NETZ-Konzept

- Vernetzung
- Netzentwicklungsplan
- Netzbetrieb und Management

für die
Ruhr-Universität Bochum

März 2009

1. NETZKONZEPT

1.1. GRUNDSÄTZE

ANGESTREBTE ZIELE

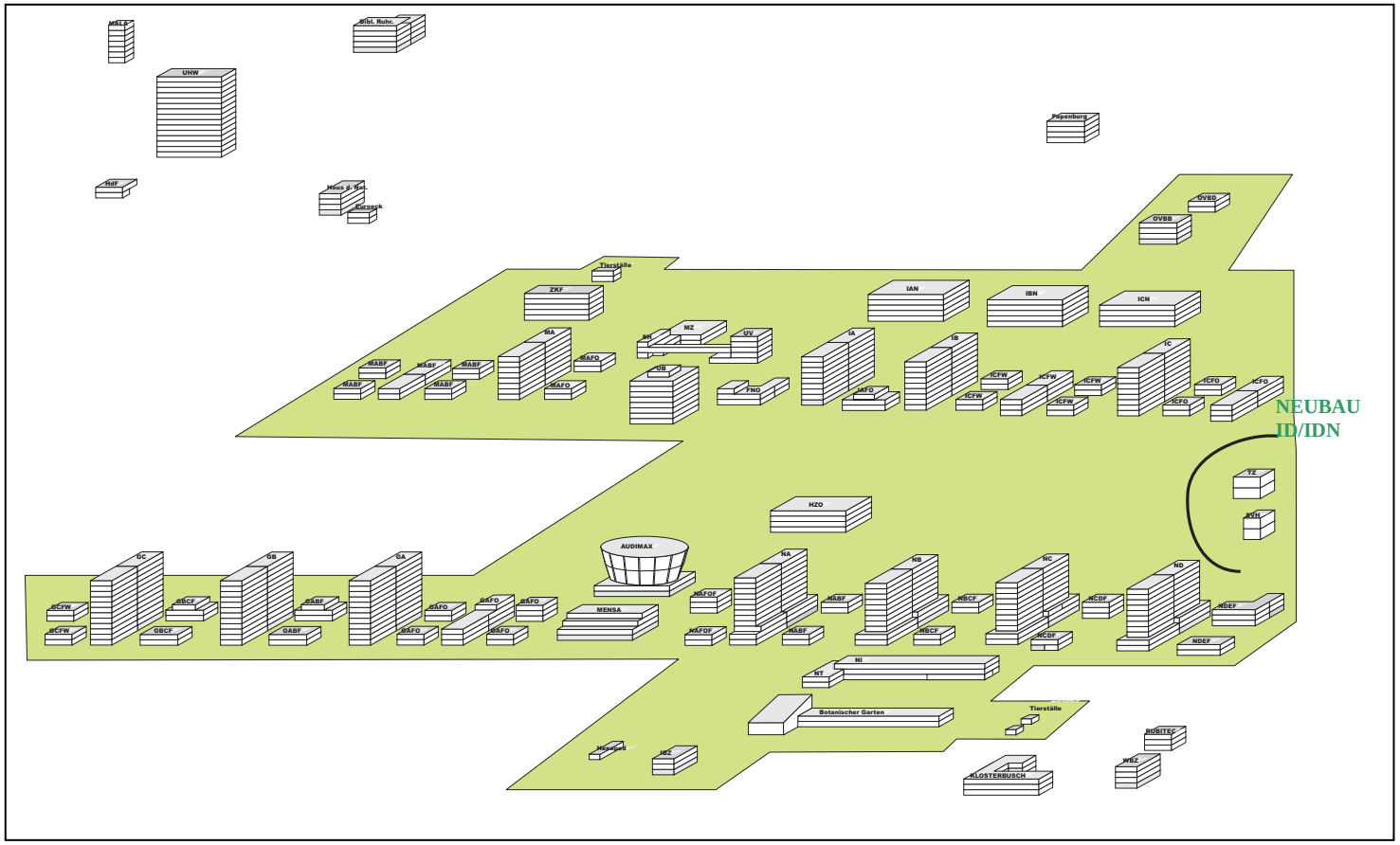
Die Vernetzung der Ruhr-Universität Bochum wird als *infrastrukturelle Voraussetzung* nicht nur in der wissenschaftlichen Arbeit am Arbeitsplatz des Wissenschaftlers, sondern ebenso in den Bereichen der Verwaltung und des technischen Betriebs aufgefasst. Es ist ein Kommunikationsinstrument, das als *Basiswerkzeug* für (vernetzte) Arbeitsabläufe dient.
In dieser Weise dient es der Forschung und der Ausbildung der Studierenden, wobei die Einbeziehung auch von deren häuslichen Arbeitsplätzen in die Kommunikationsinfrastruktur eines besonderen Augenmerks bedarf.
Ziel ist es daher, an allen Arbeitsplätzen in der Universität eine Kommunikationsinfrastruktur bereitzustellen, die es ermöglicht, ohne zusätzlichen Installationsaufwand vernetzte Arbeitsplätze ad hoc – eingebunden in eine Netzumgebung – zu konfigurieren und in Betrieb zu nehmen.
Die benötigten Kommunikationskapazitäten im lokalen Bereich (z.B. Lehrstühle) und im inner-universitären Dienstangebot (zentrale Server) müssen skalier- und erweiterbar gestaltet werden, wobei auch für anspruchsvollere Anwendungen genügende Übertragungskapazität bereitstellbar sein muss.
Für den Anwender muss gleichzeitig dafür Sorge getragen werden, dass eine einfache Nutzung möglich ist, wobei den Anforderungen nach Datenschutz und Datensicherheit Rechnung zu tragen ist.
Vernetzung und Kommunikation sind jedoch nicht erschöpfend durch die reine Datenübertragung beschrieben, sondern werden erst durch die Netzdienstleistungen, die innerhalb und außerhalb des lokalen Netzes als „Mehrwert“ angeboten werden, mit Leben erfüllt. Neben den heute üblichen Standarddienstleistungen von Email und WWW, multimedialen Angeboten, Verzeichnis- und Informationsdiensten ist es Aufgabe der Universität, dieses Angebotsspektrum weiterzuentwickeln und seinen Angehörigen anzubieten.
Es ist offensichtlich, dass der Ausbau und die Entwicklung der Kommunikationsinfrastruktur ein *strategisches Ziel* der Ruhr-Universität Bochum ist, und daher mit der entsprechenden Priorität behandelt wird.

1.2. GRUNDDATEN: DATEN ZUR RUHR-UNIVERSITÄT

ART UND GRÖßE DER HOCHSCHULE

Die Ruhr-Universität Bochum ist eine Campus-Universität, in der sich der Kernbereich durch eine besondere Nähe der einzelnen Baulichkeiten auszeichnet.

Dabei sind vernetzungstechnisch die Kernbereiche, die mittels Glasfaserstrecken (< 2 km) über Universitätsgelände erreichbar sind, im folgenden Aufriss gekennzeichnet und dunkel unterlegt.



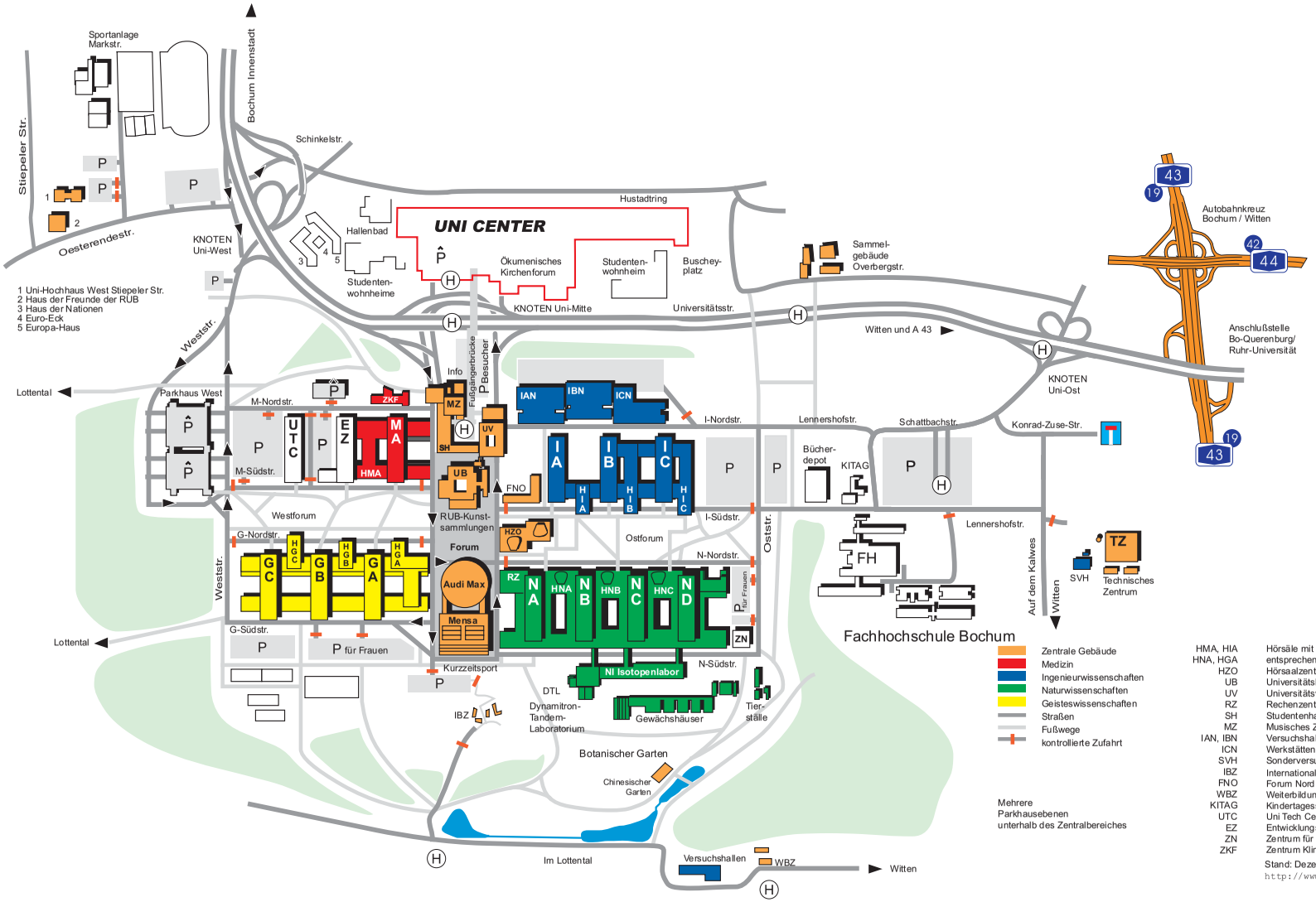
Die Baulichkeiten im Kernbereich der Universität sind durch Versorgungskanäle erschlossen, so dass die Verbindung untereinander technisch leicht durch verlegte Glasfaserleitungen zu bewerkstelligen ist.

Baulichkeiten außerhalb der hinterlegten Fläche sind nur über angemietete Leitungen, bzw. teilweise über vorhandene Telefonleitungen anschließbar.

Historisch liegen die Fachbereiche der Universität geordnet in verschiedenen baulichen Teilbereichen:

M-Gebäude:	Medizin
I-Gebäude:	Ingenieurwissenschaften
G-Gebäude:	Geisteswissenschaften
N-Gebäude:	Naturwissenschaften

wobei sich diese Aufteilung allerdings im Laufe der Jahre aufgrund sich geänderter Raumnutzungen und Kooperationen zwischen den einzelnen Fachbereichen immer weiter verwischt hat. Die „strenge“ Aufteilung in diese Fachgruppen wird sich im Rahmen der anstehenden Kernsanierung noch stärker vermischen. Die aktuellen Planungskonzepte sehen beispielsweise geisteswissenschaftliche Fakultäten in der I-Reihe.


Sportanlage Markstr.
Stiepeler Str.
Bochum Innenstadt
Schinkelstr.
Hustadtring
UNI CENTER
Hallenbad
Studenten-wohnheime
Oesterendestr.
KNOTEN Uni-West
Ökumenisches Kirchenforum
Studenten-wohnheim
Buschey-platz
KNOTEN Uni-Mitte
Universitätsstr.
Sammel-gebäude Overbergstr.
Witten und A 43
Autobahnkreuz Bochum / Witten
Anschlußstelle Bo-Querenburg/ Ruhr-Universität
KNOTEN Uni-Ost
1 Uni-Hochhaus West Stiepeler Str.
2 Haus der Freunde der RUB
3 Haus der Nationen
4 Euro-Eck
5 Europa-Haus
Weststr.
Lottental
Parkhaus West
M-Nordstr.
M-Südstr.
Info
Fußgängerbrücke
P Besucher
ZKF
MZ
SH
UV
UB
HMA
IAN
IBN
ICN
I-Nordstr.
I-Südstr.
Lennershofstr.
Schattbachstr.
Konrad-Zuse-Str.
Bücher-depot
KITAG
FNO
Westforum
RUB-Kunst-sammlungen
HZO
Forum
Ostforum
N-Nordstr.
Oststr.
G-Nordstr.
G-Südstr.
Audi Max
Mensa
RZ
HNA
HNB
HNC
ZN
P für Frauen
Kurzzeitsport
N-Südstr.
NI Isotopenlabor
DTL
Dynamitron-Tandem-Laboratorium
Gewächshäuser
Tier-ställe
IBZ
Botanischer Garten
Chinesischer Garten
Im Lottental
Versuchshallen
WBZ
Witten
FH
Fachhochschule Bochum
Auf dem Kalwes
SVH
TZ
Technisches Zentrum
Zentrale Gebäude
Medizin
Ingenieurwissenschaften
Naturwissenschaften
Geisteswissenschaften
Straßen
Fußwege
kontrollierte Zufahrt
Mehrere Parkhausebenen unterhalb des Zentralbereiches
HMA, HIA Hörsäle mit
HNA, HGA entsprechender Zuordnung
HZO Hörsaalzentrum Ost
UB Universitätsbibliothek
UV Universitätsverwaltung
RZ Rechenzentrum
SH Studentenhaus
MZ Musisches Zentrum
IAN, IBN Versuchshallen und
ICN Werkstätten
SVH Sonderversuchshalle
IBZ Internationales Begnungszentrum
FNO Forum Nord Ost
WBZ Weiterbildungszentrum
KITAG Kindertagesstätte
UTC Uni Tech Center
EZ Entwicklungszentrum an der RUB
ZN Zentrum für Neuroinformatik
ZKF Zentrum Klinische Forschung
Stand: Dezember 2000
http://www.ruhr-uni-bochum.de/Daten-Lageplan/

1.3. RUHR-UNIVERSITÄT BOCHUM PORTRÄT

Ein Darstellung zur Art, Größe und Struktur der Hochschule ist im Anhang A beigefügt. Der dort vorliegende Text entstammt dem „Abschlussbericht des Expertenrat im Rahmen des Qualitätspakts“ vom 20.2.2001 und stellt ausführlich die einzelnen Fakultäten und Bereiche der Ruhr-Universität Bochum dar.

1.4. MENGENGERÜST

RÄUME UND PORTS

In der Form der Datenstrukturierung, wie sie auch für die Veröffentlichung „Campus-Online zum Aufbau lokaler Hochgeschwindigkeitsnetze in den Hochschulen des Landes Nordrhein-Westfalen“ durch die Netzagentur NRW erfasst wurden, lauten die Bedarfszahlen auf der Raumbasis:

AKTUALISIERTE IST-ZAHLEN (STAND MÄRZ 2009)

Räume in Hauptnutzungsflächen	**Anzahl Räume**	***vernetzte Räume***			
		Mit Kategorie 5 TP-Verkabelung	*Aktive Ports*	*davon mit LWL Multimode*	*Summe davon mit Verkabelung*
Büros / Laborräume[1]	6530	*6206*		*10*	*6206*
Vorlesungs-, Seminarr.	510	*510*		*29*	*510*
Räume für PC-Pools	39	*39*		*0*	*39*
Summe	7079	*6755*	*30800*	*39*	*6755*

NUTZERZAHLEN, NUTZERGRUPPEN (MITARBEITEN STUDENTEN FORTZUBILDENDE)

Die Hochschule hat ca. 33.000 Studierende und insgesamt ca. 4.800 Beschäftigte in den verschiedenen Berufsgruppen. Allen Nutzern wird eine Zugangskennung zugewiesen.

Die Studentenwohnheime (ca. 4.200 Wohneinheiten) im Umfeld der Ruhr-Universität sind in den letzten Jahren ebenfalls strukturiert verkabelt worden und sind mittels Glasfaserleitung mit dem Netz der Universität verbunden.

1.5. NETZDIENSTE

VORHANDENE BASIS-NETZDIENSTE

Die im Umfeld einer Universität zu findenden normalen Netzdienste beinhalten die klassischen Internet-Dienste wie Email-, Domain-Name-Service zentrale FTP, NEWS und WWW-Server, wobei allen Angehörigen der Universität die Nutzung dieser Dienste offen steht.
Allen Angehörigen der Universität steht die Nutzung von zentralen Mailboxen und WWW-Speicher, sowie die Einwahlmöglichkeit über DSL/Telefon zur Verfügung, um etwa innerhalb eines VPN-Tunnels auch von zuhause oder vom Wohnheimplatz „innere“ Dienste (z.B. Datenbanken) zu nutzen.

VORHANDENE NETZDIENSTE

Als „besondere“ Dienste sind zu vermerken:

- **UMS – unified messaging services**
  Die originären Telekommunikationsdienste, FAX- und Voice-Mail-, Ansagedienste (Voice on demand), sind durch die Integration der neuen TK-Anlage in das Datennetz sowohl über das LAN als auch über Telefonzugang nutzbar.
- **E-Learning, Informationsdienste, Online-Kursangebote**

[1] Vergleichszahl: 5970 Räume der Universität besitzen einen betriebsbereiten Telefonanschluss.

Durch die verschiedenen Anbieter, wobei herausgehoben das Rechenzentrum und die Universitätsbibliothek zu nennen sind, werden diverse Informationsangebote (z.B. digitale Bibliothek) bereitgestellt.
Insbesondere wird durch Kurssysteme (Blackboard) ein Rahmen geschaffen, in dem die Einbringung von Online-Kursangeboten durch ein entsprechendes „content management“ und eine integrierte Kursverwaltung erleichtert wird,.

- **„freier“ Netzzugang - „lock-and-key“**
  An frei zugänglichen Netzanschlusspunkten besteht die Möglichkeit, sich mit mitgebrachten Laptops in das Datennetz der Ruhr-Universität einzuklinken. Dazu erfolgt vor der Freigabe von zulassenden Filtern eine Validierung der Benutzer über Login-Id und Passwort.

ANGESTREBTE UND WEITER ZU ENTWICKELNDE NETZDIENSTE

Dienstleistungen, die bei fortschreitender Bereitstellung von Übertragungskapazität weiter zu entwickeln sind:

- **File- und Archivierungssysteme,**
  File- und Archivierungssysteme auf der Basis von vernetzten Band-Robotern sind fester Bestandteil des administrativen und Dienstleistungsbereich (Rechenzentrum, Verwaltung, Bibliothek) zur Datensicherung.
- **Dokument-Management-Systeme**
  Ein Dokument-Management im Spezialfall eines „Content Management“ für Kurse ist - wie oben erwähnt - bereits jetzt verfügbar. Im Hinblick auf die Zielperspektive, ein allgemeines Dokument-Management zur kompletten elektronischen Dokumentverwaltung nicht nur für Verwaltungs- sondern auch für die Abläufe der Forschung und Lehre anzubieten, sind noch erhebliche Investitionen notwendig.
- **Video-Übertragungskapazität** (garantierte Bandbreite)
  insbesondere auf der Basis von Multi-Mediaangeboten. Im letzteren wird insbesondere durch die zukünftige Einbindung der Arbeitsplätzen in den meisten Studentenwohnheimen ein erhöhtes Nutzungspotential vorhanden sein.
- **Security-Management**
  Gleichzeitig ist auf der Basis von Chipkartentechnologie das Sicherheitsmanagement im Netz ausgebaut, um Authentifzierung und gesicherte Datenübertragung auf der Basis eines vorhanden zentralen Verzeichnisdienstes („RUBIKS“)- und Zertifizierungsdienstes zu erlauben.

1.6. VORHANDENE UND ANGESTREBTE NETZSTRUKTUR

BENUTZERSICHT

Aus der Sicht des Anwenders werden die folgenden prinzipiellen Anschlusstypen mit ihren grundsätzlichen Eigenschaften beschrieben:

a) Netzanschluss am Arbeitsplatz (Büro / Labor)
Am Arbeitsplatz findet der Benutzer eine Datensteckdose (anzustrebender Standard heute: Twisted Pair 100/1000 Mbit/s autosensing) vor, an dem er seinen Rechner, der Teil eines lokalen (Lehrstuhl-)Netzes, ist betreiben kann, wobei vorher die notwendigen Konfigurationen seines Rechners (IP-Adresse, Gateway, Netzmaske etc) vollzogen wurden.
Die Datensteckdosen der betreffenden Räume eines Bereiches (Lehrstuhl) bilden ein Netz (technisch gesprochen eine „broadcast domain“), in dem alle Rechner an jeder Datensteckdose dieses Netzes ohne Konfigurationsänderung betrieben werden können.
Wird der Rechner in einen anderen Lehrstuhl, das heißt in ein anderes Netz transferiert, so ist der Rechner entsprechend umzukonfigurieren.
Wird ein Raum, das heißt die Netzanschlüsse dieses Raumes, einem anderen Netz zugeordnet, so geschieht dies durch Konfiguration der aktiven Netzkomponenten zentral durch das Rechenzentrum.
Authenfizierung und Validierung der Zugriffe an diesem Rechner unterliegen dem Management und der Verantwortung des Benutzers bzw. des lokalen Betreibers von Servern in dem lokalen Netzwerk.

b) Netzanschluss in einer Computer-Insel
Die Datenanschlüsse einer Computer-Insel befinden sich in einer besonderes vorbereiteten Umgebung. Der einzelne Arbeitsplatz wird mit 100/1000 Mbit/s geswitchten Twistend-Pair-Anschlüssen ausgestattet. Da der Arbeitsplatz keinem Anwender persönlich zugeordnet ist, erfolgt eine Authentifizierung und Validierung innerhalb der Softwareumgebung, wobei als zusätzliche Absicherungsmechanism „lock-and-key“ und die feste Zuordnung der Geräte-MAC-Adressen zu den Datensteckdosen zur Verfügung stehen.
Langfristig wird eine standardisierte Einbeziehung einer Chipkarten gestützten Authenfizierung vollzogen.

c) Netzanschluss in einem Hörsaal
Anschlüsse in den Hörsälen werden ebenfalls mit 10/100/100 Mbit/s, zusätzlich mit LWL ausgestattet. Da die Anschlüsse frei zugegänglich sind, bedeutet dies, dass hier eine Authenfizierung vor der Nutzung des Netzes stattzufinden hat.

Die datentechnische Ausstattung auf der Netzwerkseite ist mit der rechnergestützten Ausstattung (z.B. Laptop und Beamer, Beschallung) konzeptionell zu integrieren, um lange und umständliche Rüstzeiten zu vermeiden. („IT-Präsentationspult“)
Als zusätzliche Dienstleitung wird in Hörsälen und Seminarräumen eine Funk-LAN-Unterstützen zusätzlich angeboten.

d) vernetzter „Kiosk-„Arbeitsplatz

Die typischen „Kiosk“-Arbeitsplätze finden wir in Bibliotheken, an denen in einer vorbereiteten Software-Umgebung bestimmte eingeschränkte, aber dedizierte Anwendungen beispielsweise für Recherchen zur Verfügung gestellt werden.
Die netztechnische Ausstattung soll auch hier eine Twisted-Pair-Lösung mit 100/1000 Mbit/s an Switchen sein.

e) frei nutzbarer Netzanschluss im Campus („H.I.R.N-Port“)

Neben vernetzten Arbeitsplätzen in CIP-Inseln, „Kiosk“-Arbeitsplätzen mit einer vorbereiteten Umgebung ist es sinnvoll, gerade Studierenden die Anschlussmöglichkeit für eigene mitgebrachte Rechner zu bieten (Laptops), die an „freien“ Netzwerksteckdosen angeschlossen werden können, an denen neben einem 10/100/1000 Mbit/s Twisted-Pair-Anschluss lediglich noch eine Stromversorgung und entsprechender Arbeitsplatz angeboten werden.
Vor Zulassung des Datenverkehrs findet eine Authenfizierung des Anwenders statt. Jeder Student der Ruhr-Universität Bochum besitzt einen bereits bei der Immatrikulation vergegebenen Account, so dass nach der Validierung durch öffnende Filter im Router der Zugang ins hochschulinterne Rechnernetz freigegeben wird.

f) „Heimarbeitsplatz“ Wohnheim

Der Anschluss der Arbeitsplätze in Studentenwohnheimen bedeutet die Verbindung des lokalen Wohnheimnetzes mit der Ruhr-Universität Bochum. Dies bedeutet in der Praxis, dass die Arbeitsplätze in den Wohnheimen logisch Bestandteil des Datennetzes der Universität werden. Da die Verwaltung der Räumlichkeiten der Wohnheime nicht durch die Universität erfolgt, ist auch hier für den Datenübergang in Hochschulnetz eine Absicherung über „lock-and-key“ vorgesehen.
Da der Adressraum mit offiziellen IP-Adressen eine weltweit extrem knappe Resource ist, und auch die Universität den ihr zugeteilten Adressraum streng bewirtschaftet, ist bei der Vielzahl von Anschlüssen nicht zu vermeiden, mit NAT (network adress translation) zu arbeiten. Im Wohnheimnetz wird mit lokalen, nicht weltweit gerouteten IP-Adressen gearbeitet. Erst beim Übergang ins Universitätsnetz werden dynamisch offizielle Adressen aus dem IP-Adressraum eingesetzt.

g) „**Heimarbeitsplatz“ @home**

Die Universität unterstützt die Einwahl in das Universitätsnetz über gebräuchte Einwahltechniken (Analog, ISDN, DSL), wobei zur Absicherung und Identitätsprüfung VPN-Tunnel sowie Chipkarten verwendet werden.

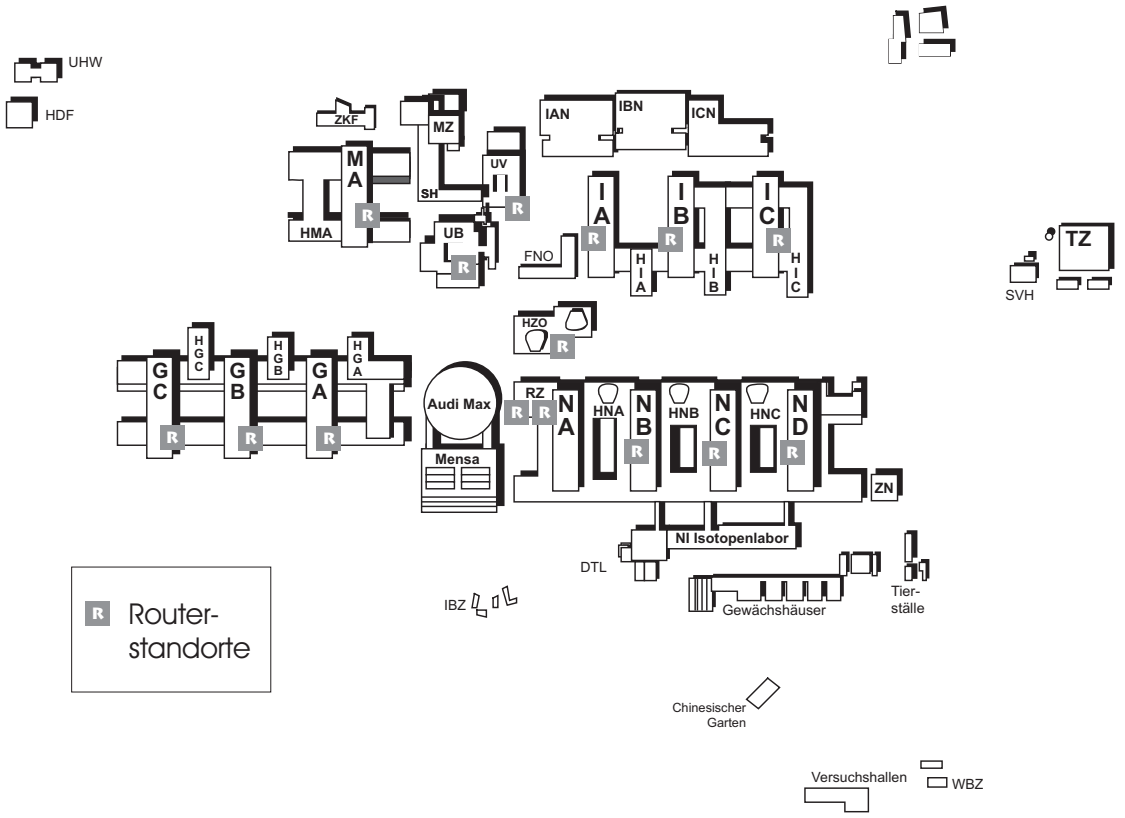
VERKABELUNG (TOPOLOGIE, KABELTYPEN)

Die baulichen Randbedingungen der Universität haben signifikanten Einfluss auf die Ausgestaltung der Netzwerktopologie.

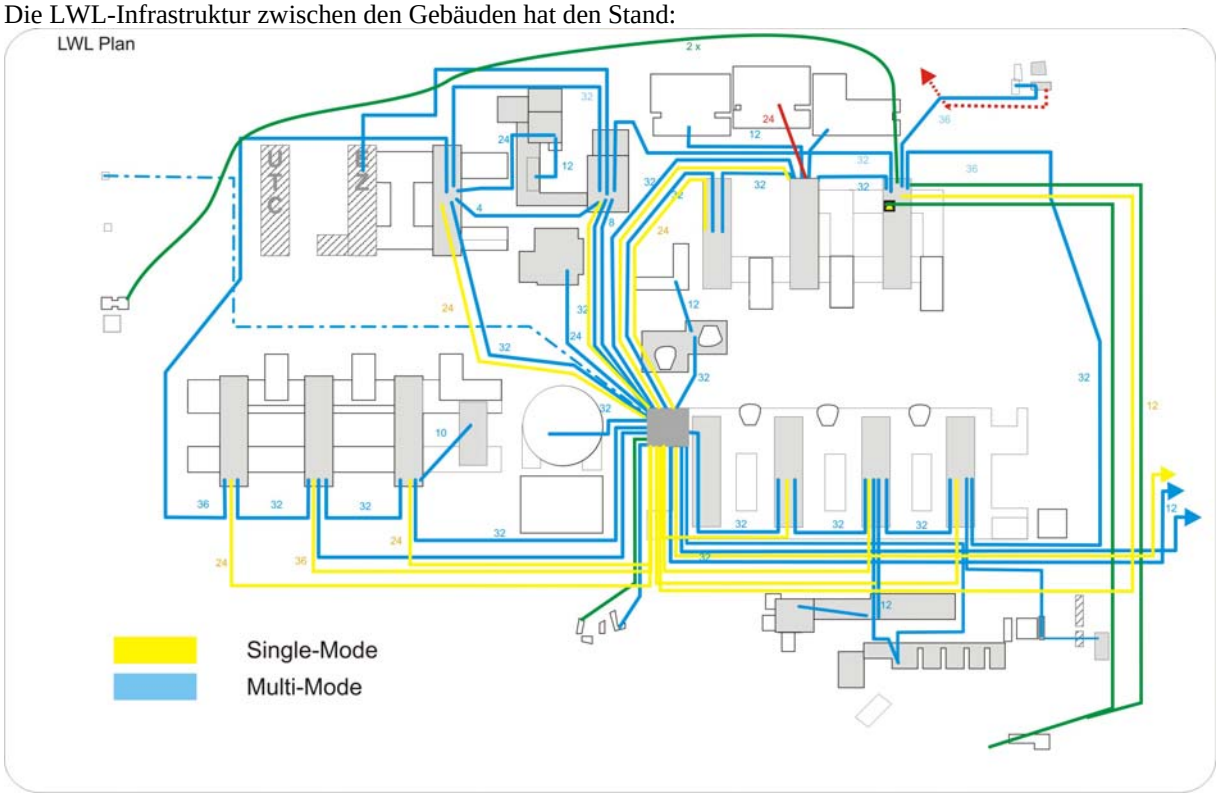
Backbone

Es ist offensichtlich, dass der typische Backbone zwischen den Gebäuden und der Zentrale (Rechenzentrum, Gebäude NA) geführt wird, wobei hierbei jeweils Glasfaserverbindungen von den zentralen Routern zu den Router in den Gebäudehauptverteilern geführt werden.
Zur Zeit werden Single- und Multi-Modefasern verwendet, wobei als Übertragungsprotokolle noch in geringem Umfang ATM mit 155 und 622 Mbit/s als auch 100 Mbit/s Ethernet verwendet werden, in Normalfall kommt allerdings 1000 Mbit/s Ethernet zum Einsatz. Das Ziel ist es, die Übertragungsgeschwindigkeit im Backbone-Bereich auf 10 Gbit/s aufzurüsten.

Die Topologie zwischen den Baulichkeiten hat die folgende Gestalt:

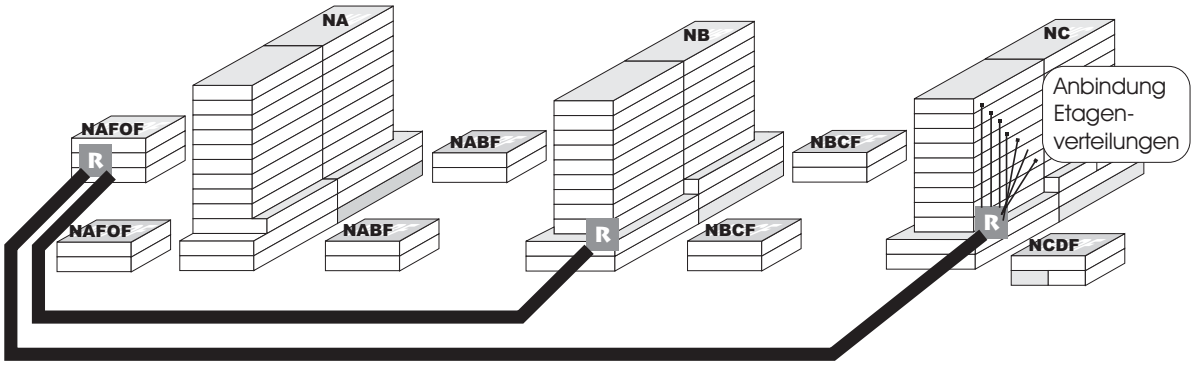


Die LWL-Infrastruktur zwischen den Gebäuden hat den Stand:



SEKUNDÄR-VERKABELUNG

Die Verbindung der Router zu den Etagenverteilern erfolgt über Multi-Modefaser. In den Etagenverteilern sind managebare Switche, VLAN- und Clusterfähig, mit einer skalierbaren Zuleitungskapazität vorgesehen (mehrere Ethernet Channel, Aufrüstbarkeit auf ATM oder Gigabit-Technolgie).



LWL-Verbindung: zentraler Router Rechenzentrum zum Gebäude Router

nach Anforderung:
ATM 155/622 Mbit/s
Ethernet 100 Mbit/s
Ethernet 1000 Mbit/s

TERTIÄRE VERKABELUNG

Der tertiäre Verkabelungsanteil wird als Twisted-Pair-Installation Kategorie 6 verlegt. Dies geschieht in den Hochgebäuden für jede Etage von jeweils 2 Verteilerstandorten im Norden und Süden eines Gebäudes. In den Flachbereichen typischerweise von einem Standort je Etage aus.
Es wird angestrebt, diese Verteilerstandorte immer in Bereichen der Gebäudetechnik unterzubringen, um Konflikte durch Mitnutzung eines Benutzerraumes zu vermeiden.
Die Installation der Tertiärverkabelung unterliegt in Bochum besonderen baulichen Erschwernissen, da aus den „Bausünden“ der Vergangenkeit, Asbestbelastung und nicht mehr nutzbare Versorgungswege, sich die Notwendigkeit erweist, praktisch überall neue Versorgungswege durch die Installation von Kabel- und Brüstungskanälen vorzuhalten. Dabei ist ein hoher Aufwand für brandgeschützte Kanäle erforderlich wegen der häufigen Notwendigkeit Flurbereiche, die früher als Versorgungswege nutzbar waren, mindestens zu queren..
Die Installation neuer Kabelkanäle in den Räumen hat allerdings den Vorteil, dass bei einer zukünftigen Nachinstallation von LWL-Infrastruktur nutzbare Versorgungswege vorhanden sind, und somit eine schnelle Ausführung ohne große bauliche Maßnahmen möglich ist.
Die Entscheidung, vorerst keine Verkabelung „Fiber to the desk“ zu installieren, ist dadurch begründet, dass

a) es aufgrund der Längenrestriktionen möglich ist, großflächige Bereiche mit einer Vielzahl von Anschlüssen ohne negative Einflüsse aufgrund von Fremdeinstrahlung mit einer TP-Installation zu versorgen
b) die Zukunftssicherheit der LWL-Kabeltypen für die verschiedenen Übertragungsgeschwindigkeiten nicht gegeben ist und
c) heute ein hoher finanzieller Aufwand für zusätzliche Umsetzer im Endkundenbereich notwendig wäre, ohne dass damit ein höherer Nutzen erreicht würde
d) auch der Umgang mit einer TP-Installation für den Anwender als einfacher erachtet wird.

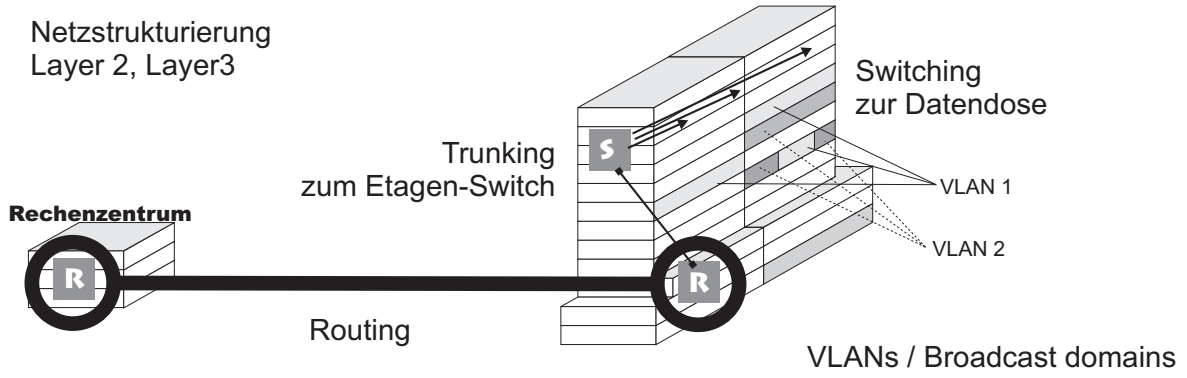
Bei der Installation von neuen Kabeltrassen wird möglichst gleichzeitig eine Trennung des DV-Elektronetzes von den anderen Stromkreisen durch die zusätzliche Einbringung neuer Stromkreise angestrebt („grüne DV-230 V Steckdosen“).

NETZSTRUKTURIERUNG (ROUTER, LAYER 3)

Das Netz hat von der Struktur die Gestalt, dass zwischen den Gebäuden gerouteter Datenverkehr (Layer 3) stattfindet, wobei die Übertragung je nach Randbedingung über

- Ethernet (1 Gbit/s, 10 Gbit/s)
- Ethernet (1 Gbit/s, 10 Gbit/s), als Trunk (VLANs nach 802.1q)
- Abzulösen, noch in wenigen Bereichen: LANE (LAN Emulation) über ATM (155 Mbit/s oder 622 Mbit/s)

erfolgt.
Die Randbedingungen ergeben sich aus der Notwendigkeit, ein lokales Netz (broadcast domain) transparent in ein anderes Gebäude mittels VLAN zu übertragen.
Eventuelle notwendigen Bandbreitengarantien (Backup-Dienste) werden bei über mehrere Verbindungen bzw. QOS-Mangement bereitgestellt.
Daher geschieht es durchaus, dass aus Optimierungsgründen mehr als eine Verbindung zwischen zwei Komponenten geschaltet wird.



Die Verteilung der Router über mehrere Gebäude bietet zusätzlich den Vorteil, dass Filterfunktionen (Firewall), lokal in den Bereich, wo sie gewünscht werden, ohne zentrale Maschinen zu belasten, durchgeführt werden können.

ETAGENSWITCHE (LAYER 2), VLANS

In den Etagen wird der Datenverkehr über evtl. kaskadierte, geclusterte VLAN-fähige Switche (802.1q) auf die einzelnen Netze verteilt.
Eine Verwendung von „shared Media“ Geräten (Hubs) verbietet sich schon aus Gründen des Datenschutzes zur Vermeidung der Mithörfähigkeit des fremden Datenverkehrs.
Diese Form der Strukturierung hat den Vorteil, dass ohne manuelles Patching die Zuordnung einer Dose zu einem Netz als reiner Managementvorgang von zentraler Stelle aus vollzogen werden kann.
Dies ist unbedingt notwendig, da die räumliche Verteilung von Lehrstühlen über nicht benachbarte Räume immer mehr zum Standard wird. Eine Zusammenführung durch physische Verkabelung mittels reinem Auflegen auf Patchfelder wäre nicht nur extrem personal- und zeitaufwendig, sondern häufig auch nicht mehr durchführbar, und führte in der Vergangenheit immer wieder zu nicht wünschenswerten Zerlegungen von Lehrstuhlnetzen in mehrere Subnetze.

Zusätzlich ist die gesamte Konfiguration revisions- und dokumentationsfähig.

Eine Selbstverständlichkeit ist in diesem Zusammenhang, dass die Komponenten via SNMP fernverwaltbar sein müssen, da sie sonst gegenüber dem Netzwerkmanagement „unsichtbar“ wären.

1.7. ÜBERLEGUNGEN ZUR NETZINTEGRATION

ZUSAMMENFÜHRUNG VON WISSENSCHAFTSNETZ, VERWALTUNGSNETZ UND TELEFONETZ

Die Vernetzung der Ruhr-Universität Bochum wird in den Bereichen LAN und klassische Telekommunikation höchst integrativ behandelt.

Es wurde bereits seit 1998 bei der Neugestaltung der Telefonanlage der Ruhr-Universität in einer hohen Zusammenarbeit zwischen den Betreibern der Telefonanlage und dem Rechenzentrum während der Konzeptionierungs- und Installationsphase zusammengearbeitet. Das Kommunikationsnetz der Telefonanlagen ist Bestandteil des Datennetzes.

Insbesondere unter dem Gesichtspunkt der „Mehrwertdienste“ (UMS = „unified messaging systems“), die dem Anwender neben dem klassischen Telefonieren die Zusatzdienstleistungen, wie zentrale Fax-, Voice-Mail und Ansagedienste integriert mit dem Email-System der Universität bieten, ist die Trennung zwischen TK und LAN in der Praxis schon aufgehoben.

Der mittelfristig anstehende Ersatz der bestehenden Telefonanlage wird sich auf das vorhandene Datennetz mittels Voice-Over-IP stützen und die Datenkommunikationsinfrastruktur mitnutzen.
Der Ersatz der Leitungsinfrastruktur, der bei der Kernsanierung der RUB unvermeidlich sein wird, wird in Zukunft auf einer einheitlichen Leitungsstruktur beruhen. Der lokale Anschlussport kann dann zur Nutzung für Datenendgeräte bzw. Telefone verwendet werden.

2. NETZENTWICKLUNGSPLAN

2.1. RANDBEDINGUNGEN

BAULICHE RANDBEDINGUNGEN – ASBEST, BRANDSCHUTZ, INFRASTRUKTURRENOVIERUNG

Die Ruhr-Universität Bochum hat in der vorhandenen Bausubstanz erhebliche Probleme. Diese sind einerseits in der Asbestproblematik begründet, andererseits durch veränderte Brandschutzvorschriften, die mit der topologischen und architektonischen Gestaltung der Universität nicht unbedingt kompatibel sind. Daraus ergeben sich erhebliche Schwierigkeiten in der Bereitstellung und Neueinbringung von Versorgungswegen, wie Kabeltrassen. Daneben sind auch eine Reihe anderer baulicher Bestandteile renovierungsbedürftig (z.B. Klima- und Energietechnik), wobei diese anstehenden Sanierungsmaßnahmen eigentlich für Datentechnik nutzbare Flächen zunächst blockieren.

Dies bedeutet leider, dass in einigen Bereichen vorübergehend mit provisorischen Maßnahmen gearbeitet werden musste und auch immer wieder muss, um zunächst Vernetzungsinfrastruktur überhaupt bereit stellen zu könnenn.

Die anstehende Sanierung des Campus wird in den nächsten Jahren eine grundsätzliche Neugestaltung der Netzinfrastruktur nachsichziehen. Dies bedeutet allerdings gleichzeitig, dass während der Umbau und Umgestaltungsphasen eine hohe Flexibilität (Umzüge!) unabdingbar ist.

MANAGEMENT DES NETZES WÄHREND DES AUFBAUS

Das zu installierende Netz ist in einer Technologie so gewählt, dass der spätere Pflegeaufwand zu minimieren ist. Insbesondere bedeutet dies, dass so wenig Arbeiten wie irgend möglich vor Ort erledigt werden sollten. Dies bedeutet, dass nur vollverwaltbare Komponenten beschafft und installiert werden.
Das gesamte Netz wird zentral durch die Netzabteilung des Rechenzentrums verwaltet.
Die Aufbauarbeiten des Netzes geschehen koordiniert und auf Vorgaben des Rechenzentrums, so dass bei Fertigstellung von Etagenteilen sofort eine Inbetriebnahme der neu installierten Netzinfrastruktur erfolgen kann.
Während der Umstellungsphase wird angestrebt, für kurze Zeit noch einen parallelen Betrieb zwischen alter und neuer Infrastruktur anzubieten, um eine weiche Umstellung zu erlauben.
Bei der Inbetriebnahme neuer Netzteile werden diese sofort in die Verwaltungs- und Überwachungssysteme des Netzwerkmanagements eingebunden, so dass die neuen Teile zu diesem Zeitpunkt vollständig in das Netz integriert sind.

2.2. REALISIERUNGSPRIORITÄTEN

Netzinfrastruktur wird heute an jeder Stelle der Universität gebraucht. Die jetzigen Auf- und Ausbaumaßnahmen dienen im wesentlichen der Qualitätssteigerung (höhere Geschwindigkeiten) bzw. der Schaffung weiterer Kapazitäten die durch erhöhte Nachfrage (mehr Anschlüsse) bedingt sind.

Die Reihenfolge der einzelnen Maßnahmen ist stark extern gesteuert durch laufende Sanierungs- und Umbaumaßnahmen, die die Termine diktieren.

Absolute Priorität hat natürlich bei einer laufenden Baumaßnahme die Ausstattung eines Neubaus durch eine geeignete Netzinfrastruktur. Die passiven Komponenten, dass heißt die strukturierte Glasfaser- und Twisted-Pair-Infrastruktur ist Bestandteil der Baumaßnahme, wird also mit der Übergabe eines neuen oder kernsanierten Gebäudes bereitgestellt.
Die Bereitstellung der aktiven Komponenten (Switche und Router etc) ist die Aufgabe des Nutzers Universität. Diese sind also Bestandteil des Netzentwicklungsplan.

Zum jetzigen Zeitpunkt ist der Neubau der Gebäude ID und IDN begonnen. Der Neubau des Gebäudes der Sportwissenschaften ist in der Planung. Der Start in die Kernsanierung der anderen Gebäudereihen ebenfalls.

2.3. EINORDNUNG DER BEANTRAGTEN MAßNAHMEN

Die in der vorliegenden Haushaltsunterlage beantragten Mittel sind zur kontinuierlichen Fortsetzung der laufenden Ausbaumaßnahmen notwendig, um eine vollständige und hochqualitative Vernetzung der Ruhr-Universität Bochum zu erreichen.

Zu Beginn der gesamten Vernetzungsmaßnahmen war seinerzeit gängige Übertragungstechnik installiert worden, um überhaupt den Anschluss der einzelnen Baulichkeiten im Kernbereich, wenn auch mit niedriger Übertragungskapazität, zu ermöglichen. Dazu waren erste Glasfaserstrecken zu den Gebäuden und innerhalb der Gebäude Backbone-Leitungen mit 10base5-Technologie in provisorischer Verlegung installiert worden, die inzwischen ersetzt wurden. An diese haben sich Lehrstühle, vielfach eigenfinanziert, mit 10base2-Infrastruktur und eigenen Routern, teilweise auf PC-Basis, angeschlossen. Diese Koax-basierte Infrastruktur ist heute entfernt bzw. stillgelegt.

In den folgenden Bauabschnitten sind die Verbindungen zu den Gebäuden und die dort installierten Gebäude-Router erweitert worden. Insbesondere wurde mit der Installation der Etagenverteiler und deren Anbindung an die Gebäudeverteiler mittels Glasfaser fortgefahren. Der Ausbau des Primär- und Sekundärnetzes ist weitestgehend abgeschlossen. Das Datennetz ist gegenwärtig so mit aktiven Komponenten bestückt, dass die vernetzten Bereiche mit 10/100 Mb/s Twisted-Pair-Infrastruktur betrieben werden können.

Zum jetzigen Zeitpunkt liegt eine flächendeckende, aber nicht immer ausreichende Ausstattung vor.

Von vornherein ist auf die Verfügbarkeit von Netzwerkmanagement-Fähigkeiten Wert gelegt worden, um eine ausreichende Netzwerküberwachung der vom Rechenzentrum verantworteten aktiven Komponenten zu gewährleisten.

2.4. MAßNAHMEN ZUR FORTSCHREIBUNG DES NETZKONZEPTES

Die Maßnahmen zur Vernetzung werden in den Gremien der Universität, sowohl Rektorat als auch dem Beirat des Rechenzentrums diskutiert und beraten.

2.5. MIGRATIONSPLÄNE

ERTÜCHTIGUNG ALTER STRUKTUREN

Alte Netzinfrastruktur (Cheapernet) ist wie oben erwähnt prkatisch nicht mehr vorhanden. Allerdings sind viele Bereich, die zu Beginn strukturiert verkabelt werden nach heutiger Sicht lediglich mit CAT5-Verkabelung, das heißt nur 100 Mbit-Fähigkeit und vergleichsweise geringen Anschlusszahlen ausgestattet.

Es ist Ziel, die Aufrüstung des Netzes gemäß den Anforderungen in Qualität und Quantität durchzuführen.

2.6. ANGABEN ZU NUTZUNGSZYKLEN

AUSTAUSCH VON ELEKTRONIKKOMPONENTEN

Aus der Erfahrung, dass die ersten Router- und Hub-Generationen, die als elektronische Komponenten Verwendung fanden, inzwischen ausgetauscht wurden, ist bei den Nutzungszyklen eine maximale Betriebsdauer von 5 Jahren zu erwarten. Da im Gesamtinvestment zur Vernetzung der Kostenanteil der aktiven Komponenten sehr hoch ist und sich der Installationsprozess des Netzes über mehrere Jahre hinstreckt, werden am Ende der Installationsphase bereits die ersten Komponenten wieder auszutauschen sein..
In der Praxis werden noch brauchbare Komponenten häufig durch eine zweite Einsatzphase an einem anderen Einsatzort weiter verwendet, an dem die Leistungsanforderungen noch ausreichen.
Die zweite Ursache, die eine Außerbetriebnahme ökonomisch sinnvoll macht, sind die Höhe der laufenden Wartungskosten und die Möglichkeit durch Austausch und Ergänzung an den Geräten notwendige Änderungen überhaupt durchführen zu können. Leider ist es so, dass Hersteller wünschenswerte Softwareergänzungen in bestimmten Produktlinien nicht mehr einbauen und den Anwender damit zu Systemwechseln zwingen.

ALTERUNGSPROZESSE

Bei den passiven Komponenten sind durch Alterung bedingte Ausfälle zu erwarten.
Aus der Erfahrung heraus sind beispielsweise nach 5 bis 10 Jahren häufig Kontaktprobleme bei Cheapernet-Komponenten, korrosionsbedingt und alterungsbedingt, beobachtet worden.
Inwieweit gespleißte Glasfaserverbindungen durch Alterung des Klebermaterials Probleme machen werden, bleibt noch abzuwarten.
Im Netzkonzept des Jahres 2001 ist die Erwartung ausgesprochen worden, dass nach 5 Jahren erste alterungsbedingte Ausfälle auftreten, werden. Aus der Erfahrung heraus ist zu sagen, dass dies nach 7-8 Jahren verstärkt zu beobachten ist, insbesondere im Zusammenhang mit Stromab- und einschaltungen. Die Netzteile älterer Geräte werden dann sehr anfällig.

3. NETZBETRIEBS- UND MANAGEMENTKONZEPT

3.1. VERANTWORTUNG UND ZUSTÄNDIGKEIT

IST-ZUSTAND

Zur Zeit werden bei Lehrstuhlnetzen (IP-Subnetze, broadcast-domains) lokale „Netzbetreuer“ als Ansprechpartner benannt. Diese sind zuständig für die lokale Zuordnung von IP-Adressen aus einem vom Rechenzentrum überlassenen Adresspool zu den einzelnen Geräten der Einrichtung. Gleichzeitig sind die Netzbetreuer auch der erste Ansprechpartner seitens des Rechenzentrums im Falle von Störungen und Problembehebungen. Den lokalen Ansprechspartnern werden zum Managment durch die zentrale Netzverwaltung im Rechenzentrum administrative und operative Hilfsmittel zur Verfügung gestellt, die eingeschränkt auf ihren Verantwortungsbereich verwendet werden können.

SOLL-ZUSTAND

Die Betriebsverantwortung des Rechenzentrums für das Funktionieren einer LAN-Verbindung ist bei der Installation einer strukturierten, geswitchten Verkabelung bis zur Datensteckdose im Raum ausgedehnt. Gleichzeitig wird auch die Zuordnung einer Datensteckdose zu einem lokalen (Lehrstuhl-)Netz – mittels VLAN-Konfiguration – in zentraler Verantwortung erledigt.
Dies beinhaltet dann auch sämtliche Komponenten (Switche und Router) von zentralen Servern oder Zugangsroutern zum Internet bis hin zur lokalen Datensteckdose.

„SOLLBRUCHSTELLE“ FIREWALL

Jedem lokalen Netzinhaber (z.B. Lehrstuhl) steht es frei, einen eigenen Firewall zu betreiben, der den Datenverkehr zwischen dem inneren Netz und der Außenwelt filtert. Dazu werden zwei VLANs - ein inneres und ein äußeres Netz - und gegebenenfalls eine DMZ („demilitarisierte Zone“) konfiguriert.
Die Administration eines lokalen Firewall-Rechner verbleibt grundsätzlich bei der lokalen Einrichtung, sofern nichts anderes vereinbart wird oder die Firewall-Funktionalität auf zentralen Maschinen bereitgestellt wird.

PERSONEN

Die Aufrechterhaltung des Netzbetriebes des hochschulinternen Rechnernetzes („HIRN“) obliegt dem Personal des Rechenzentrums, insbesondere der Abteilung für das Rechnernetz.
Der Betrieb zentraler Dienstleistungen (Email-, WWW-, News-Server) ist innerhalb des Rechenzentrums organisiert.

DATENSCHUTZ- UND IT-SICHERHEIT

Die Ruhr-Universität hat durch die Bestellung von Datenschutz- und IT-Sicherbeauftragten auch eine organisatorische Grundlage für diese Belange geschaffen. Dadurch sind bespielsweise auch organisatorisch Meldewege und Dokumentationsvorgaben (z.B. Vorabkontrollen) wohldefiniert.
Die operativen Aufgaben der IT-Sicherheit eines Netzes obliegen der Netzabteilung.

3.2. ADMINISTRATION

Die Administration der zentralen Ressourcen obliegt dem Rechenzentrum. Dieses verwaltet die vorhandenen Kapazitäten, sowohl in den Übermittlungsbandbreiten, als auch die administrativen Resourcen, die sich beispielsweise durch Einschränkung im Umfang nutzbarer IP-Adressen ergeben.
Dabei wird weitgehend subsidiär verfahren:

IP-SUBNETZE

Das Rechenzentrum übergibt beispielsweise IP-Nummernbereiche an die einzelnen Lehrstühle, die diese dann in Eigenverantwortung ihren Geräte zuordnen können.
In regelmäßigen Abständen sind durch „Netzanmeldungen“ die Daten mit den Zuordnungen an das Rechenzentrum zurückzuführen, dies ist insbesondere dann sofort notwendig, wenn der Domain-Name-Service durch das Rechenzentrum als Dienstleistung und nicht über lokale Server erledigt wird.

DNS

Der DNS-Namensraum für die Subnetze an der Universität wird zentral vom Rechenzentrum verwaltet. Bei der Zuteilung bestimmter Bezeichnungen kommt im Normalfall das Windhund-Verfahren zum Einsatz – wie im globalen DNS-Verwaltungswesen auch.

BENUTZER

Alle Angehörigen der Universität erhalten bei Immatrikulation bzw. bei Einstellung eine Benutzerkennung für den Internetzugang am Rechenzentrum.

3.3. SICHERHEIT

ABGESTUFTES FIREWALL-KONZEPT

Neben den zentralen einfachen Port-Filtern, die bereits im Zugangsrouter zum GWiN bestimmte Ports ausfiltern, werden in der zweiten Stufe durch Port-Filter in den Gebäuderoutern weitere Feinabstimmungen ermöglicht.
Eine gewünschte Abschottung eines lokalen Netzwerkes geschieht durch einen lokalen Firewall, der den Datenverkehr filtert, bevor dieser in das innere VLAN gelangt.
Der Betrieb und die Verantwortung des Firewall obliegt dem Betreiber des lokalens Netzes.

SICHERER DATENVERKEHR ÜBER UNSICHERE NETZE

Durch Bereitstellung von Endkomponenten zum Aufbau von IP-Sec-Tunneln wird die Möglichkeit bestehen einen verschlüsselten gesicherten Datentransfer aus dem Einwahlnetz und mit geeigneten Clientenprogrammen auch innerhalb des hochschulinternen Rechnernetzes durchzuführen. Mittelfristig ist hier durch die Erweiterung des Bochumer Chipkarten-Projektes an die Nutzung von Chipkartentechnologie zur Schlüsselverwaltung gedacht.

SICHERUNG DER NETZKOMPONENTEN

Die aktiven Komponenten (Router und Switche) sind grundsätzlich unter Verschluss und nicht allgemein zugänglich, insbesondere haben nur berechtigte Personen Zugriff auf Schlüssel. (Für die Zukunft sind auch hier Chip-Karten gestützte Zugriffskontrollsysteme denkbar.)
Durch Zugriffsfilter und Zugriffslisten wird der Bereich der netzseitig für konfigurierende und überwachende Eingriffe Berechtigen eingeschränkt. Versuchte Fremdzugriffe werden durch SNMP-Trap beziehungsweise zentral auflaufende Alarme und Logging überwacht.
Aus dem Netzwerkmanagement heraus können regelmäßig alle Passwörter der Netzkomponenten ersetzt werden.
Die Konfigurationen der Komponenten (Router und Switche) werden mit einer bestimmten Historie zentral gesichert.

3.4. BETRIEBS- UND NUTZUNGSREGELUNGEN

ORGANISATION

Das Rechenzentrum der Ruhr-Universität Bochum ist eine zentrale Betriebseinheit und für den Betrieb des hochschulinternen Rechnernetzes zuständig.
Die Einhaltung der Betriebs- und Nutzungsregelungen wird durch das RZ kontrolliert.
Insbesondere gelten die Vorgaben, die sich aus der Satzung des Rechenzentrums und aus den Dienstvereinbarungen zum Netzbetrieb ergeben.

3.5. DATENSCHUTZ

PERSONENZUORDNUNG

Nur berechtigte Personen sollen Eingriffe in das Netz vollziehen können.

PERSONENBEZOGENE DATEN

Personenbezogene Daten, die aufgrund der Netzverwaltung oder aufgrund von Abrechnungen anfallen, sind nur für Berechtigte zugreifbar. Daten, die für statistische Zwecke benötigt werden, werden grundsätzlich anonymisiert. Eine Datendiensteordnung liegt als Entwurf vor.

3.6. ACCOUNTING

ABRECHNUNG

Ein Verursacher bezogenes Accounting findet im Netzbereich zur Zeit nicht statt. Vor der Einführung solcher Systeme ist insbesondere zu überlegen, in welchem Verhältnis Kosten und Nutzen stehen, da für Erfassung und Auswertung sehr umfangreiche Übertragungsleistungen zu installieren sind..
Dazu kommt, dass ein Accounting, das Verursacher bezogen Übertragungsleistungen erfasst, schon aus Datenschutz-Gründen erst dann vollstellbar ist, wenn eine echte Rechnungsstellung und nicht nur ein Leistungsnachweis erfolgt.

3.7. SERVICEQUALITÄT

NETZWERK SEITIGES „QUALITY OF SERVICE“

Um bestimmte Übertragungsdienstgüten (z.B. Bandbreiten für Videoübertragungen, Videokonferenzen, Datensicherung) zu garantieren, sind Werkzeuge eines „quality of service management“ (QoS) zu installieren. Dies bedeutet, dass einerseits bestimmte Übertragungen mit hoher Priorität durch Warteschlangenmanagement innerhalb der Komponenten zu bevorzugen sind.

AUSLASTUNG

Die Auslastungsdaten *aller* Komponenten und Übertragungswege werden per SNMP abgefragt und ausgewertet. Damit sind langfristige Auswertungen und Trendanalysen möglich. Diese Daten sind teilweise grafisch aufbereitet und auch innerhalb der Universität allgemein zugänglich.
Die Auslastungsdaten werden für ein pro-aktives Management verwendet, um rechtzeitig Erweiterungen und Umkonfigurationen zur Vermeidung von Engpässen einzuleiten.

DIENSTLEISTUNGEN

Zur Fehlerverfolgung und Ablaufüberwachung von Störungsmeldungen wird ein Help-Desk- und Action-Request-System eingesetzt.

3.8. WARTUNG

Die Wartungsanforderungen der Netzwerkkomponenten sind durchaus unterschiedlich. Ziel ist es, möglichst schnell reagieren zu können. Komponenten mit zentralen Aufgaben (z.B: Zugangsrouter zum Internet) besitzen Wartungsanforderungen von wesentlich höherer Qualität als ein Verteilungsswitch in einer Etage. Dies heißt, der fiskalische Aufwand für Wartung richtet sich nach der Funktion der Komponente. Eine geschickte Ersatzteilhaltung hat in der Vergangenheit praktisch immer eine sofortige Reaktionsmöglichkeit erzeugt.
Neben den obigen Vorgaben zu Wartungsverträgen, ist es allerdings notwendig im Zuge einer vorbeugenden Wartung beispielsweise Inspektion von Standorten durchzuführen, etwa um verstaubte Schränke zu reinigen o.ä. Bei mehr als 350 Standorten bindet eine solche Aufgabe eigentlich schon einen Mitarbeiter auf Dauer ...

3.9. STÖRUNGS- UND RISIKOMANAGEMENT

Es gilt, Störungen im Vorfeld durch proaktive Überwachung zu vermeiden. Die Erfahrung hat gezeigt, dass die Fehleranfälligkeit der heutigen Netzwerkkomponenten nicht sehr hoch ist. Ältere Geräte neigen allerdings bei Elektroschaltarbeiten zum Totalausfall.
Ein Einsatz von doppelt ausgelegter, redundanter Hardware ist aufgrund von Kosten-Nutzen-Gesichtspunkten *nicht* vollzogen worden.
Störungen, die sich im Bereich weniger Minuten bewegten, sind in der Vergangenheit – auch wenn sie alle betrafen – akzeptiert worden.
Momentan ist das Datennetz der Ruhr-Universität gegen Totalausfälle zentraler Komponenten nicht ausfallsicher. Ziel ist es jedoch, während der Dienstzeiten, auch „große“ Störungen kurzfristig beheben zu können, ohne dass auf die Anlieferung notwendiger Ersatzteile gewartet werden muss.

3.10. NETZÜBERWACHUNG

NETZWERKMANAGEMENT – ALLGEMEIN

Es wird auf Standardverfahren (SNMP) und – wenn möglich – auf im Markt erhältliche Produkte zurückgegriffen. Netzwerkmanagement hat eine hohe Priorität aufgrund der eingeschränkten Personalkapazitäten. Es bietet die einzige Chance, überhaupt ein sinnvolles Netzwerk-Management zu ermöglichen.

In den Jahren hat sich allerdings herausgestellt, dass ein Datennetz von der an unserer Universität vorhandenen Größe spezielle Anforderungen stellt, die eben nicht alltäglich und nicht unbedingt mittels „Regalware“ zu befriedigen sind:

Das Skalierungsproblem:

a) *Der Umfang* - In der Praxis hat sich in den letzten Jahren leider erwiesen, dass viele professionelle Management-Tools bei der Größe unseres Datennetzes „kapitulieren“ und nicht mehr sinnvoll arbeitsfähig sind, da diese für wesentlich kleinere Netzinfrastrukturen konzipiert wurden. Häufig ist allein die Anzahl der vorhandenen Komponenten Anlass, Unbedienbarkeit zu erzeugen (z.B. unbenutzbar lange Drop-Down-Listen).

b) *Die Performance* - In der Praxis ist es notwendig, in kurzen Zeitabständen von etwa 5 Minuten von allen, das heißt mehr als 41.000 Messpunkten (=Ports) Umsatz- und Fehlerdaten abzufragen und in Datenbanken in einer sinnvoll abfragbaren Form zu speichern.

Hierdurch ist in vielen Bereichen der Überwachung die Notwendigkeit aufgetreten, durch Eigenentwicklung – vielfach allerdings auf Open-Source-Anwendungen basierend – die Probleme eines „großen Netzes“ zu lösen.

c) *Störungsfreiheit der Messungen* - Manche Formen der Messungen können aufgrund des Umfang nicht direkt in den Netzwerkkomponenten ausgeführt werden (z.B. Netflow).
Alle Messverfahren sind so zu gestalten, dass die Messungen den Datenverkehr nicht stören. Dies bedeutet, den Einsatz von Out-of-Band-Management. Die Spiegelung von Datenströmen auf sekundäre Ports erlaubtt es, die Messung an andere Rechner „out-sourcen“ zu können.

Die Datenaggregation / Datenkonsolidierung:

Konzeptionell werden alle Messdaten auf zentralen Mess- und Statistikservern erfasst und – entsprechend der Zuständigkeit und Berechtigungen – in evtl. aggregierter Form den lokalen Betreuern zur Verfügung gestellt. Der lokale Betreuer erhält dann selbstverständlich nur Auskünfte über „seine“ Anschlüsse.
Ein besonderes Augenmerk wird dabei auf die Erfassung und Visualisierung von langfristigen Trends gelegt.

Gleichzeitig ist zu vermeiden, dass von unterschiedlichen Anwendungen, die gleichen Daten von den Komponenten abgefragt werden. Allerdings sind alle Messungen mit ihren Ergebnissen geeignet in die verschiedenen nachgeschalteten Überwachungs- und Benachrichtigungssysteme (z.B. Nagios, OTRS etc) einzuspeisen.

Ein positiver, aber gewünschter Nebeneffekt ist es, dass die Datenkonsoldierung es ermöglicht, Netzüberwachungsdaten und Messdaten aus einer Anwendung (z.B. eine Antwortzeit auf eine Transaktion) miteinander kombiniert in *einer* Anwendungsüberwachungsseite darzustellen.

Das Management wird hierbei systemübergreifend verwendet. Neben dem LAN werden gleichzeitig Teile der Telefonanlage mitüberwacht. Techniken aus dem Netzwerkmanagement werden zunehmend auch in der Prozessüberwachung von Anwendungen eingesetzt.

Die folgenden Management-Bereiche werden abgedeckt:

EVENT- UND STATUS-MANAGEMENT

Das „klassische“ Management basiert auf SNMP mit geeigneten Managementsystemen. Es wird verwendet um Geräte, das heißt die einzelnen abfragbaren Zustände zu überwachen bzw. mittels SNMP-Traps Alarmmeldungen abzuhandeln.
Durch Einsatz von professionellen Tools und Eigenentwicklungen findet neben der Geräte- auch eine Leitungsüberwachung statt.
Je nach Leistungsfähigkeit wird dabei auf professionellen Managementtools, Open-Source oder auch Eigenentwicklungen zurückgegriffen, um sowohl eine Geräteüberwachung als auch eine Leitungsüberwachung erreichen.
Bestimmte Fehlersituationen führen zu automatischen Benachrichtungen der zuständigen Mitarbeiter.

KABEL- UND KONFIGURATIONSMANAGEMENT

Die Dokumentation der Verkabelung wird durch geeignete Datenbanken gestützt. Die Konfiguration der Geräte wird durch Prozesse, die durch Veränderung in der Datenbank angestoßen werden durchgeführt. Damit wird gleichzeitig eine Revisionssicherheit erreicht, die dokumentiert, wie das Netz zum Zeitpunkt „x“ konfiguriert war. Durch die Nachvollziehbarkeit der Veränderungsprozesse und auch der Dokumentation des Verändernden wird eine hohe Qualität der Geschäftsabläufe in diesem Bereich erreicht.
Alle Anschlüsse sind in diesem Verwaltungssystem erfasst und zusätzlich mit Sekundärinformationen, wie Messprotokollen, Bauzeichnungen und Fotos der jeweiligen Standorte verknüpft.
Als konzeptionell sehr praktikabel ist die Möglichkeit, Änderungen zeitgesteuert, dass heißt automatisch zu bestimmten Zeitpunkten, ohne zusätzlichen Eingriff ausführen zu lassen.

TRAFFICMANAGEMENT

Durch Aggregation und Aufbereitung von Umsatzzahlen, die per SNMP aus den Komponenten gewonnen werden, wird eine langfristige Überwachung des Trafficvolumens und der Auslastung der einzelnen Netzwerkanschlüsse erreicht. Für *jeden* Anschluss kann so nachgewiesen werden, ob Fehler oder Überlastsituationen aufgetreten sind.

TRAFFIC-ANALYSE

Durch stichprobenartige Erfassung der Paket-Header am Übergangspunkt zum Internet werden automatische statistische Analysen durchgeführt, die Rückschlüsse auf Netzwerk-Anomalien ermöglichen. Dabei werden Rechner erkannt, die beispielsweise Netzwerk-Attacken fahren. Durch die Einbindung in automatische Ablaufprozeduren wird (teilweise) erreicht, dass solche Rechner automatisch im Netz gesperrt werden.

INTRUSION-DETECTION, INTRUSION-PREVENTION, FIREWALL

Der Bereich der Netzwerkabsicherung benötigt eine zentralisierte Absicherung, die Attacken und auch komplexe Filter- und Firewallstrukturen ermöglicht. Vor dem Hintergrund, dass die Geschwindigkeit der Netzanbindungen nach Außen (ins Internet und auch zu den Nachbarhochschulen) in Zukunft 10Gbit/s betragen wird, sind hierfür leistungsfähige Komponenten notwendig, die eine Bearbeitung mit „wire-speed“ erlauben.

3.11. HELP-DESK, CALL-CENTER

CALL-CENTER

Am Rechenzentrum der Ruhr-Universität Bochum wird ein Call-Center mit integriertem Help-Desk und einer eingekoppelten Benutzerdatenbank betrieben. Dies wird das Störungs- und Service-Management mit modernen Werkzeugen wesentlich schlagkräftiger gestalten.
Neben der professionelleren Abwicklung der einzelnen Service-Anfragen wird innerhalb des Help-Desk-System durch die Bereitstellung von Information zu bereits bekannten Problem die Betreuung erheblich erleichtert und inhaltlich verbessert.

4. PERSONAL

4.1. AUFWAND ZUR NETZVERWALTUNG, NETZSTEUERUNG

Wie im obigen Text dargestellt wurde, ist die Hauptprämisse bei der Netzbetreuung dafür zu sorgen, dass alle Änderungen vom Schreibtisch durch Konfiguration erledigt werden können. Dabei sollen möglichst viele Geschäftsvorgänge automatisiert ablaufen (z.B. Zeitaufträge).
Das erwähnte „Subsidiaritätsprinzip“ gebietet es, erlaubte/erlaubbare Konfigurationsänderungen direkt durch den autorisierten Nutzer ausführen zu lassen. An dieser Stelle haben wir – zugegebenerweise – noch etwas Entwicklungsbedarf, allerdings auch schon erste Erfolge vorzuweisen.

4.2. AUFWAND ZUR NETZINSTALLATION

Bei der Installation werden *alle* Datendosen auf Switche aktiv verkabelt und sind nutzbar, auch wenn in dem betreffenden Raum heute nur 1 Rechner steht.
Der Verteilerstandort wird nur bei einer Revision, Reparatur oder einem Umbau „angefasst“, sonst müssen alle Änderungen „von ferne“ gehen.

Finanzplanung Netzaufwendungen 2009-2012

A- und B-Kapitel sind zusammengefasst.

		10 G Back-bone	Netzwerk-sicherheit Ersatz Netzwerk-Management-System (in 2010); Intrusion detection, intrusion prevention, Honey pot-Systeme	Kabel-Ertüchtigung Austausch älterer CAT5-Verkabelung (passive Komponenten)	Austausch überalterter Elektroniken (> 6 Jahre) Zurzeit. sind ca. 1700 Geräte im Einsatz, davon müssen 2/3 in den nächsten Jahre getauscht werden	ZKF II (Neu-bau)	ID/IDN (Neubau)	Sport-wissen-schaft (Neubau)	SUMME
2009		156.000	160.000	200.000	0	65.000	0	0	581.000
2010		312.000	100.000	200.000	500.000	0	1.162.118	0	2.274.118
2011		120.000[2]	50.000	200.000	400.000		0	158000	928.000
2012 *)		60.000	50.000	150000	400000				660.000
								Summe	4.443.118

*) Die Zahlenangaben für 2012 stehen unter der Maßgabe, dass die begonnene Campussanierung fortschreitet, wie zum jetzigen Zeitpunkt angenommen.

Für die Neubau-Positionen ID/IDN und ZKF II liegen detailierte Kostenschätzungen vor, da die fortgeschrittenen Ausführungsplanungen dies zu diesem Zeitpunkt ermöglichen (siehe Anlagen)

Der Gesamtansatz im Haushaltsplan 2009 beträgt 3.418.800 €. Die jetzt aufgeführten höheren Kosten sind durch die Ausstattungsplanungen der Neubauten bedingt.

[2] Anschluss der Neubau

Kostenübersicht / Netzentwicklungsplan

Tabelle A - insgesamt	Preise incl. MwSt					
	Gesamt kEUR	Jahr kEUR	Jahr kEUR	Jahr kEUR	Jahr kEUR	Jahr kEUR
Netzkosten		**2009**	**2010**	**2011**	**2012**	
Aktive Komponenten:						
Backbone	824	156	468	140	60	
Etagenversorgung						
- Anteil für TP-Anschlüsse (Kupferleitungen)	2451	65	1461	526	400	
- Anteil für LWL-Anschlüsse (Glasfaser)	8		6	2		
Kosten pro LWL-port (aktiv)						
Kosten pro TP-port (aktiv)						
Netzdienste						
Netzmanagement						
Sicherer Netzbetrieb						
Funk-LAN	49		41	8		
Firewall, Intrusion Detection, VPN ...	360	160	100	50	50	
Summe Netzelektronik	**3693**	381	2076	726	510	
Passive Komponenten:						
Primärverkabelung (Backbone)						
Sekundärbereich (Gebäudeerschließung)						
Tertiärverkabelung (Etagenversorgung)						
- Anteil TP (Kupferleitungen)	750	200	200	200	150	
- Anteil LWL (Glasfaser)						
Kosten pro LWL-Wandanschluss (passiv)						
Kosten pro TP-Wandanschluss (passiv)						
Summe Verkabelung						
Planungskosten (*nur für passives Netz*)						
Summe reine Netzkosten	**750**	**200**	**200**	**200**	**150**	
Baukosten:						
Trassierung für Netzkabel						
An- und Umbauten						
Bauwerk, Baukonstruktion						
Lüftungstechnische Anlagen						
Stromversorgungsanlagen						
Beleuchtungsanlagen						
Gefahren- u. Informationstechnische Anlagen						
Planungskosten						
Summe Baukosten						
Gesamtkosten	**4443**	**581**	**2276**	**926**	**660**	