Netzentwicklungskonzept für ein großes Universitätsnetzwerk – Bestandspflege und Erschließung neuer Technologien

Dr. Raimund Vogl, Markus Speer, Norbert Gietz, Ludger Elkemann

Zentrum für Informationsverarbeitung
Westfälische Wilhelms-Universität Münster
Röntgenstraße 9 - 13
48149 Münster
rvogl@uni-muenster.de, speer@uni-muenster.de,
gietz@uni-muenster.de, elkeml@uni-muenster.de

Abstract: Die Westfälische Wilhelms-Universität Münster (WWU) ist eine der größten Universitäten in Deutschland und mit ihren über 200 Gebäuden weiträumig über das Stadtgebiet verteilt – ein gut ausgebautes und hoch verfügbares Kommunikationssystem ist folglich von zentraler Bedeutung für die effiziente Unterstützung der Prozesse in Forschung, Lehre und Administration. So hat sich in den zurückliegenden 6 Jahren die Zahl der LAN-Anschlüsse im Netz der WWU auf über 26.500 (mit den Anschlüssen im integrierten Netz des Universitätsklinikums Münster (UKM) sogar über 43.000) mehr als verdoppelt. Mit der Integration des TK/AVM-Bereichs der Universitätsverwaltung in das Zentrum für Informationsverarbeitung (ZIV) Anfang 2008 und dem damit verbundenen Bedarf für die synergetische Umsetzung der Konvergenz der Kommunikationssysteme, mit dem immer rascher anwachsenden Bedarf für 10GE Ports in den Data Centers und der Notwendigkeit für umfangreiche Erneuerungen bei den aktiven Netzwerkkomponenten (im Edge wie auch im Core) war die Erstellung eines neuen, langfristigen Netzentwicklungskonzeptes notwendig. In einem intensiven Diskussionsprozess wurden dabei die Grundlagen für zahlreiche strategische Entscheidungen erarbeitet und die Gesichtspunkte der IT-Sicherheit, eines einfach handhabbaren personalsparenden Netz-Managements und der von Nutzerseite dringend gewünschten mobilen Konnektivität berücksichtigt.

1 Die Ziele des Netzentwicklungskonzeptes der WWU Münster

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 Westfälische Wilhelms-Universität Münster (WWU) 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 der WWU wie auch des Universitätsklinikums Münster (UKM) sind klar geregelt und ausschließlich in der Verantwortung des Zentrums für Informationsverarbeitung (ZIV) der WWU.

Mit der Ausarbeitung eines neuen, langfristigen Netzentwicklungskonzeptes wird zentral das Ziel verfolgt, 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.
- **Effizienz:** Optimierung der User-Helpdesk- und der User-Self-Care-Mechanismen

Dabei wird das Kommunikationssystem in seiner Gesamtheit adressiert – nicht nur das Datennetzwerk, sondern auch die Telekommunikation (TK) und sonstige Netzdienste. Die vorgestellten Konzepte gelten aber genauso für das ebenfalls vom ZIV betreute und voll integrierte Kommunikationssystem des UKM. Die dargestellten Planungen beziehen sich auf einen Zeitraum von ca. 7 Jahren (d.h. bis ca. 2017). Dieser Planungszeitraum wird bewusst gewählt, da dies einem realistischen kompletten Innovationszyklus bei den aktiven Netzwerkkomponenten entspricht, der nur bei dieser Laufzeit mit den verfügbaren internen Personalressourcen bewältigt werden kann.

2 Bedarfsbegründende Grunddaten

Die WWU zählt zu den sehr großen Hochschulen in Deutschland mit Schwerpunkten in den Geistes- und Sozialwissenschaften, den Gesellschaftswissenschaften, den Naturwissenschaften und der Medizin; die Ingenieurwissenschaften sind nicht vertreten. 15 Fachbereiche bilden die organisatorischen Grundeinheiten der WWU. 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. 5.500. Die ca. 5.000 Beschäftigten der WWU setzen sich wie folgt zusammen: 565 Professoren, 2.700 Wissenschaftliche Mitarbeiter, und 1.700 weitere Mitarbeiter. Bei der WWU handelt es sich um eine über die ganze Stadt Münster verteilte Flächenuniversität. Das Kommunikationsnetz der WWU ist daher ein typisches Metropolitan Area Network (MAN). Mit der flächendeckenden Erschließung aller Gebäude über das universitätseigene ca. 230 km umfassende Glasfasernetz ist ein hoher Aufwand verbunden. Das Kommunikationsnetz umfasst LAN-, traditionelle TK-Technologien, und weitere gebäuderelevante Technologien wie Gebäudeleittechnik, Sicherheits- und Zugangstechnik.

Kennzahl	**Wert**
Gebäude	212
Räume	15.340
Gesamtlänge des LWL-Netzes (WWU+UKM)	229 km
registrierte Nutzerkennungen	57.600
LAN-Verteilerstandorte	218
Netz-Anschlussdosen	28.082
WLAN Access Points	732
registrierte LAN-Endsysteme	15.971
Core/Midrange Router/Switches	15
Distribution/Edge-Switches (WWU+UKM)	ca. 2.000
(aktive) TK-Nebenstellen	8.490
TK-Standorte	47
VoIP-Telefone	470

Tabelle 1: Kennzahlen des Kommunikationssystems der WWU

3 Maßnahmenplan für Erneuerung und Ausbau

Der große Umfang des Kommunikationssystems erfordert substantielle Aufwände für die Erhaltung der Infrastruktur (insbesondere proaktiver Austausch der aktiven Komponenten nach maximal 7 Jahren Nutzungszeit zur Gewährleistung der betrieblichen Stabilität und Bereitstellung aktueller Funktionalitäten und Leistungsmerkmale). Trotz des bereits erreichten hohen Abdeckungsgrades ist weiterhin ein ungebrochenes Wachstum des Kommunikationsnetzes mit über 3.000 Neuanschlüssen pro Jahr zu erwarten, das teils aus der forcierten Installation von

WLAN-Access-Points, teils aus der Nutzung von Cat6 für TK-Verkabelung bei allen neuen Bauprojekten resultiert. Für den Zeitraum bis 2017 wird – nicht zuletzt wegen der sukzessiven Migration der TK-Anschlüsse – ein unverändertes Aufkommen an Neuanschlüssen in dieser Größenordnung erwartet.

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 erfolgen dabei kontinuierlich.

Die zentralen Maßnahmen, die zur Erreichung der eingangs genannten Hauptziele umgesetzt werden sollen sind in ihrer zeitlichen Abfolge bereits recht gut umreißbar:

- vollständige Umsetzung des 3-Layer-Core-Schemas (insb. 10GE-Anbindung des Distribution-Layers an den Midrange) und damit einhergehend der Ersatz der Multimode- durch Singlemode-Verkabelung im Laufe der Jahre 2010-2012
- Umstellung auf 40GE-Technologie in Core und Midrange in 2012-2014
- Etablierung von Data Center Switches in 2012
- vollständige Abstützung der audiovisuellen Medientechnik über das LAN und Schaffung einer zentralen Management- und Wartungsplattform bis 2014
- flächendeckende WLAN-Versorgung mit 802.11n bis 2015
- flächendeckende Bereitstellung von 1GE und Einführung von 802.1x bis 2016
- flächendeckende Einführung von VoIP und Ablösung der TDM TK Komponenten bis 2017

Begleitend dazu ist die Pflege und Erweiterung der Funktionalitäten zur Netzwerk-Administration und Dokumentation (zentral und mandantenfähig dezentral), für Netzwerk-Monitoring und für die Netzwerk-Sicherheit geplant.

4 Netzkonzept: vorhandene und angestrebte Netzstruktur

4.1 Grundzüge des Netzdesigns

Das Netzdesign der WWU wird von den Grundsätzen der Verfügbarkeit und der in das Netz eingebetteten Sicherheit bestimmt. Im Rahmen der Verfügbarkeit wird nicht auf eine erhöhte Einzelgeräteverfügbarkeit durch z.B. redundante Module sondern auf eine Doppelung der Geräte und Funktionen an unterschiedlichen Standorten gesetzt. Um sich auch bei der Stromversorgung auf unterschiedliche Quellen abzustützen zu können, werden jeweils 2 Netzteile eingesetzt. Lediglich im Edge wird im Allgemeinen auf diese Redundanzen verzichtet. Durch die ins Netzwerk eingebetteten IT-

Sicherheitsmaßnahmen wird das Gefährdungspotenzial für ganze Netzbereiche erheblich reduziert (vgl. Detaildarstellung unter 4.3). Folgende aufeinander hierarchisch aufbauende Netzbereiche werden unterschieden (siehe auch Abb. 1):

- **Edge:** Anbindung von Endsystemen, nur Layer2-Funktionalität
- **Distribution:** 16 Standorte, Aggregieren von Edge-Devices, nur Layer2-Funktionalität, Einführung dieses Bereiches um kostengünstig 10GE einsetzen zu können, Server-Anbindung
- **Midrange:** 6 Standorte, Aggregieren von Distribution-Devices großer Netzbereiche, zukünftig Anbindung von Data Centern, Layer3/IP-Funktionalität, Paketfiltering
- **Core:** 2 Hauptstandorte, Kopplung der Midrange-Bereiche, Layer3/IP-Funktionalität, Realisierung zentraler Netzfunktionen (WLAN-Switching, zentrale Security-Funktionen: Paketfilter, Firewall-Funktionalität, Intrusion-Prevention, VPN)
- **Inter-Core:** 2 Standorte zur Layer3-Kopplung der Netze der verschiedenen Einrichtungen (WWU, UKM, FH, MPI) zum WNM (Wissenschaftsnetz Münster)

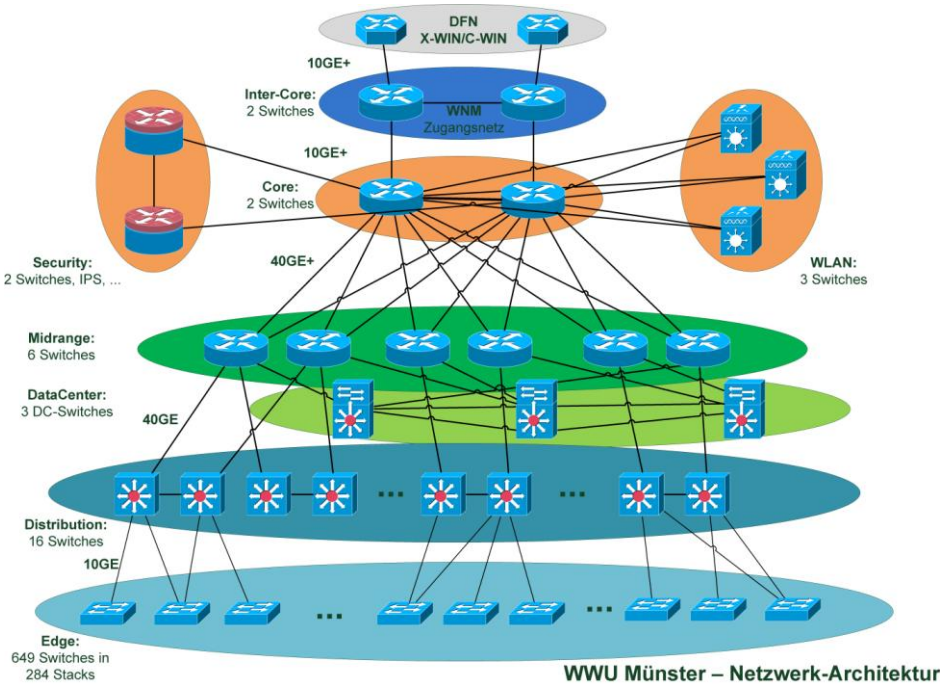

Abb.1: Schematische Darstellung der Architektur mit Core (samt zentraler Security und WLAN Switching) – Midrange (samt Data Center) – Distribution – Edge

Zur Erhöhung der Verfügbarkeit sollen einzelne Edge-Bereiche über ein Paar von Distribution-Switches angebunden werden (siehe Abb. 1). Jeder Edge-Switch wird im Normalfall mit einem der beiden der Distribution-Switches verbunden. Nur ca. 20 % der Edge-Switches mit erhöhten Verfügbarkeitsanforderungen werden mit beiden Distribution-Switches verbunden. Die Distribution-Switches sollen untereinander verbunden und jeweils eine Verbindung zum übergeordneten Midrange-Switch besitzen wodurch dieser Netzbereich redundant angebunden ist. Ein Midrange-Switch hat je eine Verbindung zu einem der Core-Switches. Die Core-Switches sind untereinander verbunden. Die Data Center sollen als Ring untereinander verbunden und jeweils an 2 Midrange-Switches angeschlossen werden.

Das Netz stützt sich auf die 2 Hauptstandorte in der Einsteinstraße und Röntgenstraße ab. An diesen Standorten sind insbesondere die Core- und Inter-Core-, aber auch die lokalen Midrange- und Distributionsfunkionalitäten realisiert. Als Gerätetyp kommt im Inter-Core, Core und Midrange ausschließlich der Cisco C6509 zum Einsatz. Im noch weitgehend zu realisierenden Distribution-Bereich soll hingegen der Gerätetyp HP 5412zl eingesetzt werden. Im Edge kommen aktuell Geräte der Hersteller HP, 3Com und Nexans zum Einsatz. Im Rahmen der internen Herstellerpolitik soll auch zukünftig eine alleinige Herstellerbindung vermieden und der Wettbewerb zwischen den Herstellern aufrechterhalten werden.

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 noch zu leistende umfangreiche Aufgabe. Darüber hinaus müssen die absehbaren Bandbreitenanforderungen durch leistungsfähige Verbindungen (10GE, Nx10GE, später 40GE bzw. 100GE) zwischen den Netzbereichen abgedeckt werden.

4.2 Ausführliche Darstellung der Netzstruktur

4.2.1 Verkabelungsstruktur

Die Verkabelung im Tertiärbereich wurde bereits frühzeitig nach dem Cat5e- und später dem Cat6-Standard ausgeführt. Lediglich die ersten Verkabelungen in den 1990er-Jahren entsprechen nur Cat5, wobei bereits die seinerzeit verwendeten Leitungen den Anforderungen der heutigen Cat5e genügen und durch Umrüsten der Anschlusstechnik leicht gigabit-fähig gemacht werden können. Zur effizienteren Ausnutzung der aktiven Technik und des House-Keepings werden bei der strukturierten Verkabelung möglichst wenige Verteiler innerhalb eines Gebäudes angestrebt. Hierdurch entfällt eine Sekundärverkabelung weitestgehend. Im Primärbereich stützt sich das Netz größtenteils noch auf eine seit den 1980er gewachsenen Multi-Mode-Verkabelung ab. Diese soll durch eine Single-Mode-Verkabelung nach den folgenden Grundsätzen abgelöst werden:

- Im Normalfall wird ein Gebäude mit nur einem LWL-Kabel an einem Distributionsswitch-Standort angebunden

- In Einzelfällen wird für Gebäude mit erhöhten Verfügbarkeitsanforderungen (z.B. Lokationen mit zentralen Services, ...) eine redundante LWL-Anbindung angestrebt.
- Durch die Installation von VoIP-Endgeräten ergeben sich keine erhöhten Verfügbarkeitsanforderungen für die LWL-Anbindung dieses Gebäudes.
- Die beiden Distributionsstandorte eines Netzbereiches werden untereinander verbunden, diese LWL-Verbindung dient auch zum Durchschalten evtl. redundanter Edge-Anbindungen.
- Distributionsstandorte werden mit beiden zugehörigen Midrange-Standorten verbunden
- Midrange-Standorte werden mit beiden Core-Standorten verbunden
- Core-Switch-Standorte werden untereinander verbunden

4.2.2 Layer2-Strukturen

Auf Layer-2-Ebene wird die VLAN-Technologie eingesetzt. Dabei werden die Verbindungen zwischen den Netzwerkkomponenten grundsätzlich „tagged“ und die Verbindungen zu Endsystemen „untagged“ ausgeführt. Lediglich ausgewählte Server werden auch „tagged“ angebunden. Hierdurch ist es möglich die einzelnen VLANs über geografische Bereiche hinweg im gesamten Netz zu verteilen. Im Edge- und Distributionsbereich werden nur Layer-2-Funktionen eingesetzt. Nach Ihrer Funktion werden folgende VLAN-Typen unterschieden:

- Endnutzer-VLANs: Anschluss von Endgeräten (Clients, Server, VoIP-Telefone)
- Insel-VLAN: spezielle Endnutzer-VLANs als abgeschottete Bereiche
- Transfer-VLANs: Verbindung von IP-Routern (physischen und virtuellen)
- VPNSM-VLANs: für die direkte VPN-Einwahl in ein Endnutzer-VLAN

Das Routing auf Layer2 erfolgt mit der STP-Protokollfamilie (Spanning Tree Protocol). Dabei sind zwei voneinander unabhängige STP-Bereiche zu unterscheiden: Im Core/Midrange-Bereich wird Rapid PVST (Per VLAN Spanning Tree), im Distribution/Edge-Bereich wird RSTP (Rapid Spanning Tree Protocol) eingesetzt. 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 der durch zukünftige und den Ausbau vorhandener Dienste (VoIP) weiter steigen wird. Durch das Aufteilen der VLAN-IDs in verschiedene Nummernräume (ID-Range) für einzelne Bereiche und Funktionalitäten (z.B. WWU, UKM, Data Center, Transfernetze) wird die Administrierbarkeit verbessert und die mehrfache unabhängige Verwendung von VLAN-IDs erleichtert.

4.2.3 Layer3-Strukturen

Layer3-Funktionen werden ausschließlich auf den Geräten im Midrange- und Core-Bereich etabliert. Hier lässt sich durch die Cisco-IOS-Funktion „VRF-lite“ die IP-Router-Funktionalität virtualisieren, wodurch eine Vielzahl von IP-Routing-Instanzen (kurz VR) auf einer Hardware definiert werden kann. Die VRs werden dabei sowohl für die Layer3-Anbindung von IP-Subnetzen für Endsysteme als auch für den Aufbau einer Hierarchie von VRs eingesetzt. Im Abschnitt 4.3 wird erläutert, wie hierdurch netzseitig eingebettete Sicherheitslösungen aufgebaut werden können. Auch bei den VRs wird dabei konsequent die Gerätedopplungsstrategie fortgesetzt, indem ein VR-Paar auf zwei Chassis aufgeteilt wird. Derzeit sind ca. 270 VRs (WWU und UKM) realisiert. Zur Erhöhung der Verfügbarkeit kommen HSRP, OSPF und BGP zum Einsatz. Dieses Layer3-Design hat sich in der Vergangenheit bewährt und soll fortgeschrieben werden. IP-Multicast und IPv6 sind noch nicht in substanziellem Umfang eingeführt. Dies soll zukünftig erfolgen.

4.2.4 Netztechnologien und Netzzugangstechnologien

Als Technologie zur Verbindung der Netzkomponenten kommt nahezu ausschließlich Ethernet zum Einsatz. Innerhalb des Core und Midrange wird derzeit ausschließlich 10GE-Technik eingesetzt. Abhängig von der Verfügbarkeit ist mittelfristig eine Hochrüstung auf 40GE-Technik vorzunehmen, alternativ ist hier auch zunächst eine Aggregation von 10GE-Verbindungen möglich. Die konsequente Einführung eines mit 10GE-Technologie angebundenen Distribution-Bereichs ist 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. Hier soll im Laufe der Jahre weitgehend auf 10GE-Technologie umgestellt werden. Vor kurzem wurde eine eigene DSL-Infrastruktur aufgebaut, um einfach und flexibel das vorhandene Kupferkabelnetz nutzen zu können, solange in Einzelfällen noch keine eigene LWL-Anbindung existiert oder diese unwirtschaftlich ist. Zu Standorten ohne eigene Leitungswege wird die DSL-Technik externer Anbieter genutzt.

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

- LAN-Festanschlüsse für registrierte Endsysteme
- „öffentliche“ LAN-Festanschlüsse mit VPN-Zugangsmöglichkeit
- VPN-Zugang aus externen Netzen
- dedizierter VPN-Zugang in eine bestimmte Netzzone (VLAN)
- WLAN (siehe 4.2.5)
- DSL/PPPoE

Der Netzzugang mit 802.1X an LAN-Festanschlüssen ist noch nicht in nennenswertem Umfang realisiert. Es ist geplant, diese Netzzugangstechnologie flächendeckend zu

etablieren. Der Nutzer soll sich dabei flexibel in eine bestimmte Netzzone „einwählen“ können. Hierfür müssen jedoch die älteren Edge-Switches erneuert werden. Beim externen VPN-Zugang soll zukünftig, dort wo die Installation einer VPN-Client-Software nicht akzeptabel ist, eine einfachere SSL-VPN-basierte Zugangsmethode implementiert werden.

4.2.5 WLAN

Derzeit sind zwei verschiedene für den Nutzer transparente WLAN-Installationen im Einsatz. Bei der älteren WLAN-Installation handelt es sich um eine Lösung der Firma Proxim mit autonomen Access Points (APs). Diese Installation ist immer noch in großem Umfang mit ca. 300 APs in Betrieb. Seit 2008 ist eine zentrale controller-basierte WLAN-Switching-Lösung der Firma Cisco, die sich im Core-Bereich auf dedizierte 6509-Switches mit WISM-Modulen abstützt, mit derzeit ca. 450 APs im Einsatz. 802.11n-fähige APs werden erst seit kurzem eingesetzt. Als Authentifizierungsverfahren für den Zugang zum WLAN kommt 802.1X zu Einsatz. Für die Verschlüsselung werden WPA und WPA2 eingesetzt. Für Gäste ist der Netzzugang mit eduroam/DFN-Roaming möglich.

Die WLAN-Versorgung soll noch wesentlich ausgebaut werden. Eine Umfrage unter den Nutzern in 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 (mit final ca. 3.000 APs) zu realisieren. In einigen Bereichen soll die WLAN-Abdeckung auch für VoIP over WLAN und evtl. für Location und Tracking ausgelegt werden. Aus Kostengründen soll von der bisherigen 1:1-Redundanz bei den zentralen WLAN-Switches auf eine 2:1-Redundanz umgestellt werden. Zusätzlich ist die Beschaffung von entsprechender WLAN-Messtechnik begleitend ebenso erforderlich wie die Schaffung von NAT- und Web-Proxy-Lösungen.

4.2.6 Erschließung von Studierendenwohnheimen

Die ca. 20 Studierendenwohnheime in Münster sind an das Glasfasernetz der WWU angeschlossen. Von hier erfolgt ein authentifizierter Zugang in das Netz der WWU. In den einzelnen Wohnheimen liegen unterschiedliche Netzinfrastrukturen vor. Im Falle einer LAN-Verkabelung erfolgt der Zugang mittels VPN-Technologie (PPTP). Bei einer DSL-Infrastruktur wird der Zugang mit PPPoE realisiert. In den ca. 15 Wohnheimen des Studentenwerks Münster existiert eine DSL-Versorgung der T-Systems. In Zusammenarbeit mit dem ZIV (sog. *Teleport-Projekt)* ist hier ein Netzzugang realisiert. Das ZIV betreibt dabei die für die Aggregation und Authentifizierung der Nutzer notwendigen Router.

4.2.7 Data Center

Derzeit existieren an der WWU zwei zentrale Server-Standorte. Es wird von einem Trend zur stärkeren Zentralisierung bei den Servern und dem Server-based Computing

sowie einer Konvergenz von LAN und SAN (Data-Center-Ethernet, FCoE, ...) ausgegangen. Eine Kapazitätserweiterung durch einen dritten Standort ist daher in Planung. Spezielle Data Center Switches mit hoher 10GE-Portdichte werden noch nicht eingesetzt. Zukünftig sollen diese Switches angeschafft und an den Midrange-Bereich angebunden werden. Die Aufteilung der Funktionen auf die Data Center soll so erfolgen, dass das IP-Routing zu den Data Centern auf den Midrange-Switches (d.h. ohne Belastung der Core-Switches) erfolgt. Die Abb. 1 verdeutlicht die Planungen. Die drei Data Center werden wie dargestellt untereinander und an jeweils 2 Midrange-Switches angebunden. Das Redundanzkonzept sieht vor, dass auch im K-Fall Data Center-Services zur Verfügung stehen. Hierfür wird einem Paar von Midrange-Switches ein Data Center für die Layer3-Anindung zugeordnet.

4.3 Konzept der netzseitigen IT-Sicherheitsmaßnahmen

4.3.1 Grundstrukturen für netzseitige Sicherheitsmaßnahmen

Netzseitige Maßnahmen erlauben das Gefährdungspotential für Netzbereiche auch dann zu begrenzen, wenn lokale, organisatorische und sonstige Maßnahmen nicht ausreichend umgesetzt werden konnten. Hierfür erfolgt eine Strukturierung des Netzes in sog. *Netzzonen* (VLANs) für Endsysteme mit identischem Sicherheitsbedarf. Netzzonen sind spezifische Sicherheitsfunktionen zugeordnet. Die Sicherheitsfunktionen sind in das Netz eingebettet; d.h. auf Netzkomponenten realisiert. Durch die Hierarchisierung von Netzzonen können Gesamtheiten von Netzzonen gegenüber anderen Netzzonen sicherheitstechnisch definiert werden. Netzseitig werden folgende Sicherheitsfunktionen eingesetzt:

- Stateless Packet Screening auf Layer-3 (IP-ACLs)
- Firewall-Funktionalität (Stateful Packet Screening)
- Intrusion-Prevention-Systeme (IPS)
- VPN-Technologie (insb. für den Zugang zu einer bestimmten Netzzone)
- Application Gateways oder Application Proxies
- *Bypassing:* Bypassing erlaubt den Einsatz von Sicherheitsfunktionen, wenn Anwendungen hohen Durchsatz erfordern. Beim Bypassing wird mittels Policy Based Routing bestimmter Datenverkehr an den durchsatzbeschränkenden Sicherheitsfunktionen vorbei gelenkt.

4.3.2 Realisierung durch Virtualisierung und mandantenfähige Administration

Netzstrukturen und funktionale Instanzen werden nicht 1:1 physisch bzw. physikalisch auf das Netzinventar abgebildet, sondern weitestgehend in virtualisierter Form realisiert.

- Mit *VLANs* können Netzzonen gebildet werden.

- Durch *Virtualisierung von IP-Routern* können flexibel Netztopologien aufgebaut werden. Zusammen mit der VLAN-Technologie kann im Grundsatz jede beliebige IP-Topologie mit den gewünschten hierarchischen Sicherheitszonen aufgebaut werden.
- Durch die *Virtualisierung von Firewall-* und *Intrusion-Prevention-Funktionalität* können Instanzen solcher Sicherheitselemente an beliebiger Stelle in das Netz eingebettet werden.
- *VPN-Technologie* erlaubt die Ausdehnung einer Netzzone auf externe Sites oder Clients

Im Konzept werden zentrale und dezentrale IT-Verantwortlichkeiten abgebildet. Folgende Funktionalitäten sind daher für eine effiziente Administration der Sicherheitsfunktionen erforderlich:

- *Mandantenfähigkeit* für Einsicht und Konfiguration der Sicherheitsfunktionen durch Netzzonen-Verantwortliche
- *Rahmenkonfigurationsmöglichkeiten und andere Generalfunktionen* für die Vorgabe von Muster-, Standard- und Mindestkonfigurationen

Beim eingesetzten IPS-Produkt sind diese Funktionalitäten gegeben. Für die besprochenen Netzbasisfunktionen VLANs, Virtuelle Router mit den Stateless-Packet-Screening-Funktionen und Virtuelle Firewalls ist die Mandantenfähigkeit bei den eingesetzten Produkten nicht verfügbar. Hier soll die Self-Care-Funktionalität der eigenentwickelten Netzdatenbank (*LANbase*) des ZIV im Rahmen einer Netzzonenverwaltung ausgebaut und mit Geräte-Steuerungsmechanismen verbunden werden.

4.3.3 Planungen bei den netzseitigen IT-Sicherheitsmaßnahmen

Bei den installierten Sicherheitsfunktionen muss zukünftig durchgängig ein Upgrade auf 10GE-Technologie durchgeführt werden. Als zusätzliche Sicherheitsfunktionalität soll eine Content-Filtering/Web-Proxy-Lösung realisiert werden. Der authentifizierte Netzzugang mittels 802.1X soll großflächig zum Einsatz kommen. Im Bereich der Statusüberwachung von Endsystemen (Policy Enforcement, NAC: Network Admission Control) gibt es derzeit noch keine Realisierung. Es ist beabsichtigt, auch diese Funktionalität zukünftig zu implementieren.

4.3.4 Organisatorische Maßnahmen im Rahmen der Netzsicherheit

Die Erarbeitung von Netzstrukturierungs-Konzepten (Definition von Netzzonen) durch das ZIV gemeinsam mit den Nutzern ist ein wesentlicher organisatorischer Bestandteil der Netzsicherheit. Mit Hilfe des selbst entwickelten Werkzeugs ISidoR wurde ein Sicherheitsaudit gemäß BSI Grundschutz Richtlinien durchgeführt. Die Anfang 2009

durchgeführte Sicherheitsbegehung hatte wichtige Impulse gegeben und soll auch zukünftig in regelmäßigen Abständen wiederholt werden.

4.4 House-Keeping: USV-Versorgung, Klimatisierung

USV-Anlagen sind primär an Standorten eingesetzt, die eine strukturelle Bedeutung für das Netz haben. Es existieren drei große USV-Anlagen an zwei Hauptnetzstandorten und einem Serverstandort. Für die Standorte existiert jeweils eine Netzersatzanlage (NEA, Dieselpufferung). An einigen Midrange-Standorten existieren USV-Versorgungen, die erneuert werden müssen. An Standorten, an denen ein Stromausfall nur lokale Auswirkungen hat, ist in der Regel keine USV-Absicherung realisiert. Bei VoIP-Installationen in Gebäuden wird eine USV-Versorgung nicht in jedem Fall realisiert. Angestrebt wird, zumindest den Midrange- und Distribution-Bereich vollständig mit einer USV-Versorgung zu versehen. Weitere USV-Versorgungen einzelner Bereiche unterliegen einer Einzelfallentscheidung. Ein USV-Versorgungsgrad von ca. 30% wird angestrebt. Die Spannungsversorgung für VoIP-Telefone und WLAN-Access-Points erfolgt über Power over Ethernet (PoE). Die obigen Ausführungen zur USV-Versorgung gelten im Grundsatz auch für die Klimatisierung der LAN-Verteilerräume.

4.5 Mediennetze, AVM (Audiovisuelle Medien)

Alle installierten medientechnischen Anlagen sind mit LAN Anschlüssen ausgestattet worden. Somit ist gewährleistet, dass die zukünftige Vernetzung der medientechnischen Anlagen über das LAN möglich ist. Zentraler Zugriff auf die Anlagen (mittels eines aufzusetzenden Managementsystems) erlaubt die Überprüfung der Funktionen und der Verfügbarkeit der Anlagen. 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.

4.6 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. 6.1) vollständig zentralisiert. In LANbase sind u.a. umfassende IPAM-Funktionen (Internet Protocol Address Management) realisiert. Über eine Webschnittstelle (sog. *NIC_Online*) 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 auf einer nicht virtualisierten Serverplattform betrieben. Dabei kommen Linux als Betriebssystemplattform und Open Source Software zum Einsatz. Da die CNSs (insb. der DNS-Service) für den Netzbetrieb von herausragender Bedeutung sind, soll eine eigene umfassende Überwachung (Verfügbarkeit, Datenaktualität, Datenkonsistenz) für der CNSs realisiert werden.

5 Konvergenz von Tele- und Datenkommunikation

5.1 Darstellung der TK-Infrastruktur

Der TK-Anlagenverbund besteht aus Sopho iS3000 Systemen des Hersteller NEC. 19 Primärmultiplexanschlüsse (PRI) an 6 Standorten und ein VoIP-Zugang über das DFN (X-WIN Anschluss) sind als Anschaltungen an das öffentliche Netz realisiert. Eine verstärkte Nutzung des X-WIN Anschlusses für VoIP ist geplant. Die hierfür erforderliche Absicherung durch einen redundanten X-WIN-Anschluss ist gegeben. Die Anzahl der PRI-Anschlüsse soll dadurch halbiert werden, was zu einer deutlichen Kostenreduzierung führt. Vertragspartner ist in beiden Fällen der DFN-Verein.

5.2 Personal

Anfang des Jahres 2008 wurde die Konvergenz von Tele- und Datenkommunikation an der WWU organisatorisch vollzogen. Der Bereich *Kommunikations- und Medientechnik* der Universitätsverwaltung wurde in das ZIV integriert (hausinterne Bezeichnung: *Fusion*). Die betroffenen Mitarbeiterinnen und Mitarbeiter sind zusammen mit Ihren Aufgaben, u.a. Bereitstellung von Telekommunikations- und Vermittlungs- und Auskunftsdiensten am Hochschulstandort Münster, sowie Bereitstellung von audiovisueller Medientechnik für die WWU, nun in der Abteilung Kommunikationssysteme des ZIV angesiedelt.

5.3 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 Bestandteil des gemeinsamen Kommunikationsnetzes geworden und stellt eine beträchtliche Ressource dar. Der Einsatz von DSL-Technologie stellt eine Komplettierung der Datenübertragungstechnik des ZIV dar und schützt die bereits getätigten Investitionen in das Kupferkabelnetz der WWU. Die Netzdatenbank *LANbase* und das Trouble-Ticket-System (Eigenentwicklung *NOCase*) werden inzwischen gemeinschaftlich genutzt.

5.4 Planung der VoIP-Migration

An der WWU werden ca. 8.500 konventionelle Telefone betrieben, sodass die Migration zu VoIP in mehreren Schritten erfolgt. Die Serviceunterstützung der TK-Anlage ist durch den Hersteller bis 2017 gesichert. Dieser Zeitpunkt wird an der WWU für die vollständige Migration nach VoIP angestrebt. Der TK-Anlagenverbund wurde frühzeitig um VoIP-Technologie, nach SIP Standard der IETF, ergänzt. Diese frühzeitige Entscheidung stellt einen substantiellen Investitionsschutz dar. Alle wichtigen Leistungsmerkmale können in der gemischten Systemumgebung realisiert werden. Die Anschaltung weiterer Serverapplikationen an den Verbund geschieht unter der Maxime, dass offene Schnittstellen und standardisierte Protokolle vorrangig berücksichtigt werden. SIP-Standard konforme Endgeräte können prinzipiell unterstützt werden, was einen hohen Freiheitsgrad bei der Beschaffung und der Marktbeobachtung bedeutet, wobei jedoch aufgrund der Logistik, der notwendigen Vorhaltung von Endgeräten, sowie insbesondere der Unterstützung von Leistungsmerkmalen, die über den SIP Standard hinausgehen, vorrangig Endgeräte des Hersteller Polycom eingesetzt werden. Zusammen mit der VoIP-Migration soll in 2011 eine flächendeckende Bereitstellung von Unified Communications-Services realisiert sein.

Die Migrationsstrategie sieht vor, dass bei Neubauten oder Sanierungen VoIP als Technik eingeführt wird. Bei einer Teilsanierung wird möglichst auch eine VoIP-Umstellung der nicht sanierten Bereiche realisiert. LAN-Netzkomponenten sollen über redundante Netzteile, Priorisierungsmöglichkeiten und PoE-Funktionalität für die Versorgung der Telefone verfügen. Die Anbindung der VoIP-Telefone an die TK-Units erfolgt mittels des SIP-Protokolls über ISG-Baugruppen (In System Gateway). VoIP-Telefone werden dabei wie fest angeschlossene, registrierte Rechner betrieben. 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.

6 Betriebs- und Managementkonzept

6.1 Administration, Dokumentation

Als zentrale Servicestelle für alle Aspekte der Netzdokumentation und -administration ist ein NIC (Network Information Center) eingerichtet. Das Hauptwerkzeug für die Netzdokumentation und -administration ist 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. In LANbase ist u.a. die einheitliche Verwaltung und Administration einer

Vielzahl von netztechnischen Objekten, Systemen und Vorgängen realisiert. Auszüge aus dem LANbase-Datenbestand stehen mandantenfähig den Systemverantwortlichen der WWU als User-Self-Care-Portal *NIC_online* zur Verfügung.

Mit steigender Ausdehnung und Komplexität des Netzwerkes werden elaborierte Werkzeuge zum Betrieb immer wichtiger. Da eine zu LANbase funktional vergleichbare kommerzielle Lösung nicht bekannt ist, wird die bewährte Weiterwicklung an *LANbase* als effektive und kosteneffiziente Notwendigkeit gesehen. Es sollen hierbei insbesondere die bereits eingeführten mandantenfähigen User-Self-Care-Funktionen noch weiter ausgebaut werden.

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.

6.2 Betrieb

Die weitgehende Redundanz im Netzdesign ist eine der wichtigsten Maßnahmen zur Sicherstellung eines störungsfreien Netzbetriebs. Für alle wichtigen Geräte bestehen Wartungsverträge, die einen Geräteaustauschservice („Next Business Day“ oder 4h) bei Defekt, Hotline-Support und vor Ort-Support bei technischen Problemen und den Zugriff auf die neuesten Softwareversionen für die Geräte beinhalten. Darüber hinaus wird für alle wichtigen Netzkomponenten eine eigene Ersatzteilhaltung durchgeführt. In Fällen in denen eine Ersatzteilhaltung aufgrund der Kosten unangemessen 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:

- LANbase (CMDB, siehe 6.1)
- Konfigurations- und Änderungsmanagement: 3Com EMS
- Netzüberwachung: CA SPECTRUM
- Trouble Ticket-System: in LANbase integrierte Eigenentwicklung NOCase
- Diverse Test- und Messgeräte, sowie Protokollanalysatoren

Als zentrale Einheit für den Betrieb des Datennetzes ist ein Network Operating Center (NOC) eingerichtet, in dem u.a. folgende Aufgaben angesiedelt sind: Annahme von Störungsmeldungen, Netzüberwachung und Entstörung, Konfigurations- und Änderungsmanagement. Um für den NOC-Service einen möglichst hohen Service-Level zu gewährleisten, sind eine Reihe von Maßnahmen umgesetzt worden:

- Erreichbarkeit über Telefon-Hotline, E-Mail, Web-Formular

- Personelle Zuordnung per Dienstplan für einen Präsenzdienst mit garantierter Erreichbarkeit während der Service-Zeiten: Mo – Fr, 8:00 – 16:30 Uhr für die Störungsbehebung
- separate Räumlichkeiten für Präsenzdienst
- außerhalb der o.g. Zeiten doppelte Rufbereitschaft (First- und Second-Level-Support)

Im Jahr 2009 wurden hier 6.327 Trouble Tickets (WWU und UKM) bearbeitet. Dabei handelte es sich zu 33,2% um Störungen, zu 54,2% um Änderungswünsche und zu 6,3% um Beratungsfälle.

Im TK-Bereich besteht ein Serviceunterstützungsvertrag, über den im Bedarfsfall Zugriff auf den Support des Herstellers besteht. In den Bereichen TK und AVM ist die Erreichbarkeit über Telefon-Hotline, E-Mail und Online-Formulare werktags in der Zeit von 7:30-16:00 Uhr gegeben. Außerhalb dieser Zeiten besteht eine Rufbereitschaft für die Beseitigung von Störungen über die TK-Mitarbeiter. Für das Management der TK-Infrastruktur (inkl. VoIP) soll eine Lösung mit umfangreichen User-Self-Care-Funktionen implementiert werden.

6.3 Netzüberwachung

Für die Überwachung sämtlicher IP-basierten Komponenten des Kommunikationsnetzes wird das Produkt CA SPECTRUM eingesetzt. Dies umfasst derzeit die eigentlichen Netzwerkkomponenten (z.B. Router, Switches, ...), Infrastrukturkomponenten (z.B. USVs) und die CNS-Server. SPECTRUM wird routinemäßig im Rahmen der Betriebsüberwachung durch das NOC genutzt. Eine Anbindung an das eingesetzte Trouble-Ticket-System NOCase ist realisiert. Um ein zeitnahes Einpflegen von Änderungen im Netz zu gewährleisten ist die regelmäßige Pflege des mit SPECTRUM zu überwachenden Gerätebestandes in die internen Betriebsabläufe integriert. Die zu überwachenden Technologien sollen stetig erweitern werden (z.B. Routing-Protokolle, Virtualisierung). Außerdem ist ein umfassendes Netzreporting für ein effektives proaktives Ressourcenmanagement geplant. Im ZIV wird begonnen mit den nutzenden Einrichtungen (UKM, Fachbereiche, Verwaltung) verbindliche Dienstqualitäten und -quantitäten zu verabreden und somit 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.