Universität Rostock

Fakultät für Ingenieurwissenschaften

Fachbereich Elektrotechnik und Informationstechnik

Institut für Nachrichtentechnik und Informationselektronik

Diplomarbeit

Thema : *Synchrone Dienste in IP Netzen*

Betreuer : Dr. H. - D. Melzer (Universität Rostock)
DI T. Kessler (Universität Rostock)
DI F. Koebsch (SIEMENS Rostock)
DI D. Jeschke (AOK Mecklenburg - Vorpommern)

Vorgelegt von : Jörn Wallstabe
MNr. 92202465

Kurzreferat

In der Diplomarbeit wird anhand von VoIP die Integration von synchronen Diensten in traditionelle Datennetze beschrieben. Die Grundlage für die beschriebenen Implementierungen von VoIP bildet die ITU - T Empfehlung H.323.
Da die Übertragung isochroner Daten eine Anpassung der Datennetze an deren spezielle Übertragungsanforderungen nötig macht, werden diesbezügliche Themengebiete aufgearbeitet.
Es werden allgemeine Integrations- und Migrationskonzepte dargestellt und am Beispiel der AOK Mecklenburg - Vorpommern Möglichkeiten zur Implementierung von VoIP vorgestellt. Des weiteren erfolgt eine Beschreibung der VoIP Umgebung des ComLabs der Universität Rostock.

Abstract

The thesis investigates the integration of synchronous services into traditional data networks with main focus on Voice over IP. ITU - T Recommondation H.323 forms the basis for the decribed implementations of VoIP.
Because data - only networks have to be adapted to the special transport requirements of isochronous data, methods are broadly covered, that enable data - only networks to integrate isochronous data transport.
The business structure of AOK brach offices in Mecklenborough and Western Pommerania is taken as an example to discuss general integration and migration concepts and possibilities to integrate VoIP into AOKs communication network.
Futhermore the thesis includes a describtion of the VoIP installation at Rostock Universitys ComLab.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

1TR6 nationales ISDN D - Kanal Protokoll

A

AAL ATM Adaption Layer
ABR Available Bit Rate
ABT/ DT ATM Block Transfer/ Delayed Transmission
ABT/ IT ATM Block Transfer/ Immediate Transmission
ACD Automatic Call Distribution
ACELP Algebraic Code Excited Linear Prediction
ACF Admission Confirm
ADPCM Adaptive Differential Pulse Code Modulation
ARJ Admission Reject
ARQ Admission Request
ATM Asynchronous Transfer Mode

B

BCF Bandwidth Confirm
BER Bit Error Rate
BRI Basic Rate Interface
BRJ Bandwidth Reject
BRQ Bandwidth Request

C

CDV Cell Delay Variation
CID Conference ID
CIF Common Intermediate Format
CELP Code Excited Linear Prediction
CER Cell Error Ratio
CFR Committed Flow Rate
CLIP Classical IP
CLR Cell Loss Ratio
CNAME Canonical Name
CNG Comfort Noise Generation
CoS Class of Service
CRTP Compressed RTP
CRV Call Reference Value
CS-ACELP Conjugative Structure Algebraic Code Excited Linear Prediction
CSRC Contributing Source
CSMA/CD Carrier Sense Multiple Access/ Collision Detection
CSTA Computer Supported Telecommunications Application
CTI Computer Telephony Integration

D

DBR Deterministic Bit Rate
DNS Domain Name System
DS Differentiated Services Information
DSCP Differentiated Services Code Point
DSS1 Digital Subscriber Signalling No.1 - ISDN D - Kanal Protokoll des Euro ISDN
DTMF Dual-Tone Multi Frequency
DV Datenverarbeitung
DVM Digital Voice Module

E

F

FDDI	Fiber Distributed Data Interface
FEC	Forward Error Correction
FIFO	First In First Out
FR	Frame Relay
FTP	File Transfer Protocol

G

GSTN	General Switched Telephon Network

H

HTML	Hyper Text Markup Language
HTTP	Hyper Text Transport Protocol

I

IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Management Group Protocol
ILS	Internet Locator Service
IMTC	International Multimedia Teleconferencing Consortium
IN	Intelligent Network
IP	Internet Protocol
IPX	Internetwork Protocol Exchange
ISDN	Integrated Services Digital Network
ISO/OSI	International Organization for Standardization/ Open System Interconnection
IT	Informationstechnologie
ITU	International Telecommunication Union

J

JTAPI	Java Telephony Applikation Programming Interface

K

L

LANE	LAN Emulation
LD-CELP	Low Delay Code Excited Linear Prediction
LFAP	Lightweight Flow Accounting Protocol
LDAP	Lightweight Directory Access Protocol

M

MAC	Media Access Control
MC	Multipoint Controller
MCR	Mean Cell Ratio
MCU	Multipoint Control Unit
MFT	Mutiflex Trunk Module
MGCP	Multimedia Gateway Control Protocol
MIPS	Million Instructions per Second
MOS	Mean Opinion Score
MP	Multipoint Processor
MTBF	Meantime Between Failure

N

N/A	Not Available
NSAP	Network Layer Service Access Point
NVP	Network Voice Protocol

O

P

PAR	Positive Acknowledgement and Retransmission
PBX	Private Branch Exchange
PCM	Pulse Code Modulation
PCR	Peak Cell Ratio
PDU	Protocol Data Unit
PHB	Per Hop Behaviour
PINT	PSTN and Internet Interworking
PRI	Primary Rate Interface
PSTN	Public Switched Telephon Network
PVP	Packet Video Protocol

Q

QCIF	Quarter Common Intermediate Format
QoS	Quality of Service
QSIG	Q-Interface Signalling Protocol

R

RAS	Registration Admission Status
RFC	Request for Comment
RSVP	Resource Reservation Protocol
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
RTP - HC	RTP - Header Compression

S

SBR1..3	Statistical Bit Rate Configuration 1..3
SCN	Switched Circuit Network
SCIF	Sub Common Intermediate Format
SCMP	Stream Control Message Protocol
SCR	Susstainable Cell Ratio
SIP	Session Initiation Protocol
SGCP	Simple Gateway Control Protocol
SNMP	Simple Network Management Protocol
SSCR	Synchronization Source
SS-CFB	Supplementary Service - Call Forwarding Busy
SS-CFNO	Supplementary Service - Call Forwarding No Reply
SS-CFU	Supplementary Service - Call Forwarding Unconditional
SS-CT	Supplementary Service - Call Transfer
ST2	Internet Streaming Protocol Version 2
SVC	Switched Virtual Circuit

T

TCP	Transmission Control Protocol
TIPHON	Telecommunication and Internet Protocol Harmonization over Networks

TSAP	Transport Layer Service Access Point
TTL	Time To Live

U

UDP	User Datagram Protocol
UPC	Usage Parameter Control
URL	Uniform Resource Locator
UU	unused

V

VAD	Voice Activity Detection
VC	Virtual Channel
VLAN	Virtual Local Area Network
VMTP	Versatile Message Transaction Protocol
VoFR	Voice over Frame Relay
VoIP	Voice over IP

W

WAN	Wide Area Network
WDM	Wavelength Division Multiplex
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection

X

XTP	Xpress Transfer Protocol

Y

Z

1 Einleitung

1.1 Thematischer Hintergrund

Computernetze sind heute integraler und unentbehrlicher Bestandteil des täglichen Lebens. Die anfänglich schmalbandigen Punkt zu Punkt Verbindungen entwickelten sich zu den heutigen High Speed Communication Backbones, die die Übertragung von Multimedia Informationen unterstützen.
Diese technische Entwicklung ermöglicht die Integration der Übertragung von isochronen Daten (wie Sprache und zeitsensitiver Datenanwendungen - Simulationen etc.) in paketbasierte Netzwerke.

Computernetzwerke aufbauend auf Ethernet und der Protokollfamilie TCP/IP sind, da sie die weitläufigsten Implementierungen im lokalen Bereich darstellen, der interessanteste Ansatz zur Integration isochroner Daten.
Andere Technologien wie ATM wurden zwar mit Ziel einer einheitlichen Netzstruktur für isochrone und anisochrone Daten entwickelt, spielen aber heute aufgrund fehlender nativer Applikationen und hohem Investitionsaufwand nur im Backbonebereich eine Rolle, wo sie hauptsächlich als High Speed Verbindung zwischen Ethernet LANs eingesetzt werden. [Indu96]

Übertragungsanforderungen von Sprache/ Daten

Computernetze und Netze zur Übertragung von isochronen Daten (hauptsächlich Sprache, auch Video) wie das Telefonnetz haben aufgrund der Datenstruktur, an die sie angepaßt sind, unterschiedliche Ansätze.

- Die Übertragung von isochronen Daten z.B. Sprache fordert vom Übertragungskanal eine für die Übertragung ***garantierte Bandbreite*** , eine ***voraussagbare Verzögerung*** und eine möglichst ***geringe Schwankung der Verzögerung (Jitter)*** . Von den aufgeführten Parametern ist die voraussagbare Verzögerung für die Übertragung von isochronen Daten der wichtigste.
  Zur Garantie der Verständlichkeit bedarf es ein Mindestmaß an Datenverfälschungs- und verlustrate (PCM Bitfehlerwahrscheinlichkeit $\leq 10^{-7}$).

- Die Übertragung von Daten (burstartig) erfordert einen Übertragungskanal mit ***hohem Durchsatz*** sowie eine ***geringe Datenverfälschungs- und verlustrate*** für die Übertragung der Information (Sicherungsmechanismen sind auf höheren Netzebenen - ab Schicht 2 ISO/OSI implementiert). [gw12/98]

In Tabelle 1 sind die Anforderungen an die Bitfehlerrate von Sprach- und Datennetzen gegenüber gestellt.

Übertragungstechnologie	***Bitfehlerrate***
ISDN/ PCM	10^{-7}
Ethernet	10^{-8}
Tokenring	10^{-9}
FDDI	2.5×10^{-12}
ATM	10^{-5} - 10^{-7} -entsprechend der Verkehrsart festgelegt

Tabelle 1 : Vergleich Übertragungsarten - Bitfehlerrate [Data99], [Timm98], [Loch95]

1.2 Motivation

Die Übertragung von Sprache ist schon seit über einhundert Jahren Realität. Ein großer Technologiesprung erfolgte in den frühen 60er Jahren durch der Digitalisierung der Sprachübertragung.
Mit der Entstehung der Datennetze in den 70er Jahren, deren Ausbreitung, die in das heutige Internet gipfelte, und den nunmehr allgegenwärtigen Computern, stellte sich die Frage, ob die Übertragung von Sprache auch über diese paketbasierten Netze realisierbar ist. Die Protokollfamilie TCP/ IP steht dabei im Mittelpunkt, da sie am verbreitetsten ist.

Diese Arbeit behandelt existierende Standards zu VoIP und untersucht die technischen Herausforderungen, die es bei der Implementierung zu lösen gilt.
Die Möglichkeiten der Integration von VoIP und werden am Beispiel der AOK Mecklenburg - Vorpommern untersucht. Dazu erfolgte eine Verkehrsanalyse des TK und des Datennetzes und die Erarbeitung von Konzepten zur Nutzung von VoIP innerhalb der AOK.

1.3 Gliederung

In Kapitel 2 werden die Grundlagen von Voice over IP behandelt. Im Mittelpunkt steht dabei die ITU T Empfehlung ***H.323 - Packet - Based Multimedia Communication Systems***.

Wie schon in der Einleitung angedeutet, müssen Datennetze an die Übertragung von isochronen Daten, die eine benötigte Bandbreite, eine maximale Verzögerung und einen zulässigen Jitter vorschreiben, angepaßt werden. In Kapitel 3 werden daher Methoden zur Datenpriorisierung bzw. Bandbreitenreservierung (z.B. RSVP) auf den ISO/ OSI Schichten 2 bis 4 betrachtet.

Da aber nicht nur an das Netzwerk sondern auch die Transportprotokolle neue Anforderungen gestellt werden, erfolgt in Kapitel 4 eine Einschätzung herkömmlicher Transportprotokolle (TCP und UDP) bezüglich ihrer Eignung zur Übertragung von isochrone Verkehr und die Vorstellung spezieller Echtzeitprotokolle wie XTP und insbesondere des für VoIP verwendeten RTP/ RTCP.

Kapitel 5 gibt am Beispiel ausgewählter VoIP Produkte der Siemens AG und Cisco Systems einen Einblick in die Konzepte der Hersteller zur Implementierung von VoIP.

In Kapitel 6 umfaßt eine Verkehrsanalyse des TK Netzes und des WAN Datennetzes der AOK Mecklenburg - Vorpommern, Vorschläge zu momentane möglichen und zukünftigen Einsatzmöglichkeiten von VoIP in Bezug mit den in Kapitel 3 erforderlichen Voraussetzungen im WAN und LAN Bereich .

Kapitel 7 behandelt die VoIP Umgebung im ComLab der Universität Rostock, beschreibt die notwendigen Arbeiten zur Konfiguration der vorhandenen Geräte und enthält entsprechende Funktionsnachweise.

2 Grundlagen VoIP

Unter Voice over IP versteht man im allgemeinen die Übertragung digitalisierter Sprache über paketbasierte Datennetze. Die Sprache wird mittels RTP übertragen. Im Kapitel 5 wird detailliert auf LAN Echtzeitprotokolle und spezielle RTP/RTCP eingegangen.
Für die notwendige Signalisierung der VoIP Übertragung stehen der Ansatz der ITU - T H.323 (siehe 2.3) und der der IETF SIP (siehe 2.2) zur Verfügung.

2.1 Standardisierungsgremien

ITU

Die ITU als multinationales Standardisierungsgremium der UNO veröffentlichte im Januar 1998 die Version 2 der Empfehlung H.323 - ***Packed - based Multimedia Communication Systems***, auf die sich heute die Implementierung von VoIP stützt.

Alle im folgenden aufgeführten Standardisierungsbemühungen der verschiedenen Organisationen basieren auf H.323.

ETSI Tiphon Szenarien

Die ETSI als Standardisierungsgremium der EU konzentriert ihre Arbeit innerhalb des ***TIPHON Projektes (Telecommunication and Internet Protocol Harmonization Over Networks)*** auf die Etablierung von Sprachkommunikation und Diensten im Frequenzbereich der Sprachkommunikation in IP Netzen und zusätzlich in Kooperation mit der ITU und IMTC auf die Standardisierung von Gateways zwischen PSTN und IP Netzen.
TIPHON definiert vier Szenarien für die Internet Telefonie:

- ***Phase 1***: Verbindungsaufbau von einem H.323 Terminal zu Telefonteilnehmer
- ***Phase 2***: Verbindungsaufbau von einem Telefonteilnehmer zu H.323 Terminal
- ***Phase 3***: Verbindung von Teilnehmern am Telefonnetz über IP Netze
- ***Phase 4***: Verbindung zwischen H.323 Terminals über das Telefonnetz.

Die laufenden Arbeiten betreffen Phase 2 und 3. Phase 1 wurde offiziell im März 1999 für beendet erklärt.

Geplant ist unter anderem die Integration von ***Back End Services*** in das TIPHON Projekt. Diese Dienste erfüllen verschiedene Funktionen, wie die Schaffung von Zugangspunkten zu intelligenten Netzen (IN) oder die Authentifizierung von Stationen bei der Einwahl.

IETF

Die IETF hat zwei Arbeitsgruppen zu VoIP eingerichtet.

IPTEL beschäftigt sich mit Internet Standards für die Sprachübertragung im Internet (basierend weitgehend auf H.323). Für die Kommunikation über Gateways wird unter anderem das vom Signalisierungsprotokoll der IP Telefonie unabhängige ***SIP - Session Initiation Protocol*** (RFC 2543) als Alternative vorgeschlagen.

PINT (PSTN and Internet Internetworking) bemüht sich um die Integration von Telefon Diensten ins Internet, z.B. Click to Dial. Erste vorläufige Implementationen werden im RFC 2458 beschrieben.

IMTC VoIP

Im Rahmen des ***International Multimedia Teleconferencing Consortium*** - ***IMTC*** - wurde eine Arbeitsgruppe namens Voice over IP Forum gebildet. In Zusammenarbeit mit der ITU und der ETSI sollen vor allem Vereinbarungen über Codecs mit guter Sprachqualität bei niedriger notwendiger Bitrate getroffen werden und die Zusammenarbeit zwischen diversen H.323 Terminals bzw. H.323 Softwareimplementierungen gewährleistet werden.
[Schu98], [Kuri99]

2.2 IETF: Session Initiation Protocol - SIP

Das SIP wird zum Aufbau, zur Modifizierung und zum Abbau von Multimedia Verbindungen genutzt.
SIP ist ein sich auf HTTP gründendes textbasiertes Protokoll und kann auf UDP und TCP aufsetzen, wobei das Nachrichtenformat unabhängig vom verwendeten Transportprotokoll ist. Dabei unterstützt es die Anwendermobilität, Capability Austausch zwischen den Endusern, Authentifikation, Access Control, Geheimhaltung (Confidetiality) und Integrität.

Da SIP ein Client/ Server Protocol darstellt, existieren zwei Nachrichtenarten: auf der Clientseite die Requests und auf der Serverseite die Responses.

Das aktuelle SIP 2.0 enthält sechs Requesttypen:

- ***INVITE*** - Nachfrage eines bestimmten Teilnehmers; Parameter Verhandlungen; dynamische Parameteränderung über neuen INVITE Request möglich;
- ***ACK*** - Bestätigung einer neuen Verbindung, enthält Session Description, mit Parametern des Medienstromes;
- ***OPTIONS*** - zur Anfrage von Fähigkeiten des Servers;
- ***REGISTER*** - Information an der Server über aktuelle Position des Users;
- ***BYE*** - Verlassen einer Session;
- ***CANCEL*** - beendet nach Auffinden des gesuchten Users, die parallele Suche (gleichzeitig in mehreren Netzwerkabschnitten)

Die Requests können mit ebenfalls sechs möglichen Response Typen beantwortet werden :

- Informational - 1xx
- Successfull - 2xx
- Redirection - 3xx
- Request failure - 4xx
- Server failure - 5xx
- Global failure - 6xx

Der SIP Server kann in zwei Arbeitsmodi operieren, als

- ***Proxy Server***, der die Responses für den User generiert, und als
- ***Redirect Server***, der den Client über die aktuelle Position des Users informiert, so daß der Client eine direkte Verbindung zum User aufbauen kann.

Falls kein SIP Server vorhanden ist, können SIP User Agenten auch direkt miteinander kommunizieren.

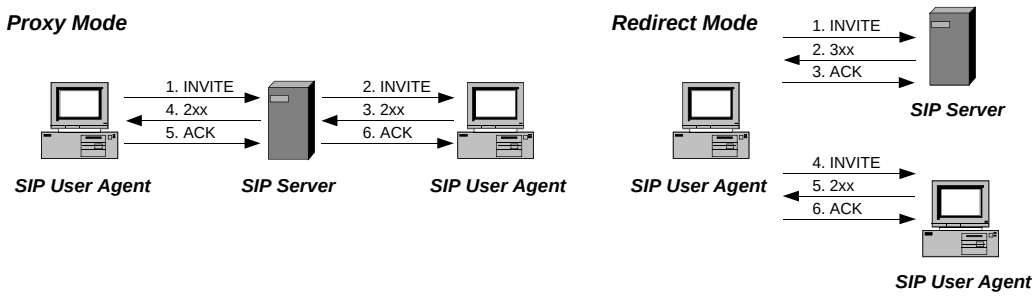

Abbildung 1 : Arbeitsmodi des SIP Servers [Cama98]

SIP Nachrichten bestehen aus einer Start Line, mehreren Header Feldern, einer Emty Line und einem optionalen Message Body, der eine Session Description - über das ***Session Description Protocol SDP*** - enthalten kann.
[Cama98]

Vergleich SIP H.323 V2

	SIP	***H.323 V2***
unterstützte Dienste	ungefähr gleich	
Medientransport	äquivalent (RTP, identische Codecs)	
Call Set up Delay	1.5 RTT	6-7 RTT; seit H.323 V2 verbessert, da H.245 Nachrichten über den H.225.0 Signalisierungskanal übertragen werden können
Komplexität	mittel, HTTP ähnliches Protokoll	hoch: ASN, Nutzung mehrerer Protokolle (H.450, H.225.0, H.245)
Codec Support	alle IANA Codecs	ITU Codecs
Third Party Call Con-trol (zusätzl. Dienste wie blind transfer, operator assisted transfer, three party calling, forwarding variations, etc.)	ja	nein
Architektur	*modular*: SIP umfaßt basic Call Signalling, User Location and Registration; andere Funktionen wie QoS, Directory Access, Service Discovery, Session Content Description in separaten Protokollen	*monolithisch*: H.323 umfaßt Capability Exchange, Conference Control, Maintenance Operations, basic Signalling, QoS, Registration, Service Discovery
Server stateful/ -less	*stateless*	*statefull:* (Server muß Call Status für die gesamte Verbindungszeit halten; zusätzl. zum TCP status) => geringere Reliability und Scalability

	SIP (fortgesetzt)	***H.323 V2(fortgesetzt)***
Conference Control	distributed multicasting Support	zentralisiert: (MC wird zum Flaschenhals bei größeren Konferenzen bzw. MCs müssen kaskadiert werden); nur unicast Signalisierung => geringere Reliability und Scalability, zusätzl. Komplexität durch spez. Handling von großen Konferenzen
Loop Detection	ja	nein => eine Umleitung kann zu unendl. Forwarding führen
Multicast capable Signalling	ja => vereinfacht User Lokation, Group Invitation, Call Center Appl.	nein
Adressierung	jede URL (email, H.323, HTTP etc.)	Host (ohne Username), GK resolved Alias, E.164 Telefonnummer
Web Integration	Integration mit anderen Internet Diensten (z.B. Verschicken von Email an nicht erreichbare Teilnehmer); Click to Dial Feature	
Inter Domain User Location	schwach	durch existierende Internet Dienste (DNS, LDAP etc.)

Tabelle 2 : Vergleich SIP und H.323 [Schul99]

Der Hauptgrund für die Existenz zweier nicht interoperabler Signalisierungsprotokolle ist, daß jeweils die TK - Welt und die Internet Welt Protokolle entsprechend ihrer Tradition bevorzugen.

Die ITU wollte eine hochentwickelte Norm aufbauend auf anderen ITU Normen, wohingegen die IETF ein Protokoll definierte, das sich einfach in die Internet Protokollfamilie integrieren läßt. VoIP befindet sich im Grenzbereich beider Welten (TK und Datennetze), und es ist schwer vorhersagbar, welcher Ansatz letztendlich die größere Akzeptanz findet.

Da aber die technische Entwicklung von SIP noch nicht so weit fortgeschritten ist wie die von H.323, befassen sich die nachfolgenden Kapitel mit H.323.

[Schul99]

2.3 ITU - T: H.323 Überblick

Die 1996 von der ITU verabschiedete H.323 Empfehlung (Januar 1998 Version 2) dient als Zusammenfassung für eine Reihe von ITU Empfehlungen zur multimedialen Kommunikation in LANs, die keinen garantierten QoS bereitstellen.
Da derartige Netzwerke heute dominieren (z.B. TCP/ IP, IPX über Ethernet, Tokenring) bildet die H.323 Empfehlung eine wichtige Grundlage für neue LAN basierte Multimedia Kommunikationsapplikationen.

Die Vorteile der Empfehlung gegenüber proprietären Ansätzen sind:

- ***Codec Standards*** - Kompressions- und Dekompressions Standards für Audio und Video garantieren Interoperabilität mit den Produkten anderer Hersteller;
- ***Interoperabilität*** - neben der Kompatibilität der Audio und Video Codecs liefert die Empfehlung Methoden für einen Common Call Setup, Kontroll - Protokolle und Verfahren zum Austausch von Informationen betreffend der Interoperabilität;
- ***Netzwerk Unabhängigkeit*** - H.323 unterstützt vielfältige Netzwerkarchitekturen (Ethernet, Tokenring, ATM - siehe 2.3 für die Implementierung von H.323 über ATM, etc.) und kann neu implementierte Netzwerkfunktionen (z.B. Bandbreitenmanagement) nutzen;
- ***Plattform und Applikations Unabhängigkeit*** - H.323 ist nicht an eine Hardware bzw. ein Betriebssytem gebunden
- ***Multipoint Unterstützung*** - MCUs [1] bilden flexible Grundlage für Multipoint Konferenzen; Multipoint Unterstützung kann auch in anderen Komponenten enthalten sein;
- ***Bandbreiten Management*** - Network Manager kann die Anzahl der gleichzeitigen H.323 Verbindungen entsprechend der H.323 Appl. zugeteilten Bandbreite begrenzen;
- ***Multicast Unterstützung*** ;
- ***Flexibilität*** - Endpunkte mit unterschiedlichen Fähigkeiten (Audio, Video, Daten) können kommunizieren;
- ***Inter Network Conferencing*** - Verbindung von LAN basierten Endpunkten mit GSTN basierten Endpunkten.

[1] MCU - Multipoint Control Unit - siehe 2.1.1; Konferenzen zwischen drei oder mehr Endpunkten auch ohne MCU möglich

2.3.1 Übersicht der Komponenten

Die H.323 Empfehlung definiert vier Hauptelemente für ein Netzwerk basiertes Kommunikationssystem: ***Terminals***, ***Gateways***, ***Gatekeeper*** und ***Multipoint Control Units***.
Ein von einem Gatekeeper gemanageder Bereich von Terminals, Gateways und MCUs wird als ***Zone*** bezeichnet. Eine Zone ist unabhängig von der Netzwerktopologie und kann somit mehrere Netzwerksegmente, die durch Router verbunden, sind umfassen.

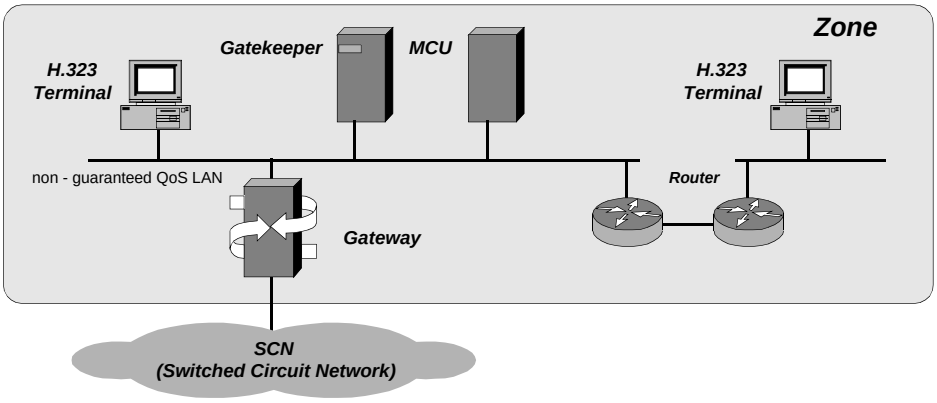

Abbildung 2 : H.323 Komponenten [nach Klein98; H.323]

H.323 beschreibt ***Endpoints*** und ***Entities***. Als H.323 Entities werden alle H.323 Komponenten bezeichnet. Endpoints sind H.323 Terminals, Gateways und MCUs und können Verbindungen aufbauen bzw. annehmen.

<u>Terminal</u>
Ein Terminal ist ein Client Endpoint innerhalb eines LANs, das eine Zwei Wege Echtzeitkommunikation bereitstellt. Die Kommunikation beinhaltet Control, Indication, Audio, Video und Daten.
Die Unterstützung von Sprache (Codecs), die Kontrollfunktionen von:

- ***H.245*** - Informationsaustausch zur Vereinbarung von Kanalnutzung und den vom Endpunkt unterstützten Fähigkeiten;
- ***Q.931*** - Call Signalisierung und Setup;
- ***RAS*** - Registration, Admission, Status - Protokoll zur Kommunikation mit dem Gatekeeper,

sowie von ***RTP/ RTCP*** ist obligatorisch.
Optional sind Video Codecs, das T.120 Daten Protokoll und die Unterstützung von MCUs.
In Abbildung 3 sind die Terminalkomponenten beschrieben.

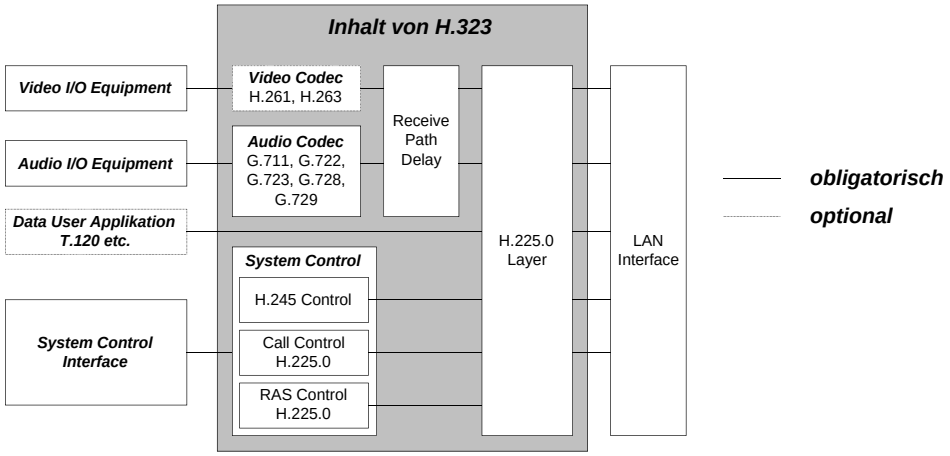

Abbildung 3 : H.323 Terminal [H.323]

Gateway

Da H.323 Endpoints direkt kommunizieren können, stellen Gateways eine optionale Komponente dar, die Funktionen zur Kommunikation von H.323 Terminals im LAN und ITU Terminals im SCN [2] bereitstellt. Diese Funktionen umfassen die Abbildung von Übertragungsformaten (z.B. H.225.0 auf H.221- siehe H.246), Kommunikationsabläufen (z.B. H.245 auf H.242) und Audio/ Video Codecs zwischen dem SCN und dem LAN.

Das Gateway initiiert auf beiden Seiten den Call Setup und das Call Clearing. Terminals kommunizieren mittels H.245 und Q.931 mit dem Gateway.
Während der Registrierung der Terminals beim Gatekeeper wird diesem mitgeteilt, welcher Endpoint ein Gateway ist.

Gatekeeper

Der Gatekeeper ist wie das Gateway optional innerhalb eines H.323 System und stellt den H.323 Endpunkten Call Control Services bereit.
Gatekeeper sind von anderen Endpunkten logisch getrennt, können aber physikalisch innerhalb eines Terminals, Gateways oder MCUs implementiert sein.

Falls ein Gatekeeper im System vorhanden ist, dient er folgenden Funktionen:

[2] H.310 - H.320 on B-ISDN; H.320 - ISDN; H.321 - ATM; H.322 - GQOS LAN; H.324 - GSTN; H.324M - Mobile; V.70 - DSVD (Digital Simultaneous Voice and Data)

- ***Address Translation*** - Abbildung von Alias Adressen auf Transportadressen [3] durch eine mittels Registrierungsnachrichten upgedateten Tabelle; andere Update Methoden sind auch zulässig;
- ***Admission Control*** [4] - Authorisierung des LAN Zugangs durch Admission Request, Confirm und Reject (***ARQ, ACF, ARJ***); Kriterien der Zugangskontrolle basieren auf Call Authorization, Bandbreite oder anderen;
- ***Bandwidth Control*** - Unterstützung für Bandwidth Request, Confirm und Reject (***BRQ, BCF, BRJ***) Nachrichten; kann auf optionalem Bandbreite Management basieren;
- ***Zone Management*** - obige Funktionen werden in Zone registrierten Terminals, MCUs und Gateways bereitgestellt.

Optional können folgende Funktionen vom Gatekeeper unterstützt werden:

- ***Call Control Signalling*** - Gatekeeper kann die Call Signalisierung selbst bearbeiten oder die Endpunkte anweisen, zwischen ihnen einen direkten Signalisierungskanal aufzubauen;
- ***Call Authorization*** - über die H.225.0 Signalisierung kann der Gatekeeper Verbindungswünsche aufgrund von Authentifizierungsfehlern (begrenzter Zugang von bestimmten Terminals bzw. zeitl. Zugangsbegrenzung) zurückweisen;
- ***Bandwidth Management*** - über die H.225.0 Signalisierung kann der Gatekeeper Verbindungswünsche aufgrund von begrenzter Bandbreite zurückweisen;
- ***Call Management*** - Erzeugung einer Liste von aktiven Verbindungen zu deren Verwaltung.
- ***Gatekeeper Management Information Data Structure*** , ***Bandwidth Reservation for Terminals not capable of this function*** und ***Directory Services*** sind in H.323 Version 2 noch nicht implementiert.

Um ad hoc Multipoint Konferenzen zu unterstützen, kann ein Gatekeeper die H.245 Kanäle zweier Terminals in einer Punkt zu Punkt Kommunikation empfangen und wenn die Konferenz zur Multipoint Konferenz wechselt diese zu einem MC[5] weiterleiten.

[3] besteht aus Netzwerkadresse (incl. Z.B. Port) und dem TSAP Identifier (genutzt, um mehrere Transportverbindungen desselben Typs einer H.323 Entity mit allen Transportverbindungen mit derselben Netzwerkadresse zu multiplexen)
[4] kann Nullfunktion sein, wie auch Bandwidth Control und Bandwidth Management
[5] MCU besteht aus MC - Multipoint Controller und MP - Multipoint Processor

Netzwerke mit einem Gateway sollten zur Abbildung von E.164 oder partyNumber Adressen in Transportadressen über einen Gatekeeper verfügen.
H.323 Entities mit einem internen Gatekeeper sollten diesen deaktivieren können, da innerhalb einer Zone nur ein aktiver Gatekeeper zulässig ist.

Mulipoint Control Unit - MCU

Die MCU ist ein Endpunkt zur Unterstützung von Multipoint Konferenzen. Eine MCU besteht aus einem Multipoint Controller - MC - und keinem bis mehreren Multipoint Processors. Eine MCU kann Centralized, Decentralized und Hybrid Multipoint Konferenzen unterstützen (siehe 2.3.2).

Der ***MC*** übernimmt über H.245 die Verhandlung zur einheitlichen Behandlung von Audio und Video zwischen allen Terminals und die Kontrolle über die Konferenzressourcen durch die Entscheidung, welche Medienströme über Multicasts verteilt werden.

Der ***MP*** befaßt sich direkt mit den Medienströmen durch Mixen, Switchen und Bearbeitung von Audio, Video und Daten.

2.3.2 Multipoint Konferenzen unter H.323

Centralized Multipoint Conferences

Eine typische MCU, die ***Centralized Multipoint Conferences*** unterstützt, besteht aus einem ***MC*** und einem Audio, Video und/ oder Daten ***MP***.
Die Kommunikation zwischen MCU und den Endpunkten erfolgt auf Punkt zu Punkt Basis.

- Der ***MC*** managed die Konferenz durch H.245 Kontrollfunktionen wie: ***centralizedControl***, ***centralizedAudio***, ***centralizedVideo***, und ***centralizedData***. Optional können ***distributed-Audio*** und ***distributedVideo*** zur Kennzeichnung der Medienaussendung über Multicast verwendet werden.

- Der ***MP*** übernimmt das Audio/ Video Switching bzw. Mixing, die T.120 Multipoint Daten Verteilung und die Konvertierung zwischen unterschiedlichen Datenformaten und Bitraten. Anschließend sendet der MP die bearbeiteten Medienströme zu den Endpunkten.

Decentralized Multipoint Conferences

Die Kommunikation mit dem ***MC*** erfolgt auf Punkt zu Punkt Basis. Die Kontrolle einer Dezentralen Multipoint Konferenz erfolgt zentral im ***MC***, dies schließt Funktionen wie Chair Protocol, Video Broadcast und Video Selection[6] mit ein.
Folgende H.245 Funktionen werden signalisiert: ***centralizedControl***, ***distributedAudio*** , ***distributedVideo*** und c***entralizedData***.

Die Empfangsterminals sind für die Bearbeitung der einkommenden Datenströme selbst verantwortlich. Die an einer Konferenz teilnehmenden Terminals senden Audio/ Video über Multicast an andere Teilnehmer.

In Abbildung 4 sind Centralized und Decentralized Multipoint Conferences gegenübergestellt.

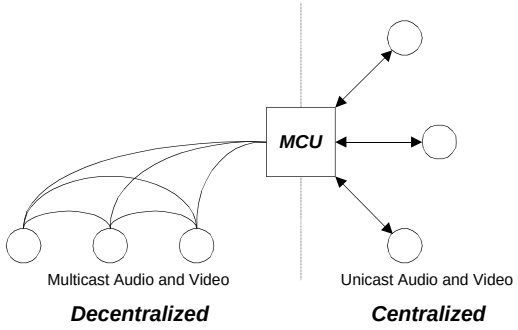

Abbildung 4 : Decentralized/ Centralized Multipoint Conferences [Beam98]

Hybrid Multipoint Conferences

Hybrid Multipoint Conferences sind Kombination von Centralized und Decentralized Multipoint Conferences.

H.245 Signale und Audio oder Video Ströme können über Punkt zu Punkt Verbindungen, die verbleibenden Signale (Video oder Audio) über Multicast übertragen werden[7] .

2.3.3 H.323 Version 2

[6] Empfang von H.245 Nachricht vom Endpunkt und Senden einer entsprechenden Kontroll Nachricht zu anderen Endpunkten, um deren Video Multicast zu de- bzw. zu ativieren, T.120 Kommandos mit gleicher Funktion optional

[7] mögliche Kombination: Hybrid Multipoint - Centralized Audio; Hybrid Multipoint - Centralized Video

Die im Januar 1998 verabschiedete Version 2 des H.323 Standards beinhaltet neue Funktionalitäten für die vorhandenen Protokolle, wie Q.931, H.245 und H.225, sowie zusätzlich neue Protokolle.

Die signifikantesten Neuerungen betreffen:

- ***Sercurity*** - der H.235 Standard enthält Funktionalitäten zur Authentifizierung, Integrität, Privathaltung (Privacy/ Confidentiality) und das Ausschließen ungewollter Dritter [8] (Non-Repudiation);
- ***Fast Call Setup*** - Verbindungsaufbau zwischen Endpunkten durch H.245 oder „Fast Connect" Prozedur; Fast Connect erlaubt Punkt zu Punkt Verbindungsaufbau und unverzügliche Medienübertragung innerhalb eines „Round Trip Message Exchange";
- ***Supplemetary Services*** - in H.450.x definierte Services: ***H.450.1*** - Signalisierungskontrollprotokoll für Suppl. Services zwischen Endpunkten, ***H.450.2*** - Call Transfer, und ***H.450.3*** - Call Diversion (Weiterleitung) - siehe auch H.450.x in späteren Abschnitten (2.4.6)
- ***T.120/ H.323 Integration*** - Endpunkte müssen nun T.120 und H.323 unterstützen; T.120 ist optionaler Bestandteil von H.323, dessen Aktivierung im Ermessen der jeweiligen Endpunkte liegt.

[H.323], [Beam98]

[8] sind an Konferenz beteiligt, bestreiten dies aber

2.4 Kommunikation unter H.323

Die Kommunikation unter H.323 kann als ein Mix aus Audio, Video, Daten und Kontrollsignalen betrachtet werden.
Audiounterstützung, ***Q.931 Call Setup*** , ***RAS Control*** und ***H.245 Signalisierung*** sind obligatorisch, alles andere, wie z.B. Video und Daten Konferenzen optional.

Falls mehrere Algorithmen zur Mediencodierung möglich sind, werden Informationen über den zu verwendenden Codec während des ***H.245 Capability Exchange*** ausgetauscht.
H.323 Terminals sind dabei auch zur ***asymmetrischen*** Arbeitsweise fähig, d.h. Verwendung verschiedener Decodier bzw. Codier Algorithmen, und können mehrere Audio/ Video Kanäle gleichzeitig senden/ empfangen.

<table>
<tr><th>Audio</th><th>Video</th><th colspan="4">Terminal Control and Management</th><th>Data</th></tr>
<tr><td>G.711
G.722
G.723.1
G.728
G.729.A</td><td>H.261
H.263</td><td rowspan="2">RTCP</td><td rowspan="2">H.225.0
RAS
Channel</td><td rowspan="2">H.225.0
Call
Control
Channel</td><td rowspan="2">H.245
Control
Channel</td><td>T.124</td></tr>
<tr><td colspan="2">RTP</td><td>T.125</td></tr>
<tr><td colspan="4">UDP</td><td colspan="2">TCP</td><td rowspan="4">T.123</td></tr>
<tr><td colspan="6">Network Layer (IP)</td></tr>
<tr><td colspan="6">Link Layer (IEEE 802.3)</td></tr>
<tr><td colspan="7">Physical Layer (IEEE 802.3)</td></tr>
</table>

Abbildung 5 : H.323 Protokoll Stack [H.225.0]

2.4.1 Adressen

Netzwerk Adressen

Jede H.323 Entity hat mindestens ***eine*** Netzwerk Adresse, die die Entity eindeutig im Netzwerk kennzeichnet. Einige Entities teilen sich eine Netzwerkadresse (z.B. Terminal mit zugehörigem MC).
Das Adreßformat ist von der Netzwerkumgebung abhängig, in dem sich der Endpunkt befindet. Innerhalb eines Calls kann der Endpunkt für jeden Kanal eigene Netzwerkadressen nutzen.

TSAP Identifier

Für jede Netzwerkadressen können mehrere TSAP[9] Identifier definiert werden, die das Multiplexen von mehreren Kanälen ermöglichen.

Endpoints - well known TSAP Identifier : ***Call Signalling Channel TSAP***

Gatekeeper - well known TSAP Identifier : ***RAS Channel TSAP Identifier***

- well known multicast address : ***Discovery Multicast Address***

Endpunkte und ***H.323 Entities*** können optional ***dynamische TSAP Identifier*** für den H.245 Control Kanal und Audio/ Video/ Daten Kanäle nutzen.

Die Nutzung von ***dynamische TSAP Identifier*** für den Call Signalling durch den ***Gatekeeper*** ist optional möglich.

RAS Kanäle und Signalling Kanäle können auf dynamisch TSAP Identifier während der Registrierung umgeleitet werden.

Alias Adressen

Endpunkte können eine oder mehrere Alias Adressen besitzen, die den Endpunkt selbst oder die durch ihn unterhaltenen Konferenzen bezeichnen. Alias Adressen schließen ein:

- ***E.164*** oder ***partyNumber*** Adressen - Network Access Number, Telefonnummer etc.,
- ***H.323 IDs*** - alphanumerische Name, email - ähnliche Adressen etc. und

andere in der Empfehlung H.225.0 definierte Adressen.

Alias Adressen müssen innerhalb einer Zone eindeutig sein. Gatekeeper, MCs und MPs dürfen keine Alias Adresse besitzen.

[H.323]

2.4.2 Control

Call Control Funktionen umfassen die Signalisierung für den Call Setup, den Capability Exchange, Command & Indication und Nachrichten zum Öffnen oder Schließen von logischen Kanälen.

Audio -, Video - und Steuer Signale passieren eine Control Layer (siehe Abbildung 3 - H.225.0 Layer), die die Anpassung der Datenströme an die Netzwerkschicht übernimmt. In der Control Layer werden durch die Q.931, RAS und RTP/ RTCP Protokoll Funktionen wie

[9] TSAP - Transport Layer Service Access Point

Logical Framing, Sequence Numbering, Error Detection und Error Correction entsprechend des Medientyps implementiert.

Die Kontrolle des Gesamtsystems übernehmen die drei separaten Signalisierungsfunktionen:

- H.245 Control Channel,
- Q.931 Call Signalling Channel und
- RAS Channel.

2.4.2.1 H.245 Call Control Channel

Die H.245 Steuerfunktion nutzt den H.245 Control Channel, um über eine gesicherte Verbindung ***Ende zu Ende Steuermeldungen*** zu übertragen. Ein H.245 Control Channel kann zwischen Endpunkten, Endpunkt und MC bzw. Endpunkt und Gatekeeper aufgebaut werden. Pro Call existiert nur ein H.245 Kanal.
Die Empfehlung H.245 beschreibt eine Reihe unabhängiger Protokoll Entities[10] .
H.323 Endpunkte müssen die Syntax, Semantik und Prozeduren der folgenden Protokoll Entities unterstützen :

- ***Capability Exchange***
- ***Master/ Slave Determination***
- ***Logical Channel Signalling***
- ***Bidirectional Channel Signalling***
- ***Close Logical Channel Signalling***
- ***Mode Request***
- ***Round Trip Delay Determination***
- ***Maintenance Loop Signalling***

In den folgenden Abschnitten wird auf den Capability Exchange, das Logical Channel Signalling und die Master/ Slave Determination näher eingegangen.
Weiterführende Erläuterungen zu allen Protokoll Entities können der Empfehlung H.245 entnommen werden.

H.245 Nachrichten fallen in vier Kategorien: ***Request***, ***Response***, ***Command*** und ***Indication***.

[10] gekennzeichnet durch Syntax, Semantik, Prozeduren zum Nachrichtenaustausch und Interaktion mit dem User

H.323 Terminals müssen alle H.245 ***MultimediaSystemControlMessage*** Nachrichten analysieren und entsprechend reagieren können. Anhang A der Empfehlung H.323 enthält eine Tabelle, die beschreibt, welche H.245 Meldungen für H.323 Terminals obligatorisch, optional oder verboten sind.

Capability Exchange

Die Empfehlung H.245 stellt für den Capabilty Exchange Prozeduren zur Aushandlung der verschiedenen Empfangs- und Sendemöglichkeiten (***Receive, Transmit Capabilities***) bereit. Der Sender darf nur einen Modus [11] wählen, den der Empfänger beim Capability Exchange signalisiert hat.
Es besteht die Möglichkeit, daß ein Sender einem Empfänger eine Auswahl möglicher Betriebsmodi anbietet, und dieser einen von ihm bevorzugten auswählt. Dem Sender bleibt es aber letztendlich vorbehalten, einen durch den Empfänger signalisierten Modus auszuwählen.

Der Sendeterminal ordnet jedem Modus, dessen er fähig ist, eine Nummer in einer ***capabilityTable*** zu.
Diese Nummern werden in ***alternativeCapabilitySet*** Strukturen gruppiert, die aussagen, daß das Terminal in exakt einem der Modi arbeiten kann (z.B. G.711, G.723, G.728 - Terminal kann nur in einem dieser Modi arbeiten).
Die ***alternativeCapabilitySet*** Strukturen werden wiederum in ***simultanousCapability*** Strukturen gruppiert. Jede der simultanousCapability Strukturen bezeichnet eine Reihe von Modi, die ein Terminal gleichzeitig unterstützt (z.B. {H.261, H.263} und {G.711, G.723, G.728} - Terminal kann mit jeglicher Kombination der aufgeführten Video und Audio Codecs arbeiten.

Die Gesamtheit der Terminal Capability wird in einem Satz von ***capabilityDescriptor*** Strukturen, bestehend aus einer ***simultanousCapability*** Struktur und einer ***capabilityDescriptorNumber***, beschrieben.
Terminals können dynamisch ***capabilityDescriptor*** Strukturen hinzufügen bzw. entfernen.

[11] entspricht verwendetem Codec von Audio bzw. Video

Logical Channel Signalling

Jeder logische Kanal transportiert Informationen vom Sender zu einem oder mehreren Empfängern und ist durch eine in jede Übertragungsrichtung eindeutigen ***Logical Channel Number*** gekennzeichnet.

Logische Kanäle werden durch die in H.245 enthaltenen Prozeduren ***openLogicalChannel*** und ***closeLogicalChannel*** geöffnet bzw. geschlossen. Die ***openLogicalChannel*** Nachricht beschreibt den Inhalt (Medientyp, genutzter Algorithmus, Optionen etc.) eines logischen Kanals vollständig.

Da ein Großteil der logischen Kanäle in H.323 unidirektional sind, ist eine ***asymetrische*** Betriebsart erlaubt (Anzahl & Typ der Informationsströme in jeder Richtung verschieden)[12] . Bestimmte Medientypen, incl. des T.120 Protokolls, erfordern bidirektionale Verbindungen. Diese werden durch ein Paar unidirektionale logischer Kanäle [13] bereitgestellt und nutzen die Prozeduren für bidirektionale Kanäle aus H.245.

Master/ Slave Determination

Die H.245 Master/ Slave Determination Prozedur wird zur Konfliktlösung zwischen Endpunkten, die innerhalb einer Konferenz beide MC sein können bzw. zwischen Endpunkten, die eine bidirektionale Verbindung aufbauen wollen, eingesetzt. Dazu werden ***TerminalTyp*** Nummern entsprechend Tabelle 3 und zusätzlich ***StatusDeterminationNumbers*** (Zufallszahl zwischen 0 und 2^{24}-1) ausgetauscht.

TerminalType Value Table	***H.323 Entity***			
Feature Set	***Terminal***	***Gateway***	***Gatekeeper***	***MCU***
Entity with no MC	50	60	NA	NA
Entity contains an MC but no MP	70	80	120	160
Entity contains MC with data MP	NA	90	130	170
Entity contains MC with data & audio MP	NA	100	140	180
Entity contains MC with data, audio & video MP	NA	110	150	190

Tabelle 3 : H.323 Terminal Types für H.245 Master/ Slave Determination [H.323]

[12] Falls der Empfänger nur zu einer symmetrischen Betriebsart fähig ist, muß er dieses im ***Receive Capability Set*** anzeigen.

[13] Paar teilt sich keine ***Logical Channel Number***, da diese für jede Übertragungsrichtung unabhängig

Im Falle einer Übereinstimmung der ***TerminalType*** Nummer werden die ***StatusDeterminationNumbers*** zur Master/ Slave Entscheidung herangezogen.
Bei einem in einer Konferenz aktivem MC erhält dieser den Wert 240 (Active MC Value), um bei nachfolgenden Master/Slave Determination aktiv zu bleiben.
Falls kein MC aktiv ist, gewinnt diese Entscheidung die Entity mit dem höchsten Feature Set.
[H.323], [Klein98]

2.4.2.2 Q.931 Call Signalling Channel

Die Call Signalling Funktion nutzt das H.225.0 Call Signalling [14] zum Verbindungsaufbau zwischen H.323 Endpunkten.
Der Call Signalling Channel ist unabhängig vom RAS bzw. H.245 Channel, nutzt nicht die H.245 Prozeduren zum Verbindungsaufbau und wird vor dem H.245 Channel bzw. anderen logischen Kanälen zwischen H.323 Endpunkten aufgebaut.
In Systemen ohne Gatekeeper wird der Kanal direkt zwischen den beteiligten Endpunkten, in Systemen mit Gatekeeper zwischen den Endpunkten und dem Gatekeeper bzw. auch direkt [1] aufgebaut.
[H.323]

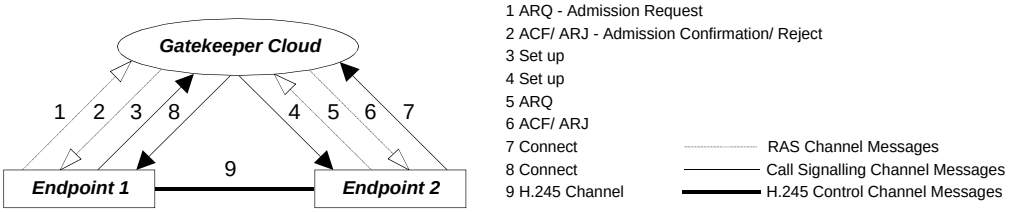

Abbildung 6 : Direkte H.245 Control Verbindung zwischen Endpunkten [weitere Möglichkeiten siehe H.323]

2.4.2.3 Registration, Admission and Status Channel

Die RAS Signalling Funktion nutzt H.225.0 Nachrichten zur Registrierung (Gatekeeper Discovery, Endpoint Registration), Zugangskontrolle, Bandbreitenwechsel, Status und Trennung von H.323 Endpunkten.

[14] H.225.0 spezifiziert die für die Verbindungssignalisierung notwendigen Q.931 Nachrichten
[1] Endscheidung darüber trifft der Gatekeeper

Die RAS Signalisierung ist unabhängig vom Call Signalling bzw. H.245 Channel, nutzt nicht die H.245 Prozeduren zum Verbindungsaufbau und wird vor allen anderen Kanälen[2] zwischen den H.323 Endpunkten aufgebaut.
In Systemen ohne Gatekeeper wird RAS Signalling nicht genutzt, in Systemen mit Gatekeeper wird die Verbindung zwischen diesem und den Endpunkten aufgebaut.
[H.323]

2.4.2.4 Call und Conference Identifizierung

Zur Kennzeichnung von gemeinsamen Verbindungen eines Calls bzw. einer Konferenz nutzt man :

- ***Call Reference Value (CRV)*** - kennzeichnet alle Call Signalling und RAS Nachrichten zwischen Entities einer Verbindung,
- ***Call ID*** - kennzeichnet alle Nachrichten zwischen allen Entities einer Verbindung,
- ***Conference ID (CID)*** - kennzeichnet alle Nachrichten zwischen allen Entities innerhalb aller Verbindungen einer Konferenz.

[H.323]

2.4.2.5 Call Signalling Procedures

Der Ablauf der Kommunikation erfolgt in folgenden Schritten:

- ***Phase A - Call Set up***
- ***Phase B - Initial Communication and Capability Exchange***
- ***Phase C - Establishment of Audiovisual Communication***
- ***Phase D - Call Services***
- ***Phase E - Call Termination***

Phase A - Call Set up

Das ***Call Set up*** nutzt die Call Control Nachrichten der Empfehlung H.225.0.
Die Aufbauphase ist entsprechend den vorhanden Komponenten (Gateway, Gatekeeper) und deren Arbeitsweise (Call Signalling Channel über Gatekeeper oder direkt) verschieden.

[2] logische Kanäle dagegen werden durch H.245 Prozeduren aufgebaut

Abbildung 7 zeigt links einen Call Setup ohne Gatekeeper und rechts einen Call Setup, bei dem beide Endpunkte beim selben Gatekeeper registriert sind (weitere Möglichkeiten sind in H.323 aufgeführt).

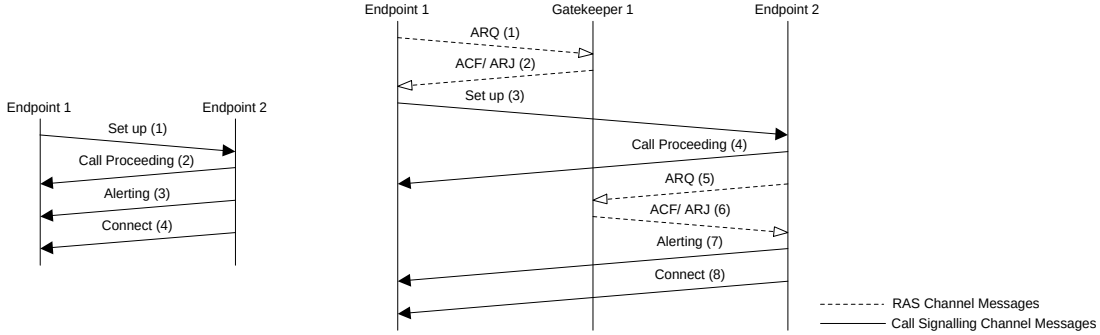

Abbildung 7 : Beispiele für Phase A - Call Set up [H.323]

Alternativ zum Call Setup über H.245 besteht mit H.323 Version 2 die Möglichkeit eines Verbindungsaufbaus über die ***Fast Connect*** Prozedur.

Fast Connect erlaubt den Endpunkten einen Punkt zu Punkt Verbindungsaufbau und eine unverzügliche Medienübertragung innerhalb eines „Round Trip Message Exchange“.

Die vom rufenden Endpunkt initiierte ***SETUP*** Nachricht enthält ein ***fastStart Element***, das aus einer Reihe von OpenLogicalChannel Strukturen besteht. Diese enthalten vom rufenden Endpunkt vorgeschlagene Sende und Empfangskanäle, inklusive der notwendigen Parameter zur sofortigen Öffnung und Medienübertragung.

Falls der gerufene Endpunkt über Fast Connect eine Verbindung aufbauen kann[3], sendet er ein in einer Q.931 Nachricht (***CALL PROCEEDING, PROGRESS, ALERTING*** oder ***CONNECT***) enthaltenes ***fastStart*** Element auf einem der vorgeschlagenen Kanäle.

Phase B - Initial Communication and Capability Exchange

Nach dem Austausch der Set up Nachrichten der Phase A, bauen die Endpunkte den H.245 Control Channel auf. Es werden die H.245 Prozeduren zum ***Capability Exchange*** und gegebenenfalls zur ***Master/Slave Determination*** durchgeführt.

Zur Ressourceneinsparung, Synchronisation von Call Signalling und Control und Reduzierung der Call Set up Time ist es möglich H.245 Nachrichten innerhalb des Q.931 Call Signalling Channels zu übertragen, anstatt einen separaten H.245 Channel aufzubauen.

Phase C - Establishment of Audiovisual Communication

Die Prozeduren der Empfehlung H.245 werden zum Öffnen von logischen Kanälen für die verschiedenen Medienströme genutzt. Audio- und Videoströme werden, gekennzeichnet mit dynamischen TSAP Identifiern, über eine ungesicherte Verbindung übertragen. Die Datenübertragung erfolgt über eine gesicherte Verbindung.
Während der Verbindung können die Channel Struktur, Capability, Receive Mode etc. entsprechend H.245 gewechselt werden.

Phase D - Call Services

Die Call Services beziehen sich hauptsächlich auf Bandbreitenwechsel, Status und Ad Hoc Conference Expansion (Einbeziehung weiterer Endpoints in eine Punkt zu Punkt Konferenz).

Phase E - Call Termination

Am Ende einer Verbindung müssen alle aufgebauten Kanäle wieder geschlossen werden. Abhängig vom Vorhandensein eines Gatekeepers beschreibt die Empfehlung H.323 verschiede Abläufe zur Call Terminierung.
Die Beendung einer Verbindung darf keine Konferenz beenden. Diese wird ausdrücklich mit der H.245 Nachricht ***dropConference*** über den MC beendet.
[H.323], [Klein98]

2.4.3 Audio

Die Verwendung eines Audio Codecs zur Digitalisierung und Kompression von Sprachsignalen ist obligatorisch.

Codec	*Verfahren*	*Bemerkung*	*Bitrate*
G.711	PCM	Puls Code Modulation	64 kbit/s
G.722	Teilbandcodierung	7 kHz Bandbreite	64 kbit/s
G.723.1	ACELP/MP-MLQ	Algebraic CELP[4]/ Multipulse Maximum Likelihood Quantization	5,3/ 6,4 kbit/s
G.726	ADPCM	folds G.721 and G.723	16/ 24/ 32/ 40 kbit/s
G.728	LD-CELP	Low Delay CELP	16 kbit/s
G.729	CS-ACELP	Conjugative Structure-Algebraic CELP	8 kbit/s

Tabelle 4 : ITU Audio Codecs [Mino98],[Klein98]

[3] kann nicht implementiert sein bzw. H.245 für bestimmte Leistungsmerkmale erforderlich
[4] CELP - Code Excited Linear Predictiv; siehe [Mino98] für nähere Informationen über Verfahren

Die verschiedenen ITU Empfehlungen (siehe Tabelle 5) zur Sprachdigitalisierung und - kompression reflektieren die unterschiedlichen Kompromisse, die zwischen Sprachqualität, Rechenleistung und Signal Delay eingegangen werden müssen.

Code Typ	***Übertragungsrate kbit/s***	***Sprachqualität MOS[5]***	***Prozessorlast MIPS***	***Verzögerung ms***
G.711 PCM	64	4,3	0	0,125
G.721 ADPCM	32	4,1	6,5	0,125
G.723 MP-MLQ ACELP	5,3; 6,4	4,1	25	70
G.726 Multirate ADPCM	16 - 40	2,0 - 4,3	6,5	0,125
G.728 LD-CELP	16	4,1	37,5	2
G.729 CS-ACELP	8	4,1	34	20
G.729.a CS-ACELP	8	3,4	17	20

Tabelle 5 : Vergleich von Qualität und Komplexität von Audio Codecs [IBM98]

H.323 Terminals müssen mindestens die ITU Empfehlung G.711 unterstützen. Der verwendete Codec wird innerhalb der ***Capability Exchange*** nach H.245 festgelegt.
Asymmetrische Kommunikation - Nutzung verschiedenen Codecs innerhalb einer Kommunikation für Sende- und Empfangsrichtung - und die gleichzeitige Übertragung mehrerer ***Audio Channels*** sind ebenfalls zulässig. Das Terminal hat dann während einer Multipoint Konferenz die Aufgabe, die Audiosignale zu mixen.
Die Formatierung des Audiosignals erfolgt nach der ITU Empfehlung H.225.0.

Neben der Sprachkompression wurden Methoden zur ***Stummunterdrückung (Silence Suppression), Voice Activity Detection (VAD)*** und ***Comfort Noise Generation (CNG)*** zur Minimalisierung der benötigten Bandbreite bzw. ***Forward Error Correction, Echo Cancellation*** und ***Anti Jitter Methoden*** zur Vermeidung möglicher Störungen in die VoIP Technologie aufgenommen.

[5] MOS - Mean Opinion Score ist eine durch den Absolute Category Rating (ACR) Test der ITU-T SG12 genutzte Einheit zur Bewertung der Sprachqualität (nähere Informationen in Mino98 S.11), die von 5=excellent bis 1=bad reicht.
Siehe ITU-T P.800 für subjektive und ITU-T P.861/ P.561 für objektive Methoden zur Beurteilung der Sprachqualität.

2.4.4 Video

Die Unterstützung von Video ist für einen H.323 Terminal optional. Falls diese vorhanden ist, muß obligatorisch H.261 unterstützt werden. Zusätzlich kann H.263 verwendet werden.
Die Übertragungsrate wird während des Capability Exchange festgelegt.

- ***H.261*** wird im Zusammenhang mit Kommunikationskanälen, die eine Bandbreite von Vielfachen von 64 kbit/s (1-30) besitzen, genutzt. Neben voll kodierten Frames wird in einigen Fällen nur die Differenz aufeinander folgender Frames übertragen.
- ***H.263*** ist zu H.261 abwärtskompatibel, bietet eine verbesserte Bildqualität durch ½ Pixel Motion Estimation, Predicted Frames und ist durch Huffmann Kodierung eine optimale Anpassung an niedrige Übertragungsraten.

Asymmetrische Kommunikation - Nutzung verschiedenen Codecs innerhalb einer Kommunikation für Sende- und Empfangsrichtung - und die gleichzeitige Übertragung mehrerer ***Video Channels*** ist ebenfalls zulässig.
Die Formatierung des Audiosignals erfolgt nach der ITU Empfehlung H.225.0.

Bildformat	***Bemerkung***	***Bildgröße***	***H.261***	***H.263***
SQCIF	Sub-QCIF	128 x 96	optional	optional
QCIF	Quarter-CIF	176 x 44	obligatorisch	obligatorisch
CIF	CIF	352 x 288	optional	optional
4CIF	4-fach CIF	702 x 576	-	optional
16CIF	16-fach CIF	1408 x 1152	-	optional

Tabelle 6 : ITU Videocodecs [Klein98]

2.4.5 Daten

Durch die optionale Unterstützung von Data Conferencing werden Whiteboard Sharing, Application Sharing und Datei Transfer ermöglicht.

H.323 ermöglicht Data Conferencing durch die T.120 Spezifikation und Interoperabilität auf Applikations, Netzwerk und Transport Ebene.
T.120 unterstützt Point to Point und Multipoint Data Conferencing.

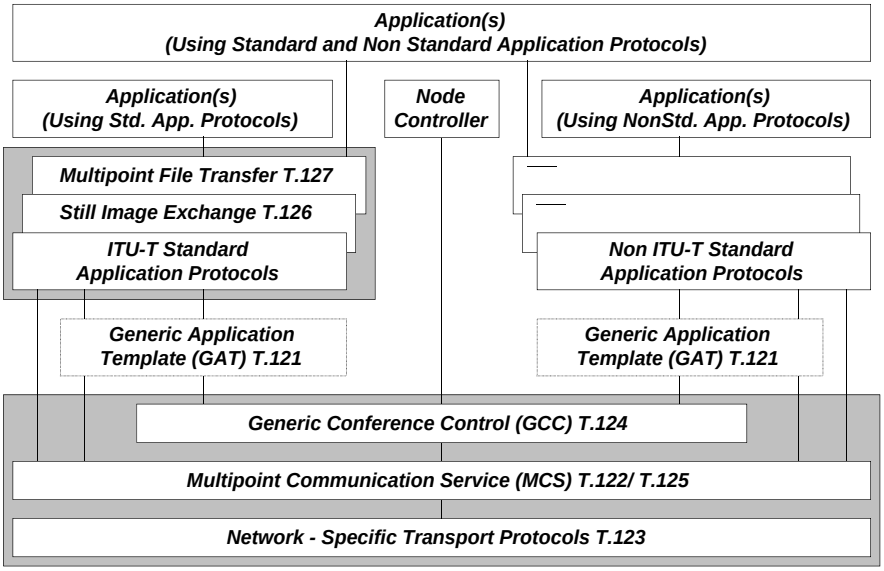

Abbildung 8 : T.120 Spezifikation [Klein98]

Die T.120 Fähigkeit kann in den Clients oder in MCUs implementiert sein. Die MCU steuert und mixt die Data Conference Informationen.
[Klein98], [H.323], [Mino98]

2.4.6 Implementierung heutiger TK Leistungsmerkmale

In der ITU Empfehlung H.323 Version 2 wurden zusätzliche Dienste (***Supplementary Services -SS***) integriert. Diese Dienste sind in den Empfehlungen H.450.x beschrieben und dienen der Abbildung von PBX Leistungsmerkmalen auf ein paketbasiertes LAN und der verbesserten Interoperabilität zwischen den H.323 Entities verschiedener Hersteller.

In den ersten drei verabschiedeten Empfehlungen der H.450 Serie sind neben der grundsätzlichen ***Signalisierung der Dienste*** (H.450.1 - Generic Funktion Control) auch ***Call Transfer*** und ***Call Diversion*** beschrieben, auf die im folgenden kurz eingegangen wird.
An weiteren Empfehlungen, die Leistungsmerkmale, wie ***Call Hold*** , ***Call Pick Up and Call Park***, ***Call Waiting*** , ***Message Waiting*** und ***Call Completion On Busy and No Reply*** wird derzeit (August 1999) gearbeitet.

H.450.2 - Call Transfer

H.450.2 beschreibt die Prozeduren und das Signalisierungsprotokoll [6] für den ***Call Transfer Supplemenary Service (SS-CT)***. Mit Call Transfer kann ein Gespräch zwischen Endpunkt A und Endpunkt B in ein Gespräch zwischen Endpunkt B und Endpunkt C übertragen werden. Endpunkt A kann, muß aber nicht vor dem Call Transfer eine Verbindung zu Endpunkt C unterhalten.

H.450.3 - Call Diversion

H.450.3 beschreibt die Prozeduren und das Signalisierungsprotokoll [7] für den Call Diversion Supplementary Service (SS-CD). Die Empfehlung umfaßt die Dienste :

- ***Call Forwarding Unconditional (SS-CFU)*** - unmittelbare automatische Weiterleitung aller ankommenden Gespräche,
- ***Call Forwarding Busy (SS-CFB)*** - automatische Weiterleitung aller ankommenden Gespräche, wenn ein Teilnehmer besetzt ist,
- ***Call Forwarding No Reply (SS-CFNR)*** - automatische Weiterleitung aller ankommenden Gespräche, wenn innerhalb einer vorgegebenen Zeit der angerufene Teilnehmer nicht antwortet,
- ***Call Deflection (SS-CD)*** - Weiterleitung aller ankommenden Gespräche nach Belieben eines Teilnehmers.

[H.450.2], [H.450.3], [Klein98]

2.4.7 Mechanismen zur Erhaltung des CoS

Die den CoS (Def. CoS, QoS siehe 3.1) betreffende Signalisierung wird durch den Terminal bzw. Gatekeeper zum frühest möglichen Zeitpunkt durchgeführt.
In einem Paket basiertem Netzwerk schließt CoS solche Charakteristiken mit ein wie :

- ***Bit Error Rate*** - die Korrektur von Bitfehlern wird in den unteren Schichten durchgeführt bzw. es resultieren aus ihnen Paketverluste,
- ***Packet Loss Rate*** - der Empfänger muß Mechanismen besitzen, den Paketverlust bis zu einem bestimmten Maß zu kompensieren [8]. Daten und Steuermeldungen werden bei Verlust erneut übertragen - ***Retransmission***,

[6] abgeleitet aus Call Tranfer Supplemetary Services in ISO/ IEC 13865 und 13869
[7] abgeleitet aus Call Division Supplemetary Services in ISO/ IEC 13872 und 13873
[8] z.B. bei Audio und Video Wiedergabe des vorangegangenen Pakets anstatt des verlorengegangenen

- ***Delay*** - es werden kurzzeitige Delay Erhöhungen und generelle, hervorgerufen durch Netzwerküberlastung, unterschieden.

Die Bewertung des CoS erfolgt anhand von RTCP

- ***Sender Reports*** - ermöglichen Synchronisation mehrerer RTP Ströme, Bekanntgabe von erwarteten Daten und Paketraten an den Receiver, Messung des Zeitabstandes zum Sender durch den Receiver

und

- ***Receiver Reports*** - Messung von CoS in H.225.0 durch Fraction Loss, cumulative packets lost, die extended highest sequence number received und interarrival Jitter.

Prozeduren zur Erhaltung von CoS

Es existieren eine Reihe von Methoden [9] für H.323 Terminals/ Gateways, auf die Erhöhung von Paketverlust und interarrival Jitter zu reagieren. Diese Methoden können in zwei Gruppen eingeordnet werden :

- ***short term response*** - reagieren auf kurzzeitige Probleme wie verzögerte oder verlorene Pakete durch : kurzzeitige Reduktion der Frame Rate, Reduktion der Paketrate durch Mixen von Audio und Video in ein Paket bzw. Nutzung von Macro Block Fragmentation des Video Stroms.
- ***long term response*** - reagieren auf langfristige Probleme, wie wachsende Belastung des Netzwerkes durch: Reduktion der Medienübertragungsrate, Reduktion auf wichtigsten Medientypen (z.B. Audio) bzw. Sendung eines Busy Signals zum Empfänger zur Anzeige von Netzwerküberlastung.

[H.225.0]

[9] Diese Methoden dienen nicht der strikten Erhaltung des derzeitigen CoS, sondern ermöglichen eine geordnete Verringerung der angebotenen Dienste

2.4.8 Transport Level Resource Reservation Procedures

H.323 schlägt die Nutzung von Ressource Reservierungs Mechanismen zum Erreichen des für die Übertragung von Real Time Audio und Video Strömen erforderlichen CoS vor .
In Appendix II werden dazu am Beispiel des ***RSVP*** allgemein die Transport Level Mechanismen zwischen den H.323 Entities beschrieben.
RSVP ist ein Ressource Reservierungsprotokoll der Transportschicht in IP Netzwerken. Zusammen mit den entsprechenden ***CoS Diensten*** [10], ***Scheduling Mechanismen*** [11] und ***Policy based Admission Control*** kann RSVP die CoS Anforderungen der H.323 Konferenzteilnehmer erfüllen.
In Kapitel 4 werden Mechanismen zur Datenpriorisierung bzw. im Zusammenhang der Vorstellung der vom Cisco IOS zur Verfügung gestellten Priorisierungsmechanismen in Kapitel 5, am Beispiel des AOK Datennetzes, Priorisierungs- und Scheduling Mechanismen näher erläutert.

QoS Support für H.323

In einem ***Admission Request*** - ***ARQ*** - an den Gatekeeper muß ein Endpunkt seine Fähigkeit zur Ressourcen Reservierung anzeigen. Aufgrund dessen und der Informationen über den Netzwerk Status trifft der Gatekeeper seine Entscheidung:

- erlaubt Endpunkt den eigenen Reservierungs Mechanismus für dessen H.323 Sitzung anzuwenden,
- führt Ressource Reservierung für den Endpunkt durch,
- Ressource Reservierung ist nicht notwendig - ***Best Effort*** ausreichend.

Die Entscheidung des Gatekeepers wird dem Endpunkt in der ***Admission Confirm*** - ***ACF*** - mitgeteilt.
Falls der Endpunkt Ressource Reservierung nicht unterstützt und der Gatekeeper entscheidet, daß diese vom Endpunkt durchzuführen ist, wird der ***ARQ*** mit einer ***Admission Reject*** - ***ARJ*** - Nachricht zurückgewiesen.

[10] z.B. Guaranteed Service, Controlled Load - siehe 3.2; RSVP fähiger H.323 Endpunkt muß mindestens Controlled Load unterstützen
[11] z.B. Weighted Fair Queuing

Das spezielle Feld, das innerhalb der H.225.0 RAS Signalisierung diese Funktionalität erlaubt, ist das ***TransportQOS*** Feld.
Zusätzlich zu diesem Feld sollte der Endpunkt die voraussichtlich von ihm genutzte Bandbreite dem Gatekeeper im ***bandWidth*** Feld der ***ARQ*** Nachricht mitteilen, unabhängig von der Ressourcenreservierung.
Erforderliche Bandbreitenänderungen werden über ***Bandwidth Request*** - ***BRQ*** - dem Gatekeeper mitgeteilt, gleichfalls unabhängig von der Ressourcenreservierung.

H.245 Capability Exchange Phase

Während der H.245 Capability Exchange Phase erfolgt ein Austausch über die Sende und Empfangsfähigkeiten zwischen den Endpunkten inclusive der ***QOSCapability***. Da diese Informationen sich aber auf die Gesamtheit aller Medienströme beziehen, ist es nur sinnvoll, allgemeine Angaben zur Unterstützung bzw. Nichtunterstützung von RSVP im ***Capability Set*** zu treffen. Dazu wird das ***QOSMode*** Feld innerhalb der Capability PDU entsprechend gesetzt.

Open Logical Channel and Setting Up Reservation[12]

Am Beispiel einer Punkt zu Punkt Verbindung werden in diesem Abschnitt das Öffnen eines Logical Channels und die Ressourcen Reservierung dargestellt.
Im ***QOSCapability*** Feld der ***OpenLogicalChannel*** Nachricht spezifiziert der Sender die RSVP Parameter des zu übertragenden Medienstroms und die von ihm unterstützten Integrated Services. Im Falle einer Punkt zu Punkt Verbindung legt der Sender keinen Receiver Port ID in dieser Nachricht fest. Dieser ID wird nach dem Erhalt der Nachricht vom Receiver ausgewählt und an den Sender in der ***OpenLogicalChannelAck*** Nachricht übermittelt.
Dann kann der Sender eine RSVP Session für den Medienstrom aufbauen und beginnen, ***Path*** Nachrichten auszusenden[13].

> Der Receiver kann den Empfang des Medienstromes bis zum vollständigen Aufbau der RSVP Reservierung verzögern, indem er das Boolean ***flowcontrolToZero*** Feld ***der OpenLogicalChannel*** Nachricht auf *true* setzt. Wenn der Sender diese Nachricht mit auf *true* gesetztem ***flowcontrol-ToZero*** Feld erhält, muß er seinerseits die Übertragung verzögern, bis die RSVP Reservierung abgeschlossen ist.

[12] Reservierungen werden nur aufgebaut, wenn beide Endpunkte RSVP Unterstützung anzeigen.
[13] Der Receiver hat bereits vor dem Versenden der OpenLogicalChannelAck Nachricht Informationen, um für den Medienstrom eine RSVP Session aufzubauen (Receiver IP Adresse oder Multicast IP Adresse, Receiver Port ID und genutztes Protokoll - UDP)

Der Receiver antwortet auf die empfangenen ***Path***[14] Nachrichten des Senders mit RSVP ***Resv***[15] Nachrichten. Die Reservierung ist abgeschlossen, wenn der Receiver daraufhin eine RSVP ***ResvConf*** Nachricht zur Bestätigung der Reservierung erhält.

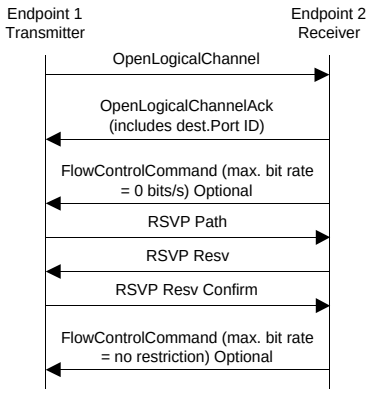

Abbildung 9 : Öfnnung eines Unicast Logical Channels mit RSVP [H.323]

Der Receiver sendet das ***FlowControlCommand*** zum Sender, um die Einschränkung der Bitrate des Medienstroms (Effekt des *true* gesetzten ***flowcontrolToZero*** Feldes) aufzuheben.

Close Logical Channel and Tearing Down Reservation

Bevor für einen speziellen Medienstrom eine ***CloseLogicalChannel*** Nachricht gesendet wird, muß, falls für diesen Strom eine RSVP Session initiiert wurde, vom sendenden Endpunkt eine ***PathTear*** Nachricht übertragen werden.

Wenn ein empfangender Endpunkt eine ***CloseLogicalChannel*** Nachricht für einen Medienstrom erhält, muß er eine ***ResvTear*** Nachricht übertragen, falls für diesen Strom eine RSVP Session initiiert wurde.

[H.323]

[14] ***Path*** Nachrichten hinterlassen in Router „states“ auf dem Weg zum Ziel - beinhaltet Quell und Zieladresse und Chrakterisierung des zu sendenden Medienstromes

[15] ***Resv*** Nachrichten beinhalten die eigentliche Reservierung

2.5 H.323 über Transportnetze mit garantiertem QoS - ATM

Annex C der Empfehlung H.323 beschreibt eine optionale Methode, die H.323 Endpoints ermöglicht, Medienströme mit QoS über die AAL 5 von ATM Netzwerken zu übertragen.

Im Allgemeinen kann H.323 immer über ATM mittels der verschiedenen IP over ATM Methoden (z.B. CLIP, LANE) genutzt werden. Diese Ansätze sind aber weniger effektiv als die direkte Nutzung der AAL 5 VCs zur Übertragung der Medienströme. Zusätzlich profitieren sie vom QoS basierten ATM VC.

Der Kommunikation von H.245 und H.225.0 liegt weiterhin ein Paket basiertes Netzwerkprotokoll (z.B. IP) zugrunde, um die Kommunikation mit H.323 Endpunkte zu gewährleisten, die ein solches Protokoll für sämtliche Verbindungen nutzen. Die Interoperabilität wird durch die Anforderung eine ***Basic Mode of Operation*** erreicht, bei dem Medienströme über den Datagram Dienst eines Paket basierten Netzwerkprotokolls (UDP/ IP über ATM) übertragen werden. Im ***Basic Mode*** kann der QoS des Netzwerkes nicht ausgenutzt werden.

Architektur

Die Protokoll Architektur in der nachfolgenden Abbildung nutzt IP über ATM für die H.225.0 bzw. die H.245 Kommunikation und für RTCP. Die Medienströme werden auf RTP direkt über die AAL 5 übertragen.

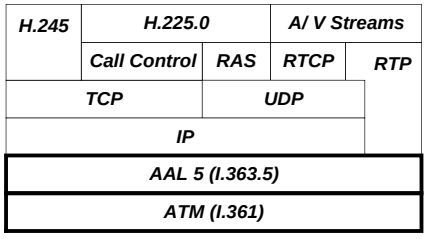

Abbildung 10 : Protkoll Stack für H.323 on ATM [H.323]

H.225.0 auf IP über ATM

Die H.225.0 Kommunikation setzt TCP/ IP und UDP/ IP, implementiert durch eine Methode von IP über ATM, voraus.

Wird der Endpunkt zusammen mit einem Gatekeeper genutzt, erfordern die Prozeduren zum GK Discover und zur Registrierung UDP Mulicast. Falls das Netzwerk dies nicht unterstützt, muß der Endpoint mit der Adresse des Gatekeepers vorkonfiguriert werden.

H.245 auf TCP/ IP über ATM

Der Aufbau von H.323 Verbindungen über die AAL 5 ist dem des Basic Mode von H.323 über IP ähnlich. Der Unterschied besteht darin, daß die abgeschlossene ***OpenLogicalChan-nel*** Prozedur in den Aufbau eines AAL 5 VC resultiert. In Abbildung 11 ist dieser Ablauf für den Aufbau einen bidirektionalen und unidirektionalen VC[16] dargestellt.

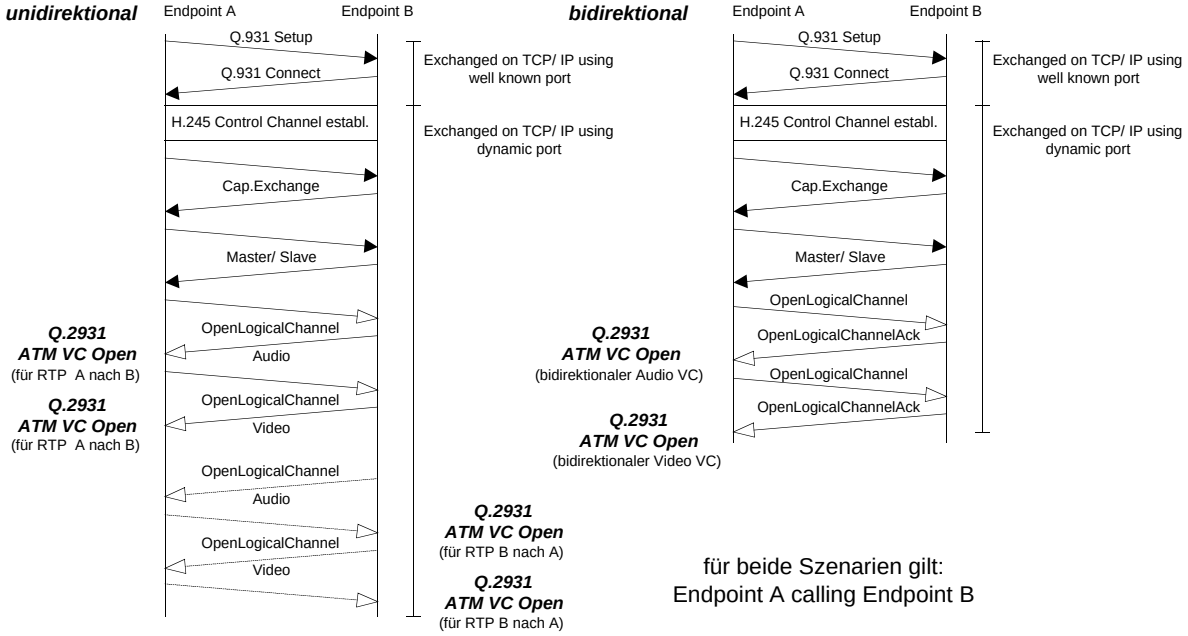

Abbildung 11 : H.323 Verbindungsaufbau über ATM [H.323]

Zusätzliche Transport Capabilities zum Terminal Capability Set (H.245)

Der Terminal Capability Set aus H.245 mußte für H.323 on AAL 5 erweitert werden. Dies umfaßt ***Transport Level Capabilities*** , wie die Unterstützung für die ***ATM Transfer Capabi-lity*** nach I.371 (DBR, SBR1, SBR2, SBR3, ABT/ DT, ABT/ IT, ABR).

Terminals die diese Erweiterung nicht unterstützen, können H.323 on ATM nicht nutzen.

[16] Da Punkt zu Punkt ATM VCs von sich aus bidirektional sind, ist es wünschenswert beide Richtungen zu nutzen. Endpunkte, die H.323 über ATM unterstützen, sollten daher bidirektionale Medienkanäle öffnen.

Adressierung von A/ V Strömen

H.323 bietet die Möglichkeit der getrennten Adressierung von A/ V Strömen und der H.245 Control Channel, sowie die getrennte Adressierung von RTP und RTCP Strömen. Somit können Audio und Videoströme an eine IP Adresse und optional direkt mittels RTP über die AAL5 an eine ATM Adresse gesendet werden.
Die ATM Adresse [17] für einen RTP Strom befindet sich im ***mediaChannel*** Subfeld der ***H2250LogicalChannelParameter*** der H.245 ***OpenLogicalChannel*** Nachricht.

A/ V Ströme auf RTP über AAL 5

Mit Beendung der H.245 ***OpenLogicalChannel*** Primitive erfolgt der Setup von Medienströmen an die Ziel ATM Adresse. Die Wahl der im AAL Parameter Informations Element enthaltenen MTU Größe beeinflußt dabei die Effektivität des Systems aufgrund der AAL 5 Paketierung (siehe I.363.5 AAL 5 Paketierungsregeln).
Der Inhalt des Adress Feldes im ***mediaChannel*** legt fest, ob ein ATM VC oder ein UDP Port geöffnet wird. Schlägt der Setup über ATM fehl, muß der Endpunkt über RTP/ RTCP und UDP einen erneuten Versuch starten.

Interoperabilität mit H.323 über IP

Da H.225.0 und H.245 weiterhin über IP ablaufen, können alle H.323 Endpunkte eines IP Net-zes miteinander kommunizieren. Falls ATM Endpunkte den neuen ***transportCapability*** Set in H.245 nicht unterstützen, müssen die ***OpenLogicalChannel*** Prozedur und die Übertragung der Medienströme im Basic Mode of Operation über UDP/ IP erfolgen.
Diese Maßnahmen ermöglichen die Interoperabilität zwischen H.323 Endpunkte, die den Annex C unterstützen und denen, die es nicht tun.
[H.323 Annex C]

[17] 20 byte NSAP Adresse; E.164 wird als IDP Teil einer NSAP Adresse gekapselt

2.6 Möglichkeiten der Implementierung im Intra-/ Internet

2.6.1 Einsatzszenarien von VoIP

Basisszenarien

Der Einsatz von VoIP läßt sich durch drei Basisszenarien (ähnlich den TIPHON Szenarien) beschreiben:

- ***PC zu PC*** - Kommunikation zwischen einzelnen PCs mittels entsprechender Software (z.B. MS Netmeeting),
- ***PC zu PSTN Telefon*** - über Gateways werden Verbindungen zum PSTN möglich,
- ***PSTN Telefon zu PSTN Telefon*** - Kommunikation zwischen PSTN Telefonen mittels Gateways über ein IP Netz.

Einsatz im Unternehmen

Ausgehend von den Basisszenarien ergeben sich verschiedenste Möglichkeiten des Einsatzes im Unternehmensfeld, in denen VoIP heute kostensparend eingesetzt werden kann.

- ***TK - Anlagenkopplung*** - sind Unternehmen an unterschiedlichen Standorten vertreten, ergibt sich die Notwendigkeit die TK Anlagen untereinander zu verbinden, damit Funktionalitäten und spezifische Leistungsmerkmale standortübergreifend zum Einsatz kommen.

  Die heute dazu genutzten Standleitungen können durch eine Kopplung über IP basierende Netze ersetzt werden, die gleichzeitig neben einer hohen Kompressionsrate für Sprache, deren Integration mit Daten bietet. Vorraussetzung ist das QSIG Tunneling, um TK Leistungsmerkmale transparent über IP zu übertragen.
- ***Call Center*** - um kurzzeitige Auslastungsspitzen abzudecken wird auf örtlich entfernte Call Center bzw. Heimarbeiter zurückgegriffen. Die Übertragung der Leistungsmerkmale und die anfallenden Sprachgebühren sind wie bei der TK Anlagenkopplung von übergeordneter Bedeutung. Ein solches Szenario mit ACD Funktionalität kann heute bereits komplett mit VoIP abgedeckt werden.
- ***Web enabled Call Center*** - zusätzliche Bedeutung erhält VoIP durch die Verbreitung von Internet Call Centern. Der Anwender kann über den ***Call Me Button*** einen Verbindungsaufbau initiieren (z.B. startet Netmeeting).

  Wichtig ist, daß die Webseite des entfernten Anwenders angezeigt wird, wodurch direkt auf Fragen des Anwenders eingegangen werden kann bzw. die Möglichkeit des ***Assisted***

Browsing besteht, bei dem der Call Center Agent eigene vorbereitete Seiten im Browser des Anwenders aktivieren kann.

[Polte98]

Nutzen für den Anwender

Entscheidungsgründe für den Anwender zum Einsatz von VoIP sind neben dem hauptsächlichen, der Reduzierung der Kommunikationskosten :

- Vereinfachung der Kommunikationsbeziehungen über standardisierte Technologie,
- Perspektive der Ausdehnung der Kommunikation mit IP über das Weitverkehrsnetz,
- geringe Komponentenkosten im Vergleich zu lokalem ATM (- falls vorhanden kann es nur zur LAN Emulation mit IP genutzt werden, wegen fehlender nativer ATM Applikationen),
- Zusammenfassung von TK und LAN Netzwerkmanagement möglich (herstellerabhängig), und
- Konzentration der bestehenden IT Organisationsstruktur in eine zentrale IT Verantwortung.

Die Kosteneinsparung ist besonders für den Betreiber der Infrastruktur von hoher Bedeutung. Für die Fachabteilungen eines Unternehmens besteht das oberste Ziel in der optimalen Aufgabenerfüllung.

Dazu gehört die durch geeignete Technik gewährleistete:

- Unterstützung relevanter Prozesse und Abläufe, sowie
- Optimierung des Kundenservice für alle dienstleistungsorientierten Abteilungen.

An dieser Schnittstelle kann IP Telefonie einen entscheidenen Beitrag leisten:

- TK relevante Informationen stehen DV Anwendungen zur Verfügung (z.B. Integration des Telefonbuches der TK Anlage - Hicom - in MS Outlook),
- einfacher Übergang von Sprach- zur Multimediakommunikation,
- Vereinfachung der Infrastruktur möglich, eventuell zusätzliche Komponenten (z.B. Server) nötig.

[Hohg3/99]

Kosteneinsparung - wirtschaftlicher Nutzen

Da im Rahmen der Diplomarbeit die technischen Möglichkeiten von VoIP erläutert werden, erfordert die unternehmensspezifische Einschätzung des wirtschaftlichen Nutzens von VoIP weitere Untersuchungen.

Im Folgenden werden einige der zu beachtenden Aspekte einer möglichen wirtschaftlichen Untersuchung (Vergleich PBX, LAN, VoIP) aufgeführt :

- Kosten für die Investition, den Betrieb, Update/ Upgrade;
- MTBF der Switche, GK, Server und Auswirkung auf die Kosten als Einzelgeräte;
- MTBF bzw. Zuverlässigkeit der Clients;
- Verfügbarkeit von S_0 und S_{2M} ;
- Stabilität des Übertragungsprotokolls;
- Kosten für redundante Steuerungen, Baugruppne und Carrieranbindungen;
- Personalvorhalt etc..

2.6.2 Möglichkeiten der Migration

Nachfolgend werden vier Möglichkeiten der Migration von VoIP dargestellt.

Die ersten beiden Möglichkeiten beschreiben die Migration innerhalb einer PBX, die zwei weiteren beschreiben die Implementierung von VoIP im LAN.

Die Vorteile einer Internet Enabled PBX bestehen in auf der

- ***Line Side*** - reduzierte Verkabelungs- und Betriebskosten durch Integration von Sprache und Daten; Sprache Daten Integration in zuküftigen Terminals - z.B. IP Telefonen
- ***Trunk Side*** - Least Cost Routing mittels Intranet und ITSP - Internet Telephony Service Provider.

Bolt On

Die vorhandene TK Anlage wird durch separate Geräte (z.B. GW) um die VoIP Funktionalität erweitert.

Dies stellt einen möglichen Weg dar, um VoIP im Unternehmen zu testen.

Eine weitere Vereinfachung der Verkabelung wird erreicht, und unter der Voraussetzung, daß alle Standards bereits implementiert wurden, sind unabhängige Line und Trunk Side Upgrades möglich.
Zu beachten ist, ob der durch VoIP bereitgestellte Feature Set ausreichend ist.

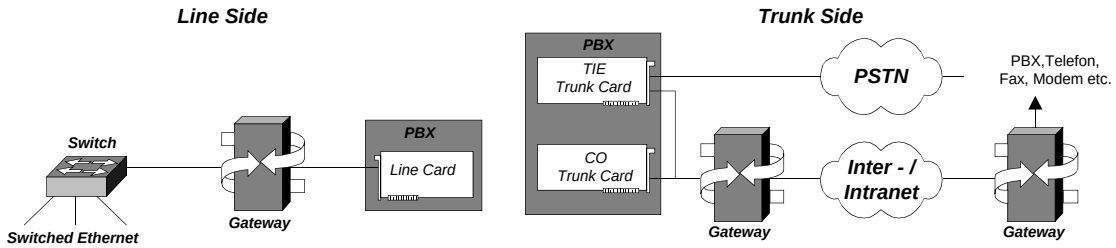

Abbildung 12 : Intergration von VoIP - Bolt On [Telo98][18]

Integrate

Die VoIP Funktionalität wird in die vorhandene TK Anlage integriert.
Die IP Line und Trunk Card beinhalten die Features der Standard PBX Karten.
Da der PBX Hersteller selbst die VoIP Lösung implementiert, kann im Verlauf der Integration eine homogene Umgebung mit einheitlichen Management geschaffen werden und frühere PBX Investitionen des Kunden geschützt werden.

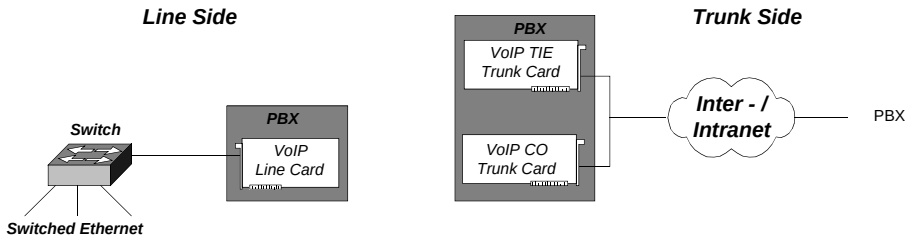

Abbildung 13 : Integration von VoIP - Integrate [Telo98]

Fork Lift

Das vorhandene LAN wird um die VoIP Funktionalität erweitert.
Diese Lösung eignet sich für kleine Umgebungen, wobei darauf zu achten ist, ob der durch VoIP benötigte Feature Set ausreichend ist. Notwendige Redundanzen bzw. Skalierbarkeit kann durch Dopplung der Server erreicht werden.

[18] TIE Trunk - Verbindung zu anderen PBXen; CO Trunk - Verbindung zum Carrier Central Office und PSTN

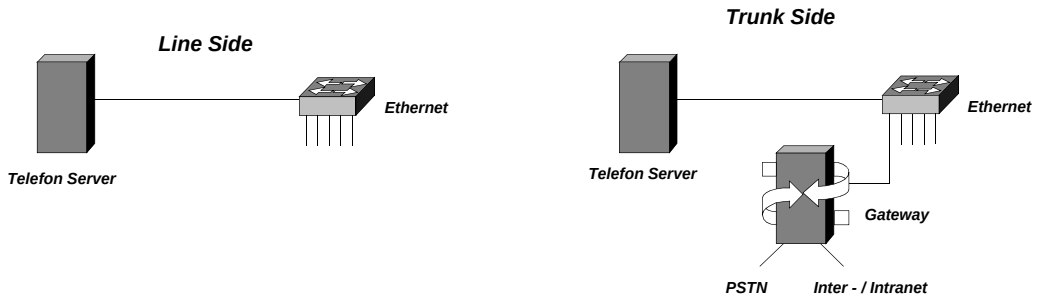

Abbildung 14 : Integration von VoIP - Fork Lift [Telo98]

Outsource

Die Bereitstellung der VoIP Funktionalität wird einem Carrier übergeben.

Kleine Office Umgebungen können so VoIP ohne größeren technischen Aufwand VoIP nutzen. Es ist jedoch in jedem Fall der betreibswirtschaftliche Aufwand (Investieren oder Finanzieren) abzuwägen. Eine entscheidende Rolle spielt dabei die Vertragsgestaltung mit dem Carrier.

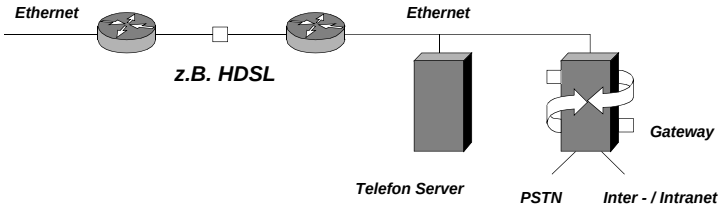

Abbildung 15 : Integration von VoIP - Outsource [Telo98]

Beispiele für VoIP Implementierungen der Hersteller sind im Kapitel 5 beschrieben.

[Telo98]

3 Mechanismen zur Optimierung des Datenflusses

Für das IP Protokoll auf Schicht 3 [19] ist das darunterliegende Netzwerk transparent und somit auch für die Implementierung von VoIP. Dennoch beeinflußt die eingesetzte LAN Technologie indirekt die Leistungsfähigkeit und Effektivität der Implementierung - eine Übersicht über die Eignung von LAN Technnologien zur Übertragung von Echtzeit Verkehr befindet sich im Anhang A.1.
Besonders in großen LAN Umgebungen, insbesondere die die WAN Verbindungen mit einschließen, erfordern besondere Maßnahmen, wie Priorisierungsmechanismen bzw. Mechanismen zur Reservierung von Bandbreite, um Delay sensitiven Verkehr zu übertragen.

Von echtzeitfähigen Datenübertragungssystemen wird gefordert, daß sie die Datagramme mit einer ***garantierten Verzögerungszeit*** und mit einer bei Verbindungsaufbau ***vereinbarten Bandbreite*** übertragen. Schwankungen der Verzögerungszeit (Jitter) müssen durch geeignete Methoden (z.B. Puffer) ausgeglichen werden, welche jedoch die Gesamtverzögerung erhöhen. Die Datagramme müssen in der ***korrekten Reihenfolge*** das Ziel erreichen.
Die Unterstützung von ***Gruppenkommunikation*** (Point to Point, Point to MultiPoint), sowie die effiziente Übertragung von kleinen Datenpaketen ist zu gewährleisten.

Delay (ms) /one way	***Bewertung***	***Topologie***	***typ. Delay (ms) / one way***
< 100	nicht wahrnehmbar	PSTN	50 - 70
100 - 200	wahrnehmbar, aber tolerierbar	Intranet	70 - 120
> 200	zunehmend störend	Internet	500 - 1200
> 400	prakt. Halbduplex		

Tabelle 7 : Verzögerungszeiten [Lang98], [IBM98]

Die Aussagen zum switched Ethernet LAN sind dabei wegen seiner Verbreitung von besonderer Bedeutung. In Tabelle 16 im Anhang A.1 sind die Ethernet Techniken entsprechend ihrer Übertragungsreichweite gegenübergestellt.
Im ***geswitchtem Ethernet-LAN*** ist Hauptkriterium für die Echtzeitfähigkeit die Paketverzögerung (IEEE: max. 10ms für Sprachverkehr - Voice Type - im LAN).

Die Paketverzögerung setzt sich zusammen aus der :

- der ***Ausbreitungsverzögerung*** - abgeleitet aus der Laufzeit im Medium - (in 100m UTP ca. 500ns) bei UTP wird je nach Güte des Kabels aber nur eine Ausbreitungsbeschwindigkeit von ca. 0,6 bis 0,7 der Lichtgeschwindigkeit erreicht,
- der ***Übertragungsverzögerung*** - abhängig von der Übertragungsgeschwindigkeit (10, 100, 1000 Mbit/s und der Paketgröße (64 - 1500 byte), und
- der ***Verarbeitungsverzögerung*** - bestehend aus der Zeit zur Paketanalyse und Bestimmung des Ausgangsports, Verzögerung durch Warteschlangen (vor allem bei hohem Verkehrsaufkommen) und der Zugriffswartezeit, wenn das Übertragungsmedium durch ein Paket einer anderen Warteschlange belegt ist.

Meßwerte belegen (siehe Flatt98), daß Transportverzögerung und Zugriffswartezeit erheblichen Einfluß auf die Gesamtverzögerung haben. Durch Erhöhung der Bandbreite kann eine deutliche Verbesserung erreicht werden. Dies ändert jedoch nichts an der Ursache des Problems. Besonders bei hoher Belastung nimmt die Verzögerung durch Warteschlangen zu, welches bis zum Paketverlust führen kann.
Das Ziel aller CoS Mechanismen (in Kapitel 3.1 erfolgt einführend eine Abgrenzung der Begriffe ***Class of Servie*** und ***Quality of Service***) ist deshalb die Entschärfung des Warteschlangenproblems z.B. durch ***Priorisierung - IEEE 802.1p*** - oder den Einsatz ***der Integrated Services Architektur***.

Die oben genannten Aussagen gelten für die Umgebung eines Switches bzw. Routers. In grossen geswitchten und gerouteten Netzwerkumgebungen mit mehreren Switching oder Routing Hops summieren sich die genannten Faktoren ohne Ergreifung besonderer Maßnahmen (z.B. Layer 3/ 4 Switching), insbesondere die erhöhte Verarbeitungsverzögerung durch mehrere Routing Hops wirkt sich negativ aus. Mit Verfahren wie Layer 3 und 4 Switching können Engpässe durch stark belastete Router umgangen werden. Nähere Aussagen über Layer 3 und 4 Switching können den Kapiteln 3.4 und 3.5 entnommen werden.

Im folgenden wird betrachtet, ob und welche Mechanismen (z.B. Datenpriorisierung, Bandbreitenreservierung, Switching) heutige Netzwerktechnologien (Schicht 2 bis 4 ISO/OSI) zur Übertragung isochroner Daten bieten.
[From95],[Flatt98]

[19] der Begriff Schicht bezieht sich hier auf das ISO/OSI Referenzmodell

3.1 Class of Service und Quality of Service

QoS/ CoS Mechanismen bilden die Grundlage für Policy Based Network Management und eine den Verkehrsanforderungen entsprechende Priorisierung.

Quality of Service

QoS Mechanismen im Sinne von ATM stellen speziell den Anforderungen des einzelnen Applikationsflows entsprechend Service Level bereit, um den erwarteten Qualitätslevel zu erhalten.

Es wird vor dem Etablieren einer Verbindung ein Verkehrsvertrag abgeschlossen, der die Einhaltung der Verkehrs- und Performance-Parameter (z.B. PCR, SNR, MCR, CDV, CLR ,CER) regelt.

RSVP auf einzelne Applikationsflows angewendet, wird ebenfalls als QoS Mechanismus akzeptiert. Im Gegensatz dazu stellt RSVP im Zusammenhang mit Integrated Services Architektur lediglich einen CoS bereit.

QoS erlaubt eine Service Level Garantie bei Übertragung von isochronen Signalen.

Class of -Service

CoS Mechanismen mappen die Flows der Applikationen entsprechend deren Anforderungen an Verzögerung und Bandbreite in wenige Service Klassen. Der Anspruch der Garantie bei QoS wird nicht aufrecht erhalten.

CoS erlaubt nur eine Priorisierung der Übertragung (siehe Kapitel 3.2 und Integrated Services Architekture in Kapitel 3.3). Im Draft Status der IEEE befindet sich ***Differentiated Services*** als Policy/ Rule basierte CoS Mechanismus (siehe Kapitel 3.3).

In den Kapiteln 3.2 und 3.3 werden die CoS Methoden näher erläutert.

[Intel99]

3.2 Verfahren zur Datenpriorisierung in Ethernet LANs auf Schicht 2

Wie in der Einleitung des Kapitels 3 dargestellt, müssen Verfahren zur Datenpriorisierung im Ethernet eingesetzt werden, um eine CoS sicher zu stellen, der die Übertragung isochroner Daten ermöglicht.

Die Grundfunktionen von CoS Mechanismen bestehen aus ***Queuing/ Scheduling*** , ***Traffic Policing***, ***Admission Control***, ***Signalisierungsmechanismen*** und ***Klassifizierung***[20].
Die wichtigsten Funktionen jedes CoS Mechanismus bestehen im Queuing und Scheduling. Neben proprietären Verfahren haben sich die ***802.1p/q Normen*** der IEEE für Netzwerkelemente auf ISO/OSI Schicht 2 (Switche) durchgesetzt.
In konventionellen LAN werden alle Datenpakete von den Koppelelementen gleichbehandelt. Es gibt ***eine*** Warteschlange, die nach dem FIFO Prinzip arbeitet. Die 802.1p/q Normen verwenden zwei und mehr Warteschlangen (entspricht mehr Traffic Classes) pro Link[21].
Am Eingang der Warteschlange entscheidet die Klassifizierung in welche Queue ein Datenpaket geleitet wird. Am Ende der Schlange erfolgt das Prioritäts Scheduling. In Abbildung 16 wird diese Prozeß verdeutlicht.

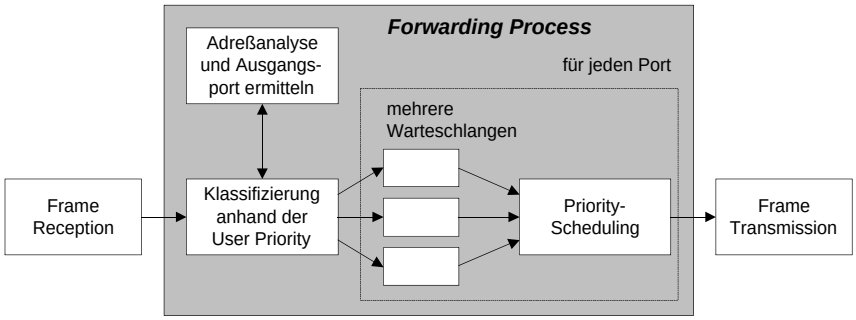

Abbildung 16: Klassifizierung und Scheduling beim IEEE 802.1p [Flatt98]

Klassifikation

Die Klassifizierung erfolgt durch eine Erweiterung des MAC Rahmens um 3 bit - das ***User Priority Feld***. Somit ist die Unterscheidung von 8 Verkehrsklassen möglich.
Die Zuordnung von User Priority und Warteschlangen hängt von deren Anzahl ab. Die Anzahl der Warteschlangen selbst ist nicht festgelegt.

Scheduling

Die IEEE spezifiziert einfaches ***Prioritäts Scheduling*** , d.h. die Warteschlange wird streng nach Priorität bedient. Dies hat den Nachteil, daß andere Warteschlangen bei einer großen Anzahl von Paketen mit hoher Priorität blockiert werden. Die Integrated Services Architektur verfolgt einen flexibleren Scheduling Ansatz (siehe 3.2).

[20] Siehe auch Verfahren zur Datenpriorisierung auf Schicht 3; einige Features, wie Signalisierung und Admission Control sind nur im dort beschriebenen Ansatz der IETF enthalten.
[21] Mehrere Warteschlangen pro Link machen Scheduling Verfahren erforderlich.

Anzahl der Warteschlangen	***unterscheidbare Verkehrsklassen***							
1	BE							
2	BE				VO			
3	BE				CL		VO	
4	BK		BE		CL		VO	
5	BK		BE		CL	VI	VO	
6	BK		BE	EE	CL	VI	VO	
7	BK		BE	EE	CL	VI	VO	NC
8	BK	-	BE	EE	CL	VI	VO	NC

Traffic Type	***Abkürzung***	***User Priority***
Background	BK	1
Frei	-	2
Best Effort	BE	0 (default)
Excellent Effort	EE	3
Controlled Load	CL	4
Video (Verzögerung < 100ms)	VI	5
Voice (Verzögerung < 10 ms)	VO	6
Network Control	NC	7

Abbildung 17 : Verkehrsklassen und Warteschlangen [Flatt98]

Signalisierung

802.1p benötigt keine Signalisierung, da jedes Frame mit der User Priority markiert wird, die seinem ***Traffic Type*** entspricht und in die zugehörige Warteschlange eingereiht wird.
Layer 2 Geräte nutzen die Information der User Priority, um kritischen Daten Vorrang vor anderen einzuräumen.
Ein Problem dabei ist, daß nicht in allen MAC Verfahren ein User Priority Feld vorgesehen ist, und das Ethernet Frame so unter Umstände länger als normale Frames wird. Deshalb müssen alle beteiligten Ethernetkomponenten auch den VLAN Standard 802.1q unterstützen. Dieser definiert eine Frame Erweiterung - ***Frame Tagging***.
In neuen Ethernet Spezifikation, wie Gigabit Ethernet ist diese Erweiterung bereits berücksichtigt.

Die Haupteigenschaften von 802.1p sind somit:

- kommt mit Layer 2 Switchen aus,
- unterscheidet Rahmen anhand von max. 8 Verkehrsklassen,
- Rahmenkennzeichnung durch User Priority,
- einfaches Priority Scheduling, keine Reservierung von Resourcen,
- kein Signalisierungsprotokoll nötig,
- keine Admission Control,
- reiner Vorrangtransfer,
- keine Garantien für die Übertragung möglich.

Der IEEE 802.1p Ansatz wird eingesetzt, wenn die Anforderungen an ein LAN klar festgelegt sind (z.B. Automatisierungstechnik). Wegen seiner geringen Komplexität wird er sich in LANs, die durch Switche segmentiert werden, durchsetzen (siehe auch 1.7 Layer 4 Switching).

Für Router muß die Layer 2 Priorisierung in ein Layer 3 Priorisierungsschema gemapped werden, damit diese die Priorisierungsinformationen nutzen können.
[Detk98], [Flatt98]

3.3 Verfahren zu Datenpriorisierung auf Schicht 3

Neben proprietären Ansätzen hat sich die ***Intergrated Services Architektur*** der IETF zur Datenpriorisierung, welche Funktionen für Koppelelemente auf ISO/OSI Schicht 3 (Router) beschreibt und die Priorisierung mittels des Type of Service Feldes des IPv4 Headers, wie in Kapitel 4.1 beschrieben, durchgesetzt. In der Draft Phase befindet sich der IETF Ansatz Differentiated Services (siehe 3.3.2).

3.3.1 Integrated Services Architekture

Unter Integrated Services (RFC 1633) versteht die IETF die Integration von echtzeitfähigen und zeitunkritischen Diensten sowie die Fähigkeit bedarfsweise Zuteilung von Bandbreite.

Die Architektur besteht im wesentlichen aus:

- ***Flows*** - Ströme zusammenhängender Datenpakete, die aus einer einzelnen Benutzeraktivität resultieren und gleichen CoS erfordern (z.B. Bilddaten einer Videokonferenz);
  der Flow kann unicast oder multicast übertragen werden, jedoch immer ***simplex***.
- ***Class of Service*** Einteilung
  1. ***Best Effort*** - heutige Datendienste im Internet (nutzbare Bandbreite und Verzögerungscharakteristiken lastabhängig)
  2. ***Controlled Load Service*** - Übertragung der meisten Datenpakete mit geringer Verzögerung und Verlustrate (auch bei Überlast); Dienst garantiert keine QoS Parameter.
  3. ***Guaranteed Service*** - Garantie von bestimmter Verzögerung, Verlust und Fehlerrate, sowie Bandbreite (Vorraussetzung: alle Koppelelemente zwischen Sender und Empfänger unterstützen Dienst).
- ***Reservierung von Ressourcen*** - über diesen Signalisierungsmechnismus teilen die Applika-tionen dem Netz ihre Anforderungen mit;
  Das ***RSVP*** (RFC 2205) als Signalisierungsprotokoll, ***Admission Control*** und ***Traffic Policing*** bilden die Grundfunktionen der Ressourcenreservierung.

RSVP wird unterstützt z.B. von Routern, Layer 3 Switchen, MS NT Server Implementierungen (< 4.0) und auf der Clientseite von der Windows 98 API bzw. Intel PC RSVP.

Klassifikation

Die Klassifikation wird anhand der Felder im IP Protokoll Header durchgeführt. Alle Datenpakete eines Flows werden in die gleiche Warteschlange eingereiht.

Scheduling

Es wird das ***Weighted Fair Queuing - WFQ*** , das die Anzahl und Länge der Datenpakete berücksichtigt, verwendet. Die Prioritäten für die Warteschlange können variabel vergeben und die Bandbreite eines Links kann so auf mehrere Verkehrsklassen aufgeteilt werden.

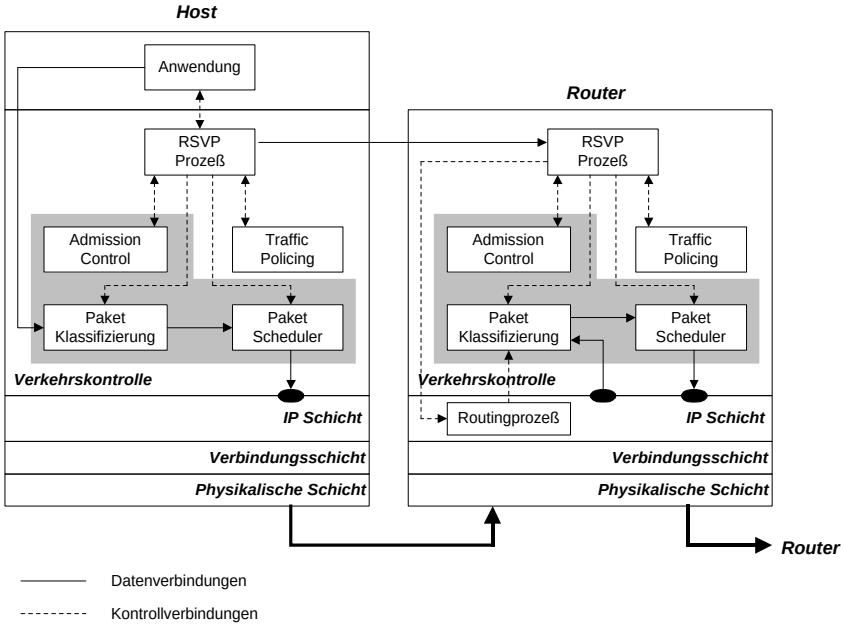

Abbildung 18 : RSVP Einbettung in das TCP/IP Protokoll [Detk98]

Die Hauptmerkmale der Integrated Services Architektur sind somit:

- benötigt Router (Layer 3/ 4 Switching),
- unterscheidet Pakete über die Datenströme (Flows),
- Kennzeichnung der Flows anhand von Adressen und Portnummern,
- Einsatz von Weighted Fair Queuing, Reservierung von Ressourcen,
- benötigt Signalisierungsprotokoll (RSVP),
- verwendet Admission Control,
- Garantien von QoS Parametern möglich.

Der IETF IS Ansatz wird wegen seiner Flexibilität vor allem im Bereich des Enterprise Networking und in strukturierten Router Netzen Verwendung finden.
[Detk98],[Flatt98]

3.3.2 Differentiated Services

Der IETF Differentiated Services - DS - Ansatz basiert nicht auf Priorisierung oder Flows, sondern auf dem möglichen Forwarding Verhalten der Pakete - Per Hop Behaviour - ***PHB***. Das PHB beinhaltet z.B. Drop Threshold, Pufferzuordnung, Service Priorität und Service Rate.
Das ***Differentiated Services Code Point DSCP*** Byte im IP Header kennzeichnet den Service Level. Es ersetzt das ToS Feld im IPv4 und das Class Octet im IPv6 Header. Die ersten 6 bit werden für 64 klassifizierbare Service Level (Definition durch den Netzwerkverantwortlichen) genutzt, wobei 2 bit reserviert bleiben.
Das DSCP mappt Pakete zum PHB und ist abwärtskompatibel zur Precedence des ToS Bytes. Das Packet Marking kann ein DS fähiger NIC, ein Traffic Classifier oder der First Hop Router übernehmen.

Da bislang nicht alle Probleme geklärt sind, wie z.B. die Frage der Managementkontrolle (dynamisch oder statisch) und der Ressourcenzuweisung (Anwender oder Netzwerkmanager), ist die weitere Entwicklung bezüglich Differentiated Services abzuwarten.

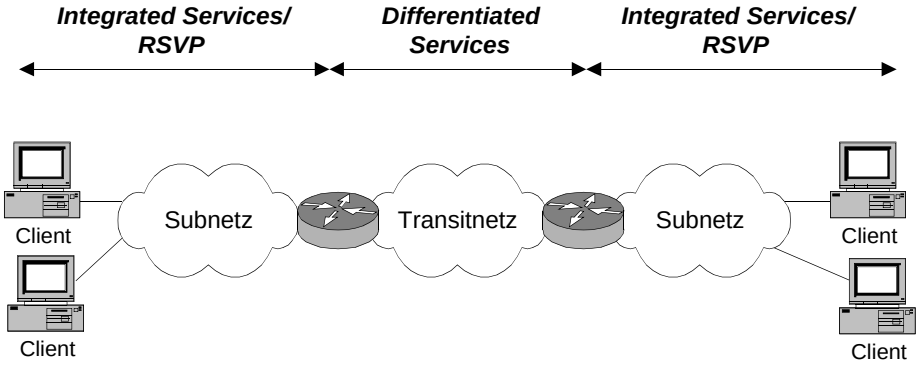

Abbildung 19 : Statische und Dynamische Kombination von CoS Mechanismen [Detk99]

Ein mögliches Zusammenspiel von Integrated Services und Differentiated Services ist in Abbildung 19 dargestellt.
[Intel99], [Detk99]

3.4 Layer 3/ 4 Switching

Switching im Netzwerk ist ein eng gefaßter Begriff. Er bezeichnet prinzipiell eine Multiport-Bridge mit schneller Forwarding-Engine, die mehrere direkte Verbindungen parallel zwischen den angeschlossenen Geräten herstellt. Damit ist ein Switch im OSI-Modell auf Layer 2 angesiedelt, da er mit Adressen aus dieser Schicht arbeiten muß. Ohne die Hardwareadressen der angeschlossenen Geräte kann ein Switch keine Verbindung aufbauen.

3.4.1 Layer 3 Switching

Layer-3-Switching oder IP-Switching, im Gefolge der Diskussion um den Einsatz von TCP/IP über ATM-Netze aufgekommen, kombinieren Technologien (Switching, Routing) der Elemente der OSI-Layer 2 und 3.
Auf Layer 3 arbeitet ein Netz mit logischen Adressen, also beispielsweise IP-Nummern, und nicht mit Hardwareadressen (MAC-Adressen). Es kommen auf Layer 3 also Router und keine Switches zum Einsatz. Ein IP- oder Layer-3-Switch kombiniert Switching- und Routing-Funk-tionen, um nach der Ermittlung eines Pfades zum Zielsystem über Routing-Protokolle eine direkte Verbindung auf Layer 2 zu schalten. Unter Umständen muß dies über mehrere Sta-tionen beziehungsweise Router oder Layer-3-Switches erfolgen.
Layer-3-Switches sind dann sinnvoll, wenn komplizierte Netzstrukturen mit Routern an ihre Grenzen stoßen.
[ctcd98]

3.4.2 Layer 4 Switching

Für die optimale Ausnutzung realer Netze muß der Datenfluß auf Applikationsebene erkannt und gesteuert werden. Applikationen lassen sich erst auf Schicht 4 unterscheiden.
Jedes Schicht 4 Paket enthält Informationen, die sich zur eindeutigen Identifizierung der Applikation verwenden lassen, zu der die Daten im Datenfeld der IP Pakete gehören. Die entsprechenden Felder im Header sind die Portnummern[22].
Die Schicht 4 Information ist allein oder in Verbindung mit Schicht 3 (IP Adresse, DS Byte) nutzbar, um den Durchsatz applikationsabhängig zu steuern.

[22] 1..255 - well known Ports (z.B. 80 http); 256..1023 reserviert für UNIX Dienste; 1024..65535 für Anwender freier Bereich; siehe auch RFC 1062 für Gesamtübersicht vorbelegter Ports

Service Qualität

Die Einteilung der Applikationen erfolgt meist in vier Prioritätsbereiche, die Verkehrsklassen, denen entsprechende ***Classes of Service (CoS)*** der Infrastruktur zur Verfügung stehen. Die Priorität selbst kann an andere Geräte weitergegeben werden.

- Durch das Setzen der 802.1p - Bits (siehe 1.4) kann ein nachfolgenden Layer 2 Switch ebenfalls die Datenpakete nach ihrer Priorität bearbeiten.
- Für die Übertragung über das Internet kann ein Layer 4 Switch nach der Klassifizierung und Priorisierung der Applikation diese Priorität in ***Differentiated Services Information*** (DS Byte) übersetzen. Dadurch kann ein Layer 3 Switch (Hardware Routing) die Datenpakete, Unterstützung von Differentiated Services vorausgesetzt, priorisiert weiterleiten.
- Weiterhin können die Prioritäten auf verschieden SVCs in ATM Netzen gemappt werden.

Die Klassifizierung und Priorisierung, sowie die Weitergabe der Information als 802.1p Tag oder DS Byte sind die Grundlage für Quality/ Class of Service.
Switching System müssen darüber hinaus die Möglichkeit haben, die einzelnen Verkehrsklassen differenziert zu behandeln. Das schließt Techniken mit ein, wie :

- Traffic Shaping und Policing (im LAN ***Committed Flow Rate - CFR*** ; bei ATM ***Usage Parameter Control - UPC***),
- ein intelligentes Congestion Control wie ***Weighted Random Early Detection - WRED*** und
- Queueing Mechanismen wie ***Weighted Fair Queueing - WFQ***.

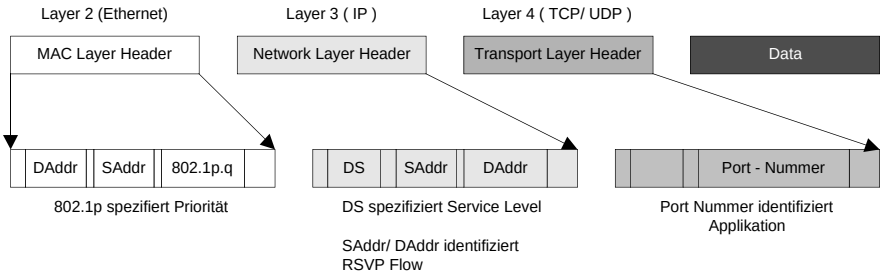

Abbildung 20 : Aufbau der Header der verschiedenen Schichten [Nisp99]

Accounting und Security

Neben der applikationsabhängigen Priorisierung kann ein Layer 4 Switch auch benutzer- bzw. adressabhängige Dienste wie Accounting und Security zur Verfügung stellen.

- Layer 4 Switche unterscheiden die Kommunikationsbeziehungen mittels Quell- und Zieladresse, DS Byte, Protokollfeld sowie Quell- und Zielport. Diese Daten bilden unter

anderem die Grundlage zur Erstellung einer nach Applikationen und Zieladressen aufgeschlüsselten Abrechnung an den Netzbenutzer (Charge Back).

Für Layer 4 Switche steht für Langzeitstatistiken und die Charge Back Funktion das ***Lightweight Flow Accounting Protocols LFAP*** (RFC 2124) zur Verfügung. LFAP dient dazu, regelmäßig Statistikdaten mittels TCP auf einen Externen Datenbank Server (Flow Admission Server - FAS) zu übertragen, wo eine Accounting Software diese Daten weiter verarbeitet.

- Beim Layer 4 Switching erfolgt die Verarbeitung der Pakete in Hardware und da die Quell- und Ziel Port Adresse bekannt sind, können Security Funktionen wie Security Filter und Access Control Listen auf Applikationsebene unter Beibehaltung von Wire Speed implementiert werden. Die Konfiguration kann dynamisch geändert werden, während die Hardware die Security Regeln umsetzt.

Diese Techniken ermöglichen die Kontrolle des Datenverkehrs, sinnvolle Reaktion auf Überlastsituationen und das Bandbreitenmanagement für die einzelnen Verkehrsklassen.

Erst das Zusammenspiel von Layer 4 Klassifizierung mit den entsprechenden Techniken der darunter liegenden Schichten bildet ein intelligentes Multiservice Netz.
Das Potential dieser Technik ermöglicht eine kosteneffiziente Ausnutzung der Netzressourcen und deren laufende Optimierung durch weitreichende Analysemöglichkeiten.
Es ist ebenso möglich, Kosten gerecht auf die Anwender umzulegen. Insbesondere profitiert die Integration der aufkommenden Direktory Services (z.B. LDAP) und der damit verbundenen Möglichkeiten benutzerbezogener Policies.
[Nisp99]

4 Protokolle zur Echtzeit Datenübertragung

4.1 Echtzeitfähigkeit der Netzwerkprotokolle der Schicht 3 - IPv4/ IPv6

Mit einem echtzeitfähigem Netzwerk auf den Schichten 1 und 2 des OSI-Referenzmodells können die Anwendungen diese Dienste noch nicht nutzen. Vielmehr müssen auch die Schichten 3 und 4, die beim Internet mit IP und TCP besetzt sind, Mechanismen zur Bandbreitenreservierung und Echtzeit-Kommunikation besitzen.
In diesem Abschnitt werden die Möglichkeiten der Unterstützung von isochronen Datenübertragungen durch Schicht 3 LAN Protokolle am Beispiel des IP Protokolls untersucht.
IP ist das zur Zeit verbreiteste Protokoll zur Datenkommunikation zwischen Rechnern und ist sowohl im LAN als auch im WAN-Bereich im Einsatz.
Es liegt daher nahe, daß die zur Zeit verfügbaren Produkte im Bereich des Multimedia-Conferencings dieses Protokoll zur Datenübertragung für Video- und Audio-Ströme nutzen. Leider bietet IP keine guten Voraussetzungen für den Transport zeitabhängiger Daten.

IPv4

Das IP Protokoll [23] stellt neben der Datenanpassung an die physikalischen Bedingungen eine Reihe von Diensten zur Verfügung, die in der nachfolgenden Tabelle 8 aufgeführt sind.

Dienst	*Funktion*
Datagrammdienst	Übertragung der Datenblöcke als Datagramme; Prüfung auf Richtigkeit jedoch nicht auf korrekte Reihenfolge
Adreßfunktion	jedes Paket wird mit Sende- und Empfangsadresse versehen
Festlegung der Protokolle höherer Schichten	Def. Protokolle höherer Schichten zum Datentransport durch Protokollkennungen
Netzwerkrouting	Umsetzung von Datagrammen auf andere Netzwerke und Wegewahl durch Router
Fragmentierung und Reassembling von Paketen	Unterstützung von Datagrammen unterschiedlicher Länge im Netzwerk, erfordert Fragmentierung in Teildatagramme und Reassembling beim Empfänger
Übertragungszuverlässigkeit	Def. der Zuverlässigkeit der Wegewahl (siehe Type of Service)
Prioritätsübertragung	(siehe Type of Service)
Wahl der Übertragungsparameter	(siehe Type of Service)

Tabelle 8 : IP Dienste [Detk98]

[23] IPv4 - RFC 791

Die Datagrammübertragung erfolgt ungesichert und verbindungslos, wobei jedes Paket unabhängig von anderen übertragen wird.
Funktionen wie Fehlererkennung, Überwachung der Reihefolge, Flußkontrolle (z.B. in TCP Empfangsbestätigung) und Sicherung der Übertragung sind durch Protokolle höherer Schichten zu implementieren.

In Abbildung 21 ist eine IPv4 PDU dargestellt. Interessant für den betrachteten Zusammenhang - Echtzeitfähigkeit - ist das ***Type of Service*** Feld.

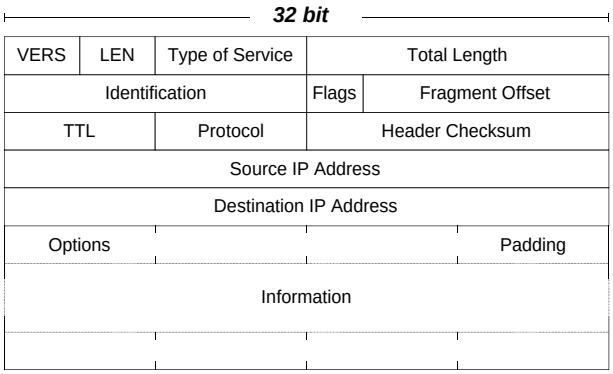

Abbildung 21 : IPv4 PDU [Mino98]

Das ***Type of Service*** Feld verteilt Prioritäten, welche Vorrangsteuerung [24], Wartezeit, Durchsatz und Zuverlässigkeit beinhalten. Diese Parameter erlauben höheren Protokollen das Anhängen von Verarbeitungsfunktionen an zu übertragende Datagramme, die ausschließlich von Netzwerkhardware der Schicht 3 und höher (z.B. Router, Layer 3/ 4 Switche etc.) ausgewertet werden. Es können somit vorrangige Datagrammbehandlung, die Durchsatzart und die Routerressource festgelegt werden - siehe Queueing Mechanismen in Kapitel 6.1.4.

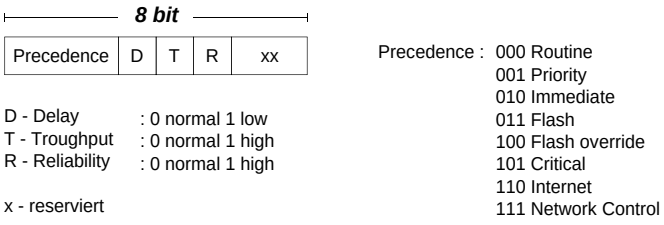

Abbildung 22 : Type of Service Feld IPv4 [Mino98]

Ein Problem besteht jedoch darin, daß Produkte das ***Type of Service*** Feld nicht unterstützen bzw. nicht vollständig implementieren.

[24] Precedence Feld entspricht der Priorität

IP-Datagramme werden nach dem Prinzip des ***Best-Effort*** (die Übertragung der IP-Pakete erfolgt sobald Kapazität vorhanden ist) übertragen. Dabei existieren weder Prioritäten der ***einzelnen*** Datagramme, noch wird die benötigte Bandbreite reserviert und überwacht.

IPv6

Aufgrund von Adressenknappheit und zur Einführung von Sicherheitsmechanismen wird die IPv4 zukünftig von der IPv6 (RFC 2460) abgelöst werden . Die wichtigsten Änderungen bzw. Erweiterungen sind in Tabelle 9 zusammengefaßt.

Erweiterung	***Funktion***
Erhöhte Adressierungskapazität	Erweiterung von 32 bit auf 128bit, Verbesserung der Skalierbarkeit des Multicast Routing durch Multicast Adressfeld; neuer Adresstyp - Anycast Adresse
Header Formatvereinfachung	Weglassen bzw. optionale Funktion von Felder der IPv4, dadurch Verringerung der Prozeß- und Bandbreitenkosten
verbesserte Erweiterungs- und Optionsunterstützung	Optionsänderungen ermöglichen effizienteren Datentransport, variablere Optionslänge und größerer Flexibilität für neue Optionen
Flußadressenleistungsspektrum	Paketkennzeichnung als Datenfluß mit speziellem Handling, wie non default QoS oder „real time“ Service (siehe Flow Labelling)
Identifikationsüberprüfung/Einhaltung der Privatsphäre	Erweiterung der Identifikationsüberprüfung und Vertraulichkeit der Information
automat. IP Adressierung	Automatisches Einstellen der Netzwerkadessen am Router

Tabelle 9: Erweiterungen /Änderungen in IPv6 [Detk98]

In Abbildung 23 ist eine IPv6 PDU dargestellt. Es ist zu erkennen, daß der Header deutlich weniger obligatorische Felder enthält als der einer IPv4 PDU. Von besonderem Interesse für die Übertragung von Echtzeitdaten sind Felder zur Datenpriorisierung, zum einen das ***Prioritätsfeld PRI*** und das ***Flow Label*** Feld.

Das ***Prioritätsfeld*** besteht aus 4 bit und ermöglicht dem Sender, Wertigkeiten für Pakete festzulegen und zu erkennen. Die Werte werden in zwei Bereiche aufgeteilt.

- Der erste Bereich von 0-7 legt die Datenpriorität fest, bei der eine Überlastkontrolle durch den Sender für rückgekoppelte Lastreaktion erfolgt (z.B. TCP Übertragung).

- Der zweite Bereich von 8-15 ist für Reaktionen spezifiziert, bei denen keine Rückkopplung auftritt (z.B. Echtzeitübertragung mit konstanter Bitrate).[25]

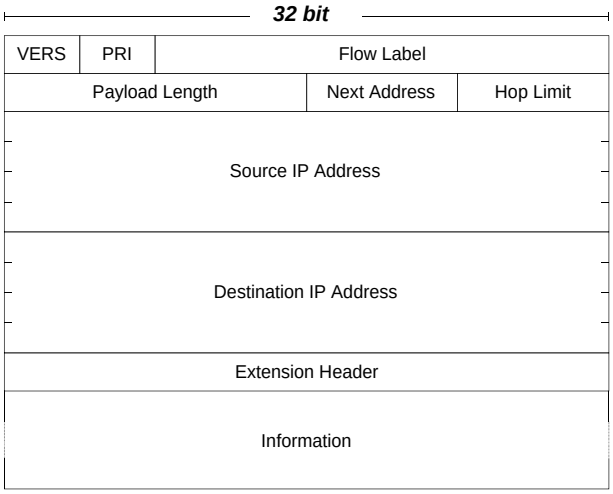

Abbildung 23: IPv6 PDU [Detk98]

Im IP Standard werden keine Richtlinien für die Zuweisung dieser Prioritäten festgelegt. Die Datenquelle kennzeichnet jedes Datagramm entsprechend der Bedeutung seines möglichen Verlustes. Eine kleinere Priorität zeigt an, daß eine spezielle Applikation tolerant auf das Verwerfen dieses Datagramms reagiert.
Das Prioritätsfeld verfolgt damit einen ähnlichen Ansatz wie das ***Type of Service*** Feld von IPv4.

Das ***Flow Label*** Feld besteht aus 24 bit und wird vom Sender genutzt um eine Paketsequenz zu kennzeichnen. Dies kann verzögerungsfreien Quality of Service oder Echtzeitdienste betreffen. Es soll damit eine einfachere Unterstützung des Datenflusses ermöglicht werden, als dies bisher der Fall war.

Das Hauptargument für die Einführung von IPv6, die Adressknappheit, hat seit der Ausbreitung geschützter Computernetze und Verfahren wie Network Address Translation - NAT- an Überzeugungskraft verloren. Es wird jedoch zur Zeit versucht, durch Initiativen zur Erschließung neuer Märkte für mögliche Geräte mit IP Adresse die Einführung von IPv6 zu forcieren.

[25] Zu beachten ist, daß keine relative Ordnung zwischen den beiden Bereichen besteht (z.B. ist Priorität 8 nicht höher oder niedriger als Priorität 7)

In der Übergangsphase wird es einen gemischten Betrieb der beiden IP Versionen geben. So werden z.B. IPv6 Datagramme über IPv4 Infrastrukturen getunnelt und IPv4 Adressen in IPv6 Adressen gekapselt.
[Detk98],[From95],[Mino 98],[[RFC 2460],[iX1/00]

4.2 Echtzeitfähigkeit der Schicht 4 Transportprotokolle - TCP/ UDP

TCP

Von den beiden bei TCP/IP vorhandenen Transportprotokollen, UDP und TCP, kann TCP für Echtzeit-Datenverkehr ***nicht*** eingesetzt werden.
TCP (RFC 793) verwendet zur Sicherung des Datenstroms ein sogenanntes PAR-Verfahren, das einen Paketverlust bemerkt und durch wiederholtes Aussenden des verlorenen Datagramms diesen Verlust kompensiert. Dadurch stellt TCP eine gesicherte Ende-zu-Ende-Verbindung her, bei der Fehler nur durch Totalverlust der Verbindung entstehen können. TCP ist zur Übertragung von Datenströmen gut geeignet und effizient, solange die Daten nicht an Zeitgrenzen gekoppelt sind.
Bei der Übertragung von Audio- und Videosignalströmen muß die kontinuierliche, isochrone Versorgung des Empfängers sichergestellt sein. Ein wiederholt ausgesandtes Paket kommt zu einer Zeit beim Empfänger an, zu der es nicht mehr aktuell ist. Da TCP die PAR-Technik für den gesamten Datenstrom verwendet, führt bereits der Verlust und das wiederholte Senden eines Datagramms zu einer andauernden Verzögerung.

UDP

Somit bleibt für das Versenden von Audio- und Videodaten nur UDP (RFC 768), das verbindungslos arbeitet.
UDP bietet zudem durch den kurzen Paket-Kopf ein gutes Nutzdaten/ Paketlängenverhältnis. Dennoch bildet auch UDP keine gute Grundlage zur Übermittlung von Echtzeitdaten. UDP verwendet keine weiteren Sicherungsmechanismen, sondern lediglich einen einfachen Mechanismus zum Multiplexen mehrerer UDP-Datenströme an einen Rechner.

Für die Übertragung von Echtzeitdaten wurden daher spezielle Protokolle entwickelt. Einen Überblick über diese gibt das folgende Kapitel.
[Detk98],[From95],[Mino98],[[RFC 2460]

4.3 LAN Echtzeitprokolle

In diesem Abschnitt werden das Protokoll ST2 (RFC 1190), das neben IP existiert und synchrone Datenübertragung übernimmt, echtzeitfähige Transportprotokolle der Schicht 4 - XTP und das von der ITU Empfehlung H.323 genutzte RTP/RTCP vorgestellt.
Abbildung 24 ordnet die Echtzeitprotokolle in die Struktur der IP Protokoll Familie ein.

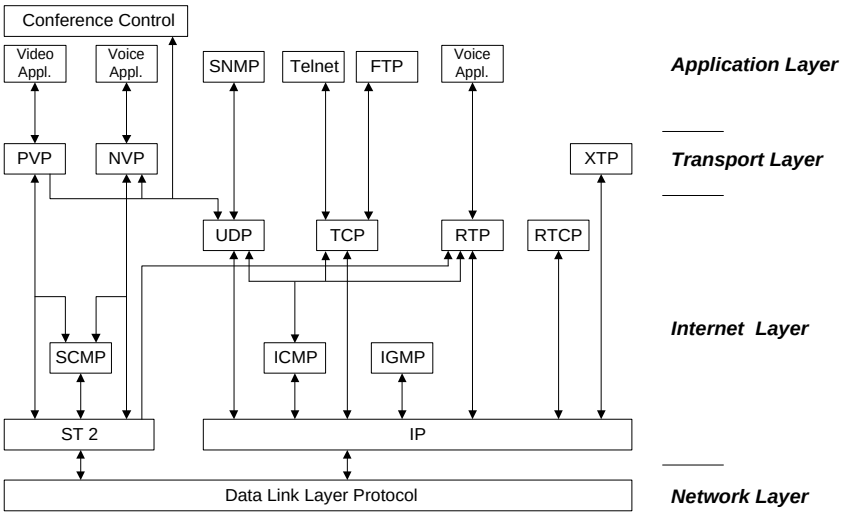

Abbildung 24 : Hierarchie der IP Protokoll-Familie [Mino98]

4.3.1 Echtzeitprotokolle der Schicht 3

ST2

Motivation zur Entwicklung von ST2 (RFC 1819) war ein Protokoll zur effizienten Übertragung von Paketströmen zu entwerfen, das die Unzulänglichkeiten von IP bezüglich garantierter Übertragungsverzögerung und garantierter Bandbreite beseitigt.
ST2 existiert neben IP auf der Schicht 3 des ISO/OSI Referenzmodells. Es ist keinesfalls ein Ersatz für IP, da es sich nur für die Übertragung von Echtzeitdaten eignet und daneben von einem verfügbaren Protokoll (z.B. IP) zur asynchronen Datenübertragung ausgeht.
ST2 arbeitet im Gegensatz zu IP ***verbindungsorientiert***. Dabei speichern ST2 Router Verbindungsinformationen, wie Transportinformationen, Multicast Unterstützung und Ressourceninformationen (Warteschlangen, Ausgangsports etc.).
Diese bereitgestellten Verbindungsinformationen erlauben die Übertragung von ST2 Datagrammen mit geringer Verzögerung, geringem Overhead und geringer Verlustwahrscheinlichkeit bei Überlastung. Rechner bzw. Router die ST2 implementieren, werden als ***ST2 Agenten*** bezeichnet.

ST2 Verbindungen[26] verfügen über eine Ende zu Ende Flußkontrolle.
Die Routenwahl und Ressourcenzuteilung erfolgt während des Verbindungsaufbaus und wird nur im Fehlerfall verändert. Es können zur Steuerung für einzelne oder Gruppen von Verbindungen globale Name vergeben werden.
Die Verbindungssteuerung übernimmt das ***SCMP - ST Control Message Protokoll*** . Es ist äquivalent dem ICMP von IP.
Das SCMP stellt Datagramme für den Verbindungsauf- /-abbau, die Zustandsabfrage, die Netzüberwachung, sowie die Änderung der Verkehrsparameter[27] zur Verfügung.

ST2 Pakete können in einer Übergangsphase über IP getunnelt werden, Garantien für Verzögerungszeiten bzw. Bandbreite gehen dabei jedoch verloren. Um ST2 ins Netz zu integrieren müssen Router ST2 Agenten werden.
ST2 wird sich nicht durchsetzen, aufgrund der aufwendigen Implementierung (IP + ST2 Agent) und da z.Z. RTP/ RTCP (baut auf vorhandenen Protokollstrukturen - IP+UDP/ TCP) mit ähnlichen Ziel-stellungen wie ST2 große Popularität erlangt hat..
[From95]

4.3.2 Echtzeitprotokolle der Schicht 4

Um den Multimedia - Anwendungen die Kommunikation zu ermöglichen, bedarf es neben einem Netzwerk-Protokoll wie IP oder ST2 einem Transportprotokoll, das die Verbindungen der verschiedenen Anwendungsprogramme auf dem Endsystem multiplext und definierte Schnittstellen zur Übertragung von Datenströmen zur Verfügung stellt.
Bei asynchroner Kommunikation wird als Transportprotokoll im allgemeinen TCP eingesetzt, das für Echtzeit-Daten aber bereits als ungeeignet eingestuft wurde.
Zudem besteht eine TCP-Verbindung immer zwischen genau zwei Endsystemen, die Übertragung eines Datenstroms an eine Gruppe von Rechnern ist mit TCP nicht möglich.
In diesem Abschnitt werden verschiedene Transportprotokolle vorgestellt, die sich dieser Problematik annehmen.
Behandelt werden das ***Xpress Transport Protocol (XTP)*** als Beispiel für eine Gruppe von Echtzeitprotokolle[28] und das ***Real-Time Transport Protocol (RTP)***.
XTP

[26] auch als ***Streams*** bezeichnet
[27] definieren Ende zu Ende Verzögerung, Datagramm Rate und Größe

Das ***XTP - Xpress Transfer Protocol*** (RFC 1453) - wurde als Transportprotokoll für Hochgeschwindigkeitsnetze entwickelt und ist auf den Schichten 3 und 4 [29] des ISO /OSI Modells positioniert. XTP wird aufgrund seiner hohen Konfigurierbarkeit vielfältigen Übertragungsansprüchen gerecht und ist sowohl für asynchrone Datanübertragung wie auch für die Übertragung von Multimediadaten geeignet.

Im XTP wurden vor allem die Datagramm-Struktur und Verarbeitungsabläufe optimiert. So besteht der XTP Rahmen aus einem Kopf und einem Trailer, der die Prüfsumme enthält. Die Prüfsumme kann dadurch während des Sendens gebildet werden, zusätzlich befindet sich die Information eines XTP Datagramms an einer festen byte Position. Beides verkürzt die Bearbeitungszeit.
Die Adressierung erfolgt ähnlich dem virtual path im ATM, die Adresse wird bei Verbindungsaufbau übertragen, danach lediglich eine Verbindungskennung. Bereits in den Kontroll Datagrammen ist Informationsübertragung erlaubt.
Da die Wahrscheinlichkeit des Verlustes eines Datagramms durch Überlastung von Netzwerkkomponenten höher ist als die durch Bitfehler, werden zur Vermeidung von Überlast jeder Verbindung eine max. mittlere Übertragungsrate und eine max. Burstrate zugeordnet.
XTP bietet außerdem :

- eine bis zu 4Gbyte[30] große Fensterweite beim ***sliding window*** Verfahren,
- die Vergaben von Prioritäten anhand einer 32 bit Zahl;
- die Übertragung von out of band Daten durch 8 byte ***tagged data*** (evtl. Nutzung als Timestamp),
- Mechanismen zur Flußkontrolle und
- die Fähigkeit zur Gruppenkommunikation durch Multicast Verbindungen.

Wie schon in der Einschätzung von ST2 aufgeführt, konnte sich XTP auf der Schicht 4 nicht gegen das populäre RTP/ RTCP behaupten und soll an dieser Stelle nur als Beispiel für die Gruppe neben RTP/ RTCP existierender Echtzeitprotokolle dienen.
[From95]

[28] MTP Multicast Transport Protocol; NVP Network Voice Protocol; VMTP Versatile Message Transaction Protocol
[29] Die Zusammenfassung von Schicht 3 und 4 wird auch als ***transfer layer*** bezeichnet.
[30] wird durch zunehmende Datenraten erforderlich; max. 64 kbyte bei TCP

RTP/RTCP

RTP - Real Time Transfer Protocol - (RFC 1889) wurde von der IETF als Echtzeit Transportprotokoll vorrangig für die Bedürfnisse von ***Multi Participant Multimedia*** Konferenzen entwickelt, ist aber nicht darauf begrenzt[31].
Das RTP liefert Ende zu Ende Verbindungsdienste für Echtzeitdaten, wie ***Payload Type Identification***, ***Sequence Numbering***, ***Time Stamping*** und ***Delivery Monitoring***.

RTP selbst beinhaltet ***keine*** Mechanismen zur Sicherung des zeitlichen Empfangs noch andere Quality of Service Garantien, sondern setzt dies von untere Schichten voraus. Es garantiert weder den Empfang noch die richtige Empfangsreihenfolge und geht nicht davon aus, daß dies untere Schichten übernehmen.
Die Sequenznummer in RTP erlaubt dem Empfänger eine Rekonstruktion der Sender Sequenz. Sie wird auch genutzt, um die Lage eines speziellen Paketes zu bestimmen, ohne daß eine Decodierung der gesamten Sequenz notwendig wird.
RTP setzt in IP Netzen auf UDP auf, kann aber auch andere Netzwerk- und Transportprotokolle wie IPX oder ATM (siehe auch 2.5 H.323 über QoS basierte Netzwerke) nutzen.

RTP ist ein Protokollrahmenwerk. Die Anpassung an die Applikationen wird durch die Definition ***spezieller Profile*** (RFC 1890 - RTP Profile for Audio and Video Conference with minimal control) und der Spezifikation eines ***Payload Formats*** erreicht. Das Payload Format legt die Übertragungsweise (z.B. Decoding) fest. Über die Profile werden einer Gruppe von Payload Formaten eine Payload Type Number zugeordnet, die von der jeweiligen Applikation genutzt werden kann.
Im Anhang A.2 sind RTP Begriffe und deren Definition aufgeführt.

In Abbildung 25 ist der ***Header*** eines RTP Paketes dargestellt. Die ersten 12 Oktets sind in jedem Header vorhanden, wohingegen die Liste von CSRC Identifiern nur nach einer Bearbeitung durch einen Mixer vorkommt.

[31] weitere Einsatzgebiete: Speicherung von kontinuierl. Datenströmen; interaktiver verteilte Simulationen; active Badge; Kontroll- und Meßapplikationen

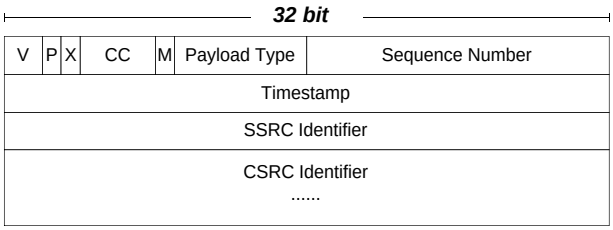

Abbildung 25 : fixer Header eines RTP Datagramms [RFC 1889]

In Verbindung mit dem RTP wird das ***RTCP - RTP Control Protocol*** - (RFC 1889) zum Monitoring der Übertragungsqualität eingesetzt.
RTCP basiert auf der periodischen Übertragung von Kontrollpaketen zu allen Session Teilnehmern. Dabei nutzt das Kontrollpaket den selben Übertragungsmechanismus wie die Daten.
Das unter RTP/RTCP liegende Protokoll muß zum Multiplexen von Daten und Kontrollpaketen fähig sein (z.B. Nutzung verschiedene Ports bei UDP).
RTCP dient vier Funktionen :

1. Die primäre Funktion ist das Liefern von ***Feedback Informationen*** über die Qualität der Datenübertragung. Die Sendung von ***Reception Feedback Reports*** an alle Teilnehmer erlaubt einem Außenstehenden die globale bzw. lokale Diagnose von Übertragungsfehlern. Mit Übertragungsmechanismen wie IP Multicast ist es möglich, als ein ***Third Party Monitor*** (z.B. als Network Service Provider) Feedback Informationen zur Netzwerkdiagnose zu erhalten.
2. RTCP überträgt einen ***canonical name*** oder ***CNAME*** genannten Transport Level Identifier für eine RTP Quelle. Da die ***SSRC Identifier*** im Fehlerfall wechseln kann, benötigt der Empfänger den ***CNAME***, um die Verbindung aufrecht zu erhalten. Der ***CNAME*** wird vom Empfänger außerdem benötigt, um Datenströme eines bestimmten Teilnehmers in einer Gruppe von RTP Sessions zuerkennen (z.B. Synchronisation von Audio und Video).
3. Für die ersten beiden Funktionen müssen alle Teilnehmer RTCP Pakete senden. Daher ist es erforderlich, die RTCP Senderate zu überwachen um RTP für eine hohe Teilnehmerzahl skalierbar zu machen. Da jeder Teilnehmer an alle anderen RTC Pakete sendet, kann die Anzahl der Teilnehmer unabhängig von jedem überprüft werden. Die Anzahl wird zur Bestimmung der RTCP Senderate bestimmt (Emp-fehlung 5% der Sendebandbreite).

4. Diese optionale Funktion überträgt minimale Session Control Informationen (z.B. die angezeigte Teilnehmeridentifikation). Die Anwendung erfolgt in Sessions, in denen Teilnehmer ohne Teilnehmerkontrolle und Verhandlung von Parametern die Session verlassen bzw. neu hinzukommen können.

Das RTCP dient als praktischer Kanal, um alle Teilnehmer zu erreichen, jedoch wird nicht angenommen, daß RTCP alle erforderlichen Kontrollfunktionen implementiert. Dies muß dann ein Session Kontroll Protokoll auf höherer Ebene übernehmen.
Weiter Informationen zu RTCP Paketformaten, Receiver und Sender Reports befinden sich in der RFC 1889 ab Seite 14.

RTP/ RTCP hat sich als Standardprotokoll zur Sprachübertragungn über Datennetze aufgrund seiner Eignung zur Gruppenkommunikation durchgesetzt und da es auf vorhanden Protkolle aufbaut (IP+UDP/ TCP).
[From95], [Indu96], [Mino98], [RFC 1889]

5 VoIP Lösungen/ Konzepte von Herstellern

Nachstehend sind noch einmal die häufigsten Einsatzszenarien von VoIP aufgelistet:

- ***PSTN Phone to PSTN Phone*** - Telefonie vom PSTN mittels Gateways über Intranet/ Internet zum PSTN
- ***PC to PSTN Phone*** - Telefonie vom PC im Intranet/ Internet zum PSTN
- ***Videokommunikation*** - in mögl. Varianten: LAN to LAN, LAN to H.320, H.320 to LAN
- ***Voice Integration am PC Arbeitsplatz*** - geforderte Leistungsmerkmale wie CT, Call Center, Workflow Integration
- ***Call Me Buttons im HTML Anwendungen*** - Verbindungsaufbau über vom User betrachtete Web Seite zum Call Center
- ***PBX Anlagenvernetzung***

Die Hersteller verfolgen mit ihren VoIP Produkten unterschiedliche Philosophien. Zum einen werden Router bzw. Access Geräte um VoIP Funktionalitäten erweitert, zum anderen werden diese Funktionalitäten in dedizierte VoIP Geräte eingebettet.

Eine Aufstellung der verschiedenen Hersteller und ihrer Produkte befindet sich im Anhang. Auf einige Produkte der Siemens AG und Cisco Systems wird exemplarisch näher eingegangen.

5.1 Siemens AG

Die Siemens AG bietet folgende Lösungen und Produkte an:

- ***Hicom Xpress C65*** - Intranet und LAN
- ***HiNET RC 3000*** - Intranet und LAN
- ***InterXpress*** - Lsg. für Carrier und ISP

Die in den folgenden Abschnitten beschriebenen Ansätze vom RC 3000 und Hicom Xpress unterschieden sich dahingehend, daß zum einen Hicom Xpress ***Client-basiert*** und RC 3000 ***Server-basiert*** sind und die Integration von Daten-, Sprach- und Videoübertragung vorsehen. Zum anderen geht der Ansatz von Hicom Xpress C65 Workflow weiter, indem versucht wird unterschiedliche Arbeitsabläufe - ***Workflows*** - so darzustellen, wie sie im täglichen Arbeits-

ablauf des Benutzers tatsächlich existieren [32]. Um die dafür geforderte Flexibilität zu bieten müssen Applikationen jeweils kundenspezifisch programmiert und konfiguriert werden

Gateway : ***Gateway L2W-323***

Als gemeinsame Basiskomponente für RC 3000 und Hicom Xpress/ Workflow Lösungen dient jeweils das ***Gateway L2W-323*** von Radvision.

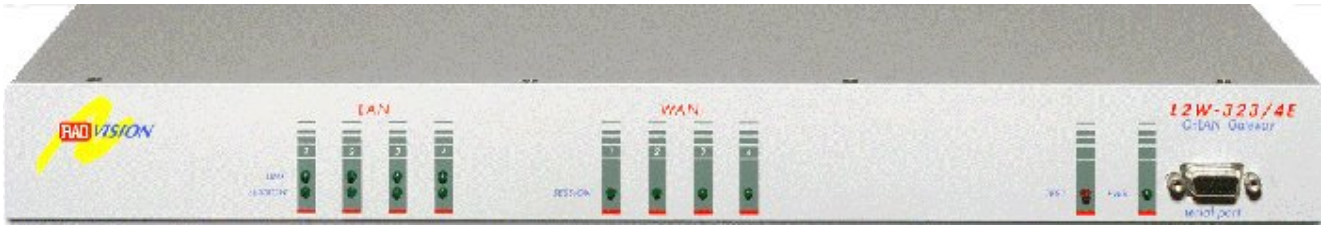

Abbildung 26 : Gateway L2W-323 [HiNet 1]

Leistungsmerkmale :

- WAN Verbindung über max. 4 BRI ISDN S_0 Schnittstellen - skalierbar in 2er Schritten; Protokoll: DSS1; PRI S_{2M} Schnittstelle - geplant; gleichzeit 16 Kanäle nutzbar
- LAN Verbindung über max. 10BaseT IEEE 802.3 (Ethernet) Schnittstellen; Protokoll: TCP/ IP
- Gatekeeper im Gateway integriert: Adresskonvertierung ISDN/ IP, Zugangskontrolle, Bandbreitenkontrolle
- unterstützte Protokolle: H.323; H.320, H.261 (Video); G.711, G.723.1, G.728 (Voice); Transcoding G.711/ G.723.1 und G.711/ G.728
- bis zu 48 gleichzeitige Verbindungen
- Silence Supression und Echo Cancellation
- Real Time Fax
- Administrierung: SNMP über V.24 oder LAN
- Anschaltmöglichkeit an Hicom 100E, 150E und 300E

[HiNet 1]

5.1.1 Hicom Xpress : Client - basiert

Clients : ***Client Escort 25 pro***

Der Escort 25 Pro Client für Hicom Xpress ist eine H.323 kompatible Desktop Lösung für Sprach- und Videokonferenzfunktionen und T.120 Unterstützung für den Datenaustausch.

Leistungsmerkmale :

- PCI Karte, halbe Baulänge „Plug and Play“-fähig, Ein-/ Ausgänge für Kamera und Handapparat,

[32] kundespezifische Integration aller Kommunikationsmedien

zweite Audio Einrichtung (Mikrofon, Lautsprecher), zweite Kamera (Dokumentenkamera)

- Handapparat, Videokamera, Software unter Windows 95 (A,B)
- unterstützte Protokolle: H.261, H.263 (Video); G.711, G.723.1, G.728
- hardwarebasiertes Echo Cancellation

Gatekeeper : ***externer Gatekeeper unter Windows NT***

Alternativ zum im Gateway integrierten Gatekeeper kann ein externer Gatekeeper unter Windows NT eingesetzt werden, der die Nutzung von 100/ 300 aktiven Verbindungen ermöglicht.

5.1.2 Hicom Xpress C 65 Workflow

Hicom Xpress C 65 Workflow stellt eine diensteintegrierende S***oftwarelösung*** auf Basis des Gateways L2W-323 dar und ermöglicht Workflow Integrationslösungen und die Realisierung IP basierter Call Center.

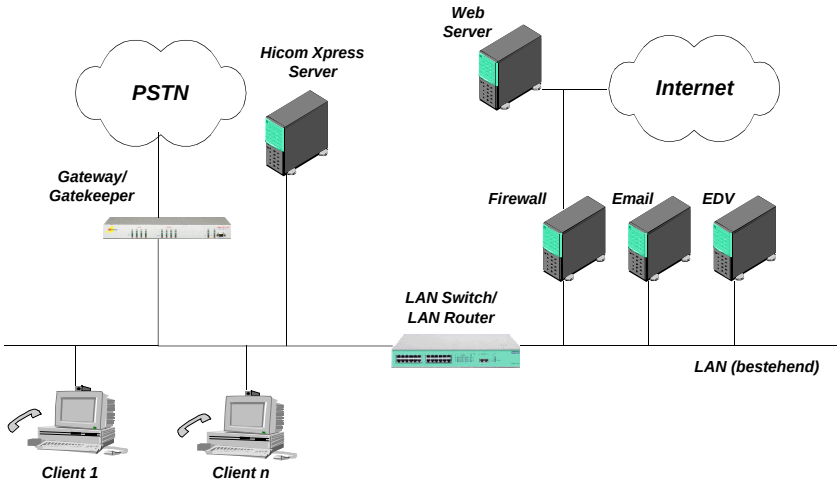

Abbildung 27 : Systemüberblick Hicom Xpress Workflow [Xpress]

Die Module des Hicom Xpress Workflow Servers bestehen in:

Multimedia Call Processing

Regelt als Hauptmodul die multimediale Verteilung aller eingehenden Verbindungen (Telefon, Email, Fax, Video). Die Verteilung erfolgt aufgrund in einer offenen für alle Einsatzzwecke frei programmierbaren relationalen Datenbank hinterlegten Einstellungen.
Das Modul ist als Expert System für ACD geeignet mit Unterstützung verschiedener Routing Möglichkeiten[33].

Telephony

Dient der Bedienung von Telefonverbindungen. Bei mehreren gleichzeitigen Anrufen können diese an andere Teilnehmer weitergeleitet oder inder Incoming Box zur Bearbeitung aufgelistet werden.

[33] z.B. skill-based oder history-based Routing

Eine integrierte ***Voice Mail Applikation*** ermöglicht das dynamische Umschalten zu einem Sprachspeicher.
Folgende Funktionen sind integraler Bestandteil des Telephony Moduls: Makeln zwischen beliebig vielen Gesprächen; Rückfrage, Direktvermitteln, Übergabe, Stummschaltung eines Teilnehmers, Anrufjournal (z.B. für entgangene Anrufe) und Voice-Mail

CorNet NQ Interworking

Ein CorNet NQ - fähiges Gateway (Unterstützung von QSIG und proprietärem CoNet-N) ermöglicht eine intelligente Verbindungen zum firmeninternen Telefonnetz[34].

Directory Service

Online Integration der Personendaten von Kunden oder internen Teilnehmern über X.500 Zugang in Hicom Xpress. Dadurch wird der Wählvorgang vereinfacht und zusätzliche Informationen können bei eingehenden Rufen aus dem vorhandenen EDV Netz bereitgestellt werden[35].

Messaging

Die Speicherung sämtlicher Voice-, Fax- und Email- Nachrichten erfolgt in einer einheitlichen Messaging Box und werden als Email weiterverarbeitet.

Voice Recording

Die Aufzeichnung von Gesprächen ist direkt auf dem Hicom Xpress Server möglich, wird aus Sicherheitsgründen aber oft auf einen eigenständigen Server in einem gesichertem Raum durch-geführt.

Automatic Dialing

Aufgrund von aus Datenbanken zusammengestellten Anruflisten erfolgt der automatische Anruf beim Kunden und dessen Verbindung mit dem entsprechend des Workflows geeignetem Hicom Xpress Mitarbeiter
Nicht erreichte Kunden werden über alternative Medien wie Fax und Email benachrichtigt.

CTI

Alle verfügbaren Informationen können automatisch auf JTAPI basierenden anderen Applikationen zur Verfügung gestellt werden.

Supervisor

Alle Hicom Xpress Aktivitäten werden in der Plattform Datenbank gespeichert und stehen zur Erstellung beliebiger über Standardschnittstellen exportierbarer Statistiken bereit.
Bei Einsatz als Customer Contact Center ermöglicht das Modul Online Eingriffe in die Administration von Agenten und Call Center Gruppen, sowie Silent Monitoring für Test und Schulungszwecke.

Technische Anforderungen

	Server	***Fax Server***	***Client***
Prozessor	Pentium 266 MHz	Pentium 200 MHz	Pentium 200 MHz
RAM	128MB	64MB	64MB
HDD	4GB	2GB	1,5GB
Netzwerk	Ethernet PCI Combo Karte	Ethernet PCI Combo Karte	Ethernet PCI Combo Karte
zusätzlich	Controller: RAID	ISDN Karte: DIVA Pro2.0	Full Duplex Soundkarte für

[34] z.B. mittels ***path replacement*** die Rückgabe von Telefongesprächen die von Hicom Xpress Arbeitsplätzen (weiter)vermittelt wurden ins firmeninterne Telefonnetz
[35] Informationen können dank LDAP aus weltweit verteilten Quellen stammen

	Backup: 4 GB DAT		Windows NT
Software	Windows NT 4.0	Windows NT 4.0	Windows NT 4.0

Tabelle 10 : Technische Anforderungen Hicom Xpress Workflow [Xpress]

5.1.3 HiNet RC 3000 : Server - basiert

HiNet RC 3000 bezeichnet eine komplette Produktlinie (HiNet) auf der Basis eines NT Servers in welchem der Gatekeeper integriert ist und des Gateways L2W - 323.
Zielsetzung ist die Ersetzung der PBX. Altendgeräte (z.B. Analoge, G3 Faxgeräte) können mittels Adapter (z.B. TA 1100) angeschlossen werden, bzw. werden durch IP Telefone ersetzt.
Geeignet ist RC 3000 für eine Teilnehmergruppe bis 50 Teilnehmern.
Im späteren Releasen soll RC 3000 auch Video unterstützen. Die geplante Weiterentwicklung ist in der Tabelle 19 im Anhang B.1 zusammengefaßt.
[HiNet 2]

5.1.4 IP Telefon LP 5100

Das LP 5100 unterstützt die Standards H.323, inclusive H.450. Als Sprachcodecs kommen G.711 und G.723 zum Einsatz.
Das IP Telefon wird über DHCP in ein bestehendes Netz eingebunden und ist über HTTP und SNMP administrierbar.

Es unterstützt unter anderem die Funktionen: Freisprechen, Direktwahltasten, Speicherung der letzen 20 eingehenden Telefonate.
Ein Upgrade ist durch den Download aktualisierter Software möglich.
[LP]

5.2 Cisco Systems

Cisco verfolgt den Ansatz, VoIP Funktionalitäten in die Geräte der bestehenden Router Produktlinie zu integrieren.
In den folgenden Kapiteln werden beispielhaft einige Cisco Produkte vorgestellt.

5.2.1 VoIP Funktionalität in Routern

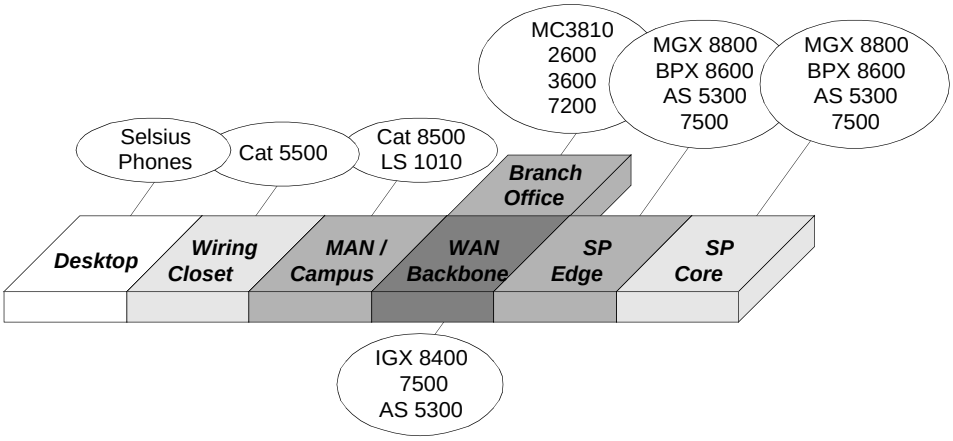

Abbildung 28 : Telefonie vom Desktop bis zum Service Provider [Cisco99]

Cisco MC 3810 Multiservice Access Concentrator

Der MC 3810 ist ein kompakter, low-cost Multiservice Access Concentrator zur Integration von Daten, Sprache und Video über Public oder Private Frame Relay, ATM oder Leased Line Netzwerke.
Der Access Concentrator ist vor allem zur Kopplung von PBXen über die jeweiligen WAN Interface geeignet und kann in kleinen TK - Losen Umgebungen als Voice Switch dienen. Weiterhin sind ein H.323 Gatekeeper, ein Multimedia Conference Manager und Proxy Funktionen für Videokonferenzen enthalten.

Ein Gateway zum Übergang ins PSTN ist nicht implementiert und muß durch andere Geräte (z.B. Cisco 2600/ 3600 Serie) bereitgestellt werden.
Einen Überblick über weitere Leistungsmerkmale des MC 3810 gibt die folgende Tabelle 11.

	Beschreibung
Interface	
T1	ANSI T1.403(1989), Bellcore TR-54016
E1	ITU G.703
Analog Voice	up to 6 Ports - FXS, FXO, E&M
Digital Voice	single T1/ E1 with cross-connect drop and insert, CAS and CCS signalling, PRI QSIG
Ethernet	Single 10baseT
Serial	2 five-in-one synchronous serial - ANSI EIA/ TA - 530, EIA/ TA - 449; ITU V.35, X.21, Bisync, Polled Async
Protocols and Services	
LAN Support	IP, transparent bridging, concurrent routing and bridging, Novell IPX, and Apple Talk, Banyan Vines, DECnet
WAN Services	T1/E1 ATM, Frame Relay, HDLC, PPP, Integrated ISDN BRI Back-up
WAN Optimization	Header, link and payload compression, custom and priority queuing, IPXWAN 2.0
IBM Support	RSRB, DLSw+, SDLC-to-LAN conversion (SDLC Logical Link Control [SDLLC]), SDLC transport (serial tunnel [STUN]), Frame Relay, SNA support (RFC 1490)
VoIP / VoFR	G.711, G.729, G.729a, ADPCM (32 kbit/s) - bis 24 Kanäle komprimierte Sprache über bis zu 6 Voice Compression Modules; Circuit Emulation for Video over ATM; VAD, Echo Cancellation;
Fax	Fax Relay bis 9,6 kbit/s

Tabelle 11 : Leistungsmerkmale Cisco MC 3810 [MC3810]

Als Cisco IOS basiertes Gerät entspricht das Management Interface dem anderer Cisco Produkte - Management über CiscoView Network Management System, Netsys Technologies Tool Suite bzw. die in der Entwicklung befindlichen Cisco Carrier Class Service Management Lösungen, welche unter anderem Call Detail Records - CDR unterstützen.

Cisco 2600 Series Modular Multiservice Platforms

Die Geräte der Cisco 2600 Serie können als ***VoIP Gateway*** eingesetzt werden.
Sie besitzen zwei User configurable ***WAN Interface Card - WIC*** - Slots, ein Network Module Slot und ein ***Advanced Integration Module - AIM*** - Slot mit Unterstützung für WAN bzw. Voice Interface Cards mit analogen (bis 16 intern), S0 (bis 10) bzw. E1 (bis 2) Schnittstellen. Die Geräte der Serie entsprechen H.323 und bieten G.729, G.723, VAD, Comfort Noise

Generation und Echo Cancellation. LAN seitig sind RSVP, WFQ und IP Precedence implementiert.

Cisco 3600 Series und 3660 Series Modular Multiservice Platforms

Die Cisco 3600 und 3660 Serie dienen als modulare Multiservice Access Plattform für mittlere Unternehmen und kleinere Internet Provider. Die Geräte der 3600 Serie - 3620 mit zwei Mo-dule Slots und 3640 mit vier Module Slots - unterstützen eine große Anzahl von Netzwerk Modulen (Ethernet, Tokenring etc.), WAN Interface Cards (Serial, E1 etc.) und Voice Inter-face Cards (ISDN BRI, PRI).
Die Cisco 3660 Serie wurde aufbauend auf der 3600 Serie für größere Unternehmen konzipiert. Die 3660 Serie bietet sechs Module Slots, die zusätzlich zu den Möglichkeiten wie bei der 3600 Serie mit ATM Interfacen (E1 - OC3) bestückt werden können, zwei Advanced Integration Module Slots und ein bis zwei Fast Ehternet Ports.

Die Geräte der Cisco 36x0 Serie können als ***VoIP Gatekeeper*** und ***VoIP Gateway*** eingesetzt werden.

5.2.2 Cisco IP Telefone

Cisco bietet zwei IP Telefone an, das ***Cisco IP Telephone Model 12 SP+*** und das ***Cisco IP Telephone Model 30 VIP***.
Beide Telefone entsprechen H.323, unterstützen die Codecs G.711 und G.723.1 inklusive VAD und CNG .
Die Telefone unterscheiden sich in der Anzahl der frei programmierbaren Tasten (12 bzw. 30 - davon 4 fest für transfer, display, hold und redail).
Ihrer IP Adresse ist statisch oder kann über DHCP bezogen werden. Administriert werden die Telefone über ein Web Interface - siehe dazu auch Cisco Call Manager.

5.2.3 Call Management

Der ***Cisco Call Manager*** setzt auf einen Windows NT Server auf und liefert die Netzwerk Intelligenz bzw. dient zur Verwaltung der IP Telefone. Die verwalteten User können lokal aber geografisch auch verteilt sein.

Er stellt Call Processing Funktionen für Cisco IP Telefone bereit, wie das Resourcen Management durch Signalisierung und Koordination von Call Control Aktivitäten bzw. das Management von Calling Zones zur effektiven Nutzung der Bandbreite und max. Audio Qualität. Zu den weiteren Funktionen des Call Manager gehören : call hold, call transfer, call forward, call park und call party identification.
Über ein SMDI Interface bietet der Call Manager Zugriff auf Voice Mail Systeme verschiedener Hersteller, auf IVR Systeme und CDR Reports zum Call Accounting und Billing.

Für zukünftige Versionen sind Verschlüsselungsmechanismen für Audio und Signalisierung, sowie die Unterstützung redundanter Call Management Server geplant.
[AS], [MC3810]

Zusammenfassung

Die Produkte der Siemens AG und Cisco Systems repräsentieren zwei Herangehensweisen.
Die Siemens AG - aus der TK Welt kommend - sieht in VoIP eine Möglichkeit, ***TK Dienste*** wie z.B. Sprachübertragung, Voicebox, Call Recording bzw. neue Mehrwertdienste wie Messaging im LAN anzubieten.
Cisco Systems - als Ausrüster für Transportnetze - sieht in VoIP eine Möglichkeit, ***Sprach-*** bzw. ***Videoübertragung*** in vorhandene LANs zu integrieren.

Die Entscheidung, welcher Ansatz bevorzugt wird, hängt allein von den individuellen Anforderungen des Nutzers ab.

6 VoIP Integration am Beispiel der AOK M-V

In den folgenden Abschnitten werden die Kommunikationsanforderungen eines strukturierten Unternehmens am Beispiel der AOK Mecklenburg - Vorpommern, hinsichtlich der Einführung von VoIP betrachtet. Integrations- bzw. Migrationskonzepte stehen dabei im Mittelpunkt neben den zur Nutzung von VoIP notwendigen technischen Voraussetzungen im WAN und LAN Bereich, deren Grundlagen im Kapitel 3 erläutert wurden.

6.1 Allgemeine Struktur der AOK in M-V

In Abbildung 29 ist die geografische Struktur der AOK in Mecklenburg - Vorpommern entsprechend der Mitarbeiterzahl gekennzeichnet dargestellt.
Zu erkennen sind die Hauptstandorte und die organisatorischen Zentren Schwerin, Rostock und Neubrandenburg.

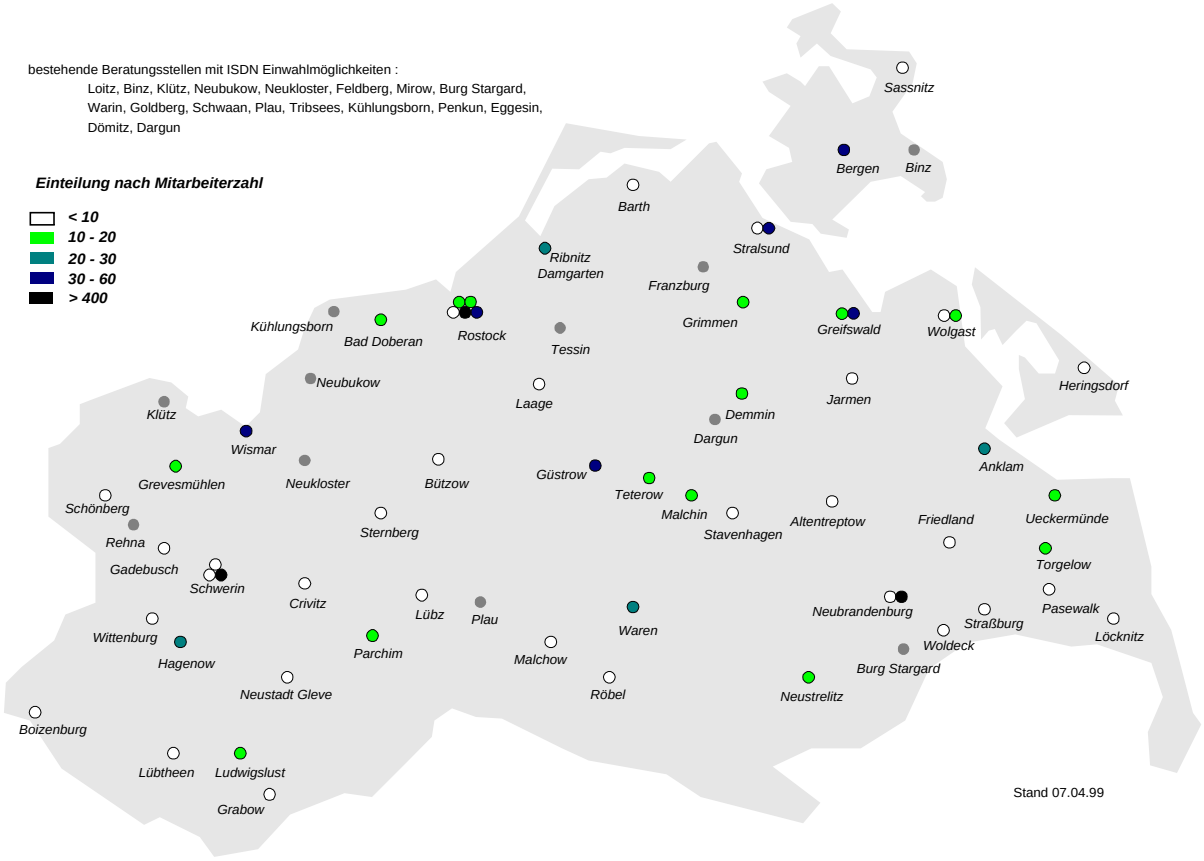

Abbildung 29 : personelle Struktur der AOK [AOK]

Nachfolgende Abschnitte untersuchen die TK- und Datennetzstruktur der AOK und stellen mögliche Szenarien zur Integration von VoIP vor.

6.2 Mögliche Szenarien zur Integration von VoIP in der AOK

Folgenden Möglichkeiten bieten sich der AOK zur Integration von VoIP :

- die TK Anlagenkopplung der Haupstandorte (Rostock, Schwerin, Neubrandenburg) über VoIP

  Ziel : Verringerung der Kosten im WAN Bereich;
- Ersetzen von TK Anlagen durch VoIP Installationen - TK lose Geschäftsstelle - in Standorten mit geringen Mitarbeiterzahlen (z.B. < 5 Mitarbeiter)

  Ziele: Verringerung des Investvolumens,
  Unterstützung der Geschäftsprozesse,
  Verringerung der Kosten im WAN Bereich.
- VoIP in dienstleistungsorientierten Abteilungen der AOK- lokal oder standortübergreifend

  Ziele: mehr Service im Wettbewerb mit anderen Kassen und Privatversicherern,
  Optimierung von Arbeitsabläufen,
  Schaffung der Basis für neue Dienste - z.B. Messaging.

Die Szenarien verfolgen unterschiedliche Ziele und Nutzenaspekte. Zur Einschätzung der Wirtschaftlichkeit sind weiterführende Untersuchungen nötig, da in dieser Diplomarbeit technische Möglichkeiten zur Integration von VoIP erläutert werden.

6.3 Allgemeine Planungsschritte zur Implementierung von VoIP

Die Planung zur Integration von Sprachübertragung in IP Netze gliedert sich in sechs Schritte: die Prüfung des vorhandenen Netzwerkes, Festlegung der Netzwerkziele, die technische Analyse, das Verhalten des Anwenders, die Planung der Kapazitäten und die Kostenanalyse.

6.3.1 Prüfung des Netzwerkes

Apriori müssen Informationen zur ***genutzten Bandbreite*** , ***Routerkapazität*** und ***Ressourcenplanung für zukünftige Projekte*** bekannt sein.

Durch die Integration von Sprache steigt die Leitungsbelastung immens an, allerdings haben Sprache und Daten unterschiedliche Eingangsmuster [36], d.h. es treten keine gleichzeitigen Spitzenwerte für Sprache und Daten auf.

[36] Sprache und Daten einzeln betrachtet, bei Diensten mit Sprach- Datenintegration summiert sich der Bandbreiten-bedarf

Ein Netzwerkupgrade für den Sprachtransport würde somit auch zusätzliche Kapazität für den Datentransport schaffen.

6.3.2 Netzwerk Ziele

Die ***Leistungsfähigkeit der Datenübertragung***, die ***Leistungsfähigkeit der Sprachübertragung*** und der ***finanzielle Aspekt*** verlangen das Hauptaugenmerk. Durch getrennte Betrachtung der beiden ersten Punkte fällt die Auswahl einer geeigneten Technik leichter.

6.3.3 Technische Analyse

Für die wirtschaftliche Einbindung der neuen Technologie müssen die Aspekte des bestehenden Netzwerkes berücksichtigt werden. Ebenso wichtig sind Entscheidungen über die die Implementierung betreffenden Außenstellen[37].

Die Qualität des Gateways ist entscheident für den Erfolg der Sprachübertragung. Folgende Punkte sind von Bedeutung:

- Schnittstellen - analoge Exchange Lines, ISDN Basis bzw. Primärraten,
- unterstützte Codecs[38],
- zentrale oder dezentrale Implementierung der Adreßverwaltung/ -auflösung,
- kann Gateway Art von individuellen Anrufen identifizieren (siehe Fußnote 39),
- allgm. auftretende Verzögerungen (z.B. Anti Jitter Methoden),
- Reaktion auf Überlastung oder Bandbreitenlimitierung,
- explizite bzw. automatische Konfiguration für Sprach-, Daten- und Faxübertragung[39],
- wie erfolgt das Management mehrerer Gateways,
- Anpassungsfähigkeit an zukünftige Entwicklung.

[37] Ein langsames oder unterhalb des Qualitätslimits arbeitendes System ist ebenso unakzeptabel, wie eines, das dem Anwender keine große Erleichterung im Datenverkehr bringt.
[38] Je geringer die Bandbreite, desto höher Komprimierung, Rechenaufwand etc., siehe Codecs
[39] Ein Gateway mit Faxunterstützung digitalisiert das Signal nicht sondern demoduliert es lokal, verpackt es in IP Pakete und verschickt es an des Remote Gateway, welches die Originalsignale rekonstruiert und den Faxversand startet.
Der Betrieb eines Modems ist nicht zu empfehlen, da Modemsignale wie Sprache behandelt werden und daher einen unverhältnismäßig großen Teil der verfügbaren Bandbreite belegen. Gateways sollten in der Lage sein, die Art (Sprache, Modemsignale) individueller Anrufe indentifizieren zu können.

6.3.4 Bedenken von Usern

Ebenso wie eine akzeptable Grundqualität für Sprache über das Netzwerk geplant wird, muß berücksichtigt werden, wie der Anwender das System empfindet. Das hängt von der vorhandenen Telefonanlage ab.
Komfortabel ist es, wenn durch das VoIP System die gewohnten akustischen Signale generiert und gewohnte Leistungsmerkmale unterstützt werden.

6.3.5 Planung der Kapazitäten

Die Planung von VoIP verlangt als einen Hauptpunkt die Planung der Kapazitäten und damit der Wahrscheinlichkeit einer freien „Leitung“ beim Abheben des Hörers. Besonders zu Spitzenzeiten muß genügend Kapazität vorhanden sein, da sich dann die größten Verbindungskosteneinsparungen realisieren lassen.
Wenn 95 % der Leitungskapazität (PSTN 99,9%) verfügbar sind, und sich dabei eine Kosteneffektivität zeigt, ist bereits ein akzeptables Ziel erreicht.

Da die Gegebenheiten von Unternehmen jedoch stark variieren spielen die Logs der vorhandenen Telefonanlagen (wieviele Gespräche, wann, wohin) zum Verständnis der Anwendungsmuster eine wichtige Rolle.

Durch Kombination der in den Logs dokumentierte Bandbreite für Sprache und den Routerstatistiken für das reine Datennetz können unter Berücksichtigung der Parameter der geplanten VoIP Installation[40] Rückschlüsse über die benötigten Kapazitäten gewonnen werden.
[PCPro 11/98]

[40] Bandbreite des Codec, Verzögerungszeiten, Sprachqualität etc.

6.4 Analyse des AOK Netzes

6.4.1 Analyse des TK Netzes

Struktur des TK Netzes

Die Standorte verfügen, wie aus Abbildung 30 ersichtlich, über Hicom 330/ 350 E TK Anlagen der Siemens AG bzw. über 80 CM TK Anlagen der Telekom AG.
Die Hauptstandorte Schwerin, Neubrandenburg und Rostock. sind über 2Mbit/ s Leitungen miteinander verbundenen und bieten somit standortübergreifende TK Kommunikation innerhalb des AOK TK Netzes. Alle Standorte sind über ISDN an das öffentliche Telefonnetz angeschlossen.

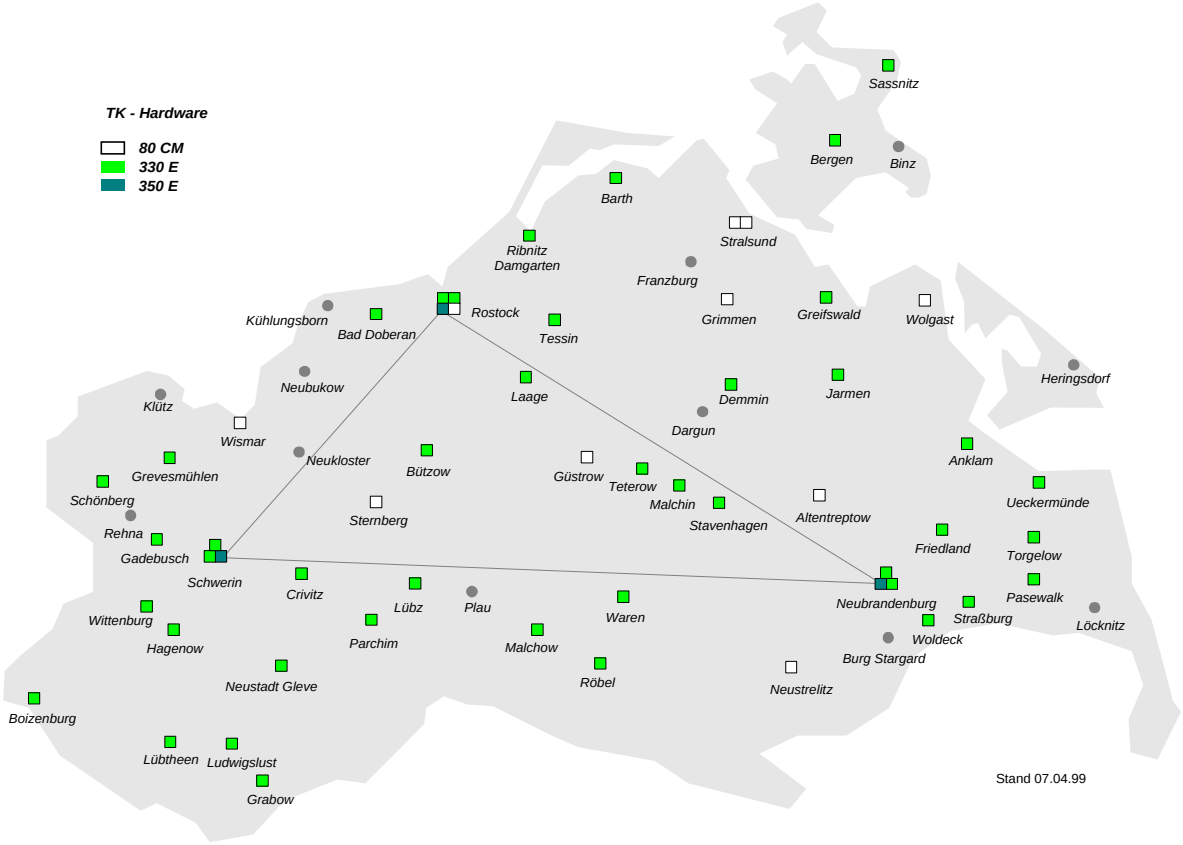

Abbildung 30 : TK Netz der AOK [AOK]

Analyse des TK Netzes

Aus zeitlichen und organisatorischen Gründen konnten von der AOK nur eine begrenzte Anzahl von standortbezogenen Verkehrsmessungen bereitgestellt werden, so daß dementspre-

chend weiterführende Untersuchungen zur Einschätzung des TK Verkehrsaufkommens notwendig sind.

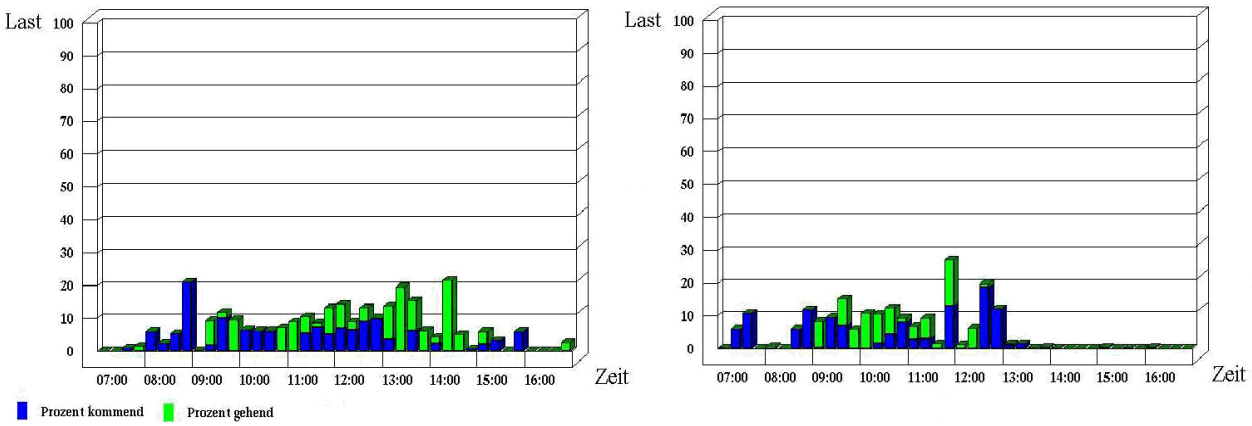

Abbildung 31 : Lastverteilung am Beispiel Altentreptow (links Do 16.12./ rechts Fr 17.12.)

In der Abbildung 31 wird beispielhaft am Standort Altentreptow das Verkehrsaufkommen eines Standortes mit ca. 10 Mitarbeitern am Donnerstag (16.12.99) und Freitag (17.12.99) dargestellt. Der Standort Altentreptow ist über 2 BRI Ports (4 x ISDN B Kanal) an das öffentliche Telefonnetz angeschlossen.

Deutlich zu erkennen ist, daß der eingehenden Verkehr überwiegt, auch übersteigt die Auslastung der der 4 B Kanäle innerhalb einer Meßperiode von 15 Minuten nicht die 30 % Marke.
Um jedoch allgemeingültige Aussagen zuerhalten sind weitere Messungen, die sich über einen längeren Zeitraum - ca. 2-3 Wochen - erstrecken notwendig.
Weiterhin müssen diese Untersuchungen eine Aussage über die zeitliche Verteilung des Gesprächsvolumen entsprechend des Gesprächsziels (extern oder AOK intern) enthalten.
Erst diese Untersuchungen, inclusive der in den folgenden Kapiteln beschriebenen Analysen des Datennetzes der AOK, machen eine realistische Einschätzung der technischen und wirtschaftlichen Aspekte beim Einsatz von VoIP innerhalb der AOK M-V möglich.

6.4.2 Analyse des Daten Netzwerkes

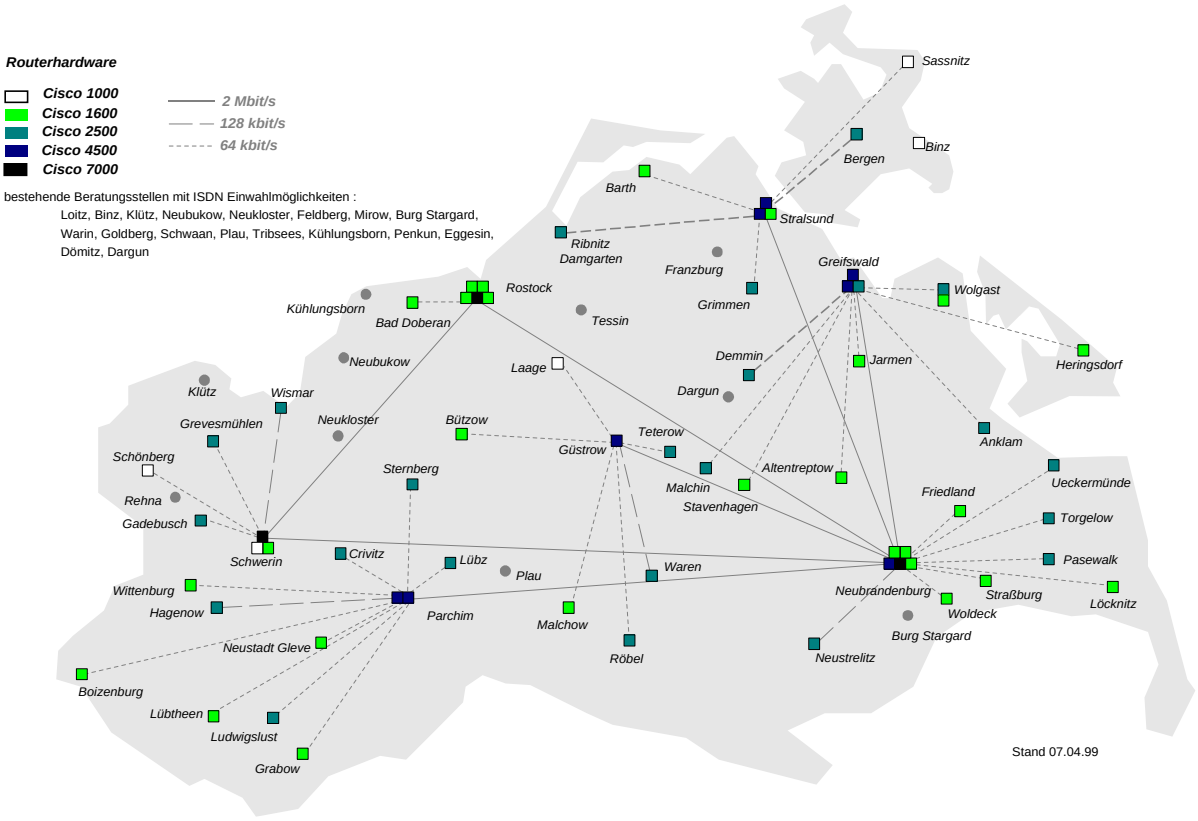

Abbildung 32 : Datennetz der AOK [AOK]

Struktur des WAN

In Abbildung 32 ist das WAN der AOK dargestellt. Es ist deutlich eine hierarchische Struktur mit Neubrandenburg als zentralen Knoten zu erkennen. Dort befindet sich das Rechenzentrum.

Die Hauptstandorte ***Neubrandenburg***, ***Rostock*** und ***Schwerin*** (> 400 Mitarbeiter) sind über serielle 2Mbit/s Leitungen vermascht.

Weitere Standorte wie ***Stralsund, Greifswald, Güstrow*** und ***Parchim*** wurden wegen ihrer geografischen Lage als lokale Zentren aufgebaut und bilden über 2 Mbit/s Verbindungen mit dem Rechenzentrum Neubrandenburg eine Stern - Topologie.

Alle anderen Standorte mit weniger als 20 Mitarbeitern sind über serielle 64kbit/s Verbindungen bzw. mit 128kbit/s Verbindungen - Waren, Hagenow, Ribnitz, Bergen Demmin, Neustrelitz und HRO Lütten Klein [41] (ca. 20 - 30 Mitarbeiter) an die Hauptstandorte bzw. lokale Zentren angeschlossen.

[41] Lütten Klein - 44 Mitarbeiter

Die IP Adress - Struktur der AOK ist hierarchisch aufgebaut. Dadurch können die Router statisch konfiguriert, und somit die Wegewahl beschleunigt werden - Vorteil bei der Übertragung isochroner Dienste.

Struktur der LANs

In den Hautstandorten Neubrandenburg, Rostock und Schwerin werden geswitchte LANs eingesetzt (Layer 2 Switching - ohne Priorisierungsmechanismen). In allen anderen Standorten der AOK werden zur LAN Vernetzung Hubs genutzt.

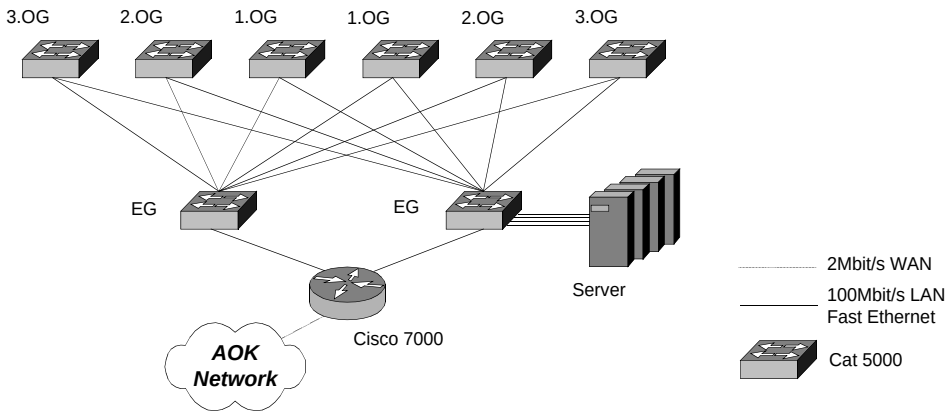

Abbildung 33 : typische LAN Umgebung am Beispiel der Hauptgeschäftsstelle Rostock

Analyse des WAN

Im Rahmen dieser Diplomarbeit wurde eine Verkehrsmessung an den WAN Verbindungen durchgeführt. Die Messung wurde mit der in der AOK eingesetzten Netzwerkmanagement Software Netview (AIX Version) durchgeführt.

In einem Zeitraum vom Donnerstag den 17.11.99 bis Mittwoch den 17.12.99 wurden im Abstand von 10 Minuten die eingehende bzw. abgehende Anzahl von ***Bytes*** auf den seriellen Interfaces des Routers in Neubrandenburg und auf den lokalen seriellen Interfacen der Router aller anderen Geschäftsstellen aufgenommen.

Als ein Beispiel für die Auslastung der ***64 kbit/s Verbindung*** ist in der folgenden Abbildung der Standort Sternberg (11 Mitarbeiter) dargestellt.

Der am Port eingehende Verkehr weist nur wenige Lastspitzen auf. Der Verkehr, der das Port verläßt bleibt bis auf wenige Ausnahmen unter 8kbit/s.

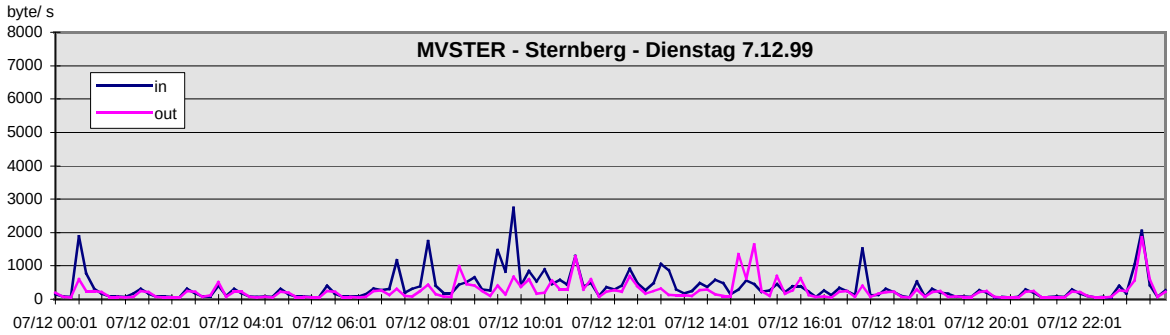

Abbildung 34 : Durchsatz (in byte/s) am seriellen Interface in Sternberg Richtung Parchim

Eine Bandbreite von 64 kbit/s ist für die Sprachintegration von bis zu 10 Mitarbeitern nicht einsetzbar, da pro Gespräch mindestens 11 kbit/s (G.729 + CRTP; mit VAD ca. 5-6 kbit/s) in eine Richtung benötigt werden. Für kleinere Geschäftsstellen mit bis zu ca. 5 Mitarbeitern ist die Bandbreite ausreichend (siehe S.90 Aussagen zur weiteren Untersuchungen).

Ein typisches Verkehrsaufkommen für Standorte, die mit einer ***128 kbit/s Verbindung*** an die Hauptstandorte angebunden sind zeigt, das folgende Diagramm am Beispiel von Wismar (38 Mitarbeiter).Wie schon im vorigen Beispiel bleiben die Lastspitzen innerhalb der Geschäftszeiten unter 40 % der verfügbaren Bandbreite, so daß prinzipielle Bandbreitenreverven für die Implementierung von VoIP (AOK internes Gesprächsaufkommen über VoIP) vorhanden sind.

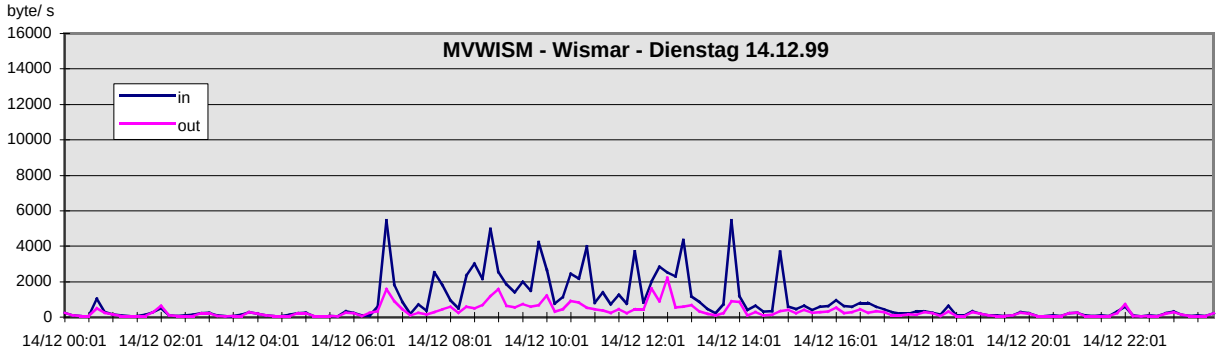

Abbildung 35 : Durchsatz (in byte/s) am seriellen Interface in Wismar Richtung Schwerin

Als Beispiel für das typische Verkehraufkommen von 2Mbit/s Verbindung ist in der folgenden Abbildung 36 eine Tagekurve der Geschäftsstelle Stralsund (35 Mitarbeiter) dargestellt. Deutlich zu erkennen ist, daß die 2 Mbit/s Verbindung nach Neubrandenburg nur bis max. 10% der verfügbaren Bandbreite (Tagespitzen) ausgelastet ist. Die durchschnittliche Grundlast beträgt ca. 5% der verfügbaren Bandbreite.
Es sind große Reserven vorhanden, die zur Integration von Sprachübertragung genutzt werden können (z.B. Kopplung der TK Anlagen).

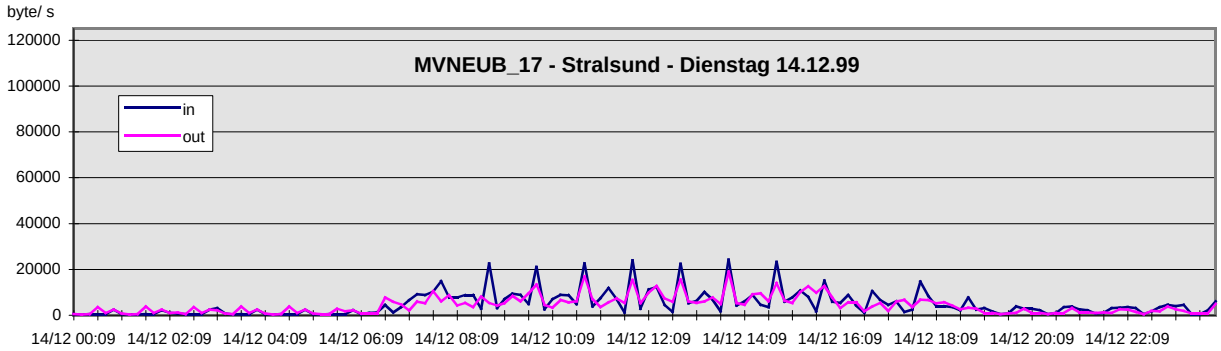

Abbildung 36 : Durchsatz (in byte/s) am seriellen Interface in NeubrandenburgRichtung Stralsund

In Abbildung 37 ist das Verkehrsaufkommen vom Rechenzentrum in Neubrandenburg in Richtung Schwerin dargestellt. Diese stellt die am stärksten ausgelastete 2 Mbit/s Verbindung der AOK in Mecklenburg - Vorpommern dar.
Auch die stark ausgelastete Strecke zwischen Schwerin und Neubrandenburg verfügt über erhebliche Reserven, die für VoIP Implementierungen genutzt werden kann.

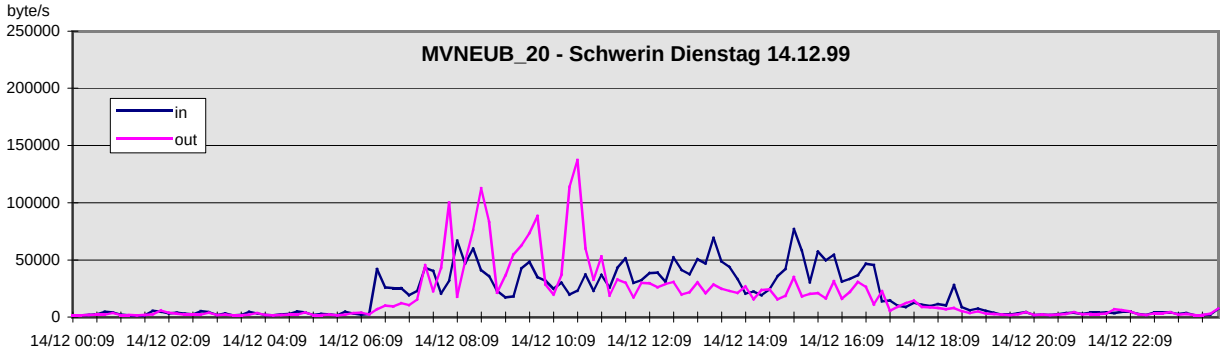

Abbildung 37 : Durchsatz (in byte/s) am seriellen Interface in Neubrandenburg Richtung Schwerin

Bei den Diagrammen der 2Mbit/s Verbindungen ist zu beachten, daß diese nicht an den lokalen Interfaces gemessen wurden, sondern am Router in Neubrandenburg - ***MVNEUB***. Dadurch sind die Graphen für ***in*** - eingehenden Verkehr - und ***out*** -ausgehenden Verkehr vertauscht.

In Anhang D sind die Graphen der obigen Beispiele für den gesamten Meßzeitraum (18.11.-17.12.) dargestellt.
Die Diagramme aller weiteren Standorte werden aus Platzgründen nicht in den Anhang aufgenommen, sind aber elektronisch als Excel Tabellen/ Diagramme verfügbar.

Analyse der Lastspitzen (Bandbreiteausnutzung >80 %)

Lastspitzen (siehe Anhang) des eingehenden Verkehrs - ***in*** - in den Diagrammen lassen sich Software Updates zuordnen, die netzweit über Microsoft SMS - Software Management System - durchgeführt werden. Beispiele sind :

15. - 18.11. - Installation Outlook und NT Service Pack 5
19. - 20.11. - Restinstallation Outlook und NT Service Pack 5
22. - 26.11. - Übertragung von Anwender Profilen
26. - 28.11. - umfangreiche fachspezifische Softwareinstallationen

Verkehrsspitzen, die kurzzeitg (ca. 1 Tag) davor auftreten, hängen mit der Softwareverteilung auf die Server zum jeweiligen Software Update zusammen.
Die SMS Software Updates erfolgen in der Regel außerhalb der Geschäftszeit (nach 20 Uhr). Komplikationen (z.B. Verzögerungen) können jedoch dazu führen, daß diese Updates im ungünstigsten Fall auch innerhalb der Geschäftszeiten durchgeführt wurden. Dies erklärt, daß einige ausgeprägte Lastspitzen in diesen Zeitraum fallen.

Lastspitzen des von den Interfacen ausgehenden Verkehrs - ***out*** - werden durch Server Backups verursacht, wenn lokale Server keine Backup Bandlaufwerke besitzen bzw. nicht mit den entsprechenden Bändern bestückt sind. Standorte für die dies zutrifft sind:

Backup nach	***Backup von***
Stralsund - tgl.	Ribnitz-Damgarten, Barth
Güstrow - tgl.	Röbel, Malchow
Parchim - tgl.	Lübz, Ludwigslust, Hagenow
Schwerin - wtl.	Gadebusch, Schwerin -Helenenstr.

Tabelle 12 : Standorte ohne eigene Server Backupmöglichkeiten; tgl. - täglich, wtl. - wöchentl.

Server Updates werden grundsätzlich außerhalb der Geschäftszeiten durchgeführt.
Beim Standort Stralsund Knieper West fällt auf, daß die Server Backups einen überdurchschnittlich langen Zeitraum beanspruchen (> 10 Std.). Ein Großteil des Backups fällt somit in die Geschäftszeiten (bis ca. 13 Uhr). Um die Situation zu entschärfen, kann der Backup um ca. 6 Std. (ab 19 Uhr) vorverlegt werden bzw. ist zu prüfen, ob ein derartig umfangreicher Back up notwendig ist. Falls die Notwendigkeit besteht, ist es sinnvoll eine lokale Backupmöglichkeit zur Entlastung des Netzwerkes einzurichten.
Andere Lastspitzen bzw. eine hohe Grundlast - > 16 kbit/s (z.B. Dierkow, Lütten Klein, HST Knieper West) - kann Datenbankverkehr (z.B. Audi) zugeordnet werden.

6.5 Integration von VoIP

Für die Implementierung von VoIP sind weitere Untersuchungen, die die wirtschaftlichen (wie in 2.1.6 angesprochen) und die konkreten technischen Aspekte betreffen, erforderlich. Dabei zu behandelnden technischen Fragen schließen z.B ein:

- die für den jeweiligen Standort benötige Bandbreite unter Beachtung der durch die Veränderung der Prozesse hervorgerufenen Änderungen im Voiceverhalten bzw. im Datenverkehr (verstärkte Nutzung von Mail und Internet zur Kommmunikation mit Kunden, geplante neue Anwendungen etc.);
- die benötigten Reserven für Spitzentage bzw. als Ausbaureserve;
- Möglichkeiten der Kompression (siehe CRTP 6.4.2);
- notwendige Software Upgrades (Cisco IOS Stände sind gerätebezogen) bzw. Hardware Upgrades (evtl. Speicherausbau bzw. neue Komponenten) etc.

Da das Datennetz der AOK in einem homogenen Cisco Netzwerk besteht, werden im folgenden allgemein die Möglichkeiten der Anpassung der aktiven Cisco Netzwerkelemente an die Integration von Sprachübertragung erläutert.

6.5.1 Notwendige Voraussetzungen des Daten Netzwerkes - WAN

Um eine Sprachübertragung über ein Datennetz zu ermöglichen müssen Mechanismen geschaffen werden, die die Anforderungen von Sprachübertragung - wie geringer Delay und Jitter (siehe ITU G.114) - einen QoS/ CoS erfüllen.
Diese Mechanismen umfassen, wie schon in Kapitel 3 vorgestellt Queueing Methoden, Methoden zur Datenpriorisierung, zur Bandbreitenreservierung und zur Steigerung der Effektivität der Übertragung (CRTP etc.).

Cisco faßt die dazu nötigen Mechanismen unter dem Begriff ***Cisco QoS Networking Tools*** zusammen. Sie beinhalten :

- Congestion Managment (WFQ, IP Precedence, RSVP),
- Congestion Avoidance (RED,WRED),
- effektiven Bandbreitenutzung (durch z.B. Ausnutzung der Packet Residency - MLPPP- bzw. RTP Header Compression und VAD) und
- Mechanismen zur Vermeidung von Circuit Speed Mismatch (Traffic Shaping)

Die Kombination dieser Mechanismen (in Router implementiert) erlaubt die Priorisierung von Verkehrarten auf Layer 3, siehe Kapitel 3.3, bzw.dient zur besseren Unterstützung (Er-höhung der Effektivität) der Übertragung von Echtzeitverkehr (z.B. LFI, RTP - HC siehe nachfolgende Beschreibung in diesem Kapitel).

Die Implementierung der vorgestellten Mechanismen im IOS muß entsprechend der Geräte-klasse (z.B. Router, Switche) überprüft werden, da die IOS Stände gerätebezogen sind.

Congestion Management - Queueing Mechanismen WFQ

Eine Möglichkeit mit einem Overflow des eingehenden Verkehrs zu begegnen, ist der Einsatz von Queueing Algorithmen, um den Verkehr zu klassifizieren und Verkehrsarten zu priori-sieren(z.B. Real Time Traffic - Voice).

Die Cisco IOS Software enthält die folgenden Queueing Mechanismen :

- ***FIFO Queueing*** - Pakete werden in der Reihenfolge ihres Eintreffens weitergeleitet mit den Nachteilen, daß keine Priorisierung erfolgt, die Ankunftsreihenfolge die genutzte Bandbreite, die Verzögerung und die Buffer Zuweisung bestimmt - demzufolge keine Eignung für Sprachintegration;
- ***Priority Queueing (PQ)*** - flexible Priorisierung entsprechend des Übertragungs-protokolls (IP, IPX etc.), der Quell- und Zieladresse usw. PQ basiert auf einer statischen Konfiguration und passt sich daher nicht automatisch veränderten Netzanforderungen an - Einsatz zur Priorisierung von Datenbankverkehr etc.;
- ***Custom Queueing (CQ)*** - Applikationen mit speziellen minimaler Bandbreite bzw. Verzögerungsanforderungen (z.B. SNA) wird eine bestimmte Bandbreite garantiert. Die Zuordnung des Queuebuffers erfolgt entsprechend der Paketklasse. Die Abarbeitung der Queues erfolgt nach dem Round Robin Verfahren. CQ basiert ebenfalls auf einer sta-tischen Konfiguration und passt sich nicht automatisch veränderten Netzanforderungen an.
- ***Weighted Fair Queueing (WFQ)*** - WFQ ist ein Flow basierter Queueing Algorithmus, interaktiver Verkehr wird bevorzugt abgearbeitet (an den Anfang der Queue gestellt), die verbleibende Bandbreite wird zwischen den anderen Anwendungen fair geteilt. WFQ wurde entwickelt, um den Konfigurationsaufwand zu minimieren und passt sich automatisch veränderten Netzwerkanforderungen an.

WFQ ist der default Queueing Mode von seriellen Interfacen ≤ E1 (2 Mbit/s).
WFQ erkennt IP Precedence [42] und RSVP, die von Cisco hauptsächlich eingesetze QoS Signalisierungs Technik .

Cisco IOS bietet eine weitere Priorisierungsmethode basierend auf Transport Protokoll und Port mit ***RTP Reserve***. RTP Reserve erzeugt im WFQ eine spezielle Queue für Real Time Pakete. Der Router füllt diese Queue entsprechend der mit RTP Reserve konfigurierten Port Nummer (meist 16384 - 16484). Jeglicher IP Verkehr, der in diesen Port Bereich fällt, wird priorisiert. Real Time Sprachverkehr wird über die UDP Ports im Bereich 16384 bis 16624 übertragen. RTP Reserve bietet keine Header Compression.

Congestion Avoidance

Congestion Avoidance überwacht die Netzlast, um Congestion zu vermeiden, im Gegensatz zu Congestion Management Techniken, welche Congestion nach deren Auftreten behandeln. Cisco implementiert ***Weighted Random Early Detection (WRED)***.
WRED nutzt den Random Early Detection (RED) Algorithmus, um die Verkehrslast zu monitoren und bei einer beginnenden Congestion stochastisch Pakete zu verwerfen.

In Kombination mit ***IP Precedence*** wird Verkehr mit hoher Priorität bevorzugt behandelt, und bei beginnender Congestion werden selektiv Pakete niedriger Priorität verworfen.
WRED kann in Zusammenhang mit ***RSVP*** einen ***Integrated Services controlled Load QoS*** liefern (siehe 3.3).

Auf Verbindungen > E1 kommt WRED zusammen mit FIFO Queueing zum Einsatz, da bei diesen der Einsatz von WFQ (Einsatz bei Verbindung <E1) nicht effektiv genug ist.

QoS Signalisierung RSVP

Mit ***RSVP*** wird Applikationen die dynamische Reservierung von Bandbreite möglich - siehe auch 3.3. Die RSVP Implementierung von Cisco erlaubt Bandbreitenreservierung mittels RSVP auch innerhalb des Netzwerkes durch RSVP Proxies, falls die Applikationen keine Bandbreitenreservierung anfordern können.

[42] ***IP Precedence*** nutzt wie in 4.1 beschrieben 3 bit des ToS Felds des IP Headers, um jedem Paket eine Class of Service zuzuordnen, die dann von den Queueing Methoden (z.B.WFQ, WRED) zur Priorisierung genutzt werden.

Über WFQ und WRED erfolgt innerhalb von RSVP die Klassifikation und das Scheduling für die reservierten Flows .
Im Zusammenhang mit ***WFQ*** liefert RSVP ***Integrated Services Guaranteed Service*** , mit ***WRED - Controlled Load Services*** (siehe Verfahren zur Datenpriorisierung auf Schicht 3).
Defaultmäßig ist RSVP bei Cisco Geräten aus Kompatibilitätsgründen zu älteren Geräten deaktiviert.

Steigerung der Effektivität der Übertragung - LFI,CRTP

Die Cisco IOS Software unterstützt zwei sogenannte Link Efficiency Mechanismen - Link Fragmentation and Interleaving (LIF) und Real Time Header Compression (RTP-HC bzw. auch CRTP).

LFI : Interaktiver Verkehr wird bei gleichzeitiger Übertragung von großen Datagrammen (z.B. FTP Verkehr) erhöhten Delay und Jitter unterworfen, besonders bei schmalbandigen Verbindungnen.
LFI reduziert Delay und Jitter durch Aufteilung großer Datagramm Pakete und Interleaving der resultierenden kleinen Pakete mit low delay Paketen (Sprache etc.). LFI erfordert ein auf dem jeweiligen Interface konfiguriertes Multilink Point to Point Protocol mit aktiviertem Interleaving.
Als Regel für die Fragmentgröße bei angenommenen max. Blocking Delay gilt von 10 ms gilt.:

$$\frac{10ms}{time\_for\_1byte\_at\_b/w} = Fragment\_size$$

Gleichung 1 : Berechnung der Fragmentgröße [Aran99]

Mit Hilfe dieser Formel kann festgestellt werden, daß Fragmentations Methoden oberhalb einer Bandbreite von 768kbit/s (Fragment 1000 byte) generell nicht notwendig sind.
Der IETF Draft Multilink PPP implementiert ähnliche Funktionen wie LFI.
RTP - HC - Für eine typische RTP Payload von 20 - 160 byte (20ms Sprache bei 8 - 64 kbit/s) - ergibt sich ein IP/ UDP/ RTP Header von 40 byte (20+8+12). RTP - HC erhöht durch die Kompression des RTP/ UDP/ IP Headers - auf 2-4 byte - die Effektivität der Übertragung. Besonders schmalbandige Verbindungen (≤ 385 kbit/s) profitieren vom kleineren Overhead und dem dadurch reduzierten Übertragungs - Delay.

Dieses Prinzip kann mit IPv6 unter Ausnutzung des Priority Feldes ebenfalls angewandt werden.

Cisco unterstützt RTP Header Compression auf seriellen Verbindungen, die Frame Relay, HDLC oder PPP Encapsulation nutzen, und auf ISDN Interfaces.
Der entsprechende IETF Standard heißt Compressed RTP (CRTP).

Beim Einsatz von RTP Header Compression ist jedoch zu beachten, daß die CPU durch die Bearbeitung des komprimierten Headers belastet wird und RTP - HC keine Form von QoS ist.

6.5.2 Notwendige Voraussetzungen des Daten Netzwerkes - LAN

Voraussetzung für die Integration von VoIP in das LAN der AOK ist die Implementierung von Mechanismen zur Unterstützung von Echtzeit Datenverkehr durch das Transportnetzwerk.
Der zentrale Punkt im Transportnetz einer VoIP Installation mit starker Datenintegration (Dienstleistungsbereich - Kundenservice) besteht in Layer 4 Switchen, da ab Schicht 4 der Datenfluß applikationsabhängig erkannt und gesteuert werden kann. Wie schon in Kapitel 3.4.2 dargestellt, werden die Applikationen in Prioritätsbereiche - Verkehrsklassen - eingeteilt, denen entsprechende CoS der Infrastruktur zur Verfügung stehen. Die Priorität selbst kann an andere Geräte (z.B. Layer 2 Switche mit Priorisierungsmechanismen - siehe 3.2) weitergegeben werden.
Priorisierungsmechanismen sind nur sinnvoll, wenn sie den Geräten des gesamten Transportweges interpretiert werden können.

Damit netzweit (WAN/ LAN) der Transport von priorisiertem Verkehr möglich ist, muß das heutige Layer 2 Switching Netzwerk der AOK M-V um Priorisierungsmechanismen (siehe 3.2) erweitert werden, einschließlich der im vorigen Kapitel aufgeführten Queueing Mechanismen.

Zusammenfassung

Die notwendigen Voraussetzungen des Datennetzes der AOK zur Integration von VoIP sind :

- im LAN : Layer 4 Switching in Hauptgeschäftsstellen; Mapping von Layer 4 auf Layer 2/ 3 Priorisierungsmechanismen für kleinere Geschäftsstellen;
- im WAN : Nutzung von Layer 3 Priorisierung durch IP Precedence (IP Protokoll) und WFQ;

bzw. Nutzung von Layer 3 Priorisierungsmechanismen (z.B. Integrated Services Architecture[43]: RSVP + WFQ oder RSVP + WRED auf breitbandigen Verbindungen);

- Anpassung der Datenstruktur an Übertragungsanforderungen durch Nutzung von LFI und CRTP.

Diese Voraussetungen des Netzwerkes bilden die Grundlage für die Implementierung von VoIP im Datenetz der AOK.

Ziele des Einsatz von VoIP sind zum einen die Reduzierung der WAN Kosten durch :

- die TK Anlagenkopplung der Hauptstandorte Schwerin, Rostock und Neubrandenburg mittels VoIP (z.B. Cisco MC 3810) bzw. Anbindung der TK Anlagen anderer Standorte, die über eine 2 Mbit/s Verbindung ins WAN verfügen;
- Ersatz von TK Anlagen in kleineren Geschäftsstellen durch VoIP Installation (Upgraden von 2500/ 4500 nach 2600/ 3600 - DSS1 Unterstützung für BRI Ports Voraussetzung), dadurch wird unter anderem die Reduzierung der Anschlüsse an das öffentliche Netz möglich, da z.B. AOK internen Sprachverkehr über VoIP übertragen wird.

zum anderen die Schaffung von Wettbewerbsvorteile gegenüber anderen Kassen und Privatversicherern durch:

- breiteres Angebot von Service Leistungen - z.B. Kundenservice über Call Me Button im Internet;
- Integration neuer Dienste, für die VoIP die Grundlage bildet z.B. Messaging.

[43] zu Integrated Services Architecture siehe Kapitel 3.3

7 VoIP im ComLab

Eine Übersicht der im ComLab befindlichen VoIP Hardware bzw. Software und deren VoIP Funktionalität befindet sich in der nachstehenden Tabelle 13.

Hardware	***Funktion***	
	Radvision L2W 323	Gateway / Gatekeeper
	Cisco MC3810*	Multiservice Access Concentrator/ Router; VoIP Funktionalität - Gatekeeper
	Cisco 2611*	Access Router; VoIP Funktionalität - Gateway
	Escort 25 pro	VoIP Client : PCI Karte mit VCON Meeting Point Software
Software		
	Netmeeting 3.01	VoIP Client
	C 65 Workflow	Gatekeeper basierend auf Windows NT 4.0 Server
		Client basierend auf auf Windows NT 4.0 Workstation

Tabelle 13 : VoIP Hard/ Software im ComLab; * - Leihgabe der AOK Rostock

Für die Durchführung von Interoperabilitätstest wurden zusätzlich Picturetel Live 200 ISDN Videokonferenz Clients und eine PC basierte Teles PBX in dieVoIP Umgebung integriert.

7.1 VoIP Integration ins bestehende Netz des ComLabs (LAN/ PSTN)

Im ComLab wurden zwei verschiedene herstellerspezifische (Siemens/ Cisco) Anordnungen realisiert.

- Eine von der Siemens AG vertriebene Lösung, bestehend aus einem ***Radvision L2W 323 Gatekeeper/ Gateway*** mit zwei 10BaseT LAN Ports und zwei BRI ISDN WAN Ports, und auf der Client Seite ***Escort 25 pro Clients*** als PCI Steckkarten mit einer VCON Meeting Point 4.0 Oberfläche.
- Eine Lösung von Cisco, bestehend aus zwei ***MC3810*** (VoIP Gatekeeper) mit je zwei E1 WAN Ports (1 x WAN Trunk, 1 x Digital Voice Port - PBX seitig) und je einem 10BaseT LAN Port, und einem ***Cisco 2611*** Router (VoIP Gateway) mit zwei BRI ISDN WAN Ports und zwei 10BaseT LAN Ports.

In den folgenden Abschnitten wird näher auf Aufbau und Konfiguration der Geräte eingegangen.

7.1.1 Anordnung mit Radvision Gatekeeper/ Gateway

a) physikalisch

Da die BRI ISDN Schnittstellen des L2W - H323 als TE1 Schnittstellen ausgeführt sind, erfordern sie zum Anschluß an ein privates ISDN bzw. an das öffentliche ISDN Netz NT Schnittstellen. Diese werden im ComLab durch die Teles PBX bereitgestellt.

Die Anschlußkonfiguration der Teles stellt sich folgendermaßen dar:

- 4 ISDN Schnittstellen, eine davon konfiguriert als externer Amtsanschluß (Protokoll DSS1; Rufnummer 5193519) mit Amtsholung 0 und drei interne bilinguale (1TR6 und DSS1) Schnittstellen 210, 220, 230 .

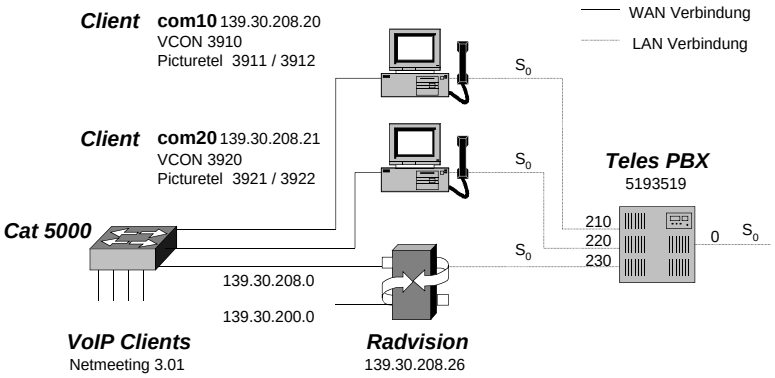

Abbildung 38 : Comlab - Anordnung mit Radvision Gatekeeper/ Gateway physikalisch

Die Ethernet LAN Schnittstellen sind zum einen dem Comlab Subnetz 139.30.208.0 und der Subnetz der Elektrotechnik 139.30.200.0 zugeordnet.

Um unnötige Last zu vermeiden, ist in der Netzkonfiguration darauf zu achten, daß die LAN Schnittstellen nicht als Default Router Interface des Netzwerkes angegeben werden.

b) schematisch

Im Radvision L2W 323 ist die H323 Entity Gatekeeper als auch das Gateway enhalten.

In der Abbildung 39 ist eine Beispielkonfiguration entsprechend der H.323 Funktionalität (GK/ GW, Client) schematisch dargestellt.

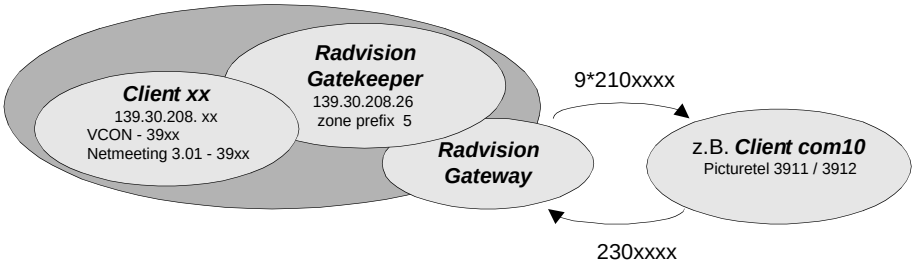

Abbildung 39 : Comlab - Anordnung mit Radvision Gatekeeper/ Gateway schematisch

7.1.1.1 Konfiguration des Radvision Gatekeepers

Dem Radvision Gatekeeper wurde die IP Adresse 139.30.208.26 zugeordnet.
Die Konfiguration des Gatekeeper als auch des Gateways erfolgt über ein GUI. Dieses beinhaltet im GK Konfigurationsmenu die Überschriften der folgenden Unterpunkte.

Service Definition

Es können bis zu 32 Dienste definiert werden, denen unterschiedliche Präfixe zugeordnet werden. Defaultmäßig sind die folgenden Dienste konfiguriert:

BRI Call - Präfix ***90,*** ;
Voice only - Präfix ***9**** ;
Forward - Präfix ***99*** ;
Zone Präfix - Präfix ***5*** .

Zusätzlich können über die Flags ***Public*** bzw. ***Default*** die Nutzbarkeit der Services durch die Endpunkte konfiguriert werden. Endpunkte können statisch - predefined - oder dynamisch bzw. nicht (out of zone) beim Gatekeeper registriert sein - siehe auch Zone Definition.

	Registration		
	static (predefined)	***dynamic only***	***out of zone***
Public	Service mögl., falls als erlaubt konfiguriert	kein Service	Service mögl.
Default	Service mögl., falls als erlaubt konfiguriert	Service mögl.	kein Service

Tabelle 14 : Parameter der Service Definition Table

Bei allen defaultmäßig konfigurierten Diensten sind das Public und das Default Flag gesetzt.

Zone Definition

Alle Endpunkte - Terminals, Gatekeeper, Gateway und MCUs - bilden eine Zone.
Die Definition einer Zone gibt dem Gatekeeper eine bessere Kontrolle über das Management der Endpunkte. Zur Definition einer Zone müssen die Endpunkte erfaßt werden, die sich beim Gatekeeper anmelden dürfen.
Die Definition einer Zone ist jedoch nicht obligatorisch.
Der Radvision Gatekeeper ist derart konfiguriert, daß alle Registration Requests akzeptiert werden.

Neighbor Gatekeeper

Die IP Adressen der Gatekeeper anderer Zonen können über die Konfigurationssoftware erfaßt werden. Wenn ein Call in eine andere Zone gerichtet wird, erfolgt die IP Adreßauflösung durch den entsprechenden Nachbar Gatekeeper.
Es wurden die Gatekeeper IP Adressen von gk1 139.30.208.24 und gk2 192.168.10.1 (GK der MC3810) mit den entprechenden Zone Präfixen - gk1 100 und gk2 200 - konfiguriert.

Network Topology

Die Network Topology Option ermöglicht die Definition von Islands für den Gatekeeper. Ein Island ist ein Cluster von IP „Subnetzen“, die durch homogene und schnelle Videokonferenz LAN Verbindungen charakterisiert sind.
Durch Teilung eines Netzwerkes in Islands kann der Gatekeeper für die Calls eine optimale Verbindung unter Vermeidung von Bottlenecks bzw. langsamen Verbindungen aufbauen.

Der Radvision Gatekeeper im ComLab beschreibt zwei Islands :

E-Technik - 139.30.200.0 Island Code 1

ComLab - 139.30.208.0 Island Code 5

Network Control

Die Network Control Option erlaubt die Einstellung von Netzwerkparameter des GK, wie z.B. das Call Routing, und enthält Informationen zum Netzwerkstatus - Online Enpoints, Ongoing Calls etc..
Die Konfiguration dieser Option im Comlab enthält weitgehend die default Parameter :
jeder kann sich beim GK anmelden; max. Number of Calls = 25 etc.

7.1.1.2 Konfiguration des Radvision Gateways

Im Miscellaneous Parameters Windows lassen sich festlegen:

- die Default Gatekeeper IP - 139.30.208.26 Port 1719
- der Default IP Router - 139.30.208.27
- die Transcoding Priority - das Gateway bietet bevorzugtes Transcoding zw.
  G.711 (WAN) ó G.728 (LAN) und
  G.728 (WAN) ó G.711 (LAN);
  Falls kein Transcoding erfolgen soll - ***Disable*** (ComLab).

Internal IVR Service und Operator - 5193520

Second Number Delimiter - Komma

Konfiguration der LAN Interface

Es werden den LAN Ports des Radvision IP Adresse und entsprechende Netzwerkmasken zugewiesen.

Falls das Gateway an ein einzelnes LAN Segment angeschlossen wird, muß LAN Port 1 genutz werden. Werden mehrere Ports angeschlossen, wird jedem Port an ein anderes LAN Router Segment zugeordnet.

Die Konfiguration der beiden LAN Port ist wie folgt:

1. LAN Port - ComLab : 139.30.208.26 / 255.255.255.224
2. LAN Port - E-Technik : 139.30.200.89 / 255.255.255.0

Konfiguration der WAN Interface

Bei den WAN ISDN Interfaces ist zu beachten, daß diese TE 1 Interface sind und einen NT zur Terminierung benötigen.

Die Tele PBX im ComLab liefert in derzeitiger Konfiguration einen Amtsanschluß und 3 S_0 NT Schnittstellen. Von diesen NT Schnittstellen ist eine (Rufnummer 2300) vom 1. WAN Port des Radvision belegt.

7.1.2 Anordnung mit Cisco Komponenten

a) physikalisch

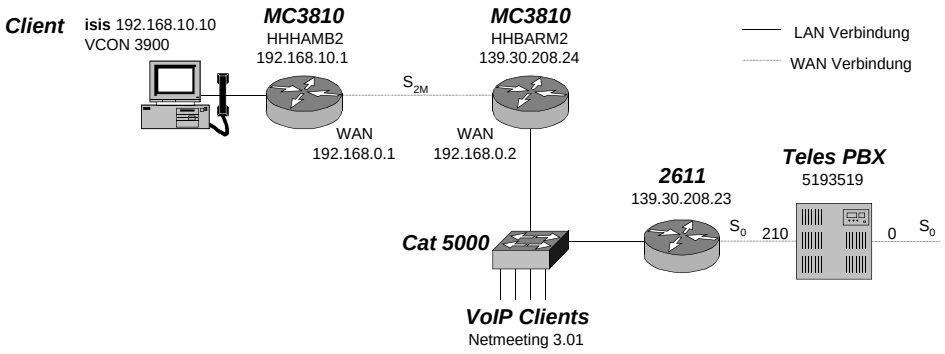

Abbildung 40 : Comlab - Anordnung mit Cisco Komponenten physikalisch

Die MC 3810 verfügen über

- jeweils zwei E1 Schnittstellen - die als MFT - ***Multiflex Trunk Module*** - zum Anschluß an das WAN bzw. als DVM - ***Digital Voice Modul*** - zum Anschluß einer PBX ausgeführt sind,
- je eine 10BaseT Ethernet Schnittstelle und
- eine BRI ISDN Schnittstelle als Daten Back Up Interface.

Über die E1 MFT Trunk Interfaces wurden die beiden MC3810 mittels eines Kreuzkabels back to back verbunden. Diese Verbindung wurde als S_{2M} HDLC Strecke konfiguriert.

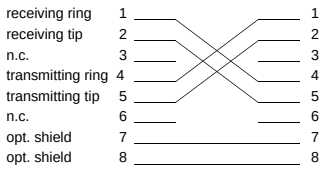

Abbildung 41 : E1 Kreuzkabel Pinout

Konfiguration eines synchronen Netztaktes

Zusätzlich mußte für diese Verbindung ein synchronisierter Takt festgelegt werden. Als Taktquelle kann eine an die E1 DVM angeschlossene PBX, der interne PLL Kreis des MC3810 oder ein über die E1 MFT angeschlossenes Netzwerkgerät dienen.
In der Konfiguration im Comlab wurden der E1 MFT Controller des ***MC3810 HHBARM*** primäre Taktquelle konfiguriert und stellt für den E1 MFT Controller des ***MC3810 HHHAMB2*** den Referenztakt.

Begrenzung der Anzahl der gleichzeitig geführten Gespräche

Die Anzahl der gleichzeitig geführten Gespräche wird durch die von den DSP des VCM - ***Voice Compression Moduls*** - unterstützten Gesamtzahl begrenzt. Jedes VCM enthält 6 DSPs, von denen jeder zwei G.729a Calls oder einen Fax Call unterstützt.
Die digitale Konfiguration im ComLab [44] enthält zwei VCM. Somit können max. 24 G.729a Gespräche gleichzeitig geführt werden.

[44] Die analoge Konfiguration enthält ein VCM und unterstützt daher nur 12 G.729a Calls.

schematisch

In Abbildung 42 ist die Konfiguration schematisch dargestellt. Anders als beim Radvision L2W H323 sind die H.323 Entities Gatekeeper und Gateway im MC3810 - Gatekeeper - und im Cisco 2611 - Gasteway physikalisch getrennt. In beiden MC3810 wurde die Gatekeeper Funktionalität aktiviert und so zwei Zonen mit den Präfixen ***100*** - ***gk1***- und ***200*** - ***gk2*** - geschaffen. Das Gateway - ***gw*** - des Cisco 2611 ist der Zone von gk1 zugeordnet.

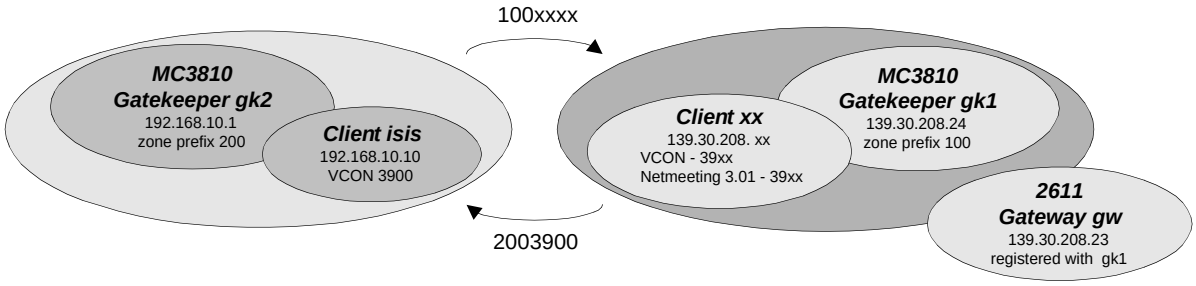

Abbildung 42 : Comlab - Anordnung mit Cisco Komponenten schematisch

7.1.2.1 Cisco MC3810 Konfiguration

Interface Konfiguration

Ethernet

Das Ethernet Interface von ***HHBARM2*** erhielt die IP Adresse :

139.30.208.24 / 255.255.255.224.

IP Routing

Das IP Routing erfolgte statisch - Beispiel ***HHBARM2***:

ip route 192.168.10.0 255.255.255.0 192.168.0.1

E1 MFT Module - E1 Controller und Interface:

Zur Erzeugung eines seriellen Interfaces über die E1 Schnittstelle muß zunächst der E1 Controller konfiguriert werden.

Als Beispiel für die Konfiguration des E1 MFT Moduls ist nachfolgend die des MC3810 ***HHBARM2*** dargestellt.

```
!
controller E1 0
 clock source internal
 channel-group 1 timeslots 1-31
!
....
!
interface Serial0:1
 ip address 192.168.0.2 255.255.255.0
 no ip directed-broadcast
```

```
!
```

Der interne PLL Schaltkreis des MC3810 wurde als Taktquelle konfiguriert.

Es wurde eine Channel Group 1 mit den Timeslots 1-31 der S2M Strecke mit jeweils 64 kbit/s je Timeslot eingerichtet. Dadurch wurde das serielle Interface ***serial interface 0:1*** erzeugt. Diesem konnte nun die IP Adresse 192.168.0.2 / 255.255.255.0 und das Übertragungsformat ***encapsulated HDLC*** zugewiesen werden.

Gatekeeper Konfiguration

Die Aktivierung der Gatekeeperfunktionalität erfolgt Cisco typisch über ***no shutdown***.

Die Konfiguration des Gatekeepers der MC3810, hier am Beispiel von ***HHBARM2***, umfaßt :

- die Definition einer lokalen Zone des Gatekeepers gk1, deren Präfix und Accessibility;
- die Definition der Nachbarzonen der Gatekeeper gk1 (MC3810 ***HHHAMB2***) und ***ComLab1*** (Radvision L2W - 323) und deren Präfixe.

```
!
gatekeeper
 zone local gk1 comlab.uni-rostock.de
 zone remote gk2 comlab.uni-rostock.de 192.168.10.1 1719
 zone remote ComLab1 comlab.uni-rostock.de 139.30.208.26 1719
 zone access gk1 default direct
 zone prefix gk1 100*
 zone prefix gk2 200*
 zone prefix ComLab1 5*
 no shutdown
!
```

7.1.2.2 Cisco 2611 Konfiguration

Interface Konfiguration

Ethernet Interface

Das Ethernet Interface erhielt die IP Adresse 139.30.208.23 .

```
ip address 139.30.208.23 255.255.255.224
```

ISDN Interface

Der Cisco 2611 im Comlab besitz ein VNM Voice Network Module, das zwei VIC - Voice Interface Cards - aufnehmen kann und im Slot 1 mit einer BRI - VIC (VIC-2BRI-S/T-TE - enthält 2 BRI Ports) belegt war.

Bei der Belegung beider Slots ist zu beachten, daß bei bestimmten Kombinationen von VICs nicht alle Ports genutzt werden können - siehe auch die Cisco Dokumentation zum 2600.

Das ISDN BRI Interface 1/0 (Slot 1 Port 0) wurde an die TELES PBX angeschlossen und konfiguriert. Da nicht DSS1 sondern lediglich 1TR6 vom Router unterstütz wird, wurde die NT Ports der PBX bilingual eingerichtet.
Nach der globalen ISDN Switch Type Konfiguration - `isdn switch type 1tr6` - die der Switch Type Konfiguration des Service Providers bzw. im Comlab der des NT Anschlusses ent-spricht, erfolgte die allgmeine Konfiguration der Interfaces - Deaktivierung einer mögl IP Adresse etc..

```
!
interface BRI1/0
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
...
```

Optional kann in der Interface Konfiguration der ISDN Switch Type festgelegt werden, der die globale Switch Type Konfiguration überschreibt.
Mit den nachfolgenden Konfigurationszeilen wird das Port für eingehende Voice Calls mit einer Bandbreite von 64 kbits/s bzw. die Sendung von ***Alert*** und ***Sending - Complete*** Meldungen eingerichtet.

```
...
 isdn switch-type basic-1tr6
 isdn incoming-voice modem 64
 isdn send-alerting
 isdn sending-complete
!
```

Gateway Konfiguration

Als H.323 Interface des Gateways kann nur das Loopback Interface oder das Interface, das mit dem Gatekeeper verbunden ist, definiert werden.
Das Interface ***Ethernet 0*** führt zum Gatekeeper ***gk1*** und wurde als H.323 Interface des Cisco 2611 definiert.
Der Gatekeeper ***gk1*** wurde für das Gateway direkt konfiguriert. Der H.323 ID des Gateways lautet ***gw***. Dieser ID wird in der Kommunikation zwischen Gateway und Gatekeeper genutzt.

```
gateway
 !
 interface Ethernet0/0
 ip address 139.30.208.23 255.255.255.224
 no ip directed-broadcast
 no ip route-cache
```

```
 no ip mroute-cache
 no cdp enable
 h323-gateway voip interface
 h323-gateway voip id gk1 ipaddr 139.30.208.24 1719
 h323-gateway voip h323-id gw
 h323-gateway voip tech-prefix 10#
!
```

Der Technologie Präfix technology prefix ***10#*** wird zur Identifikation der durch das Gateway angebotenen Dienste genutzt.

Dial Peer Konfiguration

Über Dial Peers - POTS bzw. VoIP - werden die Rufziele näher definiert.

a) POTS Dial Peer - LAN ⇒ POTS

Eine POTS Dial Peer definiert das Voice Port, zu dem VoIP Calls weitergeleitet werden bzw. welches Technologie Präfix der Ziel Telefonnummer hinzugefügt werden muß.

```
dial-peer voice 1 pots
 incoming called-number 10#220
 answer-address 10#*220
 destination-pattern 10#*220....
 direct-inward-dial
 port 1/0/0
 no register e164
```

b) VoIP Dial Peer - POTS ⇒ LAN

DieVoIP Dial Peer legt fest, wie ein auf einem lokalen Voice Port ankommender Call in die VoIP Cloud zum Ziel weitergeleitet wird.

```
dial-peer voice 2 voip
 incoming called-number 230
 answer-address 230
 destination-pattern 230....
 signal-type ext-signal
 session target ras
```

Die letzte Zeile der Konfiguration - `session target ras` - legt fest, daß ein Gatekeeper die Adressauflösung von E.164 zu IP Adresse übernimmt.

Test der Konfiguration

Mit dieser Konfiguration war ein Verbindungsaufbau zu einem an die Teles PBX angeschlos-

senes ISDN Telefon möglich, wie im Trace im Anhang D.1 dargestellt, jedoch erfolgte keine Sprachübertragung.
Der Grund dafür konnte im Zeitraum der Diplomarbeit nicht festgestellt werden.

7.2 Testszenario im Comlab

Zur Funktionsüberprüfung der im vorigen Kapitel beschriebenen Konfigurationen wurden mehrere Tests durchgeführt, die in den folgenden Unterpunkten beschrieben werden.

7.2.1 Monitoring eines Point to Point Call

Die folgenden Traces wurden während eines Point to Point Calls zwischen den Escort 25 Clients Com10 und Com20 aufgenommen.

Beide Clients sind dabei beim Radvision Gatekeeper 139.30.208.26 registriert. Dieser übernimmt für den Fall a) das Call Routing - indirect Call Routing.
Im den Fall b) sind die Endpunkte Com10 und Com20 für das Call Routing selbst verantwortlich.

a) com20 /VCON ⇒ com10 /VCON indirect Call Routing (über GK)

```
< GK:  _____________________________________________________________block 279
[50673285]  >
< GK:  eventNewCall [50673285]  >
< GK:  admission request (origin) from 139.30.208.20:1719. endpoint=1 [50673285]  >
< GK:  sending admission confirm for call  0 [50673286]  >
< GK:  setup received - Offering on call  0 [50673290]  >
< GK:  gk sending setup to destination. Present parameters of cal: 0 [50673290] >
< GK:   No. From                 To                              State    Service
[50673290]>
< GK:   --- ----                 --                              -----    -----
[50673291]>
< GK:   0   139.30.208.20:1044   139.30.208.21:1720  ,3900       CAL_HUNTING
[50673291]>
< GK:  admission request (destination) from 139.30.208.21:1719. endpoint=2
[50673310]  >
< GK:  sending admission confirm for call  0 [50673311]  >
< GK:  destination connect for call 0 [50674086]  >
< GK:  origin connect for call 0 [50674087]  >
< GK:  Call is formed  0 [50674087]  >
< lg: [4:TOUT ID2] [50674494]  >
```

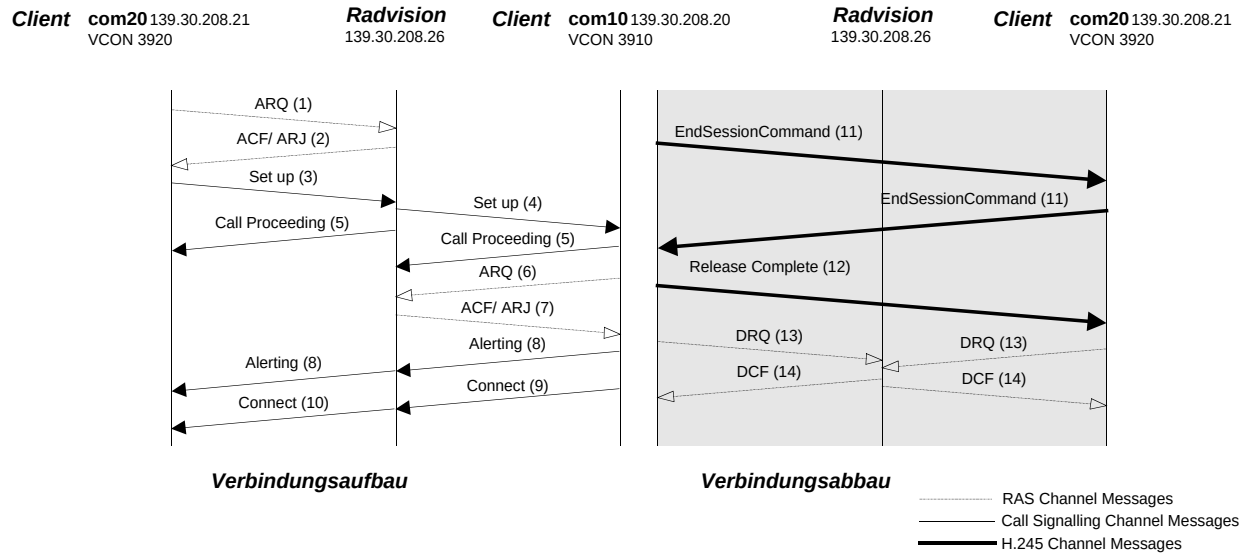

Abbildung 43 : Verbindungsauf- und abbau direct call routing [H.323]

auflegen von com 10

```
< GK:  disconnecting call  0 [50688354]  >
< GK:  _____________________________________________________________block 280
[50688357]  >
< GK:  disengage request from 139.30.208.21:1719 - destination of call 0. endpoint=2
[50688357]  >
< GK:  DCF for call 0 [50688357]  >
< GK:  _____________________________________________________________block 281
[50688363]  >
< GK:  disengage request from 139.30.208.20:1719 - origin of call 0. endpoint=1
[50688363]  >
< GK:  DCF for call 0 [50688363]  >
< GK:  clearing call  0 [50688363]  >
```

b) com20 /VCON ⇒ com10 /VCON direct Call Routing

```
< GK:  _____________________________________________________________block 12
[37394]  >
< GK:  eventNewCall [37394]  >
< GK:  admission request (origin) from 139.30.208.20:1719. endpoint=1 [37394]  >
< GK:  sending admission confirm for call  0 [37395]  >
< GK:  _____________________________________________________________block 13
[37399]  >
< GK:  eventNewCall [37399]  >
< GK:  admission request (destination) from 139.30.208.21:1719. endpoint=2 [37399]
>
< GK:  sending admission confirm for call  0 [37399]  >
```

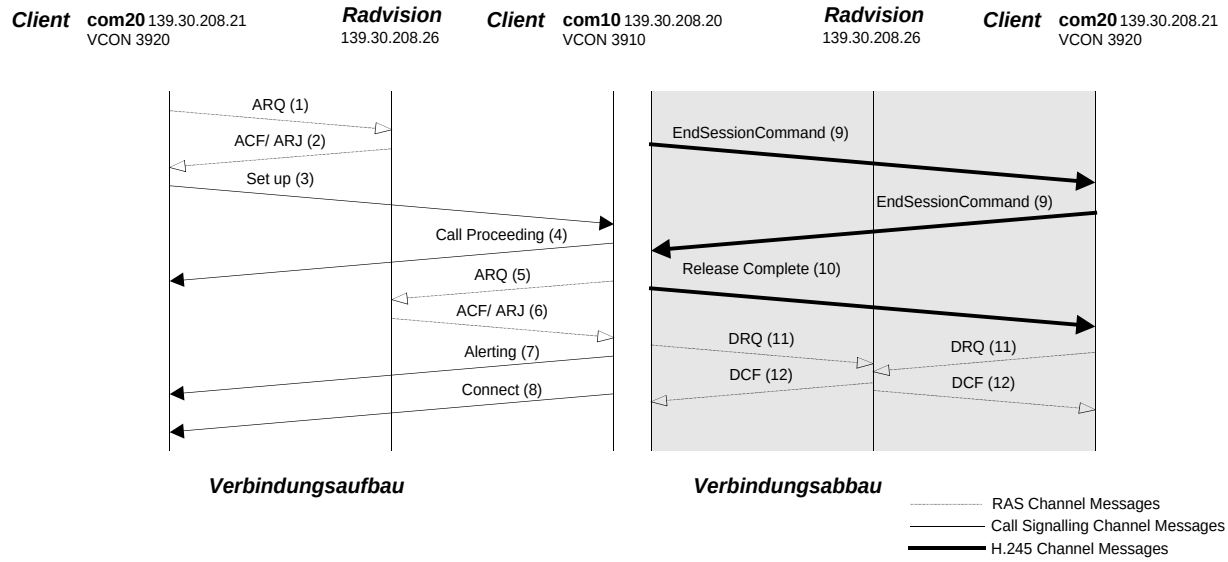

Abbildung 44 : Verbindungsauf- und abbau direct call routing [H.323]

auflegen von com 10

```
< GK:  _____________________________________________________________block 14
[42267]  >
< GK:  disengage request from 139.30.208.21:1719 - destination of call 0. endpoint=2
[42267]>
< GK:  DCF for call 0 [42267]  >
< GK:  _____________________________________________________________block 15
[42273]  >
< GK:  disengage request from 139.30.208.20:1719 - origin of call 0. endpoint=1
[42273]  >
< GK:  DCF for call 0 [42273]  >
< GK:  clearing call  0 [42274]  >
```

Die Trace entsprechen der Ausgabe des Radvision Gatekeepers und beinhalten nicht alle Phasen der Kommunikation detailliert. Es werden hauptsächlich RAS Meldungen und verallgemeinernde Meldungen, wie Setup und Connect angezeigt.

Für die detaillierte Betrachtung aller Kommunkationsschritte (RAS, Q.931, H.245 etc.) ist ein Protokollanalyzer notwendig.
Dazu stand im ComLab eine 45 Tage Evaluation Version des ***Fireberd DNA H.323 Protocol-analyzers*** der Firma TTC (www.ttc.com) zur Verfügung.

<u>Probleme</u>

Versuche, Verbindungen zwischen Netmeeting 3.01 Clients über ***indirektes Call Routing*** aufzubauen, führten nicht zum Erfolg.

Ursache dafür war das Fehlen der ***srcCallSignalAddress*** (Call Signalisierungadresse der Quelle) in der ***ARQ*** Nachricht vom Netmeeting Client zum Gatekeeper, wie eine Analyse mit dem Protocolanalyzer bestätigte (siehe auch dazu den GK Trace in Anhang D.2). Verbindungsversuche zwischen Netmeeting 3.01 Clients über ***direktes Call Routing*** waren dagegen erfolgreich.

7.2.2 Interoperabititätstest

Es wurde untersucht, ob und wie Verbindungsanforderungen zwischen den Produkten der Hersteller bearbeitet werden, und der Verbindungsauf- und -abbau zwischen den Zonen des Radvision GK und eines Cisco GK untersucht.

a) bes/ netmeeting ⇔ com20/ VCON indirect call routing (über GK)
Ein Verbindungsversuch vom Netmeeting 3.01 Client zum Vcon Client war erfolgreich - jedoch mit der Einschränkung, daß wiederum die ***srcCallSignalAddress*** von der Netmeeting Seite fehlte. Da aber die ***ARQ*** Nachricht des Vcon Client eine ***destCallSignallAddress*** enthält, konnte dennoch eine Verbindung aufgebaut werden (Trace siehe Anhang D 3. a)).

Als Ursache für dieses Problem und der im Kapitel 7.2.1 angesprochenen, werden Inkompatibilitäten zwischen H.225 Version1 (Vcon, Radvision) und H.225 Version2 (Netmeeting 3.01) vermutet.

b) amun-re/ gk1 ⇒ com 20/ radv (Kommunikation über zwei Zonen)

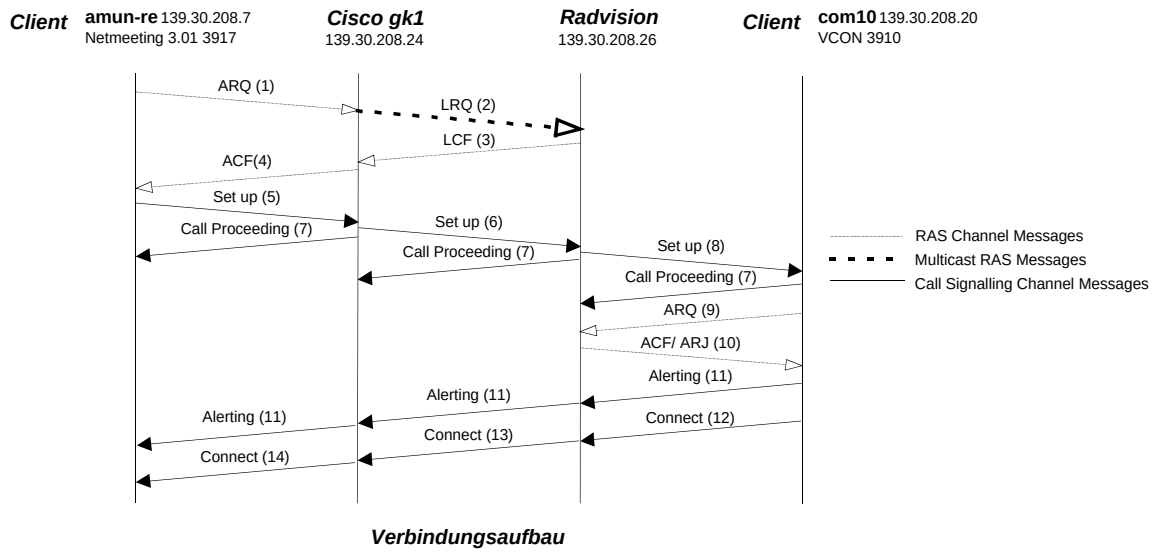

Abbildung 45 : Kommunikation über zwei Zonen [H.323]

Wenn ein Verbindungsaufbau über mehre Zonen erfolgt - die Endpunkte bei verschiedenen GK registriert sind - wird über eine ***LRQ Multicast*** Nachricht der für die Zielendpunkt zuständige GK ermittel. Dieser sendet in der ***LCF*** Nachricht seine ***Call Signalling Channel Transport Adresse***, die vom GK des Senders zur Übertragung des Setups genutzt wird. Da-nach erfolgt der Verbindungsaufbau nach dem in Abbildung 46 dargestellten Schema.

In Anhang D 3. b) ist die Ausgabe des Radvision GK während der Verbindung dokumentiert.

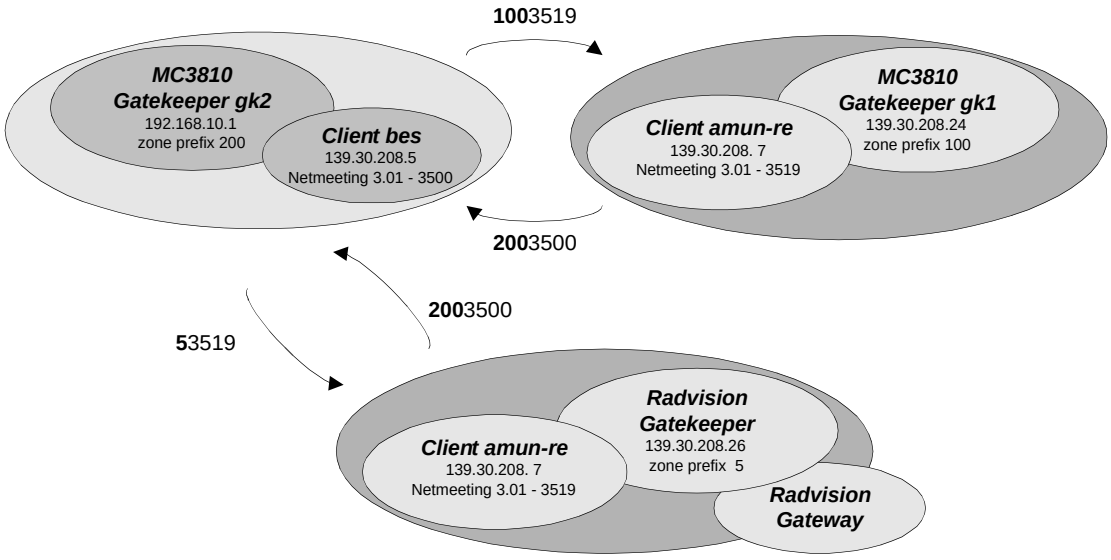

Abbildung 46 : Interoperabilität der Produkte im Comlab

7.2.3 Interworking Test

Im Interworking Test wurde die Kommunikation zum Verbindungsauf bzw. abbau zwischen VoIP Clients und ISDN Clients über den GW/ GK untersucht
Der Anhang D.4 enthält den Trace eines erfolgreichen Verbindungsauf- und -abbaus von einem Picturetel Live 200 ISDN Client (Com 10) zu einem Netmeeting 3.01 Client (Bes).

7.3 Nutzung der VoIP Installation im ComLab

Die im ComLab verbleibende VoIP Ausrüstung bestehend aus der in Kapitel 7.1.1 beschriebenen Umgebung des Radvision L2W 323, kann im weiteren genutzt werden zur :

- studentischen Ausbildung, durch Ausarbeitung eines VoIP Praktikumversuches (z.B. Erweiterung des ISDN Praktikums mit der FH Wismar um ein VoIP Praktikum);

- Präsentation von VoIP als alternative Kommunikationsplattform für interessierte Unternehmen etc..

Zusätzlich zum beschriebenen Aufbau kann eine RC 3000 Umgebung in Verbindung mit der im ComLab vorhandenen Hicom 300 als Beispiel für eine den unternehmensspezifischen Workflow unterstützende VoIP Lösung. realisiert werden.
Im Rahmen dieser Diplomarbeit war die Installation einer deratigen Umgebung aus zeitlichen und technische Gründen nicht möglich.

8 Zusammenfassung und Ausblick

Die Entwicklung von Voice over IP als isochroner Dienst über Datennetzwerke ist durch die Standardisierung als ITU - T H.323 Empfehlung und der breiten Unterstützung dieses Standards in der Hard- und Softwareindustrie, soweit fortgeschritten, daß VoIP auch im kommerziellen Umfeld eingesetzt wird.
VoIP kann entweder als integraler Bestandteil der Kommunikationslösung neben herkömmlicher Telefonie oder als Alternative betrachtet werden.
Der Einsatz von VoIP eignet sich vor allem für Unternehmen mit einem hohen Potential an integrierter Kommunikation (Sprache und Daten). Zukünftig werden neue Dienste mit starker Daten Sprach Integration, die auf dem VoIP Transportdienst aufbauen (z.B. Messaging - Verbindung Voice Mail Fax), eine immer größere Bedeutung erlangen.
Der Einsatz von VoIP als bloßer Transportdienst von Sprache wird dabei in den Hintergrund gedrängt (auch wegen der durch den anhaltenden Preiskampf auf dem Telefonmarkt fallenden Preise), bildet aber die technische Grundlage für die neuen Mehrwertdienste.
Unter dem technischem Gesichtspunkt sind Firmen mit bestehendem Routernetz für Einsatz von VoIP prädestiniert, da die VoIP Funktionalität über Upgrades der Soft - bzw. Hardware realisiert werden kann. Dies wurde im Rahmen dieser Diplomarbeit am Beispiel des strukturierten Routernetzes der AOK Mecklenburg - Vorpommern dargestellt.
Voraussetzung für die Implememtierung von VoIP ist die Bereitstellung eines CoS/ QoS in der WAN/ LAN Struktur zur Übertragung zeitkritischer Daten durch Einführung von Priorisierungsmechanismen, Queueing Methoden bzw. Methoden zur Bandbreitenreservierung.
Zukünftige Transportnetze werden von Ansätzen wie z.B. IP over Sonet/ SDH, die versuchen die komplexe Schichtung der heutigen Protokollwelt unter Beibehaltung der Struktur höherer Netzwerkschichten zu vereinfachen[45], profitieren und eventuell Prioriserungsmechanismen in Backbonebereich unnötig werden lassen. Im Access Bereich werden diese jedoch ihre Berechtigung behalten.
Eine Aufgabe die sich aus der Integration von Sprache und Daten ergibt und die es zu lösen gilt, ist die Kontrolle, Steuerung und Verwaltung von Sprach- und Datenverkehr über ein Netz-werk- bzw. Systemmanagement.

[45] Dazu werden immer mehr Funktionen in die WDM Ebene integriert, so daß der Verkehr höherer Netzwerkschichten mit minimalem Overhead direkt darüber übertragen werden kann.

Quellenverzeichnis

[AS] **Cisco Network Access System**
Cisco Systems Inc., http://www.cisco.com

[Aran99] **Designing VoIP Networks;**
G.Arantavicz; Powerpoint Präsentation; Cisco Systems 1999

[Beam98] **A Primer on the H.323 Series Standard**;
DataBeam Corp., http://www.databeam.com

[Cama98] **IP Telephony Gateways;**
G. Camarillo; Royal Institute of Technology Stockholm 1998

[Cisco99] **Cisco Multiservice Networking**
Cisco Systems Inc., http://www.cisco.com

[ctcd98] **c'thema 01 Netzwerke;**
CDROM, Heise Verlag 1998

[Data99] **Datacom online Lexikon;**
http://www.datacom-bookstore.de/lexikon

[Detk98] **ATM in TCP/ IP-Netzen;**
K.-O. Detken; Hüthig Verlag 1998

[Dekt99] **ATM, GE, IP und SDH;**
K.-O.Detken; Optinet GmbH 1999 (Powerpoint Präsetation)

[From95] **Aspekte der Echtzeitkommunikation über Rechnernetze;**
M.Fromme; Universität Hannover 1995

[Flatt98] **Neuer Schwung für alte Technik;**
F.Flatten; gateway 12/98 S.88 ff.

[Good98] **Planung vor dem Sprachtransport via IP;**
R.Goodwind; http://cockoeln.koezn.siemens.de/Fachaufsätze/vmw50022.htm

Sprachübertragung in Netzen - Die Technologie;
R.Goodwind; http://cockoeln.koezn.siemens.de/Fachaufsätze/vmw50023.htm

[H.225.0] **Call Signalling Protocol ans Media Stream Packetization for Packet Band Multimedia Communication Systems;**
ITU-T Recommondation; Version 2 1997

[H.245] **Control Protocol For Multimedia Communication;**
ITU-T Recommondation; Version 3 1998

[H.323] **Packet-Based Multimedia Communication Systems;**
ITU-T Recommondation; Version 2 1997

[H.450.1] **Generic Functional Protocol for the Support of Supplementary Services in H.323;**
ITU-T Recommondation; 1997

[H.450.2] **Call Transfer Supplementary Service for H.323;**
ITU-T Recommondation; 1997

[H.450.3] **Call Diversion Supplementary Service for H.323;**
ITU-T Recommondation; 1997

[HiNet 1] **H.323 Gateway for HiNet RC3000;**
Datenblatt, Siemens AG 1999

[HiNet 2] **HiNet IP Communication;**
Powerpoint Präsentation, Siemens AG 1999

[Hohg3/99] **Voice over IP revolutioniert die TK Landschaft**;
B.Hohgräfe, C.-S. Michalik; datacom 3/99 S.66 ff

[IBM98] **Voice Data Solution;**
http://www.ibm.com

[Indu96] **Real Time Data Communication in Computer Networks;**
A.S.Induruwa; University of Moratuwa, Sri Lanka 1997

[Intel99] **Differentiated Services - Moving towards QoS on the Ethernet;**
http://www.intel.com

[iX1/00] **Europa mit IPv6 Ambitionen;**
iX 1/2000; Heise Verlag

[Klein98] **Untersuchung von Möglichkeiten zur Substitution von konventionellen PBX-Anlagen durch alternative Telefon-/ Multimedia Systeme;**
E.Klein; Diplomarbeit FH Hamburg 1998

[Kuri99] **Sprache in Päckchen;**
J. Kuri, c't 10/99 S.228 ff; Heise Verlag

[Lang98] **Hicom Workflow;**
Langer; VKD SV CoC Siemens AG 1999

[Loch95] **Digitale Nachrichtentechnik;**
D. Lochmann; Verlag Technik Berlin 1995

[LP] **IP Telefon HiNet LP 5100;**
J.Briskorn, Powerpoint Präsentation, Siemens AG 1998

[MC3810] **Datenblatt Cisco MC3810**
Cisco Systems Inc., http://www.cisco.com

[Mino98] **Delivering Voice over IP Networks;**
D.Minoli, E.Minoli; Wiley Computer Publishing 1998

[Nisp99] **Layer 4 Switching und Quality of Service - Ein Fall für Vier;**
M.Nispel; iX 10/99; Heise Verlag

[Polte98] **Perspektiven von Voice over IP**;
T. Polte; http://cockoeln.koezn.siemens.de/Fachaufsätze/vmw50015.htm

[RFC 1889] **RTP: A Transport Protocol for Real Time Application;**
RFC 1889, 1996

[RFC 2354] **Options for Repair of Streaming Media;**
RFC 2354, 1998

[RFC 2460] **Internet Protocol, Version 6 (IPv6) Specification;**
RFC 2460, 1996

[Schu98] **Sprachregeln für IP - Netze;**
W.Schulte; gateway 12/98 S.100 ff.

[Schul99] **H.323 vs. SIP Telephony;**
H. Schulzrinne; http://www.cs.columbia.edu/~hgs7sip

[Telo98] **Migration Large Scale Voice Systems to Internet Telephony;** T. Flanagan; Powerpoint Präsentation 1999,Telogy Networks Inc.1999, http://www.telogy.com

[Timm98] **Fehlererkennung und -behandlung;** *Prof. Dr. G. Timmer*; FH Osnabrück, http://gtsun.et.fh-osnabrueck.de/lehre/kommunikationsnetze/kn-script

[Xpress] **Hicom Xpress: Kundenspezif. Integration aller Kommunikationsmedien;** Datenblatt, Siemens Schweiz AG

Anhang A

A.1 Eignung von LAN Technologien zur Übertragung von Real Time Daten - Kapitel 3

LAN - Technologie	
Tokenring/ Tokenbus IEEE 802.5 IEEE 802.4	– deterministisches Zugriffsverfahren – 8 Prioritäten (6 für Datenübertragung) – keine Instanzen zur Bandbreitenreservierung , Zugangskontrolle über externen Server - keine Bandbreitenüberwachung – Berücksichtigung der Leistungsfähig-keit der Brücken und Transit Netze, wenn Verkehr lokalen Ring verläßt
FDDI ANSI X3T9.5	– hohe Bandbreite – große Pakete – shared Media
FDDI II	– in Def. Übertragung von echtzeitf. synchronenVerkehr vorgesehen – keine Bandbreitenreservierung – synchroner Mode zur Übertragung isochroner Daten nicht überall implementiert
Ethernet shared Media IEEE 802.3	– stochastisches Zugriffsverfahren (CSMA/CD) – nicht vorhersagbare Verzögerung nach Kollision durch binary exponetial backoff – realtime Übertragung nur auf wenig belasteten Strecken
geswitched 10/100Mbit/s IEEE 802.3i IEEE 802.3u	– bessere Ausnutzung der Bandbreite – Zugriffsverfahren spielt untergeordnete Rolle – keine Prioritätsmechanismen – bei hoher Belastung nimmt Queueing Delay zu – Mechanismen zur Datenpriorisierung müssen implementiert werden
Gigabit Ethernet IEEE 802.3z	– hohe Bandbreite, einfache Migration – keine Prioriätmechanismen – Mechanismen zur Datenpriorisierung müssen implementiert werden
ATM - LAN ITU I.121 ATM Forum	– in Def. Echtzeitdatenübertragung berücksichtigt – AAL 1, AAL 2 für LAN nicht definiert, AAL-Typ 5[46] wird eingesetzt – hohe Implementierungskosten
Frame Relay ITU I.121 ITU I.122	– verbindungsorientierte Packet Switching Technologie (56kbit/s - 45 Mbit/s) – Auftreten von Jitter/ Verzögerungen aufgrund variabler Framelänge(max 1608 byte) – spezielle Hardware für Sprachübertragung erforderlich (siehe VoFR)

Tabelle 15 : LAN Technologien im Überblick [Fromme 95 Uni Hannover]

Ethernet	10Mbit/s	100Mbit/s	1000Mbit/s
Übertragungslänge	10BaseT bis 100m 10BaseFx bis 1000m	100BaseT bis 100m 100BaseFx bis 412m	1000BaseCx bis 25m 1000BaseSx bis 220m 1000BaseLx bis 5000m

Tabelle 16 : Übertragungslängen im Ethernet [Kauffels97],[Jörg Rech ctcd]

[46] AAL 1 verbindungsorientiert, konst. Bitrate, Zeitkompensierung zw. Quelle und Senke erforderlich;
AAL 2 verbindungsorientiert, var. Bitrate, Zeitkompensierung zw. Quelle und Senke erforderlich;

AAL 5 verbindungslos/ verbindungsorientiert, var. Bitrate , keine Zeitkompensierung erforderlich [Detken 98]

A.2 RTP Definitionen - Kapitel 4.3.2

Bezeichnung	***Funktion***
RTP Payload	Nutzdaten eines RTP Paketes (z.B. Audio Samples, komprimiertes Video)
RTP Paket	besteht aus fixem Header (siehe Tabelle 18; Abb. 25), einer möglicherweise leeren Liste von contributing sources (siehe CSCR) und der Payload; ein RTP Paket ist in eine Paket des darunter liegenden Protokolls (z.B. UDP) eingebettet, jedoch sind auch mehre Pakete bei entsprechenden Kapselungsmethoden möglich
RTCP Paket	besteht aus fixem Header (ähnlich RTP) gefolgt von Elementen entsprechend dem RTCP Pakettyp; durch das Length Feld im Header ist es möglich mehrere RTCP Paket innerhalb eins Paketes des darunter liegenden Protokolls zu übertragen
Port	Abstraktion des Transportprotokolls, um verschiedene Ziele innerhalb eines Host Computers zu unterscheiden; RTP verläßt sich auf die Implementierung dieser Funktion in unteren Protokollschichten[47]
Transport Adresse	Kombination einer Netzwerkadressen und eines Ports (z.B. IP Adresse und UDP Port); Pakete werden von einer Sende Transport Adresse zu einer Empfangs Transport Adresse übertragen
RTP Session	RTP Verkehr innerhalb einer Gruppe Teilnehmern; jede Session ist durch spez. Empfängertransport Adressen Paar gekennzeichnet (IP Adresse + Port für RTP und RTCP); Unicast und Multicasts sind möglich; innerhalb von Multimedia Sessions hat jedes Medium seine eigene RTP Session inclusive eigener RTCP Pakete
Synchronization Source (SSCR)	durch 32 bit Identifier[48] (siehe Abb.25) bezeichnete Quelle von RTP Paketen; Pakete einer SSRC bilden einen gemeinsamen Timing und Sequenznummern Bereich; Empfänger kann daher die Pakete entsprechend der SSRC für die Wiedergabe gruppieren; innerhalb der Übertragung kann die SSRC das Datenformat (z.B. Audio Encoding) wechseln
Contributing Source (CSRC)	Quelle , die durch einen RTP Mixer aus anderen kombiniert wird; Mixer fügt Liste (CSRC Liste) der beteiligten Einzelquellen in Header ein (siehe Abb.25); Beispiel : Audio Konferenz bei der der Mixer das Audiosignal der aktiven Sprecher kennzeichnet, so daß der Empfänger den aktiven Sprecher erkennen kann, obwohl alle Pakete den SSRC des Mixers enthalten
End System	Applikation als Quelle und Senke des Inhalts der zu übertragenden RTP Pakete; kann als eine (typisch) oder mehrere SSRC agieren

[47] wird zum Multiplexen von RTP und RTCP Paket innerhalb einer Session genutzt

[48] eine von der Netzwerkadresse unabhängige Bezeichnung der Quelle; Identifier ist eine in einer Session einmalige Zufallszahl

Bezeichnung (fortgesetzt)	***Funktion (fortgesetzt)***
Mixer	Zwischensystem zur Kombination von RTP Paketströmen, dabei ist die Änderung des Datenformats möglich; Synchronisation mehrerer SSRC (Anpassung des Timings innerhalb der Datenströme, Generierung und Weitersendung mit Mixer eigenem Timing - daher SSRC des Mixer in weitergesendeten Paketen enthalten)
Translator	Zwischensystem zum Formatkonvertierung (keine Änderung des SSRC)
Monitor	Empfang von RTCP Paketen und Bestimmung des QoS, Fehler Diagnose und Langzeitstatistiken; kann in Appl. enthalten sein oder als eigenständige Appl. (Third Party Monitors)
Non RTP Means	Protokolle und Mechanismen zusätzlich zu RTP (z.B. zur Verschlüsselung einer Session)

Tabelle 17 : RTP Definitionen [RFC 1889]

Feldbezeichnung	***Funktion***
V	2 bits; bezeichnet Version = 2 [RFC 1889], = 1 [Draft RTP], = 0 [Protokoll in vat Audio Tool]
P	1 bit; wird gesetzt, falls Paket ein oder mehrere padding Oktets enthält
X	1 bit; wird gesetzt, falls Header eine Header Extension folgt (erlaubt individuelle Implementierung experimenteller Funktionen)
CC	4 bits CSRC Count; enthält Anzahl der CSRC Identifier, die Header folgen
M	1 bit Marker; durch entsprechendes Profile definiert; Kennzeichnung von Rahmen-grenzen
Payload Type	7bit; bezeichnet Payload Typ und bestimmt dessen Interpretation durch die Applikation; Profil definiert Mapping von Payload Type Codes zu Payload Formats; dynamische Def. zusätzl. Payload Type Codes durch Non RTP Means
Sequence Number	16 bit; inkrementieren um 1 durch jedes RTP Paket; Nutzung vom Empfänger zur Erkennung von Paket Verlusten und zur Wiederherstellung einer Paket Sequenz; Anfangswert zufällig, um Plain Text Angriffe zu erschweren
Timestamp	32 bit; Anfangswert zufällig (weitere Informationen siehe RFC S.10/11)
SSRC Identifier	32 bit; wird zufällig gewählt und muß innerhalb einer Session eindeutig sein; falls Identifier nicht eindeutig müssen RTP Appl. Kollisionen erkennen und lösen können
CSRC Identifier	Anzahl: 0 - 15 je 32 bit; bezeichnen die CSRC für die Payload des jeweiligen Paketes ; Anzahl in CC Feld

Tabelle 18 : Beschreibung der Felder eines RTP Headers [RFC 1889]

Anhang B

B.1 Roadmap der Siemens HiNet RC 3000 Produktfamilie

HiNet RC 3000				
E/98 Rel.1.0	***5/99 „Kilauea“***	***8/99 „Stromboli“***	***Q1/00 „Pinatubo“***	***Q4/00 „Askja“***
• Basic System • PC Client • System Management	• Implementation of Customer Feedback – direct Inward Dialing to user – Import to pers. Address-book – Improvement of Client GUI Handling	• Enhancements to Basic System / Client/ System Management – Messaging – Teleworking based on G.723 (RAS) – Enhanced Forwarding – Central Address Book – Support of H.323 V2 – Support of LP 5100 – Support of Multimedia keyboard with hookswitch contact	• Enhancements to Basic System/ Client – Support of H.450 – Add. Telephony Featu-res – Conferencing – Communication Circle – API (JTAPI/ TAPI/ CSTA) – Security – Multi Zones	• Enhancements to all Components e.g. for Basic System Video
• BRI Gateway - Radvision		• PRI Gateway	• Gateway Siemens	
• Languages (Client) – Am. English – German		• new Appl. – Call Center (ACD) • Add. Languages – Brit. English – Spanish – Italian – French	• new Appl. – Billing & Accounting – Unified Messaging – Resource Manager	• new Appl. – LCR – Mobility – SDK
• up to 50 users		• up to 200 users	• more than 200 users	

Tabelle 19 : Roadmap der Siemens HiNet RC 3000 Familie [Siemens RC3000]

B.2 Hersteller von Gatekeeper[49]

Anbieter	*Produkt*	*OS*	*H.323*	*Bandwidth Control*	*LCR*	*Directory Service*
Cisco Systems	MC3810	--	Y	--	--	--
Elemedia www.elemedia.com	H.323 Gatekeeper GK2000S	Solaris/Win NT	Version 2	Y	--	Y
ECI Telecom www.ecitele.com	I-Keeper 120	Win NT	Y	Y	Y	--
	I-Keeper 180	Win NT	Y	Y	Y	--
	I-Keeper 1000	Win NT	Y	Y	Y	--
Ericsson www.ericsson.com	The H.323 Gatekeeper	Win NT, Unix	Version 2	Y	Y	Y
NeTrue www.netrue.com	IPT BackOffice	Win NT, Unix	Version 2	Y	Y	Y
NetSpeak www.netspeak.com	NetSpeak Gatekeeper	Win NT with Service Pack 4	Version 2	Y	Y	N
Nortel www.nortel.com	IPConnect Gatekeeper	Win NT, Unix	Version 2	--	--	Y
Quescom www.qescom.com	QWare GateKeeper	Win NT	Y	--	Y	--
Radvision www.radvision.com	L2WH.323[50]	Windows	Y	Y	--	Y
VocalTec www.vocaltec.com	VocalTec Gatekeeper	Win NT	Version 2	--	Y	Y

Tabelle 20: VoIP Gatekeeper Anbieter [voip.org]

[49] Die in den folgenden Tabellen aufgeführten Hersteller sind beispielhaft aufgeführt. Ausschlaggeben für die Aufnahme in die Tabellen waren eindeutige Aussagen der Hersteller zum H.323 Kompatibilität. Weitere Hersteller sind unter http://www.voip.org aufgeführt.

[50] ist in Siemens C65 Workflow Lösung integriert siehe Kapitel 5.1

B.3 Hersteller von Gateways

Hersteller	*Produkt*	*OS*	*H.323*	*Ports*	*Fax Support*
1World Connect	Gateway	Win NT	Y	Up to 48	Y
3Com	Total Control	--	Y	48 - 672	N
8x8	Symphony Gateway	--	Y	4	--
ACT Networks	ServiceXchange	--	Y	Up to 120	Y
ArelNet	i-Tone	Win NT	Y	Up to 6000	Y
Array Telecom	Series 3000	Win NT	Y	--	Y
Ascend	MultiVoice for the MAX	Win NT	Y	Up to 672	--
Cisco Systems	2600 Series	--	Y	2 - 48	Y
	3600 Series	--	Y	2 - 228	Y
	3660 Series	--	Y	2 - 288	Y
	AS5300	--	Y	48 - 96	Y
	7200 Series	--	Y	48 - 720	Y
	7500 Series	--	Y	48 - 720	Y
Clarent	Clarent Gateway	Win NT	Y	4 - 24	Y
Cosmobridge	CTG3000	--	Y	Up to 120	N
	CFG3000	--	Y	Up to 120	Y
iptel.de	Portline	--	Y	Up to 120	Y
Computer Protocol Malasiya	CpIP VoiceGateway	Win95, Win NT	Y	2 - 16	Y
Dialog	DM3 IP Link	Solaris 2.5, Win NT	Y	Up to 120	Y

GW Hersteller cont.	***Produkt***	***OS***	***H.323***	***Ports***	***Fax Support***
Digi Europe	NetBlazer 8500	Unix	Y	Up to 120	N
ECI Telecom	ITX 120	--	Y	Up to 120	Y
	ITX 180	--	Y	Up to 180	Y
	ITX 1000	--	Y	Up to 960	Y
eFusion	eStream	Win 95, Win NT	Y	Up to 120	N
Ericsson	IPT	WinNT	Y	Up to 780	Y
	Phone Doubler	Win NT	Y	3 - 30	Y
	PWebSwitch 2000	--	Y	Up to 16	Y
Excel Switching	EXS Media Gateway	--	Y	Up to 960	Y
Franklin Telecom	Typhoon	Linux	Y	Up to 120	Y
	Tempest	Linux	Y	Up to 96	Y
	Breeze	Linux	Y	2	Y
Global Gateway Group	Local Exchange Server	Solaris, Win 95	Y	Up to 96	Y
GlobalTel	Portal Gateway	--	Y	4	Y
	Flexgate Gateway	--	Y	16	Y
Hypercom	IP tel 4000	Win 95, Win NT, Unix, HP Unix, AIX	Y	Up to 32	Y
	IP tel 6000	Win 95, Win NT, Unix, HP Unix, AIX	Y	960	Y
Info-Dial	ID2000	--	Y	30 - 120	N
Innomedia	Infogate	Win NT	Y	4 - 16	Y

GW Hersteller cont.	*Produkt*	*OS*	*H.323*	*Ports*	*Fax Support*
Intelliswitch	iSwitch	Win NT	Y	8 - 150	Y
Internet Telecom	TELECOMMUNICATOR Pro	Win 95, Win NT, QNX	Y	4 - 32	Y
	Multiport 2400	Win NT, QNX	Y	Up to 300	--
	Multiport 2400F	Win NT, QNX	Y	Up to 300	Y
	Via IP	Win 95, Win NT	Y	4	--
InterTel	InterPrise 400	Win 95, Win NT	Y	Up to 4	Y
	InterPrise 2400	Win 95, Win NT	Y	Up to 24	Y
	InterPrise 3200D	Win 95, Win NT	Y	Up to 32	Y
	InterPrise 128D	Win 95, Win NT	Y	Up to 128	Y
	Vocal'Net 3200S	Win 95, Win NT	Y	8 to 32	Y
	Vocal'Net 9600S	Win 95, Win NT	Y	Up to 96	Y
	Vocal'Net 3200D	Win 95, Win NT	Y	Up to 128	Y
	Vocal'Net 128D	Win 95, Win NT	Y	Up to 128	Y
Interline	Analogue Gateway	Unix	Y	Up to 20	N
	Digital Gateway	Unix	Y	Up to 30	N
IPAXS	SingleAXS	--	Y	1	Y
	OmniAXS VoiceHUB	--	Y	4 - 24	Y
	OmniAXS Gateway Switch	--	Y	24 - 288	Y

GW Hersteller cont.	***Produkt***	***OS***	***H.323***	***Ports***	***Fax Support***
Lara Technology	USG10	--	Y	--	Y
	UCX10	--	Y	--	Y
	USX1000	--	Y	--	Y
Latic	LATNET	--	--	Up to 24	Y
Linkon	Link'Net IP Gateway	Sun	Y	4 - 96	Y
Lucent	IST-E	Win NT	Y	Up to 672	Y
	PacketStar	--	Y	Up to 672	Y
Lynk	TeleLynk	--	Y	Up to 90	Y
MasterMind Technologies	MasterVox	Win NT	Y	Up to 96	Y
MG 2 Technologies	MG2 VoIP	Win NT Unix	Y	90	N
Mockingbird	Nuvo 100	Solaris	Y	Up to 96	Y
	Nuvo 200	Solaris	Y	Up to 240	Y
	Nuvo 500	Solaris	Y	Up to 600	Y
MultiTech	MultiVOIP	--	Y	2	N
NetPhone	Connect	Win NT	Y	24	Y
	IPBX	Win NT	Y	24	Y
Netrix	Network Exchange 2210	--	Y	Up to 180	Y
	Network Exchange 2410	--	Y	Up to 300	Y
NeTrue	NeTrueLink	Win NT, Unix	Y	4 - 32	Y
	NTrueCom	Win NT, Unix	Y	8 - 96	Y

GW Hersteller cont.	*Produkt*	*OS*	*H.323*	*Ports*	*Fax Support*
Netspeak	Gateway Exchange Server	Win NT	??	Up to 96	??
NKO	SmartPop	--	Y	24 - 180 per Rack	Y
Nokia	IP Telephony Gateway	--	Y	16 - 60	Y
	Branch Gateway	--	Y	4	Y
Nortel Networks	Arelnet i-Tone Gateway	Win NT	Y	Up to 96	Y
	MMCS Gateway	--	Y	Up to 1800	Y
Nuera	f50ip	--	Y	4	Y
	F200ip	--	Y	Up to 30	Y
OzTel	Oztel Gateway	Win 95, Win NT	Y	2	Y
PhoNet	EtherGate	--	Y	--	Y
Quescom	Qbox R Series	Win NT	Y	Up to 120	Y
	Qbox V Series	Win NT	Y	Up to 1200	Y
Radvision[51]	L2W-323	--	Y	4	N
Ring	IVIP	Win NT	Y	4	N
Science Dynamics	The Integrator	--	Y	Up to 30	Y
Selsius Systems	Selsius IP-PBX	Win NT	Y	24	Y
Siemens	InterXpress 1000	--	Y	--	Y
	InterXpress 2000	--	Y	--	Y
Soliton Systems	SolPhone 1004	--	Y	4	Y

[51] ist in Siemens C65 Workflow Lösung integriert siehe Kapitel 5.1

GW Hersteller cont.	*Produkt*	*OS*	*H.323*	*Ports*	*Fax Support*
SOSINC	Sovereign	--	Y	2 - 48	Y
StarVox	Stargate Server	Win NT	Y	96	N
TEK DigiTel	V-Server	--	Y	2	Y
Teldat	Voxnet	--	Y	4	Y
TeleSoft	SmartGate 1000	Win 95, Win NT	Y	Up to 96	Y
Telogy	Golden Gateway	Wind River VXWorks	Y	--	Y
VegaStream	Vega 50	--	Y	8	N
	Vega 100	--	Y	Up to 120	N
	Vega 200	--	Y	Up to 30	N
VipNet	AutoVoIP	Win 95, 98, NT	Y	2	Y
	MultiVoIP	Win 95, 98, NT	Y	4	Y
VocalTec	Telephony Gateway	Win NT	Y	2 - 24	Y
Vodavi	DiscoveryIP	--	Y	2, 4, 8	Y
Vsys	Vswitch	SUN	Y	--	N
World Telecom Labs	Inx	Unix	Y	Up to 240	Y

Tabelle 21 : VoIP Gateway Anbieter [voip.org]

B.4 Beispiele für Hersteller von Software IP Telefonen

Hersteller	*Produkt*	*OS*	*H.323*	*Options*	*Video*	*Price*
01 Communique	Communicate ! Pro	Win 95, Win NT	Y	Fax Support, File Transfer, Caller ID, Text Chat	N	89,95$
Microsoft	Netmeeting	Win 95, NT	Y	Call Answer, Whiteboard, Application Share, File Transfer, Group Conference, Text Chat, Directory Assistance	Y	Free
VoxPhone	Video VoxPhone	Win 95, 98, NT	Y	Group Conference, Directory Assistance, File Transfer, Caller ID, Text Chat	Y	31,90$
White Pine	CU-SeeMe Pro	Win 95, 98, NT	Y	Whiteboard, Application Share, File Transfer, Group Conference, Directory Assistance, Text Chat Y	-	69$

Tabelle 22 : Software IP Telefon Anbieter [voip.org]

B.5 Beispiele für Hersteller von Hardware IP Telephonen

Hersteller	*Produkt*	*Options*
Cisco	12 SP+	siehe Kapitel 5.1
	30 VIP	siehe Kapitel 5.1
Nokia	IP Courier Ethernet Phone	Call hold, Call Transfer, Call Waiting, Memory Dailing, remote Administration und Konfiguration optional : 4 Port Hub, individuelle Anpassung der IP Telefonumgebung durch persönl. Profile (Speed Dial, Call Forwarding Preferences etc.)
Siemens	LP5100	siehe Kapitel 5.1

Tabelle 23 : Hardware IP Telefon Anbieter

Anhang C ist eine separate Excel Datei

Anhang D

D.1 Test der Konfiguration des Cisco 2611 - Kapitel 7.1.2.2

Anruf von Netmeeting 3.01 139.30.208.7 3519 -> ISDN Telefon 2203911

```
2600#debug isdn q931
ISDN Q931 packets debugging is on
2600#
07:41:00: ISDN BR1/0: TX ->  SETUP pd = 65  callref = 0x20
07:41:2164480932:         Channel ID i = 0x83
07:41:00:         Called Party Number i = 0x80, '2203911'
07:41:00:         Shift to Codeset 6
07:41:2164480540:         Codeset 6 IE 0x1  i = 0x0101
07:41:00:         Sending Complete
07:41:00: ISDN BR1/0: RX <-  SETUP_ACK pd = 65  callref = 0xA0
07:41:00:         Channel ID i = 0x89
07:41:00: ISDN BR1/0: RX <-  ALERTING pd = 65  callref = 0xA0
07:41:00:         Shift to Codeset 6
07:41:00:         Codeset 6 IE 0x7  i = 0x02
07:41:05: ISDN BR1/0: RX <-  CONNECT pd = 65  callref = 0xA0
07:41:05:         Shift to Codeset 6
07:41:05:         Codeset 6 IE 0x3  i = '08.11.99-14:59:52'
07:41:21474836480: ISDN BR1/0: TX ->  CONNECT_ACK pd = 65  callref = 0x20
```

Verbindung vorhanden - B Kanal belegt, jedoch keine Sprachverbindung !

Auflegen

```
07:42:21: ISDN BR1/0: RX <-  DISCONNECT pd = 65  callref = 0xA0
07:42:21:         Cause i = 0xDA - Response to STATUS ENQUIRY or number unassigned
07:42:21:         Shift to Codeset 6
07:42:21:         Codeset 6 IE 0x3  i = '08.11.99-15:01:02'
07:42:90194313216: ISDN BR1/0: TX ->  RELEASE pd = 65  callref = 0x20
07:42:92358809652: %ISDN-6-DISCONNECT: Interface BRI1/0:1  disconnected from unknown
, call lasted 76 seconds
07:42:21: ISDN BR1/0: RX <-  RELEASE_COMP pd = 65  callref = 0xA0
```

D.2 Monitoring von Point to Point Calls - Kapitel 7.2.1

amunre /rad -> bes/ rad indirect routing - Problem : Fehlen der Source IP Adresse in Setup

```
< GK:  _____________________________________________________________block 190
[41369049] >
< GK:  eventNewCall [41369049]  >
< GK:  admission request (origin) from 139.30.208.7:1053. endpoint=3 [41369050] >
< GK:  sending admission confirm for call  0 [41369050]  >
< GK:  setup received - Offering on call  0 [41369069]  >
```

```
< GK:  gk sending setup to destination. Present parameters of cal: 0 [41369069] >
< GK:   No. From                 To                          State      Service
[41369069]  >
< GK:   --- ----                 --                          -----      -------
[41369069]  >
< GK:     0   0.0.0.0:0       139.30.208.5:1720   ,3500        CAL_HUNTING
[41369069]  >
< GK:  disconnecting call  0 [41369074]  >
< GK:  _____________________________________________________________block 191
[41369085]  >
< GK:  disengage request from 139.30.208.7:1053 - origin of call 0. endpoint=3
[41369085]  >
< GK:  DCF for call 0 [41369085]  >
< GK:  clearing call  0 [41369086]  >
```

D.3 Trace Interoperabilität Netmeeting VCON - Kapitel 7.2.2

a) bes /netmeeting -> com20 /VCON indirect call routing (über GK)

```
< GK:  _____________________________________________________________block 271
[50472962]  >
< GK:  eventNewCall [50472962]  >
< GK:  admission request (origin) from 139.30.208.5:1108. endpoint=3 [50472963] >
< GK:  sending admission confirm for call  0 [50472963]  >
< GK:  setup received - Offering on call  0 [50472989]  >
< GK:  gk sending setup to destination. Present parameters of cal: 0 [50472989] >
< GK:   No. From                 To                          State      Service
[50472989]>
< GK:   --- ----                 --                          -----      -------
[50472989]>
< GK:   0   0.0.0.0:0            139.30.208.20:1720  ,3920  CAL_HUNTING
[50472989]>
< GK:  admission request (destination) from 139.30.208.20:1719. endpoint=1
[50472999]  >
< GK:  destination ARQ w/o src call signal address at locateARQCall for
call[50472999]>
< GK:  sending admission confirm for call  0 [50472999]  >
< GK:  destination connect for call 0 [50474188]  >
< GK:  origin connect for call 0 [50474189]  >
< GK:  Call is formed  0 [50474189]  >
< lg: [4:TOUT ID2] [50476229]  >
< lg: [4:I_ACK IDL] [50476232]  >
```

auflegen von bes

```
< GK:  _____________________________________________________________block 272
[50501126]  >
< GK:  disengage request from 139.30.208.5:1108 - origin of call 0. endpoint=3
[50501126]  >
< GK:  DCF for call 0 [50501126]  >
```

```
< GK:  disconnecting call  0 [50501128]  >
< GK:  _____________________________________________________________________block 273
[50501132]  >
< GK:  disengage request from 139.30.208.20:1719 - destination of call 0. endpoint=1
50501132]>
< GK:  DCF for call 0 [50501132]  >
< GK:  clearing call  0 [50501133]  >
```

b) amunre / gk1 -> com 20 / radv (Kommunikation über zwei Zonen)

```
< GK:  _____________________________________________________________________block 152
[41218509]  >
< GK:  Location Request from ip 139.30.208.24:1220 [41218509]  >
< GK:  returning GATEKEEPER ADDRESS of requested terminal [41218509]  >
< GK:  _____________________________________________________________________block 153
[41218528]  >
< GK:  eventNewCall [41218528]  >
< GK:  New call chosen:  0 [41218529]  >
< GK:  setup received - Offering on call  0 [41218529]  >
< GK:  gk sending setup to destination. Present parameters of cal: 0 [41218530] >
< GK:   No. From                  To                            State      Service
41218530] >
< GK:   --- ----                  --                            -----      -------
[41218530]>
< GK:   0   139.30.208.7:1031     139.30.208.20:1720  ,3920     CAL_HUNTING
[41218530]  >
< GK:  admission request (destination) from 139.30.208.20:1719. endpoint=1
[41218535]  >
< GK:  sending admission confirm for call  0 [41218536]  >
< GK:  destination connect for call 0 [41219259]  >
< GK:  origin connect for call 0 [41219260]  >
< GK:  Call is formed  0 [41219260]  >
```

auflegen

```
< lg: [4:TOUT ID2] [41223899]  >
< GK:  disconnecting call  0 [41223902]  >
< GK:  _____________________________________________________________________block 154
[41223905]  >
< GK:  disengage request from 139.30.208.20:1719 - destination of call 0. endpoint=1
41223905] >
< GK:  DCF for call 0 [41223905]  >
< GK:  clearing call  0 [41223906]  >
< lg: [4:I_ACK IDL] [41223907]  >
```

D.4 Trace Interworking ISDN Picturetel Live 200 -> Netmeeting/ Bes - Kapitel 7.2.3

isdn 2303911 -> bes /Netmeeting

```
< lg: [4:I_ACK IDL] [1264680]  > freq = 64
< lg: wp: Port 0 is allocated for Service 0 [1264715]  >
< SCN: Incoming call from port: 0. Options: MSN[on] TCS4[off] IVR[on] DEF_EXT[off]
[1264715] >
< SCN: SCN: MSN call =0 [1264715]  >
< APP: call0: dest=TA:139.30.208.26:1720,3500 source=TA:139.30.208.26
source=TEL:230391
1 minRate=64000 maxRate=64000 display=2303911 [1264717]  >
< GK:  ________________________________________________________________block 46
[1264720]  >
< GK:  eventNewCall [1264720]  >
< GK:  admission request (origin) from 139.30.208.26:1024. endpoint=0 [1264720] >
< GK:  sending admission confirm for call  0 [1264721]  >
< lg: [0:I_CALL IN1] [1264725]  >
< lg: [0:OK IN4] [1264725]  >
< GK:  ________________________________________________________________block 47
[1264728]  >
< GK:  eventNewCall [1264728]  >
< GK:  admission request (destination) from 139.30.208.5:2922. endpoint=1 [1264728]
>
< GK:  sending admission confirm for call  0 [1264729]  >
< APP: *****************Calls Status********************** [1264750]  >
< APP: call0 <0:0:0>    call1 <0:0:0>    call2 <0:0:0>    call3 <0:0:0>    call4
<0:0:0>    call5 <0:0:0>    call6 <0:0:0>    call7 <0:0:0> [1264750]  >
< APP: ************************************************** [1264750]  >
< lg: [0:CNCT IN5] [1264750]  >
< lg: [0:I_ACK IN7] [1264756]  >
< APP: ***********LAN's codec Capabilities********* [1264771]  >
< APP: capability:H261Video QCIF Mpi=1 [1264771]  >
< APP: capability:H261Video CIF Mpi=1 [1264771]  >
< APP: capability:G711Alaw Packet Size=180 [1264771]  >
< APP: capability:G711Ulaw Packet Size=180 [1264771]  >
< APP: capability:G728 Packet Size=0 [1264771]  >
< APP: capability:Transfere Rate=128000 [1264771]  >
< APP: capability:Restricted=0 [1264771]  >
< APP: capability:G7231 Max Frame Number=12 [1264771]  >
< APP: capability:G7231 Silence Detection=0 [1264771]  >
< APP: capability:G722 Packet Size=0 [1264771]  >
< APP: capability:T120 BitRate=825000 [1264771]  >
< APP: ********************************************************** [1264771]  >
< APP: Not a data call - LAN caps will not sent to WAN [1264771]  >
< lg: [0:I_CNCT CONT] [1264771]  >
< lg: [0:I_CNFM IN8] [1264772]  >
< SCN: scsesAppCapsRecieved: Caps not arrived yet [1264782]  >
< APP: Sending H320 Voice Capabilities to LAN for call=0 [1264782]  >
< APP: **********WAN's codec Capabilities********** [1264782]  >
< APP: capability:H261Video QCIF Mpi=0 [1264782]  >
```

```
< APP: capability:H261Video CIF Mpi=0 [1264782]  >
< APP: capability:G711Alaw Packet Size=60 [1264782]  >
< APP: capability:G711Ulaw Packet Size=60 [1264782]  >
< APP: capability:G728 Packet Size=0 [1264782]  >
< APP: capability:Transfere Rate=0 [1264782]  >
< APP: capability:Restricted=0 [1264782]  >
< APP: capability:G7231 Max Frame Number=0 [1264782]  >
< APP: capability:G7231 Silence Detection=0 [1264782]  >
< APP: capability:G722 Packet Size=0 [1264782]  >
< APP: capability:T120 BitRate=0 [1264782]  >
< APP: ********************************************************** [1264782]  >
< APP: Call:0 Converting SCN audio subtype 2 to LAN [1264784]  >
< lg: [0:I_ACNT TD1] [1264785]  >
< APP: Call:0 Converting SCN audio subtype 2 to LAN [1264789]  >
< APP: Open WAN 2 LAN AUDIO channel=0: channelName=g711Alaw64k, packetSize=60
[1264790]  >
< APP: Open LAN 2 WAN channel=24 channelName=g711Ulaw64k [1264793]  >
< APP: Software transcoding mode. Call: 0 LAN audio 3 WAN audio 2 [1264793]  >
< lg: [5:TOUT ID2] [1264992]  >
< lg: [5:I_ACK IDL] [1264995]  >
```

auflegen von isdn Seite

```
< lg: [0:I_DCNT NDCN] [1274535]  >
-0-ISDN clearing cause|class: (31)Normal, unspecified|Normal event

< APP: DISCONNECT CALL:0 from WAN cause Normal, unspecified [1274536]  >
< GK:  _____________________________________________________________block 48
[1274542]  >
< GK:  disengage request from 139.30.208.5:2922 - destination of call 0. endpoint=1
[1274542]>
< GK:  DCF for call 0 [1274542]  >
< GK:  _____________________________________________________________block 49
[1274544]  >
< GK:  disengage request from 139.30.208.26:1024 - origin of call 0. endpoint=0
[1274544]  >
< GK:  DCF for call 0 [1274544]  >
< GK:  clearing call  0 [1274546]  >
< lg: L2W 0- in START state received illegal message 7 name=HMAIN_CHAN_DROP_EVENT
[1274546]  >
< APP: ****************Calls Status********************** [1274548]  >
< APP: call0 <0:1:38>    call1 <0:0:0>    call2 <0:0:0>    call3 <0:0:0>    call4
<0:0:0>    call5 <0:0:0>    call6 <0:0:0>    call7 <0:0:0> [1274548]  >
< APP: ************************************************ [1274548]  >
< lg: l2wTask 0 :ERROR while l2wProcessEventBeforeSession() [1274548]  >
< SCN: ------------ Ses:0 Call CLEANUP procedure ------------ [1274549]  >
< lg: hportDelHndl: Port num=1 is free! [1274549]  >
< lg: hchSetChanInactive: Channel is inactive! [1274549]  >
< lg: wp - wpDropPort - Port not in use. [1274549]  >
```

```
< lg: [0:I_END IDL] [1274549]  >
```

Erklärung

Hiermit versichere ich, die vorliegende Arbeit selbständig angefertigt und keine weiteren als die angegebenen Quellen benutzt zu haben.

Jörn Wallstabe