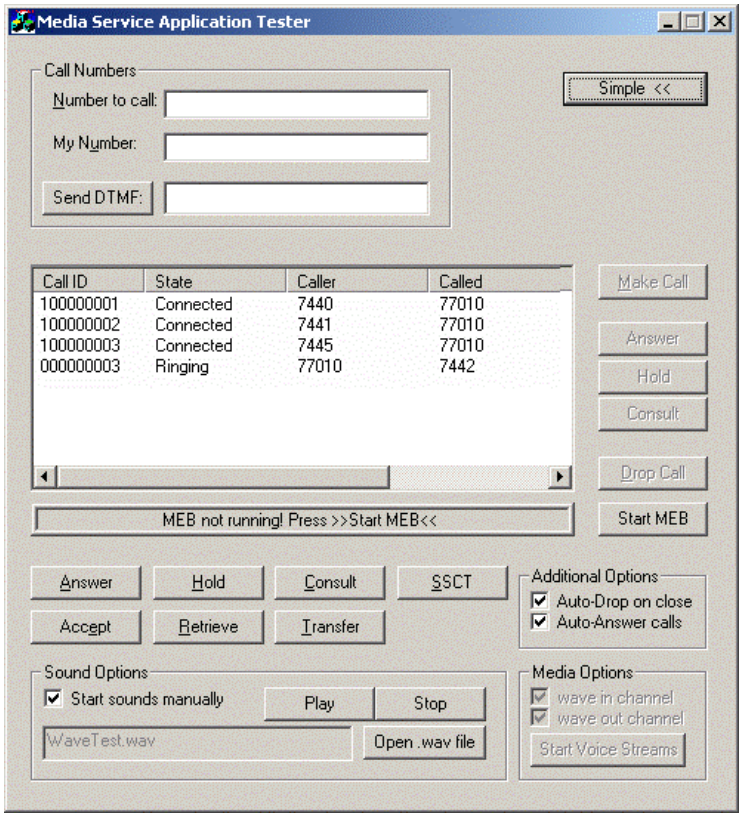
> The SCCMEB may not be active when the tool is started; if necessary you should close this service using CAP Management.
> The MEB must be started to enable the test functions to be performed. You can start the MEB using CAP Management, for example, or directly by starting the MEB program file, or by using the button in the MEB Application Tester tool.

Testing telephony functions

You can choose between **Simple** and **Advanced** mode during testing. The tool first appears in Simple mode when the program starts:



You can switch from one mode to the other by clicking the **Advanced >>** button (or **Simple <<**). In **Advanced** mode, the dialog looks as follows:



The list contains current rules under **Call ID** (unique), a **State** (call state), **Caller** and **Called**. You can perform several calls in parallel. Current status messages from the tool are shown in the status line under the list of calls.

The fields and buttons have the following meanings:

- **Number to call:**
  Target call number for the test function (called partner).
- **My number**
  Caller number for the test function. It appears in the called party's display.
- **Send DTMF**
  The numbers entered here are emitted as DTMF tones into an existing, marked connection.
- **Make Call**
  Establish an outbound call from caller number to target call number.
  Call state: first *Calling*, then *Ringing*, then when the call is answered *Connected*.
- **Answer**
  Answer an incoming call to your own phone number.
  Call state changes from *Incoming* to *Connected*.

- **Hold**
  Place an active call to your own phone number on hold.
  Call state change: from *Connected* to *Holding*.
  HiPath Music-on-Hold is played.
- **Consult**
  Perform consultation for an active call with the **Number to call**.
  Call state change: for the active call from *Connected* to *Holding*, for the new call first *Calling*, then *Ringing* and when the call is answered *Connected*.
- **Drop Call**
  End a call (irrespective of status).
  Call state change: state first changes to *Dropping*, then the call is removed from the list.
- **Start MEB**
  Starts the MEB (if it is not yet active).

Functions in Simple and Advanced modes

In both modes, the buttons to the right of the call list can only be used to test call functions that are logical and possible in the current call state, for example, "Consult" can only be tested when a call is active (*Connected*). When you click a call in the list, the buttons for unavailable functions are disabled in accordance with the current call state.

Additional function buttons only appear in the list in **Advanced** mode. You can use these buttons to start the relevant functions for calls regardless of the current call status.

Function buttons

- **Answer**
  Answer an incoming call to your own phone number.
  Call state changes from *Incoming* to *Connected*.
- **Hold**
  Place an active call to your own phone number on hold.
  Call state change: from *Connected* to *Holding*.
  HiPath Music-on-Hold is played.
- **Consult**
  Perform consultation for an active call with the **Number to call**.
  Call state change: for the active call from *Connected* to *Holding*, for the new call first *Calling*, then *Ringing* and when the call is answered *Connected*.
- **SSCT (Single Step Consultation Call)**
  Transfer an active call to the **Number to call**.
  Call state change: from *Connected* to *Holding*, for the new call first *Calling*, then *Ringing*.

– **Accept**
In an older version of the MEB, you had to use "Accept" for an incoming call before you could use "Answer".

– **Retrieve**
Retrieve a call held by your own phone number.
Call state change: from *Holding* to *Connected*.

– **Transfer** (only available in Advanced mode)
Highlight two existing MEB calls. Use "Transfer" to connect these calls with each other; they are no longer displayed in the MEB communications list.

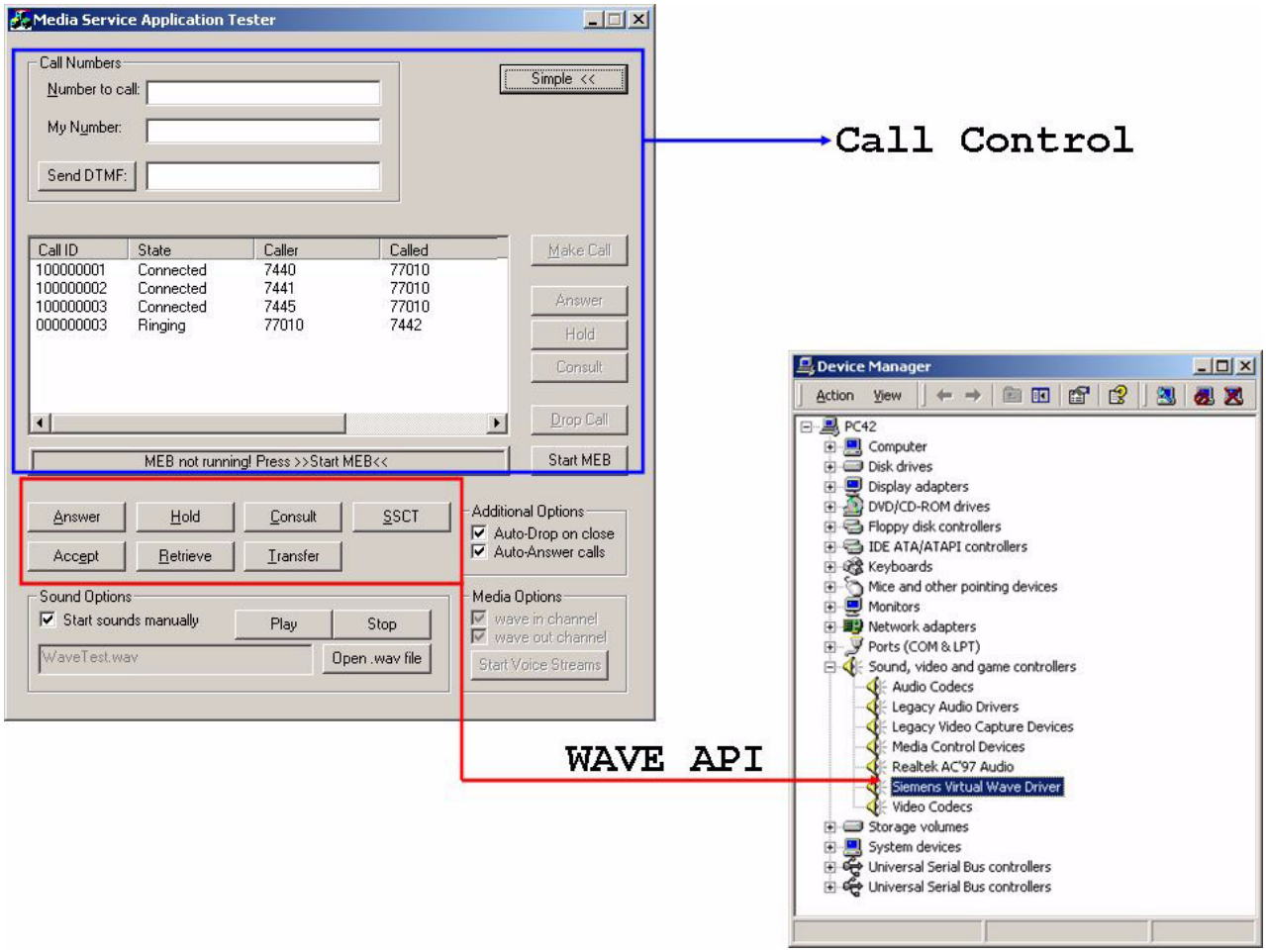
Call state

Calls can have the following state:

State	Meaning
Incoming	Incoming call to your own phone number.
Calling	Outbound call from your own phone number, connection setup (prior to *Ringing*).
Ringing	Outbound call from your own phone number, ringing.
Connected	Call connected. The `WaveTest.wav` audio file is played back in this status (music).
Busy	Call partner (**Number to call**) is busy.
Holding	Your own call number has placed an active connection on hold.
Held	The call partner has placed an active connection with his own call number on hold.
Dropping	The call is dropped (disconnected). This state is displayed for a call after **Drop Call** is activated and until the call is removed from the list.

Options for playing back the sound file (sound options)

- By default, the standard audio file (file `WaveTest.wav`) is played back immediately after a call is accepted (status *Connected*). If you want to play back the WAV file manually with the help of the **Play** and **Stop** buttons instead of automatically, activate the option **Start Sounds manually.**
- If you would like to play back a different WAV audio file, you can select the relevant sound file after clicking **Open .wav file**.



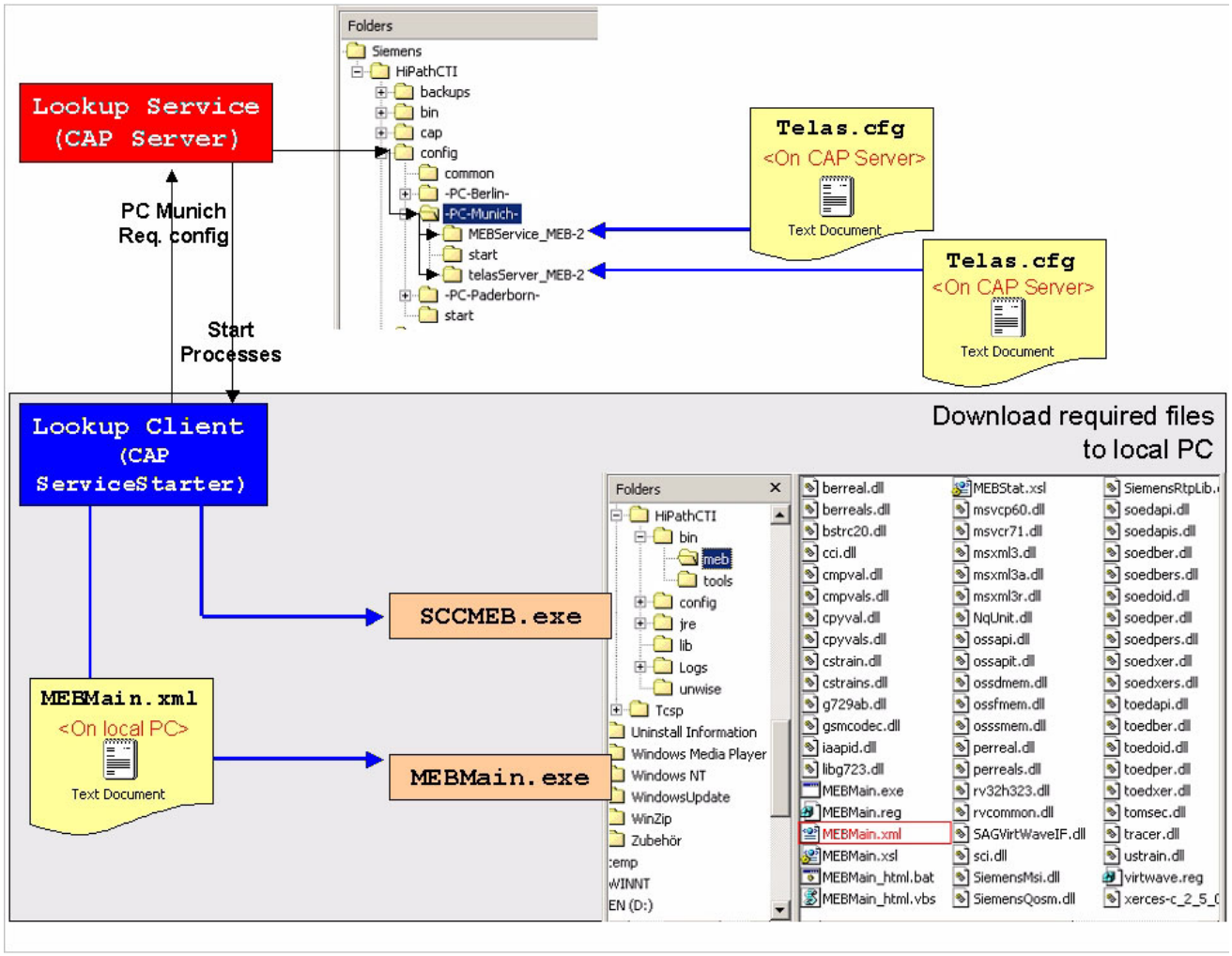
Additional options

- **Auto-Drop on Close**
  This options automatically ends all calls with the **Drop Call** function when you kill the program.
- **Auto-Answer Calls**
  This option automatically accepts all incoming calls and therefore replaces manual selection of the **Answer** function in each case.

Closing the test tool

Click the Close button in the title bar to end the MEB Application Tester tool.

9.3.7.6 MEBMain/MEBSCC Start Sequence



The MEB and the associated SCCMEB are always located on the same PC. There is no difference between the start procedures for a local and a distributed installation. With the exception of the MEB, all executable programs are located in the directory

`C:\program files\Siemens\HiPathCTI\bin.`

Only the MEB has its own directory

`C:\program files\Siemens\HiPathCTI\bin\MEB`

in a distributed environment too. During **MEBMain.exe** startup, the program takes the parameter values from `MEBMain.xml` first. The most important one is **USECAPMNGT**. If this parameter is enabled, values coming later from `telas.cfg` (CAP Management) have a higher priority than `MEBMain.xml` values. They are identified in the right column of the table in Section 9.3.7.2 with "CAP".

9.3.7.7 Trace Monitor for the MEB

Trace Monitor is an online tracing tool that displays and outputs trace messages from the MEB and Virtual Wave Driver.

The MEB and the sub-components (e.g. Wave Driver) communicate with each other by means of methods, events and messages. You can monitor and analyze the steps and messages of the MEB or Wave driver online using the Trace Monitor. The messages can also be stored or printed for further processing.

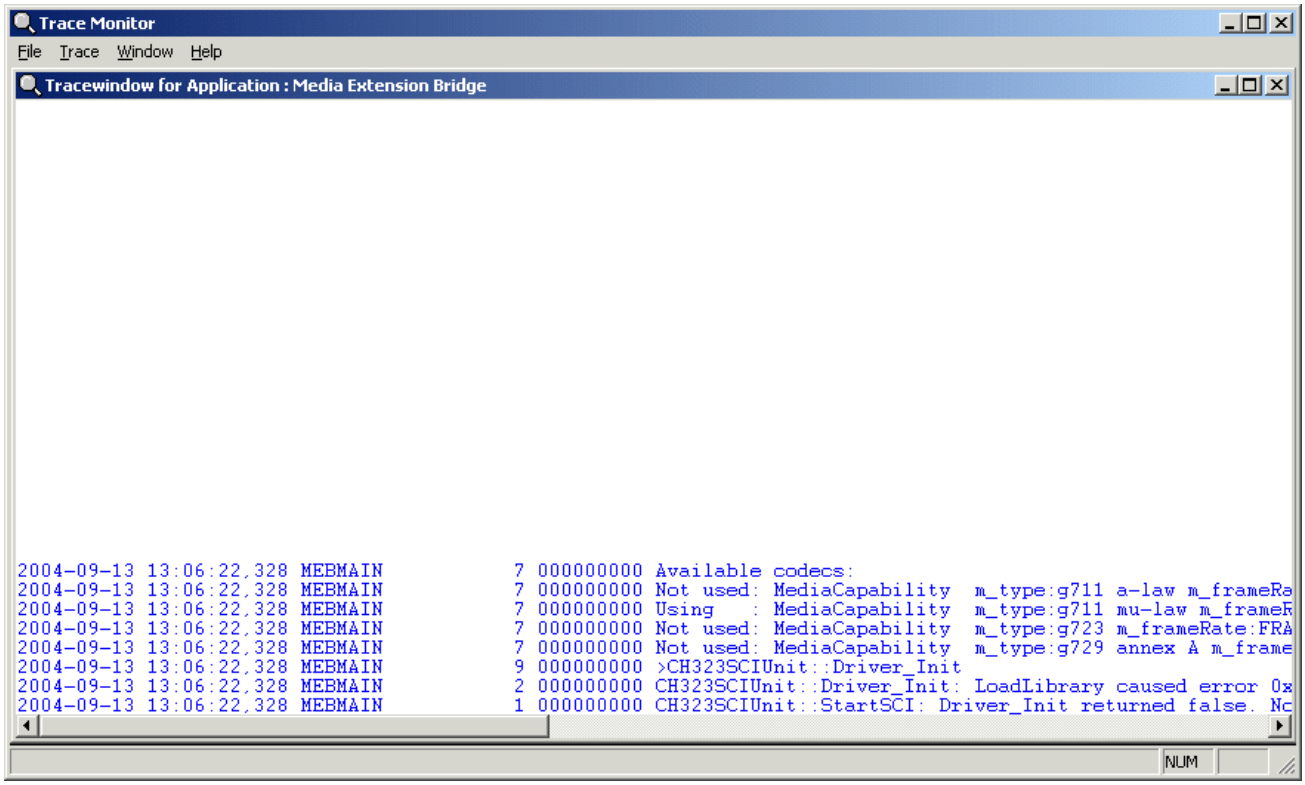
The tool is supplied with HiPath CAP 3.0 and is stored in the directory `C:\Program Files\SIEMENS\HiPath\bin\tools` when CAP 3.0 is installed. No additional installation procedures are needed because the relevant files can be called directly from this directory.

Starting the Trace Monitor

1. Change to the directory `C:\Program Files\SIEMENS\HiPathCTI\bin\tools` and start the Trace Monitor by double-clicking the file `bstrcmon.exe`.

The interpretation of the various Trace Monitor trace window contents is not covered by this documentation. Contents will be interpreted by service engineers when a problem needs to be resolved in a service scenario.
The description is this section is used to determine the steps required to navigate and control Trace Monitor and to transfer the trace contents to a file.

Displaying the Trace Monitor



Closing the Trace Monitor

To close the Trace Monitor, proceed as follows:

1. Select **File - Close**
   - or select key combination Alt + F4
   - or select **Close** from the Trace Monitor system menu.

Trace Monitor menu

The available menu titles and items are listed in the menu bar. The following menu functions are available:

Menu title	Menu item	Function
File	Printer setup	Printer for printing trace messages on a connected printer.
	Close	Closed Trace Monitor
Trace	Hexadecimal output	(Irrelevant for MEB)
	Color display	Change between color display (option enabled) and black/white display (option disabled) for trace messages.
	Show timestamp	Inserts a timestamp for each trace message when the option is enabled.
	Show new login immediately	If the option is enabled, the relevant trace window is opened when MEB is enabled. When the option is disabled, the trace window must be opened manually.
Windows	Overlapping	Trace windows are displayed overlapping.
	Tile	Trace windows are tiled.
	Cascade	Trace windows are cascaded.
	Arrange Icons	Arrangement of the minimized trace windows.
?	Info	Enables trace monitor program information.

Printer setup for Trace Monitor

A printer must be configured for printing trace window content. You can choose to print on the Windows default printer or on another installed printer. If a different printer is selected, this is entered for all applications on the PC as the Windows default printer. Printer setup can be found in the Trace Monitor under **File - Printer Setup**.

Manually opening/closing the trace window

If the **Show Window for new Application** option is not enabled in the **Trace** menu, you can open and close the trace window of the MEB **manually**. To do this, enable/disable the **MEB-Main** entry in the **Trace** menu.

Printing the contents of a trace window

You can also output a current state of a trace window on the configured printer of the trace monitor for documentation purposes:

1. Activate the System menu or, alternatively, the Context menu (right-click in the trace window) of the relevant trace window and select **Print Messages**.
2. The current content of the trace window is sent to the configured printer.

Deleting the trace window content

To delete the contents of a trace window, proceed as follows:

1. Activate the System menu or, alternatively, the Context menu (right click in the trace window) of the relevant trace window and select **Delete window contents**.
2. The content is deleted, the window is empty.

Freezing the contents of a trace window

If the current state of the trace window display is to be frozen so as to print it at a later stage for example, then proceed as follows:

1. Activate the System menu or, alternatively, the Context menu (right-click in the trace window) of the relevant trace window and select **Stop Window Scrolling**. The contents of the window are frozen and new trace messages are not displayed.
2. To clear this option, select **Freeze window contents** again. New trace messages are displayed in Windows again.

Exporting trace window content

The trace window can hold up to 500 entries. Once this capacity has been reached, the oldest entry in the trace window is deleted each time a new entry is made. You can record the current state of the trace window in an export file to document a situation from the trace window:

> Activate the System menu or, alternatively, the Context menu (right-click in the trace window) of the relevant trace window and select **Write Messages to File**.

  A message appears showing the path/file name for the trace window export file. Confirm this with OK.

The default **target directory** for export files is the Windows shell user directory:

`C:\Documents and Settings\[Windows Users]\Personal Files\[Application ID]\[Trace file name]`

- The `[application ID]` for MEB is: **MEBMAIN**
- The naming convention for the `[trace file name]` is as follows:

  `MEBMAIN`*<time>*`.trc`

  where the time is stored in *YYYYMMDDhhmm* format.

9.3.8 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".

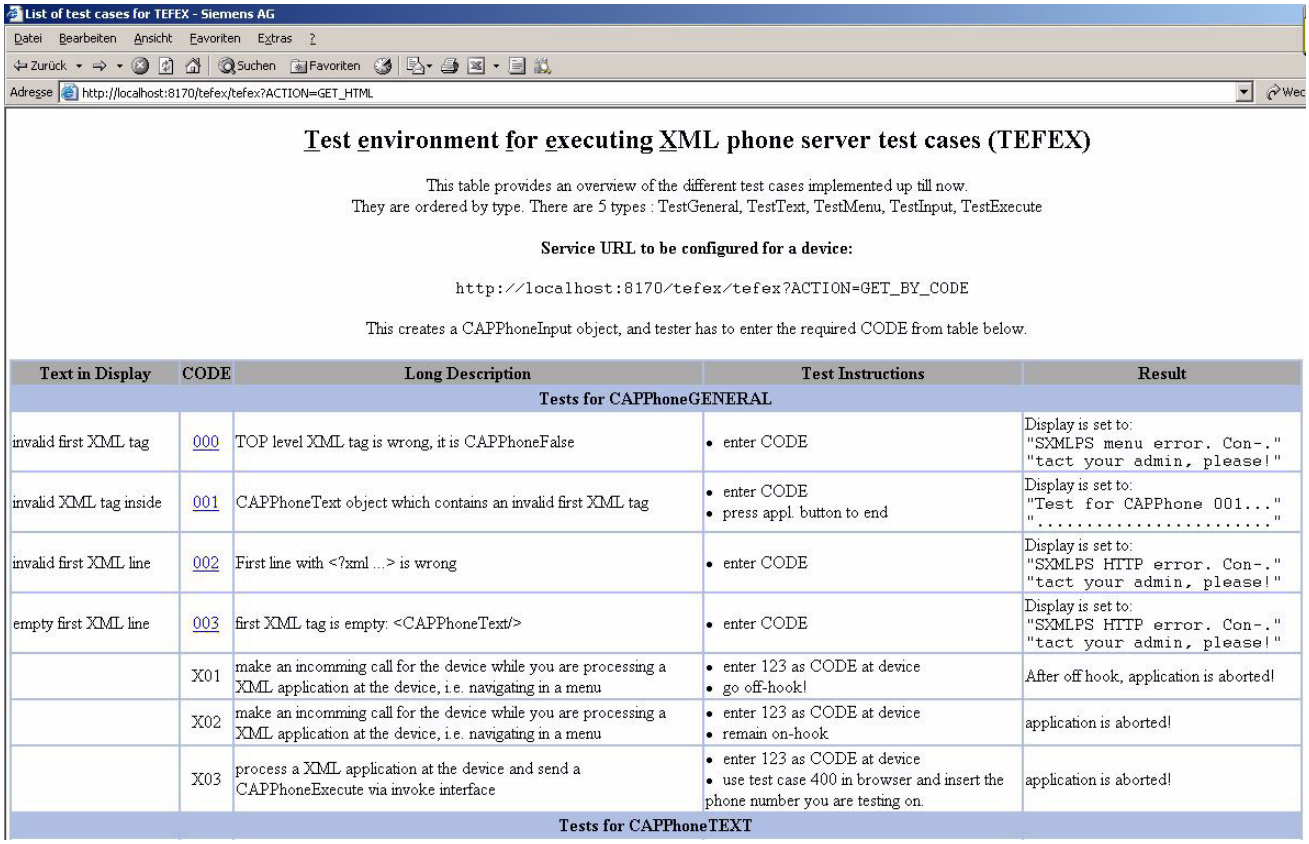
Now you can test the configuration of the XML Phone Service.

9.3.8.1 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:8170/tefex/tefex?ACTION=GET_HTML**".



List of test cases for TEFEX - Siemens AG

Datei Bearbeiten Ansicht Favoriten Extras ?

Zurück Suchen Favoriten

Adresse http://localhost:8170/tefex/tefex?ACTION=GET_HTML

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:8170/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 at the device, i.e. navigating in a menu	• enter 123 as CODE at device • remain on-hook	application is aborted!
	X03	process a XML application at the device and send a CAPPhoneExecute via invoke interface	• enter 123 as CODE at device • use test case 400 in browser and insert the phone number you are testing on.	application is aborted!
Tests for CAPPhoneTEXT				

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:

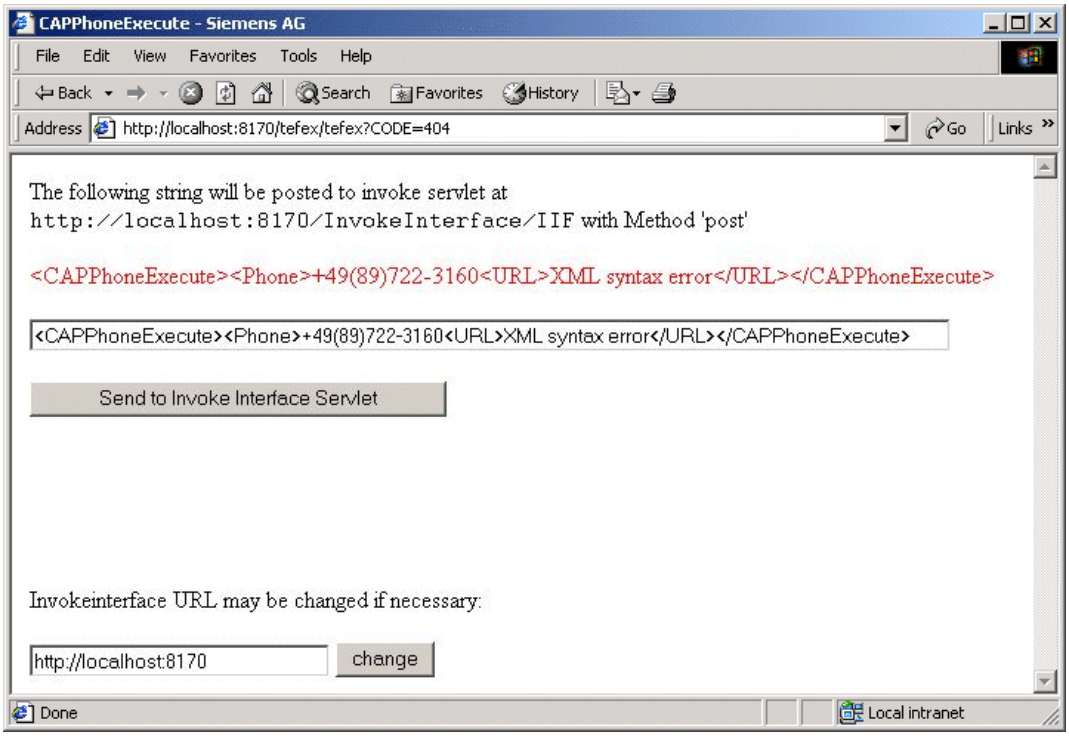
- Test for CAPPhone Text:
- Test for CAPPhone Menu:
- Test for CAPPhone Input:
- Test for CAPPhone Exec: (although this is offered here, this test is **not supported** when operating from a telephone)

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 HiPath CTI components are saved in different subdirectories of the *<InstDir>* installation directory.

When installing HiPath 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\
        global.cfg
        http-server.zip
        proc.cfg
        ROOT.war
        TelasWeb.cfg
    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 HiPath 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 HiPath 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 4.3, "Installing the HiPath CAP Service Starter").

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.

HiPath CAP Management creates this directory during installation. It is used by all HiPath CTI components.

A.1.4 Files for the user interface

All HTML pages belonging to the HiPath CAP Management and Call Control Service are saved in the `<InstDir>\WebSpace`.

Every HiPath 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; HiPath 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

HiPath 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 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 HiPath CAP Management homepage
CFG	Path to the directory containing the configuration files

The following variables are used to control logging.

log.class	**= com.siemens.log.ClientLogger**
log.serverUrl	**= lookup://LogServer**
log.level	**= 3**
tomcat.log.level	**= -1**

If necessary, general logging can be modified here; The permitted values for the logging level are:

DebugTrace	**5**
Trace	**4**
Message	**3**
Warning	**2**
Error	**1**
Fatal	**0**
OFF	**-1**

The `tomcat.log.level` file 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 SimplyPhone for Web 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.2.2 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_SSL_AUTH = "false" ?>
The secure connection to CAP Management is set up here during the login session (true/false).

<?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.2.3 TelasWeb.cfg

The `TelasWeb.cfg` file is extremely important for configuring the entire HiPath 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.

This entry is only required when the domain name of the installation host cannot be determined during the installation of HiPath 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 HiPath 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.siemens.de`
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.2.4 startNT.cfg

The `StartNT.cfg` file is used by the Start Service (`jsstart.exe`) to start the entire HiPath 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 HiPath 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.2.5 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.siemens.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.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.Usergroups,SYS-
DB.MAP.Scc,SYSDB.MAP.SCCProxy,SYSDB.MAP.Devices, SYSDB.MAP.Snrs, SYS-
DB.MAP.Licenses, SYSDB.MAP.Businessgroup, SYSDB.MAP.Urls, SYS-
DB.MAP.Ca, SYSDB.MAP.Xmlphoneservice, SYSDB.MAP.MEBService
```
Preparation for connecting external LDAP servers instead of internal CAP LDAP servers, SLAPD, for managing all data.

`ProgramMode = CAP`
HiPath 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.2.6 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 HiPath CAP Management user interface. Every entry has the following structure: "<directory name> | <selection name>,". The directory *<Inst-Dir>*`\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, 1|CSTA I,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.2.7 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 HiPath 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.2.8 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 "Siemens HiPath 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:/Program Files/Siemens/HiPathCTI/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.2.9 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:/Program Files/Siemens/HiPathCTI/data/TelasWeb/Journals`

A.2.10 Diagnose.cfg

This file contains settings for the diagnostic servlet.

A.2.11 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.2.12 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.

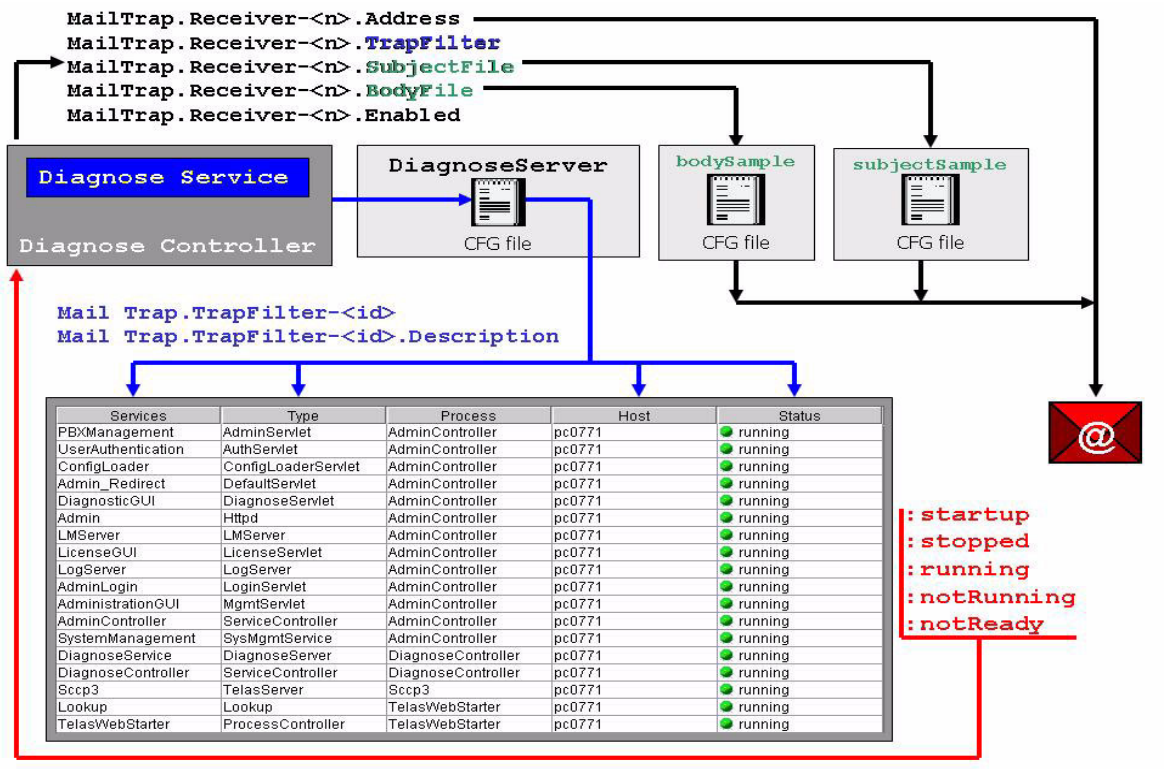
`#MailTrap.Receiver-<n>.BodyFile = <bodyTemplateFile>`
The name of the associated "Body Template File" is defined here. The "**`subjectSample.cfg`**" template file is located in the directory of the file "`bodySample. cfg`". Please note that file names are case-sensitive.

`#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|notRun-
ning
MailTrap.TrapFilter-0.Description = 0 = location/Type/Ser-
vice: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
```



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.2.13 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.

> ⚠ All files are managed via the HiPath CAP Management user interface. All CAP data can be destroyed by modifying one of these files with a text editor.

A.2.14 Configuration data for MEB

The MEB configuration parameters are stored in an ASCII configuration file that can be opened directly with an editor. CAP 3.0 Management does not need to be enabled.

Parameters should never be changed directly in this file but always in CAP Management.

The name of the configuration file is `telasXXX.cfg`, where xxx stands for the configured service name. This file is located in the CAP 3.0 default configuration folder.

You can open the file using the Explorer by double-clicking (Editor), for example to print out the parameter settings for a particular configuration.

The directories in detail:

Parameters in the file	**Meaning/Value**	**Corresp. field in the CAP Management MEB configuration**
`MEBIP`	IP address MEB	MEB IP address
`callNumberMEB`	MEB's own call number	MEB call number
`NumChannels`	Maximum number of channels (as licensed)	Max. number of channels
`UseLengthCheck`	Length check option – 0: Off – 1: On	Use length check
`CallNumberLength`	Minimum length of call number for length check	Length of the call number
`UseList`	Call number list option – 0: Off – 1: On	Use call number list
`CallNumberList`	Call number list, entries separated by a semicolon, ranges indicated with a minus sign	Call number list
`MediaGatewayIP`	Enter the IP address of the HG3570 board to which the MEB is connected.	Media gateway
`DLSIP`	IP address of the DLS servers	DLS IP address
`H225SignalingPort`	H.225 port number	H225 signaling port

A.2.14.1 Files for MEB

The following files for MEB are contained in the `C:\Program Files\SIEMENS\HiPathC-TI\bin\meb` folder after installation and configuration of the MEB:

File	Meaning
berreal.dll	Function library for MEB.
berreals.dll	Function library for MEB.
bstrc20.dll	Function library for trace monitor.
cmpval.dll	Function library for MEB.
cmpvals.dll	Function library for MEB.
cpyval.dll	Function library for MEB.
cpyvals.dll	Function library for MEB.
cstrain.dll	Function library for MEB.
cstrains.dll	Function library for MEB.
cci.dll	Function library for SCI.
g729ab.dll	Function library for SCI.
iaapid.dll	Function library for MEB.
libg723.dll	Function library for SCI.
MEBMain.exe	Program file of MEB.
MEBMain.reg	Registry entries for MEB.
MEBMain.xml	Additional configuration file for MEB.
MEBMain.xsl	Additional configuration file for MEB.
MEBMain_html.bat	Batch file for calling up the information script for MEB.
MEBMain_html.vbs	Version information script for MEB.
MEBStat.xsl	Additional configuration file for MEB statistics.
msvcp60.dll	Function library for MEB
msvcr71.dll	Function library for MEB
msxml3.dll	Function library for MEB
msxml3a.dll	Function library for MEB
msxml3r.dll	Function library for MEB
NqUnit.dll	Function library for CorNet NQ/IP support.
op1_16.avi	AVI sound file for the Tool MEB Application Tester.
ossapi.dll	Function library for CorNet NQ/IP support.

File	Meaning
ossapit.dll	Function library for CorNet NQ/IP support.
ossdmem.dll	Function library for CorNet NQ/IP support.
ossfmem.dll	Function library for CorNet NQ/IP support.
osssmem.dll	Function library for CorNet NQ/IP support.
perreal.dll	Function library for MEB.
perreals.dll	Function library for MEB.
rv32h323.dll	Function library for SCI.
rvasn1.dll	Function library for SCI
rvcommon.dll	Function library for SCI.
SAGVirtWaveIF.dll	Function library for Wave Driver Interface.
soedapi.dll	Function library for MEB.
soedapis.dll	Function library for MEB.
soedber.dll	Function library for MEB.
soedbers.dll	Function library for MEB.
soedoid.dll	Function library for MEB.
soedper.dll	Function library for MEB.
soedpers.dll	Function library for MEB.
soedxer.dll	Function library for MEB.
soedxers.dll	Function library for MEB.
toedapi.dll	Function library for MEB.
toedber.dll	Function library for MEB.
toedoid.dll	Function library for MEB.
toedper.dll	Function library for MEB.
toedxer.dll	Function library for MEB.
tomsec.dll	Function library for SCI.
Traces.dll	Function library for SCI.
ustrain.dll	Function library for MEB.
virtwave.reg	Registry entries for WAV drivers; these are entered on every MEB start.
waveTest.wav	WAV sound file for the Tool MEB Application Tester.
xerces-c_2_5_0.dll	Function library for XML support.

A.2.14.2 Files for the Siemens Virtual Wave Driver

The following are available after installation in the `C:\winnt\system32` (Windows System directory) folder:

File	Meaning
sagvirtwave.dll	Function library of the Wave driver.
virtwave.reg	Registry entries for Wave driver interface.

A.2.14.3 Files for CAP 3.0 Management and SCCMEB

After MEB/SCC has been installed/configured, the following files for SCCMEB are contained in the

`C:\Program Files\SIEMENS\HiPathCTI\bin\meb`

folder:

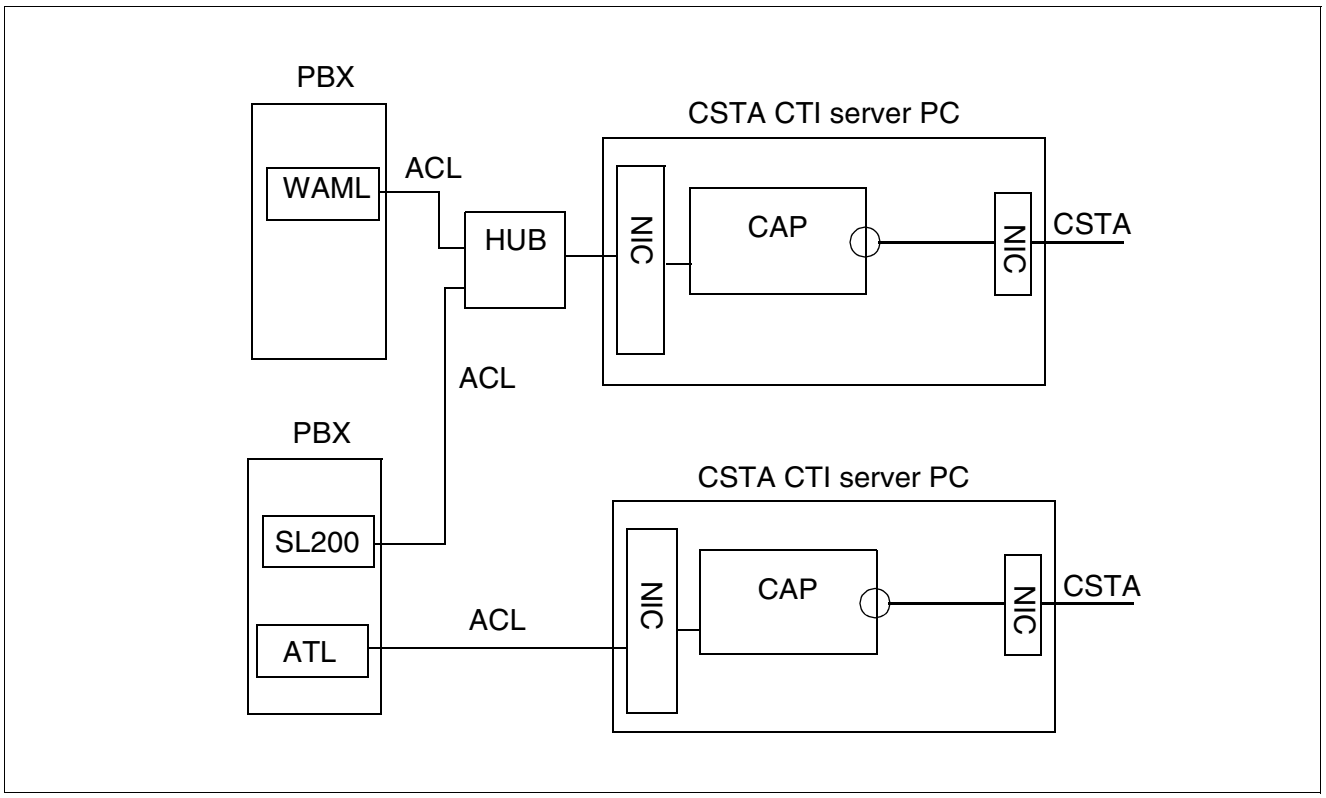
File	Meaning
imgmt.dll	Function library for access to CAP Management.
SccMEB.exe	Program file for SCCMEB.

B Connecting HiPath 4000/Hicom 300 with a Server PC

B.1 Server PC connectivity options

HiPath 4000/Hicom 300 features integrated Ethernet server bus ports. This means you can connect the HiPath 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 Siemens HiPath 4000/Hicom 300:



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 unscreened twisted-pair cable to the internal Hicom Ethernet LAN serves as the physical interface between the HiPath 4000/Hicom 300 and HiPath CP. The internal ("Atlantic") LAN provides high data bandwidth and is therefore ideal for data communication between the HiPath 4000/Hicom 300 processors and HiPath CAP. The internal Hicom Ethernet LAN can be accessed directly over the ports on the rear panel of the HiPath 4000/Hicom 300.

If there are multiple HiPath 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 Hicom 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)

HiPath CAP: 192.0.2.23 - 192.0.2.29 (default: 192.0.2.25)

If there are multiple HiPath 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/Hicom 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 Hicom 300 and HiPath 4000).

These LAN boards have freely configurable IP addresses and can be used to access the Atlantic LAN.

You cannot configure a WAML board at the same time as an SL200 board.

B.2 Configuring the HiPath 4000/Hicom 300 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.

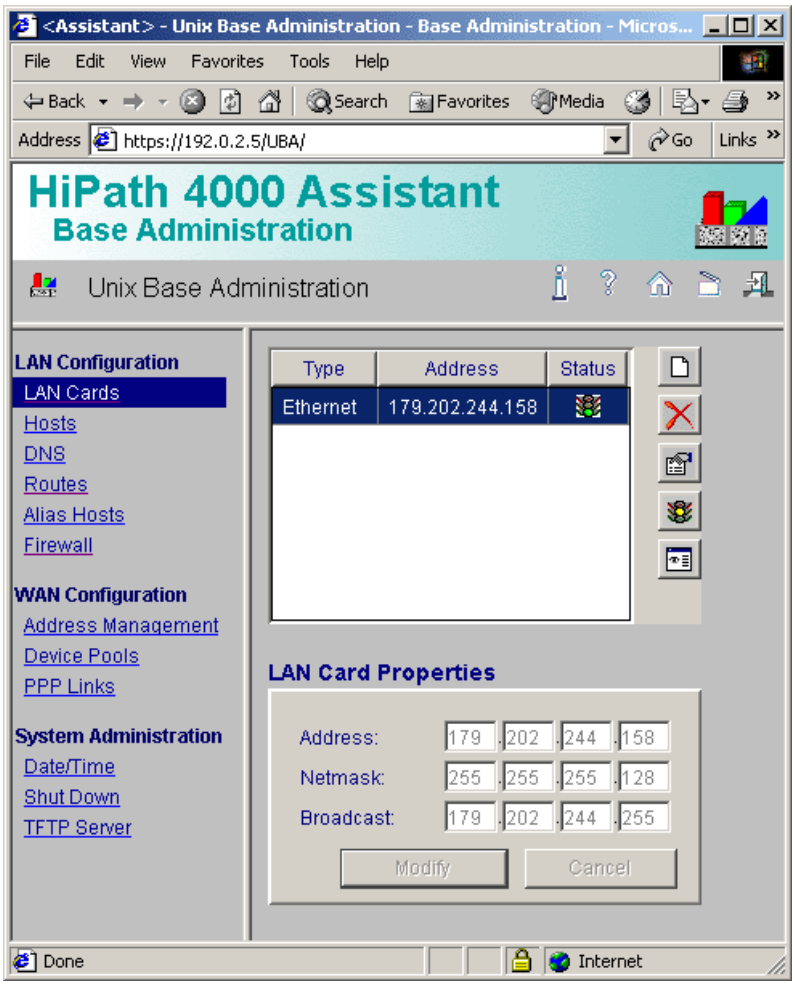
Use the UnixWare service tool 'Unix Base Administrator' (UBA) to configure the SL200 card for use with CA4000. The UBA service tool can be found under LaunchPad in the 'Base Administration' folder in HiPath 4000 Assistant.

Once the LAN settings for SL200 have been properly configured in the UBA under 'LAN Cards' and 'Routes', proceed with the section 'Firewall settings'.

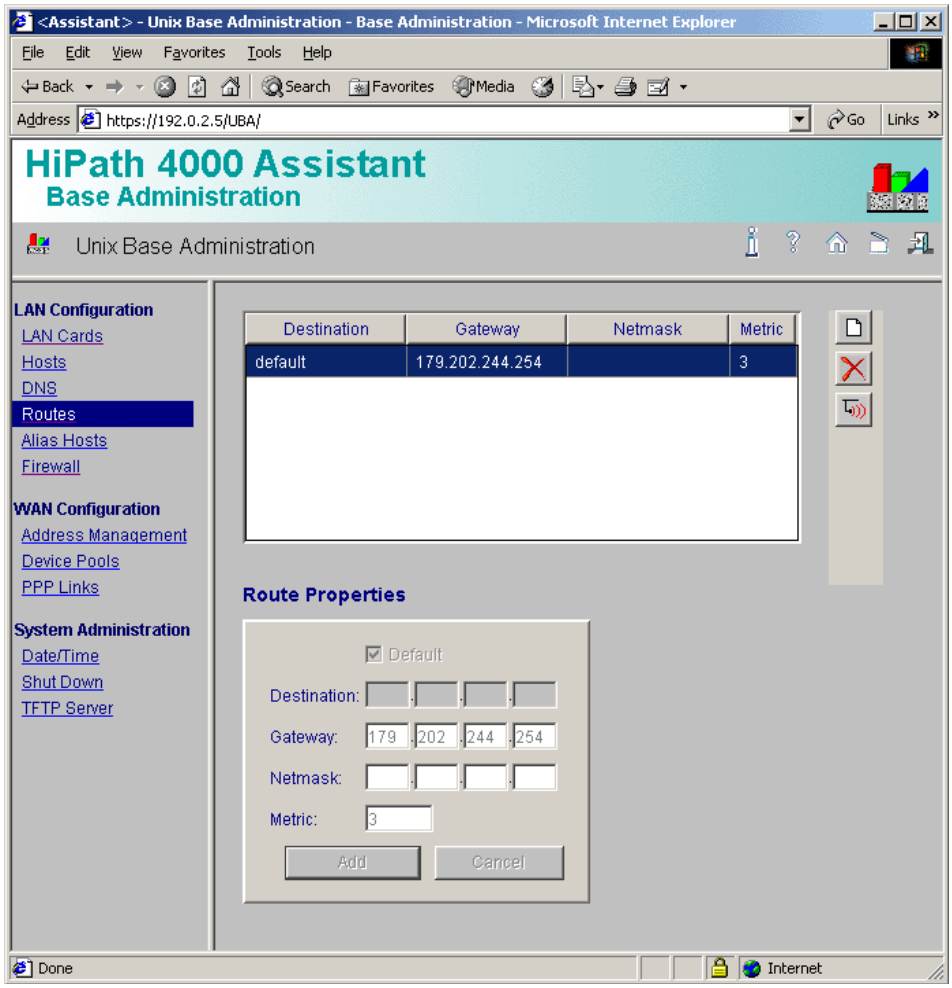
Configuring with HiPath 4000 Assistant and the UBA

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'.



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.

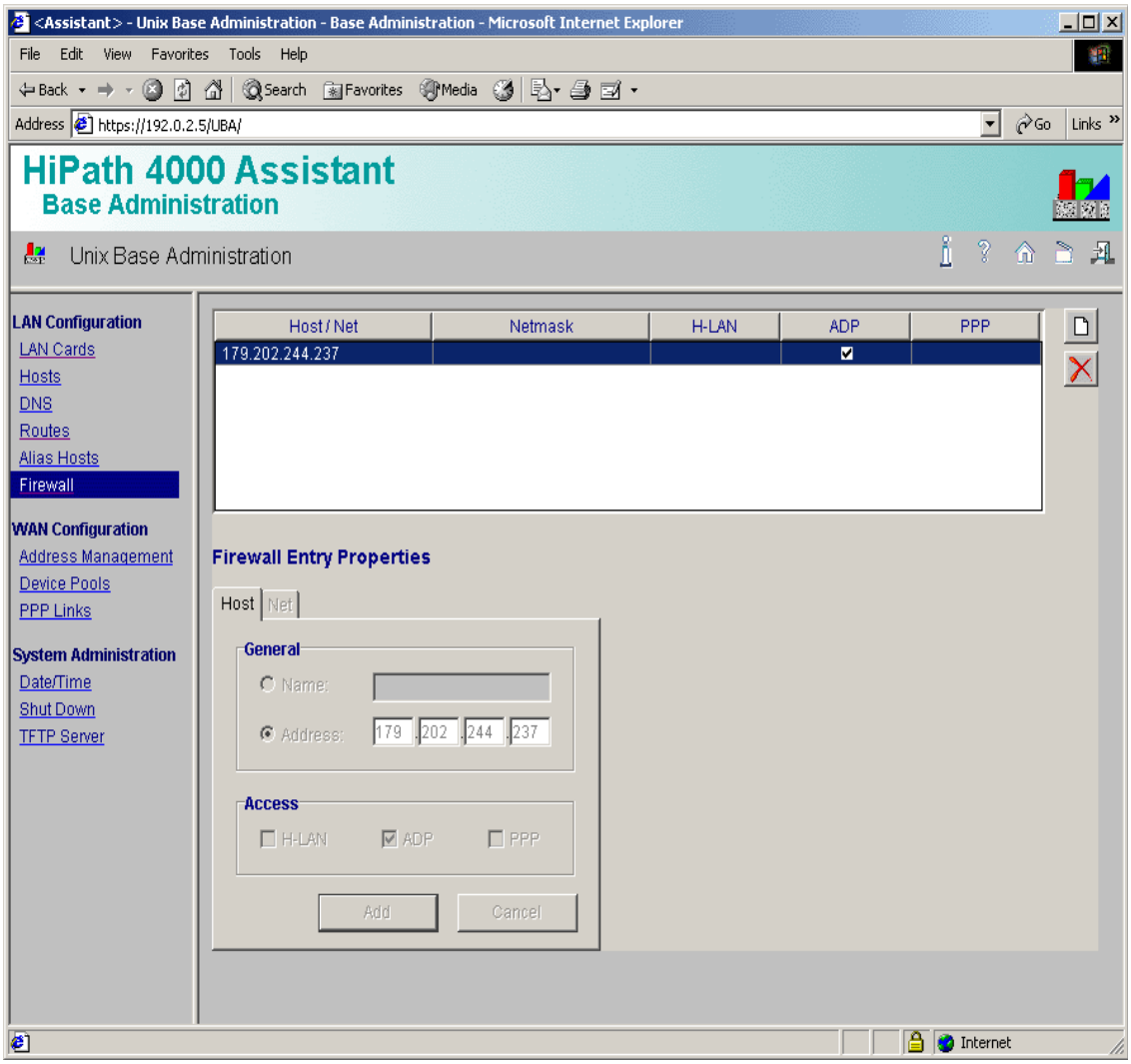


Firewall settings

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.



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/Hicom 300

The procedure includes the attachment of the connection cable and the execution of a ping on the HiPath 4000/Hicom 300. 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/ Hicom 300.
3. Send a ping to the IP address of the HiPath 4000/Hicom 300. 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/Hicom 300. 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 HiPath CAP and HiPath 4000/Hicom 300 are specially configured, that is, certain specific parameters must be set.

HiPath/Hicom 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/Hicom.

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 HiPath CAP configuration.

In particular, these are:

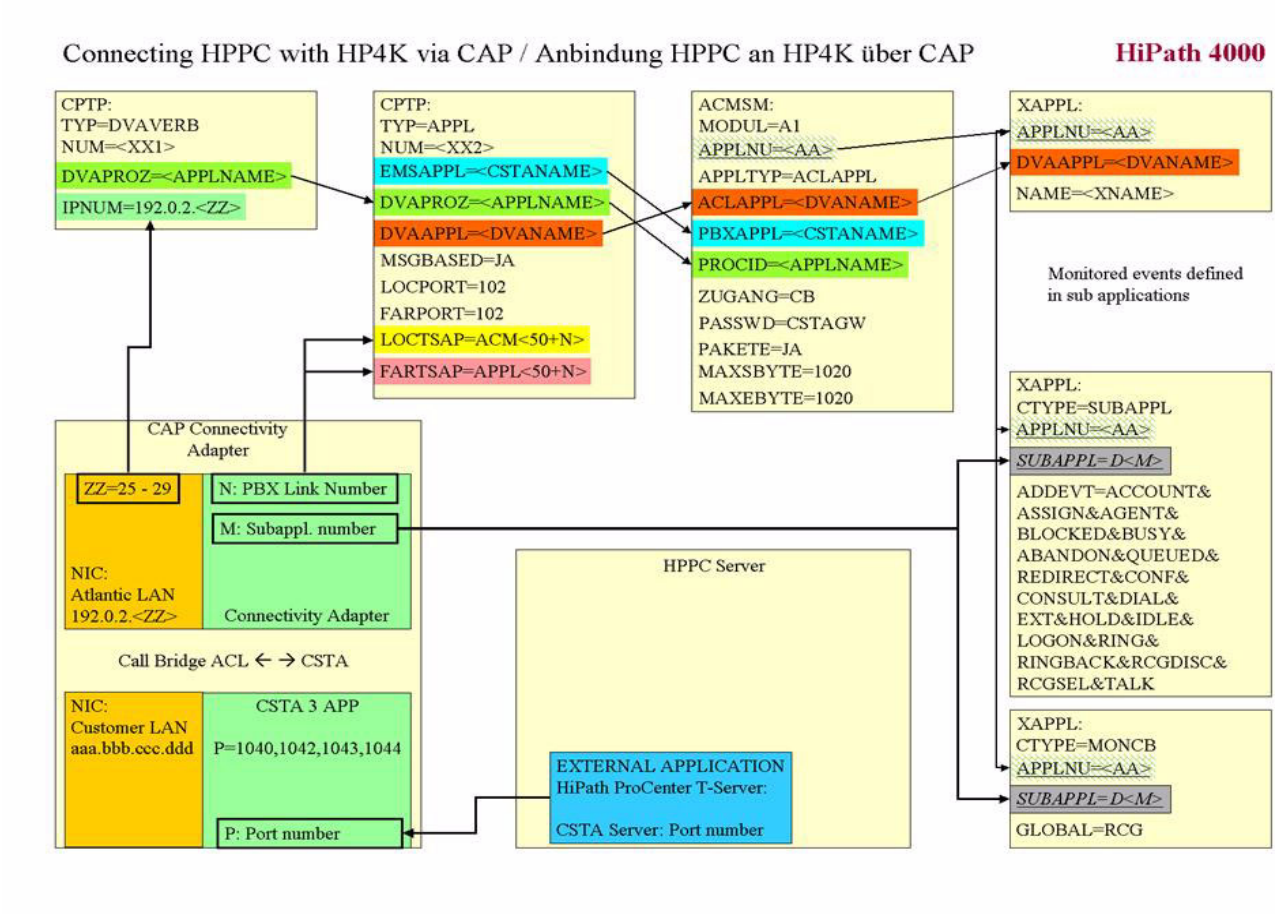
Password (ACMSM)

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
CAP Connectivity
Adapter
ZZ=25 - 29
N: PBX Link Number
M: Subappl. number
NIC:
Atlantic LAN
192.0.2.<ZZ>
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
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

B.3.2 Hicom 300/HiPath4000 configuration batch for the CA

The configuration batch for HiPath 4000/Hicom 300 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/Hicom 300 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

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,ACCOUNT&AGASSIGN&Agent&ABANDON&QUEUED;
CHANGE-XAPPL:SUBAPPL,55,D25,REDIRECT&LOGON&RCGDISC&RCGSEL&DIGDIALD;
CHANGE-XAPPL:SUBAPPL,55,D25,TTONGEN;
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 Hicom 300 batch for CA300

```
ADD-CPTP:DPCON,55,"CAPSVR1","<IP-CA300-PC>";

ADD-CPTP:APPL,55,"CAP1","CAPSVR1","CAPAPPL1",YES,102,102,"ACM55","APPL55";

ADD-XAPPL:55,CB,A1,"CAPAPPL1","APPLICATION_55";

CHANGE-XAPPL:SUBAPPL,55,D25,ACCOUNT&AGASSIGN&AGENT&BLOCKED&BUSY;

CHANGE-XAPPL:SUBAPPL,55,D25,ABANDON&QUEUED&REDIRECT&CONF&CONSULT;

CHANGE-XAPPL:SUBAPPL,55,D25,DIAL&EXT&HOLD&IDLE&LOGON;

CHANGE-XAPPL:SUBAPPL,55,D25,RING&RINGBACK&RCGDISC&RCGSEL&TALK;

CHANGE-XAPPL:MONCB,55,D25,RCG,;

/*

ADD-ACMSM:A1,55,ACLAP-
PL,"CAPAPPL1","CAP1","CAPSVR1",CB,"CSTAGW",Y,1020,1020;

/*

/* ACT-APC:"ACM",SWU,BP;

/*

/* 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.3.2.3 Hicom configuration batch – S_0 connection for Telas Server 3.1

```
ADD-BCSM:A1,EC,SW,86,S0D,"S0D";

ADD-BCSM:A1,EC,HW,N,86,"Q2120-X",,"",,"",,"",,"";

ADD-LCS0:A1,KONF,13,WAHL,DVA,216,64000TRS;

ADD-LCS0:A1,KONF,14,WAHL,DVA,220,64000TRS;

ADD-CPS0:A1,DVAVERB,5,"TELAS","216","370";

ADD-CPS0:A1,APPL,40,"DGV","TELAS","CBTD","CBTDS","CBTDR";


;ADD-CPS0:A1,APPL,41,"TDD0","TELAS","CBTT0","CBTT0S","CBTT0R";


;ADD-CPS0:A1,APPL,42,"TDD1","TELAS","CBTT1","CBTT1S","CBTT1R";


;ADD-CPS0:A1,APPL,43,"GUE","TELAS","CBTG","CBTGS","CBTGR";


ADD-SBCSU:216,FPP,DIR,1-1-79-
0,S0PP,1,1,1,1,1,1,0,0,N,0,Y,0,,SBQ9311,Y,Y,0,,,N,N,,;


ADD-SBCSU:217,MSN,216,,1,1,1,1,1,1,0,N,0,Y,0,,Y,N,N;


ADD-DAPPL:40,"DGV","CBTD","TELAS",DGV;


CHANGE-DAPPL:40,,,,EIN,DGV;
```

B.3.2.4 Hicom configuration batch – LAN connection for Telas Server 3.1

```
ADD-LANC:1,1,91,GLOBAL,155,WESTERN,ATL-
LAN&EXTLAN1,NONE,,,,,,,,,PROXY,PROXY;


ADD-LANC:1,1,91,NETWORK,EXTLAN1,195.2.109.41,255.255.255.0,;


ADD-LANC:1,1,91,IPROUTE,195.2.109.0,NET,255.255.255.0, 195.2.109.254;


ADD-DAPPL:11,"DGV","TELAS","CBTD",DGV;

CHANGE-DAPPL:11,,,,NW ,DGV ,1;


ADD-CPTP:DPCON,111,"TELAS","195.2.109.43";


ADD-CPTP:APPL,11,"DGV","TELAS","CBTD",YES,102,5000,"CBTDS","CBTDR";
```

B.3.2.5 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=827486,TD07=NAME;
```

Use the AMO ZIEL to configure a HiPath 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 Configuring HiPath 4000 for the MEB connection

B.4.1 Explanation of terms

MEB - Media Extension Bridge
The MEB is part of CAP 3.0 Management. It is implemented over IP between MEB and HiPath 4000. IP Trunking Version 2.0 is used for this in HiPath 4000 V2.0. This means that only STMI2 boards can be used. These are Q2316-X with 45 available B channels or Q2316-X10 with 90 available B channels.

B.4.2 Configuring the IP link in HiPath 4000

Call numbers, slots and IP addresses must be customized to suit the environment. Items marked in bold are variable and must be customized for installation.

B.4.2.1 Adding and configuring the STMI board

Note:
Please insert the board following the AMO STMIB as otherwise frequent board restarts will delay the configuration.

```
ADD-BCSU:TYPE=PER,LTG=1,LTU=1,SLOT=91,PARTNO="Q2316-X",FCTID=2,LW-
VAR="0",HWYBDL=A;
```

/*Note the board label for the part number

```
ADD-STMIB:MTYPE=STMI2IGW,LTU=1,SLOT=91,CUSIP=198.6.116.157,CUSPN=8000,

SNETMASK=255.255.255.0;

CHANGE-STMIB:MTYPE=STMI2IGW,LTU=1,SLOT=91,TYPE=IFDATA,DGWIP=198.6.116.254;

CHANGE-STMIB:MTYPE=STMI2IGW,LTU=1,SLOT=91,TYPE=GWDA-
TA,GWID1="MEB",GWID2="1";

CHANGE-STMIB:MTYPE=STMI2IGW,LTU=1,SLOT=91,TYPE=LEGKDATA,GWNO=1,GWD-
IRNO=2100;
```

If the STMI2 is already inserted, you must now restart it.

```
RESTART-BSSU:ADDRTYPE=PEN,LTG=1,LTU=1,SLOT=91;
```

B.4.2.2 Configuring tie trunks and TSC connection numbers

```
ADD-WABE:CD=2100,DAR=TIE;

ADD-WABE:CD=2200,DAR=TIE;


ADD-WABE:CD=2101,DAR=STN;
```

B.4.2.3 Configuring trunk groups for the IP route

```
ADD-BUEND:TGRP=20,NAME="MEB",NO=30;
```

B.4.2.4 Tie trunk to MEB

(The COT and COP standards are downloaded from the HD in this case for a tie connection to ECMAV2.)

```
COPY-COT:TYPE=COT,COTOLD=14,COTNEW=29,SOURCE=HD;

COPY-COP:TYPE=COP,COPOLD=14,COPNEW=31,SOURCE=HD;


ADD-TDCSU:OPT=NEW,PEN=1-1-91-0,COTNO=29,COPNO=31,DPLN=0,

ITR=0,COS=1,LCOSV=1,LCOSD=1,CCT="IGW-MEB",DESTNO=0,PROTVAR=ECMAV2,

SEGMENT=8,ISDNIP=00,ISDNNP=0,TRACOUNT=15,NNO=1-2-299,COTX=29,

FWDX=10,CLASSMRK=EC&G711&G729OPT,TGRP=20,SRCHMODE=DSC,INS=Y,

DEV=HG3550IP,BCHAN=1&&30,BCNEG=N,BCGR=1,LWPAR=0,

LWPP=0,LWLT=0,LWPS=0,LWR1=0,LWR2=0,DMCERL=N;
```

B.4.2.5 Routing for the TSC connection

```
ADD-RICHT:MODE=LRTENEW,LRTE=299,LSVC=ALL,NAME="MEB-1",

TGRP=20,DNNO=1-2-299;


ADD-LODR:ODR=29,CMD=ECHO,FIELD=1;

ADD-LODR:ODR=29,INFO="IP-IGW TSC",CMD=END;


ADD-LDAT:LROUTE=299,LSVC=ALL,LVAL=1,TGRP=20,ODR=29,LAUTH=1;

ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="2100",LROUTE=299,LAUTH=1;
```

B.4.2.6 Configuring the gatekeeper

Attention:
Please check the following settings in the AMO ZANDE: branch ALLDATA, GATEKPR=YES

```
ADD-GKREG:GWNO=1,GWATTR=INTGW&REGGW&HG3550V2,{SECTORNO=0},
{CLUSTNO=1},DIPLNUM=0,DPLN=0,LAUTH=1;

ADD-GKREG:GWNO=2,GWATTR=EXTGW,GWIPADDR=198.6.116.242,
GWDIRNO=2101,{SECTORNO=0},{CLUSTNO=1},DIPLNUM=0,DPLN=0,LAUTH=1;
```

The IP address (GWIPADDR) for the gateway number = 2 must match the IP address of the MEB server.

B.4.2.7 Routing for the tie trunk route to the MEB

(An open network with node access code is used here.)

```
ADD-RICHT:MODE=LRTENEW,LRTE=220,LSVC=ALL,
NAME="MEB QUER",TGRP=20,DNNO=1-2-299;

ADD-LODR:ODR=32,CMD=NPI,NPI=UNKNOWN,TON=UNKNOWN;
ADD-LODR:ODR=32,CMD=ECHO,FIELD=1;
ADD-LODR:ODR=32,CMD=ECHO,FIELD=2;
ADD-LODR:ODR=32,CMD=END;
ADD-LODR:ODR=32,INFO="IP-IGW MEB";

ADD-LDAT:LROUTE=220,LSVC=ALL,LVAL=1,TGRP=20,ODR=32,
LAUTH=1,GW1=2-0;
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="2200"-
"X",DPLN=0,LROUTE=220,LAUTH=1;
```

B.4.2.8 Saving changes

Save changes to the hard disk.

```
EX-UPDAT:BP,ALL;
```

B.4.2.9 Configuration query

The command `DIS-GKREG:;` should now show that the GW1 has registered itself and that GW2 contains an IP address. This is the IP address of the computer on which the MEB should run.

```
+-------------------------------------------------------------------------+
| GWNO      1                          GWATTR   INTGW    REGGW    HG3550V2  |
| GWIPADDR  198.6.116.157              GWDIRNO  2100                       |
| DIPLNUM   0          DPLN 0                                             |
| LAUTH     1                                                             |
| GATEWAY REGISTERED: YES   ←                                            |
| IP GATEWAY IS CONFIGURED   BY  GKREG                                    |
| INFO:                                                                   |
+-------------------------------------------------------------------------+
| GWNO      2                          GWATTR   EXTGW    HG3550V2          |
| GWIPADDR  198.6.116.242              GWDIRNO  2101                       |
| DIPLNUM   0          DPLN 0                                             |
| LAUTH     1                                                             |
| GATEWAY REGISTERED: NO                                                  |
| IP GATEWAY IS CONFIGURED   BY  GKREG                                    |
| INFO:                                                                   |
+-------------------------------------------------------------------------+
```

B.4.3 Setting the STMI voice CODEC

STMI-specific WBM (Web-Based Management): this tool is activated via HiPath4000 Assistant. It can be found under "**Expert Mode | HG3550 V2 Manager**".

1. Click the "Refresh BG List" button on the following page.
2. Connect to the appropriate STMI.
3. Open the padlock and scroll to "Explorer", then "Voice Gateway".
4. Now right-click the CODEC PARAMETER in the menu that appears and select "edit parameters". The parameters can now be edited.
5. Set the priority of codec G.711 µ-law to "1" and codec G.729AB to "4".
6. Confirm the change with "Apply Changes", press the diskette to save and reboot the card with the "Reset" button. This takes up to 10 minutes.
7. The STMI connection is interrupted by closing the padlock and selecting "Logoff" from the menu.

B.4.4 Enhancements

B.4.4.1 AMO GKREG

As the AMO GKREG was defective in SR06 Rel. 00 and Rel. 02, it is only now saved and then transferred by file transfer.

Necessary for SR06 Rel. 00

```
STA-COPY:":PDS:APSU/BGDAT00",":PAS:SICHERUNG/BGDAT00";
```

Necessary for both SR06 Rel. 00 and Rel. 02

```
STA-COPY:":PDS:APSN/S/GKREG/C",":PAS:SICHERUNG/GKREG/C";

STA-COPY:":PDS:APSN/S/GKREG/D",":PAS:SICHERUNG/GKREG/D";

STA-COPY:":PDS:APSN/S/GKREG/E",":PAS:SICHERUNG/GKREG/E";
```

B.4.4.2 Info on the protocol

IP trunking only works in connection with ECMAV2. This applies to all systems. If a different PVCD was loaded in the AMO PRODE like in the USA, the protocol must be implemented by hand.

B.4.5 Implementing the ECMAV2 protocol by hand

This applies to all systems for which IP trunking should be installed. This feature requires the ECMAV2 protocol. If a different PVCD was loaded in the AMO PRODE like in the USA, the protocol must be implemented by hand.

```
DISPLAY-PRODE:SRC=HD,KIND=PDSHORT;
```

```
+------+---------------------------+-------+---------------+
| PDNR | PDSTRING                  | IDENT | VERSION       |
+------+---------------------------+-------+---------------+
|  31  | ETSI QSIG Third ed. SS    | H/08  | B0-EL0.20.001 |
+------+---------------------------+-------+---------------+
```

The ECMAV2 protocol is listed as "ETSI QSIG Third ed. SS" on the hard disk.

```
DISPLAY-PRODE:SRC=DB,KIND=VARTAB;
```

```
+---------------------+--------+--------+---------------------------+
| PROTVAR             |        | PDNAME | PDSTRING                  |
+---------------------+--------+--------+---------------------------+
| PSS1V2              | PDNORM |  PD06  | ISO QSIG Second ed. SS    |
|                     | PDA1   |        |                           |
|                     | PDA2   |        |                           |
+---------------------+--------+--------+---------------------------+
```

The query is used to find unnecessary protocols in the database. PD06 was used here. Individual appearances may differ if PSSIV2 is needed.

```
COPY-PRODE:TYPE=PD,PDNO=31,PDNAME=PD06;
```

The following query appears when you have copied the protocol from the hard disk to the database.

```
DISPLAY-PRODE:SRC=DB,KIND=VARTAB;
```

```
+---------------------+--------+--------+---------------------------+
| PROTVAR             |        | PDNAME | PDSTRING                  |
+---------------------+--------+--------+---------------------------+
| PSS1V2              | PDNORM |  PD06  | ETSI QSIG Third ed. SS    |
|                     | PDA1   |        |                           |
|                     | PDA2   |        |                           |
+---------------------+--------+--------+---------------------------+
```

The protocol must now be activated and renamed.

```
DISPLAY-PRODE:SRC=DB,KIND=PDSHORT;
```

```
+------+--------------------------+-------+-------+---------------+
|PDNAME| PDSTRING                 | IDENT | ACTIV | VERSION       |
+------+--------------------------+-------+-------+---------------+
| PD06 | ETSI QSIG Third ed. SS   | H/08  | NEIN  | B0-EL0.20.001 |
+------+--------------------------+-------+-------+---------------+
```

```
CHANGE-PRODE:KIND=PD,PDNAME=PD06,SEC=ORG,ACTIVE=Y;

DISPLAY-PRODE:SRC=DB,KIND=PDSHORT;
```

```
+------+---------------------------+-------+--------+---------------+
|PDNAME| PDSTRING                  | IDENT | ACTIVE | VERSION       |
+------+---------------------------+-------+--------+---------------+
| PD06 | ETSI QSIG Third ed. SS    | H/08  | Y      | B0-EL0.20.001 |
+------+---------------------------+-------+--------+---------------+
```

```
CHANGE-PRODE:KIND=VARTAB,PROTVAR=ECMAV2,PDNORM=PD06;

DISPLAY-PRODE:SRC=DB,KIND=VARTAB;
```

```
+---------------------+--------+--------+---------------------------+
| PROTVAR             |        | PDNAME | PDSTRING                  |
+---------------------+--------+--------+---------------------------+
| ECMAV2              | PDNORM |  PD06  | ETSI QSIG Third ed. SS    |
|                     | PDA1   |        |                           |
|                     | PDA2   |        |                           |
+---------------------+--------+--------+---------------------------+
| PSS1V2              | PDNORM |  PD06  | ETSI QSIG Third ed. SS    |
|                     | PDA1   |        |                           |
|                     | PDA2   |        |                           |
+---------------------+--------+--------+---------------------------+
```

Two different names now exist for one and the same protocol. The name no longer used is now deleted.

```
CHANGE-PRODE:KIND=VARTAB,PROTVAR=PSS1V2;

DISPLAY-PRODE:SRC=DB,KIND=VARTAB;
```

```
+---------------------+--------+--------+---------------------------+
| PROTVAR             |        | PDNAME | PDSTRING                  |
+---------------------+--------+--------+---------------------------+
| ECMAV2              | PDNORM |  PD06  | ETSI QSIG Third ed. SS    |
|                     | PDA1   |        |                           |
|                     | PDA2   |        |                           |
+---------------------+--------+--------+---------------------------+
```

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 phonebroking agencies, 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.

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.

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 Siemens 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.

DNIS
See *Dialed Number Identification Service*.

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.

ISA
Industry Standard Architecture.

L

LAN
See *Local Area Network*.

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.

MEB
Media Extension Bridge.

N

Network Interface Card (NIC)
A board connected to the telephony server and used to exchange data over a network.

NIC
See *Network Interface Card*.

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

SCCMEB
Service Call Control for Media Extension Bridge

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 timeframe.

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

T

U

V

W

X

www.siemens.com/hipath

Reference No.: A31003-G9330-I100-2-7620
Printed in the Federal Republic of Germany.