Regionales Rechenzentrum Erlangen

Der IT-Dienstleister der FAU

Mitteilungsblatt 100

Geschichte der Datenübertragungs- und Kommunikationsnetze an der FAU

Entwicklungen zur flächendeckenden, leistungsstarken Netzinfrastruktur (Teil 2)

U. Hillmer

FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

Geschichte der Datenübertragungs- und Kommunikationsnetze an der FAU

Mitteilungsblatt des Regionalen Rechenzentrums Erlangen (RRZE)
der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)

Autor

Uwe Hillmer

Außenstellen

IZI (IT-Betreuungszentrum Innenstadt)
Bismarckstraße 1, 91054 Erlangen
IZN (IT-Betreuungszentrum Nürnberg)
Lange Gasse 20, 90403 Nürnberg
IZH (IT-Betreuungszentrum Halbmondstraße)
Halbmondstraße 6 , 91054 Erlangen
IZS (IT-Betreuungszentrum Süd)
Martensstraße 1, 91058 Erlangen

Benutzungsberechtigte Institutionen des RRZE

Friedrich-Alexander-Universität Erlangen-Nürnberg
Otto-Friedrich-Universität Bamberg
Universität Bayreuth
Hochschule Coburg
Georg-Simon-Ohm-Hochschule Nürnberg

Zum erweiterten Versorgungsbereich gehören:
Hochschule Ansbach
Hochschule Hof
Evangelische Hochschule Nürnberg

Herausgegeben im Auftrag des RRZE
ISSN 0172-2921

Mitteilungsblatt 100

Geschichte der Datenübertragungs- und Kommunikationsnetze an der FAU

Entwicklungen zur flächendeckenden, leistungsstarken Netzinfrastruktur (Teil 2)

U. Hillmer

Erlangen – Juli 2020

Kapitel

Liebe Leserinnen, liebe Leser,

die 50-jährige Geschichte des RRZE ist von enormen Entwicklungen und Fortschritten der Informationstechnologie im Allgemeinen und der Kommunikationstechnik im Besonderen geprägt. Heute erscheint es uns selbstverständlich, von jedem Platz der auf viele Standorte und Gebäude verteilten Universität Erlangen-Nürnberg mit jedem Partner Daten austauschen oder kommunizieren zu können. Die Grundlage hierfür bietet ein leistungsstarkes, nahezu flächendeckendes Kommunikationsnetz der FAU auf Basis der Internettechnik. Dieses ist natürlich nicht „vom Himmel gefallen", sondern Ergebnis einer langjährigen (auch heute noch nicht abgeschlossenen) Entwicklung, die teilweise sehr unterschiedlichen Phasen durchlaufen hat.

Schon zur Gründung des Rechenzentrums stellten sich erste Anforderungen an entfernte (remote) Zugriffe auf das zentral aufgestellte System, also nach Möglichkeiten einer Datenfernübertragung. Spätestens aber die Etablierung eines regionalen Rechensystems mit zwei Zentralsystemen und dem Versorgungsauftrag für die Nordbayerischen Hochschulen erforderte komplexere Lösungen im Sinne eines Kommunikationsnetzes. Technische Entwicklungen ermöglichten dann im Laufe der Jahre verschiedene Gestaltungen sowie Ausbau, Leistungssteigerungen oder funktionale Erweiterungen. Heute ist das Kommunikationsnetz eine tragende Säule des IT-Dienstleisters RRZE und aus dem Betrieb der Universität nicht wegzudenken.

Das 50-jährige Jubiläum des RRZE gab Anlass, auf die Entwicklung der Kommunikationstechnik der vergangenen Jahre zurückzublicken und die konkreten Ansätze an der FAU zu betrachten.

Die in einem ersten Teil erschienene Dokumentation der Anfangsjahre (1968 – 2012) wird nun durch den hier vorliegenden zweiten Teil ergänzt, der sich mit den Entwicklungen ab der Jahrtausendwende (2000 – 2018) befasst. Diese waren zwar im Vergleich zu den Anfangsjahren mit weniger grundsätzlichen, technischen Veränderungen verbunden, dafür aber umso mehr, doch nicht weniger spannend, von Ausbau und Leistungssteigerungen im Zusammenhang einer sich allgemein durchsetzenden Ethernet- und Internettechnologien geprägt.

So finde ich zum Beispiel die Anzahl von inzwischen rund 150.000 versorgten Endgeräten beeindruckend, erreichte Übertragungsgeschwindigkeiten von bis zu 100 Gbit/s faszinierend (Ich erinnere mich noch gut an die Zeit von Dialogsitzungen über Akustikkoppler mit 300 bit/s) sowie die trotz allen Wandels gewährte Betriebsstabilität mit durchschnittlichen Netzverfügbarkeiten oberhalb 99.95% (seit Aufzeichnungsbeginn 2001) und einer jüngeren Tendenz in Richtung 100% äußerst erfreulich.

Uwe Hillmer, der Autor der Dokumentation und einer der ersten Mitarbeiter des Rechenzentrums, beschreibt die Entwicklungen der Kommunikationsnetze an der FAU in ihrem zeitlichen Kontext, erläutert die grundlegenden Techniken und skizziert deren strukturelle Umsetzungen. Dabei beschränken sich die Darstellungen nicht allein auf die Kommunikationsnetze, sondern setzen sie in Beziehung zur allgemeinen Entwicklung des Rechenzentrums, wodurch sie auch aufzeichnen, wie aus dem Rechenzentrum der IT-Dienstleister der Universität geworden ist.

Im Jahr 2000 begann auch meine Zeit als Technischer Direktor des RRZE, sodass die hier im zweiten Teil beschriebene Historie weitgehend meiner Wirkungszeit entspricht. Gerne und auch mit gewissem Stolz blicke ich darauf zurück. Die Dokumentation wird dazu beitragen, positive Erinnerungen wach zu halten.

Es wünscht auch Ihnen eine interessante Lektüre

Ihr

Dr. Gerhard Hergenröder
Technischer Direktor des RRZE

Einführung & Überblick

Einführung & Überblick

Das 1968 gegründete **R**egionale **R**echen**z**entrum **E**rlangen (RRZE) der **F**riedrich-**A**lexander-**U**niversität Erlangen-Nürnberg (FAU) feierte im Jahre 2018 sein 50-jähriges Bestehen. Dabei kann heute auf eine erfolgreiche Entwicklung zurückgeblickt werden, die sowohl von allgemeinen technischen Fortschritten als auch von enormen Wandlungen und Erweiterungen des Anwendungsspektrums geprägt wurde. Hatte das Rechenzentrum ursprünglich die Aufgabe, über einen einzelnen „Großrechner“ der Universität zentrale Rechenleistung zur Verfügung zu stellen, entwickelte es sich im Laufe der Jahre zu einem umfassenden Dienstleister der **I**nformations**t**echnologie (IT), der nicht nur mit dem Betrieb zahlreicher, unterschiedlicher Rechensysteme (Server) und deren Vernetzung befasst ist, sondern darüber hinaus vielfältige Unterstützung in den Bereichen der elektronischen Informationsverarbeitung bietet.

Für die Entwicklung des Rechenzentrums und die Bewältigung seiner Aufgaben wurde es bald unerlässlich, Möglichkeiten zum Datenaustausch und zur Kommunikation bereitzustellen. Anfangs stellte sich die Aufgabe, den zentral aufgestellten Rechner von entfernten Standorten der Universität aus (remote) nutzbar zu machen. Mit dem regionalen Auftrag (etwa ab 1976) erweiterte sich die Aufgabe um die Schaffung von Zugriffen für die nordbayerischen Hochschulen in Bamberg, Bayreuth, Coburg und Nürnberg, wobei das dann einsetzende Aufkommen zusätzlicher Rechnersysteme (PCs, Workstations, Server) zunehmend flexiblere Kommunikationsstrukturen erforderte. Das aktuelle Kommunikationsnetz orientiert sich schließlich an einer flächendeckenden, leistungsstarken Verbreitung von Anschlüssen für die Arbeitsplatzrechner und Server innerhalb der Universitäten sowie Übergängen zu nationalen und internationalen Netzen. Auf-, Ausbau und Betrieb adäquater Kommunikationsstrukturen hatten und haben also für das RRZE eine fundamentale Bedeutung, sodass es sich lohnt, die entsprechende Historie gezielt zu betrachten.

Die unter vielen Aspekten beeindruckende Entwicklung der Kommunikationstechnik sowie deren Anwendungen an der Friedrich-Alexander-Universität stehen im Mittelpunkt der vorliegenden Aufarbeitung „Geschichte der Datenübertragungs- und Kommunikationsnetze an der FAU“. Sie gliedert sich in verschiedene inhaltlich und zeitlich definierte Phasen, die im jeweiligen Kontext des Rechenzentrums, der zugrundeliegenden Technologien sowie der konkreten Umsetzungen an der FAU beschrieben werden.

Neben persönlichen Erinnerungen und Erfahrungen des Autors dienten vorrangig Originaldokumente, darunter Aufzeichnungen, Mitteilungen, Vortragsunterlagen des RRZE oder auch Handbücher von Geräteherstellern als Informationsquellen. Die ihnen entnommenen Illustrationen sind daher von unterschiedlicher Qualität und Gestaltungsart. Sie zeigen zwar ein etwas inhomogenes Gesamtbild, sind dafür aber authentisch.

Die aus der Perspektive des RRZE beschriebene Historie gibt auch einen Teil der generellen Entwicklung von Techniken und Strukturen der Datenkommunikation wieder und beschreibt somit auch allgemeine Entwicklungen von der „klassischen" Datenfernverarbeitung zu den vielfältigen Kommunikationsformen etwa im Rahmen des heute allseits bekannten Internet.

Der erste, 2018 erschienene Teil beschreibt die Entwicklungen von der Gründung des Rechenzentrums bis zur Jahrtausendwende (bzw. etwas darüber hinaus) und enthält bezüglich seiner Grundlagen sehr unterschiedliche Techniken. Sie reichen von „einfacher" serieller Datenübertragung über die Mehrfachnutzung von Fernstrecken, eine regionale bis internationale Vernetzung per X.25-Protokoll, lokales Breitbandnetz, „klassisches" Ethernet mit Koaxialkabeln bis zu einem per ATM gesteuerten Datentransfer und den ersten Einsätzen des Internetprotokolls an der FAU. Die Übergänge zwischen den verschiedenen Phasen wurden stets in migrativen Schritten vollzogen. Dadurch blieb der Netzbetrieb weitgehend unbeeinträchtigt und den Benutzern stand jederzeit eine zuverlässige Kommunikationsbasis zur Verfügung. Dabei waren mit den Entwicklungen auch immer Ausbau und Leistungssteigerungen des Kommunikationsnetzes verbunden.

Der zweite, hier vorliegende Teil stellt die daran anschließenden Entwicklungen der Vernetzung dar. Spätestens nach dem Jahrtausendwechsel begannen sich eine fortentwickelte Ethernet-Technik sowie das Internetprotokoll generell als Lösungsgrundlage für Kommunikationsnetze durchzusetzen. Zudem sorgte an der FAU die Realisierung einer strukturierten Verkabelung für die flexible Bereitstellung erforderlicher Übertragungsmedien. Auf Basis einer in den Prinzipien gleichbleibenden Technik lassen sich die Fortschritte hauptsächlich durch Ausbau (geografische Ausbreitung, Erhöhung der Versorgungsdichte), Leistungssteigerungen (neue Gerätetechnologien, gesteigerte Übertragungsgeschwindigkeiten) oder auch überarbeitete Konzepte zur Netzstrukturierung (hierarchischer Aufbau) oder Betriebsgestaltung (Regularien, Sicherheitsmaßnahmen usw.) kennzeichnen. Den stetig wachsenden Anforderungen an das Rechenzentrum als IT-Dienstleister der Universität nachzukommen, bedeutete eine ständige Herausforderung an die Gestaltung des Kommunikationsnetzes der FAU.

Die beiden Teile dieser Dokumentation lassen sich nicht nur in technischer Hinsicht charakterisieren. Der erste Teil entspricht zeitlich der Wirkungsperiode von Dr. Franz Wolf als Technischem Direktor des Rechenzentrums bzw. des RRZE. Seine Verdienste um Pionier- und Aufbauarbeiten in Zeiten rasanter und umwälzender Entwicklungen von EDV und Kommunikationstechnik sind nicht hoch genug einzuschätzen. Nachdem er sich im Ruhestand für die Einrichtung der Informatik-Sammlung Erlangen (ISER) stark engagiert hatte, ist er im Dezember 2019 leider verstorben. Die „Geschichte der Kommunikationsnetze", die er in seiner Leitungsfunktion nicht unerheblich mitgestaltet hat, sei ihm im Nachhinein noch besonders gewidmet.

Im Jahr 2000 trat Dr. Gerhard Hergenröder in Ablösung von Dr. Franz Wolf sein Amt als Technischer Direktors des RRZE an. Somit beschreibt der zweite Teil dieser Dokumentation auch den neuen, von ihm wesentlich bestimmten Zeitabschnitt, der sich vor allem durch die Entwicklung des RRZE vom Hochschulrechenzentrum (Bereitstellung von Rechenleistung) zu dem IT-Dienstleister der Universität mit einem äußerst vielfältigen Angebotsspektrum charakterisieren lässt. Die Geschichte der Kommunikationsnetze bedeutet dabei zwar nur einen Teilaspekt, vermittelt aber in ihrem zweiten Teil auch einen Eindruck über die Gesamtentwicklung in der „Ära Hergenröder“. Wenn er 2020 in den wohlverdienten Ruhestand eintritt, kann er auf eine erfolgreiche Zeit zurückblicken aber auch mehr Gelegenheit finden, sich bei hoffentlich noch lange währender Gesundheit seinen Hobbies wie beispielsweise dem Schlagzeugspielen zu widmen.

Netzstrukturen auf Basis von Ethernet- und IP-Switching 2000 – 2012

6. Netzstrukturen auf Basis von Ethernet- und IP-Switching / 2000 – 2012

Mit dem Start in ein neues Jahrtausend begann die Zeit von Dr. Gerhard Hergenröder als Technischem Direktor des RRZE, der den seit seiner Gründung das Rechenzentrum leitenden Dr. Franz Wolf ablöste. Nicht erst mit diesem Wechsel, aber dann doch deutlich forciert, begann der Wandel des RRZE zu einem generellen IT-Dienstleister der Universität, dessen Angebote immer mehr über das ursprüngliche Kerngeschäft des Betreibens zentraler oder dezentraler Rechensysteme hinausgingen. So wurden z. B. mit der Ausbildung von Fachinformatikern, der Bereitstellung von Webservern für Institute, der Eingliederung der EDV der zentralen Universitätsverwaltung (ZUV) oder der Einführung eines Zugangs- und Verwaltungssystems für Studierende (mein campus) neue Aufgaben übernommen, um nur wenige zu nennen. Damit verbunden war auch eine Ausweitung der Nutzerkreise bzgl. Anzahl, Art und räumlicher Verteilung einschließlich ihrer Endsysteme sowie ein dadurch wachsender Bedarf an Service- und Kommunikationsleistungen.

Entsprechend stiegen also auch die Anforderungen an die vom RRZE bereitgestellte und betriebene Kommunikationsinfrastruktur der FAU, etwa bzgl. der Anzahl und Art zu versorgender Endgeräte, ihrer geografischen Ausbreitung sowie an die Betriebsstabilität und Leistungsfähigkeit. Die genannten Aspekte waren in dem hier betrachteten Abschnitt natürlich nicht neu. Spätestens mit der Einführung einer strukturierten Verkabelung (vgl. Teil 1, Kapitel 4) verfolgte das RRZE das Ziel einer flächendeckenden Infrastruktur, also einer weitgehend vollständigen, bedarfsgerechten Versorgung mit Netzzugängen in allen Bereichen der Universität. Auf dem Weg dahin wurde, je nach Möglichkeiten (finanzieller oder baulicher Art), kontinuierlich vorangeschritten. Diese ideale Zielsetzung gilt auch heute noch, wobei aktuelle Bedarfsentwicklungen oder das Hinzukommen neuer Standorte der FAU zu berücksichtigen sind. Ebenso ist das RRZE ständig bestrebt die Leistungsfähigkeit der Struktur zu erhöhen, die sich vornehmlich in verfügbaren Übertragungsgeschwindigkeiten der verschiedenen Netzabschnitte ausdrückt. Dies erfordert ein generelles Schritthalten mit technologischen Entwicklungen sowie deren Einbringung in vorhandene oder neuzugestaltende Strukturen, möglichst ohne Beeinträchtigung des jeweils aktuellen Betriebs.

Der in diesem Kapitel betrachtete Abschnitt (2000-2012) überschneidet sich teilweise mit der unter dem Titel „Universelles Transfernetz (ATM), Virtuelle LANs (LANE)“ (Teil 1, Kapitel 5) beschriebenen Entwicklungsphase (1995-2011). Die dort behandelte ATM-Technik war zur Zeit ihrer Einführung den verfügbaren Ethernet-Möglichkeiten in mehreren Gesichtspunkten deutlich überlegen, etwa durch Universalität (LAN- und

WAN-Fähigkeit), Leistungsstärke (Geschwindigkeitsspektrum von 155 Mbp/s bis 2.4 Gbp/s), Flexibilität (Organisation virtueller LANs mit verteilten Segmenten (LANE)) oder Videotauglichkeit durch gesicherte Einhaltung benötigter Übertragungsparameter. Sie war daher für das Netz der FAU bzw. deren Grundstruktur (Backbone) bestens geeignet. In lokalen Bereichen, d. h. zur Verteilung von Anschlüssen für Nutzerzugänge, wurden dabei LAN-Switche mit ATM-Schnittstellen zum Backbone sowie Ethernet-Ports zu den Endgeräten eingesetzt. Die allgemeine Entwicklung der Ethernet-Technik konnte im Laufe der Zeit bezüglich Leistung und Flexibilität nach und nach aufholen und in diesem Zusammenhang vor allem für Nahbereiche vergleichbare Alternativen zu ATM-Lösungen bieten. Da die Technik zudem als „unkomplizierter“ galt und sich am Markt zunehmend durchzusetzen begann, leitete das RRZE einen Migrationsprozess zur Ablösung von ATM-Strukturen durch Ethernet-basierte Konstrukte ein (nicht zuletzt auch eine „Kostenfrage“). Der in diesem Kapitel beschriebene Wandel erfolgte zunächst in lokalen Bereichen, dann aber auch im Kontext von Weitverkehrsverbindungen. Für dann nicht mehr mögliche ATM-spezifische Anwendungen (z. B. für Videoübertragungen) mussten andere Lösungen gefunden werden.

Mit der Ausnahme einzelner, dedizierter Funkverbindungen (Richtfunkstrecken) verwendete das Kommunikationsnetz gemäß der strukturierten Verkabelung fest installierte Übertragungsmedien, wie Glas- oder Kupferkabel. Durch entsprechende Entwicklungen von Funkübertragungen wurde es möglich, solche „drahtgebundenen“ Netze durch „nicht drahtgebundene“ (wireless) Segmente zu ergänzen. Diese Wireless LANs (WLANs) wurden vom RRZE zunächst zur Erschließung von unzugänglichen, (noch) nicht verkabelten Bereichen, dann zur Schaffung von Zugängen in öffentlichen Räumen (z. B. für Studierende) genutzt, bis schließlich entsprechende Entwicklungen von Endgeräten (Laptops, Tablets, Smartphones usw.) sowie damit verbundene Nutzungsformen (mobile Kommunikation) Anforderungen an standortunabhängige Netzzugriffe in allen Bereichen der Universität stellten. Auf- und Ausbau entsprechender WLAN-Strukturen wurden somit zu einem neuen, ebenfalls wichtigen Bestandteil von Netzstruktur und -betrieb bzw. zu einer Erweiterung des RRZE-Dienstleistungsspektrums.

Der innere Aufbau eines Kommunikationsnetzes ist zwar für Benutzer kaum sichtbar, für einen funktionierenden und beherrschbaren Betrieb aber äußerst wichtig. Er muss daher sorgfältig unter verschiedenen Gesichtspunkten geplant werden. Das RRZE orientiert(e) sich bei der Gestaltung des FAU-Netzes auch an allgemeinen Vorschlägen, wie sie etwa vom Router-Hersteller Cisco propagiert wurden. Obwohl diese sich hauptsächlich auf Lösungen für Campusbereiche konzentrierten, also auf solche, die in sich zusammenhängend und weitgehend durchgängig gestaltbar waren, regten die Grundideen bezüglich hierarchischer, in Core, Distribution und Access gegliederter

Netze zum Entwurf eines auch auf die über mehrere Areale verteilte Universität anwendbaren Modells an. Dieses diente als Muster für konkrete Umsetzungen und lieferte neben Leitlinien zur Strukturierung auch begriffliche Grundlagen zur Beschreibung verschiedener Aufgabenbereiche des Kommunikationsnetzes.

6.1. Entwicklung des Rechenzentrums zum IT-Dienstleister der FAU

So, wie allgemein aus der Elektronischen Datenverarbeitung (EDV) eine umfassende Informationstechnologie (IT) wurde, wandelten und erweiterten sich auch die Aufgaben des RRZE im Laufe der Jahre vom Bereitstellen zentraler Rechenleistung zum Erbringen vielfältiger Dienstleistungen im Kontext von elektronischer Informationsverarbeitung und Kommunikation. Die unter vielen Aspekten wachsenden und sich verändernden Anforderungen erforderten flexibles, vorausschauendes Handeln sowie Schritthalten mit Bedarfsentwicklungen und technologischen Fortschritten. Als Träger zentraler, fachlicher Kompetenz wurde aus dem Rechenzentrum schließlich *der* IT-Dienstleister der FAU Erlangen-Nürnberg.

6.1.1 (Re-)Zentralisierte Systembetreuung

Bereits Anfang der 90er Jahre führte das Aufkommen von PCs und Workstations zu Überlegungen über eine sinnvolle Aufgabenverteilung zwischen dem zentralen Rechenzentrum und den dezentralen Einrichtungen der Universität (Institute, Lehrstühle usw.) und dem Konzept einer mehrstufigen, kooperativen DV-Versorgung (vgl. Teil 1, Kapitel 4.1). Der damit verbundene Trend zur Dezentralisierung kehrte sich aber mit steigernder Komplexität der Endsysteme oder dem Bedarf an verstärkter Vernetzung bald wieder um. So kamen am RRZE neben dem Betreiben eigener zentraler Server auch Aufgaben der Betreuung in Nutzerbereichen verteilter Systeme hinzu. Ausgestattet mit entsprechender Kompetenz konnte es so auch in diesen Anwendungsfeldern für Kontinuität sowie stabilen und aktualisierten Betrieb sorgen. Dies zeigte sich zum Beispiel 2001 in der Gründung zwar verteilter, aber im RRZE integrierter Betreuungszentren: IZI (IT-Betreuungszentrum Innenstadt) und IZN (IT-Betreuungszentrum Nürnberg).

Ein weiteres Beispiel für die Zentralisierung bzw. eine Bündelung von Kompetenzen und Zuständigkeiten war die Übernahme des Sachgebiets Datenverarbeitung (SG DV) der Zentralen Universitätsverwaltung (ZUV) durch das RRZE. Um dabei so viel Synergie wie möglich zu erreichen, wurde das SG DV nicht einfach an das RRZE angegliedert, sondern die Aufgaben wurden – wo möglich – in die bereits vorhandenen Arbeitsgruppen des RRZE integriert. Neben einem enormen Zuwachs an Datenbanksystemen kam für das RRZE die technische Betreuung der entsprechenden Fachanwendungen als neue Aufgabe hinzu. Daher wurden sowohl Betrieb als auch Konzeption der Datenbanken und der dazugehörigen Anwendungen in der neuen Abteilung „Datenbanken und DV-Verfahren“ am RRZE zusammengefasst. Um die Zusammenarbeit mit den Kunden zu optimieren, bezogen die meisten Mitarbeiter dieser Abteilung ihren Arbeitsplatz im neu gegründeten IT-Betreuungszentrum

Halbmondstraße (IZH) in direkter Nähe der Nutzer. Nachdem das RRZE bereits seit 1995 das damalige zentrale Rechensystem der ZUV, eine Anlage Siemens 7580 BS2000, in seinen Räumen beherbergte und mitbetrieb, übernahm es mit dieser 2005 begonnenen Integration auch die Betreuung dort inzwischen zahlreich vorhandener Arbeitsplatz- und Serversysteme.

6.1.2 Nichtsystemgebundene Themen und Dienstleistungen

Wie im Zusammenhang mit der Übernahme von Aufgaben der ZUV bereits angedeutet, beschränkte sich die Ausweitung des Dienstleistungsspektrums nicht allein auf die Betreuung neu hinzukommender Rechensysteme und deren Standardsoftware, sondern beinhaltete auch zunehmend völlig unterschiedliche, von konkreten Rechnern unabhängige Angebote im Kontext der IT. Dazu seien hier stellvertretend verschiedene, markante Punkte angeführt.

Fachinformatikerausbildung

Schon seit seiner Gründung befasste sich das RRZE mit der Vermittlung von EDV- bzw. IT-Kenntnissen unter anderem durch entsprechende Veröffentlichungen, Kurse, Kolloquien oder Informatiklehrveranstaltungen für Angehörige der Universität. Bereits 1998 wagte sich dann das RRZE auf ein neues Terrain und stellte in Zusammenarbeit mit der Berufsschule Erlangen drei Ausbildungsplätze für Fachinformatiker (Fachrichtung Systemintegration) zur Verfügung. Die ersten „Azubis“ erlangten dann 2001 äußerst erfolgreich ihren Abschluss. Dieser jeweils durch drei Jahrgänge (neun Auszubildende) belegte Ausbildungsdienst, aus dem überdies einige Fachkräfte als Mitarbeiter des RRZE und der Universität hervorgingen, bedeutet auch bis heute eine Erfolgsgeschichte.

Zweiter Abschlussjahrgang 2002

Webdienst

Das World Wide Web (WWW) wurde, als eine seiner bedeutendsten Anwendungen, oft mit dem Internet identifiziert und trug nicht unerheblich zu dessen Verbreitung und Popularisierung bei. Während anfangs entsprechende Server und abrufbare Informationsseiten noch relativ einfach zu betreiben und gestalten waren, stellten schon bald wachsende Ansprüche und Möglichkeiten hohe Anforderungen an Pflegeaufwand und Fachwissen. So wurden zunächst (Stand 2005) rund zehn Millionen Dokumente auf

über 480 Webauftritten verschiedener Einrichtungen der Friedrich-Alexander-Universität im Internet bereitgestellt. Davon hostete und betreute das RRZE 446 aktive Webauftritte mit über sechs Millionen Dokumenten. Es wurde aber zunehmend ein fundiertes Expertenwissen erforderlich, um qualitativ hochwertige Webseiten zu entwickeln, die zudem den umfangreichen gesetzlichen Vorgaben entsprechen. Auch die Wünsche nach einem ansprechenden Design wurden lauter. Nicht jeder Webbetreuer war noch in der Lage, die immer anspruchsvoller werdenden Anforderungen zu realisieren. So kam es aufgrund unzureichender Kenntnisse der dezentralen Webseitenentwickler an der FAU im Jahr 2004 zu einem Arbeitszeitverlust von durchschnittlich 80 Mitarbeiterwochen (vgl. Jahresbericht 2005 des RRZE [JB-2005]). Vor diesem Hintergrund stimmte die Hochschulleitung im Sommer 2005 dem Vorschlag des RRZE-Webteams zu und genehmigte ein Projekt zur Entwicklung und Realisierung eines Webbaukastens, der künftig allen Webmastern der einzelnen Einrichtungen die Erstellung qualitativ hochwertiger Webauftritte erleichtern sollte. In der weiteren Entwicklung wurden dann auch zunehmend verteilte Webserver auf zentrale Systeme übertragen und als Dienst des RRZE betrieben und gepflegt. Es sei noch erwähnt, dass das RRZE in diesem Zusammenhang auch die Betreuung des Internetauftritts der Stadt Erlangen übernommen hat. Schon früh legte das RRZE bei der Gestaltung von Webseiten großen Wert auf Barrierefreiheit (Publikationen ab 1994 im WWW). Dies wurde beispielsweise 2005 durch die Vergabe eines goldenen BIENE-Awards (BIENE steht für „Barrierefreies Internet eröffnet neue Chancen“) der Aktion Mensch und der Stiftung Digitale Chancen für die besten deutschsprachigen barrierefreien Internetauftritte belohnt. Das RRZE erhielt in diesem Jahr übrigens bundesweit als einziges Hochschulrechenzentrum diese Auszeichnung. Zudem wurde ihm im gleichen Jahr im Rahmen des Deutschen Multimedia Awards (DMMA) für herausragende deutschsprachige Internetanwendungen ein Sonderpreis zur Barrierefreiheit verliehen (an der Vergabe waren beteiligt: Der Bundesverband Digitale Wirtschaft (BVDW) e.V., der Deutsche Multimedia Kongress (DMMK) und der Kommunikationsverband).

RRZE-Mitarbeiter mit Biene-Award, 2005

Hochschulweite Verwaltungsdienste

Mit der Übernahme bzw. Eingliederung der ZUV-EDV in das RRZE wurden auch verschiedene, hochschulweite Projekte begonnen, die Verwaltungsprozesse und zugehörige Dienstleistungen neu definieren, IT-technisch gestalten sowie allgemein verfügbar machen sollten. Dazu gehörten das 2006 mit dem Ziel des Aufbaus eines uniweiten Identity Managements gestartete „IDMone“ oder das 2007 hinzugekommene Projekt Campus IT (CIT), das zunächst die IT-Unterstützung für den Bologna-Prozess zu leisten hatte. Der Bologna-Prozess bedeutet eine sehr flexible Möglichkeit der Zusammenstellung von Studiengängen aus unterschiedlichen Fachgebieten, die letztlich nur mit Hilfe automatisierter Verfahren und passender Benutzer-Schnittstellen umzusetzen war bzw. ist. So wurde mit dem 2008 in Betrieb gegangenen und in der Folge weiter entwickelten IdM-Portal eine zentrale, webbasierte Anlaufstelle für Studierende, Beschäftigte und Administratoren rund um die Verwaltung der identitätsbezogenen Daten und IT-Dienstleistungen geschaffen, während die Online-Serviceplattform „mein campus“ eine Schnittstelle bereitstellt, die Verfahren wie Prüfungsverwaltung, Studierendenverwaltung, Bewerbung und Zulassung sowie Veranstaltungsverwaltung mittels Selbstbedienungsfunktionen im Web für alle Studierenden der Universität Erlangen-Nürnberg, aber auch für Lehrende und Fachanwender zugänglich macht(e).

Anmeldemaske „mein campus“, 2009

Druckzentrum

Bereits mit der Gründung des Rechenzentrums gehörten das Ausgeben von Texten (Drucken) oder Zeichnungen (Plotten) auf Papier zu den elementaren Diensten und entsprechende Peripheriegeräte zur Grundausstattung seiner zentralen Rechensysteme (vgl. Teil 1, Kapitel 1). Mit dem Betrieb verteilter Arbeitsplatzsysteme ging z. B. durch am Markt verfügbare, erschwingliche Drucker, auch eine gewisse Dezentralisierung der Ausgabefunktionen einher. Es blieb in diesem Zusammenhang aber dennoch ein gewisser Bedarf an zentral erbrachten Leistungen, der sogar noch zunehmen sollte. Das Rechenzentrum trug dem mit der Einrichtung eines Druckzentrums Rechnung, das im Jahr 2010 kräftig ausgebaut und modernisiert wurde. Dessen Dienste umfassen das Drucken zahlreicher Dateiformate (TIFF, JPG, BMP, PNG sowie Postscript- und PDF-Dateien), das Erstellen großformatiger Poster oder im umgekehrten Vorgang die

Großformatiger Tintenstrahldrucker, 2011

Eingabe und Umwandlung (Scannen, Digitalisierung) von Vorlagen im Format DIN A4/DIN A3. Zur technischen Ausstattung wurden ein Tintenstrahldrucker für Großformate (Stylus Pro 11880 von EPSON), ein Farblaserdrucker (Canon image RUNNER ADVANCE C5045i), ein Großformat-CAD-Plotter (HP 1055) sowie eine Stapelschneidemaschine (IDEAL 4850) für den Zuschnitt beliebiger Flyer-Größen beschafft. Die Dienste werden intensiv genutzt. So wurden 2011 im Druckzentrum über Posteraufträge rund 4.500 qm Papier geplottet und über weitere Druckaufträge ca. 1.250.000 Schwarzweiß- und Farblaserausdrucke auf DIN-A4-Papier ausgegeben. Die Zahl der Poster- und Druckaufträge belief sich dabei auf insgesamt rund 2.600.

Multimediazentrum (MMZ)

Das RRZE befasste sich im Rahmen von Hochgeschwindigkeitsprojekten schon frühzeitig nicht nur mit der technischen Basis, sondern auch mit entsprechenden Anwendungen, insbesondere mit (Live-)Übertragungen von Videos. So entstanden in Zusammenarbeit mit dem Bayerischen Rundfunk die Aufzeichnungen zu Uni-TV und es wurden erste Vorlesungen innerhalb der FAU übertragen (vgl. Teil 1, Kapitel 5.4). Über die Projektrahmen hinaus regten die Ergebnisse und gewonnenen Erfahrungen zur Weiterführung an und mündeten in die Gründung einer in der Abteilung Kommunikationssysteme des RRZE angesiedelten Arbeitsgruppe Multimediazentrum (MMZ), die sich mit dem Aufbau und Angebot eines neuen Dienstleistungsspektrums befasste. Das MMZ wurde zur Anlaufstelle für Fragen zum Thema Multimedia an der Friedrich-Alexander-Universität. So hatte das MMZ zum Beispiel 2010 den Dienst „Vorlesungsaufzeichnungen“ erfolgreich etabliert und ein Videoportal eingerichtet, über das ganze Reihen von Vorlesungen abgerufen werden können. Durch die Verknüpfung mit iTunesU, einer 2007 von der Firma Apple ins Leben gerufenen Plattform zur kostenlosen Bereitstellung und Verwaltung von Lernmaterialien, erlangte die FAU auch einen Zugang zu internationalem Publikum.

Als Ersatz für das frühere Multimedialabor wurden 2007 am RRZE zwei etwas in die Jahre gekommene Seminarräume zum neuen „E-Studio“ (die Assoziation mit E-Learning ist durchaus gewollt) der FAU umgebaut. Eingerichtet wurden:

- das „E-Studio“ mit reichlich Aufnahme- und Wiedergabetechnik,
- eine mit Übertragungs- und Produktionstechnik ausgestattete „E-Regie“,
- ein für Videokonferenzen ausgestattetes „E-Zimmer“.

Die Feuertaufe bestanden die neuen Räumlichkeiten mit ihrer Technik bei der Langen Nacht der Wissenschaften. Die im Audimax von Prof. Rudi van Eldik aufgeführten chemischen Zaubertricks wurden mit HDTV-Kameras nach Uni-TV-Manier in das E-Studio übertragen.

Zum Einsatz kamen HD-Kameras von JVC und ein 42“-Studiomonitor von Barco mit der vollen HD-Auflösung von 1.920 x 1.080 Bildpunkten. Die HD-Signale, die eigentlich eine Bandbreite von 1,6 Gbit/s haben, wurden durch Codecs auf eine Bandbreite von 500 Mbit/s komprimiert. Um den hohen Anforderungen an die Dienstqualität gerecht zu werden, wurden sie als Gigabit Ethernet über eine separate Faser transportiert. Die Bilder aus dem Audimax waren brillant und die Veranstaltung fand großen Anklang. Im darauffolgenden Jahr 2008 wurde das E-Studio offiziell eingeweiht. Auf Einladung des RRZE kamen unter anderem Alt-Präsident (Prof. Dr. Karl-Dieter Grüske) und Alt-Kanzler (Thomas A.H. Schöck) der FAU, der Dekan der Technischen Fakultät (Prof. Dr. Johannes Huber), Vertreter der Zentralen Universitätsverwaltung, der Stadt Erlangen, des Wissenschaftsministeriums, des Bayerischen Rundfunks und der Virtuellen Hochschule Bayern.

Führung durch das E-Studio (li.), Blick in die E-Regie und in den Vortragsraum, Einweihung 2008 (re.)

6.1.3 Rechnerlandschaft

Der Betrieb von Rechenanlagen und die Bereitstellung von Rechnerkapazitäten sowie die damit verbundene Pflege zugehöriger System- und Anwendungssoftware gehörte und gehört, neben der Betreuung und Beratung der Benutzer, zu den Kernaufgaben eines zentralen Universitätsrechenzentrums. Dabei traten an die Stelle der anfangs im Mittelpunkt stehenden universellen Großrechner (bspw. CDC 3300 zur Gründung des RZ, 1968) im Laufe der Entwicklung verschiedene Serversysteme zur dedizierten Lösung von Dienstaufgaben gemäß des sich ständig erweiternden Anforderungsspektrums. (Diese Entwicklung wurde bereits in den 90er Jahren mit der begonnenen Migration zu Unix eingeleitet, vgl. Teil 1, Kapitel 4).

Zentrale Systeme

Im Rahmen der zentralen Dienste betrieb und betreibt das RRZE eine ganze Farm von Servern. Einige dieser Server bieten Dienste an, die direkt sichtbar sind, wie WWW (auch für den Webserver der Homepage der Universität), Network News und E-Mail sowie eine ganze Reihe von Datenbankdiensten oder die Archivierungs- und Backupdienste. Viele Server arbeiten jedoch eher im Hintergrund. Die Zusammenstellung und Aufgabenverteilung der Server unterliegt mit der Zeit gewissen Veränderungen, die vornehmlich durch enorme Entwicklungen der Rechnertechnik sowie steigende Anforderungen an die Systeme motiviert sind. Die Tabelle aus dem Jahr 2005 vermittelt als Beispiel einen Eindruck über die (zu der Zeit) wichtigsten Dienste und deren Server.

Dezentrale Systeme

Neben den zentralen, überwiegend im Rechnerraum der ehemaligen Universalrechner TR440-3 bzw. IBM 4361/3090 im Informatikhochhaus aufgestellten Serversysteme (vgl. Teil 1, Kapitel 2-4) unterstützt(e) das RRZE auch den Betrieb dezentraler Systeme. Dies galt nicht nur für die eigenen, abgesetzten Betreuungszentren (IZI, IZN,

Dienste	Anzahl	Typ	CPUs/MHz	Hauptspeicher MB	Plattenkapazität GB
Backup, Archiv					
Backup, Archiv	1	SUN Fire V440	4 x 1.600	16.984	3.044
Dialog					
Dialog	1	SUN Fire V440	4 x 1.600	16.984	292
SUNRay, intern	1	SUN Fire V490	4 x 1.350	16.984	292
Datenbank					
Orakel-DB-Server	1	SUN ULTRA2	2 x 300	384	22
Datenbank	2	HP DL385	2 x 2.000	3.072	292
Datenhaltung					
Fileserver	1	SUN E450	2 x 250	512	270
Info					
WWW-PROXY	2	SUN E450	2 x 400	512	63
WWW	1	SUN E450	2 x 300	768	200
WWW	1	SUN Fire 280R	2 x 900	4.000	576
WWW	1	SUN Fire V240	1 x 1.500	2.048	146
FTP	1	HP DL 380	2 x 3.200	2.048	1.000
SEARCH-Engine	1	HP Netserver	2 x 1.000	1.024	100
Mail					
POP	1	SUN ULTRA60	2 x 450	1.024	72
Mail	5	SUN Fire V440	4 x 1.000	16.000	72
Mail	1	SUN Fire V490	4 x 1.350	16.984	292
Virencheck	2	SUN V40z	2 x 2.000	16.000	146
SPAM-Filter	4	SUN Fire V210	2 x 900	4.000	36
X.500-Directory	1	SUN E250	2 x 400	1.024	36
DNS	1	SUN E250	2 x 400	2.048	18
HPC					
HPC	1	HP DL585	4 x 2.200	16.984	246

Tabelle der wichtigsten Dienste und deren Server, 2005

IZH, vgl. Kapitel 6.1.1), sondern betraf auch ein umfangreiches Angebot für Institute und Lehrstühle. Es beinhaltete unter anderem Hilfen bei der Beschaffung, Installation und dem Betrieb ihrer Rechner. Besonders unterstützt wurden die mit Novell vernetzten PC-Systeme unter Windows 2000/XP, Linux-Systeme und Unix-Workstations mit dem Betriebssystem Sun Solaris. Es sei noch angemerkt, dass Novell-Vernetzungen, die sich vorrangig mit dem Bereitstellen von Dateisystemen, Druckern und Verzeichnisdiensten in lokalen PC-Gruppierungen befassten (bspw. in Kursräumen), über das proprietäre Betriebssystem Netware realisiert wurden und am RRZE in die Zuständigkeit der Systembetreuung fielen, also trotz der Bezeichnung nicht zum Netzbetrieb gehörten. Das Kommunikationsnetz der FAU bot aber dazu eine Grundlage, indem es zunächst das anfangs von Novell verwendete Protokoll IPX (Internetwork Packet Exchange) „parallel“ zu IP vermittelte (routete), bis sich Netware auch auf das Internetprotokoll stützte (etwa ab 1998 in Version 3) und sich damit so, wie andere Anwendungen, in das allgemeine IP-Routing eingliedern ließ.

Höchstleistungsrechner

Trotz enormer allgemeiner Kapazitätssteigerungen von Serversystemen und damit einhergehender Verringerung ihrer Größe bestand darüber hinaus auch immer besonderer Bedarf an noch höheren Leistungen, die nur durch speziell darauf ausgerichtete Systeme zu erbringen waren. So erfordert die Bearbeitung komplexer numerischer Problemstellungen in vielen Fällen den Einsatz jeweils modernster Hoch- und Höchstleistungsrechner. Das RRZE trug der wachsenden Bedeutung des High Performance Computing (HPC) mit der Bereitstellung zentraler Hochleistungsrechner sowie einer kompetenten Kundenbetreuung Rechnung und bündelte dazu seine Anstrengungen in einem „Center of Excellence for High Performance Computing“ (cxHPC). Ein herausragender Meilenstein wurde 2006 mit der Installation eines Parallelrechners von Bechtle/HP erreicht. Dieser High Performance Computing Cluster mit mehr als 700 Prozessorkernen sowie einem Hochgeschwindigkeitsnetzwerk konnte bis zu neun Billionen Rechenoperationen pro Sekunde ausführen und gehörte damit zu den leistungsfähigsten Rechnern der Welt: Auf der TOP500-Supercomputer-Liste vom November 2006 rangierte er im internationalen Vergleich auf Platz 124, innerhalb Deutschlands auf Platz 8 und erreichte damit die beste Platzierung eines Erlanger Systems seit der Existenz der Liste (1993). Das „Gruppenbild mit Rechenknoten“ zeigt den Alt-Kanzler der

Gruppenbild mit Rechenknoten, 2006

Universität Thomas A. H. Schöck sowie Uwe Dittrich (Firma Bechtle), Dr. Gerhard Hergenröder (RRZE) und Dr. Gerhard Wellein (RRZE) nach der Unterzeichnung des Vertrags über den Erwerb des neuen Parallelrechners.

Die hohen Rechnerleistungen werden nicht unerheblich durch Parallelisierungen von Rechenprozessen erreicht, für die die Hardwarestruktur Voraussetzungen schafft, sondern erfordern auch gezielte Programmierung zur Nutzung der Möglichkeiten. Das RRZE bot dazu mit seinem cxHPC als Kompetenzzentrum Beratung an und führte zudem eigene Forschungsprojekte durch. In diesem Zusammenhang erhielten 2006 vier Wissenschaftler der FAU, darunter Dr. Gerhard Wellein vom RRZE, einen von der internationalen Supercomputerkonferenz (ISC) vergebenen, international anerkannten Preis für neuartige Anwendungen von Höchstleistungsrechnern, speziell für die Parallelprogrammierung sehr großer Rechnersysteme.

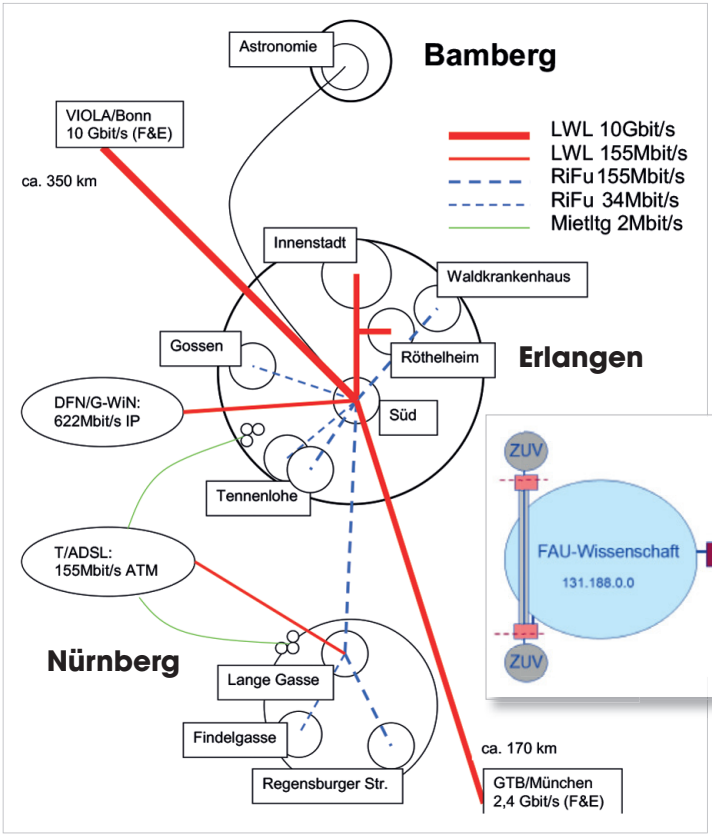
6.1.4 Kommunikationsinfrastruktur

Die Entwicklung des RRZE zum IT-Dienstleister der FAU bedingte auch einen entsprechenden Ausbau der Kommunikationsnetze, d. h. die Bereitstellung einer generell verfügbaren Infrastruktur. Ohne die Möglichkeiten zur flexiblen Kommunikation zwischen verteilten Systemen bzw. deren Nutzern wären viele der Dienste nicht sinnvoll oder auch überhaupt nicht zu erbringen; man denke etwa an Service-Plattformen, wie das bereits angeführte „mein campus“ für Studierende und Lehrpersonal, das im Prinzip von allen Standorten der Universität erreichbar sein muss(te).

Zählte es anfangs zu den Aufgaben des RRZE, den unter anderem in Erlangen und Nürnberg verteilten Standorten der FAU sowie denen nordbayerischer Hochschulen Zugänge zu seinen zentralen Rechnersystemen zu schaffen (vgl. Teil 1, Kapitel 1-2), erwuchs schon bald daraus der Bedarf einer flexiblen Vernetzung für wählbare Kommunikationsbeziehungen innerhalb und außerhalb der genannten Bereiche mit möglichst vielen, entsprechend verteilten Anschlüssen. Mit dem Einsatz der X.25-Technik (vgl. Teil 1, Kapitel 3) konnte in diesem Sinne vor allem bezüglich der Fernverbindungen bereits eine sehr gute Abdeckung erreicht werden. Mit der Verfügbarkeit neuer Techniken (Ethernet, FDDI, ATM usw.), insbesondere zur lokalen Vernetzung, konnte das Ziel einer flächendeckenden Infrastruktur verstärkt weiterverfolgt werden (vgl. Teil 1, Kapitel 4, 5). Eine systematische Umsetzung wurde spätestens mit Aufbau einer strukturierten Verkabelung (vgl. Teil 1, Kapitel 5.2.2) begonnen, die unter anderem anstrebte, jeden Büroraum der Universität mit Anschlussdosen zum Kommunikationsnetz auszustatten. Diese passive Basis wiederum schuf die Grundlage zur Gestaltung aktiver Strukturen aus zusammenwirkenden Netzkomponenten (Repeater, Switche, Router usw.). Dabei setzte sich auf der Netzebene (ISO-/OSI-Schicht 3, vgl. Teil 1, Einführung) das Internet-

protokoll (IP) zunächst als dominierend dann als alleinig eingesetztes Protokoll durch (vgl. Teil 1, Kapitel 4), sodass das Kommunikationsnetz der Universität danach auch als „Intranet der FAU“ bezeichnet werden konnte.

Diese flächendeckende, vom RRZE betreute Kommunikationsinfrastruktur umfasst(e) einerseits die verschiedenen, geografisch verteilten Bereiche, wie etwa solche in Erlangen (Südgelände, Innenstadt, Röthelheimpark), Nürnberg (WiSo, EWF, Findelgasse) oder Bamberg (Sternwarte) und gliedert(e) sich andererseits inhaltlich in die Bereiche von Forschung und Wissenschaft (FAU-Wissenschaft) , der medizinischen Versorgung (Universitätsklinikum, bis 2013) und der Zentralen Universitätsverwaltung (ZUV, ab 2005). Die unteren beiden Abbildungen „Netzbereiche (2004): geografisch und inhaltlich“ stellen die Gliederung bildlich dar.

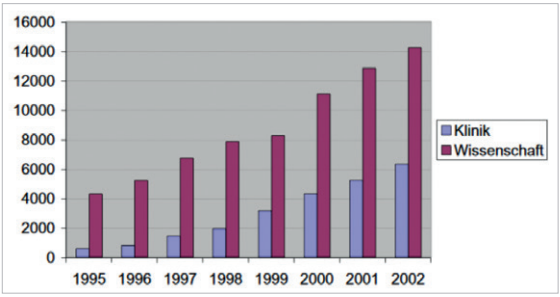


Netzbereiche (2004): geografisch (li.) / inhaltlich (re.)

Die Netzbereiche von Wissenschaft und Klinik waren zwar Teil des gemeinsamen Intranets, hatten aber eigene (IP-)Adressräume und waren aus Datenschutzgründen durch einen kontrollierenden Übergang (Firewall) voneinander getrennt. Die verteilten Teile des ZUV-Netzes waren aus Sicherheitsgründen untereinander über Zugangskontrollen und sogenannte Tunnel durch das Wissenschaftsnetz miteinander verknüpft (vgl. Kapitel 6.2.3.3 und 6.5.2).

Die Ausbreitung und der Ausbau der Infrastruktur im Zuge begonnener, strukturierter Verkabelungen spiegelten sich unter anderem im Wachstum der Anzahl von Anschlüssen wieder, die in einem Diagramm der verwendeten Internet-Host-Adressen im Wissenschafts- und Klinikbereich dargestellt wurde (Abbildung „Anzahl IP-Adressen jeweils am Jahresende, JB 2002“). Danach stieg im Zeitraum von 1995 bis 2002 (also etwa bis in den Anfang der in diesem Kapitel betrachteten Phase) die Gesamtzahl der versorgten Endgeräte von 5.000 auf rund 20.000. Im weiteren, kontinuierlichen Ausbau wurde dazu in 2010 eine Verdoppelung der Geräte auf über 40.000 erreicht.

Neben der Anzahl und Verbreitung der Zugänge spielt(e) aber natürlich auch ihre Qualität eine bedeutende Rolle, die sich unter anderem in Übertragungsgeschwindigkeiten, Antwortzeiten oder Verfügbarkeiten darstellt. Auch in dieser Beziehung stellen zunehmende Gerätezahlen, Dienste, Anwendungen oder Benutzerzahlen ständig steigende Anforderungen. Das RRZE reagiert(e) darauf mit regelmäßigen Überprüfungen, Hinterfragungen jeweils aktueller Strukturen, Beobachtungen neuer technischer Entwicklungen und leitete(e), falls sinnvoll (und finanzierbar), entsprechende Umgestaltungen ein. So wurde auch, wie schon eingangs erwähnt, die Phase mit der 1995 unter seinerzeitigen Gesichtspunkten optimale Netzstruktur auf Basis der ATM-Technologie nach und nach durch Lösungen unter Verwendung von Ethernet-Technik abgelöst, nachdem diese ihren Rückstand aufzuholen und sich am Markt durchzusetzen begonnen hatte.



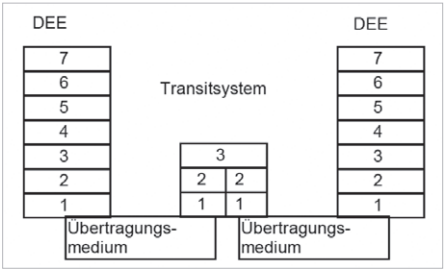
Anzahl IP-Adressen jeweils am Jahresende, JB 2002

6.2 Technische Grundlagen zur Weiterentwicklung des Kommunikationsnetzes

Mit der ständig wachsenden Bedeutung von Kommunikationsvorgängen, der Anzahl betreffender Endsysteme oder der Vielfältigkeit von Anwendungen stiegen auch die Ansprüche an die Kommunikationsnetze und die ihnen zugrundeliegenden Techniken. Zu deren Bewältigung trugen entsprechende Forschungen und Entwicklungen erheblich bei, insbesondere in Bezug auf Übertragungsgeschwindigkeiten oder Konzeptionen der Netzgestaltung. Hierbei ist vor allem die enorme Entwicklung der Ethernet-LAN-Technik hervorzuheben, die im Zusammenhang mit der Bereitstellung bzw. Verteilung von Endgeräteanschlüssen an der FAU schließlich die bestimmende Rolle einnehmen sollte.

Die folgenden Abschnitte erläutern Grundlagen zu den wichtigsten Veränderungen, Fortschritten bzgl. der unteren drei Schichten des ISO-/OSI-Referenzmodells, die für das Kommunikationsnetz als Transitsystem zur Datenübertragung stehen (vgl. „Datenübertragung im Referenzmodell“, Teil 1, Einführungskapitel).

In der Abbildung „Kommunikationsmodell gemäß ISO/OSI“ kommunizieren zwei Endsysteme (DEEs) über ein „einfaches“ Netz (Transitsystem) miteinander, wobei darin Schicht 1 für den Zugriff und die Nutzung von Übertragungsmedien (bspw. LWL) steht, während gemäß folgenden Betrachtungen Schicht 2 Ethernet-Techniken und Schicht 3 Internetprotokolle repräsentieren.



Kommunikationsmodell gemäß ISO/OSI

6.2.1 Entwicklungen zum passiven Netz (Schicht 1)

Das passive Netz ist der physikalischen Schicht zugeordnet und stellt den aktiven Komponenten Medien bzw. Schnittstellen zur Datenübertragung bereit. Hierzu begann das RRZE bereits in den 90er Jahren mit dem systematischen Aufbau einer in primäre (Verbindung zwischen Gebäuden, Bereichen), sekundäre (innerhalb von Gebäuden zwischen Etagen) und tertiäre Ebene (in Etagen zu Anschlussdosen für Endgeräte) gegliederten, strukturierten Verkabelung (vgl. Teil 1, Kapitel 5.2.2). Diese wurde in den folgenden Jahren weiter voran getrieben und ist noch heute gültiges Muster für Ausbau und Erweiterungen, bspw. bei der Einbeziehung neuer Standorte/Gebäude. Trotz eines engen Zusammenhangs zwischen passiven und aktiven Elementen erwies sich das Konzept als tragend – auch für sehr unterschiedliche Netztechniken wie etwa FDDI, ATM oder Ethernet.

Während primäre und sekundäre Ebene mit der Ausnahme spezifischer Fernverbindungen vornehmlich über verlegte Glasfasern (Singlemode, Multimode) realisiert wurden, gab es im tertiären Bereich verschiedene Ansätze, die auch in enger Verbindung mit den im folgenden Abschnitt beschriebenen Ethernet-Entwicklungen zu sehen sind. Nachdem „frühe“, vereinzelte Verkabelungen innerhalb von Gebäuden noch „dünne“ Koaxialkabel (Thin-Ethernet, 10Base2) verwendet hatten (bspw. im Rechenzentrumsgebäude für Mitarbeiter, 1990), wurden im Rahmen der Investitionsprogramme NIP (vgl. Teil 1, Kapitel 5.2.3) mit dem Baubeginn 1994 zur Innenverkabelung 4-adrige Kupferkabel (Twisted Pair) verlegt (übrigens entgegen den Planungsrichtlinien der obersten Baubehörde, die anfangs auch hier Glasfaserleitungen vorgeschrieben hatten). Dabei wurden im Laufe der Zeit verfügbare Qualitätssteigerungen berücksichtigt. Gemäß ihren elektrischen Eigenschaften (bzgl. Dämpfung, Übersprechen, Isolierung) sind TP-Kabel in verschiedene, mit Cat4, 5, 6, 7, 8 bezeichnete Güteklassen eingeordnet. So kamen im FAU-Netz zunächst Cat4-, später Cat5-Kabel zum Einsatz, während heute in der FAU vornehmlich Cat6-Kabel verlegt werden. Einen weiteren Anlass zur Modifikation der Verkabelung bzw. der Verwendung zugehöriger Patch- und Anschlussdosen ergab sich aus der Definition und Verfügbarkeit von Gigabit Ethernet (GE), das zur Nutzung über Kupferkabel acht statt vier Adern benötigt. Dies wurde (und wird) im Rahmen neuer Maßnahmen entsprechend berücksichtigt, führte aber auch zu verschiedenen Um- bzw. Nachrüstungen. Unabhängig davon, können aber bei Bedarf über jeweils zwei früher verlegte, 4-adrige Wege durch einfache Umsetzungen auch 8-adrige Verbindungen hergestellt und so für GE-Übertragungen genutzt werden.

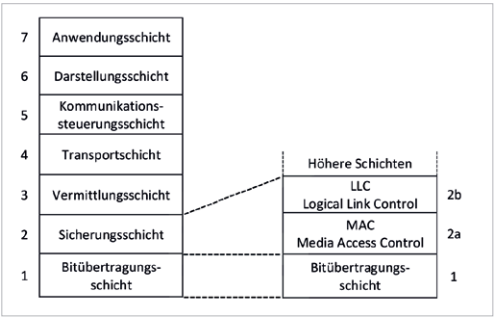
In Teil 1, Kapitel 5.2.1 sind verschiedene Übertragungsmedien mit ihren grundlegenden Eigenschaften gegenübergestellt. Das anschließende Kapitel beschreibt Verwendungen im Zusammenhang mit der Bildung von Ethernet-LANs.

6.2.2 Entwicklungen zum Ethernet (Schicht 2)

6.2.2.1 Ausgangslage

Wie in Teil 1, Kapitel 4.2 beschrieben, wurde die Ethernet-Technik zur Bildung lokaler Netze eingeführt und stellte etwa im Vergleich zu seriellen Datenübertragungen über V.24-Schnittstellen auch unter Berücksichtigung struktureller Unterschiede deutlich höhere Übertragungsleistungen zur Verfügung, die sich besonders im Vergleich der Übertragungsgeschwindigkeiten von 10 Mbp/s bzw. 10.000 kbp/s (Ethernet) zu 9.6/19.2 kbp/s (V.24) ausdrückten. Während die ersten Ausprägungen auf Basis „dicker“ Koaxialkabel (10Base5) sehr unflexibel und für einen breiteren Einsatz nicht geeignet waren, konnten unter Einsatz „dünner“ Koaxialkabel (10Base2) und verteilender Komponenten (Repeater) Netze flexibler aufgebaut werden, wie etwa das LAN im

Rechenzentrumsgebäude zur Versorgung der Mitarbeiter mit Endgeräteanschlüssen in ihren Büroräumen (vgl. Teil 1, Kapitel 4.2.2.4). Aber sowohl die an die Koaxialkabel gebundene Geschwindigkeit von 10 Mbp/s, als auch Maßnahmen zur Erhöhung von Reichweite oder Verteilungsgrad, über Repeater oder Bridges, konnten auf Dauer steigenden Anforderungen nicht gerecht werden. Das IEEE (Institute of Electrical and Electronics Engineers) hat daher zum Schritthalten entsprechende Entwicklungen und Erweiterungen der Standards im Rahmen der Projektgruppe „802“ vorangetrieben. Die Ethernet-Protokolle realisieren im ISO-/OSI-Modell eine Sicherungsschicht (Schicht 2), bieten „nach oben“ Dienste für die Vermittlungsschicht (Schicht 3, meist realisiert durch das Netzprotokoll IP) und nutzen ihrerseits „nach unten“ die Bitübertragungsschicht (Schicht 1), die durch verschiedene Übertragungsmedien repräsentiert wird. Die Ethernet-Schicht selbst wird nochmal in Logical LinK Control (LLC, meist Variante LLC2, Schicht 2b) und Media Access Control (MAC, Schicht 2a) untergliedert. In der Abbildung „Anordnung Ethernet im Referenzmodell“ (entnommen [*Rech*]) sind diese Zusammenhänge dargestellt. Die im Folgenden betrachteten Erweiterungen beziehen sich vornehmlich auf Varianten verwendeter Medien (Schicht 1) und zugehöriger Zugriffsmechanismen (Schicht 2a). Durch die klare Aufgabenverteilung wurde es möglich, deren konkrete Umsetzungen auszutauschen, ohne die Nutzung durch darüberliegende Ebenen verändern zu müssen. So galten in diesem Zusammenhang Adressierungsverfahren (MAC-Adressen), Broadcast-Eigenschaften (logische Bus-Struktur) oder grundlegende Paketformate (Frame-Aufbau) unverändert weiter.



Anordnung Ethernet im Referenzmodell

6.2.2.2 Medien und Geschwindigkeiten

Die für Einsatz und Akzeptanz der Technik bedeutendsten Erweiterungen des „klassischen“, über Koaxialkabel betriebenen Ethernets betrafen die Art der verwendeten Medien sowie damit verbundene Verfahren zum Erreichen höherer Datenübertragungsraten. Die Entwicklungen schlugen sich in entsprechenden Festlegungen des IEEE als Ergänzungen der Gruppe 802.3 nieder.

Die vom Elektronik-Kompendium [*Elkom*] zusammengestellte Tabelle „Ethernet-Standards im Überblick“ stellt die Entwicklung der Festlegungen mit Bezeichnungen, betreffenden Medien (Kabel) und Geschwindigkeiten (Datenraten) sowie den Jahren ihrer Veröffentlichungen im Überblick dar.

Ethernet-Standards im Überblick (gemäß Elektronik-Kompendium [Elkom])

Ethernet-Standard	Bezeichnung	Jahr	Datenrate	Kabel
802.3	10Base5	1983	10 MBit/s	Koaxialkabel (DIX/AUI), 500 m
802.3a	10Base2	1988	10 MBit/s	Koaxialkabel (BNC), 185 m
802.3i	10Base-T	1990	10 MBit/s	Twisted-Pair-Kabel (RJ-45), 100 m
802.3j	10Base-FL	1992	10 MBit/s	Glasfaserkabel
802.3u	100Base-TX	1995	100 MBit/s	Twisted-Pair-Kabel (RJ-45), 100 m
802.3u	100Base-FX, 100Base-SX	1995	100 MBit/s	Glasfaserkabel
802.3z	1000Base-SX, 1000Base-LX	1998	1 GBit/s	Glasfaserkabel
802.3ab	1000Base-T	1999	1 GBit/s	Twisted-Pair-Kabel (RJ-45), 100 m
802.3ae	10GBase-SR, 10GBase-SW, 10GBase-LR, 10GBase-LW, 10GBase-ER, 10GBase-EW, 10GBase-LX4	2002	10 GBit/s	Glasfaserkabel
802.3an	10GBase-T	2006	10 GBit/s	Twisted-Pair-Kabel (RJ-45), 100 m

Erläuterungen:
T = Twisted-Pair
S = 850 nm, bis 65 m, Multimode
L = 1310 nm
E = 1550 nm, bis 40 km, Singlemode
R = 64b/66b, LAN
X = 8b/10b, LAN
W = 64b/66b, WAN, SONET/SDH Framing
4 = WWDM mit vier Wellenlängen

Die für das RRZE wichtigsten Schritte, die auch im Kommunikationsnetz der FAU große Bedeutung erlangten, werden im Folgenden näher erläutert.

Mit der Definition von **Ethernet** über **TP** (E, 10Base-T, 802.3i) sollten Nachteile der Koaxialverkabelung, wie etwa deren Fehleranfälligkeit, überwunden und alternative Möglichkeiten zur Netzgestaltung eröffnet werden. Lokale Netze bzw. Segmente konn-

ten nun mit Hilfe entsprechender aktiver Komponenten (vgl. Kapitel 6.3.2.3) gebildet werden, indem die Endgeräte jeweils über Punk-zu-Punkt-Verbindungen sternförmig an einen zugehörigen Verteiler angeschlossen wurden. Die strukturierte Verkabelung ersetzte in der tertiären Ebene anfangs vereinzelt verlegte, „dünne“ Koaxialkabel durch TP-Kabel und schuf so die Voraussetzungen für den Einsatz dieser Technik und zur systematischen Ausstattung von Gebäuden bzw. Etagen mit LAN-Zugängen. Ihre Rangierfähigkeit erhöhte zudem die Flexibilität bei der Einordnung von Endgeräten in lokale Einheiten nach Bedarf. Die TP-Schnittstellen von Verkabelung und Geräten sind bezüglich Stecker und Anschlussdosen nach RJ45 (Registered Jack, Norm der US-amerikanischen „Code of Federal Regulations“ (CFR)) gestaltet. Von den acht definierten Pins wurden vier zur Übertragung von Ethernet über TP genutzt und die Kabel entsprechend aufgelegt (vgl. Darstellung „Schema FE u. GE über TP, RJ-45-Belegung“, Spalte „10/100 FDX“).

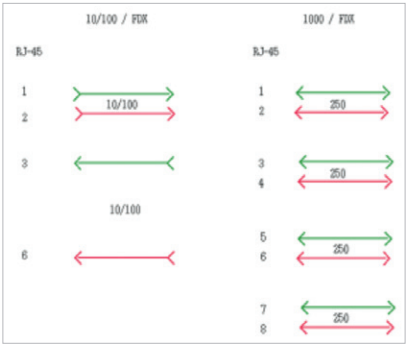
Die Verknüpfung von LAN-Segmenten unter Nutzung der sekundären strukturierten Verkabelung wurde durch die Verfügbarkeit von **Ethernet** über **Glasfaser** (E, 10Base-FL, 802.3j) möglich. Damit konnten entsprechend ausgestattete, aktive Ethernet-Verteiler der Etagen miteinander verbunden und entsprechende Segmente zu größeren LAN-Einheiten zusammengefügt werden. Dabei musste allerdings auf die jeweils entstehende „Größe“ von LANs geachtet werden, die bspw. als Kollisions- oder Broadcast-Bereiche auch in diesem Kontext in der Anzahl teilnehmender Endgeräte nicht unbegrenzt erweiterbar waren. Entsprechende Schranken ergeben sich unter anderem aus dem Nutzungsprofil (Verkehrscharakteristik) oder der Art der aktiven Komponenten (Repeater, Switch usw.), sind aber nicht starr zu fassen.

Im Gegensatz zu den Koaxialkabeln erlaubten die elektrischen Eigenschaften 4-adriger, geschirmter Kupferkabel, Übertragungstechniken für höhere Datenraten zu definieren und umzusetzen. Mit **Fast Ethernet** über **TP** (FE, 100Base-TX, 802.3u) konnten Übertragungsgeschwindigkeiten um den Faktor 10, also von 10 Mbp/s auf 100 Mbp/s, angehoben werden. Dabei konnte im Einsatz an der FAU die strukturierte Verkabelung unverändert auch für die schnelleren Übertragungen genutzt werden.

In Ergänzung dazu diente dann **Fast Ethernet** über **Glasfaser** (FE, 100Base-FX/SX, 802.3u) an der FAU vorrangig zur Beschleunigung etagenübergreifender Verknüpfungen von Segmenten, also der Herstellung von Verbindungen von 100 Mbp/s zwischen verteilenden Komponenten. Es sei noch bemerkt, dass das Mischen von Anschlüssen unterschiedlicher Geschwindigkeiten innerhalb eines so gebildeten LANs mit den anfangs eingesetzten aktive Komponenten (LAN-Repeater) unmöglich war und erst mit neu entwickelten Geräten (LAN-Swichte) zur Option wurde (vgl. Kapitel 6.3.2.3).

Die nächsthöhere Geschwindigkeitsstufe definierte wieder eine um den Faktor 10 von 100 Mbp/s auf 1000 Mbp/s bzw. 1 Gbp/s angehobene Datenrate und war in der Praxis zunächst als **Gigabit Ethernet** über **Glasfaser** (GE, 1000Base-SX/LX, 802.3u) verfügbar. Sie wurde vor allem zur Leistungssteigerung innerhalb von LAN-Strukturen genutzt, d. h. zur Herstellung entsprechend schnellerer Verbindungen zwischen betreffenden Netzkomponenten. Dabei dienten vorhandene Verkabelungen der primären und tertiären Ebene unverändert als Medien zur Übertragung von Daten.

Die Glasfasertechnik war für einen verbreiteten Einsatz im Endgerätebereich nicht geeignet. Dagegen sprachen unter anderem die Kosten für entsprechende Schnittstellen in Endgeräten und aktiven Netzkomponenten, aber auch der deutlich höhere Aufwand einer erforderlichen Verkabelung von „Glasfaser zum Arbeitsplatz“ (vgl. Teil 1, Kapitel 5.2.2). Abgesehen davon, dass die Bedienung von GE hohe Anforderungen an die „innere“ Leistungsfähigkeit von Systemen stellt und auch heute noch etwa von PCs kaum voll ausgenutzt werden kann, entstand aber doch auch bzgl. Endgeräten der Bedarf an möglichen Datenraten oberhalb von 100 Mbp/s. Die Definition von **Gigabit Ethernet** über **TP** (GE, 1000Base-T, 802.3ab) war daher ein folgerichtiger Schritt. Allerdings war dieser aufgrund der elektrischen Eigenschaften von TP (Dämpfung, Übersprechen, Störeinfluss usw.) nicht durch „einfaches“ Anheben der Bitrate bzw. einer Erhöhung entsprechender Signalfrequenzen zu erzielen. Vielmehr musste ein neuer Ansatz zur Überwindung von Beschränkungen des Mediums gefunden werden. Da aufgrund elektrischer Eigenschaften von Standard-TP-Kabeln noch Übertragungsraten bis zu 250 Mbp/s prinzipiell erzielbar waren, bestand die Lösung darin, Datenströme von 1000 Mbp/s beim Sender jeweils in vier Ströme von je 250 Mbp/s aufzuteilen, diese parallel per Kupferkabel zu übertragen und beim Empfänger entsprechend wieder zusammenzusetzen. Hierzu mussten die TP-Schnittstellen im Vergleich zu 10/100 Mbp/s modifiziert genutzt werden, denn für die Teilströme werden jeweils zwei Adern, also insgesamt acht statt vier Adern zur Signalübertragung benötigt. An den Schnittstellen konnten aber weiter die RJ-45 Steckverbindungen eingesetzt werden, nun aber mit der Belegung aller acht Pins (vgl. Abbildung „Schema FE und GE über TP, RJ-45-Belegung“). Die 4-adrige Verkabelung kann unter Einsatz



Schema FE und GE über TP, RJ-45-Belegung

entsprechender Anpassungen durch Schaltung zweier Verbindungswege auch für GE-TP genutzt werden. Neuere Verkabelungen an der FAU sind von vornherein auf 8-adrige Verbindungen ausgelegt.

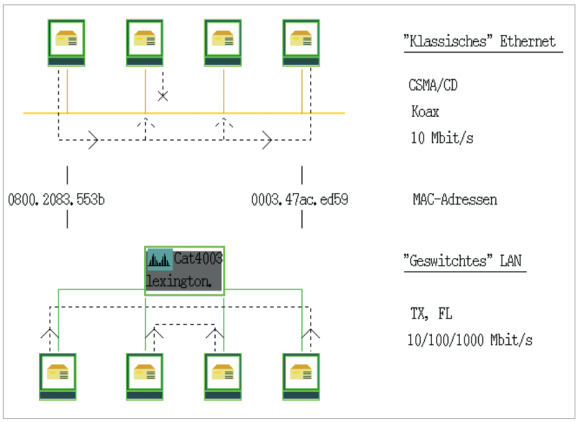
Vor allem für den Einsatz im Backbone-Bereich wurde **10 Gigabit** über **Glasfaser** (10GE, 10GBase, 802.3ae) entwickelt und an der FAU eingesetzt. Es diente bspw. zur leistungsstarken Verbindung der Bereiche im Erlanger Südgelände und der Erlanger Innenstadt unter Verwendung von Glasfasern der primären strukturierten Verkabelungsebene.

6.2.2.3 Aktive Komponenten (LAN-Switche)

Obwohl zum Aufbau „klassischer Ethernets“ auf Basis von Koaxialkabeln aktive Komponenten nicht unbedingt erforderlich sind, wurden solche Geräte oft ergänzend eingesetzt (vgl. Teil 1, Kapitel 4.2.2.4). Sie dienten unter anderem zur Reichweitenerhöhung durch Signalverstärkung (Repeater), zur Reduzierung von Zugriffskonflikten durch Lasttrennung (Bridges) sowie zur Verteilung und Strukturierung (Multiport-Repeater, -Bridges) von (Ethernet-)LANs. Da TP-Kabel im Gegensatz zu Koaxialkabeln kein BUS-Medium darstellen, sondern „nur“ Punkt-zu-Punkt-Verbindungen realisieren, benötigen sie auf jeden Fall zur lokalen Vernetzung aktive Komponenten, die jeweils mehrere Einzelanschlüsse zu einem gemeinsamen LAN vereinen (vgl. Kapitel 6.3.2.2). Als Typen solcher Verteiler kamen zunächst Repeater mit passiver Funktionsweise in Frage, die jeweils mehrere Geräte in einer gemeinsamen Kollisionsdomäne zusammenfügten, in denen konkurrierende Zugriffe über das vom Koaxialethernet bekannte CSMA-/CD-Verfahren zu regeln waren. Schnell setzten sich aber im praktischen Einsatz intelligentere Komponenten durch, die durch eine Verkehrstrennung zwischen allen Anschlüssen Kollisionen ausschlossen. Solche sogenannten LAN-Switche entsprechen in der Funktionsweise Multiport-Bridges mit jeweils (maximal) einem angeschlossenen Netzteilnehmer pro Port. Der Aufbau und die unterschiedliche Funktionsweise sind auf S. 31 in der Abbildung „Ethernet über Koaxialkabel und LAN mit Switch und TP-Anschlüssen“ gegenübergestellt. Die Abbildung zeigt, wie in der oberen Konfiguration („Klassisches“ Ethernet) die beiden äußeren Geräte Daten miteinander austauschen und die inneren diese zwar mitlesen, aber keine eigene Übertragung starten können (ein angedeuteter Zugriffswunsch des zweiten Geräts von links ist blockiert). Das untere Beispiel stellt den Switch als sternförmigen Verteiler dar und lässt erkennen, wie sowohl die beiden äußeren als auch die beiden inneren „gleichzeitig“ miteinander kommunizieren. Im Gegensatz zum Koaxialnetz spielt dabei auch keine Rolle, mit welcher Geschwindigkeit die einzelnen Teilnehmer angeschlossen sind. Unterschiede werden vom Switch grob angeglichen, während die Systeme auf höherer Protokollebene (IP, TCP) für geregelten Datenfluss sorgen (müssen).

Als grundlegende Eigenschaften von LAN-Switchen lassen sich zusammenfassen:

- Aktive Komponenten zur Bildung von Ethernet-LANs
- Ausgestattet mit Ports (Schnittstellen) zum Anschluss einzelner Endgeräte
- BUS-Charakter: Schaffung, Erhaltung von Broadcast-Domänen
- Bridge-Charakter: Kollisionsfreier Zugriff für angeschlossene Endgeräte
- Zuordnung von Port und MAC-Adresse jeweils angeschlossener Endgeräte
  - Statisch (manuelle Konfiguration)
  - Dynamisch (Lernmechanismus)
- Ports mit unterschiedlichen Anschlussgeschwindigkeiten gemischt betreibbar
- Bildung mehrerer, getrennter LANs in einem Switch durch Gruppierungen von Ports



Ethernet über Koaxialkabel und LAN mit Switch und TP-Anschlüssen

Darüber hinaus können über einzelne Ports auch Verbindungen zwischen LAN-Switchen hergestellt werden und so zur Vergrößerung und Verteilung von LANs genutzt werden. Dabei sorgt der Lernmechanismus im entsprechenden Verbund für die Verschmelzung der Bestandteile, indem er zu jedem Verbindungsport auf beiden Seiten Tabellen mit jeweils „dahinter liegenden“ MAC-Adressen aufbaut, die dann als wesentliche Kriterien zur Weiterleitung von Datenpaketen (Frames) dienen. Weitere Möglichkeiten zur Verknüpfung von LAN-Switchen einschließlich der Bildung komplexer Switch-Strukturen werden im anschließenden Abschnitt näher betrachtet.

6.2.2.4 LAN-Switch-Strukturen

Strukturbildung

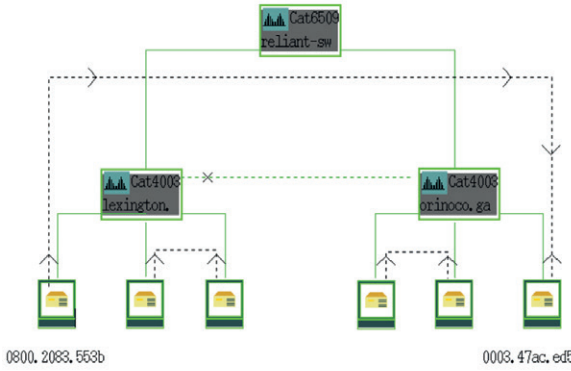
Wie bereits erwähnt, können mehrere LAN-Switche zu einem übergreifenden Verbund miteinander verknüpft werden. Im Fall eines gemeinsamen lokalen Netzes sind für die Ports der Switch-Verbindungen keine spezifischen Konfigurationen erforderlich. Jeder dabei beteiligte Switch stellt erhaltene Datenpakete (Frames, Datagramme mit Absender- und Zieladresse) gemäß gelernter Tabelleneinträge zu und leitet sie an alle seine Ports (außer an den, über den er die Adresse empfangen hat) wie Broadcasts weiter, falls die Zieladresse für ihn (noch) unbekannt ist. Das Verfahren innerhalb eines Verbundes entspricht somit dem eines einzelnen Switches.

Obwohl die Anzahl von Switchen in einem Verbund keinen prinzipiellen Beschränkungen unterliegt, sind allerdings folgende Aspekte zu beachten:

- Übertragungszeiten von Datenpaketen hängen (unter anderem) von der Anzahl der jeweils durchlaufenen Switche ab,
- Mit der Anzahl der Switche einer Struktur steigt (in der Regel) auch die Anzahl der teilnehmenden Endgeräte,
- Broadcasts und Weiterleitungen unbekannter Adressen sorgen für eine Grundlast im LAN, die mit der Anzahl der Geräte steigt und zu Beeinträchtigungen (bis hin zum Kollaps) führen kann,
- Broadcasts und unbekannte Adressen belasten nicht nur Komponenten und Verbindungsstrecken, sondern in besonderem Maße auch die Endsysteme, die gemäß Ethernet-Spezifikation jedes „vorbeikommende“ Paket zunächst annehmen müssen, um es selbst zu verarbeiten oder aber zu verwerfen.

Ausdehnung und Struktur eines LAN-Verbundes müssen also unter Beachtung der angeführten Punkte sorgsam geplant werden. So kamen etwa verlockende und von manchen Nutzern gewünschte Ansätze zur Gestaltung von Campus- oder gar universitätsweiten Ethernet-LANs für das RRZE nie in Frage. Neben der plausiblen, aber nicht exakt fassbaren Größenbeschränkung folgt aus der Funktionsweise zusammengeschalteter Switche auch eine prinzipielle Vorschrift: Strukturen dürfen keine Schleifen bzw. alternative Wege enthalten, sie müssen daher baum- oder sternförmig aufgebaut sein. Andernfalls würden etwa Broadcastpakete permanent im Kreis versendet und zum Zusammenbruch des Netzes bzw. eines Teilbereichs führen. Solche Situationen kamen übrigens auch in der Praxis des RRZE hin und wieder vor und wurden meist durch fehlerhaftes Patchen (unbewusstes Herstellen unzulässiger Verbindungen) von Seiten der Nutzer verursacht.

Die Abbildung „Verbund zur LAN-Verteilung“ zeigt eine einfache Baum- bzw. Sternstruktur mit drei Switchen, von denen zwei (lexington, orinoco) zum Anschluss von Endgeräten eingesetzt sind und einer (reliant) zwischen beiden vermittelnd wirkt. Danach kommunizieren die beiden äußeren, im Bild mit MAC-Adressen beschrifteten Geräte über ihre lokalen Switche und den zentralen Verteiler (Wurzel bzw. Sternmittelpunkt), während „gleichzeitig“ der Datenverkehr zwischen den innen skizzierten Geräten jeweils innerhalb der betreffenden Switche abgewickelt wird. Wären die beiden Endgeräteswitche, wie in der Zeichnung mit gestrichelter, grüner Linie angedeutet, miteinander (aktiv) verbunden, würde ein von einem Endgerät an „lexington“ initiierter Broadcast unter anderem an „orinoco“ gesendet, dort an „relington“ weitergegeben und dann wieder an „lexington“ geschickt werden. Dieser Vorgang würde sich ohne spezifische Vorkehrungen endlos wiederholen und zum Kollaps des Netzes führen. Andererseits erkennt man an der Skizze aber auch, dass etwa bei einem Ausfall des Verteilers die Endgeräteswitche ohne die gestrichelte Querverbindung voneinander isoliert wären, ihre Teilnehmer also nicht mehr übergreifend kommunizieren könnten.



Verbund zur LAN-Verteilung

Zur Lösung dieser Problematik dienen Verfahren, in denen, bezogen auf das Beispiel, die beiden Switche zwar physisch (per Kabel) miteinander verbunden sind, der Datentransfer darüber aber im Normalbetrieb gesperrt ist und nur im Fehlerfall freigegeben wird (vgl. folgender Abschnitt).

Ausfallsicherheit (Spanning Tree Protocol)

Baumstrukturen haben generell die Problematik, dass bei Ausfall der Wurzel oder eines anderen Verzweigungspunkts die jeweils nachfolgenden Teile voneinander getrennt werden, in einem entsprechenden Netzwerk also nicht mehr miteinander kommuni-

zieren können. Schon der Ausfall der Verbindung eines Teilbaums zu seiner höher gelegenen Verzweigung sorgt für dessen Isolierung vom sonstigen Netz. Um diesen Nachteil auszugleichen und im Zusammenhang mit Bridge- oder Switch-Strukturen für höhere Betriebssicherheit zu sorgen, hat die IEEE bereits 1990 im Rahmen der Gruppe 802.1 das „Spanning Tree Protocol“ (STP) veröffentlicht und in den darauffolgenden Jahren wie folgt weiterentwickelt:

- **802.1d-1990**, STP, Spanning Tree Protocol, für MAC-Bridges, orig. Veröffentlichung
- **802.1d-1998**, Modifikationen, Ergänzungen
- **802.1w-2001**, RSTP, Rapid Spanning Tree Protocol, beschleunigtes Verfahren
- **802.1d-2004**, Modifikationen, Ergänzungen, Zusammenfassung

Bei der Anwendung des Spanning-Tree-Verfahrens, d. h. seiner Konfigurierung auf allen beteiligten Komponenten (Bridges, LAN-Switche), ist es möglich, diese beliebig miteinander zu verschalten und dabei auch redundante Wege zu schaffen. Über einen Algorithmus wird bestimmt, welche der Verbindungen bzw. Schnittstellen (Ports) aktiv (im Zustand ‚Forwarding‘) nutzbar und welche für den Datenverkehr (im Zustand ‚Blocking‘) gesperrt sind. Der so ermittelte aktive Baum enthält entgegen der zu Grunde liegenden physischen Struktur also keine (aktiven) Schleifen. Die erzeugte Topologie wird im Betrieb laufend überprüft. Dazu versenden die beteiligten Komponenten regelmäßig (alle zwei Sekunden) sogenannte BPDUs (Bridge Protocol Data Unit) per Broadcasts mit gegenseitigen, aktuellen Zustandsinformationen. Bleiben dabei etwa erwartete BPDUs aus oder zeigen Meldungen von expliziten Schnittstellenausfällen (Port down) an, deutet dies auf Probleme hin und gibt Anlass zur Rekonfigurierung, also zu einer Neubestimmung der aktiven Topologie. Wie bei initialer Ausführung des Verfahrens, versenden die beteiligten Komponenten BPDUs zur Identifizierung und Mitteilung verschiedener, eigener Parameter. Daraus wird zunächst eine Komponente als „Root Bridge“ ausgewählt, d. h. die Wurzel der neuen Topologie bestimmt. Unter Auswertung von Parametern wie „Wegelänge zur Root Bridge“ (Anzahl zwischenliegender Komponenten), „Übertragungsgeschwindigkeiten auf der Wegstrecke“ oder auch frei konfigurierbarer Gewichtungen wird pro Komponente der jeweils günstigste Weg zur Wurzel berechnet und für jeden Switch und jeden Port über „Weiterleiten“ oder „Blockieren“ von Datenpaketen entschieden.

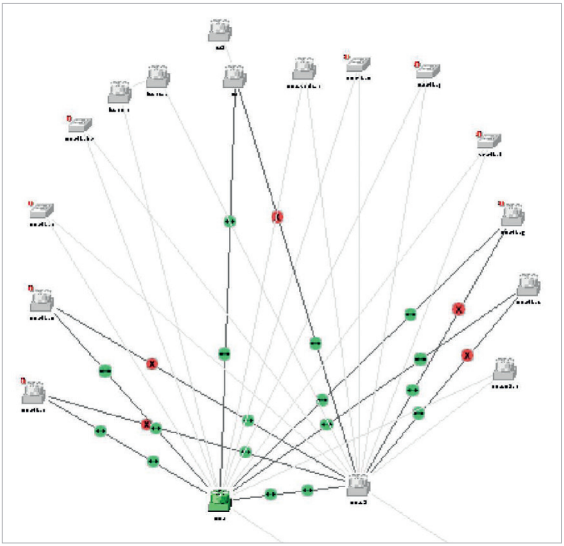
Im Laufe bzw. nach Abschluss des Verfahrens sind den Ports der beteiligten Komponenten folgende Zustände zugeordnet:

- **Disabled**: Außer Betrieb; verwirft Datenpakete (Frames); lernt keine Adressen; empfängt und verarbeitet keine BPDUs
- **Blocking**: Gesperrt; am Anfang oder Ende des Verfahrens; verwirft Datenpakete (Frames); lernt keine Adressen; empfängt und verarbeitet BPDUs

- **Listening**: Beobachtungsphase; Zwischenzustand; verwirft Frames; lernt keine Adressen; empfängt, verarbeitet und überträgt BPDUs
- **Learning**: Lernphase; Zwischenzustand; verwirft Frames; lernt Adressen; empfängt, verarbeitet und überträgt BPDUs
- **Forwarding**: Im aktiven Betrieb; am Ende des Verfahrens; leitet Frames weiter, lernt Adressen; empfängt, verarbeitet und überträgt BPDUs.

Da während der Abwicklung des STP-Verfahrens keine Datenpakete übertragen werden, ist der Netzbetrieb zur Überbrückung eines Geräte- oder Verbindungsausfalls für etwa 30 Sekunden unterbrochen. Dieser im Zuge steigender Anforderungen immer stärker als nachteilig beurteilten Schwäche wurde mit der Einführung des „Rapid Spanning Tree Protocols“ (RSTP) begegnet, das in einem modifizierten Verfahren flexibler auf signalisierte Topologieänderungen reagiert. Es beachtet den Kontext einer Ausfallsituation, grenzt die Behandlung entsprechend ein und vermeidet so im Vergleich zu STP ein komplettes Neuberechnen der Topologie. Die Dauer einer damit verbundenen Betriebsunterbrechung liegt in der Regel unter einer (1) Sekunde.

Als Beispiel stellt die Abbildung „Redundanter Stern mit Spanning Tree“ eine Switch-Struktur aus dem Netz des Universitätsklinikums dar. Es zeigt die Konfiguration im Neubau des Nichtoperativen Zentrums (NOZ, 2009). Die Darstellung wurde von dem Netzwerk-Management-System „Cisco Works“ (vgl. Kapitel 7.3.2) erzeugt und gibt einen zu der Zeit aktuell beobachteten, festgehaltenen Betriebszustand wieder. (Die



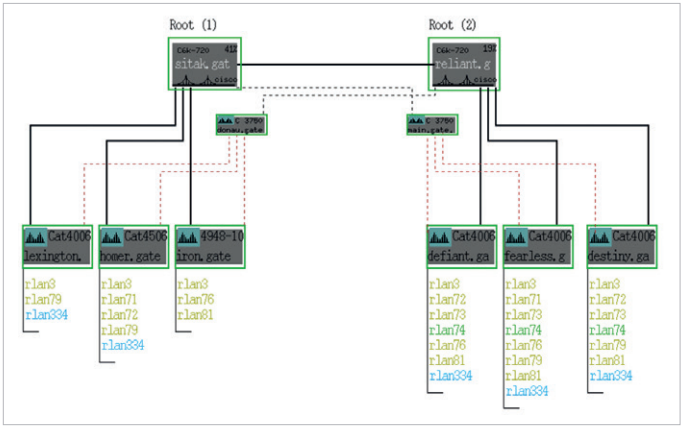
Redundanter Stern mit Spanning Tree (Beispiel NOZ, 2009)

Beschriftungen sind nicht kenntlich, spielen aber bei der Strukturbetrachtung nur eine untergeordnete Rolle). Die Konfiguration besteht aus zwei Switchen im Mittelpunkt des Sternes sowie in den Etagen verteilten LAN-Switchen, die jeweils mit beiden zentralen Verteilern (über Glasfaserkabel mit GE) verbunden sind. Die farbigen Markierungen beziehen sich auf ein, gemäß Skizze, im Gebäude (nicht in allen Etagen) verteiltes LAN. Dabei ist der aktive Verteiler (unten, linke Mitte) ebenso grün dargestellt wie die für den Datentransfer frei gegebenen Switch-Ports (farbige Punkte in der Nähe betreffender Switche). Die roten Punkte auf den Verbindungslinien weisen hingegen auf blockierte Schnittstellen hin. Anhand der Markierungen ist nachzuvollziehen, dass das hier eingesetzte RSTP-Verfahren aktive Schleifen verhindert hat. Sollte der zentrale Switch komplett ausfallen, würde der zweite an seiner Stelle aktiv werden und die Verbindungen der Etagenswitche zum neuen Mittelpunkt frei geschaltet werden, d. h. vom Zustand „Blocking“ (rot) in „Forwarding“ (grün) übergehen. Die Etagenswitche hätten dann nach kurzer (gemäß RSTP weniger als eine (1) Sekunde) Unterbrechung wieder eine Verbindung zum zentralen Gebäudeverteiler und könnten den Betrieb entsprechend fortsetzen.

Redundante Konstrukte zum Abfangen von Ausfällen erfordern in der Regel eine Verdoppelung eingesetzter Komponenten oder Betriebsmittel. So enthält bspw. die oben betrachtete Konfiguration des NOZ zwei zentrale Elemente und jeweils zwei geschaltete Kabelwege von der Zentrale zu den Etagen. Der Mehraufwand gegenüber einer singulären Lösung ist mit entsprechenden Kosten verbunden, aber auch sonst oft aus anderen Gründen nicht in idealer Form praktisch umsetzbar. Ein Beispiel für eine modifizierte, erstmals 2009 vorgestellte Lösung bot die abgebildete „Redundante Switch-Struktur im Rechenzentrum“. Diese bestand aus zwei Sternen in den Rechnerräumen des Informatikhochhauses (linke Bildhälfte) bzw. des RRZE-Gebäudes (rechte Bildhälfte), deren Mittelpunkte miteinander verbunden waren. Im Gegensatz zum NOZ-Beispiel waren die Zentren räumlich voneinander getrennt und beide im Normalbetrieb als Verteiler aktiv. Das Netz im Informatikraum diente vor allem der Anbindung dort betriebener, zentraler Server, während die Struktur im „alten“ Rechnerraum vornehmlich für Anschlüsse der Mitarbeiter des RRZE, insbesondere der Systembetreuer zuständig war. Insgesamt handelte es sich also um einen sensiblen Bereich innerhalb des Gesamtnetzes der FAU, der möglichst ausfallsicher zu gestalten war. Im Bild ist die aktive Struktur an den durchgezogenen, dicken Linien erkennbar. Sie bildete einen Baum mit dem als „Root (1)“ bezeichneten Switch als Wurzel und dem Switch „Root (2)“ als Ast mit weiterer Verzweigung.

Zwischen den beiden Rechnerräumen waren zwar Glasfaserkabel verlegt, aber nicht in der nötigen Anzahl, um alle äußeren Switche (Blätter des Baums) direkt mit beiden Zentren (entsprechend der obigen NOZ-Struktur) verbinden zu können. Deshalb

wurde an beiden Standorten je ein dedizierter Switch eingesetzt, der die betreffenden Endgeräteswitche summarisch mit dem Verteiler des benachbarten Bereichs verband. Diese Switche, im Bild etwas kleiner unter den Hauptverteilern dargestellt, wurden nur in Ausfallsituationen aktiv und konnten daher durch kostengünstige Modelle realisiert werden. Es sei noch angemerkt, dass die zentralen Switche (sitak, reliant) durch seinerzeitige Top-Modelle von Cisco (Modell Cisco 7200) realisiert waren, zusätzlich als Router fungierten sowie die Verbindungen dieser lokalen Struktur zum übrigen FAU-Netz herstellten. Die gestrichelten Linien stehen für Verbindungen, die zwar geschaltet, aber im Normalbetrieb per RSTP blockiert waren und nur im Fehlerfall gemäß Auswahl durch den Algorithmus je nach Situation für den Datenverkehr freigegeben wurden. Diese redundante Struktur war kostengünstig umzusetzen, kam mit drei Verbindungsstrecken zwischen den beiden Räumen aus, war in einfacher Weise erweiterbar und erhöhte die Betriebssicherheit bzgl. der Netzzugänge für Server und Mitarbeiter des Rechenzentrums.



Redundante Switch-Struktur im Rechenzentrum, 2009

Für viele Anwendungen reicht(e) die Fehlerbehandlung mit einer maximalen Unterbrechung von einer (1) Sekunde aus, zumal derartige Situationen im Betrieb des Kommunikationsnetzes der FAU äußerst selten vorkamen. Zudem sorgte der Einsatz des genormten RSTPs für Interoperabilität zwischen Komponenten unterschiedlicher Hersteller und damit für entsprechende Freiheiten der Netzgestaltung bzw. der Geräteauswahl. Dennoch gaben die Unterbrechungszeiten des Verfahrens, ebenso wie die Passivität der jeweils inaktiv gesetzten Elemente (Switche, Verbindungen), Anlass zu Kritik. Daher entwickelten verschiedene Hersteller eigene Methoden als Ergänzungen oder Alternativen zur Überwindung dieser Schwächen. Als Beispiele hierfür seien die

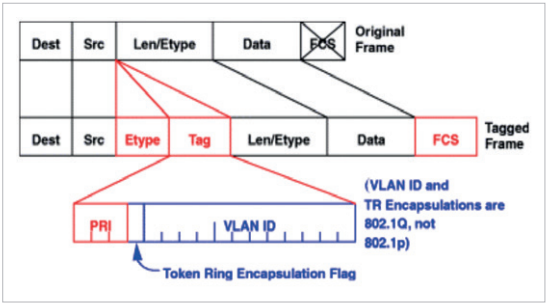
auch an der Universität und im Klinikum eingesetzten Verfahren von Cisco des „uplink fast“ und „backbone fast“ für Switch-Verbindungen zu übergeordneten Verteilern oder des „EtherChannel“-Konzepts physisch paralleler, als logische Einheiten betriebener Verbindungen erwähnt. Noch komplexere Lösungen bezogen sich auf homogene Netzwerkbereiche, wie etwa die Realisierung von Serverfarmen (Datacenter) am RRZE mit der Gerätefamilie „Nexus“ von Cisco (vgl. Kapitel 7.2.2). In einer entsprechend vermaschten Struktur können redundante Verbindungen hergestellt, ohne Blockaden genutzt und Ausfälle einzelner Bestandteile ohne messbare betriebliche Unterbrechungen kompensiert werden. Vergleichbare, herstellerspezifische Lösungen gab es aber auch von anderen Firmen wie von Hewlett Packard (Modellserien 10500, 5412zl) oder Juniper (Modellserien QFX5100, EX4300).

6.2.2.5 Virtuelle LANs in Swich-Strukturen

Verknüpft man LAN-Switche zu einer Struktur, indem man die Verbindungen zwischen ihnen über Ports (Ethernet-Schnittstellen) und Kabel (Glas oder Kupfer) herstellt, spannen sie ohne besondere Konfigurierungen ein umfassendes lokales Netz auf. Oft besteht aber der Bedarf, bspw. innerhalb eines größeren Gebäudes (vgl. Beispiel „NOZ“), mehrere LANs in den Etagen verfügbar zu machen. Dies könnte mit jeweils eigenen Strukturen pro LAN gelöst werden, wäre in der Regel aber sehr aufwendig, unflexibel und ineffektiv. Die Hersteller von LAN-Switchen entwickelten daher Konzepte, nach denen mehrere „virtuelle LANs“ (VLANs) über eine gemeinsame „reale“ physische Struktur definiert und verteilt werden konnten. Nachdem es bereits möglich war, innerhalb eines Switches durch Portgruppierung mehrere LANs zu definieren, bestand der entscheidende Schritt darin, die Ports zum Transfer zwischen den Switchen gesondert zu behandeln und für den empfangenden Partner die LAN-Zugehörigkeit eines gesendeten Frames kenntlich zu machen. Leider waren die Methoden zunächst nicht genormt und zwischen Geräten unterschiedlicher Hersteller nicht kompatibel. Da das RRZE in den Kommunikationsnetzen der Wissenschafts- und Klinikbereiche vornehmlich Switche von Cisco (meist an größeren Verteilpunkten) und 3Com (kostengünstige Alternative in der Fläche) einsetzte, bot sich hier keine gangbare Lösung an. Die Unterschiede drückten sich schon in der verwendeten Terminologie aus. So nannte Cisco die Switch-Switch-Verbindungen „Trunks“, während sie von 3Com als „Links“ bezeichnet wurden. Diese Unverträglichkeiten, verbunden mit einem zum Teil unflexiblen Gerätemanagement, gehörten neben bestehender Geschwindigkeitsnachteile zu den Gründen, aus denen das RRZE zur Realisierung virtueller LANs zunächst (ab 1995) die Techniken von ATM und LAN-Emulation (LANE) einsetzte (vgl. Teil 1, Kapitel 5).

In diesem Zusammenhang leitete die Veröffentlichung des neuen Standards **802.1q-1998, „Virtual Bridged Local Area Networks“** des IEEE eine neue Entwicklung ein. Er wurde nach und nach in verschiedenen Komponenten verfügbar, ersetzte dort spezifische Verfahren, wie etwa das Inter-Switch Link Protocol (ISL) von Cisco, und schuf so schließlich eine wichtige Voraussetzung zur Verteilung virtueller LANs in herstellerneutralen Strukturen. In diesem genormten Verfahren fügt der Sender eines Datenpakets vor dem Transfer zu einem Nachbarswitch einen sogenannten „Tag“ ein, der über eine „VLAN-ID“ die LAN-Zugehörigkeit des Frames anzeigt. Der Empfänger interpretiert den Tag, entfernt ihn und gibt das Paket an Ports des betreffenden VLANs aus oder leitet es über andere Trunks an mit ihm verbundene Switche weiter. Im zweiten Fall wird das Verfahren erneut angewandt.

Die Abbildung zum „Schema 802.1q“ skizziert, wie die Zusatzinformation in einen Frame eingefügt wird. Die Gesamtlänge des Frames wird dadurch übrigens erhöht und kann dadurch das im Zusammenhang von Ethernet „normalerweise“ erlaubte Maximum von 256 Byte überschreiten, was anfangs hin und wieder zu Schwierigkeiten führte, wie etwa zu inkorrekten Fehlermeldungen bei der Überwachung/Aufzeichnung von Übertragungen durch Leitungsmonitore (LAN-Analyzer).



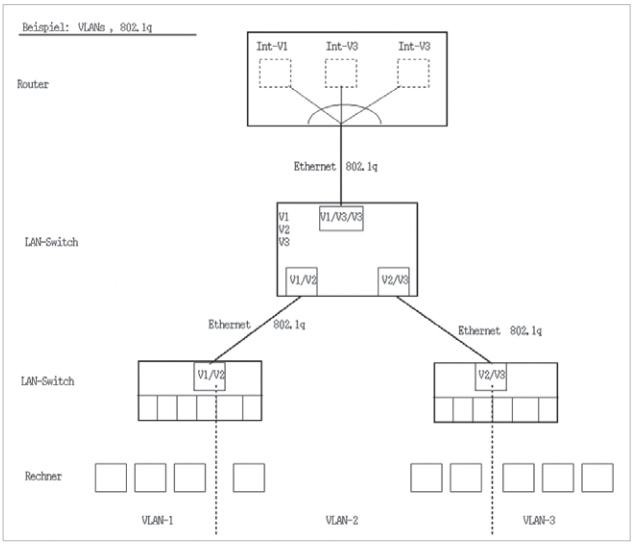
Schema 802.1q

Die beteiligten Switche einer Struktur müssen bezüglich der definierten VLANs bzw. der verwendeten Bezeichnungen (IDs) dasselbe inhaltliche Verständnis haben, sie also bspw. jeweils derselben umfassenden, zusammengehörenden Endgerätegruppe oder demselben verteilten IP-Subnetz zuordnen. Hierzu ist ein sorgsam abgestimmtes Management der Komponenten erforderlich. Zur Unterstützung bzw. Vereinfachung dieser Aufgabe bot der Hersteller Cisco auf seinen Komponenten die Möglichkeit, VLANs an einer Stelle (bzw. in einem der Komponenten) zentral zu verwalten und Informationen darüber über ein „Virtual Trunk Protocol“ (VTP) an alle Geräte der Struktur „automatisch“ zu verteilen.

Mit Hilfe virtueller LANs und dem Einsatz von 802.1q wurde es also möglich, Switch-Strukturen hauptsächlich an geografischen Gegebenheiten auszurichten und lokale Netze darin beliebig zu verteilen. Dies deuten auch die oben dargestellten Beispiele

an. So wurde etwa der Stern im NOZ entsprechend der Gliederung des Gebäudes in Etagen und einer installierten, strukturierten Verkabelung aufgebaut und virtuelle LANs gemäß der Verteilung von Nutzergruppen bedarfsgerecht verfügbar gemacht. Ebenso orientierte sich die interne Struktur im Rechenzentrum an den räumlichen und kabeltechnischen Gegebenheiten. Die Verteilung darin definierter VLANs ist in der Abbildung „Redundante Switch-Struktur im Rechenzentrum, 2009“ auf S. 37 durch die Beschriftungen an den Switchen dargestellt (rlan3, rlan79, rlan334 am Switch lexington).

Die Abbildung „Virtuelle LANs in Netzstruktur (GE)“ stellt in einem „abstrakten“ Beispiel das Konstruktionsprinzip noch etwas näher dar. (Es steht übrigens in Analogie zu einem Beispiel aus Teil 1, Kapitel 5.3.2.2, das in der Mitte einen ATM-Switch enthält, der mit Komponenten über ATM verbunden ist und in dem die virtuellen LANs über die LAN-Emulation realisiert werden).



Virtuelle LANs in Netzstruktur (GE)

Das Beispiel zeigt einen Stern mit einem LAN-Switch im Mittelpunkt, zwei LAN-Switche zum Anschluss von Endgeräten (Rechner) und einen Router (LAN-Switch mit zusätzlich routenden Eigenschaften). Die Struktur enthält drei virtuelle LANs (VLAN-1/2/3), von denen zwei jeweils auf einem Switch (VLAN-1 und -3) und eines (VLAN-2) auf beiden Endgeräteswitchen definiert sind. Die Verbindungen zwischen den Komponenten sind als Ethernet-Trunks mit 802.1q konfiguriert. Der Datenaustausch innerhalb von VLAN-1

und -3 wird jeweils innerhalb der Switche abgewickelt, Datentransfer innerhalb von VLAN-2 erfolgt bei entsprechend verteilten Anschlusspunkten der Endgeräte über den zentralen Verteiler sowie Trunk-Verbindungen. Kommunikationen zwischen verschiedenen VLANs sind auf der Ebene des Switchens nicht möglich, sondern erfordern eine Vermittlung auf Netzprotokollebene. Im Beispiel leistet dies der Router, der sowohl als LAN-Switch per Trunk mit der LAN-Struktur bzw. deren Verteiler verbunden ist, als auch als (IP-)Router pro VLAN ein internes Interface betreibt und Pakete gemäß ihrer IP-Adressen weiterleitet.

Virtuelle LANs und Spanning Tree

Wie etwa im Beispiel der NOZ-Konfiguration angedeutet, kann das Spanning Tree Protocol in einer Struktur mit mehreren virtuellen LANs eingesetzt werden. Dabei gibt es im Prinzip zwei Möglichkeiten:

- Ein gemeinsames Verfahren für alle VLANs: Ermitteln eines für alle gültigen Verteilbaums;
- Separate Anwendung des Verfahrens pro VLAN: Ermitteln eines Verteilbaums pro VLAN (auch als „Multiple Spanning Tree Protocol“ (MSTP) bezeichnet).

Das Verfahren nach MSTP ist komplexer und das Resultat betrieblich schwieriger zu verfolgen. Generell kann es zwar in spezifischen Einzelfällen gezielter auf Störungen reagieren bzw. deren Behandlung unter Umständen auf die Verteilung eines einzigen VLANs eingrenzen. Solche Situationen kamen aber im Kontext der FAU-Netze kaum vor oder waren teilweise sogar unmöglich. Es wurde daher vom RRZE in der Regel nicht angewandt, sondern jeweils ein strukturbezogener, für alle VLANs gemeinsam gültiger Verteilbaum gemäß STP oder RSTP bestimmt.

6.2.2.6 LAN-Switch-Gerätetypen

Wie beschrieben, dienen LAN-Switche als aktive Komponenten der Schicht 2 zum Aufbau von Ethernet-LANs bzw. von zu verteilenden Strukturen. Sie haben eine gleiche Grundfunktionalität und unterscheiden sich in der Form konkreter Geräte durch spezifische Einsatzzwecke oder natürlich auch durch ihren technischen Entwicklungsstand.

Verschiedene Merkmale sind:

- Anzahl und Art ihrer Schnittstellen (Ports):
  - Medien (Glasfaser, TP)
  - Geschwindigkeiten (10, 100, 1000, 10000 Mbp/s)
- Innerer Aufbau (Architektur, Technologie)
  - Fix
  - Modular

- Betriebssystem
  - Gerätemanagement
  - Kommandosprache
- Erweiterte Funktionalitäten und deren Behandlung,
  - Spanning Tree (STP, RSTP, MSTP)
  - VLAN-Definition, Verwaltung, Transfer per 802.1q
  - Spezifische Ergänzungen

Ein Beispiel für verschiedene Gerätetypen eines Herstellers gibt auf S. 43 die Tabelle „Cisco LAN Solutions Produktübersicht“ aus dem Jahr 2001. Sie dokumentiert einen Stand zu Beginn der hier betrachteten Entwicklungsphase und zeigt erste Verfügbarkeiten von Gigabit Ethernet über Glasfaser- sowie Ethernet/FastEthernet über Twisted Pair-Schnittstellen (10/100). Danach war Gigabit Ethernet zunächst für Verbindungen zwischen Switchen, später dann auch zum Anschluss von Endgeräten über Twisted Pair verfügbar. Hierzu kamen an der FAU die Typen „Catalyst 2948G-GE-TX“, „Catalyst 2950“ oder ergänzende Moduleinschübe der „Catalyst4000er“-Modelle zum Einsatz. Alternativ zu diesen Geräten, die mit dem System „CatOS“ (Catalyst Operating System) betrieben wurden, entwickelte Cisco Gerätefamilien mit dem Betriebssystem „IOS“, das eine entsprechende Erweiterung des in den Routern eingesetzten Systems darstellte. Beispiele hierfür sind die fest konfigurierten Geräte „Cisco 3550“, „Cisco 3750“oder die modularen Systeme der „4500er“-Serie, die etwa ab 2006 auch Schnittstellen mit 10 GE enthalten konnten [*CiW4*].

Mittelfristig setzte Cisco auf die IOS-Linie, unterstützte entsprechende Migrationen (vgl. Abbildung „Cisco (2007): Catalyst 4000 Series Linecards Work in the Catalyst 4500“ und begann etwa ab 2006 den Vertrieb der CatOS-Switche einzustellen.

Cisco (2007): „Catalyst 4000 Series Linecards Work in the Catalyst 4500“

Obwohl der homogene Einsatz von Geräten eines Herstellers verschiedene Vorteile zum Beispiel bezüglich einheitlicher Bedienung oder Ersatzteilhaltung hatte, befasste sich das RRZE natürlich auch mit alternativen Produkten. Während aber im Zusammenhang mit ATM-Strukturen unter anderem aufgrund ihres Preis-/Leistungsverhältnisses

	Gigabit Ethernet Ports	Switched 10/100 Ports	Switched 100BaseT Ports	Switched 100BaseFX Ports	Switched 10BaseT Ports	Shared 10/100 Ports	Andere Technologien / Module
Catalyst 3508G XL	8						
Catalyst 3512 XL	2	12					
Catalyst 3524 XL	2	24					
Catalyst 3548 XL	2	48					
Catalyst 2912 XL		12					
Catalyst 2912MF XL (2 modulare Slots)	2	4-8		12-20			• 4 Port geschaltet 10/100 Modul • 2 und 4 Port geschaltete 100BaseFX Module • 1 Port ATM Modul • 1 Port Gigabit Ethernet Modul
Catalyst 2924 XL		24					
Catalyst 2924C XL		22		2			
Catalyst 2924M XL (2 modulare Slot)	2	24		2-8			• 4 Port geschaltetes 10/100 Modul • 2 und 4 Port geschaltete 100BaseFX Module • 1 Port ATM Modul • 1 Port Gigabit Ethernet Modul
Catalyst 1912			2		12		• 1 AUI Port
Catalyst 1912C			1	1	12		• 1 AUI Port
Catalyst 1924			2		24		• 1 AUI Port
Catalyst 1924C			1	1	24		• 1 AUI Port
Catalyst 1924F				2	24		• 1 AUI Port
Catalyst 4003 (3 Slot modulares Gehäuse mit Slot 1 reserviert für Supervisor Maschine)	2-36	32-96		4-8			• 48 Port geschaltetes 10/100 Modul • 32 Port geschaltetes 10/100 plus 4 Port 100BaseFX Modul • 32 Port geschaltetes 10/100 plus 2 Gigabit Ethernet Ports Module • 6 Port Gigabit Ethernet Modul • 18 Port Gigabit Ethernet Modul
Catalyst 4006 (6 Slot modulares Gehäuse mit 1 Slot reserviert für Supervisor Engine	2-90	32-280		4-20			• 32 Ports plus 2 Gigabit mit • Layer-3-Funktionen
Catalyst 4908G-L3	8						Layer-3-Switch
Catalyst 4912G	12						
Catalyst 2848G-L3	2	48					Layer-3-Switch
Catalyst 2948G	2	48					

Cisco-LAN-Solutions-Produktübersicht, 2001

vorrangig Switche von 3Com zum Einsatz kamen, bot dieser Hersteller in Bezug auf Gigabit Ethernet keine passenden Komponenten mehr an. Die Firma verschwand übrigens vorübergehend ganz vom Markt, bis sie 2009 von Hewlett Packard (HP) übernommen wurde. Unabhängig davon bot HP schon zuvor mit der Familie „ProCurve“

LAN-Switche an, die vor allem für Anschlüsse im Endgerätebereich geeignet waren, mit denen von Cisco konkurrieren konnten und preiswerter als diese waren. So kamen ab 2004 an vielen Stellen des FAU-Netzes Switche des Typs „HP 2824“ zum Einsatz.

6.2.3 Entwicklungen zum Internetprotokoll (Schicht 3)

6.2.3.1 Protokollversionen

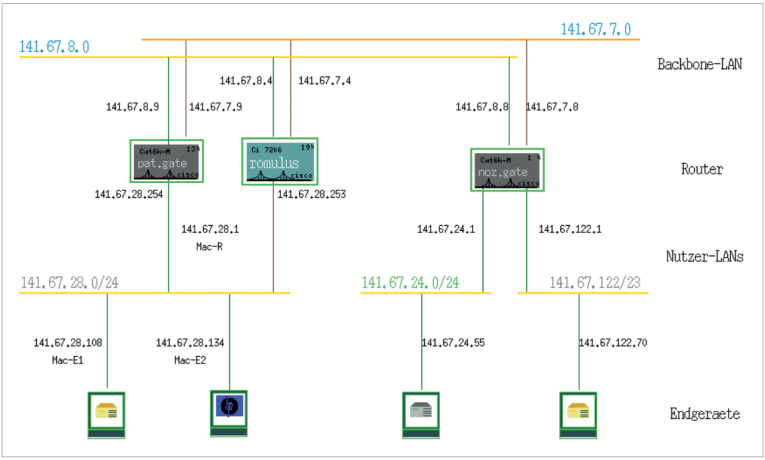
Das Internetprotokoll (IP) hat sich weltweit und insbesondere auch im Rahmen von Hochschulen als Vermittlungsschicht in Netzen weitgehend durchgesetzt. Die dazu beschriebenen Grundlagen des auch als IPv4 bezeichneten Protokolls (vgl. Teil 1, Kapitel 4.3) sind weiterhin gültig und wurden im Kern nur geringfügig verändert, abgesehen von verschiedenen Erweiterungen der zugehörigen Protokollfamilie. Eine Ausnahme bildet aber die 1998 erstmals veröffentlichte Protokollversion 6 (IPv6), deren praktische Einführung sich aus verschiedenen Gründen generell einige Jahre hinauszögerte und erst in jüngerer Zeit verstärkt in Angriff genommen wurde. Dies wird bei der Betrachtung des nachfolgenden Zeitabschnittes (Kapitel 7) im Zusammenhang aktueller Entwicklungen näher beschrieben.

6.2.3.2 Aspekte der Ausfallsicherheit

IP-Netzwerke werden durch routende Komponenten (Router) gebildet, die nach Bedarf und Gegebenheiten, aber ohne strukturelle Einschränkungen miteinander verbunden sind (vgl. Teil 1, Kapitel 4.3.6). Die Informationen zur Wegelenkung von Datenpaketen erhalten sie durch statische Konfigurationen oder den dynamischen, gegenseitigen Austausch über den Einsatz definierter Routingprotokolle (RIP, OSPF). Die Router führen danach regelmäßig aufgefrischte Tabellen, nach denen sie für jedes erhaltene Paket jeweils den nächsten Router (next Hop) zur Weiterleitung auswählen. Durch die Berücksichtigung in den Routing-Tabellen enthaltener Gewichtungen, etwa abgeleitet von Verbindungsgeschwindigkeiten oder der Anzahl zu durchlaufender Komponenten (Hops), werden die Wege entsprechend optimiert. Eine Struktur kann also zwischen zwei Endpunkten mehrere, alternative Pfade enthalten. Dies kann bspw. zur Schaffung von Redundanzen genutzt werden, um sich gegen Ausfälle einzelner Komponenten oder Verbindungen abzusichern. Das Verfahren findet dann im Fehlerfall einen alternativen Weg, sofern es die Struktur zulässt. Je nach Größe eines Netzes und der Frequenz ausgetauschter Statusinformationen (konfigurierbar durch verschiedene Timereinstellungen in den Routern) dauert es fünf bis zehn Sekunden, bis das Verfahren konvergiert bzw. eine Änderung in allen Komponenten berücksichtigt ist.

Eine etwas anders gelagerte Problematik ergibt sich bezüglich redundanter Zugänge für Endsysteme. Diese könnten zwar unter Umständen (bzw. Betriebssystemeigenschaften) ebenfalls Routingprotokolle abwickeln und sich so in den beschriebenen Mechanismus eingliedern, wären damit aber in den Netzbetrieb integriert. Derartige Überschneidungen von Verantwortlichkeiten zwischen Netz- und Endsystembetreiber haben sich in der Praxis (des RRZE) nicht bewährt, da bspw. Fehlverhalten von Rechnern Störungen im Netz zur Folge hatten und vom Netzmanagement nicht zu korrigieren waren. Das RRZE gestattet daher in seinen Richtlinien keinen Anschluss routender Endsysteme (vgl. Kapitel 7.3). Unter anderem zur Lösung dieser Problematik, insbesondere aber auch für „einfache“ Systeme (bspw. PCs), hat der Hersteller Cisco das „Hot Standby Router Protocol (HSRP) entwickelt und eine erste Version 1998 im RFC2281 offengelegt. Es erlaubt die Konfiguration zweier Router, die beide dasselbe IP-Netz (bzw. dieselben IP-Netze) bedienen und von denen der eine im Normalbetrieb und der andere nur bei Ausfall des ersten aktiv wird. Dabei wird den Endsystemen eine gemeinsame, „virtuelle“ IP-Adresse einschließlich einer zugeordneten MAC-Adresse als Default-Route zur Verfügung gestellt. Fällt also der primäre Router aus, übernimmt der sekundäre (Standby-Router) dessen Funktion, während die Endsysteme unverändert über ihren Default-Eintrag weiter Daten in das Netz senden können. Die beiden Router tauschen regelmäßig gegenseitig über HSRP Zustandsinformationen aus, um bspw. Ausfallsituationen zu erkennen und entsprechend zu reagieren. Je nach eingestellten Abständen und Reaktionszeiten bezüglich des Informationsaustausches (konfiguriert über „Timer“ in den Routern) liegt die Umschaltzeit etwa zwischen drei und zehn Sekunden.

Die beschriebenen Verfahren zur Absicherung gegen Ausfälle sind in der Darstellung „Redundantes Routing“ auf S. 46 enthalten. Sie zeigt ein abstrahiertes Beispiel aus dem Netz des Universitätsklinikums der FAU. Hier sind drei Router (pat, romulus, noz) über zwei verschiedene LANs bzw. IP-Subnetze (141.67.7.0, kurz „7“ und 141,67.8.0, kurz „8“) miteinander verbunden. Die Router in der linken Bildhälfte (pat, remulus) bedienen dasselbe Endgeräte-Subnetz (141.67.28.0, kurz „28“) und zwar „pat“ primär und „remulus“ in Standby-Funktion. Die Kommunikation zwischen den Routern erfolgt aufgrund entsprechender Gewichtung (hier nicht dargestellte Konfiguration der Geräte) in der Regel über das Subnetz „7“. So findet bspw. ein Paket vom Rechner am linken Rand (141.67.28.108) über „sein“ Netz „28“ den Router „pat“. Von dort aus gelangt es über das Netz „7“ zum Router „noz“ und schließlich über das Netz „122“ zum Rechner auf der rechten Seite (141.67.122.70). Fällt nun bspw. Netz „7“ aus (je nach Realisierung des zugehörigen LANs etwa durch Ausfall eines zu Grunde liegenden LAN-Switches oder eines ELAN-Fehlers in einem ATM/LANE-Konstrukt), sorgt OSPF dafür, dass stattdessen Netz „8“ genutzt wird. Die Endsysteme der linken Seite schicken



Redundantes Routing

ihre Pakete über die eingetragene Default-Route „141.67.28.1“ an das Netz, d. h. im Normalbetrieb an „pat“. Fällt „pat“ aus, aktiviert der Router „romulus“ sein Interface mit dieser „virtuellen“ Adresse und empfängt nun entsprechend gesendete Daten. Die Weiterleitung bspw. an die rechte Seite erfolgt dann gemäß OSPF-Anpassung direkt von „romulus“ zu „noz“ und von dort schließlich zum adressierten Endsystem („141.67.122.70“).

6.2.3.3 Ergänzende Funktionen

Die Hauptaufgabe eines IP-Netzes besteht darin, Datenpakete anzunehmen, gemäß ihrer Zieladresse weiterzuleiten und entsprechend zuzustellen. Dazu kamen im Laufe der Entwicklung noch viele ergänzende Funktionen zur Unterstützung des Netzbetriebes, die entweder in den Routern oder auch in separaten, dedizierten Komponenten bereitgestellt wurden. Davon werden verschiedene, auch im Rahmen der FAU-Netze eingesetzte Erweiterungen im Folgenden kurz erläutert:

Weiterleitung lokaler Broadcasts (Helper Address)

Für verschiedene Dienste wenden sich Clients (Endgeräte) innerhalb ihres lokalen Netzes an Server, um sich zum Beispiel über **DHCP** (Dynamic Host Configuration Protocol) Adressen zuteilen zu lassen. Entsprechende Anfragen werden per (Ethernet-)Broadcasts gestellt und verlassen das betreffende LAN bzw. Subnetz nicht. Soll aber auch ein Server außerhalb des eigenen LANs erreicht werden bzw. ein Server mehrere Clients aus verschiedenen Subnetzen bedienen können, muss der zuständige (begrenzende) Router solche Anfragen erkennen, umsetzen, weiterleiten bzw. als

Broadcast im LAN des Servers weitergeben. Bei Cisco-Routern ist dieser Mechanismus pro Client-Subnetz über das Kommando „ip helper-address“ unter Angabe der Serveradresse zu konfigurieren.

Adressumsetzung (NAT)

Verwendet eine Institution wie die FAU in ihren IP-Netzen „private“, also nicht nach außen routebare Adressen, können entsprechende Systeme nicht über das Internet kommunizieren (vgl. Teil 1, Kapitel 4.3.3.1). Sollte dies in bestimmten Fällen doch erforderlich sein, kann die Kommunikation durch Adressumsetzungen per „NAT“ (Network Address Translation) am Übergang ermöglicht werden. Dabei werden im Verfahren „Source NAT“ in ausgehenden Paketen die Absender durch routebare Adressen (bspw. aus einem definierten Pool) ersetzt und in die zugehörigen Pakete von außen wieder als Zieladressen eingesetzt. Die Zuordnungen werden über dynamisch gepflegte Umsetztabellen organisiert. Erfolgt die Initiative zur Kommunikation von außen, sind in der Regel keine gültigen Tabelleneinträge vorhanden, Systeme mit privaten Adressen also nicht erreichbar. In dem Fall besteht also die Anforderung, Zieladressen eingehender IP-Pakete durch private Adressen zu ersetzen (Destination NAT). Verschiedene Ansätze, etwa durch statische Konfigurationen oder Einbeziehung/Auswertung von TCP-Ports können die Problematik aber nur bedingt lösen. Terminologie und Überlegungen zum NAT-Verfahren wurden erstmals 1999 im „RFC 2663“ veröffentlicht. An der FAU wird Destination NAT ausführlich für Netze mit privaten Internetadressen (bspw. aus dem Adressraum 10.0.0.0) genutzt und über eine dedizierte Komponente (ursprünglich am Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ) in Garching entwickelter „NAT-o-MAT“) abgewickelt.

Verkehrskontrolle, -einschränkungen (Access-Listen, Firewalls)

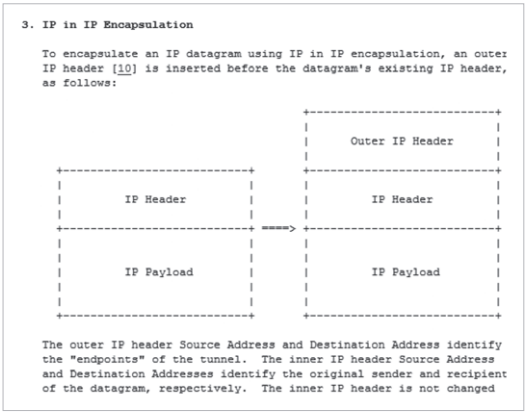
In der Grundkonzeption erlauben Netze auf Basis des Internetprotokolls beliebige Kommunikationsbeziehungen, d. h. jeder Teilnehmer kann jedem Teilnehmer über dessen Zieladresse Daten zusenden und umgekehrt von ihm empfangen. Es liegt auf der Hand, dass derartige Freizügigkeit sowohl im institutionellen Rahmen einer Universität oder eines Klinikums, als auch im globalen Internet nicht ungefährlich ist und zu Problemen führen kann. Allein unter Aspekten von Datenschutz und Sicherheit sind daher gezielte Maßnahmen zur Verkehrskontrolle und gezielten Einschränkungen angebracht. Eine Methode der Zugangskontrolle besteht in der Prüfung einzelner IP-Pakete auf bestimmte Inhalte (vornehmlich im IP-Header), bspw. in deren Ablehnung oder Weiterleitung je nach enthaltener Zieladresse. Derartige Paketfilter (bezogen auf Schicht 3) sind in der Regel auf Routern im Zusammenhang sogenannter „Access-Listen“ verfügbar und dort im Einsatz. Komplexere Prüfungen, die darüber hinaus in der Lage sind, ganze Kommunikationsvorgänge über mehrere Schritte zu verfolgen oder

das Verhalten auf Anwendungsebene (Schicht 4-7) zu überprüfen, werden meist auf dedizierten Komponenten (Firewalls) abgewickelt. (Sicherheitsproblematik und damit verbundene Maßnahmen des RRZE werden in Kapitel 7.3.3 näher behandelt).

Tunnel im IP-Netz

Die Tunneltechnik beinhaltet die Bildung von Datenkanälen durch ein IP-Netz und ermöglicht darüber transparente, von der Struktur des Netzes unabhängige Übertragung von Daten. Ein Tunnel wird zwischen zwei Endpunkten des Netzes bzw. deren IP-Adressen definiert, etwa zwischen einem Endgerät und einem Server oder zwei Routern, die diese Technik entsprechend unterstützen. Dabei werden Dateneinheiten auf der sendenden Seite als Nutzerdaten in IP-Pakete mit Absender- und Zieladresse der Tunnelenden eingepackt, über das Netz zum Empfängerpunkt geroutet und dort wieder entpackt und je nach Kontext weiterbehandelt. Dazu gibt es verschiedene Tunnelprotokolle und Anwendungsszenarien, die teils proprietär und teils als „Standards“ definiert sind.

Eine Anwendung besteht in der Verknüpfung zweier verteilter Segmente zu einem gemeinsamen Ethernet-LAN über einen **L2-Tunnel** (bspw. gemäß dem Layer 2 Tunneling Protocol, L2TP). Dabei werden also Ethernet-Frames in UDP-Datagramme eingebettet und im IP-Netz entsprechend transferiert. Die Verbindung der Segmente erfolgt gemäß einer Bridge-Funktionalität. Im Vergleich zu anderen, ähnlichen Ansätzen wurde das L2TP in den Versionen 2 und 3 von der IETF als RFC 2661 bzw. RFC 3931 definiert und veröffentlicht. An der FAU wurden L2-Tunnel vor allem im Zusammenhang mit drahtlosen Netzen genutzt (vgl. Kapitel 6.3.5, 6.3.5.2). Ansonsten passt(e) das Zusammenfügen (weit) verteilter LAN-Segmente nicht in das hierarchische, in Distributionsbereiche gegliederte Strukturkonzept des RRZE (vgl. Kapitel 6.4).



RFC 2003, IP Encapsulation within IP

Eine andere Art der Tunnelnutzung erfolgt auf der Netzwerkebene über **L3-Tunnel** oder „IP in IP“. Sie können zur Vereinigung zweier entfernt gelegener IP-(Sub-)Netze über ein größeres Netz (bspw. dem der FAU oder dem Internet) genutzt werden. Dazu werden komplette IP-Pakete des (Sub-)Netzes als

Daten zum Senden in Pakete eingepackt, die im „Outer“ IP-Header u. a. mit den Adressfeldern der Tunnelendpunkte besetzt sind. Das Routing erfolgt also auf Basis der Tunneldefinition ohne Ansicht der Informationen des originalen Pakets. Dies illustriert die Skizze „RFC 2003, IP Encapsulation within IP“ aus dem RFC 2003, der die Technik 1996 erstmals beschrieb.

Mit Hilfe von L3-Tunnel könnten verteilte Nutzergruppen, ähnlich wie bei der L2-Tunnelbildung, ein gemeinsames Subnetz über Bereichsgrenzen hinaus nutzen, was aber ebenso der klaren Strukturierung des Universitätsnetzes widerspräche.

Eine andere, prinzipielle Möglichkeit besteht darin, innerhalb von Endsystemen, Tunnel über das Universitätsnetz und das Internet zu externen Partnern aufzubauen, um darüber entsprechend zu kommunizieren. Dies kann zwar die Einordnung in ein privates (nicht extern geroutetes) Subnetz überwinden, birgt aber für den Netzbetreiber gravierende Sicherheitsrisiken, da dadurch Kontrollmechanismen unterlaufen und Missbräuche (unzulässige Kommunikationsbeziehungen) möglich werden. Derartige Anwendungen sind daher im Netz der FAU nicht zugelassen, zumal entsprechende Anforderungen meist im Rahmen anderer, komplexerer Lösungen erfüllt werden können. Diese beruhen zwar auf der Tunneltechnik, erweitern sie aber etwa um Verschlüsselungen und spezifische Protokolle (vgl. VPN).

Virtual Private Network (VPN)

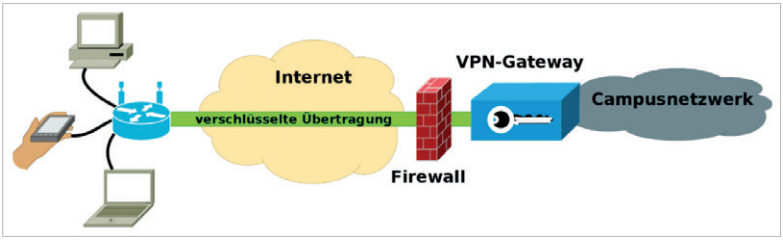
Mit „Virtual Private Network“ (VPN) wird allgemein ein virtuelles, privates Netzwerk bezeichnet, das über ein (öffentliches) (IP-)Netz als Transportmedium verknüpft ist. Es bietet den Teilnehmern eine in sich abgeschlossene, geschützte Umgebung und ist konzeptionell unabhängig von der Struktur des Trägernetzes (allgemein betrachtet sogar auch von dessen Netzwerkprotokoll). VPNs gibt es in verschiedenen Ausprägungen und Realisierungen sowie mit unterschiedlichen Anwendungsschwerpunkten.

Im einfachen Fall, zu dem auch eine entsprechende Dienstleistung des RRZE gehört, werden einzelne Endgeräte über ein öffentliches Netz (Internet) mit dem Netz einer Universität (Campusnetzwerk) verbunden, und zwar geschützt und (weitgehend) ausgestattet mit Zugriffsrechten eines internen Anschlusses. Dabei stehen die Teilnehmer(-Endgeräte) mit einem am Übergang zum Universitätsnetz betriebenen „VPN-Gateway“ in einer Client-Server-Beziehung, wobei zum Server (an der FAU) folgende Merkmale und Funktionen gehören:

- Abgestimmtes Protokoll zwischen Client und (VPN-)Server
- Vorausgesetzte Implementierung von Client-Software
  (Varianten: Vorzugsweise „Cisco AnyConnect Secure Mobility Client“, in Ausnahmen „Open VPN“)

- Aufforderung zur Eingabe von Benutzernummer und Passwort
- Authentifizierung durch den Server über Kontakt mit der Benutzerverwaltung
- Etablierung eines Kommunikationswegs durch Aufbau eines L3-Tunnels zwischen Endgerät und Server
- Zuordnung einer IP-Adresse aus dem Campusnetzwerk (gemäß „NAT“, vgl. S. 46)
- Verschlüsselung übertragener Daten gemäß eines beim Verbindungsaufbau vereinbarten Verfahrens

Die Skizze zum „VPN-Dienst an der FAU“ stellt das Prinzip einer externen Verbindung in das Universitätsnetz der FAU schematisch dar. Die Daten werden darin in einem eigenen „abgeschirmten“ Tunnel über das Internet verschlüsselt zum „VPN-Gateway“ übertragen und mit originalem Inhalt sowie angepassten Adressen im Campusnetz weitergeleitet. Die generellen Kontrollen am externen Übergang (Firewall) zum Universitätsnetz greifen dabei in der Verbindungsaufbauphase.



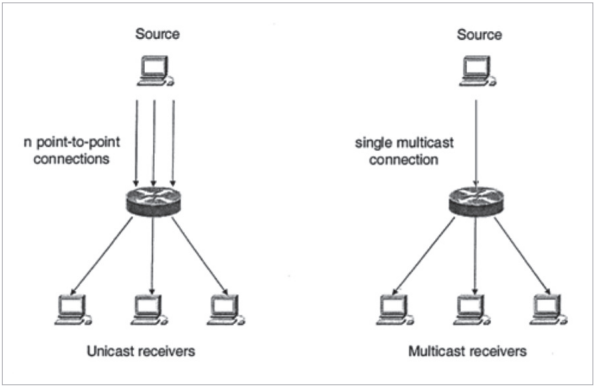
VPN-Dienst an der FAU

6.2.3.4 IP-Multicasting

Weitere Ergänzungen bzw. Erweiterungen der IP-Protokollfamilie sind mit dem IP-Multicasting verbunden, das erweiterte Kommunikationsbeziehungen ermöglicht. Es nutzt ergänzende Definitionen und zusätzliche Protokolle zur Verteilung einzelner Datenströme an mehrere Netzteilnehmer. Diese Kommunikationsform ist für Anwendungen wie Telekonferenzen, Videodienste, TV-Übertragungen, Finanzinformationsdienste oder Netzinformationsdienste charakteristisch, denen das IP-Multicasting eine Grundlage zur effektiven Umsetzung bietet. Es enthält zugehörige Adresskonventionen (Multicast-Adressen), bestimmte Verfahrensweisen zur Verwaltung von Kommunikationspartnern (dynamisches Gruppenmanagement), An- und Abmeldevorgänge (per IGMP) oder spezifische Routingprotokolle (bspw. PIM, DVMRP).

Multicast-Prinzip

Das Multicasting bietet gegenüber der üblichen Kommunikation zwischen zwei Endsystemen (1:1-Beziehung) effiziente Möglichkeiten zum (gleichzeitigen) Versenden von Daten eines Senders an mehrere Empfänger (1:n-Beziehung). Prinzipiell lassen sich Anforderungen zur Verteilung von Daten an mehrere Partner auch auf Anwendungsebene lösen, indem etwa der Sender zu jedem Empfänger einzelne (unicast) Verbindungen aufbaut und darüber mehrere Datenströme parallel erzeugt. Je nach Datenmenge, Anzahl und Verteilung der Empfänger ist damit eine starke Belastung des sendenden Servers, seines Interfaces, aber auch des genutzten Kommunikationsnetzes verbunden, das die Daten entsprechend mehrfach weitertransportieren muss. Bei Nutzung des Multicastings tritt an die Stelle mehrerer Einzelverbindungen (n point-to-point connections) eine einzige Verbindung (single multicast connection) zum Netz, das dann Vervielfältigung, Verteilung und Zustellung der Daten übernimmt (vgl. Abbildung zum „Multicast-Prinzip“ aus [*DreßM*]).



Multicast-Prinzip

IP-Adressierung

Zur (1:n)-Kommunikation bilden Sender und Adressaten eine Gruppe, der eine gemeinsame IP-Multicast-Adresse zugeordnet ist. In der Internetprotokoll-Version IPv4 ist hierfür der Adressbereich zwischen 224.0.0.0 und 239.255.255.255 reserviert. Dabei sind Netze aus dem Adressraum 239.0.0.0/8, vergleichbar mit den privaten Unicast-Adressen, nur für eine lokale Nutzung vorgesehen. Außerdem sind verschiedene Adressbereiche für bestimmte Gruppen reserviert (224.0.0.1 für „Alle Hosts im Subnetz“, 224.0.0.2 für „Alle Multicast-Router im Subnetz“, 224.0.0.3 für „Alle DVMRP-Router“ oder 224.0.0.5 für „Alle OSPF-Router“). Die Multicast-Adressen können statisch fixiert sein oder auch dynamisch zu temporärer Nutzung bezogen werden.

Gruppenmanagement

Zur Organisation von IP-Multicast-Gruppen dient das „Internet Group Management Protocol“ (IGMP), das in erster Version (IGMPv1) 1989 im RFC 1112 spezifiziert wurde. Darauf folgten 1997 die Überarbeitungen IGMPv2 in RFC 2236 sowie 2002 IGMPv3 in RFC3376. Diese Definitionen gelten ausschließlich für die IP-Version 4 (in IPv6-Netzen übernimmt das ähnliche „Multicast Listener Discovery“ (MLD) entsprechende Funktionen (vgl. Kapitel 7)).

Über das IGMP tauschen Netzteilnehmer nach definierten Paketformaten Informationen mit dem (primären) Router des betreffenden Subnetzes aus. Dazu gehören insbesondere regelmäßiges Propagieren bzw. Nachfragen des Routers (Queries), das Eintreten in eine Gruppe als Empfänger (Join per Query-Response) sowie das Verlassen (Leave) einer Gruppe (in Version 1 nur implizit über ausbleibende Responses). Der Router verwaltet damit für jede Gruppe die Subnetze, in denen sich zugehörige Empfänger befinden, d. h. an welche(n) Schnittstelle(n) er vom Sender erhaltene Daten weiterleiten bzw. vervielfachen muss. (Aktive) Empfänger außerhalb seines direkten Einzugsbereiches und die Notwendigkeit von Transfers an benachbarte Router erkennt er, ähnlich wie im Fall von Unicast-Paketen, anhand spezifischer Routingtabellen, die über entsprechende Protokolle und Verfahren aufgebaut und gepflegt werden.

Bearbeitung in lokalen Netzen (Ethernet-LANs)

Gemäß Ethernet-Spezifikation sind bestimmte Geräteadressen (MACs) für Multicast-Zwecke reserviert. Daten-Frames, die an eine Gruppe angeschlossener Teilnehmer gesendet werden sollen, enthalten demnach MACs, die durch ein (auf „1“) gesetztes „Multicast-Bit“ gekennzeichnet sind (dem niederwertigsten Bit des vordersten Oktetts der Adresse (vgl. Skizze zur „Multicast-Ethernet-Adressen“ aus [*DreßM*]).

Multicast-Ethernet-Adressen

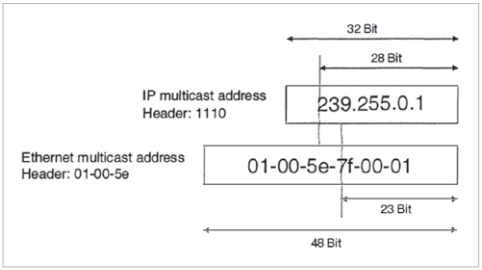


Abbildung von IP-Multicast- auf Ethernet-Adresse

Im Rahmen von IP-Multicast werden für entsprechende Gruppen die IP-Adressen (der Schicht 3) nach einer Konvention auf bestimmte Ethernet-Adressen (der Schicht 2) abgebildet. Dabei beginnen die zugeordneten MAC-Adressen mit einer festen

Startinformation (Header) und werden ergänzt durch die untersten 23 Bits der IP-Adresse der betreffenden Gruppe. Dass diese Abbildung nicht eindeutig ist, wird in Kauf genommen, da lokale Konflikte als unwahrscheinlich eingestuft werden.

Die Skizze zur „Abbildung von IP-Multicast- auf Ethernet-Adresse“ auf S. 52 zeigt als Beispiel die Bildung der MAC-Adresse aus der IP-Adresse „239.255.0.1“ mit dem festen Header „01-00-5e“ und der angefügten Folge „7f-00-01“. Dabei entsteht „7f“ (dual „111 1111“) aus „239.255“ (dual „1110 1111“) durch Streichen der obersten fünf Bits (gemäß der Übernahme der 23 untersten Bits der 28 Bits umfassenden, gesamten IP-Adresse).

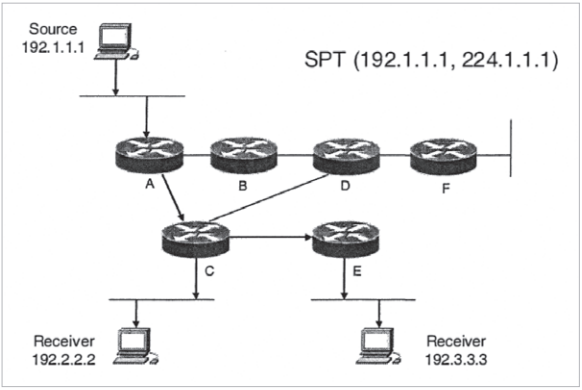
Generell erreichen Multicast-Frames im Ethernet als BUS-Medium alle Teilnehmer des lokalen Netzes, die dann entscheiden, ob sie diese zur internen Verarbeitung annehmen oder nicht. Werden in einem geswitchten LAN solche Pakete jeweils wie Broadcasts an alle Teilnehmer versandt, kann dies zu unnötigen Lastsituationen führen. Um zu erreichen, dass Multicast-Frames innerhalb eines LAN-Switch-Verbundes nur dorthin verbreitet werden, wo sich auch Empfänger einer betreffenden Gruppe befinden, wurden verschiedene Verfahren entwickelt. Dazu gehören das herstellerspezifische „CGMP“-Verfahren von Cisco (Cisco Group Management Protokoll) und das quasi genormte „IGMP-Snooping“ (beschrieben 2016 im RFC 4541). Beim CGMP arbeiten Router und Switche zusammen, wobei der Router als zentrale Instanz die (aktive) Gruppenzugehörigkeit von Endsystemen bzw. deren MAC-Adressen verwaltet und die LAN-Switche darüber informiert. Aus den jeweils aktuellen Informationen können sie ableiten, welche (Unicast-)MAC-Adressen in welcher Gruppe aktiv sind und entsprechende Multicast-Frames an die einzelnen Teilnehmer gezielt zustellen. Das IGMP-Snooping arbeitet dezentral, setzt aber bestimmte, für LAN-Switche eigentlich untypische Eigenschaften bzw. Fähigkeiten voraus. Zum Vermitteln von Ethernet-Frames (Schicht 2) anhand ihrer MAC-Adressen benötigen sie Intelligenz der höheren Protokollebene (IP, Schicht 3), um im betreffenden Kontext zugehörige Daten lesen und interpretieren zu können. Im Snooping-Verfahren werden nämlich von LAN-Switchen die Vorgänge des IGMPs verfolgt und zum Aufbau eigener Verteiltabellen ausgewertet. Dazu gehört das Erkennen des Beitritts oder Verlassens einzelner Teilnehmer einer Gruppe und natürlich das gezielte Zustellen von Multicast-Frames gemäß ermittelter Zuordnung von Unicast-MAC-Adressen. Im Zuge wachsender Leistungsfähigkeit der Switche hat sich der Einsatz des genormten IGMP-Snoopings gegenüber dem (für Switche einfacheren) herstellerabhängigen Verfahren auch am RRZE durchgesetzt.

Multicast Routing

Für das Weiterleiten von Multicast-Paketen über Router-Grenzen hinweg gibt es verschiedene Verfahren, die vom „flooding“ (Verteilen der Pakete an alle Schnittstellen

mit Ausnahme der Schnittstellen, über die die Daten jeweils empfangen wurden) bis zum abgestimmten, komplexen Aufbau von Verteilbäumen über spezifische Routingprotokolle reichen.

Eine Grundlage besteht im Ermitteln der kürzesten Wege innerhalb eines IP-Netzes vom Sender bzw. dessen Router zu den (registrierten) Empfängern der betreffenden Multicast-Gruppe, d. h. der Bildung eines als „SPT“ (Shortest Path Tree) bezeichneten Verteilbaumes. Die Abbildung „Verteilbaum „SPT“ (Shortest Path Tree)“ (entnommen [DreßM]) skizziert dazu ein Beispiel mit einer Multicast-Gruppe (Adresse „224.1.1.1“), dem Sender („192.1.1.1“) und zwei Empfängern („192.2.2.2“ und „192.3.3.3“), verteilt in einem Netz aus sechs Routern (bezeichnet mit A-E). Der zugehörige SPT ist mit Hilfe von Pfeilen dargestellt (gegenüber den einfachen Linien der Router-Struktur).



Verteilbaum „SPT“ (Shortest Path Tree)

Danach erreichen von der Quelle (Source) ausgesandte Pakete über den Router „A“ den Router „C“, der sie (unter entsprechender Vervielfachung) an „seinen“ Empfänger (Receiver) und den Router „E“ verteilt, von wo sie dann an das bei ihm angeschlossene Netz bzw. den dort lokalisierten Empfänger geschickt werden.
Der Aufbau von Multicast-Verteilstrukturen erfolgt durch Kommunikation zwischen den beteiligten Routern über entsprechende Routingprotokolle. Hier werden unterschieden:

- „Dense mode“-Protokolle, „push“-Prinzip
  - DVMRP (Distance Vector Multicast Routing Protocol), RFC 1705, 1988
  - PIM-DM (Protocol Independent Multicast – Dense Mode), RFC 3973, 2005
- „Sparse mode“-Protokolle, „pull“-Prinzip
  - PIM-SM (Protocol Independent Multicast-Sparse Mode), RFC 2117, 1988, (überarbeitet 2005, 2016)

  - SSM (Source-Specific Multicast), RFC 4607, 2006
  - CBT (Core Based Trees), RFC 2189, (1997)
- „LINK-State“ Protokolle, Mischung aus dense und sparse mode
  - MOSPF (Multicast Extensions to OSPF), RFC 1584, 1994

Während der „Dense-Mode“ unterstellt, dass die Empfängerstationen im Netz sehr dicht beieinanderliegen und ausreichend Durchsatz ermöglichen, rechnet der „Sparse-Mode“ damit, dass die Empfänger sehr weiträumig über das Netzwerk verteilt sind und wie in einer WAN-Umgebung nur über geringe Bandbreite verfügen.

Ähnlich, wie im Zusammenhang mit Unicast-Verkehr, dienen die Routingprotokolle dem Aufbau von Tabellen zur Verteilung von Multicast-Daten sowie der damit verbundenen Generierung von Verteilbäumen innerhalb eines Router-Komplexes unter Abwicklung bestimmter Algorithmen. Dabei sind unter anderem Eintreten (Join) und Verlassen (Leave) von Teilnehmern zu verwalten und die Verteilinformation entsprechend anzupassen, etwa durch Eingliedern (Grafting) neuer Elemente oder dem Zurückschneiden (Pruning) betreffender Verteilbäume. So versenden Router im PIM-Dense-Mode regelmäßig Informationen (hello messages) an alle PIM-Router (Multicast-Gruppe „All PIM-Routers“, Adresse „224.0.0.1 3“), um anhand entsprechender Rückmeldungen Nachbarschaftsbeziehungen zu ermitteln (push-Prinzip). Im Sparse-Mode erfolgt die Koordination von Multicast-Gruppen bzw. den beteiligten Routern über einen gemeinsam vereinbarten Rendezvous-Punkt. Dieser nimmt Anmeldungen von Multicast-Veröffentlichungen entgegen und beantwortet Anfragen nach entsprechend registrierten Gruppen von interessierten Teilnehmern bzw. von deren zuständigen Routern (pull-Prinzip).

Einsatz

Zum Funktionieren des IP-Multicasting gehört ein abgestimmtes Verhalten der jeweils beteiligten Router, das unter anderem in Anbetracht seiner Vielfältigkeit im globalen Internet kaum zu erreichen war bzw. ist. Einen Ansatz boten das bereits 1992 begonnene internationale „MBone“ (Multicast Backbone) und sein deutscher, vom DFN betriebener Bereich „MBone.de“, der vornehmlich nur für Universitäten und Forschungseinrichtungen verfügbar war. Im kommerziellen Kontext, etwa für TV-Übertragungen, wurde/wird das Verfahren wohl innerhalb der entsprechenden Providernetze eingesetzt (deren interne Strukturen allerdings nach außen weitgehend verborgen sind). Im Kommunikationsnetz der FAU wurde in Abstimmung mit dem DFN das PIM-SM-Verfahren konfiguriert und unter anderem als Basis für Videokonferenzen genutzt. Das IP-Multicasting ist zwar sehr effektiv, verlangt aber auch eine gute Abstimmung zwischen den beteiligten Routern bzw. Netzbetreibern. Im Zuge der Verfügbarkeit „schneller“ Netze wurden daher für entsprechende Anwendungen

oft Lösungen mit dem Aufbau einer Menge einzelner Unicast-Verbindungen (n point-to-point connections) bevorzugt, obwohl diese entsprechend höhere Netzressourcen beanspruchen. Die Bedeutung des Multicastings hat demzufolge zwar abgenommen, bietet mit dem Modell der „single multicast connection“ (vgl. Abbildung auf S. 51 „Multicast-Prinzip“) aber vielen Anwendungen dennoch einen lohnenden Ansatz.

6.2.3.5 Router-Gerätetypen

Die Ablösung der ATM-Technik rechtfertigte sich auch durch entstehende Verfügbarkeit vergleichbarer Übertragungsgeschwindigkeiten auf der Ethernet-Ebene, deren Maximum etwa zur Jahrtausendwende zunächst einen Sprung von 100 Mbit/s auf 1 Gbit/s machte, um dann später auf 10 Gbit/s und mehr zu steigen (vgl. Kapitel 6.3.2.2). Je nach Gegebenheiten waren damit auch entsprechender Ersatz oder Umrüstungen von Netzkomponenten verbunden, um den Wandel adäquat zu vollziehen.

Land	Standort Nummer	Gebäude-Etage	PLZ	Stadt
Germany			91058	Erlangen

Status	Device ID	Positions ID	Übergeordnete Positions ID	Device Type	Hardware Revision	Software Version	Artikel Nummer
alt	gossen	RZ 5974		CISCO-ROUTER 7206			CISCO7206
alt	toptenn	RZ 6161		CISCO-ROUTER 7206			CISCO7206
neu	hospital			CISCO-ROUTER-3640			CISCO3640
neu	ewf	RZ 6620		CISCO-ROUTER-3640			CISCO3640
neu	hector	RZ 8036		CATALYST-4k-S2			WS-C4006=
neu	earth			CATALYST-4k-S2			WS-C4006=
neu	wiso	RZ 6182		CATALYST-4k-S2			WS-C4006=
neu	stargazer(a)	RZ 8257		CATALYST-4k-S2			WS-C4006=
neu	constellation(a)	RZ 8038		CATALYST-4k-S2			WS-C4006=
alt	suedstern	RZ 6693		CATALYST 6509			WS-C6509
alt	general	RZ 6891		CATALYST 6509			WS-C6509
alt	reliant	RZ 7145		Cat6509			WS-C6509
alt	natur	RZ 7348		Cat6509			WS-C6509
alt	hauser	RZ 5973		CISCO-ROUTER 7206			CISCO7206
neu	botany			CATALYST 6509			WS-C6509
neu	enterprise	RZ 8039		CATALYST 6509			WS-C6509
neu	cell			CATALYST 6509			WS-C6509
neu	hector			Cat6509			WS-6509
neu	earth			Cat6509			WS-6509
neu	stargazer(a)			Cat6509			WS-6509
neu	constellation(a)			Cat6509			WS-6509
neu	like			CISCO-ROUTER-7206			CISCO7206VXR
neu-082010	sitak			Cat6509			WS-6509
neu-082010	yamato			Cat6509			WS-6509-E
neu	grissom			CATALYST 6509			WS-C6509
neu	wiso			Cat6509			WS-6509

Geräte im Wartungsvertrag (Auszug), 2010

Eingesetzte Cisco-Router

Das RRZE nutzte in den verschiedenen Entwicklungsphasen der FAU-Netze zur Gestaltung des (IP-)Routings aus verschiedenen Gründen vornehmlich Geräte des Herstellers Cisco. Zum einen bot der Hersteller stets Komponenten auf dem Stand jeweils aktueller Technik, zum anderen half diese Homogenität Kompatibilitätsprobleme zu vermeiden, die andernfalls trotz genormter Protokolle zu verzeichnen waren, vereinfachte sie das im Vergleich zu Switch-Konfigurationen doch komplexere Management durch einheitliche Oberfläche und Möglichkeiten der Automatisierung (vgl. Kapitel 7) oder ermöglichte ein effektives Lagern und Halten von Ersatzteilen/-geräten, bspw. im Zusammenhang mit flexiblem Einsatz von Einschubmodulen.

Die Tabelle auf S. 55 der „Geräte im Wartungsvertrag (Auszug), 2010“ gibt einen Überblick über die in der Migrationsphase im Wissenschaftsnetz der FAU als Router verwendeten Geräte. Darin sind bspw. die Komponenten mit „Device Type“ „CISCO ROUTER 7206“ Geräte mit ATM-Schnittstellen, die dann für den Einsatz im „schnellen“ Ethernet-Kontext nur noch bedingt geeignet waren, während die Geräte „CATALYST 6509“ sowohl ATM- als auch LAN-Schnittstellen bedienen und nachfolgenden Entwicklungen angepasst werden konnten (vgl. Teil 1, Kapitel 5.3.3.3 und folgenden Abschnitt). Diese gingen demnach auch maßgeblich in die Gestaltung des Backbonenetzes (Core) der FAU ein und werden in folgenden Abschnitten näher betrachtet.

Router-Flaggschiff „Catalyst 6500“

Mit den Geräten Catalyst 6500 verfolgte Cisco ein modulares, aktuellen Entwicklungen anpassbares Konzept, das als „Evergreen die Catalyst-Flotte über Jahre als Flaggschiff anführte“ [*CiEck*]. Sie bestehen im Grundausbau aus einem Gehäuse mit Einschubplätzen (Slots) für verschiedenartige Module, einer Backplane zum internen Datentransport (zwischen Modulen) und den je nach Einsatzzweck eingebauten

Geräte der Serie „Catalyst 6500“ in unterschiedlichen Größen

Modulen. Gehäusegröße und maximale Einschubzahl konnten variieren und die Bezeichnung näher spezifizieren, bspw. steht Cat 6509 für den an der FAU hauptsächlich eingesetzten Typ mit neun Einschubplätzen. Die Abbildung der „Geräte Catalyst 6500 in unterschiedlichen Größen“ zeigt eine Reihe von Geräten dieser Baureihe.

Zu den einschiebbaren Modultypen gehörten:

- Zentrale Steuereinheit (Supervisor Engine, SUP), unbedingt erforderlich
- Schnittstellenmodule (Line Cards), mit „8x1GE“ oder „2x10GE“
- Servicemodule mit speziellen Funktionen (gemäß [Cieck]), wie
  - Firewall-Modul, (Adaptive Security Appliance, ASA) mit 20 Gigabit pro Sekunde Firewall-Durchsatz, 300.000 Connections pro Sekunde und 10 Millionen konkurrierenden Connections, 1.000 VLANs
  - Modul zur Lastverteilung (Application Control System, ACE), zur Verteilung von Last auf mehrere, gleichwertige Endsysteme (bspw. Webserver)
  - Wireless-LAN-Servicemodule versorgen als Controller bis zu 500 Access Points und 10.000 mobile Clients (vgl. Kapitel 6.3)
  - Erweiterungsmodule mit jeweils 16 10-Gigabit-Ports, künftig auch 40-Gigabit-Ports

Die Catalyst 6500 stellten sich ursprünglich als zwei, logisch eigenständige Geräte dar, nämlich als LAN-Switch mit Betriebssystem CatOS und als Router mit Cisco-IOS, bis die beiden Funktionen unter einem gemeinsamen Native-IOS-Betriebssystem vereint wurden.

Das funktionale Herzstück eines Cat 6500 bildet jeweils ein zentrales Prozessorboard (CPU, Supervisor Engine), das unter anderem für Management und zentrale Steuerungen zuständig ist. Die CPUs ermitteln Informationen zur Weiterleitung von Paketen und stellen sie den Modulen so bereit, dass diese weitgehend eigenständig in der Lage sind, untereinander Daten ohne Inanspruchnahme der Zentraleinheit zu transferieren. Dies entlastet die CPU, beschleunigt die Vermittlungsvorgänge und vermeidet im Gegensatz zu Konstruktionen früherer Router-Generationen entsprechende Engpässe. Zur Erhöhung der Betriebssicherheit kann ein Gerät auch mit zwei SUPs ausgestattet werden, die sich gegenseitig in Redundanz ersetzen können. Diese Konstruktion ist im Vergleich zu zwei Redundanzen mit zwei eigenständigen Komponenten kostengünstiger, deckt allerdings auch weniger Problemfälle ab. Im Wissenschaftsnetz der FAU kamen beide Konfigurationen zum Einsatz. Cisco hat übrigens für eine Konstellation mit zwei separaten Geräten das Redundanzkonzept eines Virtuellen Switching Systems (VSS) entwickelt, in dem das betreffende Paar eine logische Einheit bildet, die sich der Umgebung als ein singuläres Gerät darstellt. Dabei wird zum Beispiel in aktiver Redundanz die Verkehrslast auf beide Geräte gleichmäßig verteilt. Im Gegensatz zu

den beiden anderen genannten Redundanzmethoden wurde diese Konstruktion an der FAU weder im Klinik- noch im Wissenschaftsnetz eingesetzt, da mit dem VSS eine gewisse Komplexität mit einer eigenen Problematik verbunden war.

Die Supervisor wurden im Laufe der Jahre weiterentwickelt und jeweils als neue Versionen verfügbar. Dies trug zur Leistungssteigerung und zum Schritthalten mit steigenden Anforderungen bei. Als neue Einschübe konnten sie vorhandene CPUs in der Regel problemlos ersetzen. So wurden an der FAU die zunächst eingesetzten Versionen „SUP-1A“, „SUP-2“ etwa ab 2006 durch die Typen „SUP-720“ abgelöst.

Die Servicemodule waren als eigenständige Funktionseinheiten in die Grundgeräte integriert. So konnten Schnittstellen zwischen Switch und Firewallmodul (eingehend und ausgehend) als virtuelle LANs definiert werden und die Übergänge zwischen ihnen entsprechend kontrolliert werden, was deutlich flexibler war als eine Lösung mit externer Firewall zwischen zwei physischen Schnittstellen. Diese Module kamen im Kliniknetz zum Einsatz, um Kontrollen zwischen Subnetzen innerhalb des Klinikums zu ermöglichen. Im Netz der Wissenschaft wurden, unter anderem aus Kostengründen, für derartige Anforderungen stattdessen die etwas „schwächeren“ Mechanismen des Paketfilterns angewandt (vgl. Kapitel 7.4.3.5).

Ebenfalls im Kliniknetz wurden die ACE-Module zur Lastverteilung (Load Balancing) zwischen Servern verschiedener Dienstleistungen (bspw. Patientenverwaltung, Webzugänge) eingesetzt. Im Wissenschaftsnetz wurden derartige Anforderungen später im Zuge der Installation eines Datacenters (vgl. Kapitel 7.2.2.2) mit dedizierten, externen Komponenten gelöst.

Der Ansatz mit den Wireless-LAN-Servicemodulen zur Organisation nicht drahtgebundener Netze war zwar verlockend, bedeutete aber doch eine sehr große Abhängigkeit von Produkten des Herstellers Cisco in diesem Anwendungsfeld. Hier entschied sich das RRZE daher für andere Lösungen (vgl. Kapitel 6.3).

Generell haben sich die Geräte der Serie „Catalyst 6500“ im Einsatz über viele Jahre (beginnend etwa ab 2000) als sehr entwicklungsfähig und flexibel erwiesen. Cisco stellte in diesem Zusammenhang nicht ganz zu unrecht einen „hohen Investitionsschutz“ heraus. Allerdings sind den Geräten im oberen Leistungsbereich durch eine maximale Übertragungskapazität auf der Backplane von 40 Gbit/s je Slot Grenzen gesetzt, die noch höhere Anforderungen nicht mehr erfüllen können. Dennoch sind Geräte dieses Typs aktuell (2018) immer noch nützlicher Bestandteil des Kommunikationsnetzes der FAU, werden aber im Kontext geforderter Anschlussgeschwindigkeiten oberhalb von 10 Gbit/s nach und nach durch Geräte einer neuen Generation ersetzt (vgl. Nexus, Kapitel 7.2.2.1).

6.3 Nichtdrahtgebundene Netze (WLAN)

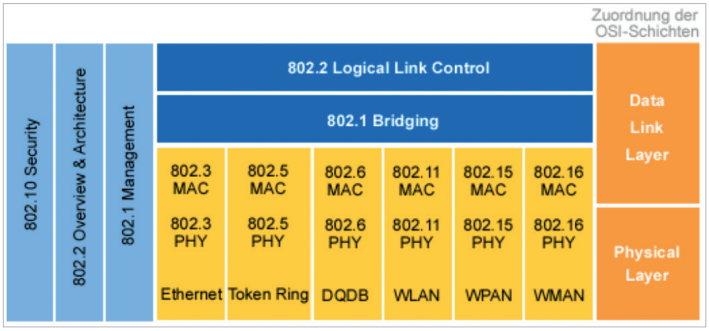
6.3.1 Netzerweiterungen und mobile Zugänge

Nichtdrahtgebundene Techniken zur Datenübertragung wurden im Rahmen der FAU-Netze bereits ab 1995 zur Verknüpfung von Standorten eingesetzt, die über feste Verbindungen nicht leistungsgerecht, nicht bezahlbar oder wegen fehlender Angebote auch überhaupt nicht hergestellt werden konnten. Dazu gehörten die Richtfunkstrecken zwischen Erlangen und Nürnberg (RZ – WiSo) oder solche innerhalb beider Städte (RZ – Tennenlohe, RZ – Nägelsbachstraße, WiSo – Findelgasse und andere). Es gab aber auch lokale Felder, bspw. in verschiedenen Altbauten, die über eine feste Verkabelung kaum voll zu versorgen waren und alternative Lösungen erforderten. Noch bedeutender war aber das Aufkommen neuartiger Anforderungen an die Vernetzung. Während nämlich die passive, strukturierte Verkabelung und das darauf aufbauende aktive Netz vornehmlich Zugänge in Büro- und Arbeitsräumen über Anschlussdosen bereitstellten, entstand und wuchs ein Bedarf an Zugängen in öffentlichen Aufenthaltsbereichen der FAU (Flure, Bibliothek, Mensa), insbesondere für Studierende. Dieser wurde durch die Verfügbarkeit und Verbreitung mobiler Endgeräte, wie zunächst tragbaren PCs (Laptops) oder später Tablets und Smartphones, erheblich gesteigert und nicht zuletzt von der allgemeinen Popularisierung des Internets angetrieben. Das RRZE stellte sich darauf ein, obwohl die damit verbundenen Nutzungen nicht immer im unmittelbaren Zusammenhang hochschulbezogener Anwendungen standen.

Mit der Entwicklung „drahtloser“ lokaler Netze (Wireless LANs, WLANs) und der Verfügbarkeit damit verbundener Komponenten wurde es möglich, den genannten Anforderungen schrittweise nachzukommen und das drahtgebundene Netz um entsprechende Zugänge zu erweitern. Das RRZE begann damit zunächst 2001 im Rahmen eines Pilotprojekts und setzte den Ausbau im Laufe der Jahre systematisch fort, soweit lokale und finanzielle Randbedingungen dies erlaubten.

6.3.2 Technische Einordnung und Standards

Der Begriff „WLAN“ bezeichnet lokale Netzwerke auf Funkbasis. Mit Hilfe der drahtlosen Technik können mehrere Segmente gemäß einer Bridgefunktion zu einem Ethernet-LAN miteinander verknüpft werden. Die Funktionalität wurde von der IEEE erstmals im Standard „802.11“ beschrieben und gliedert sich in Bezug auf das OSI-Referenzmodell in einen Teil der Sicherungsschicht (Data Link Layer) und einer physikalischen Schicht (Physical Layer), die in der Abbildung zur „Einordnung WLAN IEEE 802.11 in die IEEE-Standards“ im gestrichelten Rechteck mit „MAC“ bzw. „PHY“ bezeichnet sind.



Einordnung WLAN IEEE 802.11 in die IEEE Standards

Der nochmal untergliederte „Data Link Layer“ hat im Sinne der Sicherungsschicht die Aufgabe, für zuverlässige Datenübertragung zwischen den Teilnehmern eines WLANs zu sorgen. Wie im Falle drahtgebundener LANs tauscht er über sein „Logical Link Control“ (LLC) mit der darüberliegenden Vermittlungsschicht gemäß Ethernet gebildete Datenframes aus. Seine „MAC“-Schicht erweitert die Frames um verschiedene WLAN-spezifische Informationen, deren Parameter in „IEEE 802.11“ definiert sind, und übergibt sie dem „Physical Layer“. In umgekehrter Richtung nimmt sie Daten im WLAN-Frameformat an und leitet sie nach Auswertung und Entfernung der Parameter als Ethernet-Frames dem LLC weiter. Während das Erkennen von Übertragungsfehlern wie im kabelgebundenen Ethernet über Blockprüfungen erfolgt, wird zur Koordinierung konkurrierender Zugriffe auf das WLAN-Medium ein gegenüber CSMA/CD (vgl. Teil 1, Kapitel 4.2) modifiziertes Verfahren angewandt. Da aus technischen Gründen Kollisionen während einer Übertragung hier nicht erkannt werden können, wird versucht, sie mit dem Vorgehen „Carrier Sense Multiple Access/Collision Avoidance“ (CSMA/CA) möglichst zu vermeiden. Dazu dienen Prüfungen auf Belegungen des Mediums (physikalische Carrier-Sense Funktion) und Abschätzungen über deren Dauer unter Beobachtung oben erwähnter Parameter (virtuelle Carrier-Sense Funktion). Ein Teilnehmer sendet danach nur, wenn bei ihm beide Funktionen das Medium als „frei“ beurteilen, wodurch Kollisionen aber nicht generell verhindert werden können.

Der Physical Layer ist für die Übertragung von Bitfolgen über das Medium zuständig. Er holt also Daten von der darüberliegenden MAC-Schicht ab und wandelt sie durch entsprechende Modulation in Funksignale um. Er ist im WLAN-Kontext relativ komplex und seinerseits in einen medienunabhängigen (Physical Layer Convergence Procedure, PLCP) und einen medienabhängigen Teil zur eigentlichen Signalübertragung (Physical Medium Dependant, PMD) untergliedert. Dabei fügt das PLCP den von der MAC-Schicht erhaltenen Frames für verschiedene Zwecke weitere Daten hinzu und erhöht damit im Vergleich zum originalen Ethernet-Frame den Overhead um bis zu 29

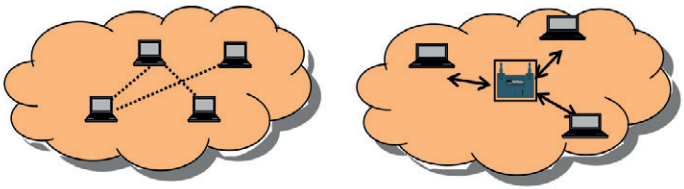
Zeichen (Bytes). Die medienabhängige Ebene PMD enthält, je nach Typ, verschiedene Modulationsverfahren zur Umsetzung von Daten in Funksignale. Sie sind vor allem durch unterschiedliche Leistungsmerkmale bzw. mögliche Übertragungsgeschwindigkeiten gekennzeichnet und in Festlegungen der IEEE spezifiziert und in folgender Übersicht von WLAN-Standards enthalten:

- **802.11** **-1997**, 4 GHz, 1 oder 2 Mbit/s, „Urstandard“ kaum noch genutzt
- **802.11a** **-1999**, 5 GHz, 6, 9, 12,18, 24, 36, 54 Mbit/s
- **802.11b** **-1999**, 2,4 GHz, 11 Mbit/s
- **802.11c** **-1998**, Einheitliches Bridging Model
- **802.11d** **-2001**, Länderspezifische Anpassungen (World Mode)
- **802.11e** **-2005**, Erweiterung zur Qualitätskontrolle (Quality of Service, QoS)
- **802.11g** **-2003**, 2,4 GHz, 54 Mbit/s, Übertragungsstandard für Europa
- **802.11h** **-2003**, 5 GHz, Harmonisierung für Europa, Sendeleistungskontrolle
- **802.11i** **-2004**, Neuer Standard für Sicherheit und Verschlüsselung im WLAN
- **802.11j** **-2004**, 5 GHz, Anpassungen für Japan
- **802.1x** **-2004**, Authentifizierung in Rechnernetzen
- **8802.11n** **-2009**, 2 GHz oder 5 GHz, Datenraten bis zu 600 Mbit/s

6.3.3 Betriebsarten

Die Nutzung der WLAN-Technik ermöglicht zwei unterschiedliche Betriebsweisen, den „Ad-Hoc“-Modus und den „Infrastrukturmodus“. Sie sind in der Abbildung „WLAN-Betriebsarten“ schematisch dargestellt.

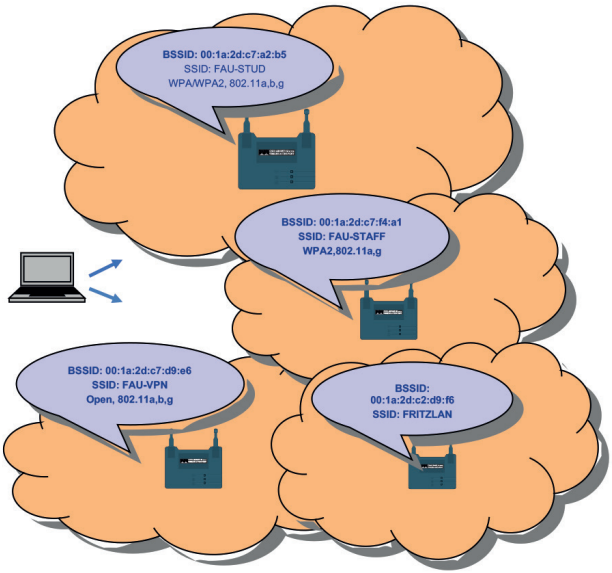
Im **Ad-Hoc-Modus** schließen sich WLAN-Geräte in loser Form ohne eine koordinierende Station zusammen. Dazu müssen sich die Teilnehmer im Vorfeld auf gemeinsame Parameter einigen. Es können also bspw. zwei Partner spontan miteinander kommunizieren, ohne eine zentrale Instanz zu benötigen. Die mangelnde Organisation hat aber auch eine Reihe von Nachteilen, etwa bezüglich Skalierbarkeit oder Sicherheitsaspekten. Daher findet diese Methode kaum Verwendung und ist insbesondere im Zusammenhang mit einem Netzwerk, wie dem der FAU, für den Einsatz nicht geeignet. Allerdings lässt sich ihre Verwendung zwischen zwei Endgeräten nicht verhindern.



WLAN-Betriebsarten: Ad-Hoc-Modus (li.) / Infrastrukturmodus (re.)

Im **Infrastrukturmodus** koordiniert ein als „Access Point“ (AP) bezeichneter, zentraler Manager die Kommunikation innerhalb eines Funkbereichs (Funkzelle). Bei ihm melden sich die WLAN-Teilnehmer an und über ihn wird sämtlicher Datenverkehr abgewickelt. Das erfordert zwar einen gewissen Aufwand an Planung, Installation und Betriebsüberwachung, schafft aber Voraussetzungen für einen geregelten Betrieb.

Ein im Infrastrukturmodus betriebenes WLAN kann aus vielen APs (bis zu mehreren Hundert) gebildet werden, die gemäß der Bridge-Funktionalität miteinander verknüpft sind. Dabei spannt jeder AP in seiner Umgebung eine Funkzelle auf, ein sogenanntes „Basic Service Set“ (BSS), und ist eindeutig durch einen „Basic Service Set Identifier“ (BSSID) gekennzeichnet. Diese Identifikation, die seiner MAC-Adresse entspricht, wird jedem übertragenen Datenpaket in der physikalischen Schicht zugefügt und sorgt so für eine eindeutige Zuordnung von Daten und Funkraum, was bei Koexistenz mehrerer APs/WLANs im gleichen Funkraum unbedingt erforderlich ist. Als übergeordnete Einheiten mehrerer Funkräume werden die WLANs jeweils mit einem „Service Set Identifier“ (SSID) benannt wie die mit „FAU-STUD“, „FAU-STAFF“ oder „FAU-VPN“ bezeichneten Netze an der Universität. Bevor Endgeräte am Betrieb eines WLANs teilnehmen können, müssen sie sich an einem AP anmelden (assoziieren). Dazu benötigen sie Informationen darüber, welche WLANs, APs mit welchen Eigenschaften in ihrer Nähe verfügbar sind. Dazu senden die APs regelmäßig (meist alle 100 ms) Nachrichtenpakete (Beacon-Frames) aus, die über die von ihnen behandelten Netze durch Angabe von Namen (SSIDs) und zugehörenden Betriebsparametern (bspw. unterstützte Verfahren gemäß IEEE der Gruppe 802.11, vgl. Kapitel 6.3.2) oder angewandte Verschlüsselungsverfahren (vgl. Kapitel 6.3.4) informieren. Die Abbildung „Access Points und Informationsdaten“ stellt dazu als Beispiel mehrere APs und im Auszug Inhalte der von ihnen ausgesendeten



Access Points und Informationsdaten

Beacons dar. Derart empfangene Informationen können also von den Endgeräten bzw. über entsprechend aufbereitete Schnittstellen von Benutzern zur Auswahl eines WLANs herangezogen werden.

Die Verknüpfung mehrerer APs zur Bildung übergreifender WLANs kann auch über Funk hergestellt werden, und zwar unter Nutzung der vorhandenen Sendeanlage (inband) oder einer zusätzlichen Sendeanlage auf eigener Frequenz (outband). Im Normalfall werden solche Verbindungen aber per Kabel, mehr noch über Anschlüsse an LAN-Switche und dort gemeinsam genutzte VLANs hergestellt. Ähnlich sind auch die APs der FAU mit dem fest geschalteten Netz verbunden, kommunizieren darüber aber nicht „direkt“ miteinander, sondern tauschen Daten „indirekt“ über spezielle, zentrale Server einer eigens gemanagten WLAN-Struktur aus, die u. a. auch gleichbenannte WLANs in verschiedenen Bereichen organisiert (vgl. Kapitel 6.3.5).

6.3.4 Sicherheitsaspekte

Die Grundkonzeption des Ethernets, in der jeder Teilnehmer alle gesendeten, also auch für ihn nicht bestimmte Datenpakete empfangen kann, birgt verschiedene Sicherheitsrisiken, die im drahtgebundenen Netz unter Einsatz von LAN-Switchen über Einzelanschlüsse erheblich gemindert werden. Ein offenes WLAN hingegen ist allgemein zugänglich, ermöglicht das Mitlesen oder Einstreuen von Daten und gewährt den Teilnehmern Anonymität. Zur Abwehr entsprechender Gefährdungen dienen Verfahren zur Verschlüsselung übertragener Daten sowie zur Authentifizierung von Nutzern.

Bereits in der ersten Festlegung 802.11 der IEEE wurde unter der Bezeichnung **WEP** (Wired Equivalent Privacy) ein Standard definiert, der sowohl den Zugang zum Netz regeln als auch die Vertraulichkeit und Integrität der Daten sicherstellen sollte. In dem Verfahren wird vom teilnehmenden Sender aus einem ihm bekannten festen WEP-Schlüssel des betreffenden WLANs (bzw. BSS) und eines pro Datenpaket generierten Initialisierungsvektors jeweils ein sogenannter Keystream berechnet, der unter Einbeziehung der Daten zu einer verschlüsselten Sequenz verknüpft wird. Das übertragene WEP-Gesamtpaket enthält auch den benutzten Initialisierungsvektor, sodass der Adressat in der Lage ist, die Ausgangsdaten zu rekonstruieren. Der WEP-Schlüssel dient auch zur Authentifizierung, d. h. jeder Client mit korrektem WEP-Schlüssel bekommt Zugang zum Netz. Wegen verschiedener Schwachstellen, etwa bedingt durch die zu geringe Länge (24 Bit) des Initialisierungsvektors sowie gelungener Versuche, den Schlüssel zu „brechen“, wurden schon bald alternative Lösungen erforderlich. Die Arbeitsgruppe 802.11i der IEEE befasste sich daher mit der Ausarbeitung neuer Sicherheitsstandards und entwickelte als „schnelle“ Lösung zunächst den als WPA (Wi-Fi Protected Access), dann als **WPA-1** bezeichneten

Mechanismus und veröffentlichte 2004 zusätzlich eine komplette, neue Sicherheitsarchitektur, benannt mit **WPA-2**, CCMP (Counter Mode with CBC-MAC-Protocol) oder WPA-AES (Advanced Encryption Standard). WPA-1 arbeitet nach dem gleichen Grundprinzip, wie WEP, verwendet aber einen doppelt so langen (48 Bit) Initialisierungsvektor sowie mehrere, hierarchisch definierte, temporäre Schlüssel (Temporal Key Integrity Protocol, TKIP), die sich mit jedem Paket ändern. WPA-2 basiert auf einem Verschlüsselungsverfahren, das 2000 von Spezialisten des US-amerikanischen NIST (National Institute of Standards and Technology) veröffentlicht wurde und ein sehr hohes Maß an Sicherheit bot und auch derzeit als sicherste Möglichkeit gilt. Es wird deshalb auch im WLAN der FAU vorrangig eingesetzt.

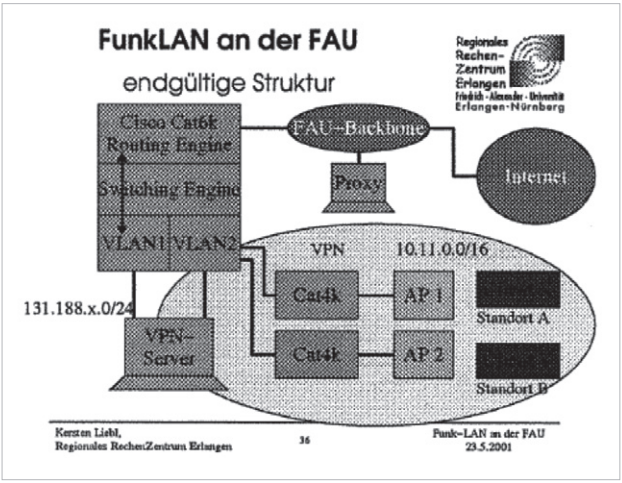
Die verschiedenen Schlüssel von WPA können auch als Grundlage verschiedener Methoden zur Authentifizierung von Nutzern dienen. Allerdings sind diese Verfahren für größere Einrichtungen wie der FAU, nicht praktikabel. Das RRZE stützt sich daher für diese Zwecke auf die von IEEE 802.1x beschriebene Festlegung 802.1x und das „Extension Authentication Protocol“ (EAP) gemäß RFC3748 in der Variante „Protected Extensible Authentication Protocol“ (PEAP). Dabei identifizieren sich die Benutzer durch Angabe von Username und Passwort an einem AP, der sich zur Überprüfung an einen Authentication Server wendet und den WLAN-Zugang entsprechend frei gibt oder ablehnt. Die zentral geführte Benutzerdatenbank (auf einem RADIUS-Server) muss natürlich regelmäßig gepflegt und aktualisiert werden. Sie ist mit der Benutzerverwaltung des Rechenzentrums verknüpft.

6.3.5 Funknetze an der FAU

6.3.5.1 Anfänge (1. und 2. Generation)

Das RRZE befasste sich etwa ab 2000 mit der Einführung von Funk-LANs und startete dazu ein Pilotprojekt, das grundsätzliche Überlegungen, Testinstallationen und Erprobungen an verschiedenen Standorten der FAU beinhaltete. So konnten ab 2001 die ersten Bereiche der Erlanger Innenstadt (Philosophische Fakultät), des Erlanger Südgeländes (Technische Fakultät) und der Nürnberger Langen Gasse (Wirtschafts- und Sozialwissenschaftliche Fakultät) in Betrieb genommen werden. Zum Einsatz kamen hauptsächlich Access Points der Firmen Cisco (Aironet AP342) und Cabletron (RoamAbout) mit der Technik nach 802.11b (2 GHz, 11 Mbit/s). Die Konzeption der ersten Installationen wurde gemäß einer Präsentation am RRZE [*Liebl*] in der Abbildung „Funk-LAN-Struktur an der FAU, 2001“ auf S. 66 skizziert. Sie zeigt zwei Standorte (A, B) mit je einem Access Point (AP1, AP2), die jeweils über einen LAN-Switch (Cat4k) an einen zentralen Switch-Router (Cat6k mit „Switching“- und „Routing

Engine“) angeschlossen sind. Die APs sind über ein gemeinsames VLAN (VLAN2) mit einem „VPN-Server“ verbunden, dem Aufpunkt zur Anmeldung und Weiterleitung ihrer WLAN-Daten. Der VPN-Server ist dazu über ein weiteres VLAN (VLAN1) mit dem Cat6k verbunden, der über das „FAU-Backbone“ die Kommunikation innerhalb des Universitätsnetzes und zum externen „Internet“ vermittelt. Da das WEP für den Einsatz im Hochschulnetz als zu unsicher beurteilt wurde, war in dem Konzept ein VPN-Server als Gegenstück zu den Endgeräten für Verschlüsselung und Authentifizierung zuständig. Da die VPN-Technik und das damit verbundene Protokoll „IPSec“ nur auf „wenigen“ Endgerätetypen in Hard- und Software unterstützt wurden (bspw. auf dem Acer 522TXV Notebook mit Cisco Aironet 542 Funk-LAN-Karte), ließen erste Realisierungen des Funk-LANs auch WEP als Verschlüsselungsverfahren zu, solange bis höherwertige Methoden (bspw. WPA) allgemein verfügbar waren.



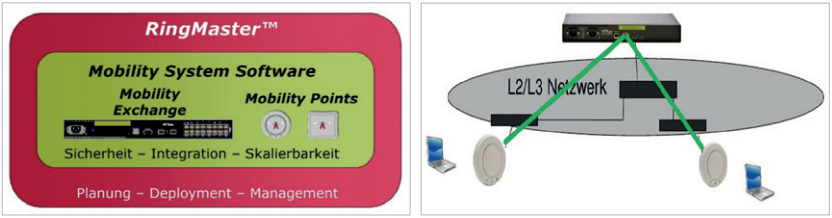
Funk-LAN-Struktur an der FAU, Konzept 2001

Der Installationsaufwand zum Auf- und Ausbau der WLANs erwies sich als sehr hoch und konnte teilweise nur mit Hilfe von Azubis im Rahmen ihrer Ausbildung zum Fachinformatiker (vgl. Kapitel 6.1.2) geleistet werden. Das Interesse an den neuen Möglichkeiten kam vor allem aus dem Mitarbeiterkreis, während es aus der Studierendenschaft zwar rege aber nicht überwältigend war. Das lag vermutlich an den zu dieser Zeit für die meisten Studierenden kaum erschwinglichen Notebookkosten und an den sonst dicht vorhandenen Zugängen der kabelgebundenen Netzinfrastruktur. Es gab zudem auch Befürchtungen, durch ein Funk-LAN würde sich der Elektrosmog intensivieren, mit entsprechend negativen Auswirkungen auf die Gesundheit. Deswegen

wurden an verschiedenen Stellen die Installationsarbeiten zunächst gestoppt. In der Folge entwickelte sich aber ein ständig steigender Bedarf an den neuen Möglichkeiten mobiler Zugänge bzw. deren Verbreitung und Leistungsfähigkeit, dem das RRZE im Rahmen seiner Kapazitäten (personell, finanziell) weitgehend nachzukommen suchte. So wurde neben weiterem Ausbau etwa ab 2004 auch mit einem Generationswechsel der Access Points begonnen, nämlich weg vom Standard 802.11b hin zu 802.11g (2,4 GHz, 54 Mbit/s).

6.3.5.2 AP-Cluster, Konzept von Trapeze (3. Generation)

Ein weiterer Schritt in eine nun 3. Generation begann ab Mitte 2006 mit dem Beginn der Umstellung auf eine neue, einheitliche Technik/Sicherheitstechnik. Sie basierte auf einem Gesamtkonzept des Herstellers Trapeze, das den strukturellen Aufbau, die verwendete Technik, eingesetzte Komponenten sowie Services zu Planung, Betrieb, Management und Sicherheit umfasste. Es enthielt statt den zuvor üblichen „Thick“ Access Points in ihrer Funktionalität stark reduzierte „Thin“ Access Points, bezeichnet als „Mobility Points“ (MPs). Diese wurden nach Bereichen in „Clustern“ zusammengefasst und jeweils von zugeordneten „Controllern“ (Mobility Exchange) bedient und konfiguriert. Sie speicherten selbst keine sensitiven Daten und boten daher diesbezüglich keine Angriffsziele für Hacker. Als übergeordnetes zwar nicht zwingend notwendiges aber kaum verzichtbares Hilfsmittel, enthielt der „Ringmaster“ (Server mit entsprechender Software) verschiedene Managementfunktionen, etwa zur Konfigurationsverwaltung, Softwareverteilung, Netzüberwachung, Statistikführung oder Planung. Wichtige Unterstützung bot der Ringmaster für örtliche Funkfelderkundungen, die im Vorfeld von Installationen zur Planung bedarfsgerechter Platzierungen von APs bzw. MPs unbedingt erforderlich waren. Die Abbildung aus einer Präsentation von Trapeze [*Trap*] stellt die „Elemente des WLAN-Konzepts von Trapeze“ und ihre Zusammenhänge grob dar. Eine weitere Skizze zeigt die prinzipiellen Verbindungen zwischen Controller und Mobility Points über ein fest konfiguriertes „L2-/L3-Netzwerk“.



Elemente des WLAN-Konzepts von Trapeze, Verbindungen zwischen Controller und MPs

In seiner Umsetzung und Gestaltung bezüglich Konfigurierung oder Einbettung in Struktur und Mechanismen eines vorhandenen, drahtgebundenen Netzes ließ das Konzept von Trapeze verschiedene Varianten zu. Zur Realisierung der Kommunikationsstruktur gemäß des obigen Prinzipienbildes wurde an der FAU wie folgt vorgegangen:

- Anschluss der APs (MPs) als Ethernet-Endgeräte an LAN-Switche des vorhandenen bzw. entsprechend erweiterten Universitätsnetzes
- Stromversorgung der APs (in der Regel) über die Anschlussports der Switche gemäß „Power over Ethernet“ (PoE) (entsprechende Eigenschaft der Switche vorausgesetzt)
- Vergabe von Host-IP-Adressen für jeden AP (aus dem privaten Adressraum)
- Zusammenfassung von APs (Cluster-Bildung) über zugehörige Controller (bzw. Mobility Exchanges) in verschiedenen Bereichen, bspw. in Erlangen-Süd oder der Nürnberg-WiSo.)
- Realisierung von Verbindungen zwischen Controller (Mobility Exchange) und seinen zugeordneten APs über (L2-)Ethernet-Tunnel mit den jeweiligen IP-Adressen als Endpunkte. Der Datenaustauch erfolgte demnach also über ein gemeinsames LAN-Segment unter Nutzung des (L3-)IP-Netzes als Transportmedium.

Die so etablierten Datenkanäle konnten also zum Management der APs, aber auch zur Vermittlung von Daten von WLAN-Teilnehmern genutzt werden. Die Controller waren nämlich auch mit dem drahtgebundenen Netz verbunden und konnten so entsprechende Übergänge schaffen. Zur Organisation des WLAN-Betriebs mussten die Controller in ihren Bereichen noch eine Reihe weiterer zentraler Aufgaben erfüllen. Dazu gehörten vor allem die Bearbeitung von Verbindungswünschen und die laufende Verwaltung entsprechend angemeldeter Benutzer bzw. Endgeräte. Dabei erforderten die Vorgänge zum Aufbau und zur Nutzung von WLAN-Verbindungen das Einbeziehen verschiedener, im Netz verteilter Komponenten.

Die folgenden Stichpunkte fassen den Ablauf einer Anmeldung zusammen und geben diesbezüglich einen Eindruck von der Komplexität und den strukturellen Zusammenhängen des WLAN-Betriebs an der FAU:

- Endgerät empfängt verfügbare WLANs über „Beacons“ nahegelegener APs, bspw. FAU-STAFF, FAU-STUD
- Nutzer wählt gewünschtes Netz aus, gibt „verbinden“ an
- Anforderung gelangt über den Funkkontakt mit dem zugehörigen AP und dessen L2-Tunnel zum Controller
- Controller fordert auf umgekehrtem Weg zur Eingabe von Benutzerkennung und Passwort auf
- Endgerät schickt Daten zur Authentifizierung (gemäß Nutzerangabe)
- Controller erhält und verzeichnet Kontaktdaten (u. a. MAC-Adresse des Endgeräts, Benutzerkennung)

- Controller schickt Anfrage an Server der Benutzerverwaltung (RADIUS) zur Prüfung von Kennung und Passwort (mit eigener IP-Adresse) über das IP-Netz nach spezifischem Protokoll
- RADIUS-Server prüft Angaben, ist mit der allgemeinen Benutzerverwaltung des RRZE koordiniert und gibt Resultat zurück
- Bei positiver Antwort ordnet der Kontroller dem Teilnehmer bzw. der akuten Verbindung ein VLAN zu (aus einem Pool des betreffenden WLANs) und speichert die Zuordnung
- Endgerät erhält positive Meldung (vom Controller über AP und Funkverbindung)
- Controller handelt mit Endgerät Mechanismus zur Verschlüsselung aus
- Endgerät fordert IP-Adresse per DHCP an (Ethernet-Broadcast)
- Controller leitet Anfrage im VLAN des Endgeräts an den zugehörigen Bereichs-Router weiter (über Trunk-Verbindung mit dem LAN-Baustein des Routers)
- Router schickt gemäß „Helper-Eintrag“ Anfrage an DHCP-Server weiter (im IP-Netz)
- DHCP-Antwort mit IP-Endadresse gelangt über Router, Controller, AP zum Endgerät
- Endgerät ist nun auch Teilnehmer im Subnetz des zugeordneten VLANs
- (IP-)Daten gelangen über Funkverbindung zum AP, über den Tunnel zum Controller, dem zugeordnetem VLAN (mit passendem „Tag“) zum Switch/Router, dem Subnetz-Interface des Routers in das IP-Netz der FAU bzw. ins Internet (und umgekehrt).

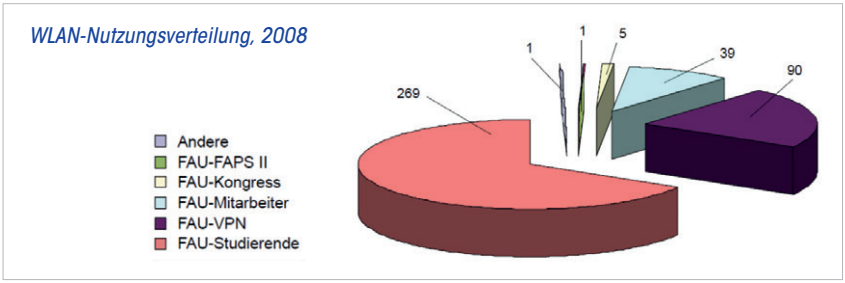
6.3.5.3 FunkLAN-Ausbau und -Nutzung

Während der Aufbau des WLANs in der Projekt- und ersten Betriebsphase etwa 35 Access Points umfasste, war es zur Jahreswende 2006/2007 auf genau 100 Access Points mit folgender Verteilung ausgebaut:

- Informatikhochhaus inklusive Bibliothek, CIP-Pool, EG (17)
- Informatik im RRZE-Gebäude (4)
- RRZE (10)
- Erlangen, Südgelände (21)
- Erlangen, Innenstadt (22)
- Nürnberg, WiSo (26)

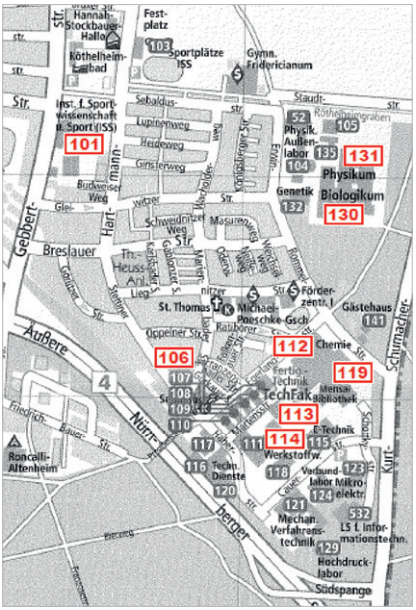
Durch unterstützende Finanzierung aus Studienbeiträgen und Eigenmitteln von Instituten ging der Ausbau des WLANs der FAU weiter zügig voran. Die Anzahl aller Access Points zusammen belief sich 2008 bereits auf 250 und bescherte einen neuen Nutzungsrekord: Am 9. Dezember 2008 waren erstmals über 400 Personen gleichzeitig aktiv – in überwiegender Mehrzahl Studierende (vgl. Grafik „WLAN-Nutzungsverteilung, 2008“).

Die Grafik wurde übrigens mit Hilfe des zentralen AP-Managements und eines zugehörigen Auswertungstools aus dem zu der Zeit bereits umgesetzten Trapeze-Konzept erstellt. Das Interesse der Studierenden am WLAN hatte sich also gegenüber den



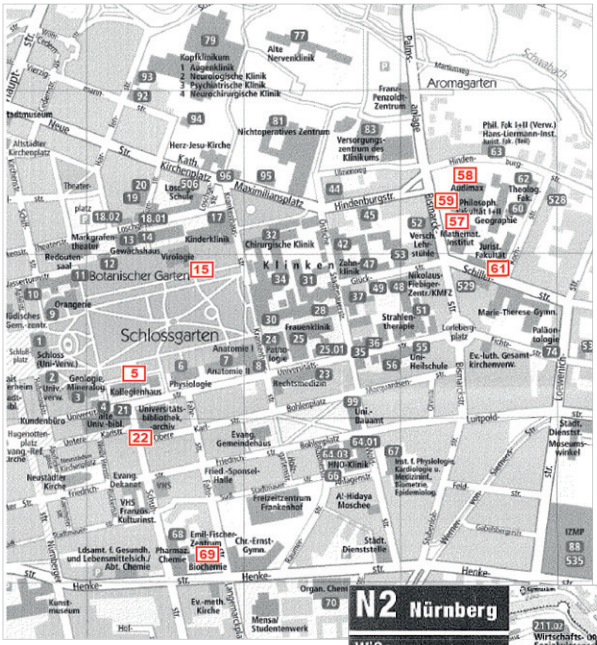
zögerlichen Anfängen im Zuge wachsender Verfügbarkeit mobiler Endgeräte enorm entwickelt und stellte eine starke Triebfeder für den Ausbau dar, der nicht zuletzt durch abgesprochene Nutzung von Mitteln aus Studienbeiträgen verfolgt werden konnte. Die 2008 erreichte örtliche Verfügbarkeit lässt sich aus den Stadtplänen der Abbildungen „WLAN-Ausbau für Studierende“ ersehen, die zu jedem Gebäude die Anzahl der Access Points anzeigen (entnommen dem Jahresbericht des RRZE von 2008).

Der zu 2008 skizzierte Status stellte aber erst den Beginn einer rasanten Entwicklung dar. Auch in den darauffolgenden Jahren wurde das Funknetz der FAU kontinuierlich planmäßig ausgebaut und erreichte gegen Ende des hier betrachteten Zeitabschnitts



Gebäude	Access-Points
101 (SportZ)	3
106 (Tech. Mech.)	2
112 (Chemie)	4
113 (Informatik)	4
114 (WW / B)	11
119 (MHB)	12
130 (Biologikum)	4
131 (Physikum)	2
RRZE-Helpdesk	2
	44

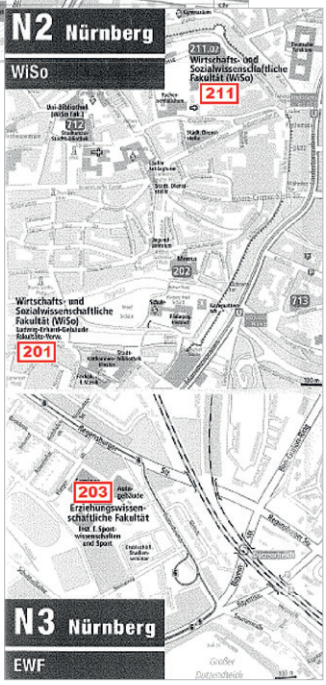
WLAN-Ausbau für Studierende, erste Ausbaustufe 2007/2008 (Erlangen - Südgelände)



Erstellt durch Ingenieurbüro für Kartographie Bernhard Spachmüller

WLAN-Ausbau für Studierende, erste Ausbaustufe 2007/2008 (Erlangen - Innenstadt)

Gebäude	Access-Points
5 (Kollegienhaus)	9
15 (Virologie)	2
22 (Neue Bibliothek)	6
57 (Mathematik)	3
58 (Phil/Audimax)	5
59 (Geographie)	6
61 (Juridicum)	7
69 (Biochemie)	3
Mensa / Studentenwerk	1
Philosophie / Stintzingstraße	3
IZI-Helpdesk	2
IZH-Helpdesk	1
	48



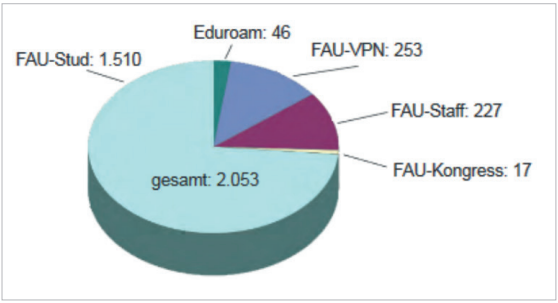
Erstellt durch Ingenieurbüro für Kartographie Bernhard Spachmüller

Gebäude	Access-Points
201 (Findelgasse)	9
203 (Regensburger Straße	14
211 (Lange Gasse)	18
	41

WLAN-Ausbau für Studierende, erste Ausbaustufe 2007/2008 (Nürnberg)

die Zahl von insgesamt 750 Access Points und eine gleichzeitige Aktivität von bis zu 2.000 Nutzern (davon 1.500 Studierende), das entspricht einer Erhöhung um den Faktor 3 (Anzahl APs) bzw. 5 (gleichzeitig aktive Nutzer) innerhalb von drei Jahren (vgl. Abbildung „WLAN-Nutzungsverteilung, 2011“). In diesem Zusammenhang wurden auch einige neue Standorte/Gebäude erschlossen, wie etwa die Flachbauten (Erlangen Südgelände), der Neubau Mathematik/Informatik (Erlangen Südgelände), das Sportzentrum (Erlangen), die Philosophie (Erlangen Zentrum), das AEG-Gelände (Nürnberg) oder das Technikum Uferstadt (Fürth). Dabei wurde in den Bereichen der FAU eine sehr hohe, wenngleich noch nicht vollständige Abdeckung erreicht. Insbesondere aber stellten auch in den folgenden Jahren die immer noch stark steigenden Nutzerzahlen wachsende Anforderungen an Erweiterungen, Verdichtungen und Leistungssteigerungen des funkbetriebenen Netzes.

Wie der Abbildung zur Nutzungsverteilung zu entnehmen ist, unterstützte die WLAN-Struktur auch eine Nutzergruppe „Eduroam“. Education Roaming (eduroam) geht auf eine auch vom DFN-Verein unterstützte Initiative zurück, jedem Angehörigen der daran beteiligten Universitäten und Organisationen mit einer einheitlichen, persönlichen Kennung an jedem der Standorte Zugang zum dortigen Netz und damit auch dem Internet zu ermöglichen. Nach einer einmaligen Registrierung können also „reisende“ Wissenschaftler oder Studierende über das inzwischen international verbreitete eduroam ohne zusätzliche Beantragung von Gastkennungen o. ä. am örtlichen und den drüber hinausgehenden Netzbetrieb teilnehmen [*Edur*].



WLAN-Nutzungsverteilung, 2011

6.4 Netzwerkarchitektur

Auch wenn der Aufbau von Netzen an eine Reihe verschiedener Voraussetzungen gebunden ist, lässt deren Gestaltung noch viele Freiheiten zu. Um aber größere, komplexe Netzwerke, wie etwa die an der FAU, effizient und beherrschbar zu halten, sind grundsätzliche Überlegungen zum Vorgehen erforderlich. Eine wichtige Orientierung, sowohl zum Entwurf als auch zur Beschreibung von Netzwerken, bietet ein in Core, Distribution und Access gegliedertes, hierarchisches Architekturmodell.

6.4.1 Voraussetzungen, Anforderungen, Zielsetzungen

Eine Voraussetzung zum Aufbau einer aktiven Struktur ist das verfügbare passive Netz mit seinen darüber schaltbaren Verbindungs- bzw. Übertragungswegen. Hier bildet(e) die planvoll installierte, an den geografischen Gegebenheiten ausgerichtete strukturierte Verkabelung der FAU eine gute Grundlage. Dies gilt im erweiterten Sinne auch für die gesamte verteilte Universität, wenn man die Fernstrecken (bspw. per RiFu) der primären Verkabelungsebene zuordnet (vgl. Teil 1, Kapitel 5.2.2).

Mit der (migrativen) Ablösung der ATM-Technik ab den 2000er Jahren dienten zur Gestaltung des aktiven Netzes im Wesentlichen „nur noch“ Router und LAN-Switche. Über die Verkabelung konnten sie, je nach verfügbaren Medien (Glas, Kupfer, RiFu) und Geräteeigenschaften (Schnittstellen, Leistungsparameter), miteinander verbunden werden. Während es dabei für Switche bestimmte Restriktionen gab (bspw. Schleifenverbot, vgl. Kapitel 6.3.2.3), konnten (IP-)Router unter den gegebenen Bedingungen nahezu beliebig miteinander verknüpft werden. Um aber einen geregelten, beherrschbaren Betrieb zu gewährleisten, waren gerade diesbezüglich gewisse Einschränkungen bzw. Strukturvorgaben erforderlich. Der Aufbau musste also dem durchgehenden Konzept einer umfassenden Netzwerkarchitektur folgen.

Wie teilweise schon erwähnt, gehören zu den generellen Zielen der FAU-Vernetzung:

- Flächendeckende Versorgung (mit Anschlüssen für Endgeräte)
- Hohe Übertragungsleistungen (nach Stand der Technik)
- Kosteneffektive Gestaltung
- Performante Basis für verschiedene Dienstleistungen (Webserver usw.)
- Stabiler Betrieb, hohe Verfügbarkeit
- Überschaubares Netzmanagement
- Schutz vor unerwünschten Zugriffen
- Erweiterbarkeit (Skalierbarkeit)
- Externe Anbindung (WiN, Internet), schnell und gesichert

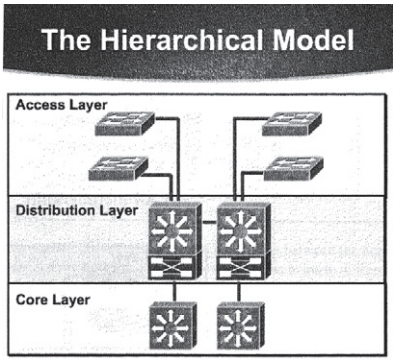
- Schritthalten mit technischer Entwicklung (Ausnutzung neuer Möglichkeiten)
- Vorausschauende Untersuchungen in spezifischen Testumgebungen
- (Inter-)nationale Kontakte und Beteiligung an Forschungsprojekten

Zum Erreichen der Ziele, die im Prinzip in allen Entwicklungsstufen der FAU-Vernetzung je nach Gegebenheiten verfolgt wurden, gehörte immer auch das Überdenken der jeweils aktuellen Lösungen und Strukturen sowie entsprechend modifizierte oder neue Designentwürfe. Die (im Kern vollziehbare) Beschränkung aktiver Komponenten auf Switche und Router (mit zusätzlicher LAN-Switch-Funktionalität) bot im Zusammenhang mit der strukturierten Verkabelung neue Möglichkeiten des Entwurfs einer angepassten, neuen Netzwerkarchitektur für die FAU.

Es sei noch angemerkt, dass zur Verfolgung solcher Ziele neben struktureller Planung jeweils auch entsprechende finanzielle Mittel erforderlich waren (sind). Diese waren in der Regel weder vom RRZE noch von der Universität aus eigener Kraft aufzubringen, sondern erforderten gesonderte Finanzierungsmaßnahmen (zum Beispiel im Rahmen von Bau- oder netzbezogenen Investitionsprogrammen, vgl. Teil 1, Kapitel 5.2.3). Insofern war (ist) das RRZE zeitweilig mit Anforderungen konfrontiert, ohne darauf wegen fehlender Mittel trotz effektiver Planungen direkt eingehen zu können − oft zum Ärger und teilweisen Unverständnis der Nutzerschaft.

6.4.2 Hierarchisches Internetworking-Modell

Um Netzwerke für größere Institutionen (Unternehmen, Firmen, Hochschulen usw.) aufbauen und dabei die oben genannten Ziele anstreben zu können, ist ein geordnetes Vorgehen mit struktureller Planung erforderlich. Hierzu definiert das „Hierarchische Internetworking-Modell“ (Drei-Schichten-Modell) eine grundsätzliche Gliederung und liefert begriffliche Grundlagen zur Einordnung von Netzelementen. Das Modell wurde stark vom Hersteller Cisco propagiert; nicht zuletzt, um seine Produkte in einen sinnvollen Kontext stellen und anbieten zu können.



Hierarchisches Modell, Cisco 2000

Das Modell gliedert sich in drei Ebenen (vgl. Abbildung „Hierarchisches Modell“, nach Cisco [*CiMsn*]):

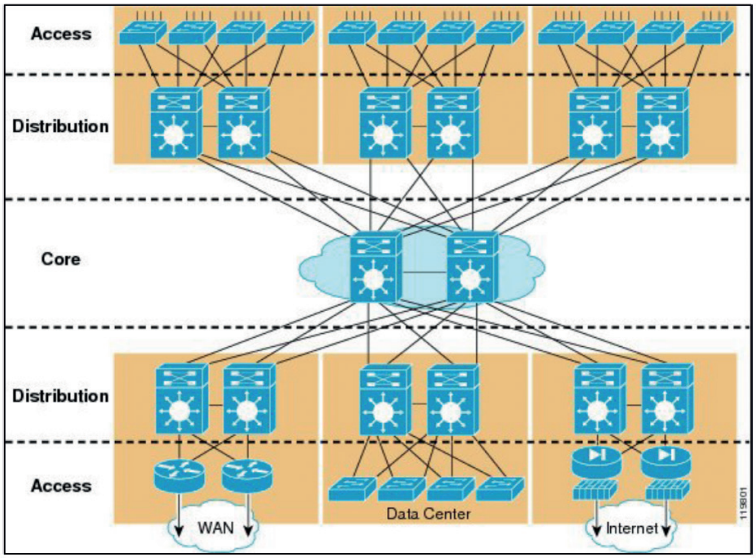
- Access Layer (Zugriffsschicht)
  Der Access Layer ist für die Zugriffe von Endgeräten (PCs, Workstations, Server

usw.) auf das Netz zuständig. Im Rahmen von Ethernet-/IP-basierten Netzen wird er Access-Layer in der Regel aus LAN-Switch-Strukturen gebildet (vgl. Kapitel 6.3.2.3), die sich über Gebäude oder Gebäudegruppen baumförmig erstrecken und Anschlüsse für (VLAN-)Zugänge bedarfsgerecht bereitstellen. Auch die drahtlosen WLANs bzw. deren Zugangspunkte (APs, vgl. Kapitel 6.3) können dem Access Layer zugeordnet werden. Die VLANs sind auf ihre jeweiligen Bereiche beschränkt, werden also nicht über deren Grenzen hinaus verteilt.

- Distribution Layer (Verteilungsschicht)
  Der Distribution Layer fasst als Zwischenschicht Bereiche des Access Layers zusammen und sorgt darin für das (IP-)Routing, also die Kommunikation zwischen den verschiedenen (V)LANs bzw. Subnetzen des betreffenden Bereichs. Über Verbindungen zur höheren Ebene (Core) wird bereichsübergreifender Datenaustausch möglich. Neben der reinen Datenvermittlung üben die Komponenten noch verschiedene, mit dem Routing verbundene Kontrollfunktionen aus. Zur Realisierung des Distribution Layers kommen in der Regel Switche/Router (bzw. Router mit zusätzlicher Switchfunktionalität) zum Einsatz, und zwar (bei nicht redundanter Auslegung) pro Bereich ein Gerät. Dessen LAN-Schnittstellen sind, gemäß dem zugehörigen Access-Bereich, jeweils an einzelne oder weiterverteilende LAN-Switche (über Trunks zum Transfer mehrerer VLANs) angebunden. Im Sinne des hierarchischen Modells werden die Router unterschiedlicher Bereiche nicht direkt untereinander, sondern ausschließlich über den Core miteinander verknüpft!
- Core Layer (Kernschicht)
  Der Core Layer verknüpft als höchste Hierarchiestufe die Bereiche des Distribution Layers miteinander. Im einfachsten Fall besteht es aus einer Komponente, die mit den Bereichs-Routern des Distribution Layers direkt (Kabel, Übertragungsstrecke o. ä) verbunden ist. Wegen seiner zentralen Bedeutung werden an den Core meist besondere Anforderungen bezüglich Zuverlässigkeit und Leistung gestellt, sodass die Komponenten meist doppelt (redundant) ausgelegt und ihre Verbindungen, gemäß technischem Stand, mit möglichst hohen Übertragungsgeschwindigkeiten betrieben werden. Die Komponenten selbst können als LAN-Switche oder Router realisiert werden. Für die LAN-Switche sprach zunächst deren höhere Vermittlungsgeschwindigkeit. Seit aber Router IP-Pakete mit entsprechender Technologie ebenso schnell „switchen“ können, gilt dieses Argument nicht mehr, sodass sie insbesondere in der Konstellation mehrerer Core-Standorte vorrangig Verwendung finden (vgl. FAU-Netze).

6.4.3 Campusnetzwerk (Strukturentwurf Cisco)

Das hierarchische Modell lässt sich besser nachvollziehen, wenn man es in Anwendung bzw. konkreterer Ausarbeitung betrachtet. Der Hersteller Cisco nahm es als Grundlage für den Entwurf einer allgemeinen Campusnetzstruktur [*CiCam*]. „Campus“ bezieht sich dabei auf ein geschlossenes Gelände einer Institution (Firma, Universität o. ä.), dessen aktives Netz effektiv und anforderungsgemäß zu gestalten ist. Im skizzierten Entwurf (Abbildung „Campusmodell, Cisco 2008“) ist eine (ausreichende) strukturierte Verkabelung vorausgesetzt. Der Core Layer besteht aus einer zentralen Verteilung (Bildmitte), der Distribution Layer aus drei gebäudeorientierten Bereichen (obere Reihe) und drei nach funktionalen Gesichtspunkten zusammengefassten Bereichen (untere Reihe), während sich der Access Layer aus LAN-Switchen (oben) und (externen) Übergangskomponenten (unten) zusammensetzt. Die vermittelnden Komponenten aus Core und Access sind in Redundanz doppelt ausgelegt, ebenso wie alle physischen Verbindungswege (durchgezogene Linien in der Abbildung) zwischen den Geräten, um eine hohe Verfügbarkeit (Ausfallsicherheit) des Netzes zu erzielen. Diese volle Redundanz ist allerdings sehr (kosten-)aufwendig. Neben der Verdoppelung der Komponenten erfordert sie auch eine doppelte Anzahl entsprechender Schnittstellen und Verbindungen (Kabelstrecken). In konkreter Umsetzung ist daher der erzielbare, betriebliche Nutzen unter anderem gegen damit verbundene Kosten, erhöhte Komplexität oder sonstige Randbedingungen (bspw. vorhandene Verkabelung) punktuell abzuwägen.



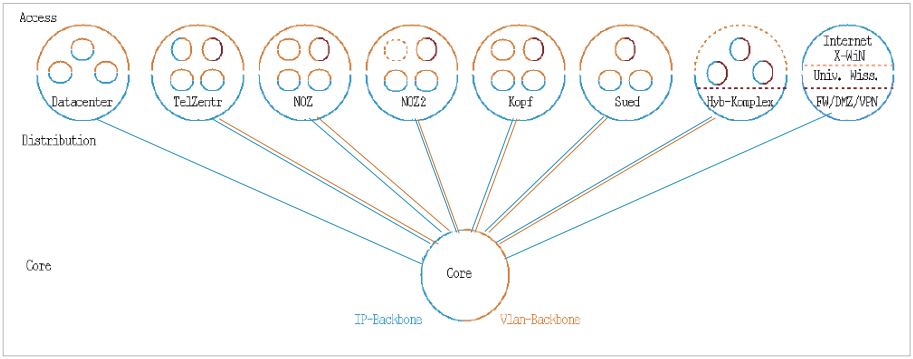
Campusmodell, Cisco 2008

6.4.4 Hierarchische Netzstruktur des Universitätsklinikums

Das Kommunikationsnetz des medizinischen Bereichs bzw. des Klinikums der Universität bildete in allen seinen „historischen“ Ausprägungen (vgl. [HillK]) zunächst vorrangig aus Gründen des Datenschutzes und spezifischer Anforderungen eine vom Netz des wissenschaftlichen Bereichs getrennte, eigene Struktur. Die Gebäude des Klinikums sind zwar auf verschiedene, nicht zusammenhängende Gelände in Erlangen verteilt, boten aber nach der in Maßnahmen der Universität erstellten, auch grundstücksübergreifenden strukturierten Verkabelung campusähnliche Voraussetzungen zur Netzgestaltung in Anlehnung an die beschriebenen Architekturmodelle.

Einige Ideen des hierarchischen Netzaufbaus gingen schon früher, ohne direkten Bezug auf die abstrakten Modelle, in die Gestaltung jeweiliger Strukturen ein. Gezielt angewendet wurden sie dann vor allem im Zuge der Migration zu reiner „Ethernet-/IP-Technik“ (bzw. Ablösung von ATM), insbesondere auch in Bezug auf Beschreibungen und verwendete Terminologie.

Ähnlich dem Campusmodell von Cisco wurde das Netz in geografische und funktionale Distributionsbereiche gegliedert. Während sich die geografische Aufteilung vornehmlich an der strukturierten Verkabelung orientierte, wurden die funktionalen Module jeweils nach spezifischen Aufgabenspektren gebildet. Die Abbildung „Hierarchische Grundstruktur des Kliniknetzes“ stellt diese Aufteilung grafisch dar.

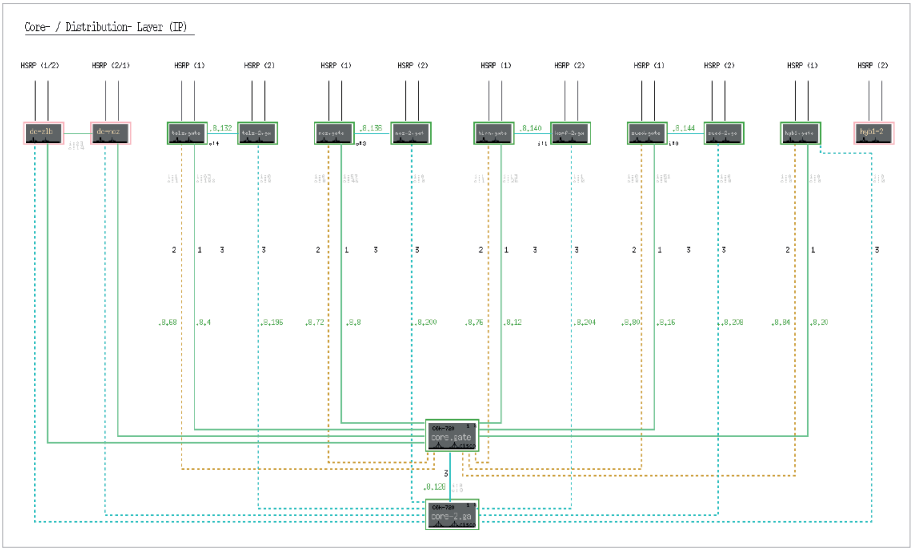


Hierarchische Grundstruktur des Kliniknetzes

Danach fassten die Bereiche zur Versorgung von Nutzerendgeräten verschiedene Gebäude oder Gebäudegruppen zusammen, und zwar mit den Zentren „TelZentr.“ (Telefonzentrale Innenstadt), „NOZ“ (Nichtoperatives Zentrum, 1. Bauabschnitt), „NOZ2“ (Nichtoperatives Zentrum, 2. Bauabschnitt), „Kopf“ (Kopfklinikum), „Sued“

(Erlangen Südgelände). Die Bereiche nach funktionalen Kriterien waren das „Datacenter“ (Zentrale Server des Klinikums), „Univ. Wiss.“ (Kontrollierter Übergang zum Wissenschaftsnetz der Universität mit Zugang zum Internet) und „Hyb-Komplex“ (Hybrid-Komplex, abgetrennter Bereich für „unsichere Systeme“ innerhalb des Klinikums). In Abweichung vom strikten Strukturmodell war es erforderlich, bestimmte (V)LANs auch über Bereichsgrenzen hinaus verfügbar zu machen, also „global“ zu verteilen. Solche Sonderfälle bildeten Systeme, die aufgrund ihrer (veralteten) Software nur innerhalb ihrer LANs bzw. Subnetze miteinander kommunizieren konnten, aber in der gesamten Klinik verteilt und unverzichtbar waren. Prägnante Beispiele dafür waren Patientenmonitore oder Labordatensysteme. Die übergreifende Verteilung erfolgte über dedizierte LAN-Verbindungen (Trunks) zwischen Core und Bereichs-Routern (mit ihren LAN-Switch-Eigenschaften) durch ein so bezeichnetes „VLAN-Backbone (in der Abbildung „orange“ gekennzeichnet). Diese Struktur bildete auch die Basis des Hybrid-Komplexes, der sowohl unsichere, gefährdende als auch besonders schützenswerte Systeme in dedizierten VLANs weitgehend vom „Normalbetrieb“ isolierte und am Übergang je nach Subnetz besondere Kontrollen durchführte.

In der konkreten Umsetzung der Grundstruktur wurden die Core- und Distributionskomponenten doppelt ausgelegt, aus Sicherheitsgründen aber nicht immer im selben Gebäude/Raum aufgestellt. So waren bspw. die Geräte des Cores auf die



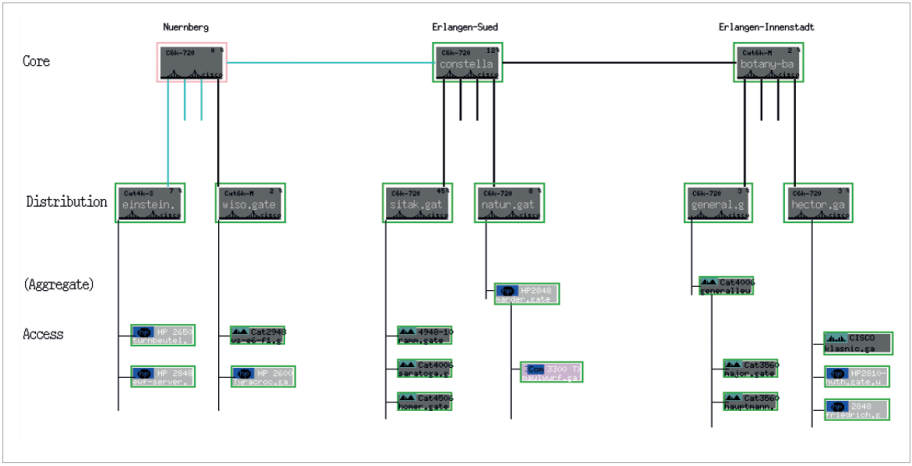
Redundante Router-Struktur des Kliniknetzes

Telefonzentrale (Primärbetrieb) und das NOZ (Sekundärbetrieb) verteilt. Dies sollte für zusätzliche Betriebssicherheit sorgen, etwa im Falle eines Stromausfalls oder Schadens an einem der Router-Standorte oder betreffenden Kabeltrassen (alles schon vorgekommen). Nicht zuletzt wegen dieser Konstellation konnten die Schaltungen der Verbindungswege nicht dem aufwendigen, „vollen“ Vermaschungskonzept von Cisco (vgl. Kapitel 6.4.2) folgen, sondern beschränkten sich auf Strecken zwischen den primären Komponenten von Core und Distribution, den entsprechenden sekundären Komponenten sowie jeweils pro Standort zwischen primärer und sekundärer Komponente. Die Abbildung „Redundante Router-Struktur des Kliniknetzes“ auf S. 78 stellt dies dar. Die primäre, also im Normalbetrieb gültige Struktur, ist darin mit durchgezogenen, grünen Linien gezeichnet. Die gestrichelten, blauen Linien stehen für Verbindungen, die je nach Ausfallsituation betrieblich aktiv werden. In dieser Konstruktion konnte, wie im aufwendigeren Cisco-Modell, jeder Ausfall einer einzelnen Komponente oder Strecke durch eine Ersatzlösung aufgefangen werden. Priorisierung und automatische Umschaltung erfolgten zwischen den Routern über das Protokoll OSPF und zu den Endsystemen über HSRP (vgl. Kapitel 6.2.3.2). Diese Vernetzung ist auch als Teil in der Abbildung „Kliniknetz, Gesamtstruktur 2010“ (vgl. Kapitel 6.5.1) dargestellt, in einer um 90 Grad gedrehten Anordnung.

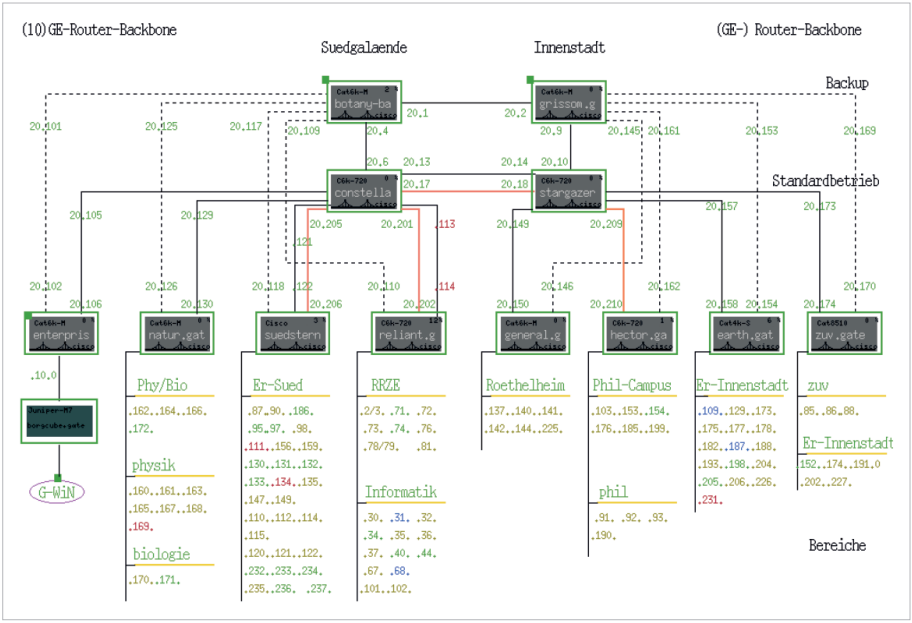
6.4.5 Hierarchische Netzstruktur des Wissenschaftsnetzes der FAU

Wie schon der Name andeutet, ist die Universität Erlangen-Nürnberg auf mehrere, voneinander getrennte Standorte verteilt. Verbindungen zwischen ihnen sind nach sehr unterschiedlichen Bedingungen mit Lokalnetz- (LAN) oder Weitverkehrs- (WAN) Charakter herzustellen. Das Campusmodell, das sehr viele Gestaltungsfreiheiten voraussetzt, ist also als Muster zum Entwurf einer umfassenden Netzarchitektur für die FAU nicht geeignet. Dennoch konnte der grundliegende Ansatz des hierarchischen Internetworkingmodells dem RRZE als Vorbild und Leitlinie auch zur Strukturierung des Universitätsnetzes dienen.

In Erweiterung des Grundmodells wurde die Universität in drei, jeweils aus Core, Distribution und Access bestehende Teile gegliedert, die durch Verknüpfung der Core-Elemente zu einem Gesamtgebilde verbunden wurden. Die Abbildung „Hierarchisches Grundmodell des wissenschaftlichen FAU-Netzes“ auf S. 80 stellt den prinzipiellen Ansatz in stark verkürzter Form dar. Die drei Core-Elemente bilden jeweils Wurzeln der Bereiche in „Nürnberg“, „Erlangen-Sued“ und „Erlangen-Innenstadt“. Gemäß verfügbarer Übertragungstechnik deuten die schwarzen Linien die Nutzung von Glasfaserkabel, die grünen Linien den Einsatz von Richtfunkstrecken an.



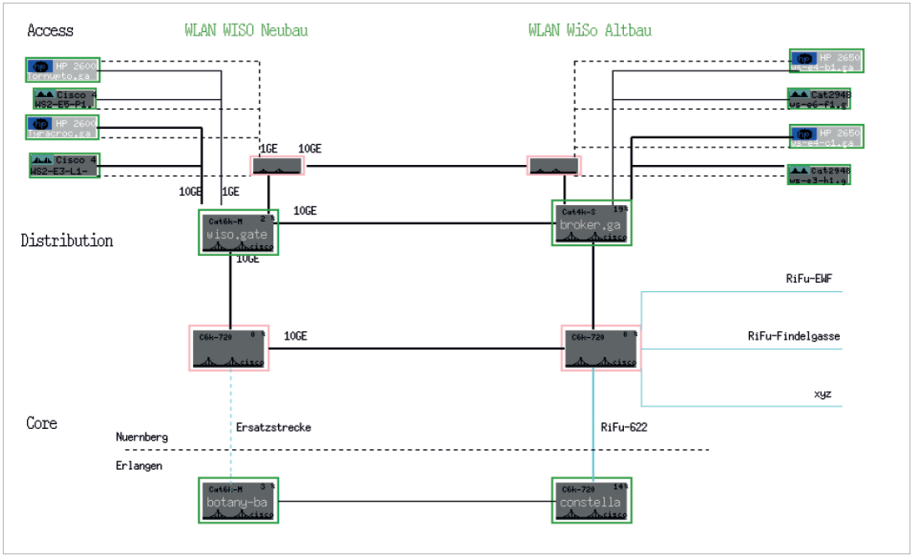
Hierarchisches Grundmodell des wissenschaftlichen FAU-Netzes



GE-Router-Backbone, Erlanger Core-Bereiche

Eine genauere Umsetzung des Modells für die beiden Erlanger Core-Bereiche zeigt die Darstellung aus einer Präsentation von 2006 (Abbildung „GE-Router-Backbone, Erlanger Core-Bereiche“) des „GE-Router-Backbones“ (so genannt wegen des Einsatzes von Gigabit Ethernet und im Vergleich zum abgelösten ATM-basierten Netz). Danach sind die Core-Router im Südgelände ebenso doppelt ausgelegt (primär: „constellation“, sekundär: „botany-bay“) wie die in der Innenstadt (primär: „stargazer“, sekundär: „grissom“). Die Distributionsrouter (untere Reihe) sind pro Bereich einfach vorhanden, aber jeweils mit beiden Core-Routern verbunden, und zwar primär im Standardbetrieb (durchgezeichnete Linien) und sekundär im Backup, d. h. aktiviert in bestimmten Ausfallsituationen (gestrichelte Linien). Die roten Linien stehen für die zu dieser Zeit bereits realisierten 10-GE-Strecken. Unterhalb der Distributionsebene sind die Access-Bereiche bzw. deren Subnetze dargestellt, die von den zugehörigen Zentralen geroutet und als (V)LANs verteilt werden.

Eine Verdoppelung der Distributionsrouter war aus Kostengründen zu der Zeit nicht realisierbar. Später konnten Redundanzen im Rahmen zentraler Serveranbindungen (Datacenter) oder dem Einsatz von Komponenten mit zwei Zentraleinheiten punktuell hergestellt werden.



Netzplanung Nürnberg, 2010

Die Einbeziehung und (Um-)Gestaltung des dritten Core-Bereichs in Nürnberg stellt die Skizze zur „Netzplanung Nürnberg, 2010“ auf S. 81 dar. Diese Planung hatte unter anderem die Ablösung von ATM und die Integration des WiSo-Neubaus zum Ziel. Sie enthielt am Standort Lange Gasse zwei (redundante) Core-Elemente (rosa umrandet), zwei lokal verbundene Distributionskomponenten (wiso.gate, broker-gate) und den Verweis auf weitere, über Richtfunk angebundene Distributionsbereiche in der EWF (Erziehungswissenschaftliche Fakultät, Regensburger Straße), Findelgasse (Alte WiSo) bzw. noch hinzukommende Standorte (xyz). Gemäß des hierarchischen Grundmodells des wissenschaftlichen FAU-Netzes (vgl. S. 80) waren die Core-Router mit denen von „Erlangen-Sued“ primär (constellation) und sekundär (botany-bay) verbunden. An Alternativen zur dargestellten Richtfunkübertragung bzw. Lösungen mit Geschwindigkeiten oberhalb von 622 Mbp/s war zu dieser Zeit noch nicht zu denken. Die Distributionsrouter wurden doppelt ausgelegt und im Neubau (wiso.gate) bzw. Altbau (broker.gate) platziert. Entsprechend waren die Access-Switche doppelt angebunden, und zwar primär, direkt mit dem Router im gleichen Gebäude und sekundär, indirekt über zwei Transferswitche mit dem jeweils anderen Router (nach dem Modell aus Kapitel 6.3.2.4 auf S. 37, „Redundante Switch-Struktur im Rechenzentrum, 2009“). Die Planung diente als Richtlinie zur konkreten Umsetzung und wurde weitgehend nachvollzogen.

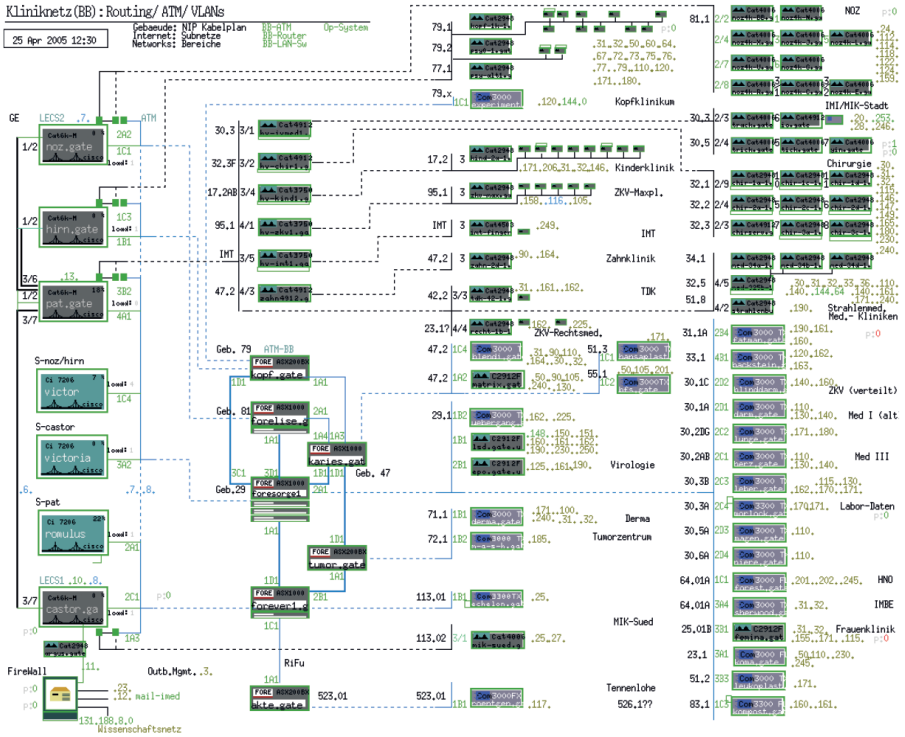
6.5 Netzausbau und Gesamtstrukturen

Wie bereits zum Überblick der Kommunikationsinfrastruktur erwähnt (vgl. Kapitel 6.1.4), lassen sich in der hier betrachteten Phase (Kapitel 6) die vom RRZE betriebenen Netze der FAU inhaltlich in drei, weitgehend voneinander getrennte Bereiche gliedern. Ihre Gestaltung erfolgte gemäß jeweils adäquat entworfener Architekturen (vgl. Kapitel 6.4) und war in der Umsetzung durch die schrittweise Ablösung der ATM-/LANE-Technik durch einen ausgeweiteten Einsatz des Ethernet-Switching geprägt.

6.5.1 Netz im Universitätsklinikum

Das Intranet im medizinischen Bereich wurde vom RRZE von Beginn an aufgebaut und bis zur Übergabe an das Medizinische Zentrum für Informations- und Kommunikationstechnik (MIK) im Jahr 2011 betrieben. Dies galt für das passive Netz (strukturierte Verkabelung, NIP-Planung) ebenso wie für das aktive Netz in den verschiedenen technischen Entwicklungs- und Ausbauphasen ([Hillk]). Die Abgabe der Verantwortung an das MIK war letztlich eine konsequente Folge aus der Etablierung des Universitätsklinikums Erlangen (UK) als eigenständige (von der FAU unabhängige) Einrichtung des öffentlichen Rechts im Jahr 2006 und dem zunehmenden Streben des MIK nach Eigenverantwortung auch im Netzbereich.

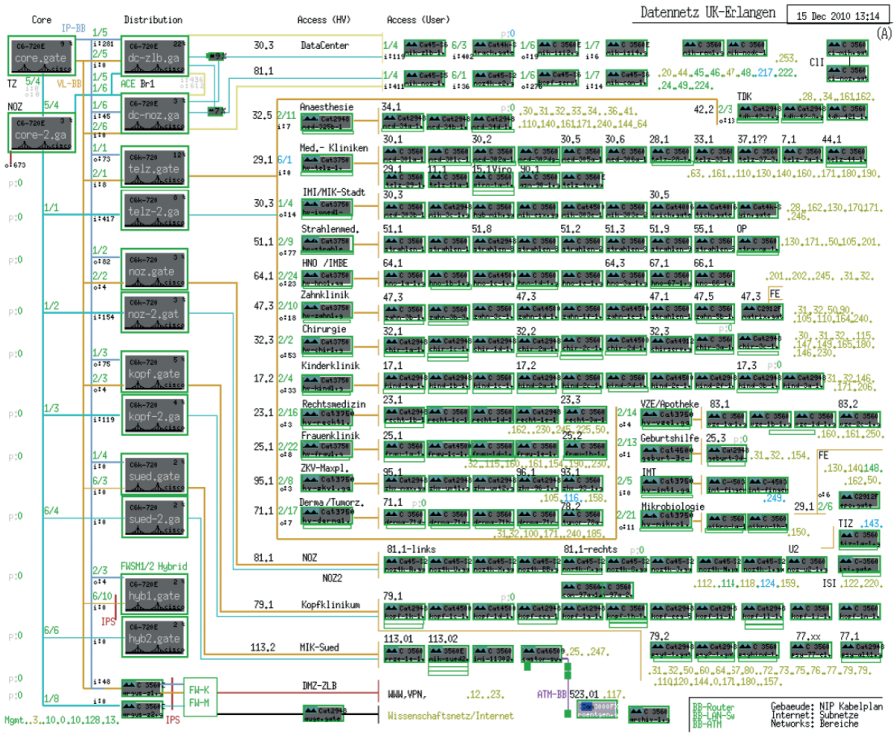
Die Darstellung „Kliniknetz, Gesamtstruktur 2005“ auf S. 84 dokumentiert einen Ausbaustand mitten in der Migrationsphase. Die linke Spalte der Abbildung zeigt die Router, die teils über Ethernet (schwarze Linien) und teils über ATM (blaue Linien) miteinander verbunden sind. Die untere Bildhälfte enthält in der zweiten Spalte das ATM-Netz und daneben die LAN-Switche, die VLANs bzw. Subnetze über LANE in verschiedene Nutzerbereiche verteilen. (Diese Teilstruktur entspricht der Gesamtdarstellung des Kommunikationsnetzes im medizinischen Bereich von 2002 in Teil 1, Kapitel 5.4 und ist dort näher erläutert.) In der oberen Bildhälfte sind die migrierten Bereiche mit der LAN-Verteilung über Switch-Strukturen dargestellt. Die Verteilung erfolgt einstufig von einer zentralen Komponente (z. B. noz.gate (links oben)) zu daran angeschlossenen Switchen (z. B. in Gebäude 81.1 (rechts oben)) oder über eine Zwischenstufe (z. B. von pat.gate (dritter Router von oben) über hv-ivmed1 (zweite Spalte, oberste Komponente)) zu einem Endgeräteswitch des MIK in Gebäude 30.3 (rechts, Innenstadtbereich unter NOZ). Das (aktive) Netz bestand in diesem Ausbau aus sieben Routern, zwölf ATM-Switchen, 28 LANE-Switchen, 100 GE-LAN-Switchen und versorgte etwa 7.100 Endgeräte (gemäß im DNS registrierter IP-Adressen).



Kliniknetz, Gesamtstruktur 2005

Der Migrationsprozess wurde in der Folgezeit weitergeführt und, wie die Abbildung „Kliniknetz, Gesamtstruktur 2010“ auf S. 85 zeigt, auch abgeschlossen. Im Vergleich zum Status von 2005 enthält sie keine ATM-Komponenten mehr. Es ist zu erkennen, wie dabei das in Kapitel 6.4.3 beschriebene, hierarchische Strukturmodell konkret umgesetzt wurde. (Die zeichnerische Anordnung der Komponenten ist dabei im Vergleich zur „Redundanten Router-Struktur“ in Kapitel 6.4.3 auf S. 77 um 90 Grad gedreht, entspricht ihr aber inhaltlich).

Die Spalte am linken Rand enthält die beiden (redundanten) Core-Elemente (core.gate, core-2.gate), die Spalte daneben die doppelten Komponenten der sieben Distributionsbereiche. Im rechten Bildteil sind die im Klinikum verteilten LAN-Switche dargestellt, die direkt oder über (redundante) Zwischenverteiler (dritte Spalte von links) mit der Distributionsebene (redundant) verbunden sind. Die Verbindungsstruktur zwischen Distributions- und Access-Ebene entspricht der des Campusmodells von Cisco und



Kliniknetz, Gesamtstruktur 2010

ist zur besseren Übersicht in der Zeichnung verkürzt wiedergegeben. Am oberen Bildrand ist der Bereich des „DataCenters“ mit den Routern im Zentrallabor (dc-zlb) und dem NOZ (dc-noz), den ebenso verteilten LAN-Switchen zur Serveranbindung und die redundante Verbindungsstruktur der Zwei-Standorte-Konstellation dargestellt. Der untere Rand zeigt die Komponenten der Außenanbindung, also des Übergangs zum Wissenschaftsnetz der Universität. Dazu gehören eine (redundante) Firewall (FW-1, FW-2) zur Zugangskontrolle und ein Intrusion-Prevention-System (IPS) zur speziellen Abwehr gegen das Eindringen von Schadsoftware oder sonstige Störattacken (vgl. Kapitel 7.3.3). Die Verbindungen in und zwischen Core- und Distributionsbereichen wurden mit 10 GE (10Gbit/s) betrieben.

Das (aktive) Netz bestand im dargestellten Ausbau (Dezember 2010) aus 14 Routern, 352 LAN-Switchen und versorgte rund 14.000 Endgeräte (gemäß im DNS registrierter IP-Adressen). Etwa doppelt so viel also, im Vergleich zu 2005.

Wegen seiner kritischen Anwendungsfelder und einer stetig wachsenden Bedeutung der Kommunikationstechnik im medizinischen Bereich, wurden an das Netz der Klinik und dessen Betrieb stets besondere Anforderungen bezüglich Betriebssicherheit, Datensicherheit oder Leistungsfähigkeit gestellt. Dies drückte sich auch in allgemeinen Überlegungen zum „Risikomanagement für medizinische IT-Netzwerke, die Medizinprodukte beinhalten“ aus und schlug sich in den Normen „IEC 80001-1:2010“ bzw. „DIN EN 80001-1:2011“ nieder. Das RRZE entsprach den darin formulierten Vorgaben unter anderem mit der nach allgemein anerkannten Richtlinien entworfenen Architektur, den konkreten Umsetzungen auf technischem Stand sowie den installierten Kontrollmechanismen. An den Normen orientierte sich aber auch die transparente Betriebsführung mit ständigem Überwachen des Netzverhaltens, dem Messen verschiedener Betriebsparameter (Verfügbarkeiten, Antwortzeiten, Übertragungsleistungen usw.) oder laufenden Statusinformationen, regelmäßigen Berichten und Präsentationen für interessierte Systembetreuer und Anwender.

In diesem Sinne konnten Netz und Betrieb vom RRZE dem UK bzw. dem MIK zur weiteren Ausgestaltung und Fortentwicklung im Juli 2011 übergeben werden.

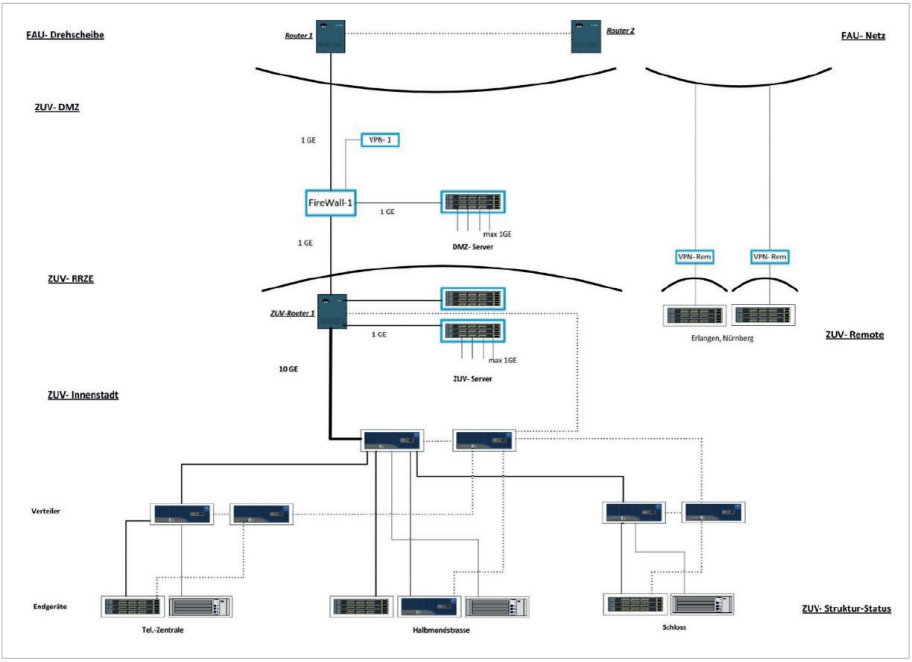
6.5.2 Vernetzung der Zentralen Universitätsverwaltung (ZUV)

Als Teil der Gesamtmaßnahmen der Universität wurden auch die Gebäude der Zentralen Universitätsverwaltung (Schloss und Umgebung) in die Versorgung mit passiver und aktiver Netzstruktur sowie deren Betreuung durch das RRZE einbezogen. Spätestens mit der Verlagerung der Verwaltungs-EDV vom Siemens-Großrechner auf verteilte Client-/Server-Systeme entstand die Notwendigkeit, für sicherheitskritische Anwendungen, die bspw. die Bearbeitung von Personal- oder Studierendendaten beinhalteten, eine separate, vom allgemeinen Universitätsnetz abgeschottete Netzstruktur zu schaffen und für einen streng kontrollierten Übergang zu sorgen. Dazu hat das RRZE etwa ab 2003 ein Sicherheitskonzept entworfen und umgesetzt. Mit der Eingliederung des Sachgebiets Datenverarbeitung (SG SGDV) als eine Abteilung des Rechenzentrums (2006), fiel die gesamte Verwaltungs-IT einschließlich Systembetreuung und Vernetzung in die Verantwortung des RRZE (vgl. auch Kapitel 6.1.1). Dies trug zur Schaffung klarer Zuständigkeiten und effektiveren Lösungsmöglichkeiten bei.

Durch die erforderliche Abgrenzung zum wissenschaftlichen Universitätsnetz ergab sich auch die Problematik der Einbeziehung verteilter Standorte der ZUV in das Verwaltungsnetz. Innerhalb Erlangens konnte die Vernetzung weitgehend auf Basis der strukturierten Verkabelung oder aber mit Hilfe spezieller Konstruktionen (bspw. Anbindung Hugenottenplatz) hergestellt werden. Auf die Verbindung der weiter ent-

fernten Standorte in Nürnberg (WiSo, EWF) waren diese Ansätze nicht übertragbar. Sie hätten den Einsatz eigener Übertragungsstrecken erfordert, der insbesondere aus Kostengründen nicht realisierbar war.

Da das allgemeine Universitätsnetz an allen in Frage kommenden Punkten verfügbar war, bot es sich an, dieses als Transfernetz zu nutzen. Dazu mussten aber aus Sicherheitsgründen bestimmte Vorkehrungen getroffen werden. Die Anbindung der entfernten Standorte erfolgte vor Ort mit Hilfe von Übergangskomponenten, die mit kontrollierender Firewall- und VPN-Funktionalität ausgestattet waren. Zum Austausch mit den anderen ZUV-Bereichen wurde jeweils ein IP-Tunnel (vgl. Kapitel 6.2.3.3) zu einem zentralen VPN-Server etabliert, sodass die entsprechenden Daten geschützt und verschlüsselt durch das Universitätsnetz übertragen werden konnten. Der zentrale VPN-Server diente übrigens auch als Einwahlpunkt für Mitarbeiter der ZUV, um die Arbeit mit Verwaltungsanwendungen auch an Heimarbeitsplätzen zu ermöglichen (Telearbeit).



ZUV-Netzstruktur, 2012

Die Abbildung „ZUV-Netzstruktur, 2012“ auf S. 87 stellt den Aufbau des Netzes schematisch dar. Die Mitte des Bildes zeigt einen zentralen, im Rechenzentrum (ZUV-RRZE) aufgestellten Switch/Router (ZUV-Router-1), der „nach oben“ über eine Firewall (FireWall-1) mit dem wissenschaftlichen Universitätsnetz bzw. einem Router (Router-1) der FAU-Drehscheibe verbunden ist. Er verteilt den Datenverkehr „nach rechts“ zu zentralen Servern der ZUV (ZUV-Server) und „nach unten“ in die LAN-Switch-Struktur für die Zugänge der (ZUV-)Mitarbeiter in der Erlanger Innenstadt. In der rechten Bildmitte (ZUV-Remote) sind zwei entfernte Standorte mit ihren separierten Netzbereichen und den Übergangskomponenten (VPN-Remote) dargestellt, die über das „FAU-Netz“ und die „FAU-Drehscheibe“ per Tunnel (nicht eingezeichnet) mit dem zentralen „VPN-1“ Verbindung zur Zentrale halten. Die Beschriftungen an den Verbindungslinien stehen für die zugehörigen Übertragungsgeschwindigkeiten „1 GE“ (1 Gbit/s) bzw. „10 GE“ (10 Gbit/s).

Das ZUV-Netz bestand 2012 aus 30 Netzkomponenten und versorgte rund 9.500 Endgeräte. Die eingesetzten Komponenten gelangten durch ständig steigende Anforderungen (Studierendenzahlen, neue Dienste usw.) teilweise an die Grenzen ihrer Kapazitäten. Insbesondere wurden auf der Firewall (Typ Cisco ASA 5500) bereits 180.000 von maximal möglichen 250.000 gleichzeitigen Verbindungen erreicht. Das RRZE bemühte sich, dies über ein angepasstes, zukunftsweisendes Konzept und einen entsprechenden Großgeräteantrag nach dem Hochschulbauförderungsgesetz (HBFG) zu lösen.

6.5.3 Netzausbau im Wissenschaftsbereich der FAU

Der Ausbau des Kommunikationsnetzes war in der hier betrachteten Phase vor allem geprägt durch die Ablösung von ATM, die Erhöhung der Leistungsfähigkeit über Ersatz „veralteter“ Komponenten, die Einbeziehung neuer Standorte sowie ein generelles Wachstum der Anzahl und Verteildichte versorgter Endgeräte.

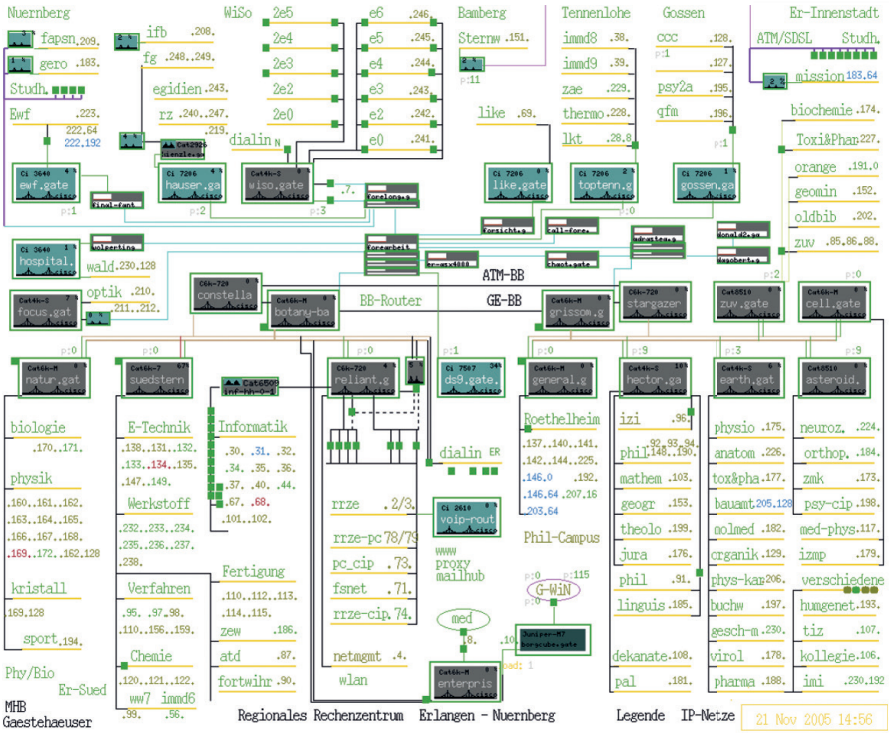
6.5.3.1 Ablösung der ATM- durch Ethernet-Technik

Dieser Migrationsprozess bezog sich sowohl auf die Verteilung der LANs / Subnetze in die Anschlussbereiche der Nutzer (Distributionsebene), als auch auf die Verbindungen der Router untereinander (Core, Distributionsebene) im Router-Backbone.

Die VLAN-Verteilung basierte in einigen Bereichen, bspw. im Erlanger Südgelände, Röthelheimpark oder in Nürnberg, von vornherein auf Strukturen von LAN-Switchen, die über Ethernet Punkt-zu-Punkt verbunden waren (vgl. Kapitel 6.3.2.3). Dies hatte zum Teil „historische“ Gründe, lag aber auch daran, dass es dort aufgrund verfügbarer Verkabelung und der Art der Verteilung von Nutzergruppen nicht erforderlich

war, mehrere VLANs über eine Switch-Switch-Verbindung (Link) „parallel“ zu transportieren. Dort entfiel also die Notwendigkeit der Mehrfachnutzung von Links und die Notwendigkeit des Einsatzes von ATM/LANE. Dies galt jedoch nicht für die auf viele (alte) Gebäude verteilten Standorte bzw. Nutzergruppen in der Erlanger Innenstadt. Zum Aufbau ihrer Vernetzung stellte der Einsatz der ATM-/LANE-Technik optimale Lösungen bereit. Nachdem die Verteilung virtueller LANs auch zwischen LAN-Switchen (genormt) möglich war (vgl. 802.1q, Kapitel 6.3.2.3) und ATM unter anderem aus Gründen der Vereinfachung generell abgelöst werden sollte, wurde die aktive Netzstruktur auch dieser Bereiche auf Ethernet-Technik umgestellt.

Wie der Abbildung „FAU-Kommunikationsnetz, Gesamtsicht 2005“ zu entnehmen ist, war die Migration der VLAN-Verteilung im Jahr 2005 weitgehend abgeschlossen. Die betroffenen Access-Bereiche sind dort in der rechten, unteren Ecke dargestellt. Die



FAU-Kommunikationsnetz, Gesamtsicht 2005 (S. 89)

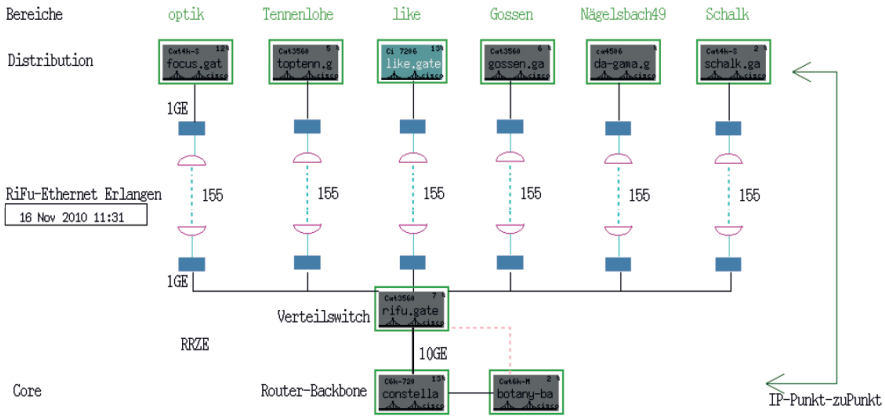
Distributionsrouter „hector“, „earth“, „asteroid“ und „cell“ bilden jeweils die Wurzeln zur Verteilung virtueller LANs bzw. IP-Subnetze zu den Nutzergruppen und sorgen für das Routing zwischen ihnen und dem übrigen Netz. So verteilt bspw. Switch/Router „earth“ das VLAN/Subnetz „.175.“ an die Nutzergruppe „physio“ und ist mit den Core-Routern „grissom“ (primär) und „stargazer“ (sekundär) verbunden (summarisch dargestellt durch hellbraune Linien). Der rechte, obere Bildrand enthält die Ausnahmen, wie bspw. die Nutzergruppe „biochemie“ mit dem VLAN/Subnetz „.174.“, die zur Erstellung der Übersicht noch nicht migriert waren.

Bezüglich der Router-Verknüpfungen zeigt die Darstellung von 2005 noch das als Basisstruktur betriebene ATM-Netz (ATM-BB). Es bestand aus einer Reihe von ATM-Switchen wie „forearbeiter“ (Bildmitte) oder „foresorge“ (darüber), die gemäß den blau/grün gezeichneten Linien untereinander verbunden waren und den angeschlossenen Routern mit ATM-Schnittstellen die Kommunikation untereinander ermöglichten wie „botany-bay“ (Erlanger Südgelände) oder „wiso“ (Nürnberg). Die ATM-Struktur entspricht der separaten Darstellung „ATM-Netz der FAU, 2004“ (vgl. Teil 1, Kapitel 5.4.3 und 5.4.4).

Das Bild enthält aber auch die bereits innerhalb Erlangens auf Gigabit-Ethernet-Technik umgestellte Struktur (GE-BB) mit den (primären) Core-Routern im Südgelände (constellation) und der Innenstadt (stargazer) sowie den daran angeschlossenen Distributionskomponenten (natur, suedstern, reliant bzw. general, hector, earth). Dieser Aufbau entspricht weitgehend dem in Kapitel 6.4.4. etwas ausführlicher beschriebenen Muster der Abbildung „GE-Router-Backbone, Erlanger Core-Bereiche“ auf S. 79.

Wie dem Übersichtsbild von 2005 auch zu entnehmen ist, wurde das ATM-Netz zu der Zeit hauptsächlich noch zur Realisierung von Fernverbindungen bzw. dem Datentransfer über die dazu betriebenen Richtfunkstrecken genutzt. Als entsprechende Anpassungs- und Umsetzeinheiten auch zur Übertragung von „Ethernet über Richtfunk“ verfügbar wurden, konnte auch in diesem Kontext der Weitverkehrsübertragungen die Ablösung von ATM eingeleitet und abgeschlossen werden.

Die Abbildung „Erlanger Bereiche mit Anbindung per Ethernet über Richtfunk“ auf S. 91 illustriert dazu den prinzipiellen Aufbau der Übertragungsstrecken. Darin gehört zu jeder Richtfunkstrecke (gezeichnet als lila Kreissegmente mit blau/grünen, gestrichelten Verbindungslinien) ein Gerätepaar (blaue Kästchen), das gemäß der Funktionalität von Remote-Bridges (vgl. Teil 1, Kapitel 4.2.2.4) an seinen äußeren Schnittstellen Daten annimmt, zur Gegenstelle transferiert, die sie dann reproduziert und weiterleitet. So spannte ein Paar jeweils ein Ethernet-LAN auf, das von den daran angeschlossenen Routern zur Kommunikation und insbesondere zum Aufbau von IP-Punkt-zu-Punkt-Verbindungen genutzt werden konnte. Auf diese Art (an zentraler Stelle hier noch unter



Erlanger Bereiche mit Anbindung per Ethernet über Richtfunk, 2010

Zwischenschaltung eines konzentrierenden Verteilswitches) wurden die entfernten Router mit einem Core-Router verbunden und als Distributionskomponenten in die hierarchische Struktur voll integriert. Zwischen den Geschwindigkeiten der Übertragungsstrecken (155 Mbit/s) und denen der angeschlossenen Router (1 Gbit/s) bestand zwar eine gewisse Diskrepanz, die auch nicht ganz unkritisch war (potentielle Gefahr des Datenverlusts durch „Überfahren"), die sich aber durch angepasstes Verhalten der Endsysteme und Protokolle von TCP/IP im praktischen Betrieb kaum auswirkte.

Nach der gleichen Methode wurden auch die Richtfunkverbindungen innerhalb Nürnbergs sowie die zwischen Erlangen und Nürnberg umgestellt. Dabei war die Strecke zwischen dem Erlanger Rechenzentrum und der Nürnberger WiSo (Lange Gasse) bereits zuvor (2010) noch in der ATM-Struktur auf die Übertragungsgeschwindigkeit von 622 Mbit/s angehoben und die Verbindungsleistung zwischen den beiden Core-Routern entsprechend verbessert worden. Die im Abschnitt zur hierarchischen Netzstruktur (vgl. Kapitel 6.4.4) gezeigte Abbildung „Netzplanung Nürnberg, 2010" auf S. 81 stellt die Nürnberger Richtfunkverbindungen nach Erlangen und innerhalb der Stadt als blau/grüne Linien dar (rechte, untere Ecke), und zwar als Teil der rein auf Ethernet basierenden, strukturellen Netzplanung für den Alt- und Neubau der Wirtschafts- und Sozialwissenschaftlichen Fakultät.

Der Vollzug des Migrationsprozesses zur Ablösung von ATM ist auch in der Statusbeschreibung (vgl. Kapitel 6.5.3.4) bzw. der dort angeführten Abbildung „FAU-Kommunikationsnetz, Gesamtsicht 2012" dokumentiert, die keine entsprechenden Komponenten mehr enthält.

Die beiden Gesamtsichten von 2005 (vgl. S. 89) und 2012 (vgl. S. 95) mit und ohne ATM-Strukturen sind vergleichbar aufgebaut (Core in mittlerer Zeile, Distribution in den Zeilen darüber und darunter sowie sich jeweils anschließende Access-Verteilungen) und geben so das beiden gemeinsame Grundkonzept der hierarchischen Architektur des FAU-Netzes wieder. Diese Einheitlichkeit trug dazu bei, dass die Migration des technischen Umbaus fließend und ohne größere betriebliche, für die Nutzer spürbare Unterbrechungen vollzogen werden konnte.

6.5.3.2 Netzerweiterungen, neue Standorte

Auch nach dem Erreichen einer weitgehend flächendeckenden Grundversorgung stellen sich dem Kommunikationsnetz des wissenschaftlichen Bereichs der FAU immer wieder zusätzliche Anforderungen zur Aufnahme neuer Standorte. Im betrachteten Zeitraum galt dies sowohl für verschiedene einzelne, „kleinere“ Einrichtungen als auch für „größere“ Bereiche der Universität.

Einen Eindruck über die Aufnahme „kleinerer“ Einrichtungen vermitteln exemplarisch die im Jahr 2009 angeschlossenen Standorte mit jeweils unterschiedlichem Charakter:

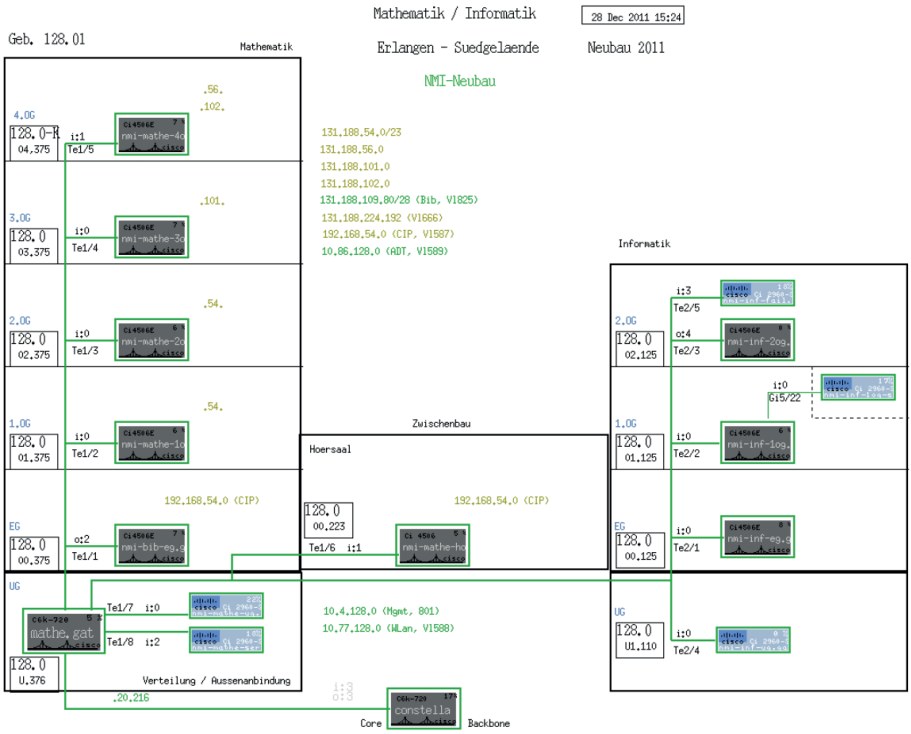
- Erlangen, Universitätsstraße 16 (Juristen), mit lizenzfreiem Richtfunk
- Erlangen, Ulrich-Schalk-Straße 3 (Bio-Verfahrenstechnik, Kirchenmusik), erst mit DSL, dann mit Richtfunk
- Erlangen, Stintzingstraße 12 (ZUV, Hörsäle Philosophie), mit DSL
- Tennenlohe, Am Weichselgarten 9 (Frauenbüro), neue Räume, in Gebäudenetz integriert
- Sozialstiftung Bamberg (Lehrkrankenhaus der FAU), mit DSL
- Nürnberg, Villa St. Paul (Department Fachdidaktiken), mit LWL an EWF-Gebäude

An „größeren“ Erweiterungen sind hervorzuheben:

- 2004 – Nürnberg, Lange Gasse, Neubau (zweites Gebäude) der WiSo, Gesamtnetzkonzept für Alt- und Neubau, Core-Standort, Verbindung nach Erlangen über Richtfunk ab 2011 mit 622 Mbit/s (vgl. auch „Netzplanung Nürnberg, 2010“ in Kapitel 6.4.4, S. 81)
- 2011 – Erlangen Südgelände, Neubau Mathematik/Informatik (NMI), Gebäude mit mustergültiger strukturierter Verkabelung und darauf aufbauender Netztopologie aus aktiven Komponenten der (seinerzeit) neuesten Generation, eigener Distributionsbereich am Core des Erlanger Südgeländes, dargestellt in „Neubau Mathematik/Informatik (NMI), Erlangen-Süd, 2011“
- 2011 – Fürth, Uferstadt am Pegnitzufer, FAU Campus Fürth, Richtfunkverbindung nach Erlangen mit 300 Mbit/s
- 2011 – Nürnberg, Fürther Straße, Energie Campus Nürnberg (EnCN) „Auf AEG“, Netzanbindung über Glasfaser (der Feuerwehr) zum WiSo-Core mit 10 Gbit/s.

6.5.3.3 Technischer Ausbau, Leistungssteigerungen

Zum technischen Ausbau des Kommunikationsnetzes zählten im passiven Bereich Nachverkabelungen in verschiedenen Gebäude(teilen) sowie Ergänzungen durch 8-adrige Kupferstrukturen als Voraussetzungen zur Realisierung von Anschlüssen mit 1 Gbit/s (vgl. Kapitel 6.3.2.2). Dies betraf zum Beispiel das „blaue“ Hochhaus (Wolfgang-Händler-Hochhaus) der Erlanger Informatik, dessen Verkabelung zuvor teilweise noch auf „alten“ koaxialen Strukturen beruhte. Zum passiven Ausbau gehörten auch die Bereitstellung eines zweiten Übertragungsweges zwischen dem Erlanger Südgelände und der Innenstadt über eine alternative Trasse sowie die bereits oben (vgl. Kapitel 6.5.3.1) erwähnten Umrüstungen von Richtfunkstrecken.



Neubau Mathematik/Informatik (NMI), Erlangen-Süd, 2011

Zu Ausbau und Leistungssteigerungen im aktiven Netz gehörte die im Schwerpunkt 2005 erfolgte Anhebung der Übertragungsgeschwindigkeiten im Core zwischen Erlangen-Süd und -Innenstadt und zwischen Core und verschiedenen Distributionsbereichen im Südgelände auf 10 Gbit/s. Dies erforderte einen Austausch betreffender Komponenten, d. h. den Ersatz eingesetzter Switche/Router (Cisco Catalyst 6500) durch entsprechende Nachfolgegeräte einer neuen Generation (Cisco 6000-720). Noch mehr waren in den Access-Bereichen, bei den Kunden vor Ort, Veränderungen durch Ablösungen veralteter Komponenten geprägt. Dies betraf vor allem den Ersatz von LAN-Switchen mit Schnittstellen von 10/100 Mbit/s (meist Geräte des Herstellers 3Com) durch gigabitfähige Komponenten (in der Regel von HP oder Cisco). Die Ablösung von 3Com-Switchen war wegen ihrer Vielzahl und weiten Verbreitung Teil eines längeren, noch nicht abgeschlossenen Prozesses. Vereinzelt waren Geräte trotz beschränkter Leistungsfähigkeit aber aufgrund ihrer Robustheit noch lange im Einsatz.

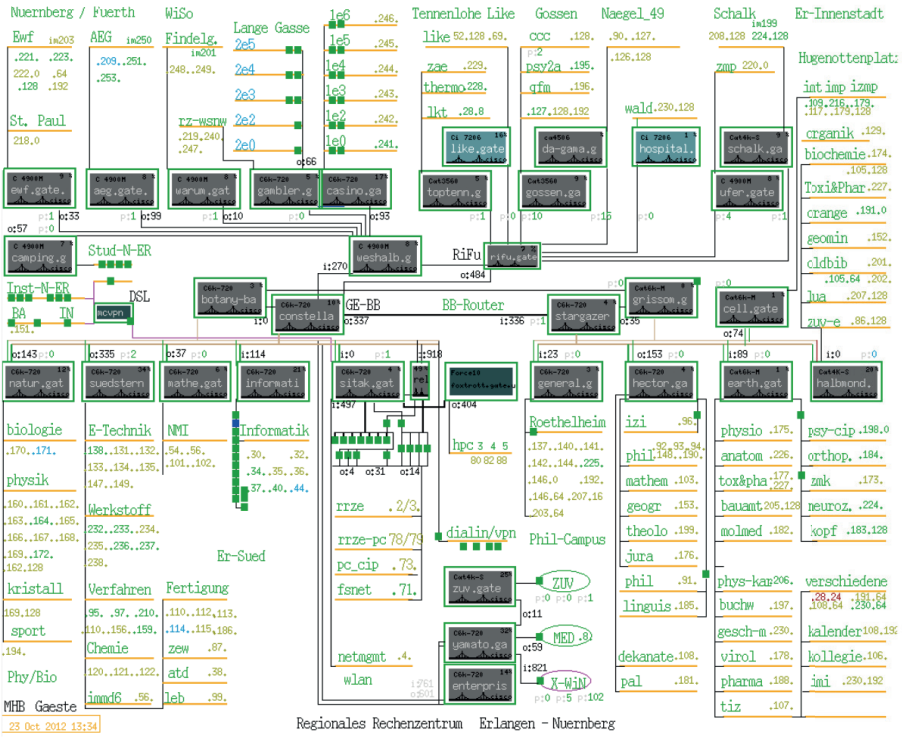
6.5.3.4 Status (2012)

Die Abbildung „FAU-Kommunikationsnetz, Gesamtsicht 2012“ auf S. 95 stellt Ausbaustand und Status des Netzes von 2012 dar. Der grundlegende Aufbau entspricht weitgehend der Gesamtsicht von 2005 (vgl. Kapitel 6.5.3.1). Im Gegensatz dazu enthält die des Jahres 2012 keine ATM-Komponenten mehr und dokumentiert somit den Vollzug des Migrationsprozesses zu rein auf Ethernet-Technik basierenden Übertragungsstrukturen und Komponenten.

Die mittlere Zeile enthält die Komponenten des Cores und zwar die redundanten Paare in Erlangen Süd („constallation“, „botany-bay“) und der Innenstadt („stargazer“, „grissom“) sowie den Verteiler in Nürnberg („weshalb“) (vgl. Kapitel 6.4.4). Unterhalb der Core-Komponenten sind die Erlanger Distributionskomponenten und ihre anhängenden Access-Bereiche dargestellt. Im Vergleich zum Status von 2005 sind hier die Bereiche der neu gestalteten Informatik (vgl. Kapitel 6.5.3.3) und des Neubaus Mathematik / Informatik (NMI) (vgl. Kapitel 6.5.3.2) hinzugekommen (Router „informatik“ bzw. „mathe“). Der obere Bildteil enthält auf der linken Seite die an ihrer Core-Komponente („weshalb“) angehängten Nürnberger Bereiche, darunter die Router („gambler“, „casino“) im neuen Gebäudekomplex der WiSo, Lange Gasse und des neu erschlossenen Campus („aeg“) auf dem ehemaligen AEG-Gelände (vgl. Kapitel 6.5.3.2). Der rechte, obere Bildteil stellt innerhalb Erlangens verteilte Bereiche dar, die über Richtfunkstrecken an den Core angebunden sind (vgl. Abbildung von 2010 in Kapitel 6.5.3.1). Die in den Statusbildern gezeichneten Router-Symbole geben für die einzelnen Objekte durch Farbgebung und den (in der präsentierten Auflösung allerdings nur schwer lesbaren) Text oberhalb ihres Namens auch Hinweise auf den jeweiligen Gerätetyp. Im Vergleich der Darstellungen von 2005 und 2012 lassen sich daher auch

verschiedene Tauschaktionen nachvollziehen, die zum Teil im Zusammenhang mit der generellen ATM-Ablösung standen, stets aber mit deutlichen Leistungssteigerungen verbunden waren, so bspw. der Typenwechsel des Routers in der EWF-Nürnberg (ewf) von „Cisco 3640“ zu „Cisco 4009M“ oder der des Routers in Tennenlohe (toptenn) vom Typ „Cisco 7206“ zu „Cisco 3560“, wodurch dann die LAN-Switch-Funktionalität für Ethernet-Schnittstellen mit bis 1 Gbit/s lokal zur Verfügung gestellt werden konnte.

Der Ausbau des passiven Netzes versorgte 2012 rund 200 Gebäudegruppen nach den Regeln der strukturierten Verkabelung und umfasste etwa 25.000 Kupfer-Anschluss-(Doppel-)Dosen in den Räumen, stellte dabei auch Netzanschlüsse in Hörsälen und Seminarräumen zur Unterstützung der Lehre bereit.



FAU-Kommunikationsnetz, Gesamtsicht 2012, S. 95

Gemäß Auswertung einer Datenbasis des Netzwerkmanagements (vgl. Kapitel 7.3.2) bestand das aktive Netz im Oktober 2012 aus 65 Routern und 750 zentral gemanagten LAN-Switchen. Auf IP-Ebene enthielt es ca. 1.050 Subnetze, davon 555 aus dem auch nach außen gerouteten Adressbereich „131.188.x.x“ der FAU (vgl. Teil 1, Kapitel 4.3.3.1), 265 aus dem internen, hauptsächlich vom Netzwerkmanagement genutzten Bereich „10.x.x.x“ und 230 sonstige Netze mit vornehmlich weiteren „privaten“ Adressen. Zur Abschätzung der Menge angeschlossener Endsysteme dienten die im Nameservice bekannten IP-Objekte. Ihre Anzahl wurde von der DNS-Verwaltung des RRZE im November 2010 mit über 40.000 angegeben und stieg in der Folge weiter an.

In Ergänzung zum drahtgebundenen Netz, wurde das flächendeckende WLAN an der FAU ständig weiter ausgebaut. So sorgten Ende 2012 rund 1.200 APs, verteilt auf alle Campusgebiete in Erlangen, Nürnberg, Tennenlohe, Bamberg und Ingolstadt, dafür, dass für Studierende wie Beschäftigte unabhängig vom Standort stets ausreichender WLAN-Empfang zur Verfügung stand. Gegenüber dem oben (vgl. Kapitel 6.3.5.3) dargestellten Nutzungsprofil von 2011 hatte sich die Anzahl der Nutzer innerhalb eines Jahres nochmals verdoppelt. In Spitzenzeiten waren mehr als 4.000 Benutzer gleichzeitig im WLAN unterwegs. Der Ansturm der Nutzer entwickelte sich ungebrochen weiter.

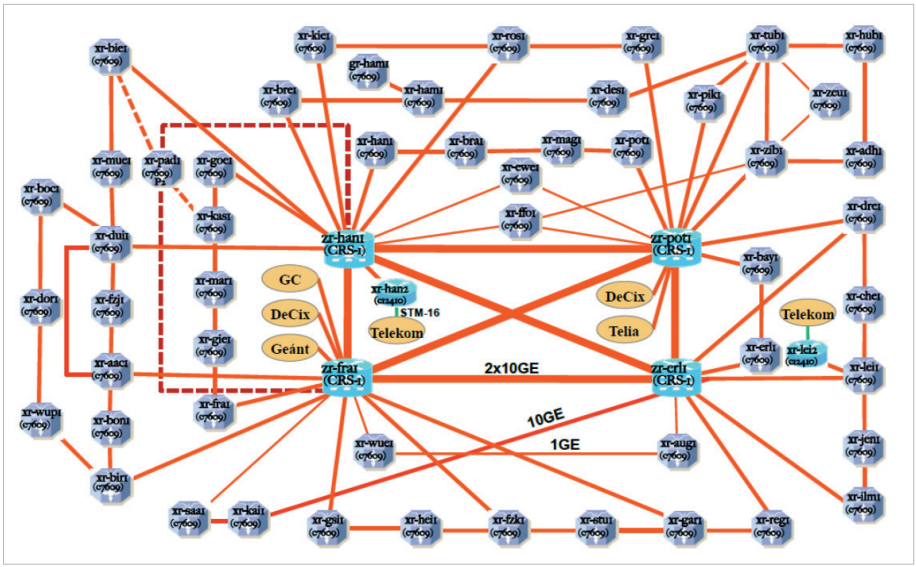
6.5.4 Kernnetzstandort des Deutschen Wissenschaftsnetzes (WiN)

Die technologische Entwicklung des vom DFN-Verein betriebenen Wissenschaftsnetzes durchlief ähnliche Stufen wie die des daran angeschlossenen Netzes der FAU. Den ersten Realisierungen auf der Basis von X.25, (WiN: 1989, ErWiN: 1992), dem ATM zu Grunde liegenden Breitbandnetz (B-WiN: 1996), folgten das Gigabitwissenschaftsnetz (G-WiN: 2000), mit Ethernet-Fernverbindungen, das beschleunigte Netz der 5. Generation (X-WiN: 2005) mit anfänglichen Anschlussgeschwindigkeiten von bis 10 Gbit/s sowie dessen Weiterentwicklung unter Berücksichtigung jeweils aktueller Anforderungen und technologischer Möglichkeiten.

Neben dem technologischen Wandel war mit der Einführung des X-WiN auch ein neuer struktureller und betrieblicher Ansatz verbunden. Dabei bezog sich eine gravierende Änderung auf die Standorte der Netzkomponenten, die nun nicht mehr bei Providern (bspw. Deutsche Telekom) aufgestellt wurden, sondern in Räumen ausgewählter Kunden. Hier kam dem RRZE die Rolle eines von 43 Kernnetzstandorten mit den Aufgaben des entsprechenden „Housings“ zu. Die Abbildung „X-WiN-Topologie, 2005“ auf S. 97 stellt die über Deutschland verteilten Standorte und ihre per Glasfaserstrecken realsierten Verbindungswege dar, darunter auch den mit „ERL“ bezeichneten an der FAU.

X-WiN-Topologie, 2005

In weiterer Differenzierung der darauf aufbauenden aktiven Struktur gehörte Erlangen zusammen mit Frankfurt, Hannover und Potsdam zu den vier Hauptstandorten des sogenannten Super-Core-Netzes, die im Kreis mit Bandbreiten von 100 Gbit/s untereinander verbunden waren. In der Abbildung zum „X-WiN Kernnetz für den Dienst DFNInternet, 2009“ sind diese als hellblaue Kästchen dargestellt.



X-WiN Kernnetz für den Dienst DFNInternet, 2009

Die Universität war dadurch sehr eng mit der Basisstruktur des Wissenschaftsnetzes verbunden und konnte mit 10 Gbit/s redundant daran angeschlossen werden.

Darüber hinaus wurde am RRZE die Zusammenarbeit mit dem DFN ausgeweitet und das „WiN-Labor“ zur Durchführung verschiedener, betriebsbegleitender Projekte eingerichtet. Diese betrafen die Bearbeitung von Themen zur Qualitätssicherung, zum Accounting, zu IP-Performance-Messungen und zu Performance Monitoring im X-WiN. Zur Projektbearbeitung gehörten Konzeptentwürfe, Entwicklungen von Werkzeugen, praktische Umsetzungen sowie regelmäßige Messungen und Aufzeichnungen (vgl. Kapitel 7.7.3).

Der Datenverkehr der FAU zum bzw. vom X-WiN stieg kontinuierlich und lag im Jahr 2012 bei einem Tagesumsatz von über acht TB (1 Terabyte = 1.000 Gigabyte).

6.6 Zusammenfassung des Abschnitts und Ausblick

Die betrachtete Phase (2000-2012) war geprägt von einem schrittweisen Abbau der ATM-Technik, zunächst beim Umbau der Anschlüsse von Endgeräten (Access), dann in Verteilstrukturen mit Lokalnetztechnik (Core, Distribution) und schließlich bei der Realisierung von Fernverbindungen (Region, Stadt) über Richtfunkstrecken. Die Netzstruktur wurde somit (ausschließlich) geprägt durch:

- Strukturierte Verkabelung, einschließlich Funkverbindungen (ISO-Schicht 1)
- Ethernet-LAN-Switching über Glasfaser- und Kupferkabel (TP) (ISO-Schicht 2)
- IP-Protokoll (überwiegend IPv4) und Routing (ISO-Schicht 3).

Hinzu kam die Einführung drahtloser Netze (WLANs), die mit der Schaffung mobiler Zugänge als Erweiterung des Access-Bereichs angesehen werden können.

Neben dem generellen Ausbau des Netzes bzgl. Verdichtungen oder neuer Standorte sind punktuelle Leistungssteigerungen bzw. Anhebungen von Übertragungsgeschwindigkeiten auf 10 Gbit/s in Core-/Distribution- sowie 1 Gbit/s in Access-Bereichen hervorzuheben.

Die Netzstruktur wurde konsequent nach dem hierarchischen Modell von Core, Distribution und Access gestaltet.

Es wurden somit Grundlagen zur Weiterführung der angeführten Entwicklungen gelegt, ohne dazu künftig prinzipielle Veränderungen vornehmen zu müssen. Die Erhöhung von Zuverlässigkeit und Leistungssteigerung (u. a. durch Anhebung der Anschlussgeschwindigkeiten) erfordert den Ersatz „veralteter“ Komponenten durch jeweils aktuelle, leistungsstärkere Geräte (nicht zuletzt ein finanzielles Problem). Auf IP-Ebene stand im Zuge eines allgemein erkennbaren Trends und zur Reduzierung der Problematik knapper IP-Adressen ein verstärkter Einsatz der Internetprotokollversion 6 an.

Das anschließende Kapitel 7 beschäftigt sich zudem mit verschiedenen Aspekten und Problemen des Netzbetriebs aus der Sicht des folgenden Zeitraums.

Hierarchische Netz- und Betriebsinfrastruktur 2013 – 2018

7. Hierarchische Netz- und Betriebsinfrastruktur 2013 - 2018

Auch die Phase von 2013 bis zum 50. Jubiläum des Rechenzentrums 2018 war von Ausbau und vielfältigen Anpassungen an stets wachsende Anforderungen gekennzeichnet. Dies galt sowohl für das Rechenzentrum allgemein als auch speziell für die Infrastruktur des Kommunikationsnetzes.

Die Bedeutung des RRZE als IT-Dienstleister der FAU wurde weiter gestärkt und durch einige markante Entwicklungen geprägt, wie etwa die einer zentralen Benutzer- und Systemverwaltung (Stichwort: IdM). Die vielfältigen Aufgaben des RRZE spiegelten sich auch in der organisatorischen Gliederung in Abteilungen mit jeweils spezifischen Arbeitsfeldern wider.

Zu den Kernaufgaben des Rechenzentrums gehörte auch weiterhin die zentrale Bereitstellung von Rechnerleistungen, und zwar direkt für verschiedene Benutzergruppen oder indirekt zur Erbringung der vielfältigen, angebotenen Dienstleistungen. Hierzu wurde die entsprechende Serverlandschaft ausgebaut und insbesondere noch effizienter auf Höchstleistungsanforderungen eingestellt (Stichworte: Datacenter, HPC). Gestiegen ist auch der Anteil an Betreuung dezentraler Systeme in lokalen Bereichen, deren Betrieb durch die zentralen Kompetenzen des RRZE effektiver und sicherer gestaltet werden konnte und die Benutzer von fachfremden Arbeiten entlastete.

Die Bereitstellung von IT-Diensten oder Rechenkapazitäten für eine Universität erfordert generell ein leistungsfähiges Kommunikationsnetz und ist ohne den Einsatz entsprechender Technik, anforderungsgemäßer, durchdachter Strukturen und zuverlässiger Betriebsführung nicht denkbar.

Demzufolge galt es technische Entwicklungen zu verfolgen und deren Anwendungsmöglichkeiten zu prüfen, wie etwa die Verbreitung einer „neuen“ Internetprotokollversion (Stichwort: IPv6) oder die Verfügbarkeit neuer Vermittlungskomponenten zur Steigerung der Übertragungsleistungen (im Vergleich zu den jeweils aktuell eingesetzten Geräten). Darüber hinaus war das RRZE auch an vorausschauenden Forschungs- und Entwicklungsprojekten beteiligt.

Zu einem möglichst stabilen und geordneten Betrieb des Kommunikationsnetzes einer stark verteilten Universität gehören auch Absprachen bzw. Regularien über Zuständigkeiten zwischen zentralen und dezentralen Einrichtungen bzw. beteiligten Personen sowie ein gewissenhaftes Management zur Überwachung und Pflege des realen Netzes bzw. seiner Komponenten. Diesbezüglich waren aus verschiedenen Gründen, etwa im Zusammenhang mit einer allgemeinen Tendenz zur Rezentralisierung von DV-Auf-

gaben an Hochschulen, verschiedene Anpassungen bzw. Modifikationen unter sich ändernden Bedingungen erforderlich. Eine wichtige Unterstützung zu Organisation und Management des Netzbetriebs boten in verschiedenen Entwicklungsphasen spezifische Hilfsmittel und Werkzeuge. Sie halfen unter anderem bei der Dokumentation, Konfiguration, Beobachtung oder Fehlerbehebung. Derartige Methoden und Ausprägungen wurden am RRZE zwar auch schon in früheren Phasen der Netzentwicklung eingesetzt, mussten aber auch aktuellen Gegebenheiten angepasst werden.

Ähnliches galt auch für die Aspekte von Datenschutz und Netzsicherheit. Das verbindungslose Internetprotokoll mit dem Ansatz einer unbegrenzten Kommunikationsbasis barg auch immer Gefahren des Missbrauches oder gar gezielter Angriffe. Diese erhöhten sich mit der wachsenden Ausbreitung des Internets und der erheblichen Ausweitung des Nutzerkreises enorm. Auch die FAU war / ist von dieser Problematik intern und extern betroffen, die allerdings nicht allein auf der Netzebene, sondern z. B. auch durch Maßnahmen in den Systemen sowie einem regelgerechten Verhalten der Universitätsangehörigen zu lösen war / ist. Im Netz können zur Minderung von Gefährdungen bestimmte Einschränkungen von Kommunikationsbeziehungen, verschiedene inhaltliche Kontrollen des Datenverkehrs oder spezielle Prüfungen konfiguriert werden. Entsprechende Maßnahmen erfordern regelmäßige Analyse, Revision und Einrichtung auf jeweils neu beobachtete Angriffsmethoden.

Die Kernaufgabe des Kommunikationsnetzes und seines Betriebs betrifft das Vermitteln und Transportieren von Daten zwischen Netzteilnehmern. Nicht direkt dazugehörend aber doch sehr eng damit verbunden, sind Anwendungsfelder wie die Elektronische Post oder das Übertragen von Audio- und Videodaten, deren Entwicklung näher betrachtet wird. Auch die Durchführung von Forschungsprojekten mit Netzthemen war nicht unmittelbar dem regulären Netzbetrieb zuzurechnen, war aber zum Teil darin integriert und regte zu künftigen Entwicklungen an.

Die Abgabe der Betreuung von Aufbau und Netzbetrieb des Universitätsklinikums Erlangen in der vorangegangenen Phase war auch mit dem Verlust verfügbaren Personals und entsprechender Synergien verbunden, schuf aber auch Entlastung und die Möglichkeit seine Aufgaben und Tätigkeiten noch stärker auf die Netze des Verwaltungs- und des wissenschaftlichen Bereiches der Universität zu konzentrieren.

Die passiven und aktiven Strukturen des drahtgebundenen und des drahtlosen Netzes wurden durch Verdichtung und Integration neuer Standorte weiter ausgebaut. Zudem wurde die Leistungsfähigkeit durch punktuellen Einsatz von Komponenten neuester Generation, besonders aber durch die möglich gewordene Nutzung von Glasfaserstrecken zwischen Erlangen und Nürnberg sowie innerhalb Nürnbergs, deutlich gesteigert und so eine gleichwertige Netzversorgung der Standorte beider Städte erreicht.

Mit den beschriebenen Entwicklungen waren Ausbau und Gestaltung des Kommunikationsnetzes im Jahr 2018 natürlich keineswegs abgeschlossen. Vielmehr bedeuteten sie auch eine Grundlage zur Weiterführung und Einstellung auf künftige Anforderungen, um weiterhin eine angemessene Netzversorgung der Universität zu gewährleisten.

7.1 Das RRZE als IT-Dienstleister der FAU Erlangen-Nürnberg

Die Entwicklung des RRZE zum IT-Dienstleister der FAU (vgl. Kapitel 6) und der erreichte Status innerhalb der Universität kann natürlich nie als abgeschlossen gelten, sondern erfordert ein ständiges Eingehen auf neue Entwicklungen bezüglich gestellter Anforderungen und technischer Möglichkeiten. Das RRZE trug / trägt dem unter den Rahmenbedingungen personeller Ausstattung oder verfügbarer Finanzen nach Kräften Rechnung, auch wenn diese Grundlagen in der Regel nur knapp bis unzureichend vorhanden waren bzw. sind.

Die Rolle des RRZE an der FAU unterstreicht auch die Mitwirkung an der Erstellung eines umfassenden Strategiepapiers zur Informationstechnologie an der Friedrich-Alexander-Universität. Das Papier wurde im Auftrag des Kanzlers der FAU erarbeitet und von den zuständigen Gremien 2014 verabschiedet. Als erstes umfassendes IT-Dokument der FAU ist das „IT-Konzept 2011-2015“ [*ITKonz*] auch für das RRZE von entscheidender Bedeutung. Es macht eine Bestandsaufnahme von Infrastruktur und Technik, erfasst die Dienste und Diensterbringer an der FAU mitsamt den dazu gehörenden Prozessen sowie den Nutzern und ihren Anforderungen. Dazu bietet es Orientierung, stellt aber auch Herausforderungen an die Universität und den IT-Dienstleister dar.

7.1.1 Abteilungen des RRZE (Organisation)

Umfang und Vielfältigkeit angebotener IT-Dienste erfordern vom Erbringer entsprechende Organisation und Strukturierung. Das RRZE ist daher in verschiedene Abteilungen mit jeweils spezifischen, themengebundenen Aufgaben gegliedert. Diese Aufteilung enthielt über die Jahre ähnliche Grundzüge, wurde aber auch nach Bedarf an aktuelle Entwicklungen angepasst. Auch bei zum Teil gleichbleibenden Bezeichnungen der Gruppen werden deren Arbeitsinhalte regelmäßig hinterfragt und gemäß neuen Anforderungen und Möglichkeiten modifiziert.

Abteilungsstruktur und Aufgabenverteilung geben auch einen groben Überblick über das vielfältige Dienstleistungsspektrum des RRZE. Nach aktueller Überarbeitung, stellten sie sich Anfang 2018 wie folgt dar:

Stabsabteilung „Beschaffung, Haushalt, Controlling“

Die Abteilung entstand aus einer funktionalen und namentlichen Wandlung der zuvor geführten Abteilung „Unterstützung dezentraler Systeme“. Der neue Name der Stabsabteilung „Beschaffung, Haushalt, Controlling“ gibt dabei einen groben Überblick über ihre Aufgaben. Dabei nehmen der Kontakt mit Softwareherstellern und Benutzern

der FAU einschließlich der mitbetreuten Region, die Verwaltung und Weitergabe von Lizenzen, Anwendung von Abrechnungsverfahren und Umsetzungen von Dokumentationspflichten einen wesentlichen Anteil des Tagesgeschäfts ein. Hinzu kommen erforderliche Anpassungen angewandter Verfahren an sich ändernde Konditionen und Projekte zur Weiterentwicklung unterstützender Software.

Abteilung „Zentrale Systeme"

Die aus der früheren „Systemgruppe" hervorgegangene Abteilung erfüllt weitgehend die „traditionellen" Aufgaben eines Rechenzentrums mit der zentralen Bereitstellung von Rechnersystemen und darauf laufender Software. Heute wird dazu eine Farm von Servern betrieben, die vorwiegend unter den Betriebssystemen Linux und Windows laufen. Einige dieser Server bieten Dienste an, die direkt sichtbar sind, wie Webangebote und E-Mail, andere wiederum eine ganze Reihe an Datenbank-, Archivierungs- und Datensicherungsdiensten, die „eher im Hintergrund" arbeiten. Weiter gehören die Betreuung besonders leistungsfähiger Rechner (HPC) und spezieller Peripherie (Farbdrucker, hochauflösende Scanner oder Großformatplotter) sowie der Betrieb einer zentralen Benutzerverwaltung (vgl. Identity Management (IdM), Kapitel 7.1.2) zu den Aufgaben dieser Abteilung.

Abteilung „Kommunikationssysteme"

Die Aufgaben der Abteilung „Kommunikationssysteme" beschreiben, wie die der Systembetreuung, ein ebenso traditionelles, seit Gründung des RRZE bestehendes Arbeitsfeld. Die Abteilung hat die in dieser Dokumentation aufgezeichnete „Geschichte der Datenübertragungs- und Kommunikationsdienste" an der FAU von den Anfängen der Datenübertragung bis zu komplexen Netzstrukturen maßgeblich geprägt bzw. gestaltet. Sie untergliedert sich aktuell in vier Arbeitsgruppen mit den Bereichen von Vernetzung und Betrieb (Netzinfrastruktur und -dienste), netznahen Anwendungen (E-Mail, Multimediazentrum) sowie Forschungen im Umfeld von Datennetzen (Forschungsgruppe Netz).

Im Kern ist die Gruppe „Netzinfrastruktur und -dienste" für Aufbau, Betrieb und Betreuung der Datennetze an der FAU zuständig. Ihre Aufgaben bzw. Tätigkeiten stehen in äußerst engem Verhältnis zu den in der vorliegenden Dokumentation beschriebenen Entwicklungen und leiten sich weitgehend daraus ab.

Die Tätigkeiten der anderen, nicht unmittelbar mit dem Kernnetzbetrieb befassten Arbeitsgruppen sind Gegenstand eines gesonderten Kapitels über „Netznahe Anwendungsfelder" (Kapitel 7.7).

Abteilung „Entwicklung, Integration, Verfahren"

Die ehemalige Abteilung „Entwicklung & Integration" und Teile der ehemaligen Abteilung „Datenbanken und Verfahren" finden sich unter dem Dach der neuen Abteilung „Entwicklung, Integration, Verfahren (EIV)" wieder. Auf diese Weise können die vielfältigen, notwendigen Anpassungen für Verfahren der ZUV noch besser unterstützt und auch größere Projekte koordiniert angegangen werden.

Die Vorgängerabteilung „Entwicklung & Integration" ging ihrerseits am 1. April aus der im Jahre 2007 am RRZE eingerichteten Stabsstelle „Projekte & Prozesse" hervor. Zahlreiche Aufgaben, die die Stabsstelle in ihrer Anfangszeit noch in enger Abstimmung mit der Universitätsleitung als Projekte in Gang gesetzt hat, haben sich im Laufe der Jahre als dauerhafte Arbeitsabläufe etabliert und werden für die FAU dauerhaft betrieben. Signifikant sticht hier die erfolgreiche Inbetriebnahme eines universitären „Identity Managements" (IdM) hervor, das inzwischen die Grundlage für eine effiziente Nutzung nahezu aller neu eingeführten universitären IT-Dienste bildet. Aber auch andere von der Stabsstelle entwickelte Anwendungen im Campus- und Verwaltungskontext haben ihren festen Platz in der Systemlandschaft der Universität gefunden. Dies begründet die Umwidmung der Stabsstelle zur Abteilung.

Die ebenfalls integrierte, vorige Abteilung „Datenbanken und Verfahren" war aus einer Zusammenlegung des ehemaligen Sachgebietes Datenverarbeitung der zentralen Universitätsverwaltung mit dem RRZE am 15. März 2005 entstanden. In ihr wurden Aufgabengebiete „Arbeitsplatzbetreuung", „Datenbanken und DV-Verfahren" der Zentralen Universitätsverwaltung (ZUV) gebündelt.

Die Abteilung EIV fasst diese Aufgabengebiete zusammen und bearbeitet sie unter den Schwerpunktthemen „Datenintegration", „Anwendungen & Datenbanken" und „Ressourcenverfahren".

Abteilung „Ausbildung und Information"

Das Ausbildungs- und Informationsangebot des IT-Dienstleisters ist vielfältig. Über ein eigenes IT-Schulungszentrum bietet das RRZE ganzjährig eine umfangreiche Palette an kostengünstigen Softwareschulungen an. Während der Vorlesungszeit kommen die Veranstaltungsreihen Campustreffen, Systemausbildung und Netzwerkausbildung hinzu. Sie stehen allen Beschäftigten und Studierenden der FAU offen und führen in die Nutzung der universitären IT-Systeme, Web-, E-Mail-, Netz- und Datenbankdienste des RRZE ein. Die Abteilung leistet Öffentlichkeitsarbeit, koordiniert (dezentrale) Beschaffungen und ist unter anderem für den beschriebenen Webdienst oder die Ausbildung zum Fachinformatiker zuständig (vgl. Kapitel 6.1.1).

Abteilung „Kundenservice"

Die neu geschaffene Abteilung „Kundenservice" setzt sich aus dem IT-Betreuungszentrum Innenstadt (IZI), dem IT-Betreuungszentrum Nürnberg (IZN), dem IT-Betreuungszentrum Halbmondstraße (IZH) und dem IT-Betreuungszentrum Süd (IZS) zusammen. Zu den Betreuungszentren gehören auch die jeweiligen Service-Theken, die für alle Nutzer von IT-Dienstleistungen an der FAU als Anlaufstelle fungieren. Die Betreuungszentren stehen den Einrichtungen der FAU bei der Beschaffung von Hard- und Software zur Seite, koordinieren notwendige Netzwerkarbeiten mit der Abteilung Kommunikationssysteme und betreuen die Arbeitsplätze ((Windows, Linux, Apple). Die Betreuungszentren IZI, IZH und IZN werden im Rahmen der fachlichen Weisungsbefugnis als Außenstellen des RRZE geführt. Den Betrieb vor Ort koordinieren die Leiter der IT-Betreuungszentren. Beschaffungen und Reparaturen von bzw. an IT-Systemen sind über die IT-Beauftragten der Fakultäten mit den IT-Betreuungszentren abzustimmen.

Die Fusion der bisher über drei Abteilungen verteilten Service-Anlaufstellen soll Kompetenzen bündeln, um die Kunden vor Ort noch besser und effizienter unterstützen zu können.

7.1.2 Ausbau der IT-Dienstleistungen (markante Beispiele)

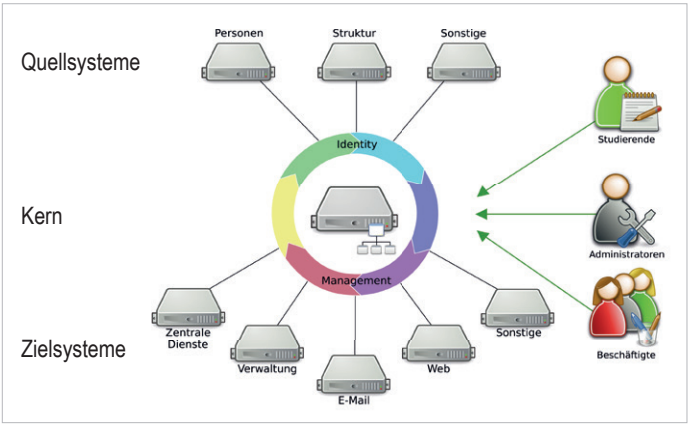
Als IT-Dienstleister der FAU muss sich das RRZE mit seinem Spektrum stets an neue oder veränderte Anforderungen anpassen, die von Universität und Nutzerschaft gestellt werden oder sich aus eigener Planung und Voraussicht ergeben. Den jüngeren Ausbau der IT-Dienstleistungen (2012 – 2018) illustrieren verschiedene, markante Beispiele. Diese machen auch deutlich, dass derartige, moderne Dienstleistungen nur auf Basis einer zuverlässigen, weit verbreiteten Kommunikationsinfrastruktur zu erbringen sind.

Identity Management (IdM)

Die etwa 2006 begonnene Einrichtung eines Identity-Management-Systems der Universität wurde weitergeführt und der Ausbau weiter vorangetrieben. Es ermöglichte (ab 2012) die Verwaltung universitärer Identitäten, d. h. die Begleitung einer Person vom ersten Kontakt mit der Universität, über das Studium, eventuelle Beschäftigungen bis zum Verlassen der Hochschule mit einer durchgehend zugeordneten Kennung. Damit sind dann unter anderem jeweilige Berechtigungen verknüpft wie etwa zur Nutzung verschiedener Rechnersysteme von Mensa, Bibliothek, Kopierdiensten oder die Zuordnung von E-Mail-Postfächern. Ebenfalls funktionieren darüber die Anmeldungen bei der Online-Serviceplattform „mein campus" (vgl. Kapitel 6, „Hochschulweite Verwaltungsdienste") und der damit verbundenen Lernplattform „StudOn".

Im Gegensatz zur klassischen Benutzerverwaltung werden im Identity-Management-System nur sehr wenige Daten direkt erfasst bzw. verwaltet. Vielmehr befindet sich das System im Zentrum vieler anderer Systeme und dient als Vermittler zwischen Quellsystemen und Zielsystemen. Quellsysteme stellen die Lebensader des Identity-Management-Systems dar, denn aus ihnen werden die aktuellen Daten bezogen (lesender Zugriff). Zu ihnen gehören Systeme der Personenverwaltung (z. B. Hochschul-Informations-System, HIS), der Strukturverwaltung (FAU.ORG) und sonstiger fachlicher Bereiche (z. B. E-Mail-Adressverwaltung). Zielsysteme sind Systeme, auf die IdM „schreibend" zugreift, d. h. zumindest ein Teil der Daten, mit denen das Zielsystem operiert, stammen aus der „Datenzentrale" IdM. Sie benötigen diese Daten, damit sie ihre Dienstleistungen anbieten können. Zu den Zielsystemen gehören unter anderem die Studierendenverwaltung „HIS-SOS", das Studierendenportal „mein campus", die Promovierendenverwaltung „docDaten", das Kartenproduktionssystem der „FAU*card*" oder das Bibliothekssystem „SISIS". Weiterhin werden einige Dienste, die das RRZE bereitstellt, mit Daten versorgt wie z. B. das WLAN-System „eduroam", das E-Mail-System, das zentrale Groupware-System „Exchange", die zentrale Windows-Benutzerverwaltung „Active Directory" oder der zentrale Anmeldedienst der FAU „Single Sign-on".

Der gesamte IdM-Komplex ist modular und erweiterbar aufgebaut. Die beschriebene Grundstruktur ist in der Abbildung zur „Architektur des Erlanger Identity Managements" illustriert.



Architektur des Erlanger Identity Managements

FAU*card* für Bedienstete und Studierende

Eng verknüpft mit der Einführung des IdM und ohne dieses nicht umsetzbar war ein Projekt zur Realisierung einer „Chipkarte für Alles“ an der FAU, d. h. einer einheitlichen elektronischen Karte für verschiedene Anwendungen an Stelle spezifischer Einzellösungen. Das betraf z. B. Bezahlvorgänge in der Mensa, Ausleihen in der Bibliothek, die Zeiterfassung von Bediensteten oder auch die Bedienung von Schließsystemen. Das RRZE übernahm als IT-Dienstleister die Leitung eines Projekts der Universität zur Entwicklung einer solchen Karte und führte als Ergebnis die „FAU*card*“ in der Praxis ein. Sie wurde zunächst an Studierende (2011), dann an Bedienstete (2012) ausgegeben, deren betreffende Prozesse sich doch erheblich voneinander unterschieden. Die Funktionen von Studierendenkarte, UB-Ausweis, Mensakarte oder Kopierkarte waren nun ebenso auf einer Chipkarte vereint wie die Möglichkeiten zum „Ein- und Ausstempeln“ von Mitarbeitern. Wie die des IdM, war die Entwicklung der FAUcard damit noch nicht abgeschlossen, sondern wurde in der Folge ebenso durch zusätzliche Funktionen und Anwendungsmöglichkeiten erweitert.

Sync-&Share-Dienst (FAUbox)

Mit der Einführung der „FAUbox“ (2014) wurde am RRZE ein System etabliert, das zur Ablage und Synchronisation, zur Bearbeitung von verschiedenen Endsystemen und zum Austausch von Daten mit Dritten geeignet ist. Damit stand an der FAU eine sichere Alternative zu den Angeboten im Internet frei verfügbarer Cloud-Dienste (z. B. Dropbox) bereit. Sicher deshalb, weil die Daten im RRZE gespeichert werden und keine externen Personen Zugang erhalten, es sei denn, der Eigentümer vergibt explizit Rechte auf seine Daten an diese Person. Zum Funktionsumfang gehören nicht nur die Standarddienste für Datenaustausch und Synchronisation, sondern auch die Möglichkeit, einmalig via Link Daten an interne oder externe Personen zu schicken. Das entlastet das E-Mail-System und umgeht die Größenbeschränkung von E-Mails.

Die FAUbox kann (seit 2015) zusätzlich in einem erweiterten Kontext genutzt werden. Im Rahmen einer entsprechenden Kooperation des RRZE mit dem Leibniz-Rechenzentrum (LRZ) in Garching bei München und der Universität der Bundeswehr in München (UniBwM) stellen diese seit 2015 einen hochschulübergreifenden Sync-& Share-Dienst für Bedienstete und Studierende aller bayerischen Universitäten und Hochschulen bereit.

Der Dienst wurde gut angenommen und erfreute sich wachsender Beliebtheit. Ende 2016 waren mehr als 12.000 Personen auf der FAUbox registriert, Ende 2018 bereits 37.000 Personen. Auch andere Hochschulen erkannten die Vorteile der „Bayern-Cloud“ und wurden daraufhin von der FAU mit der FAUbox versorgt. So zähl(t)en die Hoch-

schulen in Ansbach, Aschaffenburg, Coburg, Ingolstadt und Nürnberg zu den Kunden. Mit dem Grad der Nutzung der FAUbox wuchs auch der verbrauchte Speicherplatz: Gemäß Erhebungen von 2016 [*JB2016*] belegten Beschäftigte im Durchschnitt 2,7 GB und Studierende begnügten sich mit 1,4 GB. Dennoch stellten die Studierenden der FAU mit 61% den größten Anteil der Nutzer, während die Beschäftigten der FAU 23% des Anteils ausmachten. Der Rest verteilte sich auf die anderen Hochschulen und die Gruppe der externen Gäste.

7.1.3 Situation zentraler Server- und Speichersysteme

Auch die Rechnerlandschaft des RRZE (vgl. Kapitel 6.1.2) unterliegt einem ständigen Wandel bezüglich technischer Entwicklungen und gestellter Anforderungen. Dabei erbringen die zentralen Server den Großteil der Dienste des Rechenzentrums. Die Systeme bestehen meist aus mehreren, eng zusammengeschalteten Prozessoren (Cluster), auf denen wiederum verschiedene virtuelle Maschinen betrieben werden und entsprechende Dienstprogramme ablaufen. Die innere Struktur bleibt den Benutzern weitgehend verborgen, statt zu individuellen Rechnern treten sie mit einzelnen Diensten in Kontakt. Für den Betrieb gehören Stabilität und gute Performanz der angebotenen Dienste zu den Hauptzielen des Rechenzentrums, die durch eine Reihe gestaffelter Maßnahmen angestrebt werden. Auf der untersten Ebene steht dabei die Auswahl geeigneter Hardware. Sie muss bestimmten Qualitätsanforderungen wie „redundante Netzteile“, „gespiegelte oder im (RAID-5/6)-Verbund betriebene Platten“ und „integrierte Überwachungsfunktionen“ Genüge tun und nach verbindlichen Kriterien konfiguriert werden. Dazu gehört ein Struktur- und Betriebskonzept, das z. B. durch entsprechende Redundanzen (Doppelauslegungen) für eine Hochverfügbarkeit von Hardware und Dienstbausteinen sorgt, automatische Lastverteilung organisiert sowie Methoden zur Überwachung und Fehlerkorrektur vorsieht. Einen weiteren Aspekt der Zuverlässigkeit der zentralen Dienste bildet die Vernetzung der sie tragenden Systeme untereinander sowie deren Zugänglichkeit über das Kommunikationsnetz der FAU. Hierzu wurde das spezifische Konzept eines „Datacenters“ entwickelt und umgesetzt, das sich als eigener, funktionsbezogener Distributionsbereich in die hierarchische Struktur eingliederte (vgl. Kapitel 6.4, 7.2.2).

Auch zum Bereich der dezentral betreuten Systeme gehören zentral betriebene Server, etwa zur Anbindung an den Windows-Verzeichnisdienst der FAU (Active Directory) oder zum Download bereitgestellter Programme und der Verwaltung von Lizenzen. Das RRZE unterstützt dezentrale Rechner mit den Betriebssystemen Windows (PCs), Unix (Workstations) und macOS (Apple-Rechner).

FAU-Höchstleistungsrechner „Emmy", 2013

Zu den Diensten des Rechenzentrums gehört(e) auch stets die Bereitstellung zentraler Rechenkapazitäten, wobei insbesondere der Höchstleistungsbereich (vgl. Kapitel 6.1.2) immer mehr Bedeutung erlangte. Verschiedene Anforderungen z. B. aus Natur- und Ingenieurwissenschaften waren und sind von lokalen Systemen auch trotz deren Leistungssteigerungen nicht zu erbringen. Das RRZE orientiert(e) sich zudem mit seiner High-Performance-Computing-Gruppe (HPC-Gruppe) an nationalen und internationalen Entwicklungen, um seinen Forschern konkurrenzfähige Angebote machen zu können. So wurde z. B. im Jahr 2013 der neue HPC-Cluster „Emmy" (in Erinnerung an die 1882 in Erlangen geborene Mathematikerin Amalie Emmy Noether) in Betrieb genommen, der es mit einer gemessenen Rechenleistung der 11.200 CPU-Rechenkerne von 191 TFlop/s auf Platz 210 der Top500-Liste mit den schnellsten HPC-Systemen weltweit geschafft hatte und innerhalb Deutschlands immerhin auf Platz 14 rangierte. Durch die dadurch massiv angestiegene Rechenleistung wurden nicht nur Aufgaben lösbar, die bisher den großen Bundesrechnern in Garching, Stuttgart oder Jülich vorbehalten waren, sondern es ergaben sich auch neue Möglichkeiten, um die internationale Relevanz der Erlanger Aktivitäten auf diesen hochdynamischen Forschungsgebieten weiter auszubauen. Für zuverlässige und performante Zugriffe wurde das Clustersystem in das Datacenter des FAU-Netzes integriert.

7.1.4 Anforderungen an die Kommunikationsinfrastruktur

Mit den beschriebenen Entwicklungen von IT-Dienstleistungen und Serversystemen stiegen auch die Anforderungen an die Kommunikationsinfrastruktur. Ein großer Teil der Dienste setzt ein uniweites, funktionierendes Datennetz voraus. So wäre z. B. das FAU*card*-System mit seinen verteilten Eingabestationen, dem Zugriff auf spezifische Server und der Unterstützung durch das Identifikationssystem (IdM) ohne verfügbare Vernetzung nicht denkbar.

Wie generell im Zusammenhang mit dem Internet erweiterten sich auch an der FAU der Nutzerkreis, das Anwendungsspektrum und der Bedarf an Zugangsmöglichkeiten. Man denke dabei etwa an die allgemeine Verbreitung mobiler Endgeräte (Smartphones, Tablets) oder die Einbeziehung „wenig intelligenter“ Endgeräte im Sinne von „Internet of things“, mit denen sich auch das RRZE als Netzbetreiber der Universität auseinanderzusetzen hat(te). Das RRZE steuert zwar noch keine Kaffeemaschinen über das Netz, aber der Einsatz verteilter Drucker und Kopierer deutet bereits diese Richtung an.

Nach der Entwicklung einer hierarchischen Netzarchitektur, ihrer Umsetzung über strukturierte Verkabelung (Schicht 1, passives Netz), Ethernet-Technik (Schicht 2, aktives Switching) und Internetprotokoll (Schicht 3, aktives Routing) (vgl. Kapitel 6), ging es in der Folge nicht mehr um grundlegenden technologischen Wandel, sondern viel mehr um Konsolidierung, strukturelle Anpassungen, Ausbau, Erweiterungen sowie Erhöhung von Leistungsfähigkeit und Zuverlässigkeit auf der gelegten Basis.

Zu den Erweiterungen zählten vor allem die Hinzunahme des Standorts „Energie-Campus Nürnberg“ (ehemaliges AEG-Gelände). Die Erhöhung der Leistungsfähigkeit zeigt sich an der Anhebung verschiedener Übertragungsabschnitte auf Geschwindigkeiten von 10 Gbit/s, insbesondere im Zuge der Ablösung (bzw. Ergänzung) der Richtfunkverbindung zwischen Erlangen und Nürnberg durch eine Glasfaserstrecke.

Aus der wachsenden Popularität und Verfügbarkeit mobiler Endsysteme ergaben sich Anforderungen an den Ausbau des nicht drahtgebundenen Netzes, d. h. an die Schaffung weiterer WLAN-Zugänge in öffentlichen Bereichen der Universität. Das RRZE hat diesbezüglich eine weitgehend flächendeckende Versorgung erreicht. Steigende Nutzerzahlen und insbesondere gleichzeitige Nutzung in bestimmten Bereichen stellten dabei enorme Anforderungen an die Leistung bzw. den Ausbau der drahtlosen Struktur dar.

Neben der Konzeption und dem Aufbau von Netzstrukturen ergaben sich auch gesteigerte Anforderungen an die Gestaltung eines stabilen Netzbetriebs. Dies betraf unter anderem organisatorische Aspekte (Regularien, Zuständigkeiten), den Einsatz von Werkzeugen des Netzwerkmanagements (Überwachung, Fehlerbehandlung usw.) sowie Maßnahmen zur Erhöhung von Datensicherheit und Abwehr gefährdender Angriffe.

7.2 Grundlagen zu Weiterentwicklungen der Kommunikationstechnik

Das RRZE verfolgt die allgemeinen Entwicklungen im Bereich der Kommunikationstechnik und prüft, ob bzw. wieweit sie in die Gestaltung des Universitätsnetzes (bezogen auf die ISO/OSI Schichten 1 – 3) einzubringen sind und zu Verbesserungen führen können.

Im hier betrachteten Zeitraum der jüngeren Vergangenheit (2013 – 2018) haben besonders zwei Punkte zur Weiterentwicklung des FAU-Netzes beigetragen, deren Grundlagen im Folgenden näher erläutert werden. Sie betreffen die Einführung der Internetprotokollversion 6 sowie neue, geräteübergreifende Systemansätze bezüglich der Zusammenschaltung von Netzkomponenten.

7.2.1 Internetprotokollversion 6 (IPv6)

Das ungebremste Wachstum des Internets und seine Ausweitung etwa auch auf Afrika oder Asien machte die zentrale Vergabe von IPv4-Adressen bzw. Adressbereichen immer schwieriger bis unmöglich (die letzten fünf Blöcke von IP-Adressen wurden 2011 zentral zugeteilt). Nicht zuletzt diese sich frühzeitig abzeichnende Problematik motivierte zur Suche nach alternativen Lösungen bzw. zur Entwicklung einer neuen Protokollvariante.

Die Beschreibungen der folgenden Abschnitte orientieren sich an der Netzwerkausbildung des RRZE zum Thema IPv6 [*Wüv6*], insbesondere sind die Tabellen und bildlichen Darstellungen überwiegend den entsprechenden Präsentationen entnommen.

7.2.1.1 Historie (Entwicklung)

Bereits 1995 begannen Überlegungen zum Entwurf eines Nachfolgers der weit verbreiteten IP Version 4 (IPv4, RFC-791). Mit einer neuen Protokollgeneration (IP next generation, IPng) sollten erkannte Schwachstellen behoben und verschiedene Verbesserungen erreicht werden. Im Dezember 1998 veröffentlichte dann die Internet Engineering Task Force (IETF) den RFC-2460 mit dem Titel „Internet Protocol, Version 6 (IPv6)“. Darin werden die wichtigsten Änderungen von IPv4 zu IPv6 in folgenden Punkten beschrieben:

- Erweiterte Adressierungsmöglichkeiten (Expanded Addressing Capabilities)
  Die IPv6-Adressen haben eine Länge von 128 Bit. Sie spannen dadurch einen enormen Adressraum auf (theoretisch 340 Sextillionen) und ermöglichen ein strukturiertes Adressierungsschema mit einer hierarchischen Vergabestrategie.
  Erweiterungen im Zusammenhang von Multicasts bieten unter anderem neue Möglichkeiten zur effektiveren Behandlung und Verteilung.

- Vereinfachte Header-Formate (Header Format Simplification)
  Verschiedene Felder in Paketheadern sind entfallen oder optional und tragen zur Verkürzung und Beschleunigung von Datenübertragungen bei.
- Verbesserte Unterstützung von Erweiterungen und Optionen (Improved Support for Extensions and Options)
  Die veränderte Art der Kodierung von Erweiterungen und Optionen erlaubt eine flexiblere Handhabung der Vermittlungskomponenten (Router) und effektivere Weiterleitungsmechanismen („in Hardware“).
- Kennzeichnung von Datenströmen (Flow Labeling Capability)
  Das Protokoll unterstützt Methoden zur Behandlung von Verkehrsströmen (Traffic Flows) durch Kennzeichnung (Labeling) entsprechend zusammenhängender Datenpakete.
- Authentifizierung und Datenschutz (Authentication and Privacy Capabilities)
  IPv6 spezifiziert Erweiterungen zur Unterstützung von Sicherheitsmaßnahmen bzgl. Authentizität, Integrität und Vertraulichkeit.

Mit Version 6 wurde das IP-Protokoll von Grund auf neu verfasst. Sie stellt also kein Update des Vorgängers, sondern eher eine neue Ausgabe im Sinne eines „Major Release“ dar. Die beiden Versionen sind technisch komplett unabhängig voneinander und können bzw. müssen daher (bei entsprechenden Anforderungen) nur parallel zueinander betrieben werden.

Die neue Protokollversion 6 sollte im Laufe der Zeit Version 4 im Internet vollständig ablösen. Nachdem bereits ab 1999 die IP-Adressvergabe im Regelbetrieb erfolgte, ging die Verbreitung bzw. der Einsatz in realen Netzen nur sehr schleppend voran. Obwohl das Ende von IPv4 mehrmals prophezeit wurde, war (und ist) diese Version nur sehr schwer aus den Netzen zu verdrängen. Als Gründe hierfür sind die starke Verwurzelung in Netzkomponenten und Endgeräten (damit auch beim Management- und Benutzerpersonal) sowie verschiedene Modifikationen und Erweiterungen zur Beseitigung oder Minderung von Schwachstellen zu nennen. Auch die sich im Laufe der Zeit zuspitzende Problematik (nicht neu) verfügbarer IPv4-Adressen konnte etwa durch vermehrte Verwendung privater (nicht routebarer) Adressen (vgl. Teil 1, Kapitel 4.3.3) und Adressumsetzungen (NAT, vgl. Kapitel 6.2.3.3) an Netzübergängen weitgehend aufgefangen werden. Erst die Anforderungen an Adressräume für hinzukommende Regionen in Afrika oder Asien sorgten für einen kräftigen Motivationsschub zum Einsatz von IPv6.

Die Einführung von IPv6 im Internet bzw. von seinen verschiedenen Bestandteilen musste also schrittweise, unter Berücksichtigung bestehender Strukturen, d. h. in der Regel parallel zum vorhandenen IPv4 erfolgen. So startete das Deutsche Forschungsnetz (DFN) im Jahr 2000 nach einer vorangegangenen Testphase den Re-

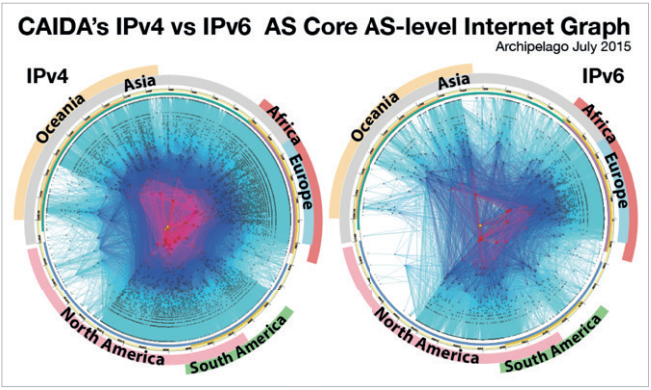
gelbetrieb von IPv6 und machte das Protokoll für entsprechende Netze und Systeme ergänzend verfügbar, ohne damit eine Ablösung von IPv4 gezielt anzustreben. Auch das RRZE konnte dadurch an der FAU erste Endsysteme mit IPv6 in eine im Aufbau befindliche, internationale Struktur einbinden. Markante Meilensteine zur Propagierung und Demonstration globaler Verfügbarkeit setzten der „World IPv6 Day“ am 8. Juni 2011 mit einem international verabredeten Feldtest und im darauffolgenden Jahr der „World IPv6 Launch Day“ am 6. Juni 2012. Dieser demonstrierte die Verbreitung und Funktionsfähigkeit des Protokolls zu diesem Zeitpunkt und kann als Startpunkt eines weltweiten Betriebes bezeichnet werden. Mehr als 400 Teilnehmer, darunter große Unternehmen wie Google, Yahoo, Facebook, YouTube, Microsoft, Cisco, Juniper, Huawei oder T-Online, aber auch zahlreiche kleinere Institutionen oder Hochschulen wie die FAU machten dabei mit. Das RRZE leistete zu beiden Ereignissen seinen Beitrag, indem es verschiedene Erlanger Systeme (u. a. einen Webserver) in die globale IPv6-Vernetzung einband und erreichbar machte. Diese Aktionen erhöhten zwar den Bekanntheitsgrad und die Bereitschaft zum Einsatz von IPv6, markierten aber mehr den Beginn eines langsam einsetzenden Migrationsprozesses, als den einer schnellen Ablösung von IPv4.

Das Nebeneinander der beiden Protokollversionen und somit eine „sanfte“ Einführung von IPv6 wurde durch Entwicklungen von Geräte- und Systemtechnik wesentlich unterstützt. Sowohl Netzkomponenten als auch viele Endgeräte (Workstations, Server) wurden in die Lage versetzt, beide Versionen parallel zu betreiben. Während es für Router generell nicht ungewöhnlich ist (war), verschiedene Netzprotokolle nebeneinander zu bedienen, stellt die Fähigkeit zur Bedienung zweier Protokolle in Endsystemen eine entsprechende Systemerweiterung zum „Dual-Stack-Betrieb“ dar. Auf einem solchen Rechner sind demnach zwei getrennte IP-Stacks implementiert, wobei die jeweilige Anwendung entscheidet, welche Version sie verwendet. Pro Stack bzw. Protokollversion sind dem Rechner dann auch spezifische Internetadressen zugeordnet. Dem Benutzer bleibt dies weitgehend verborgen, da in solchen Fällen der Nameservice (DNS) als Bindeglied dient und auf Anfrage beide Adressen ausliefert. Die Anwendung (bspw. ein Browser) wählt dann davon eine Adresse automatisch aus. Ohne Dual-Stack kann ein IPv4-Rechner jedenfalls nur IPv4-Ziele und ein IPv6-Rechner nur IPv6-Ziele erreichen (vgl. Abbildung möglicher „Kommunikationsbeziehungen ohne Dual-Stack“).

Quellsystem	Zielsystem	Ergebnis
IPv4	IPv4	OK
IPv4	IPv6	FAIL
IPv6	IPv4	FAIL
IPv6	IPv6	OK

Kommunikationsbeziehungen ohne Dual-Stack

Einen Eindruck über die Verteilung der beiden Protokollversionen vermitteln Darstellungen der Forschungseinrichtung „Center for Applied Internet Data Analysis“ (CAIDA) [*Caida*], die sich mit der Untersuchung und Visualisierung von Internettopologien befasst. So gibt die Gegenüberstellung für das Jahr 2015 bspw. Auskunft über die geografische Ausbreitung und Verbindungsstruktur von IPv4 und IPv6 (vgl. Abbildung „Internetausbau bzgl. IPv4 und IPv6“). Ohne auf Details der Darstellung näher einzugehen, deutet die farbliche Gestaltung der Grafik (durch Größe und Intensität der roten Bereiche) eine immer noch deutlich stärkere und dichtere Verteilung der Version 4 im Vergleich zu Version 6 an.



Internetausbau bzgl. IPv4 und IPv6, CAIDA 2015

Diese Unterschiede drücken sich auch in den Zahlen aus, die von CAIDA durch folgende Kenndaten angegeben werden:

Protokoll	IP-Adressen	Router-Verbindungen	Autonome Einzelnetze (AS)
IPv4	42.050.000	33.900.000	39.800
IPv6	71.400	168.600	5.300

Weltweite Zahlen zu IPv4 und IPv6, nach CAIDA 2015

Das Verhältnis der beiden Versionen zueinander hat sich auch in der Folgezeit kaum verschoben. Die Bedeutung und Nutzung von IPv6 nimmt zwar ständig zu (Zahlen nach 2015 wurden dazu von CAIDA (noch) nicht veröffentlicht), da aber auch das Wachstum von IPv4 weiter anhält (2017 wurden etwa 50 Millionen IPv4-Adressen verzeichnet), ist ein Abschluss des Migrationsprozesses bzw. eine vollständige Ablösung von IPv4 noch lange nicht abzusehen.

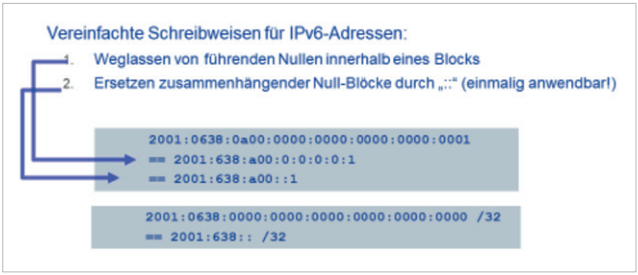
7.2.1.2 Adressierung

Wie schon erwähnt, besteht die gravierendste Änderung von IPv6 gegenüber IPv4 in der neu definierten Adressstruktur (vgl. RFCs 3513 und 4291), insbesondere aber in der enormen Erhöhung des verfügbaren Adressraums. Das betrifft vor allem die Länge der Adressen sowie zugehörige Regeln zu deren Notation. IPv6-Adressen sind 128 Bit lang und werden als eine Folge von 32 hexadezimalen Ziffern (entsprechen jeweils 4 Bit) beschrieben. In der Darstellung bilden zur besseren Übersicht jeweils vier Ziffern einen Block (entsprechend jeweils 16 Bit), wobei die Blöcke durch Doppelpunkte voneinander getrennt werden. So lautet eine typische Adresse eines Servers an der FAU:

2001:0638:a000:1022:0230:0000:0000:d76e

Unter Anwendung definierter Notationsregeln können die zum Teil sehr „unhandlichen" Adressen noch kompakter dargestellt werden (vgl. Abbildung „Notationsregeln zur Darstellung von IPv6-Adressen"). Für das angeführte Beispiel des FAU-Servers bedeutet die entsprechend verkürzte Schreibweise im Gegensatz zu der in der Abbildung angeführten allerdings kaum eine Vereinfachung:

2001:0638:a000:1022:0230::d76e



Notationsregeln zur Darstellung von IPv6-Adressen

Mit den 128 vorgesehenen Bits lassen sich theoretisch 2**128 (340 Sextillionen) Adressen bilden. Die Anzahl real verfügbarer (End-)Adressen wird allerdings durch Strukturierung und Vergabestrategie noch stark eingeschränkt, sollte aber für einen globalen IPv6-Betrieb dennoch „auf Dauer" ausreichend bemessen sein.

IPv6 unterscheidet noch differenzierter als IPv4 zwischen unterschiedlichen Adresstypen:

- Loopback-Adresse (::1 /128)
- Link-Local-Unicast-Adressen (fe80::/10)
- Unique-Local-Unicast-Adressen (fc00::/7), (private Adressen)

- Multicast-Adressen (fc00::/8)
- Global-Unicast-Adressen (2000::/3), (globale Adressen)

Die Angaben von „/nnn“ bezeichnen die Anzahl der den jeweiligen Bereich kennzeichnenden, fest definierten, führenden Bits. Diese Notation wird im folgenden Abschnitt mit der Strukturierung von Adressen näher erläutert.

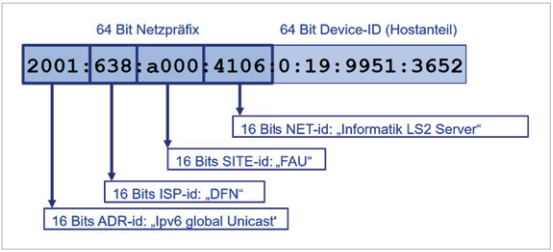
Neben den „nicht routebaren“, privaten Adressen, ist die Gruppe der „Global-Unicast-Adressen“ für die Zuordnung zu Endsystemen gedacht und daher von besonderem Interesse. Sie werden weiter unterteilt und nach festgelegten Konventionen vergeben. Ähnlich wie bei IPv4 haben auch die Global-Unicast-Adressen von IPv6 einen Netz- und einen Hostanteil. Während bei IPv4 diese Grenze durch die zugehörige Adressklasse („A“, „B“, „C“, „D“) oder eine ergänzende Subnetzmaske definiert ist (vgl. Teil 1, Kapitel 4.3.3.1), lässt IPv6 im Prinzip eine beliebige Aufteilung zu. Dabei wird der Netzanteil durch die Anzahl der zugehörigen Bits (gezählt vom Anfang der Adresse) angegeben. Gemäß allgemeingültiger Konvention hat diese Zahl in der Praxis stets den Wert 64. Danach ist eine IPv6-Adresse jeweils in 64 Bits für die Bestimmung des jeweiligen Endnutzersubnetzes und in 64 Bits zur Identifikation eines Hostsystems bzw. einer Geräteschnittstelle innerhalb des betreffenden Subnetzes aufgeteilt. Die Aufteilung einer Endsystemadresse aus dem RRZE und deren Notation ist in „Netz- und Hostanteil einer Serveradresse“ als Beispiel dargestellt.

Netz- und Hostanteil einer Serveradresse

Der Netzanteil einer Adresse ist im Kontext der zentralen Vergabe über die Institution Internet Assigned Numbers Authority (IANA) und ihr nachgeordneter Organisationseinheiten noch weiter untergliedert. Gemäß der entsprechenden Hierarchie ergeben sich daraus verschiedene Bereiche, die innerhalb einer Adresse wieder durch ihre Länge (gezählt vom Anfang der Adresse) gekennzeichnet werden. Eine derart spezifizierte Anfangssequenz einer Adresse bezeichnet man auch als „Präfix“. Die gebräuchlichsten Präfixe beziehen sich dabei auf Endanwendersubnetze (Länge 64), Organisationsnetze (Länge 48) oder Providernetze (Länge 32) (vgl. auch die Darstellung der „Präfixbereiche einer IPv6-Adresse“, S. 120).

Eine IPv6-Adresse ist also strukturiert aufgebaut. Die Untergliederung des Netzanteils wird über verschiedene Präfixe beschrieben und spiegelt die Hierarchie des Vergabevorganges bzw. die Zuständigkeit für zugehörige Adressräume wider. Am Beispiel der „Struktur einer Serveradresse“ aus dem RRZE erkennt man deren zentrale Ein-

ordnung als „Global-Unicast-Adresse“ (Präfixanteil 2001), den DFN-Verein als Internet Service Provider (ISP) (Präfixanteil 0638), dessen „Kunde“ RRZE/FAU (Präfixanteil a000) sowie die vom RRZE vorgenommene Zuordnung zu einem lokalen Subnetz der Universität (Präfixanteil 4106).



Struktur einer Serveradresse

In einem weiteren Beispiel zur Strukturierung einer IPv6-Adresse sind die „Präfixbereiche einer IPv6-Adresse“ mit Längenangaben und Bezeichnungen noch näher dargestellt. Die angeführte Adresse bezieht sich hier auf einen Arbeitsplatzrechner der Informatik 4 an der FAU. Wie auch im vorangegangenen Beispiel des RRZE-Servers gehört dieser Rechner in den (regional definierten) Bereich „Erlangen-Süd-Informatik“ der FAU. Beide Adressen haben daher bis zum 56sten Bit denselben Präfix (endend mit „41“) und unterscheiden sich dann in den Kennungen ihrer lokalen Netze, d. h. in den Werten „34“ (VLAN 34) bzw. „06“ (VLAN 6) im vierten hexadezimalen Ziffernblock.

Struktur der IPv6-Adresse (2001:0638:a000:4134::FF10:62) eines Arbeitsplatzrechners

2001::	/3	Adressblock Global Unicast Address
2001:600::	/23	Adressblock IANA – RIPE-NCC Delegation
2001:638::	/32	Präfix DFN-Verein
2001:638:a000::	/45	Delegation an RRZE
2001:638:a000::	/48	Präfix FAU-Wissenschaftsnetz (WiN)
2001:638:a000:4000:	/52	Präfix FAU-WiN Erl-Sued
2001:638:a000:4100:	/56	Präfix FAU-WiN Erl-Sued-Informatik
2001:638:a000:4134::	/64	Präfix FAU-WiN Erl-Sued-Informatik Vlan 34 (LS 4)
2001:638:a000:4134: 0000:0000:FF10:62	/128	Komplette IPv6-Adresse Letzter Teil vom IT-Betreuer / DNS-Admin vergeben

Präfixbereiche einer IPv6-Adresse

Nach dem gebräuchlichen Netzpräfix der Länge 64 stehen weitere 64 Bits zur (eindeutigen) Identifikation einzelner Endsysteme bzw. deren Schnittstellen zur Verfügung. Die Zahl der damit innerhalb (!) eines (Sub-)Netzes adressierbaren Endsysteme ist enorm hoch und scheint von einem verschwenderischen Umgang zu zeugen. Sie

macht es aber möglich, jedem Kunden weit ausreichende Adressräume zur Verfügung zu stellen und erlaubt „großzügige“, teils automatisierbare Vergabestrategien, etwa unter Einbeziehung physikalischer Adressen (bspw. Ethernet MAC-Adressen).

Für die Vergabe bzw. Zuordnung von IPv6-Adressen an Endsysteme gibt es verschiedene Methoden:

- Manuelle Adressvergabe
  Adressen werden von Systemadministratoren nach eigener Systematik vergeben. Dabei müssen sie auf Eindeutigkeit achten. Diese Methode wird vor allem bei der Festlegung von Adressen für zentrale Serversysteme angewendet.
- Dynamische Zuordnung über DHCPv6
  Adresszuweisungen erfolgen über einen spezifischen DHCPv6-Server (vgl. RFC 3319, 2003), entsprechend dem von IPv4 bekannten DHCP-Verfahren (Dynamic Host Configuration Protocol). Ein Endgerät (Client) schickt unter Angabe einer Identifikationskennung (DHCP Unique Identifier, DUID), die unter anderem die eigene MAC-Adresse sowie einen Zeitstempel enthält, per Multicast eine Anfrage an das Netz und erhält nach weiterem Informationsaustausch im positiven Fall dann eine Adresse zugeteilt. Der DHCP-Server vergibt die Adressen seinerseits an Hand statischer Konfiguration oder nach Bestimmung über automatische Verfahren (vgl. folgenden Punkt).
- Automatische Adressbestimmung (SLAAC)
  Unter Anwendung der Methode zur „IPv6 stateless address autoconfiguration“ (SLAAC, definiert in RFC 2462, 1998) kann sich ein Endgerät seine eigene IPv6-Adresse zusammenbauen. Dabei erhält es vom nahegelegenen Router (des betreffenden LANs) nach Anfrage oder per Multicast regelmäßig ausgesandte Informationen (Router-Advertisement) einen Netzpräfix der „Standardlänge 64“, eine Gateway-Adresse (Default-Route) und die Angabe einer Gültigkeitsdauer. Den Hostanteil leitet das System aus seiner (bzw. der des betreffenden Interfaces) MAC-Adresse ab, und zwar durch deren Umwandlung in eine EUI-64-Bit-Adresse (64-Bit Extended Unique Identifier). Dabei entsteht aus der 48-Bit langen Medienadresse durch Einfügen der Sequenz „ff:fe“ in der Mitte eine 64-Bit-Adresse, die zum Bestandteil der so bestimmten IPv6-Adresse wird. Das dargestellte Beispiel eines Rechners aus dem Bereich des RRZE lässt die „Automatische Adressbildung gemäß SLAAC“ nachvollziehen.

Automatische Adressbildung gemäß SLAAC

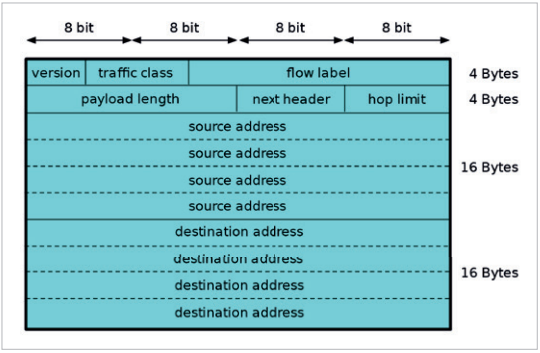
Das relativ einfache SLAAC-Verfahren zur automatischen Adressbestimmung führt zwar zu eindeutigen IPv6-Adressen und wird auch in den Endgeräten von den IPv6-fähigen Betriebssystemen meist unterstützt, erzeugt aber auch einen gewissen, unüberschaubaren „Wildwuchs“. Das RRZE verwendet daher in der Regel die administrativ im Rahmen des Netzmanagements steuerbaren Verfahren manueller Zuordnungen über „direkte“ Einstellungen in den Endsystemen oder „indirekt“ durch entsprechend kontrollierte Konfigurationen betriebener DHCPv6-Server.

7.2.1.3 Formale und funktionale Ergänzungen

Neben dem im Vergleich zu IPv4 grundlegend neuen Adressierungskonzept unterscheidet sich IPv6 noch in weiteren formalen und inhaltlichen Punkten von der Vorgängerversion. Das betrifft die im Folgenden skizzierten Aspekte.

Paketformat bzw. Aufbau des Kopfdatenbereichs (Header)

Wie bei Betrachtung der historischen Entwicklung von IPv6 bereits erwähnt (vgl. Kapitel 7.2.1.1) stellt der RFC 2460 die Vereinfachung des Paketformats bzw. der betreffenden Kopfinformation (des Headers) als besonderes Merkmal heraus. Im Gegensatz zu IPv4 haben diese eine feste Länge von 40 Bytes. Sie enthalten unter anderem die Größe des Nutzdatenbereichs (Payload Length) sowie Absender- (Source) und Zieladresse (Destination Address) des betreffenden Datenpakets. Optionale Informationen werden in Extension Header zwischen dem IPv6-Kopfdatenbereich und der eigentlichen Nutzlast ausgelagert und deren Position jeweils in einem „Next-Header“ -Feld spezifiziert. So können Optionen eingefügt werden, ohne dass sich der Header verändert. Zu den Informationen, die IPv6-Kopferweiterungen beinhalten können, zählen unter anderem



Kopfdatenbereich (Header) eines IPv6-Pakets

Knoten-zu-Knoten-Optionen, Zieloptionen, Routing-Optionen sowie Optionen zu Fragmentierung, Authentifikation und Verschlüsselung. Die einem Beitrag von Wikipedia entnommene Abbildung „Kopfdatenbereich (Header) eines IPv6-Pakets“ [WikI6] macht den generellen Aufbau eines Headers (ohne Erweiterungen) deutlich.

Lokale Hilfsadressen von Endsystemen

IPv6-fähige Endsysteme bzw. deren Betriebssysteme generieren in der Regel zu jedem ihrer Netzschnittstellen automatisch eine „verbindungslokale Adresse“ (Link-Local-Unicast-Address), die dem durch „fe80::/10“ spezifizierten Adressraum angehören und meist die MAC-Adresse des betreffenden Interfaces zur Gewährleistung von Eindeutigkeit enthalten. Diese Adressen sind unabhängig von Hostadressen des Systems und ohne deren Existenz verfügbar. Sie sind niemals Bestandteil „normaler“ Kommunikation und verlassen „ihr“ lokales Netz nicht. Ihre Verwendung finden sie bspw. in initialen Vorgängen, wie der automatischen Adressbestimmung über SLAAC (vgl. vorangegangener Abschnitt) oder im Protokoll zur Bestimmung lokaler Nachbarn (vgl. „NDP“ in folgendem Punkt).

Protokoll zur Nachbarschaftsbestimmung (NDP)

Das „Neighbor Discovery Protocol“ (NDP, 2007 beschrieben in RFC 4961) ersetzt unter anderem für IPv6 das „Address Resolution Protocol“ (ARP) von IPv4, indem es ebenso ermöglicht, IPv6-Adressen in Link-Layer-Adressen aufzulösen. Bezogen auf die lokale Umgebung unterstützt es Endsysteme bei der Bestimmung des nächsten Routers (Router Discovery), des dort gültigen Präfixes (Prefix Discovery) und der automatischen Adressbestimmung (SLAAC). Darüber hinaus erkennt das Protokoll die Nichterreichbarkeit von Nachbarn (Neighbor Unreachability Detection, NUD) oder doppelt verwendete Adressen (Duplicate Address Detection, DAD).

ICMPv6 (Internet Control Message Protocol)

Wie im Zusammenhang mit IPv4 (vgl. Teil 1, Kapitel 4.3.3.3) stellt das „Internet Control Message Protocol for the Internet Protocol Version 6“ (ICMPv6, 2006 beschrieben in RFC 4443) eine Ergänzung zum Protokoll der Netzschicht dar. Ebenso dient es zum Austausch von Fehler- und Informationsmeldungen und bietet darüber hinaus die Grundlage für die IPv6-spezifische Nachbarschaftsbestimmung per NDP. Natürlich ist es auch die Basis für Implementierungen bzw. Erweiterungen der von IPv4 bekannten Testhilfen wie Ping (Antwortzeitbestimmung) oder Traceroute (Wegeverfolgung von Paketen).

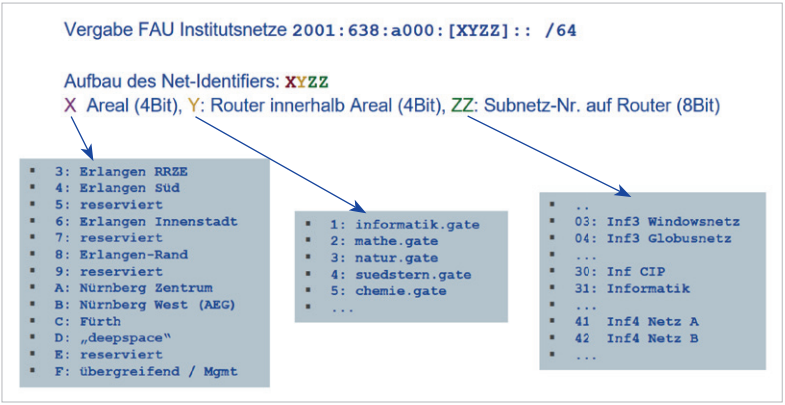
7.2.1.4 IPv6 an der FAU

Wie bereits erwähnt, hat sich das RRZE frühzeitig mit IPv6 befasst, am Testbetrieb des DFN teilgenommen, die internationalen Initiativen zum „World IPv6 Day“ und „World IPv6 Launch Day“ unterstützt sowie ab 2012 schließlich den Produktivbetrieb an der FAU schrittweise eingeführt. Danach wurden beide Protokollversionen auf derselben Netzstruktur aus Routern und LAN-Switchen nebeneinander betrieben und konnten von den Endsystemen alternativ oder im Dual-Stack-Betrieb (vgl. Kapitel 7.2.1.1) wahlweise genutzt werden. So entsprach in der Ausbauperspektive jedem v4-Netz ein paralleles v6-Netz.

Zur Zuteilung von IPv6-Adressen an Einrichtungen der Universität wurde der vom Provider DFN der FAU zugewiesene Bereich öffentlicher (Global-Unicast-)Adressen vom RRZE in einer ersten Hierarchiestufe grob untergliedert. Die Abbildung „Unterteilung des IPv6-Adressbereichs der FAU“ stellt dies dar.

Unterteilung des IPv6-Adressbereichs der FAU

Eine weitere Unterteilung des Bereichs FAU-Wissenschaftsnetz betrifft die an Institute der FAU vergebenen Netzadressen. Sie enthalten im vierten hexadezimalen Adressblock eine hierarchisch zusammengesetzte Netzkennung (Net-Identifier), in der die erste Ziffer (X) den (geografischen) Bereich (Areal), die zweite Ziffer (Y) einen Router und die weiteren beiden Ziffern (ZZ) das betreffende Subnetz bzw. VILAN spezifizieren. Die Abbildung auf S. 125 zum „Adressenaufbau von FAU-Institutsnetzen“ lässt das Verfahren nachvollziehen, wobei das durch Pfeile markierte Beispiel die Zusammensetzung der Adresse für das IPv6-Subnetz des Informatik-CIP-Pools im Hochhaus/Südgelände wiedergibt. Die so ermittelte Netzadresse lautet schließlich „2001:638:a000:4130::/64“.



Adressenaufbau von FAU-Institutsnetzen

Wie bereits beschrieben (vgl. Abschnitt 7.3.1.2), erfolgt die Zuordnung des Hostadressanteils im Kontext der FAU weitgehend administrativ, d. h. ohne Verwendung des unübersichtlichen automatischen Verfahrens (SLAAC).

Der Ausbau des IPv6-Netzes wurde vom RRZE zügig vorangetrieben, sodass das Protokoll inzwischen nahezu flächendeckend an der FAU verfügbar ist. Dabei wurden auch verschiedene Dienste zur Betriebsunterstützung spezifisch angepasst wie der Nameservice (DNS), die automatische (Host-)Adresszuordnung (DHCP), verschiedene Maildienste oder auch verschiedene Schutzeinrichtungen (ACLs, vgl. Kapitel 7.6.4).

Die Nutzung von IPv6 ist seit der Einführung an der FAU im Jahr 2012 stetig gestiegen, erreichte aber bei Weitem noch nicht das Maß von IPv4. So betrug 2017 der Datenverkehr an der externen Schnittstelle zum Internet (DFN) von IPv6 im Vergleich zu IPv4 etwa 10%, während er intern im Erlanger Süden mit etwas mehr als 5% noch darunterlag. Trotz wachsender Beliebtheit und steigender Tendenz ist ein Verdrängen bzw. das Ende von IPv4 auch an der FAU noch nicht abzusehen.

7.2.2 Neue Generation von Netzkomponenten

Die in Kapitel 6 angeführten, an der FAU eingesetzten Netzkomponenten konnten den beschriebenen Entwicklungen der Kommunikationstechnik weitgehend folgen. Das betraf die Unterstützung von IPv6, aber auch Möglichkeiten zur Datenübertragung mit „hohen" Geschwindigkeiten von 1 oder 10 Gbp/s. Allerdings konnten sie steigende, speziell gestellte Anforderungen, wie etwa im Zusammenhang mit der Vernetzung

zentraler Server und deren Bereitstellung entsprechender Dienste, mit der Zeit nur noch bedingt erfüllen. Besonders für dieses Anwendungsfeld im Zusammenhang mit Serverzentralen (Datacenter) entwickelten die Hersteller Geräte einer neuen Generation, so bspw. Cisco (Serie Nexus 7000), Hewlett Packard (Modellserien 10500, 5412zl) oder Juniper (Modellserien QFX5100, EX4300).

Für das RRZE gab es immer gute Gründe, speziell für das Routing durchgehend Geräte eines Herstellers, nämlich von Cisco, einzusetzen. Neben positiven Erfahrungen spielten die Einbettung in die jeweils vorhandene Infrastruktur, einheitliche Bedienschnittstellen, spezifisches Gerätemanagement, Ersatzteilhaltung oder der Betreuungsaufwand im Hinblick auf knapp vorhandenes Personal eine Rolle. So fiel die Wahl zur Einführung von Geräten einer neuen Generation für künftige Anwendungsspektren nach gründlicher Analyse auch auf Komponenten des Herstellers Cisco, d. h. seiner Gerätefamilie Nexus.

7.2.2.1 Cisco-Gerätefamilie Nexus

Die Geräte Cat6500 von Cisco (vgl. Kapitel 6.2.3.4) befanden sich über viele Jahre im oberen Leistungsspektrum von Router- und LAN-Switch-Komponenten. Diese Position konnte durch verschiedene Maßnahmen (Upgrades) auch lange gehalten werden. So konnten mit diesen Gerätetypen z.B. im Core des Universitätsnetzes durch Einsatz entsprechender Module Verbindungen von 10 Gbit/s realisiert werden. Auch für darüberliegende Geschwindigkeiten (bis 40 Gbit/s) entwickelte der Hersteller Interfacemodule, die aber an bestimmte Ausprägungen des Grundgerätes (E-Typ Chassis, Supervisor-Version) gebunden und bzgl. der Zusammensetzung verfügbarer Anschlüsse nicht sehr flexibel waren (alternative Ausstattung mit 4 x 40 Gbit/s oder 8 x 10 Gbit/s Ports). Damit waren die Möglichkeiten der inneren Architektur ziemlich ausgereizt und die Geräte für besondere Anforderungen, bspw. mit noch mehr Anschlüssen für die hohen Geschwindigkeiten, nur noch bedingt einsatzfähig. Cisco entwickelte daher nebenher eine neue Gerätefamilie „Nexus“, die insbesondere zum Aufbau und zur Strukturierung von Serverzentren geeignet sein und entsprechende Anforderungen erfüllen sollte.

Nexus 7000

An der Spitze dieser „next generation of switch platforms“ steht die Serie „Nexus 7000“. Cisco bezeichnet die Geräte als „Switche“, da sich damit die innere Grundfunktion der geschalteten Weiterleitung von Datenströmen benennen lässt. Natürlich enthalten die Komponenten über ihre Systemsoftware „NX-OS“ auch die Funktionalitäten sowohl von LAN-Switchen als auch IP-Routern. Sie sind in Datacenterstrukturen zur Hauptverteilung und Außenverbindung gedacht.

Die Geräte sind modular aufgebaut. Die Gehäuse enthalten je nach Größe eine bestimmte Anzahl von Einschubplätzen (Slots), die bspw. mit zentralen Prozessorboards (Supervisor) oder Schnittstellenmodulen flexibel bestückt werden können. Die Schnittstellen können Anschlüsse der Geschwindigkeiten 1/10/40/100 Gbp/s enthalten. Zur Erhöhung der Zuverlässigkeit können Supervisor-, Switching-Module (Fabric Modules), aber auch Stromversorgungen und Lüfter zweifach, d. h. in Redundanz eingesetzt werden.

Am RRZE sind die Geräte im Datacenter wie folgt zusammengesetzt:

- Grundgerät Nexus 7010 mit 10 Slots
- 2 x Supervisormodul
- 2 x Fabricmodul
- 1 x Schnittstellenmodul mit 48 Ports, wahlweise mit 1 oder 10 Gbp/s betreibbar
- 1 x Schnittstellenmodul mit 24 Ports, wahlweise mit 10 oder 40 Gbp/s betreibbar
- 2 x Stromversorgung
- 2 x Lüfter

Die Leistungsfähigkeit des Nexus 7010 wird von Cisco mit einem maximal erzielbaren Gesamtdurchsatz von 17 Tbp/s (terabits per second) beschrieben. Als weitere Kenndaten gibt der Hersteller an:

- 600 Gbp/s, „Max local switching capacity“,
  Maximale Vermittlungsleistung innerhalb von Modulen
- 550 Gbp/s, „Max inter-slot switching capacity“,
  Maximale Vermittlungsleistung zwischen verschiedenen Modulen
- 5.76 bpp/s, „billion packets per second (IPv4 unicast)“,
  Maximaler Durchsatz von IP-Paketen

Zur Illustration zeigt die Abbildung „Cisco Nexus 7000 Series Switches“ aus einem Datenblatt des Herstellers Geräte in verschiedenen Größen [*CiNex*].

Cisco Nexus 7000 Series Switches, Data Sheet 2018

Nexus 5000

Die Geräte der Serie Nexus 5000 sind als „10-Gbp/s-Switche“ speziell für den Einsatz in Serverzentren zur Verteilung oder zum Anschluss von Endgeräten geeignet. Dafür sprechen u. a. ihre geringen Verzögerungszeiten (Low Latency von 1 Mikrosekunde), ihre hohen verfügbaren Anschlussgeschwindigkeiten (1, 10 oder auch 40 Gbp/s) sowie die Anzahl möglicher Schnittstellen (bis 96). Die Serie enthält verschiedene Plattformen (Nexus 5500, 5600) mit mehreren Grundmodellen, die wiederum mit entsprechenden Modulen jeweils flexibel für ihren Einsatzzweck zusammengestellt werden können. Am RRZE kamen bspw. Modelle Nexus 5020 zum Einsatz, die 40 mit 10 Gbit/s (40 x 10 GE) betreibbare Glasfaserschnittstellen enthielten.

Die Geräte werden mit der Software NX_OS betrieben und könnten auch als Router eingesetzt werden. Eine Besonderheit bildet die Möglichkeit der Auslagerung von Schnittstellenmodulen zur Erhöhung der Anschlusskapazität und zur Platzierung in räumlicher Nähe von Endgeräten. Mit Hilfe der „Cisco Fabric Extender“-Technologie (FEX Technology) werden entsprechende Module über Kupfer- oder Glasfaserkabel mit dem Grundgerät verbunden und in dessen innere Architektur (Switching Fabric) so eingebunden, als wären sie direkt im Gehäuse eingeschobene Module. Ein derartiges, proprietäres Konstrukt aus einen Grundgerät und mehreren externen Modulen verhält sich bzgl. des Managements wie ein großes, umfassendes Gerät und kann etwa als Alternative zu einer konventionellen LAN-Switch-Struktur aus einem Verteilswitch und daran angeschlossenen Endgeräteswitchen eingesetzt werden. Mit der FEX-Architektur können bis zu 2.304 Ports innerhalb eines Gebildes unterstützt werden.

Die externen Schnittstellenmodule sind jeweils in eigenen Gehäusen untergebracht und gehören bei Cisco zur Gerätefamilie Nexus 2000.

Nexus 2000

Die Geräte der Nexus 2000 Serie sind als ausgelagerte Erweiterungen (FEX) der Familien Nexus 5000, 6000 oder 7000 konzipiert und zur Bereitstellung von Endgeräteschnittstellen gedacht. Sie funktionieren nicht als Einzelgeräte, sondern werden mit einem übergeordneten Switch verbunden, den sie in ihrem eigenen Gehäuse als „Remote Linecard“ entsprechend erweitern. Die Verbindungen können je nach Erfordernissen und Gegebenheiten mit entsprechenden Anpassungen (Transceiver) über Kupfer- oder Glasfaserkabel hergestellt werden. In der Kombination mit ihrem „Muttergerät“ bilden sie ein sogenanntes verteiltes System (Distributed Modular System) mit entsprechenden Vorteilen aufeinander abgestimmter Mechanismen, aber auch den Nachteilen geschlossener, herstellerspezifischer Lösungen.

Bei der Einrichtung des Datacenters des RRZE kamen die Varianten Nexus 2232 mit 32 x 10 GE (Glas) und Nexus 2249 mit 48 x 1 GE (TP, Kupfer) zum Einsatz.

7.2.2.2 Neugestaltung Serverzentrum (Datacenter)

Die Server des RRZE, die viele IT-Dienstleistungen für die Universität von zentraler Stelle aus erbringen, wurden im ehemaligen, oft auch als „Bunker“ bezeichneten Aufstellungsraum des Großrechners TR440 aus den Anfängen des Rechenzentrums untergebracht (vgl. Teil 1, Kapitel 1). Dabei trat an die Stelle des einen Großrechners eine Vielzahl einzelner Rechnersysteme, deren Elemente in verschiedenen Regalen (Serverschränken) untergebracht wurden (Rackaufbau). Die Vernetzung der Server erfolgte über eine (redundante) Baumstruktur aus Router und LAN-Switchen (vgl. Abbildung „Redundante Switch-Struktur im Rechenzentrum, 2009“, Kapitel 6.3.2.3). Diese Struktur bildete den Distribution-Bereich des Rechenzentrums und versorgte entsprechend nicht nur die Server, sondern auch andere Endsysteme innerhalb des Rechenzentrumgebäudes. Zudem waren Server und Mitarbeiterstationen auf logischer Ebene in dasselbe VLAN bzw. IP-Subnetz eingeordnet. Die Anschlüsse der Server wurden mit maximal 1 Gbp/s betrieben.

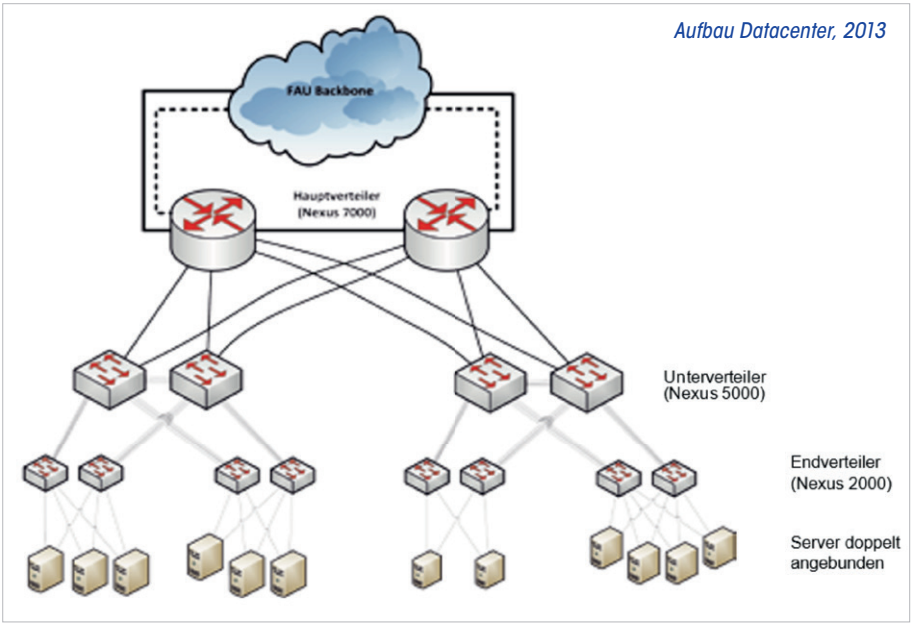
Mit einer wachsenden Zahl von Servern, kritischen Diensten sowie steigendem Nutzungsbedarf entsprach diese Konstruktion immer weniger den gestellten Anforderungen und musste daher umstrukturiert und technisch neu gestaltet werden.

Dies beinhaltete

- Trennung von Server- und Mitarbeiternetzen (bzgl. VLANs und IP-Subnetzen)
- Einrichtung eines dedizierten Distributionsbereichs mit eigener Core-Anbindung und eigenen Access-Komponenten
- Physischer Aufbau gemäß den Vorgaben der Regalstruktur und Serververteilung
- Logischer Aufbau einer baumförmigen, redundanten Netzstruktur (bzgl. der Zusammenschaltung von Komponenten)
- Einsatz leistungsfähiger Komponenten auf technisch aktuellem Stand, einschließlich Übertragungsgeschwindigkeiten von 10 Gbp/s und höher in ausreichender Zahl
- Einsatz der Gerätefamilie Nexus von Cisco
- Nutzung proprietärer Möglichkeiten bzgl. Redundanzen und deren Steuerung

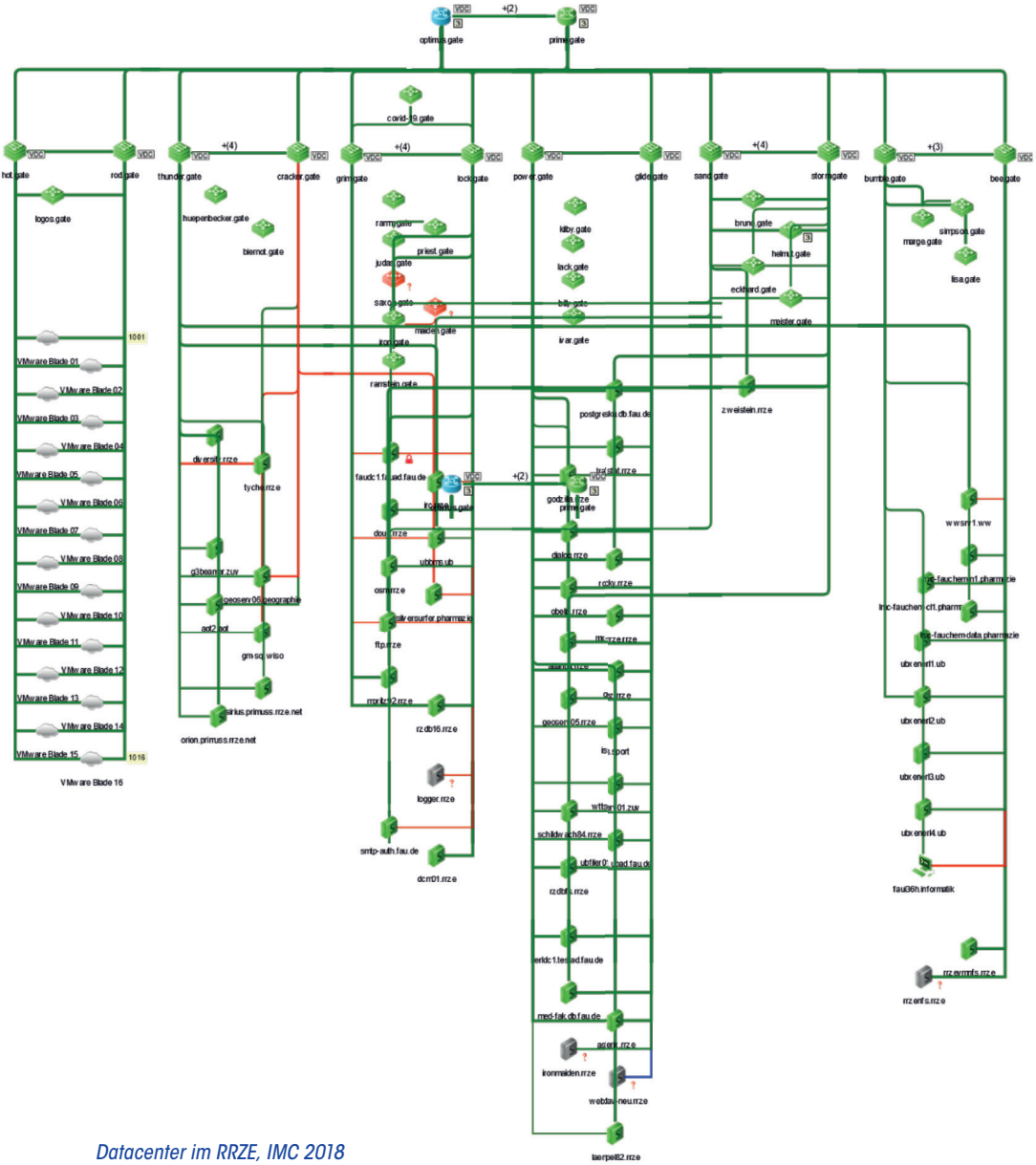
Die Skizze zum „Aufbau Datacenter“ stellt dessen neu konzipierte Struktur schematisch dar. Die Wurzel des (doppelten) Baums bildet als „Hauptverteiler“ des Bereichs ein Paar Nexus-7000-Router, das das Datacenter über ein redundant ausgeführtes Paar von 2 x 10-Gbit-Leitungen mit dem FAU-Kernbackbone verbindet. Beide Leitungen sind in Richtung Backbone gleichzeitig aktiv (sogenanntes „ECMP“-Routing) und können bei Ausfall des Partners den Gesamtverkehr übernehmen.

An die Hauptverteilung angeschlossen sind die „Unterverteiler“, zuständig für jeweils eine Serverschrankreihe. Die Versorgung einer Schrankreihe übernimmt dabei jeweils ein Paar Nexus-5000-Switche. Jedes dieser Geräte ist für sich mit jeweils einer



10-Gbit-Leitung an jeden der beiden Hauptverteiler angeschlossen. Insgesamt verfügt jede Rackreihe über einen Uplink von vier Leitungen mit jeweils 10 Gbit/s. Da auch hier wiederum unter Nutzung proprietärer Redundanzmechanismen alle Leitungen gleichzeitig aktiv sind, ergibt sich eine aggregierte Bandbreite von 40 Gbit/s für jede Rackreihe. Durch Hinzuschalten weiterer Leitungen lässt sich die Gesamtkapazität Richtung Hauptverteiler noch weiter ausbauen. Das Erkennen von Störungen und entsprechende Umschalten bewegt sich im Bereich von Millisekunden und ist somit kaum wahrnehmbar und deutlich kürzer als etwa die 20 Sekunden vergleichbarer Vorgänge unter Einsatz des (allerdings herstellerunabhängigen) Spanning Tree Protocols (vgl. Kapitel 6.3.2.).

Die unterste Hierarchie der Struktur, mit den Unterverteilern verbunden, bilden die „Endverteiler“ Nexus 2000, die in den Rackreihen nahe den Endgeräten aufgestellt sind. Sie sind mit mehrfachen 10-Gbit-Leitungen an die Unterverteiler ihrer jeweiligen Reihe angeschlossen und stellen die Anschlüsse für die Server bereit. Diese sind jeweils mit zwei Netzwerkschnittstellen von 1 oder auch 10 Gbit/s mit einem Paar Nexus 2000 so redundant verknüpft, dass der Ausfall einer Verbindung oder eines Switches automatisch kompensiert werden kann. Auch hier sorgt der Mechanismus von Nexus in Zusammenarbeit mit den Servern für Umschaltzeiten im Bereich von Millisekunden.



Datacenter im RRZE, IMC 2018

Einen Eindruck über den konkreten Aufbau des Datacenters im Serverraum vermittelt auf S. 131 die Abbildung „Datacenter im RRZE“ des Managementsystems IMC aus dem Jahr 2018. Sie lässt aufgrund der Auflösung zwar keine Details erkennen, macht aber die Hierarchie von Hauptverteilern (oberer Bildrand), Unterverteilern (Zeile darunter) und der Endverteiler mit ihrer Aufteilung auf verschiedene, senkrecht in Spalten angeordnete Rackreihen nachvollziehbar. Es sei noch bemerkt, dass die Darstellung auch Geräte enthält, die sich zwar in die Struktur einfügen, aber nicht zur Nexus-Familie gehören.

Die Struktur des Datacenters wurde durch das Konzept eines eigenen Distributionsbereichs und der Gestaltung mit Komponenten einer neuen Gerätegeneration zuverlässiger, leistungsstärker, effektiver und für künftige Anforderungen gerüstet (bspw. bzgl. Übertragungen von 100 Gbp/s).

7.3 Netzbetrieb

Über Planung, Auf- und Ausbau des Kommunikationsnetzes der FAU hinaus sind verschiedene Regelungen, Tätigkeiten und Vorkehrungen zur Gewährleistung eines stabilen, zuverlässigen Betriebs erforderlich und fallen in den Aufgabenbereich des RRZE bzw. seiner Abteilung Kommunikationssysteme (vgl. Kapitel 7.1.1). Dies betrifft z. B. Festlegung von Vorgaben und Zuständigkeiten im Rahmen eines Betriebskonzepts, Überwachung des laufenden Betriebs und Fehlerbehandlung oder Maßnahmen zur Erhöhung von Datensicherheit.

7.3.1 Betreuungs-/Betriebskonzept

In einer Institution von der Größe und Komplexität der FAU erfordern Bereitstellung und Betrieb einer Kommunikationsinfrastruktur übergreifende Konzepte zu deren Betriebsführung und Nutzung. Insbesondere sind an Universitäten Zuständigkeiten und Aufgabenverteilung zwischen zentraler Institution (Rechenzentrum) und dezentralen Einrichtungen (Instituten, Forschungsgruppen) zu definieren sowie Regelungen zur ordnungsgemäßen Nutzung zu treffen. Dabei sind entsprechende Festlegungen in übergreifende Vorgaben der generellen IT-Versorgung einzugliedern und gelegentlich an veränderte Rahmenbedingungen anzupassen.

7.3.2 Aufgabenverteilung, Verantwortungsbereiche

Auf die ursprünglich zentrale DV-Versorgung der Universität (bzw. erster Nutzergruppen) durch das Rechenzentrum folgten ebenfalls zentral betreute Strukturen für Remote-Zugriffe per Datenfernübertragung (DFÜ) sowie einer protokollgesteuerten regionalen Vernetzung (X.25) (vgl. Teil 1, Kapitel 1, 2, 3). Auch die jeweils angeschlossenen Endgeräte, in der Regel „einfache“ Dialoggeräte oder Druckerstationen (RJEs), wurden zunächst überwiegend vom RRZE zentral bereitgestellt und betrieben. Das Aufkommen dezentral verfügbarer Rechnerkapazitäten (z. B. PCs, Arbeitsplatzsysteme) sowie die Einführung lokaler Netze (LANs) und des Internetprotokolls im Kommunikationsbereich (vgl. Teil 1, Kapitel 4) stieß Überlegungen zur Neuordnung der Aufgabenteilung zwischen zentralen und dezentralen Einrichtungen an und führte zum Konzept der DFG einer kooperativen DV-Versorgung von Hochschulen. Bezogen auf die Kommunikationsstruktur waren nach dessen Umsetzung an der FAU das RRZE für den Betrieb des standortübergreifenden Backbones zuständig und die Institute für ihre jeweiligen Netzbereiche eigenverantwortlich (vgl. Teil 1, Kapitel 4.6). Eine ähnliche Unterscheidung erfolgte auch zwischen dem Betrieb zentraler Server und Dienste (RRZE) sowie lokal betreuten Systemen (Institute).

Mit zunehmender Ausweitung und Komplexität der IT-Technik allgemein und der Kommunikationstechnik im Besonderen wurde diese Aufteilung immer problematischer. So führte im Netzbereich die Betreuung von Einheiten durch lokales Personal der Institute häufig zu Fehlern, die sich nicht nur lokal auswirkten und vom zentralen Personal schwierig zu orten und zu beheben waren. Als Beispiele sind hier Fehlkonfigurationen, Schleifenbildungen, mangelnde Dokumentationen oder der Einsatz inkompatibler Geräte zu nennen. Die Behebung von Störungen, die Nutzer verursachten, zeigte sich meist aufwendiger als eine generell zentral organisierte Betreuung.

Zur Gewährleistung eines effektiven und möglichst stabilen Betriebs hat das RRZE daher die komplette Betreuung des Kommunikationsnetzes übernommen. Neben der Zuständigkeit für Gestaltung und Betrieb des Backbones (Core, Distribution) ist damit auch die zentrale Verantwortung für die verteilten Anschlussbereiche der Endgeräte (Access) verbunden. Wie schon generell definiert, deckt die zentrale Verantwortlichkeit inhaltlich die unteren drei Schichten des ISO-Modells ab (charakterisiert durch Verkabelung, Ethernet-LANs, IP-Routing) und bezieht verschiedene Netzdienste (z. B. DNS, DHCP, NAT) mit ein. Dieses etwas veränderte kooperative Modell sieht ebenso lokale Betreuer in den dezentralen Einrichtungen (Instituten) vor, die sowohl für den jeweiligen Bereich als Kontaktpersonen zum RRZE fungieren als auch die Benutzer vor Ort betreuen und z. B. in Abstimmung mit dem RRZE Endgeräte an das Netz anschließen.

Die genannte, grundsätzliche Aufgabenverteilung zwischen der zentralen Organisationseinheit (RRZE) und den dezentralen Organisationseinheiten der Universität ist in spezifischen „Richtlinien für die Nutzung des FAU-Datennetzes“ konkretisiert [*FauRd*]. Ihnen sind folgende Punkte entnommen:

Verantwortungsbereich des RRZE

- Das RRZE ist zuständig für Ausbau und Pflege der flächendeckenden drahtgebundenen sowie drahtlosen Infrastruktur und Netzwerktechnik des Datennetzes, insbesondere für Planung, Mittelbeantragung, Beschaffung, Installation, Konfiguration und laufende Betreuung. Dies erfolgt in enger Abstimmung mit dem Universitätsbauamt sowie den betroffenen Institutionen.
- Das RRZE sorgt im Rahmen gegebener Möglichkeiten für eine auf die Standorte der FAU bezogene, flächendeckende, möglichst homogene Netzinfrastruktur.
- Verknüpfungen mit oder Zugänge zu anderen (externen) Datennetzen werden ausschließlich vom RRZE konzeptioniert.
- Das RRZE sorgt durch Überwachung und Fehlerbehandlung für einen möglichst stabilen und sicheren Netzbetrieb.
- Dem RRZE obliegt der alleinige Betrieb aller grundlegenden netzbezogenen Dienste.

Verantwortungsbereich der FAU-Organisationseinheiten

Die FAU-Organisationseinheiten sind zuständig für den Anschluss von IT-Endgeräten:

- Die Leitung einer FAU-Organisationseinheit benennt gegenüber dem RRZE einen oder mehrere IT-Betreuer. Die IT-Betreuer halten Kontakt zum RRZE, informieren sich über aktuelle Entwicklungen und teilen ihrerseits dem RRZE Nutzungsänderungen und organisatorische Veränderungen mit.
- Anschlüsse an das Datennetz erfolgen nur über die vom RRZE bereitgestellten Netzzugangspunkte (ab Endgeräte-Anschlussdose mittels Netzwerkkabel oder ab Access Point mittels Funkverbindung).
- Anschlüsse an Endgeräte-Anschlussdosen koordinieren die IT-Betreuer in Kooperation mit dem RRZE.
- Die IT-Betreuer sind dafür verantwortlich, dass nur ordnungsgemäß gepflegte Endgeräte an das Datennetz angeschlossen sind.

Ergänzend enthalten die Richtlinien Verfahrensweisen zum Anschluss von Endgeräten, zur Behandlung von Störungen oder Betriebsbeeinträchtigungen und weisen auf folgende übergeordnet geltende Bestimmungen und Regelungen hin:

- Die IT-Satzung der FAU
- Die Benutzungsordnung des DFN für das Zusammenwirken der Anwender der DFN-Kommunikationsdienste [*DfnBo*]
- DFG-Richtlinien
- Gesetzliche Regelungen

Darüber hinaus ordnen sich die Regelungen zur Nutzung des FAU-Datennetzes in die allgemeinen IT-Benutzungsrichtlinien der FAU ein [*FauRb*]. Diese definieren den berechtigten Benutzerkreis, formale Benutzungsbedingungen, allgemeine Pflichten der Benutzer und Aufgaben der Systembetreiber.

Alle genannten Regelungen unterliegen gelegentlichen Überprüfungen und werden in den dafür zuständigen Gremien gegebenenfalls aktuellen Entwicklungen angepasst. Ihr jeweils gültiger Stand ist zum Beispiel auf den Webseiten des RRZE öffentlich einsehbar.

7.4 Netzwerkmanagement (Grundbegriffe, Methoden, Anwendungen)

Einrichtung, Betrieb und Betreuung eines IT-Kommunikationsnetzes erfordern vielfältige Tätigkeiten eines Netzwerkmanagements. Es umfasst etwa die Punkte Planung, Beschaffung, Auf- und Ausbau, Dokumentation, Zustandsüberwachung, Fehleranalyse, Fehlerbehebung ist aber damit bei Weitem noch nicht vollständig beschrieben. Die damit verbundenen, umfangreichen Tätigkeiten sind von handelnden Personen (Netzwerkmanagern) auszuführen und enthalten die Bedienung einzelner Geräte ebenso wie den Einsatz spezifischer Werkzeuge, die zur Unterstützung erforderlich sind. Diese reichen von speziellen Geräten (z. B. Messgeräte, Datenmonitore) über dedizierte Programme zur Lösung einzelner Aufgaben (z. B. Generierung von Konfigurationsdateien) bis zu universellen Managementsystemen zur Zustandsüberwachung und Darstellung des betreffenden Netzwerks.

In diesem Sinne stellen sich auch dem RRZE als Betreiber des Kommunikationsnetzes der FAU die Aufgaben eines Netzwerkmanagements, dessen umfangreiche Anforderungen im Kontext der Universität zu erfüllen sind.

7.4.1 Allgemeine Grundlagen

Zu den Grundlagen des Netzwerkmanagements gehören eine nach ISO genormte allgemeine Begriffsbildung und Gliederung der dazugehörenden Aufgaben sowie eine spezielle Betrachtung der Tätigkeiten, die für einzelne Komponenten im Laufe ihres Einsatzes zu erledigen sind.

7.4.1.1 Aufgabenfelder nach ISO

Die Internationale Normungsorganisation (ISO), die unter anderem das generelle Schichtenmodell zur Kommunikation verteilter Systeme entworfen hat (ISO-Referenzmodell), betrachtet das Netzwerkmanagement vorrangig unter dem kommunikationstechnischen Aspekt von Programm- und Protokollunterstützung und beschreibt dazu ein Modell (FCAPS), das die Aufgaben in die folgenden fünf Funktionsbereiche gliedert:

Fault Management/Fehlermanagement (Statusüberwachung, Problemhinweise)
Configuration Management/Konfigurationsmanagement (Verwaltung, Anpassung)
Accounting Management/Abrechnungsmanagement (Statistik)
Performance Management/Leistungsmanagement (Durchsatz, Antwortzeiten)
Security Management/Sicherheitsmanagement (Risikoerkennung, Absicherung)

Diese Einteilung gibt eine grobe Orientierung, allerdings sind in der Praxis verschiedene Maßnahmen oder Hilfsmittel nicht immer eindeutig bestimmten Aufgaben zuzuordnen.

7.4.1.2 Arbeitsschritte des Gerätemanagements

Bezieht man die Managementtätigkeiten auf einzelne aktive Netzwerkkomponenten, so kann man diese in verschiedene Entwicklungsschritte einteilen, die zum Teil nur manuell ausgeführt werden können, teilweise aber auch nahezu voll automatisierbar sind. Die Phasen lassen sich wie folgt benennen:

1. Erstkonfiguration/Grundkonfiguration vom „factory default“ zur lokalen Anpassung
2. Installation/Mechanischer Einbau, Verbindung mit anderen Komponenten
3. Funktionale Konfiguration/Konfiguration im Sinne des Verwendungszwecks
4. Inbetriebnahme/Volle Eingliederung in das Netzwerk, Übernahme seiner Aufgaben
5. Überwachung (Prüfung von Betriebsstatus, Funktionsbereitschaft, Statistik)
6. Fehleranalyse, -behebung (Reparatur, Austausch)
7. Konfigurationsänderungen/Anpassen an veränderte Anforderungen
8. Systempflege/Versionsupdate

Während Erstkonfiguration (1), Installation (2) und bestimmte Fehlerbehandlungen (6, Gerätetausch) eine direkte Handhabung der Geräte und personellen Einsatz vor Ort erfordern, können die anderen Punkte je nach Vorgehensweise und gegebenen Voraussetzungen zum großen Teil auch durch indirekten Kontakt über ein Netzwerk (remote) ausgeführt werden.

7.4.1.3 Praktische Umsetzung

Der Betreiber eines Kommunikationsnetzes hat also in der Praxis die beschriebenen Managementaufgaben zu lösen und die gestellten Aufgaben im konkreten Umfeld zu bewältigen. Das betrifft die Bedienung einzelner Komponenten ebenso wie die Gestaltung und Überwachung des Gesamtgebildes. Die anstehenden Tätigkeiten erfolgen nach verschiedenen, grundlegenden Methoden und werden von vielfältigen Hilfsmitteln unterstützt (vgl. Kapitel 7.4.2). Neben den elementaren „Standardwerkzeugen“ gehören dazu unter anderem für spezielle Aufgaben entwickelte Programme (bspw. zur Dialogunterstützung oder zur Konfigurierung von Routern), universelle Managementsysteme zum Abdecken möglichst vieler Funktionsbereiche gemäß FCAPS (vgl. NMS3000, IMC) oder auch dedizierte Testgeräte, etwa zum Aufzeichnen, Erfassen und Analysieren von Kommunikationsvorgängen (Daten-Analyzer). Allerdings sind derartige Werkzeuge ihrerseits oft komplex und erfordern spezielle Kenntnisse sowie nicht zu vernachlässigenden Aufwand bzgl. Pflege und Anpassung an die jeweilige Einsatzumgebung. (Kapitel 7.4.3 geht auf verschiedene, am RRZE eingesetzte Hilfsmittel näher ein.)

Um ein Netzmanagement zentral zu organisieren, ist zu klären, wie bzw. auf welchen Wegen Verbindungen zwischen Manager (Person oder System) und den zu bedie-

nenden Komponenten hergestellt werden sollen. Entsprechende Lösungsansätze verwenden für derartiges Remote Management das jeweilige Betriebsnetz (inline) oder eine davon unabhängige eigene Struktur (out-of-band) (vgl. Kapitel 7.4.4). Das RRZE praktiziert zum Management des FAU-Netzes beide Varianten (vgl. Kapitel 7.4.5).

7.4.2 Grundlegende Methoden, Bausteine des Komponentenmanagements

Den wesentlichen Bestandteil eines Kommunikationsnetzes bilden seine aktiven Komponenten, die mit Hilfe passiver Elemente (Verkabelungsstruktur) zu einem Netzwerk verknüpft sind. Die Behandlung dieser einzelnen Geräte ist somit wesentlicher Bestandteil des umfassenden Netzwerkmanagements. Die Geräte stellen dazu in der Regel verschiedene Schnittstellen bereit, über die sie z. B. konfiguriert oder abgefragt werden können. Die Bedienungen und Kontaktaufnahmen der Geräte erfolgen nach verschiedenen Methoden und sind jeweils an mehr oder weniger einfache Voraussetzungen geknüpft.

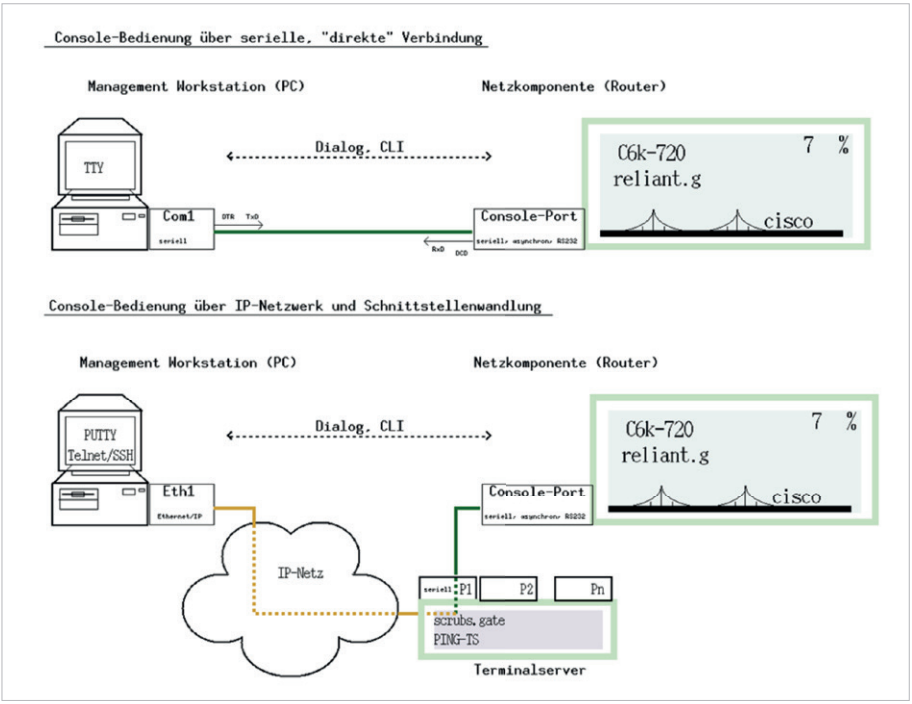
7.4.2.1 Dialog über serielle Konsolenschnittstelle

Gängige Netzwerkkomponenten, wie Router oder LAN-Switche, besitzen in der Regel eine serielle Konsolenschnittstelle für den Anschluss eines Terminals (Datensichtgerät, z. B. vom Typ DEC-VT100) oder PCs mit entsprechender Emulation (z. B. TTY), über die der Bediener (Operateur) elementare Konfigurationen oder Statusabfragen vornehmen und (Log-)Meldungen empfangen kann. Zur inhaltlichen Bedienung bieten die Geräte eine zeilenorientierte Kommandosprache (z. B. Command Line Interface von Cisco, CLI) oder menügeführte Dialoge an. Dabei gelten Menüsteuerungen als einfacher und nutzerfreundlicher, während CLIs meist mehr Flexibilität bieten und von geschultem Personal oft bevorzugt werden. Art und Ausstattung der Bedienschnittstelle sind Eigenschaften des jeweiligen Geräts und unterliegen der Gestaltung des Herstellers, stellen sich aber innerhalb zusammenhängender Gerätefamilien meist gleichartig dar.

Die seriellen Konsolenschnittstellen sind unabhängig vom Konfigurationsstand eines Geräts oder dessen Einbettung in eine Netzwerkumgebung nutzbar und daher auch im Kontext moderner LAN- und IP-Technik als elementare Zugangsform unverzichtbar. Das gilt vor allem für die initiale Gerätekonfiguration zur Anpassung des Auslieferungsstandes an lokale Gegebenheiten oder das Steuern und Verfolgen von Bootvorgängen komplexer Komponenten (z. B. Router) in Zwischenzuständen ohne Netzkonnektivität.

Will man solche Schnittstellen remote, d. h. aus der Ferne über ein (IP-)Netzwerk bedienbar machen, benötigt man Umsetzer in räumlicher Nähe der betreffenden Geräte, die sich als Server zum Führen von Netzdialogen (z. B. Telnet) anbieten und darüber ausgetauschte Daten an der seriellen Schnittstelle in Zeichenfolgen wandeln bzw. umgekehrt in IP-Pakete einpacken. Solche Wandler, die meist mehrere serielle Schnittstellen besitzen, werden als „Terminalserver“ bezeichnet. Die Auswahl einer seriellen Schnittstelle und damit die Herstellung einer Verbindung zu der daran angeschlossenen Netzwerkkomponente erfolgt in der Regel über die IP-Adresse des Servers und eine dem seriellen Port zugeordnete TCP-Portnummer.

Die Abbildung „Serielle Gerätebedienung, lokal und remote“ stellt die Verbindungsarten zwischen PC und Netzkomponente grafisch dar. Dabei zeichnet der untere Bildteil den Weg über ein IP-Netz und einen Terminalserver mit der Anpassung an die serielle Geräteschnittstelle.



Serielle Gerätebedienung, lokal und remote

7.4.2.2 Dialog über (IP-)Netzdienste (Telnet, SSH)

Sind aktive Netzkomponenten durch entsprechende Konfiguration und Installation in ein (IP-)Netzwerk integriert, bieten sie in der Regel Möglichkeiten zum Aufbau von Dialogsitzungen (z. B. per Telnet oder SSH) und darüber geführte Gerätebedienungen. Die logischen Schnittstellen entsprechen weitgehend denen der Konsolenschnittstellen, sind also durch Kommandosprache (CLI) oder Menügestaltung gekennzeichnet.

Diese Methode hängt zwar von der Funktionsfähigkeit des Netzes und der der (IP-) Schnittstelle des Geräts ab, kommt aber sonst ohne zusätzliche Hilfsmittel aus. Sie erfordert lediglich eine elementare Grundkonfiguration der betreffenden Komponente und sonst keine weiteren Maßnahmen. Daher ist sie auf nahezu alle Geräte in „einfacher“ Weise anwendbar.

7.4.2.3 Webbasierter Dialog (HTTP)

Manche Netzkomponenten sind mit einem Webserver ausgestattet, sodass sie mit Hilfe von Webbrowsern bedienbar sind. Das öffnet spezifische Möglichkeiten zur Dialogführung oder etwa auch zur grafischen Aufbereitung statistischer Ausgabedaten. Diese Technik gilt als sehr anwenderfreundlich, hat allerdings den Charakter einer indirekten Bedienung über eine abstrakte Zwischenebene mit eigenen potentiellen Fehlerquellen. In der Praxis ist bisweilen unklar, ob bzw. welche genaue Wirkung bestimmte Manipulationen auf die tatsächliche Gerätekonfiguration haben. Die Methode kann vor allem durch ihre darstellerischen Möglichkeiten sehr hilfreich sein, aber im „Ernstfall“ Gerätezugriffe mit größerer Systemnähe nicht ersetzen und ist daher eher als Ergänzung zu den angeführten Dialogformen unter Verwendung einer Kommandosprache zu sehen.

7.4.2.4 Datentransfer (FTP/TFTP)

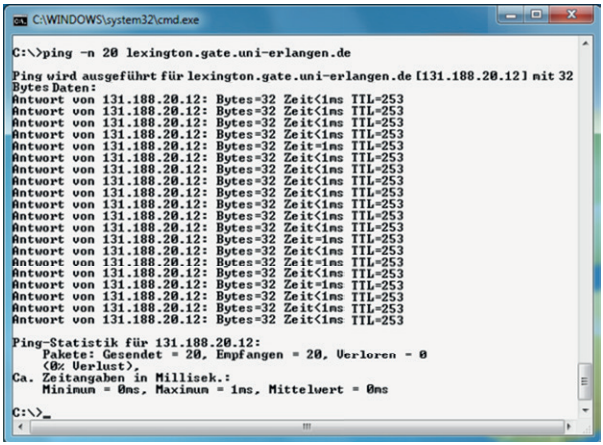
Wenn gewisse Grundkonfigurationen erfolgt sind, bieten Netzkomponenten in der Regel die Möglichkeit Daten mit einem Rechnersystem über ein Filetransferprotokoll (meist TFTP) auszutauschen. Dabei können zum Beispiel Konfigurationen auf dem Rechner in Textform erstellt und zum Gerät übertragen werden oder aber auch Gerätekonfigurationen auf einem Rechner gesichert und verwaltet werden. Dabei kann das Erstellen oder Verändern von Konfigurationsdateien durch Editiervorgänge, aber auch durch spezielle Programme erfolgen. Das RRZE hat dazu Systeme entwickelt, die es erlauben, komplexe Konfigurationen von Routern (Meta-System) und deren Sicherheitsmechanismen (FAUST, vgl. Kapitel 7.4.3.4) aus anwendungsorientierten Beschreibungen zu generieren und übertragbar zu machen.

7.4.2.5 Ping-Test

Eine elementare Methode des Fault-Managements ist der Ping-Test (ICMP Echo-Request/Echo-Reply, vgl. Teil 1 Kapitel 4). Er eignet sich zur Prüfung der grundlegenden Funktionsfähigkeit einer Komponente und deren Einbettung in seine Netzumgebung. Die über IP erreichbaren Managementschnittstellen der Geräte sind in der Regel darauf eingerichtet, auf Ping-Request-Pakete mit Echo-Replys zu antworten. Eine erfolgreiche Abfrage (Erhalt einer Antwort) bedeutet somit eine positive Aussage über den Betriebsstatus der betreffenden Komponente, allerdings nicht unbedingt deren volle Funktionsfähigkeit. Umgekehrt lässt ein negatives Testergebnis (Ping ohne Antwort) nicht direkt auf einen Geräteausfall schließen, deutet aber doch in der Regel auf ein Geräte- oder Netzproblem hin.

In der Praxis hat sich diese Methode zur Gewinnung einfacher Statusaussagen bewährt und wird sowohl gezielt in Einzelfällen (Dialog), als auch allgemeiner in umfassenden Managementsystemen (programmgesteuert) eingesetzt, vor allem dann, wenn Komponenten sonst kein spezifisches Managementprotokoll bedienen.

Weniger bewährt hat sich die Methode zur Messung von Netzlaufzeiten (Performance Management). Die über Ping ermittelten Antwortzeiten beinhalten zwar summarisch auch die jeweiligen Laufzeiten durch das Netz, hängen aber zudem sowohl vom abfragenden System, als auch sehr stark von der abgefragten Komponente bzw. dem Verhalten ihrer Managementsoftware ab. Erfahrungsgemäß schwanken deren Bearbeitungszeiten so stark, dass sie allenfalls gewisse Abschätzungen, aber kaum verwertbare Aussagen über das Netzverhalten zulassen.



Ping-Aufruf von einem Windows-PC

Im dargestellten Beispiel „Ping-Aufruf von einem Windows-PC“ führt die Abfrage von einem Arbeitsplatzrechner zu einem Core-Router („lexington“) des Universitätsnetzes über drei dazwischenliegende Komponenten. Die Rundlaufzeiten liegen dabei jeweils unterhalb einer Millisekunde. „Ausreißer“ sind in diesem kurzen Vorgang nicht enthalten.

7.4.2.6 Gerätemeldungen (Syslog)

Auch hauptsächlich dem Fault-Management zuzuordnen sind von Netzkomponenten generierte Meldungen über bestimmte Ereignisse, zu denen sie zum Nachvollziehen Informationen intern ablegen oder auch an bestimmte Ziele übermitteln. Derartige Logdaten können (je nach Gerät) z. B. über das (IP-)Netz an verschiedene Server gesendet werden, die diese dann ihrerseits in Dateien (Logfiles) ablegen, über generierte E-Mails an Managementpersonal verschicken oder auch anderweitig weiterverarbeiten. Zur Art der Übermittlung (Protokoll-Port 514/UDP) und zum Aufbau von Log-Meldungen innerhalb eines IP-Netzes gibt es eine Norm unter dem Stichwort „Syslog“ (RFC 3195, 5424, 5426), die somit geräte- und systemunabhängig verfügbar ist.

Bei diesem Mechanismus geht also die Initiative von der jeweiligen Komponente aus, die damit verschiedene Vorgänge protokollieren (z. B. Gerätestarts) oder auf Probleme aufmerksam machen kann (z. B. Überlastsituationen oder Zustandswechsel von Schnittstellen). Allerdings kann ein Gerät nur dann Meldungen generieren und versenden, wenn es diesbezüglich noch funktionstüchtig und netztechnisch korrekt eingebunden ist. Seinen eigenen Ausfall kann es somit kaum mitteilen, möglicherweise aber noch dessen Vorgeschichte dokumentieren und gegebenenfalls über einen danach (automatisch oder manuell) erfolgten Neustart informieren.

7.4.2.7 Netzwerkmanagementprotokoll (SNMP)

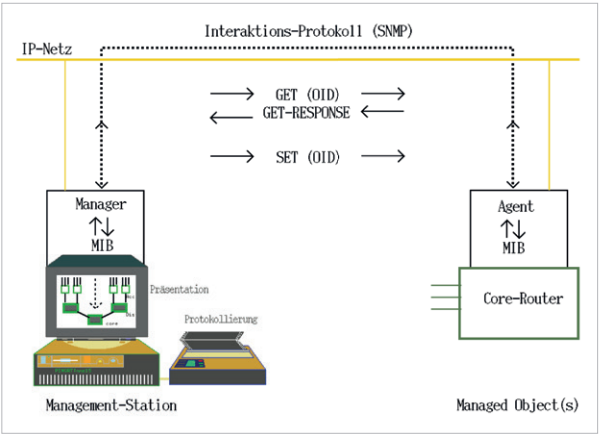
Als Basis zur Automation oder indirekten Bedienung von Komponenten im Rahmen des Configuration- oder Fault-Managements sind Ansätze gedacht, die auf einem Netzwerkmanagementprotokoll beruhen. Im IP-Kontext ist dazu das „Simple Network Management Protocol“ (SNMP) definiert. Über dieses Protokoll tauschen eine Managementstation (Rechner mit steuerndem und verwaltendem Programm) und auf jeweiligen Netzgeräten ablaufende „Agenten“ Informationen aus. Dazu definiert das Protokoll über bestimmte Paketformate Operationen zum Abfragen (Get) und Schreiben (Set) von Daten (aus Sicht der Managementstation), d. h. zum Auslesen oder Verändern einzelner Gerätevariablen. Die Komponenten sind dabei passiv, können aber darüber hinaus auch über besondere Ereignisse unaufgefordert informieren (Traps), ähnlich den Syslog-Meldungen.

Das Protokoll ordnet sich in ein „Manager-Agenten-Modell“ ein, das über verschiedene Festlegungen beschrieben und im TCP-/IP-Kontext ausgefüllt wurde:

- RFC 1155 (1990): „Structure and Identification of Management Information“ (SMI), Beschreibung des Grundmodells
- RFC 1156 (1990): „Management Information Base for Network Management“ (MIB), Beschreibung der Eigenschaften von Datenbasen für den Austausch von Managementinformationen

- RFC 1167 (1990): „Simple Network Management Protocol“ (SNMP, auch SNMPv1), Beschreibung von Protokoll und Operationen
- ISO/IEC 8825-1 (1985): „Abstract Syntax Notation One“ (ASN.1), Beschreibungssprache zur Definition von Datenstrukturen sowie Festlegungen zur Umsetzung von Datenstrukturen und Elementen in ein netzeinheitliches Format
- RFC 1158 (1991): „MIB-II“, „Standarddatenbasis“ für allgemeine IP-Objekte
- RFC 1441 (1993): „Introduction to version 2 of the Internet-standard Network Management Framework“, „SNMPv2“, Erweiterungen
- RFC 3410 (2002): „Introduction and Applicability Statements for
- Internet-standard Management Framework“ „SNMPv3“, Erweiterungen
- RFC 1285 (1992): „FDDI Management Information Base“, Datenbasis für FDDI-Objekte

Grundaufbau des Modells und protokollbezogener Informationsaustausch sind in der Abbildung „SNMP, Aktionen im Manager-Agenten Modell“ dargestellt.

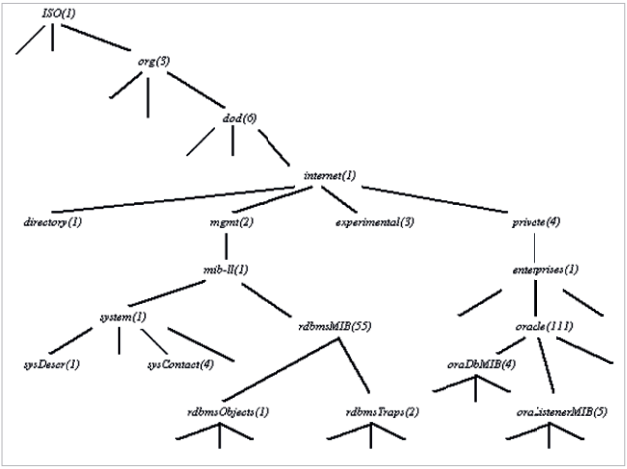


SNMP, Aktionen im Manager-Agenten-Modell

Die zwischen Manager und Agenten ausgetauschten Daten beziehen sich jeweils auf eine verabredete Datenbasis (MIB), die in einer Baumstruktur hierarchisch angeordnete Elemente (Objekte) enthält. Dabei gliedern sich die MIB-Definitionen in ein international genormtes Schema (ISO/IEC 9834) ein, über das jedes Objekt (Blatt des betreffenden Baums, Managementvariable) eindeutig mittels sogenanntem „Object Identifier“ (OID) identifiziert und in den Operationen adressiert werden kann. Jeder Position des (internationalen) Beschreibungsbaums ist eine (Knoten-)Zahl zugeordnet. Im Kontext von SNMP wird ein OID aus einer durch Punkte getrennten Zahlenfolge gebildet, die nacheinander die Knotennummern des Baums von der Wurzel bis zum

betreffenden Blatt (Objekt) enthält. Gemäß der Abbildung „Internationaler OID-Baum“ wird zum Beispiel das Objekt bzw. die Variable „sysDescr“, deren Wert einen Text zur Systembeschreibung eines über MIB-II gemanagten Geräts enthält, über den OID-String „1.3.6.1.2.1.1.1“ adressiert.

So gibt es unter den MIBs sowohl über RFCs eingeführte, als auch „private“, herstellerspezifische Festlegungen (Enterprise-MIBs).



Internationaler OID-Baum

MIBs gibt es für unterschiedliche Anwendungsbereiche oder Gerätetypen. Ihr Aufbau und die Bedeutung enthaltener Variablen werden in der abstrakten Notationssprache ASN.1 nachvollziehbar beschrieben, etwa zur klaren Abstimmung zwischen Herstellern von Managementsystemen und Netzkomponenten. Die wohl gängigste, per RFC genormte MIB ist die mit „MIB-II“ oder „Mib2“ bezeichnete Datenbasis. Sie modelliert „einfache“ Internetobjekte und enthält unter anderem Variablen zur Systembeschreibung (sysDescr) oder Status- und Zählerdaten (ifOperStatus, ifInOctets, ifOuOctets) von den Schnittstellen (Interfaces) eines betreffenden Geräts. Um auch darüberhinaus gehendes Management ihrer Netzwerkkomponenten zu ermöglichen, definieren die Hersteller oft eigene, spezifische MIBs (Enterprise MIBs). So beschreibt zum Beispiel Cisco für seine Router spezifische MIBs, die unter anderem Variablen zur aktuellen CPU-Auslastung (busyPer) oder zu aktuellen Übertragungsraten an den Geräteschnittstellen (locIfInBitsSec, locIfOutBitsSec) enthalten (vgl. „Internationaler OID-Baum“), die etwa in Mib2 nicht enthalten sind. Zudem gibt es auch unter den offiziellen RFCs

MIB-Definitionen, die auf bestimmte Gerätegruppen oder Anwendungsfelder zugeschnitten sind. Als Beispiele seien hier die MIBs zum Remote Monitoring (RMON, RFC 2819) oder dem Management des Routingprotokolls OSPF (RFC 4750) angeführt. Eine Netzkomponente kann natürlich mehrere, unterschiedliche MIB-Definitionen unterstützen. Je größer die Vielfalt der geführten Variablen ist, desto mehr ist die betreffende Komponente einem automatisierbaren, protokollgesteuerten Management zugänglich, was durchaus ein Auswahlkriterium darstellen kann.

Zur Anwendung von SNMP sind mehr oder weniger komplexe Programme erforderlich, die als Schnittstelle zwischen Bedienung und Gerätezugriff fungieren. Die elementaren Operationen von SNMP können z. B. von Unix-Systemen über einfache Zeilenkommandos (snmpget, snmpset) im Dialog aufgerufen werden (Windows-Rechner können durch Installation um entsprechende Kommandos erweitert werden, z. B. über die NET-SNMP-Tools). Diese Anwendungsart ist allerdings sehr schwerfällig und erfordert einiges an Spezialwissen. So muss bspw. zum Auslesen einer Variablen deren OID-String im Kommando explizit angegeben werden, was formal (schreib-) fehleranfällig ist und inhaltlich zum Gerät gehörende Detaildokumentation erfordert (so lautet z. B. der OID-String zur oben erwähnten CPU-Auslastung eines Cisco-Routers: „1.3.6.1.4.1.9.2.1.56.0“). Daher erfolgt die Nutzung des Protokolls meist auf einer abstrakteren Ebene, d. h. indirekt über speziell entwickelte Programme, die z. B. den Administratoren Oberflächen für problembezogene Formulierungen bieten und die Anforderungen auf SNMP-Operationen abbilden. Solche Tools reichen bis zu multifunktionalen Managementsystemen, die z. B. auch eigenständig regelmäßig Abfragen per SNMP ausführen und die Resultate nutzergerecht aufbereiten können (vgl. Kapitel 7.4.3).

Ein kritischer Punkt des Managementprotokolls ist der Sicherheitsaspekt. In der wohl heute immer noch gängigsten Version SNMPv2c sind Lese- und Schreiboperationen jeweils durch ein Passwort (Community String) abgesichert, das für jedes Gerät definiert und in den Operationspaketen anzugeben ist. Dieses Verfahren gilt als schwache Sicherung, zumal aus Bequemlichkeit oder Unkenntnis der Community String in der Praxis häufig nicht explizit definiert, sondern mit der allbekannten Voreinstellung (public) besetzt ist. Mehr Sicherheitsmechanismen, aber auch mehr Komplexität (z. B. Schlüsselverwaltung) bietet die Weiterentwicklung SNMPv3 (RFC 3410, RFC 3418), die sich allerdings noch nicht in großem Umfang durchgesetzt bzw. zur umfassenden Ablösung von SNMPv2 geführt hat.

Eine ausführliche Beschreibung des Protokolls mit zahlreichen Referenzen auf originale Dokumentationen (RFCs) ist z. B. bei Wikipedia nachzulesen [*WikS*].

7.4.2.8 Rechnergestützte Hilfsmittel und Managementsysteme

Wie in den Beschreibungen der grundlegenden Methoden und Bausteine des Komponentenmanagements bereits angedeutet (vgl. Kapitel 7.4.2), bilden diese neben quasi direkten Gerätebedienungen (im Dialog) durch handelnde Personen (Manager, Administratoren) auch die Basis für darauf aufbauende Hilfsmittel. Solche Tools beziehen sich nicht nur auf Anwendungen von SNMP, sondern auch auf Programme, Scripts, die z. B. Dialogsitzungen simulieren, statistische Daten erfassen, auswerten, präsentieren oder Gerätekonfigurationen verwalten und generieren. Solche rechnergestützten Tools dienen der Arbeitserleichterung, der Vermeidung von Fehlbedienungen oder der Darstellung von Netzstrukturen und deren aktuellem Status. In der Anwendung auf umfangreiche, komplex strukturierte Gerätemengen sind sie zur Beherrschung des entsprechenden Netzbetriebs oft sogar unverzichtbar. Beispiele sind etwa das Erlanger Generierungssystem (Meta) zur Erzeugung von Konfigurationsdateien für Router (vgl. Kapitel 7.4.3) oder der Ansatz der Ludwig-Maximilians-Universität München (LMU) zur Generierung von Gerätekommandos (gemäß CLI, vgl. Kapitel 7.4.2.1) über eine generische Schnittstelle [*Meyer*].

Über die Lösung einzelner, dedizierter Aufgaben hinaus gehen (gemäß FCAPS) universelle oder auf bestimmte Aufgabenbereiche spezialisierte Managementsysteme, deren Schwerpunkte in der Ermittlung und Darstellung von Statusinformationen des Netzes sowie einer damit verbundenen, grafischen Präsentation liegen. Sie ermitteln z. B. unter Anwendung der Protokolle Ping und SNMP den Zustand eines Netzes durch regelmäßiges Abfragen der Komponenten oder auch den Empfang von Gerätemeldungen (SNMP-Traps). Manuell oder automatisch erzeugte Grafiken stellen die Topologie eines Netzes in verschiedenen Ansichten dar und geben den jeweils aktuellen Zustand einzelner Komponenten farblich wieder, wobei meistens „grün“ für „up“ (funktionsfähig) und „rot“ für „down“ (nicht in Ordnung) stehen. Beispiele solcher Systeme sind das über lange Jahre am RRZE eingesetzte NMS3000 und das darauffolgend genutzte IMC (vgl. Kapitel 7.4.3). Neben den reinen Statusinformationen lassen sich je nach Gegebenheiten z. B. auch Daten wie CPU-Last von Routern oder Auslastung von Schnittstellen erfassen und darstellen.

Außer überwachenden Funktionen enthalten manche Systeme auch zusätzlich die Möglichkeit, Veränderungen an Geräten vorzunehmen, und zwar unter Ausnutzung der zu SNMP gehörenden Schreiboperation (SET). Dies kann vom Setzen einzelner Variablen bis zur vollständigen Konfigurierung von Komponenten reichen. Allerdings ist das in der Regel nur unter Verwendung geräte- bzw. herstellerspezifischer Datenbasen (Enterprise MIBs) möglich. Es erfordert eine enge Verknüpfung zwischen dem betreffenden Managementsystem und den Definitionen des Herstellers, die zwar nach genormtem

Schema beschrieben (RFC 1156), aber inhaltlich mit ihren Variablen auf bestimmte Produkte zugeschnitten sind. Ein Beispiel hierfür ist das LMS von Cisco (LAN Management Solution, früher Cisco Works), das vom RRZE am Universitätsklinikum Erlangen (UKER, bis 2013 vom RRZE netztechnisch betreut) unter anderem zur Konfigurationsverwaltung und für verschiedene Konfigurationsanpassungen von (Cisco-)LAN-Switchen und Routern eingesetzt wurde, ohne aber Geräte darüber komplett zu konfigurieren.

Die Konfiguration von Komponenten über ein Managementsystem kann in verschiedenen Fällen zwar nützlich sein, ist aber vor allem bei der Anwendung auf komplexe Geräte (z. B. Router) erfahrungsgemäß nicht unproblematisch. Das System bedeutet eine Zwischenebene, die spezifisch zu bedienen und deren Umsetzungen in tatsächliche Gerätekonfigurationen meist nicht transparent ist. Dadurch sind Überprüfungen besonders in Fehlersituationen oft erschwert. Wie bereits erwähnt, hat das RRZE zur Unterstützung derartiger Aufgaben daher eigene Programme entwickelt (vgl. Kapitel 7.4.3.2).

Die angeführten Beispiele deuten an, welcher Art unterstützende Hilfsmittel sein können, geben aber nur einen kleinen Teil denkbarer und verfügbarer Managementwerkzeuge wieder. Darüber hinaus gibt es eine Vielzahl von Werkzeugen zur Lösung unterschiedlicher Aufgaben im Rahmen des Netzwerkmanagements. Für konkrete Einsatzzwecke ist zu entscheiden und auszuwählen, welche Tools hilfreich und sinnvoll zu verwenden sind, zumal diese oft ihrerseits einen nicht zu vernachlässigenden Aufwand von Anpassung, Pflege und Benutzung erfordern.

7.4.3 Lösungen des Netzwerkmanagements an der FAU

Gestaltung und Gewährleistung eines zuverlässigen, stabilen Netzbetriebs an der FAU sind ohne ein adäquates Management nicht denkbar. Dabei gelten auch für den Netzbetreiber RRZE die allgemeinen Überlegungen bzgl. Aufteilung in Aufgabenbereiche, verfügbarer Methoden und hilfreicher Werkzeuge als Richtschnur zur Entwicklung eigener, im gegebenen Umfeld umsetzbarer Managementkonzepte.

Die Tabelle „RRZE/FAU-Netzwerkmanagement, Übersicht 2016“ auf S. 148 fasst zunächst die wichtigsten, über direkte Dialogbedienung hinausgehende Verfahren und Bausteine zusammen und ordnet sie den Aufgabenfeldern gemäß FCAPS zu. Die angeführten Programme und Systeme sind darin stichwortartig beschrieben. Die folgenden Abschnitte gehen pro Aufgabenfeld auf die vom RRZE praktizierten Lösungen ein.

	System	Rechner	Protokoll	Art	Einsatz
Fault	Pathfinder	PC-Client	mysql	Dokumentationssystem	Kabelmanagement, Netzwerkdokumentation
	NMS	nms15	Ping, SNMP	Univers. Mgmt. System	Statusübersicht, Dokumentation, Verfügbarkeit
	IMC	imc	Ping, SNMP	Univers. Mgmt. System	Statusübersicht, Dokumentation, Statistik
	Switchwatch	aladin	SNMP	Gez. SNMP-Abfragen	Endgeräte-Switchbelegung
	Omnivista	dreiimwegg	PING, SNMP	WLAN-Mgmt. System	WLAN-Statusübersicht
	Unix	aladin	syslog	Gerätemeldungen	Fehler-Erkennung / -Analyse
Configuration	Meta	aladin	TFTP	FAU-Scriptsystem	Generierung von Router-Konfigurationskommandos
	Cscreen	aladin	Console Dialog	FAU-Programm	Dialogunterstützung, Mehrfachnutzung
	Omniswitch	controller	Dialogoberfläche	WLAN-Controller	WLAN-Konfiguration
Accounting	Cacti	cacti	SNMP	Spez. Mgmt. System	Verkehrsstatistik
	IMC	imc	SNMP	Univers. Mgmt. System	Verkehrsstatistik
	Radius	radius	LDAP	WLAN-Zugangskontrolle	Nutzerverwaltung
Performance	IMC	imc	Ping, SNMP	Univers. Mgmt.System	Messung, Aufzeichnung Datendurchsatz
	Cacti	cacti	SNMP	Spez. Mgmt.-System	Datendurchsatz, Antwortzeiten
	NMS	nms15	Ping	Univers. Mgmt.System	Anzeige Antwortzeiten in Netzbildern
	Omnivista	dreiimwegg	proprietär	WLAN-Mgmt.System	Messungen, Statistik
Security	FAUST	aladin	TFTP	FAU-Scriptsystem	Generierung von Router -Accesslisten (ACLs)
	Omniswitch	controller	proprietär	WLAN-Controller	Verkehrskontrollen (policies)

RRZE-/FAU-Netzwerkmanagement, Übersicht 2016

7.4.3.1 Fault Management (Fehlermanagement) des RRZE

Das Fehlermanagement bildet den Kern von Abwicklung und Betreuung des täglichen Netzbetriebs. Das schließt neben dem Erkennen, Beheben und Protokollieren von im Netz aufgetretenen Fehlern auch Dokumentationsaufgaben mit ein.

Betriebsüberwachung mit Hilfe universeller Managementsysteme

Im Mittelpunkt des Fehlermanagements stehen Überwachung, Zustandsbestimmung und Darstellung des Netzwerks sowie entsprechende Bedienschnittstellen für die Netzwerkadministratoren. Das RRZE verwendete hierzu über viele Jahre (einschließlich Vorgängerversionen 1985 – 2016) das universellen Managementsystem NMS3000 (Network Management System) von GDC (Hersteller GDC heute nicht mehr existent) und löste dies dann ab 2014 nach und nach durch das IMC (Intelligent Management Center) von Hewlett Packard *[HpImc]* ab. Beide Systeme können ein (IP-)Netzwerk in Gesamtsicht oder für Teilbereiche grafisch darstellen und dabei die Zustände der enthaltenen Komponenten farblich wiedergegeben (z. B. grün für up oder rot für down). Die Netzmanager erhalten so einen Überblick über den jeweils aktuellen Betriebsstatus. Das System ermittelt die Statusinformationen über regelmäßige Echo- (Ping) oder SNMP-Abfragen sowie über eingehende Gerätealarme (Traps). Darüber hinaus enthalten die Systeme vielfältige, ergänzende Funktionen wie etwa zur Meldung und Protokollierung von Ereignissen (Alarmzustellung per E-Mail, Ablage in log-Files), zur Dokumentation, zur Geräteverwaltung oder zur Aufbereitung von Datenstatistiken. Auch schreibende Operationen (SNMP-write) sind je nach verfügbarer Datenbasis (MIB), bzw. veränderbaren Variablen möglich, wurden aber vom RRZE in der Praxis kaum verwendet, da z. B. Konfigurationsänderungen in der Regel über andere Methoden und Werkzeuge vorgenommen wurden. Generell waren/sind diese Managementsysteme zentrale Elemente der Betriebsüberwachung und wesentlich daran beteiligt, Fehler, Störungen oder sonstige Probleme (z. B. Engpässe) möglichst frühzeitig erkennen, analysieren und beheben zu können.

Das **NMS3000** wurde ursprünglich in den Versionen NGS1000 und NGS2000 vom Hersteller Netcomm als Managementsystem für X.25-Netze entwickelt und war als solches in der Lage sowohl eigene Komponenten über spezifische Protokolle als auch herstellerfremde Geräte über einfache Verbindungsprüfungen in das Netzmanagement einzubeziehen. In diesem Sinne wurden seine Vorläufer am RRZE bereits ab 1986 zur Dokumentation und Überwachung des regionalen X.25-Netzes eingesetzt (vgl. Teil 1, Kapitel 3). Weitere Entwicklungen, Erweiterungen betrafen dann das Management von IP-Komponenten und ATM-Switchen (vgl. Teil 1, Kapitel 5). Nach dem Übergang von Netcomm in die Firma „General DataComm“ wurde NMS3000 unter der Herstellermarke „GDC“ vertrieben. Das System erwies sich im Laufe der Jahre

für den Einsatz am RRZE als sehr flexibel und anpassbar. So konnten z. B. die verschiedenen, im FAU-Netz vorkommenden Komponenten (IP-Router, LAN-Switche) des Herstellers Cisco durch Integration zugehöriger Enterprise-Mibs in das Management adäquat einbezogen werden. Allerdings litt das System etwa ab 2001 zunehmend unter mangelnder Herstellerunterstützung und fehlender Weiterentwicklung, sodass z. B. SNMPv2 nie verfügbar wurde und das System an bestimmte Server gebunden blieb. Am RRZE wurde es 2005 letztmalig auf einer damaligen aktuellen Plattform neu installiert: Sun-Server, Solaris 10. Dies erlaubte zwar in der Folge noch einen adäquaten Betrieb, legte aber auch die Suche nach Alternativen nahe.

Neben den genannten sind grundlegende Eigenschaften von NMS3000 in der einer Ausbildungsveranstaltung des RRZE entnommenen Übersicht „Merkmale NMS3000“ zusammengefasst.

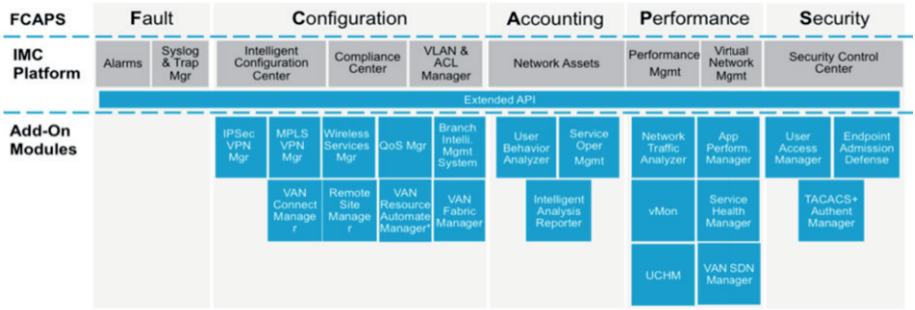

◆ Systemeigenschaften
- Grafischer Editor (objektorientiert)
- Datenbasis (objektorientiert)
- MIBs: Diverse (MIB II, Enterprise, eigene, ...)
- Protokolle: SNMP, PING, ...
- Auto Discovery (IP- Strukturen)
- Auto Draw
- Remote Zugriff
- Kommando- , Programmschnittstelle (NMSQL)
- MIB-Compiler, -Editor
- Erweiterbarkeit

Merkmale NMS3000

Ein herausragender und in dieser Form im Vergleich zu ähnlichen Systemen einmaliger Bestandteil des Systems ist sein grafischer Editor. Er erlaubt z. B. das flexible Zeichnen von Netzbildern und darin die Zuordnung enthaltener Objekte bzw. überwachter Netzkomponenten. Dies ermöglichte unter anderem eine freie Gestaltung übersichtlicher Netzgrafiken, die der Präsentation des aktuellen Netzzustandes und der Dokumentation von Netzstrukturen dienen. Darüber hinaus wurde dieser Editor vom RRZE auch häufig für didaktische Zwecke zur Erstellung erklärender Zeichnungen verwendet, die z. B. in Ausbildungsveranstaltungen und nicht zuletzt in dieser Dokumentation vielfach Verwendung fanden.

Auch **IMC** hat als Managementsystem von Hewlett Packard hat eine längere Vorgeschichte. Sie begann Mitte der 1980er Jahre mit dem „Network Node Manager“ (NNM), der sich dann zusammen mit ergänzenden Bausteinen in das „HP Openview“-Softwareportfolio eingliederte. Dieses System war zum Verwalten und Überwachen der

IT-Infrastruktur großer Unternehmen konzipiert. Ab 2008 wurde es als „HP Service Activator“ (HPSA) vertrieben und ging etwa 2012 in das aktuelle, vom RRZE genutzte „HPE Intelligent Management Center“ (Hewlett Packard Enterprise, IMC) über.



IMC-Bausteine gemäß FCAPS

Wie die Übersicht des Herstellers zeigt, bietet das IMC als universelles System Lösungen für alle Aufgabenbereiche nach FCAPS an, sowohl im Basispaket (IMC Platform), als auch über zusätzliche Module (Add-ON Modules) mit dedizierten Aufgaben (vgl. Abbildung „IMC-Bausteine gemäß FCAPS“). Das RRZE hat die Entwicklung auch dieses Systems seit seinen Anfängen verfolgt und sich in der frühen Phase aus verschiedenen Gründen gegen dessen Einsatz entschieden, da z. B. das NMS3000 durch seine Handhabung, Darstellungsmöglichkeiten und Erweiterbarkeit (auch auf nicht IP-Objekte) für das Management des FAU-Netzes deutlich besser geeignet war. Nachdem sich einerseits ein Ende der Einsatzfähigkeit von NMS300 abzeichnete und andererseits IMC deutliche Verbesserungen z. B. im Bereich der Netzdarstellungen aufwies, hat sich das RRZE für einen Systemwechsel entschieden und dazu 2014 eine „Standard Edition“ von IMC beschafft. Diese ist nach Herstellerangabe in der Lage, „sowohl HP Networking-Produkte als auch zahlreiche Modelle anderer Hersteller zentral zu verwalten“ und „beinhaltet eine umfassende Plattform mit Netzwerktechnologien und zahlreiche Funktionen“. Die Anpassung des Systems an die Gegebenheiten des RRZE und vorhandenen Strukturen des Kommunikationsnetzes der FAU bedeuteten einen nicht unerheblichen Aufwand, der im Zuge einer schrittweisen Ablösung von NMS3000 geleistet wurde und schließlich den Einsatz des Systems im täglichen Netzbetrieb möglich machte.

Die Oberfläche des IMC ist per Webbrowser aufrufbar und somit sehr flexibel zugänglich. Sie präsentiert (gemäß Gestaltung durch das RRZE) dem aufrufenden Manager (Administrator) zunächst eine Startseite (vgl. Abbildung „IMC-Startseite“). Diese stellt

im Überblick verschiedene Statusdaten dar: Anzahl der Komponenten (Device State Overview), Informationen zu ausgewählten Geräten im zyklischen Wechsel (Important Devices, hier „da-gama“), Alarmübersicht (Unrecovered Alarm Statistics), Geräte mit höchster CPU-Last und Speichernutzung (CPU Utilization (%) − Top5 bzw. (Memory Utilization (%) − Top5.

IMC-Startseite

Von der Startseite gelangt man über entsprechende Links (vgl. obere Leiste der Startseite) zu detaillierteren Informationen. Diese Punkte geben auch einen Einblick in die Merkmale des Managementsystems.

- **Ressource:** Einstieg in Darstellungen des Netzes nach verschiedenen Gesichtspunkten (Network Topology, Device View, …), darunter vor allem vom RRZE zusammengestellte Grafiken (Custom View) zur Abbildung einer Gesamtsicht oder einzelner Bereiche des Kommunikationsnetzes (vgl. Beispiele „Aufbau und Status des aktiven Wissenschaftsnetzes des FAU“, Kapitel 7.8.3 oder „ATD-Netzstruktur in Erlangen“, Kapitel 7.7.4).

  Weiter enthalten: Verwaltung und manuelles oder automatisches Hinzufügen überwachter Komponenten (Devices) sowie Steuerung eines Performance Managements.

- **User:** Verwaltung von Nutzern und Zugangsrechten zum IMC.
- **Service:** Bausteine zur Verwaltung des IMC-Systems und Hilfsmittel zur Netzkonfiguration.
- **Alarm:** Alarmansichten und Steuerungen zur Alarmbehandlung
- **Report:** Konfigurierung und Ansicht von Berichten über ausgewählte Ereignisse
- **System:** Verschiedene Einstellungen des Managementsystems

Trotz seines universellen Angebots an FCAPS-Bausteinen wurde und wird auch das IMC vom RRZE hauptsächlich im Rahmen des Fehlermanagements eingesetzt, d. h. vor allem zur Darstellung des Netzes und seiner Teilbereiche mit den jeweiligen, aktuellen Statusanzeigen sowie zur Verfolgung von Netzereignissen (Alarmen), zur Auswertung und Fehleranalyse.

Omnivista ist ein System des Herstellers Aruba Networks (ab 2007 in Kooperation mit Alcatel-Lucent, 2015 übernommen von Hewlett Packard), das speziell für Kontroll- (WLAN-Controller) und Zugangskomponenten (Access Points, APs) entwickelt worden ist. An der FAU dient es vorrangig dem Fehlermanagement im WLAN-Kontext, also der Dokumentation, Zustandsüberwachung oder Erstellung von Statistiken der Funknetze mobiler Anwendungen. Darüber hinaus arbeitet es mit dem Controller „Omni-Switch“ eng zusammen, der unter anderem als Aufpunkt des Konfigurationsmanagements fungiert.

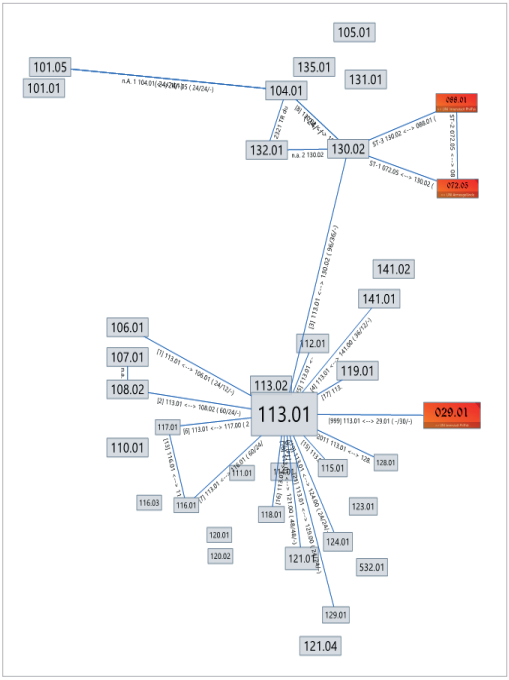
Der Hersteller führt im Datenblatt [*Omni*] des Systems u. a. folgende Merkmale an:

- **Hohe Leistung:** Skalierbare Plattform zur Beherbergung von Mobilinfrastrukturen großer Campusse.
- **Benutzerfreundlichkeit:** Webbasierte Benutzerschnittstelle für eine umfassende, netzwerkweite Verwaltungsplattform zur Steigerung der IT-Effizienz und geschäftlichen Agilität, benutzerdefinierbares Dashboard, das auf die am häufigsten vom Netzadministrator benutzten oder wichtigsten Verwaltungsfunktionen zugeschnitten werden kann.
- **Topologie:** Netzwerktopologie mit erweitertem, mehrschichtigem Discovery zur Erstellung umfassender logischer und physischer Layer-2 und -3-Maps
- **Netzwerküberwachung in Echtzeit:** In Darstellung der Topologie sorgt eine Echtzeitanzeige der Geräte, Clients, Warnmeldung und Ereignisse mit Korrekturmaßnahmen für eine globale Übersicht über alle Netzwerrkausrüstungen. Echtzeitüberwachungen und -analysen werden anschaulich präsentiert.
- **Smart Analytics:** Netzwerkanalysen überwachen die Bandbreite des Netzwerks und die wichtigsten Datenverkehrsmuster anhand von fortschrittlichen Erfassungs- und Berichtsfunktionen IT-Abteilung und CIO erhalten so genauere Informationen über die Nutzung von Netzwerkressourcen, wodurch die Endbenutzererfahrung proaktiv optimiert werden kann.

Dokumentation passiver Strukturen

Die Dokumentation von Kommunikationsnetzen und deren Strukturen ist ein wichtiger Bestandteil des Fault Managements. Dazu leisten die grafischen Darstellungen der Managementsysteme einen guten Beitrag. Allerdings beziehen sich diese hauptsächlich auf die beteiligten aktiven Elemente (z. B. Router oder LAN-Switche), deren Verknüpfungen in der Regel als Verbindungslinien dargestellt werden und von den realen Ausprägungen (z. B. im Rahmen der strukturierten Verkabelung) abstrahieren. Eine gründliche und aktuell gehaltene Dokumentation der passiven Strukturen spielt aber zur Führung eines Netzbetriebs eine ebenso bedeutende Rolle. Sie kann z. B. im Fehlerfall bei der Nachverfolgung geschalteter Kabelwege oder dem Finden von Ort und Anschl**üsse**n an aktive Komponenten sehr nützlich sein.

In diesem Zusammenhang steht das Dokumentationssystem „Pathfinder“ von Tripunkt [*TriPa*], das vom RRZE zur Beschreibung der passiven Strukturen des FAU-Netzes eingesetzt wird. Mit ihm lassen sich geografische Gegebenheiten, Räumlichkeiten, Kabelverläufe, Rangierfelder, Anschlussdosen aber auch Platzierungen aktiver Komponenten ausführlich dokumentieren. Als Beispiele zeigen zwei Pathfinder-Grafiken die „primäre Verkabelung Erlangen-Süd“ mit den Gebäuden (Kästchen mit Nummern) und den verbindenden Kabeltrassen sowie die Dokumentation eines „Verteilerschranks“ mit seinen Patchfeldern (oben) und einem eingebauten LAN-Switch (unten).

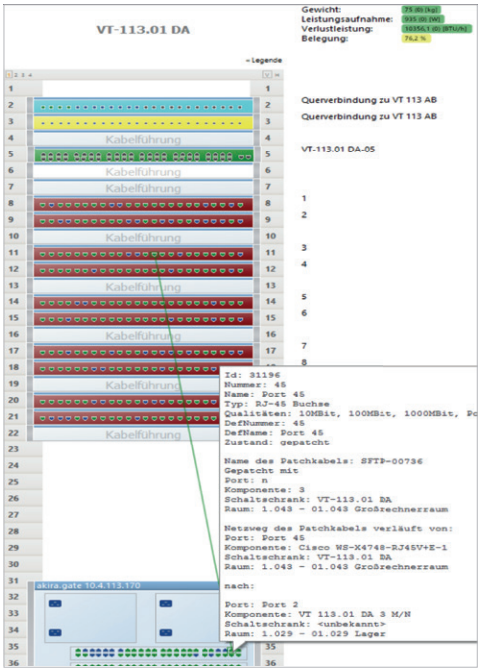


Im Programm kann man per Mausklick weitere Details abrufen. So enthält die Darstellung des Verteilerschranks eine Verbindungslinie zwischen Patchfeld und LAN-Switch sowie ein Textfeld mit ausführlichen Informationen dazu. Beides wurde vom Programm auf Anforderung über eine entsprechende Mausbewegung generiert.

Pathfinder: Primäre Verkabelung Erlangen-Süd

(Die hier schwer erkennbaren Einzelheiten sind zum Verständnis des Prinzips nicht unbedingt erforderlich.)

Die Software wurde in Kooperation des RRZE mit dem Hersteller entwickelt und wird in enger Zusammenarbeit weiter gepflegt. Sie ist daher stark an die Erfordernisse des RRZE angepasst.



Verteilerschrank Aufbau

Dedizierte Werkzeuge des Fehlermanagements

Trotz ihrer universellen Eigenschaften können die Managementsysteme nicht alle Aspekte bzw. Erfordernisse des Fehlermanagements abdecken. Das RRZE setzt(e) daher für bestimmte Aufgaben vielfältige, ergänzende Werkzeuge ein, die in der Regel aus eigener Entwicklung entstanden und als maßgeschneiderte Lösungen zu bezeichnen sind. Dazu gehören:

- **Cscreen** ist ein auf Unix-Systemen verfügbares Programm, das den Dialogzugang für Administratoren zu Netzkomponenten (vgl. Kapitel 7.4) unterstützt. Dazu bietet es eine menügesteuerte Oberfläche, über die gewünschte Komponenten ausgewählt und Verbindungen zu deren Managementschnittstellen hergestellt werden können. Als besonderen Zusatz koordiniert es dabei parallel mögliche Zugriffe von verschiedenen Stellen bzw. Administratoren auf singulär verfügbare Geräteschnittstellen (z. B. Konsolen). Das Programm dient auch dem Konfigurationsmanagement.
- **Switchwatch** ist ein Programm zu Dokumentation von Portbelegungen. Das Anschließen von Endgeräten an die LAN-Switche im Access-Bereich erfolgt in enger Zusammenarbeit der Netzbetriebsgruppe des RRZE mit den jeweiligen, lokal zuständigen

Systemadministratoren. Deren Aufgabe ist es auch, die entsprechenden Switchbelegungen zu dokumentieren, also die Zuordnungen von Endgeräten zu Switchen und deren Schnittstellen zu verwalten. Allerdings wird dies, z. B. auch durch wechselndes Personal bedingt, in der Regel nur unzureichend durchgeführt. Das RRZE hat daher ein Programm entwickelt, das derartige Belegungen automatisch ermittelt und zum Abruf aufbereitet. Dazu werden die Switche regelmäßig (per SNMP) abgefragt, d. h. ihre MAC-Tabellen ausgelesen und so die gültigen Zuordnungen von MAC-Adressen zu Ports bestimmt. Die zu den MACs gehörenden IP-Adressen werden dann (ebenfalls durch Auslesen per SNMP) den ARP-Tabellen des jeweils nächstgelegenen Routers entnommen. Über den Nameservice ermittelt das Programm schließlich die entsprechenden Internetnamen (Reverse Auflösung: IP -> Name). Im Resultat wird dadurch eine Datenbank gepflegt, die pro Switch und Port zum angeschlossenen Endgerät dessen Mac-, IP-Adresse und Namen enthält. Diese Informationen können sowohl von Administratoren des RRZE als auch von lokalen Institutionen (eingeschränkt auf ihre Zuständigkeitsbereiche) über ein Webinterface abgerufen werden.

- **Netman** steht als Programm für statistische Auswertungen von Netzereignissen bzw. zur Bestimmung der Verfügbarkeiten von Netzkomponenten. Über die Analyse von Log-files (Alarmen) bestimmt es pro Gerät dessen Ausfallzeiten aus den Abschnitten zwischen „down“- und „up“-Meldungen und setzt diese in Relation zum gesamten betrachteten Zeitraum. Derartige Statistiken geben Hinweise auf das Betriebsverhalten des Netzes und werden vom RRZE regelmäßig allgemein einsehbar veröffentlicht (In Kapitel 8 sind Statistiken vieler Jahre zusammengefasst.) Dieses Programm wurde im Kontext von NMS3000 bis 2017 eingesetzt. Danach erfolgten entsprechende Auswertungen auf Basis von Protokolldaten des IMC und teilautomatisiertem Einsatz des Tabellenprogramms Excel.

7.4.3.2 Configuration Management (Konfigurationsmanagement) des RRZE

Das Configuration Management (Konfigurationsmanagement) wird für die LAN-Switche mit ihrer relativ einfachen und für Router mit ihrer komplexeren Funktionalität unterschiedlich gehandhabt. Auch die WLAN-Komponenten werden in spezifischer Weise konfiguriert.

Die LAN-Switche der Access-Bereiche werden weitgehend durch Dialoge der Administratoren mit den einzelnen Geräten bzw. deren Kommandoschnittstellen (CLI) konfiguriert (vgl. Kapitel 7.4.2). Zur Unterstützung werden Konfigurationsdateien auf einem Serversystem gehalten, die per TFTP/FTP mit den Geräten ausgetauscht werden können. So wurden z. B. zur Unterstützung von Ersteinrichtungen Musterkonfigurationen nach allgemeinen RRZE-Standards erstellt, um sie auf einen betreffenden Switch aufzuspielen und dann manuell für ihren konkreten Einsatz aufzubereiten.

Das erfordert z. B. den Eintrag einer IP-Adresse zum Management des Geräts, die Etablierung zu verteilender VLANs oder die Einordnung von Endgeräteports in die VLANs gemäß der Verteilung von Nutzergruppen. Auch in der Folge anfallende Aktualisierungen aufgrund sich ändernder Nutzeranforderungen (z. B. durch Umzug oder den Bedarf an zusätzlichen Netzzugängen), sind erfahrungsgemäß am besten in direkter Dialog-Bedienung der betreffenden Geräte zu bewältigen. Das ergänzende Speichern der Konfigurationen in Dateien dient der Dokumentation, dem Nachvollziehen von Änderungsvorgängen, aber auch dem Backup, um in besonderen Fehlerfällen, etwa nach Konfigurationsverlust oder dem kompletten Austausch eines Geräts, die Ausgangskonfiguration wiederherstellen zu können.

In der Regel komplexer und für den allgemeinen Netzbetrieb von größerer Bedeutung ist das Konfigurieren der Core- und Distributionskomponenten, d. h. den für die Vermittlung von IP-Paketen zuständigen Routern. Die Erstellung der umfangreichen und vielfältigen Konfigurationen kann zwar auch über Einzelkommandos im Dialog erfolgen, ist aber sehr aufwendig, oft unübersichtlich und somit leicht fehleranfällig. Das RRZE hat deshalb zur Unterstützung der Administratoren ein spezielles Hilfsmittel (ein als „META“ bezeichnetes Skript-System) mit folgenden Merkmalen entwickelt:

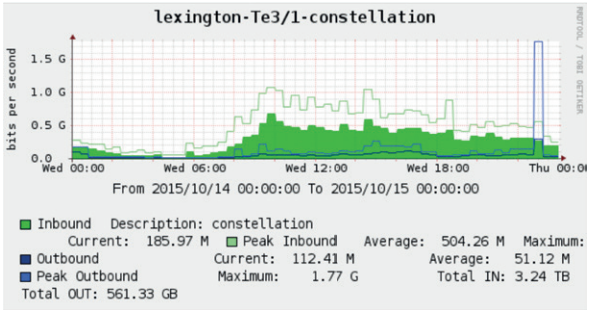
- kompakte Kommandosprache
- weitgehend unabhängig vom betreffenden Router-Typ
- Einfügen von „RRZE-Standard-Sequenzen“
- angepasste Vervielfältigung gleichartiger Angaben
- Plausibilitätsprüfungen

Aus den Angaben in der Metasprache werden einzelne Router-Kommandos erzeugt und in Konfigurationsdateien abgelegt, die dann per TFTP auf das jeweilige Gerät übertragen und dort aktiviert werden können. Das System läuft in einer UNIX-Umgebung, die auch zum Editieren und Verwalten von Meta- und Konfigurationsdateien genutzt wird. Durch seine Erweiterungs- und Anpassungsfähigkeit hat sich die Methode am RRZE über lange Jahre bewährt und zur Arbeitserleichterung und Fehlervermeidung erheblich beigetragen.

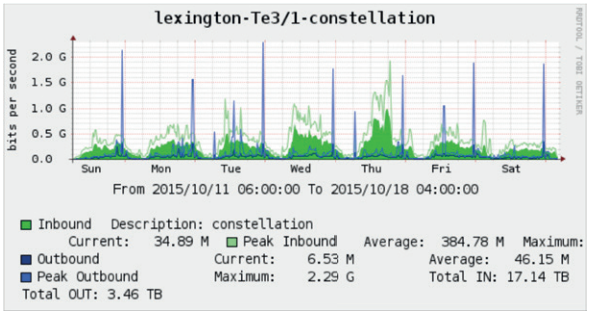
Die Konfiguration der Komponenten des drahtlosen Netzes erfolgt in direkter Bedienung einer Webschnittstelle der Hauptkontrollkomponente (Mastercontroller), die neben der Abwicklung von Steuerungsaufgaben auch für die Verteilung von Konfigurationen auf die einzelnen Zugangspunkte (APs) zuständig ist. Diese Art der Bedienung hat sich als angenehmer und zuverlässiger erwiesen als die Verwendung entsprechender Funktionalitäten des Managementsystems Omnivista, das deshalb vorrangig im Rahmen des Fehlermanagements eingesetzt wird (vgl. Kapitel 7.4.3.1.1). Versuche paralleler Nutzung beider Möglichkeiten führten zu Inkonsistenzen und waren daher nicht praxistauglich.

7.4.3.3 Accounting Management (Abrechnungsmanagement) des RRZE

Das Kommunikationsnetz der FAU steht den Angehörigen der Universität als Dienstleistung zur Verfügung. Dabei wird die Inanspruchnahme des Netzes in keiner Weise in Rechnung gestellt (Accounting im engeren Sinne), also z. B. weder bezogen auf einzelne Nutzer(-gruppen) noch bezüglich einzelner Anschlüsse von Endgeräten (Switchports). Dennoch werden diesbezügliche Verkehrs- und Lastdaten laufend gemessen und ausgewertet, um einen Überblick über die Nutzung des Netzes und deren Entwicklung zu erhalten. Diese derart erfassten (Accounting-)Daten werden in entsprechenden Darstellungen und Statistiken aufbereitet und können bereichsbezogen auch von lokalen Administratoren abgerufen werden, sowohl bezogen auf den jeweils aktuellen Stand als auch für zurückliegende Zeiträume. Dazu dient das System Cacti [*Cacti*], das am RRZE hauptsächlich zur Anzeige von Interface-Statistiken genutzt wird, also zur Darstellung der Auslastung von Verbindungen zwischen Netzkomponenten oder Netzkomponenten und Endsystemen. Als Beispiel stellen „Interface-Verkehrsstatistik-Tagesverlauf“ und „Interface-Verkehrsstatistik-Wochenverlauf“ den Datenverkehr zwischen den Core-Komponenten in Erlangen-Süd („constellation“) und



Interface-Verkehrsstatistik-Tagesverlauf



Interface-Verkehrsstatistik-Wochenverlauf

Nürnberg-Zentrum („lexington“) eines Tages bzw. einer Woche im Oktober 2015 dar. Die im Zusammenhang der Integration des AEG-Geländes als Standort der FAU neu eingerichtete Verbindung zwischen Erlangen und Nürnberg ist über eine Glasfaserstrecke realisiert, die von den Komponenten mit einer Geschwindigkeit von 10 Gigabit pro Sekunde (10 Gbp/s bzw. 10 G in der Grafiknotation) betrieben wird.

Man erkennt typische, wiederkehrende Tagesnutzungen mit vornehmlichem Datenverkehr von Erlangen in Richtung Nürnberg (grüne Kurven), die hauptsächlich durch (lesende) Zugriffe auf zentrale Server im RRZE und die Nutzung des Internets zu erklären sind sowie in den Nachtstunden starke Spitzen in umgekehrter Richtung von Nürnberg nach Erlangen (blaue Kurven), die zentrale Datensicherungsvorgänge widerspiegeln. Zusammenfassende Auswertungen stellen jeweils die Spitzen- (Peak) und Durchschnittswerte (Average) der beobachteten Übertragungsgeschwindigkeiten dar und berechnen für die betrachteten Zeiträume die übertragenen Datenvolumina (Total Out, Total In). Dabei ist zu beachten, dass die angezeigten maximalen Werte über mehrere (5) Minuten gebildete Durchschnitte wiedergeben, d. h. in Bezug auf kürzere Zeiträume durchaus auch deutlich höhere Spitzen vorkommen. Gemäß Darstellung wurden z. B. an dem gezeigten Tag insgesamt 3,24 TB von Erlangen nach Nürnberg und 561,33 Gigabyte bzw. 0,561 TB in umgekehrter Richtung übertragen.

Zur genaueren Aufschlüsselung des Datenverkehrs, etwa nach Anwendungen oder Nutzer(-gruppen), hatte das RRZE eine aus eigener Entwicklung stammende sogenannte „Accountingbox“ im Einsatz, deren Betrieb aber aus Datenschutzgründen eingestellt werden musste. Die Analyse und Speicherung solcher Daten ist nur kurzfristig in Sonderfällen, etwa im Rahmen einer konkreten Fehlersuche gestattet, nicht aber zum Zwecke genereller statistischer Erfassungen und Aufbereitungen.

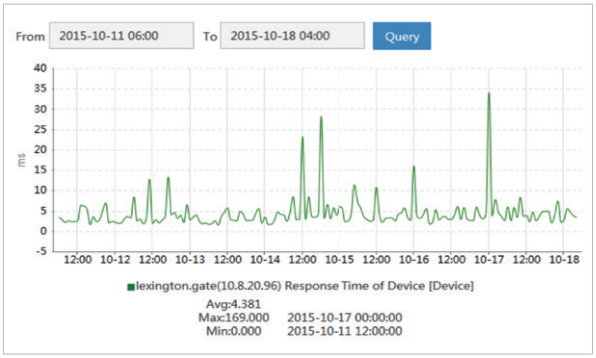
Zum Accounting Management zählt auch das Verwalten (Administrieren) von Netzbenutzern bzw. deren Kennungen. Während an den Schnittstellen des drahtgebundenen Netzes nur in Ausnahmefällen eine Autorisierung erforderlich ist (Stichwort: port security), wird an der FAU vor allem im Zusammenhang externer Zugänge (über VPN-Server) oder mobiler Anwendungen (WLAN) eine Identifikation einzelner Benutzer verlangt und über einen Radius-Server kontrolliert. Diese Kontrolle ist in das allgemeine Identifikationssystem (IdM) des RRZE bzw. der Universität integriert.

7.4.3.4 Performance Management (Leistungsmanagement) des RRZE

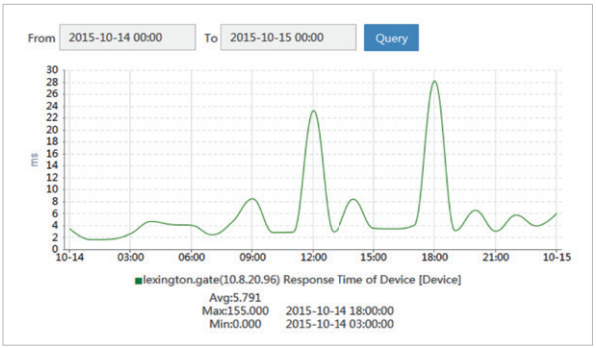
Die von Cacti und in ähnlicher Form auch von IMC erfassten Daten zur Auslastung von Verbindungsstrecken beschreiben auch Aspekte der Leistungsfähigkeit des Netzes, tragen also zum Performance Management bei. So geben etwa neben den techni-

schen Parametern von Schnittstellen und Kommunikationsstrecken die ermittelten Durchschnitts- und Maximalwerte an, welche Übertragungsgeschwindigkeiten im Betrieb tatsächlich erreicht wurden und demnach mindestens zur Verfügung stehen.

Andere, wichtige Parameter zur Leistungsbeschreibung sind Durchlauf- und Verweilzeiten (Delays) beim Übertragen von Datenpaketen über das Netz. Für gewählte Kommunikationsbeziehungen können diese über „Ping-Tests“ summarisch, d. h. durch Messung von Zeiten zwischen dem Absenden von Anfragen bis zur Ankunft zugehöriger Antworten bestimmt werden (vgl. Kapitel 7.4.2.5). Hierzu bieten die universellen Managementsysteme Unterstützung, die für regelmäßig auszuführende Messungen eingerichtet werden können. Während NMS3000 in seinen Netzbildern zum Beispiel Datenraten, CPU-Lasten, ermittelten Antwortzeiten in Zahlen auf aktuellem Stand darstellte, wird IMC zu systematischen Messungen einer Vielzahl von Geräten konfiguriert, dessen Ergebnisse über ein Performancemodul des Systems in grafischen



Ping Antwortzeiten - Tagesverlauf



Ping Antwortzeiten - Wochenverlauf

Darstellungen abrufbar sind. Ein Beispiel geben die von IMC erzeugten Abbildungen „Ping Antwortzeiten – Tagesverlauf“ und „Ping Antwortzeiten – Wochenverlauf“ , mit den über Ping-Aufrufe zum Router „lexington“ gemessenen Antwortzeiten.

Wie bereits bei der Beschreibung des Ping-Tests erwähnt (Kap. 7.4.2.5), ist zu beachten, dass so gemessene Antwortzeiten nicht allein das Verhalten des Netzwerks wiedergeben, sondern in starkem Maße auch von den beteiligten Endgeräten beeinflusst sind. Dies gilt für die einzelnen, ermittelten Werte, aber auch für deren Schwankungen im zeitlichen Verlauf. In die systematisch durchgeführten Messungen gehen also neben Eigenschaften des betreffenden Netzweges auch die der initiierenden Station (Managementserver) und des jeweils angesprochenen Endgeräts mit ein. Gerade Netzkomponenten bzw. deren Softwarebausteine zur Bearbeitung von Managementanfragen verhalten sich als Endgeräte in diesem Sinne erfahrungsgemäß nicht ideal. So liegen, anders als die hier dargestellten Werte vermuten lassen, die tatsächlichen Verweilzeiten in den durchlaufenen Netzkomponenten gemäß Herstellerangaben und anderer Beobachtungen deutlich unter einer Millisekunde. Die relativ hohen und oft schwankenden Antwortzeiten abgefragter Netzkomponenten können zum Beispiel durch nachrangige Behandlung der eingehenden Ping-Abfragen, deren Bearbeitung in der relativ “schwachen“ Zentraleinheit (CPU) oder hohe Verkehrslast des Geräts verursacht werden (schnelles Switchen oder Routen geschieht in der Regel außerhalb der CPU). Dennoch bietet diese auch in hoher Dichte und Verbreitung relativ einfach anzuwendende Messmethode (meist praktizierte Abstände zwischen 1 und 5 Min.) einen grundlegenden Anhalt zur Beurteilung von Leistungsparametern (Laufzeiten, Delays) des Netzwerks, insbesondere lassen sich so außergewöhnliche Zustände von einem Normalverhalten unterscheiden.

In besonderen Fällen, etwa zur Analyse von Durchsatzproblemen oder zum Eingehen auf außergewöhnliche Anforderungen, sind darauf gezielt ausgerichtete Messmethoden und Tests auszuführen, die in der Regel den Einsatz spezieller Geräte (z. B. Netzwerkanalysatoren) oder Messaufbauten erfordern.

7.4.3.5 Security Management (Sicherheitsmanagement) am RRZE

An bestimmten Stellen, wie dem Übergang zum Internet (bzw. dem Deutschen Forschungsnetz) oder dem Netz der Zentralen Universitätsverwaltung erfolgen Sicherheitsprüfungen über VPN-Server oder dedizierte Firewalls. Allgemein aber, d. h. für jedes Subnetz, werden eingehende und ausgehende Pakete über spezifische Filterregeln auf ihre Zulässigkeit getestet und ggfs. nicht durchgelassen (verworfen). Diese in „Access Lists“ formulierten Regeln werden für jedes Subnetz je nach lokalen und globalen Sicherheitsanforderungen definiert und auf dem betreffenden Router eingetragen.

Zur Unterstützung der Erstellung und Verwaltung von Filterlisten hat das RRZE in Ergänzung zur oben beschriebenen Router-Konfigurierung (Meta-Mechanismus, Kapitel 7.4.3.2) auch ein System zum „halbautomatischen“ Generieren zugehöriger Kommandos entwickelt: FAU-Security-Tool (FAUST). Das Aufstellen von Filterlisten, deren Wirkung von der Reihenfolge einzelner Kommandos abhängt, wird dadurch erheblich vereinfacht und z. B. durch Plausibilitätsprüfungen oder übergeordnete Anweisungen, wie „Sperre Hostadresse auf allen Netzen“, ergänzt. So wird damit zum Beispiel eine schnelle und wirksame Reaktion im akuten Bedrohungsfall möglich.

Die Absicherungen auf Netzebene sind nur ein Teil genereller Maßnahmen zu Datenschutz und Sicherheit von RRZE und FAU, auf deren Problematik im Kapitel 7.6 näher eingegangen wird.

7.5 Netzmanagement über Kommunikationsstrukturen

Effektiver Netzbetrieb und schnelle Reaktionen in Störfällen können gerade in einem weit ausgedehnten und weit verteilten Netzwerk wie dem der FAU nur erreicht werden, wenn Zugriffe auf die Komponenten „von remote“ möglich sind, d. h. von einem zentralen Standort (z. B. vom Rechenzentrum) Abfragen, Analysen und Veränderungen vorgenommen werden können. Nur so können sehr hoher Personalbedarf oder Anreisen zu Tätigkeiten vor Ort weitgehend vermieden und schnelle Reaktionszeiten in Problemfällen erreicht werden.

Bezieht man den Einsatz von Terminalservern mit ein (vgl. Kapitel 7.4.2.1, Abbildung „Serielle Gerätebedienung, lokal und remote“), lassen sich alle grundlegenden Methoden (Kapitel 7.4.2) zur Bedienung von Netzkomponenten über IP-Netzwerke abwickeln, teilweise setzen sie sogar ein Netzwerk voraus. Bei entsprechender Konfiguration und Netzgestaltung ist es daher prinzipiell möglich, sowohl von einer zentralen Managementstation als auch von verteilten Arbeitsplätzen aus jede aktive Komponente eines Netzes zu erreichen und entsprechend zu bedienen.

Zur Realisierung eines solchen „Remote-Managements“ gibt es verschiedene Ansätze, die sich bezüglich der Verknüpfung mit dem Betriebsnetz sowie des Aufwandes und verfügbarer Funktionalität unterscheiden. Die Umsetzung der Konzepte an der FAU stellen sich im Aufbau entsprechender Netzstrukturen dar.

7.5.1. Grundmodelle des Remote-Managements

Remote-Zugriffe auf Netzkomponenten zum Zwecke des Managements können auf verschiedenen Wegen über ein Übertragungsnetz realisiert werden. Dabei besteht ein grundsätzlicher Unterschied, ob solche Wege durch das betreffende Betriebsnetz oder über davon unabhängige Strukturen geführt werden.

7.5.1.1 Inline-Management

Ein naheliegender Ansatz besteht in der Integration der Gerätemanagementschnittstellen in das betreffende Betriebsnetz. Die Managementadressen der Komponenten sind dabei in die vorhandene Struktur von VLANs und (IP-Sub-)Netzen eingebettet und werden wie die Endadressen sonstiger Netzteilnehmer behandelt. Die Kommunikationswege zwischen Manager und Netzobjekten verlaufen daher innerhalb (inline) des Kommunikationsnetzes, d. h. innerhalb des allgemein genutzten Betriebsnetzes. Sie unterliegen daher dessen Verteil- und Vermittlungsmechanismen und benötigen dessen Betriebsbereitschaft.

Ein derartiges Inline-Management ist in einfacher Weise flächendeckend, d. h. für alle Netzwerkkomponenten umzusetzen, da es lediglich entsprechend angepasste Gerätekonfigurationen erfordert. Es benötigt also keine Netzerweiterungen, kommt ohne zusätzliche Hardware aus und verursacht daher keine spezifischen Kosten.

Allerdings ist das erfolgreiche Bedienen eines Geräts an verschiedene Bedingungen geknüpft:

- Die Managementschnittstelle einer Komponente muss korrekt konfiguriert und betriebsbereit sein
- Die lokale Netzwerkumgebung der Schnittstelle (VLAN, IP-Subnetz) muss intakt sein
- Zwischen bedienender Station und Managementschnittstelle muss eine stabile Verbindung hergestellt, also ein durchgängiger Pfad aufgebaut werden können

Besonders kritisch sind in diesem Zusammenhang Konfigurationsänderungen, die die Netzeinbettung einer Komponente betreffen. Das gilt z. B. für Adressmodifikationen oder Änderungen der VLAN-Zugehörigkeit. Hier können während eines Managementvorganges Inkonsistenzen entstehen, die das Gerät unerreichbar machen, was dann nur durch Einsatz vor Ort zu korrigieren ist.

Neustarts (Bootvorgänge) können im Inline-Management angestoßen, aber nicht weiterverfolgt werden, da je nach Phase vom Gerät abgesetzte Meldungen nicht mehr übertragen bzw. empfangen werden können. Ein Boot führt nämlich (naturgemäß) zum Abbruch betreffender Managementverbindungen (Dialogsitzungen), die erst nach erfolgreichem Abschluss der Normierungen wieder neu aufgebaut werden können. Das gilt auch für Konsolenzugänge über entsprechende Terminalserver, wenn diese als Komponenten im Betriebsnetz integriert sind.

Zu erwähnen sind auch bestimmte Fehlersituationen, die Gerätebedienungen über Inline-Management erschweren oder gar unmöglich machen. Dazu gehören ungewöhnlich hohe Prozessor- oder Verkehrslasten von Komponenten oder in deren Umgebung, etwa in Zusammenhang mit Schleifen in lokalen VLANs (Ethernet-Loops), oder Störungen durch Fehlverhalten angeschlossener Endgeräte, die keine stabilen Verbindungen zum Management betroffener Komponenten herstellen lassen. Problemeinkreisung oder gezielte Maßnahmen etwa zur Deaktivierung einzelner Komponenten oder Schnittstellen sind dann wesentlich behindert bis unmöglich.

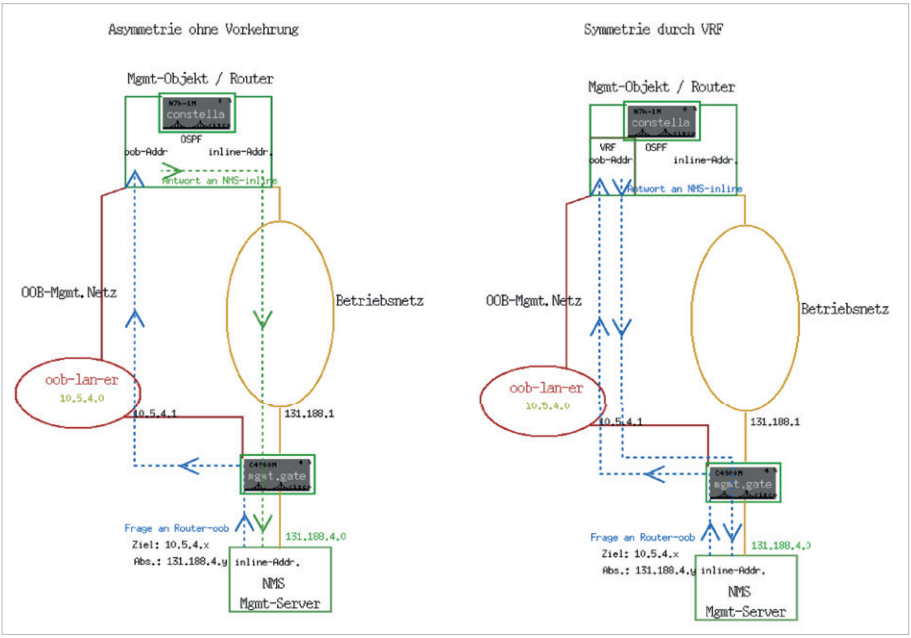
Dennoch ist das Inline-Management insbesondere für Komponenten im Access-Bereich (Endgeräteswitche) sehr gut geeignet, da es einfach und kostengünstig in der Fläche (bspw. nahezu für „alle“ LAN-Switche) zu realisieren ist und die genannten Schwierigkeiten nach Erfahrungswerten im Kontext des FAU-Netzes im Verhältnis zur Menge der Geräte nur sehr selten aufgetreten sind oder dann meistens auf andere Weise gezielt zu bearbeiten waren.

7.5.1.2 Out-of-Band-Management

Will man Netzwerkkomponenten auch bei Störungen im Kommunikationsnetz zuverlässig bedienen können, benötigt man ein separates Netzwerk, das unabhängig vom Betriebsnetz aufgebaut und strukturiert ist. Die Zugriffspfade vom Bediener bzw. von der Managementstation zu den Komponenten liegen dann außerhalb des allgemeinen Betriebsnetzes, verlaufen also „Out-of-Band“ (OOB). Diese Eigenständigkeit ist in bestimmten Problemfällen zwar ein großer Vorteil, stellt aber folgende Bedingungen:

- Über das separate Managementnetz müssen alle (zu managenden) Komponenten erreichbar sein, das Netz hat somit potentiell einen flächendeckenden Charakter
- Das Netz erfordert die gleiche Ausbreitung wie das Betriebsnetz, auch wenn es möglicherweise „einfacher“ strukturiert sein kann (weniger VLANs, IP-Subnetze)
- Das Netz muss stets funktionsfähig sein, selbst dann, wenn es „nur“ in Fällen von Störungen des „Normalbetriebs“ tatsächlich genutzt wird
- Die Komponenten des „Out-of-Band“-Netzes sind selbst auch Managementobjekte, die ihrerseits konfiguriert und überwacht werden müssen
- Managementstationen sind entweder ebenfalls separat zu betreiben oder es sind Übergänge zwischen Betriebs- und Managementnetz einzurichten
- Separate Komponenten und Struktur bedeuten extra Kosten, besonders problematisch sind dabei dedizierte Weitverkehrsverbindungen

Besonders nützlich ist ein „Out-of-Band“-Management im Zusammenhang mit Konsolenzugängen über Terminalserver. Falls die Konsolschnittstelle ansprechbar ist, ermöglicht es elementare Bedienung einer Komponente unabhängig von deren Zustand oder dem des Betriebsnetzes und erlaubt z. B. das Verfolgen und eventuelle Steuern von Bootvorgängen. Sinnvoll zu verwenden sind aber „Out-of-Band“-Verbindungen auch zu den IP-Managementschnittstellen von Komponenten, obwohl sie demgegenüber gewissen Einschränkungen unterliegen (z. B. keine Bootverfolgung). Zur Eingliederung in das OOB benötigen die Komponenten eine dedizierte Schnittstelle. Ist das Gerät ein Router, kann diese auch über ein entsprechendes VLAN/Subnetz bereitgestellt werden. Allerdings sind dann bestimmte Vorkehrungen zur Vermeidung von asymmetrischem Datenverkehr (Management-Anfragen über OOB-Netz, Antworten über Betriebsnetz) zu treffen, etwa unter Einsatz der VRF-Technik (Virtual Routing and Forwarding, VRT) von Cisco, die es erlaubt, Routingdefinitionen speziell an eine Managementschnittstelle zu binden und vom sonstigen Routing der Komponente zu entkoppeln (die Abbildung auf S. 166 „Routing mit (asymmetrisch) und ohne (symmetrisch) VRF“ stellt Problematik und Lösung grafisch dar). Das OOB-Management über IP-Schnittstellen ist gegenüber der Nutzung serieller Konsolzugänge weniger aufwendig, einfacher zu handhaben und kommt ohne zwischengeschaltete Server aus, hat aber die generellen Vorteile von Verbindungen außerhalb des Betriebsnetzes.



Routing mit (asymmetrisch) und ohne (symmetrisch) VRF

Je nach Bedeutung einer Komponente für den gesamten Netzbetrieb empfehlen sich für das Management bspw. OOB-Konsolzugänge für Core-, OOB-IP-Zugänge für Distribution- und Inline-IP-Zugänge für Access-Komponenten (vgl. Konzepte des RRZE im folgenden Abschnitt)

7.5.2 Remote-Management des RRZE

Durch die Verteilung der FAU auf viele, voneinander entfernte Standorte kam dem Remote-Management des Kommunikationsnetzes von Beginn an eine große Bedeutung zu. Insbesondere wurde durch Wachstum und Ausbreitung des auf dem Internetprotokoll basierenden Netzwerks ein vom RRZE zentral geführtes Management praktisch unerlässlich.

Zur Erfüllung der Managementaufgaben müssen daher deren aktive Komponenten für die Netzadministratoren und die unterstützenden Systeme vom zentralen Rechenzentrum aus erreichbar sein. Wie im vorangegangenen Kapitel beschrieben, kann das über verschiedene Zugriffsmethoden und strukturelle Ansätze realisiert werden,

die für den konkreten Fall auszuwählen und auszuarbeiten sind. Bei der Konzeption sind die spezifischen Anforderungen und Gegebenheiten zu berücksichtigen, aber auch Aspekte von Beherrschbarkeit oder Wirtschaftlichkeit zu beachten. Dies gilt insbesondere für das OOB-Management, das den Aufbau und Betrieb einer separaten, dedizierten Netzstruktur verlangt.

7.5.2.1 Anforderungen und Methodenwahl

Grundsätzlich besteht der Bedarf, jede aktive Komponente des Kommunikationsnetzes remote bedienen zu können. Es macht allerdings wenig Sinn, für jedes der beteiligten Geräte auch alle möglichen Zugriffsarten zu realisieren. Im Extremfall würde dies ein eigenes Netzwerk erfordern, das in Ausbreitung und Struktur der des Betriebsnetzes nahekommen und seinerseits umfangreiche Managementanforderungen stellen würde.

Es muss also zwischen Machbarkeit, Aufwand und Nutzen sowie der Wertigkeit des Bedarfs abgewogen und pro Komponente entschieden werden, welche der Zugriffsmethoden sinnvoll bereitzustellen sind. Im Einzelnen bedeutet dies die jeweilige Wahl von:

- Managementschnittstelle(n)
  - Konsole
  - Dediziertes Ethernet-Interface
  - Internes IP-Interface
  - Kombinationen davon

und

- Zugriffspfad(en)
  - Inline (innerhalb des Betriebsnetzes)
  - Out-of-Band (außerhalb des Betriebsnetzes)
  - Mischformen

Je bedeutender die Rolle einer Komponente in der Architektur und für die Funktionalität des gesamten Netzwerks ist, desto mehr verschiedene Zugangsmöglichkeiten werden benötigt. So sind etwa Konsolenzugänge und alternative Pfade für die Core-Router unverzichtbar, während für Endgeräteswitche im Access-Bereich Zugriffe auf IP-Schnittstellen über das Betriebsnetz in der Regel ausreichen. Die Vorteile von Konsolenschnittstellen werden am besten ausgenutzt, wenn sie weitgehend out-of-band erreichbar, oder die Zugangswege zumindest in der näheren Umgebung betroffener Geräte unabhängig vom Betriebsnetz sind.

In der Tabelle „Benötigte Management-Zugänge“ sind die Netzkomponenten gemäß ihrer strukturellen Einordnung klassifiziert und der jeweilige Bedarf an Zugangsarten und -Pfaden skizziert.

Benötigte Management-Zugänge, 2015

Komponenten-Klasse	Zugangsschnittstelle			Zugangspfad		Beispiel-gerät	Geräte-Anzahl
	Interne-IP	ETH-Int	Konsole	Inline	oob		
Core-Router	*	(*)	*	*	*	constellation	8
Distribution-Router (groß)	*	(*)	*	*	*	hector	30
Distribution-Router (klein)	*	-	(*)	*	(*)	astro	20
Access-Switche Verteiler	*	(*)	-	*	(*)	minerva	20
Access-Switche Endgeräte	*	-	-	*	-	messi	1000

* : erforderlich / (*) : optional, je nach Gegebenheit / - : nicht benötigt.

7.5.2.2 Umsetzung des Inline-Managements

Das Inline-Management basiert auf der Struktur des Betriebsnetzes und benötigt somit keine dedizierten Netzstrukturen, sondern lediglich entsprechende Konfigurationen der zu bedienenden Komponenten. Für die im FAU-Netz eingesetzten Gerätetypen lässt sich dies relativ einfach einrichten. Die umfassende Umsetzung erfolgte nach einheitlicher Konzeption des RRZE.

Die Router haben naturgemäß mehrere IP-Schnittstellen (z. B. die Default-Routes angeschlossener Subnetze), die alle in der Regel auch zu Managementzwecken angesprochen werden können. Die Erreichbarkeit eines Routers hängt dabei aber von dem Status des adressierten Interfaces bzw. der Funktionsfähigkeit des zugehörigen (Sub-)Netzes und des betreffenden lokalen Netzes ab. Sinnvoller ist es daher, für das Management Adressen zu verwenden, die von einzelnen, angeschlossenen Netzen unabhängig sind. Dies ist auf den im FAU-Netz eingesetzten Routern durch die Definition sogenannter „Loopbackadressen“ möglich. Diese sind als reine Hostadressen den Routern eindeutig zugeordnet, werden im Routing des Netzwerks nach den üblichen Mechanismen (OSPF) verbreitet und können somit von jedem Endpunkt

(sofern nicht aus Sicherheitsgründen gezielt eingeschränkt) „inline“ erreicht und per Dialog oder Protokoll gemanagt werden. Die Adressen der Router werden aus einem nicht nach außen („außerhalb der FAU“) gerouteten Raum vergeben (etwa als „private“ Adressen der Form 10.x.x.x).

LAN-Switche, die für das Verteilen (Switchen) von Datenpaketen (Ethernet-Frames) innerhalb lokaler Netze zuständig sind und meist mehrere virtuelle LANs (VLANs) bzw. Segmente davon bedienen, enthalten zum Management eine interne Schnittstelle, die in ein VLAN eingeordnet wird. Je nach VLAN bzw. zugehörigem IP-Subnetz kann dieser Schnittstelle eine IP-Hostadresse zugeordnet werden, über die dann die Bedienschnittstelle des jeweiligen Switches aus dem Netz erreichbar ist. Als die LAN-Switche noch vorrangig von lokalen Einrichtungen (Institute, Lehrstühle, Gebäudenutzergruppen usw.) der FAU betreut wurden, erfolgten VLAN- und Adresszuordnung der Managementschnittstellen zunächst über Eingliederung in eines der örtlich vorhandenen Nutzernetze. Im Zuge des Überganges zur umfassenden, zentralen Betreuung auch der Access-Bereiche durch das RRZE (vgl. Kapitel 7.3), wurden für das Management der LAN-Switche dedizierte VLANs bzw. -IP-Subnetze definiert und die Geräte entsprechend eingeordnet. Dies erhöhte die Übersichtlichkeit, dokumentierte klare Verantwortlichkeiten und vermied Adressreservierungen für Managementzwecke innerhalb von Nutzernetzen bzw. gab entsprechende Belegungen frei. Die Adressierung der Managementnetze und Switche erfolgt(e) aus einem „privaten“, nur innerhalb der FAU geroutetem Adressraum nach einem einheitlichen Schema. Es verwendet Gebäude- und Gerätenummern sodass aus den Hostadressen der Komponenten deren jeweilige Standorte und Identifikationen erkennbar sind. Prinzipiell sind die so definierten Managementschnittstellen der LAN-Switche aus dem gesamten Netz, also insbesondere auch von der zentralen Administration im RRZE, „inline“ erreichbar. Allerdings gib es auch gezielte Eingrenzungen (etwa durch Firewall-Mechanismen oder Access-Listen), um unbefugte Zugriffe zu verhindern.

7.5.2.3 Umsetzung des Out-of-Band-Managements

Die Realisierung des Out-of-Band-Managements (OOB) erfordert definitionsgemäß eine vom Betriebsnetz unabhängige Netzstruktur. Allerdings muss diese zwar nach den Anforderungen des RRZE (vgl. Tabelle in 7.5.2.1) im Grundgerüst alle Bereiche abdecken, nicht aber jede Verästelung der Endgeräteversorgung nachbilden. Demnach sind (nach Möglichkeit) alle Core- und Distributionskomponenten zu erfassen, während Geräte zur Versorgung der Access-Bereiche nur in Ausnahmefällen Zugang über eine separate Struktur erfordern. Neben dem Aufbau der Struktur spielt die Schaffung von Zugangsmöglichkeiten zu den Konsolenschnittstellen eine besondere Rolle. Das aktive OOB-Netz besteht somit nicht nur aus Routern und LAN-Switchen

mit deren LAN/IP-Schnittstellen, sondern enthält darüber hinaus auch dedizierte Terminalserver als wichtige Elemente, die im Bedarfsfall Abbildungen von IP-gestützten Dialogen (Telnet, SSH) auf die seriellen Bedienschnittstellen der Betriebskomponenten vornehmem können.

Die Gestaltung von OOB-Strukturen hängt stark von den jeweiligen Voraussetzungen und machbaren Erweiterungen der verfügbaren passiven Struktur ab. Sie ist also weitgehend von den Möglichkeiten zur Herstellung physischer Verbindungen (ISO Schicht 1), d. h. der Ausprägung der primären Ebene der strukturierten Verkabelung bestimmt bzw. dadurch eingeschränkt. Für das RRZE ergeben sich daraus zwei unterschiedliche Ansätze, und zwar einerseits für die über mehrfache Glasfasertrassen untereinander verbundenen Standorte (Komplex: Erlangen-Innenstadt, Erlangen-Süd) und andererseits solche Bereiche, die über einzelne Strecken (Richtfunk, DSL) mit dem Netzwerk verknüpft sind (z. B. Streulagen Erlangen, Standorte in Bamberg, Nürnberg, Fürth).

OOB-Struktur Erlangen

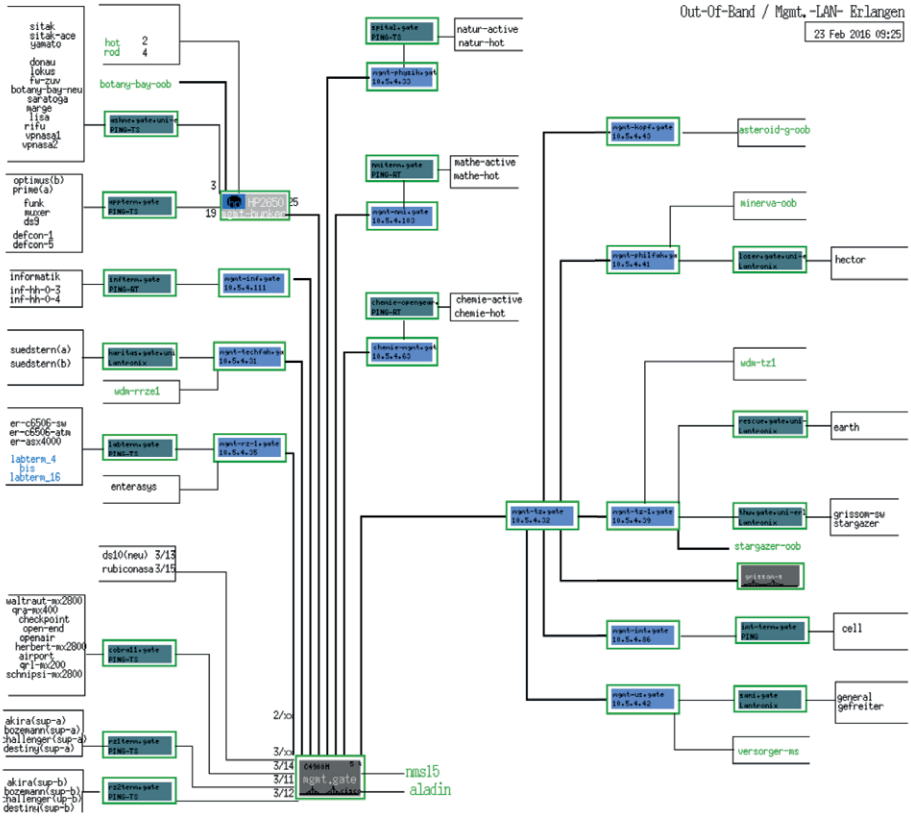
Die Gebäude der FAU innerhalb Erlangens wurden weitgehend im Rahmen von Netzwerkinvestitionsprogrammen strukturiert verkabelt. Dies beinhaltete insbesondere in der primären Ebene die Verlegung von Glasfasern in Verbindungstrassen zwischen den betreffenden Gebäuden bzw. Gebäudegruppen. In diesem Sinne wurden das Erlanger Südgelände, der Röthelheimpark und verteilte Gebäude der Erlanger Innenstadt erschlossen (vgl. Darstellungen in Teil 1, Kapitel 5). Die Anzahl der in den Trassen mehrfach verlegten Kabel reichte dabei aus, um neben den Verbindungen des Betriebsnetzes auch solche eines logisch davon unabhängigen Managementnetzes schalten zu können. Die parallele Wegeführung macht es zwar prinzipiell möglich, dass etwa im Falle eines Trassenschadens (Baggerarbeiten o. ä.) sowohl Betriebs- als auch Managementnetz unterbrochen wären, aber in einem derartigen „Katastrophenfall“ müsste die passive Struktur (vor Ort, nicht unbedingt vom RRZE) repariert werden und wären remote Zugriffe auf betroffene aktive Netzkomponenten zur Fehlerbehandlung kaum hilfreich. Auf eine völlig unabhängige Wegeführung von Betriebs- und Managementnetz oder die Erwägung sonstiger technischer Alternativen konnte in diesem Kontext daher verzichtet werden.

Die betriebliche Nutzung eines OOB-Netzes besteht im Wesentlichen aus gelegentlichen Abfragen, Konfigurationsänderungen oder speziellen Fehlerbehandlungen und erzeugt daher etwa im Vergleich zum Standardbetrieb eine relativ geringe Verkehrslast. Da sich auch die Anzahl darüber verkehrender Geräte in Grenzen hielt (derzeit etwa 50), war es vertretbar, diesen gesamten Netzbereich trotz seiner großen Ausbreitung als ein einziges lokales (LAN) und bzgl. IP-flaches Netz, also mit einer einzigen IP-Netzwerkadresse, zu gestalten. Das Netzwerk kommt somit ohne internes Routing

bzw. interne Router aus und ist daher entsprechend „einfach“ aufgebaut. Es besteht im Kern nur aus LAN-Switchen, die bedarfsgemäß aufgestellt, über verfügbare Kabelwege verbunden (vernetzt) sind. Die Endgeräteanschlüsse der Switche (Ports) führen auf dedizierte Managementschnittstellen (Ethernet-Ports) oder über Terminalserver auf die Konsolenschnittstellen der ausgewählten Komponenten des Betriebsnetzes. Die Komponenten des OOB-Netzes selbst werden diesbezüglich „inline“ gemanagt, also über ihre IP-Adressen innerhalb dieses Netzes angesprochen.

Die Struktur des Erlanger LANs zur Realisierung des Out-of-Band-Managements ist in der Abbildung „OOB-LAN Erlangen“ dargestellt (Stand Februar 2016).

OOB-LAN Erlangen, 2016



Sie ist baumförmig aufgebaut, und zwar mit einer kombinierten LAN-Switch- und Router-Komponente (Switch/Router „mgmt“) im Mittelpunkt (Standort Rechenzentrum) und einer damit verknüpften Unterverteilung (LAN-Switch „mgmt-tz“) für den Bereich der Erlanger Innenstadt (Standort Telefonzentrale). Daran direkt angeschlossene LAN-Switche (z. B. „mgmt-rz-1“ im „großen“ Rechnerraum, „mgmt-physik“ im Gebäudekomplex Biologie/Physik oder „mgmt-us“ im Röthelheimpark) verbreiten das LAN in die Nähe von Komponenten des Betriebsnetzes, die per OOB erreichbar sein sollen. Die Verbindungen zu diesen Komponenten führen meist über Terminalserver zu deren Konsolenschnittstellen (z. B. von „mgmt-techfak“ über „karitas“ zu „suedstern“), werden aber teilweise auch per Kabel direkt zwischen Switch und verfügbaren Ethernet-Management-Schnittstellen hergestellt (z. B. von „mgmt-tz-1“ zu „stargazer-oob“). Die zentrale Verteilkomponente des OOB-LANs verknüpft als Router das LAN bzw. das zugehörige, flache IP-Netz mit anderen Managementnetzen, z. B. dem Netz der Managementserver, und realisiert einen Übergang in das Betriebsnetz.

Im Rahmen der verfügbaren strukturierten Verkabelung genügt die bewusst einfach gehaltene Struktur den Anforderungen und ist sowohl in der Ausbreitung als auch in der Dichte durch Einfügen zusätzlicher Endpunkte im Erlanger Süd- und Innenstadtbereich bei Bedarf weiter ausbaubar.

OOB-Struktur für Fernbereiche

Für Standorte, die nicht im Sinne der „klassischen“ strukturierten Verkabelung über mehrfach nutzbare Kabeltrassen mit anderen verbunden sind, erfordert ein betriebsnetzunabhängiges Managementnetz Lösungen mit anderen Übertragungstechniken. Hierzu wurden verschiedene punktuell auch umgesetzte Ansätze verfolgt, wie etwa eigens gemietete Leitungen (Festverbindungen bzw. Hauptanschlüsse für Direktruf (HfD) der Telekom), Modembetrieb über das Fernsprechnetz (Wählverbindungen) oder auch das Multiplexen von Richtfunkverbindungen des Betriebsnetzes (Mehrfachnutzung von Funkstrecken auf Übertragungsebene). Solche einzelnen, je nach Standort individuell gestalteten Lösungen haben sich in der Praxis nur bedingt bewährt. So stellten z. B. Fest- und Wählverbindungen serielle Schnittstellen bereit, die in der Regel nur über spezielle Wandlungskomponenten netztechnisch zu integrieren und in ihrer Leistungsfähigkeit (Übertragungsgeschwindigkeit) sehr beschränkt waren. Zudem fielen zur Bereitstellung und Nutzung der entsprechenden Dienste nicht unerhebliche, monatliche Gebühren an, die unter anderem von Geschwindigkeiten, Entfernungen der Endpunkte (HfD) oder genutzten Verbindungszeiten (Wählbetrieb) abhingen. Die Nutzung von Teilkanälen von Richtfunkstrecken erforderte zwar keine zusätzlichen, laufenden Gebühren, wohl aber spezifische, technische Vorkehrungen. Die parallele Streckenführung über Funkverbindungen war zudem nur bedingt OOB-tauglich.

An die Stelle solcher einzelnen, individuell gestalteten Ansätze trat daher ein erweiterbares Gesamtkonzept, das auf jeden Standort anwendbar war und vom RRZE schrittweise umgesetzt wurde.

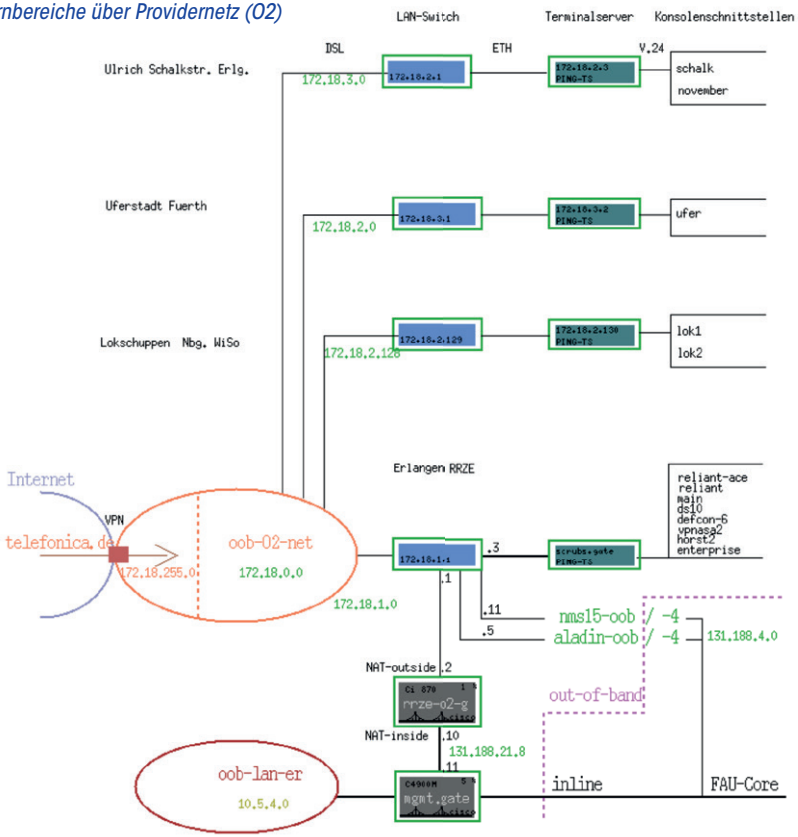
Dessen Grundpfeiler sind:

- Internet eines externen Providers (das RRZE hat dazu eine Lösung der Firma O2 gewählt)
- DSL-Internetanschlüsse des Providers für jeden anzubindenden Standort (einschließlich des Zentrums in Erlangen)
- Geschlossenes Netz (Closed User Group) innerhalb des Internets (organisiert vom Provider) zur Verknüpfung der verteilten Standorte und des Zentrums

Das dedizierte Internet verbindet also die Standorte über deren Zugänge untereinander bzw. mit dem zentralen Standort im RRZE und ist bezüglich Struktur und Betrieb völlig unabhängig vom Universitätsnetz. Darüber sind die betreffenden Komponenten des Betriebsnetzes über lokale Übergänge und Anpassungen auf unabhängigen Wegen, also „out-of-band“, erreichbar und zu managen. Die Übersicht „OOB-Fernbereiche über Providernetz (O2)“ auf S. 174 stellt z. B. dar, wie ausgehend vom Managementserver „aladin“ (unten rechts) die Konsolenschnittstelle des Routers „schalk“ (oben rechts) über den (DSL-)Zugangsswitch im Rechenzentrum, das OOB-Netz („oob-O2-net“), den (DSL-)Zugangsswitch in der Erlanger Ulrich-Schalk-Straße (Streulage) und einen Terminalserver vor Ort erreichbar ist. Die Abbildung zeigt auch, wie das OOB der Fernbereiche mit dem des Inline-Managements sowie dem Betriebsnetz über einen entsprechenden Übergang („rrze-o2“) verknüpft und somit in die Gesamtstruktur integriert ist.

Ebenfalls in der Abbildung dargestellt ist eine ergänzende Schnittstelle zwischen dem geschlossenen O2-Netz und dem offenen Internet, die vom Übergang des FAU-Betriebsnetzes zum Wissenschaftsnetz (WiN) unabhängig ist. Darüber lassen sich mit entsprechender Berechtigung nach erfolgter Identifikation über die OOB-Strukturen Operationen des Managements durchführen, wie etwa Abrufe von Statusinformationen, (geringe) Konfigurationsänderungen oder die Behandlung außergewöhnlicher, gravierender Störfälle. Solche Möglichkeiten des externen Zuganges von Punkten, die außerhalb des FAU-Netzes liegen (z. B. Heimarbeitsplätzen der Administratoren), sind generell auch über den WiN-Zugang des Betriebsnetzes gegeben, setzen allerdings voraus, dass zumindest alle zu durchlaufenden Komponenten vom FAU-Internetanschluss bis zu den Managementservern funktionsfähig sind, was besonders in schweren Problemfällen (Beispiel: Brand im Serverraum) nicht unbedingt gegeben ist. Die O2-Lösung bietet somit insbesondere für Notfälle eine gangbare Option.

OOB-Fernbereiche über Providernetz (O2)

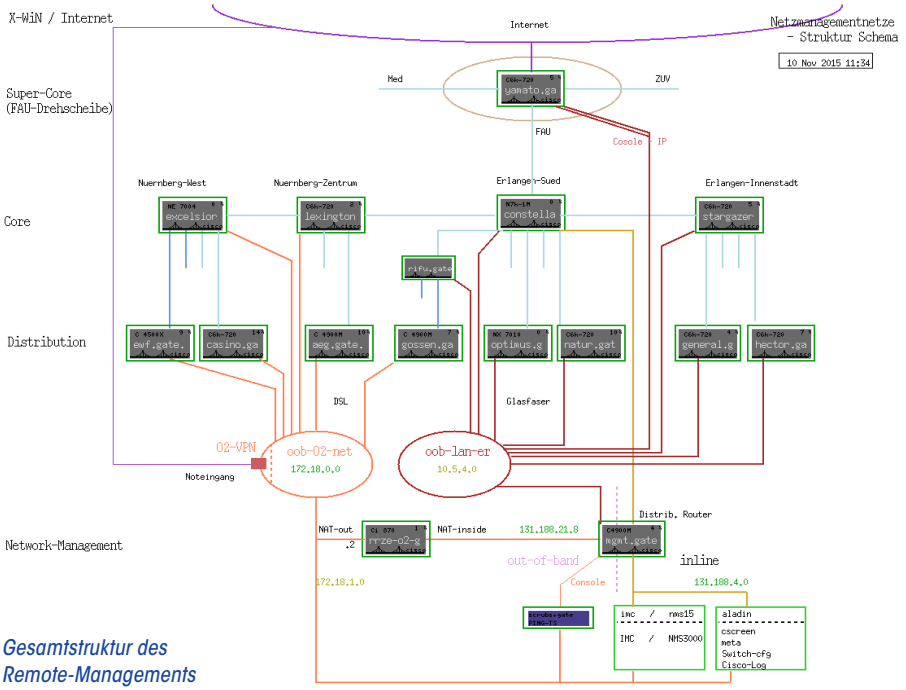


Zusammenfassung des Remote-Managements

Die Abbildung zur „Gesamtstruktur des Remote-Managements“ fasst die entsprechende Vernetzung zusammen und skizziert, wie die gestellten Anforderungen (Kapitel 7.5.2.1) bzgl. des FAU-Netzes umgesetzt wurden (Stand 2015). Der Überblick stellt das Betriebsnetz (ohne Berücksichtigung von Redundanzen) durch die Drehscheibe, die vier Cores, eine prinzipielle Auswahl von Distributionsroutern sowie deren Verbindungen untereinander vereinfacht dar (Glas: graue, RiFu: blaue Linien). Access-Komponenten sind zur besseren Übersicht nicht explizit angeführt, zumal sie in

der Regel nur Inline (über ihre Distributionsrouter) gemanagt werden. Die rötlichen Linien stehen für die Verbindungen zwischen OOB-Netzen und den Zugängen zu den Netzkomponenten über deren Konsolen oder dedizierten Ethernet/IP-Schnittstellen.

Eine besondere Rolle zur Verknüpfung der Strukturen spielt ein zentraler Management-Router („mgmt.gate“), der mit dem OOB-LAN direkt und dem OOB-O2 über eine zwischengeschaltete Kontrollkomponente („rrze-o2“) verbunden ist. Zudem steht er innerhalb des Betriebsnetzes für einen eigenen Distributionsbereich, der im Sinne der Architektur an den Core Erlangen-Süd (Router „constellation“) angebunden ist (gelb/braune Linie). Zu seinem Bereich gehören neben den OOB-Netzen auch Netze zentraler Managementserver (z. B. „aladin“). Da er als Teil des Betriebsnetzes auch mit den Inline-Netzen verbunden ist, kann er zwischen allen Managementnetzen vermitteln.



Gesamtstruktur des Remote-Managements

7.6 Aspekte von Datenschutz und Netzsicherheit

Bereits mit dem Beginn des Betriebs universeller Rechenanlagen und der Einführung darauf aufbauender Elektronischer Datenverarbeitung (EDV) für unterschiedliche Nutzergruppen und Anwendungsfelder entstand auch eine Problematik von Datenschutz und Sicherheit. Sie stellte sich z. B. im Zusammenhang mit unbefugter Nutzung von Betriebsmitteln oder Zugriffen auf schützenswerte Informationen. Mit den folgenden, enormen Entwicklungen von IT-Diensten und (globaler) Vernetzung stieg auch das Gefährdungspotential ständig an. Zu den ersten Schutzmaßnahmen gehörte die Einführung von Benutzerkennungen und Passwörtern, über die Nutzer identifiziert und auf Zugangsberechtigung überprüft werden konnten. Dieses elementare Verfahren ist auch aktuell noch Teil der Kontrollmechanismen zur Verhinderung unberechtigter Zugriffe auf Betriebsmittel oder gespeicherte Daten. Allerdings bedingt seine Wirksamkeit nach wie vor eine sorgsame Handhabung durch die Benutzer, die z. B. das Weitergeben ihrer Kennungen an andere Personen ausschließt (was schon im Kontext zentraler EDV-Anlagen nicht selten zur Vereinfachung praktiziert wurde). Maßnahmen zur Erhöhung von Sicherheit und Datenschutz im IT-Bereich sind in der Regel mit Einschränkungen oder Unbequemlichkeiten verbunden (schon das „richtige“ Setzen und Merken von Passwörtern wird oft als lästig empfunden), die aber in Anbetracht jeweiliger Erfordernisse und potentieller, negativer Konsequenzen in Kauf zu nehmen sind.

Bezüglich der Gefährdung von Sicherheit und Datenschutz lassen sich drei Problemfelder nennen, die allerdings nicht ganz unabhängig voneinander zu sehen sind. Das betrifft die Benutzer und ihr Verhalten einschließlich des Betriebs persönlicher (dezentraler) Rechensysteme, zentral betriebene Systeme und IT-Dienste sowie die Netzstrukturen als Basis weitgehend freizügiger Kommunikation.

7.6.1 Rechtliche Problematik

Die FAU und das RRZE als IT-Dienstleister tragen für die (reguläre) Nutzung der Betriebsmittel in verschiedener Hinsicht Verantwortung, dies gilt nach innen gegenüber den Mitgliedern und Einrichtungen der Universität ebenso wie nach außen z. B. gegenüber externen Personen und Institutionen. So können z. B. Verstöße einzelner Benutzer der FAU gegen Regeln und Gesetze zu Haftungsschäden und finanziellen Belastungen der Universität führen. Es gehört zu den Aufgaben der FAU und des RRZE für Folgendes zu sorgen:

- Zweckbestimmte Nutzung (im Sinne von Forschung und Lehre) bereitgestellter IT-Ressourcen (z. B. Rechensysteme, Netzstrukturen, Personal) in Verantwortung gegenüber Staat und Geldgeber

- Datenintegrität und Vertraulichkeit von Forschungsvorgängen und -resultaten in Verantwortung gegenüber Angehörigen der FAU
- Legales Verhalten seiner Nutzer im Sinne des allgemeinen Rechts, insbesondere im IT-Zusammenhang (z. B. durch Verhinderung von Urheberrechtsverletzungen über das Betreiben von Filesharing (Filme, CDs) oder anonymer FTP-Server im Kontext der FAU-Strukturen) in Verantwortung gegenüber Personen und Institutionen außerhalb der FAU

RRZE und FAU stellen sich diesen Verantwortlichkeiten durch Festlegung (interner) Regularien und Richtlinien sowie durch gezielte organisatorische und technische Maßnahmen zur Verhinderung von Missbräuchen oder Angriffen.

7.6.2 Gefährdung durch Nutzerverhalten und dezentral betreute Systeme

Die Gruppe der Benutzer gilt als Sicherheitsrisiko Nr. 1. Das betrifft unter anderem den fahrlässigen Umgang mit Benutzerkennungen, Verwendung unsicherer (unverschlüsselter) Programme oder naivem Umgang mit verleitenden Angeboten über E-Mails (Phishing Mails) oder Webseiten (irreführende Links) aus dem Internet. Aber auch kriminelle Handlungen, wie der Missbrauch von Betriebsmitteln, gezielte Spionage oder Sabotage gehören zu den gefährdenden Aktivitäten und sind dem internen oder externen Nutzerkreis zuzuordnen.

Da die Nutzung zentraler IT-Dienste weitgehend über lokale, dezentrale Systeme (PCs, Workstations, Institutsrechner usw.) erfolgt, bilden diese und der Umgang mit ihnen ein zusätzliches Gefahrenpotential. Beispiele aus der Praxis sind Systeme, die

- angreifbar über (bekannte) Schwachstellen sind,
- veraltet sind (allerdings oft im genutzten Kontext schwer zu ersetzen),
- unzureichend gepflegt sind (fehlende Aktualisierungen, Korrekturen, Patchungen),
- frei zugänglich sind, ohne Benutzerkennung und Passwort,
- ohne Virenschutz sind (trotz verfügbarer Software),
- mit selbstinstallierter Software versehen sind (z. B. aus dem Internet).

Systeme mit derartigen Schwachpunkten sind z. B. anfällig gegen das Einschleppen von Schadsoftware, die im ungünstigen Fall das gesamte IT-System der FAU stören oder gar „lahmlegen“ können. Um die Gefährdungen durch das Verhalten von Nutzern bzw. deren Systemen möglichst gering zu halten, weisen RRZE und FAU eindringlich auf entsprechende Richtlinien, Regeln, gesetzliche Bestimmungen hin und geben regelmäßig Anleitungen, technische Hilfen und Empfehlungen zur Minderung von Risiken.

Bezüglich der Administration dezentraler Systeme werden folgende Maßnahmen vorgeschlagen:

- Benutzer installieren keine Software
- Sensibilisieren: Software aus dem Internet birgt Risiken
- Verwendung sicherer Programme/Protokolle
- z. B. ssh statt telnet, https statt http,
- wechselnde Sitzungsschlüssel gemäß PFS (Perfect Forward Secrecy)
- Systeme schwerer angreifbar machen
- Systemversionen auf aktuellem Stand halten
- Systeme (automatisch) patchen, (Korrekturen einarbeiten)
- Keine Benutzeraccounts ohne Passwörter
- Verwendung „schwer erratbarer“ Passwörter (eventuell erzwingen)
- Virenschutz, gemäß verfügbarer Software
- Einschränkung der erreichbaren Dienste bzw. gezieltes Freischalten
- Absicherung durch interne Paketfilter oder Firewall-Mechanismen (sofern in den Systemen verfügbar, die Methoden sind grob mit denen der im Abschnitt 7.6.4 beschriebenen Netzmaßnahmen vergleichbar)
- Überwachung der Systeme (Auditing)
- Regelmäßige Überprüfung ergriffener Schutzmaßnahmen und deren Wirksamkeit
- Protokollierung von Vorgängen (Logging) und Analyse der Daten
- Ausnutzen betriebssystemabhängiger Hilfen, z. B. Angabe „Letzter Login-Versuch“ (Unix-„last“) oder Aufzeichnung von Anmeldevorgängen (Windows-Registry, Login-Monitoring)

Die Umsetzung von Schutzmaßnahmen ist in der Regel mit einem hohen administrativen Aufwand verbunden und erfordert entsprechendes Grundlagenwissen. Sie kann daher von Einzelpersonen oder lokalen Betreuern oft nur bedingt geleistet werden. Das RRZE bietet daher als Alternative eine zentrale Betreuung dezentraler Systeme an, die somit eine komplette Systempflege und Softwareverteilung für lokale Einrichtungen enthält. Neben der Betreuung der Rechensysteme stellt das RRZE auch lokal bezogene IT-Dienste über zentralen Service zur Verfügung. Das gilt z. B. für Internetpräsenzen, Mail-Dienste oder Datenhaltung für verteilte Einrichtungen der Universität. Die wachsende Inanspruchnahme derart zentralisierter Organisation leistet(e) einen erheblichen Beitrag zur Gewährleistung von Datenschutz und Sicherheit im gesamten IT-Komplex der Universität.

7.6.3 Gefährdung zentraler Systeme und IT-Dienste

Die vom RRZE betreuten zentralen Systeme und angebotenen Dienste stellen aufgrund ihrer herausragenden Bedeutung für die Informationsverarbeitung der Universität besonders „lohnende Objekte“ zur missbräuchlichen Nutzung oder für gezielte Angriffe dar und sind daher entsprechend gefährdet. Sie stehen im Fokus, da sie

- allgemein publik und im Prinzip global erreichbar sind
- vielfältige sensible Daten halten, z. B. bezüglich Personen (Angehörige der FAU), Einrichtungen (Institute, Lehrstühle usw.) oder Forschungen (Vorhaben, Resultate)
- spezielle, leistungsfähige und, in Bezug auf Beschaffung und Unterhalt, „teure“ Betriebsmittel zweckgebunden bereitstellen ((Höchstleistungs-)Rechner- und Speicherkapazitäten)
- für den allgemeinen Hochschulbetrieb unverzichtbar sind

Die Betreuung zentraler Server und Dienste gehört zu den Kernaufgaben des RRZE und erfolgt entsprechend professionell auch unter Gesichtspunkten des Datenschutzes. Selbstverständlich gelten dabei auch die im vorangegangenen Abschnitt (7.6.2) genannten Richtlinien und Maßnahmen bzgl. Nutzerverhalten, betriebener Einzelsysteme oder verschiedener Kontrollmechanismen. Das beinhaltet z. B. ein schritthaltendes Aktualisieren von System- und Anwendungssoftware oder den Einsatz von Absicherungsmethoden auf aktuellem technischen Stand gegen alte und neu entstehende Bedrohungsszenarien.

Einen herausragenden Beitrag zur Gewährleistung von Kontrolle und Datenschutz leistet das vom RRZE entwickelte Identity Management (IdM, vgl. Kapitel 7.2.2). Als Tor zum IT-Komplex der FAU bietet es den Benutzern einen zentralen Eingang mit Zugangskontrolle über Kennungen und Passwörter, ordnet ihnen Zugriffsberechtigungen zu und überwacht deren Einhaltung. Über einen einzigen Identifizierungsvorgang (Single Sign-on) erhalten Benutzer Zugang zu den verschiedenen Servern und Diensten, gemäß ihren eingetragenen Befugnissen.

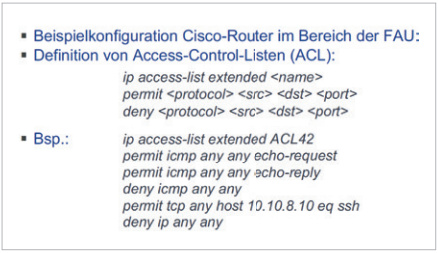
Ergänzende Maßnahmen zur Absicherung von Rechnern, Programmen oder Daten erfolgen im Rahmen spezifischer Systembetreuung, dies auch in enger Absprache mit den Netzadministratoren und deren verfügbaren Kontrollmöglichkeiten.

7.6.4 Gefährdung über das Kommunikationssystem

Das IP-basierte Kommunikationsnetz der FAU bietet einschließlich seiner Integration in das Internet grundsätzlich eine Infrastruktur zum freizügigen Informationsaustausch („jeder mit jedem“). Insbesondere gilt das auch für die Angehörigen der Universität zur Ermöglichung einer unbehinderten Ausübung von Forschung und Lehre. Allerdings zeigten Erfahrungen, dass ein stabiler, gesicherter Netzbetrieb nur unter gewissen Einschränkungen möglicher Kommunikationsbeziehungen erreicht werden kann. Zudem bietet die Netztechnik auch Mittel, über begrenzende Verkehrssteuerung (per Routing) unzulässige Zugriffe auf angeschlossene Systeme zu verhindern.

Einen gewissen Schutz (gegen Angriffe oder Eindringen von außen) bedeutet die Verwendung „privater“ Adressen, etwa für Netze von Arbeitsplatzrechnern oder „leicht“ angreifbaren Endgeräten (Drucker, Kopierer). Die so eingeordneten Geräte sind damit über das Internet nicht erreichbar bzw. angreifbar, können aber im Bedarfsfall unter Nutzung entsprechender Umsetzungsmechanismen (NAT) selbst Verbindungen zu Zielen außerhalb des FAU-Netzes aufbauen.

Eine differenziertere und gezielter zu steuernde Methode stellt der Einsatz von Filterlisten bzw. Access-Listen (ACLs) in den wegelenkenden Routern dar. Derartige Filterlisten können in den Routern pro Interface definiert werden. Sie definieren Regeln, nach denen IP-Pakete durchgelassen (weitergeleitet) oder gesperrt (verworfen) werden. Dies wird über Vergleiche der Regeln mit den Kopfinformationen (Header) der zu prüfenden Pakete entschieden. Auf diese Weise können z. B. einzelne Geräte und komplette Subnetze vor Zugriffen geschützt aber auch bestimmte Protokolle bzw. Anwendungen gesperrt werden. Einen Eindruck über den Aufbau von Access-Listen gibt die abgebildete Darstellung „ACL Definition auf Cisco-Router“. Im darin angegebenen Beispiel „ACL42“ sind an der betreffenden Schnittstelle in beiden Richtungen Ping-Anfragen und -Antworten erlaubt sowie Dialogsitzungen von jedem Endgerät („any“) per SSH zum Host mit der Adresse „10.10.8.10“ zugelassen. Alle sonstigen IP-Verbindungen werden unterbunden. Die Access-Listen sind in der Praxis meist umfangreicher und komplexer als im angeführten Beispiel. Ihre Definition und Pflege ist in der Regel aufwendig, erfordert spezielle Kenntnisse, führt nicht selten zu unübersichtlichen Anweisungsfolgen und ist daher fehleranfällig. Hier bietet das vom RRZE entwickelte Tool FAUST effektive Unterstützung, das aus



ACL -Definition auf Cisco-Router

Angaben in einer anwendungsorientierten Form Kommandos zur Konfigurierung von (Cisco-)Routern erzeugt (vgl. Kapitel 7.4.3.5). Insbesondere ermöglicht es in akuten Fällen, die z. B. aus Sicherheitsgründen das Sperren eines Rechners an verschiedenen Stellen des Netzes erfordern, schnell und wirksam in einfacher Weise zu reagieren.

Im Kommunikationsnetz der FAU werden Access-Listen am Übergang zum Internet und allen Schnittstellen zu den Subnetzen eingesetzt. Sie enthalten elementare „Standardregeln“ und solche, die auf Anforderungen der betreffenden Nutzer(-gruppen) zum differenzierten Schutz ihrer Systeme und Netze konfiguriert werden.

Die in den Routern der FAU definierten Access-Listen bieten auf Netzebene einen flexiblen, schnell arbeitenden Grundschutz für die angeschlossenen Systeme und Dienste. (ihre Abarbeitung erfolgt in Geräten aktueller Router-Generation über „Switching“-Technologie, d. h. nicht mehr über ihre zentralen Prozessoren). Dennoch können mit ihnen nicht alle Anforderungen an Schutz und Sicherheit des Kommunikationsnetzes abgedeckt werden. Die Paketfilterung in den Routern ist effektiv einsetzbar, hat aber auch verschiedene Schwachpunkte wie bspw.

- Erstellung der Listen ist fehleranfällig, insbesondere bei komplexer Schutzproblematik
- Lange Listen sind oft unübersichtlich, ihre Wirkung schwer zu verifizieren
- Kontrollen wirken nicht innerhalb von LANs/Subnetzen
- Einzelpaketanalyse erkennt den Kontext von Verbindungsvorgängen nur bedingt
- Attacken über komplexe Paketfolgen sind nicht erkennbar
- Anwendungserkennung über TCP-Ports kann durch missbräuchliche Setzung umgangen bzw. fehlgeleitet werden
- Prüfungen sind beschränkt auf IP/TCP (Schicht 3/4), d. h. ohne Analysen von Daten der darüberliegenden Protokolle (Schichten 5 und höher)

Trotz der angeführten Schwächen bleiben für die Access-Listen als positive Punkte hervorzuheben:

- Flächendeckend im Netz einsetzbar, an allen LAN/Subnetzschnittstellen der Router
- Keine spezifischen Kosten verursachend, da konfigurierbarer Bestandteil der Router
- Wirksam bei Prüfungen von Kommunikationsbeziehungen auf Zulässigkeit
- Anpassbar an Anforderungen der Nutzer(-gruppen) bzgl. Endgeräten oder Subnetzen
- Elementar schützend auch gegen verschiedene Angriffsformen
- Flexibel reaktionsfähig auf einzelne Störungen, (z. B. Sperrung auffälliger Hosts)
- Vereinfachend und fehlerreduzierend konfigurierbar bei Einsatz von FAUST

Einen weitergehenden Schutz gegen Missbrauch und Angriffe bieten sogenannte Firewalls, die als dedizierte Komponenten an besonders kritischen Punkten des Netzes eingesetzt werden können. Sie sind in der Lage, übertragene Protokolle und Daten zu analysieren und so zum Beispiel einfache Anmeldevorgänge (Logins) zu

verfolgen (unter anderem Identifizierung von Benutzern) oder Aufrufe und Zugriffe auf bestimmte Anwendungen und Dienste (Web, Datenbanken usw.) zu erkennen. Über ein darauf aufbauendes, administriertes Regelsystem können, ähnlich den ACLs in Routern, Kommunikationsvorgänge gesperrt oder frei gegeben werden. Je nach Ausprägung der Firewall lassen sich auch verschiedene Versuche des Einschleppens von Schadsoftware oder Viren abblocken. Da die Eindringverfahren ständig variieren bzw. neuartige hinzukommen, müssen die Analyseverfahren zur Abwehr stets auf aktuellem Stand gehalten werden.

Erste Firewalls wurden über entsprechende Software auf Basis herkömmlicher Serversysteme realisiert, stießen aber auch je nach Anforderungen an die Grenzen ihrer Leistungsfähigkeit, wodurch sie etwa bei der Abarbeitung von Regeln merkbare Verzögerungen im Durchsatz verursachten. Alternativ dazu wurden dedizierte Firewall-Komponenten verfügbar, wie z. B. Geräte verschiedener Größenordnung des Router-Hersteller Cisco aus dessen „ASA"-Familie (Adaptive Security Appliances, ASA). Cisco verfolgte auch einen weiteren Ansatz, der ihre Router der 6500er-Serie (vgl. Kapitel 6.2.3.4) über spezielle Einschubkarten (Firewall-Module) um Firewall-Funktionalität erweiterbar machte. Im Vergleich zur Schaltung von Firewalls zwischen zwei Komponenten bot er mehr Möglichkeiten zu mehr Integration und besseren Verteilung im Netz (angewandt im Kliniknetz). Am oberen Ende des technisch Machbaren (bzgl. Funktionsumfang und (Durchsatz-)Leistung), befinden sich speziell entwickelte Geräte der „Next Generation Firewalls". Sie ermöglichen eine besonders hohe Schutzwirkung und sind individuell konfigurierbar, also auf jeweilige Erfordernisse anpassbar. Das Ausnutzen ihrer Flexibilität bedeutet aber andererseits auch einen beliebig hohen Konfigurationsaufwand. Ebenso ist die Beobachtung des Betriebsverhaltens (z. B. durch Auswertung von Protokolldaten oder Analyse von Alarmmeldungen) äußerst (personal-)aufwendig und erfordert sehr spezielles Fachwissen. Die Geräte verursachen (im Vergleich zu anderen Netzkomponenten) zudem sehr hohe Anschaffungs- und laufende Kosten.

In vielen Fällen helfen Access-Listen und Firewalls auch beim Schutz vor Angriffen aus dem Netz, gegen gezielte, ausgeklügelte Angriffe auf das Kommunikationsnetz oder dessen Teilnehmer wirken sie aber nur bedingt. Auf die Abwehr derartiger Attacken sind sogenannte „Intrusion Detection Systeme" (IDS) spezialisiert. Bezogen auf das Netz sind sie auf dedizierten Komponenten oder als ergänzende Bausteine von Firewalls realisiert. Als passive Beobachter sammeln und analysieren sie den Netzverkehr und versuchen zu erkennen, ob

- ein potentieller Angreifer nach Sicherheitslücken sucht
- gerade ein Angriff (von innen oder außen) stattfindet
- die Firewall Schlupflöcher hat

- ein Angreifer erfolgreich gewesen ist
- Informationen geändert bzw. entwendet wurden

Ein IDS lernt (mit eigener „Intelligenz“) durch seine Beobachtungen „normales“ Verhalten und triggert dementsprechend auf „abnormale“ Kommunikationsvorgänge. Zusätzlich arbeitet es regelbasiert über Definitionen sogenannter „Signaturen“ (Angriffsmuster), anhand derer Beobachtungen als Angriffe zu bewerten sind. Die Einrichtung eines IDS erfordert zunächst eine Anpassung an lokale Bedingungen. Wegen der immer wieder neu vorkommenden Angriffsszenarien sind die Signaturen stets aktuell zu halten. Auch mit der Sichtung und Auswertung der Ereignismeldungen, die in der Praxis trotz Automatismen und sorgfältiger Konfigurierung in der Regel sehr umfangreich und oft nicht sicherheitsrelevant sind, ist ein hoher Aufwand verbunden. Wie die Firewalls eignen sich Intrusion Detection Systeme hauptsächlich für den Einsatz an ausgewählten Punkten des Netzes mit besonderem Schutzbedarf, wie etwa am Übergang zwischen dem Wissenschafts- und dem Verwaltungsnetz (ZUV) der Universität. Ansonsten ist ihr Einsatz wegen der hohen Beschaffungs- und Wartungskosten sowie dem enormen, personellen Betreuungsaufwand kaum zu rechtfertigen.

7.6.5 Zusammenfassung Sicherheit FAU

Die Sicherheitsaspekte der FAU im Allgemeinen und der Informationstechnik im Besonderen umfassen ein weites, vielfältiges Spektrum, dem durch unterschiedliche Maßnahmen zu begegnen ist.

Das RRZE, das als IT-Dienstleister der Universität unter anderem den zugehörigen Nutzerkreis bedient, zentrale und dezentrale Serversysteme betreut sowie das Kommunikationsnetz betreibt, ist somit auch für damit in Zusammenhang stehende IT-Sicherheit zuständig. So gehört das Sorgen um einen höchstmöglichen Datenschutz und die Umsetzung entsprechender Maßnahmen zu den originären Aufgaben des Rechenzentrums.

Eine wesentliche Grundlage zur Schaffung von Betriebssicherheit und Datenschutz bilden die Benutzerrichtlinien des Rechenzentrums und das Betriebskonzept des Netzes [*FauRd*]. Sie setzen Rahmen für Verantwortlichkeiten, betriebliche Regeln oder zulässiges Nutzerverhalten. Das RRZE weist daher die Angehörigen der Universität regelmäßig auf diese Regularien hin (z. B. über Benutzerinformationen oder Kolloquien) und dringt auf deren Einhaltung.

Die Umsetzung technischer Maßnahmen (vgl. Abschnitt 7.6.2) erfordert ein hohes Fachwissen, das in den lokalen Einrichtungen bzw. bei deren IT-Betreuern nur bedingt vorhanden ist bzw. sein kann. Deshalb bietet das RRZE ihnen vielfältige Beratung

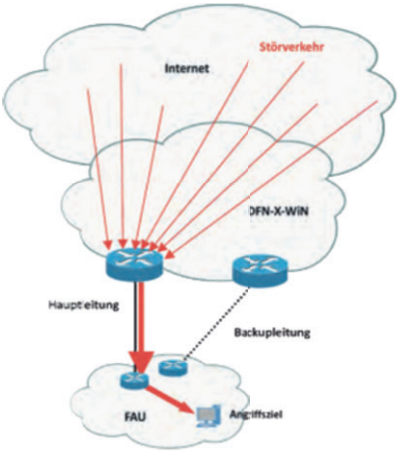
und Unterstützung wie beispielsweise bei der Systemkonfiguration, Bereitstellung von Antiviren-Software oder dem Einspielen von Patches bis hin zu einer kompletten, zentralen Betreuung dezentraler Systeme.

Bezüglich seiner (eigenen) Server und Dienste orientiert sich das RRZE weitgehend an den technisch möglichen Maßnahmen (vgl. Abschnitt 7.6.3). Je nach System gehören dazu gezielter Zugriffsschutz von Servern und Diensten, Protokollanalyse von Ereignissen oder Sicherheitsprüfungen mit Tests und Auswertungen.

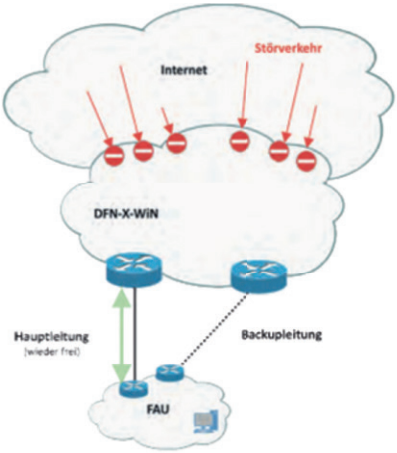
Eine Grundsicherung des Kommunikationsnetzes der FAU leisten auf allen beteiligten Routern implementierte Accesslisten, die den Datenverkehr auf Zulässigkeit prüfen und regulieren. Pro Subnetz verhindern sie im Minimum sogenanntes Spoofing, d. h. sie sperren IP-Pakete mit Absenderadressen aus dem Ziel-Subnetz (ankommend) oder mit nicht aus dem Subnetz stammenden Absendern (ausgehend). Ansonsten werden sie nach übergeordneten Erfordernissen (Einschätzung RRZE) oder auf Anforderungen lokaler IT-Betreuer spezifisch gesetzt. Besonders umfangreich sind die Prüfungen der Accessliste an der Außenschnittstelle zum Internet bzw. zum X-WiN). Dort werden z.B. als kritisch beurteilte TCP-Ports oder auch Pakete „berüchtigter“ Absender gesperrt bzw. entsprechende Pakete verworfen. An diesem Übergang betreibt das RRZE auch einen VPN-Server (vgl. Kapitel 6.2.3.3) als Kontrollinstanz, über die sich Angehörige der Universität identifizieren und bei entsprechender Berechtigung z.B. auf Geräte mit privaten Adressen oder auf sonst speziell geschützte Systeme zugreifen können.

Eine andere Art von Missbrauch an der Außenschnittstelle betrifft weniger einzelne, unbefugte Eindringversuche, sondern sogenannte volumenbasierte „DoS“-Angriffe (Denial-of-Service, kurz DoS), bei denen das Datennetz durch gezieltes Fluten mit Datenpaketen von zigtausenden infizierten Endsystemen aus dem Internet gestört wird. Selbst wenn diese Pakete am Eingang abgelehnt werden, erzeugen sie doch eine so hohe Last, dass kein produktiver Verkehr mehr möglich ist. RRZE und DFN-Verein haben deshalb technische Möglichkeiten entwickelt, um in gemeinsamen Aktionen solche DoS-Attacken abwehren bzw. deren Auswirkungen wirksam abmildern zu können. Da immer wieder neue Angriffsmuster auftreten, müssen auch die Gegenmaßnahmen (Mitigation) damit Schritt halten, d. h. entsprechend angepasst oder erweitert werden.

In einem bildlich dargestellten Beispiel auf S. 185 beziehen sich die Angriffe auf ein bestimmtes Zielsystem der Universität. Es wird gezeigt, wie die Internetzugangsleitung der FAU durch einen massiven Störverkehr von außen verstopft und die angeschlossenen Einrichtungen dadurch nicht erreichbar sind („FAU offline durch massiven Störverkehr“), während nach erfolgreicher Mitigation der identifizierte Störverkehr vom DFN ausgefiltert wird, bevor er die FAU erreichen kann („FAU online nach



FAU offline durch massiven Störverkehr



FAU online nach ausgefiltertem Störverkehr

ausgefiltertem Störverkehr“). Das ursprünglich angegriffene Ziel ist zwar in diesem Szenario weiterhin nicht erreichbar, für die übrigen Systeme und Einrichtungen gilt aber wieder normaler Betrieb.

Dedizierte Firewalls, deren Kontrollmöglichkeiten über die von ACLs hinausgehen, werden hauptsächlich im Zusammenhang mit dem Verwaltungsnetz (ZUV) eingesetzt, und zwar mit einer leistungsstarken Komponente (Cisco ASA 5500) zwischen ZUV- und Wissenschaftsnetz der Universität sowie mehreren, kleineren Geräten der ASA-Familie zur Verknüpfung der verteilten ZUV-Bereiche über das FAU-Netz (vgl. Darstellung „ZUV-Netzstruktur“, Kapitel 6.5.2). Der Übergang konnte dann 2015 unter Einsatz einer Next Generation Firewall und eines Intrusion Detection Systems noch deutlich performanter gestaltet und besser abgesichert werden (vgl. Kapitel 7.8.1).

Der Übergang zum ebenfalls sicherheitskritischen Netz des Universitätsklinikums ist übrigens ebenfalls durch eine Firewall gesichert, die vom UKER auf deren Seite betrieben wird. Bei besonders hohem, begründeten Schutzbedarf ist auch der Betrieb dezentraler Firewalls an Subnetzschnittstellen möglich, allerdings nur in Absprache und bei voller Betreuung durch das RRZE.

Mit den beschriebenen Maßnahmen und ständiger Anpassung an neue Entwicklungen und Bedrohungsformen kann das RRZE zwar keinen absoluten Schutz gewähren, aber doch ein sehr hohes Maß an IT-Sicherheit für die FAU herstellen.

7.7 Netznahe Anwendungsfelder

Während das Datennetz der FAU sich auf die unteren drei Schichten des ISO-Modells bezieht, gibt es verschiedene Anwendungsbereiche, die darauf aufbauend im erweiterten Sinne dem Kommunikationssystem zugerechnet werden können. Dies drückt sich z. B. darin aus, dass entsprechende Dienste auch von der Abteilung „Kommunikationssysteme“ des RRZE betrieben und betreut werden (vgl. Kapitel 7.1.1).

7.7.1 Elektronische Post

Neben Dialog und Dateientransfer gehörte das Versenden und Empfangen von Nachrichten zu den elementaren und früh genutzten Anwendungen von Datenübertragungs- und Kommunikationsnetzen. Zur Realisierung auch als E-Mail bezeichneter elektronischer Post entwickelten sich im Laufe der Jahre verschiedene Verfahren auf Basis unterschiedlicher Vernetzungstechniken. So wurde z. B. Anfang der 1980er-Jahre das Versenden von E-Mails über das BITNET/EARN (Teil 1, Kapitel 3.4.2) möglich, das vor allem im Wissenschafts- und Forschungsbereich international stark genutzt wurde. Hervorzuheben ist auch das Message Handling System (MHS) genannte X400, das ein E-Mail-System innerhalb des OSI-Modells beschrieb und 1984 von der CCITT (heute ITU) erstmals als Standard herausgegeben wurde. Es wurde hauptsächlich im Zusammenhang mit X.25-Netzen, wie denen von FAU oder DFN-Verein, eingesetzt, verlor dann aber im Zuge des Aufkommens von LAN- und Internettechniken vor allem im Hochschulbereich zunehmend an Bedeutung (wie sich ja auch die ISO-Protokolle generell im Ethernet-Kontext nicht durchsetzen konnten). Alternativ dazu entstanden unterschiedliche „E-Mail-Welten“, die sich über jeweils eigene Standards definieren. Dazu gehören die Firmenstandards von Novell und Microsoft für den E-Mail-Verkehr im Rahmen lokaler Vernetzung von Arbeitsplatzsystemen, vor allem aber auch der Internetstandard mit dem Simple Mail Transfer Protocol (SMTP) zum E-Mail-Austausch in IP-basierten Netzen. Dabei hat sich SMTP als Grundlage von Systemen zum Austausch von elektronischer Post weitgehend durchgesetzt. Zwischen den unterschiedlichen E-Mail-Welten kommen bei Bedarf spezielle „Gateways“ an Übergängen zum Einsatz, die so einen übergreifenden E-Mail-Verkehr ermöglichen.

7.7.1.1 Bausteine

Die Realisierung von elektronischer Post erfolgt durch Zusammenwirkung mehrerer Bausteine mit jeweils spezifischen Aufgaben.

Als **E-Mail-Clients** fungieren Programme, die über Benutzeroberflächen den Anwendern Schnittstellen zum Empfangen, Lesen, Schreiben und Versenden von E-Mails bereitstellen und für entsprechende Weitergabe sorgen. Solche, in ihrer Rolle auch als „Mail User Agents“ (MUAs) bezeichneten Programme gibt es in verschiedenen Ausprägungen, die auf unterschiedlichen Endsystemen verfügbar sind, dazu gehören z. B.

- Vernetzte PC-E-Mail-Clients (Thunderbird, Outlook, ...)
- Vernetzte Unix-WS-E-Mail-Clients (Thunderbird, mutt, …)
- Internetcafe Webbrowser (Firefox, Chrome, …)

Die Oberflächen sind in die jeweiligen Systeme integriert. Neben der Bedienung der elementaren E-Mail-Funktionen, unterstützen die Oberflächen die Benutzer z. B. beim Adressieren durch Verzeichnisse potentieller Adressaten (in merkbarer Form), bieten Zugriff auf mehrere, eigene Postfächer und ermöglichen je nach Konfiguration auch das Speichern von E-Mails auf den lokalen Rechnersystemen.

Server für den Postfach-Zugriff bilden die Gegenstellen zu den Clients. Als „Mail Submission Agents“ (MSA) sind sie mit Clients verbunden, nehmen E-Mails von ihnen entgegen, leiten diese (an einen Transport-Server) weiter oder liefern sie (auf Abruf) aus. Die MSAs verwalten Postfächer der Benutzer, legen E-Mails darin ab und sorgen für Datenschutz. Zur Kommunikation zwischen Clients und Servern sind verschiedene Zugriffsprotokolle verfügbar, die in der Regel vom Benutzer per Konfiguration ausgewählt werden können, am meisten verbreitet sind:

- POP3 (Post Office Protocol Version 3), RFC 1939-1996, …, RFC 5034-2007
  - Einfaches Protokoll mit eingeschränkten Fähigkeiten
  - Download der E-Mails vom Server auf den lokalen Rechner
  - Wahlweises Löschen oder Belassen einer Kopie auf dem Server
  - Offline-Betrieb nach Download
  - Unhandlich bei wechselnden Arbeitsplätzen
- IMAP (Internet Message Access Protocol), RFC 3501-2003, …, RFC 7162-2014
  - Wesentlich vielseitiger und leistungsfähiger
  - Download abgerufener E-Mails vom Server nicht zwingend, aber möglich
  - Verwaltung von E-Mail-Ordnern auf dem Server (z. B. Erstellen, Umbenennen, Löschen)
  - Zugriff auf zentrales Postfach von verschiedenen Arbeitsplätzen aus, Sicht unabhängig vom Standort
  - Vom RRZE empfohlene Methode

- Webmail
  - Realisiert über Browser-Schnittstelle
  - Eingeschränkter Funktionsumfang (im Vergleich zu gängigen E-Mail-Clients)
  - Unabhängig von lokalem Rechnerzugang
  - Postfachzugriff nur bei bestehender Netzverbindung (Problematik insbesondere bei Mobilgeräten)

Das Versenden von Post über den Einzugsbereich der Zugriffsserver hinaus erfolgt über Verbindungen mit spezifischen Transportservern unter Verwendung anderer Protokolle (z. B. das SMTP der Internetfamilie).

Die **Server für den E-Mail-Transport**, auch „Mail Transfer Agents“ (MTAs) genannt, kommunizieren einerseits mit den MSAs, also den Servern, die Benutzerzugriffe und Postfächer organisieren, und andererseits mit gleichartigen Servern, die für die generelle (überregionale) E-Mail-Verteilung zuständig sind. Sie sind in definierter Struktur über das Internet miteinander verbunden, und sorgen durch entsprechendes Routing für den Transport der E-Mails vom Eingang zum angegebenen Zielpunkt. Der Transfer einer E-Mail erfolgt somit von einem sendenden MUA zu dessen MSA, über gegebenenfalls mehrere MTAs zum entfernten MSA und schließlich zum MUA des adressierten Empfängers.

7.7.1.2 Übertragungsprotokoll SMTP

Das Simple Mail Transfer Protocol dient als „einfaches“ Protokoll dem Austausch von E-Mails zwischen Servern (MSAs, MTAs) in IP-basierten Computernetzen. Gemäß den Internetstandards (RFC 821-1982, RFC 5321-2008) soll es zuverlässigen und effizienten Transfer von E-Mails ermöglichen. SMTP setzt Innerhalb der Internetprotokollhierarchie auf dem Transmission Control Protocol (TCP) der Schicht 4 auf und nutzt so z. B. auch dessen Mechanismen für gesicherte Übertragungen (vgl. Teil 1, Kapitel 4.3). Das TCP ist verbindungsorientiert, d. h. zum Transfer von E-Mails werden jeweils Verbindungen aufgebaut, über die dann die E-Mail-Daten übertragen werden. Dabei geht die Initiative stets vom sendenden System aus, wobei die Verbindungen von Clients zu Servern über den TCP-Port 597 (Submission Port) hergestellt werden und zwischen zwei Servern die Portnummer 25 (SMTP-Port) verwendet wird.

Jede E-Mail bzw. jedes SMTP-Paket enthält eine Absender- und eine Zieladresse, die den kommunizierenden Partnern zugeordnet sind. Der formale Aufbau der Adressen (vgl. RFC 5322-2008) orientiert sich am Namensschema für IP-Adressen, wie sie vom Domain Name Service verwaltet werden. E-Mail-Adressen setzen sich aus einer individuellen Bezeichnung und dem Domainnamen der zugehörigen Umgebung zusammen. Sie sind personen- (oder auch bspw. dienst-)bezogen, also unabhängig

von einzelnen Endsystemen, aber eindeutig innerhalb ihrer Domains zugeordnet. Die Adressen haben allgemein die Form „name@domain“ oder lauten für einen Angehörigen der FAU zum Beispiel „max.mustermann@fau.de“. Die im DNS verwalteten Domains werden in diesem Kontext auch als „Maildomains“ bezeichnet. Eine Person bzw. deren Mailbox kann auch als Benutzer der FAU über mehrere E-Mail-Adressen erreichbar sein. Eine Erweiterung bilden sogenannte Gruppenadressen, die eine Menge zugehöriger Einzeladressen enthalten und vom E-Mail-System entsprechend vervielfacht zugestellt werden. So werden zum Beispiel mit „noc@fau.de“ adressierte E-Mails an alle Mitarbeiter der Netzbetriebsgruppe des RRZE bzw. des „Network Operation Centers“ der FAU gesendet.

Die Maildomains sind auch maßgebend für den Transport der E-Mails zwischen den dafür zuständigen Servern (MTAs), d. h. für das sogenannte E-Mail-Routing. Dies erfolgt in Zusammenarbeit mit dem DNS. Ein Server, der eine E-Mail weiterzuleiten hat, wendet sich unter Angabe der Ziel-Domain an den DNS und fragt an, welche Server für diese Domain zuständig sind. Der DNS hält eine Datenbasis mit sogenannten „MX-Records“, die entsprechende Zuordnungen zu Serveradressen enthält. Der DNS antwortet mit einem Satz von Rechneradressen inklusive Präferenzen oder aber auch mit negativem Resultat („non-existent domain“), wenn kein Eintrag gefunden wurde. Daraufhin kann der Server den nächsten Partner finden, zu ihm Verbindung aufbauen und die betreffende E-Mail dorthin übertragen.

Anfangs konnten E-Mails keine beliebig formatierten Daten enthalten, denn SMTP wurde ursprünglich zur Übertragung von Texten konzipiert, also von Zeichenfolgen im ASCII-7-Bit-Format. Zur Überwindung dieser Beschränkung wurden die Verfahren von „Multipurpose Internet Mail Extensions“ (MIME) zur Kodierung/Dekodierung von 8-Bit-Daten als erweiternde Internetstandards (RFCs 2045 bis 2049 -1996) definiert. Über deren verschiedene Varianten wurde es z. B. möglich, auch Umlaute enthaltene Texte oder Multimedia-Daten per E-Mail zu versenden.

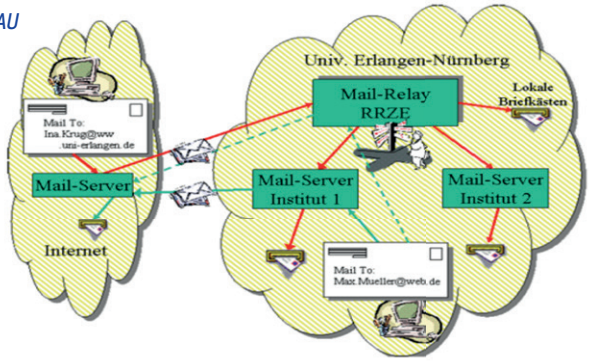
Um SMTP funktional erweitern zu können wurde mit dem „Extended SMTP“ (ESMTP), auch „Enhanced SMTP“ genannt, ein ergänzender, abwärtskompatibler Standard definiert (RFC 1869-1995). Dieser erlaubte unter anderem auch die Einführung der Methode „SMTP-Auth“ (SMTP Service Extension for Authentication, RFC 2554-1999), die zum Verhindern gewisser Arten von Missbrauch beitragen sollte. Danach authentifizieren sich E-Mails bzw. deren Absender über mitgeführte Benutzerkennungen und Passwörter. SMTP-Auth-fähige Server sind so z. B. in der Lage, nur noch authentifizierte Absender E-Mails weiterzuleiten und damit die Verbreitung von Spam-Mails stark einzuschränken. Zudem kann man in den Log-Dateien nachvollziehen, wer an einen SMTP-Server E-Mails gesendet hat bzw. senden wollte, und aus der Analyse eventuelle Maßnahmen ableiten (z. B. künftiges Blockieren von Absendern oder Hosts).

Eine andere Art von Sicherheit bzw. Wahrung von Vertraulichkeit übertragener E-Mail-Daten bieten verschiedene Verschlüsselungs- und Signatur-Methoden auf der Anwendungsebene oberhalb von SMTP, die als solche hier nicht weiter betrachtet werden. Generell handelt es sich dabei um „Ende-zu-Ende-Verschlüsselungen“ zwischen sendenden und empfangenden E-Mail-Clients, aber auch um Server-basierte Lösungen. Letztere sind meist vorzuziehen, da sie die Endteilnehmer entlasten, indem die Arbeit der Verschlüsselung und Signatur von Servern erledigt bzw. von deren Administratoren verwaltet wird.

7.7.1.3 E-Mail an der FAU (Server, Dienste)

Auch der an der FAU verfügbare und vom RRZE bereitgestellte E-Mail-Dienst ist nach den geschilderten Prinzipien aufgebaut, verwendet also SNMP und das darunterliegende (IP-)Kommunikationsnetz der Universität zum Austausch elektronischer Post. Die Abbildung „E-Mail-Struktur der FAU“ (aus einer Präsentation von 2018 [*Fisch*]) stellt die Zusammenhänge zwischen den verschiedenen Bausteinen des Dienstes dar. Im Zentrum steht das „E-Mail-Relay“ des RRZE, das aus einer Menge eng zusammenarbeitender, spezifischer Server- bzw. Rechnersystemen besteht und in seiner Gesamtheit sowohl die Funktionalitäten der E-Mail-Verteilung als auch die von Postfachzugriffen umfasst.

E-Mail-Struktur der FAU



Als Server für den E-Mail-Transport (MTA) ist das Relay zentraler Eintrittspunkt für E-Mails aus dem Internet und innerhalb der FAU mit verschiedenen E-Mail-Servern (MTAs) von Instituten oder Einrichtungen der Universität verbunden. Neben der reinen E-Mail-Verteilung erbringt der Server noch eine Reihe weiterer, für die Nutzer weitgehend unsichtbare, Hintergrunddienste. Dazu gehört z. B. die Abbildung von Gruppenadressen auf zugehörige Einzeladressen nach entsprechenden Listen und

die sich daraus ergebende, mehrfache Weiterleitung bzw. Zustellung von Post an die Mitglieder der betreffenden Gruppe. Besonders wichtig aber ist das Prüfen eingehender E-Mails nach verschiedenen Kriterien auf deren Zulässigkeit oder Gefährdungspotential. Das betrifft das

- Blockieren der Einlieferungen durch Hosts, die sich nicht protokollkonform verhalten haben
- Blockieren der Einlieferungen durch Hosts, die auf globalen schwarzen Listen (Blacklists) stehen, also als nicht vertrauenswürdig anzusehen sind
- Anwenden von Viren-/Phishingfiltern gegen das Einschleppen von Schadsoftware und betrügerischer E-Mails
- Spamanalyse und Abwehr massenhafter, unerwünschter E-Mails
- Prüfen auf zulässige Absenderadressen

Das Relay bildet so einen „Schutzwall“ für die E-Mail-Systeme innerhalb der FAU und externer Kunden. So wurden z. B. 2017 rund 70% aller externen Einlieferungsversuche blockiert und im Jahresmittel am Tag 90.000 von 217.000 E-Mails abgelehnt, die sonst ungefiltert weitergeleitet worden wären.

Als Server für den Postfach-Zugriff (MSA) fungiert das Relay auch als Kontaktpunkt für Clients und bietet den Benutzern damit zusammenhängende Dienste an.

- Postfach-Dienst „FAUMail“ (realisiert über das Programmsystem „Dovecot“)
  - Angebot der FAU für Studierende sowie für Beschäftigte von Einrichtungen mit Bedarf an reiner E-Mail-Funktionalität
  - Bereitstellung, Verwaltung von Postfächern
  - Verfügbarer Speicherplatz (Stand 2018): 2 GB (Beschäftigte), 1 GB (Studierende)
  - Posteingangsserver „faumail.fau.de“
  - Zugang über Protokolle POP3, IMAP
  - Webmail über *https://faumail.fau.de*
  - Berechtigung über E-Mail-Adresse und E-Mail-Passwort
  - Verknüpfung mit Datenbanken (Backend-Server)
- Groupware-Dienst gemäß E-Mail-System „MS-Exchange“ von Microsoft
  - Bereitstellung, Verwaltung von Postfächern
  - Posteingangsserver „groupware.fau.de“
  - Zugang über Protokolle POP3 und IMAP
  - Webmail über *https://groupware.fau.de*
  - Berechtigung über Exchange-Benutzerkennung, -Passwort
  - Angebot für Beschäftigte von Einrichtungen der FAU mit Bedarf an Kalenderfunktionalität, Terminverwaltung etc.

Die E-Mail-Dienste stehen als Angebote allen Beschäftigten und Studierenden der Universität zur Verfügung. Die personenbezogenen Adressen wurden ab 1997 nach einheitlichem Schema vergeben, das unter anderem die Zugehörigkeit zur organisatorischen Einheit innerhalb der FAU oder deren Studiengang kenntlich machte.

[<Vorname>].<Nachname>@[org.Untereinh>.]orgEinh>.uni-erlangen.de“
(im abstrakten Beispiel: max.mustermann@rrze.uni-erlangen.de“) bzw.
<Vorname>.<Initialen>.<Nachname>@<Studiengang>.stud.uni-erlangen.de

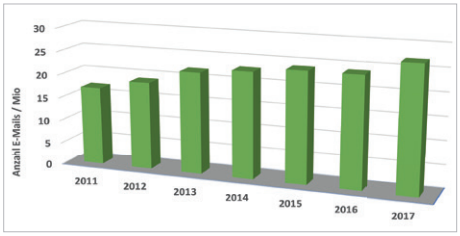
Ab 2012 wurde nach Beschluss der Universitätsleitung damit begonnen, die Marke FAU in die E-Mail-Adressen einfließen zu lassen und ein verkürztes, für alle Angehörigen gültiges Schema anzuwenden:

<Vorname>.<Initialen>.<Nachname>@fau.de
(im abstrakten Beispiel *max.mustermann@fau*)

Dieses verkürzte Schema propagiert die FAU, ist für Außenstehende einfacher zu handhaben und ermöglicht eine lebenslange Erreichbarkeit unter gleicher Adresse, da z. B. die Zugehörigkeit zu einer Einrichtung nicht immer eindeutig definiert ist oder im Laufe der Zeit wechseln kann. Ende 2017 waren demgemäß 74.300 persönliche E-Mail-Adressen vergeben, was 82% der Beschäftigten und mehr als 92% der Studierenden entspricht.

Das zentrale Relay bietet seine Vermittlungsfunktionen und insbesondere die damit verbundenen Schutzmaßnahmen den Einrichtungen, Instituten der Universität mit eigenen E-Mail-Servern an. Allerdings rät das RRZE aus verschiedenen Gründen zur Integration der lokalen E-Mail-Funktionen in das zentrale System und dessen Betreuung. Auch verschiedene externe Einrichtungen, wie etwa die Hochschule Coburg oder das Studentenwerk, nutzen das Erlanger E-Mail-Relay als Verteil- und Filterinstanz insbesondere für den E-Mail-Verkehr aus dem Internet.

Das E-Mail-Aufkommen hat sich im Laufe der Jahre ständig vergrößert. Im Jahr 2000, in dem der E-Mail-Dienst X.400 abgeschaltet und nur noch das Protokoll SMTP eingesetzt wurde, bearbeitete das Relay des RRZE etwa 9,8 Mio. E-Mails. Im Jahr 2013 (am Anfang der hier in Kapitel 7 betrachteten Entwicklungsphase) waren es 84 Mio., also etwa 8,6-mal so viel. Im Jahr 2017 stieg dann das Aufkommen an eingelieferten E-Mails auf 112 Mio. an. In den Zahlen sind allerdings auch die E-Mails enthalten, die bereits am



Entwicklung des Nutzmailaufkommens, 2011 - 2017

Eingang abgelehnt wurden oder nach weiteren Prüfungen als unerwünscht eingestuft und markiert wurden. Das danach reduzierte Nutzmailaufkommen (30% der Einlieferungen) entwickelte sich in den Jahren 2013 bis 2017 von 20 auf 27 Mio. (vgl. Abbildung auf S. 192 „Entwicklung des Nutzmailaufkommens, 2011 – 2017“).

7.7.2 Multimedia

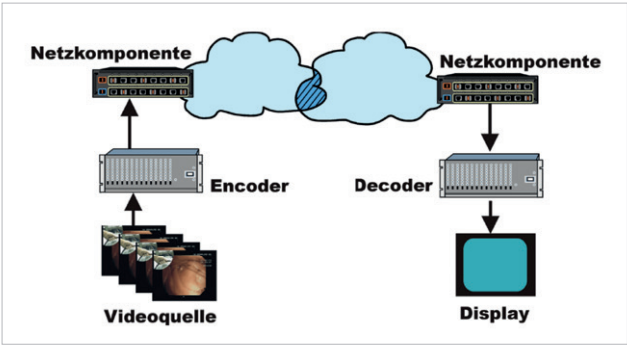
Übertragungen von audiovisuellen Daten und darauf aufbauende Video- oder Kommunikationsdienste stehen für relativ junge Anwendungsbereiche der Informations-Technik, die aber zunehmend an Bedeutung gewonnen haben. So war insbesondere im Hochschulkontext, etwa im Zusammenhang mit digitalen Lehrangeboten, verteilten Konferenzen oder Heimarbeitsplätzen (Home-Office) ein ständig wachsender Bedarf zu verzeichnen. Dies schlug sich auch im Dienstangebot des RRZE bzw. den Tätigkeiten des Multimediazentrums seiner Abteilung „Kommunikationssysteme“ nieder (vgl. Kap. 7.1.1).

7.7.2.1 Audio-, Videoübertragungen über IP-Protokolle

Als Basis zur Übertragung von Videodaten hat das Internetprotokoll verschiedene, prinzipielle Schwachpunkte, da es, etwa im Vergleich zu ATM, keine Mechanismen zur Gewährleistung von Dienstgüteparametern (QoS) enthält, die verfügbare Bandbreiten, begrenzte Verzögerungszeiten oder gleichförmigen Datenfluss garantieren. Aufgrund der „einfacheren“ Internettechnik und der weltweiten Verbreitung des Internets haben sich aber IP-basierte Übertragungen auch in diesem Anwendungsfeld weitgehend durchgesetzt. Dazu trugen die Entwicklungen der Netztechnik erheblich bei, die etwa durch Anhebungen von Übertragungsgeschwindigkeiten (z. B. auf 10-40 Gbits in Backbones oder 1-10 Gbits in lokalen Netzen) oder Verringerungen von Verweildauern in den Komponenten (Router, LAN-Switche) für Reduzierungen von Durchlaufzeiten und Verzögerungen (Delays) bei der Übertragung von Datenströmen sorgen konnten. Dadurch konnten die von Videoübertragungen an das Netz gestellten Qualitätsanforderungen für die gängigsten Anwendungen weitgehend erfüllt werden.

Wichtig waren aber auch die Entwicklungen im vielfältigen Bereich der Videotechnik, etwa in Bezug auf leistungsfähige Endgeräte und Systeme, spezifische Verfahren oder spezielle Anwendungsprogramme. Dabei stehen in engem Zusammenhang mit den Anforderungen an das Übertragungsnetz Verfahren, die aufgenommene Videosequenzen kodieren und komprimieren, wodurch der Bandbreitenbedarf erheblich reduziert wird. So benötigt etwa die Übertragung von Videos in Standardqualität (über „Serial digital interface“, „SDI“, siehe [*SDI*]) unkomprimiert 270 Mbp/s und in komprimierter Form je nach Art des Videos 0.384 bis 50 Mbp/s, also deutlich weniger.

Für High-Definition(HD)-Videos gilt ein Verhältnis von 1.500 Mbp/s (1,5 Gbp/s) zu 20 bis 600 Mbp/s. Zu berücksichtigen ist allerdings, dass die Verfahren, in der Regel handelt es sich um die standardisierten „MPEG-1“ (ISO/IEC 11172 der „Moving Picture Experts Group“, MPEG) oder dessen Nachfolger „MPEG-2“, zur Kodierung eine gewisse Verarbeitungszeit benötigen und entsprechende Delays bewirken (z. B. 250 ms, abhängig vom ausführenden Gerät) und bei der Komprimierung (im Allgemeinen nicht bemerkbar) Informationen verloren gehen. Das „Schema einer Videoübertragung“ stellt ein einfaches Beispiel des Datenflusses von einer Videoquelle (z. B. von einer Kamera erzeugt) zu einem Display (z. B. einem PC mit Monitor) dar. Kodierungen und Dekodierungen erfolgen über Encoder (spezielle Hardwarekomponenten), die jeweils über eine Netzkomponente (z. B. Router oder LAN-Switch) des Übertragungsnetzes miteinander verbunden sind.



Schema einer Videoübertragung

Im gezeichneten Beispiel haben die Encoder bei Nutzung eines IP-basierten Netzes, auch die Aufgaben der Anpassung an das Datennetz, bzw. der Abwicklung entsprechender Protokolle. In anderen Konstruktionen können Encoder- oder Netzfunktionen auch in Hard- und Software von Endsystemen integriert sein.

Oberhalb der IP-Ebene (Schicht 3) stützen sich die Anwendungssysteme zur Übertragung von Videodaten auf die Protokolle der IP-Transportebene (Schicht 4), d. h. auf TCP oder UDP. Dabei bietet TCP mit seinen Mechanismen zur Fehlererkennung und Behebung mehr Sicherheit, während UDP unkomplizierter und mit geringeren Verzögerungen arbeitet. Je nach den Anforderungen der Anwendungen an die Übertragungsqualität ist zu entscheiden, ob es mehr auf gesicherte Übermittlung (TCP) ankommt oder bei geringeren Verzögerungen mögliche Datenverluste toleriert (UDP) oder aber auch auf Anwendungsebene ausgeglichen werden können.

Auf der Anwendungsebene (Schicht 5 – 7) wurde die IP-Familie um das Real-Time Streaming Protocol (RTSP) erweitert, das von der „IETF MMUSIC Group“ entwickelt und standardisiert wurde (RFC 2326-1998, RFC 7826-2016). Es kann somit als Bestandteil von Anwendungssystemen zur Steuerung und kontinuierlichen Übertragung audiovisueller Daten (Streams) über IP-basierte Netzwerke genutzt werden. RTSP ist ein textbasiertes Protokoll und ähnelt im Aufbau und Verhalten dem von Webanwendungen bekannten HTTP. Im Gegensatz zu HTTP kennt RTSP jedoch Zustände und ist bidirektional. Es kann sowohl für Aufnahmen von Videodateien und deren Upload vom Client zum Server (bspw. mit einer Videodatenbank) als auch zum Abruf und Download gespeicherter Videodateien verwendet werden. Im Rahmen der Protokollhierarchie baut RTSP wahlweise auf UDP oder TCP auf und kommuniziert standardmäßig über den Port 554 (alternativ auch 8554). RTSP wird häufig im Zusammenhang mit Streaming-Diensten, wie solchen von Apple (Airplay, Streaming Media Player) oder auch den Diensten des RRZE (z. B. zur Aufnahme von Videos) genutzt.

Eine andere Technik zum Transfer von Streaming-Media-Dateien, insbesondere zum Abruf bzw. Download von Videodaten, über IP-basierte Netze bietet das als HTTP-Streaming oder auch als HTTP-Live-Streaming (HLS) bezeichnete Verfahren über einen konventionellen Webserver. Der Webserver wird dabei als einfacher Dateiserver zur Auslieferung von kleinen Teilstücken der gesamten Datei, sogenannten Segmenten, genutzt. Dabei können auf dem Webserver die Dateien in unterschiedlichen Qualitätsstufen abgelegt werden. Das Endgerät kann je nach verfügbarer Bandbreite diese Stufen wechseln, sodass z. B. auch in schlecht ausgebauten Mobilfunknetzen Streaming möglich ist. Eingebettet in die Anwendungsschicht des Webprotokolls HTTP baut HLS in der Transportebene auf dem TCP und bezüglich der der Netzebene natürlich dem Internetprotokoll auf. HLS wurde ursprünglich von Apple entwickelt und 2017 von der IETF als Entwurf (Internetdraft) beschrieben (HTTP Live Streaming draft-pantos-http-live-streaming-23m), bisher aber noch nicht in einem RFC standardisiert. Die Integration in das Websystem macht es möglich, gespeicherte Videos in „einfacher Weise“ über gewohnte Browser abzurufen und darstellen zu lassen, sodass HLS im Zusammenhang mit entsprechenden Portalen, wie auch dem des RRZE, bevorzugt zum Einsatz kommt.

7.7.2.2 Multimediadienste des RRZE

Die Multimediadienste stehen in engem Bezug zum Kommunikationssystem, da sie z. B. besondere Anforderungen an Übertragungstechnik und Vernetzung stellen bzw. ohne Bereitstellung benötigter Grundlagen nicht möglich wären. So befasste sich die für das Netz der FAU zuständige Abteilung des RRZE neben der Durchführung des Standardbetriebs auch immer mit technischen Entwicklungen zur Steigerung der

Leistungsfähigkeit und zur Öffnung für neue Anwendungsarten. Dazu gehörten bereits ab Mitte der 1990er Jahre die Durchführung von Projekten zur Hochgeschwindigkeitsübertragung (seinerzeit 34 Mbp/s bis 2,4 Gbits im Fernbereich, im Vergleich zu 100 Mbp/s in lokalen Netzen) im Rahmen von Testbeds des DFN sowie das Uni-TV zur Videoaufzeichnung und Übertragung von Vorträgen zum Bayerischen Rundfunk gemäß sende(r)-fähigen Anforderungen (vgl. Teil 1, Kapitel 5.4.4). Das Projekt wurde übrigens anlässlich der „Networking Conference TERENA, Lissabon 2000“ einem internationalen Publikum vorgestellt [*Uni-TV*]. Aus der Arbeitsgruppe von Uni-TV entwickelte sich dann das Multimediazentrum (MMZ) des RRZE, das 2018 auf „20 Jahre Uni-TV zurückblicken konnte [*Grä20*]. Das MMZ erweiterte im Laufe der Jahre die Inhalte seiner Tätigkeiten erheblich und berücksichtigte technische Entwicklungen bzgl. Ausstattung, Aufnahme, Übertragung, Bearbeitung, Aufbereitung, Speicherung oder Präsentation im Rahmen seiner personellen und finanziellen Möglichkeiten. Das betraf z. B. auch die grundlegende Umstellung von ATM-basierter Übertragungstechnik auf die des Internets und seiner Protokolle.

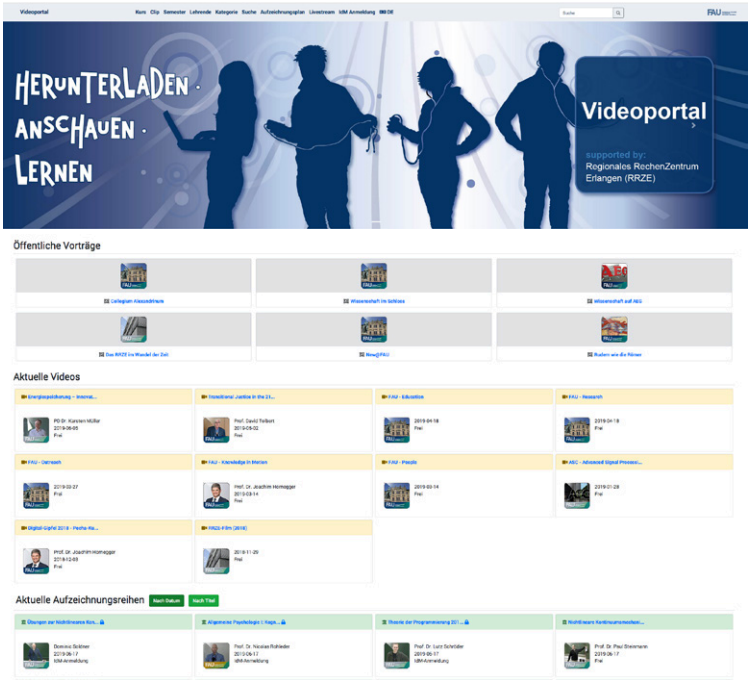
Als Meilensteine der Entwicklung können genannt werden:

- 1998: Start von Uni-TV (vgl. Teil 1, Kap. 5.4.4)
- 1999: (Web-)Videoportal zum Download von Produktionen
- 2003: Kooperativer Uni-TV-Service (FAU, BR/IRT)
- 2008: Einweihung des E-Studios (vgl. Kap. 6.1.2)
- 2009: Aufbau der Vorlesungsaufzeichnung
  - In der E-Regie, verteilte Produktion
  - Manuell vor Ort
- 2009: Videoportal zum geordneten Abruf aufgezeichneter Veranstaltungen
- 2011: Internationales Zielpublikum durch Integration von „iTunes U“ (Videoplattform der Firma Apple), Erhöhung des Bekanntheitsgrades
- 2013: Neugestaltung der Serverlandschaft
  - Aufteilung des Videoangebots auf vier virtuelle Server
  - Hinzugekommener „Live-Streaming-Server“ (Wowza Streaming Engine) zur direkten Übertragung der in E-Studio, Audimax, H4, H11 und Aula/Schloss stattfindenden Ereignisse ins Internet
  - Installation von Servern mit der Clientserver-Software „Opencast/Matterhorn“, die die zeitgesteuerte und (teil-)automatisierte Durchführung von Vorlesungsaufzeichnungen erlaubt
- 2014: Start automatisierter Aufzeichnungen
- 2016: Erstellung von Imagefilmen, Portraits, Sonderformaten
- 2018: Relaunch des Videoportals (vgl. Startseite in Abbildung „Aufzeichnungsreihen aus dem Jahr 2018“, jeweils aktuell abrufbar unter *https://www.video.uni-erlangen.de/*)

Die aufgezeichneten und über das Portal abrufbaren Videos beinhalten:

- Lehrveranstaltungen, Vorlesungen und Vorlesungsreihen
- Fach- und Forschungstage, Kongresse, Fest- und Sonderveranstaltungen
- Vorträge für die Öffentlichkeit
- In eigener Regie erstellte Filme (z. B. zum 50. Jahrestag des RRZE)

Im betrachteten Zeitraum von 2013 bis 2018 stieg Gesamtzahl der Aufzeichnungen von 722 auf 8.500. Dabei wurden von den Nutzern pro Tag zwischen 1.000 (2013) und 1.600 (2018) Videos angesehen. Pro Semester kommen aktuell (2018) rund 500 neue Aufzeichnungen hinzu.



Aufzeichnungsreihen aus dem Jahr 2018

Das Multimediazentrum (MMZ) des RRZE unterstützt als generelle Anlaufstelle für Fragen zum Thema Multimedia an der FAU darüber hinaus zum Beispiel auch bei der Durchführung von Videokonferenzen und betreibt verschiedene, in der Universität verteilte „Public Displays“, die fortlaufend über die FAU, das RRZE und aktuelle Ereignisse informieren.

Die vielfältigen Tätigkeiten und Techniken des MMZ beziehen sich zwar kaum noch direkt auf das Kommunikationsnetz bzw. dessen Ausgestaltung, das aber weiter als solide Basis zur Erfüllung spezifischer Anforderungen benötigt wird. Die Videodienste leisten einen wichtigen Beitrag zu den IT-Diensten des RRZE. Ihre Bedeutung wird zum Beispiel in Bezug auf neue Konzepte zu Lehr- und Kommunikationsformen sicher noch zunehmen.

7.7.3 Forschungsprojekte Netz

Das RRZE bzw. die Abteilung Kommunikationssysteme hat sich neben den betrieblichen Aufgaben rund um die Netzbetreuung in ihrem Themenbereich stets auch mit Projekten zu Forschung und Entwicklung befasst. Hier sind z. B. die von der DFG geförderten Entwicklungen von Grundlagen und Anwendungen der Realzeitprogrammiersprache PEARL in den 1970er Jahren (Leitung Dr. Peter Holleczek [*HollP*]), die Hochgeschwindigkeits- und Erprobungsprojekte (Testbeds) in Zusammenarbeit mit dem DFN Ende der 1990er Jahre, die betriebsbegleitenden Untersuchungen des WiN-Labors und schließlich die folgenden und aktuellen Arbeiten der daraus hervorgegangenen Forschungsgruppe Netz mit ihren vielfältigen, praktischen und theoretischen Projekten im Kontext von Kommunikationsnetzen. Folgende Auswahl gibt dazu einen im Überblick.

7.7.3.1 Betriebsbegleitende Untersuchungen zum Deutschen Forschungsnetz (X-WiN)

Im Zusammenhang mit dem Betrieb X-WiN befasste sich das RRZE bzw. die Forschungsgruppe Netz im Schwerpunkt mit Fragen von Dienstgüte, Auslastung und Laufzeiten. Insbesondere bearbeitete das WiN-Labor folgende Themen:

Interne Qualitätskontrolle im Deutschen Forschungsnetz

Das Labor unterstützte in dem Projekt den DFN-Verein bei der Erfassung, Bewertung und Historisierung von Ausfällen und Störungen, die im Deutschen Wissenschaftsnetz auftreten. Diese Daten dienen zur Ermittlung der Verfügbarkeit des IP-Dienstes. Dafür mussten Ursachen und Ausfallzeiten diskutiert und mit sämtlichen Informationsquellen abgeglichen werden, um die Ereignisse dann in einer Datenbank den betroffenen Objekten zuzuordnen. Die Reports der verschiedenen Carriers, die dem DFN-Verein Leitungen zur Verfügung stellen, mussten mit den erhobenen Daten abgeglichen werden. Zum Ende jeden Monats und am Jahresende wurden zusammenfassende Statistiken erstellt. So wurden im Jahr 2012 beispielsweise 1.107 Service Requests

erfasst, von denen 222 den unterschiedlichen Carriers zuzuordnen waren. 494 Tickets hatten eine Laufzeit von unter einer Stunde. Der Großteil aller Requests (779) wurde vom Netzüberwacher gemeldet.

Accounting im X-Win

Das WiN-Labor entwickelte bereits für mehrere Generationen des Deutschen Forschungsnetzes WiN ein Accountingsystem, das Verkehrsflüsse innerhalb des Kernnetzes misst. 2013 wurde dieses System zur Erfassung des IPv6-Verkehrs erweitert. Grundlage dazu bieten (bei entsprechender Konfiguration) in Routern verfügbare Daten des „Netflow- Accountings“, die zusammenhängende IP-Datenströme erkennen, darüber transferierte Datenmengen erfassen und abrufbereit speichern können. Begonnen wurde zunächst mit den vier Super-Core-Routern des X-WiN, dann wurden sukzessive ausgewählte XR-Router hinzugenommen. Es wurde ein System entwickelt, das das Sammeln von Netflow-Daten aus mehreren Quellen (in einem Collector) und das Exportieren dieser Daten zu mehreren Zielen (Exporter), miteinander kombinierte. Die vom WiN-Labor entwickelten Komponenten wurden 2015 dem DFN-CERT zur Aufnahme in den Regelbetrieb übergeben.

IP-Performance Messungen im X-WiN

Das im WiN-Labor entwickelte und betreute IPPM-Messsystem „Hades Active Delay Evaluation System“ (HADES) erfasst kontinuierlich die Performance-Metriken One-Way Delay, Delay Variation, Packet Loss und Hop Count im X-WiN. Das System beruht auf mehreren, im Netz verteilten Messboxen, die sich regelmäßig untereinander per UDP Daten zusenden und unter anderem zugehörige Zeitstempel in einer Matrix speichern. Wichtig ist dabei die zeitliche Synchronisierung bzw. der Bezug auf eine gemeinsame Uhr, die unter anderem über das „Network Time Protocol“ (NTP) der IP-Familie erreicht wird. So kann z. B. der Empfänger eines Pakets aus der Differenz von Ankunftszeit und Sendezeit (Stempel des Absenders) die zugehörige Laufzeit bestimmen. Verfahren und bis dahin erreichte Ergebnisse waren Gegenstand einer Präsentation auf der „2nd Internaonal Conference on Computing, Communications and Control Technologies: CCCT 2004, Volume III“ [*QosMess*].

Die Messboxen wurden im Laufe des Projekts je nach technischem Stand und Einsatzort auf unterschiedlichen Plattformen realisiert, z. B. auf Servern mit i386 Hardware an ausgewählten Punkten oder „einfachen“ Mikrorechnersystemen (embedded ARMs) in der Fläche. Durch entsprechende Verteilung von Messboxen im Wissenschaftsnetz wurden zum Zeitpunkt der Übergabe des Systems an den DFN (2015) auf über 3.500 Messstrecken Daten erhoben, gesammelt, in verschiedenen Statistiken ausgewertet und aufbereitet. Ergänzend wurden in Kooperation mit den Fachbereichen Elektro-

technik und Informatik der Hochschule Lübeck Programme zur Visualisierung von HADES-Messungen entwickelt, um dadurch weitere Möglichkeiten zur Interpretation der Daten zu schaffen.

Das RRZE setzte HADES übrigens auch im Rahmen seiner Betreuung des Netzes der Universitätsklinik (bis 2012) zur Messung von Leistungsdaten ein.

7.7.3.2 Untersuchungen auf internationaler Ebene (GÉANT)

Zu den Arbeiten im Kontext des Deutschen Forschungsnetzes X-WiN befasste sich die Forschungsgruppe Netz auch mit Aspekten internationaler Vernetzung und übernahm verschiedene, von der EU geförderte Projekte im Rahmen des europäischen Wissenschaftsnetzes GÉANT.

GÉANT ist das pan-europäische Internetverbindungsnetzwerk der europäischen Forschung, das mit dem nationalen Netz des DFN (X-WiN) sowie damit auch dem FAU-Netz verknüpft ist. Der Name entspricht dem französischen Wort „Géant“, auf deutsch „Gigant“. Es verbindet 26 nationale Forschungsnetze, darunter die DACH-Netze DFN, SWITCH und ACOnet, mittels exklusiv reservierter Multi-Gigabit-Leitungen, und darüber ca. 40 Millionen Benutzer in über 8.000 Einrichtungen in 40 Ländern mit einer Infrastruktur von 50.000 km. Das Kernnetz basiert auf 10-GBit-Leitungen, die geringsten Geschwindigkeiten liegen bei 155 Mbit. Weitere Anhebungen auf 40 und 100 Gbp/s befinden sich in Erprobung oder Planung.

Das europäische Forschungsnetz entwickelte sich in verschiedenen Generationsstufen, die sich wie folgt grob beschreiben lassen:

- 1992: EuropaNET
- 1997: TEN-34
- 1998: TEN-155
- 2001: GÉANT
- 2005: GÉANT2
- 2009: GÉANT3
- 2015: GÉANT4-P1
- 2016: GÉANT4-P2

Zum Betrieb des Netzes bzw. der betreffenden Generation gehörten jeweils auch eine Reihe wissenschaftlicher Aktivitäten zu unterschiedlichen Themenkreisen, gegliedert nach Joint Research Activities (JRA), Service Activities (SA) und Network Activities (NA), an denen sich die Forschungsgruppe Netz des RRZE mit ausgewählten Projekten beteiligt(e).

Projekt GÉANT3

Mit dem Betriebsstart von GÉANT3 im Jahr 2009 begann auch das RRZE mit einem Projekt, das der SA3-T3 zugeordnet war und das Thema „Service Monitoring Tools and Performance“ bearbeitete. Gegenstand waren die Entwicklung von Monitoring Tools, die Weiterentwicklung des IPPM-Messsystems HADES (vgl. Kapitel 7.7.3.2), einzelne dedizierte Messprojekte und transatlantische Kooperationen der Forschungsnetze zwischen „DANTE“ (Europa), „Internet2“ (USA), „2CANARIE“ (Kanada) sowie „ESnet Energy Sciences Network“ (USA).

Der Schwerpunkt des RRZE in diesem Projekt waren Performance Messungen im Europäischen Forschungsnetz mit „perfSONAR“, einem Protokoll, über welches implementierungsübergreifend Messungen am Netzwerk durchgeführt werden konnten sowie bereits verfügbare Messergebnisse abgerufen werden können. Die Hauptaufgabe lag in der Weiterentwicklung des Prototypen von GÉANT2 hin zu einem unterstützten Software-Service, der von Kunden von GÉANT, also primär nationalen Forschungsnetzen sowie großen Forschungsprojekten, installiert und eingesetzt werden konnte.

Das Projekt GÉANT3 wurde 2013 erfolgreich abgeschlossen und in GN3plus fortgesetzt.

Ergänzendes Projekt zu GÉANT3 (GN3plus)

Ebenfalls auf das „GÉANT3“-Netz bezog sich das EU-Projekt „GN3plus“, das eine Fortsetzung von GÉANT3 darstellte. Die Forschungsgruppe Netz des RRZE arbeitete dazu (ab 2013) in folgenden Bereichen bzw. „GÉANT3-Activities“:

- SA2: Testbed as a Service,
  Task 1: TaaS Architecture and Engineering
  Aufbau einer europaweiten Testbedinfrastruktur mit der Möglichkeit, in individuellen, virtuellen Testbedumgebungen über ein Webinterface Experimente durchführen zu können, ohne den normalen Netzbetrieb zu stören.
- SA2: Testbed as a Service
  Task 2: Software Tools, Protocols, and Specifications
  Entwicklung einer Architektur gemäß Task1 zur Verwaltung von Ressourcen und Bereitstellung individueller Testbeds.
- SA2: Testbed as a Service,
  Task 3: TaaS Service Management.
  Service Management zur prototypischen Einführung von TaaS und Bereitstellung von Service-Mechanismen (Helpdesk, Usertraining).
- SA4: Network Support Services,
  Task 1: Multi-Domain Monitoring (MDM).

Fortsetzung von Arbeiten des Performance Managements mit neuer strategischer Ausrichtung, Überarbeitung und Angleichung verschiedener Methoden der Datenrepräsentation.

- „JRA1: „Network Architectures for Horizon 2020“ (vgl. GÉANT4)
  Task 1: „Future Network Architectures“.
  Untersuchungen zur Zeitsynchronisation mit „PTP“ (Precision Time Protocol/IEEE 1588), in Kooperation mit dem Institut für Rundfunktechnik, Einsatztests im Bereich verteilter Fernsehproduktionen.
- JRA2: „Technology Testing for Specific Service Applications,
  Task 1: „OpenFlow/SDN for Specialized Applications“.
  Untersuchungen im Hinblick auf Monitoring in „OpenFlow“ Umgebungen.
  - „OpenFlow“: Kommunikationsprotokoll zum Zugriff auf interne Vermittlungseinheiten in Netzkomponenten (Router, LAN-Switche), z. B. zum Zweck der Analyse von Datenströmen (Flows)
  - „SDN“: „Software Defined Networking“

Projekte GÉANT4 (GN4-P1, GN4-P2)

GÉANT4 ist Teil des Rahmenprogramms „Horizont 2020“ der Europäischen Union für Forschung und Innovation. Als Förderprogramm zielt es darauf ab, EU-weit eine wissens- und innovationsgestützte Gesellschaft und eine wettbewerbsfähige Wirtschaft aufzubauen sowie gleichzeitig zu einer nachhaltigen Entwicklung beizutragen. Die netzbezogenen Projekte gliederten sich in die zwei Phasen GN4-P1 und GN4-P2. Auch hier beteiligte sich das RRZE mit seinen Arbeiten gemäß einer Einordnung in entsprechende Activities des Gesamtprojekts.

- SA1: „Network Infrastructure and Services Engineering“,
  Task 2: „Network Engineering and Planning“.
  Methoden zum automatisierten Einsatz von Testpoint Performance Service Oriented Network monitoring Architecture (perfSONAR), einer Reihe von Werkzeuge zur Messung der Netzqualität im europäischen Betrieb, um Dienstgüteparameter und Vereinbarungen jederzeit einhalten zu können.
- SA2: „Trust and Identity and Multi-Domain Services“,
  Task 3: Multi-Domain Service“
  Unterstützung des internationalen perfSONAR-Entwicklungsteams
  bei der Verbesserung und Funktionserweiterung von perfSONAR, einer Messarchitektur für Netzwerkperformancemonitoring, die es ermöglicht, End-to-End-Verbindungen zu überwachen und Performanzprobleme in Netzwerken zu lösen.

- SA3: „Network and Services Assurance“,
  Task 5: „eduPERT“.
  Als Mitglied des GÉANT-eduPERT-Teams Unterstützung der GÉANT NREN Partner aus Forschung und Lehre bei Performanzproblemen in Netzwerken.
  - „eduPERT“: „Performance Enhancement Response Team“
  - „NREN“: „National Research and Education Network“
- JRA2: „Network Services Development“
  Task 2: „Service Provider Architecture (OSS & BSS)“
  Task 3: „GÉANT-Testbedservice“
  Weiterentwicklung des GÉANT-Testbeds Services (GTS) und Gewinnung neuer Nutzergruppen, Ausbau von Benutzerverwaltung und Projektverwaltung

Die Arbeiten der FG-Netz in den Phasen von GÉANT4 bauten auf denen der Vorgängerprojekte auf und bezogen sich auf die Schwerpunkte „Monitoring und Performance“, „automatisierte Netzvirtualisierung“ sowie die Beteiligung an der Entwicklung einer Service-Architektur mit entsprechend prototypischer Umsetzung. Die Phase 2 war auch 2018 noch aktueller Projektgegenstand.

7.7.3.3 Virtuelle Netze und Testbedinfrastruktur am RRZE

Neben dem Monitoring und der Entwicklung von Systemen zur Bestimmung von Dienstgüte, Auslastung und Laufzeiten in realen Netzen, wie dem X-WiN des DFN, befasste sich das RRZE auch mit Möglichkeiten zur Schaffung virtueller Testumgebungen, die innerhalb eines Netzes gezielt zusammengestellt und zur Untersuchung des betreffenden Verkehrsverhaltens genutzt werden konnten. Da derartige virtuelle Testbeds unter Verwendung einer vorhandenen physischen Infrastruktur aufgebaut wurden, handelte es sich dabei nicht um Simulationen, sondern um „echte“ Messungen innerhalb real betriebener Netze.

In diesen Rahmen fiel das bereits 2010 gestartete Projekt „Network Innovations over Virtualized Infrastructures“ (NOVI), das am RRZE in Kooperation mit dem DFN-Verein durchgeführt wurde. Es hatte zum Ziel, seinen Nutzern eine virtuelle Plattform zur Verfügung zu stellen, die sich über eine Föderation von europaweiten Testbeds spannte, so z. B. über das EU-Testbed „Federated E-Infrastructure Dedicated to European Researchers Innovating in Computing Network Architectures“ (FEDERICA) oder über GÉANT. Dabei stellten sich Aufgaben der Entwicklung von Methoden, Algorithmen und Informationssystemen, die es Benutzern ermöglichten, virtuelle Ressourcen, Dienste und spezifische Messstrecken innerhalb der zugrundeliegenden Internetstrukturen zu verwalten und für Untersuchungen verfügbar zu machen. Zur Unterstützung der

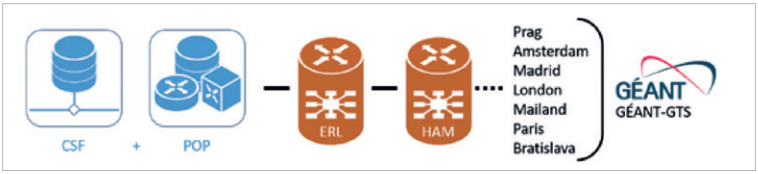
Messungen wurden auch Methoden integriert, die im Rahmen von HADES entwickelt wurden (Kapitel 7.7.3.1). Das Projekt konnte 2013 mit einem ersten Prototyp für virtuelle Netze über föderierte Umgebungen vorerst abgeschlossen werden.

Die Ideen und Werkzeuge von NOVI wurden im Kontext von GÉANT weiterverfolgt bzw. weiterentwickelt. Dort ordneten sie sich z. B. in die Aktivitäten der Bereiche „Testbed as a Service“ (Taas) oder „Software Defined Networking“ (SDN) ein (vgl. Kapitel 7.7.3.2) und führten zum Angebot eines „GÉANT Testbeds Service“ (GTS). GTS ist ein automatisierter Service, der dem Anwender die Möglichkeit bietet, selbst virtuelle Netze über die europäische Infrastruktur für Forschungszwecke zu erstellen. Diese virtuellen Testbeds sind voneinander unabhängige, getrennte virtuelle Netze (Virtual Networks, VN), die erlauben, dass ein Anwender in einer eigenen Testumgebung Experimente durchführen kann, ohne andere Nutzer oder den Produktionsbetrieb zu stören. Dem Anwender stehen für das Einrichten der Netzumgebung verschiedene Ressourcen wie Rechenleistung, Kapazitäten für Routing oder physischer Speicher zur Verfügung, die er reservieren kann.

Analog zum europäischen GÉANT-GTS wurde am Standort Erlangen der deutsche „DFN Generalized Virtualization Service“ (DFN-GVS) 2018 als neuer Pilotservice aufgebaut. Mit der entsprechenden Hardware stellte der DFN-GVS seinen Anwendern am RRZE einen Testbed-Service zur Verfügung, der sich zusammen mit dem GÉANT-GTS in eine Multidomain-Umgebung des europäischen Forschungsnetzes einbinden ließ. Auch eine künftige Erweiterung auf weitere Standorte außerhalb des RRZE wurde damit möglich.

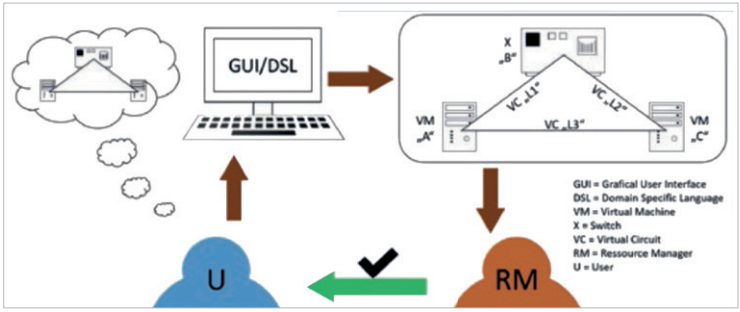
Das Projekt kann unter verschiedenen Aspekten betrachtet werden:

- Grundstruktur der DFN-GVS-Domain
  Die „DFN-GVS-Domain“ setzt sich aus der „GVS-Central-Server-Facility“ (GVS-CSF) für das zentrale Management der GVS-Domain und derzeit einem am RRZE angesiedelten Knotenstandort, dem „Point of Presence“ (GVS-PoP) für die Bereitstellung der Ressourcen, zusammen. Zur Einbindung in den GÉANT-GTS wurde der DFN-GVS über den DFN-X-WiN-Kernnetzknoten mit dem Kernnetzknoten in Hamburg verbunden, der wiederum an das europäische Forschungsnetz GÉANT angebunden ist. Die Abbildung „Grundlegende Infrastruktur“ stellt dies dar.



Grundlegende Infrastruktur

- Anwender des Systems
  Um eigene Ideen, wie zum Beispiel die Entwicklung eines bestimmten Internetprotokolls in einer eigenen Testbedumgebung produktiv evaluieren zu können, benötigen die Anwender zunächst einen Zugang. Beispielsweise können sie als Mitglied einer Forschungseinrichtung ihre Testbedumgebung über eine Web-GUI beantragen, indem sie ihre gewünschten Ressourcen definieren und die Netztopologie beschreiben, die sie für ihre Zwecke reservieren möchten. Diese Beschreibung der Anwenderumgebung basiert auf dem „Domain Specific Language“ (DSL)-Code, der dann auf semantische und syntaktische Korrektheit geprüft wird. In einer neueren Version (GVS-Version 6.0) kann alternativ auch ein visueller Editor verwendet werden. Er ermöglicht, das VN, wie benötigt, per Mausklick und „drag & drop“ zusammenzustellen. Ein Ressourcenmanager stellt schließlich – wenn möglich – die benötigten Ressourcen zur Verfügung. Der Anwender kann sie aktivieren, deaktivieren oder auch wieder freigeben, falls er sie nicht mehr benötigt. Sofern die Ressourcen lediglich deaktiviert sind, bleiben sie noch reserviert. Der Aufbau eines VN ist somit ohne großen zeitlichen Aufwand möglich und erleichtert, die nötige Basis für Forschungsprojekte schnell zu erstellen. Die Abbildung „Planung und Aufbau einer virtuellen Testumgebung“ stellt den Vorgang von der Entwicklung einer Idee über deren Umsetzung mit Hilfe grafischer Schnittstelle (GUI) und abstrakter Beschreibungssprache (DSL) sowie die Reservierung benötigter Komponenten dar. Nach positiver Rückmeldung durch den „Ressource Manager“ steht das erstellte Testbed für Messungen und Analysen zur Verfügung.



Planung und Aufbau einer virtuellen Testumgebung

- Verfügbare Ressourcen
  Ressourcen können für ein regionales Forschungsnetzwerk jeweils individuell zusammengestellt werden. In Erlangen stehen aktuell Ressourcen für den Datenfluss, Routing-Komponenten, virtuelle Maschinen sowie physischer Speicher zur Verfügung.

Die in Erlangen angebotenen Hardware-Komponenten setzten sich (Stand 2018) wie folgt zusammen:

- 3 x Dell-Power-Edge-R-530-Server (Compute Nodes, 1 GE- und 10 GE-Network Interface Connections) für die Bereitstellung virtueller Maschinen,
- 1 x Juniper-MX-80-Router (48*1 GE, 4*10 GE) für Data-Plane-Verbindungen,
- 1 x CORSA DP2100 Switch ermöglicht den Anwendern, OpenFlow Testbeds mit (virtueller) Portbelegung zu definieren, unabhängig von der physischen Portbelegung,

Für das Management bzw. die Control Plane sollte die Konfiguration noch um weitere Server und Netzkomponenten erweitert werden.

Das Projekt zum Aufbau einer Testbedinfrastruktur am RRZE stand 2018 am Anfang einer weiterzuführenden Entwicklung.

7.7.3.4 Forschungsgruppe Netz (Resümee)

Zusammenfassend bezogen sich die Arbeiten der Forschungsgruppe Netz im Schwerpunkt auf Themen der Qualitätssicherung von IP-Netzen und damit verbundenen Messsystemen sowie der Modellierung virtueller Testumgebungen in realen Netzen der Internettechnik. Dabei hat sich die Gruppe durch ihre praxisbezogenen und theoretischen Arbeiten unter Leitung von Dr.-Ing. Susanne Naegele-Jackson nationale und internationale Reputation erworben. Mit ihrer erfolgreichen Projektarbeit wird sie sicher auch weiterhin einen Beitrag zum wissenschaftlichen Profil des Rechenzentrums leisten.

7.7.4 Projekt zur Telefonie über das Intranet (VoIP)

Telefonie und Datenübertragung waren/sind innerhalb von Universitäten in der Regel unterschiedlichen Organisationseinheiten zugeordnet, stehen aber inhaltlich in gewissem Zusammenhang. Während zu den Anfängen der EDV bzw. der DFÜ das Telefonnetz auch zur Datenübertragung genutzt wurde (vgl. Teil 1, Kapitel 1, 2), wurde später das IP-basierte Kommunikationsnetz auch zur Übertragung von Sprachdaten, d. h. zum Telefonieren, eingesetzt (Stichwort: Voice over IP, VoIP). Die Nutzung des Datennetzes zur Sprachübertragung hat gegenüber der konventionellen Technik mit Vermittlungsanlagen, Kupferverkabelung und Telefonapparaten verschiedene Vorteile, da sie keine separate (passive) Infrastruktur benötigt oder mehr Komfort bietet. Allerdings ist die Technik insgesamt komplexer und belegt dann doch Ressourcen des aktiven Netzes (Schnittstellen) oder je nach Ausbau auch dedizierte aktive Komponenten (LAN-Switche). Eine einheitliche Netzbasis kann zwar von Vorteil sein, schafft

aber auch Abhängigkeiten, die bei Parallelbetrieb so nicht gegeben sind, z. B. kann bei Ausfall einzelner Netzkomponenten unter Umständen nicht mehr telefoniert werden. Die Einführung von VoIP und eventuell einhergehender Ersatz der konventionellen Technik sind daher sorgfältig zu überlegen, insbesondere für Bereiche der FAU mit einer vorhandenen Infrastruktur der Telefonie.

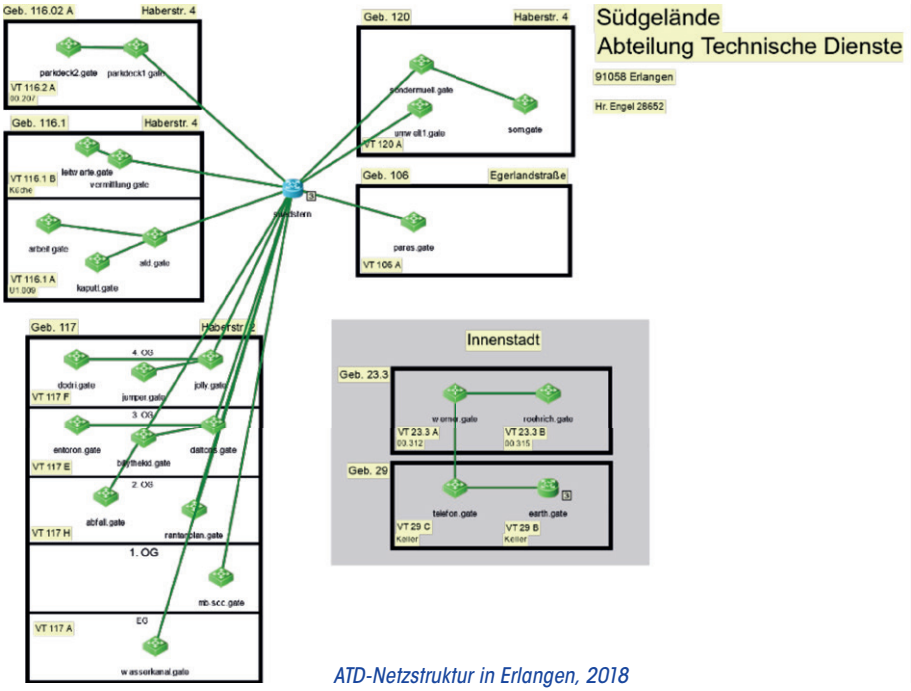
Das RRZE befasste sich bereits 2001 mit der allgemeinen Thematik von „Voice over IP in Weitverkehrsnetzen?“ [*VoIp*] und startete 2012 in der Netzabteilung eine Projektgruppe, die mit Überlegungen und Untersuchungen zu praktischen Umsetzungen im Kontext der FAU begann. In allgemeiner Tendenz verlagerten sich immer mehr klassische Dienste von den bisherigen getrennten Strukturen hinein in das Datennetz. Für die Telefonie bedeutete diese Verschmelzung eine intensivere Zusammenarbeit zwischen der Betriebstechnik als Betreiber der Telefondienste an der FAU und dem RRZE. Im Rahmen des Projekts begann das RRZE mit umfangreichen Markterkundungen auf dem Gebiet VoIP, um eine möglichst breite und unverstellte Sicht über eine potentielle flächendeckende Einführung von VoIP in der Zukunft zu erlangen. Mögliche Einsatzszenarien wurden evaluiert.

Eng mit dem VoIP-Themenkomplex verbunden sind auch Maßnahmen zur Erhöhung der Betriebssicherheit des Datennetzes, wie z. B. der Ausbau redundanter Strukturen, insbesondere im Kontext der zentralen Telefonanlage.

Die praktischen Arbeiten des Projekts zur IP-Telefonie an der FAU enthielten folgende Schwerpunkte:

- Erprobung durch punktuelle Installationen von IP-Telefonen, z. B. im Rechenzentrum
- Verbindung konventioneller Telefonanlagen über das Datennetz, z. B. zwischen der Telefonzentrale in der Erlanger Innenstadt mit Verteilern im Südgelände und an Nürnberger Standorten
- Die Darstellung der „ATD-Netzstruktur in Erlangen“ des IMC-Managers auf S. 208 zeigt die Netzbereiche der Betriebstechnik, die auch zur Verknüpfung von Elementen der IP-Telefonie eingesetzt wird.
- Ausstattung von Neubauten (unter Verzicht auf konventionelle Technik), zum Beispiel am Interdisziplinären Zentrum für nanostrukturierte Filme (IZNF)

Im Rahmen der Inbetriebnahme des IZNF-Neubaus erarbeitete die kooperative Projektgruppe mit Vertretern aus RRZE und ATD/G3 (Betriebstechnik) ein Betriebskonzept für die dort eingesetzten VoIP-Telefone. Die für die Versorgung der dortigen Telefone zuständige zentrale Software des VoIP-Systems wurde neu konzipiert und auf der zentralen RRZE-Infrastruktur installiert. Sie kann als Ausgangsbasis bzw. Muster für eine VoIP-Versorgung der gesamten FAU betrachtet werden.



ATD-Netzstruktur in Erlangen, 2018

7.8 Netzausbau und aktuelle Strukturen

Das Kommunikationsnetz der FAU war nie ein statisches oder fertiges Gebilde, sondern stets von Entwicklungen geprägt, die sich aus steigenden oder neu gestellten Anforderungen, technologischem Wandel aber auch finanziellen Möglichkeiten ergaben. Ein entsprechender Ausbau enthielt somit Maßnahmen zur Erweiterung und Verdichtung (im Sinne einer flächendeckenden Versorgung), Integration neuer Standorte, Verstärkung von Fernverbindungen oder den Austausch im Laufe der Zeit veralteter Komponenten. Sie betrafen sowohl das passive als auch das aktive Netz mit entsprechender Wechselwirkung.

7.8.1 Netzbereich der Zentralen Universitätsverwaltung (ZUV)

Wie die Zentrale Universitätsverwaltung (ZUV) generell, sind auch deren EDV bzw. IT-Dienste Teile der FAU, die vom RRZE entsprechend betreut werden. Dies drückt sich bspw. in der Einrichtung des IT-Betreuungszentrums Halbmondstraße (IZH) oder der Eingliederung des Sachgebiets Datenverarbeitung (SG DV) in die Abteilungsstruktur des RRZE aus (vgl. Kapitel 6.1.1). Ebenso stellt sich die Vernetzung der ZUV als Teil des Kommunikationsnetzes der Universität dar, bildet darin aber einen eigenen, abgeschirmten Bereich. Wegen der Verarbeitung sicherheitskritischer Daten (bzgl. Verwaltung, Haushalt, Personal, Studierenden, vielfältigen Dokumenten usw.) wurde das Netz der ZUV zwar eigenständig und vom wissenschaftlichen Bereich der Universität scharf getrennt, aber doch über einen kontrollierten Übergang damit verbunden (vgl. Kapitel 7.6.5).

Innerhalb des Kommunikationsnetzes der FAU bildete das Netz der ZUV einen eigenen Distributionsbereich, der über eine Firewall an die Erlanger Drehscheibe angebunden war. Mit der Ausweitung angebotener Dienste und intensiverer Nutzung stiegen auch die Anforderungen an den Übergang bezüglich Leistung und Stabilität. Seine Konstruktion mit einer dedizierten Firewall, einem Bereichs-Router sowie der Aufteilung in neutrale (DMZ) und interne Netze wurde den Anforderungen auf Dauer nicht mehr gerecht. Abgesehen von unzureichender Leistungsfähigkeit der eingesetzten Komponenten (Schnittstellen mit „nur“ 1 Gbit/s statt 10 Gbit/s) war auch die Struktur zu überarbeiten. Insbesondere ließ sich eine Einordnung von Servern bzw. Diensten in den Zwischenbereich (DMZ) oder das interne ZUV-Netz aufgrund der Rechner- und Kommunikationsstrukturen der ZUV oft nicht mehr klar treffen. Die neue Konzeption sah daher eine leistungsstarke, integrierende Komponente vor, die sowohl das Routing (Distributionsrouter) als auch bedarfsgerechte Firewallfunktionen zu bzw. zwischen allen Netzen der ZUV übernehmen konnte. Sicherheit und Performanz des Gesamt-

komplexes wurden danach erhöht. Nach Prüfung einer Reihe von Produkten auf ihre Eignung beschaffte das RRZE schließlich 2014 ein Gerät neuester Technologie der ASA-Familie von Cisco.

Gemäß der neuen Konzeption und der Verfügbarkeit erforderlicher Komponenten wurde der Übergang zwischen Wissenschafts- und Verwaltungsnetz in den Jahren 2015 und 2016 komplett neu saniert: Neben dem regulären geräteseitigen Ausbau von Redundanz- und Leistungsreserven wurde für die Server der Verwaltungs-DV und anderer Systeme mit hohem Schutzbedarf und personenbezogenen Daten eine räumliche Abtrennung im RRZE-Datacenter eingerichtet und dort ein Sonderschutzbereich ZUV etabliert. Wie im übrigen Bereich des Datacenters ließen sich Server in diesem Sonderschutzbereich nun sicher, redundant und performant mit mehreren 1- oder 10-Gigabit-Schnittstellen anbinden. Die zuvor oft schwer zu ermittelnde Abwägung zwischen Performanz und Sicherheit konnte damit entfallen.

7.8.2 Netzausbau im Wissenschaftsbereich der FAU

Auch im Zeitraum der in diesem Kapitel betrachteten Phase (2013-2018) erfolgte ein Ausbau der passiven und aktiven Strukturen des Kommunikationsnetzes im Wissenschaftsbereich der Universität.

7.8.2.1 Ausbau des passiven Netzes

Das passive Netz, d. h. die strukturierte Verkabelung, bietet im Sinne der Schicht 1 des Referenzmodells die Basis zum Aufbau aktiver Netzstrukturen und schafft Voraussetzungen zu deren Verbreitung und Leistungsfähigkeit. Entsprechend erfordert es regelmäßig (Bau)-Maßnahmen zur Anpassung an jeweils neu gestellte Anforderungen. Dazu gehören Gebäudesanierung (bspw. durch gigabitfähige Verkabelung für Endgeräte), Erschließung zusätzlicher Gebäude und Standorte, komplette Integration von Neubauten oder die Bereitstellung neuer Übertragungstechniken im Fernbereich.

Gebäudesanierungen und Ausbau betrafen

2014:
- Gebäude Kochstraße 4, Erlangen
- Verteilte Nachverkabelungen zum Anschluss von Kopierern

2017:
- Gebäude der elektrotechnischen Institute Cauerstraße 7, Erlangen Süd
- Sanierung Altbau WiSo, Findelgasse, Nürnberg

Als **neue Standorte**/Gebäude sind hervorzuheben

2014:
- ZUV-Anmietung Hauptstraße 32, Erlangen
- Neubau Chemikum Südgelände, Erlangen
- Nutzung des AEG-Geländes in Nürnberg (Energiecampus EnCn „Auf AEG“)
- Maßnahmen im Rahmen der Anmietung von AREVA-Liegenschaften in Erlangen als Ausweichquartiere zur Überbrückung von Umbauten im Südgelände
- Campus Busan, Südkorea, mit spezieller Anbindung über das Internet

2017:
- Neubau IZNF im Erlanger Südgelände

2018:
- LFT-Prüfzentrum, Nürnberg
- Siemens Technologiepark, angemietete Glasfaserverbindung (Dark Fiber, 1 Gbp/s)
- FAU Digital Health Innovation Platform, Henkestraße 125, Erlangen, Mietleitung Ethernet 1 Gbp/s
- Seminargebäude Stintzingstraße 23, Erlangen, Mietleitung Ethernet 1 Gbp/s
- LS Informatik 14, Carl-Thiersch-Straße 2b, Erlangen, Mietleitung Ethernet 1 Gbp/s

An umgerüsteten oder neuen **Fernstrecken** sind zu nennen:

2015:
- Ergänzung der RiFu-Strecke (bis 600 Mbp/s) durch Anmietung einer „breitbandigen“ (10 Gigabit/s) Übertragungsstrecke der Telekom
- Aufrüstung der Anbindung des LIKE innerhalb von Tennenlohe von 100 Mbp/s-RiFu auf Glasfasertechnik
- Upgrade der Richtfunkverbindung zum Areal „Gossengelände“ (Nägelsbachstraße 25, Erlangen) von 150 auf 300 Mbp/s
- Neuanbindung des Campusareals Uferstadt/Fürth per LW im Rahmen von Umstrukturierungen in Nürnberg über Glasfaserstrecke zum AEG-Campus (vgl. Kapitel 7.8.2.4)
- Upgrade der Anbindung des Areals „AREVA“ auf 10-Gigabit-Technologie
- Anbindung des neuen Standorts der Zentralen Universitätsverwaltung (ZUV) am Bahnhofplatz in Erlangen mit angemieteter Leitung von 100 Mbp/s

2017:
- Anbindung Sternwarte Bamberg mit 1-Gigabit-Festverbindungsleitung

Der Ausbau der strukturierten Verkabelung umfasste 2018 etwa 200 Gebäudegruppen der Universität und ermöglichte damit die Bereitstellung von ca. 65.000 Anschlusspunkten zum Anschluss von Endgeräten der Benutzer (2013 gab es 30.000 Kupfer-Anschluss-(Doppel-)Dosen).

7.8.2.2 Regulärer Ausbau des aktiven Netzes

Entsprechend dem Ausbau der passiven Struktur, erfordert auch das aktive Netz regelmäßig Maßnahmen zu Ausbau und Verbesserungen der Netzversorgung. Diese betrafen ebenso Sanierungen, Ergänzungen und neue Standorte, aber auch Umstrukturierungen.

Mit dem Ziel flächendeckend Endgeräteanschlüsse mit Geschwindigkeiten von 1 Gbp/s anbieten zu können, wurde im **Access-Bereich** schrittweise die Ablösung veralteter Netztechnik der letzten und vorletzten Generationen vorangetrieben. In der Praxis bedeutete dies den Ersatz von LAN-Switchen der Marken 3Com und Allied Telesys (u. a. beschränkt auf 100 Mbp/s) durch zeitgemäße gigabitfähige Geräte der Hersteller Cisco und HP.

Einen speziellen Ausbau erforderten wachsende Anforderungen im zentralen Rechnerraum des RRZE. Im sogenannten „Bunker“ wurden weitere Regalreihen inklusive moderner Netzwerktechnik (500 1- und 10-Gigabit-Anschlüsse) für das Housing von Serverhardware eingerichtet.

Auch auf der Ebene der **Distributionsbereiche** erfolgten verschiedene Sanierungen durch Ersatz älterer Verteilkomponenten und strukturelle Anpassungen, dazu zählten

- die Neugestaltung und Einrichtung des Datacenters als eigener Distributionsbereich (vgl. 7.2.2.2)
- der Verteiler im Campusbereich Röthelheimpark Erlangen (Cisco 6500 gegen 6807)
- der zentrale Datenverteiler des Bereichs High Performance Computing am RRZE
- der Datenverteiler der Campusbereiche in der Nürnberger WiSo
- der Datenverteiler für die zentrale Aggregation von WLAN, VPN und Streulagenkoppelungen (ds9/ds10.gate)
- der Datenverteiler des Campusbereichs Biologikum und Physikum
- der Datenverteilung des zentralen Rechnerraums der Informatik (ehemals EGPA-Raum)

Im Bereich des **Kernnetzes** konnte der **Core**, einschließlich verschiedener Anbindungen von Komponenten der Distributionsebene, ebenfalls durch einzelne Maßnahmen verstärkt werden. Dazu zählten bspw. das Upgrade des stark beanspruchten Kernnetzknotenpunkts Erlangen Süd über den Ersatz des Routers (Cisco 7600) durch ein Gerät neuerer, leistungsfähigerer Technologie (Cisco Nexus). Ebenso gehörte dazu der Ausbau redundanter Strukturen, in dessen Rahmen die Geräte in den Campusgebieten Gossengelände, Ulrich-Schalk-Straße, EWF sowie LIKE durch Komponenten aktueller Bauart (2015) ersetzt und auf redundante Betriebspaare erweitert wurden. Hierzu motivierte nicht zuletzt die zunehmende Nutzung des Datennetzes durch kritische Dienste wie die der Telefonie oder Steuerleittechnik (vgl. Kapitel 7.7.4).

Über den regulären Ausbau hinausgehende Maßnahmen zur Erweiterung bzw. Umstrukturierung des Cores sind Gegenstand eines eigenen Abschnitts (Kap. 7.8.2.4).

7.8.2.3 Ausbau durch Erschließung neuer Standorte , Gebäude

Die Aufnahme neuer Standorte in das Kommunikationsnetz erforderte in der Regel (je nach Gegebenheiten) Maßnahmen zur strukturierten Verkabelung, d. h. die Schaffung von Strukturen innerhalb der betreffenden Gebäude (Ebenen 2 und 3) und einer Verbindung zum bestehenden Netz. Darauf aufbauend konnten dann in Ergänzung des aktiven Netzes jeweils Distributionsbereiche und ihre Anbindung an das Kernnetz eingerichtet werden.

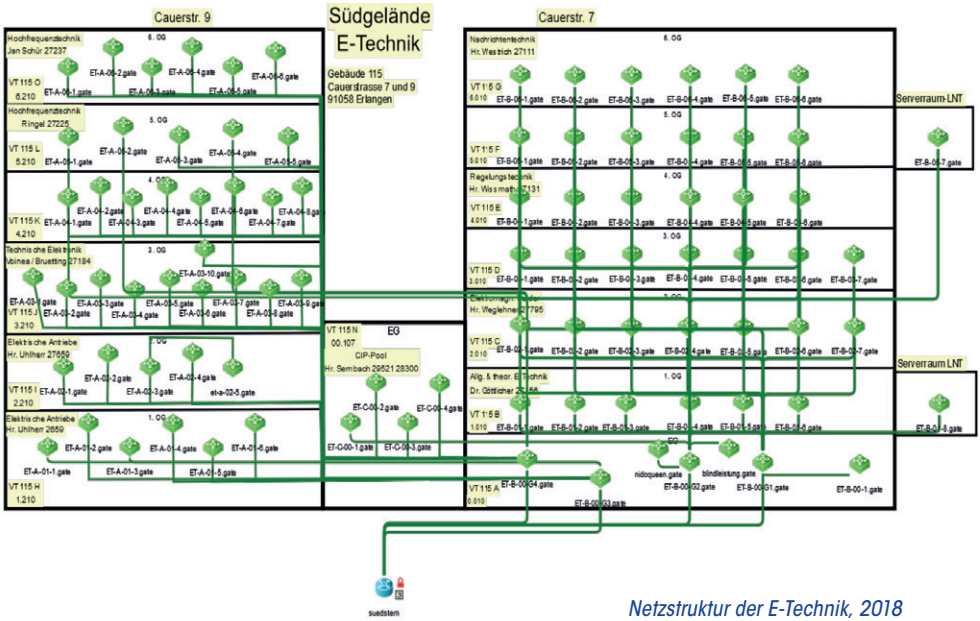
Im Zusammenhang mit dem Ausbau des passiven Netzes (Kapitel 7.8.2.1) wurden bereits einige neu hinzugekommene Standorte angeführt, verschiedene prägnante Punkte werden im Folgenden näher beschrieben:

- AREVA-Liegenschaften, Erlangen-Tennenlohe
  Die Universitätsleitung entschied sich, freiwerdende Räume des Nuklearkonzerns Areva in Erlangen-Tennenlohe anzumieten. Ziel war die Schaffung von Ausweichquartieren für verschiedene Institute, deren Stammsitz renoviert oder sonst zeitweilig geräumt werden mussten. Ersten Anstoß hierfür gab die erforderliche Notsanierung (Deckeneinsturz) der Philosophischen Fakultät (Erlangen, Kochstraße), wo das dortige Gebäude kurzfristig komplett gesperrt werden musste. Durch die Wechsel der Nutzergruppen und sich entsprechend verändernde Anforderungen, war ein flexibles Netzkonzept erforderlich. Zur Einweihung Ende 2013 war der Komplex mit einer Infrastruktur versorgt, die mehr als 1.100 Netzwerkanschlüsse erlaubte. Die Außenanbindung führte über eine eigens angemietete Festverbindung von 1 Gbp/s. Die Ausweichräumlichkeiten im ehemaligen AREVA-Firmensitz erfreuten sich mit der Zeit zunehmender Beliebtheit. 2016 konnte die Anbindung zur Erhöhung der Performanz auf 10-Gigabit Technologie angehoben werden.
- Busan, Südkorea
  Die 2014 eingerichtete Anbindung der FAU-Außenstelle in Busan/Südkorea (Campus Busan) stellt eine Besonderheit dar: Die Technik der dortigen Liegenschaft wird von einem ortsansässigen Dienstleister betreut und durch koreanische Provider mit Netzzugang versorgt. Die Verbindung führt somit über die Strukturen des Internet (einschließlich X-WiN) zum RRZE und zwar unter Nutzung des zentralen VPN-Einwahldienstes der FAU. Dadurch ist die Nutzung der FAU-Ressourcen (bspw. Lizenzen, Groupware) durch die Kolleginnen und Kollegen vor Ort in Korea gesichert möglich.
- AEG-Komplex, Nürnberg
  Das aus mehreren Gebäuden bestehende, ehemalige Gelände der Firma AEG in Nürnberg, Fürther Straße (AEG-Komplex) wurde von der FAU als zusätzlicher Stand-

ort zur Unterbringung von Forschungseinrichtungen und kooperierenden Partnern ausgewählt. In diesem Zusammenhang erfolgte 2014 die Ausrufung zum neuen „Hightech Campus“, aus dem dann 2015 der neue „Nuremberg Campus of Technology“ (NCT) „auf AEG“ hervorging. Die FAU hat dort auf dem Gelände mehrere Liegenschaften angemietet bzw. übernommen und bringt sich unter dem Dach des „Energie Campus Nürnberg“ (EnCN) in eine Kooperation wissenschaftlicher Partnerinstitute auf dem Gebiet der Energieforschung ein. Gemeinsam an einem Campus forschen die EnCN-Wissenschaftler an neuen Technologien zur Realisierung der Energiewende. Da keine Netzinfrastruktur in dem Komplex vorhanden war, waren entsprechende Baumaßnahmen zum Aufbau einer Verkabelung erforderlich. Die Außenanbindung erfolgte zunächst über eine Richtfunkstrecke zum Nürnberger Core-Standort in der Langen Gasse, bis diese durch eine Datenverbindung der Deutschen Telekom abgelöst werden konnte (2015) und seitdem die Übertragung von Nutzdaten mit einer Geschwindigkeit von bis zu 10 Gbp/s möglich wurde. Dies schuf auch die Grundlage zur Erweiterung des Cores und einer Neugestaltung der Standort-Verbindungen im Bereich Nürnberg/Fürth mit erheblich schnelleren Übertragungsgeschwindigkeiten (vgl. nächstes Kapitel 7.8.2.4).

- Chemikum, Erlangen-Süd
  Im Rahmen der Errichtung des Chemikums im Südgelände der Universität wurden die Arbeiten zur Verkabelung des Neubaus im Jahr 2014 abgeschlossen. Ebenso wurde die Installation des aktiven Netzes vom RRZE fertiggestellt und in Betrieb genommen. Das Netz wurde als eigener Distributionsbereich ausgelegt (angebunden am Core Erlangen Süd) und bestand aus einem Router mit interner Redundanz (Steuereinheit, Stromversorgung) und 20 LAN-Switchen, die in einer Sternstruktur jeweils mit 10 Gbp/s untereinander verbunden wurden. Die Subnetze der Benutzer wurden durch entsprechende VLAN-Zuordnungen auf die Anschlussschnittstellen der Switche gelegt und können jederzeit nach Bedarf modifiziert werden.
- Elektrotechnik, Erlangen-Süd
  Im Rahmen einer generellen, bautechnischen Sanierung des Gebäudes der E-Technik im Erlanger Südgelände wurde auch die Verkabelung komplett neu strukturiert. Entsprechend wurde auch das aktive Netz neugestaltet. Die Netzinfrastruktur des 2018 fertiggestellten Turms A bestand damit aus 45 neu aufgebauten und strukturiert angebundenen Switchen zur Versorgung von insgesamt rund 1.600 Endanschlüssen. Als Beispiel ist hier die neu aufgebaute „Netzstruktur der E-Technik“ in einer Abbildung auf S. 215 des Managers IMC dargestellt. Darin sind Einzelheiten zwar nur bedingt nachzuvollziehen, aber man erkennt die beiden Gebäudeblöcke („Cauerstraße 9“ und „Cauerstraße 7“) mit je sechs Etagen sowie den Mitteltrakt im Erdgeschoss („EG“). Das aktive Netz bildet einen Access-Bereich aus vier Teilen mit je einem eigenen Verteiler („ET-B-00-G1/2/3/4“, untere Zeile des rechten Blocks), die nach außen an

die Distributionskomponente des Südgeländes („suedstern“, unterer Bildrand) angeschlossen sind. Entsprechend der strukturierten Verkabelung sind die LAN-Switche für die Endgeräte in den Etagen verteilt und jeweils mit einem der Verteiler verbunden (bspw. „ET-A-06-02“, 6. OG des linken Blocks). Innerhalb dieser physischen Struktur sind die logischen VLANs bzw. IP-Subnetze nach Bedarf verteilt und den Anschlussports für Endgeräte zugeordnet. (Diese Zuordnungen können natürlich jederzeit auf Anfrage über das zentrale Management des RRZE modifiziert werden.)



Netzstruktur der E-Technik, 2018

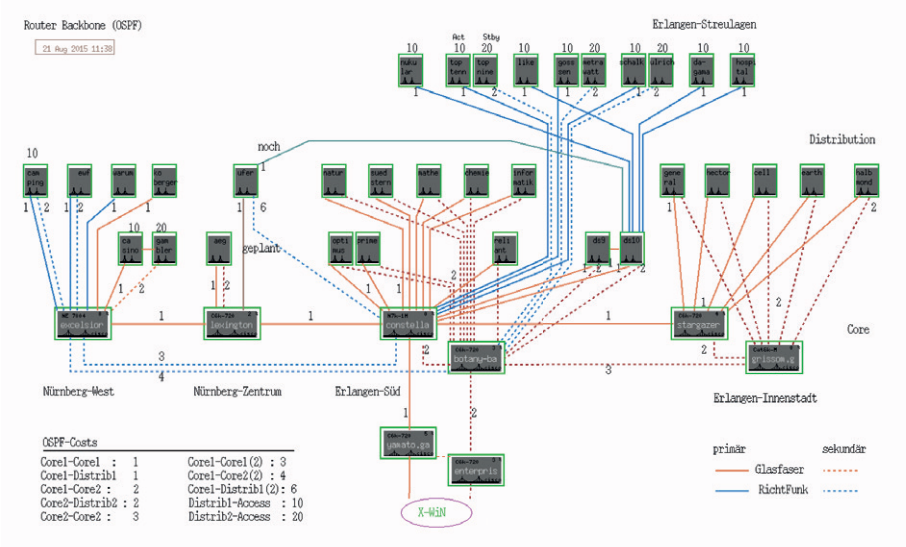
7.8.2.4 Erweiterung der Kernnetzstruktur

Mit der Integration des Standorts „auf AEG“ in Nürnberg ergaben sich auch neue Möglichkeiten zur deutlichen Verbesserung der Verbindungsstrecken innerhalb Nürnbergs, aber auch nach Erlangen. Der erwünschte Bau einer eigenen LWL-Trasse zwischen Erlangen und Nürnberg war aus finanziellen wie organisatorischen Gründen ebenso nicht durchführbar, wie die Anmietung einer entsprechenden Verbindung zwischen der WiSo und dem RRZE zu tragbaren Gebühren. Generell hing/hängt die Verfügbarkeit von Glasfaserstrecken sehr stark von den potentiellen Providern und deren

vorhandener Infrastruktur ab, da insbesondere eventuell erforderliche Baumaßnahmen auf öffentlichem Grund gravierende Kosten verursachen und sich auf die Höhe der Mieten niederschlagen.

In diesem Sinne waren für den AEG-Komplex deutlich bessere Voraussetzungen gegeben als für den Core-Standort an der Nürnberger WiSo. So konnten nach entsprechender Markterkundung durch Verhandlungen mit der Deutschen Telekom zur Bereitstellung und Preisgestaltung sowie der zentralen Universitätsverwaltung zur Übernahme der dennoch nicht unerheblichen, laufenden Kosten zunächst eine Glasfaserverbindung vom AEG-Komplex zum RRZE, dann zur WiSo in Betrieb genommen werden. Ergänzend konnte über eine vertragliche Vereinbarung mit der Feuerwehr der Stadt Nürnberg eine LWL-Leitung zum Campusareal Uferstadt/Fürth angemietet werden. So wurde auch der Großraum Nürnberg-Fürth „breitbandig“ (bis 10 Gbits) an das universitäre Datennetz samt Internet angeschlossen, d. h. in gleicher Weise versorgt wie die Standorte in Erlangen.

Die so geschaffene, neue passive Basis legte auch eine Umgestaltung der aktiven Struktur nahe, nämlich die Erweiterung des Kernnetzes um einen vierten Core-Router „auf AEG“.



Router-Struktur (Core, Distribution), 2015

Die abgebildete „Router-Struktur“ auf S. 216 stellt den erweiterten Aufbau dar. Sie enthält in der mittleren Zeile die vier Core-Standorte Erlangen Innenstadt (Router „stargazer“, „grissom“ in der Telefonzentrale), Erlangen-Süd (Router „constellation“, „botany“ im RRZE), Nürnberg Zentrum (Router „lexington“, neu auf AEG) und Nürnberg-West (Router „excelsior“ in der WiSo). Diese sind darin primär in einer Reihe über LWL verbunden (rote, durchgezeichnete Linien). In bestimmten Ausfallsituationen übernehmen die sekundären Strecken (blaue, gestrichelte Linien) die Übertragung teils in LWL-, teils in Richtfunk- Ausprägung. Oberhalb des Cores sind die verschiedenen Distributionsrouter und ihre Verbindungen zum jeweils zuständigen Core-Router dargestellt, darunter ist die Drehscheibe (Router „enterprise“, „yamato“) mit dem externen Übergang zum X-WiN skizziert. Die Wegelenkung zwischen den Routern erfolgt über das Routingprotokoll OSPF, das auch in bestimmten Störfällen für das Umschalten auf Ersatzwege sorgt. Hierzu helfen den Verbindungen zugeordnete Prioritäten (OSPF-Costs), die zur Bewertung bei der Wegwahl ausgewertet werden.

7.8.2.5 Ausbau des nicht drahtgebundenen Netzes (WLAN)

Das nicht drahtgebundene Netz (WLAN, vgl. Kapitel 6.3) stellt eine Erweiterung des Kommunikationsnetzes um Zugänge für mobile Endgeräte dar und kann so der Access-Ebene zugeordnet werden. Es wurde mit der Zeit als selbstverständlicher, fester Bestandteil des universitären Datennetzes angenommen. Bei Neuerschließungen von Liegenschaften hat die WLAN-Versorgung inzwischen in der Regel die gleiche Wertigkeit wie das drahtgebundene Netz erreicht. Gleichzeitig stellten sich dem WLAN immer größere Herausforderungen: So besaßen immer mehr Personen Zweit- oder gar Drittgeräte, wurden die angestrebten Übertragungsraten immer höher und immer mehr Geräte verlagerten sich vom drahtgebundenen in den drahtlosen Bereich.

Entsprechend galt es auch in diesem Zusammenhang die WLAN-Strukturen auszubauen, Kapazitäten und Leistungen zu erhöhen sowie mit technischen Entwicklungen Schritt zu halten. Dies spiegelte sich 2018 im Austausch von ca. 400 Access Points der ältesten Generation und dem Ersatz von 20 LAN-Switchen mit Schnittstellen (Power over Ethernet, PoE) zur Energieversorgung und Datenableitung dieser APs wider.

Wurden 2011 noch 1.750 Access Points mit einer gleichzeitigen Aktivität von bis zu 2.000 Nutzern (vgl. Kapitel, 6.3.5.3) betrieben, waren 2018 über 1.800 Zugangspunkte regelmäßig mehr als 10.000 Nutzer gleichzeitig im WLAN aktiv.

In Ergänzung zum WLAN der FAU beteiligte sich die Universität auch an der Initiative des Bayerischen Staatsministeriums der Finanzen und für Heimat zur Bereitstellung eines WLANs für „jedermann“. Das von der bayerischen Staatsregierung im Jahr

2015 initiierte Projekt „BayernWLAN“ will einen möglichst weit verfügbaren freien WLAN-Zugang innerhalb Bayerns schaffen. Zu diesem Zweck gingen bis zum Jahr 2020 rund 20.000 Access Points bayernweit an unterschiedlichsten Standorten in Betrieb. Nach den Planungen des RRZE erfolgte die Realisierung von BayernWLAN an der FAU über die zahlreichen vorhandenen Access Points des RRZE, der darüber vermittelte Internetzugang ist jedoch komplett losgelöst vom Datennetz der FAU bzw. von dessen verwendetem Internetzugang über das Deutsche Forschungsnetz (DFN). Stattdessen wird der Datenverkehr aller BayernWLAN-Teilnehmer über eine eigens bereitgestellte Glasfaserleitung direkt zum Provider Vodafone weitergeleitet, der im Auftrag des Freistaates Bayern die gesamte Infrastruktur hinter BayernWLAN betreibt und gleichzeitig allen weitergehenden Anforderungen (Landingpage, Jugendschutzfilter, ...) nachkommt.

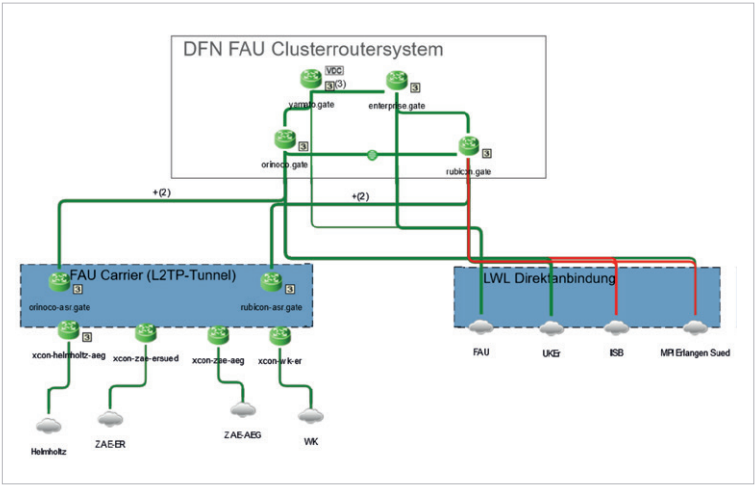
7.8.2.6 Ausbau des externen Anschlusses zum X-WiN

Die Schnittstelle des Kommunikationsnetzes der FAU zum Deutschen Forschungsnetz X-WiN steht für die generelle Anbindung der Universität an das Internet. Da das RRZE einen Kernnetzknoten des X-WiN beherbergt, gestaltet sich die physische Verbindung relativ einfach. Dieser Übergang ist durch hohe Inanspruchnahme gefordert. So betrug der Tagesumsatz im Jahr 2015 über zwölf Terabyte und stieg 2018 auf 60 Terabyte an. Das RRZE ist in Kooperation mit dem DFN daher stets bestrebt, die Übertragungsleistung gemäß verfügbarer Technologie auf einem möglichst hohen Niveau zu halten. So konnten bereits 2013 zwei (redundant geschaltete) Interfaces von je 10 Gbp/s in Betrieb genommen und 2018 die Geschwindigkeiten auf je 20 Gbits verdoppelt werden. An eine weitere Erhöhung in Richtung 40 oder 100 Gbits ist gedacht. Neben verfügbarer Technik sind allerdings auch die Kosten bzw. Gebührengestaltung zur eventuellen Umsetzung mitzuberücksichtigen.

Neben dem technischen Ausbau des Übergangs erfolgte auch eine Revision der Netzversorgungsgrundlagen in Bezug auf die der FAU angeschlossenen Dritteinrichtungen.

Damit das RRZE in Zukunft in Zusammenarbeit mit dem DFN-Verein Hochschulen bzw. hochschulnahen Einrichtungen der Region Netzzugänge zur Verfügung stellen kann, erfolgte eine vertragliche Umstellung des X-WiN-Zugangs der FAU vom bisherigen Modell des Regelanschlusses zum Clusteranschluss, die 2014 abgeschlossen wurde. Danach konnten Kunden anderer Hochschuleinrichtungen im Auftrag des DFN-Vereins mit Zugang zum XWiN als sog. DFN-Clusterkunden versorgt werden. Dies ermöglichte Einsparung von Kosten sowie die Bündelung von Ressourcen, kam allen Seiten zugute und stärkte den Standort Erlangen in seiner Funktion als überregionaler Knotenpunkt.

Die Abbildung „Erlanger WiN-Anschluss und Clusterkunden“ stellt die beiden redundanten Router (yamato, enterprise) am externen Übergang dar, an denen das FAU-Netz per LWL direkt angeschlossen ist (grüne Linie von enterprise zu FAU), der Zugang des Klinikums (UKEr) über die Zwischensysteme (orinoco, rubicon) führt und entfernte Institutionen über Tunnel (L2P-Tunnel) im FAU-Netz am WiN angebunden sind wie bspw. das Helmholtz-Institut Erlangen-Nürnberg (Helmholtz) auf dem AEG-Gelände in Nürnberg (in der Abbildung links unten).

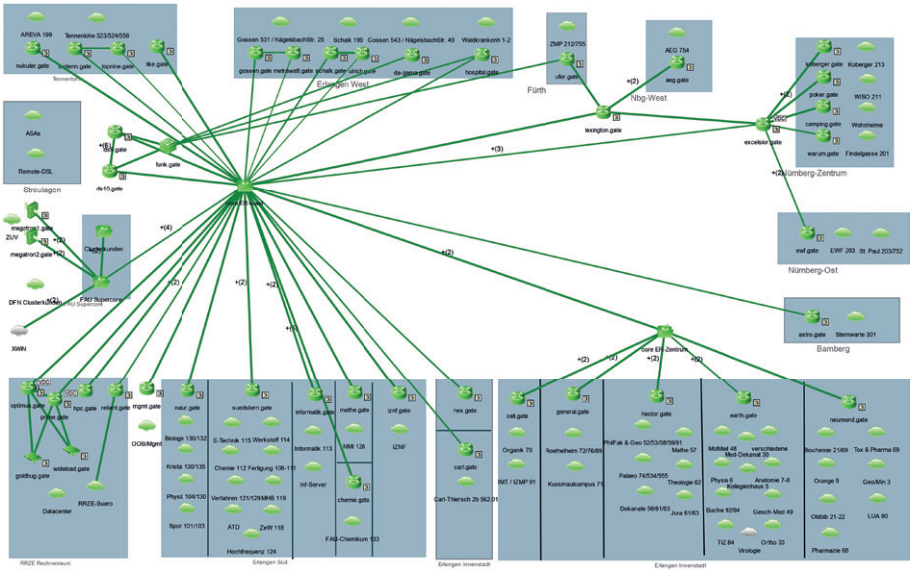


Erlanger WiN-Anschluss und Clusterkunden

7.8.3. Struktur des Kommunikationsnetzes der FAU (Stand 2018)

Die Darstellung aus dem Netzwerkmanagementsystem IMC zum „Aufbau und Status des aktiven Wissenschaftsnetzes des FAU“ stellt die Struktur des Kommunikationsnetzes gemäß Stand im Jahr 2018 dar.

Darin enthält der mittlere Teil der Abbildung mit weißem Hintergrund die Core-Komponenten (zeichnerisch etwas anders bezeichnet und angeordnet als in der NMS-Abbildung der „Router-Struktur in Kapitel 7.8.2.4 auf S. 2016, aber in derselben Verknüpfung), und zwar „ER-Zentrum“, „Er-sued“, „lexington“ (Standort Nürnberg West) und „excelsior“ (Standort Nürnberg Zentrum). Die grau hinterlegten Felder stehen für die Distributionsbereiche und deren Anbindung an den jeweiligen Core-Router. Am linken Bildrand sind die Komponenten der Drehscheibe dargestellt („enterprise“, „yamato“),



Aufbau und Status des aktiven Wissenschaftsnetzes des FAU, 2018

die an den Core Er-sued angebunden sind und den Übergang zum X-WiN herstellen. Zudem stellen sie die Verbindung zum ZUV-Netz her (Router „megatron1/2“) und enthalten die Schnittstellen zu den verschiedenen Clusterkunden.

Das aktive Netz enthielt 2018 insgesamt 80 Router und 1.600 LAN-Switche. Eine grobe Abschätzung der am Netz angeschlossenen Endsysteme bietet die Anzahl der vom RRZE verwalteten IPv4-Adressen, also derjenigen, die im Nameservice DNS eingetragen waren. Das waren 2018 insgesamt 152.808 Adressen, aufgeteilt in öffentliche (28.463) und private (125.345) private Adressen. Davon waren 108.718 Geräte zusätzlich IPv6-Adressen zugeordnet (4.358 öffentliche, 104.360 private). Geräte ohne IPv4-, also nur mit IPv6-Adresse, kamen in der Regel nicht vor.

7.9 Zusammenfassung des Abschnitts und Ausblick

Das Kommunikationsnetz der FAU hat auch in der betrachteten Periode im Rahmen von Ausbau und Verstärkungen verschiedene Veränderungen erfahren. Die Abbildung „Verteilte Netzbereiche der FAU“ stellt deren Standorte mit ihren Verknüpfungen im Überblick dar, gemäß Stand von 2018. Besonders hervorzuheben sind dabei das Hinzukommen des AEG-Geländes in Nürnberg (Auf AEG) und vor allem aber die in diesem Zusammenhang möglich gewordenen „schnellen“ Glasfaserverbindungen zwischen Erlangen und Nürnberg, über die eine gleichwertige Netzversorgung beider Städte der Universität erreicht werden konnte. Dies gilt darüber hinaus auch für die verstärkte Einbindung des Fürther Standorts (Uferstadt) in die umfassende Netzinfrastruktur.

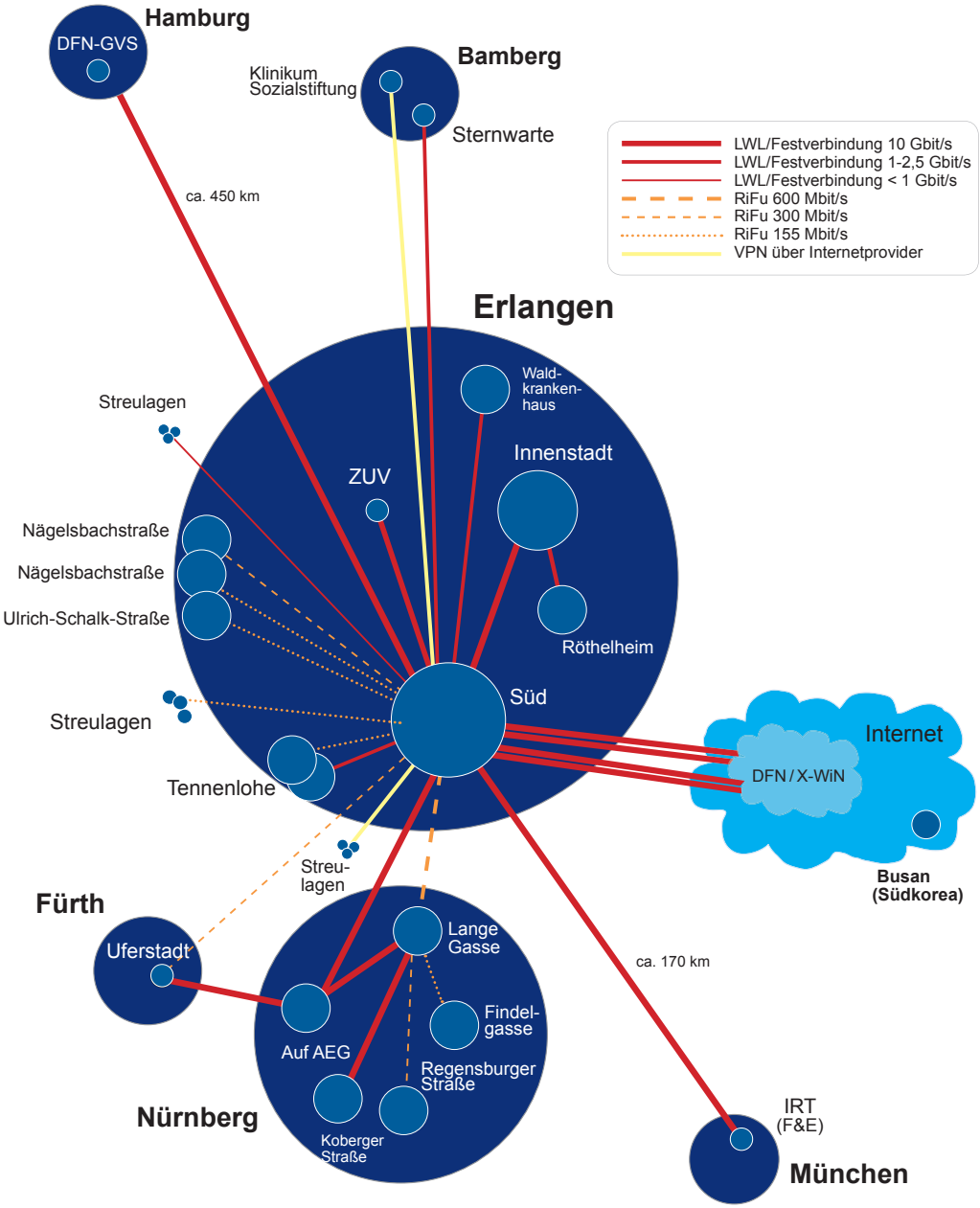
Auch in den Nahbereichen (Distribution, Access) erfolgten einige Maßnahmen, die die Sanierung bestehender Gebäude (bspw. zur Versorgung der Endteilnehmer mit höheren Anschlusskapazitäten) oder die Integration neuer Gebäude betrafen und natürlich auch den Ausbau der Funk-LAN-Strukturen für mobile Anwendungen.

Wichtig für die Durchführung eines stabilen Betriebs (vgl. Kapitel 8.3) waren auch verschiedene Anpassungen bezüglich der Regelung von Verantwortlichkeiten und eines zentralen Netzmanagements, wodurch der Betrieb effektiver gestaltet werden konnte und Störungen durch Fehlbedienungen von Nutzerseite deutlich weniger vorkamen.

Mit der Einführung einer neuen Gerätegeneration (vornehmlich im Bereich des Serverzentrums) oder dem verstärkten Einsatz einer „neuen“ Internetprotokollversion (IPv6) wurden Grundlagen zur technischen Weiterentwicklung geschaffen, mit der das Netz auch künftig den Anforderungen des IT-Dienstleisters RRZE und seinen vielfältigen Anwendungen gerecht werden kann.

Allein das Anwendungsfeld rund um Videoübertragungen wird etwa im Hinblick auf Arbeiten im Heimbüro, Online-Lehrangebote oder Konferenzen künftig noch mehr Netzkapazitäten (Übertragungsleistung, Verzögerungszeiten, …) erfordern. Ebenso könnte eine verstärkte Einbindung der Telefonie (VoIP) erhöhte Ansprüche (Leistung, Zuverlässigkeit) an das Kommunikationsnetz stellen.

Angesichts der immer noch zu erwartenden, steigenden Anforderungen (qualitativ und quantitativ) an das Netz, wird sich der Bedarf an bzw. der Trend zu höheren Übertragungsgeschwindigkeiten weiter fortsetzen. Dies gilt nicht nur für die Bereiche des Backbones oder der Serveranbindung (hier werden nach 10 und 40 sogar schon 100 Gbit/s anvisiert), sondern auch für die Verteilung und Versorgung mit Endgeräteanschlüssen. Entsprechende Umsetzungen hängen allerdings auch stark von verfügbaren Sach- und Personalmitteln ab. Im aktiven Netz werden an vielen Stellen



Struktur des FAU-Wissenschaftsnetzes (mit Fernnetz), 2018

(selbst auch im Backbone) noch Komponenten eingesetzt, die von den Herstellern schon länger als „out of life“ gekennzeichnet, zwar meist noch funktionsfähig, aber nicht mehr wartungsfähig und in ihren Leistungen nicht mehr erweiterbar bzw. auf aktuellen Stand zu bringen sind. Ihr Austausch scheiterte bisher an finanziellen Mitteln. Bleibt zu hoffen, dass betreffende Komponenten durchhalten und Besserung in Aussicht ist.

Die hierarchische Architektur, die strukturierte Verkabelung, virtuelle lokale Netze (VLANs, LAN-Switching) und das Internetprotokoll (Subnetze, Routing) werden auf absehbare Zeit wohl weiter die Grundlage des Kommunikationsnetzes bilden. Ebenso stehen voraussichtlich wieder Ausbau-, Sanierungs- und Umgestaltungsmaßnahmen an, man denke etwa nur an die geplante Verlagerung der ehemaligen EWF in Nürnberg oder den Umzug der Philosophischen Fakultät von der Erlanger Innenstadt in den „Himbeerpalast“ (ehemaliges Siemensgebäude in Erlangen). Ungewiss ist dabei, ob bzw. wieweit RRZE und FAU von der Neueinrichtung der Technischen Universität Nürnberg (TUN) betroffen sein werden.

Das RRZE wird auch weiter bestrebt sein, das Kommunikationsnetz der FAU und dessen Betrieb im Rahmen seiner Möglichkeiten optimal zu gestalten, um mit der soliden Grundlage seine Funktion als IT-Dienstleister der Universität erhalten bzw. ausbauen zu können.

Zeitübergreifende Statistiken 1968 – 2018

8. Phasenübergreifende Betrachtungen, Statistiken

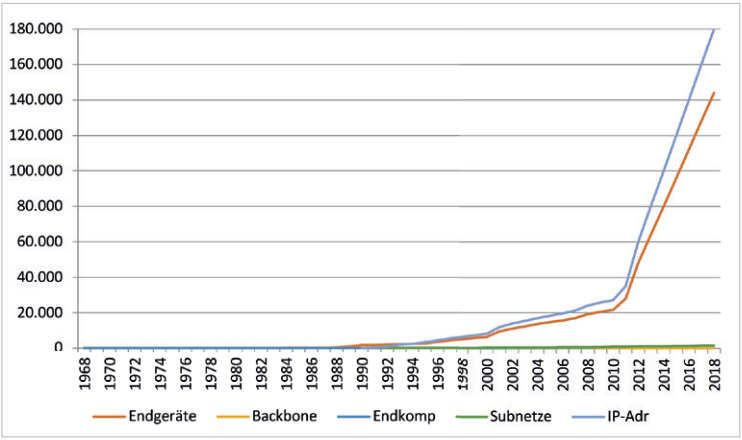
Verschiedene Aspekte der gesamten Entwicklung des Kommunikationsnetzes über die einzelnen Phasen und Zeitabschnitte hinweg lassen sich an Hand verschiedener Parameter kompakt beschreiben, d. h. mittels entsprechender Statistiken und Grafiken im Überblick verdeutlichen.

8.1 Ausbauparameter (Endgeräte und Netzkomponenten)

Der Ausbaustand des Netzes stellt sich auch über die Anzahl seiner Komponenten und der angeschlossenen Endgeräte dar. Für die vom RRZE betreuten Netzkomponenten bildeten Jahresberichte und interne Aufzeichnungen des Rechenzentrums eine solide Basis zur Aufstellung entsprechender Daten. Dagegen ließen sich die Zahlen der Komponenten mit Anschlüssen für Endgeräte, insbesondere nach der Einführung lokal betreuter LAN-Switche, nur grob (nach unten) abschätzen, da sie in dezentraler Administration durch verteilte Institutionen meist nur unzureichend oder vom RRZE nicht einsehbar dokumentiert wurden. Ähnliches galt für die Anzahl der Endgeräte, die in den ersten Jahren durchgängiger, zentraler Versorgung noch gut erfasst wurden, dann aber kaum noch zu ermitteln waren. Allerdings bot die Einführung und Verbreitung des Internetprotokolls in der FAU-Vernetzung auch eine neue Möglichkeit, die Anzahl der angeschlossenen Endgeräte abzuschätzen. Es wurde nämlich zur Pflicht, alle derartig betriebenen Geräte im zentralen Nameservice (DNS) des RRZE anzumelden und in diesem Sinne erfassen zu lassen. Obwohl diese Vorschrift von den Nutzern nicht in jedem Fall eingehalten wurde, man außer Betrieb genommene Geräte oft nicht wieder abmeldete oder aber auch zu manchen Geräten mehrere Adressen gehörten, ergab sich aus den eingetragenen IP-Adressen auch eine Grundlage zur Abschätzung der Gerätezahlen. Der dazu gewählte Ansatz mit einem Verhältnis von 80 (Endgeräten) zu 100 (IP-Adressen) sollte der Realität ziemlich nahekommen.

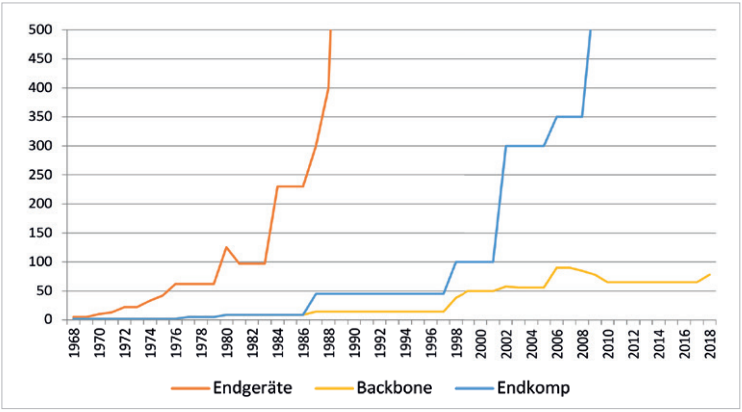
Die Aufstellung der Daten seit der Gründung des RRZE enthält je nach Entwicklungsphase teilweise sehr unterschiedliche Komponenten, die sich zwar nicht direkt miteinander vergleichen lassen, aber doch gemäß ihrer Bedeutung und Funktionalität entsprechend einzuordnen sind.

Die gesamte „Gerätestatistik, 1968 – 2018“ auf S. 227 stellt pro Jahr die Anzahl der Endgeräte, der jeweiligen Komponenten des Backbones, der Komponenten für Endgeräteanschlüsse sowie die auf IP bezogenen Zahlen der Subnetze und IPv4-Adressen dar. In der Gesamtansicht dominieren die jüngeren Zahlen der IP-Adressen in ihrer Größenordnung (z. B. 2018: 180.000), sodass die Verläufe der anderen Werte kaum differenzierbar zu erkennen sind.



Gerätestatistik, 1968 - 2018

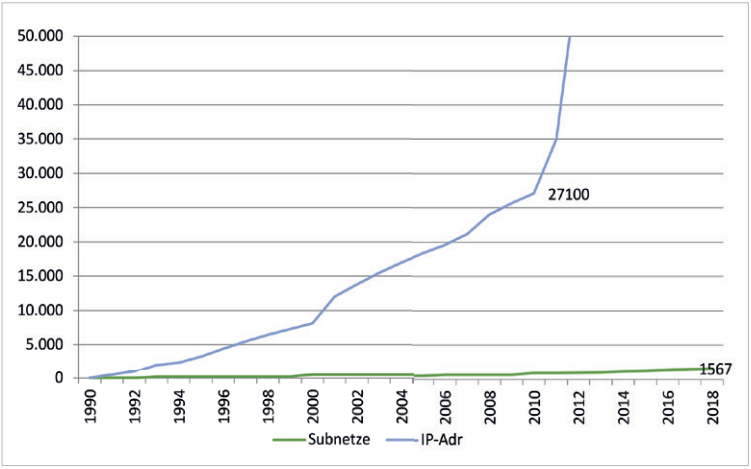
Betrachtet man die Statistik ohne Einbeziehung der IP-Adressen, so ist bei angepasster Skalierung die „Entwicklung der Gerätezahlen“ deutlicher zu erkennen. Allerdings verlassen darin die Kurven „Endgeräte“ ab 1989 und „Endkomp.“ ab 2009 wegen Überschreitens der Grenze von 500 den in der Grafik angezeigten Bereich. Während der weitere Verlauf der Endgerätekurve in der Grafik der gesamten „Gerätestatistik“ gut erkennbar ist, sei zur Ergänzung angegeben, dass die Anzahl der Komponenten zum Anschluss von Endgeräten zwischen 2009 und 2018 von 580 auf 1588 relativ gleichmäßig gestiegen ist.



Entwicklung der Gerätezahlen

Die angezeigten Stufen bzgl. der Endgeräte und Anschlusskomponenten entsprechen dabei mehr den nicht immer kontinuierlich erfolgten und teilweise geschätzten Datenerfassungen als den tatsächlichen Steigerungen, die sicher etwas weniger sprunghaft verlaufen sind. Ziemlich genau hingegen ist die Entwicklung der Backbone-Komponenten dokumentiert. Sie ist durch relativ gleichmäßige Abschnitte und moderate Anstiege gekennzeichnet. Je nach eingesetzter Technologie stellt sie die Anzahl von Multiplexern, X.25-Vermittlern, LAN-Switchen, IP-Routern oder ATM-Knoten dar. Der etwas „unglatte“ Verlauf zwischen 2004 und 2010 ist durch Auf- und Abbau von ATM-Geräten als phasenweise Bestandteile des Backbones zu erklären.

Die Grafik „IP-Adressen und Subnetze“ zeigt die Entwicklung der vergebenen Adressen seit der Einführung der IP-Netztechnik an der FAU. Dabei entsprechen die Einzeladressen (IPv4) aktuell grob den angeschlossenen Endgeräten, während die Subnetze weitgehend den verteilten, virtuellen LANs zuzuordnen sind. Wie auch in der Gesamtstatistik wurden sowohl Adressen aus dem Class-B-Bereich der FAU (131.188.x.x), als auch private Adressen (z. B. 10.x.x.x) bei der Bestimmung der Anzahlen berücksichtigt. Auch in dieser Darstellung ist die Skalierung angepasst (und die Kurve ab 2011 abgeschnitten), um die Anzahl der Subnetze besser erkennbar zu machen. Da jedem IPv6-Gerät in der Regel (bisher) auch eine IPv4 zugeordnet ist, würde eine Einbeziehung dieser Protokollversion (derzeit) keinen zusätzlichen Beitrag erzeugen.

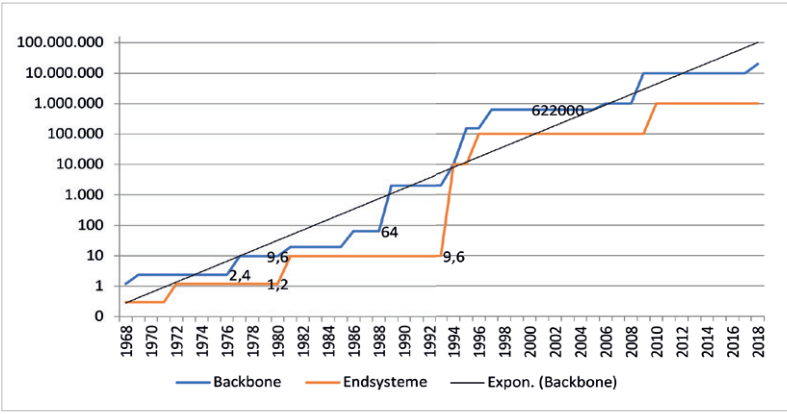


IP-Adressen und Subnetze

8.2 Leistungsparameter (Übertragungsgeschwindigkeiten)

Die enorme Entwicklung der Netztechnik in den vergangenen 50 Jahren allgemein sowie speziell des Kommunikationsnetzes der FAU zeigt sich besonders bei Betrachtung der in den verschiedenen Phasen jeweils verfügbaren Übertragungsgeschwindigkeiten.

Die Grafik „Eingesetzte Übertragungsgeschwindigkeiten“ enthält die Werte für Schnittstellen innerhalb des Backbones zwischen Netzkomponenten und Anschlüssen von Endgeräten, die „naturgemäß“ etwas niedriger sind. Die in kbit/s angegebenen Werte reichen im Backbone von 1 kbit/s (genauer 1.200 bit/s) zu Beginn von Datenfernübertragungen über aktuelle 20.000 kbit/s (bzw. 20 Gbit/s) bis zu einer absehbaren Perspektive von 100 Gbit/s. Die eingezeichnete Gerade „Expon.- (Backbone)“ zeigt im Vergleich eine exponentielle Steigerung, die der realen Kurve ziemlich nahekommt. Und wer hätte in den Anfangszeiten (1968) daran gedacht, dass statt 110 Baud für Fernschreiber, 300 Baud (0.3 kbit/s) über Akustikkoppler einmal (2018) Netzanschlüsse mit 1 Mbit/s die Regel für den Zugang von Endgeräten sein würden (weitere Steigerungen nicht ausgeschlossen). Es ist fraglich, ob bzw. wie sich das Wachstum weiter fortsetzen wird. Sicher sind im Bereich der Endgeräte zumindest punktuelle Steigerungen bzw. Anpassungen an Möglichkeiten und Bedarf zu erwarten, deren Kostenfaktor in der Breite nicht zu unterschätzen ist. Im Backbone sind mit 100 Gbit/s bereits Grenzen erreicht, die wohl nur etwa durch Parallelisierungen oder völlig neue technologische Ansätze überschritten werden können.



Eingesetzte Übertragungsgeschwindigkeiten

8.3 Betriebsparameter (Netzverfügbarkeiten)

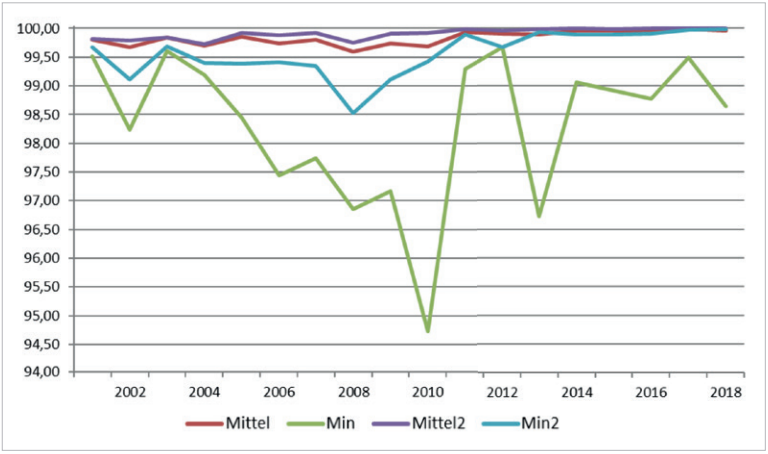
Ein wichtiges Kriterium zur Beurteilung des Netzbetriebs ist dessen Stabilität, die sich z. B. in Aussagen über Ausfallzeiten bzw. Verfügbarkeiten von Netzkomponenten ausdrückt. Um subjektiven, oft pauschal geäußerten Eindrücken („Das Netz geht nicht“) mit objektiv ermittelten Fakten begegnen zu können, ermittelt das RRZE seit 2001 monatlich entsprechende Verfügbarkeitswerte zu den Kernnetzkomponenten, veröffentlicht entsprechende Statistiken und ergänzt sie durch erläuternde Kommentare zu auffälligen Ereignissen.

Ursprünglich wurden die Daten über das Managementsystem NMS3000 erfasst und auf dessen Webseiten präsentiert. Ab 2017 wurde dann das System IMC als Grundlage der Ermittlungen verwendet, deren Auswertungen seitdem über *https://www.rrze.fau.de/internet-e-mail/datennetz-der-fau/netzverfuegbarkeit/* abrufbar bereitstanden. Die monatlichen Auswertungen wurden in jährlichen Statistiken zusammengefasst und gingen auch in die betreffenden Jahresberichte des RRZE [*JB-jjjj*] ein.

Beide Systeme erzeugten im Einsatz als Werkzeuge zur betrieblichen Überwachung des Netzes (vgl. Kapitel 7.4.3) sogenannte Ereignislogs oder Alarmdaten, die Fehlsituationen bzgl. einzelner Komponenten vom Eintreten bis zur Behebung protokollierten. Diese konnten zur Bestimmung von Ausfallzeiten bzw. im Komplement von Verfügbarkeiten herangezogen werden.

So ergaben sich in den Auswertungen des RRZE die relativen Verfügbarkeiten einzelner Geräte aus den Zeiten ohne Ausfälle im Verhältnis zu einer Gesamtbetriebszeit von 24 Stunden an allen Tagen eines betrachteten Zeitraums (Monat, Jahr). Dabei gingen alle Problemfälle in die Berechnung ein, unabhängig von ihren Ursachen, also auch solchen, die nicht oder allenfalls indirekt vom RRZE-Netzbetrieb zu verantworten waren (externe Stromausfälle, lokale Probleme usw.). Statt aus der Perspektive des Betreibers, wurde das Netzverhalten also vorrangig aus Nutzersicht betrachtet („Das Netz geht oder geht nicht − egal warum“).

Zu den Statistiken gehörten Durchschnittswerte und Minima betreffender Zeitabschnitte (Maxima liegen in der Regel bei 100% und konnten daher weggelassen werden). Um besonders extreme Ereignisse auszublenden, wurden zusätzlich „geglättete“ Werte bestimmt, zu deren Bildung jeweils die beiden größten und die beiden kleinsten Werte unberücksichtigt bleiben. (Die Methodik, die übrigens auch im Rahmen der Betreuung des Kommunikationsnetzes des Universitätsklinikums durch das RRZE als Qualitätsnachweis der erreichten Betriebsstabilität Anwendung fand, wurde auch im DFN-Forum der Öffentlichkeit vorgestellt [*HilVd*].)



Jährliche Netzverfügbarkeiten, 2001 - 2018

Die Grafik „Jährliche Netzverfügbarkeiten“ stellt die ermittelten Jahreswerte von 2001 bis 2018 dar. Die Durchschnitts- (Mittel) und Minimalwerte (Min) sowie die Durchschnittswerte (rote Kurve) bewegten sich über die Jahre durchgängig oberhalb von 99,5 %, die geglätteten Werte erwartungsgemäß etwas darüber. Die Minimalwerte (grüne Linie) stehen für Unterbrechungen einzelner Geräte, die in der geglätteten Kurve (blaue Linie) rausgefallen und in den Durchschnittsbildungen (Mittel und Mittel2) über alle betrachteten Komponenten weitgehend kompensiert worden sind. Als besonders extreme Fälle mit geringen Verfügbarkeiten fallen 2010 mit 94,7 % und 2013 mit 96,7 % auf, wobei die Störung 2010 an einem Wochenende auf einen Defekt der Richtfunkverbindung zur Sternwarte Bamberg zurückzuführen war, während 2013 externe Bauarbeiten einen gravierenden Kabelschaden einer Strecke innerhalb Erlangens (zum Standort Ulrich-Schalk-Straße) verursacht hatten. Diese beiden Ereignisse betrafen durchaus wichtige Punkte, allerdings nicht den engeren Kern des Netzes und ließen damit den Großteil der Nutzerschaft unbeeinträchtigt.

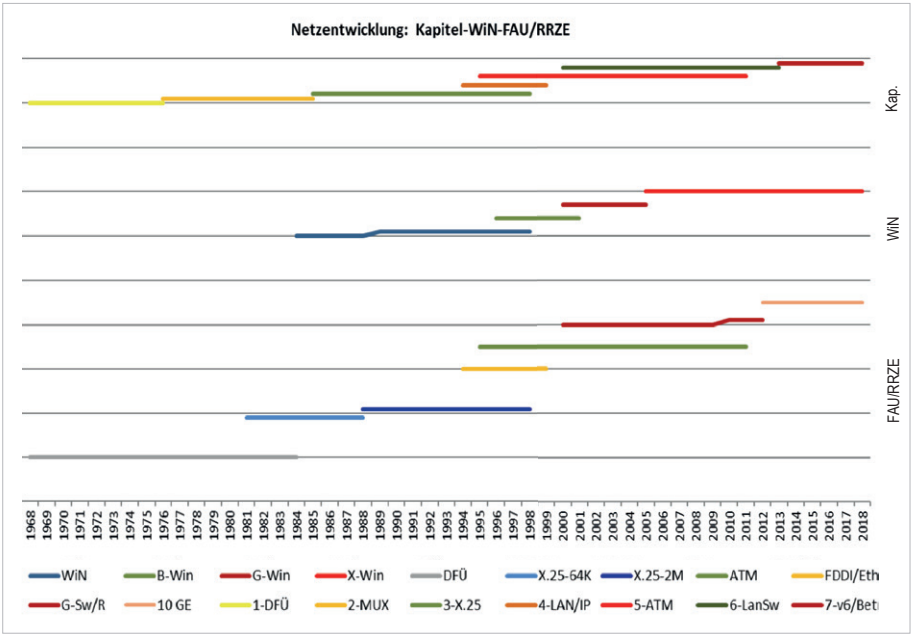
Die jüngeren Entwicklungen der Mittelwerte zeugen von einer wachsenden Betriebsstabilität. So lagen die Jahresdurchschnittswerte der Geräte seit 2011 oberhalb von 99,9 %, die geglätteten Werte erreichten 2018 das Maximum von 100 %. (Eine Jahresverfügbarkeit von 99,9 % entspricht der Ausfallzeit von 53 Minuten im Jahr.) Diese positiv zu bewertenden Zahlen schließen zwar das Vorkommen einzelner Problemfälle nicht aus, wie etwa 2018 im Zusammenhang mit einer defekten Richtfunkverbindung, zeigen aber einen erfreulichen Gesamttrend, der etwa in verbesserten Eigenschaften eingesetzter Komponenten, redundanten Konstruktionen oder einer stärker zentralisierter Betriebsführung begründet sein könnte.

8.4 Zusammenfassende Übersicht der Kapitel und Entwicklungsphasen

Als abschließende Übersicht stellt die „Zeitliche Zuordnung der Kapitel und themenbezogenen Phasen“ die verschiedenen Entwicklungsstufen des Kommunikationsnetzes und ihre Behandlung in den Kapiteln dieser Dokumentation dar und ordnet ihnen die betreffenden Zeiträume in den 50 Jahren Rechenzentrum zu.

Die Bedeutung der farblich dargestellten Linien ist in der Legende erläutert. So steht die graue Linie (DFÜ) für die Anfangsphase der Datenfernübertragung (1968 – 1984) oder die obere, dunkelgrüne Linie (6-LanSw) für das sechste Kapitel (2000 – 2013), das sich in einem Schwerpunkt mit LAN-Strukturen und virtuellen LANs befasst und sich auf die Jahre 2000 – 2013 bezieht.

In den unteren fünf Zeilen sind die verschiedenen Technologien in Geraden dargestellt, die die Jahre ihres Einsatzes an der FAU bzw. am RRZE wiedergeben. Die Überlappungen kennzeichnen jeweils fließende Übergänge zwischen ihnen.



Zeitliche Zuordnung der Kapitel und themenbezogenen Phasen

Die darüberliegende, etwa in der Mitte angeordnete Zeile, enthält die technischen Stufen der vom DFN betriebenen Wissenschaftsnetze (Varianten des WiN), die mit denen des Universitätsnetzes grob vergleichbar sind. Sie dokumentieren, dass das RRZE keinen einzig auf sich bezogenen Weg verfolgt hat, sondern sein Netz auch im Einklang mit nationalen und internationalen Entwicklungen gestaltet hat.

Die oberste Zeile gibt noch einmal eine Übersicht der Zeiträume, auf die sich die verschiedenen Kapitel dieser „Geschichte der Datenübertragungs- und Kommunikationsnetze an der FAU“ beziehen. Auch hier gibt es verschiedene Überlappungen, da sich die Kapitel zwar vornehmlich an zeitlichen Abschnitten orientieren, aber auch nach thematischen Gesichtspunkten zusammengestellt sind.

9. Schlussbetrachtung

Die Beschäftigung mit der Geschichte der Datenübertragungs- und Kommunikationsnetze an der FAU zeigt in Bezug auf das 50 Jahre bestehende Rechenzentrum in vielerlei Hinsicht eine beeindruckende Entwicklung. Dies betrifft sowohl die Rechner- und Übertragungstechnik als auch ein darauf aufbauendes bzw. dadurch erst möglich gewordenes, umfangreiches Dienstleistungs- und Anwendungsspektrum. So wurden aus dem Rechenzentrum mit seinem Angebot zentraler Rechenkapazität der IT-Dienstleister der Universität und aus den Ansätzen zu Dialogsitzungen mit entsprechenden Datenübertragungen eine an der FAU flächendeckende, national und international eingebettete Netzinfrastruktur.

Zur generellen Entwicklung des Rechenzentrums hat Dr. Peter Holleczek anlässlich des Jubiläums einige Schlaglichter in einer „Chronik − 50 Jahre RRZE“ [*HollC*] beschrieben und illustriert sowie die zeitliche Abfolge markanter Ereignisse („Hall of Fame“) als Beilage in Tabellenform dargestellt. Über aktuelle Entwicklungen und den Status als IT-Dienstleister informiert das RRZE auf vielfaltige Weise, seine Internetpräsenz gibt dazu einen guten Überblick [*RRZE*].

Die, historisch gesehen, relativ kurze Zeitspanne von 50 Jahren war sehr ereignisreich und bezüglich der Datenübertragung von mehreren technischen und konzeptionellen Wandlungen geprägt, die sich an der FAU in den verschiedenen, hier beschriebenen Phasen ausdrückten. Dennoch waren entsprechende Veränderungen auch von einer gewissen Kontinuität gekennzeichnet, deren Umsetzungen jeweils das übergeordnete Ziel der Bereitstellung einer Kommunikationsbasis verfolgten, die stets den neu gestellten, steigenden Anforderungen gewachsen war. Zur Gestaltung fließender Übergänge zwischen unterschiedlichen Technologien ohne große betriebliche Brüche trugen auch die generellen Entwicklungen der Kommunikationstechnik bei. Deren Orientierung am Schichtenmodell der ISO/OSI ermöglichte es z. B. innerhalb von Geräten die physische Ebene (Schicht 1) der Übertragungsmedien auszutauschen, ohne die darüberliegenden Ebenen (insbesondere die Sicherungsschicht 2) grundlegend ändern zu müssen. Zusammen mit den Festlegungen und einer weitgehenden Einhaltung internationaler Normen schuf dies eine hohe Flexibilität. Die einzelnen Wechsel zwischen den unterschiedlichen Konzepten und deren Umsetzungen bzw. die Ablösung „alter“ durch „neue“ Techniken hatten zwar stets Fortschritte und Verbesserungen zum Ziel, folgten zum Teil aber auch gewissen Trends und Marktbedingungen, die unter anderem von dominanten Herstellern oder großen Providern bestimmt wurden. So wurde z. B. vom Netzprotokoll X.25 abgerückt, indem es als „langsam“ bezeichnet wurde, trotz erfolgversprechender Ansätze zur Beschleunigung und seiner international verbreiteten Infrastruktur. Der Ausbau der ATM-Technik wurde als zu kompliziert (und

in weitem Einsatz zu teuer) eingestellt, obwohl sie etwa bezüglich Verkehrssteuerung besondere Stärken hatte und zunächst auch bezüglich Übertragungsgeschwindigkeiten anderen Lösungen klar überlegen war. Auf der Netz- und Anwendungsebene haben sich schließlich die Internetprotokollfamilie und damit verbundene Techniken generell durchgesetzt und als alleinige Grundlage eines weltweiten Kommunikationsnetzes, dem Internet, entwickelt. Als Gründe sind hier z. B. eine gewisse Einfachheit der Protokolle, insbesondere hinsichtlich Implementierungen, und die (kostenlose) Verfügbarkeit und entsprechende Verbreitung auf dem wachsenden Markt kleinerer und mittlerer Unix-Systeme, insbesondere auch im innovativen Hochschulbereich, zu nennen. Es sei aber bemerkt, dass die Einfachheit des verbindungslosen Internetprotokolls (etwa im Vergleich zu entsprechenden OSI-Ansätzen) auch einige Sicherheitsprobleme aufwirft, die im Zuge der Ausweitung des Internets und seiner unüberschaubaren Nutzerschaft nur unter erheblichem Aufwand zu mindern sind.

Das RRZE verfolgte diese allgemeinen Entwicklungen und orientierte sich an ihnen, sofern sie in die Gestaltung des FAU-Kommunikationsnetzes einzubringen waren. Darüber hinaus nahm das RRZE in manchen Phasen auch eine Vorreiterrolle ein, etwa bei der Einführung von 2 Mbit/s im regionalen X.25-Netz, die die Deutsche Bundespost zur Umstrukturierung ihres DATEX-P-Netzes und einer entsprechenden Anhebung (von bis dahin 9.600 bit/s) ihrer Anschlussgeschwindigkeiten motivierte, oder bei der Aufstellung eines Weltrekordes der Datenübertragung mit einer Geschwindigkeit von 2,43 Gbit/s über eine ATM-Fernverbindung. Zudem führte die enge Zusammenarbeit mit dem DFN-Verein zur Installation eines Kernnetzstandortes in Erlangen. Das RRZE ist auch weiterhin an zahlreichen Forschungsprojekten zu Vernetzungsthemen bzw. an der Vorausschau und Vorbereitung auf zukünftige Entwicklungen der Kommunikationstechnik beteiligt.

Die beiden unterschiedlichen Großrechner am Anfang, die starke Verteilung der Universität auf verschiedene Standorte (verteilteste Universität) sowie der Auftrag zur Versorgung der nordbayerischen Region stellten dem RRZE schon frühzeitig Anforderungen zur Schaffung von Übertragungsstrukturen, die über „klassische“ Datenfernübertragungen mit Anbindungen von Terminals an eine Zentrale hinausgingen. So realisierte das regionale X.25-Netz erstmals die Idee einer Vernetzung der FAU und der nordbayerischen Hochschulen von verteilten Rechnern und Endgeräten mit gegenseitigen, wählbaren Kommunikationsbeziehungen. Mit den folgenden Entwicklungen sind der Aufbau einer strukturierten Verkabelung, die Bildung und Integration lokaler Netze sowie die Einführung und Verbreitung des Internetprotokolls als Basis einer uniweiten Infrastruktur verbunden. Auch die Zukunft wird durch Prozesse von Ausbau, Ausweitung, Verdichtung oder Leistungssteigerung weiter geprägt sein und ein zuverlässiges, anforderungsgemäßes Kommunikationsnetz an der FAU bereitstellen.

Der Rückblick auf die vergangenen 50 Jahre bzgl. Datenübertragungs- und Kommunikationsnetzen zeichnet (nach meinem Empfinden) eine spannende Geschichte. Sie sollte nicht ganz in Vergessenheit geraten und mehr als nur in nostalgischer Erinnerung behalten bleiben.

Die vorliegende Beschreibung der Netzhistorie erfolgte aus einer persönlichen Perspektive im Kontext von RRZE und FAU. Sie versuchte ihre Entwicklungsschritte möglichst vielfältig und umfassend darzustellen sowie damit verbundene Grundlagen zu erläutern, allerdings ohne dabei einen Anspruch auf Vollständigkeit zu stellen.

Der gegebene Überblick möge auf Interesse stoßen und zur Verfolgung künftiger Entwicklungen anregen, die sicher auch noch einiges Unerwartete und Erstaunliche bieten werden.

Referenzen

Referenzen

Literatur, Dokumentationen

[*BI-nn*] RRZE: „Benutzerinformation (BI) Nr. nn“, regelmäßige Publikation des RRZE, RRZE-Archiv, ab „BI 60“ (1998) einsehbar unter *https://www.rrze.fau.de/infocenter/wir-ueber-uns/veroeffentlichungen/bi/*

[*Cacti*] Cacti: „The Complete RRDTool-based Graphing Solution“, Webpräsentation aktualisiert 2020, *http://www.cacti.net/*

[*Caida*] CAIDA: „IPv6 AS Core“, Webpräsentation, 2015, *https://www.caida.org*

[*CiC6k*] Cisco: „Cisco Catalyst 6500 Series: Optimized for Wiring Closet Deployments“, Produktbroschüre, 2008

[*CiCam*] Cisco: „Campus Network for High Availability Design Guide“, Dokumentation 2008, *https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html#wp1107563*

[*CiEck*] Cisco: „Eckpfeiler im expandierenden IP-Universum“, White Paper 2011, *https://www.cisco.com/c/dam/global/de_de/assets/cisconnect/2011-05/media/Whitepaper_Routing_und_Switching_web.pdf RRZE-Archiv*

[*CiMed*] Cisco: „Cisco Medical-Grade Network (MGN) 2.0 Campus Architecture“, Student Guide, 2012, Cisco Learning Product

[*CiMsn*] Cisco: „Building Cisco Multilayer Switched Networks, Rev 1.1“, Student Guide, 2000, Cisco Learning Product

[*CiNex*] Cisco: „Cisco Nexus 7000 Series Switches Data Sheet“, Produktbeschreibung, 2018, *https://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/Data_Sheet_C78-437762.html*

[*CiW4*] Cisco: „Why Migrate from Cisco Catalyst 4000 Series to Cisco Catalyst 4500 E-Series“, Produktbroschüre, 2007

[*DfnBo*] DFN: „Benutzungsordnung für das Zusammenwirken der Anwender der DFN-Kommunikationsdienste“, Webveröffentlichung 1994, aktualisiert 2020, *https://www.dfn.de/dienstleistungen/dfninternet/benutzungsordnung*

[*DfnX*] DFN: „X-Win, Die Netzinfrastruktur des Deutschen Forschungsnetzes“, Broschüre DFN-Verein, 2009

[*DreßM*] F. Dreßler: „IP Multicast“, Netzwerkausbildung ‚Grundzüge der Datenkommunikation‘ am RRZE 2002, RRZE-Archiv

[*Elkom*] Elektronik Kompendium: „Ethernet-Standards von IEEE 802.3“, Webpräsentation 2020, *https://www.elektronik-kompendium.de/sites/net/1406171.htm*

[*FauRb*] FAU: „Benutzungsrichtlinien“, Webveröffentlichung 2017, *https://www.rrze.fau.de/files/2018/02/19950602-Benutzungsrichtlinien.pdf*

[*FauRd*] FAU: „Richtlinien für die Nutzung des FAU-Datennetzes“, Webveröffentlichung 2017, *https://www.rrze.fau.de/files/2017/06/Datennetzrichtlinien.pdf*

[*Fisch*] R. Fischer: „E-Mail-Grundlagen“, Netzwerkausbildung ‚Praxis der Datenkommunikation‘, RRZE 2018, *https://www.rrze.fau.de/files/2018/02/20180207-E-Mail-Grundlagen-NWA-WS17-18.pdf*

[*Grä20*] M. Gräve: „20 Jahre Uni TV“, Vortrag am RRZE 2018, *https://www.rrze.fau.de/files/2018/07/20180503-50-J-IT-Geschichte-Uni-TV_SoSe18.pdf, Videoaufzeichnung: https://www.video.uni-erlangen.de/clip/id/9086.html*

[*GrNaeV*] M. Gründl, S. Naegele-Jackson: „Videoübertragungen, Performanz und Sicherheit“, Netzwerkausbildung ‚Grundzüge der Datenkommunikation‘ am RRZE 2010, RRZE-Archiv

[*GrNaeP*] M. Gründl, S. Naegele-Jackson: „Forschungsprojekte in der Netzabteilung des RRZE“, Vortrag am RRZE 2011, RRZE-Archiv

[*Hellf*] E. Hellfritsch: „Multimedia und Videokonferenzen am RRZE“, Interner Arbeitsbericht 519, 1996, RRZE-Archiv

[*HilUk*] U. Hillmer: „Das Kommunikationsnetz im Universitätsklinikum – Entwicklung 1994 – 2011“, Mitteilungsblatt 88, 2011, RRZE-Archiv

[*HilN*] U. Hillmer: „Netzstrukturen an der FAU“, Netzwerkausbildung ‚Praxis der Datenkommunikation‘ am RRZE, regelmäßig, RRZE-Archiv

[*HilVi*] U. Hillmer, „Untersuchung von Netzwerkverfügbarkeiten des Kommunikationsnetzes der FAU“, Interner Arbeitsbericht 91, RRZE 2013, RRZE-Archiv

[*HilVd*] U. Hillmer: „Exemplarisches Langzeitreporting von Netzverfügbarkeiten“, 5. DFN-Forum Kommunikationstechnologien, 21.-22. Mai 2012 Regensburg, enthalten auch in *http://www.rrze.uni-erlangen.de/wir-ueber-uns/publikationen/Netzbroschuere-2013-Screen.pdf*

[*HollC*] P. Holleczek: „Chronik – 50 Jahre RRZE“, Präsentation und Veröffentlichung am RRZE 2018, *https://www.rrze.fau.de/infocenter/wir-ueber-uns/veroeffentlichungen/rrze-chronik/*

[*HollP*] P. Holleczek: „50 Jahre PEARL & Echtzeit und ein Archiv dazu“, Präsentation am RRZE 2019, *https://www.real-time.de/archiv/ez19/EZ19-Holleczek.pdf*

[*HpImc*] Hewlett Packard, D. Davis: „Review: HP Intelligent Management Center (IMC)” Webveröffentlichung aktualisiert 2020, *http://www.networkmanagementsoftware.com/hp-intelligent-management-center-imc-review*

[*Ieee8*] IEEE: „IEEE 802 LAN/MAN Standards Committee“, IEEE 802 Working Groups and Study Groups, *http://www.ieee802.org/*

[*IetfS*] IETF: „International Standard RFCs”, Memos in the RFC document series contain technical and organizational notes about the Internet, *https://www.ietf.org/standards/rfcs/*

[*IetfF*] IETF: „Index of RFC”, Liste der von der Internet Engineering Task Force (IETF) bereitgestellten RFC-Dokumente, abrufbar über: *https://www.ietf.org/rfc.html*

[*ITKonz*] FAU: „IT-Konzept 2011-2015“, FAU-Publilkation, 2013

[*JB-jjjj*] RRZE: „Jahresbericht des RRZE (Jahr-jjjj)“, jährliche Publikation des RRZE, RRZE-Archiv, ab „JB 1996“ einsehbar unter: *https://www.rrze.fau.de/infocenter/wir-ueber-uns/veroeffentlichungen/jb/*

[*Liebl*] K. Liebl: „FunkLAN an der FAU“, Bericht zur WLAN-Tagung am 18./19.6.2001 in Rostock, RRZE-Archiv

[*Meyer*] M. Meyer: „Ein generisches Werkzeug zur Automatisierung der CLI-basierten Konfiguration von Netzkomponenten“, Publikation an der Ludwig-Maximilians-Universität München, *http://www.nm.ifi.lmu.de/pub/Fopras/meye12/PDF-Version/meye12.pdf*

[*MaSch*] H. Marquardt, V. Scharf: „Elementare Sicherheitsmaßnahmen“, Netzwerkausbildung ‚Praxis der Datenkommunikation‘ 2018, RRZE-Archiv

[*Omni*] Alcatel-Lucent:“ OmniVista 2500 Network Management System”, Datenblatt, 2020, *https://www.al-enterprise.com/de-de/produkte/netzwerkmanagement-sicherheit/omnivista-2500-netzwerkmanagement*

[*QosM*] S. Naegele-Jackson, R. Kleineisel, P. Holleczek: „IPPM Measurements and Network Load Behavior of the German Research Network G-WiN“. In: Proceedings of the 2nd International Conference on Computing, Communications and Control Technologies: CCCT 2004, Volume III

[*Rech*] J. Rech: „Ethernet, Technologien und Protokolle für Computervernetzung“ Verlag Heinz Heise, 2002

[*ReiH*] J. Reinwand: „Handeln mit Adressen ARP, DHCP, DNS“, Netzwerkausbildung ‚Praxis der Datenkommunikation‘ 2015, RRZE-Archiv

[*RRZE*] Regionales Rechenzentrum Erlangen: „Internetstartseite“, aktuelle Internetpräsenz des RRZE, *https://www.rrze.fau.de*

[*SDI*] S. Naegele-Jackson, P. Holleczek, A. Metz: „The Effects of SDI-to-ATM Adaptation on Communication and Control in Distributed Interactive Multimedia Applications“ In: Proceedings of the International Conference on Computer, Communication and Control Technologies: CCCT ‚03, Orlando, FL, USA, 31.7.-2.8.2003

[*TecC*] TecChannel: „Netzwerk-Special“, Artikel zu Netzthemen, 2001, IDG Interactive GmbH

[*Trap*] Trapeze: „Enterprise WLAN mit Trapeze Networks“, Webpräsentation 2010, *https://de.slideshare.net/netlogix/trapeze-wlan-lsung-4451927*

[*TriPa*] Tripunkt: „Pathfinder – Kabelmanagement und Netzwerkdokumentation”, Produktbroschüre 2020, *http://www.tripunkt.eu/wp-content/uploads/2013/12/Pathfinder-Produktbrosch%C3%BCre.pdf*

[*UniTV*] S. Naegele-Jackson, M. Gräve, N. L. M. Eschbaum, P. Holleczek: „Distributed TV-Productions and Video-on-Demand Services at Universities“ In: Proceedings of the Networking Conference 2000: TERENA, Lissabon, Portugal, 05/2000

[*VoIP*] F. Dressler; U. Hilgers; P. Holleczek: „Voice over IP im Weitverkehrsnetzen?“. In: GI-Fachgruppe 3.4; (Hrsg:) Anwendungs- und System-Management im Zeichen von Multimedia und E-Business (Fachtagung der GI-Fachgruppe 3.4 Betrieb von Informations- und Kommunikationssystemen (BIK 2001), Tübingen, April 2001)

[*WikS*] Wikipedia: „Simple Network Management Protocol“, Webartikel, aktualisiert 2020, *https://de.wikipedia.org/wiki/Simple_Network_Management_Protocol*

[*WikF*] Wikipedia: „FCAPS“, Beschreibung des Netzwerkmanagementmodells der ISO, kurz (deutsch): *https://de.wikipedia.org/wiki/FCAPS*, ausführlich mit weiterführenden Verweisen: *https://en.wikipedia.org/wiki/FCAPS*

[*Wüv6*] H. Wünsch: „IP-FAU-6 (Teil 1 und 2)“, Netzwerkausbildung ‚Praxis der Datenkommunikation‘ am RRZE 2017, *https://www.rrze.fau.de/files/2017/12/20171206-IPv6-Teil1-NWA-WS17-18.pdf*

Bildnachweise

Bilder aus externen Quellen sind im Folgenden aufgelistet. Alle weiteren Fotos und Abbildungen stammen aus dem Bestand des RRZE.

S. 26 Rech, Verlag Heise, [*Rech*]
S. 27 Elektronik Kompendium, Internet, [*Elkom*]
S. 38 Cisco, Cat4000 Produktbroschüre, 2007, [*CiW4*]
S. 43 Cisco, LAN Solutions, Produktblatt, 2001
S. 57 Cisco, Catalyst 6500 Series, „At-A-Glance“, 2008, [*CiC6k*]
S. 61 TecChannel, Netzwerk-Artikel [*TecC*]
S. 67 Trapeze, Internet, [*Trap*]
S. 74 Cisco, Student Guide, 2000, [*CiMsn*]
S. 76 Cisco, Dokumentation, 2008, [*CiCam*]
S. 97 X-Win-Topologie, 2005 ?
S. 98 DFN, Broschüre, [*DfnX*]
S. 117 CAIDA, Internet, 2005, [*Caida*]
S. 122 Wikipedia, Thema IPv6 [*WikI6*]
S. 150 Hewlett Packard, Internet, [*HpImc*]
S. 127 Cisco, Nexus 7000, Datenblatt [*CiNex*]

Abkürzungen

AAL ATM Adaption Layer (Teil 1, Kapitel 5)
ABR Available Bit Rate (Teil 1, Kapitel 5)
ACE Application Control System (Teil 2, Kapitel 6)
ACK Acknowledge (Teil 1, Kapitel 1)
ACL Access List(e) (Teil 2, Kapitel 7)
ADo Anschlußdose (Teil 1, Kapitel 2)
AFI Authority Format Identifier (Teil 1, Kapitel 5)
AP Access Point (Teil 2, Kapitel 6)
ARM Acorn Risc Machines (Prozessor) (Teil 2, Kapitel 7)
ARP Adress Resolution Protocol (Teil 1, Kapitel 4)
ARPANET Advanced Research Project Agency Network (Teil 1, Kapitel 3)
ASA Adaptive Security Appliances (Teil 2, Kapitel 6)
ASA Adaptive Security Appliances (Cisco) (Teil 2, Kapitel 7)
ASN.1 Abstract Syntax Notation One (Teil 2, Kapitel 7)
ATD Abteilung Technischer Dienst, FAU (Teil 2, Kapitel 7)
ATM Asynchron Transfer Mode (Teil 1, Kapitel 5)

Azubi Auszubildender (Teil 2, Kapitel 6)

BB Backbone (Teil 1, Kapitel 5)
BHN Bayerisches Hochschulnetz (Teil 1, Kapitel 3)
BIENE Barrierefreies Internet eröffnet neue Chancen (Teil 2, Kapitel 6)
B-ISDN Broadband Integrated Services Digital Network (Teil 1, Kapitel 5)
BITNET ursprünglich: Because It's There NETwork (Teil 1, Kapitel 3)
BPDU Bridge Protocol Data Unit (Teil 2, Kapitel 6)
BS2000 Betriebssystem 2000, Siemens (Teil 1, Kapitel 4)
BSC Binary Synchronous Communication (Teil 1, Kapitel 1)
BUS Broadcast and Unknown Server (Teil 1, Kapitel 3)
BVDW Bundesverband Digitale Wirtschaft (Teil 2, Kapitel 6)

CATX Categorie x, Kabelqualitätsstufe (Teil 1, Kapitel 5)
CBR Constant Bit Rate (Teil 1, Kapitel 5)
CBT Core Based Trees (Teil 2, Kapitel 6)
CCITT Comité Consultatif International Télégraphique et Téléphonique (Teil 1, Kapitel 1)
CDVT Cell Delay Variation Tolerance (Teil 1, Kapitel 5)
CERT Computer Emergency Response Team (Teil 2, Kapitel 7)
CFR Code of Federal Regulations (Teil 2, Kapitel 6)
CGMP Cisco Group Management Protokoll (Teil 2, Kapitel 6)
CIO Chief Information Officer (Teil 2, Kapitel 7)
CIP Computer-Investitions-Programm (Teil 1, Kapitel 5)
CIT Campus IT (Teil 2, Kapitel 6)
CLI Comand Line Interface (Teil 2, Kapitel 7)
CLP Cell Loss Priority (Teil 1, Kapitel 5)
CSMA/CD Carrier Sense Multiple Access / Collision Detection (Teil 2, Kapitel 6)
CSF Central-Server-Facility (Teil 2, Kapitel 7)

DAD Duplicate Address Detection (Teil 2, Kapitel 7)
DANTE Delivery of Advanced Network Technology to Europe (Teil 2, Kapitel 7)
DBP Deutsche Bundespost (Teil 1, Kapitel 3)
DEE Datenendeinrichtung (Teil 1, Kapitel 1)
DFG Deutsche Forschungsgemeinschaft (Teil 1, Kapitel 2)
DFN Deutsches Forschungsnetz (Teil 1, Kapitel 3)
DFÜ Datenfernübertragung (Teil 1, Kapitel 1)
DFV Datenfernverarbeitung (Teil 1, Kapitel 1)
DHCP Dynamic Host Configuration Protocol (Teil 2, Kapitel 6)
DMMA Deutscher Multimedia Award (Teil 2, Kapitel 6)
DMMK Deutsche Multimedia Kongress (Teil 2, Kapitel 6)

DMZ Demilitarized Zone (Teil 2, Kapitel 7)
DNS Domain Name Service (Teil 2, Kapitel 7)
DOS Denial of Service (Teil 2, Kapitel 7)
DSL Domaiun Specific Language (Teil 2, Kapitel 7)
DÜE Datenübertragungseinrichtung (Teil 1, Kapitel 1)
DVMRP Distance Vector Multicast Routing Protocol (Teil 2, Kapitel 6)

EARN European Academic Reseaech Network (Teil 2, Kapitel 7)
ECB Ethernet Control Board (Einschubkarten) (Teil 1, Kapitel 3)
ECMP Equal-Cost Multi-path Routing (Teil 2, Kapitel 7)
EDV Elektronische Datenverarbeitung (Teil 1, Einführung)
ELAN Emuliertes LAN (Teil 1, Kapitel 5)
EMAIL E-Mail, elektronische Post (Teil 2, Kapitel 7)
ErWiN Erweitertes Wissenschaftsnetz (Teil 1, Kapitel 5)
EWF Erziehungswissenschaftliche Fakultät (Teil 1, Kapitel 4)

FAU Friedrich-Alexander-Universität Erlangen-Nürnberg (Teil 1, Einführung)
FAUST FAU Security Tool (Teil 2, Kapitel 7)
FCAPS Fault, Configuration,Accounting, Performance, Security Mgmt. (Teil 2, Kapitel 7)
FDDI Fiber Distributed Data Interface (Teil 1, Kapitel 4)
FE Fast Ethernet (Teil 2, Kapitel 6)
FEDERICA Federated E-Infrasructure Dedicated to European Researchers Innovating in Computing Network Architectures (Teil 2, Kapitel 7)
FEX Fabric Extender (Teil 2, Kapitel 7)
FIN Flag zur Endekennung (Teil 1, Kapitel 4)
FT Filetransfer (Teil 1, Kapitel 4)
FTP File Transport Protocol (Teil 2, Kapitel 4)

GE Gigabit Ethernen, Übertragungsgeschwindigkeit (Teil 2, Kapitel 6)
GEANT Franz. „Gigant“, Europäisches Netzwerk (Teil 2, Kapitel 7)
GFC Generic Flow Control (Teil 2, Kapitel 7)
GTS GEANT Testbed Service (Teil 2, Kapitel 7)
GUI Graphical User Interface (Teil 2, Kapitel 7)
GVS Generalized Virtualization Service (Teil 2, Kapitel 7)

HADES Active Delay Evaluation System (Teil 2, Kapitel 7)
HBFG Hochschulbau Förderungsgesetz (Teil 2, Kapitel 6)
HDLC High-Level Data Link Control (Teil 1, Kapitel 3)
HEC Header Error Check (Teil 1, Kapitel 5)
HIS Hochschul Informationssystem (Teil 2, Kapitel 7)
HfD Hauptanschluss für Direktruf (Teil 1, Kapitel 1)

HLS	HTTP-Live-Streaming (Teil 2, Kapitel 7)
HPC	High Performance Computing (Teil 2, Kapitel 6)
HSRP	Hot Standby Router Protocol (Teil 2, Kapitel 6)
HTTP	Hypertext Transfer Protocol (Teil 1, Kapitel 4)
IANA	Internet Assigned Numbers Authority (Teil 2, Kapitel 7)
ICMP	Internet Control Message Protocol (Teil 1, Kapitel 4)
IDM	Identity Management (Teil 2, Kapitel 6)
IDS	Intrusion Detection System (Teil 2, Kapitel 7)
IEEE	Institut of Electrical Electronics Engineers (Teil 1, Kapitel 4)
IETF	Internet Engeneering Task Force (Teil 2, Kapitel 6)
IPNG	IP Next Generation (Teil 2, Kapitel 7)
IGMP	Internet Grpup Management Protocol (Teil 2, Kapitel 6)
IMAP	Internet Message Acess Protocol (Teil 2, Kapitel 7)
IMC	Intelligent Mnagement Center (Teil 2, Kapitel 7)
IP	Internet Protocol (Teil 1, Kapitel 4)
IPPM	IP Performance Measurement (Teil 2, Kapitel 7)
IPS	Intrusion-Prevention-System (Teil 2, Kapitel 6)
IPv4	Internet Protocol Version 4 (Teil 2, Kapitel 6)
IPv6	Internet Protocol Version 6 (Teil 2, Kapitel 6)
IPX	Internetwork Packet Exchange (Teil 2, Kapitel 6)
ISER	Informatik Sammlung Erlangen (Teil 2, Kapitel 6)
ISL	Inter Switch Link (Cisco) (Teil 2, Kapitel 6)
IT	Informations Technologie (Teil 2, Kapitel 6)
ITU	International Telecommunication Union (Teil 1, Kapitel 5)
IVMed	Informationsverarbeitung Medizin (Teil 1, Kapitel 4)
IZH	IT-Betreuungszentrum Halbmondstraße (Teil 2, Kapitel 6)
IZI	IT-Betreuungszentrum Innenstadt (Teil 2, Kapitel 6)
IZN	IT-Betreuungszentrum Nürnberg (Teil 2, Kapitel 6)
JRA	Joint Research Activities (Teil 2, Kapitel 7)
L2TP	Layer 2 Tunneling Protocol (Teil 2, Kapitel 6)
LAN	Local Area Network (Teil 1, Einführung)
LANE	LAN-Emulator (Teil 1, Kapitel 5)
LCN	Logical Channel Number (Teil 1, Kapitel 3)
LEC	LAN Emulation Client (Teil 1, Kapitel 5)
LECS	LAN Emulation Configuration Server (Teil 1, Kapitel 5)
LES	LAN Emulation Server (Teil 1, Kapitel 5)
LLC	Local Link Control (Teil 1, Kapitel 4)

LLC2 Local Link Control 2 (Linkprotokoll) (Teil 1, Kapitel 3)
LMS Lan Management Solution, Cisco (Teil 2, Kapitel 7)
LMU Kudwig Maximilians Universität. München (Teil 2, Kapitel 7)
LN LocalNet (Teil 1, Kapitel 3)
LN20 LocalNet20 (Teil 1, Kapitel 3)
LRZ Leibniz-Rechenzentrum, Mümchen (Teil 1, Kapitel 3)
LWL Lichtwellenleiter (Glasfaser) (Teil 1, Kapitel 5)

MAC Media Access Control (Teil 1, Kapitel 4)
MAN Metropol Area Network (Teil 1, Kapitel 4)
MAU Media Access Unit (Teil 1, Kapitel 4)
MBONE Multicast Backbone (Teil 2, Kapitel 6)
MHS Message Handling System (Teil 2, Kapitel 7)
MIB Management Information Base (Teil 2, Kapitel 7)
MIK Medizin. Zentrum für Informations- & Kommunikationstechnik (Teil 1, Kapitel 4)
MIME Multipurpose Internet Mail Extensions (Teil 2, Kapitel 7)
MLD Multicast Listener Discovery (Teil 2, Kapitel 6)
MMZ Multi Media Zentrum (RRZE, FAU) (Teil 2, Kapitel 7)
MOSPF Multicast Extensions to OSPF (Teil 2, Kapitel 6)
MP Mobility Points (Trapeze) (Teil 2, Kapitel 6)
MPEC Moving Picture Experts Group (Teil 1, Kapitel 5)
MSA Mail Submission Agent (Teil 2, Kapitel 7)
MSTP Multiple Spanning Tree Protocol (Teil 2, Kapitel 6)
MSV Medium Speed Version (Teil 2, Kapitel 7)
MTA Message Transfer Agent (Teil 2, Kapitel 7)
MUA Mail User Agent (Teil 2, Kapitel 7)
MX Mail Exchange (Teil 2, Kapitel 7)

NAT Network Activities (Teil 2, Kapitel 7)
NAT Network Address Translation (Teil 2, Kapitel 6)
NDC Neighbor Discovery Protocol (Teil 2, Kapitel 7)
NFS Network File System (Teil 1, Kapitel 4)
NIP Netzwerk-Investitions-Programm (Teil 1, Kapitel 5)
NIS Network Information System (Teil 1, Kapitel 4)
NIST National Institute of Standards and Technology (Teil 2, Kapitel 6)
NMS Network Management System (Teil 2, Kapitel 7)
NNI Network to Network Interface (Teil 1, Kapitel 5)
NOVI Network Innovations over Virtualized Infrastructures (Teil 2, Kapitel 7)
NOZ Nicht Operatives Zentrum (NOZ) (Teil 2, Kapitel 6)
NSAP Network Service Access Point (Teil 1, Kapitel 5)

NTP Network Time Protocol (Teil 2, Kapitel 7)
NUD Neighbour Unreachability Detection (Teil 2, Kapitel 7)
NX-OS Nexus Operating System (Teil 2, Kapitel 7)

OID Object Identifier (Teil 2, Kapitel 7)
OOB Out of Band Management (Teil 2, Kapitel 7)
QOS Quality of Service (Teil 2, Kapitel 7)
OSPF Open Shortest Path First (Teil 1, Kapitel 4)

PAD Packet Assembler Disassembler (Teil 1, Kapitel 3)
PC Personal Computer (Teil 1, Kapitel 3)
PCR Peak Cell Rate (Teil 1, Kapitel 5)
PEAP Protected Extensible Authentication Protoco (Teil 2, Kapitel 6)
PHY Physical Layer (Teil 1, Einführung)
PIM Protocol Indepent Multicast (Teil 2, Kapitel 6)
PLCP Physical Layer Convergence Procedure (Teil 2, Kapitel 6)
PLP Packet Layer Protocol (Teil 1, Kapitel 3)
PMD Physical Medium Dependant (Teil 2, Kapitel 6)
POE Power over Ethernet (Teil 2, Kapitel 6)
POP Post Office Protocol (Teil 2, Kapitel 7)
PT Payload Type (Teil 1, Kapitel 5)
PVC Permanent Virtual Circuit (Teil 1, Kapitel 3)

QoS Quality of Service (Teil 1, Kapitel 5)

RAID Redundant Array of Independent Disks (Teil 2, Kapitel 7)
RARP Reverse Adress Resolution Protocol (Teil 1, Kapitel 4)
REVUE Rechnerverbund Universität Erlangen-Nürnberg (Teil 1, Kapitel 4)
RFC Request for Comment (Teil 1, Kapitel 4)
RIP Routing Information Protocol (Teil 1, Kapitel 4)
RMON Remote Monitoring (Teil 2, Kapitel 7)
RRZE Regionales Rechenzentrum Erlangen (Teil 1, Einführung)
RTP Real Time Protocol (Teil 1, Kapitel 4)
RSTP Rapid Spanning Tree Protocol (Teil 2, Kapitel 6)
RZMF Rechenzentrum der Medizinischen Fakultät (Teil 1, Kapitel 4)

SA Service Activities (Teil 2, Kapitel 7)
SDH Synchrone Digitale Hierarchie (Teil 1, Kapitel 5)
SDN Software Designet Networking (Teil 2, Kapitel 7)
SFTPS Secure File Transfer Protocol (Teil 1, Kapitel 4)
SG DV Sachgebiet Datenverarbeitung (der Universitätsverwaltung) (Teil 2, Kapitel 6)

SLAAC	IPv6 stateless address autoconfiguration (Teil 2, Kapitel 7)
SMI	Structure and Identification of Management Information (Teil 2, Kapitel 7)
SMTP	Simple Mail Transfer Protocol (Teil 1, Kapitel 4)
SNMP	Simple Network Management Protocol (Teil 1, Kapitel 4)
SPT	Shortest Path Tree (Teil 2, Kapitel 6)
SPVC	Soft Permanent Virtual Circuit (Teil 1, Kapitel 5)
SSH	Secure Shell (Teil 1, Kapitel 4)
SSID	Service Set Identifier (Teil 2, Kapitel 6)
SSM	Source Specific Multicast (Teil 2, Kapitel 6)
STP	Spanning Tree Protocol (Teil 2, Kapitel 6)
SUP	Supervisor Engine (Teil 2, Kapitel 6)
SVC	Switches Virtual Circuit (Teil 1, Kapitel 3)
TAAS	Teatbed as a Service (Teil 2, Kapitel 7)
TB	Terra Byte (Teil 2, Kapitel 7)
T-Box	LocalNet20 Anschlussbox (Teil 1, Kapitel 4)
TEN	Trans-European Networks (Teil 2, Kapitel 7)
TFTP	Trivial File Transfer Protocol (Teil 2, Kapitel 7)
TKIP	Temporal Key Integrity Protocol (Teil 2, Kapitel 6)
TP	Twistet Pair (Kabel) (Teil 2, Kapitel 6)
TP	Transport Protocol (Teil 2, Kapitel 7)
TTY	Teletypewriter (Teil 2, Kapitel 7)
UBR	Unspecified Bit Rate (Teil 1, Kapitel 5)
UDP	User Datagram Protocol (Teil 1, Kapitel 4)
UKER	Universitätsklinikum Erlangen (Teil 1, Kapitel 4)
UNI	User to Network Interface (Teil 1, Kapitel 5)
UUCP	Unix to Unix Copy Protocol (Teil 1, Kapitel 4)
VBR	Variable Bitrate (Teil 1, Kapitel 5)
VCI	Virtual Channel Identifier (Teil 1, Kapitel 5)
VC	Virtual Connection (Teil 1, Kapitel 5)
VLAN	Virtuelles LAN (Teil 1, Kapitel 5)
VN	Virtual Network (Teil 2, Kapitel 7)
VOIP	Voice over IP (Teil 2, Kapitel 7)
VPI	Virtual Path Identifier (Teil 1, Kapitel 5)
VPN	Virtual Private Network (Teil 2, Kapitel 6)
VSS	Virtuelles Switching System (Cisco) (Teil 2, Kapitel 6)
WAN	Wide Area Network (Teil 1, Einführung)
WEP	Wired Equivalent Privacy (Teil 2, Kapitel 6)

WiN Wissenschaftsnetz (Teil 1, Kapitel 3)
WISO Wirschafts und Sozialwissenschaftliche Fakultät (FAU) (Teil 2, Kapitel 7)
WLAN Wireless LAN (Teil 2, Kapitel 6)
WWW World Wide Web (Teil 1, Kapitel 4)

ZUV Zentrale Universitätsverwaltung (der FAU) (Teil 2, Kapitel 6)

Musikalischer Nachtrag

Liebe Leserinnen, liebe Leser,

wie schon im ersten Teil erwähnt, bin ich neben meiner Tätigkeit als Mitarbeiter der Abteilung Kommunikationssysteme des RRZE in meiner Freizeit als Musiker aktiv (Gesang, Gitarre, Schlagzeug). Dabei schreibe ich gelegentlich auch eigene Stücke für Gesang und Gitarrenbegleitung.

Das hier angefügte Lied befasst sich mit der Abteilung Kommunikationssysteme, die auch als „Mafia“ bezeichnet wurde. Das geht wohl auf die Zeit zurück, als das Rechenzentrum in der Aufbauphase des Kommunikationsnetzes von neu angeschlossenen Instituten eine einmalige Pauschale von 20.000 DM als Beitrag zur Finanzierung verlangte („Mafia-Methoden“).

Der Text ist im Laufe der Zeit modifiziert und aktualisiert worden. Er enthält verschiedene Anspielungen, die zum Teil nur intern nachvollziehbar sind, deshalb ist er durch verschiedene Erläuterungen ergänzt, die in den Fußnoten zu finden sind.

Viel Spaß beim Lesen.

Mafia (Text/Musik: U. Hillmer)

Strophe (lang):
Wer ist überall präsent, Mafia
Unser Club, den jeder kennt, Mafia
In Land und Stadt, in jedem Haus, Mafia
Liegen unsre Netze aus, Mafia

Refrain:
Mafia, wo man uns braucht
Woll´n als Dankeschöngebühr
Sind wir da, schützen dich auch
20 Riesen nur von Dir! Mafia

Strophen (kurz):
Unser Boss, wer hat´s gecheckt?
Geachtet, gefürchtet, wohlbekannt,
Ist der Boss wieder mal verreist,
Fragt man mich geheime Dinge
Ist Dottore Holleczek[1].
Nicht nur hier im Frankenland.
Dann vertrete ich[2] ihn meist
Ich nur dieses Lied hier singe, Mafia

Schneller Anschluss, neues Netz?
Ob Gigabit oder Netzstruktur
Kontrolle ist besser als Vertrau`n,
Wer darf wo rein, was darf raus?
„Wünsch Dir was“, so heißt das jetzt!
Unser Helmut[3] hält die Spur.
Jeden Zugang schützt ein Zaun.
Holger regelt das mit FAUST[4]. Mafia

Alle Daten in der Luft
Gibt`s Probleme, klemmt wo was,
Sie sind dabei nicht allein,
Das Netzwerk duldet keinen Riss,
Überwacht der schlaue Fuchs[5],
Markus kommt, der „Schaffert“[6] das!
Bringen sich ins Team mit ein.
Es flicken Techniker und Azubis. Mafia

Deine Post zu jedem Ort
Spams von draußen gibt’s hier nicht
Jeden Weg auf Schritt und Tritt,
Gestochen scharf, an Farben satt
Schickt die Mailertruppe fort.
werden von Fischern[7] abgefischt!
Multimedia schneidet mit
weil Micha[8] den Farbfilm nicht vergessen hat!
Mafia

Auch ein Pate sieht mal ein,
Legt die Führung voll Vertrau´n,
Und so heißt es ab sofort
Susanne über die Projekte wacht
Boss kann man nicht ewig sein.
In die Hände von zwei Frau´n
Alles hört auf Gabis[9] Wort
Und „Nägele“[10] mit Köpfen macht. Mafia

Unsre Gabi geht von Bord,
Zu neuen Ufern mit Elan,
Gewissenhaft, exakt ihr Stil
Hier hat sie sehr viel erreicht

Kämpft an einem andren Ort
Heuert sie in Nürnberg an
Führt sie wohl auch dort zum Ziel
Ja, der Abschied fällt nicht leicht. Mafia

Strophe (lang)
Wechselt auch der Kapitän, Mafia
Das Schiff wird niemals untergeh`n, Mafia
Immer weiter, Fahrt voraus, Mafia
Legen wir die Netze aus, Mafia

Schluss-Refrain:
Mafia, wo man uns braucht,
Jetzt auch ohne Schutzgebühr,

Sind wir da, schützen Dich auch,
Doch das Netzwerk sind nur wir!
Mafia, Mafia, …

Fußnoten

1) Dr. Peter Holleczek, Leiter Abteilung Kommunikationssysteme bis 2012
2) Uwe Hillmer, stellvertr. Leiter Abteilung Kommunikationssysteme bis 2013
3) Helmut Wünsch, Leiter Gruppe Netzbetrieb bis 2018
4) Holger Marquardt, Autor der „FAU Security Tools“
5) Thomas Fuchs, Techniker, Schwerpunkt Funk-LAN
6) Markus Schaffer, Techniker, Schwerpunkt Fehlerbehebung
7) Martin Fischer, Dr. Reiner Fischer, E-Mail-Gruppe
8) Michael Gräve, Leiter Multimediazentrum (MMZ)
9) Dr. Gabi Dobler, Leiterin Abteilung Kommunikationssysteme 2012 − 2018
10) Dr. Susanne Nägele-Jackson, Leiterin Forschungsgruppe Netz
11) Dr. Gabi Dobler verlässt das RRZE und gibt die Abteilungsleitung an Helmut Wünsch weiter.

Bezüge zu Mitarbeitern erfolgten gemäß Anlass und nach „künstlerischen“ Gesichtspunkten. Fehlende Erwähnung bedeutet keinesfalls eine geringere Wertschätzung.

Genderhinweis

Aus Gründen der Klarheit und Verständlichkeit wurde auf eine sprachliche Differenzierung zwischen weiblicher und männlicher Form im Wortlaut dieses Dokuments verzichtet. Alle Geschlechter sind in gleicher Weise gemeint.

Herausgeber:

Regionales Rechenzentrum Erlangen (RRZE)
Dr. G. Hergenröder
Martensstraße 1, 91058 Erlangen
Tel.: +49(0)9131 85-2 70 31
Fax.: +49(0)9131 30 29 41
www.rrze.fau.de
Friedrich-Alexander-Universität Erlangen-Nürnberg