Julius-Maximilians-Universität Würzburg
Rechenzentrum

# Das Hochschulnetz der Universität Würzburg

**Konzepte, Dienste, Infrastrukturen, Management**

Chr. Rossa
Dr. H. Plehn

Stand: 11.11.2002

# Inhaltsverzeichnis

# Vorwort

Dieser Bericht dient vorrangig der nachträglichen Untermauerung des „zweiten Bauabschnitts“ zur Einrichtung der hochschulinternen Vernetzung der Universität Würzburg im Rahmen des Netzwerk-Investitionsprogramms NIP. Da dieses Vorhaben sich bereits in der Ausführungsphase befindet, beschreibt der vorliegende Bericht den „Status quo ante“. Er basiert also eigentlich auf dem Zeitpunkt der Antragsphase, d.h. zwischen Frühjahr 1999 und Herbst 2000. Darüber hinaus soll das Netzkonzept bzw. der Netzentwicklungsplan aber stets die aktuellen Entwicklungen widerspiegeln.

Das bedeutet, dass einerseits die Argumentation aus dieser Sicht erfolgen muss, andererseits es aber notwendig ist, auch die weiteren Entwicklungen mit einfließen zu lassen.

Zum Teil lassen sich manche Angaben aus Sicht des damaligen Zeitpunkts nicht mehr ermitteln. Die zeitliche Argumentationslinie ist also nicht immer konsistent. Wenn angebracht, erfolgt die Argumentation aus heutiger Sicht.

Die Gliederung des Berichts richtet sich grob nach dem Netzkonzept / Netzentwicklungsplan des Leibniz-Rechenzentrums München, angepasst an Besonderheiten der Universität Würzburg.

# 1 Grundsätze

Das Hochschulnetz der Universität Würzburg ist als flächendeckende zentrale Infrastruktur kontinuierlich auf dem jeweils aktuellen Stand der Technik zu halten. Jeder Mitarbeiter und jeder Studierende der an diesem Netz angeschlossenen Institutionen soll an seinem Arbeitsplatz und bei Bedarf auch zu Hause oder unterwegs komfortablen und uneingeschränkten Zugang zu allen Netzdiensten haben, die er für seine Arbeit in Forschung, Lehre und Studium benötigt. Das Netz vermittelt den Zugang zu Servern bzw. zu Netzdiensten innerhalb der Hochschule, zu nationalen und internationalen Wissenschaftsnetzen und zum allgemeinen Internet.
Für die Erstellung und Fortschreibung des Netzkonzeptes ist das Rechenzentrum der Universität zuständig. Bei Planung und Ausbau des Hochschulnetzes wirken das Rechenzentrum, das zuständige Bauamt und die Einrichtungen der Universität eng zusammen. Für den Betrieb des Hochschulnetzes ist ebenfalls das Rechenzentrum zuständig, wobei es von den Netzverantwortlichen der Fachbereiche unterstützt wird.
An den Backbone des Hochschulnetzes der Universität Würzburg sind neben den Einrichtungen der Universität auf der Grundlage eines Versorgungsauftrags auch die Einrichtungen der Fachhochschule Würzburg-Schweinfurt, Abteilung Würzburg, sowie der Hochschule für Musik Würzburg angeschlossen.

# 2 Bedarfsbegründende Grunddaten

Der Kommunikationsbedarf der Universität Würzburg lässt sich grundsätzlich aus den Basisdaten ableiten.

## 2.1 Allgemeine Angaben zur Universität Würzburg

Die Universität Würzburg ist eine Flächenuniversität mit insgesamt 68 Gebäuden / Gebäudekomplexen, die über 4 Campusbereiche sowie Einzelgebäude verteilt sind. Hinzu kommt die Ökologische Außenstation Fabrikschleichach.

**Fakultäten**

Katholisch-Theologische Fakultät
Juristische Fakultät
Medizinische Fakultät
Philosophische Fakultät I (Altertums- und Kulturwissenschaften)
Philosophische Fakultät II (Neuphilologen, Geschichte, Kunstgeschichte)
Philosophische Fakultät III (Philosophie, Erziehungs- und Gesellschaftswissenschaften)
Fakultät für Biologie
Fakultät für Chemie und Pharmazie
Fakultät für Geowissenschaften
Fakultät für Mathematik und Informatik
Fakultät für Physik und Astronomie
Wirtschaftswissenschaftliche Fakultät

**Studierende (im SS 2002)**

ca. 16.600 Studierende

**Personal (inkl. Kliniken) (Stand 09.2002)**

ca. 10.000 Mitarbeiter, davon ca. 3.200 wissenschaftliches Personal

**Räume (ohne Kliniken) (Stand 01.1999)**

Rund 5.500 Räume auf 188.000 qm Hauptnutzfläche, davon haben z. Z. rund 3.000 Räume einen oder mehrere Netzanschlüsse.

## 2.2 Standorte

Die Universität Würzburg umfasst eine große Anzahl von Standorten, die über die Stadt Würzburg verteilt sind. Die Ökologische Außenstation Fabrikschleichach befindet sich rund 80 km von Würzburg entfernt.

Derzeit sind an das Hochschulnetz allein 16 Standorte der Universität mit insgesamt 68 Gebäuden angebunden (siehe Abb. 1 und Abb. 2; die Zuordnungen von Nummern zu Gebäuden/Fachbereichen sind der Tabelle 1 zu entnehmen). Die Größe der zu versorgenden Standorte ist sehr unterschiedlich; sie reicht von einem einzelnen Gebäude bis zu einem Campusbereich. Als Standort wird ein topologisch abgegrenzter und über Punkt-zu-Punkt-Verbindungen an das Backbone angeschlossener Bereich mit einem oder mehreren LANs interpretiert.

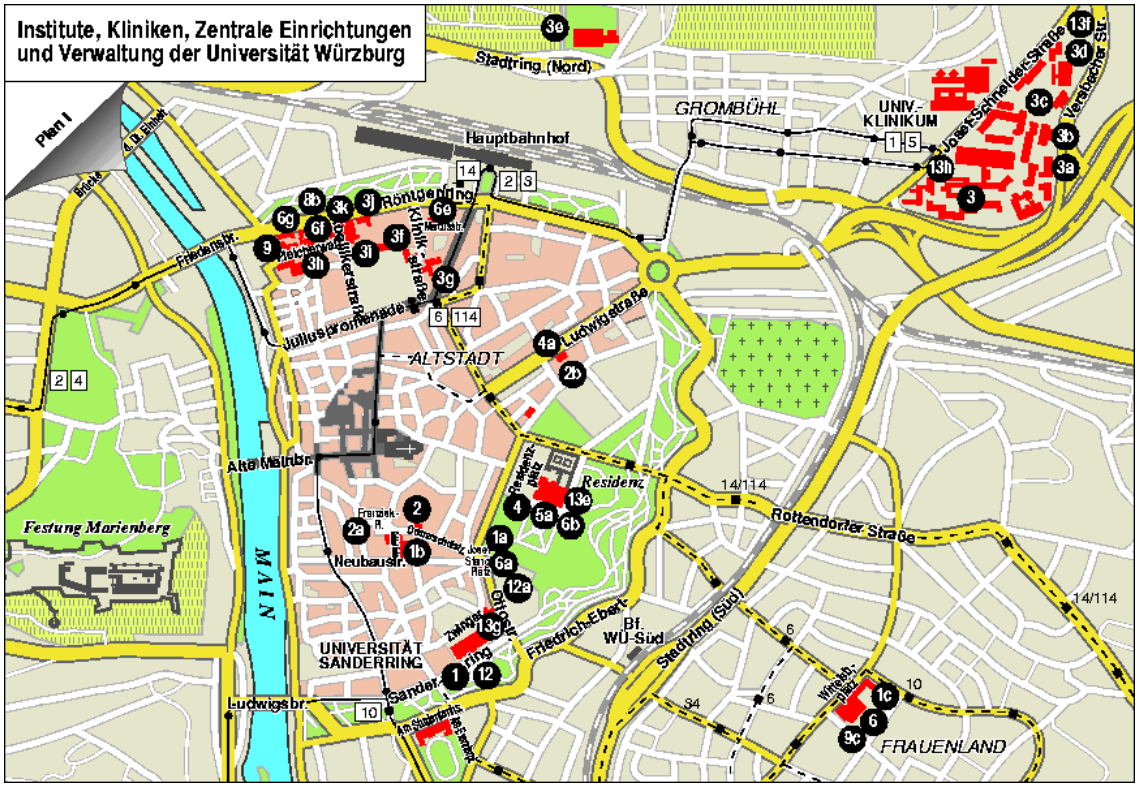


**Abb. 1**: Lageplan Nord mit Campusbereichen Sanderring, Röntgenring und Kliniken

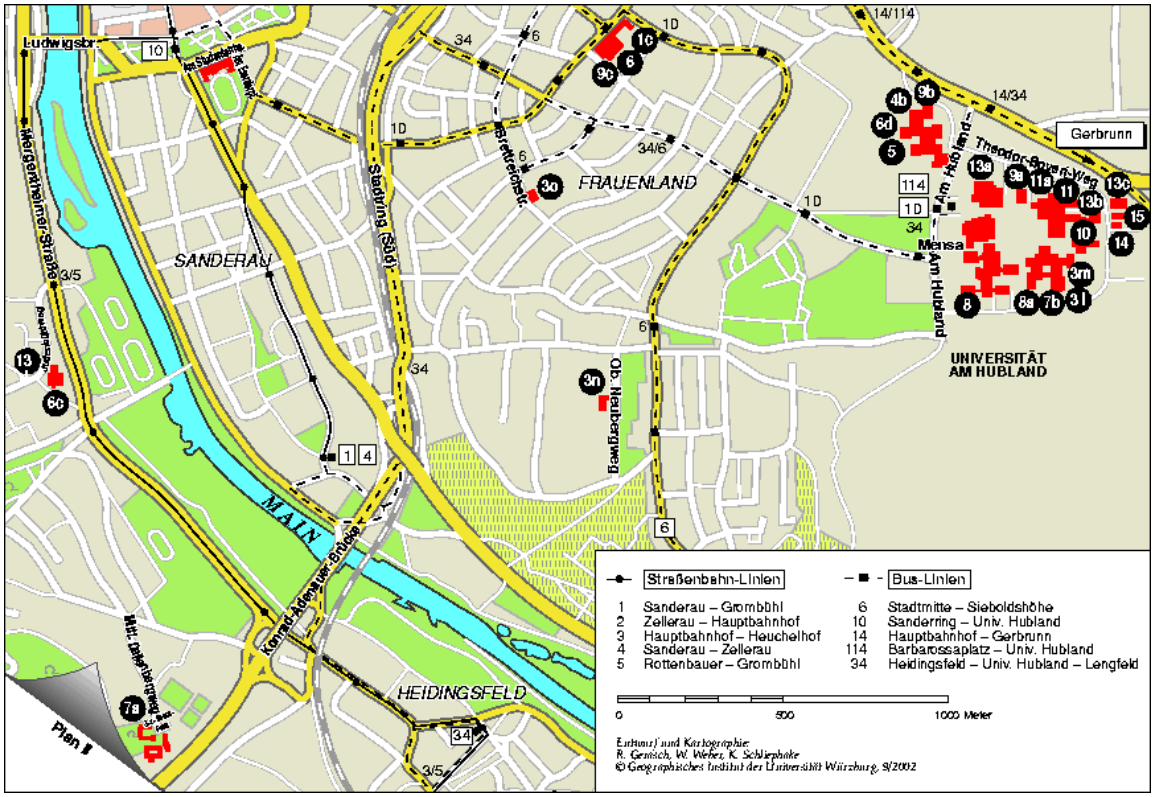


**Abb. 2**: Lageplan Süd mit Campusbereich Hubland

Das Hochschulnetz der Universität Würzburg setzt sich zusammen aus dem Lehre- & Forschungsnetz, dem Verwaltungsnetz, dem Medizinischen Versorgungsnetz und dem Außenzugangsnetz (Wählzugänge, Funknetze, Studentenwohnheime).
Die Zentralverwaltung der Universität, der Fachbereich Medizin, die Träger der Studentenwohnheime sowie die Fachhochschule und die Hochschule für Musik betreiben die in ihren Bereichen gelegenen Netzstrukturen selbst. Dies ist begründet in den geänderten Anforderungen an Verwaltungs- und Medizinnetze sowie den Zuständigkeiten.
Der Anschluss an das Wissenschaftsnetz G-WiN sowie DFN-ATM wird jedoch gemeinsam genutzt.

## 2.3 Mengengerüst Netznutzung

**Nutzungsberechtigte**

Alle Mitglieder und Angehörigen der Universität Würzburg sowie der angeschlossenen Einrichtungen sind berechtigt das Hochschulnetz zu nutzen.

**Eingetragene Nutzer**

Derzeit sind am Rechenzentrum rund 13.500 Nutzer (Stand Juli 2002) eingetragen, davon 4.500 Nutzer von Lehrstühlen und Instituten (Angehörige des wissenschaftlichen und nichtwissenschaftlichen Personals und Studenten höherer Semester) und ca. 9.000 Studierende der Würzburger Hochschulen. Hinzu kommen noch Benutzer, die derzeit noch von den einzelnen Einrichtungen der Universität sowie der Fachhochschule und der Hochschule für Musik selbst verwaltet werden.

**Arbeitsplatzrechner**
Allein im Bereich Lehre & Forschung sind etwa 6.500 Endgeräte zu versorgen. Davon werden etwa 10% als Server eingesetzt.

**Netzdienste**
Charakteristische Daten für die wichtigsten Netzdienste (Stand Juli 2002):

- Durchsatz G-WiN ca. 3.500 GB/ Monat (empfangene Daten)
- Etwa 40.000 E-Mails pro Tag über das Mail-Relay des Rechenzentrums
- Etwa 3.000 Wählverbindungen pro Tag über die Wählzugänge.

# 3 Netzdienste

## 3.1 Stand der Netzdienste (Juli 2002)

### 3.1.1 Standarddienste

Die vom Rechenzentrum betriebenen Dienste (WWW, E-Mail, FTP, News usw.) stehen allen Berechtigten auf der Basis von Servern und systemnahen Diensten (DNS, NTP, DHCP u. a.) zur Verfügung. Es werden jedoch auch von einigen Institutionen selbst solche Dienste betrieben.
Flächendeckend werden derzeit als Protokoll TCP/IP und IPX eingesetzt. IPX wird vermutlich ab 2004 aus Aufwandsgründen nicht mehr im Backbone unterstützt. Andere Protokolle werden nur nach Absprache lokal innerhalb eines Subnetzes zugelassen.

### 3.1.2 Backup und Archiv

Das Rechenzentrum betreibt einen zentralen Archivierungsdienst mit einer maximalen Kapazität von 9 TB. Die zentralen Novell-Server, die ca. 2.000 Arbeitsplatzrechner versorgen, werden über ein zentrales Backup regelmäßig gesichert. Derzeit wird vom Rechenzentrum ein zentrales Backup-Konzept für Unix- und Novell-Server erarbeitet.

### 3.1.3 Multicast

Multicastfähigkeit ist nur im eingeschränkten Umfang im Hochschulnetz verfügbar, da das Multicast-Protokoll nicht von allen in Betrieb befindlichen Netzwerkkomponenten in erforderlichem Umfang unterstützt wird.

### 3.1.4 ATM & Multimedia

Vorlesungsübertragungen werden bereits seit einigen Jahren praktiziert. Derzeit werden folgende Veranstaltungsreihen über Kommunikationsnetze in multimedial ausgestattete Hörsäle, Seminar- bzw. Büroräume übertragen:

- Wirtschaftsinformatik (Kooperation mit Universität Erlangen-Nürnberg),
- Bioinformatik (Kooperation mit den Universitäten Bayreuth und Erlangen-Nürnberg),
- Telekonferenz der Bayerischen RZ-Leiter,
- Wirtschaftswissenschaften (hochschulintern).

Nach anfänglichen Versuchen über MBone werden seit Mitte 2001 die Vorlesungsübertragungen

über ATM abgewickelt, das grundsätzlich in allen Gebäuden verfügbar ist. Die Entwicklung von Codecs auf IP-Basis wird interessiert beobachtet. Eine mögliche Migration muss mit den Kooperationspartnern abgestimmt werden.

In den Jahren 2001 und 2002 wurden mit Mitteln der Universität und über ein Sonderprogramm des Ministeriums folgende Hörsäle multimedial ausgestattet:

- Hubland, Informatik, Zuse-Hörsaal,
- Sanderring, Neue Universität, Auditorium Maximum,
- Sanderring, Neue Universität, Hörsaal 166,
- Röntgenring, Anatomie, Hörsaal,
- Klinik, Virologie, Hörsaal.

Darüber hinaus verfügen etwa 20 weitere Hörsäle und Seminarräume über eine präsentationsorientierte Multimedia-Infrastruktur.

## 3.2 Entwicklung des Dienst-Spektrums

Vor der Würdigung einzelner Dienste wird kurz auf die wesentlichen Qualitätskriterien eingegangen, die für jeden Dienst zu berücksichtigen sind.

### 3.2.1 Kriterien

- Verkehr
  Hohe Verkehrslasten bzw. hohe Lastspitzen können auch im best-effort Bereich nur mit „genügend“ hoher Summen-Bandbreite abgefangen werden.
- QoS/CoS
  Unter QoS („Quality of Service“) werden die engeren Parameter wie Delay und Jitter mit absoluten Grenzwerten verstanden. CoS („Class of Service“) stellt mit relativen Prioritäten eine Annäherung an QoS dar, die für manche Anwendungen ausreicht.
- Verfügbarkeit
  Unter Verfügbarkeit wird im engeren Sinne die Vermeidung von Ausfällen verstanden.
- Sicherheit
  Unter Sicherheit wird der Schutz vor unbefugtem Zugriff auf Netze und Datenbestände verstanden.

Zu den netztechnischen Qualitätskriterien kommen natürlich Forderungen nach einem grundsätzlichen Ausbau (Erweiterung, zusätzliche Bandbreite) hinzu.

### 3.2.2 Dienste-Spektrum

Die im Hochschulnetz der Universität Würzburg angebotenen Dienste werden einzeln anhand obiger Kriterien näher betrachtet.

#### 3.2.2.1 Standarddienste

Zur zukunftssicheren Abwicklung der Standarddienste (WWW, E-Mail, FTP, News usw.) muss das jeweils anstehende Verkehrsvolumen bewältigt werden, d.h. es muss genügend Bandbreite vorhanden sein. Im Backbone sollten überall Bandbreiten von 1 Gbit/s mit Ausbauoption auf 10 Gbit/s verfügbar sein, im Subnetzbereich in der Regel 100 Mbit/s und schwerpunktmäßig auch 1 Gbit/s (z.B. für Server).

#### 3.2.2.2 Daten- und Speicherverwaltung

Bei der Daten- und Speicherverwaltung ist darauf zu achten, dass im Hochschulnetz ausreichende Bandbreite zum Transport der Daten zur Verfügung steht und eine hohe Sicherheit zum Schutz der Bestände gewährleistet ist. Es soll das Ziel verfolgt werden, auf den Arbeitsplatzrechnern eine getrennte Administration von Daten (auf Fileservern) und Programmen (Applikationserver bzw. Arbeitsplatzrechner) zu erreichen.

#### 3.2.2.3 Verzeichnisdienste

Der Zugriff auf zentrale Verzeichnisdienste (z.B. NDS, DNS) erfordert neben ausreichender Bandbreite für Lastspitzen auch eine hohe Verfügbarkeit. Die im Einsatz befindlichen Verzeichnisdienste sollen auf der Basis eines übergreifenden LDAP-basierten Verzeichnisdienstes zusammengeführt werden.

#### 3.2.2.4 Multicast, IP-Telefonie, Videokonferenzdienste, Videoübertragungen

Die multimediabasierten Dienste stellen die insgesamt umfassendsten Ansprüche an das Kommunikationsnetz. Grundsätzlich muss aber festgestellt werden, dass es derzeit noch an vielen Stellen an der geeigneten Infrastruktur für multimediale Anwendungen mangelt.

- Die *Multicast-Verteildienste* erfordern ausreichende Bandbreite, sowie leistungsfähige Router und Switches, die diese Verteildienste auch interoperabel unterstützen. Bei zukünftig zu beschaffenden Komponenten muss darauf geachtet werden.
- Die *IP-Telefonie* setzt eine Mindest-Dienstqualität und eine hohe Verfügbarkeit voraus, wenn sie als Dienst zukünftig eine ernstzunehmende Rolle spielen soll.
- *Videokonferenzdienste* stellen sehr hohe Anforderungen an Bandbreite, Firewall-Konfigurationen und Verfügbarkeit. Ob CoS zum Einsatz kommen kann, wird möglicherweise vom DFN-Verein im Rahmen der Einführung des DFN-Videokonferenzdienstes geprüft.
- Vorlesungsübertragungen stellen die am weitesten verbreitete Form der *Videoübertragung* dar. Sie werden nur dann akzeptiert, wenn sie nahezu TV-Qualität haben. Das bedeutet neben einer hohen Bandbreite und einer hohen Verfügbarkeit insbesondere verlässliche QoS.

### 3.2.3 Folgerungen

Aus den Anforderungskriterien für die oben genannten Dienste ergeben sich folgende Schlussfolgerungen für die zukünftige Entwicklung der Datennetze:

- Verkehr:
  Naturgemäß muss von einem kontinuierlich steigenden Verkehrsaufkommen ausgegangen werden, auch wenn der Anstieg sich seit etwa 2 Jahren verlangsamt hat. Die jährlichen Steigerungsraten liegen derzeit ausnahmslos unter dem Faktor 2. Zur Verkehrsentwicklung innerhalb des Hochschulnetzes werden an neuralgischen Stellen Messungen durchgeführt und durch (Router-)Statistiken mit Hilfe von MRTG ausgewertet. Aus den auf dieser Basis erstellten Jahresstatistiken kann durchaus eine deutliche Steigerung abgelesen werden.
- Dilemma QoS / CoS:
  Für Dienstqualität auf IP-Basis ist genügend Bandbreite notwendig, aber nicht hinreichend. Eine noch vor wenigen Jahren als ausreichend betrachtete Überbuchung (Over-

subscription) der Bandbreite reicht offensichtlich nicht aus. Eine Einführung von QoS / CoS stellt tief greifende Forderungen an die aktiven Netzkomponenten und an deren einheitliche Konfigurierung sowohl im eigenen Netz als auch bei Providern und bei Netzübergängen. Regelungen im eigenen Netz müssten mit denen im Wissenschaftsnetz und in Netzen Dritter abgestimmt werden.

  - CoS / IP:
    Da hier demnächst nicht mit praktischen Fortschritten zu rechnen ist, hat der DFN-Verein die Einführung von CoS bis auf weiteres verschoben. Was bleibt, ist die Forderung nach „ausreichender Bandbreite“. Exemplarische Versuche sollen anhand des DFN-Videokonferenzdienstes unternommen werden.
  - QoS / ATM:
    ATM erlaubt eine Garantie von QoS je Service. Es wird, soweit nötig, weiter betrieben und bei Bedarf auch punktuell ausgebaut.

- Verfügbarkeit:
  Zur Sicherung einer hohen Verfügbarkeit wird eine weitgehende Redundanz im gesamten Backbonenetz – sowohl auf der passiven als auch auf der aktiven Ebene – angestrebt. Dazu zählen auch die Gebäudezuführungen. Erforderlich ist ebenfalls eine Absicherung der aktiven Komponenten durch Notstrom und USV-Anlagen.
  Eine höhere Verfügbarkeit kann auch durch Steigerung der Qualität des Netzmanagements (z.B. Einsatz von Monitoring-, Steuerungs- und Reporting Tools) erreicht werden. Die Einrichtung einer Rufbereitschaft außerhalb der Dienstzeiten ist aus personellen Gründen derzeit nicht realisierbar.
- Sicherheit:
  Die Nutzer im Netzbereich der Universität Würzburg verfügen an vielen Stellen über hochsensible, schützenswerte Daten (Personaldaten, Patientendaten, Forschungsergebnisse). Für deren Schutz ist „die Universität Würzburg“ verantwortlich. Neben dem Schaffen und Fördern eines Sicherheitsbewusstseins, der qualifizierten und kompetenten Betreuung der IT-Systeme und der Einführung organisatorischer Sicherheitsmaßnahmen sind technische Vorkehrungen unumgänglich. Die Entscheidung für den Einsatz eines Firewall-System muss von der ganzen Universität getragen werden. Die Planung, Umsetzung und der Betrieb eines solchen Firewall-Systems ist sehr personalaufwändig.

# 4 Netzstruktur

Das Hochschulnetz der Universität Würzburg setzt sich aus einem Backbonenetz (Stadtnetz und vier Campusnetze) und den einzelnen Gebäudenetzen zusammen. Das Backbonenetz verbindet die Gebäude der Universität, einschließlich der Gebäude im medizinischen Versorgungsbereich, miteinander und bietet Anschlusspunkte für die Einrichtungen der Fachhochschule und der Hochschule für Musik.
Zunächst wird der aktuelle Ausbaustand und danach der derzeitige Planungsstand des Hochschulnetzes aufgezeigt. Dabei werden die passiven und die aktiven Netzstrukturen sowie die Außenzugänge getrennt beschrieben.

## 4.1 Aktueller Stand (Juli 2002)

### 4.1.1 Passives Netz

Das Stadtnetz verbindet die einzelnen (Sub-)Netze der vier Campusbereiche und der Einzelgebäude miteinander. Es basiert auf „dark-fiber"-Leitungen (Monomode-Lichtwellenleiter), die langfristig (10 Jahre) von der Telekom und wücom/Arcor (siehe Abb. 3) angemietet sind. Im Zentrum des Stadtnetzes befindet sich ein eng vermaschtes Viereck der zentralen Punkte der 4 Campusbereiche. Die einzelnen Gebäude bzw. Gebäudekomplexe sind sternförmig an einen der Campusaufpunkte angeschlossen. Derzeit werden im Stadtbereich 8 Verbindungsstrecken von der Telekom und 18 von wücom/Arcor zum Aufbau des Backbonenetzes genutzt. Redundante Leitungen mit getrennten Wegeführungen von den Campusaufpunkten zu den Gebäuden sind aus Kostengründen nicht realisiert. Jedoch sind LWL-Reservefasern auf allen Verbindungsstrecken im Stadtnetz in den gleichen LWL-Bündeln vorhanden.

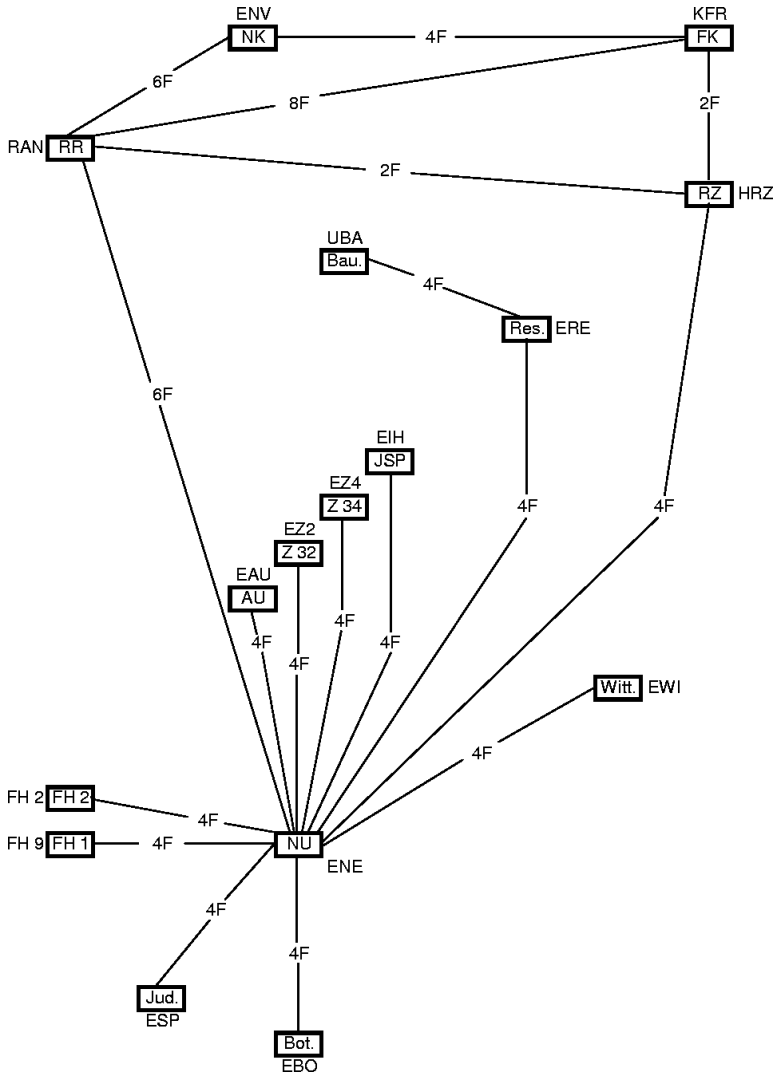


**Abb. 3**: Dark-Fiber-Netz im Backbone

In den einzelnen Campusbereichen sind die anzubindenden Gebäude in der Regel ebenfalls sternförmig an den jeweiligen Campusaufpunkt angebunden. Die physikalische Struktur der Campusnetze ist stern- bzw. ringförmig. Hierzu wurden im Rahmen des Netz-Investitions-Programms (NIP I) 12, 20 bzw. 24 Monomode-Fasern Lichtwellenleiter (LWL) verlegt. Redundanz der Anbindung ist teilweise über eine Vermaschung einzelner Gebäude technisch möglich, wird derzeit aber nur vereinzelt genutzt.

Bei der gebäudeinternen Verkabelung gibt es derzeit noch Defizite in der Realisierung einer flächendeckenden, strukturierten Verkabelung. Der Versorgungsbereich des Rechenzentrums (ohne Kliniknetz) umfasst ca. 5.500 Räume. Im Rahmen von NIP I wurde versucht, eine möglichst hohe Versorgungsdichte zu erreichen und die bereits vorhandenen Netzinseln zu integrieren. Dabei wurde eine bedarfsorientierte, gleichmäßige Versorgung aller Fachbereiche angestrebt. So konnte aus Kostengründen überwiegend lediglich eine „Cheapernet-Verkabelung“ (10Base2) realisiert werden. Dabei wurde das Verkabelungskonzept entscheidend durch die Bausubstanz (relativ großer Anteil alter Gebäude, teilweise unter Denkmalschutz stehend), die Raumknappheit (keine Etagenverteilerräume) und die meistens unzureichende Infrastruktur geprägt. So wurde in der Vertikalen (Sekundärbereich) grundsätzlich Lichtwellenleiter (LWL) mit 20 - 30 Fasern und in der Horizontalen (Tertiärbereich) überwiegend Koaxkabel und nur in Ausnahmefällen LWL-Kabel bis in die Arbeitsräume installiert. Lediglich bei Neubauten und auch in der Endphase von NIP I wurde bereits strukturiert mit Lichtwellenleitern verkabelt. Derzeit sind rund 3.000 Räume im Versorgungsbereich des Rechenzentrums mit mindestens einem Netzanschluss ausgestattet.

Das aktuelle Vernetzungskonzept für die Universität Würzburg trägt den in NIP I gesammelten Erfahrungen und dem höherer Bedarf nach einem strukturierten Datennetz Rechnung. Das überarbeitete Konzept berücksichtigt den gestiegenen und weiter steigenden Bandbreitenbedarf und die höheren Anforderungen an die Sicherheit von Netzverbindungen. Da auf Grund fehlender Etagenverteilerräume eine strukturierte TP-Verkabelung lediglich bei wenigen kleineren Gebäuden möglich wäre, wird aus Gründen der Einheitlichkeit grundsätzlich der strukturierten LWL-Verkabelung der Vorzug gegeben. Dabei wird das Fibre-To-The-Office-Konzept (FTTO) als Zwischenschritt zum Fibre-To-The-Desk-Konzept (FTTD) gesehen. Bei der reinen Verkabelung unterscheiden sich die beiden Konzepte FTTO und FTTD nicht, wohl aber auf der aktiven Seite. Beim FTTO-Konzept wird normalerweise eine einzige LWL-Verbindung für die Versorgung eines Arbeitsraumes genutzt. Dabei werden über einen Umsetzer mehrere TP-Schnittstellen in dem Arbeitsraum zur Verfügung gestellt.
Die wesentlichen Vorteile des FTTO-Konzeptes sind:

- zukunftssichere Verkabelung bis zum Arbeitsplatz,
- Konzentration der Verteilung und der aktiven Komponenten auf einen einzigen zentralen Raum,
- Flexibilität der Anschlusstechnik,
- geringere Anzahl von Ports an den zentralen aktiven Komponenten in der Anfangsphase und dynamische Erweiterungsmöglichkeiten,
- geringere Kosten für die Anbindung von Endgeräten.

Im Rahmen der Phase II des Netz-Investitions-Programms (NIP II), das auf der Basis des aktuellen Vernetzungskonzeptes realisiert wird, wurde im Frühjahr 2002 damit begonnen, die Vernetzungslücken zu schließen und eine „Sanierung“ der koax-basierten Vernetzung durchzuführen.

Ziel ist es, in den nächsten Jahren nach und nach alle Gebäude der Universität mit einer strukturierten LWL-Verkabelung auszustatten.

Die bestehende und die im Rahmen von NIP II umgesetzte Verkabelungsstruktur des Hochschulnetzes lässt sich somit folgendermaßen schematisch darstellen:

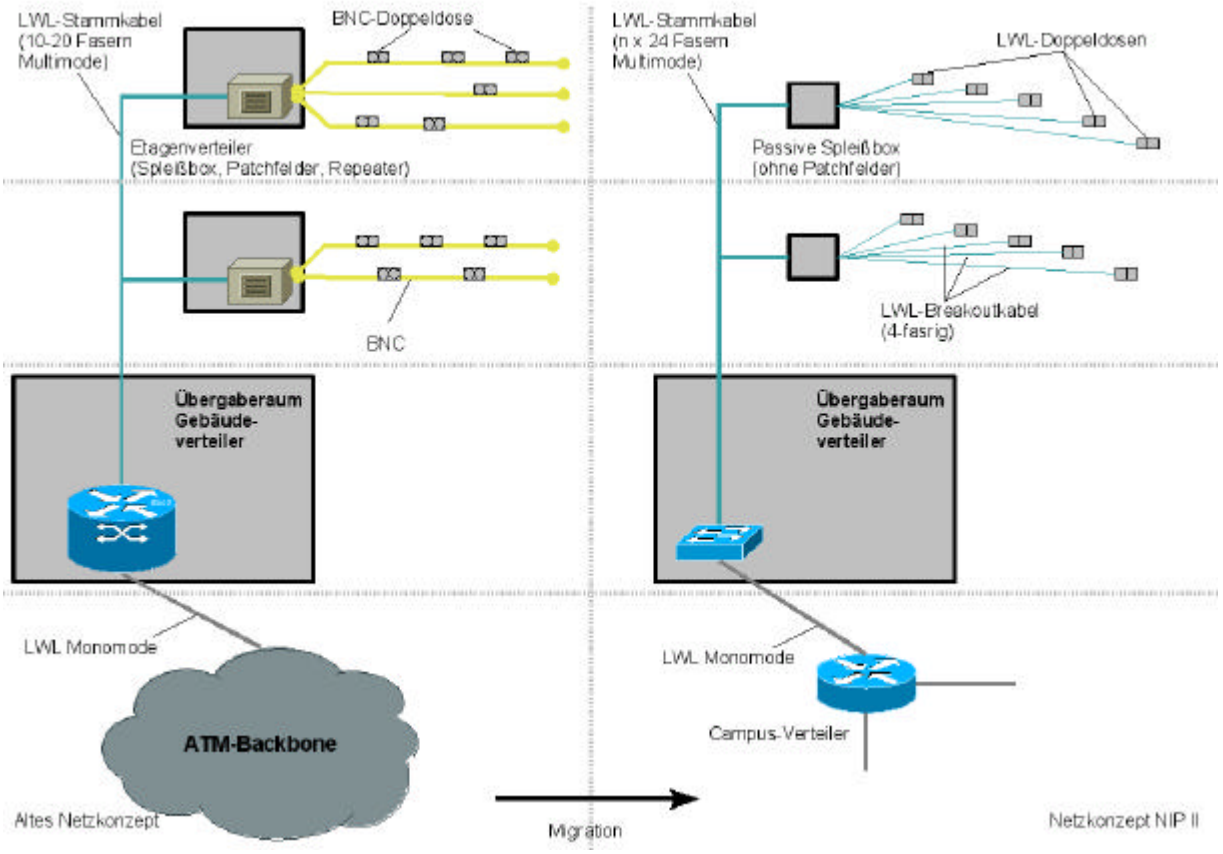


**Abb. 4**: Schematische Darstellung des Migrationskonzepts der passiven Verkabelungsstruktur

### 4.1.2 Aktives Netz und Netzstrukturierung

Auf der oben beschriebenen passiven Infrastruktur wird das Hochschulnetz betrieben. Es besteht im Wesentlichen aus einem aktiven Backbonenetz, an dem über Router die einzelnen Gebäudenetze an den verschiedenen Standorten angeschlossen sind. Die Router sind untereinander größtenteils mit ATM (in der Regel 622 Mbit/s) und zunehmend mit Ethernet (100 Mbit/s oder 1 Gbit/s) verbunden. Die Bandbreite der Anschlüsse an das Backbone richtet sich nach dem transferierten Datenvolumen und der Größe des jeweiligen Standortes (Anzahl angeschlossener Endgeräte). Sie wird aufgrund der Auslastungsdaten des Netzmanagementsystems sowie in Absprache mit den Nutzern bei Bedarf angepasst.

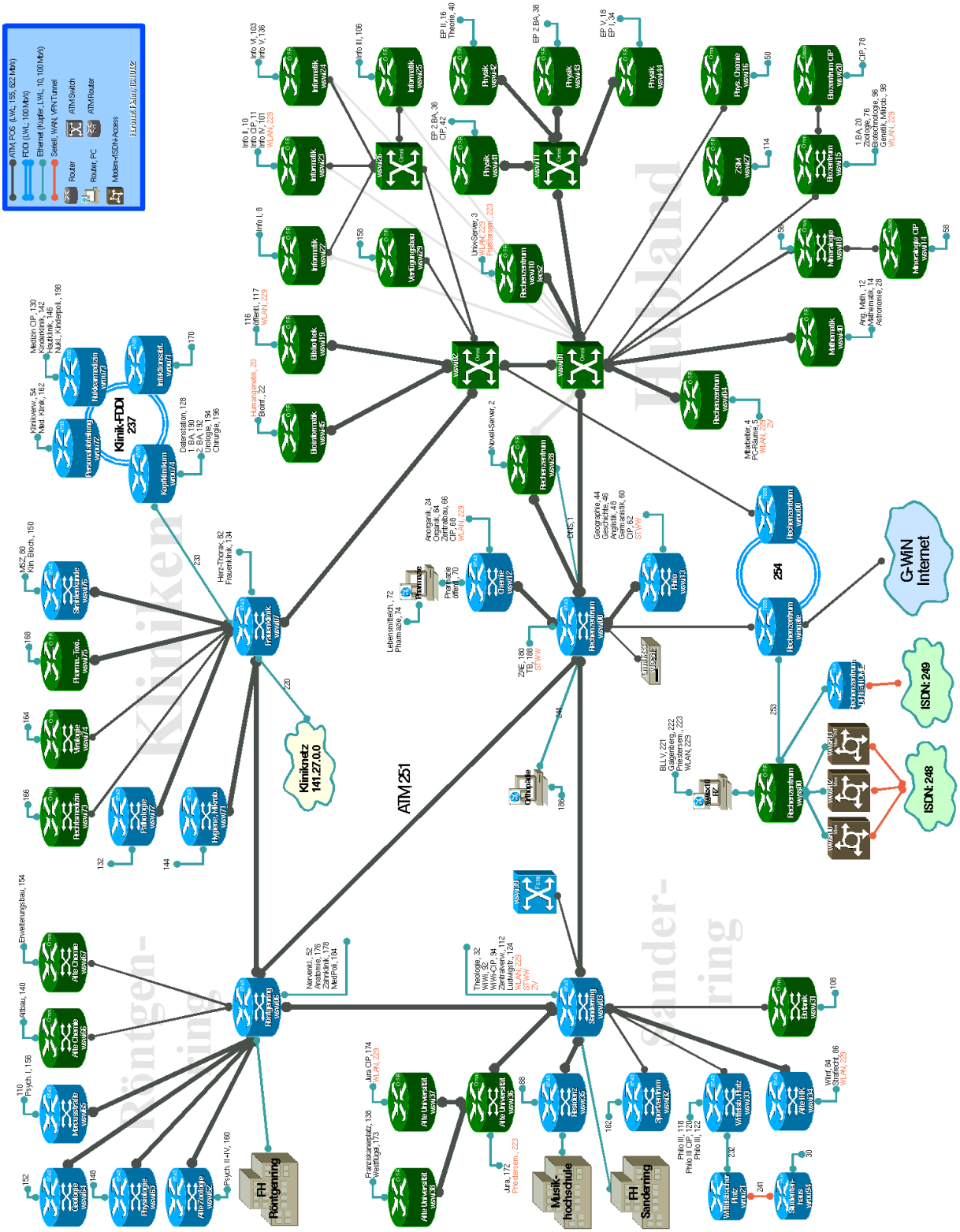


**Abb. 5**: Backbone des Hochschulnetzes

An den Routern sind die einzelnen Instituts- bzw. Gebäude-LANs angebunden. Derzeit sind gebäudeseitig etwa 100 lokale Routerinterfaces konfiguriert. Abhängig von der verfügbaren Verkabelungsinfrastruktur wird mittels Switches entweder

- ein komplett geswitchtes Netz bis zum Endgerät, Anschlussgeschwindigkeit entweder 100 Mbit/s oder gelegentlich 1 Gbit/s bei Servern realisiert, wenn das Gebäude strukturiert verkabelt ist, oder aber
- es werden die einzelnen Koax-Segmente über Etagen-Multiportrepeater oder direkt auf einen zentralen Gebäude-Switch geführt. Server werden bei Bedarf evtl. dediziert mit 100 Mbit/s angeschlossen.

In der Abb. 6 soll die Realisierung der aktiven Netzstruktur schematisch veranschaulicht werden. Derzeit sind

- 4 ATM-Switches der Fa. Alcatel (wswi01, wswi02, wswi11, wswi26),
- 4 Core-Switches der Firma Cisco (wswi00, wswi03, wswi06, wswi07),
- 22 Switch-Router der Firma Alcatel,
- 13 Switch-Router der Firma Cisco,
- 15 Omni-Switches der Firma Alcatel,
- 45 LAN-Switches der Firmen HP, Allied Telesyn, Alcatel, D-Link,
- 162 Repeater der Firma Allied Telesyn

im Einsatz. Aus Gründen der Interoperabilität und des Supports (Management, Konfiguration, Logistik) wird versucht, die Gerätevielfalt möglichst gering zu halten (d.h. für einzelne Aufgaben nur Geräte weniger Hersteller bzw. einen bestimmten Gerätetyp einzusetzen).

Zur Verbindung der einzelnen Standorte des Hochschulnetzes werden 4 Core-Switches (Cisco Catalyst 8540) eingesetzt.
Bei den größeren Arealen werden zur Anbindung Router des Typs Cisco 8540 bzw. SwitchRouter der Fa. Alcatel eingesetzt. Diese Geräte unterstützen alle gängigen Medien und Technologien. In der Regel verfügen sie neben ATM- auch über Fast- und Gigabit-Ethernet-Schnittstellen.
Im Gebäudebereich kommen LAN-Switches der Firmen HP, Allied Telesyn, Alcatel und D-Link zum Einsatz. Diese Geräte unterstützen Ethernet-, Fast-Ethernet- und teilweise auch Gigabit-Ethernet-Infrastrukturen.

Im Hochschulnetz werden zum Anschluss von Gebäudenetzen derzeit die folgenden Netztechnologien unterstützt

- ATM
- Ethernet
- Fast-Ethernet
- Gigabit-Ethernet

Im Backbonebereich ist derzeit ATM am stärksten vertreten. Eine Migration zu Gigabit-Ethernet wird vorbereitet. ATM-Anschlüsse sollen bei Bedarf auch in Zukunft an ausgewählten Standorten vorhanden sein.

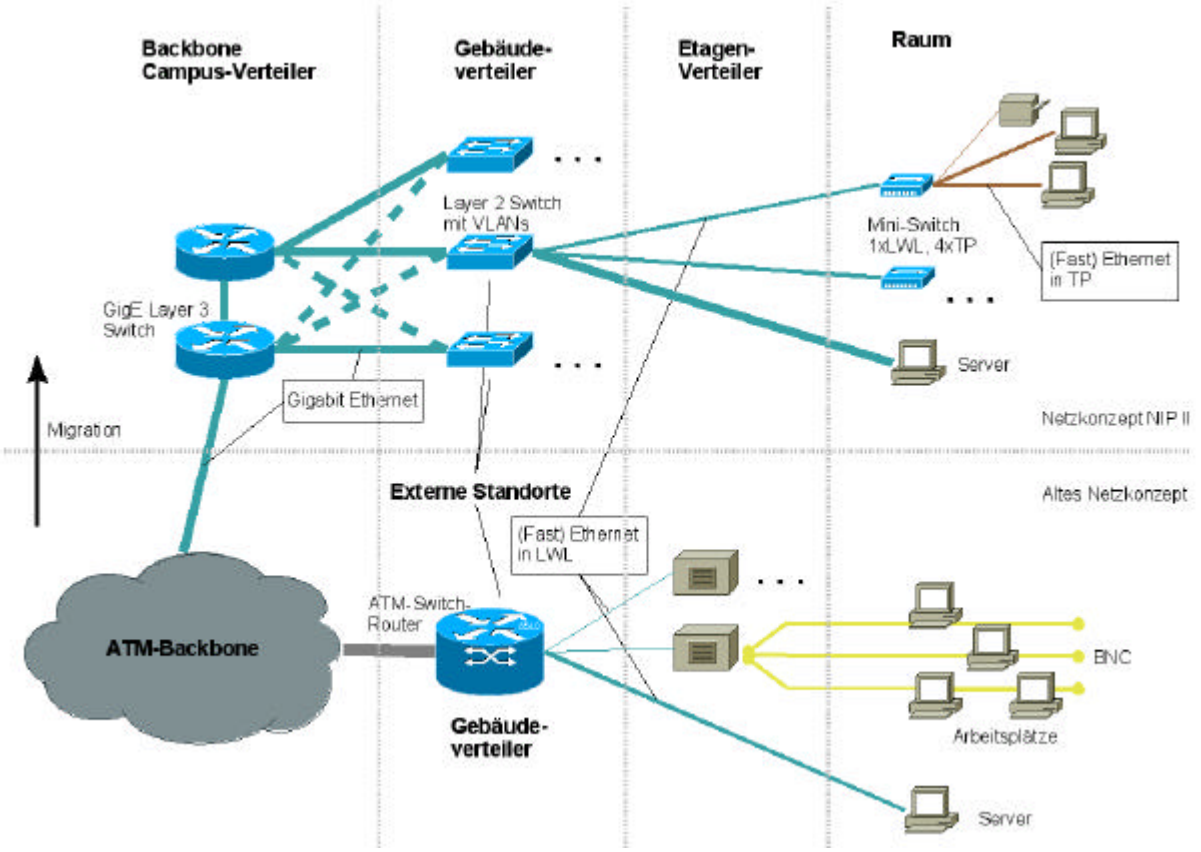


**Abb. 6**: Schematische Darstellung des Migrationskonzeptes für aktive Komponenten

### 4.1.3 WDM-Systeme

Derzeit werden keine WDM-Systeme im Hochschulnetz der Universität Würzburg eingesetzt.

### 4.1.4 Zugänge von außerhalb

Das Rechenzentrum stellt derzeit 240 parallele Einwahlzugänge aus dem öffentlichen und 30 aus dem universitätsinternen Telefonnetz auf 3 Ascend-Einwahlservern zur Verfügung. In Rahmen von Uni@Home wurde einer dieser Einwahlserver von der Deutschen Telekom bereitgestellt. Zudem können sich Nutzer deutschlandweit über DFN@home kostengünstig und mit universitätsinternen IP-Adressen ins Hochschulnetz einwählen. Für den Zugang zum Hochschulnetz über andere Provider soll ein VPN-Server eingerichtet werden. Die Authentifizierung geschieht derzeit über einen Verbund von Radius-Servern.

### 4.1.5 Zugang für mobile Endgeräte

Für den Anschluss von mobilen Endgeräten stehen derzeit im gesamten Hochschulnetz 36 Access-Points und zusätzlich im Rechenzentrum vorkonfigurierte Datendosen zur Verfügung.
Der Zugang zum Hochschulnetz über diese Anschlusstechniken ist mit derselben Benutzerkennung möglich, mit der auch die Wählzugänge genutzt werden können. Die Authentifizierung geschieht über einen speziellen Authentifizierungs-Server auf Firewall-Basis. Dazu werden die Access-Points und die vordefinierten Datensteckdosen in ein eigenes VLAN eingebunden. Von diesem VLAN gibt es nur einen gesicherten Übergang über den Authentifizierungs-Server in das

Hochschulnetz. Dadurch wird sowohl der administrative Aufwand möglichst klein gehalten, als auch ein Schutz gegen den Missbrauch dieses Netzes erreicht.
Zu Beginn einer Sitzung ist eine Authentisierung mittels eines gesicherten WWW-Formulars über diesen Server erforderlich. In diesem Formular müssen die auch für die Modem/ISDN-Einwahl gültigen Benutzerkennungen und Passwörter eingegeben werden. Die Benutzerdaten werden zum Authentifizierungs-Server übertragen und dort gegenüber der zentralen Radius-Datenbank geprüft. Falls die Authentifizierung erfolgreich war, werden im Firewall die zuvor per DHCP vergebene IP-Adresse und die zugehörige MAC-Adresse frei geschaltet. Ohne eine erfolgreiche Authentisierung kann keine Kommunikation mit Rechnern im Hochschulnetz oder Internet erfolgen. Die Abb. 7 zeigt schematisch das Vorgehen zur Anmeldung am Netzwerk.
Über eine Transparent-Proxy genannte Funktionalität wird sichergestellt, dass der noch nicht authentifizierte Benutzer beim Aufruf beliebiger WWW-Seiten das WWW-Login-Formular mit der Aufforderung seine Benutzerdaten anzugeben präsentiert bekommt. Dadurch verringert sich der Beratungsaufwand erheblich.
Die beschriebene Authentifizierungsmethode wird völlig analog auch bei öffentlich zugänglichen Ethernet-Anschlüssen und bei den Wohnheimen eingesetzt.

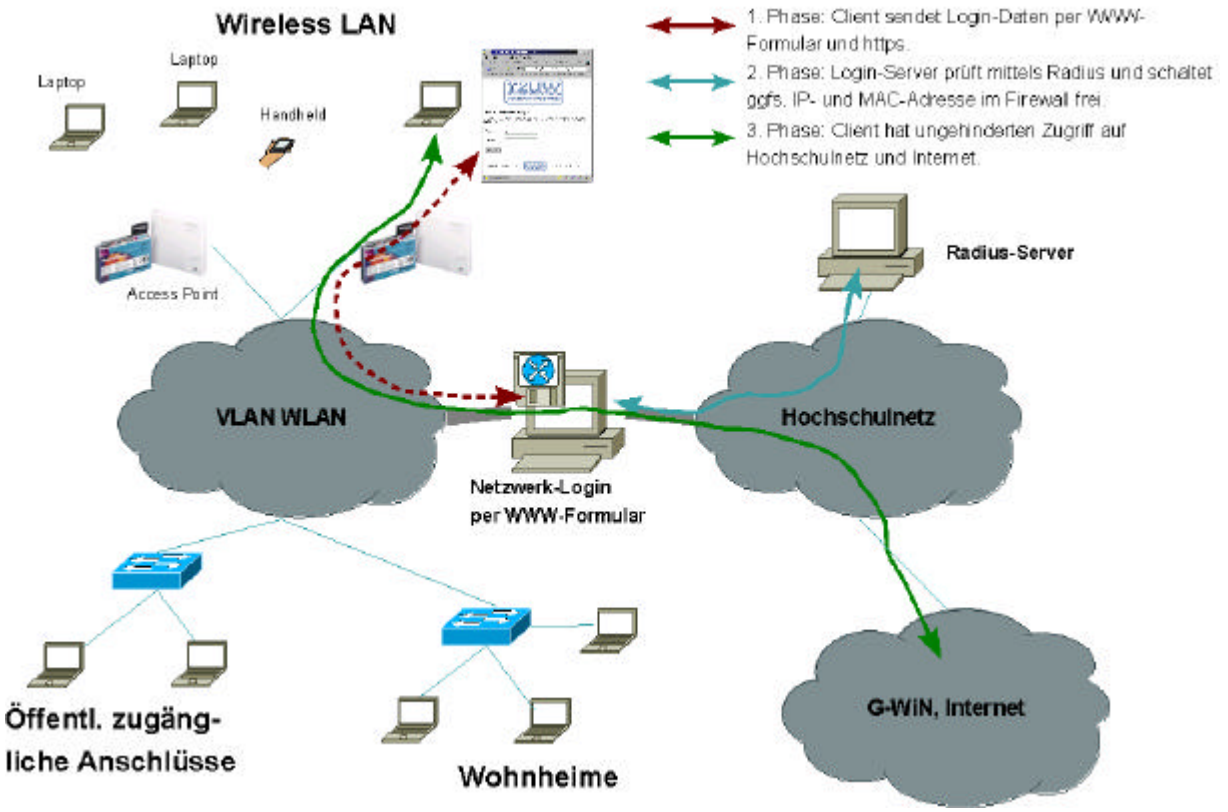


**Abb. 7**: Zugang zum Hochschulnetz über Netzwerk-Login

Da die auf Firewall-Regeln basierende Lösung keine Verschlüsselung auf Netzwerk-Ebene bietet und von IP- und MAC-Adressen abhängt, die prinzipiell manipulierbar sind, ist mit zunehmender Unterstützung in Client-Betriebssystemen die Einrichtung eines VPN-Servers auf Basis von IPSec, PPTP oder L2TP vorgesehen.

## 4.2 Entwicklung

### 4.2.1 Verkabelung

Im Rahmen des Netz-Investitions-Programms (NIP I) wurde zwar eine flächendeckende Vernetzung erreicht, diese ist jedoch auf den Etagen zum großen Teil noch in Koax-Technik ausgeführt. In den nächsten Jahren wird es nun vorrangig im Rahmen von NIP II Aufgabe sein, einerseits die Vernetzungslücken zu schließen und andererseits die Koax-Verkabelung durch eine strukturierte Verkabelung (Lichtwellenleiter oder Kupfer) zu ersetzen.

Im Bereich der Universität Würzburg sind die in der folgenden Tabelle aufgelisteten Gebäude vom Netzausbau und der Netzsanierung betroffen. Die Zuordnung der Nummern in Spalte 2 zu den Gebäuden ist den Lageplänen (Abb. 1 und Abb. 2) zu entnehmen.

| **Bereich** | **Nummer** | **Gebäude-Kürzel** | **Gebäude-Bezeichnung** |
|---|---|---|---|
| | | | |
| Hubland | 5 | HPL | Philosophie |
| | 8 | HCH | Chemie (Zentralbau, Organische, Anorganische) |
| | 8 | HCH | Chemie (Physik. Chemie) |
| | 11a | HPH | Mikrostrukturlabor |
| | 11 | HHN | Hörsaalbau Naturwissenschaften |
| | 13a | HZB | Universitätsbibliothek |
| | 7b | HBI | Biozentrum |
| | 9a | HMI | Mineralogie |
| | bei 15 | HTB | Technischer Betrieb |
| | | HME | Mensa |
| | | | |
| Sanderring | 1 | ENE | Neue Universität |
| | 13g | EOS | Ottostr. 16 |
| | 13g | EZ2 | Zwinger 32 |
| | 13g | EZ4 | Zwinger 34 |
| | 1a | EIH | Alte IHK |
| | | ESW | Studentenhaus |
| | | | |
| Röntgenring | 6e | RMS | Marcusstr. 9 – 11 (Alte Physik. Chemie) |
| | 3j | RPH | Physiologie |
| | 3i | RAN | Anatomie |
| | 6f | RAZ | Röntgenring 10 (Alte Zoologie) |
| | 3k | RAC | Röntgenring 11 (Alte Chemie) |
| | 9 | RGE | Geologie |
| | | | |
| Klinik | 3 | KPA | Pathologie |

| | | | |
|---|---|---|---|
| | 3a | KRE | Rechtsmedizin |
| | 3b | KMS | Med. Strahlenkunde |
| | 3c | KVI | Virologie und Immunologie |
| | 3d | KPT | Pharmakologie und Toxikologie |
| | 3 | KHM | Hygiene und Mikrobiologie (Bau 17) |
| Einzelgebäude | 6 | EWI | Wittelsbacherplatz |
| | 3n | EON | Geschichte der Medizin |
| | 2 | EAU | Alte Universität |
| | 2 | EPS | Psychologie, Domerschulstr. 13 |
| | 4 | ERE | Residenz |
| | 7a | EBO | Botanik |
| | 6c | ESP | Sportzentrum |
| | | EFS | Ökologische Außenstation Fabrikschleichach |

Tabelle 1: Vom Netzausbau betroffene Gebäude

Für dieses Vorhaben wurde im Januar 1999 ein Bauantrag in Höhe von DM 24.600.000 (bzw. EUR 12.778.000) gestellt. Dabei wurde der Bauantrag in zwei Ausbaustufen unterteilt. Auf die erste Ausbaustufe entfallen rund DM 12.600.000, auf die zweite die verbleibenden DM 12.000.000.
Für die erste Teilbaumaßnahme wurde im Herbst 2000 eine Haushaltsunterlage (HU-Bau) vorgelegt mit einem Volumen von rund DM 12.600.000 bzw. EUR 6.443.000. Diese HU-Bau ist wiederum in drei Teilbauabschnitte unterteilt:

| | **Gebäude-Bezeichnung** |
|---|---|
| | |
| 1. Teilbauabschnitt „Am Hubland“: | |
| | Biozentrum |
| | Universitätsbibliothek |
| | Chemie (Zentralbau, Organische, Anorganische) |
| | Philosophie |
| | Mikrostrukturlabor |
| | Mineralogie |
| | Mensa |
| | Technischer Betrieb |
| | Hörsaalbau Naturwissenschaften |
| | |
| 2. Teilbauabschnitt „Innenstadt“: | |
| | Neue Universität |
| | Wittelsbacherplatz |
| | Botanik |

| | |
|---|---|
| | Alte Universität |
| | Alte IHK |
| | Ökologische Außenstation Fabrikschleichach |
| | Geschichte der Medizin |
| | Domerschulstrasse 13 (Alte Psychologie) |
| 3. Teilbauabschnitt „Röntgenring“: | |
| | Röntgenring 11 (Alte Chemie)<br>Anatomie |
| | Röntgenring 10 (Alte Zoologie) |
| | Geologie |
| | Marcusstr. 9 – 11 (Alte Physik. Chemie) |
| | |
| Restliche Gebäude (derzeit nicht in der 1. Teilbaumaßnahme enthalten): | |
| | Residenz |
| | Pathologie |
| | Hygiene und Mikrobiologie (Bau 17) |
| | Rechtsmedizin |
| | Pharmakologie und Toxikologie |
| | Virologie und Immunologie |
| | Physiologie |
| | Ottostr. 16 |
| | Zwinger 32 |
| | Zwinger 34 |
| | Med. Strahlenkunde |
| | Sportzentrum |
| | Chemie (Physik. Chemie) |
| | Studentenhaus |

Tabelle 2: Drei Teilbauabschnitte der ersten Teilbaumaßnahme NIP II

Für den ersten Teilbauabschnitt wurde im Herbst 2001 eine Ausführungsunterlage (AFU-Bau) in Höhe von EUR 3.232.882 vorgelegt. Nach einer Ausschreibung befindet sich der 1. Teilbauabschnitt „Am Hubland“ seit Juni 2002 in der Realisierung.

Wie bereits in der HU-Bau erwähnt, wird erwartet, dass in der 1. Teilbaumaßnahme mehr Gebäude vernetzt werden können als ursprünglich geplant.
In der 2. Teilbaumaßnahme soll der verbleibende Rest der Gebäude vernetzt werden. Außerdem sollen Maßnahmen zur Erhöhung der Verfügbarkeit (passive und aktive Redundanz, Übergang von FTTO zu FTTD, Notstrom-Anbindungen und USVen) im Vordergrund stehen.
Einen weiteren Schwerpunkt der 2. Teilbaumaßnahme soll die multimedia-orientierte Vernetzung darstellen. Sie betrifft im Wesentlichen die Hörsaalverkabelung und -ausstattung. Dabei ist der Übergang von der klassischen Datenkommunikation zur AV-Kommunikation fließend (ersicht-

lich z.B. durch Beamer mit Netzwerk- oder Digital-Anschluss sowie mit eigenem Präsentationsspeicher).
Aufwändig und teuer in Hörsälen sind erfahrungsgemäß die Verlege- und Bauarbeiten, insbesondere durch die knappe verfügbare Zeit. Auch aus diesem Grund ist es sinnvoll und notwendig, klassische Daten- und Multimedia-Vernetzung aus einer Hand zu planen und in einem Arbeitsgang aufzubauen.
Die wesentlichen Aufpunkte für eine Vernetzung sind:

- Pult bzw. Referentenstandort,
- Kanzel bzw. Regie,
- Vorbereitung,
- Beamer bzw. Technik.

Insgesamt sind zu berücksichtigen:

- digitale und analoge Kabel (LWL-, TP-, VGA-, Koax-, Strom-, Schalt-Kabel),
- Patchfelder (digital und analog) bzw. Kreuzschienenverteiler,
- Leitungstreiber (bei Überlängen),
- Datenprojektoren,
- Steuerungen,
- 19"-Schränke.

### 4.2.2 Netzstrukturierung und Komponenten

#### 4.2.2.1 Netzstrukturierung

Die bisherige Netzstruktur (zentraler Switch, Backbone-Router, Gebäude-Switches) soll beibehalten werden. Allerdings muss die Übertragungsgeschwindigkeit der Verbindungsstrecken, die Funktionalität und die Verfügbarkeit dem geänderten Bedarf angepasst werden.
In Zukunft sind Verbindungen mit 10 Gbit/s oder Leitungsverdopplungen mittels WDM-Systemen im Backbone-Bereich und bis zu 1 Gbit/s flächendeckend im Anschlussbereich denkbar.
An Funktionalität der Komponenten wird die Unterstützung von VLANs, von CoS und von Zugangskontrollen gefordert werden.
Es muss von einer komponenten- oder gebäudelokalen zu einer netzweiten, leicht managebaren VLAN-Strukturierung übergegangen werden.
Eine durchgehende CoS-Unterstützung aller Komponenten kann für die Übertragung zeitkritischer Daten wie Bild und Ton wichtig werden.
Zugangskontrollen am Netzrand (IEEE 802.1x) werden ein wichtiges Sicherheits- und Kontrollinstrument werden.
Die Stabilität und Ausfallsicherheit im Netz muss soweit sinnvoll und möglich durch passive und aktive Vernetzungsmaßnahmen gefördert werden. Dazu können redundante Leitungsführung, redundante Komponententeile sowie der Einsatz von USVen beitragen.

Im Rahmen des Umbaus der Vernetzung von Koax auf strukturierte Verkabelung müssen auch die bisher eingesetzten Netzkomponenten (Repaeter und Switches mit 10 Mbit/s und angeschlossenen Koax-Strängen) durch Switches mit hoher Übertragungsleistung ersetzt werden. In Richtung Netzbackbone sind Geschwindigkeiten von 1 bis 10 Gbit/s, in Richtung Nutzeranschluss 10/100/1000 Mbps autosensing Switched Ethernet Ports denkbar.

#### 4.2.2.2 Flächendeckender Ausbau

Auch bei der laufenden Vernetzungsmaßnahme werden aus Kostengründen nur wirklich benötigte Leitungen aktiv beschaltet. Auf eine Vollversorgung aller vorhandenen Dosen mit aktiven Komponenten wird derzeit normalerweise verzichtet, so dass bei den strukturiert vernetzten Gebäuden zurzeit lediglich 60 % der vorhandenen passiven Anschlüsse auch aktiv geschaltet sind.
Bei Umzügen oder Neuanschlüssen muss die Verbindung im Patchfeld entfernt und/oder neu geschaltet werden. Es ist in nächster Zeit zu untersuchen, ob dieses personalaufwändige Änderungsmanagement nicht durch eine (fast) volle Beschaltung aller Anschlüsse erheblich reduziert werden kann. Dadurch könnte der Aufwand für das manuelle Patchen im Verteilerfeld, die Dokumentation und die Fehlersuche erheblich verringert werden. Die Inbetriebnahme eines Ports könnte dann per Management erfolgen. Diese Lösung würde insgesamt zu einer besseren Dienstqualität und zusätzlich zu einem geringeren Personalaufwand führen.

### 4.2.3 Zugänge zum Hochschulnetz von außerhalb

Die Zugänge vom häuslichen Arbeitsplatz müssen für Mitarbeiter und Studierende noch interessanter werden (preisgünstiger und leistungsfähiger). Neben den vorhandenen Möglichkeiten soll für den Zugang zum Hochschulnetz über externe Provider vom Rechenzentrum ein VPN-Server zur Verfügung gestellt werden. Die Entwicklung auf dem Markt lassen auch die Hoffnung zu, dass es bald spezielle xDSL-Angebote für Mitarbeiter und Studierende geben wird. Wichtig wird es sein, die sich dann ergebenden Strukturen gut in das Hochschulnetz einzubinden. Das wird durch Einrichtung geeigneter VPN-Server geschehen, die die Nutzung aller Dienste des Hochschulnetzes – unter Berücksichtigung der geltenden Zugangsregelungen – vom häuslichen Arbeitsplatz aus ermöglichen.

### 4.2.4 Zugang zum Hochschulnetz für mobile Endgeräte

Der Zugang für mobile Endgeräte wird weiter ausgebaut werden. Dabei sollen neben der drahtlosen Kommunikationstechnik (derzeit auf Basis von IEEE 802.11b mit einer Brutto-Bandbreite von 11 Mbit/s) auch in Zukunft an ausgewählten Stellen vorkonfektionierte Datendosen angeboten werden.
Funknetze sind vor allem zur Anbindung mobiler Rechner gedacht, ein Ersatz für Festnetzanschlüsse ist damit nicht zu erreichen und auch nicht vorgesehen. Eine flächendeckende Versorgung für mobile Endgeräte erscheint derzeit weder notwendig noch sinnvoll. Daher sollte auch in Zukunft der Schwerpunkt bei öffentlichen, vernetzungstechnisch aber schwer zu erschließenden Bereichen (z.B. Hörsaal, Seminarraum, Mensa, Cafeteria, Foyer, Ausstellungsbereich) liegen. Der Zugang soll über geeignete VPN-Server abgesichert werden.

# 5 Netz-/ Dienstintegration

## 5.1 Telefonie

Innerhalb der Universität Würzburg wird eine volle Integration des Daten- und Telefon-Dienstes derzeit nicht angestrebt. Die TK-Anlagen der Universität Würzburg müssen momentan weder erweitert noch ersetzt werden. Die Betriebsverantwortung für die Telefonanlagen liegt bei den Technischen Betrieben, getrennt nach Lehre&Forschung und Kliniken.
Aus wirtschaftlichen Gründen wird aber durchaus eine gemeinsame Nutzung von kostspieliger Infrastruktur verfolgt. Bedingung dafür ist aber eine sehr hohe Betriebsstabilität.

## 5.2 IP-Telefonie

Seit 2001 betreibt das Rechenzentrum der Universität ein kleines internes IP-Telefonie-Pilotnetz, das mittlerweile mit anderen Pilotpartnern im DFN-Bereich über das Wissenschaftsnetz verbunden ist. Es dient in erster Linie zum Sammeln von Erfahrungen und zum Durchführen wissenschaftlicher Tests. Im Pilotnetz werden die Randbedingungen für einen Wirkbetrieb und die Einführung komfortabler Mehrwertdienste getestet. Das Pilotnetz stellt derzeit aber keine Basis für die Übernahme des universitätsweiten Telefonnetzes dar. Voraussetzung dafür wäre, dass entsprechende Vorkehrungen für eine extrem hohe Verfügbarkeit getroffen und erforderliche Personalstellen bereitgestellt werden würden.

## 5.3 Gebäudeleittechnik

Die schrittweise Umstellung der universitätsweiten Gebäudeleittechnik (GLT) von proprietären auf netzbasierte Standardlösungen legt nahe auch die Infrastrukur gemeinsam zu nutzen. Zur klaren Trennung zwischen Daten- und GLT-Diensten erscheint es aber nötig, entweder getrennte Fasern oder zumindest getrennte Wellenlängen zu verwenden und auch die Übergabepunkte in den Gebäuden getrennt auszuweisen.

# 6 Verantwortungs- und Zuständigkeitsverteilung

Das Rechenzentrum der Universität ist grundsätzlich für Planung, Betrieb und Management des Hochschulnetzes bis zur Datendose im Arbeitsraum zuständig.
Dies geschieht in enger Zusammenarbeit mit den Netzverantwortlichen der Fachbereiche/Institute und Einrichtungen der Universität. Die Aufgaben, die der jeweilige Netzverantwortliche in seinem Zuständigkeitsbereich wahrzunehmen hat, sind in der Netzbenutzungsordnung festgelegt und umfassen im Einzelnen:

- Verwaltung der zugeteilten Namens- und Adressräume,
- Führung einer Dokumentation über die ans Hochschulnetz angeschlossenen Endgeräte bzw. Netze,
- Zusammenarbeit mit dem Rechenzentrum bei der Planung und Inbetriebnahme von Erweiterungen der Gebäudenetze (neue Anschlusspunkte, neue Netzstrukturen),
- Mitarbeit bei der Fehlerbehebung (z.B. Durchführen von mit dem Rechenzentrum abgestimmten Tests zur Fehlereingrenzung),
- Zusammenarbeit mit dem Rechenzentrum bei der Eindämmung missbräuchlicher Netznutzung.

Falls gewünscht, können einzelne Fakultäten und Institute in Absprache mit dem Rechenzentrum mehr oder weniger weitgehende Teilaufgaben der Netzadministration auch selbständig wahrnehmen.
Die DV-Abteilung der Zentralverwaltung plant und baut das Verwaltungsnetz in enger Abstimmung mit dem Rechenzentrum, betreibt es völlig selbständig. Am Übergang vom Hochschulnetz zum Verwaltungsnetz ist eine Firewall installiert, die vom DV-Personal der Zentralverwaltung betrieben wird.
Die medizinische Fakultät plant, baut und betreibt ihre internen Netze (Medizinisches Versorgungsnetz und Wissenschaftsnetz) völlig selbständig. Am Übergang vom Hochschulnetz zum Medizinischen Versorgungsnetz ist eine Firewall installiert, die vom DV-Personal der Klinik betrieben wird.

Der Zugang zum Wissenschaftsnetz und Internet wird gemeinsam genutzt und vom Rechenzentrum betrieben.

## 6.1 Planung

Die Planung der Netzinfrastruktur für das komplette Backbonenetz und die Gebäudenetze im Bereich Lehre&Forschung wird vom Rechenzentrum in Absprache bzw. in Zusammenarbeit mit folgenden Gremien durchgeführt:

- Ständige Kommission für Angelegenheiten des Rechenzentrums:
  Begutachtung von Anträgen, Sachstandsberichte,
- Universitätsbauamt Würzburg:
  Feinplanung der Verkabelung über Fachplaner und Auftragsvergabe,
- Zentralverwaltung, Referat Bauplanung:
  Grobe Zielvorgaben, Bearbeitung von Anträgen.

In Zusammenarbeit mit den einzelnen Instanzen der Universität (Zentralverwaltung, IT-Bereichsmanager der Fakultäten, Netzverantwortliche usw.) ermittelt das Rechenzentrum den Bedarf und entwickelt auf dieser Basis eine Planung für die mittelfristige Entwicklung in quantitativer und qualitativer Hinsicht unter besonderer Berücksichtigung der Nutzung innovativer Netztechniken.
Diese Planung ist Grundlage für die Umsetzung in konkrete Anträge, Bau- und Beschaffungsmaßnahmen.

## 6.2 Betrieb

Die grundsätzliche Zuständigkeit für den Betrieb des Hochschulnetzes liegt beim Rechenzentrum. Der Betrieb selbst bedarf wegen seiner Komplexität und der knappen Personalressourcen im Rechenzentrum arbeitsteiliger Verfahren. Die hohe Fluktuation des häufig zu Betreuungsdiensten herangezogenen wissenschaftlichen Personals in den Einrichtungen der Universität führt dazu, dass die Verfahren instabil werden und oft reorganisiert werden müssen.

### 6.2.1 Prinzip

Grundsätzlich erfolgt der Betrieb noch nach dem von der DFG seinerzeit ins Leben gerufenen Prinzip der Kooperativen DV-Versorgung. Das heißt, das Rechenzentrum betreibt alle zentralisierbaren Teile des Hochschulnetzes (Backbone und zentrale Server und Dienste) und die Nutzer ihre Subnetze (einschl. Gebäude-Netzkomponenten und Server).
Für die Netzverantwortlichen werden vom Rechenzentrum regelmäßige Treffen sowie Aus- und Weiterbildungsmaßnahmen durchgeführt. Außerdem werden die Netzverantwortlichen bei Bedarf vom Rechenzentrum bei der Durchführung ihrer Arbeit unterstützt.
Es ist aber zu beobachten, dass aufgrund der hohen Fluktuation des Betreuungspersonals viele Informationen und viel Know-how verloren gehen und so einige Einrichtungen entweder nicht mehr willens oder nicht mehr in der Lage sind, ihre Subnetze in Eigenregie zu betreiben.

### 6.2.2 Betrieb Backbonenetz / Subnetze

- **Verkabelungsinfrastruktur** (Kabelwege, Verteilerräume, Primär-, Sekundär-, Tertiärverkabelung, Funkstrecken):
  Der Technische Betrieb ist zuständig für die Bereitstellung und den Betrieb von Kabelwe-

gen und Verteilerräumen. Das Rechenzentrum ist zuständig für die Beschaltung der Verteilerschränke einschl. zugehöriger Dokumentation sowie alle Messungen (sofern nicht Bestandteil einer Baumaßnahme) und die Beseitigung von Störungen im Backbonenetz. Die Netzverantwortlichen sind zuständig für das Lokalisieren und Beheben von Störungen in Gebäudenetzen. Ggfs. werden sie dabei vom Rechenzentrum unterstützt.

- **Netzkomponenten** (Medienkonverter, Switches, Router, Wählzugänge, usw.):
  Sowohl das Konfigurieren und Überwachen als auch das Beseitigen von Störungen sind grundsätzlich Aufgaben des Rechenzentrums. Die Netzkomponenten sind in den Verteilerräumen untergebracht. Sofern sie zum Betrieb lokaler, fachbereichseigener Infrastrukturen dienen (CIP und WAP-Cluster), können sie nach Absprache mit dem Rechenzentrum auch in den Räumen der Fachbereiche aufgestellt und von diesen betreut werden. Darüber hinaus ist der Betrieb der Intranets der Zentralverwaltung, der medizinischen Fakultät (Medizinisches Versorgungsnetz und Wissenschaftsnetz), der Fachhochschule Würzburg-Schweinfurt, Abt. Würzburg und der Hochschule für Musik Würzburg komplett in der Hand eigenständiger Betriebsabteilungen.

Rechte und Pflichten des Rechenzentrums, der Netzverantwortlichen und der Nutzer sind in öffentlich verfügbaren Ordnungen (http://www.zv.uni-wuerzburg.de/rechtsamt/Sonst.html) geregelt.

### 6.2.3 Betrieb von Netzdiensten

Das Rechenzentrum betreibt eine Reihe zentraler Netzdienste. Die administrativen Vorgaben und Einschränkungen sind unter http://www.rz.uni-wuerzburg.de/infos/benutzungso/ festgelegt und werden bei Bedarf fortgeschrieben. Zu den vom Rechenzentrum betriebenen Netzdiensten gehören insbesondere:

- DNS/NDS
- DHCP
- GWiN-Anschluss
- ATM-Anschluss
- Multicasting
- Radius
- VPN/IPsec (geplant)
- Novell
- Mail-Relay/-Server/-Viren-Scanner
- Proxies-/Cache-Server
- NTP-Server
- FTP-Server

### 6.2.4 Betrieb von Multimedia-Diensten

Eine Koordinierung der Multimedia-Aktivitäten findet derzeit noch nicht statt. Das Rechenzentrum unterstützt die Einrichtungen der Universität in der Pilotphase im Betrieb des Multimedia-Equipments. Die Ständige Kommission für die Angelegenheiten der Universitätsbibliothek und des Zentrums für Sprachen und Mediendidaktik berät derzeit ein Konzept für den Einsatz von Multimedia an der Universität Würzburg.

# 7 Administration

## 7.1 Adressraum

Der Universität Würzburg sind derzeit folgende offizielle IP-Adressen zugeordnet:

- Lehre & Forschung: 132.187.0.0/16
- Med. Versorgung: 141.27.0.0/16
- Sonstige: 194.95.75.128/25

Der Universität Würzburg sind derzeit folgende Namensräume zugeordnet:

- uni-wuerzburg.de

Die Struktur der Namensräume unterhalb dieser Ebene folgt den Strukturen auf der Ebene der Institute, Lehrstühle und Arbeitsgruppen. Die expliziten Regelungen sind in http://www.rz.uni-wuerzburg.de/infos/benutzungso/domain.html dokumentiert.
Daneben existieren unter Kenntnis und Genehmigung der zuständigen Stellen weitere Second-Level-Domains, die von einzelnen Instituten, Lehrstühlen und Arbeitsgruppen beantragt und gepflegt werden.
IPX wird derzeit noch im Hochschulnetz unterstützt. Es existiert eine einheitliche Vorgabe für die Namensverwaltung.

## 7.2 Benutzerverwaltung

In Zusammenarbeit mit der Zentralverwaltung der Universität wurde für die Studierenden eine Plattform für eine universitätsweite einheitliche Benutzerverwaltung eingerichtet. Für die Mitarbeiter der Universität wird das ebenfalls angestrebt. Ein Arbeitskreis soll entsprechende Lösungen erarbeiten. Für die vom Rechenzentrum angebotenen zentralen Dienste (Zentrale Server, Wählzugänge, Funknetzzugänge, öffentliche Arbeitsplätze) gilt derzeit bei Studierenden der universitätsweite Account und bei Mitarbeitern der Rechenzentrums-Account. In den einzelnen Einrichtungen existieren für Mitarbeiter für interne Zwecke teilweise eigene, davon unabhängige Benutzerverwaltungen.

## 7.3 Geräte

Das Rechenzentrum versucht in Zusammenarbeit mit den Netzverantwortlichen, Kenntnis über alle am Datennetz angeschlossenen Endgeräte zu erhalten. Nur Endgeräte, deren Adresse im DNS eingetragen ist, dürfen im Hochschulnetz betrieben werden.
Die Mindestangaben für jeden Rechner sind:

- IP-Adresse,
- Geräte-Typ / OS,
- Ansprechpartner.

Auf diese Weise kann der Anteil nicht registrierter Rechner relativ klein gehalten werden.

# 8 IT-Sicherheit und Datenschutz

## 8.1 Schutz gegen Missbrauch und Angriffe

### 8.1.1 Grundlegendes

Aufgrund üblicherweise freizügig betriebener Netzzugänge und breitbandiger Internet-Anbindungen sind die IT-Ressourcen von Universitäten ein bevorzugtes Ziel von Angriffen. Betrachtet man die an einer Universität typischerweise verarbeiteten Daten anhand der Schadensszenarien des BSI (Bundesamtes für Sicherheit in der Informationstechnik), so ist ein erhöhter Schutz der Daten und IT-Systeme dringend erforderlich. Neben den Daten sind aber genauso die IT-Ressourcen wie z.B. das Hochschulnetz und die IT Systeme selbst, zu schützen.

**Bedrohungsszenarien**

Zu den gängigen Bedrohungsszenarien zählen:

- Denial-of-Service-Attacken,
- Trojanische Pferde,
- Viren,
- Active Contents,
- Scans,
- Sniffing,
- Kompromittierung von Rechnersystemen.

Die Angriffe erfolgen sowohl von außen (Internet) als auch von innen. Dabei geht ein Teil der Bedrohungen aus dem Hochschulnetz von Rechnern aus, die bereits von Dritten kontrolliert werden.

**Netztechnische Maßnahmen**

Netztechnisch lässt sich den Bedrohungen begegnen durch:

- Filtereinsatz:
  auf verschiedenen Ebenen, am Übergang nach außen, am Übergang zu Subnetzen
- Strukturelle Maßnahmen:
  - Doppel-Router-Systeme zur Entkopplung von Filterlast und betrieblichen Aufgaben
  - striktes LAN-Switching
  - dezentrale Firewalls, die zentral vom Rechenzentrum administriert werden
- Unterstützende Maßnahmen:
  - Überwachung des Datenverkehrs und Untersuchung nach verdächtigen Mustern
  - Diensttopologische Umstrukturierung des Rechenzentrums als Beispiel für die Institute und Einrichtungen der Universität

**Anwendungstechnische Maßnahmen**

Da sich Bedrohungen durchaus gegen bestimmte Server bzw. Services richten, muss sich auch die Abwehr daran orientieren. Entsprechende Maßnahmen sind:

- Zentralisierung von Services,
- Minimalisierung der Services pro Server,
- Einrichten von VPNs zwischen Zentrale und Außenstellen von Universitätseinrichtungen
- Aufbau eines VPN-Systems für Universitätsangehörige, die von außerhalb auf interne

Hosts zugreifen müssen,
- Kompetente und qualifizierte Systembetreuung aller IT-Systeme,
- Einsatz geeigneter Virenschutz-Mechanismen.

**Organisatorische Maßnahmen**
Um für die Universität und die einzelnen Einrichtungen den erforderlichen Schutzbedarf feststellen und geeigneten Schutzmaßnahmen treffen zu können, ist nach BSI ein IT-Sicherheitsprozess notwendig. Dieser sollte durch geeignete IT-Sicherheitsmanagement-Strukturen organisiert werden, deren wichtigste Elemente ein zentrales IT-Sicherheitsmanagement-Team und in den Einrichtungen IT-Sicherheitsbeauftragte sind. Wesentliche Bestandteile des IT-Sicherheitsprozesses sind die Dokumentation der vorhandenen IT-Umgebungen, eine Schutzbedarfsfeststellung sowie die Festlegung, die Einführung und die Überwachung der geeigneten Schutzmaßnahmen.

### 8.1.2 Ansatz der Universität Würzburg

Auf der Basis des kooperativen Betreuungskonzepts liegt die Verantwortung sowohl für die Daten als auch für die IT-Systemen und Netzkomponenten bei den jeweiligen Betreibern. Andererseits ist festzuhalten, dass an der Universität Würzburg in erheblichem Umfang schutzwürdige Daten verarbeitet werden:
- Im Rahmen von Projekten, bei denen Drittmittel in erheblichem Umfang eingesetzt werden und deren Forschungsergebnisse durch vertragliche Vereinbarungen der Geheimhaltung unterworfen sind,
- im Rahmen von Forschungsarbeiten, die als besonders schützenswert einzustufen sind,
- im Bereich der Zentralverwaltung die Verarbeitung personenbezogener Daten, die dem Datenschutz unterliegen. (Zu deren Schutz wurden jedoch bereits in der Vergangenheit entsprechende Maßnahmen getroffen.)

Die Hochschulleitung der Universität Würzburg hat die Bedeutung der IT-Sicherheit erkannt und bereits im März 2001 einen Arbeitskreis mit der Erstellung einer „IT-Security-Policy“ und einer Basisfassung eines „IT-Security-Konzepts“ beauftragt. Im April 2002 wurde der Bericht des Arbeitskreises fertig gestellt und der Hochschulleitung übergeben.
Ziel eines IT-Sicherheitskonzepts ist es, mit einem Bündel von IT-Sicherheitsmaßnahmen die IT-Sicherheitsrisiken auf ein akzeptables Maß zu reduzieren. Das Bündel muss neben technischen auch organisatorische Maßnahmen enthalten.

Um den IT-Sicherheitsanforderungen schon jetzt ein Stück gerecht zu werden, sind vorab eine Reihe zentraler Maßnahmen im Hochschulnetz umzusetzen. Die Kernpunkte sind:

**Netztechnische Maßnahmen**
Im Vordergrund sollte eine Neustrukturierung des Hochschulnetzes stehen, bei der das Netz in verschiedene Sicherheitsbereiche unterteilt wird, die je nach Bedarf durch mehr oder weniger stark ausgeprägte Firewall-Funktionalitäten abgeschottet sind.
Besonderes wichtig ist, dass die Sicherheitsmaßnahmen die Charakteristik des Netzwerks in Bezug auf Performance und Multimedianutzung möglichst nicht beeinträchtigen.

**Anwendungstechnische Maßnahmen**
Eine Reihe von Maßnahmen auf der Ebene der Anwendungen wurde bereits in den letzten Jahren umgesetzt. Weitere müssen folgen. Im Vordergrund stehen hier:

- Weitere Zentralisierung der Web-, FTP- und E-Mail-Server,
- Betrieb eines zentralen E-Mail-Viren-Scanners,
- Verteilen eines kostenlosen Virenschutzprogramms (wichtig für mobile Geräte),
- Einsatz von Autopatch- bzw. Online-Update-Mechanismen und Forcierung von automatischen Betriebssystem-Installationen (Windows), um bei den begrenzten Personalressourcen den Administrationsaufwand bei den IT Systemen möglichst gering zu halten, andererseits jedoch ein hohes Niveau an Qualität zu sichern,
- Betrieb eines Monitoring-Systems zur Verkehrsbeobachtung,
- Einsatz zentraler Filtermechanismen mit Positivliste, um Dienste für das Internet nur von kooperativen Systemen erbringen zu können,
- Einsatz eines zentralen VPN-Dienstes,
- Ersatz von Protokollen mit Klartext-Übertragung sensitiver Daten (z.B. ssh statt telnet).

**Organisatorische Maßnahmen**
Neben den technischen Maßnahmen kommt eine besondere Bedeutung den organisatorischen Maßnahmen zu. Dazu zählen:

- Einrichten eines IT-Sicherheitsmanagement-Teams,
- Benennen von IT-Sicherheitsbeauftragten durch die Einrichtungen und Fachbereiche,
- Zuordnen der Befugnisse an die einzelnen Verantwortungsbereiche,
- Fortschreiben von Benutzungsordnungen,
- Durchführen von Schulungs- und Sensibilisierungsmaßnahmen,
- Verpflichten zur Dokumentation der eingesetzten IT-Ressourcen,
- Einführen einer universitätsweiten personenbezogenen Benutzerverwaltung (incl. Zentralisierung),
- Erstellen von Notfallplänen.

## 8.2 Sicherung der Endgeräte und Zugangskontroll-Strategien

**Berechtigte Geräte**
Es dürfen nur die vom Rechenzentrum den Fachbereichen zugewiesenen und von den Netzverantwortlichen verwalteten IP-Adressen verwendet werden. An den Netzwerkknoten könnte zwar sichergestellt werden, dass nur IT-Systeme mit registrierten MAC-Adressen einen Zugang zum Hochschulnetz erhalten, dies wird jedoch wegen des hohen Verwaltungsaufwandes derzeit nicht durchgeführt. Durch diese Maßnahme kann zudem nicht sichergestellt werden, dass nur „berechtigte Nutzer“ die IT-Infrastruktur verwenden.

**Berechtigte Nutzer**
Durch die Vereinbarung und Umsetzung einer universitätsweiten Benutzerverwaltung soll mittelfristig im gesamten Bereich der Universität sichergestellt werden, dass nur authentifizierte Nutzer Zugriff auf Endgeräte und insbesondere Netzdienste erhalten. Eine anonyme Nutzung des Netzes sollte es bereits jetzt in keinem Fall geben.
Der jeweilige Systembetreiber hat durch entsprechende Maßnahmen stets dafür Sorge zu tragen, dass die IT-Systeme nur von berechtigten Nutzern verwendet werden und für den Fall eines Missbrauchs der Nutzer auch identifiziert werden kann.
Bei der Nutzung der zentralen Dienste des Rechenzentrums und in öffentlichen PC-Räumen ist dies auf Basis der Benutzerverwaltung mittels Nutzerkennung und Passwort bereits geregelt.

Beim Wählzugang, bei der Nutzung von WLAN-Zugängen und beim Zugang über öffentliche Netze erfolgt eine Authentifizierung der Nutzer derzeit über Radius-Server.

## 8.3 Maßnahmen zum sicheren Betrieb des Netzes

**Sicherung der Übergaberäume**

Der Zugang zu den Übergaberäumen (Verteilerräumen) ist durch ein Zugangskontrollsystem geregelt. Zugangsberechtigt sind neben Mitarbeitern des Rechenzentrums die zuständigen Netzverantwortlichen und teilweise das Personal des Technischen Betriebs.

**Stromversorgung der Verteilerräume, Klimatisierung und Brandschutz**

Alle Übergaberäume sind mit einer unterbrechungsfreien Stromversorgung (USV) zur Überbrückung kurzer Unterbrechungen versehen. Je nach Relevanz der abzusichernden Komponenten können hierdurch Überbrückungszeiten bis zu 2 Stunden gewährleistet werden. Zudem ist vorgesehen den punktuellen Anschluss an Notstromversorgungen zu realisieren, so dass auch längere Unterbrechungen nicht zu Netzausfällen führen. Die USVen werden derzeit bereits durch das zentrale Netzmanagement überwacht. Zur Verbesserung des Brandschutzes sind in den Übergaberäumen grundsätzlich Rauchmelder zu installieren.

**Ausfallsicherheit durch Redundanz**

Um eine sehr hohe Verfügbarkeit im Primärnetz (Backbone) zu erreichen, wären u.a. eine flächendeckende doppelte Auslegung der Netzkomponenten und eine redundante Anbindung der Primärnetzknoten notwendig. Derzeit scheint jedoch der Aufwand nicht gerechtfertigt (Prinzip der Verhältnismäßigkeit). Teilweise verfügen die zum Betrieb des Backbones erforderlichen Netzkomponenten über ein redundantes Netzteil. Darüber hinaus ist beabsichtigt (soweit möglich), die eingesetzten Backbone-Router mit redundanten Managementmodulen auszustatten.
Die aktiven Komponenten für die Gebäudenetze werden zunehmend redundant an die Primärnetzknoten angeschlossen.

**Managementnetz**

Aus Sicherheitsgründen ist zum Management aller Netzkomponenten ein eigenes Management-Netz auf der Basis eines nur im Hochschulnetz gerouteten privaten Netzes vorgesehen. Über dieses Netz können alle Netzkomponenten von den Managementsystemen erreicht werden. In Zukunft könnte dieses Netz auch zu Accounting-Zwecken benutzt werden.
Bei Störungen müssen wichtige Netzkomponenten zusätzlich über ein Outband-Management erreichbar sein (Modem, etc.). Dies ist derzeit für alle Backbone-Router realisiert. Der Zugang wird überwacht und ggf. protokolliert. Mit entsprechenden Sicherungsmaßnahmen ist ein kontrollierter Zugang auf das Managementnetz auch über einen dedizierten Wählzugang für Ferndiagnose- und Fernwartungszwecke (für Mitarbeiter des Rechenzentrums) möglich.
Für das zentrale Netz- und Systemmanagement werden als Plattform HP OpenView Network NodeManager und Open-Source-Produkte wie MRTG und MON unter Linux eingesetzt.

## 8.4 Datenschutz

Das vorliegende Papier behandelt schwerpunktmäßig den Bereich Lehre und Forschung, ohne auf die speziellen Belange des Verwaltungsnetzes bzw. der Medizinischen Versorgungsnetze einzugehen. Die angeschlossenen Institutionen regeln bei Bedarf direkt mit dem Datenschutzbeauftragten die Verarbeitung, Speicherung und Weitergabe schutzwürdiger Daten in eigener Verantwortung.

# 9 Accounting

Unter Accounting wird die Zuordnung von Verkehrsdaten zu Verursachern verstanden. Es wird grundsätzlich benötigt für

- Informations- und Planungszwecke,
- ggf. Abrechnungzwecke.

Mangels harter Trennungsstrukturen in Hochschulnetzen lassen sich beide Ziele z. T. nicht genau trennen. Eine nutzerorientierte Abrechnung von Netzleistungen ist z. Z. kein Ziel der Universität Würzburg.

Die Informationsquellen über Verkehrsflüsse sind über das gesamte Netz verteilt. Sie können verschiedenen Instanzen entnommen werden

- Logs von Netzkomponenten, z.B. Routern,
- Logs von Proxy-Servern und
- Logs von Spezialinstanzen, die aktiv oder passiv den Verkehr untersuchen.

Einen umfassenden Überblick könnte man sicher durch Auswertung der Logdateien aller protokollierenden Instanzen im Hochschulnetz erhalten. Der Aufwand hierfür wäre immens, so dass sich die Frage stellt, ob er in einem sinnvollen Verhältnis zum Nutzen steht. Reine Verkehrsplanungsdaten kann man sicher mit weniger Aufwand durch Stichproben erhalten.

Eine Alternative besteht deshalb darin, den Verkehr an neuralgischen Stellen, z.B. am Übergang zum WiN zu überwachen. Diese Methode hat den Vorteil, dass genau an der Stelle gemessen wird, an der durch den WiN-Übergang regelmäßige und hohe Kosten entstehen. Außerdem ist davon auszugehen, dass das Profil der internen Netz-Nutzung dem Nutzungsprofil am WiN-Übergang vermutlich sehr ähnlich ist.

An der Universität Würzburg wird der Verkehr deshalb am WiN-Übergang mit Hilfe von Cisco Netflow gemessen. Es werden für alle Verbindungen folgende Daten festgehalten:

- Absender- und Zieladresse,
- Port-Nr.,
- Beginn- und Ende-Zeit einer „Verbindung“,
- Anzahl Pakete / Bytes.

Die ermittelten Daten werden umgehend soweit anonymisiert, dass die Erstellung von nutzerbezogenen Profilen nicht möglich ist.

Einen effektiven Beitrag zur Verkehrsregelung liefert auch eine offensive Informationspolitik. In Diskussionen mit Nutzervertretern lassen sich neue Nutzungsprofile identifizieren und ggf. Fehlentwicklungen vermeiden.

# 10 Benutzungsordnungen

Die Benutzungsordnungen und Betriebsregelungen für die Nutzung der IT-Ressourcen im Bereich der Universität Würzburg befinden sich in der jeweils gültigen Fassung unter http://www.rz.uni-wuerzburg.de/infos/benutzungso/.

# 11 Unterstützung dezentraler Systeme und Dienste

## 11.1 Mail-Service

Das Rechenzentrum betreibt eine zentrale E-Mail-Virenscanner-Anordnung, bestehend aus

- einem Rechner, der den ankommenden und gehenden Mail-Verkehr (ca. 40.000 Mails pro Tag) annimmt,
- dem E-Mail-Virenscanner
- einem Rechner, der die E-Mails an die Mail-Server des Rechenzentrums, der Einrichtungen der Universität sowie der angeschlossenen Einrichtungen weiterleitet.

Aus Sicherheitsgründen wird derzeit nur noch einer ausgewählten kleinen Anzahl von Mail-Servern gestattet, direkt E-Mails aus dem Internet zu empfangen (Sperre des Ports 25). Die Mail-Server im Rechenzentrum selbst verwalten ca. 4.500 aktive Mitarbeiter-Mailboxen und 9.000 aktive Studenten-Mailboxen. Die E-Mails werden überwiegend per POP-Protokoll von den Mail-Servern über das Netz abgeholt. Vermehrt wird aber (auch über Web-Mail-Interfaces) der Zugriff mittels IMAP-Protokoll genutzt.

## 11.2 WWW-Dienste

Das Rechenzentrum betreibt zurzeit 4 WWW-Server für die folgenden Funktionen:

- Zentraler WWW-Server der Universität,
- WWW-Darstellung des Rechenzentrums,
- WWW-Seiten von Studierenden,
- über 30 virtuelle WWW-Server für Einrichtungen aus dem Bereich der Universität.

Der Gesamtdatenbestand im WWW-Bereich der Universität umfasst derzeit knapp 100.000 Dokumente, von denen sich ca. 20.000 auf den vom Rechenzentrum betriebenen zentralen WWW-Servern befinden. Die Anzahl der Zugriffe allein auf diese zentralen WWW-Server beträgt ca. 7.000.000 pro Monat.
Im Bereich des Hochschulnetzes betreiben derzeit noch viele Institute und Einrichtungen eigene Web-Server (ca. 160). Eine stärkere Zentralisierung der WWW-Server wird angestrebt.

## 11.3 File-Service

Vom Rechenzentrum werden für ca. 2.600 Unix-Nutzer Home-Directories bereitgestellt. Der verfügbare Speicherplatz beträgt 600 GByte.
Für ca. 13.500 Novell-Nutzer werden 35 Server zentral betrieben und zusätzlich 35 dezentral betreut. Der Datenbestand beläuft sich zentral auf ca. 500 GB, dezentral auf ca. 250 GB.

## 11.4 Backup/Archivierung

Der vom Rechenzentrum angebotene Archivierungsdienst umfasst einen Datenbestand von ca. 9 TB.
Die zentralen Unix-Server sowie die zentralen Novell-Server werden über ein rechenzentrumsinternes Backup regelmäßig gesichert. Die Datenmenge beläuft sich auf etwa 1.000 GB wöchentlich.
Derzeit wird vom Rechenzentrum ein zentrales Backup-Konzept für Unix- und Novell-Server erarbeitet. Jedoch ist zumindest im ersten Schritt nicht beabsichtigt, die Sicherung aller hochschulweit verteilten Systeme zu übernehmen.

## 11.5 Softwareverteilung

Das Rechenzentrum betreibt zur Softwareverteilung mehrere FTP-Server, um über einen passwortgeschützten Zugang lizenzpflichtige Software und über einen freien Zugang Free- and Share-Software anzubieten. Das Schwergewicht liegt derzeit noch auf einer Softwareverteilung mit Datenträgern. Aber bereits mittelfristig ist mit einer deutlichen Zunahme der Verteilung über das Netz zu rechnen.
Für die zentrale Verteilung von PC-Soft- und UNIX-Software stehen derzeit insgesamt rund 180 GB zur Verfügung.
Im Bereich der Institute werden weitere FTP-Server betrieben. Auch hier ist zu prüfen, in welchem Umfang eine Zentralisierung sinnvoll und notwendig ist.

## 11.6 Verzeichnisdienste

Derzeit wird im Rechenzentrum neben DNS der Verzeichnisdienst NDS für die Verwaltung der Novell-Ressourcen betrieben. Eine Kopplung mit den zentralen UNIX-Systemen ist derzeit nicht realisiert.
Ein Arbeitskreis des Rechenzentrums soll Vorschläge für den Einsatz eines zentralen Directory-Systems für die komplette Benutzer- und Ressourcenverwaltung erarbeiten.

# 12 Netz- und Dienst-Management

## 12.1 Ziele

Ein wesentliches Ziel des Rechenzentrums ist es, mit dem vorhandenen Personalbestand eine maximale Verfügbarkeit des Hochschulnetzes zu gewährleisten. Derzeit kann das Kommunikationsnetz jedoch nur nach dem „Best-Effort-Prinzip“ betrieben werden. Dazu zählt neben einer proaktiven Überwachung des gesamten Netzwerks, der Abschluss von Wartungsverträgen für Netzkomponenten, eine intensive kooperative Zusammenarbeit mit den Netzverantwortlichen, die als Ansprechpartner für das Rechenzentrum in den Instituten vor Ort fungieren, und die Einbeziehung der Nutzer.
Eine Entstörung erfolgt grundsätzlich nur während der üblichen Arbeitszeit. Einsätze außerhalb der üblichen Arbeitszeit erfolgen derzeit lediglich auf freiwilliger Basis.
Den Anforderungen an die Dienstqualität (wie z.B. Delay, Jitter etc) wird durch Betrieb eines best-effort IP-Netzes und eines ATM-Netzes für garantierte Dienstqualität Rechnung getragen.

## 12.2 Überwachung

Die in Betrieb befindlichen Netzkomponenten werden regelmäßig durch den Einsatz folgender Programme überwacht:

- Netzwerk-Management-System HP Open View,
- MON,
- MRTG.

### 12.2.1 Open View

Mit Open View werden Netzwerk-Objekte des Hochschulnetzes mit SNMP- oder Ping-Abfragen überwacht. Für das Bedienpersonal bietet Open View eine flexible und ausgefeilte graphische Oberfläche, mit der der Zustand des Gesamtnetzes übersichtlich angezeigt werden kann.

### 12.2.2 MON

Der Service Monitoring Daemon (MON) wird zur Überwachung von Netzkomponenten, Systemen und Diensten durch eine periodische Abfrage der Verfügbarkeit verwendet. Im Fehlerfall werden anhand eines abhängigkeitsbezogenen Verfahrens die zuständigen Mitarbeiter informiert.

### 12.2.3 MRTG

Mit MRTG werden die Verkehrsdaten der meisten Switches und Router gesammelt und nach den üblichen Verfahren (auf Jahres-, Monats-, Wochen- und Tagesbasis) aufbereitet. Statistiken über die Auslastung ausgewählter Backbone-Interfaces (G-WiN-Anschluss, Backbone-Router), Nutzung der Wählzugänge usw. sind für die Netzverantwortlichen zugänglich.

## 12.3 Wartung

Im Hochschulnetz wird derzeit aus Gründen der Kostenoptimierung folgendes Wartungskonzept realisiert:

- Für das passive Außennetz gibt es einen langfristigen Wartungsvertrag mit Telekom bzw.wücom/Arcor,
- Für die passiven Gebäudenetze wurde ein spezieller Bauunterhalt „Hochschulnetz“ eingerichtet,
- Das Eingrenzen von Störungen im Backbone erfolgt durch das Rechenzentrum,
- Das Eingrenzen von Störungen in den Gebäudenetzen erfolgt durch die Netzverantwortlichen (u. U. mit Unterstützung des Rechenzentrums),
- Wenn verfügbar und möglich, sollen redundante Netzteile bei allen wichtigen Netzwerkkomponenten und zusätzlich redundante Managementmodule in den zentralen Backbone-Routern eingesetzt werden,
- Die Störungsbehebung - einschließlich Ein- und Ausbau von Komponenten – erfolgt ausschließlich durch das Rechenzentrum,
- Für alle Netzkomponenten existiert ein einheitliches Servicekonzept mit den folgenden Anforderungen:
  - Vorhaltung von Ersatzteilen (gleichzeitig Testequipment) für alle zentralen Komponenten, so dass ein Austausch eines defekten Elementes jederzeit möglich ist,
  - Bring-In-Service mit Tausch der defekten Hardwarekomponenten innerhalb von 48 Stunden,
  - Service für Beratung (Hotline und Fernwartung des Serviceanbieters),
  - Softwareservice (Updates, Problemdatenbank,..).

Dieses Konzept erfordert eine möglichst homogene Geräteausstattung. Abhängig von der Funktion im Netz werden i. d. R. nur bestimmte, durch das Rechenzentrum in regelmäßigen Zeitintervallen validierte Netzwerkprodukte eingesetzt. Dadurch lässt sich auch eine zentrale Ersatzteilhaltung realisieren, ohne dass sehr restriktive Zeitvorgaben beim Bring-in-Service benötigt werden und die Qualität und die Verfügbarkeit des Netzes darunter leiden. Mit Hilfe der Ersatzkomponenten kann neue Firmware für Netzkomponenten so im Testbetrieb ausprobiert werden.

## 12.4 Störungs-Management

Störungen werden durch das Netzwerk-Management-System erkannt und/oder durch Nutzer gemeldet. Fehlermeldungen der Nutzer können sowohl telefonisch als auch per E-Mail an die zentrale Anlaufstelle des Rechenzentrums erfolgen.

In Abhängigkeit von der Art der Störung werden vom Rechenzentrum (ggf. in Zusammenarbeit mit anderen, wie z. B. externen Providern, Netzverantwortlichen und Lieferanten) geeignete Maßnahmen eingeleitet.
Derzeit wird im Rechenzentrum ein Helpdesk-System installiert, das als zentrale Anlaufstelle zur Abgabe und Überwachung von Trouble-Tickets dienen soll. Begleitend wird die dafür erforderliche Organisationsstruktur erarbeitet.
Ein zuverlässiger Netzbetrieb auch außerhalb der normalen Dienstzeiten sollte sichergestellt werden. Die Möglichkeiten einer Rufbereitschaft wurden gemeinsam mit der Zentralverwaltung geprüft. Aus personellen Gründen ist aber die Einrichtung einer Rufbereitschaft derzeit nicht möglich.