INSTITUT FÜR INFORMATIK
DER TECHNISCHEN UNIVERSITÄT MÜNCHEN

Diplomarbeit

Entwicklung eines Managementkonzepts für den Dienst ”Voice over IP”

Bearbeiter:	Andreas Dirscherl
Aufgabensteller:	Prof. Dr. Heinz-Gerd Hegering
Betreuer:	Michael Brenner Martin Sailer

INSTITUT FÜR INFORMATIK
DER TECHNISCHEN UNIVERSITÄT MÜNCHEN

Diplomarbeit

Entwicklung eines Managementkonzepts für den Dienst ”Voice over IP”

Bearbeiter:	Andreas Dirscherl
Aufgabensteller:	Prof. Dr. Heinz-Gerd Hegering
Betreuer:	Michael Brenner Martin Sailer
Abgabetermin:	28. Februar 2005

Hiermit versichere ich, dass ich die vorliegende Diplomarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 28. Februar 2005

. . . .
(Unterschrift des Kandidaten)

Zusammenfassung

Voice over IP (VoIP) ist ein Verfahren, um über ein IP-basiertes Netz zu telefonieren. Zahlreiche Unternehmen sehen in dieser Technologie die Hauptantriebsfeder für ein Zusammenwachsen von Sprach- und Datenkommunikation und investieren deshalb in diese Technologie.

Die Entscheidung zum Einsatz von VoIP bedeutet aber nicht nur den Kauf der benötigten Komponenten, sondern auch die Integration in die Aufbau- und Ablauforganisation des Unternehmens. Dies betrifft unter anderem in technischer Hinsicht die Integration der telefonie- und netzspezifischen Managementfragestellungen sowie in prozeßorientierter Hinsicht die Einarbeitung der neuen VoIP-spezifischen Prozesse in bestehende Strukturen und Prozeßabläufe.

In dieser Diplomarbeit soll ein übergreifendes Managementkonzept für den Dienst VoIP entwickelt werden, das auch die konzeptionellen und planungsrelevanten Fragestellungen vor Inbetriebnahme eines VoIP-Systems beinhaltet, wobei auch betriebswirtschaftliche Aspekte zu berücksichtigen sind. Eine prototypische Realisierung dient als Beleg für die Realisierbarkeit dieses Managementkonzepts.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einführung

1.1 Einleitung

Mit der Erfindung des Fernsprechers 1861 durch Johann Philipp Reis (in Europa) und 1876 durch Alexander Graham Bell (in Amerika) hat sich die Telefontechnologie in den über 140 Jahren seit ihrer Erfindung immer weiter entwickelt und ihren Siegeszug um die Welt angetreten:
Seit Anfang des 20. Jahrhunderts existiert ein weltumspannendes Fernsprechnetz, mit dem es möglich ist, (fast) jeden Winkel der Erde telefonisch zu erreichen. Dieses Netz basierte bis weit in das 20. Jahrhundert hinein auf Analogtechnik, hatte und hat aber eine Verfügbarkeit von beinahe 100%, was für eine derartig komplexe technische Anwendung bzw. Infrastruktur ein außerordentlich guter Wert ist.

Durch die Entwicklung der Computertechnologie und neuer Verkabelungsverfahren wurden die Telefonnetze (zumindest in den Industrienationen) seit Anfang der 1980er-Jahre zu einem Großteil digitalisiert, was der Telefontechnik einen neuen Schub durch die neuen Möglichkeiten und Komfortverbesserungen gegeben hat.

Bis heute existiert für die Telefonie weltweit ein eigenes Netz, während sich auch die Datennetze für die Rechnerkommunikation durch die Einführung des Internets in den letzten Jahren rasant weltumspannend entwickelt haben.

Seit einigen Jahren laufen Bestrebungen, diese beiden Netze (langfristig) zu vereinen. Hierzu wurde für das Internet ein Dienst entwickelt, der es erlauben soll, Telefondienstleistungen über das Internet abzuwickeln: Voice over IP (VoIP).

Anfangs bestanden große Probleme in Bezug auf die Sprachqualität von VoIP, da sich das Telefonnetz und das Internet hinsichtlich der Vermittlungstechnik gravierend unterscheiden. Durch die Entwicklung von Strategien zur bevorzugten Behandlung von Sprachdaten und neuer Standards haben sich diese Anfangsprobleme aber deutlich gebessert.
Außerdem besteht die Problematik der Integration von VoIP in das Telefonnetz, da die Unternehmen und Kunden nicht bereit sind, ihre (teilweise) erst seit einigen Jahren in Betrieb befindliche Telekommunikationstechnik auf einmal auszutauschen (Investitionsschutz).

In den letzten Jahren ist die Entwicklung von VoIP-Systemen (auch unter Berücksichtigung dieser Gesichtspunkte) sehr weit fortgeschritten. Mittlerweile werden solche VoIP-Systeme in immer größerem Umfang produktiv von Unternehmen eingesetzt. Dabei erfolgt die Telefonie innerhalb des Unternehmens nicht auf herkömmliche Weise über eine eigene TK-Verkabelung, sondern über das firmeneigene IP-Netz.

Mit dem Einsatz eines VoIP-Systems ergeben sich für die Unternehmen erhöhte Anforderungen an das Management eines solchen Systems, da zum einen die grundverschiedenen Welten der klassischen Telefonietechnik und des Internets vereinigt werden und zum anderen die Managementprozesse hinsichtlich der Arbeitsabläufe und der Aufbau- und Ablauforganisation des Unternehmens umgebaut bzw. neu konzipiert werden müssen. Überdies werden sehr hohe Anforderungen hinsichtlich Verfügbarkeit und Latenz- und Laufzeiten an das Datennetz gestellt, die durch Investitionen in die Infrastruktur und geeignete Überwachungsmaßnahmen sichergestellt werden müssen.

1.2 Aufgabenstellung

In der vorliegenden Arbeit wird ein Mangementkonzept für den Dienst VoIP entwickelt, das größtenteils bei der Installation eines VoIP-Systems universell einsetzbar sein soll, wobei Unternehmensspezifika - wie bei jeder Produkteinführung - im Rahmen eines Customizingverfahrens berücksichtigt werden.

Durch Verwendung sowie Integration klassischer Managementansätze und ITIL (IT Infrastructure Library), die hauptsächlich die prozessorientierte Sichtweise des Managements beleuchtet, soll ein übergreifendes Managementkonzept für VoIP erstellt werden, das - bei entsprechender Bereitschaft der einsetzenden Unternehmen - in die Aufbau- und Ablauforganisation integriert werden kann.

Management bedeutet neben dem Einsatz von technischer Infrastruktur zu einem nicht unerheblichen Teil den Einsatz von Personal, dessen Kosten in den westlichen Industrieländern einen immer höheren Anteil an den Gesamtkosten einnimmt.

Daher wird angestrebt, der betriebswirtschaftlichen Sichtweise des Managements einen hohen Stellenwert zukommen zu lassen, um personalintensive Abläufe von vorne herein zu vermeiden bzw. zu minimieren.

1.3 Vorgehensweise der Arbeit

In diesem Abschnitt wird die Vorgehensweise der Arbeit erläutert. Sie besteht in der Erstellung eines Anforderungskatalogs für VoIP-Systeme, der Abstraktion der Produkte verschiedener Hersteller von VoIP-Systemen, der Erarbeitung des Managementkonzepts und einer prototypischen Realisierung des Managementkonzepts (siehe auch Abbildung 1.1).

Anforderungskatalog Die Grundlage für die Erstellung des Managementkonzepts bildet ein Anforderungskatalog. Ein Teil der darin enthaltenen Anforderungen ergibt sich aus jeweils den Normen, Standards und Protokollen der TK- und IT-Welt. Eine weitere Komponente stellen die funktionalen Anforderungen der Nutzer dar, wobei Nutzer sowohl die einsetzenden Unternehmen als auch die eigentlichen Nutzer des VoIP-Systems, also die Angestellten, einschließt. Außerdem fließen die organisatorischen und technischen Gegebenheiten und Anforderungen der einsetzenden Unternehmen ein.

Abstraktion Verschiedene Hersteller bieten derzeit VoIP-Systeme an; hier werden die Produkte der Hersteller architekturell klassifiziert und so Gemeinsamkeiten herausgearbeitet.

Managementkonzept In das Managementkonzept fließen folgende Komponenten ein:

- klassische Managementansätze
- Konzepte von ITIL
- Anforderungskatalog
- Abstraktion der Herstellerarchitekturen

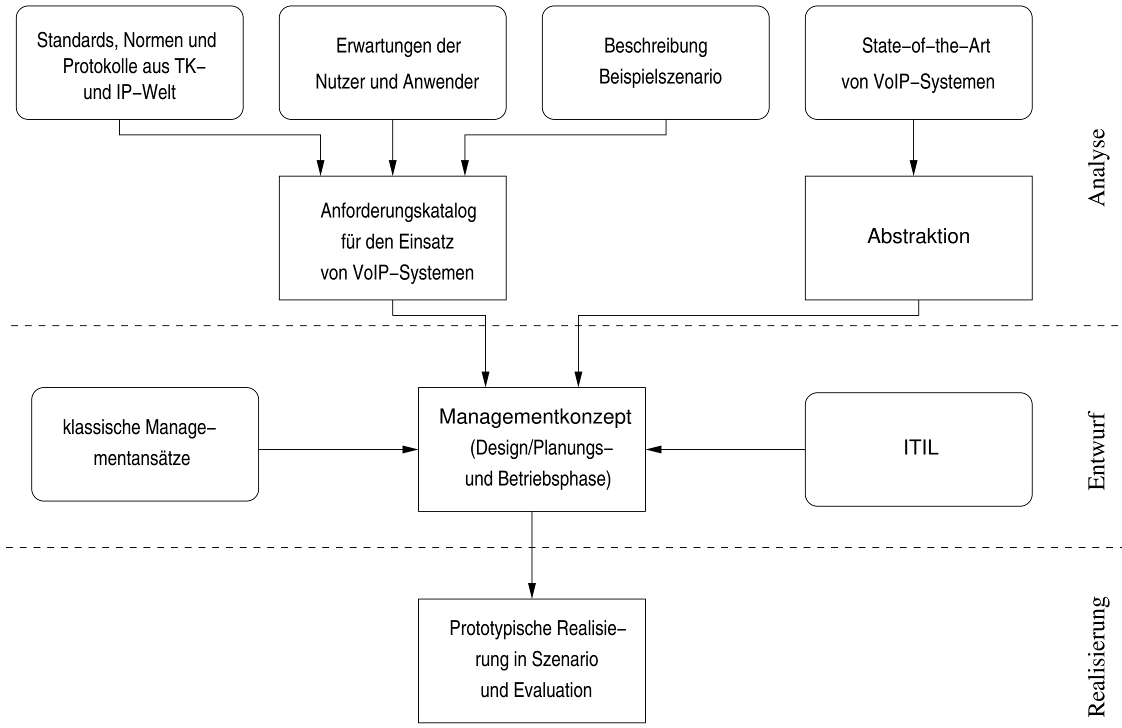

Abbildung 1.1: Vorgehensweise der Arbeit

Das Managementkonzept unterteilt sich in die Abschnitte

- Konzeption/Planung und Installation/Inbetriebnahme
- laufender Betrieb.

Diese Unterteilung wird gewählt, weil sich grundlegende Festlegungen bei der Konzeption bzw. Planung eines Systems durch alle Phasen der Management- und Betriebsprozesse ziehen und hierbei schon entscheidende Weichenstellungen für das gesamte Managementsystem entstehen. Das Managementkonzept befaßt sich hierbei schwerpunktmäßig mit dem Konfigurations- und Servicemanagement, da diese Bestandteile die meisten Problemfelder in sich bergen.

Prototypische Realisierung in einem Szenario Das entwickelte Managementkonzept soll in einem Szenario prototypisch realisiert werden. Hierbei handelt es sich - verkürzt gesagt - um die Einführung eines VoIP-Systems mit etwa 140 Teilnehmern in ein bestehendes TK-System mit etwa 700 Teilnehmern bei der Bezirksfinanzdirektion München, einer Behörde des Freistaats Bayern.

1.4 Gliederung der Arbeit

Die Arbeit gliedert sich in acht Kapitel.
In diesem ersten Einführungskapitel wurde die Geschichte der TK-Technik mit ihren verschiedenen Entwicklungsstufen bis hin zu VoIP dargestellt; daraus wurde die Notwendigkeit eines ganzheitlichen Managementansatzes für den Dienst VoIP hergeleitet. Danach wurden die Aufgabenstellung und Vorgehensweise der Arbeit entwickelt.

Das zweite Kapitel stellt die Kurzbeschreibung eines Beispielszenarios vor, in dem das zu entwickelnde Managementkonzept realisiert und evaluiert werden soll. Dieses Szenario stellt die Motivation für diese Arbeit dar; sie soll aber bewußt allgemein gehalten sein, um auch auf andere Fallgestaltungen angewendet werden zu können.

Im dritten Kapitel wird der Dienst VoIP definiert, d. h. welche Teilaspekte in dieser Arbeit zum Dienstbegriff gezählt werden. Überdies werden die Komponenten eines VoIP-Systems abstrakt vorgestellt.

Im vierten Kapitel wird ein Anforderungskatalog für VoIP erstellt. Dies beinhaltet zum einen die Vorstellung der wichtigsten verwendeten Standards, Normen und Protokolle und zum anderen die funktionalen, technischen und organisatorischen Anforderungen der Nutzer. Aus diesen Aspekten erfolgt die Erarbeitung des Anforderungskatalogs.

Das fünfte Kapitel befaßt sich mit den Produkten verschiedener Hersteller von VoIP-Systemen, deren Architekturen abstrahiert und verglichen werden.

Im sechsten Kapitel erfolgt die Erarbeitung des Managementkonzepts auf Grundlage der bisherigen Kapitel. In diesem Kapitel werden die Grundlagen klassischer Managementansätze und von ITIL erläutert und das Konzept mit den Phasen Konzeption/Installation und Inbetriebnahme sowie laufender Betrieb erstellt; außerdem werden phasenübergreifende Managementfragestellungen erörtert.

Das siebte Kapitel stellt die Realisierung des Managementkonzepts in dem in Kapitel zwei vorgestellten Szenario dar. Hierzu erfolgen eine detailliertere Beschreibung des Szenarios und der Architektur des eingesetzten Herstellers; anschließend wird erläutert, wie das Managementkonzept umgesetzt wurde. Am Schluß des Kapitels erfolgt eine Evaluation durch die Anwender im Szenario.

Das abschließende achte Kapitel beinhaltet eine Kurzzusammenfassung der Diplomarbeit und gibt Anregungen für zukünftige Systementwicklungsprojekte/Fortgeschrittenenprojekte und Diplomarbeiten, wobei hierin zukünftige Entwicklungen auf den zusammenwachsenden Netzen von TK und IT eine zentrale Rolle spielen.

Kapitel 2

Szenariobeschreibung

Zu Beginn wird ein Beispielszenario vorgestellt, in dem das zu erstellende Managementkonzept prototypisch zu realisieren ist. Diese Beschreibung stellt eine Kurzbeschreibung dar, die in Kapitel 7 in den relevanten Punkten ausführlicher erfolgt. Sie dient an dieser Stelle zur Einführung in die Thematik und zum Wecken der Motivation des Lesers dieser Arbeit; darüber hinaus soll sie verdeutlichen, daß die Planung, Installation und der Betrieb eines VoIP-Systems, das sich nicht nur im Teststadium, sondern sich von Beginn an im harten Alltagsbetrieb bewähren muß, keine zu unterschätzende Aufgabe ist.

2.1 Allgemeines

Das Szenario besteht in der Realisierung eines VoIP-Systems in einem Gebäude der Bezirksfinanzdirektion München.
Die Bezirksfinanzdirektion München ist eine Behörde des Freistaats Bayern und als Mittelbehörde dem Bayerischen Staatsministerium der Finanzen unterstellt; unterhalb sind die Vermessungsämter angesiedelt. Im Freistaat gibt es in jedem Regierungsbezirk (bis auf Oberfranken) eine Bezirksfinanzdirektion. Die weiteren liegen in Augsburg, Ansbach, Landshut, Regensburg und Würzburg.
Die Bezirksfinanzdirektionen sind prinzipiell für folgende Gebiete innerhalb des jeweiligen Regierungsbezirks zuständig:

- Prozeßvertretung des Freistaats Bayern für alle zivilrechtlichen Streitigkeiten
- Liegenschaftsmanagement aller im Eigentum des Freistaats befindlichen Immobilien
- Lohn- und Gehaltsabrechnung aller Arbeiter, Angestellten, Beamten und Pensionisten
- Abwicklung aller Buchungs- und Kassenvorgänge für andere Behörden des Freistaats
- Vermessungsangelegenheiten

Daneben betreibt die Bezirksfinanzdirektion München ein Rechenzentrum, in dem die Lohn- und Gehaltsabrechnung für alle Mitarbeiter und Pensionisten des Freistaats (derzeit etwa 250.000) sowie der Vollzug des Staatshaushalts (Aufstellung, Buchung und kassenmäßige Vorgänge) abgewickelt wird.
Die Bezirksfinanzdirektion München hat derzeit etwa 850 Beschäftigte und ist auf die Standorte München (730 Mitarbeiter) und die Außenstelle Ingolstadt (120 Mitarbeiter) aufgeteilt.
Innerhalb Münchens ist sie auf folgende Standorte verteilt:

- Alexandrastr. 3, Alexandrastr. 1, Liebigstr. 23 und Wagmüllerstr. 14 (560 Mitarbeiter): Hauptstandort, Straßenzug, der durch die genannten Straßen und die Prinzregentenstraße begrenzt wird
- Reitmorstr. 29 (40 Mitarbeiter)

- Maillinger Str. 11 (150 Mitarbeiter)

Abbildung 2.1 zeigt einen schematischen Lageplan des Hauptstandorts. Das Gebäude Liebigstr. 23 (früher

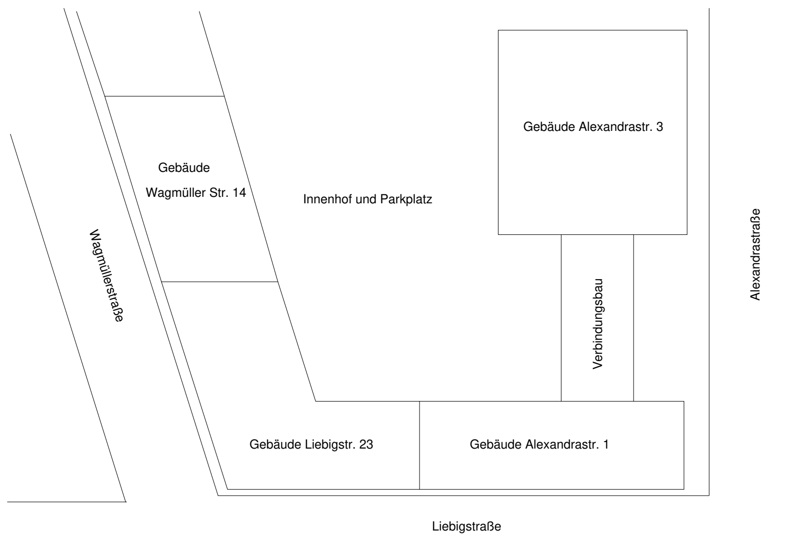

Abbildung 2.1: Lageplan des Hauptstandorts der Bezirksfinanzdirektion München

Wagmüllerstr. 12) wurde 1957 errichtet; Ende 1999 wurden bei Verkabelungs- und Brandschutzarbeiten weitreichende Statik- und Brandschutzrisiken festgestellt. Daher wurde entschieden, das Gebäude abzureißen und durch einen Neubau (an gleicher Stelle) zu ersetzen.
Ein Teil der Mitarbeiter des Gebäudes Wagmüllerstr. 12 wurden daraufhin (ab Ende 2000) in das Gebäude Prinz-Ludwig-Str. 9 ausgelagert; der Rest wurde in die anderen Gebäude verteilt.
In der folgenden Zeit wurde der Neubau konzipiert, wobei er auf etwa 140 Nutzer ausgelegt wurde (in Bezug auf die kommunikations- und EDV-technische Ausstattung wurden durch die Oberste Baubehörde und das Staatliche Hochbauamt München II lediglich eine Grobplanung auf Basis von Glasfasertechnologie und konventioneller Kommunikationstechnik erstellt; weitere Anmerkungen und Detaillierungen hierzu erfolgen in Abschnitt 7.4.
Mitte 2002 wurde das Gebäude abgerissen und mit dem Neubau begonnen; Mitte 2003 wurde Richtfest gefeiert und das Gebäude am 15.12.2004 an die Bezirksfinanzdirektion München übergeben.
In diesem Gebäude ist ein Kommunikationssystem und eine EDV-Infrastruktur zu realisieren, die – bedingt durch den kompletten Neubau – dem Stand der Technik entsprechen soll. Außerdem ist sie in die bisherigen Systeme zu integrieren. Hierbei ergibt sich für den Bereich der Sprachkommunikation die Wahlmöglichkeit zwischen einem konventionellen und einem VoIP-System. Beide Möglichkeiten können prinzipiell realisiert werden; die Entscheidung, welche Variante ausgeführt wird, ist ebenfalls Bestandteil des Managementkonzepts und wird unter anderem in Kapitel 7 erläutert.
Damit sich der Leser an dieser Stelle einen Überblick verschaffen kann, werden in den Abschnitten 2.2 und 2.3 die bestehende Infrastruktur im TK- und EDV-Sektor kurz vorgestellt. In Abschnitt 7.1 erfolgt eine detailliertere Beschreibung des Szenarios.

2.2 Beschreibung der bestehenden TK-Infrastruktur inkl. Applikationen

Jede Lokation der Bezirksfinanzdirektion München besitzt je ein konventionelles TK-System. Diese Systeme sind untereinander mittels S_{2M}-Strecken vernetzt, wobei als D-Kanal-Signalisierungsprotokoll Q.SIG (Details hierzu siehe Abschnitt 3.2.5.2) eingesetzt wird. Anbindungen an das PSTN sind in der Alexandrastr. 3 und Ingolstadt vorhanden. Abbildung 2.2 zeigt den Netzverbund schematisch. Dieser Netzverbund

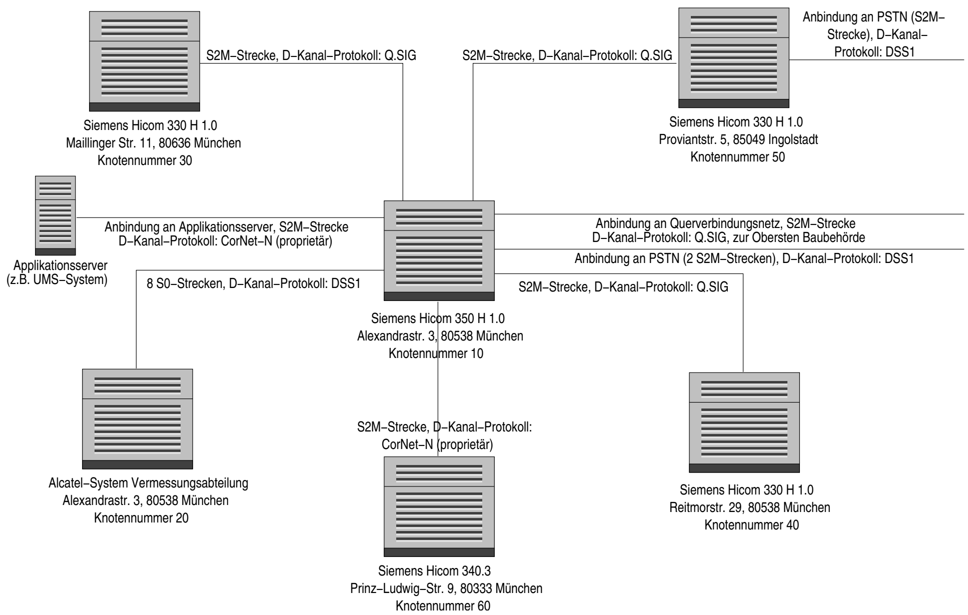

Abbildung 2.2: Netzverbund zu Beginn des Szenarios

stellt ein in Abschnitt 3.2.6.2 beschriebenes Verbundnetz dar. Zum einen sind die Anlagen untereinander vernetzt, zum anderen besteht eine Anbindung an das Querverbindungsnetz des Freistaats Bayern. In diesem Netz sind alle großen Münchner Behörden (derzeit etwa 80) und Universitäten nebst Klinika des Freistaats Bayern über eigene/angemietete Strecken verbunden, was kostenlose Interngespräche zur Folge hat (die korrekte Implementierung in die Routingtabellen vorausgesetzt).
Das TK-System der Prinz-Ludwig-Str. 9 wurde als Gebrauchtsystem (für die Dauer der Nutzung des Ausweichquartiers) gekauft, ist daher älter (Baujahr 1995) und unterstützt Q.SIG noch nicht. Daher wird das Siemens-proprietäre D-Kanal-Protokoll CorNet-N verwendet (mit Bezug des Neubaus wird dieses System außer Betrieb genommen und verwertet bzw. entsorgt).
Der Rufnummernplan der Bezirksfinanzdirektion München basiert auf einer verdeckten Nummerierung, d.h. alle TK-Systeme haben dieselbe Amtskopfnummer (089/2190-X in München) bzw. (0841/9386-X in Ingolstadt). Zum korrekten internen Routing besitzt jede Anlage als Adressierung eine Knotennummer (so befindet sich z.B. Nebenstelle 2290 an Knotennummer 10, Nebenstelle 1699 an Knotennummer 50). Die Außenstelle Ingolstadt ist in den Rufnummernplan von München integriert.
Die Telefonvermittlung ist zentral in der Alexandrastr. 3 angesiedelt; dies bringt Synergieeffekte, da an den einzelnen Standorten so kein eigenes Vermittlungspersonal notwendig ist.
Weitere Details zum Netzverbund (v.a. zu den Themen LCR-Tabellen, Routing, Berechtigungs- und Leistungsmerkmalkonzepte) folgen in späteren Abschnitten.

2.3 Beschreibung der Datennetzstruktur

Die EDV-Infrastruktur im Datennetz des Freistaats Bayern basiert auf einem IP-Netz, an dem prinzipiell alle Behörden sowie die Kommunen angeschlossen sind. Innerhalb des Netzes existieren VPNs (Steuer-VPN, Polizei-VPN, Haupt-VPN und Kommunen-VPN), zwischen denen ein Übergang nur über Firewallsysteme möglich ist, die am Bayerischen Landesamt für Statistik und Datenverarbeitung (LfStaD) angesiedelt sind. Der Betrieb des Netzes auf WAN-Seite ist einem großen internationalen Telekommunikations- und Datennetzanbieter (British Telecom) übertragen worden. LAN-seitig ist jede Behörde selbst verantwortlich.
Das Netz ist ein privates Netz; die Adreßverwaltung der Netze erfolgt zentral über das LfStaD. Ein Übergang zum Internet (mit DMZ, Firewallsystemen, Proxies, . . .) ist nur am LfStaD möglich und zulässig.

Firewallsysteme (außer den beschriebenen) existieren grundsätzlich nicht, da im Sinne eines „Corporate-Networks“ alle Behörden untereinander Datenkommunikation betreiben sollen.

2.4 Anforderungen

An das VoIP-System werden durch die Bezirksfinanzdirektion München folgende Anforderungen gestellt (wobei die Reihenfolge der Aufzählung eine Gewichtung von äußerst wichtig bis weniger wichtig darstellt):

- gleiche Sprachqualität (im Vergleich zu konventioneller Technik)
- ähnlich hohe Verfügbarkeit wie bei konventioneller Technik
- wirtschaftliches System und kostensparender Einsatz im laufenden Betrieb
- Realisierung derselben Leistungsmerkmale wie in konventionellen Systemen
- Anbindung an das interne Querverbindungsnetz
- Anbindung an bestehende Applikationen (z.B. Unified-Messaging-System)
- keine (oder nur geringe) zusätzliche Komplexität im Bereich des Managements des Systems
- Standardkonformität aller Komponenten (d.h. keine Einführung proprietärer Standards)

Diese Anforderungen haben sich aus der täglichen Praxis sowie aus den in [DIKO03] gewonnen Erfahrungen ergeben.
Ein allgemeiner Anforderungskatalog für VoIP-Systeme wird in Kapitel 4 erarbeitet, der zum Großteil die hier stichpunktartig genannten Aspekte ausführt.

2.5 Zusammenfassung

Zusammengefaßt stellt sich die Szenariobeschreibung demnach wie folgt dar:

- Konzeption und Realisierung eines VoIP-Systems (für etwa 140 Teilnehmer)
- Integration in bestehende TK- und EDV-Systeme (auf München und Ingolstadt verteilte Systeme der restlichen Mitarbeiter) unter Beachtung der jeweiligen Spezifika
- Integration in bestehende Managementsysteme und ggf. Neuaufbau von Teilkomponenten
- Berücksichtigung der sonstigen Anforderungen (Verfügbarkeit, Sprachqualität, Kosten und Leistungsmerkmale)

Kapitel 3

Grundlagen und Definitionen

Die Telefonie- und Datennetze befinden sich in einem langfristigen Verschmelzungsprozess. Die Möglichkeiten, die nachrichtenvermittelte Datennetze gegenwärtig bieten, beschränken sich nicht mehr nur darauf, PCs mit dem Internet zu verbinden.
Der Gedanke liegt nicht fern, die Telefondienste vollständig in Computernetze zu integrieren; dies geschieht durch „Voice over IP“. Da sich jeder unter VoIP etwas anderes vorstellt, erfolgt zuerst eine Definition des Dienstes VoIP; danach werden grundlegende Begriffe, Standards, Normen und Begriffe sowohl aus der TK-Welt als auch der IP-Welt vorgestellt.

3.1 Dienstdefinition von Voice over IP

In diesem Abschnitt erfolgt eine grundlegende Definition des Dienstes „VoIP“. Hierbei wird der Dienst einmal im Sinne von OSI und einmal unter serviceorientierten Gesichtspunkten definiert.

3.1.1 Definition im Sinne von OSI

Ein Dienst im Sinne des ISO-OSI-Modells ist eine Gruppe von Operationen, die eine Sicht der über ihr liegenden Schicht zur Verfügung stellt. Ein Dienst sagt aus, welche Operationen eine Schicht ausführen kann, nicht jedoch wie diese Operationen implementiert werden. Ein Dienst läuft über die Schnittstelle zwischen zwei Schichten, wobei die untere Schicht der Dienstanbieter und die obere der Dienstnutzer ist [TAN00]. Beispiele für Dienste sind: ISDN, Video-on-Demand, Videokonferenzen, ...

Bei VoIP sind dies alle Operationen, die die Sprachtelefonie im herkömmlichen Sinn bietet. Der Unterschied besteht darin, daß die Telefonie hier über IP-basierte Netze abgewickelt wird. Mit „Voice“ ist hier im wesentlichen die Telefonie gemeint. Anders geartete Sprachübertragungen, wie z. B. Live-Audio-Streaming über das Internet werden zwar häufig mit derselben Technologie durchgeführt, werden aber nicht unter dem Begriff „VoIP“ zusammengefaßt.

3.1.2 Serviceorientierte Definition

Bei dieser Definitionssicht wird der Dienst als VoIP als Serie von Interaktionen und Beziehungen bestimmter Akteure aufgefaßt ([MNM01]). Diese Akteure haben Rollen. Bezogen auf VoIP sind dies:

- Benutzer: Mitarbeiter eines Unternehmens bzw. Kunden eines VoIP-Anbieters
- Provider: das einsetzende Unternehmen bzw. der VoIP-Anbieter

Daneben existieren für die Dienstbeschreibung verschiedene Sichten ([MNM01]):

- **rollenunabhängige Aspekte:** Diese Aspekte beinhalten die Nutzungs- und Managementfunktionalität. Beide müssen spezifische QoS-Parameter (sowohl qualitativ als quantitativ) erfüllen. Bei VoIP sind dies Verfügbarkeit des Dienstes und Sprachqualität.
  Die nutzerspezifische Funktionalität umfaßt das Führen von Telefongesprächen (sowie Datenübertragung) über IP-basierte Netze. Außerdem besteht die Definition eines Dienstzugangspunkts (SAP) für die Nutzer.
  Bezogen auf die managementspezifischen Problemstellungen ist ein Service Agreement erforderlich, das die Dienstfunktionalität sowie die QoS-Parameter beschreibt. Darüber hinaus sind Schnittstellen notwendig, die eine Verbindung der Nutzer zum Dienstmanagement herstellen (z.B. Hotlinenummern, Abrechnungsmodalitäten, Preistabellen, ...).

- **nutzerspezifische Aspekte:** Auf Nutzerseite ist festzulegen, wie der Nutzer den Dienst (über den SAP) erreichen kann. Bei VoIP sind dies entweder separate VoIP-Endgeräte oder eine Software auf einem Rechner.

- **anbieterseitige Aspekte:** Auf Providerseite liegt das Hauptaugenmerk auf der Verfügbarkeit des Dienstes. Er hat zum einen die Lauffähigkeit des Dienstes innerhalb der vereinbarten QoS-Parameter sicherzustellen (wozu ein Monitoring- und Managementsystem nötig ist) und eine komplette Dienstdokumentation vorzuhalten. Diese beinhaltet u.a. alle Betriebsmittel (Hardware, Software, Personal, Wissen, ...), die nötig sind, um den Dienst einzurichten und zu betreiben (bei VoIP: Systemdokumentation bzw. -beschreibung des VoIP-Gesamtsystems, eingesetztes Personal, ...).

Zusammengefaßt befaßt sich diese Sicht der Dienstdefinition mit den einzelnen Akteuren, die an der Dienstnutzung und -erbringung beteiligt sind, sowie den Beziehungen untereinander, die für eine reibungslose Lauffähigkeit des Dienstes notwendig sind.

In den nächsten Abschnitten werden die Anwendungsbereiche und die Einsatzgebiete von VoIP definiert.

3.1.3 Anwendungsbereiche von VoIP

Bei VoIP gibt es zwei Anwendungsbereiche [NOE03]:

- **Internet-Telefonie**: Internet-Telefonie bedeutet das Führen von Telefongesprächen mittels VoIP über das Internet, d.h. somit sind weltweite Telefonate über das weltumspannende Internet möglich. Die Internet-Telefonie kennzeichnet einen Anwendungsbereich von VoIP, enthält jedoch genau genommen keine Referenz auf die eingesetzte Technologie. Letztlich ist jedoch durch die Tatsache, daß die Funktion des Internets auf dem IP-Protokoll beruht, festgelegt. Bei der Internet-Telefonie wird eine wesentlich schlechtere Sprachqualität als in anderen Anwendungsbereichen hingenommen, weil sich der gesamte Datenpfad einer Sprachverbindung nicht vom Sender bis zum Empfänger kontrollieren läßt. Deshalb können netzbezogene Verfahren zur Verbesserung der Sprachqualität, die in den nachfolgenden Kapiteln beschrieben werden, nicht oder nur in unzureichendem Maße eingesetzt werden, Insbesondere treten im Internet häufig sehr große Paketübertragungszeiten, hoher Jitter und hohe Paketverlustraten auf, die eine Sprachübertragung beeinträchtigen.

- **Intranet-Telefonie**: Die Intranet-Telefonie kennzeichnet ebenfalls einen Anwendungsbereich, in diesem Fall die Sprachtelefonie innerhalb eines geschlossenen Unternehmensnetzes. Dies impliziert, daß Telefonate innerhalb des unternehmenseigenen IP-basierten Netzes mittels VoIP über dieses Intranet abgewickelt werden; darüber hinausgehende Telefonate werden über klassische Telefoniedienste abgewickelt. Weil unterschiedliche Netzwerktechnologien in Firmennetzwerken eingesetzt werden, enthält der Begriff Intranet-Telefonie keine eindeutige Klärung bezüglich der verwendeten Netzwerktechnik, der Großteil der Unternehmensnetze beruht jedoch auf der Ethernet-Technologie.

Darauf aufbauend ergeben sich zwei grundsätzliche Einsatzbereiche von VoIP.

3.1.4 Einsatzbereiche von VoIP

- **VoIP für Carrier**: Bei der Nutzung von VoIP durch die Telefonanbieter (auch „Carrier“ genannt) bedeutet dies, daß die Carrier in ihren eigenen Netzen sowie zur Kundenanbindung (für Sprachdienste) VoIP einsetzen. Dies bedeutet, daß die Carrier die Sprachdaten über eigene IP-Netze sowie über Teile des Internets leiten, d. h. die Sprachdaten laufen als IP-Pakete durch die Netze; klassische auf dem Zeitmultiplexverfahren basierende Techniken werden aber weiterhin eingesetzt.
  Die Kundenanbindung wird über eine (u. U. separate) IP-Strecke zum VoIP-Telefonsystem des Kunden realisiert, wobei hierbei bei der Nutzung der bisher bestehenden Internetanbindung des Kunden hohe Sicherheitshürden überwunden werden müssen, da eine (hoffentlich) existierende Firewallösung des Kunden mit der zufälligen Wahl von UDP-Ports zurechtkommen muss (Einzelheiten der Notwendigkeit zur Nutzung von UDP werden in 3.3 erläutert).

- **VoIP für Endkunden**: Als weitere Nutzungsmöglichkeit ergibt sich die Nutzung von VoIP durch den Endkunden. Dies bedeutet, daß der Kunde weiterhin über eine „klassische“, auf dem Zeitmultiplexverfahren basierende Anbindung an das öffentliche Telefonnetz (PSTN) verfügt, innerhalb des Unternehmens aber ein Großteil der Gespräche/alle Gespräche über VoIP abgewickelt werden.
  Dies ist besonders für größere Kunden interessant, die über mehrere Standorte verfügen, die über interne Verbundnetze (für den Telefonverkehr) miteinander verbunden sind (Gründe für den Betrieb solcher Verbundnetze sind in 3.2.6.2 erläutert). Parallel dazu besitzen die Unternehmen/Kunden meist noch separate Datennetze zur datenmäßigen Vernetzung der Standorte.
  Durch den Einsatz von VoIP ergibt sich die grundsätzliche Möglichkeit, die bisher separaten Netze (Telefon- und Datennetz) zu verschmelzen, d. h. Abbau der Telefonnetze, was u. U. hohe Einsparpotentiale bietet.

Derzeit wird (fast) ausschließlich der zweite Einsatzbereich (also VoIP für Endkunden) eingesetzt, was technische, organisatorische und regulative Gründe (z. B. RegTP) hat, auf die hier nicht eingegangen wird, da dies den Rahmen der Diplomarbeit sprengen würde. Dem Verfasser ist kein Carrier bekannt, der zum jetzigen Stand Carrierdienstleistungen für Großkunden/Unternehmen auf Basis von VoIP anbietet.
Aus diesem Grund befaßt sich die Diplomarbeit primär mit dem Einsatz von VoIP beim Endkunden; dies bedeutet aber keine wirkliche Einschränkung, da das vorgestellte Managementkonzept mit zusätzlichen Erweiterungen auch für Carrier anwendbar wäre.

VoIP bietet ein weites Einsatzspektrum, das sowohl den Einsatz bei Carriern als auch bei Endkunden/Unternehmen ermöglicht, wobei sowohl das Internet als auch interne IP-Netze (Intranets) verwendet werden können.
Grundlage der Sprachübertragung bildet hierbei die Sprachübertragung über IP-Netze, wobei die Sprachdatenpakete als IP-Pakete versandt werden.

3.1.5 Historische Entwicklung

Seit Erfindung der Telefonie (etwa 1850) wurde die Analogtechnik zur Übertragung der Sprachsignale verwendet. Hierbei werden die Sprachfrequenzen mittels Mikrofonen in elektrische Spannungen übertragen und auf der Gegenseite über einen Lautsprecher ausgegeben.
Hierbei wird das Frequenzspektrum von Sprache (300 Hz - 3,4 kHz) nach den Abtasttheoremen von Nyquist und Shannon (siehe [TAN00]) mit einer Abtastfrequenz von 6,8 kHz ($2 * 3,4kHz$; eigentlich würden 6,2 kHz = 2 * (3,4 kHz - 300 Hz) ausreichen – da hier eine Frequenzverschiebung nötig wäre, wird der Einfachheit halber die untere Grenze auf 0 gesetzt) und einer Abtastfrequenz von 5 Bit (was 32 verschiedenen Spannungsniveaus entspricht) quantisiert. Somit ergibt sich eine Bandbreite von 34 kbps ($5Bit * 6,8kHz$) für einen analogen Kanal.

Mit Einführung der Computertechnik zu Beginn der 1980er-Jahre wurden die Telefonnetze digitalisiert. Dies bedeutet, daß die Sprachsignale nicht mehr über analoge Spannungssignale, sondern über digitale Bitfolgen übertragen werden.
Außerdem wird hierbei eine Abtastfrequenz von 8 kHz sowie eine Abtasttiefe von 8 Bit verwendet, was eine Bandbreite von 64 kbps ergibt. Mit Einführung der Digitaltechnik wurde die ISDN-Architektur entwickelt und implementiert (siehe Kapitel 3.2.1).
Überdies wird bei der Digitaltechnik das Zeitmultiplexverfahren eingesetzt, was in Kapitel 3.2.4 am Beispiel von ISDN vorgestellt und erläutert wird.

Als Vermittlungsverfahren wurde und wird bei Analog- und Digitaltechnik die Leitungsvermittlung verwendet, d.h. zuerst wird der Pfad vom Sender zum Empfänger durchgeschaltet und reserviert; danach werden auf diesem (dedizierten) Kanal die Sprachdaten übertragen (Details hierzu werden in Kapitel 4.1.1 erläutert).

Als nächsten Schritt ergab sich etwa zur Jahrtausendwende die Möglichkeit, die digitalisierten Sprachdaten nicht mehr über separate Netze zu transportieren (Voice-over-IP), sondern über das Internet, das auf der Nachrichtenvermittlung und der Ethnernet-Technologie sowie dem Internet-Protokoll (IP) basiert. Die hiermit einhergehenden Problemfelder werden in Kapitel 3.2.4 aufgezeigt.

3.2 Einführung in die TK-Technologie

Um die Funktionsweise von VoIP verstehen zu können, werden in diesem Abschnitt die theoretischen Grundlagen klassischer Telefontechnik vorgestellt, wobei Analogtechnik ausgeklammert wird, da sie für das Verständnis nicht nötig ist.

Dieser Abschnitt der Diplomarbeit ist in Teilen aus einem vom Verfasser in Zusammenarbeit mit Csaba Korényi erstellten Systementwicklungsprojekt entnommen [DIKO03].

Heutzutage ist die herkömmliche TK-Technologie zu einer selbstverständlichen, aber unverzichtbaren Komponente unseres täglichen Lebens geworden. Jedoch ist nur eine Minderheit der Bevölkerung mit den grundlegenden Konzepten dieser Technologie vertraut.
Um die Probleme und Möglichkeiten von VoIP zu verstehen, befasst sich dieser Abschnitt mit den Elementen und Standards der klassischen TK-Technologie. Darüber hinaus werden elementare Standards von VoIP erläutert.
Hierbei wird besonderer Schwerpunkt auf die Gatewayfunktionalität zwischen dem klassischen TDM-basierten Netz und einem nachrichtenvermittelten Netz gelegt.

Moderne TK-Systemverbünde basieren auf digitaler Übertragungstechnik. Der Durchbruch für diese Übertragungsform war die Standardisierung von ISDN ab dem Jahre 1984. Das vorrangige Ziel von ISDN besteht in der Sprach- und Datenintegration.

3.2.1 ISDN-Dienste

Der wichtigste Dienst ist auch bei ISDN die Sprachübermittlung, allerdings mit vielen neuen Funktionen gegenüber der analogen Übertragung. Bezeichnend für ISDN sind verschiedene spezifische Leitungsmerkmale, wie z. B.:

- Mehrfachrufnummer
- Übermittlung der Rufnummer
- Umleitung eingehender Anrufe
- geschlossene Benutzergruppen

- Dreierkonferenz
- Anklopfen
- Fangschaltung
- Makeln
- Parken
- Subadressierung
- Übermittlung von Tarifinformationen

3.2.2 ISDN-Architektur

ISDN stellt eine digitale Übertragungsform dar, die sowohl synchron als auch transparent ist. Hauptunterscheidung zu analoger Übertragungstechnik ist die Outband-Signalisierung, d. h. die Signalisierung erfolgt unabhängig von den Nutzdaten ([TAN00]).
ISDN basiert auf einer „digitalen Bit-Pipeline", die mehrere unabhängige Kanäle durch Anwendung des Zeitmultiplexverfahrens (TDM) auf den Bitstrom legt. Das Format der Pipeline und das Multiplexen des Bitstroms sind in der ISDN-Schnittstellenspezifikation definiert.

Für diese Bit-Pipeline wurden zwei grundsätzliche Standards ausgearbeitet:

- ein Standard mit niedriger Bandbreite für Privathaushalte (S_0)
- ein Standard mit höherer Bandbreite für kommerzielle Nutzer (S_{2M}).

Die physikalische Schicht (OSI-Layer 1) ist durch die ITU-T Empfehlungen I.430 (für S_0) sowie I.431 (für S_{2M}) festgelegt und regelt beispielsweise die Anschlußarten der beiden Standards.

3.2.3 ISDN-Schnittstelle

Die ISDN-Pipeline unterstützt mehrere Kanäle, die durch das Zeitmultiplexverfahren (TDM) aufgeteilt werden [TAN00]. Mehrere Kanaltypen wurden hier standardisiert: Bisher wurden von der CCITT drei

A	analoger Telefonkanal (4 kHz)
B	digitaler PCM-Kanal für Sprache oder Daten (64 kbps)
C	digitaler Kanal (8 oder 16 kbps)
D	digitaler Kanal für bandexterne Zeichengabe (Signalisierung) (16 kbps)
E	digitaler Kanal für interne Signalisierung (64 kbps)
H	digitaler Kanal (384, 1.536 oder 1.920 kbps)

Tabelle 3.1: Kanaltypen von ISDN

Kombinationen von Kanälen standardisiert:

- Basisanschluss: 2B + 1D
- Primärmultiplexanschluss: 30B + 1D (Europa)
- Hybridanschluss: 1A + 1C (wird nicht verwendet)

Die Kanäle des Basis- und Primärmultiplexanschlusses sind in Abbildung 3.1 dargestellt. Der Basisanschluss (auch S_0-Schnittstelle genannt) kann als Ablösung des konventionellen Telefondienstes (POTS) für Privathaushalte oder kleinere Firmen betrachtet werden. Jeder B-Kanal mit 64 kbps unterstützt einen Kanal mit 8-bit-Mustern, die 8.000mal pro Sekunde abgetastet werden, auf dem sowohl Sprache als auch

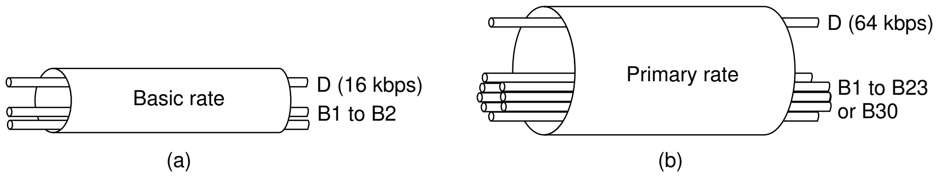

Abbildung 3.1: a) ISDN-Basisanschluß b) ISDN-Primärmultiplexanschluß

Daten (inkl. Faxe) übertragen werden können. Insofern ist völlig unerheblich, was auf einem B-Kanal übertragen wird; diese Eigenschaft wird transparent genannt. Die Signalisierung, also die Übertragung der ISDN-Dienst- bzw. Leistungsmerkmale (siehe 3.2.1), erfolgt auf einem getrennten D-Kanal mit 16 kbps, sodaß dem Nutzer die vollen 64 kbps zur Verfügung stehen.

Die S_0-Schnittstelle ist eine 4-Draht-Schnittstelle, d.h. die Installation eines Basisanschlusses in Form eines passiven Busses besteht aus einem Kabel mit zwei verdrillten Adernpaaren. Alle drei Kanäle (2 B-Kanäle und 1 D-Kanal) garantieren, daß die zu übertragenden Bitströme im Vollduplex-Betrieb ausgetauscht werden können. Weiterhin hat jedes Endgerät die Möglichkeit, die beiden B-Kanäle für Misch- oder Mehrfachkommunikation zu nutzen (z.B. Telefongespräch und Datenübertragung). Alle Endgeräte können gleichzeitig auf den D-Kanal zugreifen, um eigene Steuerungen vorzunehmen; Zugriffsverfahren für den D-Kanal ist das CSMA/CA-Verfahren (Carrier Sensing Multiple Access - Collision Avoidance) ([SIE01]); dieses Verfahren wird auch bei WLANs verwendet. Es ergibt sich also für die Übertragung über die S_0-Schnittstelle eine Nettobitrate von 144 kbps (64 + 64 + 16).

Der Primärmultiplexanschluss (auch S_{2M}-Schnittstelle genannt) ist für Unternehmen mit einer privaten Nebenstellenanlage (PBX) gedacht. Er hat 30 B-Kanäle und einen D-Kanal (64 kbps) (Europa). Für die Kombination von 30B + 1D hat man sich entschieden, damit ein ISDN-Rahmen angenehm in das 2.048-Mbps-System der CCITT passt. Die Zeitschlitze von 30 Sekunden im CCITT-System werden für die Rahmenbildung und die allgemeine Netzwartung benutzt. Die Anzahl von D-Kanälen pro B-Kanal im Primärmultiplexanschluss ist viel geringer als beim Basisanschluss, da in diesem Bereich prozentual weniger Signalisierungsdaten anfallen. Die Netto-Übertragungskapazität beträgt 1.984 kbps. Daher rührt auch die Abkürzung S_{2M}, die auf S2Mbit/s zurückzuführen ist.

S_0- und S_{2M}-Schnittstellen können (und werden) neben dem Anschluss an das PSTN auch zur internen Vernetzung von TK-Systemen verwendet. Somit ist es möglich, einen TK-Systemverbund, der sich z. B. über verschiedene Standorte oder abgesetzte TK-Anlagen erstreckt, zu erzeugen (weitere Einzelheiten siehe 3.2.6.2).

3.2.4 Rahmenaufbau bei S_0 und S_{2M}

Wie bereits in 3.2.3 erläutert, erfolgt bei ISDN für Sprache 8.000-mal pro Sekunde, d. h. alle 125 μs, ein Abtastvorgang (bei Daten erfolgt keine Abtastung, da die Signale bereits in Binärform vorliegen). Bei jedem Abtastvorgang wird ein Rahmen (sog. „Frame") erstellt, der an die Gegenseite übermittelt wird. Die beiden folgenden Abschnitte zeigen den Rahmenaufbau bei S_0 und S_{2M}, wobei hier die grundlegenden Aspekte des Data-Link-Layers (OSI-Layer 2) wie Fehlererkennung und -behebung sowie Synchronisation beschrieben werden. Die zugrundeliegenden Dokumente wurden von der ITU-T unter den Bezeichnungen Q.920 bzw. Q.921 veröffentlicht.

- Rahmenaufbau bei S_0
  Ein S_0-Frame besteht, wie es Abbildung 3.2 zeigt, aus 2 B-Kanälen zu je 8 bit (8 bit x 8.000/s = 64 kbps), einem D-Kanal zu 2 bit (2 bit x 8.000/s = 16 kbps) sowie einem Kanal zu 6 bit (6 bit x 8.000/s = 48 kbps), der Steuerinformationen enthält, aufgebaut ([TAN00]). Die B-Kanäle und der D-Kanal wurden bereits in 3.2.3 erklärt.

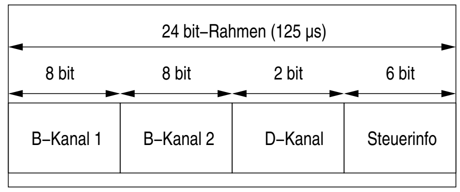

Abbildung 3.2: S_0-Frameaufbau

Die Steuerinformationen dienen zur Rahmensynchronisation der Frames, zur Zugriffssteuerung der Geräte auf den D-Kanal und zur Fehlererkennung bzw. -korrektur. Zur Framesynchronisation wird z. B. die Bitfolge „1010…“ verwendet; die Synchronisation hat den Zweck, daß sich aus dem Takt geratene Endstellen schnell wieder synchronisieren können (also die Framegrenzen wieder erkennen können), indem sie nach dem genannten Bitmuster suchen. Somit ist eine rasche Synchronisation möglich.
Die S_0-Schnittstelle erfordert demnach eine Bruttodatenrate von 192 kbps (24 bit x 8.000/s), wovon 128 kbps (die beiden B-Kanäle) effektiv nutzbar sind (wenn man von einer möglichen Mitnutzung des D-Kanals für Nutzdatenübertragung absieht).

- Rahmenaufbau bei S_{2M}
  Ein S_{2M}-Frame beinhaltet folgende Komponenten (Gesamtlänge 256 bit, siehe Abbildung 3.3):
  - 30 B-Kanäle (je 8 bit bzw. 64 kbps)
  - 1 D-Kanal (8 bit bzw. 64 kbps)
  - 1 Kanal für Steuerinformationen (8 bit bzw. 64 kbps, dieselbe Funktion und Aufbau wie bei S_0)

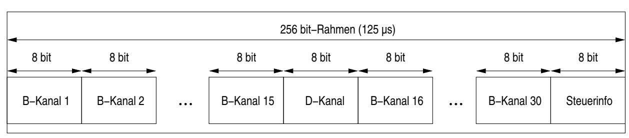

Abbildung 3.3: S_{2M}-Frameaufbau

Somit benötigt die S_{2M}-Schnittstelle eine Bruttodatenrate von 2.048 kbps (256 bit x 8.000/s), von denen hier 1.920 kbps effektiv nutzbar sind (30 B-Kanäle), wenn man auch hier von einer Mitnutzung des D-Kanals absieht.

3.2.5 D-Kanal-Signalisierungsprotokolle

Die folgenden (auf OSI-Layer 3) befindlichen Protokolle stellen die höchste für ISDN festgelegte Kommunikationsschicht unterhalb der Anwendungsschicht dar und sind unter Q.930 bzw. Q.931 von der ITU-T veröffentlicht worden (Q.930 enthält eine Übersicht über die Layer-3-Spezifikation mit Referenzen auf Standards der Anwendungsschicht sowie eine Interfaceübersicht für die Rufsteuerung.

In diesem Abschnitt werden die Protokolle Q.931 und Q.SIG vorgestellt. Q.931 stellt das Standard-ISDN-Signalisierungsprotokoll dar und wird im PSTN sowie bei H.323 (siehe Kapitel 3.3.1) verwendet.
Demgegenüber wird Q.SIG bei internen Verbundnetzen (siehe Kapitel 3.2.6.2) verwendet, wenn die verwendeten TK-Systeme (meist verschiedener Anbieter) es unterstützen (sonst muß Q.931 eingesetzt werden). Der große Vorteil von Q.SIG liegt in der im Vergleich zu Q.931 erweiterten Anzahl an Leistungsmerkmalen, die v.a. in internen Netzen gewünscht und gefordert wird.

3.2.5.1 DSS1/Q.931-Protokoll

Das DSS1/Q.931-Protokoll ist das europäische ISDN-Protokoll für den D-Kanal des paneuropäischen Euro-ISDN [SIE01]. In Europa haben sich die meisten Netzbetreiber in fast allen europäischen Staaten zu der Einführung des DSS1 verpflichtet (Q.931 ist das von der ITU-T spezifizierte weltweit gültige ISDN-D-Kanal-Signalisierungsprotokoll, auf dem DSS1 basiert, wobei bei DSS1 einige europäische Besonderheiten integriert sind).
Das DSS1-Protokoll unterscheidet zwischen vier Codesätzen für Informations-Elemente. Der Codesatz 0 entspricht dem Regelcodesatz nach Q.931, der Codesatz 5 dem ETSI-Codesatz, der Codesatz 6 ist für nationale Anwendungen und der Codesatz 7 für private Anwendungen über die Nebenstellenanlage. Das Netz verwendet derzeit nur den Codesatz 0.
Q.931 definiert folgende Nachrichten, die ausgetauscht werden können:

- Nachrichten für den Verbindungsaufbau:
  - Alerting
  - Call Proceeding
  - Connect/Connect Acknowledge
  - Progress
  - Setup/Setup Acknowledge
- Nachrichten während einer Verbindung:
  - Resume/Resume Acknowledge/Resume Reject
  - Suspend/Suspend Acknowledge/Suspend Reject
- Nachrichten für den Verbindungsabbau:
  - Disconnect
  - Release/Release Complete
- sonstige Nachrichten:
  - Information
  - Notify
  - Segment
  - Status/Status Enquiry

3.2.5.2 Das Q.SIG-Protokoll

In den folgenden Abschnitten wird das Q.SIG-Protokoll vorgestellt, das die Interoperabilität von TK-Systemen verschiedener Hersteller mit einer größeren Zahl an Leistungsmerkmalen als bei DSS1/Q.931 ermöglicht.

- **Allgemeines**

  Wie in 3.2.6 erläutert, ist es für Unternehmen u. U. sinnvoll, ein eigenes Verbundnetz aufzubauen. Dies geschieht hierbei (abhängig von der Anzahl der zwischen den Standorten benötigten B-Kanäle) mittels S_0- bzw. S_{2M}-Strecken. Hierbei kommt dem verwendeten D-Kanal-Signalisierungprotokoll (siehe 3.2.4 und 3.2.5) eine besondere Bedeutung zu:
  Abhängig vom verwendeten Protokoll sind nur bestimmte Leistungsmerkmale möglich (so sind z. B. bei Verwendung von DSS1 nur die ISDN-Leistungsmerkmale - siehe 3.2.1 - verfügbar). Die Vorteile des Verbundnetzes entfalten aber nur bei Vorhandensein zusätzlicher Leistungsmerkmale

(wie z. B. Rückruf, netzweite Anrufweiterleitung, ...) ihre volle Wirkung. Da die Unternehmen aber größtenteils TK-Anlagen verschiedener Hersteller einsetzen, ergibt sich folgendes Problem:
Vor der Entwicklung von Q.SIG arbeitete jeder Telefonanlagenhersteller mit einem proprietären D-Kanal-Signalisierungsprotokoll (bei Siemens war es zum Beispiel das Protokoll „CorNet“). Das bedeutet, daß die im proprietären Signalisierungsprotokoll implementierten Leistungsmerkmaltabelle zwar netzweit im Verbund von TK-Anlagen des gleichen Herstellers verfügbar waren. Sobald aber ein TK-System eines Fremdherstellers in den TK-Verbund integriert wurde, musste auf den Verbindungsstrecken zur TK-Anlage des Fremdherstellers auf den kleinsten gemeinsamen Nenner zurückgegriffen werden. Dies war und ist ISDN.

Sobald das System des Fremdherstellers tangiert war, waren damit aber die Vorteile des gemeinsamen Netzes nicht mehr vorhanden, da nur noch der Minimalstandard der ISDN-Leistungsmerkmale übertragen wurde (nicht einmal die Namensübermittlung war somit möglich.)

Da jedoch viele Unternehmen im TK-Bereich keine Ein-Marken-Strategie und damit die Abhängigkeit von einem einzigen Hersteller toleriert haben und der Druck zum Handeln wegen der Marktmacht der Kunden immer größer wurde, wurde mit der Entwicklung eines Standards für Vernetzungsprotokolle begonnen: dem Q.SIG-Standard.

Das Q.SIG-Protokoll (Q-Interface Signalling Protocol) ist ein internationaler von der ECMA definierter Signalisierungsstandard für die logische Signalisierung zwischen zwei privaten Vermittlungsknoten, z.B. TK-Anlagen. Damit soll Betreibern von Corporate Networks die Möglichkeit gegeben werden, verschiedene TK-Systeme zu einem heterogenen Netz zusammenzuschalten und anlagenübergreifend Leistungsmerkmale, wie die automatische Rufumleitung, zu nutzen.

Das Signalisierungssystem ist so konzipiert, daß es alle Netzwerkstrukturen wie beispielsweise Sterntopologie, Bustopologie, vermaschtes Netz oder Baumtopologie unterstützt, ebenso wie eine beliebige Anzahl an Knotenrechnern.
Q.SIG basiert auf dem D-Kanal-Protokoll nach dem ITU-T-Standard der Q.93x-Serie für Basic Call und der Q.95x-Serie für die Leistungsmerkmale. Damit ist sichergestellt, daß Q.SIG und ISDN kompatibel in ihren Leistungsmerkmalen sind und ISDN-Applikationen bzw. -Zusatzdienste der öffentlichen ISDN-Netze auch in einem privaten Netz genutzt werden können.

Die Architektur von QSIG entspricht im wesentlichen der ISDN-Architektur, wobei allerdings neben den N-, T- und S-Bezugspunkten (Kommunikation zwischen zwei Netzknoten, Netzknoten und Basisanschluss und S_0-Geräte) zwei neue Referenzpunkte hinzukommen, der Q-Punkt und der C-Punkt (siehe 3.4).
Der Q-Referenzpunkt ist der logische Signalisierungspunkt zwischen zwei privaten Nebenstel-

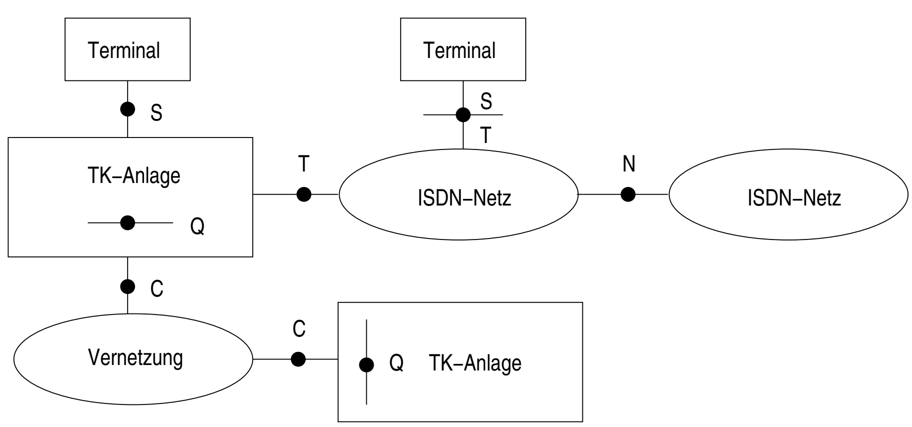

Abbildung 3.4: Referenzpunkte von Q.SIG und ISDN

lenanlagen, d.h. jede PBX besitzt einen solchen Referenzpunkt, über den die Kommunikation mit den anderen PBX und ihren Q-Referenzpunkten stattfindet. Der C-Referenzpunkt bildet den Bezugspunkt für die physikalische Verbindung. Das soll heißen, die Kommunikation zwischen zwei Q-Referenzpunkten findet über den C-Referenzpunkt statt. Der Q.SIG-Standard spezifiziert ein Signalisierungs-Protokoll am Q-Referenzpunkt, das primär auf jedem gewöhnlichen Kanal benutzt werden kann. Beide orientieren sich am bereits genannten OSI-Referenzmodell und arbeiten auf OSI-Schicht 3.

- **Ziele von Q.SIG**

  Allgemeine Daten [SIE02]:

  - Q.SIG = Signalisierung am Q-Referenzpunkt
  - 1988 durch Europäische Kommission initiiert
  - herstellerunabhängiger internationaler Standard
  - Ziel: Der offene Markt. „Jeder kann mit jedem", der Kunde kann frei wählen
  - heterogene Firmennetze mit Leistungsmerkmalen sollen möglich werden
  - Standard auf S_0/S_{2M}-Basis für die ISDN-Welt
  - basierend auf ITU-T-Empfehlungen für die Basisverbindungen

  Gründe für heterogene PBX-Netze:

  - Firmen fusionieren, Organisationen bilden internationale Verbünde
  - Netze mit Zweitlieferant aus politischen Gründen
  - Erstlieferant nicht mehr auf dem Markt

  Vorteile von Q.SIG:

  - Fremd- / Spezialprodukte in Verbindung mit Nebenstellenanlagen können angeschaltet werden (z.B. Multiplexer, Sprachspeichersysteme (VMS), Anrufverteilsysteme (ACD))
  - Fortschreibung des Standards entsprechend dem technischen Fortschritt und der Einführung neuer Funktionen

  Nachteil von Q.SIG: Die diversen Q.SIG-Normen lassen sehr viel Interpretationsspielraum zu

- **Beteiligte Kommissionen und Standardisierungsgremien**

  Die Q.SIG-Standards wurden durch ETSI und ISO zu europäischen und internationalen Standards erhoben. Die ISO hatte zeitgleich mit der ETSI einen Q.SIG-Standard unter der Bezeichnung PSS1 entwickelt und veröffentlichte ihren Standard, dem sich die ETSI angepasst hat, unter der Bezeichnung *ISO-Q.SIG*.

  Mitglieder des IPNS-Forums:

  - Alcatel Business Systems
  - Ascom Business Systems
  - Bosch Telecom
  - Ericsson
  - Lucent Technologies (AT&T)
  - Matra Communication
  - NORTEL

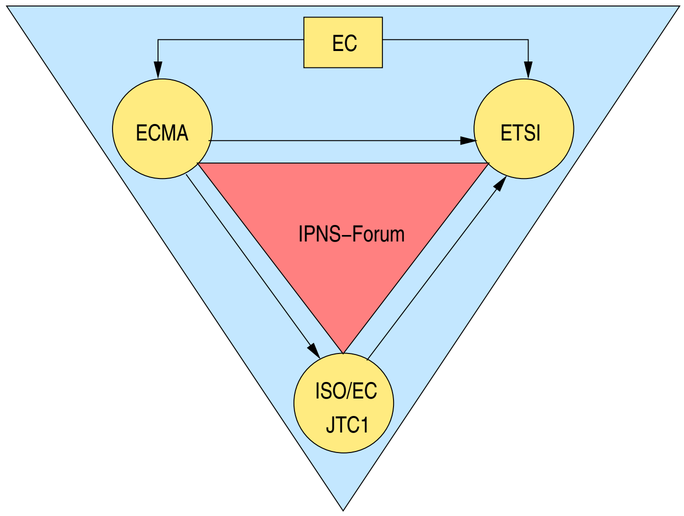

Abbildung 3.5: Q.SIG-Organisationen

  - Philips Communication Systems
  - Siemens

- **Q.SIG-Standards**

  Die folgende Abbildung 3.6 zeigt die Q.SIG-Standards, die nacheinander entwickelt wurden [SIE02].
  Erläuterungen:

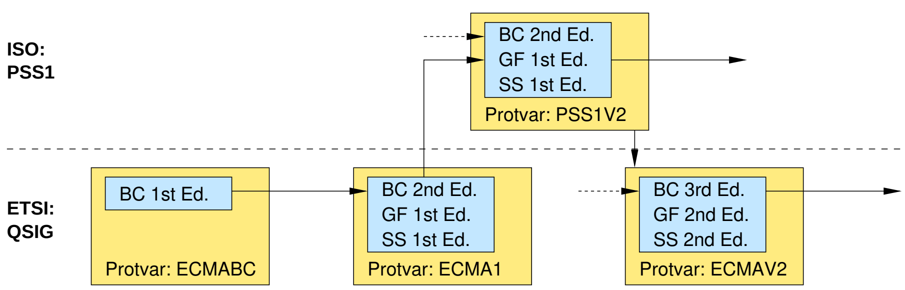

Abbildung 3.6: Q.SIG-Standards

BC : Basic Call

GF : Generic Functions

SS : Supplementary Services

Grundsätzlich bietet Q.SIG mit den sog. Generic Functions ein solides Fundament, um, ähnlich einem Baukastenprinzip, unterschiedliche Leistungsmerkmale auf dem Basic Call aufzusetzen.

  - Basic Call
    Der Basic Call hat als Basisverbindung dieselben Leistungsmerkmale wie bei ISDN.

  - Generic Functions
    Zu den Generic Functions gehören die Bereiche Namensanzeige, Rückruf sowie Gebührenanzeige.

Eine Besonderheit der Generic Functions ist das Generic Functional Protocol (GFP): Es dient dazu, Systeme eines Herstellers mit proprietären Protokollelementen im heterogenen Netz über Transitknoten anderer Hersteller miteinander zu verbinden [SIE02].

Voraussetzungen:

* Die proprietären Protokollelemente des einen Herstellers müssen gemäß dem GFP „verpackt“ sein.

* Der Transitknoten des anderen Herstellers muss GFP-Transitfunktionalität implementiert haben.

Die folgende Abbildung 3.7 verdeutlicht dies.
Da noch nicht alle Elemente des Siemens-proprietären Protokolls CorNet-NQ in Q.SIG

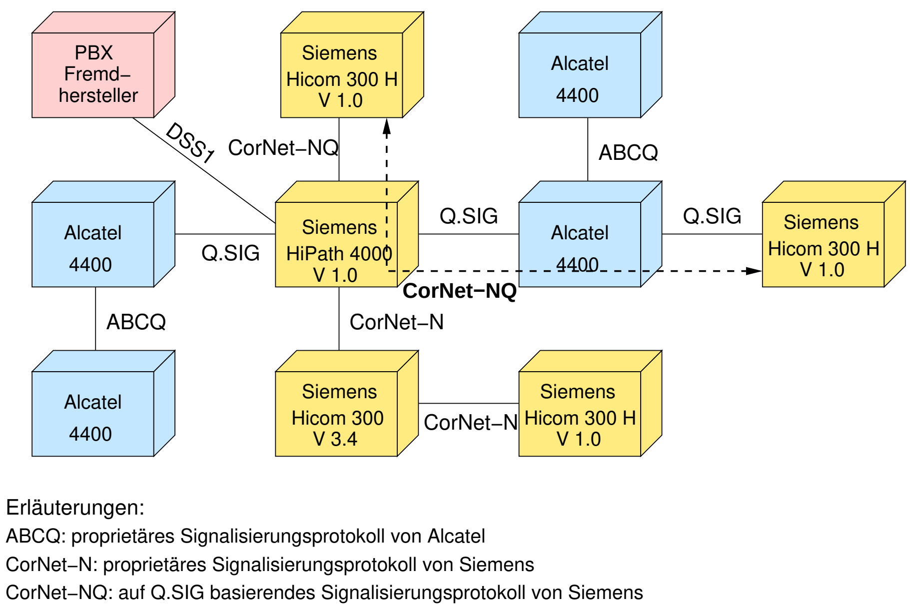

Abbildung 3.7: Beispielszenario für das Generic Functional Protocol

standardisiert sind, ist es möglich, über die Alcatel- 4400-Anlage (die das GFP implementiert haben muss) die proprietären CorNet-Protokollelemente transparent mittels des GFP zu übertragen.

Die Wirkungsweise des GFP wird in Abbildung 3.8 nochmals verdeutlicht.

– **Supplementary Services**
Die Supplementary Services stellen diverse Leistungsmerkmale dar, die grundsätzlich für ressourcenschonende B-Kanal-Nutzung gebraucht werden. Der Nutzer merkt von ihnen so gut wie nichts. Das wichtigste Leistungsmerkmal aus diesem Bereich ist „Path replacement“ (Wegeoptimierung, d. h. Verhinderung von Schleifenbildung). Die Funktion und der Nutzen werden in [SIE01] erläutert. Eine Aufstellung der wichtigsten derzeit in Q.SIG veröffentlichen Standards ist in Tabelle 3.2 zu finden.

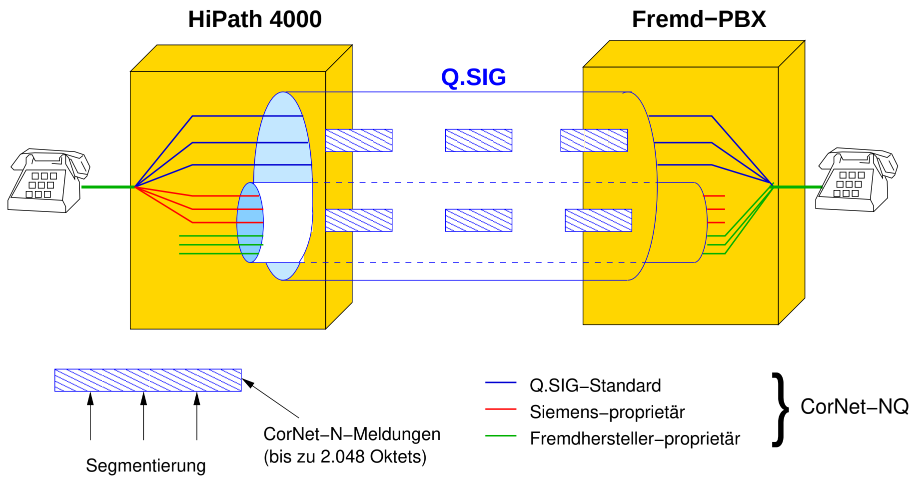

Abbildung 3.8: Funktionsweise des Generic Functional Protocols

3.2.6 Allgemeine TK-System-Ausstattungsmerkmale

Im Folgenden werden die allgemeinen Ausstattungsmerkmale eines TK-Systems beschrieben. Dies sind zum einen die Komponenten eines TK-Systems und zum anderen die Vorstellung von TK-System-Verbundnetzen.

3.2.6.1 Komponenten eines TK-Systems

Wenn man eine TK-Anlage als „black box“ (und diverse Zusatzkomponenten und Applikationen, wie z.B. ein Unified-Messaging-System außer Acht läßt) betrachtet, bietet ein TK-System folgende Dienste an:

- externe Verbindungen:
  - Verbindungen in das PSTN (Amtsanschlüsse)
    - Realisierung über S_0- bzw. S_{2M}-Schnittstellen
    - D-Kanal-Signalisierungsprotokoll: Q.931/DSS1
  - Verbindungen zu anderen TK-Anlagen in einem Systemverbund
    - Realisierung über S_0- bzw. S_{2M}-Schnittstellen
    - D-Kanal-Signalisierungsprotokoll: Q.931/DSS1 oder Q.SIG (Erläuterung in 3.2.5.2) oder proprietäres Signalisierungsprotokoll
- interne Verbindungen: Teilnehmeranschlüsse mittels
  - Analoganschlüssen: a/b-Ports (z. B. Faxgeräte Typ G3, analoge Teilnehmer)
  - ISDN-Anschlüssen: S0-Ports (z. B. Faxgeräte Typ G4, Datendienste)
  - Teilnehmeranschlüssen: U_{P0}- (zumeist proprietär) oder sonstigem Signalisierungsprotokoll für digitale Systemteilnehmer

Definition U_{P0}-Schnittstelle [SIE01]:
Die U_{P0}-Schnittstelle ist wie alle U-Schnittstellen eine Zweidrahtschnittstelle und wurde vom ZVEI festgelegt. Die Übertragung über diese Schnittstelle erfolgt im Halbduplex-Betrieb. Die Sende- und Empfangsdaten werden zeitlich getrennt in 125-Mikrosekunden-Rahmen übertragen. Um sowohl die zwei B-Kanäle

mit jeweils 64 kbit/s, einen D-Kanal mit 16 kbit/s als auch zusätzliche Synchronisationssignale und Schutzzeitperioden zu garantieren, beträgt die Dauer eines Binärsignals ca. 2 Mikrosekunden. Dies schränkt die Reichweite der Schnittstelle auf ca. 2 bis 4 km ein.
Somit sind bei einer U_{P0}-Schnittstelle alle ISDN-Merkmale möglich, wobei hier nur zwei Drähte verwendet werden (im Gegensatz zu S_0, das 4 Drähte benötigt, siehe 3.2.3). Dies stellt den Hauptvorteil dar, da bei einer Digitalisierung der Teilnehmernebenstellen der Umstellung von Analogbetrieb – der auch nur 2 Drähte benötigt – eine bestehende TK-Verkabelung nicht geändert werden muss.

3.2.6.2 TK-System-Verbundnetze

In 3.2.6.1 wurden TK-Systemverbünde bereits kurz angesprochen. Sie stellen eine Vernetzung von TK-Systemen über Festverbindungen dar, die (normalerweise) nicht über das PSTN sondern über eigene Festverbindungen geroutet werden, und werden heute sehr häufig von Unternehmen eingesetzt. Diese Festverbindungen müssen somit in Eigenregie betrieben und bezahlt werden.

Welche Vorteile bieten diese Verbundnetze trotz der u. U. hohen Kosten, die für Wartung und Betrieb dieser Verbundnetze anfallen?

Im Folgenden werden die wichtigsten Vorteile eines solchen Verbundnetzes angeführt:

- Ein Vorteil ist die **gemeinsame Nutzung zentraler Dienste** und die hiermit verbundene **Kosteneinsparung durch Synergieeffekte**: Bestes Beispiel hierzu ist die Telefonvermittlung. Angenommen, ein Unternehmen besitzt 3 Standorte mit jeweils etwa gleich vielen Mitarbeitern pro Standort. Durch die Schaffung eines Systemverbundes, der die TK-Systeme dieser drei Standorte miteinander vernetzt, ist nur eine zentrale Telefonvermittlung erforderlich (die die Vermittlungstätigkeit für die drei Standorte erledigt), die prozentual deutlich weniger Personalkapazitäten bindet (durch gemeinsame Vermittlungstätigkeit und geringere Personalreserven für urlaubs- und krankheitsbedingte Personalfehlzeiten) und so weniger Personal- und Infrastrukturkosten verursachen als bei einer nicht intern (sondern nur über das PSTN) vernetzten Variante.

- Ein weiterer Vorteil besteht in der **Einsparung von Telefongebühren** für netzinterne Gespräche: Durch ein TK-Verbundnetz können (bei korrekter Definition der Routingmechanismen, z. B. in LCR-Tabellen) Gesprächskosten für netzinterne Telefonate entfallen, die sonst an den jeweiligen Telefonnetz-Carrier zu zahlen gewesen wären. (Ohne Vernetzung hätte jeder Standort eine eigene Amtskopfnummer und wäre somit nur über das PSTN zu erreichen.)

- Hinsichtlich des **Corporate-Identity-Gedankens** hat für viele Unternehmen auch das **äußere Erscheinungsbild** und die Wahrnehmung in der Öffentlichkeit eine große Bedeutung: Durch den Einsatz von Verbundnetzen ist es möglich (einen passende Rufnummernplan für die Teilnehmernebenstellen vorausgesetzt), das Unternehmen für Außenstehende als Einheit darstellen zu können, d. h. alle Nebenstellen (egal wie weit entfernt die Standorte liegen) können über eine Amtskopfnummer erreicht werden. Ohne Vernetzung hätte jeder Standort eine eigene Amtskopfnummer, was zu großer Verwirrung bei Kunden, Geschäftspartnern und Investoren führen würde.

Diese Vorteile wiegen in den meisten Fällen die Kosten für den Betrieb des Verbundnetzes auf; daher haben sich viele Unternehmen zur Errichtung interner Verbundnetze entschieden.

Bisher wurden die Standards klassischer (auf dem Zeitmultiplexverfahren basierender) Telefontechnologie erläutert; außerdem wurden die Gründe für die Schaffung von unternehmensweiten Verbundnetzen dargelegt.
Im nächsten Abschnitt werden die für VoIP spezifischen Standards und Konzepte dargelegt, wobei auch hier viele Merkmale und Standards klassischer Telefontechnik verwendet werden.

3.3 Standards und Konzepte im VoIP-Umfeld

Die heutigen Standards und Protokolle im VoIP-Umfeld wurden und werden immer noch zum größten Teil von zwei Vereinigungen erarbeitet.

Zum einen von der IETF - der Internet Engineering Task Force - einer Gemeinschaft von Ingenieuren und Informatikern, die sich primär mit dem Standardisieren von Protokollen für die Internetwelt beschäftigen.

Zum anderen von der ITU - der International Telecommunications Union - einer internationalen Organisation innerhalb der Vereinten Nationen durch die Regierungen und der private Sektor die Weiterentwicklung und Standardisierung von globalen TK-Netzen und TK-Diensten koordinieren.

Die zwei derzeit wichtigsten Standards im VoIP-Umfeld sind H.323 und das SIP-Protokoll.
Im Folgenden werden der H.323-Standard und das SIP-Protokoll genauer vorgestellt.

3.3.1 Der H.323-Standard

Dieses Unterkapitel stellt den H.323-Standard vor. Hierzu werden zuerst Grundlagen von H.323 beschrieben; anschließend erfolgt die Erläuterung der H.323-Architektur.

3.3.1.1 Grundlegendes über H.323

Dieser von der ITU definierte Standard legt fest, wie PCs untereinander kommunizieren, um Audio- und Videodatenströme innerhalb von Computernetzwerken - z. B. im Intranet oder Internet - zu übertragen.

H.323 beschreibt die Struktur eines Videokonferenzsystems über paketbasierte Netzwerke und nimmt dabei auf verschiedene andere Standards (u. a. H.225 und H.245) Bezug. Man kann somit bei H.323 von einer „Sammlung von Standards“ sprechen.

Die erste Version von H.323 wurde im Jahr 1996 unter dem Namen „Packet based Multimedia Communication Systems“ veröffentlicht und ermöglichte multimediale Kommunikation über lokale Netzwerke (LAN). Zwei Jahre später erfolgte mit der zweiten Version von H.323 eine Erweiterung auf alle IP-basierten Netzwerke. Dazu gehören Local Area Network (LAN), Metropolitan Area Network (MAN) und Wide Area Network (WAN). Die zweite Version von H.323 wird heute häufig für VoIP-Lösungen verwendet.

Zusammen mit anderen Standards bildet H.323 eine Protokoll-Familie für Multimediakommunikation über verschiedene Netzwerke. So gibt es Spezifikationen für die Kommunikation über ISDN (H.320), ATM (H.321) und PSTN (H.324). Alle diese Systeme sind darauf ausgelegt, daß ihre Komponenten mit Endgeräten der anderen Konferenzsystemklassen kooperieren können. Der Standard spezifiziert sowohl Punkt-zu-Punkt-Verbindungen als auch Mehrpunkt-Verbindungen.

3.3.1.2 Die H.323-Architektur

- Bestandteile von H.323
  H.323 spezifiziert vier logische Komponenten: Terminals, Gateways, Gatekeeper und Multipoint Control Units (MCUs). Terminals, Gateways und MCUs werden als Endpunkte bezeichnet. Das Hauptziel von H.323 ist, den Austausch des Medienstroms zwischen den H.323-Endpunkten zu ermöglichen.
  Im Folgenden werden die vier logischen Komponenten von H.323 näher beschrieben:

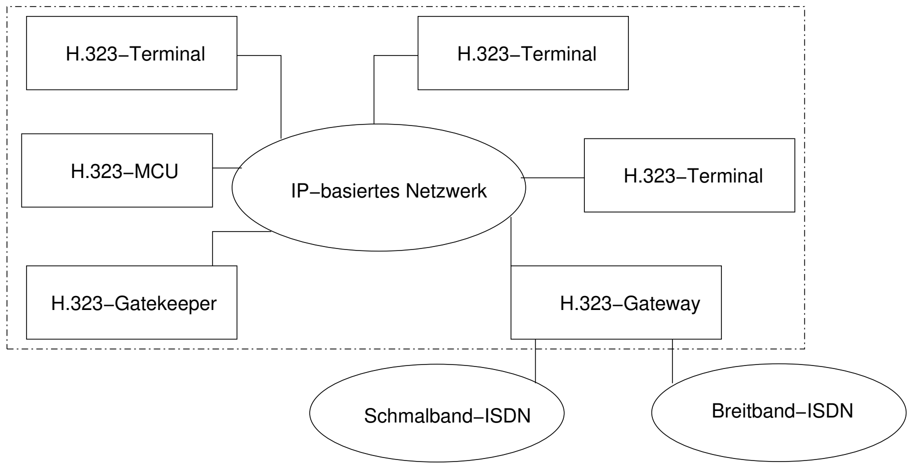

Abbildung 3.9: H.323-Bestandteile

– H.323-Terminal: Ein H.323-Terminal ist ein Netz-Endpunkt für die Echtzeitkommunikation mit anderen H.323- Endpunkten. Ein Terminal muss mindestens einen Audio-Codec unterstützen. Die meisten H.323-Terminals unterstützen jedoch mehrere Audio- und Video-Codecs.

– H.323-Gateway: Ein H.323-Gateway ist ein Netz-Endpunkt, der einen Übersetzungsdienst zwischen H.323- Netzwerk und Netzwerken anderer Typen anbietet. Eine Seite des Gateways unterstützt H.323-Signalisierung und beendet die Paketübertragung nach der Anforderung von H.323. Die andere Seite des Gateways ist die Schnittstelle zu einem leitungsvermittelten (circuit-switched) Netzwerk und unterstützt dessen Übertragungseigenschaften und Signalisierungsprotokolle.
  Auf der H.323-Seite hat das Gateway die Eigenschaft eines H.323-Terminals. An der leitungsvermittelten Seite hat das Gateway die Eigenschaft eines Knotens des entsprechenden Netzes.
  Ein H.323-Gateway bietet unterschiedliche Dienste an, die in der H.246-Empfehlung spezifiziert sind:

  * Übersetzung zwischen Übertragungsformaten (z.B. H.225 zu H.221) und zwischen Kommunikationsprozeduren (z.B. H.245 zu H.242).

  * Verbindungsaufbau und -abbau, sowohl auf der Netzwerk- als auch auf der PSTN-Seite

  * Übersetzung zwischen unterschiedlichen Video-, Audio- und Datenformaten

– H.323-Gatekeeper: Ein Gatekeeper ist ein optionaler Bestandteil im H.323-Netzwerk; er wird in größeren Systemen meistens eingesetzt. Wenn vorhanden, steuert der Gatekeeper einige H.323-Terminals, Gateways und MCs (Multipoint Controllers). Steuerung heißt, daß der Gatekeeper die ihm zugeordneten Terminals und sonstigen Geräte von Vermittlungsfunktionen entlastet.
  Die Gruppe von Terminals, Gateways und MCs, die ein Gatekeeper kontrolliert, wird als Zone des Gatekeepers bezeichnet. Innerhalb einer Zone kann nur ein logischer Gatekeeper aktiv sein.
  Die wichtigsten Aufgaben eines Gatekeepers umfassen:

  * Adreßübersetzung zwischen Alias-und Transportadressen (also z. B. E.164-Rufnummern in IP-Adressen)

  * Zonenmanagement der registrierten Endgeräte sowie Zugriffssteuerung mit Hilfe von Autorisierungsmechanismen:
    Bei Verwendung eines Gatekeepers für die Verbindungssteuerung wird eine Registrierung des Endgeräts beim Gatekeepers durchgeführt werden. Diese Registrierung erfolgt mittels

spezieller Nachrichten (Gatekeeper-Request), die über ein Multicast übermittelt werden, um den zuständigen Gatekeeper zu finden; anschließend erfolgt die Bestätigung der Registrierung (Gatekeeper Confirmation) bzw. die Ablehnung (Gatekeeper Reject).
Die Registrierung am Gatekeeper wird mittels „Registration, Admission and Status" (RAS)-Nachrichten über H.225.0 durchgeführt. Dabei wird - wie später erläutert - die RAS-Signalisierung über einen eigenen Datenkanal unabhängig vom „H.225.0 Call Signalling Channel" und dem „H.245 Control Channel" abgewickelt. Die Registrierung eines Endgeräts ist für die Erreichbarkeit eines Teilnehmers unter einer bestimmten Rufnummer bzw. Adresse notwendig und geschieht zeitlich vor dem ersten Ruf bzw. der ersten Rufannahme.

∗ Rufsteuerung und -signalisierung
Zu Beginn des Verbindungsaufbaus wird ein Rufsignalisierungskanal geöffnet, der direkt zwischen zwei Endgeräten aufgebaut wird, falls kein Gatekeeper vorhanden ist. Ist ein Gatekeeper vorhanden, entscheidet dieser selbst, ob der Steuerkanal direkt zwischen den Endgeräten mit der Methode des *Direct Routed Signalling* (siehe Abbildung 3.10) oder zwischen den jeweiligem Endgerät und Gatekeeper mit der Methode des *Gatekeeper Routed Signalling* (siehe Abbildung 3.11) aufgebaut wird.

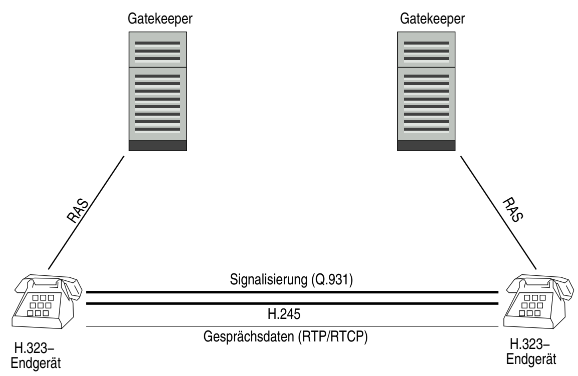

Abbildung 3.10: Direct Routed Signalling

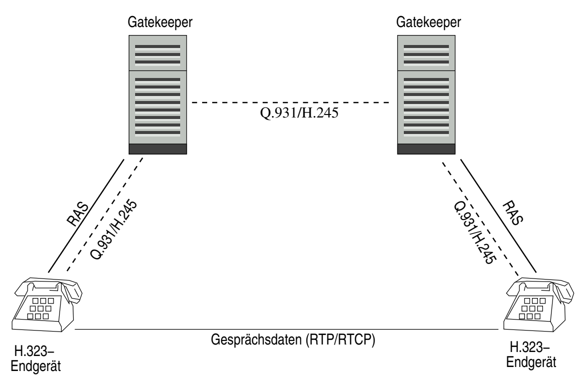

Abbildung 3.11: Gatekeeper Routed Signalling

– MC, MP und MCU: Ein Multipoint Controller (MC) ist ein H.323-Endpunkt, der Multipoint-Konferenzen zwischen zwei oder mehreren Terminals und/oder Gateways verwaltet.
Ein Multipoint Prozessor (MP) ist hingegen Teil einer MCU und empfängt Audio-, Video- und Datenströme von Endpunkten in zentralen Multipoint-Konferenzen und sendet diese nach erfolgter Verarbeitung zu den Endpunkten zurück.

Eine Multipoint Control Unit (MCU) nimmt einen zentralen Stellenwert in der Mehrpunktkommunikation ein, da sie die Unterstützung für Multipoint-Konferenzen anbietet. Sie besteht aus einem MC und kann durch ein oder mehrere MPs ergänzt werden.

- Der H.323-Protokoll-Stack
  Abbildung 3.12 zeigt den H.323-Protokollstack. Man unterscheidet zuverlässige und unzuverlässige

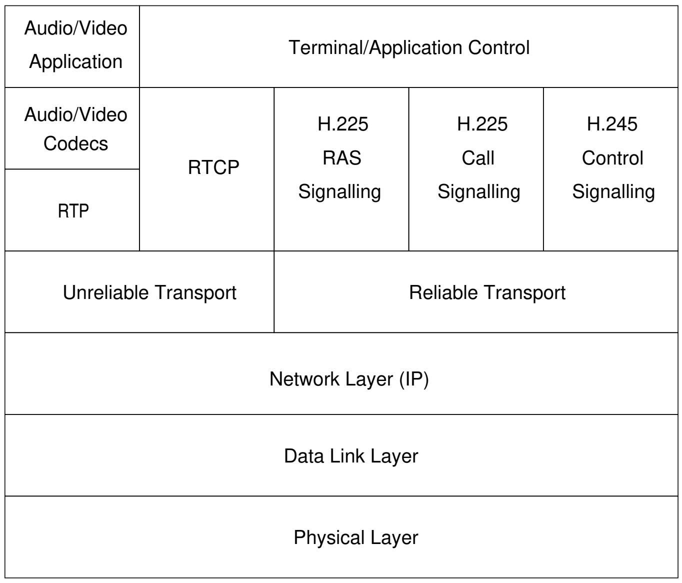

Abbildung 3.12: Protokollstack von H.323

  Transportprotokolle.
  In einem IP-Netz sind diese entsprechend das TCP- (Transport Control Protocol) und das UDP-Protokoll (User Datagram Protocol).
  Aus dieser Abbildung ist zu entnehmen, daß der Austausch von Medieninformationen bei H.323 durch Benutzung von RTP über UDP erfolgt. Eine Definition und Erläuterung von RTP erfolgt in 3.3.5. Über die Protokolle H.225 und H.245 erfolgt die Echtzeitübertragung der Nachrichten, die zwischen H.323-Endpunkten ausgetauscht werden. Die eigentlichen Signalisierungsinformationen zur Anrufsteuerung werden - wie in der TDM-basierten Technik- über das in 3.2.5 beschriebene Protokoll Q.931 übermittelt.

  Abbildung 3.13 zeigt den Ablauf eines H.323-Telefonats mittels Gatekeeper Routed Signalling. Hierbei wird deutlich, daß die signalisierungsrelevanten Informationen über das ISDN-Layer-3-Protokoll Q.931 abgewickelt werden, sodass insoweit volle Kompatibilität zu ISDN besteht.

3.3.2 Das SIP-Protokoll

In diesem Abschnitt wird das SIP-Protokoll beschrieben. Zuerst werden Grundlagen vorgestellt; danach erfolgt eine Einordnung von SIP in die IETF-Architektur.

3.3.2.1 Grundlegendes über das SIP-Protokoll

Das von der IETF standardisierte SIP-Protokoll (Session Initiation Protocol) nach RFC-3261 ist ein Signalisierungsprotokoll zum Aufbau, zur Verwaltung und zum Abbau von Multimediasitzungen. Dazu gehören z.B. IP-Telefonie und Multimediakonferenzen.

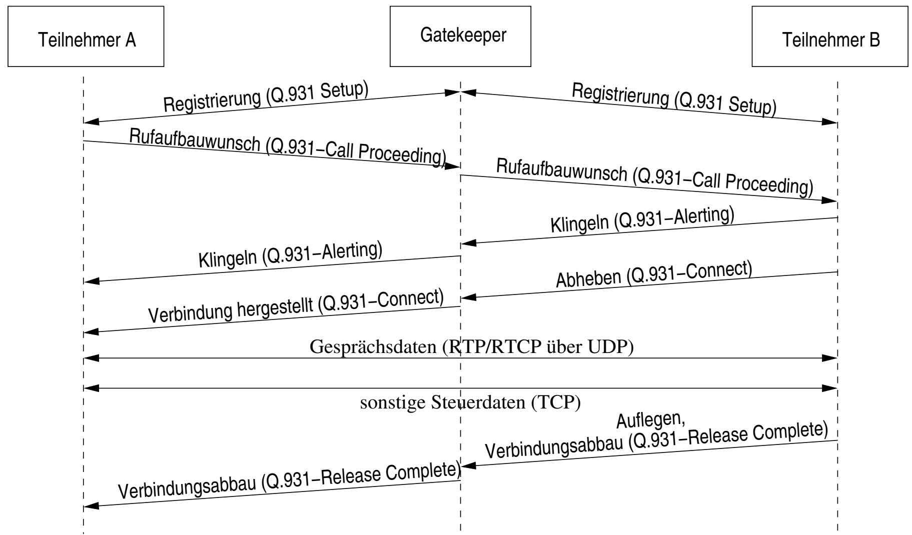

Abbildung 3.13: Ablauf eines auf H.323 basierenden Telefonats (Gatekeeper Routed Signalling)

Es ist ebenfalls das Protokoll für die Mobilkommunikation der dritten Generation (3G) des Universal Mobile Telecommunications Systems (UMTS) in der zweiten Phase der Netzrealisierung.
Im Vergleich zu „H.323“ ist „SIP“ die Bezeichnung für ein spezielles Protokoll. „H.323“ hingegen ist die Bezeichnung für den gesamten H.323-Stack mit RAS, H.225, H.245 bzw. den entsprechenden Codecs. Aus diesem Grund spricht man auch von „SIP-Protokoll“ und „H.323-Standard“.

3.3.2.2 Das SIP-Protokoll innerhalb der IETF-Architektur

SIP wurde von der IETF als Teil einer umfassenden Multimedia-Daten- und Kontrollarchitektur entwickelt, die im Vergleich zur H.323-Protokoll-Familie der ITU ein *Light Weight Session Model* darstellt.
SIP kann mit einer ganzen Reihe anderer IETF-Protokolle effizient „zusammenspielen“. Dabei ist SIP nicht von einem dieser Protokolle - die im Folgenden aufgelistet sind - abhängig, sie dienen lediglich zur Unterstützung.

- Session Announcement Protocol (SAP): Protokoll für die Anzeige von Multimediasitzungen über Multicast (RFC-2974)
- Description Protocol (SDP): Protokoll für die Beschreibung von Multimediasitzungen (RFC-2327)
- Resource Reservation Protocol (RSVP): Signalisierungsprotokoll zur Ressourcenreservierung (RFC-2205)
- Real-Time Transport Protocol (RTP): Echtzeitprotokoll für den Transport von isochronen Datenströmen und QoS-Rückmeldungen (RFC-1889)
- Real-Time Streaming Protocol (RTSP): Protokoll für die Kontrolle von Streaming Media (RFC-2326)

SIP ist für den Aufbau, die Kontrolle und die Terminierung einer Multimediasitzung zuständig. Es beschreibt, zusammen mit anderen Protokollen, die Eigenschaften und die Teilnehmer einer Sitzung. Prinzipiell kann ein beliebiges Transportprotokoll für den Transport von Medien in einer SIP-Sitzung benutzt werden, jedoch ist RTP das am meisten benutzte Protokoll.
Der folgende Header einer SIP-Invite-Nachricht zeigt den HTML-ähnlichen Aufbau von SIP beispielhaft:

Listing 3.1: Header einer SIP-INVITE-Nachricht

```
INVITE sip:bob@biloxi.com SIP/2.0
```

```
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSqe: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
...
Nachricht
...
```

SIP-Nachrichten und die eigentlichen Sitzungsdaten werden zumeist durch dasselbe physikalische Verbindungsmedium transportiert, jedoch sollte die SIP-Signalisierung separat behandelt werden. Abbildung 3.14

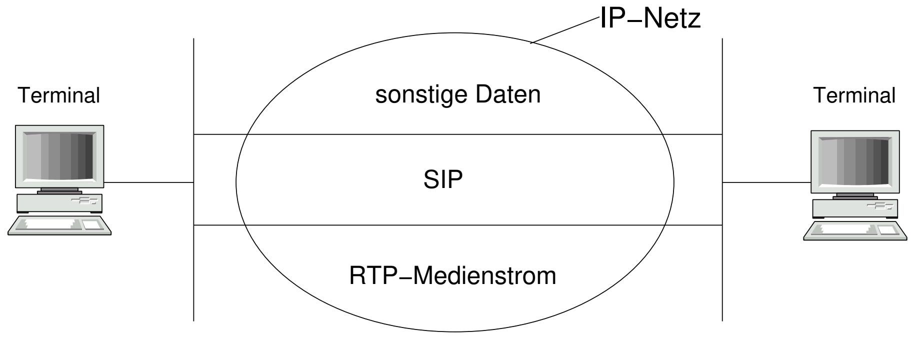

Abbildung 3.14: Trennung von Signalisierungs- und Mediendaten

zeigt die logische Struktur von Signalisierungs- und Sitzungsdaten.
Diese Trennung ist wichtig, da die Signalisierung mithilfe eines oder mehrerer Proxy- oder Redirect-Server am Ziel ankommen kann, während die Datenströme durch einen viel direkteren Pfad das Ziel erreichen. Diese Strategie ist analog zur Trennung von Signalisierungs- und Mediendaten bei H.323.
Das SIP-Protokoll hat eine Client-Server-Struktur, d.h. der Client stellt eine Anfrage an den Server, der Server bearbeitet die Anfrage und schickt die Antwort an den Client zurück oder leitet die Anfrage an einen anderen Server weiter. (In diesem Fall spielt der Server in der Weiterleitung wieder die Rolle eines Clients.) Anschließend sendet er die vom anderen Server kommenden Antworten an den Client zurück.
Abbildung 3.15 zeigt den SIP-Verbindungsaufbau mittels HTML-basierten Textnachrichten:

3.3.3 SIP vs. H.323

Das erst im Jahre 1999 erstmals veröffentlichte SIP-Protokoll stellt eine ernstzunehmende Alternative gegenüber dem „älteren Bruder“ H.323 für den Aufbau, die Kontrolle und die Terminierung für Multimediasitzungen dar.
In diesem Bereich gibt es bereits seit vielen Jahren zahlreiche Anwendungen, die auf H.323 aufgesetzt worden sind. Zum Beispiel die in der Windows-Welt recht bekannte Applikation „Netmeeting“.
Viele Hersteller steigen jedoch momentan von H.323 auf SIP um. Die Gründe hierfür werden durch die folgende Gegenüberstellung beider Protokolle verdeutlicht.

- Architektur: H.323 beschreibt nicht ein bestimmtes Protokoll, sondern ist eine monolithische Zusammenfassung von mehreren Protokollen, u. a. H.225 und H.245. Es definiert die Regeln für das Zusammenwirken dieser Protokolle. Die Architektur von H.323 ist vertikal. Die drei Signalisierungsgruppen gewährleisten verschiedene Aufgaben in einer Sitzung. Jede Änderung der Funktionalität in

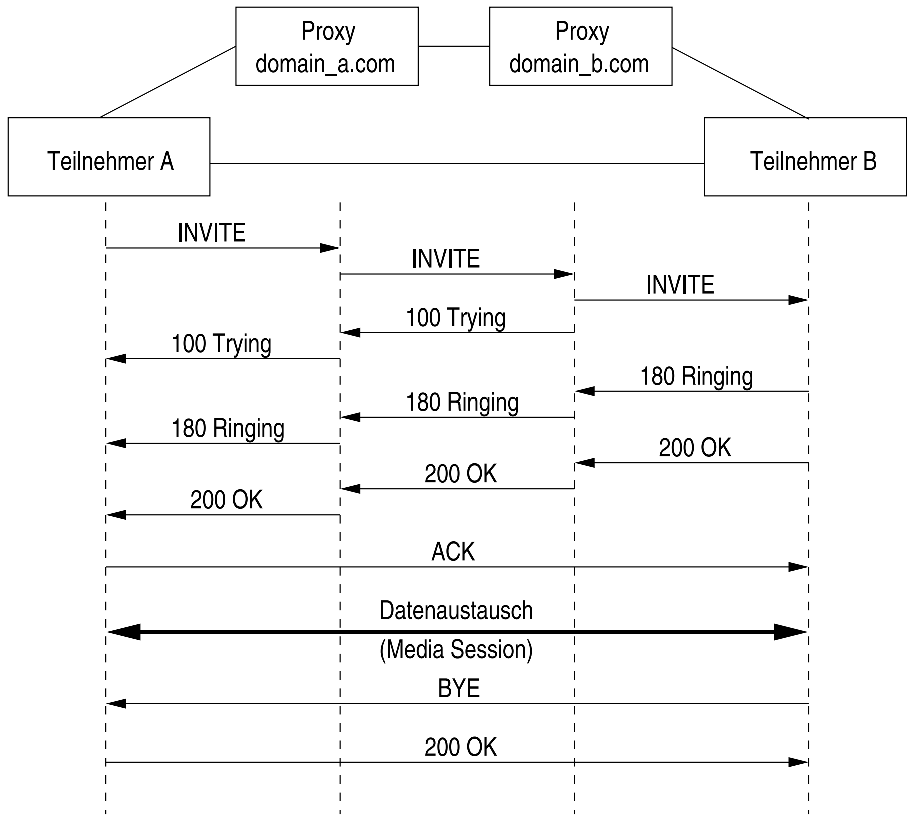

Abbildung 3.15: SIP-Verbindungsaufbau

einer Signalisierungsgruppe hat unmittelbare Auswirkungen auf die anderen Signalisierungsgruppen. Somit ist die Erweiterung von Features einer Anwendung enorm aufwendig. Falls irgendein Fehler in einer Signalisierungsgruppe existiert, besteht sogar die Gefahr, daß die gesamte Anwendung nicht benutzbar wird.
Im Vergleich zu H.323 ist SIP ein speziell für die Multimediakommunikation entwickeltes Protokoll. Es hat eine modulare Architektur, wodurch die Erweiterbarkeit deutlich unproblematischer ist als bei H.323. Zum Beispiel kann die Information über die zu übertragenden Medien über SDP beschrieben und anschließend bei SIP in den Nachrichtenteil integriert werden, während bei H.323 eine solche Beschreibung in einer separaten H.245-Nachricht verfasst werden muss.

- Codec-Unterstützung: Unter H.323 können nur Audio- und Video-Codecs nach den ITU-Standards verwendet werden. Eine solche Beschränkung gibt es bei SIP nicht. Da bei SIP die Codec-Informationen in SDP beschrieben werden können und damit keine dem Medienformat entsprechende Änderung in den SIP-Nachrichten gemacht werden muss, besteht nur das Problem, ob beide Gesprächsparteien über eine Applikation zur Bearbeitung der Medien verfügen. Deswegen sind mit SIP alle Codecs benutzbar.

- Transport: Im Gegensatz zu H.323 kann SIP sowohl mit TCP als auch mit UDP arbeiten. Die Verwendung von UDP führt bei Paketverlusten zu einer geringeren Systembelastung. Somit ist UDP für den Transport von Echtzeit-Daten besser geeignet als TCP. Da TCP sicherstellt, daß die Pakete vollständig und in der richtigen Reihenfolge beim Ziel kommen, wird durch Paketverluste eine große Zeitverzögerung im Netz verursacht, was für Echtzeit-Kommunikation unerwünscht ist. UDP gewährleistet im Vergleich zu TCP keinerlei Sicherheit für ein erneutes Senden der verlorenen Pakete, was ein besonderes Augenmerk auf die Implementierung eines Quality-of-Service-Mechanismus erfordert, weil eine zu hohe Paketverlustrate eine für den Nutzer inakzeptable Sparchqualität be-

dingt.
Bei H.323 muss der Gatekeeper, welcher für das Routing von Gesprächen zuständig ist, für die Dauer des Gesprächs die Datenströme verarbeiten und bei mehreren Teilnehmern mehrere TCP-Verbindungen halten. Im Vergleich dazu gibt es bei SIP keine Netzwerkkomponente, die unbedingt mit TCP arbeiten muss.

- Konferenzmodell: Bei SIP kann jeder Benutzer Anfragen an Multicast-Adressen verschicken, ohne spezielle Netzwerkkomponenten zu benötigen. Im Vergleich dazu ist bei der Benutzung von H.323 für die Realisierung einer Mehrparteienkonferenz eine MCU oder eine MC sowie ein MP unverzichtbar.
  Das Konferenzmodell ist somit bei SIP verteilt und bei H.323 zentralisiert. Obwohl mit Hilfe einer MCU eine dezentralisierte Konferenz auch beim H.323-Standard realisiert werden kann, wird dieses „dezentralisierte“ Modell zerstört, falls die MCU die Konferenz verlässt.
- Teilnehmer-Adressierung: Bei H.323 kann die Adressierung der Teilnehmer über URLs, E.164-Nummern (Telefonnummern im internationalen Format, also z. B. +498921803456) oder über Alias-Adressen erfolgen, wohingegen sie bei SIP die Adressierung nur über URLs definiert ist.

3.3.4 Kodierungsstandards

In diesem Abschnitt werden die gebräuchlichsten Kodierungsstandards im VoIP-Umfeld genannt [NOE03], wobei hier nicht auf die Algorithmen der Kodierung bzw. Kompression eingegangen wird, da dies den Umfang der Arbeit sprengen würde.

Die in VoIP-Anwendungen verwendeten Audiokodierungen sind durchweg ITU-T-Standards. Sie haben sich in der Festnetztelefonie und anderen Bereichen bewährt. An dieser Stelle sind keine Literaturverweise enthalten, da die Kodierungsstandards nur kurz vorgestellt werden.

- G.711: Der Standard kodiert reine PCM-Daten mit 8 Bit Auflösung und 8 kHz Samplingrate, was 64 kbps ergibt. Dieser Codec ist vorteilhaft, da er zum einen ohne Komprimierung arbeitet (was keine Zeitverzögerung durch das Komprimieren/Dekomprimieren impliziert) und zum anderen auch bei klassischer TDM-basierter Technik verwendet wird.
- G.721: Adaptive Variante der PCM-Kodierung (G.711). Sie erreicht bei 4 Bit Auflösung mit 32 kbps die halbe Datenrate bei kaum wahrnehmbarem Qualitätsverlust.
- G.723: Eine Erweiterung von G.721 mit 24 bzw. 40 kbps.
- G.726: Eine variable ADPCM-Kodierung (*Adaptive Differential PCM*) mit 16, 24, 32, 40 kbps bei 8 kHz Samplingrate
- G.729: Komprimierungsverfahren gemäß *Conjugate-Structure Algebraic-Coide-Excited Linear-Prediction* mit 8 kbps; dieser Algorithmus basiert auf einem Hybridverfahren aus PCM- und Quellkodierung.

Derzeit werden meist G.711, G.723 und G.729 verwendet; Tabelle 3.3 stellt die genannten Standards gegenüber, wobei hier auch der Mean Opinion Score (MOS) angegeben wird.
Der MOS ist eine von den Bell Labs definierte Skala, die statisch das Empfinden der Sprachqualität durch Benutzer ermittelt ([SIE01]).
Hierzu wird die Sprachqualität durch Testpersonen bewertet; er stellt somit eine subjektive Einschätzung dar. Durch eine repräsentative Personenmischung (sowohl zahlenmäßig als auch anteilmäßig nach Nutzergruppen) läßt sich hierdurch eine (annähernd) objektive Bewertung ermitteln, da sich die „Ausreißer“ wegen der Durchschnittsberechnung nivellieren.
Der MOS reicht zwischen einer Spanne von 1 bis 5 (die Werte repräsentieren folgende Qualitätseinschätzungen, [P.800]):

- „1“: mangelhaft (keine Kommunikation möglich)

- „2“: mäßig
- „3“: ordentlich
- „4“: gut
- „5“: exzellent (kein Unterschied zum Original).

Für die Sprachübertragung in Carrier-Netzen ist der MOS-Wert größer 4 und entspricht damit der ITU-Empfehlung für die sogenannte „Toll Quality“. Zum Vergleich: Die Sprachqualität in Mobilfunknetzen wird heute mit dem Begriff „Business Quality“ beschrieben, was einem MOS kleiner 4 entspricht ([P.800] und [SIE01]).

3.3.5 Gemeinsam verwendete Protokolle (RTP/RTCP)

Das Real Time Transport Protocol [SCHU96] der IETF hat sich weltweit als Übertragungsstandard für Audio- und Video-Echtzeitdaten durchgesetzt und wird bei VoIP stets als Protokoll für die Übertragung der Sprachtelefonie eingesetzt. Das Protokoll arbeitet verbindungslos, sodaß ein Sender – bei alleiniger Betrachtung des RTP-Protokolls – theoretisch ohne aktiven Empfänger beginnen kann, Daten zu senden. RTP bietet keinerlei Mechanismen, die eine Übermittlung der Pakete an den Empfänger sicherstellen. Es wird lediglich eine Statistik über die Qualität der Übertragung geführt, aus der sich Rückschlüsse auf den QoS ziehen lassen.

RTP ist unabhängig von den unterliegenden Protokollschichten, wird aber überlicherweise in Zusammenhang mit UDP verwendet, wie in 3.3.1.2 und 3.3.2 erläutert wird. Dabei werden RTP-Pakete als Nutzdaten in UDP-Pakete eingebettet. Es ist in der Lage, sowohl *Unicast*-Datenströme zwischen einem Sender und einem Empfänger als auch *Multicast*-Datenströme zwischen einem Sender und mehreren Empfängern auszutauschen (häufig Mehrpunktkonferenzen).

Für jede Datenquelle wird eine eigene RTP-Sitzung, auch als *RTP-Session* bezeichnet, und bei Verwendung von UDP ein Portpaar festgelegt. Ein Port wird für die Übertragung von Nutzdaten mit RTP-Paketen, der zweite für die Übertragung von Informationen über die Dienstgüte der Sitzung verwendet. Hierfür wird das *RTP Control Protocol* (RTCP) verwendet, das zusammen mit RTP in [SCHU96] spezifiert worden ist.

Das RTP-Protokoll besteht aus zwei Teilen: RTP selbst überträgt die Nutzdaten. Es führt eine Sequenznumerierung durch, damit die Pakete auf Empfangsseite sortiert werden können, falls sie in falscher Reihenfolge eintreffen. Durch die Verwendung von Zeitstempeln können Übertragungsparameter wie Round-Trip-Time (RTT), Delay und Jitter berechnet werden.

Der zweite Teil (RTCP) enthält ein eigenes Protokoll zur Kontrolle des RTP-Datenflusses. Es tauscht QoS-Informationen zwischen Sendern und Empfängern aus. Sender verwenden den sogenannten *Sender-Report* (SR), um einem oder mehreren Empfängern Informationen zu übermitteln, während Empfänger den *Receiver-Report* (RR) zum Versand der Empfangsstatistik einsetzen.
Die Abbildung 3.16 zeigt einen RTP-Protokollablauf beispielhaft.
Endgeräte können, wie bei Sprachtelefonie der Fall, gleichzeitig Sender und Empfänger sein. In diesem Fall wird der SR verwendet. Als Sender wird ein Endgerät definiert, das seit dem letzten verwendeten Report selbst RTP-Nutzdaten gesendet hat.

Sitzungsteilnehmer, die RTP-Pakete (also Nutzdaten) empfangen, übermitteln ihre Empfangsstatistik dem sendenden Teilnehmer mit Hilfe von SR- oder RR-Paketen. SR-Pakete enthalten für einen Teilnehmer die Information, wie viele RTP-Datenpakete er seit dem letzten empfangenen Report der sendenden Station erhalten haben müßte. Sender übermitteln dabei mit Hilfe des SR-Pakets die Anzahl Pakete, die insgesamt während der Verbindung gesendet wurden. Empfangende Teilnehmer können diese Information mit dem zuletzt erhaltenen Report-Paket vergleichen. Auf diese Weise läßt sich ermitteln, ob alle Datenpakete

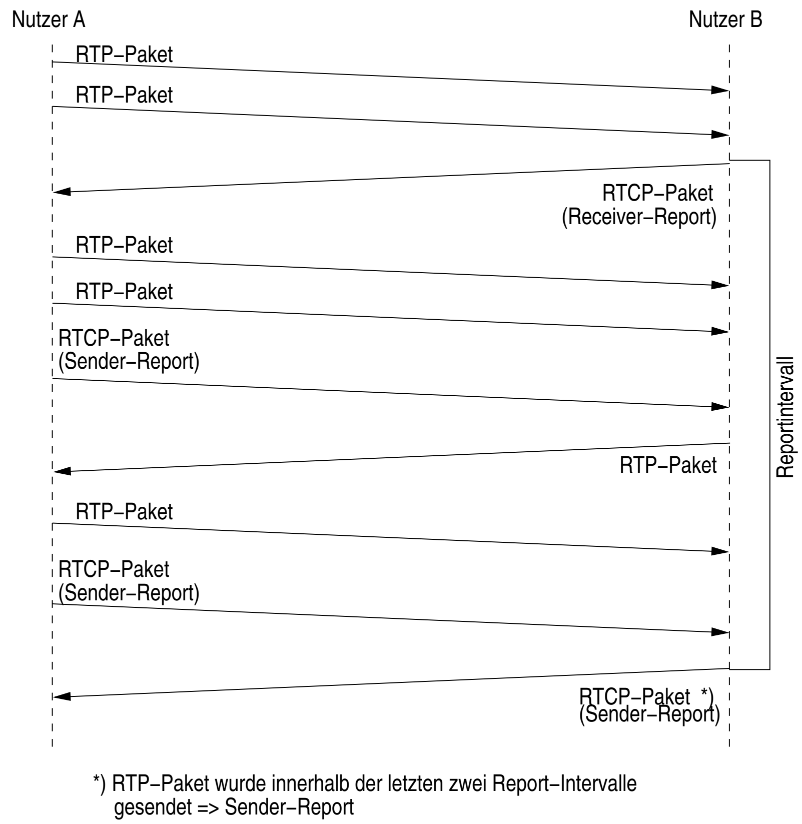

Abbildung 3.16: RTP-Protokollablauf

empfangen wurden. Zusätzlich ist ein Datenfeld *Fraction Lost* enthalten, das die Anzahl verlorener Pakete zu der erwarteten Paketanzahl ins Verhältnis setzt.

Sowohl Sender als auch Empfänger nehmen diese Informationen lediglich zur Kenntnis, veranlassen bei Verlust von Daten jedoch kein wiederholtes Senden. Genügt die Übertragungsstrecke festgelegten Anforderungen nicht, kann ein Abbruch der Verbindung von jedem Verbindungspartner durchgeführt werden.

Das RTP-Protokoll legt keine Reaktion auf schlechte Übertragungsgüte fest. Wenn beispielsweise die Paketverlustrate steigt, kann jedoch eine sendende Applikation selbst aufgrund der empfangenen Statistikdaten reagieren und das Datenvolumen reduzieren. Im Fall von VoIP könnten eine Umschaltung auf einen stärker komprimierenden Codec (siehe 3.3.4) initiiert werden. Ein solches während einer Verbindung ist nicht verbreitet, dennoch aber möglich, und muß von dem jeweils eingesetzten Signalisierungsprotokoll unterstützt werden.

RTCP enthält neben den reinen Report-Funktionen noch eine minimale Sitzungssteuerung. Neue Sitzungsteilnehmer veröffentlichen ihre Teilnahme durch das Senden von Sender- und Receiverreports, währen ein spezielles *RTCP-BYE*-Paket allen Teinehmern die Abmeldung aus einer Sitzung mitteilt.

Die Zeitabstände zwischen zwei Reports werden aufgrund der verwendeten Bandbreite, der Teilnehmerzahl einer Sitzung und der Rolle als Sender bzw. Empfänger berechnet. Die IETF empfiehlt, das RTCP-Datenvolumen auf 5% der verfügbaren Sitzungs-Bandbreite für alle Teilnehmer einer Sitzung zu begrenzen.

3.4 Zusammenfassung

In diesem Kapitel wurden zuerst der Dienstbegriff von VoIP spezifiziert und danach die Grundlagen klassischer TK-Technik wie ISDN, Signalisierungsprotokolle und Verbundnetze erläutert.
Anschließend wurden die grundlegenden Standards von VoIP – H.323 und SIP – dargestellt, wobei in der Anrufsignalisierung weiterhin ISDN-Protokolle verwendet werden, was bedeutet, daß die grundlegenden Techniken auch bei VoIP verwendet werden.
Darauf aufbauend wurden die bei VoIP verwendeten Kodierungsstandards sowie die Trennung und unterschiedliche Behandlung von Sprach- und Signalisierungsdaten vorgestellt; abschließend wurden noch auf die Problematik der Stromversorgung der VoIP-Endgeräte eingegangen.
Damit sind nun die Grundlagen von VoIP gelegt.
Im nächsten Kapitel wird ein Anforderungskatalog für den Einsatz von VoIP-Systemen erstellt, wobei die Kriterien, die in diesem Katalog aufgeführt werden, als K.o.-Kriterien verstanden werden, da einerseits bei Nichterfüllung dieser Kriterien die Akzeptanz eines VoIP-Systems nicht vorhanden und zum anderen der Einsatz nicht sinnvoll implementiert und gemanagt werden könnte.

Q.SIG Service Name (english)	**Q.SIG Service Name (deutsch)**	**ECMA name**	**ECMA Standard and date of publication**	**ETSI Standard and date of publication**	**ISO/IEC Standard and date of publication**
Call Offer	Anklopfen	CO	ECMA-192 3. edition Juni 1997	EN 300 362 v1.2.1 März 1999	ISO/IEC 14843 1996
Do Not Disturb / Override	Ruhe vor dem Telefon / Aufheben	DNDO	ECMA-194 3. edition Juni 1997	EN 300 364 v1.2.1 März 1999	ISO/IEC 14844 1996
Call Intrusion	Aufschalten	CI	ECMA-203 3. edition Juni 1997	EN 300 426 v1.2.1 März 1999	ISO/IEC 14846 1996
Advice of Charge, Start of Call	Gebührensanzeige vor der Verbindung	AOC-S	ECMA-212 2. edition Juni 1997	EN 301 264 v1.1.1 Oktober 1998	ISO/IEC 15050 1997
Advice of Charge, During Call	Gebührenanzeige während der Verbindung	AOC-D	ECMA-212 2. edition Juni 1997	EN 301 264 v1.1.1 Oktober 1998	ISO/IEC 15050 1997
Advice of Charge, End of Call	Gebührenanzeige nach der Verbindung	AOC-E	ECMA-212 2. edition Juni 1997	EN 301 264 v1.1.1 Oktober 1998	ISO/IEC 15050 1997
Recall	Rückruf	RE	ECMA-214 2. edition Juni 1997	EN 301 258 v1.1.1 Oktober 1998	ISO/IEC 15052 1997
Call Interception	Abhören	CINT	ECMA-221 2. edition Juni 1997	EN 301 265 v1.1.1 Oktober 1998	ISO/IEC 15054 1997
Transit Counter	Anzahl der Übermittlungsknoten	TC	ECMA-225 2. edition Juni 1997	EN 301 048 v1.1.1 September 1997	ISO/IEC 15056 1997
Message Waiting Indication	Briefkastenlampe	MWI	ECMA-242 2. edition September 1997	EN 301 255 v1.1.1 Oktober 1998	ISO/IEC 15506 1997
Common Information	Allgemeine Informationen	CMN	ECMA-251 2. edition Dezember 1998	EN 301 820 v1.1.1 Oktober 2000	ISO/IEC 15772 1998
Call Priority Interruption / Protection	Anrufprioritätsunterbrechung /-schutz	CPIP	ECMA-264 2. edition Dezember 1998	EN 301 656 v1.1.1 August 1999	ISO/IEC 15992 1998
PUM (Personal User Mobility) Registration	PUM (Personal User Mobility) Registrierung	PUMR	ECMA-282 3. edition Dezember 2001	EN 301 821 v1.1.1 Oktober 2000	ISO/IEC 17876 2000
PUM Call Handling	PUM Anrufhandling	PUMCH	ECMA-284 3. edition Dezember 2001	EN 301 657 v1.2.1 Juni 2003	ISO/IEC 17877 2000

Tabelle 3.2: Q.SIG-Leistungsmerkmale ([Q.SIG01])

Standard	Verfahren	Bandbreite [kbps]	Quanti-sierung [bit]	Band-breite [kHz]	Mean Opinion Score (MOS)	Frame-größe [ms]	typische Verzöge-rung [ms]
G.711	PCM	64	8	3,3	4,4	Sample	0,125
G.721	ADPCM	32	8	3,3	4,2	Sample	0,125
G.723	ACELP	24/40	8	3,3	4,0	Sample	30
G.726	ADPCM	16/24/32/40	8	3,3	3,3 - 4,2	Sample	0,125
G.729	CS-ACELP	8	8	3,3	3,9	10	15

Tabelle 3.3: gebräuchliche Kodierungsstandards im Vergleich

Kapitel 4

Erstellung eines Anforderungskatalogs

Beim Einsatz eines VoIP-Systems müssen diverse Anforderungen erfüllt sein, um zum einen eine für die Kunden und Anwender akzeptable Telefonielösung darstellen und realisieren zu können und zum anderen – im Vergleich zu klassischer Telefonietechnik – in einem wirtschaftlich tragbaren Umfang rechtfertigen zu können. Der Anforderungskatalog legt ein besonderes Augenmerk auf eine dienstfokussierte Betrachtung (z. B. Benutzerfreundlichkeit, Verfügbarkeit und angemessene Dienstqualität), da die Nutzer und Anwender hierauf bestehen (ein häufiger Ausspruch lautet: „Wozu brauchen wir eine neue Technik, wenn sie nicht die gleiche Leistung wie die bisherige bietet? Mir ist egal, wie die Technik aufgebaut ist, sie muß funktionieren.“).
Daher erfolgt eine Aufteilung auf die Anforderungen aus Kunden- und Anwendersicht sowie hinsichtlich wirtschaftlicher Anforderungen, wobei beide Teilbereiche in etwa gleich gewichtet sind (aus Nutzer- bzw. Betreibersicht). Innerhalb der jeweiligen Abschnitte erfolgt eine Gewichtung nach der Reihenfolge der Aufzählung (je früher genannt, desto wichtiger).
Die Gewichtung der Anforderungen basiert auf [TAY04]; darin wurden Unternehmen und Behörden u.a. zu den Anforderungen, die sie für den Einsatz von VoIP-Systemen als verpflichtend sehen, befragt. Abbildung 4.1 zeigt das Ergebnis dieser Umfrage (die fünf häufigsten Antworten), wobei Mehrfach-

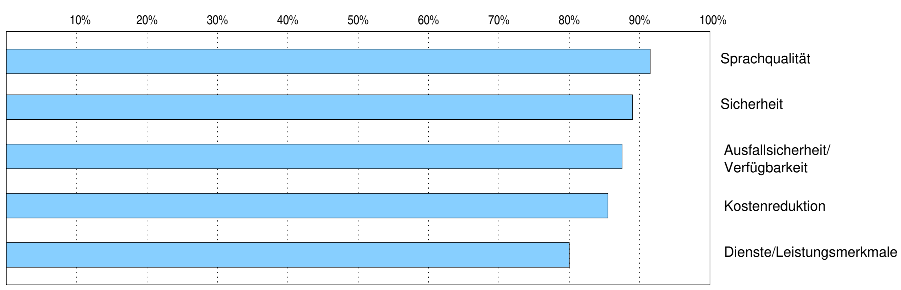

Abbildung 4.1: Anforderungen an VoIP-Systeme [TAY04]

nennungen möglich waren. Diese Anforderungen sind (fast) mit den in Kapitel 2.4 aus Sicht der Bezirksfinanzdirektion München vorgestellten identisch, obwohl sie in Unkenntnis dieser Studie aufgestellt wurden; sie werden daher – auch hinsichtlich der Gewichtung als repräsentativ angesehen (wobei eine Betonung auf der dienstorientierten Betrachtung liegt).
Wenn eine/mehrere (gewichtige) Anforderungen von einem Anbieter nicht erfüllt werden können, sollte sich der Nutzer überlegen, den Anbieter zu wechseln. Insofern kann man hierbei von K.o.-Kriterien für den Einsatz eines VoIP-Systems sprechen.
Diese Anforderungen betreffen auch einen Großteil der im Managementkonzept (siehe Kapitel 6 behandelten Fragestellungen, sodaß hier eine detaillierte Ausarbeitung des Anforderungskatalogs erfolgt.

4.1 Anforderungen aus Kunden-/Anwendersicht

Aus Kunden-/Anwendersicht wurden die in den folgenden Abschnitten erläuterten Anforderungen identifiziert (wobei die in Abbildung 4.1 genannten Anforderungen integriert sind).

4.1.1 Sprachqualität

VoIP bedeutet, dass die Sprachdaten über ein IP-Datennetz geleitet werden (siehe Kapitel 3). IP-basierte Netze verwenden Nachrichtenvermittlung (message switching, store-and-forward) als grundlegendes Vermittlungsverfahren und sind deswegen verbindungslos. Hierbei nimmt jedes Transitsystem entlang des Weges die komplette Nachricht entgegen und speichert diese zwischen. Falls das nächste Wegstück nicht belegt ist, wird die Nachricht weitergesendet, sonst muss gewartet werden, bis dieses Wegstück frei ist. Das Prinzip der Nachrichtenvermittlung ist in Abbildung 4.2 dargestellt.

Demgegenüber wird bei herkömmlicher TK-Technologie Leitungsvermittlung (Durchschaltung,

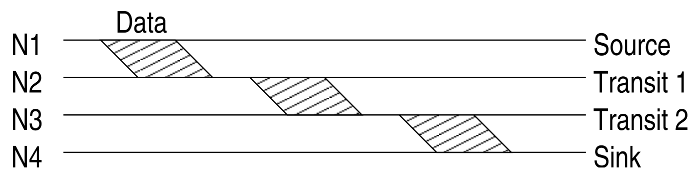

Abbildung 4.2: Prinzip der Nachrichtenvermittlung

circuit switching) verwendet. Das bedeutet, dass das Verbindungsaufbausignal gemäß eines Wegewahlalgorithmus durch das Netz zum Zielsystem geleitet wird. Es teilt dabei den Transitsystemen den Ressourcenbedarf mit. Nach einer positiven Quittung steht für die gesamte Verbindungszeit ein dedizierter Übertragungskanal zur Verfügung (verbindungsorientiert). Abbildung 4.3 zeigt dieses Prinzip.

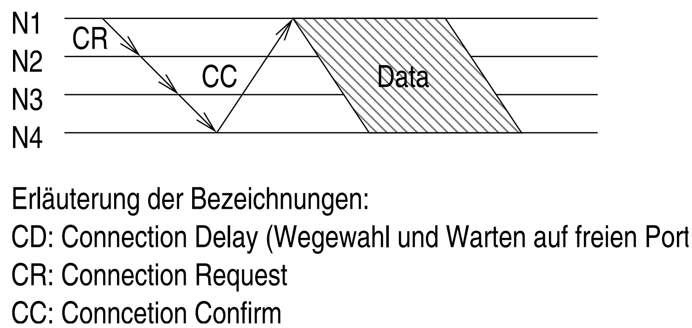

Abbildung 4.3: Prinzip der Leitungsvermittlung

Somit stellt VoIP die Herausforderung dar, die Charakteristika eines verbindungsorientierten Netzes in einem verbindungslosen Netz zu bieten.

Es ergibt sich nämlich die Problematik, daß die Sprachdaten im IP-Netz nicht von dem sonstigen Datenverkehr zu unterscheiden sind.
Telefoniedienste stellen folgende Anforderungen für eine ordnungsgemäße Sprachqualität:

Dauer des Verbindungsaufbaus: die Zeit, die von der Anforderung einer Verbindung bis zum Eintreffen der Bestätigung beim Benutzer des Transportdienstes benötigt wird (einige Zehntelsekunden).

Durchsatz: gibt an, wieviele Bytes bzw. Bits pro Sekunde übertragen werden können. Bei digitaler TK-Technik sind es pro B-Kanal 64 kbps.

Jitter: Abweichung der einzelnen Übertragungszeit vom Mittelwert aller Übertragungszeiten. Im Telefonbereich sollte die Abweichung vom Mittelwert nicht mehr als 20-30 ms betragen, da sonst Qualitätseinbußen bei den Sprachdaten auftreten (es ist unmöglich, länger als eine bestimmte Zeitspanne auf verspätet eintreffende Pakete zu warten, da sonst die bidirektionale Echtzeitkommunikation gestört wird; verspätete Pakete sind daher zu verwerfen). Somit gilt grundsätzlich: Je kleiner der Jitter, desto besser.

Übertragungsverzögerung: Die vom Sendemoment bis zum Empfang der Nachricht benötigte Zeitspanne. Hinsichtlich des Mediums ist dieses Kriterium (fast) egal, da auf jedem Medium die Daten immer mit einem hohen Prozentsatz der Lichtgeschwindigkeit übermittelt werden (etwa 70-80 % der Lichtgeschwindigkeit). Hinsichtlich der Vermittlungskomponenten spielt die Übertragungsverzögerung aber eine große Rolle, da mit zunehmender Zahl dieser Komponenten die Übertragungsverzögerung zunimmt (dieser Effekt basiert darauf, dass die Vermittlungskomponenten eine gewisse Verarbeitungszeit benötigen). Außerdem ist zu berücksichtigen, mit welchem zugrunde liegenden Algorithmus die Vermittlung erfolgt.

Diese Anforderungen stellen für ein verbindungsloses Netz, wie es die Internettechnologie darstellt, eine große Herausforderung dar, da sie nach dem Best-Effort-Prinzip arbeitet, d.h. alle Datenpakete werden (ohne irgendeine Vorrangbehandlung durchführen zu können), in der Reihenfolge des Eingangs bearbeitet und weitergeleitet. Somit kann nicht garantiert werden, wann alle Nachrichten ihr Ziel erreichen. Dies ist natürlich hinsichtlich der beim Telefonverkehr (und sonstiger bidirektionaler Echtzeitkommunikation) immanenten Bedingung eines minimalen Jitters nicht tolerierbar.

Lösungsmöglichkeiten hierzu und derzeit verfügbare Standards werden in Kapitel 5.4 vorgestellt.

Neben der Erfüllung von Sprachqualität sind noch weitere Anforderungen an ein VoIP-System zu setzen:

4.1.2 Sicherheit

VoIP-Systeme sollten aus sicherheitsrelevanten Gesichtspunkten nicht angreifbar sein.
Die Hauptangriffspunkte bestehen in folgenden Aspekten ([HET04] und [SIE06]):

- herkömmliche Datennetze:
  - Denial-of-Service-Attacken
  - Sniffing, Hacking
  - Spoofing
  - Schadprogramme (Viren, Würmer, ...)
- zusätzlich bei Sprachnetzen (auch VoIP):
  - unbefugter Zugang zu den System
  - Gebührenbetrug
  - „Man-in-the-Middle-Attacken"

VoIP-Systeme sollten die Möglichkeit bieten, durch eingebaute Sicherheitsmechanismen und Aktivitäten in den Betriebsphasen (hier vor allem Planung), die genannten Sicherheitsgefährdungen auszuschließen bzw. die Möglichkeit der Nutzung deutlich zu reduzieren.
Lösungsansätze hierzu werden in den Kapiteln 6.5.1 und 6.5.6.4 vorgestellt.

4.1.3 Ausfallsicherheit und Verfügbarkeit

In der Telekommunikationsbranche besitzen Produkte üblicherweise eine Ausfallsicherheit sehr nahe an der 100%-Marke (meistens etwa 99,5%). Die etablierten TK-Systeme sind seit vielen Jahren ausgereift und in der täglichen Praxis sehr ausfallsicher.
Während Systemabstürze von PC´s eine beinahe alltägliche Erscheinung darstellen, sind Ausfälle von Telefonanlagen, lokalen und öffentlichen Telefonnetzen äußerst selten.
Ein VoIP-System stellt hierbei deutlich erhöhte Anforderungen, um die geforderte Ausfallsicherheit zu erhalten, da hier eine deutlich höhere Anzahl an Komponenten erforderlich ist:

- Zentralkomponenten: Gateways, Gatekeeper, Server, ...
- Netzinfrastruktur: Router, Switches, Bridges, ...
- VoIP-Endgeräte
- Anbindung an das PSTN

Für alle Komponenten sind somit zum einen die Stromversorgung und die sonstige Funktionsfähigkeit abzusichern.
Dies ist bei klassischer TK-Technik nicht in diesem Maß erforderlich, da dort nur die TK-Anlage als Zentralsystem sowie die Zugänge aus dem PSTN bzw. zu firmeninternen Systemverbünden abgesichert werden muss, was deutlich weniger Aufwand bedeutet, da hier keine so hohe Vielzahl an Komponenten (sowohl quantitätsmäßig als auch funktionell) vorhanden ist.

4.1.4 Dienste/Leistungsmerkmale

Die Nutzung von Leistungsmerkmalen ist bei VoIP nicht selbstverständlich, da hierbei entscheidend ist, welche standardisierten oder proprietären Dienste bzw. Leistungsmerkmale ein Hersteller in seine Produkte implementiert.
Standardmäßig sind dies nur die ISDN-Leistungsmerkmale (siehe 3.2.1), da zum einen die Anbindung an das PSTN auf ISDN basiert und der derzeit vorherrschende H.323-Standard Q.931 als Signalisierungsprotokoll verwendet.
Weitergehende Leistungsmerkmale lassen sich (vor allem übergreifend mit Systemen verschiedener Hersteller) nur realisieren, wenn die entsprechenden Q.SIG-Leistungsmerkmale implementiert sind. Auf eine möglichst weitreichende Implementierung der Q.SIG-Leistungsmerkmale (siehe 3.2.5.2) ist ein besonderes Augenmerk zu richten, da mit dem Vorhandensein dieser Leistungsmerkmale die Akzeptanz der Nutzer stehen oder fallen kann, weil den meisten Nutzern egal ist, welche Technik bzw. Infrastruktur verwendet wird; ihnen ist nur die gewohnte Funktionalität wichtig.

4.1.5 Netzwerk/Bauliche Anforderungen

An das Netzwerk werden spezifische Anforderungen beim Einsatz VoIP gestellt, wenn man das System ausfallsicher betreiben will: die Regelung der Stromversorgung der Endgeräte (siehe Kapitel 5.5).
Wie im genannten Kapitel genannt, kann die Stromversorgung der Endgeräte per Steckernetzteil geregelt werden, was immense Nachteile bringt.
Demgegenüber ist die zentrale Stromversorgung mittels Power-over-LAN (gem. dem Standard IEEE 802.3af) möglich, was die Stromversorgung über die Netzverkabelung darstellt.
Hier ergibt sich die Anforderung an das Medium auf der Strecke Switch-Telefon (Tertiärebene einer strukturierten Verkabelung). Zum Einsatz von IEEE 802.3af ist es erforderlich, daß das Medium im Tertiärbereich ein Kupferkabel ist (die Datenübertragung basiert hier auf Elektronen, die elektrische Ladung darstellen und damit die Übertragung von Strom ermöglichen), da über Glasfaserkabel kein Stromtransport realisiert werden kann (die Übertragung basiert bei LWL auf Licht, das aus Photonen besteht, die elektrisch nicht geladen sind und daher keinen Strom übertragen können).

4.1.6 Standardkonformität

Viele Hersteller von TK-Systemen und Netzwerkinfrastruktur versuchen, um den Kunden von eigenen Produkten abhängig zu machen, proprietäre Standards einzusetzen. Generell sollten aber in heterogenen Netzinfrastrukturen nur standardkonforme Normen und Protokolle (IEEE, IETF, ITU, ...) verwendet werden, um diese Abgängigkeit nicht entstehen zu lassen.
Durch die Verzahnung von Daten- und Sprachnetz ergibt sich verstärkt die Gefahr einer zu großen Abhängigkeit von einem Hersteller, da der Kunde dem Hersteller dann auf Gedeih und Verderb ausgeliefert ist.
Dies könnte z. B. entstehen, wenn sowohl das VoIP-System als auch die Netzwerkinfrastruktur von einem Hersteller stammen und dieser Hersteller zu einem großen Teil proprietäre Protokolle einsetzt, d.h. Komponenten anderer Hersteller können nicht mehr (oder nur mit großen Einschränkungen) eingesetzt werden. Dann könnten sich folgende Abhängigkeiten ergeben:

- Preisdiktat durch den Hersteller
- Gefahr der Verfügbarkeit von Ersatzbeschaffungen und Erweiterungen (z.B. im Konkursfall des Lieferanten).

In diesem Fall wäre die dauerhafte Funktionsfähigkeit des Datennetzes und der anderen Komponenten nicht gewährleistet.
Wie diese Ausführungen zeigen, hat die strategische Wahl der Lieferanten und deren Standardkonformität eine große Auswirkung auf den langfristigen Unternehmenserfolg.

4.1.7 Bedienbarkeit

Die Bedienung ist für Endanwender schon bei vielen herkömmlichen Telefon-Endgeräten zu kompliziert. Neue Funktionalitäten können dazu führen, daß mehr Funktionen die Bedienbarkeit und Akzeptanz negativ beeinflussen.
Die Menüführung und die Funktionmöglichkeiten von Endgeräten sollten daher für Normalanwender auf ein (aus Unternehmenssicht tolerierbares) Mindestmaß reduziert werden („Weniger ist mehr“).

4.2 Wirtschaftliche Anforderungen

Neben den Anforderung aus Kunden-/Anwendersicht existieren wirtschaftliche Anforderungen, die hauptsächlich für die Nutzer von Bedeutung sind, da der Einsatz von VoIP diese einen längeren Zeitraum bindet (einige Jahre).

4.2.1 Investitionsschutz

Investitionsschutz bedeutet, daß bei einem Umstieg auf VoIP vorhandene Komponenten (Endgeräte, Applikationen, ...) weiterhin verwendet werden können. Führt beispielsweise ein Kunde ein VoIP-System nur in einem Teilbereich seines Betriebsareals ein, ist er im Vorteil, wenn er z. B. vorhandene Endgeräte weiterhin nutzen kann und keine neue Hardware beschaffen muß.
Ein weiterer Aspekt betrifft die Zukunftssicherheit der eingesetzten Technologie. Eine langfristige Nutzbarkeit sollte durch Einsatz zukunftsweisender Standards gewährleistet sein. Moderne Hardware sollte die Möglichkeit von Softwareupdates bieten, damit neue Protokolle und Funktionen auch nachträglich in Geräten unterstützt werden können. Produktfamilien sollten langfristig am Markt verfügbar sein und Erweiterungs- bzw. Ersatzlieferungen für den angestrebten Einsatzzeitraum ermöglichen.

4.2.2 Kostenreduktion

Bei den Kosten sind sowohl die Anschaffungs- als auch die Betriebskosten zu betrachten, wobei die Wartungskosten zu den Betriebskosten zählen.

- **Anschaffungskosten**
  Die Anschaffungskosten für VoIP-Systeme (Endgeräte, Systemeinheiten, ...) liegen auf einem ähnlichen Preisniveau wie für konventionelle Telefoniesysteme. An dieser Stelle ergeben sich somit keine Einsparungen. Die Anschaffungskosten lassen sich nur senken, wenn auf Endgeräteseite verstärkt Software-Clients als Ersatz für Tischtelefone eingesetzt werden. Bei Neuinstallationen liegt das Einsparpotential in der entfallenden zusätzlichen Verkabelung, weil keine eigenständigen Telefonnetzwerke aufzubauen sind. Werden mehrere dezentrale TK-Anlagen durch ein zentrales VoIP-System ersetzt, lassen sich so ebenfalls Kosten sparen.

- **Betriebskosten**
  Als häufiges Argument für die Einführung von VoIP in Unternehmen wird die Senkung der Betriebskosten angeführt, weil kein separates Telefonnetzwerk mehr betrieben werden und gewartet werden muß. Das Datennetzwerk integriert die Telefoniedienste, wodurch eine Unified-Messaging-Architektur entsteht, bei der Sprach-/Datenübertragung, Fax, Anrufbeantworter (Voicemail), E-Mail und weitere Funktionen miteinander verschmelzen.
  Neben der Telefonie können auch weitere Dienste, die bisher mit eigener Verkabelung realisiert wurden, in einem digitalen Netzwerk integriert werden. Beispiele hierfür sind die Übertragung von Einbrüchen bzw. Alarmmeldungen in zentralen Alarmmeldesysteme.
  Trotz allem verursachen VoIP-fähige Komponenten ähnliche Kosten wie herkömmliche Telefonanlagen (detailliert wird hierauf in Kapitel 6 eingegangen, da das Ziel dieser Diplomarbeit darin besteht, ein tragfähiges sowie kostenminimales Managementkonzept zu entwickeln):

  - Administration TK-spezifischer Funktionen: sämtliche Grundkonfigurationen sind genauso wie bei herkömmlichen TK-Systemen weiterhin durchzuführen. Beispiele hierfür: Administration der Least-Cost-Routing-Tabellen (LCR), Berechtigungen und generelle Leistungsmerkmale für die Teilnehmer, ...

  - Netzwerkadministration: durch die Integration in das Datennetz mit den in 4.1.1 gestellten Anforderungen ist eine erhöhter Gesamtaufwand für die Netzadministration notwendig.

  - MAC-Szenarien (Move-and-Change): bei Umzügen und sonstigen Änderungen ergibt sich hingegen eine große Kostenersparnis, da im Gegensatz zu konventionellen TK-Systemen nicht erst eine nicht belegte Leitung zum Zielpunkt gesucht/gelegt werden muß, sondern das Datennetz benutzt wird. Außerdem können die Nutzer die Endgeräte ohne erneuten Konfigurationsaufwand mitnehmen, was ebenfalls zu einer Kostenersparnis erführt.

4.2.3 Zusammenfassung

Ein VoIP-System sollte unter der Voraussetzung ausgewählt werden, daß es genügend Zukunftssicherheit bietet und somit möglichst lange kompatibel zu anderen Systemen ist bzw. eine langfristige Erweiterbarkeit und Austauschbarkeit von Komponenten ermöglicht. Die in einem System integrierten technischen (herstellerunabhängigen) Standards und Protokolle sind maßgebliche Faktoren für die Zukunftssicherheit. Durch eine sorgfältige Auswahl sollte gewährleistet werden, daß VoIP-Systeme im Rahmen der heute üblichen Abschreibungsfristen von fünf bis zehn Jahren eingesetzt werden können. In diesem Zeitraum müssen die Systeme erweitert, aktualisiert und Einzelteile bei Defekten ersetzt werden können.

Im nächsten Kapitel werden die verschiedenen Lösungen der Hersteller von TK-/VoIP-Systemen vorgestellt.

Kapitel 5

State-of-the-Art von VoIP-Systemen

In den vorangegangenen Kapiteln wurden Grundlagen von klassischer TK-Technik und VoIP dargelegt sowie ein Anforderungskatalog für den Einsatz von VoIP-Systemen erstellt. Dieses Kapitel beschreibt den derzeitigen Stand der von den (großen) Herstellern von VoIP-Systemen angebotenen Lösungen und Architekturen abstrakt, indem sie in zwei Gruppen eingeteilt und diese miteinander verglichen werden.
In einem weiteren Abschnitt werden die gebräuchlichsten Einsatzszenarien für VoIP-Systeme in vernetzten/verteilten Systemen, also z.B. Unternehmensnetzwerken (siehe Kapitel 3.2.6.2) dargestellt.
Im nächsten Abschnitt dieses Kapitels werden Lösungansätze für die Realsierung einer guten Sprachqualität (siehe 4.1.1) dargestellt.
Zuletzt erfolgt die Vorstellung mehrer Möglichkeiten zur Stromversorgung der Endgeräte, die bei einem VoIP-System (im Gegensatz zu klassischer Technik) nicht zentral vom VoIP-System mit Strom versorgt werden können.

5.1 Grundlegende Unterscheidung

Bei den angebotenen Systemen der Hersteller lässt sich grundsätzlich eine Unterscheidung in zwei Gruppen vornehmen:

- Hybridsysteme (LAN-PBX-Systeme)
- Soft-PBX-Systeme.

Diese beiden werden im folgenden vorgestellt.

5.1.1 Hybridsysteme

Leitungsvermittelte TK-Anlagen sind in den meisten Fällen modular aufgebaut. Hierbei werden die herkömmlichen Telefonschnittstellen durch Gatewayschnittstellen zum lokalen Datennetz ersetzt bzw. erweitert.
Telefonanlagen mit LAN-Schnittstellen werden im allgemeinen Sprachgebrauch als LAN-PBX bezeichnet. Eine Beispielkonfiguration zeigt Abbildung 5.1.
Die Gatewayschnittstellen zum LAN sind meist als Einsteckkarten konzipiert. Durch diese Schnittstellen können die TK-Systeme – je nach Ausbauoption des Herstellers – modular erweitert werden. Die Einbindung in lokale Datennetze erfolgt durch den Anschluß der Ethernet-Schnittstellen der Gateways an einen lokalen Switch. Modulare LAN-PBX-Anlagen ermöglichen den gemischten Betrieb von leitungsvermittelten Telefonen und IP-Endgeräten. Sie werden daher vor allem in Szenarien eingesetzt, bei denen nur ein Teil der Netzwerkinfrastruktur mit VoIP ausgestattet werden kann bzw. eine schrittweise

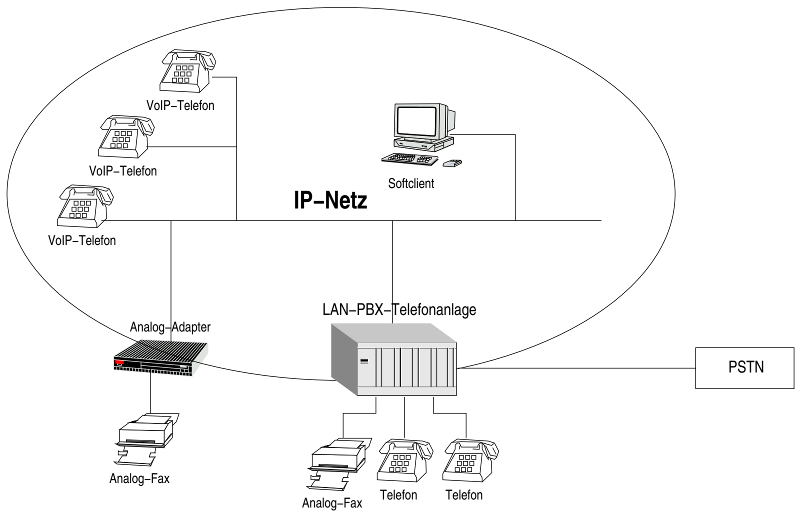

Abbildung 5.1: LAN-PBX-Konfigurationsbeispiel

Migration mit Erweiterungskomponenten eines Herstellers stattfindet. Mit diesen Systemen können auch reine VoIP-Systeme realisiert werden.

IP-Telefone für LAN-PBX-Anlagen sind meist herstellerabhängig implementierte IP-Systemtelefone, bei denen die proprietären Leistungsmerkmale der TK-Anlage unterstützt werden. Aus Sicht der PBX-Anlagenadministration lassen sich diese Endgeräte wie herkömmliche Systemtelefone konfigurieren und verwalten, was dazu führt, daß die Anwender keinen Unterschied bei der Bedienung von IP-Systemtelefonen und klassischen Systemtelefonen bemerken. Einzig sichtbares Unterscheidungsmerkmal ist die Netzwerkschnittstelle.
Daneben sind auch Software-Telefone (Softclients) verfügbar, die als Installation auf den Arbeitsplatzrechnern zum Einsatz kommen können.
Die derzeit am Markt befindlichen Systeme verwenden als grundsätzlichen Standard derzeit H.323 (siehe 3.3.1.2), wobei ein Einsatz von SIP (siehe 3.3.2) prinzipiell möglich wäre (durch Einspielen einer anderen Softwareversion auf die IP-Telefone sowie die Gatewayschnittstellen).

Anbieter dieser Hybridsystem sind die Hersteller von klassischen TK-Systemen, deren Kunden eine Vielzahl an Systemen mit klassischer Technik im Einsatz haben und somit eine Migration zu VoIP nur schrittweise vollziehen (können).
Dies sind z.B. Siemens, Alcatel (Nextira One), Tenovis (Bosch).

5.1.2 Soft-PBX-Systeme

Bei einer Soft-PBX werden die Funktionen der lokalen TK-Anlage von einer Telefonanlagensoftware übernommen, die bei vielen Herstellern als Anwendung auf einem Rechner installiert ist.
Der Einsatz einer Soft-PBX lohnt sich vor allem dann, wenn die bestehende IT/TK-Infrastruktur vollständig erneuert werden soll, oder bei komplett neuen Installationen, wenn auf keine vorhandene IT/TK-Installation Rücksicht genommen werden muß. Die klassische Telefonieumgebung wird dabei vollkommen ersetzt. Die Soft-PBX – auch als Call-Server bezeichnet – ist auf einem Rechner installiert und verfügt über eine Ethernet-Schnittstelle, die mit dem lokalen Datennetz verbunden wird. Die IP-Telefone sind als Hardwaregeräte an das Datennetz angeschlossen, wobei auch hier Softclients zum Einsatz kommen können. Externe Gateways im Netzwerk ermöglichen den Übergang vom lokalen Datennetz zu anderen Sprachnetzen. Abbildung 5.2 zeigt ein Konfigurationsbeispiel für ein Soft-PBX-System.

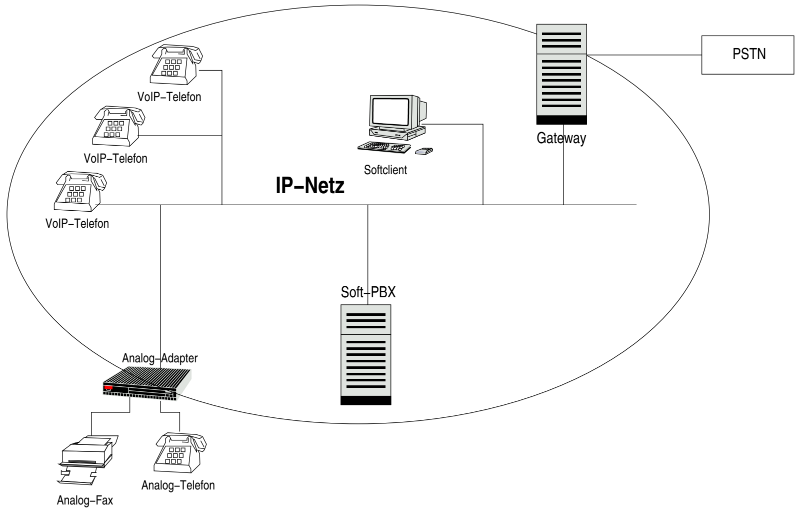

Abbildung 5.2: Soft-PBX-Konfigurationsbeispiel

Neben den IP-Endgeräten zur Sprachübertragung werden aber in den meisten Fällen weiterhin konventionelle Schnittstellen (analog, S_0, S_{2M}) z.B. für den Betrieb von Faxgeräten oder die Realisierung von Einwahlmöglichkeiten in das Datennetz von Heimarbeitern benötigt.
Hierfür gibt es derzeit nur eine Lösung für analoge Schnittstellen: Terminal-Adapter. Diese Adapter sind spezielle Schnittstellenadapter mit analoger a/b- und Ethernet-Schnittstelle.
Für die ISDN-basierten Schnittstellen ist eine Lösungsmöglichkeit eigentlich unmöglich (siehe die in 4.1.1 genannten Problemfelder), da bei diesen das Soft-PBX-System die anbieterseitige (netzseitige) Anbindung emulieren muß, was bedeutet, daß sich kein Frameausfall bzw. keine Reihenfolgevertauschung ereignen darf (siehe 3.2.4), da die daran angeschlossenen ISDN-Systeme sich sonst immer wieder synchronisieren müssten; jeder Synchronisationvorgang impliziert aber den Verlust einiger Frames. Wenn dies oft vorkommt, gehen viele Frames verloren, sodaß die Übertragungsqualität zum ISDN-Endgerät nicht mehr annehmbar ist.

Hersteller von Soft-PBX-Systemen sind Anbieter von Netztechnologie, die sich erst in den letzten Jahren mit der Übertragung von Sprachdiensten beschäftigt haben. Prominente Beispiele sind Cisco und 3Com.

5.2 Vergleich

In diesem Abschnitt werden die beiden grundsätzlichen Lösungsmöglichkeiten von VoIP-Systemen verglichen und bewertet. Hierbei erfolgt ein Vergleich hinsichtlich den Kriterien des Anforderungskatalogs (siehe Kapitel 4) sowie dem zusätzlichen Gesichtspunkt architektureller Aufbau.

5.2.1 Vergleich in architektureller Hinsicht

Wenn man die beiden Architekturen (LAN-PBX-System und Soft-PBX-System) vergleicht, fällt auf, daß sie sich nur hinsichtlich des Orts des Zentralsystems des VoIP-Zentrums und dem Standort des Gateways in das PSTN unterscheiden:

- Beim LAN-PBX-System befindet sich das Gateway in das PSTN integriert im TK-System, beim Soft-PBX-System ist das Gateway auf einer separaten Plattform untergebracht. Von der Funktionalität und dem Aufbau ergibt sich aber hier kein Unterschied, da prinzipiell egal ist, wieviele Rechner eingesetzt werden, um grundlegende Funktionalitäten darzustellen.

- Beim LAN-PBX sind die zentralen VoIP-Komponenten, die von H.323 bzw. SIP benötigt werden (siehe 3.3.1.2 und 3.3.2), innerhalb einer konventionellen TK-Anlage untergebracht (über Betriebssystemerweiterungen des TK-Systems sowie zusätzliche Einschubkarten mit LAN-Anschluß realisiert), bei der Lösung über ein Soft-PBX-System sind diese auf einem Rechner installiert.
  Hinsichtlich des architekturellen Aufbaus besteht aber kein prinzipieller Unterschied, da eine digitale konventionelle TK-Anlage – als Black Box gesehen – auch nur einen Rechner darstellt, der zusätzlich über eine/mehrere „LAN"-Karten verfügt.

Somit sind beide Systeme unter architekturellen Gesichtspunkten als gleichwertig anzusehen.

5.2.2 Vergleich in funktionaler Hinsicht

In funktionaler Hinsicht ergibt sich bei beiden Systemen aber ein bedeutender Unterschied: Wie in 5.1.2 erläutert, ist es bei Soft-PBX-Systemen unmöglich, ISDN-spezifische Dienste (S_0 bzw. S_{2M}) anzubieten. Damit scheidet die Realisierung von Sprach-, Daten- und Faxdiensten, die ISDN benötigen, prinzipiell aus. Außerdem ist es unmöglich, für spezielle Anschlüsse eine garantierte Verbindung bzw. Verbindungsqualität herzustellen (siehe Erläuterungen in 4.1.1), die derzeit nur mit konventioneller TK-Technologie geboten werden – man denke an Einsatzgebiete für hochverfügbare Telefonanschlüsse wie in Rettungsleitstellen, Flughafentowers und sonstigen sicherheitskritischen Bereichen.
Hier ist ein LAN-PBX-System konzeptionell überlegen, da mit ihm weiterhin klassische TK-Technik realisiert werden kann. Hinsichtlich der im Anforderungskatalog (siehe Kapitel 4) genannten Punkte wie Quality-of-Service, Bedienbarkeit, Ausfallsicherheit des Gesamtsystems, Dienste/Leistungsmerkmale und den wirtschaftlichen Anforderungen) ergeben sich zwischen beiden Systemen keine Unterschiede.

5.2.3 Zusammenfassung

Zusammenfassend kann festgestellt werden, daß die beiden Lösungsmöglichkeiten LAN-PBX-System und Soft-PBX-System architekturell gleichwertig sind. Hinsichtlich funktionaler Aspekte ist das LAN-PBX-System im Vorteil (es stellt sich nur die Frage, wie dieser Punkt vom Nutzer gewichtet wird).

Alles in allem sind beide Systeme als gleichwertig anzusehen. Für die Entwicklung eines Managementkonzepts, die im nächsten Kapitel erfolgt, ergeben sich keine Unterschiede, sodaß das Managementkonzept gleichermaßen für beide Systeme Anwendung finden kann.

5.3 Einsatzszenarien für VoIP-Systeme in Verbundnetzen

Bei verteilten Netzen (z. B. in Unternehmensnetzwerken) sind prinzipiell drei Lösungsansätze möglich (wobei Anrufmanagement als VoIP-System zu verstehen ist, da – wie bereits gezeigt – kein großer Unterschied zwischen einer Soft-PBX- und einer LAN-PBX-Variante besteht):

- mehrere Standorte mit unabhängigen Telefonsystemen
- mehrere Standorte mit jeweils eigenem Anrufmanagement
- mehrere Standorte mit einem zentralen Anrufmanagement.

Diese Varianten werden nun beschrieben sowie ihre spezifischen Vor- und Nachteile erläutert.

5.3.1 Mehrere Standorte mit unabhängigen Telefonsystemen

Bei diesem Modell sind die Kommunikationsstrukturen mehrfach aufgebaut, jeder Standort verfügt über sein eigenes Anrufmanagement bzw. Telefonsystem. Die Kommunikation über die Standortgrenzen erfolgt über das leitungsvermittelte Festnetz, IP-Telefonie bleibt also eine reine Inhouse-Veranstaltung. In diesem Fall geht es nicht um das Einsparen von Telefonkosten, sondern um die Vereinheitlichung der Infrastruktur und die Konzentration der Administration in der IT-Abteilung. Abbildung 5.3 illustriert dieses Szenario.

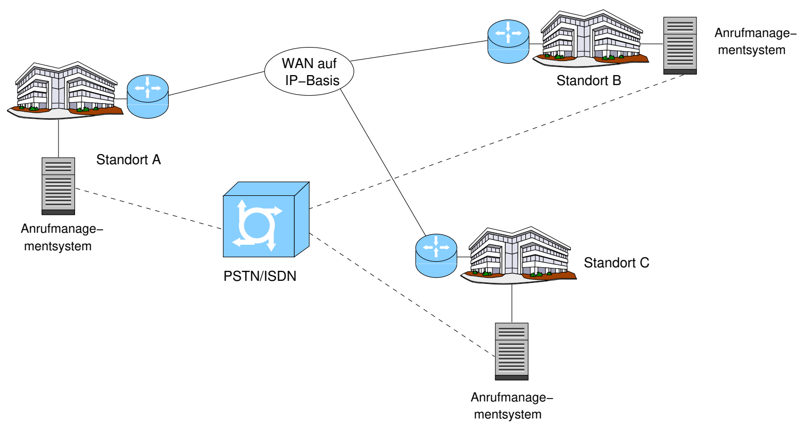

Abbildung 5.3: Mehrere Standorte mit jeweils separatem Anrufmanagementsystem und Inhouse-VoIP-Nutzung

5.3.2 Mehrere Standorte mit jeweils eigenem Anrufmanagement

Technisch interessanter sind die beiden nächsten Konstellationen.
Bei mehreren Standorten mit dezentralem Anrufmanagement wird neben einem VoIP-System pro Standort ein übergeordneter Gatekeeper zur zentralen Zugangskontrolle und Rufnummernadressauflösung benötigt. Dieser sorgt auch für die Verbindung der Einzelnetzwerke über das IP-Netz (siehe Abbildung 5.4).
Zur Sicherheit sollte man parallel eine PSTN-Verbindung vorsehen, um beim Ausfall der Internet-

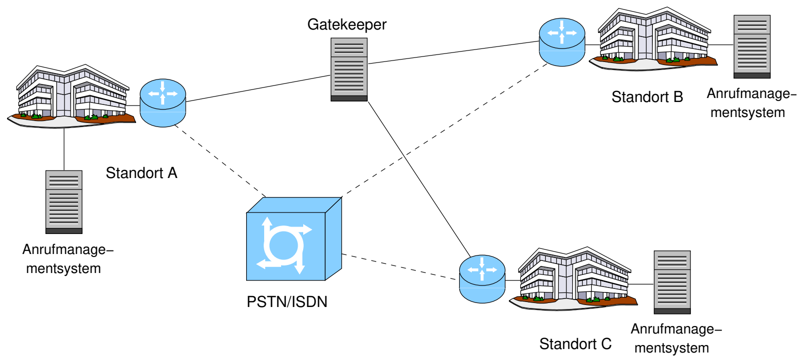

Abbildung 5.4: Mehrere Standorte mit jeweils eigenem Anrufmanagement

Verbindung nicht den kompletten Sprachverkehr stillzulegen. Ein zweiter Grund für die sekundäre PSTN-Verbindung ist zeitweise fehlende WAN-Bandbreite. Der Gatekeeper entscheidet dann auf Basis der Anzahl und Art der vorhandenen Verbindungen, ob er eine zusätzliche Verbindung über das WAN zulässt oder die PSTN-Leitung zum Einsatz kommt. Aus Gründen der Kostendisziplin sollte das den Gesprächsteilnehmern signalisiert werden.

Laut [CIS01] lassen sich so bis zu 100 Standorte miteinander verbinden, wobei für die Sprachübertragung rund 80 kBit/s Bandbreite pro Verbindung zur Verfügung stehen sollten.

5.3.3 Mehrere Standorte mit einem zentralen Anrufmanagement

Im dritten Szenario, mit zentralem Anrufmanagement, sieht die Situation ein wenig anders aus.
In diesem Falle läuft an einem Standort, naheliegender Weise der Firmenzentrale, ein zentrales VoIP-System für alle IP-Telefone an allen Standorten. Durch eine solche Architektur ist ein zentrales Anrufmanagement gewährleistet, die Anzahl von Teilnehmern jedoch limitiert. Die Grenzen setzt die jeweilige Soft- und Hardware, [CIS01] spricht beispielsweise von 2500 Teilnehmern an theoretisch beliebig vielen Standorten. Die Teilnehmeranzahl variiert hierbei je nach Architektur des Herstellers des VoIP-Systems. Preisgünstiger, aber mit Single-Point-of-Failure: Alle Standorte nutzen einen gemeinsamen

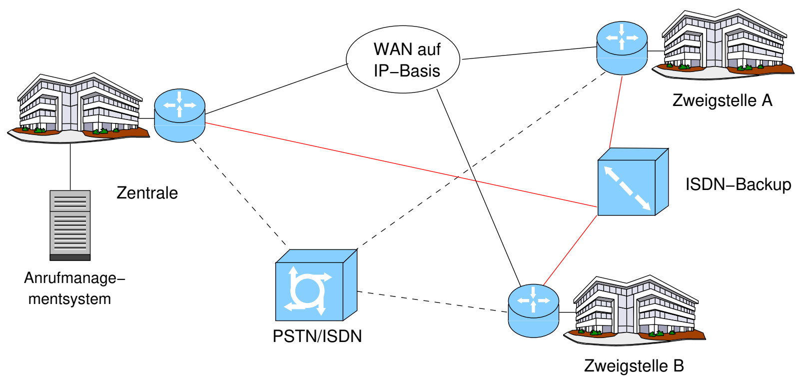

Abbildung 5.5: Mehrere Standorte mit zentralem Anrufmanagement

Anrufmanager (Abbildung 5.5), was bei einem Ausfall die komplette Sprachkommunikation im Unternehmen lahmlegt.
Vorteil dieses Modells ist, daß weniger Hardware erforderlich ist. Hier sollte, aufgrund der besonderen Abhängigkeit von einem zentralen Standort, neben der PSTN-Verbindung zum Abfangen von Überlast zusätzlich eine Backup-Leitung installiert werden, über die im Notfall noch die Verbindung zum Anrufmanagementsystem gewährleistet ist, da nur so für die Filialstandorte eine Kommunikationsmöglichkeit besteht.

Wenn man die drei Lösungsansätze vergleicht, ergeben sich jeweils spezifische Vor- und Nachteile. Alle drei Varianten sind aber prinzipiell realisierbar; welche eingesetzt wird, hängt zum einen von der Struktur und Größe des Unternehmens (räumlich gesehen) und zum anderen von der betriebswirtschaftlichen (finanziellen) Betrachtung ab.
Auch aus Managementgesichtspunkten haben alle drei Szenarien ihre Vor- und Nachteile, wobei keines zu bevorzugen ist.

5.4 Sprachqualität

Wie bereits in Kapitel 4.1.1 aufgezeigt, ist eine angemessene Sprachqualität Dreh- und Angelpunkt für die Akzeptanz eines VoIP-Systems für die Anwender, da sie eine gute bzw. hervorragende Qualität von der klassischen Telefonietechnik gewohnt sind.
Diese Anforderungen erzwingen es, weiter auszuholen und den prinzipiellen Aufbau einer Quality-of-Service-Architektur zu erläutern – basierend auf [DIKO02], das der interessierte Leser auch zur Vertiefung verwenden kann.

5.4.1 Quality-of-Service-Architektur

Grundlage einer Quality-of-Service-Architektur ist das sog. „Flowkonzept“.
Bei IP gibt es nur Datenpakete, die (wie bereits gesagt) nach dem „best-effort“-Prinzip durch das Netz geleitet werden, d. h. der Zustand des Netzes ist verbindungslos. Zur Bereitstellung von QoS ist es aber notwendig, zusammengehörende Pakete (die z.B. einen Medienstrom ein VoIP-Telefonat darstellen) – durch eine entsprechende Kennzeichnung (sog. „marking“) – zu bündeln (um dadurch die Pakete einer bestimmten Instanz eines Dienstes eindeutig zuordnen zu können, was eine schnelle Identifikation ermöglicht und so die Einhaltung der notwendigen Parameter erleichtert). Dies geschieht durch einen Identifikator. Die Gesamtheit aller durch denselben Bezeichner gekennzeichneten Pakete nennt man „Fluß“ bzw. „flow“. Durch die Einführung solcher Flüsse ist es nun bedeutend leichter, den geforderten QoS zu liefern, da in jeder Komponente nur gespeichert werden muß, welche Anforderungen für den jeweiligen Fluß gelten.
Das Flowkonzept stellt also in der Internetwelt eine vollkommen neue Sichtweise dar (es versucht, ein verbindungsorientiertes Netz zu emulieren), während sie bei ATM (siehe [TAN00]) ein Grundbestandteil ist.
Basierend auf dem Flowkonzept und weiteren Leitlinien, die u.a. die Punkte

- Aufstellung von Metriken und Messungen
- Klassifikation und Abschätzung des Nutzerverhaltens
- Bereitstellung von QoS
- Management Policy
- Differenzierungsmöglichkeiten / Cost of Service

umfassen, ist eine Quality-of-Service-Architektur, wie in Abbildung 5.6 gezeigt, aufgebaut.
Erläuterungen zur Abbildung:

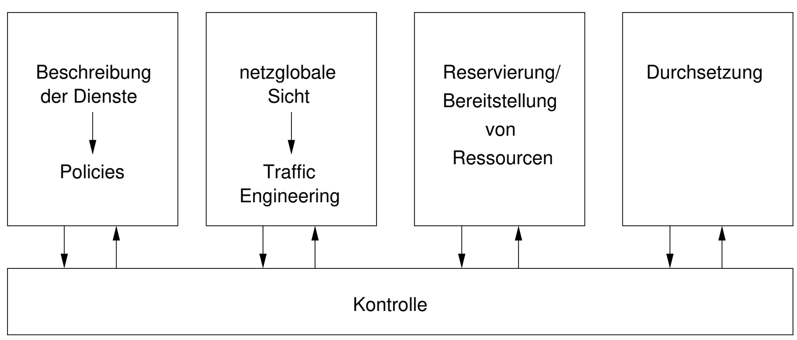

Abbildung 5.6: Aufbau einer QoS-Architektur

- **Beschreibung der Dienste**:
  Aus Verkehrsmessungen erhält man ein ungefähres Lastverhalten der im Netz genutzten Dienste (aufgeteilt auf die einzelnen Dienstklassen). Dieses Lastprofil muss alle mit den Nutzern abgeschlossenen SLA’s erfüllen, da sonst Vertragsstrafen drohen können. Um diese zu vermeiden, ist es notwendig, für jede Dienstklasse (und damit implizit für alle Dienste) Richtlinien über die Bearbeitung im Netz zu erstellen. Diese Richtlinien nennt man „Policies“.
- **Traffic Engineering**: Ausgehend von den Policies und dem Lastverhalten, sowie den bisherigen netzspezifischen Gegebenheiten ist es erforderlich, die Netzperformance bzw. -durchsatz zu optimieren. Dies kann z.B. durch Nutzung zusätzlicher Leitungsverbindungen sowie zusätzlicher oder leistungsfähigerer Netzkomponenten geschehen.
  Ein weiterer Teilbereich des Traffic Engeneering besteht darin, die Datenströme aus netzglobaler Sicht einzuteilen und globale Regeln für Problemstellungen wie z.B. Klassifizierung, Scheduling, ... zu entwerfen.

- **Bereitstellung von Ressourcen**: Die Bereitstellung von Ressourcen ist ein sehr wichtiger Bestandteil. Hierbei ist der Vorgang des Reservierens bzw. allgemeiner dem Schaffen von Nutzungsmöglichkeit der Ressource gemeint. Wenn in der QoS-Architektur eine Anforderung zur Herstellung einer Verbindung von A nach B für eine bestimmte Dienstklasse entsteht, müssen alle Komponenten auf dem Pfad von A nach B (der auch noch zu bestimmen ist) für diese Anforderung exklusiv Ressourcen bereitstellen. Außerdem ist hierbei zu entscheiden, wo und wie die Datenpakete gekennzeichnet werden. Dies kann entweder intern oder beim Kunden (extern) geschehen. Den Vorgang der Kennzeichnung nennt man „Marking“.
  Für diesen Architekturbestandteil werden folgende Mechanismen benötigt:
  - QoS Mapping: QoS Mapping erfüllt die Übersetzung zwischen den Ausprägungen von QoS auf verschiedenen Ebenen (z.B. Betriebssystem, Transportschicht, Netz). Dies bedeutet, dass die verschiedenen QoS-Kriterien auf die einzelnen Ebenen umgelegt werden. (Das Betriebssystem hat andere Schwachstellen als das Netz.)
  - Admission Testing: Admission Testing ist dafür verantwortlich, dass überprüft wird, ob die verfügbaren Ressourcen eine neue Anfrage qualitätsmäßig bedienen können. Dies geschieht sowohl unter Beachtung der netzweiten Policies als auch der Verfügbarkeit der Ressourcen.
    Ein mögliches Verfahren wäre:
    - Überprüfung, ob eine Anforderung in jeder einzelnen Ressource erfüllt werden kann.
    - Wenn diese Prüfung in einer Ressource erfolgreich war, wird die Ressource insoweit gesperrt (also ähnlich einer Semaphore).
    - Bei erfolgreicher Ende-zu-Ende-Verbindung wird die gesamte Verbindung endgültig reserviert (ähnlich dem „commit“-Befehl bei Datenbanken).
- **Resource Reservation**: Resource Reservation hängt eng mit Admission Testing zusammen: Ressource Reservation Protokolle dienen zur Errichtung einer vom Nutzer gewünschten Verbindung in Abstimmung mit den verfügbaren Ressourcen. Zuerst wird mittels eines Routing-Verfahrens ein Pfad zum Ziel ermittelt, danach erfolgt in jeder Ressource QoS-Mapping und Admission Control, sodaß schließlich die Verbindung aufgebaut ist.
- **Kontrolle**: Im laufenden Betrieb ist zur Überwachung aller Komponenten und Verkehrsströme der gesamte Zustand aller Bestandteile zu übermitteln und zu protokollieren. Kontrolle bzw. Maintenance ist der wichtigste Bestandteil der Architektur, da nur bei Kenntnis aller managementrelevanten Daten der ordnungsgemässe Betrieb aufrechterhalten werden kann. Somit ergibt sich vom Kontrollblock eine ständige Interaktion mit allen Komponenten, um diese ggf. anzupassen. Details (insbesondere die Konzeption von Managementarchitekturen) sind [HAN99] zu entnehmen.
  Hierfür werden die Mechanismen QoS Monitoring, QoS Maintenance, QoS Degradation, QoS Signalling und QoS Scaling benötigt, die hier nicht weiter erläutert werden.
- **Durchsetzung**: Um einen den Policies entsprechenden Betrieb zu gewährleisten, ist es erforderlich, die im Rahmen des Kontroll- bzw. Überwachungsblocks gewonnen Daten zur Überprüfung zu verwenden, inwieweit die einzelnen Komponenten bzw. Flows im Rahmen der erstellten Regeln arbeiten. Bei Verstößen sind geeignete Maßnahmen einzuleiten (z.B. Durchsatzbeschränkungen, Umleitungen über andere Pfade, wenn möglich).

Analog dazu ist auch eine prozeßorientierte Sichtweise auf eine QoS-Architektur möglich (siehe 5.7). Zu diesem Aufbau werden kurz einige Erläuterungen gegeben (Details sind in [DIKO02] zu finden). Diese QoS-Architektur besteht aus einem theoretischen und einem abstrakten Teil, sowie einer Systemkomponente (siehe Abbildung 5.7).

- **Abstrakte Komponenten**: Mit dem Nutzer wird ein Service Level Agreement (SLA) abgeschlossen. Das bedeutet, dass ihm bestimmte Garantien wie z.B. Durchsatz 2 Mbit/s, Jitter < 10 ms, u.a. gegeben werden und diese dann auch eingehalten werden müssen. Wie in den Beispielen schon genannt, werden dabei bekannte Metriken verwendet bzw. neue definiert (z.B. korrekte Farbtiefe).

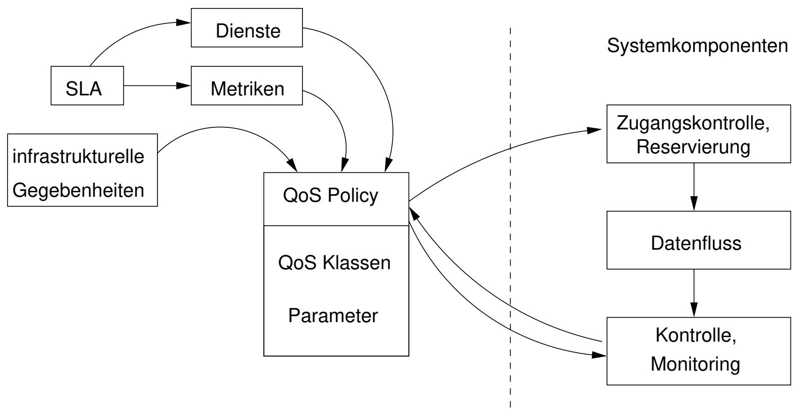

Abbildung 5.7: Prozeßorientierter Aufbau einer QoS-Architektur

In Verknüpfung mit den Netzgegebenheiten (wie z.B. Leitungsdurchsätze, Routerzahl und -durchsatz, ...) entsteht aus diesen beiden Komponenten eine QoS Policy. Diese Policy beinhaltet zum einen QoS-Klassen und Parameter, die für die Ressourcenzuteilung verwendet werden, als auch Richtlinien,

  - was bei Verletzung der Grenzwerte geschehen muss,
  - welche Abrechnungstarife gelten und wie die Abrechnung zu erfolgen hat.

- **Systemkomponenten**: Das System hat folgende Komponenten:
  - Zugangskontrolle, Reservierung
  - Datenfluss
  - Wartung, Kontrolle, Monitoring

  Wie man der Abbildung entnehmen kann, hängen die beiden Teile sehr eng zusammen. Beide Komponenten geben sich jeweils gegenseitig Rückmeldung und bauen aufeinander auf.
  So wird die QoS-Policy für die Zugangskontrolle bzw. Reservierungsstrategie verwendet.
  Vom Wartungs- und Kontrollblock fließen Daten zurück, die wieder für die Änderung der QoS-Policy verwendet werden können. Ein Beispiel hierfür wäre:
  Im Netz sind ein paar Verbindungen ausgefallen. Dadurch können die im SLA vereinbarten Parameter nicht mehr eingehalten werden bzw. die Policy muss hinsichtlich der Ressourcenzuteilungsstrategie geändert werden, um die geforderten Kriterien garantieren zu können. So ergibt sich ein Rückkopplungseffekt, der versucht, die SLA's so gut wie möglich zu erfüllen.

Zusammenfassung Dieser Abschnitt hat den grundlegenden Aufbau einer QoS-Architektur aufgezeigt. Eine QoS-Architektur besteht aus den großen Blöcken

- Beschreibung der Dienste
- Traffic Engineering
- Bereitstellung von Ressourcen
- Kontrolle
- Durchsetzung

In den beiden nächsten Abschnitten werden – für die IP-Welt – zwei verschiedene Ansätze zur (partiellen) Realisierung einer QoS-Architektur vorgestellt, von denen mindestens einer zur Realisierung einer guten Sprachqualität implementiert sein sollte.

5.4.2 Integrated Services

Der Begriff Integrated-Services (IntServ) bezieht sich auf die von der *IETF (Internet Engineering Task Force)* in den Jahren 1995 bis 1997 erstellten Arbeiten der gleichnamigen Arbeitsgruppe und sind in [RFC1633], [RFC2205] und [RFC3272] prinzipiell dargestellt. Die Integrated-Services-Arbeitsgruppe entwickelte Spezifikationen für verschiedene Dienstklassen. Daneben definierte sie auch, wie das Reservierungsprotokoll *RSVP* benutzt werden kann, um bei Integrated-Services die gezielte Reservierung von Ressourcen durchzuführen.
Die folgenden Absätze liefern einen Überblick über die von der IETF entwickelten Spezifikationen und von den Mechanismen, mit denen sie implementiert werden.

Der strukturelle Aufbau dieses Kapitels lehnt sich im weiteren Verlauf an den in Abschnitt 5.4.1 dargestellten Aufbau einer QoS-Architektur.

- **Dienstklassen bei Integrated-Services** Bei Integrated-Services gibt es – neben der Standarddienstklasse *Best Effort* – im Grunde genommen zwei Hauptdienstklassen: *Guaranteed-Service (GS)* und *Controlled-Load-Service (CLS)*.

  1. *Guaranteed-Service* wurde für **intolerante Anwendungen** ausgelegt. Bei dieser Art von Anwendungen darf ein Paket nie zu spät ankommen. Das Netz muss stets garantieren, dass die maximale Verzögerung, der ein Paket ausgesetzt ist, einen spezifizierten Wert hat. Dieser im vornherein festgelegte Wert ist somit eine obere Schranke für die (möglicherweise) auftretenden Paketverzögerungen. Dadurch kann z.B. eine Audioanwendung ihren Wiedergabepunkt immer so setzen, dass kein Paket zu spät ankommt und die abgespielte Tonsequenz somit fehlerfrei und in guter Qualität abgespielt werden kann. Zu früh eintreffende Pakete werden (bis zu dem Moment an dem sie benötigt werden) in einem Zwischenspeicher abgelegt.

  2. Zusätzlich zum Guaranteed-Service zog die IETF mehrere weitere Dienste in Betracht, entschied sich aber schließlich für die Entwicklung einer Dienstklasse namens *Controlled-Load*, die die Anforderungen **toleranter, adaptiver Anwendungen** erfüllt. Anwendungen dieser Art zeichnen sich einerseits durch ihre Toleranz gegenüber Datenverlust, andererseits duch ihre Anpassungsfähigkeit aus. Sie laufen daher recht gut in nur leicht belasteten Netzen. Manche Audioanwendungen berichtigen beispielsweise ihren Wiedergabepunkt entsprechend den Schwankungen der Netzverzögerung und produzieren eine angemessene Audiogüte, solange die Verlustraten in der Größenordnung von 10% oder darunter liegen.

  Für den Dienst VoIP ist somit Guaranteed-Service die relevante Dienstklasse.
  Selbstverständlich sind diese beiden Dienstklassen lediglich eine Untermenge aller Klassen, die bereitgestellt werden können. Es bleibt im Zuge des praktischen Einsatzes von Integrated-Services abzuwarten, ob sich die Anforderungen aller oben beschriebenen Anwendungsarten mit diesen beiden Dienstklassen erfüllen lassen.

- **Traffic Engineering bei Integrated-Services**

  – Flussspezifikation: Das *Flowkonzept* (siehe Abschnitt 5.4.1) von Integrated-Services realisiert bei IP das Aufbrechen der Verbindungslosigkeit (während IP verbindungslos ist, wird bei Integrated-Services „künstlich“ eine Verbindungsorientiertheit aufgezwungen).
  Die *FlowSpec (Flussspezifikation)* bei Integrated-Services besteht aus zwei separaten Teilen und realisiert das Traffic Engineering. Der eine Teil beschreibt die Verkehrsmerkmale des Datenflusses (*TSpec*), der andere Teil den vom Datenfluss angeforderten Dienst (*RSpec*).

  – Paketklassifizierung und -Scheduling: Damit bei Integrated-Services die Router den angeforderten Dienst für die Datenpakete bereitstellen können, müssen folgende Dinge durchgeführt werden:

    * Verknüpfung der Pakete mit der entsprechenden Reservierung, sodaß jedes Paket korrekt

behandelt werden kann. Diesen Prozess nennt man *Paketklassifizierung* bzw. allgemein *Marking*. Bei Integrated-Services wird das Marking der Pakete vom Sender übernommen.

  * Verwaltung der Pakete in den Warteschlangen, sodass sie stets den angeforderten Dienst erhalten. Diesen Prozess nennt man das *Packet-Scheduling* bzw. in der allgemeinen Architektur *Durchsetzung*.

  Die Verknüpfung der Pakete mit den entsprechenden Reservierungen erfolgt durch Überprüfung von bis zu fünf Feldern im Paket-Header: Quelladresse, Zieladresse, Protokollnummer, Quell-Port und Ziel-Port. Auf der Grundlage dieser Informationen können die Pakete in Klassen eingeordnet und (in Warteschlangen) verarbeitet werden .

- **Packet Dropping**
  Das kontrollierte Verwerfen von einzelnen Datenpaketen (zumeist *Packet Dropping* genannt) ist genauso wichtig wie das beschriebene *Packet-Scheduling*.
  Ein Router muss immer dann Pakete verwerfen, wenn alle ihm zugehörigen Warteschlangen voll bzw. stark überlastet sind. Dies legt jedoch noch nicht fest, *welche* Datenpakete verworfen werden sollen. Stets nur das *eintreffende* Paket zu verwerfen, kann zu „unerwünschten" Ergebnissen führen. Ob – bei einem Router, dessen Warteschlangen stark überlastet sind – immer das aktuell eintreffende Paket verworfen werden soll (damit die weiter eintreffenden Pakete ohne größere Verzögerung durch den Router geleitet werden können) oder ob jedes Paket im Netz nach seiner Priorität gewichtet werden soll und bei einer Überfüllungssituation zuerst immer die Pakete mit der geringsten Wichtigkeit verworfen werden sollen, hängt von den Anforderungen des jeweiligen Dienstes ab.

- **Zugangskontrolle**
  Die Zugangskontrolle bei Integrated-Services basiert auf folgendem Konzept. Wenn ein neuer Dienst (bzw. Flow) ein bestimmtes Maß an Dienstgüte erhalten möchte, überprüft die Zugangskontrolle die TSpec und RSpec des Datenflusses und ermittelt, ob der gewünschte Dienst für den Verkehrsumfang angesichts der momentan verfügbaren Ressourcen bereitgestellt werden kann, ohne die bereits anderen Datenflüssen zugestandenen Dienste zu beeinträchtigen. Kann der Dienst bereitgestellt werden, wird der Datenfluss zugelassen, andernfalls wird er abgewiesen. Schwierig daran ist die Entscheidung, wann das Netz „Ja" und wann es „Nein" sagen soll.

- **Das Reservierungsprotokoll RSVP**
  Bei Integrated-Services wird die Bereitstellung von Ressourcen durch eine Reservierung durchgeführt. Das Reservierungsprotokoll hierfür heisst *RSVP (Ressource Reservation Protocol)*.
  In Anlehnung an [RFC2205] wird die prinzipielle Funktionsweise erläutert.
  Während verbindungsorientierte Netze schon immer ein Setup-Protokoll hatten, um den nötigen Zustand virtueller Leitungen in den Switches aufzubauen, besitzen verbindungslose Netze wie das Internet keine solchen Protokolle.
  Die Entwickler der Integrated-Services-Arbeitsgruppe erkannten in den 90er Jahren den wachsenden Bedarf an Echtzeitanwendungen (zumeist multimedialer Art) im Internet. Wenn man nun aber dem Internet Echtzeitdienste abfordert, muss man ihm (wie aus diesem Abschnitt hervorgeht) genaue und strukturierte Informationen bereitstellen. In den letzten Jahren wurden verschiedene Setup-Protokolle für das Internet vorgeschlagen, von denen allerdings heute das oben erwähnte *RSVP-Protokoll* vorrangige Beachtung findet. Es ist besonders interessant, weil es sich erheblich von den konventionellen Signalisierungsprotokollen für verbindungsorientierte Netze unterscheidet.

  RSVP beruht u.a. auf der wichtigen Vorgabe, dass seine Anwendung die Robustheit der heutigen verbindungslosen Netze nicht beeinträchtigen sollte. Da verbindungslose Netze von keinen im Netz selbst gespeicherten Zuständen abhängen, können Router abstürzen und neu starten oder Leitungen auf- und abgebaut werden, während die Ende-zu-Ende-Verbindung weiterhin bestehen bleibt. RSVP versucht, diese Robustheit durch die Benutzung des *Soft-State-Konzeptes* in den Routern zu wahren. Im Gegensatz zum Hard-State wie bei verbindungsorientierten Netzen muss der

Soft-State nicht ausdrücklich gelöscht werden, wenn er nicht mehr benötigt wird. Statt dessen läuft er nach einer relativ kurzen Dauer (im Minutenbereich) ab, wenn er nicht periodisch aufgefrischt wird.
Ein weiteres wichtiges Merkmal von RSVP ist die Tatsache, dass es sowohl *Multicast-*, als auch *Unicast-Datenflüsse* unterstützt.
Die Entwickler von RSVP erkannten unter anderem, dass die meisten Multicast-Anwendungen viel mehr Empfänger als Sender haben, wie beispielsweise eine große Zuhörerschaft neben einem Sprecher bei einer Vorlesung. Außerdem können die Empfänger unterschiedliche Anforderungen stellen. Ein Empfänger möchte z.B. Daten von nur einem Sender empfangen, während ein anderer von allen Sendern gleichzeitig Daten empfangen möchte. Statt die Sender eine potentiell große Anzahl von Empfängern verwalten zu lassen, erscheint es sinnvoller, dass sich die Empfänger um ihre eigenen Bedürfnisse kümmern. Aus dieser Erkenntnis heraus entstand der in RSVP umgesetzte *empfängerorientierte Ansatz*. Demgegenüber überlassen verbindungsorientierte Netze normalerweise die Ressourcenreservierung dem Sender, so wie es bei einem Telefongespräch üblich ist, bei dem der wählende Teilnehmer die Zuteilung von Ressourcen im Telefonnetz veranlasst.
Die *Soft-State* und der *empfängerorientierte Ansatz* verleihen RSVP mehrere angenehme Eigenschaften. Beispielsweise ist es sehr einfach, den Umfang der Ressourcenzuteilung, der einem Empfänger bereitgestellt wird, zu erhöhen oder zu senken. Jeder Empfänger sendet in konstanten Abständen Auffrischungsnachrichten, um den Soft-State aufrechtzuerhalten. Daher ist es recht einfach, eine neue Reservierung zu senden, mit der neue Ressourcen angefordert werden. Sollte ein Host abstürzen, läuft natürlich der Timer für die Ressourcen, die diesem Host zugeteilt sind, ab und die Ressourcen werden freigegeben.
Unter anderem durch RSVP ist auch die Verbindungsorientiertheit von Integrated-Services erkennbar. Zuerst wird über den RSVP-Prozess die Verbindung und die genaue Route festgelegt, erst anschließend werden die Daten zwischen den jeweiligen Geräten ausgetauscht (wobei das Hauptaugenmerk auf die strikte Trennung von Management- und Datenverkehr zu legen ist).
Das RSVP-Protokoll ist nicht speziell für bzw. zusammen mit Integrated-Services entwickelt worden. Es ist ein eigenständiges Reservierungsprotokoll, das lediglich von der QoS-Architektur Integrated-Services für die Bereitstellung von Ressourcen verwendet wird.

- **Kontroll- und Durchsetzungsmöglichkeiten bei Integrated-Services**
  Außer den standardmäßigen Management-Protokollen sind bei Integrated-Services keine weiteren Kontroll- und Durchsetzungsmechanismen vorhanden.

- **Implementierungsbeispiel für VoIP**
  Wie in 3.3.1 und 3.3.2 erläutert, sind für VoIP

  - ein UDP-basierter Datenstrom für die Gesprächsdaten
  - ein TCP-basierter Datenstrom für die Signalisierungsdaten

  erforderlich. Daneben existieren noch weitere Datenströme der anderen Dienste, die der Einfachheit halber als „best-effort“-Datenstrom eingeordnet werden.
  Für die Implementierung von IntServ ergibt sich hieraus ein Implementierungsvorschlag:

  - jeder UDP-Datenstrom als „Guaranteed-Service“-Fluß mit Reservierung von etwa 80 kbps (bei Codierung mit G.711: 64 kbps + Overhead für Headerinformationen), da diese Daten ihr Ziel mit minimalem Jitter erreichen sollen.
  - jeder TCP-Datenstrom mit Signalisierungsdaten sowie die sonstigen „best-effort“-Datenströme als „Controlled-Load“-Flüsse, da hier die Paketlaufzeiten keine essentielle Rolle für die Diensterbringung (u.a. von VoIP) spielen.

  Somit ergibt dieser Vorschlag eine tragfähige Realisierungsmöglichkeit für IntServ in Netzen, die VoIP anbieten, da alle Anforderungen für VoIP erfüllt werden.

Zusammenfassend ist festzustellen, daß IntServ eine Möglichkeit zur Realisierung einer QoS-Architektur für VoIP darstellt, wobei die inhärente Schwäche einer Bandbreitenadaption für VoIP nicht kritisch ist, da die Bandbreite eines Telefonats (in Abhängigkeit vom verwendeten Kodierungsstandard) feststeht. Der Nachteil an IntServ besteht in der großen Zahl an verschiedenen Flüssen, deren Verwaltung in den beteiligten Vermittlungselementen große Tabellen bzw. intelligente Datenstrukturen zur Minimierung von Suchzeiten erfordert.

5.4.3 Differentiated Services

Differentiated Services (DiffServ) wurde von der IETF ab etwa 1998 in [RFC2474], [RFC2475], [RFC2597], [RFC2598] und [RFC3260] vorgestellt.
Im Gegensatz zu IntServ, das ein Quality-of-Service-Verfahren darstellt, ist DiffServ ein Class-of-Service-Verfahren zur Realisierung von QoS. Das bedeutet, daß bei DiffServ keine feste Bandbreitenreservierung für die verschiedenen Datenströme erfolgt, sondern eine differenzierte Verarbeitung dieser Flüsse in den Vermittlungselementen geschieht. Außerdem arbeitet DiffServ verbindungslos.
Konkret bedeutet das eine Einteilung in Dienstklassen und entsprechend dieser Klassen eine Verarbeitung in den Vermittlungselementen.

- **Einteilung in Dienstklassen**: Zusammengehörige Flüsse bzw. Datenströme werden zu Dienstklassen zusammengefasst und entsprechend gekennzeichnet. Diese Kennzeichnung geschieht durch Belegen des „Type-of-Service“-Felds im IP-Header mit der jeweiligen Klassennummer (Differentiated-Service-Feld, DS-Feld).

- **Verarbeitung in den Vermittlungselementen**: Der wichtigste Schritt von DiffServ geschieht in den Vermittlungselementen. Ohne Einsatz von DiffServ besitzen die Vermittlungselemente nur eine (FIFO)-Warteschlange, in der die Pakete in der Reihenfolge des Eintreffens bearbeitet und weitergeleitet werden. Die Vermittlungselemente besitzen bei DiffServ mehrere (FIFO)-Warteschlangen, von denen eine/mehrere vorrangig bearbeitet werden.
  Dies hat den Zweck, bestimmte Datenpakete, die zu einer Dienstklasse gehören, unabhängig von den anderen Klassen zu verarbeiten und weiterzuleiten.
  Ein Beispiel für die Realisierung in den Vermittlungselementen wäre (3 Klassen – wobei Klasse 1 vor Klasse 2 behandelt werden soll und Klasse 3 die Best-Effort-Klasse ist – und 3 Warteschlangen): jede Klasse eine Warteschlange, zuerst Verarbeitung von Warteschlange der Klasse 1; wenn diese leer, dann Warteschlange der Klasse 2; wenn weder Warteschlangen der Klassen 1 und 2 belegt sind, erfolgt die Verarbeitung von Paketen aus der Warteschlange 3.

- **Domänenbildung**: Wie bisher erläutert, werden zusammengehördende Flüsse zu Klassen zusammengefasst und diese Klassen in den Vermittlungselementen ggf. vorrangig behandelt. Damit dies geschehen kann, müssen mehrere Komponenten zusammenarbeiten, die dieselben Klassen- und Queueing-Definitionen besitzen.
  Daher ist für diesen Abschnitt des Netzes eine Domänenbildung erforderlich, d. h. innerhalb dieser Domäne erfolgt die Anwendung von DiffServ.
  Dies erfordert eine Unterteilung der beteiligten Vermittlungselemente und Komponenten in:

  – Interior-Komponenten: Vermittlungselemente innerhalb der DiffServ-Domäne, die die Verarbeitung und Weiterleitung gemäß den definierten Klassen und Warteschlangen vornehmen (sie ändern das DS-Feld der Pakete nicht!). Außerdem sind dies auch die beteiligten Nutzer, die ein Marking ihrer Datenpakete gemäß den DiffServ-Regeln vornehmen und ihre Pakete in das Netz leiten.

  – Edge-Komponenten: Vermittlungselemente, die sich an den Endpunkten der DiffServ-Domäne befinden. Zusätzlich zur DiffServ-konformen Weiterleitung der Pakete innerhalb der DiffServ-Domäne haben sie Pakete von außerhalb der DiffServ-Domäne zu markieren, d.h. in eine der Klassen der DiffServ-Domäne einzuteilen. Dies ist meist die niedrigste Klasse (d.h. best-effort), da ankommende Pakete entweder kein belegtes DS-Feld bzw. ein DS-Feld einer anderen DiffServ-Domäne besitzen, die nicht konform mit den Klasseneinteilungen ist, zu der das Vermittlungselement gehört.

- **Folgerungen**:

  - DiffServ kann keine harten Garantien für die Realisierung von QoS bieten, da die Verarbeitung basierend auf einer Klasseneinteilung erfolgt (wenn alle Pakete zur höchstwertigen Klasse gehören, gibt es faktisch keine Unterteilung mehr, sodaß DiffServ keinerlei Wirkung mehr zeigen kann).

  - Bei DiffServ ist regelkonformes Verfahren aller Teilnehmer der DiffServ-Domäne verpflichtend, da sonst diverse Teilnehmer versuchen, ihre Datenpakete als höherwertig zu markieren und so eine bevorzugte Verarbeitung zu erreichen. Wenn dies eine Mehrheit macht, kommt das Verhalten einem reinen best-effort-Netz sehr nahe, da fast nur Pakete mit hochwertigen Klassen vorhanden sind.

  - Eine sorgsam getroffene Klassendefinition ist notwendig, da sehr viele verschiedene Dienste bzw. Flüsse zu einer begrenzten Klassenanzahl aggregiert werden müssen (Verwaltungsaufwand bei vielen Klassen!).

  - In stark belasteten Netzen bringt DiffServ nur für die hochwertigsten Klassen eine Verbesserung; demgegenüber besteht bei niederwertigen Klassen die Gefahr des „Verhungerns“ der Datenpakete, da sie entweder nicht mehr zeitgerecht weitergeleitet werden oder wegen Überfüllung einer Warteschlange verworfen werden müsen, was u.U. Retransmissionen auslöst, die die Netzbelastung noch weiter erhöhen.

- **Implementierungsbeispiel für VoIP**:
  Klasseneinteilung (nach Priorität aufsteigend geordnet):

  - Klasse 1: UDP-Gesprächsdatenströme

  - Klasse 2: TCP-Signalisierungdaten

  - Klasse 3: best-effort (sonstiger Netzverkehr)

  Verarbeitung in den Vermittlungselementen:

  - Warteschlange 1 (für Klasse 1): vorrangige Behandlung (Priority-Queue)

  - Warteschlange 2 (für Klasse 2): Behandlung, wenn Klasse 1 leer

  - Warteschlagen 3 (für Klasse 3): Verarbeitung, wenn Warteschlange 1 und 2 leer

  Alternative zu obigem Vorschlag, da viele Vermittlungselemente nur eine Priority-Queue unterstützen: Warteschlange 1 ist Priority-Queue, Warteschlangen 2 und 3 werden im Round-Robin-Verfahren bearbeitet (wenn Warteschlange 1 leer).

DiffServ stellt auch eine Möglichkeit dar, QoS zu realisieren.
Zwischen IntServ und DiffServ vergleichend, ist zu sagen, daß DiffServ – im Gegensatz zu IntServ – keine harten QoS-Garantien bieten kann. Dafür ist Implementierung und Administration einfacher, da bei DiffServ die Anzahl der Dienstklassen viel kleiner als die Anzahl der Flüsse bei IntServ ist (durch die Aggregation von zusammengehörenden Flüssen zu Dienstklassen bedingt).

Ein VoIP-System sollte mindestens eine der beiden Möglichkeiten bieten (derzeit unterstützen die meisten Anbieter von VoIP-Systemen nur DiffServ).

5.5 Power over Ethernet

5.5.1 Möglichkeiten der Stromversorgung von Endgeräten

Bei VoIP ergibt sich für die Endgeräte das Problem, daß sie mit Strom versorgt werden müssen. Im Gegensatz zur klassischen TK-Technik, wo die Stromversorgung über die Verkabelung zur TK-Anlage erfolgt, ist eine Stromversorgung in IP-Netzen a priori nicht vorgesehen.
Zur Lösung dieses Problems gibt es prinzipiell mehrere Möglichkeiten, wobei diese unter den Gesichtspunkten Notstromversorgung, Fehlerwahrscheinlichkeiten und Managebarkeit beleuchtet werden:

- **Stromversorgung über ein separates Netzteil**: Diese Variante hat den Nachteil, daß zum einen im Fall eines Stromausfalls alle IP-Telefone stromlos wären (dies hat u. a. zur Folge, daß keine Notrufe mehr abgesetzt werden können) und zum anderen ergeben sich höhere Fehlerquellen (Defekt des Netzteils, Herausrutschen des Stromsteckers, versehentliches Abstecken, ...); außerdem sind die Netzteile und somit die Stromversorgung nicht managebar. Somit ist diese Alternative nicht empfehlenswert.

- **Stromversorgung über sog. „Power-Hubs“**: Die Power-Hubs werden zwischen Switch und IP-Telefon geschaltet, wobei pro Hub eine bestimmte Portzahl mit Strom versorgt werden kann. Hinsichtlich Notstromversorgung ist eine brauchbare Lösung möglich, nämlich die Anbindung von Power-Hubs an unterbrechungsfreie Stromversorgungen (USV). Die Fehlerwahrscheinlichkeit ist im Vergleich mit den separaten Steckernetzteilen deutlich geringer und die Power-Hubs sind prinzipiell managebar. Als Fazit ist diese Lösung empfehlenswert.

- **Stromversorgung über die Switches**: Die eleganteste Lösung stellt prinzipiell die Stromversorgung der IP-Telefone über die Switches dar, d. h. die Stromeinspeisung erfolgt direkt am LAN-Port des Switches. Im Vergleich zu den Power-Hubs ergibt sich hier der Vorteil, daß nur noch ein Gerät für die Daten- und Stromnetzanbindung vorhanden ist (im Vergleich zu den zwei Geräten Switch und Power-Hub), was die Fehleranfälligkeit reduziert. Außerdem ist die Managebarkeit deutlich erleichtert, da die Switchports normalerweise sowieso überwacht werden (hier werden zusätzlich die Werte, die die Stromversorgung betreffen, verwendet).

Das einzige Handicap für die Nutzung der dritten Alternative bestand darin, daß im gebräuchlichen Standard für (Fast)-Ethernet IEEE 802.3 keine Möglichkeit für die Stromversorgung definiert wurde (bei Ethernet werden die Pinpaare 1/2 und 3/6 für die Datenübertragung verwendet). Daher wurde Ende 2003 eine Erweiterung verabschiedet, die die Stromversorgung über Ethernet erlaubt: IEEE 802.3af [IEEE 802.3af](gebräuchliche Bezeichungen hierfür sind auch „Power over Ethernet“ (PoE) sowie „Power over LAN“ (POL)). Im folgenden Abschnitt wird dieser Standard eingehend vorgestellt.

5.5.2 Der Standard IEEE 802.3af

IEEE 802.3af verwendet die bisher bestehende Netzverkabelung, also z.B. Twisted-Pair-Kabel nach Cat. 5, was impliziert, daß wegen ihres geringen Leitungsquerschnitts relativ hohe Leitungswiderstände bestehen, was die maximale Übertragungsleistung einschränkt. Daher beträgt die maximale Leistungsaufnahme pro Port 15,4 Watt bei einer Spannung von 48 Volt und einer Stromstärke von 350 Milliampere (bei der Kabellänge von 100 Metern bleiben so noch etwa 13 Watt für das Endgerät verfügbar, [BBE04]). Er ist für Ethernet und Fast-Ethernet spezifiziert.
Im Standard werden zwei Gerätetypen unterschieden, wobei besonderes Augenmerk auf Geräte gelegt werden muß, die mit IEEE 802.3af nicht umgehen können:

- Powered Devices (PD): die Endgeräte

- Power Source Equipment (PSE): die Stromversorger

Bezogen auf die Stromversorgung kann die Stromeinspeisung entweder über die von Ethernet verwendeten Adernpaare (1/2 und 3/6) - auch „Phantomspeisung“ genannt (was bei einigen Verkabelungsstrukturen von Vorteil ist, da vor einigen Jahren häufig „Cable Sharing“ eingesetzt wurde, d. h. die prinizipiell zur Verfügung stehenden acht Adern pro Twisted-Pair-Kabel wurden für zwei LAN-Ports verwendet) oder über die beiden nicht verwendeten Paare 4/5 und 7/8 erfolgen. Die Tabelle 5.1 zeigt die verschiedenen Pinbelegungen im Überblick, wobei der Vollständigkeit halber auch die Belegungen für S_0 und S_{2M} angegeben werden. Standardkonforme Abnehmer (PD) müssen beide Verfahren unterstützen, dem Versorger

RJ45-Pin	(Fast) Ethernet	802.3af Phantom	802.3af Spare Pairs	S_0	S_{2M}
1	RX+	RX+, V+	RX+	n.b.	RX+
2	RX-	RX-, V+	RX-	n.b.	RX-
3	TX+	TX+, V-	TX+	TX+	n.b.
4	n.b.	n.b.	V+	RX+	TX+
5	n.b.	n.b.	V+	RX-	TX-
6	TX-	TX-, V-	TX-	TX-	n.b.
7	n.b.	n.b.	V-	n.b.	n.b.
8	n.b.	n.b.	V-	n.b.	n.b.

Tabelle 5.1: Pinbelegungen

(dem PSE) steht es frei zu wählen, wobei die gleichzeitige Nutzung beider Verfahren untersagt ist.
Um die Sicherheit älterer Netzwerkkomponenten zu garantieren, schreibt der Standard vor, daß sie PoE-Endgeräte identifizieren müssen, bevor sie die Spannungsversorgung aktivieren. Dies geschieht über eine Prüfspannung beim Anstecken von Verbrauchern, die ihrerseits einen spezifizierten Innenwiderstand und Kapazität aufweisen müssen.

Durch den Standard IEEE 802.3af ist somit eine integrierte Lösung zur Stromversorgung möglich, die nach Möglichkeit eingesetzt werden sollte (auf weitere proprietäre Standards zur Stromversorgung, die vor der Verabschiedung von IEEE 802.3af verwendet wurden, wird hier nicht eingegangen).

5.6 VLAN-Tagging

Die meisten Hersteller von VoIP-Systemen bieten Ihre VoIP mit einem integrierten Switch zur Anschaltung eines IP-basierten Geräts an (normalerweise wird hier der PC des Mitarbeiters angesteckt, da jeder Mitarbeiter üblicherweise zu seinem Telefon einen Arbeitsplatzrechner besitzt).
Vorteil dieser Lösung ist, daß somit zum Access-Switch (Switch in der Tertiärebene in einer strukturierten Verkabelung) nur noch eine Verbindung benötigt wird („One-wire-to-the-desk“).

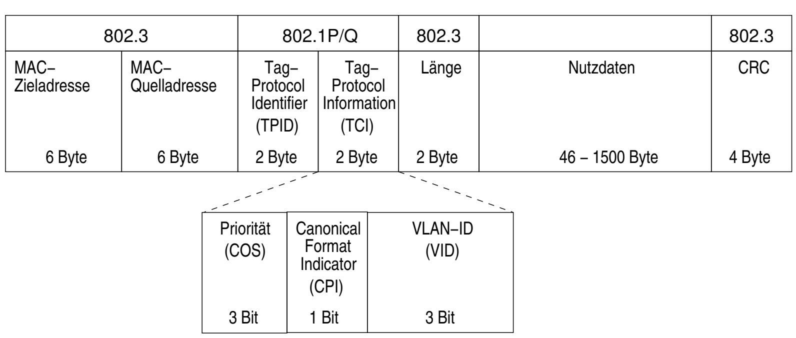

Abbildung 5.8: Ethernet-Frame mit IEEE 802.1P/Q-Tag

Darüber hinaus unterstützen diese VoIP-Endgeräte noch die Standards IEEE 802.1p/q ([IEEE 802.1p] und [IEEE 802.1q]), die auf dem Wegstück zwischen Access-Switch (Tertiärebene) und VoIP-Telefon die Zusammenfassung mehrerer VLAN´s sowie eine Priorisierung auf Layer-2-Ebene erlauben.
Hierbei wird der Ethernet-Frame – wie Abbildung 5.8 zeigt – um 4 Byte verlängert. Diese Informationen werden von den Netzkomponenten (bei entsprechender Konfiguration) gelesen und verarbeitet.
Ein VLAN (Virtual LAN) stellt ein logisches Netz auf einem physischen Netz dar, d.h. die jeweiligen VLAN´s haben verschiedene Adreßbereiche, liegen aber in einem physischen LAN. Hierbei wird am Access-Switch-Port ein sog. „Trunk-Port“ eingerichtet, dem die beiden VLAN´s zugeordnet sind; hierbei wird das VLAN für die Sprachdaten als „tagged“ definiert und das andere stellt das sog. „native“ VLAN dar. Abbildung 5.9 illustriert diese Konfiguration.

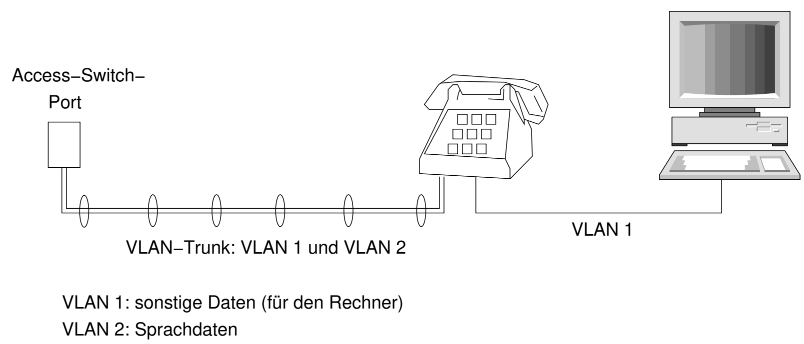

Abbildung 5.9: Schematische Darstellung von „VLAN-Trunking“ und „One-wire-to-the-desk“

Vorteil dieser Lösung ist die Möglichkeit der Verkehrstrennung von Sprach- und Datenverkehr, d.h. die Sprachdaten können durch die VLAN-Bezeichnung von den sonstigen Datenpaketen unterschieden und separat (z.B. bevorrechtigt) behandelt werden.

Dieses „VLAN-Tagging“ wird normalerweise nur in den Primär- und Sekundärebenen (z.B. zur redundanten Anbindung von Routern oder Switches) verwendet; im Tertiärbereich wird dies Verfahren bisher nicht eingesetzt, da es bisher nicht notwendig war (daher konnte bisher kaum ein Gerät den Abschluß eines Trunk-Ports bilden).
Weitere Einzelheiten zum Einsatz dieser Technik werden in Kapitel 7.4.2.2 erläutert.

5.7 Zusammenfassung

Von den Herstellern von VoIP-Systemen werden zwei verschiedene Architekturen angeboten: LAN-PBX- und Soft-PBX-Systeme. Im Vergleich sind diese (bis auf kleine Ausnahmen) als gleichwertig anzusehen.
Für Verbundnetze gibt es prinzipiell mehrere Realisierungsmöglichkeiten, wobei diese sich im Prinzip nur in der Anzahl und dem Standort der zentralen Komponenten (Anrufmanagementsysteme) unterscheiden, von denen keines bei abstrakter Betrachtung einen herausstechenden Vorteil besitzt.

Somit ergeben sich bei diesen Systemen und Realisierungsmöglichkeiten grundsätzlich keine gravierenden Unterschiede in Hinblick auf das Management.
Folglich ist es möglich, für diese Systeme ein übergreifendes Managementkonzept zu entwickeln, was im nächsten Kapitel erfolgt.

Kapitel 6

Erstellung des Managementkonzepts

In diesem Kapitel wird das Managementkonzept für VoIP – basierend auf den im Anforderungskatalog (Kapitel 4) und dem State-of-the-Art 5 vorgestellten und erarbeiteten Aspekten – erstellt und aufgebaut.
Es ist wie folgt aufgebaut: Zu Beginn werden allgemeine Grundsätze für das Managementkonzept aufgestellt; danach werden klassische Managementansätze und „Best practices“ (nach ITIL) vorgestellt und erläutert.
Daraufhin werden im eigentlichen Konzept Ansätze für die Betriebszustände Planung, Installation/Inbetriebnahme und laufender Betrieb erläutert.
Diese Ansätze stellen eine Handlungsempfehlung für ein VoIP-System dar und sind bei der Implementierung auf die örtlichen und betrieblichen Gegebenheiten anzupassen. In diesem Kapitel werden Ratschläge für den Aufbau einer Organisation zur Umsetzung dieses Managementkonzepts gegeben. Hierbei kann es sich nur um Ratschläge handeln, da die Aufbau- und Ablauforganisation eines Unternehmens zu stark von der Firmenphilosophie und örtlichen Gegebenheiten abhängt, als daß sie verallgemeinert werden könnten. Daher erfolgt hier keine weitere Ausarbeitung der organisatorischen Empfehlungen; diese sind unternehmensspezifisch umzusetzen.
Eine Realisierung dieses Managementkonzepts erfolgt in Kapitel 7; darin werden auch die organisatorischen Aufbau- und Ablaufaspekte am Beispiel des in Kapitel 2 vorgestellten Szenarios behandelt.
Prinzipiell ist dieses Managementkonzept aber in jeder Fallgestaltung einsetzbar und berücksichtigt die im Anforderungskatalog (siehe Kapitel 4) aufgestellten Forderungen.

6.1 Allgemeine Grundsätze

Management stellt in der Industrie einen beträchtlichen Anteil an der betrieblichen Leistungserstellung dar und daher wird ihm auch in der Betriebswirtschaftslehre ein hoher Stellenwert zugewiesen.
Seit Beginn der 1980er-Jahre wurde in der Industrie die betriebliche Leistungserstellung in die Gebiete Planung, Ausführung, Überprüfung und Neujustierung aufgeteilt und darüberhinaus alle Aktivitäten in Prozesse untergliedert.
Die Ursprünge dieser Techniken kamen aus der japanischen Automobilindustrie, die diese zum damaligen Zeitpunkt bereits erfolgreich einsetzte, was ihren Weltmarktanteil und die Gewinne der Automobilkonzerne in nennenswertem Umfang steigen ließ.
Grundprinzip dieser Techniken war und ist das „Just-in-time“-Prinzip. Dies bedeutet, daß die benötigten Ressourcen zur richtigen Zeit in der richtigen Menge am richtigen Ort verfügbar sind, wobei hierbei besonderes Augenmerk auf ein aktives Bestands- und Kapazitätsmanagement gelegt wird, da ein Großteil kalkulatorischer Kosten durch Lagerbestände entsteht, die eventuell nicht notwendig sind.
Anmerkung: Im Folgenden werden einige Arbeiten und Vorlesungsunterlagen von Herrn Prof. Dr. Dr. Horst Wildemann zitiert und verwendet. Herr Dr. Wildemann ist Professor für Betriebswirtschaftslehre (mit Schwerpunkte Logistik) an der TU München und hat Mitte der 1980er-Jahre das Just-in-Time-Prinzip

(mit anderen Kollegen) nach Europa übertragen und (ebenfalls bei der Automobilindustrie) eingeführt; hierfür wurde er mit dem Bundesverdienstkreuz der Bundesrepublik Deutschland ausgezeichnet.
Er ist darüber hinaus in der Industrie sehr angesehen und integriert Gastvorträge von Vorstands- und Aufsichtsratsmitgliedern großer deutscher Unternehmen (z.B. Allianz, BASF, DaimlerChrysler, Siemens) in seine Veranstaltungen. Desweiteren richtet er einmal pro Jahr (in den Räumen der TU München) das „Münchner Management Forum“ aus, das sich mit aktuellen Fragestellungen des Managements und der Logistik in Unternehmen beschäftigt und an dem Vorstandsmitglieder vieler Unternehmen teilnehmen.
Das JIT-Konzept fußt auf folgenden Bausteinen:

- Integrierte Informationsverarbeitung: Implementierung des Holprinzips (KANBAN, Engpaßsteuerung), papierlose Produktion und Beschaffung, Methodenintegration
- Fertigungssegmentierung: Kapazitätsentflechung (modulares Unternehmen), Flußoptimierung (Losgrößenreduzierung, selbststeuernde Regelkreise), Gruppenorganisation (TQM, Qualitätssicherung)
- Produktionssynchrone Beschaffung: partnerschaftliches Verhältnis zwischen Abnehmer und Lieferant (Teile- und Lieferantenauswahl, Informationsfluß, Qualitätssicherungskonzept), Reduzierung der Zulieferzahl pro Teil und Produkt), Vertragsmanagement zwischen Abnehmer und Lieferant.

Weitere Grundprinzipien bestehen in von JIT-Grundsätzen ([WIL01]) abgeleiteten Aspekten. Empirische Untersuchungen zeigen, daß bei Anwendung dieses Konzepts Zeit- und Bestandsverkürzungen um 50 % bei gleichzeitiger Stückkostenreduzierung um 10 %, Qualitätsverbesserungen um das 5- bis 10-fache und Flexibilitätserhöhungen erreichbar sind ([WIL01]), die durch analoge Anwendung auf IT-Organisationen in ähnlicher Weise erreichbar sind.
Diese Prinzipien wurden vom Produktionsbereich auf die IT-Services übertragen, indem bei ITIL der Prozeß (mit Qualitätssicherungsmechanismen) in den Mittelpunkt gestellt wurde (die Prozesse entstehen durch die Abstraktion der Managementaufgaben).
Um dieses Just-in-Time-Prinzip umsetzen zu können, sind noch andere Aspekte von Bedeutung:

- aktives Prozeßmanagement, d.h. Abstimmung aller Produktionsprozesse aufeinander durch Reduktion von Leerlaufzeiten sowie optimales Layout der Arbeitsmittel
- Lieferantenbewertung, d.h. Auswahl der Lieferanten nicht nur über den Preis, sondern auch durch Qualität der Produkte, Zuverlässigkeit, …; u.U. ist der Lieferant auch als Lieferant bzw. Produzent größerer Teilsysteme in die Produktionsprozesse einzubinden – siehe auch die Unterlagen zu „Supply-Chain-Management“ ([WIL04]).

Hintergrund dieser integrierten Logistikprozesse ist, daß zum einen ein beträchtlicher Kostenanteil in Overheadkosten, Leerlaufkosten und kalkulatorische Zinsen besteht und zum anderen in Dienstleistungsbetrieben die Personalkosten den größten Kostenblock darstellen (in den anderen Sektoren betragen die Personalkosten auch einen sehr großen Kostenanteil), der mit integrierten Konzepten minimiert und so in Richtung eines minimalen Wertes geführt werden kann.

Wie die obigen Ausführungen zeigen, basieren Managementkonzepte auf der Integration von Prozessen, um Leerlaufzeiten und Überkapazitäten abzuschaffen bzw. zu minimieren und den Personalkostenanteil zurückzufahren.

In der IT-Industrie setzt sich dieser Trend in den letzten Jahren langsam durch:
Zu Beginn des EDV-Einsatzes und bis zur Jahrtausendwende waren die Kosten (fast) egal. Hauptsache für die einsetzenden Unternehmen war die Funktionsfähigkeit der IT-Systeme (die IT wurde damals zur Rationalisierung und Kosteneinsparung in den anderen Unternehmensbereichen eingesetzt; Stichwort sind Enterprise-Ressource-Planning-Systeme, ERP-Systeme). In diesem Stadium fehlte meist auch ein Prozeßmanagement bzw. Kostenbewußtsein bei den IT-Verantwortlichen und Mitarbeitern. Prozeßorientierung, Dokumentation und Formalisierung waren gering ausgeprägt.
Durch immer komplexere Systeme, fortschreitenden Einsatz von IT, dem Platzen der „Neuen-Markt-Blase“ sowie weitgehender Rationalisierung in den anderen Bereichen durch integrierte Systeme, ergab sich ab Anfang des Jahrtausends eine zunehmende Kürzung der IT-Budgets und – damit verbunden – eine

wachsende Tendenz zu Outsourcing von IT-Dienstleistungen.
Um IT-Abteilungen und IT-Dienstleister effizienter zu machen, entstand und entsteht der Druck, ein Prozeßmanagement einzuführen (also Abläufe zu formalisieren), da dieselben Abläufe und Tätigkeiten bei diversen IT-Unternehmen immer wieder vorkommen und zum anderen Vergleichbarkeit von IT-Unternehmen herzustellen.
Diese Ansätze wurden von verschiedenen Organisationen und Unternehmen aufgegriffen und Richtlinien zum IT-Management herausgegeben. Beispiele hierfür sind ITIL, auf das in 6.3 eingegangen wird, und eTOM.

Um dieses Managementkonzept zu konzipieren, werden zuerst klassische Managementansätze und danach – basierend auf klassischen Managementansätzen, ITIL und betriebswirtschaftlichen Grundsätzen das Managementkonzept erstellt.

6.2 Kurzdefinition klassischer Managementansätze

Dieser Abschnitt ist an die Definitionen und Erläuterung in [HAN99] angelehnt. Das Management aus klassischer Sicht befaßt sich prinzipiell mit technischen und übergreifenden Fragestellungen. Hierbei wurden Managementdimensionen (wie in Abbildung 6.1 dargestellt) entwickelt. Das technische Management

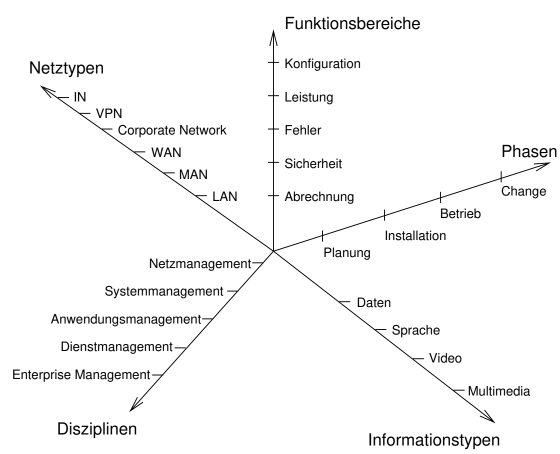

Abbildung 6.1: Managementdimensionen ([HAN99])

eines Systems besteht aus dem Lebenszyklus des Systems (Phasen), den verschiedenen Informationstypen des Systems, den verwendeten Netztypen, Funktionsbereichen und Managementdisziplinen.
Ein Rahmenwerk für managementrelevante Standards wird *Managementarchitektur* genannt.
Im *Informationsmodell* einer solchen Architektur erfolgt eine Festlegung, welche Möglichkeiten syntaktisch und semantisch zur managementrelevanten, herstellerübergreifenden Modellierung und Beschreibung von Ressourcen und Informationen bestehen. Das *Kommunikationsmodell* definiert die Zugriffe auf Managementobjekte und -protokolle. Das *Funktionsmodell* gliedert den Komplex „Management“ in handhabbare Einheiten und definiert generische Managementfunktionen. Damit wird die Basis für ein Baukastensystem von modularen Managementlösungen bzw. Management-by-Delegation festgelegt. Das *Organisationsmodell* schließlich legt Rollen, Kooperationsmodelle und Domänen fest.
Diese Modelle werden in den folgenden Abschnitten beschrieben und ihre Teilaufgaben dargestellt.

6.2.1 Informationsmodell

In heterogenen Umgebungen gibt es grundsätzlich keine gemeinsame Definition über die Informationen, die zur Lösung der Managementaufgaben ausgetauscht werden müssen. Das Informationsmodell stellt einen Beschreibungsrahmen für Managementobjekte dar; hierbei sind nur managementrelevante Parameter der Managementobjekte darzustellen. Somit kann diese Darstellung als Abstraktion der tatsächlichen Ressourcen gesehen werden.
Hierbei sind folgende Objekte charakterisiert:

- Managed Objects (MO): Die eigentlichen Objekte, die verwaltet werden sollen. Im Informationsmodell ist festzulegen, wie es identifiziert werden kann, welches Verhalten es zeigt, wie es geändert werden kann, welche Beziehungen zu anderen Managed Objects bestehen und über welches Managementprotokoll mit ihm kommuniziert werden kann.
- Management Information Base (MIB): Eine „Datenbank“ bzw. Datenbasis managementrelevanter Attribute von Managed Objects. Hierbei kann jedes MO eine eigene MIB beinhalten oder eine MIB für mehrere Managed Objects vorhanden sein.
  In Abhängigkeit von der verwendeten Managementarchitektur werden unterschiedliche Modellierungsansätze gewählt. Beispielsweise ist beim ISO-Management ein objektorientierter Ansatz vorhanden, beim Internet-Management ist dies ein Datentypansatz.

Zusammengefaßt stellt das Informationsmodell eine Abstraktion der realen Hard-/Softwareumgebung dar sowie eine Datensammlung managementrelevanter Informationen bereit.

6.2.2 Organisationsmodell

Das Organisationsmodell einer Managementarchitektur beschreibt die (technische) Aufbau- und Ablauforganisation von vernetzten Systemen; dies beinhaltet z. B. die Kooperationsformen, Rollen, Gruppenbildungen. Grundlegend für die Strukturbeschreibung ist hierbei die Existenz von „Managern“ und „Managed Ressources“ (MR); ein Manager ist für die ihm unterstellten Managed Ressources verantwortlich, wobei aus Managersicht auch eine Aufteilung hinsichtlich bestimmter Funktionsbereiche vorhanden sein kann (Sicherheitsmanagement, Leistungsmanagement, . . .). Hierbei gibt es vielerlei Möglichkeiten, von denen einige beispielhaft genannt werden:

- zentralistischer Ansatz: ein Manager, der alle MR´s kontrolliert
- hierarchischer Ansatz: baumartige Struktur von Managern mit den MR´s an den Blättern des Baums
- verteilter Ansatz: mehrere gleichberechtigte Manager, von denen jeder einige MR´s verantwortet

Das Organisationsmodell stellt somit die Aufbauorganisation des vernetzten Systems dar.

6.2.3 Kommunikationsmodell

Das Kommunikationsmodell legt Prinzipien und Konzepte zum Austausch von Managementinformationen zwischen den Akteuren fest. Hierbei sind unterschiedliche Zielsetzungen möglich, wobei die Initiative meist vom Managementsystem bzw. vom Manager ausgeht: Monitoring, Controlling (Eingriff auf das MO) sowie Absetzen von asynchronen Meldungen (vom MO ausgehend, beispielsweise bei schwerwiegenden Fehlfunktionen).
Im Kommunikationsmodell ist u.a. festzulegen,

- welche Partner zur Kommunikation miteinander berechtigt sind
- welcher Kommunikationsmechanismus verwendet wird, d.h. Protokoll- und Dienstspezifikation zum Informationsaustausch unter Berücksichtigung der zugrundeliegenden Kommunikationsarchitektur
- wie die Syntax und Semantik der Protokoll-Datenstrukturen aufgebaut ist.

Zusammengefaßt legt das Kommunikationsmodell fest, wie und mit welchen Protokollen auf die MIB´s der MO´s zugegriffen werden kann.

6.2.4 Funktionsmodell

Das Funktionsmodell einer Managementarchitektur gliedert die Gesamtaufgaben des Managements in Funktionsbereiche und legt allgemeine Managementfunktionen fest. Im Funktionsmodell sind für die einzelnen Funktionsbereiche die erwartete Funktionalität und die Dienste sowie die Managementobjekte zur Erbringung der Funktionalität zu definieren. Allgemein wurden folgende Bereiche festgelegt (FCAPS):

- **F**ault Management: Fehler sind Soll-Ist-Abweichungen im Verhalten von Ressourcen. Das Fehlermanagement umfaßt sowohl reaktive als auch proaktive Maßnahmen. Die Hauptaufgabe des Fehlermanagements liegt in der Aufrechterhaltung einer hohen Verfügbarkeit durch schnelle Identifizierung und Beseitigung von Fehlern. Teilaufgaben hierbei sind u.a.:
  - Überwachung des Netz- und Systemzustands
  - Entgegennahme und Verarbeitung von Alarmen
  - Diagnose von Fehlerursachen
  - Einleitung und Überprüfung von Maßnahmen zur Fehlerbehebung
  - Einrichtung eines Help-Desks
  - Einsatz eines Trouble-Ticket-Systems (TTS)
- **C**onfiguration Management: Der Begriff „Konfiguration“ kann grundsätzlich mehrere Bedeutungen haben. Im Bereich des Netz- und Systemmanagements wird hierunter folgendes verstanden:
  - Die *Beschreibung* des vernetzten Systems durch die eingesetzten Komponenten, die realen Verbindungen und logischen Beziehungen.
  - Der *Vorgang* der Konfiguration als Aktivität oder Manipulation an der Struktur der verteilten Systeme.
  - Das *Ergebnis* des Konfigurationsvorgangs (das System in seiner derzeitigen Ausprägung).

  Normalerweise ergibt sich aus dem Kontext, welche Bedeutung der Begriff „Konfiguration“ jeweils hat. Zur Konfiguration gehört auch die Erstellung einer Dokumentation, um Transparenz sicherzustellen und die Folgen bei Personalwechseln o.ä. gering zu halten.
  Das Konfigurationsmanagement umfaßt folglich das Setzen von Parametern, Festlegung von Schwellwerten und Filtern, die Dokumentation des Gesamtsystems und von Änderungen sowie das aktive Ändern der Konfiguration.
- **A**ccounting Management: Die Bereitstellung von Kommunikations- und sonstigen Diensten führt zu Kosten, die auf die Verursacher umgelegt werden müssen. Wie diese Aufteilung erfolgt, ist Gegenstand der Abrechnungspolitik. Eine wichtige Anforderung an das Abrechnungsmanagement besteht somit in der Möglichkeit, diese Aufteilung gemäß den Vorgaben der Abrechnungspolitik durchführen zu können.
  Teilaufgaben des Abrechnungsmanagements sind: Festlegung von Abrechnungsdaten, Führung von Abrechnungskonten, Kostenzuordnung auf die Konten, Kontingentverwaltung und -überwachung, Führung von Verbrauchsstatistiken sowie die Festlegung der Abrechnungspolitik sowie der Tarife.
- **P**erformance Management: Das Leistungsmanagement ist von seiner Zielsetzung her als eine Weiterführung des Fehlermanagements zu verstehen. Es setzt sich zum Ziel, die Lauffähigkeit des Systems innerhalb bestimmer Dienstgüteparameter sicherzustellen. Diese Parameter sind in Service-Levels mit dem Kunden festzulegen, wobei hierauf im weiteren Verlauf des Kapitels detailliert eingegangen wird.
  Die Teilaufgaben des Performance Managements bestehen beispielsweise in:

  - Bestimmung von Dienstgüteparametern und Metriken
  - Ressourcenüberwachung hinsichtlich Engpässen
  - Durchführung von Messungen
  - Aufzeichnung von Systemprotokollen
  - Aufbereitung und Aggregation von Meßdaten
  - Durchführung von Leistungs- und Kapazitätsplanungen.

- **S**ecurity Management: Sicherheit bedeutet in diesem Kontext das Management der Sicherheit in einem verteilten System, basierend auf den schützenswerten Ressourcen in einem Unternehmen (wie Informationen, Infrastruktur, Dienstleistungen, . . .).
  Dem Verlust dieser Werte ist durch Sicherheitsmaßnahmen vorzubeugen, die abhängig von einer Bedrohungsanalyse sind. Bedrohungen für verteilte Systeme entstehen u.a. durch:

  - passive Angriffe
  - aktive Angriffe
  - Fehlfunktion von Ressourcen
  - Fehlbedienung

  Basierend auf der Bedrohungsanalyse und den zu schützenden Werten ergeben sich Sicherheitsziele bzw. -anforderungen, auf deren Grundlage Sicherheitspolitiken entstehen müssen. Teilaufgaben des Sicherheitsmanagements bestehen beispielsweise in der Durchführung von Bedrohungsanalysen, Identitätsfeststellung, Sicherstellung von Vertraulichkeit und Datenintegrität sowie ständiger Berichterstattung.

6.3 Kurzdefinition von ITIL

6.3.1 Allgemeines

Der Hintergrund der Definition von ITIL besteht darin, daß Organisationen zunehmend von der IT abhängig sind, um ihre Unternehmensziele zu erreichen. Diese wachsende Abhängigkeit hat zu einem zunehmenden Bedarf an IT-Services geführt. Deren Qualität sollte gleichzeitig den Zielen der Organisation entsprechen und die Anforderungen des Kunden erfüllen ([ITSM04].
Innerhalb des Lebenszyklus eines IT-Systems erfordern Betrieb und notwendige Anpassungen sowie Wartung einen Großteil des gesamten Kosten- und Zeitaufwands. Effektivität und Effizienz des IT-Betriebs sind daher essentiell für den erfolgreichen Einsatz von IT-Systemen.
Die Inhalte des IT-Service-Managements bestehen in der Lieferung und der Unterstützung genau der IT-Services, die auf die Anforderungen und Bedürfnisse der einsetzenden Organisation zugeschnitten sind. Kurz gesagt hat IT-Service-Management die *Planung und Bereitstellung* einer *kundenorientierten Dienstleistung* mit Hilfe eines *prozeßorientierten Verfahrens* zum Ziel ([BKP02]).
Zur systematischen Umsetzung von IT-Service-Managements haben sich die in der Infrastructure Library (ITIL) entwickelten „Best Practices“, die von der OGC – einer britischen Behörde, die staatliche Rechenzentren betreibt – entwickelt, definiert und vorgestellt wurden und werden ([OGC00] und [OGC01]).

Zentrale Aspekte für die Umsetzung sind darin die Servicequalität und die Errichtung effektiver, effizienter Prozesse. Diese Prozesse befinden sich in einem immerwährenden Kreislauf von Planung, Ausführung, Überwachung und Nachjustierung zur Verbesserung der Prozeßqualität.
Bei ITIL bedeutsame Definitionen und Begriffsbestimmungen:

Prozeß: sich wiederholende Menge von Aktivitäten. Ein Prozeß hat eine Ein- und Ausgabe und besteht aus drei Teilaspekten, die jeweils voneinander abhängig sind:

- *Prozeßüberwachung*: Prozeßinhaber und Prozeßziel definieren und Bestimmung der Leistungsindikatoren und Qualitätsparameter des Prozesses.
- Die *Prozeßausführung* besteht aus Aktivitäten und Subprozessen.
- Die *Prozeßbedingungen* werden durch die verfügbaren Ressourcen und den Rollen der Beteiligten bestimmt.

Abbildung 6.2 verdeutlicht das Prozeßmodell sowie die Interdependenzen der Teilaspekte.

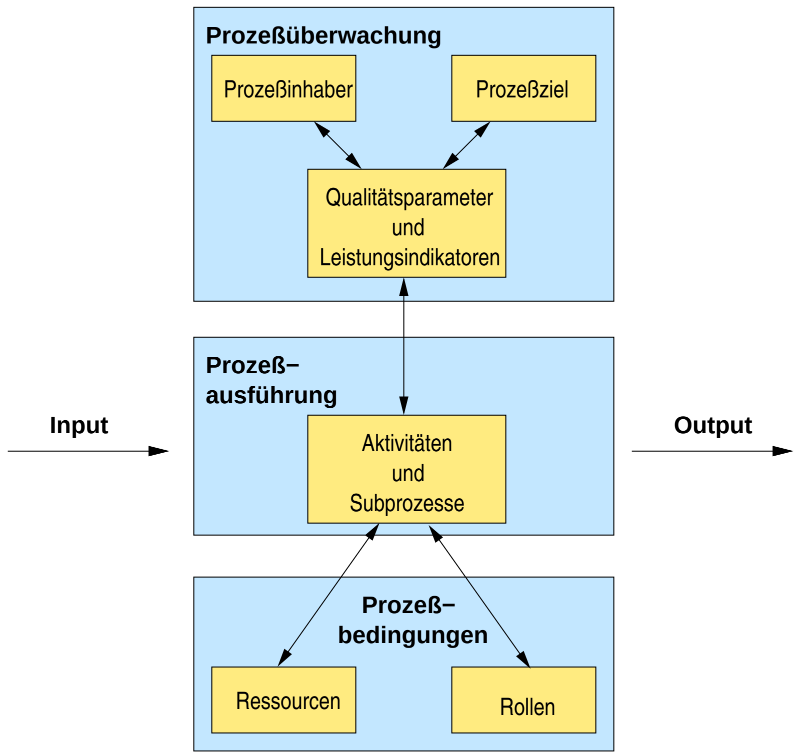

Abbildung 6.2: Generisches ITIL-Prozeßmodell

Prozeßinhaber: gegenüber dem Management der Organisation und den anderen Einheiten Verantwortlicher für die gesamte Prozeßplanung- und ausführung.

Ressourcen: sind beispielsweise Personal, Finanzmittel, Infrastrukturobjekte oder Wissen.

Kunde: einsetzendes Unternehmen bzw. Organisation

Anwender: Mitarbeiter des Kunden

Mit den Prozessen beschreibt ITIL vor allem die notwendigen Maßnahmen für die Lieferung von IT-Services in der gewünschten Qualität. Wie die Aufgaben und Zuständigkeiten auf Funktionen und Abteilungen verteilt werden, hängt nicht nur von der Art der IT-Organisation ab (in der Praxis soll eine ständige Anpassung der Organisation an die Prozeßstrukturen erfolgen).

Die nachstehende Aufzählung nennt beispielgebend Vorteile sowie Hindernisse von ITIL und deren Umsetzung (basierend auf [BKP02]).

- Vorteile für Kunden und Anwender:
  - bessere Ausrichtung der IT-Services auf Kundenbedürfnisse
  - besseres Kundenverhältnis durch Absprachen und (Qualitäts)-Vereinbarungen

  - bessere Kosten- und Qualitätskontrolle

- Vorteile für die IT-Organisation:
  - übersichtlichere und effizientiere Ausrichtung der IT-Organisation auf die Unternehmensziele
  - Formalisierung der Abläufe und Prozesse führt zu Vergleichbarkeit von IT-Organisationen (und schafft Voraussetzung von eventuellem Outsourcing)
  - Einführung eines Qualitätssicherungssystems und Fokussierung auf Kundenbedürfnisse

- mögliche Hindernisse:
  - Widerstände innerhalb der bestehenden Organisation, da die Einführung von ITIL u.U. einen kompletten Umbau der Aufbau- und Ablauforganisation machen kann
  - Aufbau überdimensionierter bürokratischer Strukturen bei zu feingliedriger Definition der Prozesse und Abläufe
  - Bewußtseinswandel und Kulturveränderung der Mitarbeiter notwendig

Die ITIL hat – wie die Ausführungen zeigen – viel mit den Kapitel 6.1 genannten Just-in-Time-Grundsätzen gemeinsam; daher hat auch der betriebswirtschaftliche Aspekt bei ITIL einen hohen Stellenwert.

6.3.2 ITIL-Teilkonzepte

Die OGC hat ITIL verschiedene Teilbereiche aufgeteilt, von denen einige noch nicht vollständig sind ([BKP02]).
Alle in ITIL veröffentlichten Aspekte stellen nur Handlungsempfehlungen dar und beschreiben die Vorteile und Fallstricke bei einer Realisierung; wie dies in der Praxis erfolgt, ist Angelegenheit der einsetzenden Organisation. Im Folgenden werden die einzelnen Grobteilgebiete kurz vorgestellt und die einzelnen Problemfelder genannt. Im den nächsten Unterkapiteln erfolgt jeweils eine genauere Definition (sofern bei VoIP besonders relevant) und Empfehlungen beim Einsatz von VoIP.
In ITIL sind folgende Oberpunkte definiert ([OGC00]):

- Die geschäftliche Perspektive (The Business Perspective)
- Planung und Lieferung von IT-Services (Service Delivery)
- Unterstützung und Betrieb der IT-Services (Service Support)
- Management der Infrastruktur (ICT Infrastructure Management)
- Anwendungsmanagement (Applications Management)

6.3.2.1 The Business Perspective

Dieses Themengebiet behandelt Themen, die sich mit dem Verständnis und der Verbesserung von IT-Services als integralem Bestandteil des Managements eines Unternehmens befassen.
Teilbereiche hiervon sind:

- Business Continuity Management
- Partnerships und Outsourcing
- Überleben von Änderungen
- Managing Facilites Management
- Managing Supplier Relationships

6.3.2.2 Service Delivery

Bei Service Delivery sind die Prozesse zur Planung und Lieferung von IT-Services, die das Unternehmen eines Kunden benötigt, sowie die zur Erbringung dieser Services erforderlichen Voraussetzungen und Maßnahmen definiert ([OGC01]).
Hierzu zählen folgende Unterpunkte:

- Service-Level-Management
- Financial Management
- Capacity Management
- Availability Management
- Continuity Management
- Security Management

6.3.2.3 Service Support

In diesem Bereich werden sowohl die Prozesse zur Unterstützung und zum Betrieb der IT-Services als auch der Zugang der Anwender und Kunden zum richtigen IT-Service erläutert. Hierbei werden folgende Themen behandelt ([OGC00]):

- Service-Desk
- Incident Management
- Problem Management
- Configuration Management
- Change Management
- Release Management

Die Veröffentlichungen zu Service Delivery und Service Support sind in einer neuen, detaillierteren Version erschienen und werden daher derzeit als Hauptbestandteile von ITIL betrachtet. Abbildung 6.3 verdeutlicht nochmals die Prozesse der Teilbereiche Service Delivery und Service Support.

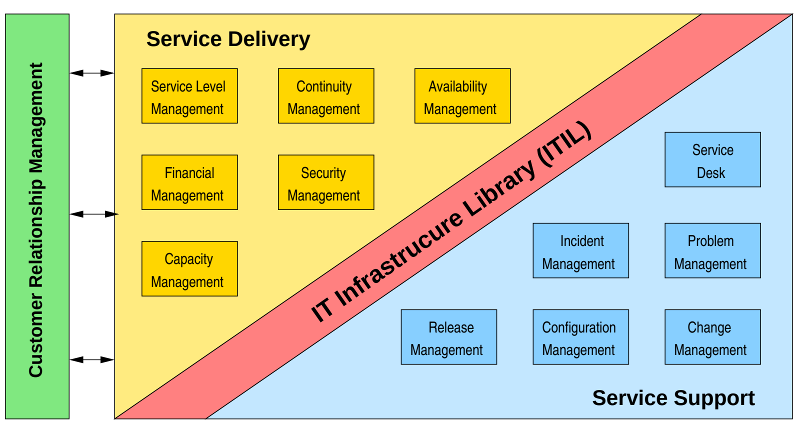

Abbildung 6.3: Aufteilung und Prozesse von ITIL

6.3.2.4 ICT Infrastructure Management

IT Infrastructure Management behandelt Fragestellungen, die sich mit dem Management großer (u.U. komplexer) Infrastrukturen beschäftigen; dieser Bereich ist noch nicht komplett veröffentlicht.
Unterpunkte hiervon sind ([OGC02]):

- Network Services Management
- Operations Management
- Management of Local Processors
- Computer Installation and Acceptance
- Systems Management

6.3.2.5 Applications Management

Applications Management beschäftigt sich mit dem Management des Software-Lebenszyklusses, insbesondere Software Lifecycle Support und Test ([BKP02].
Teilbereiche hiervon bestehen in:

- Software Lifecycle Support
- Testing an IT Service for Operational User

Der Lebenszyklus eines jeden Systems besteht aus den Phasen Planung/Design, Installation/Inbetriebnahme, laufender Betrieb und Abbau.
Da die in einer Phase getroffenen Entscheidungen und Festlegungen sehr viele Implikationen für die anderen Phasen im Zyklus hervorrufen, erfolgt im Managementkonzept eine Betrachtung der für VoIP relevanten Aspekte getrennt nach den einzelnen Phasen.

6.4 Allgemeines

In den folgenden Abschnitten werden – basierend auf den ITIL-Prozessen – Grundsätze für das Managementkonzept aufgestellt. Jeder Prozeß ist grundsätzlich in die Abschnitte Begriffsdefinitionen, Zielsetzung des Prozesses, allgemeiner Prozeßaufbau und Aktivitäten (mit Prozeßsteuerung), die auf [BKP02], [ITSM04], [OGC00], [OGC01] und [OGC02] basieren, und spezifischen Aktivitäten beim Einsatz von VoIP-Systemen aufgeteilt.
Bei den Abbildungen, die die Prozesse bzw. Prozeßabläufe illustrieren sollen, werden – soweit anwendbar – Farbschema und Symbole verwendet, wie in Abbildung 6.4 dargestellt. Zusätzlich werden in eigenen

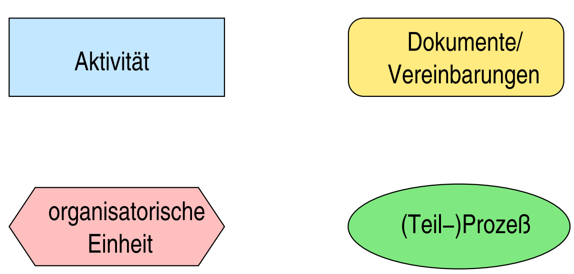

Abbildung 6.4: Farbschema und Symbole

Unterkapiteln nochmals die relevanten Aspekte für Design/Planung und den laufenden Betrieb zusammengefaßt.

Die Steuerung aller Prozesse besteht in zyklischen Berichten an die Geschäftsleitung bzw. das Management, die die relevanten Daten und Leistungsindikatoren der Prozesse beinhalten; bei den Prozessen werden daher nur die Leistungsindikatoren genannt, falls sich diese nicht sowieso aus der Natur des Prozesses ergeben.
Vorab wird eine Empfehlung für die Aufbauorganisation für den Bereich VoIP gegeben.
Bisher sind in den meisten Unternehmen die Bereiche Telekommunikation und allgemeine IT/Netzplanung- und Netzmanagement organisatorisch getrennt.
Wie bereits ausgeführt, bedeutet VoIP das Zusammenwachsen von Sprach- und Datenkommunikation. Um Synergieeffekte aus der gemeinsamen Nutzung und Verwaltung der Netzinfrastruktur ziehen zu können, sollten die beiden Bereiche ineinander integriert werden und gemeinsam für VoIP und Netzinfrastrukturen verantwortlich sein.
Grundlagen für diese Empfehlung sind

- verringerter Informationsfluß zwischen den Organisationseinheiten, da bei einer Integration viele Abläufe vom selben Mitarbeiter erledigt werden können
- gesteigertes Verantwortungsbewußtsein, da bei einer Trennung der beiden Bereiche viele Reibungsverluste entstehen können und ein „Hin- und Herschieben" der Verantwortlichkeiten bei Problemen und Fehlern möglich ist („Ich bin nicht schuld, die anderen sind es"). Durch die Konzetration der Aufgaben in einer Organisationseinheit ergibt sich so eine Verantwortung, die in einer Hand liegt und die Mitarbeiter anspornt.
- die sog. „economies of scale", d.h. Kostendegression durch Skaleneffekte; dies bedeutet, daß bei Produktion größerer Stückzahlen durch die Fixkostendegression die Stückkosten sinken (bei doppelter Produktionsmenge sind die Stückkosten nicht gleich hoch, sondern sie fallen hyperbelartig)
- der sog. „Erfahrungskurveneffekt", d.h. je länger eine Tätigkeit ausgeübt wird, desto mehr ergeben sich Rationalisierungseffekte und Zeitgewinne durch verbesserte Herstellungstechniken, verbesserte Prozeßabläufe, …

6.5 Design und Planung

Die Phase Design/Planung besteht in der Grundsatzentscheidung und der Grundkonzeption für den Einsatz eines VoIP-Systems. Hierbei sind v.a. folgende Dinge von Bedeutung:

- Network-Services-Management
- Service-Level-Management
- Finance-Management
- Capacity-Management
- Availability-Management
- Security-Management
- Continuity-Management

In den folgenden Abschnitten werden diese Prozesse dargestellt.

6.5.1 Network-Services-Management

Der Prozeß des Network-Services-Management ist in den Service-Delivery-Prozessen von ITIL eigentlich nicht enthalten; er wird in einem separaten Werk behandelt („ICT Infrastructure Management", siehe [OGC02]). Da das Design und die Planung des Kommunikationsnetzes bei VoIP-Systemen eine große Bedeutung hat, wird der Prozeß hier kurz vorgestellt.

6.5.1.1 Zielsetzung und Prozeß

Der Prozeß des Network-Services-Management konzentriert sich auf die Planung und Steuerung von Kommunikationsnetzwerken, zu denen auch Telefonsysteme, LAN- und WAN-Netzwerke zählen. Das Network- Services-Management beschäftigt sich des weiteren mit den langfristigen Kommunikationsbedürfnissen des Unternehmens und arbeitet mit dem Capacity-Management zusammen ([OGC02]).

6.5.1.2 Aktivitäten bei VoIP

Beim Einsatz von VoIP-Systemen spielt der Prozeß des Network-Service-Managements eine bedeutende, wenn nicht sogar die zentrale Rolle, da, wie im Anforderungskatalog erläutert, die Aspekte Sprachqualität, Verfügbarkeit und unterstützte Dienste/Leistungsmerkmale (siehe Abschnitte 4.1.1, und 4.1.3 und 4.1.4) die zentralen Knackpunkte für das ordnungsgemäße Funktionieren von VoIP-Systemen – und die damit zusammenhängende Akzeptanz durch die Anwender und Nutzer – darstellen. Um diese Punkte erfüllen zu können, sind die Aktivitäten des Network-Service-Managements in Bandbreitenplanung, Netzdesign, Routing- sowie Berechtigungs-/Leistungsmerkmalkonezpte unterteilt.

- **Bandbreitenplanung**:
  Die Bandbreitenplanung wird im Rahmen des Capacity-Managements (siehe Abschnitt 6.5.4.4) durchgeführt; daher erfolgt an dieser Stelle keine Erläuterung.

- **Netzdesign:**

  – des IP-Netzes:
    Zentrale Fragestellung ist hierbei der logische Aufbau der Netzstruktur, der Folgewirkungen auf viele andere managementrelevante Teilbereiche hat (wie z.B. Security Management). Bei einem VoIP-System existieren, wie Kapitel 5.3 aufgezeigt hat, drei logisch getrennte Systeme:

    * Teilnetz mit den Zentralkomponenten
    * Teilnetz mit den VoIP-Endgeräten
    * Teilnetz für den sonstigen Datenverkehr

    Für das Netzdesign stellt sich die Frage, wie diese Subsysteme logisch in die Netzinfrastruktur zu implementieren sind.
    Eine Lösungsmöglichkeit besteht in der Bildung eines logischen Netzes für alle drei Subsysteme, d.h. alle sind in einem logischen LAN-Segment angesiedelt und haben denselben IP-Adreßbereich. Eine andere Lösungsmöglichkeit ist die logische Trennung durch die Bildung von „Virtual LAN´s“ (VLAN´s), d.h. die Teilsysteme können phsyisch im selben LAN-Segment angesiedelt sein (was in der Praxis aufgrund der räumlichen Unternehmensgröße fast unmöglich ist), haben aber jeweils verschiedene Adreßbereiche. Dies würde die Bildung von mindestens drei VLAN´s bedeuten:

    * ein VLAN für die Zentralkomponenten
    * mindestens ein VLAN für die VoIP-Endgeräte
    * mindestens ein VLAN für den sonstigen Datenverkehr

    Um die Vorteile und Notwendigkeit einer Aufteilung in verschiedene VLAN´s aufzeigen zu können, ist es zuerst notwendig, aufzuzählen, welche Konfigurationsdaten ein VoIP-Endgerät üblicherweise benötigt:

    1. IP-Adressdaten (IP-Adresse, Netzmaske, Gateway)
    2. IP-Adresse des Gatekeepers
    3. IP-Adresse von TFTP-/FTP-Server für Softwareupdates

4. VLAN-ID für getaggtes VLAN
5. Daten für Quality-of-Service-Architektur

Diese Daten können selbstverständlich per Hand an jedem VoIP-Telefon eingegeben werden; zeit- und kostensparend ist dies nicht.
Daher ist es erstrebenswert, möglichst viele dieser Daten automatisiert zu erhalten. Hierfür bietet sich DHCP an (Dynamic Host Configuration Protocol); Ziffer 1 ist per Definition von DHCP zu übermitteln; die Ziffern 2-4 können über spezielle Optionen übergeben werden (z.B. Option 43 – Vendor Specific Info oder ab Option 150, die Bootserver und damit zusammenhängende Parameter beinhalten).
Mit der Nutzung von DHCP ergibt sich somit ein sehr gewichtiger Grund für die Aufteilung in mehrere VLAN´s: Zur Automatisierung der Konfiguration der VoIP-Endgeräte ist DHCP unerläßlich. Hierbei werden spezielle Option benötigt; diese Optionen werden auch im sonstigen Netz (z.B. für den Bootvorgang von Rechnern) verwendet. Um hier keine Konflikte zu erzeugen, ist ein separates VLAN für die Endgeräte erforderlich. Somit scheidet die Lösungsmöglichkeit der manuellen Eingabe aus (sie ist allenfalls für kleine VoIP-Implementierungen geeignet).
Weitere Aspekte für die Aufteilung in verschiedene VLAN sind Verkehrsseparierung (z.B. Sicherstellung einer akzeptablen Sprachqualität – siehe Kapitel 4.1.1), Management- (bereits getrennte Datenströme) und Sicherheitsaspekte, die in 6.5.6 erläutert werden.
Zusammengefaßt sollte daher das Netzdesign aus getrennten VLAN´s für die Zentralkomponenten, VoIP-Endgeräte und den sonstigen Datenverkehr bestehen. Überdies kann so das in Kapitel 5.6 vorgestellte Konzept von „One-wire-to-the-desk“ mit Verkehrstrennung realisiert werden.

– des konventionellen Netzes:
Sollten (v.a. in Migrations- oder Hybridszenarien bzw. Anbindung an das PSTN) TK-/VoIP-Systeme noch mit TDM-basierten Strecken (S_0 bzw. S_{2M} vernetzt werden (u.a. in Firmenverbundnetzen, siehe Abschnitt 3.2.6.2), sind aufgrund der bei der Bandbreitenplanung (Abschnitt 6.5.4.4) ermittelten Werte die entsprechende Anzahl an S_0 bzw. S_{2M}-Strecken zur Verfügung zu stellen.

– Signalisierung (D-Kanal-Protokoll):
Für die Vernetzungsstrecken und die Anbindung an das PSTN (IP oder konventionell) hat daneben die Wahl des Signalisierungsprotokolls (hier v.a. die Prüfung der Konformität mit Systemen verschiedener Hersteller) eine große Bedeutung, da hiervon die Anzahl der möglichen Leistungsmerkmale (z.B. Namensanzeige) abhängt. Standard ist, wie in Abschnitt 3.2.5.1 vorgestellt, das Q.931/DSS1-Protokoll (es wird sowohl für konventionelle als IP-basierte (H.323 bzw. SIP, siehe Abschnitte 3.3.1.2 und 3.3.2) Verbindungen verwendet.
In Verbundnetzen ist dies aber meist – wegen der Erwartungen der Anwender, die erweiterte Leistungsmerkmale bei konventioneller Technik seit Jahren gewöhnt sind – nicht ausreichend. Daher ist sowohl auf konventionellen als auch IP-basierten Strecken Q.SIG (Abschnitt 3.2.5.2) einzusetzen, um diese Anforderung umsetzen (dies ist wegen der zahlreichen Q.SIG-Implementierungen der Hersteller – die mitunter auch nicht alle Leistungsmerkmale implementiert haben – nicht immer möglich). Daher ist, soweit es die Betrachtungen des Finance-Managements (Abschnitt 6.5.3) erlauben – die Herstellerauswahl auf diejenigen einzugrenzen, die eine Vielzahl an Q.SIG-Leistungsmerkmalen bieten.

- **Routingkonzept (LCR)**:
Im Routingkonzept ist festzulegen, wohin die Gespräche (sowohl abgehend als ankommend) geleitet werden sollen. Die Aktivität ist bei konventionellen als auch bei IP-basierten Verbindungen gleich. Im Routing- bzw. LCR-Konzept ist unter dem Aspekt der Kostenminimierung zu entscheiden, auf welches Interface des VoIP-Systems die Gespräche gelenkt werden; dabei sind sowohl der Erstweg als auch für den Ausfall des Erstwegs alternative Routen zu planen. Hierzu ein Beispiele: In firmeninternen Verbundnetzen sind Gespräche an andere Standorte primär über die eigenen Vernet-

zungsstrecken zu leiten; bei Ausfall der für die Verbindung benötigten Strecke ist das Gespräch über das PSTN zu leiten.
Dieses LCR-Konzept ist in die TK-/VoIP-Systeme einzupflegen (im Rahmen der Inbetriebnahme) und ständig zu warten (im Rahmen des Change- bzw. Release-Managements).

- **Berechtigungs- und Leistungsmerkmalkonzept:**
  Hierbei ist zu definieren, welche Nummern von den Anwendern direkt (z.B. ohne Einschaltung der Telefonvermittlung) gewählt werden dürfen (Berechtigungskonzept) und welche Leistungsmerkmale den Anwendern zur Verfügung stehen. Beispiele: Mitarbeiterkreis A darf weltweit telefonieren, Mitarbeiterkreis B nur national; A darf Anrufe zu externen Zielen (u.a. Handys) umleiten (hierbei sind aber die Gefahren des „Breakthrough“ zu bedenken, siehe 6.5.6.4), B nicht.

6.5.2 Service-Level-Management

6.5.2.1 Begriffsdefinitionen

IT-Service: Bereitstellung eines oder mehrerer technischer Systeme, um Geschäftsprozesse zu ermöglichen oder diese zu unterstützen.

Kunde: Vertreter einer Organisation bzw. einer Organisationseinheit (das einsetzende Unternehmen), der zum Vertragsabschluß über die Inanspruchnahme von Dienstleistungen bzw. Services befugt ist. Der Kunde ist also in der Regel *nicht* der (End-)Anwender.

Dienstleister: Anbieter der Services und Vertragspartner des Kunden. Der Dienstleister kann hierbei sowohl im Unternehmen (z.B. unternehmenseigene IT-Abteilung) als auch extern angesiedelt sein.

Service-Anforderungen: Die Service-Level-Requirements (SLR) beschreiben die Anforderungen des Kunden und dienen als Grundlage für die Vereinbarung im SLA.

Service-Katalog: Verzeichnis aller Angebote (Sevices) einer IT-Organisation.

Service-Level-Agreement: Vertrag zwischen Dienstleister und Kunden über den zu leistenden IT-Service; es unterhält unter anderem Vereinbarungen über die zu leistende Qualität, Vertragsdauer, beiderseitige Rechte und Pflichten sowie Kosten und wird nicht-technisch abgefaßt.

Service-Spezifikationen: Beschreibung der technischen Umsetzung der Service-Level-Agreements und den sich daraus ergebenden Folgerungen für den Dienstleister (wie erforderliche Ressourcen, Personal, . . .).

Operational-Level-Agreement: Vereinbarung mit einer *internen* Abteilung über die Erbringung von einem benötigten (Teil)-Service; diese Vereinbarung stellt keinen Vertrag im juristischen Sinn dar.

Underpinning-Contract: Vertrag mit *Externem* über die Erbringung von einem benötigten (Teil)-Service.

Service Quality Plan: Planung nebst Spezifikation interner Ziele, das alle Managementinformation zur Steuerung der IT-Organisation sowie die Parameter für das operative Management und die Service-Management-Prozesse enthält (z.B. Lösungszeiten im Incident-Management).

Abbildung 6.5 illustriert diese Begriffe sowie die Beziehungen untereinander.

6.5.2.2 Zielsetzung

Die Zielsetzung des Service-Level-Managements ist die Pflege und ständige Verbesserung der mit dem Kunden vereinbarten Dienste. Hierzu trifft es Vereinbarungen hinsichtlich der Leistungen der IT-Organisation (und vertritt sie somit gegenüber dem Kunden), überwacht und dokumentiert Leistungen

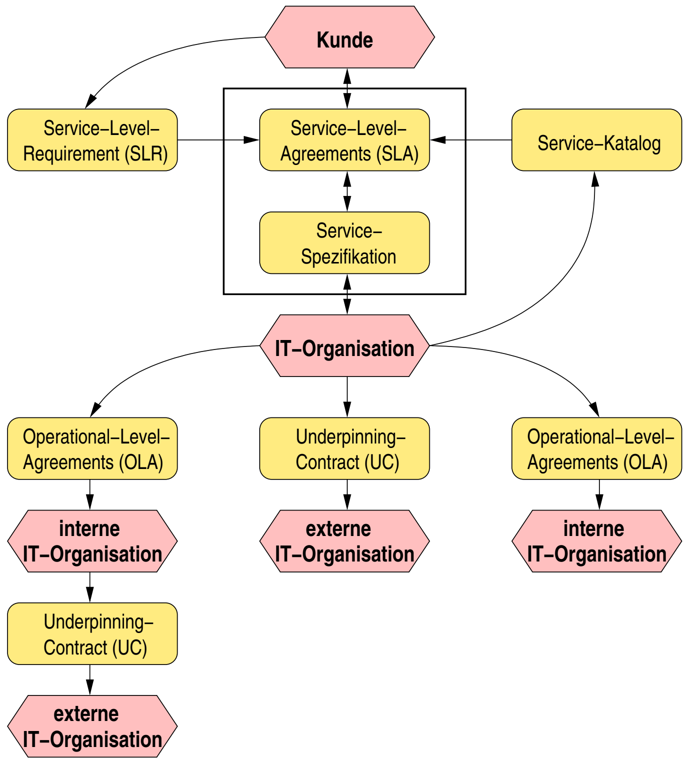

Abbildung 6.5: Grundbegriffe des Service-Level-Managements

([BKP02]). So wird eine gute Geschäftsbeziehung dem Kunden und Dienstleister ermöglicht, was als Folge die Zufriedenheit des Kunden erhöht. Außerdem ist somit die Leistung der IT-Organisation meßbar und führt zu einer besseren Kostentransparenz (sowohl intern als auch zum Kunden).

6.5.2.3 Prozeß

Das Service-Level-Management dient als Brücke zwischen dem Kunden und Dienstleister. Der Prozeß dokumentiert die Dienste in einer für den Kunden verständlichen Sprache und sorgt für eine Integration der Komponenten, aus denen der Service besteht ([OGC01]).
Das Service-Level-Management hat eine Schlüsselrolle innerhalb der Service-Managementprozesse inne und unterhält enge Beziehungen zu den sonstigen Delivery- und Supportprozessen. In seiner verbindenden Funktion führt es Gespräche mit dem Kunden über dessen Anforderungen, wobei es nicht die technischen Aspekte in den Vordergrund stellt. Die IT-Organisation übertragt diese Anforderungen anschließend in technische Spezifikationen und organisatorische Abläufe. Der Erfolg hängt davon ab, ob die technische Umsetzung und damit die erbrachten Dienste den Anforderungen entsprechen. Die Aufgaben des Service-Level-Managements bestehen in (Abbildung 6.6 illustriert den Prozeßaufbau sowie die Abhängigkeiten graphisch):

- Identifizierung der Kundenbedürfnisse und Beziehungspflege
- Definition der zu erbringenden Services durch Ausrichtung auf Kundenwünsche und -bedürfnisse sowie Festlegung in SLR´s sowie Service-Spezifikationen und Erstellung eines Service-Katalogs und Service-Quality-PLans.
- Verhandlung mit dem Kunden in Hinblick auf die gewünschten Dienste, Leistungsumfang und Kosten sowie Fixierung in SLA´s (als Konsequenz für den Dienstleister ergibt sich u.a. der Abschluß von OLA´s und UC´s).

- Überwachung (Monitoring) der in den SLA´s definierten Kriterien sowie Dokumentation der Ergebnisse.
- Erstellung von Berichten aus den dokumentierten Ergebnissen und Vorlage der Berichte beim Kunden
- Auswertung der Berichte in Zusammenarbeit mit dem Kunden und evtl. Veranlassen von Änderungen bei Nichteinhaltung der SLA´s; außerdem Erfahrungsaustausch mit dem Kunden hinsichlich Anregungen, Veränderungswünschen oder sonstigen Diskussionspunkten.

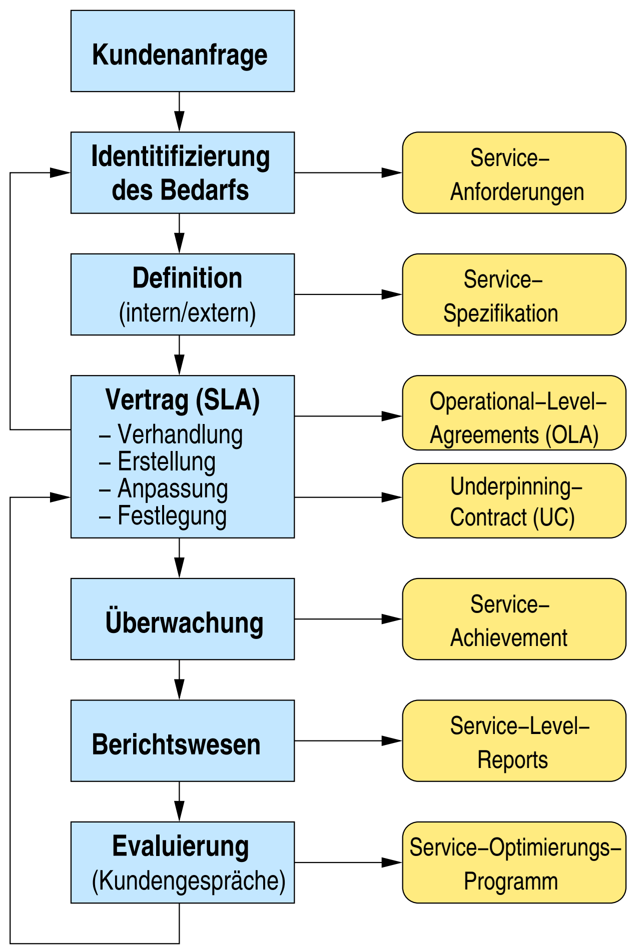

Abbildung 6.6: Prozeß des Service-Level-Managements

Alle Prozesse und Funktionen haben als oberstes Ziel die Erbringung qualitativ hochwertiger Leistungen für den Kunden. Daher ist das Service-Level-Management der Dreh- und Angelpunkt für diese Prozesse, wobei es einerseits von diesen Prozessen Informationen erhält, die für die SLA´s von Bedeutung sind (z.B. Kostenrechung vom Finance-Management) und andererseits Vorgaben für die Diensterbringung der einzelnen Prozesse aufstellt (z.B. Verfügbarkeitsanforderungen für das Availability-Management oder Reaktionszeiten für den Service-Desk bzw. Incident-Management). Eine genaue Aufzählung dieser Beziehungen entfällt hier, da sie bei den einzelnen Prozessen bereits erfolgt.

6.5.2.4 Aktivitäten bei VoIP

Bezogen auf den Dienst VoIP werden die in der Prozeßbeschreibung erläuterten Schritte im Folgenden spezifiziert:

- Identifizierung der Kundenbedürfnisse:
  Für den Dienst VoIP bestehen die Kundenbedürfnisse in der Aufrechterhaltung und den Betrieb von Sprachkommunikationsdiensten mittels VoIP-basierten Systemen. Die abstrakten (qualitativen) Anforderungen hierfür ergeben sich aus dem Anforderungskatalog für VoIP-Systeme, wie er in Kapitel 4.1 vorgestellt wurde.

- interne Definition der Anforderungen und Erstellung einer Service-Spezifikation unter Berücksichtigung der Kundenbedürfnisse: Dieser Teilaspekt stellt den Entwurfsvorgang (auch in technischer Hinsicht) für ein VoIP-System dar; hierbei ist zu berücksichtigen, welche externen und internen Dienstleister benötigt werden und welche Qualitätsanforderung diese erbringen können, da nur aufgrund dieser Angaben eigene Zusicherungen gegenüber dem Kunden eingegangen werden können.
  Zentrale Anforderung an ein VoIP-System besteht in der Verfügbarkeit (und damit indirekt auch an einer guten/akzeptablen Sprachqualität, da eine schlechte Sprachqualität die Nichtverfügbarkeit impliziert). Relevante Aspekte zur Sicherstellung einer hohen Verfügbarkeit sind u.a. in den Kapiteln Availability-Management (6.5.5.4) und Security-Management 6.5.6.4) erläutert. Der wichtigste Punkt ist aber die Ermittlung des Maßes an Verfügbarkeit, das dem Kunden garantiert werden kann. Grenze sind hierbei die Garantien, die von Internen oder Externen gegeben werden können (bei VoIP sind hierbei die Carrier – die eine Verbindung in das PSTN herstellen oder Vernetzungsstrecken zwischen TK-/VoIP-Systemen bereitstellen – sowie der Bereich, der für die Aufrechterhaltung des Datennetzes zuständig ist und andere Externe wie Stromlieferanten, etc.).
  Abgeleitet von der Verfügbarkeit sind die Teilgebiete Reaktions- und Wiederherstellungszeiten im Fehlerfall.
  Aus den so erhaltenen Erkenntnissen werden Service-Spezifikationen erstellt, die die Anforderungen des Kunden und die Konsequenzen für die interne Organisation enthalten. Diese Aktivitäten sind unternehmensabhängig, daher kann hier keine konkrete Aussage gemacht werden.

- Verhandlung und Erstellung des SLA mit dem Kunden:
  Auf Grundlage der intern ermittelten Service-Spezifikationen werden diese Daten dem Kunden vorgestellt und ein SLA ausgehandelt.
  Bei VoIP enthält ein SLA u.a. folgende Punkte:
  - allgemeine Daten über den Kunden (Größe, räumliche Gegebenheiten, ...)
  - allgemeine (qualitative) Dienstbeschreibung
  - quantitative Beschreibungen und Meßverfahren
    - Verfügbarkeitszeiten: rund um die Uhr
    - Festlegung eines Verfügbarkeitsniveaus
    - Sprachqualität (MOS)
    - Servicezeiten
    - Störungsdefinitionen
    - Reaktionszeiten
  - Berichtsdefinitionen und Erstellungszyklen
  - Kosten

  Die vereinbarten Parameter hängen fast ausschließlich von den Kosten ab, die der Kunde zu zahlen bereit ist; ein Verfügbarkeitsniveau von unter 99% und ein MOS von unter 4 sollte mit dem Kunden aber nicht abgeschlossen werden, da der Kunde sonst u.U. nicht zufriedengestellt werden kann (1% Nichtverfügbarkeit bedeutet 3,65 Tage im Jahr Ausfall oder Beeinträchtigungen!).
  In Abhängigkeit von den vereinbarten Werten sind schließlich OLA´s und UC´s (intern bzw. extern) zu vereinbaren.

Die folgende Tabelle 6.1 gibt ein SLA für den Dienst VoIP beispielhaft an, wobei hier nur die wichtigsten Parameter vorgestellt werden (die Werte sind ambitioniert, aber nur so kann ein VoIP-System auf ähnlichem Niveau wie ein klassisches TK-System betrieben werden).

Name	**Beschreibung/Wert**
Sprachqualität:	MOS $>= 4,0$
Verfügbarkeit:	Funktionsfähigkeit (Gesprächswunsch erfüllbar) sowie akzeptable Sprachqualität und Ausfall von weniger als 10% der Teilnehmer
Verfügbarkeitszeiten des Dienstes:	rund um die Uhr
Verfügbarkeitsniveau:	99,5% (Verhältnis von tatsächlicher Verfügbarkeit zu der prinzipiell möglichen Verfügbarkeitszeit; Bestimmung wochen-, monats- und jahresbezogen)
Datenquellen zur Ermittlung der Verfügbarkeit:	Logfiles der Systeme, ...
Servicezeiten (des Service-Desks):	Mo. - Fr. 7 - 17 Uhr
Störungsdefinitionen:	
Teilnehmerausfall:	Ausfall oder Störung eines Teilnehmers
kleine Störung:	Ausfall von weniger als 10% der Teilnehmer oder Ausfall von Teilen des Datennetzes sowie von Vernetzungsstrecken sowie der Anbindung an das PSTN, wobei alle Gesprächswünsche weiterhin erfüllt werden können (z.B. durch anderes Routing)
schwerwiegende Störung:	Ausfall von mehr als 10% der Teilnehmer sowie Ausfall von Teilen des Datennetzes oder von Vernetzungsstrecken sowie der Anbindung an das PSTN, was dazu führt, daß Gesprächswünsche nicht erfüllt werden können
Totalausfall:	Ausfall des Gesamtsystems (Zentralkomponenten), Datennetz, Vernetzungsstrecken oder Anbindung an das PSTN
Reaktionszeiten:	
Totalausfall:	Reaktionszeit: 15 Min., Behebungszeit: 2 Stunden
schwerwiegende Störung:	Reaktionszeit: 30 Min., Behebungszeit: 4 Stunden
kleine Störung:	Reaktionszeit: 1 Stunde, Behebungszeit: 8 Stunden
Teilnehmerausfall:	Reaktionszeit: 2 Stunden, Behebungszeit: 1 Tag

Tabelle 6.1: Beispiel-SLA für VoIP

- Überwachung:
  Für die Überwachung der Einhaltung des SLA sind die Überwachungsverfahren und Methoden zu vereinbaren; die Daten kommen aus den Überwachungsteilprozessen des Availability- (Kapitel 6.5.5.5), Capacity- (Kapitel 6.5.4.5) und dem Incident-Management (Kapitel 6.5.5.5).

- Berichtswesen und Kundengespräche:
  Aus den Überwachungsinformationen sind die im SLA vereinbarten Berichte turnmusmäßig zu erstellen und dem Kunden vorzulegen, zu erläutern und mit ihm zu besprechen, wobei die Berichte die vereinbarten Service-Levels mit den tatsächlich erreichten vergleichen.

- Änderungsmanagement:

In Abhängigkeit von der Erreichung der vereinbarten Service-Levels sind die Vereinbarungen im SLA anzupassen oder Reaktionen des Dienstleisters zu erbringen.

6.5.3 Finance-Management

6.5.3.1 Begriffsdefinitionen

Um die weiteren Abschnitte verstehen zu können, ist zuerst eine Defintion verschiedener betriebswirtschaftlicher Begriffe notwendig.

Kostenträger: konkretes Produkt oder Dienstleistung, dem Kosten zugeordnet werden (z.B. Audi A6); die Kostenträgerrechnung ist u.a. Grundlage für die Bestimmung der Angebotspreise.

Kostenstelle: abgegrenzter Teilbereich der Aufbauorganisation, der für einen/mehrere Kostenträger Leistungen erbringt; die Kostenstellenrechnung ist eine Aufteilung von Kosten auf Kostenstellen, um für bestimmte Teilbereiche der betrieblichen Leistungserbringung jeweils die anfallenden Kosten zu ermitteln.

Kostenkategorien: Alle Kosten lassen sich in verschiedene Kategorien unterteilen, wobei hier jeweils ein anderes Hauptaugenmerk auf einen bestimmten Aspekt gelegt wird ([WIL00]):

- nach der Entstehung:
  - direkte Kosten: Kosten, die einem Kostenträger bzw. einer Kostenstelle direkt zugeordnet werden können.
  - indirekte Kosten: Kosten, die den verursachenden Kostenträgern bzw. Kostenstellen nicht direkt, sondern über einen Schlüssel zugeordnet werden.
- nach dem Leistungsvolumen:
  - fixe Kosten: Kosten, die verbrauchsunabhängig anfallen
  - variable Kosten: Kosten, die stückzahlabhängig anfallen
- nach Kostenarten (Art der verbrauchten Produktionsfaktoren):
  - Personalkosten
  - Materialkosten
  - Dienstleistungskosten
  - Abgaben
  - kalkulatorische Kosten (Zinsen, Abgaben, Unternehmerlohn)

6.5.3.2 Zielsetzung

Das Finance Management dient zur Sichtbarmachung aller Kosten, die für die Erbringung eines Dienstes anfallen. Hierzu ist eine vollständige Erfassung aller Kosten sowie eine Zuordnung zu den jeweiligen Kostenstellen und Kostenträgern erforderlich. Die so erhaltenen Daten sind für die Unternehmensleitung Grundlage der Entscheidungsfindung und dienen gleichzeitig zur Ermittlung der Kostentreiber und so zu wirtschaftlichem Arbeiten ([OGC01].
Ein effektives Finanzmanagement sollte daher folgende Ziele erfüllen:

- Unterstützung des Managements bei der Erstellung einer Investitionsstrategie sowie der Entscheidungsfindung
- Kostenmanagement und -kontrolle für sämtliche Mittel

- Flexibilität (d.h. auch Berücksichtigung sich ändernder Technologien und Prozesse).

Zur Abdeckung der in Kapitel 6.1 vorgestellten Grundsätze der mittel-/langfristigen sowie kurzfristigen Planung sowie der genannten Ziele erfolgt eine Unterteilung in drei Teilbereiche ([BKP02]):

- **Finanzplanung**: Die Finanzplanung (Budget) betrifft die Kostenvorhersage (Prognose anhand von Kundenanforderungen) und das Ausgabenmanagement (Schätzung aus Erfahrungswerten). Hierbei erfolgt auch eine Vorhersage über die gesamte Zahlungsreihe und die Gesamtkosten eines Systems/eines Dienstes. Dieser Aspekt deckt somit die langfristige Planung ab.

- **Kostenrechnung**: Die Kostenrechnung bezieht sich auf Aktivitäten, die den finanziellen Aspekt abdecken; hierbei geht es um die Bestimmung der Kosten pro Einheit (z.B. Stückkosten). Hierbei wird die Kostenträgerrechnung durchgeführt, die kurzfristiger Natur ist.

- **Leistungsverrechnung**: Unter Leistungsverrechnung werden alle erforderlichen Aktivitäten zusammengefaßt, um die Abrechnung (z.B. gegenüber Kunden) sicherzustellen. Dies betrifft somit das in 6.2.4 vorgestellte Accountingmanagement. Hierbei erfolgt die Verrechnung der Kosten- und Leistungen auf die Kostenstellen.

6.5.3.3 Prozeß

Die folgende Abbildung 6.7 stellt den grundsätzlichen Prozeßablauf des Finance Managements dar. Dabei sind alle in 6.5.3.2 genannten Teilbereiche integriert. Dabei stellen die Teilbereiche einen immerwährenden

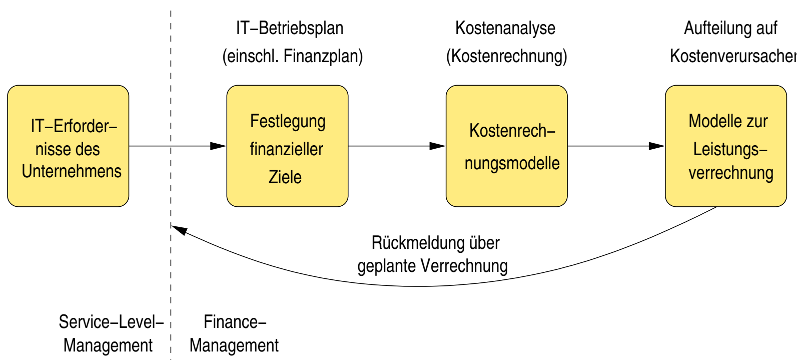

Abbildung 6.7: Prozeß des Finance-Managements

Kreislauf dar ([BKP02]):
Zuerst können nur aufgrund von Schätzungen ungefähre Aussagen bei der Finanzplanung getroffen werden. Diese sind natürlich nicht genau.
Durch die im Laufe des Lebenszyklus eines Produkts/Dienstes aus der Kosten- und Leistungsverrechnung gewonnen Daten ist es möglich, eine immer genauere Verrechnung durchführen zu können und außerdem detaillierte Daten für die weitere Finanzplanung des Dienstes bzw. für folgende Entwicklungen zu erhalten.
Beziehungen zu anderen Prozessen:

- Beziehung zum Service-Level-Management: In den SLA´s sind die zwischen Kunden und IT-Organisation vereinbarten Services (nebst diversen Parametern wie z.B. Verfügbarkeit) niedergelegt. Diese Parameter und Vereinbarungen haben einen großen Einfluß auf die Höhe der Kosten und Aufwendungen, die für einen vertragsgemäßen Betrieb erforderlich sind. Somit ist ein ständiger Austausch zwischen Service-Level-Management und Finance Management erforderlich.

- Beziehung zum Capacity-Management: Das Capacity Management stellt sicher, daß die vorgehaltenen Ressourcen den Anforderungen des Kunden entsprechen und kostengünstig zur Verfügung gestellt werden. Informationen über die Kosten werden im Rahmen der Kapazitätsplanung und Verfügbarkeit ermittelt.

- Beziehung zum Configuration-Management: Das Configuration-Management spezifiziert, identifiziert und erfaßt Veränderungen an allen Infrastrukturkomponenten. Der Einsatz der CMDB als Datensammlung (die auch die Daten über die Kosten enthält) vereinfacht die Verwendung von historischen Informationen über die Kosten. Außerdem ermöglicht das Configuration-Management die korrekte Darstellung von Informationen über Vermögenswerte.

6.5.3.4 Aktivitäten bei VoIP

Im Bereich von VoIP ergeben sich vielfältige Aktivitäten, von denen die wichtigsten beispielhaft vorgestellt werden. Bestimmung von Aufgaben und Begriffszuordnungen:

- Prozeßinhaber: Der Prozeßinhaber des Finance-Managements sollte der Finanzchef bzw. Controller der IT-Organisation sein, da er als einzige Schnittstelle zum Management fungieren und außerdem die Teilprozesse überwachen sollte.
- Kostenträger (und Produkt) bei VoIP ist die „Erbringung von (Sprach-)Kommunikationsleistungen“.
- Die Kostenstellen, auf die die Verrechnung erfolgt, sind die Kostenstellen des einsetzenden Unternehmens, da der VoIP-Teilbereich eine Gemeinkostenstelle darstellt, die Dienstleistungen für den Kunden/das Unternehmen erbringt.

Die Teilprozesse bieten folgende Besonderheiten:

- **Finanzplanung**: Die Finanzplanung umfaßt zwei Bereiche, zum einen die Grundsatzentscheidung zum Einsatz eines VoIP-Systems und zum anderen den Vergleich der Anbieter.
  Bei beiden sind die Gesamtkosten, die aus einmaligen und laufenden Kosten bestehen, zu berücksichtigen. Zur besseren Vergleichbarkeit verschiedener Alternativen sind diese in Zahlungsreihen umzuwandeln, die sich über die gesamte Nutzungsdauer (der Abschreibungszeit) erstreckt (einmalige Kosten werden mit ihren Abschreibungsbeträgen angesetzt); diese Zahlungsreihen werden auf ihren Barwert umgerechnet und schließlich verglichen (Barwertmethode). Diese Methode hat den Vorteil, daß der Zeitfaktor durch die kalkulatorischen Zinsen (daher Umrechnung in einen Barwert) berücksichtigt wird. Der verwendete Zinssatz ist unternehmensabhängig und wird durch die Kapitalkosten bestimmt (diese setzen sich aus den Eigen- und Fremdkapitalkosten zusammen).
  Bei der Grundsatzentscheidung für ein VoIP-System ist zwischen den Kosten eines klassischen Systems und einem VoIP-Systems zu vergleichen. Hierzu zählen:
  - einmalige Kosten: Anschaffungs- und Installationskosten
  - laufende Kosten: Wartungs-, Leitungs-, Gesprächskosten und Kosten, die bei Umzügen und sonstigen Änderungen entstehen (bei VoIP sind diese tendenziell deutlich geringer, da der zeitintensive physische Aspekt fast komplett entfällt) sowie Verwaltungs- und Managementkosten.

  Hierbei können die Gesamtkosten oder die Kosten pro Port (Telefon) angesetzt und verglichen werden (firmenpolitische Präferenzen außer acht gelassen).
  Bei einem Vergleich von Systemen verschiedener Anbieter sind prinzipiell die gleichen Kostenblöcke anzusetzen, wobei hier besonderes Augenmerk auf die Anschaffungs-, Wartungs- und Verwaltungs-/Managementkosten gelegt werden muß, da sich bei den sonstigen Infrastrukturkosten (Datenleitungen, Gesprächskosten) keine Änderungen ergeben.
- **Kostenrechnung**:
  Bei der Kostenrechnung ist ein ständiges Augenmerk besonders auf die laufenden Kosten zu legen; hierbei sollte vor allem ein aktives Provider- und Carriermanagement betrieben werden, d.h. eine ständige Marktbeobachtung und evtl. Wechsel zu anderem Anbieter, da sich in der Carrierbranche häufig Änderungen ergeben (z.B. Datenleitungen sowie Telefon- und VoIP-Tarife). Dies schließt in der Vertragsgestaltung eine möglichst kurze Laufzeit ein, um schnell wechseln zu können.
- **Leistungsverrechnung**:
  Die Leistungsverrechnung stellt ein großes Teilgebiet im Prozeß des Finance-Managements dar. Hier

ist eine Unterscheidung der Kosten in direkte (Kosten, die direkt den Verursachern zugeordnet werden können) sowie in indirekte Kosten (Kosten, die nicht direkt zugeordnet werden können und daher per Verteilungsschlüssel umgelegt werden müssen) zu treffen.
Die direkten Kosten sollten über ein Metering- und Accounting-System, das alle Verbindungen erfaßt, ermittelt werden. Hierbei ist die Unterscheidung zu treffen, welche Gesprächstypen (ankommend/abgehend sowie intern/extern) erfaßt werden und wie die Tarifierung erfolgt.
Zuerst (im Anfangsstadium) sollten nur abgehende Externgespräche aufgezeichnet und berechnet werden, da hierfür konkrete Beträge durch die Carrier vorlegen. Die anderen Typen sind daher den indirekten Kosten zuzurechnen und per Schlüssel umzulegen, wobei hier die Infrastrukturkosten (Mitbenutzung der Datenleitungen und Netzkomponenten sowie Vorrangbehandlung von Datenpaketen durch Einsatz einer Quality-of-Service-Architektur berücksichtigt werden müssen) den größten Anteil ausmachen. Bei zunehmendem Reifegrad des Systems sind auch diese Gespräche zu erfassen und deren Kosten direkt den Verursachern (den einzelnen Teilnehmern) zuzurechen. Hierzu sind Daten anderer Bereiche (wie IT-Infrastrukturmanagement) notwendig, deren Erfassung und Tarifierung einen nicht unerheblichen Aufwand darstellt. Diese Entscheidung sollte in Abhängigkeit vom Aufwand erfolgen (je genauer die Zuordnung, desto mehr Managementoverhead ist erforderlich).
Die Realisierung eines Accouting-Systems wird in Kapitel 7.4.2.4 dargestellt.
Für die Verteilung der indirekten Kosten (z.B. Abschreibung, kalkulatorische Zinsen, ...) ist ein Verteilungsschlüssel zu ermitteln. Am praktikabelsten ist hier die Verrechnung gemäß der Anzahl der genutzten Ports, d.h. wenn ein Kunde 10 von 100 Ports nutzt, werden ihm 10% berechnet.
Die Gesamtkosten pro Verursacher bzw. Port (direkte und indirekte Kosten) werden den Kunden in Rechnung gestellt bzw. im selben Unternehmen auf seiner Kostenstelle und den beteiligten Kostenträgern verrechnet.

6.5.4 Capacity-Management

6.5.4.1 Begriffsdefinitionen

Performance-Management: Messung, Überwachung und Angleichung der Leistung der Komponenten an die Infrastruktur

Application Sizing: Bestimmung der erforderlichen Kapazität (z.B. Hardware oder Netzwerk), um neue oder veränderte Anwendungen zu unterstützen

Modellierung: Vorgehen, anhand von Rechenmodellen die Folgen verschiedener Alternativen für den Einsatz verfügbarer (oder anzuschaffender) Kapazität zu bestimmen (z.B. Berücksichtigung unterschiedlicher Szenarien für Nachfragezunahme von Diensten)

Kapazitätsplanung: Erstellung eines Kapazitätsplans, in dem eine Analyse der aktuellen Situation erfolgt sowie eine Prognose über die künftige Nutzung und die daraus zur Befriedigung der Nachfrageänderung erforderlichen Mittel

6.5.4.2 Zielsetzung

Das Capacity-Management ist aus dem zentralen Element des „Just-in-Time"-Prinzips (siehe Kapitel 6.1), der produktionssynchronen Beschaffung, abgeleitet und hat folglich die Zielsetzung, die *richtigen Kapazitäten* zu *vertretbaren Kosten* entsprechend der *bestehenden und künftigen Bedürfnisse* zum *richtigen Zeitpunkt* zur Verfügung zu stellen ([ITSM04]).
Die Vorteile der Einführung des Capacity-Managements liegen u.a. in

- der Vermeidung von Überkapazitäten, da diese durch vorausschauende Planung und Abstimmung mit dem Kunden auf die zukünftigen Bedürfnisse deutlich reduziert werden können

- der Vermeidung kalkulatorischer Kosten für Zinsen auf Lagerkapazitäten (in Lagerbeständen ist Kapital (meist unnötig) gebunden)
- steigender Effizienz, da Angebot und Nachfrage in einem frühen Stadium aufeinander abgestimmt werden können
- Kosteneinsparungen im Beschaffungsprozeß, da durch die vorausschauende Planung verschiedene Angebote eingeholt werden können und so das preiswerteste ausgewählt werden kann (somit werden Käufe unter Termindruck vermieden, in denen der Anbieter seine Marktmacht ausspielen kann).

6.5.4.3 Prozeß

Der Prozeß des Capacity-Managements besteht aus folgenden Eingangs- und Ausgangsgrößen sowie Subprozessen ([BKP02]):

- Eingangsgrößen: Technologie, Service-Levels, Geschäftspläne, -strategien, -bedarf und -volumen, RfC´s, Verwaltungs-/Überwachungmuster, Projekt-, Finanz-, Implementierungspläne, Störungen und Probleme
- Subprozesse:
  - Business-Capacity-Management: Trendanalyse, Prognose, Modellierung und Dokumentierung der zukünftigen Kundenbedürfnisse
  - Service-Capacity-Management: Überwachung und Analyse, Berichterstattung über Leistung der Services, Nachfrageangleichung
  - Ressource-Capacity-Management: Überwachung und Analyse, Berichterstattung über Komponentennutzung, Überwachungsfestlegung der normalen Nutzung
- Ausgangsgrößen: Kapazitätsplan, Capacity Database, Schwellwerte und Alarme, Kapazitätsberichte, Service-Level-Empfehlung, Kostenverrechnungsempfehlung, Proactive Changes, Serviceverbesserungen, ...

Die Subprozesse werden kurz erläutert:

- **Business-Capacity-Management**: Das Ziel besteht in der Vorhersage der zukünftigen Bedürfnisse und Anforderungen der Kunden; eine solche Prognose kann durch Kundeninformationen oder Trendanalysen erstellt werden; unter Bezugnahme auf die Anforderungen des Kunden oder die Prognosen ist ein Kapazitätsplan zu erstellen und turnusmäßig zu aktualisieren. Das BCM ist proaktiv ausgerichtet und ist eng mit dem Service-Level-Management verbunden (Aushandlung von Servicevereinbarungen).
- **Service-Capacity-Management und Ressouce-Capacity-Management**: Diese Subprozesse umfassen dieselben Aktivitäten, Unterschied ist der jeweilige Schwerpunkt. Das Management der Service-Capacity ist auf die Erbringung von IT-Services ausgerichtet, während sich das Ressource-Capacity-Management auf die Technik konzentriert, die benötigt wird, um die Dienste zu erbringen. Die genannten Aktivitäten sind in Abildung 6.8 dargestellt.
  - **Überwachung (Monitoring)**:
    Die Überwachung beschäftigt sich mit der Verfolgung und Kontrolle verschiedener Komponenten der Infrastruktur (überdies sind Schwellwerte einzurichten, bei deren Über- oder Unterschreitung automatisiert Hinweismeldungen generiert werden).
  - **Analyse**:
    Die erhaltenen Meßdaten sind zu analysieren. Mit Hilfe einer Trendanalyse sind Prognosen über die künftige Nutzung möglich. Aufgrund der Ergebnisse sind Maßnahmen zur Steigerung der Effizienz oder die Beschaffung von zusätzlichen Komponenten einzuleiten.

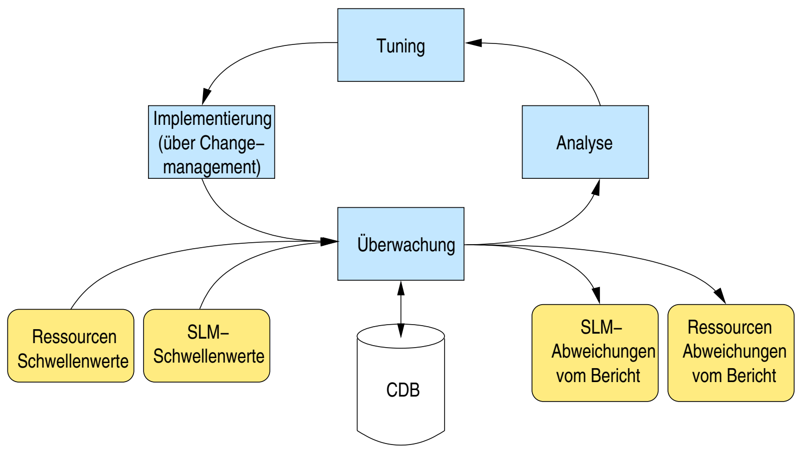

Abbildung 6.8: Management von Ressourcen und Serviceleistung

- **Tuning**:
  Tuning bedeutet die optimale Einstellung von Systemen auf die tatsächliche oder erwartete Arbeitsbelastung anhand der gemessenen, analysierten und interpretierten Daten.

- **Implementierung**:
  Das Ziel der Implementierung besteht in der Bereitstellung der angepaßten oder erneuerten Kapazität. Diese Aktivität wird unter Beteiligung des Change-Managements durchgeführt.

- **Aufbau der Kapazitäts-Datenbank, CDB**:
  Der Aufbau der CDB umfaßt das Sammeln und die Pflege technischer, geschäftlicher und sonstiger Daten, die für das Capacity-Management von Bedeutung sind.

Beziehungen zu anderen Prozessen:

- Beziehung zum Incident-Management: Das Incident-Management informiert das Capacity-Management über Störungen, die aufgrund von Kapazitätsproblemen entstanden sind. Im Gegenzug sollte das Capacity-Management Werkzeuge zur Erkennung und Behebung zur Verfügung stellen.

- Beziehung zum Change-Management: Das Capacity-Management sollte im CAB vertreten sein. Somit kann das Capacity-Management Informationen über den Kapazitätsbedarf sowie die Auswirkung von Änderungen zur Verfügung stellen; im Gegenzug können die erhaltenen Informationen über Änderungen in den eigenen Kapazitätsplänen berücksichtigt werden.

- Beziehung zum Service-Level-Management: Wie bereits erläutert, besteht eine ständige Wechselbeziehung zum Service-Level-Mangement, da zum einen bei der Ausgestaltung der Service-Levels Informationen geliefert werden können und zum anderen Vorgaben vom Service-Level-Management bezüglich aller das Gebiet des Capacity-Managements betreffenden Bereiche gegeben werden.

- Beziehung zum Finance-Management: Das Capacity-Management stellt seine Unterstützung bei der Erstellung von Investitionsfinanzplänen, für Kosten-Nutzen-Überlegungen sowie im Rahmen von Investitionsentscheidungen zur Verfügung.

- Beziehung zum Availability-Management: Auch hier besteht eine enge Verbindung zwischen beiden Prozessen, da Leistungs- und Kapazitätsprobleme zu Funktionsstörungen sowie zum Totalausfall von Diensten führen können. Infolge der Überschneidungen können beide Prozesse dieselben Werkzeuge und Techniken und Methoden verwenden.

6.5.4.4 Aktivitäten bei VoIP

Bestimmung eines Prozeßmanagers, der den kompletten Prozeßablauf zu steuern hat und für die ständige Aktualisierung der Subprozesse verantwortlich ist.
Innerhalb des Capacity-Managements sind System- und Anwendungsmanager einzurichten, die den Bedarf des Kunden in relevante Anforderungen umsetzen können und das System so überwachen und betreuen, daß es eine optimale Leistung erzielt.

- **Business-Capacity-Management:**
  Bei VoIP sollte der Kapazitätsplan folgende Bestandteile haben:

  - **Entwicklung der Teilnehmerzahl und Typen der benötigten Anschlußtypen**. In Abhängigkeit von der Teilnehmerzahl und des jeweiligen Anschlußtyps (analog, ISDN, VoIP-Teilnehmer, evtl. konventioneller Teilnehmer bei Hybridsystemen) ist die Beschaffung von zusätzlicher Hardware wie Endgeräten oder Einschubkarten in den Zentralsystemen sowie die dafür notwendige Anzahl an Softwarelizenzen erforderlich; u.U. Umständen kann auch eine Erweiterung der Zentralsysteme um zusätzliche Server oder Shelfs erforderlich werden.
    Für die tatsächliche Beschaffung empfiehlt sich eine Unterteilung der benötigten Komponenten in verschieden Kategorien wie Massenware und Spezialkomponenten. Spezialkomponenten sollten beim Anbieter des VoIP-Systems direkt gekauft werden, da nur dieser meist die notwendigen Werkzeuge zur Erweiterung besitzt (so ist z.B. beim Kauf neuer Softwarelizenzen meist ein neuer Lizenzschlüssel erforderlich, der von anderen Firmen nicht erzeugt werden kann). Außerdem bestehen Wartungs- oder Instandhaltungsverträge mit den Herstellern oder Anbietern, in die fremdbeschaffte Komponenten nicht aufgenommen werden. Massenware (wie Endgeräte oder Einschubkarten) kann dagegen beliebig bezogen werden. Zur Vermeidung von Transaktionskosten (Kosten für die Vertragsanbahnung) sollte turnusmäßig (z.B. jedes Jahr) eine Stichprobe von benötigten Artikeln bei einer gewissen Zahl von Anbietern und Händlern abgefragt werden und dann in diesem Zeitraum nur beim preiswertesten eingekauft werden. Preiswert bedeutet aber nicht nur billig, sondern auch die Einbeziehung anderer Merkmale wie Lieferzeit und -treue, Zahlungsbedingungen, Verhalten bei Mängeln und im Reklamationsfall, ...
    Dieses Vorgehensmodell führt zu kurzen Beschaffungszeiten, da die Anbieterauswahl wegfällt, und damit ist kein Aufbau eines großen Lagerbestandes notwendig, was die Lagerkosten (v.a. die kalkulatorischen Zinsen auf die Bestände!) deutlich senkt. Es wird aber darauf hingewiesen, daß dies nicht die Streichung der Lagerbestände bedeutet, da ein gewisser Vorratsbestand immer vorhanden sein sollte (z.B. beim Ausfall kritischer Komponenten).

  - **Dimensionierung des VoIP-Systems**. In Abhängigkeit von der geplanten Nutzerzahl und den sonstigen Anforderungen (inklusive mindestens eines Sicherheitspuffers von mindestens derselben Anzahl) ist das VoIP-System zu dimensionieren. Hierbei geht es um die Hard- und Softwareausstattung des Zentralsystems. Dies betrifft die Auswahl der Prozessoren (kann der Prozessor alle Verbindungswünsche verarbeiten, da die Gesprächsverarbeitung in Echtzeit erfolgen muß), die Systemarchitektur (Einfach-/Mehrfachsteuerung, reines VoIP-System/Hybridsystem – siehe Kapitel 5.1), die Anzahl der sonstigen Hardwarekomponenten wie Einschubkarten oder Endgeräte und die Anzahl und den Typ der Softwarelizenzen.

  - **Bestimmung der Bandbreite von Vernetzungsstrecken sowie für die Anbindung an das öffentliche Telefonnetz**. Unabhängig von der Realisierung der Vernetzung von VoIP-/TK-Systemen in Firmenverbünden (siehe Kapitel 3.2.6.2) mittels konventioneller TDM-basierter Technik bzw. mittels VoIP ist eine Bandbreitenbestimmung für jede Strecke vorzunehmen (wieviele Gespräche werden gleichzeitig geführt?); die Maßeinheit für die Anzahl gleichzeitiger Gespräche lautet Erlang, wobei ein Erlang ein Gespräch bedeutet.
    Dies kann entweder über Messungen geschehen, wobei der Spitzenwert angesetzt werden sollte (abhängig von der Vereinbarung im SLA); im Telefoniedienst kann aber davon ausgegangen werden, daß eine Verbindung mit einer Wahrscheinlichkeit sehr nahe an 100% zustande kom-

men sollte.
Eine andere Möglichkeit besteht in der mathematischen Berechnung mittels stochastischer Methoden (Markov-Ketten, siehe [STS01]). Hierzu ist die Bestimmung der durchschnittlichen Gesprächsdauer sowie des Intervalls, in dem neue Gespräche eintreffen, erforderlich (was über Messungen bzw. Trendvorhersagen zu erfolgen hat). Aus diesen Größen kann berechnet werden, wieviele Kanäle zur Verfügung stehen müssen, damit mit einer Wahrscheinlichkeit von x % ein zusätzliches Gespräch aufgebaut werden kann.
Wenn der Erlang-Wert bekannt ist, ist – abhängig von der gewählten Codierung (siehe 3.3.4) – die benötigte Bandbreite durch Multiplikation dieser beiden Werte (und eines Sicherheitspuffers) zu ermitteln. Basierend auf diesem Wert ist die benötigte Anzahl von S_{2M}- oder S_0- bzw. Bandbreite auf IP-Strecken vorzuhalten, wobei bei IP-Verbindungen noch der sonstige Datenverkehr (unter Berücksichtigung eines ausreichenden Sicherheitspuffers) dazugezählt werden muß, daß die Paketlaufzeiten bei zunehmender Auslastung exponentiell anwachsen ([TAN00]). Bei der Unterhaltung von S_0-Verbindungen ist zu berücksichtigen, daß – wenn mehrere benötigt werden – eine S_{2M}-Strecke günstiger sein kann.

– **Realisierung einer QoS-Architektur**. Um eine zu den SLA´s konforme Sprachqualität (siehe Kapitel 4.1.1) – auch zu Spitzenzeiten – garantieren zu können, sollte eine Quality-of-Service-Architektur eingesetzt werden . Beispiele und Realisierungsalternativen sind in Kapitel 5.4 dargestellt, wobei die Auswahl des verwendeten Verfahrens den angebotenen Alternativen des Herstellers und den Präferenzen des Kunden entsprechen muß, da mit dem Quality-of-Service-Verfahren tief in die Netzinfrastruktur des Kunden eingegriffen wird.

• **Service-Capacity-Management und Ressource-Capacity-Management:**

– **Überwachung (Monitoring)**:
Wie bereits ausgeführt, beschäftigt sich das Monitoring mit der Verfolgung und Kontrolle verschiedener Komponenten der Infrastruktur. Bei VoIP sind dies: Auslastung des Zentralsystems (Prozessorlast, Speicherauslastung, Lizenzbelegung, Belegung der Hardwareports), Auslastung der Verbindungsstrecken und sonstigen Applikationen (wie z.B. Unified-Messaging-Systeme). Werkzeuge hierzu sind entweder SNMP-basierte Managementplattformen oder eigenständige Werkzeuge, die auf dem Internet-Management basieren sowie Anwendungen der Hersteller des VoIP-Systems, um auf nicht mit dem Internet-Management abfragbare Informationen zugreifen zu können.

– **Analyse**:
Aufgrund der Ergebnisse des Analyseprozesses sind Maßnahmen zur Steigerung der Effizienz oder die Beschaffung von zusätzlichen Komponenten (Hard- oder Software sowie zusätzliche Verbindungsstrecken oder Erhöhung der Bandbreite) einzuleiten.

– **Tuning und Implementierung**:
optimale Einstellung von Systemen auf die tatsächliche oder erwartete Belastung anhand der gewonnenen Daten (z.B. ein geändertes Routing von Gesprächen über andere Strecken oder Interfaces).

– **Implementierung**

– **Aufbau der Kapazitäts-Datenbank, CDB**:
Wegen der Vielzahl der Informationen aus verschiedenen Systemen ist bei VoIP die Speicherung in einer (physischen) Datenbank nicht machbar. Im Bereich von VoIP besteht die CDB aus den Teilbereichen Hard-/Softwaredimensionierung und -nutzung, Netzdesign und Bandbreitenplanung, Finanzdaten und Zukunftsprognosen.

6.5.4.5 Prozeßsteuerung

Wie bei den anderen Prozessen auch, sind in zyklischen Abständen Berichte an das Management zu erstellen, die Abweichungen von der Planung zur tatsächlichen Inanspruchnahme und den diesbezüglichen Einfluß auf die Service-Levels darstellen und die die Trendanalysen illustrieren.
Problematisch für das Capacity-Management ist, daß es in hohem Maß von den Anforderungen des Kunden abhängig ist. Daher ist (soweit möglich) der Kunde darauf hinzuweisen, daß er seine Wünsche frühzeitig äußern soll, da sonst eine termingerechte Ausführung nicht möglich ist. Außerdem ist – gerade in diesem Punkt – ein ständiger Dialog mit dem Kunden zu führen (auch was den Einsatz neuer Techniken betrifft).

6.5.5 Availability-Management

6.5.5.1 Begriffsdefinitionen

In Abbildung 6.9 sind die wichtigsten Begriffe im Availability-Management graphisch dargestellt.

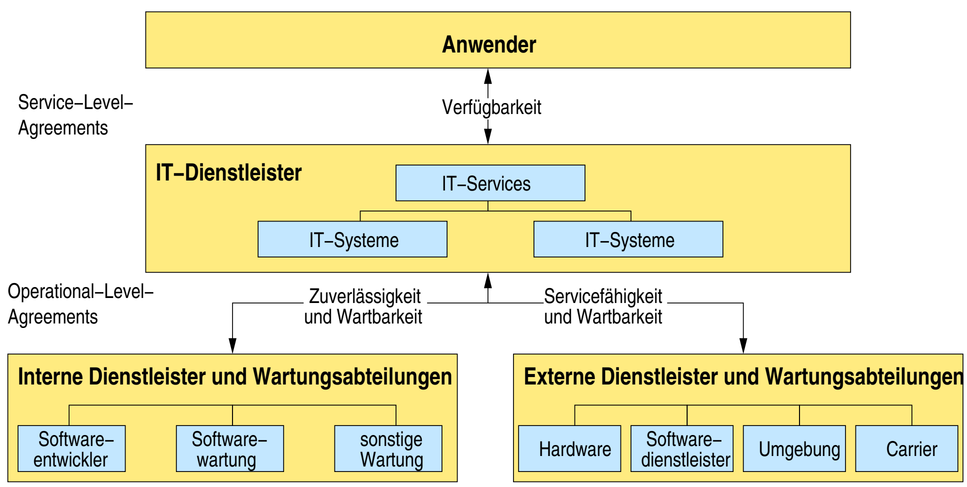

Abbildung 6.9: Grundbegriffe des Availability-Managements

Verfügbarkeit (Availability): Verfügbarkeit ist gegeben, wenn der Kunde/Anwender den Dienst – wie im SLA vereinbart – nutzen kann. Daneben werden im SLA weitere Parameter wie Service- und Reaktionszeiten vereinbart.

Zuverlässigkeit (Reliability): Störungsfreie Funktion des Dienstes für einen gewissen Zeitraum (je geringer die Ausfallzeiten und die Anzahl der Ausfälle, desto höher ist die Zuverlässigkeit). Die Fehlertoleranz von Systemen (Resilience) hat ebenfalls Einfluß auf die Zuverlässigkeit.

Wartbarkeit (Maintainability): Wartbarkeit stellt den Aufwand dar, der zum Betrieb eines Dienstes oder zur Wiederherstellung der Funktionsfähigkeit bei/nach einem Ausfall erforderlich ist; hierzu zählen auch proaktive Maßnahmen wie regelmäßige Überprüfungen.

Servicefähigkeit (Serviceability): Die Möglichkeit, für Komponeten des Dienstes externen Support zu beauftragen

Zyklus einer Störung :

- Auftreten der Störung (durch Anwender oder technisches Hilfsmittel erkannt)
- Erkennung (Information des Dienstleisters über Störung)
- Reaktion (Diagnosezeit des Dienstleisters)

- Reparatur
- Dienstwiederherstellung

6.5.5.2 Zielsetzung

Die Zielsetzung des Availability-Managements besteht in der *Gewährleistung* eines auf den Kunden zugeschnitten, effizienten *Verfügbarkeitsniveaus* ([OGC01]).
Voraussetzung hierfür ist die Übereinstimmung der Anforderungen des Kunden mit den Möglichkeiten, die die Infrastruktur und die IT-Organisation bieten.
Das Availability-Management legt ein besonderes Gewicht auf den Qualitätsgedanken (Ansatz des Total-Quality-Managements (TQM) und Total Productive Maintenance (TPM) – vorbeugende Wartung – des Just-in-Time-Konzepts (Kapitel 6.1). Ein hoher Anteil an Fehlteilen (wird in Teilen pro Million gemessen) bzw. lange Ausfallzeiten (nicht nur im IT-Sektor) verursachen immense Kosten zur Fehlerbehebung (v.a. in mehrstufigen Produktionsprozessen)und demotivieren die Mitarbeiter; daher sind auch proaktive und begleitende Maßnahmen erforderlich (z.B. regelmäßige Wartung).
Darüber hinaus sind die Verantwortlichkeiten in Bezug auf die Verfügbarkeit eines Dienstes genau definiert, sodaß der Kunde nur einen Ansprechpartner hat.

6.5.5.3 Prozeß

Der Prozeß des Avalability-Managements beinhaltet neben organisatorischen Maßnahmen auch diverse Tätigkeiten im technischen Umfeld des Dienstes. Diese Aktivitäten sind aber dienst- und infrastrukturspezifisch, daher kann an dieser Stelle keine generelle Aufteilung in Teilprozesse und -aspekte gemacht werden; es werden nur allgemein die Eingangs- und Ausgangsgrößen des Availability-Managements in 6.10 vorgestellt. Eine detaillierte Ausarbeitung für VoIP erfolgt im nächsten Abschnitt (Kapitel 6.5.5.4).

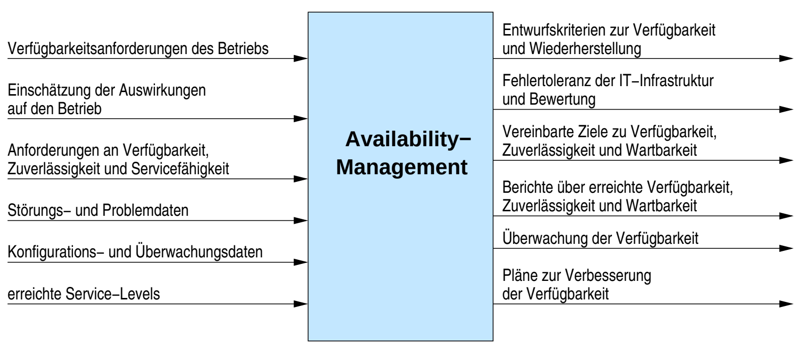

Abbildung 6.10: Prozeß des Availability-Managements

Beziehungen zu anderen Prozessen ([BKP02]):

- **Service-Level-Management**: Die Verfügbarkeit (nebst sich daraus ergebenden Parametern) ist einer der wichtigsten Aspekte, der in SLA´s festgelegt wird.
- **Configuration- und Capacity-Management**: Lieferanten von Informationen über die IT-Infrastruktur sowie Abstimmung mit dem Availibility-Management (v.a. bei Erweiterungen).
- **Continuity-Management for IT-Services**: Zuständigkeit für Dienstwiederherstellung nach (unkalkulierbaren) Katastrophen; liefert Informationen über unternehmenskritische Prozesse.
- **Security-Management**: gegenseitiger Informationsaustausch (Sicherheitskriterien gehören auch zur Verfügbarkeit).

- **Change-Management**: Availibility-Management ist Informationslieferant für Wartungsprozeduren, die im Rahmen der Realisierung von Änderungen ausgeführt werden sollen, und Informationsempfänger für geplante Änderungen des Change-Managements.
- **Incident- und Problem-Management**: Übermittlung von Verfügbarkeitsproblemen (beim Problem-Management: zusätzlich Identifizierung von Behebung)

6.5.5.4 Aktivitäten bei VoIP

Für das Availability-Management ist ein Prozeßmanager zu benennen, der für alle Aktivitäten verantwortlich ist.
Das Availability-Management umfaßt diverse Aktivitäten, die auf Planung und Kontrolle ausgelegt sind.

- Planung
  - Verfügbarkeitsanforderungen: Die Verfügbarkeitsanforderungen (nebst Arbeits- bzw. Rahmenzeiten des Kunden) für VoIP werden im SLA (Kapitel 6.5.2.4) festgelegt. Ausgehend davon sind vom Availability-Management mit dem Kunden Zeiten für geplante Wartungs- oder Reparaturarbeiten abzusprechen (da bei VoIP eine Betriebszeit rund um die Uhr gefordert wird, sind diese Arbeiten bei geringer Last des Systems – z.B. an Wochenenden – durchzuführen). Daneben sind im SLA Reaktions- und Servicezeiten festzulegen; diese sind Grundlage für die eigenen SLA´s mit Externen sowie für die Planung des Servicezyklusses.
  - Infrastruktur:
    - VoIP-System (Zentralkomponenten): Die Zentralkomponenten sind besonders gegen Ausfälle zu schützen, da beim Ausfall dieser Systeme ein Teil oder alle VoIP-Endgeräte keinerlei Gespräche mehr verarbeiten können (die grundlegenden Architekturen sind in Kapitel 5.1 beschrieben).
      Hierbei sind die Speichermedien (Festplatten) redundant bzw. fehlertolerant (z.B. mittels RAID-Systemen) zugleich die Rechner ebenfalls redundant auszuführen, um bei Hardwaredefekten und Ausfällen dieser Komponenten gar keine oder eine nur minimale Dienstbeeinträchtigung zu erleiden. Außerdem sind diverse kritische Teilsysteme in einem Reservebestand verfügbar zu halten oder eine Vereinbarung mit Externen zur Lieferung innerhalb bestimmter Zeiten abzuschließen (weitere Ausführungen in diesem Abschnitt unter „Wartung“).
    - Datennetz: Im Datennetzbereich ist eine strukturierte Verkabelung auszuführen, wobei im Tertiärbereich eine Ausführung auf der Basis des Mediums Kupferkabel in der derzeit aktuellen Kategorie (derzeit Cat. 6/7) zu realisieren ist, um die Stromversorgung der VoIP-Endgeräte vom Tertiär-Switch (Access-Switch) sicherzustellen (mittels IEEE 802.3af, siehe Kapitel 5.5) – beim Medium Glasfaserkabel ist dies nicht möglich, da mit Photonen keinerlei elektrische Energie übertragen werden kann.
      Im Primär- und Sekundärbereich sind alle Komponenten und Kabelwege redundant einzurichten – falls die Redundanz der Netzkomponenten nicht wirtschaftlich ist, sind die verwendeten Netzkomponenten zumindest so auszuwählen, daß eine Konfigurationsänderung (einschließlich des Ein- oder Ausbaus von Modulen) im laufenden Betrieb erfolgen kann. Diese Redundanz erfordert daneben zwingend dynamische Verfahren (auf Layer 2 das STP und auf Layer 3 OSPF).
    - Stromversorgung: Alle Komponenten (VoIP-Zentralkomponenten, Netzkomponenten (Datennetz und eine eventuell vorhandene konventionelle Vernetzung von TK-Systemen, siehe Kapitel 3.2.6.2, und die Anbindung an das öffentliche Telefonnetz) sind gegen Stromausfälle abzusichern. Dies geschieht entweder über unterbrechungsfreie Stromversorgungen oder zentrale Systeme (Batterieräume mit entsprechenden Wechselrichtern). Die Notwendigkeit und die minimale Absicherungszeit ergibt sich aus gesetzlichen Bestimmungen

zum Betrieb bestimmter Einrichtungen (z.B. Aufzüge – Absetzen von Notrufen). Dies bedeutet einen deutlich höheren Aufwand (v.a. für das Datennetz) als ohne den Einsatz von VoIP, da durch die Nutzung des Datennetzes für Sprachkommunikation deutlich längere Überbrückungszeiten gefordert und erwartet werden.

– Wartung: Wie bereits in 6.5.5.2 ausgeführt, ist vorbeugende Wartung sowie ein Wartungskonzept unerläßlich für die Vermeidung von Fehlern oder Störungen sowie das schnelle Wiederaufsetzen nach Ausfällen. Daher wird im Folgenden ein Wartungskonzept für ein VoIP-System vorgestellt.
Wie in Kapitel 5.1 erläutert, bestehen VoIP-Systeme aus Zentralkomponenten, Endgeräten und dem zugrundliegenden Datennetz. Im Wartungskonzept sind diese Teilbereiche nach Risiken zu unterscheiden:
Personell ist ein Administrator (nebst dazugehörigem Team) des VoIP-Systems einzusetzen und weiterzubilden; dieser Personenkreis soll prinzipiell in der Lage sein, alle im täglichen Betrieb anfallenden Störungen zu beheben und ist dafür auszubilden bzw. zu schulen. Dies hat den Vorteil, daß kleine Probleme und Ausfälle schnell und ohne die Hilfe Externer behoben werden können.
Hardwaremäßig sind alle Komponenten in die Gruppen Massenware (z.B. Endgeräte) sowie Spezialkomponenten (z.B. Einschubkarten) einzuteilen (dies kann auch nach dem Wiederbeschaffungswert erfolgen); außerdem ist eine Einteilung hinsichtlich der Wichtigkeit für die Verfügbarkeit vorzunehmen (Component Failure Impact Analysis, [BKP02].
Von Massenware (z.B. Endgeräten) und niedrigpreisigen (kritischen und unkritischen) Spezialkomponenten ist ein kleiner Austauschbestand vorzuhalten und bei Bedarf vom im Capacity-Management bestimmten Anbieter/Händler nachzukaufen (siehe 6.5.4.4). Dies hat den Vorteil, daß sowohl Kapitalbindungskosten als auch der mit der Lagerung verbundene Aufwand durch den geringen Lagerbestand niedrig sind. Hinsichtlich der Endgeräte ist beim Availbility-Management – außer dem Vorhalten eines Reservebestands – nichts zu bedenken. Man sollte aber versuchen (was häufig wegen Sonderwünschen von Führungskräften nicht möglich ist), die Anzahl verschiedener Endgerätevarianten und Zubehörteile gering zu halten, um die Lager- und Reservebestände nicht allzusehr anwachsen zu lassen (der Hintergrund hierfür liegt auch im Just-in-Time Konzept, Kapitel 6.1, nämlich der Reduzierung der Variantenvielfalt, da sich durch diese Reduktion überproportional Kosten sparen lassen).
Hochpreisige, systemkritische Spezialkomponenten sind in einen Wartungsvertrag mit einem Externen aufzunehmen.
Dieser Wartungsvertrag sollte wie folgt ausgestattet sein (die vom Externen einzuhaltenden Fristen leiten sich aus dem eigenen SLA oder der eigenen Risikobereitschaft ab):

  ∗ Lieferung von hochpreisigen Spezialkomponenten innerhalb bestimmter Fristen
  ∗ Hilfestellung innerhalb bestimmter Fristen (in Fällen, in denen das Administrationsteam fremde Hilfe benötigt)
  ∗ Verfügbarmachung von Software-Updates für das VoIP-System.

Eine Komplettwartung ist nicht zu vereinbaren, da dafür das Administrationsteam vorhanden ist; der Vertrag soll den Charakter eines Servicevertrags haben, d.h. daß bei Bedarf Hilfe angefordert wird, die aufwandsbezogen abgerechnet wird (durch die Ersatzbestände sowie die Schulung und Erfahrung des eigenen Personals wird die Hilfe des Externen nur in Ausnahmefällen erforderlich, wie z.B. Defekt in kritischen Spezialkomponenten). Ein weiterer Grund gegen eine Komplettwartung besteht in der geringen Ausfallwahrscheinlichkeit der Endgeräte, die in einem Wartungsvertrag einen Großteil der Kosten ausmachen; das Vorhalten eines Reservebestands, wie oben erläutert, kostet einen Bruchteil der Ansätze in einem Wartungsvertrag. Alle anderen Störungen werden vom eigenen Personal erledigt, was überdies zu einer Verbesserung der Reaktions- und Fehlerbehebungszeiten führt, da die Anfahrts- und Einarbeitungszeiten des Externen entfallen.

– Datensicherungskonzept: Alle zum Wiederaufsetzen des VoIP-Systems erforderlichen Daten sind in regelmäßigen Abständen zu sichern und in einem feuer- und explosionsgeschützten Behältnis (möglichst in einem anderen Gebäude) aufzubewahren.

  – sicherheitsrelevante Gesichtspunkte (v.a. personell) werden in Kapitel 6.5.6.4 vorgestellt.

- Kontrolle: Messung und Berichtswesen sind eine wichtige Aktivität für das Availability-Management, weil sie die Kontrolle von Servicevereinbarungen, die Behebung von Problemsituationen und die Formulierung von Verbesserungsvorschlägen darstellt. Hierzu sollen dem Availability-Management Werkzeuge u.a. zur Ermittlung von Ausfallzeiten, Speicherung von Historikdaten, Berichtserstellung und Durchführung von Analysen zur Verfügung stehen. Bei VoIP ist Grundlage hierfür ein auf dem Internetmanagement basierendes Monitoringsystem, das den Systemzustand aller Komponenten, Latenzzeiten, Datenvolumina, . . . aufzeichnet.
  Hierzu sind zyklisch die Fehler- und Protokolldateien der VoIP-Zentralsysteme und Netzkomponenten auszuwerten, da sich große Ausfälle oder Problemsituationen meist über kleinere Fehlermeldungen ankündigen (proaktives Handeln). Außerdem sind automatisiert Meldungen bei kritischen Problemen oder Fehler zu generieren (z.B. über SNMP-Trap-Meldungen), wobei hierzu die Erfahrungen aus den proaktiven Auswertungen der Protokolldateien zur Definition von Schwellwerten genutzt werden können.

6.5.5.5 Prozeßsteuerung

Im Rahmen der Prozeßsteuerung des Availability-Managements sind Berichte an den Kunden (hinsichtlich der Einhaltung der SLA´s und für das Management detailliertere Berichte, die zusätzlich z.B. Verbesserungs- und Änderungspotential aufzeigen, zu erstellen.
Kritische Faktoren und Hindernisse im Availability-Management bestehen u.a. in der hohen Abhängigkeit von anderen Prozessen und in der fehlenden Akzeptanz (jeder Prozeß geht davon aus, seine Aufgaben optimal zu erfüllen, und sieht daher die Notwendigkeit und Wichtigkeit einer Gesamtsteuerung im Rahmen des Availability-Managements nicht). Dieses Bewußtsein ist in der Organisation aufzubauen und weiterzuentwickeln.

6.5.6 Security-Management

6.5.6.1 Begriffsdefinitionen

Zu Beginn werden einige Begriffe erläutert, die von zentraler im Bereich des Sicherheitsmanagements sind ([BKP02]).

Safety (Sicherheit): Sicherheit vor bekannten und größtmögliche Vorbeugung vor unbewußten Risiken

Security (Schutz): Mittel, die zur Realisierung von Sicherheit eingesetzt werden. Hierbei ist der Wert der Informationen zu schützen. Dieser Wert bestimmt sich aus Vertraulichkeit, Integrität und Verfügbarkeit.

Vertraulichkeit (Confidentiality): Schutz von Informationen vor unautorisierter Kenntnisnahme und unbefugter Benutzung

Integrität (Integrity): Richtigkeit, Vollständigkeit und Korrektheit der Information

Verfügbarkeit (Availability): Verfügbarkeit der Information zu jedem Zeitpunkt

6.5.6.2 Zielsetzung

Die Zielsetzung des Security-Managements besteht in der *Einführung* und *Erhaltung* eines definierten Sicherheitsniveaus in der IT-Infrastruktur sowie in der *Gewährleistung* einer vordefinierten Reaktion auf sicherheitsrelevante Vorfälle ([OGC01]).

Grundlagen hierfür sind einerseits die in den Service-Level-Agreements vereinbarten Sicherheitsanforderungen und andererseits Sicherheits-Grundsätze des Unternehmens (intern oder extern, wie z.B. Handbücher des Bundesamts für Sicherheit in der Informationstechnik).
Ergebnis des Sicherheitsmanagements sind die Planung und Realisierung von Sicherheitsmaßnahmen sowie die Definition von Zuständigkeiten in der Aufbau- und Ablauforganisation.

6.5.6.3 Prozeß

Organisationen und Organisationssysteme sind ständigen Änderungen unterworfen. Daher sind reine Checklisten und Handlungsanweisungen im Rahmen des Sicherheitsmanagements nicht ausreichend. Erforderlich ist vielmehr die ständige Überprüfung und Überarbeitung, um die Effektivität des Sicherheitsmanagements zu erhalten.
Dieser Abschnitt behandelt den Prozeß des Security-Managements sowie die Beziehung zu anderen Prozessen ([BKP02]).
In Abbildung 6.11 ist der Managementzyklus für das Security-Management dargestellt. Der Kunde stellt

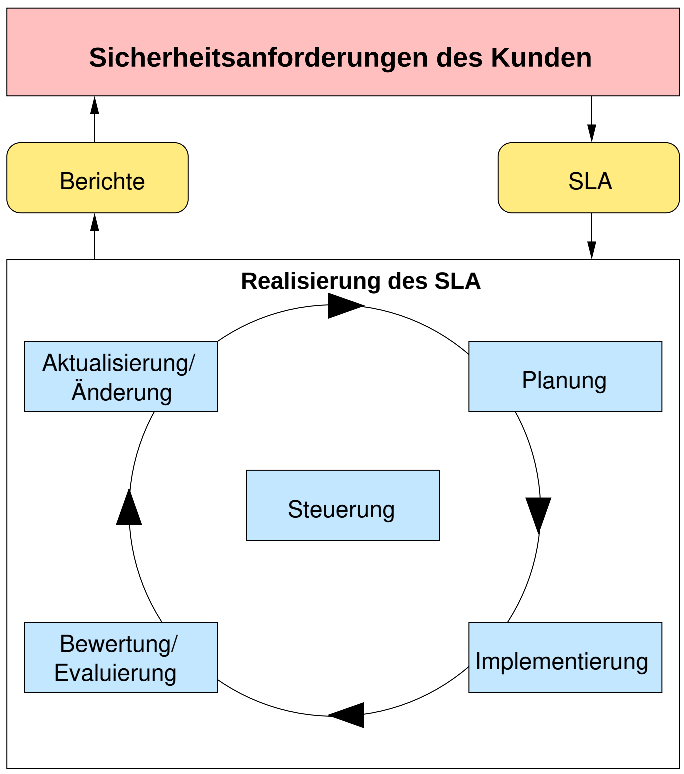

Abbildung 6.11: Prozeß des Security-Managements

seine Sicherheitsanforderungen und gibt so die Eingangsgrößen vor. Diese Anforderungen werden in die zu erbringenden Sicherheits-Services und deren Qualität in den Sicherheitsheitspassagen des SLA umgesetzt (siehe Kapitel 6.5.2.4).
Der Service-Provider detailliert diese Vereinbarungen entsprechend seiner Organisation in Form eines Sicherheitsplans, in dem die Sicherheitsnormen und -vereinbarungen auf Betriebsebene festgelegt werden. Dieser Plan wird implementiert und bewertet. Anschließend werden sowohl der Plan als auch seine Implementierung gepflegt. Dem Kunden wird über die Aktivitäten Bericht erstattet. Der Zyklus schließt sich hier sowohl beim Kunden als auch beim Anbieter. Erstens kann der Kunde auf der Grundlage der Berichte seine Anforderungen und Wünsche anpassen. Zweitens kann der Service-Provider auf der Grundlage seiner Erfahrungen seinen Plan oder dessen Implementierung anpassen oder die Anpassung der Vereinbarungen

im SLA anstreben.
Beziehungen zu anderen Prozessen:
Wie bereits erläutert, unterhält das Security-Management quasi per Definition Beziehungen zu allen anderen Prozessen, da innerhalb dieser Prozesse alle Aktivitäten hinsichtlich sicherheitsrelevanter Problematiken überprüft werden müssen. Dies erfolgt selbständig innerhalb der jeweiligen Prozesse; das Sicherheitsmanagement erteilt den Prozessen jedoch Anweisungen über die Implementierung der sicherheitsgerichteten Aktivitäten. Diese Vereinbarungen und Anweisungen werden in Abstimmung mit den Prozessmanagern und dem Prozeßmanager des Sicherheitsmanagements getroffen.
Diese Interferenz unterstreicht die Bedeutung des Security-Managements innerhalb des Managementkonzepts, da zum einen alle Prozesse den Aspekt „Sicherheit" immer berücksichtigen müssen und zum anderen eine Sicherheitskultur in den Köpfen der Mitarbeiter entstehen muß. Denn eine magelhafte (oder gar keine) Umsetzung des Sicherheitsgedankens kann die Nichtverfügbarkeit ganzer Systeme bzw. die Insolvenz des Kunden bedeuten.
Im folgenden werden nur die wichtigsten Prozesse aufgeführt und Erläuterungen hinsichtlich der Querbeziehungen gegeben.

- **Service-Level-Management**: Wie bereits ausgeführt, bestimmen die SLAs die Eingangsgrößen für das Security-Management. Dies betrifft den Sicherheitsbedarf des Kunden sowie sich das daraus ergebende Sicherheitsmaß. Darauf aufbauend werden interne Sicherheitsnormen (für den Serviceprovider) erstellt und diese überwacht. Darüberhinaus wird an das Service-Level-Management hinsichtlich der Einhaltung der vereinbarten Kriterien berichtet.

- **Incident-Management**: Das Incident-Management ist *der* Prozeß für die Meldung von Sicherheitsstörungen, für die ein anderes Verfahren als bei „normalen" Störungen gelten kann. Es ist Voraussetzung, daß eine Sicherheitsstörung vom Incident-Management als solche erkannt wird, wobei diese Meldungen in nicht nur von den Anwendern, sondern auch von Alarm- oder sonstigen Meldungen aus diversen System kommen können. Sobald eine Sicherheitsstörung erkannt und klassifiziert ist, ist vom Incident-Management das Security-Management zu beteiligen bzw. einzuschalten.

- **Change-Management**: Change-Management und Security-Management müssen eng zusammenarbeiten, da sich beim Auftreten von Sicherheitsstörungen häufig Änderungsaufgaben ergeben, die schnell bzw. sofort ausgeführt werden müssen. Das Security-Management erstellt also einen Teil der RfC´s, die vom Change-Management abgearbeitet werden müssen.
  Auf der anderen Seite sollte das Sicherheitsmanagement bei allen Änderungen, die vom Change-Management durchgeführt werden sollen, beteiligt werden. Dies könnte beispielsweise durch die Mitgliedschaft des Security-Management-Prozeßmanagers im CAB geschehen.

6.5.6.4 Aktivitäten bei VoIP

Für das Security-Management ist ein Prozeßmanager zu bestimmen, der nicht identisch mit dem Manager eines anderen Prozesses sein sollte. Er sollte außerdem ein Mitspracherecht bei den anderen Prozessen haben, da die Einhaltung von Sicherheit hohe Priorität haben sollte. Der weitere Aufbau ist an den in 6.5.6.3 genannten Bausteinen des Security-Management angelehnt, wobei der Planung der Sicherheitsaspekte der größte Anteil zukommt.

- *Planung*:
  Die Planung enthält alle grundsätzlichen Fragestellungen für die Realisierung des vereinbarten Sicherheitsniveaus. Da ein VoIP-System alle sicherheitsrelevanten Fragestellungen von Telekommunikationssystemen und Datennetzen in sich vereint, sind für folgende Bereiche Festlegungen zu treffen:

  – Infrastrukturell: Telekommunikationssysteme stellen einen unverzichtbaren Beitrag zur Kommunikation mit Geschäftspartnern, Kunden und sonstigen Personengruppen dar. Daher sollten sie, wie in 4.1.3 gefordert, ausfallsicher sein. Da ein VoIP-System vollkommen in das Datennetz integriert ist, ergeben sich hier alle sicherheitsrelevanten Problemstellungen in verschärfter

Form, da bei einer Sicherheitsstörung aus dem Bereich des Datennetzes ein Totalausfall drohen kann.

* Wahl des Betriebssystems und der Anwendungssoftware (sowohl für die Zentralkomponenten als auch die VoIP-Teilnehmer): Einige Hersteller setzen für ihre Zentralkomponenten Windows-basierte Betriebssysteme und sonstige Anwendungen wie Datenbanksysteme (z.B. Cisco) ein, die, wie die Viren- und Wurmattacken („Blaster"- und „Sasser"-Wurmattacken in 2003 und 2004) der letzten Jahre sowie das immerwährende Erscheinen von Sicherheitsupdates zeigen, nicht für hochverfügbare Systeme geeignet sind. Daher ist vom Einsatz solcher Systeme in unternehmenskritischen Einheiten abzuraten. Es muß betont werden, daß alternative Betriebssysteme (wie z.B. Linux oder Unix) ebenfalls Sicherheitslücken aufweisen, deren Verbreitung aber einen Bruchteil der Windows-Systeme ausmacht, sodaß allein aufgrund der statistischen Angriffswahrscheinlichkeit diese Systeme zu bevorzugen sind.
  Andere Hersteller (z.B. Siemens) setzen Multiprozessorsysteme mit verschiedenen Betriebssystemen ein, die jeweils für den Einsatzzweck entwickelt worden sind (UnixWare – ein Unix-Derivat – für den Verwaltungsserver des VoIP-Systems sowie RMX – ein ursprünglich von Intel entwickeltes Echtzeitbetriebssystem, das von Siemens weiterentwickelt wurde – für die eigentliche Gesprächsverarbeitung). Die genaue Architektur wird in Kapitel 7.2.1 erläutert. Diese Systeme sind aus diesem Blickwinkel zu bevorzugen.

* Abschottung vom sonstigen Datennetz: VoIP-Systeme sind zum einen wegen der Gefahr, die durch Schadprogramme (Viren, Würmer, ...) und zum anderen wegen der möglichen Einbruchgefahr und Gebührenbetrug vom übrigen Datennetz abzuschotten. Bei firmeninternen Netzen bzw. dem Internet ist man nie vor Personen sicher, die in die Zentralsysteme eindringen wollen oder auf fremde Kosten telefonieren wollen, da sie nur ein VoIP-Endgerät (oder die notwendige Software) und die Registrierungsdaten zum Gatekeeper brauchen.
  Durch die in Kapitel 6.5.1.2 vorgestellte Trennung in logische Netze für die Zentralsysteme, die VoIP-Endgeräte und den sonstigen Datenverkehr ist die Abschottung relativ einfach zu realisieren: Installation einer Packet-Filter-Firewall bzw. Routingbeschränkungen in den Switches oder Routern dergestalt, daß von und in das Netz der Zentralsysteme nur Verbindungen aus dem Netz der VoIP-Endgeräte sowie einem bestimmten Kreis von sonstigen Rechnern (z.B. Wartungs-, Administrations- und Managementzwecke) zugelassen werden (und umgekehrt für das Netz der VoIP-Endgeräte).

* Abschottung vom öffentlichen Telefonnetz: Zu diesem Punkt existieren zwei relevante Aspekte, die berücksichtigt werden müssen: Einbruchgefahr durch Wartungszugänge und Gebührenbetrug durch sog. „Breakthough".
  Grundsätzlich sind Wartungszugänge für Externe (sei es durch eine direkte Einwahlmöglichkeit auf das VoIP-System oder durch einen Übergang durch die Firewallsysteme) wegen der damit verbundenen Sicherheitsrisiken auszuschließen (z. B. ungeschützter Zugang). Diese Risiken können zwar mit hohem Aufwand begrenzt oder ausgeschlossen werden, aber hier stellt sich die betriebswirtschaftliche Frage, ob dies die Bezahlung der sonstigen Kosten bei einem Einsatz der Wartungsfirma vor Ort und den Zeitgewinn aufwiegt.
  Wenn auf einen Wartungszugang nicht verzichtet werden kann, sollte sichergestellt sein, daß

  - keine Verbindung zum übrigen Datennetz möglich ist, da der Externe sonst u.U. volle Zugangsmöglichkeit hätte
  - eine Authentifizierung erforderlich ist
  - alle Aktionen protokolliert werden
  - bei der Nutzung von Telefonieverbindungen eine Rufnummernüberprüfung, ver-

schlüsselte Passwortübertragung sowie eine verschlüsselte Verbindung an sich sowie eine Callback-Funktion sichergestellt ist

· ein Zugang nur durch vorhergehende Reaktion eines Mitarbeiters möglich ist (z.B. Aktivierung der Rufnummer oder eines Programms, Einstecken der physischen Verbindung).

Der Aspekt „Breakthough“ betrifft den Gebührenbetrug. Breakthrough bedeutet, daß eine eingehende Verbindung vom VoIP-System wieder herausgeleitet wird (z.B. Rufumleitung auf ein Handy bei Abwesenheit eines Mitarbeiters). Dies sollte sehr restriktiv gehandhabt werden, da mit der Nutzung dieser Funktion sehr viel Schaden angerichtet werden kann und wurde. Beispiel hierfür ist, daß ein Mitarbeiter auf die „0“ zur Umleitung könnte und dann ein Anrufer dies ausnützen kann, da er danach nur noch die eigentliche Nummer nachwählen muß (im Extremfall zu Satellitentelefonnummern). Daher sollte dieses Leistungsmerkmal der Systeme gesperrt werden bzw. die Umleitungsmöglichkeit der Mitarbeiter auf fest vorgegebene Nummern eingeschränkt werden.
Mißbrauch durch Breakthrough kann aber auch durch unbewußte Konfigurationsfehler im Netzverbund eintreten (ein Unternehmen wollte für seine Mitarbeiter für Telefonate nach Südafrika eine kostengünstige Alternative einrichten; durch einen Fehler war diese Möglichkeit vom öffentlichen Telefonnetz erreichbar und wurde bekannt, sodaß dem Unternehmen ein großer Schaden bis zur Entdeckung entstanden ist).

∗ Zugangsschutz: Für die Räume, in denen die VoIP-Zentralsysteme bzw. die Netzkomponenten ist ein Zugangsschutzkonzept zu entwickeln, das nur bestimmten Personen den Zutritt gestattet.

– Personell: Im Security-Management ist eine organisatorische Hierarchie zu schaffen, die aus Administratoren und sonstigen Mitarbeitern besteht. Die Administratoren erhalten volle Systemrechte, spezielle Schulungen und sollten in der Lage sein, das VoIP-System eigenständig bedienen zu können (dazu zählt auch eine vollständige Außer- und Inbetriebnahme des Systems).
Die sonstigen Mitarbeiter erhalten die gemäß ihrem Aufgabengebiet benötigten Rechte und Kennungen.
Auch hier sind alle Aktionen zu dokumentieren und zu archivieren.

- *Implementierung*:
Die Implementierung umfaßt u.a.

  – die Implementierung von IT-Werkzeugen zur Realisierung der in der Planung getroffenen Richtlinien

  – personell die Erstellung von Schulungsplänen für die Mitarbeiter, Förderung des Sicherheitsbewußtseins, Unterzeichnung von Verpflichtungserklärungen der Mitarbeiter und bei Verstößen Disziplinarmaßnahmen

  – Realisierung eines Zugriffs- und Zutrittsschutzkonzepts

- *Evaluierung und Aktualisierung*:
Die Evaluierung besteht in der Überprüfung durch die Mitarbeiter, interne oder externe Audits dahingehend, ob alle eingesetzten Sicherheitsmechanismen ordnungsgemäß funktionieren und evtl. noch unbekannte Sicherheitslücken bestehen. Sollten Mängel gefunden werden, sind diese durch eigene Änderungen innerhalb des Sicherheitsmanagements oder durch RfC´s (wenn mehrere Prozesse beteiligt sind) abzustellen.

- *Steuerung*:
Unter Steuerung wird die Erstellung von Sicherheitsgrundsätzen und der organisatorische Aspekt der Informationssicherheit zusammengefaßt.
Die Sicherheitsgrundsätze umfassen beispielhaft:

- Zielvorgaben, allgemeine Prinzipien und Bedeutung
- Beschreibung der Teilprozesse
- Zusammenarbeit mit anderen Prozessen
- Vorgehen bei Sicherheitsstörungen.

Die Organisation der Informationssicherheit beinhaltet die

- Erstellung eines Managementrahmens
- Aufbau einer Organisationsstruktur und Zuteilung von Verantwortlichkeiten
- Beschreibung der Autorisierungsprozesse
- Zusammenarbeit mit Dritten (Sicherheitsrichtlinien, Realisierung durch Dritte bei Fremdvergabe, Beratungstätigkeit und Auditgestaltung)

6.5.6.5 Prozeßsteuerung

Wie bereits in der Prozeßbeschreibung (siehe 6.5.6.3) erläutert, hat das Security-Management regelmäßig Berichte über die Einhaltung über den Grad der im SLA vereinbarten Parameter und Kriterien sowie über Sicherheitsvorfälle und die eingeleiteten Maßnahmen zu erstellen.
Darüber hinaus sind diese Berichte auch für das eigene Management zu erstellen und zusätzlich noch Berichte hinsichtlich der eigenen Organisation anzufertigen (Qualität des Prozessverlaufs, interne Sicherheitspläne, Fortschritte in der Sensibilisierung des Personals, ...). Diese Berichte dienen zur Einleitung von Maßnahmen zur Verbesserung der inneren Organisation des Security-Managements.

6.5.7 Continuity-Management

6.5.7.1 Zielsetzung

Die Aufgabe des Continuity-Management liegt in der Unterstützung des übergeordneten Business Continuity-Management (BCM), indem sichergestellt wird, daß der Geschäftsbetrieb nach einer Katastrophe möglichst rasch wiederhergestellt werden kann ([ITSM04]). Für IT-Services ist ein Teilbereich des BCM das ITSCM (IT Service Continuity-Management, das im Katastrophentfall für eine schnelle Wiederherstellung der IT-Infrastruktur und der IT-Services verantwortlich ist. Beide Teilgebiete sind sehr eng miteinander verzahnt, da ohne funktionierende IT-Systeme meist kein ordnungsgemäßer Geschäftsbetrieb möglich ist.

6.5.7.2 Prozeß

Die Hauptaufgaben des Continuity-Managements bestehen in

- der Einschätzung der Folgen einer Katastrophe auf den Geschäftsbetrieb
- der Ermittlung geschäftskritischer Dienste, für die zusätzliche Maßnahmen ergriffen werden müssen
- der Ergreifung von Maßnahmen, um Katastrophen vorzubeugen oder zu verringern
- der Erarbeitung eines Kontinuitätsplans, in dem ausgeführt wird, wie mit einer Katastrophe umzugehen ist und wie die notwendigen Dienste wiederhergestellt werden können ([BKP02]).

Im Proeß des Continuity-Managements (ITSCM) sind folgende Teilschritte abzuarbeiten:

- Festlegung des Umfangs des ITSCM:
  Zu Beginn des ITSCM ist die Organisation einer Prüfung zu unterziehen, die die Aktivitäten Festlegung von Grundsätzen, Definition der Schwerpunkte und des Umfangs (z.B. für Versicherungen), Ressourcenzuweisung und Einrichtung einer Projektorganisation umfaßt.

- Business-Impact-Analyse:
  Die Erstellung der Business-Impact-Analyse dient der Verdeutlichung der Auswirkung einer Katastrophe und der damit verbundenen Ausfälle auf das Unternehmen (Marktanteils- und Umsatzverlust, Imageschaden, Verlust von Kunden, ...). Zusätzlich sind die Dienste und Infrastruktur einer Analyse hinsichtlich der Wichtigkeit für den Geschäftsbetrieb zu definieren. Kommunikationsdienste gehören hierbei zu den kritischen Diensten bzw. Systemen, die nach einer Katastrophe primär wiederherzustellen sind, da hiervon die meiste Außenwirkung eines Unternehmens ausgeht.

- Risiko-Analyse:
  Um die Bedrohungen zu ermitteln, ist für das Unternehmen eine Risiko-Analyse zu erstellen. Hierzu sind die Betriebsmittel (gesamte Infrastruktur und insbesondere IT-Infrastruktur) zu ermitteln; diese sind möglichen Bedrohungen und Abgängigkeiten für das Eintreten einer Katastrophe (z.B. unzuverlässige Stromversorgung, Unwetter, Bedrohung durch terroristische Angriffe) sowie der jeweiligen Eintrittswahrscheinlichkeit gegenüberzustellen. Danach werden die Schwachstellen (fehlende Blitzableiter, ungenügender Wachdienst, ...) ermittelt und ebenfalls bewertet.
  Schließlich werden die Bedrohungen und Schwachstellen den Betriebsmitteln gegenübergestellt und so die Risiken ermittelt, wobei in den letzten Jahren tendenziell die Gefahr von Terrorismus (z.B. Bombenanschläge) gegenüber klassischen Katastrophen (Brand, Gebäudeeinsturz, ...) – v.a. für bestimmte Branchen – deutlich zugenommen hat; dies ist in diesen Branchen besonders zu berücksichtigen.
  Die folgende Abbildung illustriert das Vorgehen der Risikoermittlung und -bewertung nochmals.

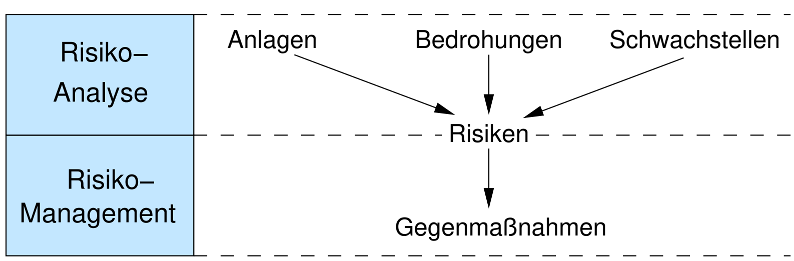

Abbildung 6.12: Risk-Assessment-Modell

- Erstellung einer Kontinuitätsstrategie:
  Ausgehend von der Risikoermittlung erfolgt die Erstellung einer Kontinuitätsstrategie, die die Elemente Risikobegrenzung und Wiederherstellungsplanung als Gegenmaßnahmen auf die Risiken enthält.
  Präventivmaßnahmen werden größtenteils mit dem Availability-Management abgeckt (siehe Kapitel 6.5.5), das bei VoIP einen der zentralen Prozesse darstellt, da die Verfügbarkeit im Kommunikationsbereich einen sehr hohen Stellenwert hat (Kapitel 4.1.3).
  Wenn Präventivmaßnahmen das Risiko nicht abdecken können, ist für diese Risiken die Erstellung einer Kontinuitätsstrategie zu ermitteln. Diese beinhaltet die Möglichkeiten

  - Nichts tun („Vogel-Strauß-Politik“)
  - Manueller Rückgriff
  - Wechselseitiges Abkommen (Vereinbarung zweier Unternehmen zur gegenseitigen Unterstützung im Katastrophenfall bei etwa gleichartiger Infrastruktur)
  - mehrere Wiederherstellungsvarianten (schrittweise innerhalb bestimmter Zeiträume: Tage/-

Stunden/sofort): hierbei ist das Vorhalten eines alternativen Standorts (intern oder extern), mobiler Ersatz oder redundante Systeme (z.B. Dopplung von Systemen) möglich.

  – Kombination obiger Möglichkeiten

- Erstellung eines Wiederherstellungsplans, Schulung der Mitarbeiter, Tests:
  Nach der grundlegenden Festlegung auf die Wiederherstellungsoptionen ist ein Wiederherstellungsplan zu erstellen, der alle Beschreibungen, Verfahren und Komponenten sowie Zuständigkeitsverteilungen für den Katastrophenfall enthält, die zur Wiederherstellung notwendig sind. Er ist allen notwendigen Institutionen und Prozessen bekannt zu geben und zu verteilen; für eine erfolgreiche Implementierung ist die aktive Teilnahme des Managements sowie die Unterstützung aller Mitarbeiter im gesamten Unternehmen erforderlich.
  Darüberhinaus sind die relevanten Mitarbeiter zu schulen und der Wiederherstellungsplan in regelmäßigen Abständen – falls möglich – zu testen und auf die Wirksamkeit zu überprüfen.

Das ITSCM arbeitet mit allen anderen ITIL-Prozessen zusammen, wobei diese Prozesse dem ITSCM die Grunddaten für eine Planung des Katatstrophenfalls liefern (SLA´s, Aufbau und Konfiguration der IT-Infrastruktur, Ressourcenplanung, ...) und ihrerseits Maßnahmen zur Verringerung des Katastrophenrisikos treffen (Präventivmaßnahmen, ...).

6.5.7.3 Aktivitäten bei VoIP

Die VoIP betreffenden Aktivitäten beim ITSCM stützen sich primär auf die klassischen Aufgaben zum Betrieb einer IT-Infrastruktur ab (Aufrechterhaltung und Wiederherstellung des Datennetzes); dies würde den Rahmen der Diplomarbeit sprengen – daher werden im folgenden die allgemeinen Aktivitäten des ITSCM kurz erläutert und die VoIP- bzw. kommunikationsspezifischen Problempunkte angesprochen.

- Festlegung des Umfangs des ITSCM:
  Das ITSCM bei VoIP-Systemen zielt auf einer raschen Wiederherstellung des Kommunikationsdienstes, da von der Erreichbarkeit des Unternehmens eine große Außenwirkung ausgeht.

- Business-Impact-Analyse:
  Da VoIP einen Teil der Kommunikationsinfrastruktur darstellt, und ein funktionierendes Kommunikationssystem für Unternehmen „lebenswichtig“ ist, stellt ein Ausfall nach einem unvorhersehbaren Ereignis eine sehr große Bedrohung für den Fortbestand des Unternehmens dar. Es sollte daher als erstes wieder in Betrieb genommen werden.

- Risiko-Analyse:
  Das Continuity-Management zielt auf die Vorbereitung gegen unvorhergesehene Ereignisse (wie z.B. Erdbeben, Brand, ...), die meist einen großen Teil des Gebäudebestandes des Unternehmens unbrauchbar machen bzw. zerstören, sodaß die Daten- und/oder Telekommunikationsinfrastruktur nicht mehr funktionsfähig ist. Bei VoIP – das gemäß der Intention dieser Diplomarbeit bei Endkunden eingesetzt wird (siehe Kapitel 3.1.4) – empfiehlt sich, falls das Datennetz sehr schnell wiederhergestellt werden kann (innerhalb weniger Stunden), das Vorhalten von Ersatzkomponenten (Zentralkomponenten, Endgeräte) oder eine Vereinbarung mit Externen zur Lieferung dieser Komponenten, um ein allmähliches bzw. schnelles Wiederaufsetzen zu ermöglichen.
  Falls die Wiederherstellung des Datennetzes einen längeren Zeitraum in Anspruch nimmt, sollte ein Notbetrieb mit konventioneller TK-Technik in Betracht gezogen werden.
  Im Fall des Verlusts der kompletten Infrastruktur (z.B. nach einem Brand), ist in alternative Gebäude umzuziehen (intern im Unternehmen oder durch Anmietung von fertig ausgestatteten (Büro)-Räumen).
  Zur Konfiguration der Systeme können die im Rahmen des Availability-Managements (Kapitel 6.5.5.4) erstellten Sicherungen der Zentralkomponenten verwendet werden.

- Kontinuitätsstrategie, Erstellung eines Wiederherstellungsplans, Schulung der Mitarbeiter, Tests:

Hierzu können keine konkreten Aussagen gegeben werden, da diese Aspekte unternehmensspezifisch geregelt werden müssen und hierbei die Unternehmensphilosophie eine große Rolle spielt.

6.5.7.4 Prozeßsteuerung

Zur Implementierung des Continuity-Managements ist ein Prozeßmanager zu benennen, der für die Erstellung der Wiederherstellungspläne verantwortlich ist und direkt der Geschäftsleitung untersteht. Im Katastrophenfall sollte dieser – neben der Geschäftsleitung – weitgehende Entscheidungsbefugnisse (auch in anderen Zuständigkeitsbereichen) erhalten. Er ist zur laufenden Berichterstattattung an die Geschäftsleitung verpflichtet.
Problemfelder und Hindernisse im Continuity-Management liegen im teilweise fehlenden Bewußtsein der Mitarbeiter und den zur Aufrechterhaltung des Continuity-Managements anfallenden Kosten; hierzu ist anzumerken, daß diese Mittel gut angelegt sind, da diverse Unternehmen nach Katastrophen in ihrer Existenz bedroht waren und diejenigen, die eine Katastrophenvorsorge geplant haben, im Markt bestanden und sogar weitere Kunden dazugewonnen haben. Beispiele hierzu sind in den Folgen der Terroranschläge des 11. September 2001 zu finden, bei denen das World-Trade-Center in New York eingestürzt ist und weitere Bürogebäude in der Nähe unbenutzbar wurden; dies führte zum Verlust Zehntausender Quadratmeter Büroraums im größten Finanzzentrum der Welt, da die Wall Street (Börse) nur einige Straßen entfernt liegt und in den beeinträchtigten Gebäuden sehr viele Finanzinstitute und Dienstleistungsunternehmen untergebracht waren.

6.5.8 Zusammenfassung – Design-/Planungskonzept für VoIP-System

In den vorhergehenden Abschnitten wurden die planerischen Komponenten für den Einsatz eines VoIP-Systems vorgestellt. Das Hauptaugenmerk lag hier darauf, in dem Spannungsfeld Verfügbarkeit und Zuverlässigkeit des Dienstes gegenüber finanziellen Aspekten einen vernünftigen Ausgleich zu finden. Die Vergabe von Tätigkeiten an Externe wurde auf ein Minimalmaß begrenzt (im Gegensatz zum derzeit vorherrschenden Trends des Outsourcings – auch von Kernbereichen); die kommunikationstechnische Erreichbarkeit eines Unternehmens stellt derzeit einen unverzichtbaren Bestandteil der Außenwirkung dar und ist somit ein Kernbereich in der EDV-/IT-Infrastruktur. Bei Implementierung der gegebenen Anregungen – die viele Elemente präventiver Wartung und Vorsorge beinhalten – werden Externe nur in Extremfällen als letzte Risikoabsicherung benötigt. Darüberhinaus nutzt ein VoIP u.a. das Datennetz und sonstige Infrastrukturkomponenten eines Unternehmens, die das Rückgrat einer Kommunikationsarchitektur darstellen und somit wegen der direkten, schnellen Eingriffsmöglichkeit nicht an Externe vergeben werden sollten (das Management und der Betrieb des Datennetzes und von Telekommunikationssystemen stellen eine der Kernkompetenzen einer IT-Abteilung dar).
Im den nächsten Abschnitten werden die planerischen Aspekte für die Installation eines VoIP-Systems und die Inbetriebnahme nochmals zusammengefaßt. Eine organisatorische Übersicht über die gesamten Prozesse und Funktionen erfolgt in Abschnitt 6.7.

6.5.8.1 Konzeption eines VoIP-Systems

Dieser Abschnitt faßt das Designkonzept für ein VoIP-System zusammen und ist in die Unterpunkte bauliche Infrastruktur, Technik, Administration, Finanzen und Vertragsmanagement aufgeteilt, wobei hier teilweise nur die Problemkreise genannt werden, da viele Dinge unternehmensspezifisch geregelt werden müssen.

- bauliche Infrastruktur:
  achtadrige strukturierte Verkabelung mit dem Medium Kupfer im Tertiärbereich (Cat. 6 oder 7), im Primär- und Sekundärbereich Verwendung des Mediums Glasfaser; Einhaltung der Längenbeschränkung für LAN-Segmente im Tertiärbereich (etwa 90m), Klimatisierung der Verteilerräume

- Technik:
  - zusätzliche Anforderungen an Netzkomponenten: Unterstützung der Standards IEEE 802.1p/q sowie 802.3af
  - Netzdesign: redundante, getrennte Leitungswege im Primär- und Sekundärbereich sowie redundante, hot-standbyfähige Komponenten (impliziert Verwendung von STP und OSPF), Trennung von Sprachdaten, Signalisierungsdaten und sonstigen Daten in separate VLAN´s (Verkehrsseparierung)
  - Zentralkomponenten: Einsatz redundanter Systeme, Absicherung gegen Hardwaredefekte im Servicevertrag mit Externem (mit garantierten Reaktionszeiten), Datensicherungskonzept (für Wiederherstellung bei Hardwaredefekten und im Katastrophenfall)
  - Stromversorgung: Absicherung der Zentralkomponenten, Netzkomponenten und Carrier-/Außenanbindungen mit Batterien und Wechselrichtern oder USV´en
  - Sicherheit: Zugänge für Externe (z.B. Wartung) nach Möglichkeit vermeiden (wenn trotzdem nötig: Trennung vom Datennetz (Viren- und Einbruchgefahr) unter Verwendung von Rufnummernidentifizierung, Callback und zumindest verschlüsselter Paßwortübermittlung); Abschottung der Subnetze der Zentralkomponenten und VoIP-Endgeräte durch Firewalls oder Routingbeschränkungen
- Administration: Konzepterstellung
  - Routing-/LCR-Konzept (externes Routing): Implementierung alternativer Wegewahlen bei Leitungsausfall (die meisten VoIP-Systeme lassen derzeit nur feste Routingtabellen zu), korrekte Rufnummernmodifikation, Verhinderung von Breakthrough-Szenarien
  - Aufbau des Firmenverbunds (evtl. mehrere VoIP-Systeme) und Applikationsserver (z.B. UMS, CTI)
  - Rufnummernplan (internes Routing): Erstellung eines Rufnummernplans (offene oder verdeckte Nummerierung, d.h. bei offener Nummerierung läßt sich über die Nummer bzw. die Nebenstelle direkt ermitteln, an welchem System/Standort sich der Anwender befindet)
  - Berechtigungskonzept: Definition von Richtlinien über Nummernbereiche, die von den Anwendern direkt (ohne Zuhilfenahme der Telefonvermittlung) gewählt werden (Bsp.: Mitglieder der Geschäftsleitung dürfen internationale Ziele anwählen, sonstige Anwender nicht), sowie Nummernbereiche, die generell gesperrt werden (z.B. 0190er-Nummern)
  - Leistungsmerkmalkonzept: Erarbeitung von Standards, welche Leistungsmerkmale welchen Mitarbeitern zur Verfügung stehen (Mitarbeiterkreis A darf Rufnummernunterdrückung aktivieren, z.B. in Callcentern, Mitarbeiterkreis B nicht)
  - Konzeption Monitoring- und Überwachungssystem (basierend auf dem Internet-Management)
- Finanzen:
  - Vergleich VoIP-Systeme verschiedener Hersteller und konventionelles TK- gegenüber VoIP-System (Barwertmethode)
  - Konzeption variable Kosten: Accouting-Management (Architektur, Collecting, Tariftabellen, . . .)
  - Erstellung Kostenverrechnungsschlüssel für Fixkosten
- Vertragsmanagement:
  - Abschluß von SLA mit dem Nutzer

- Verträge mit Externen: Abschluß von Servicevertrag zur Wartung sowie Verträgen mit Carrieren oder Leitungsanbietern (jeweils mit SLA, das die Obergrenze des eigenen SLA mit dem Nutzer darstellen sollte)
- Anbieterauswahl für Ersatzbeschaffungen und Aufbau Ersatzteilbestand von Massenware

6.6 Laufender Betrieb

Das Betriebskonzept befaßt sich mit den Prozessen

- Incident-Management
- Problem-Management
- Configuration-Management
- Change-Management
- Release-Management

und der Funktion des Service-Desks.
Der Service-Desk und die genannten Prozesse werden in den folgenden Abschnitten erläutert.

6.6.1 Service Desk

6.6.1.1 Zielsetzung und Aktivitäten

Der Service-Desk hat die *Erreichbarkeit* der IT-Organisation zu garantieren und die in den SLA´s vereinbarten Dienste zu unterstützten. Er ist die *einzige* Schnittstelle des Anwenders und *koordiniert* die nachfolgenden Supporteinheiten ([BKP02]).
Hierzu hat er die eingehenden Störungen (Incidents) und Anfragen (Service Requests) anzunehmen, zu kategorisieren und – falls sie von ihm nicht gelöst werden können – folgenden Einheiten weiterzuleiten und diese zu koordinieren.
Die wichtigste Zusammenarbeit besteht mit dem Incident-Management, denn der Großteil der eingehenden Meldungen sind Störungen. Darüber hinaus kann er mit der Annahme und Realisierung von Standardaufträgen im Rahmen des Change-Managements betraut sein (Installation von Hard-/Software, Durchführung von Arbeitsplatzumzügen, ...). Ein weiteres Aufgabengebiet liegt in Teilgebieten des Configuration-Managements, da er bei der Aufnahme einer Anfrage verifiziert, ob die Realität der IT-Komponenten noch mit den im Configuration-Management gespeicherten Daten übereinstimmt ([OGC00]).
Durch seine Nähe zu den Anwendern ergibt sich für den Service-Desk eine gute Möglichkeit, die Zufriedenheit der Anwender festzustellen.

6.6.1.2 Implementierung für VoIP-Systeme

Die Implementierung und Installation eines Service-Desks lässt sich in folgende Aspekte unterteilen, wobei jeweils auch ein Vorschlag für VoIP-Systeme gegeben wird:

- Erreichbarkeit und Technologien:
  Dreh- und Angelpunkt einer Service-Desk-Organisation ist die Gewährleistung der Erreichbarkeit der IT-Organisation für die Anwender (siehe 6.6.1.1). Daher hat er während der im SLA vereinbarten Zeiträume präsent und erreichbar zu sein; hierbei sind alle Anwender in der gleichen Weise zu behandeln (z.B. Höflichkeit). Alle Aktivitäten des Service-Desks sollten transparent sein, d.h. die Anwender sollten jederzeit den Status ihrer Anfragen verfolgen können. Hierzu bieten sich Trouble-Ticket-Systeme (TTS) an. Tickets können hierbei entweder manuell durch den Service-Desk erfaßt

oder automatisiert (z.B. durch Monitoringsysteme) erstellt werden und dann auf die Bearbeiter verteilt werden. Alle Meldungen (inkl. Status und Lösung) sind zu erfassen und dienen so zum einen zur Dokumentation der Leistungsfähigkeit des Service-Desks, zum anderen zur Aggregation von Meldungen und zum Aufbau einer Wissensdatenbank.
Die Anwender sollten den Service-Desk über alle zur Verfügung stehenden Kommunikationsmöglichkeiten erreichen können (telefonisch, Fax, E-Mail, ...), wobei sichergestellt sein muß, daß eine Kontaktaufnahme möglich ist (z.B. durch Weiterleitung an Unified-Messaging-Systeme (UMS), auf mobile Endgeräte wie Handys oder Laptops).
Zur Lösung der Anfragen sollten Wissen-, Such- oder Diagnosetools (wie z.B. FAQ, Wissendatenbank) vorhanden sein.
Für den Bereich VoIP ergeben sich hier keinerlei Besonderheiten.

- Organisation: Die Organisation des Service-Desks lässt sich in funktionale und räumliche Gesichtspunkte unterteilen.
  - Funktional:
    Hinsichlich der funktionalen Organisation des Service-Desks gibt es einerseits die Möglichkeit, mehrere Service-Desks für verschiedene Anfragebereiche einzurichten (z.B. getrennt für Telefonie- und EDV-Probleme) oder den Service-Desk alle Anfragen aller Bereiche bearbeiten zu lassen. Für den Einsatz von VoIP wird empfohlen, für den Bereich Telekommunikation keinen eigenen Service-Desk, sondern einen für alle Bereiche aufzubauen, da VoIP-Systeme und EDV-Bereich z.B. durch die Nutzung einer gemeinsamen Infrastruktur eng verzahnt sind und sonst Kommunikationsprobleme zwischen verschiedenen Service-Desk-Organisationen (Unwissenheit, Mißverständnisse, ...) entstehen können, was zu Unzufriedenheit unter den Anwendern führt.
  - Räumlich:
    Für die räumliche Realisierung eines Service-Desk bestehen die Möglichkeiten eines
    * zentralen Service-Desks, d.h. es existiert nur ein Service-Desk für das gesamte Unternehmen, was nur eine Kontakadresse für alle Anwender bedeutet. Da dies einen relativ großen Service-Desk (personell und räumlich) impliziert, bietet sich zusätzlich die Möglichkeit, eine eigene Gruppe nur für Anfragen – nicht für Störungen – einzurichten, da die reinen Anfragen einen Großteil der eingehenden Meldungen ausmacht.
    * lokalen Service-Desks, d.h. jeder Service-Desk befindet sich an einem anderen Standort und ist für diesen Standort zuständig). Hierbei besteht noch die Möglichkeit, einen zentralen Service-Desk als alleinige Anlaufstelle einzurichten (dieser verteilt die Anfragen an die jeweiligen lokalen Service-Desks) oder einen zentralen Service-Desk zur Koordination und Unterstützung der lokalen Service-Desks einzusetzen (die Anwender wenden sich an den jeweiligen lokalen Service-Desk). Die Nachteile dieser Lösung bestehen in den hohen Kosten (pro Standort ist mindestens ein Mitarbeiter anzusetzen – inkl. Urlaubs- und Krankheitsvertretungen; bei kleinen Standorten führt dies zu überproportionalen Personalkosten).
    * virtueller Service-Desks, der sich aus mehreren lokalen Service-Desks zusammensetzt, die eine virtuelle Einheit bilden. Dies ist eine spezielle Form des Service-Desks, der unabhängig vom Standort ist. Somit ist es unerheblich, wo sich der Service-Desk und die Lösungsgruppen befinden, was die Möglichkeit eröffnet, einen Rund-um-die-Uhr-Support anzubieten (bei Besetzung in mehreren Ländern und Kontinenten). Nachteilig hieran ist, daß ein Vor-Ort-Service fast unmöglich ist.

Hinsichtlich der Organisation eines Service-Desks, der auch für VoIP-Systeme zuständig ist, bestehen für jedes Unternehmen verschiedene firmenpolitisch geprägte Präferenzen, da jedes der Konzepte ein anderes Ziel (mit den daraus resultierenden Nachteilen) verfolgt; eine generelle Empfehlung kann daher nicht gegeben werden (es sollte – auch bei einem virtuellen Service-Desk – auch die Möglichkeit vorhanden sein, in bestimmten Zyklen einen Vor-Ort-Service anzubieten, da bei

VoIP ein Ausfall von Endgeräten die Kommunikationsmöglichkeiten des Anwenders u.U. stark eingeschränkt).

- Besetzung: Hinsichtlich der personellen Struktur des Service-Desks bestehen die Alternativen des Einsatzes
  - eines Call-Centers (mit unqualifizierten Mitarbeitern): Hier erfaßt das Personal lediglich die Anfragen und leitet sie an die spezialisierten Einheiten weiter. Vorteil hierin liegt in der einheitlichen Erfassung der Anfragen; nachteilig ist die längere Reaktionszeit durch eine zusätzliche Kommunikations- (und Übermittlungsstufe).
  - von qualifizierten Mitarbeitern: Dieser Service-Desk erfaßt nicht nur die Anfragen, sondern versucht aufgrund seiner Sachkenntnis, alle Anfragen und Störungen, die er abarbeiten kann, zu lösen. Dies bedeutet, daß ein Großteil aller Anfragen schnell erledigt werden kann (die Mehrzahl der Meldungen betreffen „einfache" Störungen oder Anfragen); ein gewisser Teil wird aber immer noch an Spezialisten zur Lösung weitergeleitet.
  - von „Experten": Bei dieser Alternative können die Service-Desk-Mitarbeiter durch ihr umfassendes Wissen und ihre weitreichenden Kompetenzen fast alle Störungen selbst lösen, sodaß nur noch ein kleiner Anteil an die Spezialisten weitergeleitet werden muß. Der Nachteil hieran besteht in den höheren Kosten für die Service-Desk-Mitarbeiter und dem höheren Schulungsaufwand für diesen Personenkreis).

  Auch hier kann – bedingt durch firmenbezogene Strategien – keine Empfehlung bezugnehmend auf den Einsatz eines VoIP-Systems gegeben werden (für den Einsatz eines VoIP-Systemes sind alle Alternativen geeignet; sie haben jeweils Vor- und Nachteile, die unter Berücksichtigung der Unternehmensspezifika beurteilt werden müssen).

6.6.1.3 Erfolgsfaktoren

Die Erfolgsfaktoren eines Service-Desks bestehen in seiner Erreichbarkeit und Effizienz.
Ist die Erreichbarkeit des Service-Desks nicht gegeben, versuchen die Mitarbeiter, die Probleme selbst oder durch direkte Kontaktaufnahme mit den spezialisierten Einheiten (Incident-Management, Problem- oder Change- Management, ...) zu lösen, was die Dokumentation aller aufgetretenen Störungen und Anfragen unmöglich macht (direkte Kontaktaufnahme der Anwender mit den „Spezialisten" ist aus diesem Grund zurückzuweisen und die Anwender an den Service-Desk weiterzuleiten).
Die Effizienz des Service-Desks mißt sich u.a. an

- der Anteil an Störungen, die direkt gelöst werden können
- der Gesamtzahl der Anfragen und der Verteilung an die Mitarbeiter des Service-Desks
- dem durchschnittlichen Zeitaufwand der Lösung von Störungen
- Statistiken über die Erreichbarkeit (Dauer, bis Anruf entgegengenommen wird, Dauer des Telefonats, Auflegen des Anrufers).

Bei allen Verfahren zur Effizienzbestimmung wird auf die mitbestimmungsrechtliche Problematik hingewiesen, da der Betriebsrat vielen Kontroll- und Überwachungsinstrumenten zustimmen muß (hier ist der Rückschluß auf die Arbeitsleistung des Mitarbeiters möglich).

Zusammenfassend ergeben sich an den Service-Desk (beim Einsatz eines VoIP-Systems) keine besonderen Anforderungen; die Entgegennahme aller Maßnahmen, die VoIP-Systeme betreffen, sollten – wie in 6.6.1.2 erläutert – in eine bestehende Service-Desk-Organisation integriert werden.

6.6.2 Incident-Management

6.6.2.1 Begriffsdefinitionen

Incident: Eine Störung (Incident) ist ein Ereignis, das nicht zum standardmäßigen Betrieb eines Dienstes gehört und tatsächlich oder potentiell eine Unterbrechung oder eine Minderung der Service-Qualität verurusacht.

Service-Request: Anfrage des Anwenders bezüglich eines Dienstes, die keine Störung (Incident) im eigentlichen Sinn darstellt. Beispiele: Anfrage zu Handhabung oder Funktionalität (RFA), Passwortrücksetzung (RFI), Installation neuer Hard- oder Software (RfC)

Problem: Ursache eines oder mehrerer Störungen. Die Analyse von Incidents (reaktiv) sowie Trendbeurteilung (proaktiv) lassen Probleme (Fehlerursachen) erkennen und sorgen so für eine grundsätzliche Behebung bzw. Vermeidung von Störungen.

Known Error: Problem, dessen Ursache erfolgreich festgestellt wurde.

Workaround: Übergangslösung, die dem Incident-Management zur Verfügung gestellt wird, bis das Problem gelöst ist.

Request for Change: Vorschlag bzw. Forderung einer Änderung (z.B. zur Problemlösung).

Priorität: Merkmal zur Steuerung der Störungsbearbeitung. Einflußgrößen für die Priorität sind Auswirkung (Folgen der Störung auf Aktivitäten des Kunden, Meßgröße: z.B. Anzahl Betroffene) und Dringlichkeit (maximal tolerierbarer Verzug der Störungsbeseitigung aus Sicht des Kunden).

Eskalation: Mechanismus, der Behebung von Störungen unterstützt; Eskalation ist notwendig, wenn eine Störung nicht von der jeweiligen Instanz oder nicht innerhalb einer vereinbarten Zeit behoben werden kann. Sie lässt sich in funktionale (Weiterleitung einer Störung an und Anforderung von Spezialisten) und hierarchische Eskalation (Einschaltung übergeordneter Weisungsgeber aus der Aufbauorganisation, wenn die funktionale Eskalation nicht zum Erfolg führt) unterteilen.

Multi-Level-Support: Mitarbeiter verschiedener Funktionen werden Support-Teams zugeteilt; wenn eine Störung von einem Support-Team nicht gelöst werden kann (n. Level), wird sie an das nächste (weiter spezialisierte) Supportteam weitergeleitet (n+1. Level).

6.6.2.2 Zielsetzung

Das Ziel des Incident-Managements besteht in der schnellstmöglichen Behebung von Störung, um negative Auswirkungen auf Geschäftsprozesse so gering wie möglich zu halten. Darüber hinaus soll es so die Produktivität der Anwender erhöhen und die generelle Verfügbarkeit des Dienstes verbessern ([ITSM04]). Vorteile des Incident-Managements liegen u.a. in der verbesserten Überwachung der Leistungsfähigkeit (gemäß dem vereinbarten SLA), Berichtswesen für Management und weitere Prozesse, Aktualisierung der CMDB und der Verbesserung der Kundenzufriedenheit.

6.6.2.3 Prozeß

In Abbildung 6.13 sind Eingangs- und Ausgangsgrößen sowie Aktivitäten graphisch dargestellt. Die einzelnen Prozeßschritte und Aktivitäten werden in diesem Abschnitt kurz erläutert (siehe auch [BKP02]).

- Störungsannahme und -erfassung:
  Die Störung wird entweder manuell durch den Service-Desk (sieh Kapitel 6.6.1) oder automatisiert (Meldungen und Ereignisse aus Systemmanagement- und Überwachungssystemen) erfaßt und ein Datensatz (z.B. in TTS) erstellt. Hierbei sollte eine mehrfache Erfassung einer Störung vermieden werden; gleichartige Störungen sind zusammenzufassen und evtl. Prioritätswerte neu zu setzen.

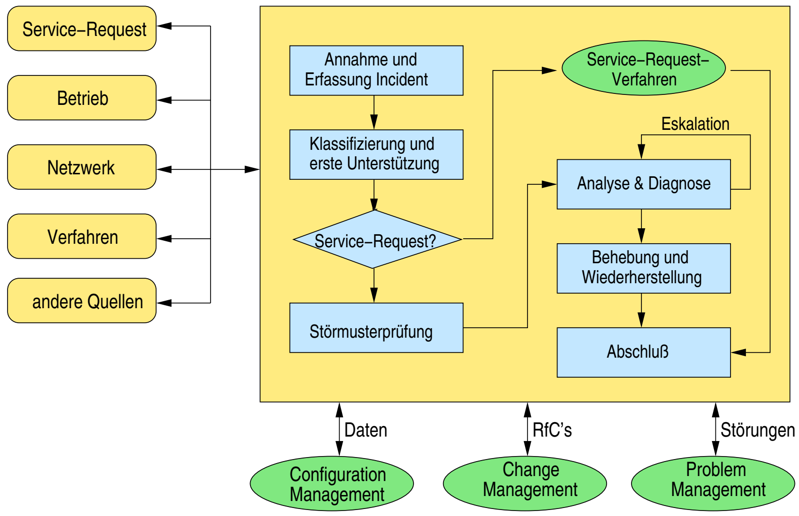

Abbildung 6.13: Prozeß des Incident-Managements

- Klassifizierung und erste Unterstützung:
  Um eine reibungslose Bearbeitung der Incidents zu ermöglichen, werden die Störungen klassifiziert, d.h. in Kategorien (z.B. Netzwerk, Arbeitsplatz eines Anwenders, Service-Request, ...) und – falls möglich – Lösungsmöglichkeiten oder Hinweise zum Fortsetzen der Arbeit gegeben.

- Störmusterprüfung:
  Nach der Klassifikation wird überprüft, ob ähnliche Störungen bereits aufgetreten sind und hierfür bereits Lösungen oder Workarounds verfügbar sind (und mit den bereits bekannten Störungen verknüpft), was Informationen zur Behebung der Störung zur Verfügung stellt.

- Analyse und Diagnose:
  Störungen, für die es noch keine Lösung gibt oder den Kenntnisstand des Mitarbeiters des Service-Desks übersteigen, werden dem jeweiligen Support-Team zugewiesen. Ab diesem Zeitpunkt ist dieses Team für die weitere Bearbeitung zuständig. Der Service-Desk hat jedoch weiterhin die Möglichkeit, in die Abarbeitung einzugreifen.

- Behebung und Wiederherstellung:
  Wenn die Störung analysiert worden ist, eine Lösungsmöglichkeit gefunden wurde und umgesetzt wurde, wird die Lösung im System erfaßt (falls weitere Prozesse wie z.B. das Change-Management benötigt werden, wird dies ebenfalls dokumentiert).

- Abschluß:
  Sobald die Störung behoben wurde (auch unter Zuhilfenahme anderer Prozesse), wird die Störung von der Lösungsgruppe wieder an den Service-Desk gegeben. Dieser hat sich beim Melder der Störung zu vergewissern, ob sie tatsächlich (auch zu seiner Zufriedenheit) behoben wurde. Wenn dem so ist, erfolgt der Anschluß der Störung (wenn nicht, beginnt die Störungsbeseitigung von vorne). Beim Abschluß werden zusätzliche Daten wie in Anspruch genommene Ressourcen, Kategoriezuordnung oder die verursachenden Komponenten aufgenommen (dienen u.a. für das Berichtswesen).

- Verfolgung und Überwachung (ggf. Eskalation):
  Die gesamte Überwachung und Kontrolle der Störungsbeseitigung liegt in der Verantwortung des Service-Desks. Er hat den Anwender über den Status der Störungsbeseitigung zu informieren und ggf. die Störungsbehandlung zu eskalieren.

Schnittstellen zu weiteren Prozessen:

- Configuration-Management: Ermittlung von Informationen über Konfigurationsdaten (und evtl.

Änderung bei Nichtübereinstimmung mit Realität)

- Problem-Management: Unterstützung durch das Problem Management (Lieferung von Informationen über Probleme, bekannte Fehler und Workarounds)
- Change-Management: Entgegennahme und Bearbeitung von Service-Requests durch das Incident-Management (Abwicklung durch das Change-Management); Information des Incident-Managements über Änderungen
- Service-Level-Management: Informationsaustausch hinsichtlich vereinbarter Service-Levels zur Störungsbeseitigung und deren Einhaltung
- Capacity-Management: Informationslieferung des Incident-Managements über Störungen, die wegen fehlender Ressourcen aufgetreten sind (Bearbeitung durch das Capacity-Management).

6.6.2.4 Aktivitäten bei VoIP

Die Aktivitäten des Incident-Managements wurden im vorigen Unterkapitel 6.6.2.3 allgemein vorgestellt und erläutert.
Hinsichtlich des Einsatzes von VoIP ergeben sich grundsätzlich keine Besonderheiten. Die Aufgaben des Incident-Managements für Telekommunikationssysteme (hier: VoIP-Systeme) sollten mit dem Einsatz eines VoIP-Systems in das Incident-Management der EDV-Systeme integriert werden, da sich – wie schon öfter gesagt – VoIP- und EDV-Systeme größtenteils dieselbe Infrastruktur nutzen (bisher ist dies in den meisten Unternehmen getrennt, da zwei getrennte Infrastrukturen für TK- und EDV-Systeme vorgehalten werden).
Die Spezialisten für VoIP-Systeme (wie in 6.5.5.4) sowie Externe als nächsthöhere Supportebene sind in die bestehenden Supportstufen zu integrieren, wobei sie etwa (in der Supporthierarchie) auf der Höhe der Netzwerkspezialisten anzusiedeln sind.
Bezugnehmend auf die Einbeziehung Externer ist die mögliche Inanspruchnahme dieser in den in Kapitel 6.5.5.4 vorgestellten Servicevertrag (abgespeckter Wartungsvertrag) aufzunehmen. Hierbei sind die möglichen Zeiten der Inanspruchnahme der Hotline des Externen (und evtl. von Servicepersonal) und der Personenkreis zu vereinbaren, der Kontakt mit den Externen aufnehmen darf und befugt ist, Aufträge zu erteilen. Die Servicezeiten des Externen sollten hierbei nicht unter denen der vorgeschalteten Supporthierarchiestufe (den Experten für VoIP-Systeme) liegen; wenn dies nicht eingehalten wird, ergeben sich u .U. Wartezeiten für die Störungsbeseitigung, die Einfluß auf den Servicegrad haben. Dies stellt eine Abwägung zwischen den Kosten und der Risikobereitschaft (Wahrscheinlichkeit, daß eigene Experten die Störung nicht selbst beheben können).

6.6.2.5 Prozeßsteuerung

Zur Kontrolle und Überwachung des Prozesses werden Berichte für verschiedene Zielgruppen erstellt und enthalten demzufolge verschiedene Schwerpunktsetzungen. Zielgruppen sind u.a. das Service-Level-Management (Informationen hinsichtlich Qualität der erbrachten Dienste) sowie die Prozeßmanager der in 6.6.2.3 genannten Prozesse, die Verbindungen zum Incident-Management besitzen.
Um die Prozeßqualität messen zu können, sind Leistungsindikatoren nötig, die Grundlage der zu erstellenden Berichte bilden. Beispiel für solche Indikatoren sind: Gesamtzahl der Störungen, durchschnittliche Lösungzeit, Durchschnittskosten je Störung, Erstlösungsquote (Prozentsatz der direkt vom First-Level-Support gelösten Störungen).

6.6.3 Problem-Management

Das Problem ist eng mit dem Incident-Management verwandt, da es „Ursachenforschung“ der Störungen betreibt. Daher wurden die erforderlichen Begriffe „Problem“, „Known Error“, „Workaround“ und „RfC“

bereits in Kapitel 6.6.2.1 erläutert.

6.6.3.1 Zielsetzung

Das Problem-Management hat die nachhaltige Vermeidung von Störungen (Incidents) zum Ziel, wobei hier sowohl proaktive als auch reaktive Maßnahmen eingesetzt werden können und sollen ([ITSM04]).
Die Aufgabe des Problem-Managements besteht darin, dafür zu sorgen, daß

- strukturelle Fehler lokalisiert, dokumentiert und verfolgt werden
- Symptome und Workarounds von Störungen dokumentiert sind
- RfC´s erstellt und eingereicht werden
- neue Störungen verhindert werden
- die Qualität der Infrastruktur und des Prozesses dokumentiert wird.

6.6.3.2 Prozeß

Der Prozeß des Problem-Managements hat Eingangsgrößen, Aktivitäten und Ausgangsgrößen.
Die wichtigsten Aktivitäten (basierend auf [BKP02]) bestehen in der

- Problembehandlung (Problem Control): Definition und Untersuchung von Problemen
- Fehlerbehandlung (Error Control): Kontrollieren von bekannten Fehlern und Vorlage von Änderungsvorschlägen
- Problemverhütung (Proactive Problem Management): Identifizierung potentieller Störungen, bevor Störungen auftreten können.

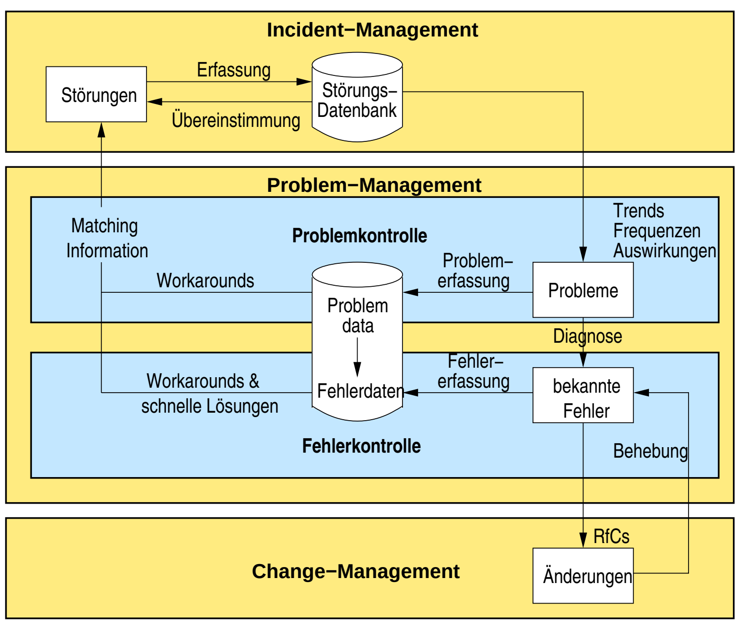

Abbildung 6.14: Zusammenhang zwischen Incident-, Problem- und Change-Management

Die Eingangsdaten stammen in den vom Incident übermittelten Störungen, die Ausgangsgrößen stellen Änderungsvorschläge für das Change-Management (RfC´s) dar. Diese Prozesse unterhalten daher die meisten Beziehungen zum Problem-Management. Abbildung 6.14 illustriert dies und die Abhängigkeiten der

drei Prozesse untereinander graphisch ([OGC00]).
Daneben bestehen weitere Beziehungen zum Availability-Management (gegenseitiger Informationsfluß zur Planung und Realisierung der in SLA´s vereinbarten Verfügbarkeit), Capacity-Management (gleiche Beziehung wie zwischen Incident- und Capacity-Management) und dem Service-Level-Management (Information hinsichtlich der vereinbarten Service-Levels, z.B. zur Dimensionierung proaktiver Maßnahmen im Rahmen des Problem-Managements) dar.

6.6.3.3 Aktivitäten bei VoIP und Prozeßsteuerung

In Anblick der besonderen Spezifika von VoIP-Systemen bestehen beim Problem-Management keine Besonderheiten zu den allgemeinen Empfehlungen hinsichtlich den Aktiviäten und der Prozeßsteuerung, wie sie beispielsweise in [BKP02] gegeben werden.
Auch hier sollte das Problem-Management in bereits bestehende Problem-Management-Prozesse integriert werden. In Anbetracht einer hohen Verfügbarkeitsanforderung (Kapitel 4.1.3 und 6.5.2.4) an VoIP-Systeme sollte ein besonderes Augenmerk auf proaktive Maßnahmen (z.B. zyklische Auswertung von Fehlerprotokollierungsdaten) gelegt werden, da sich v.a. Hardwaredefekte durch vorhergehende Fehlermeldungen ankündigen.

6.6.4 Configuration-Management

6.6.4.1 Begriffsdefinitionen

Configuration Item (CI): für die Erbringung der Dienste notwendige Komponenten, die erfaßt und gepflegt werden

Configuration Management Database (CMDB): Datenbank, die alle relevanten Daten von CI´s sowie die Beziehungen untereinander enthält (z.B. Attribute, Geschichte). Die CMDB stellt hierbei den Sollzustand der Infrastruktur dar; sie ist nicht mit dem Istzustand der Infrastruktur zu verwechseln, die z.B. aus Inventarisierungsprogrammen oder mit Managementwerkzeugen (beispielsweise mit Hilfe des Internet-Managements) generiert werden.

Definite Software Library (DSL), Definite Hardware Store (DHS): Teil der CMDB, der die gesamte vom Release-Management freigegebene Hard- und Software enthält (siehe Kapitel 6.6.6)

6.6.4.2 Zielsetzung

Das Ziel des Configuration-Managements besteht darin, die Überwachung der wirtschaftlichen Bedingungen des IT-Services zu unterstützen, indem ein logisches Modell aus Infrastruktur und Diensten gepflegt wird (die CMDB) und andere Prozesse Informationen hieraus erhalten. Dafür identifiziert, überwacht, kontrolliert und pflegt das Configuration-Management die vorhandenen CI´s und ihre Versionen ([BKP02]). Somit stellt es einen gesicherten Datenbestand der Betriebsmittel und Dienste zur Verfügung. Die Vorteile liegen folglich u.a. in der Verbesserung der Kostentransparenz für die Erbringung der Dienste, einer höheren Betriebssicherheit (Auswirkungen von Änderungen können bereits im Vorfeld ermittelt werden) und einer Grundlage für zukünftige Finanz- und Strategieplanungen.

6.6.4.3 Prozeß

Die Eingangsgrößen des Prozesses des Configuration-Managements sind Änderungsdaten sowie Daten aus dem Einkauf; den Output stellen die CMDB (an die Anfragen von anderen Prozessen gestellt werden können) sowie Berichte an die Prozesse sowie das Management dar.
Innerhalb des Prozesses sind die Aktivitäten

- Planung (Festlegung von Strategien, Grundsätzen und Zielsetzung des Prozesses)
- Identifizierung (Modellierung der CMDB, was auch das Verfahren für spätere Änderungen mit einschließt)
- Kontrolle (Überwachung der CMDB hinsichtlich des ausschließlichen Einsatzes zugelassener Komponenten, der Dokumentation von Änderungen sowie eines konsistenten (aktuellen) Datenbankzustands
- Statusüberwachung (Speicherung und Änderung von Statuszuständen der CI´s)
- Verifizierung (Ermittlung des Istzustands der Infrastruktur und Vergleich mit dem Sollzustand, der CMDB)
- Berichtswesen

einzurichten und auszuführen ([ITSM04]).
Das Configuration-Management unterhält Beziehungen zu verschiedenen Prozessen. Die Beziehungen zum Change- und Release-Management illustriert Abbildung 6.15. Zu den anderen Prozessen werden die

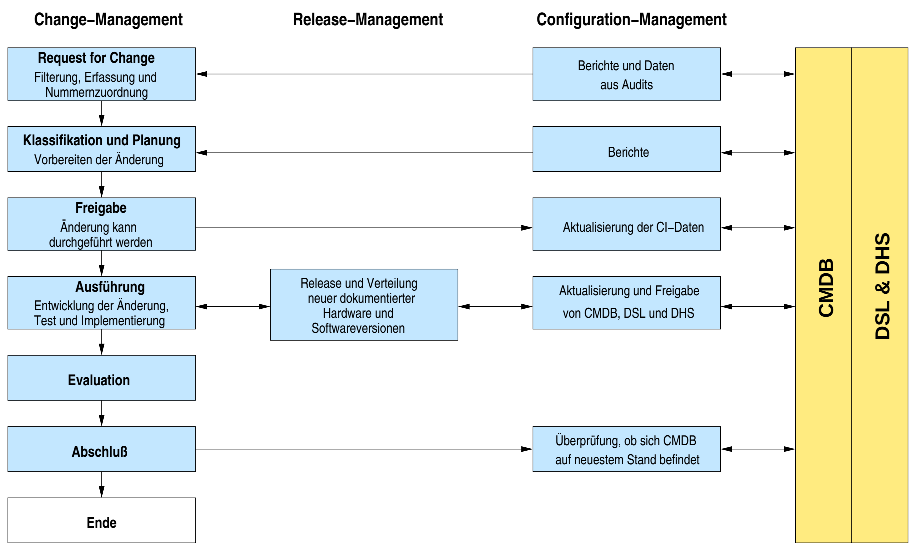

Abbildung 6.15: Beziehungen zwischen Change-, Release- und Configuration-Management

Abhängigkeiten kurz erläutert (siehe auch [OGC00], falls dies nicht bereits beim jeweiligen Prozeß erfolgt ist):

- Problem-/Incident-Management: Lieferung von Informationen zur Störungs- und Problemanalyse (z.B. Verknüpfung von Störungen mit Infrastruktur)
- Service-Level-Management: benötigt Informationen über Eigenschaften der Dienste sowie der zugrundeliegenden Infrastruktur
- Finance-Management: Informationsbedarf hinsichlich der Dienstnutzung (z.B. wer nutzt PC) zur Kostenverrechnung (mit Daten aus SLA und Preisen); außerdem Überwachung und Planung von Investitionen und Betriebsmitteln

6.6.4.4 Aktivitäten bei VoIP und Prozeßsteuerung

Bezogen auf den Einsatz von VoIP-Systemen ergeben sich bei allen Aktivitäten keine Änderungen zu den bisher – im Rahmen des Managements der sonstigen Dienste und Infrastruktur – verwendeten Aktivitäten, Methoden und Modellierungstechniken. Die Komponenten, Dokumentationen und sonstigen Informationen (z.B. über abgeschlossene Verträge) eines VoIP-Systems sind wegen der Integration in eine gemeinsame Infrastruktur (sonstige EDV-Systeme) in die bisher bestehende CMDB zu integrieren. Hierbei ergibt sich die Problematik, daß VoIP-Komponenten spezielle Attribute und Beziehungen besitzen, die „normale“ IT-Komponenten nicht besitzen. Daher wird im Folgenden eine Beispielmodellierung für die VoIP-spezifischen Komponenten vorgestellt (bisher nicht vorhandene Attribute und Beziehungen sind in vorhandene Modellierungen einzubauen). Grundsätzlich ist für die Datenmodellierung das relationale Modell in einer möglichst hohen Normalform zu verwenden, um Redundanzen und Updateprobleme weitestmöglich zu vermeiden (detaillierte Ausführungen hierzu sind [KEI01] zu entnehmen).

- DHS:
  Der DHS enthält alle Hardwarekomponenten, die u.a. für ein VoIP-System erforderlich sind. Dies sind VoIP-Endgeräte, Zentralkomponenten (inkl. evtl. vorhandener Baugruppen), netzwerkspezifische Komponenten (Switches mit PoE-Unterstützung) und sonstiges Zubehör. Beispiel für ein Element des DHS zeigt Tabelle 6.2, wobei hier die Minimalanzahl an Attributen dieser Entität angegeben wird. Erwerbsdaten, Preise und sonstige spezifische Daten sind in einer weiteren Enitität zu speichern (auch bei der DSL).

Attribut	**Beispielwerte**
ID:	12345
Typ:	VoIP-Endgerät
Name:	Optipoint 410 Standard
Hersteller:	Siemens AG
Versionsnummer:	9. Hardware-Build
Bestellnummer:	S123456-789-9
Farbe:	Arctic
Anforderungen an Zentralkomponenten:	Baugruppe STMI-HFA (Nummer xyz)
Freigabedokumentation:	Pfadangabe
Status:	aktiv
Abschreibungsdauer:	3 Jahre
Anmerkungen:	2-zeiliges Display, PoE-fähig, integrierter Mini-Switch, ...
Handbücher, Datenblätter:	Pfadangabe

Tabelle 6.2: Beispiel-Attribute für DHS

- DSL:
  Die DSL enthält die für die VoIP-Endgeräte, Softphones und Zentralkomponenten freigegebene Software. Die Minimalanzahl an Attributen dieser Entität gibt Tabelle 6.3 wieder.

Attribut	**Beispielwerte**
ID:	12345
Typ:	Software für VoIP-Endgerät
Name:	Software für Optipoint 410 Standard (Betriebssystem und Applikation)
Hersteller:	Siemens AG
Versionsnummer:	2.1.5
Lizenzdaten:	nicht erforderlich
hardwareseitige Anforderungen:	optipoint 410 standard (8. build oder später)
softwareseitige Anforderungen:	–
Anforderungen an Zentralkomponenten:	HiPath 4000 V 1.0 Release 12
Speicherort:	Pfadangabe
Freigabedokumentation:	Pfadangabe
Status:	aktiv
Abschreibungsdauer:	1 Jahr
Anmerkungen:	

Tabelle 6.3: Beispiel-Attribute für DSL

- CMDB:
  Die CMDB enthält alle CI´s, die – wie bereits gesagt – nicht nur aus Hard- und Softwarebestandteilen besteht, sondern auch aus Dokumentationen über die Konfiguration, Wartungsverträge, etc. In [BKP02] ist auf Seite 82 eine umfangreiche Beispieltabelle mit Attributwerten angegeben, die für die meisten bei VoIP relevanten Fragestellungen ausreichen dürfte.
  Abbildung 6.16 zeigt ein Grundmodell für den Aufbau einer CMDB für VoIP-Systeme, das im Zuge der Entity-Relationship-Modellierung und der Anwendung des relationalen Datenbankmodells noch erweiterbar ist (eine weitere Detaillierung würde an dieser Stelle den Rahmen der Diplomarbeit sprengen). Dieser Vorschlag stellt, wie in diesem Abschnitt erläutert, einen Teil der Gesamt-CMDB dar und ist nach Möglichkeit in eine vorhandene CMDB zu integrieren.

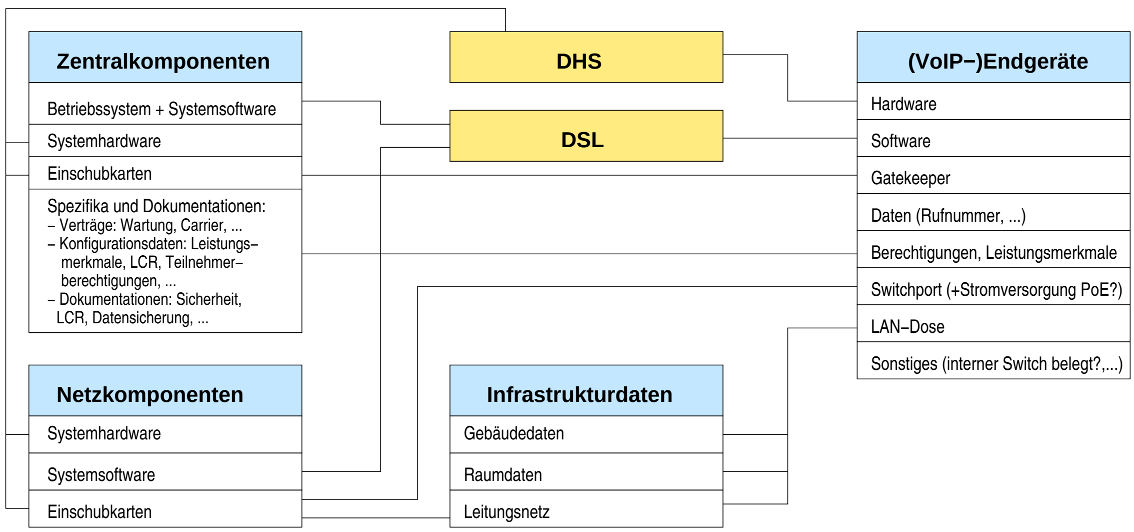

Abbildung 6.16: Mustermodellierung einer CMDB für VoIP-Systeme

- Verifizierung: Hierzu ist ein auf dem Internet-Management basierendes Managementsystem aufzubauen, da die meisten VoIP-Komponenten nur das Internet-Management unterstützen, um den aktuellen Zustand der VoIP-Infrastruktur ermitteln zu können.

6.6.5 Change-Management

6.6.5.1 Begriffsdefinitionen

Request for Change (RfC): Änderungsantrag und Auslöser des Change-Management-Prozesses; kann von jedem Prozeß gestellt werden

Change: angenommer RfC, wird als Change bearbeitet und nach Überprüfung (Audit) abgeschlossen

Change-Advisory-Board (CAB): zyklisch tagendes Kommittee, das über die Annahme und Ausführung der Änderungsanträge entscheidet; es besteht aus ständigen Mitgliedern (z.B. Change-, Security-Manager, Service-Level-Manager) und aus Mitgliedern der von der Änderung betroffenen Prozesse.

Executive Committee (EC): bei dringenden Änderungen Übernahme der Aufgaben des CAB

Forward Schedule of Change (FSC): zu veröffentlichender Zeitplan geplanter Änderungen

Rückfallplan: bei unvorhersehbaren Schwierigkeiten eintretender Notfallplan, der detaillierte Anweisungen zur Rückkehr auf die letzte funktionierende Konfiguration enthält

6.6.5.2 Zielsetzung

Das Change-Management stellt standardisierte Methoden und Verfahren zur Änderungsbearbeitung zur Verfügung und garantiert die Autorisierung und Dokumentation aller Veränderungen der Infrastruktur, was eine schnelle Durchführung von Veränderungen und geringe Auswirkungen die die Servicequalität erreichen soll ([ITSM04]).
Die Ziele des Change-Managements liegen somit in

- Risikominimierung der Durchführung von Änderungen (inklusive Rückfallplan bei unvorhergesehenen Problemem)
- Minimierung negativer Auswirkungen der Änderungen auf die Dienste (insbesondere zur Ausführungszeit der Änderungen)
- Produktivitätssteigerung der Prozesse und Dienste, da die Anzahl ungeplanter Änderungen sinkt und die Koordination aller Beteiligten erhöht wird
- Dokumentation der Änderungen und Lieferung managementrelevanter Daten zur besseren Diagnosemöglichkeit bei Problemen/Störungen.

6.6.5.3 Prozeß

Der Prozeß des Change-Managements wird durch das Einrichen eines RfC (durch einen anderen Prozeß) initiiert. Durch das Change-Management wird der Entscheidungs- und Realisierungsprozeß nachvollzogen. Die einzelnen Phasen und Aktivitäten des Prozesses sowie die Beziehungen zu anderen Prozessen werden

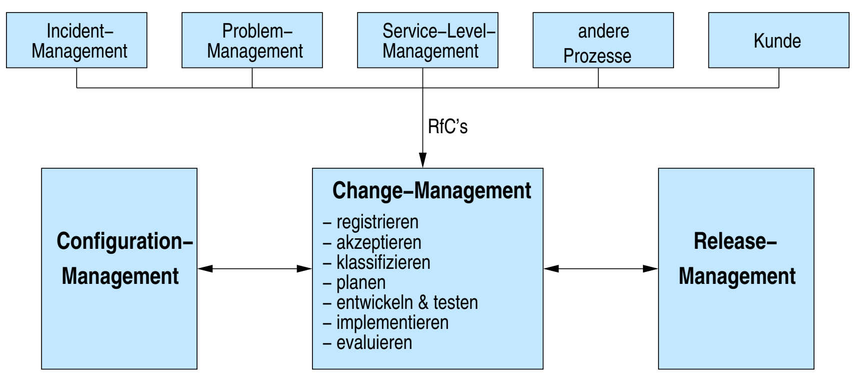

Abbildung 6.17: Prozeß und Beziehungen des Change-Managements

in Abbildung 6.17 illustriert ([OGC00]). Ergebnis des Change-Management-Prozesses sind die Erstellung eines Zeitplans geplanter Änderungen (FSC), Sitzungsdaten für das CAB sowie Managementdaten zur Einarbeitung in die CMDB für das Configuration-Management.
Einige Aktivitäten werden hinsichtlich Ihrer Spezifika kurz erläutert:

- Erfassung und Akzeptanz RfC:
  Der RfC hat vom zur Antragstellung berechtigten Personenkreis gestellt zu werden; andere Anträge sind abzulehnen.
- Klassifikation:
  Jeder RfC ist nach Kategorie und Priorität zu einzuteilen. Folgende Kategorien und Prioritäten sind standardmäßig definiert:
  - Kategorie:
    * Standard/vorautorisiert

    * geringfügig
    * erheblich
    * weitreichend
  – Priorität:
    * dringend
    * hoch
    * mittel
    * niedrig

- Autorisierung:
  Alle Änderungsanträge sind zu autorisieren. Dies geschieht in den allermeisten Fällen durch das CAB; lediglich in dringenden Fällen ist er (der Antrag) sofort auszuführen und durch das EC genehmigen zu lassen.

6.6.5.4 Aktivitäten bei VoIP und Prozeßsteuerung

Beim Einsatz von VoIP-Systemen ergeben sich verschiedene Teilgebiete, auf denen Änderungen erforderlich sein können. Hierbei ist zu beachten, daß – zur Nutzung von Synergieeffekten – bei Umzügen von Mitarbeitern (falls erforderlich) das sonstige EDV-Inventar gleich mitgenommen und am neuen Arbeitsplatz wieder eingerichtet wird.
Die Teilgebiete werden im Folgenden genannt und hierzu beispielhaft die wichtigsten Aktivitäten (mit RfC-Berechtigung, Kategorie/Priorität und Autorisierung und sonstigen eventuellen Besonderheiten angegeben). Zur RfC-Berechtigung wird ein (+) hinzugefügt, falls zusätzlich der betroffene Kostenstellenverantwortliche miteinzubeziehen ist (Entscheidungen, die finanzielle Auswirkungen haben). Zusätzlich werden noch Vorschläge für die Besetzung des CAB und des EC gemacht.

- Teilbereiche:
  – Teilnehmerverwaltung (Berechtigung durch Nutzer, Kategorie: Standard, Priorität: niedrig, Autorisierung: allgemein erteilt)
    * MAC-Szenarien (Umzüge, Namensänderungen, ...)
    * Neueinrichtung/Löschung Teilnehmer (+)
    * Berechtigungs-/Leistungsmerkmaländerung Teilnehmer (+) (z.B. weltweite Berechtigung)
  – Administration Zentralkomponenten (Kategorie: erheblich, Priorität: meist mittel, Autorisierung: CAB)
    * Änderung Routingkonzept (z.B. LCR-Änderungen); Berechtigung: Finance-/Service-Level-/Network-Services-Manager
    * Änderung Berechtigungskonzept (z.B. Sperrung von 0900er-Rufnummern); Berechtigung: Nutzer/Finance-/Service-Level-/Network-Services-Manager
    * Änderung Datensammlung für Accounting-Management (z.B. Aufzeichnung von Interngesprächen zur späteren Kostenverrechnung); Berechtigung: Finance-Manager
  – Implementierung freigegebener Releases (Hard- und/oder Software) (Berechtigung: Release-Management), inklusive kritischer Updates (Autorisierung: EC)
  – Allgemeines

  * Erweiterungen (Hard- und Software für zusätzliche Komponenten wie z.B. Teilnehmer, Anbindungen, Applikationssysteme, Netzkomponenten) (Berechtigung: Capacity-/Finance-/Service-Level-Manager)
  * Pflege der Carriertariftabellen des Accounting-Management (Berechtigung: Finance-Manager; Autorisierung: allgemein erteilt)
  * Management und Pflege Netzkomponenten (Hard- und Softwareaktualisierungen, ...)

- Vorschlag für die Besetzung des CAB:
  - ständige Mitglieder: Change-, Security-, Service-Level-, Network-Services- und Finance-Manager (Manager der bedeutendsten Prozesse)
  - nichtständige Mitglieder: Manager des betroffenen Prozesses
- Vorschlag für die Besetzung des EC:
  - Change-Manger
  - Security-Manager
  - vertretungsberechtigtes Mitglied der Geschäftsleitung (dringende Änderungen können (fast) nicht im Vorfeld getestet werden und sind daher bei der Ausführung deutlich anfälliger; daher für die Genehmigung solcher Änderungen die Geschäftsleitung hinzuziehen, damit sie informiert ist und eventuelle Risiken mitträgt).

6.6.6 Release-Management

6.6.6.1 Begriffsdefinitionen

Release-Einheit: Beschreibung von (zusammenhängender) Hard- und Software, die zusammenhängend getestet, freigegeben und in die Produktivumgebung überführt wird.

Release-Identifikation: Numerierungsvergabe zur eindeutigen Identifizierung von Release-Einheiten

Release-Arten: Unterscheidung nach Umfang

- Delta-Release: enthält nur geänderte Hard-/Software
- Full-Release: Komplettpaket (auch nicht geänderte Komponenten)
- Package-Release: Zusammenfassung mehrerer Releases
- Emergency-Fix: Notfallösung bzw. Sofortbehebung für kritische Probleme oder Fehler

6.6.6.2 Zielsetzung

Die Zielsetzung des Release-Managements besteht in der Kontrolle und Verteilung von produktiv genutzten Hard- und/oder Softwareversionen zur Verbesserung der Servicequalität ([BKP02]).
Als Vorteile ergeben sich beispielsweise die Reduktion von Fehlerquoten im Zuge der Ausbringung neuer Hard-/Softwarekomponenten, die Standardisierung der Komponenten (was zu Kosteneinsparungen führt, siehe Abschnitt 6.1 – Stichwort: Komplexitätsreduzierung) sowie einer leichteren Kontrollmöglichkeit in Bezug auf nicht autorisierte/illegale Komponenten (meist Software: Raubkopien).

6.6.6.3 Prozeß

Der Prozeß des Release-Managements erfaßt in chronologischer Reihenfolge die Aktivitäten Festlegung von Release-Grundsätzen, Entwurf und Entwicklung der Release-Zusammenstellung, Test und Abnahme des Releases, Einführungsplanung Kommunikation und Schulung und Verteilung bzw. Installation des Releases ([ITSM04]). Abbildung 6.18 verdeutlicht den Prozeß des Release-Managements graphisch. Es unterhält eine wechselseitige Beziehung zum Change-Management, die bereits in Abschnitt 6.6.5.3 erläutert wurde. Zu den einzelnen Prozeßschritten werden allgemeine Erläuterungen gegeben:

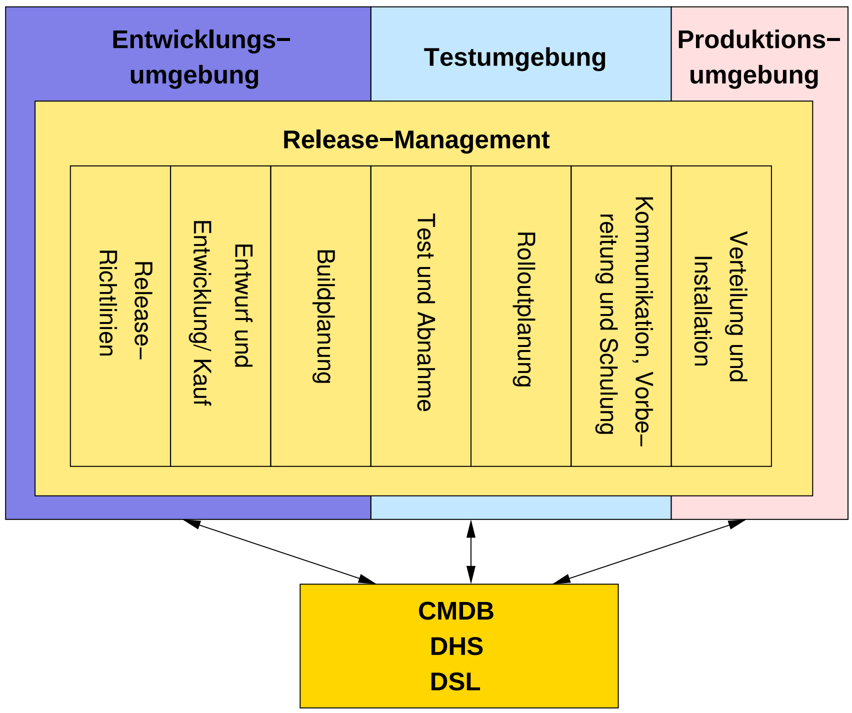

Abbildung 6.18: Prozeß des Release-Managements

- Erstellung von Release-Richtlinien:
  Grundsätze, wie und wann Releases zusammengesetzt und zur Verfügung gestellt werden. Darüberhinaus sind allgemeine Richtlinien zur Releaseplanung festzusetzen (Absprachen mit anderen Prozessen, Bestimmung der benötigten Ressourcen, Beschaffungsplanung sowie die Planung eines Qualitätsplans).
- Entwurf und Entwicklung/Kauf:
  Entscheidung, aus welchen Quellen das Release bezogen wird („Make-or-buy“-Entscheidung, meist ist dies durch proprietäre Komponenten bereits vorgezeichnet); außerdem grundsätzliche Entscheidung, aus welchen Komponenten das Release bestehen und wie die Installation erfolgen wird (Build-Planung); zusätzlich ist ein Notfallplan zu erstellen, falls bei der Implementierung des Releases (schwerwiegende) Probleme auftreten.
- Test und Abnahme:
  Der umfangreichste Teil aller Aktivitäten im Release-Management; hierbei sind alle Releasekomponenten in einer Testumgebung auf Standardinfrastruktur (und ggf. Spezialkomponenten) ausgiebig zu testen (inklusive funktionale Tests durch die Anwender) und alle Schritte und Ergebnisse zu dokumentieren. Zusätzlich sind auch Installationsanweisungen und Notfallpläne sowie evtl. geänderte Ablaufprozeduren zu testen; zusätzlich sind bei den Tests auch Werkzeuge zur automatisierten Verteilung des Releases miteinzubeziehen (Kostenersparnis – insbesondere Personalkostenersparnis).

Nach Abschluß der Tests ist das Release in Zusammenarbeit mit dem Change-Management abzunehmen, da das Change-Management für die Implementierung zuständig ist.

- Rolloutplanung:
  Die Rolloutplanung beinhaltet die Erstellung eines detaillierten Zeitplans sowie die Koordination aller für die Implementierung benötigter Ressourcen; zur Berücksichtigung von Nutzerinteressen ist die Geschäftsleitung (oder Anwender) zu beteiligen.

- Kommunikation und Schulung:
  Information und Einweisung aller vom Release betroffenen Mitarbeiter (z.B. Service-Desk, Incident- und Problemmanagement, primär nicht die Anwender!) über die Releasebestandteile sowie die daraus resultierenden Folgen.

- Verteilung und Installation:
  Das Change-Management führt die eigentliche Implementierung der Releaseänderung durch, da dies eine Veränderung der Systemkonfiguration darstellt (siehe Abschnitt 6.6.5.3). Begleitend hat das Release-Management die Durchführung zu überwachen und insbesondere begleitende Logistik sicherzustellen (z.B. Beschaffung, Lagerung und Lieferung der Komponenten). Abschließend sind die CMDB, der DHS und die DSL zu aktualisieren (falls noch nicht in einem der Schritte vorher geschehen).

6.6.6.4 Aktivitäten bei VoIP

Als Grundsatz für die Releaseplanung bei VoIP ist festzuhalten, daß prinzipiell nur bei Fehlfunktionen oder Problemen sowie beim Vorliegen neuer (benötigter Features) ein Release geplant und implementiert werden sollte („Never change a running system“), da unnötige Releases (die keinen Mehrwert bringen) nur Ressourcen binden und damit Geld kosten sowie die Systemstabilität und Verfügbarkeit des Dienstes beeinträchtigen können (mittlerweile erscheinen z.B. neue Softwareupdates für VoIP-Endgeräte beinahe monatlich). Dies bedeutet aber nicht, daß nur im letzten Ausnahmefall der Releasezyklus in Gang gesetzt wird; für die Releaseplanung ist hier ein Mittelweg zu finden, der beide Aspekte (Kosten) und Mehrwert angemessen berücksichtigt.
Hinsichtlich des Umfangs der Releases handelt es sich bei VoIP-Systemen meist um Delta-Releases, da ein Full-Release zum einen sehr hohen Zeitaufwand (z.B. Komplettinstallation von Software) bedeutet – was die Verfügbarkeit einschränkt – und zum anderen diverse (Hardware-)Komponenten über einen langen Zeitraum (u.U. Jahre) nicht gewechselt werden.
Somit empfiehlt es sich, bei VoIP-Systemen Hard- und Softwarekomponenten zu unterscheiden, was im Folgenden gemacht wird (in Klammern wird ein Vorschlag zum Implementierungsverfahren gegeben).

- Hardware (manuell):
  - Teile oder Gesamtheit von Zentralkomponenten (Komplettsystem, Einschubkarten, Zubehör, ...)
  - Endgeräte
  - Netzkomponenten
  - Hardware sonstiger Applikationssysteme (Unified-Messaging, CTI, Accounting-Management, ...)
- Software:
  - Software für Zentralkomponenten (Betriebssystem, Anwendungssoftware) (manuell, wegen geringer Stückzahl und u.U. hoher Komplexität zur Konfiguration)
  - Software für Endgeräte (automatisiert, z.B. über Tools)
  - Software für Netzkomponenten (automatisiert, z.B. Upload auf Komponente und Aktivierung zu im SLA vereinbarten Wartungsfenstern)

– Software sonstiger Applikationen (manuell/automatisiert – abhängig von der Anzahl der Systeme, Beispiele wie oben).

Allgemein ist anzumerken, daß die Implementierungsmethode nach einer Kostenabschätzung zu wählen ist (Vergleich manuelles Rollout zu Kosten für Finden einer Automatisierungslösung und automatisiertem Rollout); bei geringen Stückzahlen (und ggf. hoher Komplexität der Bestandteile) wird die manuelle Methode vorteilhafter sein.
Die Ausführungstermine der Releases sollten auf lastarme Zeiten (Rücksprache mit dem Nutzer) bzw. im SLA vereinbarte Wartungsfenster gelegt werden. In Bezug auf Steuerung des Prozesses sind dem Management auch hier Berichte vorzulegen (z.B. Anzahl der Releases, Probleme im Rahmen der Releaseausführung, Informationen über den DHS und die DSL, Leitungsindikatoren, . . .).
Leistungsindikatoren für das Release-Management sind u.a. die Anzahl der zeitgerechten Releases (unter Einhaltung des Budgetrahmens), Anzahl der Releases, bei denen der Einsatz des Notfallplans notwendig war, Fehler in im Einsatz befindlichen Versionen, Anzahl nicht autorisierter Versionen, etc.

6.6.7 Zusammenfassung – Betriebskonzept für VoIP-System

Dieser Abschnitt stellt ein Betriebskonzept für ein VoIP-System vor, wobei die in den vorhergegangenen Prozessen gegebenen Vorschläge und Anmerkungen zusammengefaßt und zu einem Gesamtkonzept verschmolzen werden.
Hauptintention des Betriebskonzepts ist die Integration in bereits vorhandene Strukturen und Abläufe für das Servicemanagement der sonstigen EDV-Infrastruktur. Diese Integration hat, wie bereits gesagt, den Hintergrund, daß VoIP-Systeme nicht – wie bisher TK-Systeme – als von der IT-Struktur getrennte Systeme gesehen werden dürfen, da die meisten Fehler und Probleme auf die gemeinsam genutzte Infrastruktur, nämlich das Datennetz, zurückzuführen sind (lediglich VoIP-spezifische Probleme sind im Incident- und Problem-Management separat zu behandeln); außerdem ergibt sich so die Möglichkeit, Kosten zu sparen (durch die Integration beider Systeme in eine Organisation werden prozentual weniger Ressourcen – hier v.a. Personal – benötigt als bei einem getrennten Aufbau). Der organisatorische Aufbau für die Betriebsprozesse (der direkt die Abläufe des Betriebskonzepts impliziert) wird in Kapitel 6.7 gezeigt, wobei hierbei auch die Aufbauorganisation der Designprozesse, also der gesamte organisatorische Aufbau des Managementskonzepts vorgestellt wird, da zwischen beiden Teilgebieten vielfältige Wechselbeziehungen vorhanden sind.
Hier werden die Besonderheiten des Betriebskonzepts (im Vergleich zur sonstigen EDV-Infrastruktur) kurz erörtert. Detailliertere Angaben können hier nicht gemacht werden, da der Aufbau zu unternehmensspezifisch ist (eine beispielhafte Realisierung wird in Kapitel 7 gezeigt).
Zentrale Komponenten und Werkzeuge im Betriebskonzept stellen folgende Elemente dar:

- der Service-Desk (der alle Anfragen entgegennimmt und erfaßt)
- ein TTS (das vom Service-Desk, dem Incident- und Problem-Management genutzt wird)
- die CMDB – mit DSL und DHS (die vom Configuration-Management entworfen und in Zusammenarbeit mit dem Change- und Release-Management gepflegt wird)
- Monitoring- und Loggingsysteme der Infrastruktur-, Netz- und VoIP-System-Komponenten (die von allen Betriebsprozessen genutzt werden können)

Beim Incident-Management ist in den n-ten-Level-Support die im Wartungs-/Servicevertrag (siehe Abschnitt 6.5.5.4) vereinbarte Hilfestellung des Anbieters/Herstellers/Dienstleisters zu integrieren, um VoIP-spezifische Probleme und Störungen beheben zu können.
Im nächsten Abschnitt wird die Aufbauorganisation des Managementkonzepts in abstrakter Form vorgestellt.

6.7 Organisatorischer Aufbau

Die vorgestellten Prozesse und Abläufe stehen für sich separat und haben ihre spezifischen Wechselbeziehungen zu den genannten anderen Prozessen. Prinzipiell besteht jeder Prozeß aus einem Prozeßmanager, der für den Prozeß nach außen verantwortlich ist, und einem Team, das die Aufgaben des Prozesses erledigt. Die Aufteilung in verschiedene Prozesse dient zwar der Identifizierung und Abstrahierung der Teilaufgaben eines Gesamtsystems, bedingt aber – wenn man jeden Prozeß separat installiert – einen immensen Informations- und Abstimmungsbedarf, was (alleine wegen der Anzahl) zwangsläufig zu Koordinationsproblemen und damit zu einer Vielzahl an Reibungsverlusten, die das Management deutlich erschweren, da die Organisation zu einem Großteil nur mit sich selbst beschäftigt ist.
Daher ist es sinnvoll, mehrere Prozesse, die ein gemeinsames Oberziel besitzen, organisatorsich zu vereinen und ineinander zu integrieren. Dies hat überdies den Vorteil, Ressourcen zu sparen, da insbesondere bei VoIP-Systemen je ein spezieller Themenkreis Priorität hat und so nicht für jeden Prozeß eine definierte Ressourcenmenge vorgehalten werden muß (Beispiel: Network-Service-Management befaßt sich mit der Neukonzeptionierung des Routingkonzepts (LCR) nach einem Carrierwechsel; ein Carrierwechsel findet aber nicht häufig statt, so sind die Kapazitäten für Aufgaben des Availability-Managements verfügbar).
Das Maß der Zusammenlegung und Integration von Prozessen zu Obergebieten ist auch von der Größe und Komplexität der Systeme abhängig; eine pauschale Empfehlung kann hier – wegen der vielen unternehmensbezogenen Spezifika – nicht gegeben werden. Wichtig ist nur die Auseinandersetzung mit dieser Thematik beim Aufbau der Organisation.
Abbildung 6.19 stellt daher einen Vorschlag dar, der prinzipiell für die meisten Unternehmen eine gangbare Lösungsmöglichkeit sein sollte. Personell ist nun für jedes der Oberziele und für die gelb hinterlegten

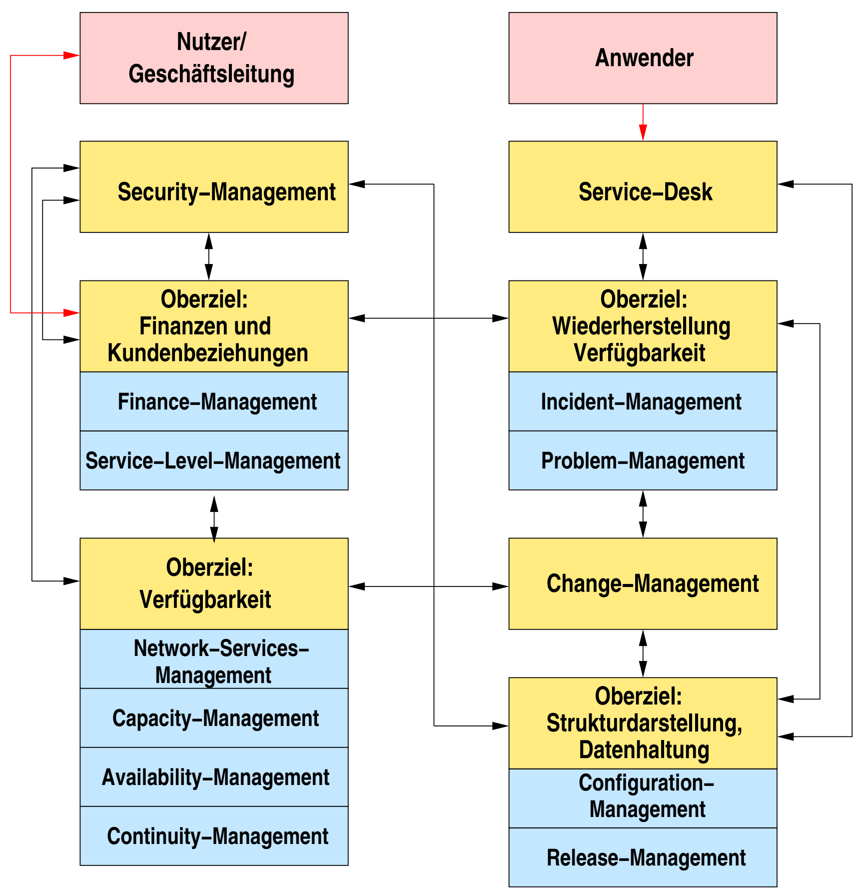

Abbildung 6.19: Aufbauorganisation

Prozesse ein Prozeßmanager zu benennen, der die Verantwortung über die Prozesse trägt (die Beziehungen der Prozesse untereinander sind ebenfalls dargestellt); für Prozeßmanager (inkl. der Oberziele) ergibt sich somit ein geringerer Kommunikationsbedarf, da ein Großteil innerhalb des eigenen Bereichs abgewickelt werden kann. Die Aufgaben der jeweiligen Prozesse ergeben sich aus den bereits vorgestellten jeweiligen Aktivitäten. Zusätzlich ist zur Unterstützung aller Prozesse im Rahmen des Incident- und Problem-Managements ein Administrationsteam einzurichten, das aus einem/mehreren Administratoren des Systems (Datennetz und VoIP-Spezifika) und Mitarbeitern besteht. Diese Personen besitzen des meiste Fachwissen innerhalb der Organisation und können bei grundsätzlichen Fragestellungen von den anderen Prozessen konsultiert werden (diese Personen waren im Idealfall bei den Planungsprozessen vor der Inbetriebnahme beteiligt). Primär sind sie aber innerhalb des Incident- und Problem-Managements für die Störungs- und Problembeseitigung zuständig.

Damit ist das Managementkonzept für VoIP-Systeme sowohl funktional als auch organisatorisch erstellt.
Im nächsten Kapitel erfolgt eine prototypische Realisierung am Beispiel der Bezirksfinanzdirektion München.

Kapitel 7

Prototypische Realisierung

…

7.1 Ergänzungen zur Szenariobeschreibung

7.1.1 Gebäudebeschreibung

…

7.1.2 Beschreibung der Leitungswege

…

7.2 Systembeschreibung

…

7.2.1 Zentralkomponenten

…

7.2.1.1 Architektur

…

7.2.1.2 Baugruppen

…

7.2.1.3 Steuerung

...

7.2.1.4 Lizenzierung

...

7.2.1.5 Zusammenfassung

...

7.2.1.6 Ausstattung im Szenario

...

7.2.2 Netzinfrastruktur

...

7.2.3 Applikationen

...

7.2.4 VoIP-Endgeräte

...

7.2.5 Zusammenfassung

...

7.3 Aufbauorganisation

...

7.4 Design/Planung

...

7.4.1 Finance-Management

...

7.4.1.1 Finanzplanung

...

7.4.1.2 Kostenrechnung

...

7.4.1.3 Leistungsverrechnung

...

7.4.2 Network-Services-Management

7.4.2.1 Netzkomponenten und Nutzung von IEEE 802.3af

...

7.4.2.2 Netzdesign

...

7.4.2.3 Routing-/LCR-Konzept

...

7.4.2.4 Aufbau Accountingmanagement

...

7.4.2.5 Rufnummernplan

...

7.4.2.6 Berechtigungskonzept

...

7.4.2.7 Leistungsmerkmalkonzept

...

7.4.3 Security-Management

...

7.4.4 Availability-Management

7.4.4.1 Verfügbarkeitsanforderungen

...

7.4.4.2 Infrastruktur

...

7.4.4.3 Datensicherungskonzept

...

7.4.4.4 Zusammenfassung

...

7.4.5 Continuity-Management

...

7.4.5.1 Kontinuitätsstrategie

...

7.4.5.2 Erstellung von Notfallplänen, Schulung der Mitarbeiter

...

7.4.6 Capacity-Management

7.4.6.1 Business-Capacity-Management

...

7.4.6.2 Service-Capacity- und Ressource-Capacity-Management

...

7.4.7 Service-Level-Management

...

7.4.7.1 Identifizierung der Kundenbedürfnisse

...

7.4.7.2 Erstellung einer Servicespezifikation

...

7.4.7.3 Vereinbarung eines SLA

...

7.4.7.4 Überwachung

...

7.4.7.5 Berichtswesen

...

7.4.7.6 Änderungsmanagement

...

7.5 Installation/Inbetriebnahme

...

7.6 Laufender Betrieb

...

7.6.1 Aufbau Service-Desk

7.6.1.1 Allgemeines

...

7.6.1.2 Erreichbarkeit

...

7.6.2 Technische Systeme

...

7.6.2.1 Netzmanagement

...

7.6.2.2 Management der Zentralkomponenten und Endgeräte

...

7.6.2.3 Zusammenfassung

...

7.6.3 Configuration-Management

...

7.6.4 Incident-Management

...

7.6.5 Problem-Management

...

7.6.6 Release-Management

...

7.6.6.1 Prozeßschritte

...

7.6.7 Change-Management

...

7.7 Evaluierung

...

7.7.1 Vorstellung

...

7.7.2 Ergebnisse

...

7.7.3 Bewertung

...

7.8 Zusammenfassung

...

Kapitel 8

Zusammenfassung und Ausblick

In der vorliegenden Arbeit wurde ein Managementkonzept für VoIP-Systeme entwickelt. In diesem Rahmen wurde ein besonderes Augenmerk auf die Prozeßorientierung gelegt, die zu einem bedeutenden Teil für ein ressourcenschonendes Management – hierbei v.a. an Personalkosten, da Personalkosten einen der größten Kostenblöcke darstellen – erforderlich ist.
Voraussetzung für die Entwicklung des Managementkonzepts war die Darstellung von Normen, Standards und Definitionen, die zum Verständnis von VoIP-Systemen notwendig sind.
Darüberhinaus wurde ein (dienstorientierter) Anforderungskatalog für den Betrieb von VoIP-Systemen erstellt, der Voraussetzung für den erfolgreichen Betrieb (wobei Betrieb mit Management gleichgesetzt werden kann) ist. Daneben wurden die Architekturen der derzeit am Markt befindlichen VoIP-Systeme vorgestellt und abstrahiert, wobei herausgearbeitet wurde, daß architekturell nur geringe Unterschiede zwischen den verschiedenen Herstellern bestehen (jeder Hersteller preist seine Lösung als das „Nonplusultra“ an).
Darauf folgend wurde das Managementkonzept entwickelt, wobei – wie bereits erläutert – besondere Schwerpunkte auf Prozeßorientierung und Effizienz gelegt und versucht wurde, eine sinnvolle Balance zwischen Outsourcing und den Aktivitäten, die innerhalb des Unternehmens verbleiben, zu finden; eine prototypische Realisierung des Managementkonzepts belegt dessen Implementierbarkeit.

Viele IT-Systeme werden zwar von den Herstellern angeboten und angepriesen, ein Einsatz – v.a. in großem Stil – führt bei den einsetzenden Unternehmen häufig zu großen Anstrengungen, diese Systeme in die bisherige Infrastruktur, Systeme und Prozesse zu integrieren. Hierbei ergeben sich immer die gleichen Frage- und Problemstellungen, die in jedem Unternehmen separat gelöst werden.

Daher wurde (für VoIP-Systeme) ein Managementkonzept entworfen, das im Sinne eines „Empfehlungshefts“ Anregungen, Hinweise und Vorschläge für die Betriebsphasen eines VoIP-Systems gibt; Basis hierfür waren die im Rahmen der ITIL entwickelten Prozesse.
Dieses Managementkonzept wurde unter dem Aspekt erarbeitet, universell einsetzbar zu sein. Somit sind die Standardfragestellungen für VoIP-Systeme bereits herausgearbeitet und Empfehlungen zur Lösung werden ebenfalls gegeben.
Tiefergehende Anregungen zur Aufbauorganisation konnten nicht gemacht werden, da dieser Teilbereich zu unternehmensspezifisch ist, als ihn in einem allgemeinen Managementkonzept vollständig zu bearbeiten (allgemeine Empfehlungen bzw. ein Beispielaufbau ist vorgestellt).
Um das Managementkonzept mit Leben zu füllen und die gegebenen Empfehlungen in der Praxis einsetzen zu können, wurde es prototypisch in einem Szenario bei der Bezirksfinanzdirektion München, einer Behörde des Freistaats Bayern, realisiert und implementiert.
Die vollständige Inbetriebnahme des VoIP-Systems und die Realisierung des Managementkonzepts fanden im Dezember 2004 statt. Seitdem gab es keinerlei Probleme mit dem VoIP-System und den im Rahmen des Managements getroffenen Entscheidungen, obwohl bereits einige Nagelproben zu bewältigen waren

(u.a. ein mehrminütiger Stromausfall, in dem das gesamte VoIP-System – inkl. aller Komponenten – ohne Beeinträchtigung weitergelaufen ist).

Das Managementkonzept wurde für den primär für den Einsatz von VoIP-Systemen bei Endkunden (also z.B. Unternehmen) entwickelt; VoIP wird in den nächsten Jahren das zentrale Thema im Bereich der Kommunikation sein (sowohl im Carrier- als auch im Endkundenbereich, wobei hier auch die Privatkunden dazugezählt werden) und – nach derzeitigen Prognosen – den Telekommunikationsmarkt radikal umwälzen.
Aufbauend auf dieser Diplomarbeit ergeben sich somit Vorschläge für weitere Arbeiten. Dies sind beispielsweise:

- *Adaption des Managementkonzepts auf Carrier:* Anpassung des Managementkonzepts an die Belange der Carrier
- *Nutzung von WLAN:* in letzter Zeit werden auch VoIP-Lösungen für mobile Mitarbeiter angeboten, die Wireless-LANs als Übertragungsmedium nutzen. Diese Lösungen sind in Bezug auf Verfügbarkeit und Zuverlässigkeit sowie unter Sicherheitsgesichtspunkten zu untersuchen (und wenn die Möglichkeit besteht zu evaluieren). In einem weiteren Schritt ergibt sich darüber hinaus prinzipiell die Möglichkeit, mit öffentlich zugänglichen WLAN-Access-Points schnurlose VoIP-Endgeräte zu nutzen und (bei Vollausbau des WLAN-Verbreitungsgebiets) Mobilkommunikation auf Basis von VoIP zu ermöglichen, was als Folgerung die bisherigen Handynetze (und die Investitionen in die UMTS-Technologie) zum Großteil überflüssig machen würde.
- *im Bereich des Security-Managements (Firewallsysteme):* in der Diplomarbeit wurde ein sehr restriktiver (statischer) Ansatz zur Abschottung der betroffenen Subnetze gemacht (Paketfilterfirewall); dies ist für Endkunden mit festen Adressen bzw. Adreßbereichen ausreichend. Zur Einbeziehung wechselnder Adressen (z.B. Telearbeiter und Außendienstmitarbeiter) sind die Firewallsysteme adaptiv anzupassen, damit sie auch diese Anforderungen realisieren können. Darüberhinaus ist zu berücksichtigen, daß die Portwahl für die UDP-Sprachdatenpakete (innerhalb eines Bereichs) zufällig erfolgt.
- *im Bereich des Accounting-Managements:* Wie in dieser Arbeit erläutert, benutzt VoIP ein IP-Netz, wobei dringend – v.a. über WAN-Strecken – empfohlen wird, ein Quality-of-Service-Verfahren einzusetzen. Dies impliziert in jeder der verschiedenen Ansatzmöglichkeiten eine – wie auch immer geartete – Vorrangbehandlung der Sprachpakete, die in Geldeinheiten auszudrücken ist.
  Hierbei ist ein Konzept zu erarbeiten, mit welchen Mitteln die Preisbildung erfolgen kann (und welche unter verschiedenen Fallgestaltungen praktikabel ist) und wie bzw. wo die Accountingdaten gesammelt und verarbeitet werden.

Ausblickend ist festzustellen, daß VoIP in den nächsten Jahren die Strukturen und Preismodelle in der Telekommunikationsbranche radikal verändern wird und die Geschäftsmodelle der Telekommunikationsunternehmen in Frage stellen wird. Dieser Prozeß befindet sich aber erst im Anfangsstadium; erste Ansätze sind (u.a. durch den Einsatz von VoIP-Systemen bei den Endkunden) bereits gemacht.

Abkürzungsverzeichnis

CAB Change Advisory Board

CCITT Comité Consultatif International de Téléphonie et Télégraphie (Teil der ITU)

CDR Call Detail Record, Gesprächsdatensatz

CI Configuration Item

CMDB Configuration Management Database

DHCP Dynamic Host Configuration Protocol

DHS Definite Hardware Store

DSL Definite Software Library

DSS1 Digital subscriber system no. 1

EC European Commission

ECMA European association for standardizing information and communication systems, 1960 als European Computer Manufacturers Association gegründet

eTOM Enhanced Telecom Operations Management

ETSI European Telecommunications Standards Institue

HDLC Higher Data Link Control

IEC International Electrotechnical Commission

IETF Internet Engineering Task Force

IP Internet Protocol

IPNS ISDN PBX Networking Specification

ISDN Integrated Services Digital Network

ISO International Standards Organization

ITIL IT Infrastructure Library

ITU International Telecommunications Union

JIT Just-in-time

JTC1 Joint Technical Committee on Information Technology

LCR Least Cost Routing

MAC Move and Change

MIB Management Information Base

MO Managed Object

MOS Mean Opinion Score

MR Managed Ressource

OGC Office of Government Commerce

OLA Operational-Level-Agreement

OSPF Open Shortest Paths First

PBX Private Branch Exchange

PCM Pulscodemodulation

POTS Plain Old Telephony System

PSTN Public switched telephone network

Q.SIG Q-Interface-Signalling

RAID Redundant Array of Inexpensive Disks

RegTP Regulierungsbehörde für Telekommunikation und Post

RFA Request for Advice

RfC Request for Change

RFI Request for Information

RTCP Real Time Transport Control Protocol

RTP Real Time Transport Protocol

SAP Service Access Point

SIP Session Initiation Protocol

SLA Service Level Agreement

SLR Service-Level-Requirement

SNMP Simple Network Management Protocol

SRTP Secure Real Time Transport Protocol

STP Spanning Tree Protocol

TCP Transport Control Protocol

TDM Time Division Multiplexing

TK Telekommunikation

TLS Transport Layer Security

TMN Telecommunications Management Network

TQM Total Quality Management

TTS Trouble-Ticket-System

UC Underpinning Contract

UDP User Datagram Protocol

UMS Unified-Messaging-Systeme

USV unterbrechungsfreie Stromversorgung

VoIP Voice over IP

Literaturverzeichnis

[BBE04] ZEITSCHRIFT „C'T“, HEFT 10/2004: *Spannung im Netz*, Mai 2004.

[BKP02] BON, JAN VAN, GEORGES KEMMERLING und DICK PONDMAN: *IT Service Management – Eine Einführung*. Jan van Haren Publishing, ISBN 90-806713-5-5, 2002. 228 S.

[CIS01] CISCO, INC.: *Cisco IP Telephony Design Guide*, http://www-search.cisco.com/global/DE/consultant/pdf/ip-teldg_dt.pdf .

[DIKO02] A. DIRSCHERL, C. KORÉNYI: *Dienstgüte in Quality-of-Service-Architekturen*, 2002, http://wwwhegering.informatik.tu-muenchen.de/Hauptseminare/ws0203/handouts/QoSArchitekturen_Ausarbeitung.pdf .

[DIKO03] A. DIRSCHERL, C. KORÉNYI: *Produktevalutation von VoIP-Systemen bei der BMW AG – Systementwicklungsprojekt*, 2003, http://wwwhegering.informatik.tu-muenchen.de/php-bin/pub/show_pub.php?key=diko03 .

[HAN99] HEGERING, H.-G., S. ABECK und B. NEUMAIR: *Integriertes Management vernetzter Systeme — Konzepte, Architekturen und deren betrieblicher Einsatz*. dpunkt-Verlag, ISBN 3-932588-16-9, 1999, http://www.dpunkt.de/produkte/management.html . 607 S.

[HET04] L. HETTICK, S. TAYLOR: *Technology Backgrounder on Network Security Basics*, August 2004, http://www.webtorials.com .

[IEEE 802.1p] IEEE: *LAN Layer 2 QoS/CoS Protocol for Traffic Priorization*, http://www.ieee802.org/1/p .

[IEEE 802.1q] IEEE: *Virtual LANs*, http://www.ieee802.org/1/q .

[IEEE 802.3af] IEEE: *Power over Ethernet*, August 2003, http://www.ieee802.org/3/af .

[ITSM04] SERVICE MANAGEMENT, MUNICH INSTITUTE FOR: *Unterlagen zum Seminar „Prozeßorientiertes IT-Service-Management anhand von Unternehmensplanspielen“*, Oktober 2004.

[KEI01] KEMPER, A. und A. EICKLER: *Datenbanksysteme – Eine Einführung, 4. Auflage*. Oldenbourg-Verlag, ISBN 3-486-25706-4, 2001, http://www.db.fmi.uni-passau.de/publications/books/DBMSeinf . 608 S.

[MNM01] H.-G. HEGERING, M. GARSCHHAMMER, B. KEMPTER ET AL.: *Towards generic Service Management Concepts: A service Model Based Approach*, Mai 2001.

[NOE03] NÖLLE, JOCHEN: *Voice over IP – Grundlagen, Protokolle, Migration*. VDE Verlag, ISBN 3-8007-2708-0, 2003. 240 S.

[OGC00] GOVERNMENT COMMERCE STAFF (OGC), OFFICE OF: *Service Support*. ISBN 0113300158, März 2000. 323 S.

[OGC01] GOVERNMENT COMMERCE STAFF (OGC), OFFICE OF: *Service Delivery*. ISBN 0113300174, Mai 2001. 300 S.

[OGC02] GOVERNMENT COMMERCE STAFF (OGC), OFFICE OF: *ICT Infrastrucure Management*. ISBN 0113308655, Oktober 2002. 297 S.

[P.800] ITU-T: *Recommendation P.800: Methods for subjective determination of transmission quality*, August 1996.

[Q.SIG01] Q.SIG-ORGANISATIONS: *Q.SIG-Standards*, http://www.qsig.ie/qsig/updates/index.htm .

[RFC1633] R. BRADEN, D. CLARK, S. SHENKER: *Traffic Control Mechanisms – Integrated Services in the Internet Architecture*, 1994, http://www.ietf.org/rfc/rfc1633.txt .

[RFC2205] R. BRADEN, L. ZHANG, S. BERSON: *Resource ReSerVation Protocol (RSVP)*, 1997, http://www.ietf.org/rfc/rfc2205.txt .

[RFC2474] S. BLAKE, D. BLACK, K. NICHOLS: *Definition of the differentiated service field (ds field) in the IPv4 and IPv6 headers*, Dezember 1998, http://www.ietf.org/rfc/rfc2474.txt .

[RFC2475] S. BLAKE, D. BLACK, S. CARLSON: *An Architecture for differentiated Service*, Dezember 1998, http://www.ietf.org/rfc/rfc2475.txt .

[RFC2597] J. HEINANEN, T. FINLAND, F. BAKER: *Assured forwarding phb group*, Juni 1999, http://www.ietf.org/rfc/rfc2597.txt .

[RFC2598] V. JACOBSON, K. NICHOLS, K. PODURI: *An expedited forwarding phb group*, Juni 1999, http://www.ietf.org/rfc/rfc2598.txt .

[RFC3260] GROSSMANN, D.: *New terminology and clarifications for DiffServ*, April 2002, http://www.ietf.org/rfc/rfc3260.txt .

[RFC3272] D. AWDUCHE, A. CHIU, A. ELWALID: *Overview and Principles of Internet Traffic Engineering – Generic Non-functional Recommendations*, 2002, http://www.ietf.org/rfc/rfc3272.txt .

[SCHU96] SCHULZRINNE, H.: *A Transport Protocol for Real-Time Application, RFC 1889*, Januar 1996.

[SIE01] SIEMENS AG, GESCHÄFTSBEREICH INFORMATION und COMMUNICATION NETWORKS (ICN): *Online-Lexikon*, http://w3.siemens.de/solutionprovider/_online_lexikon .

[SIE02] SIEMENS AG, GESCHÄFTSBEREICH INFORMATION und COMMUNICATION NETWORKS (ICN): *Q.SIG - Das Protokoll für heterogene Netze*, März 1999.

[SIE06] SIEMENS AG, GESCHÄFTSBEREICH INFORMATION und COMMUNICATION NETWORKS (ICN): *Security in Real-Time IP Communications*, 2004, http://www.webtorials.com .

[STS01] STEGER, ANGELIKA und THOMAS SCHICKINGER: *Diskrete Strukturen – Band 2, Wahrscheinlichkeitstheorie und Statistik*. Springer Verlag, ISBN 3-540-67599-X, 2001. 249 S.

[TAN00] TANENBAUM, ANDREW S.: *Computernetzwerke, 3. Auflage*. Pearson Studium Verlag, ISBN 3-8273-7011-6, 2000, http://www.cs.vu.nl/~ast . 873 S.

[TAY04] TAYLOR, STEVEN: *VoIP – State of the Market Report*, Oktober 2004, http://www.webtorials.com .

[WIL00] WILDEMANN, HORST: *Unterlagen zur Vorlesung „Kosten- und Leistungsrechnung“*, 2000.

[WIL01] WILDEMANN, HORST: *Das Just-In-Time-Konzept – Produktion und Zulieferung auf Abruf*. TCW Verlag, ISBN 3-934155-63-4, 2001.

[WIL04] WILDEMANN, HORST: *Supply Chain Management*, 2004.