Westfälische Wilhelms-Universität Münster

> Antrag zum Ausbau des Kommunikationssystems

Teil B - Netzkonzept, Netzentwicklungsplan, Betriebs- und Managementkonzept, Personalsituation

Gemeinsame Darstellung für die Westfälische Wilhelms-Universität und das Universitätsklinikum Münster

wissen.leben
WWU Münster

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Inhaltsverzeichnis

1 Netzkonzept 5
1.1 Vorbemerkungen 5
1.2 Grundsätze 5
1.2.1 Angestrebte Ziele 5
1.2.2 Entscheidungsträger 6
1.2.3 Verbindlichkeit 9
1.3 Bedarfsbegründende Grunddaten 10
1.4 Mengengerüst 10
1.4.1 Gebäudesituation 10
1.4.2 Kennzahlen des Kommunikationsnetzes 11
1.4.3 Nutzungsintensität 12
1.5 Netzdienste 14
1.5.1 Externe Netze 14
1.5.2 Intranet / LAN 16
1.5.3 TK-Netz 16
1.5.4 Telefon- und Video-Konferenzen 16
1.5.5 Intranet / Mediennetze (AVM: Audiovisuelle Medien) 16
1.5.6 Weitere Netzdienste an der WWU 17
1.6 Vorhandene und angestrebte Netzstruktur 18
1.6.1 Grundsätze des Netzdesigns: Verfügbarkeit und eingebettete Sicherheit 18
1.6.2 Begriffsklärungen 19
1.6.3 Grobe topografische und funktionale Struktur der Netze von WWU und UKM 20
1.6.4 Ausführliche Darstellung der Netzstruktur 24
1.6.5 Konzept der netzseitigen IT-Sicherheitsmaßnahmen 32
1.6.6 "Herstellerpolitik" 39
1.6.7 House-Keeping: USV-Versorgung, Klimatisierung 40
1.6.8 Mediennetze, AVM (Audiovisuelle Medien) 41
1.6.9 Core Network Services 42
1.7 Netzintegration 43
1.8 Konvergenz von Tele- und Datenkommunikation 43
1.8.1 Darstellung der TK-Infrastruktur 43
1.8.2 TK-Managementsystem 45

1.8.3 Personal ... 46
1.8.4 Gemeinsame Nutzung von Netzinfrastruktur und Werkzeugen ... 47
1.8.5 Planung der VoIP-Migration ... 47
1.8.6 Konzeptdarstellung "Zusätzliche Verkabelung für VoIP" ... 48
1.8.7 Potential der Konvergenz ... 49
2 Netzentwicklungsplan ... 51
2.1 Vorbemerkung ... 51
2.2 Bereiche mit stetiger Entwicklung ... 51
2.2.1 Netzausbau ... 51
2.2.2 Edge-Switches ... 52
2.2.3 WLAN ... 53
2.2.4 TK- und Medien-Konvergenz ... 54
2.2.5 House-Keeping ... 54
2.3 Bereiche mit wesentlichen Entwicklungsschritten („Meilensteinen“) ... 54
2.3.1 Core – Midrange - Distribution ... 54
2.3.2 Data Center ... 55
2.3.3 Sicherheit ... 55
2.3.4 Netzmanagement: Netzadministration, Netzbetrieb, Netzüberwachung ... 56
3 Betriebs- und Managementkonzept ... 58
3.1 Verantwortungs- und Zuständigkeitsverteilung ... 58
3.2 Dienstleistungsvereinbarung mit dem Universitätsklinikum ... 58
3.3 Betriebs- und Nutzungsregelungen ... 59
3.4 Unterstützung dezentraler Systeme und Dienste über das Netz ... 59
3.5 Abrechnungspolitik ... 59
3.6 Administration ... 60
3.6.1 Netzdokumentation und -administration mit *LANbase* ... 60
3.6.2 Weitere Dokumentationswerkzeuge ... 62
3.6.3 Planungen im Bereich Administration ... 62
3.6.4 Konzeptdarstellung „Eigenentwicklungen statt Einsatz kommerzieller Produkte“ ... 62
3.7 Sicherheit, Datenschutz ... 63
3.8 Betrieb - LAN/Datennetz ... 65
3.8.1 Technische Maßnahmen ... 65
3.8.2 Administrative, organisatorische Maßnahmen ... 65
3.9 Betrieb - Telekommunikation, Mobilfunk, Medienservice ... 66
3.10 Netzüberwachung ... 67

3.11 Störungs- und Risikomanagement, Servicequalität 69
3.11.1 Risikomanagement 69
3.11.2 Störungsmanagement und Servicequalität 69
3.12 Planungen hinsichtlich Konvergenz von Tele- u. Datenkommunikation 70
4 Personalsituation 71
5 Tabellenverzeichnis 72
6 Abbildungsverzeichnis 73
7 Abkürzungsverzeichnis 75
Anhang: Ausgewählte Abbildungen in hoher Qualität 77
Abb. 2: Verteilung der Gebäude von WWU und UKM über das Stadtgebiet vom Münster inkl. der LWL-Verbindungen 77
Abb. 8: Kernnetzkomponenten der WWU mit Zuordnung zu Standorten 77
Abb. 18: Schematische Darstellung des TK-Anlagenverbundes des Hochschulstandortes Münster 77
Abb. 19: Schematische Darstellung der Anschaltung von weiteren zentralen Systemen und Verbindungen an den TK-Anlagenverbund 77

1 Netzkonzept

1.1 Vorbemerkungen

Dieser Antrag bezieht sich auf das Kommunikationssystem der Westfälischen Wilhelms-Universität Münster (WWU) – damit soll deutlich werden, dass nicht nur der Stand und weitere Ausbauplan des Datennetzwerks in diesem Konzept dargestellt wird, sondern auch die Telekommunikation (TK) und sonstigen Netzdienste.

Die in diesem Dokument dargestellten Konzepte für das Kommunikationssystem gelten in aller Regel sowohl für die WWU als auch für das Universitätsklinikum Münster (UKM). Sollten deutliche Unterschiede zwischen den beiden Einrichtungen bestehen, so wird immer darauf hingewiesen. Die dargestellten Planungen beziehen sich auf einen Zeitraum von ca. 7 Jahren (d.h. bis ca. 2016/17). Der Planungszeitraum von 7 Jahren in diesem Antrag (abweichend von der ansonsten üblichen 5 Jahresperiode) wird bewusst gewählt, da dies einem realistischen kompletten Innovationszyklus bei den aktiven Netzwerkkomponenten entspricht. Die im Antrag dargestellte Erneuerung der kompletten aktiven Netzwerkkomponenten und die begleitend notwendige Erweiterung der LWL-Infrastruktur sind mit den verfügbaren personellen Ressourcen nur im gewählten Planungszeitraum von 7 Jahren bewältigbar.

1.2 Grundsätze

1.2.1 Angestrebte Ziele

Information hat sich in den letzten Jahrzehnten zum zentralen Faktor für ein erfolgreiches Arbeiten in allen Bereichen der Wirtschaft und des öffentlichen Lebens entwickelt. Vom Fluss der Informationen, und von der Funktionsfähigkeit der Systeme zur Informationsverarbeitung hängt inzwischen die Arbeitsfähigkeit moderner Organisationen ab. Insbesondere zuverlässige und weitum verfügbare Datennetzwerke sind dafür die Grundvoraussetzung. Sie bilden die Infrastruktur für die Forschung im Sinne von „eScience“ und unterstützen die Gestaltung neuer, zukunftsorientierter Lehr- und Lernumgebungen.

Insbesondere für Universitäten ohne homogene Campus-Struktur stellt der Auf- und Ausbau eines umfassenden Kommunikationssystems einen bedeutenden personellen und finanziellen Faktor dar.

Die WWU Münster hat schon sehr früh mit einem umfangreichen Ausbau der Netzwerkinfrastruktur begonnen und konnte eine sehr weitreichende Abdeckung erreichen – aktuell kann von Vollausbau gesprochen werden. Die Kompetenzen für Ausbau und Betrieb des Netzwerkes sind klar geregelt und ausschließlich in der Verantwortung des Zentrums für Informationsverarbeitung (ZIV) der WWU.

Das für den Antragszeitraum angestrebte Ziel ist es, auch bei beträchtlichen Fluktuationen im weitverstreuten Gebäudebestand der WWU diesen Status des Vollausbaus zu erhalten und einen höchst zuverlässigen Betrieb des Kommunikationssystems, der allen zukünftigen Leistungsanforderungen gerecht wird, zu gewährleisten.

Das Kommunikationssystem darf kein limitierender Faktor für die zukünftige Entwicklung der WWU Münster in Forschung und Lehre sein.

Dabei sind die Hauptziele:

- Konvergenz: Zusammenführung von Telekommunikations-, Daten- und Speichernetzwerk in technischer und personeller Sicht.
- Verfügbarkeit: höchste Zuverlässigkeit und umfassende Abdeckung aller Bereiche der WWU durch das Kommunikationssystem.
- Leistungsfähigkeit: proaktive Adressierung absehbarer Leistungs-Anforderungen zur Verhinderung behindernder Engpässe bei laufendem Wachstum.
- Sicherheit: Gewährleistung eines Höchstmaßes an Datensicherheit durch organisatorische Sicherheitsmaßnahmen, netzseitige Sicherheitseinrichtungen und Netzdienste für Datenhaltung und Sicherung.

1.2.2 Entscheidungsträger

1.2.2.1 Die IT-Governance Struktur der WWU Münster

Die fachbezogenen Anforderungen an die Informationsverarbeitung (IV) in Forschung und Lehre sind an der WWU Münster als einer der größten Universitäten des Landes sehr komplex. Das IV-Gesamtsystem trägt diesem Aspekt durch eine zweischichtig zentrale IT-Organisation angemessen Rechnung.

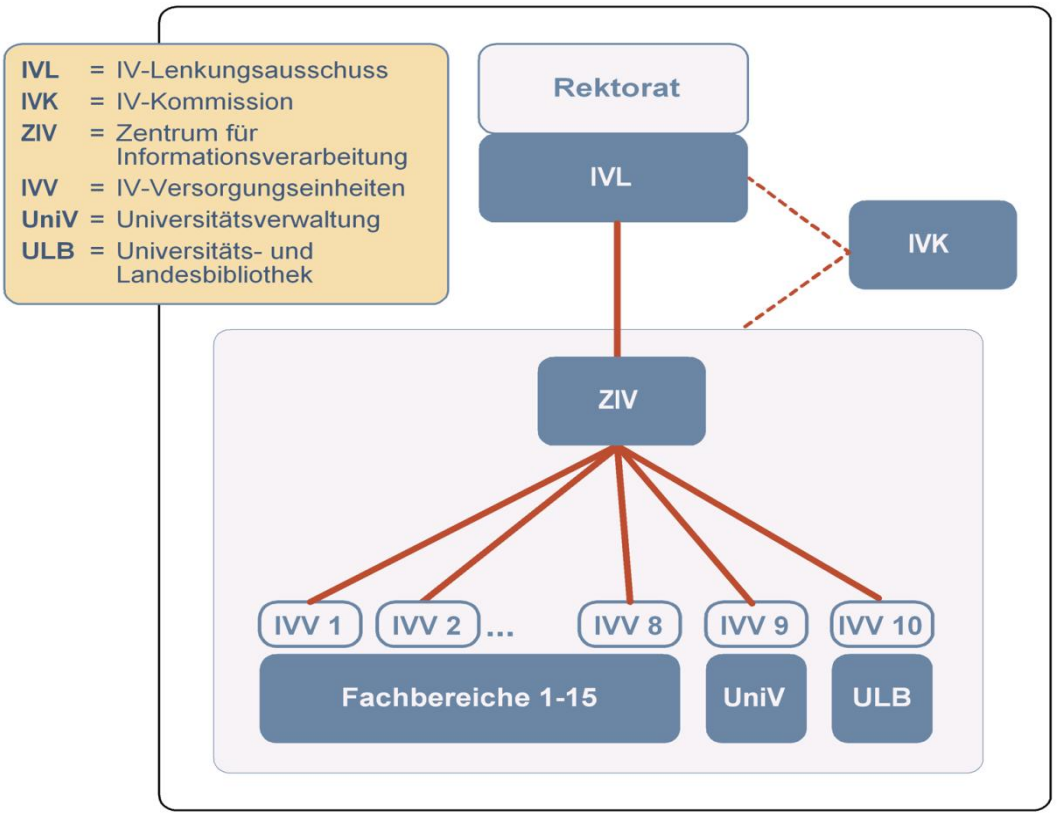


Abb. 1: Das IV-System der WWU Münster – Entscheidungsgremien und operative Einheiten.

Die Leitungsstruktur wird durch einen dem Rektorat zugeordneten IV-Lenkungsausschuss als Entscheidungsgremium mit CIO-Funktion und eine vom Senat gewählte IV-Kommission repräsentiert. Die für die IV-Versorgung notwendigen Arbeiten werden aufeinander abgestimmt vom Zentrum für

Informationsverarbeitung und von 10 IV-Versorgungseinheiten in den Fachbereichen und zentralen Universitätseinrichtungen wahrgenommen. Die konkrete Aufteilung der Zuständigkeiten wird durch eine Liste festgelegt, die regelmäßig von der IV-Kommission aktualisiert wird und vom IV-Lenkungsausschuss beschlossen wird.

Diese Organisationsform ist von der DFG im Rahmen der Ausschreibung Centers of Excellence durch Bewilligung des MIRO-Projektes (Münster Information System for Research and Organization), das gemeinsam von der Universitäts- und Landesbibliothek, der Universitätsverwaltung und dem ZIV im Kontext des IKM (Information, Kommunikation und Medien) beantragt wurde, gewürdigt worden und hat sich seit ihrer Etablierung im Jahr 1996 bestens bewährt.

In der Terminologie der HIS-Untersuchung zu IT-Diensten an Universitäten und Fachhochschulen von 2005 handelt es sich in Münster um eine zweischichtig zentrale Organisationsform mit einem IV-Lenkungsausschuss und einer IV-Kommission, in der Empfehlungen aus den Fachbereichen aufgenommen werden. Das Münsteraner Modell wird dort prototypisch für diese Organisationsform eingehend dargestellt. Diese Organisation entspricht für eine große Universität weitgehend den Empfehlungen des Landesrechnungshofes NRW zur Konzentration der IT-Services.

1.2.2.2 Organisatorische Strukturen der Informationsverarbeitung

Die Organisation des Systems der Informationsverarbeitung (IV-System) der WWU ist durch eine Reihe von Ordnungen und Regelungen bestimmt. Kern dieser Ordnungen ist der Senatsbeschluss vom 8.7.1996 betreffend „Das System der Informationsverarbeitung der WWU Münster“. Daneben gibt es weitere Regelungen, insbesondere auch zur Zusammenarbeit des Zentrums für Informationsverarbeitung (ZIV) und der IV-Versorgungseinheiten (IVV).

Das Gesamtsystem der Informationsverarbeitung an der WWU wird organisatorisch durch die folgenden Organe gebildet:

- IV-Lenkungsausschuss (IV-L)
- IV-Kommission (IV-K)
- Zentrum für Informationsverarbeitung (ZIV)
- IV-Versorgungseinheiten (IVVen)

1.2.2.2.1 Der IV-Lenkungsausschuss

Zur Sicherstellung des nutzergerechten und wirtschaftlichen Betriebs des IV-Gesamtsystems ist ein IV-Lenkungsausschuss als Rektoratskommission eingerichtet. Dieser trifft die dazu notwendigen Grundsatzentscheidungen, legt im Einvernehmen mit dem Rektorat und der IV-Kommission die Ziele und Aufgaben der verschiedenen Funktionsträgerinnen/Funktionsträger auf der zentralen und der dezentralen Ebene fest und kontrolliert die Entscheidungs- und Betriebsabläufe innerhalb des Systems sowie die Ergebnisse der Arbeit im IV-System.

Dem IV-Lenkungsausschuss gehören an:

- die Rektorin/der Rektor oder eine Prorektorin/ein Prorektor,
- die Kanzlerin/der Kanzler,
- die/der Vorsitzende der IV-Kommission,
- drei weitere vom Rektorat für eine Amtszeit von vier Jahren bestellte Mitglieder, die auf dem Gebiet der Informationsverarbeitung besonders ausgewiesen sind, auch von außerhalb der WWU stammen können und die Interessen aller Nutzergruppen vertreten und nicht gleichzeitig Mitglieder der IV-Kommission sind,

- die Direktorin/der Direktor der ULB,
- die Direktorin/der Direktor des ZIV.

1.2.2.2.2 Die IV-Kommission

Die IV-Kommission wird auf der Grundlage von Artikel 34 Abs. 3 UG sowie Artikel 77, Abs. 4 UV durch den Senat der WWU gebildet. Ihr gehören sechs Mitglieder der Gruppe der Professorinnen und Professoren und je zwei Mitglieder der Gruppe der wissenschaftlichen Mitarbeiterinnen und Mitarbeiter, der Studierenden und der nichtwissenschaftlichen Mitarbeiterinnen und Mitarbeiter an. Bei der Zusammensetzung sollten die dezentralen IV-Versorgungseinheiten berücksichtigt werden. Die Amtszeit beträgt zwei Jahre. Die Direktorin/der Direktor des ZIV nimmt an den Sitzungen mit beratender Stimme teil.

Die IV-Kommission gibt Empfehlungen für Aufgaben, Aufbau, Verwaltung und Nutzung des Systems der Informationsverarbeitung an der WWU. Diese Empfehlungen werden an den Lenkungsausschuss weitergeleitet.

1.2.2.2.3 Das Zentrum für Informationsverarbeitung (ZIV)

Die Aufgaben, Rechte und Pflichten des ZIV werden vom Lenkungsausschuss in Abstimmung mit dem Rektorat, der Leitung des ZIV und der IV-Kommission vorgeschlagen und vom Senat beschlossen. Zur Erfüllung dieser Aufgaben gibt sich das ZIV eine eigene Organisationsstruktur.

Das kooperative, an zentralen und dezentralen Aufgaben orientierte Versorgungssystem macht es erforderlich, dass das ZIV sowohl zentrale, universitätsumfassende als auch dezentrale, auf Nutzerinnen/Nutzer oder Nutzergruppen ausgerichtete Leistungen erbringt. Diese Leistungen umfassen die Planung, die Installation, den Betrieb, die Beratung sowie die Wartung bzw. Pflege im ZIV sowie die Unterstützung solcher Aufgaben auf dezentraler Ebene im Rahmen des gesamten Kommunikationsnetzes, der Telekommunikationssysteme, der Audio-Visuellen-Medien (AVM), der Rechner, der Systemsoftware und der Anwendungssoftware. Dem ZIV obliegt im Übrigen die betriebsfachliche Aufsicht aller DV-Anlagen der WWU.

Zu den weiteren Aufgaben des ZIV zählen die Kooperation mit Hochschulrechenzentren bzw. Zentren für Informationsverarbeitung anderer Hochschulen, die fortlaufende Informationsbeschaffung über neueste Entwicklungen in der Informationstechnologie, die Unterstützung der Hochschulleitung, der IV-Kommission und des IV-Lenkungsausschusses in allen Fragen der Informationsverarbeitung.

Dazu kooperiert das ZIV hochschulübergreifend im Rahmen von DFN (Deutsches Forschungsnetzwerk), ARNW (Arbeitskreis der Leiter wissenschaftlicher Rechenzentren in NRW), ZKI (Zentren für Kommunikation und Informationsverarbeitung) und DINI (Deutsche Initiative für Netzwerkinformation).

Das ZIV betreibt das Kommunikationsnetz und die Telekommunikationssysteme für das UKM sowie das Wissenschaftsnetz Münster (WNM) für die Vernetzung der ortsansässigen Hochschulen und Forschungseinrichtungen (FH-Münster, Kunsthochschule, MPI) und beteiligt sich aktiv am RV-NRW (Ressourcenverbund NRW).

1.2.2.2.4 Die IV-Versorgungseinheiten (IVVen)

Auf der dezentralen Ebene werden für die IV-Versorgung 10 IV-Versorgungseinheiten gebildet:

1. Philologien, Geschichte, Philosophie
2. Wirtschaftswissenschaften incl. Wirtschaftsinformatik
3. Rechtswissenschaften

4. Naturwissenschaften (ohne Geowissenschaften)
5. Mathematik, Informatik, Psychologie, Sportwissenschaften
6. Geowissenschaften und Geographie
7. Erziehungs– und Sozialwissenschaften, Theologien, Musikhochschule
8. Medizinische Einrichtungen.
   Die Medizinischen Einrichtungen bilden für die Bereiche Lehre, Forschung, Krankenversorgung und Verwaltung eine dezentrale Versorgungseinheit mit spezifischen Organisationsstrukturen, die gesondert geregelt werden.
9. Zentrale Universitätsverwaltung
   Sie betreibt die IT-Anwendungssysteme für die Verwaltungsaufgaben in eigener Regie
10. Universitäts- und Landesbibliothek.
    Für den gesamten Bereich des Sammelns, der Erschließung und der Bereitstellung von Informationen in Form von Printmedien und elektronischen Medien sowie gegebenenfalls für die Bereitstellung der entsprechenden technischen Infrastruktur ist die Universitäts- und Landesbibliothek zuständig.

Die an den IVVen beteiligten Fachbereiche und zentralen Einrichtungen bestimmen deren interne Organisationsform und stellen die Finanzierung sicher. Die Leiter der IVVen werden von den beteiligten Fachbereichen und Einrichtungen vorgeschlagen und vom Senat bestätigt.

1.2.2.2.5 Aufgabenteilung und Zusammenarbeit zwischen ZIV und IVVen

Die Verteilung der Aufgaben und Zuständigkeiten zwischen dem Zentrum für Informationsverarbeitung und den IV-Versorgungseinheiten wird mittels einer Liste der Aufgaben festgelegt. Diese Liste wird von der IV-Kommission erarbeitet und vom IV-Lenkungsausschuss beschlossen.

Die Kommunikation zwischen den IVVen und dem ZIV ist ein wesentlicher Punkt des Gesamtsystems. Sie findet zwischen den Experten beider Seiten statt, aber auch zwischen den leitenden Mitarbeitern in regelmäßigen Arbeitstreffen.

1.2.3 Verbindlichkeit

In den vom Rektorat der WWU Münster am 16.4.2002 beschlossenen „Regelungen zur IV-Sicherheit“ werden die Betriebsregelungen unter §3 wie folgt festgelegt:

Alle Kommunikationssysteme (campusweites LAN, WAN, Einwahleinrichtungen usw.) werden ausschließlich vom Zentrum für Informationsverarbeitung (ZIV) betrieben. Eigene LAN-Installationen und unerlaubte Betriebsformen dürfen von Dritten nicht vorgenommen werden. Alle an das Kommunikationssystem anzuschließenden Endgeräte außerhalb von besonders ausgewiesenen Netzbereichen, die eine netzbasierte Authentifizierung erlauben (z.B. VPN), sind anzumelden. Neben den zentral bereitgestellten Netzzugängen (z.B. Einwahlzugängen) dürfen keine weiteren geschaffen werden. Spezielle Netzzugänge sind mit dem ZIV abzustimmen.

Damit ist sichergestellt, dass das Kommunikationssystem der WWU Münster eine einheitliche und professionelle Betreuung durch das ZIV erhalten und somit Potenzial für Störungen minimiert wird. Diese Regelungen sind konsequent umgesetzt – der Ausbau und Betrieb des Kommunikationssystems der WWU wird bis zur Endgeräteanschlussdose durch das ZIV gewährleistet.

1.3 Bedarfsbegründende Grunddaten

Die WWU zählt zu den sehr großen Hochschulen in Deutschland. Die Schwerpunkte der WWU liegen in den Geistes- und Sozialwissenschaften, den Gesellschaftswissenschaften, den Naturwissenschaften und der Medizin; die Ingenieurwissenschaften sind nicht vertreten. Die WWU gliedert sich in 15 Fachbereiche, welche die organisatorischen Grundeinheiten der Hochschule bilden:

- FB1: Evangelische Theologie
- FB2: Katholische Theologie
- FB3: Rechtswissenschaften
- FB4: Wirtschaftswissenschaften
- FB5: Medizin
- FB6: Erziehungswissenschaften und Sozialwissenschaften
- FB6: Erziehungswissenschaften und Sozialwissenschaften
- FB7: Psychologie und Sportwissenschaft
- FB8: Geschichte/Philosophie
- FB9: Philologie
- FB10: Mathematik und Informatik
- FB11: Physik
- FB12: Chemie und Pharmazie
- FB13: Biologie
- FB14: Geowissenschaften
- FB15: Musikhochschule

In über 110 Studienfächern mit 250 Studiengängen gab es im Wintersemester 2008/09 ca. 37.000 Studierende. Die Zahl der jährlichen Absolventen liegt bei ca. 5500. Die ca. 5.000 Beschäftigten der WWU setzen sich wie folgt zusammen:

- 565 Professoren
- 2.700 Wissenschaftliche Mitarbeiter
- 1.700 weitere Mitarbeiter

Zusätzlich sind 7.000 Mitarbeiter im UKM beschäftigt.

Bei der WWU handelt es sich um eine über die ganze Stadt Münster verteilte Flächenuniversität. Das Kommunikationsnetz der WWU ist daher ein typischen Metropolitan Area Network (MAN). In der Folge ergibt sich ein hoher Aufwand bei der flächendeckenden Erschließung aller Gebäude. Dabei sind erfahrungsgemäß auch regelmäßig neue Gebäude netztechnisch anzubinden. Das Kommunikationsnetz umfasst dabei sowohl LAN-Technologien (diverse Ethernet-Varianten, WLAN), als auch traditionelle TK-Technologien und Mediennetze (AVM: Audiovisuelle Medien). In Bezug auf Planung, Installation und Betrieb der Kommunikationsnetze gibt es dabei eine enge Kooperation mit dem UKM.

1.4 Mengengerüst

1.4.1 Gebäudesituation

Die Gebäude der WWU und des UKM sind über das gesamte Stadtgebiet von Münster verteilt. Folgende Kenndaten charakterisieren die Gebäudesituation der WWU und des UKM:

Kennzahl	WWU	UKM	insgesamt
Gebäude	212	99	311
Räume	15.340	17.920	33.260
Hauptnutzfläche	257.000 qm	202.000 qm	459.000 qm

Tabelle 1: Kenngrößen zur Gebäudesituation von WWU und UKM

Die Erschließung der Gebäude erfolgt über ein universitätseigenes Glasfasernetz (vgl. Abb. 2).

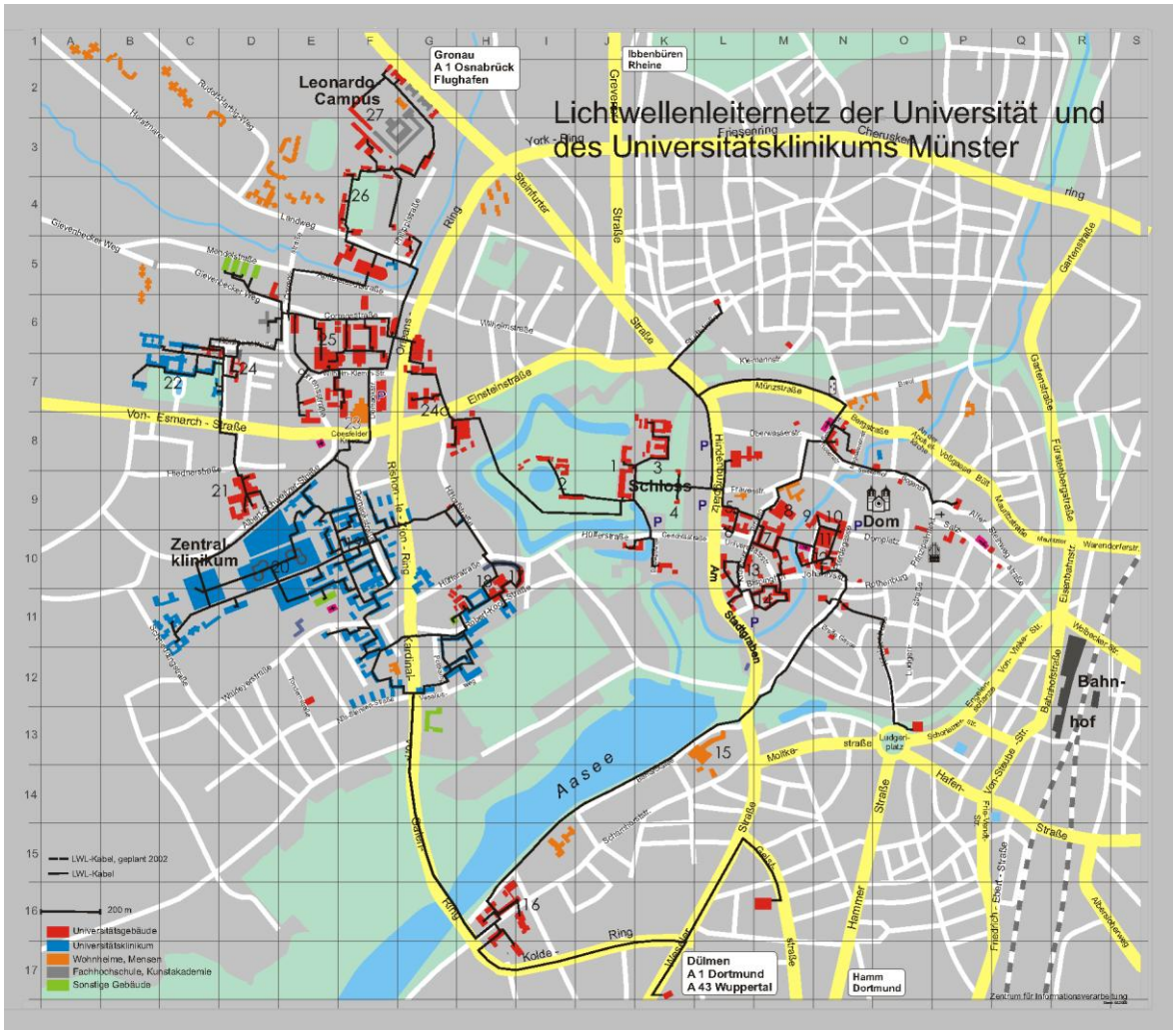


Abb. 2: Verteilung der Gebäude von WWU und UKM über das Stadtgebiet vom Münster inkl. der LWL-Verbindungen (hochauflösende Version der Abb. im Anhang)

1.4.2 Kennzahlen des Kommunikationsnetzes

Das Kommunikationsnetz von WWU und UKM lässt sich durch die in Tabelle 2 bis Tabelle 4 angegebenen Kennzahlen charakterisieren:

Kennzahl	WWU	UKM	sonst	insgesamt
erschlossene Gebäude	160	76	28	264
versorgte Räume	9.126	7.758	302	17.186
Gesamtlänge des LWL-Netzes				227 km
registrierte Nutzerkennungen	57.600			

Tabelle 2: Technologieunabhängige Kennzahlen

Kennzahl	WWU	UKM	sonst	insgesamt
LAN-Verteilerstandorte	218	145	13	376
Netz-Anschlussdosen, s.u. (1.)	26.454	15.845	755	43.054
passive LAN-Ports				s.u. (2.)
WLAN Access Points	623	165	0	788
registrierte LAN-Endsysteme	15.971	10.971	309	27.251
Core/Midrange Router/Switches (Cisco 6509)	15	4	0	21
Distribution/Edge-Switches, s.u. (3.)				ca. 2000
Bandbreite der IP-Außenanbindung (10GE zu DFN X-WiN)				2 Gbps

Tabelle 3: *LAN-Kennzahlen (Stichtag: 1.1.2009)*

Bemerkungen zur Tabelle 3:

1. Bei den Netzanschlussdosen handelt es sich um auf strukturierter Verkabelung basierende Anschlüsse. In den allermeisten Fällen sind dieses LAN-Dosen. Außerdem sind hier auch einige Hundert Anschlüsse für Telefonie mit erfasst.
2. Die Zahl passiver Netz-Anschlussdosen ist vernachlässigbar, da in aller Regel Dosen bei der Installation auch aufgelegt werden. Eine bedarfsweise Aktivierung von Netz-Anschlussdosen ist vom personellen Aufwand her nicht zu leisten.
3. Bemerkung zur Zahl der Edge-Switches: Diese Anzahl ist wenig aussagekräftig, da mit dieser Zahl unterschiedliche Gerätetypen zusammen erfasst sind. Das Spektrum an Gerätetypen erstreckt sich von Einbauswitches mit 4 Endnutzerports bis hin zu modularen oder gestackten Systemen mit dreistelligen Portzahlen.

Die zeitliche Entwicklung einiger LAN-Kennzahlen ist in Abb. 20 auf der Seite 52 dargestellt.

Kennzahl	WWU	UKM	sonst	insgesamt
(aktive) TK-Nebenstellen	8.490	7.540	1.870	17.900
Standorte	47	25	11	83
Hauptstandorte (TK-Units)	8	3	1	12
RPMs (abgesetzte Anlagenteile)	58	42	12	112
Voice Mailboxen	1.250	1.220	660	3.130
VoIP-Telefone	430	0	0	430
Mobiltelefonieverträge	460			460

Tabelle 4: *TK-Kennzahlen*

1.4.3 Nutzungsintensität

Die folgenden exemplarischen Zahlen für das Jahr 2008 kennzeichnen die Nutzungsintensität der IT-Systeme/Services des (d.h. nicht nur des Kommunikationsnetzes) an WWU und UKM:

Kennzahl	Wert
empfangenes X-WiN Datenvolumen	534 TB
gesendetes X-WiN Datenvolumen	431 TB
verschiedene WLAN-Nutzer	7.800
davon externe eduroam-Nutzer	180
davon FH Münster	120
Betriebsfälle im NOC (Network Operating Center)	6.160
Externe Telefonie-Verbindungen (ein- und ausgehend)	ca. 13,4 Mio
Gesprächsminuten (ausgehend)	ca. 4,3 Mio
Vermittlungen	ca. 35.000 externe Gespräche pro Monat
Zugestelltes Mail-Datenvolumen	ca. 6,5 GB pro Tag
Zentrale Web-Präsenz der WWU	ca. 5 Mio. Zugriffe pro Tag

Tabelle 5: Kennzahlen zur Nutzungsintensität für das Jahr 2008

Die beiden folgenden Grafiken stellen die Auslastung des X-WiN-Anschlusses des WNM dar.

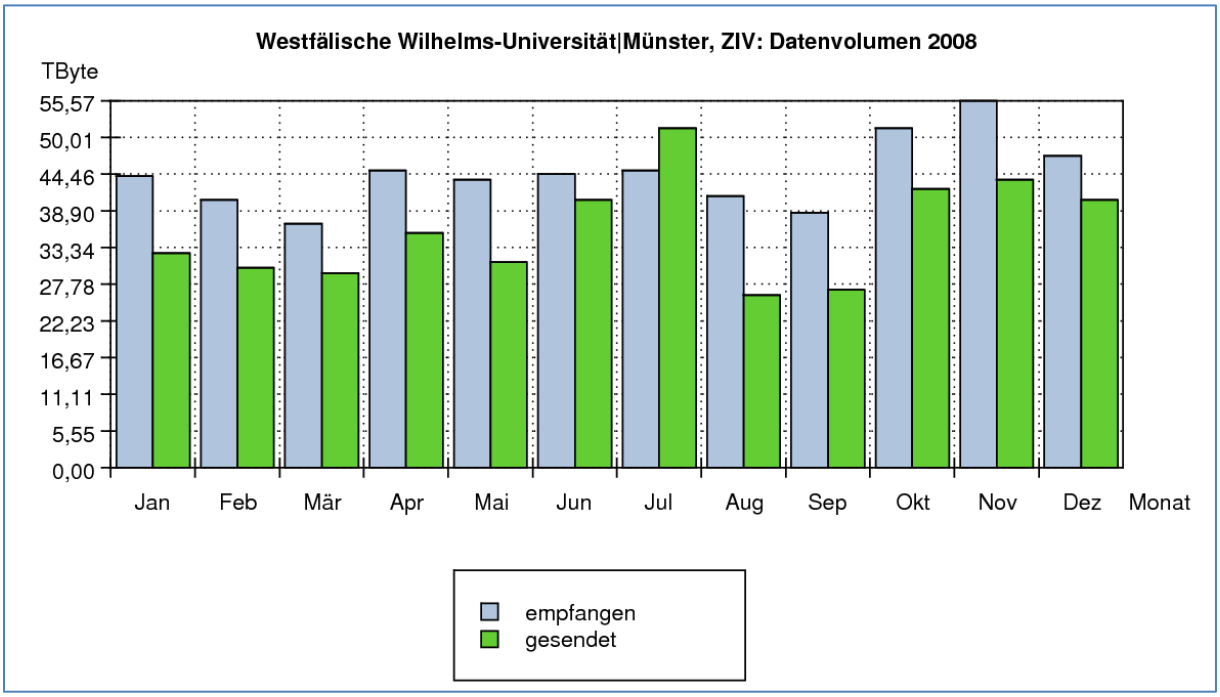


Abb. 3: Über den X-WiN-Anschluss des WNM in 2008 übertragenes Datenvolumen

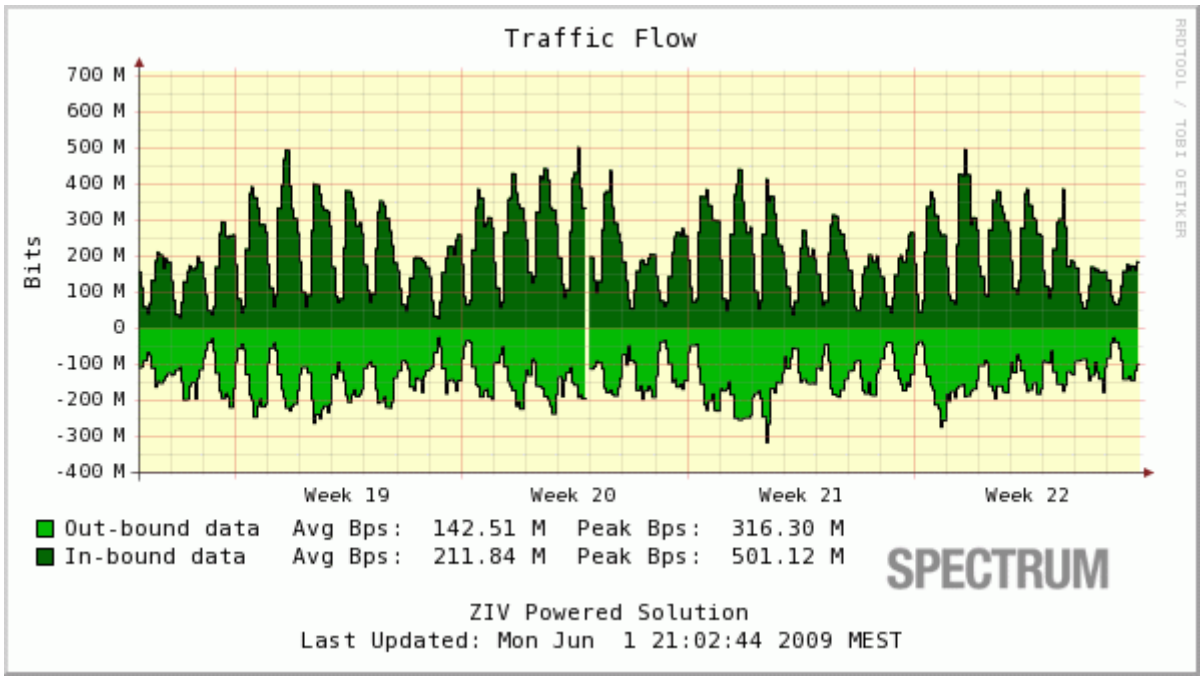


Abb. 4: Auslastung der X-WiN-Hauptleitung des WNM im Mai 2009

1.5 Netzdienste

Das Zentrum für Informationsverarbeitung (ZIV) der WWU ist der zentrale Dienstleister der WWU im Bereich der Informationsverarbeitung (IV). Im Bereich des Kommunikationsnetzes der WWU und des UKM leistet das ZIV ein umfassendes Spektrum an Netzdiensten von der Planung über die Installation bis zum Betrieb. Dabei umfasst das Kommunikationsnetz ausdrücklich sowohl den LAN- als auch den TK-Bereich. Wenn im Folgenden nicht ausdrücklich darauf hingewiesen wird, erbringt das ZIV die verschiedenen Netzdienste in gleicher Weise für die WWU und das UKM. Darüber hinaus betreibt das ZIV für die Fachhochschule Münster und die Kunstakademie Münster die zentralen Telekommunikationssysteme.

1.5.1 Externe Netze

Am Hochschulstandort Münster existiert ein Netzverbund (Wissenschaftsnetz Münster, kurz WNM), der der Kommunikation von Wissenschaftseinrichtungen und damit kooperierenden Einrichtungen untereinander und über das Wissenschaftsnetz des DFN e.V. dient. Ein sogenanntes Zugangsnetz, das vom ZIV eingerichtet wurde und betrieben wird, stellt die notwendigen physikalischen und routing-technischen Verbindungen her. An das Zugangsnetz sind folgende Teilnehmer angeschlossen:

- Westfälische Wilhelms-Universität Münster
- Universitätsklinikum Münster
- Fachhochschule Münster (FH)
- Max-Planck-Institut für molekulare Biomedizin (MPI)
- Studentenwerk Münster
- ca. 20 Studierendenwohnheime

Dabei werden die Netze der Fachhochschule, des Max-Planck-Instituts und des Studentenwerks eigenständig von der jeweiligen Einrichtung betrieben. In den Mensen des Studentenwerks besteht für die Studierenden eine vom ZIV betriebene WLAN-Zugangsmöglichkeit zu den Hochschulnetzen.

Die Netze in den Studierendenwohnheimen werden in der Regel in enger Abstimmung mit dem ZIV betrieben. Außerdem sind insgesamt 14 An-Institute in das WNM integriert.

Die gemeinsame IP-Außenanbindung der WNM-Teilnehmer (außer dem Studentenwerk) erfolgt über das X-WiN (vgl. Abb. 5). In Räumen der WWU ist ein X-WiN Kernnetzstandort angesiedelt. Die Teilnehmeranschlussbreite beträgt 2 Gbps, wobei zur Erhöhung der Verfügbarkeit eine doppelte Anbindung an das X-WiN realisiert ist.

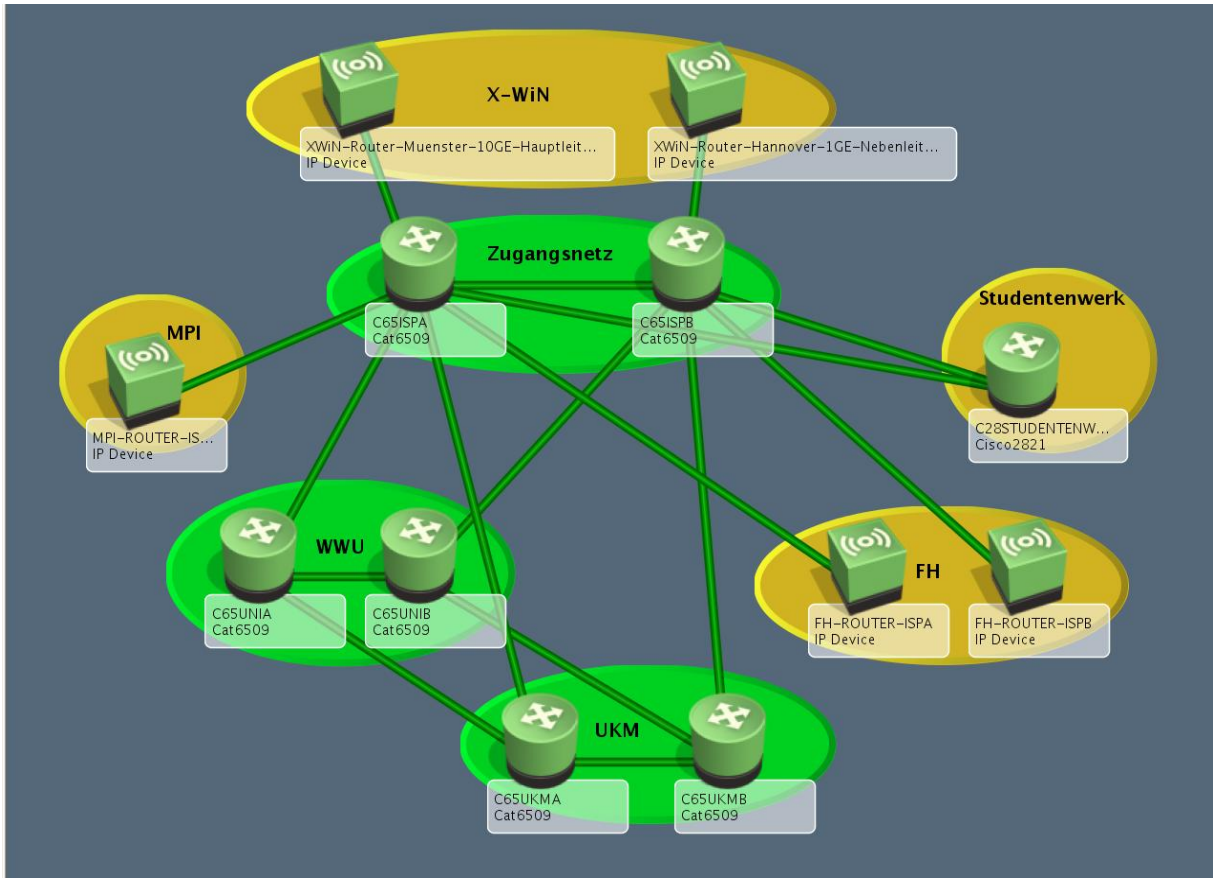


Abb. 5: Wissenschaftsnetz Münster (WNM) - Die "grünen" Netze werden vom ZIV betrieben. Dargestellt sind die physikalischen Verbindungen (1GE od. 10GE) zwischen Routern. Zwischen WWU und UKM existieren auch direkte Verbindungen für die Realisierung von Layer2-Funktionen (auf beide Netze ausgedehnte VLANs).

Für die Zukunft ist geplant, die Verfügbarkeit der X-WiN/Internet-Anbindung des WNM (und damit der WWU und des UKM) über das Zugangsnetz noch weiter zu verbessern, da die Verfügbarkeitsanforderungen an die Internet-Anbindung weiterhin zunehmen werden (z.B. für VoIP). Im Moment stellt der Raum, in dem die X-WiN Kernnetzkomponenten angesiedelt sind, noch einen Single Point of Failure (SPoF) dar, da eine Abhängigkeit von den aktiven Komponenten (DWDM-Technik) in diesem Raum gegeben ist. Auch die bereits realisierte zusätzliche Anbindung an einen weiteren Kernnetzrouter des X-WiN an einem anderen Standort (sog. "Nebenleitung") verbessert zwar die Situation, da nun keine Abhängigkeit mehr vom X-WiN-Router in Münster gegeben ist, allerdings besteht immer noch die Abhängigkeit vom DWDM-Equipment hier in Münster.

1.5.2 Intranet / LAN

Für die WWU erbringt das ZIV ein umfassendes Spektrum an Netzdiensten von der Planung über die Installation bis hin zum Betrieb. Die Netzdienste erstrecken sich hierbei zum Einen über die gesamte passive Kommunikationsinfrastruktur der WWU: das LWL-Backbone, die Gebäudeverkabelung und die Netzanschlussdosen in den einzelnen Räumen. Auch die aktive Kommunikationsinfrastruktur wird vollständig vom ZIV geplant, installiert und betrieben. Über die reinen Netzkomponenten (Router, Switches, WLAN Access Points, ...) hinaus liegen auch die netzseitigen Sicherheitsfunktionen und die CNSs (Core Network Services: DNS, DHCP, RADIUS, ...) im Zuständigkeitsbereich des ZIV.

Für den Zugang zum Kommunikationssystem wird eine Reihe von Zugangstechnologien unterstützt:

- LAN-Festanschlüsse für registrierte Endsysteme
- WLAN
- VPN
- "öffentliche" LAN-Festanschlüsse mit VPN-Zugangsmöglichkeit für nicht registrierte Endsysteme (sog. *pLANet*-Anschlüsse: persönlicher LAN-Netzzugang)
- DSL/PPPoE

Der Netzzugang mit 802.1X ist noch nicht in nennenswertem Umfang realisiert. Für eine flächendeckende Einführung dieser Technologie muss ein erheblicher Teil der eingesetzten Switches ausgetauscht werden.

Eine über die hier erfolgte erste grobe Darstellung von Netzdiensten hinausgehende Beschreibung erfolgt in Abschnitt 1.6 *„Vorhandene und angestrebte Netzstruktur“*.

1.5.3 TK-Netz

Die aktuelle Situation und die Planungen im TK-Bereich sind stark geprägt von der Thematik Konvergenz von Tele- und Datenkommunikation. Hierauf wird daher gesondert innerhalb des gleichnamigen Abschnitts eingegangen.

1.5.4 Telefon- und Video-Konferenzen

Für Telefonkonferenzen wird eine eigene MCU (Multipoint Control Unit) betrieben. Für Videokonferenzen wurde ein zentraler Videokonferenzraum mit einem leistungsfähigen HD-tauglichen Konferenzsystem geschaffen. An mehreren Stellen der WWU sind weitere fest installierte oder mobile Konferenzsysteme verfügbar. Ein H.323 Software-Client, der die Standards H.261, H.263 und H.264 unterstützt, wird vom ZIV für Notebooks oder auch PCs angeboten. Das ZIV berät bei der Nutzung des DFN VC Dienstes.

1.5.5 Intranet / Mediennetze (AVM: Audiovisuelle Medien)

Im Laufe der vergangenen Jahre wurden 211 Räume, Hörsäle und Seminarräume mit Medientechnik ausgestattet. So wurden beispielsweise allein 48 Räume im Jahr 2008 neu mit Medientechnik ausgestattet. Die Standards der Ausstattung reichen von Beamer-Installationen mit Audiounterstützung in kleinen Seminarräumen bis hin zu komplexen Multimedia-Installationen in Hörsälen. In der Vergangenheit wurde bei der Konzeptionierung und Installation darauf geachtet, dass zukünftige Technologien bei der Installation der Infrastruktur bereits berücksichtigt wurden. Als Beispiele seien erwähnt, dass sowohl die Beamer-Standorte als auch die medientechnischen Zentralen mit LAN Anschlüssen versehen wurden und die Einbettung der Hörsäle und Seminarräume in die Videokonferenzinfrastruktur möglich ist.

1.5.6 Weitere Netzdienste an der WWU

Über die zum engeren Bereich der Kommunikationsnetze gehörenden Dienste hinaus betreibt das ZIV weitere wesentliche Netzdienste:

- Zentrales Identitätsmanagement-System und Benutzer-, Rechte- und Rollenverwaltung (vgl. Abb. 6): Provisionierung von Zielsystemen des ZIV und der IVVen mit Benutzer-, Rechte- und Rollendaten. Unter anderem sind die Benutzerdaten auch via einen angebundenen LDAP-Server abfragbar (z.B. Auch für VoIP-Telefone).
- Web Single Signon System Shibboleth (Identity Provider im Identitätsmanagementsystem): Authentifizierung und Authorisierung für webbasierte Informationssysteme (beispielsweise für eLearning). Insbesondere für Bibliotheksdienste ist hier die Integration mit der DFN AAI in Umsetzung.
- Zentraler Web-Server-Park: auf dieser hochverfügbaren und skalierbaren Plattform wird allen Einrichtungen der Universität das Hosting von Web-Präsentationen und Anwendungen angeboten. Das zentrale Content Management System Imperia wird darüber bereitgestellt. Zwar betreiben zwei Fachbereiche noch eigene Webpräsentationen mit stark anwendungsintegrierten CMS, doch wird die zentrale Web-Plattform des ZIV immer stärker genutzt (bereits wesentlich mehr als die Hälfte der Lehrstühle).
- eLearning Systeme: Das ZIV stellt die Betriebsplattform (im Wesentlichen über den zentralen Web-Server-Park) für die weitest verbreiteten eLearning Systeme (Moodle und die Eigenentwicklung OpenUSS) an der WWU bereit.
- Zentraler Oracle RAC Datenbank-Cluster: Eine hochverfügbare Serverplattform für die über einer NRW Landeslizenz beschaffte Orcale RAC (Real Application Cluster) Datenbank wird vom ZIV für die WWU betrieben.
- Zentraler eMail Service: ein zentrales eMail Gateway (mit Virus/SPAM Filter) wird vom ZIV für die WWU betrieben und umfassend genutzt. Der IMAP-Dienst des ZIV steht allen Mitarbeitern und Studierenden der WWU offen und wird umfänglich genutzt (derzeit wird dazu auch das im Haus entwickelte WebMail Frontend permail angeboten). Vom ZIV wird weiterhin ein auf Microsoft Exchange basierender Groupware-Service für die zentralen Einrichtungen und Gremien der WWU bereitgestellt.
- Active Directory und Fileservices: Das ZIV betreibt gemeinsam mit den IVVen das Active Directory für das Windows Domain Netzwerk. An allen an das Datennetz der WWU angebundenen Arbeitsstationen ist ein Netzwerk-Login obligatorisch. Fileservices für Mitarbeiter und Studierende werden beispielsweise über das Scale-out Filesystem angeboten.
- Festplattenspeicher und virtuelle Maschinen: Das ZIV stellt für Einrichtungen der WWU Plattenplatz in zentralen virtualisierten Speichernetzwerken bereit sowie virtuelle Maschinen auf einem zentralen VMware ESX Cluster. Dies soll auch die Basis für das im Aufbau befindliche Enterprise Content Management System (ECM) der Universitäts- und Landesbibliothek(ULB) bilden. Daran angebunden ist auch der vom ZIV betriebene Streaming-Server für in Web-Seiten integrierten Video-Content.
- Archiv- und Backupsystem: Das ZIV stellt ein zentrales TSM-Bandarchivsystem für Datenarchivierung- und Backup bereit.
- Print-Service: Über ZIVprint sind zahlreiche Drucker für Mitarbeiter und Studierende zugänglich. Ca. 450 Multifunktionsgeräte sind WWU-weit über das Datennetz angebunden und können neben der Funktion als Kopierer auch als Drucker und Scanner genutzt werden.

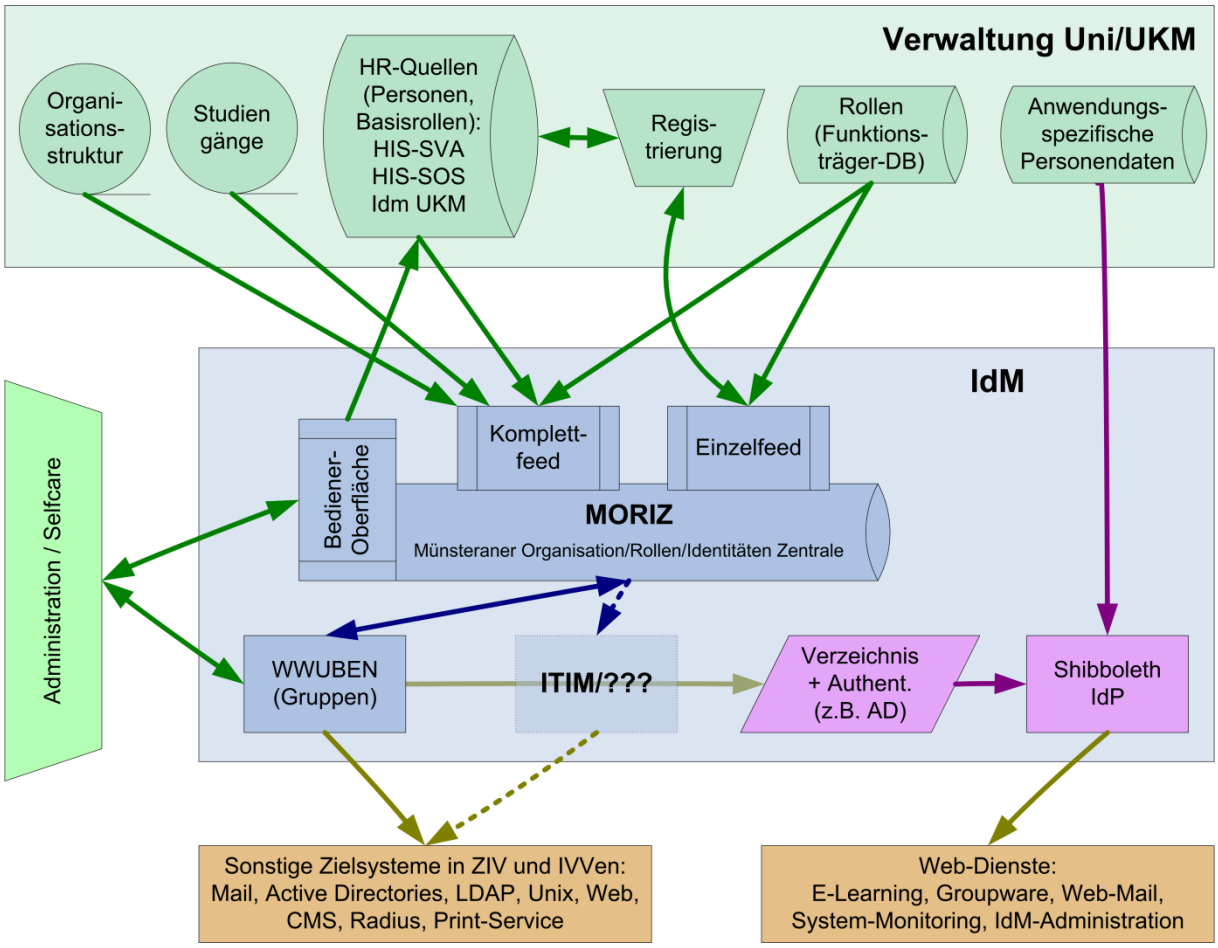


Abb. 6: Die Struktur des Identitätsmanagementsystems (IdM) der WWU mit den Schnittstellen für den Datenimport sowie für die Provisionierung verschiedenster Zielsysteme. Ein Produkt für die Provisionierung als Ersatz für IBM Tivoli TIM (ITIM) wird derzeit evaluiert.

Darüber hinaus werden im UKM zahlreiche klinikumsweit genutzte Informationssysteme (z.B. Patientenverwaltungssystem Medico/S, Krankenaktensystem ORBIS, PACS-System der Firma GE) über das Datennetzwerk betrieben. Auch die Datenübertragung der bildgebenden Modalitäten, die mit aktuellen Verfahren zur hochauflösenden und funktionalen Bildgebung immer umfangreichere Datensätze liefern, erfolgt mit sehr hohen Verfügbarkeitsanforderungen über das gemeinsame Datennetzwerk.

Für das derzeit in Beschaffung befindliche High Performance Computing System ist eine leistungsfähige Anbindung mit 10GE an das Datennetz vorgesehen, da hier sehr große Datenmengen sowohl zur Analyse importiert (z.B. im Bereich der Lebenswissenschaften – medizinische Bilddaten und bioinformatische Datensätze) wie auch Berechnungsresultate mit hohem Datenvolumen exportiert und an Visualisierungssysteme weitergeleitet werde müssen.

1.6 Vorhandene und angestrebte Netzstruktur

1.6.1 Grundsätze des Netzdesigns: Verfügbarkeit und eingebettete Sicherheit

Das gesamte Netzdesign der WWU und des UKM ist von zwei Grundsätzen bestimmt: Verfügbarkeit und eingebettete Sicherheit.

Die Gewährleistung der Ausfallsicherheit in Rechnernetzen ist in den letzten Jahren vermehrt in den Vordergrund gerückt. Dies ist insbesondere durch die verstärkte Verbreitung bzw. Einführung neuer Dienste und Technologien sowie die zunehmende Zentralisierung zu erklären. Im Netz von WWU und UKM wird dabei folgender Ansatz verfolgt: Eine verbesserte Verfügbarkeit des Netzes wird primär nicht durch die Erhöhung der Verfügbarkeit eines einzelnen Gerätes (z.B. redundante Module in einem Gerät) sondern durch den Betrieb von zwei Geräten mit identischer Funktionalität erzielt (Gerätedopplung). Einzige Ausnahme hiervon ist die redundante Ausstattung mit Netzteilen. Auf eine redundante Ausstattung mit einer zweiten Supervisor Engine o.ä. wird verzichtet. Abgesehen vom Edge-Bereich soll diese Gerätedopplungsstrategie beginnend mit dem Distribution-Bereich (s.u.) konsequent umgesetzt werden. Die beiden Geräte werden dabei an unterschiedlichen Standorten aufgestellt. Bei einem Ausfall können sich die Geräte gegenseitig ersetzen. Auch Wartungsmaßnahmen können durch diese Gerätedopplung in der Regel für die Nutzer unterbrechungsfrei erfolgen. Von den meisten Gerätetypen existiert neben den produktiven Geräten ein Ersatzgerät, das auch für Testzwecke genutzt werden kann.

Mit dem Konzept der in das Netz eingebetteten Sicherheit soll das Gefährdungspotenzial für ganze Netzbereiche erheblich reduziert werden. Zu den Sicherheitsfunktionen gehören beispielsweise Paketfilter, Firewall- und Intrusion Prevention-Funktionalität. Essentiell im entworfenen Sicherheitsdesign ist das Konzept der *Netzzone*. Netzzonen enthalten Endsysteme mit identischem Sicherheitsbedarf. Dabei wird eine Hierarchie von Netzzonen aufgebaut. Diese Netzzonen-Strukturierung entspricht den vorhandenen Informationsverarbeitungs-Strukturen an der WWU und dem UKM. Für eine Netzzone können die o.g. Sicherheitsfunktionen bedarfsgemäß eingerichtet werden. Der Vorteil dieser Vorgehensweise ist, dass sie unabhängig von den ebenfalls notwendigen Maßnahmen auf den Endsystemen oder im organisatorischen Bereich wirksam ist. Eine ausführliche Darstellung findet man im Abschnitt 1.6.5 *„Konzept der netzseitigen IT-Sicherheitsmaßnahmen“*.

1.6.2 Begriffsklärungen

Zwischen folgenden aufeinander hierarchisch aufbauenden Netzbereichen wird nach topografischen und funktionalen Gesichtspunkten unterschieden:

Netzbereich	Funktion
Edge	Anbindung von Endsystemen, nur Layer2-Funktionalität
Distribution	Aggregierung von Edge-Devices, nur Layer2-Funktionalität, Einführung dieses Bereiches u.a. um kostengünstig 10GE-Technologie einsetzen zu können, Anbindung von Servern
Midrange	Nebenstandorte zur Aggregierung von Distribution-Devices großer Netzbereiche, Anbindung von Data Centern, Layer3/IP-Funktionalität
Core	Hauptstandorte zur Kopplung der Midrange-Bereiche, Layer3/IP-Funktionalität, Realisierung zentraler Netzfunktionen (WLAN-Switching, Security-Funktionen: Paketfilter, Firewall-Funktionalität, Intrusion-Prevention, VPN)
Inter-Core	Kopplung von Netzen verschiedener Einrichtungen (konkret: das WNM-Zugangsnetz)

Tabelle 6: Definition von Bezeichnungen für Netzbereiche

Edge, Distribution, Midrange und Core bezeichnen dabei Teilbereiche eines Netzes einer einzelnen Einrichtung (z.B. WWU, UKM). Mit Inter-Core wird ein Netzbereich bezeichnet, der die IP-Verbindung der Netze verschiedener Einrichtungen miteinander verbindet und die Verbindung zum Internet herstellt. Es sei bereits an dieser Stelle ausdrücklich erwähnt, dass die konsequente Einführung des Distribution-Bereichs eine noch in großem Umfang zu realisierende Aufgabe ist.

1.6.3 Grobe topografische und funktionale Struktur der Netze von WWU und UKM

Ausgehend von der bereits erfolgten Darstellung von Topografie und Gebäudebestand ist die grobe topografische Struktur der Netze von WWU und UKM in Tabelle 7, Tabelle 8 und Abb. 7 bis Abb. 9 zusammengefasst. Dabei sind die Switches des Inter-Core-Bereichs der WWU zugeordnet. Auch die Core-Switches für die Security-Funktionen und das WLAN-Switching, die auch vom UKM genutzt werden, sind der WWU zugeordnet. Wie aus den Darstellungen deutlich wird, sind an den beiden Hauptnetzstandorten ZIV-Gebäude Einsteinstraße und ZIV-Gebäude Röntgenstraße die zentralen Geräte/Funktionen in redundanter Form konzentriert. Jeder Nebenstandort ist mit beiden Hauptstandorten verbunden. Die TK-Technik ist am Standort ZIV-Gebäude Orleansring konzentriert.

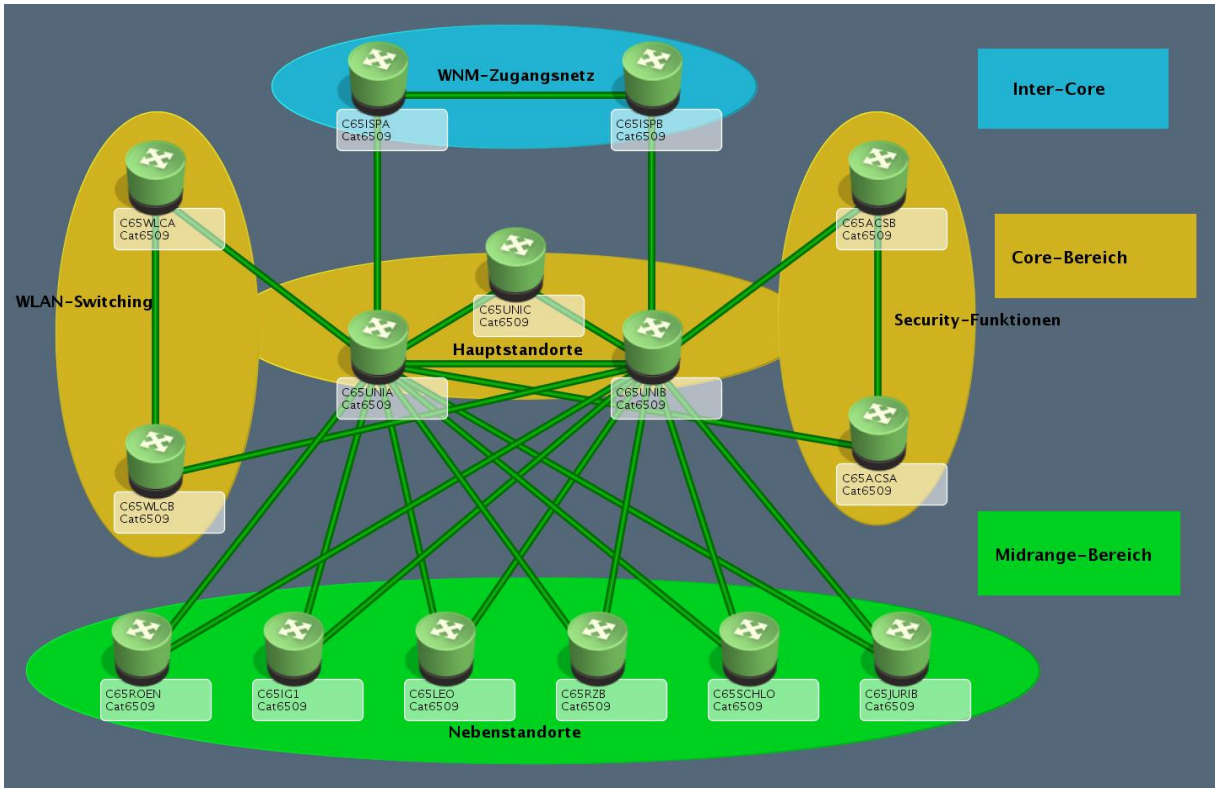


Abb. 7: Struktur des Netzes der WWU - dargestellt sind die physikalischen Verbindungen (10GE oder 1GE-Aggregierung) zwischen Switches.

Netzbereich	Standorte	Besonderheiten	eingesetzter Gerätetyp
Inter-Core	ZIV Einsteinstraße	-	1 x Cisco C6509
	ZIV Röntgenstraße	-	1 x Cisco C6509
Core	ZIV Einsteinstraße	-	1 x Cisco C6509
	ZIV Einsteinstraße	Security-Funktionen	1 x Cisco C6509
	ZIV Einsteinstraße	WLAN-Switching	1 x Cisco C6509
	ZIV Röntgenstraße	-	1 x Cisco C6509
	ZIV Röntgenstraße	Security-Funktionen	1 x Cisco C6509
	ZIV Röntgenstraße	WLAN-Switching	1 x Cisco C6509
	ZIV Orleansring	IP-Routing-Redundanz	1 x Cisco C6509
Midrange / Nebenstandorte	ZIV Einsteinstraße, s.u. (1.)	-	1 x Cisco C6509
	ZIV Röntgenstraße, s.u. (1.)	-	1 x Cisco C6509
	Institutsgruppe 1 im Naturwissenschaftlichen Zentrum	-	1 x Cisco C6509
	Schloss	-	1 x Cisco C6509
	Juridicum	-	1 x Cisco C6509
	Leonardo-Campus	-	1 x Cisco C6509
Distribution	diverse	-	weitgehend Planung: HP 5412zl
Edge	diverse	-	diverse Hersteller, hauptsächlich: HP, 3Com, Avaya, Nexans

Tabelle 7: Grober Überblick über Struktur und Geräte des Netzes der WWU

Bemerkungen zur Tabelle 7:

1. Auch an den beiden Hauptstandorten befindet sich je ein separater Midrange-Switch für die Aggregierung von Distribution-Switches.

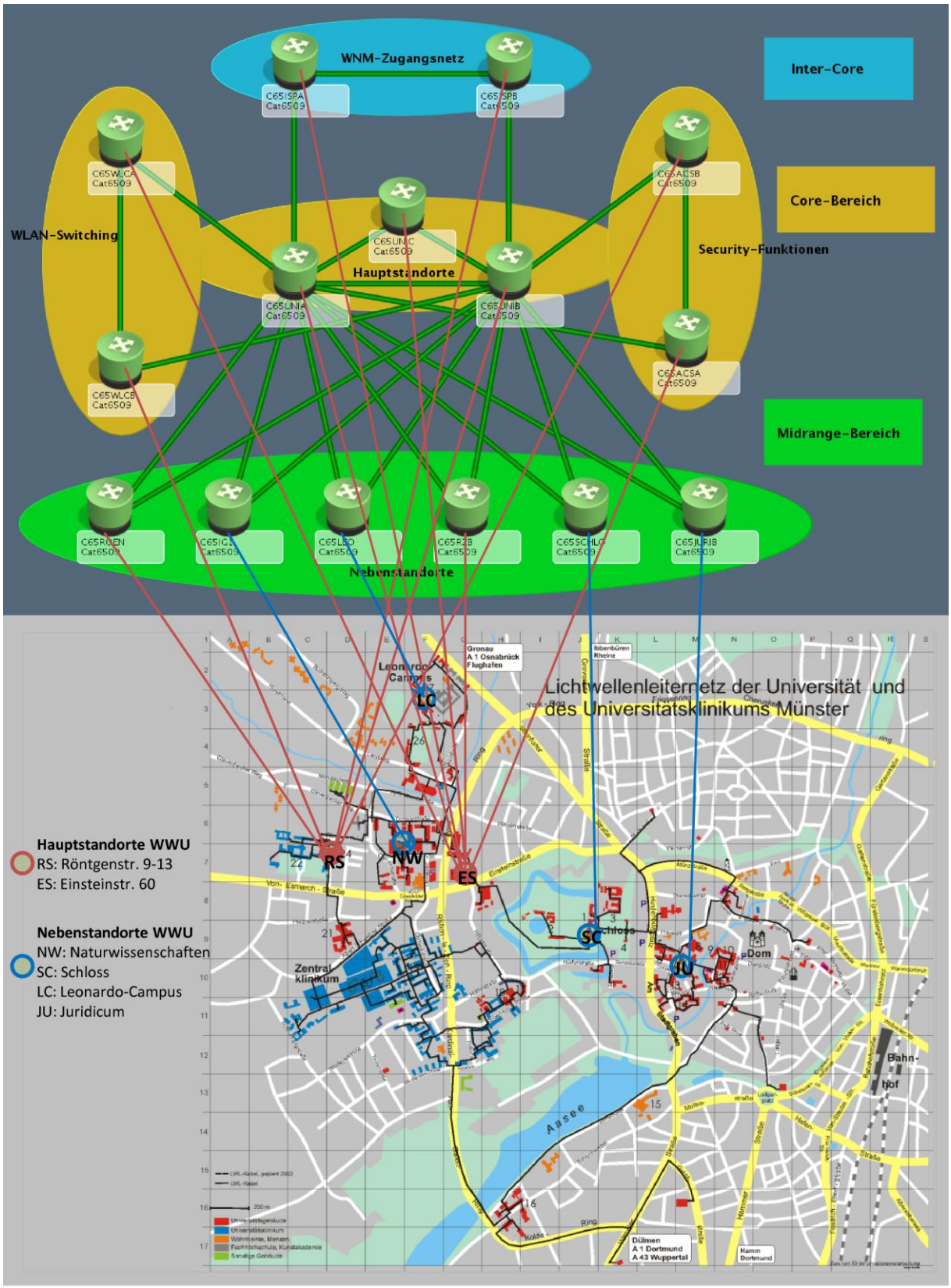


Abb. 8: Kernnetzkomponenten der WWU mit Zuordnung zu Standorten (hochauflösende Version der Abb. im Anhang)

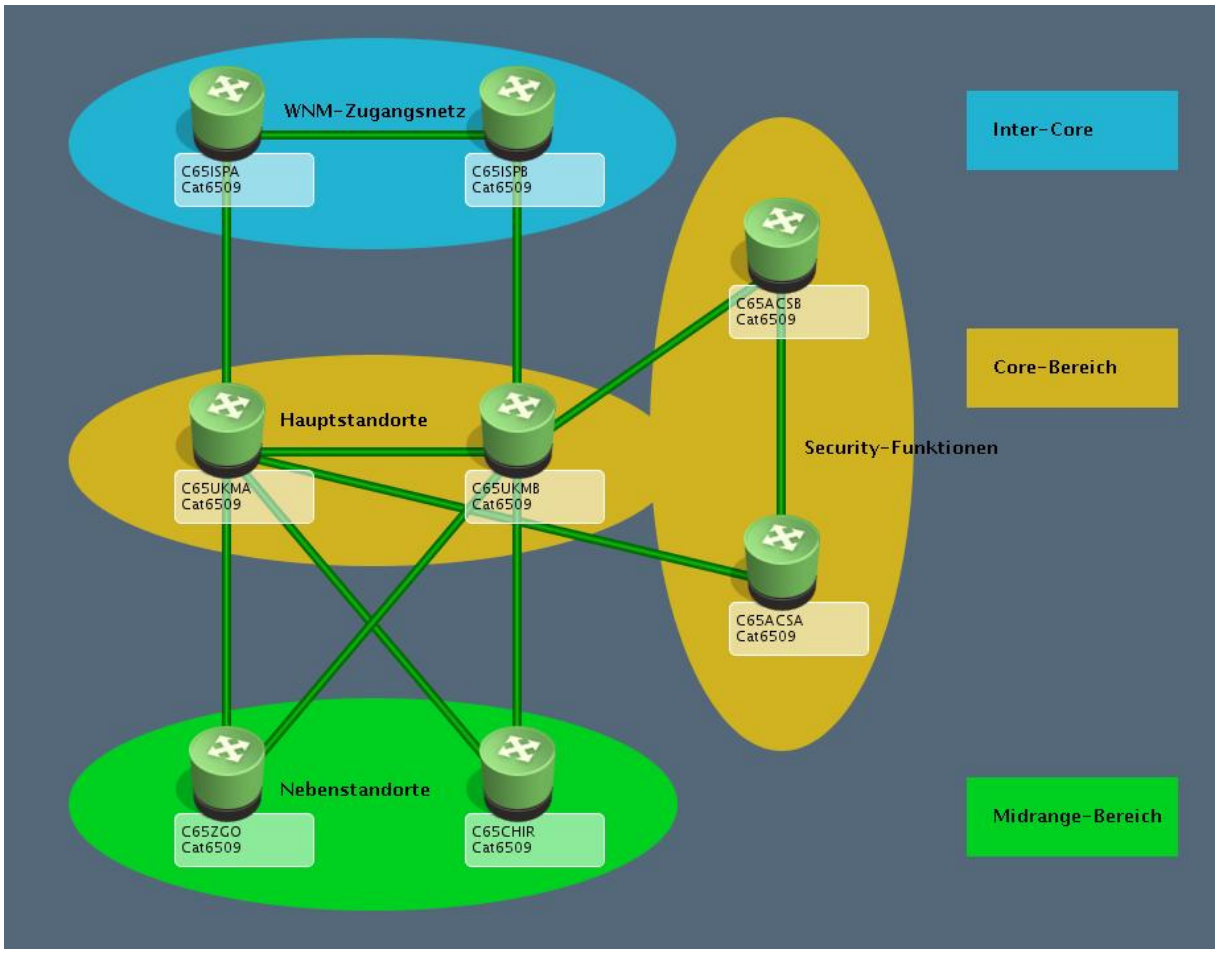


Abb. 9: Struktur des Netzes des UKM – dargestellt sind die physikalischen Verbindungen (10GE oder 1GE-Aggregierung) zwischen Switches. Zur Verdeutlichung sind die Switches des WNM-Zugangsnetzes und der Security-Funktionen hier ebenso wie bei der WWU (vgl. Abb. 7) dargestellt. Physikalisch befinden sich diese Switches in der WWU und sind auch der WWU zugeordnet. Die direkte physikalische Anbindung der WLAN-Switches an die Core-Switches an den Hauptstandorten des UKM ist noch nicht realisiert.

Netzbereich	Standorte	Besonderheiten	eingesetzter Gerätetyp
Core	Zentralgebäude West	-	1 x Cisco C6509
	Gebäude Alte Post	-	1 x Cisco C6509
Midrange	Zentralgebäude Ost	-	1 x Cisco C6509
	Chirurgische Klinik	-	1 x Cisco C6509
Distribution	diverse	-	weitgehend Planung: HP 5412zl
Edge	diverse		diverse Hersteller, hauptsächlich: HP, 3Com, Avaya, Nexans

Tabelle 8: Grober Überblick über Struktur und Geräte des Netzes des UKM

1.6.4 Ausführliche Darstellung der Netzstruktur

1.6.4.1 Endgerätezugangsbereich

Bei der strukturierten Verkabelung innerhalb von Gebäuden von WWU und UKM wird darauf geachtet, möglichst wenige Verteilerstandorte innerhalb eines Gebäudes zu realisieren. Das bedeutet, dass in der Regel auf eine Sekundärverkabelung verzichtet wird. Dies wird als die auf lange Sicht gesehen kostengünstigere Realisierungsmöglichkeit erachtet, da auf Grund des höheren Ausnutzungsgrades weniger aktive Technik zum Einsatz kommt.

Da in der Vergangenheit immer auf hochwertige Verkabelungssysteme geachtet wurde, ist überwiegend eine Tertiärverkabelung vorhanden, die den Standard Cat5e übertrifft. Neu installierte Verkabelung entspricht derzeit dem Cat6-Standard. Damit ist die überwiegende Zahl an Endgeräteanschlusspunkten Gigabit-fähig. Auch zukünftig sollen nur hochwertigste Verkabelungssysteme zum Einsatz kommen.

1.6.4.2 LWL-Netz

Von folgenden Grundannahmen zur Verfügbarkeit wird beim Konzept des Ausbaus des LWL-Netzes ausgegangen:

- Der Ausfall von LWL-Verbindungen (Kabeldefekte) ist ein vergleichsweise seltenes Ereignis.
- Der Ausfall aktiver Komponenten oder mehr noch Softwareprobleme auf aktiven Komponenten sind sehr viel wahrscheinlicher.
- Neben Redundanzkonzepten ist ein geregeltes Change-Management (Vermeidung von Störungen durch Konfigurationsfehler) für die Verfügbarkeit von größter Bedeutung.

Aus diesen Grundannahmen leiten sich folgende Grundsätze für die LWL-Anbindung von einzelnen Gebäuden, die für das Netz keine strukturelle Bedeutung haben, ab:

- Im Normalfall (d.h. Gebäude ohne erhöhte Verfügbarkeitsanforderungen) erfolgt für ein Gebäude keine redundante LWL-Anbindung.
- In Einzelfällen wird für Gebäude mit erhöhten Verfügbarkeitsanforderungen (z.B. Lokationen mit zentralen Services, ...) eine redundante LWL-Anbindung angestrebt.
- Für normale VoIP-Endnutzer-Kommunikation ergeben sich keine erhöhten Verfügbarkeitsanforderungen in Bezug auf LWL-Anbindung von Gebäuden.

Zur Erhöhung der Verfügbarkeit sollen einzelne Netzbereiche über ein Paar von Distribution-Switches angebunden werden (vgl. Abb. 10). Edge-Switches werden im Normalfall mit einem der Distribution-Switches verbunden. Bestehen für einen Edge-Bereich erhöhte Verfügbarkeitsanforderungen, so wird der entsprechende Edge-Switch mit beiden Distribution-Switches verbunden. Die Distribution-Switches sollen untereinander verbunden und jeweils eine Verbindung zum übergeordneten Midrange-Switch besitzen. Ein Midrange-Switch hat je eine Verbindung zu beiden Core-Switches. Die Core-Switches sind untereinander verbunden.

Das beschriebene Konzept ist bereits im Core- und Midrange-Bereich umgesetzt worden. Die Implementierung des Distribution-Bereichs ist bislang exemplarisch in einigen Bereichen vorgenommen worden. Die netzweite Umsetzung dieses Konzepts ist allerdings eine im Zuge dieses Antrags noch zu leistende umfangreiche Aufgabe.

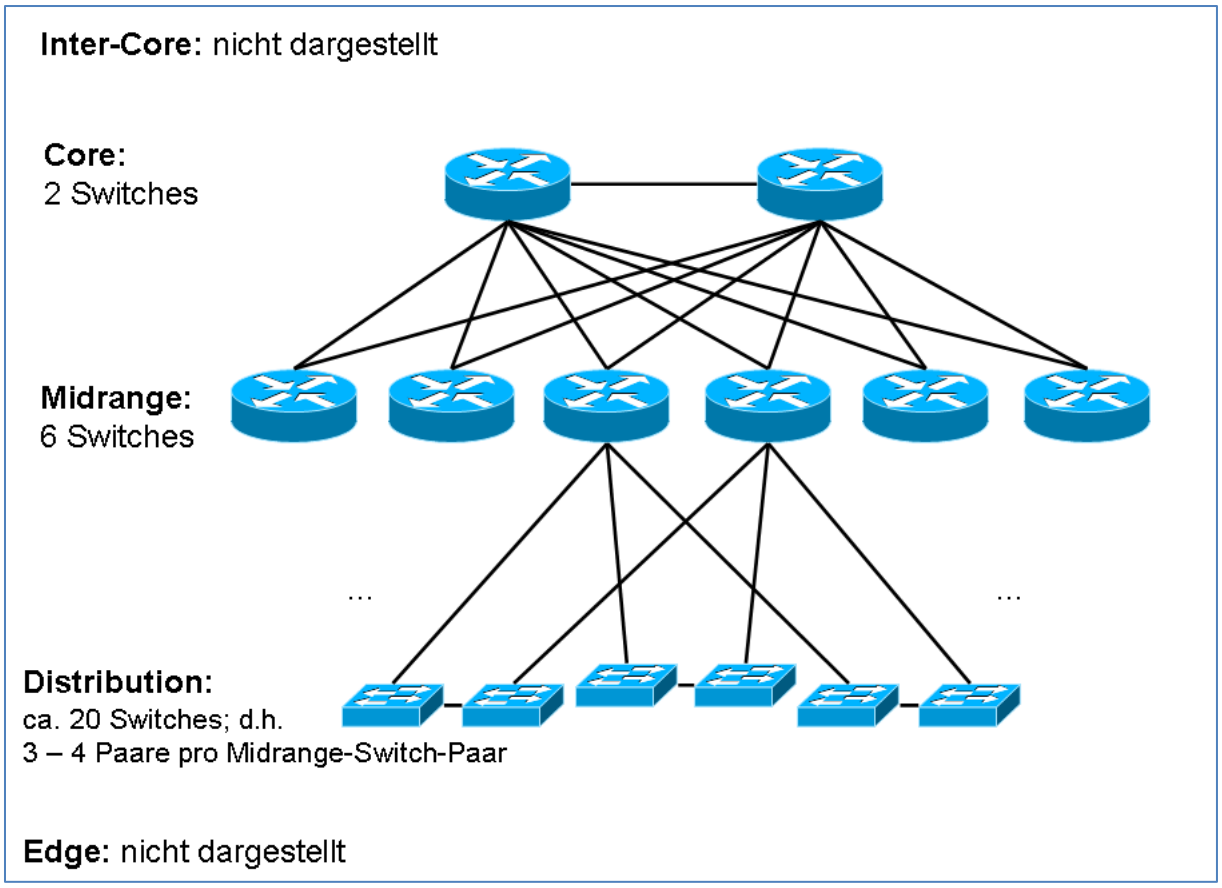


Abb. 10: Geplante Netzstruktur bzgl. des noch im Aufbau begriffenen Distribution-Bereichs

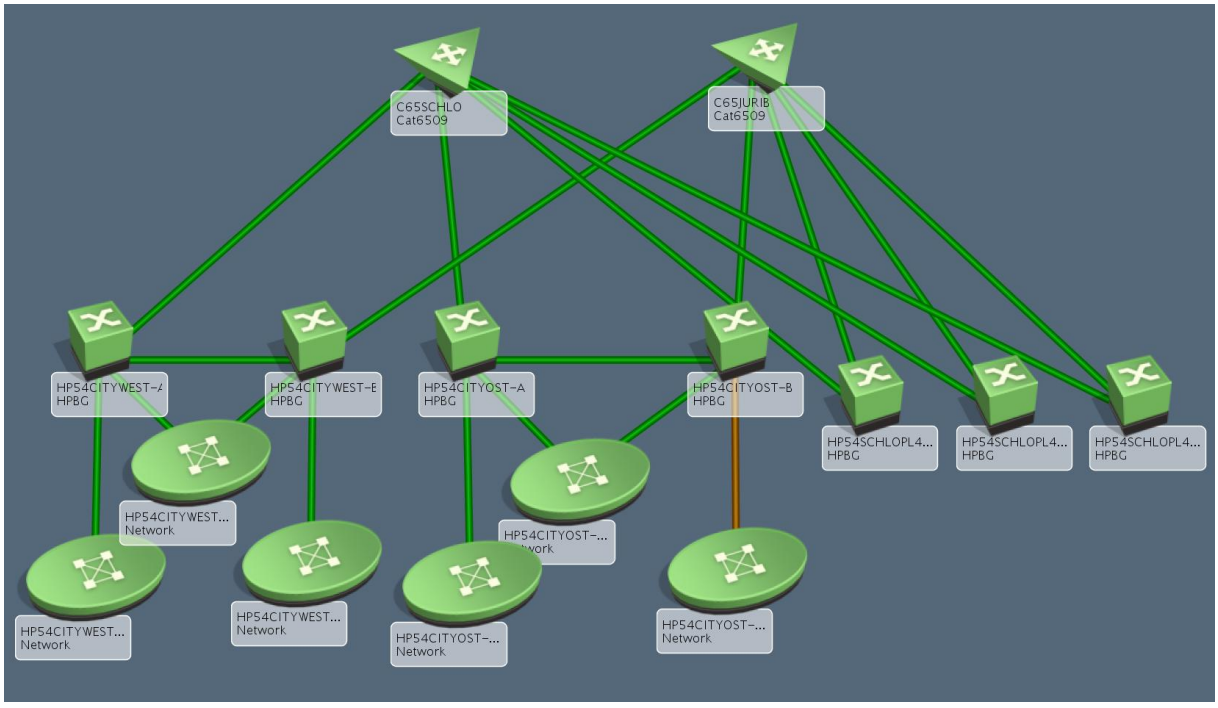


Abb. 11: Exemplarische Realisierung einer Verbindung zwischen Midrange- und Distribution-Switches. Die (einfach oder doppelt angebundenen) Edge-Switches sind nur in zusammengefasster Form dargestellt. Die 3 Distribution-Switches ohne angehängten Edge-Bereich binden einen zentralen Server-Standort an.

Die noch in großem Umfang vorhandenen Anteile an Multimode-Kabeln im LWL-Netz von WWU und UKM sollen vollständig durch Singlemode-Kabel ersetzt werden.

1.6.4.3 Layer2-Strukturen

Auf Layer-2 wird die “Virtual-Bridged-Local-Area-Network (VLAN)”-Technologie gemäß dem IEEE 801.Q Standard eingesetzt. Dabei ist ein einzelnes VLAN grundsätzlich nicht auf einen bestimmten geografischen Bereich beschränkt. Die Ports eines VLANs können sich an beliebiger Stelle im Netz (d.h. im ganzen Stadtgebiet von Münster) befinden. Folgende VLAN-Typen werden unterschieden:

- 990 Endnutzer-VLANs: Anschluss von Endgeräten unterschiedlichster Art (insb. auch Server, VoIP-Telefone)
- 479 Transfer-VLANs: VLAN zur Verbindung von IP-Routern (physischen und virtuellen)
- 39 Insel-VLAN: abgeschottete Netzbereiche ohne IP-Verbindung zum Rest des Netzes
- 115 VPNSM-VLANs: für die direkte VPN-Einwahl in ein Endnutzer-VLAN

VLANs sind dabei die im Moment vorherrschende technische Realisierungsvariante für die in Konzept der netzseitigen IT-Sicherheitsmaßnahmen beschriebenen Netzzonen.

Für das Routing auf Layer2 wird die STP-Protokollfamilie (Spanning Tree Protocol) eingesetzt. Dabei sind zwei voneinander unabhängige STP-Bereiche zu unterscheiden.

- Core/Midrange: Hier kommt Rapid PVST (Per VLAN Spanning Tree) zum Einsatz, da es hiermit möglich ist, sämtliche vorhandenen redundanten physikalischen Verbindungen auch zu nutzen und nicht einfach abzuschalten. Konkret werden die VLANs mit geraden und ungeraden Nummern auf die beiden vorhandenen Verbindungen zwischen Core- und Midrange-Switch aufgeteilt.
- Distribution/Edge: Hier kommt RSTP (Rapid Spanning Tree Protocol) zum Einsatz, da die eingesetzten Geräte PVST nicht unterstützen.

Die Distribution-Switches leiten die Rapid PVST-Pakete der Midrange-Switches (auch über ihre Querverbindung) transparent weiter. In der Konsequenz sind beide Verbindungen zwischen Midrange- und Distribution-Switch aktiv, wobei aber pro VLAN real nur eine benutzt wird.

Als Variante der VLAN-Technologie kommt bei den mit DSL/PPPoE-Technologie versorgten Wohnheimen des Studentenwerks Münster auch das sog. Q-in-Q (gemäß IEEE 802.1ad) zum Einsatz. Das "äußere" VLAN identifiziert dabei das einzelne Wohnheim. Die einzelnen DSL-Nutzer werden über die "innere" VLAN-Nummer unterschieden.

Der Ansatz, die VLAN-Technologie intensiv zu nutzen, hat sich in der Vergangenheit bewährt und soll fortgeschrieben werden. Eine Konsequenz des oben erläuterten Konzepts ist ein großer Bedarf an VLANs. Durch die für die Umsetzung des IT-Sicherheitskonzeptes erforderliche, noch in großen Teilen umzusetzenden Strukturierungsmaßnahmen ("Bilden von Netzzonen"), wird dieser Bedarf zukünftig noch größer. Auch zukünftige Dienste oder der Ausbau vorhandener Dienste (VoIP) werden weiteren VLAN-Bedarf verursachen. Bis vor kurzem wurde für sämtliche verwendeten VLANs ein gemeinsamer Nummernraum verwendet. Es werden zukünftig verschiedene getrennte VLAN-Nummernräume für einzelne Bereiche eingerichtet werden: z.B. WWU-VLANs, UKM-VLANs, Transfer-VLANs, Data Center-VLANs.

1.6.4.4 Layer3-Strukturen

In Edge- und Distribution-Bereich kommen keine Layer3-Funktionen zum Einsatz. Die für die Layer3-Funktionen zuständigen Geräte im Midrange- und Core-Bereich werden dabei nicht als eine einzige IP-Router-Instanz betrieben. Durch den Einsatz des Cisco IOS-Features VRF-lite wird die IP-Router-Funktionalität virtualisiert und kommt vielfach auf einem Gerät zum Einsatz. Im Abschnitt 1.6.5 *„Konzept der netzseitigen IT-Sicherheitsmaßnahmen“* wird erläutert, warum eine große Anzahl an IP-Routing-Instanzen erforderlich ist. Die virtuellen Router (kurz VR) werden dabei sowohl für die Layer3-Anbindung von peripheren IP-Subnetzen für Endsysteme als auch für den Aufbau einer Hierarchie von VRs für die Realisierung des Konzepts der netzseitig eingebetteten Sicherheitsfunktionen eingesetzt. Auch bei den VRs wird dabei konsequent die Gerätedopplungsstrategie fortgesetzt. Ein VR-Paar wird dabei auf die Chassis zweier Midrange- oder Core-Switches aufgeteilt. Insgesamt sind derzeit ca. 230 aktive VRs (WWU und UKM) realisiert.

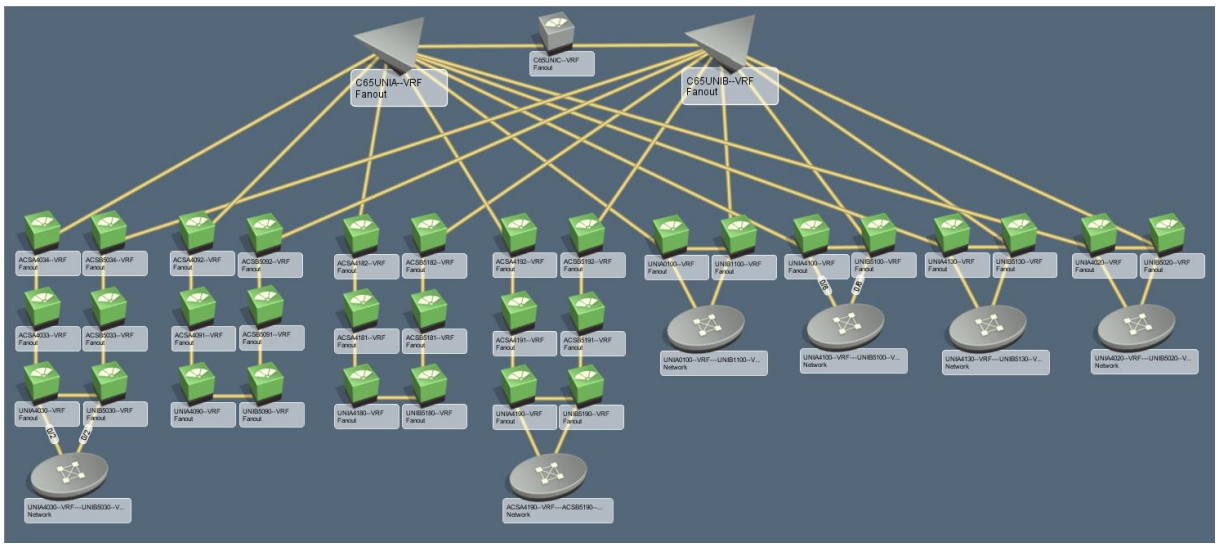


Abb. 12: Exemplarische Darstellung eines Teils der VR-Struktur. Die grünen Symbole repräsentieren dabei einen virtuellen Router (VR). Zu erkennen sind auch die VR-Paare und die Transfer-VLANs/Subnetze zwischen den VRs.

Zur Erhöhung der Verfügbarkeit von Default-Gateways kommt in den IP-Subnetzen, über die Endsysteme angebunden werden, durchgängig HSRP zum Einsatz. In den Netzen von WWU und UKM wird OSPF als Interior Gateway Protocol auf den physischen und virtuellen Routern eingesetzt. Im Inter-Core-Bereich kommt BGP als Exterior Gateway Protocol für das Routing zwischen dem Zugangsnetz und den angeschlossenen Einrichtungen und zum X-WiN zum Einsatz.

Das beschriebene Layer3-Design hat sich in der Vergangenheit bewährt und soll fortgeschrieben werden.

1.6.4.4.1 IP-Multicast

IP-Multicast-Routing ist derzeit nicht konfiguriert. Es ist beabsichtigt, eine Multicast-Anbindung an den DFN und ein netzinternes PIM-Routing im Core- und Midrange-Bereich zu realisieren. Ein Multicast-Routing in Endnetze soll nur nach Absprache und Anforderung erfolgen. Als Multicast-Anwendungen sind beispielsweise die Nutzung diverser internationaler multicast-basierender Angebote, IPTV (Internet Protocol Television), Live-Streaming und effiziente Softwareverteilung denkbar. Das IP-Multicast-Routing stellt zukünftig die Basistechnologie für die Übertragung von

Veranstaltungen und Vorlesungen dar. Im Abschnitt 1.6.8 *“Mediennetze, AVM (Audiovisuelle Medien)“* wird die weitere geplante Entwicklung näher dargestellt.

1.6.4.4.2 IPv6

Seit 1994 besteht eine IPv6-Anbindung der WWU. Jedoch erfolgt das Routing nur in wenige Teilbereiche des Netzes und nur mit dedizierten Routern; d.h. ein natives IPv6-Routing auf den Core/Midrange-Routern ist noch nicht realisiert. Wegen des langjährigen an der WWU angesiedelten JOIN-Projekts (Join Open Inter Networks) liegen gute IPv6-Kenntnisse und Erfahrungen vor.

Für eine substanzielle IPv6-Einführung sind umfangreiche konzeptionelle Vorarbeiten nötig (Adressraum-Planung, Routingprotokolle, DNS/DHCP-Service, Netzadministration, Security etc.). Zeitgleich mit diesen Vorarbeiten soll die native IPv6-Teilnahme am DFN-IPv6 und das Routing von IPv6 auf den Core/Midrange-Routern realisiert werden. Ein IPv6-Routing in Endnetze soll nur nach Absprache und Anforderung erfolgen. Auch aus Sicherheitsgründen darf IPv6 nicht sofort überall eingeschaltet werden, da viele Firewalls (netzwerk- als auch endsystemseitig) noch nicht IPv6-fähig sind.

1.6.4.5 Netztechnologien und Netzzugangstechnologien

1.6.4.5.1 Netztechnologien

Als Technologie zur Verbindung der reinen Netzkomponenten untereinander kommt nahezu ausschließlich Ethernet-Technologie zum Einsatz. Innerhalb des Core-Bereichs der WWU wird derzeit ausschließlich 10GE-Technik eingesetzt. Es ist beabsichtigt mittelfristig (abhängig von der Verfügbarkeit) eine Hochrüstung auf 40GE-Technik vorzunehmen. Falls erforderlich kann hier auch zunächst eine Aggregierung von 10GE-Verbindungen vorgenommen werden. Bei den Verbindungen vom Core- zum Midrange-Bereich wird auch überwiegend 10GE-Technik eingesetzt. In einigen Fällen wird eine Link-Aggregierung von mehreren Gigabit-Verbindungen zu einem sog. Port-Channel durchgeführt. Auch hier ist eine Migration zur 40GE-Technik beabsichtigt. Wie bereits erwähnt ist die konsequente Einführung eines mit 10GE-Technologie angebundenen Distribution-Bereichs eine noch in großem Umfang zu realisierende Aufgabe. Bei den Downlink-Verbindungen vom Distribution-Bereich zum Edge-Bereich handelt es sich je nach Konstellation (Portdichte, Performance-Anforderungen) um 1GE, aggregierte 1GE oder 10GE-Verbindungen.

DSL-Technik kommt zum Einsatz, um in Einzelfällen einfach und flexibel das vorhandene Kupferkabelnetz nutzen zu können, solange noch keine LWL-Anbindungsmöglichkeit existiert. So wird die Anbindung abgelegener Standorte in Einzelfällen mit DSL-Technik realisiert.

Einige Standorte werden auch mit Site-to-Site-VPN-Technologie angebunden. Auch einige kooperierende Einrichtungen werden häufig (insb. im Bereich des UKM) mit Site-to-Site-VPN-Technologie angebunden.

1.6.4.5.2 Netzzugangstechnologien

Für den Zugang von Endgeräten zum Kommunikationssystem wird eine Reihe von Zugangstechnologien unterstützt:

- LAN-Festanschlüsse für registrierte Endsysteme
- "öffentliche" LAN-Festanschlüsse mit VPN-Zugangsmöglichkeit (Cisco/IPsec-VPN und PPTP) für nicht registrierte Endsysteme (s.g. *pLANet*-Anschlüsse: persönlicher LAN-Netzzugang)

- VPN-Zugang aus externen Netzen
- dedizierter VPN-Zugang in eine bestimmte Netzzone (VLAN)
- WLAN (vgl. separaten Abschnitt 1.6.4.6 *„WLAN“*)
- DSL/PPPoE

Der Netzzugang mit 802.1X an LAN-Festanschlüssen ist noch nicht in nennenswertem Umfang realisiert. Es ist geplant 802.1X systematisch als Netzzugangstechnologie für Festanschlüsse zu etablieren. Der Nutzer soll sich dabei flexibel in eine bestimmte Netzzone (VLAN) "einwählen" können. Für eine flächendeckende Einführung dieser Technologie muss ein erheblicher Teil der eingesetzten Switches ausgetauscht werden. Im WLAN ist der Zugang mit 802.1X bereits flächendeckend eingeführt.

Im Bereich des VPN-Zugangs soll zukünftig in Konstellationen, in denen die Installation einer VPN-Client-Software nicht akzeptabel ist, eine einfachere SSL-VPN-basierte Zugangsmethode implementiert werden.

Auch für Gäste existieren Netzzugangsmöglichkeiten. Im Bereich WLAN ist der Netzzugang mit eduroam (bzw. DFN-Roaming) möglich. Im Bereich der Teleport/DSL-Zugänge in den Wohnheimen des Studentenwerks Münster ist eine Zugangsmöglichkeit sowohl für Studierende der WWU als auch für Studierende der Fachhochschule Münster realisiert.

1.6.4.6 WLAN

Derzeit sind zwei verschiedene für den Nutzer transparente WLAN-Installationen im Einsatz. Bei der ersten WLAN-Installation im Netz von WWU und UKM handelt es sich um eine Lösung der Firma Proxim mit autonomen Access Points. Diese Installation ist immer noch in großem Umfang mit ca. 300 APs (Access Points) in Betrieb. Diese Installation soll vollständig durch eine moderne WLAN-Lösung abgelöst werden. In Teilen ist dieses auch schon geschehen. Die ursprüngliche Installation umfasste weit über 400 Access Points.

Seit 2008 ist auch eine zentrale controller-basierte WLAN-Switching-Lösung der Firma Cisco mit ca. 450 APs im Einsatz. Dabei werden 802.11n-fähige APs erst seit kurzem und damit in sehr geringem Umfang eingesetzt. Die zentralen Cisco C6509-Switches für die WLAN-Versorgung sind wie bereits zuvor angesprochen Bestandteil des Core-Netzbereichs.

Als Authentifizierungsverfahren für den Zugang zum WLAN kommt 802.1X zu Einsatz. Für die Verschlüsselung werden WPA und WPA2 eingesetzt.

Die WLAN-Versorgung soll noch wesentlich ausgebaut werden. Eine Umfrage unter den Nutzern im 2. Quartal 2009 hat gezeigt, dass das WLAN eines der am stärksten nachgefragten Angebote des ZIV ist. Es ist langfristig geplant, eine WLAN-Vollversorgung mit 802.11n zumindest für Datenkommunikation zu realisieren. In einigen Bereichen soll die WLAN-Abdeckung auch für VoIP over WLAN und evtl. (insbesondere im UKM) für Location und Tracking ausgelegt werden. Aus Kostengründen soll von der bisherigen 1:1-Redundanz bei den zentralen WLAN-Switches (vgl. Abb. 7) auf eine 2:1-Redundanz umgestellt werden.

1.6.4.7 Erschließung von Studierendenwohnheimen

Die ca. 20 Studierendenwohnheime in Münster sind an das Glasfasernetz der WWU angeschlossen. Aus den Studierendenwohnheimen erfolgt ein authentifizierter Netzzugang in das WNM (und damit

in das Netz der WWU). In den einzelnen Wohnheimen findet man je nach Träger eine unterschiedliche Netzinfrastruktur vor. Liegt eine LAN-Verkabelung vor, so erfolgt der Zugang mittels VPN-Technologie (PPTP). Bei einer DSL-Infrastruktur wird der Zugang mit PPPoE realisiert.

Bei den ca. 15 vom Studentenwerk Münster betriebenen Wohnheimen ist eine von der T-Systems betriebene DSL-Versorgung vorhanden. In Zusammenarbeit mit dem ZIV im sog. *Teleport-Projekt* ist hier ein Zugang zum WNM realisiert. Das ZIV betreibt dabei die für die Aggregierung und Authentifizierung der DSL-Nutzer notwendigen Router. Zwischen dem Teleport-Netz der T-Systems und dem Netz der WWU existiert eine redundante LWL-Verbindung.

1.6.4.8 Eingesetzte Netzkomponenten

Im Inter-Core-, Core- und Midrange-Bereich werden ausschließlich Geräte vom Typ Cisco Catalyst C6509 eingesetzt. Die Realisierung des Distribution-Bereichs mit HP 5412zl-Geräten ist noch weitgehend umzusetzen. Insgesamt werden folgende Gerätetypen in den angegebenen Einsatzbereichen entweder in hoher Anzahl oder für wichtige Funktionen eingesetzt:

Typ	Einsatzbereich
Cisco C6509	Inter-Core, Core, Midrange, WLAN-Switching, Firewall-Funktionalität, VPN
Cisco SPA-IPSEC-2G Modul für C65xx	IPsec-VPN
Cisco Firewall Services Module für C65xx	Firewall-Funktionalität
Cisco Wireless Controller WS-SVC-WISM-1-K9	Modul für C65xx WLAN-Switching
McAfee IntruShield 4010	Intrusion Prevention
HP 5412zl	Distribution-Bereich, Server-Standorte
Cisco 7206VXR	Aggregierung von DSL/PPPoE-Nutzern in Wohnheimen, PPTP-VPN, IPv6
Cisco 876 Router	Remote Standorte (DSL, VPN)
HP 5406zl	Edge-Bereich
HP 2510B-24	Edge-Bereich
HP 2810-48G	Edge-Bereich
HP 4108GL	Edge-Bereich
HP 4208vl	Edge-Bereich
3Com Switch 5500G	Edge-Bereich
3Com Switch 3870	Edge-Bereich
3Com Switch 3300	Edge-Bereich
diverse Nexans Einbau-Switches	Edge-Bereich: Einbau in Kabelkanal
diverse Avaya Cajun P33x	Edge-Bereich
diverse Avaya Cajun P13x	Edge-Bereich
Cisco AIR-LAP1131AG-E-K9	WLAN-Access Point
Proxim AP-4000	"alter" WLAN-Access Point

Tabelle 9: Im Netz von WWU und UKM eingesetzte Gerätetypen

1.6.4.9 Data Center

Derzeit existieren an der WWU zwei zentrale Server-Standorte. Ein dritter Standort ist in Planung. Im UKM gibt es zwei zentrale Server-Standorte. Spezielle Data Center Switches werden noch nicht eingesetzt. Derzeit erfolgt die Anbindung von Servern oft über Distribution-Switches.

Die Planung sieht vor, zukünftig Data Center-Switches auf Layer3 an den Distribution-Bereich anzubinden. Die Aufteilung der Funktionen auf die Data Center soll so erfolgen, dass das IP-Routing zu den Data Centern möglichst lokal auf den Midrange-Switches (d.h. ohne Belastung der Core-Switches) erfolgt. Die Abb. 13 soll die Planungen am Beispiel von 3 Data Centern der WWU verdeutlichen. Die drei Data Center werden wie dargestellt jeweils doppelt physikalisch an die Midrange-Switches angebunden. Die Beschreibung des Redundanzkonzepts im folgenden Absatz bezieht sich immer auf ein ganzes Data Center. Die Betrachtungen gelten aber auch uneingeschränkt für den Fall, dass Teilfunktionen eines Data Centers netzseitig redundant ausgelegt werden sollen.

Einem Paar von Midrange-Switches wird ein Data Center für die redundante Layer3-Anindung zugeordnet. Zum Beispiel sind die beiden Midrange-Switches MS1 und MS2 dem Data Center DC1 zugeordnet. Jedem Data Center ist ein Backup-Data Center zugeordnet. Beispielsweise ist dem Data Center DC1 das Backup-Data Center DC2 zugeordnet. IP-Instanzen (VRs) auf den beiden Midrange-Switches werden über ein Transfer-IP-Subnetz mit einer IP-Instanz auf dem zugeordneten Data Center und auf dem Backup-Data Center verbunden. In der Konfiguration der Data Center wird dafür gesorgt, dass die Konnektivität vom Backup-Data Center zum Data Center gegeben ist. Über eine IP-Instanz des Backup-Data Centers (DC2) sind dann sämtliche IP-Subnetze des zugeordneten Data Centers (DC1) erreichbar. Bei Totalausfall eines Data Center sind dann sämtliche betroffenen IP-Subnetze über das Backup-Data Center erreichbar.

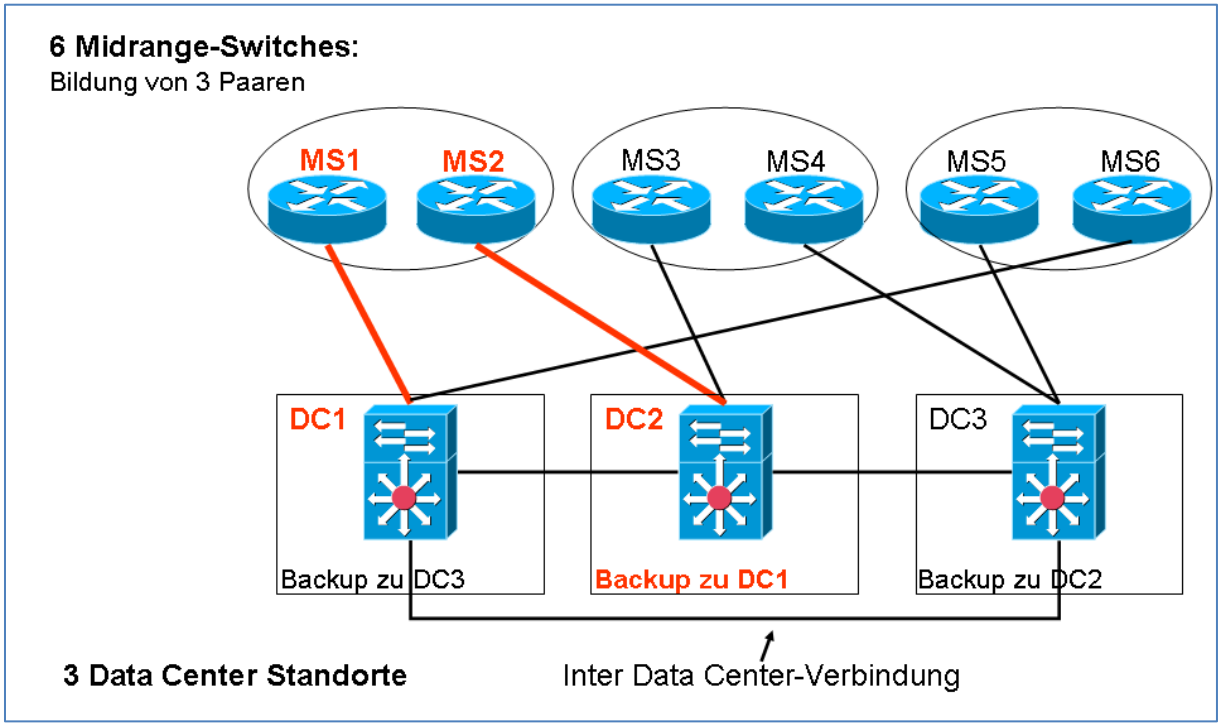


Abb. 13: Geplante Anbindung von Data Centern

1.6.4.10 Veranstaltungs-Netze

Es ist geplant für die Versorgung von festen und variablen Veranstaltungsorten ein logisches Veranstaltungsnetz zur Erreichung aller möglichen Standorte zu realisieren. Für die Veranstaltungsunterstützung ist geplant, auf Dauer folgende Funktionen/Dienste zu realisieren: Peer-to-Peer-Livestream, Video on Demand, Veranstaltungsaufzeichnung, Video-Conferencing, Rundfunksendungen (LAN-TV). Die hierfür erforderlichen Geräte sind allesamt noch zu beschaffen: Geräte für die Netzeinspeisung, Encoder, Decoder, Management-Station.

1.6.5 Konzept der netzseitigen IT-Sicherheitsmaßnahmen

1.6.5.1 Netzseitige Maßnahmen zur IV-Sicherheit

Das ZIV führt im Auftrag der WWU und des UKM und in Abstimmung mit den Verantwortlichen in den IV-Versorgungsbereichen netzseitige Maßnahmen durch, die die Gefährdung der Informationsverarbeitung, ihrer Verarbeitungsprozesse, IT-Systeme und Daten verringern und damit die direkten und indirekten Aufwendungen für eingetretene Schäden reduzieren sollen. Konzeptionell sind diese Maßnahmen selbstverständlich nur ein Teil der Gesamtmaßnahmen – Maßnahmen auf den IT-Endgeräten selbst, organisatorischen Maßnahmen, Ausbildungsmaßnahmen etc. wird in der Gesamtheit ein noch größeres Gewicht zugeordnet. Netzseitige Maßnahmen erlauben jedoch in wichtigen Fällen und gezielt für wichtige Bereiche das Gefährdungspotential auch dann zu begrenzen, wenn lokale, organisatorische und sonstige Maßnahmen nicht ausreichend umgesetzt werden konnten. In bestimmten Fällen können auch nur netzseitige Maßnahmen Schutz bieten, z.B. zur Abwehr bestimmter Denial-of- Service-Angriffe.

1.6.5.2 Grundstrukturen für netzseitige Sicherheitsmaßnahmen

Grundgedanke des Systems der netzseitigen Sicherheitsmaßnahmen ist die Einbettung von Sicherheitsfunktionen in ein strukturiertes Netz. Grundelemente sind hierbei

- ein strukturiertes Netz mit *Netzzonen*, die den Kommunikations- und Sicherheitsbedürfnissen der Teilnehmersysteme mit ihren Anwendungen und Daten entsprechen (vgl. Abb. 14). Diese Strukturierung ist mitunter ein wechselseitiger Prozess: Zur Optimierung der Sicherheit bei gleichzeitig möglichst geringer Beschränkung der erforderlichen Kommunikationsmöglichkeiten muss zum einen
    - Einfluss auf die Verteilung der Anwendungen und Daten auf IT-Systeme (Server, Proxies, Clients) genommen werden und zum anderen muss
    - eine Verteilung der IT-Systeme auf geeignet zu definierende Netzzonen (Subnetze, VLANs, etc.), denen zonenspezifische Sicherheitsfunktionen (z.B. Paketfilter, Firewalls) zugeordnet sind, durchgeführt werden. Gesamtheiten von Netzzonen können so entsprechend den Bedürfnissen ganzheitlich gegenüber anderen übergeordneten Netzzonen sicherheitstechnisch definiert und betrieben werden. Eine solche Strukturierung entspricht den vorhandenen IV-Strukturen, die häufig auch vielstufig ausgeprägt sind (vgl. Abb. 15).
- die Einbettung von Sicherheitsfunktionen in das Netz: „Die Firewall“ im Sinne eines „Border Defense Gateway am Netz-Perimeter“ ist für größere Netze als alleinige netzseitige Maßnahmen unzureichend. Vielmehr sind alle netzseitigen Sicherheitsmaßnahmen möglichst überall dort im Netz, wo eine sicherheitstechnische Abgrenzung eines informationsverarbeitenden Bereiches gegenüber anderen Bereichen erwünscht scheint, zu integrieren. Damit werden Verbände von Netzzonen aufgebaut, die nicht nur nach außen

geschützt sind, sondern in denen auch für überschaubare Bereiche innerhalb eines Zonenverbundes gleichermaßen Sicherheitsfunktionen bereitstellt werden können.

Unter Maßgabe der technischen Möglichkeiten und der verfügbaren finanziellen und personellen Ressourcen wurde eine optimierte Struktur aus Netzzonen mit Sicherheitsfunktionen an Übergängen aufgebaut.

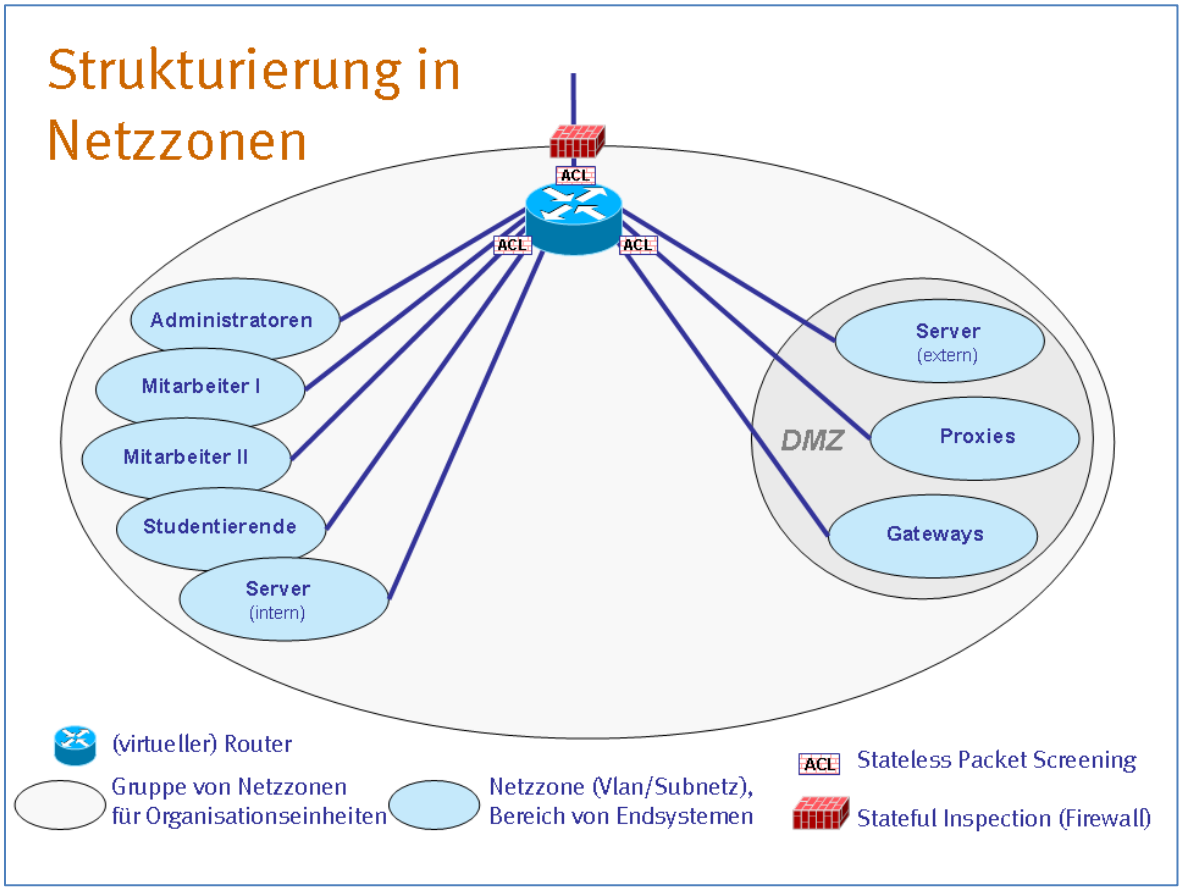


Abb. 14: Konzeptdarstellung: Strukturierung in Netzzonen

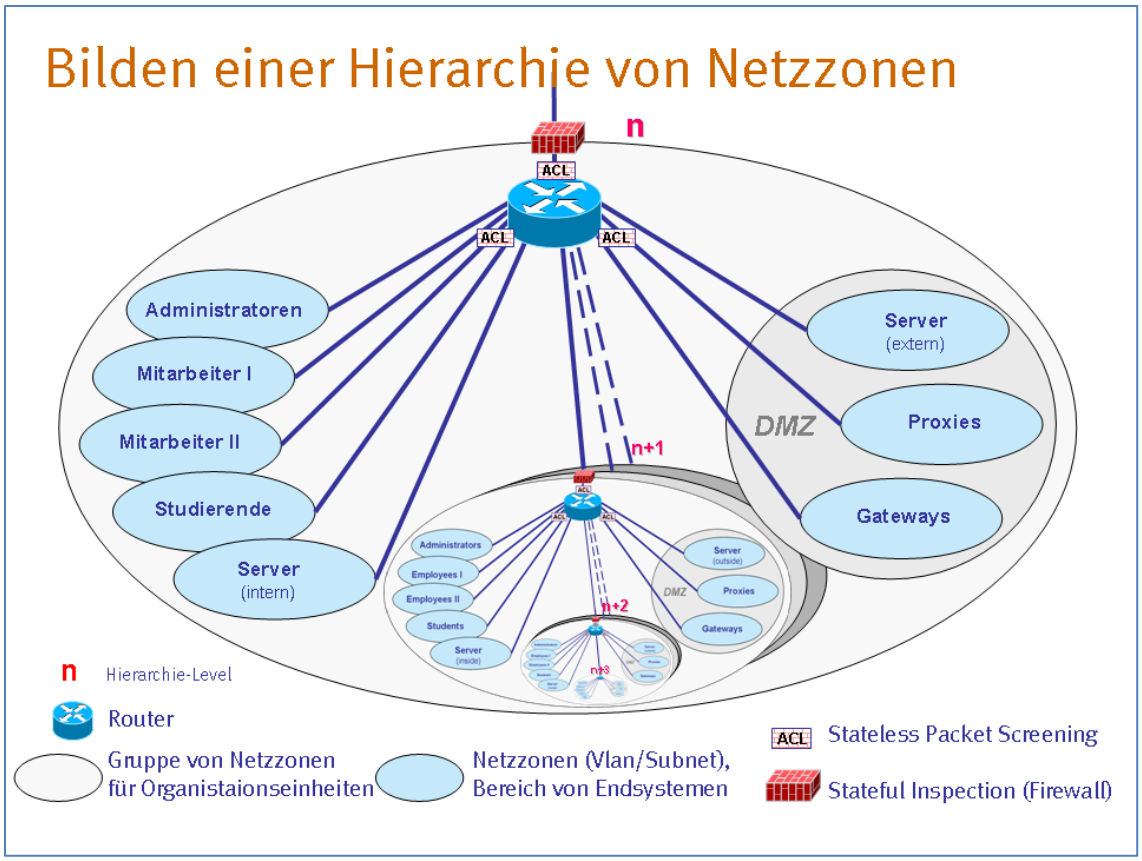


Abb. 15: Konzeptdarstellung: Hierarchie von Netzzonen

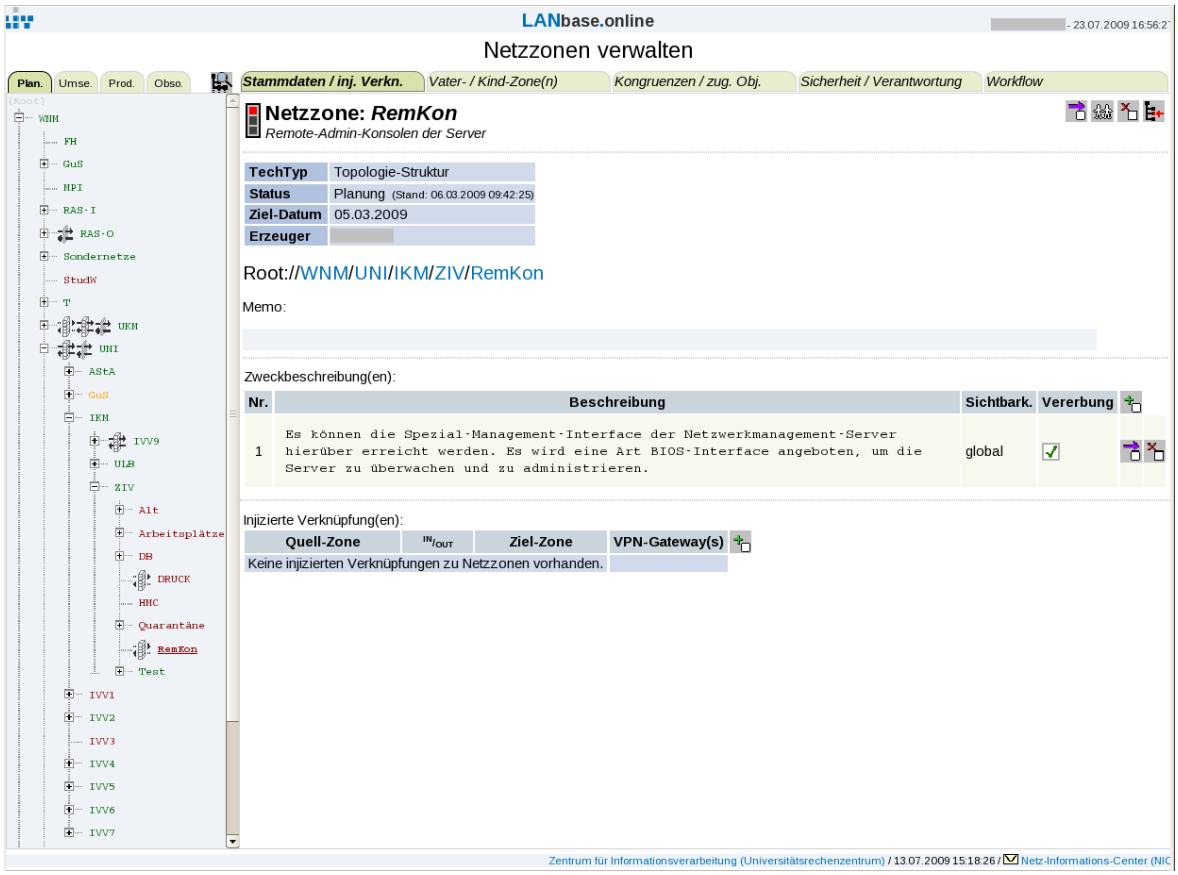


Abb. 16: Screenshot des Administrationswerkzeugs für Netzzonen („Netzzonenbrowser“)

1.6.5.3 Sicherheitsfunktionen im Netz

Netzseitig werden folgende Sicherheitsfunktionen eingesetzt:

- Stateless Packet Screening, insbesondere auf den Layer-3-Switches (Routern), kontrolliert die Konnektivität im Wesentlichen auf der Basis von Kommunikationsquellen und –zielen (IP-Adressen und logische Interfaces von Routern) sowie bestimmter höherer Protokollmerkmale (Anwendungsprotokolltypen, d.h. z.B. TCP-/UDP-Ports, und einige weitere Protokollelemente). Diese Methode bietet sich kostengünstig und hoch performant überall dort an, wo die mit Zugangskontrolllisten in Routern (ACLs, Access Control Lists) erreichbare Grundsicherheit ausreichend ist oder wo hoher Durchsatz als vorrangig betrachtet werden muss. Hier kann in Zusammenhang mit besonderen Netzzonen, in denen Applikation Gateways mit Sicherheitsfunktionen (Application Proxies, auch Terminal Server, Web- und FTP-Server mit Sicherheitsfunktionen, etc.) installiert werden, bereits eine sehr hohe Sicherheit erreicht werden, ohne dass besondere Kosten anfallen würden, da moderne Router meistens dazu geeignet sind und ohnehin Bestandteil der Netze sind. Ein Einsatz solcher Funktionen ist technisch praktisch immer möglich, erfordert allerdings auch einen Verwaltungsaufwand, der nicht zu unterschätzen ist.
- Firewalls im Sinne eines Stateful Packet Screening unter Berücksichtigung port-agiler Protokolle (wie z.B. FTP, SIP, H.323) sind sicherheitstechnisch den Routern deutlich überlegen, da die Blockierung unerwünschter Konnektivität sitzungsbezogen (Flow basiert) erfolgen kann. Auch sind die Möglichkeiten des Reportings wesentlich umfangreicher und detaillierter. Hier kann wie bei den Stateless Packet-Filtern eine noch weitergehende Sicherheitsqualität im Zusammenhang mit besonderen Netzzonen für Applikations-Gateways (quasi DMZs, „Demilitarisierte Zonen“) erreicht werden. Nachteil solcher Firewalls sind die vergleichsweise geringen Durchsatzmöglichkeiten, die weit hinter den Möglichkeiten von Routern zurückbleiben. Deshalb können solche Systeme nur dann eingesetzt werden, wenn die Durchsatzbeschränkungen unkritisch sind oder wenn die Erhöhung der Sicherheit gegenüber den ACL-basierten Funktionen Vorrang hat vor der Performance. Gleichzeitig muss der Kostenaufwand betrachtet werden; leistungsfähige Firewalls beruhen stets auf spezieller und damit vergleichsweise teurer Hardware und Software. Dies gilt insbesondere für monolithische Firewall-Systeme, die gleichzeitig auch Applikation Gateways und zum Teil auch VPN- und Intrusion-Prevention-Funktionen (s.u.) integrieren.
- Intrusion-Detection- und -Prevention-Systeme (IPS) analysieren Datenströme und können Dateneinheiten oder Flows aufgrund bestimmter maliziöser Datenmuster (Signaturen), Verhaltensanomalien oder Kombinationen beider Merkmale automatisch erkennen und blockieren. Damit können Angriffe für ganze Infrastrukturbereiche abgewehrt werden. So genannte Zero-Day-Attacken, also bisher unbekannte Angriffstypen, können oft erkannt und abgewehrt werden. Auch können Denial-of-Service(DoS)-Angriffe, die von den betroffenen Systemen kaum selbst beherrscht werden können, abgewehrt werden.
- Sicherer Zugang zu Netzzonen durch verschlüsselte Tunnel mit Hilfe der VPN-Technologie ermöglicht den kontrollierten Zugang (authentifiziert, unter Autorisierungsüberwachung) zu Ressourcen auch in geschützten Bereichen.
- Application Gateways oder Application Proxies können auf der Ebene von Anwendungsprotokollen und unter Berücksichtigung der Inhalte für besondere Sicherheitsfunktionalitäten sorgen (z.B. Mail-Relays bzw. SMTP-Gateways mit Virenschutzfunktionen oder entsprechende Systeme für HTTP, d.h. Web- Proxies, und FTP

etc; auch Terminal Server können hier eine ausgezeichnete Funktion als Übergangsmöglichkeit in fremde Netzbereiche einnehmen). Hier muss im Einzelfall entschieden werden, ob eine spezielle Funktionalität durch die Verantwortlichen bereit zu stellen ist, die auch sonst für den Bereich der IV-Anwendungen verantwortlich sind (z.B. Systemadministratoren) oder ob eine spezielle Funktionalität im Sinne eigentlicher netzseitiger Sicherheitsmaßnahmen betrachtet werden kann. Netzseitig ist hier jedoch in jedem Fall für die Abstimmung und entsprechende Bereitstellung von Netzzonen („DMZ“) zu sorgen.

- Bypassing erlaubt überall in der Sicherheitsarchitektur den Einsatz der genannten Sicherheitsfunktionen, auch wenn Anwendungen mit externen oder zentralen Servern hohen Durchsatz erfordern. Beim Bypassing wird mittels Policy Based Routing bestimmter Datenverkehr an den durchsatzbeschränkenden Sicherheitsfunktionen vorbei gelenkt.

1.6.5.4 Virtualisierung als Voraussetzung

Eine bedarfsweise Einbettung der genannten Sicherheitsfunktionen in ein unter Sicherheitsgesichtspunkten strukturiertes Netz unterliegt stets drei wichtigen Gesichtspunkten, die mitunter untrennbar miteinander verbunden sind:

- der technologischen Machbarkeit,
- der Finanzierbarkeit und
- der Administrierbarkeit.

Die technologische Machbarkeit und die Finanzierbarkeit würden sehr schnell an ihre Grenzen stoßen, wenn Netzstrukturen und funktionale Instanzen 1:1 physisch bzw. physikalisch auf das Netzinventar abgebildet werden müssten. Eine hierarchische Netzstruktur mit einer Vielzahl den einzelnen Netzzonen zugeordneten Geräten (Switches, Routern, Firewalls, IPS etc.) ist kaum vorstellbar. Selbst Kabelwege müssten in solchen Szenarien im schlimmsten Fall gesondert für die einzelnen Netzzonen errichtet werden. Die Administration einer Vielzahl von Firewalls in einem solchen Netz, das auch noch anforderungsgerecht betrieben werden soll, ist für Netzverantwortliche ein Schreckensszenario.

Als Weg aus diesem Dilemma wurde eine weitgehende Virtualisierung von Funktionalitäten realisiert (vgl. Abb. 17):

- Durch Virtuelle LANs (VLANs), eine bewährte Layer-2-Netztechnologie, können Netzzonen gebildet werden, ohne dass dabei jedes Mal Kabelwege speziell geschaffen werden müssten. Die Zusammenfassung von Arbeitsplätzen in einer gemeinsamen Netzzone gelingt so auch über größere Entfernungen hinweg, gebäudeübergreifend und weitgehend beliebig für jeden einzelnen Arbeitsplatz.
- Durch Virtualisierung von IP-Routern können flexibel auch relativ komplexe Netztopologien aufgebaut werden, die den jeweiligen sicherheitstechnischen Strukturierungsanforderungen entsprechen, ohne dass gleich bei neuen Zonenstrukturen neue (physische) Router beschafft werden müssten. Vielmehr kann heute ein einzelner physischer Switch ohne besondere weitere Kosten in mehrere „virtuelle Router“ aufgeteilt werden. Im Zusammenhang mit der VLAN-Technologie kann im Grundsatz so jede beliebige IP-Topologie mit den gewünschten hierarchischen Sicherheitszonen aufgebaut werden (vgl. auch Abb. 12 auf Seite 27). Ein Seiteneffekt dieses Ansatzes ist neben der Kostenersparnis, insbesondere durch bessere

Ausnutzung von Geräten, eine Konzentration auf weniger Geräte und damit verbesserte Möglichkeiten der Betriebsführung.

- Durch die Virtualisierung von Firewalls und der Virtualisierung von Intrusion-Prevention-Systemen kann eine größere Zahl an Instanzen solcher Sicherheitselemente auf der Basis einer geringen Anzahl leistungsfähiger Geräte an beliebiger Stelle in das Netz „eingebettet“ werden.
- VPN-Technologie (in engerem Sinne) erlaubt seit langem die Ausdehnung einer Netzzone (meistens als „Intranet“ deklariert) über so genannte Tunnel auf externe Netze (Sites) oder Arbeitsplätze (Clients). Die eingesetzten VPN-Systeme unterstützen VLANs unter spezieller Berücksichtigung des IP-Routings, so dass virtuelle multiple VPN-Zugangsmöglichkeiten für VPN-Clients und -Sites im Rahmen des vorgestellten Zonenkonzeptes bestehen.

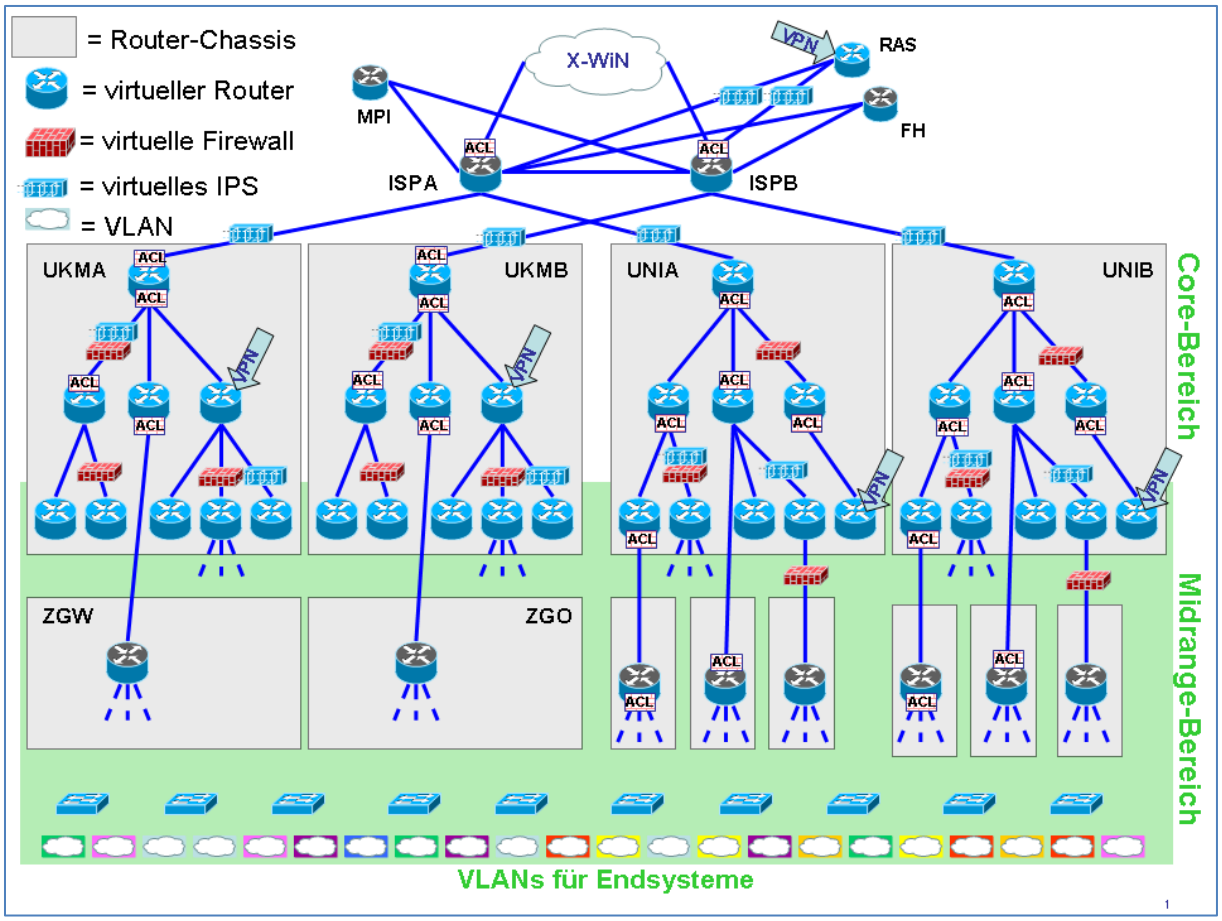


Abb. 17: Virtualisierung: VLANs, virtuelle IP-Router, virtuelle Firewall-Instanzen, virtuelle Intrusion Prevention Systeme, VPN-Einwahl in ein VLAN. Die physikalischen Verbindungen zwischen den Chassis sind hier nicht dargestellt.

1.6.5.5 Zentrale und dezentrale Administrationsfähigkeit

In dem vorgestellten Konzept wird die Rolle mehr und weniger zentraler und dezentraler IV-Strukturen abgebildet, wobei das Netz als einheitliche Infrastruktur für alle durch das ZIV bereit gestellt wird und in dieser Form Grundvoraussetzung für die korrekte Funktion des Netzzonenkonzeptes ist. Netzseitig eingebettete Sicherheitsfunktionen sind unter diesem Gesichtspunkt zunächst kritisch zu betrachten,

- da netzseitig und damit zentral Funktionen bereitgestellt werden, die in engstem Zusammenhang mit den spezifischen Regelungen der dezentralen IV bis hin zu kleinsten Teilbereichen zu sehen sind.
- Andererseits können in das Netz eingebettete Sicherheitsfunktionen so massiv in die Ende-zu-Ende-Kommunikation eingreifen, dass die Netzbetriebsführung als zentrale Aufgabe mit flächendeckendem Charakter illusorisch würde, wenn eine uneingeschränkte dezentrale Administration der eingebetteten Sicherheitsfunktionen ermöglicht würde.

Für die Lösung dieser Problemstellung sind folgende Funktionalitäten erforderlich:

- Mandantenfähigkeit erlaubt Einsicht bzw. selbstständige Konfiguration der Sicherheitsfunktionen und des spezifischen Reporting für die zugeordneten virtuellen Ressourcen durch die jeweiligen Netzzonenverantwortlichen.
- Rahmenkonfigurationsmöglichkeiten und andere Generalfunktionen für die Netzverantwortlichen erlauben dagegen die Vorgabe von Muster-, Standard- und Mindestkonfigurationen zur Unterstützung der Netzzonenverantwortlichen und die Gewährleistung der Netzmindestfunktionalitäten sowie eine allgemeine Reporting- und Eingriffsmöglichkeit.

Beim eingesetzten IPS-Produkt sind diese Funktionalitäten gegeben. Für die besprochenen Netzbasisfunktionen Virtuelle LANs, Virtuelle Router mit den Stateless-Packet-Screening-Funktionen und Virtuelle Firewalls ist die Mandantenfähigkeit als Funktionalität der eingesetzten Produkte nicht verfügbar. Hier muss die Self-Care-Funktionalität der Netzdatenbank (LANbase) des ZIV im Rahmen einer Netzzonenverwaltung ausgebaut und mit Geräte-Steuerungsmechanismen verbunden werden. Für die Administration der VPN-Zugangsmöglichkeiten (Clients und Sites) wurde bereits die Möglichkeit, VPN-Zugangsmöglichkeiten nutzerseitig zu aktivieren oder zu deaktivieren implementiert. Eine Anbindung an das z.Zt. vorhandene Identitätsmanagement (Nutzerdatenbank) für personenbezogene Authentifizierung und Autorisierung beim netzzonenspezifischen VPN-Zugang ist ebenso realisiert.

1.6.5.6 Planungen bei den netzseitigen IT-Sicherheitsmaßnahmen

Die Umsetzung des Netzzonenkonzeptes ist ein aufwendiger, kontinuierlicher Prozess, der nur in enger Zusammenarbeiten mit den einzelnen Einrichtungen von WWU und UKM durchgeführt werden kann. Die in einer Einrichtung betriebenen Endsysteme müssen bzgl. der Sicherheitsanforderungen charakterisiert werden und anschließend einzelnen zu definierenden Netzzonen zugeordnet werden.

Bei den installierten Sicherheitsfunktionen muss durchgängig ein Upgrade auf 10GE-Technologie durchgeführt werden. Im Bereich des Intrusion Prevention Systems ist hier ein Upgrade dringend erforderlich. Als zusätzliche Sicherheitsfunktionalität soll noch eine Content-Filtering/Web-Proxy-Lösung implementiert werden. In diesem Zusammenhang wurde kürzlich ein kleines System beschafft, um in diesem Bereich erste Erfahrungen sammeln zu können. Wie bereits angesprochen, soll der authentifizierte Netzzugang mittels 802.1X großflächig zum Einsatz kommen. Im Bereich der Statusüberwachung von Endsystemen (Policy Enforcement, NAC: Network Admission Control) gibt es derzeit noch keinerlei realisiert Funktionalität. Es ist beabsichtigt, auch diese Funktionalität zukünftig zu implementieren.

1.6.6 "Herstellerpolitik"

Da die beantragten Komponenten kontinuierlich in Betrieb genommen werden (vgl. Abschnitt 2 *„Netzentwicklungsplan“*) und nicht im Rahmen einer einzelnen großen Umstellungsmaßnahme, soll die Beschaffung über Rahmenverträge durchgeführt werden, die periodisch neu ausgeschrieben werden. Dabei soll gegebenenfalls auch auf Rahmenausschreibungen der DFG zurückgegriffen werden, wenn dies wirtschaftlich sinnvoll und von den Gerätetypen passend ist. So wird sichergestellt, dass die technologische Weiterentwicklung und die Preisentwicklung während des gesamten Umsetzungszeitraums mitberücksichtigt werden kann.

1.6.6.1 LAN-Technologie

Grundsätzlich wird eine möglichst geringe Typenvielfalt bei den eingesetzten Geräten angestrebt. Für Spezialfunktionen lässt sich dieses Ziel nicht immer erreichen. Bedingt durch die hohen Verweilzeiten vieler Gerätetypen innerhalb des Rechnernetzes und den deutlich kürzen Verkaufszeiträumen dieser Geräte kommt es trotzdem zu einem Parallelbetrieb mehrerer Gerätetypen und –generationen im gleichen Einsatzgebiet. Um die Heterogenität innerhalb des Netzes nicht noch weiter zu steigern, ist es deswegen notwendig, sich langfristig auf wenige Hersteller festzulegen. Im ZIV ist aus diesen Gründen die Entscheidung gefallen, sich auf im Wesentlichen auf 4 Hersteller zu beschränken:

- Cisco im Core und Midrange-Bereich: L2-Switching und L3-Routing, WLAN-Switching, Firewall-Funktionalität (Stateful Packet Screening), VPN-Funktionalität
- HP ProcCurve im Edge-/Distribution-Bereich: L2-Switches, Verteilerbereiche (19“), Distributionsebene
- 3Com/H3C im Edge-Bereich: L2-Switches, Verteilerbereiche (19“)
- Nexans im Edge-Bereich: L2-Switches im Installationsbereich (Kabelkanaleinbau im Office)

Dabei besaßen folgende Hersteller in ihren Kerneinsatzgebieten im ZIV zum Beschaffungszeitpunkt ein Alleinstellungsmerkmal:

- Nexans: besondere Bauform und gleichzeitig Managebarkeit
- Cisco: virtuelles IP-Routing (IOS-Feature VRF-lite)

Bei den Geräten, die in hohen Stückzahlen zum Einsatz kommen, wird möglichst durch die Realisierung eines Rahmenvertrags versucht, den erforderlichen kontinuierlichen Beschaffungsprozess gewährleisten.

In der Vergangenheit hat sich herausgestellt, dass durch die Wettbewerbssituation zwischen Vertriebs- und Supportpartnern eines Herstellers am Markt allein wenig Einfluss auf die Preisbildung und Supportqualität des Herstellers genommen werden kann. Erst die Wettbewerbssituation zwischen Herstellern führte zu einer deutlichen Verbesserung der Situation. Dieses hat sich gerade in dem Segment der Edge-Devices, das von hohen Stückzahlen und einem breiten Herstellerspektrum gekennzeichnet ist, verdeutlicht. Es stehen ca. alle 3-4 Jahre neue Gerätegenerationen und damit verbunden Geräte- und Herstellerentscheidungen an. Im Edge-Bereich soll daher tendenziell weiterhin eine 2-Herstellerstrategie zum Einsatz kommen.

1.6.6.2 TK-Technologie

Bereits frühzeitig wurde der Telekommunikationsanlagenverbund am Standort Münster um die VoIP Technologie (Hybridansatz), unter der strikten Priorisierung der verabschiedeten SIP-Standards der IETF, erweitert, was ein hohes Maß an Investitionssicherheit gewährleistet. Der

Telekommunikationsanlagenverbund besteht aus Systemen des Hersteller NEC. Alle wichtigen Leistungsmerkmale, bis hin zu komplexen Chef-Sekretär Lösungen, können sowohl in der traditionellen Welt als auch in der VoIP-Welt und in einer gemischten Umgebung realisiert werden.

Durch die strikte Umsetzung des SIP-Standards seitens der Systeme können prinzipiell alle SIP-tauglichen Endgeräte unterstützt werden, was einen hohen Freiheitsgrad bei der Beschaffung und der Marktbeobachtung bedeutet. Aus Gründen der Logistik, der notwendigen Vorhaltung von Endgeräten, der Unterstützung von Leistungsmerkmalen, die über den SIP Standard hinausgehen, werden jedoch die Endgeräte des Hersteller Polycom priorisiert eingesetzt. Der weitere Ausbau der VoIP-Technologie wird mittelfristig über redundante IP-Serverlösungen, die ebenfalls vollständig in den bestehen Verbund eingebunden werden können, vorangetrieben.

1.6.7 House-Keeping: USV-Versorgung, Klimatisierung

Abgesehen vom Edge-Bereich sind die Netzkomponenten mit redundanten Netzteilen ausgestattet. Beide Netzteile sind möglichst an verschiedene Stromkreise angeschlossen. Die derzeit betriebenen Edge-Geräte besitzen in den allermeisten Fällen keine redundanten Netzteile. Neu beschaffte Netzkomponenten haben (außer in Sonderfällen auch im Edge-Bereich) redundante Netzteile.

Eine Absicherung der Stromversorgung durch eine USV-Anlage wird primär an den Standorten durchgeführt, die eine strukturelle Bedeutung für das Netz haben. Das ist an allen Haupt- und Nebenstandorten der Fall. Im noch im Aufbau befindlichen Distribution-Bereich muss auch die USV-Versorgung noch realisiert werden.

Drei große USV-Anlagen an den beiden Hauptnetzstandorten und einem Serverstandort werden von den Technischen Diensten der WWU betrieben (Wartung, Überwachung). In einigen Fällen erfolgt auch eine Einbindung in die Netzüberwachung (Alarmierung per SNMP). Als Überbrückungszeit sind hier ca. 25 Minuten realisiert. Für diese drei Standorte existiert auch eine Netzersatzanlage (NEA, Dieselpufferung). Darüber hinaus gibt es an einigen Midrange-Standorten eine vom ZIV selbst betriebene USV-Versorgung. Bei diesen nicht von den Technischen Diensten betriebenen "kleineren" USV-Anlagen gibt einen umfassenden Erneuerungsbedarf. Die Standzeit ist oft weit überschritten.

An Standorten, an denen ein Stromausfall nur lokale Auswirkungen hat, ist in der Regel keine USV-Absicherung realisiert. Auch bei einer VoIP-Installation in einem Gebäude ist eine USV-Versorgung nicht in jedem Fall realisiert. In den zur Verfügung stehenden Räumlichkeiten ist die Installation von USV-Geräten oft mit großen Problemen verbunden (Platzprobleme, Klimatisierung). Es ist angestrebt, zumindest den Midrange- und Distribution-Bereich vollständig mit einer USV-Versorgung zu versehen. Darüber hinaus muss im Einzelfall entschieden werden, ob eine USV-Versorgung sinnvoll ist.

Die Versorgung mit Power over Ethernet (PoE) erfolgt für VoIP-Telefone und WLAN-Access-Points.

Alle Telekommunikationsanlagen, sowohl die TK-Units als auch die abgesetzten Anlagenteile (RPMs) sind batteriegepuffert. Die Überbrückungszeiten belaufen sich auf ca. 30 min. An einigen Hauptstandorten können im Störungsfall Netzersatzanlagen (Notstromdiesel) die Stromversorgung, innerhalb der batteriegepufferten Überbrückungszeit, wieder herstellen.

Die obigen Ausführungen zur USV-Versorgung gelten im Grundsatz auch für die Klimatisierung, wobei der Betrieb der Klimaanlagen ausschließlich durch die Technischen Dienste erfolgt. Daher ist in diesem Antrag die Klimatisierung nicht berücksichtig.

1.6.8 Mediennetze, AVM (Audiovisuelle Medien)

1.6.8.1 Schaffung einheitlicher Userinterfaces für die Lehre

Bei der Entwicklung der Standards für die Medientechnik an der WWU Münster wurde bereits zu Anfang darauf geachtet, dass ein einheitliches, von der Verwendung einzelner Komponenten unabhängiges Benutzerinterface geschaffen wurde. Dieses bezieht sich in besonderem Maße auf das grafische Userinterface (GUI) in den größeren Hörsälen. In der Regel dienen frei programmierbare Touch-Panel mit gleichen Bedienoberflächen als Steuerungsgerät der Medientechnik. Somit konnte in kurzer Zeit ein sicherer Umgang mit der neuen Medientechnik bei den Lehrenden erreicht werden. Die Erneuerung der Technik und Geräte, die im Hintergrund für die Versorgung der Räume mit Medientechnik wichtig sind, ist für die Lehrenden zweitrangig, denn das Nutzerinterface bleibt nahezu identisch. Für kleinere Seminarräume wurden eigene Steuerungen entwickelt, unter der Maßgabe, dass auch hier die Benutzung für den Lehrenden nahezu in jedem Raum identisch ist. Diese Standards haben dazu beigetragen, dass die Nutzer, unabhängig davon in welchen Räumen sie Vorlesungen oder Seminare abhalten, sehr schnell mit der vorhandenen Medientechnik und deren Bedienung vertraut sind.

1.6.8.2 Weitere Entwicklung

Es ist zu erkennen, dass der qualitative und quantitative Ausbau von Seminarräumen und Hörsälen in gleicher Weise stattfinden muss. Die Sanierungs- und Neubaumaßnahmen, die innerhalb der Liegenschaften der WWU notwendig sind, lassen nicht von einer Stagnation im Bereich der Erneuerung der medientechnischen Anlagen ausgehen.

Alle installierten medientechnischen Anlagen sind bereits mit LAN Anschlüssen ausgestattet worden. Somit wurde gewährleistet, dass die zukünftige Vernetzung der medientechnischen Anlagen über das LAN möglich ist. Der Ausbau der Seminarräume und Hörsäle mit Multimediatechnik erfordert die gebäudeübergreifende Vernetzung dieser Technik, um zukünftig über zentrale standardisierte Verfahren die Betreuung der Anlagen, die Funktion und Verfügbarkeit der Anlagen gewährleisten zu können.

Darüber hinaus ist die große Anzahl an installierten medientechnischen Anlagen einer regelmäßigen Wartung zu unterziehen. Um diesen Anforderungen gerecht werden, zu können ist ein zentrales Managementsystem aufzusetzen. Neben der in zeitlichen Abständen notwendigen Wartung der Anlagen vor Ort ist es erforderlich, dass die Zustände der medientechnischen Anlagen zentral über das LAN abfragbar sind, bzw. wichtige Informationen wie z.B. Betriebsstunden der Beamerlampen direkt an das übergeordnete zentrale Managementsystem gemeldet werden. Ein weiterer Aspekt ist die Möglichkeit der zentralen zeitlichen Steuerung der medientechnischen Anlagen, um unnötige Standby Zeiten der Anlagen zu vermeiden. Hierdurch werden unnötige Betriebszeiten und Betriebskosten vermieden, was sich unmittelbar auf die Wartungszyklen und die Lebensdauer der Technik auswirkt. Im Zuge der in den vergangenen Jahren umgesetzten medientechnischen Konzepte, ist in einigen Gebäuden die Möglichkeit der Übertragung von Veranstaltungen innerhalb des Gebäudes realisiert worden. Eine Abstützung der Übertragungen aus den einzelnen Hörsälen findet z.Zt. nicht standardmäßig über die LAN Infrastruktur statt. Das zukünftige Konzept für die

Übertragung von Veranstaltungen beinhaltet als Basisinfrastruktur das lokale Netz der WWU. Encoder- und Decoder-Technologie werden hierfür in den einzelnen Gebäuden der WWU bereit zustellen sein.

1.6.9 Core Network Services

Folgende CNSs (Core Network Services) werden vom ZIV zentral für die WWU und das UKM betrieben:

- DNS
- DHCP
- WINS
- RADIUS
- NTP

Die für den Betrieb dieser Services notwendige Verwaltung von z.B. Rechnernamen, IP-Adressen und MAC-Adressen ist mit Hilfe der Netzwerkdatenbank *LANbase* (vgl. Abschnitt 3.6.1 *„Netzdokumentation und -administration mit LANbase“*) vollständig zentralisiert. In LANbase sind u.a. umfassende IPAM-Funktionen (Internet Protocol Address Management) realisiert. Über eine Webschnittstelle (sog. *NIConline*) können die für Endsysteme technisch Verantwortlichen Änderungen weitgehend selbst vornehmen. Die Provisionierung des DNS-, DHCP- und WINS-Services erfolgt aus LANbase heraus. Beim zentralen DNS-Service ist dabei die Anbindung an die für den Betrieb einer Microsoft Active Directory Infrastruktur notwendigen DNS-Funktionen gegeben. Der RADIUS-Service wird aus der zentralen Nutzerdatenbank provisioniert. Die Produktivsysteme aller oben genannten Services werden in einer nicht virtualisierten server-basierten Form betrieben. Das bedeutet, dass keine speziellen Appliances zum Einsatz kommen. Dabei kommen Linux als Betriebssystemplattform und Open Source Software zum Einsatz.

Für die Zukunft ist geplant, die Open Source basierte Realisierung der CNSs beizubehalten, da sie sich in der Vergangenheit als sehr flexibel, insbesondere in Bezug auf Provisionierung, erwiesen hat. Außerdem ist eine langfristige Kalkulierbarkeit der Kosten (insb. für Wartung) ohne volumensabhängige oder funktionsabhängige Lizensierungsbestandteile gegeben. Durch Servervirtualisierung ist auch eine kostengünstige Realisierung von Redundanz-, Test- und Entwicklungssystemen möglich. Die Server für die einzelnen Services sollen dabei doppelt redundant ausgelegt werden (d.h. 3 Server pro Service), da dann selbst bei Ausfall eines Servers kein akuter betrieblicher Handlungsbedarf ausgelöst wird, da immer noch einfache Redundanz gegeben ist. Der personelle Aufwand kann so reduziert werden. Der tertiäre Server für einen Service kann dabei als virtuelle Maschine ausgelegt werden.

Wegen der außerordentlichen betrieblichen Bedeutung der CNSs (insb. DNS) ist geplant, ein umfassendes Monitoring für diese Services zu realisieren. Neben der Überwachung von Verfügbarkeit und Performance soll dabei außerdem die Aktualität und Konsistenz der Daten überwacht und auch eine umfassende Fehleranalyse möglich sein. Außerdem ist geplant, durch den Einsatz von IP-Anycast eine deutliche Verbesserung der Verfügbarkeit des DNS-Service zu erzielen.

Wegen der ebenso zunehmenden betrieblichen Bedeutung des authentifizierten Netzzugangs (u.a. wegen der netzweiten Einführung von 802.1X) soll die RADIUS-Infrastruktur bzgl. Funktionalität und Verfügbarkeit noch deutlich verbessert werden.

1.7 Netzintegration

Eine physikalische Trennung des Kommunikationsnetzes (Daten-, TK- und Mediennetz) in ein Wissenschaftsnetz und ein Verwaltungsnetz o.ä. existiert nicht. Für die gesamte WWU und das UKM existiert ein alle Einrichtungen versorgendes, gemeinsames physikalisches Kommunikationsnetz. Die Zuständigkeit des ZIV reicht dabei bis zum Endsystemanschlusspunkt (Netzanschlussdose in den einzelnen Einrichtungen, Switchport im Serverraum, ...). Die aus verschiedensten Gründen notwendige Separierung in Teilnetze wird durch die bereits beschriebenen verschiedenen Virtualisierungstechnologien und Einordnung in die hierarchische Sicherheitsarchitektur (Netzzonenzuordnung) realisiert.

Neben dem Kommunikationsnetz existieren noch Netze in anderen Gewerken wie z.B. der Gebäudeleittechnik (GLT). Die Integration dieser Netze ist derzeit noch in ihren Anfängen. Durch die vorhandenen Virtualisierungstechnologien und die hierarchische Sicherheitsarchitektur ist die Integration dieser Netze allerdings konzeptionell bereits vollständig berücksichtigt.

1.8 Konvergenz von Tele- und Datenkommunikation

1.8.1 Darstellung der TK-Infrastruktur

Als zentrale TK-Anlage ist ein Telekommunikationsanlagenverbund, bestehend aus Sopho iS 3000 Systemen von NEC Philips, im Einsatz. Angeschlossen an diesen Verbund sind die Einrichtungen

- Westfälische Wilhelms-Universität Münster
- Universitätsklinikum Münster
- Fachhochschule Münster einschließlich Standort Steinfurt
- Kunstakademie Münster
- Centrum für Nanotechnologie
- Außenwirtschaftsakademie und
- diverse An-Institute der WWU
- Studentenwerk (Querverbindung)

Der Betrieb der Telekommunikationssysteme und das Vorhalten der zum Verbund gehörenden notwendigen Server (Backup-Server, Gebühren-Server, Voicemail-Server etc.) ist Aufgabe des ZIV. Die systematische Weiterentwicklung des Telekommunikationsanlagenverbundes unter Einbeziehung neuer Technologien und der Berücksichtigung der bereits getätigten Investitionen ist ein wichtiger Aufgabenteil, welcher durch das ZIV abgedeckt wird.

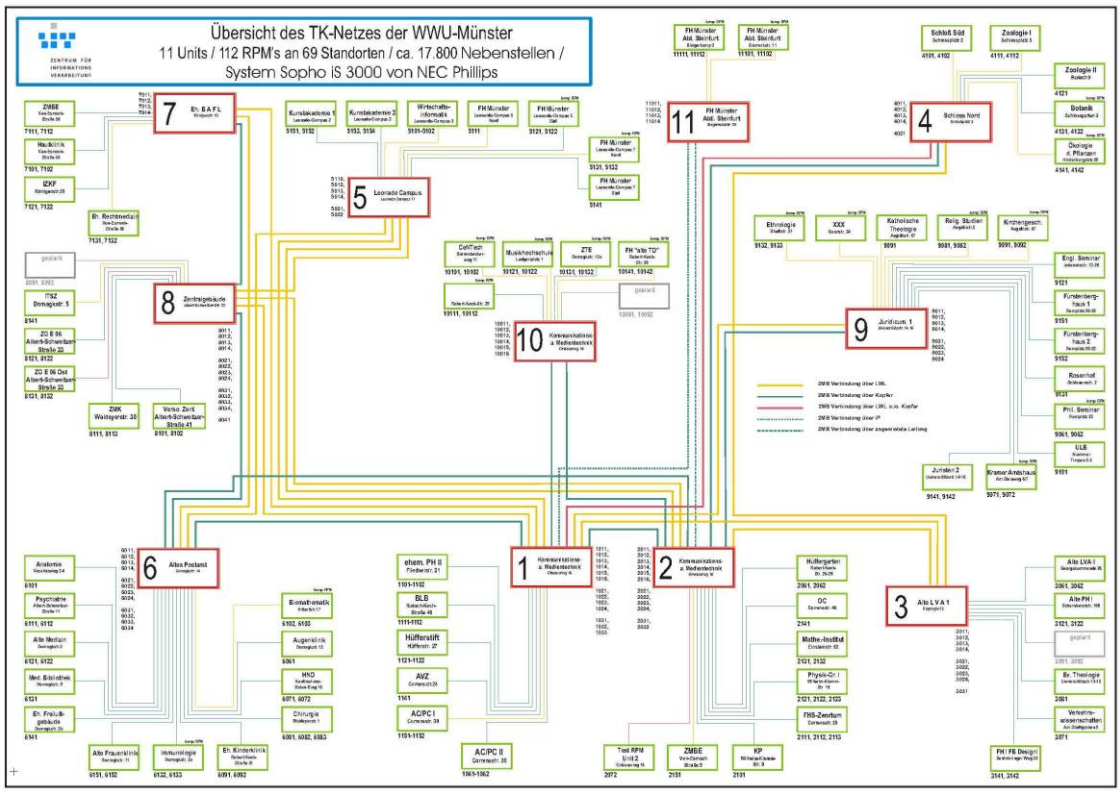


Abb. 18: Die Abbildung stellt schematisch den gesamten Telekommunikationsanlagenverbund des Hochschulstandortes Münster dar. Die übergeordneten TK-Units sind rot gekennzeichnet, die angeschalteten RPMs sind grün gekennzeichnet (hochauflösende Version der Abb. im Anhang).

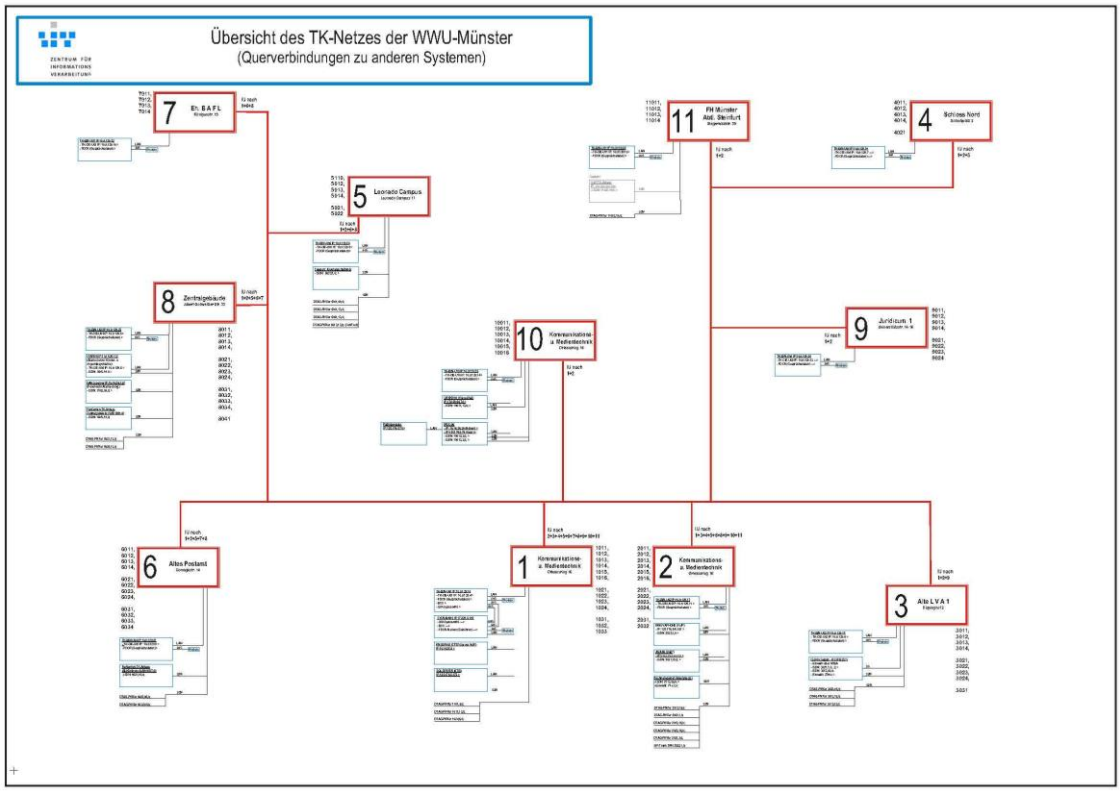


Abb. 19: Die Abbildung stellt schematisch die Anschaltung von weiteren zentralen Systemen und Verbindungen an den Telekommunikationsanlagenverbund dar.

1.8.1.1 Provideranschaltungen

Die Übergänge in das öffentliche Telefonnetz sind sowohl mit konventioneller TDM-Technik (Time Division Multiplexing) als auch mit VoIP realisiert. Zum einen gibt es 19 Primärmultiplexanschlüsse (PMX) zur Deutschen Telekom AG (DTAG). Diese PMX-Anschlüsse sind auf 6 Standorte verteilt. Außerdem gibt es eine Festverbindung zum Fachhochschulstandort Steinfurt. Per VoIP gibt es auch über den X-WiN-Anschluss eine Übergangsmöglichkeit in das öffentliche Telefonnetz. Die Verkehrsweglenkung ist derzeit so, dass der weitaus überwiegende Teil der Gespräche über die PMX-Anschlüsse geführt wird. Die Planung sieht vor, dass in den nächsten zwei Jahren der externe Sprachverkehr deutlich auf den X-WiN-Anschluss verlagert wird. Die hierfür erforderliche Absicherung durch einen redundanten X-WiN-Anschluss ist gegeben. Die Anzahl der Primärmultiplexanschlüsse soll dadurch halbiert werden, was zu einer deutlichen Kostenreduzierung führt. Vertragspartner ist in beiden Fällen der DFN-Verein. Derzeit gibt es noch Probleme mit langen Verbindungsaufbauzeiten bei VoIP-Verbindungen nach extern.

Die Anschaltung des Fachhochschulstandortes Steinfurt an den Telekommunikationsanlagenverbund ist über zwei Arten realisiert. Zum einen über eine dedizierte digitale 2 Mb/s Festverbindung und zum anderen als VoIP-Trunkverbindung über die bestehende WAN-Infrastruktur der Fachhochschule Münster. Neben den Sprachverbindungen werden über diese Verbindungen auch die für den Systemverbund wichtigen Signalisierungs- und Synchronisierungsdaten übertragen. Durch Nutzung einer weiteren vorhandenen WAN-Datenverbindung der Fachhochschule Steinfurt kann die 2 Mb/s Festverbindung abgelöst werden. Somit stellen WAN-Verbindungen der Fachhochschule Münster unter Nutzung der IP-Technologie die Leitungswege für die Übertragung von Sprache und die Übertragung von für den Telekommunikationsanlagenverbund so relevanten Signalisierungs- und Synchronisationsdaten, dar.

Im Bereich Mobilfunk gibt es ca. 460 Mobiltelefone innerhalb eines Rahmenvertrags mit T-Mobil.

Als zentrale Dienste aus dem TK-Bereich sind zu nennen:

- Vermittlung
- Rufnummernverwaltung
- Gebührenabrechnung
- Endgerätesupport
- Voice-Mail
- Fax-Service
- ACD (Automatic Call Distribution)

  Insgesamt kommen ca. 8 ACD-basierte Hotlines innerhalb der WWU zum Einsatz. Auch im ZIV werden im Bereich der zentralen Hotline und auch im Bereich Kommunikationssysteme ACD-basierte Hotlines eingesetzt.

1.8.2 TK-Managementsystem

ISDN-Technologie war ursprünglich die Basis des bestehenden Telekommunikations-anlagenverbundes. Mit einer im Jahr 2005 erfolgten Hochrüstung ist ein hybrider Anlagenverbund geschaffen worden, der zusätzlich VoIP-Technologie unterstützt, was im Wesentlichen eine sanfte Migrationsmöglichkeit darstellt. Die Konfigurations- und Administrationstools des bestehenden Managementsystems wurden entsprechend den erweiterten Funktionen angepasst, ohne dass

allerdings die Integration in übergeordnete Umbrella Managementsysteme (neuerdings auch Cross Domain Management genannt) ermöglicht werden konnte.

Durch verstärkte Anstrengungen des Hersteller NEC, verbunden mit einer Neuausrichtung der Produkte, was teilweise mit einer Neuentwicklung von TK-Systemen einher ging, wurden die Grundlagen für ein neues Managementsystem geschaffen. Dieses neue Managementsystem, welches mit vertretbarem Aufwand auf übergeordnete Managementsysteme aufgesetzt werden kann, stellt die Grundlage für die Schaffung weiterer Synergien dar. Erste wesentliche Schritte werden hierbei die Kopplung an das Managementsystem CA SPECTRUM und die Bereitstellung von Mandantenfunktionen sein, die über die Einstellungsmöglichkeiten, die mittels der Telefonendgeräte vorgenommen werden können, hinausgehen. Mittels Webbrowser können Nutzer ihr Endgerät komfortabel und sicher programmieren bzw. Einstellungen ändern. Sie können Rufweiterleitungen, Tastenprogrammierung, zeitgesteuerte Funktionen, Wichtigkeit der Anrufe steuern und auf vorgegebene Ziele leiten (VIP-Funktion), Speed Dialing, komfortable Möglichkeit der Anpassung an diverse andere Applikationen wie Adressverwaltung, Kontaktdaten, Abwesenheitsgründe, um nur einige zu nennen. Für den Administrationsbereich stellen sich ebenfalls wichtige Neuerungen mit Einführung der Managementsuite ein. Auch hier seien lediglich exemplarisch nur einige genannt, wie umfassendes Monitoring, umfassendes Alerting, LDAP-Provisionierung, Verfügbarkeit von APIs (Application Programming Interface) für die tiefe Integration der Systeme in bestehende Strukturen.

1.8.3 Personal

Anfang des Jahres 2008 wurde die Konvergenz von Tele- und Datenkommunikation an der WWU organisatorisch vollzogen. Das ehemalige Dezernat 4.43 Kommunikations- und Medientechnik der Universitätsverwaltung wurde in das Zentrum für Informationsverarbeitung integriert. Im ehemaligen Dezernat 4.43 waren zuvor das TK-Netz und die damit verbundenen Dienste und außerdem die Medientechnik (AVM: Audiovisuelle Medien) angesiedelt. Die betroffenen Mitarbeiterinnen und Mitarbeiter sind zusammen mit Ihren Aufgaben nun in der Abteilung Kommunikationssysteme des ZIV angesiedelt. Die räumliche Zusammenführung der gesamten Abteilung konnte allerdings bedauerlicherweise wegen mangelnder Flächen-Kapazitäten noch nicht vollzogen werden. Für diese organisatorische Zusammenführung wird hausintern der Begriff *Fusion* verwendet. Dieser Begriff wird der Kürze wegen in den kommenden Ausführungen weiter verwendet.

Es wurden schon vor der offiziell vollzogenen Fusion routinemäßig gemeinsame (d.h. mit Personal aus dem TK- und dem LAN-Bereich) Projekte insbesondere an den technischen Berührungspunkten (VoIP, gemeinsam genutztes LWL-Netz) durchgeführt.

Mit der Fusion wurden Fernmelderevisoren bereits in die Gruppe „Peripherieservice Kommunikationssysteme“ umgesetzt und mit den für die Betriebsfälle des Datennetzes zuständigen Mitarbeitern zusammengeführt. Die Gruppen „TK-Systeme“, „Auskunft und Vermittlung“ und „Medienservice“ sind nach wie vor gesondert organisiert – hier erscheint das Synergiepotenzial auch weniger groß.

Bei der Eingruppierung der von der Universitätsverwaltung übernommenen Mitarbeiter zeigt sich eine Uneinheitlichkeit mit der der angestammten ZIV Mitarbeiter. In „Auskunft und Vermittlung“ ist diese durchwegs E5, maximal E6. Die Fernmelderevisoren sind durchwegs in E7 eingestellt – hier tritt

der größte Unterschied zu den in E9 eingestellten LAN-Technikern des „Peripherieservice“ auf. Die TK-System-Experten sind mit E9 gleichwertig zu den LAN-Technikern eingestuft.

Punktuell konnten bereits bei einigen der qualifizierten ehemaligen Verwaltungsmitarbeiter Verbesserungen bei der Vergütung ihrer Tätigkeiten erzielt werden.

1.8.4 Gemeinsame Nutzung von Netzinfrastruktur und Werkzeugen

Bereits vor der Fusion gab es zwischen den zuvor organisatorisch getrennten Bereichen eine enge Zusammenarbeit. So wurde beispielsweise das LWL-Netz gemeinschaftlich genutzt. Auch die ersten VoIP-Installationen wurden bereits vor der Fusion gemeinsam vorangetrieben. Das im TK-Bereich genutzte hochpaarige Kupferkabelnetz ist nun Bestandteil des gemeinsamen Kommunikationsnetzes geworden und stellt eine beträchtliche Ressource dar. Über das vom ZIV bereitgestellte Kommunikationsnetz werden zusätzlich Dienste anderer universitärer zentraler Einrichtungen abgestützt. Häufig handelt es sich um Alarmierungs- oder Störmeldungen, die einen zeitnahen Einsatz, z.B. der Feuerwehr, der Polizei oder des Bereitschaftsdienstes der WWU, erforderlich machen. Eine hohe Verfügbarkeit des Kommunikationsnetzes ist daher zwingend gefordert. Im Einzelnen sind das:

- Universitätsgebäudeweite Gebäudeleittechnikvernetzung
- Hauptmeldeleitungen der einzelnen Brandmeldeanlagen (WWU, UKM, FH Münster, Kunstakademie Münster)
- Störmeldeleitungen für Brandmelde-, Einbruchmeldeanlagen (Brandmeldeanlagennetzwerk und Einbruchmeldeanlagennetzwerk)
- Störmelde- und Alarmleitungen für analoge Systeme (analoge Störmeldezentrale)
- Notrufsysteme in Aufzügen der WWU
- Vernetzung der Zugangskontrollsysteme

Eine Möglichkeit, diese Dienste performanter an das Kommunikationsnetz des ZIV anzuschalten, ist die Nutzung der am ZIV eingesetzten DSLAMs (Digital Subscriber Line Access Multiplexer), unter Verwendung der bestehenden Kupferkabelverbindungen, wobei Übertragungsraten von bis zu 50 Mbit/sec. (VDSL2) und 16 Mbit/sec. (ADSL2+) realisiert werden. Der Einsatz dieser Technologie stellt eine Komplettierung der Datenübertragungstechnik des ZIV dar und schützt die bereits getätigten Investitionen der WWU.

Die an anderer Stelle beschriebene Netzdatenbak LANbase wird inzwischen gemeinschaftlich genutzt. So werden beispielsweise VoIP-Telefone und DSLAMs in LANbase erfasst. Für die Installation von VoIP-Telefonen werden die in LANbase vorhandenen Change-Management-Prozeduren verwendet. Für eine gemeinsame Projektverwaltung kommt LANbase ebenso zum Einsatz. Als nächstes soll das im LAN-Bereich eingesetzte Trouble-Ticket-System (Eigenentwicklung *NOCase*) für die gemeinsame Nutzung weiterentwickelt werden.

1.8.5 Planung der VoIP-Migration

Allein wegen der großen Zahl von ca. 8.500 konventionellen Telefonen an der WWU (ca. 7.500 am UKM) ist klar, dass die vollständige Migration zu VoIP sich über einen sehr langen Zeitraum erstrecken wird. Eine Wartung der TK-Anlage ist durch den Hersteller bis 2017 gesichert. Dieser Zeitpunkt wird an der WWU für die vollständige Migration nach VoIP angestrebt. Für das UKM wird erwartet, dass im Jahr 2010 eine genauere Festlegung des Migrationsplans nach VoIP erfolgt.

Die Migrationsstrategie sieht vor, dass bei Neubauten oder Sanierungen die Gelegenheit zur VoIP-Einführung genutzt wird. Bei einer Teilsanierung wird dann möglichst auch eine VoIP-Umstellung der nicht sanierten Bereiche realisiert. Netzkomponenten für die VoIP-Anbindung sollten über redundante Netzteile, PoE-Funktionalität für die Versorgung der Telefone und Priorisierungsmöglichkeiten verfügen. Die Integration der VoIP-Geräte in das Kommunikationsnetz ist bereits vollständig in der beschriebenen IT-Sicherheitsarchitektur vorgesehen (Festlegung entspr. Netzzonen bzw. VLANs).

Die Anbindung der VoIP-Telefone an die TK-Units erfolgt dabei mittels des SIP-Protokolls über sog. ISG-Baugruppen (In System Gateway). VoIP-Telefone werden dabei wie ein fest angeschlossener (d.h. registrierter Rechner) betrieben. Eingesetzt werden derzeit für Neuinstallationen Polycom Soundpoint IP 650 (oder 450) VoIP-Telefone. Für das VoIP-Telefon wird ein eigenes Tertiärkabel verwendet (vgl. Abschnitt 1.8.6 *„Konzeptdarstellung "Zusätzliche Verkabelung für VoIP"“*).

Um eine angemessene Dienstgüte der VoIP-Kommunikation zu realisieren, wurde bislang eine Überprovisionierung ohne Qualitätseinbußen vorgenommen. Zukünftig könnte eine Priorisierung der VoIP-Kommunikation notwendig sein. Ggf. soll dann eine datenbankgestützte Konfiguration dieser Funktionen realisiert werden.

1.8.6 Konzeptdarstellung "Zusätzliche Verkabelung für VoIP"

Die Einführung von VoIP-Telefonen am Arbeitsplatz führt zu einer ungefähren Verdopplung der Anzahl der personengebundenen Endgeräte. Für diese erhöhte Portzahl gibt es verschiedene Realisierungsvarianten:

- "Cable-Sharing" zwischen VoIP-Telefon und Arbeitsplatzrechner
- Einsatz des VoIP-Telefons als LAN-Switch zum Anschluss des Arbeitsplatzrechners
- Nutzung der vorhandenen Kupferverkabelung mittels DSL-Technik für den Anschluss der VoIP-Telefone
- zusätzliche Verkabelung für den Anschluss der VoIP-Telefone

Aus betrieblicher Sicht muss dabei unbedingt eine Beschränkung auf eine Standardvariante angestrebt werden. Die Entscheidung zugunsten einer zusätzlichen Verkabelung für den Anschluss von VoIP-Telefonen soll hier erläutert werden.

Mit "Cable-Sharing" wäre der Einsatz von Gigabit-Ethernet-Technologie am Desktop nicht möglich.

Beim Einsatz eines VoIP-Telefons als LAN-Switch zum Anschluss des Arbeitsplatzrechners muss sichergestellt sein, dass aktuelle und zukünftige Funktionalitäten aus dem LAN-Bereich am Switch-Port des Telefons zur Verfügung stehen, da die Anschlussmöglichkeiten und die Verfügbarkeit des PCs durch das Telefon festgelegt sind. Als aktuelle Funktionalitäten wären beispielsweise zu nennen:

- Gigabit-Ethernet-Geschwindigkeit
- 802.1q (portbasierte VLANs als derzeitiger Standard im Netz von WWU und UKM)
- 802.1p (Priorisierung)

Selbst wenn geforderte Features zu einem bestimmten Zeitpunkt verfügbar sein sollten, so muss angezweifelt werden, ob technologische Entwicklungen im LAN-Bereich bei der Entwicklung von VoIP-Telefonen als LAN-Switch zeitnah nachvollzogen werden. Auch wenn das der Fall sein sollte,

würde dann eine Technologiefortschreibung einen steten Austausch von VoIP-Telefonen erfordern. Der Betrieb und stete Austausch von VoIP-Telefonen wäre bei derzeit ca. 17.000 Telefonen (WWU und UKM) selbst bei einer deutliche Reduktion der Zahl von Telefon-Festanschlüssen eine nicht zu bewältigende Aufgabe. Das gegenseitige Störpotential zweier Desktop-Geräte stellt ein weiteres erhebliches betriebliches Problem dar. Zu erwähnen wäre noch, dass mit dieser Variante auch ein größerer Stromverbrauch der Telefone verbunden ist. Bei einer PoE-Versorgung der Telefone bedeutet das in der Folge Mehrkosten für PoE-Switches und House-Keeping (Klimatisierung, USV-Versorgung).

Bei der Nutzung der vorhandenen Kupferverkabelung mittels DSL-Technik für den Anschluss der VoIP-Telefone kommt man zwar ohne Investition in eine zusätzliche Verkabelung aus. Allerdings ist diese Variante betrieblich deutlich aufwendiger, da mit DSL eine zusätzliche Technik und die damit verbundenen Geräte (auch am Desktop) zum Einsatz kommen. Da DSL-Technik jedoch im Netz der WWU bereits zum Einsatz kommt, kann diese Variante in absolut untergeordneter Größenordnung in Spezialfällen in Betracht gezogen werden.

Eine zusätzliche Verkabelung für den Anschluss der VoIP-Telefone bedeutet zwar einen hohen investiven Aufwand, jedoch sind die langfristigen Vorteile gegenüber den anderen Varianten kaum zu überschätzen. Für den Desktop-PC und auch für das VoIP-Telefon ist dauerhaft sichergestellt, dass zukünftige Anforderungen und technologische Weiterentwicklungen abgedeckt werden können. Außerdem sind Anforderungen an das House-Keeping geringer und die Auswahlmöglichkeiten für VoIP-Telefone größer. Auf lange Sicht relativieren sich insgesamt die hohen Investitionskosten dieser Variante.

1.8.7 Potential der Konvergenz

Waren bis dato, durch die Trennung der beiden großen Netze bedingt, an der WWU und den angeschlossenen Einrichtungen immer Übergänge zu berücksichtigen, können die Mehrwertdienste zukünftig ohne Medienbruch bereitgestellt werden. Auch hier findet zukünftig eine sanfte Migration statt, so dass die Bereitstellung von Gateways für den Übergang von der IP-Welt in die ISDN-Welt nur begrenzt stattfinden muss. Vorrangig bezieht sich diese Entwicklung auf die zentral durch das ZIV bereitzustellende Unified Communication Lösung mit Diensten wie Fax-Funktionen, Voicemail-Funktionen, Instant Messaging-Funktionen, SMS-Funktionen. Pilotinstallationen dieser Funktionen im virtuellen Serverumfeld sind bereits mit Erfolg durchgeführt worden.

Das Bereitstellen eines zentralen kommunikationsnetzweiten elektronischen Telefonnummernverzeichnisses konnte bereits als eines der ersten erfolgreichen Projekte realisiert werden. Mittels eines LDAP basierenden Verzeichnisses steht das zentrale Telefonbuch den Nutzern eines VoIP-Endgerätes zur Verfügung.

Als weiterer Punkt ist zu erwähnen, dass die gesamte Videokonferenzinfrastruktur ebenfalls bereits unter dem Aspekt der Konvergenz in das Kommunikationsnetz eingebunden werden konnte. Alle Verbindungsmöglichkeiten, sowohl intern als auch extern können unter Nutzung von IP und/oder ISDN frei gewählt werden. Bei den zentralen Systemen, vorrangig der MCU, sind die Userinterfaces so gestaltet, dass technisch unbedarfte Nutzer durchaus eigenständig, nach kurzer Anleitung, Mehrfachkonferenzen weltweit aufsetzen können. Hier ist ein weiterer Ausbau unter Einbeziehung der zu schaffenden IP Streaming Umgebung geplant. In Abschnitt 1.5.5 *„Intranet / Mediennetze (AVM: Audiovisuelle Medien)“* und Abschnitt 1.6.8 *„Mediennetze, AVM (Audiovisuelle Medien)“*

wurden bereits die Themen IP-Multicast und IPTV unter den Aspekten der Synergie und Konvergenz behandelt.

Umfangreiche DECT-Installationen (Digital Enhanced Cordless Telecommunications) stellen zur Zeit eine breite Basis für mobile Sprachkommunikation in Gebäuden, sowohl der WWU als auch des UKM und der Fachhochschule, dar. Ein weiterer Ausbau der mobilen Sprachkommunikation soll zukünftig mittels der WLAN-Infrastrukturen erfolgen. Hierbei ist eine flächendeckende Versorgung mit WLAN - Accesspoints in den Gebäuden der angeschlossenen Einrichtungen ein Ziel der Kommunikationsinfrastrukturentwicklung. Hierbei stellt das FMC (Fixed Mobile Convergence) eine bedeutende Entwicklung dar. Eine deutliche Minimierung der momentanen Kosten für Mobilkommunikation, abgestützt durch GSM/UMTS-Fremdnetze, steht in unmittelbarem Zusammenhang mit der Entwicklung dieser Technologie. Die Erreichbarkeit unter einer Rufnummer, sowohl festnetz- als auch mobilfunknetzseitig sei hier der Vollständigkeit halber erwähnt.

Diese mögliche Entwicklung stellt für die WWU mit ihrer dezentralen Gebäudestruktur eine große Herausforderung dar.

2 Netzentwicklungsplan

2.1 Vorbemerkung

Das Datennetz der WWU Münster ist mit derzeit bereits ca. 44.000 Anschlüssen sehr umfangreich – das jährliche Wachstum mit über 3.000 Anschlüssen sehr hoch. Eine Abflachung dieser Entwicklung ist für den Antragszeitraum 2010-2016/17 nicht zu erwarten. Auf Grund dieses Mengengerüstes ist klar, dass der Ausbau und die Erneuerung des Netzwerkes nur kontinuierlich und nicht in disruptiven Projektschritten erfolgen kann – die personellen Kapazitätsanforderungen und die logistischen Voraussetzungen dafür wären zu groß und die Gefahren für eine nicht tolerierbare Beeinträchtigung des Netzbetriebs zu hoch.

Insbesondere der Ausbau der Netzanschlüsse, die Verbesserung des House-Keepings, der Ausbau des WLAN, der Austausch der Edge-Switches und der Übergang zu VoIP im TK-Bereich erfolgen dabei kontinuierlich.

Aber auch Projektmeilensteine des Entwicklungsplans mit besonderer Priorität können aufgezeigt werden. Dabei sind von der zeitlichen Abfolge folgende bereits recht klar umreißbar:

- Erneuerung des Intrusion Prevention Systems bereits in 2010
- Flächendeckende Bereitstellung von Unified Communication-Services in 2011
- Vollständige Umsetzung des 3-Layer Core Schemas durch vollständige Umsetzung eines mit 10GE an den Midrange angebundenen Distribution Layers und damit einhergehend Ersatz der Multimode- durch Singlemode LWL-Verkabelung im Laufe der Jahre 2010-2012
- Umstellung auf 40GE zwischen Core und Midrange Layer in 2012-2014
- Etablierung von Data Center Switches in 2012
- Flächendeckung mit 11N WLAN bis 2015
- Flächendeckende Einführung von 802.1X bis 2016
- Flächendeckende Umstellung auf VoIP-Telefonie bis 2017

Zeitlich weniger klar und von der weiteren technologischen Entwicklung und der Bedarfslage abhängig sind folgende Meilensteine:

- Einführung von Network Access Control
- Einführung von Content Filtering Technologie
- Einführung von IP Multicast
- Umfassende Einführung von IPv6

2.2 Bereiche mit stetiger Entwicklung

2.2.1 Netzausbau

Das ungebrochene Wachstum des Kommunikationsnetzes ist deutlich sichtbar (Abb. 20). Das auch weiterhin im Bereich von über 3.000 Neuanschlüssen pro Jahr liegende Wachstum ist zum Teil auch auf Installation von WLAN-Access-Points und die bei allen neuen Projekten durchwegs mit Cat6 erfolgende TK-Verkabelung zurückzuführen. Für den Zeitraum bis 2016/17 wird – nicht zuletzt wegen der sukzessiven Migration der TK-Anschlüsse – ein unverändertes Aufkommen an Neuanschlüssen in dieser Größenordnung erwartet. Dabei sind auch Erweiterungen nach individuellem Bedarf von Einrichtungen der WWU auf Grund der immer noch wachsenden Intensivierung der IT-Nutzung, die

Einbindung der Gebäudeleittechnik (GLT) in das Datennetz, Umbauten, Sanierungen und Fluktuationen bei den von der WWU genutzten Liegenschaften zu berücksichtigen. Die Ingenieurleistungen dafür werden vom ZIV direkt erbracht, wodurch ein flexibler, termintreuer und kosteneffizienter Ausbau des Netzwerkes gewährleistet wird.

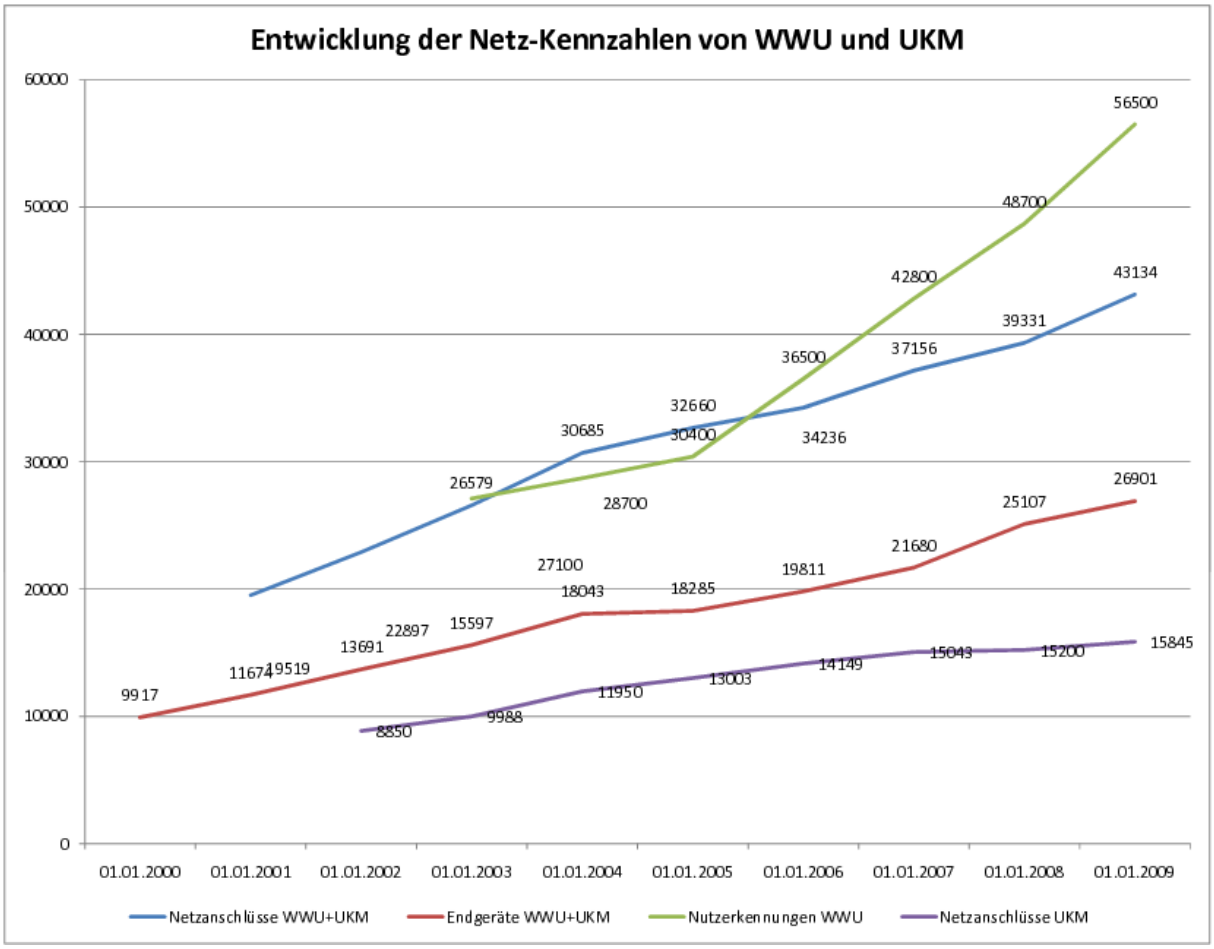


Abb. 20: Entwicklung der netzbezogenen Kennzahlen – in den zurückliegenden 8 Jahren haben sich die Zahlen von Netzanschlüssen und Endgeräten mehr als verdoppelt. Die Zahlen für die im Gelände des UKM befindlichen Netzanschlüsse sind separat ausgewiesen. Bei den Endgeräten ist eine Trennung nicht klar nach UKM und WWU möglich, da im Bereich des UKM neben den für die Patientenversorgung verwendeten Endgeräten auch die der Medizinischen Fakultät der WWU angebunden sind.

2.2.2 Edge-Switches

In der Laufzeit dieses Antrages bis 2016/17 ist der komplette Austausch der Edge-Switches notwendig. Wegen des teilweise schon sehr hohen Alters (siehe Abb. 21) einer großen Zahl von Geräten und den damit verbundenen Problemen (erhöhte Störungshäufigkeit mit entsprechend hohem Betreuungsaufwand; fehlende Ersatzteilversorgung; mangelnde Backplane-Performance; hohe Port-Überbuchung und fehlende Funktionalitäten) ist partiell sehr dringender Handlungsbedarf gegeben. Bezüglich der Funktionalität werden die nachstehenden Ziele verfolgt:

- Flächendeckende Ausstattung mit 1GE to the desktop bzw. für die Anbindung von WLAN Access-Points mit 802.11N (oder nachfolgendem) Standard

- Für sensible Bereiche (ca. 20% der Switch-Stacks) redundante Uplinks für höhere Verfügbarkeit.
- Bereitstellung von PoE, PoE+ und 802.3af Energiemanagement-Funktionalität für Endgeräte wie 11N Access-Points, VoIP Telefone, Netbooks etc…
- Flächendeckende 802.1X Authentifizierung zur Erhöhung der Netzsicherheit und zur Ablösung der derzeit VPN-basierten Authentifizierung für pLANet ("öffentliche" LAN-Festanschlüsse).
- Q-in-Q-Support zur Unterstützung einer höheren Zahl von VLANs – insbesondere im Access-Bereich.
- IPv6 Multicast Group Support
- Energieeinsparungen

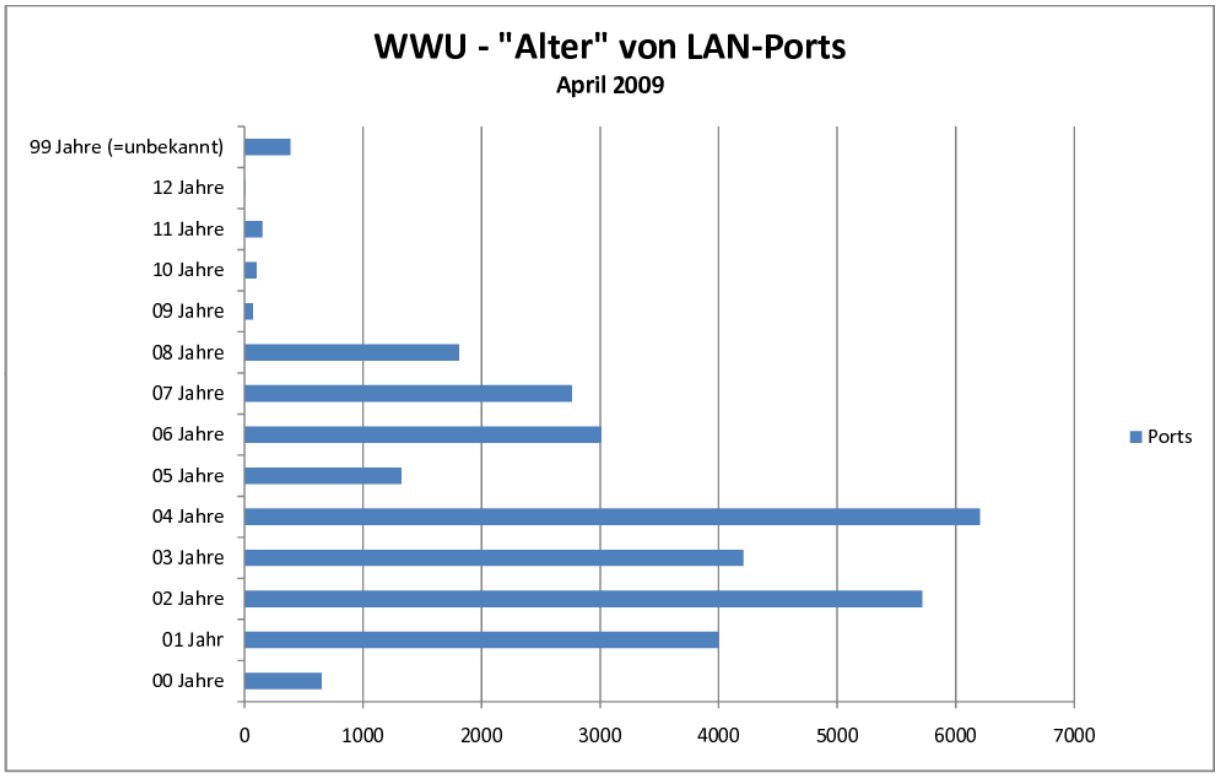


Abb. 21: *Die Altersverteilung der Edge-Switches zeigt den in den nächsten Jahren akut anstehenden Investitionsbedarf. Ca. 9.000 Ports sind 5 Jahre alt oder älter und müssen dringend mit aktueller Technologie ersetzt werden.*

2.2.3 WLAN

Nicht zuletzt die im Mai 2009 durchgeführte Nutzerbefragung des ZIV hat ergeben, dass WLAN als ein sehr wichtiger Service des ZIV gesehen wird, und dass die Flächendeckung und Geschwindigkeit trotz der bislang bereits ca. 700 eingesetzten Access-Points noch als sehr verbesserungsfähig empfunden wird. Es wird deshalb die zügige Umsetzung eines flächendeckenden Ausbaus einer 11N-basierten WLAN Infrastruktur (mit final ca. 3.000 Access-Points) angestrebt. Dazu ist in einem ersten Schritt der Austausch der teils schon recht betagten Proxim Orinoco APs notwendig. Die Zukünftige 11N-Infrastruktur muss über eine entsprechend dichte Abdeckung verfügen, um zumindest auch VoIP over WLAN Services unterstützen zu können (schnelles Roaming muss über zentrales WLAN-Switching unterstützt werden). In manchen Bereichen (insbesondere im Klinikum) wird auch von der Nutzung von Location-Services ausgegangen. Die Beschaffung von entsprechender WLAN-

Messtechnik für die damit beschäftigten ZIV-Mitarbeiter ist begleitend ebenso erforderlich wie die Schaffung von NAT- und Web-Proxy-Lösungen.

2.2.4 TK- und Medien-Konvergenz

Die bestehende Telefonanlage erlaubt durch die Einbindung von VoIP-Endgeräten eine sanfte Migration. Neubau-Vorhaben werden an der WWU bereits mit VoIP-Telefonen ausgestattet. Im Bereich der Tertiärverkabelung werden bereits konsequent eigene Cat6-Anschlüsse für Telefone verlegt. Im Bereich der Primär- und Sekundärverkabelung wird ausschließlich der Ausbau der Lichtwellenleitertechnologie vorangetrieben. Die Verfügbarkeit der klassischen TDM-basierten Telefonsysteme ist durch den Hersteller bis 2017 gewährleistet, wobei danach keine weiteren Entwicklungen geplant sind, jedoch eine Ersatzteilvorhaltung seitens des Herstellers bis 2023 zugesichert wurde. Dieses Statement seitens des Herstellers NEC ist besonders wichtig im Bezug auf die weitere Entwicklung der Sprachdienste am UKM und der eventuell nicht vollständigen Umstellung auf VoIP an der WWU zum Jahr 2017.

Die Entwicklung der Tätigkeitsprofile, der im Bereich Peripherie-Service tätigen Mitarbeiter, muss innerhalb dieser geschlossenen Zeitintervalle forciert werden und dazu führen, dass eine einheitliche Endgerätebetreuung möglich wird. Die USV-Versorgung für die VoIP-Telefone muss zumindest in dem Maße sichergestellt werden, wie das für Notfallpläne notwendig ist. Die Erweiterung des Veranstaltungsnetzwerkes soll durch den Medien-Service unter Einsatz von Encoder-/Decodertechnologie, die Video-Streaming Übertragung von Veranstaltungen campusweit ermöglichen, umgesetzt werden. Der Einsatz von IPTV ist in nächster Zeit wegen der damit verbundenen Einsparmöglichkeiten bei den Rundfunkgebühren ebenfalls umzusetzen.

2.2.5 House-Keeping

Um den wachsenden Anforderungen an die Verfügbarkeit des Kommunikationsnetzwerkes gerecht zu werden (VoIP-Telefonie mit Notruf-Funktionen, GLT, unentbehrliche Informationssysteme, …) ist die Absicherung der Netzwerk-Standorte durch USV-Anlagen, Klimatisierungen, Standort-Überwachung und Konsol/KVM-Zugangssysteme notwendig. Für die wichtigsten Standorte (Core/ Midrange/ Distribution und Edge-Verteilerstandorte mit hoher Port-Zahl) wird deshalb eine USV-Ausstattung (wo noch nicht vorhanden) eingeplant (ca. 30% der Standorte). Bei der Klimatisierung ist allerdings die Realisierung der Baumaßnahmen über das Technik-Dezernat notwendig.

2.3 Bereiche mit wesentlichen Entwicklungsschritten („Meilensteinen“)

2.3.1 Core – Midrange - Distribution

Das Hauptaugenmerk bei der Fortentwicklung des aktiven Backbones liegt auf der flächendeckenden Umsetzung des bereits begonnen 3-Layer-Konzeptes mit Core, Midrange und Distribution – es sollen also die Anbindungen der Edge-Switches komplett vom Midrange auf den Distribution-Layer migriert werden. Um bei den Uplinks des vervollständigten Distribution-Layers höhere Bandbreiten von 10GE einsetzen zu können, ist eine teilweise Erneuerung der passiven Infrastruktur von der anfänglich noch verwendeten Multi-Mode- auf Single-Mode-Verkabelung notwendig. Um den absehbaren Bandbreitenanforderungen gerecht zu werden, die sich beispielsweise auch aus der flächendeckenden 1GE to the desktop Ausstattung ergeben, ist für den Distribution-Layer der Einsatz von 2x 10GE Uplinks in den Midrange-Layer geplant. Vom Midrange zum Core sind 4x 10GE eingeplant (hier besteht die Erwartung, dass bis zur Realisierung die 40GE bzw. 100GE Technologie verfügbar ist und hier eingesetzt werden kann). Da für die in Midrange und Core eingesetzten Cisco

Catalyst 6500 Geräte auch Entwicklungswege zu 2 Terabit Backplane-Leistung und für den Einsatz von 40GE Modulen aufgezeigt werden, wird hier von einem Upgrade dieser Geräte ausgegangen, womit eine sanfte Migration sichergestellt ist.

Es ist zu erwarten, dass während der Laufzeit des Antrages die Bandbreitenanforderungen im Backbone stetig wachsen werden, da immer größere Datenmengen auf zentralisierten Speichersystemen vorgehalten werden (z.B. SoFS-Fileservice) und entsprechend auch die Backup- und Archiv-Nutzung anwächst, die Rezentralisierung der Serversysteme und der Trend zum Server-based Computing den Datenverkehr zu den Data Centers verstärkt und auch Videostreaming (z.B. für Veranstaltungsübertragung oder IPTV) immer verbreiteter wird. In diesem Umfeld ist auch mit einem steigenden Bedarf für die Einführung von IP Mulitcast zu rechnen.

Der Transfer und die Visualisierung (z.B. in Virtual Reality oder Augmented Reality Umgebungen) großvolumiger Simulationsdatensätze aus dem High Performance Computing, aber auch große Datenmengen von neuen bildgebenden Verfahren in der Medizin müssen zukünftig bewältigt werden und machen einen für Leistungsspitzen dimensionierten Backbone erforderlich.

Für die Periode bis 2016/17 ist auch endgültig mit der flächendeckenden Einführung von IPv6 zu rechnen. Die Voraussetzungen dafür sind in Münster durch die frühe Beteiligung am EU JOIN Projekt sehr gut – die Core-Geräte unterstützen prinzipiell alle IPv6 – trotzdem ist von substantiellem Aufwand für diese Umstellung auszugehen.

Das bewährte VLAN-Konzept wird in diesem Zeitraum evtl. evaluiert werden müssen, da die stetig wachsende Zahl von VLANs administrativ und bei den einsetzbaren Geräten auf Grenzen stoßen könnte.

2.3.2 Data Center

Wie bereits beim Core beschrieben, wird von einem Trend zur stärkeren Zentralisierung bei den Servern und zum Server-based Computing ausgegangen. Neben dem Rechnersaal des ZIV wurde 2007 ein gemeinsam mit den dezentralen IT-Organisationseinheiten (IVVen) genutztes Data Center geschaffen. Da dessen räumliche Ressourcen bald erschöpft sein werden und insbesondere von den IVVen ein zweiter Standort für Failover Lösungen benötigt wird, befindet sich ein weiteres gemeinsames zentrales Data Center in Planung. In diesen 3 Data Centers ist mit einem entsprechend hohen Datenaufkommen und einem Bedarf für eine hohe 10GE Portdichte zu rechnen. Die absehbare Konvergenz zwischen LAN und SAN (Data-Center-Ethernet, FCoE, …) und die hohen Verfügbarkeitsanforderungen machen den Einsatz großer Data Center Switches mit hoher Resilienz und hoher Portdichte in absehbarer Zeit erforderlich. Es wird deshalb für jeden der drei Standorte ein solcher Switch (mit jeweils 100x 10GE Ports) vorgesehen mit redundanter Anbindung an den Midrange-Layer, um auch im K-Fall Data Center Services durchgängig verfügbar zu halten. Mit der weiteren technischen Entwicklung erscheint auch bei zukünftigen Generationen von HPC-Cluster-Systemen die Nutzung von 100GE-basierten konvergenten Fabrics anstelle gesonderter Infiniband-Infrastrukturen als high performance low latency Interconnect denkbar.

2.3.3 Sicherheit

Das Thema Netzsicherheit wird nicht nur technisch, sondern auch organisatorisch vorangetrieben. Die Anfang 2009 durchgeführte Sicherheitsbegehung hatte sehr wichtige Impulse gegeben und soll auch zukünftig in regelmäßigen Abständen wiederholt werden. Die Erarbeitung von

Netzstrukturierungs-Konzepten durch das ZIV gemeinsam mit den Nutzern ist ebenfalls ein wichtiger organisatorischer Bestandteil der Netzsicherheit und soll so fortgeführt werden.

An technischen Maßnahmen sind eine Erneuerung des IPS zur Anpassung an die steigenden Bandbreitenanforderungen geplant, eine Content-Filtering-Lösung, weitere Netzanalyse-Werkzeuge sowie eine flächendeckende Umsetzung von 802.1X. Eine Lösung für Network Access Control (NAC) wird während der Antragslaufzeit absehbarer weise etabliert werden müssen – dabei muss jedoch eine Nutzungsbeschränkung, die die Universitätsangehörigen bei Ihren Tätigkeiten behindert, unbedingt vermieden werden und der Vielzahl an eingesetzten Gerätetypen Rechnung getragen werden. Deshalb ist zum gegenwärtigen Zeitpunkt hierzu nur eine grobe Abschätzung möglich, da noch keine Lösungen, die die Anforderungen der WWU vollumfänglich erfüllen, am Markt verfügbar sind.

2.3.4 Netzmanagement: Netzadministration, Netzbetrieb, Netzüberwachung

Mit steigender Ausdehnung und Komplexität des Netzwerkes werden elaborierte Werkzeuge zum Netzmanagement immer wichtiger. Die realisierten Konzepte im Bereich Netzmanagement werden in den Abschnitten 3.6, 3.8, 3.9 und 3.10 ausführlich beschrieben.

Die Eigenentwicklung *LANbase* ist das zentrale Werkzeug für Dokumentation, Administration und Betrieb des Netzwerkes. Eine funktional vergleichbare kommerzielle Lösung ist nicht bekannt. Somit kann die Weiterentwicklung dieser bewährten Lösung als effektivster und kosteneffizientester Zugang gesehen werden (vgl. Ausführungen hierzu unter 3.6.4 *„Konzeptdarstellung „Eigenentwicklungen statt Einsatz kommerzieller Produkte““*). Dieses Teilprojekt soll in den Jahren 2010-2014 durch eine im Rahmen des Ausbaus des Kommunikationssystems finanzierte wissenschaftliche Mitarbeiterstelle (E13) erarbeitet werden. Es soll hierbei insbesondere ein mandantenfähiges Change-Management (für dezentrale Administratoren über das LANbase-basierte Portal *NIC_online*) mit folgenden Meilensteinen realisiert werden:

- Vergabe von IP-Adressen durch authorisierte Nutzer
- Switchport-Einstellungen der Netzanschlussdose: z.B. Speed, Duplex-Mode, VLAN, PoE, QoS/CoS
- Erstanalyse bei Fehlersituationen durch Anzeige von Fehlerinformation des Switch-Ports
- Verwaltung netzseitiger Sicherheitsmaßnahmen: ACL-Verwaltung (Stateless Packet Screens von IP-Routern)

Aber auch in folgenden Bereichen gibt es Bedarf für weitere Eigenentwicklungen im Rahmen dieses Teilprojektes:

- Weiterentwicklung des (LAN-)Trouble-Ticket-Systems (in LANbase integrierte Eigenentwicklung NOCase) für die gemeinsame Nutzung im LAN- und TK-Bereich
- Scheduler für kurzzeitige Änderungen (z.B. Veranstaltungen)

Für die Netzüberwachung wurde in 2008 mit CA SPECTRUM eine zukunftsträchtige Nachfolgelösung für das auslaufende Tivoli NetView-System aus Haushaltsmitteln beschafft. Mit SPECTRUM soll ein Kundenportal für den Zugang zu Netzstatus-/Netzüberwachungsinformation aufgebaut werden. Außerdem sollen Netzperformance-Messagenten, die von SPECTRUM gesteuert werden, an ausgewählten Standorten im Netz installiert werden. Hierfür sollen kleine, dedizierte Router (vgl. Cisco IOS-Feature IP-SLA) eingesetzt werden.

Außerdem ist beabsichtigt, im Bereich Netzreporting (systematische Erfassung von Netznutzungszahlen) eine umfassende Lösung zu realisieren. In Frage kommt hierfür das Produkt *eHelath*. eHealth stammt ebenso wie SPECTRUM von der Firma CA und bietet eine einfache Anbindung an SPECTRUM. Grundsätzlich käme aber auch ein funktional vergleichbares alternatives Produkt in Frage.

Für das für Change Management und Workflow-Automatisierung derzeit eingesetzte Produkt *EMS* von der Firma 3Com ist vom Hersteller der Verkauf im Sommer 2009 eingestellt worden. Bis Ende 2011 wurden noch geringfügige Weiterentwicklungen und Fehlerbehebungen zugesagt. Jedoch ist abzusehen, dass die Beschaffung eines Nachfolgeprodukts notwendig ist.

Da der DNS-Service für den Netzbetrieb von herausragender Bedeutung ist, soll eine eigene umfassende Überwachung (Verfügbarkeit, Datenaktualität, Datenkonsistenz) für den DNS-Service realisiert werden. In Frage kommt hierfür das Produkt *Men & Mice DNS Performance Monitor und DNS Expert AD*.

Darüber hinaus ist geplant, in den Bereichen Netzüberwachung und Troubleshooting folgende Funktionalitäten zu realisieren (bzw. Tools einzusetzen):

- Check von Verbindungen durch FWs, ACLs
- Bereitstellen von Counter und Statistiken (Durchsatz, Fehler, Laufzeiten etc) für Kunden
- Protokollanalyse-Tools mit 10GE-Support
- zentrale Analyse-PCs
- WLAN Messtechnik
- Netzanalysetools (Fluke Nettools oder vergleichbar für GE-Technik)
- DSL-Testtool
- Netzanomalie-Erkennung

3 Betriebs- und Managementkonzept

3.1 Verantwortungs- und Zuständigkeitsverteilung

Die Verantwortungs- und Zuständigkeitsverteilung der Informationsverarbeitung an der WWU wurde bereits ausführlich im Abschnitt 1.2.2 *„Entscheidungsträger“* erläutert. An dieser Stelle wird daher nur die *Zuständigkeit für das Kommunikationssystem* kurz gesondert dargestellt.

Das Kommunikationssystem der gesamten WWU und des UKM wird vom ZIV verantwortlich geplant, aufgebaut und betrieben. Konkret ist diese Verantwortlichkeit in der Abteilung 1 "Kommunikationssysteme" des ZIV angesiedelt. Das ZIV ist hierbei sowohl für das gesamte passive Netz inkl. Verkabelung bis zu den Netzanschlusspunkten (Schnittstelle zu den Nutzern) in den einzelnen Räumen als auch für sämtliche aktiven Netzkomponenten zuständig. Die realisierten Netzdienste wurden bereits ausführlich im Abschnitt 1.6 *„Vorhandene und angestrebte Netzstruktur“* dargestellt.

Netzerweiterungen werden ausschließlich vom ZIV geplant, beauftragt und koordiniert. Für die beim Aufbau anfallenden Verkabelungs- und Bauarbeiten sind entsprechende Verträge mit mittelständischen Betrieben abgeschlossen worden. Bei neuen Gebäuden oder größeren Gebäudesanierungen wird die Installation des passiven Netzes vom Bau- und Liegenschaftsbetrieb NRW gemäß den Technischen Anschlussbedingungen (TAB) des ZIV ausgeschrieben und beauftragt und in Zusammenarbeit mit dem ZIV koordiniert.

3.2 Dienstleistungsvereinbarung mit dem Universitätsklinikum

Zur Darstellung des Umfangs der Leistungen, die vom ZIV für das UKM erbracht werden, und auch um die Qualität dieser Dienstleistungen einvernehmlich zu regeln, wurde im ersten Halbjahr 2009 nach längerem Vorlauf eine Dienstleistungsvereinbarung (auch Service Level Agreement – SLA) erstellt. Deren Strukturierung soll im Weiteren auch für die Erbringung von Dienstleistungen durch das ZIV für andere Bereiche der WWU oder im Wissenschaftsnetz Münster prototypisch sein. Dabei wird insbesondere auf die folgenden Themenfelder eingegangen (Näheres dazu siehe Abschnitt 3.11 *„Störungs- und Risikomanagement, Servicequalität“*):

- Geltungsbereich der Vereinbarung
- Zuständigkeiten
- Störungsmanagement
- Eskalationsmanagement
- Verfügbarkeiten
- Erstattung von Aufwendungen des Leistungserbringers
- Pflichten des Leistungsnehmers
- Abstimmungsprozess zwischen Leistungserbringer und Leistungsnehmer
- Berichtswesen
- Überwachung der Erfüllung der Dienstleistungsvereinbarung
- Änderung der Dienstleistungsvereinbarung

Dabei ist begleitend anzumerken, dass die Sachmittelaufwände für den Ausbau und Betrieb des Kommunikationsnetzwerks direkt durch das UKM getragen werden. Für die dem ZIV durch den Netzbetrieb entstehenden personellen Aufwendungen werden Mitarbeiter des UKM dem ZIV unterstellt und sind dort in der Abteilung 1 organisatorisch integriert.

3.3 Betriebs- und Nutzungsregelungen

Es existieren folgende insbesondere für den Betrieb und die Nutzung des Kommunikationssystems wichtige Ordnungen und Regelungen:

- IV-Versorgungskonzept der WWU Münster
- Das System der Informationsverarbeitung der WWU Münster
- Benutzungsordnung des Zentrums für Informationsverarbeitung und der IV-Versorgungseinheiten der Westfälischen Wilhelms-Universität Münster
- Aufgabenteilung zwischen IV-Versorgungseinheiten und ZIV
- Die/ der Technisch Verantwortliche für vernetzte IV-Systeme
- Ordnung für IT-Administratoren an der Universität Münster
- Regelungen für den Zugang zum Internet für Studierende
- Regelungen zur IV-Sicherheit in der Universität Münster
- Betriebsregelung für das Datennetz der WWU Münster
- Detailregelungen für den Zugang zum Datennetz der WWU
- Ausschließliche Nutzung des IP-Protokolls im Rechnernetz der WWU
- Pauschalpreisregelungen für LAN-Anschlüsse
- Betriebsregelung für die Nutzung der Netzdienste
- Detailregelungen zur Verwendung von Namen im Datennetz der WWU Münster
- Betrieb von E-Mail-Servern im Netz der WWU
- Dienstvereinbarung über die Nutzung der ISDN-TK-Anlage

Darüber hinaus existieren weitere Ordnungen und Regelungen zur Informationsverarbeitung (IV) der WWU, die nicht schwerpunktmäßig das Kommunikationssystem betreffen.

3.4 Unterstützung dezentraler Systeme und Dienste über das Netz

Das Spektrum unterstützter zentraler Systeme und Dienste wurde bereits im Abschnitt 1.5.6 *„Weitere Netzdienste an der WWU“* dargestellt. Ein Arbeitsschwerpunkt der Unterstützung der Netzintegration sowohl zentraler als auch dezentraler Systeme und Dienste ist die Einordnung in die netzseitige Sicherheitsarchitektur (vgl. Abschnitt 1.6.5 *„Konzept der netzseitigen IT-Sicherheitsmaßnahmen“*). Das bedeutet, dass in Zusammenarbeit mit den Systemverantwortlichen die Zuordnung zu einer Netzzone vorgenommen werden muss. Evtl. muss eine neue Netzzone angelegt werden. Die zu implementierenden Sicherheitsfunktionen (z.B. Stateless Packet Screens, Firewall-Funktionalitäten, Intrusion Prevention-Funktionalitäten) müssen festgelegt werden.

Es ist beabsichtigt, im Rahmen der Netzüberwachung Erweiterungen für die Betreiber dezentraler Systeme und Dienste vorzunehmen (vgl. Abschnitt 3.10 *„Netzüberwachung“*).

3.5 Abrechnungspolitik

Auf ein Netznutzungs-Accounting für Abrechnungszwecke wird weitgehend verzichtet. Für die Erstellung von zusätzlichen LAN-Festanschlüssen existiert eine Pauschalpreisregelung. Dabei handelt es sich um eine degressive Preisregelung („Mengenrabatt“), um auf eine Bündelung von Maßnahmen hinzuwirken. Auch für die Installation von WLAN-Access Points gibt es eine Pauschalpreisregelung.

Für die Sprachkommunikation allgemein gibt es bereits eine umfangreiche Billing- and Accounting-Lösung. Den Teilnehmer werden sowohl die privaten als auch die dienstlichen Festnetz-

Gesprächsübersichten und die Mobilfunkgesprächsdaten online zur Verfügung gestellt. Dieses geschieht teilnehmerbezogen. Der Zugang ist personenbezogen geschützt.

3.6 Administration

Als zentrale Servicestelle für alle Aspekte der Netzdokumentation und -administration ist ein NIC (Network Information Center) eingerichtet. Das NIC ist telefonisch, über E-Mail und über das User-Self-Care-Portal *NIC_online* erreichbar.

3.6.1 Netzdokumentation und -administration mit *LANbase*

Als das zentrale Werkzeug für die Netzdokumentation und -administration existiert die auf einer Oracle-Datenbank basierende, langjährige Eigenentwicklung *LANbase*. LANbase wird dabei nicht nur zur Dokumentation, sondern auch für ein breites Spektrum an administrativen Aufgaben verwendet. LANbase ist gekoppelt an das Produkt EMS (Enterprise Management Suite) der Firma 3Com. EMS ist ein Workflow Automation Tool (z.B. für Konfigurations- und Change-Management von Netzkomponenten). Mit LANbase steht eine Fülle von Funktionalitäten einer CMDB (Configuration Management Database) nach ITIL zur Verfügung (vgl. Abb. 22). In LANbase ist u.a. die einheitliche Verwaltung und Administration von netztechnischen Objekten, Systemen und Vorgängen realisiert:

- Gerätedatenbank: einschließlich Verkabelung, Anschlüsse und Rangier-/Verbindungskonfigurationen
- Endsystemdatenbank: Erfassung sämtlicher an das LAN angeschlossenen Endsysteme und Verwaltung von
    - netztechnischen Parametern: IP-Adressen, MAC-Adressen, Erfassung und Konfiguration des Netzanschlusspunkts, ...
    - Verantwortlichkeiten: leitend und technisch Verantwortliche
- vollständig zentrales IP-Adress-Management (IPAM) mit automatischer Provisionierung der Core Network Services DNS, WINS, DHCP, RIS-DHCP
- Verwaltung von Sicherheitsstrukturen (Netzzonen, VLANs)
- zentrale ACL-Verwaltung (Stateless Packet Screens auf IP-Routern) mit automatischer Provisionierung von Cisco-Routern

In Verbindung mit EMS wird LANbase intensiv zur revisionssicheren, rationellen und Fehler vermeidenden Konfiguration von Netzkomponenten verwendet.

Darüber hinaus sind folgende Funktionen realisiert:

- Projektverwaltung
- voll integriertes Trouble-Ticket-System (Eigenentwicklung *NOcase*) mit unmittelbarem Zugriff auf netzrelevante Daten
- Dokumenten-Archiv
- Implementierung des Security-Audit-Tools *ISidoR*

Auszüge aus dem LANbase-Datenbestand stehen mandantenfähig den Systemverantwortlichen in der WWU und dem UKM als User-Self-Care-Anwendung *NIC_online* zur Verfügung (vgl. Abb. 23).

Abb. 22: Einstiegsseite des zentralen Netzadministrationstools LANbase

Anmeldungen / Anträge	2007	2008
Endgeräteanmeldungen	3.346	4.094
Endgeräte-LAN-Anträge (für ein oder mehrere Endgeräte)	1.640	1.695

Tabelle 10: Zahlen zu den neu angemeldeten Endgeräten in den Jahren 2007 und 2008

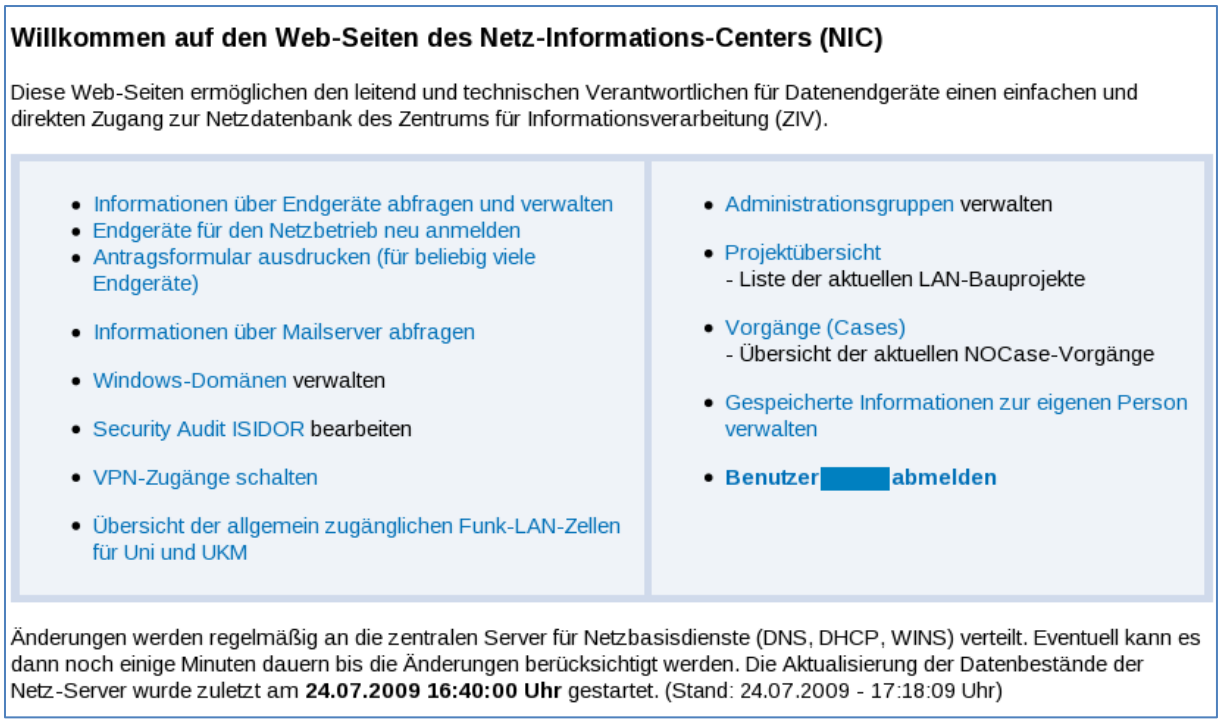


Abb. 23: *Einstiegsseite des User-Self-Care-Portals NIC_online*

3.6.2 Weitere Dokumentationswerkzeuge

Als weiteres Netzdokumentationswerkzeug existiert die auf AutoCad basierende Eigenentwicklung *LANcad*. Mit LANcad werden Grundrisspläne verwaltet und die topografische Dokumentation von Kabeln, Kabeltrassen, Anschlussdosen, etc. durchgeführt. Für LWL-Strukturpläne wird darüber hinaus noch VISIO verwendet.

3.6.3 Planungen im Bereich Administration

Es ist beabsichtigt, die bereits im Bereich Endsystemverwaltung vorhandenen User-Self-Care-Funktionen in LANbase noch deutlich auszubauen. Folgende Funktionen sollen u.a. implementiert werden:

- Vergabe von IP-Adressen durch authorisierte Nutzer
- Switchport-Einstellungen der Netzanschlussdose: z.B. Speed, Duplex-Mode
- Erstanalyse bei Fehlersituationen durch Anzeige von Fehlerinformation des Switch-Ports
- Verwaltung netzseitiger Sicherheitsmaßnahmen: ACL-Verwaltung (Stateless Packet Screens von IP-Routern)

3.6.4 Konzeptdarstellung „Eigenentwicklungen statt Einsatz kommerzieller Produkte“

Die Eigenentwicklungen im Bereich Netzadministration/betrieb (insb. für Workflow-Automatisierung und User-Self-Care-Funktionen) bedeuten einen hohen personellen Aufwand. Jedoch sind kommerzielle Produkte mit einem den Eigenentwicklungen vergleichbaren Funktionsumfang (s.o.) von den Kosten her als extrem kritisch zu beurteilen. Wegen des großen Mengengerüsts der Netze von WWU und UKM liegen die Beschaffungskosten für mandantenfähige CMDB-/Netzadministrations-/Dokumentationstools allein für Teilfunktionen teilweise im sechsstelligen Euro-Bereich wie letztens bei der Untersuchung von Produkten für den Bereich IPAM (IP Address Management) wieder festgestellt werden musste. Darüber hinaus liegen die jährlichen Wartungskosten für derartige Produkte typischerweise bei ca. 20%. Wegen des großen

Funktionsumfangs von LANbase (u.a. auch Trouble Ticket-System) wären für einen LANbase-Ersatz also mehrere Produkte zu beschaffen. Die notwendige bei LANbase bereits vorhandene Integration unter einer einheitlichen Oberfläche wäre dann aber noch zu leisten. Auch für kommerzielle Produkte entsteht ein regelmäßiger Konfigurations-, Pflege-, Wartungs- und Consulting-Aufwand, der entweder selbst zu leisten wäre oder aber zu weiteren Kosten führen würde. Mit Eigenentwicklungen besteht außerdem die Möglichkeit, flexibel auf neue Anforderungen (Kundenwünsche, Vorschriften, Regelungen, Workflows) reagieren zu können. Daher ist beabsichtigt, den Eigenentwicklungsaufwand in diesem Bereich weiter zu betreiben und auf die Beschaffung von entsprechenden Produkten im Rahmen dieses Antrags zu verzichten. Um den Eigenentwicklungsaufwand leisten zu können, ist beabsichtigt, Personalkosten über diesen Antrag zu finanzieren.

3.7 Sicherheit, Datenschutz

Die Sicherheit der Informationsverarbeitung wird an der WWU auf verschiedensten Ebenen sichergestellt. Seit 2002 besteht eine vom Rektorat verabschiedete Regelung zur IV-Sicherheit beruhend auf den Empfehlungen des ARNW (Arbeitskreis der Leiter Wissenschaftlicher Rechenzentren in NRW). Diese Ordnung wird ergänzt durch die IT-Administratorenordnung der WWU, mit der die Anforderungen an die Qualifikation und Rahmenbedingungen der Bestellung von IT-Administratoren für sämtliche IT-Systeme an der WWU festgelegt werden. Insbesondere ist damit bei der Bestellung der IT-Administratoren eine explizite Übertragung von Unternehmerpflichten vorgesehen, mit der auch die Feststellung des Vorliegens der notwendigen Qualifikation sowie eine Belehrung zu den Verantwortlichkeiten eines IT-Administrators bei der Datensicherheit sowie der im Bereich Datenschutz-, Telekommunikations- und IT-Strafrecht zu beachtenden Regelungen einhergehen.

Sämtliche Regelungen und gremialen Beschlüsse zur IT-Sicherheit sind über das Sicherheitsportal der WWU abrufbar.

Im Rahmen eines aus Mitarbeitern des ZIV, der IVVen und des UKM besetzten IT-Sicherheitsteams werden in monatlichen Sitzungen aktuelle Themen der IT-Sicherheit diskutiert und Lösungswege erarbeitet. In diesem Rahmen wird das IT-Sicherheitshandbuch der WWU erstellt.

Aufbauend auf der Netz-Dokumentationsplattform LANbase wurde (wie bereits unter 3.6.1 *„Netzdokumentation und -administration mit LANbase“* beschrieben) mit ISidoR ein Werkzeug zur Durchführung eines Sicherheitsaudits gemäß BSI Grundschutz Richtlinien geschaffen, das es den IT-Administratoren und technisch Verantwortlichen erlaubt, den Schutzbedarf für alle registrierten Endgeräte zu dokumentieren. Bis zum Sommer 2009 konnte ein Erfassungsgrad von ca. 73% der Endgeräte erreicht werden (siehe Abb. 24).

IVV (zurück)	Anzahl DEG	davon erfasst	davon unerfasst	E.-Grad
IVV 01 Geisteswissenschaften	1695	963	732	56,81 %
IVV 02 Wirtschaftswissenschaften	1778	1763	15	99,16 %
IVV 03 Rechtswissenschaften	756	701	55	92,72 %
IVV 04 Naturwissenschaften	3857	2145	1712	55,61 %
IVV 05 Mathematik und Psychologie	1257	1243	14	98,89 %
IVV 06 Geowissenschaften	1203	1150	53	95,59 %
IVV 07 Sozialwissenschaften	1345	1257	88	93,46 %
IVV 08 Medizinische Einrichtungen	7879	3827	4052	48,57 %
IVV 09 Zentrale Universitätsverwaltung	1896	1775	121	93,62 %
IVV 10 Universitäts- und Landesbibliothek	757	727	30	96,04 %
UKM IT-Zentrum	4211	3890	321	92,38 %
ZIV - Zentrum für Informationsverarbeitung	1638	1395	243	85,16 %
außeruniversitäre Einrichtung	310	48	262	15,48 %
Endgeräte ohne spez. Zuordnung	335	118	217	35,22 %
Gesamt	**28917**	**21002**	**7915**	**72,63%**

Abb. 24: *Endgeräte am Datennetz (DEG) von WWU und UKM, aufgeschlüsselt nach den IVVen, UKM und ZIV, dazu der jeweilige Erfassungsgrad beim BSI Grundschutz-konformen IT-Sicherheitsaudit (Stand: August 2009)*

Zur Überprüfung der Umsetzung der Regelungen zur IT-Sicherheit und der Qualität der Dokumentation des Sicherheitsaudits wurde die IV-Kommission durch den IV-Lenkungsausschuss beauftragt, mit Unterstützung des IT-Sicherheitsteams eine Sicherheits-Begehung durchzuführen, welche im Frühjahr 2009 stattfand und zu der gegenwärtig ein Bericht erstellt wird.

In einem anschließend an die Sicherheitsbegehung vom Rektorat versandten Schreiben wurden die Leiterinnen und Leiter sämtlicher Dienststellen der WWU nochmals auf die Regelungen zur IV-Sicherheit und die neue IT-Administratorenordnung hingewiesen.

Die geschilderten organisatorischen Strukturen und Maßnahmen sind eine wichtige Voraussetzung für einen professionellen IT-Betrieb und Umgang mit den Themen IT-Sicherheit und Datenschutz.

Durch die Bereitstellung von Anti-Virus-Software im Rahmen einer Campuslizenz für alle Angehörigen der WWU (auch für die Heimnutzung), durch einen zentralen Email-Virus- und SPAM-Filter, durch Backup-gesicherten hochqualitativen Fileserver-Platz für Mitarbeiter und Studierende sowie durch ein zentrales Archiv- und Backup System wird die Datensicherheit weiter unterstützt.

Wichtigster netztechnischer Bestandteil des Sicherheitskonzeptes sind außerdem die netzseitigen IT-Sicherheitsmaßnahmen (siehe Abschnitt 1.6.5 *„Konzept der netzseitigen IT-Sicherheitsmaßnahmen“*). Durch das Zusammenspiel von stateless Firewalling (ACL), stateful Firewalling und Intrusion Detection und Prevention Systeme wird ein Höchstmaß an netzseitiger Sicherheit für Endgeräte geboten. Diese Maßnahmen werden wie beschrieben im Rahmen der ständig laufenden Netzstrukturierungsmaßnahmen (Definition von *Netzzonen* nach Sicherheitsaspekten) in Abstimmung mit den Nutzern an die Bedürfnisse angepasst und nachjustiert.

Durch die Bereitstellung von Einwahlknoten für 3DES/AES-verschlüsselte VPN-Verbindungen, durch Zugangs-Terminalserver und authentifizierte Web-Portale wird auch extern arbeitenden Nutzern ein abgesicherter Zugang zu den Diensten im Datennetz der WWU geboten.

Im WLAN werden die Verschlüsselungsverfahren WPA und WPA2 eingesetzt.

Für die Administration von Serversystemen werden zur Authentifizierung am ZIV ausschließlich Sicherheits-Tokens verwendet, und auch die IVVen übernehmen vermehrt diese Technik.

Zur Bearbeitung der trotzdem auftretenden IT-Sicherheitsvorfälle unterhält das ZIV ein CERT, das eng mit dem DFN-CERT kooperiert.

VoIP-Sprachverkehr, der über ISG-Baugruppen initiiert wird, kann mittels SRTP (Secure Real-Time Transport Protocol) und TLS (Transport Layer Security) verschlüsselt übertragen werden

Alle wichtigen, für das Kommunikationsnetz relevanten Räume im Bereich der WWU sind verschlossen und lediglich für autorisiertes Personal zugänglich. Die Räume sind mit einbruchhemmenden Türen und Fenstern ausgestattet und teilweise mit Alarmsystemen und elektronischen Zutrittskontrollsystemen versehen. Der Aufbau einer Schließung, die Teil eines neuen Schließkonzeptes an der WWU ist, beinhaltet diese Notwendigkeit. In Gebäuden die neu geschaffen werden oder einer Kernsanierung unterzogen werden, wird vorrangig eine elektronische Schließung (elektronische Zutrittskontrolle) zum Einsatz kommen. Diese Maßnahme ist mit anderen wichtigen technischen Bereichen innerhalb der WWU abgestimmt.

3.8 Betrieb - LAN/Datennetz

3.8.1 Technische Maßnahmen

Die weitgehende Redundanz im Netzdesign ist eine der wichtigsten Maßnahmen zur Sicherstellung eines störungsfreien Netzbetriebs. Darüber hinaus wird für alle wichtigen Netzkomponenten eine eigene Ersatzteilhaltung durchgeführt. In Fällen in denen eine Ersatzteilhaltung aufgrund des Gerätepreises und der Einsatzhäufigkeit unangemessen ist und eine Redundanzschaltung vorhanden ist, wird durch Wartungsverträge ein Hardwaretauch innerhalb 4 Stunden gewährleistet. Damit kann bei einem Geräteausfall schnellstmöglich ein Austausch vorgenommen werden. Die Ersatzgeräte werden außerdem für Testzwecke verwendet. Als wesentliche Betriebswerkzeuge werden eingesetzt:

- Netzwerkdatenbank: Eigenentwicklung LANbase
- Konfigurations- und Änderungsmanagement: 3Com EMS
- Netzüberwachung: CA SPECTRUM
- Trouble Ticket-System: in LANbase integrierte Eigenentwicklung NOCase
- Diverse Test- und Messgeräte, sowie Protokollanalysatoren

3.8.2 Administrative, organisatorische Maßnahmen

Für alle wichtigen Geräte sind Wartungsverträge abgeschlossen. Die Verträge beinhalten einen Geräteaustauschservice („Next Business Day“ oder 4 Stunden) bei Defekt, Hotline-Support und vor Ort-Support bei technischen Problemen und den Zugriff auf die neuesten Softwareversionen für die Geräte.

Als zentrale Einheit für den Betrieb des Datennetzes ist ein Network Operating Center (NOC) eingerichtet. Im NOC sind u.a. folgende Aufgaben angesiedelt:

- Annahme von Störungsmeldungen
- Behebung von Störungen

- Netzüberwachung
- Konfigurationsmanagement
- Änderungsmanagement

Um für den NOC-Service einen möglichst hohen Service-Level gewährleisten zu können, sind eine Reihe von Maßnahmen umgesetzt worden:

- Erreichbarkeit über Telefon, E-Mail, Web-Formular
- Dienstplan für NOC-Präsenzdienst für garantierte Erreichbarkeit während der Service-Zeiten: Mo – Fr, 8:00 – 16:30 Uhr für die Störungsbehebung
- separate Räumlichkeiten für NOC-Präsenzdienst
- außerhalb der o.g. Zeiten doppelte Rufbereitschaft (First- und Second-Level-Support)

Der NOC-Service wird dabei schwerpunktmäßig vom Geschäftsbereich 2 „Betriebsservice“ der Abteilung Kommunikationssysteme erbracht. Um den hohen Service-Level gewährleisten zu können, erfolgt eine geregelte Beteiligung aus den beiden anderen Geschäftsbereichen (vgl. Abschnitt 4 *„Personalsituation“*).

Kundenbereich	2007	2008
Vorgänge insgesamt	5.959	6.160
Vorgänge WWU	46,0%	45,8%
Vorgänge UKM	40,0%	40,4%
ZIV-interne Vorgänge	8,6%	9,5%

Tabelle 11: NOC-Vorgänge (Trouble Tickets) nach Kundenbereich in den Jahren 2007 und 2008

Vorgangsart	2007	2008
Störung	38,0%	33,5%
Änderungswünsche	48,6%	53,1%
Beratung	9,1%	8,5%

Tabelle 12: NOC-Vorgänge (Trouble Tickets) nach Vorgangsart in den Jahren 2007 und 2008

3.9 Betrieb - Telekommunikation, Mobilfunk, Medienservice

Im Bereich der Telekommunikation besteht ein Serviceunterstützungsvertrag. Lediglich im Bedarfsfall wird auf den Support des Herstellers, mit unmittelbarem Zugriff auf die Systemspezialisten, zurückgegriffen. Architektonisch stellt ein Vierfach-Rechnerkonzept, vier CPUs arbeiten parallel, wobei auf 2 x 2 Rechnerbetrieb umgeschaltet werden kann, das Kernstück der TK-Units dar. Ein zentraler Ausfall einer TK-Unit hat in den vergangenen Jahren nicht stattgefunden.

Alle wichtigen zentralen Baugruppen (Netzteil, CPU-Baugruppen, Teilnehmerbaugruppen, etc) sind vorrätig. Die Bevorratung der wenigen notwendigen Baugruppen ist aufgrund der Homogenität der eingesetzten Telekommunikationssysteme eine kostengünstige und effektive Vorgehensweise. Gleiches gilt für den Serviceunterstützungsvertrag.

Als wichtige Aufgaben dieses Bereichs sind zu nennen:

- Annahme von Störungsmeldungen
- Behebung von Störungen
- Konfigurationsmanagement

- Änderungsmanagement
- Bereitstellung von Diensten (Sprach-, Voicemail-, Videokonferenz- und Faxdienste)
- Gebühren- und Abrechnungsmanagement
- Bereitstellung von Mobilkommunikation (DECT / GSM)

Im Bereich des Medienservice sind alle wichtigen Baugruppen ebenfalls vorhanden, so dass im Störungsfall, Ausfall eines Beamers, einer zentralen Mediensteuerung, Mikrofonanlagen etc. unverzüglich ein Austausch vorgenommen werden kann. Wegen des Vorlesungsbetriebes und einer starken Frequentierung der Räume ist eine Reparatur der Geräte vor Ort nicht angemessen.

In beiden Bereichen ist die Erreichbarkeit über Telefon, E-Mail und Formulare gegeben. Im Bereich der Telekommunikation ist die Erreichbarkeit der Kollegen in der Zeit von 7:30 -16:00 Uhr gegeben. Nach 16:00 Uhr besteht eine Rufbereitschaft für die Beseitigung von Störungen. An Sonn- und Feiertagen besteht ebenfalls eine Rufbereitschaft. Im Bereich des Medienservice ist die Erreichbarkeit der Kollegen in der Zeit von 7:30 -16:00 Uhr gegeben. Darüber hinaus wird bei wichtigen Störungen über die Rufbereitschaft der Telekommunikation Hilfe angefordert. Aufgrund der Tatsache, dass eine Fülle von Veranstaltungen medientechnisch betreut wird und daher das technisch versierte Personal im Dienst ist, konnte bisher von einer strengen Regulierung bzw. dem Aufbau eines stringenten Rufbereitschaftsdienstes abgesehen werden.

Der Dienst in der Vermittlung und Auskunft, der ebenfalls Bestandteil der Abteilung Kommunikationssysteme des ZIV ist, ist in einem Schichtdienstmodell organisiert. Dabei sind die verkehrsstarken Zeiträume personell stark besetzt unter Beibehaltung durchgängiger Arbeitszeiten für die Mitarbeiter. Die Dienstzeiten sind werktags von 7:00 – 21:00 Uhr und am Wochenende und feiertags von 10:00 – 17:30 Uhr.

Die Vermittlungs- und Auskunftsdienste, die über den oben genannten Zeitraum hinaus erforderlich sind, werden durch Mitarbeiter an der „Information Ost“ des UKM, bereitgestellt. Die „Information Ost“ des UKM ist 24 Stunden am Tag besetzt.

3.10 Netzüberwachung

Seit Mitte 2008 wird für die Überwachung des Netzes das Produkt CA SPECTRUM eingesetzt. Dabei wurde der komplette Funktionsumfang des Produktes (sog. Premium Suite) aus Haushaltsmitteln beschafft. Es wurde damit das zuvor über einen Zeitraum von ca. 15 Jahren eingesetzte Tivoli NetView abgelöst. Im März 2009 wurde von der SPECTRUM Version 8.1 auf die Version 9.0 umgestellt. Seit Juli 2009 ist die Version 9.1 im Einsatz. Bei den in diesem Antrag verwendeten Darstellungen von real existierenden Netztopologien handelt es sich größtenteils um SPECTRUM-Screenshots.

SPECTRUM wird für die systematische Überwachung sämtlicher IP-basierten Komponenten des Kommunikationsnetzes (ca. 2.300 Geräte) eingesetzt. Das umfasst derzeit die eigentlichen Netzwerkkomponenten (z.B. Router, Switches, Firewall-Module, IPS, ...), Infrastrukturkomponenten (z.B. USVs) und die Netzbetriebsserver (CNS: Core Network Services, z.B. DNS, DHCP). Andere Systeme (z.B. Anwendungsserver des ZIV oder der IVVen) werden im Moment auf Anfrage ebenfalls überwacht.

Folgende Auflistung gibt einen Überblick über den Umfang der bisher realisierten Überwachung. Die Aufstellung umfasst dabei sowohl Funktionen, die SPECTRUM bereits von sich aus überwacht, als auch Funktionen, für die eigens Erweiterungen implementiert werden mussten:

- IP/SNMP-Erreichbarkeit von Geräten
- IP-Erreichbarkeit von virtuellen Routern (VRs)
- sämtliche physikalischen Verbindungen zwischen überwachten Geräten
- Auslastung physikalischer Verbindungen (für sämtliche GE- und 10GE-Verbindungen im Core- und Midrange-Bereich)
- Core Network Services: derzeit DNS-Verfügbarkeit/Performance
- diverse Betriebsparameter von Netzwerkkomponenten (z.B. CPU-Auslastung von IOS-Systemen)
- Betriebsparameter von Netzbetriebsservern (DNS, DHCP, RADIUS, ...)

Aufgrund dieser Überwachung erfolgt eine intelligente Alarmierung, in die auch die von den überwachten Systemen verschickt SNMP-Traps einbezogen werden.

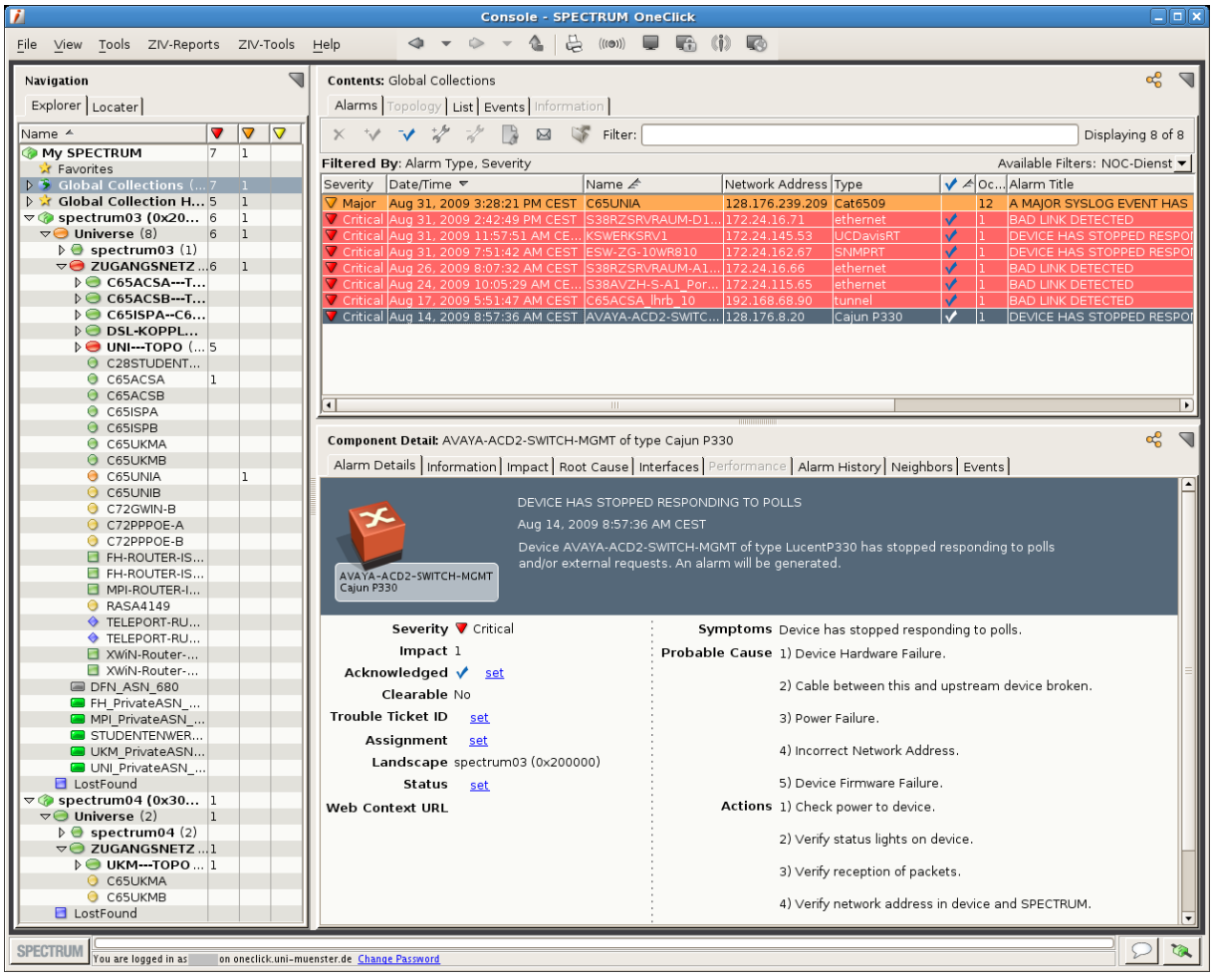


Abb. 25: Screenshot der Konsole des eingesetzten Netzwerkmanagementproduktes CA SPECTRUM. Die in diesem Antrag verwendeten Screenshots mit Netztopologiedarstellungen entstammen größtenteils der SPECTRUM-Installation.

SPECTRUM wird routinemäßig im Rahmen der Betriebsüberwachung durch das NOC eingesetzt. Eine Anbindung an das im NOC eingesetzte Trouble-Ticket-System NOCase wurde realisiert. Die regelmäßige Pflege des in SPECTRUM zu überwachenden Gerätebestandes ist dabei in die internen Betriebsabläufe integriert, um eine zeitnahes Einpflegen von Änderungen im Netz (Neuinstallationen, Deinstallationen) zu gewährleisten. Für einen dauerhaften, effektiven Einsatz von SPECTRUM werden ständig eigene Anpassungen und Erweiterungen vorgenommen. Außerdem werden bei Bedarf externe Support- und Consulting-Dienstleistungen in Anspruch genommen.

Zukünftig sollen die zu überwachenden Technologien stetig erweitern werden (z.B. um HSRP, Routing-Protokolle, Virtualisierung). Außerdem ist geplant, ein umfassendes Netzreporting für die systematische Erfassung von Netznutzungskennzahlen einzuführen, um proaktiv Engpässe zu erkennen und absehbare zukünftige Leistungsanforderungen zu adressieren. In der WWU und am UKM wird damit begonnen, zwischen Fachbereichen, Kliniken und Verwaltungen auf der einen und dem ZIV auf der anderen Seite verbindliche Dienstqualitäten und -quantitäten zu verabreden, um die Verlässlichkeit des Netzbetriebes zu regeln und für den Nutzer transparent zu machen. Daher ist auch ein Kundenportal für den Zugang zu Netzwerküberwachungsinformationen (Service-Überwachung) in der Planung. Viele dieser geplanten Erweiterungen können mit SPECTRUM realisiert werden. Im Bereich Netzreporting (u.a. systematische Erfassung von Netznutzungskennzahlen) reichen die Funktionalitäten von SPECTRUM allerdings nicht aus. Daher ist beabsichtigt, das ebenfalls von der Firma CA stammende Reporting-Werkzeug eHealth, das eine enge Kopplung mit SPECTRUM erlaubt, zu beschaffen.

3.11 Störungs- und Risikomanagement, Servicequalität

Wie bereits unter 3.2 dargestellt, wurde bereits eine Dienstleistungsvereinbarung mit dem UKM abgestimmt, die die bereits seit langem etablierten Umstände bei Ausbau- und Betrieb des Kommunikationsnetzwerks explizit macht und festschreibt. Auf dieser Basis sollen zukünftig auch mit weiteren internen und externen Nutzern der Dienstleistungen des ZIV entsprechende Vereinbarungen getroffen werden.

3.11.1 Risikomanagement

Als lange etablierte Praxis werden die mit geplanten Eingriffen in das Kommunikationsnetz verbundenen Risiken vorab in Besprechungen in geeignetem Rahmen (Mitarbeiter verschiedener betroffener Abteilungen des ZIV, Nutzervertreter, ggf. auch Lieferanten) erörtert und Zeitpläne sowie Rückstiegsszenarien festgelegt.

Speziell für Risikoabschätzungen bei Themen der IT-Sicherheit bildet das IT-Sicherheitsteam der WWU den geeigneten Rahmen.

Durch die intrinsische Ausfallssicherheit des Kommunikationsnetzes werden Risiken minimiert.

Insbesondere im Bereich des UKM wird auf Grund von Risiko-Betrachtungen zum gegenwärtigen Zeitpunkt noch auf den Einsatz der komplexeren und bzgl. der möglichen Fehlerszenarien schwerer abschätzbaren VoIP Technologie verzichtet.

3.11.2 Störungsmanagement und Servicequalität

Wie bereits unter 3.2 dargestellt gliedert sich das Muster für Dienstleistungsvereinbarungen wie folgt:

1. Geltungsbereich der Vereinbarung
2. Zuständigkeiten
3. Störungsmanagement
4. Eskalationsmanagement
5. Verfügbarkeiten
6. Erstattung von Aufwendungen des Leistungserbringers
7. Pflichten des Leistungsnehmers
8. Abstimmungsprozess zwischen Leistungserbringer und Leistungsnehmer
9. Berichtswesen
10. Überwachung der Erfüllung der Dienstleistungsvereinbarung
11. Änderung der Dienstleistungsvereinbarung

Beim Störungsmanagement werden insbesondere Störungs-Levels (Prioritäten 1 bis 4) und Reaktions- bzw. Bearbeitungszeiten während verschiedener Servicezeiten (normale Dienstzeit vs. Nacht/Wochenende) festgelegt. Festlegungen für die Abgabe von Störungsmeldungen und Dokumentation der Störung werden vereinbart sowie verantwortliche Ansprechpartner und Eskalationswege bei Nichterfüllung der Vereinbarung (Details zu den Service-Zeiten des NOC siehe Abschnitt 3.8.2 *„Administrative, organisatorische Maßnahmen“*) benannt.

Zur Überwachung der Verfügbarkeiten (typischerweise 99,0% bis 99,5%) und Ausfallszeiten wird die Datenbasis des Netzwerk-Mangement-Systems CA SPECTRUM genutzt, auf dessen Basis zumindest jährlich Berichte erstellt werden.

3.12 Planungen hinsichtlich Konvergenz von Tele- u. Datenkommunikation

Im Rahmen der Konvergenz von Tele- und Datenkommunikation ist beabsichtigt, in möglichst vielen Bereichen von Administration, Betrieb und Management eine Vereinheitlichung bzgl. Tele- und Datenkommunikation zu realisieren. Im Abschnitt 1.8 *„Konvergenz von Tele- und Datenkommunikation“* sind die ersten in diese Richtung unternommenen Schritte bereits erläutert worden.

4 Personalsituation

Die Abteilung „Kommunikationssysteme“ des ZIV ist in 3 sog. *Geschäftsbereiche* unterteilt. In der folgenden Aufstellung ist in Klammern die Zahl der Mitarbeiter im jeweiligen Geschäftsbereich angegeben. Dabei sind studentische Mitarbeiter und Auszubildende nicht mit berücksichtigt. 5 Mitarbeiter sind wissenschaftlich Angestellte. Unter den Mitarbeitern stehen 7 in einem Beschäftigungsverhältnis mit dem UKM.

- *Abteilungsleitung (1 MA)*
- *Geschäftsbereich 1 „Funktionen und Dienste für Kommunikation und Medien“ (11 MA)*
    - Gruppe 1.1: Netzsicherheits- und Netzsonderfunktionen
    - Gruppe 1.2: Zentrale Netzfunktionen
    - Gruppe 1.3: Informationsmanagement
        - Ein-/Ausgangsabwicklung
        - Betreuung der Auszubildenden (IHK/HWK)
- *Geschäftsbereich 2 „Betriebsservice Kommunikationssysteme“ (12 MA)*
    - Gruppe 2.1: Zentralservice
    - Gruppe 2.2: Peripherieservice
- *Geschäftsbereich 3 „Infrastruktur, Telekommunikation und Medien“ (29 MA)*
    - Gruppe 3.1: Netzinfrastrukturservice
    - Gruppe 3.2: Medienservice
    - Gruppe 3.3: Auskunft und Vermittlung
    - Gruppe 3.4: TK-Systeme

Die Mitarbeiter eines Geschäftsbereichs sind dabei schwerpunktmäßig in dem einem Geschäftsbereich zugeordneten Aufgabenbereich tätig. Die Planung, der Ausbau, der Betrieb und die Weiterentwicklung sind dabei Querschnittsaufgaben, die nicht fest einem Geschäftsbereich zugeordnet sind. Mitarbeiter aus allen Geschäftsbereichen beteiligen sich an diesen Querschnittsaufgaben.

In den letzten Jahren ist der Ausbau des LAN unvermindert fortgeschritten (vgl. Abb. 20 auf Seite 52). Durch Effizienzsteigerungen (u.a. im Bereich Konfiguration-/Change-Management) konnte das LAN mit einer seit 7 Jahren unveränderten Personalausstattung betrieben werden. Allerdings ist es wegen weiter zunehmender Anforderungen an die Funktionalität der Kommunikationsinfrastruktur ebenso weiterhin notwendig, stetig Funktionalitätserweiterungen bei den Netzbetriebswerkzeugen vorzunehmen. Wie zuvor beschrieben sollen durch Weiterentwicklungen an der zentralen Netzwerkdatenbank *LANbase* und der damit zusammenarbeitenden Tools eine weitere Effizienzsteigerung und vermehrt User-Self-Care-Funktionen realisiert werden. Hierfür soll über diesen Antrag eine E13-Stelle für Entwicklungsaufgaben finanziert werden. Auch durch im Rahmen dieses Antrags beantragte, extern erbrachte Planungsleistung für das passive Netz soll die adäquate Umsetzung der beantragten Investitionen unterstützt werden. Es wird erwartet, dass durch die Erschließung von Synergien mit dem fusionierten TK-Bereich weitere Effizienzsteigerungen realisiert werden können.

Insgesamt wird damit davon ausgegangen, dass das beantragte Volumen im geplanten Zeitraum von 7 Jahren tatsächlich mit dem vorhandenen Personalbestand installiert und betrieben werden kann.

5 Tabellenverzeichnis

Tabelle 1: Kenngrößen zur Gebäudesituation von WWU und UKM 11
Tabelle 2: Technologieunabhängige Kennzahlen 11
Tabelle 3: LAN-Kennzahlen (Stichtag: 1.1.2009) 12
Tabelle 4: TK-Kennzahlen 12
Tabelle 5: Kennzahlen zur Nutzungsintensität für das Jahr 2008 13
Tabelle 6: Definition von Bezeichnungen für Netzbereiche 19
Tabelle 7: Grober Überblick über Struktur und Geräte des Netzes der WWU 21
Tabelle 8: Grober Überblick über Struktur und Geräte des Netzes des UKM 23
Tabelle 9: Im Netz von WWU und UKM eingesetzte Gerätetypen 30
Tabelle 10: Zahlen zu den neu angemeldeten Endgeräten in den Jahren 2007 und 2008 61
Tabelle 11: NOC-Vorgänge (Trouble Tickets) nach Kundenbereich in den Jahren 2007 und 2008 66
Tabelle 12: NOC-Vorgänge (Trouble Tickets) nach Vorgangsart in den Jahren 2007 und 2008 66

6 Abbildungsverzeichnis

Abb. 1: Das IV-System der WWU Münster – Entscheidungsgremien und operative Einheiten. 6
Abb. 2: Verteilung der Gebäude von WWU und UKM über das Stadtgebiet vom Münster inkl. der LWL-Verbindungen (hochauflösende Version der Abb. im Anhang) 11
Abb. 3: Über den X-WiN-Anschluss des WNM in 2008 übertragenes Datenvolumen 13
Abb. 4: Auslastung der X-WiN-Hauptleitung des WNM im Mai 2009 14
Abb. 5: Wissenschaftsnetz Münster (WNM) - Die "grünen" Netze werden vom ZIV betrieben. Dargestellt sind die physikalischen Verbindungen (1GE od. 10GE) zwischen Routern. Zwischen WWU und UKM existieren auch direkte Verbindungen für die Realisierung von Layer2-Funktionen (auf beide Netze ausgedehnte VLANs). 15
Abb. 6: Die Struktur des Identitätsmanagementsystems (IdM) der WWU mit den Schnittstellen für den Datenimport sowie für die Provisionierung verschiedenster Zielsysteme. Ein Produkt für die Provisionierung als Ersatz für IBM Tivoli TIM (ITIM) wird derzeit evaluiert. 18
Abb. 7: Struktur des Netzes der WWU - dargestellt sind die physikalischen Verbindungen (10GE oder 1GE-Aggregierung) zwischen Switches. 20
Abb. 8: Kernnetzkomponenten der WWU mit Zuordnung zu Standorten (hochauflösende Version der Abb. im Anhang) 22
Abb. 9: Struktur des Netzes des UKM – dargestellt sind die physikalischen Verbindungen (10GE oder 1GE-Aggregierung) zwischen Switches. Zur Verdeutlichung sind die Switches des WNM-Zugangsnetzes und der Security-Funktionen hier ebenso wie bei der WWU (vgl. Abb. 7) dargestellt. Physikalisch befinden sich diese Switches in der WWU und sind auch der WWU zugeordnet. Die direkte physikalische Anbindung der WLAN-Switches an die Core-Switches an den Hauptstandorten des UKM ist noch nicht realisiert. 23
Abb. 10: Geplante Netzstruktur bzgl. des noch im Aufbau begriffenen Distribution-Bereichs 25
Abb. 11: Exemplarische Realisierung einer Verbindung zwischen Midrange- und Distribution-Switches. Die (einfach oder doppelt angebundenen) Edge-Switches sind nur in zusammengefasster Form dargestellt. Die 3 Distribution-Switches ohne angehängten Edge-Bereich binden einen zentralen Server-Standort an. 25
Abb. 12: Exemplarische Darstellung eines Teils der VR-Struktur. Die grünen Symbole repräsentieren dabei einen virtuellen Router (VR). Zu erkennen sind auch die VR-Paare und die Transfer-VLANs/Sub-netze zwischen den VRs. 27
Abb. 13: Geplante Anbindung von Data Centern 31
Abb. 14: Konzeptdarstellung: Strukturierung in Netzzonen 33
Abb. 15: Konzeptdarstellung: Hierarchie von Netzzonen 34
Abb. 16: Screenshot des Administrationswerkzeugs für Netzzonen („Netzzonenbrowser“) 34
Abb. 17: Virtualisierung: VLANs, virtuelle IP-Router, virtuelle Firewall-Instanzen, virtuelle Intrusion Prevention Systeme, VPN-Einwahl in ein VLAN. Die physikalischen Verbindungen zwischen den Chassis sind hier nicht dargestellt. 37
Abb. 18: Die Abbildung stellt schematisch den gesamten Telekommunikationsanlagenverbund des Hochschulstandortes Münster dar. Die übergeordneten TK-Units sind rot gekennzeichnet, die angeschalteten RPMs sind grün gekennzeichnet (hochauflösende Version der Abb. im Anhang). 44
Abb. 19: Die Abbildung stellt schematisch die Anschaltung von weiteren zentralen Systemen und Verbindungen an den Telekommunikationsanlagenverbund dar. 44
Abb. 20: Entwicklung der netzbezogenen Kennzahlen – in den zurückliegenden 8 Jahren haben sich die Zahlen von Netzanschlüssen und Endgeräten mehr als verdoppelt. Die Zahlen für die im Gelände

des UKM befindlichen Netzanschlüsse sind separat ausgewiesen. Bei den Endgeräten ist eine Trennung nicht klar nach UKM und WWU möglich, da im Bereich des UKM neben den für die Patientenversorgung verwendeten Endgeräten auch die der Medizinischen Fakultät der WWU angebunden sind. 52
Abb. 21: Die Altersverteilung der Edge-Switches zeigt den in den nächsten Jahren akut anstehenden Investitionsbedarf. Ca. 9.000 Ports sind 5 Jahre alt oder älter und müssen dringend mit aktueller Technologie ersetzt werden. 53
Abb. 22: Einstiegsseite des zentralen Netzadministrationstools LANbase 61
Abb. 23: Einstiegsseite des User-Self-Care-Portals NIC_online 62
Abb. 24: Endgeräte am Datennetz (DEG) von WWU und UKM, aufgeschlüsselt nach den IVVen, UKM und ZIV, dazu der jeweilige Erfassungsgrad beim BSI Grundschutz-konformen IT-Sicherheitsaudit (Stand: August 2009) 64
Abb. 25: Screenshot der Konsole des eingesetzten Netzwerkmanagementproduktes CA SPECTRUM. Die in diesem Antrag verwendeten Screenshots mit Netztopologiedarstellungen entstammen größtenteils der SPECTRUM-Installation. 68

7 Abkürzungsverzeichnis

3DES	Triple DES
ACD	Automatic Call Distribution
ACL	Access Control List
AES	Advanced Encryption Standard
AP	(WLAN) Access Point
API	Application Programming Interface
ARNW	Arbeitskreis der Leiter wissenschaftlicher Rechenzentren in NRW
AVM	Audiovisuelle Medien
BGP	Border Gateway Protocol
CERT	Computer Emergency Response Team
CMDB	Configuration Management Database
CNS	Core Network Services
DECT	Digital Enhanced Cordless Telecommunications
DEG	Datenendgerät
DES	Data Encryption Standard
DFN	Deutsches Forschungsnetz
DHCP	Dynamic Host Configuration Protocol
DNS	Domain name System
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DTAG	Deutsche Telekom AG
DWDM	Dense Wavelength Division Multiplex
EGP	Exterior Gateway Protocol
FCoE	Fibre Channel over Ethernet
FH	Fachhochschule Münster
FMC	Fixed Mobile Convergence
GE	Gigabit Ethernet
GLT	Gebäudeleittechnik
GSM	Global System for Mobile Communications
HSRP	Hot Standby Router Protocol
IdM	Identitätsmanagement
IGP	Interior Gateway Protocol
IP	Internet Protocol
IPv6	IP Version 6
IPAM	IP Address Management
IPS	Intrusion Prevention System
IPTV	Internet Protocol Television
ISDN	Integrated Services Digital Network
ISG	In System Gateway
ISidoR	Informations-Sicherheit ist die oberste Regel
IT	Informationstechnik (engl. Information Technology)
ITIL	IT Infrastructure Library
JOIN	Join Open Inter Networks
IV	Informationsverarbeitung
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAN	Metropolitan Area Network
MCU	Multipoint Control Unit

MPLS	Multiprotocol Label Switching
NAC	Network Admission Control
NCS	Core Network Services
NOC	Network Operating Center
NTP	Network Time Protocol
OSPF	Open Shortest Path First
PIM	Protocol Independent Multicast
pLANet	persönlicher LAN- Netzzugang
PMX	Primärmultiplexanschluss
PoE	Power over Ethernet
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PVST	Per-VLAN Spanning Tree
RADIUS	Remote Authentication Dial-In User Service
RPM	Remote Peripheral Module
RSTP	Rapid Spanning Tree Protocol
SIP	Session Initiation Protocol
SoFS	Scale out File Services
SPoF	Single Point of Failure
SSL	Secure Sockets Layer
SRTP	Secure Real-Time Transport Protocol
STP	Spanning Tree Protocol
TAB	Technische Anschlussbedingungen
TDM	Time Division Multiplexing
TK	Telekommunikation
TLS	Transport Layer Security
UKM	Universitätsklinikum Münster
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WINS	Windows Internet Naming Service
WLAN	Wireless Local Area Network
WNM	Wissenschaftsnetz Münster
WWU	Westfälische Wilhelms-Universität Münster
ZIV	Zentrum für Informationsverarbeitung

Anhang: Ausgewählte Abbildungen in hoher Qualität

Einige Abbildungen sind als separate Dokumente in hoher Qualität beigefügt:

Abb. 2: Verteilung der Gebäude von WWU und UKM über das Stadtgebiet vom Münster inkl. der LWL-Verbindungen

Abb. 8: Kernnetzkomponenten der WWU mit Zuordnung zu Standorten

Abb. 18: Schematische Darstellung des TK-Anlagenverbundes des Hochschulstandortes Münster

Abb. 19: Schematische Darstellung der Anschaltung von weiteren zentralen Systemen und Verbindungen an den TK-Anlagenverbund

Westfälische Wilhelms - Universität Münster

ÜberBlick

1 **Schloss (J 8/9)**
Universitätsverwaltung, Hörsäle, Studierendensekretariat, Schlossplatz 2, Auslandsamt, Schlossplatz 2A

2 **Botanischer Garten (I 8/9)**
Schlossgarten 3

3 **Zentrale Studienberatung (K8)**
Schlossplatz 5

4 **AStA (K9)**
Schlossplatz 1

5 **Hörsaalgebäude (L9)**
Hindenburgplatz 10 - 12

6 **Die Brücke (L9/10)**
Internationales Begegnungszentrum der Universität, Wilmergasse 2

7 **Juridicum (M10)**
Rechts- und Wirtschaftswissenschaften, Universitätsstraße 14-16

8 **Universitäts- und Landesbibliothek/ULB (D2)**
Krummer Timpen 3-5

9 **Katholische Theologie (M/N9)**
Johannisstraße 8-10

10 **Geisteswissenschaften (N9)**
Domplatz 23

11 **Fürstenberghaus (N10)**
Geisteswissenschaften, Hörsäle, Domplatz 20-22

12 **Audimax (N10)**
Philologien, Hörsäle, Johannisstraße 12-20

13 **Evangelische Theologie (L10)**
Universitätsstraße 13-17

14 **Georgskommende (M11)**
Erziehungswissenschaft, Philologien, Kommunikationswissenschaft, Sprachenzentrum, Georgskommende 25 - 33, Bispinghof 2 - 14

15 **Mensa I (L13)**
Studentenwerk, Wohnheimverwaltung, Bafög-Amt, Bismarckallee 5/11

16 **Sozialwissenschaften (H/I 16)**
Hörsäle, Aula, Scharnhorststraße 100-121

17 **Hüfferstift (H/I 10)**
Katholische Theologie, Mensa Hüfferstift, Hüfferstraße 27

18 **Geowissenschaften (H10/11)**
Robert-Koch-Straße 26/28

19 **Alte Kliniken, Klinikenverwaltung (F10)**
Domagkstraße

20 **Zentralklinikum (D/E10)**
Albert-Schweitzer-Straße 33

21 **Psychologie (D9)**
Fliednerstraße 21

22 **Hautklinik (C6/7)**
Von-Esmarch-Straße 56
Verwaltung II, Röntgenstraße 17-19

23 **Mensa II (F7/8)**
Domagkstraße 61

24 **Zentrum für Informationsverarbeitung/ZIV (D7)**
Röntgenstraße 9 -13

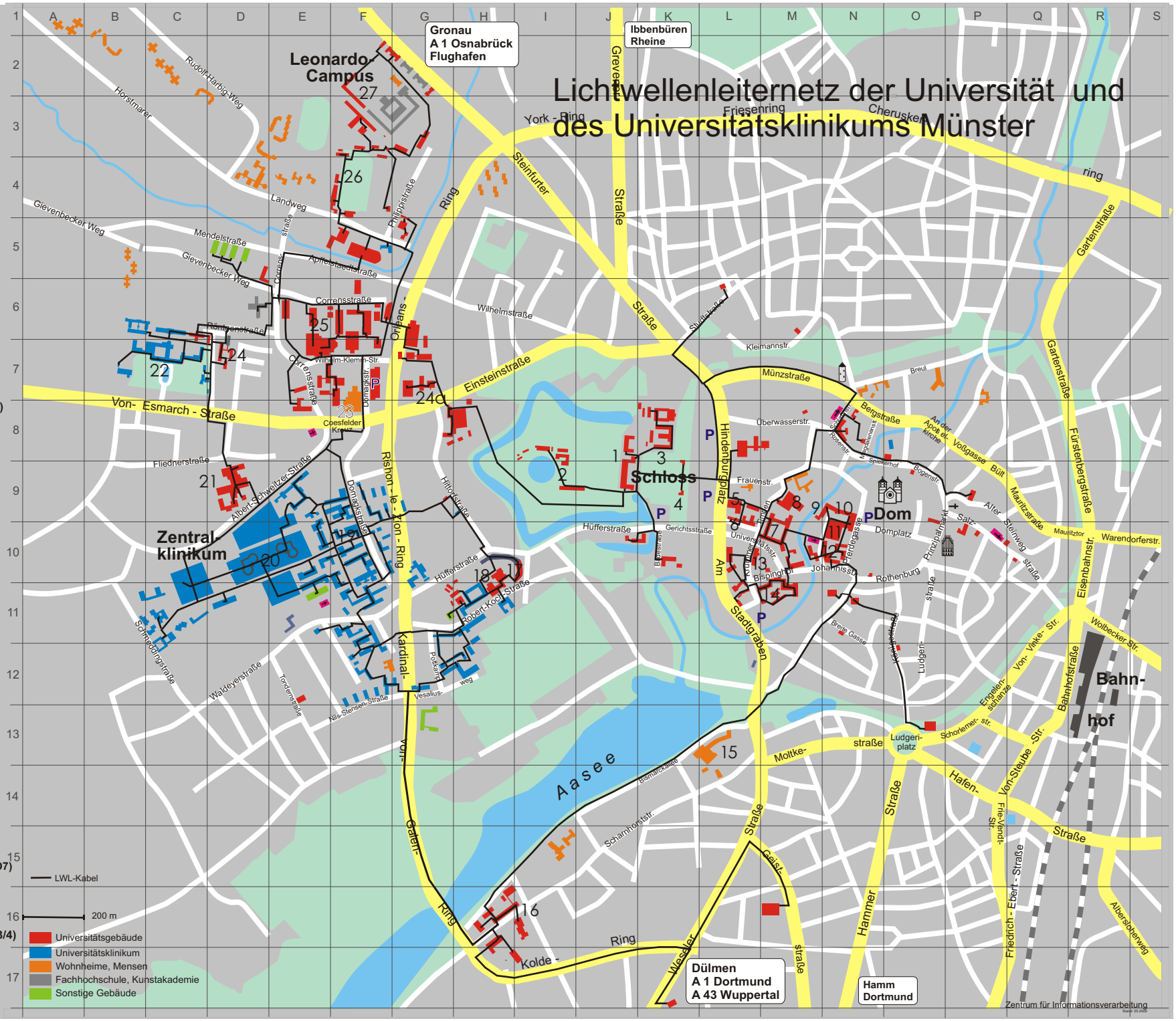
24a **ZIV (G7)**
Einsteinstraße 60

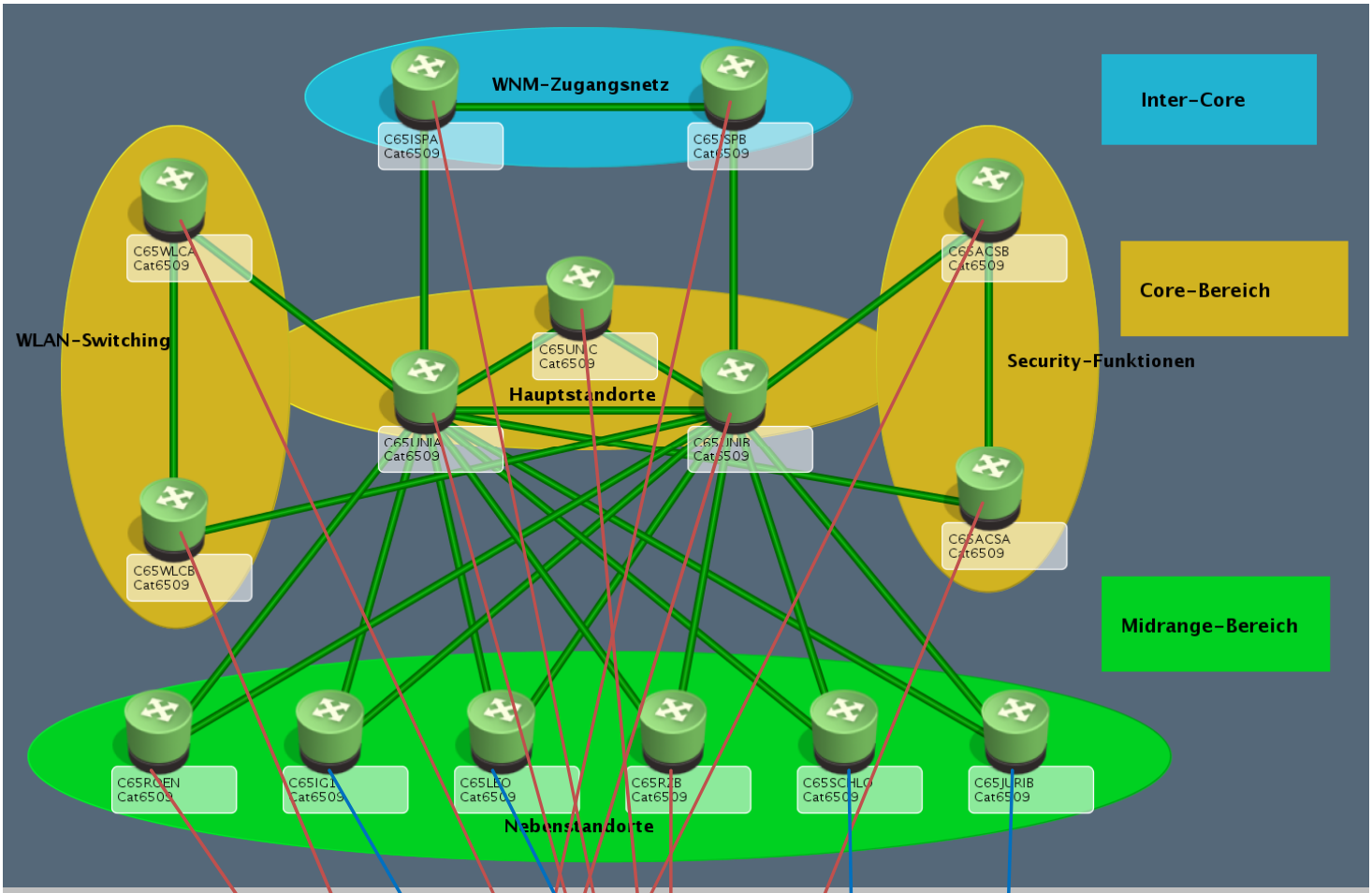
25 **Naturwissenschaftliches Zentrum (E6-F7)**
Wilhelm-Klemm-Straße, Corrensstraße

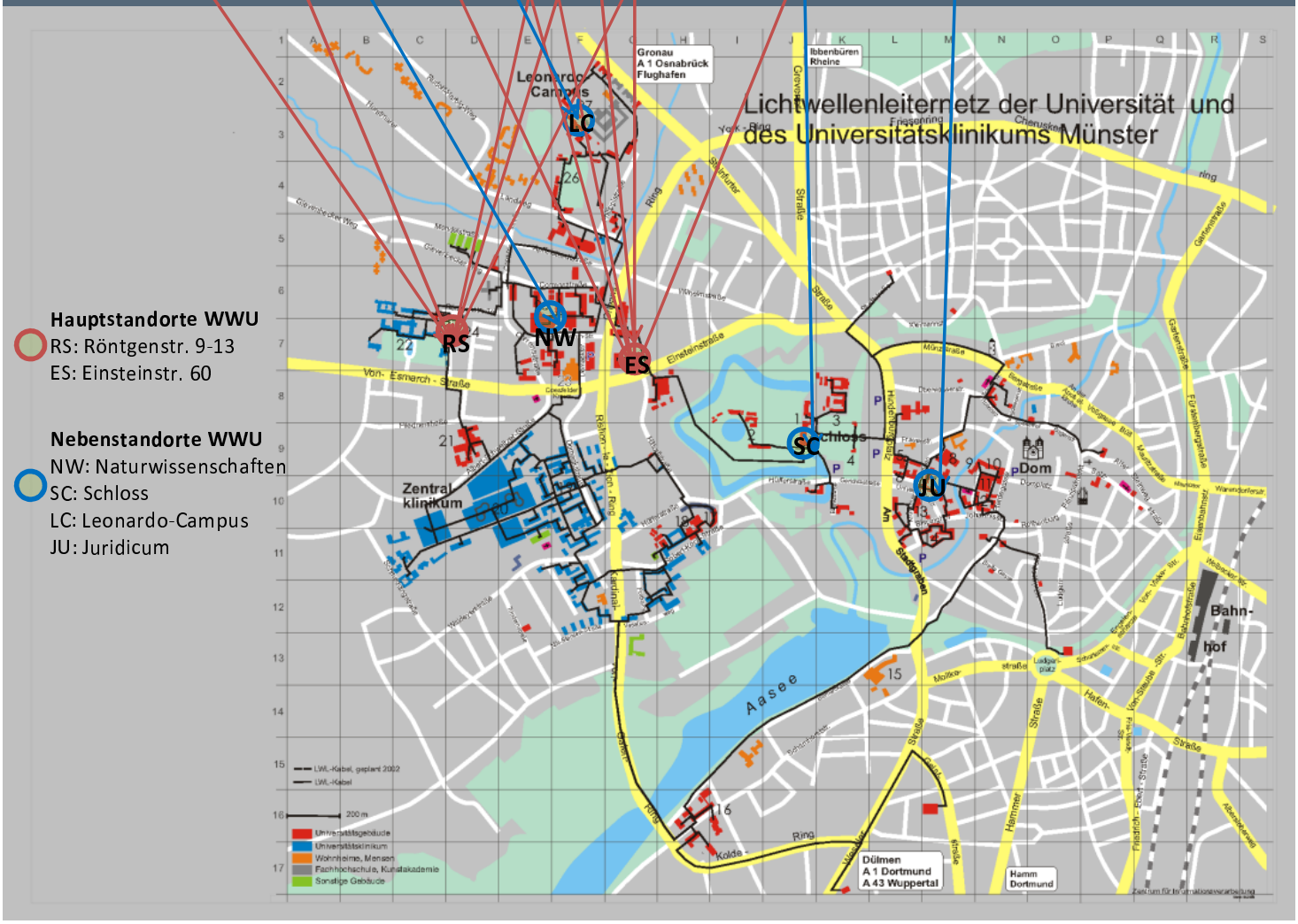
26 **Hochschulsport/HSP, Sportwissenschaft (F3/4)**
Horstmarer Landweg 62

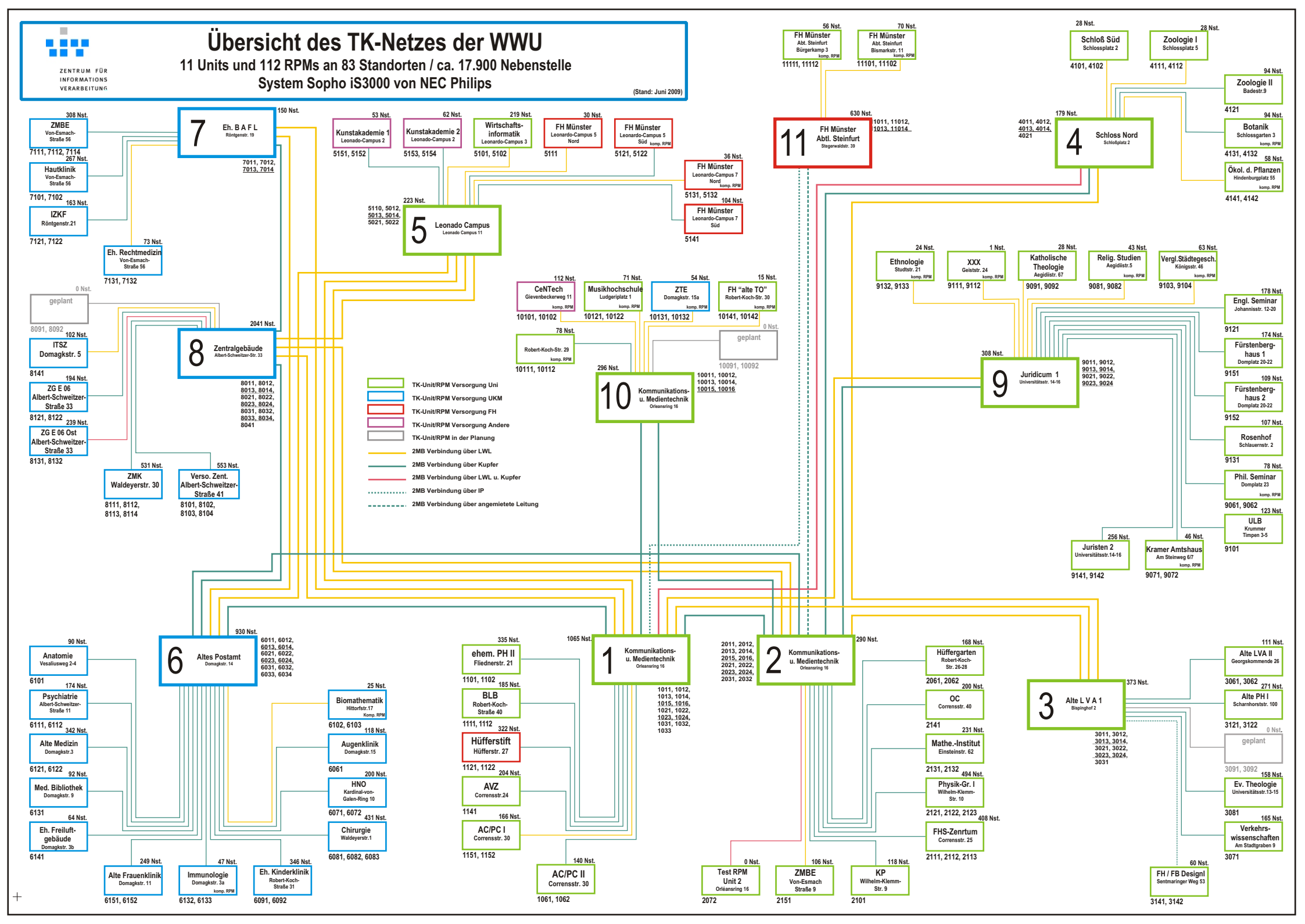
27 **Leonardo - Campus (F2-G3)**
Primarstufe, Universitätsarchiv, Philippistraße17
Wirtschaftsinformatik, Steinfurter Straße 109

Lichtwellenleiternetz der Universität und des Universitätsklinikums Münster




WNM-Zugangsnetz
C65ISPA Cat6509
C65ISPB Cat6509
Inter-Core
C65WLCA Cat6509
C65UNIC Cat6509
C66ACSB Cat6509
Core-Bereich
WLAN-Switching
Hauptstandorte
Security-Funktionen
C65UNIA Cat6509
C65UNIR Cat6509
C65WLCB Cat6509
C66ACSA Cat6509
Midrange-Bereich
C65ROEN Cat6509
C65IGI1 Cat6509
C65LEO Cat6509
C65R3B Cat6509
C65SCHLO Cat6509
C65JURIB Cat6509
Nebenstandorte


Lichtwellenleiternetz der Universität und des Universitätsklinikums Münster
Gronau
A 1 Osnabrück
Flughafen
Ibbenbüren
Rheine
Leonardo Campus
LC
RS
NW
ES
SC
JU
Schloss
Dom
Zentral klinikum
Bahn-hof
Aasee
Dülmen
A 1 Dortmund
A 43 Wuppertal
Hamm
Dortmund
Hauptstandorte WWU
RS: Röntgenstr. 9-13
ES: Einsteinstr. 60
Nebenstandorte WWU
NW: Naturwissenschaften
SC: Schloss
LC: Leonardo-Campus
JU: Juridicum


ZENTRUM FÜR INFORMATIONS VERARBEITUNG
Übersicht des TK-Netzes der WWU
11 Units und 112 RPMs an 83 Standorten / ca. 17.900 Nebenstelle
System Sopho iS3000 von NEC Philips
(Stand: Juni 2009)
7 Eh. B A F L Röntgenstr. 19
150 Nst.
7011, 7012, 7013, 7014
308 Nst. ZMBE Von-Esmach-Straße 56 7111, 7112, 7114
267 Nst. Hautklinik Von-Esmach-Straße 56 7101, 7102
163 Nst. IZKF Röntgenstr.21 7121, 7122
73 Nst. Eh. Rechtmedizin Von-Esmach-Straße 56 7131, 7132
0 Nst. geplant 8091, 8092
102 Nst. ITSZ Domagkstr. 5 8141
194 Nst. ZG E 06 Albert-Schweitzer-Straße 33 8121, 8122
239 Nst. ZG E 06 Ost Albert-Schweitzer-Straße 33 8131, 8132
8 Zentralgebäude Albert-Schweitzer-Str. 33
2041 Nst.
8011, 8012, 8013, 8014, 8021, 8022, 8023, 8024, 8031, 8032, 8033, 8034, 8041
531 Nst. ZMK Waldeyerstr. 30 8111, 8112, 8113, 8114
553 Nst. Verso. Zent. Albert-Schweitzer-Straße 41 8101, 8102, 8103, 8104
5 Leonado Campus Leonado Campus 11
223 Nst.
5110, 5012, 5013, 5014, 5021, 5022
53 Nst. Kunstakademie 1 Leonado-Campus 2 5151, 5152
62 Nst. Kunstakademie 2 Leonado-Campus 2 5153, 5154
219 Nst. Wirtschafts-informatik Leonado-Campus 3 5101, 5102
30 Nst. FH Münster Leonado-Campus 5 Nord 5111
FH Münster Leonado-Campus 5 Süd komp. RPM 5121, 5122
36 Nst. FH Münster Leonado-Campus 7 Nord komp. RPM 5131, 5132
104 Nst. FH Münster Leonado-Campus 7 Süd 5141
11 FH Münster Abtl. Steinfurt Stegerwaldstr. 39
630 Nst.
1011, 11012, 1013, 11014
56 Nst. FH Münster Abt. Steinfurt Bürgerkamp 3 komp. RPM 11111, 11112
70 Nst. FH Münster Abt. Steinfurt Bismarkstr. 11 komp. RPM 11101, 11102
4 Schloss Nord Schloßplatz 2
179 Nst.
4011, 4012, 4013, 4014, 4021
28 Nst. Schloß Süd Schlossplatz 2 4101, 4102
28 Nst. Zoologie I Schlossplatz 5 4111, 4112
94 Nst. Zoologie II Badestr.9 4121
94 Nst. Botanik Schlossgarten 3 komp. RPM 4131, 4132
58 Nst. Ökol. d. Pflanzen Hindenburgplatz 55 komp. RPM 4141, 4142
24 Nst. Ethnologie Studtstr. 21 komp. RPM 9132, 9133
1 Nst. XXX Geiststr. 24 komp. RPM 9111, 9112
28 Nst. Katholische Theologie Aegidiistr. 67 9091, 9092
43 Nst. Relig. Studien Aegidiistr.5 komp. RPM 9081, 9082
63 Nst. Vergl.Städtegesch. Königsstr. 46 komp. RPM 9103, 9104
112 Nst. CeNTech Gievenbeckerweg 11 komp. RPM 10101, 10102
71 Nst. Musikhochschule Ludgeriplatz 1 komp. RPM 10121, 10122
54 Nst. ZTE Domagkstr. 15a komp. RPM 10131, 10132
15 Nst. FH "alte TO" Robert-Koch-Str. 30 komp. RPM 10141, 10142
78 Nst. Robert-Koch-Str. 29 komp. RPM 10111, 10112
0 Nst. geplant 10091, 10092
10 Kommunikations- u. Medientechnik Orleansring 16
296 Nst.
10011, 10012, 10013, 10014, 10015, 10016
9 Juridicum 1 Universitätsstr. 14-16
308 Nst.
9011, 9012, 9013, 9014, 9021, 9022, 9023, 9024
178 Nst. Engl. Seminar Johannisstr. 12-20 9121
174 Nst. Fürstenberg-haus 1 Domplatz 20-22 9151
109 Nst. Fürstenberg-haus 2 Domplatz 20-22 9152
107 Nst. Rosenhof Schlauerstr. 2 9131
78 Nst. Phil. Seminar Domplatz 23 komp. RPM 9061, 9062
123 Nst. ULB Krummer Timpen 3-5 9101
256 Nst. Juristen 2 Universitätsstr.14-16 9141, 9142
46 Nst. Kramer Amtshaus Am Steinweg 6/7 komp. RPM 9071, 9072
TK-Unit/RPM Versorgung Uni
TK-Unit/RPM Versorgung UKM
TK-Unit/RPM Versorgung FH
TK-Unit/RPM Versorgung Andere
TK-Unit/RPM in der Planung
2MB Verbindung über LWL
2MB Verbindung über Kupfer
2MB Verbindung über LWL u. Kupfer
2MB Verbindung über IP
2MB Verbindung über angemietete Leitung
6 Altes Postamt Domagkstr. 14
930 Nst.
6011, 6012, 6013, 6014, 6021, 6022, 6023, 6024, 6031, 6032, 6033, 6034
90 Nst. Anatomie Vesaliusweg 2-4 6101
174 Nst. Psychiatrie Albert-Schweitzer-Straße 11 6111, 6112
342 Nst. Alte Medizin Domagkstr.3 6121, 6122
92 Nst. Med. Bibliothek Domagkstr. 9 6131
64 Nst. Eh. Freiluft-gebäude Domagkstr. 3b 6141
25 Nst. Biomathematik Hittorfstr.17 Komp. RPM 6102, 6103
118 Nst. Augenklinik Domagkstr.15 6061
200 Nst. HNO Kardinal-von-Galen-Ring 10 6071, 6072
431 Nst. Chirurgie Waldeyerstr.1 6081, 6082, 6083
249 Nst. Alte Frauenklinik Domagkstr. 11 6151, 6152
47 Nst. Immunologie Domagkstr. 3a komp. RPM 6132, 6133
346 Nst. Eh. Kinderklinik Robert-Koch-Straße 31 6091, 6092
1 Kommunikations- u. Medientechnik Orleansring 16
1065 Nst.
1011, 1012, 1013, 1014, 1015, 1016, 1021, 1022, 1023, 1024, 1031, 1032, 1033
335 Nst. ehem. PH II Fliednerstr. 21 1101, 1102
185 Nst. BLB Robert-Koch-Straße 40 1111, 1112
322 Nst. Hüfferstift Hüfferstr. 27 1121, 1122
204 Nst. AVZ Corrensstr.24 1141
166 Nst. AC/PC I Corrensstr. 30 1151, 1152
140 Nst. AC/PC II Corrensstr. 30 1061, 1062
2 Kommunikations- u. Medientechnik Orleansring 16
290 Nst.
2011, 2012, 2013, 2014, 2015, 2016, 2021, 2022, 2023, 2024, 2031, 2032
168 Nst. Hüffergarten Robert-Koch-Str. 26-28 2061, 2062
200 Nst. OC Corrensstr. 40 2141
231 Nst. Mathe.-Institut Einsteinstr. 62 2131, 2132
494 Nst. Physik-Gr. I Wilhelm-Klemm-Str. 10 2121, 2122, 2123
408 Nst. FHS-Zenrtum Corrensstr. 25 2111, 2112, 2113
0 Nst. Test RPM Unit 2 Orleansring 16 2072
106 Nst. ZMBE Von-Esmach Straße 9 2151
118 Nst. KP Wilhelm-Klemm-Str. 9 2101
3 Alte L V A 1 Bispinghof 2
373 Nst.
3011, 3012, 3013, 3014, 3021, 3022, 3023, 3024, 3031
111 Nst. Alte LVA II Georgskommende 26 3061, 3062
271 Nst. Alte PH I Scharnhorststr. 100 3121, 3122
0 Nst. geplant 3091, 3092
158 Nst. Ev. Theologie Universitätsstr.13-15 3081
165 Nst. Verkehrs-wissenschaften Am Stadtgraben 9 3071
60 Nst. FH / FB Designl Sentmaringer Weg 53 3141, 3142

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Übersicht des TK-Netzes der WWU-Münster
(Querverbindungen zu anderen Systemen)