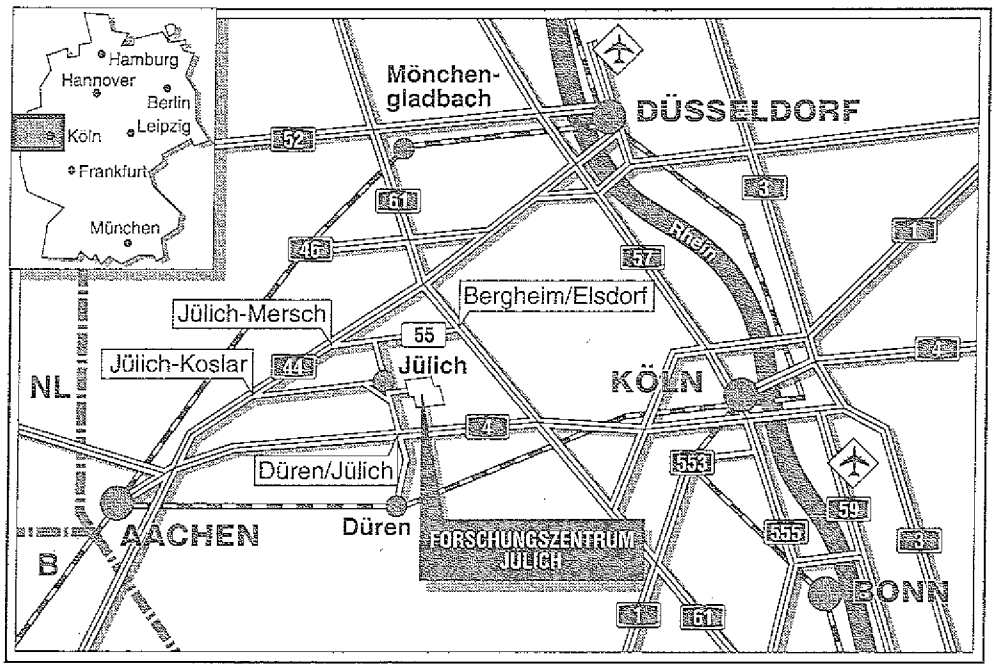
Zentralinstitut für Angewandte Mathematik

KFAnet – Schnelle Datenkommunikation im Forschungszentrum Jülich (KFA)



Berichte des Forschungszentrums Jülich ; 2623
ISSN 0366-0885
Zentralinstitut für Angewandte Mathematik Jül-2623

Zu beziehen durch: Forschungszentrum Jülich GmbH · Zentralbibliothek
Postfach 1913 · D-5170 Jülich · Bundesrepublik Deutschland
Telefon: 02461/61-6102 · Telefax: 02461/61-6103 · Telex: 833556-70 kfa d

KFAnet – Schnelle Datenkommunikation im Forschungszentrum Jülich (KFA)

W. Anrath, R. Bornschein, D. Conrads, R. Grallert, L. Loup,
R. Malzkorn, J. Meißburger, B. Mertens, O. Mextorf,
R. Niederberger, F.J. Schoenebeck, S. Werner
Zentralinstitut für Angewandte Mathematik

H. Bongartz, W. Geier, F.J. Kayser, W. Stevens, H. Stoff
Zentrallabor für Elektronik

Zusammenfassung

Der vorliegende Bericht beschreibt den aktuellen Zustand des schnellen Datenkommunikationsnetzes im Forschungszentrum Jülich, KFAnet, als Ergebnis eines parallel zum technischen Fortschritt verlaufenen Evolutionsprozesses. Die generellen Zielsetzungen sowie die derzeitige Infrastruktur, die Netztechnik und vor allem die angebotenen Kommunikationsdienste werden beschrieben. Da der Istzustand Ausgangspunkt weiterer Entwicklungsschritte ist, werden auch die bevorstehenden Ausbaustufen von KFAnet sowie generelle Zukunftsperspektiven der Datenkommunikation aufgezeigt.

Vorwort

Der vorliegende Bericht beschreibt den aktuellen Zustand des schnellen Datenkommunikationsnetzes im Forschungszentrum Jülich, KFAnet, als Ergebnis eines parallel zum technischen Fortschritt verlaufenen Evolutionsprozesses. In diesem Sinne markiert auch der Istzustand nicht einen Abschluß, sondern ist selbst wieder Ausgangspunkt für weitere Entwicklungsschritte. Es werden deshalb auch die bevorstehenden weiteren Ausbaustufen von KFAnet sowie generelle Zukunftsperspektiven der Datenkommunikation aufgezeigt.

Am Aufbau bzw. Ausbau und Betrieb eines umfassenden Datennetzes sind viele Personen in unterschiedlichen Funktionen beteiligt. Neben den in der Autorenliste aufgeführten direkt Beteiligten sind dies auf der einen Seite Personen, die durch Bereitstellung attraktiver Anwendungsdienste die Akzeptanz und Nutzung eines solchen Netzes fördern, sowie Benutzer in den Instituten, die durch Artikulation ihrer Anforderungen und ihre Kooperationsbereitschaft Einfluß auf die Gestaltung des Netzes nehmen. Auf der anderen Seite sind es die Mitarbeiter zentraler Dienstleistungseinrichtungen – vor allem der Abteilung Anlagenplanung und der Technischen Dienste –, die für einen sachgerechten Ausbau und das Funktionieren der Infrastrukur Sorge tragen. Ihnen allen sei an dieser Stelle für die gute Zusammenarbeit gedankt.

Besonderer Dank gebührt den Leitern der beiden direkt für KFAnet zuständigen Institute ZAM und ZEL, Herrn Prof. Dr. F. Hoßfeld und Herrn Dr. K.D. Müller.

Jülich, im Februar 1992 D. Conrads

Inhaltsverzeichnis

1.0 Einführung

Ein wesentliches Kriterium für Großforschungseinrichtungen ist die interdisziplinäre Zusammenarbeit unterschiedlicher Fachrichtungen, die in der KFA durchweg als Institute oder zentrale Abteilungen organisiert sind. Daraus ergibt sich mit dem verbreiteten Einsatz von Rechnern zwangsläufig auch die Notwendigkeit der Datenkommunikation zwischen Rechnern und Terminals in verschiedenen Instituten. In der Vergangenheit stand dabei die Nutzung zentraler Ressourcen des Rechenzentrums im Vordergrund.
Bei der relativ eigenständigen Position der Institute kann die institutsübergreifende (KFA-weite) Datenkommunikation nicht durch die wissenschaftlichen Institute selbst organisiert werden, sondern nur durch das Dienstangebot einer zentralen Einrichtung sichergestellt werden. Auch die große Zahl von ca. vierzig Instituten und anderen Organisationseinheiten auf dem KFA-Gelände und die dadurch sehr große Vielfalt möglicher Kommunikationsbeziehungen verbietet die Organisation der KFA-weiten Kommunikation auf der Basis bilateraler oder multilateraler Absprachen.
Zuständig für die Organisation der institutsübergreifenden Datenkommunikation ist das Zentralinstitut für Angewandte Mathematik (ZAM), das diese Aufgabe seit den frühen Tagen des Rechnereinsatzes wahrnimmt. Es handelt sich hierbei um eine permanente Aufgabe, die aufgrund sich wandelnder Anforderungen und sich weiterentwickelnder technischer Möglichkeiten immer wieder neue Lösungen erfordert, die sich zum Schutz der Investitionen der Benutzer (insbesondere Geräte und Know-how) am besten als Fortschreibung bestehender Lösungen darbieten.

Das ZAM hat in Wahrnehmung dieses Teils seiner Aufgaben nicht nur immer wieder technische Lösungen erarbeitet und umgesetzt, sondern die Grundlagen des Handelns auch immer wieder in Strategiepapieren (z.B. 'Elektronische Kommunikation – 1984' [10], Strategiepapier 'Konzept zur Entwicklung der Elektronischen Kommunikation in der KFA' [16] und in Papieren zu bestimmten wichtigen Themen (z.B. 'Mittelfristiges Konzept für den Einsatz von Glasfasern in den allgemeinen Kommunikationsnetzen der KFA' [18], 'Sicherheitsuntersuchung TCP/IP-basierender Kommunikationsdienste' [21]) dargelegt.
Die hier vorgelegte Dokumentation über KFAnet beschreibt das aktuelle Zeitfenster eines sich in dem beständigen Bemühen um zeitgerechte und für die Belange der KFA optimierte Lösungen permanent im Wandel befindlichen Angebots an Datenkommunikationsdienstleistungen.

Die Verantwortlichkeit des ZAM für die Datenkommunikation beschränkt sich innerhalb der KFA auf die KFA-weiten Datennetze, die auch als A-Netze bezeichnet werden. A-Netze – wie KFAnet – sind allgemeine Netze mit einem offenen Dienstangebot, das alle Institute bzw. Mitarbeiter der KFA nutzen können, sofern sie die erforderlichen technischen Voraussetzungen und organisatorischen Randbedingungen erfüllen.
Datennetze innerhalb einzelner Institute und Projekte (Bezeichnung: B-Netze = besondere Netze) liegen in der Verantwortung der jeweiligen Institute und Projekte. Die Institute können auf Wunsch durch zentrale Einrichtungen (ZAM und ZEL (Zentrallabor für Elektronik)) Unterstützung bei der Konzipierung und beim Betrieb ihrer Netze erhalten. Im Hinblick auf eine mögliche Anbindung an ein A-Netz, d.h. zur Sicherstellung der über die Institutsgrenzen hinausgehenden Datenkommunikation, sollte in jedem Falle eine Beratung durch das ZAM bzw. ZEL erfolgen.

Netztechnisch besteht KFAnet aus einem Backbone-Netz (A-Netz), das die Verbindung zwischen den Instituten sicherstellt, und den mit diesem verbundenen Institutsnetzen (B-Netze).
Aufgrund der historischen Gegebenheiten hat das ZAM beim Aufbau und Betrieb von KFAnet eine Zusammenarbeit mit dem ZEL verabredet. Hierbei ist das ZEL für den KFAnet-Ethernet-Backbone und die DECnet-Software zuständig.

Das ZAM trägt auch die Verantwortung für die externe Datenkommunikation. Kommunikation mit externen Partnern der gleichen Fachrichtung ist oftmals von gleichrangiger Bedeutung wie die interne Kommunikation mit Kollegen anderer Organisationseinheiten. Eine wichtige Funktion eines internen Netzes wie KFAnet ist es deshalb, den Teilnehmern den Zugang zu externen Kommunikationsdienstleistungen zu ermöglichen.

Sprachkommunikation fällt in die Zuständigkeit von TD–N (Technische Dienste–Nachrichtentechnik). Die Nutzung öffentlich angebotener Netz- und Textkommunikationsdienste und deren Anbindung an die KFA-internen Netze und Dienste werden gemeinsam von den zuständigen Einrichtungen, insbesondere TD–N und ZAM betrieben. Die sich für die Zukunft abzeichnende Diensteintegration auf der Netzebene wird besondere Absprachen erfordern, evtl. sogar Anpassungen in der Organisation nahelegen.

1.1 Historische Entwicklung

1.1.1 JOKER

Direkte Vorläufer des heutigen KFAnet mit den Protokollfamilien DECnet und Internet sind das JOKER-System, das von 1972 bis 1985 in Produktion war und dessen Nachfolger HYPERNET, dessen Betrieb als Teil von KFAnet 1991 eingestellt wurde.
Neben diesen ausgesprochenen Rechnernetzen gab es – und gibt es weiterhin – Terminalnetze in der KFA wie DATASWITCH/DEVELNET oder das IBM 3270-Terminalnetz, bei denen der Anschluß von Terminals an Rechner in organisierter Weise im Vordergrund steht.

An der Entwicklung JOKER → HYPERNET → INTERNET lassen sich grundsätzliche Entwicklungslinien aufzeigen, und es wird deutlich, daß jede dieser Lösungen unter den Gesichtspunkten aktuelle Gegebenheiten, Anforderungen und technische Möglichkeiten eine eigenständige Position einnimmt.

Das JOKER-System kann durch folgende Merkmale charakterisiert werden, die nachfolgend kurz erläutert werden, um die seitherigen Entwicklungen aufzuzeigen:

- Totale Ausrichtung auf den Host-Rechner
  Die Ausrichtung auf den Host kommt schon im Namen zum Ausdruck:
  JOKER = Jülicher Online Kopplungssystem für Experimentrechner mit einem zentralen Timesharing-Rechner. Sie hatte ihre Hauptursache in den Unzulänglichkeiten der damaligen Experimentrechner, die oftmals ohne eigene Sekundärspeicher und ohne Betriebssystem auskommen mußten. Neben der höheren Rechenleistung war es in noch stärkerem Maße die Verfügbarkeit von allgemein unterstützender Software, von Anwendungssoftware sowie der weit überlegene Bedienungskomfort,

der es erstrebenswert machte, einen möglichst großen Teil der eigentlichen Daten-Verarbeitung in den Host zu verlegen.
Kommunikationsbedarf zwischen Experimentrechnern untereinander bestand nicht. Die notwendigen Sicherheits- und Managementfunktionen standen auf den Experimentrechnern gar nicht zur Verfügung, so daß schon aus diesem Grunde eine solche Kommunikation nur unter Zwischenschaltung des Hosts möglich gewesen wäre, der diese Funktionen hätte wahrnehmen müssen.

- Spezielle Netzhardware
  Anfang der siebziger Jahre gab es den Begriff eines lokalen Netzes (LAN) als generischen Begriff noch gar nicht. Lokale Netze als eigenständige (d.h. von den speziellen Gegebenheiten und Anwendungen unabhängige) Gattung wurden erstmals 1976 mit der Veröffentlichung des Ethernet-Konzepts vorgestellt, und es dauerte danach nochmals eine Reihe von Jahren bis Produkte verfügbar waren.
  Infolgedessen waren Übertragungseinrichtungen im lokalen Bereich immer spezielle, auf die vorhandenen Gegebenheiten und die geplanten Anwendungen zugeschnittene Entwicklungen.

- Spezielle (eigenentwickelte) Netzsoftware
  Aufgrund der im vorigen Punkt erläuterten Randbedingungen (spezielle Hardware, an örtliche Gegebenheiten angepaßte Lösungen) war die erforderliche Netzsoftware notwendigerweise ebenfalls eine spezielle Entwicklung.

- Angebotene Kommunikationsdienste: *Low Level*
  Die den Benutzern angebotenen Kommunikationsfunktionen lagen etwa auf dem Niveau von Read/Write (etwa Schicht 5 im OSI-Modell, wobei auch noch Schicht-4-Funktionen wahrzunehmen waren); dafür gab es mehrere Ursachen:

  - Es gab noch kein allgemeines Verständnis über sinnvollerweise anzubietende Netzfunktionen, schon gar keinen allgemeinen Konsens.

  - Spezialentwicklungen, d.h. Adaptionen an örtliche Gegebenheiten und Anforderungen, verhinderten die Entwicklung allgemein verbindlicher Funktionen.

  - Das verbreitete Streben nach Effizienz verhinderte Generalisierungen.

- Wichtige Zielvorgaben: Konnektivität, Effizienz, kurze Reaktionszeiten
  Kommunikationsfähigkeit war zur Zeit der Entstehung des JOKER-Systems schon zwischen gleichartigen Rechnern eine Seltenheit, so daß das Herstellen von Konnektivität zwischen Rechnern verschiedener Hersteller bereits eine wichtige Zielvorgabe war.
  Die Forderung nach effizienter Abwicklung aller mit dem Kommunikationsprozeß verbundenen Aufgaben ergab sich generell – und nicht nur für die Kommunikation – aus der aus heutiger Sicht sehr beschränkten Leistungsfähigkeit der am Kommunikationsvorgang beteiligten Rechner. Beim JOKER-System kam zu der generellen Vorgabe einer effizienten Nutzung der vorhandenen Rechenkapazitäten hinzu, daß die Experimentrechner ohne eigenen Sekundärspeicher Datenübertragungen zum Großrechner möglichst schnell und mit möglichst geringen Verzögerungen ausfüh-

ren können sollten, um laufende Messungen für diesen Zweck nur kurzzeitig unterbrechen zu müssen.
Dieses Ziel wurde so gut erreicht, daß die Datenraten, die der einzelne Benutzer damals sah, kaum niedriger waren als heute, und die Reaktionszeiten (Overhead) deutlich niedriger waren.

1.1.2 HYPERNET

Die kennzeichnenden Merkmale des Nachfolgesystems HYPERNET (1985-1991), die die Entwicklungen bei den angeschlossenen Rechnern ebenso widerspiegeln wie die Fortschritte in der Netztechnologie, sind folgende:

- De-facto-Ausrichtung auf den Host
  Die angeschlossenen Rechner waren durchaus leistungsfähig und hatten vor allem leistungsfähige Betriebssysteme, die unter Berücksichtigung der etwas anderen Anforderungen denen im Großrechner durchaus gleichwertig waren und insbesondere bezüglich Handhabung und Komfort eher Vorteile hatten. Infolgedessen waren in erster Linie Leistungsgesichtspunkte (Rechenleistung, Speicherkapazität, große Programmpakete) maßgebend für einen Netzanschluß und deshalb der Host fast ausschließlich der Kommunikationspartner. Von der Netzsoftware und der Netztechnik her kam aber jeder angeschlossene Rechner in gleicher Weise als Kommunikationspartner in Frage.

- Herstellerspezifische Netzhardware
  Die Netzhardware, HYPERchannel, war ein käufliches Standardprodukt eines einschlägigen Herstellers. Zum Zeitpunkt der Systementscheidung zugunsten dieses Produktes (Mitte 1984) waren Standard-LANs noch nicht auf dem Markt (Token-Ring) oder noch nicht in der Lage, ein Areal von der Größe des KFA-Geländes abzudecken (Ethernet), da Brücken zur Strukturierung des Netzes noch nicht verfügbar waren.

- Herstellerspezifische und eigenentwickelte Software
  Die Netzsoftware wurde (üblicherweise) vom Lieferanten der Hardware bereitgestellt und war herstellerspezifisch.

- Angebotene Funktionen: *High Level*
  Aufbauend auf der herstellerspezifischen Software der Schicht 5 (NETEX) hat das ZAM in Eigenentwicklung *High-level*-Kommunikationsfunktionen *(File Transfer, Remote Function Call)* bereitgestellt. *Remote Terminal Access* wurde nicht entwickelt, weil dadurch der Aufwand an eigener Entwicklungsarbeit unnötigerweise hochgetrieben worden wäre, da diese Funktion in der KFA durch spezielle Netze abgedeckt wird.

- Wichtige Zielvorgabe: Integration verschiedener Rechnerwelten
  Wichtige Zielvorgabe und Grund für die Wahl von Produkten eines Herstellers von Netzprodukten war die Integration der Rechnerwelten verschiedener Hersteller, insbesondere der für die KFA wichtigen Firmen DEC, IBM und CRAY, was mit den jeweiligen Netzarchitekturen dieser Firmen nur unzulänglich möglich war. Hohe Übertragungsleistungen sollten realisiert werden, um die Übertragung großer Da-

tenmengen zu ermöglichen. Kurze Reaktionszeiten waren angesichts reichlich vorhandener Sekundärspeicherkapazitäten in den angeschlossenen Systemen und der Tatsache, daß die meisten Datenübertragungen von Sekundärspeicher zu Sekundärspeicher erfolgten, deren Zugriffszeiten also ohnedies wirksam wurden, kein vorrangiges Ziel.

1.1.3 INTERNET

Der Übergang von KFAnet/HYPERNET auf KFAnet/INTERNET im Jahre 1990 hatte in der Anfangsphase weder leistungsmäßig noch funktional deutliche Vorteile, war aber wegen des Wegfalls firmenspezifischer Lösungen von immenser Bedeutung. Die Merkmale von KFAnet/INTERNET sind:

- Das Netz steht konzeptionell im Mittelpunkt
  Ein wichtiges Kennzeichen der Entwicklung ist, daß sowohl netztechnisch wie auch konzeptionell der Host nicht mehr im Mittelpunkt steht, obwohl ihm als Erbringer wichtiger Service-Leistungen für eine Vielzahl von Netzteilnehmern (z.B. als *Compute Server* oder *File Server*) immer noch eine erhöhte Bedeutung zukommt. Die angeschlossenen Systeme (heute vielfach PCs oder Workstations) verfügen z.T. über beachtliche Rechenleistungen und sind hinsichtlich der Bedienoberfläche und des Bedienungskomforts den Großrechnern eindeutig überlegen, so daß nun Konzepte in den Vordergrund rücken, bei denen für alle Anwendungen die Workstation die Schnittstelle zum Benutzer bildet, für die Durchführung aber unter Umständen andere, besser geeignete Systeme im Netz in Anspruch genommen werden (*Client/-Server*-Modell, Workstation-Konzept).

- Standard Netzhardware
  Als Netzhardware kommen ausschließlich auf Standards basierende Produkte zum Einsatz, was die Aufhebung der Abhängigkeit von bestimmten Herstellern zur Folge hat; insbesondere die zum Anschluß von Rechnern erforderlichen Interfaces sind oftmals im Lieferumfang des Rechnerherstellers enthalten und zunehmend sogar integraler Bestandteil der Rechner Die wichtigsten Hardwareplattformen sind Ethernet (oder CSMA/CD gemäß IEEE 802.3 bzw. ISO 8802/3) oder Token-Ring (IEEE 802.5 bzw. ISO 8802/5; in der KFA kaum eingesetzt) und in Zukunft vermehrt FDDI (ISO 9314). Der Anteil herstellerspezifischer Netzhardware nimmt derzeit weltweit rapide ab.

- Standard Netzsoftware
  Der für die Zukunft wichtigste Aspekt der Ablösung von KFAnet/HYPERNET durch KFAnet/INTERNET ist der Ersatz der herstellerspezifischen/eigenentwickelten HYPERNET-Software durch die TCP/IP-Protokollfamilie (Internet). Diese Protokollfamilie hat in der Praxis alle Eigenschaften eines (akzeptierten) internationalen Standards: Sie ist nicht herstellerabhängig und findet umfassende Unterstützung durch alle namhaften Hersteller (es gibt praktisch keinen Rechner im gesamten Spektrum vom kleinen PC bis zum Höchstleistungsrechner, für den diese Kommunikationsprotokolle nicht verfügbar sind). Ihr einziger Nachteil: Sie sind nicht formale Standards einer internationalen Standardisierungsorganisation und werden

deshalb langfristig durch (funktional mindestens gleichwertige) ISO-Standards abgelöst werden.

- Netzfunktionen: *High Level*; identisch für Lokal- und Fernbereich; *Client/Server*-Anwendungen
  Die zunächst im Rahmen von KFAnet/INTERNET angebotenen Dienste unterscheiden sich nicht wesentlich von den entsprechenden HYPERNET-Diensten. Es ergeben sich dennoch einige Vorteile und deutlich verbesserte Perspektiven:

  - Integraler Bestandteil der Internet-Protokolle ist TELNET, so daß mit der Einführung dieser Protokolle *Remote Terminal Access* zusätzlich zu den im Rahmen von KFAnet/HYPERNET angebotenen Funktionen zur Verfügung steht.

  - Die Internet-Dienste sind nicht auf KFAnet, d.h. auf die KFA-interne Kommunikation, beschränkt; sie stehen in gleicher Weise für die externe Kommunikation zur Verfügung, und wegen der weiten Verbreitung insbesondere im wissenschaftlich-technischen Bereich können darüber potentiell sehr viele Kommunikationspartner erreicht werden.

  - Die Last der Anpassung an neue Betriebssystemversionen/Betriebssysteme und der Weiterentwicklung liegt nicht mehr bei der KFA und auch nicht mehr bei einzelnen Herstellern. Die Akzeptanz einer einheitlichen Hardware- und Softwareplattform bündelt die weltweit verfügbaren Entwicklungskapazitäten und verspricht erheblich beschleunigte Fortschritte bei der Bereitstellung weiterer Netzdienste (z.b. Network Computing, Management).

- Wichtige Zielvorgabe: Integration
  Durch den Einsatz international akzeptierter Standards ergeben sich umfassende positive Perspektiven, insbesondere

  - Überwindung der negativen Auswirkungen der Inkompatibilitäten in einer heterogenen Rechnerumgebung (offene Kommunikationsumgebung),

  - Bündelung der Entwicklungskapazitäten und dadurch beschleunigte Fortschritte hinsichtlich Funktion, Performance und Stabilität; Integration neuer, fortschrittlicher Netzdienste.

1.1.4 DECnet/Ethernet

DECnet bezeichnet die Netzwerkprodukte der Fa. DEC, die auf der firmeneigenen Netzwerkarchitektur DNA *(Digital Network Architecture)* basieren. DECnet-Produkte gibt es seit Mitte der siebziger Jahre; sie haben sich von funktional bescheidenen Anfängen der ersten Entwicklungsstufe (Phase I) zu sehr umfassenden (im Funktionsumfang etwa der TCP/IP-Protokollwelt entsprechenden) Netzdiensten der derzeit aktuellen Phase IV weiterentwickelt und werden in der Phase V, die ab 1992 eingeführt wird, OSI-Kompatibilität erlangen.
DECnet in der KFA kann wie folgt charakterisiert werden:

- Standard Netzhardware
  Die KFA setzt DECnet nur für die interne Kommunikation ein. Die Standard Hardwareplattform für lokale DECnet-Kommunikation ist Ethernet (gemäß Ethernet-2-Spezifikation), die derzeit noch am weitesten verbreitete Version eines CSMA/CD-Netzes, die nicht ganz dem IEEE 802.3-Standard entspricht; in DECnet Phase V wird auch der IEEE-Standard unterstützt werden. Beide Versionen können auf dem gleichen Kabel koexistieren.
  Der KFAnet-Ethernet-Backbone wurde etabliert, um KFA-weite DECnet-Kommunikation zu ermöglichen. Da Ethernet auch die wichtigste Basis für die lokale Internet-Kommunikation ist, wurde damit auch die Voraussetzung für die KFA-weite Internet-Kommunikation geschaffen.

- Herstellerspezifische Netzsoftware
  Vorrangiges Ziel von DECnet ist die optimale Vernetzung von DEC-Rechnern, auch wenn PCs unterstützt werden und ein Gateway zu IBM SNA-Netzen verfügbar ist. Diese Aussage gilt bis DECnet Phase IV. DECnet Phase V ist eine weitgehende OSI-Implementation (mit dem Ziel, im Laufe der Entwicklung eine vollständige zu werden); d.h. DECnet wandelt sich von einer firmenspezifischen Architektur zu einem offenen Standard, und nur der firmenspezifische Name wird bleiben.

- Netzfunktionen: *High Level*; identisch für Nah- und Fernbereich
  Die Funktionen entsprechen im wesentlichen denen im Internet-Umfeld.

- Bedeutung von DECnet für die Datenkommunikation in der KFA
  In der Vergangenheit war die KFA in ihrem experimentorientierten Teil sehr stark durch DEC-Produkte geprägt, so daß für eine Vernetzung in diesem Bereich DECnet die natürliche Lösung war. Diese DEC-Dominanz ist in diesem Ausmaß heute nicht mehr vorhanden: PCs und Workstations auch anderer Hersteller (HP, IBM, SUN,...) sind inzwischen weit verbreitet und mindern die Bedeutung firmenspezifischer DEC-Lösungen auch im Netzbereich. Tatsächlich trägt DEC der nicht nur in der KFA beobachtbaren Entwicklung zu heterogenen Rechnerumgebungen Rechnung und befindet sich derzeit in einer Phase der Ablösung der firmenspezifischen Kommunikationsprotokolle. Die Fa. DEC bietet heute bereits eine weitgehende Unterstützung der Internet-Protokolle auf ihren Rechnern, und DECnet Phase V ist eine Implementation der OSI-Protkolle. Die Entwicklung bei DEC läuft – den faktischen Gegebenheiten entsprechend – auf die Unterstützung einer Multiprotokollwelt mit den Schwerpunkten Internet und OSI hinaus und liegt damit hinsichtlich der Einschätzung der gegenwärtig und für die Zukunft bedeutsamen Protokollwelten voll auf der Linie der KFA.

2.0 Ziele und Prinzipien

Grundsätzliches Ziel von KFAnet ist es, in Funktion und Leistung ein Angebot an Kommunikationsdienstleistungen bereitzustellen, das den überwiegenden Teil der Anforderungen aus dem wissenschaftlich-technischen Bereich abdeckt.

2.1 Netzstruktur

Die Entwicklung im Bereich der Datenkommunikation ist derzeit geprägt von einer rasch fortschreitenden Einbindung einer großen Zahl kleiner und kleinster Rechner (Workstations, PCs) in einen weltweiten Kommunikationsverbund.
Wegen der Vielzahl der Kommunikationsanforderungen, die überdies sowohl bezüglich der geographischen Randbedingungen als auch der geforderten Funktionalität wechseln, wäre ein Realisierungskonzept auf der Basis individuell zugeschnittener Lösungen nicht durchhaltbar. Das heute allgemein angewendete, tragfähige Konzept besteht darin, ein möglichst universelles Netz bereitzustellen, das in der Lage ist, den überwiegenden Teil der Kommunikationsanforderungen abzudecken. Hierdurch wird eine offene Netzumgebung geschaffen, in der potentiell jeder Teilnehmer mit jedem anderen Teilnehmer kommunizieren kann.
Die grundsätzliche Struktur von KFAnet, bestehend aus den Komponenten Backend-Netz, Backbone-Netz und nachgeordnete Netze (Institutsnetze), ist in Abb. 1 dargestellt.

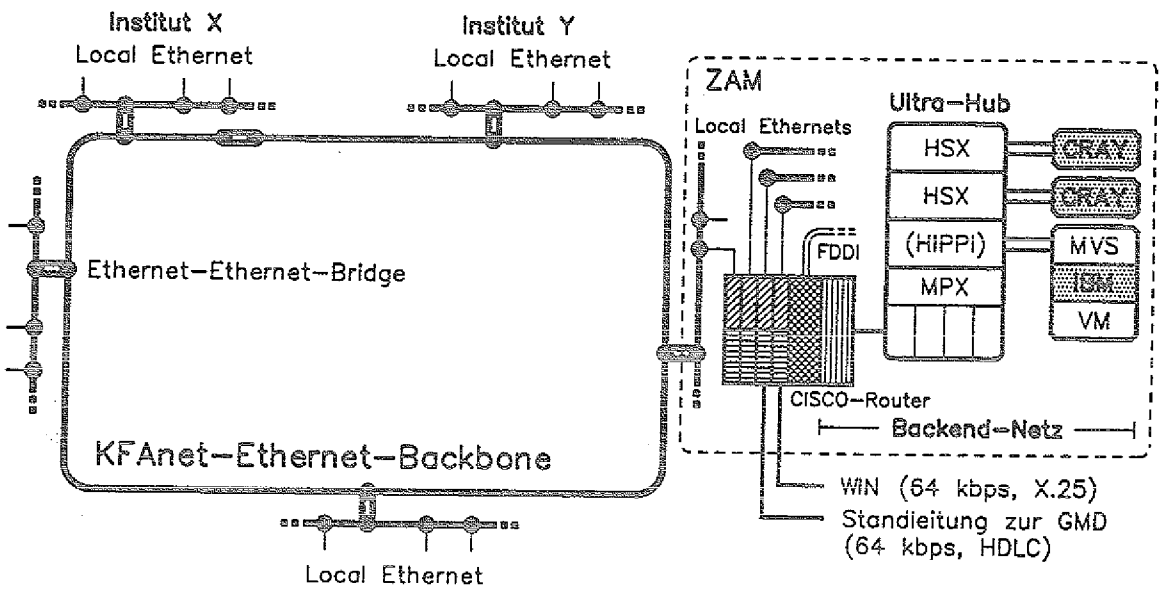


Abb. 1. KFAnet – Grundstruktur

KFAnet ist ein lokales Netz, welches auf LAN-Technologien basiert. Kennzeichen dieser Technologie sind Übertragungskanäle recht hoher Bandbreite, in die sich aber – je nach Netzstruktur – eine größere Anzahl von Stationen teilen muß.
Es ist heute unbestritten (und in vielen Fällen auch bereits realisiert), daß in großen Einrichtungen mit entsprechend großen lokalen Netzen eine Strukturierung dieser Netze

erforderlich ist, dies um so mehr, als die heutigen LANs Broadcast-Netze sind, d.h. jedes Informationsbit durch das gesamte Netz geschleust und allen Teilnehmerstationen angeboten wird. Es muß sichergestellt werden, daß Informationen, die ihrer Natur nach lokal sind (bezogen auf ein Experiment, ein Institut oder ein Projekt), auch lokal bleiben und nur solche Daten den engeren Bereich verlassen, die einen Adressaten außerhalb des Bereichs haben. Dies wird durch eine Strukturierung der Netze mit Hilfe von Gateways (Brücken oder Router) erreicht.
Sehr verbreitet – und auch in KFAnet realisiert – ist eine hierarchische Strukturierung in ein Backbone-Netz (KFAnet-Backbone) und nachgeordnete Netze (Institutsnetze). Die hierarchische Struktur ist deshalb weit verbreitet, weil sie

1. gut verstanden und beherrschbar ist,
2. gute Voraussetzungen für das Netzmanagement mitbringt,
3. i.a. gut in die Organisationsstruktur eines Unternehmens einpaßbar ist.

Es ergibt sich daraus eine Reihe von Vorteilen:

1. Für die nachgeordneten Netze:

   - Lokale Datenflüsse bleiben lokal.

     ⇒ Verbesserte Datensicherheit

     ⇒ Lokale Kommunikationsfunktionen sind auch bei Ausfall des Backbone sichergestellt

   - Auswahl und Strukturierung der Institutsnetze können gemäß den lokalen Anforderungen und Gegebenheiten erfolgen. Randbedingung ist, daß ein Gateway zum Backbone verfügbar ist.
     Generell geht der Trend dahin, eine Vielzahl kleiner LANs einzurichten, so daß die Institutsnetze in vielen Fällen selbst wieder durch Brücken (oder Router) strukturierte Netze sein werden. Das berührt aber nicht den Backbone. Aus Sicht des Backbone handelt es sich dabei um ein logisches Netz, das an genau einer Stelle an den Backbone angebunden ist.

   - Die verwendete Netzsoftware ist nicht auf die in KFAnet unterstützten Protokolle beschränkt. Im internen Verkehr können auch andere Protokolle verwendet werden. Von dieser Freiheit sollte allerdings aus Gründen der Bedienung und des Managements nur dann Gebrauch gemacht werden, wenn es gute Argumente dafür gibt.

2. Für den Backbone:

   - Der Backbone wird nicht mit dem lokalen Verkehr der einzelnen Institute beaufschlagt d.h. die Gefahr einer Überlastung ist geringer.

   - An den Backbone müssen und sollen aus Gründen der Datensicherheit, der Betriebssicherheit und des Managements keine Endgeräte (Benutzerstationen) direkt angeschlossen werden.

Es ist denkbar, daß in der Anfangsphase des Aufbaus des KFAnet-FDDI-Backbone aus Kostengründen vorübergehend von dieser Forderung abgewichen werden muß, als strategisches Prinzip bleibt sie aber bestehen.

- Die Netztechnik im Backbone kann von der in den nachgeordneten Netzen verschieden sein. Dies ist bedeutsam, weil bei großem Netzausbau mit vielen nachgeordneten Netzen der Backbone als Sammelschiene eine höhere Leistung als die einzelnen angeschlossenen Netze haben sollte. Die damit einhergehenden höheren Kosten sind im Backbone-Bereich generell, aber auch wegen der begrenzten Zahl erforderlicher Anschlußeinheiten vertretbar. Genau aus diesen Gründen wird FDDI als neues und noch vergleichsweise teures Hochleistungs-LAN nicht nur in der KFA, sondern weltweit derzeit vorrangig und überwiegend im Backbone-Bereich eingeführt.

Als Gateways zwischen dem im Aufbau befindlichen KFAnet-FDDI-Backbone und den daran anzuschließenden Institutsnetzen sollen ausschließlich Router (Level-3-Gateways) eingesetzt werden.
Die Vor- und Nachteile des Einsatzes von Routern bzw. Brücken zur Strukturierung lokaler Netze werden in der gemeinsamen Dokumentation von ZAM und ZEL mit dem Titel 'Entwicklung KFAnet' diskutiert. Im Rahmen der hier dargelegten Grundsätze soll nur noch einmal ein grundsätzlicher Unterschied herausgestellt werden:
Brücken vermitteln als Level-2-Gateways von Hause aus protokolltransparent auf der Basis der Hardware(*MAC-level-*)- Adressen zwischen den Teilnetzen, die sie verbinden. Um im Backbone die Beschränkung auf die in KFAnet unterstützten Protokollwelten durchzusetzen (d.h., um zu verhindern, daß sich angeschlossene Teilnehmer über diese Beschränkung hinwegsetzen und andere, möglicherweise Probleme erzeugende Protokolle verwenden), ist in Brücken zusätzlicher Aufwand erforderlich; es müssen – so vorhanden – entsprechende Filter definiert werden, und es sind Konstellationen denkbar, wo es überhaupt nicht geht.
Bei Routern ist die Situation genau umgekehrt: Router vermitteln protokollspezifisch, d.h., alle Verbindungen, die nicht auf den explizit zugelassenen Protokollen basieren, sind automatisch gesperrt. Sollen andere – insbesondere nicht allgemein verbreitete – Protokolle vermittelt werden, so müssen diese explizit zugelassen werden, oder es muß – so vorhanden – die Brückenfunktion aktiviert werden, und es kann sein, daß sie überhaupt nicht vermittelt werden können.
Grundsätzlich bewirken Router eine stärkere, auf allen Ebenen des Netzbetriebs und der Netzverwaltung nachvollziehbare Abtrennung der nachgeordneten Netze.

Durch das Backend-Netz werden besonders leistungsfähige Verbindungen (bis zu 800 Mbps) zwischen den wichtigsten Server-Systemen im ZAM hergestellt. Kern ist ein UltraNet-Hub (zentrale Vermittlungseinrichtung), an den die zu verbindenden Komponenten sternförmig angeschlossen sind; derzeit sind dies die beiden CRAY-Systeme sowie das MVS-System auf der IBM ES/9000-620 und der CISCO-Router, über den die Verbindung zur Außenwelt (insbesondere KFAnet) hergestellt wird.
Konzeptionell ist das Backend-Netz nichts anderes als ein B-Netz im ZAM, dem allerdings aufgrund der Aufgabenstellung des ZAM, Ressourcen zentral für die gesamte KFA bereitzustellen, eine besondere, über das ZAM selbst hinausgehende Bedeutung zukommt.

2.2 Leistungsüberlegungen

Typisch für den heutigen Entwicklungsstand in lokalen Netzen ist, daß die Übertragungsleistungen, die der einzelne Netzteilnehmer sieht, nicht durch die Leistungsfähigkeit des Netzes, sondern durch den Overhead in der Kommunikationssoftware der beteiligten Rechner bestimmt wird, und das Netz selbst nur durch Summeneffekte zum begrenzenden Faktor wird. Besonders anfällig dafür ist der KFA-weite Backbone als Verbindungskanal für eine große Zahl von Institutsnetzen. Dem Backend-Netz als Medium zur Verbindung der Hochleistungssysteme im ZAM untereinander und mit dem KFA-weiten Backbone ist aufgrund der Leistungsfähigkeit dieser Komponenten und wegen der Bedeutung dieser Systeme (z.B. als *Compute Server* oder *File Server*) für das zentrale Dienstangebot des ZAM ebenfalls besondere Beachtung zu schenken.
Es ist das erklärte Ziel des ZAM, Backend-Netz und Backbone-Netz als zentrale Komponenten von KFAnet leistungsmäßig so auszubauen, daß Engpässe vorhersehbar nicht auftreten können.
Dies ist eine strategisch bedeutsame Position, weil die Entwicklung bei den Anwendungen dahin geht, daß zunehmend (z.T. ohne explizites Zutun und Wissen des Benutzers) auch größere Datenmengen kurzfristig über das Netz ausgetauscht werden müssen. Damit dies (etwa beim interaktiven Vor- bzw. Nachbereiten großer Datenmengen in hochauflösender graphischer Darstellung im Zusammenspiel einer Workstation mit einem Höchstleistungsrechner) in für den Benutzer befriedigend kurzer Zeit erfolgen kann, ist die Verfügbarkeit sehr hoher Übertragungsleistungen unabdingbar, die i.a. aber nur sporadisch genutzt werden, so daß daraus eine geringe mittlere Netzauslastung resultiert (die auch schon für heutige LANs typisch ist). Kernpunkt der Aussage ist, daß in diesem Umfeld die Auslegung der Netzkapazitäten sich an den Maximalanforderungen orientieren muß und nicht – wie in der klassischen Kommunikation üblich – an den mittleren Belastungen.

2.3 Funktionen, Dienste

Die über KFAnet bereitgestellten Funktionen sind zunächst die klassischen Kommunikationsfunktionen

- *Remote Terminal Access (Interactive Login),*
- *File Transfer,*
- *Electronic Mail* und
- *Remote Execution.*

Darauf aufbauend lassen sich für weite Anwendungsbereiche *Server* etablieren, deren Dienste über das Netz bereitgestellt werden können.
Längerfristig wird eine wirkliche (und weitgehend automatische) Verteilung von Funktionen im Netz angestrebt, zumindest für solche Anwendungen, für die dies von Nutzen ist. Die Werkzeuge hierfür (z.B. das *Distributed Computing Environment* (DCE) der OSF) befinden sich aber noch in der Entwicklung.
Die bereitgestellten Dienste und die diese Dienste realisierenden Protokolle werden ausführlich in Kapitel 5 behandelt. Hier sollen nur einige grundsätzliche Aspekte angesprochen werden.

Es stehen heute mehrere Plattformen (Hardware und Software) zur Verfügung, um bestimmte Kommunikationsfunktionen realisieren zu können.
In einer großen Forschungseinrichtung mit einem sehr weiten Aufgabenspektrum und demzufolge auch sehr vielfältigen Kommunikationsanforderungen muß von einer Vielfalt von Endgeräten und einer Vielzahl von Implementationen der ausgewählten Protokolle ausgegangen werden. Es kann deshalb nur solche Netzhardware und -software zum Einsatz kommen, die eine große Herstellerbasis hat (am besten international anerkannte Standards), so daß Interoperabilität sichergestellt ist und in einem großen und komplexen Netz sowohl aus Sicht des einzelnen Teilnehmers wie auch des Netzbetreibers ein stabiler Betrieb möglich ist.

Eine wichtige Voraussetzung für ein über einen längeren Zeitraum gültiges Dienstangebot in einer sehr heterogenen Umgebung ist die Schaffung langfristig stabiler Randbedingungen für die Datenkommunikation innerhalb von KFAnet.
Es war von Anfang an die Philosophie von KFAnet, den Benutzern Kommunikationsdienste anzubieten und nicht ein bezüglich der darüber abzuwickelnden Protokolle transparentes Transportnetz. Hierfür waren und sind folgende Gründe ausschlaggebend:

1. In einer Umgebung wie der KFA wäre in einem transparenten Netz kaum steuerbar, wer mit welchen Endgeräten was auf dem Netz treibt, mit unabsehbaren Folgen für die Sicherheit und Stabilität des Netzbetriebs.
   Die Gefährdung geht nicht in erster Linie von den verwendeten Protokollen als solchen aus, sondern ist mehr die Folge oft unvollständiger oder fehlerhafter Implementationen in Hardware und Software. Die Erfahrung in der KFA zeigt, daß aufgrund fehlerhafter Software massive Probleme bei bestimmten Rechnerfamilien bei (versuchsweisem) Einsatz vorher nicht genutzter Protokolleigenschaften auftreten können.

2. Ein transparentes Netz kann zwar von allen Teilnehmern gleichermaßen genutzt werden, miteinander kommunizieren können aber nur solche Teilnehmer, die die gleichen Protokolle verwenden. Dabei wäre es fast unvermeidlich, daß sich verschiedene untereinander nicht kommunikationsfähige Protokollgemeinschaften bilden würden. Es stünde also zu befürchten, daß die KFA kommunikationsmäßig in verschiedene Teilbereiche zerfallen würde.
   Da diese Gefahr in einer multidisziplinären Einrichtung wie der KFA stets besteht, ist es immer das Anliegen des ZAM gewesen, wenn – wie in KFAnet – aus historischen Gründen die Zulassung von mehr als einer Protokollwelt unvermeidlich ist, durch Bereitstellung von Gateways ein solches Auseinanderfallen zu verhindern.

3. Die Beschränkung auf wenige Protokollfamilien hilft, die zentrale Unterstützung der Nutzer qualitativ und quantitativ sicherzustellen.
   Grundsätzlich sollte die Zahl der unterstützten Protokollwelten möglichst gering gehalten werden, und mit der Verfügbarkeit der OSI-Protokolle besteht längerfristig vielleicht sogar die Chance einer Vereinheitlichung für weite Anwendungsbereiche.

2.4 Externe Kommunikation

Wenn auch in großen Einrichtungen ein großer Teil der Kommunikation interne Kommunikation ist (dies gilt gleichermaßen für Sprach- wie für Datenkommunikation), so gibt es dennoch in erheblichem Umfang auch Nachfrage nach externer Kommunikation, und zwar sowohl national wie auch international.
Als Aufgabe der Weitverkehrsnetze (WANs) wird heute nicht mehr die Verbindung einzelner geographisch weit voneinander entfernter Rechner, sondern in erster Linie die Interkonnektion der lokalen Netze geographisch entfernter Einrichtungen gesehen. Die Folge ist, daß durch eine solche Verbindung alle Teilnehmer des lokalen Netzes einer Einrichtung potentiell mit allen Teilnehmern des lokalen Netzes einer anderen Einrichtung kommunizieren können.
Da überdies auch intern nach Möglichkeit keine speziellen Verbindungen mehr zwischen Kommunikationspartnern etabliert werden, sondern wie in KFAnet ein möglichst universell nutzbares Netz einen möglichst großen Teil der Kommunikationsanforderungen abdecken soll, ergibt es sich, daß durch den Anschluß an ein solches allgemeines Netz ein Teilnehmer nicht nur die (u.U. sehr wenigen) gewünschten Kommunikationspartner, sondern potentiell alle Teilnehmer dieses Netzes und, falls dieses Netz eine Außenanbindung besitzt, auch alle Teilnehmer des weltweiten Kommunikationsverbunds erreichen kann; und weil diese Beziehungen symmetrisch sind, ist er selbst auch von allen diesen potentiell erreichbar. Eine solche offene Netzumgebung erfordert es deshalb, daß jede Teilnehmerstation zum eigenen Schutz dafür Sorge tragen muß, daß sie nicht von außen korrumpiert werden kann.
Der Einsatz von Gateways bei der Außenanbindung und bei der Anbindung der Institutsnetze an den Backbone erlaubt es, Sicherheitsfunktionen und darüberhinaus allgemeine Management- und Verwaltungsfunktionen netzseitig, d.h. unabhängig vom einzelnen Teilnehmer zu etablieren.
Über die KFA-weite Kommunikation hinaus ist es also die Aufgabe von KFAnet, jedem Teilnehmer an einer zentralen und überwachbaren Stelle in wohldefinierter Weise die Kommunikation mit der Außenwelt zu ermöglichen.
Aus Benutzersicht ist zu fordern, daß für die externe Kommunikation (national wie international) die gleichen Dienste zur Verfügung stehen wie intern und sich vor allen Dingen unabhängig vom Ziel in gleicher Weise darbieten. Dies ist für die beiden derzeit in KFAnet unterstützten Protokollwelten, DECnet und Internet, gegeben. Für DECnet ist diese Aussage nur von theoretischem Wert, da DECnet nur KFA-intern angeboten wird.
Die Internet-Protokolle werden für die interne und die externe Kommunikation angeboten, und einen grundlegenden Unterschied gibt es weder in den verfügbaren Funktionen noch in der Bedienung. Dennoch gibt es signifikante Unterschiede, die sich aus der um mehrere Größenordnungen geringeren Leistung der externen Übertragungskanäle ergeben. Derzeit erfolgt die Außenanbindung mit 64 kbps an das X.25-Wissenschaftsnetz. Diese Übertragungsleistung setzt den sinnvoll übertragbaren Datenmengen (und damit auch File-Größen) sehr viel engere Grenzen als das KFA-interne 10-Mbps-Ethernet. Auch *Remote Terminal Access* (TELNET), wiewohl funktional uneingeschränkt möglich, ist wegen der oftmals großen Zahl von Zwischenstationen (*Multi-hop*-Verbindungen) mit großen Verzögerungen behaftet und deshalb für interaktive Anwendungen mit hoher Interaktionsrate nur unbefriedigend nutzbar.

Diese Aussagen gelten für die augenblickliche Situation. Wie im internen Bereich sind aber auch im externen Bereich Leistungssteigerungen zu erwarten. So ist für 1992 eine Erhöhung der Übertragungsleistung im WIN (Wissenschaftsnetz) von 64 kbps auf 2 Mbps angekündigt, wodurch sich die leistungsbedingte Schwelle für extern sinnvoll betreibbare Anwendungen deutlich nach oben verschieben wird.
Sehr langfristig werden mit der Verfügbarkeit sehr breitbandiger (und bezahlbarer) Übertragungskanäle (etwa im Breitband-ISDN) die Beschränkungen, denen die externe Kommunikation aus übertragungstechnischen Gründen gegenüber der internen Kommunikation noch unterliegt, weitgehend verschwinden.

3.0 Infrastruktur

Eine sehr wichtige und im Gegensatz zu elektronischen Komponenten und zur Software langfristig stabile Größe ist die Kabelinfrastruktur. Während die Lebensdauer einer Generation der Systemtechnik (elektronische Geräteausstattung) heute allenfalls 5–7 Jahre beträgt, liegt die Nutzungsdauer der Kabelinfrastruktur bei mindestens 15–20 Jahren, d.h. eine einmal realisierte Kabelinfrastruktur muß mehrere Generationen der Elektronik überdauern. Diese Aussage bezieht sich nicht auf Adhoc-Verkabelungen (etwa in einem Labor), sondern auf Verkabelungen zwischen Gebäuden oder systematische Verkabelungen in Gebäuden.
Daß die Kabelinfrastruktur langfristig zu sehen ist, liegt nicht nur daran, daß die technisch sinnvolle Nutzungsdauer passiver Kabel eben so lang ist, sondern auch daran, daß Verkabelungsmaßnahmen einen langen Planungsvorlauf benötigen und aus Kostengründen auch nur abschnittsweise durchgeführt werden können, so daß der Aufbau einer flächendeckenden bzw. bedarfsgerechten Netzinfrastruktur eine Reihe von Jahren in Anspruch nimmt. Dies ist zumindest in der KFA so, wo die Finanzierung aller Kommunikationsvorhaben einschließlich der Infrastrukturmaßnahmen aus regulären jährlichen Etatmitteln erfolgt, was zu einer eher evolutionären und kontinuierlichen Entwicklung der Kommunikationssysteme zwingt, bzw. da dies über alles positiv zu werten ist, eine solche erlaubt. Im Gegensatz dazu führt eine projektorientierte Finanzierung – wie sie für Hochschulen typisch ist – tendenziell zu spektakulären Entwicklungsschritten (mit anschließendem Stillstand bis zum nächsten gravierenden Entwicklungsschritt).
Unter den gegebenen Randbedingungen bietet vorhandene Kabelinfrastruktur, die einerseits natürlich eine Einengung der Planungsfreiheit zukünftiger Systeme darstellt, andererseits aber – wenn es gelingt, sie sinnvoll in neue Konzepte und Vorhaben einzubeziehen – die Chance, sehr viel schneller zu viel weitreichenderen Ergebnissen zu kommen als dies sonst unter den gegebenen finanziellen Randbedingungen möglich wäre.

3.1 Das 75 Ω Koaxialkabelnetz

Die erste systematische Verkabelung für die Datenkommunikation in der KFA war der Aufbau des 75 Ω Koaxialkabelnetzes für das JOKER-System. Dieses Netz in Baumstruktur ist deshalb auch zum ZAM (Rechenzentrum) hin orientiert (im Gegensatz zur Fernmeldeverkabelung, die zur Telefonzentrale (TD-N) orientiert ist). Es wurde in den siebziger Jahren in mehreren Bauabschnitten realisiert. Das Kabel ist ein Standardkabel der Deutschen Bundespost, das aus 12 Koaxtuben nebst Beipack besteht und auch nach den Richtlinien der DBP verlegt wurde (was sich im nachhinein, als die Kabel neuen Verwendungszwecken zugeführt wurden, als sehr positiv herausgestellt hat). Das Kabel ist erdverlegt und zur Sicherheit druckluftüberwacht. Ein derart steifes Kabel mit so großen minimalen Biegeradien wäre keinesfalls – selbst wenn dort Platz gewesen wäre – im vorhandenen Formsteinnetz der KFA verlegbar gewesen.
Bei den Koaxtuben handelt es sich um sogenannte Minituben, d.h. Tuben kleiner Abmessung, die aber gute Signaleigenschaften haben und – da als Dielektrikum Luft verwendet wird – eine sehr hohe Signalausbreitungsgeschwindigkeit (0,99 c) aufweisen.

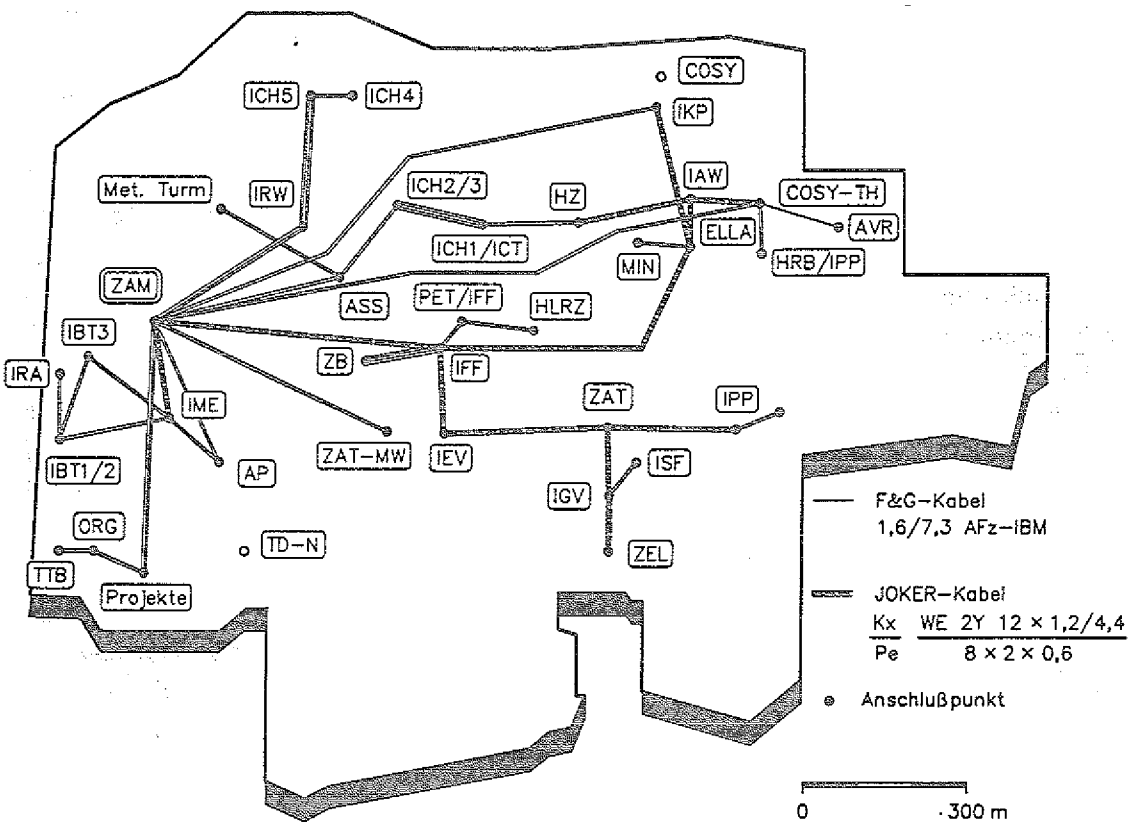


Abb. 2. 75 Ω Koaxialkabelnetz der KFA (Stand: IV/1991)

Eine zweite, sich ebenfalls über mehrere Jahre hinziehende Phase des Ausbaus des Koaxialkabelnetzes begann 1985 mit dem Aufbau des HYPERbus/HYPERchannel-Netzes in der KFA. Hierbei kam ein hochwertiges Hochfrequenzkabel zum Einsatz, das von F&G für die Verwendung mit IBM 5080 Graphiksystemen und für allgemeine LAN-Anwendungen ertüchtigt wurde. Dieses Kabel besitzt die gleichen Abmessungen und Leistungsdaten wie das von NSC für den Anschluß von HYPERchannel-Komponenten vorgeschriebene Kabel, so daß in der KFA auf den Einsatz der von NSC aus den USA importierten und um ein Vielfaches teureren Originalkabel verzichtet werden konnte. Verlegt wurden Einzeltuben in das vorhandene Formsteinnetz der KFA.
Das 75 Ω Koaxialkabelnetz wird auch für den KFAnet-Ethernet-Backbone genutzt, was den Einsatz modifzierter *Transceiver* erforderlich macht.
Auf einigen wenigen kurzen Verbindungsstrecken (zwischen den IPP-Baracken und der Halle, zwischen dem ZAM und der ISR-Baracke sowie zwischen dem IFF-Neubau und den benachbarten Leichtbauten (ATÖ, HLRZ, ISI)) sind auch 50 Ω Koaxialkabel *(Yellow Cable)* verlegt.
Der derzeitige Ausbau des Koaxialkabelnetzes ist in Abb. 2 dargestellt und kann als endgültig angesehen werden, da Koaxialkabel in der Kommunikation der Zukunft keine Rolle mehr spielen werden (im unteren Leistungsbereich werden sie durch verdrillte Kupferleitungen, im oberen Leistungsbereich durch Glasfasern verdrängt).

3.2 Verdrillte Kabel

Das im vorigen Kapitel beschriebene Koaxialkabelnetz betrifft in erster Linie Verbindungen zwischen den Instituten, die für die KFA-weite Kommunikation benötigt werden. Da bei HYPERbus/HYPERchannel die F&G-Kabel bis an die anzuschließenden Geräte herangeführt werden mußten, sind diese Kabel insbesondere für Rechneranschlüsse auch in den Gebäuden verlegt worden. Dieser Kabeltyp ist aber nicht für systematische Verkabelungen in Gebäuden eingesetzt worden.
Inzwischen werden Netzanschlußpunkte für die Datenkommunikation – wie Telefonanschlüsse im Bereich der Sprachkommunikation – zunehmend als obligatorischer Bestandteil der Gebäudeinfrastruktur angesehen, und dementsprechend rücken Methoden und Konzepte für eine systematische, strukturierte und universell verwendbare Verkabelung von Gebäuden in den Vordergrund des Interesses.
Auf der untersten hierarchischen Verkabelungsebene, die als *horizontal* (Etagenebene) bezeichnet wird, werden heute überwiegend verdrillte Kupferdoppeladern eingesetzt, die in abgeschirmten (STP = *Shielded Twisted Pair*) und in ungeschirmten (UTP = *Unshielded Twisted Pair*) Ausführungen verfügbar sind. Durch Fortschritte in der Kabeltechnik, mehr aber noch durch Fortschritte in der Übertragungstechnik können über solche Kabel heute Übertragungsleistungen realisiert werden, die vor wenigen Jahren noch für unmöglich gehalten wurden. Über die für die horizontale Ebene geforderte Entfernung von 100 m (und z.T. noch deutlich darüberhinaus) funktionieren Ethernet (10 Mbps), Token-Ring (4 und 16 Mbps) und selbstverständlich ISDN und E1 (2 Mbps), ja es gibt bereits erste Ankündigungen für 100 Mbps-Systeme (FDDI, wobei das 'F' nicht mehr gilt), wenn auch noch nicht über die vollen 100 m.
Eine solche Kabelinfrastruktur ist also universell verwendbar und erlaubt Kommunikation auf der Basis der meisten der heute aktuellen Systeme.
In der nächst höheren Hierarchiestufe (als *vertical* bezeichnet) können ebenfalls verdrillte Kabel oder Lichtwellenleiter zum Einsatz kommen. Auch Koaxialkabel können verwendet werden; dank der Leistungssteigerungen bei verdrillten Kabeln und der Kostensenkungen in der Glasfasertechnik haben sie im Grunde genommen aber keine Daseinsberechtigung mehr, d.h. da, wo verdrillte Leitungen leistungsmäßig nicht mehr ausreichen, werden heute sinnvollerweise Lichtwellenleiter eingeplant.
Für die oberste Hierarchiestufe, Verbindungen zwischen Gebäuden, sind Lichtwellenleiter obligatorisch.

In der KFA werden derzeit in Neubauten oder bei systematischen Neuverkabelungen in Gebäuden vorzugsweise geschirmte verdrillte Kabel (IBM Verkabelungssystem, Kabel Typ 1) verlegt.
Solche Verkabelungen sind aber Angelegenheit der Institute und der für Infrastrukturmaßnahmen zuständigen KFA-Stelle (AP) und nur insofern für KFAnet bedeutsam, als darüber Institutsnetze betrieben werden können, die durch Anschluß an KFAnet Bestandteil von KFAnet werden können.

3.3 Glasfasern

Es kann heute kein Zweifel daran bestehen, daß das (leitungsgebundene) Übertragungsmedium der Zukunft die Glasfaser ist, und zwar die Monomodefaser. Nachdem sich die

Postgesellschaften weltweit für die ausschließliche Verwendung von Monomodefasern entschieden haben (etwa 90% des weltweiten Produktionsvolumens entfällt auf Monomodefasern), kommt den Gradientenfasern nur noch für eine befristete Zeit und in bestimmten Bereichen Bedeutung zu. Ein solcher Bereich sind die heutigen Glasfaser-LANs, die unter den Gesichtspunkten der unmittelbaren Verfügbarkeit, der Langzeitstabilität und der Kosten auf LED-Übertragungstechnik setzen und damit den Einsatz von Gradientenfasern erfordern.

Die ersten LWL-Verbindungsstrecken in der KFA (vgl. Abb. 3) zwischen IFF und ELLA und zwischen dem ZAM und TD-N bestehen aus Gradientenfasern der Abmessung 50/125 μm, was seinerzeit die Standardabmessung der Deutschen Bundespost (und anderer europäischer Postverwaltungen) für Gradientenfasern war.

Nachdem die Postverwaltungen den Übergang zu Monomodefasern vollzogen haben, haben sich die mit der Standardisierung von Glasfaser-LANs befaßten Gremien auf die von AT&T propagierte Gradientenfaser der Abmessung 62,5/125 μm als Referenzfaser geeinigt, d.h., Fasern anderer Abmessung (insbesondere 50/125 μm) können ebenfalls verwendet werden, u.U. aber mit Einschränkungen hinsichtlich der in Standards angegebenen Entfernungen. Infolge dieser Entwicklung hat die KFA seit 1989 Gradientenfasern der Abmessung 62,5/125 μm verlegen lassen. Seit 1990 werden Kabel verlegt, die zusätzlich auch eine Anzahl Monomodefasern enthalten, um möglichst frühzeitig auch mit diesen Fasern experimentieren und Erfahrungen sammeln zu können und sie in besonders kritischen Anwendungsfällen auch für konkrete Anwendungen zur Verfügung zu haben.

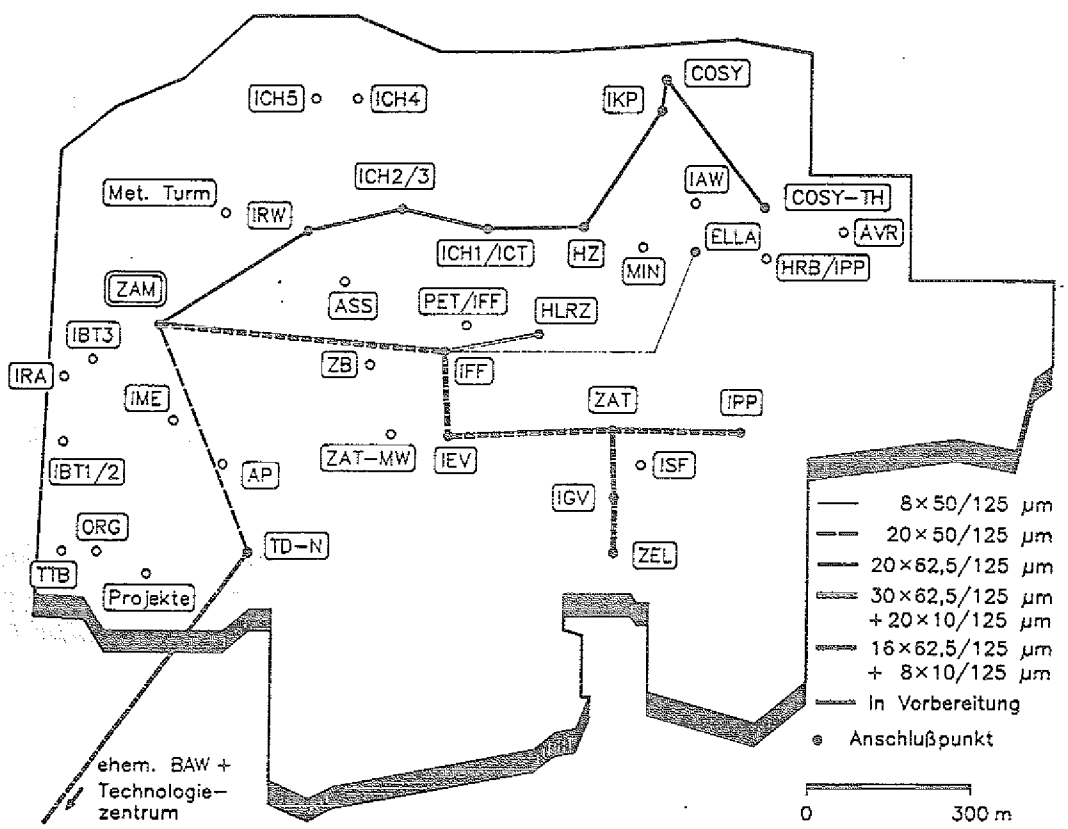


Abb. 3. Glasfasernetz der KFA (Stand: IV/1991)

Die Streckenführung bzw. die Aufpunkte im Glasfasernetz orientieren sich an denen des Koaxialkabelnetzes, so daß ein Overlay-Netz entsteht, das bedarfsgerecht ausgebaut werden kann und an den Anforderungsschwerpunkten den Übergang auf die leistungsfähigere Glasfasertechnik erlaubt.
Die bisher betriebenen und in Abb. 3 dargestellten Glasfaserstrecken stellen eine Zwischenstufe dar, die es gestattet, unmittelbar Glasfaser-LANs aufzubauen sowie Leistungsengpässe und Störprobleme mit zeitgemäßen technischen Mitteln beseitigen zu können. Langfristig wird eine systematische Neuverkabelung der KFA mit Monomodefasern als Ersatz des heutigen Fernsprechkabelnetzes anstehen.

3.4 Grundsätzliche Überlegungen

Sowohl beim Koaxialkabelnetz wie auch beim Glasfasernetz erfolgte und erfolgt der Ausbau bedarfsorientiert, d.h. aufgrund konkreter Anforderungen unter Berücksichtigung der Zahl und Bedeutung dieser Anforderungen nach Maßgabe der verfügbaren Mittel. Dies betrifft jedoch nur die Ausdehnung und die Streckenführung, nicht aber die Zahl der verlegten Leitungen. Seit jeher sind mehr Leitungen verlegt worden als für den die Infrastrukturmaßnahme auslösenden Zweck benötigt wurden: Für JOKER wurden 12 Koaxtuben verlegt (plus Beipack), obgleich das JOKER-System selbst nur fünf Tuben benötigte, von den F&G-Kabeln wurde grundsätzlich mindestens ein Kabel mehr verlegt, als für den Aufbau des HYPERchannel-Netzes erforderlich war, und bei dem noch im Ausbau befindlichen Glasfasernetz werden deutlich mehr Fasern verlegt als für den absehbaren Aufbau des KFAnet-FDDI-Backbone benötigt werden. Die so über den Bedarf von KFAnet (bzw. seiner Vorgänger) hinaus geschaffenen Reservekapazitäten sind außerordentlich wichtig und haben strategische Bedeutung:

- In einer heterogenen Umgebung wie der KFA entstehen immer wieder, u.U. zeitlich und/oder bereichsmäßig begrenzte Kommunikationsanforderungen, die über ein allgemeines Netz (KFAnet) nicht oder nur schwer abzudecken sind. Wenn zur Befriedigung solcher Anforderungen keine Infrastruktur zur Verfügung steht, muß versucht werden, solche Anwendungen in die bestehenden Systeme hineinzupressen, u.U. mit erheblichem Aufwand und oft genug mit negativen Auswirkungen für alle Beteiligten. Die Bereitschaft, in solchen Fällen gegebenenfalls die notwendige Infrastruktur zu schaffen genügt nicht:

  1. In jedem Falle würden langwierige Diskussionen ausgelöst. Die Anforderungen, die an die Gewichtigkeit der Argumente gestellt werden, um für eine Einzelanforderung eine Infrastrukturmaßnahme durchzusetzen, sind sehr viel höher als wenn es darum geht, eine vorhandene Leitung zu nutzen.

  2. Der Zeitfaktor spielt eine große Rolle. Die Erfahrung lehrt, daß eine nichttriviale Verkabelungmaßnahme ein halbes bis ein Jahr in Anspruch nimmt. Dies kann für kurzfristig entstehende Kommunikationsanforderungen im Forschungsbereich ein unzumutbar langer Zeitraum sein.

  Ein gutes Beispiel ist die Einführung des KFA-weiten CAD-Systems CATIA auf der Basis des IBM 5080 Graphiksystems, mit dessen Test und nachfolgendem Aufbau unmittelbar begonnen werden konnte, weil die erforderlichen Koaxialkabel zur Ver-

fügung standen. Die Tatsache, daß die Kabelreserven weitgehend ausgenutzt sind, zeigt, daß vielfältige Anwendungen außerhalb von KFAnet ein Faktum sind.

- Auch für KFAnet selbst sollten Reserven vorhanden sein, weil gegenüber den ursprünglichen Planungen Veränderungen eintreten können, etwa daß aus Last- oder Sicherheitsgründen Streckenabschnitte redundant ausgelegt werden müssen oder die Topologie verändert werden muß. Auch ist die Technik von KFAnet nicht für alle Zukunft festgeschrieben und ein Nachfolgesystem muß im Test- und Pilotbetrieb parallel und unabhängig vom Produktionsbetrieb erprobt werden können. Und sollte es ein inkompatibles Nachfolgesystem geben, was nicht a priori ausgeschlossen werden kann, dann müssen beide Systeme auch für eine befristete Zeit parallel betreibbar sein.

Zusammenfassend: Die Verfügbarkeit ausreichender Reserven in der Kabelinfrastruktur schafft Freiheitsgrade und die Möglichkeit, schnell und angepaßt auf außergewöhnliche, nicht langfristig vorhersehbare Kommunikationsanforderungen reagieren zu können, was in einer Forschungsumgebung außerordentlich wichtig ist.

4.1 Ethernet

Seit der Betriebseinstellung von HYPERNET/HYPERchannel basiert KFAnet sowohl im Backbone-Bereich wie auch im Bereich der nachgeordneten Institutsnetze vollständig auf Ethernet.

4.1.1 Allgemeines

Mit Ethernet wurde erstmals ein lokales Netz (LAN) als ein eigenständiges, von den geplanten Kommunikationsdiensten unabhängiges Element der lokalen Kommunikation eingeführt. Ethernet wurde im Palo Alto Research Center (PARC) der Fa. Xerox als Teil eines Systems für die Büroautomatisierung entwickelt und erstmals 1976 durch eine Veröffentlichung von Metcalfe/Boggs [17] der Öffentlichkeit vorgestellt. Die Weiterentwicklung und das Einbringen in die Standardisierung bei IEEE wurde von der DIX (DEC - Intel - Xerox)- Firmengruppe betrieben. Der Durchbruch auf breiter Front bezüglich der praktischen Anwendung erfolgte aber erst nach 1985. Heute ist Ethernet das am weitesten verbreitete LAN und hat auch die mit Abstand größte Firmenbasis.
Konzeptionell ist Ethernet eine Weiterentwicklung des ALOHA-Konzepts, woran auch noch die Bezeichnung *Ether* für das Übertragungsmedium erinnert.
Der Zugriff zu dem allen Stationen gemeinsamen Übertragungsmedium erfolgt nach dem CSMA/CD-Prinzip, einem probabilistischen Medienzugriffsverfahren. Beim CSMA/-CD-Verfahren gibt es einen kritischen Zusammenhang zwischen den Netzparametern Übertragungsgeschwindigkeit, Netzausdehnung (Bus-Länge) und minimale Blocklänge, der eine Weiterentwicklung entsprechend dem technischen Fortschritt (etwa zu höheren Geschwindigkeiten oder größeren Entfernungen hin) verhindert.
Überdies ist das Verfahren instabil, d.h. bei hoher Last oder Überlast kann der Durchsatz an Nutzdaten sinken und schließlich sogar gegen Null gehen. Ob und wann instabiles Verhalten auftritt, ist von der Laststruktur abhängig, ab etwa 40-50% Belastung können aber Instabilitäten nicht mehr ausgeschlossen werden.
Die bislang LAN-typischen Netzauslastungen von wenigen Prozenten hatten von den als kritisch anzusehenden Werten einen genügend großen Sicherheitsabstand, und bei niedrigen Lasten ist das CSMA/CD-Verfahren wegen des geringen verfahrensbedingten Overhead und der kurzen Reaktionszeiten sogar von Vorteil.
Mit allgemein steigendem Kommunikationsaufkommen und dem zunehmenden Einsatz von leistungsfähigen Workstations, wo bereits einzelne Teilnehmer eine hohe Last erzeugen können, werden die Grenzen aber spürbar. Dem wird derzeit durch eine verstärkte Strukturierung der Netze und damit der Lokalisierung der Verkehrsströme entgegengewirkt, d.h. es werden viele kleine miteinander verbundene Ethernet-Segmente eingerichtet.
Ethernet ist derzeit das populärste LAN, das die weiteste Verbreitung und die größte Herstellerbasis hat und niedrige Anschlußkosten bietet, und es ist außerdem für die wichtigsten Netzarchitekturen (DECnet, Internet) im lokalen Bereich die klassische Basis. Das Konzept ist aber – da nicht entwicklungsfähig – nicht zukunftsweisend; als *Low-cost*-LAN für normale Belastungen wird Ethernet aber noch lange eingesetzt werden.

4.1.2 Der KFAnet-Ethernet-Backbone

Wegen der Längenbeschränkung auf 500 m pro Segment und der Restriktion, daß Kommunikationsverbindungen über maximal drei über Repeater verbundene Koaxialkabelsegmente aufgebaut werden können, ist ein Ethernet für ein flächendeckendes Netz in einer Einrichtung von der Ausdehnung der KFA nicht ausreichend.
Erst die Verfügbarkeit von Brücken, die bezüglich des Medienzugriffs unabhängig arbeitende Ethernet-Teile verbinden, erlaubte eine flächendeckende und vernünftig strukturierte Versorgung der KFA mit Ethernet.
Deshalb erfolgte seit 1988 ein massiver Ausbau von Ethernet in der KFA, und zwar sowohl im Backbone-Bereich wie auch in den einzelnen Instituten.

Der KFAnet-Ethernet-Backbone besteht konzeptionell aus einem Ethernet-Bus, der aus Gründen der Längenbeschränkungen für Ethernets aus fünf durch Brücken verbundenen (und weitere zwanzig Repeater enthaltenden) Ethernet-Segmenten besteht [20]. Die Topologie ist ein nicht geschlossener Ring durch die KFA, der dadurch an Betriebssicherheit gewinnt, daß an den offenen Ringenden eine Brücke installiert ist, durch die die Ringenden verbunden werden können, wenn ein Defekt auftritt (Ausfall eines Repeaters oder einer Brücke, Leitungsunterbrechung usw.), so daß wieder ein (an der Unterbrechungsstelle offener Ring entsteht (Abb. 4).

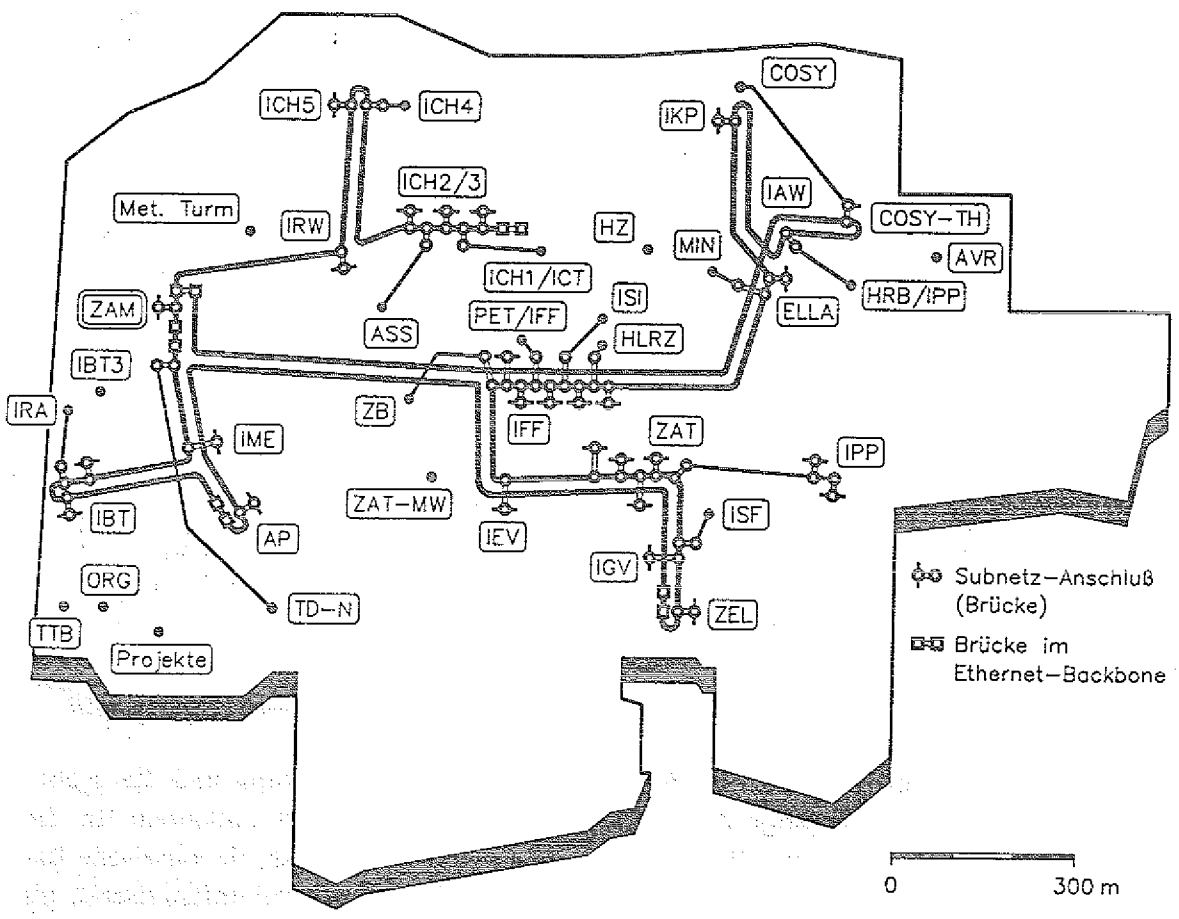


Abb. 4. Der KFAnet-Ethernet-Backbone

In jedem der fünf Segmente ist zusätzlich ein *LAN Traffic Monitor* (das ist eine Brücke mit Managementsoftware) zur Überwachung der Netzfunktion installiert.
An den Backbone sind etwa 40 Netze von Organisationseinheiten der KFA jeweils über eine Ethernet-Ethernet-Brücke als Subnetze angekoppelt.
Im Gesamtnetz sind derzeit

- ca. 60 Rechner,
- ca. 250 Workstations,
- ca. 350 PCs,
- ca. 150 Terminal-/Druckserver sowie
- ca. 25 Spezialgeräte (Analysegeräte usw.)

angeschlossen.
Da die meisten der in Frage kommenden Organisationseinheiten bereits an den Backbone angeschlossen sind, ist mit einem massiven weiteren Ausbau nicht mehr zu rechnen. Dennoch wird es – dem allgemeinen Trend zur Vernetzung folgend – wohl solange einen weiteren Ausbau geben, bis nahezu alle KFA-Einrichtungen angeschlossen sein werden. Der generelle Trend zu vielen kleineren LANs (bzgl. der Zahl der angeschlossenen Einheiten) hält ebenfalls unvermindert an und wird in den Instituten zur Einrichtung weiterer Ethernets führen, mit der Konsequenz, daß die Institutsnetze (Subnetze aus Sicht des Backbone) zunehmend selbst komplexe, über Brücken oder evtl. Router strukturierte Netzgebilde werden.

Um 1987/88 ohne Zeitverlust und größere Investitionen in die Kabelinfrastruktur mit dem Aufbau des Ethernet-Backbone beginnen zu können, benutzt dieser in weiten Teilen das seinerzeit in der KFA bereits vorhandene 75 Ω Koaxialkabelnetz. Diese Kabel entsprechen nicht den Ethernet-Spezifikationen und ihre Verwendung machte die Modifikation von Komponenten *(Transceiver)* erforderlich. Das außerordentliche Wachstum sowohl hinsichtlich der Ausdehnung wie auch der Anzahl der angeschlossenen Komponenten (aufgrund der großen Zahl angeschlossener Subnetze) zeigt nun die Grenzen dieser Vorgehensweise, die sich in folgenden Problemen manifestieren:

- Alterung der (modifizierten) Komponenten, für die kein Ersatz erhältlich ist,
- zu viele Verstärkerbausteine im Netz erforderlich,
- zu große Leitungslängen, so daß ein Teil der Komponenten im Grenzbereich und entsprechend störanfällig arbeitet.

In der Folge ist der für die Sicherstellung eines stabilen Netzbetriebs erforderliche Aufwand permanent angestiegen. Um auch bei weiterem Wachstum des Ethernet-Backbone einen zuverlässigen Betrieb langfristig sicherzustellen, ist eine Ertüchtigung des Ethernet-Backbone erforderlich. ZAM und ZEL haben sich auf ein Konzept hierfür unter Nutzung moderner Glasfasertechnologien verständigt.

4.2 FDDI

FDDI *(Fiber Distributed Data Interface)* ist ein nach ISO (ISO 9314) standardisiertes Hochleistungs-LAN auf Glasfaser-Basis, dessen Einsatz in der KFA – wie in vielen anderen vergleichbaren Einrichtungen auch – zunächst vorwiegend im Backbone-Bereich vorgesehen ist.

4.2.1 Allgemeines

FDDI arbeitet nach dem Token-Verfahren, wobei das vom Token-Ring (IEEE 802.5) her bekannte Medienzugriffsverfahren zur Anpassung an die höhere Übertragungsgeschwindigkeit von 100 Mbps leicht modifiziert ist.
Als Medium ist Gradientenfaser der Abmessung 62,5/125 μm vorgesehen (Referenzfaser); es können aber auch Fasern anderer Abmessungen (insbesondere der in Europa verbreiteten Abmessung 50/125 μm) verwendet werden, u.U. aber mit Abstrichen in den überbrückbaren Entfernungen.
Definiert wird ein gegenläufiger Doppelring von maximal 100 km Ausdehnung. Der zweite Ring ist aus Sicherheitsgründen vorhanden. Bei einer Unterbrechung (Ausfall einer Station, Leitungsunterbrechung) führen die der Unterbrechungsstelle benachbarten Stationen eine automatische Rekonfiguration unter Einbeziehung des Ersatzrings durch. Die maximale Ringausdehnung nach Leitungslängen beträgt also 200 km. Theoretisch (d.h. der Standard läßt dies zu) kann der Ersatzring auch unabhängig vom Primärring genutzt werden; dies führt beim Eintreten des Backup-Falles u.U. aber zu Problemen.
Es können maximal 500 Stationen an den Doppelring angeschlossen werden, und die maximale Entfernung zweier benachbarter Stationen beträgt 2 km. Eine Fortschreibung des Standards für Monomodefasern ist im Gange, bei deren Einsatz die maximale Entfernung benachbarter Stationen auf mindestens 15-20 km steigt.

Für den Anschluß an einen FDDI-Ring sind drei Typen von Stationen vorgesehen:

- *Dual Attached Stations* (DAS; auch *Class 'A'* oder Typ 'A'-Stationen), die an beide Glasfaser-Ringe angeschlossen sind und bei Bedarf auch die Rekonfiguration über den Ersatzring vornehmen können *(Wrap Mode)*. Sie sind überdies mit einem *Bypass Switch* ausgestattet; das ist ein optischer Überbrückungsschalter, durch den – entweder explizit gesteuert oder auch automatisch (etwa bei Stromausfall) – die Glasfaserverbindung an der betreffenden Station vorbeigeführt wird *(Thru Mode)*. Dies kann natürlich nur funktionieren, wenn für die Verbindung der dann benachbarten Stationen (zwischen denen sich eine oder mehrere Stationen im *Thru Mode* befinden können) die zulässige Maximalentfernung nicht überschritten wird; andernfalls müssen diese Stationen in den *Wrap Mode* schalten.

- *Single Attached Stations* (SAS; auch *Class 'B'* oder Typ 'B'-Stationen), die nur an einen Ring angeschlossen werden können.

- *Dual Attached Concentrators* (DAC). Konzentratoren werden wie DAS-Stationen an beide Glasfaser-Ringe angeschlossen. Sie stellen eine Anzahl sogenannter M-*Ports* zur Verfügung, über die daran angeschlossene SAS-Stationen in den Ring eingebunden werden. Konzentratoren können kaskadiert werden, so daß eine Ring-

Baum-Struktur entsteht (vgl. Abb. 5). Zum Anschluß an übergeordnete Konzentratoren gibt es auch *Single Attachment Concentrators* (SACs).

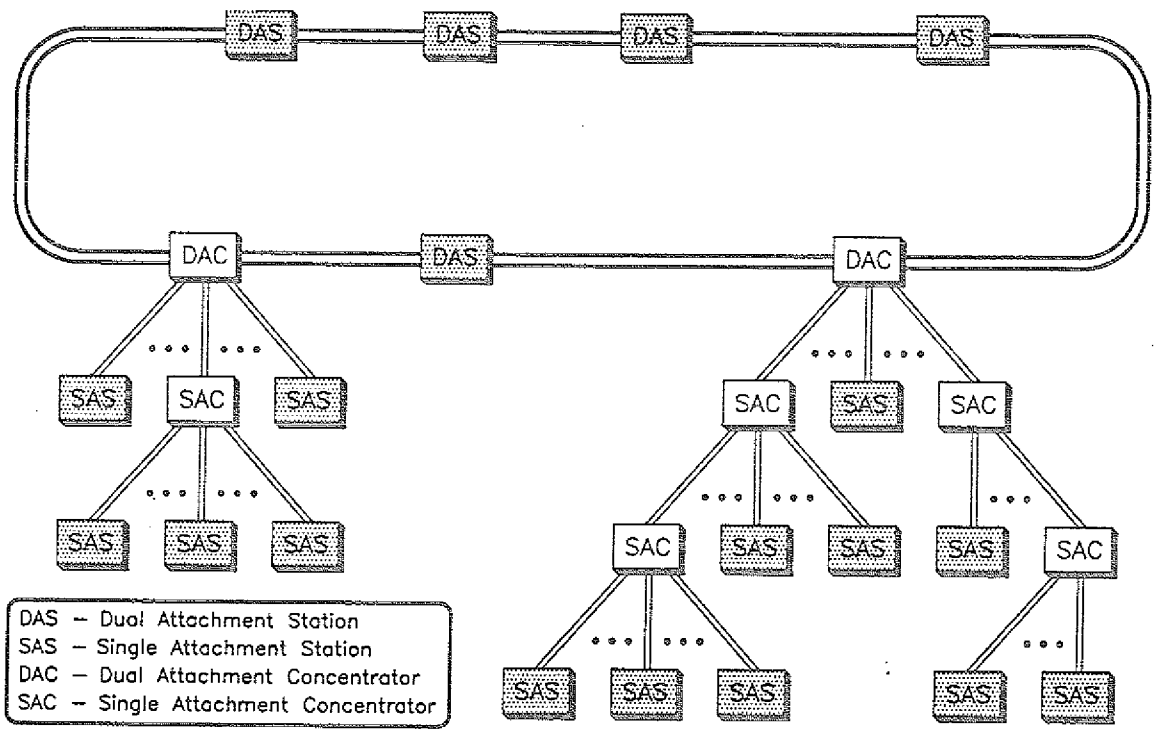


Abb. 5. Ring-Baum-Struktur beim Einsatz von Konzentratoren an einem FDDI-Ring

Dual Attached-Stationen sind aktive Element im Ring und kritisch für die Funktion eines FDDI-Rings. Der direkte Anschluß von (beliebig manipulierbaren, insbesondere jederzeit ausschaltbaren) benutzereigenen DAS-Stationen an einen FDDI-Ring birgt deshalb Risiken. Diese Risiken werden zwar durch durch die *Wrap*- und *Thru*-Funktion gemildert, es ist aber nicht akzeptabel, wenn die eingebauten Sicherheitsreserven durch derartiges Fehlverhalten von Benutzern aufgebraucht werden. Um dieser Gefahr zu entgehen, wird oftmals die Strategie verfolgt (auch DEC tut dies), den Anschluß von Benutzerstationen nur über (dem Zugriff der Benutzer entzogene) Konzentratoren (DACs) zuzulassen.

Die Standardisierung von FDDI bei ANSI und ISO ist weitgehend abgeschlossen, und FDDI ist als LAN-Standard der Zukunft weltweit akzeptiert, was durch eine Vielzahl von Herstellern dokumentiert wird, die FDDI-Produkte bereits im Angebot oder zumindest doch angekündigt haben.
FDDI befindet sich noch in der Hochpreisphase der Systemeinführung, was zunächst einen begrenzten Einsatz im Backbone-Bereich nahelegt. Nach den erwarteten und sich bereits abzeichnenden Kostensenkungen wird FDDI zunehmend auch im Bereich der Subnetze eingesetzt werden können und bei weiter steigender Leistungsfähigkeit von Workstations mit hohem Kommunikationsbedarf auch eingesetzt werden müssen.

4.2.2 Der KFAnet-FDDI-Backbone

Die erwartete Preisentwicklung von FDDI-Komponenten legt die beim Ausbau der Datenkommunikation stets praktizierte bedarfsorientierte Vorgehensweise auch für den Aufbau des FDDI-Backbone nahe.
Die grundlegenden Voraussetzungen für den Ausbau des FDDI-Backbone in der KFA sind bereits erfüllt. Neben der Verfügbarkeit der benötigten Glasfaser-Infrastruktur ist das die Gleichstellung der an den FDDI-Backbone angeschlossenen Benutzer mit den übrigen KFAnet-Benutzern:

- Sie müssen in gleicher Weise Zugriff auf das zentrale Dienstangebot des ZAM haben.
- Sie müssen Zugang zu den externen Kommunikationsdiensten haben.
- Es muß bezüglich der in KFAnet angebotenen Dienste volle Konnektivität zwischen Nutzern (Subnetzen) am KFAnet-Ethernet-Backbone und am KFAnet-FDDI-Backbone bestehen.

Diese Voraussetzungen sind durch die Installation eines CISCO-Routers vom Typ AGS+ mit Zugriff zum ZAM-internen UltraNet, zum FDDI-Backbone, zum Ethernet-Backbone sowie zum X.25 WIN bereits seit Ende 1990 erfüllt (Abb. 6).

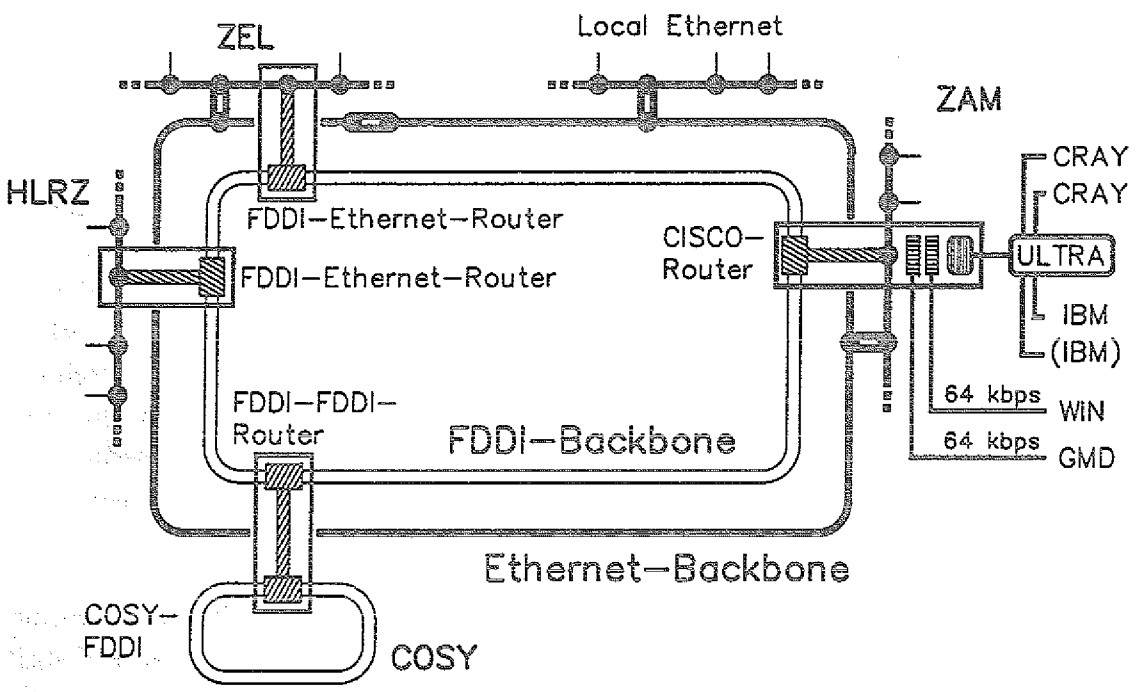


Abb. 6. KFAnet-Struktur mit FDDI-Backbone

Da dieser Router eine kritische zentrale Funktion hat, wurde bereits ein zweiter weitgehend gleich ausgestatteter Router für Backup-Zwecke beschafft.
Aufgrund der konkreten Anforderung wird der FDDI-Backbone zunächst zwischen dem ZAM und COSY etabliert werden. Da COSY innerhalb des Beschleunigerbereichs einen eigenen FDDI-Ring aufbauen will, handelt es sich hier um einen FDDI-FDDI-Übergang (vgl. Abb. 7).

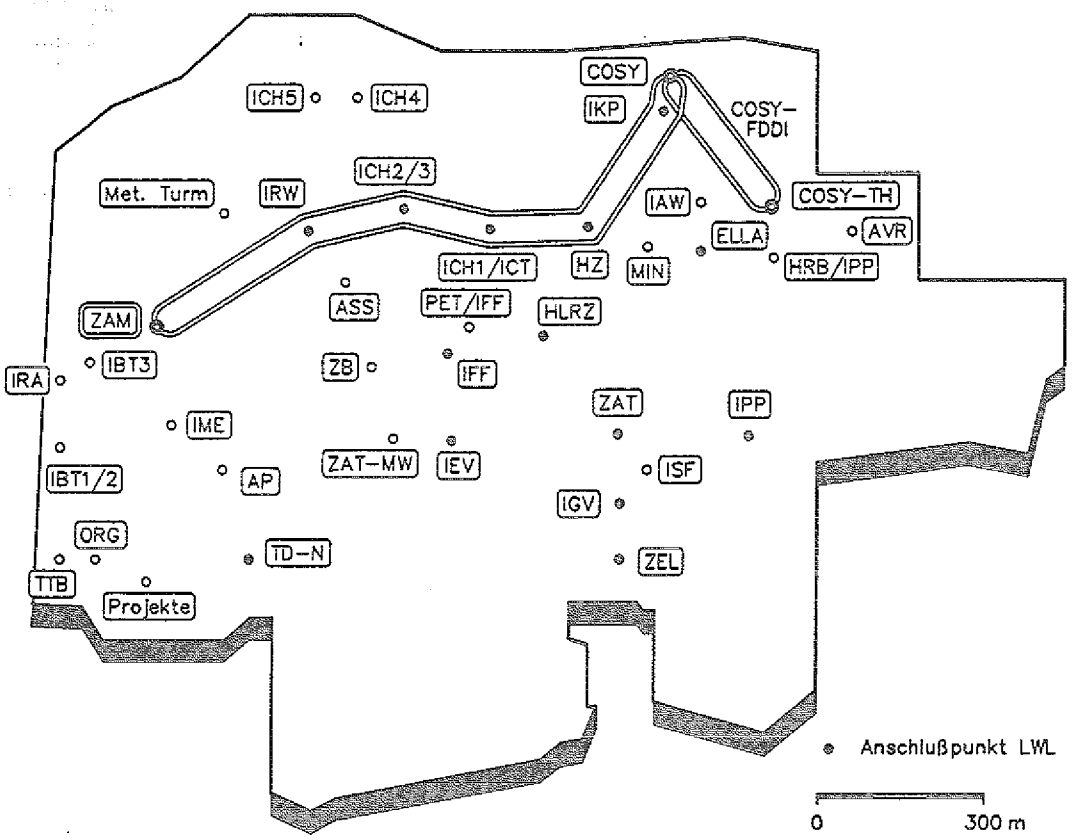


Abb. 7. KFAnet-FDDI-Backbone: 1. Ausbaustufe

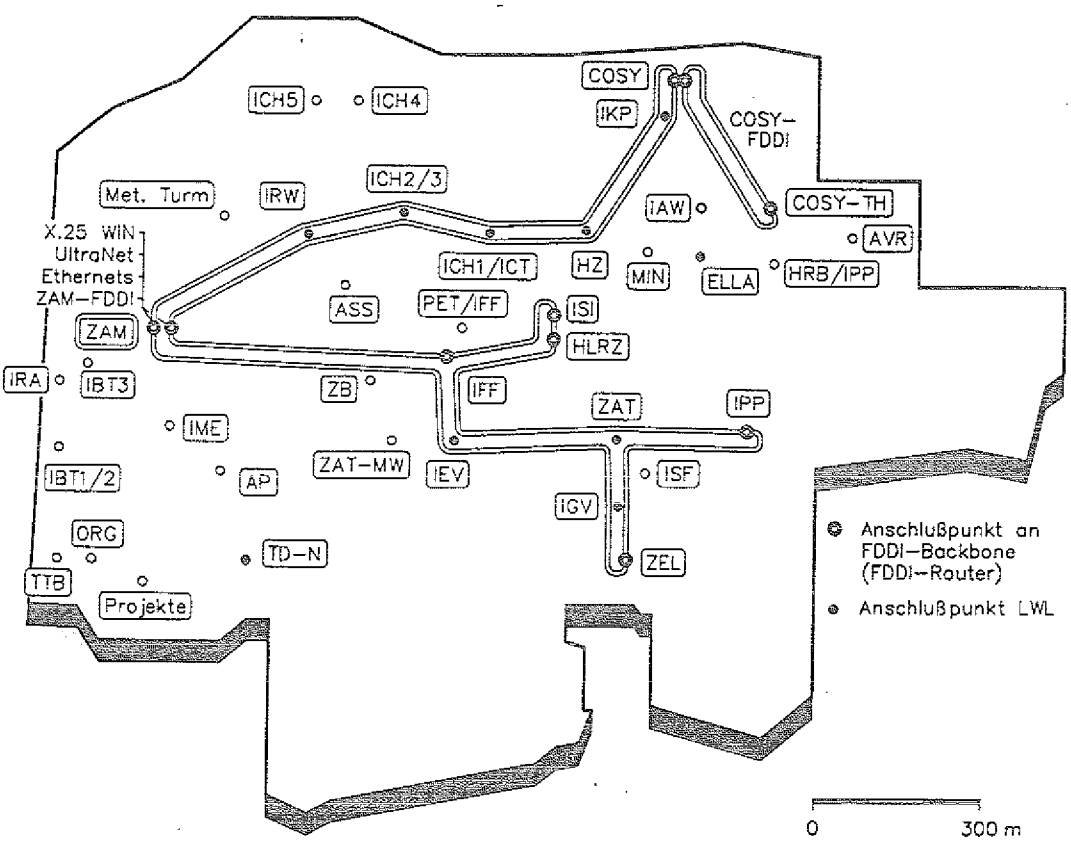


Abb. 8. KFAnet-FDDI-Backbone: Denkbarer weiterer Ausbau

1992 und in den Folgejahren können bedarfsorientiert weitere Subnetze an den FDDI-Backbone angeschlossen werden. Zunächst werden die anzuschließenden Subnetze überwiegend Ethernets sein. In dem Maße, wie mit sinkenden Preisen für FDDI-Komponenten dann auch in den Instituten FDDI-Ringe entstehen werden, sind diese dann natürliche Kandidaten für den Anschluß an den FDDI-Backbone.
Ein solcher Anschluß setzt voraus, daß der FDDI-Backbone-Ring bis in das jeweilige Institut verlängert und dort ein FDDI-Ethernet- bzw. ein FDDI-FDDI-Router installiert wird.
Wenn man die heutigen Nutzungsschwerpunkte zugrunde legt, könnte der FDDI-Backbone in einigen Jahren aussehen wie in Abb. 8 dargestellt.

5.0 Dienste (Protokolle)

Die Netzinfrastruktur von KFAnet – wie im vorigen Kapitel beschrieben – steht den Teilnehmern nicht zur beliebigen Verwendung zur Verfügung, sondern es ist das Ziel von KFAnet, dezidierte Kommunikationsdienste anzubieten. Die derzeit in KFAnet unterstützten Plattformen sind Internet (TCP/IP) und DECnet (Phase IV). Hinzukommen werden in absehbarer Zeit nach OSI standardisierte Kommunikationsdienste, insbesondere MOTIS (*Message Oriented Text Interchange System*; entspricht den CCITT-Empfehlungen X.400 ff.) und File Transfer (FTAM).

5.1 Internet (TCP/IP)

5.1.1 Allgemeines

Basierend auf den Erfahrungen im ursprünglichen ARPANET, das das erste paketvermittelnde Netz war, begann Mitte der siebziger Jahre die Entwicklung der heutigen Internet-Protokolle. Diese wurden ab 1980 in den konkreten Netzbetrieb eingeführt, und seit 1983 ist ihre Verwendung im DoD-INTERNET obligatorisch. Gleichzeitig wurde das DoD-INTERNET (auch DDN= *Defense Data Network*) aufgespalten in einen nichtmilitärischen Teil (ARPANET) und einen militärischen Teil (MILNET). 1986 fiel die Entscheidung, im NSFnet (*National Science Foundation Network*) – ursprünglich als Verbindungsnetz der amerikanischen Supercomputer-Zentren gegründet – ebenfalls die Internet-Protokolle zu verwenden. Dieses Netz mit seinen nachgeordneten *Mid-level Networks* (in der Regel regionale Netze) und den diesen nachgeordneten *Access Networks* (typischerweise Campusnetze einzelner Universitäten) ist der wichtigste Teil des heutigen INTERNET.
Parallel dazu wurden nach 1980 – ebenfalls mit finanzieller Unterstützung des amerikanischen Verteidigungsministeriums – die Internet-Protokolle in das Betriebssystem UNIX integriert und insbesondere mit den Berkeley-Versionen dieses Betriebssystems (BSD 4.x, BSD= *Berkeley System Distribution*) in großem Umfang kostenlos an Universitäten und Forschungseinrichtungen verteilt. Gleichzeitig wurden, basierend auf IP und TCP, weitere Kommunikationsdienste entwickelt und verbreitet, so daß eine über die eigentlichen Internet-Protokolle hinausgehende Kommunikationskultur entstanden ist. Zu nennen sind hier vor allem die *Berkeley Services*, die in UNIX-typischer Weise von lokalen UNIX-Systemen her bekannte Dienste auf entfernten UNIX-Systemen verfügbar machen, und NFS (*Network File System*), eine inzwischen von sehr vielen Herstellern unterstützte Entwicklung der Fa. SUN Microsystems, die es ermöglicht, einen File auf einem entfernten System wie einen lokalen File zu benutzen, d.h. satzweise darauf zuzugreifen (vgl. Abb. 9).
Etwa seit 1987 hat ein massives Wachstum des DoD-INTERNET eingesetzt, das heute über 5000 Teilnetze mit mehr als 300.000 Rechnern umfaßt und über drei Millionen potentielle Nutzer hat. Dieses außerordentliche, von den Entwicklern der Protokolle nicht vorhergesehene Wachstum (in der von Großrechnern geprägten, LAN-freien Welt der siebziger Jahre waren einige dutzend Netze und einige hundert Hosts eine realistische Vorstellung) hat Probleme bereitet und eine Weiterentwickung der Konzepte hin zu einer stärkeren (hierarchischen) Strukturierung erzwungen.

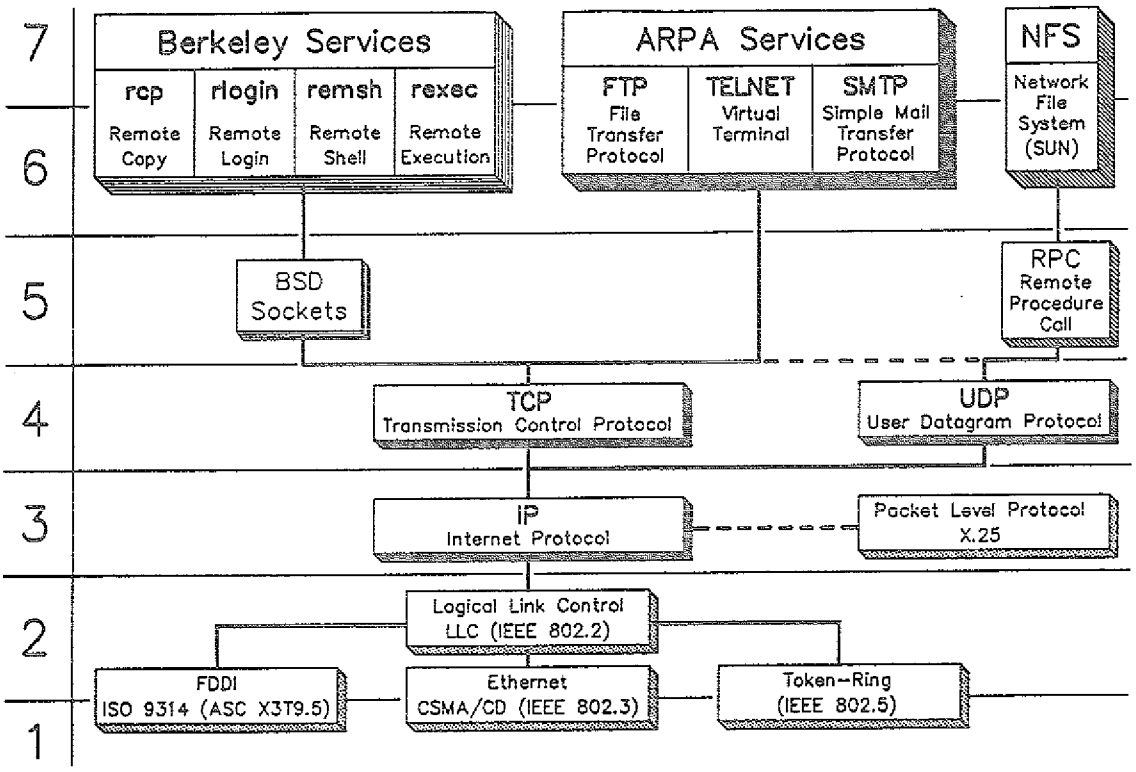


Abb. 9. Kommunikationsprotokolle und -dienste im Internet-Umfeld

Die Internet-Protokollfamilie ist kein Standard einer einschlägigen Institution, sondern ein firmenunabhängiger de-facto-Standard des amerikanischen Verteidigungsministeriums. Abgesehen von diesem formalen Manko, existiert mit diesen Protokollen erstmals ein wirklicher Standard in dem Sinne, daß über diese Protokolle praktisch alle auf dem Markt erhältlichen Computer vom kleinen PC bis zum Supercomputer miteinander kommunizieren können.

5.1.1.1 Einführung

Die TCP/IP-Protokollfamilie (auch ARPA- oder Internet-Protokolle) umfaßt als Protokoll für die Schicht 3 das *Internet Protocol* (IP), darauf aufsetzend für die Schicht 4 das *Transport Control Protocol* (TCP) sowie für die Schichten 5–7 die Kommunikationsdienste

- TELNET (interaktiver Terminaldienst),
- FTP *(File Transfer Protocol)* und
- SMTP *(Simple Mail Transfer Protocol)*.

Zusätzlich gibt es mit dem UDP *(User Datagram Protocol)* noch ein sehr einfaches Ebene-4-Protokoll, das im wesentlichen die Funktionen der IP-Schicht den Anwendungen zugänglich macht, und die darauf basierenden Dienste *Trivial File Transfer Protocol* (TFTP) und den *Domain Name Service* (DNS). Auf Anwendungsebene ist auch SNMP *(Simple Network Management Protocol)*, das Internet-Management-Protokoll angesiedelt.

Unter einem Internet wird die Realisierung eines Netzverbunds auf der Basis der TCP/IP-Protokollfamilie verstanden. Wenn vom DoD-INTERNET oder vom internationalen INTERNET oder auch nur kurz vom INTERNET die Rede ist, so ist damit ein ganz bestimmter weltweiter Netzverbund auf der Basis dieser Protokolle angesprochen, der im Auftrag des amerikanischen Verteidigungsministeriums organisiert worden ist und deshalb die Bezeichnung *Defense Data Network* (DDN) trägt und der zentral verwaltet wird.

Ein Internet ist ein Netz von miteinander verbundenen Teilnetzen, das den Teilnehmern den Eindruck eines einzigen großen Netzes vermittelt. Die Teilnetze sind durch Gateways (Router) miteinander verbunden. Da Gateways Teilnehmerstation in allen Teilnetzen sind, die sie verbinden, können sie in jedem der Teilnetze direkt adressiert werden.
IP als Ebene-3-Protokoll ist die unterste der im Rahmen der TCP/IP-Protokollfamilie festgelegten Schichten; über die darunterliegenden Netzebenen wird keine Aussage getroffen, und sie können sehr unterschiedlich sein.
Teilnetze können sein:

- LANs
  Standard-LANs wie Ethernet, CSMA/CD gemäß IEEE 802.3, Token-Ring, FDDI, aber auch firmenspezifische LANs wie beispielsweise HYPERchannel; das im TCP/IP-Umfeld originäre und mit Abstand am weitesten verbreitete LAN ist Ethernet.

- WANs,
  insbesondere öffentliche X.25-Netze (in Deutschland das Datex-P-Netz oder das WIN, ein X.25-Sondernetz der Deutschen Bundespost Telekom für die deutsche Wissenschaft).

- Einzelne Punkt-zu-Punkt-Verbindungen
  (im Nah- wie im Fernbereich).

Es ist offensichtlich, daß die Gateways neben dem *Routing* weitere nichttriviale Funktionen haben, wenn sie zwischen bezüglich der Übertragungsleistung sowie sonstiger Netzparameter (etwa maximale Größe eines Datenpakets) unterschiedlichen Teilnetzen vermitteln.

5.1.1.2 Namen und Adressen im Internet

In einem Internet hat man drei unabhängige Namens-/Adreßebenen (vgl. Abb. 10).

Domain-Namen
Da Bezeichnungen (Adressen), die in technischen Systemen zur eindeutigen Identifikation von adressierbaren Geräten (z.B. Rechnern) dienen, in der Regel aus strukturierten Zahlenkombinationen von beträchtlicher Länge bestehen, sind sie ungeeignet für die Benutzung durch Menschen. In modernen Datennetzen (wie auch Internet) ist deshalb die Verwendung von Namen erlaubt, die durch Hinzufügen sinnhafter qualifizierender Merkmale eindeutig gemacht werden. Die Umsetzung von Namen auf Adressen erfolgt

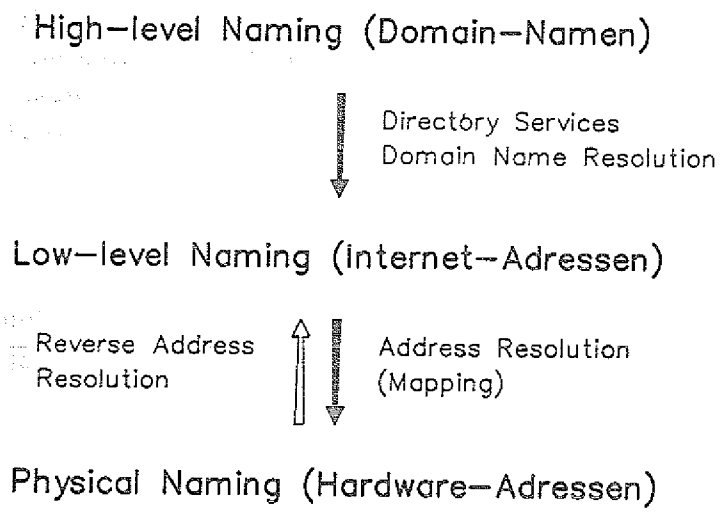


Abb. 10. Namen und Adressen im Internet

automatisch durch einen im Netzwerk verfügbaren Dienst, der die Bezeichnung *Directory Services* trägt.
Die qualifizierenden Elemente eines Internet-Namens bilden einen hierarchischen Namensraum. Der Namensraum einer einzelnen Hierarchiestufe wird als *Domain* bezeichnet.
Im *Domain Name System* (DNS) des Internet besteht ein Name aus einer Folge von Elementen (*labels*), die durch Punkte getrennt sind.

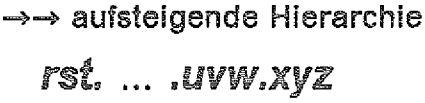


Abb. 11. Struktur von Internet-Namen

Im internationalen INTERNET bezeichnet die oberste Hierarchiestufe inneramerikanisch den Verwendungszweck des Netzes (z.B. *.edu* für *educational institutions*), außeramerikanisch besteht sie aus einem zweibuchstabigen Ländercode, z.B. *.de* für Deutschland. In den einzelnen Ländern muß es nun eine Institution geben (in Deutschland z.B. der DFN-Verein), die für diese *Domain* das Recht der Namensvergabe besitzt, d.h. die Elemente der nachgeordneten *Subdomain* eindeutig benennt. Diese Stufe kennzeichnet Organisationen (Firmen, Universitäten, Forschungseinrichtungen usw.) in dem jeweiligen Land.
In einer solchen Einrichtung existiert dann i.a. wieder eine für die Namensvergabe auf dieser Ebene (typischerweise Kurzbezeichnungen für Abteilungen oder Institute) autorisierte Stelle. Darunter können dann Namen für einzelne Rechner vergeben werden. Die Namen sind netzweit eindeutig, wenn jede zur Namensgebung autorisierte Stelle (*naming authority*) gewährleistet, daß die Namen innerhalb einer Hierarchiestufe eindeutig sind. Eine *Naming Authority* hat darüberhinaus die Verpflichtung, einen *Name Server* bereitzustellen, der im Zusammenspiel mit anderen *Name Servern* in der Lage ist, den Namen Internet-Adressen zuzuordnen.

Internet-Adressen

Die entscheidenden Größen im Internet sind die Internet-Adressen (auch IP-Adressen). Sie identifizieren Teilnetze und Rechner im Gesamtnetz und müssen deshalb netzweit eindeutig sein. Das *Routing* im Internet basiert auf diesen Adressen.
Für das internationale INTERNET werden die Adressen (wie auch die Namen) von einer zentralen Stelle vergeben, wodurch die weltweite Eindeutigkeit gewährleistet werden kann. Um nicht weltweit einzelne Adressen vergeben zu müssen, bekommen nationale Einrichtungen (wie etwa das DFN) Adreßkontingente zur eigenständigen Verteilung zugewiesen.

Die Internet-Adressen haben eine Länge von 32 Bits; die allgemein verbreitete Notation ist:

ddd.ddd.ddd.ddd mit **ddd** ganze dezimale Zahlen $\in [0,255]$.

Die Adressen sind unterteilt in eine ***netid***, die das Teilnetz identifiziert, und eine ***hostid***, die eine Station in einem Teilnetz kennzeichnet.
Um den vorhandenen 32-Bit-Adreßvorrat gut ausnutzen zu können, ist die Aufteilung eines Adreßwortes in ***netid*** und ***hostid*** variabel. Es entstehen so verschiedene Netzklassen:

Class	Initial Bits	No. of Bits netid	No. of Bits hostid	Value of High Order Byte	32-Bit Net Mask
A	0xx	7	24	0–127	FF 00 00 00
B	10x	14	16	128–191	FF FF 00 00
C	110	21	8	192–223	FF FF FF 00
D	111	21	8	224–255	

Die in der Tabelle angegebene Netzmaske (*net mask*) ist eine 32-Bit-Maske, die B'0'-Werte in allen der Host-Identifikation dienenden Bitpositionen enthält und in den der Netzidentifikation zugeordneten Bitpositionen B'1'-Werte; sie ist bei der nachfolgend beschriebenen Subnetz-Adressierung von Bedeutung.
Die Aufteilung der Internet-Adresse in eine ***netid*** und eine ***hostid*** hat vor allem den Vorteil, daß außerhalb eines Teilnetzes nur die ***netid*** (hinter der sich eine große Zahl von Hosts verbergen kann) für *Routing*-Zwecke herangezogen werden muß, wodurch die *Routing*-Tabellen klein gehalten werden können und der *Routing*-Vorgang effizient wird.

Wie bereits erwähnt, erfolgt die Vergabe der Netzadressen für das gesamte INTERNET zentral; die Vergabe von Host-Adressen ist dagegen eine lokale Aufgabe einer (zentralen) Stelle in einer Organisation, der eine Netzadresse zugewiesen wurde. Bei größeren Netzen (insbesondere Klasse-B-Netzen) ist ein flacher Adreßraum von vielen tausend Hosts nur sehr schwer verwaltbar und entspricht auch nicht den netztechnischen Gegebenheiten, da große Einrichtungen heute i.a. sehr komplexe, strukturierte lokale Netze besitzen. Es ist deshalb wünschenswert, daß sich hinter einer Internet-Netzadresse einer Einrichtung mehrere physikalische Netze verbergen können und daß sich dieses auch in der Adresse widerspiegelt.

Subnetting ist die allgemeinste (und standardisierte) Methode, um hinter einer Internet-Netzadresse mehrere physikalische Netze etablieren zu können. Es ist dies eine Erweiterung des ursprünglichen Adressierungsschemas, die aufgrund des nicht vorhergesehenen außerordentlichen Größenwachstums des INTERNET notwendig wurde. Durch *Subnetting* kann das Entstehen einer Vielzahl kleiner Internet-Teilnetze innerhalb einer Institution verhindert werden, wodurch auch die durch die Adreßaufteilung in ***netid*** und ***hostid*** angestrebte *Routing*-Effizienz in Frage gestellt würde.
Beim *Subnetting* (vgl. Abb. 12) wird der lokale Teil der Internet-Adresse (bisher als ***hostid*** bezeichnet) nochmals unterteilt in Subnetz-Adresse und ***hostid*** (im Subnetz). Die Aufteilung ist von der lokalen Autorität frei wählbar, sie sollte jedoch für alle Subnetze gleich sein, und alle Stationen müssen daran teilnehmen. Bei Klasse-B-Netzen wird häufig die Byte-Grenze gewählt (ein Byte für die Subnetz-Adressierung und ein Byte für die Host-Adressierung), weil dies zu leicht lesbaren Adressen führt und effizient implementierbar ist. Bekanntgemacht wird die gewählte Aufteilung durch die Subnetzmaske (*subnet mask*), eine 32-Bit-Maske, bei der alle der Netzidentifikation dienenden Bitpositionen *(**netid** + **subnet-id**)* auf B'1' und die der Host-Identifikation dienenden Positionen auf B'0' gesetzt sind.

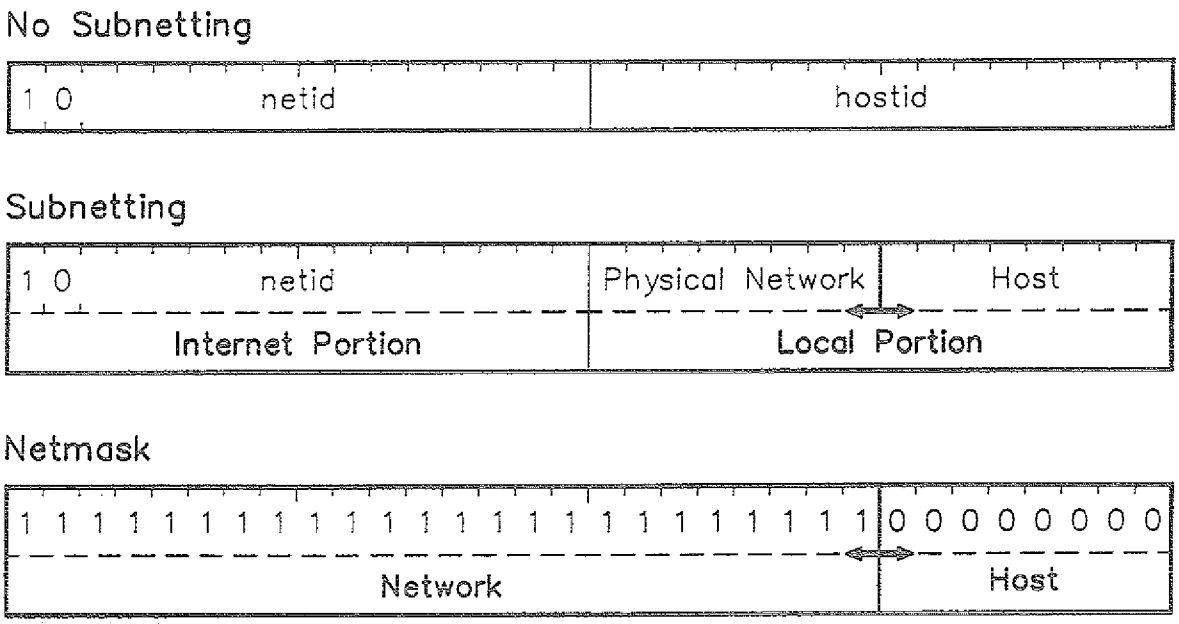


Abb. 12. Internet-Adreßstruktur ohne/mit Subnetting (Klasse-B-Netz)

Hardwareadressen

Wenn konkret in einem physikalischen Netz Daten von einer Station zu einer anderen transportiert werden sollen, so kann dies nur auf der Basis der Hardwareadressen geschehen; d.h. eine Station, die die Internet-Adresse des gewünschten Zielrechners kennt, muß – um tatsächlich Daten senden zu können – auch deren Hardwareadresse in dem physikalischen Netz kennen, durch das sie mit dieser Station verbunden ist.
Zwischen den 32-Bit-Internet-Adressen und den Hardwareadressen (etwa von IEEE vergebene 48-Bit-LAN-Adressen oder nach CCITT-Empfehlungen aufgebaute Adressen in öffentlichen Netzen) besteht keine funktionale Beziehung, so daß eine Zuordnung von physikalischen Adressen zu Internet-Adressen nur über Tabellen möglich ist.

Bei lokalen Netzen mit Broadcast-Fähigkeit auf Hardwareebene (z.B. im Ethernet) gibt es eine standardisierte Vorgehensweise, die *Address Resolution Protocol* (ARP) genannt wird, um eine solche Tabelle dynamisch aufzubauen.

5.1.1.3 IP (Internet Protocol)

Das Internet-Protokoll ist in der Lage, ein Internet-Datagramm (auch als Internet-Paket bezeichnet) von einem Quellknoten über mehrere Zwischennetze zu einem Zielknoten in einem anderen Teilnetz zu transportieren. Es handelt sich hierbei um einen verbindungslosen Dienst (*connectionless packet service*), einen *Unreliable Datagram Service*, bei dem auf dieser Ebene weder die Richtigkeit der Daten, noch die Einhaltung der Sequenz oder die Vollständigkeit und Eindeutigkeit einer Folge von Datagrammen garantiert wird.
Wenn den Applikationen ein zuverlässiger, verbindungsorientierter Dienst zur Verfügung gestellt werden soll, so muß dieser durch die darüberliegende Transportschicht erbracht werden; TCP leistet das. Dazu wird den Daten einer Applikation ein TCP-*Header* vorangestellt. Aus dieser Einheit, einem TCP-Segment, wird durch Voranstellen des Datagramm-*Header* (IP-*Header*) ein IP-Datagramm der Internet-Schicht. Zur Übertragung in einem physikalischen Netz wird aus dem IP-Datagramm durch Einschluß zwischen *Frame Header* und *Frame Trailer* ein in seiner Ausprägung vom physikalischen Netz abhängiger *Frame* (Rahmen) erzeugt (z.B. ein Ethernet-*Frame* in einem Ethernet).
Die maximale Datagrammlänge ist sinnvollerweise auf die maximale Rahmenlänge des für eine Übertragung benutzten physikalischen Netzes abgestimmt. Es kann aber nicht ausgeschlossen werden, daß ein Datagramm auf seinem Weg zum Zielknoten ein Teilnetz passieren muß, dessen maximale Rahmenlänge kleiner als die gewählte Datagrammlänge ist (maximale Rahmenlängen gängiger Netze sind: Datex-P: 128 Bytes, Ethernet: 1500 Bytes, FDDI: 4500 Bytes). In einem solchen Fall muß ein Datagramm zum Weitertransport in mehrere Fragmente aufgespalten werden (Fragmentierung).

Ein Internet-Datagramm (IP-Datagramm) besteht aus dem Datenteil und dem vorangestellten IP-*Header*, der die notwendigen Kontrollinformationen enthält, um ein Datagramm ordnungsgemäß von der sendenden Station zur Zielstation befördern zu können.

5.1.1.4 ICMP (Internet Message Protocol)

Das *Internet Control Message Protocol* ist ein Vehikel zum Austauschen von Fehler- und Kontrollnachrichten zwischen Gateways und Hosts auf IP-Ebene.
ICMP-Nachrichten benutzen Internet-Datagramme wie ein Ebene-4-Protokoll; ICMP ist aber ein integraler Bestandteil jeder IP-Implementation.
Die ICMP-Nachrichten dienen nicht dazu, den *Unreliable Packet Delivery Service* des IP zu einem *Reliable Service* aufzuwerten. Vielmehr sollen Hosts und Gateways, die über das Schicksal eines einmal abgeschickten Datagramms ansonsten keinerlei Information hätten, durch Bereitstellung von Informationen in den Stand gesetzt werden, sachgerechte Entscheidungen zu treffen und insbesondere sinnlosen Netzverkehr zu vermeiden (der z.B. dadurch entstehen könnte, daß Datagramme wiederholt werden, deren Zielknoten nicht erreichbar ist).

5.1.1.5 TCP (Transmission Control Protocol)

Aufbauend auf einem verbindungslosen, nicht sicheren Dienst der Schicht 3 (IP) stellt TCP als Schicht-4-Protokoll einen verbindungsorientierten, sicheren Transportdienst (vergleichbar ISO/TP4) zur Verfügung. Sicherheit wird durch positive Rückmeldungen (*acknowledgements*) und Wiederholung fehlerhafter Datenblöcke erreicht.
TCP-Verbindungen sind vollduplex. Wie bei allen verbindungsorientierten Diensten muß zunächst eine Verbindung (*virtual circuit*) aufgebaut werden, bevor Nutzdaten fließen können, und zur Beendigung des Kommunikationsvorgangs muß diese Verbindung wieder abgebaut werden.
Logisch transportiert TCP einen unstrukturierten Strom von Datenbytes, der zum Zweck der Übertragung in Segmente (das sind die Transporteinheiten im TCP) unterteilt wird. Die Segmentgröße sollte auf die Größe eines IP-Datagramms abgestimmt sein; i.a. wird ein Segment in einem IP-Datagramm übertragen.
Ausgangspunkt und Endpunkt eines Datenstroms werden durch *Ports* definiert, d.h. Anwendungen nehmen über einen Port die Dienste des Transportnetzes in Anspruch, und umgekehrt sind die Anwendungen gegenüber dem Transportnetz durch *Ports* identifiziert. Allgemein verfügbare Dienste sind über sogenannte *well-known Ports*, d.h. fest zugeordnete und allgemein bekannte *Port*-Nummern erreichbar (z.B. TELNET (*Port* 23), FTP (*Port* 21) und viele andere). Ansonsten werden *Port*-Nummern – und dies betrifft den größeren Teil des Nummernvorrats – beim Aufbau einer Verbindung zur Identifikation der Verbindung vergeben. Insgesamt ist jede Verbindung durch ihre Endpunkte (IP-Adresse + *Port*-Nummer) eindeutig bestimmt.
Eine Verbindung *(connection)* kann von einem Teilnehmer (Prozeß) durch ein *Active Open* zu einem Kommunikationspartner aufgebaut werden, der zuvor durch ein *Passive Open* angezeigt hat, daß er bereit ist, eine Verbindung zu akzeptieren. Im Falle allgemein verfügbarer Dienste wird ein den Dienst erbringender *Server* seine Dienste durch ein *Passive Open* auf die dem Dienst zugeordnete *well-known Port*-Nummer anbieten. Danach kann von einem Teilnehmer *(Client)* aus durch ein *Active Open* auf diese *Port*-Nummer eine Verbindung zu dem *Server* hergestellt und damit der Dienst in Anspruch genommen werden.
Um die TCP-Dienste erbringen zu können, ist den Daten eines Segments ein Segment-*Header* vorangestellt.

5.1.1.6 UDP (User Datagram Protocol)

UDP ist ein sehr einfaches Schicht-4-Protokoll, das den Benutzern (Anwendungen) im wesentlichen die Funktionalität von IP zur Verfügung stellt, d.h. einen nicht zuverlässigen verbindungslosen Transportdienst ohne Flußkontrolle. UDP erlaubt aber zwischen zwei Rechnern (identifiziert durch ihre IP-Adressen) mehrere unabhängige Kommunikationsbeziehungen (Multiplexen/Demultiplexen). Die Identifikation der auftraggebenden bzw. auftragnehmenden Prozesse geschieht wie bei TCP durch *Port*-Nummern, hier UDP- *Port*-Nummern. Wie bei TCP gibt es *well-known Port*-Nummern, die allgemein bekannten Anwendungen fest zugeordnet sind, und solche, die dynamisch zugeordnet werden.
Die Transporteinheiten bei UDP tragen die Bezeichnung *User Datagram* oder auch UDP-Datagramm. Sie bestehen aus einem UDP-*Header* und den UDP-Daten.

Entsprechend der geringen Funktionalität ist auch der Protokoll-Overhead für UDP niedrig. Dies ist der Grund, weshalb die meisten NFS-Implementationen auf UDP aufsetzen. Ansonsten wird UDP vor allem bei kurzen Transaktionen wie z.B. Anfragen beim *Name Server* eingesetzt.

5.1.2 Internet in der KFA

5.1.2.1 Namen und Adressen

Die KFA hat die INTERNET-Netzadresse **134.94.0.0** zugewiesen bekommen (Klasse-B-Netz) und nimmt mit dieser weltweit eindeutigen Adresse am internationalen INTERNET teil.
Der *Domain*-Name der KFA lautet: ***kfa-juelich.de***. Diese *Domain* wird vom ZAM verwaltet. Das ZAM hat – basierend auf den bekannten Institutskürzeln – eine weitere, nachgeordnete *Domain* eingerichtet, in der die einzelnen Rechner benannt werden, so daß ein vollständiger Name eines Rechners z.B. lautet:

zam001.zam.kfa-juelich.de

Das ZAM betreibt auch den *Name Server*, der in der Lage ist, diese Namen auf die zugehörenden IP-Adressen umzusetzen (zam048, Backup: zam049). Andere Rechner im INTERNET können entweder über ihren Namen (der dann auf die IP-Adresse umgesetzt werden muß) oder direkt über ihre IP-Adresse (die i.a. aber nicht bekannt ist und auch nicht bekannt zu sein braucht) angesprochen werden.
Um die internen Netze der KFA im Internet-Sinne zu strukturieren, wird *Subnetting* verwendet. Die bei einer Klasse-B-Netzadresse für die lokale Adressierung zur Verfügung stehenden zwei Bytes wurden so aufgeteilt, daß ein Byte für die Subnetz-Adressierung und ein Byte für die Host-Adressierung verwendet wird: unter Weglassung der ausgezeichneten Bitkombinationen steht also ein Adreßraum von 254 Subnetzen mit je maximal 254 Hosts zur Verfügung.
Echte Subnetze müssen durch *Router* voneinander getrennt sein. Der KFAnet-Ethernet-Backbone und alle daran über Brücken angeschlossenen Ethernet-Segmente bilden im Internet-Sinne ein Subnetz, welches die Subnetz-Adresse 80 hat, so daß alle Rechner dieses Subnetzes Adressen der Form **134.94.80.ddd** haben.

5.1.2.2 Organisation

Bevor ein Benutzer mit seinem System (Rechner, Workstation, PC) an KFAnet/-INTERNET teilnehmen kann, müssen zwei Voraussetzungen erfüllt sein:

1. Der Rechner muß physikalisch an KFAnet (Ethernet, später auch FDDI) angeschlossen sein.
2. Es muß vom ZAM eine KFA-weit (und damit weltweit) eindeutige INTERNET-Adresse sowie ein Name zugewiesen worden sein, und der Name muß im *Name Server* eingetragen sein.

Das ZAM hat zu diesem Zweck ein Anmeldeformular (s. Folgeseite) entwickelt, welches gemeinsam vom Benutzer und einem zuständigen ZAM-Mitarbeiter auszufüllen ist.

A n m e l d u n g

Host_Id (8)[1] :	

für einen Anschluß an:

KFA net

INTERNET / DECNET

Vom Anmelder auszufüllen:

Rechner-Typ					
Standort	Gebäude		Raum		
Betriebssystem			Version		
Host-Name[1] (canonical name)	DECNET (12)				
	INTERNET (8)				
Alias-Namen	DECNET (12)				
	INTERNET(12)				
Host soll bekannt sein	KFA-weit		weltweit		

Vom KFAnet-Netzmanagement auszufüllen:

Netzwerk-Adressen	DECNET				
	INTERNET	Address			
		Domain			
		Subnet			
Hardware-Adressen	Ethernet	Segment			
		Hardw-Addr			
		Phys-Addr			
	FDDI	Segment	-		
		Hardw-Addr	-		
		Phys-Addr	-		
	Token Ring	Segment			
		Address		PUID	

Vom Systemverantwortlichen auszufüllen:

Systemverantwortlicher		Org.Einh.	
KFA-Telephon		Funkruf (74) -	
E-Mail (für Mitteilungen an den Systemverantwortlichen)	EARN		
	DECNET		
	INTERNET		

Anmeldung bitte an: W.Anrath oder R.Niederberger , ZAM , ☎: 4772 (INTERNET) oder
H.Stoff , ZEL , ☎: 5159 (DECNET)

---

1 In Abstimmung mit dem Netzmanagement (Tel: 4772), **Default = Host_Id**
Für Gateways bitte je Interface 1 Formblatt ausfüllen

Bitte schützen Sie Rechner und Daten vor unbefugtem Zugriff:

- alle Benutzer-IDs durch nicht-triviale Paßwörter schützen, keine anonymen Accounts
- alle Dienste ohne Paßwortschutz (z.B. rcp, rlogin, rshell) und Dienste, die Informationen über Benutzer liefern (z.B. rwhod, fingerd), nicht aktivieren
- vertrauliche Informationen nicht über Netze verschicken
- Rechner mit besonderen Sicherheitsbedürfnissen nicht an Netze anschließen
- keine Programme aus unbekannten Quellen ausführen, zumindest nicht privilegiert (SYSTEM, root)
- Logging und Accounting wenn möglich nicht abschalten
- Vorsicht bei E-Mail: Ein falscher Absender kann leicht vorgetäuscht werden.

Hinweis: Im Zusammenhang mit dem Anschluß an KFAnet werden personenbezogene Daten gespeichert.

(Rückseite des Anmeldeformulars)

Die für den Netzbetrieb wichtigen Daten werden in einer Datenbank abgelegt, und der Benutzer bekommt einen Auszug aus dieser Datenbank (auf dem gleichen Formular), dem er die ihn betreffenden Angaben und Zuordnungen entnehmen kann.
Der erste Komplex des Formulars enthält Angaben zum anzuschließenden Rechner und dessen Aufstellungsort. Diese Angaben dienen Managementzwecken und können auch beim Auftreten von Fehlerbedingungen von Nutzen sein.
Der zweite Teil enthält die eigentlichen Internet-Daten. Da manche Systeme gleichzeitig Teilnehmer im KFAnet/INTERNET und im KFAnet/DECnet sind, sind auch Felder für die wichtigsten DECnet-Parameter vorhanden.
Im dritten Teil wird der für das anzuschließende System verantwortliche Mitarbeiter erfaßt und dessen Erreichbarkeit sichergestellt.
Zusätzlich werden auch einige Sicherheitshinweise für den Betrieb von Rechnern am INTERNET gegeben.

Die Randbedinungen für eine Teilnahme am KFAnet/INTERNET und die angebotenen Dienste sind in einer Reihe von Technischen Kurzinformationen (TKIs) beschrieben [1,..., 9, 14, 20].

5.1.2.3 Dienste im Internet

Die wichtigsten über KFAnet/INTERNET angebotenen Kommunikationsdienste sind die ARPA-*Services* TELNET, FTP und SMTP.
Die Inanspruchnahme bzw. Bereitstellung der Internet-Anwendungsdienste (auch der ARPA-*Services*) basiert auf dem *Client-Server*-Prinzip. Auf einer *Server*-Maschine wird ein Dienst durch einen *Server*-Prozeß erbracht, der seine Bereitschaft durch eine Verbindung zu dem dem betreffenden Dienst zugeordneten *well-known Port* bekundet.
Soll der Dienst von einem anderen System im Internet aus in Anspruch genommen werden, so muß dort für den Dienst ein *Client*-Prozeß existieren, der eine (TCP-) Verbindung zu dem *well-known Port* auf der *Server*-Maschine herstellt, über die dann Kommandos/Daten des Anwenders (Anwender kann i.a. auch ein Programm sein) zum *Server* geleitet werden und dessen Antworten/Daten zum Anwender zurückfließen.
Beim Aufbau einer Verbindung zwischen *Client* und *Server* wird nur auf der *Server*-Seite die Nummer des dem Dienst zugeordneten *well-known Port* verwendet, auf der *Client*-Seite wird eine beliebige freie *Port*-Nummer zugeordnet. Da eine TCP-Verbindung durch das Paar von *Port*-Nummern an den beiden Enden der Verbindung identifiziert wird, können mehrere unterscheidbare Verbindungen zur gleichen *Port*-Nummer im *Server*-System hergestellt werden. Dies ist die Voraussetzung dafür, daß ein *Server* seine Dienste gleichzeitig für mehrere Benutzer/*Clients* erbringen kann.
Server sind meist deutlich komplexer als *Clients*, da die Dienste i.a. von mehreren Benutzern/*Clients* zeitgleich in Anspruch genommen werden können. Dies kann so realisiert werden, daß ein *Master Server* eine Verbindung annimmt, evtl. auch einige Überprüfungen o.ä. durchführt, für die eigentliche Durchführung des Dienstes (etwa den Transfer eines Files), die längere Zeit in Anspruch nehmen kann, aber einen *Slave Server*-Prozeß erzeugt und dann selbst für die Annahme weiterer Verbindungen wieder frei ist. *Slave Server* werden dynamisch in benötigter Anzahl generiert und nach Abschluß ihrer Arbeit wieder beendet.
Es ist offensichtlich, daß ein solches Konzept ohne unterstützende Fähigkeiten des Betriebssystems (insbesondere *Multitasking*-Fähigkeit, d.h. die Fähigkeit, mehrere Pro-

zesse gleichzeitig in Bearbeitung zu haben) kaum zu realisieren ist. *Multitasking*-Fähigkeit ist auf *Server*-Seite auch dann erforderlich, wenn nur ein *Server*-Prozeß existiert, weil dieser ansonsten – sobald er gestartet ist – den Rechner blockieren würde. Aus diesen Gründen wird auf kleinen Systemen ohne entsprechende Betriebssystem-Fähigkeiten (etwa PCs) oftmals nur der *Client*-Teil eines Dienstes implementiert, d.h. der betreffende Dienst kann von einem solchen System aus in Anspruch genommen werden, wird aber für andere nicht auf diesem System bereitgestellt. Bei fast allen Internet-Diensten (Ausname TFTP) kann bei der Angabe des Zielsystems (auf dem der Dienst in Anspruch genommen werden soll) die IP-Adresse oder der *Domain*-Name verwendet werden, wobei im letzteren Fall der *Client* die Auflösung unter Benutzung des *Name Server* vornimmt.

TELNET

Die Funktion *Interactive Terminal Login* wird in der TCP/IP-Protokollfamilie durch das TELNET-Protokoll realisiert.
TELNET erlaubt es einem Benutzer (kann auch ein Anwendungsprogramm sein), eine TCP-Verbindung zu einem *Login-Server* auf einem entfernten System herzustellen, und sendet dann Eingabedaten vom Terminal direkt zur entfernten Maschine und leitet in Gegenrichtung Ausgaben vom entfernten System an das Terminal, so, als sei dieses ein lokales Terminal des entfernten Systems (Abb. 13). Dazu ist es erforderlich, daß das Betriebssystem der *Server*-Maschine eine als Pseudo-Terminal bezeichnete Schnittstelle unterstützt, die es gestattet, von einem Progamm aus Zeichen einzuschleusen als ob sie von einem realen Terminal kämen, und umgekehrt für ein Terminal bestimmte Ausgaben zu übernehmen.

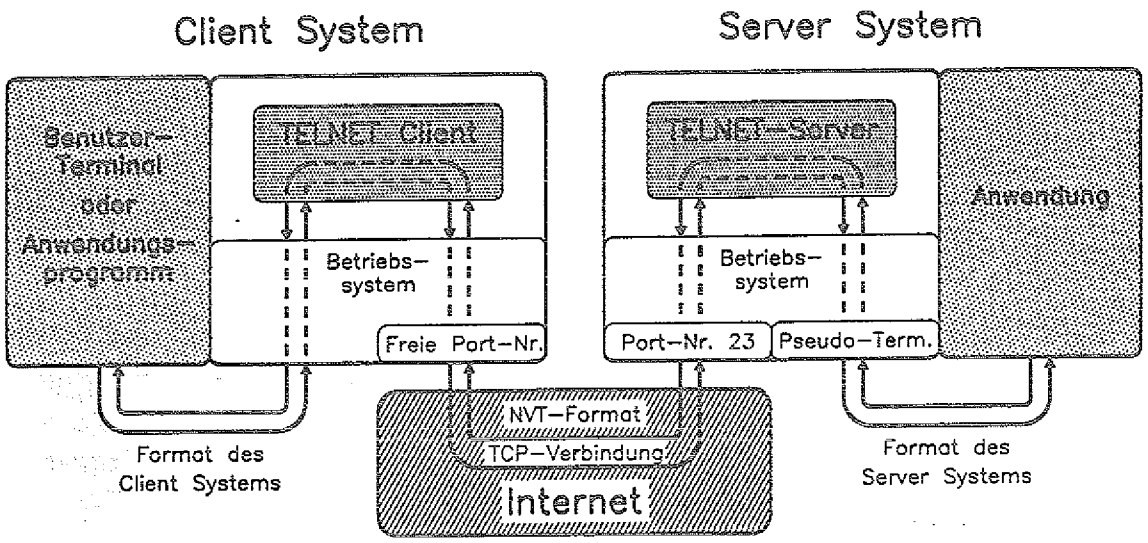


Abb. 13. TELNET Client-Server-Beziehung

TELNET hat zwei wichtige Komponenten:

1. Um die mögliche Heterogenität in den Terminals (die wichtigsten Terminaltypen sind DEC VTxxx und IBM 3270) und in den beteiligten Systemen zu beherrschen, ist das *Network Virtual Terminal* (NVT) als Standard-Interface zwischen den betei-

ligten Systemen definiert (betrifft insbesondere die Interpretation von Steuerzeichen). Auf der Internet-Verbindung zwischen *Client* und *Server* wird das Standard-NVT-Format benutzt. Im *Client* werden die vom Terminal kommenden und im lokalen System gültigen Zeichen zum Weitertransport zum *Server* auf das NVT-Format umgesetzt, und umgekehrt werden die vom *Server* im NVT-Format ankommenden Sequenzen in das im *Client*-System gültige Format gewandelt.
Der *Server* realisiert die entsprechenden Umwandlungen.

2. Es ist ein Mechanismus vorhanden, mit dessen Hilfe *Client* und *Server* Optionen für die TELNET-Verbindung aushandeln können (z.B., ob 7- oder 8-Bit ASCII-Code verwendet werden soll), und ein Satz von Standardwerten. Dieser Mechanismus ist symmetrisch, d.h. *Client* und *Server* sind beim Aushandeln von Optionen gleichberechtigt.

FTP (File Transfer Protocol)

FTP ist das Standard File Transfer Protokoll der TCP/IP-Protokollfamilie und setzt auf TCP als zuverlässiger Transportverbindung auf.
FTP leistet nicht nur den bittransparenten Transfer von Dateien zwischen den beteiligten Systemen.

- FTP kann von Programmen aus benutzt werden. Die meisten Implementationen haben aber zusätzlich eine interaktive Schnittstelle, über die ein Benutzer über den FTP-*Server* im entfernten System mit dem File-System dieses Rechners korrespondieren kann. Er kann etwa eine Liste aller Files in einem Verzeichnis (*Directory*) anfordern, aber auch konkrete Maßnahmen durchführen (z.B. ein neues *Subdirectory* einrichten).

- FTP verlangt zwingend, daß sich ein Benutzer durch eine User-Id eindeutig identifiziert und durch ein Paßwort legitimiert. Ohne dieses verweigert der *Server* jeden Zugriff auf das dortige File-System.

- FTP erlaubt nicht nur einen bittransparenten Transport ganzer Dateien. Der Benutzer kann Datenformate angeben, z.B. ob die Inhalte binäre Zahlenwerte darstellen oder alphanumerische Zeichen sind, und, wenn es Zeichen sind, ob sie ASCII- oder EBCDIC-verschlüsselt sind. Beim Transfer werden die gegebenenfalls erforderlichen Umsetzungen (z.B. ASCII $\Leftrightarrow$ EBCDIC) automatisch vorgenommen. Es ist zu beachten, daß bei solchen Umsetzungen Information verloren gehen kann, und die Umsetzungen dann nicht mehr umkehrbar eindeutig sind (wenn etwa zwei Systeme unterschiedliche Gleitkommadarstellungen haben, so daß bei einer Umwandlung Genauigkeit verloren geht, so kann diese bei einer anschließenden Rückkonversion nicht wieder hinzugefügt werden).

Wie bei anderen Internet-Diensten auch, können die Dienste eines FTP-*Servers* gleichzeitig von mehreren *Clients* aus in Anspruch genommen werden. Anders als bei den anderen Diensten werden für eine FTP-Sitzung u.U. aber mehrere Transportverbindungen zwischen einem *Client* und dem *Server* etabliert. Zu Beginn einer FTP-Sitzung wird zunächst eine Kontrollverbindung aufgebaut, über die z.B. die Authentisierungs-Prozedur abgewickelt wird und über die Steuerinformationen (auch Kommandos) laufen. Falls es zum Transfer einer Datei kommt, wird dafür eine separate Verbindung aufgebaut (vgl.

Abb. 14). Beide Verbindungen basieren auf TCP als Transportprotokoll; bei der Kontrollverbindung handelt es sich um eine TELNET-Verbindung mit reduzierter Funktionalität (keine aushandelbaren Optionen).

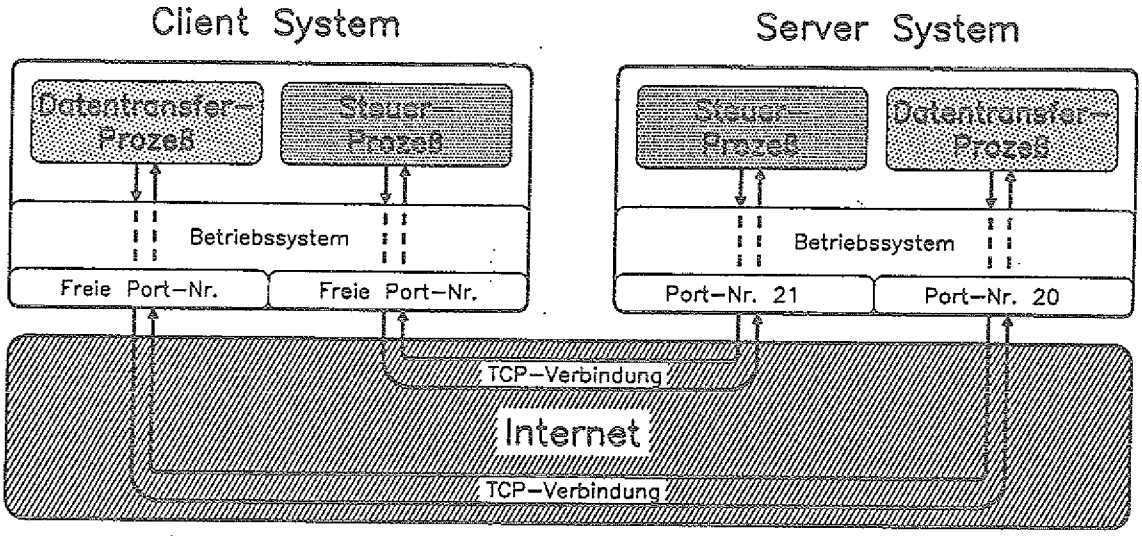


Abb. 14. FTP Client-Server-Beziehung

Während die Kontrollverbindung für die gesamte Dauer einer FTP-Sitzung bestehen bleibt, werden Datentransfer-Verbindungen dynamisch für die Übertragung von Dateien auf- und anschließend wieder abgebaut.

TFTP (Trivial File Transfer Protocol)

Das normale File Transfer Protokoll der TCP/IP-Protokollfamilie, FTP, ist vergleichsweise komplex und verlangt sogar auf der einfacheren *Client*-Seite, daß parallel mehrere TCP-Verbindungen unterhalten werden, was auf kleineren Systemen ohne adäquate Betriebssystemunterstützung nicht leicht zu realisieren ist.
Für solche Anwendungsfälle, wo die volle Funktionalität von FTP nicht erforderlich und die Komplexität nicht erwünscht ist, enthält die TCP/IP-Protokollfamilie ein sehr viel einfacheres und unaufwendigeres File Transfer Protokoll, TFTP.

TFTP sieht keine Authentisierung vor und unterstützt nur einfache File Transfers. Es basiert auch nicht auf TCP als Transportprotokoll, sondern auf dem sehr viel einfacheren UDP. Um die Verbindung gegen Fehlerbedingungen (z.B. Verlust von Datagrammen) robust zu machen, existiert symmetrisch auf Sender- und Empfängerseite ein Timeout- und Wiederholungsmechanismus. Ein File wird in Blöcken fester Länge (512 Bytes) transferiert, die mit 1 beginnend durchnumeriert werden. Nach dem Absenden eines Blocks wartet der Sender die Bestätigung der betreffenden Block-Nummer ab. Trifft diese nicht (rechtzeitig) ein, wird der Timeout also wirksam, so wird der Block wiederholt. Umgekehrt bestätigt der Empfänger einen empfangenen Block sofort mit seiner Block-Nummer. Trifft vor Ablauf des Timers kein weiterer Block ein (obwohl der File noch nicht komplett übertragen ist), so wird die Bestätigung der betreffenden Block-Nummer wiederholt. Das Ende der Übertragung wird durch einen Block mit einer Blocklänge von weniger als 512 Bytes erkannt.

TFTP beschränkt sich auf wenige Kernfunktionen, und die Implementationen nehmen deshalb auch vergleichsweise wenig Speicherplatz ein, so daß das Programm auch leicht in ROMs untergebracht werden kann. TFTP ist deshalb ein geeignetes Protokoll für das initiale Laden der Betriebssoftware von *Diskless Workstations* von einem *Load Server* im Netz aus.

SMTP

Electronic Mail ist der (nicht nur im INTERNET) am weitesten verbreitete Datenkommunikationsdienst.
Der Dienst wird durch zwei Standards beschrieben,

- das *Simple Mail Transfer Protocol* (SMTP), das beschreibt, wie die *Mail*-Systeme (*Client* und *Server*) Mitteilungen austauschen, und
- das in RFC 822 festgelegte Format der Mitteilungen.

Eine Adresse hat die Form:

local part @ domain name

Der *Domain*-Name identifiziert einen Rechner (wird in üblicher Weise im *Name Server* zu einer IP-Adresse aufgelöst). Der *Local Part* ist im einfachsten Fall die User-Id des Benutzers in dem angegebenen Rechner.
Das hier angegebene Adreßformat ist nur für Mitteilungen innerhalb des INTERNET so einfach. Es ist aber wünschenswert, auch Teilnehmern anderer Netze Mitteilungen zukommen lassen zu können bzw. von diesen erreichbar zu sein. Dafür müssen *Mail Gateways* oder *Mail Relays* die Netze verbinden. Über die dann erforderlichen Adreßformate lassen sich keine generellen Aussagen machen; sie sind i.a. aber aufwendiger, da sowohl ein geeigneter Gateway als auch der Adressat im fremden Netz eindeutig daraus hervorgehen müssen.

Eine Internet-Nachricht enthält nur druckbare Zeichen.
Dies gilt auch für die Kommunikation zwischen *Client* und *Server* im Rahmen von SMTP. Eine Aktion zwischen *Client* und *Server* beginnt mit einem 3-ziffrigen Code, dessen Interpretation für bessere menschliche Lesbarkeit angefügt ist. So antwortet beispielsweise der *Server*, nachdem der *Client* eine TCP-Verbindung zu ihm aufgebaut hat, mit

220 READY FOR MAIL

Der Dienst *Electronic Mail* unterscheidet sich seiner Natur nach von den anderen Anwendungsdiensten:

- Eine Identifikation ist nicht erforderlich, d.h. ein Teilnehmer soll einem anderen Teilnehmer eine Mitteilung zukommen lassen können, ohne sich ausgewiesen zu haben. Infolgedessen ist eine Authentifizierungs-Prozedur beim Versenden von Nachrichten nicht vorgesehen. Dies hat allerdings zur Konsequenz, daß letztlich auf die Absenderangabe nicht vertraut werden darf.
  Für den Empfang von Nachrichten ist eine Authentifikation erforderlich.

- Der Austausch von Nachrichten ist seiner Natur nach ein asynchroner Vorgang, d.h. es besteht keine Notwendigkeit, daß Absender und Empfänger eine direkte (zeitgleiche) Verbindung zueinander aufnehmen. Ein Absender kann zu irgendeinem (ihm genehmen) Zeitpunkt eine Mitteilung absenden, und der Empfänger zu irgendeinem späteren Zeitpunkt darauf zugreifen. Der *Client* agiert deshalb – was den Transport der Mitteilung angeht – nicht im unmittelbaren Auftrag des Teilnehmers. Der Teilnehmer übergibt die zu sendende Nachricht dem *Client*, der die Nachricht bearbeitet (z.B. Alias-Namen auflöst u.ä.) und in einem eigenen Speicherbereich (*outgoing mail spool area*) ablegt. Damit ist die Interaktion zwischen dem Absender und dem *Client* beendet.
  In einem zweiten unabhängigen Vorgang versucht der *Client* dann, die Nachricht an die angegebene Zieladresse zu transportieren. Wenn das Zielsystem vorübergehend nicht erreichbar ist, so wird dieser Versuch in regelmäßigen Abständen wiederholt. Erst wenn sich die Nachricht nach einer vorgegebenen (langen) Zeit als unzustellbar erweist, wird sie an den Absender zurückgegeben.
  Auf dem Zielsystem übernimmt der *Mail Server* die Nachricht, bearbeitet sie (überprüft beispielsweise, ob sie weitergeleitet werden muß) und speichert sie gegebenenfalls in der dem Adressaten zugeordneten *Mailbox*.

Die bisher beschriebenen Dienste sind die klassischen ARPA- oder Internet-Dienste. Darüberhinaus können mit dem vorhandenen Instrumentarium, d.h. auf der Basis des *Client/Server*-Konzeptes weitere, u.U. auch sehr spezielle Dienste etabliert werden. Die zusätzlichen über KFAnet/INTERNET verfügbaren Dienste sind in der nachfolgenden Tabelle zusammengestellt; weitere Dienstangebote sind geplant (z.B. zentraler *Print Server, File Server*).

Dienst	Beschreibung	Verfügbar auf
BIND-Service	TKI 147	*zam048 (zam049)*
DECnet-Internet-Gateway	TKI 144	*zam049 (zam048)*
REXEC (Remote Execution)	TKI 153	- - -
Anonymous FTP	TKI 147	*zam103*
NetNews	TKI 169	*zam103*
Remote Installation Service (RIS)	TKI 159	*zam103*
Time Service	TKI 175	*zam048 (zam049)*

BIND-Service

Für eine komfortable Nutzung der Internet-Dienste müssen *Directory Services* etabliert sein, die die Umsetzung von Internet-Namen auf Internet-Adressen bewerkstelligen. Der BIND-*Server (Berkeley Internet Name Daemon)* hat diese Funktion. Die Dienste dieses *Servers* werden i.a. automatisch, d.h. transparent für den Benutzer, von den *Client*-Implementationen der diversen Dienste in Anspruch genommen.
Es gibt darüberhinaus eine Benutzerschnittstelle (nslookup), über die Benutzer interaktiv auf die Informationen des *Servers* zugreifen können.

Im *Server* können neben Internet-Namen und -Adressen noch weitere Informationen abgelegt werden, wie Alias-Namen, Host-Informationen usw.

DECnet-Internet-Gateway

Als für die institutsübergreifende Datenkommunikation der KFA zuständige Einrichtung war und ist es eine wesentliche Aufgabe des ZAM, zu verhindern, daß die KFA bzgl. der Datenkommunikation in disjunkte Bereiche zerfällt. Diese Gefahr besteht nur dann nicht, wenn nur ein einziges Kommunikationssystem (Protokollwelt) eingesetzt wird. Es besteht jetzt die Hoffnung, daß dieser Zustand mit der allgemeinen Hinwendung zu den OSI-Protokollen erreicht werden könnte.
Solange es aber noch technische und historische Gründe gibt, in der KFA mehr als eine Protokollwelt zu unterstützen, müssen diese Welten miteinander verbunden werden. Damit die Probleme beherrschbar bleiben, ist es das Anliegen des ZAM und auch des ZEL, die Zahl der eingesetzten Protokollfamilien so klein wie möglich zu halten.
Die derzeit in KFAnet unterstützten Protokollwelten sind DECnet und Internet. Zur Verbindung dieser Welten ist somit ein DECnet-Internet-Gateway erforderlich. Die erforderliche Gateway-Software wird von der Fa. DEC angeboten, die im eigenen Produktspektrum die beiden in der KFA verbreiteten Protokollwelten hat (nämlich VMS/DECnet und ULTRIX/Internet) und der daraus resultierenden Notwendigkeit der Interkonnektion durch Bereitstellung eines entsprechenden Produkts Rechnung trägt.
DEC bietet für das Betriebssystem ULTRIX ein lizensiertes Softwareprodukt an, durch das ein ULTRIX-System *End-Node*-Funktionalität in einem DECnet erhält. Das ZAM hat diese Software auf dem DECnet-Internet-Gateway installiert (zam049) und bietet damit KFAnet/DECnet- und KFAnet/INTERNET-Benutzern die Möglichkeit, Ziele in der jeweils anderen Protokollwelt zu erreichen. Über den Gateway hinweg unterstützte Dienste sind *Remote Terminal Access (Virtual Terminal)*, *File Transfer* und *Electronic Mail*.
Die vorgenannte DECnet-Software für ULTRIX kann auch auf ULTRIX-Systemen der Benutzer installiert werden, die dann als zugelassene Teilnehmer in KFAnet/DECnet und KFAnet/INTERNET beide Kommunikationsschienen gleichrangig benutzen können, ohne auf den zentralen Gateway angewiesen zu sein.
Eine analoge Möglichkeit haben auch VMS-Benutzer, da auch TCP/IP-Implementationen für VMS sowohl von DEC selbst (VMS-ULTRIX-CONNECTION) als auch von anderen Anbietern (z.B. MULTINET, WOLLONGONG) zur Verfügung stehen.
Mit diesen Möglichkeiten ist das Problem der Konnektivität zwischen den in KFAnet unterstützten Protokollwelten DECnet und Internet zufriedenstellend gelöst.

REXEC (Remote Execution)

REXEC bietet die Möglichkeit, Anwendungen auf einem Zielrechner direkt von einer lokalen Workstation aus zu starten und zu steuern. Dies kann ohne manuellen Eingriff des Anwenders (d.h. ohne virtuelles Login auf dem Zielrechner) direkt aus einer lokalen Anwendung heraus geschehen. REXEC ist einer der sogenannten *Berkeley Services*.

Anonymous FTP

Anonymous FTP ist eine auf FTP basierende Methode, Informationen und Programme bereitzustellen und auf diese Weise zu verteilen. Dazu wird auf dem *Server* ein *Account* (User-Id) ohne Paßwort-Überprüfung eingerichtet (üblich ist die Eingabe der eigenen E-Mail-Adresse bei der Paßwortabfrage), auf dem die bereitgestellten Informationen in

geeigneter Strukturierung von dazu authorisierten Teilnehmern eingespeichert werden und nachfolgend von allen Netzteilnehmern abgerufen werden können.
Bereitgestellt werden:

- Informationen über KFAnet/INTERNET (z.B. Hosts- und Networks-Tabellen)
- Im KFAnet-Umfeld bedeutsame Software für Workstations und PCs (z.B. Terminal-Emulationen)
- Informationen des ZAM an KFA-Mitarbeiter (z.B. ZAM-TKIs).

NetNews
Hierbei handelt es sich um ein weltweit über INTERNET erreichbares Konferenzsystem. Das Dienstangebot umfaßt:

- Bereitstellen und Versenden von Artikeln und Nachrichten
- Public Domain Software
- Fehler-Requests
- Diskussionsforen

Im Unterschied zu Mailing-Listen werden die Nachrichten den individuellen Benutzern nicht zugestellt, sondern (für eine bestimmte Zeit) auf zentralen (NetNews-) *Servern* bereitgestellt, auf die die Benutzer zugreifen können (Abholprinzip).
Dies hat bei einem umfangreichen Informationsangebot den Vorteil, daß

1. für eine größere Zahl von Teilnehmern nur eine einzige Kopie auf dem *Server* gespeichert werden muß und
2. der einzelne Benutzer nicht mit Information zugeschüttet wird.

Es gibt zwei Typen von News-Gruppen:

- Moderierte Gruppen,
  die einen Moderator haben und nur von diesem gutgeheißene Beiträge aufnehmen.

- Nicht-moderierte Gruppen,
  bei denen Beiträge "unzensiert" direkt an NetNews gehen.

Die von der KFA abonnierten News-Gruppen stellen eine Auswahl wissenschaftlicher Themen dar, die bei Bedarf noch erweitert werden kann. Bei einer angestrebten Aufbewahrungsdauer der Beiträge von 14 Tagen beläuft sich die gespeicherte Informationsmenge derzeit auf ca. 600 MByte.

Es werden auch KFA-interne (d.h. nur innerhalb der Domain *kfa-juelich.de* zugreifbare) News-Gruppen eingerichtet.

Remote Installation Service (RIS)
Durch diesen Service werden DEC-ULTRIX-Softwareprodukte für die Installation auf DEC-ULTRIX-Systemen im Netz bereitgestellt. Dadurch kann auf diesen Systemen ein Medium für das Einspielen von Software eingespart werden.

Time Service
Auf dem *Time Server* wird die amtliche Zeit bereitgestellt (erfaßt über DCF77). Sie kann von anderen Systemen dort abgerufen werden. Ein Protokoll dafür wurde ebenfalls ent-

wickelt und steht zur Verfügung. Längerfristig (d.h. so, wie Implementationen verfügbar werden) ist die Verwendung von NTP *(Network Time Protocol)* als Internet-Standard für die Synchronisation der Rechner im Netz vorgesehen.
Bei solchermaßen synchronisierten Rechnern liegen die Zeitabweichungen im Bereich von Hundertstelsekunden.

5.2 DECnet

5.2.1 Allgemeines

DECnet ist die Bezeichnung für die Netzwerkprodukte der Fa. DEC, die sich an der Netzwerkarchitektur der Firma, DNA *(Digital Network Architecture)*, ausrichten.
Generelle Entwicklungsziele von DNA sind:

- Den Benutzern bzw. den Anwendungen der Benutzer soll für Kommunikationszwecke eine einheitliche Schnittstelle zur Verfügung gestellt werden, die ein breites Spektrum unterschiedlicher Kommunikationsanforderungen abdeckt.

- Die Architektur soll unterschiedliche Kommunikationseinrichtungen unterstützen und an neue Entwicklungen in der Kommunikationstechnik anpaßbar sein.

- Die Lösung soll kostengünstig sein. Netzwerkseitig sollen Effizienz und Performance eines DNA-basierten Netzes den bis dahin üblichen speziellen Lösungen vergleichbar sein. Verteilte Anwendungen sollen wegen des eingesparten Aufwands für die Kommunikation schneller, leichter und kostengünstiger implementierbar sein.

- Die Architektur soll unabhängig vom Transportnetz Datenkommunikation zwischen Benutzern unterstützen; Struktur und Leistungsfähigkeit des Übertragungssystems sollen keinen Einfluß auf die logischen Kommunikationsfähigkeiten haben.

- Die Verfügbarkeit soll hoch sein, die Funktion des Gesamtnetzes nicht durch den Ausfall einzelner Komponenten gefährdet werden. Wichtige Funktionen sollen verteilt vorhanden sein und nicht kritisch von einzelnen Komponenten abhängen.

- Sie soll in der Übertragungstechnik ebenso wie in der Datenverarbeitungstechnik an neue Entwicklungen anpaßbar sein; vertikale Integration (Verschiebung zeitkritischer oder häufig benutzter Funktionen in die Hardware oder Firmware) soll ebenso möglich sein wie die Definition funktionaler Untermengen für weniger leistungsfähige Knoten.

- Sie soll nicht von Charakteristika der Rechner oder Betriebssysteme abhängen und dadurch problemlos auf unterschiedlichen Hardware- und Softwaresystemen implementierbar sein.

Aus diesen generellen Forderungen, die in ähnlicher Form für alle Netzwerkarchitekturen aufgestellt worden sind, wurden konkrete Vorgaben abgeleitet (wie beispielsweise eine Strukturierung in Schichten, eine einheitliche Adressierung aller Knoten usw.), auf die hier nicht weiter eingegangen werden soll. Die Umsetzung dieser Ziele hat seit den Anfängen Mitte der siebziger Jahre zu mehreren Fortschreibungen (Phasen) der

Architektur und damit auch zu korrespondierenden Phasen der diese realisierenden DECnet-Produkte geführt. Jede neue Phase umfaßt grundsätzlich alle Funktionen und Fähigkeiten der vorherigen Phase:

Phase I (1976):
- *File Transfer* (Austausch von Dateien)
- Programm-zu-Programm-Kommunikation
- Verfügbar für PDP 11-Rechner unter dem Betriebssystem RSX-11M

Phase II (1978):
- *Remote File Access* (Zugriff auf Dateien entfernter Rechner)
- Netzwerkmanagement-Funktionen
- Alle wichtigen Rechnertypen und Betriebssysteme
- Punkt-zu-Punkt-Verbindungen

Phase III (1980):
- Netzwerk-Terminals *(virtual terminal service)*
- Fernladen von Programmen *(downline loading)*
- Erweitertes Netzwerkmanagement
- Adaptives *Routing* (Anpassung an veränderte Netzzustände)
- Mehrpunktverbindungen
- X.25-Unterstützung

Phase IV (1982):
- Große Netze möglich (65.535 Knoten; Phase III: 255 Knoten)
- Unterstützung von Ethernet
- SNA-Gateway
- Anschluß von DEC Professional 300 Workstations
- Anschluß von IBM-kompatiblen PCs

Phase V (1992):
- Integration von OSI-Standards
- Verbesserte Unterstützung bei großen Netzen
- *Naming Service (Directory Services)*

Die wichtigsten dieser Phasen sind die Phase IV, die den derzeitigen Leistungsumfang von DECnet-Netzen beschreibt, und die Phase V, die aufzeigt, in welche Richtung sich DNA weiterentwickelt. Hervorzuheben an Phase V ist die Integration von OSI, die sich nicht nur auf den derzeitigen Stand bezieht, sondern auch die strategische Aussage beinhaltet, daß Phase V auch während ihrer Lebensdauer in Richtung OSI weiterentwickelt wird, so wie dort Fortschritte gemacht werden.

DNA unterteilte den Kommunikationsvorgang ursprünglich in fünf Schichten. Von dort ausgehend hat auch von der Struktur her eine Entwicklung in Richtung auf das ISO-Referenzmodell stattgefunden. Das Strukturmodell für die Phase V zeigt die vollständige Übereinstimmung mit den OSI-Schichten, wobei oberhalb der Ebene 4 wahlweise die bisherigen DNA-Dienste angeboten werden, um die Zusammenarbeit mit Phase-IV-Produkten sicherzustellen.

Auf der untersten Ebene unterstützt DNA Ethernet (nicht CSMA/CD gemäß CCITT 802.3), EIA RS-232-D, CCITT V.24 und CCITT X.21.

Auf der Ebene 2 wird bei den lokalen Netzen ISO 8802/2 (LLC1 *Connectionless Mode*) unterstützt; darüberhinaus werden LAPB (X.25) und auch noch DDCMP (*Digital Data Communications Message Protocol*, das DEC-eigene Ebene-2-Protokoll) angeboten.

Auf Ebene 3 unterstützt DNA normalerweise den verbindungslosen Dienst, nur bei X.25-Verbindungen auch den verbindungsorientierten Dienst.
Ein Gesamtnetz kann aus einer Anzahl von Teilnetzen *(subnetworks)* zusammengesetzt sein. Die Teilnetze können auf öffentlichen Paketnetzen (X.25) basieren, können LANs sein (Ethernet) oder vermaschte Netze auf der Basis von HDLC- oder DDCMP-Punkt-zu-Punkt-Verbindungen.
Organisatorisch sind Gesamtnetze in sogenannte *Administrative Domains* aufgeteilt, die alle Netzknoten bzw. Teilnetze enthalten, die unter der Verwaltung einer einzelnen Organisation stehen. Eine *Administrative Domain* enthält eine oder mehrere *Routing Domains*. Eine *Routing Domain* ist dadurch definiert, daß sie alle Knoten und Teilnetze enthält, bei denen die *Routing*-Funktion in gleicher Weise durchgeführt wird. Da die *Routing Domains* sehr groß werden können, können sie vom Netzwerkmanager in *Subdomains* unterteilt werden, die als *Areas* bezeichnet werden. Jedes System (Knoten) gehört genau einer *Area* an. Es muß dementsprechend auch zwei Ebenen des *Routing* geben: *Level 1 Routing* innerhalb einer *Area (Adaptive Routing)* und *Level 2 Routing* zwischen den *Areas*. Zwischen verschiedenen *Routing Domains* wird das *Routing* durch statische *Routing*-Tabellen realisiert.
DNA kennt zwei Typen von Systemen (Knoten):

- ***End Systems:*** Diese können nur Anfangs- oder Endpunkt einer Netzverbindung sein. Sie sind nicht in der Lage, Informationseinheiten anderer Systeme weiterzuvermitteln.

- ***Intermediate Systems:*** Sie haben zusätzlich zu der Funktionalität von Endsystemen die Fähigkeit, als Zwischenknoten innerhalb einer Netzverbindung zwischen anderen Knoten Informationseinheiten vermitteln zu können. Solche Systeme werden als *Router* bezeichnet. Entsprechend der Strukurierung von *Routing Domains* in *Areas* gibt es zwei *Router*-Typen:

  - ***Level 1 Router:*** Diese vermitteln Informationseinheiten innerhalb der eigenen *Area* direkt; Informationen für Systeme außerhalb der eigenen *Area* geben sie an einen *Level 2 Router* weiter.

  - ***Level 2 Router:*** Sie haben innerhalb der eigenen *Area* die *Level 1 Router*-Funktionalität, können zusätzlich aber Daten an andere *Areas* weitervermitteln.

Für die Schicht 4 steht das herstellerspezifische *Network Services Protocol* (NSP) zur Verfügung. NSP weist große Ähnlichkeiten mit dem Transportprotokoll ISO 8073 *Class 4* auf.

5.2.2 DECNet in der KFA

5.2.2.1 Namen und Adressen

Alle Rechner an einem DECnet müssen eindeutig identifizierbar sein, was durch die Vergabe von eindeutigen *Area-/Node*-Nummern geschieht. Um die Eindeutigkeit sicherzustellen, werden diese Nummern in der KFA zentral vom ZEL vergeben. Maximal können 63 *Areas* mit bis 1023 *Nodes* eingerichtet werden. In der KFA wird für Rechner und PCs nur die *Area* 1 benutzt. Aus dem Vorrat von 1023 *Node*-Nummern sind den einzelnen KFA-Instituten Nummernkontingente zugeordnet.
LAT *Terminal Server* (LAT= *Local Area Transport Protocol)* sind in der *Area* 56, und auch dafür sind den Instituten Nummernkontingente zugeordnet. *Terminal Server* sind bezüglich ihrer eigentlichen Funktion keine DECnet-Knoten, können aber – wenn sie eine DECnet-Adresse haben – über diese für Managementzwecke angesprochen werden. Da alle DECnet-Rechner in der gleichen *Area* sind, ist *Level-2-Routing* nicht erforderlich, und weil KFAnet-Ethernet durch Brücken realisiert ist, im Sinne der höheren Protokollebenen also ein Ethernet darstellt, entfällt auch das *Level-1-Routing*; d.h. alle DECnet-Rechner können als Endknoten (*end systems*) konfiguriert werden.

5.2.2.2 Organisation

Um an KFAnet/DECnet teilnehmen zu können, muß vom ZEL eine *Area-/Node*-Nummer angefordert werden. Erforderliche Angaben sind:

Rechnertyp
Standort (Gebäude- und Raumnummer)
System-Manager (Name, Telefon)

Die KFAnet/DECnet-Prozeduren, die eine den KFA-Richtlinien entsprechende Installation bzw. Konfiguration von DECnet sicherstellen, sind in [20] beschrieben. Überdies gewährt das ZEL einen Installations- und Konfigurations-Service.
Für Anmeldungen, Zugang zu Software-*Kits* oder Mitteilungen über Netzprobleme steht die E-Mail-Adresse **ZELNET::KFANET** zur Verfügung.

5.2.2.3 Dienste

Die im DECnet zur Verfügung stehenden Dienste entsprechen funktional im wesentlichen denen in der TCP/IP-Protokollwelt.

6.0 Management

Das Management komplexer heterogener Netze stellt eine große Herausforderung dar. Netzwerkmanagement wird unter verschiedenen Gesichtspunkten betrieben, z.B.

- Verwaltung
- Monitoring
  Beobachtung des Betriebs im Sinne einer Funktionsüberwachung,
  Erkennen und Lokalisieren von Schwachstellen und Fehlern,
  Beseitigung von Fehlerbedingungen.
- Performance
  Optimierung der Nutzung der vorhandenen Ressourcen,
  Ableiten von Informationen für den weiteren Ausbau.
- Sicherheit
- Abrechnung *(Accounting)*
  Abrechnung erbrachter Dienste,
  Zuordnung der erbrachten Leistungen zu Instituten, Projekten und Personen.

6.1 Netzverwaltung

In einem Internet sind von der zuständigen Instanz der lokale Teil der Internet-Adresse (bei einer Klasse-B-Adresse also die beiden letzten Bytes der 4-Byte Internet-Adresse) und die Namen der zugeordneten *Subdomain* zu verwalten.
Zu jeder adressierbaren Einheit im Netz müssen eine Reihe von Informationen festgehalten werden. Das sind im wesentlichen:

- Systemkennung (z.B. Rechner-Typ)
- Betriebssystem/Version
- Organisationseinheit (Eigentümer)
- Systemverwalter (Name, Telefon, Mail-Adr.)
- Aufstellungsort (Gebäude, Raum)
- Name des Hosts
- Alias-Namen
- Netzanbindung (z.B. Hardware-Netzadresse)
- Sonstiges (z.B., ob ein Host außerhalb der eigenen Organisation im INTERNET sichtbar sein soll).

Alle diese Informationen werden in einer zentralen Datenbank gespeichert. Wann immer Informationen dieser Art benötigt werden, werden sie dieser Datenbank entnommen und sind deshalb immer konsistent.
Aus der Datenbank werden die für den Netzbetrieb erforderlichen Tabellen generiert, wie

- Hosts-/Networks-Tabellen (gemäß RFC 952),
- BIND-Tabellen (für die *Name Server*).

Diese Tabellen sind per *Anonymous FTP* auf dem Rechner *zam103* für alle Netzteilnehmer zugänglich. Sie können von dort auf Initiative eines Benutzers bei Bedarf in angeschlossene Rechner geladen werden, aber auch automatisch zu bestimmten Zeiten (empfohlenerweise jede Nacht) in angeschlossene Rechner übernommen werden; dadurch kann sichergestellt werden, daß Hosts jeweils am nachfolgenden Tag aktualisierte Tabellenversionen besitzen.
Bei jeder Veränderung/Ergänzung der Infomationen in der Datenbank werden neue Versionen der genannten Tabellen generiert und dem *Anonymous-FTP-Server* überspielt.

Durch entsprechende Hilfsprogramme wird auch die Bedienung des Systems durch die Systemverantwortlichen erleichtert.
Die Formulare, durch die die Informationen für die Datenbank erfragt werden (und die bei Beantragung einer INTERNET-Adresse für jeden Benutzer ausgefüllt werden müssen), stehen formatgleich auch als Datenbankauszüge zur Verfügung, und werden den Benutzern als Beleg über die zu ihrem System gespeicherten Angaben zugeschickt.
Auch bei der Vergabe neuer Adressen und Namen wird Unterstützung geliefert. Die nächste freie Adresse in einem Subnetz wird vom System auf Wunsch bereitgestellt, und grundsätzlich werden alle Adreß- und Namenseingaben sofort auf Eindeutigkeit überprüft.
Für eine Reihe von Feldern stehen Defaults zur Verfügung.
Die Informationen der Datenbank sind von autorisierten Personen online an jedem Terminal abrufbar und können für vielfältige Netzverwaltungsaufgaben herangezogen werden; sie sind insbesondere auch dann nützlich, wenn beim Auftreten von Fehlern die für ein gezieltes Eingreifen notwendigen Randbedingungen zu klären sind.

6.2 Monitoring

Monitoring findet auf verschiedenen Ebenen statt.
Auf der Ethernet-Ebene stehen die Hilfsmittel für eine umfassende Überwachung des Betriebs zur Verfügung.
Wichtig sind die *LAN Traffic*-Monitore (LTM), die im KFAnet-Ethernet-Backbone und z.T. auch in den nachgeordneten Netzsegmenten eine permanente Verkehrsüberwachung durchführen. Beim Auftreten von Besonderheiten oder Fehlern besteht die Möglichkeit, praktisch jedes Bit auf der Leitung zu analysieren *(LAN Analyzer, Network Quality Analyzer)*, und auch die Möglichkeit, die Funktionsfähigkeit der Kabelinfrastruktur zu überprüfen *(Time Domain Reflectometer)*. Beim Erkennen einer Bus-Unterbrechung, was durch die eingesetzte Überwachungssoftware automatisch geschehen kann, wird die Backup-Brücke im Ethernet-Backbone automatisch aktiviert, so daß wieder volle Konnektivität hergestellt wird.
Durch die automatische Überwachung erkannte Fehlerbedingungen werden auch an die Betreuungsmannschaft gemeldet.

Völlig anders stellt sich die Situation bei FDDI dar. Es gibt nur wenige wirklich leistungsfähige Überwachungswerkzeuge, und die sind außerordentlich teuer. Hinzu kommt, daß nicht nur der Aufbau eines FDDI-Rings in der KFA gerade erst begonnen hat, sondern daß sich die FDDI-Technologie generell in einem frühen Stadium der Markteinführung befindet, so daß auch die Techniker der Lieferfirmen durchweg weder

über ausreichende Erfahrungen noch über eine ausreichende Geräteausstattung verfügen.
Es ist aber klar geworden, daß unter diesen Randbedingungen ein qualifizierter Aufbau und Betrieb eines FDDI-Netzes nicht möglich ist, ohne die entsprechenden Hilfsmittel zur Verfügung zu haben. Dies beinhaltet das Dilemma, daß gerade in der Anfangs- und Lernphase Hilfsmittel benötigt werden, deren Kosten sehr hoch sind im Vergleich zum Wert der zu diesem Zeitpunkt installierten Komponenten, die mit ihrer Hilfe analysiert und überwacht werden sollen.

Für die Überwachung der X.25-Verbindungen werden die Hilfsmittel, die im und für den eingesetzten DATUS-Untervermittler verfügbar sind, genutzt. Damit ist eine permanente Überprüfung der ordnungsgemäßen Funktion der Leitungen möglich, und es wird eine Nutzungsstatistik erstellt. Im Fehlerfalle können auch einzelne Pakete analysiert werden.

Ein weiteres Monitoring findet auf der darüberliegenden Vermittlungsebene (Internet-Ebene) statt.
In regelmäßigen Abständen (derzeit halbstündlich) werden alle KFA-Hosts (INTERNET und DECnet) angesprochen und so auf ihre Funktionsfähigkeit überprüft. Diese Information steht den mit der Netzüberwachung befaßten ZAM-Mitarbeitern zur Verfügung (sie könnte auch allen KFAnet-Teilnehmern zugänglich gemacht werden).
Einer schärferen Überwachung unterliegen die für den Netzbetrieb wichtigen Komponenten; das sind alle Router (auch die Router der wichtigsten externen Partner), sowie alle zentralen *Server* (BIND-*Server* usw.) und die zentralen Großrechner. Die Ergebnisse dieser Überprüfung stehen den Operateuren im Maschinenraum in graphischer Form zur Verfügung (nicht antwortende Komponenten werden rot markiert).
Wenn auf der Internet-Ebene eine Komponente nicht erreichbar ist, kann die Ursache dafür in der Komponente selbst liegen oder in der Netzverbindung zu dieser Komponente. Im letzteren Fall müssen die im vorigen Abschnitt erwähnten Hilfsmittel der darunterliegenden Netzebene (Ethernet, X.25 usw.) herangezogen werden.

6.3 Sicherheit

Im Zuge der Einführung der Internet-Protokolle hat das ZAM eine umfangreiche Studie zur Sicherheit in Netzwerken ([21], nicht allgemein verfügbar) erstellt und insbesondere auch auf diesbezügliche Defizite in der UNIX/INTERNET-Welt aufmerksam gemacht. Manche der Schwächen sind systeminhärent und auf Anwenderebene nicht behebbar, weshalb das ZAM empfiehlt, sensitive Daten nicht über offene Netze zu kommunizieren. Darüberhinaus rät das ZAM zu einem sorgfältigen Umgang mit den vorhandenen Instrumenten (insbesondere Paßwörtern) und gibt Empfehlungen, wie Systeme zu konfigurieren sind, um im Rahmen des derzeit Möglichen die Gefährdungen zu minimieren.
Da weltweit das Problembewußtsein steigt, ist mit konzeptionellen Verbesserungen der Sicherheit von Systemen und Netzen durch die Hersteller zu rechnen, was angesichts der explosionsartigen Zunahme der Datenkommunikation (insbesondere im INTERNET) auch dringend erforderlich ist.
Derzeit bereitet das ZAM den Test sicherer Authentisierungsverfahren (KERBEROS) vor.

6.4 Performance und Accounting

Systematische Performance-Messungen und Accounting werden bisher nur in einigen wichtigen Teilbereichen durchgeführt. Derzeit laufen Arbeiten mit dem Ziel, die für ein umfassendes Accounting notwendige systematische Erhebung von Statistikdaten zu etablieren.

Ein Schwachpunkt aller bisherigen Management-Aktivitäten ist, daß es sich dabei um Einzelaktivitäten handelt, die nicht als Teilaspekte eines umfassenden Management-Konzeptes verstanden werden können.
Inzwischen liegen von verschiedenen Firmen (DEC, HP, IBM) Konzepte für ein umfassendes Management auch heterogener Netze vor, und es gibt auch erste Produkte im Rahmen dieser Management-Architekturen. Auch OSI hat sich unter dem Oberbegriff OSI-Management des Themas angenommen und eine Reihe von Standards verabschiedet bzw. in Arbeit. Nachteil des OSI-Managements ist, daß es auf das Management von OSI-Netzen beschränkt ist, die bekanntermaßen nicht die heutige Netz-Wirklichkeit sind. Die Firmenansätze sind insofern umfassender und realistischer, als sie die OSI-Konzepte berücksichtigen, aber darüberhinaus auch Nicht-OSI-Netze einbeziehen wollen.
Das ZAM prüft die Leistungsfähigkeit der Herstellerplattformen sowohl unter allgemeinen Gesichtspunkten wie auch im Hinblick auf die Gegebenheiten in der KFA und wird baldmöglichst ein solches Produkt für übergeordnete Management-Aspekte wie auch in bestimmten Teilbereichen einsetzen.

7.0 Zukunftsperspektiven

Die Zukunftsperspektiven werden in zwei unterschiedlichen Ansätzen dargestellt. Einerseits werden – ausgehend vom derzeitigen Entwicklungsstand von KFAnet – die absehbaren Schritte der evolutionären Weiterentwicklung dargelegt. Andererseits werden allgemeine Entwicklungen, die sich im Kommunikationsbereich abzeichnen, aufgezeigt und die Folgerungen für die KFA diskutiert.

7.1 Geplante Weiterentwicklungen von KFAnet

Es wurde schon mehrfach darauf hingewiesen, daß es weltweit eine allgemeine – derzeit allerdings noch überwiegend ideelle – Hinwendung zu den OSI-Standards gibt. Zumindest im Forschungsbereich ist die augenblickliche Situation jedoch durch einen massiven Einsatz der TCP/IP-Protokolle mit dramatischen Zuwachsraten gekennzeichnet. Dadurch werden Fakten geschaffen, die sich bei der nach wie vor angestrebten Migration zu den OSI-Protokollen auswirken werden, vor allem dahingehend, daß nur eine weiche Migration in Frage kommt und daß dieser Vorgang sehr viel länger dauern wird als viele OSI-Befürworter sich das wünschen.
Die Verzögerungen bei der Einführung der OSI-Protokolle haben zwei zusätzliche Ursachen:

1. Mit den Internet-Protokollen ist bereits eine weltweite offene Kommunikation auf einer einheitlichen Basis möglich, also das, was durch die OSI-Protokolle erreicht werden sollte, dort aber noch erst unter Beweis zu stellen ist; d.h. das Ziel einer unbeschränkten, offenen Kommunikation ist bereits ohne OSI-Protokolle erreicht.

2. Der allgemeine Reifezustand von TCP/IP-Implementationen ist – angesichts eines mehrjährigen Entwicklungsvorsprungs nicht überraschend – deutlich besser als der von OSI-Implementationen. In dieser Hinsicht kommt erschwerend hinzu, daß die OSI-Protokolle durchweg komplexer sind als die Internet-Protokolle, was eine Folge der höheren Funktionalität der OSI-Dienste ist. Um dadurch bedingte weitere Verzögerungen bei der Verfügbarkeit von OSI-Produkten zu vermeiden, hat man den entsprechenden Internet-Diensten vergleichbare Untermengen der OSI-Standards definiert (etwa als europäische Vornormen), die in einem ersten Schritt realisiert werden.
   Es ist deutlich erkennbar, daß die Anwender unter Berücksichtigung der unter 1. geschilderten Lage kaum bereit sind, unfertige und überdies oftmals auch noch überteuerte OSI-Implementationen in Produktion zu nehmen.

Wichtig für die Migration von Internet nach OSI ist auch die Tatsache, daß auch die Internet-Protokolle einer Weiterentwicklung unterliegen, die u.a. eine Fortentwicklung in Richtung auf OSI-Verträglichkeit beinhaltet. Dabei wird zunächst eine Koexistenz von Internet-Diensten und OSI-Diensten auf einem Transportnetz angestrebt. Damit wird die in jedem Falle unvermeidliche parallele Nutzung der beiden Protokollwelten erleichtert und eine allmähliche Schwerpunktverschiebung in Richtung OSI in Abhängigkeit von der Verfügbarkeit und der Qualität von Produkten möglich.

Das ZAM bereitet derzeit den testweisen Einsatz erster OSI-Dienste auf Workstations vor. Dies betrifft zunächst die X.400 MHS-Dienste (*Message Handling Systems*). Hierbei handelt es sich um erstmals 1984 verabschiedete (und 1988 erweiterte) CCITT-Empfehlungen, die aufgrund ihrer Bedeutung und allgemeinen Akzeptanz von ISO unter der Bezeichnung MOTIS (*Message Oriented Text Interchange System*) übernommen wurden (ISO 10021). Für eine sinnvolle Nutzung muß gleichzeitig ein *Mail Relay* etabliert werden, um den Übergang zu anderen *Mail*-Systemen (insbesondere SMTP und EARN) sicherzustellen.
Darüberhinaus ist der Test von FTAM-Produkten (dem OSI File Transfer) geplant.
Für beide Dienste ist es notwendig, die für eine sinnvolle Nutzung erforderlichen *Directory Services* gemäß den CCITT X.500 Empfehlungen von 1988 zu etablieren. Insbesondere ist die Relation zum DNS (*Domain Name Service*) der TCP/IP-Welt zu klären und eine Migrationsstrategie zu erarbeiten.
Wenn die Tests erfolgreich abgeschlossen und die sonstigen Voraussetzungen erfüllt sind (*Directory Services, Mail Relay* und evtl. FTAM-Gateway), können die Dienste in KFAnet zugelassen werden.

Auch bei DECnet, der zweiten in KFAnet unterstützten Protokollwelt, findet eine Migration zu OSI statt. Die bereits seit langem angekündigte nächste Entwicklungsstufe, DECnet Phase V, ist eine Implementation der OSI-Protokolle, die die traditionelle Bezeichnung DECnet trägt, weil sie von DEC stammt und weil es über die eigentliche OSI-Implementation hinaus ein Anliegen der Fa. DEC ist, die Koexistenz alter DECnet-Versionen (insbesondere Phase IV) mit der neuen Version sicherzustellen und so Kontinuität im Netzangebot zu demonstrieren. Die Strategie ist dabei ähnlich der für die Internet-OSI-Migration beschriebenen: Oberhalb eines gemeinsamen Transportnetzes werden parallel zwei Protokollsäulen (Klassen von Anwendungsdiensten) angeboten: OSI-Dienste und DECnet-Dienste.
Mit der Implementation von OSI werden in DECnet nun auch *Directory Services* definiert und etabliert. Dies berührt direkt die X.500-Aktivitäten im ZAM, denn es müssen zwar *Directory Services* verfügbar sein, um OSI-Dienste mit dem gewohnten Komfort in einer offenen Umgebung anbieten zu können, aber es darf nicht sein, daß für jede OSI-Implementation eigene *Directory Services* und *Directories* etabliert werden. In der KFA sollte es nur einen *Directory Server* geben, der seinerseits eingebunden ist in ein übergeordnetes Netz externer *Directory Server*.

Über die mit den OSI-Diensten im Laufe der Zeit – wenn vollständige Implementationen der Standards vorliegen – automatisch einhergehenden funktionalen Verbesserungen hinaus, wird speziell auch eine stärkere Unterstützung einer verteilten Verarbeitung im Netz angestrebt, im Sinne einer Erweiterung (und Vereinfachung) der durch REXEC gegebenen Möglichkeiten.
Die OSF (*Open Software Foundation*) hat eine solche als DCE *(Distributed Computing Environment)* bezeichnete Funktion definiert und wichtige Anbieter (insbesondere IBM, DEC, HP) bieten für ihre Workstations eine entsprechende Funktion an. Alle diese Produkte basieren auf einer alten Entwicklung eines Netzbetriebssystems der Fa. Apollo (NCS= *Network Computing System*). Auch ISO arbeitet an der Standardisierung eines solchen Dienstes, liegt zeitlich aber zurück, weil hier gegenüber den oben erwähnten Produkten neue Features und Konzepte hinzukommen sollen.

Im Zusammenhang mit den Aktivitäten zum Workstation-Konzept testet das ZAM die verfügbaren Produkte auf verschiedenen Workstation-Plattformen mit dem Ziel, solche Dienste über KFAnet/INTERNET verfügbar zu machen.

Ein weiterer Komplex in der evolutionären Fortentwicklung von KFAnet betrifft alle Aspekte des Netzmanagements in heterogenen, komplexen Netzen.
Ein konkretes Anliegen, das nicht so sehr für KFAnet als lokales Netz wie für KFAnet als Teilnetz des weltweiten INTERNET relevant ist, betrifft die Möglichkeit, Ressourcenverbrauch und damit Kosten einzelnen Instituten, Projekten und gegebenenfalls Personen zuordnen zu können. Bisher fehlen dazu vielfach die Werkzeuge, und sie waren auch nicht zwingend erforderlich, weil – nicht zuletzt, um die Nutzung der neuen Datenkommunikationsdienste zu fördern – diese Dienste den Benutzern kostenfrei zur Verfügung gestellt wurden. Diese Situation wandelt sich nun: Die Nutzung der Datenkommunikation nimmt derzeit explosionsartig zu, was deutlich erhöhte Aufwendungen zur Folge haben wird, wenn massive Engpässe vermieden bzw. beseitigt werden sollen. Diese Mittel müssen begründbar und abrechenbar sein. Deshalb ist es erforderlich, die Nutzung der Netzdienste genau zu erfassen, um die Kosten umlegen zu können.

7.2 Generelle Zukunftstrends

Voraussagen über zukünftige Entwicklungen sind mit Risiken behaftet, die unvermeidlich mit der zeitlichen Entfernung von der Gegenwart steigen. Fehleinschätzungen in der jüngeren Vergangenheit betrafen allerdings weniger die grundsätzlichen technischen Entwicklungen als vielmehr die zeitlichen Horizonte, d.h. **wann** diese verfügbar bzw. wirksam werden würden.
Die Perspektiven sind für die verschiedenen Ebenen der Kommunikation aufzuzeigen, d.h. für die Dienste und für die Techniken (Netze und Infrastrukturen).

7.2.1 Anwendungen

Die Informationen, die heute noch überwiegend verwendet und damit über Netze übertragen werden, sind alphanumerisch. Wir befinden uns derzeit in einer Phase des Übergangs zu graphischer Informationsdarstellung (Festbild). Dies deshalb, weil in vielen Fällen eine graphische (bildliche) Darstellung die sachgerechte ist und weil jetzt Datenverarbeitungseinrichtungen ebenso wie Endgeräte und Übertragungseinrichtungen einen Leistungsstand erreicht haben, daß eine graphische Darstellung zu vertretbaren Kosten allgemein verfügbar gemacht werden kann. Die allgemeine Verfügbarkeit führt wiederum dazu, daß Anwendungssysteme diese Möglichkeiten zunehmend nutzen.
Damit ist das Ende der Entwicklung aber noch nicht erreicht. Wenn es um die Veranschaulichung von Bewegungsvorgängen geht, sind Bewegtbilddarstellungen am besten geeignet, gegebenenfalls in Realzeit. In ein oder zwei Generationen werden die Kommunikationssysteme in der Lage sein, vermittelte Bewegtbildkommunikation zu unterstützen. Sie wird jedoch nur dort genutzt werden, wo diese Darstellungsart adäquat ist. Auch wenn Bewegtbilddarstellung möglich ist, wird es weiterhin Anwendungen geben, bei denen alphanumerische oder Festbilddarstellung angemessen ist. Wenn man die Kette alphanumerisch–Festbild–Bewegtbild bildet, so ist die Technik der anspruchsvolleren Darstellungsart immer auch in der Lage, die weniger anspruchsvollen Darstel-

lungsarten zu realisieren (d.h. alphanumerische Information kann als Graphik dargestellt werden, und Festbilder sind mit den Mitteln der Bewegtbildkommunikation erzeugbar); dieses zu tun, käme aber einer massiven Verschwendung von Ressourcen gleich. Es kommt also darauf an, daß ein Kommunikationssystem, jede Art der Informationsdarstellung unterstützt, so daß für jede Anwendung die adäquate, evtl. auch eine geeignete Kombination gewählt werden kann. Dazu gehört aber auch, daß entsprechend flexible und mächtige Ein- und Ausgabemedien zur Verfügung stehen. Wenn Übertragungssystem, Endgeräte und Kommunikationsdienste diese Fähigkeiten aufweisen, spricht man von Multimedia-Kommunikation. Am Beispiel der Mitteilungsvermittlungssysteme (E-Mail) kann man sich das so vorstellen, daß zusätzlich zu den heute üblichen Textinformationen auch Graphiken, Audio-Information (Tondokumente, aber z.B. auch Anmerkungen in gesprochener Form) und in fernerer Zukunft auch Bewegtbildsequenzen übermittelt werden können.
Mit der Verfügbarkeit der Bewegtbildkommunikation wird insofern eine Grenze erreicht, als keine Einzelanwendungen bekannt sind, die höhere Anforderungen an ein Kommunikationssystem stellen. Das bedeutet, daß weitere Leistungssteigerungen nicht mehr das Ziel haben, neue, bisher aufgrund technischer Unzulänglichkeiten nicht mögliche Nutzungsarten zu erschließen (weil keine bekannt sind), sondern nur noch der Bewältigung des Massenproblems dienen werden.
Soweit absehbar, besteht für die KFA aufgrund ihrer derzeitigen Aufgabenstellungen nicht die Notwendigkeit, eine Vorreiterrolle bei der Nutzung oder gar Entwicklung der neuen Kommunikationstechniken und -dienste zu spielen. Pionierleistungen werden wohl in medienorientierten und angrenzenden Bereichen (z.B. Computeranimation) erbracht werden.
Viele in der KFA zu bearbeitende technisch-wissenschaftliche Fragestellungen betreffen aber Bewegungsvorgänge, und Bewegtbilddarstellungen werden auch heute schon benutzt, notgedrungen unter Hinnahme eines Medienbruchs, indem die nicht in die normale Datenkommunikation integrierten klassischen Bewegtbildmedien Film und Video zur Anwendung kommen. Ein Bedarf ist in der KFA also vorhanden, und es ist deshalb davon auszugehen, daß die neuen Techniken – wenn sie entwickelt und zu erschwinglichen Kosten zur Verfügung stehen – in den dafür sinnvollen Anwendungen auch genutzt werden.

7.2.2 Übertragungssysteme

In KFAnet stehen derzeit Übertragungssysteme von 10 Mbps (Ethernet) allgemein zur Verfügung, und mit FDDI beginnt – zunächst vorwiegend im Backbone-Bereich – der Aufbau eines 100 Mbps-Systems. Diese Systeme, insbesondere FDDI, werden bis über die Mitte der neunziger Jahre hinaus die Basis der lokalen Kommunikation bilden, wobei mit dem zu erwartenden Preisverfall FDDI im Laufe der Zeit zum Standard-Medium für den Anschluß von Workstations werden wird. FDDI wird diese Zeitspanne auch abdecken müssen, weil deutlich leistungsfähigere Systeme vorher für einen allgemeinen Einsatz nicht zur Verfügung stehen dürften.
Die Frage ist, welche Übertragungssysteme notwendig wären, um die im vorigen Abschnitt erwähnte Bewegtbildkommunikation zu ermöglichen.
Um alphanumerische Information zufriedenstellend übertragen zu können, sind Übertragungsgeschwindigkeiten von 10–100 kbps im allgemeinen voll ausreichend, Graphik (Festbild) erfordert zwei Größenordnungen höhere Leistungen (also 1–10 Mbps) und

Bewegtbildkommunikation nochmals eine um den Faktor 100 höhere Übertragungsleistung, d.h. 100 Mbps bis 1 Gbps. Letztlich hängt die erforderliche Übertragungsrate von vielen, teils gegenläufigen Faktoren ab wie Auflösung, Bildwiederholfrequenz, Anzahl darstellbarer Farben, Nutzung von Kompressionstechniken usw.; für eine hochauflösende Darstellung ohne oder mit nur geringer Kompression ist 1 Gbps ein Richtwert.
Es ist aber nicht nur die erforderliche Datenrate, die den heutigen Übertragungssystemen (LANs) noch fehlt, sondern auch die Fähigkeit, isochrone Datenströme übertragen zu können (d.h. mit einer garantierten Datenrate nicht nur im Mittel über einen längeren Zeitraum, sondern bezogen auf einen vorgegebenen Zeittakt). Bewegtbildkommunikation erfordert diese Netzfähigkeit, ebenso wie auf einem viel niedrigeren Niveau die Sprachkommunikation.
Die bisher zumindest in Teilen standardisierten, im Stadium prototyphafter Realisierung befindlichen universellen (d.h für asynchronen und isochronen Verkehr geeigneten) Netze, das sind IEEE 802.6 DQDB *(Distributed Queue Dual Bus)* als MAN *(Metropolitan Area Network)* und ATM *(Asynchronous Transfer Mode)* als CCITT-Vorgabe für das zukünftige Breitband-ISDN, erreichen im derzeitigen Stadium der Entwicklung geringere oder zumindest nicht signifikant höhere Übertragungsgeschwindigkeiten als FDDI. Für beide steht nicht zu erwarten, daß vor Mitte der neunziger Jahre allgemein einsetzbare Produkte verfügbar sein werden, und bezüglich ATM wird sogar die Aussage gewagt, daß darauf basierende Systeme bis zum Ende dieses Jahrzehnts keine nennenswerte praktische Rolle spielen werden.

Hier soll sich eine Bemerkung zum heute bereits von der DBP Telekom angebotenen Schmalband-ISDN anschließen.
Die Hoffnungen, die Mitte der achtziger Jahre an das ISDN als auch im lokalen Bereich für die Datenkommunikation nutzbare Technik geknüpft wurden, haben sich nicht erfüllt, da sowohl die Bundespost wie auch die einschlägigen Hersteller das ISDN zunächst als modernes Telefonsystem gesehen haben und die Belange der Datenkommunikation (und damit auch die Integration von Sprach- und Datenkommunikation) keine ausreichende Berücksichtigung gefunden haben. Dieses Defizit ist bis heute nicht vollständig beseitigt.
Die Probleme, die zu deren Lösung seinerzeit ISDN ins Auge gefaßt worden war, sind inzwischen durch andere Techniken gelöst worden.
Im lokalen Bereich werden für die Datenkommunikation allenthalben LANs eingesetzt, und eine Nutzung von ISDN-Technik in größerem Umfang ist selbst bei bester Verfügbarkeit von ISDN-Komponenten nicht mehr denkbar.
Im externen Bereich wird die Datenkommunikation im Forschungsbereich (in Deutschland) überwiegend über das paketvermittelnde WIN und ergänzend über Standleitungsverbindungen abgewickelt. Das WIN bietet derzeit Übertragungsgeschwindigkeiten von 9,6 kbps und 64 kbps an und wird ab Anfang 1992 auch 2 Mbps Anschlüsse bereitstellen, die die KFA auch zu nutzen beabsichtigt.
Wenn die Bundespost, wie geplant, Anfang 1994 in Jülich ISDN-Anschlüsse bereitstellen wird (was sich wegen der Anstrengungen in den neuen Bundesländern noch verzögern könnte), wird das ISDN für die Datenkommunikationsbelange der KFA kaum mehr als eine weitere Lösungsmöglichkeit für längst gelöste Probleme sein:
Im lokalen Bereich wird sich kaum etwas ändern, da die breite Nutzung von LANs nicht rückgängig zu machen ist (was sinnvollerweise auch nicht angestrebt werden kann).

Im Fernbereich, wo zu diesem Zeitpunkt seit langem 2 Mbps im WIN zur Verfügung stehen, wird die Neigung, auf ISDN mit einer Standard-Kanalgeschwindigkeit von 64 kbps umzuschwenken, äußerst gering sein.
Diese Aussagen gelten für den Forschungsbereich und insbesondere für große Forschungseinrichtungen wie die KFA; im kommerziellen Umfeld und auch bei kleinen Forschungseinrichtungen könnten die Voraussetzungen für eine ISDN-Nutzung günstiger sein.
In einem bestimmten Umfeld könnte die ISDN-Nutzung auch für die KFA von Vorteil sein, obwohl auch für diesen Problemkreis heute schon andere Lösungen existieren: Die allgemeine Verfügbarkeit des ISDN könnte genutzt werden, um ohne große technische Vorkehrungen Mitarbeitern von zu Hause aus mit Mitteln der Datenkommunikation Zugriff auf die Ressourcen der KFA zu verschaffen.
Die Einsetzbarkeit von ISDN für die Datenkommunikation wird vorbehaltlos geprüft werden, sobald es verfügbar ist; es ist aber absehbar, daß eine grundlegend neue Situation, die auch neue Grundsatzentscheidungen erfordern wird, erst durch die Verfügbarkeit des Breitband-ISDN entstehen wird.

7.2.3 Infrastruktur

Die in der KFA verfügbare Infrastruktur ist für den bisherigen Ausbau des Ethernet ausreichend und für den geplanten Aufbau von FDDI geeignet. Ein weiterer punktueller Ausbau des bisherigen Glasfasernetzes kann in den kommenden Jahren mit der Verbreitung von FDDI notwendig werden.
Bei den zuletzt realisierten Ausbaustufen des Glasfasernetzes wurden zusätzlich zu den für FDDI benötigten Gradientenfasern auch Monomodefasern mitverlegt. Es ist sicher, daß die nächste Generation von Netzen (grob der Schritt von 100 Mbps auf 1 Gbps) auf Monomodefasern basieren wird, so daß längerfristig eine auf dieser Faser basierende Verkabelung erforderlich sein wird. Weitere Investitionen in Gradientenfasern sollten deshalb nur bei unmittelbarem Bedarf getätigt werden und die Verwendbarkeit von Monomodefasern insbesondere bei Verkabelungen zwischen Gebäuden sorgfältig geprüft werden (der FDDI-Standard ist beispielsweise auf Monomodefasern erweitert worden; die entsprechenden Komponenten sind jedoch deutlich teurer als die für Gradientenfasern).
Schwieriger ist die Prognose im Teilnehmeranschlußbereich, bekannt unter dem Schlagwort *fiber to the desk*, weil dieser Bereich besonders kostensensitiv ist. Technisch wünschenswert wäre die Ausdehnung des Glasfasernetzes (auch Monomode) in alle Büros und ein direkter Anschluß der Endgeräte daran. Weniger die Faserkosten selbst als vielmehr die noch recht hohen Anschlußkosten an eine Glasfaser (insbesondere Monomode) erfordern Zwischenlösungen, die es gestatten, für weniger leistungsfähige und billige Endgeräte die Kosten für einen Glasfaseranschluß auf mehrere Endgeräte umzulegen.

Literatur

[1] Anrath, W., Grallert, R., Loup, L., Meißburger, J., Niederberger, R.:
KFAnet/INTERNET: Hinweise zur Systemkonfiguration von TCP/IP Hosts.
Technische Kurzinformation, KFA-ZAM-TKI-0147, 21.11.1991.

[2] Anrath, W., Grallert, R., Meißburger, J., Niederberger, R. (ZAM);
Stoff, H. (ZEL):
KFAnet DECNET/INTERNET Dienste, Anschlußmöglichkeiten und Voraussetzungen.
Technische Kurzinformation, KFA-ZAM-TKI-0146, 07.11.91.

[3] Anrath, W., Höfler-Thierfeldt, S.,Meißburger, J., Niederberger, R.,
Schumacher, Her. (ZAM);
Heinen, J. (IFF):
KFAnet/INTERNET: Installation und Benutzung von NetNews.
Technische Kurzinformation, KFA-ZAM-TKI-0169, 06.12.91.

[4] Anrath, W., Meißburger, J.:
KFAnet/INTERNET: Zeitsynchronisation.
Technische Kurzinformation, KFA-ZAM-TKI-0173, 01.10.91.

[5] Anrath, W., Meißburger, J.:
KFAnet/INTERNET: Benutzung des KFA Info-Servers (Anonymous FTP).
Technische Kurzinformation, KFA-ZAM-TKI-0179, 03.11.91.

[6] Anrath, W., Meißburger, J., Niederberger, R.:
KFAnet/INTERNET: DECNET/INTERNET-Gateway Benutzung.
Technische Kurzinformation, KFA-ZAM-TKI-0144, 22.10.90.

[7] Anrath, W., Meißburger, J., Niederberger, R.:
KFAnet/INTERNET: DEC-ULTRIX Remote Installation Service, RIS.
Technische Kurzinformation, KFA-ZAM-TKI-0159, 01.10.91.

[8] Anrath, W., Meißburger, J., Niederberger, R., Schoenebeck, F.J.:
KFAnet/INTERNET (TCP/IP) unter VM/XA und MVS/XA.
Technische Kurzinformation, KFA-ZAM-TKI-0137, 13.06.1991.

[9] Anrath, W., Meißburger, J., Niederberger, R., Schoenebeck,F.J.:
KFAnet/INTERNET: Remote Execution, rexec und rexecd.
Technische Kurzinformation, KFA-ZAM-TKI-0153, 25.07.91.

[10] Conrads, D.:
Elektronische Kommunikation 1984 – Eine Übersicht.
Spezielle Berichte der Kernforschungsanlage Jülich, Jül-Spez-295, Januar 1985.

[11] Conrads, D.:
Datenkommunikation – Verfahren-Netze-Dienste.
Vieweg-Verlag, Braunschweig, 2.Aufl., erscheint 1992.

[12] Conrads, D., Moritz, H.E., Mühlstroh, R.:
JOKER – Ein System zur Kopplung von Experimentrechnern verschiedener Fabrikate mit einem zentralen Timesharingrechner.
Berichte der Kernforschungsanlage Jülich, Jül-1004-MA, Jülich, Oktober 1973.

[13] Cracker, D.:
Standard for the format of ARPA Internet text messages.
RFC 822, 1982.

[14] Erwin, D., Homrighausen, H.W., Mertens, B.:
Angebot des ZAM zum kooperativen Computing in der KFA (Workstation-Konzept).
Interner Bericht, KFA-ZAM-IB-9015, Version 1, 27. November 1991.

[15] Harrenstien, K., Stahl, M., Feinler, E.:
DoD Internet Host Table Specification
RFC 952, 1985.

[16] Konzept zur Entwicklung der Elektronischen Kommunikation in der KFA.
Strategiepapier des Zentralinstituts für Angewandte Mathematik (ZAM), September 1985 und September 1987.

[17] Metcalfe, R.M., Boggs, D.R.:
Ethernet: Distributed Packet for Local Computer Networks.
CACM 19, 7 (1976), S. 395–404.

[18] Mittelfristiges Konzept für den Einsatz von Glasfasern in den allgemeinen Kommunikationsnetzen der KFA.
Strategiepapier des Zentralinstituts für Angewandte Mathematik (ZAM), Dezember 1988.

[19] Niederberger, R.:
KFAnet/HYPERNET and its Implementation on MVS.
Proc. SEAS Anniversary Meeting, 25.-29. September 1989, Vol. I, S. 399–418.

[20] Stoff, H.:
KFAnet/DECNET – Prozeduren.
Interner Bericht, KFA-ZEL-IB-501589, November 1989

[21] Theisen, R.:
Sicherheitsuntersuchung TCP/IP-basierender Kommunikationsdienste.
Interner Bericht, KFA-ZAM-IB-9010, Mai 1990.

FORSCHUNGSZENTRUM JÜLICH GmbH

KFA

Jül-2623
Mai 1992
ISSN 0366-0885