Hochverfügbarkeitsdesign für das Datennetz eines Universitätsklinikums unter Gesichtspunkten der Anforderungen klinischer IT-Systeme

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

Zentrum für Informationsverarbeitung
Westfälische Wilhelms-Universität Münster
Röntgenstraße 7 - 13
48149 Münster
rvogl@uni-muenster.de, gietz@uni-muenster.de,
speer@uni-muenster.de, elkeml@uni-muenster.de

Abstract: Das Zentrum für Informationsverarbeitung (ZIV) der Westfälischen Wilhelms-Universität Münster (WWU) betreibt das Kommunikationssystem (Datennetz und Telekommunikation) sowohl der WWU wie auch des Universitätsklinikums Münster (UKM). Dabei wird auf einheitliche technische Standards und Konzepte für die insgesamt ca. 50.000 Netzanschlüsse, von denen ca. 20.000 im Bereich des UKM liegen, gesetzt. Obwohl schon der Netzbetrieb für Forschung und Lehre hohe Anforderungen an die Verfügbarkeit stellt, die auch beim Netzdesign berücksichtigt wurden, stellt der Betrieb in der Krankenversorgung, insbesondere mit zunehmender Verbreitung der elektronischen Krankengeschichte, noch wesentlich weitergehende Anforderungen. Auf Basis betrieblicher Erfahrungen, die speziell die Notwendigkeit für die lokale Eindämmung von Netzstörungen sehr deutlich machen, wurde für die Steigerung der Datennetzverfügbarkeit speziell im Kontext der Einführung der mobilen Visite ein Konzept für die resiliente Layer-3 Entkopplung der DataCenter vom LAN-Core bei gleichzeitig direkter DataCenter-Anbindung einer gesonderten Netzverteilinfrastruktur, die eine besonders robuste Anbindung für selektierte, speziell konfigurierte klinische Arbeitsplätze bieten soll, geschaffen.

1 Die Struktur des Datennetzwerks der WWU und des UKM

Als im Jahr 2000 die Medizinischen Einrichtungen der WWU Münster als UKM zu einer eigenständigen Anstalt wurden, war dies bereits umfänglich mit LAN erschlossen und netztechnisch eng mit dem Netz der Universität verbunden. Insbesondere zentrale Netzfunktionen, Internet-Anschluss, Dokumentation und Betrieb wurden gemeinsam durch das ZIV bereitgestellt. Aus diesem Grunde blieb die Verantwortung für den Netzbetrieb auch des UKM beim ZIV als Dienstleister. Die Konzepte und Standards für das Datennetz, die im Rahmen eines DFG-LAN-Ausbauantrages in 2010 für die Periode 2011-2017 [Ant10, Vog10] neu festgeschrieben wurden, finden auch für das UKM Anwendung.

Die etablierten Eckpunkte des Netzkonzeptes für WWU und UKM können wie folgt zusammengefasst werden:

Performance: Die weit im Stadtgebiet verteilten Liegenschaften von WWU und UKM werden mit einem leistungsfähigen Dark-Fiber-Backbone (insgesamt 250km im Stadtgebiet Münster) mit überwiegend 10GE-Technologie verbunden. Aus Redundanzgründen wird eine Doppel-Stern Topologie (siehe Abb.1) jeweils für WWU und UKM verwendet. Diese getrennten Topologien sind über das für die Vernetzung des gesamten Wissenschaftsstandort Münster aufgebaute WNM (Wissenschaftsnetz Münster, bindet auch FH, MPI, Kunstakademie und das Studentenwerk ein) auf Layer-3 verbunden. Die aktiven Komponenten im Netz des UKM sind in die Schichten Core (Layer-3), Distribution und Access (Layer-2) gegliedert (vgl. Abb.1). Die Verbindungen zwischen den 3 Schichten sind weitgehend in 10 GE realisiert (Reste in 1 GE), die Endgeräteanbindung ist historisch gewachsen (1 GE, 100 MBit/s und in Resten noch 10 MBit/s).

Sicherheit: Für die feingranulare Realisierung von Netzsicherheitszonen und Zugangskontrolle sind an WWU und UKM zusammen ca. 1.000 Endnutzer-VLANs in Betrieb. Damit werden insbesondere auch die parallel abzudeckenden Sicherheits- bzw. Zugangsanforderungen für Forschung und Lehre einerseits und Krankenversorgung andererseits adressiert. Die Layer-3-Funktionalitäten werden durch umfangreichen Einsatz des Cisco IOS-Features VRF-lite (ca. 230 virtuelle Routing-Instanzen) realisiert. Auch die Sicherheitsfunktionen (stateful Firewalling, IPS, VPN) werden virtualisiert in den Netzzonen abgebildet (vgl. [Ant10]). Dabei werden die virtualisierten Sicherheitsfunktionen für WWU und UKM zentral an zwei Netzknoten realisiert. Mit Hilfe des darauf aufsetzenden organisatorischen Netzzonen-Konzeptes lassen sich abgestuft Netzzonen mit an die Nutzungssituation genau angepassten Sicherheitseinstellungen definieren – diese werden vom ZIV gemeinsam mit den Nutzern erarbeitet und reichen von komplett abgeschotteten VLANs für medizinische Spezialsysteme bis zu Bereichen für Forschung&Lehre ohne Einschränkungen des Internetzugangs (abgesehen von den obligatorisch zwischengeschalteten IPS Systemen).

Verfügbarkeit: Es wird primär auf Geräte-Dopplung (an zwei getrennten Standorten, mit getrennt geführten Kabelwegen) und nicht auf intrinsische Redundanz in den Geräten gesetzt. Für Redundanzfunktionen auf Layer-2 wird derzeit noch Spanning Tree in verschiedenen Varianten (RSTP und PVST+) sowie auf Layer-3 HSRP und OSPF eingesetzt.

Management und Dokumentation: Ein im Hause entwickeltes, integriertes Datenbank- und Anwendungssystem wird für Konfigurationsverwaltung, Workflow-Automatisierung, Case Management, LAN-Dokumentation und Bauprojektabwicklung (LAN-Base) eingesetzt. Die Netzüberwachung wird mit dem Produkt CA Spectrum realisiert.

Service: Für WWU und UKM gemeinsam werden ein NOC (Network Operating Center für die Netzbetriebsführung), ein NIC (Network Information Center für die

Netzanschluss-, Endgeräte- und Adressenverwaltung), ein NTC (Network Technology Center für Lagerverwaltung) sowie eine gemeinsame 365x24 Rufbereitschaft angeboten.

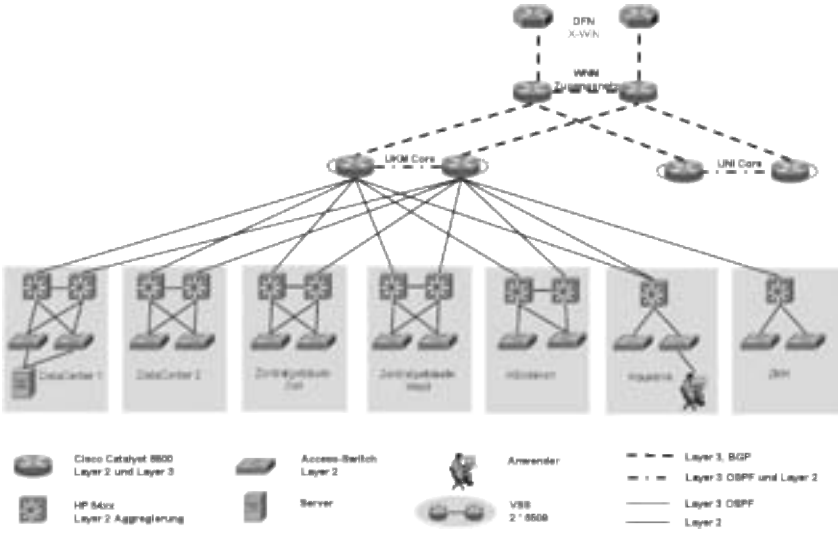

Abb.1: Ist-Situation des Netzes des UKM - Ein Core mit 2 redundanten Switches bildet das Zentrum des Doppelsterns der Layer-2 Verteilstruktur. Auch die beiden DataCenter sind auf Layer-2 direkt an die Core-Switches angebunden. Die Betriebserfahrung zeigt, dass sich dadurch leicht Störungen über den Core in den sensiblen DataCenter-Bereich ausbreiten. Die Verbindung zum Netz der WWU erfolgt über Layer-3 über die Router des Wissenschaftsnetzes Münster (WNM). Hierüber werden auch weitere Hochschulen und Forschungseinrichtungen am Standort eingebunden und die Konnektivität zum DFN hergestellt.

2 Betriebliche Erfahrungen – Bedarf für die lokale Eindämmung von Störungen

Das oben beschriebene Netzdesign wurde seit 2002 aufgebaut und seitdem stetig von anfänglich ca. 23.000 auf gegenwärtig ca. 50.000 Netzanschlüsse im gemeinsamen Netz von WWU und UKM erweitert. In dieser Zeit ist es zu mehreren umfänglicheren Störungen des Netzes gekommen, die im Case Management Tool umfänglich dokumentiert sind.

Ein zentraler Aspekt bei den betrieblichen Erfahrungen der letzten Jahre ist dabei, dass die aus Gründen der hohen Flexibilität bei der Bereitstellung von Netzanschlüssen in derselben Netzzone für auf verschiedene Liegenschaften verteilte Arbeitsgruppen und der feingranular zentral bereitstellbaren Sicherheitsfunktionen etablierte Strategie der geografie-unabhängigen Bereitstellung von Endnutzer-VLANs problematisch ist. Auch die uneingeschränkte Zentralisierung der Netzsicherheits- (stateful Firewall, IPS, VPN)

und Kerndienstfunktionen (DHCP, DNS, …) steht mit wachsender Netzausdehnung im Konflikt mit den drastisch gestiegenen Anforderungen an die Netzverfügabrkeit.

So ist festzustellen, dass beispielsweise die Absicherung von sensiblen Netzzonen einzelner Bereiche im Klinikum durch zentral realisierte Firewall und IPS Funktionen bei Störungen des WWU Netzes durch hohe Netzbelastung (z.B. DoS Attacken) deren netzmäßige Isolierung bewirken, obwohl im UKM Netz ansonsten keine Störungen bestehen. Ein ähnliches Bild stellt sich auch bei Störungen und Fehlkonfigurationen der zentralen Sicherheits- und Kerndienstfunktionen dar.

Wiederholt war auch zu bemerken, dass Schleifen im Netzwerk (wegen versehentlicher „Kurzschluss-Patchungen“ durch Endnutzer) – entgegen der Erwartung in die zu deren Erkennung und Unterdrückung eingesetzten Funktionalitäten der Netzkomponenten – immer wieder zu großflächigen Störungen führen, die insbesondere innerhalb des gesamten betroffenen Layer-2 Bereichs (also im dargestellten Netz-Design potenziell campusweit) ausgebreitet werden, und durch Überlastung aller davon betroffenen Switches auch Kollateraleffekte in anderen Layer-2 Bereichen haben können. Die Überlastung der switchinternen Controlplane bewirkt ein willkürliches Verwerfen von Steuerpaketen, in dessen Folge verschiedenste Protokolle zur Kontrolle und Redundanzbereitstellung kollabieren (beispielsweise die Routingprotokolle - OSPF, STP) oder gar die Links der Coreswitches wegen des Verwerfens der UDLD (Unidirectional Link Detection) Pakete in den Zustand Errordisable schalten.

Entsprechende großflächige Störungen waren Anfang 2010 zu bewältigen, eine niemals aufgeklärte Störung Anfang 2008 dürfte eine ähnliche Ursache gehabt haben. Ebenso können nicht beeinflussbare Störquelle wie ein defektes Switchmodul in einem der Coreswitches in April 2010 durch ein Fehlverhalten mit falsch weitergeleiteten Paketen zu campusweiten Störungen führen. Auch zeitlich sehr beschränkte Störungsquellen führten dabei zu schmerzhaft langen Netzausfällen, bis sämtliche Links wieder aktiviert und die Kontrollprozesse wieder stabilisiert werden konnten. Die Fehlersuche in solchen großen Störungssituationen gestaltet sich nicht nur durch den dann erheblichen Druck auf die Mitarbeiter als äußerst schwierig, auch sind viele Netzkomponenten wegen der Netzprobleme nicht mehr erreichbar und durch die hohe CPU-Auslastung kaum noch bedienbar. Die Bedeutung eines umfassenden und verlässlich verfügbaren out-of-band Management für die Core-Switches wird dabei deutlich. Auch Wartungsmaßnahmen (z.B. Softwareupdates) stellen in der aktuellen betrieben Netzarchitektur ein großes Störpotenzial dar, führen doch Reboots immer (bedingt durch die Layer-2 Ausdehnung und der Layer-3 Konzentration) zu campusweiten Störungen des IT-Betriebes, die durch ihre Rückwirkungen auf die Anwendungssysteme (z.B. Clusterschwenks und hängende Dienste) deutlich über die kurzzeitige Downtime des LAN hinausgehen.

Ein im Oktober 2010 gemeinsam mit Gerätehersteller Cisco, dem ZIV und dessen Servicepartner durchgeführtes Customer Proof-of-Concept (CPOC) in den Cisco-Labors in London zeigte, dass in dem vorhandenen Netzdesign keine verlässlichen Funktionen der Netzwerkkomponenten genutzt werden können, um auftretende Netzstörungen in den lokalen oder funktionalen Bereich ihrer Entstehung zu begrenzen. Hierbei zeigte sich auch für den Hersteller Cisco unerwartet die generelle Empfindlichkeit von

Netzwerkkomponenten und Protokollen bei einer starken Aus- und Überlastung der Controlplane. Verschiedenste Versuche durch steuernden Eingriff in das Aufkommen von Control-Datenpaketen einzugreifen oder deren Transport auf der Controlplane zu priorisieren brachten keine nennenswerte Verbesserung der Netzstabilität oder führten zu anderen mindestens ebenso schmerzlichen neuen Verwundbarkeiten des Netzes. Einzig eine drastische Reduzierung der Komplexität im bestehenden Netzdesign durch Beschränkung der Anzahl der VLANs auf eine kleine zweistellige Zahl gewährte einen ausreichenden Schutz und zeigte, dass die eingesetzten Verfahren und Protokolle in der Lage sind, die Störungen abzufangen bzw. zu begrenzen.

Offensichtlich besteht also trotz durchdachtem Netzdesign und gut organisierter Betriebsführung eine gefährliche, nicht vermeidbare Verletzlichkeit des Datennetzwerkes als Ganzes durch geringfügige lokale Störungsursachen (z.B. Schleifen im Endnutzerbereich). Auch wenn durch einzelne Konfigurationsmaßnahmen (aktualisierte Softwarestände mit Bugfixes im Bereich Ressourcen-Allozierung auf den Switches; Automatisches Wiederanlaufen nach Errordisable; Priorisierung von Steuerpaketen auf der Controlplane; Prävention von Schleifen durch Deaktivierung der bequemen auto-cross-out Funktion) kurzfristig eine Verbesserung bei der Verwundbarkeit möglich ist, besteht ein Bedarf für eine grundlegende Überarbeitung des Netzdesigns, speziell mit Augenmerk auf die mit wachsender Durchdringung des klinischen Bereiches mit IT-gestützten Verfahren und der integrierten Nutzung des Datennetz für die Kommunikation (z.B. VoIP) immer bedeutsamer werdenden Anforderung für höchste Verfügbarkeit.

3 Das klinische Anforderungsszenario – die mobile Visite

Das UKM plant im Zuge der Etablierung der elektronischen Krankengeschichte die Einführung der mobilen Visite auf sämtlichen Bettenstationen. Dabei soll, gestützt über das dafür flächendeckend zu etablierende WLAN, der Abruf und die Erfassung von Krankengeschichtsdaten (Vitalparameter, Medikation, etc…) über mobile Geräte direkt am Patientenbett realisiert werden. Durch den geplanten Verzicht auf die Papier-Form wird die „100%-ige“ Verfügbarkeit der elektronischen Krankengeschichte unverzichtbar für die adäquate Behandlung.

Wegen der hohen Belastungen und des Erfolgsdruckes in diesem ambitionierten Projekt sieht sich insbesondere auch das ZIV als Betreiber des dafür unverzichtbaren Datennetzes mit der verständlichen Anforderung konfrontiert, alle Möglichkeiten zur Sicherstellung der höchstmöglichen Netzverfügbarkeit (Forderung: 100%) auszuschöpfen. Die obige Darstellung der in den letzten Jahren offenkundig gewordenen Verwundbarkeiten des Datennetzwerkes macht deutlich, dass dafür neue technische Designkonzepte notwendig sind.

Nach der Abwägung zahlreicher auch unorthodoxer Lösungsansätze (z.B. Rückgriff auf externe Mobilfunknetze) zur Schaffung von redundanten Systemen zur Bewältigung von – effektiv unvermeidbaren – Störungen konnte das im nächsten Abschnitt beschriebene Redesign für die Schaffung selektierter hochverfügbarer klinischer Arbeitsplätze

erarbeitet und mit der Nutzerseite akkordiert werden, das folgenden zentralen Forderungen genügt:

1. Das Konzept soll einfach und überschaubar sein. Komplexe und nicht unter eigener Kontrolle stehende Technologien und Systeme (wie z.B. bei einem Backup über externe 3G Netze) sind genauso ungeeignet wie neue, betrieblich noch nicht erprobte Komponenten.

2. Im Störungsfall muss für selektierte „hochverfügbare" Arbeitsplätze ein nahtloses Weiterarbeiten ohne die Notwendigkeit von Interventionen zur Umkonfiguration möglich sein.

3. Die hochverfügbaren Arbeitsplätze müssen in täglicher Routineverwendung stehen, da nur so die Funktion im Krisenfall sichergestellt ist.

4. Der Kommunikationsweg zwischen den hochverfügbaren Arbeitsplätzen und den DataCenters, in denen die Anwendungssysteme der elektronischen Krankengeschichte betrieben werden, muss möglichst direkt sein.

4 Hochverfügbarkeits-Redesign für das Datennetz

Auf Basis der betrieblichen Erfahrungen der letzten Jahre hatte sich die großräumige Ausbreitung von Störungen mit dezentral lokalisierbaren Ursachen als Kernproblem herausgestellt. Eine grundlegende Erneuerung des gesamten LAN, die sowieso an der Zeit ist und in deren Zuge auch diese Problematik adressiert werden soll, ist mittelfristig geplant. Kurzfristig ist eine Abkehr vom etablierten VLAN-Konzept im UKM Campus Backbone mit seinen ca. 20.000 Netzanschlüssen jedoch nicht bewerkstelligbar.

Die netztechnische Grundlage für die Hochverfügbarkeit der zentralen klinischen Informationssysteme der elektronischen Krankengeschichte an einer überschaubaren Zahl (wenige 100) von selektierten und funktional eingeschränkten klinischen Arbeitsplätzen lässt sich jedoch mit überschaubarem Aufwand (in puncto Material, Zeit und Arbeitsleistung) mit folgenden Maßnahmen realisieren.

Layer-3 Entkopplung der DataCenter vom Campus-Backbone

Die Ausbreitung von Störungen im normalen Campusnetzwerk in die DataCenter muss unterbunden werden. Nur so kann die Verfügbarkeit der dort betriebenen IT-Systeme der elektronischen Krankengeschichte sichergestellt werden. Die Entkopplung auf Layer-3 durch ein eigenes Switch-Paar ist eine Maßnahme dafür, die sich anhand der betrieblichen Erfahrungen bewährt hat – Störungen im WWU Netz wurden durch die Layer-3 Entkopplung im WNM effektiv vom UKM Netz ferngehalten. Der Materialaufwand dafür hält sich in Grenzen. Die damit verbundene Möglichkeit zur Etablierung neuer „virtual switching" Technologien (VSS: Virtual Switching System), die aktiv/aktiv Redundanz ohne von STP bekannten langen Konvergenzzeiten ermöglicht, und somit die Perspektive zur Eliminierung der Cluster-Schwenks bei den

hochverfügbar geclusterten und auf die beiden DataCenters verteilten Systemplattformen der klinischen IT-Systeme bietet, ist ein höchst willkommener Zusatznutzen. Der Vergleich von Abb.1 und Abb.3 verdeutlicht die Umstellungen im LAN zur Entkopplung der DataCenter. Die in Abb.2 und Abb.3 dargestellten Strukturen wurden ebenfalls im oben beschriebenen Cisco-CPOC geprüft und boten hier den einzigen verlässlichen Schutz vor einer Übertragung von Störungen im vorhandenen Netz auf den DataCenter-Bereich. Es muss hierbei nicht auf die Bildung von Netzzonen und deren Entkoppelung per VRF-lite verzichtet werden. Es besteht die Möglichkeit eines virtualisierten Backbones im Core, über den die einzelnen VRFs mittels Tranfer-VLANs verbunden werden. Diese dürfen sich jedoch lediglich als Punkt-zu-Punkt-VLAN auf einzelnen Links befinden, ein Weiterleiten dieser Tansfer-VLANs durch Geräte hinweg ist im ersten Schritt nicht mehr zulässig (siehe Abb.2). Die Erfahrungen aus den CPOC zeigen zusätzlich, dass eine Beschränkung auf wenige VLANs in dem entkoppelten Netzbereich die Netzstabilität - auch in extremen Störungssituationen innerhalb der DataCenter - erhöhen kann. Auch wenn keine exakte Menge ermittelt wurde (oder ermittelt werden kann) scheint eine Anzahl von nicht wesentlich mehr als 30 VLANs, die sich in unserem Fall sinnvoll auf 2-3 VRFs-lite verteilen lassen, sinnvoll.

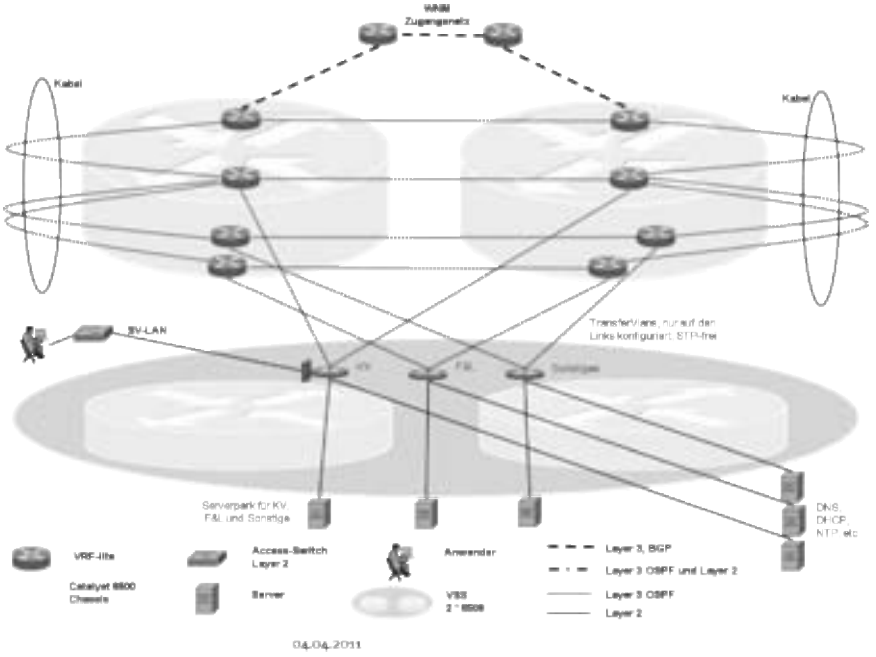

Abb.2: Netzzonen können weiterhin mittels VRF-lite voneinander getrennt werden. Die Verbindung der VRF-lite erfolgt über ein virtualisiertes Backbone mittels link-begrenzten Tansfer-VLANs.

Eine wichtige Konsequenz bei der Umsetzung dieser Layer-3 Entkopplung ergibt sich jedoch für den Betrieb von Client-Server Systemen. Da die selben VLANs nicht mehr im Campusnetzwerk und im DataCenter definiert sein können, müssen die

Kommunikationsbeziehungen zwischen Clients und Servern aufwändig neu organisiert werden – generell müssen neue IP Service-Adressen konfiguriert werden, und nicht gerouteter Datenverkehr zwischen Clients und Servern ist nicht mehr möglich.

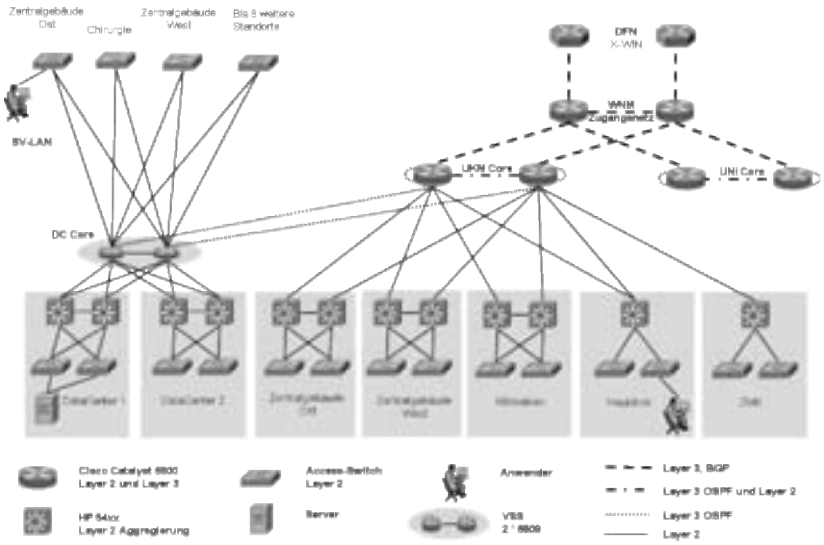

Abb.3: Soll-Konzept für das Netz des UKM - Die DataCenter werden auf Layer-3 vom Core des Campusnetzes entkoppelt, um die Fortpflanzung von Störungen in diesen sensiblen Bereich zu verhindern. Die redundante Anbindung der Verteilstruktur im DataCenter wird anstelle aktiv/passiv (Spanning Tree) über eine aktiv/aktiv Link-Aggregation Verbindung an die über „virtual switching“ (VSS) gekoppelten DataCenter-Switches realisiert. Eine direkt an die DataCenter Switches angebundene hochverfügbare Verteilstruktur (SV-LAN) für selektierte Arbeitsplätze reduzierter Funktionalität stellt auch im Falle großflächiger Netzstörungen im Rest des UKM-Netzes deren Verbindung zu den DataCenters sicher.

Gesondertes Verteilnetz mit enger Anbindung an die DataCenter

Für die Verfügbarkeit der elektronischen Krankengeschichtssysteme in den klinischen Bereichen ist die Datennetzkonnektivität von dortigen Arbeitsplatzsystemen zu den Servern in den DataCenters notwendig. Da Störungen im „normalen“ Campus-LAN des UKM – wie zuvor dargestellt - realistisch nicht ausgeschlossen werden können und eben deswegen die vorstehend beschriebene Abkopplung der DataCenter umzusetzen ist, ist für hochverfügbare Arbeitsplatzsysteme auch ein vom „normalen“ Campus-LAN unabhängiger Kommunikationsweg notwendig. Dieser muss direkt zu den DataCenter-Switches führen und den normalen Campus-Backbone umgehen. Dies bedingt auch direkte passive Netzverbindungen von Access-Switches an die DataCenter-Switches. Hierfür kann glücklicherweise auf eine multimode Fiber-to-the-Desk-Verkabelung aus früheren Jahren, mit denen anfänglich wegen langer Wegstrecken in den Bettentürmen des UKM Arbeitsplätze mit Datennetz versorgt wurden, zurückgegriffen werden. Abseits des seit längerem auf CAT6 Kupferkabeln basierenden normalen Campus-LAN

lassen sich damit wenige selektierte Arbeitsplatzsysteme (ca. 2 bis 3 je Station, ca. 250 insgesamt) auf sehr direktem Weg an wenige Access-Switches an den DataCenters anbinden (vgl. Abb.3). Durch das weitestgehende Vorhandensein der passiven Infrastruktur und den geringen Bedarf an aktiven Komponenten hält sich auch hier der Materialaufwand in engen Grenzen. In Analogie zur Energieversorgung wird dieses LAN-Segment als Sonderversorgungs-LAN (SV-LAN) bezeichnet.

Selektierte funktional eingeschränkte klinische Arbeitsplätze

Die Anbindung der ca. 250 ausgewählten Arbeitsplatzsysteme erfolgt sehr direkt an die DataCenter-Netze. Aus offensichtlichen Gründen der Verfügbarkeit muss hier auf den Rückgriff auf die zentralen virtualisierten Netzsicherheitsfunktionen (stateful FW, IPS, VPN) verzichtet werden – allenfalls können ACLs und Edge-Portbasierende Funktionen (MAC-Security, DHCP-Snooping, etc) genutzt werden. Folglich muss mit diesen Arbeitsplätzen sehr restriktiv bzgl. Sicherheit verfahren werden. Der möglichst ausschließliche Einsatz von ThinClients, die auf die klinischen IT-Systeme nur im Wege der ebenfalls in den DataCenters betriebenen Citrix Terminalserver zugreifen, gewährleistet hohe Sicherheit und optimiert durch die Minimierung von clientseitigen Störungen weiter die Verfügbarkeit. Da diese Arbeitsplätze aber voll für die tägliche Routinearbeit genutzt werden können, ist sichergestellt, dass clientseitige Störungen sofort bemerkt werden und diese Geräte somit im Krisenfall wesentlich verlässlicher bereitstehen als ausschließlich auf standby bereitgehaltene Notlösungen. Darüber hinaus evaluiert der für die Betreuung dieser Arbeitsplatzsysteme zuständige Geschäftsbereich IT des UKM Verfahren zur zentralen Überwachung der Citrix-Clients sowie der notwendigen Serverdienste und Schnittstellen. Die Bereitstellung einer dedizierten Citrix-Farm für die Clients im SV-LAN wird ebenfalls diskutiert.

5 Zusammenfassung und Ausblick

Das dargestellte Konzept verspricht eine wesentliche Erhöhung der Verfügbarkeit der klinischen IT-Systeme der elektronischen Krankengeschichte im UKM durch Verbesserung der Netzkonnektivität für selektierte Arbeitsplatzsysteme in den klinischen Bereichen. Durch die moderaten Umsetzungsaufwände konnte eine schnelle Umsetzung bereits in Angriff genommen werden. Die erhofften Verfügbarkeitsverbesserungen sollen durch Monitoring (sowohl über die Netzmanagement-Systeme wie auch durch Beobachtung und Evaluation gemeinsam mit den Nutzern) verifiziert werden.

Das dargestellte Designprinzip der Layer-3 Entkopplung soll bei der anstehenden Erneuerung des LAN-Backbone von WWU und UKM weitergehend angewandt werden und damit ultimativ auch im „normalen“ Campus-LAN des UKM die Verfügbarkeit erhöhen.

In diesem Konzept ist die deutliche Abkehr von einem in der bisher etablierten Netzarchitektur gültigen Prinzip erkennbar. Wurde bislang jeder Layer-2 Bereiche global im ganzen Netz angebunden, die Layer-3 Vermittlung zwischen diesen aber nur an

wenigen zentralen Core-Routern, sollen zukünftig die Layer-2 Bereiche im Sinne des Störungs-Containments lokal beschränkt werden, und die Vermittlung in andere Layer-2 Bereiche durch dezentrale Routing-Instanzen erfolgen, die ihren Datenverkehr untereinander über wenige Transfer-VLANs über wenige leistungsfähige zentrale Layer-2 Switches austauschen.

Selbstverständlich hat dies auch substantielle Auswirkungen auf die Betreiber von Client-Server-Systemen, da die bislang mögliche Bereitstellung der Endnutzer-Ports auch im DataCenter nicht mehr möglich ist, und auch im Hinblick auf die neuen Konzepte des DataCenter Bridging (DCB) nicht mehr zeitgemäß ist.

Literaturverzeichnis

[Ant10] Antrag zum Ausbau des Kommunikationssystems – Netzkonzept, Netzentwicklungsplan, Betriebs- und Managementkonzept, Personalsituation – Gemeinsame Darstellung für die Westfälische Wilhelms-Universität und das Universitätsklinikum Münster. Münster, 2010.
http://www.uni-muenster.de/imperia/md/content/ziv/pdf/antrag_ausbau_kommunikationssystem_teil_b-version16-release_mit_anhaengen.pdf.

[Vog10] Vogl, R; Speer, M; Gietz, N; Elkemann, L.: Netzentwicklungskonzept für ein großes Universitätsnetzwerk – Bestandspflege und Erschließung neuer Technologien. In (Müller, P. et.al. Hrsg.): Proceedings 3. DFN-Forum Kommunikationstechnologie, Konstanz 2010, Gesellschaft für Informatik, Bonn, 2010; S. 45-60.