

## 5. Analyse des Kommunikationsnetzes und Optimierungsvorschläge

### 5.1 Analyse und Empfehlungen für die Fest- und Wählverbindungen

Ausgehend von den Messungen des Kommunikationsaufkommens des Institutes sind die Meßergebnisse des Abschnittes 4.1.1 für die Analyse der Auslastung der verschiedenen Verbindungen in folgender Tabelle zusammengefaßt.

#### Sprachkommunikation:

Typ des Bündels	Richtung	Bezeichnung der Verbindung	Anzahl der bereitgestellten Sprachkanäle	Mittlere Auslastung des Bündels in %	Maximale Auslastung des Bündels in %
Festverbindung	K1 – K5	1 x T2MS	25	6	22
	K1 – K10	1 x T2MS	23	3	13
	K10 – E30	1 x TS02	1	20	100
Wählverbindung	K1 zum Amt	1 x S <sub>2m</sub>	30	6	7
	K5 zum Amt	4 x S <sub>0</sub>	8	12	44
	K10 zum Amt	5 x S <sub>0</sub>	10	12	41
	E30 zum Amt	1 x S <sub>0</sub>	2	5	53

Die Meßwerte zeigen, daß die Festverbindung zwischen K1 und K5 bis zu maximal 22 % ausgelastet ist. Diese Übertragungsstrecke besitzt damit eine Bandbreiten-Reserve von über 70 %. Die zum Meßzeitpunkt angeschlossenen Geschäftsstellen sind E17, E18 und E19. Aufgrund der zukünftig anzukoppelnden Geschäftsstellen E16, E20, K6 und E21 kann die Festverbindung als nicht überdimensioniert angesehen werden, da der weitere Ausbau der Netzstruktur eine Erhöhung der maximalen Auslastung um 30 % bewirken wird. Die maximale Auslastung der Sprachkanäle wird damit bei 50 bis 60 % liegen. Die Bandbreiten-Reserve ist dabei zwischen den Sprach- und Datenkanälen im Verhältnis 3:1 aufzuteilen. Die Auslastung der Übergänge zum öffentlichen Fernsprechnetzt beträgt 44 %, wobei auch hier eine weitere Erhöhung von bis zu 30 % zu erwarten ist. Die maximale Auslastung der Übergänge in das öffentliche Fernsprechnetzt beträgt 70 % (6 Sprachkanäle). Die bereitgestellte Anzahl von 8 Sprachkanälen wird als optimal angesehen. Die maximale Auslastung der Sprachkanäle zwischen K1 – K10 beträgt 13 %. Mit der Erweiterung der Vernetzung des Standortes K10 um K11, E31, E32, K12 und E33 wird eine weitere Erhöhung der Auslastung von bis zu 40 % zu beobachten sein. Die Auslastung der Sprachkanäle wird maximal bis zu 60 % betragen. Die Erhöhung der Auslastung wird durch die Anzahl der anzukoppelnden

Geschäftsstellen und deren PBX mit der institutsübergreifenden „Least Cost Routing“-Funktionalität begründet. Der Übergang zum öffentlichen Fernsprechnet in K10 ist maximal zu 41 % ausgelastet. Die Auslastung wird mit der Anzahl der weiteren Geschäftsstellen nur um 10 % ansteigen, weil die anzuschließenden Geschäftsstellen einen Übergang zum öffentlichen Fernsprechnet im Knoten K11 besitzen. Die Anschlüsse von K10 sind bis zum vollständigen Ausbau dieses Netzabschnitts weiter zu beobachten und bei Übereinstimmung der Prognosen zu minimieren (1 - 2 Basisanschlüsse).

Der Standort E30 wird über einen Sprachkanal an den Knoten K10 gekoppelt. Die maximale Auslastung von 100 % kann als optimal bezeichnet werden, weil diese Auslastung nur kurzzeitig erreicht wird und zusätzlich die Möglichkeit des Übergangs zum öffentlichen Fernsprechnet in dieser Geschäftsstelle besteht. Die Auslastung des Übergangs zum öffentlichen Fernsprechnet wird mit maximal 53 % als optimal angesehen, weil die Bandbreiten-Reserve von über 40 % auch im Überlastfall der Festverbindung eine Kommunikation gewährleistet.

Der Übergang von K1 zum öffentlichen Fernsprechnet erfährt nur eine maximale Auslastung von 7 %, was 3 Sprachkanälen entspricht. Die weitere Nutzung des Übergangs ist abhängig von der Konfiguration der „Least Cost Routing“-Funktionalität der PBX. Bei der Zusammenfassung aller Telefonate von den Außenstellen zum öffentlichen Netz durch diesen Anschluß wird eine weitere Erhöhung der Auslastung eintreten. Diese Konfigurationsvariante wird befürwortet, weil K1 die Wurzel der Baumstruktur darstellt. Eine Weiterleitung der Gespräche zu den öffentlichen Übergängen in K5 und K3 würde nur die Auslastung zu diesen Standorten erhöhen und keine Kosten sparen, weil sich alle Standorte innerhalb einer City-Tarifzone befinden. Falls die Planung eine Weiterverteilung der Gespräche vorsieht, sollte der Primärmultiplexanschluß mit 30 Sprachkanälen durch 3 S<sub>0</sub>-Basisanschlüsse mit 6 Sprachkanälen ersetzt werden.

Bei der Analyse der Festverbindungen muß festgestellt werden, daß der Netzabschnitt trotz der geringen mittleren Auslastung nicht überdimensioniert ist. Die künftigen Erweiterungen der Knoten werden eine weitere Erhöhung der Auslastung bewirken, wobei maximal 60 % der Sprachkanäle gleichzeitig genutzt werden. Die dabei zur Verfügung stehende Bandbreiten-Reserve kann für die Sprach- **und** Datenübertragung genutzt werden. Bei dem Aufbau und der Analyse eines Standortes ist zu beachten, daß entweder die Festverbindung mit 100 % und der Übergang mit weniger als 100 % (siehe E30) belastet wird. Die Geschäftsstelle ist dann immer durch den Kunden oder die Mitarbeiter des Institutes telefonisch zu erreichen. Die Übergänge zum öffentlichen Fernsprechnet sind mit Ausnahme von K5 und E30 noch nicht

optimal ausgenutzt. Da die mittlere Auslastung bei 10 % und die maximale Auslastung bei 50 % liegt, werden die künftig anzukoppelnden Standorte unterschiedlichen Einfluß auf die Übergänge besitzen. Die Übergänge sind deshalb weiter zu beobachten und gegebenenfalls in der Anzahl der Sprachkanäle zu minimieren (z.B.: K1 und K10). Eine Minimierung der Anzahl der Kanäle zum öffentlichen Fernsprechnetz sollte erst nach dem vollständigen Ausbau des jeweiligen Netzabschnittes erfolgen, wobei danach eine Meßperiode von drei Monaten die zu treffenden Entscheidungen bestätigen sollte. Bei der Minimierung sind die Maxima der Auslastung und eine Bandbreiten-Reserve von 20 % mit einzubeziehen.

#### Datenkommunikation:

WAN-Verbindung	Datenübertragungsrate in kbit/s	Mittlere Auslastung der Verbindung in %	Maximale Auslastung der Verbindung in %
K1 – K3	384 kbit/s	5	28
K1 – K5	128 kbit/s	9	58
K1 – K9	128 kbit/s	0,5	12
K1 – K10	192 kbit/s	3	70
K1 – E2	256 kbit/s	3	23
K1 – E5	64 kbit/s	18	48
K5 – E17	128 kbit/s	3	35
K5 – E19	64 kbit/s	1	1,5
K1 – E1	128 kbit/s	1,5	3
K1 – E8	64 kbit/s	3	5
K1 – E21	64 kbit/s	3	5
K1 – E32	64 kbit/s	2	4
K10 – E29	64 kbit/s	3	5
K10 – E30	64 kbit/s	1	1,5

Für die WAN-Verbindung K1 – K3 kann festgestellt werden, daß diese Verbindung derzeit maximal zu 30 % ausgenutzt wird. Diese Auslastung wird durch die Kommunikation im Institut und zum Rechenzentrum erzeugt. Die Auslastung der WAN-Verbindung ist als optimal anzusehen, weil die Bandbreiten-Reserve von 70 % eine Einführung von weiteren Client-Server-basierenden Applikationen und deren Pflege über diese WAN-Verbindung erlaubt.

Die WAN-Verbindung K1 – K5 mit einer maximalen Auslastung von 58 % ist derzeit optimal ausgenutzt. Im Gegensatz zu K1 – K10 werden über diese Verbindung breitbandige Kommunikationsbeziehungen zum Rechenzentrum eingegangen, weshalb der Einsatz eines separaten Routers des Rechenzentrums im Standort K5 empfohlen wird. Der Einsatz des

Routers wird wesentlich zur Entlastung der WAN-Verbindung K1 – K5 beitragen. Mit dem Fortbestehen der Pflege der Bildinformationen des Kundenleit-Servers und der Kommunikation von K3 zu E17, wird empfohlen die Datenübertragungsrate auf 256 kbit/s zu erhöhen. Die Erhöhung der Bandbreite kann durch eine Überbuchung des „Frame Relays“ und durch den Einsatz von Kompression ermöglicht werden, welche im Abschnitt 5.2.1 beschrieben sind. Mit der Erhöhung der Bandbreite und der Nutzung eines separaten Routers werden die breitbandigen Kommunikationsbeziehungen zum Rechenzentrum über diese WAN-Verbindung entfallen und damit die Bandbreite zur internen Kommunikation zur Verfügung steht. Mit diesen Maßnahmen wird eine Überlastsituation auf der WAN-Verbindung infolge des Einsatzes weiterer Applikationen und Servern vermieden. Der zusätzliche Router des Rechenzentrums in K5 wird auch den gesamten Verkehr der zukünftigen Standorte (E16, E20, K6 und E21), welche an K5 gekoppelt sind, übernehmen und so zur Entlastung der WAN-Verbindung beitragen.

Die WAN-Verbindung K1 – K9 wird derzeit maximal zu 12 % ausgelastet. Die Auslastung der Verbindung wird mit der Erweiterung des Netzabschnittes um die Stationen E25, E26 und E27 um maximal 20 % steigen. Die Verbindung besitzt damit eine Bandbreiten-Reserve von über 60 %, die für künftige Applikationen genutzt werden kann. Die WAN-Verbindung sollte weiter beibehalten werden.

Die WAN-Verbindung K1 – K10 wird zu maximal 70 % ausgelastet. Die Erweiterung des Netzabschnittes um die Standorte K11, E31, E32, K12 und E33 und die Übertragung von Bildinformationen zum Kundenleit-Server werden eine weitere Erhöhung der Auslastung bewirken. Die maximale Auslastung wird dabei jedoch den Wert von 80 % nicht überschreiten, weil das Maximum nicht aus dem „Normalbetrieb“ resultiert (siehe Abschnitt 4.1.2.2). Die mittlere Auslastung wird 40 % betragen, wodurch eine Bandbreiten-Reserve von 60 % gegeben ist. Die bereitgestellte Bandbreite wird derzeit als ausreichend angesehen. An diesem Standort kann der Nutzen eines separaten Routers zum Rechenzentrum festgestellt werden, weil keine breitbandigen Kommunikationsbeziehungen (vgl. K5) zum Rechenzentrum über diese WAN-Verbindung eingegangen werden.

Die WAN-Verbindungen K1 – E5 sowie K5 – E17 werden bis zu 50 % ausgelastet. Die Auslastung der Verbindungen resultiert aus der standortübergreifenden Kommunikation zu K1 und K3. Die bereitgestellte Bandbreiten-Reserve von 50 % wird derzeit als ausreichend angesehen, da die zu erwartende weitere Nutzung der vorhandenen Server keine Erhöhung der Auslastung bewirkt.

Die weiteren in der Übersicht enthaltenen WAN-Verbindungen besitzen eine maximale Auslastung von bis zu 20 % mit einer daraus resultierenden Bandbreiten-Reserve von über 80 %. Aufgrund der hohen Reserve besteht die Möglichkeit, die Standorte weiter auszubauen und neue Systeme, Applikationen und Server einzusetzen.

Zusammenfassend kann für die betrachteten Standorte festgestellt werden, daß die Festverbindungen im Sprach- und Datenbereich den Kommunikationsanforderungen genügen und darüber hinaus eine hohe Bandbreiten-Reserve von bis zu 80 % besteht. Bei den Festverbindungen zwischen den Knoten ist eine Erhöhung der Auslastung um bis zu 30 % mit steigendem Ausbau der Netzabschnitte zu erwarten. Dabei wird die Festverbindung **K1 – K5** nur eine geringe Bandbreiten-Reserve aufweisen, weshalb diese Verbindung hinsichtlich der Bandbreitenvergabe zu optimieren ist. Aufgrund der bisher fehlenden Möglichkeit der Überprüfung der Festverbindungen zwischen K1 – K3, K1 – K8, K1 – K9, K10 – K11, K1 – K13, K1 – K14, K1 – K15, K1 – K16 und der beobachteten hohen Übertragungsrate auf den WAN-Verbindungen einzelner Knoten (z.B.: K1 – K3) sollten für diese Verbindungen künftig Möglichkeiten zur Messung geschaffen werden. Speziell bei den derzeit bereits bestehenden Verbindungen zwischen den Knoten **K1 – K3** sowie **K1 – K15** sind Messungen auf den Sprach- und Datenkanälen durchzuführen, weil diese Verbindungen ein ähnlich hohes Verkehrsaufkommen besitzen bzw. besitzen werden wie die Verbindung K1 – K5 und deshalb auch dort Optimierungsmaßnahmen durchgeführt werden müssen. Für die genannten Festverbindungen gelten folgende Empfehlungen hinsichtlich der Optimierung und Weiterbeobachtung.

Festverbindung	Bisherige Messungen	Zukünftige Messungen	Messungen und Meßpunktabstand (Sprache & Daten)	Optimierung der Bandbreitenvergabe (Sprache & Daten)
K1 – K5	Sprache & Daten	Sprache & Daten	fortlaufend 15 min & 5 min	notwendig
K1 – K3	Daten	Sprache & Daten	fortlaufend 15 min & 5 min	nach Beobachtung der Sprachkanäle, aber zukünftig notwendig
K1 – K10	Sprache & Daten	Sprache & Daten	fortlaufend 15 min & 5 min	notwendig durch LCR und Routerverbindung zum RZ und weiteren Ausbau (K10 – K11)
K1 – K15	Nicht möglich	Sprache & Daten	fortlaufend 15 min & 5 min	notwendig durch LCR und <b>zweite</b> separate Routerverbindung zum RZ und weiteren Ausbau

Festverbindung	Bisherige Messungen	Zukünftige Messungen	Messungen und Meßpunktstand (Sprache & Daten)	Optimierung der Bandbreitenvergabe (Sprache & Daten)
K1 – E2 K1 – E5 K1 – K9 K5 – E17	Daten	Sprache & Daten	fortlaufend 15 min & 5 min	nach weiterer Beobachtung der Sprach- und Datenkanäle
K1 – K4 K1 – K7 K1 – K8 K1 – K13 K1 – K14 K1 – K16	Nicht möglich	Sprache & Daten	fortlaufend 15 min & 5 min	nach weiterer Beobachtung der Sprach- und Datenkanäle
Alle weiteren Festverbindungen	Je nach Ausbauphase möglich (oft nur Daten)	Sprache & Daten	In Abhängigkeit von der Netzwerksituation 15 min & 10 min	Mit weiterer Beobachtung 1. nach Inbetriebnahme 2. nach Installationen, Umkonfigurationen von Netzkomponenten (Servern) 3. zyklisch nach 6 Monaten

In Abhängigkeit von der Ausbauphase müssen die Übergänge in das öffentliche Fernsprechnet des jeweiligen Standortes parallel zu den geschalteten Festverbindungen überwacht werden (z.B.: K1 – K15 **und** K15 – Amt) und bei Überlast zusätzliche Basisanschlüsse oder ab 8 Basisanschlüsse ein Primärmultiplexanschluß angemietet werden. Für die Optimierung der Festverbindungen können die im folgenden Abschnitt vorgeschlagenen Maßnahmen verwendet werden. Weiterhin verursachen die Kommunikationsbeziehungen zwischen den Fachabteilungen von K3, K1, E5 und E17 eine netzweite hohe Auslastung. Aufgrund der Standortunabhängigkeit der Fachabteilungen wird empfohlen, diese im Standort K1 zusammenzufassen, um so die Kommunikationsbeziehungen im lokalen Bereich zu halten. Des weiteren sollte bei einem Ausbau der Standorte E33 und E39 zuerst die Datenverbindung über einen B-Kanal der TS02-Festverbindung aufgebaut werden und bei Feststellung eines höheren Kommunikationsbedarfes eine D64S angemietet werden. Für die Sprachkommunikation sollten nicht mehr als zwei TS02-Festverbindungen (E1, E16, E17) zwischen den verschiedenen Standorten geschaltet werden. Diese Empfehlung ist mit dem geringen Sprachkommunikationsaufkommen zwischen den Knoten (maximal 4 Kanäle in der aktuellen Ausbauphase) zu begründen. Mit diesen Maßnahmen können die Anschlußkosten

für die Festverbindungen (4000 DM) und die monatlichen Gebühren (250 DM) gespart und erst bei Bestätigung des Kommunikationsaufkommens aufgewendet werden. Für den Fall einer zu geringen Bandbreitenreserve zwischen verschiedenen Standorten können verschiedene Typen von Festverbindungen zusätzlich angemietet werden. Für künftige Anmietungen von SFV der Deutschen Telekom AG zur Datenübertragung ist die D64S2 zu empfehlen. Diese Festverbindung besteht aus 2 x B-Kanälen. Die aufzuwendenden Kosten betragen gegenüber der eingesetzten TS02-Verbindung lediglich 56 % (außerhalb eines Anschlußbereiches der DTAG). Aufgrund der Stellung der passenden Terminaladapter durch die DTAG ergeben sich hinsichtlich der für den Verbindungsaufbau benötigten D-Kanal-Information keine Probleme.

## 5.2 Optimierung der bestehenden Netzwerkkomponenten

### 5.2.1 Multiplexer

Bei den eingesetzten Multiplexern werden die Kanäle für die Sprachkommunikation und die Datenkommunikation zeitlich ineinander geschachtelt und über eine T2MS-Festverbindung übertragen. Die Verteilung der Bandbreite für die **Sprach-** und **Datenkommunikation** wird durch die Installation festgelegt und kann **nicht** dynamisch **zueinander** verändert werden. Die Kanäle für die Sprachkommunikation werden zu einem Bündel in der PBX HICOM 300 und die Kanäle für die Datenkommunikation in DLCI des Frame Relay - Netzes zusammengefaßt. Die folgende Skizze veranschaulicht die Vergabe der Zeitschlitz innerhalb eines PCM 30 – Rahmens für die Kommunikation zwischen den Standorten K1 und K10 (vgl. Punkt 3.4.4).

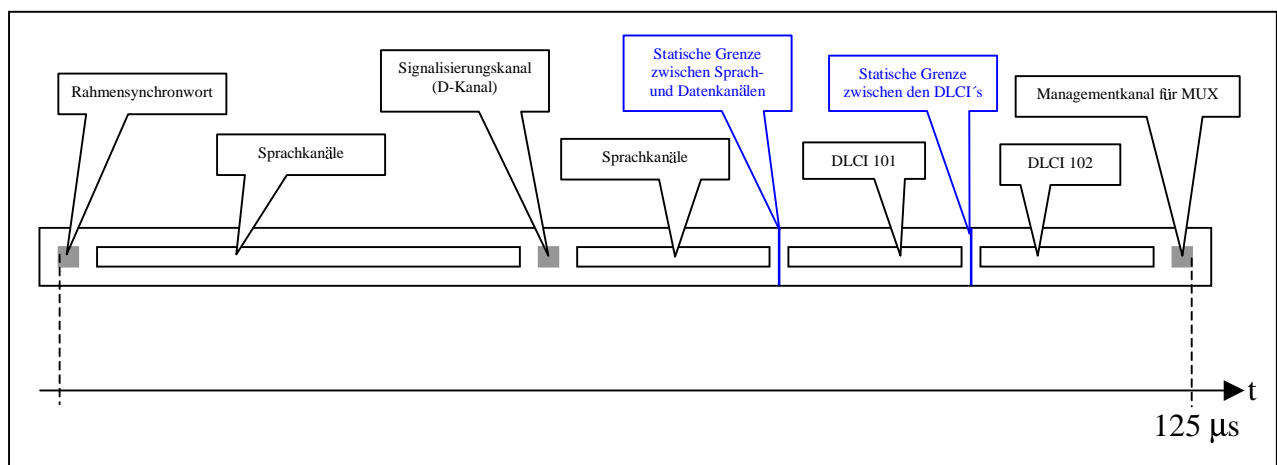


Abb.5.1: PCM 30 Rahmenstruktur auf der Verbindung K1 – K10

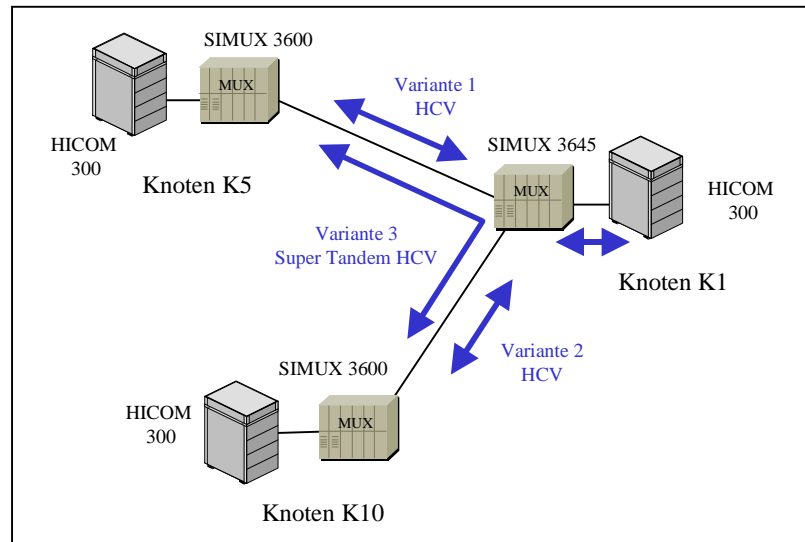
Wie aus der Abbildung ersichtlich, kann eine Optimierung der Rahmenaufteilung nur durch die separate Betrachtung der Kommunikationsformen erreicht werden. Die Kanäle der Sprachkommunikation können über eine Kompression mit verschiedenen Stufen optimiert werden. Bei der Kompression eines Sprachkanals mit 64 kbit/s können folgende Verfahren und Bitraten unterschieden werden.

Bitrate	Kompressionsverfahren
32 kbit/s	Adaptive Differential Pulse Code Modulation (ADPCM) G.721
32 kbit/s	Vector Quantization Coded (VQC)
16 kbit/s	Code Excited Linear Prediction (CELP)
8 kbit/s	Code Excited Linear Prediction (CELP)

Das verwendete CELP-Verfahren stellt eine Eigenentwicklung der Siemens AG dar und wird auch als High Capacity Voice (HCV) - Algorithmus bezeichnet. Bei dem Vergleich der Verfahren wird die Kompression eines Sprachkanals von 64 kbit/s auf 16 kbit/s favorisiert, weil bei dieser Übertragungsrate eine hohe Kompression (4:1), ein Mean Opinion Score (MOS) - Wert von 4,1 und eine Ende-zu-Ende-Verzögerung von 60 ms zu erwarten ist. Die Vergleichswerte sind: MOS = 5 (sehr gute Sprachqualität) und Verzögerung = 100ms (kaum wahrnehmbare Störungen). Zusätzlich wird eine Echokompensation verwendet. Ein Zusatzmodul ermöglicht die Zusammenfassung von maximal 6 komprimierten Kanälen mit jeweils 16 kbit/s sowie die transparente Weiterleitung von Fax-Signalen der Gruppe 3. Bei dem Einsatz eines strukturierten Netzes und komprimierter Sprachkanäle werden mehrfache Dekompressions- und Kompressionsphasen durchlaufen, wobei die Sprachqualität bedeutend abnimmt. Für die Lösung dieses Problems wird das „Super Tandem HCV“ - Verfahren der Multiplexer eingesetzt. Bei diesem Verfahren leitet der SIMUX den komprimierten Sprachkanal zur PBX. Laut D-Kanal-Information vermittelt die PBX diesen komprimierten Kanal an einen Teilnehmer des Standortes oder an einen weiteren Standort, welcher über den SIMUX erreicht wird. Wenn die PBX zu einem weiteren Standort über den SIMUX vermittelt, „erkennt“ der SIMUX den eingegangenen und den von der PBX kommenden Datenstrom als denselben und leitet diesen Datenstrom zum nächsten Standort ohne Dekompressions- und Kompressionsphase weiter. Wird hingegen zu einem Teilnehmer des Standortes vermittelt, wird der Datenstrom nicht wieder zum SIMUX geleitet. Das wird vom SIMUX „erkannt“ und eine Dekompression des Sprachkanals vorgenommen. Die Entscheidung zur einsetzenden Dekompression wird in der Phase des Verbindungsaufbaus vorgenommen, weshalb sie von den Teilnehmern nicht wahrgenommen wird. Wichtig für den



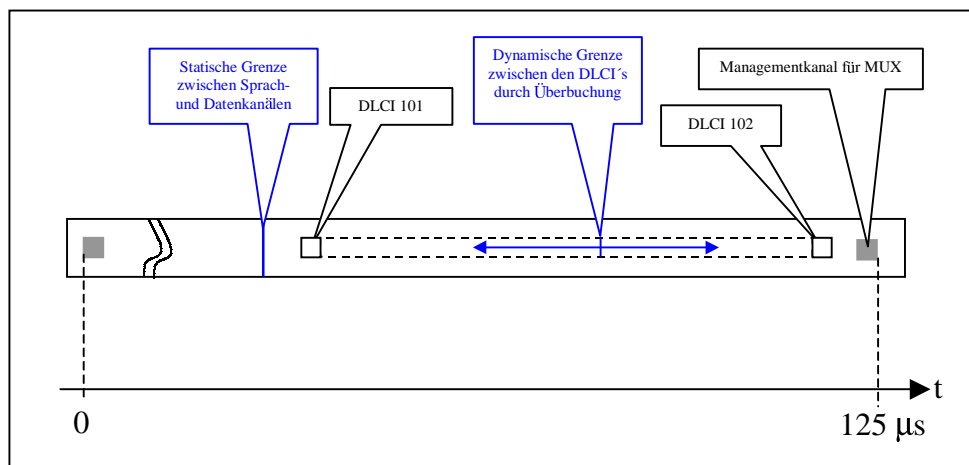
Einsatz des Verfahrens ist, daß die PBX eine transparente Vermittlung der komprimierten Informationen vornimmt und somit keine Veränderung der B-Kanal-Informationen bewirkt.



**Abb.5.2: Super Tandem HCV**

Bei den dargestellten Varianten 1 und 2 der Kommunikation wird das Super Tandem HCV-Verfahren nicht genutzt, weil bei diesen Varianten die unmittelbaren Nachbarstationen miteinander kommunizieren. Bei der Variante 3 kommt das Super Tandem HCV – Verfahren zum Einsatz, wodurch eine transparente Weiterleitung der Informationen von K5 zu K10 durch den Knoten K1 bewirkt wird. Das so aufgebaute Netzwerk besitzt eine hohe Sprachqualität mit geringem Bandbreitenbedarf.

Für die Optimierung der Datenübertragungskanäle wird die Überbuchung einer Anschlußleitung durch die Vergabe eines „Booking“-Faktors eingesetzt. Dieser Faktor ist eine Kenngröße eines „Frame Relay“-Zugangspunktes. Die im Abschnitt 2.8.2.2 genannte Überbuchung eines Frame Relay - Anschlusses kann im Multiplexer konfiguriert werden. Die aktuelle Konfiguration sieht laut Abbildung 5.1 eine statische Bandbreitenvergabe zwischen den DLCI 101 und DLCI 102 mit einer CIR = maximale Bandbreite = 192 kbit/s (bei K10) vor. Der Vorschlag lautet: Übergang von der statischen zu einer dynamischen Bandbreitenvergabe zwischen den DLCI's, welche in der Abbildung 5.3 veranschaulicht wird.



**Abb.5.3: Bandbreitenvergabe der DLCI's**

Frame Relay besitzt hinsichtlich der Rahmengröße (11...5004 Bytes) eine hohe Dynamik, welche zu einer optimalen Ausnutzung der bereitgestellten Bandbreite führt. Dabei werden die Rahmen der Nutzinformation angepaßt und keine Füllbits übertragen, was keine Erhöhung des Overheads im Netz bewirkt. Die dabei entstehende Bandbreiten-Reserve wird bei Vergabe eines DLCI's mit einer CIR von 192 kbit/s auftreten, wobei diese Reserve nicht durch eine weitere Verbindung genutzt werden kann. Bei den eingerichteten DLCI's handelt es sich um Verbindungen für den Normal- und Standby-Betrieb. Die Bandbreite des „Standby“-DLCI's wird daher nur im Fehlerfall genutzt. Bei dem Einsatz einer gegenseitigen Überbuchung werden beide DLCI's einer Verbindung auf eine CIR = 64 kbit/s gesetzt und entsprechend der noch zur Verfügung stehenden Bandbreite (restliche Datenübertragungskanäle) überbucht (bei K10 mit Faktor 4 = 256 kbit/s). In diesem Fall wird die sonst nicht genutzte Bandbreite für die WAN-Verbindungen im Normalbetrieb und im Fehlerfall (Nutzung von DLCI 102) bereitgestellt. Die weitere Reduzierung der CIR sollte erst nach Überprüfung der Routerkommunikation auf dem Reserve-Pfad (DLCI 102) erfolgen. Um die Bandbreite aller WAN-Verbindungen optimal auszunutzen, wird empfohlen, diesen Vorschlag auf allen Frame Relay - Verbindungen zwischen den Multiplexern umzusetzen. Insbesondere die WAN-Verbindungen K1 - K3 und K1 - K5 sind auf diese Weise zu optimieren. Mit dieser Maßnahme kann Bandbreite zum „Nulltarif“ bereitgestellt werden. Weitere Optimierungsmöglichkeiten des Frame Relays sind durch das RAPID (**R**eserved **A**lternate **P**ath with **I**mmEDIATE **D**iversion) - Verfahren gegeben. Bei diesem Verfahren wird in einem vermaschten Netz bei Ausfall einer Verbindung (Trunk) automatisch

ein vorkonfigurierter alternativer Pfad genutzt. Für den Einsatz dieser Funktion ist es sinnvoll, das Netz zwischen den Knoten K5, K10 und K15 zu vermaschen. Das so entstehende Netz besitzt eine maximale Verfügbarkeit. Aufgrund der hohen Kosten für die Festverbindungen ist derzeit jedoch ein Einsatz nicht zu empfehlen.

### 5.2.2 Router

Für eine Minimierung der Datenübertragungsrate kann auf den Routern eine Kompression eingesetzt werden. Für die Realisierung dieser Funktion müssen je nach Typ des Routers Hardware (Co-Prozessor) und Software (IP Access Suite) installiert werden. Die Kompression wird nach dem „Lempel Ziv“-Algorithmus vorgenommen, wobei die Daten ohne Verlust komprimiert über die WAN-Verbindung geleitet werden. Das Kompressionsverhältnis beläuft sich dabei auf 2,5:1. Bei der Übertragung der komprimierten Datenpakete können zwei Modi unterschieden werden. Im „kontinuierlichen“ Modus werden die Datenpakete eines vorgegebenen zeitlichen Fensters zusammengefaßt, komprimiert und als kontinuierlicher Datenstrom übertragen. Diese Methode erfordert den Einsatz einer Synchronisation der End-Punkte der Verbindung durch ein Data Link Protokoll, damit der Strom der komprimierten Datenpakete wieder zuverlässig getrennt werden kann. Im „Paket-Modus“ wird jedes einzelne Datenpaket einzeln komprimiert und übertragen, weshalb auf eine Synchronisation verzichtet werden kann. Für eine maximale Auslastung und eine hohe Geschwindigkeit auf der WAN-Verbindung ist eine Kompression im synchronen Modus zu empfehlen. Bei dem Einsatz sollten zuerst die Router auf den WAN-Verbindungen zwischen den Knoten um diese Funktion erweitert werden, was auch schon teilweise realisiert ist.

Für die Übertragung von zeitempfindlichen und wichtigen Informationen können für die Routerinterfaces Prioritäten gesetzt werden. Die Vergabe kann in Abhängigkeit vom Protokolltyp des Nutzdatenfeldes (SNA, NetBios), vom Quell- und Ziel-Netzsegment, vom übertragenden Paket-Typ (IP, IPX) und von weiteren Informationen des Paketkopfes erfolgen. Die Stufen der Prioritäten lauten: niedrig, normal und hoch. Im Rahmen der Vergabe von Prioritäten kann den Prioritätsklassen auch eine feste Bandbreite garantiert werden. Diese Bandbreite wird jedoch nicht statisch belegt, sondern nur im Überlastfall an den jeweiligen Protokolltyp vergeben. Da der gesamte Finanzdatenverkehr über SNA und die Kommunikation zu den Servern über NetBios abgewickelt wird, sollten die Prioritäten für diese Protokolltypen vergeben werden. Es wird dabei empfohlen, dem SNA-Verkehr 60 % und dem NetBios Verkehr 40 % zu garantieren. Mit dieser Verteilung können alle

zeitsensitiven Finanzdaten bevorzugt über hoch ausgelastete WAN-Verbindungen zum Host übertragen werden und auch eine Kommunikation zu den Servern mit verringerter Übertragungsgeschwindigkeit wird ermöglicht. Bei einem Übergang von DLSw zu einer „reinen“ TCP/IP-Adressierung des Host's sollte der Verkehr über die Zieladressen priorisiert werden. Der Verkehr zum Host-Netzsegment sollte auch hier wieder die höchste Priorität erhalten und eine Bandbreiten-Garantie von 60 % besitzen.

Mit dem weiteren Ausbau des Netzes hinsichtlich der verwendeten Applikationen, der Anzahl der Geschäftsstellen und der Nutzung breitbandiger Übertragungsverfahren kann die Leistung der ASN-Router durch den Aufbau eines Stacks und die Kopplung der Einheiten über den SPEX erhöht werden. Aufgrund des Einsatzes dieses Router-Typs in den Knoten müssen die vorhandenen Geräte bei einem Ausbau des Netzes nicht umgesetzt, sondern nur erweitert werden.

Die realisierte Möglichkeit des Aufbaus einer Wählbackup-Verbindung durch den Router kann auch im Überlastfall genutzt werden. Die Empfehlung lautet, daß die Dial-Up-Funktion der Router für den Überlastfall konfiguriert zu konfigurieren ist. So sollte bei einer Auslastung des Routerinterface von 95 % und nach dem Anhalten des Zustandes von einer Minute die Dial-Up-Verbindung über die geschlossene ISDN-Rufnummerngruppe (siehe Abschnitt 3.3) der Backup-Verbindung aufgebaut und so die Lastspitzen abgefangen werden. Bei einem Absinken des Verkehrsaufkommens auf unter 85 % und dem Anhalten dieses Zustandes sollte die Backup-Verbindung nach einer Minute wieder abgebaut werden.

### 5.2.3 Token Ring-Komponenten

Mit der Nutzung der in der IEEE 802.5 verabschiedeten Vergabe von Prioritäten kann eine Optimierung der Komponenten im Token Ring erreicht werden. Für die Optimierung des Backbones des Zentralknotens sind die Switches „Centillion 100“ in den Token Ringen mit der höchsten Priorität (P-bits = 8, siehe Abschnitt 2.8.1.2) zu versehen. Das Setzen der Priorität erlaubt die bevorzugte Reservierung von Frei-Token in den Ringen, wodurch die Switches ihre zu vermittelnden Datenpakete mit maximaler Geschwindigkeit in die Token Ringe leiten können. Ein Nichtsetzen der Priorität erzeugt einen „Flaschenhals“ zwischen den Bereichen SKP1 und SKP2 und bewirkt die Gleichbehandlung der Switches mit allen Netzstationen der angeschlossenen Token Ringe.

Mit der Ankopplung von „isolierten“ Servern an die Switches ist zwischen den Komponenten der Vollduplex-Modus einzusetzen. Das gleichzeitige Senden und Empfangen von Signalen

bewirkt eine Erhöhung der Übertragungsgeschwindigkeit der Serveranbindung auf bis zu 32 Mbit/s. Die Kombination aus beiden Verfahren erlaubt den Aufbau eines hinsichtlich der Übertragungsgeschwindigkeit gut strukturierten Backbones.

Für die Optimierung der Ankopplung der weiteren Server an die Token Ringe sind diese mit einer Priorität von 7 zu versehen, um alle auf die Server zugreifenden Netzstationen mit hoher Geschwindigkeit zu bedienen.

Die Geschwindigkeit der WAN-Übergänge in die LAN's ist durch Setzen der Priorität 6 für das Routerinterface zu erhöhen. Alle weiteren Netzstationen sind mit der niedrigsten Priorität zu versehen, um keine zu hohe Konkurrenz zwischen den Stationen zu erzeugen und um dabei keine Stationen vom Betrieb auszuschließen.

Wenn eine Priorisierung der Netzstationen eingesetzt werden kann, sollte dazu übergegangen werden, Multi-Port-Netzadapter in den Servern zu installieren. Aufgrund der mehreren Ports erhält der Server trotz gleicher Priorität öfter als alle anderen Netzstationen einen Frei-Token. Infolgedessen können die Netzstationen je nach Port-Anzahl eines Servers schneller bedient werden.

### 5.3 Sicherheit im Netz des Institutes

Für die Erhöhung der Sicherheit im Netzwerk des Institutes ist es notwendig, die realisierten Maßnahmen zu betrachten. Die derzeitigen Sicherheitsmaßnahmen für das Netz sind:

- Geschlossene Rufnummerngruppen im ISDN der Deutschen Telekom AG,
- Nutzung der Netzressourcen durch Login am zuständigen Domain Control Server und damit Vergabe von Netzressourcen durch Einführung von Domänen,
- Freigabe der Netzressourcen durch Zuweisung durch den DV-Verantwortlichen,
- Bildung einer STUB-Area im Backbone des Rechenzentrums und damit Realisierung einer geschlossenen OSPF-Area gegenüber den weiteren Instituten des Verbandes und Durchsetzung dieser Maßnahme auf allen Routern des Kreditinstitutes (von der Siemens AG zusätzlich durchgeführt),
- Standard-Login's an den NMS-Stationen (DMS, Optivity für NetView und Mainstreet),
- Standard-Passwörter an den Netzkomponenten wie Routern, Switches und Hubs,
- Zentralisierung des Finanzdatenverkehrs auf den Host.

Die genannten Maßnahmen stellen einen grundsätzlichen Schutz des Netzes bereit. Aufgrund der derzeitigen und künftigen Aufgaben des Netzes und den damit verbundenen Sicherheitsanforderungen können die Maßnahmen keinesfalls als ausreichend angesehen werden.

### 5.3.1 Schutzbedürfnisse

Ein Schutzbedürfnis besteht nicht nur hinsichtlich des unberechtigten Zugriffs von außen, sondern es ist ein wesentlich umfassenderes Schutzbedürfnis vorhanden. Die Schutzvorkehrungen sind wie folgt zu unterscheiden.

#### a) *Schutz vor unberechtigten Zugriffen von Mitarbeitern des eigenen Institutes*

Dieser Schutz beinhaltet alle Verfahren und Maßnahmen zur Begrenzung der Möglichkeiten eines Mitarbeiters und eine Garantie über ein begrenztes Wissen (soviel wie nötig). Speziell diese Maßnahme ist ein wesentliches Kriterium für die Sicherheit im Institut, weil die problemlose netzweite Kommunikation optimal, aber nicht sicher ist. Gerade die Mitarbeiter des Institutes können durch Unwissenheit oder Vorsatz den höchsten Schaden verursachen, weil sie besser als jeder andere die Struktur des Netzes bzw. des genutzten Netzabschnitts kennen.

#### b) *Schutz vor unberechtigten Zugriffen von Mitarbeitern der Institute des Verbandes*

Diese Maßnahmen beinhalten den Schutz vor den Instituten des Verbandes, weil mit der Nutzung eines gemeinsamen Rechenzentrums die Kreditinstitute über gemeinsame Router und FEP's im Backbone des RZ integriert sind. Die überregionale Nutzung von Kreditinstituten durch den Kunden verstärkt die Wettbewerbssituation untereinander, obwohl die geographischen Grenzen zwischen den Wirkungsbereichen der Institute klar definiert sind.

#### c) *Schutz vor unberechtigten Zugriffen von Mitarbeitern des Rechenzentrums*

Diese Maßnahmen dienen der Erreichung einer Selbständigkeit des Institutes in Bezug auf Datenkommunikation, weil durch die Nutzung der Mitarbeiter des RZ zusätzliche Kosten entstehen. Für das Vorbeugen fehlerhafter Handlungen ist auch in diese Richtung ein Schutz vorzusehen. Die dabei entstehenden definierten Grenzen führen zur einer

eindeutigen Klärung von Schuldfragen bei Ausfall von Verbindungen zum Host und den damit verbundenen finanziellen Verlusten des Kreditinstitutes.

d) *Schutz vor unberechtigten Zugriffen von sonstigen Personen*

In diesen Sicherheitsmaßnahmen sind alle Funktionen zum Schutz vor „fremden“ Personen enthalten, die sich zufällig oder arbeitsbedingt in Räumen des Kreditinstitutes aufhalten oder anderweitig mit dem Kreditinstitut kommunizieren. Bei diesen Personen handelt es sich um Servicetechniker, Lieferanten, Vertreter und sonstige Personen, die in die Sicherheitsbereiche einen Zutritt erhalten und dort über einen begrenzten Zeitraum tätig sind. Zusätzlich beinhalten diese Maßnahmen alle Funktionen zum Schutz vor Personen, die über Online-Dienste oder über ähnliche Kommunikationseinrichtungen bzw. -Verfahren mit dem Kreditinstitut in Verbindung treten.

### **5.3.2 Maßnahmen zur Erhöhung der Sicherheit**

Die folgenden Empfehlungen beinhalten alle im Abschnitt 5.3.1 genannten Schutzfunktionen, weshalb die Maßnahmen zusammen eine optimale Sicherheit im Netzwerk gewährleisten. Die Empfehlungen für die Erhöhung der Sicherheit können nach dem Inhalt klassifiziert werden.

#### Organisatorische Maßnahmen

- 1) Keine Nutzung von Standard-Paßwörtern, wie Namen oder Begriffe, weil diese Begriffe über zyklische Routinen schnell erkannt bzw. erraten werden. Es ist die Nutzung von Zufallsgeneratoren zur Erzeugung der Paßwörter zu empfehlen. Weiterhin sollten die Paßwörter aus einer Buchstaben-Zahlen-Zeichen-Kombination bestehen und nie die minimale Länge besitzen (mindestens 10 Zeichen).
- 2) Umfassende Vergabe von Paßwörtern für die Datenbanken und Dateibereiche, um eingedrungenen und sonst nicht zuständigen Personen den Zugriff auf die Netzressourcen zu erschweren bzw. unmöglich zu machen.

- 3) Schutz der Sicherheitsbereiche durch Verschuß und Vermeidung offenstehender Türen in der Ausbauphase. Ständige Beaufsichtigung von Servicetechnikern „fremder“ Unternehmen durch Mitarbeiter des Kreditinstitutes.
- 4) Keine Vergabe von Standard-Paßwörtern (Techniker-Paßwörter) an Mitarbeiter von Kreditinstituten für Konfigurationen oder Neustarts der Router des Rechenzentrums. Diese Paßwörter schaffen die Möglichkeit eines Mißbrauchs von Routern weiterer Kreditinstitute. Es sollte somit immer versucht werden, daß Mitarbeiter von Kreditinstituten keine oder nur speziell für **einen** Router gültige Paßwörter erhalten. Diese Maßnahme ist mit den Verantwortlichen des Rechenzentrums abzustimmen.
- 5) Es sind zwischen dem Kreditinstitut und dem Rechenzentrum Verhandlungen über die künftige Gewährleistung der Netzwerksicherheit zu führen, wenn das Rechenzentrum als alternativer Telekommunikationsanbieter auftreten sollte. Im gleichen Maße sind auch die Fragen der zukünftigen Kosten (eventuell Reduzierung) zu klären, weil die Kreditinstitute jährlich Kosten für die Unterhaltung des Rechenzentrums mit seinem Equipment und Mitarbeitern aufwendet.
- 6) Es wird weiterhin empfohlen, den Abgleich von Kundeninformationen nicht in breitbandigen und zusammenhängenden Kommunikationsbeziehungen vom Rechenzentrum aus vorzunehmen, weil dies eine eindeutige Verkehrsflußanalyse (Auftreten eines Maximum) erlaubt und die Informationen dabei leicht abzufangen wären. Es sollte vielmehr dazu übergegangen werden, die Dateitransfers nur abschnittsweise und mit einer geringen Übertragungsrate durchzuführen. Damit können die umfangreichen Kunden- oder Finanzdaten nicht eindeutig lokalisiert und gezielt abgefangen werden.
- 7) Empfehlung der Unterbindung der dezentralen Kommunikation zu Online-Diensten, Internet-Providern, Mail-Boxen über Modems und ISDN-Adapterkarten an den Arbeitsplätzen der Mitarbeiter. Bei dem Einsatz dieser Komponenten und der Existenz eines LAN-Netzadapters in einem System kann der PC von einem Eindringling als Router benutzt werden und damit kann auf einfache Weise in das Netz des Institutes eingedrungen werden. Die Adressen (MAC und IP) – Listen in den Hubs und Routern sind dabei unwirksam, weil sich der Eindringling als Nutzer des Netzes identifiziert. Dieser Eindringling kann damit problemlos zu Nodes des Institutsnetzes und des Rechenzentrums



vordringen und diese angreifen. Die langen Download-Zeiten der Internet-Provider wären für den Angriff vorteilhaft, weil damit genug Zeit bestünde, Sicherheitslücken zu testen und danach Änderungen an den Netzkomponenten vorzunehmen (Paßwörter, Routen, Filter oder Dial-Up-Telefonnummern). Als sofortige Maßnahme sind die Modems zu entfernen und Stand-Alone-PC-Systeme für den Zugriff auf Online-Dienste zu errichten, welche keine Netzverbindung besitzen. Ausgehend davon und von der vorhandenen Forderung nach Online-Diensten ist künftig der Einsatz von Firewall-Systemen im Netz des Kreditinstitutes in Betracht zu ziehen.

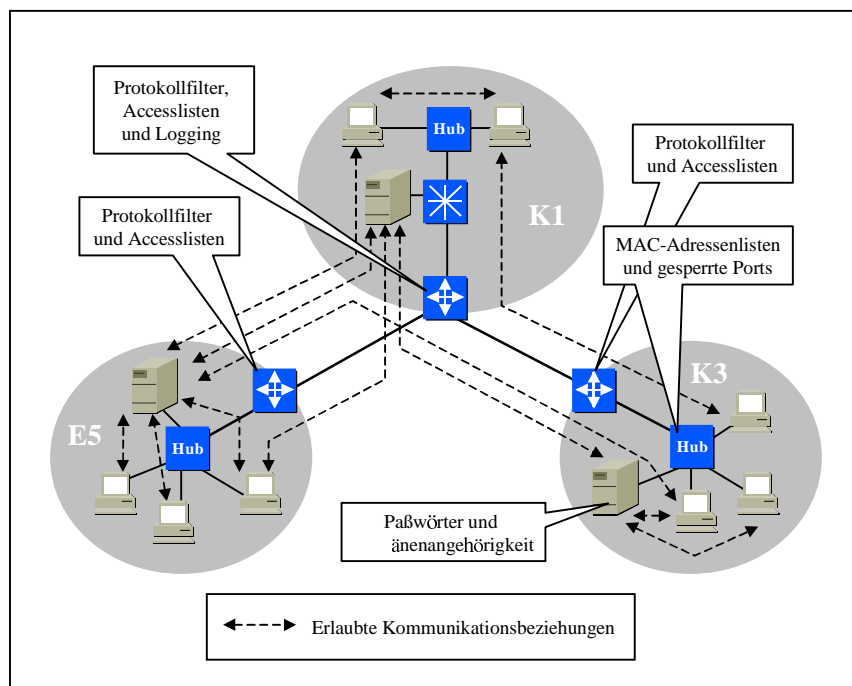
[For 96], [Eber 94], [FW 96]

### Technische Maßnahmen

- 8) Sperren aller freien Ports an den Routern, Hubs, Switches und weiteren Kommunikationszugängen, weil sonst unbeaufsichtigte Personen (Servicetechniker) leicht einen Zugang zum Netzwerk erhalten.
  - 9) Nutzung der Konfiguration der MAC-Adressenlisten der Hubs, damit auch bei Sperrung der Ports keine Person durch Abziehen einer Netzadapter - Verbindung Zugang zum Netzwerk erhält. Der Hub verwaltet dabei die „eingebrennten“ MAC-Adressen der zugelassenen Netzadapter und sperrt bei Änderung der MAC-Adresse den Port. Weiterhin verhindert die Liste das Umstecken zugelassener Adapter am Hub, wodurch auf dem Hub mehrere geschlossene Benutzergruppen sicher gebildet werden können.
- [S5 96]
- 10) Nutzung der Access-Listen und Protokollfilter der Router zwischen den Standorten, weil mit der Möglichkeit der Filterung von Datenpaketen die Mitarbeiterzugriffe zwischen den Standorten kontrolliert und wenn nötig verhindert werden können. Bei der Konfiguration von Filtern können z.B. alle Informationen des DCS und der Backup-DCS durchgelassen werden und gleichzeitig alle Zugriffe der Mitarbeiter auf weitere Standorte abgelehnt werden. Zusätzlich können definierte Personen von diesem Standort auf benötigte Server weiterer Standorte zugreifen. Die Abbildung 5.4 veranschaulicht die Zugriffe. Der Einsatz dieser Protokollfilter erhöht gleichzeitig die Sicherheit des Domänenkonzeptes, weil damit nur so viele Mitarbeiter wie nötig Zugriff auf die Netzsegmente erhalten. Somit wird die derzeitige Problematik vermieden, daß ein Eindringling (oder Mitarbeiter) auch ohne Anmeldung an einer Domäne eine beliebige Station im gesamten Netzwerk des Institutes

angreifen kann. Die Domain Control Server verwalten und schützen nur die Rechte an den Netzressourcen und nicht die Zugangspunkte zu den Netzsegmenten. Neben der Verwendung von Protokollfiltern besteht die Möglichkeit des Einsatzes einer Logging-Funktion auf den Routern zur Protokollierung der Ablehnung von Datenpaketen und der Identifizierung des Angreifers. Für den Einsatz von Protokollfiltern in den Routern ist die aktuelle Prozessorauslastung dieser Systeme zu überprüfen (aktueller Wert = 10 %). Ausgehend von diesem Wert ist der Umfang der zu setzenden Filter festzulegen.

[BS 96], [Bay], [BLN 96]



**Abb.5.4: Zusammenwirken von möglichen Sicherheitsmaßnahmen**

- 11) Es wird für die Zukunft Übergang zu dem im Abschnitt 2.7.8 beschriebenen SNMPv2 empfohlen, weil bei dieser Version die Paßwörter für die administrierten Nodes verschlüsselt, und nicht wie bei SNMPv1 unverschlüsselt, übertragen werden. Mit dem Abfangen oder sonstigen Bekanntwerden des Paßwortes eines Routers könnte ein Angreifer das Paßwort auf dem Router ändern und den Router umkonfigurieren (Beseitigung von Adressen-Filter und Routen). Infolgedessen kann der Systemadministrator keine kurzfristige Rekonfiguration vornehmen. Bei dem Router BLN-2 oder Switch Centillion 100 würde dies gesamte Netzsegmente abkoppeln und zu einer starken Beeinträchtigung der Funktionsfähigkeit des Netzes führen.

- 12) Aufbau von zwei Sicherheitsdomänen, in denen sich nur die zugelassenen Personen befinden.

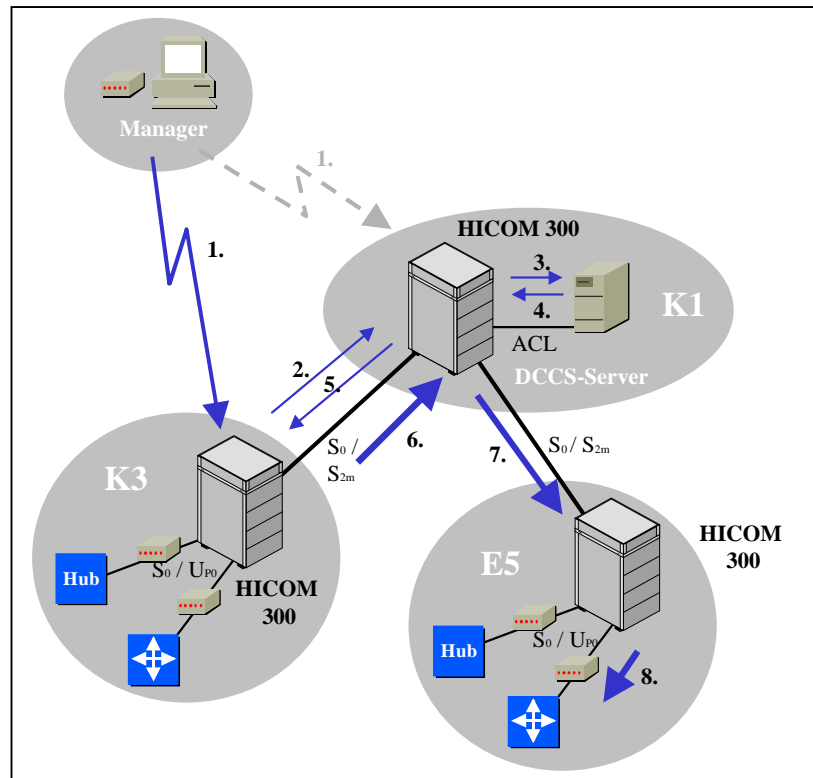
**Domäne 1:** alle Personen und Netzkomponenten, welche **allgemeine** Informationen (z.B.: Bestellungen, Rundschreiben, E-Mail, Software) nutzen bzw. bereithalten

**Domäne 2:** alle Personen oder Server, die wichtige zentrale Datenbanken für die gesamten Finanzdienstleistungen laut Abschnitt 3.4.5 (z.B.: E12 und E17) und genaue personenbezogene Informationen (z.B.: Unterschriften) bearbeiten bzw. bereitstellen

- 13) Bildung einer allseitigen STUB-Area gegenüber allen Netzzugängen, weil künftig vier Zugänge zum Backbone des Rechenzentrums bestehen und damit die Möglichkeiten des Zugriffs auf Netzressourcen durch Mitarbeiter weiterer Institute, dort eingedrungene Personen oder Mitarbeiter des Rechenzentrums bestehen. [BS 96]

- 14) Einsatz eines **Data Connection Control System-Servers** für die Bereitstellung eines „Out of Band“-Managements für die Hubs und Router in den Knoten. Mit dem Einsatz dieses Servers im Zentralknoten werden alle eingehenden Anrufe für die Telefonnummern der Modems entgegengenommen, überprüft und bei Richtigkeit der Verbindung zum Modemanschluß ermittelt. Die Identifizierung des Teilnehmers erfolgt anhand der Rufnummerninformation des ISDN-D-Kanals, welche durch den Teilnehmer nicht manipuliert werden kann. Eine zusätzliche Sicherheitsmaßnahme dabei ist der Abbruch der Verbindung durch den DCCS-Server und der Aufbau einer Call-Back-Verbindung zum Teilnehmer mit der registrierten und vorher erkannten Rufnummer. Mit dieser Identifikation und Kontaktaufnahme wird sichergestellt, daß sich nur der gewünschte Teilnehmer in die Modems einwählen kann. Für die Realisierung dieser Funktionen im gesamten Netz des Kreditinstitutes muß zwischen den Standorten mit PBX-Systemen und dem DCCS-Server ein B-Kanal bereitgehalten werden, worüber der DCCS-Server mit der HICOM 300 kommuniziert und die Daten für das Anschluß-Monitoring übertragen werden. Die Verbindung wird über einen **Application Connectivity Link (ACL)** aufgebaut und ständig aufrecht erhalten. Die Abbildung 5.5 veranschaulicht die Zusammenhänge.

[DCCS 97]



**Abb.5.5: Einsatz eines DCCS**

#### Die Schritte des Verbindungsaufbaus

1. Manager wählt sich an einem beliebigen Standort in die PBX des „Corporate Network“ des Institutes ein.
- 2.+3. Die den Anruf annehmende PBX HICOM 300 leitet die Rufnummern-Information zum DCCS-Server über den ACL-Link, welcher auf der Festverbindung über einen B-Kanal aufgebaut wurde. Der DCCS-Server überprüft den rufenden mit dem gerufenen Teilnehmer und leitet eine der folgenden möglichen Berechtigungsaktionen ein:
  - Zulassen
  - Zulassen und Protokollieren
  - Abwurf zu anderem Teilnehmer
  - Abwurf und Protokollieren
  - Verhindern
  - Verhindern und Protokollieren

- 4.+5. Die auszuführende Aktion wird an die HICOM 300 übermittelt und von dieser ausgeführt (z.B.: Zulassen). Zusätzlich kann die aufgebaute Verbindung unterbrochen und ein Call Back (Rückruf) durchgeführt werden.
- 6.+7. Der Kanal wird durch das Netz zum Anschluß des Modems vermittelt.
8. Der Manager erhält Zugriff auf das „Out of Band“- Management – Modem des Routers und kann dort nach erfolgter Synchronisation administrative Aufgaben wahrnehmen. [DCCS 97]

Mit dem DCCS steht ein ISDN-Firewall-System zur Verfügung, welches ständig mit den Knoten (HICOM 300) des privaten ISDN-Netzes kommuniziert. Für das Zustandekommen einer vom DCCS geschützten Rufnummer werden interne wie auch externe Datenverbindungen zu diesen Rufnummern über ISDN-Anrufer-Identifikation überprüft und gegebenenfalls zugelassen. Das DCCS-System ist für Windows NT oder Windows 95 konzipiert, weshalb das System eine einfach zu bedienende Oberfläche besitzt. Das DCCS-System ist eine spezielle Entwicklung der Siemens AG für das PBX-System HICOM 300, welche im Netzwerk des Kreditinstitutes zum Einsatz kommen kann.

Die Modems für das „Out of Band“- Management der Multiplexer können mit dieser Lösung geschützt jedoch im Fehlerfall nicht angesprochen werden, weil bei Ausfall eines Multiplexers die Verbindung zum Zentralknoten unterbricht und damit keine Autorisierung des „Out of Band“- Manager erfolgen kann. Die Multiplexer müssen über ein separates Sicherheitssystem verfügen oder über die Wählbackupverbindungen der Router erreichbar sein.

Abschließend wird empfohlen, eine umfassende Studie zu erstellen, die eine Bedrohungsanalyse enthält und sich **nur** mit dem Thema Sicherheit im Netzwerk des Kreditinstitutes beschäftigt. Diese Studien zeigen detailliert die Möglichkeiten des Eindringens in Netzwerke auf und enthalten weitere Vorschläge zur Netzgestaltung. Ein Beispiel dafür sind die an der Universität Rostock durchgeführten Sicherheitsanalysen der Diplomarbeit [Hab 97].

## **5.4 Komponenten und Protokolle zur Erhöhung der Netzfunktionalität**

### **5.4.1 HICOM 300E**

Die PBX HICOM 300E stellt eine Weiterentwicklung der im Institut eingesetzten HICOM 300 dar. Die Erweiterungen beziehen sich auf die Sprach-Daten-Integration und den

Übergang zur Bereitstellung von breitbandigen Datenübertragungskanälen. So erlaubt die HICOM 300E die Blockbildung von ISDN-B-Kanälen zu H-Kanälen, welche die B-Kanäle zusammen und nicht nacheinander aufbauen.

Die möglichen H-Kanäle besitzen folgende Datenübertragungsraten:

$$H0 = 6 \times 64 \text{ kbit/s} = 384 \text{ kbit/s}$$

$$H11 = 24 \times 64 \text{ kbit/s} = 1536 \text{ kbit/s}$$

$$H12 = 30 \times 64 \text{ kbit/s} = 1920 \text{ kbit/s}$$

[LL 3/97]

Zusätzlich erlaubt der Einsatz einer ATM - Interworking Unit (IWU) den Anschluß und die Kommunikation der PBX mit einem ATM-Netz mit einer Übertragungsgeschwindigkeit von 155 Mbit/s. Aufgrund dieser Funktionen kann eine Sprach-Datenintegration im ATM-Backbone erreicht werden. Weiterhin ist das Vernetzungsprotokoll Cornet-N, QSIG und E-DSS1 im gesamten PBX-Verbund verfügbar. Alle Anwender können so über das ATM-Netz oder über die ISDN-Festverbindungen die Leistungsmerkmale nutzen. Die ATM-IWU schafft weiterhin eine Kopplung von ISDN und ATM, wobei kundenspezifische Lösungen mit einem Application Connectivity Link (ACL) und Call-Center-Lösungen (ACD) eine einfache Implementierung erfahren. Mit den genannten Verfahren kann der Service, die Effizienz und die Sicherheit der Kommunikation eines Unternehmens erhöht werden.

Mit dem Einsatz eines ISDN-Routers für Remote-Zugriffe auf die HICOM kann eine einfache Fernwartung der Anlage und eine gleichzeitige Nutzung von weiteren ACL-basierenden Anwendungen erfolgen, wobei mehrere Baugruppen (Modems, ISDN-Adapter) für die jeweiligen Applikationen entfallen und damit Kosten gespart werden.

Die HICOM 300E unterstützt die Kommunikation in einer homogenen HICOM 300E-Umgebung und die Sprachkompression nach G.728, welche das Low Delay – CELP Verfahren enthält. Das Verfahren ermöglicht durch die Kompression eine Verzögerung von unter zwei Millisekunden, so daß die Echokompensationsverfahren entfallen können. Dabei wird eine Kompression um Faktor 4 erreicht. Die so entstandenen Sprachsignale werden durch HICOM 300E - Systeme mit Unterstützung dieser Funktionalitäten transparent weitergeleitet. Die Vermittlung von komprimierten Informationen umgeht das Problem des hohen Qualitätsverlustes bei mehrfacher Kompression und Dekompression und erlaubt den Aufbau von Netzen mit hoher Sprachqualität und geringen Kosten für gemietete Festverbindungen zwischen den Standorten. Sinnvollerweise werden Fax-Signale der Gruppe 3 durch das

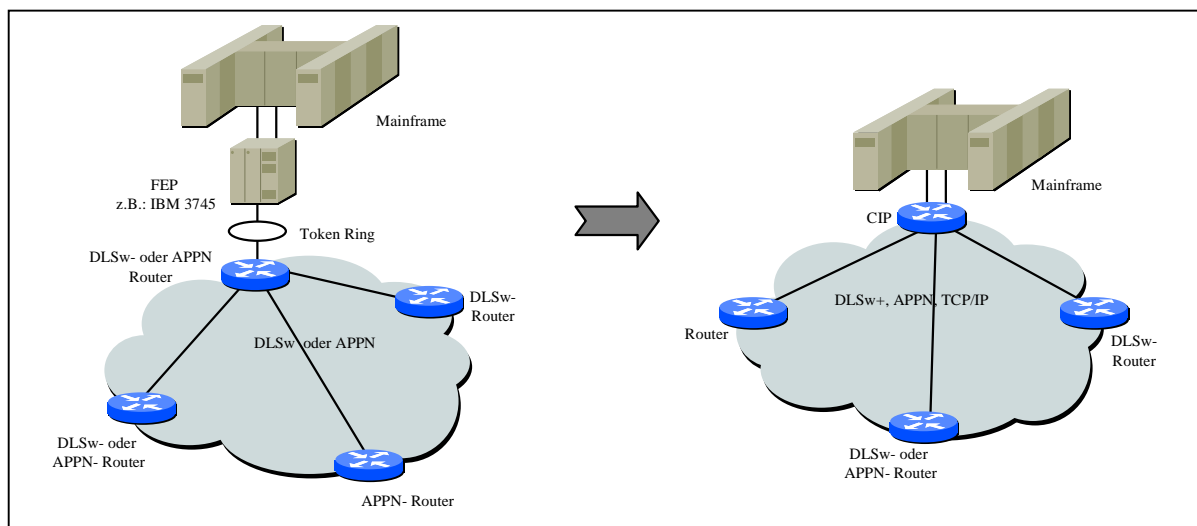
Kompressionsmodul erkannt und transparent weitergeleitet. Die HICOM 300E unterstützt auch die Integration von schnurlosen Telefonen, die nach dem DECT-Standard mit der Basisstation kommunizieren. In Abhängigkeit von der Teilnehmerzahl können die Sprachkanäle bedarfsorientiert zugewiesen werden.

Ein weiterer Vorteil der HICOM 300E besteht in der Möglichkeit des sanften Übergangs zu diesem HICOM-Typ, weil die Baugruppen früherer HICOM 300 - Systeme in diesem Typ weiterhin genutzt werden können. Diese Möglichkeit schafft eine stufenweise Migration, wobei die getätigten Investitionen langfristig geschützt werden.

Insgesamt eröffnet dieses System einen Weg zur Sprach-Daten-Integration in einem ATM-Backbone, den netzweite Einsatz von Kompression zur Reduzierung von Leitungskosten, die Erhöhung des Servicegrades eines PBX-Verbundes, die problemlose Anbindung von lokalen DECT-Funkstationen und die Bereitstellung von H-Kanälen für eine breitbandige Kommunikation im ISDN. Aufgrund dieser Funktionen und der Tatsache, daß die Baugruppen vorhandener HICOM 300 - Systeme weiter genutzt werden können, wird empfohlen, diesen PBX-Typ für künftig auszubauende Standorte einzusetzen. Der Einsatz wäre ein Investitionsschutz, weil diese PBX sowohl die aktuellen Standards des breitbandigen ATM, die Vorteile einer Sprach-Daten-Integration (z.B.: für ACD), als auch die kostenreduzierende Kompression von Sprachkanälen (nach G.728) unterstützt. Der Einsatz einer netzweiten **Kompression der PBX** wird die **transparente Durchschaltung** der Kanäle durch die **Multiplexer** bedingen, wobei alle geplanten Sprachkanäle auf den Festverbindungen reduziert werden könnten. Die dabei frei werdenden Sprachkanäle könnten für den Aufbau eines WAN mit hoher Bandbreite eingesetzt werden. Auf diese Weise kann die Bandbreite für die WAN-Verbindungen erhöht oder die Anzahl der TS02 - Verbindungen verringert und so die Kosten für die Festverbindungen minimiert werden. Die Festverbindungen könnten bis auf eine TS02-Verbindung zwischen den Geschäftsstellen reduziert werden. Der Übergang von T2MS auf TS02 sollte nicht vorgenommen werden, weil für den Einsatz von zwei TS02-SFV die gleichen Kosten wie für eine T2MS-SFV (außerhalb der Ortszone 1) aufzuwenden wären. Bei einem Anschluß an das zukünftige Corporate Network des Rechenzentrums wäre zu empfehlen, daß auch diese Institution die Funktionen dieses PBX-Typs unterstützt. Die Einführung eines Corporate Networks durch das Rechenzentrum sollte sich dabei nach dem Equipment der Institute richten, um eine hohe Kompatibilität zu erreichen und die Investitionen der Institute nicht in Frage zu stellen. Mit wachsender Akzeptanz der eingesetzten Technik werden auch die Institute die Dienste des Rechenzentrums im stärkerem Maße nutzen.

### 5.4.2 CIP

Mit der Erweiterung der Netze der Institute und der verstärkten Nutzung von IP in diesen Netzen werden zukünftige Applikationen mehr und mehr über TCP/IP (Abschnitt 3.2.3.1) kommunizieren. Um die Kommunikation zum SNA-Host aufrechtzuerhalten, werden Techniken wie DLSw und APPN eingesetzt. Die vorhandene Struktur der Kommunikation zum Host ist im Abschnitt 3.2.3.2 dargestellt. Ausgehend von der Darstellung kann erkannt werden, daß die gesamte Kommunikation über eine Vielzahl von Routern und dann über einen FEP zum Host vorgenommen wird. Diese Lösung wird sich auf lange Sicht nicht durchsetzen, da die FEP's hohe Unterhaltungskosten verursachen, auf die Kommunikation mit dem Mainframe spezialisiert sind und nicht die Vielzahl von Schnittstellen und Protokollen eines Routers unterstützen. Eine kostensparende Lösung wäre es, den Mainframe direkt an einen Router zu koppeln und damit die Kommunikation im WAN- und LAN-Bereich zu realisieren. Der **Channel Interface Prozessor** stellt eine Entwicklung der Fa. Cisco Systems dar. Diese Netzkomponente beinhaltet einen Router, der direkt über eine Busverlängerung („ESCON“ oder „Bus and Tag“) an den Mainframe gekoppelt wird. Der CIP kommuniziert direkt mit dem Host und ermöglicht dabei eine für TCP/IP optimierte Kommunikation mit dem Host. Der Einsatz des CIP gestaltet sich folgendermaßen.



*Abb.5.6: Einsatz eines CIP [CIP 95]*

Mit dem Einsatz eines CIP kann der FEP eingespart und weiterhin eine Kommunikation zum Host gewährleistet werden. Die vorhandenen Router für APPN und DLSw können weiter



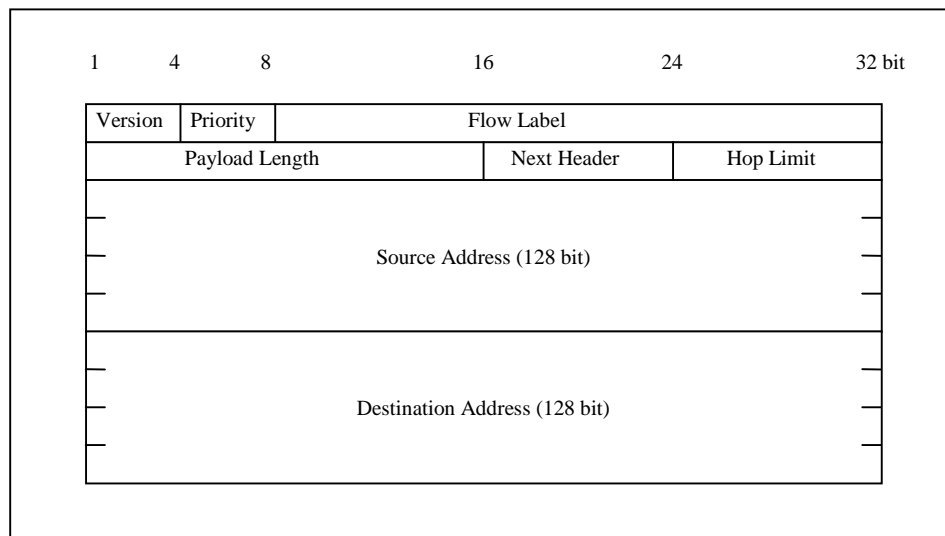
genutzt werden. Zusätzlich kann dazu übergegangen werden, den Host mit TCP/IP zu adressieren. Aufgrund der dadurch erreichten Kompatibilität kann ein Mainframe einfach in vorhandene oder neu aufzubauende IP-Netze integriert werden. Für das Institut wäre die Nutzung eines CIP vorteilhaft, weil der Host jetzt über TCP/IP zu adressieren wäre und das vorhandene DLSw nach RFC 1434 durch DLSw+ weiter unterstützt wird. Zusätzlich erlaubt das DLSw+ den Aufbau eines „On Demand Peer“-Netzes, in dem im Gegensatz zum DLSw mit seiner permanenten TCP-Session ein Dial on Demand Routing ausgeführt wird. Ein Einsatz von CIP's führt zu einer flexiblen Kommunikation im Netz des Rechenzentrums, wobei das Problem der SDLC-Verbindungen vom Host zu den Übergangspunkten in den Rechenzentrum-Backbone besteht. Der CIP muß mit seinem Channel-Interface am Standort des Host eingesetzt werden. Mit der Möglichkeit des Anschlusses von ATM- und E1-Festverbindungen an den CIP können die geschalteten Festverbindungen weiterhin betrieben werden. Die Bestrebungen des Rechenzentrums, als alternativer Netzanbieter aufzutreten, werden den Einsatz von Multiplexern, PBX-Systemen und Routern an den Übergangspunkten bedingen. Über diese Komponenten kann damit eine Informationsweiterleitung zu den Standorten der Institute erfolgen. Die Institute können so über eine definierte Bandbreite z.B.: 64 kbit/s über den CIP auf den Host zugreifen. Ein weiterer Vorteil wäre die zentrale Stellung des CIP's am Host, wodurch das Rechenzentrum jederzeit eine hohe Verfügbarkeit des „FEP – Ersatzes“ garantieren kann. Aufgrund der genannten Tatsachen bewirkt der Übergang zu CIP's die Migration zu künftigen Übertragungsverfahren und Applikationen, welche ohne Tunneln und mehrfache Protokollumsetzung den Host direkt adressieren und mit einer hohen Bandbreite nutzen können. Der CIP ist derzeit für das System Cisco 7000 verfügbar, wobei das System ständig in seiner Leistung und in seinem Funktionsumfang (CIP 2) weiterentwickelt wird. Mit dem Einsatz von CIP's können die Kosten der Kreditinstitute des Verbandes verringert und die Kommunikation zum Host verbessert werden, wobei dazu eine umfassende Studie zu erarbeiten ist. Bei einer solchen Studie ist die Möglichkeit des Einsatzes von IPv6 zu berücksichtigen, weil dadurch die Realisierung des Vorschlages im Abschnitt 5.4.3 begünstigt wird.

[DL+ 96], [CIP 95]

### 5.4.3 IP Version 6

Die wachsende Akzeptanz des Internets und der damit verbundene Mangel an Adressen führte zur beschleunigten Weiterentwicklung des im Abschnitt 3.2.3.1 beschriebenen Internet Protokolls in der Version 4 zu der IP Version 6. Die Spezifikation für dieses Protokoll ist im

RFC 1883 enthalten, der im Dezember 1995 veröffentlicht wurde. Mit dem Übergang von 32 bit-Adressen zu 128 bit-Adressen können jetzt  $3,4 \times 10^{38}$  Netzstationen adressiert werden. Für die Veranschaulichung wurde die Header-Struktur in der Abbildung 5.7 dargestellt.



**Abb. 5.7: IPv6 – Header** [PCN 10/96]

#### Felder im Header:

Version: enthält Kennung für verwendete IP-Version des Paketes,

Priority: Vergabe von Prioritäten für Bevorzugung von Datenpaketen bei der Weiterleitung,

Die Vergabe gestaltet sich folgendermaßen: 0-7 lastgesteuerter Verkehr,

8-15 nicht lastgesteuerter Verkehr  
(Echtzeit),

Flow Table: Nutzung vom Sender zur Kennzeichnung von zusammengehörigen Datenpaketen, die von Routern gesondert behandelt werden müssen, um bestimmte Qualitätsmerkmale (Echtzeitinformationen) zu erfüllen,

Payload Length: Länge des gesamten Pakets einschließlich Erweiterung-Header und Daten,

Next Header: Kennung, ob nach dem Standard-Header ein Extension-Header folgt,

Hop Limit: Zähler, der für die Kontrolle beim Source Routing benötigt wird (vergleichbar mit „Time to Live“ - Feld in der Version 4 (Abb. 3.15),

Source Address: Absenderadresse im 128 bit - Format,

Destination Address: Zieladresse im 128 bit – Format.

Die Adressen bei IPv6 werden über bis zu vier zusammenhängende Ziffern und Buchstaben im hexadezimalen Format angegeben und durch Doppelpunkte getrennt (z.B.:

**FFC:CD3:0:0:0:0:232:2**), wobei auf die Nullen verzichtet werden kann (z.B.: **FFC:CD3::232:2**). Bei gemischten Umgebungen von IPv4 und IPv6 kann die 4Byte-Adresse der Version 4 (z.B.: **22.10.100.300**) in der Version 6 in der alten Notation angegeben werden (z.B.: **::22.10.100.300**).

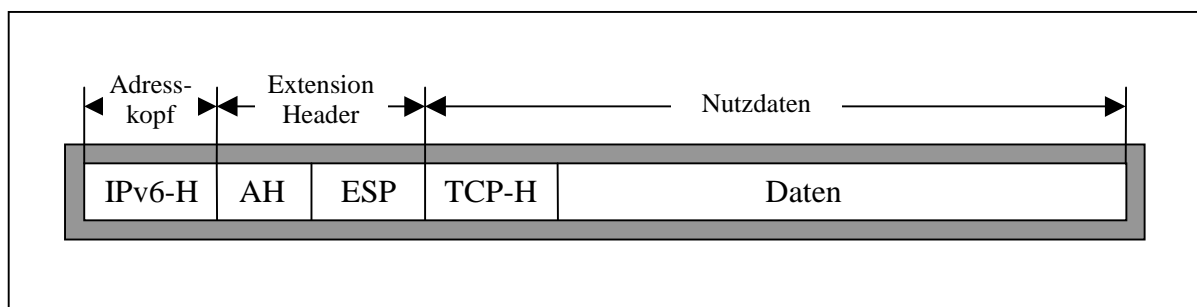
Um die Headergröße zu reduzieren und um keinen zu hohen Overhead im IP-Netz zu erzeugen, wurde der dargestellte Adressenkopf des IP-Paketes wesentlich vereinfacht. Zur Realisierung zusätzlicher Funktionen wird dieser Standard-Header um die sogenannten „Extension Header“ erweitert.

Bisher sind folgende Extensions definiert worden.

- Hop-By-Hop Options
- Destination Options
- Routing
- Fragment
- Authentication
- Encapsulation
- Resource Reservation
- Interdomain Routing

Weitere optionale Header können später entwickelt werden.

Der Standard-Header wird, wie in der Abbildung 5.8 dargestellt, erweitert, wobei die Verknüpfung der aufeinanderfolgenden Protokolle durch das dem jeweiligen Header vorangestellte „Next Header“ und „Header Length“ – Feld erfolgt.



**Abb. 5.8: Struktur eines erweiterten IPv6-Paketes**

[Wun 97]

Die Abschnitte lauten:

IPv6-H: Standard-Header der IP Version 6

- AH: Authentication Header dient zur Überprüfung der Echtheit eines Absenders und der Erkennung der Unverfälschtheit eines Datenpaketes (AH mit MD5-Schlüssel RFC 1828)
- ESP: Encapsulated Security Payload dient zur Mitteilung, daß die nachfolgenden Nutzdaten verschlüsselt sind, wobei hier nicht die Methode durch IPv6 vorgegeben wird (RFC 1827)
- TCP-H: Transmission Control Protocol-Header bei einem TCP/IP-Paket

Zusätzlich werden bei IPv6 sogenannte „Plug and Play“-Funktionen implementiert, die es erlauben, durch das Protokoll einer neu hinzugekommenen Netzstation automatisch eine IP-Adresse zuzuweisen. Wird eine schon belegte IP-Adresse erkannt, wird die vorhandene automatisch geändert. Mit dieser Funktion können viele Installationsprobleme umgangen werden. Weiterhin erlauben die schon vorgesehenen Header für Security den Einsatz von Verschlüsselung im IP-Paket (TCP-Header + Nutzdaten), womit diese Option einfach zu implementieren ist und damit auch oft eingesetzt werden kann. Die Vergabe von Prioritäten und die Kennzeichnung von „Flow Labels“ ermöglicht die kontrollierte Übertragung von multimedialen Informationen über ein IP-Netz. Der ARP-Prozeß von IP wurde in der Version 6 durch eine „Neighbor Discovery“-Funktion des ICMPv6 ersetzt. Als wesentlicher Bestandteil von IPv6 muß dieses Protokoll immer implementiert sein. Eine Migration von IPv4 zu IPv6 kann auf drei Wegen erfolgen.

#### Migration von IPv4 zu IPv6:

- 1) Dual Stack: paralleler Betrieb beider IP-Stacks (4 und 6) auf den Netzstationen (z.B.: Router)
- 2) Tunneling: Encapsulation von IP Version 6 in IP Version 4 (später umgekehrt)
- 3) Header Translation: Übersetzung der Header-Informationen von einer IP-Version in die andere

Mit diesen verschiedenen Möglichkeiten bleibt die Kompatibilität im Netz gewahrt und erlaubt die sanfte Migration zu IPv6.

Die wesentlichen Vorteile des Protokolls in der Version 6 gegenüber Version 4 sind:

- Modularer Header-Aufbau (soviel Information wie nötig),
- Hohe Anzahl von Adressen,
- Verbesserte Subnetz-Struktur,
- Automatische Konfiguration (Adreßvergabe),
- Unterstützung von umfassenden Sicherheitsfunktionen,
- Leichteres Routing durch einfachen Headeraufbau und Kennzeichnung eines Flows und damit direkte Unterstützung von IP-Switching-Technologie, die auch von Bay Networks in Form eines „Switch Node“ künftig angeboten wird,
- Unterstützung von Multimedia und Echtzeit - Informationsübertragung durch Nutzung von Prioritäten und Bandbreitenzuweisung zwischen zwei Adressen mittels RSVP.

Die mit dem Einsatz verbundenen Nachteile oder Bedingungen sind:

- Übertragung von gleicher Information mit größerem Protokoll-Header (mindestens 16 Byte)
- Bedingung der Verkehrsmessung im Netzsegment vor dem Einsatz von IPv6 und bei hoher Auslastung eines Segmentes Schaffung von Bandbreitenreserve
- Aufrüstung des Arbeitsspeicher der Router wegen höherer Paketlänge

[Gate 11/96],[Gate 6/95], [ntz 10/96], [PcN 10/96]

Mit dem Einsatz des IPv4 im Kreditinstitut auf den WAN-Verbindungen und der Möglichkeit des Einsatzes im LAN (Unterstützung durch IBM LAN Manager) ist zu empfehlen, daß Internet Protokoll in der Version 6 künftig im gesamten Institut einzusetzen. Mit dieser Version von IP können die Aufgaben, wie Übertragung multimedialer Informationen, automatische IP-Adressenvergabe oder Sicherheit von Datenpaketen durch Verschlüsselung, einfach bewältigt werden. Nach Aussage von Bay Networks [PcN 10/96 S.90] wird die IP Version 6 ab der Router-Software Version 12 als Standard-Protokoll zur Verfügung stehen. Das IPv6 wird als zusätzliches Protokoll behandelt, weshalb beide Protokolle parallel (Dual Stack) in den Netzen eingesetzt werden können (Update der Router erforderlich). Auch IBM will die IPv6 unterstützen und in weiteren Produkten implementieren. Aufgrund des weiteren Wachstums des Internets werden künftig multimediale Applikationen auf IPv6 aufsetzen. Diese Applikationen besitzen eine hohe Funktionalität mit gleichzeitiger Bandbreiteneffektivität. Oft werden dabei die allgemeinen Lösungen zu kundenspezifischen

Applikationen weiterentwickelt, welche als Branchenlösungen vermarktet werden. Auch aus diesem Grund ist der Einsatz des Protokolls zu empfehlen.

## **5.5 Verfahren zur Erhöhung des Kundenservice**

### **5.5.1 Call Center**

In der heutigen Zeit wird im zunehmenden Maße das Telefon-Banking für die Kontoführung durch die Kunden eines Kreditinstitutes eingesetzt. Die darauf spezialisierten Direkt-Banken können so mit einem Minimum an Mitarbeitern ein Maximum an Finanzdatenverkehr bewältigen. In einem Unternehmen wie dem Beispielinstitut wäre der Einsatz eines solchen Service sinnvoll, weil damit einem „Abwandern“ der Kunden entgegengewirkt und eine neuer Kundenkreis gewonnen werden kann. Für den Aufbau eines Telefon-Banking-Service ist es notwendig, die ankommenden Anrufe zu organisieren und gleichmäßig auf die Mitarbeiter zu verteilen. Für die Realisierung dieser Funktionen werden **Automatic Call Distribution (ACD)**-Systeme eingesetzt. Die Systemfunktionen werden durch die Kopplung von einer PBX und einem ACD-Server bereitgestellt. Die Struktur eines Call Centers für Telefon-Banking wird in der Abbildung 5.9 dargestellt. Bei diesem System werden die eingehenden Anrufe direkt oder über eine Anrufverzögerung mit Ansage entgegengenommen. Wenn in diesen Bereichen eine Überlast eintritt, kann der Anrufende zu Überlast-Gruppen vermittelt werden oder auf dem „Voice Mail Server“ eine Nachricht hinterlassen. Der Manager kann jederzeit die aktuelle Lage der Auslastung der ACD-Gruppe überprüfen und eine umfassende Statistik führen. Weiterhin können sämtliche Informationen gespeichert und anschließend ausgewertet werden. Das Ziel aller ACD-Systeme ist es, kein Gespräch zu verlieren und damit jederzeit für den Kunden erreichbar zu sein. Mit der Nutzung von HICOM-PBX-Systemen im Kreditinstitut empfiehlt sich der Einsatz des ACD-System „HICOM ACD 300“ der Siemens AG, welches die genannten Funktionen bereitstellt. Darüber hinaus können künftig „Voice Processing“-Systeme eingesetzt werden, welche über Sprachsynthese Informationen für den Kunden (z.B.: Kontoinformationen) oder Mitarbeiter (z.B.: Organisationsinformationen) bereitstellen. Künftig können auch die „Interactive Voice Response“ (IVR) – Systeme verstärkt zum Einsatz kommen, wobei über die Spracherkennung oder die Telefontastatur „Sprach“-Menüs bedient werden. Durch die Bedienung der Menüs können Kontoinformationen abgerufen, Überweisungen getätigt, Konfigurationsdaten (z.B.: PIN-Nummern) geändert oder gezielt Berater in Anspruch genommen werden. Mit diesen Systemen realisiert das Kreditinstitut



Personalkosten zu sparen, kurzfristig auf dem Finanzmarkt zu reagieren, ein Maximum an Finanzdatenverkehr zu bewältigen und für zukünftige Kunden weltweit präsent zu sein. Diese Vorteile können auch dem Beispielinstitut dienlich sein, um künftig höhere Gewinne zu erzielen und auf dem Finanzmarkt weiter zu bestehen.

Für die Nutzung des Internets durch das Kreditinstitut können folgende Varianten unterschieden werden:

- a) Allgemeine Darstellung des Kreditinstitutes mit Informationen über die Struktur der Geschäftsstellen, die möglichen Dienstleistungen im Finanzbereich (z.B.: Darstellung von Immobilien und Finanzierungsmodellen), Bereitstellung von Kontaktadressen (z.B.: E-Mails oder Telefonnummern von Fachberatern), Integration und Aktivitäten im öffentlichen Leben der Hansestadt Rostock und weiterer Geschäftsgebiete, Unterstützung von allgemeinnützigen Projekten (z.B.: Kontonummern von Hilfsorganisationen) und sonstigen Aufgaben und Maßnahmen,
- b) Realisierung interaktiver Kommunikation zwischen Kunde und Kreditinstitut unter Verwendung von Sicherheitsmaßnahmen, wie z.B.: Datenverschlüsselung, Einsatz von Firewall-Systemen, und damit Bereitstellung von Kontoinformationen und weiteren Dienstleistungen der Finanzunternehmen,
- c) Bereitstellung eines elektronischen Kontos für den Kunden zur Bestellung oder „Einkauf“ im Internet,
- d) Nutzung des Internets für die private Kommunikation und Bildung eines Virtual Private Network (VPN) mit verschlüsselter Datenübertragung (Tunnelung von Datenpaketen) und damit Möglichkeit des Zugriffs von Mitarbeitern auf das Netzwerk des Institutes (Nutzung von Netzressourcen).

Für die Präsenz des Kreditinstitutes im Internet ist in der Anfangsphase die Variante a) zu empfehlen, da bei dieser Variante die Kosten und das Sicherheitsrisiko gering sind und die derzeitigen Aufgaben des Institutes unterstützen. Mit dieser Variante können erste Erfahrungen hinsichtlich der Sicherheit, Kundenakzeptanz und Informationsbereitstellung mit dem Internet gewonnen und ein künftiger höherer Leistungsumfang abschnittsweise eingeführt werden. Da derzeit bereits eine Kommunikation mit dem Internet erfolgt, sollte

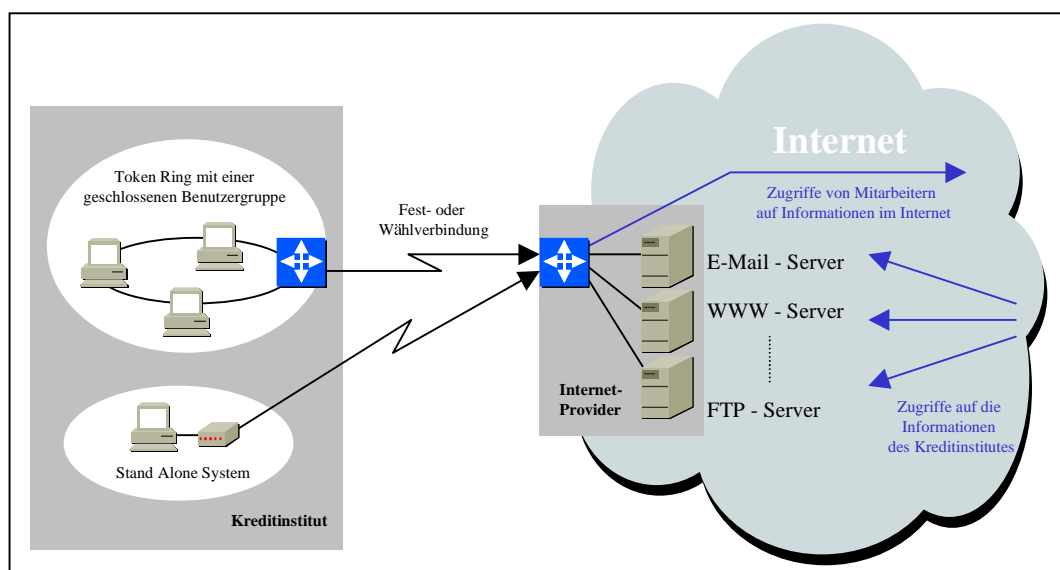


diese mit den Maßnahmen der Variante a) zusammengefaßt und eine einheitliche Lösung angestrebt werden. Sinnvoll für die Präsenz im Internet ist die Bereitstellung und Nutzung von verschiedenen Diensten wie:

- WWW
- FTP
- E-Mail
- News
- Telnet
- Gopher
- Archie
- und sonstige

Die Dienste WWW und E-Mail stellen für das Kreditinstitut die wichtigsten Dienste dar, weshalb dafür durch das Kreditinstitut Informationen oder Ressourcen bereitzustellen sind. Der WWW-Server ermöglicht die Präsentation der Informationen und der E-Mail-Server die Kommunikation mit dem Kunden zur Ermittlung der Kundenresonanz. Alle weiteren Dienste wären zusätzlich und würden die Qualität der zu erbringenden Leistungen erhöhen (z.B.: FTP-Server für MPEG-Files von Immobilien). Für die Bereitstellung dieser Informationen können folgende Ankopplungen an das Internet empfohlen werden:

- 1) Bereitstellung der Informationen des Kreditinstitutes durch die Server des Internet-Providers und zusätzlicher Zugriff auf das Internet durch Mitarbeiter des Kreditinstitutes

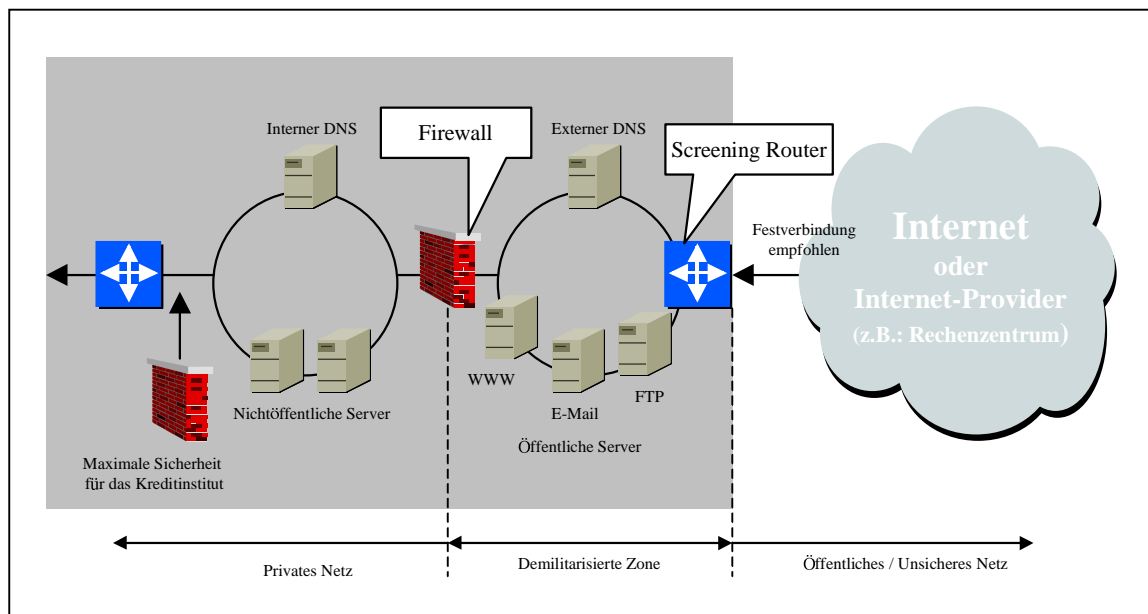


**Abb.5.10: Informationsbereitstellung für das Internet über einen Provider**

Bei dieser Variante muß das Kreditinstitut für den Zugriff auf das Internet lediglich geschlossene Benutzergruppen oder „Stand Alone“- Systeme einführen, um den Zugriff von Mitarbeitern des Institutes zu ermöglichen. Die Informationen des Kreditinstitutes werden auf den Servern des Providers für das Internet bereitgehalten und können durch die Verknüpfung mit der Internet-Adresse des Kreditinstitutes von interessierten Personen abgerufen werden. Der Inhalt der Informationen kann dem Provider in Form von bekannten Dateiformaten, schriftlichen Unterlagen oder HTML-Dokumenten bereitgestellt werden. Der Provider pflegt diese Informationen in den virtuellen Web-Server des Kunden ein, welcher dadurch ständig aktualisiert wird. Der vom Provider bereitgehaltene E-Mail-Server empfängt die Nachrichten der Internet-Nutzer wodurch die Kundenresonanz geprüft werden kann. Zusätzlich zu dieser Maßnahme kann auf dem WWW-Server ein Programm zur Zählung der Zugriffe für die Ermittlung der Akzeptanz eingesetzt werden. Mit dieser einfachen Variante eines virtuellen Web-Servers kann das Kreditinstitut die Wirksamkeit eines Internet-Servers prüfen, ständig im Internet präsent sein und durch eine Wählverbindung Kosten sparen. Für den Aufbau einer solchen Verbindung zum Internet sind Angebote der regionalen Internet-Provider im Anhangshefter enthalten, weil diese einen umfassenden Service bieten, bandige Kopplungen zum Internet besitzen und zum Ortstarif zu erreichen sind. Bei Übergang zu einer solchen Lösung sind künftig auch die überregionalen Anbieter zu betrachten.

- 2) Bei einer zweiten Variante werden die Internet-Server direkt beim Kreditinstitut aufgestellt und administriert. Mit dem Einsatz dieser Variante der Kopplung mit dem Internet kann eine umfassende Bereitstellung von Informationen und die problemlose Integration von interaktiver Kommunikation (Kontoführung durch den Kunden über das Internet) ermöglicht werden. Die Struktur der Internet-Anbindung ist in der Abbildung 5.11 dargestellt. Bei der Verbindung zu einem „unsicheren“ Netz (Internet) wird durch den Screening Router und den Firewall eine demilitarisierte Zone gebildet, in der die öffentlichen Server enthalten sind. Diese Server stellen allgemeine Informationen für das Internet bereit. Der Screening Router übernimmt dabei die Vorfilterung der Datenpakete nach Kriterien wie Adressen, Ports und Protokolltypen. Dieser Schutzmechanismus kann durch Hacker mit Funktionen wie IP-Spoofing (Vortäuschung einer gültigen IP-Adresse) umgangen werden, weshalb der Schutz für die Anbindung an das Internet nicht als ausreichend angesehen werden kann. [FW 96] Zusätzlich zum Screening Router kommt ein Firewall-System zum Einsatz, welches die demilitarisierte Zone vom privaten Netzwerk des Institutes trennt. Bei den Firewall-Systemen können verschieden Typen zum Einsatz

kommen, wobei sich geschlossenen Systeme mit Adressen-Umsetzung (Network Address Translation nach RFC 1631), wie z.B.: Cisco PIX, als sehr wirksam erweisen. Die Adressenumsetzung besitzt den weiteren Vorteil, daß die internen Adressen des Netzes des Kreditinstitutes weiterbestehen können und nicht auf die des Internets abgestimmt werden müssen.



**Abb.5.11: Informationsbereitstellung für das Internet im Kreditinstitut**

Diese Struktur der Anordnung der Komponenten wird als „Dual Homed Bastion Host (Firewall) mit demilitarisierter Zone“ bezeichnet. [Hab97] Die hinter dem Firewall angeordneten Server können zur Kommunikation mit dem Kunden im Internet oder im Kreditinstitut eingesetzt werden. Die Installation eines weiteren Firewalls hinter den nichtöffentlichen Servern ermöglicht die größtmögliche Sicherheit, weil selbst beim Durchbrechen des ersten Firewalls der Eindringling noch nicht in das Netz des Institutes gelangt ist. Bei Durchbrechen des zweiten Firewalls besteht noch eine weitere Sicherheit durch das Segmentieren von Netzabschnitten und den Einsatz von Paket-Filtern auf den (Screening-) Routern des Kreditinstitutes. Die in den Zonen installierten DNS-Server dienen der Zuordnung von IP-Adressen zu Domain-Namen und beinhalten damit die internen Strukturen eines Netzes. Aufgrund dieser Tatsache sind die DNS-Server doppelt auszuführen, wobei der DNS-Server in der demilitarisierten Zone nur nichtvertrauliche und minimale Informationen enthält. [Hab97] Mit der Nutzung dieser Netzwerkstruktur kann eine ständige Präsenz im Internet erreicht werden, wobei das Kreditinstitut sämtliche Maßnahmen und Aufgaben zur Gewährleistung

der Bereitstellung von Informationen übernimmt. Die bereitzustellenden Informationen (von der Abteilung Marketing) können durch das Kreditinstitut schnell und einfach auf dem WWW-Server eingepflegt werden. Die Kopplung des vorhandenen Lotus Notes Servers mit dem Internet erlaubt das weltweite Empfangen und Senden von E-Mails über diesen Server.

Für die Kopplung zum Internet ist langfristig die zweite Variante zum empfehlen, weil damit das Kreditinstitut selbst alle Informationen schnell und problemlos im Internet bereitstellen kann. Dies verursacht jedoch erhebliche Kosten, weshalb die erste Variante für den Beginn der Internet-Nutzung empfohlen wird. Das künftige Auftreten des Rechenzentrums als alternativer Dienstanbieter und Internet-Provider kann auch einen Anschluß an das Internet ermöglichen. Das Kreditinstitut könnte dann über das Rechenzentrum einen Anschluß an das Internet erhalten. Bei dieser Lösung bleibt aber abzuwarten, ob und wann diese Lösung angeboten wird, welche finanziellen Aufwendungen dabei zu tätigen sind und wie hoch der Serviceumfang sein wird. Weiterhin sollte die Bandbreite der Anbindung an das Internet geklärt werden, weil die Kosten eines breitbandigen Anschlusses an das weltweite Internet (Transatlantik-Verbindungen in Frankfurt) sehr hoch sind. Viele Provider in Deutschland verfügen daher über einen breitbandigen Backbone und einen schmalbandigen Übergang in Frankfurt. Mit dem direkten Übergang zu einem Business-Internet-Provider wie Xlink (regionaler Vertreter: Gecko mbH Rostock) kann dieses Problem umgangen und eine durchgehende breitbandige Ankopplung an das ständig wachsende Internet erreicht werden. Die Wahl des Internet-Providers stellt somit einen wesentlichen Faktor für die Qualität eines Internet-Servers dar.

Bei einem Anschluß des Kreditinstitutes an das Internet sollte das Kreditinstitut in der bereits bestehenden Domäne des Verbandes registriert werden, um ein einfaches Auffinden des Servers durch interessierte Personen zu ermöglichen.

Der Anschluß des Kreditinstitutes wird somit von der weiteren Netzgestaltung und den Aktivitäten des Rechenzentrums abhängen, weshalb hier nur Varianten zur selbständigen Anbindung vorgeschlagen wurden. Der bei den Vorschlägen genannte Einsatz von Firewall-Systemen sollte aber nicht auf Internet-Zugänge beschränkt werden. Die Qualität und die Handhabbarkeit dieser Systeme sind enorm gestiegen, weshalb sie auch intern für den Schutz sensibler Dateibereiche (z.B.: zentraler Datenbanken mit statischen und temporären Personendaten) eingesetzt werden sollten.

## 5.6 Liberalisierung des Telekommunikationsmarktes

Ausgangsbasis der gegenwärtigen Liberalisierungsbemühungen bilden die Entschlüsse des Telekommunikationsrates vom 22.07.1993 und 22.12.1994 zur Liberalisierung des Sprachtelefondienstes und der Telekommunikationsinfrastruktur in der Europäischen Union ab dem 01.01.1998. Weiter konkretisiert diese Maßnahme eine Richtlinie der EG-Kommission zur Einführung des vollen Wettbewerbs im Telekommunikationsmarkt zum 01.01.1998. In Deutschland wurde hierfür im Zusammenhang mit dem „Gesetz zur Neuordnung des Postwesens und der Telekommunikation“ („Postreform II“) vom 14.09.1994 durch eine Ergänzung des Grundgesetzes die notwendige verfassungsrechtliche Grundlage geschaffen. Danach hat die Bundesregierung für „flächendeckend angemessene und ausreichende Dienstleistungen“ im Bereich der Telekommunikation Sorge zu tragen (Art. 87f GG). Die Verfassung verknüpft dabei die hoheitliche Aufgabe mit einer privaten wie folgt: „Die im Bereich der Telekommunikation am Markt angebotenen Dienstleistungen werden nicht als hoheitliche, sondern als privatwirtschaftliche Tätigkeiten erbracht, und zwar durch die Deutsche Telekom AG und andere Marktteilnehmer“. Erfüllt wird der verfassungsmäßige Auftrag durch das neue „Telekommunikationsgesetz“, welches das Bundesministerium für Post und Telekommunikation am 08.08.1995 im Entwurf der Öffentlichkeit vorstellte und das am 25.07.1996 vom Bundestag verabschiedet wurde. Die Schritte zur Liberalisierung des Telekommunikationsmarktes werden in der folgenden Tabelle dargestellt.

Etappen der Liberalisierung	Geplante Zeitabschnitte
1. Verkündung des Telekommunikationsgesetzes	25.07.1996
2. Liberalisierung der TK-Netze	Sommer 1996
3. Lizenzvergabe für Telekommunikationsdienstleistungen	Sommer 1996
4. Lizenzvergabe für Sprachtelefondienst	Frühjahr 1997
5. Liberalisierung des „Sprachtelefondienst“ (voller Wettbewerb)	01.01.1998

***Tabelle: Fahrplan zur Liberalisierung des TK-Marktes in Deutschland***

[Bund 96]

### 5.6.1 Nutzung überregionaler Netzanbieter

Ausgehend vom Zeitplan der Liberalisierung bildeten sich Dienstleistungsanbieter, welche regional oder national tätig werden und die dafür notwendigen Lizenzen erwarben. Für die Analyse der Möglichkeit der Nutzung eines Dienstleistungsanbieters war es nötig, die vergebenen Lizenzen zu kennen und danach eine Überprüfung der Handlungsfähigkeit vorzunehmen. Die aktuelle Lizenzvergabe erfolgt in Klassen, die folgende Dienste beinhalten. Klasse 1 = Lizenz für Mobilfunkdienstleistungen

Klasse 2 = Lizenz für Satellitenfunkdienstleistungen

Klasse 3 = Lizenz für Telekommunikationsdienstleistungen

(sonstige Übertragungswege-Lizenzen)

Klasse 4 = Lizenz für Bereitstellung von Sprachtelefondienst auf der Basis selbstbetriebener Telekommunikationsdienste (schließt nicht das Recht zum Betreiben von Übertragungswegen ein)

Die zugelassenen Lizenzinhaber der genannten Klasse 3 sind in folgender Tabelle enthalten.

Unternehmen	Lizenz seit	Lizenzgebiet
Deutsche Telekom AG	September 1996	Bundesrepublik Deutschland
Bayernwerk Netkom GmbH	Oktober 1996	Bayern, Thüringen, Frankfurt a. M., Leipzig
Colt Telecom GmbH	Oktober 1996	Freie und Hansestadt Hamburg
Colt Telecom GmbH	Oktober 1996	Bundesland Berlin und Potsdam
Colt Telecom GmbH	Oktober 1996	Land- und Stadtkreise Darmstadt, Offenbach, Hoch-Taunus-Kreis, Mainz-Bingen, Groß-Gerau und Dieburg
Colt Telecom GmbH	Oktober 1996	Land- und Stadtkreise München, Ebersberg, Erding, Freising, Landshut, Pfaffenhofen an der Ilm, Neuburg-Schrobenhausen, Aichach-Friedberg, Augsburg, Dachau, Fürstenfeldbruck, Landsberg am Lech und Starnberg sowie die kreisfreien Städte München, Landshut, Ingolstadt und Augsburg
HEAG Media-Net GmbH	Oktober 1996	Südhausen
MFS Deutschland GmbH	Oktober 1996	Berlin, Düsseldorf, Frankfurt a. M., Hamburg, Köln, München, Stuttgart, sowie Verbindungen zwischen den Standorten und zu internationalen Standorten
Netcologne GmbH	Oktober 1996	Regierungsbezirk Köln
RWE Telliance AG	Oktober 1996	Bundesrepublik Deutschland
Vebacom Service GmbH	Oktober 1996	Bundesrepublik Deutschland
Thyssen Telecom	Oktober 1996	Bundesrepublik Deutschland
ISIS Multimedia Net GmbH	November 1996	Düsseldorf, Neuss, Grevenbroich, Dormagen, Kaarst, Korschenbroich, Meerbusch, Willich, Mettmann, Erkrath, Haan, Hilden, Langenfeld, Monheim und Ratingen
Mannesmann Arcor (mit DBKom und CNI)	Dezember 1996	Bundesrepublik Deutschland
Teleglobe GmbH (Teleglobe Inc. Canada)	Dezember 1996	Bundesrepublik Deutschland
VEW Telnet	Dezember 1996	Orte in den Regionen Arnsberg, Detmold, Düsseldorf, Emsland und Münster
Colt Telecom GmbH	Januar 1997	Regionalverband Ruhrgebiet
Colt Telecom GmbH	Januar 1997	Gebiete am mittleren Neckar und mittleren Oberrhein
M-net Telekommunikations GmbH	Januar 1997	Gebiet der Stadt München und Unterföhring

***Tabelle: Lizenzinhaber der Klasse 3***

Die in der Tabelle enthaltene RWE Telliance AG und die Vebacom Service GmbH bilden derzeit ein Joint Venture mit dem Namen „O.tel.o“. Dieses Projekt wird zukünftig für beide Partner auf dem Telekommunikationsmarkt auftreten.

Die Lizenzinhaber der Klasse 4 für den Sprachtelefondienst sind in der nachfolgenden Tabelle enthalten.

Unternehmen	Lizenz seit	Lizenzgebiet
Colt Telecom GmbH	Dezember 1996	Freie und Hansestadt Hamburg, Berlin, Potsdam, Großraum Frankfurt a. M., Großraum München und Verbindungen zwischen den Lizenzgebieten
Netcologne GmbH	Dezember 1996	Regierungsbezirk Köln
Vebacom Service GmbH	Dezember 1996	Bundesrepublik Deutschland
Viag Intercom GmbH & Co.	Januar 1997	Bundesrepublik Deutschland
Mannesmann Arcor (mit DBKom & CNI)	Januar 1997	Bundesrepublik Deutschland
Tele globe GmbH	Januar 1997	Bundesrepublik Deutschland

***Tabelle: Lizenzinhaber der Klasse 4***

[Nc 4/97]

Von den in den Tabellen enthaltenen Lizenzinhabern wurden nur die Lizenzinhaber der **Klasse 3** betrachtet. Diese Lizenzinhaber können private Übertragungsstrecken und sämtliche Datendienste bereitstellen, was bereits zum Zeitpunkt der Diplomarbeit laut „Telekommunikationsgesetz“ möglich war. Von den genannten alternativen Netzanbietern wurden die Anbieter mit einer **bundesweiten** Lizenz überprüft, weil es ihnen gestattet ist, im Land Mecklenburg-Vorpommern und speziell im Raum Rostock tätig zu werden. Die betrachteten alternativen Netzanbieter sind:

### **5.6.1.1 Mannesmann Arcor**

Dieser Netzanbieter besitzt im Moment eines der größten LWL- und Kupferkabelnetze innerhalb Deutschlands, welches ständig weiter ausgebaut wird. Eine hohe Kilometerzahl wurde durch die Deutsche Bahn Tochter DBKom eingebracht. Das übernommene Unternehmen CNI bringt zusätzliches Know How in Netzwerkfragen mit ein, weshalb dieser Netzanbieter über ein hohes Potential an Wissen und Technik verfügt. Da sich das Netz dieses Anbieters noch im Aufbau befindet, kann derzeit kein Angebot erstellt werden. Die bereitzustellenden Übertragungswege müssten vollständig von der Deutschen Telekom AG angemietet werden, wodurch höhere Kosten als bei der derzeitigen Vernetzung des Kreditinstitutes entstehen. Die Vernetzung der Standorte (Knoten) wird über das Equipment

von Mannesmann vorgenommen, wobei Multiplexer und Router durch Mannesmann gestellt werden. Die angebotenen Dienste gliedern sich wie folgt:

Sprachdienste	Datendienste	Mehrwert	Technik
Business Service	Frame Relay Service	Videokommunikation	Technischer Kundendienst
PBX-Connect Service	X.25 Service	Fax Service	Informationstechnik
PBX-Lease	LAN-Connect Service	Call Center Service	Bürotechnik
VPN Service	X.400 Service	Teleworking	Sicherheitstechnik
IN Service		E-Mail Service	Sondertechnik
			LAN-Service

Die genannten Service-Dienste sind dem Zusatzhefter zu entnehmen. Die internationalen Partner sind AT&T und Unisource. Dieser Netzanbieter ist künftig weiter zu beobachten, da laut Ausbauplan und Aussagen der Mitarbeiter von Mannesmann Arcor Rostock einen Knoten im Gesamtnetz darstellen wird.



*Abb.5.12: Geplante Netzstruktur von Mannesmann Arcor*

[TA 97]

### 5.6.1.2 Vebacom Service GmbH

Die Vebacom Service GmbH besitzt mit ihrem Partner RWE Telliance AG einen Partner, der über 4000 Glasfaserkilometer verfügt. Beide zusammen bilden das Joint Venture Projekt „O.tel.o“. Das derzeit aufgebaute Netz stützt sich auf Standard-Festverbindungen der Deutschen Telekom AG, die redundant ausgelegt und im Bedarfsfall erweiterbar sind. Das



Unternehmen baut einen breitbandigen Backbone über das gesamte Bundesgebiet aus, in dem Rostock einen wesentlicher Knoten darstellen wird. Im Bereich Rostock ist derzeit ein Unternehmen über X.25 an das Netz der Vebacom Service GmbH angeschlossen. Im Rahmen der Diplomarbeit wurden umfangreiche Verhandlungen zu einem Angebot für die Knoten geführt, deren Ergebnis war, daß die derzeit aufzuwendenden Kosten der Vebacom Service GmbH zu hoch wären und damit kein sinnvolles Angebot gemacht werden konnte. Bei den Verhandlungen wurde von der Seite der Vebacom Service GmbH von Telefonkosten in Höhe von mindestens 10.000 DM pro Monat für den Anschluß eines Standortes ausgegangen. Der Anschluß der Standorte wäre über vom Netzanbieter gestelltes Equipment (Multiplexer, Router (Cisco Systems)) und von der DTAG angemietete Standard-Festverbindungen vorgenommen worden. Das Unternehmen verfügt über folgende Dienste:

- Sprachmehrwertdienste
- Paketvermittelte Datenübertragung (X.25-, Frame Relay-, X.31-, X.31plus-Service)
- Managed Router Service
- Multimedia Breitbandkommunikation über ATM
- Netz Outsourcing
- Außendienststeuerung
- Zentrales Netzwerkmanagement
- I-Gate-Service / Internet
- EDI-Services
- E-Mail (X.400/X.500)
- Fax Services

Internationaler Partner ist Cable & Wireless, mit dem zusammen der sogenannte „Global Managed Data Service“ ermöglicht wird. Das Unternehmen wird sein Netzwerk künftig verstärkt ausbauen, wobei nach Aussagen von Mitarbeitern für den Knoten Rostock gute Anschlußmöglichkeiten entstehen werden.

[TA 97]

### **5.6.1.3 Thyssen Telecom**

Die Thyssen Telecom AG besitzt mit der Plusnet GmbH eine 100 % Tochtergesellschaft, die den Netzwerkservice übernimmt. Das aufgebaute Netz stützt sich auf Standard-Festverbindungen zwischen den Knoten, die im Bedarfsfall durch ATM-Festverbindungen (je nach Bedarf) erweitert werden. Die in der Abbildung 5.14 (Anhang) dargestellte Netzstruktur besteht aus 30 Knoten, die sich in den größten Ballungszentren befinden. Neben den Knoten

in der Bundesrepublik Deutschland existieren 22 weitere Knoten in der Schweiz, die von der Schwestergesellschaft Plusnet AG Bern betrieben werden. Der Bereich Mecklenburg-Vorpommern (Rostock) ist in der derzeitigen Ausbauphase nicht in den Backbone integriert (siehe Abbildung im Anhang). Die Verhandlungen mit der Plusnet GmbH führten zu keinem akzeptablen Ergebnis, weil der Anschluß an dieses Netz über Berlin erfolgen müßte. Bei der Erstellung eines entsprechenden Angebotes müßten zusätzliches Equipment und angemietete Standard-Festverbindungen der Deutschen Telekom AG berücksichtigt werden. Diese Aufwendungen sind nicht tragbar, weshalb auf ein Angebot verzichtet werden kann. Die Plusnet GmbH bietet folgende Dienste an:

- Sprachkommunikation
- Telefon Service
- Videokommunikation
- Paketorientierte Datenfernübertragung
- LAN-Kopplung
- E-Mail
- File-Transfer
- EDI (elektronischer Datenaustausch)
- Internet
- Sprach-Mehrwertdienste
- Calling Card (kostenfreie internationale Einwahl)
- Service Number Calling (kostenfreier Netzzugang)
- Corporate Network Funktionen
- Mobile Extended Corporate Networks mit E-Plus
- Anbindung an internationale Mobilfunk- und Satellitennetze

Servicepartner der Plusnet GmbH sind Xtend Gesellschaft für Mehrwertdienste mbH, Ontel Gesellschaft für Onlinedienste mbH, Spaceline Communication Service sowie Internet Service GmbH. Das Unternehmen verfügt über vielfältige Funktionen zur kostenreduzierenden Kommunikation. Wie aus dem derzeitigen, im Anhang enthaltenen Ausbauplan ersichtlich, orientiert sich das Unternehmen an den wichtigsten Wirtschaftsregionen, weshalb abzuwarten bleibt, wann das Unternehmen den Bereich Mecklenburg-Vorpommern in den Backbone integrieren wird.

#### **5.6.1.4 Telelobe GmbH**

Dieses Unternehmen stellt eine Tochtergesellschaft des weltweiten Telekommunikationsanbieters Telelobe Inc. mit Hauptsitz in Kanada dar. Das Unternehmen verfügt über eine Vielzahl von internationalen Telekommunikationseinrichtungen. Mit dem Aufbau zweier POP's in Frankfurt und Düsseldorf und der Lizenz der Klassen 3 und 4 kann dieses Unternehmen künftig Telekommunikationsdienstleistungen innerhalb Deutschlands anbieten. Aufgrund der vorangegangenen Tätigkeiten auf dem weltweiten Telekommunikationsmarkt verfügt das Unternehmen über handlungsfähige Strukturen, die ein hohes Niveau an Wissen und Technik aufweisen. Da sich das Netz des Unternehmens in Deutschland im Aufbau befindet, müßten für den Bereich Mecklenburg Vorpommern SFV der Deutschen Telekom AG angemietet werden, um die Standorte des Kreditinstitutes zu verbinden. Die Bereitstellung dieser Verbindungen ist nicht oder nur in begrenztem Umfang von einer Stellung von Equipment durch die Telelobe GmbH abhängig. Da sich die Organisationsstrukturen dieses Anbieters im Aufbau befinden und derzeit noch keine genauen Angaben über die zukünftigen Netzstandorte gemacht werden, mußte auf eine Angebotserstellung verzichtet werden. Mit dem weiteren Aufbau des Netzes wird dieser Telekommunikationsanbieter umfassende und preiswerte Leistungen anbieten können, weshalb künftige Betrachtungen diesen Netzanbieter immer mit einschließen sollten. Weiterhin bleibt auch bei diesem Anbieter abzuwarten, wann der Bereich Mecklenburg Vorpommern in den Backbone integriert wird.

[TA 97]

#### **5.6.2 Nutzung regionaler Netze**

Für die Nutzung alternativer Übertragungswege besteht die Möglichkeit der Kooperation mit den regionalen Unternehmen, die über Kabeltrassen bzw. private Netze im Bereich der Hansestadt Rostock verfügen. Bei der Recherche wurden folgende relevante Institutionen und Unternehmen genauer betrachtet.

##### **5.6.2.1 HEVAG**

Die Hanseatische Energieversorgung AG Rostock besitzt ein LWL-Netz aus Monomodefasern und Kupferkabeln, die an den Trassen der Hochspannungsleitungen verlaufen. Die LWL-Faser sind dabei teilweise in den verseilten Hochspannungsleitungen enthalten. Dieses Netz weist eine Bandbreite von 34 Mbit/s auf, wobei auch 2 Mbit/s Verbindungen auf der Grundlage von PCM-Technik vorhanden sind. Die HEVAG besitzt

damit ein breitbandiges Netz, welches derzeit für die interne Kommunikation genutzt wird. Anfragen bezüglich der Bereitstellung von Bandbreite für das Kreditinstitut ergaben, daß die HEVAG sich derzeit hinsichtlich der Netzöffnung in der Entscheidungsfindungsphase befindet. Es werden Bemühungen unternommen, um zu prüfen, inwieweit das Netz geöffnet werden kann und zu welchem Zeitpunkt dies geschehen soll. Die Öffnung des Netzes und das Auftreten der HEVAG als alternativer Netzanbieter wird aber nicht vor 1998 zu erwarten sein. Mit der HEVAG sollten weitere Gespräche geführt werden, weil die LWL-Fernverbindungen einen breitbandigen Anschluß des Knotens K15 erlauben.

### **5.6.2.2 Stadtwerke Rostock AG**

Die Stadtwerke Rostock AG verfügen über ein Kupferleiter- und LWL – Netz, das an den Trassen der Fernwärmeleitungen verläuft. Bei den eingesetzten LWL - Fasern handelt es sich um Monomodefasern [Har 96], die derzeit, ausgehend vom Holbeinplatz, entlang der S-Bahn-Linie in Richtung Erich-Schlesinger-Straße verlaufen. Das Unternehmen führt derzeit Untersuchungen bezüglich des Auftretens als alternativer Netzanbieter durch. Dabei werden die Möglichkeiten der Bereitstellung von Netzressourcen (Bandbreite oder Fasern) und Internet-Diensten geprüft. Das Unternehmen befindet sich damit auch in der Entscheidungsfindungsphase, weshalb im derzeitigen Stadium Gespräche nur zu einer künftigen Kooperation führen. Mit der Nutzung dieses Netzes könnten die Standorte K4, E13 erreicht werden.

### **5.6.2.3 Rostocker Straßenbahn AG**

Die RSAG besitzt ein LWL-Netz, ausgehend vom Betriebshof in Bramow über den Holbeinplatz und die Doberaner Straße bis hin zum Doberaner Platz. Zusätzlich werden in den neu auszubauenden Strecken LWL-Monomode-Fasern im Gleisbett verlegt. So werden bei einem Ausbau des Straßenbahn-Schienen-Netzes im Süden und im Nordwesten von Rostock LWL-Kabeltrassen parallel zum Gleisbett entstehen. Laut Aussagen der RSAG sollen die bereitgestellten Fasern zur Amortisierung des Schienen-Netzes beitragen, weshalb diese Maßnahmen im Zuge des Ausbaus des Schienennetzes mit Sicherheit durchgeführt werden. Laut Ausbauplan des Netzes können durch die Kooperation mit der RSAG die Standorte K1, K5, E16, E14 und E2 miteinander vernetzt werden. Die RSAG will künftig keine Telekommunikationsdienste bereitstellen, aber in Zusammenarbeit mit den Senat der

Hansestadt Rostock Fasern der LWL-Trassen anbieten. Für eine Kooperation mit der RSAG müssen Gespräche mit dem Senat der Hansestadt Rostock geführt werden.

#### **5.6.2.4 Universität Rostock**

Die Universität Rostock verfügt über ein Breitband-ATM-Netz, welches sich in der Aufbauphase befindet. Das aufgebaute Netz stellt eine Sterntopologie dar, in deren Zentrum sich das Rechenzentrum in der Albert-Einstein-Straße befindet. Die Verbindungen zwischen den Standorten werden über Lichtwellenleiter-Kabel mit Monomodefasern realisiert. Innerhalb der Standorte werden Multimodefasern zur Kopplung der einzelnen Gebäudekomplexe eingesetzt. Die Installation der Verbindungen zwischen den Standorten wird von der Deutschen Telekom AG vorgenommen, weshalb sich bestimmte Abschnitte noch im Eigentum der DTAG befinden. Um eine Nutzung dieses Netzes durch das Kreditinstitut zu ermöglichen, müßte zunächst eine Betreibergesellschaft für das Universitätsnetz gegründet werden. Ferner konnte festgestellt werden, daß ein kostengünstiger Übergang von K1 in das Netz (Wismarsche Straße 8 = FB Biologie) möglich ist. Die übrigen Standorte der Universität befinden sich aber von denen des Kreditinstitutes zu weit entfernt. Die aufzuwendenden Kosten für die Anmietung von Standard-Festverbindungen zu den Fachbereichen, das Verlegen eigener Kabel zu den Standorten und der Aufbau einer (optischen) Richtfunkverbindung (K5 zur Möllner Straße 10 = Juristische Fakultät) wären zu hoch. Aufgrund dieser Tatsachen und der fehlenden Existenz einer Betreibergesellschaft des Universitätsnetzes kann derzeit keine Nutzung des Universitätsnetzes durch das Kreditinstitut erfolgen. Die Möglichkeit des Übergangs in das Universitätsnetz ist weiter zu prüfen, weil die Universität künftig ihr Netz öffnen will, um den regionalen Unternehmen eine Nutzung der Netzressourcen zu ermöglichen.

#### **5.6.2.5 Senat Hansestadt Rostock**

Der Senat der Hansestadt Rostock baut derzeit ein privates Netz im Rostocker Innenstadtbereich auf. Das Netz besteht dabei aus privaten LWL-Kabeln und Standard-Festverbindungen der DTAG. Bei den Lichtwellenleitern werden für hohe Übertragungsstrecken Monomode- und für geringe Übertragungsstrecken Multimode-Fasern eingesetzt. Die Trassen der LWL-Verbindungen verlaufen ausgehend vom Rathaus über die Richard-Wagner-Straße zur John-Brinckman-Straße. Eine weitere Trasse führt parallel zur Langen Straße in Richtung Doberaner Platz und von dort über die Doberaner Straße zum Holbeinplatz. Vom Holbeinplatz aus werden LWL-Monomode-Fasern der Stadtwerke AG

angemietet, um eine Verbindung zur Erich-Schlesinger-Straße aufzubauen. Zusätzlich wird in einer künftigen Ausbauphase angestrebt, die aufzubauenden Trassen der RSAG (Südstadt und Nordwesten) für die Kopplung verschiedener Ämter zu nutzen. Die Vernetzung der genannten Standorte wird in der Abbildung 5.13 im Anhang dargestellt. Die Nutzung von Lichtwellenleitern erlaubt den Aufbau eines breitbandigen Kommunikationsnetzes zwischen den Standorten des Senates. Die breitbandige Auslegung des Netzes erlaubt dem Senat, weiteren Interessenten Bandbreite oder einzelne Fasern bereitzustellen.

Ausgehend von den Verkehrsmessungen (siehe Abschnitt 4) sind die derzeitig eingesetzten Standard-Festverbindungen hinsichtlich der Bandbreite als optimal anzusehen. Die Kosten für die T2MS-Verbindungen zwischen den Knoten, die sich **innerhalb** von Rostock befinden, sind jedoch sehr hoch (z.B.: K1 – K5 mit 2.765 DM / Monat oder K1 – E2 mit 1.450 DM / Monat). Aufgrund dieser Tatsache ist es sinnvoll, Verhandlungen mit der Stadt aufzunehmen, um eine Kooperation anzustreben und dadurch künftig die Kosten zu reduzieren. Die Gespräche mit den Verantwortlichen im Senat ergaben, daß die Stadt sehr an einer Kooperation interessiert ist. Da die Trassen der angestrebten Vernetzung der städtischen Ämter sehr nahe (teilweise nur 50m entfernt) an den Geschäftsstellen des Institutes entlang verlaufen (werden), wird empfohlen, hinsichtlich der Vernetzung der Standorte des Institutes, welche sich in der Nähe dieser Trassen befinden, Verhandlungen aufzunehmen. So können rechtzeitig die Trassenführung, die Lage der Übergabepunkte sowie die benutzten LWL-Typen abgestimmt werden. Aus den Gesprächen beim Senat ergab sich, daß folgende Unterstützungsvarianten in Betracht kommen:

- 1) Das Kreditinstitut beteiligt sich an den Kosten für künftig zu nutzende Übertragungsstrecken und könnte dabei eigene LWL-Fasern finanzieren oder deren zeitlich begrenzte kostenlose Anmietung ermöglichen.
- 2) Das Institut könnte sich an Finanzierungen von Kabeltrassen, die nicht vom Institut genutzt werden, beteiligen. Im Gegenzug der Unterstützung erhält das Institut Fasern oder Bandbreite auf benötigten Verbindungen.

Im Rahmen der Verhandlungen wurde von einer Beteiligung von 20 DM / Meter gesprochen. Mit diesem Ausgangspunkt und einem Abstand von 1.200 Meter zwischen dem Knoten K1 und E2 würden die Aufwendungen rund 24.000 DM betragen, was den Kosten einer Standard-Festverbindung für 17 Monate entsprechen würde. Daneben wäre eine Aufrüstung mit einem LWL-Monomode-Modul „IOTU“, welches auf das SIMUX-Motherboard beider

Multiplexer der Standorte installiert wird, notwendig. Die Gesamtkosten für diese Maßnahmen würden sich auf etwa 50.000 DM belaufen. Diese Summe entspräche den Kosten für die Standard-Festverbindung über 35 Monate (2,9 Jahre). Nach diesem Zeitraum rentiert sich die Verbindung. Zusätzlich würde die LWL-Verbindung den Übergang zu einem Übertragungsverfahren mit hoher Bandbreite (155 Mbit/s) erlauben und stünde im Eigentum des Kreditinstitutes. Aus den vorher genannten Gründen wird empfohlen, ausführliche Gespräche mit der Stadt zu führen. Eine spätere Kooperation wäre problematisch, weil die Übergangspunkte zu den Trassen oder Fasern nicht optimal zu den Geschäftsstellen liegen würden. Festverbindungen zu den Übergangspunkten erzeugen wieder hohe Kosten und machen den Einsatz einer sonst preiswerten breitbandigen Verbindung unrentabel. Bei einer Kooperation mit der Stadt könnte man zusätzlich die Übertragungswege der RSAG, SWAG nutzen und so eine umfassende Vernetzung der innerstädtischen Geschäftsstellen und Standorte erreichen. Die alternativen Übertragungstrecken wären K1 – E2, K1 – E3, K1 – E4, K1 – E5, K1 – K4, K4 – E13, K4 – E15, K1 – K5, K5 – E16 sowie K4 – E15, wenn E15 von E14 aus an das Netz des Institutes angebunden wird. Weitere Gespräche beim Senat sollten zum Inhalt haben:

- Erörterung der Fragen der Kostenbeteiligung und die damit verbundene Möglichkeit der Nutzung von Glasfasern (Erwerb und Miete)
- Abstimmung über den Verlauf der Kabeltrassen und die Lage der Übergabepunkte für das Institut
- Möglichkeit der Erweiterung der Baumaßnahmen des Senates und dabei direkter Anschluß von Geschäftsstellen (Tiefbau sowie LWL-Anschluß)
- Abstimmung der einzusetzenden LWL-Typen (Mono- oder Multimode) und Erörterung der Nutzung von Kupferkabeln
- Frage der Nutzungsmöglichkeiten und des späteren Ausbaus der LWL- oder Kupferkabel-Netze von RSAG und SWAG (wichtig für K1 – K5)
- Klärung der Frage der Kooperation und Kopplung mit der Universität Rostock (z.B.: als Internet-Provider)
- Möglichkeiten der späteren Anmietung von Bandbreite oder Glasfasern beim Senat

Die dabei ausgehandelten Kosten wären durch das Kreditinstitut leicht zu kontrollieren, wobei die Möglichkeit für den Aufbau eines eigenen breitbandigen Netzes entsteht. Die Bandbreite kann sicherlich zu diesem Zeitpunkt als zu hoch angesehen werden, was aber für eine künftige Nutzung von Vorteil wäre. Das Institut kann über diese LWL-Verbindungen Applikationen

und Anwendungen mit hoher Bandbreite und Qualität einsetzen, um seine Leistungen dem Kunden gegenüber zu erhöhen. In Hinblick auf die Verfügbarkeit dieser Verbindungen können die eingerichteten ISDN-Backup-Pfade weiter beibehalten werden. Weiterhin ist auch die Möglichkeit für die „sanfte“ Migration zu ATM im WAN- und im LAN-Bereich gegeben. Auch ausgehend von den Erweiterungs-möglichkeiten der installierten Komponenten kann die Nutzung der LWL-Verbindungen und zukünftig auch ATM empfohlen werden.

Diese Kooperation zum Aufbau des Netzes wird allen Beteiligten weiterhelfen, die derzeitigen Kosten für die Kommunikation zu reduzieren und die Kommunikationsinfrastruktur sowie die Deregulierung im Bereich Rostock voranzutreiben.

### **5.6.3 Empfehlungen zur Nutzung von alternativen Übertragungswegen**

Abschließend ist für die Nutzung von alternativen Netzanbietern folgendes festzustellen. Im Bereich der Hansestadt Rostock existieren verschiedene Netze, die sich in einer ständigen Erweiterungsphase befinden. Bei den genutzten Übertragungswegen handelt es sich oft um Standard-Festverbindungen der Deutschen Telekom AG oder um private LWL-Kabel.

Die Nutzung eines überregionalen alternativen Netzanbieters ist derzeit kostengünstig nicht möglich, weil die Standorte des Institutes nicht in den privaten Netzen der Anbieter enthalten sind und dafür Festverbindungen der Deutschen Telekom AG angemietet werden müssen. Zusätzlich ist die Nutzung eines überregionalen alternativen Netzanbieters oft an die Bedingung der Stellung von Equipment gebunden, wodurch zusätzliche Kosten entstehen. Ein Übergang zu einem solchen Netzanbieter wäre nur sinnvoll, wenn das Kreditinstitut einen „Outsourcing“-Prozeß bezüglich dieser Komponenten vornehmen will. Da aber das Netzwerk des Institutes mit eigenen Netzkomponenten neu aufgebaut wird und derzeit umfangreiche Investitionen getätigt wurden, muß aus Gründen des Investitionsschutzes und hinsichtlich der Fragen der Netzwerksicherheit von einer Nutzung dieser Anbieter abgesehen werden.

Die Kooperation mit den regionalen Unternehmen und die Nutzung der dabei bereitgestellten Netzressourcen (definierte Bandbreiten oder LWL-Fasern) kann befürwortet werden. Besonders eine Kooperation mit dem Senat ist empfehlenswert, weil diese Institution für den Bereich Rostock ein eigenes Netzwerk aufbaut und sich dabei die Möglichkeit der Nutzung der Übertragungswege des Senates der Hansestadt Rostock, der Rostocker Straßenbahn AG und der Stadtwerke Rostock AG bietet. Die für den Aufbau eines Netzes notwendigen Wegerechte stünden dabei automatisch zur Verfügung. Aufgrund der vorhandenen



Verhandlungsbereitschaft des Senates und der künftigen Unterstützung des Projektes der Stadt durch das Institut ist es möglich, eigene Übertragungswege zwischen den Geschäftsstellen aufbauen und dabei problemlos die Kosten zu kontrollieren. Die Kooperation mit dem Senat wäre hinsichtlich der Standorte E2 und K5 sehr sinnvoll, weil für diese Standorte hohe Kosten für die Standard-Festverbindungen zu entrichten sind. Der Standort K5 ist zusätzlich durch ein hohes Verkehrsaufkommen gekennzeichnet. Beim Zustandekommen einer Zusammenarbeit in Bezug auf diese Geschäftsstellen wären weitere kostensparende Maßnahmen sicher problemlos zu realisieren. Im Gegenzug entsteht ein höherer Koordinationsbedarf für das Kreditinstitut, weil jetzt weitere Ansprechpartner für die Übertragungstrecken existieren (Senat HRO, RSAG).