A MITEL
PRODUCT
GUIDE

OpenScape CAP V3

Common Application Platform

Servicedokumentation

Servicedokumentation
09/2024

A31003-G9330-I100-18-20

Mitel

Notices

Senden Sie Ihr Feedback zur Verbesserung dieses Dokumentes an edoku@unify.com.
Als Reseller wenden sich für spezifische Presales-Fragen bitte an die entsprechende Presales-Organisation bei Unify oder Ihrem Distributor. Für spezifische technische Anfragen nutzen Sie die Support Knowledgebase, eröffnen - sofern entsprechender Software Support Vertrag vorliegt - ein Ticket über das Partner Portal oder kontaktieren Ihren Distributor.

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Inhalt

1 Einleitung

In diesem Kapitel wird Ihnen kurz eine Übersicht über den Inhalt dieser Dokumentation gegeben und es wird Ihnen aufgelistet, in welchen unterschiedlichen Formaten diese und zusätzliche Dokumentationen zur Verfügung stehen. Zudem werden Ihnen die Layout-Konventionen erklärt, die in dieser Dokumentation verwendet werden.

1.1 Struktur dieser Dokumentation

Diese Dokumentation ist folgendermaßen gegliedert:

- In **Kapitel 2** finden Sie eine Übersicht über die Architektur von OpenScape CAP sowie typische Konfigurationen und Einsatz-Szenarien.
- In **Kapitel 3** sind die Systemvoraussetzungen für OpenScape CAP aufgeführt.
- In **Kapitel 4** ist die Installation der OpenScape CAP-Komponenten beschrieben. Das Kapitel behandelt die Server- und Client-Installation. Zusätzlich finden Sie Hinweise zur Migration (insbesondere Migration von Konfigurations- und Benutzerdaten aus früheren Versionen von CAP und TELAS) und zum Datenimport (insbesondere Synchronisation von Daten mit HiPath / OpenScape 4000).
- In **Kapitel 5** lernen Sie die Oberfläche des CAP Managements kennen.
- In **Kapitel 6** ist die Konfiguration der OpenScape CAP-Komponenten mit Hilfe des OpenScape CAP Managements beschrieben. Es wird die Anbindung von OpenScape CAP an die Vermittlungssysteme HiPath / OpenScape 4000, HiPath 3000 und andere erläutert. Es wird auch die Einrichtung des XML Phone Services beschrieben.
- In **Kapitel 7** erhalten Sie eine Übersicht über die Funktionen des OpenScape CAP Managements.
- In **Kapitel 8** wird die Diagnose und Fehlerbehandlung bei Installations- und Laufzeit-Problemen behandelt.
- In **Kapitel 9** werden die von der OpenScape CAP unterstützten Betriebsarten “Single Domain Native Mode” und “Multi Domain Harmonized Mode” erklärt.
- **Anhang A** umfasst die Implementierungs-Details sowohl zur Struktur der OpenScape CAP-Software als auch zum Layout von Konfigurations-Dateien und Konfigurations-Parametern.
- **Anhang B** beschreibt die Anbindung des Server-PCs an ein HiPath 4000 Kommunikationssystem.

Zusätzlich enthält die Dokumentation ein **Glossar** und einen **Index**.

1.2 Versionen dieser Dokumentation

- **Dokumentation im PDF-Format**

  Diese Version des Dokuments heißt *manual.pdf*.

  Die deutsche Fassung ist abgelegt im Verzeichnis
  <InstDir>\WebSpace\Admin\webapps\mgmnt\lang\de\admManual.

  Die englische Fassung ist abgelegt im Verzeichnis
  <InstDir>\WebSpace\Admin\webapps\mgmnt\lang\en\admManual.

  Das PDF-Format ist besonders für den Ausdruck geeignet und ist online über die Bedienoberfläche von OpenScape CAP Management verfügbar.

- **Dokumentation im HTML-Format**

  Diese Version des Dokuments heißt *manual.html*.

  Die deutsche und englische Fassung sind jeweils in den gleichen Verzeichnissen wie oben abgelegt.

  Die HTML-Version der Anleitung ist auch als Online-Hilfe verfügbar.

- **Release Notes**

  Release Notes mit wichtigen Informationen zu kurzfristigen Produktänderungen sind auf der CD unter dem Namen *<xxx>Readme.txt* abgelegt.

  Sie werden ausschließlich in Englisch bereitgestellt.

1.3 Zusätzliche Dokumentationen

Folgende Dokumentationen enthalten weitere Themen zu OpenScape CAP:

- OpenScape CAP Application Developers' Guide
  Vol.1 - Basics
  Vol.2 - TAPI
  Vol.3 - JTAPI
  Vol.4 - CSTA XML
  Vol.5 - CSTA III ASN.1
  Vol.6 - XML Phone Server
  Vol.7 - Fault Management
  Vol.9 - Management
- OpenScape CAP TAPI Service Provider, Serviceanleitung

1.4 Layout-Konventionen

... Schaltfläche **OK** ...	**Schaltflächen** und **Menüs** sind **fett** gekennzeichnet.
... Datei `global.cfg` ...	`Dateien` oder `Verzeichnisse` sind durch die Schriftart `Courier` gekennzeichnet.
<*Platzhalter*>	Einträge oder Ausgaben, die je nach Situation unterschiedlich sein können, stehen zwischen spitzen Klammern.

> Hinweise oder Empfehlungen sind mit diesem Symbol gekennzeichnet.

7 Warnhinweise, die unbedingt zu beachten sind, sind mit diesem Symbol gekennzeichnet.

1.5 Feedback zur Dokumentation

Wenn Sie ein Problem im Zusammenhang mit diesem Dokument melden möchten, wenden Sie sich an das jeweils nächsthöhere Supportlevel.

- Als Unify-Mitarbeiter wenden Sie sich bitte an das für Ihr Land zuständige Support Center.
- Kunden wenden sich an das Unify Customer Support Center.

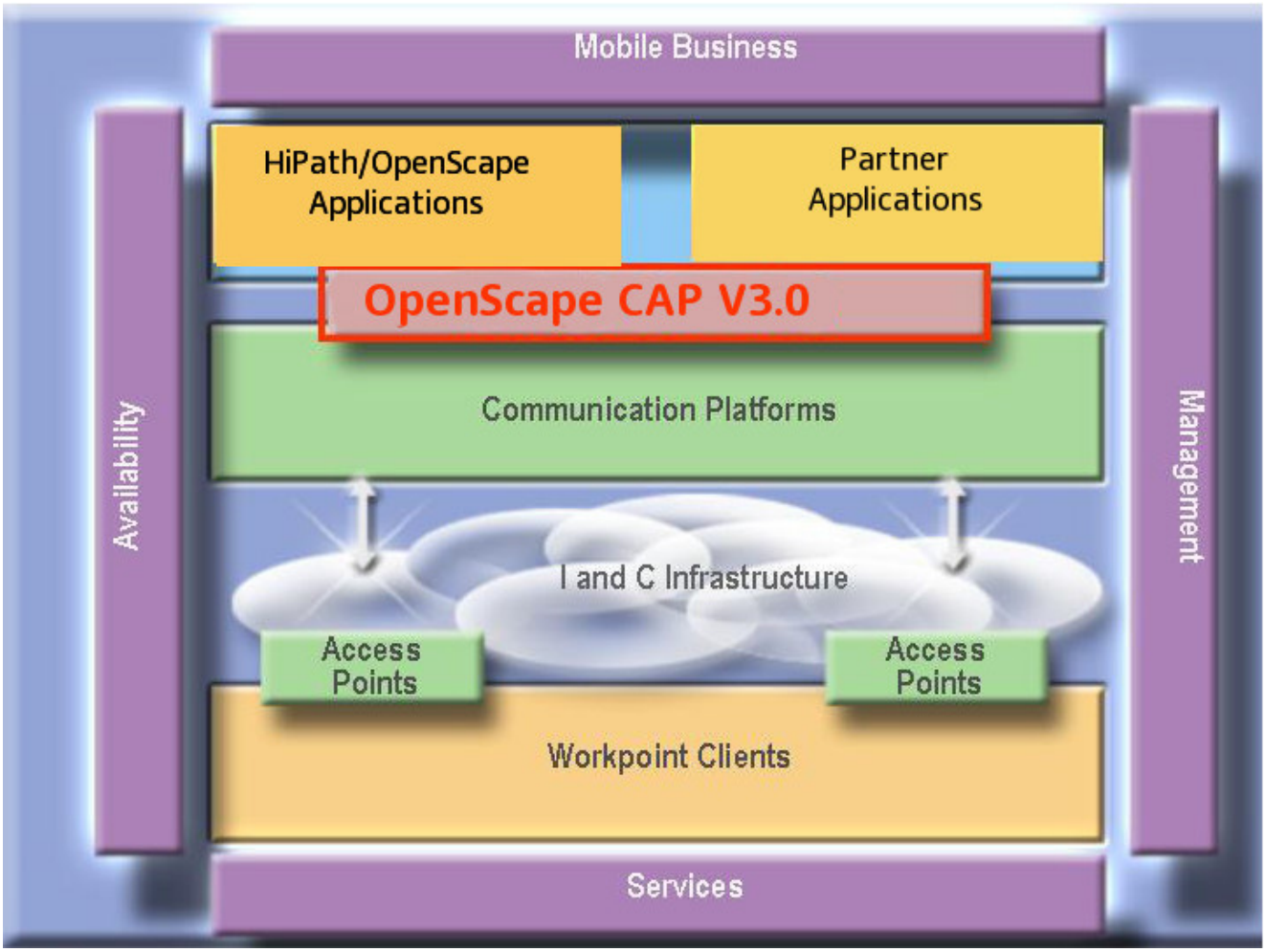
Halten Sie für entsprechende Anfragen bitte unbedingt die nachfolgend genannten Informationen bereit, damit sich das Dokument, mit dem es Probleme gibt, eindeutig ermitteln lässt.

- **Titel:** OpenScape CAP V3, Common Application Platform, Servicedokumentation
- **Sachnummer:** A31003-G9330-I100-18-20

2 Übersicht

Dieses Kapitel beschreibt die Common Application Platform innerhalb der OpenScape Architektur. Im Folgenden wird als Synonym die Abkürzung CAP oder OpenScape CAP verwendet.

2.1 Generelle Rolle der OpenScape CAP in der HiPath / OpenScape Architektur



OpenScape CAP ist ein zentraler Bestandteil der HiPath / OpenScape Architektur. Sie dient als leistungsstarke Middleware und verbindet Applikationen, die auf Standardprotokollen basieren, sowohl mit HiPath / OpenScape Systemen, als auch mit TK-Anlagen von Fremdherstellern.

Die Lizenzierung erfolgt für jedes Device (Phone, Trunk,...), welches durch die Applikationen gesteuert wird. Die unterstützten Leistungsmerkmale werden in fünf unterschiedliche Lizenzpakete geordnet. Dabei gibt es keine Unterschiede zwischen den Protokollen, den Kodierungsvarianten und den Verbindungsarten.

Leistungen

- Flexibilität beim Einsatz von Applikationen, die auf Standards basieren.
- CTI-Applikationsunterstützung für Clients in unterschiedlichen Infrastrukturen.
- Unterstützung für Sprach- / Medien-Transport ohne kostspielige Hardware
- Integration von OpenScape CAP und Applikationen in das OpenScape Management System.
- Durchgängige Nutzung einer Applikation bei Migration der Infrastruktur vom klassischen Telefon-Netzwerk zum IP-Netzwerk.
- Integration von XML-basierten Applikationen.
- CTI-Erweiterungen für vorhandene Applikationen.

Services für Applikations-Partner

- Applikationen wurden nur einmal entwickelt - OpenScape CAP stellt sicher, dass sie mit verschiedenen Infrastrukturen in unterschiedlichen Technologien arbeiten.
- Bei Verwendung der durch die OpenScape CAP bereitgestellten Services können eigene Applikationen um Leistungsmerkmale im Bereich Administration, Serviceability und Sicherheit erweitert werden.
- Beschleunigung von Applikationsentwicklungen durch die Ankopplung eigener Applikationen an HiPath / OpenScape Applikationen. Dadurch werden sie zu einem vollen Bestandteil des HiPath / OpenScape Portfolios.
- Reduzierte Trainingsaufwände durch Nutzung von XML.
- Programmierschnittstelle mit interaktivem Entwicklungswerzeug für XML Phone Services.
- Harmonisierung von Schnittstellen reduziert Entwicklungs- und Wartungsaufwendungen.
- Zusätzliche Geschäftsmöglichkeiten durch große Marktdurchdringung.

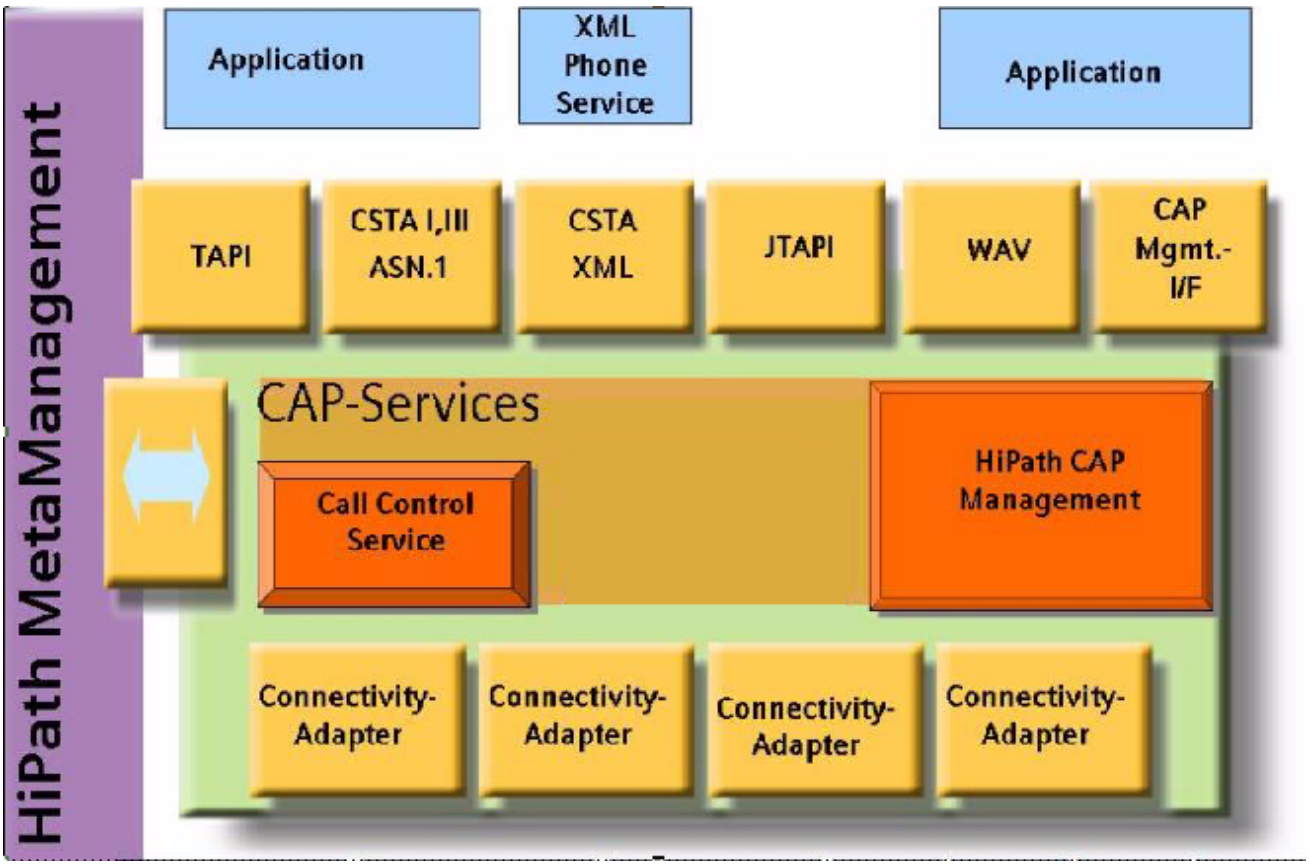
2.2 Leistungsmerkmale und Übersicht der Services

OpenScape CAP ist eine leistungsfähige Middleware, die modular skalierbar ist. Sie unterstützt effiziente Verbesserungen und ermöglicht eine Kostenreduzierung durch:

- die Unterstützung von Standard-APIs für Applikationsentwickler,
- die Unterstützung von Applikationsentwicklungen durch Services für CTI, Management und Lizenzierung, verfügbar über ein SDK,

Die folgende Grafik zeigt die Grundstruktur der OpenScape CAP mit ausführlichen Informationen über die unterstützten Protokolle und Kodierungsvarianten, die CAP internen Services und einige unterstützte TK-Anlagen. **CSTA I ist nicht mehr unterstützt**.

Highlights



- Standard Protokolle und API´s: Microsoft TAPI 2.x/3.0, JTAPI, CSTA III ASN.1, CSTA XML, Microsoft Wave API
- Call Control Service (SCC) für CTI
  - Multi Domain Leistungsmerkmale

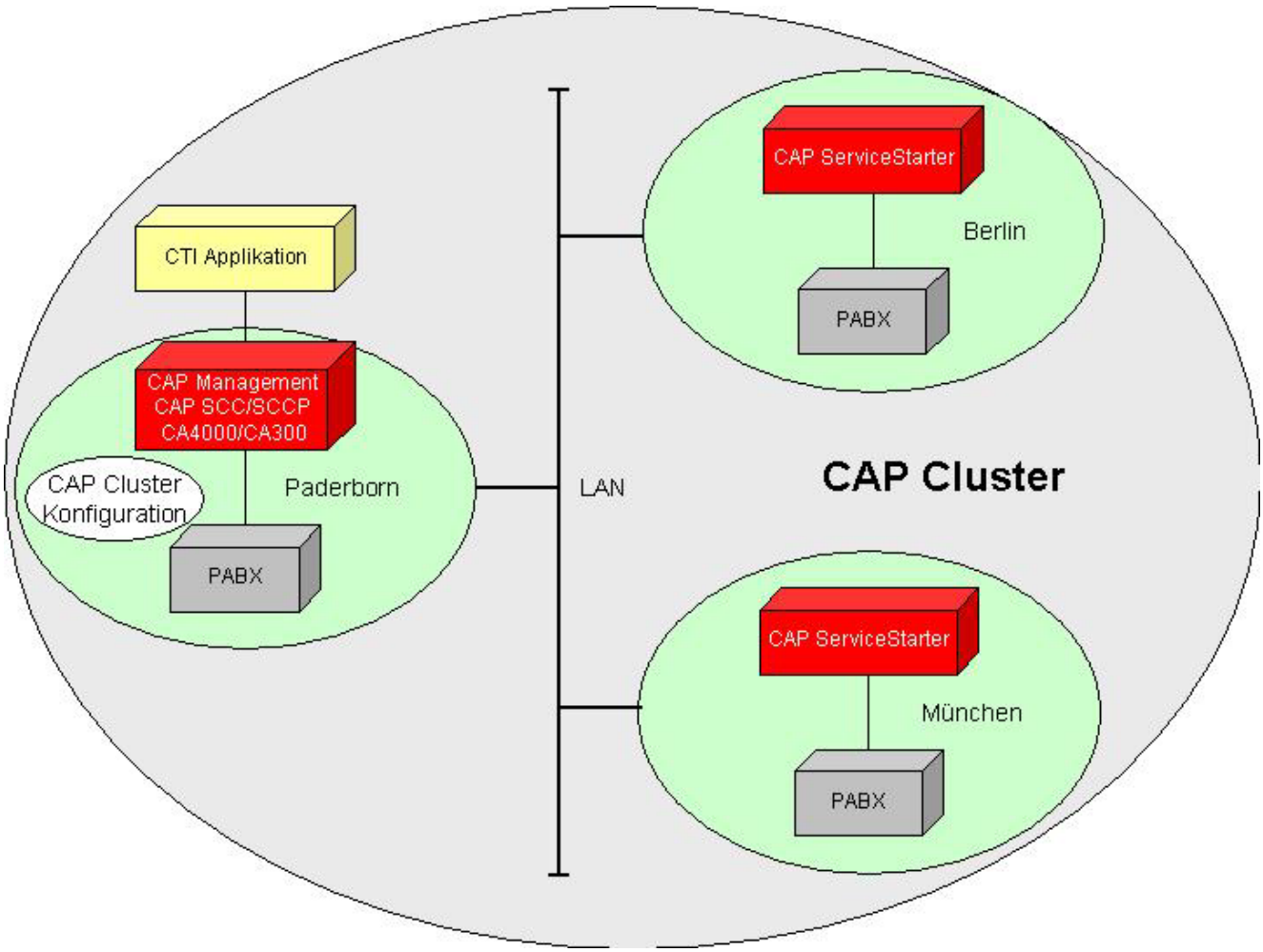
  - Harmonisierung der Call-Modelle der HiPath 3000, HiPath 4000, OpenScape 4000, HiPath 5000, HiPath 8000, OpenScape Voice für TAPI und CSTA basierende Applikationen

- Fault Management Service
  - Integration in das OpenScape Management (vom CAP Management unabhängig)
- Lizenz-, Benutzer-, und Konfigurations-Management Services
  - Einheitliche Lizenzstruktur
  - Integriertes Lizenz- und Benutzermanagement
  - LM als ein Service um OpenScape CAP und Applikationen in gleicher Weise zu lizenzieren
- Unterstützung spezieller Leistungsmerkmale
  - LiRus, AP emergency, XML PhoneServices

2.3 OpenScape CAP Management

Das CAP Management ist die zentrale Komponente in einem CAP Cluster. Es administriert und steuert alle Prozesse und Services in einer lokalen oder einer verteilten OpenScape CAP Installation. Die Cluster ID ist eine eindeutige Kennzeichnung von CAP Komponenten in dem gleichen CAP Cluster.

Das nachfolgende Schaubild verdeutlicht die Lage und Konfiguration der einzelnen CAP Komponenten bei einer verteilten Installation.



Das CAP Management wird durch den Windows Dienst **OpenScape CTI** gestartet und bietet zur Administration eine Web-basierte Oberfläche.

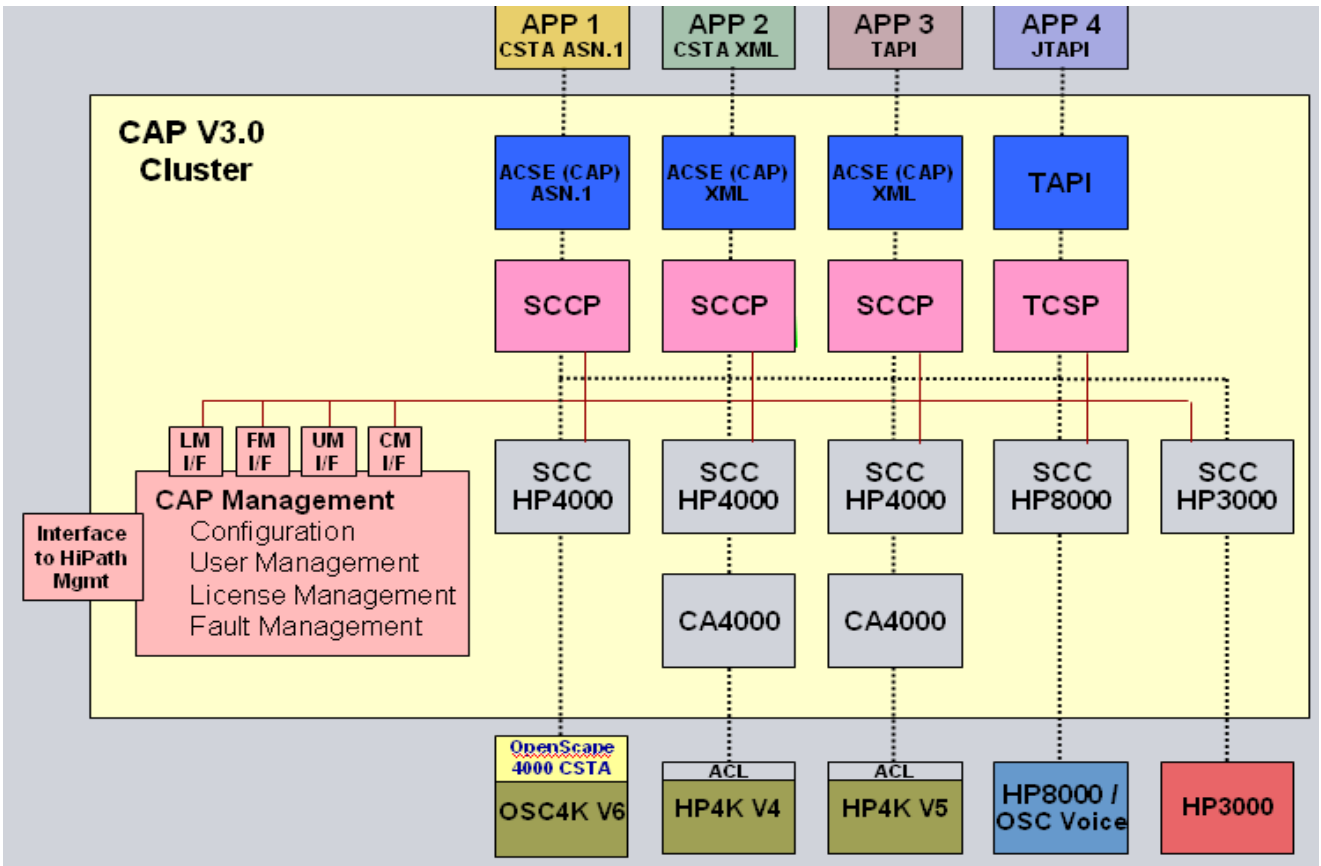
Aufgaben des CAP Managements

- Administration von zentralen und verteilten Komponenten
- Administration von Benutzern
- Administration von Devices
- Administration von Lizenzen
- Lizenzüberprüfung und Zugriffkontrollen von Benutzern und Devices
- Verwaltung von Statusinformationen der verschiedenen Prozesse und Services

Services des OpenScape CAP Managements

Das CAP Management kann in verschiedene Services aufgeteilt werden, welche unterschiedliche Aufgaben haben:

- Konfigurationsmanagement (SCM)
- Benutzermanagement (SUM)
- Lizenzmanagement (SLM)
- Address Translation Service (SAT)
- PBX Interface (SPI)
- CallIdRepository
- Open LDAP Server
- FaultManagement (SFM) (vom CAP Management unabhängig)



Diese Services werden nicht separat, sondern automatisch über den Setup-Menüpunkt **CAP Management** installiert. Die einzige Ausnahme ist das OpenScape CAP FaultManagement, das später noch genauer betrachtet wird.

Die wichtigen Services SCM, SUM und SLM des OpenScape CAP Managements können über http-Requests angesprochen werden. Sie werden zunächst intern von weiteren Services (SCC, SCCP, CAP TCSP) verwendet, ohne dass sie für eine Applikation direkt sichtbar sind. Dennoch lassen sie sich auch von externen Applikationen nutzen, so dass die entsprechenden Leistungsmerkmale ohne großen Aufwand dort integriert werden können.

> Die http-Requests werden aus Gründen der Abwärtskompatibilität noch unterstützt und nach und nach durch entsprechende XML-Requests ersetzt.

2.3.1 Das OpenScape CAP Konfigurationsmanagement (SCM)

Im OpenScape CAP Konfigurationsmanagement werden Verbindungen zu den verschiedenen TK-Anlagen administriert, die mit der CAP verbundenen sind. Dazu wird für jede einzelne TK-Anlage ein sogenannter Call Control Service (SCC) eingerichtet, der für jeden TK-Anlagen-Typ unterschiedlich ist. Jedem SCC wird eine eindeutige Service-Knoten-ID zugeordnet, die nur bei einem eventuellen Datenimport nicht beliebig sein kann. In gleicher Weise werden für Applikationen im **Multi Domain Mode** Call Control Service Proxy (SCCP) mit einer eindeutigen Service Knoten-ID eingerichtet und verwaltet. Wie Sie die Komponenten SCC und SCCP konfigurieren, sowie weitere Funktionen des OpenScape CAP Configuration Management sind in Kapitel 6, “Konfiguration mit OpenScape CAP Management” und Kapitel 7, “Weitere Funktionen von OpenScape CAP Management” beschrieben.

Über den http-Request:
`http://<fqdn>:8170/mgmnt/admin/req?getPBXSvcAddr=<Service-Knoten-ID>`
kann eine Applikation die IP-Adresse und Portnummer eines SCC anhand seiner Service Knoten ID erfragen.

Nebenstellen, Sammelanschlüsse, ACD-(RCG-)Gruppen der verschiedenen TK-Anlagen werden anhand ihrer Device-ID verschiedenen SCC zugeordnet. Die Device-ID ist die Langrufnummer im kanonischen Format (z.B. +49(5251)8-27486). Ebenso werden Leitungen eingerichtet. Um sie zu verwalten, werden sie ebenfalls als Device mit einer nur dem SCM bekannten Device-ID eingerichtet. Da die HiPath / OpenScape 4000 für Sammelanschlüsse, Leitungen und RCG-Gruppen sogenannte "LODEN"-Nummern zur Adressierung benötigt, übernimmt der "Address Translation Service" (SAT) die Umsetzung von deren Device-ID in eine "LODEN"-Nummer.

Über den http-Request:
`http://<fqdn>:8170/mgmnt/admin/req?getServiceForDevice=<Device-ID>`
kann eine Applikation die IP-Adresse und Portnummer eines SCC erfragen, an den ein CSTA Request für ein bestimmtes Device geschickt werden soll.

Die Komponenten SCCP und CAP TCSP nutzen aktiv diese Funktion des Konfigurationsmanagements. Als externe Applikation verwendet ebenfalls der Phone Controller des ComAssistant das XML-Pendant dieser Funktion.

2.3.2 Das OpenScape CAP Benutzermanagement (SUM)

Hauptbestandteil der OpenScape CAP ist das Benutzermanagement. Jeder CTI-Benutzer muss im CAP Benutzermanagement eingerichtet sein. Er wird durch eine eindeutige Benutzer ID verwaltet und bekommt ein Passwort zugewiesen. Zudem können Sie Benutzer zu Endgeräten/Vermittlungsanlagen zuordnen sowie Zugriffsrechte/Lizenzen an Endgeräte/Benutzer vergeben, wie in Abschnitt 7.3, “Benutzer” und Abschnitt 7.5, “Lizenzverwaltung” beschrieben.

Eine Verknüpfung mit der Windows Benutzerverwaltung ist möglich.

Über den http-Request:
`http://<fqdn>:8170/mgmnt/auth/req?authenticate=<User ID>&pass-wd=<Password>&encoding=b64`
kann eine Applikation Benutzer und zugehöriges Passwort überprüfen lassen.

Die Komponenten SCCP, SCC und CAP TCSP nutzen aktiv diese Funktion des Benutzermanagements. Als externe Applikation verwendet ebenfalls der Phone Controller des ComAssistant das XML-Pendant dieser Funktion.

2.3.3 Das OpenScape CAP Lizenzmanagement (SLM)

Das Lizenzmanagement wird von OpenScape CAP Komponenten und OpenScape CAP basierenden Applikationen verwendet .

Über ein Menü können Lizenzschlüssel installiert werden. Diese beinhalten u.a. eine Applikations-ID und die Anzahl der zur Verfügung stehenden Client-Lizenzen.

Demo-Lizenzen stehen zur Verfügung.

Durch die Lizenzschlüssel CAP-E (Entry), CAP-S (Standard) und CAP-A (Advanced) werden die entsprechenden Client-Leistungsmerkmale freigeschaltet. Darüberhinaus besteht die Möglichkeit, applikationsspezifische Lizenzschlüssel zu verwenden. Diese sind gleichwertig zur CAP-A Lizenz. Sie werden zum Beispiel von den OpenScape CTI Applikationen SimplyPhone for Outlook (SimplyPhone O), SimplyPhone for Lotus Notes (SimplyPhone N) und ComAssistant genutzt. Als erste externe Applikation verwendet auch “XPhone” (c4b) das Lizenzmanagement der CAP.

Eine Lizenz wird einem Device zugeordnet. Dies kann bei der Device-Einrichtung oder durch implizite Zuweisung bei einer Lizenzüberprüfung geschehen; die Zuordnung bleibt danach bestehen.

> Die HiPath CAP V1.0 Lizenz “UNKNOWN”, die die Anzahl der zu setzenden Monitorpunkte einer CA4000 lizenziert hat, wird ab der HiPath CAP V2.0 nicht mehr benötigt. Ab der CA4000 Version 6.0.0.0 besitzt diese keine eigene Verbindung zum CAP SLM und benötigt deshalb auch keine eigene Lizenz mehr!

Lizenzvarianten

Entry-Client (CAP-E)	Nur das Leistungsmerkmal "MakeCall" wird unterstützt.
Standard-Client (CAP-S)	Alle Leistungsmerkmale werden unterstützt, mit Ausnahme der ACD Leistungsmerkmale.
Advanced-Client (CAP-A)	Alle Leistungsmerkmale werden unterstützt, auch ACD Leistungsmerkmale.
Linux-Client (CAP-L)	zusätzlich zu den CAP-E / CAP-S / CAP-A oder applikationsspezifischen Lizenzen ist eine CAP-L-Lizenz erforderlich, wenn die CAP-Installation auf Linux betrieben wird.

Die nachfolgende Tabelle zeigt eine Übersicht der verschiedenen Vermarktungspakete.

Lizenz	**je Kanal**	**1**	**10**	**25**	**100**	**site >500**
Entry / CAP-E			X			
Standard / CAP-S			X	X	X	X
Advanced / CAP-A			X	X	X	X
Linux / CAP-L		X	X	X	X	X
Media FAX / CAP-FM	X					
applikationsspezifische Lizenz	für interne Applikationen - HiPath ProCenter / OpenScape Contact Center - HiPath SimplyPhone family - HiPath Com Assistant - etc. sowie für ausgewählte OEM Applikationen Jede applikationsspezifische Lizenz enthält implizit eine CAP Client-Lizenz					

Eine Applikation muss sich bei der CAP zunächst anmelden (authentifizieren) und dabei eine Applikations-ID übergeben. Diese Applikations-ID muss mit einer der installierten Lizenz übereinstimmen. Eine Lizenzüberprüfung findet bei jedem Request statt, der von dieser Applikation an die CAP für ein definiertes Device gesendet wird. Wurde die entsprechende Client-Lizenz diesem Device zugeteilt, wird der Request an die TK-Anlage weitergeleitet.

Bitte beachten Sie, dass Lizenzen CAP-L in Abhängigkeit von den Gegebenheiten einer Installation von den entsprechenden CAP-Komponenten implizit überprüft werden; explizite Anmeldung zur Nutzung von CAP-L ist nicht erforderlich und nicht sinnvoll.

Über den http-Request:
`http://<fqdn>:8170/mgmnt/admin/req?registerLicense=<ApplicationID>&userId=<DeviceID>`

überprüfen die CAP Komponenten, ob einem Device eine geforderte Lizenz zugeteilt wurde, bevor ein Request weitergeleitet werden kann. Auch externe Applikationen können über den gleichen Request oder das XML-Pendant überprüfen, ob einem in der eigenen Applikation eingerichteten Device eine entsprechende Lizenz zugeteilt wurde.

Fazit: Es wird immer eine Lizenzüberprüfung stattfinden!

Überschreitung der Anzahl von Client-Lizenzen

Wird die Anzahl der installierten Client-Lizenzen einer Applikation überschritten, werden temporäre Lizenzen mit einer zweimonatigen Gültigkeit zugeteilt. Gleichzeitig findet eine Benachrichtigung per Email an eine definierte Email-Adresse statt. Alle temporären Lizenzen werden mit einem "*" gekennzeichnet. Nach Ablauf der Gültigkeit werden Requests für diese CTI-Benutzer abgewiesen.

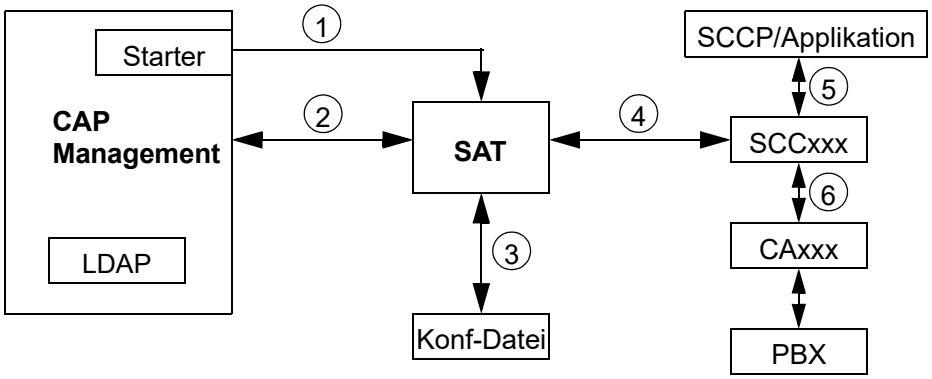
2.3.4 Address Translation Service (SAT)

Der "Address Translation Service (SAT)" hat die Aufgabe, in der Kommunikation einer Applikation mit dem SCCP oder mit dem SCC immer die Rufnummer im internationalen oder kanonischen Format zu verwalten. Das kanonische / internationale Format ist im ECMA CSTA III Standard beschrieben.

- Er konvertiert eine gewählte Rufnummer vom internationalen oder kanonischen Format in eine wählbare Nummer. Das "Overlapping" von Nebenstellennummer mit einem Teil der Hauptanschlußnummer wird dabei berücksichtigt.
- Er konvertiert die zu monitorende Rufnummer aus dem internationalen / kanonischem Format in ein zur jeweiligen PBX passendes Format, wobei auch das "Overlapping" berücksichtigt wird.
- Er konvertiert die in einem Event oder in einer Response übermittelte Rufnummer von den Format "Nebenstellennummer", "NAC-Nummer" (Nummer mit vorangestellter Querkennzahl), "PNP-Nummer" in das kanonische Format, damit eine Applikation diesen Event immer eindeutig einem Device zuordnen kann und beispielsweise in einem zentralen Adressverzeichnis suchen bzw. wählen kann.
- Zur Adressierung von "non-station devices" (Leitungsbündel, Sammelanschluss, Route-Control-Gruppe) in der HiPath / OpenScape 4000 konvertiert er die anlagen-interne Benennung (LODEN) in die in der CAP eingerichtete Nummer.

Um abwärtskompatibel zu sein, wurde ein "Legacy Mode" eingeführt. In diesem Modus ist die Adresskonvertierung ausgeschaltet, so dass sich die CAP3.0 bzgl. der Rufnummern wie eine CAP2.0 verhält. Der "Legacy Mode" kann entweder für die ganze CAP oder für spezifische SCC-Instanzen aktiv sein, ist aber nicht applikationsindividuell einstellbar. Die Aktivierung / Deaktivierung wird über Konfigurationsdateien gesteuert (siehe Abschnitt A.2.15). Änderungen in Konfigurationseinstellungen werden jeweils nach einem Neustart des Services wirksam.

Das folgende Bild zeigt, wie SAT in die CAP V3.0 eingebettet ist (Schnittstellen 1,2,3,4) und welche sonstigen Schnittstellen SAT beeinflusst (5,6).



Schnittstelle 1: SAT wird vom Starter Prozess des CAP Managements gestartet und kann nicht mittels des Diagnose Agents gestoppt und neu gestartet werden. SAT kann nur durch das Neustart von dem ganzen OpenScape CTI Service neugestartet werden.

Schnittstelle 2: SAT holt sich vom CAP Management die Liste aller SCC-Daten einmal beim Start. Ändern sich diese Daten, verständigt das CAP Management den SAT und gibt ihm die geänderten Daten (mit Push-Technik). Die Device-Daten holt sich SAT ebenfalls in bestimmten Fällen vom CAP Management.

Schnittstelle 3: SAT liest beim Neustart aus der Datei SatServer.cfg Informationen wie TCP Port, Log Level oder "Legacy Mode".

Schnittstelle 4: XML Schnittstelle, über die der SCC die Konvertierungswünsche an SAT sendet und über die er das Ergebnis der Konvertierung erhält. Standardmäßig wird für diese Kommunikation das Port 8999 verwendet, es kann aber über die Konfigurationsdatei ein anderes Port gewählt werden (siehe Abschnitt A.2.15, “Konfigurationsdateien für SAT”).

Das XML Kommando kann folgende Tags enthalten:

- ConvertToDialable
  Kommando, das eine internationale/kanonische Rufnummer in das PBX-Dialable-Format konvertiert.
- ConvertToSFR
  Kommando, das eine internationale/kanonische Rufnummer in das PBX-SFR-Format konvertiert.

– ConvertToSwitchFormat
Kommando, das eine internationale/kanonische Rufnummer oder Leitung in das entsprechende PBX-Format konvertiert (z.B. LODEN bei Leitungen).

– ConvertToPbxDeviceNumber
Kommando, das eine Leitung, die in einer netzwerkweiten, kanonischen Form vorliegt, in das entsprechende PBX-Format konvertiert (z.B. LODEN).

– ConvertToCanonical
Kommando, das eine PBX spezifische Rufnummer oder Leitung (z.B. LODEN) in eine internationale/kanonische Rufnummer oder Leitungsbezeichnung konvertiert.

Hinweis: Die Konvertierung von Leitungen, RCG (Route Control Group) und Sammelanschlüssen ist von SAT vorgeleistet, aber noch nicht in allen CAP V3.0 Komponenten implementiert.

– SatEntry: Klammer über alle folgenden Tags

– DeviceID
Rufnummer im CSTA III Format mit allen Sub-Tags, z.B. typeOfNumber

– CallingCalledInfo
Art der Rufnummer aus vermittlungstechnischer Sicht (mögliche Werte sind CallingIncoming, CallingOutgoing, CalledIncoming, CalledOutgoing)

– CallingPbxId
PBX Identifikation im CAP Management, dort als SccId bezeichnet

– PerformedInfo
Rückmeldung, ob Konvertierung erfolgreich
(mögliche Werte sind OKCanonicalNo, OKDialingNo, OKSFR, OKDeviceNumber, NoTransMgmt, NoTransParam, OKAlreadyFormatted)

Schnittstelle 5: An dieser bereits in der CAP V2.0 bestehenden Schnittstelle werden durch Aufruf des SAT die CSTA deviceID’s verändert, sobald der "Legacy Mode" ausgeschaltet ist.

Die folgenden CSTA III deviceID Formate werden in Richtung PBX unterstützt:

? Dialing number, kanonisches Format (z.B. +49(89)722-1234)

? Dialing number, internationales Format (z.B.+49897221234)

? SFR number, kanonisches Format (z.B. N+49(89)722-1234)

? SFR number, internationales Format (z.B. N+49897221234)

? SFR number mit Namen, kanonisches Format (z.B. N<+49(89)722-1234>Heinz M.)

? SFR number mit Namen, internationales Format (z.B. N<+49897221234>Heinz M.)

- Andere Formate ohne vorangestelltes + Zeichen werden nicht von SAT konvertiert, sondern unverändert zur PBX weitergeleitet.

Die folgenden CSTA III deviceID Formate werden in Richtung Applikation unterstützt:

- SFR number, kanonisches Format (z.B. N+49(89)722-1234)
- SFR number, internationales Format (z.B. N+49897221234)
- SFR number mit Namen, kanonisches Format (z.B. N<+49(89)722-1234>Heinz M.)
- SFR number mit Namen, internationales Format (z.B. N<+49897221234>Heinz M.)
- Falls eine Rufnummer, die von der PBX empfangen wurde, nicht konvertierbar ist, wird sie unverändert zur Applikation geschickt. Der "typeOfNumber" einer solchen deviceID wird auf "dialingNumber" oder "other" gesetzt, abhängig davon, ob auf eine Rufnummer geschlossen werden kann oder nicht.

Schnittstelle 6: Diese bereits in der CAP2.0 bestehende Schnittstelle wird durch SAT nicht verändert, so dass in den CA'n und den PBX'n keine Anpassungen erforderlich sind.

Man beachte, dass die Adresskonvertierung kann nur erfolgreich sein, wenn die SCC-Daten wie z.B. Länderkennzahl aller PBX'n, die miteinander kommunizieren, im CAP Management konfiguriert sind.

Eine CallingIncoming Rufnummer, die mit Ursprung in einer fremden PBX gemeldet wird, kann konvertiert werden

- wenn sie eine Amtsrufnummer ist (z.B. 0030..., d.h. der Anruf aus Berlin kommt)
- wenn sie in einem PBX spezifischen Rufnummernplan, einem privaten Rufnummernplan (PNP) oder als Nebenstellenrufnummer abgebildet ist und das Device im CAP Management konfiguriert ist (z.B. 991234, wobei 99 die Querkennziffer darstellt)

Liegt daher eine PBX Netzwerkskonfiguration vor, in der nicht alle Devices von CAP verwaltet werden und trotzdem eine sichere Konvertierung gewünscht wird, ist die Einrichtung eines sogenannten "Virtuellen SCC" und das Importieren aller Devices erforderlich. Details dazu werden in Abschnitt 6.4 beschrieben.

Zur erfolgreichen Konvertierung einer wählbaren Nummer ins internationale oder kanonische Format ist sicherzustellen, dass die für eine Vermittlungsanlage eingerichtete Amtsausstiegs-Kennzahl nicht als Beginn einer auf dem gleichen Switch eingerichteten Rufnummer vorkommt (d.h. für eine Anlage, auf der "20" als Amtsausstieg verwendet wird, darf keine Rufnummer mit "20..." beginnen).

Schnittstelle 6: Für die erfolgreiche SAT Konversion sollen alle Devices in CAP Datenbank einkonfiguriert werden, ausser die Devices, welcher mit VNR Nummern konfiguriert sind. (Ausführliche Infromations in CAP ADG Vol 1. Kapitel 5.6 Non-unique numbering plan).

2.3.5 PBX Information

Der PBX information service (SPI) ist ein neuer Dienst, der den Datenabgleich zwischen CAP und PBX erleichtern soll. Als Ergänzung für die Import-Funktion, aus Import-*Dateien* aufgebaut, die von externen Quellen bereitzustellen sind, baut SPI eine direkte Verbindung zur PBX-Administration auf und holt sich Daten zu Benutzern und Devices ohne dass zwischengeschaltete Dateien erforderlich sind.

SPI kann aus der CAP Management-Bedienoberfläche aufgerufen werden; derzeit wird es ausschließlich für die Verbindung zur HiPath / OpenScape 4000 bereitgestellt (vgl. Abschnitt 6.2.3).

2.3.6 CallIdRepository

Der interne Service "CallIdRepository" ist für keine Applikation direkt sichtbar. Er hat die Aufgabe, für einen Call die ursprüngliche zugeordnete Call-ID vom Anfang bis zum Ende seiner Existenz zu verwalten und sie an eine Applikation über den SCC weiterzuleiten.

Dieser Dienst wird ausschließlich für die Anbindung von HiPath / OpenScape 4000 bereitgestellt. Er wird nur für sehr spezielle Applikations-Szenarien benötigt; demzufolge ist er standardmäßig ausgeschaltet.

2.3.7 Open LDAP Server

Der "Open LDAP Server" verwaltet die gesamten Konfigurationsdaten der CAP.

2.3.8 Das OpenScape CAP FaultManagement (SFM)

Strategisch und vertrieblich befindet sich das OpenScape CAP FaultManagement zwar auf der OpenScape CAP CD, ist aber dennoch völlig losgelöst von den anderen OpenScape CAP Services zu betrachten. Details zum OpenScape CAP FaultManagement enthält ein eigenes Handbuch “OpenScape CAP FaultManagement Developer’s Guide”; dort werden auch Installation und Konfiguration behandelt.

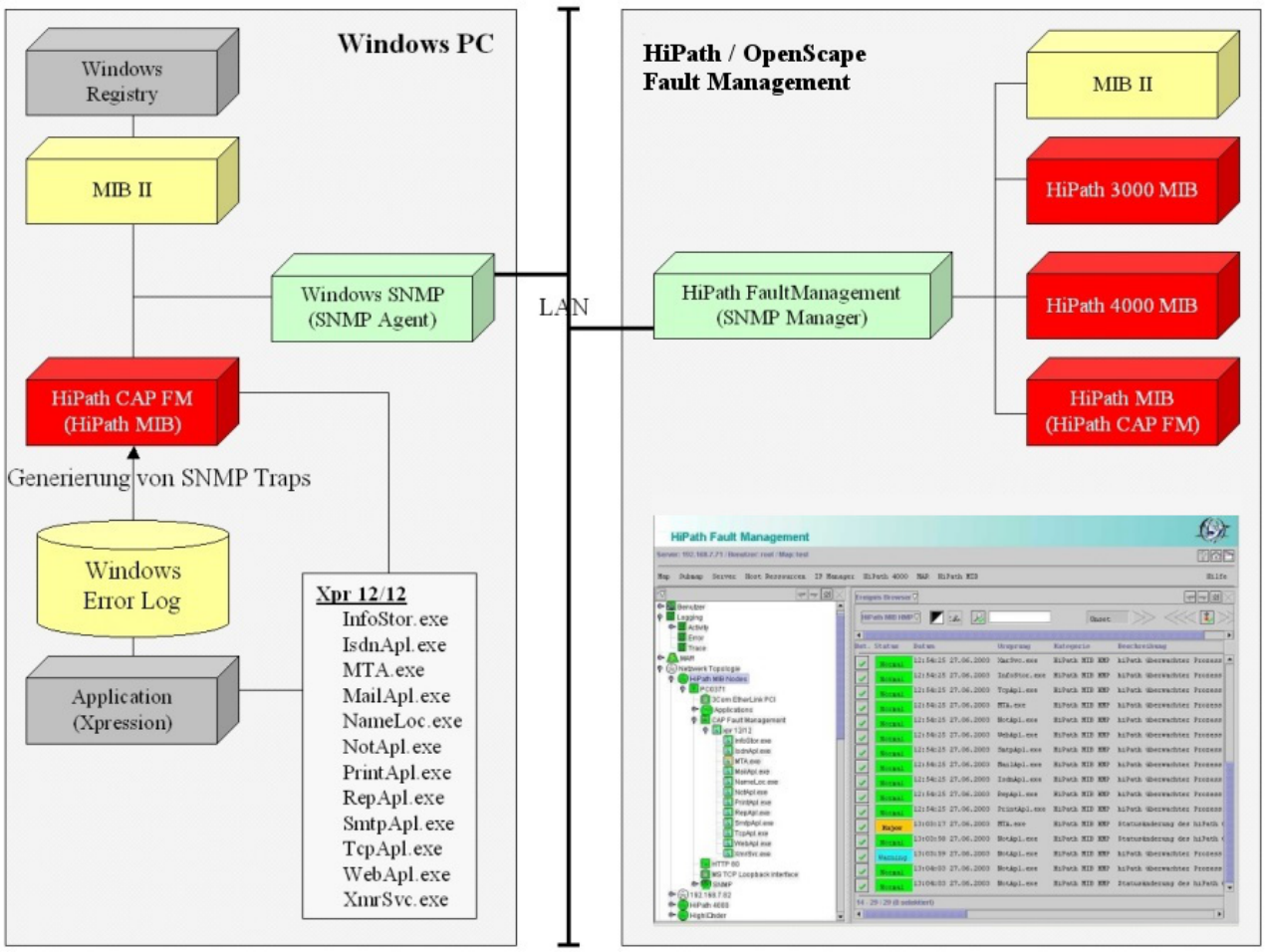
Das OpenScape CAP Fault Management besteht aus 6 DLLs. Es ist kein eigenständiger Dienst, sondern an den Windows SNMP Dienst gekoppelt. Windows basierende Programme können durch Integration dieser DLL durch das OpenScape Fault Management verwaltet werden (siehe ADG vol 7).

Folgende Leistungsmerkmale werden durch das CAP FM unterstützt:

- Auto Discovery
- OpenScape MIB basierende Informationen
- Trap notification

Neben den über die MIB II zur Verfügung stehenden Informationen erhält das OpenScape FaultManagement Informationen zu den CAP FM unterstützenden Applikationen und den zu überwachenden Prozessen. In der Richtung zum OpenScape FaultManagement werden entweder Traps über den CAP FM SNMP Agent weitergeleitet oder der CAP FM Agent erzeugt sie basierend auf speziell gekennzeichneten Meldungen im Windows Ereignisprotokoll.

Die folgende Grafik verdeutlicht das vom OpenScape FaultManagement initiierten Auto Discovery eines Windows PC mit aktivem SNMP Agent, installiertem Xpression 450 und dem integrierten OpenScape CAP FM.



Verwaltung der CAP durch das OpenScape FaultManagement

Die CAP stellt eine XML Schnittstelle bereit, welche automatisch vom dem OpenScape FaultManagement erkannt wird. Über diese Schnittstelle wird eine Verbindung zum OpenScape CAP Diagnose Manager hergestellt. Informationen bezüglich der Stati der verschiedenen CAP Prozesse werden vom OpenScape FaultManagement zyklisch abgefragt und im FM-Desktop dargestellt. Ein direkter Link zum Diagnose Agent existiert im OpenScape FaultManagement ebenfalls.

2.4 OpenScape CAP Betriebsarten

Die OpenScape CAP unterstützt zwei unterschiedliche Betriebsarten.

Single Domain Native Mode

HiPath / OpenScape 4000 CSTA III ASN.1

Multi Domain Harmonized Mode

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

Je nach Betriebsart werden unterschiedliche TK-Anlagen, Protokolle und Kodierungsvarianten unterstützt. Details zu den einzelnen Betriebsarten finden Sie im Kapitel 9, “Betriebsarten”.

Genaue Informationen bezüglich der unterstützten Services entnehmen Sie bitte dem OpenScape CAP Prospect, der OpenScape CAP Technical Information oder dem OpenScape CAP ADG. Dort werden explizit alle unterstützten Services für die einzelnen TK-Anlagen in den Betriebsarten "Native Mode" und "Harmonized Mode" für die verschiedenen Protokolle und Kodierungsvarianten aufgelistet.

2.4.1 Erklärung der Begriffe

Single Domain	Nur eine TK-Anlage, SCC Anbindung.
Multi Domain	Eine oder mehrere TK-Anlagen, SCCP Anbindung; unterschiedliche Typen von TK-Anlagen möglich.
Native Mode	Proprietäre CSTA-Protokollelemente, Standard und Private Services werden unterstützt.
Harmonized Mode	Nur Standard CSTA Services werden unterstützt.

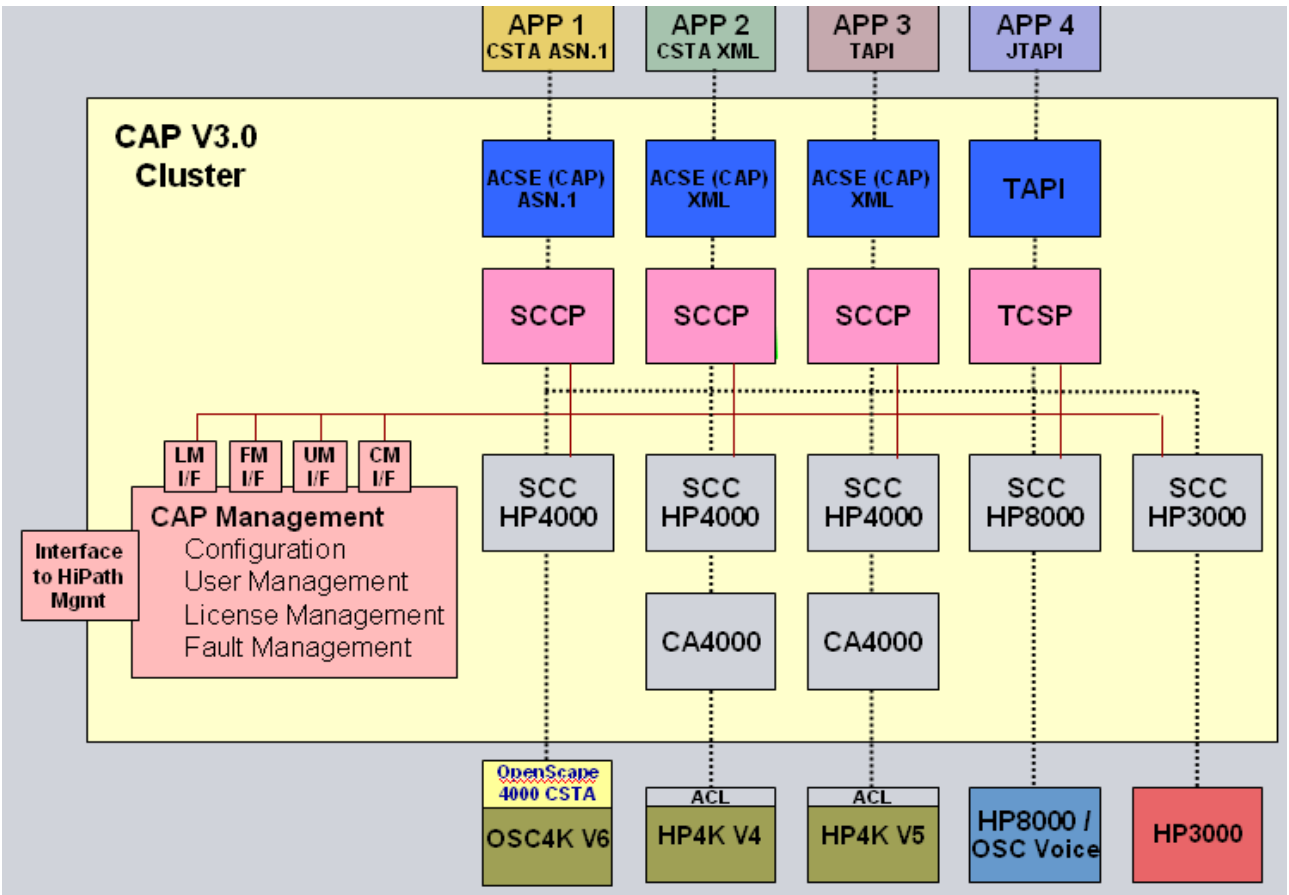
Der **Single Domain Native Mode** wird zur CTI-Anbindung von bisher bestehenden Applikationen verwendet, ohne dass eine Änderung in der Software der Applikation vorgenommen werden muss. Die Applikation erkennt das Vorhandensein der OpenScape CAP nicht.

Der **Multi Domain Harmonized Mode** wird in modifizierter Form vom Phone Controller von ComAssistant verwendet. Auch der CAP TCSP nutzt ihn. Weitere Applikationen werden derzeit entwickelt. Ein Applikation muss den neuen ACSE_AARQ der CAP, Nebenstellennummern im langen kanonischen Format und eine Call ID in 8 Bytes Länge unterstützen.

2.5 OpenScape CAP Komponenten

Die Komponenten SCC, SCCP, CA4000 und CAP TCSP stellen in unterschiedlichen Kombinationsmöglichkeiten die Verbindung zwischen einer Applikation und verschiedenen TK-Anlagen her.

Die folgende Grafik ist eine strukturelle Darstellung der CAP im "Multi Domain Harmonized Mode". **H300 ist nicht mehr unterstützt**.



2.5.1 Der Call Control Service Proxy (SCCP)

Der SCCP ist eine CAP Komponente, welche den “Multi Domain Mode” unterstützt. Der SCCP stellt Applikationen einen TCP/IP-Verbindungsport zur Verfügung. Der erste Request zum SCCP nach einem Verbindungsaufbau muss ein ACSE_AARQ sein. Dieser beinhaltet Benutzername, Passwort, Applikations-ID, CSTA Version, Native Mode = True/False

Mit einem gültigen CAP-Benutzer/-Passwort muss sich eine Applikation beim SCCP authentifizieren. Dazu verwendet der SCCP den SUM des CAP Managements.
Der SCCP speichert die Applikations-ID zur Client-Lizenzierung nachfolgender Requests. Dazu verwendet der SCCP den SLM des CAP Managements. Der SCCP speichert erfolgreiche CTI-Benutzer-Lizenzüberprüfungen 3600 Sekunden.
Die CSTA Version definiert, in welcher CSTA III-Kodierung nachfolgende Requests übermittelt werden.
Für die Kommunikation mit JTAPI-Applikation wird das CSTA XML-Protokoll verwendet. Dazu müssen von diesen Applikationen die von der CAP zur Verfügung gestellten JAR-Dateien importiert worden sein.
Native Mode = True/False definiert, ob nachfolgende Requests proprietäre Protokollelemente enthalten und ob ein erweiterter Leistungsumfang und “private services” unterstützt werden sollen.

Konfigurationsparameter eines SCCP

Ein SCCP wird nicht durch Konfiguration auf “Native Mode” oder “Harmonized Mode” eingestellt, sondern die unterschiedlichen Betriebsarten werden durch die Kennzeichnung “Native Mode = True/False” im ACSE_AARQ aktiviert.

Durch Konfigurationsparameter werden verschiedene Positionen eines SCCP definiert.

Für die Applikation	Eine Applikation verbindet sich mit einem SCCP über eine IP Adresse und einem von SCCP geöffneten Port.
Lokale Position	Der Name des CAP Cluster PC, auf dem der SCCP laufen soll.
Zur TK-Anlage	Die Richtung ist nicht konfigurierbar. Ein SCCP verbindet sich nur mit SCC-Instanzen. Er ermittelt die IP Adresse und den zugehörigen Port eines SCC durch den SCM des CAP Managements. Dazu muss zwingend für jeden ersten Request die Nebenstellennummer im langen kanonischen Format übermittelt werden.

2.5.2 Der Call Control Service (SCC)

Der SCC ist eine CAP-Komponente mit einer definierten Verbindung zu einer TK-Anlage. Für jeden durch die CAP unterstützten TK-Anlagen-Typ wird eine entsprechende Variante eines SCC verwendet.
Jeder SCC wird durch eine konfigurierbare Service Knoten-ID verwaltet. Diese ID muss eindeutig sein und ist nur im Falle von einem späteren Benutzerdatenimport nicht beliebig. Weiterhin werden jedem SCC die Rufnummern der angeschlossenen TK-Anlage zugeteilt.

Konfigurationsparameter eines SCC

Im **Multi Domain Mode** werden in Richtung zum SCCP die Protokolle und Kodierungsvarianten CSTA III ASN.1, CSTA XML und zum CAP TCSP das NetTSPI unterstützt.

Im **Single Domain Native Mode** werden Applikationen direkt mit einem SCC verbunden (nur HiPath / OpenScape 4000). Dazu wird ein SCC4000 fest in einer der Protokollvarianten "CSTA III ASN.1" oder "ACSE (CSTA III ASN.1)" konfiguriert.

Durch **Konfigurationsparameter** werden verschiedene Positionen eines SCC definiert:

Für die Applikation	Ein SCCP, CAP TCSP oder eine Applikation verbindet sich mit einem SCC über eine IP-Adresse und einem vom SCC geöffneten Port.
Lokale Position	Der Name des CAP Cluster-PC, auf dem der SCC laufen soll.
Zur TK-Anlage	Die Richtung zu einer TK-Anlage wird über eine IP-Adresse und Portnummer definiert, mit dem sich der SCC verbindet. Der SCCHiPath3000 verbindet sich direkt mit der HiPath 3000. Die HiPath 3000 kann auch über S_0 angebunden werden. Der SCCHiPath4000 verbindet sich mit der CA4000.

2.5.3 Der Connectivity Adapter 4000 (CA4000)

Der CA4000 konvertiert das proprietäre CTI-Protokoll der HiPath 4000 (ACL-C+) in ein standardisiertes Protokoll (CSTA). Die Verbindung zur HiPath 4000 ist über das ATL, die WAML und die SL100/200 freigegeben. Der CA4000 unterstützt CSTA III oder ACSE (CSTA III) Links in der Kodierung ASN.1. Der CA4000 wird immer zusammen mit dem zugehörigen SCC im CAP Management eingerichtet.

Konfigurationsparameter des CA4000

Für die Kommunikation mit der HiPath 4000 werden die IP-Adresse der HiPath 4000, eine PBX Link-Nummer und eine Subapplikationsnummer eingerichtet. Zur Kommunikation der SCCs mit dem CA4000 werden wiederum die IP-Adresse sowie ein Port im Bereich von 1025 - 5000 konfiguriert.

> PROBLEME IM ZUSAMMENSPIEL CA4000 UND WINDOWS DIENSTEN:
> Es ist zu beachten, dass der Windows Taskplaner und der Windows Logondienst Ports im Bereich von 1025 - 1299 belegen, welche nach jedem Neustart des entsprechenden Dienstes variieren werden können.

2.5.4 Der CAP TAPI Service Provider (CAP TCSP)

Der CAP TCSP ist eine CAP-Komponente, welche den “Multi Domain / Harmonized Mode” unterstützt. Er stellt das TAPI Service Provider Interface (TSPI) für Windows TAPI basierte Applikationen zur Verfügung. Seine Multi Domain-Fähigkeit basiert auf der Nutzung des SCM der CAP; er kommuniziert direkt mit dem SCC über ein proprietäres Protokoll (NetTSPI). Eine gleichzeitige Verbindung mit mehreren SCCs ist möglich.

Konfigurationsparameter eines CAP TCSP

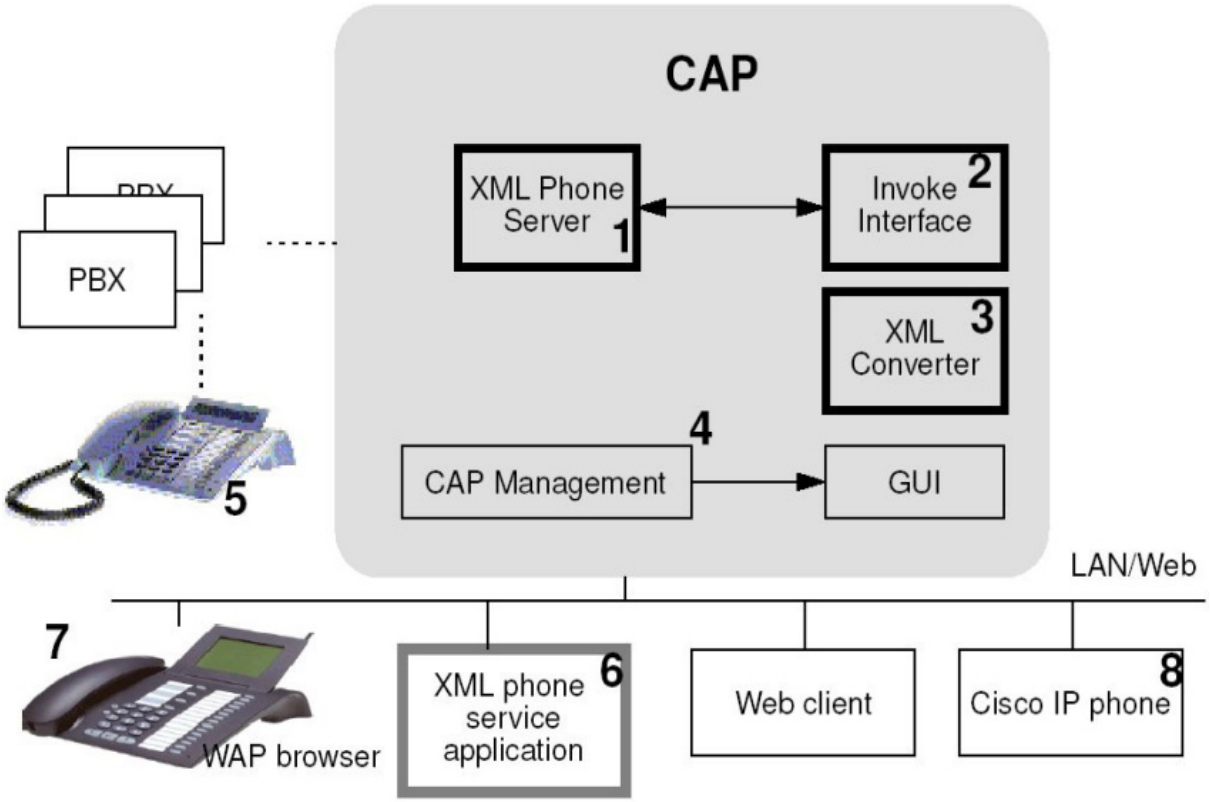
Der CAP TCSP wird über das separate Installationsprogramm setupTapi.exe eingerichtet. Er bindet sich in die erweiterten Windows "Telefon und Modemoptionen" ein und wird über den Windows "Telephonie" Dienst gestartet.

Konfigurationsparameter sind die IP-Adresse oder der PC-Name des CAP Management-Rechners und die Portnummer des CAP Managements (Default 8170). Die verschiedenen Lines werden durch die Device-ID (Langrufnummer im kanonischen Format) eingerichtet. Sie müssen einmalig im SUM eingerichtet sein. Eine automatische Synchronisation zwischen CAP TCSP Lines und allen in der CAP eingerichteten CTI-Benutzern ist möglich. Das ist aber nur sinnvoll, wenn eine entsprechende Applikation dieses auch benötigt. Der CAP TCSP verwendet wie eine externe Applikation das SUM zur Authentifizierung von Benutzern (Devices). Default-Passwörter müssen während der ersten Anmeldung geändert werden. Erst nach einer erfolgreichen Authentifizierung wird eine Verbindung mit einem SCC aufgebaut. Die Client-Lizenzierung erfolgt automatisch durch eine interne SCC-Routine. Die beginnt linear mit der Applikations-ID "CAP-A", "CAP-S" und endet mit "CAP-E". TAPI-Applikationen haben die Möglichkeit, individuelle Applikations-ID zur Lizenzierung zu übergeben.

2.5.5 Der XML Phone Service (XMLPS)

Der "XML Phone Service (XMLPS)" setzt als Applikation auf einem in der CAP konfigurierten SCCP auf. Er stellt externen Applikationen eine neue XML-Schnittstelle zur Verfügung. Die XML-Applikationen verwenden für die Kommunikation mit dem XMLPS das Standard HTTP/ HTTPS-Protokoll. XMLPS-Applikationen können Endgeräte einer HiPath 4000 oder HiPath 3000 als Eingabe-/Ausgabegeräte nutzen (z.B. nutzt OpenScape den XMLPS). Durch einen optionalen WML-Adapter können auch WAP-fähige Endgeräte (z.B. optiPoint 600) oder mobile phones Zugriff auf diese Applikationen haben. Der XML Phone Service besteht aus drei Hauptkomponenten:

- **OpenScapeCAP XMLPS Phone Server Prozess** (sxmlps.exe)
  Dieser Prozess ist die Verbindungskomponente zum SCCP.
- **OpenScape CAP XMLPS Invoke Interface**
  Dieses Interface ermöglicht die Ansteuerung der Endgeräte (Display, LED der Tasten)
- **OpensScape CAP XMLPS Konverter Servlets**
  Die Konverter sind Java-Servlets, welche XML nach WML konvertieren. Eine Konvertierung von Cisco WAP Phones ist ebenfalls integriert (CAPPhone Syntax nach CiscoPhone Syntax, CiscoPhone Syntax nach CAPPhone Syntax).



Der XML Phone Server verhält sich wie ein Browser und behandelt die Endgeräte als Endpunkte mit:

- einem zweizeiligen Display,
- Audio Indikator (beep),
- Applikationstasten mit zugeordneter LED,
- Menü Item Selektionstasten,
- OK-Taste,
- die normale Tastatur als alphanumerische Tastatur.

Wird am Endgerät eine Applikationstaste gedrückt, so wird die XML Phone Applikation durch Aufruf der konfigurierten URL gestartet, die in der CAP mit dieser Taste assoziiert ist. Die Applikation sendet via Invoke Interface als Ergebnis ein CAPPhone-Objekt (als einen HTTP-Response mit dem MIME-Typ: XML), welche für das Endgerät verarbeitet werden soll, an dem die Taste gedrückt wurde.

Die Applikation kann

- eine Textnachricht am Display anzeigen lassen,
- einen Signalton generieren,
- den Lampenstatus setzen.

Zusammen mit dem XML Phone Service werden unter dem Namen "**On A Button Suite**" einfache, aber nützliche Applikationen ausgeliefert:

- **EasyLookup**
  Ermöglicht die Suche in einem LDAP-Directory ohne Nutzung eines PCs. Während einer bestehenden Verbindung werden bei Aufruf der Funktion die zu den Gesprächsteilnehmern verfügbaren Informationen aus dem LDAP-Directory ermittelt und angezeigt. Ansonsten kann manuell im LDAP-Directory nach Namen oder Telefonnummern gesucht werden. Die Namen und evtl. weitere Informationen werden im Display des Telefons angezeigt. Verfügbare Informationen können hierbei auch zur gehenden Wahl verwendet werden.
- **Easy See**
  Auf Knopfdruck werden für alle Teilnehmer des Gesprächs die im LDAP-Directory verfügbaren Informationen ermittelt und als "Phone Card" auf dem PC angezeigt.
- **EasyShare**
  Startet NetMeeting auf allen PC, welche den im Gespräch verbundenen Teilnehmern (über SysTray) zugeordnet sind.
- **EasyMail**
  Öffnet eine neue E-Mail für alle im Gespräch verbundenen Teilnehmer.

- **EasyConference**
  Unterstützt die Verwaltung von Konferenz-Schaltungen über das Telefon; zum Betrieb ist der Einsatz eines MMCSBoards in der HiPath / OpenScape 4000 erforderlich. EasyConference verwaltet nur MMCS "Master Conference Rooms"; es stellt dem Conference Master eine bequeme Schnittstelle zur Steuerung der Konferenz zur Verfügung. Die übrigen Konferenzteilnehmer brauchen die EasyConference-Applikation nicht.
  Sobald der erste Teilnehmer den Conference Room betreten hat, wird der Master auf seinem Endgerät über Display, Klingelton oder blinkende "EasyConference"-Lampe informiert; er kann dann
  - ebenfalls den Conference Room betreten
  - sich alle derzeit anwesenden Teilnehmer anzeigen lassen
  - einzelne Teilnehmer aus der Konferenz entfernen.

Zusätzliche Information zum XML Phone Service ist verfügbar über den XMLPS Application Developers' Guide, der Teil der CAP-Dokumentation ist; nach Abschluss der CAP Installation ist diese Information auch online über die URL `http://<CAP host>:8172` abrufbar.

3 Systemvoraussetzungen

In diesem Kapitel werden alle Hardware- und Software-Voraussetzungen beschrieben, um OpenScape CAP installieren zu können. Einige CAP-Komponenten können sowohl auf dem zentralen Server-PC als auch auf abgesetzten PC oder auf Client-PCs installiert werden. Die Durchführung der kompletten Installation finden Sie im Kapitel 4, “Installation”.

3.1 Hardwarevoraussetzungen

Nachstehend sind die Hardwareeigenschaften für den Server-PC als auch für die abgesetzten PCs (falls vorhanden) aufgelistet. Alle betroffenen PCs müssen in einem gemeinsamen Netzwerk integriert sein.

3.1.1 Zentraler Server-PC (für CAP Management)

Auf dem zentralen Server-PC müssen alle OpenScape CAP-Server-Komponenten installiert werden, wie z.B. OpenScape CAP Management oder die CAP Call Control Services.

Mindestanforderungen

- Prozessor mit mindestens 2GHz
- mindestens 1GB Arbeitsspeicher
- ca. 1 GB freier Festplattenspeicher
  (10 GB ist empfolen für Log-Dateien)

Bemerkung: Wenn VMWare benutzt wird, dann ist das minimale Anforderung von CAP Speicheraustattung nicht 1GB, sonder 2GB.

Je nach Ausbau Ihres Systems ist es ratsam, besser ausgestattete PCs zu verwenden als unter den Mindestanforderungen angegeben. Welche PCs für welche Ausbaustufen verwendet werden sollen, finden Sie in folgender Tabelle.

Konfiguration	PC-Typ
Call Control	
no	A
small	A
medium	A
large	B
large to very large	C

Call Control

- small bis zu 100 Nutzer
- medium bis zu 500 Nutzer
- large bis zu 2.000 Nutzer
- very large bis zu 20.000 Nutzer

PC-Typ

- A 2 GHz CPU / 1 GB RAM / 40 GB HD (Mindestanforderung)
- B 2 GHz CPU/ 1 GB RAM / 60 GB HD (Mindestanforderung)
- C Verteiltes System bestehend aus den PC-Typen B oder Multi-Prozessor PC mit mindestens 8 GB RAM

3.1.2 Client-PCs (für CAP Service Starter)

Client-PCs sind zusätzliche PCs im Netzwerk, auf denen bei einer verteilte Installation der CAP Service Starter installiert wird. Sie können OpenScape CAP-Komponenten wie z.B. Call Control Services oder Connectivity Adapters enthalten. Die Anforderungen hängen von der Anzahl und dem Typ der zu unterstützenden Komponenten ab. Die folgenden Daten können daher nur als Anhaltswerte dienen. Zudem laufen auf den Client-PCs auch die CTI-Anwendungen.

Mindestanfoderungen

- 1,6 GHz processor
- mindestens 1 GB Arbeitsspeicher
- ca. 800 MB Plattenspeicher

3.1.3 Kommunikationssystem

Stellen Sie sicher, dass das Kommunikationssystem (z.B. HiPath / OpenScape 4000, HiPath 3000, usw.), mit dem OpenScape CAP zusammen laufen soll, voll funktionsfähig ist. Eine von dem Kommunikationssystem und OpenScape CAP unterstützte Anschlussmöglichkeit muss verfügbar sein (z.B. über eine TCP/IP-Verbindung).

3.2 Softwarevoraussetzungen

Nachstehend sind die Softwarevoraussetzungen für den Server-PC als auch für die Client-PCs (falls vorhanden) aufgelistet.

3.2.1 Zentraler Server-PC / Client-PC

Betriebssystem

- In den Freigabemitteilungen finden Sie die aktuell unterstützten Windows-Versionen.
- SuSE Linux Enterprise Server (SLES 10)
- SuSE Linux Enterprise Server (SLES 11)

Web-Browser

Es wird empfohlen, auf dem Server-PC einen Web-Browser für Tests und Konfigurationsarbeiten nach der Erstinstallation zur Verfügung zu halten.

3.2.2 WEB Client-PC

> Jeden PC, von dem eine Verbindung zum OpenScape CAP Management hergestellt wird, bezeichnet man als WEB Client-PC. Hierbei handelt es sich **nicht** um den PC, auf dem der CAP Service Starter installiert ist!

Betriebssystem

Das Betriebssystem auf dem Client-PC unterliegt keinen Einschränkungen. Neben den Windows-Betriebssystemen kann auch UNIX, Linux, MacOS, etc genutzt werden.

Web-Browser

- Internet Explorer 8.0 aufwärts
- Firefox 10.x aufwärts
- Chrome 24.x aufwärts

Der Web-Browser muss JavaScript und Cookies unterstützen und zulassen. Der Internet Explorer muss so eingestellt werden, dass er immer beim Laden einer Seite nachschaut, ob es eine neue Version davon gibt (einzustellen unter **Extras** | **Internetoptionen** | **Temporäre Internetdateien** | **Einstellungen** | **Neuere Versionen der gespeicherten Seiten suchen: Bei jedem Zugriff auf die Seite**).

> Die einwandfreie Funktion von CAP Management kann nur mit den genannten Browser-Versionen garantiert werden.
> Man beachte insbesondere, dass Netscape nicht mehr unterstützt wird.

3.3 Weitere Installationsvoraussetzungen

- Der Rechnername (host) darf keine nicht standardiserten Zeichen enthalten. Standardisierte Zeichen sind Buchstaben (A-Z, a-z), Zahlen(0-9) und der Bindestrich(-).
- Der Rechner muss ein feste und gültige IP-Adresse haben und im DNS eingetragen sein. Überprüfen Sie die korrekte Namensauflösung mit dem DOS-Befehl `nslookup` und der Eingabe `<PC-Name>` bzw. `<IP-Adresse>`.
- Falls mehr als eine NIC in dem PC installiert ist, muss die erste NIC mit dem Kunden-LAN verbunden sein.
  Überprüfen Sie die korrekte Bindung der NIC durch einen `PING` auf den eigenen PC-Namen. Als Rückgabe muss die IP-Adresse des Kunden-LAN ausgegeben werden.

  Die Bindung der NIC wird geändert über den Menüpunkt **Systemsteuerung | Netzwerk und DFÜ-Verbindungen | Erweitert | Erweiterte Einstellungen | Verbindungen**.

- Falls das CAP Management nicht auf einem Server-Betriebssystem installiert wird, müssen die Systemleistungsoptionen geändert werden über **Arbeitsplatz | Eigenschaften | Erweitert | Systemleistungsoptionen | Reaktionsgeschwindigkeit für Anwendungen | Systemleistung optimiert für Hintergrunddienste**.
- Achten Sie darauf, das die dem CAP Management zugeordnete Cluster-ID nicht von einem anderen CAP Management-Server im selben IP-Netz verwendet wird.
- Große Teile des CAP-Systems sind in Java implementiert. Diese nutzen das Java Runtime Environment JRE 1.7. Die JAVA Anforderungen in der SMR12 haben sich deutlich geändert. JAVA wird aus Lizenzierungsgründen mit CAP nicht mehr mitgeliefert. Vor der CAP SMR 14 Installation muss Java 7 auf dem PC installiert werden.
- Bei Installation auf relativ neuen Windows -Betriebssystemen (mit Aktivierung aktueller Security Patches) kann es Probleme beim Start der CAP Management-Oberfläche geben; dort ist üblicherweise der Internet Explorer mit deaktivierter Sicherheits-Einstellung “META REFRESH zulassen” eingerichtet - stellen Sie sicher, dass die Einstellung aktiviert ist!
- Hier gibt es die folgenden Vorgehensalternativen:
  - Firewall deaktivieren (eher unerwünscht).
  - Firewall explizit zur Nutzung mit CAP konfigurieren (vgl. Abschnitt 4.9.3, “Betrieb der CAP hinter einer Firewall”)
  - Die Name, Vollname und IP-Addresse von dem PC zu Vertrauenswürdige Site Internet Explorer zufügen: **Extras | Internetoptionen | Sicherheit | Vertrauenswürdige Sites | Hinzufügen.**

4 Installation

Dieses Kapitel beschreibt die komplette Installation von OpenScape CAP. Im Unterschied zu früheren Versionen wird die aktuelle Version mit einem MSI-Installer-Paket für Windows ausgeliefert. Mit diesem ist sowohl eine Standard-Installation als auch eine den spezifischen Bedürfnissen angepaßte Installation möglich.

Die Standard-Installation ("Complete") sorgt für die Bereitstellung aller verfügbaren CAP-Dienste auf dem CAP-Rechner. Näheres dazu in **Abschnitt 4.1**

Die angepasste Installation ("Server") dient ebenfalls für den zentralen CAP-Rechner; sie gestattet die individuelle Auswahl einzelner Pakete zur Installation. Details sind in **Abschnitt 4.2** beschrieben.

Bei verteilter Installation muss auf den abgesetzten Rechnern eine "Starter"-Installation erfolgen. Diese ist in **Abschnitt 4.3** beschrieben.

Die Installation unter Linux wird gesondert in **Abschnitt 4.4** beschrieben.

Darüber hinaus gibt es in diesem Kapitel folgende Information:

- **Abschnitt 4.6** beschreibt das generelle Vorgehen bei der Installation in allen Varianten
- **Abschnitt 4.7** beschreibt Besonderheiten der verteilte Installation
- **Abschnitt 4.8** beschreibt die Startreihenfolge der CAP-Prozesse bei einer nichtverteilten und einer verteilten Installation.
- Die Installation weiterer Komponenten ist in **Abschnitt 4.5** (CAP TAPI Service Provider) beschrieben.
- **Abschnitt 4.9** behandelt spezifische Probleme während der Installation oder Wartung
- **Abschnitt 4.10** beschreibt die Deinstallation von OpenScape CAP.

Zur Erhöhung der Übersichtlichkeit werden hier nur die “üblichen” Installationsaufgaben erläutert. Für spezielle Aspekte sowie die Fehlersuche bei Installations- und Konfigurationsproblemen werden Querverweise in andere Kapitel dieses Handbuchs sowie weitere Handbücher angegeben. Viele dieser Aspekte werden in Kapitel 8 und Anhang A abgedeckt.

7	In Kapitel 2, “Übersicht” werden typische Einsatzszenarien einschließlich der Wechselbeziehungen SCCP/SCC beschrieben. Achten Sie darauf, für den jeweiligen Einsatzfall das adäquate Szenario mit entsprechender Kombination von SCCP- und SCC-Varianten auszuwählen. OpenScape CAP Configuration Management kann mit jetzigem Stand die Definition technisch unsinniger Kombinationen von SCC-Instanzen nicht vollständig verhindern.

Reihenfolge der Installation

Die korrekte Einrichtung von OpenScape CAP erfordert genaue Einhaltung einer Reihe von Schritten:

1. Lizenzen für OpenScape CAP und Applikationen besorgen.
2. OpenScape CAP wie im folgenden beschrieben installieren.
3. Nach Bedarf Switch-Anbindungen konfigurieren; dazu gehören jeweils Call Control Services (SCCs) mit passenden Connectivity Adapters (CAs) und Anbindung an die Vermittlungsanlage.
4. In Abhängigkeit von der aufsetzenden Applikation eventuell SCCPs einrichten.
5. Lizenzen über CAP Management installieren.
6. Devices einrichten oder importieren.
7. Benutzer einrichten oder importieren und Devices zuordnen.

Für den Fall, dass direkt anschließend eine Applikation installiert werden soll,

8. Applikationen installieren.

Voraussetzungen

Bevor Sie mit der Installation beginnen, sollten Sie folgende Voraussetzungen klären:

- Haben Sie alle Lizenzen für OpenScape CAP?
- Ist ein Web-Browser (Internet Explorer, Netscape Navigator) installiert und konfiguriert?
- Unterstützt dieser Browser Cookies und JavaScript? Sind Cookies zugelassen und JavaScript aktiviert?
- Hat der PC eine gültige IP-Adresse, und ist er im DNS eingetragen?
- Diejenige Person, die die Installation durchführt, muss auf dem PC Administrator-Rechte besitzen.

4.1 "Complete"-Installation

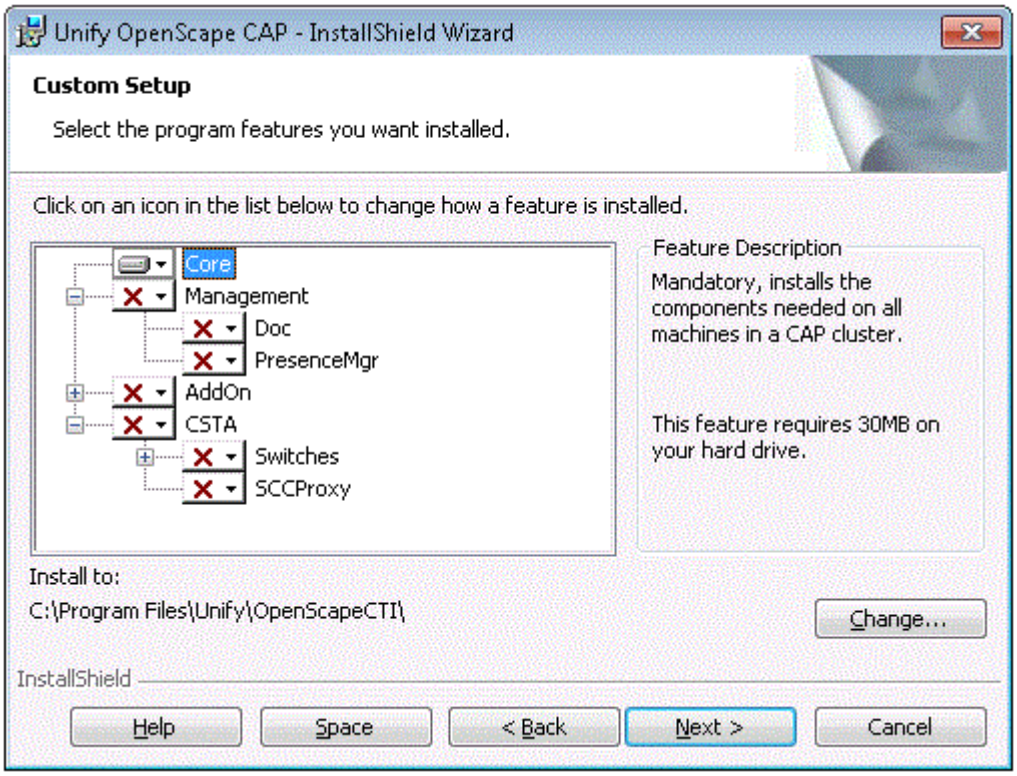
Diese Installation ist für den zentralen CAP-Server gedacht; sie hat den größten Speicherplatzbedarf, läuft dafür aber am einfachsten ohne weitere Bediener-Interaktion.

Rufen Sie zum Starten der Installation aus dem Software-Verzeichnis der CAP-CD `CAP.msi` auf. Auf Nachfrage nach dem Setup-Typ wählen Sie "Complete" - alle Systemkomponenten einschließlich der optionalen Teile werden installiert.

4.2 "Server"-Installation

Diese Installation ist für den zentralen CAP-Server gedacht; sie erlaubt die gezielte Auswahl der zu installierenden Komponenten.

Rufen Sie zum Starten der Installation aus dem Software-Verzeichnis der CAP-CD `CAP.msi` auf. Auf Nachfrage nach dem Setup-Typ wählen Sie "Server" - CAP Management und CSTA-Dienste nach Bedarf installieren.



Während der Installation erscheint ein Auswahl-Fenster zur Definition der zu installierenden Komponenten.

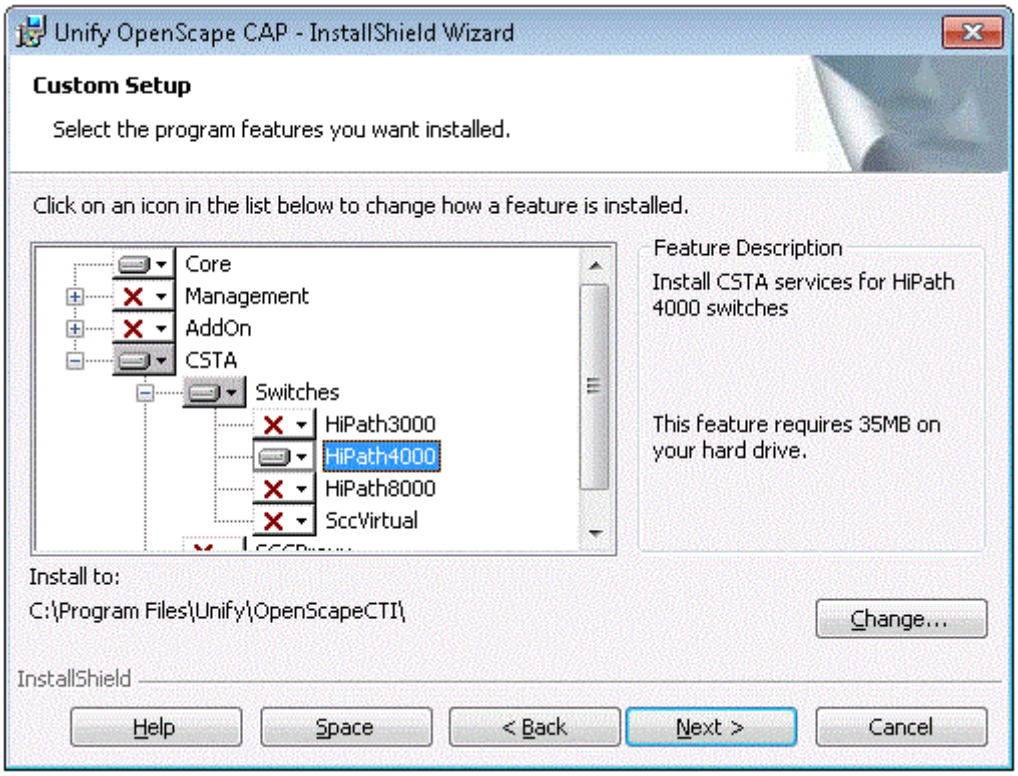
Das **Core**-Paket enthält alle CAP Management-Dienste; dieses ist immer erforderlich und kann nicht abgewählt werden.

Das **Management**-Paket enthält die online-Dokumentation und ist optional.

Das **AddOn**-Paket enthält die optionalen PhoneServices (vgl. Abschnitt 2.5.5) sowie die derzeit noch irrelevante UMIntegration.

Das **CSTA**-Paket enthält die Auswahl verfügbarer Switch-Anbindungen sowie SCCP (Kapitel 6 enthält eine detaillierte Beschreibung dieser Komponenten). Bitte beachten Sie, dass durch Auswahl eines der angebotenen Switches alle für die Anbindung erforderlichen CAP-Komponenten automatisch installiert werden. Separate Behandlung von z.B. SCC4000 und CA4000 zur Anbindung einer HiPath 4000 ist nicht länger erforderlich.

Das folgende Bild zeigt eine mögliche Komponentenauswahl, zur Anbindung von HiPath 4000



4.3 "Starter"-Installation

Diese Installation ist für einen abgesetzten Server in einer verteilten CAP-Installation gedacht; hier gibt es keine zusätzlichen Auswahlmöglichkeiten.

Rufen Sie zum Starten der Installation auf dem abgesetzten Server aus dem Software-Verzeichnis der CAP-CD `CAP.msi` auf. Auf Nachfrage nach dem Setup-Typ wählen Sie "Starter" - ein CAP Process Starter wird installiert.

4.4 Installation unter Linux

> 7 Bitte beachten Sie, daß die gesamte CAP-Installation komplett unter Linux oder komplett unter WIndows erfolgen muß. "Gemischte" Linux+Windows-Installationen werden nicht unterstützt.
> Die nachfolgende Beschreibung beschränkt sich auf Besonderheiten der Linux-Installation. Wenn hier nicht spezifisch etwas anderes beschrieben ist, gelten die ausführungen zur WIndows-Installation gleichermaßen unter Linux.
>
> In den restlichen Kapiteln dieser Serviceanleitung finden sich (zum Beispiel zum "Starten des Service OpenScape CTI") an einigen Stellen Windows-spezifische Nutzungshinweise; es wird aus Gründen der Übersichtlichkeit darauf verzichtet, an allen diesen Stellen zusätzlich auch die Linux-Variante zu beschreiben. Bitte entnehmen Sie bei Bedarf die Linux-Besonderheiten dem nachfolgenden Abschnitt.

Zur Installation von HiPath CAP V3.0 SMR 5 unter SuSE Linux Enterprise Server 9 wird ein Satz von rpm-Installationspaketen bereitgestellt (xx entsprechend der endgültigen Freigabe):

- Grundpaket
  CAP-V3.0-R14.032.0.i386.rpm
- CAP Management-Paket
  CAP-mgmt-V3.0-R14.032.0.i386.rpm
- Dokumentations-Paket
  CAP-doc-V3.0-R14.032.0.i386.rpm
- CSTA-Pakete zur Anbindung von TK-Systemen
  CAP-Scc<TK-System>-V3.0-R14.032.0.i386.rpm
  CAP-SccP-V3.0-R14.032.0.i386.rpm
  CAP-SccVirtual-V3.0-R14.032.0.i386.rpm

Für die "Starter"-Installation (analog zu Abschnitt 4.3) ist nur das Grundpaket zu installieren.

Für die "Server"-Installation (analog zu Abschnitt 4.2) sind das Grundpaket sowie CAP Management zu installieren. Dazu kommen die gewünschten CSTA-Pakete sowie optional das Dokumentations-Paket.

Die "Complete"-Installation (analog zu Abschnitt 4.1) ergibt sich durch Installation aller vorhandenen Pakete.

4.4.1 Vorgehensweise zur Installation unter Linux

1. Als "root" auf dem Linuxsystem anmelden
2. Gewünschte rpm-Pakete installieren
   `rpm -U -h -v <paket_1> [ <paket_2> ...]`
   (-h zur Fortschritts-Anzeige, -v für verbose / ausführliche Information)

   Es können mehrere Pakete gemeinsam installiert werden; falls die Pakete einzeln hintereinander installiert werden, ist die Reihenfolge zu beachten: als erstes das Grundpaket, dann das CAP Management-Paket und anschließend die übrigen Pakete in beliebiger Reihenfolge. Wird die Reihenfolge nicht eingehalten, so wird rpm entsprechende Fehlerhinweise ausgeben.
3. In das Installationsverzeichnis wechseln, default: "/opt/unify/OpenScapeCTI"
4. Den folgenden Eintrag in `/etc/hosts löschen:`
   `127.0.0.2 servername.domain.com servername`
5. Den Konfigurator aufrufen
   `./bin/tools/configure.sh`
   oder explizit
   `/opt/unify/OpenScapeCTI/bin/tools/configure.sh`

   Der configure.sh Konfigurator speichert die Host-Name und die IP-Adresse des PC, darauf die Installtion durchgefuehrt wird, in Konfigurationsdateien.
   Abhängig von der Linux-Systemkonfiguration sowie der Arbeitsumgebung des Benutzers erscheint nun eine grafische Oberfläche (wenn ein X-Server läuft und der Benutzer dazu Zugang hat), die der grafischen Oberfläche der Windows-Installation gleicht, oder eine textbasierte Oberfläche. Damit ist es möglich, CAP auch remote mittels einer ssh-Verbindung o.ä. zu installieren und zu konfigurieren.
6. Die Konfiguration durch Drücken der Verify Taste überprüfen.

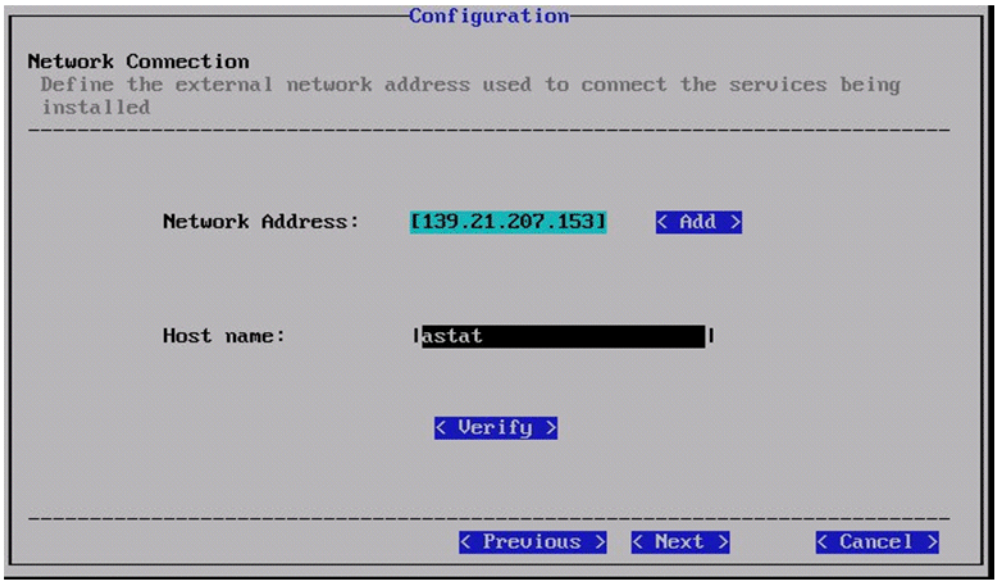
Die grafische Konfigurationsoberfläche wurde im Windows-Umfeld bereits beschrieben. Hier werden deshalb nur die Abweichungen der textbasierten gegenüber der grafischen Konfigurationsoberfläche aufgezeigt.

7	Die Konsole zur textbasierten Konfiguration muss einen Mindestumfang von 80x25 Zeichen besitzen, da es sonst zu Darstellungsfehlern kommen kann.

Die textbasierte Konfiguration lehnt sich sehr stark an die grafische Konfiguration an, hat jedoch auf Grund der beschränkten Darstellungsmöglichkeiten einige Besonderheiten:

- Die Navigation erfolgt grundsätzlich mit den Cursortasten. Eingaben per Maus werden nicht unterstützt.
- Die Auswahl einer Checkbox ([ ]) erfolgt mittels Leertaste. Zur Betätigung eines Buttons (blau) ist die Return / Enter-Taste zu verwenden.
- Die Reihenfolge der Konfigurationsdialoge ist mit der Reihenfolge in der grafischen Konfiguration identisch.

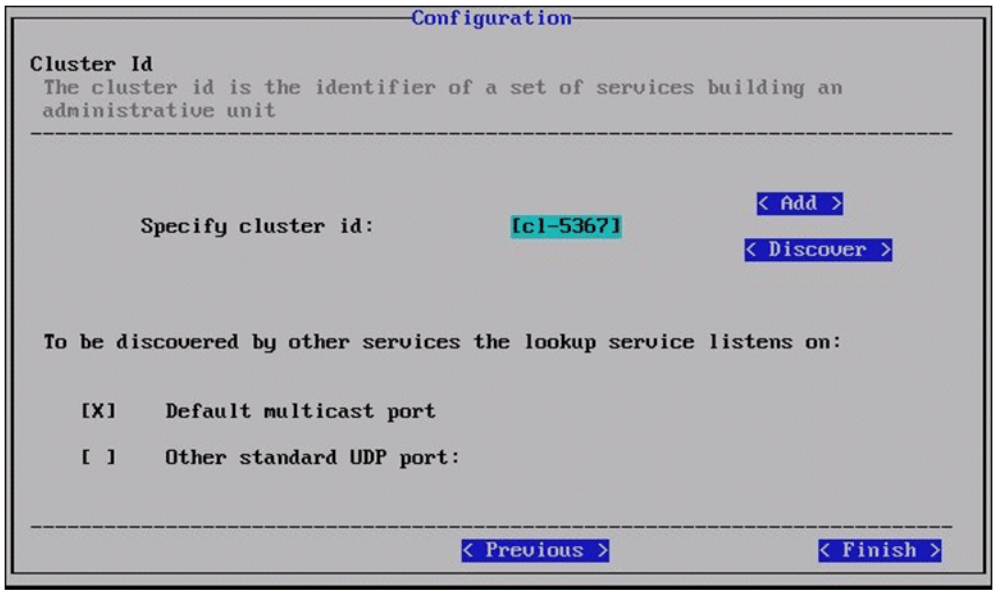
Netzwerkdialog



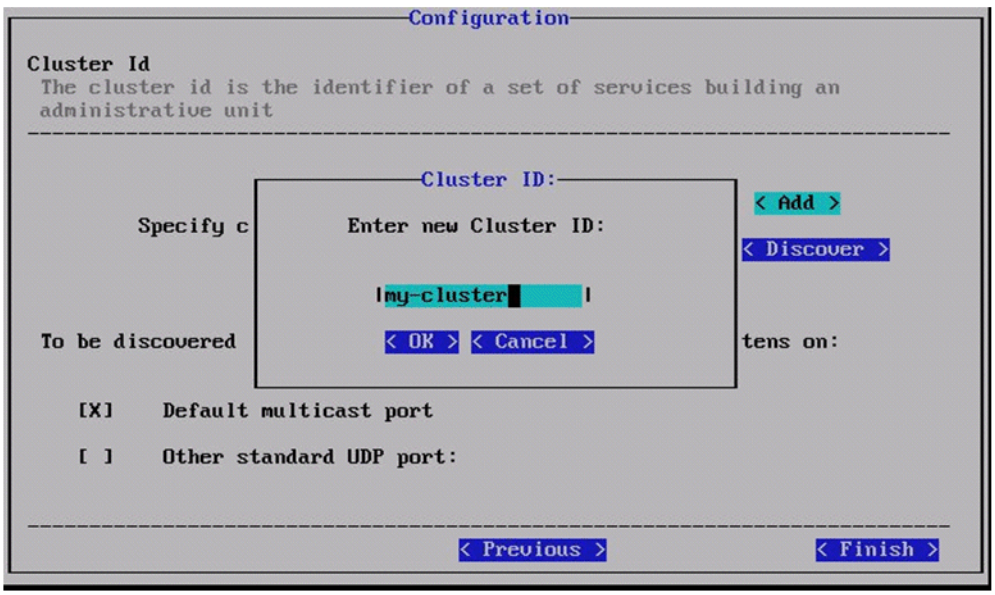
Im Feld "Network Address" wird ein Pull-Down-Menü angeboten, das über Return / Enter geöffnet werden kann. Die Auswahl erfolgt über Cursortasten und Return / Enter zur Bestätigung.

Sollte die gewünschte IP-Adresse nicht in der Liste verfügbar sein, so kann über den Button <Add> eine IP-Adresse hinzugefügt werden. Eine korrekt eingegebene IP-Adresse erscheint anschließend in dem vorher erwähnten Pull-Down-Menü.

Clusterdialog



Im Feld Cluster-ID wird wieder ein Pull-Down-Menü angeboten. Um eine eigene Cluster-ID zu definieren, ist wieder der <Add> Button zu verwenden.



Der Eintrag findet sich anschließend im Pull-Down-Menü wieder.

Alle weiteren Funktionen sind identisch zum grafischen Konfigurationsdialog.

4.4.2 Start und Stop von OpenScape CAP-Diensten unter Linux

Die Steuerung von CAP-Diensten unter Linux erfolgt wie üblich über den init daemon:

`/opt/unify/OpenScapeCTI/bin/tools/cti.rc [start|stop|forced_stop|status|restart]`
für die CAP-Dienste auf dem Server-PC

`/opt/unify/OpenScapeCTI/bin/tools/cti.rc [start|stop|forced_stop|status|restart]`
für die CAP-Dienste auf dem Starter-PC

`start` - Start des Dienstes

`stop` - Anhalten des Dienstes über "soft shutdown"

`forced_stop` - Anhalten des Dienstes über "kill"

`status` - Zustandsabfrage

`restart` - entspricht stop mit anschließendem start

4.4.3 Upgrade-Installation unter Linux

Die Upgrade-Installation ist der Installation ähnlich. (Siehe vorhergehenden Abschnitt.)

4.4.4 Deinstallation unter Linux

1. Als "root" auf dem Linuxsystem anmelden
2. Übersicht installierter CAP-Pakete anzeigen
   `rpm -q -a | grep CAP`
   (-q für "query", -a für "all")
3. Gewünschte rpm-Pakete deinstallieren: ertens doc und Scc Paketen, dann mgmt und Basis.
   `rpm -e -v <paket_1> [ <paket_2> ...]`
   (-v für verbose / ausführliche Information)

   Sollen alle installierten CAP-Pakete in einem Schritt deinstalliert werden,
   so können die beiden Schritte kombiniert werden zu
   `rpm -e -v $(rpm -q -a | grep CAP)`

4.4.5 Weitere Besonderheiten unter Linux

Bei Nutzung der web-basierten OpenScape CAP Management-Bedienoberfläche in einem Browser auf Linux-Systemen gibt es keine Unterschiede gegenüber Windows-Systemen.

Lediglich die Nutzung das Diagnose-Agenten erfordert gesonderte Aufmerksamkeit: Damit der Diagnose-Agent im Browser korrekt gestartet werden kann, muss auf dem jeweiligen System / Browser ein Plugin für JRE installiert sein. Diese Installation ist auf Linux-Systemen aus Sicherheitsgründen üblicherweise dem Administrator vorbehalten und wird deshalb nicht "on-the-fly" durchgeführt, wenn beim Start des Diagnose-Agenten festgestellt wird, dass das Plugin nicht installiert ist.

Wenn also beim Start des Diagnose-Agenten auf einem Linux-System Probleme auftreten, sollte der Administrator des entsprechenden Systems das Vorhandensein des passenden Plugins überprüfen; gegebenenfalls kann es über einen Link in die CAP-Installation verfügbar gemacht werden:

```
ln -s /opt/unify/OpenScapeCTI/jre/plugin/i386/ns7/libjavaplugin_o-
ji.so
      <MOZILLA_ROOT>/lib/plugins
```

4.5 Weitere Installations-Pakete

Es gibt einige weitere Pakete die wegen einfacherer Bedienbarkeit bzw. aus implementierungstechnischen Gründen nicht in den CAP MSI-Installer integriert sind.

OpenScape CAP TAPI Service Provider

Für Applikationen, die die TAPI-Schnittstelle der CAP nutzen wollen, ist auf dem jeweiligen Client-Rechner lokal der TAPI Service Provider zu installieren.

Rufen Sie zum Starten der Installation aus dem Software-Verzeichnis der CAP-CD `setupTapi.exe` auf. Details zur Installation und Konfiguration von TAPI sind in der separaten Dokumentation zum TAPI Service Provider enthalten, die ebenfalls Teil der CAP-CD ist.

4.6 Generelles Vorgehen zur Installation

Bei allen Installations-Varianten über den CAP.msi - Installer ist wie folgt vorzugehen:

1. Legen Sie die Installations-CD in das CD/DVD-Laufwerk des betreffenden PC ein. Starten Sie die Installation durch Doppelklick auf folgende Datei:

   `<CD/DVD-Laufwerk>:\software\CAP.msi`

2. Bestätigen Sie das Begrüßungsfenster mit **Next** und stimmen Sie den Lizenzbedingungen zu. Klicken Sie auf die Schaltfläche **Next**.

3. Wählen sie den passenden Setup-Typ und folgen Sie den Anweisungen auf dem Bildschirm.

4. Bei der Installation können Sie bei Bedarf das Installationsverzeichnis ändern.

   Das Standard-Installationsverzeichnis ist “`Programme\Unify\OpenScapeCTI`“.

   Falls Sie einen anderen Pfad wählen, beachten Sie bitte, dass als letzte Ebene immer automatisch `OpenScapeCTI` angehängt wird.

   Das Installationsverzeichnis wird im folgenden *<InstDir>* genannt.

5. Nun werden die Software-Komponenten installiert und alte Daten ggf. migriert.

   Belassen Sie die vorgegebene Einstellung auf “All services run on this host”.

   Der <PC Name> als eindeutige CAP Cluster-ID kann nachträglich in der folgenden Datei gesetzt werden:

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

   Der Eintrag lautet:

   ```
   args: "<PC-Name>/TelasWebStarter"
   ```

   Dieser Eintrag kann nach der Installation manuell geändert werden und wird nach einem Neustart des Dienstes "OpenScape CTI" aktiviert.

6. Sind mehrere Netzwerkkarten in Ihrem PC installiert (z.B. 1x für Zugang zum Netzwerk und 1x für Zugang zum Kommunikationssystem), müssen Sie die IP-Adresse auswählen, auf der die CAP Prozesse gestartet werden. In diesem Fall ist die IP-Adresse des Kunden-LAN auszuwählen. Ist nur eine Netzwerkkarte installiert, so ist keine Auswahl erforderlich.

   Der <PC Name> und die <IP Adresse> für die zu startenden Prozesse der CAP können nachträglich in den folgenden Dateien gesetzt werden:

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

Die Einträge lauten:

```
args: -localAddr
args: "<PC Name>/<IP Adresse>"
```

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

Die Einträge lauten:

```
<?x set INST_HOST = "<PC-Name>" ?>
<?x set INST_IP = "<IP-Adresse>" ?>
```

`<InstDir>\/startMenu/startPageAdmin`
Passen Sie die URL hinter dem Link an wie unterstrichen
`http://<PC-Name>:8170/`

Diese Einträge können nach der Installation manuell geändert werden und werden nach einem Neustart des Dienstes “OpenScape CTI” aktiviert.

7. Vervollständigen Sie die Installation, indem Sie die abschließenden Anweisungen am Bildschirm befolgen.
8. Starten Sie den PC neu.

Nun sind die Server-Komponenten **OpenScape CAP Management**, **Call Control Proxy** (SCCP) und **Call Control Service** (SCC) entsprechend der vorherigen Auswahl auf dem PC bereitgestellt. Wie Sie die Komponenten einrichten, erfahren Sie in Kapitel 6, “Konfiguration mit OpenScape CAP Management”.

Überprüfen der erfolgreichen Installation

Nach dem erfolgreichen Start des Dienstes "OpenScape CTI" kann eine Verbindung über einen Web Browser mit dem CAP Management aufgebaut werden.

Mit den folgenden Schritten können Sie überprüfen, ob die Installation erfolgreich verlaufen ist.

1. Überprüfen Sie über **Systemsteuerung | Verwaltung | Dienste**, ob der neue Windows Dienst “OpenScape CTI” hinzugefügt wurde. Nach dem Neustart des PCs sollte dieser Service bereits automatisch gestartet worden sein. Wenn Sie die Überprüfung ohne vorherigen Neustart durchführen, können Sie hier den Service “OpenScape CTI” jetzt auch manuell starten.
2. Verbinden Sie sich über einen Web-Browser mit dem OpenScape CAP Management aus dem Startmenü über **Start | Programme | OpenScape CAP | Management** oder über direkten Zugriff auf folgende Adresse: `http://<CAP Management PC>:8170/`

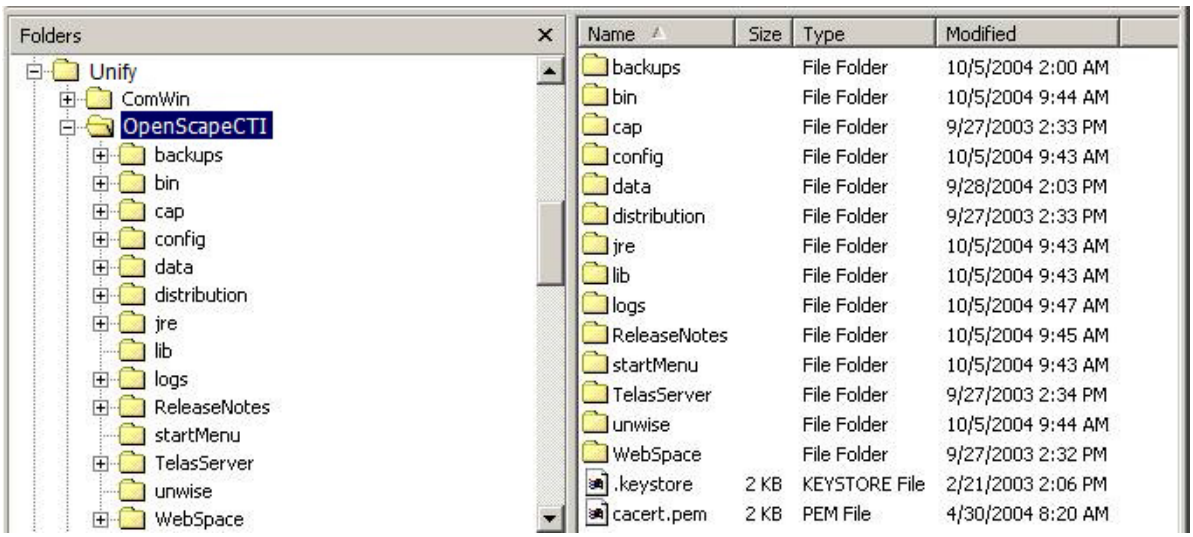
> Die Verbindung zwischen Web-Browser und CAP Management kann auch im SSL-Mode betrieben werden. Dazu muss in der Datei
> `<InstDir>\config\common\ports.cfg`
> der Parameter `<?x set CAP_SEC_MODE = "OFF" ?>` auf
> `<?x set CAP_SEC_MODE = "FULL" ?>` geändert werden.
> Danach muss der Dienst "OpenScape CTI" neu gestartet werden. Nun kann das CAP Management über den Default-Port `8470` adressiert werden:
> `https://<CAP Management PC>:8470/.`

Authentifizieren Sie sich am OpenScape CAP Management mit Benutzername **`Admin`** und Passwort **`Admin`**. Beachten Sie dabei die Groß-/Kleinschreibung. Benutzername und Passwort sollten später geändert werden. Falls eine Migration alter Daten erfolgt ist, gilt natürlich das Passwort der alten Version.

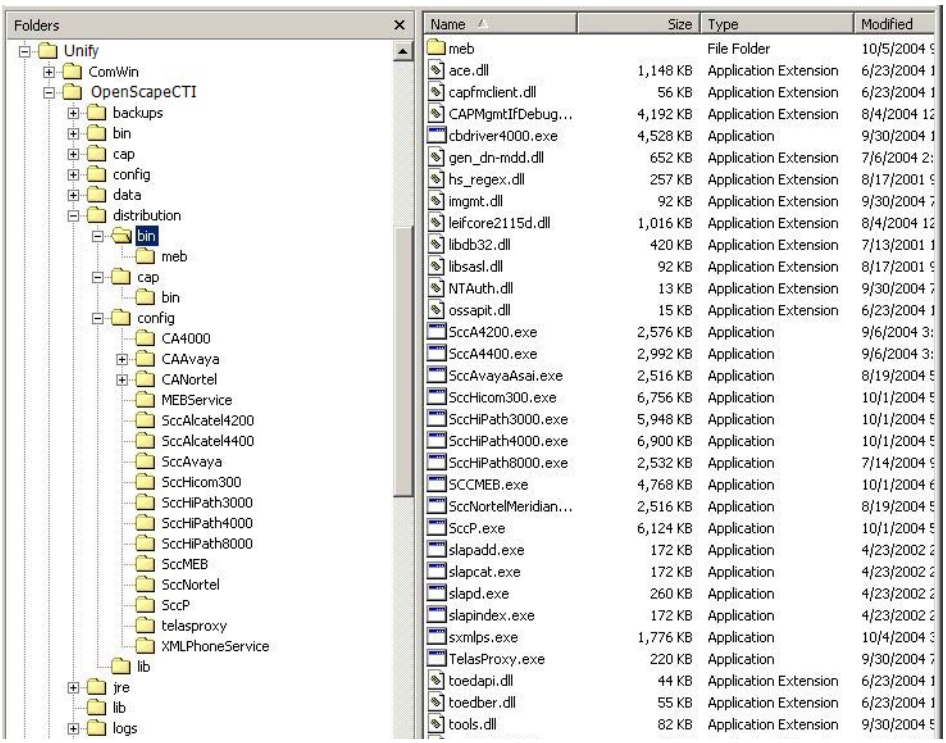
Nach einer erfolgreichen Authentifizierung des Benutzers “Admin” erscheint die Oberfläche des CAP Managements (siehe Kapitel 5, “Arbeitsbereich”). Wählen Sie z.B. im Hauptmenü den Menüpunkt **Hilfe** und klicken Sie in der angebotenen Liste auf **CAP Serviceanleitung (HTML)**. Es öffnet sich die Online-/HTML-Version der CAP Serviceanleitung.

3. Nun können Sie die Installation auch im Dateisystem überprüfen; bitte beachten Sie, dass die im folgenden gezeigten Bildschirmabzüge aus einer Beispiel-Installation entnommen wurden; konkrete, "echte" Installationen können in Details anders aussehen.

   Das Installationsverzeichnis für den CAP Management-Kern ist standardmäßig
   `C:\Programme\Unify\OpenScapeCTI\`



   Das Installationsverzeichnis der CAP Call Control Services ist standardmäßig
   `<InstPfad>\distribution\`

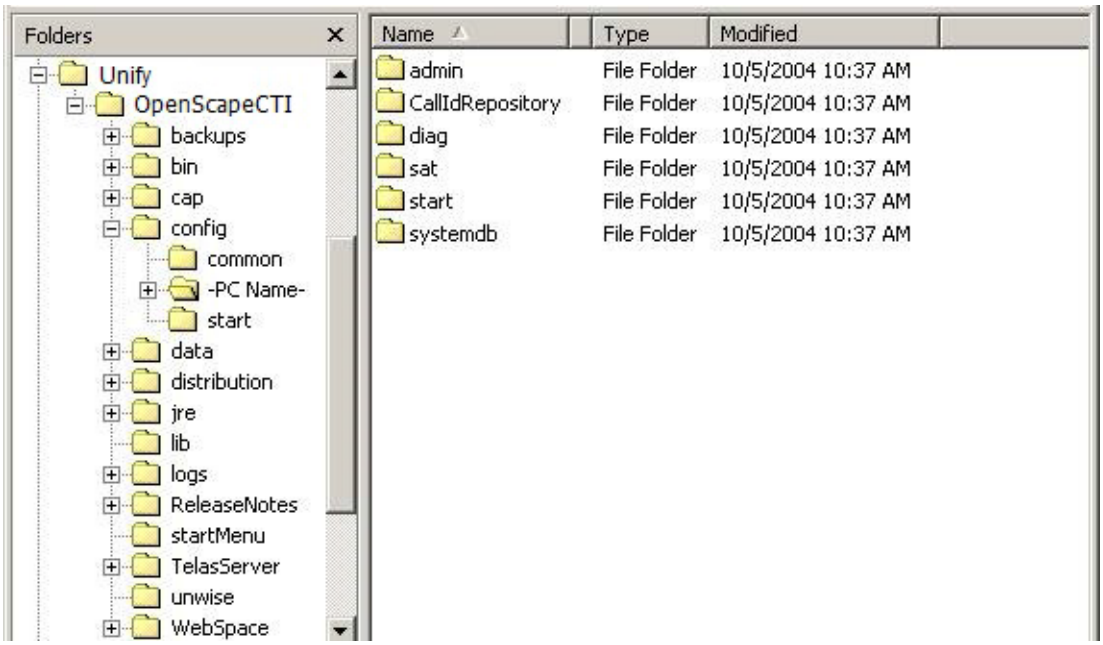


In dem Verzeichnis `distribution` existieren weitere Unterverzeichnisse. Im Verzeichnis `distribution\bin` befinden sich die ausführbaren Programme SCC/SCCP. Im Verzeichnis `distribution\config` befinden sich die Konfigurationsdateien `telas.cfg` des SCC/SCCP, aufgeteilt in individuelle Unterverzeichnisse

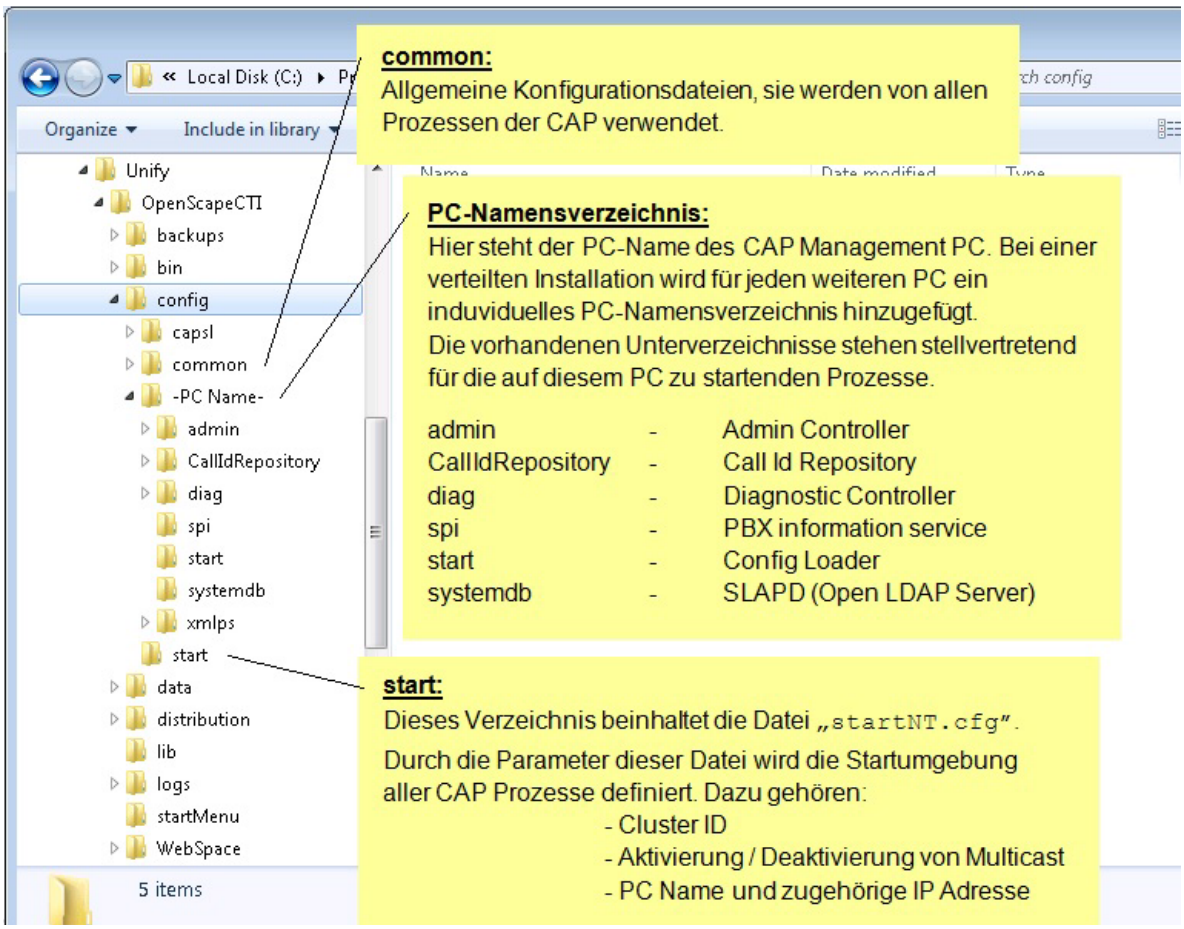
Von hier aus werden die SCC/SCCP im gesamten CAP-Cluster in Abhängigkeit von der Konfiguration verteilt, d.h. die Installation der Komponente SCC/SCCP erfolgt immer nur einmalig auf dem CAP Management-PC, egal ob auf diesem auch eine dieser Komponenten später aktiv ist oder nicht! Sollten zu einem späteren Zeitpunkt die ausführbaren Programme SCC/SCCP im Rahmen einer Fehlerbehebung ausgetauscht werden, so geschieht dieses ausschließlich im Verzeichnis `distribution\bin`. Danach werden alle Dienste im CAP-Cluster neu gestartet und eine Verteilung der neuen Programmversionen wird automatisch durchgeführt. Das ist auch der Fall, wenn sich die gesamte Konfiguration nur auf einem PC befindet. Die Struktur der CAP macht dabei keinen Unterschied. Die gleiche Struktur und die gleiche Beziehung gilt auch für den XML Phone Service (XMLPS).

Die Konfigurationsdateien für sämtliche Komponenten eines CAP-Clusters befinden sich unter dem Verzeichnis
`<InstDir>\config\`

Alle diese Konfigurationsdateien befinden sich immer nur auf dem CAP Management-PC, auch bei einer verteilten Installation!

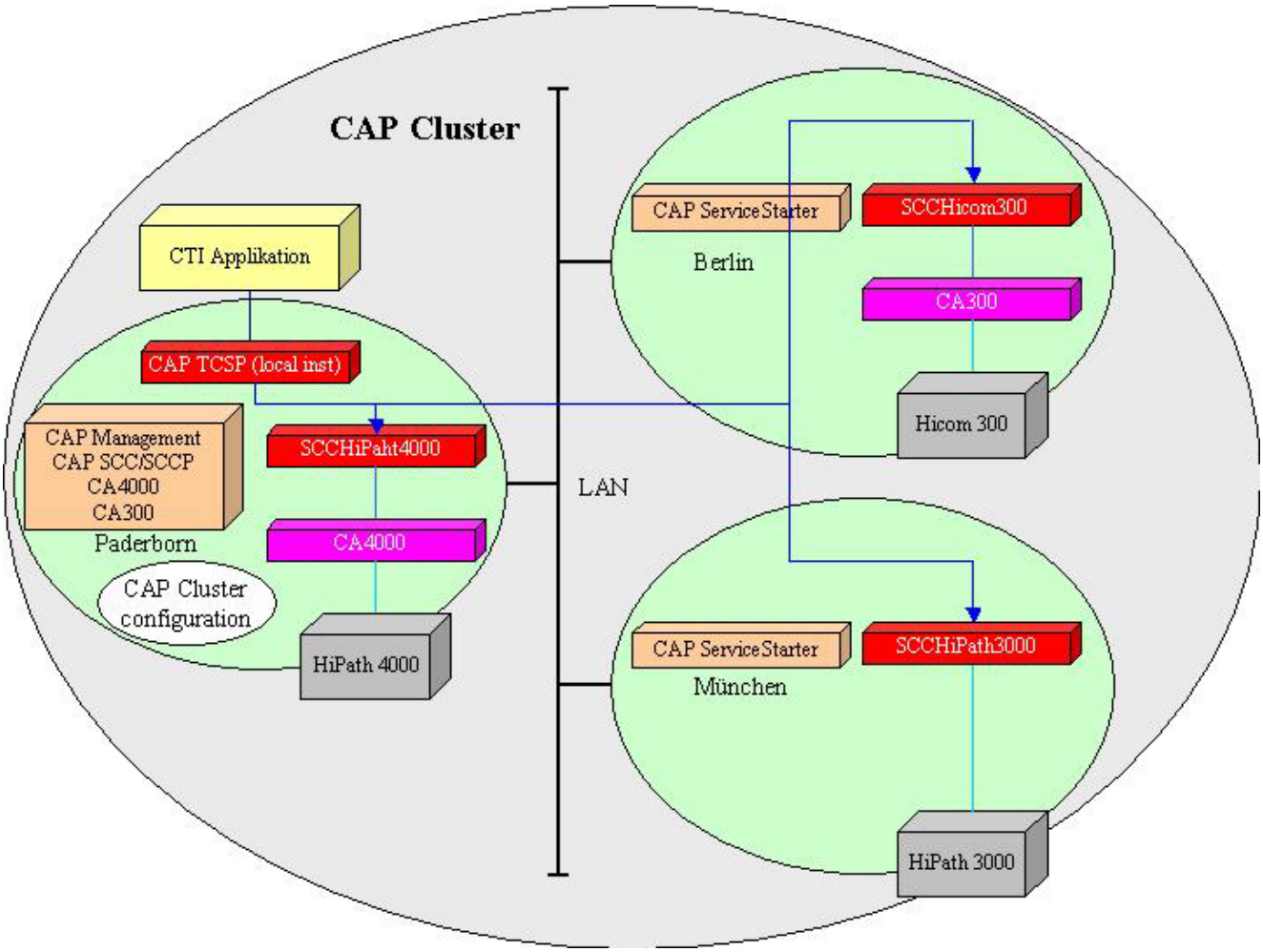


Es ist möglich, den Unterverzeichnissen im Konfigurationsverzeichnis `config` definierte Kategorien zuzuordnen.


common:
Allgemeine Konfigurationsdateien, sie werden von allen Prozessen der CAP verwendet.
PC-Namensverzeichnis:
Hier steht der PC-Name des CAP Management PC. Bei einer verteilten Installation wird für jeden weiteren PC ein induviduelles PC-Namensverzeichnis hinzugefügt.
Die vorhandenen Unterverzeichnisse stehen stellvertretend für die auf diesem PC zu startenden Prozesse.
admin - Admin Controller
CallIdRepository - Call Id Repository
diag - Diagnostic Controller
spi - PBX information service
start - Config Loader
systemdb - SLAPD (Open LDAP Server)
start:
Dieses Verzeichnis beinhaltet die Datei „startNT.cfg".
Durch die Parameter dieser Datei wird die Startumgebung aller CAP Prozesse definiert. Dazu gehören:
- Cluster ID
- Aktivierung / Deaktivierung von Multicast
- PC Name und zugehörige IP Adresse
Local Disk (C:)
Organize
Include in library
Unify
OpenScapeCTI
backups
bin
config
capsl
common
-PC Name-
admin
CallIdRepository
diag
spi
start
systemdb
xmlps
start
data
distribution
lib
logs
startMenu
WebSpace
5 items

4.7 Verteilte Installation

Wird eine Applikation mit mehreren TK-Anlagen an verschiedenen Standorten über eine CAP verbunden, so kann aus Netzlastgründen eine verteilte Installation eingerichtet werden. Dazu wird nur an einem Standort ("CAP Management PC") das CAP Management zusammen mit den CAP Call Control Services (SCC/SCCP) sowie CA4000 (falls benötigt) installiert. Dabei ist es unerheblich, ob auf dem CAP Management-PC später auch Instanzen von SCCP/SCC (und CA) oder XMLPS gestartet werden sollen. **Hicom 300 is nicht mehr unterstützt**..



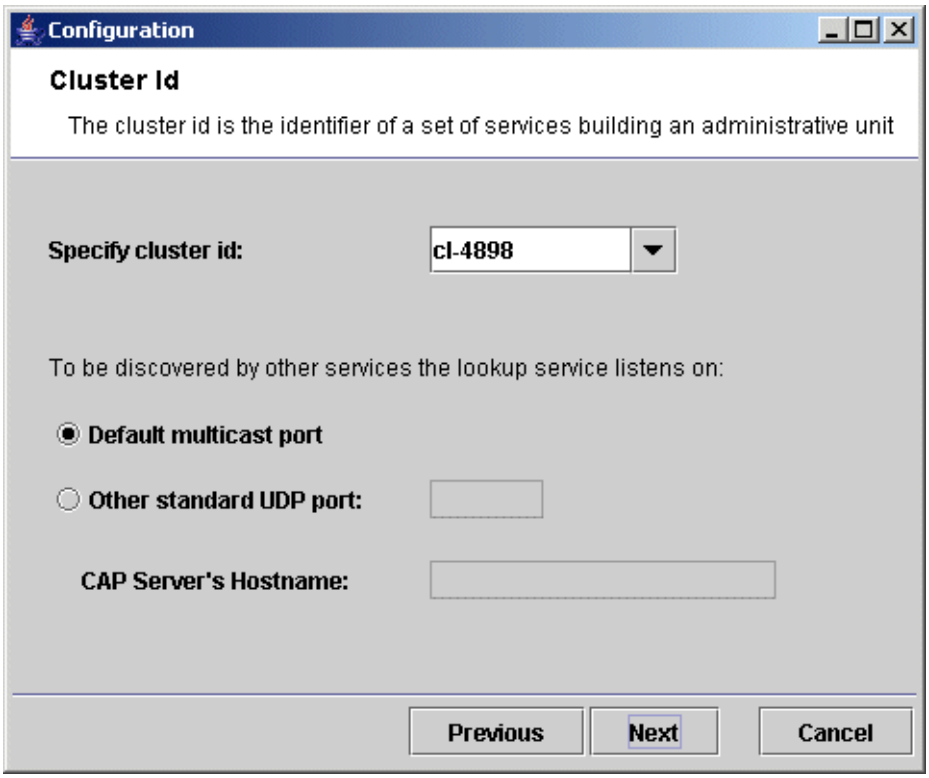
Die abgesetzten Rechner, auf denen Instanzen von SCCP/SCC (und CA) oder XMLPS laufen werden sollen, müssen dazu durch Installation des CAP Service Starter entsprechend vorbereitet werden (vgl. Abschnitt 4.3 und Abschnitt 4.6).

Zum Abschluss der Installation muss der Service Starter an einen vorhandenen CAP Management-Server angebunden werden; dies geschieht über Identifikation des entsprechenden CAP-Clusters.

Der Bediener wird zunächst aufgefordert, die Netzwerk-Schnittstelle zur externen Anbindung des Service Starter zu identifizieren (analog zum Ablauf in Abschnitt 4.6, Schritt 6). Dieses Interface wird anschließend genutzt, um die im Netzwerk vorhandenen Cluster zu ermitteln. Ein “Lookup Client“ schickt dazu ein Multicast in das LAN und versucht, dort vorhandene CAP Management Lookup Services zu finden.

Die gefundenen Lookup Services mit ihrer Cluster-ID werden zur Auswahl angeboten. Wählen Sie die Cluster-ID des zugehörigen CAP Managements aus oder geben Sie diese manuell ein.

> Falls die Cluster Id des zugehörigen CAP Managements nicht angeboten wird, so muss die Kommunikation zwischen CAP Management und CAP Service Starter von Multicast auf eine feste IP-Adresse:UDP-Port geändert werden. Folgen Sie dazu den Anweisungen in dem Abschnitt “Deaktivierung von Multicast”.



Die CAP Cluster-ID kann nachträglich in der folgenden Datei gesetzt werden:

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

Der Eintrag lautet:

```
args: "<PC-Name>/TelasWebStarter"
```

wobei <PC-Name> als Synonym für die Cluster-ID verwendet wird. Dieser Eintrag kann nach der Installation manuell geändert werden und ist nach einem Neustart des Dienstes **OpenScape CTI** aktiv.

Zum Abschluss der Service Starter-Installation starten Sie den Service **OpenScape CTI** über

– **Systemsteuerung | Verwaltung | Dienste**

Damit ist die Installation auf dem abgesetzten PC abgeschlossen.

Der Service Starter-Prozess wird bei jedem Hochlauf des PC automatisch gestartet. Dabei nimmt er mit dem OpenScape CAP Management-PC Verbindung auf, ermittelt alle Daten zu den für den abgesetzten PC eingerichteten Komponenten, lädt die aktuellen Softwarestände und erforderlichen Konfigurationsdaten und startet die entsprechenden Prozesse.

> Starten Sie den Dienst **OpenScape CTI** erst nach einer vollständig durchgeführten Konfiguration von CAP-Komponenten (SCC, CA, SCCP, XMLPS) für diesen PC!

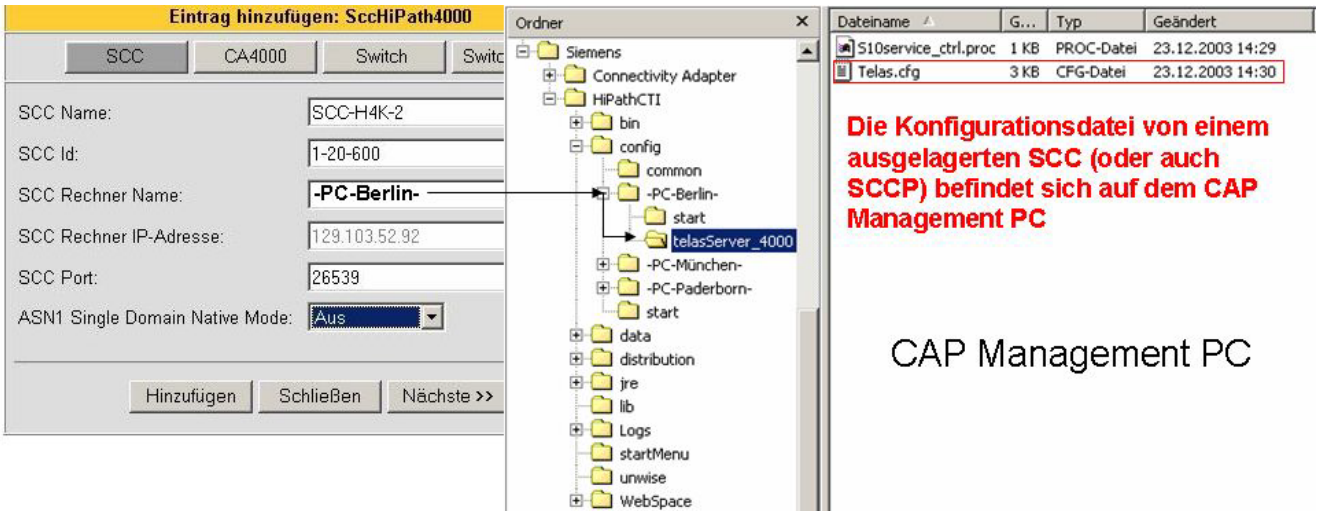
Nach der Installation

Bitte beachten Sie, dass (anders als beim zentralen CAP Management) nach der Installation auf dem abgesetzten Rechner keine Komponenten SCC, SCCP, CA4000, etc. im Verzeichnis `<InstDir>\bin` vorhanden sind.

Die Einrichtung der Komponenten für den abgesetzten Rechner erfolgt auf dem CAP Management-Rechner.

> Während der Konfiguration von SCC oder von SCCP muß das IP-Adresse des abgesetzten Rechners angegeben werden. Deswegen werden diese Tasks in der Diagnose-Agent nur gezeigt, wenn der abgesetzten Rechner mit Startersatz richtig konfiguriert ist und Lauft.

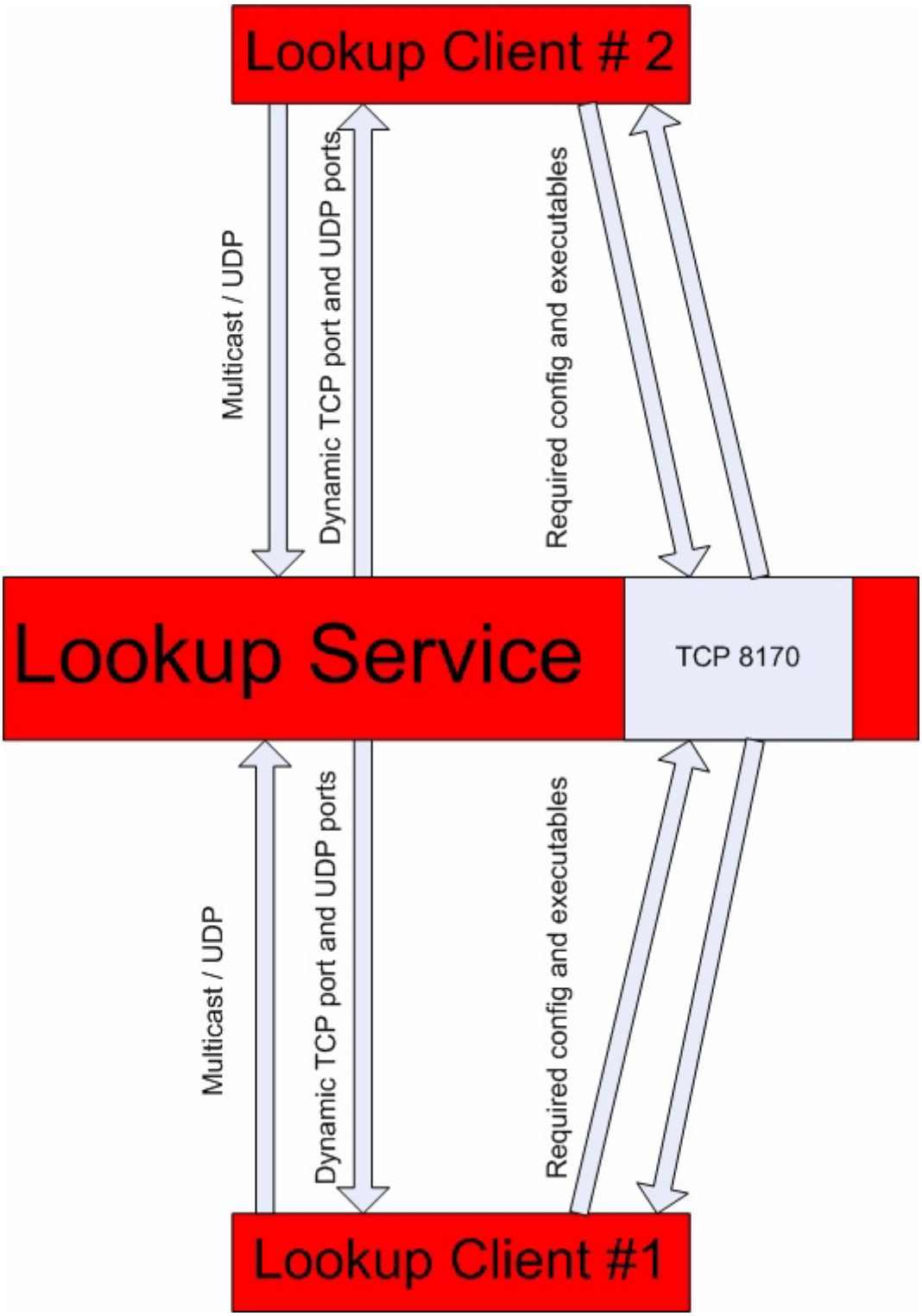
Es wird automatisch anhand des PC-Namens des abgesetzten Rechners auf dem CAP Management-PC im Verzeichnis <InstDir>\config\ ein neues Unterverzeichnis angelegt.



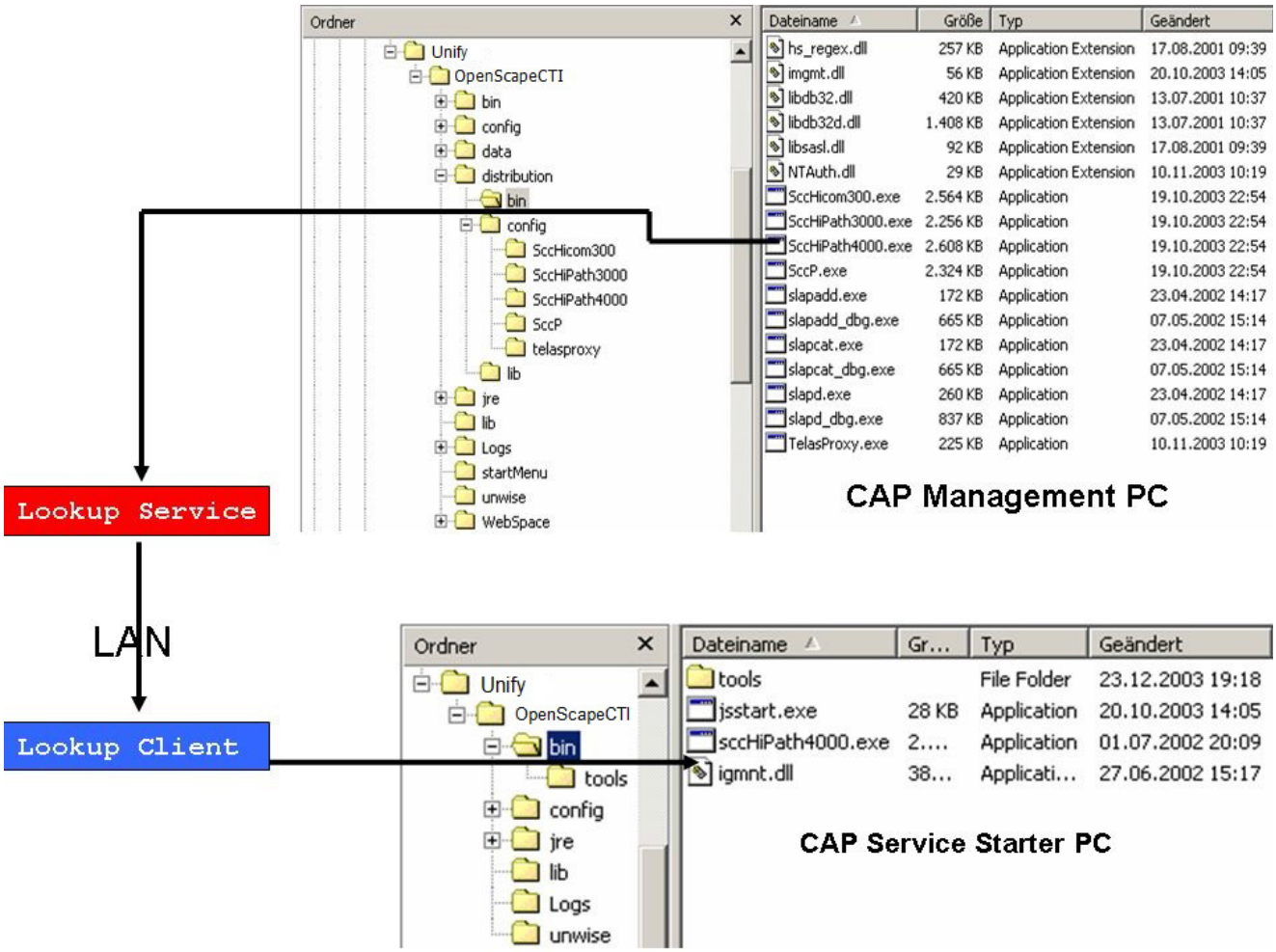
Die Einrichtung der Komponenten für den abgesetzten Rechner erfolgt auf dem CAP Management-Rechner; dazu wird automatisch anhand des PC-Namens des abgesetzten Rechners auf dem CAP Management-PC im Verzeichnis `<InstDir>\config\` ein neues Unterverzeichnis angelegt.

Dadurch verbleiben sämtliche Konfigurationsdateien aller ausgelagerten Prozesse in einem CAP-Cluster auf dem CAP Management-PC im Verzeichnis `<InstDir>\config\<PC-Name>\`

Die Übertragung dieser Durchgeführende Files laufen auf dem TCP Port 8170 von CAP Management PC, wie Sie die folgende Seite sehen können.


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

Aus diesem Verzeichnis werden der Konfiguration entsprechend die Programme auf die PCs übertragen, auf denen sie entsprechend der Konfiguration gestartet werden sollen.



4.8 Startreihenfolge der CAP Prozesse

In diesem Kapitel wird unterschieden, ob die CAP-Prozesse auf einer verteilten Installation oder einer nichtverteilten Installation laufen.

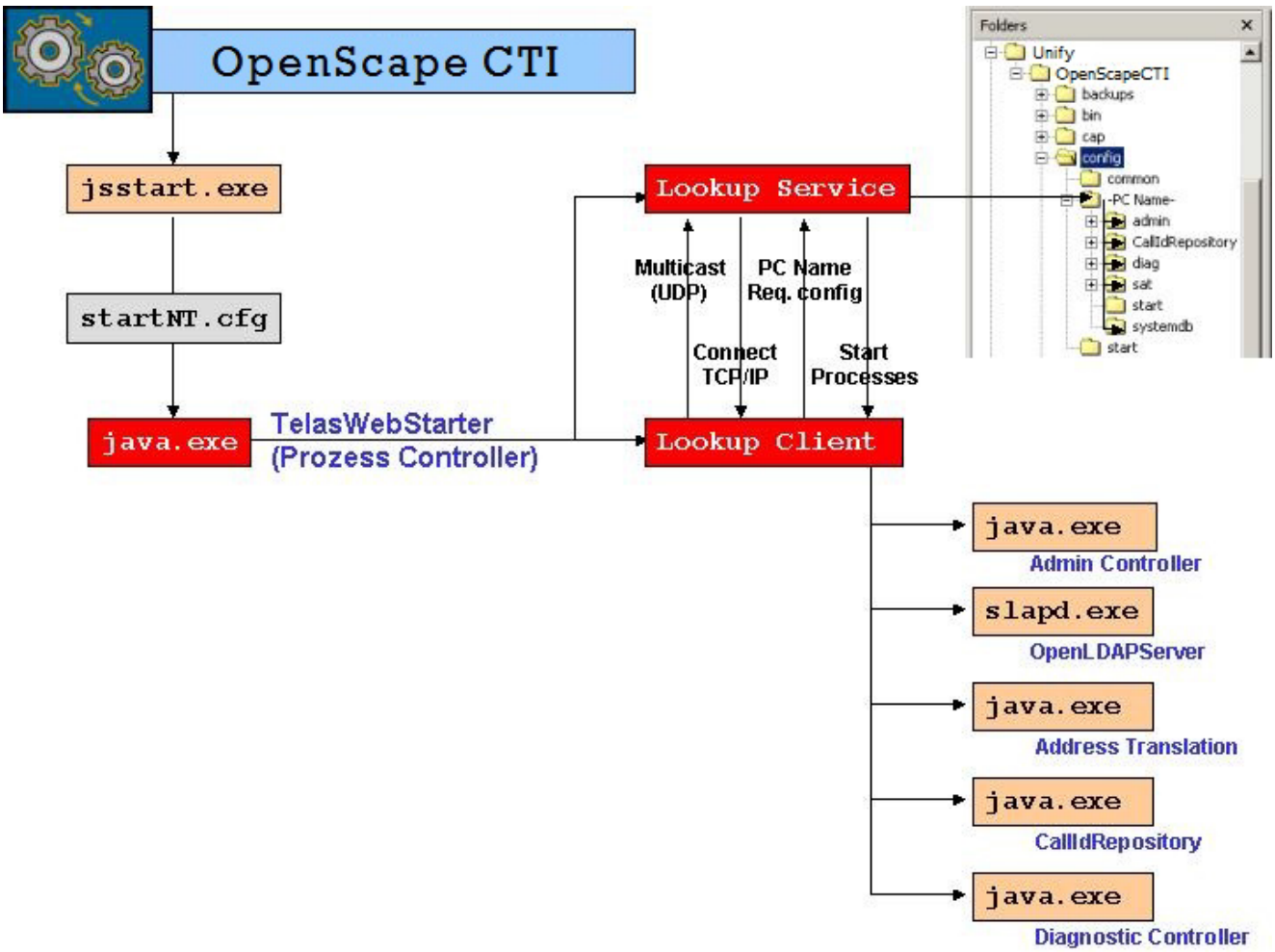
Bitte beachten Sie, das die gezeigten Bildschirmabzüge großzügig zu interpretieren sind - sie können für unterschiedliche reale Installationen / CAP-Versionen im Detail anders aussehen.

4.8.1 Nichtverteilte Installation

Der Dateistruktur folgend werden bestimmte Prozesse auf dem CAP Management-PC gestartet. Der Windows Dienst **OpenScape CTI** ist verknüpft mit dem Programm `jsstart.exe` (java Service Starter).

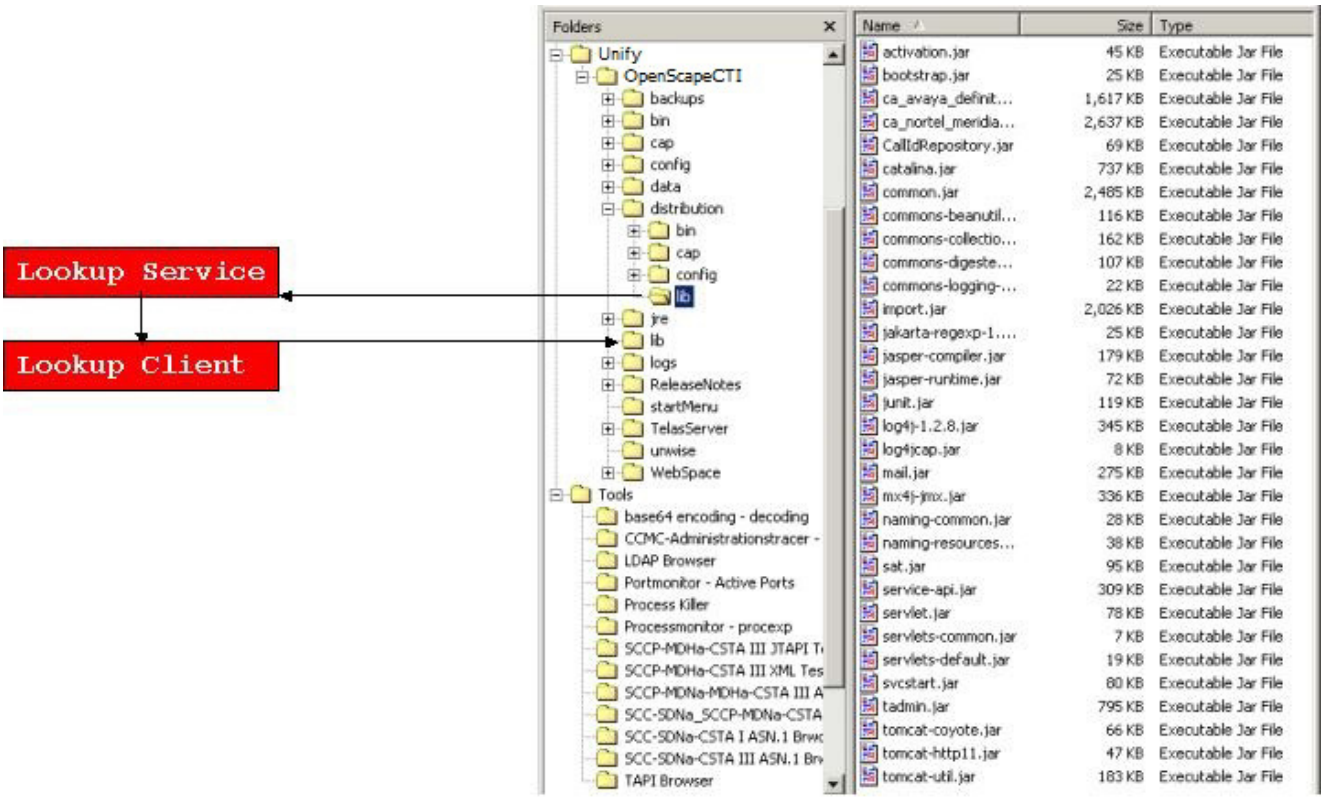
Die Startprozedur der CAP Prozesse

Die nachfolgende Grafik verdeutlicht die interne Struktur und die Zusammenhänge der CAP Prozesse, welche durch den Windows Dienst "OpenScape CTI" gestartet werden.



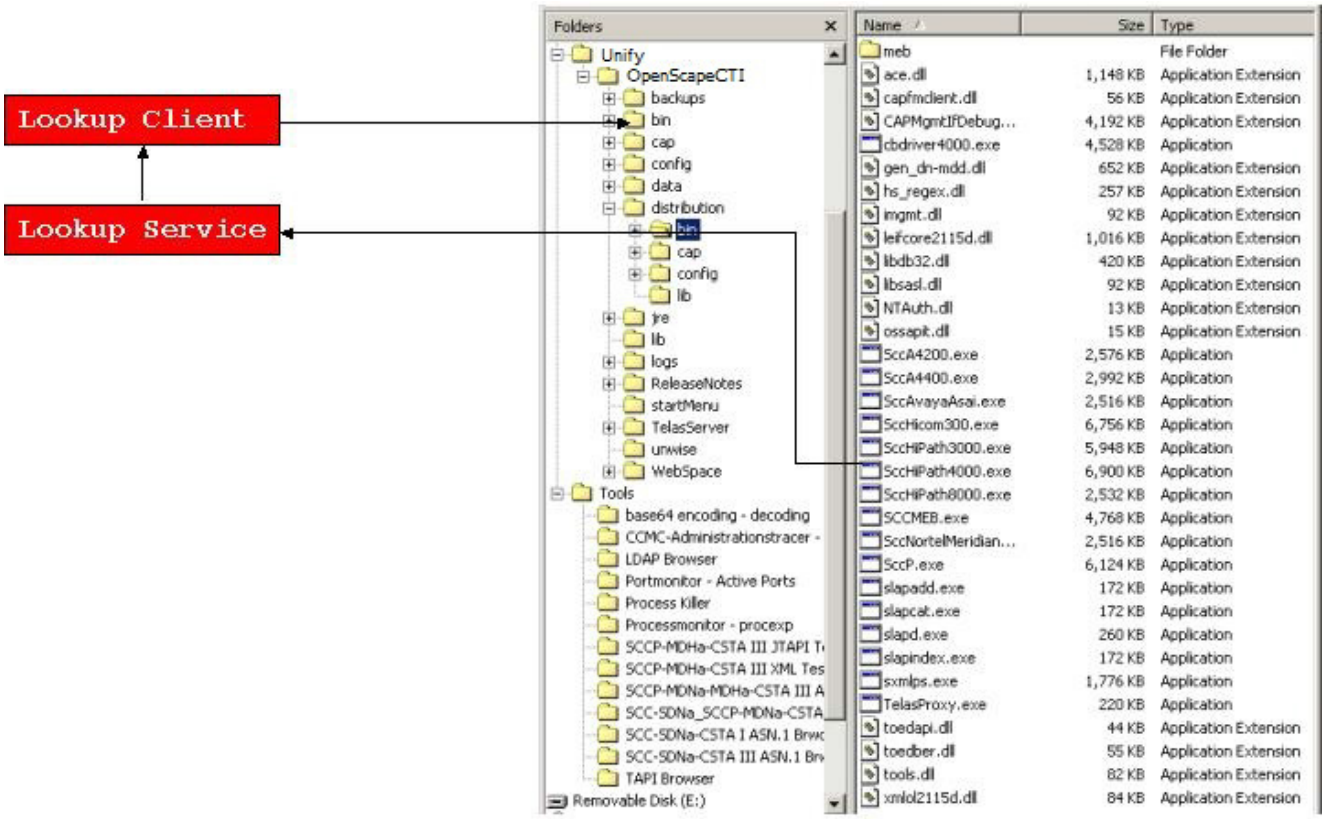
Der Windows Dienst “OpenScape CTI” startet den Prozess `jsstart` (Java Service Starter); der wiederum startet den ersten “java”-Prozess. Dieser “java”-Prozess hat die Bezeichnung “TelasWebStarter” und ist der Prozess-Controller des CAP-internen Service “Lookup Service” und “Lookup Client”.
Beide internen Services kennen sich zunächst gegenseitig nicht. Über ein “Multicast”, initiiert durch den “Lookup Client” (vergleichbar einem Broadcast, adressiert aber eine Class D IP-Adresse) muss dieser zunächst den im selben CAP-Cluster befindlichen “Lookup Service” finden.
Nach dem erfolgreichen Verbindungsaufbau überträgt der “Lookup Client” seinen lokalen PC-Namen dem “Lookup Service”. Dadurch wird eine Anforderung der Informationen bezüglich der zu startenden Prozesse an den “Lookup Service” gestellt, welcher diese Daten nachfolgend übermittelt. Alle ausführbaren Programme werden übertragen und die entsprechenden Prozesse gestartet.

Die erfolgreiche Übertragung kann anhand des Prinzips der Verteilung von ausführbaren Programmen nachvollzogen werden.



Durch diesen Mechanismus werden die “jar”-Dateien aus dem Verzeichnis
`<InstDir>\distribution\lib\`
in das Zielverzeichnis
`<InstDir>\lib`
kopiert. Hier befinden sich die Versionen der aktuell genutzten “jar”-Dateien.

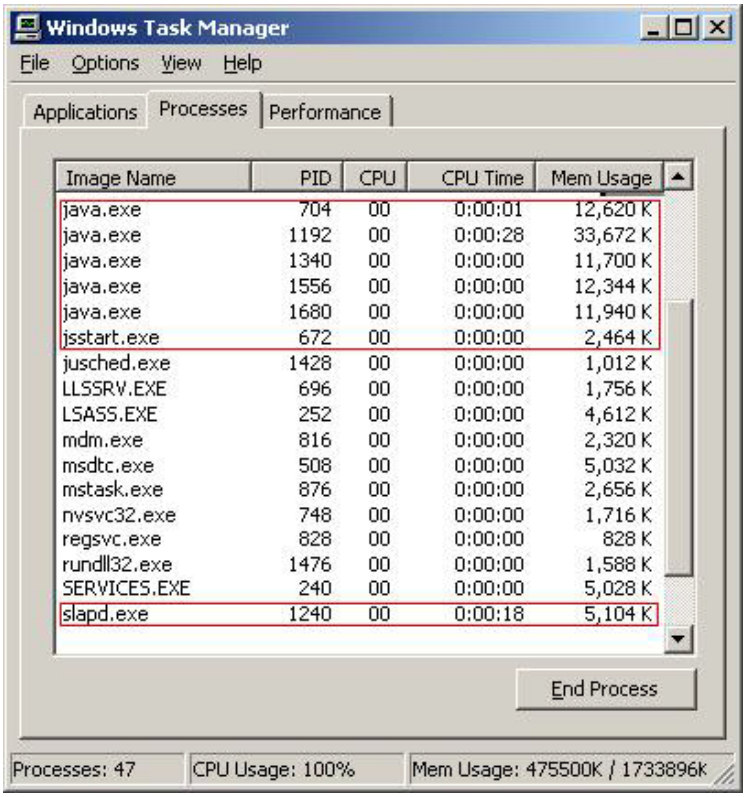
Das gleiche Prinzip wird auch bei der Verteilung des SCC/SCCP verwendet.



Durch diesen Mechanismus werden die “exe”-Dateien aus dem Verzeichnis
`<InstDir>\distribution\bin\`
in das Zielverzeichnis
`<InstDir>\bin`
kopiert. Hier befinden sich die Versionen der aktuell genutzten “exe” Dateien.

CAP Prozessübersicht auf dem CAP Management PC im Windows Taskmanager

Im Windows Taskmanager müssen folglich die Prozesse der CAP auf dem CAP Management PC ohne zusätzliche Konfiguration (z.b.: SCC, CA) erscheinen.
Dem entsprechend dürfen nach dem Stoppen des **Dienstes OpenScape CTI** diese Prozesse nicht mehr erscheinen! Ist dies trotzdem der Fall, müssen diese Prozesse manuell beendet werden.



Manuelles Beenden von CAP-Prozessen

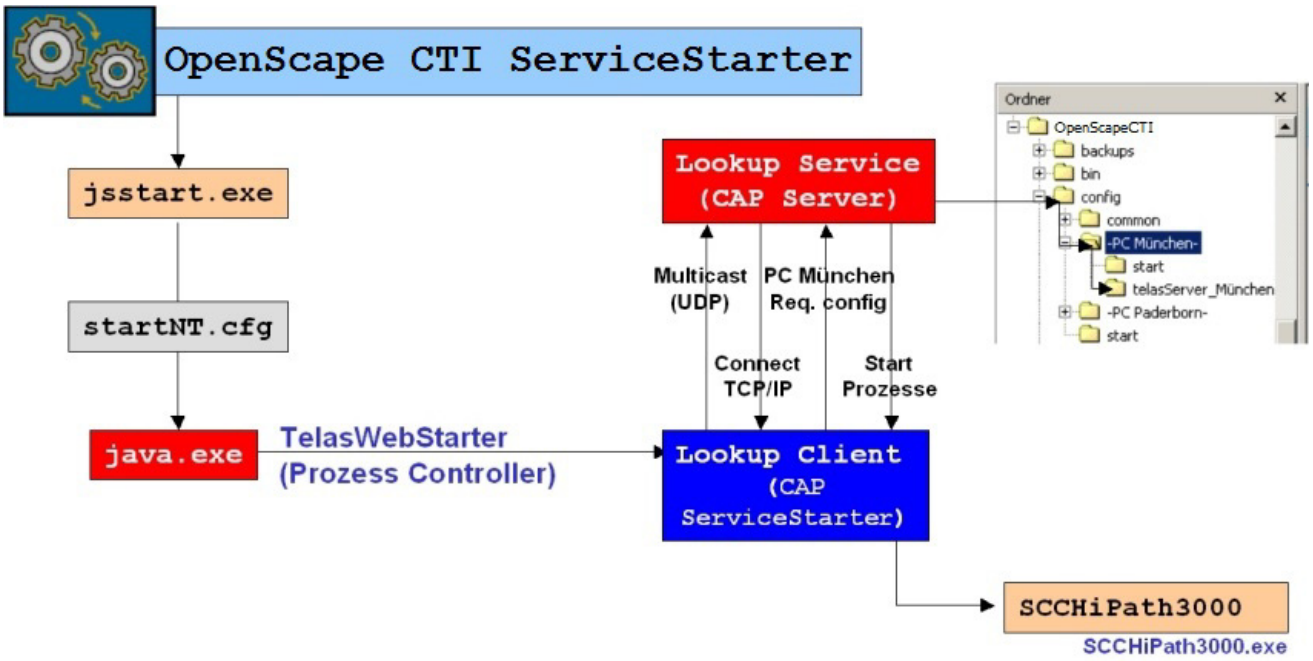
Die Prozesse der CAP können nicht durch die Funktion "Prozess beenden" beendet werden. Es ist gerade während der Installationsphase darauf zu achten, dass mit dem Stoppen des Dienstes "OpenScape CTI" auch alle Prozesse beendet werden. Es wird empfohlen (falls erforderlich), den Dienst zu stoppen und danach zu kontrollieren, ob auch alle Prozesse beendet wurden, und erst im Gutfall den Dienst neu zu starten.

Sollten CAP-Prozesse trotz gestopptem Dienst "OpenScape CTI" weiterhin laufen, so muss der PC neu gestartet werden.

> Durch das Programm "kill.exe" können diese Prozesse beendet werden. Ein PC-Neustart ist dann nicht erforderlich.

4.8.2 Verteilte Installation

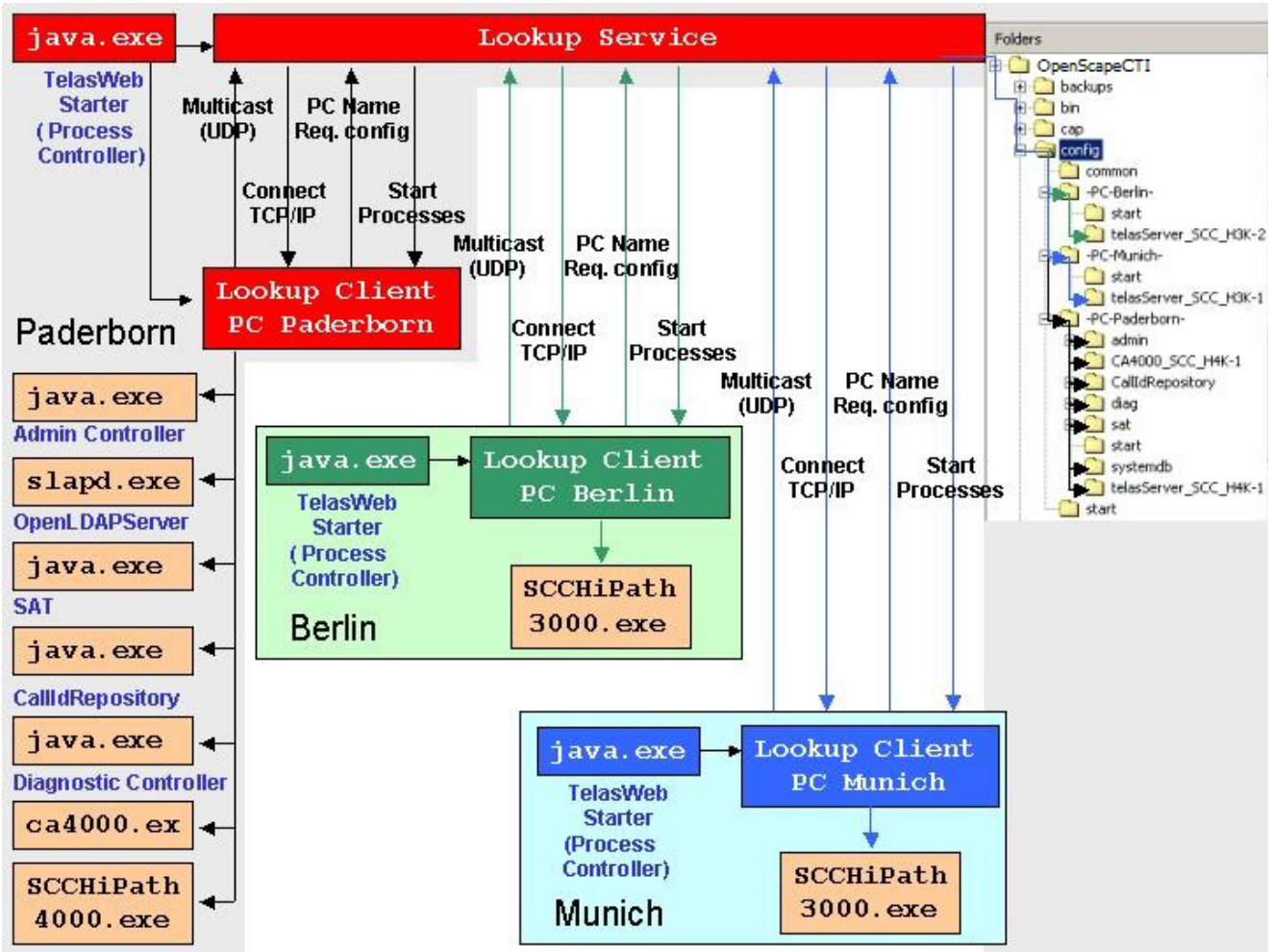
Der Dateistruktur folgend werden bestimmte Prozesse auf dem CAP Management-PC und dem CAP Service Starter-PC gestartet. Der Windows Dienst **OpenScape CTI** ist verknüpft mit dem Programm `jsstart.exe` (java Service Starter).



7	Der Dienst "OpenScape CTI" darf nicht vor der Konfiguration von verteilten Komponenten gestartet werden! Wird der Windowsdienst "OpenScape CTI" ohne eine, auf dem CAP Management PC vorhandene Konfiguration gestartet, so verbindet sich der Lookup Client (`java.exe`) des CAP Service Starter-PC mit dem Lookup Service des CAP Management-PC, übergibt seinen PC-Namen und erfragt die zu startenden, ausgelagerten Prozesse. Ist zu diesem Zeitpunkt keine Konfiguration vorhanden, so beendet sich der Lookup Client (`java.exe`) auf dem CAP Service Starter-PC und kann nur durch einen Neustart des Windows Dienstes "OpenScape CTI" neu gestartet werden.

Die Startprozedur der CAP Prozesse

Die nachfolgende Grafik verdeutlicht die interne Struktur und die Zusammenhänge der CAP Prozesse, welche auf dem CAP Management-PC sowie auf dem CAP Service Starter-PC jeweils durch den Windows Dienst "OpenScape CTI" gestartet werden.



Der Windows Dienst “OpenScape CTI” startet den Prozess “jsstart” (Java Service Starter); der wiederum startet den ersten “java”-Prozess. Dieser “java”-Prozess hat die Bezeichnung “TelasWebStarter” und ist der Prozess-Controller der CAP-internen Services “Lookup Service” und “Lookup Client”.

Beide internen Services kennen sich zunächst gegenseitig nicht. Über ein "Multicast", initiiert durch den "Lookup Client" (vergleichbar einem Broadcast, adressiert aber einen Class D IP-Adresse) muss dieser zunächst den im selben CAP-Cluster befindlichen "Lookup Service" finden.

Nach dem erfolgreichen Verbindungsaufbau überträgt der "Lookup Client" seinen lokalen PC Namen dem "Lookup Service". Dadurch wird eine Anforderung der Informationen bezüglich der zu startenden Prozesse an den "Lookup Service" gestellt, welcher diese Daten nachfolgend übermittelt.

Alle ausführbaren Programme werden übertragen und die entsprechenden Prozesse gestartet.

Nach dem gleichen Prinzip suchen auch die “Lookup Clients” der CAP Service Starter-PC nach dem “Lookup Service”. Wurde diese gefunden, wird die gleiche Prozedur gestartet wie intern auf dem CAP Management PC.

Automatische Verteilung der Komponente CAP SCC oder SCCP

In dem Verzeichnis `distribution` existieren weitere Unterverzeichnisse `distribution\bin` und `distribution\config`.

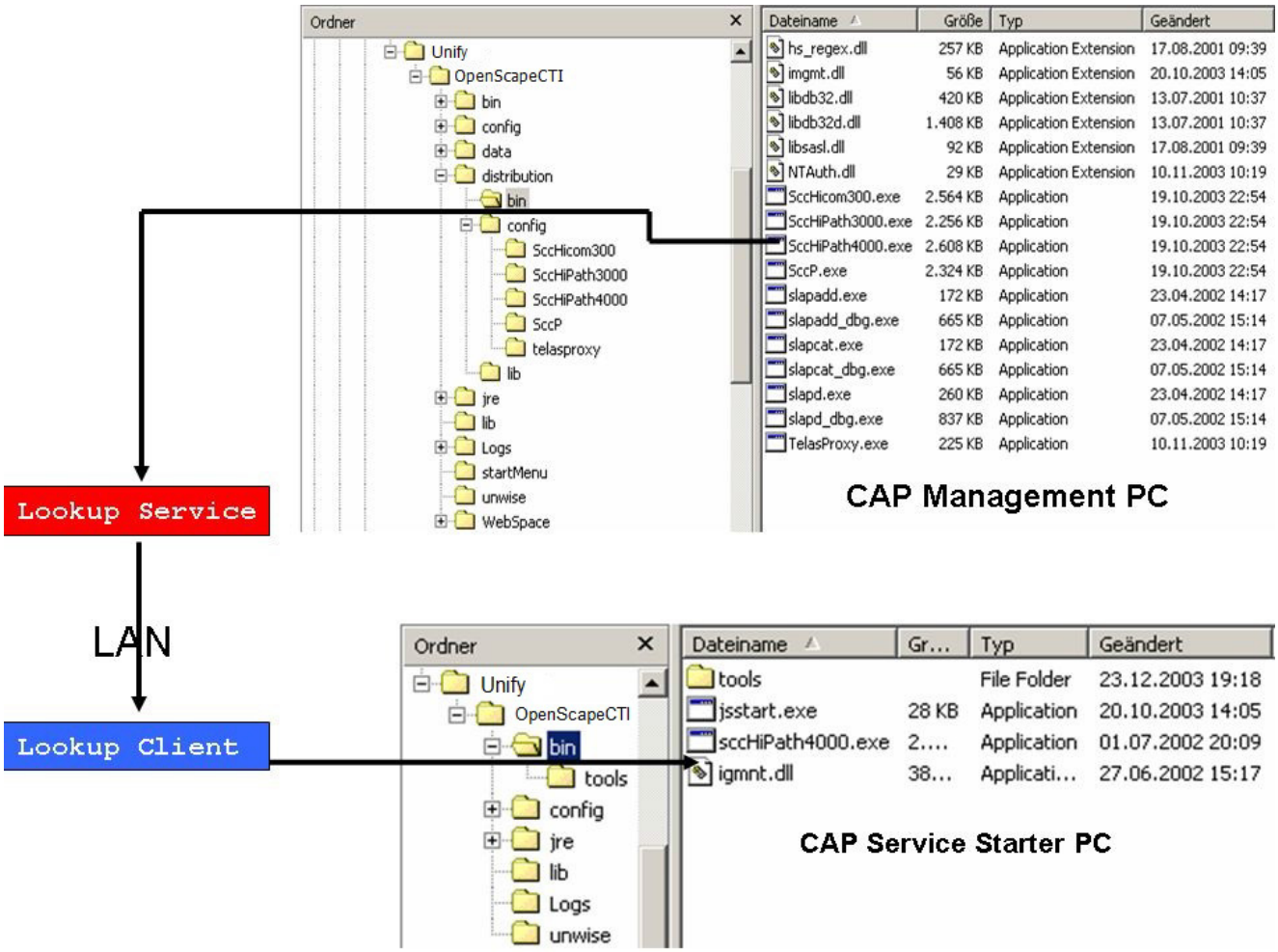
Im Verzeichnis `bin` befinden sich die ausführbaren Programme SCC/SCCP. Im Verzeichnis `config` die Konfigurationsdateien "telas.cfg" des SCC/SCCP, aufgeteilt in individuelle Unterverzeichnisse.

Von hier aus werden die SCC/SCCP im gesamten CAP-Cluster in Abhängigkeit von der Konfiguration verteilt, d.h. die Installation der Komponente SCC/SCCP erfolgt immer nur einmalig auf dem CAP Management-PC, egal ob auf diesem auch eine dieser Komponenten später aktiv ist oder nicht! Sollten zu einem späteren Zeitpunkt die ausführbaren Programme SCC/SCCP im Rahmen einer Fehlerbehebung ausgetauscht werden, so geschieht dieses ausschließlich im Verzeichnis `distribution\bin`. Danach werden alle Dienste im CAP-Cluster neu gestartet und eine Verteilung der neuen Programmversionen wird automatische durchgeführt. Das ist auch der Fall, wenn sich die gesamte Konfiguration nur auf einem PC befindet. Die Struktur der CAP macht dabei keinen Unterschied.

Die ausgewählte Komponente “CAP Call Control Service” wird bereitgestellt im Verzeichnis

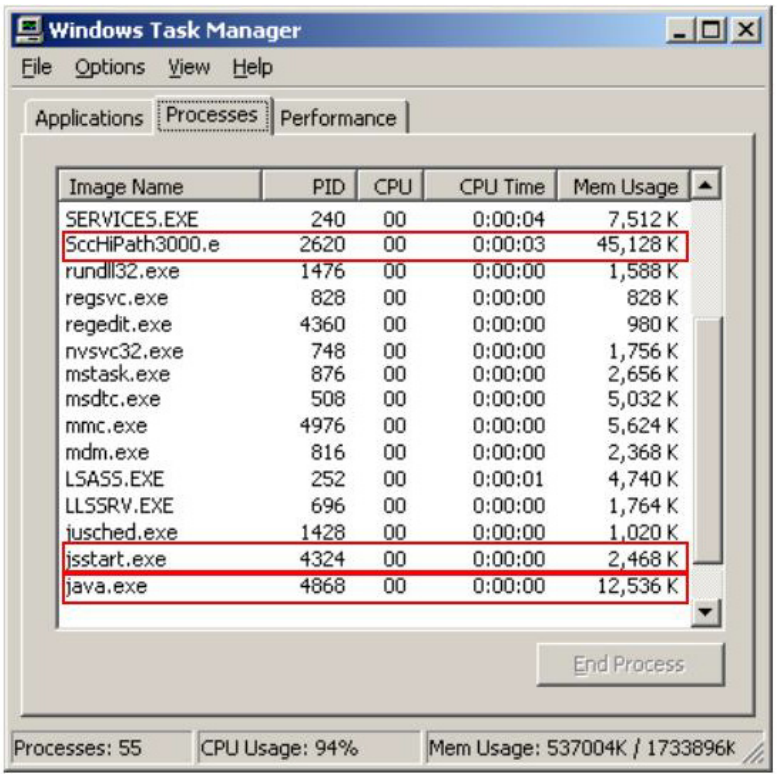
`<InstDir>\distribution\bin`

Aus diesem Verzeichnis werden die Programme auf die PCs übertragen, auf denen sie der Konfiguration folgend gestartet werden sollen.


Ordner
Unify
OpenScapeCTI
bin
config
data
distribution
bin
config
SccHicom300
SccHiPath3000
SccHiPath4000
SccP
telasproxy
lib
jre
lib
Logs
startMenu
unwise
WebSpace
Dateiname
Größe
Typ
Geändert
hs_regex.dll 257 KB Application Extension 17.08.2001 09:39
imgmt.dll 56 KB Application Extension 20.10.2003 14:05
libdb32.dll 420 KB Application Extension 13.07.2001 10:37
libdb32d.dll 1.408 KB Application Extension 13.07.2001 10:37
libsasl.dll 92 KB Application Extension 17.08.2001 09:39
NTAuth.dll 29 KB Application Extension 10.11.2003 10:19
SccHicom300.exe 2.564 KB Application 19.10.2003 22:54
SccHiPath3000.exe 2.256 KB Application 19.10.2003 22:54
SccHiPath4000.exe 2.608 KB Application 19.10.2003 22:54
SccP.exe 2.324 KB Application 19.10.2003 22:54
slapadd.exe 172 KB Application 23.04.2002 14:17
slapadd_dbg.exe 665 KB Application 07.05.2002 15:14
slapcat.exe 172 KB Application 23.04.2002 14:17
slapcat_dbg.exe 665 KB Application 07.05.2002 15:14
slapd.exe 260 KB Application 23.04.2002 14:17
slapd_dbg.exe 837 KB Application 07.05.2002 15:14
TelasProxy.exe 225 KB Application 10.11.2003 10:19
CAP Management PC
Lookup Service
LAN
Lookup Client
Ordner
Unify
OpenScapeCTI
bin
tools
config
jre
lib
Logs
unwise
Dateiname
Gr...
Typ
Geändert
tools File Folder 23.12.2003 19:18
jsstart.exe 28 KB Application 20.10.2003 14:05
sccHiPath4000.exe 2.... Application 01.07.2002 20:09
igmnt.dll 38... Applicati... 27.06.2002 15:17
CAP Service Starter PC

CAP Service Starter Prozessübersicht im Windows Taskmanager

Im Windows Taskmanager müssen folglich die Prozesse des CAP Service Starters erscheinen. Der `SCCHiPath3000.exe` wurde durch eine Konfiguration auf dem CAP Management-PC nach dem Start des Dienstes **OpenScape CTI** übertragen. Dem entsprechend dürfen nach dem Stoppen des Dienstes **OpenScape CTI** diese Prozesse nicht mehr erscheinen! Ist dies trotzdem der Fall, müssen diese Prozesse manuell beendet werden.



Manuelles Beenden von Prozessen

Die Prozesse des CAP Service Starters können nicht durch die Funktion "Prozess beenden" beendet werden. Es ist gerade während der Installationsphase darauf zu achten, dass mit dem Stoppen des Dienstes "OpenScape CTI" auch alle Prozesse beendet werden.

Es wird empfohlen (falls erforderlich), den Dienst zu stoppen, danach zu kontrollieren ob auch alle Prozesse beendet wurden und erst im Gutfall den Dienst neu zu starten.

Sollten CAP Prozesse trotz gestoppten Dienst "OpenScape CTI" weiterhin laufen, so muss der PC neu gestartet werden.

> Durch das Programm "kill.exe" können diese Prozesse beendet werden. Ein PC Neustart ist dann nicht erforderlich.

4.9 Besonderheiten bei der Installation

4.9.1 Mehrere Netzwerkkarten

Wenn in einem CAP PC mehrere Netzwerkkarten/NIC-Karten eingerichtet sind (z.B. eine zur Einbindung ins Kunden-LAN, eine zur Anbindung des HiPath / OpenScape-Vermittlungsrechners), ist es wichtig, während der Einrichtung die Netzwerkkarte zu identifizieren, über die OpenScape CAP ins Kunden-LAN eingebunden ist. Dies ist nicht in jedem Fall eindeutig automatisch möglich; deswegen gibt es während der Installation ein entsprechendes Auswahlfenster zur Identifikation der passenden NIC-Karte. Dieses Auswahlfenster erscheint auch, wenn nur eine Karte konfiguriert ist - wählen Sie dann einfach diese Karte aus, und fahren Sie mit der Installation fort.

Der <PC Name> und die <IP Adresse> für die zu startenden Prozesse der CAP können nachträglich in den folgenden Dateien gesetzt werden:

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

Die Einträge lauten:

```
args: -localAddr
args: "<PC Name>/<IP Adresse>"
```

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

Die Einträge lauten:

```
<?x set INST_HOST = "PC-Name" ?>
<?x set INST_IP = "IP-Adresse" ?>
```

Diese Einträge können nach der Installation manuell geändert werden und sind nach einem Neustart des Dienstes **OpenScape CTI** aktiv.

4.9.2 Einrichtung mehrerer Cluster

In einer verteilten Installation (d.h. OpenScape CAP-Komponenten wie SCC, CA4000, XMLPS oder SCCP laufen auf anderen PCs als OpenScape CAP Management), identifizieren sich zusammengehörige Komponenten über einen Lookup-Service auf Basis einer sogenannten `cluster id`.

Für den Fall, daß Sie in Ihrer Netzwerkumgebung OpenScape CAP Management mehrfach installieren wollen (z.B. zum unabhängigen Betrieb verschiedener OpenScape CAP-Installationen), ist zur eindeutigen Identifizierung für jede dieser Installationen eine eigene cluster id vorzusehen.

Bei einer verteilten Installation (Installation des CAP Service Starters, Auswahl von “Some services will run on other hosts” in dem u.a. Fenster) werden Sie immer aufgefordert, eine cluster-ID einzugeben. Als Hilfe dazu werden die über “Multicast” gefundenen Cluster-IDs in einem

Auswahlfenster angezeigt. Wählen Sie die Cluster-ID aus, welche durch das zugehörige CAP Management definiert wurde. In der Regel erscheint, bzw. erscheinen dort Cluster-IDs, die dem oder den PC-Namen der zugehörigen CAP Management PCs entsprechen. Erscheint in dem Auswahlfenster keine Cluster-ID, so ist entweder das CAP Management noch nicht installiert bzw. nicht gestartet oder “Multicast” durch Netzwerkkomponenten geblockt. Nun ist die direkte Eingabe der Cluster-ID notwendig. Sie muss immer mit der Cluster-ID des zugehörigen CAP Managements übereinstimmen.

Der <PC Name> als eindeutige CAP Cluster-ID kann nachträglich auf dem CAP Management PC und auf dem CAP Service Starter PC in der folgenden Datei gesetzt werden:

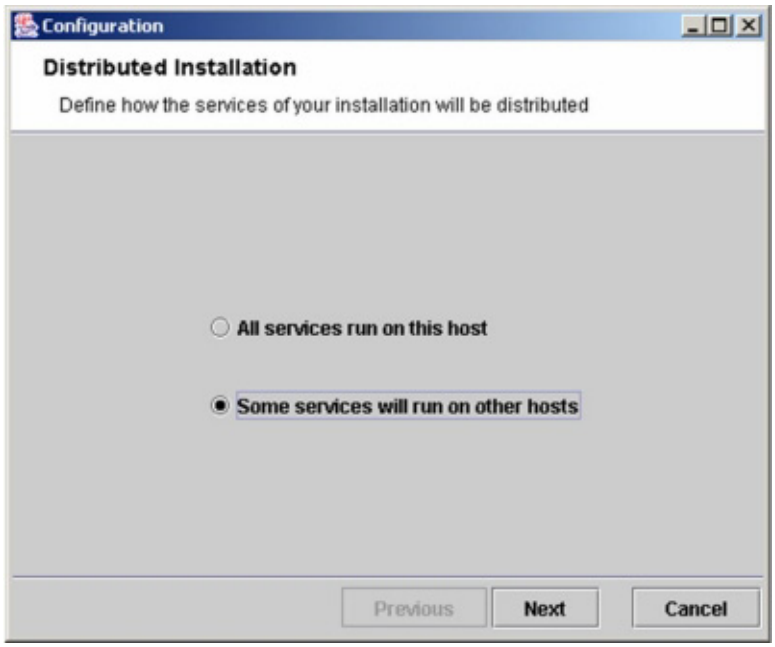
```
<InstDir>\config\start\startNT.cfg
```

Der Eintrag lautet:

```
    args: "<PC-Name>/TelasWebStarter"
```

Dieser Eintrag kann nach der Installation manuell geändert werden und ist nach einem Neustart des Dienstes “OpenScape CTI” aktiv.

Ist “Multicast” geblockt, verfahren Sie entsprechend der Anweisungen im nächsten Abschnitt.



4.9.3 Betrieb der CAP hinter einer Firewall

Um ihren CAP Server gegen externe Attacken zu schützen wird empfohlen die Firewall zu aktivieren die das abblocken soll, mit Aussnahme der nötigen Ports für die externen Zugriffe.

Die Ports welche für den zugehörige CAP-Betrieb geöffnet bleiben müssen, sind anschliessend beschrieben. Viele von ihnen sind allgemein gültig, aber einige sind von der aktuellen Installationsumgebung abhängig; die zugehörige Aktionen müssen speziell im Fall einer verteilten Installation durchgeführt werden (z.B. CAP-Komponenten sind auf mehreren Servern verteilt). Die Firewall-Konfiguration bezieht sich auf den "zentralen" CAP-Server.

- Port 8169
  CAP Management Schnittstelle, XML via TCP/IP
  - muss in jedem Fall geöffnet bleiben
- Port 8170
  CAP Management Schnittstelle, http via TCP/IP
  - muss in jedem Fall geöffnet bleiben
- Port 8470
  CAP Management Schnittstelle, https via TCP/IP
  - muss geöffnet bleiben falls, die Kommunikation via SSL-Verschlüsselung (https) durchgeführt wird
- Client Ports für SCC und / oder SCCP Services
  wie für die Kunden-Installation konfiguriert (Default-Werte im Bereich zw. 26535… und 27535)
  - muss in jedem Fall geöffnet bleiben
- Port für DiagnosisService
  wird dynamisch zugewiesen, siehe nachstehend die explizite Zuweisung
  - muss in jedem Fall geöffnet bleiben
- Port für LookupService
  Regulär ein UDP-Port für Multicast, siehe nachstehende Anweisungen um den Multicast-Betrieb abzuschalten
  - Der Multicast-Betrieb wird mit expiziten Port-Definitionen abgeschaltet;
  ist nur im Fall der verteilten Installation erforderlich

4.9.3.1 Explizite Port-Zuweisung für den DiagnosisService

Sorgen Sie dafür, dass der Dienst "OpenScape CTI" gestoppt wird.

Gehen Sie ins Installationsverzeichnis und öffnen Sie die Konfigurationsdatei

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

Sie können die bestehende Version dieser Datei als Sicherungskopie speichern.

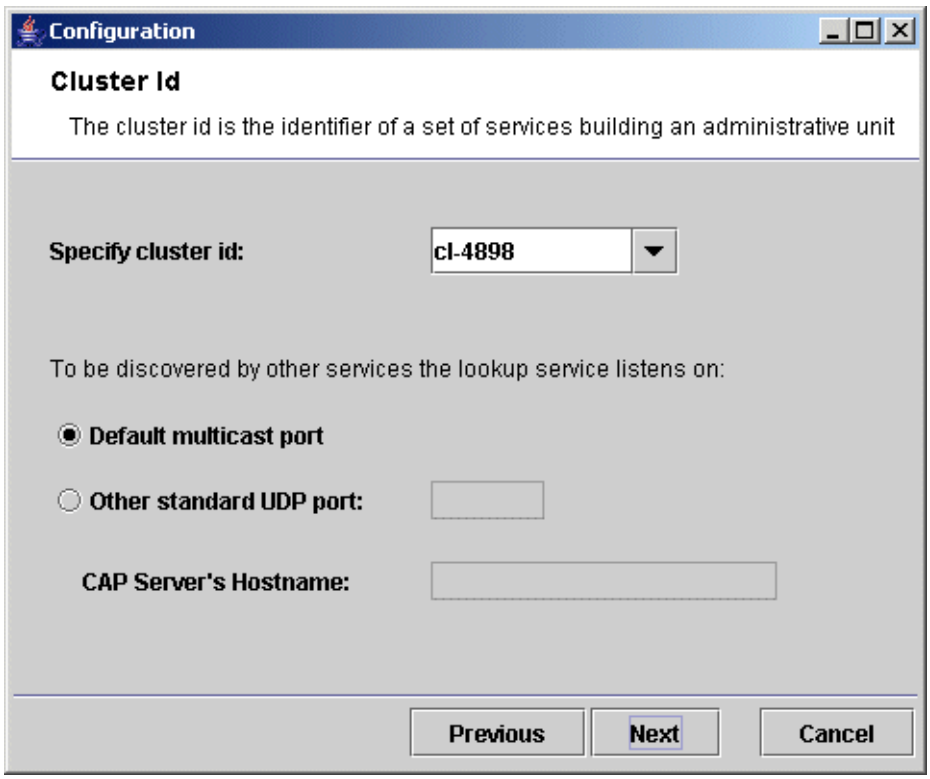
Nun fügen Sie folgende Zeile hinzu

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

<xxxx> repräsentiert eine beliebige gültige und freie Port-Nummer, und speichern Sie nun die Datei. <xxxx> ist jener Port der zum Zugriff für das DiagnosisService dient, welcher in der Firewall-Konfiguration geöffnet bleiben muss.

4.9.3.2 Explizite Konfiguration des LookupService ohne Multicast-Betrieb

Diese Konfiguration kann bereits während der Installation durchgeführt werden. Für den Fall dass Sie die Option "Some services run on other hosts" auswählen, erhalten Sie nachfolgendes Dialogfenster.



Sie können einen Namen für die spezifische Cluster-ID eingeben (oder den vorgeschlagenen Default-Wert beibehalten). In jedem Fall sollen Sie sicher gehen, dass Sie die Option "Default multicast port" abwählen, dafür aber die Option "Other standard UDP port" wählen und hier einen gültigen freien Wert für den UDP-Port definieren.

Die Werte die Sie hier definiert haben werden in einer Konfigurationsdatei gespeichert. Falls sie eine bestehende Installation haben, ist es möglich diese Datei nachträglich zu ändern.

Sorgen Sie dafür, dass der Dienst "OpenScape CTI" gestoppt wird.

Gehen Sie ins Installationsverzeichnis und öffnen Sie die Konfigurationsdatei

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

Sie können die bestehende Version dieser Datei als Sicherungskopie speichern.

Nun ändern Sie folgenden Eintrag

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

zu lesen

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

mit <ClusterId> und <UDPPort> welche die Werte vom vorangegangenen Installations-Dialog beschreiben und speichern Sie die Datei. <UDPPort> ist jener Port der zum Zugriff für das LookupService dient, welcher in der Firewall-Konfiguration geöffnet bleiben muss.

Es ist absolut notwendig, dass die Einträge an allen PCs im CAP-Cluster ident sind, sowohl an den CAP-Remote-PCs also auch am zentralen CAP-Management-Host.

> Bitte beachten Sie, dass die Änderungen in den Konfigurationsdateien, wie oben beschrieben, dann wirksam werden, sobald sie den Dienst **OpenScape CTI** neu starten.

4.9.4 Anpassung der IP-Adresse beim OpenScape CAP-PC

Während der Installation der OpenScape CAP Software werden Informationen zum PC - insbesondere Host-Name und IP-Adresse des PC, auf dem installiert wird - ermittelt und gespeichert (in Konfigurationsdateien sowie in Form von Verzeichnis- und Dateinamen). Deswegen machen spätere Änderungen von Host-Name oder IP-Adresse die Installation inkonsistent und ohne entsprechende Anpassung unbrauchbar.

Dieser Abschnitt beschreibt, welche Änderungen zur Anpassung an geänderte Host-Namen oder IP-Adressen erforderlich sind. Dasselbe Vorgehen kann auch genutzt werden, wenn OpenScape CAP in Form eines *ghost image* installiert wird, um die Konfiguration von der Produktionsumgebung auf die Einsatzumgebung anzupassen.

Ausgangssituation

OpenScape CAP Management wurde wie in Abschnitt 4.1 beschrieben installiert. Die Komponenten OpenScape CAP Call Control Service, Connectivity Adapter CA 4000 können ebenfalls installiert sein.

Anpassungen

Alle erforderlichen Anpassungen beziehen sich auf Inhalte des Installations-Verzeichnisses *<InstDir>* wie oben definiert.

> 7 Der vollqualifizierte Pfadname für das Installationsverzeichnis wird ebenfalls an verschiedenen Stellen in der Installation abgelegt; deswegen ist im Fall der Installation über ghost image unbedingt darauf zu achten, dass der bei Erzeugung des ghost image verwendete Installationspfad auf dem Zielrechner ebenfalls gültig ist.

1. Datei <*InstDir*>/config/start/startNT.cfg
   Passen Sie die zwei unterstrichenen Definitionen an
   args: -localAddr
   args: "mypc.area.xxxxxx.de/142.33.22.11"

2. Datei <*InstDir*>/config/common/global.cfg
   Passen Sie die drei unterstrichenen Definitionen an
   <?x set INST_HOST = "mypc.area.xxxxx.de" ?>
   <?x set INST_IP = "142.33.22.11" ?>
   <?x set CONFIG_URL = "http://mypc.area.xxxxxx.de:
   <?x $CAP_STD_PORT ?>" ?>

3. Verzeichnis <*InstDir*>/config/
   Das Unterverzeichnis <host name> ist entsprechend dem geänderten host name anzupassen.

4. Datei <*InstDir*>/config/<host name>/systemdb/S02service_ctrl.proc
   Passen Sie die unterstrichene Definition an
   args: <*InstDir*>/config/mypc/systemdb/slapd_cap.conf

5. Datei <*InstDir*>/config/<host name>/systemdb/slapd_cap.conf
   Passen Sie die unterstrichenen Definitionen an
   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
   Passen Sie die URL hinter dem Link an wie unterstrichen
   http://mypc.area.xxxxxx.de:8170/ oder
   https://mypc.area.xxxxxx.de:8170/

7. Verzeichnis <*InstDir*>/bin/tools/
   Dieses Verzeichnis enthält einige Werkzeuge / Stapeldateien für administrative Zwecke (vgl. Abschnitt 8.6.3). Die Stapeldateien sind ggf. ebenfalls anzupassen.

Falls zusammen mit OpenScape CAP auch HiPath ComAssistant installiert wurde, sind vier weitere Punkte zu modifizieren.

8. Datei <*InstDir*>/config/<host name>/addrbkdb/S02service_ctrl.proc
   Passen Sie die unterstrichene Definition an
   <?x include "/mypc/journal_access/backup.cfg" ?>
   args: <*InstDir*>/config/mypc/addrbkdb/slapd_twpabs.conf

9. Datei <*InstDir*>/config/<host name>/addrbkdb/slapd_twpabs.conf
   Passen Sie die unterstrichenen Definitionen an
   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. Datei <*InstDir*>/config/<host name>/twebdb/S02service_ctrl.proc
    Passen Sie die unterstrichene Definition an
    <?x include "/mypc/journal_access/backup.cfg" ?>
    args: <*InstDir*>/config/mypc/twebdb/slapd_tweb.conf

11. Datei <*InstDir*>/config/<host name>/twebdb/slapd_tweb.conf
    Passen Sie die unterstrichenen Definitionen an
    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. Datei <*InstDir*>/config/<host name>/journal_access/S40service_c-
    trl.proc
    Passen Sie die unterstrichene Definition an
    <?x include "/mypc/journal_access/backup.cfg" ?>

13. Link <*InstDir*>/startMenu/startPageUser
    Passen Sie die URL hinter dem Link an wie unterstrichen
    http://mypc.area.xxxxxx.de:8180/ oder
    https://mypc.area.xxxxxx.de:8180/

4.9.5 Konflikte bei der Port-Zuweisung

Während der CAP-Installation werden die meisten für die interne Kommunikation genutzen Ports automatisch zugewiesen; einige Ports werden mit Hilfe von Betriebssystem-Diensten dynamisch zugewiesen. Für die Services, die über den Administrator eingerichtet werden, ist die Zuordnung von Ports Bestandteil der Service-Einrichtung.

Bei jeder Port-Zuordnung besteht die Gefahr von Konflikten.

Bei dynamischer Port-Zuordnung sorgt das Betriebssystem für die Vermeidung von Port-Konflikten.

Bei Port-Zuordnung während der Service-Einrichtung liegt es in der Hand des Administrators, Port-Konflikte zu vermeiden; CAP Management unterstützt hier durch Vorschläge für die Port-Vergabe, bei der die Standardwerte jeweils automatisch inkrementiert werden.

Bei Port-Zuordnung während der Installation besteht immer das Risiko von Konflikten. Die zugewiesenen Port-Nummern werden regelmäßig in Konfigurations-Dateien abgelegt. Im Konfliktfall könnten Sie die entsprechenden Dateien anpassen, um den Konflikt zu umgehen. Ein während des Systemtests beobachteter Konflikt ergibt sich in einem HiPath 3000 / 5000 - Netz, bei dem standardmäßig der Common Web Service installiert wird; dieser nutzt Port 8280, der normalerweise auch vom OpenScape CAP Process Controller genutzt wird. In diesem Fall kann in `startNT.cfg` ein anderer Port eingestellt werden.

> Zum Vorgehen bei der Port-Zuweisung vgl. auch die Hinweise in Abschnitt 4.9.3, “Betrieb der CAP hinter einer Firewall”

4.9.6 Deaktivieren von Services

Manchmal ist es sinnvoll, einzelne Services (SCC oder SCCP) zeitweilig abzuschalten, ohne dabei die Konfigurationsdaten zu verlieren.

1. Zu diesem Zweck wählen Sie **Service** im Hauptmenü und aktivieren den Menüpunkt **Switch Verbindung** oder **SCC Proxy** in der Navigationsleiste. Wählen Sie den betreffenden Service aus der Liste und klicken Sie auf das Symbol **Bearbeiten**  .
2. Aktivieren Sie die Option **PBX deaktivieren** und drücken Sie **Ändern**.
   Nun wird der entsprechende Service in der Übersichtsliste mit einem roten Punkt angezeigt. Deaktivierte Services können wieder aktiviert werden, indem Sie das Häkchen bei **PBX deaktivieren** wieder entfernen; sie werden dann in der Übersichtliste wieder mit einem grünen Punkt angezeigt.

> Bitte beachten Sie, dass sich das Deaktivieren eines Service nicht direkt auf laufende SCC-Prozesse auswirkt. Dazu ist es erforderlich, auf dem betroffenen PC den Systemdienst **OpenScape CTI** anzuhalten und neu zu starten; erst dann wird die Änderung wirksam!

4.10 Maintenance-Installation

Korrekturen im installierten HiPath CTI System können ebenfalls unter Kontrolle des CAP.msi Installers durchgeführt werden.

Wählen Sie über **Start | Einstellungen | Systemsteuerung | Software | Programm ändern oder entfernen** die Komponente **OpenScape CAP** zum Ändern / Entfernen aus. Damit öffnen Sie den MSI Installer zur "Maintenance Installation".

Der Installer bietet "Modify", "Repair" sowie "Remove" zur Auswahl an; nutzen Sie "Modify", um Komponenten hinzuzufügen, die bei einer früheren Installation nicht berücksichtigt wurden. "Repair" kann genutzt werden, um Probleme in einer bestehenden Installation zu beheben.

Wählen Sie "Remove" um CAP zu deinstallieren. Damit werden alle zuvor installierten Komponenten ohne weitere Benutzereingabe entfernt. Bitte beachten Sie, dass die gezielte Deinstallation einzelner CAP-Komponenten weder erforderlich noch wünschenswert ist.

> Nach der Deinstallation sollten Sie das Installationsverzeichnis überprüfen: dort könnten Dateien verblieben sein, die entweder Konfigurationsdaten enthalten die bewußt aufgehoben wurden oder die nicht gelöscht werden konnten, weil sie als "noch in Benutzung" ausgewiesen waren. Wenn Sie das Installationsverzeichnis komplett löschen wollen, müssen Sie die verbliebenen Dateien manuell entfernen.

4.11 Upgrade von SMR3 auf SMR5 oder neue Version

Bevor Sie die Upgrade starten:

- Überprüfen Sie, ob Sie die Lizenz-File mit Ihren Lizenzen haben!
  Wenn Sie Ihre HiPath CAP benutzen möchten, wird eine Lizenz benötigt. Sie sollten dieses nur das erste mal kaufen, nachher können Sie es in alle Version von HiPath CTI importieren, unabhängig von der Versionsnummer. Vergessen Sie aber nicht den Ablaufdatum zu überprüfen, weil nachdem es abgelaufen ist, müssen Sie ein neues kaufen. Wir versehen es normalerweise mit einer *.lic Dateinamenserweiterung.!
  Die Lizenzen sind nur für den Computer gültig, dessen MAC-Adresse am Anfang der Lizenz-Anforderungs-Verfahren angegeben wurde. Es bedeutet, daß die Lizenz nur für eine fixe MAC-Adresse gültig ist.

- Notieren Sie alle Konfigurationsdaten von Ihren SCCs und SCCPs!
  Nach der Upgrade, werden die Einstellungen von SCCs und von SCCPs vom HiPath Management angezeigt, aber es sind physikalisch nicht gespeichert. Deswegen wird es vorgeschlagen diese Daten zu notieren bevor Sie mit der Upgrade beginnen. Wenn Sie mehrere SCCs und SCCPs konfiguriert haben, nimmt es viel Zeit in Anspruch, aber es ist jedenfalls erforderlich. Nach der Upgrade Löschen Sie alle SCCs und SCCPs, und richten Sie den erneut ein mit dem Konfigurationsdaten die Sie vorher notiert haben.

- Überprüfen Sie, das Ihre alte Version von HiPath CTI gestoppt ist!
  Zuerst müssen Sie die HiPath CTI Windows Dienst stoppen.
  Um dies zu tun, starten Sie Dienste (Start| Einstellungen | Systemsteuerung | Verwaltung | Dienste) und wählen Sie HiPath CTI. Klicken Sie darauf mit rechte Maustaste und wählen Sie Beenden.

Starten der Upgrade:

Sie können nicht die Upgrade von SMR3 auf SMR5 direkt tun. Zuerst müssen Sie den Upgrade von SMR3 auf SMR4 machen, und nachher können Sie mit die Upgrade auf SMR5 fortsetzen. Wegen diese Gründe benötigen Sie die HiPath CTI V3.0 Installations-Pakete Version SMR4 und SMR5. **Die Upgrade von SMR5 auf eine neues Version kann direkt durchgeführt werden.**

Schritten der Upgrade:

1. Beenden Sie die aktuell laufende Version von HiPath CTI. (Das Dienst kann von den Verwaltung gestoppt werden.)
2. Die Installation der neueren Version von HiPath CTI kann mit das CAP.msi gestartet werden.
3. Der Installations-Software erkennt die schon installierte Version von HiPath CTI, und bietet ein Upgrade an. Der Upgrade muß in das gleiche Verzeichnis installiert werden (wie der originale).
4. Nach dem der Installation beendet wurde, setzen Sie fort mit der Datenmigration. Diese Schritte sind in Kapitel 4.11.4 beschrieben. (Sehen Sie Schritt 9.)
5. Nach dem der Datenmigration beendet wurde , starten Sie den HiPath CTI Service (vom Verwaltung | Dienste).
6. Starten Sie CAP Management und überprüfen Sie alle Eigenschaften die im Schritt 14. von Kapitel 4.11.4 beschrieben sind. Zusätzlich machen Sie das gleiche mit SCCP als mit SCC zum beenden der Installation.

Am Ende der Migration von SMR3 auf SMR4 sollten Sie mit Migration von SMR4 zu SMR5 fortfahren. Das Verfahren ist das gleiche wie der Upgrade von SMR3 auf SMR4. Unterschied gibt es nur in der Migration der Daten. Die Datenmigration wird in Kapitel 4.11.4 beschrieben. (Sehen Sie Schritt 11.).

4.12 Hochrüstung Anweisungen

> Nach dem Hochrüstung auf einem neueren Version sollten Sie die Versionsnummer von den benutzen Prozesse übergeprüft werden, um Inkonsistenz zu vermeiden.

Sie können es folgendermassen durchführen:

.exe: **DiagnoseAgent** (Prozesse -> Prozess -> Snapshot -> (Status) -> version)

.jar: CAP Management (Hilfe -> Produktinformation)

5 OpenScape CAP Management kennen lernen

In diesem Kapitel erfahren Sie, wie Sie sich am CAP Management an- und abmelden können und lernen die Oberfläche des CAP Managements kennen.

5.1 Starten von CAP Management

> Um eine optimale Darstellung des CAP Managements zu erzielen, sollte eine Bildschirmauflösung von 1024x768 Pixeln oder höher gewählt sein.

1. Starten Sie das OpenScape CAP Management über **Start | Programme | O[penScape CAP | Management**.
2. Es öffnet sich Ihr HTML-Browser und es erscheint der Anmelde-Dialog.

5.1.1 Anmelden

Die Funktionen von OpenScape CAP Management sind erst nach einer erfolgreichen Anmeldung zugänglich. Das Anmelden am CAP Management geschieht über die Eingabe einer Kennung und eines Passworts. Die mit der Installation eingerichtete Administrator-Standardkennung dazu lautet “Admin“ mit dem Standardpasswort “Admin“. Das Passwort sollte baldmöglich vom Administrator geändert werden (siehe unten).

1. Zur Anmeldung geben Sie die Administrator-Standardkennung "Admin“ und das Administrator-Standardpasswort "Admin“ in die entsprechenden Eingabefelder ein. Das eingegebene Kennwort wird verdeckt durch Sternchen angezeigt.

   > Bei der Texteingabe von Kennung und Passwort wird zwischen Groß- und Kleinschreibung unterschieden.

2. Klicken Sie auf die Schaltfläche **OK**. Die Daten werden überprüft und das CAP Management ist erfolgreich gestartet.

   > Nach 30 Minuten ohne Aktion wird die Verbindung zwischen Browser und System automatisch getrennt. Falls Sie weitere Aktionen mit dem CAP Management durchführen wollen, müssen Sie sich nochmals anmelden.

Um das Passwort des Administrators "Admin" zu ändern, gehen Sie wie folgt vor:

1. Aktivieren Sie im Hauptmenü **Benutzer**.
2. Wählen Sie im Navigationsbereich **Suchen/Ändern**.

3. Geben Sie als Suchbegriff unter Benutzer-ID **`Admin`** ein, und drücken Sie **Suchen**.
4. Ändern Sie im darauf folgenden Dialog das Passwort.

Zur Definition eines neuen Benutzers mit Administrator-Rechten richten Sie einen Benutzer ein wie in Abschnitt 7.3.1 beschrieben, und wählen Sie dabei **Admin** als Rolle des Benutzers.

Bitte beachten Sie, dass ab HiPath CAP V3.0 SMR4 neben dem Administrator mit unbegrenzten Administrationsrechten auch "Business-Gruppen-Administratoren" (BGAdmin) eingerichtet werden können; diese sind in ihren Administrationsrechten auf die jeweilige Business-Gruppe beschränkt. Details dazu finden sich in Abschnitt 7.1. Da in verschiedenen Business-Gruppen die gleiche Benutzer-ID vergeben werden kann, ist ggf. nur die Kombination Business-Gruppe + Benutzer-ID systemweit eindeutig. In diesem Fall muss die Anmeldung mit "<Business-Gruppe>/<Benutzer-ID>" erfolgen, bzw. (bei Authentisierung über Windows-Login) mit "<Domain>\ <Windows-Login>".

5.1.2 Abmelden

Zum Beenden des CAP Managements brauchen Sie sich nicht extra abmelden. Es reicht, wenn Sie das CAP Management normal schließen.

Wenn Sie die CAP Management-Sitzung beenden möchten, ohne das Fenster zu schließen, wählen Sie bitte **Abmelden** im Hauptmenü. Daraufhin erfolgt eine Bestätigungsabfrage, und die Sitzung wird beendet. Zum weiteren Arbeiten mit dem CAP Management ist danach eine Neuanmeldung erforderlich (siehe Abschnitt 5.1.1, “Anmelden”).

5.2 Oberfläche des CAP Managements

Die Oberfläche des CAP Managements besteht aus HTML-Seiten, die mit einem HTML-Browser (Internet Explorer ab V5.5 SP2 oder Netscape Navigator ab V7.1) geöffnet werden können. Daher arbeitet das CAP Management plattformunabhängig unter allen gängigen Betriebssystemen.

Grundsätzlich besteht jede der HTML-Seiten aus den drei Bereichen:

- Hauptmenü
- Navigationsbereich
- Arbeitsbereich

> Können Navigationsbereich und Arbeitsbereich aufgrund der Größe des Browserfensters nicht komplett angezeigt werden, so erscheinen horizontale oder vertikale Rollbalken an den Rändern, mit denen Sie den angezeigten Ausschnitt verschieben können.

> CAP Management benutzt URL Umschreibung. Sollte die Länge des URL überschreiten, so wird die URL Umschreibung nicht funktionieren. In solchen Fällen ist der Gebrauch eines Browsers mit höheren Version oder sogar eines anderen Browsers empfohlen.

5.2.1 Hauptmenü

Im Hauptmenü finden Sie die verschiedenen Menüpunkte des CAP Managements. Bei einem Klick auf einen Menüpunkt ändert sich die Auswahlliste im Navigationsbereich und entsprechend auch die Anzeige im Arbeitsbereich.

5.2.2 Navigationsbereich

Im Navigationsbereich finden Sie die verschiedenen Untermenüpunkte zum Hauptmenü. Bei einem Klick auf einen der Untermenüpunkte wird die zugehörige Seite im Arbeitsbereich dargestellt.

5.2.3 Arbeitsbereich

Im Arbeitsbereich können Sie die Daten zur Konfiguration von OpenScape CAP eingeben oder auswählen. Die angebotene Informations- und Aktionsmöglichkeiten sind dabei von der im Navigationsbereich gewählten Menüpunkt abhängig. Die Beschreibung der Informationen und Aktionen finden Sie unter dem jeweiligen Menüpunkt.

6 Konfiguration mit OpenScape CAP Management

Sie können an die OpenScape CAP V3.0 die unterschiedlichsten Kommunikationssysteme anbinden, wie z.B.

- HiPath 8000 / OpenScape Voice
- HiPath / OpenScape 4000
- HiPath 3000 / 5000

Für jeden Vermittlungsrechner, der mit OpenScape CAP verbunden werden soll, muss eine entsprechende SCC-Instanz eingerichtet werden, z.B.:

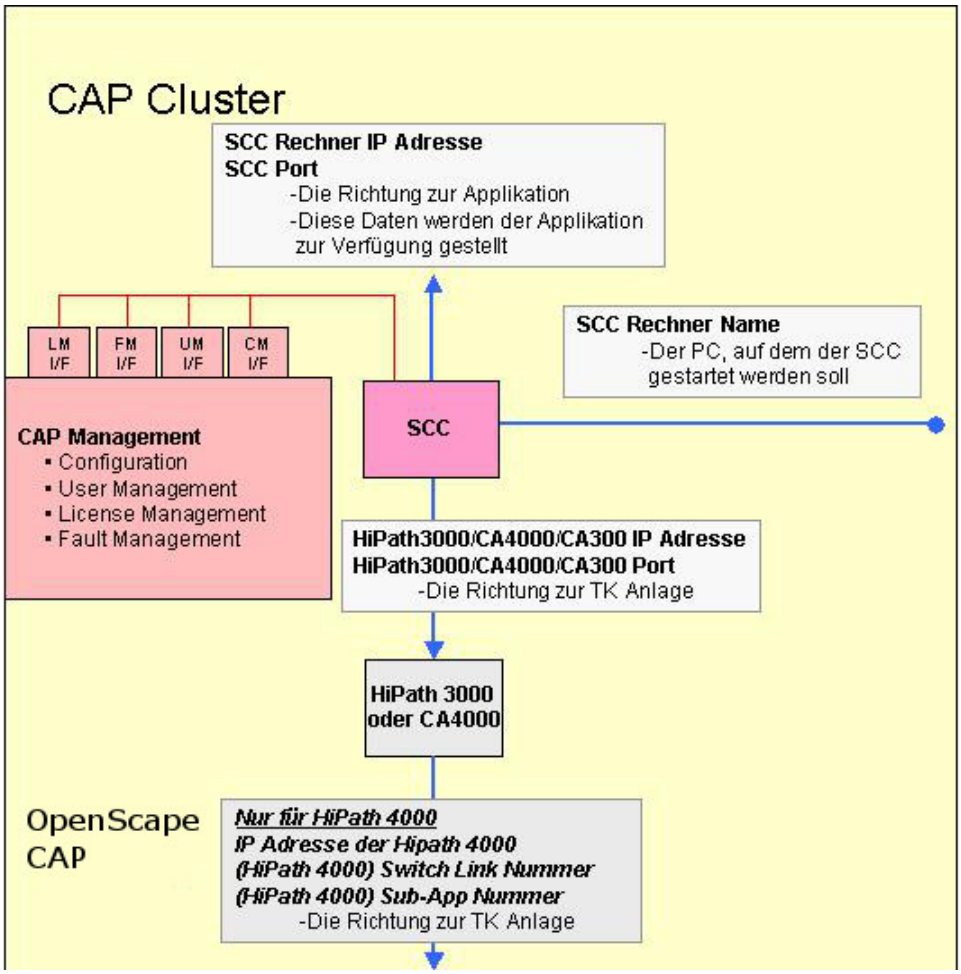
- SCC4000 für HiPath 4000 bis V5
- SCC4000V6 für HiPath 4000 V6 und OpenScape 4000 V7
- SCC3000 für HiPath 3000
- SCC8000 für HiPath 8000 und OpenScape Voice

Zur Einrichtung und Konfiguration einer neuen SCC-Instanz wählen Sie **Administration** im Hauptmenü und aktivieren Sie **Switch Verbindung** in der Navigationsleiste. Klicken Sie in der Arbeitsfläche, um einen neuen Eintrag zu erzeugen, und wählen Sie die gewünschte SCC-Variante in der eingeblendeten Auswahl-Box.

Um die Multi Domain Fähigkeit für die Protokolle CSTA XML und CSTA III ASN.1 (auch für JTAPI und XMLPS Applikationen) zu ermöglichen, ist der Einsatz eines SCCP notwendig. Der SCCP ist in der Lage, gleichzeitig mit mehreren SCC zu kommunizieren.

In diesem Kapitel erfahren Sie, welche Einstellungen Sie im OpenScape CAP Management treffen müssen, um die oben genannten Kommunikationssysteme an die OpenScape CAP anzubinden. Weiterhin wird erklärt, wie ein SCCP und der einzurichten sind.

Nachfolgend wird die Positionierung eines SCC in der CAP mit den Erläuterungen zu den wesentlichen Konfigurationspunkten dargestellt.


CAP Cluster
SCC Rechner IP Adresse
SCC Port
-Die Richtung zur Applikation
-Diese Daten werden der Applikation zur Verfügung gestellt
LM I/F
FM I/F
UM I/F
CM I/F
SCC Rechner Name
-Der PC, auf dem der SCC gestartet werden soll
CAP Management
• Configuration
• User Management
• License Management
• Fault Management
SCC
HiPath3000/CA4000/CA300 IP Adresse
HiPath3000/CA4000/CA300 Port
-Die Richtung zur TK Anlage
HiPath 3000 oder CA4000
OpenScape CAP
Nur für HiPath 4000
IP Adresse der Hipath 4000
(HiPath 4000) Switch Link Nummer
(HiPath 4000) Sub-App Nummer
-Die Richtung zur TK Anlage

6.1 Anbindung der HiPath 8000 / OpenScape Voice

6.1.1 Übersicht

CSTA ist ein Standard für computergestützte Telefonie (CTI), der von der internationalen Normungsorganisation ECMA (European Computer Manufacturers Association) ausgearbeitet wurde. Die physikalische Verbindung zwischen der HiPath 8000 / OpenScape Voice und einem PC, auf dem ein SCCHiPath8000 läuft, wird mit Hilfe einer TCP/IP-LAN-Verbindung realisiert.

6.1.2 Vorbereitung

Zum Anschluss einer HiPath 8000 / OpenScape Voice ist die CSTA-Verbindung wie in der Switch-Dokumentation beschrieben einzurichten.

6.1.3 Konfiguration

Um die Anbindung einer HiPath 8000 / OpenScape Voice erstmalig einzurichten oder eine bestehende Verbindung neu zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie im Navigationsbereich auf den Menüpunkt **Switch Verbindung**.

   a) Es ist noch keine Verbindung eingerichtet. Weiter mit 2a.

   b) Es sind bereits eine oder mehrere Verbindungen eingerichtet. Diese werden Ihnen in einer Liste angezeigt. Weiter mit 2b.

2. Konfigurieren Sie die Verbindung.

   a) Ist noch keine Verbindung eingerichtet, klicken Sie auf das Symbol **Neuen Eintrag hinzufügen** und wählen als Server Version den Eintrag **HiPath 8000** aus.

   b) Sind bereits eine oder mehrere Verbindungen eingerichtet, werden Ihnen diese in einer Liste angezeigt. Wählen Sie eine Verbindung aus, indem Sie auf das Symbol **Bearbeiten** der gewählten Verbindung klicken.

   Im Arbeitsbereich erscheint nun der Konfigurationsdialog HiPath 8000 mit den drei Teilbereichen SCC, Switch und Switch-PNP.

> Bitte beachten Sie, dass es nicht zulässig ist, die entsprechenden Abschnitte der Konfigurationsdatei telas.cfg (vgl.Abschnitt A.2.15) nachträglich zu verändern!

Dialog SCC

Feld	Beschreibung
SCC Name	Geben Sie hier einen symbolischen Namen für den SCC ein, z.B. „SCC-HP3800“. Dieser Name kann vom Administrator nach Belieben vergeben werden. Er muss innerhalb der gesamten CAP-Installation eindeutig sein. Bis zu 32 Zeichen (Buchstaben, Ziffern, Unterstrich und Bindestrich) sind erlaubt. Akzentbuchstaben/Umlauten sind nur unter Windows unterstützt.
SCC Id (optional)	Geben Sie hier einen Bezeichner für den SCC ein; dieser Bezeichner muss innerhalb der gesamten OpenScape CAP-Installation eindeutig sein und kann nach der Einrichtung nicht mehr geändert werden. Im Diagnose-Agenten wird ein SCC in der Prozess-Übersicht mit dieser SCC Id dargestellt. Üblicherweise wird hier die HiPath/OpenScape-Knotennummer (z.B. 10-60-200, 30-70-600,...) verwendet. Bis zu 32 Zeichen (Buchstaben, Ziffern, Unterstrich und Bindestrich) sind erlaubt. Akzentbuchstaben sind nur unter Windows Installation unterstüzt. **Hinweis**: Beim Benutzerdatenimport muss die SCC Id mit der PBX Id in der Import-Datei übereinstimmen.
SCC Rechner Name	Geben Sie hier den Rechnernamen (hostname) des PC ein, auf dem der SCC-Prozess laufen soll. Anhand des “Rechner-Namens” wird ein PC-Namensverzeichnis im Verzeichnis `<InstDir>\config\` erstellt. Für den SCC wird ein Unterverzeichnis mit dem Namen `telas-server_<SCC-ID>` hinzugefügt. Dieses Unterverzeichnis enthält sämtliche Konfigurationsdateien für diesen zu startenden Prozess. **Hinweis:** Bei verteilter Installation (d.h. der SCC-PC ist nicht der eigene PC/localhost) ist auf dem hier spezifizierten SCC-PC unbedingt der OpenScape CAP Service Starter zu installieren (vgl. Abschnitt 4.3).
SCC Rechner IP-Adresse (nicht editierbar)	Hier wird die IP-Adresse des PCs angegeben, auf dem der SCC-Prozess laufen soll. Sie wird aus dem Rechnernamen ermittelt und nur zur Kontrolle angezeigt.

Feld	Beschreibung
SCC Port (optional)	Sie können hier optional den Port angeben, der dem SCC-Prozess zugeordnet wird. Als Standardwert wird Port **26535** verwendet. Wurde dieser Port bereit durch die CAP-Konfiguration einem anderen SCC zugewiesen , so wird automatisch der nächste freie Port angeboten (z.B.: 26537)

Dialog Switch

Feld	Beschreibung
Switch IP-Adresse	Geben Sie hier die IP-Adresse der HiPath 8000 / OpenScape Voice ein, über die die CSTA-Schnittstelle der HiPath 8000 / OpenScape Voice erreichbar ist.
Switch Port (optional)	Geben Sie hier den Port am Vermittlungsrechner ein.
Backup Switch IP-Adresse	Geben Sie hier die IP-Adresse der Backup HiPath 8000 / OpenScape Voice ein, über die die CSTA-Schnittstelle der Backup HiPath 8000 / OpenScape Voice erreichbar ist.
Backup Switch Port (optional)	Geben Sie hier den Port am Vermittlungsrechner ein.
Kurzwahlnummern	Kurzwahlnummern werden nur vom PhoneController von ComAssistant verwendet. Bei einer über die Applikation initiierten Wahl wird überprüft, ob die gewählte externe Rufnummer in der zugeordneten Kurzwahlliste eingerichtet ist. Wird sie dort gefunden, wird anstelle der Langrufnummer die konfigurierte Kurzwahlnummer vom SCC zur HiPath 3000 als Wahl geschickt. Kurzwahllisten werden nur dann verwendet, wenn CTI-Benutzer keine Vollamtsberechtigung besitzen, sondern nur Zugriff auf die Anlagenkurzwahl haben und dennoch eine Wahl aus einem LDAP-Suchergebnis heraus durchführen möchten. In einem LDAP-Server werden Rufnummern von Personen in der Regel als Langrufnummer im kanonischen Format abgelegt.
Zugangsnummern	Im linken Teil wird die Liste eingerichteter Zugangsnummern / Domain-Informationen (vgl. Abschnitt 7.2.3) angezeigt. Übernehmen Sie die für diesen Switch relevanten Einträge per Pfeil-Taste auf die rechte Seite.

Feld	Beschreibung
NAC	Im linken Teil wird die Liste eingerichteter Querkennzahlen / NACs (vgl. Abschnitt 7.2.4) angezeigt. Übernehmen Sie die für diesen Switch relevanten Einträge per Pfeil-Taste auf die rechte Seite.
Privater Nummerierungsplan	Im linken Teil wird die Liste eingerichteter Privater Nummerierungspläne / PNPs (vgl. Abschnitt 7.2.5) angezeigt. Übernehmen Sie die für diesen Switch relevanten Einträge per Pfeil-Taste auf die rechte Seite.

Aktionen

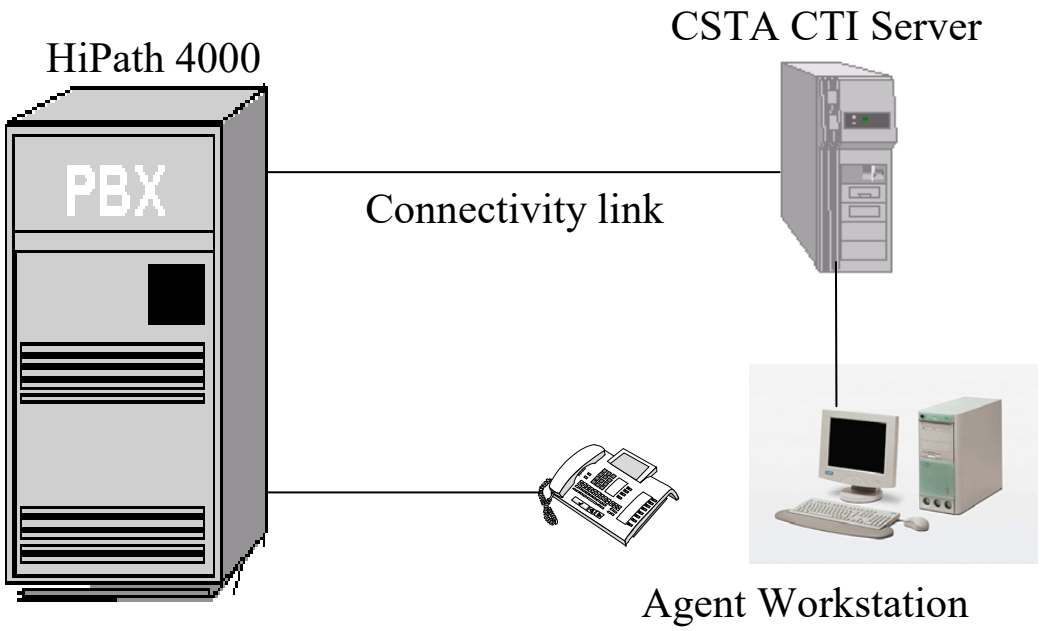
Aktion	Beschreibung
Hinzufügen	Prüft die Daten auf Vollständigkeit und fügt den Eintrag zur Liste der Switch-Verbindungen hinzu.
Schließen	Schließt den kompletten Dialog **Eintrag hinzufügen** ohne die Eingaben zu sichern.
Löschen	Löscht eine bestehende Switch-Verbindung. **Hinweis**: Diese Schaltfläche erscheint nur, wenn bereits mindestens eine Switch-Verbindung eingerichtet ist.
Nächste >>	Ruft den nächsten Dialog auf.
<< Vorherige	Ruft den vorherigen Dialog auf.

> Wenn Sie die Verbindung zur HiPath 8000 / OpenScape Voice für die Nutzung durch ComAssistant V2.0 einrichten, wird die Applikation nur die Konfigurationsdaten nutzen; der SCC8000-Dienst selbst wird umgangen.
> Dementsprechend könnte der SCC nach Abschluss der Konfigurierung deaktiviert werden (vgl. Abschnitt 4.9.6) - außer er wird von einer anderen Applikation genutzt.

6.2 Anbindung der HiPath / OpenScape 4000

6.2.1 Übersicht

Die HiPath 4000 bis V5 unterstützt für die Kommunikation mit Applikationen kein standardisiertes Protokoll. Deshalb ist der Einsatz des Protokoll-Konverters "Connectivity Adapter HiPath 4000" (CA4000) zwingend erforderlich. Der CA4000 wandelt das proprietäre Protokoll der HiPath 4000 (ACL-C+) in ein standardisiertes Protokoll (CSTA III) um. CSTA ist ein Standard für computergestützte Telefonie (CTI), der von der internationalen Normungsorganisation ECMA (European Computer Manufacturers Association) ausgearbeitet wurde. Mit der OpenScape CAP V3.0 kann der CA4000 nur noch zusammen mit dem SCCHiPath4000 verwendet werden. Sämtliche Konfigurationsparameter des CA4000 sind in der SCCHiPath4000 Konfiguration integriert worden. Die physikalische Verbindung zwischen der HiPath 4000 und einem PC, auf dem ein CA4000/SCCHiPath4000 läuft, wird mit Hilfe einer TCP/IP-LAN-Verbindung realisiert.
Die HiPath4000 unterstützt gleichzeitig 32 "ACL-C+"-Applikationsverbindungen. Abhängig von der Softwareversion können weniger als 32 "ACL-C+"-Applikationsverbindungen freigegeben sein.



6.2.2 Vorbereitung

Zum Anschluss einer HiPath 4000 ist der SCCHiPath4000 einzurichten. Sein Konfigurationsmenü bietet zusätzlich die CA4000-Konfigurationsparameter an. Falls die Verbindung zur HiPath 4000 über die SL100/200 realisiert wird, muss die IP-Adresse oder das IP-Netz des SCCHiPath4000/CA4000-PCs in der Firewall-Liste der HiPath 4000 aufgenommen werden.

BERMERKUNG: im Fall von HiPath 4000 V6 / OpenScape 4000 V7 der CAP startet keinen CA4000 Prozess, abert SCC konnektiert zu dem HiPath 4000 V6 CSTA direkt. Also im Fall HiPath 4000 V6 / OpenScape 4000 V7 Swith Verbindung keine Applikations/SubApplikationsNummer soll man in dem GUI eingeben

Im Fall von Hochruestung von einem HiPath 4000 V4/5 auf HiPath 4000 V6 die Device und User Daten in dem CAP Datenbank soll man erst exportieren, dann in der exportierte Datei soll man die SCCId von der alten Verbindung mit dem neuen Switchverbindung ersetzen, un dann nach dem Loeschen der alten SwitchVerbindung und den Device/UserDaten soll man die geanderte User/Device Daten wieder importieren.

6.2.3 Konfiguration

Um die Anbindung einer HiPath 4000 erstmalig einzurichten oder eine bestehende Verbindung neu zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie im Navigationsbereich auf den Menüpunkt **Switch Verbindung**.
   a) Es ist noch keine Verbindung eingerichtet. Weiter mit 2a.
   b) Es sind bereits eine oder mehrere Verbindungen eingerichtet. Diese werden Ihnen in einer Liste angezeigt. Weiter mit 2b.
2. Konfigurieren Sie die Verbindung.
   a) Ist noch keine Verbindung eingerichtet, klicken Sie auf das Symbol **Neuen Eintrag hinzufügen** und wählen als Server Version den Eintrag **HiPath 4000** aus.
   b) Sind bereits eine oder mehrere Verbindungen eingerichtet, werden Ihnen diese in einer Liste angezeigt. Wählen Sie eine Verbindung aus, indem Sie auf das Symbol **Bearbeiten** der gewählten Verbindung klicken.

   Im Arbeitsbereich erscheint nun der Konfigurationsdialog HiPath4000 mit den vier Teilbereichen SCC, CA4000, Switch und Switch-PNP.

Dialog SCC

Feld	Beschreibung
SCC Name	Geben Sie hier einen symbolischen Namen für den SCC ein, z.B. „SCC-HP4000“. Dieser Name kann vom Administrator nach Belieben vergeben werden. Er muss innerhalb der gesamten CAP-Installation eindeutig sein. Bis zu 32 Zeichen (Buchstaben, Ziffern, Unterstrich und Bindestrich) sind erlaubt. Akzentbuchstaben sind nur unter Windows Installation unterstüzt.

Feld	Beschreibung
SCC Id (optional)	Geben Sie hier einen Bezeichner für den SCC ein; dieser Bezeichner muss innerhalb der gesamten OpenScape CAP-Installation eindeutig sein und kann nach der Einrichtung nicht mehr geändert werden. Im Diagnose-Agenten wird ein SCC in der Prozess-Übersicht mit dieser SCC Id dargestellt. Der zugehörige CA4000-Prozess wird analog dazu als `CA4000_<SCC Id>` aufgelistet. Üblicherweise wird hier die HiPath/OpenScape-Knotennummer (z.B. 10-60-200, 30-70-600,...) verwendet. Bis zu 32 Zeichen (Buchstaben, Ziffern, Unterstrich und Bindestrich) sind erlaubt. Akzentbuchstaben sind nur unter Windows Installation unterstützt. **Hinweis**: Beim Benutzerdatenimport muss die SCC Id mit der PBX Id in der Import-Datei übereinstimmen.
SCC Rechner Name	Geben Sie hier den Rechnernamen (hostname) des PC ein, auf dem der SCC-Prozess laufen soll. Anhand des "Rechner-Namens" wird ein PC-Namensverzeichnis im Verzeichnis `<Inst-Dir>\config\` erstellt. Für den SCC wird ein Unterverzeichnis mit dem Namen `telas-server_<SCC-ID>` hinzugefügt. Für den zugehörigen CA4000 wird ein Unterverzeichnis mit dem Namen `ca4000_<SCC-ID>` hinzugefügt. Diese Unterverzeichnisse enthalten sämtliche Konfigurationsdateien für diese zu startenden Prozesse. **Hinweis:** Bei verteilter Installation (d.h. der SCC-PC ist nicht der eigene PC/localhost) ist auf dem hier spezifizierten SCC-PC unbedingt der OpenScape CAP Service Starter zu installieren (vgl. Abschnitt 4.3).
SCC Rechner IP-Adresse (nicht editierbar)	Hier wird die IP-Adresse des PCs angegeben, auf dem der SCC-Prozess laufen soll. Sie wird aus dem Rechnernamen ermittelt und nur zur Kontrolle angezeigt.
SCC Port (optional)	Sie können hier optional den Port angeben, der dem SCC-Prozess zugeordnet wird. Als Standardwert wird Port **26535** verwendet. Wurde dieser Port bereit durch die CAP-Konfiguration einem anderen SCC zugewiesen, so wird automatisch der nächste freie Port angeboten (z.B.: 26536).

Feld	Beschreibung
ASN1 Single Domain Native Mode	Wird dieser SCC mit einem SCCP oder einem TCSP verbunden (Multi Domain Mode), ist der voreingestellt Wert **Aus** beizubehalten. Im “Multi Domain Mode” unterstützt der SCC die Protokolle CSTA III ASN.1, CSTA XML und NetTSPI. Der Status des SCC ist immer “aktiv”. Wird eine CSTA-Protokollversion ausgewählt, ändert sich die Betriebsart des SCC in den “Single Domain Native Mode”. In diesem Modus wird ein Protokoll eins-zu-eins vom SCC durchgereicht und sein Status ist ohne Applikationsverbindung “nicht bereit”! Entsprechend den Erfordernissen der Applikation ist auszuwählen: ? `CSTA ACSE`: Schnittstelle auf CSTA Phase III eingerichtet und verlangt Anmeldung am SCC über ACSE-Request (Details im OpenScape CAP Application Developers Guide), ? `CSTA III`: Schnittstelle auf CSTA Phase III eingerichtet.
CallID Management für TAPI	Dieses Feld ermöglicht die Aktivierung der Call-ID-Behandlung mittels CallIDRepository; dies ist nur für spezielle TAPI-Anwendungen erforderlich (siehe Dokumentation zu den jeweiligen Applikationen). Normalerweise sollten Sie die Voreinstellung **Aus** unverändert beibehalten.

Dialog CA4000

Feld	Beschreibung
CA4000 IP-Adresse (nicht editierbar, nicht angezeigt)	Diese IP-Adresse wird vom SCC für die Kommunikation zum CA4000 genutzt. Sie wird automatisch identisch zur SCC Rechner IP-Adresse eingestellt und im GUI nicht mehr angezeigt.
CA4000 Port (optional)	Sie können hier optional den Port angeben, den der CA4000 für diese Anbindung bereitstellt (“1025-5000”). Dieser Port wird vom SCC für die Kommunikation zum CA4000 adressiert. Als Standardwert wird Port “4640” verwendet. Da vereinzelt Probleme mit Windows-Prozessen auftreten, die Ports im Bereich von “1025 - 1299" nutzen, wird ein Port ab “1300” empfohlen.

Feld	Beschreibung
Switch Link Number (optional)	Diese Nummer muss in der CA-Konfiguration und im AMO CPTP:APPL übereinstimmen. Die entscheidenden Parameter in dem AMO sind die ACM-Nummer und die APPL-Nummer. Sie werden errechnet aus dem Vorgabewert "50" plus die Switch Link Nummer. (ACM 50 + Switch Link Nummer; APPL 50 + Switch Link Nummer). Beispiel: Switch Link Nummer = 5 >>> ACM55;APPL55;
Switch Sub-App Number (optional)	Diese Nummer muss in der CA-Konfiguration und im AMO XAPPL übereinstimmen. Der entscheidende Parameter in dem AMO ist die Sub-Applikationsnummer "Dxx" (D01-D32). Beispiel: Switch Sub Appl Nummer = 25 >>> D25
Use External DNIS (optional)	Die Aktivierung von DNIS (Dialed Number Identification Service) ist ein zusätzliches Informationsfeld im "Delivered-, Queued-, Diverted-, Established-, Connection Cleared-Event" und wird derzeit von der HiPath / OpenScape 4000 nicht im vollen Umfang unterstützt. Wird DNIS aktiviert, so übermittelt die HiPath / OpenScape 4000 in diesem Feld die von einem externen Anrufer angewählte Nummer. Ist DNIS nicht aktiv, so wird die ANI (Automatic Number Identification) in diesem Feld übermittelt, welches die Rufnummer des externen Anrufers ist.

Dialog Switch

Feld	Beschreibung
Switch IP-Adresse	Geben Sie hier die IP-Adresse der HiPath / OpenScape 4000 ein. Achten Sie darauf, dass bei einer Verbindung über die SL100/200 die IP-Adresse oder das gesamte IP-Netz des SC-CHiPath4000/CA4000-PC in der Firewall-Liste eingetragen ist
SPI-Kennung **SPI-Passwort** **Business Gruppe**	Zum direkten Zugriff auf die HiPath / OpenScape 4000-Administration über den PBX Interface Service (SPI), sind hier die Login-Daten zum "Expert Access (ComWin)" anzugeben. Dadurch wird der Knopf "**Hole Device Daten**" aktiviert, über den Sie zu jeder Zeit den Import von Device-Daten aus dem Switch anstoßen können. Bitte beachten Sie, das mit dieser Funktion Devices erzeugt sowie die Daten vorhandener Devices modifiziert werden können; es werden keine Devices aus der CAP Management-Datenbank gelöscht. Die Devices werden immer in die ausgewählte BG importiert - Aufteilung der über SPI gefundenen Devices in mehrere unterschiedliche BGs ist derzeit nicht möglich.

Feld	Beschreibung
Kurzwahlnummern	Kurzwahlnummern werden nur vom PhoneController von Com-Assistant verwendet. Bei einer über die Applikation initiierten Wahl wird überprüft, ob die gewählte externe Rufnummer in der zugeordneten Kurzwahlliste eingerichtet ist. Wird sie dort gefunden, wird anstelle der Langrufnummer die konfigurierte Kurzwahlnummer vom SCC zur HiPath / OpenScape 4000 als Wahl geschickt. Kurzwahllisten werden nur dann verwendet, wenn CTI-Benutzer keine Vollamtsberechtigung besitzen, sondern nur Zugriff auf die Anlagenkurzwahl haben und dennoch eine Wahl aus einem LDAP-Suchergebnis heraus durchführen möchten. In einem LDAP-Server werden Rufnummern von Personen in der Regel als Langrufnummer im kanonischen Format abgelegt.
Zugangsnummern	Im linken Teil wird die Liste eingerichteter Zugangsnummern / Domain-Informationen (vgl. Abschnitt 7.2.3) angezeigt. Übernehmen Sie die für diesen Switch relevanten Einträge per Pfeil-Taste auf die rechte Seite.
NAC	Im linken Teil wird die Liste eingerichteter Querkennzahlen / NACs (vgl. Abschnitt 7.2.4) angezeigt. Übernehmen Sie die für diesen Switch relevanten Einträge per Pfeil-Taste auf die rechte Seite.
Privater Nummerierungsplan	Im linken Teil wird die Liste eingerichteter Privater Nummerierungspläne / PNPs (vgl. Abschnitt 7.2.5) angezeigt. Übernehmen Sie die für diesen Switch relevanten Einträge per Pfeil-Taste auf die rechte Seite.

Aktionen

Aktion	Beschreibung
Hinzufügen	Prüft die Daten auf Vollständigkeit und fügt den Eintrag zur Liste der Switch-Verbindungen hinzu.
Schließen	Schließt den kompletten Dialog **Eintrag hinzufügen** ohne die Eingaben zu sichern.
Löschen	Löscht eine bestehende Switch-Verbindung. **Hinweis**: Diese Schaltfläche erscheint nur, wenn bereits mindestens eine Switch-Verbindung eingerichtet ist.
Nächste >>	Ruft den nächsten Dialog auf.
<< Vorherige	Ruft den vorherigen Dialog auf.

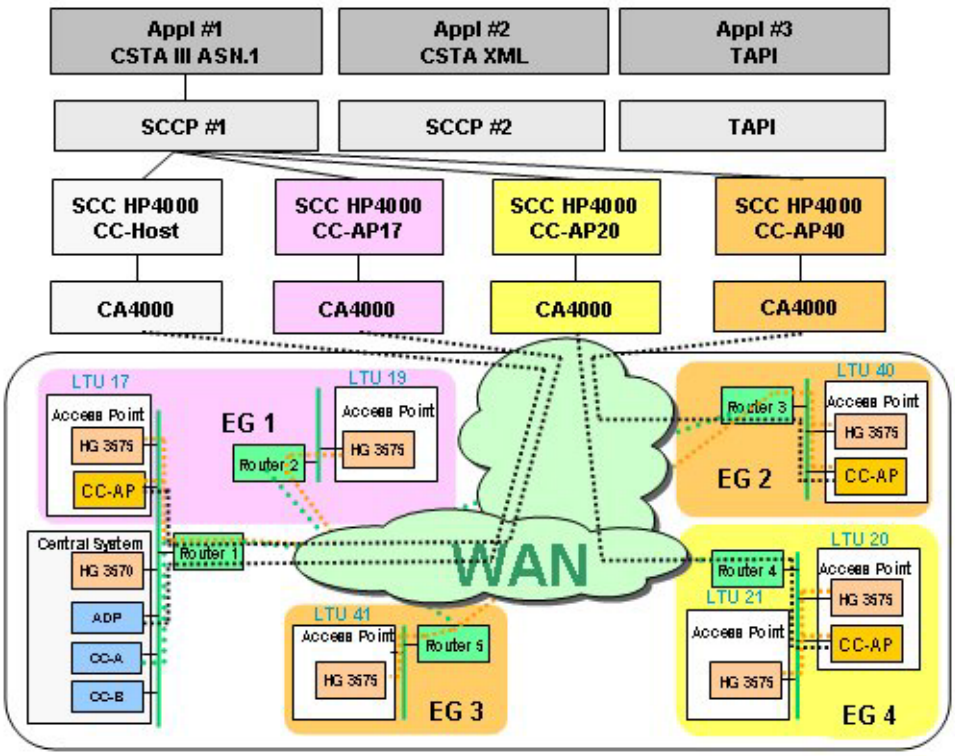
6.2.4 Anbindung einer HiPath / OpenScape 4000 AP Emergency Konfiguration

Damit die erweiterte Erreichbarkeit auf HiPath / OpenScape 4000 Ebene (siehe Abschnitt B.4) auch von einer Applikation genutzt werden kann, wurde die CAP V3.0 um zusätzliche AP Emergency-spezifische Konfigurationsmöglichkeiten erweitert.

6.2.4.1 Architektur

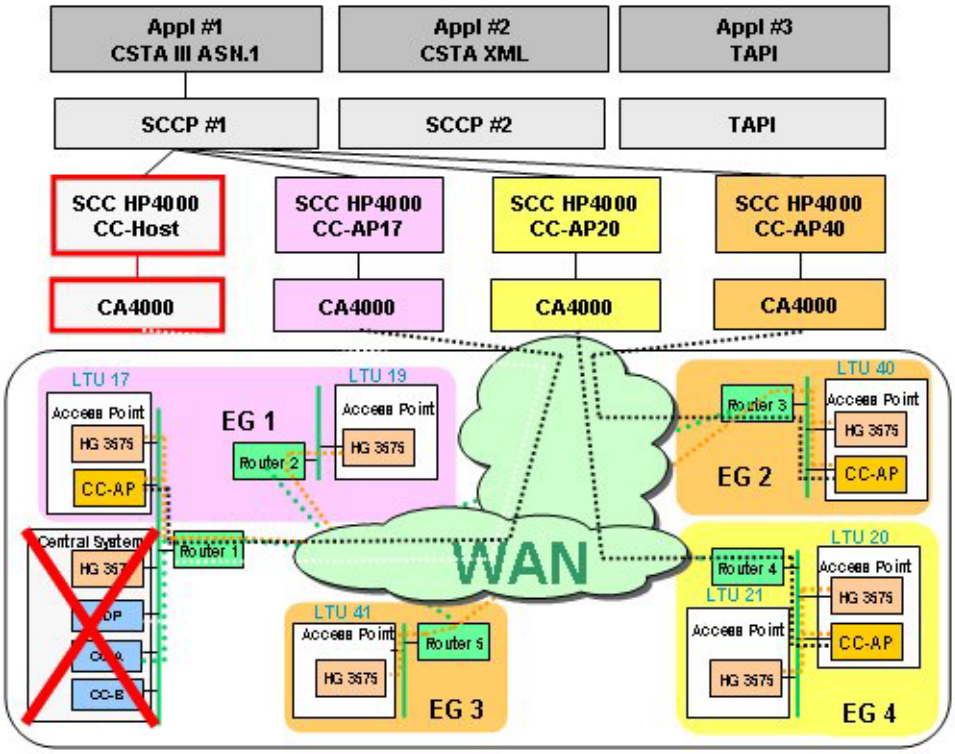
Aus CAP-Sicht wird jeder HiPath / OpenScape 4000 CC-AP wie eine eigene "Mini-4000-Systeme" behandelt, d.h. zum Anschluss eines HiPath / OpenScape 4000 CC-AP ist wie gewohnt ein eigener SCC4000 mit CA4000 einzurichten. Als koordinierende Instanz mit dem Überblick, welcher Teilnehmer jetzt über welchen Weg erreichbar ist, wird hier zwingend ein eigener SCC Proxy pro Applikation benötigt. Schließlich muss bei jedem AP-Emergency fähigen Device neben dem primären Weg (also der SCC4000 zum HiPath / OpenScape 4000 Server) auch der alternative Weg (also der SCC4000 zum entsprechenden HiPath / OpenScape 4000 CC-AP) eingestellt werden.

> Bitte beachten Sie, dass die AP Emergency-Funktionalität in der CAP nur für Applikationen verfügbar ist, die über SCCP angebunden werden.
> Bei direktem Zugriff auf einzelne SCCs und auch bei Anbindung über TAPI wird AP Emergency nicht unterstützt!



6.2.4.2 Ausfall-Szenarien

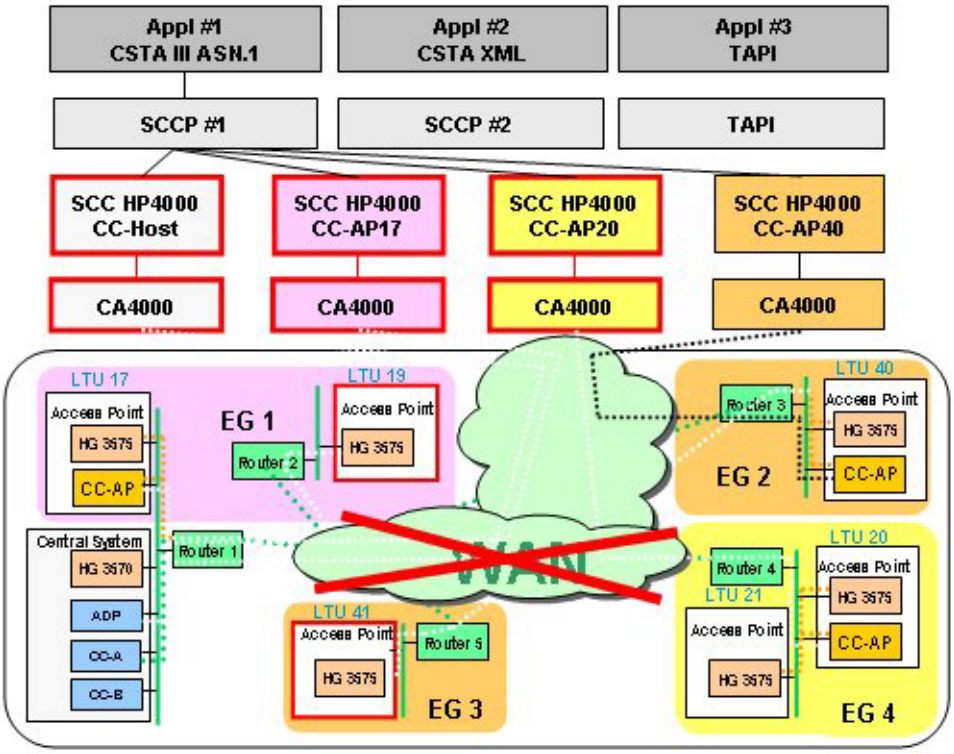
Ausfall des HiPath / OpenScape 4000 Servers



Auf HiPath / OpenScape 4000-Ebene sind alle **lokal** (d.h. an Shelves innerhalb des Servers) angeschlossenen Endgeräte nicht mehr erreichbar. Dagegen überleben alle **Access Points** den Ausfall, weil jeder AP seinen zugeordneten CC-AP erreichen kann.

Auf CAP-Ebene ist lediglich die Verbindung zwischen SCC4000 ("CC-Host") und HiPath / OpenScape 4000 Server unterbrochen, d.h. die lokal angeschlossenen Endgeräte sind nicht mehr erreichbar.

(Komplett- oder Teil-)Ausfall des WAN



Auf HiPath / OpenScape 4000 Ebene überleben alle **lokal** (d.h. an Shelves innerhalb des Servers) angeschlossenen Endgeräte sowie jeweils die **Access Points**, die noch ihren zugeordneten CC-AP erreichen können (im Beispiel AP20, AP21, AP40) oder aber direkt mit dem HiPath / OpenScape 4000 Server verbunden sind (im Beispiel AP17). Die restlichen Access Points fallen total aus (im Beispiel AP19, AP41).

Auf CAP-Ebene fallen im Beispiel fast alle SCC4000 Verbindungen aus - lediglich die Endgeräte am AP40 können noch erreicht werden, weil der SCC4000 "CC-AP40" von dem WAN-Teilausfall nicht betroffen ist.

6.2.4.3 Konfiguration

Wie oben bereits skizziert, sind folgende Komponenten zu administrieren:

- Switch-Verbindungen
  SCC4000 zu jedem HiPath 4000 CC-AP
- SCC Proxy
  SCCP pro Applikation als übergeordnete Instanz
- Device
  Eintrag des alternativen SCC4000 zum CC-AP bei jedem AP-fähigen Device

Zum Einrichten der Switch-Verbindung gehen Sie prinzipiell vor wie in Abschnitt 6.2.3 beschrieben; im folgenden wird nur auf Abweichungen / Besonderheiten hingewiesen.

1. Klicken Sie im Navigationsbereich auf den Menüpunkt **Switch Verbindung**.
   Hier sollten Sie bereits den SCC4000 zum HiPath 4000 Server sehen können
2. Konfigurieren Sie die Verbindung: klicken Sie auf das Symbol **Neuen Eintrag hinzufügen** und wählen als Server Version den Eintrag **HiPath / OpenScape 4000** aus.

   Im Arbeitsbereich erscheint nun der Konfigurationsdialog HiPath / OpenScape 4000 mit den vier Teilbereichen SCC, CA4000, Switch und Switch-PNP.

Grundsätzlich hat jeder HiPath / OpenScape 4000 CC-AP (bis auf geringfügige Abweichungen) die gleichen Administrationsdaten wie der HiPath / OpenScape 4000 Server (insbesondere sind Teilnehmerrufnummern und Wählplan identisch).

Aufgrund der identischen HiPath / OpenScape 4000 Daten empfiehlt es sich, für die jetzt folgende Konfiguration der zusätzlichen SCC4000s die entsprechenden SCC4000 oder SCC4000V6 Einstellungen für den HiPath / OpenScape 4000 Server als Vorlage zu nehmen.

Dialog SCC

Feld	Beschreibung
SCC Name	Für das Feld SCC Name ist ein neuer String zu definieren. Dabei ist es später hilfreich, wenn aus dem String ablesbar ist ? dass es sich um den SCC zu einem HiPath / OpenScape 4000 CC-AP (und nicht um einen HiPath / OpenScape 4000 Server) handelt ? welchem HiPath / OpenScape 4000 Server der CC-AP zugeordnet ist ? um welchen von mehreren CC-APs es sich handelt Es gelten die Regeln wie in Abschnitt 6.2.3 beschrieben.
SCC Id (optional)	Für das Feld SCC Id ist ein neuer String zu definieren. Dabei ist es später hilfreich, wenn aus dem String ablesbar ist ? dass es sich um den SCC zu einem HiPath / OpenScape 4000 CC-AP (und nicht um einen HiPath / OpenScape 4000 Server) handelt ? welchem HiPath / OpenScape 4000 Server der CC-AP zugeordnet ist ? um welchen von mehreren CC-APs es sich handelt Es gelten die Regeln wie in Abschnitt 6.2.3 beschrieben.

Feld	Beschreibung
SCC Rechner Name	Geben Sie hier den Rechnernamen (hostname) des PC ein, auf dem der SCC-Prozess laufen soll. Dieser muss nicht identisch mit dem für die 4000 Server-Verbindung eingerichteten sein! Es gelten die Regeln wie in Abschnitt 6.2.3 beschrieben.
übrige Felder	wie in Abschnitt 6.2.3 beschrieben.

Dialog CA4000

Feld	Beschreibung
CA4000 IP-Adresse (nicht editierbar, nicht angezeigt)	wie in Abschnitt 6.2.3 beschrieben.
CA4000 Port (optional)	Hier muss ein neuer, bisher noch nicht benutzer Port angegeben werden. Es gelten die Regeln wie in Abschnitt 6.2.3 beschrieben.
Switch Link Number (optional)	Hier ist jeweils eine neue, noch nicht benutzte Kombination (6 / 26 etc.) anzugeben. Voraussetzung ist, dass diese Kombination auf HiPath / OpenScape 4000-Seite entsprechend eingerichtet ist (AMOs wie in Abschnitt 6.2.3 beschrieben).
Switch Sub-App Number (optional)	
Use External DNIS	wie in Abschnitt 6.2.3 beschrieben.

Dialog Switch

Feld	Beschreibung
Switch IP-Adresse	Geben Sie hier die IP-Adresse des LAN-Anschlusses für den HiPath / OpenScape 4000 CC-AP ein. Achten Sie darauf, dass bei einer Verbindung über die SL100/200 die IP-Adresse oder das gesamte IP-Netz des SCCHiPath4000/CA4000-PC in jedem CC-AP in der Firewall-Liste eingetragen ist.
übrige Felder	wie in Abschnitt 6.2.3 beschrieben.

Zum Einrichten des SCC Proxy gehen Sie vor wie in Abschnitt 6.5.2 beschrieben.
Beachten Sie insbesondere die Erläuterungen zum Feld "AP Emergency deaktivieren".

Zum Einrichten der Devices gehen Sie vor wie in Abschnitt 7.4.2 beschrieben.
Beachten Sie insbesondere die Erläuterungen zum Feld "Emergency".

6.3 Anbindung der HiPath 3000

6.3.1 Übersicht

Die HiPath 3000 unterstützt für die Kommunikation mit Applikationen ein standardisiertes Protokoll CSTA III mit vorheriger ACSE-Anmeldung. CSTA ist ein Standard für computergestützte Telefonie (CTI), der von der internationalen Normungsorganisation ECMA (European Computer Manufacturers Association) ausgearbeitet wurde. Die physikalische Verbindung zwischen der HiPath 3000 und einem PC, auf dem ein SCCHiPath3000 läuft, wird mit Hilfe einer TCP/IP-LAN-Verbindung oder einer ISDN-S_0-Verbindung realisiert.
Die HiPath 3000 unterstützt gleichzeitig maximal acht CSTA III Verbindungen. Abhängig von der verwendeten HiPath 3000 Softwareversion können weniger als acht CSTA III Verbindungen freigegeben sein.

> Die TCP/IP-Verbindung zur HiPath 3000 ist nur über die HG1500 freigegeben. Die TCP/IP-Verbindung über das **LIM-Modul** wird **nicht** unterstützt!
> Auch HiPath 3000-Konfigurationen mit der Komponente **CSP** werden **nicht** unterstützt; das "CSP flag" muss in der HiPath 3000-Konfiguration deaktiviert sein. Andernfalls können sich CSTA-Meldungssequenzen ergeben, die im SCC3000 Probleme verursachen.

6.3.2 Vorbereitung

Zum Anschluss einer HiPath 3000 ist die CSTA-Verbindung wie in der HiPath 3000-Dokumentation beschrieben einzurichten. Standardmäßig ist die CSTA-Schnittstelle der HiPath 3000 von allen IP-Adressen aus erreichbar. Durch die Application-Firewall-Liste können aber einzelne IP-Adressen oder ganze IP-Netze freigegeben oder gesperrt werden.

6.3.3 Konfiguration

Um die Anbindung einer HiPath 3000 erstmalig einzurichten oder eine bestehende Verbindung neu zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie im Navigationsbereich auf den Menüpunkt **Switch Verbindung**.
   a) Es ist noch keine Verbindung eingerichtet. Weiter mit 2a.
   b) Es sind bereits eine oder mehrere Verbindungen eingerichtet. Diese werden Ihnen in einer Liste angezeigt. Weiter mit 2b.

2. Konfigurieren Sie die Verbindung.

   a) Ist noch keine Verbindung eingerichtet, klicken Sie auf das Symbol **Neuen Eintrag hinzufügen** und wählen als Server Version den Eintrag **HiPath 3000** aus.

   b) Sind bereits eine oder mehrere Verbindungen eingerichtet, werden Ihnen diese in einer Liste angezeigt. Wählen Sie eine Verbindung aus, indem Sie auf das Symbol **Bearbeiten** der gewählten Verbindung klicken.

   Im Arbeitsbereich erscheint nun der Konfigurationsdialog HiPath 3000 mit den drei Teilbereichen SCC, Switch und Switch-PNP.

Dialog SCC

Feld	Beschreibung
SCC Name	Geben Sie hier einen symbolischen Namen für den SCC ein, z.B. „SCC-HP3000“. Dieser Name kann vom Administrator nach Belieben vergeben werden. Er muss innerhalb der gesamten CAP-Installation eindeutig sein. Bis zu 32 Zeichen (Buchstaben, Ziffern, Unterstrich und Bindestrich) sind erlaubt. Akzentbuchstaben sind nur unter Windows Installation unterstüzt.
SCC Id (optional)	Geben Sie hier einen Bezeichner für den SCC ein; dieser Bezeichner muss innerhalb der gesamten OpenScape CAP-Installation eindeutig sein und kann nach der Einrichtung nicht mehr geändert werden. Im Diagnose-Agenten wird ein SCC in der Prozess-Übersicht mit dieser SCC Id dargestellt. Üblicherweise wird hier die HiPath/OpenScape-Knotennummer (z.B. 10-60-200, 30-70-600,...) verwendet. Bis zu 32 Zeichen (Buchstaben, Ziffern, Unterstrich und Bindestrich) sind erlaubt. Akzentbuchstaben sind nur unter Windows Installation unterstüzt. **Hinweis**: Beim Benutzerdatenimport muss die SCC Id mit der PBX Id in der Import-Datei übereinstimmen.

Feld	Beschreibung
SCC Rechner Name	Geben Sie hier den Rechnernamen (hostname) des PC ein, auf dem der SCC-Prozess laufen soll. Anhand des “Rechner-Namens” wird ein PC-Namensverzeichnis im Verzeichnis `<InstDir>\config\` erstellt. Für den SCC wird ein Unterverzeichnis mit dem Namen `telas-server_<SCC-ID>` hinzugefügt. Dieses Unterverzeichnis enthält sämtliche Konfigurationsdateien für diesen zu startenden Prozess. **Hinweis:** Bei verteilter Installation (d.h. der SCC-PC ist nicht der eigene PC/localhost) ist auf dem hier spezifizierten SCC-PC unbedingt der OpenScape CAP Service Starter zu installieren (vgl. Abschnitt 4.3).
SCC Rechner IP-Adresse (nicht editierbar)	Hier wird die IP-Adresse des PCs angegeben, auf dem der SCC-Prozess laufen soll. Sie wird aus dem Rechnernamen ermittelt und nur zur Kontrolle angezeigt.
SCC Port (optional)	Sie können hier optional den Port angeben, der dem SCC-Prozess zugeordnet wird. Als Standardwert wird Port **26535** verwendet. Wurde dieser Port bereit durch die CAP-Konfiguration einem anderen SCC zugewiesen , so wird automatisch der nächste freie Port angeboten (z.B.: 26537)

Dialog Switch

Feld	Beschreibung
Switch Connectivity	Wählen Sie hier aus, ob der Switch über **LAN**, über **ISDN Link** oder über **V24** angebunden werden soll. Die weitere Struktur des Switch-Dialogs hängt von der hier getroffenen Auswahl ab. Im folgenden wird zunächst die Anbindung über LAN beschrieben. Für die Anbindung über ISDN siehe Abschnitt 6.3.4. Für die Anbindung über V.24 siehe Abschnitt 6.3.5.
Switch IP-Adresse	Geben Sie hier die IP-Adresse der HiPath 3000 ein, über die die CSTA-Schnittstelle des HiPath 3000-Vermittlungs-PC erreichbar ist.
Switch Port (optional)	Geben Sie hier den Port **7001** ein. Die HiPath 3000 unterstützt keinen anderen Verbindungsport!

Feld	Beschreibung
Kurzwahlnummern	Kurzwahlnummern werden nur vom PhoneController von Com-Assistant verwendet. Bei einer über die Applikation initiierten Wahl wird überprüft, ob die gewählte externe Rufnummer in der zugeordneten Kurzwahlliste eingerichtet ist. Wird sie dort gefunden, wird anstelle der Langrufnummer die konfigurierte Kurzwahlnummer vom SCC zur HiPath / OpenScape 4000 als Wahl geschickt. Kurzwahllisten werden nur dann verwendet, wenn CTI-Benutzer keine Vollamtsberechtigung besitzen, sondern nur Zugriff auf die Anlagenkurzwahl haben und dennoch eine Wahl aus einem LDAP-Suchergebnis heraus durchführen möchten. In einem LDAP-Server werden Rufnummern von Personen in der Regel als Langrufnummer im kanonischen Format abgelegt.
Zugangsnummern	Im linken Teil wird die Liste eingerichteter Zugangsnummern / Domain-Informationen (vgl. Abschnitt 7.2.3) angezeigt. Übernehmen Sie die für diesen Switch relevanten Einträge per Pfeil-Taste auf die rechte Seite.
NAC	Im linken Teil wird die Liste eingerichteter Querkennzahlen / NACs (vgl. Abschnitt 7.2.4) angezeigt. Übernehmen Sie die für diesen Switch relevanten Einträge per Pfeil-Taste auf die rechte Seite.
Privater Nummerierungsplan	Im linken Teil wird die Liste eingerichteter Privater Nummerierungspläne / PNPs (vgl. Abschnitt 7.2.5) angezeigt. Übernehmen Sie die für diesen Switch relevanten Einträge per Pfeil-Taste auf die rechte Seite.

Aktionen

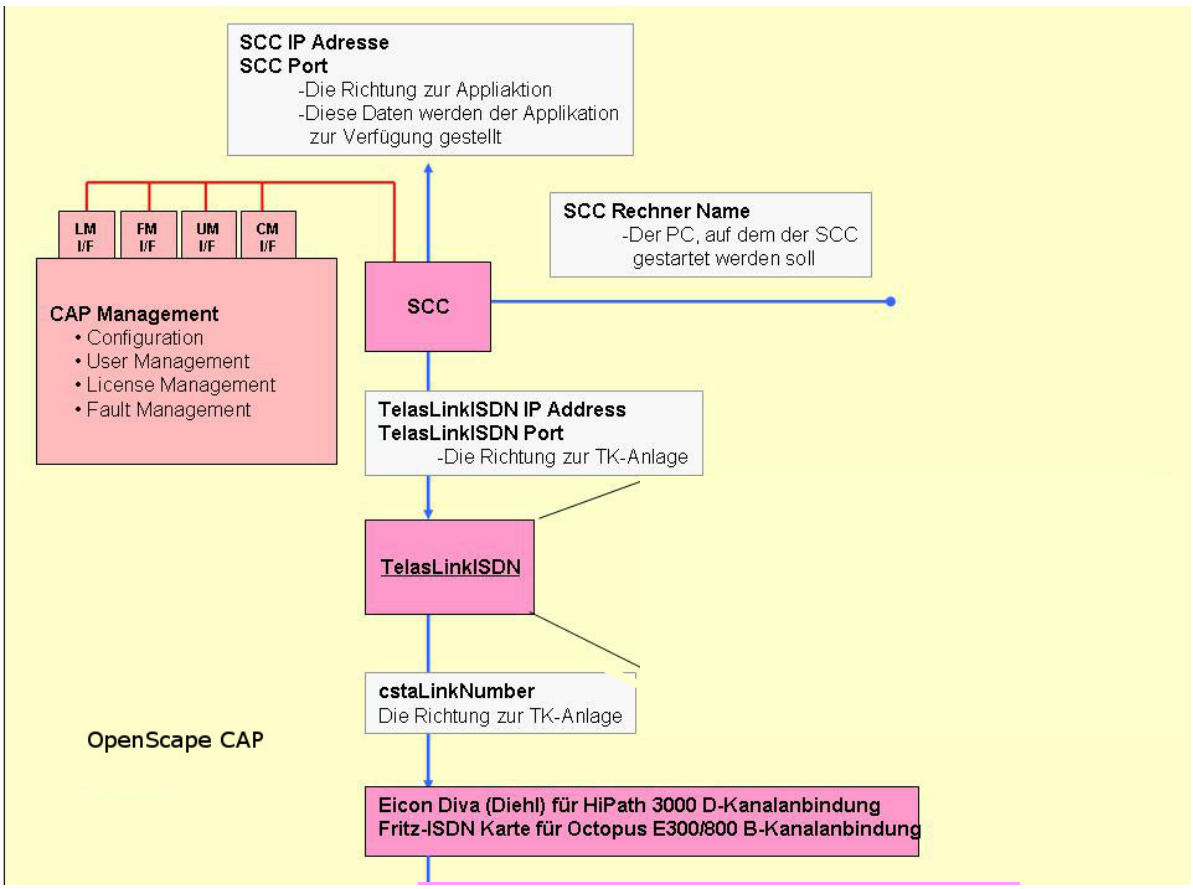
Aktion	Beschreibung
Hinzufügen	Prüft die Daten auf Vollständigkeit und fügt den Eintrag zur Liste der Switch-Verbindungen hinzu.
Schließen	Schließt den kompletten Dialog **Eintrag hinzufügen** ohne die Eingaben zu sichern.
Löschen	Löscht eine bestehende Switch-Verbindung. **Hinweis**: Diese Schaltfläche erscheint nur, wenn bereits mindestens eine Switch-Verbindung eingerichtet ist.
Nächste >>	Ruft den nächsten Dialog auf.
<< Vorherige	Ruft den vorherigen Dialog auf.

6.3.4 HiPath 3000 Anbindung per ISDN-Link

Die HiPath 3000 bietet optional die Anschaltung eines SCC via ISDN an. Dazu wird eine Komponente `TelasLinkISDN.exe` als TCP/IP-ISDN-Wandler bereitgestellt. Pro PC kann dieses Programm nur einmal gestartet werden, so dass für jede HiPath 3000 ISDN-Anschaltung ein eigener PC verwendet werden muss.

Das Programm öffnet auf der einen Seite einen TCP-Port, mit dem sich der SCC verbinden kann. Auf der anderen Seite wird auf die erste ISDN-Karte im PC zugegriffen.

> Die ISDN-Verbindung zur HiPath 3000 wird über den D-Kanal realisiert und nur durch die Eicon Diva (Diehl) ISDN-Karte unterstützt.



`TelasLinkISDN.exe` wird wie die SCCs als Komponente des CAP Call Control Service automatisch installiert und bei Einrichtung einer HiPath3000-Verbindung konfiguriert.

Dabei müssen die zusammengehörigen Komponenten SCC, LinkISDN und ISDN-Karte auf dem gleichen PC laufen.

Die Einrichtung erfolgt wie in Abschnitt Abschnitt 6.3.3 beschrieben; lediglich der Dialog Switch ändert sich wie folgt:

Dialog Switch

Feld	Beschreibung
Switch Connectivity	Wählen Sie hier **ISDN Link** aus.
Link IP-Adresse (nicht editierbar, nicht angezeigt)	Diese IP-Adresse wird vom SCC für die Kommunikation zum LinkISDN genutzt. Sie wird automatisch identisch zur SCC Rechner IP-Adresse eingestellt und im GUI nicht mehr angezeigt.
Link Port	Geben Sie hier den Port ein, über den der SCC den LinkISDN ansprechen kann.
Link Nummer	Geben Sie hier die Rufnummer (ISDN-Telefonnummer) an, über die die HiPath 3000 via ISDN angesprochen werden kann.
Kurzwahlnummern	... restliche Felder wie in Abschnitt 6.3.3 beschrieben.

6.3.5 HiPath 3000 Anbindung über V.24

Die HiPath 3000 bietet optional die Anschaltung eines SCC via V.24 an. Dazu wird eine Komponente `TelasLinkV24.exe` bereitgestellt. Pro PC kann dieses Programm nur einmal gestartet werden, so dass für jede HiPath 3000 V.24-Anschaltung ein eigener PC verwendet werden muss.

Das Programm öffnet auf der einen Seite einen TCP-Port, mit dem sich der SCC verbinden kann. Auf der anderen Seite wird auf die V.24-Schnittstelle des PC zugegriffen.

`TelasLinkV24.exe` wird wie die SCCs als Komponente des CAP Call Control Service automatisch installiert und bei Einrichtung einer HiPath 3000-Verbindung konfiguriert. Dabei müssen die zusammengehörigen Komponenten SCC und LinkV24 auf dem gleichen PC laufen. Die Einrichtung erfolgt wie in Abschnitt Abschnitt 6.3.3 beschrieben; lediglich der Dialog Switch ändert sich wie folgt:

Dialog Switch

Feld	Beschreibung
Switch Connectivity	Wählen Sie hier **V24** aus.
Link IP-Adresse (nicht editierbar, nicht angezeigt)	Diese IP-Adresse wird vom SCC für die Kommunikation zum LinkV24 genutzt. Sie wird automatisch identisch zur SCC Rechner IP-Adresse eingestellt und im GUI nicht mehr angezeigt.
Link Port	Geben Sie hier den Port ein, über den der SCC den LinkV24 ansprechen kann.
Kurzwahlnummern	... restliche Felder wie in Abschnitt 6.3.3 beschrieben.

6.4 "Virtuelle" Anbindung einer Vermittlungsanlage

6.4.1 Übersicht

In bestimmten Szenarien möchten Applikationen die Rufnummern-Verwaltung der CAP (inklusive SAT, vgl. Abschnitt 2.3.4) nutzen, ohne die entsprechenden Endgeräte selbst steuern zu wollen. Dazu müssen alle Konfigurationsdaten zum Rufnummernplan der entsprechenden Vermittlungsanlage verfügbar sein, aber die Einrichtung eines SCC oder Connectivity Adapters ist nicht erforderlich.

Diese spezifische Konfiguration wird mit Hilfe einer "virtuellen" Anbindung bereitgestellt. Danach können zu dieser "virtuellen" Anbindung Endgeräte definiert / importiert werden, deren Daten im SAT entsprechend verarbeitet werden.

6.4.2 Konfiguration

Um eine "virtuelle" Anbindung erstmalig einzurichten oder eine bestehende Verbindung neu zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie im Navigationsbereich auf den Menüpunkt **Switch Verbindung**.

   a) Es ist noch keine Verbindung eingerichtet. Weiter mit 2a.

   b) Es sind bereits eine oder mehrere Verbindungen eingerichtet. Diese werden Ihnen in einer Liste angezeigt. Weiter mit 2b.

2. Konfigurieren Sie die Verbindung.

   a) Ist noch keine Verbindung eingerichtet, klicken Sie auf das Symbol **Neuen Eintrag hinzufügen** und wählen als Server Version den Eintrag **Virtual** aus.

   b) Sind bereits eine oder mehrere Verbindungen eingerichtet, werden Ihnen diese in einer Liste angezeigt. Wählen Sie eine Verbindung aus, indem Sie auf das Symbol **Bearbeiten** der gewählten Verbindung klicken.

   Im Arbeitsbereich erscheint nun der Konfigurationsdialog Virtual mit den drei Teilbereichen SCC, Switch und Switch-PNP.

Dialog SCC

Feld	Beschreibung
SCC Name	Geben Sie hier einen symbolischen Namen für den SCC ein, z.B. „Virtual1“. Dieser Name kann vom Administrator nach Belieben vergeben werden. Er muss innerhalb der gesamten CAP-Installation eindeutig sein. Bis zu 32 Zeichen (Buchstaben, Ziffern, Unterstrich und Bindestrich) sind erlaubt. Akzentbuchstaben sind nur unter Windows Installation unterstüzt.
SCC Id (optional)	Geben Sie hier einen Bezeichner für den SCC ein; dieser Bezeichner muss innerhalb der gesamten OpenScape CAP-Installation eindeutig sein und kann nach der Einrichtung nicht mehr geändert werden. Üblicherweise wird hier die HiPath/OpenScape-Knotennummer (z.B. 10-60-200, 30-70-600,...) verwendet. Bis zu 32 Zeichen (Buchstaben, Ziffern, Unterstrich und Bindestrich) sind erlaubt. Akzentbuchstaben sind nur unter Windows Installation unterstüzt. **Hinweis**: Beim Benutzerdatenimport muss die SCC Id mit der PBX Id in der Import-Datei übereinstimmen.
SCC Rechner Name **SCC Rechner IP-Adresse** **SCC Port**	Da für eine virtuelle Anbindung kein SCC eingerichtet wird, werden diese Felder ignoriert.

Dialog Switch

Feld	Beschreibung
Switch IP-Adresse **Switch Port**	Da für eine virtuelle Anbindung keine Verbindung zur Vermittlungsanlage eingerichtet wird, werden diese Felder ignoriert.

Feld	Beschreibung
Kurzwahlnummern	Kurzwahlnummern werden nur vom PhoneController von Com-Assistant verwendet. Bei einer über die Applikation initiierten Wahl wird überprüft, ob die gewählte externe Rufnummer in der zugeordneten Kurzwahlliste eingerichtet ist. Wird sie dort gefunden, wird anstelle der Langrufnummer die konfigurierte Kurzwahlnummer vom SCC zur HiPath 3000 als Wahl geschickt. Kurzwahllisten werden nur dann verwendet, wenn CTI-Benutzer keine Vollamtsberechtigung besitzen, sondern nur Zugriff auf die Anlagenkurzwahl haben und dennoch eine Wahl aus einem LDAP-Suchergebnis heraus durchführen möchten. In einem LDAP-Server werden Rufnummern von Personen in der Regel als Langrufnummer im kanonischen Format abgelegt.
Zugangsnummern	Im linken Teil wird die Liste eingerichteter Zugangsnummern / Domain-Informationen (vgl. Abschnitt 7.2.3) angezeigt. Übernehmen Sie die für diesen Switch relevanten Einträge per Pfeil-Taste auf die rechte Seite.
NAC	Im linken Teil wird die Liste eingerichteter Querkennzahlen / NACs (vgl. Abschnitt 7.2.4) angezeigt. Übernehmen Sie die für diesen Switch relevanten Einträge per Pfeil-Taste auf die rechte Seite.
Privater Nummerierungsplan	Im linken Teil wird die Liste eingerichteter Privater Nummerierungspläne / PNPs (vgl. Abschnitt 7.2.5) angezeigt. Übernehmen Sie die für diesen Switch relevanten Einträge per Pfeil-Taste auf die rechte Seite.

Aktionen

Aktion	Beschreibung
Hinzufügen	Prüft die Daten auf Vollständigkeit und fügt den Eintrag zur Liste der Switch-Verbindungen hinzu.
Schließen	Schließt den kompletten Dialog **Eintrag hinzufügen** ohne die Eingaben zu sichern.
Löschen	Löscht eine bestehende Switch-Verbindung. **Hinweis**: Diese Schaltfläche erscheint nur, wenn bereits mindestens eine Switch-Verbindung eingerichtet ist.
Nächste >>	Ruft den nächsten Dialog auf.
<< Vorherige	Ruft den vorherigen Dialog auf.

6.5 Konfiguration eines OpenScape CAP Call Control Proxy (SCCP)

6.5.1 Übersicht

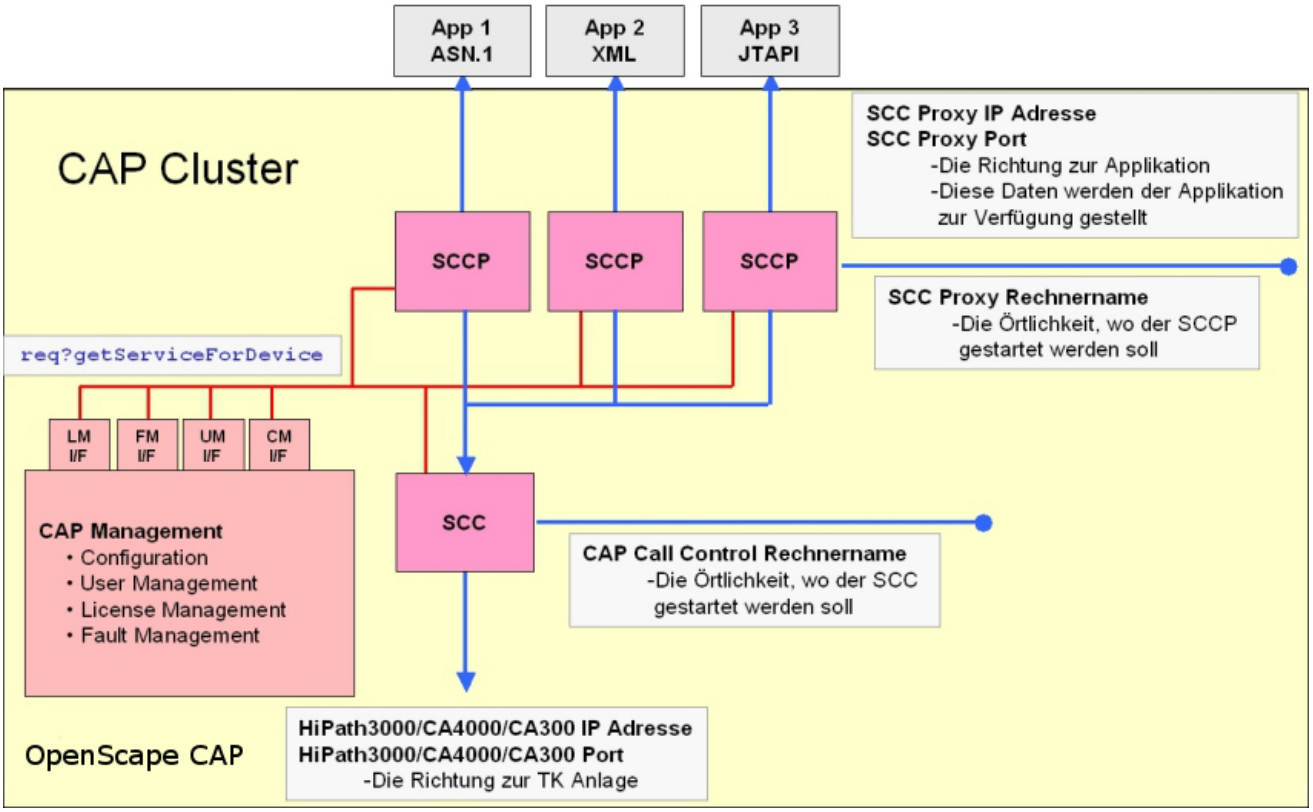
Für jede Applikation, die OpenScape CAP in einer CSTA oder JTAPI Multi-Domain-Konfiguration nutzen möchte, und für jeden XML-PhoneSevice ist eine SCCP-Instanz einzurichten.

SCC Proxies werden nur im “Multi Domain Mode” verwendet. Ein SCCP unterstützt die Protokolle CSTA III ASN.1 und CSTA XML. Ein SCCP unterstützt immer nur eine Verbindung mit einer Applikation. Mehrere SCCP können gleichzeitig eine Verbindung mit demselben SCC aufbauen. Der SCCP hat die Aufgabe der Applikationsauthentifizierung, Benutzerlizenzierung und die Ermittlung der den CAP-Devices zugehörigen SCCs. Er nutzt dafür die Services des CAP Managements.

Bei einem Verbindungsaufbau mit einem SCCP muss eine Applikation zunächst einen ACSE_AARQ schicken. Dieser Request beinhaltet:

- Benutzer
- Passwort
- CSTA-Version
- Applikations-ID
- Native (Mode) true oder false (default)

Nach einer erfolgreichen Authentifizierung wird die Applikations-ID vom SCCP für diese bestehende Verbindung gespeichert und für die spätere Benutzerlizenzierung verwendet. Bei jedem weiteren CSTA-Request (für ein Device) überprüft der SCCP durch eine Verbindung zum CAP Lizenzmanagement (SLM), ob für dieses Device (oder für den zugehörigen Benutzer) eine Lizenz (entsprechend der Applikations-ID) zugeteilt ist. Bei aktivierter implizierter Lizenzzuteilung wird, falls nicht bereits vorhanden, einem Device/Benutzer automatisch eine entsprechende Client-Lizenz zugeteilt. Ist die Lizenzüberprüfung erfolgreich, so speichert der SCCP dieses 3600 Sekunden und leitet den Request an den dem Device zugehörigen SCC weiter.



6.5.2 Konfiguration

Um eine SCCP-Instanz erstmalig einzurichten oder eine bestehende SCCP-Instanz neu zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie im Navigationsbereich auf den Menüpunkt **SCC Proxy**.

   a) Es ist noch keine SCCP-Instanz eingerichtet. Weiter mit 2a.

   b) Es sind bereits eine oder mehrere SCCP-Instanzen eingerichtet. Diese werden Ihnen in einer Liste angezeigt. Weiter mit 2b.

2. Konfigurieren Sie die SCCP-Instanz.

   a) Ist noch keine SCCP-Instanz eingerichtet, klicken Sie auf das Symbol **Neuen Eintrag hinzufügen**.

   b) Sind bereits eine oder mehrere SCCP-Instanzen eingerichtet, werden Ihnen diese in einer Liste angezeigt. Wählen Sie eine SCCP-Instanz aus, indem Sie auf das Symbol **Bearbeiten** der gewählten SCCP-Instanz klicken.

Dialog

Feld	Beschreibung
SCC Proxy Name	Geben Sie hier einen symbolischen Namen für den SCC Proxy ein; dieser Name kann vom Administrator nach Belieben vergeben werden. Er muß innerhalb der gesamten CAP-Installation eindeutig sein. Bis zu 32 Zeichen (Buchstaben, Ziffern, Unterstrich und Bindestrich) sind erlaubt; Leerzeichen sind nicht erlaubt!
SCC Proxy Identifier (optional)	Geben Sie hier einen Bezeichner für den SCC Proxy ein; dieser Bezeichner muss innerhalb der gesamten OpenScape CAP-Installation eindeutig sein und kann nach der Einrichtung nicht mehr geändert werden. Im Diagnose-Agenten wird ein SCCP in der Prozess-Übersicht mit dieser SCCP Id dargestellt. Bis zu 32 Zeichen (Buchstaben, Ziffern, Unterstrich und Bindestrich) sind erlaubt. Akzentbuchstaben sind nur unter Windows Installation unterstüzt. Leerzeichen sind nicht erlaubt!
SCC Proxy Rechnername	Geben Sie hier den Rechnernamen (hostname) des PC ein, auf dem der SCCP-Prozess laufen soll. Anhand des “Rechner-Namens” wird ein PC-Namensverzeichnis im Verzeichnis `<InstDir>\config\` erstellt. Für den SCCP ein Unterverzeichnis mit dem Namen sccp_<SCCP Id> hinzugefügt. Diese Unterverzeichnisse enthalten sämtliche Konfigurationsdateien für diesen zu startenden Prozess. **Hinweis**: Bei verteilter Installation (d.h. der SCCP-PC ist nicht der eigene PC / localhost) ist auf dem hier spezifizierten SCCP-PC unbedingt der OpenScape CAP Service Starter zu installieren (vgl. Abschnitt 4.3).
SCC Proxy IP-Adresse (nicht editierbar)	Hier wird die IP-Adresse des PCs angegeben, auf dem der SCCP-Prozess laufen soll. Sie wird aus dem Rechnernamen ermittelt und nur zur Kontrolle angezeigt.
SCC Proxy Port (optional)	Sie können hier optional den Port angeben, der dem SCCP-Prozess zugeordnet wird. Als Standardwert wird Port **27535** verwendet. Wurde dieser Port bereits durch die CAP-Konfiguration einem anderen SCCP zugewiesen, so wird automatisch der nächste freie Port angeboten (z.B.: 27536)

Feld	Beschreibung
AP Emergency deaktivieren	Hier ist es möglich, die AP Emergency Funktionalität als CAP-Leistungsmerkmal (und damit auf Applikations-Ebene) auszuschalten, während sie auf HiPath / OpenScape 4000-Ebene noch wirkt: Bei einer HiPath / OpenScape 4000 mit AP Emergency Konfiguration kann ein (über ein AP-Shelf abgesetztes) Device vom SCCP nur über den regulären SCC4000 ("SCC ID") erreicht werden. Selbst wenn für das Device unter "Emergency" eine zweite SCC Verbindung eingerichtet wäre, würde diese im Emergency Fall nicht genutzt werden (so dass dieses Device für die Zeitdauer des AP Emergency Modes für die Applikation nicht erreichbar wäre). Das Ausschalten der AP Emergency Funktionalität auf CAP-Ebene macht z.B. Sinn, wenn ? der SCCP nur Verbindungen zu Switches != HiPath / OpenScape 4000 haben wird (AP Emergency ist ein HiPath 4000 Feature) ? der SCCP (über SCC4000) auch Verbindungen zu HiPath / OpenScape 4000-Anlagen hat, das AP Emergency Feature aber an keiner dieser TK-Anlagen genutzt wird ? die übergeordnete Applikation über SCCP und SCC4000 zwar Verbindung zu HiPath / OpenScape 4000-Anlagen mit AP Emergency Konfiguration hat, aber nicht an einer "geräuschlosen" APE Umschaltung interessiert ist **ACHTUNG**: Eine Einschränkung dieses Leistungsmerkmals auf bestimmte Devices oder HiPath /OpenScape 4000-Anlagen ist nicht möglich - die De-/Aktivierung gilt für den SCCP und alle damit verbundenen HiPath /OpenScape 4000-Anlagen!

Aktionen

Aktion	Beschreibung
Hinzufügen	Fügt den Eintrag zur Liste der SCCP Services hinzu.
Schließen	Schließt den kompletten Dialog **Eintrag hinzufügen** ohne die Eingaben zu sichern.
Löschen	Löscht eine bestehende SCCP-Instanz. **Hinweis**: Diese Schaltfläche erscheint nur, wenn bereits mindestens eine SCCP-Instanz eingerichtet ist.

7 Weitere Funktionen von OpenScape CAP Management

Mit OpenScape CAP Management können Sie die komplette OpenScape CAP konfigurieren. Dazu bietet Ihnen das OpenScape CAP Management folgende Funktionen:

- **Service**
  Hier richten Sie die Switch-Verbindungen (SCC) und SCCP-Instanzen ein. Außerdem können Sie für die Verwendung bei Switch-Verbindungen und Devices Domain-Information, Querkennzahlen, PNP sowie Kurzwahlnummern einrichten, den XML Phone Service konfigurieren und URLs für XML Phone Service definieren.
- **Benutzer**
  Dieser Menüpunkt umfasst die Benutzerverwaltung, mit der Sie Benutzer hinzufügen, ändern oder löschen und Benutzer zu Benutzergruppen zusammenfassen können. Gemeinsame Einstellungen wie Standard-Passwörter können hier ebenfalls definiert werden.
- **Device**
  Hier werden die Devices (Phones, Trunks, Huntgroups,...) der verschiedenen TK-Anlagen mit Zuordnung zu einem SCC eingerichtet und modifiziert. Lizenzen werden den Devices zugeordnet.
- **Lizenzen**
  Unter diesem Menüpunkt werden Lizenzen eingerichtet und gelöscht. Es gibt eine Übersicht zu installierten und verwendeten Lizenzen sowie einen Mechanismus zur Steuerung der Lizenz-Zuordnung.
- **Daten**
  Treffen Sie hier die Einstellungen, um Daten in die OpenScape CAP-Datenbank zu importieren oder zu exportieren.
- **Diagnose**
  Unter diesem Menüpunkt starten Sie den CAP Management Diagnose Agent. Es gibt Funktionen zur Überwachung, Konfiguration und Problemdiagnose für alle Komponenten des Systems: Logging-Informationen, Anzeige und Änderung von Konfigurationsdaten, von Zustände von Services und Prozessen, Anzeige beteiligter Hosts, Restart von Prozessen. Außerdem bietet die Funktion "Download Daten" die Möglichkeit, Diagnosedaten zur separaten Analyse in eine Datei zu schreiben.
- **Abmelden**
  zur Beendigung einer CAP Management-Sitzung; es gibt hier keine Untermenüs.
- **Hilfe**
  Hier können Sie sich die Dokumentation zur OpenScape CAP in unterschiedlichen Formaten und Sprachen anzeigen lassen.

Die hier aufgelisteten Funktionen finden Sie als Menüpunkte im Hauptmenü von OpenScape CAP Management wieder. Bei einem Klick auf einen Menüpunkt ändert sich die Auswahlliste im Navigationsbereich und entsprechend auch die Anzeige im Arbeitsbereich.

7.1 Business-Gruppen

HiPath CAP V3.0 SMR4 bietet erstmals eine Unterstützung für Business-Gruppen (BG); diese dienen dazu, den gesamten Administrationsbereich in getrennte Sichtbarkeits- und Verantwortungsbereiche zu gliedern. Der Administrator kann Business-Gruppen und zugeordnete Business-Gruppen-Administratoren (BGAdmin) definieren. Jeder BGAdmin sieht dann nur die Daten der zugeordneten BG und kann auch nur dort administrieren.

Die einer BG zugeordneten Objekte sind

- Benutzer
- Devices
- Lizenzen
- Benutzergruppen
- URLs für XML Phone Service

Um auch die Objekte zu erfassen, die nicht einer bestimmten BG zugeordnet werden sollen, wird mit der Installation automatisch eine "Pseudo"-Business-Gruppe "Standard" bzw. "none" eingerichtet.

Die einem BGAdmin zugänglichen Funktionen sind (jeweils in der zugeordneten BG)

- Benutzer (nur Rolle CTI Benutzer) und Devices anlegen und verwalten
- Daten importieren / exportieren, jeweils beschränkt auf Benutzer und Devices der BG
- Benutzergruppen einrichten und verwalten
- Attribute der BG verwalten
- URLs für XML Phone Service definieren
- Zugeteilte Lizenzen verwalten
- sowie unbeschränkter Zugriff auf Diagnose-Funktionen

Ausschließlich dem "Super"-Administrator zugängliche Funktionen sind

- Services (SCC, SCCP, XML Phone Service) konfigurieren
- Domains / PNPs / NACs einrichten
- BGs einrichten und löschen
- Administratoren und BG-Administratoren anlegen und verwalten
- Lizenzen installieren / deinstallieren
- Installierte Lizenzen auf BGs aufteilen
- Sicherheits-Einstellungen für Kommunikationsbeziehungen verwalten

Die nachfolgenden Beschreibungen beziehen sich immer auf die komplette Admin-Funktionalität; die Bereiche, die für BGAdmin nicht zugänglich sind, sind mit "**nicht für BGAdmin**" gekennzeichnet.

7.2 Service

Im Menüpunkt **Service** wird die Konfiguration der Call Control Services und Call Control Proxies durchgeführt. Außerdem können Sie den XML Phone Service konfigurieren und Kurzwahlnummern vergeben.

7.2.1 Switch-Verbindung (nicht für BGAdmin)

Die Konfiguration der Call Control Services mit OpenScape CAP Management ist in Abschnitt 6.2 bis Abschnitt 6.4 beschrieben.

7.2.2 SCC Proxy (nicht für BGAdmin)

Die Konfiguration der Call Control Proxies mit OpenScape CAP Management ist in Abschnitt 6.5 beschrieben.

7.2.3 Domain-Information (nicht für BGAdmin)

Domain-Informationen werden als Teil der Wahlinformation zum Einrichten einer TK-Anlage verwendet; sie können hier definiert, mit einem Identifier versehen und dann bei der Konfiguration von Switch-Anbindungen mehrfach verwendet werden.

1. Klicken Sie auf **Service** im Hauptmenü und wählen den Menüpunkt **Domain-Information** im Navigationsbereich aus. Es wird eine Liste bereits eingerichteter Domain-Informationen angezeigt, die ausgewählt / modifiziert werden können.
2. Zum Einrichten einer neuen Domain-Information klicken Sie auf die Schaltfläche  in der Kopfzeile.

   Es erscheint das Fenster für die Eingabe einer neuen Domain-Information:

Feld	Beschreibung
Domain Name	Geben Sie hier einen sprechenden Namen ein.
Domain Id (optional)	Hier können Sie optional eine Id eingeben; diese Id muss systemweit eindeutig sein, sie wird ggf. automatisch vergeben.
Landesvorwahl	Landeskennzahl (z.B. "49“ für Deutschland). Durch sie wird die Standardwahlregel eines Landes abgeleitet. Sie definiert den ersten Teil einer Device-ID im kanonischen Format, welche den jeweiligen SCCs zugeordnet wird. Um inkonsistente Einstellungen zu verhindert, ist hier keine direkte Dateneingabe möglich. Wählen Sie im Pull-Down-Menü eines der unterstützten Länder aus; der entsprechende Wert wird dann automatisch übertragen.
Nationale Vorwahl	Kennzahl (Präfix) für eine nationale E.164-Rufnummer. Sie wird implizit aus der Wahlregel eines Landes abgeleitet und muss nur dann konfiguriert werden, wenn sie nicht dem nationalen Standard entspricht. Die "Nationale Vorwahl" (implizit/explizit) wird vom SAT zur eindeutigen Identifizierung eines Devices verwendet, falls in einem Event eine Rufnummer mit der "Nationalen Vorwahl" übertragen wird.
Internationale Vorwahl	Kennzahl (Präfix) für eine internationale E.164-Rufnummer. Sie wird implizit aus der Wahlregel eines Landes abgeleitet und muss nur dann konfiguriert werden, wenn sie nicht dem nationalen Standard entspricht. Die "Internationale Vorwahl" (implizit/explizit) wird vom SAT zur eindeutigen Identifizierung eines Devices verwendet, falls in einem Event eine Rufnummer mit der "Internationalen Vorwahl" übertragen wird
PBX-Format	kann je nach den Gegebenheiten einer TK-Anlage auf "international" oder "national" (d.h. US-Format!) eingestellt werden.

Feld	Beschreibung
Amtsvorwahl , Internationale Amtsvorwahl	Kennzahl für den Amtsausstieg (z.B. "0"). Die "Amtsvorwahl" wird vom SAT zur eindeutigen Identifizierung eines Devices verwendet, falls in einem Event eine Rufnummer mit der "Amtsvorwahl" übertragen wird. Weiterhin nutzt ComAssistant diese Kennzahl bei jeder gehenden externen Wahl.
Ortsvorwahl (optional)	Geben Sie hier die Ortskennzahl (z.B. "89" für München) ein. Sie definiert den zweiten Teil einer Device-ID im kanonischen Format, welche den jeweiligen SCCs zugeordnet wird.
Hauptnummer	Geben Sie hier die Nummer des Hauptanschlusses innerhalb eines Ortsnetzes (z.B. "722" für Unify, München, Hofmannstraße) ein. Sie definiert den dritten Teil einer Device-ID im kanonischen Format, welche den jeweiligen SCCs zugeordnet wird.
Overlap (optional)	Anzahl der überlappenden Ziffern von Hauptnummer und Extension, z.B. bei 49(89)722:1, d.h. bei Overlap=1 ist für das Device +49(89)722-345 das PBX-Format -> 2345, d.h. die letzte Ziffer der Hauptnummer (hier: 2) wird der Extension (hier: 345) vorangestellt, die resultierende Rufnummer 2345 ist in der PBX konfiguriert. Es ist nicht erlaubt 0 einzustellen!
Virtual node Code	Es kann speziell in dem Fall von einer HiPath / OpenScape 4000 Anlage benutzt werden, wenn die Leistunsmerkmal „Non-unique Nummerierung Plan“ (NUNP) aktiviziert. Bitte konfigurieren Sie diese Zahl, wenn die Domaininformation zu einem SCCHiPath4000 Anschluss, der NUNP Konfiguration hat, zugewiesen wird. Für mehrere Information bitte sehe das Kapitel „5.6 (NUNP)“ von dem OpenScape CAP Application Developers’ Guide Vol. 1.

3. Geben Sie die gewünschten Daten ein, und bestätigen Sie mit **Hinzufügen**.
4. Die neue Domain-Information wird in der Übersichtsliste angezeigt.
5. Klicken Sie im Hauptdialog auf **Speichern**, um die Konfiguration endgültig einzutragen.

   Die Domain-Information ist jetzt eingerichtet und kann beim Einrichten oder Ändern der PBX-Zugangsdaten verwendet werden.

   Wenn die Domaininformation geändert wird, dann soll der OpenScape CTI Dienst neugestartet werden!

7.2.4 Querkennzahlen (nicht für BGAdmin)

Querkennzahlen (Network Access Codes - NAC) werden als Teil der Wahlinformation zum Einrichten einer TK-Anlage verwendet; sie können hier definiert, mit einem Identifier versehen und dann bei der Konfiguration von Switch-Anbindungen mehrfach verwendet werden.

1. Klicken Sie auf **Service** im Hauptmenü und wählen den Menüpunkt **Querkennzahlen** im Navigationsbereich aus. Es wird eine Liste bereits eingerichteter Querkennzahlen angezeigt, die ausgewählt / modifiziert werden können.
2. Zum Einrichten einer neuen Querkennzahl klicken Sie auf die Schaltfläche  in der Kopfzeile.

   Es erscheint das Fenster für die Eingabe einer neuen Querkennzahl:

Feld	Beschreibung
NAC Name	Geben Sie hier einen sprechenden Namen ein.
NAC Id (optional)	Hier können Sie optional eine Id eingeben; diese Id muss systemweit eindeutig sein, sie wird ggf. automatisch vergeben.
NAC	NAC (Node Access Code) ist bei offen numerierten HiPath / OpenScape Netzen die Knotenkennzahl, d.h. die Rufnummer eines PBX-Knotens. Diese Knotenkennzahl wird der Extension beim Wählen vorangestellt (z.B. 96-2345 bei NAC=96 und 99-2345 bei NAC=99). Dieselbe Extension (hier: 2345) kann dadurch in mehreren PBX-Knoten (hier: 96 und 99) konfiguriert sein, die Eindeutigkeit ergibt sich erst durch das Voranstellen des NAC. Der NAC wird vom SAT zur eindeutigen Identifizierung eines Devices verwendet, falls in einem Event eine Rufnummer mit der "NAC" übertragen wird.
Overlap (optional)	Anzahl der überlappenden Ziffern von NAC und Extension, z.B. bei 962:1, d.h. bei Overlap=1 ist für das Device 962-345 das PBX Format -> 2345, d.h. die letzte Ziffer des NAC's (hier: 2) wird der Extension (hier: 345) vorangestellt, die resultierende Rufnummer 2345 ist in der PBX konfiguriert.

3. Geben Sie die gewünschten Daten ein, und bestätigen Sie mit **Hinzufügen**.
4. Die neue Querkennzahl wird in der Übersichtsliste angezeigt.
5. Klicken Sie im Hauptdialog auf **Speichern**, um die Konfiguration endgültig einzutragen.

   Die Querkennzahl ist jetzt eingerichtet und kann beim Einrichten oder Ändern der PBX-Zugangsdaten verwendet werden.

7.2.5 PNP (nicht für BGAdmin)

Private Rufnummernpläne (Private Numbering Plans - PNP) werden als Teil der Wahlinformation zum Einrichten einer TK-Anlage verwendet; sie können hier definiert, mit einem Identifier versehen und dann bei der Konfiguration von Switch-Anbindungen mehrfach verwendet werden.

1. Klicken Sie auf **Service** im Hauptmenü und wählen den Menüpunkt **PNP** im Navigationsbereich aus. Es wird eine Liste bereits eingerichteter PNPs angezeigt, die ausgewählt / modifiziert werden können.
2. Zum Einrichten einer neuen Querkennzahl klicken Sie auf die Schaltfläche  in der Kopfzeile.

   Es erscheint das Fenster für die Eingabe eines neuen PNP:

Feld	Beschreibung
PNP Name	Geben Sie hier einen sprechenden Namen ein.
PNP Id (optional)	Hier können Sie optional eine Id eingeben; diese Id muss systemweit eindeutig sein, sie wird ggf. automatisch vergeben.
PNP Amtsvorwahl	Kennzahl für den Ausstieg in ein privat nummeriertes Netz. Diese Netze sind nach ECMA-155 PNP (Private Network Numbering Plan) aufgebaut. Die "PNP Amtsvorwahl" wird vom SAT zur eindeutigen Identifizierung eines Devices verwendet, falls dieser in einem Event zusammen mit einer Rufnummer übertragen wird.
Vorwahl für Stufe 2	Kennzahl (Präfix) für eine Level 2 PNP Rufnummer. Der "Prefix level 2 code" wird vom SAT zur eindeutigen Identifizierung eines Devices verwendet, falls dieser in einem Event zusammen mit einer Rufnummer übertragen wird.
Vorwahl für Stufe 1	Kennzahl (Präfix) für eine Level 1 PNP Rufnummer. Der "Prefix level 1 code" wird vom SAT zur eindeutigen Identifizierung eines Devices verwendet, falls dieser in einem Event zusammen mit einer Rufnummer übertragen wird.
Nummer für Stufe 2 (optional)	PNP Level 2 Kennzahl (entspricht bei E.164 der Landeskennzahl) Der "Level 2 code" definiert den ersten Teil einer Device-ID im kanonischen Format, welche den jeweiligen SCCs zugeordnet wird.

Feld	Beschreibung
Nummer für Stufe 1 (optional)	PNP Level 1 Kennzahl (entspricht bei E.164 der Ortskennzahl) Der "Level 1 code" definiert den zweiten Teil einer Device-ID im kanonischen Format, welche den jeweiligen SCCs zugeordnet wird.
Hauptnummer	PNP Level 0 Kennzahl (entspricht bei E.164 der Hauptnummer) Der "Local code" definiert den dritten Teil einer Device-ID im kanonischen Format, welche den jeweiligen SCCs zugeordnet wird.
Overlap (optional)	Anzahl der überlappenden Ziffern von "Local code" und Extension, z.B. bei 33-44-552:1, d.h. bei Overlap=1 ist für das Device 3344552-345 das PBX Format -> 2345, d.h. die letzte Ziffer des Local codes (hier: 2) wird der Extension (hier: 345) vorangestellt, die resultierende Rufnummer 2345 ist in der PBX konfiguriert.

3. Geben Sie die gewünschten Daten ein, und bestätigen Sie mit **Hinzufügen**.
4. Der neue PNP wird in der Übersichtsliste angezeigt.
5. Klicken Sie im Hauptdialog auf **Speichern**, um die Konfiguration endgültig einzutragen.

   Der PNP ist jetzt eingerichtet und kann beim Einrichten oder Ändern der PBX-Zugangsdaten verwendet werden.

7.2.6 Kurzwahlnummern (nicht für BGAdmin)

Kurzwahlnummern werden von der CTI-Anwendung ComAssistant zur Wahloptimierung verwendet. Ihre Nutzung ist allerdings nicht zwingend erforderlich. Die Konfiguration ist daher optional. Kurzwahlnummern sind sinnvoll, wenn einige ComAssistant-Benutzer nur eine Anlagenkurzwahlberechtigung besitzen, sie aber aus einem LDAP-Suchergebnis heraus wählen möchten und der LDAP-Server die vorhandenen Rufnummern nur im kanonischen Format unterstützt (Standard). Die Umsetzung von kanonischer Rufnummer in Kurzwahlnummer erfolgt in ComAssistant.
Die Kurzwahlnummern werden in frei konfigurierbaren Listen verwaltet. In der SCC-Konfiguration kann einem SCC jeweils nur eine Liste zugeordnet werden.

1. Klicken Sie auf **Service** im Hauptmenü und wählen den Menüpunkt **Kurzwahlnummern** im Navigationsbereich aus.

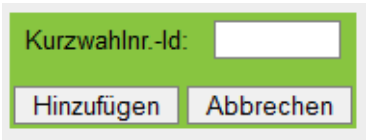
   Definieren Sie einen Namen für den Standort durch eine **Kurzwahlnummern-ID**, die als Kurzwahlnummern-Listenbezeichnung verwendet wird. Zu jedem selektierten Eintrag im ersten Auswahlfenster **Kurzwahlnummern-Id** werden die bereits zugeordneten Einträge

im zweiten Auswahlfenster **Kurzwahlnummer / Langwahlnummer** angezeigt. Die Kurzwahlnummer-Id muss im gesamten System eindeutig sein. Geben Sie möglichst eine sprechende Bezeichnung ein (z.B. die genaue Bezeichnung des Standorts); diese wird bei Einrichtung einer PBX in einem Auswahldialog angeboten.

Zum Einrichten einer neuen Kurzwahlnummer gehen Sie wie folgt vor:

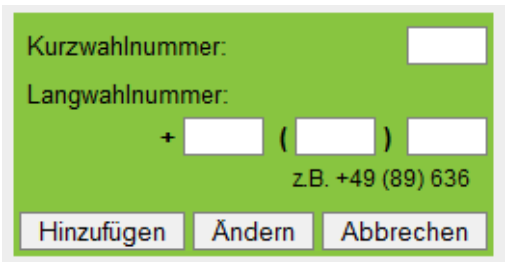
2. Klicken Sie auf die Schaltfläche  in der Kopfzeile.

   Es erscheint das Fenster für die Eingabe der Kurzwahlnummer-Id:



3. Geben Sie den Text in das Eingabefeld ein und bestätigen Sie mit **Hinzufügen**. Das Fenster wird geschlossen und Ihre Eingabe erscheint im Auswahlfenster **Kurzwahlnummern-Id**.

   Es erscheint das Fenster für die Eingabe der Nummernkombination:



4. Geben Sie die Kurzwahlnummer und die Langwahlnummer ein.

   Die Langwahlnummer besteht aus drei Teilen: Landesvorwahl ohne führendes **+**; Ortsvorwahl ohne führende **0**; und Hauptnummer der Nebenstellen-Anlage.

> Beachten Sie unbedingt das Nummern-Format.

5. Bestätigen Sie mit **Hinzufügen** und Ihre Eingabe erscheint im Auswahlfenster **Kurzwahlnummer / Langwahlnummer**.
6. Klicken Sie auf **Abbrechen**, um das Fenster zu schließen.
7. Klicken Sie im Hauptdialog auf **Speichern**, um die Konfiguration endgültig einzutragen.

   Die Kurzwahlnummer ist jetzt eingerichtet und kann beim Einrichten oder Ändern der PBX-Zugangsdaten verwendet werden.

7.2.7 XML Phone Service (nicht für BGAdmin)

Allgemeiner Überblick

Mit Hilfe von XML Phone Services für OpenScape CAP können XML-Entwickler eine Vielzahl von Anwendungen für Endgeräte einer HiPath 4000 oder HiPath 3000 erstellen und integrieren.

Über den (optionalen) WML-Adapter können WAP-fähige Endgeräte, wie z.B. optiPoint 600 oder auch Mobiltelefone, auf XML-Anwendungen zugreifen. Künftige Erweiterungen der CAP XML Phone Services unterstützen auch einen sprachgesteuerten Zugriff.

CAP-Anwender sind damit in der Lage, neue Anwendungen zu entwickeln, bei denen das Endgerät (leitungsvermittelt oder IP-basiert) als Ein-/Ausgabegerät verwendet wird. Zudem lassen sich Büroanwendungen dahin gehend erweitern, dass per Telefon auf sie zugegriffen werden kann. Die Bereitstellung der XML-Anwendungen erfolgt über das von Standard-Webservern (z.B. Microsoft IIS, Apache, EJB Server, Servlet Engine) unterstützte HTTP/HTTPS-Protokoll. Dabei ist es unerheblich, welche Programmiersprache für die XML-Anwendung verwendet wird, d.h. die XML-Anwendung kann sowohl mit Hilfe einer Skriptsprache wie PHP oder Perl als auch mit Standard-Programmiersprachen wie C# in der .Net-Umgebung, Java oder einer anderen Programmiersprache entwickelt werden.

Beispiele für entsprechende XML-Anwendungen wären u.a.:

- Informationssysteme (z.B. Börsenkurse, Reiseverbindungen, Kundenauskunft usw.)
- Persönliche oder Gruppen-Adressbücher
- Management-Anwendungen (z.B. zur PIN-Verwaltung)
- Ändern von Präsenzkontexten
- Aktivierung einer Anrufumleitung aus einer Liste von möglichen Zielen
- Instant Messaging

Zusätzliche Information zum XML Phone Service ist verfügbar über den XMLPS Application Developers' Guide der Teil der CAP-Dokumentation ist; nach Abschluss der CAP Installation ist diese Information auch online über die URL `http://<CAP host>:8172` abrufbar.

XML PhoneService

Der XML PhoneService (XMLPS) ist selbst eine CSTA XML-Applikation, die immer auf einem SCCP aufsetzt. Ein XMLPS kann unterschiedliche XML-Applikationen gleichzeitig bedienen. Wird der Einsatz von mehr als einem XML PhoneService gewünscht, so muss pro XMLPS ein neuer SCCP eingerichtet werden. Außerdem benötigt jeder XMLPS zwingend eine individuelle TDD-Applikationsnummer (default = 999).

Diese Änderung erfolgt in der Konfigurationsdatei `<InstDir>\XMLPSSvc_<XMLPS-ID>\telas.cfg` mit dem Parameter "`globalAppId = ...`" für jeden eingerichteten XMLPS.

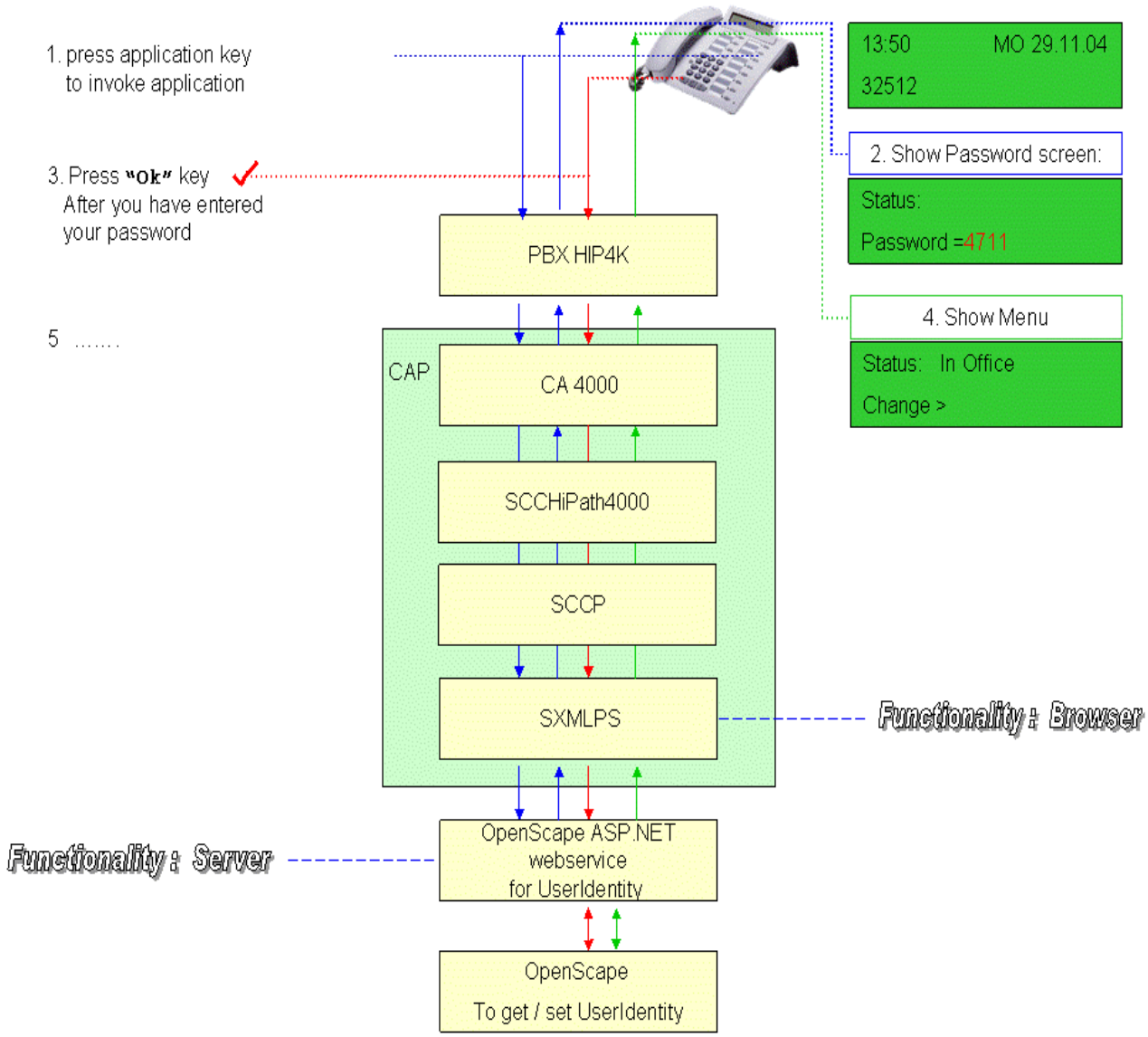
XMLPS Servicestart: beim Start des Service meldet dieser sich bei SCCP mit einem vorgeleisteten Benutzer/Password und der Applikations-ID "XMLPS" an. Diese Applikations-ID muss als Lizenz im CAP Management einem Benutzer zugeteilt worden sein. Die auf dem XMLPS aufsetzende Applikation wird hingegen nicht expliziert lizenziert.

XMLPS Leistungsmerkmale: die CAPPhone XML Objekte werden vom XMLPS zur Darstellung von Menüs, Eingabeformate oder zur reinen Textdarstellung an Optiset oder OptiPoint Endgeräten an einer HiPath 4000 oder HiPath 3000 verwendet. Der XML Phone Server verhält sich wie ein Browser, der die Endgeräte als Ausgabegeräte nutzt. Die Kommunikation zwischen Endgerät und XMLPS-Applikation erfolgt durch den Telefon-Datendienst (TDD).

Folgende Leistungsmerkmale werden unterstützt:

- Zwei- oder vier-zeiliges Display mit 16 oder 24 Zeichen pro Zeile (entsprechend der Konfiguration über XMLPS Device Typ)
- Alle automatisch generierten Begriffe (EXIT, BACK, SUBMIT) sind in englisch, deutsch und französisch verfügbar. Weitere Sprachen für die Kommandobegriffe muss eine Applikation explizit selbst definieren.
- Audio Indikator (BEEP, SILENT).
- Applikationstasten mit assoziierter Lampe, wobei der Lampenstatus verändert werden kann (STEADY, WINK, FLUTTER, OFF).
- "OK" Taste.
- die normale Tastatur wird im Numerischen- und im Text-Mode unterstützt.

XMLPS Applikationsbeispiel: Die nachfolgende Grafik zeigt den möglichen Kommunikationsstart eines Endgeräts mit einer XMLPS Applikation.



XMLPS Invoke Interface: das Invoke Interface wird von einer Applikation zur Ansteuerung von Endgeräten (CAPPhone Execute) durch eine "case sensitive" URL adressiert. Eine Ansteuerung kann zu jeder Zeit an einem Endgerät durchgeführt werden. Das Verhalten des XML Phone Servers steht in Abhängigkeit vom Verbindungsstatus des Endgeräts.

- Keine XMLPS-Applikation ist gestartet - In diesem Fall werden alle XMLPhoneExecute Nachrichten sofort ausgeführt:
  - falls angesteuert, wird ein Texttitel für 5 Sekunden angezeigt.
  - falls angesteuert, wird ein Signalton (BEEP) ausgegeben.

- falls angesteuert, wird die Lampe der Taste angesteuert, die in der CAP-Konfiguration mit der entsprechenden URL konfiguriert wurde. Dieser Lampenstatus wird beibehalten, solange er nicht überschrieben oder die zugeordnete XMLPS-Applikation gestartet wird.

- Eine XMLPS-Applikation ist gestartet - In diesem Fall wird der Lampenstatus der Taste gesetzt, die dieser Applikations-URL zugeordnetet ist.
  - Dieser Status ist abhängig von dem Konfigurationsparameter `"lampModeActiv"` in der Datei `"telas.cfg"` eines XMLPS.
  - Jede weitere Invoke Nachricht überschreibt den Lampenstatus.
  - Deshalb werden alle CAPPhoneExecute Aufträge erst nach Beendigung der aktiven Applikation ausgeführt.

Um einen XML Phone Service erstmalig einzurichten oder einen bestehenden XML Phone Service neu zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie auf **Service** im Hauptmenü und wählen Sie den Menüpunkt **XML Phone Service** im Navigationsbereich aus.
   a) Es ist noch kein XML Phone Service eingerichtet. Weiter mit 2a.
   b) Es ist bereits ein XML Phone Service eingerichtet. Dieser wird Ihnen in der "Liste der XML Phone Services" angezeigt. Weiter mit 2b.
2. Konfigurieren Sie den XML Phone Service.
   a) Ist noch kein XML Phone Service eingerichtet, klicken Sie auf das Symbol **Neuen Eintrag hinzufügen**.
   b) Ist bereits ein XML Phone Service eingerichtet, werden Ihnen dieser in der "Liste der XML Phone Services" angezeigt. Wählen Sie einen XML Phone Service aus, indem Sie auf das Symbol **Bearbeiten** des XML Phone Services klicken.

3. Füllen Sie die nachstehend beschriebenen Felder aus:

Feld	Beschreibung
Phone Service Name	Geben Sie hier einen symbolischen Namen für den XML Phone Service ein. Dieser Name kann vom Administrator nach Belieben vergeben werden. Er muss innerhalb der gesamten CAP-Installation eindeutig sein. Bis zu 32 Zeichen (Buchstaben, Ziffern, Unterstrich und Bindestrich) sind erlaubt.
Phone Service Id (optional)	Geben Sie hier einen Bezeichner für denXML Phone Service ein; dieser Bezeichner muß innerhalb der gesamten OpenScape CAP-Installation eindeutig sein. Er wird später bei der Zuordnung von Endgeräten einer HiPath 4000 zu einem XMLPS und damit zu einer bestimmten XMLPS-Applikation benötigt und um den XMLPS-Prozess im Diagnose Agent eindeutig darzustellen. Bis zu 32 Zeichen (Buchstaben, Ziffern, Unterstrich und Bindestrich) sind erlaubt.
SCC Proxy Id	Wählen Sie den SCCP aus, der nur von diesem spezifischen XMLPS genutzt wird.
Phone Service Rechner Name	Geben Sie hier den Namen des Rechners an, auf dem der Prozess “sxmlps” läuft. Anhand des “Rechner-Namens” wird ein PC-Namensverzeichnis im Verzeichnis `<Inst-Dir>\config\` erstellt. Für den XMLPS wird ein Unterverzeichnis mit dem Namen `XMLPhoneSvc_<Phone Service Id>` hinzugefügt. Diese Unterverzeichnisse enthalten sämtliche Konfigurationsdateien für diesen zu startenden Prozess.
Phone Service Rechner IP-Adresse (optional)	Geben Sie hier die IP-Adresse des Rechners an, auf dem der Prozess "sxmlps" läuft. Wenn Sie nichts eingeben, wird die IP-Adresse aus dem Rechnernamen ermittelt.
Invoke Interface Port	Über die hier festlegbare Port-Nummer kann das Invoke Interface Servlet adressiert werden. Die Standard-Port-Nummer ist "3102". Über das Invoke-Interface erfolgt die Ansteuerung der Endgeräte-Displays.
XML Phone Service deaktivieren	Aktivieren Sie diese Option, wenn während des Hochlaufens von OpenScape CAP kein bereits konfigurierter XML Phone Service starten soll.

4. Schließen Sie Ihre Eingaben mit einer der folgenden Aktionen ab:

Aktion	Beschreibung
Hinzufügen bzw. **Ändern**	Fügt den Eintrag zur "Liste der XML Phone Services" hinzu.
Abbrechen bzw. **Schließen**	Schließt den Dialog ohne die Eingaben zu sichern.
Löschen	Löscht den bestehenden XML Phone Service. **Hinweis**: Diese Schaltfläche erscheint nur, wenn bereits ein XML Phone Service eingerichtet ist.

7.2.8 URLs für XML Phone Service

Sie können an einem Endgerät (Device der HiPath 4000) durch Drücken einer speziell eingerichteten Taste eine XML-Anwendung aufrufen und einen Dialog mit dieser beginnen. Dazu muss in der HiPath 4000 pro XMLPS Applikations-URL eine Taste am Endgerät als Namenstaste mit dem Ziel “TDD-Applikationsnummer und der zugehörigen Tastennummer” eingerichtet sein. Im nächsten Schritt werden einem “Phone-Device” (siehe Abschnitt 7.4.1, “Device hinzufügen”) die hier konfigurierten URLs diesen Endgerätetasten zugeordnet. Alle XMLPS Applikations-URLs werden in einer Liste im CAP Management verwaltet. Diese Liste mit den URLs gilt für alle eingerichteten XML Phone Services innerhalb OpenScape CAP.

Fügen Sie hier die URLs der XML Phone Service Anwendungen hinzu, die später den "Phone Devices" zugeordnet werden können. Die XMLPhoneService Standardapplikationen sind bereits eingerichtet.

1. Klicken Sie auf **Service** im Hauptmenü und wählen den Menüpunkt **URLs für Phone Service** im Navigationsbereich aus.
2. Füllen Sie die Felder wie in nachstehender Tabelle beschrieben aus:

Feld	Beschreibung
Business Gruppe (für BGAdmin fest eingestellt)	Die Default-Auswahl ist "Standard" bzw. "none". Zusätzliche BGs werden zur Auswahl angeboten sobald BGs eingerichtet wurden. Die URLs werden in der angegebenen BG eingerichtet; diese Zuordnung kann später nicht mehr verändert werden (kein BG-Wechsel).
URL	Geben Sie hier die URL einer XML Phone Service Anwendung ein inkl. aller Parameter. Die Parameter sind für alle Benutzer gleich.

Feld	Beschreibung
URL Name	Geben Sie hier einen symbolischen Namen für die URL des XML Phone Services ein. Dieser Name kann vom Administrator nach Belieben vergeben und genutzt werden. Er wird intern nicht verwendet. Bis zu 32 Zeichen (Buchstaben, Ziffern, Unterstrich und Bindestrich) sind erlaubt.
URL Beschreibung	Geben Sie hier bei Bedarf eine genauere Beschreibung für die URL an.

3. Klicken Sie auf die Schaltfläche **Hinzufügen** und Ihr Eintrag erscheint in dem unteren Fenster.

   Mit der Schaltfläche **Ändern** können Sie einen bestehenden Eintrag zu einer URL abändern und mit der Schaltfläche **Löschen** können Sie den Eintrag löschen.

7.3 Benutzer

Im Hauptmenü unter **Benutzer** sind die Funktionen zur Administration von Benutzern des OpenScape CTI-Systems zusammengefasst, wie z.B.:

- Benutzer hinzufügen,
- Benutzer suchen,
- Benutzereinträge ändern,
- Benutzer zu Benutzergruppen zusammenfassen,
- Sicherheitseinstellungen verwalten (wie z.B. Passworteinrichtung und Authentifizierungs-Modi)

Applikations-Authentifizierung

Eine Applikation muss nach dem Verbindungsaufbau mit einem SCCP immer einen ACSE_AARQ Request schicken. Der in diesem Request enthaltene Benutzer/Passwort (z.B. CAP/123) muss mit einem CAP CTI- oder CAP-Admin-Benutzer übereinstimmen. Ein entsprechender http-Request `(http://<fqdn>:8170/mgmnt/auth/req?authenticate=<User ID>&passwd=<Password>&encoding=b64)` wird vom SCCP an das CAP Benutzermanagement gestellt. Wird der Benutzer erfolgreich authentifiziert, wird die TCP/IP-Verbindung zur Applikation gehalten. Ist die Authentifizierung nicht erfolgreich, so wird die TCP/IP-Verbindung zur Applikation unterbrochen.

Die im ACSE_AARQ enthaltene "ApplicationID“ ist zu diesem Zeitpunkt irrelevant. Sie wird vom SCCP gespeichert und für eine spätere CTI Client Lizenzierung (anhand der Rufnummer im kanonischen Format) von CSTA-Requests verwendet. In gleicher Weise arbeitet auch der SCC mit der vom CAP TCSP optional übermittelten ApplikationsID im TAPI `“lineDevSecificFeature”`.
Ein entsprechender http-Request `(http://<fqdn>:8170/mgmnt/admin/req?registerLicense= <ApplicationID>&userId=<DeviceID>)` wird vom SCCP/SCC an das CAP Lizenzmanagement gestellt. Ist eine Lizenzüberprüfung erfolgreich gewesen, so speichert der SCCP/SCC diese Information für 3600 Sekunden.

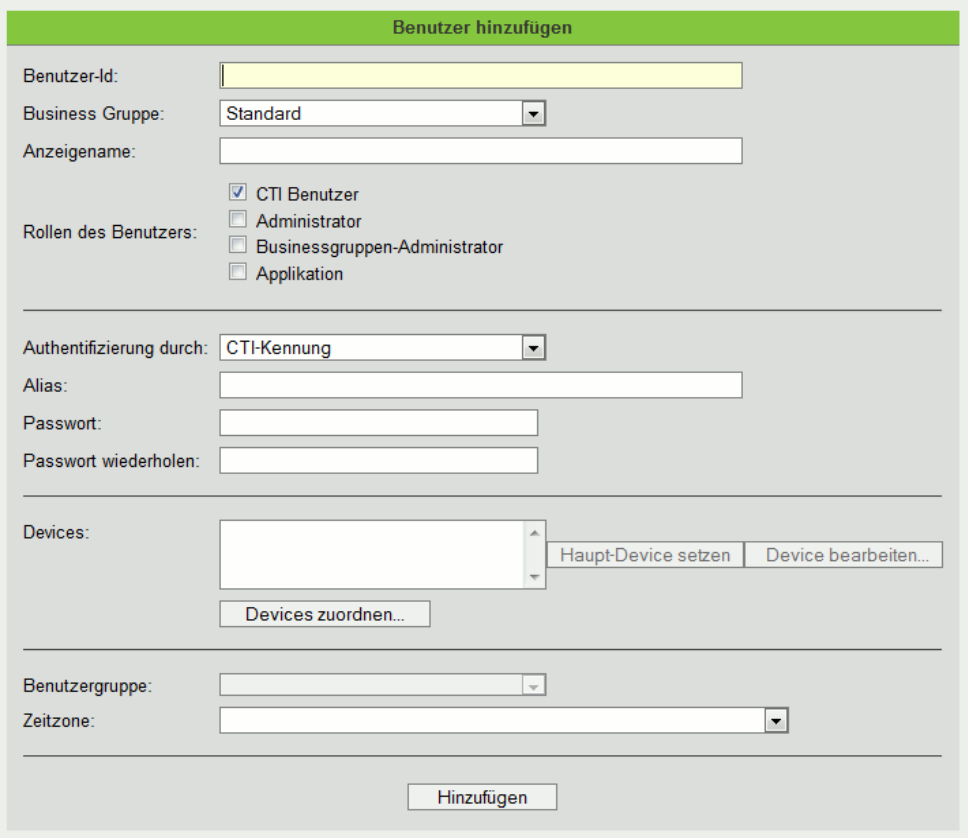
ComAssistant: die Applikation ComAssistant nutzt das CAP Benutzermanagement, um eine Authentifizierung seiner Applikationsbenutzer durchführen zu lassen. Zur eindeutigen Identifizierung eines CAP Benutzers können Benutzer-Id, Alias (-Name) oder Device-Id (Rufnummer im kanonischen Format) genutzt werden.

SimplyPhone For Outlook/Notes: diese TAPI basierenden Applikationen unterstützen nur die Device-ID (Rufnummer im kanonischen Format) zur eindeutigen Identifizierung eines CAP Benutzers.

7.3.1 Benutzer hinzufügen

Sie können Benutzer mit verschiedenen Rollen bzw. Rechten einrichten. Die Authentifizierung kann durch OpenScape CAP Management oder durch das Betriebssystem Windows 2000/ 2003/XP erfolgen.

1. Klicken Sie auf **Benutzer** im Hauptmenü und wählen Sie den Menüpunkt **Hinzufügen** im Navigationsbereich aus.



2. Geben Sie in die Felder die Daten für den neuen Benutzer ein. Die Felder sind in der nachstehenden Tabelle beschrieben.

   Dialog Benutzer hinzufügen

Feld	Beschreibung
Benutzer-Id	Die Benutzer-Id identifiziert den Benutzer eindeutig und ist zwingend. Existiert schon ein Benutzer mit dieser Id, so erscheint eine Fehlermeldung. Der Benutzer kann sich mit dieser Benutzer-ID anmelden. Optional besteht die Möglichkeit, sich auch mit dem "Alias" oder der Telefonnummer als Benutzer zu authentifizieren. ACHTUNG! Sollten vor einem Benutzerdatenimport manuell bereits CTI-Benutzer eingerichtet worden sein, so müssen die Benutzer-IDs zwingend gleich der entsprechenden Rufnummer des zugeordneten Phone-Devices ohne Sonderzeichen sein. Ist dies nicht der Fall, so führt der Benutzerdatenimport zu gravierenden Datenbankfehlern. Es ist auch nicht möglich, zunächst die Benutzerdaten zu exportieren und anschließend wieder zu importieren!
Anzeigename	Der Anzeigename wird für Meldungen und Anzeigen verwendet, die diesen Benutzer betreffen (z. B. *Das Journal für <Anzeigename> enthält keine Einträge*). Der Anzeigename wird derzeit nur von der Applikation ComAssistant verwendet.
Rollen des Benutzers	Der Benutzer kann in der Rolle ? CTI-Benutzer; “normaler” Anwender mit zugeordneten Devices ? Administrator, mit Zugriff auf Funktionen des OpenScape CAP Management (nicht für BGAdmin) ? Businessgruppen-Administrator, mit eingeschränkter Administrator-Berechtigung für die weiter unten definierte Business-Gruppe (nicht für BGAdmin) ? Applikation, zur generischen Nutzung durch eine Applikation, ohne zugeordnete Devices (nicht für BGAdmin) eingerichtet werden. Eine Applikation kann generell über einen "Applikation"-Benutzer oder individuell über einzelne CTI-Benutzer authentifiziert werden.

Feld	Beschreibung
Authentifizierung durch	Über das Aufklappmenü können Sie zwei verschiedene Arten der Authentifizierung wählen: ? **CTI-Kennung:** Das Login wird vollständig von OpenScape CAP Management abgewickelt. Dazu müssen Sie einen Aliasnamen und ein Passwort vergeben. ? **System-Kennung:** Hierbei wird ein CTI-Benutzer mit einem Windows-Benutzer (einer Domäne oder der lokalen Benutzerverwaltung) verknüpft. Bei einer CAP-Authentifizierung muss ein CTI-Benutzer seine Benutzer-Id oder seine Device-Id und das Passwort des Windows-Benutzers eingeben. Der Vorteil hierbei ist, dass der CTI-Benutzer nur noch das Windows-Passwort behalten muss.
Alias (nur bei Authentifizierung durch CTI-Kennung)	Neben der Benutzer-Id, die im System eindeutig ist und vom Benutzer nicht geändert werden kann, kann ein Alias vergeben werden, der ebenfalls eindeutig sein muss. Dieser Alias kann vom Benutzer jederzeit geändert werden. Der Alias (-Name) wurde eingeführt, weil bei einem Benutzerdatenimport die Benutzer-Id nur ein Zahlenstring ist und man einen individuellen Benutzernamen nach einem erfolgreichen Import unterstützen möchte. Ein Benutzer kann sich dann auch mit seinem Alias authentifizieren.
Passwort (nur bei Authentifizierung durch CTI-Kennung)	Hier wird das individuelle Passwort festgelegt, das **nicht** zwingend bei der ersten Authentifizierung geändert werden muss. Bei der Eingabe werden aus Sicherheitsgründen nur Sterne angezeigt. Wird kein Passwort eingegeben, so wird für diesen Benutzer das Standard-Passwort eingetragen. Der Benutzer wird dann beim ersten Anmelden aufgefordert, sein Passwort zu ändern. Das Standard-Passwort legen Sie über **Benutzer** | **Einstellungen | Standardpasswort** fest. Weitere Informationen dazu finden Sie in Abschnitt 7.3.3.
Passwort wiederholen (nur bei Authentifizierung durch CTI-Kennung)	Geben Sie zur Bestätigung / Verifikation das Passwort erneut ein; auch hier werden bei der Eingabe aus Sicherheitsgründen nur Sterne angezeigt.

Feld	Beschreibung
Benutzername (nur bei Authentifizierung durch System-Kennung)	Geben Sie hier der Windows-Benutzernamen ein, der in einer Domäne oder der lokalen Benutzerverwaltung existiert. Bei einer CAP-Authentifizierung muss ein CTI-Benutzer seine Benutzer-Id oder seine Device-Id und das Passwort des zugeordneten Windows-Benutzers eingeben.
Domain (nur bei Authentifizierung durch System-Kennung)	Geben Sie hier die Domäne an, in der der zugeordnete Windows-Benutzer eingerichtet ist. Das kann neben einer echten Domänenkennung auch die lokale Benutzerverwaltung sein. In diesem Fall muss der lokale PC-Name eingegeben werden. Die Authentifizierung über das Betriebssystem hat den Vorteil, dass der CAP-Benutzer und der Domänen-Benutzer dasselbe Passwort verwenden (das Domain-Benutzer-Passwort). Diese Passwort wird nur noch in der Domäne verwaltet.
Devices	Selektieren Sie aus der Liste der bereits eingerichteten Phone-Devices die Devices, die diesem Benutzer zugeordnet werden sollen. Bitte beachten Sie, dass es möglich ist, einem Benutzer mehrere Devices zuzuordnen. Die Schaltfläche **Devices zuordnen** öffnet ein separates Dialogfenster zur Auswahl / Definition von Devices. Mit **Schließen** kommen Sie wieder zurück in den Dialog **Benutzer hinzufügen**. Bereits zugeordnete Devices werden im Feld Devices angezeigt; über Selektion und **Device bearbeiten** können sie einzeln geändert werden. Für Anwendungen, die eine 1-1-Zuordnung von Benutzer und Device voraussetzen (wie ComAssistant), ist es möglich, ein Device als **Haupt-Device** zu identifizieren; die Applikation kann dann die übrigen zugeordneten Devices ignorieren. Das erste einem Benutzer zugeordnete Device wird als Haupt-Device angenommen; Sie können diese Zuordnung jederzeit über **Haupt-Device setzen** verändern. Das aktuell gesetzte Haupt-Device wird in Blau angezeigt.

Feld	Beschreibung
Business Gruppe (für BGAdmin fest eingestellt)	Die Default-Auswahl ist "Standard" bzw. "none". Zusätzliche BGs werden zur Auswahl angeboten sobald BGs eingerichtet wurden. Die Zuordnung des Benutzers zu einer BG erfolgt zweckmäßig auf Basis aus der TK-Anlage importierter Daten beim Einrichten des Benutzers; sie kann später nicht mehr verändert werden (kein BG-Wechsel).
Benutzergruppe	Um den Benutzer einer Benutzergruppe zuzuordnen, wählen Sie hier eine Benutzergruppe aus. Anwendungsbeispiele: ComAssistant zeigt anhand der Benutzergruppen die Buddy-Liste eines Benutzer an. Der CAP TCSP ist in der Lage, die einer spezifischen Benutzergruppe zugeordneten Benutzer/Devices automatisch als TAPI-Lines aufzunehmen. **Hinweise:** ? Um eine Benutzergruppe auswählen zu können, muss diese vorher unter **Benutzer | Benutzergruppen** eingerichtet sein.
Zeitzone	Wählen Sie aus dem Pull-Down-Menü die dem Benutzer zuzuordnende Zeitzone aus.

3. Klicken Sie auf die Schaltfläche Hinzufügen. Es wird ein neuer Benutzerdatensatz angelegt und es erscheint folgende Meldung:

   ```
   Der Benutzer wurde eingetragen: <Benutzer-Id> (z.B. 495251827486)
   ```

   Existiert bereits ein Benutzer mit gleicher Id, wird folgende Fehlermeldung ausgegeben:

   ```
   Der Benutzer existiert bereits: <Benutzer-Id> (z.B. 495251827486)
   ```

7.3.2 Benutzereinträge suchen und ändern

1. Klicken Sie auf **Benutzer** im Hauptmenü und wählen Sie den Menüpunkt **Suchen/Ändern** im Navigationsbereich aus. Es öffnet sich ein Fenster zur genaueren Spezifikation der Suchanfrage:

2. Geben Sie in einem der Felder Ihren Suchbegriff ein. Die Felder sind in der nachstehenden Tabelle beschrieben.

   Dialog Benutzer suchen

Feld	Beschreibung
Benutzer-Id, **Anzeigename**, **Alias**, **Gruppe**, **Lizenz**, **SCC ID**, **Telefonnummer,** **Rolle des Benutzers,** **Business Gruppe**	Diese Eingabefelder können zur genaueren Eingrenzung der gesuchten Benutzerdaten verwendet werden. In jedem dieser Felder kann der Stern als Platzhalter-Symbol genutzt werden: ***** findet alle Einträge, C***** alle mit C beginnenden Einträge, *****n alle auf n endenden Einträge etc. Die unter “Gruppe”, “Lizenz”, “SCC Id”, “Rolle des Benutzers” und “Business Gruppe” zur Verfügung stehenden Auswahlmenüs zeigen immer nur das an, was auch in der CAP eingerichtet wurde.
Maximale Trefferanzahl	Begrenzt die Zahl der als Suchergebnis dargestellten Einträge. Damit lässt sich die Suche vor endgültiger Darstellung des Ergebnisses entsprechend eingrenzen.
Anzahl Treffer pro Seite	Die Darstellung des Suchergebnisses kann auf mehrere Seiten aufgeteilt werden.
Suchergebnis zum Löschen markieren	Wie unten beschrieben, können in der Ergebnisanzeige einzelne Einträge explizit zum Löschen markiert werden. Wenn die Suche mit dem Ziel erfolgt, alle gefundenen Einträge zu löschen, kann hier eingestellt werden, dass für alle Einträge schon vorab die Löschmarkierung gesetzt wird.
Suchergebnis zum Exportieren markieren	Wie unten beschrieben, können in der Ergebnisanzeige einzelne Einträge explizit zum Export markiert werden. Wenn die Suche mit dem Ziel erfolgt, alle gefundenen Einträge zu exportieren, kann hier eingestellt werden, dass für alle Einträge schon vorab die Exportmarkierung gesetzt wird.

Aktionen

Feld	Beschreibung
Felder löschen	Feldinhalte werden gelöscht (mit Ausnahme der Felder Rolle des Benutzers und Business Gruppe - dort werden die Standard-Einträge "CTI Benutzer" und "Standard Business Gruppe" beibehalten), und die Felder **Maximale Trefferanzahl** und **Anzahl Treffer pro Seite** werden aus der Konfigurationsdatei `adminIF.cfg` neu belegt.
Suchen	Suchanfrage anstoßen

Feld	Beschreibung
Letzte Suche	Alle Felder werden mit den bei der letzten Suchanfrage genutzen Werten belegt. Nach Abschluss einer Browser-Sitzung liefert “Letzte Suche” keine Daten mehr. **Hinweis:** Das Ergebnis der letzten Suche erhalten Sie auch direkt, indem Sie den Menüpunkt **Letztes Suchergebnis** in der Navigationsleiste auswählen.

3. Klicken Sie auf die Schaltfläche **Suchen**. Das Ergebnis der Suchanfrage wird (falls mehr als ein Treffer) in einer Liste dargestellt.

   Verwenden Sie die Pfeiltasten, um durch mehrere Seiten zu navigieren (erste - vorige - nächste - letzte Seite).

   Mit dem Drucker-Symbol können Sie eine Druck-Vorschau der Ergebnisliste in einem separaten Fenster anzeigen lassen.

   Die Spalte "Löschen" bietet die Möglichkeit, einzelne Zeilen durch Haken zum Löschen zu markieren; durch Klick auf das Lösch-Symbol / Kreuz in der Kopfzeile werden alle markierten Einträge endgültig gelöscht.

   Die Spalte "Export" bietet die Möglichkeit, einzelne Zeilen durch Haken zum Exportieren zu markieren; durch Klick auf das Export-Symbol / FD Icon in der Kopfzeile werden alle markierten Einträge im Excel csv (comma separated value) Format in einer Datei abgespeichert.

4. Wählen Sie mit dem Symbol  einen Benutzer aus der Liste aus, um seine Daten zu ändern.

5. Die aktuellen Daten des ausgewählten Benutzers werden zur Änderung angezeigt.

6. Ändern Sie die Benutzerdaten wie in Abschnitt 7.3.1 beschrieben.

> 7 Die Benutzer-Id kann nicht geändert werden, da sie als eindeutige ID für den Benutzer gilt.
> Die Information bezüglich Lizenzen (diese sind den Devices zugeordnet) wird in der Benutzer-Maske lediglich angezeigt; sie kann hier ebenfalls nicht geändert werden. Bitte beachten Sie: da ein Benutzer mehrere Devices zugeordnet haben kann, die die gleiche Lizenz besitzen, kann ein Benutzer indirekt eventuell mehrere Lizenzen des gleichen Typs "verbrauchen" (z.B. drei CAP-S).

Im Aufklappmenü **Password** stehen Ihnen verschiedene Optionen zur Änderung des Passworts zur Verfügung. Sie können das Passwort ändern, beibehalten oder auf das Standardpasswort zurücksetzen.

> Das Standardpasswort legen Sie in **Benutzer | Business-Gruppen | Standard-passwort** fest.
> Informationen dazu finden Sie in Abschnitt 7.3.3.

7. Bestätigen Sie Ihre Eingaben mit der Schaltfläche **Ändern**. Die Durchführung der Änderungen wird Ihnen mit folgender Meldung bestätigt:

   `Die Benutzerdaten wurden geändert für: <Benutzer-Id>` (z.B. `hm007`)

   Über die Schaltfläche **Schließen** verlassen Sie den Dialog, ohne dass die Änderungen durchgeführt werden.

7.3.3 Konfiguration von Business-Gruppen

1. Klicken Sie auf **Benutzer** im Hauptmenü und wählen Sie den Menüpunkt **Business-Gruppen** im Navigationsbereich aus. Es wird eine Liste bereits eingerichteter Business-Gruppen angezeigt, die ausgewählt / modifiziert werden können. Der BGAdmin sieht nur die ihm zugeordneten BGs.
2. Zum Einrichten einer neuen Business-Gruppe (nicht für BGAdmin)

   klicken Sie auf die Schaltfläche  in der Kopfzeile.

   Es erscheint das Fenster für die Eingabe einer neuen BG.
3. Geben Sie die gewünschten Daten in die Eingabefelder ein.

   Dialog Konfiguration von Business-Gruppen

Feld	Beschreibung
Business Gruppe ID, Name (für BGAdmin fest eingestellt)	Die Default-Auswahl ist "Standard" bzw. "none". Zusätzliche BGs werden zur Auswahl angeboten, sobald BGs eingerichtet wurden.
Standardpasswort	Legen Sie das Standardpasswort fest. Dieses Passwort gilt, wenn Sie beim Anlegen eines neuen Benutzereintrags kein Passwort angeben oder wenn Sie beim Ändern von Benutzereinträgen das Passwort über **Rücksetzen** zurücksetzen (siehe Abschnitt 7.3.2). Wird bei Neueinträgen oder Änderungen von Benutzerdaten das Standardpasswort verwendet, wird der Benutzer beim ersten Anmelden aufgefordert sein Passwort zu ändern. Das Default-Standardpasswort ist “**`123456`**”.

Feld	Beschreibung
Gültigkeitsdauer des Passworts (in Tagen)	Geben Sie die Gültigkeitsdauer für das Passwort in Tagen an. Nach Ablauf dieses Zeitraums wird der Benutzer automatisch aufgefordert, sein Passwort zu ändern oder zu bestätigen.
Authentifizierungsmodus	Stellen Sie über das Aufklappmenü die Art der Authentifizierung ein: ? **Alle Kennungen**: Bei der Einrichtung eines CTI- oder Admin-Benutzers stehen immer beide Möglichkeiten der Authentifizierung für jeden einzelnen Benutzer selektiv zur Verfügung. ? **CTI-Kennung:** Die Authentifizierung wird vollständig von OpenScape CAP Management abgewickelt. Eine Authentifizierung wird durch die "Benutzer-Id", den "Alias" oder die "Device-Id" und das zugehörige Passwort im CAP Management durchgeführt. ? **System-Kennung:** Für eine Authentifizierung muss ein CAP-Benutzer immer mit einem Windows-Benutzer verknüpft sein. Eine Authentifizierung wird durch die "Benutzer-Id" oder die "Device-Id" und das Passwort des zugeordneten Windows-Benutzers durchgeführt.
Voice Box Phone (nur HQ8000)	derzeit nicht relevant.

4. Klicken Sie zur Bestätigung der Änderungen auf die Schaltfläche **Ändern**.

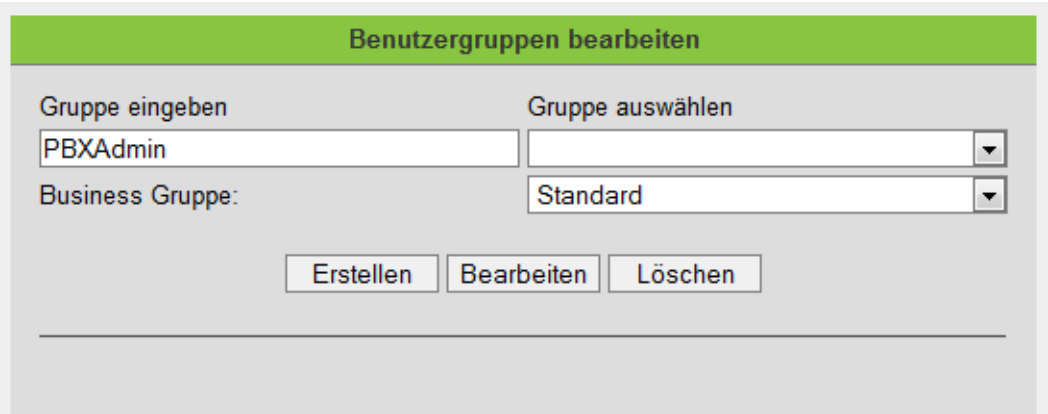
Im wesentlichen den gleichen Ablauf nutzen Sie, um die Daten einer vorhandenen BG (soweit zulässig) zu ändern oder eine BG zu löschen.

> Löschen einer BG ist für BGAdmin nicht verfügbar; es ist nur zulässig, wenn in der zu löschenden BG keinerlei Objekte (Benutzer, Devices) eingerichtet sind. Falls die BG nicht "leer" ist, erfolgt ein entsprechender Warnhinweis an den Administrator.

7.3.4 Benutzergruppen

Hier können Sie Benutzergruppen definieren und bestehende Benutzergruppen ändern. Benutzergruppen werden derzeit vom ComAssistant zur Anzeige der Buddy-Liste und vom CAP TCSP zur automatischen Übernahme einer definierten Benutzergruppe als TAPI Line-Device verwendet.

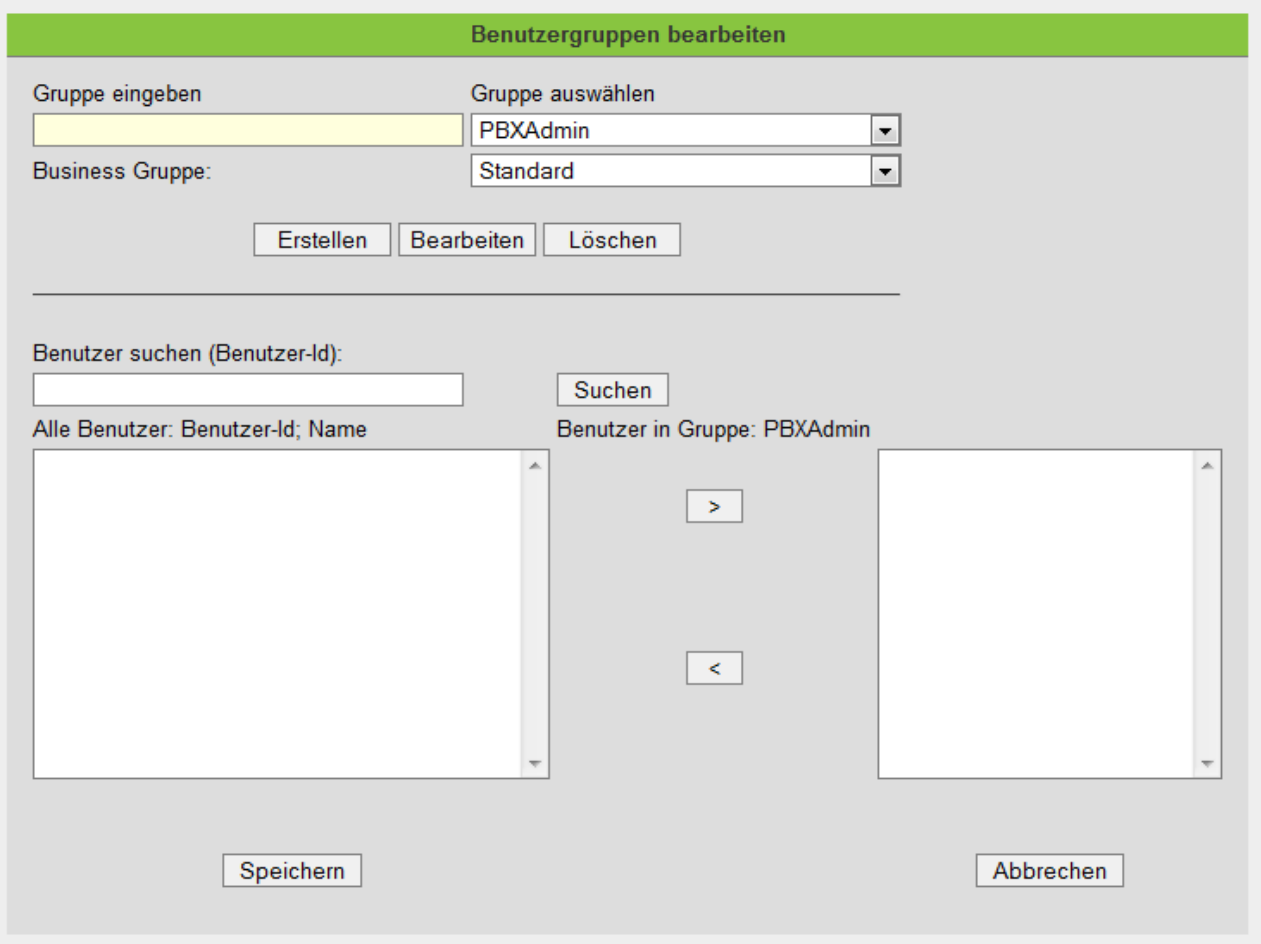
1. Klicken Sie auf **Benutzer** im Hauptmenü und wählen Sie den Menüpunkt **Benutzergruppen** im Navigationsbereich aus. Es erscheint das folgende Fenster.



   Der Sichtbarkeitsbereich kann durch Angabe einer spezifischen Business-Gruppe eingeschränkt werden; für BGAdmin ist diese Auswahl voreingestellt.

2. Zur Definition einer neuen Gruppe geben Sie unter **Gruppe eingeben** den Namen der zu erstellenden Gruppe ein und drücken Sie **Erstellen**.
   Zum Ändern oder Löschen einer vorhandenen Gruppe wählen Sie die gewünschte Gruppe unter **Gruppe auswählen** und drücken Sie **Bearbeiten** oder **Löschen**.
   Beim Löschen einer Gruppe werden auch bei allen Benutzern, die zu dieser Gruppe gehören, die Verweise auf diese Gruppe entfernt.

3. Zum Erstellen oder Ändern einer Gruppe erscheint ein neues Fenster.



Das rechte Auswahlfenster zeigt die aktuell der Gruppe zugeordneten Benutzer, das linke Auswahlfenster alle übrigen Benutzer an. Sie können Benutzereinträge zwischen den Fenstern verschieben, entweder durch Doppelklick auf einzelne Einträge oder (nach Auswahl von Benutzereinträgen) über die Pfeiltasten. Mehrfachselektion von Einträgen ist möglich.

4. Sobald die Definition / Änderung der Gruppenzusammensetzung abgeschlossen ist, können Sie über **Speichern** die Definition abschließen. Über **Abbrechen** gelangen Sie ohne Änderung zurück in die Darstellung aus Schritt 2.

7.3.5 Integration mit HiPath User Management (nicht für BGAdmin)

Mit der vorliegenden Version der OpenScape CAP V3.0 besteht die Möglichkeit der Integration von CAP und HiPath User Management zum weitgehend automatischen Abgleich von User-Daten.

Bitte beachten Sie, dass im HiPath User Management ausschließlich User-Daten zu HiPath / OpenScape 4000-Systemen verwaltet werden. User, die anderen Switches zugeordnet sind, müssen weiter über CAP Management administriert werden!

7.3.5.1 Anbindung von CAP an HiPath User Management

Die Unterstützung für HiPath User Management wird durch folgenden Eintrag in `<InstDir>/config/<host>/admin/mgmnt/admin.cfg` aktiviert:

```
ProgramMode = HiPathUserManager
```

Durch diesen Eintrag wird folgende gleichlautende Konfigurationsdatei aktiviert:

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

In dieser Datei kann das Verhalten der Dialoge für Benutzer und Device konfiguriert werden. Standardmäßig sind schon sinnvolle Voreinstellungen gewählt, z.B. sind alle Eingabefelder des Benutzerdialogs gesperrt, das Passwort und die Lizenzvergabe können jedoch geändert werden. Weiteres ist dieser Datei zu entnehmen. Wird der ProgramMode auf der Standardeinstellung "CAP" belassen, so ist ebenfalls eine Anbindung an HiPath User Management möglich, es gibt jedoch keinerlei Einschränkungen in den Dialogen für Benutzer und Device.

Damit die Anbindung von CAP an HiPath User Management funktioniert, müssen folgende Konfigurationsdateien nach der CAP-Installation überprüft werden:

`<InstDir>/config/<host>/admin/semi/config/LocalConfigHiPathCAP.xml` sollte folgenden Inhalt haben und braucht nicht verändert werden:

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

`<InstDir>/config/<host>/admin/semi/config/SdkConfig4448.xml` entsteht bei aktiver Verbindung von CAP zu HiPath User Management automatisch und muss nicht angepasst werden:

```
<HPM ver="2.0">
   <ENVIRONMENT>
      <HPM-UM_SERVER_IP>192.168.111.228</HPM-UM_SERVER_IP>
      <HPM-UM_SERVER_PORT>4443</HPM-UM_SERVER_PORT>
```

```
      <HPM-DS_SERVER_IP>192.168.111.228</HPM-DS_SERVER_IP>
      <HPM-DS_SERVER_PORT>2600</HPM-DS_SERVER_PORT>
      <EM_ID>192.168.111.129-4448</EM_ID>
   </ENVIRONMENT>
</HPM>
```

`<InstDir>/config/<host>/admin/semi/config/traceconfig.xml`
sollte folgenden Inhalt haben und braucht nicht verändert werden. Hier wird vor allem das Trace-Verzeichnis (<TRACE_PATH>) eingestellt. Für Tests kann auch der Trace-Level (XML,DEBUG,INFO,WARN,ERROR,FATAL) bei der Einstellung "<TRACER_LEVEL>" verändert werden. Diese Datei beeinflusst das Traceverhalten des HiPath User Management Interfaces.

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

   </DETAILS>
</HPM>
```

7.3.5.2 Vorgehensweise für den Administrator

Sollen beide Management-Systeme (CAP und HiPath User Management) zusammen betrieben werden, so wird folgende Vorgehensweise empfohlen. Dabei sind vier Fälle zu unterscheiden:

- Fall 1: In keinem der beiden Systeme sind Benutzer eingerichtet
- Fall 2: Benutzer sind in CAP eingerichtet, in HiPath User Management nicht

- Fall 3: Benutzer sind in HiPath User Management eingerichtet, in CAP nicht
- Fall 4: In beiden Systemen sind bereits Benutzer eingerichtet

Für alle Fälle gilt:

- In CAP müssen die notwendigen SCC-Konfigurationen für die entsprechenden PBX-Anlagen eingerichtet werden. Dabei ist darauf zu achten, dass die Namen der konfigurierten SCC-Instanzen mit den Namen der PBX-Anlagen, die in HiPath User Management verwendet werden, übereinstimmen.
- Einrichten des Element Manager für CAP in HiPath User Management. Dabei ist darauf zu achten, dass die Porteinstellung mit dem Eintrag in der Datei `LocalConfigHiPathCAP.xml` übereinstimmt. Standardeinstellung ist 4448.

Fall 1: In keinem der beiden Systeme sind Benutzer eingerichtet

- Die Benutzer sollten in HiPath User Management mit ihren Telefon-Ressourcen eingerichtet werden; dies setzt natürlich auch die Einbindung der HiPath / OpenScape 4000 voraus.
- Hochladen der CAP Daten nach HiPath User Management. Dadurch werden CAP-spezifische Eigenschaften dem HiPath User Management bekannt gemacht, z.B. welche Lizenzen in CAP installiert sind bzw. auf welche Nachrichten von HiPath User Management in CAP reagiert wird.
- "Benutzerdaten hinunterladen" in HiPath User Management ausführen. Dabei ist die dritte Option ("Alle Benutzerdaten hinunterladen") zu wählen.
- War das Hinunterladen erfolgreich, so wurden alle Benutzer mit ihren Telefonnummern in CAP angelegt.
- Ab jetzt werden die Benutzerdaten soweit möglich automatisch synchronisiert, z.B. wenn einem Benutzer in CAP durch eine Benutzeranmeldung über ComAssistant eine Lizenz zugewiesen wird, wird diese Lizenzbelegung dem HiPath User Management gemeldet. Dies funktioniert auch umgekehrt. Andere Benutzerattribute, in HiPath User Management CAP Attribute genannt (findet man in "HiPathApplikationen"), sollen immer nur in HiPath User Management geändert werden, da diese nur vom HiPath User Management nach CAP automatisch synchronisiert werden. Lizenzen werden jedoch in beide Richtungen automatisch synchronisiert.
- Die Benutzerdaten können auch manuell synchronisiert werden (siehe unten).

Fall 2: Benutzer sind in CAP eingerichtet, in HiPath User Management nicht

- Menüpunkt "Extras/Element Manager Sync" in HiPath User Management auswählen
- Benutzerdaten hochladen - Taste "Daten hochladen".
- Benutzer in HiPath User Management einpflegen (Taste: "Benutzerdaten einpflegen")

- Telefon-Ressourcen den Benutzern in HiPath User Management zuweisen
- "Benutzerdaten hinunterladen" in HiPath User Management ausführen. Dabei ist die zweite Option ("Telefonnummern synchronisieren") zu wählen.
- Nochmals Benutzerdaten hochladen. Dadurch werden jetzt auch die Lizenzbelegungen mitgeteilt.
- Benutzer in HiPath User Management einpflegen.
- Ab jetzt werden die Benutzerdaten soweit möglich automatisch synchronisiert.

Fall 3: Benutzer sind in HiPath User Management eingerichtet, in CAP nicht

- Dieser Fall ist wie Fall 1 zu behandeln, nur dass die Benutzer schon Telefon-Ressourcen besitzen.

Fall 4: In beiden Systemen sind bereits Benutzer eingerichtet

- Benutzerdaten hinunterladen in HiPath User Management ausführen. Dabei ist die dritte Option (Alle Benutzerdaten hinunterladen) zu wählen.
- Benutzerdaten hochladen (in HiPath User Management auslösen).
- Benutzer in HiPath User Management einpflegen
- Ab jetzt werden die Benutzerdaten soweit möglich automatisch synchronisiert.

7	Wie oben beschrieben (vgl. Abschnitt 7.3.1, “Benutzer hinzufügen”), dürfen Benutzern, die einer Benutzergruppe angehören, nicht mehr als ein Device zugeordnet werden; dies wird derzeit in der Konfigurationsoberfläche des CAP Management weitestgehend sichergestellt, kann aber beim Datenabgleich zwischen CAP und HiPath User Management nicht gewährleistet werden. Deshalb muss der Administrator überprüfen, dass diese Einschränkung im HiPath User Management erfüllt ist, bevor er den Datenabgleich anstößt.

7.4 Device

In der CAP werden Devices unterschiedlichen Typs verwaltet:

- Nebenstellen (Typ “Phone”)
- virtuelle Nebenstellen (Typ “Virtual Device”)
- Leitungsbündel (Typ “Trunk”)
- Sammelanschlüsse (Typ “HuntGroup”)
- Route-Control-Gruppen (Typ “RCG”)
- SIP-Endgeräte (Typ “SIP”)
- MGCP-Endgeräte (Typ “MGCP”)
- Fax-Geräte (Typ “FaxNumber”)
- Mail-Adressen (Typ “MailAddress”)
- Routing Devices (Typ “RoutingDevice”)

Devices, Benutzer und Lizenzierung

Sogenannte **Station Devices** (Nebenstellen, virtuelle Nebenstellen, SIP- bzw. MGCP-Endgeräte etc.) sind jeweils einem CAP-Benutzer zugeordnet. Bitte beachten Sie, dass nur Devices der Typen “Phone” und “Virtual Device” über die Administrations-Oberfläche eingerichtet werden können. Andere Telefontypen können nur durch ein Import der Gerät-typen über SPI möglich. Von SMR9 an ist es möglich den device-typ SIP-device an SIP-Telefonen zuzuordnen, so können sie von anderen Telefontypen unterscheidet werden.

Non-Station Devices (Leitungsbündel, Sammelanschlüsse, Route Control Gruppen, Routing Device), auch als "logische Devices" bezeichnet, haben keinen zugeordneten CAP-Benutzer. Sie werden ausschließlich über Import (vgl. Abschnitt 7.6.1) oder bei der HiPath / OpenScape 4000 über die SPI-Schnittstelle (vgl. Abschnitt 6.2.3) eingerichtet.

Devices werden anhand ihrer Device-ID eindeutig einem SCC und damit jeweils einer TK-Anlage zugeordnet. Die Device-ID ist entweder ein wählbare Langrufnummer im kanonischen Format (z.B. +49(5251)8-27486) oder für Leitungsbündel eine eindeutige Verwaltungsnummer im CAP Management, die sich aus der SCC-ID und der Position des entsprechenden Modul/ Kanals zusammensetzt (z.B. +SCC-H4K-1+1-67-1+0 = +<SCC-ID>+<Lage>+Kanal).

Lizenzen der unterschiedlichen Typen werden einheitlich den Devices zugeordnet. Die Lizenz-Zuordnung kann wahlweise "implizit bei Lizenzüberprüfung" oder "bei Device-Einrichtung" (vgl. Abschnitt 7.5.3) erfolgen. Da aber Devices aller Typen außer "Phone" und "Virtual Device" nicht über die CAP-Management-Oberfläche bearbeitet werden können, können die Lizenzen für diese nur implizit zugeordnet werden; achten Sie deshalb darauf, dass für die entsprechen-

den Lizenzen die Zuordnung “implizit bei Lizenzüberprüfung” eingestellt ist (vgl. Abschnitt 7.5.3). Damit findet die Lizenzvergabe automatisch statt, sobald das Device benutzt wird.

Alle Lizenzen (egal, ob implizit oder explizit zugeordnet) sind im Device-Dialog sichtbar und können bei der Device-Suche abgefragt werden (vgl. Abschnitt 7.4.2).

Für eine Lizenzbestellung ist es also wichtig, dass nicht nur die Anzahl der Telefone (Station Devices), sondern auch die Anzahl logischer Devices (Non-Station Devices) berücksicht wird, die über die CTI-Schnittstellen der CAP angesprochen werden sollen.

Devices und Applikationen

Eine Applikation ist durch Leistungen des “Address Translation Service” (SAT) in der Lage zur Adressierung eines Devices immer die zugehörige Rufnummer im kanonischen Format zu verwenden. Die Umsetzung in eine für den SCC adressierbare Nummer erfolgt entsprechend der Anzeige im Feld “PBX-Format” eines Devices. Eine eventuell vorhandene Overlap-Konfiguration wird dabei berücksichtigt. Für “Route Control Gruppen”, “Sammelanschlüsse” und “Leitungsbündel” der HiPath / OpenScape 4000 wird in diesem Feld die zugehörige LODEN-Nummer angezeigt.

In Events bekommt eine Applikation ebenfalls immer die Langrufnummer im kanonischen Format übermittelt. Um diese Funktion zu gewährleisten, werden entsprechend der einem Device zugehörigen SCC-Konfiguration die PNP-Nummer und die Querkennzahl in der Device-Konfiguration verwaltet. Beinhaltet ein Event eine der Konfiguration entsprechenden Rufnummer (z.B.: Nebenstellennummer, PNP-Nummer, Querkennzahl+Nebenstellennummer, ISDN-Nummer), so wird vor der Weiterleitung durch den SAT eine Konvertierung in die Device-ID vorgenommen.

Zusammenfassend - damit eine Applikation logische Devices steuern kann, ist erforderlich

1. die Daten zu den logischen Devices über Import / SPI im CAP Management einzurichten;
2. für die betreffenden SCC / SCCP Services die Nutzung des SAT zu aktivieren (vgl. Abschnitt A.2.15);
3. Lizenzen verfügbar zu haben und auf implizite Zuordnung einzustellen.

Beschränkung: Falls ein Applikation nicht das kanonische Format in dem CSTA Request verwendet (nur das Nebenstelle/PBX Format), dann das Nebenstelle/PBX Format muss in CAP Management datenbank einzigartig sein.

Im Hauptmenü **Device** können Sie die Endgeräte (“Nebenstellen” - Typ Phone, “virtuelle Nebenstellen” - Typ Virtual Device) hinzufügen und einrichten. Folgende Funktionen stehen Ihnen zur Verfügung:

- Device hinzufügen,
- Device suchen,
- Device ändern.

7.4.1 Device hinzufügen

1. Klicken Sie auf **Device** im Hauptmenü und wählen Sie den Menüpunkt **Hinzufügen** im Navigationsbereich aus.
2. Geben Sie in die Felder die Daten für das neue Endgerät ein. Die Felder sind in der nachstehenden Tabelle beschrieben.

Dialog Device hinzufügen

Feld	Beschreibung
SCC ID	Wählen Sie hier die benutzte Switch-Verbindung aus. Anhand dieser Selektion wird eine Nebenstelle oder virtuelle Nebenstelle fest einer TK-Anlage zugeordnet. Weiterhin werden entsprechend der zugehörigen SCC-Konfiguration die ISDN-Nummer(n), PNP-Nummer(n) und Querkennzahl(en) angezeigt.

Feld	Beschreibung
Emergency (nur HiPath / OpenScape 4000)	Wählen Sie hier die im AP Emergency Fall ersatzweise zu benutzende Verbindung aus. Dadurch kann das Device auch bei einem Ausfall der unter SCC ID angegebenen primären SCC4000/CA4000 Verbindung noch angesprochen werden. **ACHTUNG** Dies gilt nur für ein AP Emergency fähiges Device: ? per HiPath / OpenScape 4000 Administration ist das Device an einem AP-Shelf konfiguriert, ? per HiPath / OpenScape 4000 Administration ist das Device einer AP-EmergencyGroup zugeordnet ? per HiPath / OpenScape 4000 Administration ist die AP-EmergencyGroup mit einem CC-AP ("Common Control for Access Point Emergency" - notwendige HW Komponente in einem AP-Shelf, die für die lokale Survivability sorgt) assoziiert ? per CAP Administration ist ein eigener SCC4000/ CA4000 zu diesem CC-AP konfiguriert **ACHTUNG** Ist im übergeordneten SCCP das AP Emergency Feature auf CAP-Ebene ausgeschaltet ("AP Emergency deaktivieren", vgl. Abschnitt 6.5.2), so werden von diesem SCCP etwaige Ersatz-Verbindungen nicht genutzt! Obwohl das Device auf HiPath / OpenScape 4000 Ebene manuell genutzt werden kann, ist es für die Applikation solange nicht erreichbar, bis die unter "SCC ID" angegebene primäre SCC4000/CA4000 Verbindung wieder steht.
Business Gruppe (für BGAdmin fest eingestellt)	Die Default-Auswahl ist "Standard" bzw. "none". Zusätzliche BGs werden zur Auswahl angeboten sobald BGs eingerichtet wurden. Die Zuordnung des Devices zu einer BG erfolgt zweckmäßig auf Basis aus der TK-Anlage importierter Daten beim Einrichten des Devices; sie kann später nicht mehr verändert werden (kein BG-Wechsel).
Device Typ	Wählen Sie hier den Typ des Endgerätes aus. Die unterstützten Typen sind "Phone" und "VirtualDevice". Devices aller weiteren Device-Typen können nur importiert werden.
ISDN Nummer	Pull-Down-Menü mit eingerichteten Domain-Informationen (vgl. Abschnitt 7.2.3); Wählen Sie den für dieses Device relevanten Eintrag.

Feld	Beschreibung
PNP Nummer	Pull-Down-Menü mit eingerichteten Privaten Numerierungsplänen / PNPs (vgl. Abschnitt 7.2.5); wählen Sie den für dieses Device relevanten Eintrag.
Querzahl	Pull-Down-Menü mit eingerichteten Querkennzahlen / NACs (vgl. Abschnitt 7.2.4); Wählen Sie den für dieses Device relevanten Eintrag.
Extension	Nummer der Nebenstelle, d.h. des Devices. Normalerweise ist diese Nummer genauso in der PBX konfiguriert. **Ausnahme:** Falls Overlap eingestellt wurde, muss die Extension-Nummer ohne die Overlap-Nummer eingetragen werden. Diese Extension-Nummer ist folglich nur ein Fragment der in der PBX konfigurierten Nummer (z.B. Hauptanschluss/Extension = 722-1234, Overlap=1: in der PBX ist die Nebenstelle 21234 konfiguriert).
PBX-Format (nur Ausgabe-Feld nach “Device suchen”)	Dieses Feld ist nicht administrierbar! Hier wird für alle Devices, die in CSTA über eine wählbare Nummer adressiert werden, die in der PBX konfigurierte Rufnummer angezeigt. Eine eventuell vorhandene Overlap-Konfiguration wird dabei berücksichtigt (z.B. Hauptanschluss/Extension = 722-1234, Overlap=1: in dem Feld PBX-Format erscheint die Nebenstelle 21234). Bei HiPath / OpenScape 4000 Devices, die in CSTA über eine CSTA-Device-Id (RCG, Trunk, Huntgroup) adressiert werden, erscheint die zugehörige LODEN-Nummer. Diese Daten werden vom SAT zur Konvertierung benötigt.
XML Phone Service (nur für Typ “Phone”)	Wählen Sie einen XML Phone Service aus der Aufklappliste aus, den Sie für das Endgerät aktivieren möchten. Anschließend ist die Schaltfläche **XML Phone-Einstellungen** aktiv (siehe unten).

Feld	Beschreibung
XML Phone-Einstellungen (nur für Typ “Phone”)	Wenn Sie auf die Schaltfläche **XML Phone-Einstellungen** klicken, erhalten Sie folgende Einstellmöglichkeiten: ? **Geräteinformation** Auswahl aus einer Liste unterstützter Geräte-Typen ? **Sprache** Auswahl aus einer Liste unterstützter Sprachen ? **Tastennummer** Nummer der Taste am Endgerät, die der URL der XML-Anwendung zugeordnet werden soll. Durch Drücken der Taste wird die XML-Anwendung gestartet und am Display des Endgeräts ausgegeben. ? **URL Parameter** Weitere Parameter können den Aufruf einer URL erweitern. Diese Konfiguration ist abhängig von der XML Applikation.
Lizenz erteilt für	Wenn bei Anwendungen die Zuordnung von Lizenzen durch den Administrator eingestellt wurde (siehe Abschnitt 7.5.3, **Benutzer | Lizenzen zuordnen,** Option **bei Device-Einrichtung** aktiviert), müssen hier die Lizenzen zur Nutzung der Anwendungen explizit vergeben werden. Wählen Sie die Anwendung in der Liste aus. Es können Lizenzen für mehrere Anwendungen gleichzeitig vergeben werden. Bereits vergebene Lizenzen können auch wieder gelöscht werden. Auch implizit zugeteilte Lizenzen werden hier angezeigt.
Zugeordneter Benutzer	Dies ist ein reines Ausgabe-Feld. Zuordnung von Benutzern und Devices erfolgt über "Benutzer hinzufügen" bzw. "Benutzer ändern" (vgl. Abschnitt 7.3.1, Abschnitt 7.3.2)

3. Klicken Sie auf die Schaltfläche **Hinzufügen**. Die Eingaben werden als neuer Device-Datensatz übernommen.

> Kein Gerät kann hinzugefügt werden, bis das Domain nicht existiert.

7.4.2 Device suchen und ändern

1. Klicken Sie auf **Device** im Hauptmenü und wählen Sie den Menüpunkt **Suchen/Ändern** im Navigationsbereich aus. Es öffnet sich ein Fenster zur genaueren Spezifikation der Suchanfrage.
2. Geben Sie in einem der Felder Ihren Suchbegriff ein. Die Felder sind in der nachstehenden Tabelle beschrieben.

Dialog Devices suchen

Feld	Beschreibung
Device, **Device Typ,** **SCC ID,** **SCC Emergency,** **XML Phone Service,** **Lizenz,** **Zugeordneter Benutzer,** **Business Gruppe**	Diese Eingabefelder können zur genaueren Eingrenzung der gesuchten Device-Daten verwendet werden. In jedem dieser Felder kann der Stern als Platzhalter-Symbol genutzt werden: ***** findet alle Einträge, C***** alle mit C beginnenden Einträge, *****n alle auf n endenden Einträge etc. Die unter “Device Typ”, "SCC ID", "SCC Emergency", "XML Phone Service", “Lizenz” und “Business Gruppe” zur Verfügung stehenden Auswahlmenüs zeigen immer nur das an, was auch in der CAP eingerichtet wurde. Von den Release SMR9 an können auch nur die SIP-Geräten in sich selbst ausgelistet werden.
Maximale Trefferanzahl	begrenzt die Zahl der als Suchergebnis dargestellten Einträge; damit läßt sich die Suche vor endgültiger Darstellung des Ergebnisses entsprechend eingrenzen.
Anzahl Treffer pro Seite	Über kann die Darstellung des Suchergebnisses auf mehrere Seiten aufgeteilt werden.
Suchergebnis zum Löschen markieren	Wie unten beschrieben, können in der Ergebnisanzeige einzelne Einträge explizit zum Löschen markiert werden. Wenn die Suche mit dem Ziel erfolgt, alle gefundenen Einträge zu löschen, kann hier eingestellt werden, dass für alle Einträge schon vorab die Löschmarkierung gesetzt wird.
Suchergebnis zum Exportieren markieren	Wie unten beschrieben, können in der Ergebnisanzeige einzelne Einträge explizit zum Export markiert werden. Wenn die Suche mit dem Ziel erfolgt, alle gefundenen Einträge zu exportieren, kann hier eingestellt werden, dass für alle Einträge schon vorab die Exportmarkierung gesetzt wird.

Aktionen

Feld	Beschreibung
Felder löschen	Mit Klick auf werden alle Feldinhalte gelöscht sowie Maximale Trefferanzahl und Anzahl Treffer pro Seite aus der Konfigurationsdatei `adminIF.cfg` neu belegt.
Suchen	Suchanfrage anstoßen
Letzte Suche	Mit Klick auf werden alle Felder mit den bei der letzten Suchanfrage genutzen Werten belegt. Nach Abschluss einer Browser-Sitzung liefert “Letzte Suche” keine Daten mehr. **Hinweis:** Das Ergebnis der letzten Suche erhalten Sie auch direkt, indem Sie den Menüpunkt **Letztes Suchergebnis** in der Navigationsleiste auswählen.

3. Klicken Sie auf **Suchen**. Das Ergebnis der Suchanfrage wird (falls mehr als ein Treffer) in einer Liste dargestellt.

   Verwenden Sie die Pfeiltasten, um durch mehrere Seiten zu navigieren (erste - vorige - nächste - letzte Seite).

   Mit dem Drucker-Symbol können Sie eine Druck-Vorschau der Ergebnisliste in einem separaten Fenster anzeigen lassen.

   Die Spalte "Löschen" bietet die Möglichkeit, einzelne Zeilen durch Haken zum Löschen zu markieren; durch Klick auf das Lösch-Symbol / Kreuz in der Kopfzeile werden alle markierten Einträge endgültig gelöscht.

   Die Spalte "Export" bietet die Möglichkeit, einzelne Zeilen durch Haken zum Exportieren zu markieren; durch Klick auf das Export-Symbol / FD Icon in der Kopfzeile werden alle markierten Einträge im Excel csv (comma separated value) Format in einer Datei abgespeichert.

4. Wählen Sie mit dem Symbol  ein Device aus der Liste aus, um seine Daten zu ändern.
5. Die aktuellen Daten des ausgewählten Devices werden zur Änderung angezeigt.
6. Ändern Sie die Endgeräte-Daten in dem Dialog wie in Abschnitt 7.4.1 beschrieben.
7. Bestätigen Sie Ihre Eingaben mit **Ändern**. Die Durchführung der Änderungen wird Ihnen mit folgender Meldung bestätigt:

   `Die Endgerätedaten wurden geändert für: <device>` (z.B. `optiPoint 410`)

7.5 Lizenzverwaltung

> ACHTUNG: Als wichtige Änderung gegenüber CAP V2.0 und früherer Versionen der CAP V3.0 werden Lizenzen nicht länger einem Benutzer sondern ausschließlich einem Device zugeordnet.Für die bislang üblichen Installationen mit 1-zu-1-Zuordnung von Benutzer und Device ergibt sich daraus inhaltlich für den Endanwender keine neue Lizenzbehandlung. Dieser konzeptionell sauberere Ansatz bringt aber einige Anpassungen in der CAP Management-Bedienoberfläche.
> Natürlich werden die vorher einem Benutzer zugeteilten Lizenzen beim Hochrüsten auf CAP V3.0 SMR3 entsprechend übertragen.

Das Lizenzmanagement der CAP verwaltet die Anzahl der zur Verfügung stehenden Client-Lizenzen einer Applikation. Eine Lizenz ist immer an eine MAC-Adresse einer aktiven NIC im CAP Management gebunden und wird bei jedem Neustart des Dienstes und jeder Lizenzinstallation überprüft.

Jede Applikation muss sich bei der CAP mit einer Applikations-ID identifizieren. Diese Applikations-ID wird im ACSE_AARQ übergeben. Alle weiteren Requests für Benutzer werden anhand dieser Applikations-ID lizenziert. Die Lizenzüberprüfung findet im Zusammenspiel zwischen SCCP/SCC und dem SLM statt. Applikationen ist es ebenfalls möglich, eine Lizenzüberprüfung per http-Request an das SLM anzufordern.

Unter dem Hauptmenü **Lizenzen** werden Ihnen die Funktionen zur Administration von Lizenzen für die Nutzung des OpenScape CTI-Systems angeboten:

- Lizenzen anzeigen,
- Lizenzen zuordnen,
- Lizenzen installieren,
- Lizenzen deinstallieren,
- Lizenzen aufteilen.

Die Lizenzüberprüfung wird durch den SCC/SCCP durchgeführt. Nach einer erfolgreichen Überprüfung speichert der SCC/SCCP diese Info für einen Zeitraum von 3600 s. Eine Lizenzüberprüfung findet für ein CAP-Device beim ersten CSTA- oder NetTSPI-Aufruf statt.
Ist das Leistungsmerkmal “Implizit bei Lizenzüberprüfung” aktiviert, so wird einem Device bei der Lizenzüberprüfung automatisch die Lizenz zugeteilt, die im ACSE_AARQ (für CSTA-Request) als Applikations-ID übergeben wurde. Natürlich muss diese entsprechende Lizenz bereits installiert worden sein!
Bei TAPI-Applikationen (CAP TAPI Service Provider / NetTSPI) wird durch eine interne Routine zunächst die Lizenz CAP-A, dann CAP-S, CAP-E abgefragt, wenn nicht innerhalb der ersten 10 sec nach einem TAPI “lineOpen” eine andere Applikations-ID durch ein TAPI “lineDevSpecificFeature” übergeben wird.

> Die HiPath CAP V1.0 Lizenz “UNKNOWN”, welche die Anzahl der zu setzenden Monitorpunkte eine CA4000 lizenziert hat, wird ab der HiPath CAP V2.0 nicht mehr benötigt. Ab der CA4000 Version 6.0.0.0 unterstützt diese keine eigene Verbindung zum CAP SLM und benötigt deshalb auch keine eigene Lizenz mehr!

Demolizenzen / Überschreiten von zugeteilten Lizenzen

Demolizenzen sind vorab installiert (MAC-Adresse FF-FF-FF-FF-FF-FF). Nach der ersten Vergabe einer Client-Lizenz ist der betreffende Demolizenz-Schlüssel noch 2 Monate gültig und wird mit einem “Verfallsdatum” gekennzeichnet. Wird dieser Zeitpunkt erreicht, können die Device mit Demolizenzen von der entsprechenden Applikation nicht mehr gesteuert werden.

Ebenso wird für reguläre Lizenz-Schlüssel verfahren, wenn keine Client-Lizenzen mehr zur Verfügung stehen. Dann bekommt das Device eine temporäre Lizenz mit einer Gültigkeit von 2 Monaten zugeteilt (Kennzeichen “*” in der Device-Verwaltung), und die entsprechender Lizenz wird mit einem “Verfallsdatum” gekennzeichnet. Wird dieser Zeitpunkt erreicht, können die Devices mit temporärer Lizenz von der entsprechenden Applikation nicht mehr gesteuert werden.

Um aus temporären wieder reguläre Lizenzen zu erstellen, müssen Sie entweder entsprechend der Applikations-Id weitere Client-Lizenzen installieren oder über folgende Schritte die vorhandenen Lizenzen neu verteilen:

- Bereits CTI-Benutzern zugeteilte Lizenzen löschen.
- CTI-Benutzer mit temporären Lizenzen suchen, einen nach dem anderen auswählen und explizit durch "**Ändern**" bestätigen.

> Bitte beachten Sie, dass in HiPath CAP V3.0 SMR4 Lizenzen Business-Gruppen-spezifisch verwaltet werden; dementsprechend kann das Kontingent einer BG erschöpft sein (und es greifen die Mechanismen bei Lizenzüberschreitung), obwohl bei Gesamtbetrachtung des Systems durchaus noch freie Lizenzen vorhanden sind. Der Administrator kann in diesem Fall evtl. die Aufteilung der Lizenzen auf die BGs anpassen.

Emailbenachrichtigung bei Lizenzüberschreitung

Überschreitet die Anzahl der zugeteilten Lizenzen die Anzahl der installierten Lizenzen, kann eine täglich sich wiederholende Emailbenachrichtigung eingerichtet werden. Dazu müssen in der Datei `<InstDir>\config\common\global.cfg` die folgenden Textzeilen geändert werden:

```
<?x set MAIL_SERVER = "Name des SMTP fähigen Emailservers"?>
<?x set MAIL_SENDER = "<?x $TelasWebName?> notification
                                          <Name des Emailsenders>"?>
<?x set MAIL_SYSADMIN = "Name des Emailempfängers"?>
```

7.5.1 Lizenzen installieren (nicht für BGAdmin)

Lizenzen werden über Lizenzdateien installiert. Diese Dateien erhalten Sie von der gleichen Stelle, die auch die OpenScape CAP-Software liefert. Für Unify-Kunden ist dies normalerweise die Fertigung. Auf Basis von Bestell- und Lieferdaten ist der Administrator in der Lage, über eine spezielle Web Site der Fertigung Lizenzen zur Herunterladen generieren zu lassen.

Zur Vermeidung von Missbrauch sind Lizenzschlüssel über die MAC-ID an den OpenScape CAP Management-PC gebunden. Deshalb muss diese MAC-ID zur Lizenzgenerierung mit übermittelt werden.

> Mit der OpenScape CAP-Installation werden Demo-Lizenzen zur Verfügung gestellt; diese sind nicht an eine bestimmte MAC-ID gebunden und nur für einen begrenzten Zeitraum gültig.

1. Beschaffen Sie die Lizenzdatei, und speichern Sie diese lokal ab.
2. Klicken Sie auf **Lizenzen** im Hauptmenü und wählen Sie den Menüpunkt **Installieren** im Navigationsbereich aus.
3. Geben Sie den vollen Pfadnamen der Lizenzdatei an.
4. Mit der Schaltfläche **Installieren** werden die Lizenzdatei ausgewertet und die neuen Lizenzen bereitgestellt.

7.5.2 Lizenzen anzeigen

1. Klicken Sie auf **Lizenzen** im Hauptmenü und wählen Sie den Menüpunkt **Anzeigen** im Navigationsbereich aus.

Übersicht Lizenzverwendung Prüfen

Applikation	Installierte Lizenzen	Benutzte Lizenzen	Freie Lizenzen
CAP-E	100	0	100
CAP-S	100	0	100
CAP-A	100	0	100
ComAssistant	100	0	100
CAP-L	100	0	100

Installierte Lizenzschlüssel

Hersteller	Applikation	Version	Kunde	Datum	Gültig bis	Installierte Lizenzen	MAC-Adr. / Seriennr.
ICN EN	CAP-E	V2.0	Evaluation	29.04.2003		100	FF-FF-FF-FF-FF-FF
ICN EN	CAP-S	V2.0	Evaluation	29.04.2003		100	FF-FF-FF-FF-FF-FF
ICN EN	CAP-A	V2.0	Evaluation	29.04.2003		100	FF-FF-FF-FF-FF-FF
ICN EN	ComAssistant	V1.0	Evaluation	29.04.2003		100	FF-FF-FF-FF-FF-FF
COM ESY	CAP-L	V3.0	Evaluation	07.06.2006		100	FF-FF-FF-FF-FF-FF

Die **Übersicht**-Tabelle enthält Informationen zu den lizenzierten Applikationen, der Anzahl der installierten Lizenzen und der Anzahl der genutzten / noch verfügbaren Lizenzen je Applikation. Die untere Tabelle zeigt Detailinformationen für jeden installierten Lizenzschlüssel.

Die MAC-ID “FF-FF-FF-FF-FF-FF” kennzeichnet die Demo-Lizenzschlüssel. Deren Gültigkeitsdauer läuft ab der erstmaligen Nutzung einer Demo-Lizenz; sie wird deshalb in der oberen Tabelle hinter der Anzahl freier Lizenzen in Klammern angegeben. Demo-Lizenzen haben eine Gültigkeit von 2 Monaten.

Diese Komplett-Anzeige ist nur für den Administrator verfügbar; die Übersicht umfasst die Lizenz-Nutzung in allen Business-Gruppen.

Der BGAdmin sieht nur den oberen Teil (Übersicht), bezogen auf die eigene BG. Die Zahl "freier Lizenzen" wird ebenfalls BG-spezifisch ermittelt. Lizenzen, die zwar in der CAP installiert aber nicht für die BG zugeteilt wurden, werden mit einem roten Punkt gekennzeichnet.

7.5.3 Lizenzen zuordnen

Zur Zuteilung von Lizenzen an einzelne Devices gibt es zwei Möglichkeiten:

- Verwendet man Demo-Lizenzen oder werden **neue Lizenzen** installiert, so ist standardmäßig das Leistungsmerkmal **“implizit bei Lizenzüberprüfung”** aktiv. Das bedeutet, dass bei jedem ersten Lizenzierungsrequest (`registerLicense`) für ein CAP-Device an das CAP Management eine entsprechende Lizenz zugeteilt wird, falls diese Lizenz vorhanden ist und dem Device die geforderte Lizenz noch nicht zugeteilt wurde. Wird dabei die Anzahl der zur Verfügung stehenden Client-Lizenzen überschritten, werden automatisch temporäre Lizenzen mit der Gültigkeit von 2 Monaten zugeteilt.
  Hinweis bei TAPI-Applikationen: Da fast alle TAPI-Applikationen keine individuelle Applikations-Id zur Lizenzierung übermitteln (`lineDevSpecificFeature`), erfolgt intern durch den SCC Schritt für Schritt eine Lizenzabfrage in der Reihenfolge “CAP-A”, “CAP-S”, “CAP-E”. Diese wird solange durchlaufen, bis eine Lizenz erfolgreich überprüft wurde oder keine Lizenz zur Verfügung steht. Wenn ein Kunde z.B. eine CAP-S Lizenz gekauft hat, muss in diesem Fall die Zuteilung der CAP-A Demo-Lizenz auf “bei Device-Einrichtung” gesetzt werden, oder die CAP-A Demo-Lizenz muss deinstalliert werden. So werden Demo-Lizenzen nicht ungewollt zugeteilt.
- Alternativ dazu kann der Administrator einem Device Lizenzen *explizit* bei Einrichtung des Benutzers im OpenScape CAP User Management (vgl. Abschnitt 7.3.1) zuordnen. Stehen keine Lizenzen mehr zur Verfügung, erhält der Administrator beim Einrichten der Benutzerkennung eine Fehlermeldung.

1. Klicken Sie auf **Lizenzen** im Hauptmenü und wählen Sie den Menüpunkt **Zuordnen** im Navigationsbereich aus, um das Zuteilungsverfahren zu definieren.
2. Anschließend muss die Business-Gruppe ausgewählt werden, für die der Zuteilungsmodus angezeigt / geändert werden soll. Der Administrator hat hier komplette Auswahlmöglichkeiten (und kann sich mit "Übersicht" eine druckbare Zusammenfassung der Zuteilungsmodi in allen Business-Gruppen anzeigen lassen). Der BGAdmin sieht immer nur die Daten der eigenen BG.
3. Wählen Sie für jeden der verfügbaren Lizenzschlüssel/Applikations-Id "implizit bei Lizenzüberprüfung" (first come / first served) oder “bei Device-Einrichtung” (explizite Zuordnung durch den Administrator).
4. Klicken Sie **Speichern** zur Bestätigung Ihrer Auswahl.

Die einem Device (auf einem der beiden beschriebenen Wege) zugeordneten Lizenzen werden regelmäßig im Dialog **Devices suchen / ändern** angezeigt. In gleicher Weise zeigt der Dialog Benutzer suchen / ändern alle Lizenzen, die der Benutzer indirekt (d.h. über ihm zugeordnete Devices) belegt. Da einem Benutzer mehrere Devices zugeordnet sein können, die jeweils die gleiche Lizenz tragen, kann ein Benutzer mehrere Lizenzen des gleichen Typs belegen. Diese werden angezeigt z.B. als "CAP-S[2]" - der Benutzer belegt 2 CAP-S-Lizenzen.

7.5.4 Lizenzen löschen (nicht für BGAdmin)

Manchmal ist es erforderlich, bereits installierte Lizenzschlüssel zu löschen.

1. Klicken Sie auf **Lizenzen** im Hauptmenü und wählen Sie den Menüpunkt **Deinstallieren** im Navigationsbereich aus.
2. Wählen Sie die Applikation / den Lizenzschlüssel, der gelöscht werden soll.
3. Wenn Sie die zu löschenden Lizenzen bei den Devices, denen solche Lizenzen zugeordnet wurden, ebenfalls entfernen möchten, selektieren Sie “Zugewiesene Lizenzen auch entfernen“.
4. Klicken Sie **Deinstallieren** zum Ausführen der Aktion.

> In früheren Releases der CAP V3.0 war es nicht möglich, Demolizenzen zu löschen. Dies wird nun unterstützt - dies ist zum Beispiel nützlich, um Situationen wie in Abschnitt 7.5.3 beschrieben zu umgehen, wo eine Demolizenz zugeteilt wird, obwohl eine reguläre Lizenz vorhanden ist.

7.5.5 Lizenzen aufteilen (nicht für BGAdmin)

Diese Funktion ist neu in HiPath CAP V3.0 SMR4 und dient der Aufteilung der installierten Lizenzen auf die einzelnen Business-Gruppen. Nach der Lizenzinstallation (Abschnitt 7.5.1) sind alle installierten Lizenzen automatisch der Standard-BG / "none" zugewiesen, alle anderen BGs (soweit bereits eingerichtet) bleiben bei 0. Um diese Aufteilung zu ändern,

1. Klicken Sie auf **Lizenzen** im Hauptmenü und wählen Sie den Menüpunkt **Aufteilen** im Navigationsbereich aus.
2. Anschließend muss die Business-Gruppe ausgewählt werden, der Sie Lizenzen zuteilen wollen. Der Administrator hat hier komplette Auswahlmöglichkeiten (und kann sich mit "Übersicht" eine druckbare Zusammenfassung der aktuellen Aufteilung auf alle Business-Gruppen anzeigen lassen).
3. Anschließend wird in einer Tabelle angezeigt
   "Applikation" - installierte Lizenzkeys / ApplicationIDs
   "Installiert" - die über Installation insgesamt bereitgestellte Anzahl von Lizenzen
   "Restliches Kontingent" - Anzahl der noch nicht an BGs zugeteilten Lizenzen
   "Kontingent" - Eingabe der Zuteilung für die ausgewählte BG
   "Benutzt" - Anzahl der in der ausgewählten BG aktuell genutzten
   (d.h. an Devices zugewiesenen) Lizenzen
   "Frei" - Anzahl der in der ausgewählten BG aktuell nicht genutzten
   (d.h. nicht an Devices zugewiesenen) Lizenzen
4. Nach Eingabe der Kontingente klicken Sie **Speichern** zur Bestätigung der Aufteilung.

7.6 Daten

Sie können im Menüpunkt **Daten** des Hauptmenüs aus einer Datei in unterschiedlichen Formaten Daten in die CAP Management-Datenbank importieren. Dies ist insbesondere nützlich zum Datenabgleich mit externen Quellen wie der Switch-Administration. Außerdem gibt es ein spezielles Programm zum Import großer Datenmengen, das im Stapelbetrieb arbeitet und offline angestoßen werden kann.

Die CAP Management-Daten können auch in eine Datei exportiert werden; dies hilft um in einfach lesbarer Form den Inhalt der Datenbank anzuzeigen und überprüfen zu können. Bitte beachten Sie auch die Export-Mechanismen in Zusammenhang mit Benutzer- und Device-Suche (Abschnitt 7.3.2 und Abschnitt 7.4.2), die zum gleichen Zweck genutzt werden können.

Zur gesteuerten Synchronisation in geplanten Zeitintervallen besteht die Möglichkeit, Import- (und Export-) Tasks / Timer einzurichten.

7	Bitte beachten Sie, dass Export / Import nicht als Ersatz für Sichern / Wiederherstellen gedacht ist. Generell ist es weder möglich noch vernünftig, eine über Export erzeugte Datei als Eingabe für einen anschließenden Import zu verwenden. Außerdem kann sich das Format von Export- oder Import-Dateien zwischen unterschiedlichen CAP-Versionen ändern; stellen Sie nach Umstellung auf eine neue Version sicher, dass ihre Import-Dateien noch gültiges Format haben! Es gibt keine Zusicherung, dass eine für CAP Version x gültige Import-Datei in Version x+1 problemlos weiterhin genutzt werden kann. Bitte beachten Sie, dass wenn mehrere Geräte zu einem Benutzer gehören, funktioniert Export/Import nur in dem folgenden Fall: zuerst müssen die Geräte, dann der Benutzer und die Geräte exportiert werden. Bei dem Import müssen zuerst die Geräte, dann der Benutzer und die Geräte importiert werden mit Modus add/update.

Die Konfigurations- und Benutzerdaten der CAP werden durch eine Open LDAP Server (Prozess "SLAPD") verwaltet und befinden sich im Verzeichnis:

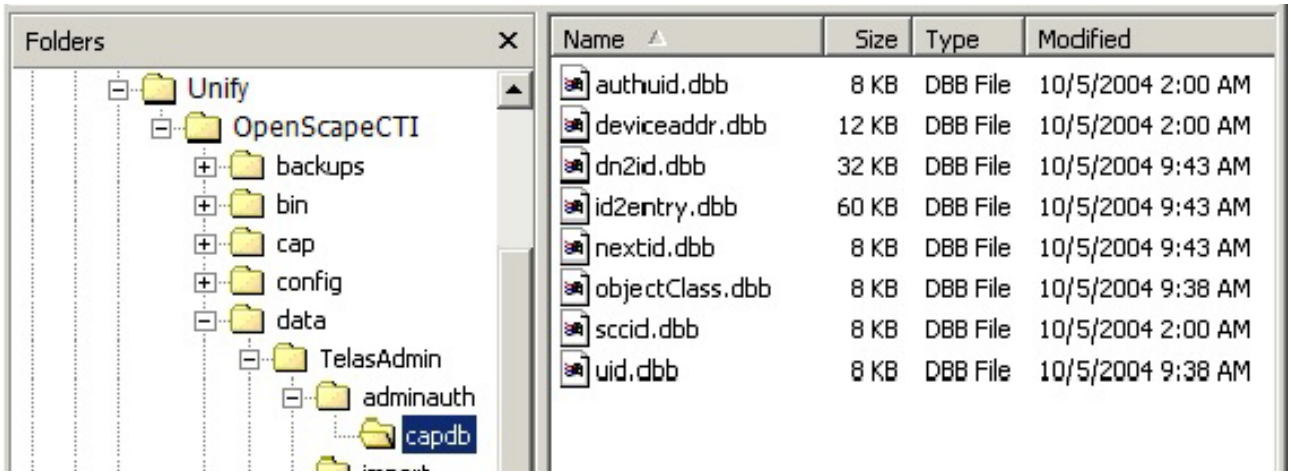
```
<InstDir>\data\TelasAdmin\adminauth\capdb
```

Im Fall von Benutzer und Device Inkonsistenz sollten folgende Maßnahmen getroffen werden:

1. Kontrollieren Sie, ob CAP-Denste "OpenScape CTI" läuft

2. Starte Sie das Kommando <InstDir>\bin\tools\user2device.bat

3. Falls es um einen sehr großen Datenbak handelt, kann es passieren, dass im output ein "NO Response" literal auftaucht.
In dem Fall sollteder Wert des Parameters soTimeOut gehoben werden.
Um das ergebnis des Processes einfach handhaben zu können, es ist ratsam, das Startkommando auf folgender weise auszuführen: user2device.bat > out.txt


Folders
Unify
OpenScapeCTI
backups
bin
cap
config
data
TelasAdmin
adminauth
capdb
Name
Size
Type
Modified
authuid.dbb 8 KB DBB File 10/5/2004 2:00 AM
deviceaddr.dbb 12 KB DBB File 10/5/2004 2:00 AM
dn2id.dbb 32 KB DBB File 10/5/2004 9:43 AM
id2entry.dbb 60 KB DBB File 10/5/2004 9:43 AM
nextid.dbb 8 KB DBB File 10/5/2004 9:43 AM
objectClass.dbb 8 KB DBB File 10/5/2004 9:38 AM
sccid.dbb 8 KB DBB File 10/5/2004 2:00 AM
uid.dbb 8 KB DBB File 10/5/2004 9:38 AM

7.6.1 Daten importieren

Datenimport wird immer gesteuert über eine Import-Datei; diese enthält eine Kopfzeile, die die zur Interpretation des Dateiinhalts erforderliche Information liefert, gefolgt von einer Zeile je Eintrag / Datensatz. Eine genauere Beschreibung folgt weiter unten.

Wenn Sie Daten aus einer bestimmten Datei importieren wollen, wählen Sie den Menüpunkt **Daten | Import**

1. Klicken Sie auf **Daten** im Hauptmenü und wählen Sie **Import** im Navigationsbereich.
2. Geben Sie in die Felder die Daten ein. Die Felder sind in der nachstehenden Tabelle beschrieben.

Dialog Import

Feld	Beschreibung
Datentyp	Wählen Sie die zu importierenden Elemente aus: ? Benutzer- und Devicedaten ? Devicedaten ? Benutzerdaten ? Benutzer- und Devicedaten HiPath 8000 / OpenScape Voice Abhängig von der Auswahl können in der Import-Datei unterschiedliche Datenfelder vorhanden sein. Die letzte Auswahl ist ausschließlich für die Zusammenarbeit mit dem "GEM-Tool" der HiPath 8000 / OpenScape Voice gedacht.
Importmodus	Wählen Sie aus: ? Alle Daten aus Importdatei neu erstellen der entsprechende Anteil der Datenbank wird vor dem Import gelöscht; danach stimmen also Inhalte von Datenbank und Datei überein ? Einträge aus Importdatei ergänzen / aktualisieren heißt nur Hinzufügen / Ändern - die in der Datei vorhandenen Einträge werden in der Datenbank erzeugt / modifiziert, andere DB-Einträge bleiben unberührt ? Einträge aus Importdatei aktualisieren heißt die in der Import-Datei vorhandenen Einträge werden entsprechend einer jeweils spezifizierten Aktion (ADD, MOD, DEL) bearbeitet; alles andere bleibt unberührt
Importdatei	Definieren Sie die Datei, aus der importiert werden soll, entweder durch Angabe des vollständigen Pfadnamens oder durch Auswahl in einem Suchdialog.

Feld	Beschreibung
Business Gruppe (für BGAdmin fest eingestellt)	Die Default-Auswahl ist "Standard" bzw. "none". Zusätzliche BGs werden zur Auswahl angeboten sobald BGs eingerichtet wurden. Die Bearbeitung der Import-Daten erfolgt auf Basis des mitgelieferten "Business Group"-Wertes: Stimmt dieser mit der ausgewählten BG überein, wird der Datensatz übernommen, andernfalls wird er ignoriert. Bleibt das Auswahlfeld leer (nicht für BGAdmin), so gelten alle BGs als ausgewählt. In diesem Fall werden alle Datensätze übernommen und entsprechend dem mitgelieferten "Business Group"-Wert einsortiert; wenn eine spezifizierte BG noch nicht existiert, wird sie implizit eingerichtet. Datensätze ohne "Business Group"-Spezifikation werden der Standard / "none"-BG zugeordnet.

3. Starten Sie den Import mit der Schaltfläche **Transfer starten**.

Alle nachfolgend beschriebenen Konfigurations- und Schemadateien befinden sich im Verzeichnis

```
<InstDir>\data\TelasAdmin\import
```

Import-Konfigurationsdatei

Die Datei `impAdmData.cfg` definiert Parameter für den Datenimport.

```
ExecuteAllChanges = 1 (Default unset)
```

Diese Option wurde eingeführt, um die unbeabsichtigte Veränderung / Verfälschung großer Teile der Datenbasis zu verhindern.Ist der Parameter nicht gesetzt (Eintrag auskommentiert), so wird der Datenimport in Abhängigkeit von der Anzahl der in der CAP-DB existierenden Einträge und der Anzahl der durchzuführenden Änderungen gesteuert. Bei einer Anzahl <100 CTI-Benutzern wird ein Import nur durchgeführt, wenn weniger als 10% geändert werden sollen. Bei einer Anzahl von 100 und mehr CTI-Benutzern wird ein Import bei maximal 1% Datenänderungen durchgeführt.

Wenn dieser Schutz nicht für erforderlich gehalten wird, kann durch Entfernen des Kommentarzeichens vor diesem Eintrag die Ausführung aller Änderungen in jedem Fall erzwungen werden.

Der Grenzwert kann kundenspezifisch auch auf einen anderen Wert als 1% eingestellt werden.

Dazu dient der neue Parameter

```
# Maximum number of objects which can be changed before import stops (
in percent )

#NumOfChangesInPercent = 1
```

Um einen kundenspezifischen Wert einzustellen, ist der gewünschte Prozentwert != 1 einzutragen und das Kommentarzeichen vor NumOfChangesInPercent zu entfernen. Damit wird dieser Wert generell als Grenzwert (ohne Unterscheidung für "kleine" wie für "große" Datenbanken) genutzt. Auch dieser Grenzwert kann durch Aktivieren von ExecuteAllChanges = 1 aufgehoben werden.

Bitte beachten Sie, dass Änderungen nach Abspeichern in der Datei impAdmData.cfg mit der nächsten Import-Aktion (angestoßen über die CAP-Bedienoberfläche oder über einen Timer) wirksam werden.

Ein Neustart der CAP oder einzelner CAP-Dienste ist dazu nicht erforderlich.

Daten-Import-Dateien

Abhängig vom gewählten Datentyp und Importmodus werden unterschiedliche Formate verwendet. Die Template-Dateien `devices.hdms`, `user.hdms` oder `user.txt` können als Ausgangspunkt für die Erzeugung eigener Import-Dateien dienen.

Mögliche Felder in Import-Datei "Devicedaten"

Feld	Beschreibung
action	nur für Modus "Einträge aus Importdatei aktualisieren"; definiert die für den jeweiligen Eintrag gewünschte Aktion ADD (neuer Eintrag), MOD (ändern), DEL (löschen)
countryCode	z.B. "49" für Deutschland, "43" für Österreich
areaCode	Ortskennzahl ohne führende 0, z.B. "89" für München
number	Rufnummer ohne Nebenstelle, z.B. "722" für Unify MUC
extension	Nebenstelle, z.B. die "1234" aus +49(89)722-1234
sccId	ID des für das Device zuständigen Dienstes (SCC)
sccId2	ID des alternativ für das Device zuständigen DIenstes (SCC) (AccessPointEmergency-Konfiguration, nur für HiPath / OpenScape 4000)
deviceId	Device-Nummer im kanonischen Format, z.B. "+49(89)722-1234"

Feld	Beschreibung
devType	unterstützte Werte sind Phone (Standardwert), SIP, HuntGroup, VirtualDevice, RoutingDevice, Trunk
deviceInfo	ID für die mit XMLPS genutzte Device-Beschreibung; unterstützte Werte sind CMI, Optipoint_410, Optiset_Advanced
pbxFormat	Device-Nummer im Format wie es in Richtung PBX genutzt wird +49(89)722-1234 wird z.B. zu "897221234" (HiPath 8000 / OpenScape Voice) oder "1234" (HiPath / OpenScape 4000, overlap 0) oder "21234" (HiPath / OpenScape 4000, overlap 1)
pnp	Definition eines privaten Rufnummernplans im Format <L2C>-<L1C>-<LC>:<overlap> (z.B. "49-89-722:2") <L2C> und <L1C> sind optional
nac	node access code
XMLPSId	ID eines XML Phone Service, für den das Device konfiguriert ist
urlAssignList	Liste von Paaren <invoke button>:<URL Id> die für das Device eingerichtet ist, z.B. "2:url1"
licenses	Liste von Lizenzen, die dem Device zugeordnet sind, z.B. "CAP-S,ComAssistant"
businessGroup	Business-Gruppe, der das Device zugeordnet ist
deviceCategory **namedDeviceTypes** **routeingDevice** **groupHunt** **groupACD** **groupPick** **groupUser** **deviceModelName** **nidGroup**	diese Felder werden wie im CSTA Standard beschrieben genutzt

Pflichtfelder für Devicedaten-Import sind sccId sowie entweder deviceId oder eine Kombination aus countryCode, areaCode, number und extension.

7	Für den konsistenten Ablauf des Imports ist es zwingend erforderlich, dass der für ein Device ausgewiesene SCC bereits in CAP Management eingerichtet ist und die gleiche Kombination countryCode/areaCode/number zugeordnet hat wie das Device. Beispiel: Import eines Eintrags "+49(89)722-1234|007" führt zu Inkonsistenzen, falls - ein SCC mit ID 007 noch nicht eingerichtet ist oder - SCC "007" eingerichtet ist, aber z.B. mit "+49(89)700". SCC "007" muss eingerichtet sein mit "+49(89)722".

Beispiel (minimale Devicedaten-Importdatei):

```
countryCode|areaCode|number|extension|sccId
49|89|722|53111|0220
49|89|722|53517|0220
```

ist inhaltlich gleichwertig zu:

```
deviceId|sccId
+49(89)722-53111|0220
+49(89)722-53517|0220
```

Mögliche Felder in Import-Datei "Benutzerdaten"

Feld	Beschreibung
action	nur für Modus "Einträge aus Importdatei aktualisieren"; definiert die für den jeweiligen Eintrag gewünschte Aktion ADD (neuer Eintrag), MOD (ändern), DEL (löschen)
name	Benutzername, z.B. "James Bond"
credentials	Passwort in Klartext; falls dieser Eintrag leer ist, wird der Benutzer mit Standard-Passwort eingerichtet
credStamp	Gültigkeitsdauer für das Passwort (dieses Feld wird nur beim Export unterstützt!)
authUId	eindeutiger alias zum Login (bei Windows Login ist <domain>\<loginName> anzugeben)
uid	eindeutige ID für den Benutzer
roles	Benutzer-Rollen; unterstützte Werte sind CTI Benutzer (Standardwert), Admin, Application

Feld	Beschreibung
authMode	Authentisierungs-Modus; unterstützte Werte sind TELAS (Standardwert), NT
userGroups	komma-getrennte Liste von Benutzer-Gruppen, denen der Benutzer zugeordnet ist
timeZone	Zeitzone für den Benutzer
businessGroup	Business-Gruppe, der der Benutzer zugeordnet ist
removable	Dieses Kennzeichen zeigt ob der Benutzer gelöscht werden darf oder gegen Löschen geschützt ist (dieses Feld wird nur beim Export unterstützt!)

Pflichtfelder für Benutzerdaten-Import sind entweder uid oder authUId; in jedem Fall ist es ratsam, auch einen Namen zu definieren.Für auhMode=NT (Authentisierung über Windows Login) ist die Angabe von authUId Pflicht.

Beispiel (Benutzerdaten-Importdatei):

```
name|credentials|authUId
James Bond||jamie
```

Mögliche Felder in Import-Datei "Benutzer- und Devicedaten"

Hier sind alle für Device- und Benutzer-Import beschriebenen Felder zulässig.

Pflichtfelder für Benutzer- und Devicedaten-Import sind die gleichen wie für Devices spezifiziert. Falls weder uid noch authUId mitgeliefert werden, wird aus number / deviceId eine uid gebildet. Bitte beachten Sie dass dies zu Problemen führen kann, falls sich mehrere Benutzer ein Device teilen! Beispiel (Benutzer- und Device-Daten-Importdatei, Modus update):

```
action|countryCode|areaCode|number|extension|sccId|name|credentials|authUId|licenses
ADD|49|89|722|53111|0220|JAHN|myPasswd|janni|
MOD|49|89|722|53517|0220|Gustav Meier||gustl|CAP-A
```

Log-Dateien zum Datenimport

Nach einem Import befindet sich in diesem Verzeichnis die Datei `"updatePerm.cmd"`. Sie beinhaltet sämtliche durchgeführten Import-Aufrufe. Gleichzeitig wird der Import protokolliert. Die Protokolldatei lautet:

```
<InstDir>\logs\<PC-Name>\import.log
```

Diese Datei wird laufend aktualisiert und enthält alle über Import veranlassten Änderungen.

Importieren von logischen Geräten in der HiPath / OpenScape 4000

Wenn Anwendungen “Non-Station Devices” (vgl. Abschnitt 7.4) in der HiPath / OpenScape 4000 ansprechen, muss eine Adresstypumwandlung erfolgen. Solche Geräte werden in Richtung HiPath / OpenScape 4000 über ihre “LODEN-Nummer” angesprochen, aber in Richtung Applikation über eine (symbolische) Device ID / Rufnummer identifiziert.

Beispiel:

```
RCG 100     Rufnummer: +49(5251)2214-7661     LODEN: 33554442
```

Das HiPath / OpenScape 4000 "Expert Access (ComWin)" unterstützt eine Funktion, mit der die Informationen für alle Devices (Nebenstellen, Sammelanschlüsse, RCG-Gruppen, Leitungen, sowie deren LODEN-Nummern) in der Anlage in eine Datei heruntergeladen werden können.

7	Bitte beachten Sie, dass zum erfolgreichen Import das “Canonical Präfix” [Beispiel: +49(5251)2214] genau so wie in OpenScape CAP verwendet auch in der HiPath / OpenScape 4000 eingerichtet sein muss (AMO KNDEF).

Man kann die Device-Daten über den Service SPI importieren (in Abschnitt 6.2.3 beschrieben) - die Nutzung auf diese Weise ist vermutlich die bequemere.

7.6.2 Import großer Datenmengen (nicht für BGAdmin)

Um den ersten Aufbau eines CAP-Datenbestandes bei einer großen Zahl von Benutzern / Devices zu beschleunigen, gibt es eine spezielle Funktion zum Import großer Datenmengen ("bulk import"). Diese ist nur im offline-Betrieb einsetzbar (Service OpenScape CTI läuft nicht). Sie setzt auf einer Import-Datei auf (übliches Format wie auch für den online-Import) und erzeugt daraus eine Datei im ldif-Format, die über das Kommando slapadd direkt in die Datenbank eingelesen wird.

Bitte verfahren Sie wie folgt:

1. Stoppen Sie den Dienst OpenScape CTI.
2. Passen sie die Konfigurationsdatei `impAdmData.cfg` (vgl. Abschnitt 7.6.1) an; aktivieren Sie den Eintrag

   ```
   UsingLdif = true
   ```

   indem Sie das Kommentarzeichen entfernen.
3. Rufen Sie aus einem command-Fenster im Verzeichnis `.../OpenScape/CTI/bin/tools`

   ```
   import.bat <import file name>
   ```

auf; dabei ist `<import file name>` entweder ein Pfadname relativ zum Verzeichnis `.../OpenScapeCTI/data/TelasAdmin/import` oder ein absoluter Pfadname.

Dadurch wird im Verzeichnis `.../import` eine Datei `objects.ldif` erzeugt, die anschließend mit dem Datenbank-Tool slapadd in die Datenbank eingelesen wird.

4. Nach Abschluss der Aktion kann es sinnvoll sein, den Eintrag "UsingLdif" wieder zu deaktivieren.
5. Starten Sie den Dienst OpenScape CTI wieder.

7	Der "bulk import" führt unweigerlich zu Doppeleinträgen im CAP-Datenbestand, sofern die zu importierenden Devices bereits mit dem "normalen Import" eingebracht wurden. Daher wird empfohlen ausschliesslich nur eines der hier beschriebenen Import-Verfahren zu nutzen.

7	Das Passwort-Handling bedarf während des "bulk imports" einer gesonderten Beachtung. Der Bulk import läuft im Offline-modus, daher können von der CAP-Datenbank zum Zeitpunkt der Passwort-Änderung keine Daten abgerufen werden; das gilt auch für die Änderung des "default passworts". Deswegen soll in der bulk import Datei für jeden Benutzereintrag ein Passwort eingetragen sein; Beachten sie auch, dass das Passwort im "Klartext" angegeben wird und aus mindestens 3 Zeichen bestehen muss.

7.6.3 Daten exportieren

Wenn Sie den Datenbank-Inhalt in eine Datei (.csv-Format, komma-separierte Liste) exportieren wollen, wählen Sie den Menüpunkt **Daten | Export**.

1. Klicken Sie auf **Daten** im Hauptmenü und wählen Sie **Export** im Navigationsbereich aus.
2. Geben Sie in die Felder die Daten ein. Die Felder sind in der nachstehenden Tabelle beschrieben.

Dialog Export

Feld	Beschreibung
Datentyp	Wählen Sie aus: ? Benutzer- und Devicedaten ? Devicedaten ? Benutzerdaten ? Benutzer- und Devicedaten HiPath 8000 / OpenScape Voice Abhängig von der Auswahl sind unterschiedliche Datenfelder zum Export verfügbar. Details sind im Zusammenhang mit dem Inport in Abschnitt 7.6.1 beschrieben.
Business Gruppe (für BGAdmin fest eingestellt)	Die Default-Auswahl ist "Standard" bzw. "none". Zusätzliche BGs werden zur Auswahl angeboten sobald BGs eingerichtet wurden. Es werden nur die Daten der ausgewählten BG exportiert. Bleibt die Auswahl leer (nicht für BGAdmin), so gelten alle BGs als ausgewählt.

3. Klicken Sie **Felder auswählen**, falls Sie nur bestimmte Felder der Device- oder Benutzerdaten exportieren wollen. Nach Auswahl der gewünschten Felder klicken Sie auf **Transfer starten**.
4. Alternativ dazu klicken Sie **Alle Felder exportieren**, falls Sie alle vorhandenen Benutzer- und/oder Device-Datenfelder exportieren wollen.
5. Danach erfolgt ein Standard-Windows-Dialog, in dem Sie die erzeugte Export-Datei entweder direkt öffnen oder an einer definierten Stelle speichern können.

> Bitte beachten Sie, daß aus Sicherheitsgründen nur die Daten für Benutzer mit der Rolle "CTI Benutzer" exportiert werden. "Admin"- oder "Application"-Benutzer werden nicht exportiert.

7.6.4 Geplante Tasks

Hier können Sie einen Task einrichten oder einen bestehenden Task neu konfigurieren. Mit Hilfe eines Tasks (Timer) können Sie festlegen, zu welchen Zeiten die Dateien automatisch aus einer bestimmten Datei importiert werden sollen oder die CAP CTI-Benutzer in eine bestimmte Datei exportiert werden sollen.

Um einen Task (Timer) erstmalig einzurichten oder einen bestehenden Task neu zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie auf **Daten** im Hauptmenü und wählen Sie den Menüpunkt **Geplante Tasks** im Navigationsbereich aus.

   a) Es ist noch kein Task eingerichtet. Weiter mit 2a.

   b) Es ist bereits ein Task eingerichtet. Dieser wird Ihnen in der "Liste der laufenden Timer" angezeigt. Weiter mit 2b.

2. Konfigurieren Sie die Tasks.

   a) Ist noch kein Task eingerichtet, klicken Sie auf das Symbol **Neuen Timer anlegen**.

   b) Ist bereits ein Task eingerichtet, wird Ihnen in der "Liste der laufenden Timer" angezeigt. Wählen Sie den Task aus, indem Sie auf das Symbol **Bearbeiten** klicken.

3. Füllen Sie die nachstehend beschriebenen Felder aus:

Dialog Timer konfigurieren

Feld	Beschreibung
Timername	Geben Sie hier einen frei wählbaren Namen für den Task an.
Datentyp	Wählen Sie aus: ? Benutzer- und Devicedaten ? Devicedaten ? Benutzerdaten ? Benutzer- und Devicedaten HiPath 8000 / OpenScape Voice Abhängig von der Auswahl können in der Import-Datei unterschiedliche Datenfelder vorhanden sein. Details sind im Zusammenhang mit dem Inport in Abschnitt 7.6.1 beschrieben.
Transferrichtung	Wählen Sie hier Import oder Export aus.
Importmodus (für Export ist dieses Feld inaktiv)	Wählen Sie aus: ? Alle Daten aus Importdatei neu erstellen ? Einträge aus Importdatei ergänzen / aktualisieren ? Einträge aus Importdatei aktualisieren Details dazu in Abschnitt 7.6.1
Transferintervall	Geben Sie hier an, in welchem Abstand die Datenbank importiert oder exportiert werden soll. Sie können dabei zwischen folgenden Intervallen wählen: ? täglich ? wöchentlich ? monatlich
Startzeit	Geben Sie die Startzeit des Transfers in Stunden (hh) und Minuten (mm) an.

Feld	Beschreibung
Startdatum	Geben Sie hier das Startdatum des Transfers in der Form DD/MM/YYYY (z.B. 16/05/2004) an. Sie können das Datum auch aus einem Kalender auswählen. Klicken Sie dazu auf das Kalendersymbol rechts neben dem Eingabefeld.
Quell-/Zielverzeichnis	Geben Sie hier den Ablageort an, an dem die zu exportierende Datenbank abgelegt werden soll oder an dem die zu importierende Datei liegt.
Dateiname	Definieren Sie den Namen der Import- / Export-Datei
Business Gruppe (für BGAdmin fest eingestellt)	Die Default-Auswahl ist "Standard" bzw. "none". Zusätzliche BGs werden zur Auswahl angeboten sobald BGs eingerichtet wurden. Die geplante Task bezieht sich auf die jeweils angegebenen BGs.

4. Schließen Sie Ihre Eingaben mit einer der folgenden Aktionen ab:

Aktion	Beschreibung
Speichern	Speichert Ihre Eingaben und fügt den Task zur "Liste der laufenden Timer" hinzu.
Pause	Setzt den gewählten Task in den Standby-Modus, d.h. er wird solange nicht mehr ausgeführt, bis Sie ihn mit dieser Schaltfläche wieder freisetzen.
Löschen	Löscht den gewählten Task aus der “Liste der laufenden Timer”.
Abbruch	Schließt den Dialog ohne die Eingaben zu speichern.

Durch Click auf das Symbol am Ende jedes Timer-Eintrags in der Timer-Liste erhalten Sie detaillierte Information zum aktuellen Zustand des jeweiligen Timers.

7 Zur korrekten Durchführung der "geplanten Tasks" ist es unerlässlich, dass die spezifizierten Dateien zum geplanten Zeitpunkt verfügbar (Schreiben / Lesen) sowie beim Import auch aktuell sind. Um zu vermeiden, dass ein und dieselbe Datei immer wieder importiert wird (ohne zu erkennen, dass die Bereitstellung aktueller Daten fehlgeschlagen ist), wird jede Datei nach erfolgreichem Import durch Voranstellen eines Unterstrichs "_" umbenannt.

7.7 Diagnose

Hier werden die Funktionen zur Überwachung, Konfiguration und Problemdiagnose für alle Komponenten des Systems behandelt: Logging-Informationen, Anzeige und Änderung von Konfigurationsdaten, Zustände von Services und Prozessen, Anzeige beteiligter Hosts, Restart von Prozessen.

1. Klicken Sie auf **Diagnose** im Hauptmenü und wählen Sie den Menüpunkt **Diagnose** im Navigationsbereich aus.

   Es wird eine Übersichtsmeldung zum Zustand des gesamten Systems angezeigt.

2. Klicken Sie auf die Schaltfläche  rechts neben der Meldung.

   Das Diagnose-Applet **CAP Management Diagnose Agent** wird gestartet und stellt alle Funktionen für Diagnose und Konfiguration in einem eigenen Fenster zur Verfügung.

Es besteht auch die Möglichkeit, den CAP Management Diagnose Agenten lokal zu installieren. Diese Applikation läuft dann lokal auf dem PC, unabhängig vom Web-Browser.

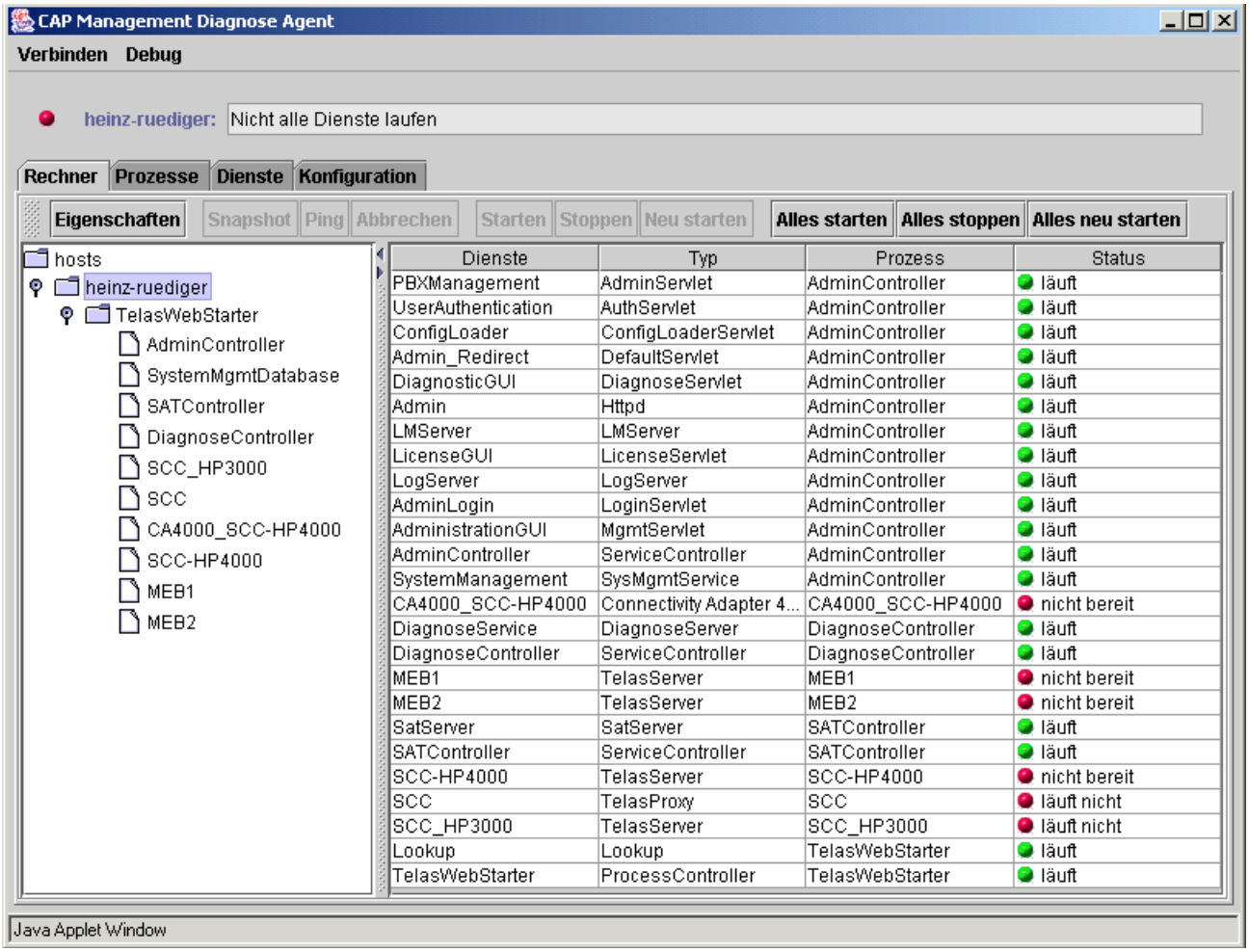
Lokale Installation des CAP Management Diagnose Agenten

1. Starten Sie den Download der Datei `twebDiagAgent.jar`.
2. Merken Sie sich den Speicherort der Download-Datei.
3. Wechseln Sie mit dem Explorer in den Ordner, in dem die Datei gespeichert wurde.
4. Starten Sie den CAP Management Diagnose Agenten mit Doppelklick.

> Bei einer lokalen Installation des "Diagnose Agenten" darf diese Applikation nicht in einem Pfad installiert worden sein, der Leerzeichen enthält. Ist dies der Fall, kann der lokale "Diagnose Agent" nicht gestartet werden.
> Durch eine Änderung in der REGISTRY kann dieses Problem jedoch gelöst werden.
> Ändern Sie in `HKEY_CLASSES_ROOT\jarfile\shell\open\command` den Eintrag:
> "`<jre-path>\bin\javaw.exe" -jar %1`
> nach:
> "`<jre-path>\bin\javaw.exe" -jar "%1`".
> `<jre-path>` ist der Pfad zum lokal installierten Java Runtime Environment.
> Begrenzung: der Diagnose Agent ab SMR13 benötigt Java 1.7!

Ist beim Download als Browser-Sprache Deutsch eingestellt, so wird die deutsche Version des CAP Management Diagnose Agenten geliefert - analog die englische Version für die Browser-Sprache Englisch.

Der Diagnose Agent ist immer mit einem Diagnose Controller verbunden, der auf dem PC mit CAP Management läuft, von dem er heruntergeladen wurde. Das folgende Bild zeigt die Bedienoberfläche des CAP Management Diagnose Agenten:



Dienste	Typ	Prozess	Status
PBXManagement	AdminServlet	AdminController	läuft
UserAuthentication	AuthServlet	AdminController	läuft
ConfigLoader	ConfigLoaderServlet	AdminController	läuft
Admin_Redirect	DefaultServlet	AdminController	läuft
DiagnosticGUI	DiagnoseServlet	AdminController	läuft
Admin	Httpd	AdminController	läuft
LMServer	LMServer	AdminController	läuft
LicenseGUI	LicenseServlet	AdminController	läuft
LogServer	LogServer	AdminController	läuft
AdminLogin	LoginServlet	AdminController	läuft
AdministrationGUI	MgmtServlet	AdminController	läuft
AdminController	ServiceController	AdminController	läuft
SystemManagement	SysMgmtService	AdminController	läuft
CA4000_SCC-HP4000	Connectivity Adapter 4...	CA4000_SCC-HP4000	nicht bereit
DiagnoseService	DiagnoseServer	DiagnoseController	läuft
DiagnoseController	ServiceController	DiagnoseController	läuft
MEB1	TelasServer	MEB1	nicht bereit
MEB2	TelasServer	MEB2	nicht bereit
SatServer	SatServer	SATController	läuft
SATController	ServiceController	SATController	läuft
SCC-HP4000	TelasServer	SCC-HP4000	nicht bereit
SCC	TelasProxy	SCC	läuft nicht
SCC_HP3000	TelasServer	SCC_HP3000	läuft nicht
Lookup	Lookup	TelasWebStarter	läuft
TelasWebStarter	ProcessController	TelasWebStarter	läuft

Navigation in diesem Fenster ist durch Anwahl der entsprechenden Register möglich. Die Bedeutung der einzelnen Register wird im folgenden erläutert.

Diagnoseinformationen

Folgende Informationen sind für die Analyse von Problemen wichtig und hilfreich:

- **Produktinformation**: Gibt einen Überblick über das installierte Produkt. Wichtig ist dabei die Version und der Build-Stand. Diese Daten sollten immer bei Kontaktaufnahme mit der Hotline angegeben werden.
- **Prozess-Informationen**: Zeigt die Tabelle der zur Zeit gestarteten Prozesse. Wichtig ist, dass der Status aller angezeigten Prozesse in Ordnung ist. Hier kann der Administrator einen ersten Überblick über Probleme erhalten.
- **Service-Informationen**: Genaue Informationen über die im System gestarteten Services und ihren Status erhält man in dieser Tabelle. Auch hier zeigt der Status evtl. ein potentielles Problem. Weiterhin wird die Prozess-/Servicezuordnung angezeigt.

- **Konfigurationsinformationen**: Die Konfigurationsdateien können eingesehen, analysiert und geändert werden. Nach Änderung von Konfigurationsdateien müssen die zugehörigen Komponenten (ggf. auch das Gesamtsystem) gestoppt und neu gestartet werden.
- **Logging-Informationen**: Während des Betriebs werden laufend Logging-Informationen in Dateien geschrieben. Alle Logging-Dateien sind im Verzeichnis <Inst-Dir>\Logs abgelegt. Eine besondere Rolle spielt die Datei “errors.log”. In dieser Datei werden zu allen Services Fehler abgelegt und mit der Kennzeichnung des Services versehen. Es ist sinnvoll, diese Datei regelmäßig zu überprüfen und wenn nötig zurückzusetzen, damit im Fehlerfall auftretende Probleme schneller erkannt werden können.
  Zur genauen Analyse eines konkreten, reproduzierbaren Problems sollte zunächst die Logging-Historie gelöscht (Logging zurücksetzen) und dann der Fehler erneut provoziert werden. Dadurch werden veraltete Logging-Informationen entfernt und der Umfang der zu analysierenden Logging-Daten reduziert.
  Bei Neustart des Systems werden entsprechend der Logging-Konfiguration eventuell vorhandene Logging-Dateien auf <name>_last.log umbenannt, damit die enthaltene Information nicht verloren geht. Abhängig vom eingestellten Log-Level werden mehr oder weniger Informationen gespeichert. Log-Levels für aktive Prozesse werden über Zeige Logging angezeigt. Sollte ein Problem bei einem dieser Prozesse erkannt worden sein, so kann gezielt dessen Level hochgesetzt werden, um genauere Informationen zu bekommen.
- **Download Daten**: Mithilfe dieser Option können Diagnoseinformationen für Auswertungen und zu Weiterleitungszwecken in einer Datei gespeichert werden. Die Daten werden in ein Zip-Archiv verpackt und können per Download von der Entwicklung oder Hotline abgeholt werden.

> Die im Diagnose-Agenten angezeigte Zustandsinformation wird in regelmäßigen Zeitabständen mit den jeweiligen Prozessen / Diensten abgeglichen; sie kann aber bei Zustandsänderungen zwischen zwei Synchronisationspunkten ungenau sein. Sie können zu jedem Zeitpunkt die Synchronisation über Verbinden -> Aktualisieren explizit anstoßen.
> Weiterführende Informationen zum Thema Diagnose finden Sie in Kapitel 8, “Problembehandlung”.

7.7.1 Rechner

Wird das Register **Rechner** gewählt, so werden im linken Teilfenster alle Rechner in der Netzumgebung, auf denen ein OpenScape CTI-Service läuft, in einer Baumstruktur angezeigt. Wird ein Rechner ausgewählt, so werden alle auf diesem Rechner laufenden Services mit Zuständen und Prozesszuordnung angezeigt.

- **Eigenschaften**
  Generell können über **Eigenschaften** Zusatzinformationen in einem separaten Fenster angezeigt werden, sobald ein Rechner oder eine Zeile in der Liste der Services ausgewählt ist. Diese Informationen können in der Entwicklung zu Diagnosezwecken ausgewertet werden.

- **Alles starten, Alles stoppen, Alles neu starten**
  Mit dieser Funktion ist es möglich, alle CAP/CTI-Prozesse auf bestimmten Rechnern (gewünschte Rechner in der Baumdarstellung selektieren) oder auf allen Rechnern im Netzverbund (obersten Eintrag **hosts** in der Baumdarstellung selektieren) zu starten, zu stoppen oder zu stoppen und direkt wieder neu zu starten.

7.7.2 Prozesse

Wird das Register **Prozesse** gewählt, so wird die Liste aller im Gesamtsystem laufenden Prozesse angezeigt. Wird ein Prozess ausgewählt, so können wiederum verschiedenen Funktionen zu diesem Prozess ausgeführt werden.

- **Eigenschaften**
  Analog zu oben (Abschnitt 7.7.1), entsprechend für den gewählten Prozess.

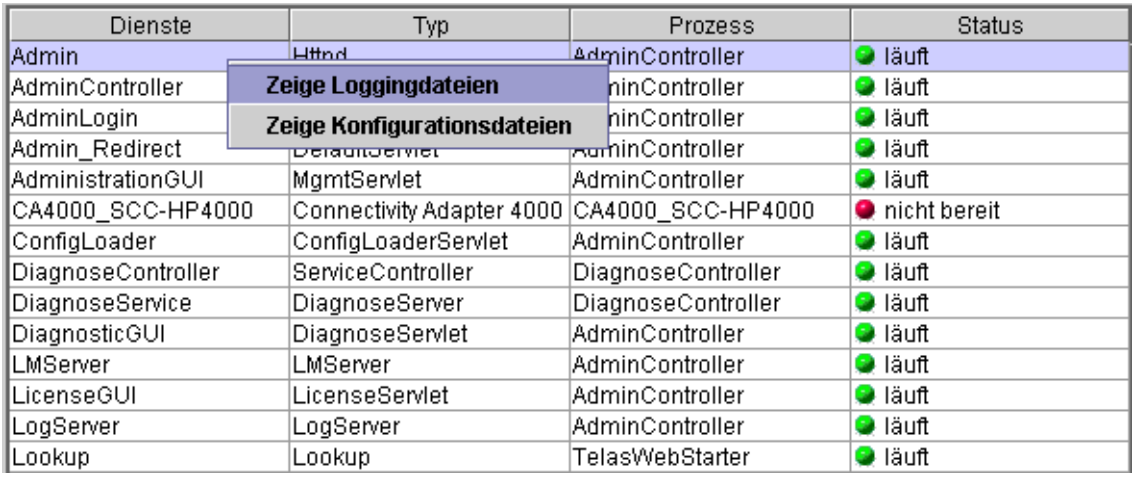
- **Snapshot**
  Für den ausgewählten Prozess können über **Snapshot** Informationen zu Environment, Logging und Threadzustand des Prozesses eingeholt werden. Zusätzlich lassen sich die aktuell geladenen Parameter abfragen (z.B. Port-Abfrage eines SCCs).

- **Ping**
  Für den ausgewählten Prozess kann über **Ping** der aktuelle Empfangszustand geprüft werden.

- **Starten, Stoppen, Neu starten**
  Diese Funktionen können auf alle Prozesse mit Ausnahme des besonderen Prozesses **TelasWebStarter** angewendet werden.

- **Alles starten, Alles stoppen, Alles neu starten**
  Über den Prozess **TelasWebStarter** werden alle anderen Prozesse gestartet. Nach Auswahl dieses Prozesses kann damit das System komplett angehalten und wieder gestartet werden.

- **Zeige Loggingdateien, Zeige Konfigurationsdateien**



Dienste	Typ	Prozess	Status
Admin	Httpd	AdminController	läuft
AdminController		AdminController	läuft
AdminLogin		AdminController	läuft
Admin_Redirect	DefaultServlet	AdminController	läuft
AdministrationGUI	MgmtServlet	AdminController	läuft
CA4000_SCC-HP4000	Connectivity Adapter 4000	CA4000_SCC-HP4000	nicht bereit
ConfigLoader	ConfigLoaderServlet	AdminController	läuft
DiagnoseController	ServiceController	DiagnoseController	läuft
DiagnoseService	DiagnoseServer	DiagnoseController	läuft
DiagnosticGUI	DiagnoseServlet	AdminController	läuft
LMServer	LMServer	AdminController	läuft
LicenseGUI	LicenseServlet	AdminController	läuft
LogServer	LogServer	AdminController	läuft
Lookup	Lookup	TelasWebStarter	läuft

Diese Funktionen sind über Kontextmenü verfügbar: Prozess auswählen, mit rechter Maustaste Kontextmenü öffnen und Funktion auswählen. Die Liste von Logging-/Konfigurationsdateien wird angezeigt. Durch Doppelklick kann der Dateiinhalt angezeigt werden.

7.7.3 Dienste

Wird das Register **Dienste** gewählt, so wird die Liste aller im System vorhandenen Services mit ihrer Prozesszuordnung und ihrem aktuellen Zustand angezeigt. Auch hier sind nach Auswahl eines Services wieder folgende Funktionen verfügbar:

- **Eigenschaften, Snapshot** und **Ping**
  Analog zu oben (Abschnitt 7.7.1, Abschnitt 7.7.2), entsprechend für den gewählten Service.

- **Zeige Loggingdateien, Zeige Konfigurationsdateien**
  Analog zu oben (Abschnitt 7.7.2), über Kontextmenü für den gewählten Service.

- **Konfiguration neu laden**
  Diese Funktion erlaubt für den ausgewählten Service das Aktualisieren seiner Konfigurationsdaten, ohne ihn komplett neu zu starten. Sie ist noch nicht für alle Typen von CAP-Diensten verfügbar; abhängig vom Typ des gewählten Dienstes wird die entsprechende Schaltfläche deshalb kontext-sensitiv aktiviert oder deaktiviert.

7.7.4 Konfiguration

Wird das Register **Konfiguration** gewählt, so kann die komplette Systemkonfiguration eingesehen und bearbeitet werden. Im linken Teilfenster wird das Konfigurations-Verzeichnis `<InstDir>\config\` in Baumstruktur angezeigt, mit der Möglichkeit wie von Explorer gewohnt

zu navigieren. Im rechten Teilfenster werden die in dem ausgewählten Verzeichnis vorhandenen Konfigurationsdateien angezeigt. Folgende Funktionen sind in dieser Anzeige verfügbar:

- **Eigenschaften**
  Für das ausgewählte Verzeichnis werden die Anzahl der vorhandenen Daten, das letzte Modifikationsdatum und der Name des Verzeichnisses angezeigt.

- **Anzeigen**
  Für die ausgewählte Konfigurationsdatei wird der Dateiinhalt in einem Fenster zum Ändern angezeigt. Eine Besonderheit bei der Anzeige besteht darin, dass in der Datei verwendete Variablen oder Include-Anweisungen durch die Funktion **Ersetze Variablen** entsprechend aufgelöst werden können um damit eine vollständige Information zu erhalten. Das Speichern von Änderungen ist nur im Zustand *nicht ersetzt* möglich.

7.7.5 Logging

Während der Laufzeit werden von allen Services des Systems Laufzeitinformationen in Dateien abgelegt. Dazu gehören Meldungen zu Informationen, Warnungen und Fehlern. Der Umfang der aufgezeichneten Daten hängt vom eingestellten Logging-Level ab.

Grundsätzlich werden alle Logging-Dateien im Verzeichnis `<InstDir>\Logs` abgelegt. Bei verteilten Installationen wird für jeden beteiligten PC ein eigenes Unterverzeichnis mit dem Rechnernamen ohne Domainzusatz angelegt.

Die Steuerung des Loggings und Anzeige von Logging-Dateien erfolgt im CAP Management Agenten entweder über das Register **Logging** oder über den Menüpunkt **Debug**.

Wird das Register **Logging** gewählt, so werden zunächst alle Logger angezeigt, die Informationen in Dateien ablegen (File-Logger). Anhand der Namen lässt sich leicht die Zuordnung zum zugehörigen Prozess bzw. Service erkennen. Dazu wird als wichtigste Information für alle Logger der aktuell eingestellte Logging-Level in der rechten Spalte angezeigt. Nach Auswahl einer Zeile in dieser Tabelle kann der Level für diesen ausgewählten Logger geändert werden.

- **Eigenschaften**
  Über Eigenschaften werden Zusatzinformationen zum ausgewählten Logger in einem Fenster angezeigt. Diese Informationen sind nur für Servicetechniker bzw. die Entwicklung vorgesehen.

- **Logging zurücksetzen**
  Mit dieser Funktion ist es möglich, ältere Logging-Informationen, die evtl. bei der Fehleranalyse stören, zu entfernen. Dabei werden ältere Logging-Dateien gelöscht und die aktuell verwendete Logging-Datei geleert.

- **Logging-Level ändern**
  Wählen Sie aus dem Aufklappmenü neben **Level setzen** den gewünschten Level aus. Die Auswahl gilt für den momentan gewählten Logger. Um die Einstellung wirksam werden zu

lassen, muss sie noch mit **Level setzen** bestätigt werden. Die Änderung des Logging-Level wirkt nur temporär bis zum nächsten Neustart des zugehörigen Service. Änderungen werden also nicht in die Konfigurationsdateien übernommen.

> Änderungen des Logging-Levels beziehen sich nur auf den jeweils ausgewählten Logger. Einstellungen für das ErrorLog, das übergreifend von allen Loggern genutzt wird, können hier nicht geändert werden, sondern nur direkt in `LogServer.cfg`.

? **Log-Filter setzen**
Hier kann inklusiv oder exklusiv ein Log-Filter gesetzt werden. Er kann das Logging erweitern oder einschränken. Dieser Filter bezieht sich auf den gesamten Inhalt der Log Datei eines selektierten CAP-Prozesses. Er ist vergleichbar mit einem Suchberiff in einem Text- oder Word-Dokument.

Um sich den Inhalt der Logging-Dateien anzusehen, wählen Sie aus der Liste der File-Logger den gewünschten aus. Über Kontextmenü (rechte Maustaste) **Zeige Loggingdateien** wird die Liste aller von diesem Logger erstellten Logging-Dateien angezeigt. Um den Dateiinhalt zu sehen genügt ein Doppelklick auf den Dateinamen.

7.7.6 “Prozess-Controller” und Dienste

Die laufenden Windows CAP Java-Prozesse haben jeweils ein eigenes Startskript, welches sich im Unterverzeichnis <PC_name> befindet. Die Konfigurationsdatei hat die Dateiendung .proc. Die Nummer **Sxx** bezeichnet die Startnummer für den Prozess.

```
Beispiel: <InstDir>\config\<pc-name>\admin\S01service_ctrl.proc
```

Die Prozesse sind im Einzelnen: TelasWebStarter, Admin Controller, Diagnostic Controller, SAT Controller und CallIdRepository. Diese fungieren als “Prozess-Controller” und “Dienst-Controller”. Nach dem erfolgreichen Start eines Prozesses startet jede “java.exe”-Datei weitere interne Dienste. Die Konfigurationsdatei für den jeweiligen Dienst hat die Dateiendung .svc. Die Nummer **Sxx** bezeichnet die Startnummer für den Dienst.

Der Admin-”Dienst-Controller” wird ebenfalls gestartet und steuert den CAP HTTP Server. Die Konfigurationsdatei für den Webserver hat den Namen “`http-server.props`”.

Admin-Controller

Zu den Admin-Controller-Diensten gehören im Einzelnen:

- PBXManagement
- UserAuthentication
- ConfigLoader
- Admin_Redirect
- DiagnosticGUI
- Admin (HTTP-Server)
- LMServer
- LicenseGUI
- LogServer
- AdminLogin
- AdministrationGUI
- CallIdRepository
- SATServer
- AdminController (als Dienst-Controller)

Diagnose-Controller

Zu den Diagnose-Controller-Diensten gehören:

- DiagnosticService
- DiagnosticController (als Dienst-Controller)

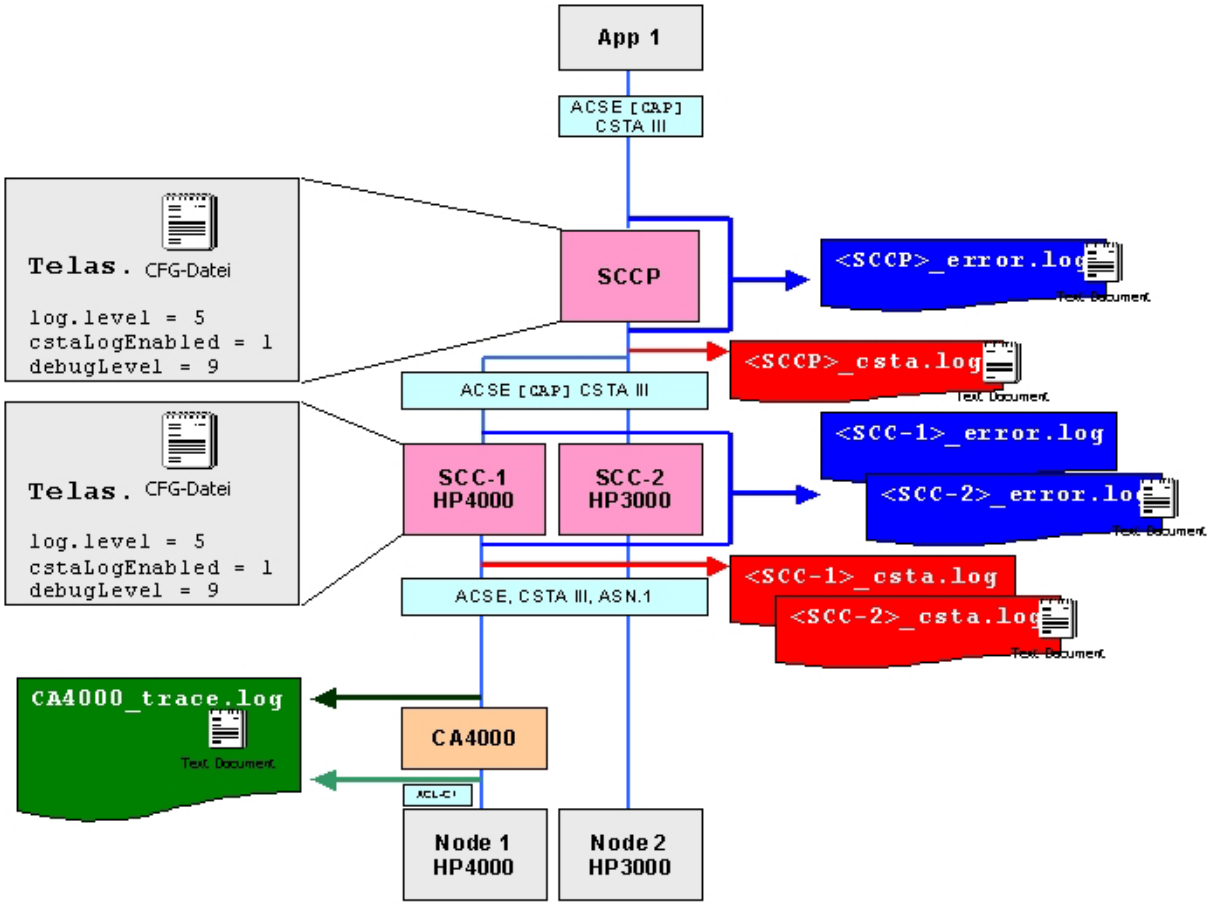
TelasWebStarter

Zu den TelasWebStarter-Diensten gehören:

- Lookup
- TelasWebStarter (als “Prozess-Controller”) (es handelt sich um den Lookup-Client!!!)

7.7.7 CSTA-Verbindungstrace

In Abhängigkeit von den verschiedenen Schnittstellen kann für die Kommunikation von der Anwendung zu einer Anlage ein vollständiger CSTA-Verbindungstrace aktiviert werden.



7.7.7.1 SCCP-Logging

Bei SCCP handelt es sich um eine “Multi-Domain-Komponente”, die das Protokoll CSTA III mit den Codierungsarten ASN.1 und XML unterstützt. Eine SCCP unterstützt immer nur eine einzelne Verbindung zu einer einzelnen Anwendung.

<SCCP>_error.log

Wenn der richtige Log-Level-Parameter gesetzt wurde, enthält die Datei “<SCCP>_error.log” Meldungen in den Codierungsarten CSTA ASN.1, CSTA XML u.a. Der Datenaustausch zwischen Applikation und SCCP sowie die Meldungen zum CAP Management (SUM, SCM, SLM) werden angezeigt.

<SCCP>_csta.log

Wenn der richtige Log-Level-Parameter gesetzt wurde, enthält die Datei “<SCCP>_csta.log” den Datenaustausch mit sämtlichen SCCs in CSTA III ASN.1. CSTA XML wird in ASCII konvertiert.

7.7.7.2 SCC-Logging

Bei SCC handelt es sich um eine “Single-Domain/Multi-Domain-Komponente”, die das Protokoll CSTA III mit den Codierungsarten ASN.1 und XML unterstützt. Je nach Betriebsart unterstützt eine SCC immer nur eine einzelne Verbindung zu einer einzelnen Anwendung oder aber mehrere gleichzeitige Verbindungen zu SCCP und TCSP.

<SCC>_error.log

Wenn der richtige Log-Level-Parameter gesetzt wurde, enthält die Datei “<SCC>_error.log” Meldungen in den Codierungsarten CSTA ASN.1, CSTA XML, NetTSPI (auf TCSP) u.a. Datenaustausch mit der Anwendung oder SCCP, zu und von der Anlage oder CA4000 sowie zu und von CAP Management (SUM, SCM, SLM) wird angezeigt.

<SCC>_csta.log

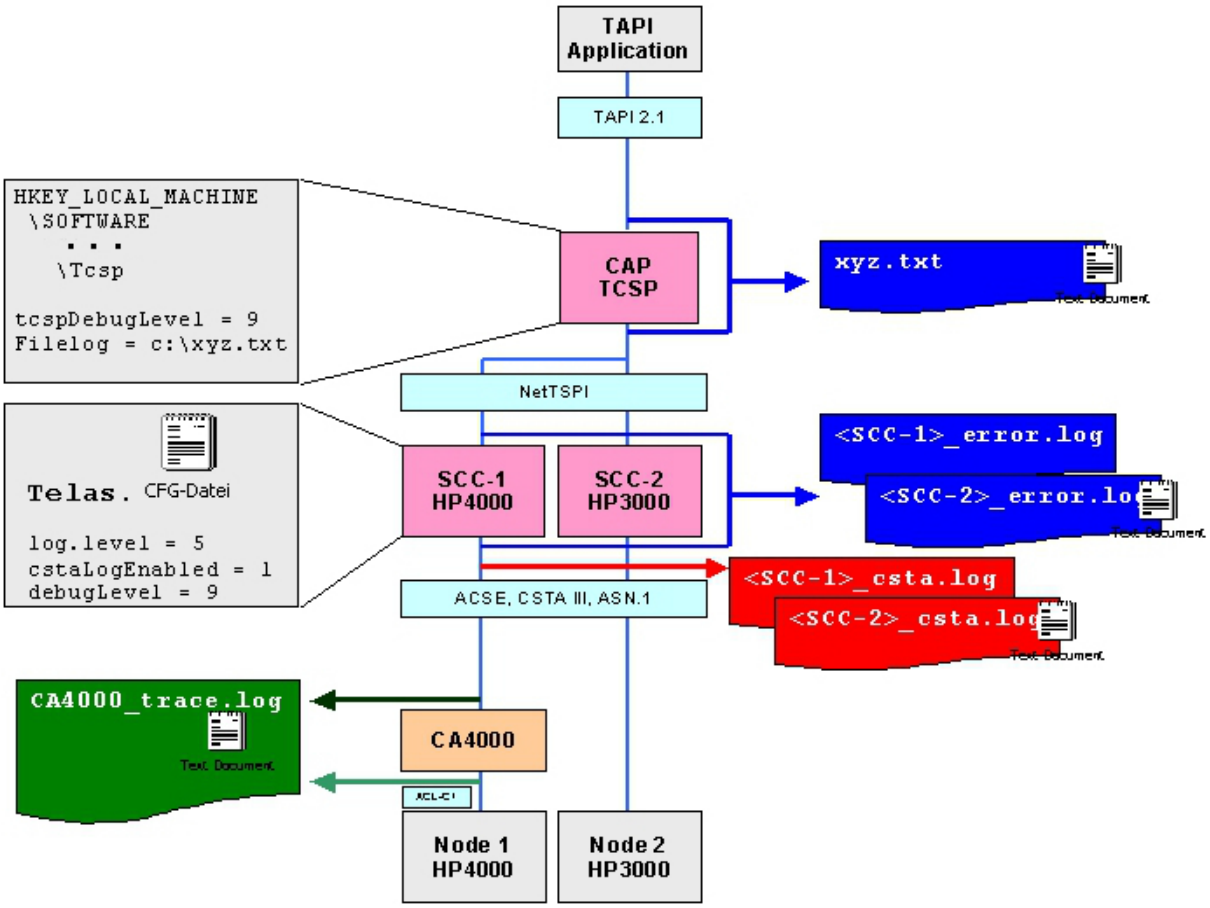
Wenn der richtige Log-Level-Parameter gesetzt wurde, enthält die Datei “<SCC>_csta.log” die Meldungen zur Anlage oder CA4000 in CSTA ASN.1.

7.7.7.3 CA4000-Logging

Der CA4000-Trace ist Bestandteil der Standard-Loggingfunktion in CAP. Die Logdatei “xxx_-CA4000_trace.log” enthält die ACL-Meldungen zur HiPath / OpenScape 4000 und die CSTA ASN.1-Meldungen zur SCC.

7.7.8 TAPI-Verbindungstrace

In Abhängigkeit von den verschiedenen Schnittstellen kann für die Kommunikation von der Anwendung zu einer Anlage ein vollständiger TAPI/CSTA-Verbindungstrace aktiviert werden.



Bei dieser Kommunikationsart wird SCCP durch CAP TCSP ersetzt. Das CAP TCSP-Log-Level und der Dateiablageort werden über die Registrierung festgelegt.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ ... \Tcsp

        tcspDebugLevel = 9
        filelog = "C:\csp_log.TXT"
```

7.7.9 Diagnose-Daten speichern

Diese Funktion ist nützlich, wenn aufgrund von Netzzugangsberechtigungen eine direkte Ferndiagnose des Systems nicht möglich ist. Es werden alle Logginginformationen, Konfigurationsdaten und sonstige für die Diagnose wichtigen Systemdaten in einem ZIP-Archiv verpackt.

1. Klicken Sie auf **Diagnose** im Hauptmenü und wählen Sie den Menüpunkt **Download Daten** im Navigationsbereich aus.
2. Sie können nun auswählen, welche Daten gespeichert werden sollen:
   - Logdateien aus allen Log-Verzeichnissen oder nur für bestimmte Rechner
   - Konfigurationsdateien
   - Zustandsinformationen der Dienste
3. Klicken Sie auf die Schaltfläche **Download**.
4. Danach erfolgt ein Standard-Windows-Dialog, in dem Sie die erzeugte Datei entweder direkt öffnen (normalerweise nicht sinnvoll) oder an einer definierten Stelle speichern können.

7.8 Hilfe

Unter diesem Menüpunkt steht Ihnen die Dokumentation zu OpenScape CAP und zu allen installierten OpenScape CTI-Komponenten zur Verfügung.

1. Wählen Sie **Hilfe** im Hauptmenü.

   Im Navigationsbereich sind alle zur Verfügung stehenden Dokumentationen aufgelistet.

2. Wählen Sie eine Dokumentation aus der Liste aus. Es wird Ihnen eine Tabelle mit den zugehörigen Dokumenten oder direkt die Information angezeigt.

Manuale stehen üblicherweise sowohl im PDF- als auch im HTML-Format in Deutsch und Englisch zur Verfügung. Release Notes werden als Textdateien nur in Englisch angeboten.

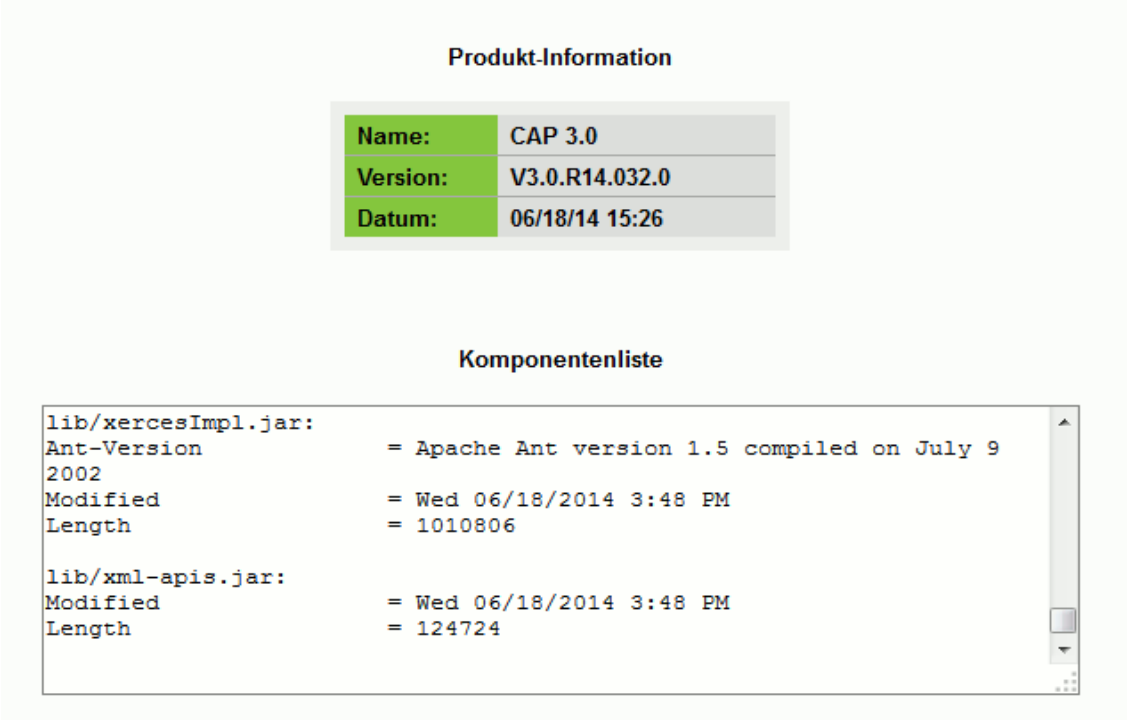
Zum Online-Zugriff empfiehlt sich die HTML-Version, zum Ausdrucken ist die PDF-Version besser geeignet.

Produktinformation

Auch die Produktinformation ist über den Menüpunkt **Hilfe** im Hauptmenü zu erreichen. Wenn Sie **Produktinformation** im Navigationsbereich wählen, erhalten Sie wichtige Produktinformationen und auch Informationen zu Lizenzbedingungen und Copyright.

Bei Störungen und Problemen kann über die Produktinformationen die Software-Version, das Erstellungsdatum usw. ermittelt werden.

Beispiel für die Produktinformation:



8 Problembehandlung

Das vorliegende Kapitel behandelt die folgenden Punkte:

- Vorgehensweisen zur Eingrenzung von Problemen,
- Schritte zur Fehlerbehandlung,
- Hinweise, wie Sie technische Hilfe bekommen.

8.1 Zuständigkeiten bei Problemen

Beim Betrieb der Hardware oder Software kann es zu Problemen kommen. Im Falle eines Problems gibt es im Wesentlichen vier Stellen, die zuständig sein können:

- der LAN-Betreiber,
- Microsoft,
- Unify oder
- der Hersteller der Anwendung.

Mit nachfolgender Tabelle können Sie ermitteln, wer im konkreten Fall zuständig ist.

Problembereich	**Beschreibung**	**Zuständigkeit**
LAN	Physikalische Verbindungen, Bridge, NIC (Network Interface Card)	LAN-Betreiber
Windows/SUSE Linux	Betriebssystem	Microsoft/Novell
PC- und Server-Hardware	Server, Clients	Kunde
OpenScape CAP	CA4000, SCCHiPath4000, SCCP, CAP TCSP, XMLPS	Unify
Anwendung	Installation, Konfiguration	Hersteller der Anwendung

8.2 Allgemeine Vorgehensweisen zur Problembestimmung

Gehen Sie zur Behebung von Problemen beim Betrieb des Systems folgendermaßen vor:

1. Reproduzieren Sie das Problem, um festzustellen, ob es weiterhin besteht. Notieren Sie sich sämtliche Symptome.
2. Vergewissern Sie sich, dass die Client-Server-Anwendung ordnungsgemäß funktioniert. Ist dies nicht der Fall, wenden Sie sich an den Hersteller der Anwendung bzw. an die für die Fehlerbehebung zuständige Stelle.
3. Befolgen Sie die Hinweise zur Problembestimmung. Gehen Sie nacheinander die vorgeschlagenen Maßnahmen durch, bis das Problem behoben ist.
4. Falls Sie das Problem nicht selbst beheben können, lesen Sie Abschnitt 8.8, “Technische Unterstützung” zu Hinweisen dazu, wie Sie technische Hilfe bekommen können.

8.3 Probleme bei der Installation

Überprüfen Sie folgende Punkte, wenn es nach der Installation Probleme gibt:

- Sind alle Installationsvoraussetzungen erfüllt?
- Ist die Netzkonfiguration des PC ordnungsgemäß durchgeführt?
- Sind Rechnername, IP-Adresse, Domain Name bekannt und korrekt konfiguriert?
- Ist der PC im DNS eingetragen und hat er einen gültigen Namen?
- Läuft der **OpenScape CTI Service** (prüfen z. B. über **Systemsteuerung | Dienste**)?
- Ist ein Web-Browser installiert und konfiguriert?
- Haben Sie Benutzer und Passwort korrekt angegeben (**`Admin, Admin`**)?
- Wurde der PC nach der Installation gebootet?

> Wenn Sie eine Veränderung an der Konfiguration vorgenommen haben, stoppen Sie den laufenden CTI Service und starten Sie ihn erneut, da einige Änderungen der Konfiguration nur nach einem Neustart des Programms wirksam werden. Weitere Probleme und Hinweise zur Behebung finden Sie im folgenden Abschnitt.

8.3.1 Allgemeine Probleme

- Haben Sie nach der Installation einen Neustart durchgeführt? Wenn nicht, tun Sie dies.
- Überprüfen Sie, ob Logging-Dateien (im Verzeichnis `logs`) Meldungen enthalten wie **`... port 8170 in use ...`**
  In diesem Fall ist der von OpenScape CAP Management benötigte Port auf dem System belegt.

  Voreingestellt ist der **Port 8170**. Der Port kann bei Bedarf umkonfiguriert werden: Durchsuchen Sie im Verzeichnis `config` alle Dateien (`*.*`) nach dem Inhalt **`8170.`** Ersetzen Sie die Portnummer **`8170`** durch eine neue Portnummer, die vom System nicht benutzt wird. Zum Editieren der Dateien können Sie jeden Text-Editor (z. B. **notepad**) nutzen.
- Führen Sie nach den Änderungen einen Neustart durch.

8.3.2 Probleme mit inkonsistenten IP-Adressen

Wenn der PC, auf dem eine OpenScape CAP-Komponente installiert ist und der CTI Service läuft, mit mehreren Netzwerkkarten ausgerüstet ist (z.B. eine für die Anbindung ins Kunden-LAN, eine für Anschluss des Vermittlungsrechners), kann es passieren, dass zur Kommunikation über LAN die falsche IP-Adresse verwendet wird. Normalerweise wird diese Frage bereits während der Installation behandelt (vgl. Abschnitt 4.9). Zur Lösung dieses Problems editieren Sie die Datei *`InstDir`*`>\config\start\startNT.cfg`, indem Sie an der folgenden Stelle die korrekte IP-Adresse zum Zugriff auf das Kunden-LAN eingeben:

```
args: -localAddr
args: <HostNameOfServer>/<IPAddrOfServer>
```

Beispiel:

```
args: -localAddr
args: PC08154711/139.21.25.245
```

> Nach dieser Änderung ist der CTI-Service anzuhalten und neu zu starten.

8.3.3 Login funktioniert nicht

Beim Anmelden mit **User Name** und **Passwort** gibt der Browser eine Fehlermeldung aus wie **`Authorization failed. Retry?.`**

- Stellen Sie sicher, dass der Service **OpenScape CTI** läuft.
- Überprüfen Sie, ob die Login-Daten korrekt angegeben wurden (Groß-/Kleinschreibung beachten).

8.3.4 Administrator-Einstiegsseite wird nicht geöffnet

In diesem Fall gibt der Browser eine Fehlermeldung aus wie
Netscape is unable to locate the server localhost:8170.
Please check the server name and try again.

- Stellen Sie sicher, dass der **Service OpenScape CTI** läuft (z. B. über **Control Panel | Services**).

8.3.5 CAP Management funktioniert nicht auf allen PCs im Intranet

OpenScape CAP Management funktioniert einwandfrei auf dem Installationsrechner. Auf einigen PCs im Intranet werden jedoch die Seiten nicht korrekt dargestellt.

1. Überprüfen Sie, ob der Name des Server-PC bekannt ist.

   Testweise kann der Proxy für diesen PC bei den Browsereinstellungen ausgeschaltet werden.

2. Wenn dieser Schritt hilft, administrieren Sie den PC im DNS.

8.3.6 CAP Management Diagnose-Applet arbeitet nicht korrekt

Nach dem Start des Diagnose-Applets (wie in Abschnitt 7.7 beschrieben) startet das Applet nicht oder bleibt mit einer Meldung wie “Wait for Diagnose Server” hängen.

Dies kann damit zusammenhängen, dass der PC des OpenScape CAP Management mit zwei Netzwerkkarten ausgerüstet ist. Falls zum Zugriff auf die OpenScape CAP Management-Bedienoberfläche die eine der beiden entsprechenden IP-Adressen, zum Start des Diagnose-Applets aber die andere IP-Adresse genutzt wird, kommt es zu einer Fehlersituation (security violation) im Java-Laufzeitsystem.

Die einzige Umgehungsmöglichkeit ist in diesem Fall die explizite Angabe von IP-Adressen:

1. Wie oben in Abschnitt 8.3.2 beschrieben, sorgen Sie für korrekte Angabe von Rechnername und IP-Adresse in der Datei `startNT.cfg`
2. Nach dem Start von OpenScape CAP Management über **Start | Programme | OpenScape CAP | Management** ersetzen Sie in der in Ihrem Browser angezeigten CAP Management-URL den symbolischen Rechnernamen durch die IP-Adresse.

Damit ist (zumindest für die laufende OpenScape CAP Management-Sitzung) die konsistente Nutzung der eingestellten IP-Adresse sichergestellt.

8.3.7 Bei jedem Browser-Neustart wird Authentifizierung gefordert

Überprüfen Sie, ob der betreffende Browser Cookies unterstützt und ob diese aktiviert sind.

8.4 Probleme mit Connectivity Adapter HiPath 4000

Bei Problemen, die sich auf Connectivity Adapter HiPath 4000 eingrenzen lassen, gehen Sie folgendermaßen vor, um den genauen Fehler in Connectivity Adapter HiPath 4000 zu ermitteln.

1. Werten Sie die Unify System- und Fehlerprotokolle aus.
2. Kontaktieren Sie die zuständige Unify-Serviceabteilung.

Unify System- und Fehlerprotokolle

Untersuchen Sie die Unify System- und Fehlerprotokolle und prüfen Sie, ob es darin Aktivitäten oder Fehlermeldungen gibt, die auf eine Fehlfunktion von Connectivity Adapter HiPath 4000 hindeuten.

8.5 Probleme in der Verbindung zur HiPath 3000

Wenn die Fehleranalyse auf Probleme in der Verbindung zur HiPath 3000-Vermittlungsanlage hindeutet, die in den bisherigen Hinweisen nicht behandelt werden, liefert der HiPath 3000-Dokumentation detailliertere Informationen.

8.6 Systemdiagnose-Funktionen

Um eine möglichst einfache und schnelle Diagnose bei Problemen durchführen zu können, bietet OpenScape CAP Management Funktionen zur Systemdiagnose. Details zur Bedienoberfläche sind in Abschnitt 7.7, “Diagnose” beschrieben.

Mit Hilfe dieser Web-basierten Bedienoberfläche ist eine Diagnose nur am Konfigurations-Server sondern auch von jedem anderen Rechner im Intranet-Rechnerverbund aus möglich.

Damit nicht jeder Benutzer sich diese Daten anzeigen lassen oder ändern kann, ist der Diagnosebereich dem Administrator vorbehalten und durch Eingabe von Administrator-Name und -Passworts geschützt.

8.6.1 Allgemeines

In diesem Kapitel werden Hinweise zur Nutzung der in Abschnitt 7.7 beschriebenen Funktionalität gegeben. Die Diagnose liefert Informationen, die nicht in allen Fällen für den Administrator gedacht sind, sondern die evtl. auch für eine Detail-Analyse an Hotline / Service / Entwicklung übermittelt werden müssen.

8.6.1.1 Diagnoseinformationen

Folgende Informationen sind für die Analyse von Problemen wichtig und hilfreich.

- **Produktinformation**

  Gibt einen Überblick über das installierte Produkt. Wichtig ist dabei die Version und der Build-Stand. Diese Daten sollten immer bei Kontaktaufnahme mit der Hotline angegeben werden.

- **Prozess-Informationen**

  Zeigt die Tabelle der zur Zeit gestarteten Prozesse. Wichtig ist, dass der Status aller angezeigten Prozesse in Ordnung ist. Hier kann der Administrator einen ersten Überblick über Probleme erhalten.

- **Service-Informationen**

  Genaue Information über die im System gestarteten Services und ihren Status erhält man in dieser Tabelle. Auch hier zeigt der Status evtl. ein potentielles Problem. Weiterhin wird die Prozess-/Service-Zuordnung angezeigt.

- **Konfigurationsinformation**

  Die in Anhang A.2, “Beschreibung der Konfigurations-Dateien” beschriebenen Konfigurationsdateien können eingesehen, analysiert und geändert werden. Nach Änderung von Konfigurationsdateien müssen die zugehörigen Komponenten (ggf. auch das Gesamtsystem) gestoppt und neu gestartet werden.

- **Logging-Informationen**

  Während des Betriebs werden laufend Logging-Informationen in Dateien geschrieben. Alle Logging-Dateien sind im Verzeichnis `<InstDir>\Logs` abgelegt.

  Eine besondere Rolle spielt die Datei **`errors.log`**. In dieser Datei werden von allen Services Fehler abgelegt und mit der Kennzeichnung des Services versehen. Es ist sinnvoll, diese Datei regelmäßig zu überprüfen und wenn nötig zurückzusetzen, damit im Fehlerfall auftretende Probleme schneller erkannt werden können.

  Zur genauen Analyse eines konkreten, reproduzierbaren Problems sollte zunächst die Logging-Historie gelöscht (**Logging zurücksetzen**) und dann der Fehler erneut provoziert werden. Dadurch wird veraltete Logging-Information entfernt und der Umfang der zu analysierenden Logging-Daten reduziert.

  Bei Neustart des Systems werden entsprechend der Logging-Konfiguration eventuell vorhandene Logging-Dateien auf `<name>_last.log` umbenannt, damit die enthaltene Information nicht verloren geht.

Abhängig vom eingestellten Log-Level werden mehr oder weniger Informationen gespeichert. Log-Levels für aktive Prozesse werden über **Zeige Logging** angezeigt. Sollte ein Problem bei einem dieser Prozesse erkannt worden sein, so kann gezielt dessen Level hochgesetzt werden, um genauere Informationen zu bekommen.

- **Speichern von Diagnoseinformationen**

  Eine nützliche Funktion, alle Diagnoseinformationen zusammenzufassen und in einer Datei zur Analyse und Weitergabe zu speichern, ist mit **Daten speichern** möglich. Die Daten werden in ein Zip-Archiv verpackt und können per Download von der Entwicklung oder Hotline geholt werden.

8.6.1.2 Start / Neustart

Bei Änderungen der Systemkonfiguration (Editieren von Konfigurationsdateien) oder auch bei Laufzeitproblemen von Prozessen/Services des OpenScape CTI-Systems muss ein Neustart der betroffenen Komponenten durchgeführt werden. Über die Diagnose-Oberfläche von OpenScape CAP Management (Abschnitt 7.7) ist dies von jedem PC mit Zugang zum Netz möglich, auch bei einer verteilten Installation des OpenScape CTI-Systems.

In vielen Fällen ist es nicht erforderlich das komplette System neu zu starten. Stoppen und Neustart einzelner betroffener Prozesse könnte ausreichen. Nutzen Sie zu diesem Zweck ebenfalls die Diagnose-Oberfläche; dabei können Sie gleichzeitig den Status der beteiligten Prozesse überwachen.

8.6.2 Diagnose von Laufzeitproblemen

Anhand dieses Beispiels soll gezeigt werden, wie der Administrator einen Service analysiert, dessen Status auf *not running* (Rote Lampe an) steht.

Zunächst kann über das Register **Services** der Status aller Services angezeigt werden.

Angenommen der Service **Phone** im Prozess **PhoneController** zeigt Status **not running***:*

- Wechseln Sie in das Register **Logging**. Falls es noch nicht angezeigt wird, muss es über das Menü **Debug | Logging anzeigen** aktiviert werden.
- In der erscheinenden Liste wird u. a. der Logger **Phone** mit dem eingestellten Trace-Level angezeigt. Nach Auswahl der Zeile kann, wenn erforderlich, der Level erhöht werden.
- Um die zugehörige Loggin-Information zu erhalten, muss bei ausgewählter Zeile über Kontext-Menü (rechte Maustaste) **Zeige Loggingdateien** ausgewählt werden. Durch Doppelklick wird der Inhalt der gesuchten Logging-Datei angezeigt.
- Falls auch Konfigurationsdaten erforderlich sind, wählen Sie **Zeige Konfigurationsdateien** aus dem gleichen Kontextmenü.

8.6.3 Diagnose von Hochlaufproblemen

Im Normalfall werden die zum OpenScape CTI-System gehörenden Services von einem zentralen Service, dem Start-Service, der Reihe nach gestartet. Im Windows-Betriebssystem ist dieser als Service **OpenScape CTI** sichtbar.

Zur Analyse von Hochlaufproblemen werden beim normalen Start Logging-Informationen erzeugt. Falls diese Logging-Informationen nicht ausreichen um das Problem zu lokalisieren, ist es möglich, die Services des Systems einzeln zu starten.

Dazu werden im Verzeichnis `<InstDir>\bin\tools` Stapel-Dateien bereitgestellt.

1. **`startNT.bat`**

   Startdatei für den OpenScape CAP Service Starter (OpenScape CTI)

2. **`admin_ctrl.bat`**

   Startdatei für die Administrationsfunktionen (AdminServiceController)

3. **`diag_ctrl.bat`**

   Startdatei für die Diagnosefunktionen (DiagnoseController)

4. **`phone_ctrl.bat`**

   Falls ComAssistant installiert ist, ist dies die Startdatei für Telefoniefunktionen (PhoneController)

5. **`jaccess_ctrl.bat`**

   Falls ComAssistant installiert ist, ist dies die Startdatei für Journal-Funktionen (JournalAccessController)

Um einen Fehler einzukreisen gehen Sie wie folgt vor:

- Öffnen Sie ein Shellfenster und rufen Sie `startNT.bat` auf.
  Dies entspricht dem Start des Service **OpenScape CTI**. Allerdings mit dem Vorteil, dass alle Fehler beim Versuch die restlichen Services zu starten auf **standard error** geschrieben werden. Lenken Sie diese Ausgabe am besten in eine Datei.

  z.B.: `startNT 2>startNT.txt`

  Jetzt startet das komplette System, und Hochlaufprobleme werden in `start.txt` protokolliert.

Stellt sich dabei heraus, dass nur einer der oben genannten Prozesse Probleme macht, so sollten Sie diesen aus dem automatischen Hochlauf herausnehmen; dies ist wie folgt möglich:

- Im Installationsverzeichnis `<InstDir>\config\<HostName>\<ProcessName>`, das dem Prozess <ProcessName> auf dem PC <HostName> zugeordnet wird, findet sich eine Datei `S<xx>service_ctrl.proc` (<xx> steht für eine Nummer, die pro Prozess unterschiedlich sein kann).
- Deaktivieren Sie diese Datei durch Umbenennen der Extension `.proc`.
- Starten Sie über `startNT.bat` oder den NT-Service das System.
  Dabei wird alles gestartet außer dem Prozess, dessen Startdatei umbenannt wurde.
- Öffnen Sie ein Shellfenster für den Start dieses Prozesses über das zugehörige .bat file.
- Lenken Sie dazu wieder **standard error** in eine Datei um.

  z. B. `admin_ctlr 2>adminStart.txt`

Analog kann mit den anderen Prozessen verfahren werden. Da die Services während des Betriebs miteinander kommunizieren, werden laufend weitere Meldungen in den zugehörigen Shell-Fenstern ausgegeben, die analysiert werden können. Meistens kann jedoch bereits beim Start eines der Services ein Problem erkannt werden.

7	Denken Sie bitte daran, die deaktivierten Prozess-Startdateien wieder zu aktivieren (`Extension.proc` wieder herstellen), sobald das Problem behoben ist.

8.7 Spezielle Diagnose-Informationen

Dieses Kapitel beschreibt welche Konfigurationseinstellungen in der CAP nötig sind, um im Fehlerfall ausreichend Diagnose-Informationen zu erhalten.

Es gibt zum einen Einstellungen die vorgenommen werden müssen bevor das gesamte System gestartet wird und zum anderen spezifische Einstellungen zu spezifischen Problemen.

8.7.1 Allgemeine Einstellungen

Im Fehlerfall ist immer die Datei **sysdiag.zip** bereitzustellen, welche die Konfigurations-Einstellungen und die CAP-Protokolle beinhaltet!

8.7.1.1 Standard-Protokollierung

Die Standard-Protokollierung soll eingeschaltet sein für alle

- SCC (3000,4000,8000,DX,etc..) und
- SCCP

LogLevel Einstellungen

Bitte editieren sie die Datei

<installdir>\OpenScapeCTI\config\<Server Name>\sccp_<SCCP Id>**Telas.cfg** !

Die folgenden Parameter und Werte sollen eingestellt sein:

log.level = 5

debugLevel = 9

cstaLogEnabled = 1

Für CA4000 editieren sie bitte die Datei:

<installdir>\OpenScapeCTI\config\<Server Name>\ca4000_<ca4000 Id>**ca4000.cfg**

log.level = 4

Für SAT editieren sie bitte die Datei:

<installdir>\OpenScapeCTI\config\<Server Name>\sat\sat_svc**SatServer.cfg**

LOG_LEVEL = 5

Für SPI editieren sie bitte die Datei:

<installDir>\OpenScapeCTI\config\<Server Name>\spi**Telas.cfg**

log.level = 5

debugLevel = 9

traceLevel = 5

8.7.1.2 Setup DrWatson

Das Programm *DrWatson* soll am CAP-Server installiert und aktiviert sein, Dieses Werkzeug generiert Diagnose-Informationen für den Fall, dass es in einer CAP-Komponente zu einem Programmabsturz kommt.

DrWatson aktivieren:

Benutzen sie den Kommandozeilen-Modus und geben sie den Befehl „drwtsn32 -I“ ein.

Sie werden nachfolgende Meldung erhalten:

Um zu prüfen, ob die DrWatson-Installation erfolgreich war, benutzen sie den Kommando-zeilen-Modus und geben sie den Befehl „regedit“ ein.

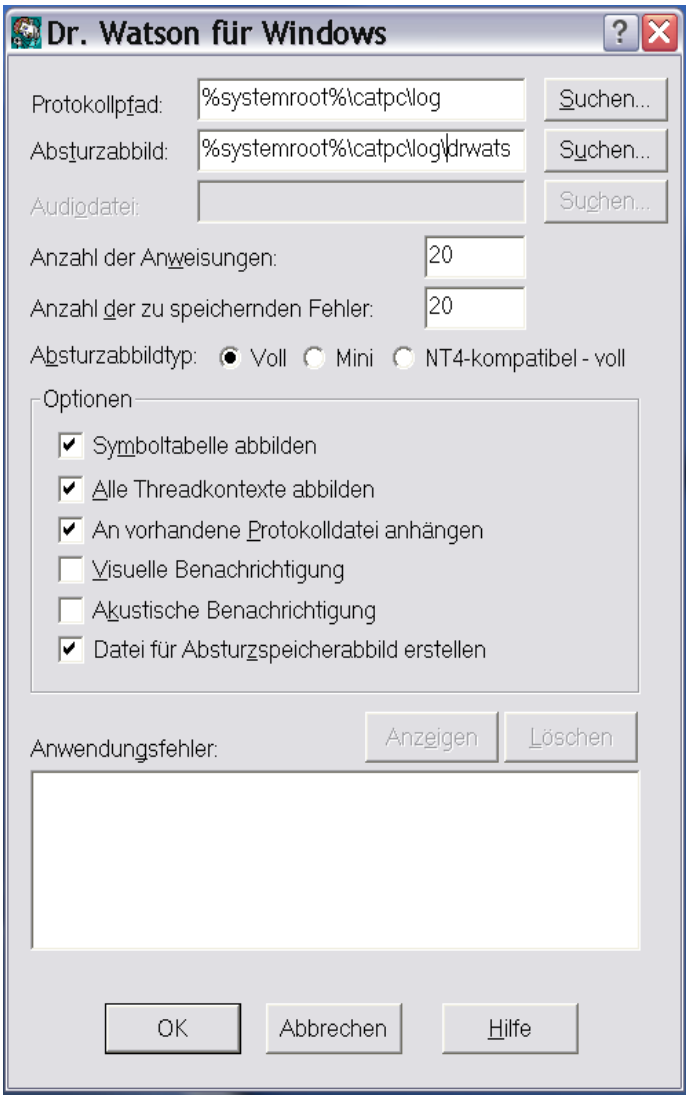
In Verzeichnis:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug

Der Paremeter ***Debugger*** soll den Wert *drwtsn32 -p %ld -e %ld -g* haben

Einstellen der Optionen für den DrWatson:

Benutzen sie den Kommandozeilen-Modus und geben sie den Befehl „drwtsn32“ ein. Stellen sie folgende Optionen ein.



Der Name des Protokolls ist ***drwtsn32.log*** und wird im angegebenen Verzeichnis (Protokollpfad) erstellt. Der Name und das Verzeichnis des Absturz-Protokolls (Absturzabbild) kann editiert werden.

Wenn ein Programmabsturz einer CAP-Komponente eintritt, dann sichern sie so schnell wie möglich:

- sysdiag.zip (Protokolle der CAP-Komponenten)
- drwtsn32.log (DrWatson-Protokoll) und Absturzabbild
- Windows Ereignisprotokoll

8.7.2 Fehler-spezifische Protokoll-Einstellungen

8.7.2.1 Absturz-Situationen

Im Falle eines Programm-Absturzes einer SCC oder SCCP-Komponente ist es hilfreich eine zusätzliche Trace-Datei zu haben. Dieses kann folgendermassen aktiviert werden:

- Stoppen des SCCP in der Prozess-Tabelle des Diagnose-Agent
- Im Verzeichnis

  <installdir>\OpenScapeCTI\config\<Server Name>\telasServer_<SCC or SCCP Id>

  kopieren sie folgende Zeilen in die Datei ***S10service_ctrl.proc***:

  args: -l

  args: 6

  args: -f

  args: <?x $INST ?>/logs/<SCC or SCCP Id>**Trace.txt**

  Der Name der Txt-Datei kann z.B. lauten:

  args: <?x $INST ?>/logs/SCC4000Trace.txt
- Starten des SCCP in der Prozess-Tabelle des Diagnose-Agent

8.7.2.2 Performance-Probleme

Es ist möglich, dass es zu Performance-Problemen kommen kann, insbesondere wenn nachfolgende Symptome im System auftreten:

- es treten Zeitverzögerungen im Message-Prozessing der CAP auf
- eine CAP-Komponente nutzt für mehr als 1-2 Sekunden 100% CPU
- der Speicherverbrauch einer Komponente steigt stetig (ohne Ende)

In diesem Fall sind für die weitere Analyse Performance-Protokolle nötig. Es dazu mehr und längere CAP-Protokolle und Performance-Monitor-Protokolle erforderlich.

Für mehr und längere CAP-Protokolle editieren sie bitte:

<installdir>\OpenScapeCTI\config\<Server Name>\admin\log**LogServer.cfg**

Hier sind die Einträge, die geändert werden sollen (für alle betroffenen SCCP):

log.maxLines.<SCCP Id>_Error = 500000 (max. Größe der Protokolle in Zeilen)

log.maxFiles.<SCCP Id>_Error = 20 (max. Anzahl der Protokolle)

log.maxLines.<SCC4000 Id>_Error = 500000

log.maxFiles.<SCC4000 Id>_Error = 20

z.B.:

log.maxLines.SCCP_Error = 500000

log.maxFiles.SCCP_Error = 20

log.maxLines.HP4000_Error = 500000

log.maxFiles.HP4000_Error = 20

Um Performance-Monitor-Protokolle zu erhalten, starten sie bitte den Performance-Monitor!

(perfmon.exe)

Wählen und markieren sie "Leistungsindikatorenprotokolle", dann durch Drücken der rechten Maustaste im Pulldown-Menü "Neue Protokolleinstellungen..."

Geben sie einen Namen für das Protokoll ein und fügen sie die Leistungsindikatoren für alle betroffenen SCCP-Prozesse hinzu:

– Datenobjekt *Process*, Instanz *SCCP*, Leistungsindikator *%Processor Time* und Hinzufügen wählen

– Datenobjekt *Process*, Instanz *SCCP*, Leistungsindikator *Private Bytes* und Hinzufügen wählen

Fügen sie auch den Leistungsindiaktor für die allgemeine Prozessor-Zeit hinzu:

– Datenobjekt *Processor*, Instanz *_Total*, Leistungsindikator *%Processor Time* und Hinzufügen wählen

Setzen sie das Intervall auf 1 Sekunde.

Wählen sie bei der Protokolldatei den Dateityp "Textdatei (Komma getrennt)" und als Dateierweiterung "mmddhhmm"

Legen sie schliesslich den Zeitplan für die Messung so fest, dass diese manuell gestartet und gestoppt wird.

Durch Drücken der rechten Maustaste können sie im Pulldown-Menü die Messung starten und stoppen. Das Protokoll wird im angegebenen Verzeichnis generiert.

8.7.2.3 Probleme mit dem SPI Service

Falls sie Probleme mit dem Service für die PBX Informations-Komponente wahrnehmen, dann passen sie folgende Einstellungen an.

Für den Fall dass viele Endgeräte im jeweiligen Switch konfiguriert sind, dann soll, für die Abfragen über alle Endgeräte von den Switchen, der Wert für für den Timeout angepasst werden.

In der Konfigurations-Datei <installPfad>\OpenScapeCTI\config\<Server name>\admin\mgmnt**admin.cfg**

SysMgmtTimeout = 600000

Wenn sie weiterhin Probleme wahrnehmen, dann aktivieren sie biite das SPI-Tracing

XML-Trace für SPI Service

SPI.traceDir = <?x $INST_DIR ?>/logs

SPI.traceHeader = true

Diese Änderungen machen einen Restart des CAP-Service notwendig.

Die zusätzlichen SPI-Traces werden in den folgenden Dateien abgelegt:

<intsallPfad>\OpenScapeCTI\logs\SPITraceFile.txt

<intsallPfad>\OpenScapeCTI\logs\SPI_XML.trc

8.8 Technische Unterstützung

Falls Sie Probleme beim Betrieb des Systems nicht selbst beheben können, wenden Sie sich an folgende Stellen:

- Bei Problemen mit dem Anwendungsprogramm auf dem Computersystem wenden Sie sich an den Hersteller der Anwendung.
- Bei Problemen mit dem Kommunikationsserver oder der Server-Software wenden Sie sich an die zuständige Unify-Serviceabteilung.
- Bei Problemen mit dem CTI-Server wenden Sie sich an den Anbieter Ihrer CSTA-Anwendung.

9 Betriebsarten

Die OpenScape CAP unterstützt zwei unterschiedliche Betriebsarten. Je nach Betriebsart werden unterschiedliche TK-Anlagen, Protokolle und Kodierungsvarianten unterstützt.

Single Domain Native Mode

HiPath / OpenScape 4000, nur CSTA III ASN.1

Multi Domain Harmonized Mode

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

> Bitte beachten Sie dass die Bereitstellung der unterschiedlichen Betriebsarten für verschiedene TK-Anlagen erfolgreiche Tests sowie eine spezifische Freigabe für die jeweilige CAP-Version erfordert.
> Definitive Aussagen über die unterstützten Betriebsarten erhalten Sie jeweils über die für eine Versionsfreigabe erstellten ReleaseNotes.

9.1 Single Domain Native Mode

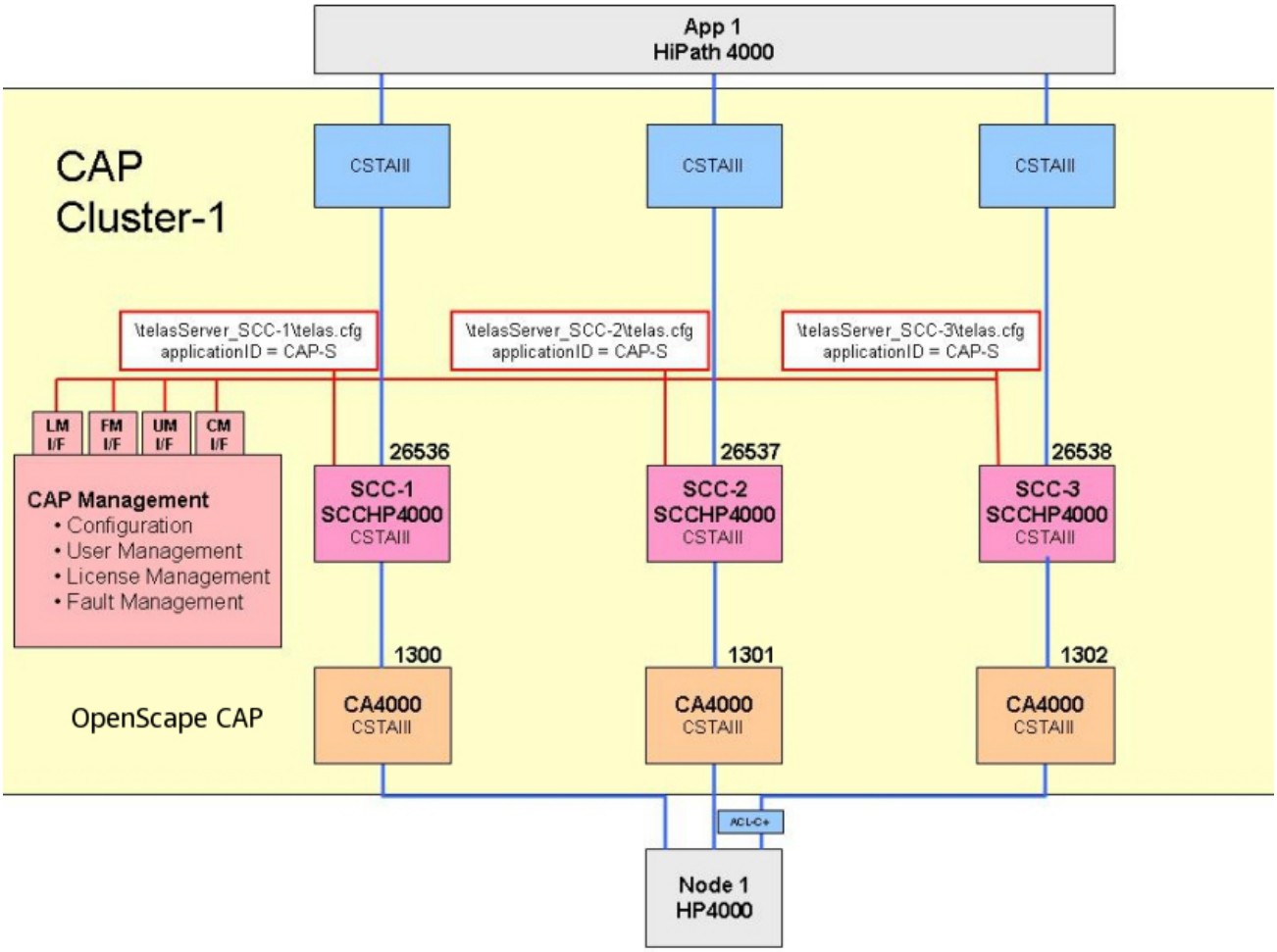
Im "Single Domain Native Mode" wird eine Applikation über eine CAP mit einer TK-Anlage verbunden. Proprietäre Protokollelemente, Private Services und ein erweiterter Leistungsumfang werden unterstützt. Die Anzahl der dabei genutzten SCC ist unerheblich. Aber die gesetzte **ApplicationID** aller SCC muss identisch sein.

Der Single Domain Native Mode wird zur CTI-Unterstützung für bereits entwickelte CSTA Applikationen bereitgestellt. Dabei ist nicht erforderlich, Softwareänderungen in der Applikation vorzunehmen. Der Applikation ist das Vorhandensein eines SCC nicht bekannt.

9.1.1 Installationsbeispiele

Der zum Anschluss der HiPath / OpenScape 4000 in der CAP einzurichtende SCC wird dabei fest für ein definiertes Protokoll konfiguriert.

Eine andere Installationsvariante ist die Verbindung einer Applikation mit einer TK-Anlage über mehrere Links zur Lastverteilung. Bei dem folgenden Beispiel werden konkrete Werte (TK- Anlage, Protokolle und Portnummern) eingesetzt.



9.1.2 HiPath4000 SCC Konfiguration im Single Domain Native Mode

Die HiPath 4000 unterstützt das proprietäre Protokoll ACL-C+ und benötigt zwingend den Protokoll-Konverter CA4000. Dieser unterstützt das CSTA III ASN.1 kodierte Protokoll (nach ECMA 285), auch mit zusätzlicher Kennzeichnung per ACSE. **(CSTA phase I ist nicht mehr unterschtützt.)**

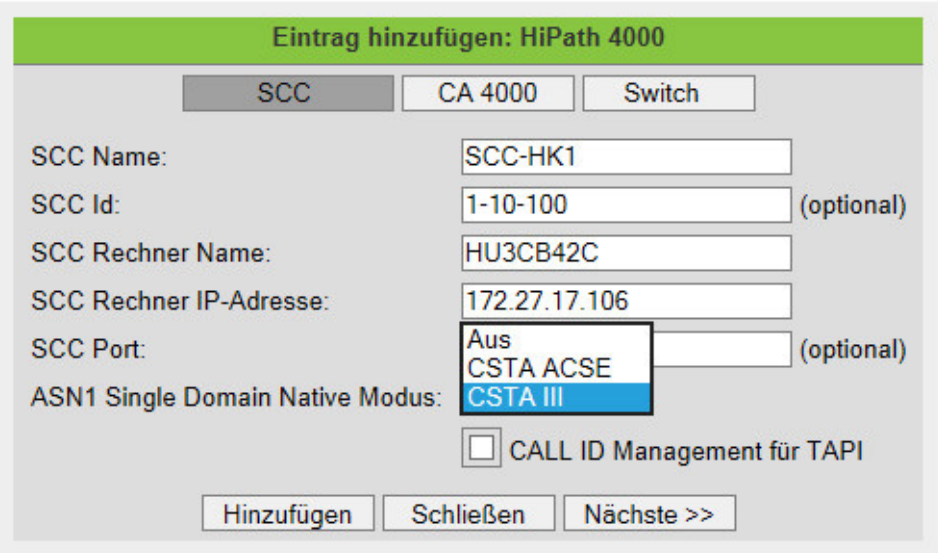
Einige Protokollelemente des ACL-C+ werden nicht verwendet.

Fügen Sie über den Menüpunkt **Service | Switch Verbindung** einen "SCCHiPath4000" hinzu.

Der "ASN.1 Single Domain Native Mode" wird geändert auf:

- **CSTA ACSE**, der entsprechende Port des CA4000 wird ebenfalls im "CSTA ACSE" Mode konfiguriert!
- **CSTA III,** der entsprechende Port des CA4000 wird ebenfalls im "CSTA III" Mode konfiguriert!

Diese Konfiguration ist immer abhängig von der aufsetzenden Applikation.



9.1.2.1 CTI-Benutzer im Single Domain Native Mode

Unter der Benutzerverwaltung müssen alle CTI-Benutzer mit einem zugeordneten Device eingerichtet werden.

9.1.2.2 Lizenzierung im Single Domain Native Mode

Die Zuordnung, welche Lizenz eine CTI -Benutzer zugeteilt sein muss, erflogt durch die Konfiguration der Parameters "ApplicationID = ???" in der Konfigurationsdatei `telas.cfg` des SCC.

Bei dem ersten CSTA-Request kontaktiert der SCC das CAP Lizenzmanagement und stellt die Anfrage, ob die in der Datei `telas.cfg` vergebene "ApplicationID" als Lizenz dem CTI-Benutzer zugeteilt ist. Ist die Lizenzvergabe im Modus "Bei der Benutzeranmeldung (Default) aktiv, so wird immer eine Lizenz zugeteilt. Wurde für einen Benutzer eine Lizenz erfolgreich überprüft, so speichert der SCC diese Information 3600 Sekunden. Bei einen SCC Neustart werden diese Informationen ebenfalls gelöscht.

9.1.3 Test der HiPath / OpenScape 4000 "Single Domain Native Mode" für die Konfiguration CSTA III

CSTA Testprogramm für CSTA III

Um diese Konfiguration zu testen, wird das Programm `CSTA3Host.exe` verwendet. Konfiguriert wird als Ziel der Verbindung die CAP Call Control IP-Adresse und der CAP Control Port.

SCC Status

Der Status des SCC ist ohne Applikationsverbindung "**nicht bereit**".

Applikationsanmeldung (ACSE_AARQ)

Wird nicht verwendet.

Applikations-ID

Die Applikations-ID wird in der SCC Konfigurationsdatei `telas.cfg` durch den Parameter "ApplicationID" definiert.

Native Mode = True/False

Eine explizite Kennzeichnung des Native Mode ist nicht erforderlich, da dieser direkt für jeden SCC konfiguriert wird.

Nebenstellen

Nebenstellen werden durch ihre kurze Nebenstellennummer in jedem Request adressiert.

Call ID

Die "Call ID" is 2 Byte lang.

9.1.4 Test der HiPath / OpenScape 4000 "Single Domain Native Mode" für die Konfiguration ACSE

CSTA Testprogramm

Um diese Konfiguration zu testen, wird das Programm `CSTA3Host.exe` verwendet. Konfiguriert wird als Ziel der Verbindung die CAP Call Control IP-Adresse und der CAP Control Port.

SCC Status

Der Status des SCC ist ohne Applikationsverbindung "**nicht bereit**".

Applikationsanmeldung (ACSE_AARQ)

Es erfolgt die Kennzeichnung der CSTA Version (version five).

Applikations-ID

Die Applikations-ID wird in der SCC Konfigurationsdatei `telas.cfg` durch den Parameter "ApplicationID" definiert.

Native Mode = True/False

Eine explizite Kennzeichnung des Native Mode ist nicht erforderlich, da dieser direkt für jeden SCC konfiguriert wird.

Nebenstellen

Nebenstellen werden durch ihre kurze Nebenstellennummer in jedem Request adressiert.

Call ID

Die "Call ID" is 2 Byte lang.

9.2 Multi Domain Harmonized Mode

Im “Multi Domain Harmonized Mode” werden ein oder mehrere Applikation/en über eine CAP mit einer oder mehreren TK-Anlage/n gleichen oder unterschiedlichen Typs verbunden. Standard CSTA Services werden unterstützt, proprietäre Protokollelemente und Private Services werden nicht unterstützt! Somit ist eine Applikation unabhängig von der darunter liegenden Infrastruktur. Die Anzahl der dabei genutzten SCC/SCCP ist unerheblich. Jede aufsetzende Applikation verwendet eine individuelle ApplikationsID, welche durch den ACSE_AARQ übermittelt wird.

Im "Harmonized Mode" werden folgende die Protokolle und Kodierungsvarianten unterstützt:

- CSTA III ASN.1
- CSTA XML
- TAPI 2.1/3.1
- JTAPI

HINWEIS ZUR UNTERSCHEIDUNG "HARMONIZED MODE" / "NATIVE MODE"

Der "Harmonized Mode" unterscheidet sich vom "Native Mode" ausschließlich durch die Kennzeichnung "Native = false" (Default) im ACSE_AARQ!

HINWEIS ZUR VERBINDUNG EINER APPLIKATION MIT DER CAP

Eine Applikation wird immer nur mit einem SCCP verbunden.

HINWEIS ZUR KONFIGURATION EINES SCC IM "MULTI DOMAIN HARMONIZED MODE"

Der "Multi Domain Harmonized Mode" eines SCC wird durch den Konfigurationspunkt: "ASN.1 Single Domain Native Mode = Aus" aktiviert.

HINWEIS ZUR "APPLICATION ID" IN DER SCC KONFIGURATIONSDATEI "TELAS.CFG"

Der Parameter "ApplicationID" in der SCC Konfigurationsdatei "telas.cfg" ist im "Multi Domain Harmonized Mode" automatisch deaktiv.

Der Multi Domain Harmonized Mode wird zur CTI-Unterstützung für neue CSTA Applikationen bereitgestellt, die das Leistungsmerkmal "Multi Domain" der CAP nutzen möchten, Standard CSTA Services benötigen und TK-Anlagen unabhängig sein möchte.

9.2.1 Protokollanforderungen an eine Applikation

Für Applikationen gilt für den "Multi Domain Harmonized Mode":

1. Anmeldung über ACSE

   Der ACSE_AARQ muss folgenden Informationen enthalten:

   – Benutzername (CAP CTI- oder CAP Admin-Benutzer)

   – Passwort (des CAP CTI- oder CAP Admin-Benutzers)

   – ApplicationID (wird zur Lizenzierung benötigt)

   – CSTA Version (version five, version six)

   – Native = False (default)

2. Nebenstellen im langen kanonischen Format

   Die Nebenstellennummer müssen für bestimmte Requests (wie z.B.: MakeCall, SnapshotDevice, MonitorStart) im langen kanonischen Format (z.B.: +49(5251)8-27486) übermittelt werden. Diese Format ist für die korrekte Lizenzierung und die Weiterleitung eines Requests von einem SCCP an einen SCC notwendig.

3. Die CallID ist maximal 9Byte lang.

9.2.2 Authentifizierung und Lizenzierung

Applikations-Authentifizierung

Eine Applikation muss nach dem Verbindungsaufbau mit einem SCCP immer einen ACSE_AARQ schicken. Der in diesem Request enthaltene Benutzer/Passwort (z.B.: CAP/123) muss mit einem CAP CTI- oder CAP Admin Benutzer übereinstimmen. Ein entsprechender http-Request (`http://<fqdn>:8170/mgmnt/auth/req?authenticate=<User ID>&passwd=<Password>&encoding=b64`) wird vom SCCP an das CAP Benutzermanagement gestellt. Wird der Benutzer erfolgreich authentifiziert, wird die TCP/IP Verbindung zur Applikation gehalten. Ist die Authentifizierung nicht erfolgreich, so wird die TCP/IP Verbindung zur Applikation unterbrochen. Die im ACSE_AARQ enthaltene “ApplicationID” muss hier gültig sein! Für eine erfolgreiche Authentifizierung muss die entsprechende Lizenz in der CAP installiert sein.

CTI Client-Lizenzierung

Die im ACSE_AARQ übermittelte “ApplicationID” wird vom SCCP gespeichert und für eine spätere CTI Client Lizenzierung (anhand der Rufnummer im kanonischen Format) von CSTA Request verwendet. Ein entsprechender http-Request (`http://<fqdn>:8170/mgmnt/admin/req?registerLicense= <ApplicationID>&userId=<DeviceID>`) wird vom SCCP an das CAP Lizenzmanagement gestellt. Ist eine Lizenzüberprüfung erfolgreich gewesen so speichert der SCCP diese Information für 3600 Sekunden.

9.2.3 Test der CAP "Multi Domain Harmonized Mode" für die Konfiguration CSTA III ASN.1

CSTA III ASN.1 Testprogramm

Um die Konfiguration für die CSTA III ASN.1 zu testen, wird das Programm `CAPHost.exe` verwendet.

Konfiguriert wird als Ziel der Verbindung die CAP SCCP IP-Adresse und der CAP SCCP Port.

Im ACSE_AARQ wird die Kennzeichnung "Native = false" übermittelt und entfällt, da der Default "Native = false" ist. Nur im "Harmonized Mode" können während einer Verbindungssession unterschiedliche TK-Anlagen Typen getestet werden.

SCCP Status

Der Status des SCCP ist ohne Applikationsverbindung "läuft".

SCC Status

Der Status des SCC ist ohne Applikationsverbindung "läuft".

Applikationsanmeldung (ACSE_AARQ)

Eine Applikation muss sich mit einem CAP CTI- oder Admin-Benutzer (z.B.: CAP) und dem zugehörigen Passwort (z.B.: 123) authentifizieren. Diese Authentifizierung wird über den SCCP von dem CAP Management durchgeführt. Zusätzlich erfolgt die Kennzeichnung der CSTA Version (version five).

Applikations-ID

Die Applikations-ID wird im ACSE_AARQ übergeben

Native Mode = True/False

Eine explizite Kennzeichnung des Native Mode ist nicht erforderlich, “Native = false” (default).

Nebenstellen

Nebenstellen werden durch ihre lange Rufnummer adressiert., wenn keine der entsprechende Request keine weitere Referenz-ID enthält (z.B.: CallID)

Call ID

Die "Call ID" ist maximal 8 Byte lang.

9.2.4 JTAPI

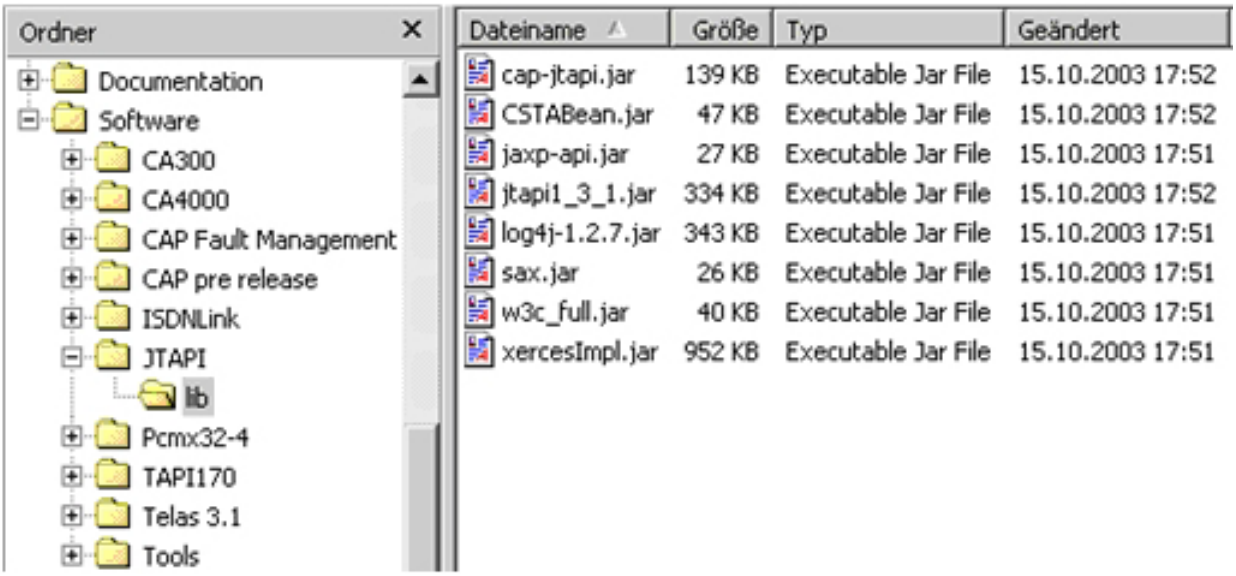
Das Protokoll JTAPI wird nur im "Multi Domain Harmonized Mode" unterstützt.

Die OpenScape CAP V3.0 stellt dazu entsprechende Java Klassen zur Verfügung.

Der Vorteil von JATPI ist die Betriebssystem-Unabhängigkeit.

Die Kommunikation mit einem SCCP erfolgt durch CSTA XML.

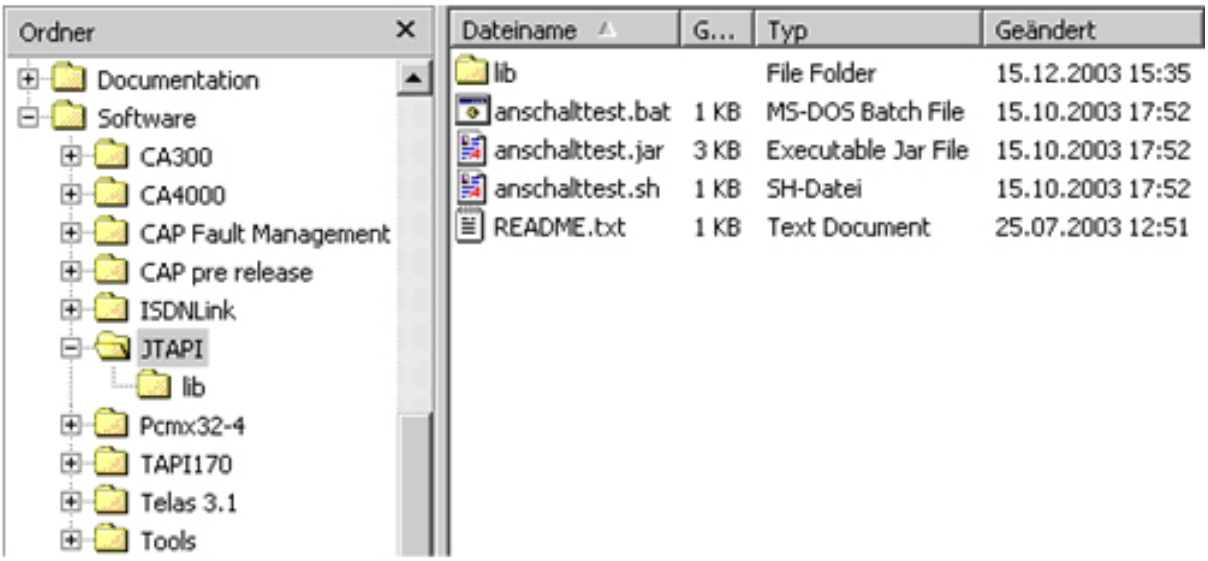
Auf der OpenScape CAP V3.0 CD befinden sich die Java-Klassen im Verzeichnis: “Software\JTAPI\lib”



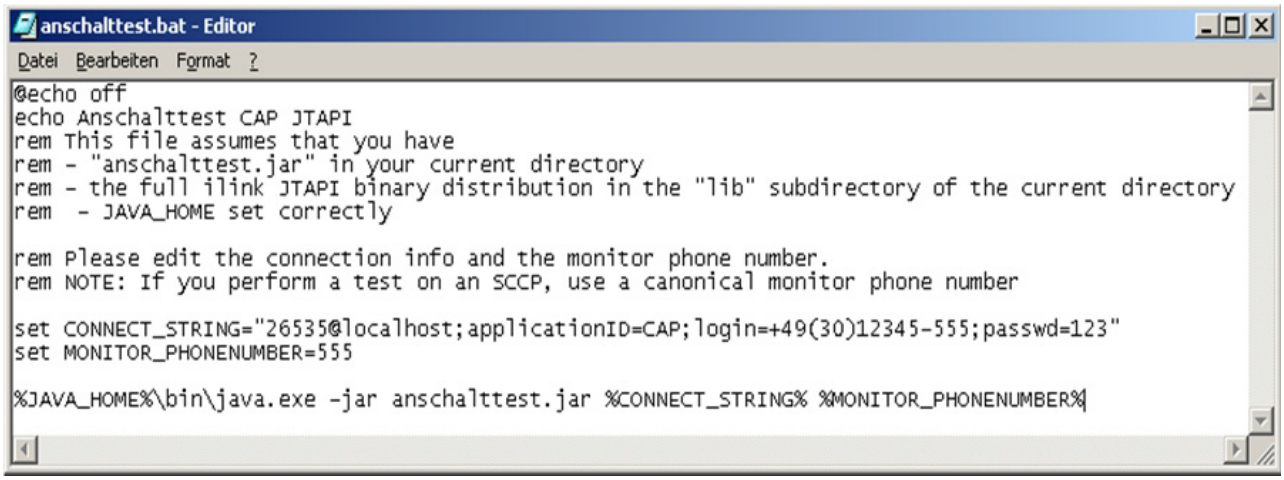
9.2.4.1 JTAPI Test

Um JTAPI testen zu können, bedarf es der Installation des "Java Runtime Environments 1.3.1" oder höher.

Auf der OpenScape CAP V3.0 CD befindet sich im Verzeichnis “Software\JTAPI” das Testprogramm “anschalttest.bat”.



Der Inhalt der Datei muss der Installation entsprechend angepasst werden.



`26535@localhost`

Eingabe der Portnummer und IP-Adresse (oder PC Name) des Rechners, auf dem der SCCP läuft.

`applicationID=CAP`

Eingabe der "ApplicationID". Sie muss einer installierten Lizenz entsprechen

`login=+49(30)12345-555`

Eingabe des CAP CTI- oder Admin-Benutzers zur Applikations-Authentifizierung.
`MONITOR_PHONENUMBER=555`

Eingabe der Rufnummer (z.B.: 27486) zur Überprüfung des Leistungsmerkmals “MonitorStart” am SCC.
Eingabe der Rufnummer im kanonischen Format (z.B.: +49(5251)2421-27486) zur Überprüfung des Leistungsmerkmals “MonitorStart” am SCCP.

`%JAVA_HOME%`

Die Variable, welche auf das Java Installationsverzeichnis gesetzt ist. Ist diese Variable nicht gesetzt, so muss diese Variable ersetzt werden (z.B.: C:\Programme\Java\j2re1.4.2_06\).

Start der Stapeldatei `anschalttest.bat`

1. Kopieren Sie das “\Software\JTAPI” Verzeichnis, welches die CAP Java Klassen enthält, in ein beliebiges Verzeichnisses (z.B.: C:\tmp\) auf die Festplatte kopieren und modifizieren Sie den Inhalt der Datei “anschalttest.bat” ihrer Konfiguration folgend.
2. Öffnen Sie ein CMD Fenster

3. Wechseln Sie in dieses gewählt Verzeichnis (z.B.: C:\tmp\) und starten Sie die Stapeldatei “anschalttest.bat”. Dadurch wird versucht, einen Monitorpunkt auf diese Device zu setzen. Ist dies nicht möglich, werden im CMD-Fenster entsprechende Fehlermeldungen ausgegeben.

9.2.5 TAPI

Der OpenScape CAP TAPI Service Provider (CAP TCSP) kann von allen Windows TAPI basierenden Programmen genutzt werden.

9.2.5.1 Lizenzierung

Bei dem ersten NetTSPI-Request kontaktiert der SCC das CAP Lizenzmanagement und stellt die Anfrage, ob die entsprechende "ApplicationID" als Lizenz dem CTI-Benutzer zugeteilt ist. Ist die Lizenzvergabe im Modus "Bei der Benutzeranmeldung (Default) aktiv, so wird immer eine Lizenz zugeteilt. Wurde für einen Benutzer eine Lizenz erfolgreich überprüft, so speichert der SCC diese Information 3600 Sekunden. Bei einen SCC Neustart werden diese Informationen ebenfalls gelöscht.

Standard TAPI Applikationen verwenden keine individuelle "ApplicationID" und werden durch eine interne Routine durch eine SCC lizenziert

Der angesprochene SCC startet nach dem Empfang des ersten NetTSPI Requests eines CAP TCSP für einen CTI-Benutzer die Lizenzüberprüfung in folgender Reihenfolge:

1. CAP-A
2. CAP-S
3. CAP-E

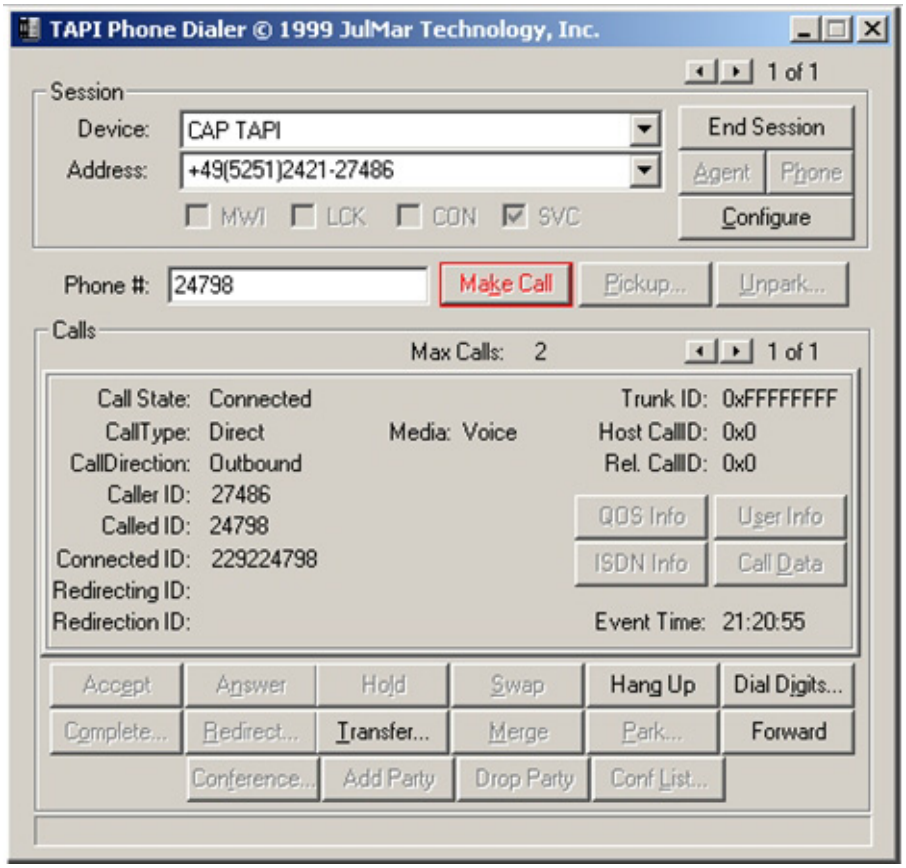
Ist keine der geforderten Lizenzen vergeben, wird die Verbindung zum CAP TCSP unterbrochen. Der CAP TCSP reagiert mit der Anzeige einer Fehlermeldung auf dem Monitor.

Neue TAPI Applikationen (z.B.: xPhone) verwenden eine individuelle “ApplicationID” durch das Setzten eines Parameters in “LineDevSpecificFeature”.

9.2.5.2 TAPI Test

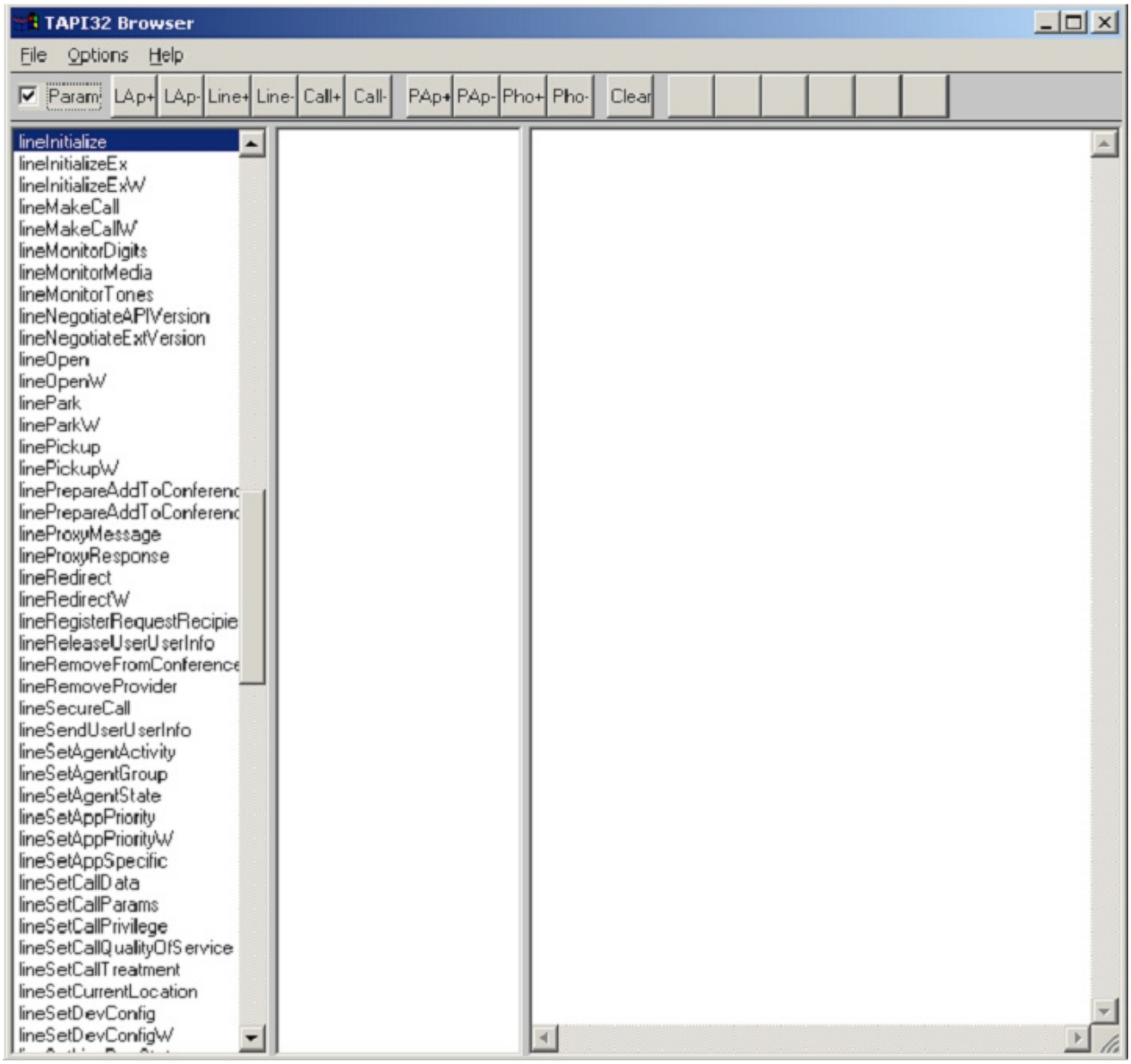
TAPI Testprogramm `Phone.exe`.

Um die Konfiguration für die TAPI zu testen, kann jedes Windows TAPI basierende Programm verwendet werden (Outlook, Wählhilfe). Es ist darauf zu achten, dass der Windows TAPI Server direkt nach dem Öffnen der Line automatisch einen Monitorpunkt auf das Device setzen., welches die Lizenz “CAP-E” eigentlich nicht unterstützt. Die “CAP-E” Lizenz verhindert erst später eine Eventweiterleitung vom Windows TAPI Server an die TAPI Applikation.



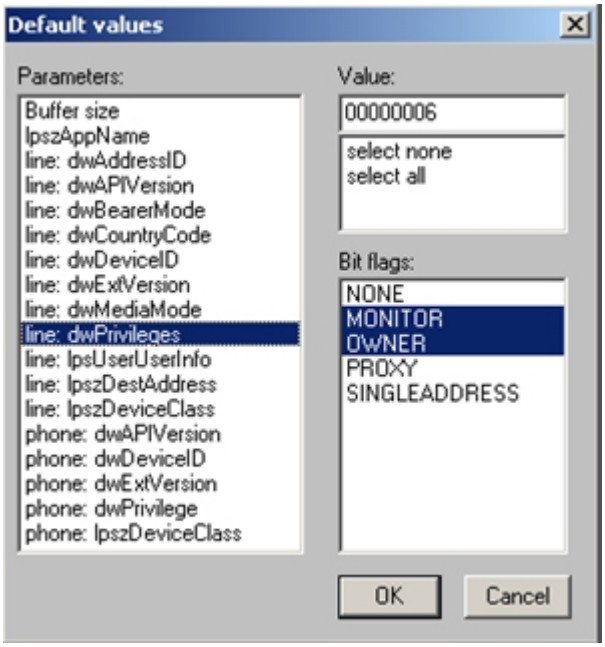
TAPI-Testprogramm `tb20.exe`

Mithilfe des TAPI-Testprogramms “tb20.exe” lassen sich grundlegende TAPI-Anfragen konfigurieren. Für die jeweilige Anfrage können dabei sämtliche verfügbare Parameter eingestellt werden.



Wählen Sie zunächst **Options | Default values**.

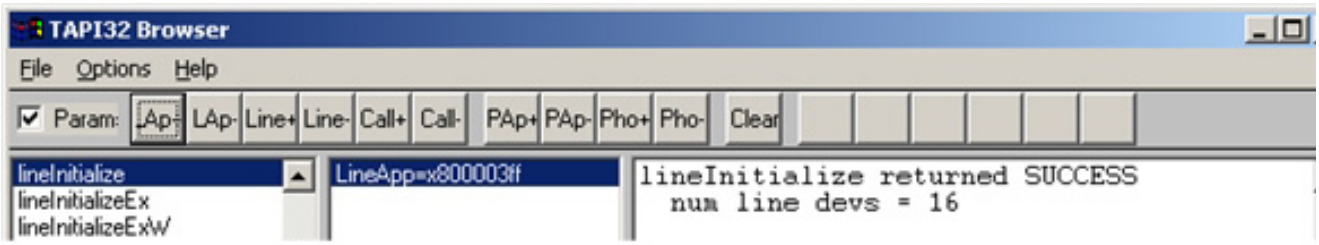
Setzen Sie **line dwPrivileges** auf **Monitor** und **Owner**.



Herstellen der Verbindung zum Windows TAPI Server

```
"lineInitialize"
```

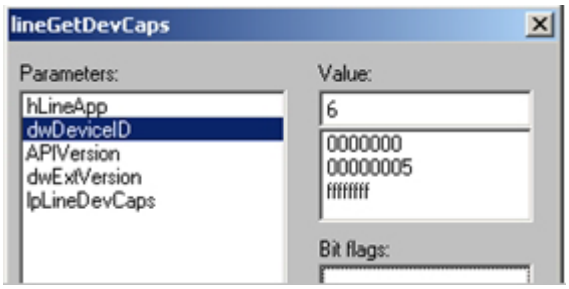
Hierauf erhalten Sie den **LineApp**-Handler und die Anzahl der verfügbaren Anschlusseinrichtungen, die von den installierten TAPI-Dienstanbietern bereitgestellt werden.



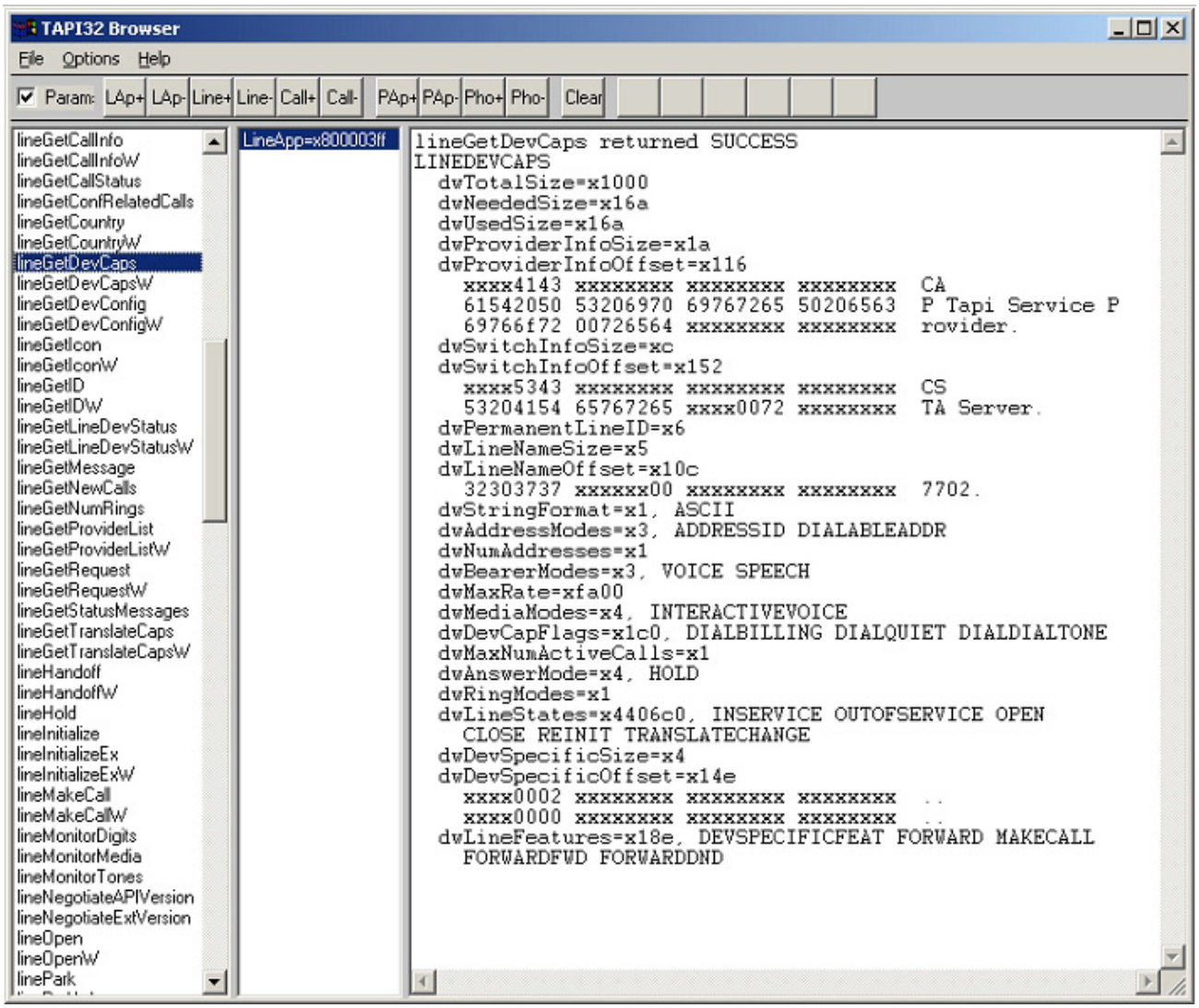
Ermitteln einer passenden TAPI-Anschlusseinrichtung

```
"lineGetDevCaps"
```

Geben Sie einzeln nacheinander die Gerätekennungen ein, um die zugehörigen Anschlusseinrichtungen zu suchen.



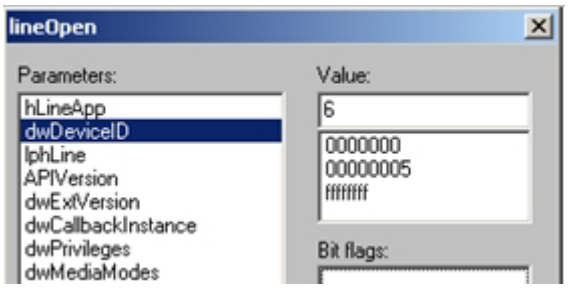
Sie erhalten detaillierte Informationen zu sämtlichen verfügbaren Anschlusseinrichtungen.



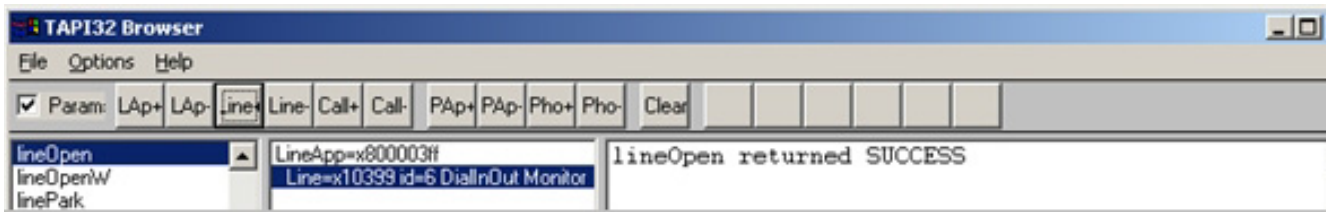
Öffnen einer TAPI-Anschlusseinrichtung

`"lineOpen"`

ID der Anschlusseinrichtung eingeben.



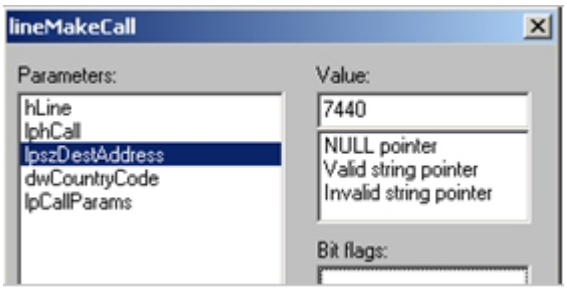
Hierauf erhalten Sie Informationen zur Anschluss-Sitzungskennung.



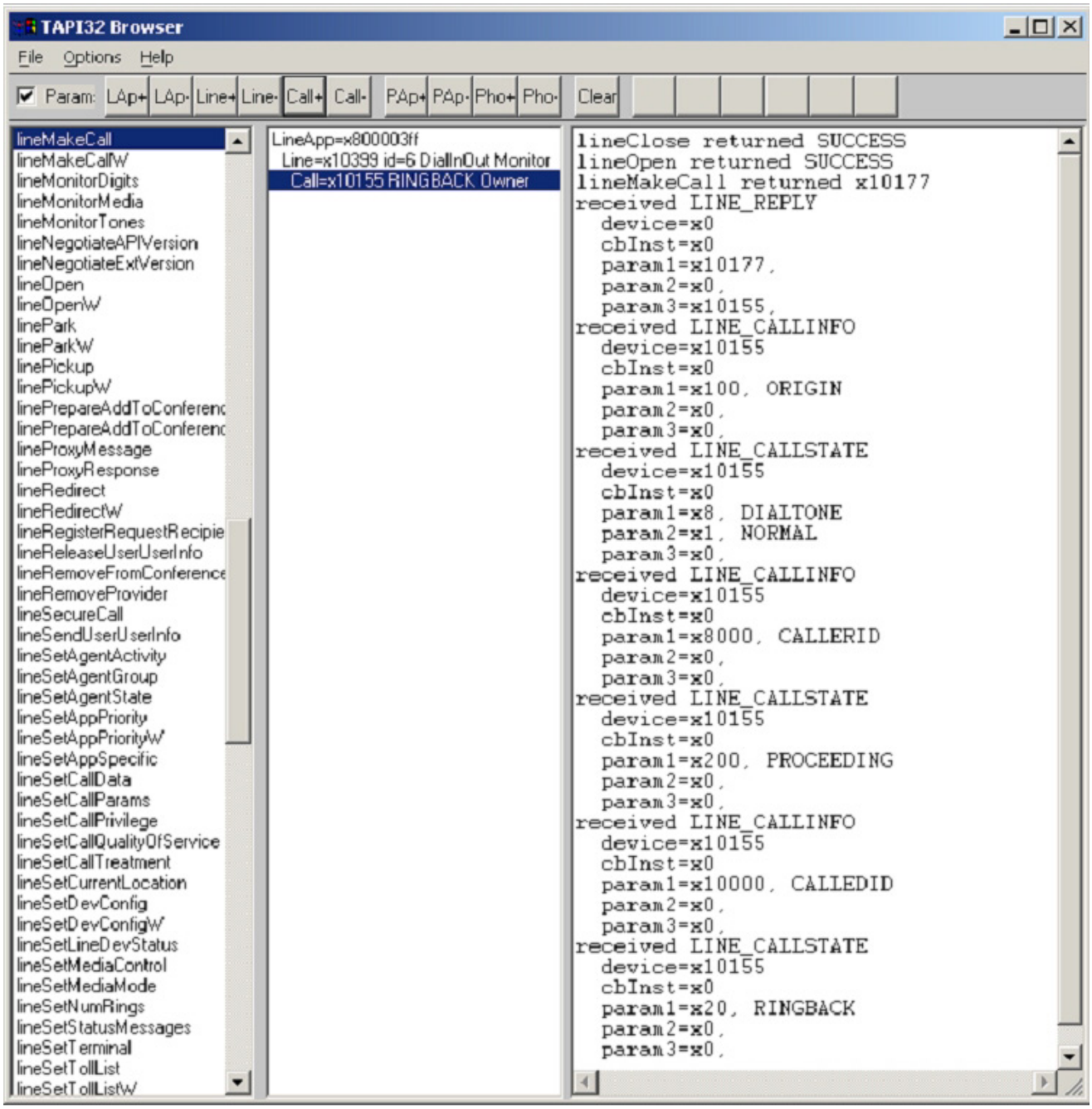
Durchführen eines Anrufs

`"lineMakeCall"`

Geben Sie die Zielnummer unter **lpszDestAddress** ein.



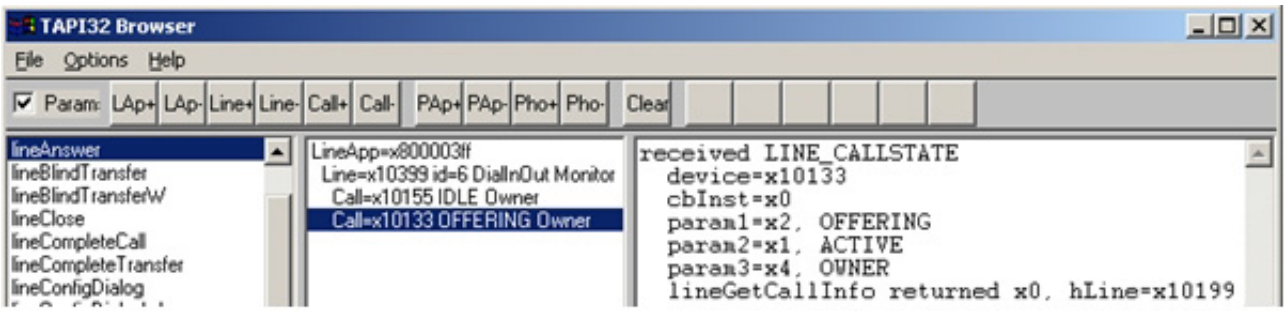
Hierauf erhalten Sie Informationen zur Anrufkennung.


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,

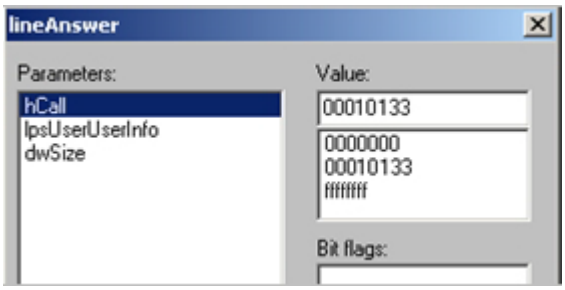
Entgegennehmen eines Anrufs

```
"lineAnswer"
```

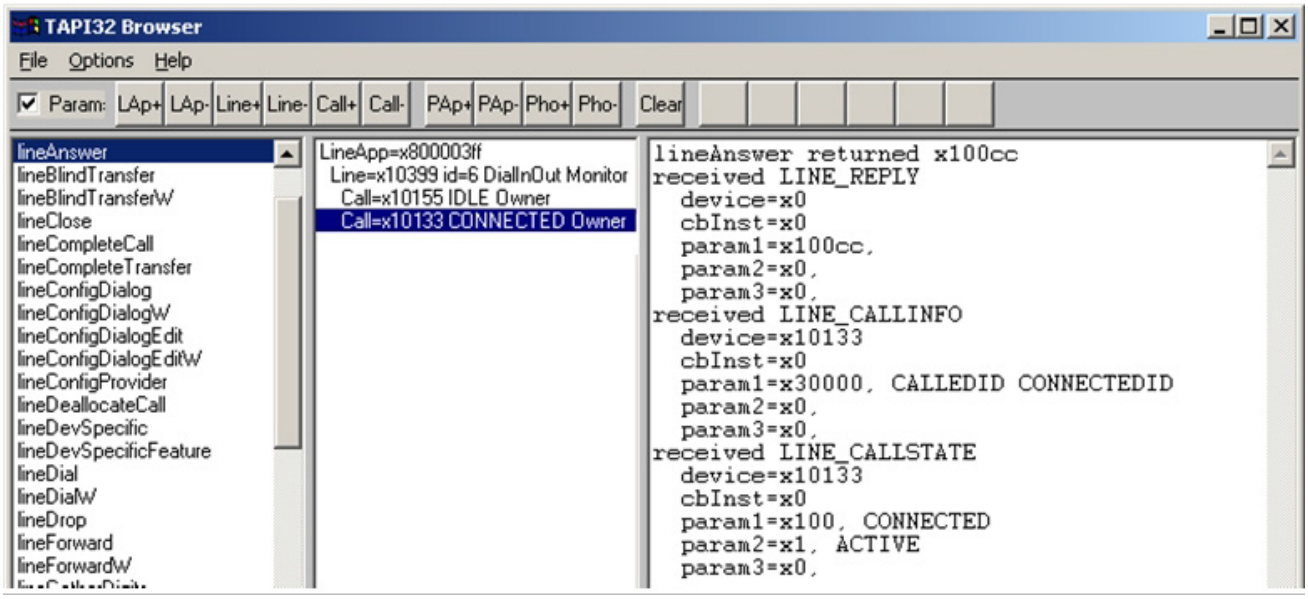
Dem Besitzer des Anschlusses wird ein kommender Anruf angeboten.



Geben Sie zu dem angebotenen Anruf die **hcall**-Nummer ein.



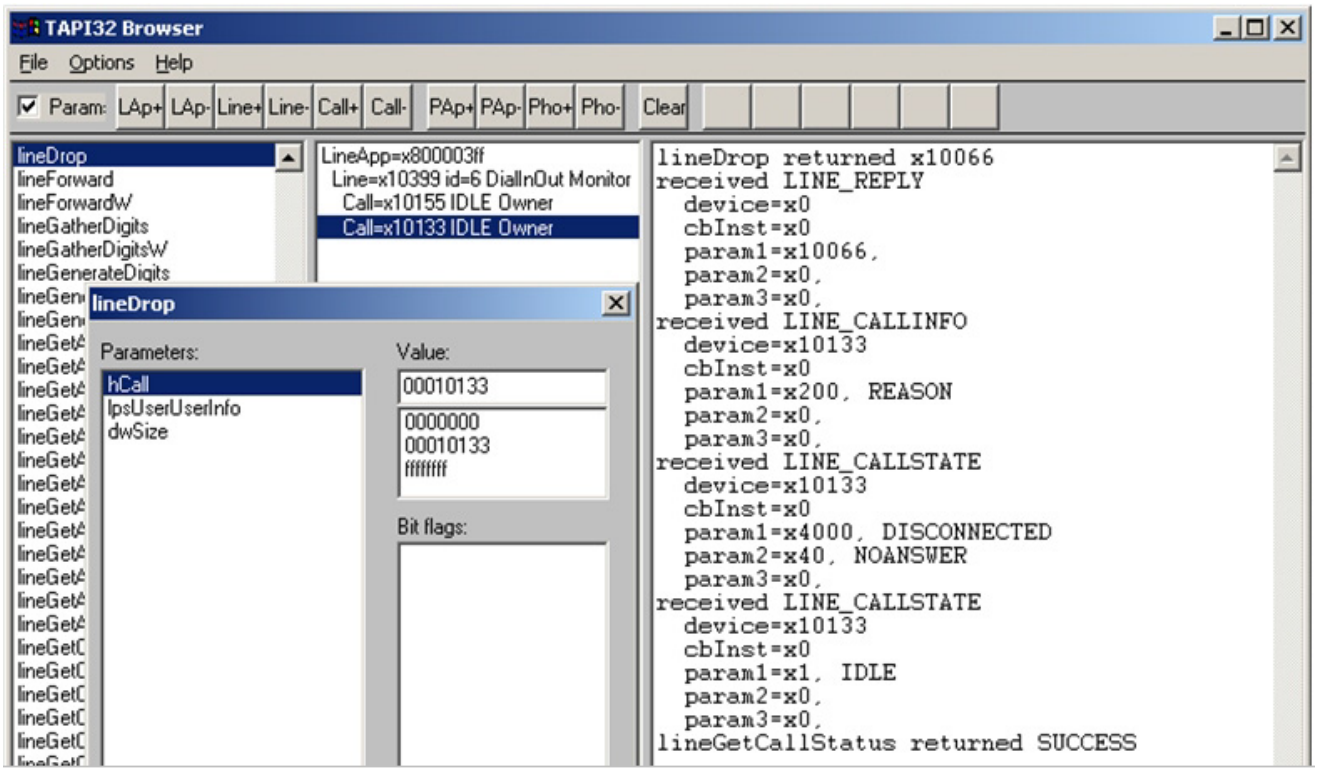
Hierauf erhalten Sie Informationen zum durchgeschalteten Anruf.



Auflegen

```
"lineDrop"
```

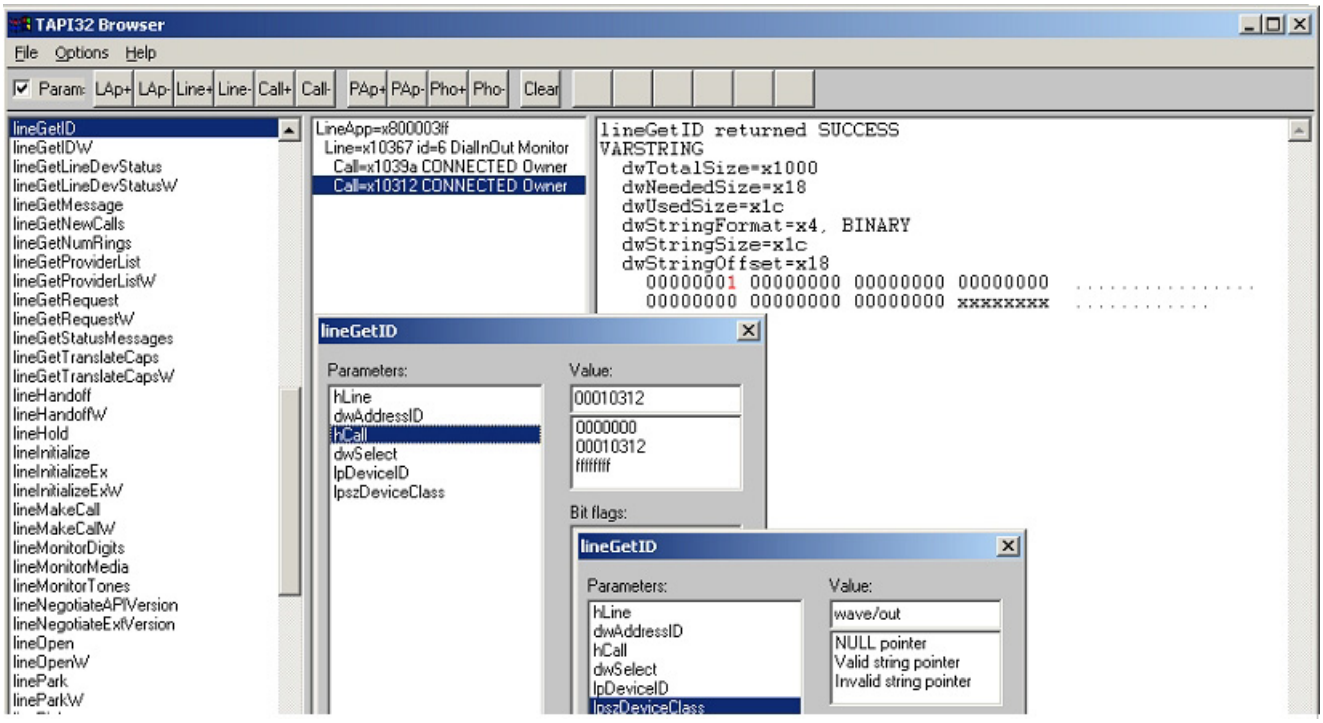
Geben Sie zu dem durchgeschalteten Anruf die **hcall**-Nummer ein.



Ermitteln der Media Device-Kennung

"lineGetID"

Geben Sie zu dem durchgeschalteten Anruf die **hcall**-Nummer ein und geben Sie bei **lpzDeviceClass** entweder **wave/out** oder **wave/in** ein.

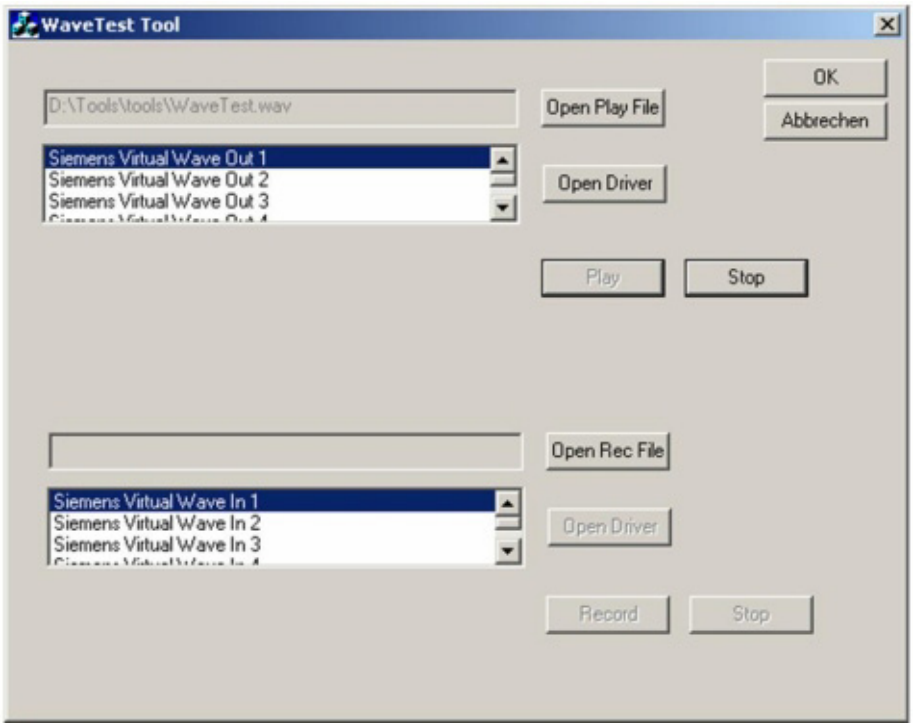


Abspielen einer Wave-Datei mit “WaveTest.exe”

Programm starten:

<InstDir>`\bin\tools\WaveTest.exe`

1. Wave-Datei öffnen, die abgespielt werden soll.
2. Kanalnummer für “dvStringOffset” auswählen
   (dvStringOffset 0 = Kanal 1, dvStringOffset 1 = Kanal 2,…).
3. Klicken Sie “Open Driver”.
4. Wave-Datei abspielen.
5. Für Pause, einmal “Stop” klicken; zum Stoppen, zweimal.



9.2.6 XML Phone Service

Zum Test des XML Phone Services wird die Testapplikation **TEFEX** automatisch mitinstalliert. Sie ermöglicht in Verbindung mit einem Endgerät der HiPath 4000 die Ein- und Ausgabefunktionen und die Signalisierung der XMLPS zu testen.

Um einen Test durchzuführen, sind folgende Schritte notwendig:

1. Richten Sie unter "URL Liste für XML PhoneService" die URL **"http://localhost:8172/tefex/tefex"** mit den URL Namen "TEFEX" ein.
2. Richten Sie an einem Endgerät eine Namenstaste mit dem Ziel **"C13999xx"** ein, wobei "xx" für die Tastennummer steht.
3. Starten Sie die Device-Konfiguration für dieses Endgerät und ordnen Sie unter "XML Phone-Einstellungen" der Taste "xx" die URL der Applikation **TEFEX** zu.

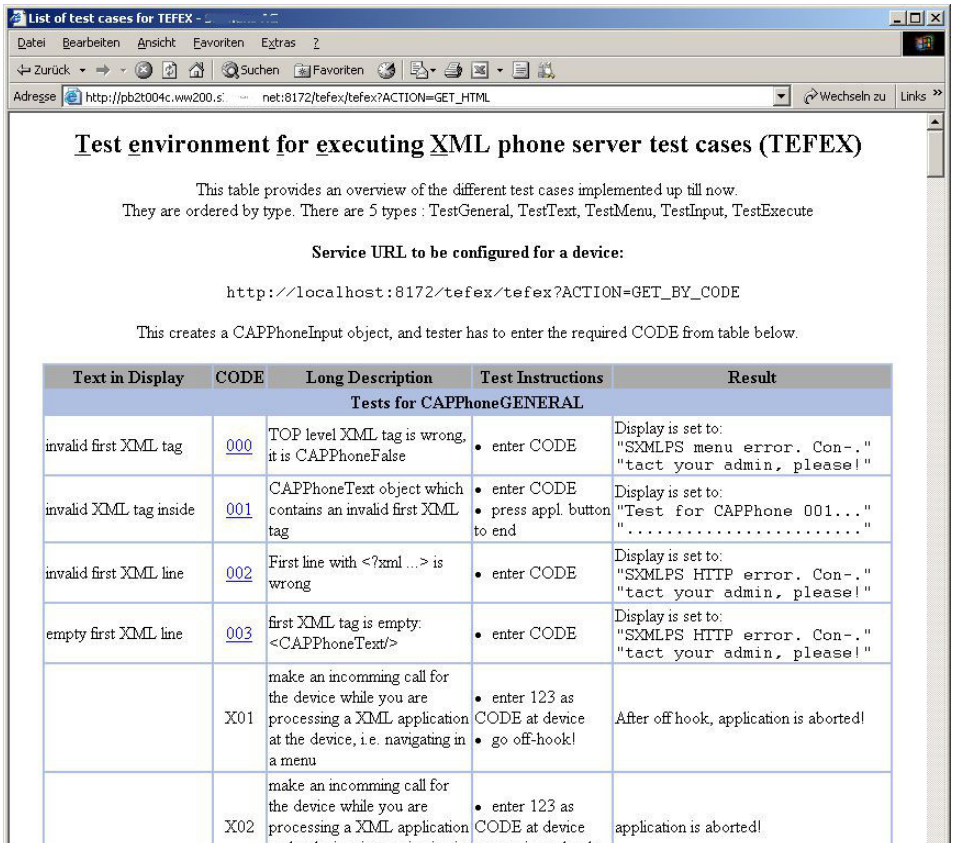
Nun können Sie die Einrichtung des XML Phone Service testen.

9.2.6.1 TEFEX

TEFEX ist eine Testapplikation, welche drei unterschiedliche Funktionen unterstützt:

- Eingabe am Telefon per Code,
- Eingabe am Telefon per Typ,
- Ausführung von "CAPPhoneEXECUTE" von einem Browser aus.

Die vollständige Beschreibung aller verfügbaren Funktionen wird auf folgender html-Seite aufgeführt: "**http://localhost:8172/tefex/tefex?ACTION=GET_HTML**".



List of test cases for TEFEX -

Datei Bearbeiten Ansicht Favoriten Extras ?

Zurück Suchen Favoriten

Adresse http://pb2t004c.ww200.s net:8172/tefex/tefex?ACTION=GET_HTML Wechseln zu Links

Test environment for executing XML phone server test cases (TEFEX)

This table provides an overview of the different test cases implemented up till now.
They are ordered by type. There are 5 types : TestGeneral, TestText, TestMenu, TestInput, TestExecute

Service URL to be configured for a device:

`http://localhost:8172/tefex/tefex?ACTION=GET_BY_CODE`

This creates a CAPPhoneInput object, and tester has to enter the required CODE from table below.

Text in Display	CODE	Long Description	Test Instructions	Result
Tests for CAPPhoneGENERAL				
invalid first XML tag	000	TOP level XML tag is wrong, it is CAPPhoneFalse	• enter CODE	Display is set to: "SXMLPS menu error. Con-." "tact your admin, please!"
invalid XML tag inside	001	CAPPhoneText object which contains an invalid first XML tag	• enter CODE • press appl. button to end	Display is set to: "Test for CAPPhone 001..." "....."
invalid first XML line	002	First line with <?xml ...> is wrong	• enter CODE	Display is set to: "SXMLPS HTTP error. Con-." "tact your admin, please!"
empty first XML line	003	first XML tag is empty: <CAPPhoneText/>	• enter CODE	Display is set to: "SXMLPS HTTP error. Con-." "tact your admin, please!"
	X01	make an incomming call for the device while you are processing a XML application at the device, i.e. navigating in a menu	• enter 123 as CODE at device • go off-hook!	After off hook, application is aborted!
	X02	make an incomming call for the device while you are processing a XML application	• enter 123 as CODE at device	application is aborted!

Alle unterstützten Testfunktionen sind unterteilt in folgende Gruppen:

- Tests for CAPPhoneGENERAL
- Tests for CAPPhoneTEXT
- Tests for CAPPhoneMENU
- Tests for CAPPhoneINPUT
- Tests for CAPPhoneEXECUTE (nur vom Browser aus nutzbar)

Alle unterstützten Testfunktionen sind sortiert nach:

- Text im Display (beim Test: "get test by type"),
- CODE (beim Test: "get test by code"),
- Long Description (Ausführliche Beschreibung),
- Test Instructions (Beschreibung der Eingaben am Telefon oder im Browser),
- Result (Testergebnis, was wirklich gestestet wird).

Eingabe am Telefon per Code (Test by Code)

Nachdem eine **TEFEX**-Session gestartet und der Testmodus "get test by code" ausgewählt wurde, erscheint im Display des Telefons die Nachricht:

Test Environment for CAP
CODE:

Nun kann ein Code eingegeben werden, der in der Spalte "CODE" aufgeführt ist. Ob eine weitere Eingabe am Endgerät erforderlich ist (Test Instructions), hängt vom eingegebenen Code ab. Am Display des Endgeräts sollten bei einem erfolgreichen Test entsprechend dem Code die Meldungen der Spalte Result (Display is set to:) dargestellt werden.
Wenn Sie über einen Browser auf einen Code klicken, so wird in diesem Browser die XML-Message angezeigt, die bei einem Test für diesen Code von TEFEX an den XMLPS geschickt wird.

Eingabe am Telefon per Typ (Test by Type)

Nachdem eine **TEFEX**-Session gestartet und der Testmodus "get test by type" ausgewählt wurde, erscheint im Display des Telefons ein weiteres Menü:

Test Environment for CAP
Test for CAPPhone:

Nun können Sie durch die "**<**" "**>**" in diesem Menü blättern und folgende Typgruppen durch die Taste "**OK**" auswählen:

- Test for CAPPhone Text:
- Test for CAPPhone Menu:
- Test for CAPPhone Input:
- Test for CAPPhone Exec:
  (Obwohl hier angeboten, wird dieser Test **nicht von Telefon** aus unterstützt!)

Wählen Sie eine Testgruppe aus!

Nun wird Ihnen in Menüform Schritt für Schritt entsprechend der ausgewählten Testgruppe der Text aus der Spalte "Text im Display" angeboten. Zur Auswahl eines Tests drücken Sie die "OK" Taste. Ob eine weitere Eingabe am Endgerät erforderlich ist (Test Instructions), hängt von dem ausgewählten Test ab. Am Display des Endgeräts sollten bei einem erfolgreichen Test entsprechend dem Testaufruf die Meldung in der Spalte Result (Display is set to:) dargestellt werden.
Wenn Sie über einen Browser auf einen Code klicken, so wird in diesem Browser die XML-Message angezeigt, die bei einem Test für diesen Code von TEFEX an den XMLPS geschickt wird.

Ausführung von "CAPPhoneEXECUTE" von einem Browser aus

Wenn Sie auf der html-Seite von TEFEX einen CODE aus der Gruppe "Test for CAPPhoneExecute" (z.B.: CODE 400) anklicken, wird eine neue html-Seite dargestellt.

Ändern Sie in dem XML-String den Wert für das Tag <Phone> und geben Sie die Device-Id des für diesen Test benutzten Endgeräts ein. Drücken Sie nun die Schaltfläche **Send to Invoke Interface Servlet**. Am Display des Endgeräts sollten bei einem erfolgreichen Test entsprechend dem Testaufruf die Meldung in der Spalte Result (Display is set to:) dargestellt werden.

A Implementierungs-Details

A.1 Aufbau der Installation

A.1.1 Konfigurations-Dateien

Die Konfigurationsdateien aller OpenScape CTI-Komponenten werden bei der Installation in verschiedene Verzeichnisse unterhalb des Installationsverzeichnisses *<InstDir>* abgelegt.

Bei Installation von OpenScape CAP Management wird der Verzeichnisbaum wie folgt eingerichtet. Einzelne Verzeichnisse werden nach und nach mit der Installation und Konfiguration weiterer Komponenten gefüllt.

```
<InstDir>\config\
    common\
        cap.cfg
        global.cfg
        http-server.zip
        ports.cfg
        proc.cfg
        ROOT.war
    start\
        StartNT.cfg
    <hostI>\
        start\
            JStarter.cfg
        <process1>\
            S<x>service_ctrl.proc
            <service1>\
                S<x><service1>.svc
                <service1>.cfg
                http-server.props
            ...
            <serviceN>\
                S<x><serviceN>.svc
                <serviceN>.cfg
                http-server.props
        ...
        <processN>\
            ...
```

? **<*InstDir*>**\config\common\
enthält für alle OpenScape CTI Komponenten wichtige Konfigurationsdateien.

- *<InstDir>*\config\start\
  enthält die Konfigurationsdatei für den Start-Service, über den das geamte System gestartet wird.

- *<InstDir>*\config\localhost\
  Alle Konfigurationen für die Prozesse und Services, die auf dem Installationsrechner laufen sollen, werden hier abgelegt. Der Inhalt dieses Verzeichnisses spielt bei einer Netzverteilung des Systems eine wesentliche Rolle.

- *<InstDir>*\config\<hostI>\
  Für jeden im System konfigurierten Rechner wird ein solchen Verzeichnis eingerichtet und entsprechend dem Rechnernamen (ohne Domain-Erweiterung) benannt. Das Verzeichnis enthält alle Informationen und Konfigurationsdaten für die Prozesse und Services, die auf diesem Rechner laufen sollen. Bei einer Standardinstallation gibt es genau ein solches Verzeichnis (für den lokalen Rechner).

- <*InstDir*>\config\<hostI>\<processN>\
  Für jeden Prozess, der auf <hostI> laufen soll, existiert ein solches Verzeichnis. In diesem Verzeichnis existiert immer eine Datei S<x>service_ctrl.proc mit der Information, wie der Prozess zu starten ist. Der Namensbeginn S<x> dient der Ermittlung der Prozess-Startreihenfolge. <x> ist dabei eine Zahl (z. B. S47service_ctrl.proc. Dieser Prozess wird vom System vor S49service_ctrl.proc gestartet) Mit dem Dateinamen wird also die Hochlaufreihenfolge der Prozesse festgelegt.
  Sollten mehrere Services als Threads innerhalb eines Prozesses laufen, existiert für jeden Service ein eigenes Unterverzeichnis mit dem Servicenamen <serviceN>. Läuft im Prozess nur ein Service, so entfällt das Unterverzeichnis.

- <*InstDir*>\config\<hostI>\<processN>\<serviceN>\
  Dieses Verzeichnis existiert für jeden Service-Thread innerhalb eines Prozesses. In diesem Verzeichnis existiert immer eine Datei S<x><serviceN>.svc mit der Information, wie der Service zu starten ist. Über den Namen der Datei wird wie bei den Prozessen die Startreihenfolge festgelegt. Weiterhin enthält das Unterverzeichnis alle für den Service spezifischen Konfigurationsdateien. Handelt es sich bei dem Service um eine Servlet Engine muss auch eine Konfigurationsdatei http-server.props enthalten sein.

- *<InstDir>*data\TelasAdmin\
  Hier legt OpenScape CAP Management die Daten für Security Service, Administration Service und das Import Tool ab.

Durch diese flexible Architektur ist es leicht möglich, die Prozesse des Systems auf verschiedene Rechner zu verteilen. Für jeden neuen Rechnerknoten wird automatisch bei der Einrichtung einer verteilten Komponente für diesen Rechner auf dem Master-Server ein neues Verzeichnis <hostI> angelegt, und die Prozess-Unterverzeichnisse der Prozesse, die auf <hostI> laufen sollen, werden dorthin übertragen.

Auf <hostI> muss jetzt noch der **Service-Starter** installiert werden. Dieser besorgt sich eigenständig beim ersten Start die notwendigen Daten und Prozesse vom Master-Server (siehe auch Abschnitt 4.7, “Verteilte Installation”).

A.1.2 Programm-Dateien

Bei der Installation werden Programmdateien, zum Produkt gehörige Java-Klassenbibliotheken, Stapeldateien und DLLs im Verzeichnis *<InstDir>*\distribution abgelegt.

Beim Start werden diese Komponenten in die Verzeichnisse *<InstDir>*\bin, *<InstDir>*\bin\tools und *<InstDir>*\lib kopiert. Dabei wird geprüft, ob eine Kopie notwendig ist. Dies ist immer dann der Fall, wenn es sich bei den Komponenten aus *<InstDir>*\distribution um andere Versionen handelt.

- *<InstDir>*\bin
  enthält das Programm jsstart.exe (Startservice für WinNT) und im Unterverzeichnis tools verschiedene Batch-Dateien für den Datenimport und den Einzelstart von Komponenten des Systems
- *<InstDir>*\jre
  enthält das Java-Laufzeitsystem
- *<InstDir>*\lib
  enthält die zum Produkt gehörenden Java-Klassenbibliotheken

A.1.3 Log-Dateien

Im Verzeichnis *<InstDir>*\Logs werden während des Betriebs Logging-Dateien erzeugt und abhängig vom eingestellten Logging-Level mit Informationen, Fehlern und Zuständen der Telas-Komponenten gefüllt. Hier existiert immer ein Unterverzeichnis mit dem PC-Namen des CAP Management Rechners. Bei einer verteilten Installation werden entsprechend der PCs weitere PC-Namensverzeichnisse angelegt. Jedes Verzeichnis für sich beinhaltet alle Log-Dateien der auf diesem PC laufenden Prozesse.

OpenScape CAP Management legt dieses Verzeichnis bei der Installation an. Es wird von allen OpenScape CTI-Komponenten genutzt.

A.1.4 Dateien zur Bedienoberfläche

Alle zu OpenScape CAP Management und Call Control Services gehörenden HTML-Seiten liegen im Verzeichnisses `<InstDir>\WebSpace`.

Jede OpenScape CTI -Komponente legt dort eigene Unterverzeichnisse an, in denen sprachunabhängige HTML-Seiten (`*.html`) sowie sprachabhängige Headerdateien (`*.h`) und Programm-Resource-Dateien (`*.properties`) abgelegt sind. Dazu gehören die Bedienoberfläche und die Installations- und Administrationshandbücher.

Die sprachabhängigen Dateien befinden sich dabei immer in einem Unterverzeichnis mit dem Namen `lang.` Die darin befindlichen Verzeichnisse tragen den Namen der jeweilig enthaltenen Sprache; OpenScape CAP Management wird in den Sprachvarianten `de` (Deutsch) und `en` (Englisch) ausgeliefert.

Da die verschiedenen HTML-Seiten untereinander referenziert werden, dürfen sie zwar im Layout angepasst, aber nicht umbenannt werden. Beachten Sie bitte, dass bei Neuinstallation evtl. Änderungen an den Seiten überschrieben werden.

Das Verzeichnis `css` enthält für alle HTML-Seiten genutzte Styles; normalerweise wird `std_-style.css` verwendet.

Das Verzeichnis `Plugin` enthält das für das Diagnose-Applet notwendige Java Runtime Plugin für die Web-Browser Netscape Navigator/Communicator und Microsoft Internet Explorer. Eventuell muss vor der ersten Nutzung der Diagnose diese Installation ausgeführt werden, damit das Plugin verfügbar ist.

A.2 Beschreibung der Konfigurations-Dateien

OpenScape CAP Management stellt Konfigurationsdateien, wie in Abschnitt A.1.1 beschrieben, im Verzeichnis <*InstDir*>\config\ bereit. Im folgenden werden nur die Konfigurationsdateien angesprochen, in denen wichtige Konfigurationsänderungen vorgenommen werden können.

A.2.1 Konfiguration des Logging und Tracing

Zur Einrichtung des Logging / Tracing spielen eine Reihe von Einträgen in diversen Konfigurations-Dateien zusammen. Im folgenden werden die wesentlichen beteiligten Dateien beschrieben sowie sinnvolle Einstellungen beispielhaft dargestellt.

1. Die Datei **/config/common/global.cfg** enthält eine Reihe von allgemein genutzten Konfigurationseinstellungen (vgl. Abschnitt A.2.2), unter anderem auch für Logging / Tracing. Da `global.cfg` in zahlreichen weiteren Konfigurations-Dateien inkludiert wird, wirken sich Änderungen hier implizit in allen abhängigen Komponenten aus.

   Relevante Konfigurationsparameter:

   ```
   log.class        = com.xxxxxx.log.ClientLogger
   log.serverUrl    = lookup://LogServer
   log.level        = 3
   log.maxLines     = 2000
   log.maxFiles     = 3
   ```

   `log.class` sowie `log.serverUrl` bleiben unverändert

   `log.level` definiert den Umfang des Logging / Tracing (steigender Level -> mehr Daten)

   ```
   OFF       = -1
   FATAL     = 0
   ERROR     = 1
   WARNING   = 2
   MESSAGE   = 3
   TRACE     = 4
   DBG_TRACE = 5
   ```

   `log.maxlines` definiert die maximale Anzahl von Zeilen je LogFile

   `log.maxfiles` definiert die maximale Anzahl von anzulegenden LogFiles (vgl. Abschnitt A.1.3) ; diese werden benannt nach dem Schema

   ```
   <name>.log
   <name>_last.log
   <name>_last1.log
   <name>_last2.log
   ...
   ```

Die folgenden Einstellungen sind in der Standardversion der Konfigurationsdatei nicht vorhanden; sie können bei Bedarf hinzugefügt werden:

`log.daily = <number>`
Anzahl von Tagen, für die Log-Dateien aufgehoben werden sollen; für jeden Tag wird im Verzeichnis `<INST_DR>/logs` ein Unterverzeichnis angelegt
`log.daily = 0` heißt kein tageweises logging
`log.daily = 7` heißt logging für sieben Tage; ältere Log-Dateien werden gelöscht

`log.filter = <string>`
`log.filterModus = expand | exclusive`
gestattet selektives logging, gesteuert über Filter-Kriterien; alle Ereignisse, die zum eingestellten Filter passen, werden mit höchstem Logging Level 5 aufgezeichnet.
Diese Funktion ist nur für die dem CAP Management zugeordneten Logger verfügbar.

Anwendungsbeispiele

```
log.filter = 51234
log.filterModus = expand
log.level = 3
```
Logging-Daten werden auf Level 3 gesammelt; zusätzlich werden alle Daten, die den Text "51234" enthalten, auf Level 5 aufgezeichnet.

```
log.filter = 722,89*4132
log.filterModus = exclusive
log.level = 3
```
Es werden nur Daten aufgezeichnet, die den Text "722" oder "89" gefolgt von beliebigen Zeichen gefolgt von "4132" enthalten, und zwar auf Level 5;
die Einstellung log.level = 3 ist in diesem Fall ohne Bedeutung.

Diese Parameter gelten für alle Logger mit den jeweils zugehörigen LogFiles. Die Übersicht aller aktiven Logger erhalten Sie im DiagnoseAgent (Abschnitt 7.7.5) über Debug -> Show Logging. Dazu gehören

- Zentrale Logger des Management-Frameworks wie
  - start
  - admin
  - lookup
  - diag
- Logger für Services / SCC-Instanzen wie
  - <SCC name>_Sys

- <SCC name>_Error
- <SCC name>_CA4000_Sys (für HiPath 4000-Verbindung)
- <SCC name>_CA4000_Trace (für HiPath 4000-Verbindung)

- Loger für weitere Services und Applikationen wie ComAssistant

Daneben ist es möglich, diese Einstellungen für einzelne Logger spezifisch anzupassen. Dazu ist jeweils der Parameter mit dem Namen des Loggers zu qualifizieren, wie z.B.

```
log.maxLines.admin          = 10000
log.maxFiles.admin          = 5
log.maxlines.<SCC name>_Sys = 20000
log.maxFiles.<SCC name>_Sys = 10
```

2. Bitte beachten Sie, dass für das globale, von allen Komponenten gemeinsam benutzte **`errors.log`** spezifische Einstellungen gelten; diese folgen nicht dem beschriebenen Schema, sondern sind an zentraler Stelle in der Konfigurationsdatei `/config/<host>/admin/log/LogServer.cfg` abgelegt:

   ```
   include "/common/global.cfg"
   errorsLog.file     = errors.log
   errorsLog.maxLevel = 1
   errorsLog.maxLines = 10000
   errorsLog.maxFiles = 2
   ```

   Hier ist es möglich, `maxLines` und `maxFiles` wie oben beschrieben anzupassen. Dies wird normalerweise nicht erforderlich sein.

3. Für jede konfigurierte Switch-Anbindung wird eine SCC-Instanz mit zugehöriger Konfigurationsdatei **`telas.cfg`** eingerichtet:

   ```
   include "/common/global.cfg"
   log.class          = com.xxxxxx.log.ClientLogger
   log.serverUrl      = lookup://LogServer
   log.level          = 3
   cstaLogEnabled     = 0
   debugLevel         = 0
   ```

   `log.class` sowie `log.serverUrl` bleiben unverändert

   `log.level` kann hier erneut definiert werden und würde den aus `global.cfg` importierten Wert überschreiben. Dies ist meist nicht sinnvoll - eher sollte die Einstellung des Log-Levels für alle Komponenten identisch in `global.cfg` erfolgen, in `telas.cfg` kein Eintrag stehen und service-spezifische Abweichungen temporär über den DiagnoseAgent eingestellt werden.

`cstaLogEnabled = 1` schaltet spezifisch für diese SCC-Instanz zusätzlich zum "normalen" Logging die Aufzeichnung des CSTA-Meldungsverkehrs in die Datei `<SCC name>_CSTA.log` ein; diese ist normalerweise ausgeschaltet.

`debugLevel` verfeinert über die LogLevel-Einstellung hinaus den Umfang des SCC-spezifischen Tracing nach `<SCC name>_Error.log`. Hier sind Werte zwischen 0 (ausgeschaltet, Standardwert) und 9 (maximale Information) möglich.

Für CAP V3.0 SMR3 wurde eine weitere Logging-Möglichkeit spezifisch für SCCs realisiert; diese wird über neue Einträge in telas.cfg gesteuert. Die Logging-Ausgaben können nur in der Entwicklung interpretiert werden; dieses Logging sollte dementsprechend nur auf Anweisung und mit Unterstützung eines Entwicklers aktiviert werden

4. Zusätzlich zu den oben beschriebenen Einstellungen über Konfigurations-Dateien können Sie jederzeit über den **DiagnoseAgent** die aktuellen Logging-Einstellungen anzeigen (Debug -> Show Logging) und auch den LogLevel verändern; dazu ist der betreffende Logger zu selektieren, ein neuer LogLevel-Wert auszuwählen und über "SetLevel" einzustellen. Bitte beachten Sie, dass diese Einstellung nicht in die Konfigurations-Dateien eingetragen wird und demzufolge nach dem Neustart des Systems wieder verloren geht.

A.2.2 `global.cfg`

Diese Datei enthält globale Einstellungen für alle Prozess- und Service-Controller des gesamten Systems. Die Variablen werden bei der Installation für die Installationsumgebung entsprechend vorbelegt. Daher muss im Normalfall an dieser Datei nichts geändert werden.

Am Anfang der Datei werden globale Variablen und Konfigurationsparameter gesetzt, die damit in allen weiteren Konfigurationsdateien genutzt werden können. Die Werte werden automatisch von der Installation korrekt eingetragen.

`INST_HOST`	enthält den Rechnername im User-LAN ohne Domainzusatz
`INST-IP`	enthält die IP-Adresse des Rechners im User-LAN (nicht zur PBX-Anbindung)
`CONFIG_URL`	URL zur Startseite von OpenScape CAP Management
`CFG`	Pfad zum Verzeichnis mit den Konfigurationsdateien

Die danach folgenden Variablen werden zur Steuerung des Loggings verwendet. Details dazu sind in Abschnitt A.2.1 beschrieben

7	Die Einstellung `tomcat.log.level` (Standardwert -1 / ausgeschaltet) dient der Steuerung des Web-Server Loggings. Es sollte nur in speziellen Fällen eingeschaltet werden, da es sehr ausführlich ist und damit große Datenmengen entstehen.

`useDaylightTime = true`
Dieser Schalter steuert die automatischen Umschaltung auf Sommerzeit. Wenn Sie in Ihrem Betriebssystem die automatische Umschaltung aktiviert haben (Standard-Einstellung), muss dieser Schalter auf `true` gesetzt sein, damit die Zeiten, die z. B. beim Logging genutzt werden, mit der Systemuhr übereinstimmen. Ist diese Funktion im Betriebssystem deaktiviert, so muss dieser Schalter auf `false` gesetzt werden.
Sie können die Betriebssystem-Einstellungen über **ControlPanel | Date/Time | TimeZone** überprüfen.

`MaxCookieAge = 43200`
Lebensdauer eines Cookies in **Minuten**. In einem Cookie wird die erfolgreiche Authentifizierung eines CAP-Benutzers für ComAssistant gespeichert. Nach dieser Zeit wird eine erneute Authentifizierung eines CAP-Benutzers erzwungen.

`CustomizedPath =`
Sollen eigene HTML-Seiten verwendet werden, so kann hier ein Pfad auf diese Dateien angegeben werden. Nähere Informationen finden Sie im ComAssistant Installations- und Administrationshandbuch, Abschnitt “Kundenspezifische HTML-Seiten”.

`<?x set TelasWebName = "CAP" ?>`
Definition des CAP Server Namens zur eindeutigen Identifizierung bei einer Notification-Email

`<?x set MAIL_SERVER = "mail.org.de" ?>`
Eingabe des SMTP Email-Server-Namens. Die Eingabe erfolgt an der Position von mail.org.de.

```
<?x set MAIL_SENDER = "<?x $TelasWebName ?> notifica-
tion<tws@mail.org.de>" ?>
```
Eingabe des Email-Senders. Die Eingabe erfolgt an der Position von tws@mail.org.de.

`<?x set MAIL_SYSADMIN = "sysadm@mail.org.de" ?>`
Eingabe des Email-Empfängers. Die Eingabe erfolgt an der Position von sysadm@mail.org.de.

`PasswordMode = ADMIN [ADMIN/AUTO]`
`ADMIN` = ComAsststant-Benutzer müssen bei einem vergessenen Passwort den CAP-Administrator kontaktieren, um einen neues Passwort zu bekommen.
`AUTO` = ComAsststant-Benutzer können bei einem vergessenen Passwort ein neues Passwort per Email anfordern. Dazu muss dem CAP-Benutzer in einem definiertem LDAP-Server eine Email-Adresse zugeteilt worden sein. Die Konfiguration des LDAP-Servers erfolgt in der Datei `admin.cfg`.

A.2.3 ports.cfg

In dieser Datei werden die Ports für die http- und https-Verbindung zum CAP Management und zu ComAssistant definiert.

`<?x set CAP_SSL_PASSWD = "changeit" ?>`
Hier wird das Passwort definiert, das bei der Generierung der Verschlüsselungsdatei vergeben wurde.

`<?x set CAP_SSL_FILE = ".keystore" ?>`
Hier wird der Dateiname der Verschlüsselungsdatei für die CAP definiert. Die Datei "`.keystore`“ mit dem Passwort "`changeit`“ ist im Default bereits vorhanden.

`<?x set CAP_SEC_MODE  = "OFF" ?>`
Hier wird die gesicherte Verbindung zum CAP Management eingerichtet (OFF/ON).

`<?x set CAP_SEC_PORT  = "8470" ?>`
Hier wird der Port für die gesicherte Verbindung zum CAP Management definiert (default = 8470). Dieser Port wird vom Web-Server der CAP geöffnet.

`<?x set CAP_STD_PORT  = "8170" ?>`
Hier wird der Port für die normale Verbindung zum CAP Management definiert (default = 8470). Dieser Port wird vom Web-Server der CAP geöffnet.

`<?x set SPW_SSL_PASSWD = "changeit" ?>`
Hier wird der Dateiname der Verschlüsselungsdatei für die CAP definiert. Die Datei "`.keystore`“ mit dem Passwort "`changeit`“ ist im Default bereits vorhanden.

`<?x set SPW_SSL_FILE  = ".keystore" ?>`
Hier wird die gesicherte Verbindung zum CAP Management eingerichtet (OFF/ON).

`<?x set SPW_SEC_MODE  = "OFF" ?>`
Hier wird die gesicherte Verbindung zu ComAssistant eingerichtet (OFF/ON).

`<?x set SPW_SSL_AUTH  = "false" ?>`
Hier wird die gesicherte Verbindung zu ComAssistant während der Login Session eingerichtet (true/false).

`<?x set SPW_SEC_PORT  = "8480" ?>`
Hier wird der Port für die gesicherte Verbindung zum CAP Management definiert (default = 8470). Dieser Port wird vom Web-Server von ComAssistant (Phone Controller) geöffnet.

`<?x set SPW_STD_PORT  = "8180" ?>`
Hier wird der Port für die normale Verbindung zum CAP Management definiert (default = 8470). Dieser Port wird vom Web-Server von ComAssistant (Phone Controller) geöffnet.

`<?x set SPW_MGMT_PORT = "8168" ?>`
Hier wird der Port für die XML Verbindung von ComAssistant zum CAP Management definiert (default = 8168). Dieser Port wird vom Web-Server der CAP geöffnet.

A.2.4 `TelasWeb.cfg`

Für die Konfiguration des gesamten OpenScape CTI Systems ist die Datei `TelasWeb.cfg` von wesentlicher Bedeutung. Bei der Standard-Installation brauchen hier zunächst keine Änderungen vorgenommen werden.

Erläuterung zu den wichtigsten Einträgen in dieser Datei:

`ConfigDomain`
Domänenname des Rechners, auf dem der zentrale Konfigurationsservice installiert wurde.

7	Diese Angabe wird nur dann benötigt, wenn während der Installation von OpenScape CAP Management der Domainname des Installationsrechners nicht ermittelt werden konnte. Dies ist leicht daran erkennbar, dass die folgenden URL-Angaben nur den Rechnernamen enthalten!

`PhoneURL`
URL zum Zugriff auf den Phone-Service

`Journal.AccessUrl`
URL zum Zugriff auf den Journal-Access-Service.

`Journal.MailUrl`
URL zum Zugriff auf den Mail-Service.

`RequestTimeout = 10`
Maximale Zeitspanne in Sekunden, die auf eine Antwort auf einen Request an den Phone-Service gewartet wird.

`PBX.PingInterval = 120000`
Falls über längeren Zeitraum keine Requests abgesetzt wurden, wird in dem angegebenen Intervall über einen Ping-Request geprüft ob der Server noch arbeitet. Zeitangabe in Millisekunden.

`NoExpireDate = 0`
Die Verfallszeit für Passwörter ist im OpenScape CTI System administriert und festgelegt. ComAssistant nutzt im Standardfall diese Daten. Ist eine Verfallszeit für Passwörter nicht gewünscht, kann dieser Schalter auf 1 gesetzt werden.

`EnableConsultation = YES`
Zeigt an, ob die verwendete PBX-Anlage die Telefon-Sonderfunktionen Makeln und Konferenz unterstützt oder nicht. Normalerweise werden diese Funktionen unterstützt (YES). Genauere Informationen finden Sie im Installations- und Administrationshandbuch für ComAssistant.

`#EnableCMCSupport = YES`
Aktivierung der "Client-Matter-Code“ Unterstützung für ComAssistant. Ist das Leistungsmerkmal aktiviert, so wird die Wahl einer Projektkennzahl zur expliziten Kennzeichnung eines Gesprächsdatensatzes ermöglicht.

`#SametimeServer = mhpa48wc.mchp.xxxxxx.de`
Hier können Sie den Sametime Server (Lodus Domino Server) für ComAssistant definieren. Dazu muss zwingend zusätzlich das SameTime Paket für ComAssistant auf dem CAP-Server installiert sein. Diese Anbindung ermöglicht die Darstellung der An- und Abwesenheit von verknüpften Lotus Notes Benutzern in ComAssistant.

`UserDBAccessParams = NO`
Hier können Sie die WEBDAV-Schnittstelle des Exchange Servers für ComAssistant Benutzer zur optionalen Verwendung der eigenen, auf dem Exchange Server befindlichen Outlook Kontakte aktivieren anstelle des ComAssistant PABS.

A.2.5 `startNT.cfg`

Die Datei `StartNT.cfg` wird vom Start-Service (`jsstart.exe`) verwendet, um das gesamte OpenScape CTI-System als System-Service zu starten. Die Variablen werden bei der Installation entsprechend richtig gesetzt.

Wichtige Argumente für den Start sind:

`args:` **<CAP-Managment-PC-Name>**`/TelasWebStarter`

Jedes OpenScape CTI System wird über eine ClusterId identifiziert. Damit ist eindeutig festgelegt, welche Prozesse und Services einem Cluster angehören.
Bei der Installation des CAP Managements wird in der Regel der eigene PC-Name als Cluster-Id gesetzt. Bei einer verteilten Installation steht er bei im LAN unterstütztem Multicast als Auswahl in einem Selektionsmenü zur Verfügung. Sollte bei einer verteilten Installation Multicast vom einem Kunden nicht gewünscht oder im LAN nicht möglich sein, so muss zwingend auf allen CAP-Rechnern (auch auf dem CAP-Server) der Eintrag wie folgt erweitert werden:

`args:` **<CAP-Management-PC-Name>@<CAP-Management-PC-Name>:<Free-UDP-Port>**`/TelasWebStarter`

`#args:-v`

Falls beim Start Probleme auftreten, kann über die Option **`-v`** ein ausführlicheres Logging zugeschaltet werden. Zu diesem Zweck entfernen Sie hier das Kommentarzeichen #.

`args:-port`
`args: 8280`

Durch diese Angabe wird der Port für den Diagnose Agenten festgelegt. Dieser Port muss nur geändert werden, wenn er auf dem Rechner bereits belegt sein sollte.

A.2.6 Prozess-Steuerung durch `.proc` files

Im CAP-Framework kann der ProcessController jeden vorkonfigurerten Prozess starten, stoppen und steuern. Jeder Prozess wird mittels einer `.proc` Konfigurations-Datei beschrieben, in der Lokalisierung und Name des Prozesses ebenso definiert werden wie weitere Argumente, die der ProcessController dem anlaufenden Prozess zu übergeben hat.

Die komplette Menge aller von einem ProcessController zu startenden Prozesse ergibt sich über die Sammlung aller `.proc` files unterhalb des Verzeichnisses, das nach dem Rechner benannt ist, auf dem der entsprechende ProcessController läuft.

Syntax der `.proc` files

`.proc` files werden wie property files interpretiert. Jede Zeile mit dem Zeichen ":" definiert ein Konfigurations-Datum, und das Zeichen "#" leitet eine Kommentarzeile ein. Im ersten Eintrag im Skript muss der Service Identifier festgelegt werden. Die Reihenfolge der übrigen Einträge ist ohne Bedeutung; alle Einträge mit den jeweiligen Datenwerten werden gesammelt und erst danach angewendet. Bei der Schreibweise der Schlüsselbegriffe ist Groß-/Kleinschreibung irrelevant (nicht aber bei den Datenwerten!).

Auswahl wichtiger Schlüssel, die in ausgelieferten `.proc` files genutzt werden:
(Bitte beachten Sie, dass von Änderung bereitgestellter `.proc` files dringend abgeraten wird; dies könnte die korrekte Arbeit des Gesamtsystems beeinträchtigen; lediglich die Schlüssel aus der "`restart`"-Gruppe könnten für spezifische Anpassungen von Kundeninstallationen interessant sein)

`service: <service-identifier>`

eindeutiger Bezeichner für den Prozess / Dienst

`cmd: <command>`

absoluter Pfadname für das auszuführende Kommando / Programm

`args: <argument>`

Argument zur Übergabe an den Prozess / Dienst (darf mehrfach vorkommen)

`env: <environment>`

Umgebungs-Variable für den Prozess (darf mehrfach vorkommen)

`wait: <timeout in seconds>`

Wartezeit vor Ausführung des nächsten Kommandos (nur im Synchron-Modus)

`mode: <synchronize mode>`

Prozess ist synchron (mode 0) oder asynchron (mode 1 - Standardwert) zu starten

`workdir: <working directory>`

Pfad zur Definition des Arbeitsverzeichnisses für den Prozess

`mkdir: <directory path>`

Pfad neu einzurichten, falls noch nicht vorhanden (darf mehrfach vorkommen)

`restart: <auto restart mode>`

Prozess kann im Fall des Absturzes (Stop ohne Aufforderung) automatisch neu gestartet werden
restart:0 heißt kein auto restart (Standardwert), restart:1heißt auto restart

`restartexitvalue: <exit value>`

auto restart wird nur ausgeführt, wenn der Prozess mit einem definierten exit code beendet wurde

`restartwaittime: <timeout>`

der abgestürzte Prozess wird erst nach Ablauf einer definierten Wartezeit (in Sekunden) automatisch neu gestartet

`get: <get command>`

das get-Kommando überträgt eine Datei aus dem distribution-Verzeichnis ins lib-Verzeichnis (Standard-Einstellung) oder in ein anderes, vollständig spezifiziertes Zeilverzeichnis. Wenn im Zielverzeichnis eine Datei dieses Namens bereit vorhanden ist, werden die Änderungs-Zeiten verglichen, und nur bei unterschiedlichen Daten wird die Datei erneut übertragen (kann mehrfach vorkommen)

Hinweis: Das get-Kommando hat bis zu drei Parameter

`<relative source path> [<relative dest path>] [<replace argument]`

Das replace argument beschreibt in einer durch Kommata getrennten Liste Anweisungen an den Page-Generator zur Ersetzung von Variablen in der kopierten Datei, z.B.

`"replace=INST_HOST=<hostname>,INST_DIR=<install path>"`

Wenn kein Ziel / dest path angegeben ist, wird die Datei ins lib-Verzeichnis kopiert, wobei der relative Pfad der Quelldatei als Pfad der Zieldatei relativ zum lib-Verzeichnis interpretiert wird

`getunzip: <get and unzip command>`

wie das get.Kommando, aber die zu übertragende Datei ist ein zip-Archiv und wird im Zielverzeichnis extrahiert.

A.2.7 admin.cfg

Diese Datei ist im Verzeichnis *<InstDir>*\config\<hostname>\admin\mgmt abgelegt. Sie dient der Konfiguration des Administration-Services. Alle Einstellungen werden bei der Installation vorgenommen.

```
Ldap.server = scd2ldap.xxxxxx.net:389
```
In Verbindung mit ComAssistant kann bei vergessenem Passwort eine Email mit einem neuen automatisch generierten Passwort angefordert werden. Um eine Verifizierung eines CAP-Benutzers und eingegebener Email-Adresse durchzuführen, wird die Zusammengehörigkeit der Email-Adresse und der dem Benutzer zugeordneten „Phone-Device Number“ (Rufnummer im kanonischen Format) in diesem LDAP-Server überprüft. Geben Sie hier den LDAP-Servernamen bzw. die IP-Adresse und den LDAP-Port ein.

```
#Ldap.user = cn=Test Benutzer,ou=Eine OU,o=Xxxxxx
#Ldap.password = meinsehrgeheimeskennwortdasniemandsieht
```
Um eine Verbindung zum LDAP Service zu erhalten, muss in einigen Fällen der LDAP Client sich beim Server anmelden. Um die Authentisierungs-Daten für die "Anbindung" (login) bereitzustellen, tragen Sie den vollquailifizeirten eindeutigen Benutzernamen (Distinguished Name) und das unverschlüsselte Passwort des Clients hier ein.

```
#Ldap.ssl = 1
```
Das oben genannte Verfahren mit der Passwort-Vergabe stellt ein Sicherheits-Risiko dar, da dieses im Netzwerk gelesen werden kann. Das können sie vermeiden, wenn sie die Authentisierung mittels eines Verschlüsselungs-Mechanismus durchführen, vorausgesetzt daß dieser durch den LDAP Server unterstützt wird.

Wenn der LDAP Server auf den sie zugreifen möchten den Service der SSL-Verschlüsselung unterstützt, dann wird empfohlen dies auch zu nutzen. Entfernen sie dazu im angeführten Befehl das Kommentarzeichen(#)

Prüfen Sie bitte, ob Sie den korrekten Port im Ldap.server Parameter benutzen, an dem der LDAP Server die SSL-Verbindung anbietet.

Sie müssen sicherstellen, daß der Client dem LDAP Server vertrauen kann. Dazu müssen sie die Sicherheitszertifizierung des LDAP Servers (oder seine CA's Zertifizierung) in die JRE-Datenbank zu den vertrauenswürdigen Zertifikaten installieren.
```
# cd JAVA_HOME/lib/security
# keytool -import -file server_cert.cer -keystore cacerts
```
Wichtig! Benutzen Sie für den Parameter -keystore immer den Wert "cacerts".

```
#Ldap.phone-number = telephoneNumber
#Ldap.mailaddress = mail
```
Falls die Suchfeldbezeichnungen (Mapping) nicht dem Default in diesem LDAP-Server entsprechen, geben Sie die entsprechende Suchfeldbezeichnung ein. Links befindet sich die Feldbezeichnung in der CAP, rechts die im LDAP Server.

`Ldap.timeLimit = 30`
Hier definieren Sie die Zeit bis zu einem Such-Timeout. Ist nach dieser Zeit für eine Rufnummer und eine Email-Adresse kein gemeinsamer Eintrag gefunden worden, so wird die Suche beendet. Dies hat zur Folge, dass keine Email mit automatisch generiertem Passwort an den ComAssistant Benutzer gesendet wird.

`Language = de`
Definieren Sie die Sprache für die Email mit automatisch generiertem Passwort für den ComAssistant Benutzer: `de = German, en = English`

`DatabaseServerList = SYSDB,SYSDB.MAP.Users,SYSDB.MAP.Usergroups,SYSDB.MAP.Scc,SYSDB.MAP.SCCProxy,SYSDB.MAP.Devices, SYSDB.MAP.Snrs, SYSDB.MAP.Licenses, SYSDB.MAP.Businessgroup, SYSDB.MAP.Urls, SYSDB.MAP.Ca, SYSDB.MAP.Xmlphoneservice`
Vorbereitung zur Anbindung von externen LDAP-Servern anstelle des CAP internen LDAP-Servers SLAPD zur Verwaltung der gesamten Daten.

`xml.logRequests = 1`
`xml.traceDir = <?x $INST_DIR ?>/logsXML`
Diese Einträge sind standarmäßig inaktiv (auskommentiert). Falls der XML-Meldungsverkehr vom / zum CAP Management aufgezeichnet werden soll, ist das Kommentarzeichen zu entfernen. Dadurch wird eine beträchtliche Menge von Trace-Daten erzeugt, was aber in gewissen Situationen (z.B. zur Analyse der Aktivitäten in Zusammenhang mit dem Feature Access-Point-Emergency) durchaus hilfreich sein kann.

`ProgramMode = CAP`
OpenScape CAP V3.0 ermöglicht die automatische Integration von Benutzerdaten. Dadurch ist es nicht mehr nötig, eine doppelte Benutzerverwaltung, sowohl in der CAP als auch in einer Applikation zu pflegen. Folgende Applikationen können exklusiv angebunden werden:

- `CAP =` Die CAP interne Benutzerverwaltung **(Default)**
- `HiPath4000Manager =` Intergration in den HiPath 4000 Manager **(nicht freigegeben)**
- `HiPathUserManager =` Integration in das HiPath User Management
- `HQ8000 =` Integration der HQ8000 Benutzerverwaltung **(kommt nicht)**
- `OpenScape =` Integration der Open Scape Benutzerverwaltung **(kommt nicht)**

`#ModesListDir = modes`
Im Verzeichnins `<InstDir>\config\<hostname>\admin\mgmnt\modes` befinden sich im Default die Konfigurationsdateien für die Anbindung der verschiedenen Benutzerverwaltungssysteme. Die Dateinamen entsprechen der Parametereingaben für „`ProgramMode`“. Es besteht die Möglichkeit, eine anderes Verzeichnis auszuwählen, in dem sich die entsprechenden Konfigurationsdateien befinden. Geben sie in diesem Fall den vollständigen Pfadnamen an.

A.2.8 adminIf.cfg

Diese Datei ist im Verzeichnis `<InstDir>\config\<hostname>\admin\mgmt` abgelegt. Sie dient der Konfiguration des AdminInterfaceService. Alle Einstellungen werden bei der Installation vorgenommen.

`TelasWebInstalled = 1/0`
Ist dieser Schalter gesetzt (1), so wird in der CAP GUI ein Link zur ComAssistant Hilfe angeboten.

`TelasServerNames`
(Nicht verändern!) Diese Parameter enthält eine Liste der unterstützten PBX-Anbindungen mit den dazugehörigen Namen für die Darstellung in der OpenScape CAP Management-Bedien-oberfläche. Jeder Eintrag entspricht folgender Struktur: „<Verzeichnisname> | <Selektionsname>,“. Das Verzeichnis `<InstDir>\config\distribution\config\<Verzeichnisname>` enthält die Vorlagen aller Konfigurationsdateien für diesen spezifischen SCC. Der <Selektionsname> wird aus Auswahl beim Hinzufügen eines SCC angeboten.

`Asn1Modes = false|off, acse|CSTA ACSE, 3|CSTA III`
(Nicht verändern!) . Hier wird das Mapping für die im „Single Domain Native Mode“ eingerichteten SCC definiert.

`MaxResult = 300`
`PageResult = 10`
Hier definieren Sie die Standardparameter in der Suchmaske, die beim Aufruf "Suche nach Benutzern“ im CAP Management angeboten werden.

`MaxTeamAgentMembers = 20`
Hier definieren Sie die maximale Anzahl der zu einer Buddy-Liste zugehörigen Benutzern für ComAssistant.

`DeviceTypes = Phone|Phone, VirtualDevice|VirtualDevice`
(Nicht verändern!) . Hier wird das Mapping für die Devices angegeben, die in der CAP Management Device-Konfiguration hinzugefügt werden können.

A.2.9 auth.cfg

Diese Datei dient der Konfiguration des SecurityService. Alle Einstellungen werden bei der Installation vorgenommen. Wichtigste Angabe in dieser Datei ist die Verfallsdauer und das Standardpasswort für CTI-Benutzer. Diese Daten werden in der Bedienoberfläche des OpenScape CAP Management über den Dialog *Standardpasswort* eingestellt.

`ExpirePeriod = 40`
Maximale Gültigkeit eines individuellen Passworts in Tagen. Dieser Parameter wird über die CAP GUI geändert.

`ExpirePeriodAutoPassword = 60`
Maximale Gültigkeit eines individuellen automatisch generierten Passworts in Tagen. Dieser Parameter wird über die CAP GUI geändert.

`StandardPassword = MTIzNDU2`
Das Standardpasswort für einen CAP Benutzer in Base64 codierter Form.

A.2.10 backup.cfg

Diese Datei enthält die Einstellungen für das automatische Backup der Daten der CAP und von ComAssistant. Achten Sie darauf, dass bei einem Backup auf ein Netzlaufwerk der Windows Dienst "OpenScape CTI“ einem Domain-Benutzer zugeordnet wurde, welcher selbst die Berechtigung zum Zugriff auf dieses Netzlaufwerk besitzt und ebenfalls die lokale Berechtigung "Anmelden als Dienst“ hat. Die verschiedenen Backups müssen zu unterschiedlichen Zeiten stattfinden.

`NrBackups = 7`
Definieren Sie hier die Anzahl der zu sichernden Backups. Pro Tag wird ein Backup erstellt. Der Sicherungsverzeichnisname entspricht dem Format:
"<Monat>-<Tag>.<Sicherungszähler>“

`BackupRootDir = <installPfad>/OpenScapeCTI/backups`
Definieren Sie hier das Zielverzeichnis für alle Backups.

`<?x set RULES_BACKUP_TIME = "01:55:00" ?>`
Hier wird die Uhrzeit für das Backup der Daten des ComAssistant Regelassistenten definiert.

`<?x set USERS_BACKUP_TIME = "02:00:00" ?>`
Hier wird die Uhrzeit für das Backup der Daten der CAP definiert.

`<?x set PABS_BACKUP_TIME = "02:10:00" ?>`
Hier wird die Uhrzeit für das Backup der persönlichen Adressbücher der ComAssistant Benutzer definiert.

`<?x set JOURNAL_BACKUP_TIME = "02:30:00" ?>`
Hier wird die Uhrzeit für das Backup der Rufjournale der ComAssistant Benutzer definiert.

`<?x set CAP_LDAP_MODE = "STANDALONE" ?>`
Bei einer Windows Installation muss der Parameter auf "`Standalone`“ verbleiben. Nur bei einer erst später möglichen Installation unter LINUX kann eine Replizierung durch "`Replica`“ aktiviert werden.

A.2.11 ConfigLoader.cfg

Diese Datei enthält die Einstellungen für den ConfigLoaderService und darf im Normalfall nicht geändert werden. Hier sind u. a. Pfadangaben zu den Konfigurations-Verzeichnissen und zum Namen der Vorlage für die persönlichen Journaleinstellungen gemacht.

Durch Änderung der folgenden Angabe ist es möglich die persönlichen Journaleinstellungen aller Nutzer in einem anderen Verzeichnis abzulegen. Grund dafür kann Platzmangel auf der Festplatte oder Datensicherung sein.

`PersonalConfigDir` =
`<installPfad>/OpenScapeCTI/data/TelasWeb/Journals`

A.2.12 Diagnose.cfg

In dieser Datei werden Einstellungen für das Diagnose-Servlet vorgenommen.

A.2.13 Login.cfg

In dieser Datei können vom Administrator Login-Domains vorbelegt werden, die dann bei der Anmeldung von CTI-Benutzern, die Authentifizierung durch „System-Kennung“ gewählt haben, zur Auswahl angeboten werden.

A.2.14 DiagnoseServer.cfg

Über die Datei `DiagnoseServer.cfg` ist es möglich, Email-Benachrichtigungen bei Systemstörungen zu konfigurieren. Die Emails werden dann vom Diagnose-Service an die spezifizierten Mail-Adressen verschickt. Dazu ist die Konfiguration eines Email-Servers zwingend erfoderlich. Dieser wird in der Date i"`global.cfg`“ definiert.

`#Diagnose.Timer.PingInterval = 150`
Hier wird die Ping-Intervallzeit definiert (Default = 150 Sekunden). Nach Ablauf dieses Timers überprüft der Diagnose Server den aktuellen Status eines CAP internen Services durch einen Ping.

`#Diagnose.Timer.CheckProcInterval = 128`
Hier wird die Snapshot-Intervallzeit definiert (Default = 128 Sekunden). Nach Ablauf dieses Timers überprüft der Diagnose-Server den aktuellen Status eines CAP Prozess Controllers (TelasWebStarters) durch einen Snapshot und bekommt zusätzlich Informationen bezüglich der gestarteten Prozesse.

`#Diagnose.Timeout.Request = 20`
Hier wird die Wartezeit nach einen Ping oder Snapshot definiert (Default =20 Sekunden). Nach Ablauf dieses Timers wird erneut ein Ping oder Snapshot geschickt bis der "Retry Counter“ überschritten wurde.

`#Diagnose.Timeout.Resend = 2`
Hier wird die Zeit definiert (Default =2 Sekunden) nach der nach einem "Timeout.Request“ erneut ein Ping oder Snapshot geschickt wird.

`#Diagnose.Timeout.RetryCount = 3`
Hier wird der Wiederholzähler nach "Timeout.Request“ definiert (Default =3 Wiederholungen). Nach Ablauf diese Wiederholzählers wird der Status eines Prozess Controllers oder CAP internen Services geändert.

`#MailTrap.Receiver-<n>.Address = <?x $MAIL_SYSADMIN ?>`
Hier wird die Email-Adresse eines Empfängers einer Diagnose-Email definiert. Die Variable `<?x $MAIL_SYSADMIN ?>` kann ersetzt werden. <n> steht für die Blocknummer. Jeder Block kann unterschiedliche Konfigurationen enthalten.

`#MailTrap.Receiver-<n>.TrapFilter = <id> [|<id>] ...`
Hier werden die für diesen Block aktiven Filter definiert. <id> steht für die Filternummer, welche später konfiguriert sein müssen. Trifft ein Filter zu, so wird eine Email generiert und an die zugehörige Blockadresse geschickt.

`#MailTrap.Receiver-<n>.SubjectFile = <subjectTemplateFile>`
Hier wird der Dateiname des zugehörigen "Subject Template Files“ definiert. Im Verzeichnis der Datei "`DiagnoseDerver.cfg`“ befindet sich die Template-Datei `subjectSample.cfg`.
Achten Sie auch bei dem Dateinamen auf Groß-/Kleinschreibung.

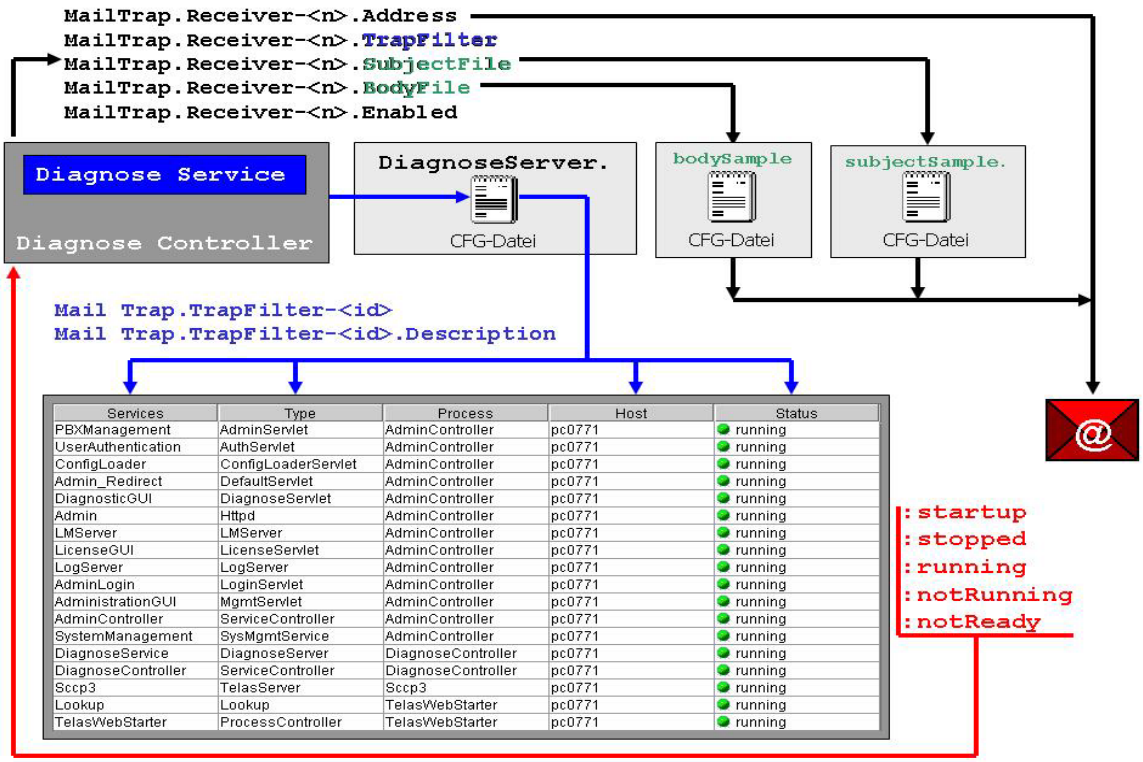
`#MailTrap.Receiver-<n>.BodyFile = <bodyTemplateFile>`
Hier wird der Dateiname des zugehörigen "Body Template Files“ definiert. Im Verzeichnis der Datei "`DiagnoseDerver.cfg`“ befindet sich die Template-Datei `bodySample.cfg`.
Achten Sie auch bei dem Dateinamen auf Groß-/Kleinschreibung.

`#MailTrap.Receiver-<n>.Enabled = true`
Hier können Sie diesen Konfigurationsblock aktivieren oder deaktivieren.

`MailTrap.TrapFilter-<id> = <host>/[<svcType>/]<svcId>:<thresh-old>:<state>[|<state>]`
`MailTrap.TrapFilter-<id>.Description = <id>= Filterbeschreibung`
Hier können Sie den Filter explizit definieren und eine Beschreibung hinzufügen.
`<host>` - Der PC, auf dem ein Prozess oder ein CAP interner Service läuft.
`<svcType>` - Der CAP interne Servicename
`<svcId>` - Der Service Identifier
`<threshold>` - Der Schwellwert
`<state>` - Der Status eines Prozesses oder CAP internen Services.
Folgende Status werden unterstützt:
`notReady|notRunning|stopped|startup|running`

Beispiel einer Trapkonfiguration

```
MailTrap.Receiver-0.Address = DAuser0771@tipb.de
MailTrap.Receiver-0.TrapFilter = 0|1|2|3|4|5|6
MailTrap.Receiver-0.SubjectFile = subjectSample.cfg
MailTrap.Receiver-0.BodyFile = bodySample.cfg

MailTrap.TrapFilter-0 = pc0771/TelasServer/sccp-1:1:notReady|notRunning
MailTrap.TrapFilter-0.Description = 0 = location/Type/Service:amount:status

MailTrap.TrapFilter-1 = */Httpd/*:1:notReady|notRunning
MailTrap.TrapFilter-1.Description = 1 = One Httpd is notReady or notRunning

MailTrap.TrapFilter-2 = */TelasServer/*:1:notReady|notRunning
MailTrap.TrapFilter-2.Description = 2 = One TelasServer is notReady or
notRunning

MailTrap.TrapFilter-3 = *ccp*:1:notReady|notRunning
MailTrap.TrapFilter-3.Description = 3 = *ccp*

MailTrap.TrapFilter-4 = */Httpd/*:1:*
MailTrap.TrapFilter-4.Description = 4 = One Httpd is notReady or notRunning

MailTrap.TrapFilter-5 = *:1:stopped
MailTrap.TrapFilter-5.Description = 5 = One of the processes/services has
stopped

MailTrap.TrapFilter-6 = *:*:running
MailTrap.TrapFilter-6.Description = 6 = All processes/services are running
```



Services	Type	Process	Host	Status
PBXManagement	AdminServlet	AdminController	pc0771	running
UserAuthentication	AuthServlet	AdminController	pc0771	running
ConfigLoader	ConfigLoaderServlet	AdminController	pc0771	running
Admin_Redirect	DefaultServlet	AdminController	pc0771	running
DiagnosticGUI	DiagnoseServlet	AdminController	pc0771	running
Admin	Httpd	AdminController	pc0771	running
LMServer	LMServer	AdminController	pc0771	running
LicenseGUI	LicenseServlet	AdminController	pc0771	running
LogServer	LogServer	AdminController	pc0771	running
AdminLogin	LoginServlet	AdminController	pc0771	running
AdministrationGUI	MgmtServlet	AdminController	pc0771	running
AdminController	ServiceController	AdminController	pc0771	running
SystemManagement	SysMgmtService	AdminController	pc0771	running
DiagnoseService	DiagnoseServer	DiagnoseController	pc0771	running
DiagnoseController	ServiceController	DiagnoseController	pc0771	running
Sccp3	TelasServer	Sccp3	pc0771	running
Lookup	Lookup	TelasWebStarter	pc0771	running
TelasWebStarter	ProcessController	TelasWebStarter	pc0771	running

A.2.15 Konfigurationsdateien für SAT

Der Address Translation Service (SAT, genauere Beschreibung in Abschnitt 2.3.4) wird nur über Konfigurationsdateien, die explizit angepasst werden müssen, eingerichtet. Hier gibt es keine Konfiguration über die Management-Oberfläche. Die betroffenen Konfigurationsdateien sind

SatServer.cfg (im Verzeichnis `<InstDir>/config/<host>/admin/sat_svc`)

Telas.cfg (im Verzeichnis `<InstDir>/config/<host>/sccp_<sccp_name>`)

Telas.cfg (im Verzeichnis `<InstDir>/config/<host>/telasServer_<scc_name>`)

SatServer.cfg ist die zentrale Konfigurationsdatei für SAT; Struktur

```
#------------------------------------------------------------------------
# Environment for Service Address Translation
#------------------------------------------------------------------------

<?x include "/common/global.cfg" ?>

...

#
# configuration of SatServer local TCP port
#
LOCAL_PORT = 8999 <-- TCP port hier eingeben (8999 ist Standardwert)
LOG_LEVEL = 2     <-- log level hier eingeben (2 heißt Fehlerausgabe)

#
# legacy mode setting - used to set CAP V3.0 operation in CAP V2.0 mode:
# Applications that don't want to adapt don't get canonical or interntl
# format numbers except for PBXes which are newly supported in CAP V3.0
#
# Default setting: SAT bypassed
LEGACY_MODE = true
# Unset legacy mode to activate SAT!
#LEGACY_MODE = false
```

Die **Telas.cfg** Konfigurationsdateien für eingerichtete SCCs und SCCPs enthalten zusätzliche Einträge zur Steuerung des SAT, die gemeinsam mit der Aktivierung / Deaktivierung des SAT angepasst werden sollten:

```
# ================================================================
# CAP Management      -      Service Configuration      -     SCCP
# ================================================================
# WARNING: Please don't change values manually, use CAP Management
# ----------------------------------------------------------------

..
# Flag sets legacy mode operation for the SCCP to SCC direction;
# 1 (legacy mode set) is default value
# Uncomment subsequent entry to activate SAT!
#CFR_SATLegacyMode = 0


# ================================================================
# CAP Management      -      Service Configuration       -     SCC
# ================================================================
# WARNING: Please don't change values manually, use CAP Management
# ----------------------------------------------------------------

..

# Flags set legacy mode operation for the SCC - Switch connection;
# 1 (legacy mode set) is default value
# Uncomment subsequent entries to activate SAT!
# Computing Function to Switching Function (SCC to switch)
#CFR_SATLegacyMode = 0
# Switching Function to Computing Function (switch to SCC)
#SFR_SATLegacyMode = 0

# Flag for SAT tuning (populate SAT cache on MonitorStart)
# Regularly it is recommended to keep the default value 1
#noMStartSATMode = 0
```

Remark: special setting (for customer EON) - explanation and desription only in english

The following text need to insert into the **`SatServer.cfg`** (im Verzeichnis `<InstDir>/config/<host>/admin/sat_svc`):

```
DomainCacheMode = 1

DBCache = 7
```

DomainCacheMode: the value can be either 1 or 2:
The DomainCacheMode configuration adds special rules to convert

dialing numbers to canonical format even if the number is not in the database. The conversion is based on the VNR prefix.

Mode 1 (DOMAIN_CACHE_PREFIX_BY_SCC) goes through all the SCC's domains and if the number starts with the VNR code of the domain, we have a match and this domain is used for the conversion.

Mode 2 (DOMAIN_CACHE_FIXED_LENGTH_BY_SCC) uses hashmaps. The length of the VNR number is fixed (vncLength) and the domain is looked up in the hashmap by a key pair which holds the scc id and the first vncLength characters of the dialing number.

Mode 1 is more general and faster, mode 2 not recommended.

DBCache: cache CAP management data, possible values:

1 - cache domain entries

2 - cache scc entries

4 - cache scc list

The values can be combined (added) to cache multiple data types.

A.2.16 Keine Umlaut via CSTA (ASN.1)

Remark: onyl english description is available

The CAP can deliver accent characters via CSTA II ASN1, but since that is not CSTA conform, tha’s why the following settings can be applied for applications, which want to be ASN1 conform.

It is possible to convert the CallInfo (and ExtendedCallInfo) fields in ACL events to a 7 bit only ASCII string. There are 3 options which affect the conversion and two of them is new and available only from this version. These options must be set

in ca4000.cfg file.

1. USE_ACCENTED_CHARACTERS=0

This option should work on all switch version. It turns on the the conversion to 7bit call info (and extended call info) conversion without that the call info received from swith is sent out on the CSTA side without modification. The default value is 1 (when there's no conversion). To turn it on please set it to 0 as above.

2. CALLINFO_CONVERT_MODE=w1252

This option only affects the callinfo conversion (V3 basically, but the specification allows it on later versions). It can have 3 values:
off - no callinfo conversion
w1252 - windows codepage 1252 mode where the chars above 127 are mapped to a similar lower char. (For example Ü -> U, Á -> A etc.) Unmappable chars (for exmple 0x81 or 0xfe) are changes to the default char (see option 3.)
defaultchar - all chars above 127 mapped to the default char (see option 3.) The default mode is 'defaultchar'

3. CALLINFO_CONVERT_DEFAULT_CHAR=.

Unmappable characters are changed to this one. The default value is _ (underscore).

An example configuration:

USE_ACCENTED_CHARACTERS=0

CALLINFO_CONVERT_MODE=w1252

CALLINFO_CONVERT_DEFAULT_CHAR=.

These lines can be anywhere in the config file, but if it is at the and please make sure that there's a new line after the last config entry!

A.2.17 Konfigurationsdaten für CAP Management

Alle Daten, die ausschließlich von CAP Management zur PBX-Anbindung und zur Berechtigungsprüfung genutzt werden, sind im Verzeichnis `<InstDir>\data\TelasAdmin\adminauth\capdb` abgelegt.

Das Unterverzeichnis `capdb` enthält die Authentifizierungsinformation für den Authentifizierungs-Service von OpenScape CAP Management in einer LDAP-Datenbank. Hier sind alle Informationen der autorisierten Benutzer (z. B. Benutzertyp, Passwort und Zeitstempel) eingetragen. Weiterhin sind die Zuordnung der PBX zu IP-Adresse und Port des zuständigen CAP Call Control Service-Prozesses dort abgelegt.

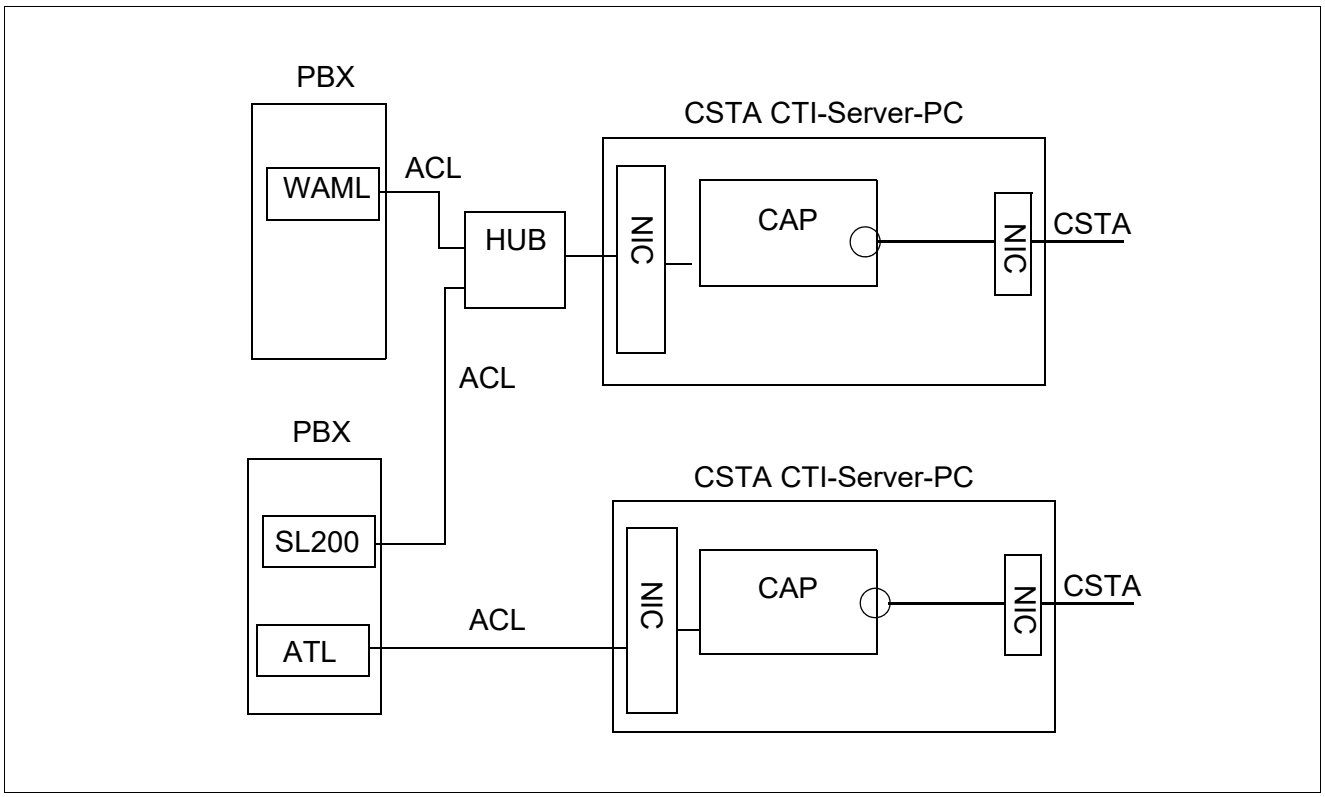
7	Die Dateien werden komplett über die OpenScape CAP Management-Bedienoberfläche verwaltet. Eine Änderung in einer dieser Dateien mit einem Texteditor ist nicht zulässig.

B Verbindung HiPath 4000 mit Server-PC

B.1 Anschlussmöglichkeiten des Server-PC

Die HiPath 4000 verfügt über integrierte Ethernet Server-Busanschlüsse. Damit können Sie den OpenScape CAP Server-PC über eine Ethernet TCP/IP-Verbindung anschließen. Bei einer TCP/IP-Verbindung handelt es sich um eine logische Datenverbindung zwischen zwei Adressen, die sich jeweils aus einer Portnummer (für TCP) und einer logischen IP-Adresse zusammensetzen. Bei dieser Konfiguration können über eine physikalische Adresse (die TCP-Portnummer) mehrere logische Ziele erreicht werden. Über das TCP-Protokoll wird dabei sichergestellt, dass die übertragenen Datenpakete die logische IP-Zieladresse in der richtigen Reihenfolge und ohne Datenverlust erreichen. Falls ein Fehler auftritt, wird die Verbindung komplett abgebrochen.

Das nachfolgende Diagramm zeigt mögliche Anschaltungen an eine HiPath 4000:



Der CSTA CTI-Server kann grundsätzlich auch mit einer einzigen LAN-Karte konfiguriert werden, wobei dies jedoch nicht empfohlen wird.

B.1.1 Anschluss an Atlantic LAN

Als physikalische Schnittstelle zwischen der HiPath 4000 und OpenScape CAP dient eine ungeschirmte Twisted Pair-Leitung zum internen Ethernet LAN. Das interne ("Atlantic") LAN stellt eine hohe Datenbandbreite zur Verfügung und ist somit ideal für die Datenkommunikation zwischen den Prozessoren der HiPath 4000 und OpenScape CAP geeignet. Das interne Ethernet LAN ist direkt über die Anschlüsse an der Rückwandplatine der HiPath 4000 verfügbar.

Sollen mehrere OpenScape CAP-Server am selben Atlantic LAN angeschlossen werden, muss jeder Server eine eindeutige IP-Adresse haben. Zusätzlich ist ein externer Hub erforderlich. Die physikalische Verbindung zum externen Hub erfolgt jeweils über ein Standard-Twisted Pair-Kabel. Bei dem externen Hub kann es sich um einen beliebigen handelsüblichen Hub mit RJ45-Ports handeln, z.B. Office Connect Ethernet Hub 4 (4 TP/RJ45-Ports) von 3Com (Herstellernummer 3C16704A). Bei den Anschlüssen des Hubs sollte es sich immer um MDI/MDIX-Switch-Ports handeln.

IP-Adressen

Der Zugriff auf die am Atlantic LAN angeschlossenen Server erfolgt über IP-Adressen (IP-Netzwerknummern plus Servernummern). Die IP-Netzwerknummer des Atlantic LAN lautet ’192.0.2.0’, womit eine Class C-Adresse definiert wird. Diese Netzwerknummer verwenden sämtliche am Atlantic LAN angeschlossenen Server.

Die Komponenten haben feste IP-Adressen, und zwar wie folgt:

CC-A: 192.0.2.1
CC-B: 192.0.2.2
ADS/ADP: 192.0.2.3

Die folgenden Adressbereiche sind für externe Anwendungen reserviert:

ext. ACD-Server: 192.0.2.10 - 192.0.2.19 (Standard: 192.0.2.16)

OpenScape CAP: 192.0.2.23 - 192.0.2.29 (Standard: 192.0.2.25)

Sollen mehrere OpenScape CAP-Server am selben Atlantic LAN angeschlossen werden, muss jeder Server eine eindeutige IP-Adresse haben. Zusätzlich ist ein externer Hub erforderlich. Die Adresse des ersten CAP-Servers lautet standardmäßig 192.0.2.25. Für jeden weiteren Server wird die Adressnummer um 1 erhöht (192.0.2.26, 192.0.2.27 usw.). Insgesamt können maximal 5 Server angeschlossen werden.

B.1.2 Anschluss an der SL200- oder WAML-Baugruppe

Im Atlantic LAN sind für die HiPath Komponenten feste IP-Adressen definiert. Somit ist es nicht möglich, im selben LAN weitere PBXen zu konfigurieren. Diese Beschränkung kann durch Verwendung einer SL200-Baugruppe (bei HiPath 4000) oder einer WAML-Baugruppe (bei HiPath 4000) umgangen werden.

Über diese LAN-Baugruppen, deren IP-Adressen frei konfigurierbar sind, kann auf das Atlantic LAN zugegriffen werden.

7	Es ist nicht möglich, gleichzeitig eine WAML- und eine SL200-Baugruppe einzurichten.

B.2 Konfiguration der HiPath 4000-Software

B.2.1 Konfiguration der Verbindung zur SL200-Baugruppe (nur bei HiPath 4000)

Bevor Sie mit der Konfiguration der SL200-Baugruppe beginnen, muss das Atlantic LAN richtig konfiguriert sein.

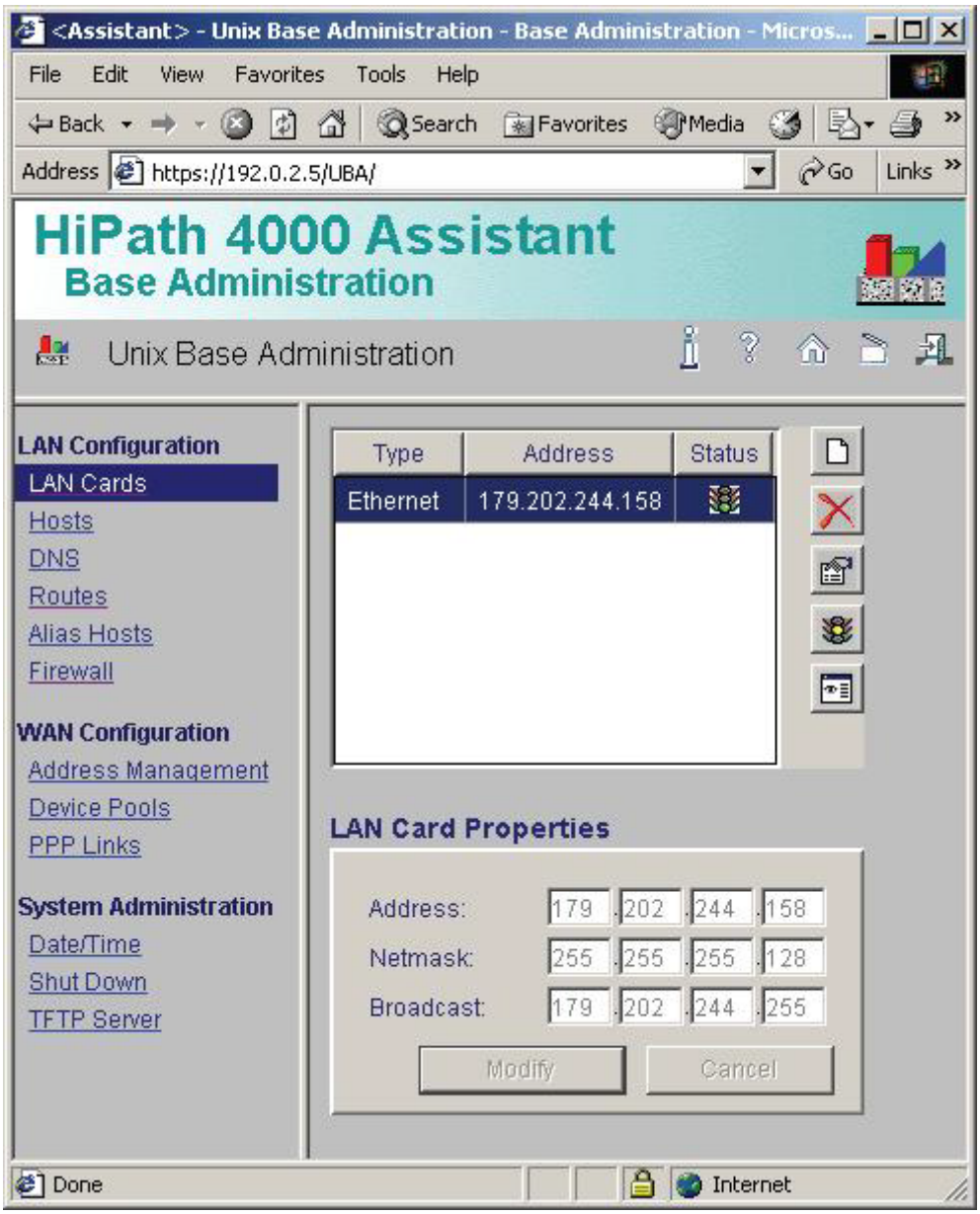
Zum Einrichten der SL200-Karte für den Einsatz mit CA4000 ist das UnixWare Service-Tool 'Unix Base Administration' (UBA) zu verwenden. Sie finden das Service-Tool UBA im HiPath 4000 Assistant unter LaunchPad im Ordner 'Base Administration' (Basis-Administration).

Wenn Sie die LAN-Einstellungen für die SL200 in UBA über 'LAN Cards' (LAN-Karten) und 'Routes' (Richtungen) bereits richtig konfiguriert haben, fahren Sie mit dem Abschnitt 'Firewall-Einstellungen' fort.

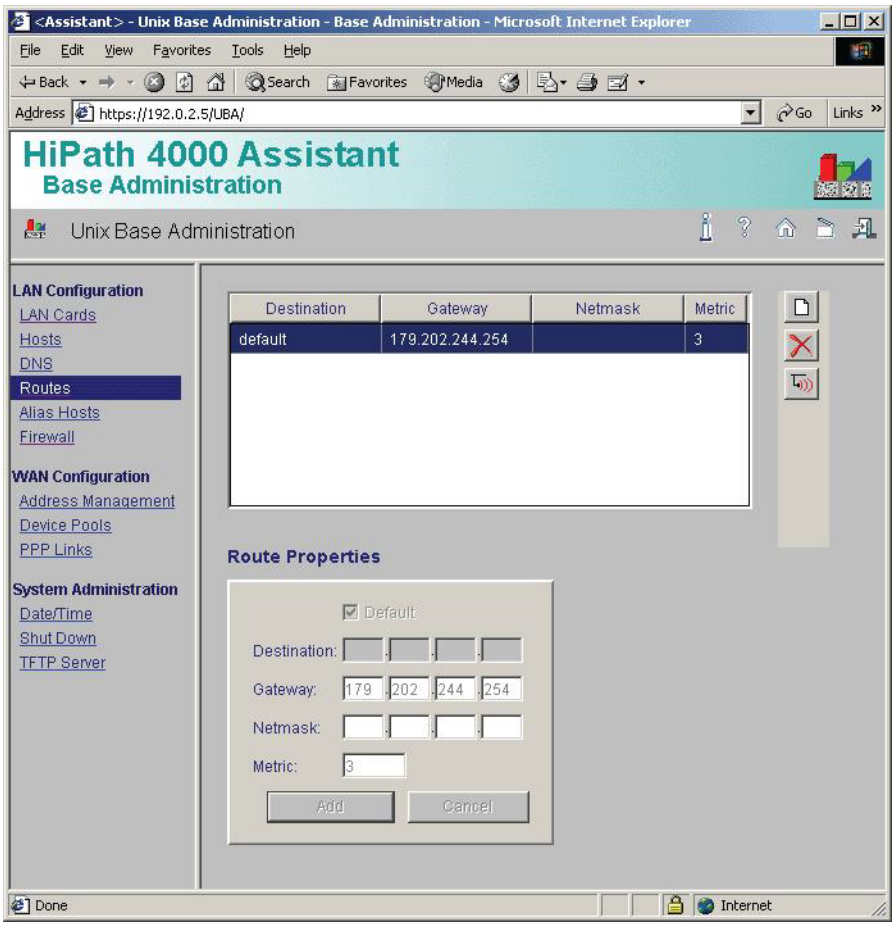
Einrichtung mit dem HiPath 4000 Assistant und UBA

Rufen Sie auf einem PC mit Direktanschluss zum Atlantic LAN einen Webbrowser auf. Gehen Sie zum öffentlichen Bereich des HiPath 4000 Assistant unter http://192.0.2.5 und befolgen Sie die Anweisungen unter der Verknüpfung 'Client Preparation' (Vorbereitung des Clients). Rufen Sie anschließend mithilfe des Browsers das Tool UBA unter dem folgenden Link auf: https://192.0.2.5/UBA

Sie müssen nun als erstes die LAN-Karte konfigurieren. Klicken Sie hierfür unter 'LAN Configuration' (LAN-Konfiguration) auf den Menüpunkt 'LAN Cards' (LAN-Karten). Die Tabelle im rechten Rahmen sollte leer sein (gibt es bereits einen Eintrag, wurde die LAN-Karte schon eingerichtet und muss nicht nochmals eingerichtet werden). Klicken sie auf das Symbol 'New LAN Card Configuration' (oben rechts im rechten Rahmen) und tragen Sie für IP-Adresse, Netmask und Broadcast die Werte ein, die Ihnen der Systemadministrator für die SL200 genannt hat. Fügen Sie die Karte zum Eintrag hinzu. Der neue Eintrag erscheint dann nach einigen Sekunden in der Tabelle. Starten Sie anschließend UnixWare per 'ShutDown' oder durch Eingabe von 'shutdown -y -g0' als privilegierter Benutzer in einer Unix-Shell neu.



Sobald der Neustart von UnixWare abgeschlossen ist und sämtliche UnixWare-Dienste gestartet wurden, rufen Sie UBA auf und wählen Sie den Menüpunkt ’Richtungen’. Klicken Sie auf das Symbol ’New Route’ (Neue Richtung) (oben rechts im rechten Rahmen). Aktivieren Sie das Kontrollkästchen ’Default’ (Standard), tragen Sie den Wert für das Gateway ein, den Sie vom Systemadministrator bekommen haben und geben Sie bei ’Metric’ (Metrik) 3 ein. Bei ’Netmask’ muss normalerweise kein Wert eingetragen werden. Fragen Sie im Zweifelsfall Ihren Systemadministrator, Klicken Sie für die Richtung auf ’Add’ (Hinzufügen/Einrichten), warten Sie, bis sie in der Tabelle erscheint und starten Sie UnixWare anschließend neu.

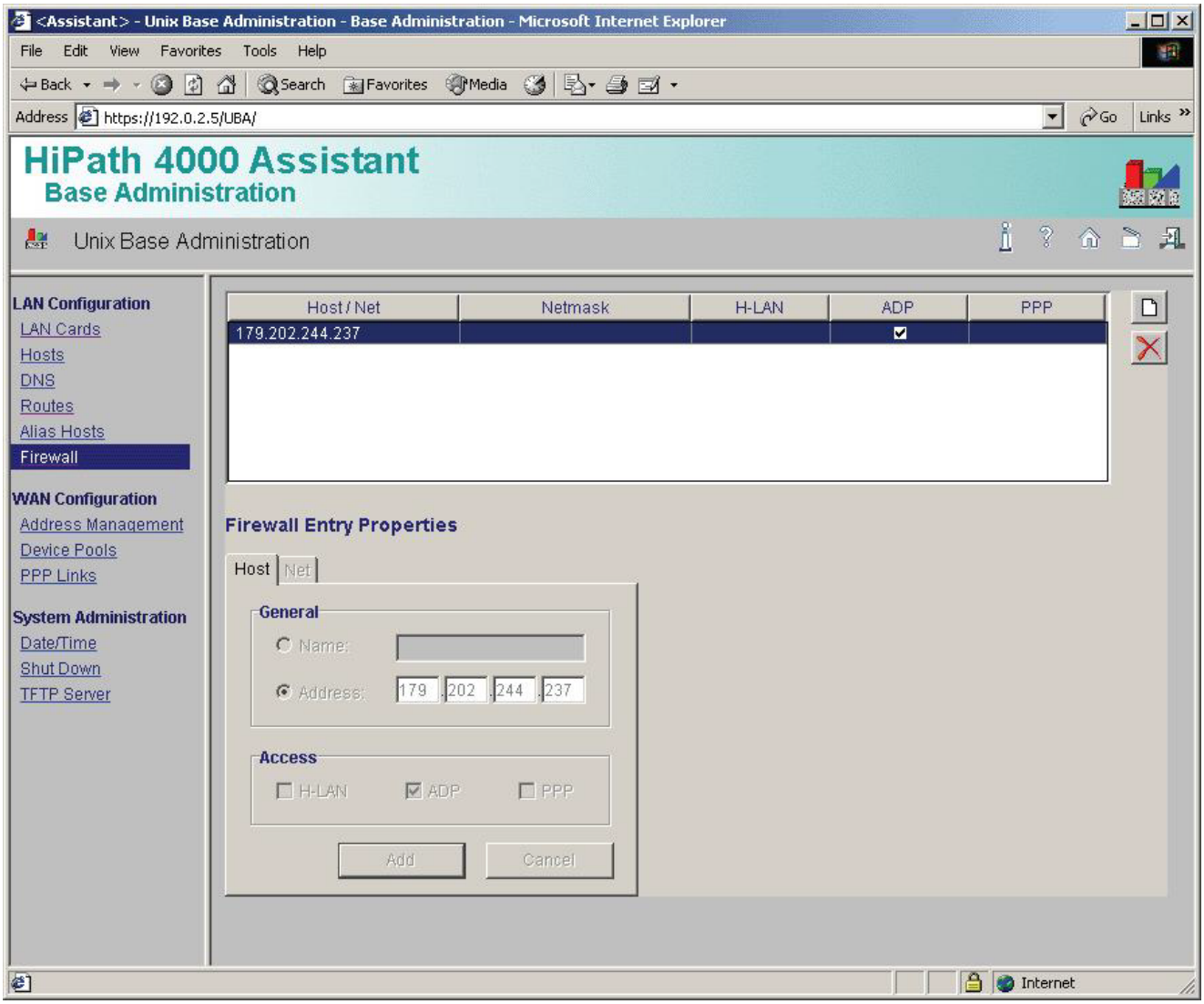


Firewall-Einstellungen

Nachdem die LAN-Konfiguration für die SL200 über die Optionen ’LAN Cards’ (LAN-Karten) und ’Routes’ (Richtungen vorgenommen wurde und UnixWare neu gestartet wurde, müssen die folgenden Schritte durchgeführt werden:

1. Wählen Sie unter ’LAN Configuration’ (LAN-Konfiguration) die Option ’Firewall’.Nach einigen Sekunden werden im rechten Rahmen die Firewall-Einstellungen angezeigt.
2. Im Feld ’New Firewall Entry’ (Neuer Firewall-Eintrag) ist standardmäßig ’Host’ eingestellt. Klicken Sie auf die Option ’Adresse’.
3. Geben Sie die IP-Adresse des Rechners ein, von dem aus auf CA4000 zugegriffen werden soll.
4. Im Feld ’Access’ (Zugang/Zugriff) darf hierbei nur die Option ’ADP’ markiert sein.
5. Klicken Sie auf die Schaltfläche ’Add’ (Hinzufügen/Einrichten).

6. Nach wenigen Sekunden erscheint in der Tabelle Host / Net oben im rechten Rahmen eine neue Zeile.
7. Falls zusätzliche Workstations eingerichtet werden müssen, klicken Sie auf das Symbol 'New Firewall Entry' rechts oben und wiederholen Sie die Schritte 2-6 für jede weitere Workstation. Sobald ein Rechner zur Liste hinzugefügt wurde, sollte er für den Einsatz mit CA4000 zur Verfügung stehen.



B.2.2 Konfiguration der Verbindung zur WAML-Baugruppe

Vor dem Konfigurieren der WAML-Baugruppe muss das Atlantic LAN richtig konfiguriert werden und über ein LAN-Kabel mit der WAML-Baugruppe verbunden sein.

Zur Konfigurierung der WAML-Baugruppe für die LAN-Kommunikation kann der AMO LANC verwendet werden. In einer HiPath-Anlage können maximal 4 WAML-Baugruppen eingerichtet werden.

B.3 Anschluss des CAP PCs an die HiPath 4000

Dieser Vorgang umfasst den Anschluss der Verbindungskabel und das Ausführen eines Ping auf die HiPath 4000. Führen Sie folgende Schritte durch:

1. Schließen Sie an der Adapterkarte auf der Rückseite des CTI-Servers ein RJ45-Kabel an.
2. Schließen Sie das andere Ende des RJ45-Kabels an der Hub-C/SL200/WAML-Karte in der HiPath 4000.
3. Führen Sie ein Ping auf die IP-Adresse der HiPath 4000 durch. Geben Sie hierzu folgende Zeichenfolge in der Eingabeaufforderung ein:

   ping 192.0.2.3 (bei einer Verbindung zum Atlantic LAN)
4. Falls eine Verbindung besteht, erhalten Sie eine Rückmeldung von der HiPath 4000. Andernfalls überprüfen Sie die Verbindungen und wiederholen Sie das Ping. Besteht das Problem weiterhin, tauschen Sie das Kabel aus und wiederholen Sie das Ping.

B.3.1 Konfiguration der ACL-Verbindung

Für einen ordnungsgemäßen Betrieb des Systems müssen OpenScape CAP sowie die HiPath 4000 speziell konfiguriert werden, d.h. es müssen jeweils bestimmte Parameter gesetzt werden.

Die Parametrisierung der HiPath erfolgt mithilfe von MML-Kommandostapeln (AMOs).

Sollen für dasselbe HiPath-System mehrere Gateways konfiguriert werden, müssen hierfür in der HiPath 4000 jeweils eigene ACL-C-Anwendungsparameter gesetzt werden.

Die folgenden Schritte müssen bei jeder Installation ausgeführt werden:

1. Festlegen der Höchstzahl von ACL-C-Anwendungen
   AMO: DIMSU
   Parameter: DGV:
2. Festlegen der Höchstzahl überwachter Geräte
   AMO: DIMSU (DIMensioning of features, Switching Unit)
   Parameter: ACDMONID, Anzahl überwachter ID-Gruppen (z.B. ACD-Agenten - nur ACD-G)

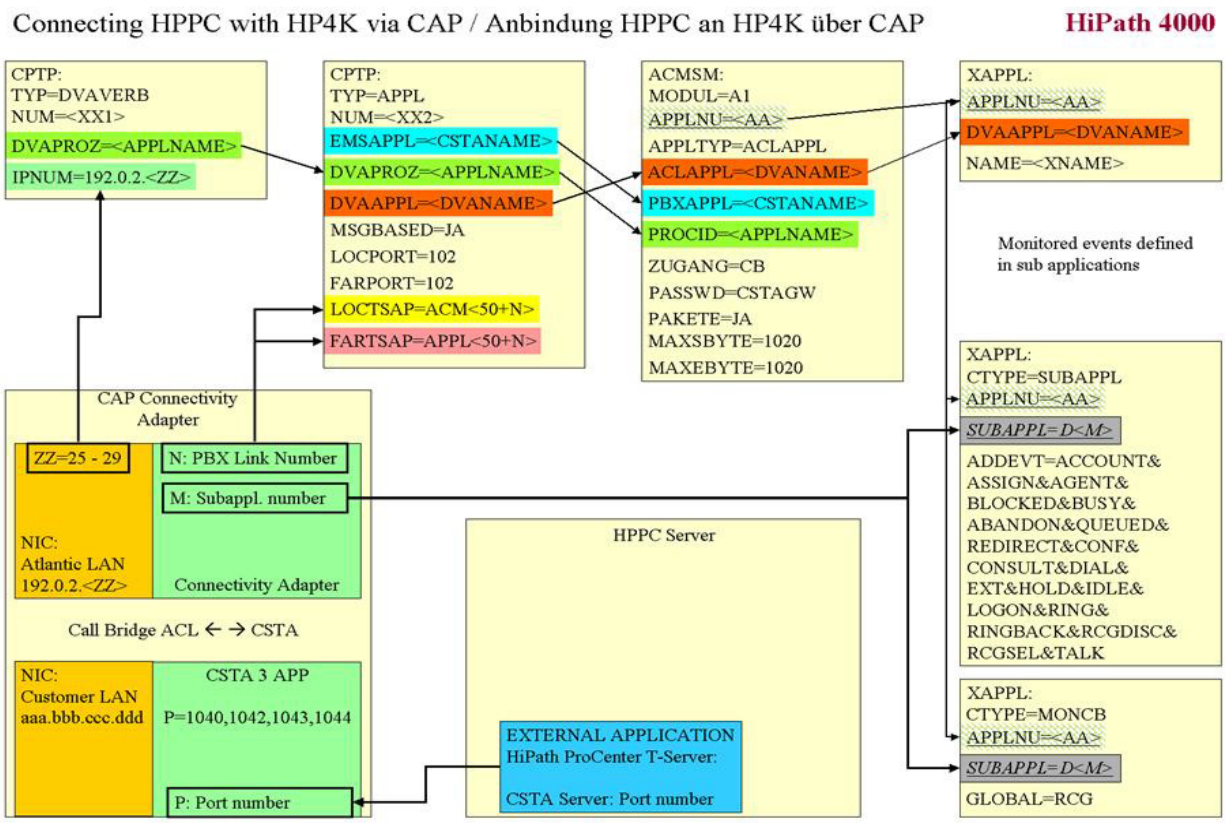
Zulässige Höchstzahl überwachter Geräte. Versucht die Anwendung, über die zulässige Höchstzahl überwachter Geräte hinaus Monitorpunkte zu setzen, werden diese Versuche zurückgewiesen.

3. Festlegen der Call Processing-Timer
   AMO: CTIME, kundenspezifische CP-Timer, Switching Unit
   Administration der Call Processing-Timer, die vom "MakeCall"-Event ausgewertet werden.
4. Konfiguration der physikalischen Anschlüsse für die TCP/IP-Datenkommunikation
   AMO: CPTP, Kommunikationsparameter für TCP/IP-Anschluss
   Typ: DVAVERB
5. Festlegen der Schnittstellenparameter (Transport-Adresse)
   AMO: CPTP, Kommunikationsparameter für TCP/IP-Anschluss
   Typ: APPL
6. Konfiguration von ACL Manager-Parametern
   AMO: ACMSM, ACL Manager-Kommunikationsparameter
   APPLTYP=ACLAPPL
7. Konfiguration von Parametern für Unter-Anwendungen
   AMO: XAPPL, DVA - Anwendungs-ACL
8. AMO-Anwendungsadministration
   AMO: APC

Bestimmte mittels AMOs eingestellte Parameter müssen mit den in der OpenScape CAP-Konfiguration eingestellten Werten identisch sein.

Dies betrifft insbesondere folgende Parameter:

Passwort	(ACMSM)
Blockgröße bei Senden/Empfangen	(ACMSM)
IP-Adresse des Gateways	(CPTP)
Generierte ACL-C-Events	(XAPPL)
ID der Unter-Anwendung	(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 Einrichtungsstapel der HiPath 4000 zum CA

Der Konfigurationsstapel der HiPath 4000 enthält drei Parameter, welche für die Kommunikation mit dem CAP CA-Server von Bedeutung sind:

- IP Adresse des CAP CA-Server PC
- PBX Link Nummer
- PBX Sub Appl Nummer

7	Die Sub Appl Nummer muss zwischen D17 und D32 sein, um Devicen monitorieren zu können.

IP Adresse des CAP CA-Server PC

Wenn man es richtig macht, wird hier die entsprechende IP-Adresse eingetragen. Allerdings ist sie derzeit im Zusammenspiel mit der CA ohne Bedeutung. Sie wird nur dann verwendet, wenn die HiPath 4000 die TCP/IP-Verbindung selbständig aufbauen würde.

PBX Link Nummer

Sie muss in der CA-Konfiguration im AMO CPTP:APPL übereinstimmen. Der entscheidende Parameter in dem AMO ist die ACM-Nummer und die APPL-Nummer. Sie wird errechnet aus dem Vorgabewert „50“ plus die PBX Link Nummer (ACM 50 + PBX Link Nummer; APPL 50 + PBX Link Nummer).

Beispiel: PBX Link Nummer = 5 >>> ACM55;APPL55;

PBX Sub Appl Nummer

Sie muss in der CA-Konfiguration und im AMO XAPPL übereinstimmen. Der entscheidende Parameter in dem AMO ist die Sub-Applikationsnummer „Dxx“.

Beispiel: PBX Sub Appl Nummer = 25 >>> D25

B.3.2.1 HiPath 4000 Stapel für CA4000

```
EINR-CPTP:DVAVERB,55,"CAPCONN1","<IP-CA4000-PC>";
EINR-CPTP:APPL,55,"CAP1","CAPCONN1","CAPAPP1",JA,102,102,"ACM55","APPL55";
/*
EINR-XAPPL:55,"CAPAPP1","CAP1",,J;
AEND-XAPPL:SUBAPPL,55,D25,ALL;
CHANGE-XAPPL:MONCB,55,D25,RCG,;
/*
EINR-ACMSM:,55,ACLAPPL,"CAPAPP1","CAP1","CAPCONN1",CB,"CSTAGW",J,1020,1020;
/*
/* Einstellung der Signalisierungszeit (hier 15 Sekunden) beim
/* "MakeCall" an der Ruf initierenden Nebenstelle für analoge
/* Endgeräte
AEND-CTIME:ARTSWU=CPTIME1,DGVPROAB=15;
/*
/* EXEC-UPDAT:BP,ALL;
/* EXEC-UPDAT:A1,ALL
/* EXEC-REST:SYSTEM,RELOAD;
```

B.3.2.2 Einrichtung eines HiPath 4000-Endgeräts für den XML Phone Service

Um XML Phone Services nutzen zu können, muss mindestens eine freie Namenstaste an einem Endgerät zur Verfügung stehen. Ist dies nicht der Fall, so kann im AMO-TAPRO die Funktion einer Taste geändert werden.

Beispiel:

```
AENDERN-TAPRO:TLNNU=<Nebenstelle>,TD<Tastennummer_xx>=NA;
```

```
AENDERN-TAPRO:TLNNU=27486,TD07=NA;
```

Um eine OpenScape CAP XML Phone Service als eine "non voice" Applikation einzurichten, verwenden Sie AMO-ZIEL

Beispiel:

```
EINRICHTEN-ZIEL:TYP=NA,QLRUFNU=<Nebenstelle>,TASNU=xx,TZLRUFNU=C13999xx;
```

```
EINRICHTEN-ZIEL:TYP=NA,QLRUFNU=27486,TASNU=07,TZLRUFNU=C13999 07;
```

Die URL, welche mit der vorkonfigurierten Taste assoziiert ist, wird in der CAP Management GUI dem Device zugeordnet.

Weitere Einstellungen in der HiPath 4000

Der "Repdail Pause Timer" in der "Switching Unit" muss auf den niedrigsten Wert eingestellt werden. Verwenden Sie dazu den AMO CTIME.

Beispiel:

```
AENDERN-CTIME:ARTSWU=CPTIME2,REPAUSE=1;
```

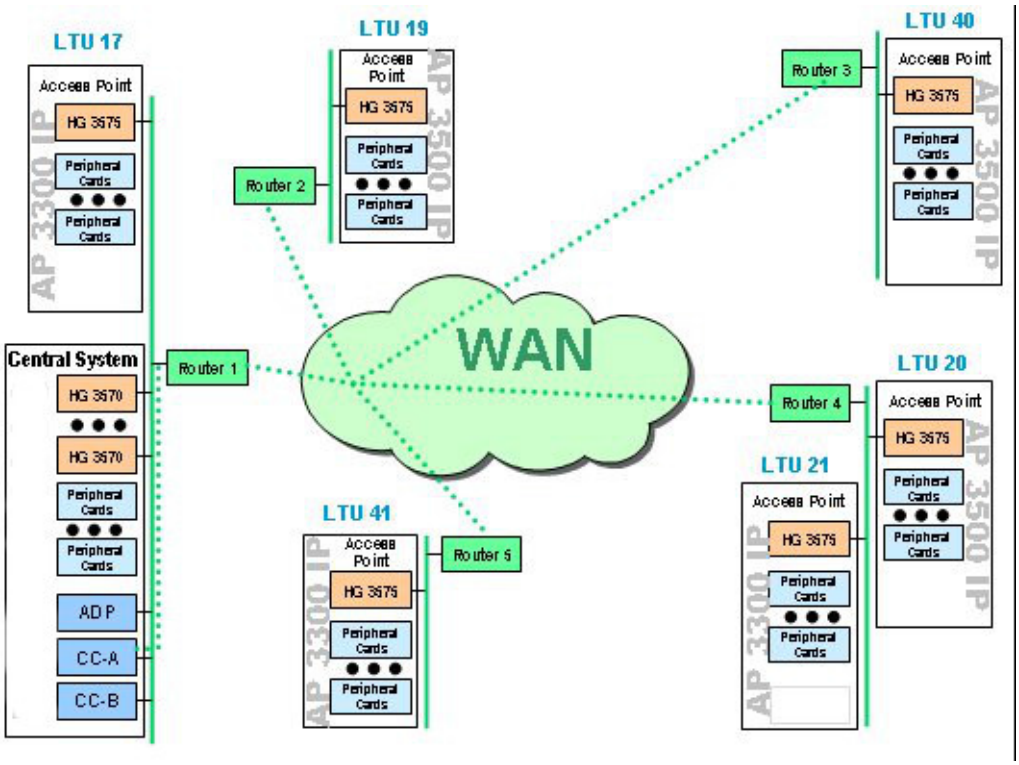
B.4 HiPath / OpenScape 4000 mit AP Emergency

Eine detaillierte Beschreibung des AP Emergency Features aus HiPath / OpenScape 4000 Sicht einschliesslich der auf HiPath / OpenScape 4000 Ebene erforderlichen HW-Komponenten und SW-Einstellungen würde sicherlich den Rahmen dieser Beschreibung sprengen.

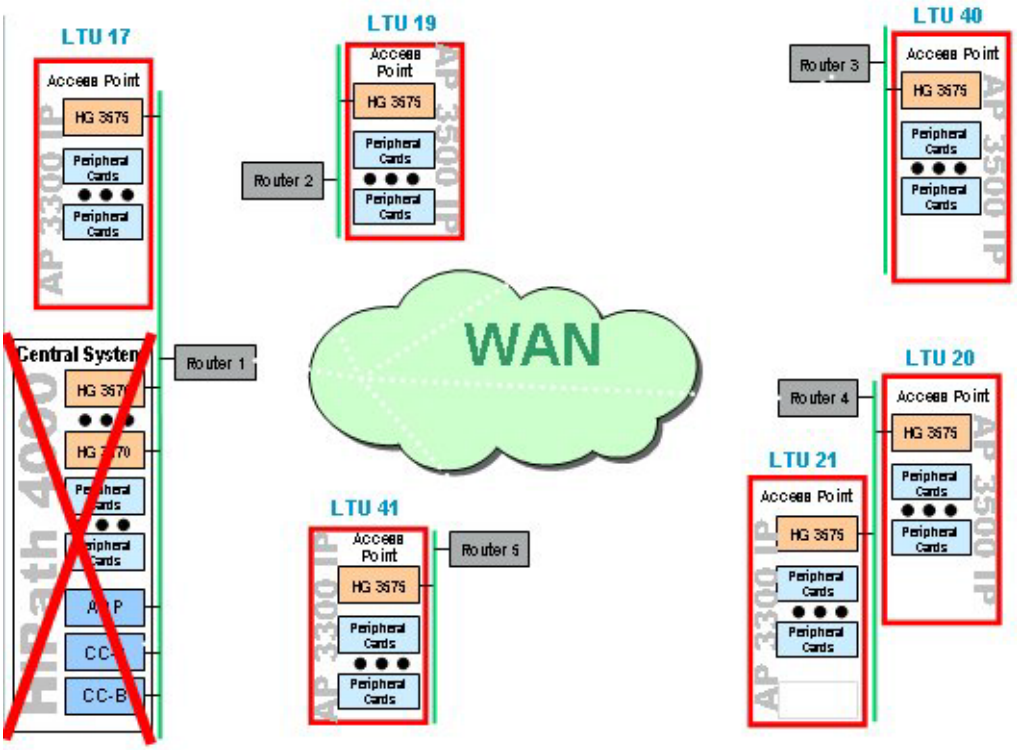
Deshalb sollen an dieser Stelle nur grob die funktionellen Unterschiede zwischen einer HiPath / OpenScape 4000 mit und ohne AP Emergency Konfiguration skizziert werden. Wer an detaillierteren Informationen interessiert ist, dem wird die mehr als ausführliche Beschreibung im HiPath / OpenScape 4000 Servicehandbuch (Komplexe Lösungen - IPDA & APE) empfohlen.

B.4.1 Zustand vor AP Emergency

Das HiPath 4000 V1.0 Feature IPDA (IP Distributed Architecture) erlaubte es bisher schon, Access Points (Rahmen für HiPath 4000 Standard Anschlussbaugruppen) über ein IP-Netz zu verteilen. Die Teilnehmeranschlüsse an diesen Access Points werden dabei genau so behandelt, als wären sie, wie bisher üblich, direkt an einem HiPath 4000 Server angeschlossen. Auch die Administration der gesamten über IP verteilten Komponenten erfolgt als ein System über einen Einstiegspunkt des HiPath 4000 Servers.



Kam es zum Ausfall beteiligter Komponenten (z.B. Ausfall des HiPath 4000 Servers, Störung des IP-Netzes), konnten bislang auch die an den abgesetzten Access Points angeschlossenen Teilnehmerendgeräte nicht mehr betrieben werden (auf die existierende Umgehungslösung mittels einer Modem Verbindung zwischen HiPath 4000 Server und Access Point über PSTN soll hier nicht eingegangen werden).



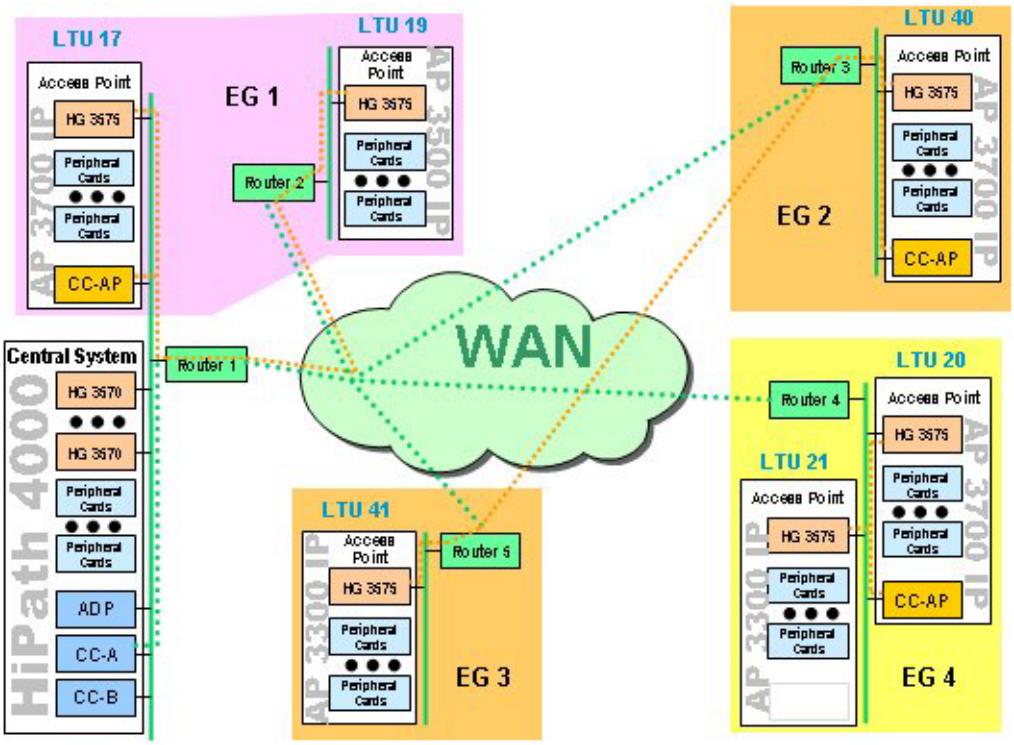
B.4.2 Verbesserungen durch AP Emergency

Das mit HiPath 4000 V2.0 freigegebene AP Emergency Feature soll helfen, die oben beschriebene eingeschränkte Erreichbarkeit bei Komponentenausfällen zu verbessern.

Bei Ausfall des HiPath / OpenScape 4000 Servers oder des IP-Netzes soll möglichst noch die lokale Erreichbarkeit der an das AP-Shelf angeschlossenen Endgeräte gewährleistet werden (d.h. die Teilnehmer desselben AP-Shelfs können sich untereinander noch erreichen, aber z.B. nicht mehr einen Teilnehmer an einem Server-Host-Shelf, also einem Non-AP-Shelf).

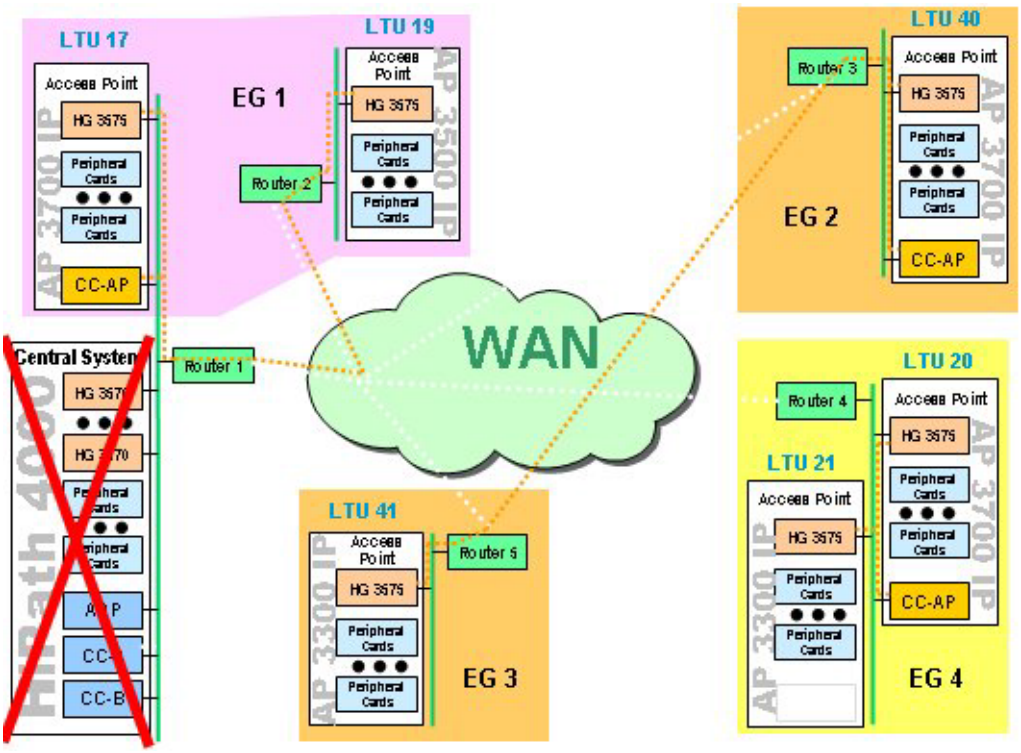
HiPath / OpenScape 4000 AP Emergency Konfiguration

- HiPath / OpenScape 4000 Server mit über IP abgesetzten Access Points nebst erforderlichen APE spezifischen HW/SW-Komponenten



Ausfall des HiPath / OpenScape 4000 Servers

- alle lokal (d.h. an Shelves innerhalb des HIPath / OpenScape 4000 Servers) angeschlossenen Endgeräte sind nicht mehr erreichbar.
- Dagegen überleben alle Access Points den Ausfall, weil jeder AP seinen zugeordneten CC-AP erreichen kann.

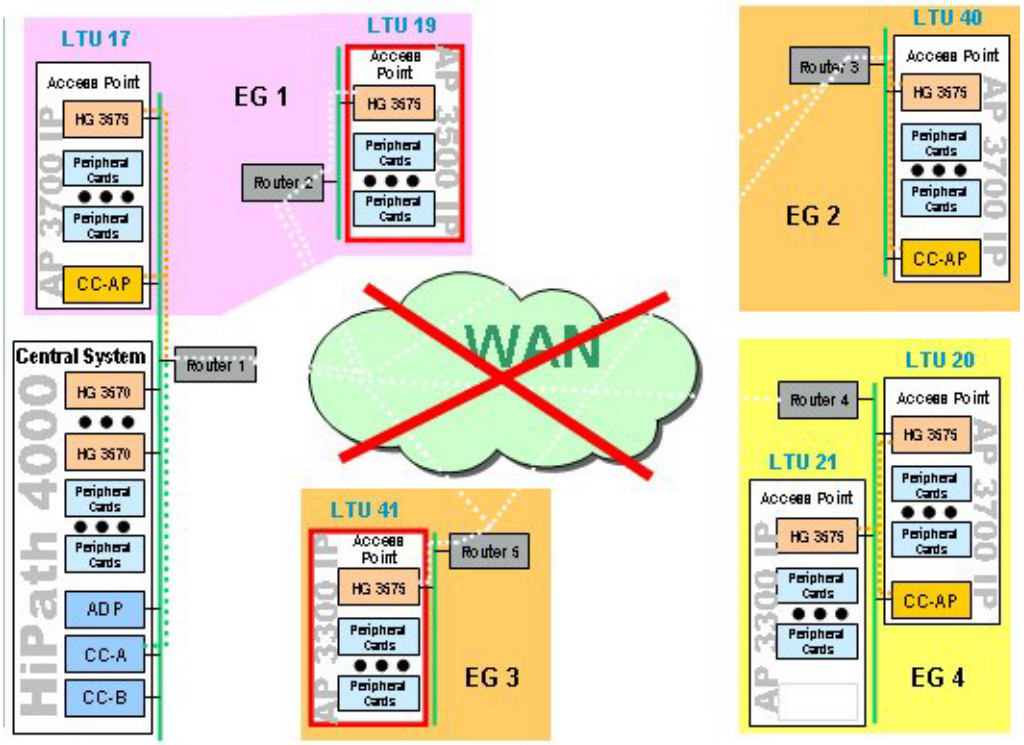


(Komplett- oder Teil-) Ausfall des WAN

Es überleben jeweils nur die Access Points, die

- noch ihren zugeordneten CC-AP erreichen können (im Beispiel AP20, AP21, AP40) oder aber
- direkt mit dem HiPath / OpenScape 4000 Server verbunden sind (im Beispiel AP17).

Die restlichen Access Points fallen total aus (im Beispiel AP19, AP41).



Glossar

A

ACD

Siehe *Automatic Call Distribution*.

ACD-Gruppe

Eine Gruppe von ACD-Agenten, die für die Bearbeitung bestimmter Anrufe zuständig sind (z.B. Anrufe zu Börsengeschäften, zu Krediten oder zur Flugbuchung). Siehe auch *Automatic Call Distribution*.

Agent

Ein Kundendienst-Mitarbeiter, der über eine Agenten-Workstation Kundenanrufe tätigt oder empfängt.

Agenten-Workstation

Eine Workstation mit einem am HiPath 4000-System angeschlossenen Telefon und einem Terminal mit einer Verbindung zum LAN.

ANI

Siehe *Automatic Number Identification*.

Answer Call

Ein Dienst, bei dem ein rufendes Gerät (z.B. bei einem geparkten Anruf) abgefragt und anschließend der gehaltene Teilnehmer umgekoppelt wird.

Anwendungs-Lieferant

Eine Firma, die Anwendungsprogramme vertreibt, die in der LAN-Umgebung laufen, in welche die HiPath 4000 eingebunden ist.

AP

Access Point - Rahmen zur Aufnahme von HiPath / OpenScape 4000 Standard-Anschlussbaugruppen.

AP Emergency (APE)

Access Point Emergency (siehe Abschnitt B.4, “HiPath / OpenScape 4000 mit AP Emergency”*)*.

API

Siehe *Application Program Interface*.

Application Connectivity Link (ACL)

Siehe *Connectivity Adapter HiPath 4000 Application Connectivity Link*.

Application Program Interface (API)

Die Software, über die das LAN die HiPath 4000 veranlasst, bestimme Telefonie-Funktionen (z.B. den Aufbau von Gesprächsverbindungen oder die Übergabe von Gesprächen) auszuführen.

Automated Outbound Dialing (automatisierte Wahl)

Ein Leistungsmerkmal, mit dem ein Agent über eine Telefonie-Anwendung einen Anruf zu einem Kunden tätigen kann.

Automatic Call Distribution (ACD)

Ein Systemleistungsmerkmal, mit dem sich große Mengen kommender Anrufe, die über eigens eingerichtete Leitungen eingehen, effizient im System verteilen lassen.

Automatic Number Identification (ANI)

Ein Leistungsmerkmal, das im digitalen Telefonnetz zur Verfügung steht und Benutzern der HiPath 4000 die Identifizierung externer Anrufer ermöglicht. An der HiPath 4000 angeschlossene Agenten können über ANI Informationen zum Anrufer ablesen und sind damit besser auf das Gespräch vorbereitet.

C

Call

Sämtliche Verbindungen zwischen zwei oder mehr Teilnehmern, z.B. eine Verbindung zwischen einer kommenden Amtsleitung und einer Nebenstelle oder zwischen zwei oder mehr Nebenstellen.

Call Center

Ein Kundenservicezentrum, bei dem die Kontaktaufnahme per Telefon erfolgt. Call Center-Mitarbeiter nutzen häufig Terminals, um auf Datenbanken mit Informationen zuzugreifen.

Call Handling Services

Dienste, bei denen ein Agent über die Telefonie-Anwendung Anforderungen wie Make Call, Clear Connection, Consultation Call, Transfer Call und Answer Call absetzen kann.

CC-AP

Common Control Access Point - Spezielle HiPath / OpenScape 4000 Hardware in Access Points, die für die lokale Survivability (bei Ausfall des HiPath / OpenScape 4000 Servers oder bei Ausfall des IP-Netzes) der am AP- Shelf angeschlossenen Teilnehmerendgeräte sorgt.

Clear Connection

Ein Dienst, mit dem eine Gesprächsverbindung bei einem bestimmten Gerät ausgelöst wird.

Connectivity Adapter HiPath 4000 Application Connectivity Link

Eine synchrone bidirektionale Kommunikationsverbindung, mittels derer die HiPath 4000 über den Telefonie-Server an das LAN angeschlossen wird.

Connectivity Adapter HiPath 4000

Ein Unify-Produkt, mit dessen Hilfe sich ein HiPath 4000-System in verschiedene LAN-Umgebungen einbinden lässt.

Computer Supported Telephony Application (CSTA)

Ein von der ECMA (European Computer Manufacturers Association) entwickelter Standard zum Anschluss von Computern an Telefonanlagen.

Computer Telephony Integration (CTI)

Eine Schnittstelle, über die Anwendungen im LAN Telefonie-Funktionen in der HiPath 4000 steuern und überwachen können.

Consultation Call

(1) Rückfrageverbindung (eine Verbindung, bei der der Teilnehmer den Gesprächspartner auf Halten legt, um bei einem anderen Gesprächspartner Informationen einzuholen). (2) Ein Dienst, bei dem ein bestehendes Gespräch auf einem Gerät auf Soft Hold gelegt wird und dann vom selben Gerät eine neue Verbindung aufgebaut wird.

Coordinated Voice and Data Transfer

Ein Leistungsmerkmal, mit dem bei der Übergabe eines Gesprächs von einem Agenten zu einem anderen gleichzeitig Sprache und Daten übergeben werden.

CSTA

Siehe *Computer Supported Telephony Application*.

CSTA-Link

Eine Verbindung, mittels derer die HiPath 4000 am Telefonie-Server angeschlossen wird.

CTI

Siehe *Computer Telephony Integration*.

D

Dialed Number Identification Service (DNIS)

Ein Dienst im Kundennetzwerk, bei dem die Telefonie-Anwendung je nach gewählter Rufnummer entsprechende Daten an der Agenten-Workstation einblendet.

DLS

Deployment and Licensing Server

E

Enhanced Business Statistics

Ein Leistungsmerkmal, mit dessen Hilfe die Anwendung Ereignisstromdaten von der HiPath 4000 auswerten und Statistiken zu Anrufern generieren kann.

Ereignisstrom

Informationen zu Anrufen, die vom HiPath 4000-System generiert und an die Telefonie-Anwendung weitergegeben werden. Diese Informationen dienen der Telefonie-Anwendung zur Ermittlung der Agentenverfügbarkeit und zur Unterstützung von Leistungsmerkmalen wie Intelligent Answering und Coordinated Voice and Data Transfer.

I

Intelligent Answering

Ein Leistungsmerkmal, bei dem die Telefonie-Anwendung transaktions- oder kundenbezogene Daten am Monitor des Agenten anzeigt, wenn dieser einen Kundenanruf tätigt oder empfängt.

IPDA

IP Distributed Architecture - HiPath / OpenScape 4000 Architektur, bei der Access Points nicht mehr direkt mit demHiPath / OpenScape 4000 Server verbunden sein müssen, sondern über ein IP-Netz verteilt werden können.

ISA

Industry Standard Architecture.

L

Local Area Network (LAN)

Ein Kommunikationsnetzwerk mit mehreren Servern und Workstations innerhalb eines geografisch begrenzten Bereichs.

M

Make Call

Eine Kommunikationsverbindung von einer Nebenstelle zu einer anderen.

N

Network Interface Card (NIC)

Eine Baugruppe, die am Telefonie-Server angesteckt wird und den Austausch von Daten über ein Netzwerk steuert.

P

Performance-Daten

In einem Puffer gespeicherte Diagnosedaten, anhand derer sich die Systemleistung auf Basis von Verkehrsdaten auswerten lässt, die über einen bestimmten Zeitraum erfasst wurden.

Port

Eine Schnittstelle oder ein Anschlusspunkt an einem Computer oder an einem anderen Datengerät.

Profil

Eine Gruppe von Parameterwerten, mit deren Hilfe die Software individuell angepasst werden kann. So lässt sich beispielsweise das Passwort festlegen, das zum Zugriff auf das System eingegeben wird.

S

SCC

Service Call Control

SCI

Session Control Interface

T

TCP/IP

Siehe *Transmission Control Protocol/Internet Protocol*.

Telefonie-Anwendung

Ein Anwendungsprogramm, das in einem LAN ausgeführt wird und das direkt oder indirekt Telefonie-Funktionen wie etwa Rufnummernwahl, Anrufannahme und -übergabe oder die Abwicklung von Sprach- und Datenverbindungen ausführt.

Tracedaten

In einem Puffer gespeicherte Diagnosedaten, mit deren Hilfe die zwischen der HiPath 4000 und dem LAN ausgetauschten Meldungen zurückverfolgt werden können.

Traffic-Daten

In einem Puffer gespeicherte Diagnosedaten über die Anzahl von Meldungen, die innerhalb eines bestimmten Zeitraums zwischen der HiPath 4000 und dem LAN ausgetauscht wurden.

Transfer Call

Ein Dienst, mit dessen Hilfe eine gehaltene Verbindung an eine andere Nebenstelle in der CBX übergeben werden kann.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Ein Netzwerkprotokoll, das die Kommunikation zwischen Computern mit verschiedenen Hardware-Architekturen und Betriebssystemen über miteinander verbundene Netzwerken ermöglicht.

Index