Dezentrale Verwaltung der Netzwerkinfrastruktur

Christopher Ritter, Michael Flachsel, Thomas Hildmann

tubIT – IT-Service-Center der TU-Berlin
Technische Universität Berlin
Einsteinufer 17
10587 Berlin
christopher.ritter@tu-berlin.de
michael.flachsel@tu-berlin.de
thomas.hildmann@tu-berlin.de

Abstract: Mit der zunehmenden Nutzung mobiler Arbeitsgeräte steigt auch die Herausforderung an Hochschulen die dafür benötigte Netzwerkinfrastruktur bereit zu stellen. Diese muss zum einen flächendeckend und zuverlässig verfügbar sein, zum anderen aber auch einen hohe Flexibilität aufweisen um schnell auf sich ändernde Anforderungen reagieren zu können. Forschungseinrichtungen wünschen meist eigene Subnetze zur Realisierung ihrer Forschungsumgebungen. Diese sollten schnell erweiterbar sein und möglichst überall zur Verfügung stehen, wo sie gerade benötigt werden. An Hochschulen mit mehreren hundert Einrichtungen führt diese ständige Änderung an Netzwerkbereichen zu einem hohen Auftragsaufkommen im Bereich der Netzbetreuung. Neben der durch die Masse gegebene Verzögerung der Abarbeitung, führen häufig fehlende oder fehlerhafte Informationen zu weiteren Verzögerungen. Hier verspricht die Auslagerung von Teilen der Netzwerkverwaltung direkt in die Einrichtungen eine starke Beschleunigung sowie eine größere Flexibilität. Durch die Verknüpfung des hochschulweiten Identitätsmanagement Systems mit dem zentralen DNS- und DHCP-Server, einer Integration in die WLAN- und VPN-Infrastruktur sowie dem zentralen Netzwerkinfrastrukturmanagementsystems, gelingt es genau dies zu erreichen.

1 Einleitung

Die Netzwerkversorgung der TU Berlin, mit über 40.000 Nutzern, über 60 Gebäuden, etwa 2.000 Access Points und mehreren Hundert Einheiten mit zumeist eigenen Subnetzen stellt grundlegend eine permanente Herausforderung dar. Die Netzwerk-Grundversorgung im LAN- und WLAN-Bereich wird durch tubIT, den zentralen IT Dienstleister bereitgestellt. Mit wenigen Ausnahmen, findet die Vorortbetreuung der Nutzer und Arbeitsplätze durch dezentrale Netzwerkverwalter statt. Um den praktisch täglich wechselnden Anforderungen, insbesondere in Forschungsnetzwerken gerecht zu werden und um Verzögerungen und Missverständnisse in der Endgeräteversorgung zu vermeiden, setzt tubIT auf einen Satz von Selbstbedienungswerkzeugen, die über das Web-Portal bereitgestellt werden. Um die Funktionalität und Sicherheit dieser

Anwendungen gewähren zu können, bedarf es der Integration einer Reihe von IT-Komponenten, wie z.B. dem rollenbasierten Identity Management (TUBIS), der DNS-/DHCP-Appliance (Infoblox [INF]), dem VPN-Zugangspunkt (Cisco ASA [CIS2]), den Controller-basierten WLAN in Kombination mit der eingesetzten MPLS-Technologie [CIS1], dem Netzwerkinfrastrukturmanagementsystem (FNT Command [FNT]) sowie eingebettet in entsprechende Web-Portalanwendungen und kombiniert mit Daten aus Personal- und Studierendenverwaltung, sowie der Datenbasis aus dem Flächenmanagement aus der TU Bauabteilung (Abbildung 1).

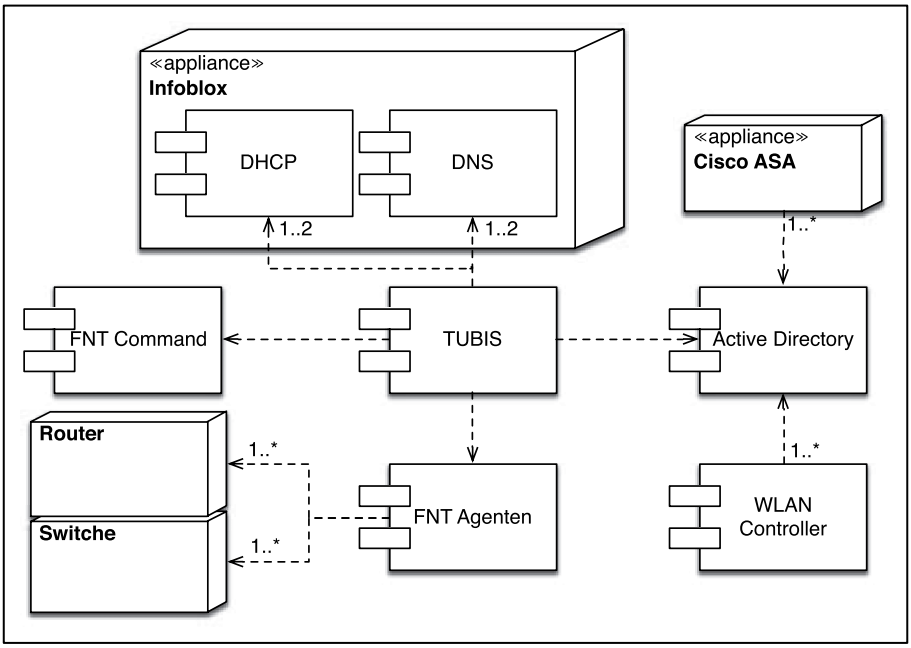

Abbildung 1: Zur Realisierung benötigte IT-Komponenten

Der Artikel stellt zunächst die Voraussetzungen vor, die zur Umsetzung der Selbstbedienungsfunktionen nötig sind. Wir stellen dann die Verwaltung von Subnetzen und IP-Adressen, das Beschalten von Netzwerkdosen mit eigenem Subnetzen (VLANs) sowie die Funktion WLAN und VPN in das eigene VLAN vor. Im Ausblick werden die aktuellen und künftigen Erweiterungen des Gesamtkonzepts vorgestellt.

2 Voraussetzungen

Kern unserer Arbeit ist die Integration von verschiedenen Technologien und Produkten zur Abbildung der häufigsten Arbeitsprozesse im Betrieb des wissenschaftlichen Netzwerkes. Die Voraussetzungen zur Umsetzung der nutzergesteuerten

Netzwerkverwaltung (Identitymanagement, Orgnamen und Netzwerkinfrastruktur) werden im folgenden vorgestellt.

2.1 Identitätsmanagement als Grundlage

Die Veränderungen der letzten Jahre in der IT-Hochschullandschaft spiegeln den Trend zur Integration vielfältiger Universitätsbereiche wieder, die vorher weitgehend unabhängig voneinander gearbeitet haben. Der Bedarf für eine solche Integration entsteht durch die Erwartungen von Studierenden und Mitarbeitern, zahlreiche Dienste durch Selbstbedienungsfunktionen zu nutzen und somit mehr Zeit für Studium und Forschung zu gewinnen. Die Umsetzung eines integrierten Dienstangebots stellt die Hochschulen wiederum vor signifikante technische und organisatorische Herausforderungen. Geschäftsprozesse und Verantwortlichkeiten sind selten umfassend dokumentiert, wodurch eine übergreifende Planung, Steuerung und Operationalisierung erschwert wird.

Neben den notwendigen Veränderungen in der Leitungs- und Organisationsstruktur wartet noch eine Reihe von technischen Problemen auf eine Lösung. Das dominierende Thema ist in diesem Bereich ein funktionierendes System für das Identitätsmanagement, als Grundlage der darauf aufsetzenden Dienste des Campusmanagement.

Jedes Mitglied der Universität muss eindeutig und mit allen Befugnissen, Kontexten wie etwa Status (Studierender, Mitarbeiter), Rolle (Dekan, FG-Leiter, Abteilungsleiter, …) oder Studiengang, bekannt sein, damit ein möglichst einfacher, einheitlicher Zugang zu allen für ihn relevanten Diensten möglich wird; und dies gleichgültig, ob sich die Person am Arbeitsplatz, zu Hause oder auf einer Dienstreise befindet.

Die TU-Berlin hat zur Erfüllung der Aufgaben eines Identitätsmanagementsystems das universitätsweite, rollenbasierte Autorisierungssystem TUBIS entwickelt [HKR08b, HR07]. Dieses integriert sich in die bestehende Infrastruktur der Campusmanagementsysteme und überwacht die Identitäten dabei während des gesamten Lebenszyklus zwischen Eintritt uns Ausscheiden.

Dabei werden sowohl die Lebenszyklen der Personen als auch die der Einrichtungen selbst berücksichtigt (Abbildung 2). Das IDM bietet den jeweiligen Einrichtungen die Möglichkeit der dezentralen Rechteverwaltung [RHK10]. So entsteht die Möglichkeit eine Vielzahl von IT-Dienstleistungen, die bisher von Mitarbeitern des Rechenzentrums erledigt werden mussten, direkt in die Einrichtungen zu verlagern. Dabei bietet TUBIS eine Reihe von webbasierten Selbstbedienungsfunktionen, aber auch auf Basis von Web-Services realisierte Schnittstellen, zur Bereitstellung von Diensten für bestimmte Module der eingesetzten Campusmanagementsysteme.

Diese Schnittstellen sind eine Voraussetzung für die nachfolgend beschriebenen Verfahren.

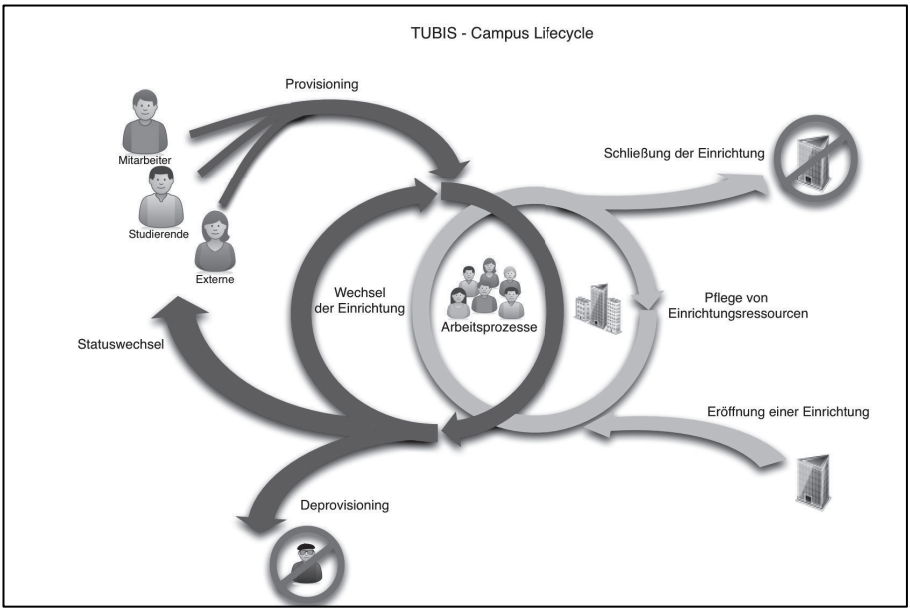

Abbildung 2. Lebenszyklus von Identitäten und Einrichtungen

2.2 Der Orgname

Das Pendant zum Provisioning von Personen ist die Einrichtung des sog. Orgnamen für eine Einheit an der Universität. Die Beantragung (Abbildung 3) ist die Voraussetzung zur Nutzung eines Großteils der Selbstbedienungsanwendungen für Einrichtungen. Dahinter verbirgt sich eine maximal 20 Zeichen lange Kurzbezeichnung der Einrichtung, die als Subdomain unterhalb von tu-berlin.de eingerichtet wird. Dieser wird u.a. für die Einrichtung eines Auftritts im Contentmanagement-System benötigt, zum Vergeben von E-Mailaliasen oder auch zur Einrichtung von Mailinglisten. Neben dieser Hauptdomain einer Einrichtung kann jede Einrichtung beliebig viele sog. Internetnamen beantragen. Diese sind technisch identisch mit dem Orgnamen und führen ebenfalls zum Anlegen einer entsprechenden Subdomain. Sie werden logisch aber den Orgnamen untergeordnet. „Internetnamen“ können daher nur für eine Teilmenge der Dienste genutzt werden.

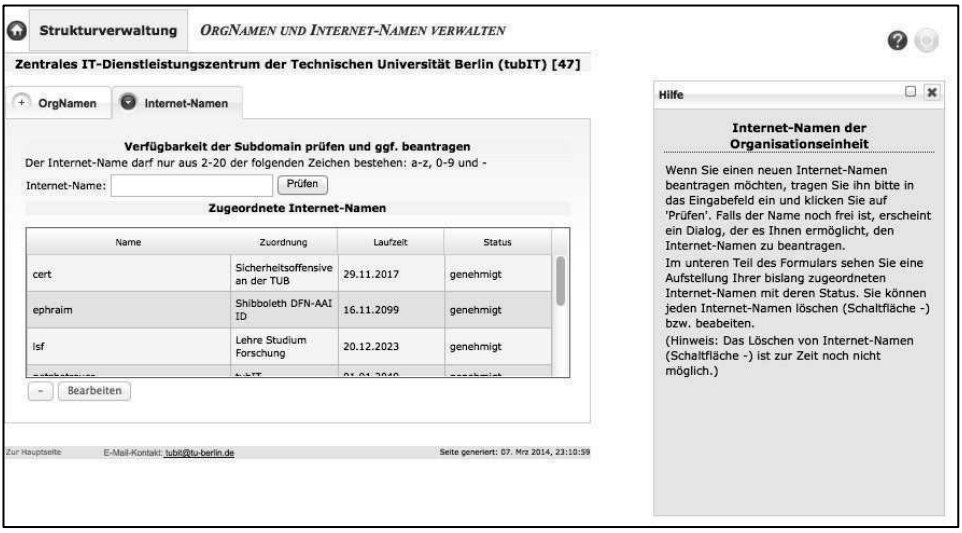

Abbildung 3: Selbstverwaltungsfunktion für "Internetnamen"

2.3 Netzwerkinfrastruktur

Die TU Berlin verteilt sich flächenmäßig auf etwa 60 Gebäude an drei Standorten innerhalb von Berlin. Für den Betrieb des Netzwerkes ist zentral tubIT als Dienstleister verantwortlich. Zur Versorgung dieser Flächen mit Netzwerk wurde ein mehrstufiges Konzept zum Betrieb des Netzwerkes über MPLS eingeführt. Die Basis bilden 11 MPLS-Knoten, die das Kernnetz (Backbone) der TUB aufbauen. Zwei der Kernnetzknoten beherbergen je einen Übergang zum Internet um diesen redundant anzubieten (Abbildung 5). Diese 11 Kernnetzknoten erschließen ihrerseits die verschiedenen Gebäude und Flächen der TU. Der Backbone bildet damit gleichzeitig den Distribution-Layer (vgl. Abbildung 4). Das grundlegende Routing-Protokoll innerhalb des Backbone ist OSPF. Zur Übergabe an die Internetprovider wird BGP eingesetzt.

Untereinander sind jeweils mindestens zwei der Knoten in Maschenform miteinander direkt über Glasfasern verbunden um redundante Wege innerhalb des Kernnetzes realisieren zu können.

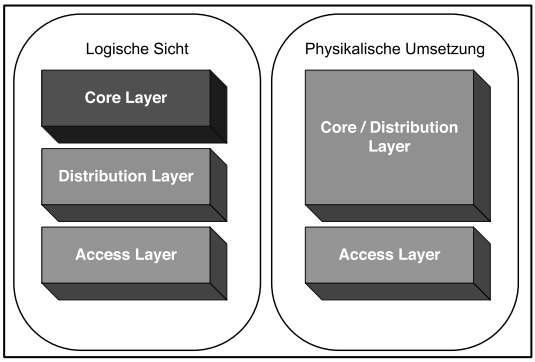

Abbildung 4: Netzwerkebenen

Die Übertragungsgeschwindigkeit zwischen den Kernnetzknoten beträgt zur Zeit 2 x 10 GBit/s.

Innerhalb dieser Knoten werden die Layer-2-Verbindungen der Endkundennetze terminiert und auf Layer-3 umgesetzt. Gleichzeitig befindet sich innerhalb der Kernnetzrouter die Firewallinfrastruktur zur Absicherung der an dem jeweiligen Knoten gerouteten Netze.

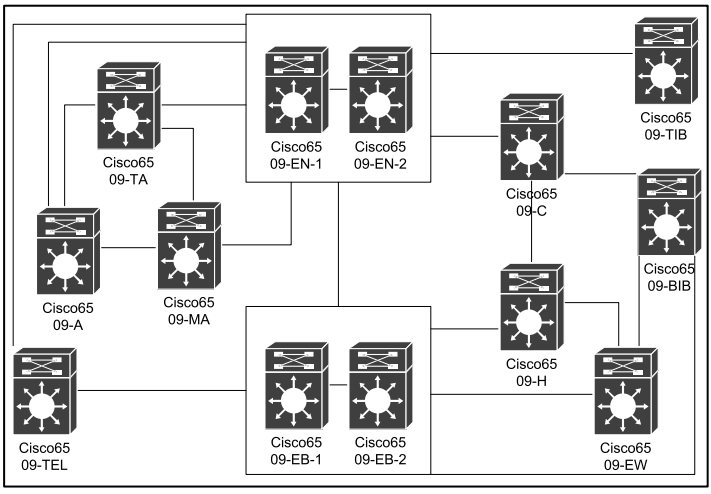

Abbildung 5: MPLS Kernnetzlayout

Diese Endkundennetze stehen dann an den jeweiligen Switchen der Gebäude eines Knotens zur Verfügung und können auf die Dosen in den Räumen geschaltet werden. Die Access-Switches sind direkt mit den Routern verbunden, auch hier kommen, soweit die Verbindungen vorhanden sind, redundante Anbindungen mit jeweils mindestens 10 GBit/s über Glasfasern zum Einsatz. Insgesamt sind an der TUB ca. 60.000 Endnutzerports mit ca. 450 Switchen unterschiedlicher Größe und Güte verbunden.

Jedes Endkundennetz ist organisatorisch einer Einrichtung an der TUB zugeordnet und wird durch mindestens einen dezentralen Betreuer verwaltet. Technisch werden die Endkundennetze durch separate VLANS in den jeweiligen Knoten realisiert. Jedem dieser VLANS ist ein eigenes Subnetz innerhalb der Class-B-Netze der TUB zugeordnet. Zur Zeit existieren ca. 500 verschiedene Endkundennetze an der TUB. Das derzeitige Sicherheitskonzept der TUB ist nicht Personen orientiert, sondern Einrichtungsorientiert.

Die Umsetzung des Netzwerkkonzeptes erfolgt im Backbone mit Cisco Catalyst 650x-Geräten, die an den beiden Internetausstiegen in einem VSS-Verbund aufgebaut sind, an den anderen Standorten mit jeweils einer zweiten Supervisor-Engine ausgestattet sind um die Anforderungen an Redundanz und Verfügbarkeit zu erfüllen. Im Access-Bereich kommen Cisco Catalyst 2960s und 4510 zum Einsatz, die die Anbindung der Endkunden, sowie die Versorgung der Thin AccessPoints übernehmen. Zur Sicherung der Netzwerke werden flächendeckend STP und MAC-Lockdown eingesetzt.

Die Netzwerkverwalter der Endkunden-Netze können je Netzwerk die von Ihnen gewünschten initialen Firewall-, DNS- und DHCP-Settings beantragen. Diese werden dann bei der Einrichtung vom Netzwerkbetriebsteam umgesetzt.

3 Verwaltung von Subnetzen und IP-Adressen

Erster Bestandteil des Systems zur dezentralen Verwaltung der Netzwerkinfrastruktur ist eine Appliance (Infoblox 1550) zur DNS und IP-Adressen Verwaltung. Diese bildet den redundant ausgelegten DNS- und DHCP - Server der TU-Berlin. Über eine vom Hersteller angebotene Schnittstelle ist es möglich bestimmte Funktionen nach außen zur Verfügung zu stellen. Um eine flexible Verwaltung der Zugriffsrechte zu ermöglichen wurde eine Selbstbedienungsanwendung in das personalisierte Portal der TU-Berlin integriert, deren Zugriffskontrolle direkt im zentralen Identitätsmanagement stattfindet.

Die Anwendung ermöglicht es entsprechend berechtigten Personen einer Einrichtung für diese Einrichtung neue Subnetzte zu beantragen, bestehende Netze zu erweitern oder zu entfernen. Die Anwendung sorgt an dieser Stelle dafür, dass alle für die Ausführung des Antrags benötigten Informationen vorliegen (Abbildung 6).

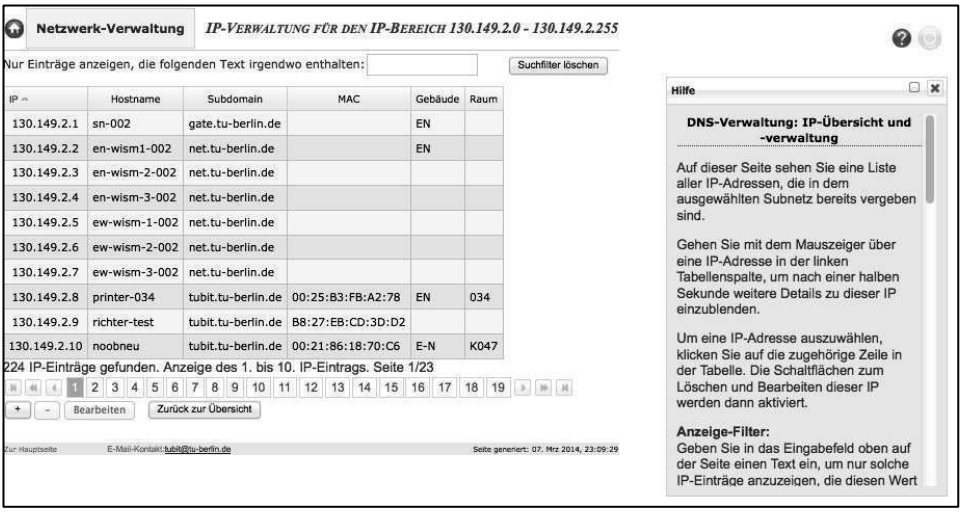

Abbildung 6: Verwaltung von IP-Adressen

Neben dem Verwalten von Subnetzen bietet die Anwendung die Möglichkeit IP Adressen innerhalb der zur Verfügung stehenden Subnetze zu verwalten. So können einzelne Host definiert werden, aber auch DHCP Bereiche festgelegt werden. Änderungen der Einträge oder neu erzeugte Angaben werden direkt an die Appliance übermittelt und sind somit ohne zeitliche Verzögerung produktiv.

4 Das eigene Netz vor Ort - Schalten von Netzwerkdosen

Besitzt eine Einrichtung Subnetze, so möchte sie diese auch flexibel innerhalb der ihr zur Verfügung stehenden Räume schalten können. Durch das Zusammenspiel des Flächenmanagementsystems der Zentralen Universitätsverwaltung, des Netzwerkinfrastrukturmanagementsystems und den verteilten Netzwerkkomponenten des Rechenzentrums sowie dem zentralen Identitätsmanagementsystems ist es möglich diese Beschaltung der Netzwerkdosen direkt durch die Verantwortlichen der Einrichtungen vornehmen zu lassen.

Über eine Selbstbedienungsanwendung im persönlichen Portal sehen die Netzwerkverwalter der jeweiligen Einrichtung zunächst alle Gebäude, Stockwerke und Räume, die ihr im Flächenmanagementsystem zugewiesen sind. Durch die Informationen des Netzwerkinfrastrukturmanagementsystems kann nun für jeden Raum die verfügbaren Netzwerkdosen sowie deren Belegung eingesehen werden (Abb. 7).

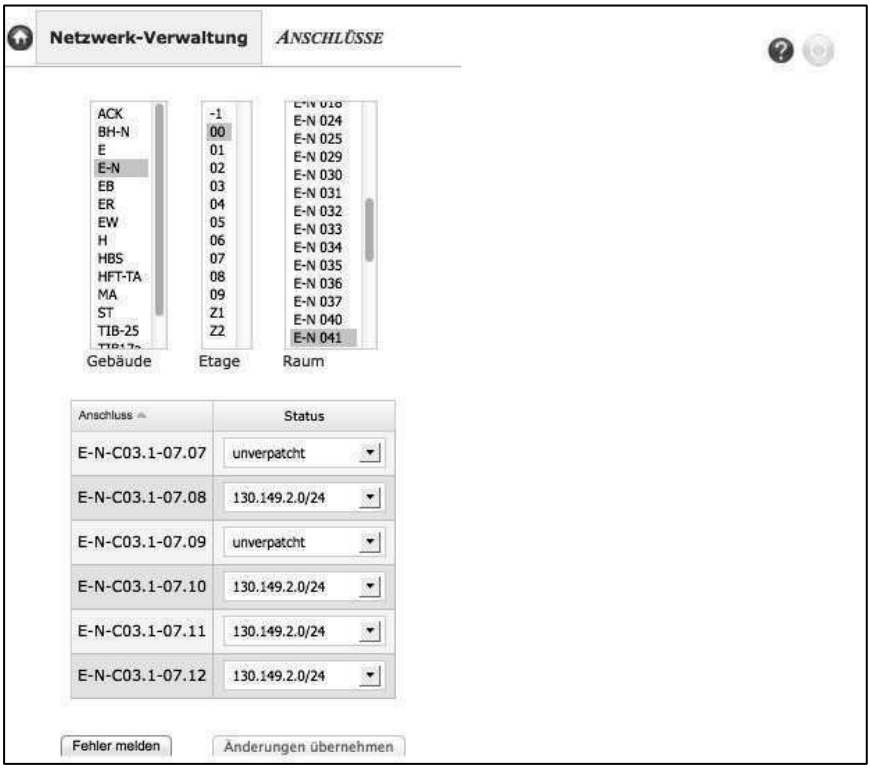

Abbildung 7: Beschaltung von Netzwerkdosen

Jedem Anschluss kann ein anderes der Einrichtung zugewiesenes Subnetz zugeordnet werden. Dabei werden alle Subnetze angezeigt, die in der DNS Verwaltung der Einrichtung zugewiesen wurden. Netze, die an den lokalen Netzwerkknoten nicht anliegen, werden dabei automatisch herausgefiltert. Das Ändern einer Beschaltung führt wie auch bei den anderen Selbstbedienungsfunktionen direkt zu einer Aktion in den betroffenen Netzwerkkomponenten. Diese werden über realisierte Schnittstellen umprogrammiert, so dass die neue Beschaltung sofort zur Verfügung steht. Die vorgenommenen Änderungen werden bei Erfolg in das Netzwerkinfrastruktur-managementsystem übertragen. Zusätzlich zur Belegung mit einem Netzwerk ist es auch möglich Anschlüsse als Telefonanschlüsse zu definieren. Da die derzeitige Telefonanlage keine entsprechende Schnittstelle besitzt, führt diese Aktion allerdings nur zu einem Antrag bei der zuständigen Abteilung. Neben der Möglichkeit zur Konfiguration der Netzwerkdosen bietet die Anwendung auch noch eine Exportfunktion der aktuellen Belegungen an sowie ein Fehlermeldungssystem bei fehlenden oder falschen Angaben bei Gebäuden, Stockwerken, Räumen, Netzwerkdosen oder deren Beschaltungen.

Um sicherzustellen, dass im Netzwerkinfrastrukturmanagement jeweils aktuelle Informationen zur Switch-Konfiguration vorliegen, werden die VLANs aller Switche einmal täglich in der Nacht ausgelesen und mit der Datenbank des Netzwerk-infrastrukturmanagements abgeglichen.

5 Und auch von Unterwegs - WLAN und VPN ins eigene VLAN

Die wachsende Mobilität durch den Einsatz tragbarer Endgeräte weckt den Wunsch das Subnetz einer Einrichtung auch unterwegs nutzen zu können. Mit der hochschulweiten Abdeckung durch WLAN Accesspoints wurde an der TU-Berlin bereits die erste Voraussetzung dafür geschaffen.

Mit der Erweiterung der Selbstbedienungsfunktionen für Einrichtungen ist es nun möglich die einer Einrichtung zugeordneten Subnetze für WLAN und / oder VPN freizugeben.

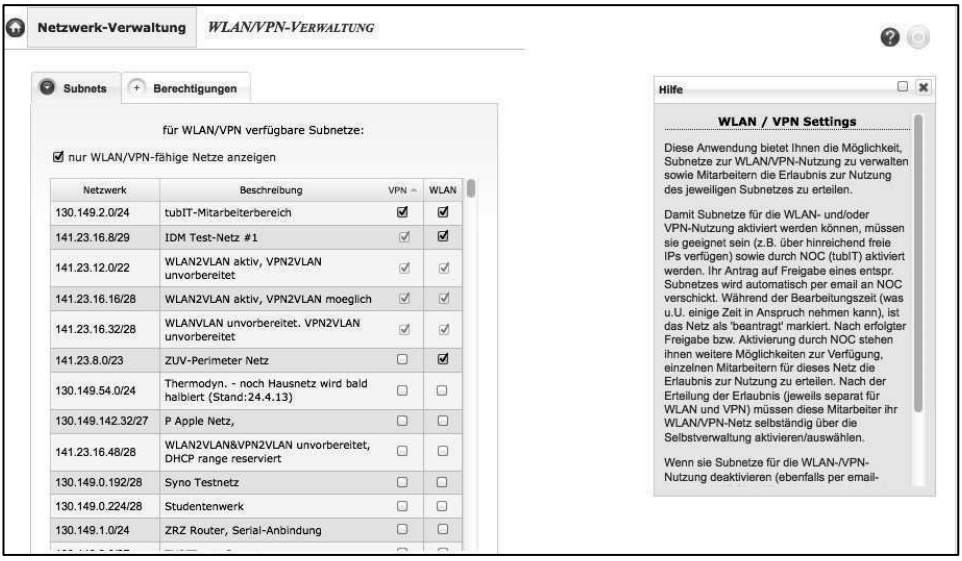

Abbildung 8: Freigabe von Subnetzen für VPN / WLAN

Der Netzwerkverwalter einer Einrichtung kann diese Einstellung jederzeit anpassen (Abbildung 8). Für alle Subnetze, die mindestens für eine der beiden Methoden freigeschaltet wurde, kann anschließend definiert werden, wer dieses Netz über die entsprechende Methode nutzen darf. Dabei ist die Auswahl der Nutzer nicht auf die Mitarbeiter der Einrichtung selbst begrenzt, sondern kann für jedes Mitglied der Hochschule gesetzt werden.

Jeder an der TU Berlin provisionierte Nutzer kann in seinem Profil einstellen, in welchem Netz er bei der Nutzung von WLAN oder VPN arbeiten möchte. Auch diese Einstellungen können jederzeit geändert werden und sind sofort wirksam.

Zur Realisierung dieser Funktionen sind einige technische Prozesse an der TUB angepasst worden. Die Grundfunktionalität wird dadurch erreicht, dass das WLAN an der TUB als eine Art „Overlay-Netz“ realisiert ist. Neben jeder klassischen Netzwerkdose ist an der TUB flächendeckend WLAN durch Cisco Thin-AP mit einer controllerbasierten zentralen Verwaltung realisiert worden. Damit nun aber die Nutzer direkt in ein spezielles VLAN geschaltet werden können, egal an welchem AccessPoint an der TUB sie sich verbinden, müssen alle in den 11 dezentralen Knoten gerouteten Layer-2 Netze zu den beiden zentralen Controllerstandorten übertragen werden. Hierzu wird von jedem der Knotenrouter zu den Routern, in denen die WLAN-Controller verbaut sind, ein EoMPLS-Tunnel aufgebaut, in dem die vom Knoten verwalteten Netze an den zentralen WLAN-Knoten übergeben werden. Die WLAN-Controller besitzen in jedem der dezentralen Netze jeder eine eigene IP sowie ein Interface und können damit den Traffic der WLAN-Nutzer direkt in ihr eigenes VLAN ausbrechen lassen. Zur Bestimmung des jeweiligen Netzwerkes ist im zentralen RADIUS-Server (Cisco ACS) ein Regelwerk hinterlegt, welches auf Gruppenmitgliedschaften der jeweiligen Nutzer überprüft und, wenn ein entsprechender Eintrag vorhanden ist, dem WLAN-Controller das ausgewählte VLAN des Nutzers übergibt. Für den Nutzer wird dann ein entsprechender Tunnel aufgebaut, mit dem seine Daten in das gewählte Netz übertragen werden.

Für die VPN-Nutzung werden die gleichen Techniken verwendet. Der Nutzer wird hierbei allerdings von Außen eine Verbindung mit dem Netzwerk der TUB herstellen. Damit dies für viele Nutzer gleichzeitig möglich ist, wird hierfür ein Cluster aus Cisco ASA eingesetzt, der auf die gleichen Regelsätze im RADIUS zurückgreift wie die WLAN-Lösung.

6 Ausblick

Wie bereits beschrieben, gibt es in der aktuellen Implementierung der Verwaltungswerkzeuge z. T. noch manuelle Prozesse wie z.B. die Beantragung der o.g. Orgnamen oder die Erstellung der Subnetze, die es gilt in der Zukunft weiter zu automatisieren oder zumindest zu optimieren. Im Betrieb sind diverse Nutzerwünsche in Bezug auf die IP-Verwaltung aufgetaucht, wie z.B. das Setzen bestimmter DHCP-Attribute zur Nutzung von DHCP-Ranges in VDI-Umgebungen usw. Diese Wünsche werden aufgenommen, gemeinsam mit den Nutzern priorisiert und umgesetzt.

Zur Zeit ist die Netzwerkverwaltung hauptsächlich Datensenke von Daten aus der zentralen Universitätsverwaltung. Ein Nutzen, den das Flächenmanagement bereits aus der Anwendung ziehen kann, sind die Rückmeldungen durch die Netzwerkbetreuer über (vermeintlich) falsch zugeordnete Räume. Ein weiterer Nutzen könnte jedoch auch ein Reporting der Anwendung an die Bauabteilung mit Kenndaten wie Verpatchungsgrad und Qualität/Modernität der Netzwerkkomponenten sein. Diese Reports könnten für die

Planung in Bezug auf Netzwerkanforderungen nützlich sein. Ein weiterer logischer Schritt ist die Einbeziehung der Telefonie in die Selbstbedienungsfunktion. Diese Integration ist aktuell mit einem physikalischen Umstecken der Leitungen im Wiring-Center nicht umsetzbar. In Zukunft werden jedoch neue Technologien auf Basis von VOIP oder LTE zum Einsatz kommen und weitere Möglichkeiten sowohl lokal, wie auch im mobilen Umfeld eröffnen.

Zuletzt sei noch erwähnt, dass schon heute Cisco Firewall-Service-Module zum Einsatz kommen, die über Kontexte mandantenfähig gemacht wurden und somit eine dezentrale Steuerung von Firewallregeln ermöglichen. Diese Funktionalität ist jedoch zur Zeit nicht in die restlichen Portalanwendungen integriert. Eine Kopplung mit den übrigen Funktionen wäre auch hier denkbar.

7 Fazit

Durch die geeignete Auswahl von Produkten und deren Integration in die eigene Verwaltungsinfrastruktur kann auch in einem großen Forschungsnetzwerk eine schnelle und flexible Gestaltung auf Basis von dezentralen Administratoren ermöglicht werden. Über, in unser Web-Portal integrierte, Anwendungen ist der Zugriff jeder Zeit von nahezu überall möglich. Dabei wird über das Identitäts- und Rollenmanagement sichergestellt, dass nur autorisierte Personen Zugriff auf die Konfiguration des Netzwerkes bekommen. Selbst die Vertretungsregelungen können dabei ohne Zutun der zentralen IT geregelt werden. Mit der direkten Kopplung an das Identitätsmanagement können auch Workflows für das Ausscheiden eines Nutzers oder dem Wechsel der Einrichtung realisiert werden.

8 Literaturverzeichnis

[HKR08b] T. Hildmann, O. Kao, and C. Ritter. Rollenbasierte Identitäts- und Autorisierungsverwaltung an der TU Berlin. 1. DFN-Forum Kommunikationstechnologien Verteilte Systeme im Wissenschaftsbereich, 2008.

[HR07] T. Hildmann and C. Ritter. TUBIS-Integration von Campusdiensten an der Technischen Universitat Berlin. PIK-Praxis der Informationsverarbeitung und Kommunikation, 30(3):145–151, 2007.

[RHK10] C. Ritter, T. Hildmann, O. Kao. Erfahrungen und Perspektiven eines rollenbasierten IdM , 3. DFN-Forum Kommunikationstechnologie, 26. Mai 2010

[CIS1] Cisco Catalyst 6500er Serie, http://www.cisco.com/c/en/us/products/switches/catalyst-6500-series-switches/index.html, Stand 20.04.2015

[CIS2] Cisco Adaptive Security Appliance 5500 Serie, http://www.cisco.com/web/DE/products/security/asa_5500_series_next_generation_firewalls.html, Stand 20.04.2015

[INF] Infoblox DNS-/DHCP Appliance Server, https://www.infoblox.com, Stand 20.04.2015

[FNT] FNT Command, http://www.fntsoftware.com/produkte/fnt-command, Stand 20.04.2015

Cloud Computing