GWDG-Bericht Nr. 73

Thomas Baumann, Dieter Ruder,
Bertram Smolny (Hrsg.)

24. DV-Treffen der Max-Planck-Institute

6. - 8. November 2007
in Jena

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Thomas Baumann, Dieter Ruder,
Bertram Smolny (Hrsg.)

24. DV-Treffen der Max-Planck-Institute

6. - 8. November 2007
in Jena

Thomas Baumann, Dieter Ruder,
Bertram Smolny (Hrsg.)

24. DV-Treffen der Max-Planck-Institute

6. - 8. November 2007
in Jena

GWDG-Bericht Nr. 73
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Am Faßberg
D-37077 Göttingen
Telefon: 0551 201-1510
Telefax: 0551 201-2150
E-Mail: gwdg@gwdg.de

Satz: Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Druck: Goltze Druck, Göttingen

ISSN 0176-2516

Inhalt

Vorwort

So vielfältig wie die Forschungsgebiete der MPG, so vielfältig sind auch die Anforderungen, die an die IT-Verantwortlichen respektive IT-Abteilungen der Max-Planck-Institute gestellt werden.

Die Mitarbeiterinnen und Mitarbeiter im Bereich der Datenverarbeitung sorgen mit der Entwicklung und dem Betrieb einer modernen ITK-Infrastruktur dafür, dass Wissen systematisch und effizient genutzt werden kann, dass Wissenschaft produktiv ist und bleibt.

Anfang November 2007 trafen sich dazu 170 Teilnehmer in Jena. Eingeladen hatten die Informations- und Telekommunikationstechnik-Gruppen (ITK) des MPI für Biogeochemie, des MPI für chemische Ökologie und des MPI für Ökonomik.

Die Agenda des 24. DV-Treffens unterstrich die Vielfalt der Aufgaben und bot Workshops und Referate zu den unterschiedlichsten Facetten eines modernen DV-Betriebs: Motto: „Diversität der Ideen“.

Der vorliegende Band enthält mehrere Beiträge des 24. DV-Treffens der Max-Planck-Institute, das vom 6. bis 8. November 2007 im Abbe-Zentrum des Campus Beutenberg in Jena stattfand.

Jena, 15.10.2008 Thomas Baumann, Dieter Ruder, Bertram Smolny

Das Organisatoren-Team des 24. DV-Treffens der Max-Planck-Institute in Jena

Direktgekühlte Serverschränke im Maschinenraum der GWDG – ein Erfahrungsbericht

Herbert Witt

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

1. Einleitung

Die zunehmende Leistungsdichte von neuen Servergenerationen bedingt ein Umdenken bei deren Unterbringung in den Rechnerräumen der Institute und in noch größerem Maße in den Maschinenräumen der Rechenzentren.

Während anfangs die Server noch als Desktopgeräte auf Tischen oder in Regalen standen, werden sie heute fast ausschließlich in kompakten 19-Zoll-Gehäusen für den direkten Einbau in Schränken mit entsprechenden Einbaurahmen angeboten. Solange die Gesamtwärmeleistung der in diesen Serverschränken eingebauten Geräte unterhalb von ca. 5 Kilowatt (kW) blieb, war die ausreichende Zufuhr kalter Luft zur Kühlung mit vertretbarem Aufwand noch gut zu realisieren.

Die Server wurden jedoch immer kompakter – bei rasant zunehmender Leistungsfähigkeit – und damit verbunden größerer Wärmeentwicklung. Da die Rechnerräume notorisch zu klein bemessen sind, kommt eine „halbe“ Befüllung der Schränke zumeist nicht infrage. So hat man das Problem, Wärmeleistungen von 8 kW bis 15 kW – und in Zukunft bis mindestens 25 kW –

abzuführen, die auf einer Schrankstellfläche von etwa einem Quadratmeter erzeugt werden.

Hier versagt die „klassische“ Raumkühlung, bei der die kalte Luft von einem zentralen Umluftkühlgerät erzeugt und zum Beispiel über einen Doppelboden mehr oder weniger gleichmäßig im Raum verteilt wird. Stattdessen geht man dazu über, die kalte Luft gezielt dort zu erzeugen, wo sie gebraucht wird und spricht dann von einer Direktkühlung oder closed coupled cooling.

Im Wesentlichen sind dafür zwei Lösungen verfügbar:

- Bei der „offenen“ Lösung wird die Kaltluft in der Nähe - aber außerhalb - der Schränke im ausreichenden Maße zur Verfügung gestellt und nach dem Prinzip der „heißen“ und „kalten“ Gänge zwischen den Schrankreihen gezielt gelenkt.
- Die „geschlossene“ Betriebsweise verlegt die Erzeugung der Kaltluft direkt in die Serverschränke, wo diese in einem geschlossenen Kreislauf zirkuliert.

Im Maschinenraum der GWDG sind zurzeit (Jahresende 2007) 15 closed-coupled-Serverschränke im Einsatz, die insgesamt eine Wärmeleistung von 200 kW erzeugen. Den Weg dahin mit seinen wichtigsten Richtungsentscheidungen bezüglich des Infrastrukturausbaus und wie es weitergehen wird (könnte), stellt dieser Bericht vor.

2. Rückblick

Die Planungen für die Infrastruktur von Rechnerräumen werden von einem Faktor stark beeinflusst:

Kann man „bei Null“ anfangen, ist also außer der Lage und eventuell der Größe des Raumes alles noch frei gestaltbar, oder ist der Raum bereits im Betrieb und soll nur verändert (angepasst) werden.

Im letzteren Fall ist bei größeren Anlagen gerade die Raumkühlung zumeist baulich schon vorgegeben und nur schwierig umzugestalten. Traditionell wird die Kaltluft über einen aufgeständerten Boden (Doppelboden, Unterboden) im Raum verteilt, über Bodenplatten mit Schlitzauslässen gezielt in den Raum geführt und unterhalb der Raumdecke bzw. im Zwischenraum einer abgehängten Decke wieder abgeführt.

Dieses Prinzip funktionierte und funktioniert solange gut, wie die aus einem Serverschrank abzuführende Wärmeleistung sich im Bereich von maximal ca. 3 bis 5 kW bewegt. Aber durch die zunehmende Packungsdichte der Ser-

ver und den steigenden Energiehunger der Prozessoren ist diese Wärmeleistung pro Schrank immer weiter angestiegen.

Die nachfolgende Grafik zeigt die Entwicklung der Wärmeleistung pro Schrank für die im Maschinenraum der GWDG betriebenen Clustersysteme.

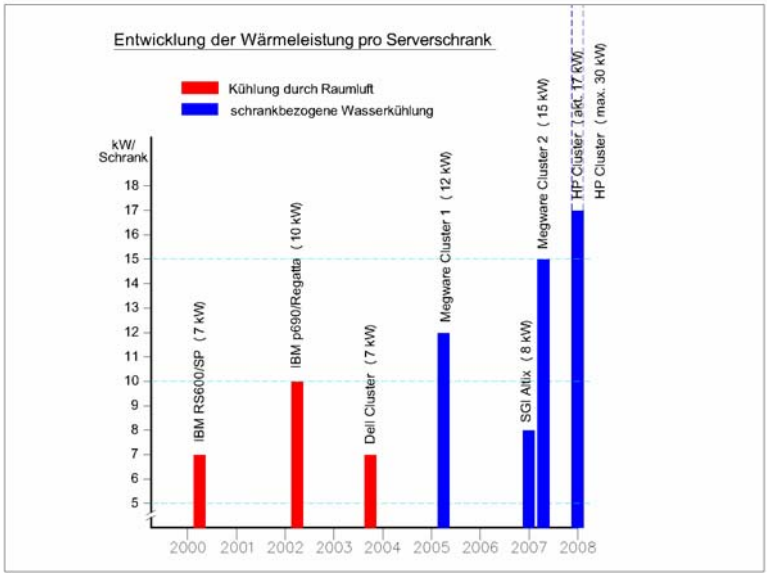


Bild 1: Cluster-Installationen bei der GWDG

Die bis zum Jahre 2004 beschafften Systeme waren ausschließlich raumluftgekühlt. Aber selbst bei einer Wärmeleistung von 7 bis 10 kW pro Schrank mussten bereits bauliche Maßnahmen für die Raumluftkühlung ausgeführt werden, die sich insbesondere aus dem Problem ergaben, die enorme Menge an benötigter Kaltluft gezielt an die Frontseiten der Serverschränke zu führen. Insgesamt mussten 15 Schränke mit einer Gesamtwärmeabgabe von 120 kW berücksichtigt werden (siehe Bild 2).

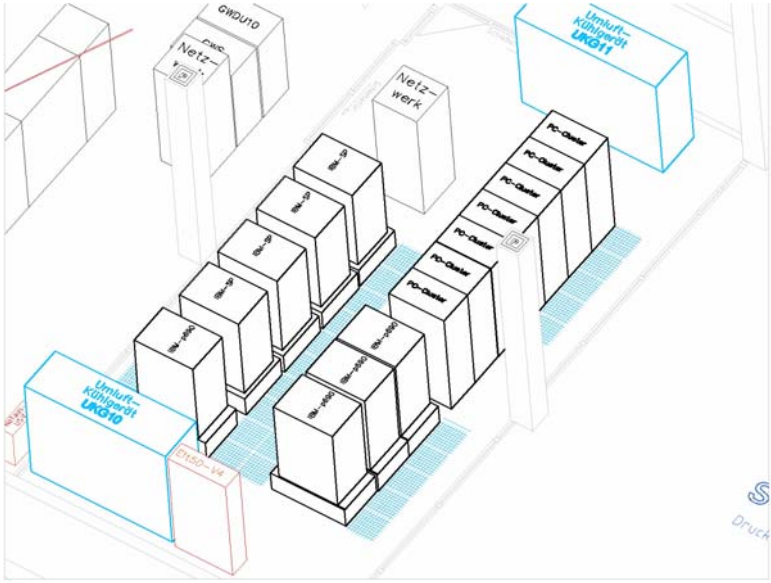


Bild 2: Abgeschotteter Bereich des Maschinenraums für den Betrieb raumluftgekühlter Cluster-Systeme

Dazu wurde ein Teil des Maschinenraumes (ca. 70 m²), inklusive des Unterbodens und des Raumes oberhalb der abgehängten Decke, abgeschottet. Dadurch sollte verhindert werden, dass der druckvolle Kaltluftstrom, der von zwei an gegenüberliegen Raumseiten aufgestellten Umluft-Kühlgeräten mit je einer Leistung von 100 kW erzeugt wurde, in benachbarte Bereiche abfließt. Ein angenehmer Nebeneffekt dieser Schottung war die spürbare Reduzierung der Lärmeinwirkung auf den restlichen Maschinenraum.

Anstatt der üblichen Schlitzplatten mussten Gitterrasterplatten mit größeren Austrittsöffnungen in den Doppelboden eingesetzt werden, um dem Luftstrom einen möglichst geringen Strömungswiderstand zu bieten.

Mit diesen Vorbereitungen glaubte man nun, alle Anforderungen für die Kühlung der „7 bis 10 kW“-Serverschränke erfüllen zu können. Letztendlich war dem auch so, aber:

- Die hohen Luftströmungen im Unterboden kehren deren Strömungsrichtung in der Nähe der Umluft-Kühlgeräte um. Die Luft wird durch die Gitterplatten in den Unterboden gesaugt, statt dort in den Raum zu strömen.

- Auch die im nur 45 cm hohen Doppelboden verlegten Kabel und Kaltwasserrohre behinderten die Luftströmung der Umluftkühlgeräte und verursachten störende Wirbel.
- Der Raum war ein unwirtlicher Arbeitsplatz; stürmische und kalte Zugluft gab es im Bereich der Schrank-Frontseiten, heiße Wüstenwinde an den Rückfronten. Dazu war es sehr laut.
- Der rückseitige Abstand der Schränke zu den Schottungswänden hätte größer bemessen sein müssen, um Wärmestaus (Wärmenester) in diesem Bereich zu verhindern. Abhilfe verschaffte nur eine „Todsünde“: Gitterrasterplatten wurden im Bereich der Schrankrückseiten, dem so genannten „heißen Gang“, eingelegt, um Warmluft nach oben zu drücken.
- Aber auch ein Cluster-Hersteller hatte die Wärmeabfuhr aus seinen Serverschränken nicht im Griff: die komfortablen horizontalen Kabelführungseinrichtungen mussten ausgebaut werden, da sie den Ausströmbereich für die Warmluft fast vollständig abdeckten und sich die Server überhitzten.
- Zur vollen Ausnutzung der theoretischen maximalen Kühlleistung (200 kW) wären zusätzliche bauliche Abschottungsmaßnahmen oberhalb der Schränke notwendig gewesen, um die teilweise Vermischung von Kalt- und Warmluft zu verhindern.

Fazit: Trotz einer theoretischen Kühlleistung vom 200 kW war mit der installierten Leistung von 120 kW die Auslastungsgrenze des Raumes erreicht. Eine Kapazitätserweiterung hätte nur über erhebliche bauliche Veränderungen erreicht werden können.

Insofern kam es der GWDG sehr gelegen, dass die nächsten Cluster-Generationen (anfangs manchmal auch nur alternativ oder mit leichtem Drängen) in wassergekühlten Schränken angeboten wurden.

3. Wassergekühlte Serverschränke und vorbereitende Infrastruktur

Das erste Clustersystem in zwei wassergekühlten Schränken wurde im Jahre 2005 beschafft (Bild 7). Da die primäre Kaltwasserversorgung der Umluftkühlgeräte für die Raumluftkühlung im Maschinenraum mit einer Vorlauftemperatur von 6°C zu kalt für eine direkte Einspeisung in die Serverschränke war (dazu später mehr), wurde ein Wasser-Wasser-Wärmetauscher (Firmenbezeichnung Cooltrans Unit, CTU, links im Bild 3) in der Nähe der Schränke installiert. An diesen sind zwischenzeitlich vier Schränke

angeschlossen, die jeweils in 42 Höheneinheiten (HE) Geräte mit einer Gesamtwärmeleistung bis zu 15 kW aufnehmen können.

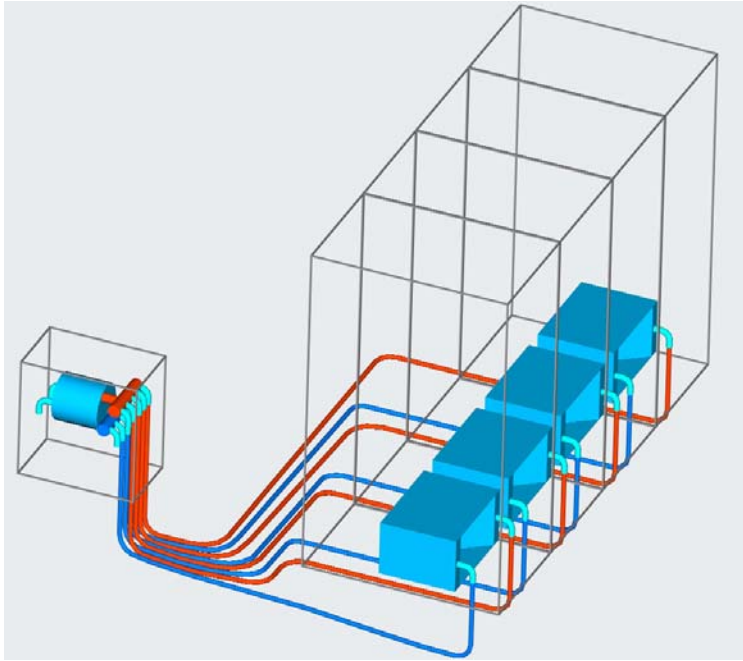


Bild 3: Wassergekühlte Serverschränke mit 75 kW Wasser-Wasser-Wärmetauscher (links im Bild)

Bei diesem Schranktyp (Herstellerfirma Knürr) ist der Wasser-Luft-Wärmetauscher unterhalb der eingebauten Server installiert. Über einen Luftkanal mit integrierten Ventilatoren an der Rückwand wird die erwärmte Luft durch den Wärmetauscher geleitet und strömt an der Frontseite gekühlt wieder aus (Bilder 4 und 5).

Die CTU ist mit 45 cm (B) x 99 cm (H) x 95 cm (T) sehr kompakt (Bild 5). Sie ist für den Anschluss von maximal fünf Serverschränken mit einer Gesamtleistung von 75 kW ausgelegt.

Die Trennung der Kaltwasserversorgung in einen Primär- und Sekundärkühlkreislauf hat viele Vorteile:

- Die Temperatur des Wassers für den Sekundärkreislauf (Schrankseite) kann unabhängig von der Temperatur im Primärkreislauf eingeregelt werden und ist auch bei Schwankungen im letzteren stabil.

- Ebenso werden Druckschwankungen im Primärkreislauf auf der Schrankseite kompensiert.
- Die maximal ausfließende Wassermenge ist bei einer Leckage in einem der angeschlossenen Schränke oder der Zuleitung dahin um ein Vielfaches geringer, als wenn die Schränke direkt im Primärkreislauf eingebunden wären.
- Über Feuchtefühler im Bereich der CTU kann der Taupunkt (diejenige Temperatur, unterhalb derer Wasser kondensieren würde) überwacht und die Vorlauftemperatur des Wasser gegebenenfalls angehoben werden. Dies erspart die Isolierung der Verrohrung und Armaturen im Sekundärkreislauf.

Bild 4: Wassergekühlter Schrank der Firma Knürr, Rückseite

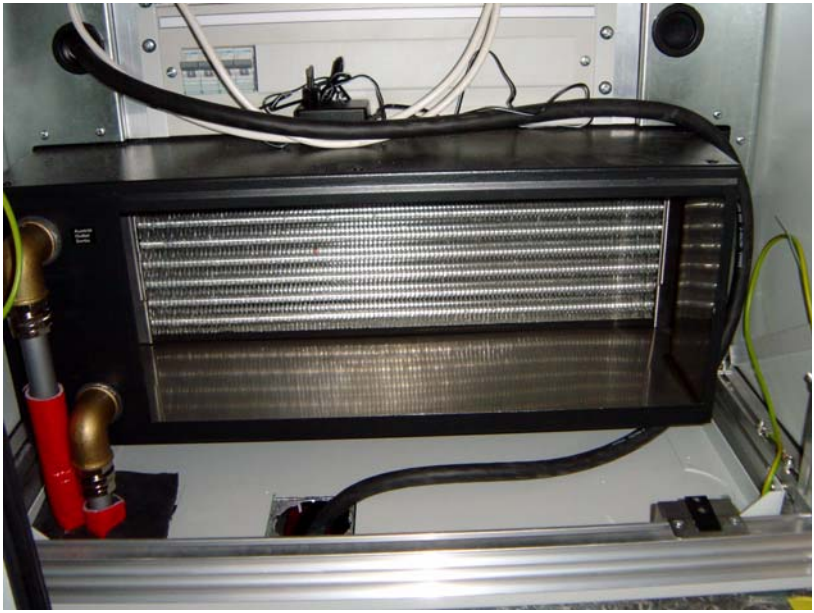


Bild 5: Wasser-Luft-Wärmetauscher im Serverschrank

Bild 6: Wasser-Wasser-Wärmetauscher (CTU) mit 75 kW Leistung

Bild 7: Linux-Cluster der Firma Megware, installiert im Jahre 2005

Seit der Inbetriebnahme im Jahre 2005 sind keine Störungen bzw. Ausfälle der angeschlossenen Cluster-Systeme zu verzeichnen, die auf das Kühlsystem zurückzuführen sind.

Für die Folgejahre wurde dann absehbar, dass die anstehenden Neubeschaffungen im Bereich Parallelrechner-/Cluster-Systeme sowohl hinsichtlich der Anzahl der neu hinzukommenden Serverschränke als auch der zusätzlich erforderlich werdenden Kühlleistung bereits in der ersten Ausbaustufe über fünf Schränke und 75 kW Gesamtwärmeleistung liegen würde. Mehrere Neuinstallationen auf Basis der bestehenden „kleinen“ Lösung (fünf Schränke, 75-100 kW Kühlleistung) wären nicht sinnvoll gewesen, da zum einen die zusätzlichen CTUs weitere Stellflächen im Maschinenraum belegt hätten und zum anderen für jede Erweiterung umfangreiche klimatechnische Installationen (vermutlich mit Abschaltzeiten für die primäre Kaltwasserversorgung) erforderlich gewesen wären.

Aus diesen Gründen sollte das neue Kühlsystem für die Serverschränke folgende Kriterien erfüllen:

- Die zur Verfügung gestellte Kühlleistung muss über die 200 kW der ersten Ausbaustufe hinaus bis 400 kW aufrüstbar sein.
- Das Kühlwasser soll durch ein im Doppelboden vorverlegtes Rohrsystem bereits unmittelbar bis in die Bereiche geführt werden, die für die Aufstellung wassergekühlter Serverschränke vorgesehen sind.
- Der Anschluss eines neuen Serverschrankes muss ohne Unterbrechung der Kühlwasserversorgung für die anderen Cluster-Systeme möglich sein.

Im Februar 2007 wurde die neue Kaltwasserversorgung in Betrieb genommen (Bild 8).

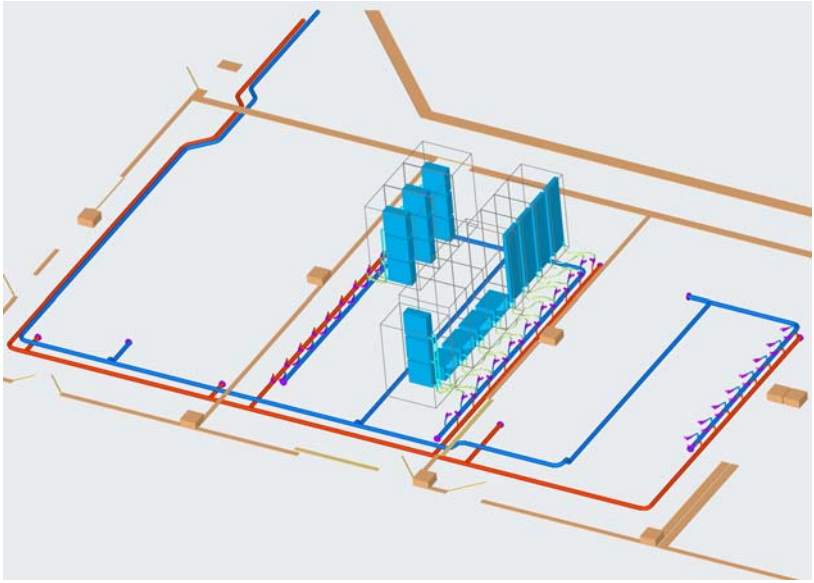


Bild 8: Vorinstalliertes Kaltwasserrohrnetz im Doppelboden des Maschinenraums der GWDG

Zurzeit sind 38 Anschlüsse für drei Schrankreihen vorinstalliert. Die Anschlüsse für drei weitere Reihen können bei Bedarf ohne Betriebsunterbrechung nachgerüstet werden. Die Verrohrung ist als so genannter Tichelmann-Ring ausgeführt. Bei dieser Verlegungsart ist die Gesamtlänge der Rohre (Vor- und Rücklauf) vom Wasser-Wasser-Wärmetauscher zu jedem Serverschrank einer Reihe immer gleich. Dadurch ergeben sich die gleichen Druckverhältnisse an jedem Wärmetauscher in den Schränken, was für die Einregulierung der Durchflussmengen und deren Konstanz von Bedeutung ist. Zwei Wasser-Wasser-Wärmetauscher mit je einer Leistung von 100 kW sind außerhalb des Maschinenraums im Technikbereich des Gebäudes installiert (Bild 9) und im Bild 8 nicht mit eingezeichnet.

Bild 9: Zwei Wasser-Wasser-Wärmetauscher mit je 100 kW Leistung erzeugen das 12° C kalte Kühlwasser für die Serverschränke.

Die Vorlauftemperatur des Kühlwassers beträgt nominell 12° C. Eine Taupunktüberwachung erhöht die Wassertemperatur automatisch auf bis zu 16° C, wenn durch eine extrem hohe Luftfeuchte die Gefahr besteht, dass sich Kondenswasser an den nicht isolierten Edelstahlrohren bilden könnte. Auf eine Isolierung der Rohre wurde verzichtet, da diese den freien Quer-

schnitt für die Kabel- und Luftführung im nur 45 cm hohen Raum im Doppelboden zu stark reduziert hätte.

Bild 10 zeigt als Ausschnitt den Bereich, in dem jetzt bereits Serverschränke betrieben werden. Die Ansicht der Schränke ist auf den Schrankrahmen und die integrierten Wasser-Luft-Wärmetauscher reduziert. Die Pfeile sollen die Strömungsrichtung der Luft im Schrank verdeutlichen. Neben der bereits beschriebenen Anordnung der Wärmetauscher unterhalb des 19-Zoll-Einbaurahmens sind diese bei jeweils vier weiteren Schränken vertikal neben den Einbauebenen bzw. als Schrankrückwand eingebaut. Bei beiden Einbauten wird ein horizontaler Luftstrom erzeugt. Mit dem Prinzip der Rückwandkühlung wird eine Belastung des Raumes durch Wärme zwar ebenfalls verhindert, aber diese entsteht durch den Luftstrom und der damit fehlenden Geräuschkapselung.

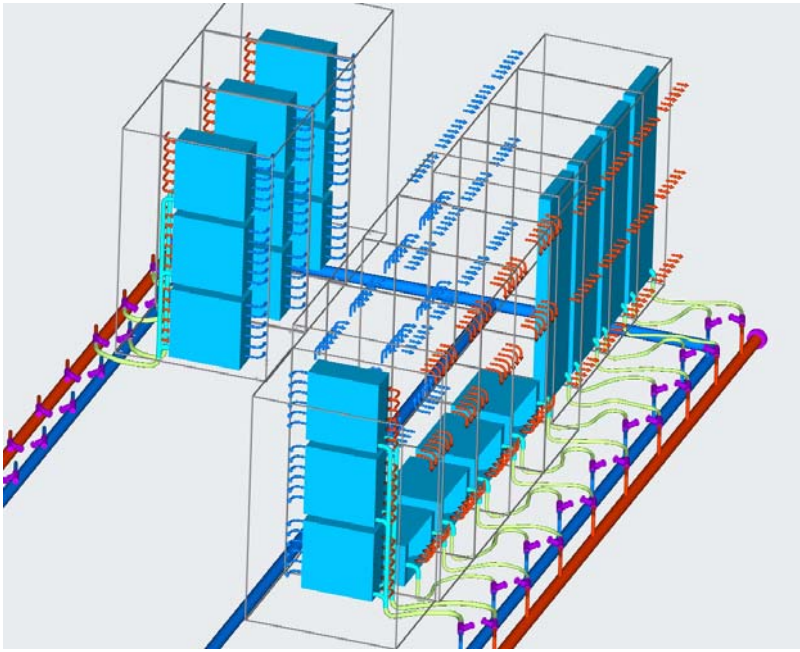


Bild 10: Unterschiedliche Ausführungsformen der Wasser-Luft-Wärmetauscher

Betriebserfahrungen

Der Tichelmann-Ring ist seit einem Jahr im Betrieb. Acht Serverschränke waren von Anfang an angeschlossen, drei weitere wurden im Dezember 2007 zugefügt. Die Stabilität der Kühlwasserversorgung war über die ganze Betriebszeit gegeben. Auch der Anschluss weiterer Schränke im laufenden Betrieb entsprach der Planungsvorgabe, dass dieses ohne Auswirkungen auf die Kühlung der übrigen Schränke erfolgen sollte.

Lediglich die Taupunktsteuerung führte im Sommer indirekt zu einem Problem. Die Feuchtefühler für die Steuerung waren in dem abgeschotteten Bereich, in dem die Serverschränke zurzeit aufgestellt sind, im Doppelboden installiert. Wie sich herausstellte, war die Luftfeuchtigkeit hier durch das 100-kW-Umluftkühlgerät und die „offene“ Rückwandkühlung von vier Serverschränken um fast 10 Prozent geringer als in den übrigen Maschinenraumbereichen, durch die die unisolierten Kaltwasserrohre ebenfalls verlegt worden sind. Dadurch wurde an Tagen mit hoher Luftfeuchtigkeit die Vorlauftemperatur nicht ausreichend angehoben und es kam zu Kondenswasserbildung (siehe Bild 11).

Da die Schränke mit unten integriertem Wärmetauscher bis zu 220 Zentimeter hoch sind, sollte frühzeitig geprüft werden, ob die Zugangswege eine ausreichende lichte Höhe haben. Ansonsten bleibt nur die Möglichkeit, den leeren (immerhin noch 310 kg schweren Schrank) liegend zu transportieren (Bild 12) und erst vor Ort zu bestücken, worauf sich sicherlich die meisten Firmen nicht einlassen werden.

Bild 11: Kondenswasserbildung an den Kaltwasserrohren durch falsch installierte Feuchtefühler

Bild 12: Höhere Schränke (220 cm) müssen häufig gekippt zum Aufstellungort transportiert werden

4. Vorhaltung wassergekühlter Schränke

Der Betrieb von Clustern in Serverschränken mit integriertem Kühlsystem, wie er im vorherigen Abschnitt vorgestellt wurde, hat sich für die GWDG als ein richtiger Schritt erwiesen, gerade auch in Hinblick auf die zu noch zu erwartende Steigerung der Leistungsdichte. Bisher wurde jedoch davon ausgegangen, dass die Schränke mehr oder weniger betriebsbereit und zumeist voll bestückt angeliefert und während ihrer Betriebszeit nur wenigen Veränderungen unterworfen werden. Wie steht es aber mit der Vorhaltung von leeren Schränken, die vor Ort nach und nach mit Servern aufgefüllt werden? Können wassergekühlte Schränke die Standard-Serverschränke mit Raumluftkühlung ersetzen? Dazu müsste z. B. die Kühlleistung soweit heruntergeregelt werden können, dass eine Erstbestückung von nur 500 Watt möglich ist, oder Lastschwankungen von einigen Kilowatt müssen ausgeregelt werden. Um diesen und weiteren Fragen auf den Grund gehen zu können, wurde im Jahre 2005 ein unbestückter Schrank mit einer Kühlleistung von 15 kW beschafft (einer der Schränke im Bild 3) und umfangreichen Tests unterzogen. Für die Wärmeerzeugung wurden acht Heizregister mit je einer Wärmeleistung von 2 kW eingebaut, die einzeln über funkgesteuerte Schalter beliebig zugeschaltet werden konnten (siehe Bild 13).

Bild 13: Frontseite des getesteten Schrankes mit acht Heizregistern zu je 2 kW

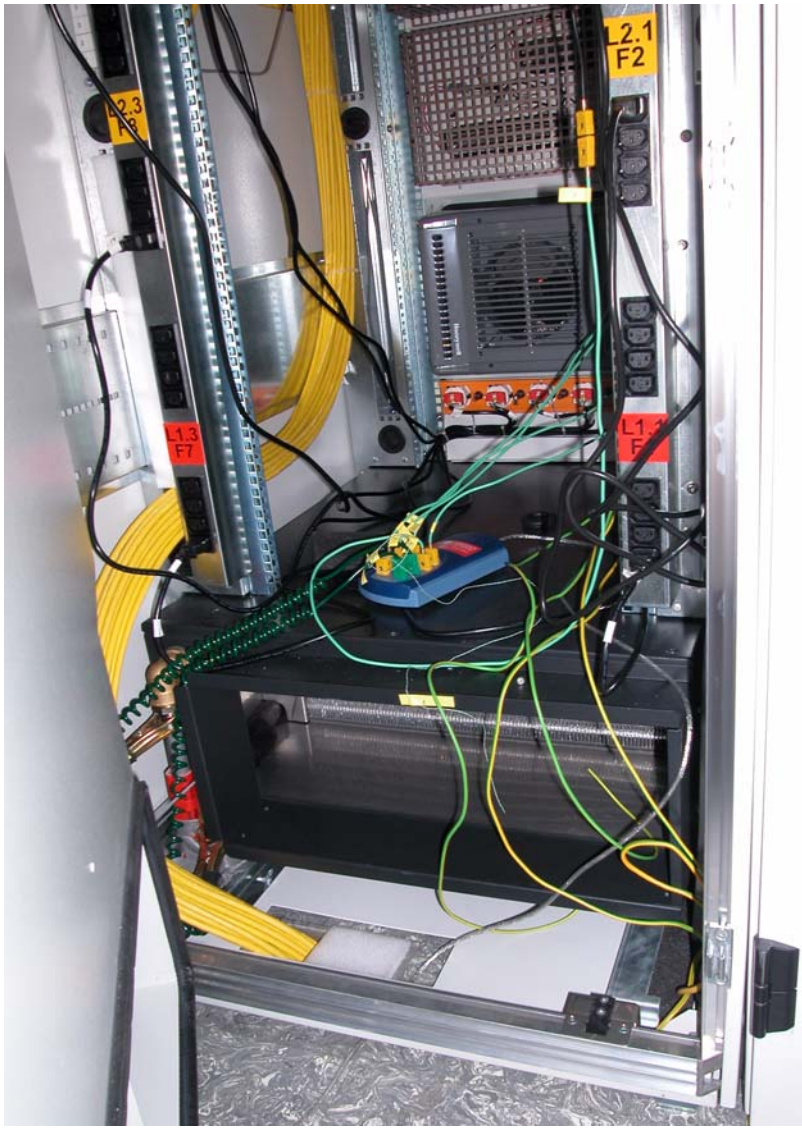


Bild 14: An acht Punkten wird der Temperaturverlauf im Schrank protokolliert

An acht markanten Punkten (wie z. B. Lufteintritt, -austritt des Wärmetauschers, Frontseite unterer und oberer Bereich, Kaltwasservor- und -rücklauf) wurde der Temperaturverlauf während der Tests protokolliert (Bild 14). Weiterhin wurde die Luftströmungsgeschwindigkeit und der Differenzdruck zwischen Schrankfrontseite und Innenraum gemessen.

Bild 15 zeigt ein typisches Testprotokoll, das die Temperaturentwicklung im Schrank bei ansteigender Wärmeleistung darstellt. Allerdings waren seitens des Lieferanten des Wasser-Wasser-Wärmetauschers (CTU) noch Nachbesserungen erforderlich, bis es so „geordnet“ zuging.

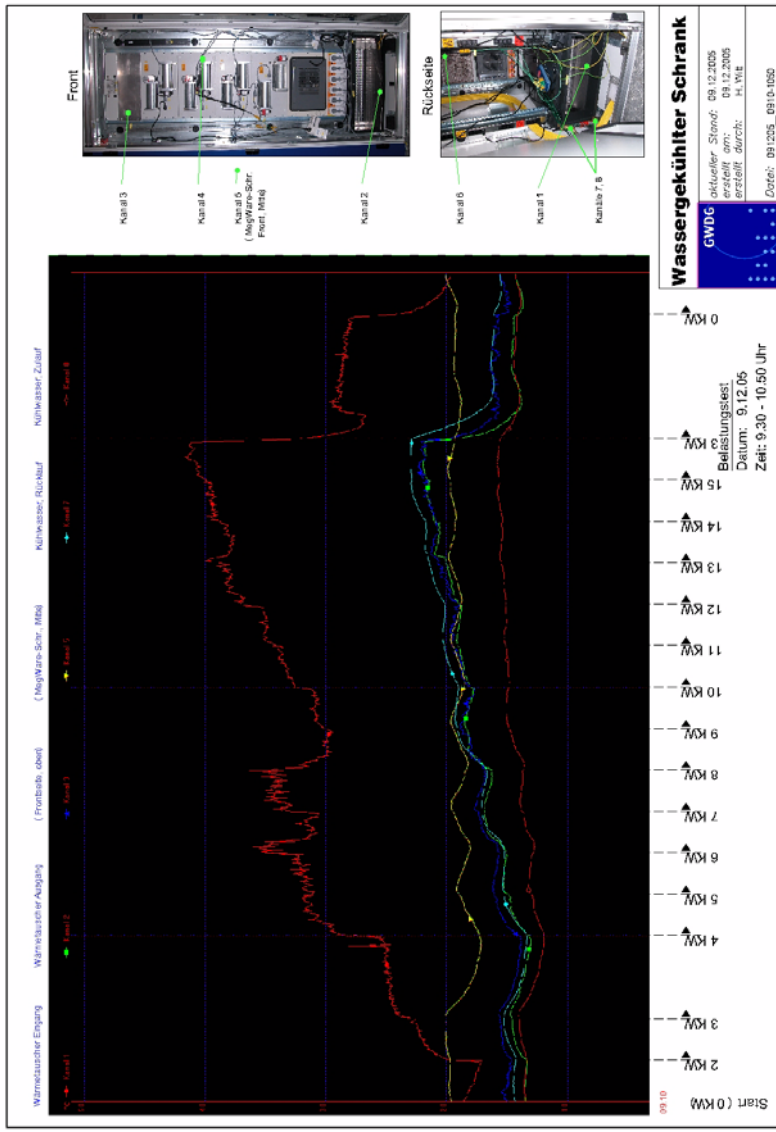


Bild 15: Belastungstest des wassergekühlten Serverschranks: Beispiel für die Temperaturentwicklung bei Laständerung

So war anfangs die Durchflussmenge an Kaltwasser für den Schrank zu gering einjustiert. Dies hatte zur Folge, dass bei Volllast die frontseitige Schranktemperatur über 35° C anstieg und die schrankinterne Temperaturüberwachung die Stromversorgung abschaltete (immerhin war deren Funktion damit auch gleich überprüft). Dann gab es noch ein Problem mit der Taupunktüberwachung, die die Vorlauftemperatur des Kühlwassers immer dann anheben soll, wenn aufgrund von hoher Luftfeuchtigkeit die Gefahr der Kondensation von Wasser gegeben ist. Die Regelschwingungen in Bild 16 zeigen, dass dieses anfänglich nicht funktionierte.

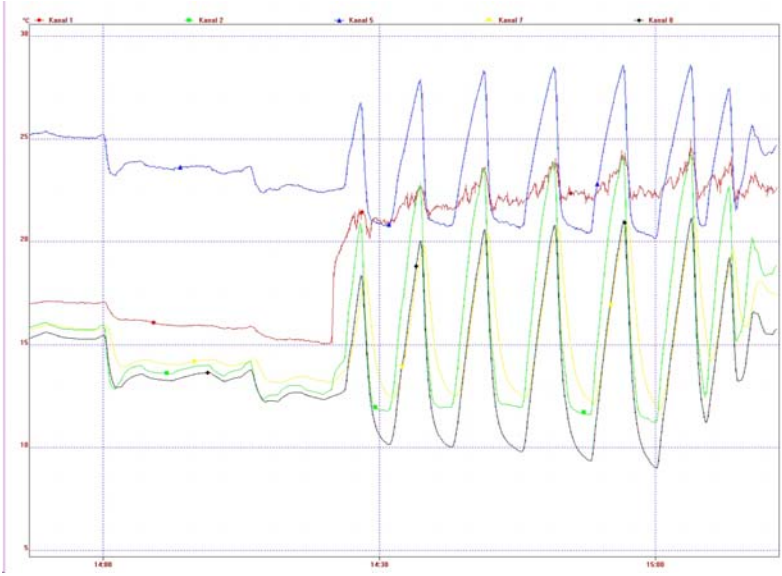


Bild 16: Die Taupunktregelung des Kühlsystems war anfangs instabil (Untere Kurve ist die Wasservorlauftemperatur)

Am Ende der Testreihen und Nachbesserungen stand jedoch als Ergebnis fest, dass geschlossene wassergekühlte Serverschränke durchaus für die sukzessive Bestückung geeignet sind. Allerdings sollte die Erstbestückung mit 3 kW anfangen, da die minimal einstellbare Durchflussmenge an Kaltwasser sonst immer noch zu einer „Unterkühlung“ des Schrankes führen könnte, was z. B. die einwandfreie Funktion von Festplatten beeinträchtigen könnte. Möglicherweise ist dieses Problem aber mit den jetzt auf den Markt kommenden Serverschränken mit einer Drei-Wege-Ventil-Regelung am Wärmetauschereingang beseitigt.

Das Öffnen der Schranktüren im laufenden Betrieb, um z. B. weitere Server einzubauen, ist ebenfalls möglich. Während dieser Öffnungszeit versorgen sich die Server mit Kaltluft aus dem umgebenden Raum. Der muss dann aber so leistungsfähig klimatisiert sein, dass die zusätzliche Wärmelast des Serverschranks abgefedert werden kann.

Auch die Mindestausstattung eines Schrankes für die Stromversorgung der Server sollte bedacht werden. Theoretisch können bis zu 40 Server (je 1 HE) eingebaut werden, die vermutlich größtenteils zwei Netzteile für den Betrieb an zwei getrennten Stromeinspeisungen besitzen. Idealerweise hat ein Serverschrank also zwei Stromkreise mit je 15 kVA Leistung, die sich über mindestens zweimal zehn C16-Sicherungsautomaten auf zweimal 42 Steckdosen aufteilen, die möglichst seitlich des 19-Zoll-Einbaurahmens vertikal installiert sein sollten, um keine Einbauplätze für Server zu blockieren.

5. Zusammenfassung

Im Maschinenraum der GWDG sind im Jahre 2000 die ersten Clustersysteme in Betrieb genommen worden, deren Wärmeabgabe pro Serverschrank über 7 kW betrug. Diese – sowie weitere bis zum Jahre 2004 beschafften Systeme – nutzten zur Kühlung die Raumluft. Bei so großen Leistungsdichten pro Schrank war es schwierig, das erforderliche Kaltluftvolumen über zentrale Klimageräte gezielt an die Frontseiten der Schränke zu leiten. Nur mit einem aufwändigen Um- und Ausbau wäre es möglich gewesen, die theoretisch zur Verfügung stehende Kühlleistung auch nutzen zu können. Als Alternative bot sich der Einstieg in eine so genannte closed-coupled-Kühlung an, bei der die Kaltluft direkt dort erzeugt wird, wo sie benötigt wird. Dies bedeutet, dass Wasser-Luft-Wärmetauscher möglichst nahe den zu kühlenden Serverschränken installiert sind oder sogar in die Schränke integriert werden.

Ab dem Jahre 2005 haben alle neu beschafften oder gehosteten Serverschränke eine schrankbezogene Wasserkühlung. Die Wärmetauscher sind entweder als Rückwand der Schränke ausgebildet (offenes System) oder sie sind unterhalb oder neben den Einbaurahmen für die Server direkt im allseitig abgedichteten Schrank installiert (geschlossenes System).

Um flexibel und ohne Betriebsunterbrechung weitere wassergekühlte Serverschränke in Betrieb nehmen zu können, wurde im Doppelboden des Maschinenraums ein Kaltwasserrohrnetz verlegt, an das im derzeitigen Ausbauzustand bis zu 38 Schränke mit einer Gesamtwärmeleistung von 400 kW angeschlossen werden können. Zurzeit sind 15 wassergekühlte Serverschränke mit einer Wärmeleistung von bis zu 15 kW pro Schrank und circa

200 kW insgesamt im Betrieb. Von anfänglichen – eher geringfügigen – Planungs- und Konstruktions- und Installationsfehlern abgesehen, funktioniert die Kühlwasserversorgung bisher fehlerfrei und war nie die primäre Ursache für eine Cluster-Abschaltung.

Umfangreiche Tests bei der GWDG haben gezeigt, dass wassergekühlte Serverschränke auch für eine sukzessive Bestückung geeignet sind, also erst am Einsatzort nach und nach mit Geräten aufgefüllt werden. Allerdings sollten die Geräte der Erstbestückung mindestens eine Wärmeleistung von 3 kW haben, da die Kühlleistung des Schrankes nicht ganz auf Null heruntergeregelt werden kann.

Aufbau eines Grid-Rechenzentrums unter den Aspekten Kompaktheit und Energie-Effizienz

Manfred Alef, Holger Marten

Forschungszentrum Karlsruhe GmbH
Institut für Wissenschaftliches Rechnen (IWR) /
Steinbuch Centre for Computing (SCC)
Eggenstein-Leopoldshafen

1. Einführung

Seit 2001 entsteht im Grid Computing Centre Karlsruhe (GridKa) des Forschungszentrums Karlsruhe ein PC-Cluster mit aktuell rund 2.600 CPU-Cores und 1.300 TB Online-Plattenplatz. Wesentliches Ziel dieses Projektes ist, parallel zu Planung und Aufbau des Teilchenbeschleunigers LHC am CERN eine Rechner- und Dateninfrastruktur („Tier-1-Zentrum“) zu entwickeln und zu betreiben, welche es den deutschen Wissenschaftlern ermöglicht, ab 2008 die LHC-Experimente Alice, Atlas, CMS und LHCb auszuwerten. Parallel dazu dienen die GridKa-Ressourcen den ständig wachsenden Anforderungen der bereits produktiven Teilchen- und Astroteilchenphysik-Experimente BaBar, CDF, D0, Compass und Auger sowie weiteren Communities der deutschen Grid-Initiative D-Grid.

Der Aufbau dieser Grid-Installation im vorhandenen Rechenzentrum stellt hohe Anforderungen an die Kompaktheit, Stromversorgung und ausreichende Kühlung der Systeme. Vor allem um die erforderliche Packungsdichte an Rechnern und Plattensystemen unter den räumlichen Gegebenheiten zu erreichen, hat das Forschungszentrum mit GridKa frühzeitig als erstes Rechenzentrum weltweit wassergekühlte Rechnerschränke eingeführt. Gleichzeitig wurde mit eingehenden Untersuchungen begonnen, wie der Stromverbrauch bereits „an der Quelle“, also im Rechner, minimiert werden kann. Als Ergebnis dieser Messungen werden seit einigen Jahren in den Ausschreibungen von Cluster-Erweiterungen Energieverbrauch und Platzbedarf der angebotenen Systeme berücksichtigt. Damit werden insgesamt zwei Ziele erreicht: eine optimale Nutzung der RZ-Infrastruktur sowie die Einsparung von Energie und Gesamtkosten.

2. Anforderungen

Die im Jahr 2001 zusammengestellten Anforderungen an die von GridKa im Laufe der Jahre bereitzustellenden CPU-Rechenleistungen, Festplatten- und Bandkapazitäten, mit exponentiellem Wachstum vor allem in den Jahren 2006 bis 2008, sind in Abb. 1 skizziert.

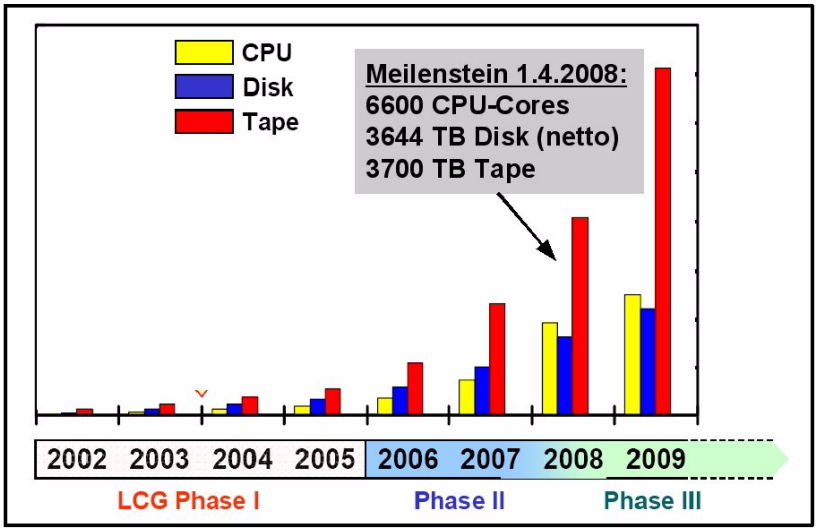


Abb. 1: Anforderungen an GridKa (Rechenleistung, Festplattenplatz, Magnetbandkapazitäten)

3. Frühe Schritte

Als einer der ersten Schritte nach der Gründung des Grid Computing Centres Karlsruhe (GridKa) wurden die zu erwartenden Anforderungen an die Infrastruktur (Raum, Stromversorgung, Kühlung) abgeschätzt. Es zeigte sich, dass die vorhandenen raumlufttechnischen Anlagen für eine ausreichende Kühlung der vorgesehenen Komponenten unterdimensioniert waren. Als Alternative zum Ausbau der Luftkühlung wurden wegen der geschätzten großen Luftmengen und -geschwindigkeiten („Hurrican“) auch die Möglichkeiten einer Wasserkühlung untersucht. Marktuntersuchungen ergaben allerdings, dass es zu dieser Zeit keine fertige Lösung „von der Stange“ gab. Deshalb wurde 2001 ein Leistungsverzeichnis erstellt und eine Ausschreibung für wassergekühlte Rechnerschränke gestartet.

4. Wassergekühlte Clustersysteme

Die von der Fa. Knürr angebotene und im GridKa installierte Lösung ist in Abb. 2 skizziert. In dem geschlossenen 19"-Rechnerschrank sind ein Luft-Wasser-Wärmetauscher sowie zwei (redundante) temperaturgeregelte Lüfter montiert.

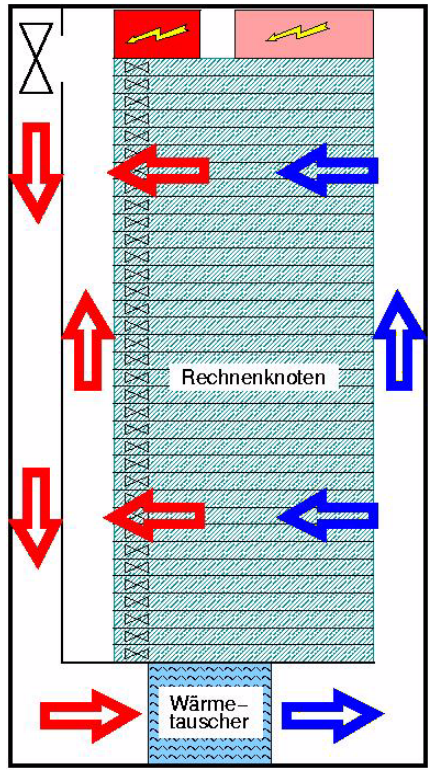


Abb. 2: Wassergekühlter Rechnerschrank (Querschnitt)

Ein kritischer Parameter bei der Vorbereitung der Ausschreibung war die Festlegung, wieviel Wärme pro Schrank maximal entstehen kann und per Wasserkühlung abzuführen ist. Messungen der vorhandenen Cluster ergaben damals (2001) eine maximale Stromaufnahme von rund 3,5 kW pro Schrank (s. Abb. 3). Unter Berücksichtigung gewisser Reserven erschien deshalb eine Auslegung der Wasserkühlung auf höchstens 10 kW ausreichend.

Bei den Abnahmetests des im Oktober 2002 gelieferten Prototypen mussten noch Heizlüfter verwendet werden, um eine Gesamt-Heizleistung im Schrank von 10 kW zu erreichen. Leider war jedoch die eingeplante Reserve schneller erreicht als erwartet. Bereits im Jahre 2004 lagen die installierten Cluster-Erweiterungen geringfügig oberhalb der 10 kW ... (s. Abb. 3).

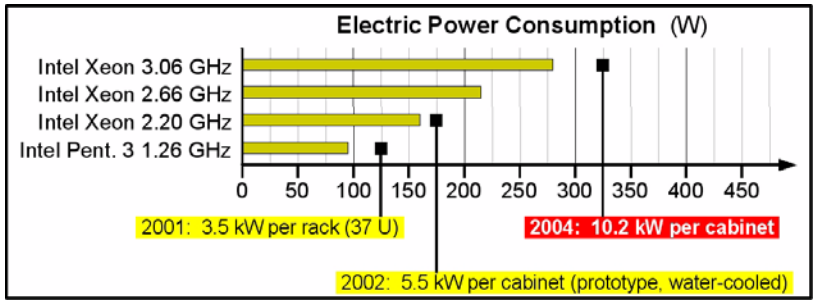


Abb. 3: Entwicklung der Stromaufnahme (= Wärmeabgabe) eines Rechner-Clusters (pro 19“-Schrank)

Ferner lagen die geschätzten Stromkosten für Betrieb und Kühlung dieser Systeme über eine prognostizierte Lebensdauer von drei Jahren bei über 50 % der Anschaffungskosten!

5. Wieviel Strom verbraucht unser Cluster pro Rechenoperation?

Um diese Entwicklung näher zu untersuchen und die zukünftige Entwicklung der Stromaufnahme sowie Möglichkeiten für Einsparungen zu analysieren, wurde nun mit systematischen Untersuchungen insbesondere auch des Verhältnisses zwischen Rechenleistung und Stromaufnahme begonnen. Zur Messung der Rechengeschwindigkeit wurden die Integer-Benchmarks aus der SPEC CPU2000[1] verwendet, auf denen auch die Spezifikation der Anforderungen an GridKa basiert (Abb. 1).

Erstaunlicherweise demonstrierten diese Untersuchungen, dass zwischen 2002 und 2004 der Stromverbrauch wesentlich stärker angestiegen ist als die erzielte Rechenleistung (Abb. 4).

1. SPEC und SPECint sind eingetragene Warenzeichen der Standard Performance Evaluation Corporation (SPEC, www.spec.org).

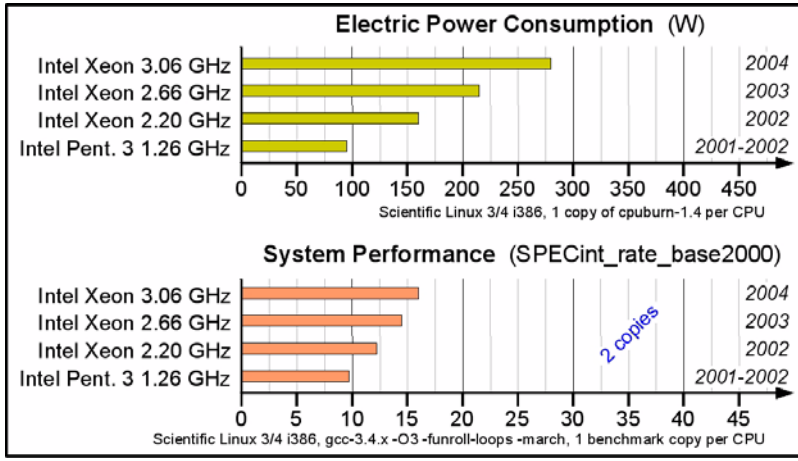


Abb. 4: Gegenüberstellung von Rechenleistung und elektrischer Stromaufnahme der im GridKa installierten Clustersysteme von 2001 bis 2004

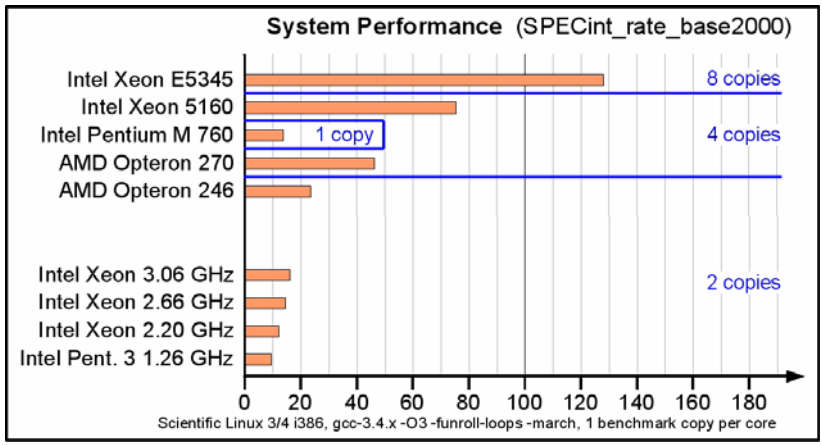
6. Sparen an der Quelle?

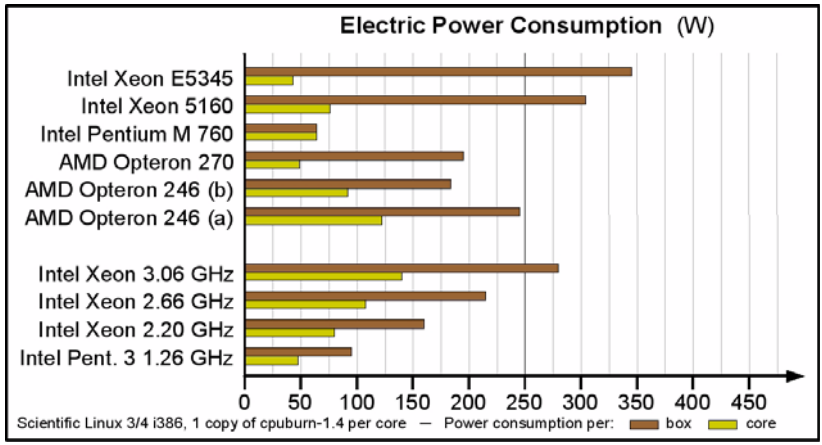
Nach diesen Erfahrungen wurden Messreihen auf unterschiedlichen Systemen mit verschiedenartigen Prozessoren gestartet. Darin einbezogen waren auch Systeme auf der Basis stromsparender Mobil-Technik. Als Ergebnis konnte festgestellt werden, dass sowohl Systeme mit AMD-Opteron-CPUs als auch mit Pentium-M-Prozessoren von Intel eine deutlich höhere Rechenleistung bei gleichzeitig niedrigerem elektrischem Stromverbrauch hatten als die damaligen Systeme mit Intel-Xeon-CPUs auf Basis des Pentium 4.

Daraufhin wurden bei neuen Ausschreibungen die Bewertungskriterien erweitert: Neben den reinen Anschaffungskosten werden auch die im Laufe der erwarteten Nutzungsdauer der Clustersysteme anfallenden Stromkosten (Betrieb, Kühlung) mit gewertet. Die Folge war, dass die Anbieter – zumindest kleinere Firmen, die ihre Systeme aus den am Markt verfügbaren Komponenten kurzfristig weitgehend beliebig zusammenstellen können – jetzt in der Regel auf energiesparende Bauteile achten. Besonders deutlich wurde dies in zwei aufeinander folgenden Beschaffungen, bei denen jeweils Systeme auf der Basis des AMD Opteron 246 (2,0 GHz, single-core) geliefert wurden. Bei der letzten Serie, der ersten Ausschreibung mit Berücksichtigung der Energiekosten, wurde allein durch ein anderes Grundsystem – sog. Barebones bei ansonsten gleicher Hardwareausstattung (RAM, Fest-

platten, ...) und völlig identischer Rechenleistung – eine Stromeinsparung von rund 20 % gemessen!

Die Abbildungen 5a bis 5c zeigen Rechenleistung, Stromaufnahme und Effizienz verschiedener Rechnergenerationen im GridKa.





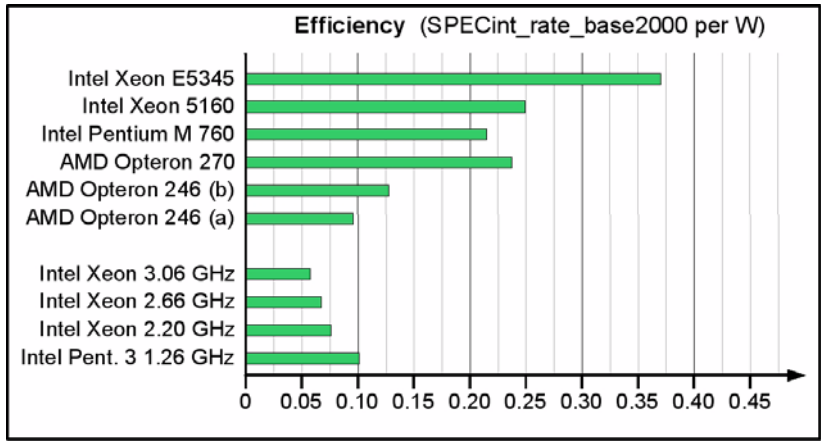


Abb. 5a-c: Rechenleistung (gemessen in SPECint_base2000), Stromaufnahme und Effizienz verschiedener Generationen von Clustersystemen im GridKa

7. Fazit

Der Aufbau des Grid-Rechenzentrums GridKa war in der Anfangszeit geprägt durch Engpässe vor allem im Bereich der Kühlung. Durch die Einführung der wassergekühlten Rechnerschränke – die im GridKa weltweit zum ersten Mal eingesetzt wurden – sowie durch gezielte Suche nach stromsparenden Clustersystemen mit entsprechender Gestaltung der Ausschreibungsbedingungen konnten diese Engpässe überwunden und gleichzeitig natürlich eine Senkung von Energieverbrauch und -kosten erzielt werden.

Die Ergebnisse unserer Rechenleistungs- und Verbrauchsmessungen sind auf den Seiten http://hepix.caspur.it/processors/ der High Energy Physics UNIX Interest Group (HEPiX) zusammengestellt und werden – gemeinsam mit weiteren Projektpartnern – ständig aktualisiert.

Anhang – Hardware-Übersicht

Die in den Abbildungen dargestellten Messungen (Benchmarks, Stromaufnahme) erfolgten an diesen Systemen:

- **Intel Xeon E5345** (2,33 GHz quad-core, 2x):
  Barebone: Supermicro CSE-812L-520CB, Mainboard: Supermicro X7DBE,
  RAM: 16 GB DDR2-677, Festplatte: 2 IDE
- **Intel Xeon 5160** (3,0 GHz dual-core, 2x):
  Barebone: Intel SR1530CL, Mainboard: Intel S5000VCL,
  RAM: 6 GB DDR2-677, Festplatte: SATA
- **Intel Pentium M 760** (2,0 GHz, 1x):
  Mainboard: AOpen i915GMm-HFS,
  RAM: 1 GB DDR2-533, Festplatte: IDE
- **AMD Opteron 270** (2,0 GHz dual-core, 2x):
  Barebone: MSI-9245-100, Mainboard: MSI K1-1000D with BMC,
  RAM: 4 GB DDR-400, Festplatte: IDE
- **AMD Opteron 246** (2,0 GHz single-core, 2x):
  (a) Barebone: Tyan Transport GX28, Mainboard: Tyan S2882,
  RAM: 2 GB DDR-333, Festplatte: IDE
  (b) Barebone: MSI-9245, Mainboard: MSI-9145 with BMC,
  RAM: 2 GB DDR-400, Festplatte: IDE
- **Intel Xeon 2,66 GHz und 3,06 GHz** (2x):
  Mainboard: TYAN Tiger i7501 S2723GN, HyperThreading ausgeschaltet,
  RAM: 1 GB DDR-266, Festplatte: IDE
- **Intel Xeon 2,2 GHz** (2x):
  Mainboard: TYAN Tiger i7500 S2720GN, HyperThreading ausgeschaltet,
  RAM: 1 GB DDR-200, Festplatte: IDE
- **Intel Pentium 3, 1,26 GHz** (2x):
  Mainboard: TYAN Thunder LE-T S2518,
  RAM: 1 GB SD-133, Festplatte: IDE

Zielgenaue Verteilung, Konfiguration und Verwaltung von Software in mobilen heterogenen IT-Umgebungen – eine Manöverkritik

Bertram Smolny, Mario Gzuk

Max-Planck-Institut für Biogeochemie, Jena

Zusammenfassung

Die Anwender werden bis 2010 das Zepter von den IT-Verantwortlichen übernehmen. Sie werden über mehr als die Hälfte aller Software-, Hardware- und Service-Erwerbungen selbst bestimmen. Das schreibt Gartner in einer aktuellen Studie [1]. Welche Probleme sich daraus ableiten und welche Maßnahmen seitens der IT-Verantwortlichen dazu anstehen, soll der folgende Artikel auch unter dem Aspekt der Manöverkritik des Beitrages zum Berichtsband zum 23. DV-Treffen [23] und zum Workshop UA-GUI beim 24. DV-Treffen beleuchten.

1. Motivation

„Leben heißt sich verändern, eigentlich eine banale Aussage, aber man vergisst sie immer wieder“. [11]

Wer arbeitet mit welcher Software?

Wer nimmt welche Lizenzen in Anspruch?

Wer hat zuletzt Änderungen am Rechner vorgenommen?

Dieses sind einige der Fragen, mit denen sich die IT-Verantwortlichen mit der Einführung der Kosten-Leistungs-Rechnung in der MPG beschäftigen mussten; eine Antwort darauf verursacht bis heute eine Menge Arbeit, hatte man keine Werkzeuge zur Hand, die einem das erleichtern können. In [7] wurde aus diesem Grund eine Palette von Werkzeugen vorgestellt, die diese Fragen umfassend lösen können und die bis heute weiterentwickelt werden. Auch aus dem Blickwinkel der Entwickler soll diese Arbeit hinterfragt werden.

Die IT-Infrastruktur eines Max-Planck-Instituts wird auch heute zumeist von einer internen IT-Gruppe betreut, die je nach Lage aus einem bis zu mehreren Dutzend Teil- oder Vollzeitbeschäftigten bestehen kann. Grundlage dieser Arbeit ist dabei meistens ein Betriebskonzept, z. B. [2].

In diesem Konzept wird bisher davon ausgegangen, dass die zu betreuenden Rechner auf dem Labor- oder Schreibtisch stehen, eine interne IP-Adresse besitzen und dass ein IT-Administrator zu diesem Rechner physikalischen Zugang hat.

Nun lag der Marktanteil von Desktop-PCs in 2007 bei noch ca. 50 % – er wird sich weiter abschwächen. Das hat mehrere Ursachen, wobei mit a) der ultramobile Benutzer und b) die gewachsene Leistungsfähigkeit der mobilen Rechner die beiden wichtigsten zu nennen wären.

Dabei sagen die Prognosen der Marktforscher, dass auch bald die Notebooks auf dem Schreibtisch stehen bleiben – ultraportable Rechner für die Jackentasche sind schon da, sie werden funktionell immer weiter aufgebohrt.[1]

Und die Prognosen sagen weiter, dass für diese Geräte die Anwender bis 2010 das Zepter von den IT-Verantwortlichen übernehmen werden. Sie werden über mehr als die Hälfte aller Software-, Hardware- und Service-Erwerbungen selbst bestimmen (wollen) [1].

Angefeuert wird dies vor allem dadurch, dass Wissenschaftler wie Mitarbeiter diese auch privat nutzen (wollen).

1. Das hat möglicherweise auch damit zu tun, dass neuerdings die „großen“ Technologien nicht mehr aus den etablierten Firmen wie IBM, SUN oder Miscosoft kommen, sondern das der Markt der Consumer-Produkte diese Big-Player vor sich her treibt nach dem Motto: „Besser schnell als groß“.

Dabei ist „always-on“ nicht nur Trend, sondern wird Realität. Das Ausbau der WIFI-Netze, deren Bandbreite sich ebenfalls vergrößert, schreitet voran, und Technologien wie Google-Gears [21] werden eine asymmetrische Arbeit ermöglichen zu Zeiten, in denen mal keine Netzwerkverbindung zur Verfügung steht, mit dem langfristigen Ziel, on- und offline ununterscheidbar zu machen

Ebenso wird Speicherplatz keine Rolle mehr spielen; Microsoft-Chef Ballmer sagt die fünfte Computerrevolution auf Basis von „quasi unendlichem Speicherplatz“ [3] voraus. Und das hat auch handfeste ökonomische Gründe: Kostet ein Gigabyte heute ca. 50 Cent, so hätte man vor 25 Jahren noch 1,8 Millionen Euro dafür bezahlt. Geht man nun davon aus, dass sich diese Entwicklung in den nächsten 25 Jahren (nur) linear fortsetzt, so könnte man annehmen, dass sich dann das gesamte Wissen der Menschheit auf einem Gerät speichern lässt, das nicht teurer ist als ein iPod®. [4]

Die Fragen ändern sich also und haben enorme Konsequenzen für die IT-Abteilungen, von Security über Datensicherheit bis zum Problem Rollout und Pflege dieser (mobilen) Strukturen; dabei ist die Konvergenz der Netze, Hardware, Betriebssysteme und Software noch gar nicht näher einkalkuliert. [5]

Durch das immer breiter werdende Spektrum wird aber auch immer mehr Zeit benötigt, diese Geräte zu warten, zu aktualisieren, Probleme zu beheben etc. Obwohl sich die Komplexität in Hard- und Software in dieser Zeit vervielfacht hat, ist die Zahl der IT-Mitarbeiter nicht adäquat mitgewachsen.

Nüchtern betrachtet besteht die Gefahr, dass das eigentliche Wissen nur noch auf Wenige verteilt sein wird. Der Begriff „Wissen ist Macht“ bekommt eine neue Gewichtung.

2. „Kreative Individualisten“

Mobile Computer nehmen so stark zu, dass das Wachstum der Zunahme wohl das eigentliche Problem ist – wie kann man den Spagat zwischen der geforderten einheitlichen Pflege der Systeme und Benutzern, die sich in der Mehrzahl als „Kreative Individualisten“ verstehen, hinbekommen?[2]

2. Die Schnelligkeit der Änderungen macht vielen zu schaffen; sie merken nicht, dass Technologie schon längst wieder obsolet geworden ist, in dem Moment, wo sie mit großem Brimborium in die Produktion übernommen wurde, oder sie hoffen unter den wenigen zu sein, die bleiben.

„Kreative Individualisten“ („KI“) – das ist ja genau die Zielgruppe von Herstellern wie z. B. Apple; so sind und verstehen sich auch die meisten Wissenschaftler: kreativ und individuell.

Auf Grund dieses Fakts und der Möglichkeit, dass Apple neben innovativen Lösungen[3], auch einen „Hippness-Faktor“ in die mobilen Geräte einbaut, ist genau dies auch ein Teil des Problems: Der Hersteller will oder kann sich nicht mit den „Niederungen“ des Infrastrukturmanagements herumschlagen, der Endnutzer allein ist ihm lieber.

Für ihn sind so genannte nonfunktionale Eigenschaften wie attraktives Äußeres der Geräte, einfachere Bedienbarkeit, Kapazität oder – geben wir es ruhig zu – ein „Coolness-Faktor“ mehr von Bedeutung als eine Infrastruktur zum Support für Firmenkunden.

Die Bereitstellung dieser Infrastruktur ist nicht attraktiv – man hätte es dann mit einen „Enterprise-Markt“ zu tun, dessen Teilnehmer bei großen Stückzahlen auch eine gewisse Marktmacht darstellen würden und vom Hersteller die Einhaltung von Standards verlangen könnten (siehe z. B. das standardisierte Protokoll H.323 für Video-Conferencing etc.); aber man fühlt sich eher dem Shareholder verpflichtet – der Schwenk zur Life-Style-Company hat den Aktienkurs von Apple gepusht.

In [1] wird übrigens eine Verdopplung des Marktanteils von Apple bis 2011 vorausgesagt, nicht zuletzt ist dabei die Rolle der oben genannten Faktoren nicht unbedeutend.

Durch eine vermehrte Beschaffung von mobilen Endgeräten angetrieben durch die „Kreativen Individualisten“ kommt man aber genau in das Problem: Man braucht ein Infrastrukturkonzept, um 50, 100 oder 200 mobile (heterogene) Endgeräte pflegen zu können – einzeln ist das sicher kein Thema, auch nicht bis zu einer Anzahl von mehreren Dutzend, aber darüber hinaus wird das schwer, mit einem begrenzten Personal einen Überblick über den Stand der mobilen, wenn auch „hippen“ Rechner zu behalten.[4]

3. Z. B. „Spotlight“ genannte Indizierung der gesamten Nutzerdaten, um eine Suche nach Inhalten mit hoher Genauigkeit zu gewährleisten – Benutzer anderer Plattformen mailen sich ihre Dokumente selbst zu, um durch den Index des Mailclienten genau diesen Effekt zu erreichen, was wiederum zu sehr großen Datenbanken im Mailserver und daraus abgeleiteten Problemen führt.

4. So gelingt es vielen bis heute nicht, auf Knopfdruck in einem Report die IT-Rechte aller internen und externen Mitarbeiter exakt darzustellen.

Ein weiteres Problem ist das der dezentralen Beschaffung: die Diversität der Hardware-Basis, mit der jede IT in der Forschung umgehen muss, resultiert auch aus den dezentralen Budgets, aus der Möglichkeit, via Drittmittel Dinge tun zu können, die sonst nicht möglich wären. Da ist alles dabei: Notebooks, Portables, Smart-Phones, Navigationsgeräte mit PC-Eigenschaften und und und.

Als Programmierer und Anwender eines Konzepts zur Einbindung all dieser relevanten, institutsweit verfügbaren Informationen kommt man auf die Frage: Wie passt unser bisheriges Konzept des „unattended setup“ und des UA-GUI [25] in diese Entwicklung? Welche Konsequenzen hat das für dessen Existenz?

3. Industriestandards

Der Ansatz, Infrastruktur nur mit „Industriestandards“ zu betreiben, ist sicher in vielen Fällen verlockend und die angestrebte Lösung, bietet sie doch alle Vorteile einer „Monokultur“, mit der sich Prozesse, die stark standardisierbar sind, abbilden lassen.

Softwareverteilung, Inventarisierung von Hard- und Software, Installation und Migration von Betriebssystemen, IT-Sicherheit, Fernwartung und Disaster-Recovery sind heute in diesem Kontext mit einer Produktfamilie möglich.

Das gibt es alles mehr oder weniger komfortabel und mehr oder weniger funktionabel und ist meist für den „Industriestandard“ verfügbar.

Aber bildet das die Wirklichkeit ab?

Ein Max-Planck-Institut ist kein statischer Wissenschaftsbetrieb; heute kommt jeder Kunde (Nutzer, „KI“) in ein Institut mit einem „digitalen Vorleben“, das so vielfältig ist wie seine Wissenschaft, muss mit den verschiedensten Applikationen arbeiten, die verschiedenste Datenstrukturen in den verschiedensten Formaten erzeugen. Kann man das ignorieren resp. lässt sich das standardisieren? Man sollte sich an der Wirklichkeit orientieren und der Internationalisierung und dem daraus folgendem digitalen Vorleben Rechnung tragen. Demographisch bedingte Heterogenität der Benutzer (Kunden, „KI“) bedingt eine höhere soziale Kompetenz mit deren Anforderungen – es gibt einfach keine einfachen Antworten, das gerade macht die MPG ja so attraktiv für qualifiziertes Personal.[5]

Nach Evard [6] ist der Lebenszyklus eines Computers stark bestimmt durch das Schwingen zwischen Neuinstallation des Betriebssystems und einem

unbestimmtem Zustand. Um diesen Zustand entgegen zu wirken, werden vielerorts regelmäßig Neuinstallationen flächendeckend durchgeführt. Das soll heute aber mit Hilfe von Technologien erfolgen, die möglichst Automatisierung bieten, weil IT-Leistung ja teure Arbeitszeit ist.

Automatische Installation heißt aber auch im erweiterten Sinne, dass, um Fehler durch menschliche Schwächen zu vermeiden, alle notwendigen Entscheidungen im Vorfeld so getroffen worden sind, dass auch bei unterschiedlichen Personen das Installationsergebnis vollkommen identisch ist, dass im Nachhinein keine Korrekturen per Hand mehr erforderlich sind und dass alle Arbeitsschritte unabhängig vom Bearbeiter protokolliert sind.

Am Markt sind derzeit Produkte zu finden, die bei der Lösung dieser Probleme in geeigneter Weise helfend zur Seite stehen. Allen gemein ist sehr häufig die ausschließliche Unterstützung einer einzigen Betriebssystemumgebung. So sind beispielsweise Produkte wie enteos NetInstall oder der Microsoft Systems Management Server in homogenen Umgebungen mit Desktop-Rechnern sehr leistungsstark. Hat man nebenher aber auch, wie in Forschungsumgebungen üblich, MAC- und Linux-Systeme, und diese noch in mobiler Form im Einsatz, so bedarf es schnell weiterer Lösungen, um die Problematik des mobilen Nutzers genügend zu berücksichtigen, ohne den Verlockungen der „Featureritis“ zu erliegen.

Man kann sich anstrengen wie man will, als Konsequenz erhält man zu seiner heterogenen IT-Installation eine heterogene Administration, die für jede Betriebssystemumgebung in der Regel auch einen eigenen Workflow verlangt. [7]

Der Trend zu einer Dezentralisierung der Rechenkapazität durch den verstärkten Einsatz von mobilen Rechnern wird voraussichtlich den Betreuungsaufwand pro Rechner weiter erhöhen, da – bei gleicher Rechenkapazität in der Summe – wenige zentrale Rechner einfacher zu warten sind als eine Vielzahl von Rechnern an (mobilen) Arbeitsplätzen. Diese Entwicklung kann für einen ortsfesten Office-Arbeitsplatz evtl. mit Terminal-Servern o. ä. aufgefangen werden. Für mobile Rechner hingegen ist mit einem deutlich erhöhten Betreuungsaufwand zu rechnen: Die Vielfalt an Hardware und die nicht ständige Erreichbarkeit des Rechners für den Administrator führt zu mehr Schulungsbedarf und aufwendigen Abstimmungen mit den Benutzern.

---

5. In der jährlichen Umfrage nach einem attraktiven Arbeitsplatz für IT-Absolventen hat sich die MPG im vergangenen Jahr von Platz 9 auf Platz 18 bewegt. [13]

Infrastruktur ausschließlich nach „Industriestandards“ zu betreiben, ist also auch nur scheinbar möglich.

4. Trend „Cloud Computing“

Kostengünstige Breitband-Verbindungen verändern das Web. Es entwickelt sich zu einer „riesigen Plattform der Zwei-Wege-Kommunikation“. Mail, Instant Messaging, Kalender, mobile Sprach- und Videofunktionen und Social-Network-Websites werden sowohl privat als auch am Arbeitsplatz genutzt. Die klassischen Mobilfunkanbieter bangen um ihren Marktanteil, weil sich mittels Flatrate und VOIP ein völlig anderes Benutzerverhalten einstellen wird. Web 2.0 ist angekommen; laut Forrester [19] nutzen 72 Prozent der IT-Abteilungen irgendeine Form von Web 2.0-Technologie. Kantel beschreibt in [20] die Möglichkeit eines „grassroots-web“, in der Gruppen und Organisationen ohne grossen Aufwand miteinander kommunizieren können.

Als Beispiele gibt er dabei so etwas wie *flickr* oder *sevenload* an, die innerhalb der MPG als Kommunikationsplattformen aufgezogen, nicht nur die IT-Abteilungen beflügeln würden, aber, so sie bei den RZs angesiedelt würden, die Möglichkeit des lebenslangen Zugriffs auf die Publikation ermöglichen müssten, sonst würden sie nicht angenommen. Als größtes Hemmnis wird dabei das Problem des Datenschutzes fokussiert: Mit welchen Möglichkeiten ist man ausgestattet, die Daten, die außer Haus liegen, auch zu kontrollieren?

Ein anderer Vorschlag in die gleiche Richtung ist SAAS (Software as a Service) [8] – eine Technologie, wie sie z. B. Google mit Google-Apps [9] vorantreibt. Dabei soll die Anwendung im Mittelpunkt stehen; CPU, Betriebssystem und Patchlevel sind völlig egal: Es soll nur ein Browser erforderlich sein, mit dem die Anwendung intuitiv bedienbar ist – die offene Schnittstelle Browser wird zum Non-Plus-Ultra[6].

Vorteil dieser Art von Lösung ist die Möglichkeit, unabhängig vom Endbenutzer verschiedene SW-Stände auszurollen. Man muss also keine administrativen Tätigkeiten mehr am Endgerät vornehmen und kann, je nach Finanzlage, entsprechende SW-Schichten anbieten. Nützlich kann das in Organisationen eingesetzt werden, um z. B. Microsoft Office in rudimentären Formen zu substituieren und dabei ohne eine eigene MS-Umgebung auszukommen.

6. Anmerkung: Ob sich alle bei der Entwicklung ihres Browsers an die RFCs halten, sei hier mal nicht näher beleuchtet [26]

Die vielzitierten Kosteneinsparungen durch Nutzung von SAAS werden mit zunehmender Größe des Unternehmens kleiner – das käme dem Harnack-Prinzip entgegen, und besonders bei kolloborativem Arbeiten über Institutsgrenzen hinweg sind die Vorteile klar zu erkennen.[7]

Nachteil ist: Das funktioniert bisher nicht alles so browser-unabhängig wie versprochen (z .B. verlangt eine Einbindung von MS Office in „Lotus Quickr2 zwingend Active-X-Controls) und nur bei ungestörtem Netzzugang.

Des weiteren liegen alle Daten „außer Haus“, was bei sensitiven Einrichtungen einem Tabubruch gleichkommt und auch sonst bei unternehmenskritischen Daten nicht akzeptabel ist; Google wertet die Informationen gezielt aus, um entsprechende Werbung schalten zu können [23]. Erschwerend kommt eine Problematik hinzu, die sich mit einer „Verschärfung der Gefährdungslage im Internet“ beschreiben ließe [16].

Ein weiterer hemmender Faktor ist, dass mit dieser Art von Service das bisher (erfolgreiche) Lizenzmodell von Microsoft ausgehebelt werden kann (z. B. keine lokalen Office-Lizenzen mehr), was zu einem nicht unerheblichen Widerstand in diesem Marktsegment auch von Drittanbietern führen wird. Die Kundenbindung wird damit geringer, aber die Anbieter erhalten auch spezielle Daten über das Kundenverhalten, die sie auswerten können.

Aber möglicherweise entwickelt sich das Verhältnis von SAAS zu herkömmlicher Software genauso, wie seinerzeit das Verhältnis von Kleinanzeigen zu Online-Auktionen und von gedruckten Lexika zu Wikipedia.

5. „Menschen hassen Veränderungen“ [12]

Wird Vielfalt nicht als Bedrohung verstanden sondern als Zukunftschance, dann kann man damit auch besser umgehen. Die betriebliche und damit auch die soziale Realität ist wesentlich diverser, als im Allgemeinen angenommen wird – und es ist geradezu eine Sisyphusarbeit, der Sukzession entgegen zu wirken.

Dabei sind Schlagworte wie „Grüne IT“ bisher nichts als Mogelpackungen, solange auch Themen wie Nachhaltigkeit nicht wirklich Beachtung finden .

Zum Thema „Ökologie“: Organismen versuchen immer wieder, ein stabiles Lebensumfeld zu erreichen; das scheint ihnen in ihrer DNA mitgegeben

7. Was wir unter dem Begriff „wiki“ kennen, ist eine Untermenge, weil hier ja bestimmte programmiertechnische Kenntnisse vorhanden sein müssen, um z. B. Tabellen dazustellen

worden zu sein. Die Angst vor Veränderungen, denen Menschen unterliegen können, macht sie unruhig: Veränderung bedeutet Gefahr, Gefahr, mehr Energie aufwenden zu müssen, um zu überleben. Nicht in jedem Jahr sind die (klimatischen) Bedingungen gleich gut, um z. B. den Bauern gleiche oder bessere Erträge zu ermöglichen. Man versucht deshalb, sich auf eine Kulturpflanze zu konzentrieren, die wiederum aber auch sensibel für nur eine Art von Schädling ist, der das Resultat der Ernte blitzartig in Frage stellen kann.

Verhält sich ein „Farmer“, der ein „Ökosystem Rechnernetz“ zu verantworten hat, anders?

Man versucht, sich auf eine Lösung zu fokussieren, kann Energie sparen, lebt scheinbar sicher, weil „sichere Lebensumstände“ vorhanden sind, lebt aber in der Angst vor dem „einen Schädling“ und in der Abhängigkeit des einen Herstellers. Sozialdruck („Die anderen machen das auch.“) verstärkt diesen Aspekt noch – angestrebte und erreichte Stabilität sind nur scheinbar im Gleichgewicht.

Also doch alles der Intelligenz der „Kreativen Individualisten“ („KI“) [sic!] überlassen ? Sämtliche Systeme, die dem zweiten Hauptsatz der Wärmelehre entgegen wirken, werden scheitern.

Die Ideen, mittels Simplifizierung der Probleme Herr zu werden, müssen wohl als gescheitert betrachtet werden. Das fängt bei der Steuer an und hört bei Homogenisierung von Strukturen im IT-Bereich auf – es versuchen sich auch Wissenschaftler daran, die das große Ganze im Auge haben und sind nur mittelmäßig erfolgreich [10].

Dann aber muss man nicht nur die Ansprüche an Datenintegrität und Revisionierbarkeit herunter schrauben, dann sind die Direktiven von Präsidenten geradezu Makulatur.

6. Offene Standards

Immer wieder findet auch das so genannte „Utility Computing“ in der Literatur Erwähnung. Dieser Begriff leitet sich ab aus der Industrie der öffentlichen Versorgungsbetriebe, der „Public-Utility-Industrie“ [18].

Direkt vom Anbieter beziehbare IT-Ressourcen ähnlich wie Wasser und Strom bereitzustellen, die aus einem Verbund von Rechnern, die netzartig zusammenhängen und gemeinsam Prozesse abarbeiten (Cloud, Grid), gespeist werden, sollen Synergieeffekte ermöglichen, die zur Folge haben, dass nur die Ressourcen abgefragt werden, die auch benötigt werden.

Obwohl der Grundgedanke des Utility-Computings simpel erscheint, ist die Umsetzung viel komplexer als beispielsweise die Bereitstellung von Trinkwasser, da eben die Anwendungen auch viel komplexer sind – offene Schnittstellen sind aber im hart umkämpften Markt kein Mittel, den Kunden zu binden. Mit diesem Widerspruch muss Utility Computing fertig werden [24] [26].

Das wohl breiteste Angebot im Bereich „Utility-Computing“ bietet derzeit wohl Amazon.com - mit Diensten wie „Elastic Compute Cloud“ (EC2) oder „Simple Storage Service“ (S3), dank denen Kunden auf die „quasi unbegrenzten“ Rechen- und Bandbreitenkapazitäten des online-Anbieters zurückgreifen können, die dieser ohnehin für sein Vertriebssystem vorhalten muss. Mit „SimpleDB“ wurde außerdem eine große Datenbank nach dem gleichen „Pay-as-you-go“-Prinzip aufgesetzt.

Während für die Festplatte spricht, dass man die dort gespeicherten Informationen aus Gründen des Datenschutzes besser unter Kontrolle hat, spricht für den online-Speicher die nur an die Netzverfügbarkeit gebundene Verfügbarkeit. Wenn das aber nicht applikationsgebunden passieren muss, neigt sich die Waage zu Letzterem.

Ob wir uns wirklich im Zeitalter der serverlosen Internetfirmen befinden, die einfach vom Browser aus gesteuert werden, beantwortet Amazon-Technikchef Werner Vogels: Das sei längst Realität. Beispiele gäbe es genug [15]. Wie diese Beispiele mit den Firmengeheimnissen umgehen, wird nicht erläutert. Carr sagt aber in [26] klar den Siegeszug dieser Industrie voraus.

7. Diversität leben

Organisationen sind dann stark, wenn zwischen ihnen ein offener Informationsaustausch stattfinden kann – nun ist die MPG deshalb stark, weil so viele verschiedene interkulturelle Einflüsse hier zusammenwirken können, die auch ein „digitales“ Vorleben haben – dieses zu kappen und jedem Neuankömmling („KI“) bei Null beginnen zu lassen, in dem man eine Technologie vorschreibt, ist verfänglich.

Die Entwicklung der Informationstechnik bewegt sich zunehmend in Richtung der Inhalte. Klar ist, dass ohne Normung nichts läuft, aber diese muss unbedingt mit offenen Schnittstellen einhergehen, ohne die Fessel der Herstellerbindung, denn Hersteller lieben Bindungen, speziell die der Kunden an ihre Produkte. Zurzeit ist klar ein Rückfall in alte Rollen zu beobachten. Der Anwender läuft Gefahr, nicht mehr Herr seiner Entscheidungen zu sein und in immer komplexere Abhängigkeiten zu geraten. Dabei wird ihm aber Entscheidungsfreiheit vorgegaukelt.

Die zentrale Schlussfolgerung, die sich daraus ableitet: Kern-Infrastrukturen gehören nicht in den Besitz eines Herstellers. Es gilt, die Vor- und Nachteile über die ganze Lebensdauer der Lösung abwägen. Häufig ist die herstellerspezifische Lösung einfacher für den Einstieg, am Ende wird aber ein gewaltiger Preis mit hoher Komplexität bezahlt (exit-costs).

Verstehen, wo das Problem liegt, wie eine Technologie arbeitet, systematisch das notwendige Wissen für offene Architekturen aufbauen und den Unterschied zwischen den herstellerspezifischen und den offenen Lösungen systematisch analysieren, das wird dauerhaft Vorteile für die IT-Struktur der MPG bringen.

Offenheit schafft auf Dauer immer den maximalen Mehrwert. Ein gutes Beispiel ist der SIP-Standard für IP-Telefonie. Damit dies aber über alle Grenzen hinaus funktioniert, ist die Nutzung eines offenen, internationalen Standards ein absolutes Muss. Wer auf die Vorteile, per Drag und Drop Dokumente, Bilder, Videos und Präsentationen zwischen verschiedenen Plattformen austauschen zu können, durch den Kauf einer herstellerspezifischen Telefonie-Lösung verzichtet, der muss einen sehr guten Grund haben. SIP mag für den Einstieg mit einer Reihe von Schwierigkeiten versehen sein, aber die Perspektive ist mehr als überzeugend.

Wir laufen Gefahr, uns mehr und mehr von den Herstellern einlullen zu lassen. Der Wegfall kritischer Medien, die massive Marketing-Macht führender Hersteller und die scheinbare Normalität des Ganzen haben uns möglicherweise abstumpfen lassen. Dabei gibt es fast immer Alternativen. Der systematische Aufbau von Wissen über offene Lösungen und das bewusste Abwägen, was für meine Institution in der geplanten Lebensdauer eines Produkts der bessere Weg ist, wird langfristig zum Erfolg führen

Bei all diesen aufgeworfenen Fragen ist eine Antwort richtig: herstellerspezifische Lösungen ohne offene Schnittstellen werden in die Sackgasse führen – man muss sich nur die *„exit-costs“* vorrechnen lassen.

8. Ausblick

Komplexe Netzwerkstrukturen und aufwendige Installationen auf mobilen Klienten fordern einen hohen Aufwand; hier hilft die im Max-Planck-Institut für Biogeochemie entwickelte UA-GUI r2 [25] mit seinen offenen Schnittstellen und seinen bewährten Technologien. Bei der Weiterentwicklung muss darauf Wert gelegt werden, die Möglichkeiten einer automatisierten Installation und Inventur auch für mobile Rechner so zu erweitern, dass Prozesse nach wie vor automatisiert ablaufen können, damit der IT-Verantwortliche weiterhin die Übersicht behalten kann. Auf Grund der oben skizzierten

anstehenden Paradigmenwechsel wird sich die Rolle der IT-Abteilungen an den Instituten mehr und mehr in Richtung der wissenschaftlichen IT verschieben; die Anforderungen des mobilen Wissenschaftlers werden komplexer und weiter steigen. Ob die Personaldecke adäquat mitwächst, bleibt ein Rätsel.

Alle, die UA-GUI einsetzen, sind auf diesen Schritt schon vorbereitet.

Literatur

[1] Gartner: „Highlights Key Predictions for IT Organisations and Users in 2008 and Beyond“ [http://www.gartner.com/it/page.jsp?id=593207]

[2] Bertram Smolny: „Betriebskonzept für eine wissenschaftliche Datenverarbeitung“ [http://www.bgc-jena.mpg.de/~bsmolny/ITS/Betriebskonzept.html]

[3] heise online: „Ballmer sagt fünfte, sechste Computerrevolution voraus“ [http://www.heise.de/newsticker/meldung/print/104421]

[4] Ross O. Storey, CIO Asia: „The world in an iPod by 2020“, Google [http://www.macworld.co.uk/digitallifestyle/news/index.cfm?RSS&NewsID=19932]

[5] Wikipedia: „Next_Generation_Network“ [http://de.wikipedia.org/wiki/Next_Generation_Network]

[6] Rémy Evard: An analysis of unix system configuration. 11th Systems Administration Conference (LISA ’97), pages 179–194, 1997

[7] Bertram Smolny u. a.: „Zielgenaue Verteilung, Konfiguration und Verwaltung von Software in heterogenen IT-Umgebungen“. GWDG-Bericht Nr. 71, S. 103ff

[8] http://de.wikipedia.org/wiki/Software_as_a_Service

[9] http://www.google.com/a/?hl=de

[10] Jason H. Steffen: „Optimal boarding method for airline passengers“ [http://arxiv.org/PS_cache/arxiv/pdf/0802/0802.0733v1.pdf]

[11] Hansjörg Küster: „Das ist Ökologie“. Beck, 2005, ISBN 3406534635

[12] Tom DeMarco: „Wien wartet auf Dich!“. Hanser Fachbuch, 1999, ISBN 3446212779

[13]Das Deutsche Absolventenbarometer 2007 – IT Edition [http://www.trendence.com/fileadmin/pdf/trendence_DAB07__IT_Edition.pdf]

[14]Richard Sietmann: UMTS und seine Nachfolger [http://www.heise.de/mobil/Breitband-Zukunft-im-Mobilfunk--/artikel/65778]

[15]http://www.allthingsdistributed.com/

[16]BSI-Lagebericht IT-Sicherheit 2007: [http://www.bsi.bund.de/literat/lagebericht/lagebericht2007.pdf]

[17]Pär Ström: „Die Überwachungsmafia. Das gute Geschäft mit unseren Daten“. Hanser, 2005, ISBN 3446229809

[18]Nicholas G. Carr: „Does IT Matter? Information Technology and the Corrosion of Competitive Advantage“. Harvard, 2004, ISBN 1591394449

[19]Matthew Brown, Kyle McNabb, Rob Koplowitz: „Embrace The Risks And Rewards Of Technology Populism“ [http://www.forrester.com/Research/Document/Excerpt/0,7211,44664,00.html]

[20]Jörg Kantel: „Web 2.0: Werkzeuge für die Wissenschaft“, GWDG-Bericht Nr. 71

[21]Wikipedia: http://de.wikipedia.org/wiki/Gears

[22]Watzlawik: „Wie wirklich ist die Wirklichkeit?: Wahn, Täuschung, Verstehen“. Piper ,2005, ISBN 3492243193

[23]Gerald Reischl: „Die Google-Falle“. Ueberreuter 2008, ISBN 3800073234

[24]Nocholas G. Carr: „The Big Switch. Rewiring the world. From Edison to Google“, B&T 2008, ISBN 0393062287

[25]http://unattended-gui.sourceforge.net/

[26]Michael Clever: „Der Browser-Krieg – eine wettbewerbsstrategische Analyse“. Grin, 2002, ISBN 363826663X

Sichere Gästenetze

Holger Beck

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

1. Einleitung

Die herausragende Position der Max-Planck-Institute in der Forschung erfordert einen nationalen und internationalen Austausch, durch den kontinuierlich Gäste in den Instituten anwesend sind. Zu optimalen Arbeitsbedingungen für Gäste gehört auch der Zugang zu internen und externen Netzen.

Häufig bringen Gäste ihre eigene Arbeitsumgebung auf einem eigenen Computer mit und wollen diese auch im Max-Planck-Institut nutzen.

Die Sicherheitsrisiken für vernetzte IT-Systeme wuchsen in den vergangenen Jahren immer weiter an. Zur Gewährleistung einer hinreichenden IT-Sicherheit wurden die Netze der Max-Planck-Institute durch Sicherheitssysteme[1] gegen Angriffe aus dem Internet geschützt.

1. Sicherheitssysteme sind vor allem Firewalls. Darunter fallen aber auch Intrusion-Prevention-Systeme (IPS), Intrusion-Detection-Systeme (IDS), VPN-Gateways u a.

Die Anbindung von Gästerechnern an die internen Netze birgt das Risiko des Einschleppens von Schadsoftware vorbei an allen Sicherheitssystemen. Gästerechner sollten daher nur nach einer sorgfältigen Sicherheitsprüfung an interne Netze angeschlossen werden.

Sollte eine solche Prüfung nicht möglich oder nicht erwünscht sein, so sollten solche ungeprüften und nicht an die Sicherheitsregeln des Instituts angepassten Rechner nur an ein spezielles Gästenetz angeschlossen werden.

2. Implementieren von Gästenetzen

2.1 Grundprinzipien

Für den Anschluss von Gästerechnern ist ein separater Netzbereich zu schaffen. Von diesem Gästenetz aus dürfen **Zugriffe auf das interne Netz nur über die Sicherheitssysteme** des Instituts möglich sein. Das Gästenetz ist damit logisch ein externes Netz analog dem gesamten Internet, sodass in diesem Netz keine besonderen Anforderungen an dort betriebene Rechner gestellt werden müssen.

Soweit man Gästen **Zugang zu speziellen Diensten im internen Netz** gewähren will, können auf den Sicherheitssystemen am Übergang zum internen Netz entsprechende Regeln geschaltet werden. Dabei ist genau abzuwägen, ob die damit verbundenen Risiken übernommen werden sollen. In vielen Fällen wird das Risiko voraussichtlich vertretbar sein, denn in der Regel werden die Systeme, die solche Dienste erbringen, vergleichsweise hohen Sicherheitsanforderungen genügen und relativ robust gegenüber möglichen Angriffen sein.

Aus dem Gästenetz kann ein weitgehend unbegrenzter **Zugriff auf das Internet** eingerichtet werden. Allerdings sind Beschränkungen am Übergang zum Internet gegen Missbrauch – z. B. die Unterbindung von Tauschbörsen oder des Betriebs von Servern – oder zum Schutz der Gästerechner vor Angriffen aus dem Internet im Interesse des Instituts bzw. der Gäste zu empfehlen.

2.2 Technische Umsetzung

2.2.1 Trennung auf Netzwerkebene

Das Gästenetz muss als ein auf Netzwerkebene (Schicht 3 des OSI-Referenzmodells) eigenes Netz betrieben werden. Damit wird erzwungen, dass ein Übergang nur über die Sicherheitssysteme erfolgen kann. Die Anbindung dieses Netzes muss dann über einen eigenen Anschluss an Sicherheits-

systeme des Instituts, in der Regel die Firewall, erfolgen. Hier sind nötigenfalls Investitionen zur Bereitstellung einer zusätzlichen Schnittstelle erforderlich.

2.2.2 Trennung auf Linkebene

Ein physikalisch getrenntes Netz mit eigenen Netzwerkverteilern ist nicht praktikabel. Die Trennung des Gästenetzes von internen Netzen sollte daher in der Regel durch Bildung virtueller Netze (VLANs) in den Netzwerkverteilern realisiert werden. VLANs gewährleisten die notwendige Trennung der Netze. Die Netzwerkinfrastruktur aller Max-Planck-Institute sollte so modern sein, dass die Nutzung von VLANs technisch überall möglich ist.

Die Zuordnung einzelner Anschlüsse (Anschlussdosen in den Räumen oder Ports auf den Verteilern) zum VLAN des Gästenetzes kann auf unterschiedliche Weise erfolgen.

1. Statische VLAN-Konfiguration

Die technisch am wenigsten komplexe Art der Realisierung ist die statische Zuordnung bestimmter Ports der Verteiler zum Gästenetz-VLAN.

Um das Gästenetz dann an bestimmten Anschlussdosen zur Verfügung zu stellen, ist jeweils eine geeignete Rangierung im Verteiler notwendig. Solche Rangierungen können permanent oder bedarfsorientiert vorgenommen werden. Permanente Rangierungen werden in der Regel aus Kostengründen (Vorhaltung zusätzlicher Verteiler-Ports) nur in Bereichen vorgenommen, in denen regelmäßig Gästenetz-Zugänge benötigt werden.

Alternativ zum Umrangieren der Kabel kann das Gästenetz auch durch Umkonfigurieren der VLAN-Zuordnung auf den Verteilern unter Beibehaltung der Rangierung verfügbar gemacht werden.

Diese Lösung bietet den Nutzern und ihren Gästen eine technische saubere Möglichkeit zum Anschluss von Rechnern, die ein potenzielles Sicherheitsrisiko darstellen. Sie setzt aber die aktive Mitarbeit aller Nutzer voraus. Es werden mit dieser Lösung keine technischen Hürden eingerichtet, die einen versehentlichen oder absichtlichen Anschluss nicht erwünschter Rechner an das interne Netz verhindern. Jede freie oder vorübergehend frei gemachte Anschlussdose kann in der Praxis immer noch zum Anschluss beliebiger Rechner verwendet werden. Dieses Risiko könnte nur dann ausgeschlossen werden, wenn zusätzlich Restriktionen bezüglich erlaubter MAC-Adressen auf allen Ports im internen Netz aktiviert würden (Portsecurity). Neuere Netzverteiler stellen in der Regel ein solches Verfahren zur Verfügung. Die damit verbundene Administration ist jedoch aufwändig.

2. Dynamische VLAN-Konfiguration auf Basis von MAC-Adressen

Über die statischen Konfigurationen hinaus verfügen moderne Verteiler über Möglichkeiten zur dynamischen Zuordnung von Ports zu VLANs.

Eine dynamische VLAN-Zuordnung kann auf Basis der MAC-Adressen der Endgeräte erfolgen. Hier bieten Hersteller von Netzverteilern unterschiedliche Lösungen an. Teilweise basieren diese vollständig auf herstellerspezifischen Verfahren, teilweise setzten sie auf dem Standard IEEE 802.1x mit herstellerspezifischen Erweiterungen auf.

Eine solche Lösung ist daher nur mit einer bezüglich der Netzverteiler homogenen Infrastruktur umsetzbar.

Darüberhinaus ist die Erfassung und Verwaltung aller im internen Netz zugelassen Rechner und insbesondere deren MAC-Adressen notwendig – also ein relativ hoher Aufwand nötig.

Eine solche Lösung ist primär für eine zentral verwaltete und bezüglich der Rechneranschlüsse flexible Strukturierung des internen Netzes gedacht. Die Nutzung zum Implementieren eines Gästenetzes ist nur ein Abfallprodukt einer solchen Lösung, indem Rechner mit unbekannten MAC-Adressen automatisch einem Gästenetz zugeordnet werden.

Eine Umgehung der Schutzmaßnahmen ist hier nur möglich, wenn einem nicht zugelassenen Rechner gezielt eine zugelassene MAC-Adresse eingetragen wird. Das ist technisch möglich, setzt aber bewusstes Unterlaufen der Sicherheitsregeln und ein für Anwender überdurchschnittliches Know-how voraus.

3. Dynamische VLAN-Konfiguration auf Basis von Benutzer-Authentifizierung

Die meisten neueren Netzwerkverteiler unterstützen dynamische VLAN-Zuordnungen auf Basis einer Benutzer-Authentifizierung. Diese Methoden basieren auf dem Standard IEEE 802.1x. Dieser Standard definiert allerdings nur die Authentifizierung beim Netzzugang. Die Verfahren, wie ein Verteiler nach erfolgter Authentifizierung den Netzwerkzugang erlaubt, sind nicht standardisiert. Auch hier existieren daher nur herstellerspezifische Lösungen, die demnach nur bei einer homogenen Netzwerkinfrastruktur sinnvoll eingesetzt werden können.

Eine Authentifizierung wird in der Regel mittels Benutzername und Kennwort erfolgen. Möglich sind auch zertifikatsbasierte Lösungen.

Eine solche Lösung erfordert eine 802.1x-Unterstützung auf allen beteiligten Endgeräten. Aktuelle Betriebssysteme bieten eine solche 802.1x-Unterstützung. In der Regel ist diese jedoch nicht aktiviert, sodass zunächst eine Konfiguration und zudem eine Schulung der Nutzer nötig wird. Voraussetzung einer solchen Lösung ist auch eine Infrastruktur aus Authentifizierungsservern.

Auch diese Lösung ist primär zur Zugangskontrolle im internen Netz gedacht. Das Zugangskontrollsystem muss dann so konfiguriert werden, dass Gäste, die sich nicht authentifizieren können, in einem speziellen VLAN Zugang erhalten.

Eine Umgehung der Schutzmaßnahmen ist hier relativ leicht möglich, wenn ein autorisierter Benutzer bereit ist, sich an einem fremden Rechner anzumelden.

4. Dynamische VLAN-Zuordnung auf Basis von Agenten-Software

Die modernste Lösung für einen Zugangskontrolle zur Netzwerkinfrastruktur ist eine agentenbasierte Kontrolle. Auch bei solchen Lösungen liegt der Fokus nicht auf Bildung von Gästenetzen, sondern bei der Kontrolle des Zugangs eigener Rechner.

Agentenbasierte Systeme werden von verschiedenen Herstellern angeboten und unter der Bezeichnung Network Admission Control (NAC) vermarktet. Dabei wird auf dem Endgerät eine Agenten-Software installiert, die die Authentifizierung des Rechners gegenüber einem Authentifizierungsserver übernimmt. Dabei wird nicht nur die Identität des Rechners, sondern auch die Konformität bezüglich Sicherheitsrichtlinien (aktuelle Virenscanner und Signaturen, Firewall-Einstellungen sowie Installation von Systempatches) geprüft.

Nicht konforme Rechner werden in einer solchen Umgebung einem Quarantänenetz zugeordnet. Dieses Quarantänenetz würde dann auch als Gästenetz genutzt.

Eine Umgehung der Schutzmaßnahmen ist hier nur schwer möglich. Dazu müsste zunächst der Agent installiert werden. Im Weiteren müsste dann der Rechner den Sicherheitsrichtlinien entsprechen. Damit wäre dann aber auch das Sicherheitsrisiko „Einschleppen von Schadsoftware“, wegen dem das separate Gästenetz eingeführt wurde, nicht mehr gegeben. Verbleiben würde dann nur das Problem, dass fremde Rechner im internen Netz z. B. wegen Wahrung der Vertraulichkeit von Informationen in diesem Netz nicht erwünscht sind.

5. Vergleich der Lösungen

Lösungen mit dynamischer VLAN-Zuordnung haben den Vorteil der Automatisierung des Gästenetz-Zugangs an beliebigen Anschlüssen, während die statische Konfiguration häufig manuelle Eingriffe für die Bereitstellung von Gästenetz-Zugängen erfordert (soweit nicht großzügig zusätzliche Anschlüsse fest für diesen Zugang zur Verfügung gestellt werden). Insbesondere eine statische VLAN-Zuordnung ohne zusätzliche Sicherheitsmaßnahmen (Portsecurity) setzt Disziplin aller Mitarbeiter beim Anschluss von Rechnern voraus.

Alle Lösungen zur dynamischen VLAN-Zuordnung haben dafür den Nachteil, dass sie einen hohen Aufwand für die Verwaltung des internen Netzes erfordern, wobei eine bessere Verwaltung des internen Netzes natürlich auch einen Wert an sich darstellt. Das Gästenetz ist dann nur noch ein „Abfallprodukt“ einer konsequenten Netzwerkverwaltung. Diese Lösung verursacht zudem Kosten für eine geeignete Verwaltungssoftware und Schulung des technischen Personals.

Insbesondere die agentenbasierte Netzwerkzugangskontrolle wäre aber auch ein wesentlicher Fortschritt für die IT-Sicherheit im internen Netz. Aufwand und Kosten einer solchen Lösung sind jedoch erheblich. Soweit nicht insgesamt eine institutsweite Sicherheitslösung angestrebt wird, erscheint bisher eine Lösung mit statischer Zuordnung von Ports zu VLANs immer noch als die geeignetste Lösung zum Aufbau eines Gästenetzes.

2.3 WLAN als Zugangsnetz

Für die Anbindung von Gästerechnern im Institut können auch WLAN-Zugänge unter bestimmten Voraussetzungen genutzt werden, wenn bestimmte Voraussetzungen erfüllt sind.

Das Institut sollte kein allgemein offenes Funk-LAN betreiben, d. h, der Zugang zu diesem Netz darf nur nach einer Autorisierung durch das Institut möglich sein (Mitteilung geheimer Zugangsparameter). Das für Gäste offene Funk-LAN muss die oben beschriebene Trennung vom internen Netz umsetzen.

IT-Zielkonflikte

Rainer Walke

Max-Planck-Institut für demografische Forschung

1. Einleitung

Drei Gruppen bemühen sich um Software in unserem Institut.

Da gibt es die große Bandbreite Endanwender; von Leuten die einfach nur benutzen, bis hin zu Experten, die viele Fertigkeiten haben und strategisches Gespür besitzen.

Als zweite Gruppe betrachte ich Softwarehersteller und Softwarehändler. Diese versuchen Marktanteile zu sichern, neue Geschäftmodelle zu implementieren und natürlich Umsatz zu generieren.

Und die IT-Abteilung wäre die dritte Gruppe. Diese setzt Unternehmensziele um. Dazu zähle ich die Förderung zukunftsweisender Software im Sinne der wissenschaftlichen Abteilungen, die Förderung einheitlicher Softwareplattformen, soweit es sinnvoll ist, und die Identifikation überholter Software.

Mit Beispielen möchte ich auftretenden Konflikte andeuten und Lösungen skizzieren.

2. Wer legt Ziele für die Informationstechnologie fest?

Im ungünstigsten Fall legt niemand Ziele fest.

Dieser Fall tritt nicht ein, denn die Softwarefirmen haben feste Ziele im Blick: Umsatz und Marktanteil.

Im günstigsten Fall legen die Direktoren die Ziele für die IT mittelbar fest. Die Direktoren geben die Richtung vor, wo von wem Antworten auf wissenschaftliche Fragen zu suchen seien. Eine große Zahl von Doktoranden macht sich dann auf den Weg.

Meist hört der „befestigte Weg“ irgendwann auf, sie landen in unwegsamem Gelände und müssen sich einen eigenen Pfad bahnen.

Kurz: Wir als IT-Abteilung legen unsere IT-Ziele so fest, dass es den Doktoranden leichter fällt, vorwärts zu kommen.

Die personellen und finanziellen Ressourcen dürfen wir dabei nicht überfordern. Und einige Gesetze und Regelungen müssen wir auch einhalten.

3. Beispiele Konfliktsituationen

Ein Referent möchte für einen eintägigen Kurs das Simulationsprogramm NetLogo[1] im Computerraum benutzen.

Die Software ist frei verfügbar. Die Autoren haben kein direktes wirtschaftliches Interesse.

Im Test bei uns stellte sich die Software als interessantes, zukunftsweisendes Produkt dar.

Die Vorbereitung eines Installationsskripts erwies sich als trivial. Damit war die Verteilung auf beliebige Rechner gelöst.

NetLogo wurde in das Standard-Softwareangebot des Instituts übernommen.

Nicht immer entwickelt sich das so günstig.

Ein anderer Referent wollte für einen ebenfalls eintägigen Kurs das Statistik/Grafik-Programm DeltaGraph[2] im Computerraum durch die Studenten benutzen lassen.

Der Hersteller verkauft diese Software für etwa 200 US-Dollar pro Lizenz.

1. http://ccl.northwestern.edu/netlogo/
2. http://www.redrocksw.com/deltagraph/

Als IT-Abteilung konnten wir keine offensichtlichen Vorzüge gegenüber ähnlichen im Haus vorhandenen Programmen entdecken (z. B. SigmaPlot[3], S-Plus[4]).

Der Aufwand für eine Ein-Tages-Veranstaltung erschien unangemessen hoch. Wir empfahlen, bei Bedarf DeltaGraph mittels Notebook und Projektor vorzuführen.

Auch im Zusammenhang mit Produkten von Adobe gibt es zuweilen Konflikte.

Ein zugeschicktes Formular (PDF) sollte ausgefüllt und ausgedruckt werden. Leider war das Dokument offensichtlich undurchdacht erstellt worden. Der Adobe Reader forderte ohne Not die Nachinstallation eines Sprachpaketes. Dazu waren lokale Administratorrechte notwendig. Nach Zuteilung dieser Rechte bot Adobe weitere Updates an.

Eigentlich will unser Nutzer nur ein Formular ausfüllen, abspeichern und ausdrucken. Unbestellte Fragen sind dabei unerwünscht.

Die Firma Adobe dagegen will neue Versionen ihrer Produktpalette verkaufen. Dazu sollten möglichst viele Adobe-Reader-Installationen alle neuen Möglichkeiten unterstützen. Deshalb drängt Adobe auf die Installation der neuesten Komponenten. Selbstverständlich wird auch auf diesem Wege versucht, viele Prozesse in den Unternehmen mit Adobe-Software abzubilden.

Natürlich wollen wir auch, dass der Benutzer das Formular ausfüllen und ausdrucken kann. Aber schon im eigenen Interesse möchten wir unsere Mitarbeiter und Gäste vor unbestellten Fragen bewahren. Darüber hinaus soll die Anzahl der Updates und Upgrades auf ein notwendiges Minimum beschränkt werden. Denn nur durch eine unternehmenseinheitliche Softwarebasis können die Kosten für Lizenzen, Nutzerunterstützung, Nutzerschulung und Umlernen im Rahmen gehalten werden. Ebenfalls ist es uns wichtig, die Abhängigkeit von einem einzelnen Softwareunternehmen zu verhindern.

Lösung: Standardmäßig werden bei uns keine Administratorrechte ausgegeben. Damit entfallen schon viele Fragen nach Softwareupdates, welche die Nutzer beantworten müssten. Nach einem Test wurde das fehlende Sprach-

3. http://www.systat.com/products/SigmaPlot/
4. http://www.insightful.com/products/splus/

paket von Hand installiert. Leider haben wir keinen Einfluss auf den PDF-Absender, zukünftig kompatible Dokumente zu erstellen.

Mit dem an sich sehr interessanten Format PDF sind bei uns auch andere Fragen verbunden.

Eine Wissenschaftlerin verwendet Adobe Acrobat[5], um PDF-Dokumente elektronisch zu kommentieren.

Andere haben ebenfalls vor, PDF-Dokumente am Bildschirm zu lesen und mit Kommentaren zu versehen.

Die Firma Adobe möchte gern, dass wir flächendeckend Adobe Acrobat lizenzieren und einsetzen.

Als IT-Abteilung suchen wir Möglichkeiten, das einfache Kommentieren mit Softwarealternativen abzuwickeln. Gut wäre eine frei verfügbare Software. Diese könnten wir Studenten einfach jederzeit mitgegeben.

Die freie Alternative Jarnal[6] hat aus meiner Sicht derzeit nicht die Funktionalität, um sie als Alternative im Hause empfehlen zu können.

Als kommerzielle Alternative könnte der Foxit Reader[7] eingesetzt werden (etwa 39 US-Dollar).

Entweder werden wir Adobe Acrobat als Concurrent-User-Lizenz lizenzieren und als Installationsskript im Hause allgemein anbieten, oder alternativ lizenzieren wir den Foxit Reader und bieten ihn ebenfalls über ein Installationsskript an.

Ein Wissenschaftler benötigt die Software CAIC[8] (Thema Evolutionäre Biologie). Sie ist frei erhältlich und läuft unter MacOS 7.5-9.2. Wir benutzen aber grundsätzlich Rechner mit Windows-XP-Betriebssystem.

Die Autoren bieten diese Software zwar frei an, scheinen aber keine Ressourcen für die weitere Entwicklung zu haben. Die aktuelle Version ist vom März 2002. Seit Mai 2001 wird eine Version für Windows angekündigt. Offensichtlich bisher fruchtlos.

---

5. http://www.adobe.com/products/acrobat/
6. http://www.dklevine.com/general/software/tc1000/jarnal.htm
7. http://www.foxitsoftware.com/
8. http://www.bio.ic.ac.uk/evolve/software/caic/

Als IT-Abteilung möchten wir eine einheitliche Betriebssystemplattform erhalten. Die Einführung einer nicht mehr aktiv entwickelten Software scheint fragwürdig.

Leider hat in diesem konkreten Fall eine Mac-Emulation nicht ausgereicht. Dann haben wir einen Mac mit passendem Betriebssystem gefunden und als Zusatzrechner aufgestellt. Damit war dem Wissenschaftler erstmal geholfen.

Parallel versuchen wir aktiv entwickelte Alternativen aufzuzeigen, die sowohl zu unserem Betriebssystem als auch zu im Hause beliebten Statistik-Programmen passen. Das könnte möglicherweise die Softwarebibliothek Ape[9] für das Statistik-Paket R[10] sein. Von Kollegen wurde dem Wissenschaftler die Software Mesquite[11] als Alternative empfohlen.

Ein anderes Thema.

Viele Gäste und gerade Studenten halten Kontakt mittels Instant Messaging. Natürlich lassen sie diesen Kontakt nicht gern abbrechen.

Die einzelnen Hersteller von Instant-Messaging-Produkten wollen ihre eigene Community stärken und andere marginalisieren. Sie sind an einer Interoperabilität nicht interessiert. Zusätzlich blähen sie ihre Produkte mit ungeahnten Features auf, um zusätzliche Einnahmen zu erzielen.

Für die IT-Abteilung sind solche Produkte ein Graus. Niemand weiß so genau, was diese machen. Eine solche Fülle verschiedener Software zu verwalten, ist unwirtschaftlich und der Nutzen für die Forschung scheint mir höchstens mittelbar. Als Lösung verteilen wir per Skript Miranda[12]. Dies ist mit etlichen Instant-Messaging-Produkten kompatibel und für uns überschaubar. Sicherlich sind die Einstellungen nicht immer einfach, aber es funktioniert.

Viele Leute installieren generell gern Software. Und zwar unabhängig davon, ob sie diese brauchen, unabhängig davon, ob sie sich mühselig einarbeiten müssten, und unabhängig davon, ob man für die Software etwas bezahlen muss.

Die Software-Industrie sagt, sie mag keine Raubkopien.

---

9. http://pbil.univ-lyon1.fr/R/ape/
10. http://www.r-project.org/
11. http://mesquiteproject.org/mesquite/mesquite.html
12. http://www.miranda-im.org/

Andererseits scheint die Raubkopie als Vertriebsweg fest einkalkuliert zu sein.

So war bei HEISE im März dieses Jahres zu lesen[13]:

„Jeff Raikes, Chef der Business Division bei Microsoft, meint, wenn schon Software illegal verwendet wird, dann sei es am besten, sie stamme aus seinem Haus."

Für die IT-Abteilung sind Raubkopien unerwünscht.

Sie verhindern Preistransparenz. Ein Hersteller, der sich auf seine Raubkopierer verlassen kann, hält seine Verkaufspreise hoch und die Benutzer in einer rechtlichen Grauzone.

Raubkopien verhindern die Suche nach Alternativen. Nur wenige denken nach, wenn der Zugang zu Kopien einfach ist.

Wir konzentrieren uns im Institut auf Concurrent-User-Lizenzen. Jeder im Institut kann sie probieren. Gezahlt wird für gleichzeitiges Benutzen. Grundsätzlich installieren wir Institutssoftware nur auf Institutshardware. Damit halten wir den dienstlichen und privaten Bereich getrennt.

Günstige Software zu Forschung- und Lehre-Konditionen kann auch Konfliktstoff bergen.

Viele Softwarehersteller bieten Software für Nutzer in diesem Bereich zu deutlich günstigeren Konditionen an.

Damit soll die Forschung gefördert werden. Andererseits erhalten die Hersteller Zugang zu jungen, motivierten Leuten und können diese auf ihre Software konditionieren.

Als IT-Abteilung sind wir natürlich erfreut über jeden Rabatt. Andererseits wächst so den Nutzern dieser Software, den IT-Verantwortlichen und besonders den in der Lehre engagierten Mitarbeitern eine besondere Verantwortung zu.

Denn die Anschaffungskosten betragen oft nur einen Bruchteil der vollen Kosten. Für die Einarbeitung sind oft Monate notwendig. Damit trägt das Individuum persönlich eine große Last. Lohnt sich diese Investition mittelfristig und langfristig? Dies sollte beantwortet werden, bevor man Zeit in eine neue Software investiert oder dies anderen empfiehlt.

13. http://www.heise.de/newsticker/meldung/86615

4. Schluss

Wichtig ist es, den direkten Kontakt zu den Leuten im Institut, zu den Problemträgern zu suchen. Aufgaben aus zweiter Hand sind selten zufriedenstellend erfüllbar.

Wenn der eigentliche Kern des Problems identifiziert ist, suchen wir eine Lösung und implementieren sie innerhalb der bestehenden IT-Struktur. Bei Software heißt das bei uns, ein Installationsskript zu erstellen. Gute Lösungen sollten dann auch im Hause bekannt gemacht werden. Manchmal gelingt es sogar, alte und überholte Programme komplett zu ersetzen.

Videokonferenzen via Accessgrid Node

Almuth Barta

Max-Planck-Institut für Gravitationsphysik / Albert-Einstein-Institut, Potsdam-Golm

Am Max-Planck-Institut für Gravitationsphysik werden seit einigen Jahren und mit zunehmender Tendenz Videokonferenzen durchgeführt.

Dabei werden neben den Standard-Videokonferenzen nach H.323 auch Accessgrid-Node-Konferenzen verwendet. Die Merkmale von Konferenzen mit Accessgrid Node sollen in diesem Vortrag dargestellt werden.

Die folgende Gliederung zeigt die Schwerpunkte des Vortrags:

- Audio-/Videokonferenzen am Albert-Einstein-Institut (AEI)
- Videokonferenzen via H.323 oder Access Grid Node (AGN)
- Raumausstattung für AGN
- Hardware für AGN
- AGN-Software
- Netzwerk – Virtual Venues – VenueServer – BridgeServer

- Ergänzende nützliche Tools
  - Tigerboard (interaktives Whiteboard)
  - AGVCR (Aufzeichnung von AGN-Konferenzen)
- Ausblick

1. Audio-/Videokonferenzen am Albert-Einstein-Institut (AEI)

Videokonferenzen werden immer häufiger durchgeführt, um regelmäßige Besprechungen auch über mittlere oder große Distanzen zu erleichern bzw. überhaupt erst zu ermöglichen.

Da das Albert-Einstein-Institut zwei Standorte, Potsdam-Golm und Hannover, hat, gibt es immer öfter Videokonferenzen zwischen den beiden Teilinstituten.

Zum anderen werden regelmäßige Konferenzen mit verschiedenen Kooperationspartnern, z. B. Louisiana State University (LSU), USA, durchgeführt.

Für die Videokonferenzen werden verschiedene Techniken eingesetzt. Die Entscheidung für eine der Optionen richtet sich zum einen nach der verfügbaren Technik auf der Gegenseite, aber auch nach den jeweiligen Anforderungen der Teilnehmer an das Videokonferenzsystem.

Zum Einsatz kommen Telefonkonferenzen, Videokonferenzen nach dem Standard H.323 und Videokonferenzen via Accessgrid Node (AGN).

2. Videokonferenzen via H.323 oder Access Grid Node (AGN)

2.1 Telefonkonferenzen

Hierfür wird ein Konferenztelefon

- Polycom Soundstation

verwendet. Mit Zwei Mikrophonen und Lautsprecher eignet es sich gut für kleine Konferenzräume.

2.2 Videokonferenzen via Standard H.323

Für diese Technik gibt es eine Vielzahl fertiger Systeme zu kaufen. Der Installations- und Konfigurationsaufwand ist dementsprechend gering.

Es werden Ton und Videobilder zwischen zwei miteinander verbundenen Standorten ausgetauscht. Zusätzlich können ggf. Applikationen/Daten parallel gesendet werden.

Die Verbindung mehrerer Standorte miteinander erfordert den Einsatz einer leistungsstarken MCU (Multipoint Connection Unit). Jeder der teilnehmenden Standorte sendet sein Bild und Ton an die MCU, welche die Bilder entsprechend der Konfiguration zu einem Videobild zusammensetzt und dieses mit dem Ton an alle Teilnehmer versendet. Dabei kann das Bild aus Einzelbildern der jeweiligen Teilnehmer zusammengesetzt sein oder es kann nur ein spezielles Bild, z. B. das des aktuellen Sprechers, ausgewählt sein. In jedem Fall erfolgt die Konfiguration zentral und alle Teilnehmer sehen immer das gleiche Bild.

Für diese Anwendung sind am Albert-Einstein-Institut folgende Geräte vorhanden:

- Tandberg 880
- Sony PCS G50

Statt der oben genannten Geräte können auch, insbesondere wenn an den jeweiligen Standorten nur einzelne Personen teilnehmen, Softwarelösungen wie NetMeeting, Xmeeting oder Ekiga verwendet werden.

2.3 Videokonferenzen via Access Grid Node (AGN)

Hierbei handelt es sich um ein Open-Source-Softwareprdukt. Die benötige Hardware wird individuell zusammengestellt.

„LSU Life Sciences A663 Node"
Louisiana State University, Baton Rouge, USA
Quelle: http://www.accessgrid.org/

Die Software besteht aus einem Client, der für die Konfiguration und den Verbindungsaufbau zuständig ist, und weiteren Tools für die Tonübertragung sowie für das Senden und Empfangen der Videobilder. Im Client ist ein Chat-Tool (Jabber) integriert.

In der Regel werden 2-4 Kameras verwendet. Jedes einzelne der Videobilder wird übertragen. Entsprechend werden alle einzelnen Videobilder der anderen Standorte empfangen. Der Operator des AGN ist dafür verantwortlich, hieraus jeweils die Bilder auszuwählen, die dann auf der Präsentationsfläche zu sehen sind. Dabei kann er Anordnung und Größe der Darstellung wählen.

Meist verwendet man 2-3 Präsentationsflächen. So kann man gleichzeitig viele Bilder darstellen oder auch auf den Präsentationsflächen verschiedene Inhalte zeigen. Auf einer Präsentationsfläche könnte man die Bilder der Teilnehmer und auf der anderen die Präsentation des Vortragenden oder andere Dokumente, die alle Teilnehmer sehen sollen, zeigen.

Verbindungen zwischen mehreren Standorten sind standardmäßig enthalten.

3. Raumausstattung für AGN

3.1 Mobiler Accessgrid Node

Der erste bei uns eingesetzte Accessgrid Node sollte mobil und so in verschiedenen Seminarräumen einsetzbar sein.

So entschieden wir uns für eine „kleine“ Lösung, die auf einem fahrbaren Computertisch untergebracht werden konnte:

Mobiler AGN bestehend aus

- Rechner
- Echo-Canceller
- 3 Kameras
- 2-4 Mikrophone
- 2 Lautsprecher
- Beamer nicht auf dem Wagen

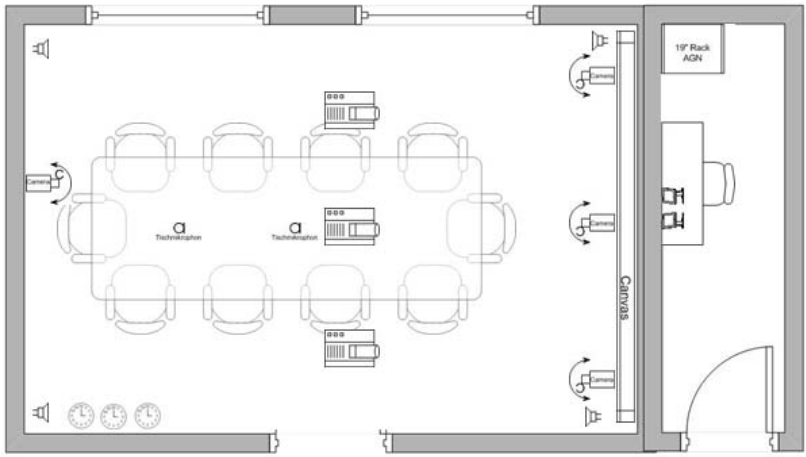
Obwohl alles auf einem fahrbaren Wagen untergebracht ist, bleibt für jede Konferenz ein relativ hoher Aufwand für Auf- und Abbau, denn es müssen Kameras, Mikrophone und Lautsprecher im Raum platziert werden und die entsprechenden Kabel stolperfrei verlegt werden. Sofern Beamer im Raum fest installiert sind, müssen diese nur angeschlossen werden, anderenfalls müssen diese

noch hinzugenommen werden, und/oder es können alternativ Plasma-Bildschirme eingesetzt werden.

3.2 Accessgrid Node als Raum-Node

Zur Einrichtung eines Seminarraumes für Accessgrid-Konferenzen ist die Platzierung zahlreicher Geräte zu planen. Es sind 2-3 Projektionsflächen und Beamer, die Kameras, Lautsprecher und Mikrophone zu platzieren. Steht ein separater Technikraum zur Verfügung, kann dort der Rechner und ggf. weitere Technik wie Echocanceler oder ggf. Audio-/Video-Kreuzschienen untergebracht werden.

Hier ist die Skizze einer typischen Raumeinrichtung:



An unserem Institut hatten wir die Gelegenheit, einen neuen Seminarraum entsprechend den Bedürfnissen der Videokonferenzen einzurichten.

Hier ein Blick in den Raum:

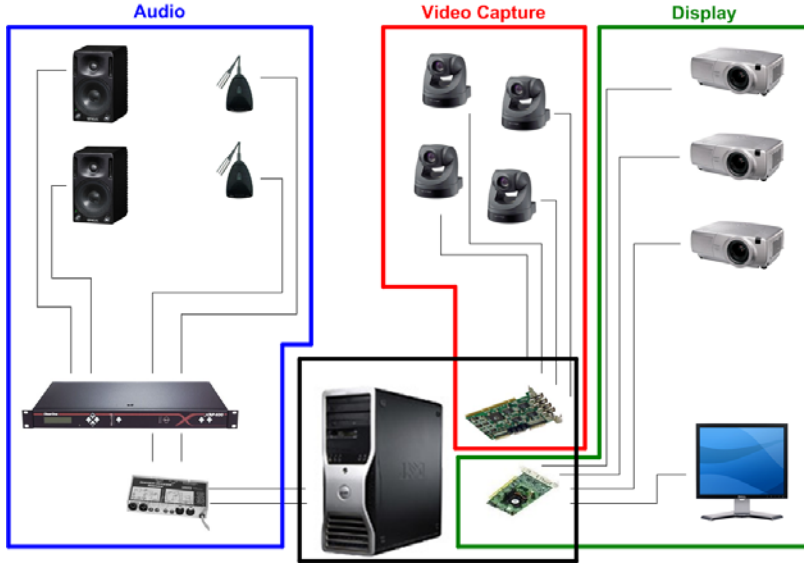
4. Hardware für AGN

Um einen Accessgrid Node aufzubauen, benötigt man einen Rechner, der insbesondere mit Capture-Karten für die Kamerabilder und Graphikkarten für 3-4 Bildschirme ausgestattet ist.

Entsprechend der Anzahl Displays benötigt man Beamer und Projektionsflächen, wobei ein Display für den Operator mit Monitor vorgesehen werden sollte.

Für Video und Audio sind Kameras, Lautsprecher und Mikrophone notwendig, für die Echounterdrückung ein Echocanceler sowie ggf. ein Signalwandler zwischen dem Echocanceler und dem Rechner.

Einen Überblick gibt die folgende Abbildung:



Die nachfolgende Tabelle listet die genaueren Hardware-Spezifikationen der bei uns verwendeten Nodes auf:

AGN	**Mobiler Node**		**Raum Node**	
Bezeichnung	**Anzahl**	**Typ**	**Anzahl**	**Typ**
Rechner	1	DELL Precision 530 2x2 GHz / 1 GB RAM / 2x80 GB HD	1	DELL Precision 490 2x3 GHz / 4 GB RAM / 3x500 GB Raid5
Video card	1	Matrox G450 MMS Quadro-head (1x Operator, 1-3x Projektion)	1	Nvidia NVS285 (1x Operator) Matrox G550 (2x Projektion)

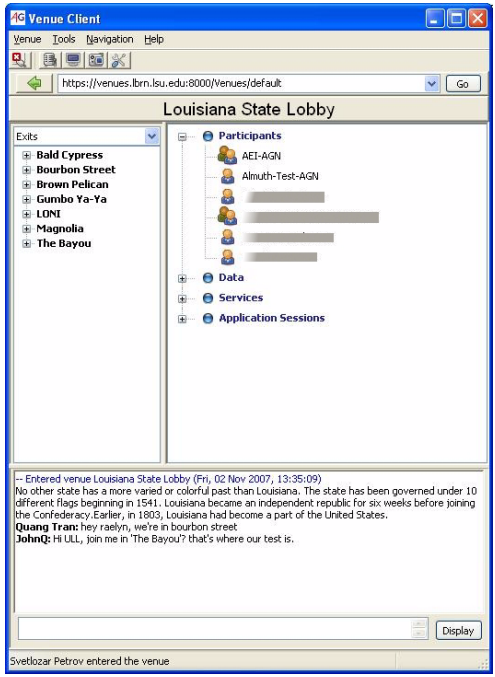
AGN	Mobiler Node		Raum Node	
Bezeichnung	**Anzahl**	**Typ**	**Anzahl**	**Typ**
VideoCapture Card	3	Viewcast Osprey OSP-220	1	Viewcast Osprey OSP-440 (4-fach)
Monitor	2	17" TFT (LG Flatron L1710B)	1	19” TFT (DELL)
Kamera	3	Sony EVI-D31	7 (davon 4 aktiv)	Sony EVI-D70
Stativ	3	Sony VCT-D480RM		
Gentner XAP400	1	Gentner XAP400	1	Gentner XAP400
Matchmaker	1	MatchMaker MM100	1	MatchMaker MM100
Lautsprecher	2	Gelenec 1029A	1	Bose MA12, MB 4
Tischmikrofon	1	Shure MX391/0	2	Shure MX391/0
Beamer	1-3	je nach Verfügbarkeit im Aufstellungsraum, alternativ Plasma Screen	2	Hitachi CP-SX1350 SXGA+ (1400x1050, 3500 ANSI Lumen)

AGN	Mobiler Node		Raum Node	
Bezeichnung	**Anzahl**	**Typ**	**Anzahl**	**Typ**
				Der AGN ist in die weitere Ausstattung des Seminarraums integriert. Weitere Geräte wie Video-/Audio-Kreuzschiene und Mediensteuerung sind eingebaut, werden hier aber nicht aufgeführt, da nicht AGN-spezifisch

5. AGN-Software

5.1 Der AGN-Client

Für den Operator ist der zentrale Teil der Software der AGN-Client.



Hierin werden alle Konfigurationen vorgenommen. Dazu gehören die Grundeinstellungen des Nodes, die Voreinstellungen für Audio und die Anzahl und Einstellung der Videobilder. Hier erfolgen Verbindungsaufbau und -kontrolle.

Integriert ist ein Chat-Tool, basierend auf Jabber, das dem Operator ermöglicht, sich mit den Operatoren der anderen Standorte in Verbindung zu setzen.

Hier können auch Dateien den anderen Teilnehmern zur Verfügung gestellt werden. Durch einfaches Drag&Drop können Dateien hoch- oder heruntergeladen werden.

Applikationen wie Powerpoint können gemeinsam genutzt werden, was die visuelle Qualität in der Darstellung der Folien bei Vorträgen erheblich verbessert.

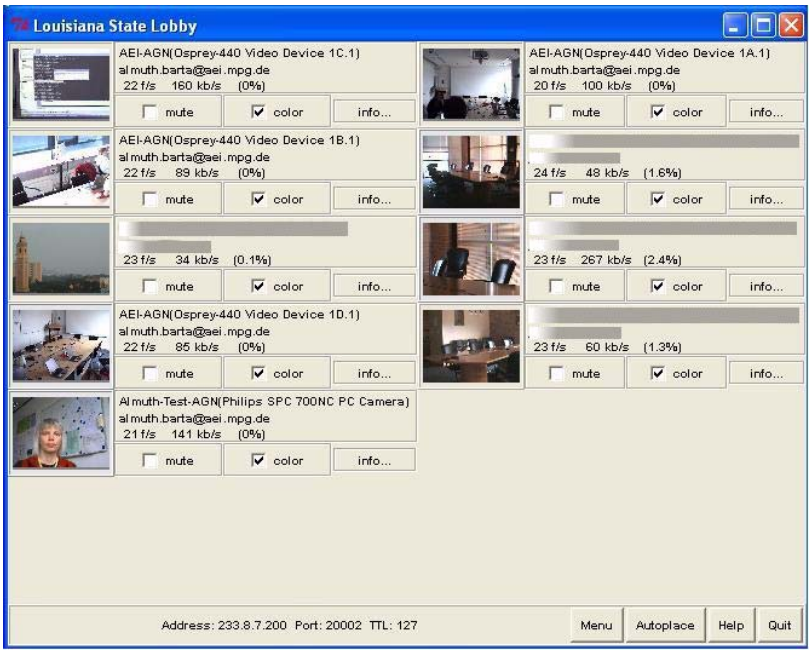
5.2 Das Audio-Tool RAT

Bei Verbindungsaufbau öffnet sich automatisch ein Fenster zur Kontrolle des Audio-Streams.

Hierin kann man die übrigen verbundenen Standorte und ihren Audio-Status sehen. Es können die eigenen Audio-Einstellungen justiert werden, die Lautstärke der anderen Standorte kann generell oder individuell angepasst werden. Sogar die Tonaufzeichnung der laufenden Konferenz ist von hier aus möglich.

5.3 Das Video-Tool VIC

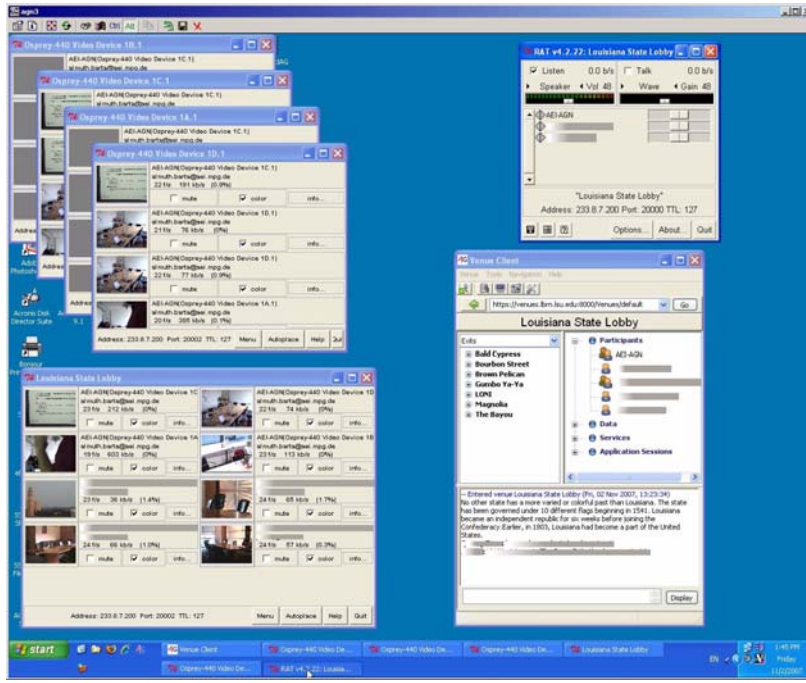
Das VIC-Tool dient der Kontrolle der verschiedenen Video-Streams. Es öffnet sich automatisch ein Fenster je konfigurierter Kamera. In dem jeweiligen Fenster können Einstellungen zur Übertragung des zugehörigen Video-Streams vorgenommen werden.



Darüber hinaus öffnet sich ein weiteres VIC-Fenster, in dem alle empfangenen Video-Bilder dargestellt werden.

Aufgabe des Operators ist es, die Bilder für die Projektion auszuwählen und in gewünschter Größe und Anordnung auf die Präsentationsflächen zu schieben.

Insgesamt ergibt sich etwa folgende Ansicht des Operator-Monitors:



6. Netzwerk – Virtual Venues – VenueServer – BridgeServer

Alle Audio- und Videostreams einer AGN-Konferenz werden per Multicast übertragen.

Es ist daher notwendig, sich vorher über die zu verwendenden Mulitcast-Adressen und Portnummern zu verständigen.

Hierzu werden **Virtual Venues** verwendet.

Ein Virtual Venue ist ein virtueller Konferenzraum, definiert durch Multicast-Adresse und Portnummer für Video und Audio. Zur leichteren Handhabung wird einem solchen Adressenpaar ein Name zugeordnet.

Ein (öffentlich erreichbarer) **Venueserver** verwaltet diese Namen und Adressen. Diese werden zusätzlich mit einer URL verknüpft.

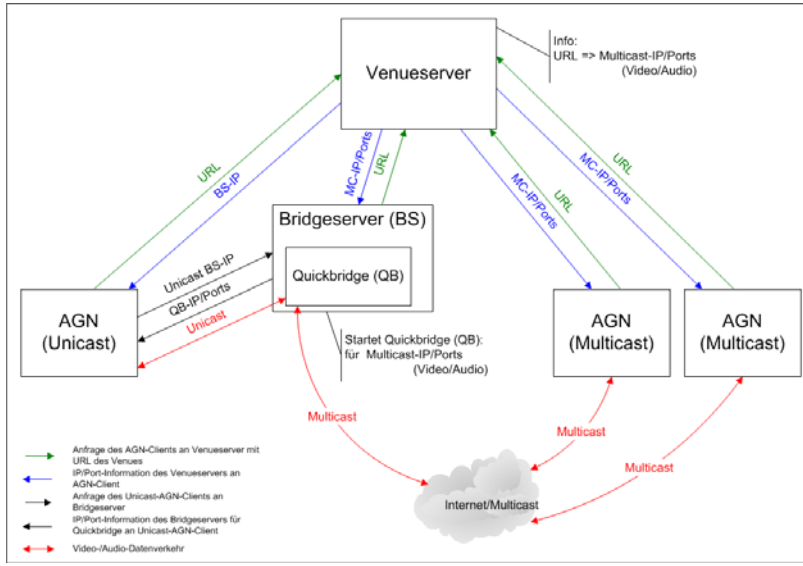
Für eine Konferenz einigt man sich somit auf einen Venueserver und einen von diesem verwalteten Venue. Der Client fragt den Venueserver mit dem Namen des Venues oder der URL an und erhält von diesem die benötigten Multicast-Adressen und Portnummern. Mit diesen öffnet er dann die Audio- und Video-Streams via RAT- und VIC-Tool.

Der Venueserver hält auch den Filespace für die zu einer Konferenz hinterlegten Dateien vor.

Da nicht alle AGN-Clients multicastfähig sind, kann ein **Bridgeserver** eingerichtet werden.

Der Client kommuniziert dann unicast mit dem Bridgeserver. Der Bridgeserver muss multicast-fähig sein. Er wickelt den Multicast-Verkehr ab und leitet ihn unicast an den Client weiter.

Das folgende Schaubild skizziert die Datenströme für eine AGN-Konferenz:



7. Ergänzende nützliche Tools

7.1 Tigerboard (interaktives Whiteboard)

Tigerboard ist ein interaktives Whiteboard, das mit allen verbundenen Standorten gemeinsam genutzt werden kann. Die Anwendung befindet sich noch im Beta-Stadium, wird aber teilweise schon regelmäßig eingesetzt.

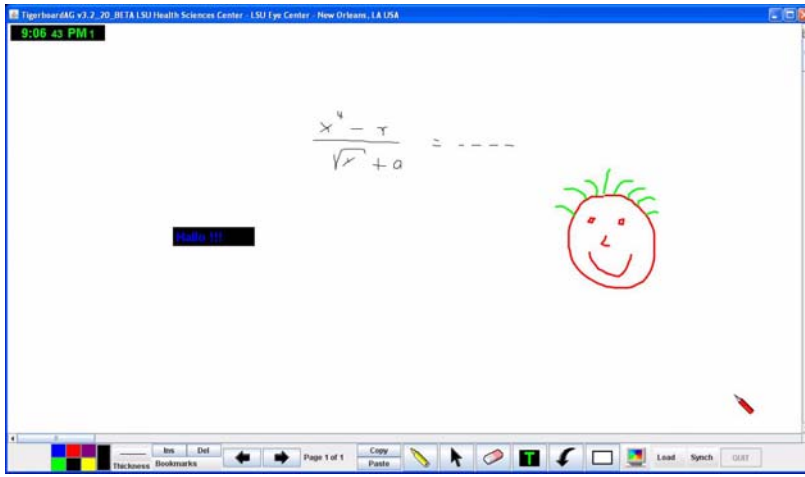
Die erstellten Seiten können gespeichert werden.

Zusätzlich ist eine Funktion für gemeinsam genutzte Applikationen integriert. Shared Powerpoint steht schon zur Verfügung, die Integration von PDF ist geplant.

Denkbar ist die Verwendung von Tigerboard auf einem Tablet-PC, so dass z. B. auch Gleichungen, über die während einer Konferenz diskutiert wird, per Stift geschrieben werden.

Ebenso ist auch möglich, einen Plasmaschirm, auf dem die Tigerboard-Anwendung dargestellt wird, mit einem vorgesetzten interaktiven Board zu versehen, so dass hierauf geschrieben werden kann.

Die folgende Abbildung zeigt einen Screenshot der Tigerboard-Anwendung:



7.2 AGVCR (Aufzeichnung von AGN-Konferenzen)

AGVCR ist ein zusätzliches Tool, das die Aufzeichnung und Wiedergabe von AGN-Konferenzen ermöglicht.

Die Aufzeichnung von AGN-Konferenzen erfordert die Aufzeichnung von einer Vielzahl von Video-Streams. All diese stehen bei der Wiedergabe zur Verfügung.

Die Wiedergabe kann wahlweise in einen Virtual Venue oder auch lokal erfolgen.

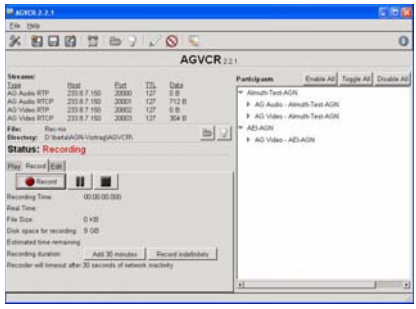
Bei Wiedergabe in einen Virtual Venue werden die aufgezeichneten Video-Bilder in diesen Venue dargestellt, ggf. zusätzlich zu den live-Bildern in diesem Venue. Die Aufzeichnung kann auf diese Weise auch an andere Standorte übertragen werden.

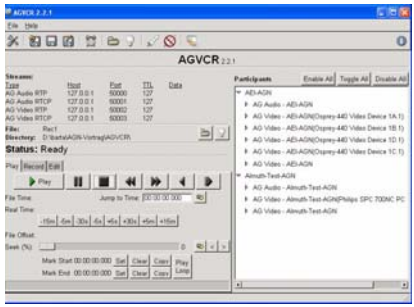
Für die lokale Wiedergabe enthält der AGVCR die notwendigen RAT- und VIC-Tools.

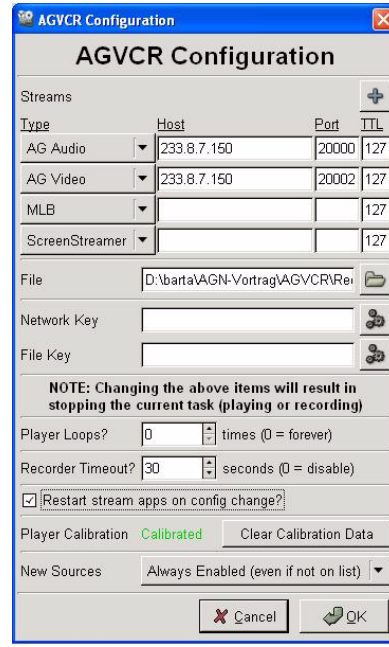
Jeder Standort und sogar jeder einzelne Video-Stream kann für die Wiedergabe selektiert oder ausgeschlossen werden.

Für die Aufzeichnung werden die Multicast-Adressen und Ports der Audio- und Video-Streams benötigt. Diese zeigt der AGN-Client nach Verbindung mit dem Virtual Venue an.

Die folgenden Abbildungen zeigen Screenshots des AGVCR-Tools zum Aufnehmen, Wiedergeben und Konfigurieren der aufzunehmenden Konferenz:







8. Ausblick

Die Accessgrid-Software wird von der OpenSource-Community permanent weiterentwickelt.

Zur Zeit gibt es Projekte für die Unterstützung von HD-Video.

Manche Funktionalität wird über externe Tools abgedeckt.

So gibt es großes Interesse an Screen Capture. Dabei soll der komplette Bildschirminhalt an die anderen Standorte gesendet werden.

Ebenso soll die Installation vereinfacht werden oder weitere Shared Applications unterstützt werden.

Die Palette ist, da es sich um Open Source handelt, natürlich weit gefächert und richtet sich nach den Interessen der aktuellen Entwickler und Nutzer.

Weitere Informationen

Alle weiteren Informationen, Dokumentation, Software, Hardware-Empfehlungen sind hier erhältlich:

http://www.accressgrid.org/

Mailinglisten zu Accessgrid:

ag-tech@mcs.anl.gov

ag-users@mcs.anl.gov

ag-announce@mcs.anl.gov

Alle Fotos und Screenshots sind, soweit nicht anders angegeben, am Albert-Einstein-Institut entstanden.

Kontakt:

Almuth Barta
Max-Planck-Institut für Gravitationsphysik / Albert-Einstein-Institut
Wissenschaftspark Golm
Am Mühlenberg 1
14476 Potsdam-Golm

Tel.: +49 331 567 7304
e-mail: almuth.barta@aei.mpg.de

Zusammenarbeit in der MPG: Der Aufbau eines CMS für fünf juristische Institute – ein Erfahrungsbericht[1]

Jochen Jähnke

Max-Planck-Institut für Ausländisches und Internationales Strafrecht, Freiburg

1. Entwicklung des Projekts: Auftakt

Am MPI für Strafrecht wurden wir im Jahr 2003 durch die Direktoren aufgefordert, uns an einem Projekt zur Einführung eines gemeinsamen Content-Management-Systems (CMS) mit vier weiteren juristischen Instituten zu beteiligen. Das Projekt eröffnete die Chance, die Zusammenarbeit mit den anderen Instituten zu stärken, Synergieeffekte zu nutzen und gleichzeitig unsere bis dahin von Hand gepflegte Internetpräsenz auf eine modernere Basis zu stellen.

1. Dieser Vortrag wurde auf dem 24. DV-Treffen der Max-Planck-Gesellschaft in Jena gehalten. Die Vortragsform wurde für die Veröffentlichung beibehalten.

Die beiden Hauptziele, die durch die Einführung des CMS erreicht werden sollten, waren

1. Redaktion und Aktualisierung der Webseiten zu unterstützen,
2. Entzerrung der Arbeitsabläufe, die von nur wenigen Personen abhängig waren.

Alle Wissenschaftlerinnen und Wissenschaftler sowie alle Beschäftigten in den Servicebereichen sollten in die Lage versetzt werden, die in ihrer oder seiner Verantwortung liegenden Seiten selbst zu pflegen. Dennoch sollte eine Kontrolle stattfinden und der so genannte „Workflow“ im System entsprechend hinterlegt und überprüfbar sein. An dieser Stelle kann bereits vorweg genommen werden, das diese Ziele ohne Einschränkungen erreicht werde konnten!

Dieser Artikel soll von unseren Erfahrungen berichten und die organisatorischen Herausforderungen beleuchten, die bewältigt werden mussten, um die gesteckten Ziele zu erreichen.

Zu Beginn war keinesfalls allen Beteiligten klar, was das CMS leisten solle oder was ein CMS denn überhaupt sei. Es entstand hin und wieder der Eindruck, dass – insbesondere in den Köpfen der Wissenschaftler – ein CMS eine Mischung aus „eierlegender Wollmilchsau“ und einer Chefsekretärin mit riesigem Organisationstalent sei.

Dies ist sicher ein bekanntes Phänomen, das vielfach bei Projekten zu beobachten ist: Dass in technischen Lösungen gleichzeitig auch eine Lösung für Organisationsprobleme gesehen wird. Andererseits wird in die unbekannte Technik oft die Bedrohung alles Bekannten, Guten und Althergebrachten projiziert. Beide Vorstellungen sind meist falsch und erschweren den Blick auf die Realität und die Kommunikation über Projektziele und deren Erreichung. Es handelt sich meist um unreflektierte Wünsche oder Ängste. Beiden Vorstellungen begegneten wir in verschiedenen Stadien des Projekts. Und mit beiden Vorstellungen hatten wir zu kämpfen.

2. Meilensteine

Zuerst musste, wie bei jedem Projekt, ein Plan entworfen und die Finanzierung sichergestellt werden. Danach konnte es an die Arbeit gehen. Nach und nach zeigte es sich, dass ein sinnvoller Plan und eine gute Organisation bei weitem schwieriger waren als die Finanzierung konkreter Hardware oder bestimmter Serviceaufträge. Im Folgenden will ich zuerst auf die technische Realisierung eingehen, danach einige Herausforderungen des Projektmana-

gements und der Gruppenarbeit diskutieren, um danach an einem Teilprojekt den Werdegang zu beleuchten.

3. Kurzer Abriss der technischen Realisierung und die Architektur des Systems

Individuelle Instanzen des CMS-Redaktionssystems laufen auf einem Server, der am MPI für Völkerrecht in Heidelberg betrieben wird. Das CMS-System der Firma Contens läuft auf SUN Solaris mit einer Oracle-Datenbank (für die Objekte) und Cold Fusion als Script-Sprache. Es gibt neben den in das CMS integrierten Standardapplikationen wie zum Beispiel einem Kalender noch eigene Applikationen, die auf unseren Auftrag hin entwickelt wurden. Hervorzuheben ist hier vor allem der Stipendienworkflow der im Auftrag des MPI für Geistiges Eigentum entwickelt wurde.

Aus Sicherheitsgründen hat jedes Institut lediglich Zugriff auf seine Instanz des CMS. Zusätzlich gibt es ein gemeinsames Entwicklungs- und Testsystem.
Die individuellen Webserver inklusive der Datenbank-Instanzen und des Coldfusion-Servers laufen bei den Instituten. Der Zugriff auf den Redaktionsserver und die Publikation auf den Webserver erfolgt verschlüsselt und nur von bestimmten Quell- und Zielrechnern aus. Die Benutzerpflege erfolgt bei uns zurzeit von Hand. Noch offen ist die geforderte Anbindung an das Microsoft Active Directory.

4. Finanzierung

Mit einem erfolgreichen BAR-Antrag konnte als Anschubfinanzierung ein großer Teil der notwendigen Lizenzen und Hardware beschafft werden. Sämtliche weiteren Kosten wurden von den einzelnen Instituten finanziert. Die Abrechnung erfolgte zentral über ein Institut, das die Kosten sammelte und nach einem ausgehandelten Berechnungsschlüssel den anderen Instituten in Rechnung stellte.

5. Softwareevaluation

Um unter den vielen möglichen Anbietern auswählen zu können, mussten wir uns mit den einzelnen Vorstellungen auseinandersetzen, was ein CMS für uns denn sei oder sein könnte, um eine Anforderungsspezifikation für die anstehende Softwareevaluation zu entwerfen. Da es hier in erster Linie um die Benutzerschnittstelle für das CMS ging, war relativ schnell Einigkeit erzielt. Als Ergebnis der Softwareevaluation wurde das System der Firma Contens ausgewählt, da es dem der anderen Anbieter funktional äquivalent

war und zur damaligen Zeit als einziges System über einen WYSIWYG-Editor verfügte.

6. Hindernisse: Gruppenorganisation und mangelnde Personalressourcen

Die erste Hürde war die Konsolidierung der Gruppe mit ihren unterschiedlichen und wechselnden[2] Teilnehmern. Dadurch verschlang die Selbstorganisation der Gruppe relativ viel Energie. Es galt, viele verschiedene Qualifikationen und Hintergründe sowie die Erfahrung der einzelnen Projektmitarbeiter zu berücksichtigen und zu integrieren. Die meisten Gruppenmitglieder hatten nur geringe oder gar keine Erfahrung mit Projekten dieser Größenordnung.

Für fast alle Beteiligten am Projekt war dies eine Zusatzaufgabe zur täglichen Arbeit, die meist den engagierten und erfahrenen Mitarbeitern zusätzlich zur täglichen Arbeit zugewiesen wurde. Deshalb war kaum jemand wirklich frei für das Projekt. Dies erklärt den häufigen Mangel an Personal-Ressourcen und Kontinuität.

Zum Teil waren auf allen Hierarchieebenen ähnlich viele Mitarbeiter mit dem Projekt befasst. Zu manchen Zeiten waren auf der Leitungsebene fast alle Direktoren beteiligt. In der nächsten Ebene dann jeweils mindestens ein Wissenschaftler und meist ein IT-Spezialist. In der Ebene, die den Code schreiben sollte war dann oft nur noch ein oder gar kein Mitarbeiter vorhanden. Die Hierarchie-Pyramide stand praktisch auf dem Kopf: „Es gab viele Häuptlinge und fast keine Indianer."

7. „Don't try this at home": Herausforderungen beim Projektmanagement

Sowohl auf ein Pflichtenheft als auch auf ein Lastenheft wurde vor allem wegen des erwähnten Zeitmangels und den fehlenden Personalressourcen bei einigen Projektteilen verzichtet. Diese Vorgehensweise hat sich nicht bewährt. Eine genaue Projektdefinition durch ein in natürlicher Sprache verfasstes Lastenheft sowie Pflichtenhefte für spezielle Unterbereiche des Projekts wären sicherlich oft hilfreich gewesen.

2. Zudem wurden im Projektverlauf mehrfach eingearbeitete Mitarbeiter aus institutsinternen Gründen abgezogen oder konnten nicht im vereinbarten Umfang eingesetzt werden.

Lange Zeit erfolgte die Terminplanung nach der „Nice to have“-Methode. Das heißt, die Termine wurden nach Wunschvorstellungen gesetzt, ohne Planungssicherheit und Wissen über den notwendigen Aufwand oder die verfügbaren Ressourcen.

8. Die Wege zum Erfolg: Kommunikation und Workshops über Projektmanagement

Trotz der erwähnten Hindernisse gelang es – insbesondere durch die Projektmanagementseminare[3] – im Laufe der Zeit eine funktionierende Gruppenstruktur aufzubauen.

Die Seminare ermöglichten den Aufbau einer guten Kommunikation im Projekt und den Projektmitarbeiterinnen und -mitarbeitern das Erarbeiten von Regeln, die die gute Kommunikation erhalten und sicherstellen sollten.

Diese Regeln legen zum Beispiel den Umgang mit Frustrationen und die Kommunikationskultur fest. So sind etwa die Vetorechte einzelner Institute und Mitarbeiter oder auch die Form der „Subjects“ der umfangreichen email-Kommunikation festgelegt. Die Einhaltung der Regeln sorgte in den zahllosen Arbeitstreffen, Video- und Telefonkonferenzen für eine bessere und produktivere Atmosphäre.

Neben den Kommunikationsregeln brachte die Aufteilung in spezielle Arbeitsgruppen und die Einführung von „Jour Fixe“-Terminen einen großen Gewinn an Produktivität.

Einen weiteren nicht zu unterschätzenden Anteil am Erfolg hatten auch die informellen Anteile der Treffen, bei denen die Mitglieder des Teams sich besser kennenlernten.

Es wurden im Laufe des Projekts mehrere Arbeitstreffen durchgeführt. Die beiden Workshops über Projektmanagement haben den Erfolg sichergestellt und sehr zum Erreichen der Ziele beigetragen. Bei einem erneuten Projekt wäre für solche Treffen ein möglichst früher Zeitraum zu empfehlen. Aus den Erfahrungen würde ich bei längeren Projekten eine regelmäßige Durchführung solcher Workshops alle ein bis zwei Jahre empfehlen.

3. Die Seminare waren eine Mischung aus Coaching und Organisationsberatung und wurden von den Projektleitern zusammen mit Herrn Schwartz von der Firma Spyral GbR aus Esslingen durchgeführt.

9. Barrierefreie Seiten?

Der Workshop über Barrierefreiheit wurde relativ früh abgehalten. Im Laufe des Workshops wurde der Begriff Barrierefreiheit hinterfragt und auch anhand von Beispielen genauer formuliert und konkretisiert, was der Begriff Barrierefreiheit im Rahmen des Projekts bedeuten sollte.

Durch unvorhersehbare Verzögerungen lag ein unnötig großer Zeitraum zwischen dem Workshop und der Phase der Codegenerierung. Als dann die ersten Templates vorlagen, wurde schnell klar, dass mit den damals verfügbaren Personalressourcen das Ziel barrierefreier Seiten nicht in der vorgegebenen Zeit zu erreichen war. Das Ziel der barrierefreien Seiten wurde also dem extern forcierten Ziel online zu gehen und dem Nachbau der „Corporate Identity“ geopfert.

Ein Nebeneffekt der streng getrennten unterschiedlichen Instanzen ist, dass diese sich auseinander entwickeln, da sie sich – von einem gemeinsamen Prototyp ausgehend – auseinander entwickeln. Dadurch wurden gewünschte Synergieeffekte und die Möglichkeiten der Zusammenarbeit in der Zukunft reduziert.

Deshalb wurde das Teilprojekt Codebereinigung und Barrierefreiheit vorgeschlagen und durchgeführt.

Da inzwischen klar war, dass ohne dezidierte Ressourcen dieses Ziel nicht erreichbar wäre, wurde an unserem Institut ein Mitarbeiter eingestellt, der sich neben der Umsetzung unserer CMS-Seiten einzig der Entwicklung einer barrierefreien Version widmete. Dieser Teil seiner Arbeit wird von allen Instituten finanziert. Der erste Teil dieses Projekts ist erfolgreich abgeschlossen. Der finale Prototyp ist abgenommen und wird im Moment bei laufendem Betrieb aktiviert. Bis Ende Dezember 2007 soll die Internet-Präsenz unseres Instituts umgestellt und der Code für die anderen Institute verfügbar und dokumentiert sein.[4]

Im neuen Code besteht eine strenge Trennung von Inhalt (XHTML) und Form (CSS). Auf „Scripting“ wurde in jeder Form verzichtet, außer dort, wo es notwendig war, um gewisse Komfortfunktionen zu implementieren. Leider können wir Herrn Thomas Breitner, der die Sache umgesetzt hat, aus Mangel an Planstellen nicht weiter beschäftigen.

4. Dies ist inzwischen erfolgt.

10. Zusammenfassung und Ausblick

Zu Beginn wurde recht viel Zeit mit interner Organisation verbracht. Es wäre wünschenswert gewesen, das Projektmanagementseminar kurz nach dem Start durchzuführen. Eine stärkere Orientierung an einer der klassischen Projektmanagement-Methoden, wie etwa die schriftliche Fixierung von Projektzielen und eine straffere Organisation, hätten manche Prozesse und Teile des Projekts beschleunigen können.

Eine realistischere Zeitplanung zu Projektbeginn wäre gut gewesen und hätte unrealistische Erwartungen seitens der Direktoren gedämpft. Im Projektverlauf hat sich die tatsächliche Freistellung oder Neueinstellung von Mitarbeitern als absolute Notwendigkeit erwiesen. Produktiv waren auch eine Verschlankung der Hierarchie in der Leitungsebene und eine Verbreiterung der Basis.

Die Umstellung und Re-Launch der Internetseiten der jeweiligen Institute war über einen großen Zeitraum verteilt. Dies lag jedoch nicht in erster Linie am Stand des Projekts, sondern eher an jeweils institutsinternen Faktoren. So vergingen vom Beginn im Sommer 2003 bis zum endgültigen Re-Launch des letzten Instituts insgesamt vier Jahre.

Als positiver und gewünschter Nebeneffekt kam es durch das Projekt zu einer stärkeren Vernetzung der beteiligten Institute nicht nur in den mit dem Projekt befassten Bereichen. Synergieeffekte wurden und werden weiter genutzt.

Trotz aller Herausforderungen wurde das gesteckte Ziel erreicht und man kann das Projekt als einen vollen Erfolg bezeichnen.

Dieses Projekt und die Projektgruppe hat zweifellos das Potenzial, noch weitere Ziele zu erreichen. Denkbar wäre hier die bereits projektintern als „Ausbaustufe II“ bezeichnete Integration von Literatur- und Informationsdatenbanken der MPDL in das CMS.

Die größte Datenbank der Welt – ein Oracle?

Langzeitarchivierung von Kimamodelldaten am Welt-Klimadatenzentrum und Deutschen Klimarechenzentrum

Frank Toussaint [(1)], Michael Lautenschlager [(1)], Wolfgang Stahl [(2)]

[(1)] World Data Center for Climate (WDCC)
Max-Planck-Institut für Meteorologie, Hamburg

[(2)] German Climate Computing Centre (DKRZ), Hamburg

Zusammenfassung

Im Bereich der Produktion von Erdsystem-Modelldaten wächst die Computerleistung schneller als die Preise für Speichermedien zurückgehen. Ohne Änderung der Archivierungspolitik werden die Kosten für Langfristspeicherung der Daten mit dem Übergang zur nächsten Rechnergeneration die reinen Rechenkosten übersteigen.

WDCC und DKRZ haben daher ihre Langfristdatenhaltung neu geordnet und stellen ein Konzept vor, das diesen Problemen gerecht wird. Darüber

hinaus verbessert es Qualität und Nutzbarkeit der gespeicherten Daten. Das neue Konzept trennt schon auf Projektebene die Daten funktional in Test-, Projekt- und Langzeit-Archivdaten. Parallel dazu erfolgt eine Aufteilung nach Speicherdauer in vier Ebenen.

Die Umstellung auf den neuen Archivierungsansatz hat bereits begonnen. An ihrem Ende werden die vollständig dokumentierten und katalogisierten Langzeit-Archivdaten stehen.

Stichwörter: Klimamodelldaten, Langzeitarchivierung, Datenkonservierung, Qualitätssicherung, Nutzbarkeit

1. Einleitung

Die Menge von Output aus Klimadatenmodellen hängt von raumzeitlicher Auflösung (Fig. 2), Variablenzahl und Speicherformat ab sowie von der Detailtreue, mit der das Modell physikalische und chemische Prozesse abbildet (Fig. 1). Mit wachsender Rechnerleistung steigen die Wünsche der Nutzer in jeder dieser Dimensionen.

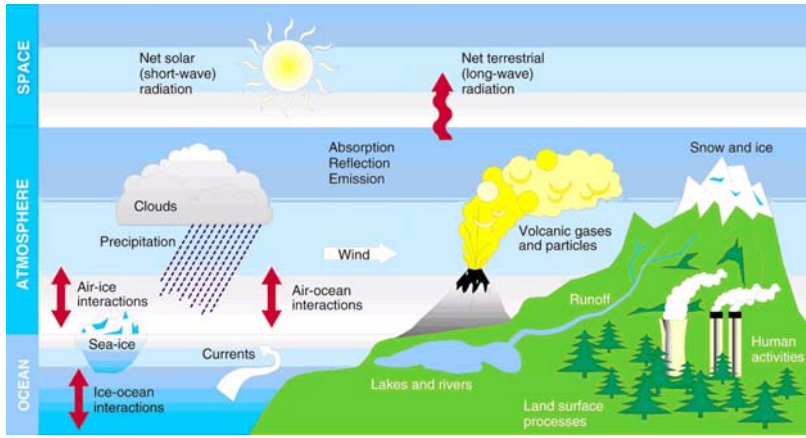


Fig. 1: In Klimamodellen sind zahlreiche unterschiedliche Prozesse zu beachten

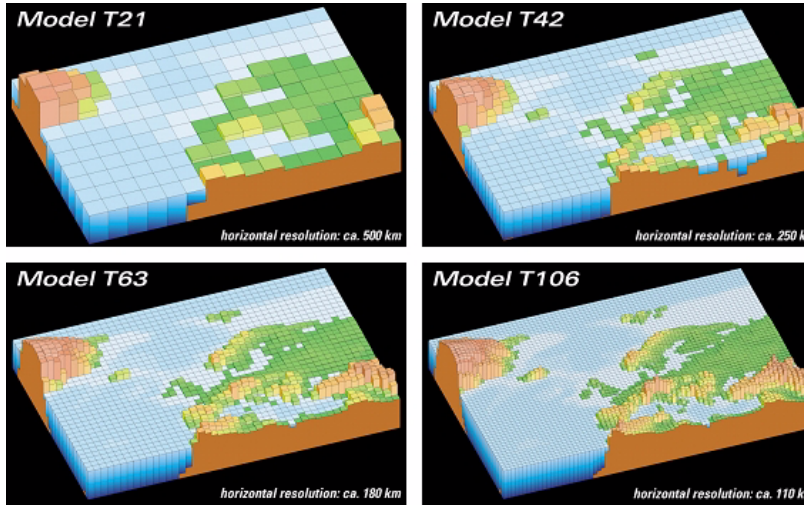


Fig. 2: Nordatlantikregion des Hamburger Klimamodells (ECHAM) in vier verschiedenen Horizontalauflösungen (Gitterabstände von 500 km, 250 km, 180 km und 110 km)

In der Vergangenheit wuchs der am DKRZ gespeicherte Modelldatenoutput etwa linear mit der installierten Computerleistung an, ohne dass eine Änderung dieses Zusammenhangs abzusehen wäre. Gegenwärtig werden die am DKRZ produzierten Daten nahezu direkt ins Langzeitarchiv migriert, wo sie auf Magnetbändern gespeichert werden. Dabei werden Daten aus dem Projektlauf und -management nicht von Langzeitdaten getrennt, Verfalldaten werden nicht vergeben (Fig. 3). Eine Fortsetzung dieses Schemas würde in Management und Finanzierung zu Problemen führen und damit zu mangelnder Akzeptanz. Letztlich würden die Kosten der Datenverwaltung die Rechenkosten übersteigen, was nicht akzeptabel wäre.

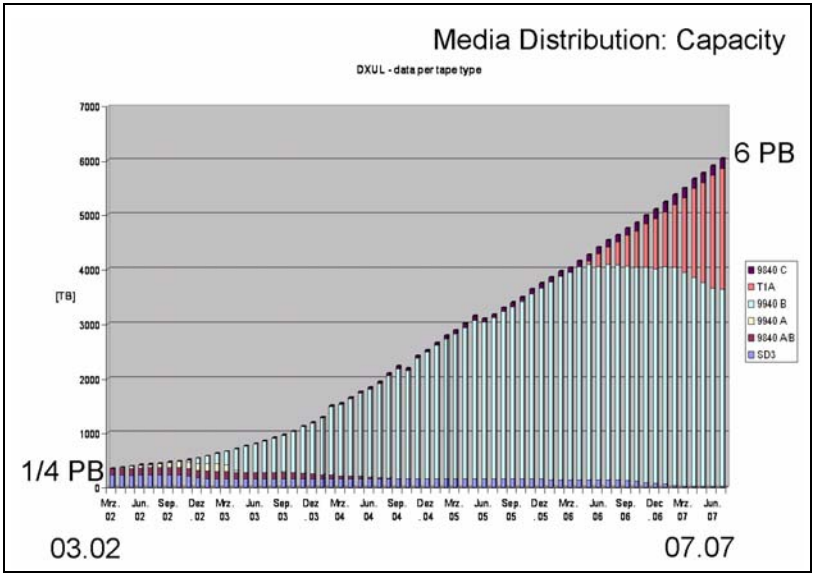


Fig. 3: Entwicklung des Massenspeichers am DKRZ von Februar 2002 bis Juli 2007 einschließlich Wechsel von Speichertechniken.

Die kommende Rechnergeneration am DKRZ wird konservativ geschätzt eine Leistungssteigerung von Faktor 10 – 15 mit sich bringen, optimistisch könnte es ein Faktor 60 werden. Daher muss für das Archiv bei gleichbleibender Datenpolitik mit linear steigendem Zuwachs von heute 1 auf 13 oder mehr PByte jährlich gerechnet werden (Fig. 4).

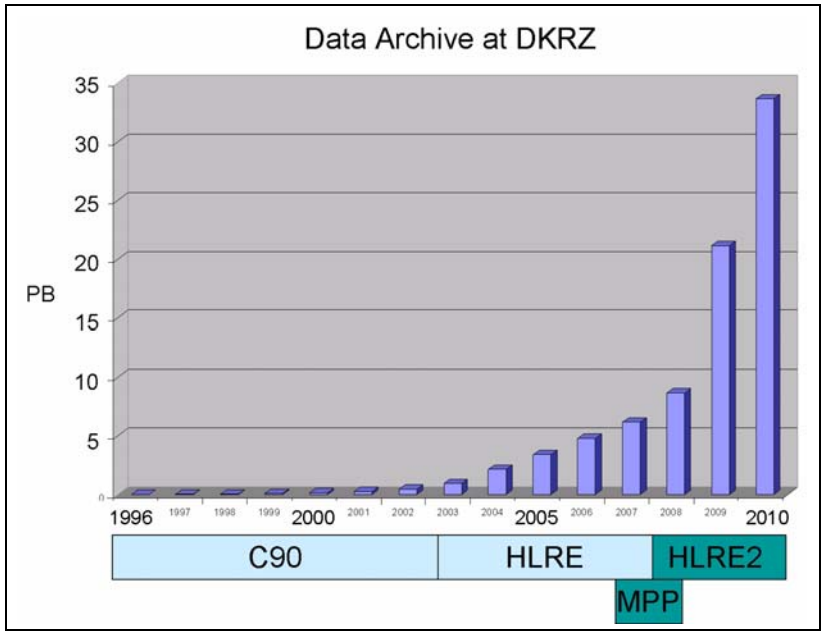


Fig. 4: Extrapolierte Entwicklung des DKRZ-Gesamtarchivs 1996 bis 2010. Die Angaben der Rechenserver-Architekturen beziehen sich auf Cray C90 (C90), NEC SX-6 (HLRE), Sun Cluster (MPP) sowie auf die kommende Rechnergeneration (HLRE2)

Die Techniken des Managements solcher Datenmengen sind zwar grundsätzlich bekannt, aber der finanzielle Aufwand steht in keinem angemessenen Verhältnis mehr zu den Rechenkosten. Obwohl die Medienkosten pro Speichervolumen sinken, wachsen die Gesamtkosten durch steigende Rechnerleistung und wachsenden Datenoutput an (Fig. 5). Dadurch würde der Kostenanteil der Datenhaltung am DKRZ auf 25 bis 50 % ansteigen.

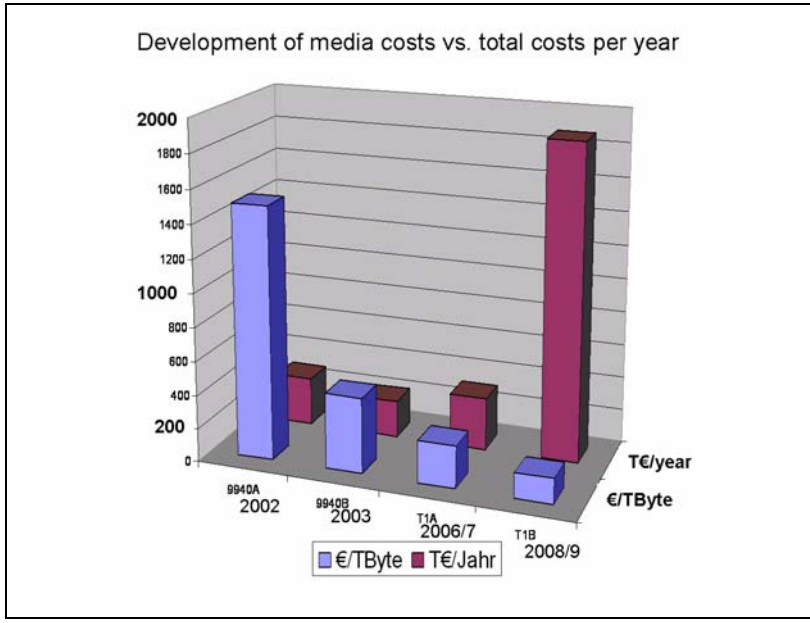


Fig. 5: Kostenentwicklung der Speichermedien pro TByte und gesamt am DKRZ für 2002, 2003, 2006/7 and 2008/9

Über die Datenhaltungskosten hinaus wächst der Aufwand für Qualitätssicherung, Katalogisierung und Benutzerfreundlichkeit für das Gesamtarchiv. Auch unter diesem Aspekt muss es zu einer Änderung des Archivierungskonzeptes kommen. Dafür wurde davon ausgegangen, dass Projektdaten begrenzter Lebensdauer frühzeitig von solchen Daten getrennt werden, die sich für eine Langfristspeicherung eignen. Dies sollte in einer bewussten Entscheidung der Projektleitung erfolgen, die die Regeln guter wissenschaftlicher Praxis [1] berücksichtigt.

2. Strategien zur Langzeit-Archivierung für Computer der 50 TFlops-Klasse

Kernaktivität des DKRZ ist die Erdsystemmodellierung. Dazu gehören Klimasimulationen von Vergangenheit, Gegenwart und Zukunft. Dabei arbeiten an den Rechnern neben Wissenschaftlern der DKRZ-Anteilseigner auch Angehörige anderer Forschungsinstitute. Die dabei anfallenden Daten kann man nach ihrer Lebensdauer in drei Klassen unterteilen: Testdaten, Projektdaten und Endergebnisse.

- Testdaten: Lebensdauer Wochen oder Monate

  Der Anfall von Testdaten ist in der Regel eng mit der Entwicklung des numerischen Codes verbunden. Dies betrifft beispielsweise die Implementierung neuer Algorithmen oder Parametrisierungen. Dabei wird eine große Zahl kurzer Modellläufe durchgeführt, um die Neuerungen zu testen. Die dabei anfallenden Daten werden in der Regel nur einige Wochen oder Monate benötigt, bis die Programmänderungen zuverlässig funktionieren. Im folgenden Entwicklungsschritt werden dann die wissenschaftlichen Fragestellungen untersucht, die zu den Neuerungen des Programms gehören.

- Projektdaten: Lebensdauer während der Projektlaufzeit (drei bis fünf Jahre)

  Die Arbeiten am DKRZ sind projektweise aufgeteilt. Jedem Projekt werden nach einer Bewertung Ressourcen zugeteilt. Nach technischer Verifikation des numerischen Modells werden mit seiner Hilfe wissenschaftliche Fragestellungen angegangen. Dabei verringert sich zwar die Zahl der Rechnerläufe, aber CPU-Zeit und Verweilzeit im System steigen deutlich an. Typische Projektlaufzeiten liegen bei drei bis fünf Jahren, was daher auch die Lebensdauer der meisten Projektdaten ist.

- Endergebnisse: Lebensdauer zehn Jahre und mehr

  Nicht alle Projektdaten werden in die Langfristspeicherung übernommen. Dies gilt nur für ausgewählte Daten, die zum Beispiel in internationalen Kooperationen wie den IPCC Reports erstellt werden. Sie sind dann meist Teil wissenschaftlicher Publikationen. Nach den Regeln guter wissenschaftlicher Praxis müssen solche Daten zu Verifikationszwecken wenigstens zehn Jahre verfügbar und zugreifbar sein. Sie sind Teil des gesammelten Wissens und werden auch interdisziplinär genutzt.

  Die beiden Aspekte der Langzeitarchivierung, Wissensspeicherung und Verifizierbarkeit, stellen vor allem bei interdisziplinärem Arbeiten erhöhte Anforderungen an Datenschutz, Qualitätssicherung und Benutzerfreundlichkeit, als es bei den beiden vorhergehenden Kategorien der Fall ist. Vor allem, weil die Daten nicht ohne Weiteres reproduzierbar sind und Dritte vielfach nicht das zu ihrer Handhabung und Einschätzung nötige Hintergrundwissen haben. Daraus folgen Anforderungen an Beschreibung und Katalogisierung.

Die Zugriffsanforderungen der vorgenannten drei Datenklassen spiegeln sich in einer vierstufigen Datenhierarchie wider. Nach den erwarteten

Lebensdauern richten sich dabei die Verfallsdaten, bei deren Überschreitung die Daten nach einer weiteren Ankündigung gelöscht werden. Die vier für das DKRZ verwendeten Hierarchieebenen sind temporäre, Arbeits-, Archiv- und Dokumentations-Ebene. Ihre volumenmäßige Verteilung ist in Fig. 6 aufgeschlüsselt.

- **Temporäre Daten** (TEMP)

  Die schnellen Festplatten zur Speicherung der temporären Daten bilden den Basisarbeitsbereich für laufende Rechnungen. Die Daten müssen anschließend verlagert oder gelöscht werden. Gegenwärtig wird diese Speicherebene vom Scratchbereich des Rechenservers repräsentiert.

- **Arbeitsdaten** (WORK)

  In der WORK-Speicherebene steht am DKRZ jedem Projekt auf seine Laufzeit begrenzter, projektverwalteter Plattenplatz zur Verfügung, so dass für bestimmte Rechnungen und Auswertungen keine Daten auf die Bänder des Massenspeicherarchivs migriert werden müssen. Diese Ebene ist noch nicht voll implementiert. Eine Vorversion besteht mit dem NEC Global File System (GFS).

- **Archivdaten** (ARCH)

  In der ARCH-Ebene erhalten die Projekte Platz im Bandarchiv, damit Arbeitsgruppen beispielsweise Kopien von Projektfiles undokumentiert speichern können.

  Dabei soll für erst später im Projekt zu verwendende Daten Massenspeicherplatz zur Verfügung gestellt werden, der über die Plattenvolumina hinaus geht. Nach Ankündigung sollen diese Daten ein Jahr nach Projektende gelöscht werden, können jedoch falls nötig in die DOCU-Speicherebene übernommen werden.

- **Dokumentationsdaten** (DOCU)

  Die Daten des DOCU-Bereiches werden gemäß bibliothekarischer Regeln dokumentiert und zehn oder mehr Jahre gespeichert. Sie befinden sich im Bandarchiv des DKRZ, eine Sicherheitskopie wird angefertigt. Kern der Dokumentation ist der bestehende Datenkatalog des WDC Climate. Für die nächste Rechnergeneration wird dieses Konzept auf alle Daten ausgedehnt werden, gleichgültig ob sie in der Datenbank selbst liegen oder im Filesystem gespeichert sind. Dadurch wird das Langzeitarchiv des DKRZ vollständig dokumentiert sein. Die Daten in diesem Bereich sind eingefroren und unterliegen keinen weiteren Veränderungen mehr.

Ziel ist es, mit der DOCU-Datenebene eine Infrastruktur zu schaffen, die den zunehmend strengeren Anforderungen an Daten gerecht wird, die Grundlage hochwertiger, einem weiten Publikum angebotener wissenschaftlicher Publikationen sind.

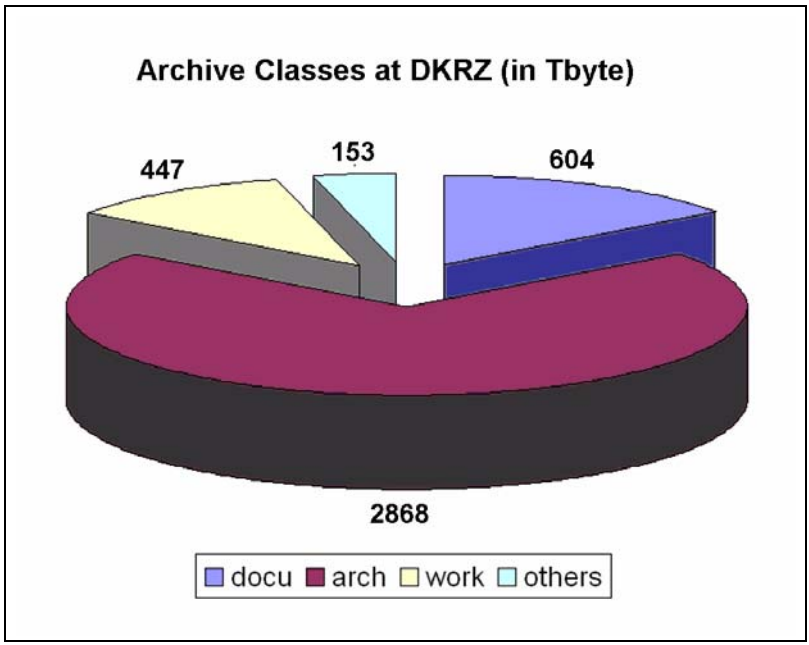


Fig. 6: Mengenverteilung der Daten des DKRZ-Bandarchivs nach Klassen Anfang 2007

Neu am Massenspeicherkonzept des DKRZ sind vor allem drei Dinge: Die Aufteilung zwischen Projekt- und Langzeitdaten, das automatische Löschen nach Überschreitung des Verfallsdatums, wenn nicht aktiv widersprochen wird (ARCH-Ebene), und die Dokumentationsanforderungen an die langfristig gespeicherten Daten (DOCU-Ebene). Letztere gehen auf die Erfahrung zurück, dass undokumentierte Daten außerhalb der Projektumgebung in der Regel ihren Informationswert verlieren.

Die Katalogisierung und Dokumentation erfolgen im Rahmen des am WDC Climate bereits bestehenden, im Internet publizierten Datenkataloges und Metadatenmodells CERA-2 (Climate and Environmental data Retrieval and Archiving) [2]. Es enthält Funktionalitäten für Durchsicht, Suche, Identifizierung und Download der Informationen des Datenbanksystems sowie der außerhalb der DB ohne physikalische Verbindung in einfachen Dateien

gespeicherten Daten. Die zur Nutzung erforderlichen Metadaten sind im Datenmodell enthalten, so dass nach Größen wie Variablen, raumzeitlicher Auflösung, Zuständigkeiten oder Datenqualität problemlos gesucht werden kann.

Das CERA-Datenmodell erfüllt den ISO-19115-Standard für Metadaten [3]. Daher kann der Katalog von internationalen Datenportalen angesprochen werden, die diesen Standard einhalten. Das Füllen des Kataloges erfolgt in der Regel über XML-Dateien, bei einer anschließenden Kontrolle können die Einträge noch manuell korrigiert werden. Die automatisierte Eingabe in die DB ist im Internet dokumentiert (http://input.wdc-climate.de), der Datenexport kann ebenfalls in XML erfolgen und daher leicht in jedes benötigte Format umgewandelt werden.

Klimadaten im DOCU-Bereich können sowohl als Teil der Datenbank archiviert sein als auch als flache Dateien, die vom Katalog der DB nur referenziert werden. Endergebnisse, die international freigegeben werden, befinden sich überwiegend als *Binary Large Objects* (BLOBs) zusammen mit ihren Metadaten in DB-Tabellen, von wo aus sie über das Internet weltweit zugreifbar sind. Dabei können mittels Browser einzelne oder mehrere Zeitschritte kopiert werden. Anders bei den nur referenzierten Daten des Langzeitarchivs: Sie sind einfache Dateien, die im CERA-Datenkatalog beschrieben sind, jedoch über dessen Nutzerinterface nicht direkt zugänglich sind.

In allen Fällen sind die Einträge des DOCU-Bereiches keinen Veränderungen mehr unterworfen. Sollten solche aus Korrekturgründen trotzdem erwünscht sein, wird mit Anhängen gearbeitet oder ein Neueintrag erstellt

und dies im Katalog dokumentiert. Ein anderes Vorgehen verstieße gegen die Regeln guter wissenschaftlicher Praxis.

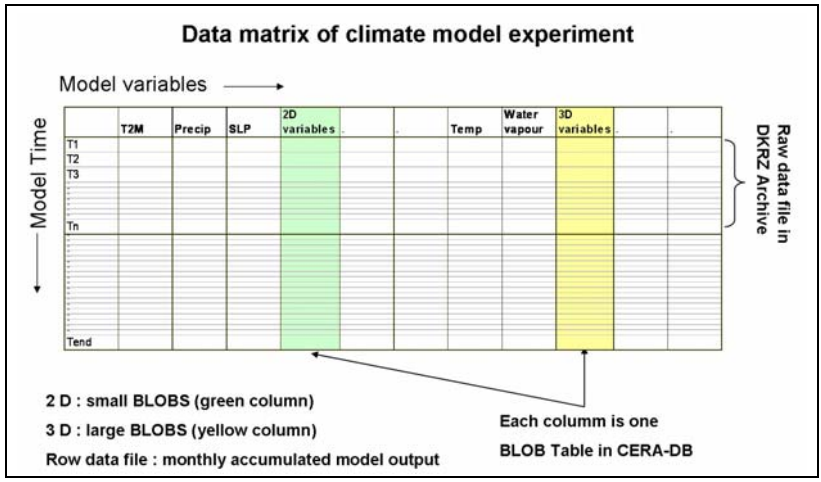


Fig. 7: Die Klimamodelldaten sind nach Variablen in Tabellen aufgegliedert. In ihnen befinden sich zeilenweise die Zeitschritte

3. Primärdatenpublikation am WDC Climate

Für die Veröffentlichung von Primärdaten, die von allgemeinem Interesse sind, bietet das WDC Climate einen Publikationsservice an. Diese Daten finden sich in der Regel in der wissenschaftlichen Literatur zitiert, so dass auf sie selbst auch in den üblichen Bibliothekskatalogen verweisen werden kann. Dieses gemeinsam mit der Technischen Informationsbibliothek Hannover (TIB) entwickelte Verfahren ordnet den Datenpublikationen sogenannte STD-DOI (Scientific and Technical Data - Digital Object Identifier, http://www.std-doi.de) [4], [5] zu, mit denen auf sie verweisen werden kann (vgl. Ablaufdarstellung in Fig. 8). Zusammen mit ihren Metadaten durchlaufen die Daten einen Review-Prozess der Qualitätssicherung, bevor ihnen eine persistente Kennung (DOI) zugewiesen wird. Die DOI werden bei der TIB zentral registriert und offen über Internet weltweit auch anderen Informationssystemen verfügbar gemacht. Dadurch sind sie in der wissenschaftlichen Literatur zitierfähig.

Das Konzept der STD-DOI integriert die Primärdatenpublikation in allgemeinere Publikationssysteme, wie sie in Textpublikationen bereits üblich sind. Zu den am WDC Climate gehaltenen Daten gelangt man im Katalog der TIB (TIBORDER, URL: http://tiborder.gbv.de/psi/DB=2.63/LNG=DU/)

mit dem Schlüsselwort WDCC (Fig. 9). Über den DOI ist ein direkter Download der Daten möglich.

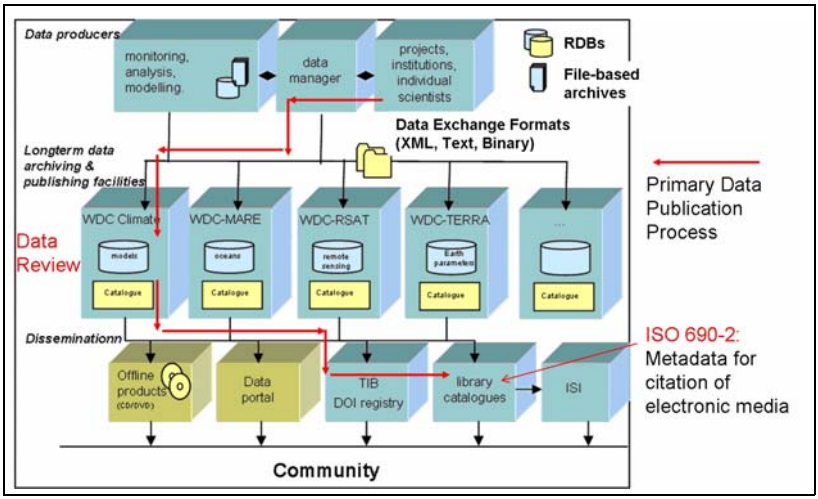


Fig. 8: Datenfluss und Ablaufplan der STD-DOI-Veröffentlichung von Primärdaten

Fig. 9: Repräsentation von WDCC-Daten im Bibliothekskatalog der TIB (Bilder oben) sowie die wissenschaftlichen Metadaten im WDCC-Datenkatalog (Bilder unten)

4. Datenschutz, Qualitätssicherung und langfristige Zugreifbarkeit

Das vorliegende Langzeit-Archivierungskonzept von DKRZ und WDC Climate stellt eine intensive Datenpflege für Daten des DOCU-Bereiches in den Vordergrund. Dies begrenzt natürlich die Menge an Daten, die in dieser Weise behandelt werden können.

Bitgenaue Wiederherstellung von Dateien wird durch Doppelhaltung der Daten gewährleistet, die auf voneinander unabhängigen Bändern verschiedener Hersteller an unterschiedlichen Lagerorten erfolgt. Darüber hinaus wird die Zahl der Bandzugriffe protokolliert, so dass die Daten nach Erreichen einer bestimmten Zugriffszahl auf Neubänder kopiert werden können. Gegenwärtig sind Kopien mit gleicher Technik am gleichen Lagerort unter Anwendung von *tape refreshment* im Gebrauch (Fig. 10).

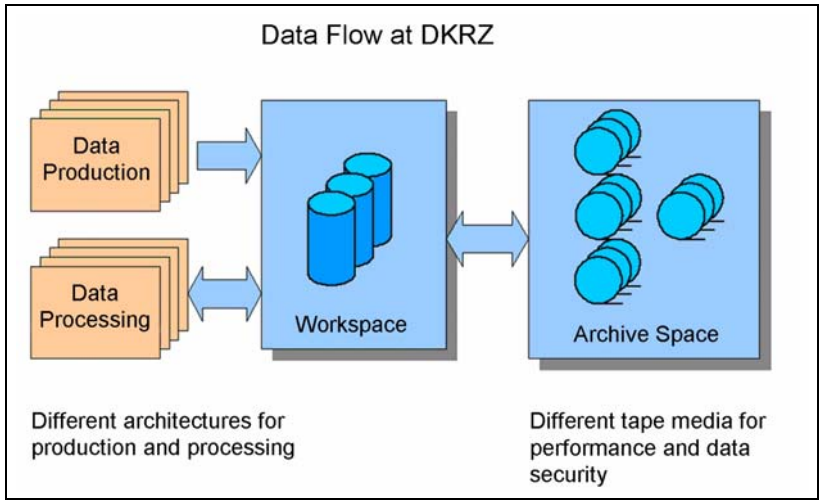


Fig. 10: Datenflüsse am DKRZ und zu installierende Datenebenen

Aufgrund der großen Datenmengen ist eine Qualitätsprüfung auf Zahlenebene nicht möglich. Stattdessen erfolgen Stichproben unterschiedlicher Komplexität.

Qualitätssicherung bezieht sich bei Modelloutput primär auf semantische und syntaktische Prüfungen. Dabei heißt semantisch, das Verhalten des numerischen Modells im Vergleich zu Beobachtungen und anderen Modellen zu untersuchen, was überwiegend Aufgabe des wissenschaftlichen Validierungsprozesses ist. Die Ergebnisse finden sich üblicherweise in der wissenschaftlichen Literatur. Die syntaktische Prüfung hingegen bezieht sich auf die formalen Aspekte der Datenarchivierung und soll deren Fehlerfreiheit so weit wie möglich sicher stellen. Dazu gehört bei Modelldaten die Prüfung von

- Konsistenz von Daten und Metadaten,
- Vollständigkeit der Daten,

- Standard-Wertebereichen und
- raumzeitlicher Datenstruktur.

Diese Prüfungen sind trotz teilweiser Automatisierbarkeit relativ zeitaufwändig, sind aber unverzichtbar, um das Vertrauen der Nutzer in die Daten zu sichern.

Qualitätssicherung wird im Langzeitarchiv von WDC Climate und DKRZ in drei Stufen umgesetzt.

1. Die semantische Prüfung wird bereits zur Projektlaufzeit im wissenschaftlichen Bereich durchgeführt, um Validität und Nutzbarkeit der Daten sofort sicher zu stellen. Ein positiver Ausgang dieser Tests ist Basiskriterium, um die Endergebnisse vom ARCH- in den DOCU-Bereich zu übernehmen.
2. Während der Integration der Daten ins Langzeitarchiv erfolgen Datendokumentation und automatisierte syntaktische Prüfung. Gegenwärtig erfolgen für die wichtigsten Variablen Stichproben auf Konsistenz, Vollständigkeit, Wertebereich und raumzeitliche Struktur.
3. Sowohl Daten als auch Metadaten, die für den STD-DOI-Publikationsprozess bestimmt sind, werden besonderen Prüfungen unterzogen. Zurzeit geschieht das am WDC Climate als komplette syntaktische Prüfung aller Zeitserien der Publikation. Für einzelne, oft nachgefragte Variablen werden die Untersuchungen in Zusammenarbeit mit den STD-DOI-Autoren durchgeführt. Dabei werden normalerweise zweidimensionale Plots der Modellfelder mit den erwarteten räumlichen Verteilungen verglichen. Die Ergebnisse werden in den Metadaten dokumentiert.

Die Zugreifbarkeit der Daten in der DB wie in einfachen Dateien wird durch eine komplett durchsuchbare Dokumentation im Katalog des WDC Climate sicher gestellt. Zusätzlich wird ein webbasierter, feingranularer Download von 2D-Feldern einzelner Zeitschritte angeboten. Gegenwärtig stehen am WDC Climate über 320 TByte solcher Daten zur Verfügung, die in etwa 1.000 Modellexperimenten zusammengefasst und auf 120.000 DB-Tabellen mit 5,6 Mrd. einzelnen Einträgen (BLOBs) verteilt sind. Die durchschnittliche Größe eines solchen einzeln zugreifbaren Eintrags beträgt 60 KB.

Auch auf der technischen Ebene muss die Zugreifbarkeit unterstützt werden. Technische Neuerungen im Archiv müssen durch Abwärtskompatibilität die andauernde Lesbarkeit gewährleisten. Auch die Software muss jeweils auf der neuen Plattform zur Verfügung stehen, denn Serviceprogramme und -bibliotheken müssen auch ältere Daten verarbeiten können.

5. Zusammenfassung

Im neuen Archivkonzept des DKRZ werden den Inhalten Verfallsdaten zugeordnet. Nur ausgewählte, gut dokumentierte Daten werden in die Langzeitarchivierung übernommen. Dabei werden vom WDC Climate die Grundlagen des wissenschaftlichen Datenmanagements übernommen. Auch bei einer Steigerung der Rechenleistung um den Faktor 30 oder mehr sollte sich das Wachstum des Archivs auf das Zehnfache, das der DB des WDC Climate auf das Fünffache der heutigen Werte beschränken lassen.

Weil das Gesamtwachstum der Daten begrenzt wird, erhöht sich gleichzeitig die Zuverlässigkeit der Datenhaltung. Dazu gehören Dokumentation, bitgenaue Reproduzierbarkeit, Qualitätssicherung sowie komfortable Zugreifbarkeit.

Literatur

[1] Senate of the Max Planck Society: Rules for Good Scientific Practice. November 2000 http://www.mpibpc.mpg.de/groups/jahn/PDF/gutwiss.pdf

[2] Lautenschlager, M., F. Toussaint, H. Thiemann and M. Reinke: The Cera-2 Data Model. Technical Report No. 15, DKRZ, Hamburg, 1998

[3] Technical Committee Geographic Information (TC 211): ISO 19115 – Geographic Information – Metadata. International Standards Organisation, 2003.

[4] Lautenschlager, M. und I. Sens: Konzept zur Zitierfähigkeit wissenschaftlicher Primärdaten. Information – Wissenschaft & Praxis, 54 (2003) , S. 463-466

[5] Klump, J., R. Bertelmann, J. Brase, M. Diepenbroek, H. Grobe, H. Höck, M. Lautenschlager, U. Schindler, I. Sens and J. Wächter: Data Publication in the Open Access Initiative. CODATA Data Science Journal, p 79-83, 2006

Virtualisierung in der MPG – ein Thema?

Andreas Oberreuter

Max-Planck-Institut für Radioastronomie, Bonn

Vom 27.-28.09.2007 fand bei der GWDG (Göttingen) ein erstes Arbeitskreistreffen zum Thema „Server- und Speicher-Virtualisierung“ statt. Neben der GWDG nahmen zehn Max-Planck-Einrichtungen daran teil und diskutierten den Einsatz von Server- und Speicher-Virtualisierung in den eigenen Instituten.

Anlass waren zum einen die inzwischen über dreijährige, durch den BAR finanzierte und inzwischen der Pilotphase längst entwachsene Server-Virtualisierung am MPI für Radioastronomie und die zahlreichen Erfahrungen mit der Storage-Virtualisierung an der GWDG. In beiden Einrichtungen stehen nun massive weitere Ausbauschritte an, die als Beispiele dienten.

Auch an vielen anderen MPIen sind inzwischen kleinere und größere Test- und Produktionsumgebungen entstanden, andere informieren sich, ob die Virtualisierung nur ein Hype oder eine ernst zu nehmende neue Dimension in den Rechenzentren, aber auch den Arbeitsplätzen ist.

Das Treffen beschäftigte sich an einem Tag schwerpunktsmäßig mit der Server- und am nächsten Tag der Storage-Virtualisierung. In beiden Fällen stellten die Teilnehmer ihre eigenen Umgebungen bzw. Erwartungen bzgl. dieser

Thematik vor. Es bestand Konsenz, dass sich hier eine hilfreiche, wenn auch komplexe, aber doch zukunftsweisende Technologie abzeichnet. Es wurden die aktuelle Marktlage sowohl hinsichtlich der Technik als auch der Beschaffungs- und Lizenzpolitik beleuchtet. Trotz verschiedener Anbieter zeichnet sich noch ein recht übersichtliches Angebot ab, das sich vor allem bei der Server-Virtualisierung in der MPG auf einen Hersteller fokussiert - VMware. Bei der Storage-Virtualisierung sind vor allem Datacore und Falconstor in der MPG vertreten.

Die Teilnehmer zeigten durchweg großes Interesse, diese neue Technologie gemeinsam anzugehen und als langfristiges Ziel auch die Bereitstellung gemeinsamer Ressourcen (Dienste = Images, Dienstleistungen = Hilfestellung aus Pilotprojekten) anzustreben. Dies könnten bspw. Referenzinstallationen sein, die beim Setup neuer Umgebungen zu Rate gezogen werden können, oder Handreichungen in Form von Foren und Wikis. Vor allem in der Server-Virtualisierung würde es sich anbieten, Standarddienste wie bspw. einen Web- oder Mailserver als virtuelle Maschine ortsunabhängig zu entwickeln und dann als Image von einer MPG-internen Seite herunterzuladen, in seine ESX-VMware-Serverfarm zu integrieren und gemäß den institutsinternen Umgebungen nur noch leicht zu modifzieren. So könnten u. a. institutsübergreifende Standards geschaffen und Know-How der Entwickler und Bereitsteller des Images genutzt werden, statt eigene wertvolle Zeit in die Definition und den Aufbau zu stecken. In Nachfolgetreffen könnte man über die Anforderungen der Applikationen, der notwendigen infrastrukturellen Voraussetzungen, diskutieren, unter denen das Sinn macht. Eine gute Synergie des IT-Wissens in der MPG könnte hier auf jeden Fall erreicht werden.

Am Rande des Treffens wurden dann auch mögliche andere Szenarien für Virtualisierung gestreift wie virtuelle Desktops, Filesysteme, Tapes etc. Dieses Mal waren das noch untergeordnete Themen, aber auch hier zeigen sich langfristige Änderungen in der Denkweise, wie IT zukünftig in den Einrichtungen der MPG umgesetzt werden könnte. Somit sind auch neue Ziele anvisiert, aber noch nicht klar definiert und in Angriff genommen worden.

In der tiefergehenden Diskussion darum, für wen denn nun die Virtualisierung Sinn macht, zeigte sich, dass jede Einrichtung, die sich mit diesem Gedanken auseinandersetzt, abwägen muss, was es langfristig zu ersetzen gilt, welchen Aufwand man insbesondere in der Startphase zu tragen bereit ist, finanziell, aber vor allem auch personell, um dann dauerhaft die Früchte dieser Investition zu ernten. Auch wenn die genaue kritische Masse nicht zu bestimmen ist, sollten bestimmte Randbedingungen vorliegen:

- es gibt viele Server(dienste) am MPI
- es lassen sich weitestgehend viele Applikationen in einer virtuellen Umgebung betreiben (Migration, Durchsatz)
- es ist eine recht große Storage-Infrastruktur zu integrieren bzw. in Kürze bereitzustellen
- es sind typischerweise Zoos von Storage-Einheiten zu verwalten und lassen sich nicht durch homogene Lösungen für einen längeren Zeitraum abdecken
- es wird Personal geschult, um die neuen Anforderungen umsetzen zu können

Die Einstiegskosten in die Virtualisierung sind sowohl bei Server wie Storage derzeit noch recht hoch, vor allem an Lizenzgebühren. Hier muss eine vernünftige Relation bei den zu konsolidierenden Servern und den angeschlossenen Kapazitäten liegen, um wirtschaftlich tragfähige Lösungen aufzubauen. Wenn dieser break even allerdings geschafft ist, dann muss sichergestellt sein, dass das nicht ein Mitarbeiter noch nebenbei erledigt, sondern gezielt und dauerhaft in die neue Materie eingearbeitet wird. Wenn auch diese Hürde genommen ist, dann wird man sich am Ende nicht vor Anfragen retten können, diese Lösungen nutzen zu wollen.

Somit steht nach einer sorgfältigen Bestandsaufnahme und Kalkulation am Ende ein neues Niveau an Angebot, Verfügbarkeit und Auslastung dem Nutzer bereit, das auch wirtschaftlich tragbar ist. Die bisherigen Vorreiter unter den MPIen und der GWDG sind wichtige Investitionen und Pfadfinder, um diese Technik breiter in die MPG hineinzutragen. Darum lohnt es sich, in solche Referenzinstallationen zu investieren, evtl. zukünftig nicht nur finanziell, sondern auch personell, um für viele gleich zu Beginn das Optimum herauszuholen.

Der Arbeitskreis „Virtualisierung“ wird neben den vorhandenen Installationen auch weiterhin Lösungsszenarien anderer Anbieter, vor allem der Open-Source-Gemeinde beobachten, um nicht einseitig, aber doch fundiert selektierend die jeweils sinnvolle Technologie zu evaluieren und weiter zu empfehlen.

Es ist angedacht in 2008 einen mehrtägigen Workshop mit Herstellern und Lösungsanbietern durchzuführen, der anhand von konkreten Fallbeispielen und Pflichtenheften aus den MPIen die verschiedenen Ansätze der Hersteller miteinander in den Wettbewerb stellt, um diese 1:1 zu vergleichen. Das können bspw. Referenzinstallationen eines einzelnen Institutes, eines Verbundes

oder angeschlossener Außenstationen sein. U. a. sollen redundante Rechenzentren, hochverfügbare Dienste und skalierbare IT-Landschaften vorgestellt werden, ebenso wie die Integration von bekannten Technologien wie FC, iSCSI und Infiniband im Storageumfeld. Die vielversprechendste Lösung soll im Anschluss an die Präsentation unter den Teilnehmern aus der MPG intern diskutiert und evtl. danach an einer Einrichtung aufgebaut werden.

Die Thematik der Visualisierung hat neben der rein technischen Umsetzung auch die Frage nach der zukünftigen Verrechnung der angebotenen Dienstleistung aufkommen lassen. Firmen wie Vizioncore bieten erste „Billing"-Modelle an.

Das Arbeitstreffen endete mit dem Wunsch eines gemeisamen Wikis, um den Erfahrungsaustausch festzuhalten. Dies wurde zwar umgehend im Anschluss durch die GWDG realisiert, ist derzeit aber nicht aktiv.

Letztlich bleibt festzuhalten, dass das virtuelle Rechenzentrum auch in der MPG näher rückt und manche Vorteile bringen wird. Virtuelle Mitarbeiter wünschen wir uns aber allesamt keine, denn auch die Virtualisierung muss von motiviertem, gut ausgebildetem und bezahltem Personal geplant, implementiert und betrieben werden.

Und irgendjemand muss ja auch einen Bericht schreiben.

Speichervirtualisierung

Reinhard Sippel

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

1. Einleitung

Mit immer schneller wachsenden Datenbeständen ist die Realisierung eines zentralen Datenmanagementsystems in verteilten, heterogenen DV-Umgebungen oft unverzichtbar. Storage-Area-Network-(SAN)- und Network-Attached-Storage-(NAS)-Systeme erhöhen die Effizienz der Administrationstätigkeit, optimieren den Datenzugriff, erhöhen die Ausfallsicherheit und verbessern die Datensicherheit in verteilten Systemen. Zur Flexibilisierung und Optimierung der Massenspeicherverwaltung bietet sich das Konzept einer Speichervirtualisierung an. Dieser Artikel beschreibt die Integration einer Speichervirtualisierung in die SAN-Infrastruktur der GWDG.

2. Allgemeines über Speichernetze

In einer SAN-Umgebung sind Rechner und Storage-Systeme über Switches durch Fibre-Channel-Kabel verbunden. Ein solches Netzwerk wird *Fabric* genannt. Rechner, die in das SAN integriert sind, müssen über FC-Adapter (Hostbus Adapter, HBA) verfügen. Auf die über das SAN zur Verfügung gestellten Speicherbereiche kann wie auf lokale Platten zugegriffen werden.

Der Betrieb eines SAN erhöht die Effizienz der Administrationstätigkeit, optimiert den Datenzugriff, erhöht die Ausfallsicherheit und verbessert die Datensicherheit in verteilten Systemen.

3. Die SAN-Umgebung bei der GWDG

Der Einstieg in die Fibre-Channel-Architektur bei der GWDG begann mit der Massenspeicherbeschaffung im Jahr 2001. Zwei Massenspeichersysteme „COMPAQ EMA12000“ (HSG80) und zwei SAN-Switches „Brocade Silkworm 2800“ bildeten zusammen mit Rechnern von Compaq das Kernstück der ersten Fabric. Die SAN-Umgebung der GWDG ist historisch gewachsen. Die Topologie hatte das Design einer so genannten *Meshed Fabric*.

In einer Meshed Fabric sind Storage Devices, Switches und Rechner so über Fibre Channel gleichwertig verbunden, dass keine Komponente eine zentrale Position hat. Die Switches sind in der Regel sowohl mit Rechnern und Storage Devices als auch mit anderen Switches vernetzt.

Zur Erhöhung der Ausfallsicherheit und zur Vereinfachung der Administration wurde die Fabric der GWDG Schritt für Schritt in zwei redundante Fabrics, die jeweils einem so genannten *Core-Edge*-Design entsprechen, umkonfiguriert.

In einer Core Edge Fabric sind mehrere leistungsfähige Switches an einer zentralen Position platziert. Sie bilden den Kern der Fabric. Core Switches sind ausschließlich mit Switches verbunden. Der Rand des Fabric-Kerns ist mit so genannten *Edge Switches* vernetzt; diese stellen die Verbindung zu den Geräten und Rechnern her.

4. Vorteile einer Virtualisierungslösung

Eine Speichervirtualisierung ermöglicht eine flexible und effiziente Verwaltung von Massenspeicherressourcen. In die Virtualisierung können Plattenbereiche von RAID-Systemen unterschiedlicher Hersteller eingebunden werden. Auf diesen physikalischen Speicherbereichen können logische Speicherbereiche, so genannte SAN-Resources definiert werden. Die SAN-Resources werden an Rechner (SAN-Clients) mit unterschiedlicher Hardware-Architektur und unterschiedlichem Betriebssystem freigegeben.

Aus der Sicht der Rechner zeigt sich die Speichervirtualisierung wie ein großes, einheitliches RAID-System. Auf den Klienten ist man jetzt nicht mehr auf spezielle raid-system-spezifische Driver-Software angewiesen. Durch die Verwendung einer Speichervirtualisierung wird der Einsatz kostengünstiger RAID-Systeme möglich.

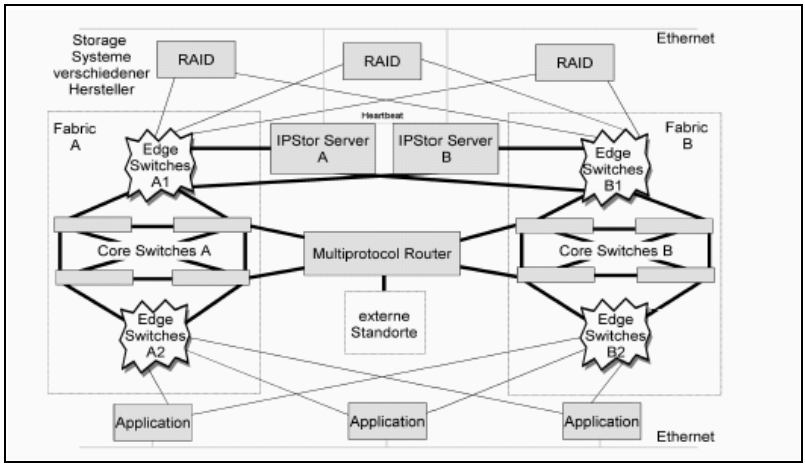
Einen weiteren Vorteil der Virtualisierung bietet der Einsatz synchroner Spiegel. Mit dieser Funktionalität kann die Migration großer Datenbereiche von einem RAID-System auf ein anderes für den Anwendungsbetrieb völlig transparent erfolgen.

5. Die Speichervirtualisierung mit IPStor bei der GWDG

Die GWDG setzt für die Speichervirtualisierung das Produkt IPStor der Firma FalconStor ein. Die Speichervirtualisierung ist als inband-Lösung in die SAN-Infrastruktur integriert.

Die zentralen Komponenten der Virtualisierungsschicht bilden zwei Virtualisierungsserver, die als Cluster mit Failover-Betrieb konfiguriert sind. Die beiden Server sind durch eine *Heartbeat-Verbindung* verbunden. Beim Ausfall des einen Servers wird dessen Funktionalität von dem anderen vollständig und für den Anwendungsbetrieb völlig unterbrechungsfrei übernommen. Die Synchronisation des Clusters erfolgt über eine Quorumdisk, auf die beide Server gemeinsam zugreifen.

Das Cluster kann sowohl als *active-active* oder als *active-passive* Konfiguration betrieben werden. Eine active-active-Konfiguration bietet im normalen Betrieb (nicht Failover-Fall) den Vorteil einer Lastverteilung auf beiden Server, wodurch die Leistungsfähigkeit der Virtualisierung erhöht wird.



6. An die Speichervirtualisierung angebundenen Raid-Systeme

Zur Zeit sind die folgenden Raid-Systeme an die Speichervirtualisierung angebunden:

- 1 Raid-System EVA5000 (HSV110) (HP)
- 1 Raid-System EVA3000 (HP)
- 1 Raid-System DS4500 (IBM)
- 1 Raid-System DS4800 (IBM)
- 1 Raid-System DS4100 (IBM)
- 1 Raid-System CX500 (EMC)
- 1 Raid-System CX3-80 (EMC)
- 6 Raid-Systeme T6100 (Transtec/Infortrend)

7. In die Virtualisierung integrierte Applikationen bei der GWDG

Die folgenden Services werden bei der GWDG zur Zeit über die Speichervirtualisierung angeboten:

- der File-Service für das UNIX-Cluster
- der File-Service für das Active-Directory
- der File-Service für den Mailer und die Mailbox
- der File-Service für die VMware-Anwendungen
- die Datenbank-Services Aleph, Elan, Digilib, Vweb und GCG
- der FTP-Server
- Anwendungen der SUB

8. Ausstattung der IPStor-Server bei der GWDG

Die beiden IPStor-Server sind mit folgender Hardware ausgestattet.

- Server: Dell Power Edge 6850
- Processor: Intel(R) Xeon(TM) MP CPU 3,66 GHz
- Memory: 4 GByte

- 4 x HBAs: Qlogic qle2362

Das Betriebssystem ist SuSE Linux 9.3 (x86-64) mit der IPStor-Version FalconStor IPStor Server v5.10 -(Build 5187).

Die Realisierung eines Workflows für den Transport und die Verarbeitung großer Datenmengen

Ulrich Degenhardt, Markus Uhr

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Max-Planck-Institut für biophysikalische Chemie, Göttingen

Zusammenfassung

Das Projekt EURExpress zielt auf die Erstellung eines Expressionsatlasses des Genoms der Maus und liefert große Mengen an Bilddaten. Diese Daten von Laboratorien an verschiedenen Standorten in Europa müssen zur GWDG transferiert und dort weiter verarbeitet werden. Anschließend werden die Bilddaten im Web dargestellt und auf Bändern gespeichert. Neben diesen Anforderungen müssen Teilmengen der Daten für andere wissenschaftliche Institute generiert und zum Download bereitgestellt werden. Es wird eine skalierbare Lösung vorgestellt, mit der die benötigten Anforderungen implementiert werden. Besonderes Augenmerk wird dabei auf den Workflow der Bilddaten und auf die Bereitstellung von Teilmengen der Bilder gelegt.

1. Einleitung

Die Abteilung „Gene und Verhalten“ des MPI für biophysikalische Chemie ist an dem europäischen Projekt EURExpress zur Genexpressionsanalyse beteiligt, das innerhalb des 6. EU-Forschungsrahmenprogramms (http://www.rp6.de) stattfindet. In diesem Projekt werden an verschiedenen Standorten in Europa große Mengen von Schnitten durch Mausembryonen erzeugt und die Aktivität von Tausenden von Genen in diesen Schnitten durch molekularbiologische Methoden sichtbar gemacht. Bild 1 zeigt ein Beispiel eines solchen ISH-Schnittbildes (Quelle: www.genepaint.org, Gen cadherin (cdh2), Set ID DA95, Embryo_C1470_6_4A).

Bild 1: Ein ISH-Bild eines Mausembryos

Als Ergebnis entstehen mit Hilfe von automatisierten Mikroskopieverfahren große Mengen hochauflösender digitaler Bilddaten, die bei der GWDG gespeichert werden. Wichtigstes Ziel des Projekts EURExpress ist die Erstellung eines Internet-basierten Expressionsatlasses für das Genom der Maus, das heisst eine Kartierung der Aktivität der einzelnen Bestandteile des Erbguts. Im Rahmen des Vorläuferprojektes Genepaint, das vom MPI für experimentelle Endokrinologie in Hannover durchgeführt wurde, wurden dazu bereits automatisierte Verfahren zur Genexpressionsanalyse entwickelt und erprobt. Außerdem wurde eine Web-Datenbank (www.genepaint.org) entwickelt, die es ermöglicht, die Bilddaten der wissenschaftlichen Gemeinde zugänglich zu machen. Eine genauere Beschreibung der Ziele des Projektes findet sich in einem Artikel von Visel et al. (A. Visel, C. Thaller, G. Eichele; GenePaint.org: an atlas of gene expression patterns in the mouse embryo. Nucleic Acids Research, 2004, vol. 32, pp. D552-D556).

Aufgabe der GWDG innerhalb des Projektes EURExpress ist der Transfer der anfallenden Bilddaten von verschiedenen Standorten in Europa (s. Bild 2) nach Göttingen und der Betrieb der Server, die zur Darstellung und zur Realisierung von Recherchemöglichkeiten in den gewonnenen Bilddaten notwendig sind.

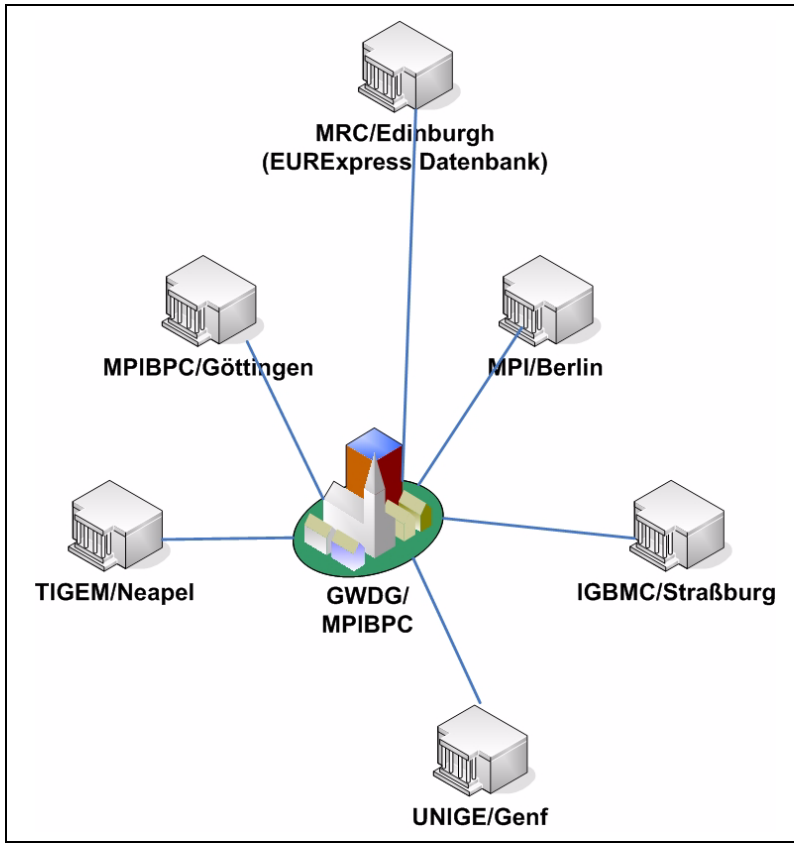


Bild 2: Die beteiligten Institutionen

Neben diesen Anforderungen müssen die anfallenden Bilddaten auf Bändern archiviert und Teilmengen der Daten für andere wissenschaftliche Institute generiert und zum Download bereitgestellt werden.

2. IT-Aspekte des Projektes EURExpress

In Projekten wie EURExpress fallen große Mengen an Daten an, die organisiert werden müssen. Zur Zeit generieren die am Workflow beteiligten Institute mit molekularbiologischen Methoden Bilddaten, die von der GWDG über schnelle Datenleitungen nach Göttingen transferiert werden. Die Originalbilder liegen im TIFF-Format vor und sind pro Bild ca. 60 MB bis 100 MB groß. Pro Woche werden etwa 300 GB an Bilddaten übertragen. Die

beteiligten Institute sind über schnelle Leitungen miteinander verbunden, so dass die anfallenden Datenvolumina problemlos bewältigt werden können. Bei der GWDG liegen im Augenblick ca. 30 Terabyte an Daten, die im Laufe des Projektes erzeugt wurden. Insgesamt wird die Datenmenge, die nach Ablauf des Projektes EURExpress vorliegen wird, auf etwa 50 Terabyte geschätzt.

Die ankommenden Daten werden in einem ersten Schritt in einem RAID-System eines UNIX-Servers auf schnellen Platten gespeichert und danach automatisch auf Band archiviert. Nach der Speicherung werden die gewonnenen Bilder für die wissenschaftliche Gemeinde recherchierbar gemacht. Das wird mit Hilfe einer Website und einer Datenbank realisiert, in die von allen beteiligten Institutionen die experimentellen Hintergrunddaten, so genannte Metadaten, zu den jeweiligen Bildern eingetragen werden.

3. Funktionsweise und Architektur der Anwendung

Im direkten Vorgängerprojekt von EURExpress, dem Genepaint-Projekt, wurden vom damaligen MPI für experimentelle Endokrinologie in Hannover, der Firma Orgarat aus Essen und der GWDG Verfahren für Transfer der Bilddaten, Datenhaltung, Darstellung und Recherchemöglichkeiten entwikkelt, die im Folgenden kurz beschrieben werden. Für das EURExpress-Projekt wurden die bereits bestehenden Verfahren übernommen und erweitert.

Ankommende TIF-Dateien werden zunächst auf RAID-5-Festplatten eines Transferservers gespeichert (s. Bild 3). Nach dem Transfer werden die TIF-Bilder in andere Formate konvertiert, die für die weitere Verwendung benötigt werden. Zunächst werden die Bilder in ein Format konvertiert, bei dem mehrere Auflösungen innerhalb einer Datei gespeichert werden können (Flashpix-Format). Zusätzlich werden aus den TIF-Bildern noch Thumbnail-Bilder für eine schnelle Anzeige im Internet und hoch aufgelöste JPG-Bilder für wissenschaftliche Auswertungen generiert.

Wenn das Dateisystem der TIF-Bilder auf den Festplatten zu mehr als 65 % gefüllt ist, werden die ältesten Bilddateien automatisch auf Bänder ausgelagert, bis die Platten nur noch zu etwa 50 % voll sind (hierarchisches Speichermanagement, HSM). Wird eine Datei ausgelagert, bleibt auf dem Dateisystem eine kleine Datei gleichen Namens zurück, welche die Information enthält, wo die eigentliche Datei zu finden ist. Auf diese Weise wird der verfügbare Plattenplatz auf Kosten der Zugriffszeit vergrößert, ohne dass das

Festplattensystem erweitert werden muss. Damit werden teure Festplatten durch preisgünstigere Bänder ergänzt.

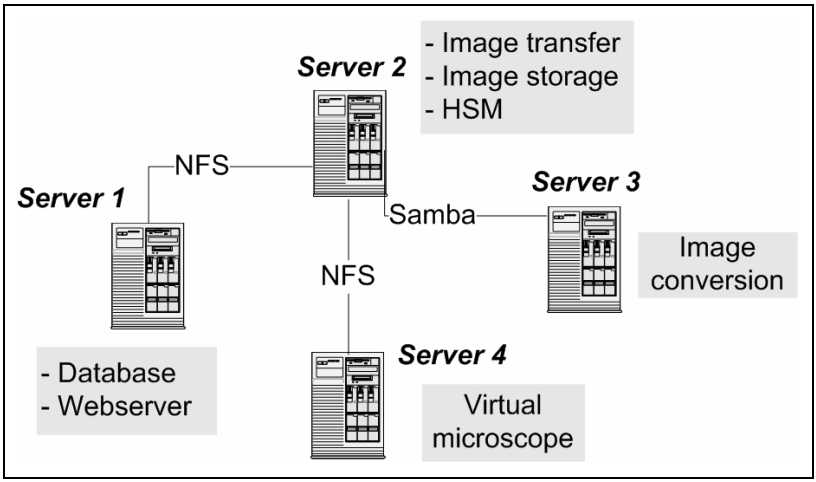


Bild 3: Die im Projekt EURExpress verwendeten Server

Dieser automatisch ablaufende Vorgang ist für den Benutzer nicht zu erkennen. Für ihn ist der einzige Unterschied zur Speicherung der Daten auf Festplatte, dass der Zugriff auf die Originalbilder nun länger dauert als bei Bilddaten, die auf den Platten gespeichert sind. Ein Beispiel: Ein 100 MB großes Bild, das von einer Festplatte geladen wird, benötigt etwa 20 Sekunden, bis es in einem Anzeigeprogramm betrachtet werden kann. Ist das Bild auf ein Band ausgelagert, dauert es bis zu drei Minuten, bis das Bild zur Verfügung steht. Diese Verzögerung liegt daran, dass der Bandroboter, in dem die Bänder mit den ausgelagerten Dateien verwaltet werden, nach der Anforderung einer Datei eine gewisse Zeit braucht, bis er das entsprechende Band herausgesucht und die gewünschte Datei wieder auf die Festplatten des Servers zurückkopiert hat. Benutzer und Programme können die Dateien wie gewohnt verwenden und müssen sich weder um die Migration der Daten auf Bänder noch um das Zurückholen von migrierten Daten kümmern.

Wenn Dateien auf Band ausgelagert werden, wird automatisch eine weitere Kopie dieser Dateien in einer Bandbibliothek im Medizinischen Rechenzentrum der Universität Göttingen angelegt. Damit sind die ausgelagerten Dateien noch einmal an einem anderen Standort gespeichert und ein weiteres Mal gegen Datenverlust gesichert. Neben dem hierarchischen Speichermanagement werden alle Daten – auch die ausgelagerten Dateien – im Rahmen des üblichen Backups jede Nacht auf Band gesichert.

Neben den reinen Bilddaten werden von den beteiligten Institutionen Metadaten zur Beschreibung der Bilder generiert und über eine webbasierte Anwendung in einer Datenbank abgelegt, die auf einem Server der GWDG betrieben wird (s. Bild 3). Mit diesen Metadaten werden Recherchemöglichkeiten im Rahmen einer Webanwendung implementiert.

Die Flashpix-Bilder können über die Webapplikation mit einem virtuellen Mikroskop betrachtet werden. Der Zugriff auf eine solche Datei wird von einer speziellen Software, die das virtuelle Mikroskop implementiert und auf einem eigenen Server läuft (s. Bild 3), verwaltet. Mit dieser Software ist es möglich, die Bilder in verschiedenen Vergrößerungen zu betrachten, ohne dass für jede Vergrößerung eine eigene Datei angelegt werden muss. Der Ausschnittt, mit dem der Betrachter das Bild sieht, kann von ihm festgelegt werden und es gibt eine Lupenfunktion, mit der interaktiv Ausschnitte eines Bildes in größerer Auflösung untersucht werden können.

Die Vergrößerung der Bilder kann über ein Applet, über ein Plugin oder browserunabhängig mit dynamisch generiertem HTML-Code erstellt werden, so dass die Benutzer aller Plattformen, auf denen ein Browser einsetzbar ist, dieses virtuelle Mikroskop verwenden können. Daten aus dem Vorgängerprojekt Genepaint, Recherchemöglichkeiten und die verschiedenen Zoomfunktionen stehen bereits jetzt im Portal www.genepaint.org zur Verfügung.

4. Der Workflow zu Übertragung und Konvertierung von Bilddaten

In den Laboratorien der Partnerinstitutionen werden Mausembryonen in ca. 20 Scheiben geschnitten, die mit der Methode der ISH für ein bestimmtes Gen behandelt und unter einem Mikroskop fotografiert werden. Jedes Gen ist einer so genannten Set-ID zugeordnet und jeder Schnitt bekommt eine Nummer. Der Name einer einzelnen Datei besteht aus Set-ID und laufender Nummer des Schnittes (z. B. EN00002377_00001B.TIF). Die von den Mikroskopen kommenden Bilder werden im TIF-Format abgelegt und sind ca. 100 MB groß.

Die Bilddaten werden in den Laboratorien der Partnerinstitutionen zum Transfer zur GWDG vorbereitet. Dazu werden die erzeugten Bilder mit Metadaten versehen, die mit Hilfe einer Webschnittstelle in eine zentrale Datenbank des Projektes eingegeben werden. Danach werden die Bilddaten in ein Verzeichnis eines Servers übertragen, das als Transferbereich dient. Zusätzlich werden Prüfsummen für alle zu übertragenden Dateien und Steuerdateien mit Informationen zu den zu übertragenden Dateien erstellt (Bild 4).

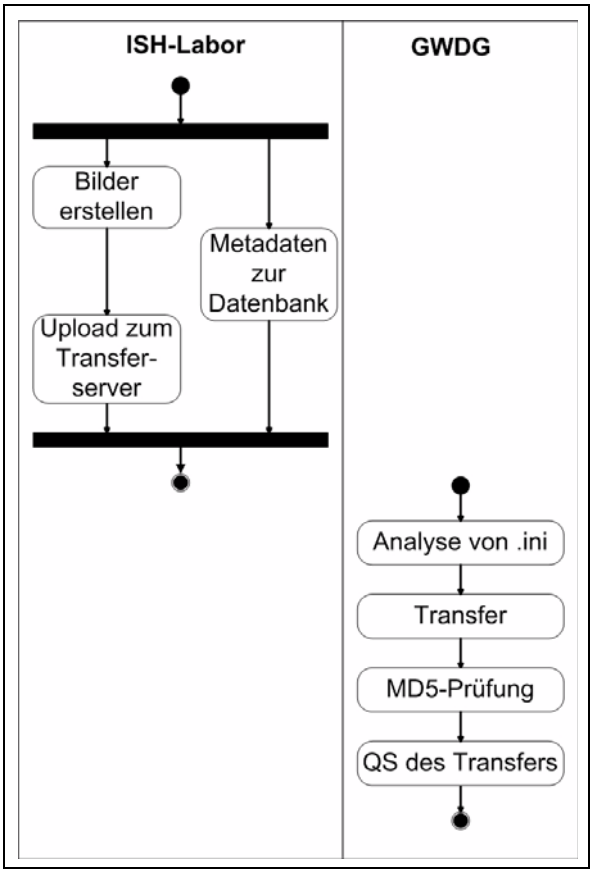


Bild 4: UML-Diagramm des Transport-Workflows

Eine Steuerdatei hat die folgende Form:

```
[ANALYSIS]
ArchivesServer=apoll.gwdg.de
CopyPathTIF=/cm/web/genepaint/039
CopyPathJPG=/cm/web/genepaint/039
CopyPathFPX=/home/MHEE/zoomserver/images/039
[Image1]
tif_Filename=EN00002377_00001B.TIF
[Image2]
```

…

```
[Image24]
tif_Filename=EN00002377_00024B.TIF
[Summary]
TotalImages=24
TIFFonly=YES
```

Auf der Seite der GWDG wird zeitgesteuert ein Skript gestartet, das den Transfer der Bilddaten mit dem Protokoll FTP und eine erste Qualitätskontrolle durch einen Vergleich der am entfernten Standort generierten Prüfsummen mit bei der GWDG generierten Prüfsummen durchführt. Ein weitere Kontrolle des Transfers findet statt, indem die Anzahl der zu übertragenden Dateien aus den Steuerdateien ausgelesen wird und mit der Anzahl der tatsächlich übertragenen Dateien verglichen wird. Zusätzlich wird noch die syntaktische Korrektheit der Steuerdatei geprüft. Die zweite Kontrolle führt auf eine in Bild 5 dargestellte Protokolldatei, die einen schnellen Überblick über den Datentransfer ermöglicht.

```
Analysis of INI files and related TIF files started on Mon Jan  7 07:55:10 2008

transferEN00002153.ini | Ordner Nr. 38 | Skript OK | 1 Dateien | uebertragene TIF-Bilder OK
transferEN00002154.ini | Ordner Nr. 38 | Skript OK | 1 Dateien | uebertragene TIF-Bilder OK
transferEN00002155.ini | Ordner Nr. 38 | Skript OK | 1 Dateien | uebertragene TIF-Bilder OK
transferEN00002156.ini | Ordner Nr. 38 | Skript OK | 22 Dateien | uebertragene TIF-Bilder OK
transferEN00002157.ini | Ordner Nr. 38 | Skript OK | 23 Dateien | uebertragene TIF-Bilder OK
transferEN00002158.ini | Ordner Nr. 38 | Skript OK | 23 Dateien | uebertragene TIF-Bilder OK
transferEN00002159.ini | Ordner Nr. 38 | Skript OK | 23 Dateien | uebertragene TIF-Bilder OK
transferEN00002160.ini | Ordner Nr. 38 | Skript OK | 22 Dateien | uebertragene TIF-Bilder OK
transferEN00002161.ini | Ordner Nr. 38 | Skript OK | 23 Dateien | uebertragene TIF-Bilder OK
transferEN00002162.ini | Ordner Nr. 38 | Skript OK | 22 Dateien | uebertragene TIF-Bilder OK
transferEN00002163.ini | Ordner Nr. 38 | Skript OK | 1 Dateien | uebertragene TIF-Bilder OK
transferEN00002164.ini | Ordner Nr. 38 | Skript OK | 23 Dateien | uebertragene TIF-Bilder OK
transferEN00002165.ini | Ordner Nr. 38 | Skript OK | 23 Dateien | uebertragene TIF-Bilder OK
transferEN00002166.ini | Ordner Nr. 38 | Skript OK | 1 Dateien | uebertragene TIF-Bilder OK
transferEN00002167.ini | Ordner Nr. 38 | Skript OK | 1 Dateien | uebertragene TIF-Bilder OK
transferEN00002168.ini | Ordner Nr. 38 | Skript OK | 1 Dateien | uebertragene TIF-Bilder OK
transferEN00002169.ini | Ordner Nr. 38 | Skript OK | 1 Dateien | uebertragene TIF-Bilder OK
transferEN00002170.ini | Ordner Nr. 38 | Skript OK | 1 Dateien | uebertragene TIF-Bilder OK
transferEN00002171.ini | Ordner Nr. 38 | Skript OK | 1 Dateien | uebertragene TIF-Bilder OK
transferEN00002172.ini | Ordner Nr. 38 | Skript OK | 24 Dateien | uebertragene TIF-Bilder OK

DONE
```

Bild 5: Eine typische Logdatei der Qualitätssicherung für den Datentransfer

Nach dem Transport und der anschließenden Qualitätskontrolle wird die Konvertierung der übertragenen Bilder in andere Formate angestoßen. Die übertragenen Bilder liegen auf einem Dateisystem des Transferservers und sind für den Server, der die Konvertierung durchführen soll, als Samba-Freigabe sichtbar. Der Konvertierungsrechner muss unter Windows arbeiten, da eine zuverlässige Konvertierungssoftware für eines der Dateiformate (Flashpix) nur unter Windows vorliegt. Auf dem Konvertierungsrechner wird ein Batchsystem (Condor) verwendet, das die Ressourcenverteilung regelt und

die vorhandenen vier CPUs optimal ausnutzt. Eine Qualitätskontrolle des Konvertierungsprozesses findet statt, indem die Anzahl der Quelldateien mit der Anzahl der konvertierten Dateien verglichen wird. Zusätzlich dazu wird noch geprüft, ob die konvertierten Dateien größer als 0 Byte sind. Mit diesen beiden Kriterien lässt sich feststellen, ob es bei der Konvertierung Probleme gab. Es ist zwar prinzipiell möglich, die erzeugten Dateien auf Korrektheit des entsprechenden Bildformates hin zu überprüfen (z. B. mit JHOVE), ein solches Vorgehen würde aber die Laufzeit und die Komplexität des Workflows deutlich erhöhen. Für praktische Zwecke kann man unseren Erfahrungen nach die hier beschriebene Vorgehensweise verwenden. Bild 6 zeigt schematisch die Datei, die von den Skripten, die eine Qualitätskontrolle durchführen, erzeugt wird.

```
Analysis of TIF files and converted images started on Mon Jan  7 11:17:33 2008

Set           | INI | TIF | JPGTH | JPGED | FPX | Directory | # of images|
--------------------------------------------------------------------------
EN00002153    |  1  |  1  |   1   |   1   |  1  |    38     |    o.k.    |
EN00002154    |  1  |  1  |   1   |   1   |  1  |    38     |    o.k.    |
EN00002155    |  1  |  1  |   1   |   1   |  1  |    38     |    o.k.    |
EN00002156    | 22  | 22  |  22   |  22   | 22  |    38     |    o.k.    |
EN00002157    | 23  | 23  |  23   |  23   | 23  |    38     |    o.k.    |
EN00002158    | 23  | 23  |  23   |  23   | 23  |    38     |    o.k.    |
EN00002159    | 23  | 23  |  23   |  23   | 23  |    38     |    o.k.    |
EN00002160    | 22  | 22  |  22   |  22   | 22  |    38     |    o.k.    |
EN00002161    | 23  | 23  |  23   |  23   | 23  |    38     |    o.k.    |
EN00002162    | 22  | 22  |  22   |  22   | 22  |    38     |    o.k.    |
EN00002163    |  1  |  1  |   1   |   1   |  1  |    38     |    o.k.    |
EN00002164    | 23  | 23  |  23   |  23   | 23  |    38     |    o.k.    |
EN00002165    | 23  | 23  |  23   |  23   | 23  |    38     |    o.k.    |
EN00002166    |  1  |  1  |   1   |   1   |  1  |    38     |    o.k.    |
EN00002167    |  1  |  1  |   1   |   1   |  1  |    38     |    o.k.    |
EN00002168    |  1  |  1  |   1   |   1   |  1  |    38     |    o.k.    |
EN00002169    |  1  |  1  |   1   |   1   |  1  |    38     |    o.k.    |
EN00002170    |  1  |  1  |   1   |   1   |  1  |    38     |    o.k.    |
EN00002171    |  1  |  1  |   1   |   1   |  1  |    38     |    o.k.    |
EN00002172    | 24  | 24  |  24   |  24   | 24  |    38     |    o.k.    |

DONE
```

Bild 6: Eine typische Logdatei der Qualitätssicherung für die Konvertierung

Bei den anfallenden Datenmengen ist ein solcher schneller Überblick über das Ergebnis der Konvertierung notwendig.

Nach der Qualitätskontrolle der Konvertierung werden die Daten an ihren endgültigen Speicherort verschoben. Die originalen TIF-Bilder werden dabei in ein Dateisystem verschoben, das dem hierarchischen Speichermanagement unterliegt. Diese Dateien werden dann ab einem bestimmten Füllstand des Dateisystems auf Bänder ausgelagert.

5. Erfolgsfaktoren

Der hier beschriebene Workflow wurde in der ersten Hälfte des Jahres 2006 entwickelt und wird seid Mitte 2006 erfolgreich eingesetzt. Seither wurden ca. 30 TB Daten (ca. 250.000 Dateien) übertragen und in andere Bildformate konvertiert. Diese Datenmengen und diese Anzahl an Dateien können nur verarbeitet werden, wenn einige Voraussetzungen gegeben sind:

1. Es muss hinreichend viele Qualitätskontrollen an wichtigen Stellen des Workflows geben. Die Art der Qualitätskontrollen hat sich aus schmerzhaften praktischen Erfahrungen mit Transport und Konvertierung ergeben und wurde im Laufe der Zeit immer wieder angepasst. Zum Beispiel hat sich herausgestellt, dass einzelne TIF-Bilder gelegentlich nicht vollständig, aber syntaktisch korrekt waren. Eines der Konvertierungsprogramme erzeugt eine korrekte (aber unvollständige) Datei, die auch gelesen werden kann. Das andere Konvertierungsprogramm erzeugt mit der gleichen Eingabedatei eine Datei, die 0 Byte groß ist und bricht dann ab. Diesen Fall kann man erkennen, wenn man prüft, ob beim Konvertierungsvorgang eine 0 Byte große Datei generiert wird.

2. Der Workflow darf nicht vollständig automatisiert sein. Eine weitergehende Automatisierung als implementiert würde bedeuten, dass man viel mehr programmieren müsste, um mögliche Fehler abzufangen. Der Aufwand dazu wird irgendwann sehr hoch, so dass ein Kompromiß zwischen Automatisierung und Programmieraufwand gefunden werden muß. Es muß im Workflow Stellen geben, an denen eine menschliche Intervention notwendig ist, damit es weitergeht. Als ein Beispiel sei hier die Konvertierung genannt, die erst beginnen kann, wenn ein Mensch entscheidet, dass die Qualitätsprüfung des Transfervorganges in Ordnung ist. Das könnte man zwar automatisieren, man würde sich dann aber die Möglichkeit erschweren, den Workflow an dieser Stelle anzuhalten, wenn beim Transfer ein Fehler passiert ist.

3. Die Sicht auf die Daten muss einfach und vollständig sein. Der Einsatz einer Samba-Freigabe auf dem zentralen Dateiserver und die Kontrolle der anfallenden Daten mit einem Windows-PC und dem Explorer als Anzeigewerkzeug sind für das Funktionieren des Workflows von eminenter Bedeutung.

6. Zusammenfassung

Im Projekt EURExpress soll ein öffentlich zugänglicher, genomweiter Expressionsatlas der Maus erstellt werden. Dabei entstehen große Datenmengen, die transportiert und verarbeitet werden müssen. Ein Workflow, der

das leistet, wurde beschrieben. Wichtig für den Erfolg eines solchen Vorhabens sind enge Zusammenarbeit der Beteiligten am MPIBPC und bei der GWDG, gutes Design des Workflows und viele Möglichkeiten der Qualitätssicherung.

Benutzerverwaltung auf vollelektronischer Basis

Wilfried Grieger

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

1. Benutzerverwaltung bisher

Um als Benutzerin oder Benutzer in der Benutzerverwaltung der GWDG registriert zu werden, musste bisher ein Antrag auf Zuweisung einer Benutzerkennung auf Papier gestellt werden. Mit der Benutzerkennung können alle von der GWDG angebotenen Ressourcen und Dienste in Anspruch genommen werden.

Der Antrag musste vollständig ausgefüllt, von der Benutzerin oder dem Benutzer unterschrieben und von der zuständigen Geschäftsführung gegengezeichnet werden. Häufig wurden Anträge dann unvollständig oder unleserlich ausgefüllt per Post zur GWDG geschickt. Da diese Anträge nicht selten zurückgeschickt werden mussten, kam es unweigerlich zu äußerst langen Laufzeiten, die die Bearbeitung deutlich verzögerten.

Bei der GWDG selber mussten die Daten aus dem Antrag wieder abgetippt werden. Dieses Verfahren war fehleranfällig. War dann die gewünschte Benutzerkennung doch endlich eingefügt, musste das zugewiesene erstmalige Passwort in der Regel bei der Information der GWDG abgeholt werden. Trotz der langen Öffnungszeiten war das für viele äußerst lästig.

Ein neues Verfahren soll nun das althergebrachte ablösen.

2. Ziele des neuen Verfahrens

Mit der Einführung des neuen Verfahrens wurden die folgenden Ziele verfolgt:

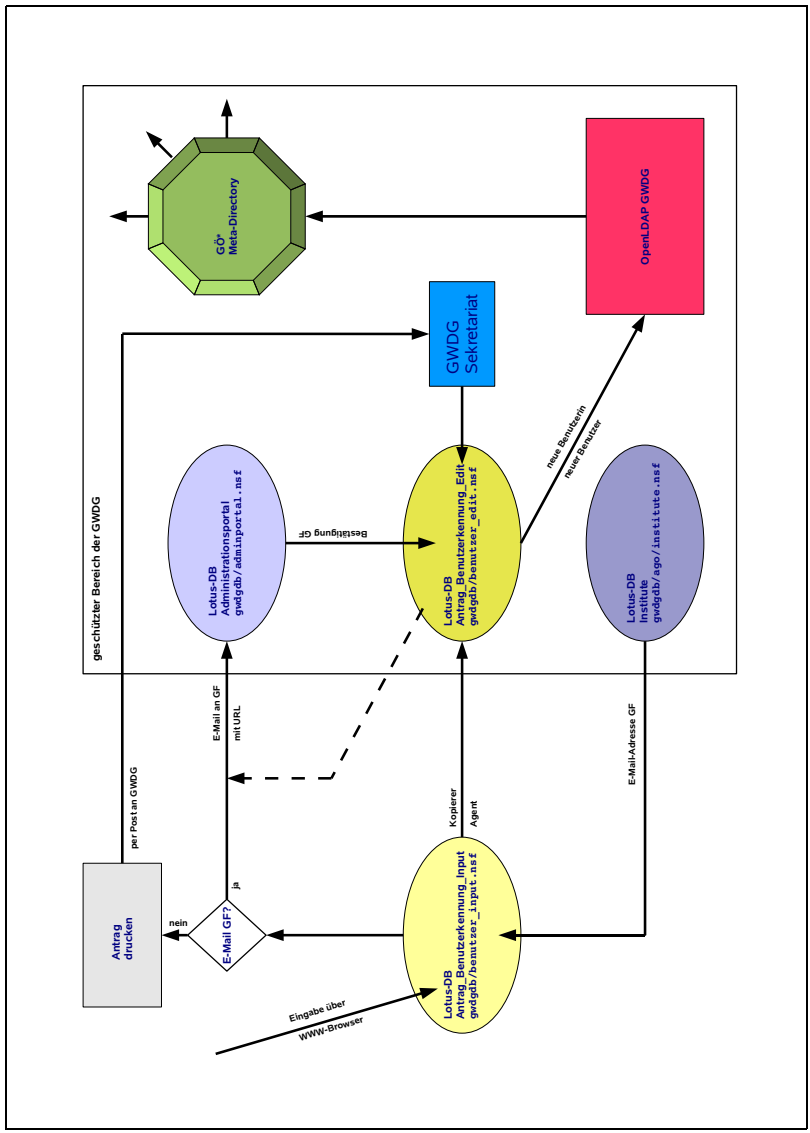
- Das System wird technisch auf einen neuen Stand gebracht und damit deutlich modernisiert.
- Die Antragsbearbeitung beschleunigt sich erheblich.
- Unnötige Bürokratie wird abgebaut.
- Die „Kernsysteme“ sind bereits nach zwei Stunden verfügbar. Zu den Kernsystemen gehört beispielsweise der Mailer der GWDG.
- Die „Zusatzsysteme“ sind am nächsten Tag verfügbar. Ein Zusatzsystem ist das Archiv.
- Die Verteilung der Benutzerkennungen auf weitere angeschlossene Verzeichnisdienste übernimmt ein Meta-Directory-System.
- Die Arbeitsabläufe von der Antragstellung bis zum Einbringen in das Meta-Directory-System werden optimiert und sind ITIL-konform.
- Zur Steuerung und zur Erkennung von Schwachstellen wird auch die Dauer von Teilprozessen gemessen.

Die Struktur des neuen Verfahrens soll im folgenden Abschnitt erläutert werden.

3. Struktur des neuen Verfahrens

Ein Antrag auf Zuweisung einer Benutzerkennung wird grundsätzlich über einen WWW-Browser von der zukünftigen Benutzerin oder dem zukünftigen Benutzer gestellt. Die eingegebenen Daten werden automatisch in eine Lotus-Datenbank kopiert, in der sie weitestgehend automatisch verarbeitet werden. Daran sind auch noch weitere Lotus-Datenbanken beteiligt. Insbesondere wird die zugehörige Benutzerkennung als erstes im OpenLDAP-System der GWDG erzeugt.

Die folgende Zeichnung soll die Struktur des neuen Verfahrens darstellen:



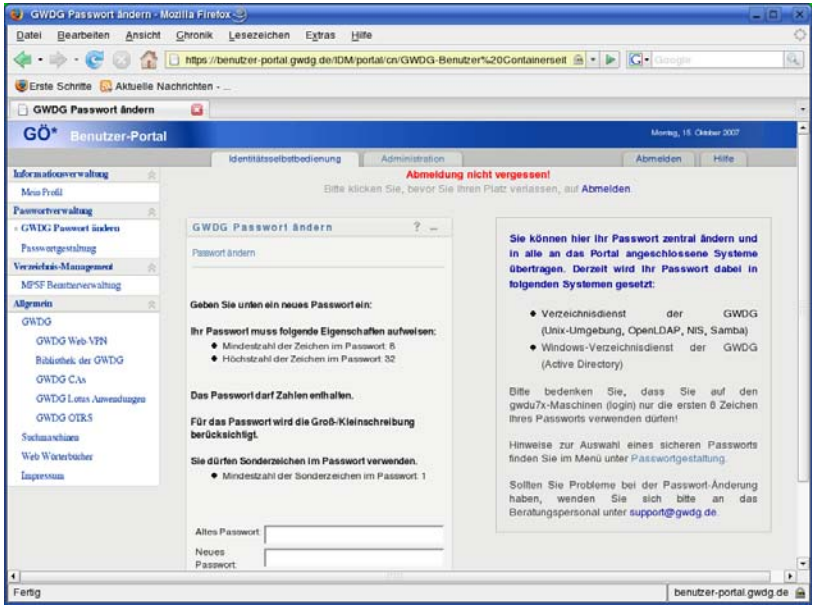
Die Verteilung der Benutzerkennung auf weitere angeschlossene Verzeichnisdienste übernimmt ein Meta-Directory-System, nämlich der Novell Identity Manager, den die GWDG nach einer ausgiebigen Produktuntersuchung für diese Zwecke erworben hat.

Das Meta-Directory-System synchronisiert zurzeit unter anderem das OpenLDAP-System der GWDG, das Microsoft Active Directory der GWDG, das System der Studierenden der Georg-August-Universität Göttingen sowie das System der Universitätsmedizin Göttingen. Insgesamt sind 20 Systeme angebunden; der Novell Identity Manager verwaltet ca. 70.000 Verzeichnisobjekte.

4. Benutzerportal

Insbesondere wird über das Meta-Directory-System ein Benutzerportal angeboten, über das jede Benutzerin und jeder Benutzer ihr bzw. sein Passwort ändern kann. Nach der Änderung wird das neue Passwort in den unterschiedlich benötigten Verschlüsselungstechniken wieder auf die angeschlossenen Systeme verteilt, sodass das einzugebende Passwort auf allen Systemen identisch bleibt.

Dieses Benutzerportal ist natürlich ebenfalls über einen WWW-Browser erreichbar:



5. Antrag per WWW-Browser

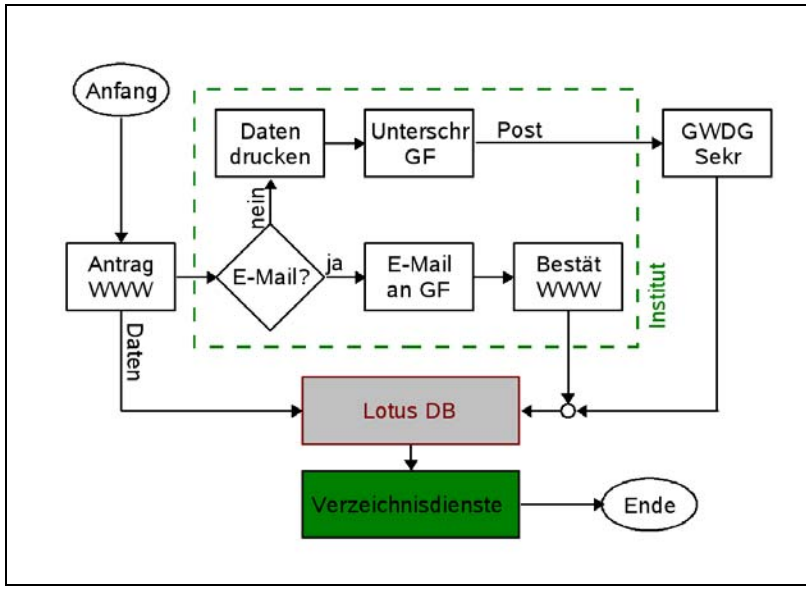
Der Antrag auf Zuweisung einer Benutzerkennung wird per WWW-Browser von einer Lotus-Datenbank entgegengenommen. Da diese Eingabe von Daten mit möglichst vielen unterschiedlichen WWW-Browsern möglich sein

soll, wurden im Vorfeld eine Reihe von Browsern getestet und die Datenbank passend gestaltet. Mit folgenden Browsern sollte die Eingabe danach problemlos möglich sein:

- Mozilla Firefox (auf unterschiedlichen Betriebssystemen)
- Microsoft Internet Explorer
- Opera (auf unterschiedlichen Betriebssystemen)
- Konqueror
- Safari

6. Workflow zur Antragsbearbeitung

Die folgende Zeichnung soll den Workflow verdeutlichen, der von der Antragsstellung bis zur Einrichtung der Benutzerkennung abläuft:



Nachdem die Antragsdaten in die Lotus-Datenbank eingegangen sind, wird automatisch geprüft, ob von der zuständigen Geschäftsführung eine E-Mail-Adresse hinterlegt ist, an die Meldungen geschickt werden, wenn neue Anträge aus dem betroffenen Institut eingegangen sind.

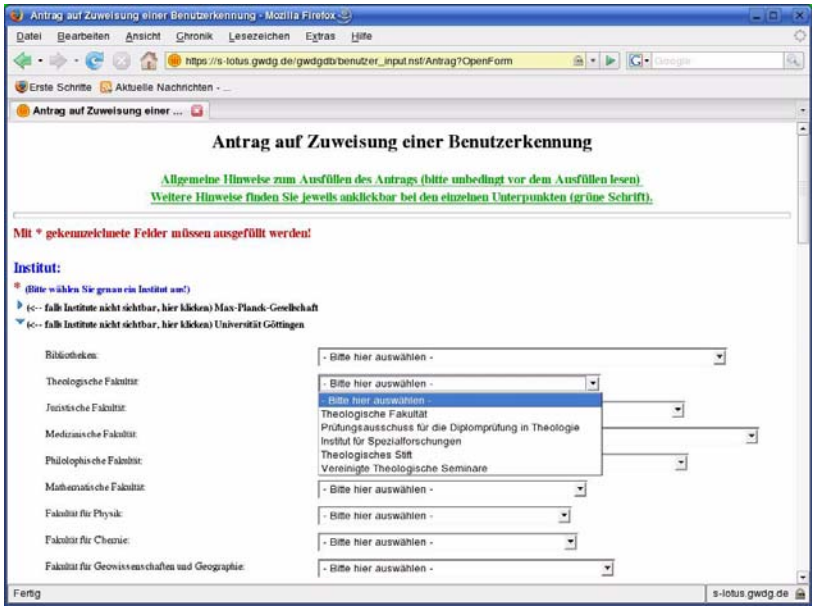
Wenn solch eine E-Mail-Adresse vorliegt, wird die Geschäftsführung darüber über den neuen Antrag informiert und gebeten, ihn zu genehmigen oder abzulehnen. Dazu ist von der Geschäftsführung aus der E-Mail heraus ein Link anzuklicken. Dieser Link ist zur Sicherheit Userid- und Passwortgeschützt. Nach der Eingabe der richtigen Kombination kann die Geschäftsführung den Antrag durch das Anklicken einer Schaltfläche genehmigen.

Wenn die E-Mail-Adresse nicht vorliegt, wird die Antragstellerin oder der Antragsteller aufgefordert, eine am Bildschirm angezeigte Seite auszudrukken, zu unterschreiben, von der Geschäftsführung des Instituts unterschreiben zu lassen und per Post an die GWDG zu schicken. Die Genehmigung wird dann in diesem Fall stellvertretend durch die Mitarbeiterinnen und Mitarbeiter im Sekretariat der GWDG erfolgen.

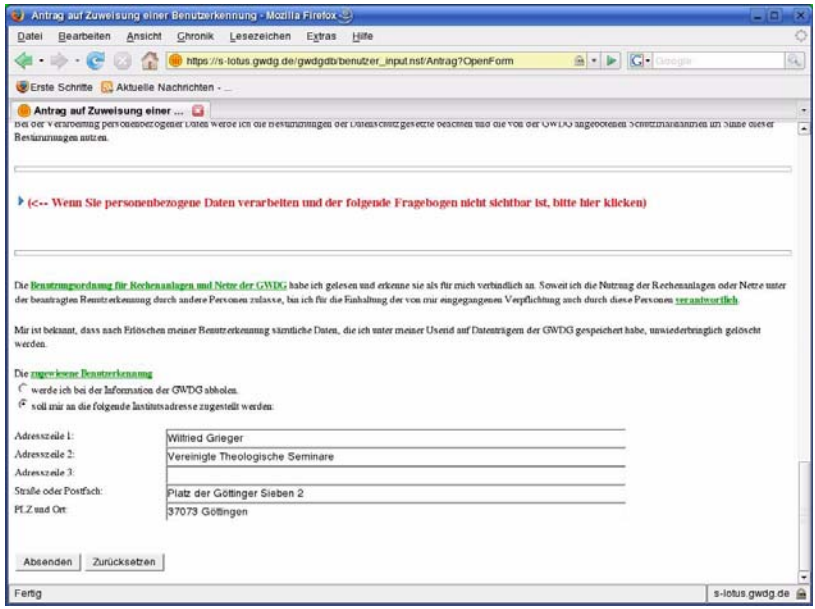
Unmittelbar nach der Genehmigung wird aus der Lotus-Datenbank heraus die gewünschte Benutzerkennung im OpenLDAP-System erzeugt und per Meta-Directory-System verteilt.

7. Antragstellung und Genehmigung

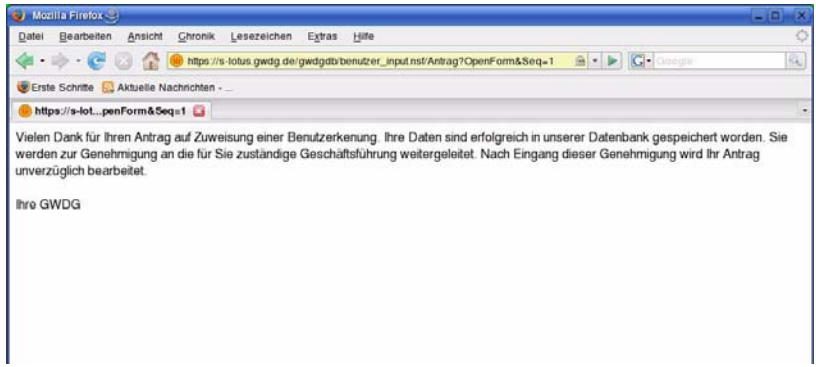
Wie auch beim herkömmlichen Antrag auf Papier müssen per WWW-Broswer einige benötigte Felder ausgefüllt werden:



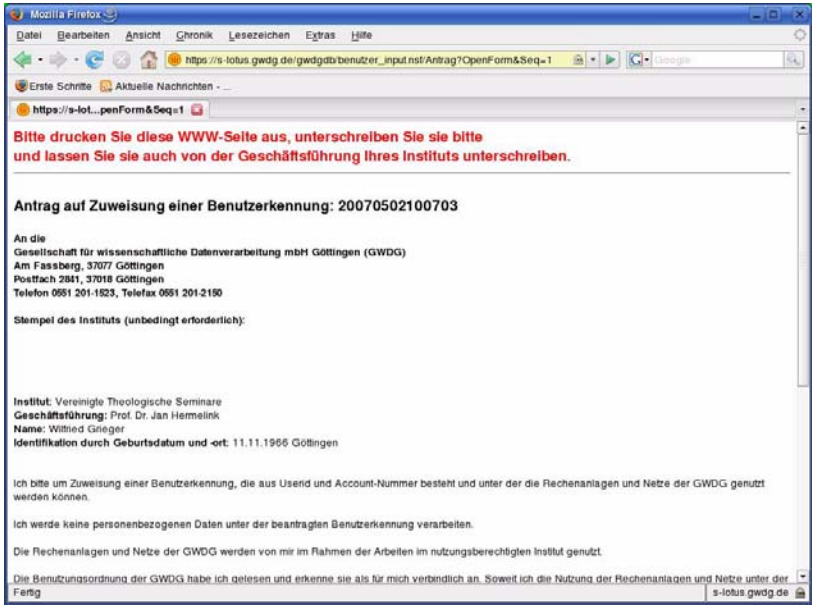
Insbesondere lässt sich im unteren Teil des Antrags vermerken, ob und an welche Institutsadresse die Informationen zur neuen Benutzerkennung geschickt werden sollen:



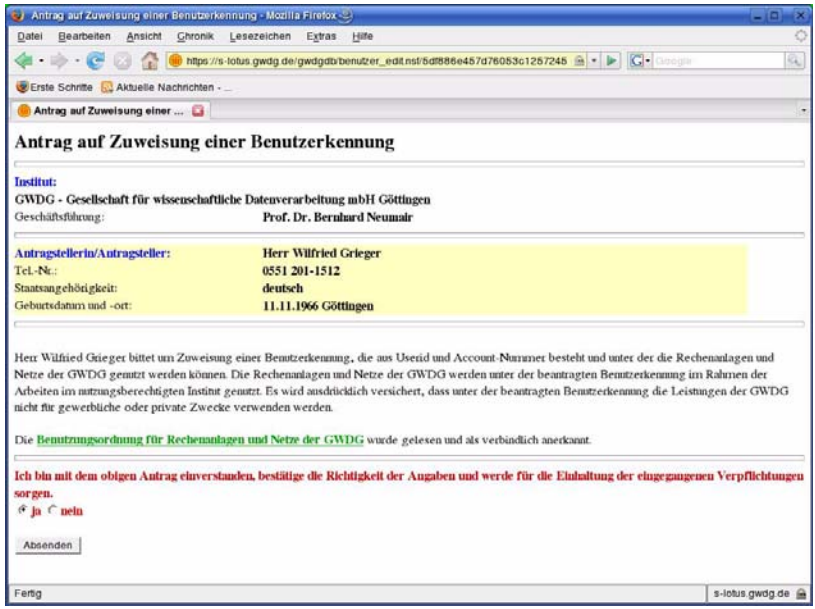
Nachdem alle Felder erfolgreich ausgefüllt sind und die E-Mail-Adresse der Geschäftsführung bei der GWDG vorliegt, ist die Antragstellung erfolgreich abgeschlossen:



Die Alternative, das Ausdrucken, Unterschreiben und Verschicken per Post, sollte natürlich vermieden werden:



Der Genehmigung des Antrags durch die Geschäftsführung steht nun nichts mehr im Wege, und sie kann über die folgende Seite erfolgen. Allerdings hat die GWDG an dieser Stelle keinen Einfluss auf den Zeitpunkt der Genehmigung. Die zuständige Geschäftsführung entscheidet alleine, ob und wann sie die Genehmigung aussprechen wird. Ungenehmigte Anträge werden nach vier Wochen automatisch wieder aus der Datenbank entfernt.



8. Ausblick

Das neue System wird selbstverständlich weiter entwickelt werden, neue Techniken und neue Kommunikationswege sollen eingebunden werden.

Bei Fragen dazu kann sich jeder an die Arbeitsgruppe „Basisdienste und Organisation“ der GWDG wenden , insbesondere an:

- Sigrun Greber, sgreber@gwdg.de
- Wilfried Grieger, wgriege@gwdg.de

Funk-LAN-Lösungen

Andreas Ißleiber

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

1. Einleitung

Funk-LANs erhöhen ganz erheblich die Mobilität der Wissenschaftlerinnen und Wissenschaftler. Darüber hinaus sollen Netzzugänge über Funk auch die Komplexität und den Aufwand hinsichtlich Anbindung und Integration von Gäste-Rechnern reduzieren. Funk-LAN-Technologien im Netzwerkbereich sind nicht neu, und viele Systeme sind heutzutage ausgereift genug, um mit vertretbarem Aufwand eine drahtlose Infrastruktur aufzubauen. Überdies ist die Verbreitung von Funk-LAN-Systemen ausgesprochen groß, sodass nahezu jeder moderne Laptop bereits für den Anschluss an ein Funk-LAN vorbereitet ist oder mit geringem Aufwand nachgerüstet werden kann. Die Auswahl der Geräte mit einem Netzzugang über Funk wächst stetig an und erreicht mit Funk-LAN-fähigen PDAs[1] und Kombinationsgeräten aus Mobiltelefon und Funk-LAN-Telefon[2] ihren derzeitigen Höhepunkt.

1. PDA, Personal Digital Assistant
2. GSM-Telefone mit integriertem Funk-LAN-Zugang (WLAN-Zugang)

Die GWDG beschäftigt sich seit Mitte 1999 intensiv mit diesem Thema und kann mittlerweile auf eine mehrjährige Erfahrung im Aufbau und Betrieb von Funk-LAN-Systemen im wissenschaftlichen Umfeld zurückblicken. Auch das GNZ[3] hatte durch detaillierte Produktvergleiche die Situation hinsichtlich Funk-LAN am Markt untersucht und die Erfahrungen durch Teststellungen im eigenen Hause ergänzt. Ein gemeinsamer BAR-Antrag (5/2006) der sieben Berliner Max-Planck-Institute konnte inzwischen erfolgreich umgesetzt werden. In diesem Dokument sind die Erfahrungen beider Institutionen eingeflossen und in abgestimmter Form dargestellt.

2. Funk-LAN-Grundlagen

2.1 Allgemeines

Computervernetzungen auf Basis von Funkübertragung existieren bereits seit Mitte/Ende der 90er-Jahre. Diverse Standards und unterschiedliche Protokollimplementierungen der Hersteller führten erst in den letzten fünf bis sechs Jahren in Form des IEEE-802.11-Standards zu einer akzeptablen Vereinheitlichung und der daraus resultierenden raschen Verbreitung. Funk-Netzwerke erhöhen die Mobilität der Anwender. Sie dienen immer noch als Ergänzung zu den kabelgebundenen Netzzugängen, da die im Funkbereich möglichen Bandbreiten im Vergleich zum Kabel-Netzwerk deutlich geringer sind.

Moderne Verfahren reduzieren allerdings das Ungleichgewicht, da insbesondere durch unmittelbar vor der Einführung stehende Standards wie 802.11n die Bandbreite deutlich an die der kabelgebundenen Netze heranreicht.

2.2 Standards im Funk-LAN

Im Folgenden sind die relevanten Standards im Bereich Funk-LAN und deren Eigenschaften aufgeführt.

2.2.1 IEEE 802.11

IEEE 802.11 ist der Oberbegriff für eine Reihe von Standards. Er wurde 1997 verabschiedet und stellt die große Gruppe weiterer Standards für die drahtlose Kommunikation dar.

3. Gemeinsames Netzwerkzentrum der Berlin-Brandenburgischen Max-Planck-Einrichtungen am Fritz-Haber-Institut

2.2.2 IEEE 802.11a

IEEE 802.11a ist ein 1999 verabschiedeter Standard für Funk-LANs im Frequenzbereich von 5 GHz:

Frequenzbereich	5 GHz
Bandbreite	54 Mbit/s
Kanäle	19 nicht überlappende Kanäle
Pro	aufgrund der geringen Verbreitung ist mit wenig Störungen zu rechnen

2.2.3 IEEE 802.11b

IEEE 802.11b ist ein seit 1999 gültiger Standard mit der momentan größten Verbreitung:

Frequenzbereich	2,4 GHz
Kanäle	11 - 13, nur 3 nicht überlappende Kanäle
Sendeleistung	100 mW an der Antenne
Bandbreite	11 Mbit/s
Pro	große Verbreitung und Unterstützung der Hersteller
Kontra	viele Störungen, da auch Fremdgeräte das Frequenzband nutzen (z. B. Mikrowellenherde, Babyphones, Videoübertragung)

2.2.4 IEEE 802.11g (vgl. 802.11b)

IEEE 802.11g ist ein Funk-LAN-Standard aus dem Jahr 2002/2003. Er ist vollständig abwärtskompatibel zum 802.11b-Standard, besitzt aber eine höhere Bandbreite. Neben 802.11b ist auch 802.11g ein sehr verbreiteter Standard, welcher mittlerweile in fast allen modernen Geräten integriert ist.

Frequenzbereich	2,4 GHz
Kanäle	11 - 13, nur 3 nicht überlappende Kanäle

Sendeleistung	100 mW an der Antenne
Bandbreite	54 Mbit/s
Pro	große Verbreitung und Unterstützung der Hersteller
Kontra	viele Störungen, da auch Fremdgeräte das Frequenzband nutzen (z. B. Mikrowellenherde, Babyphones, Videoübertragung)

Es existiert noch eine Reihe weiterer Standards und Abwandlungen im Bereich des IEEE 802.11, die sich mit unterschiedlichem Schwerpunkt speziellen Aufgaben widmen. Hierzu zählen die Standards 802.11e, welcher QoS und Streaming-Erweiterungen beschreibt, sowie 802.11i, der die Authentifizierung und Verschlüsselung der 802.11a/b/g-Standards behandelt. Diese und noch weitere Standardisierungen sollen hier lediglich erwähnt werden, da sie aber für die momentanen Betrachtungen eine untergeordnete Rolle spielen.

Eine Ausnahme bildet hier der zukünftige Standard 802.11n, welcher erhebliche Neuerungen im Bereich Funk-LAN verspricht und dessen Entwicklung nicht unbeachtet bleiben darf.

2.2.5 IEEE 802.11n

Der Standard IEEE 802.11n stellt einen vielversprechenden Ansatz zur Erneuerung von Funk-LAN-Systemen dar. Obwohl bereits seit mehreren Jahren in der Entwicklung, verzögerte sich aufgrund der Uneinigkeiten rivalisierender Gruppierungen innerhalb des EWC-Standardisierungskonsortiums die endgültige Verabschiedung immer wieder. Dennoch rechnen viele Experten mit der Verabschiedung von 802.11n noch in 2007, sodass die ersten Geräte gegen Ende 2007 bzw. Anfang 2008 erwartet werden.

Bereits seit Ende 2006 ist eine Reihe von Herstellern dazu übergegangen, einige Produkte, basierend auf dem ersten „Draft“ von 802.11n, auf den Markt zu bringen. Ein Aufbau einer Funk-LAN-Umgebung mit Geräten des ersten „Draft“ ist keinesfalls sinnvoll, da eine Kompatibilität zum zukünftigen Standard nicht sichergestellt werden kann.

Das EWC[4] besteht aus einer großen Gruppe namhafter Hersteller aus dem Netzwerkbereich, sodass nach der endgültigen Verabschiedung des Standards mit einer raschen Umsetzung zu rechnen ist.

Die wesentlichen Kenndaten des 802.11n sind im Folgenden aufgelistet:

- Frequenzband: 2,4 GHz
- Antennen basierend auf MIMO (Multiple-in, Multiple-out), mehrere Antennen
- bessere Richtwirkung = höhere Reichweite
- Bandbreiten (auf kurze Distanz) bis 540 Mbit/s (brutto)
- höhere Reichweiten als bei 802.11a/bg (bis zu 4-fach)

3. Funk-LAN-Verfahren und -Produktgruppen

In den letzten Jahren entstanden ganz unterschiedliche Lösungen für die Vernetzung über Funk. In der Zeit zwischen 1999 und 2003 wurden mangels homogener, integrierter Lösungen der Hersteller Funk-LAN-Infrastrukturen meist in Eigenregie durch Aneinanderreihen diverser Teillösungen realisiert.

3.1 Getrennte Funk-LAN/VPN-Lösungen

Bei der getrennten Funk-LAN/VPN-Lösung erfolgt eine Aufteilung des Gesamtsystems in die Bereiche „Funk-LAN“ und „Sicherheit“. Dabei bilden die Accesspoints die eigentliche Funk-Infrastruktur, welche lediglich den Zugang zum kabelgebundenen Netzwerk ermöglicht. Die bei Funk-LAN-Lösungen erforderliche Verschlüsselung der Datenströme übernimmt als zweite Instanz ein getrenntes VPN-Gateway.

3.1.1 MAC-Authentifizierung

Als sehr einfaches Zugangsverfahren kann die Authentifizierung der Benutzer über deren MAC-Adresse eingesetzt werden. Hier vergleicht meist ein RADIUS-Server die MAC-Adressen mit einer eigenen Datenbank und erlaubt oder verweigert den Zugang. Dieses Verfahren ist ausgesprochen unsicher, da MAC-Adressen leicht von fremden Benutzern ausgespäht und deren eigene MAC-Adressen durch gültige Adressen ersetzt werden können.

4. **EWC**, **E**nhanced **W**ireless **C**onsortium: Apple, Atheros, Broadcom, Buffalo, Cisco, Conexant, D-Link, Intel, Lenovo, Linksys, Netgear, Sanyo, Sony, Ralink, Toshiba und weitere

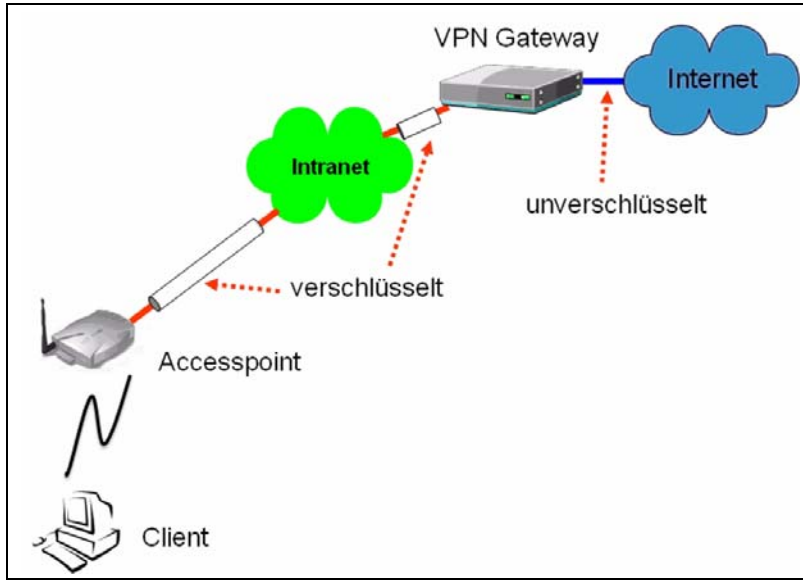


Abb. 1: Zentrales VPN-Gateway im Funk-LAN

3.1.2 Verfahren

Als VPN-Gateway können diverse Systeme und Verfahren eingesetzt werden. Mögliche Lösungen hierfür sind:

1. **VPN-Systeme** als eigenständige Geräte (z. B. CISCO VPN-Gateway 3000 oder Checkpoint)
2. **Serverlösungen**, wobei ein Rechner mit einem entsprechenden Betriebssystem die Aufgabe der VPN-Terminierung übernimmt. Hier sind als Betriebssysteme Windows 2003 Server oder diverse Linux-Distributionen geeignet.
3. **Webbasierte Verschlüsselung** mittels SSL (WebVPN). Hierbei ist keine spezielle Software auf Seiten des Clients zu installieren. Für den verschlüsselten Zugang zum Netzwerk und der Authentifizierung ist lediglich ein Webbrowser erforderlich. Allerdings ist die Nutzung auf wenige Netzwerk-Anwendungen beschränkt. Meist sind es Webseiten, die über WebVPN-Gateways erreicht werden können. Spezielle IP-Protokolle können durch WebVPN nicht übertragen werden, insbesondere dann

nicht, wenn auch Rückverbindungen mit unterschiedlichen Ports für die Kommunikation erforderlich sind.

Die o. g. Verfahren übernehmen in der Regel auch die Authentifizierung, damit der Zugang zum Netzwerk kontrolliert und auf bekannte Benutzer beschränkt werden kann. Als VPN-Protokoll stehen mehrere Verfahren zur Verfügung. Mit IPSec existiert eine standardisierte Protokoll-Suite, die diese Verfahren für das IP-Protokoll bereitstellt und auf Netzwerkebene realisiert.

Werden Windows-Systeme als VPN-Gateways verwendet, so sind häufig L2TP sowie PPTP als Verschlüsselungs-Protokoll verwendbar, wenngleich das letztgenannte Verfahren aufgrund diverser Schwächen nicht zum Einsatz kommen sollte. Entscheidend ist häufig der einfache Zugang für die Nutzerschaft. Viele VPN-Systeme benötigen einen speziellen VPN-Client auf Benutzerseite. Die Installation erfordert einen gewissen Aufwand und entsprechende Wartung, die allerdings im Vergleich zum Nutzen durchaus vertretbar ist.

Aufgrund der Häufigkeit von Microsoft-Betriebssystemen bei den Benutzern, liegt der Gedanke nahe, gerade für dieses Client-Betriebssystem den Zugang zum VPN-Gateway möglichst einfach zu gestalten. Hier würden VPN-Gateways zum Einsatz kommen, welche die bereits in den Betriebssystemen integrierten VPN-Fähigkeiten nutzen können. Abgesehen von PPTP ist es vor allem L2TP, welches eine ausreichende Verschlüsselung bietet. Ein Windows 2003 Server als VPN-Gateway kann hier als VPN-Endpunkt eingesetzt werden, wenngleich die Stabilität des Betriebssystems entscheidend für die Stabilität der Gesamtlösung ist. Mit Windows XP als Client können dann einfachere VPN-Zugänge auch ohne zusätzliche Software auf dem Client realisiert werden. Für größere Umgebungen wäre diese Variante jedoch ungeeignet.

3.1.3 Fazit

Werden Gateway- und Server-basierte Lösungen miteinander verglichen, so ist für große Funk-LAN-Strukturen der Einsatz von VPN-Gateways als eigenständige Systeme sinnvoller als softwarebasierte Gateways, welche auf PC-Hardware installiert sind. Viele integrierte VPN-Gateways beherrschen neben IPSec auch PPTP und L2TP als Protokoll, sodass auch ohne spezielle Software auf dem Client ein verschlüsselter Zugang über Funk möglich ist. Wird eine starke Verschlüsselung benötigt, so ist der Einsatz von VPN-Clients in Verbindung mit einem VPN-Gateway als Endpunkt sowie als Verschlüsselungsprotokoll IPSec (3DES) unabdingbar.

Eine Sonderrolle spielen die unter 3.1.1, Pkt. 3 genannten WebVPN-Gateways mittels SSL. Da es sich bei SSL um eine Verschlüsselung auf Applikationsebene handelt (z. B. für Webbrowser), lassen sich sehr gezielt Daten schützen, die von der jeweiligen Applikation verwendet werden. Wenn sich die Nutzung des Funk-LAN auf den Besuch von weiteren Webseiten im Internet beschränkt, so ist ein WebVPN eine einfache Möglichkeit, dieses ohne spezielle Client-Software zu erreichen. Ein WebVPN sollte als Ergänzung gesehen werden und erfüllt selten vollständig die Bedürfnisse der Benutzer hinsichtlich Nutzung des Netzwerks. Einige herstellerspezifische Erweiterungen von WebVPN-Gateways ermöglichen durch spezielle Verfahren auch das „Durchtunneln“ weiterer Protokolle, meist aber nur zu ganz bestimmten und vorher definierten Zielen. Das kann dann zum Beispiel der Zugriff auf einen Mailserver sein.

3.2 Verschlüsselung auf den Accesspoints (dezentraler Ansatz)

Viele Accesspoints stellen mit unterschiedlichen Ansätzen die Verschlüsselung direkt auf dem Accesspoint sicher. Dabei werden unterschiedliche Verschlüsselungsalgorithmen eingesetzt, welche sich hinsichtlich der Verschlüsselungstiefe und der daraus resultierenden Abhörsicherheit unterscheiden.

3.2.1 WEP

WEP[5] stellt eine einfache Verschlüsselung auf den Accesspoints dar und zählt zu den ersten verbreiteten Standards im Funk-LAN. Aufgrund eklatanter Sicherheitsdefizite ist WEP als völlig unsicher einzustufen und sollte ohne zusätzliche Sicherheitsmaßnahmen auch nicht benutzt werden.

3.2.2 WEP Plus

WEP Plus ist eine Erweiterung von WEP mit der Verwendung alternierender Schlüssel. Auch WEP Plus gilt als unsicher und sollte nicht mehr eingesetzt werden.

3.2.3 WPA

WPA[6] basiert auf WEP, bringt jedoch zusätzlichen Schutz durch dynamische Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren. Es

5. WEP, **W**ireless **E**quivalent **P**rivacy
6. WPA, **W**iFi **P**rotected **A**ccess

ist sicherer als WEP und WEP Plus und wird bei vielen Accesspoints eingesetzt. Allerdings existieren auch hier seit 2004 Programme wie „WPA Cracker“, die erfolgreiche Angriffsmöglichkeiten bieten.

3.2.4 WPA2

WPA2 stellt eine Erweiterung des WPA dar. Hier kommt AES[7] als Verschlüsselungsverfahren zum Einsatz. Es gilt als derzeit hinreichend sicher. Lediglich Dictionary-Attacken sind bei WPA2 bekannt.

3.2.5 Fazit

Der Aufbau eines Funk-LANs unter alleiniger Verwendung der Verschlüsselung auf den Accesspoints ist bereits in mittleren bis großen Netzwerken nicht sinnvoll. Es existiert meist keine zentrale Schlüsselverwaltung und der Aufwand auf Seiten des Clients ist dadurch entsprechend hoch. Überdies besteht das Problem der fehlenden Authentifizierung. Benutzer, die Zugriff auf die Schlüssel erlangen, die bei TKIP meist clientseitig durch eine „Passphrase“ realisiert sind, bekommen damit Zugang zum Netzwerk, ohne dass ein Administrator feststellen kann, wer der Benutzer ist. WPA2/TKIP ist eine gute Lösung für die Anbindung von ein bis wenigen Clients, meistens im Heimbereich. Professionelle Funk-LAN-Lösungen nutzen zwar teilweise WPA2, besitzen aber eine zentrales Management für die Accesspoints und bieten Erweiterung hinsichtlich der Authentifizierung der Benutzer.

3.3 Controller-basierte Lösungen

Der bislang vielversprechendste Ansatz für eine Funk-LAN-Lösung sind die Controller-basierten Systeme. Hierbei wird versucht, alle entscheidenden Komponenten für eine Funk-LAN-Infrastruktur in ein homogenes Konzept zu integrieren. Bei Controller-basierten Systemen wird jeder Accesspoint entweder direkt an einem speziellen Switch angeschlossen oder mehrere Accesspoints, netzwerktechnisch zusammengefasst, an einen zentralen Port angebunden. Hierbei steuert der WLAN-Switch (Controller) die Weiterleitung der Daten vom Accesspoint zum kabelgebundenen Netz.

Abhängig vom Hersteller werden unterschiedliche Konzepte verfolgt. Eine Variante „degradiert“ die Accesspoints lediglich zu schlichten Kabel-Funk-LAN-Wandlern, wobei die „Intelligenz“ der WLAN-Lösung in die zentralen Switches integriert ist (Beispiel: Trapeze). Bei dieser Lösung werden Authentifizierung und Verschlüsselung direkt vom Controller übernommen.

7. AES, **A**dvanced **E**ncryption **S**tandard

Andere Systeme verlagern einen Teil der „Intelligenz“ auf die Accesspoints, wobei der Controller die Steuerung übernimmt (Beispiele: CISCO Airespace und Aruba).

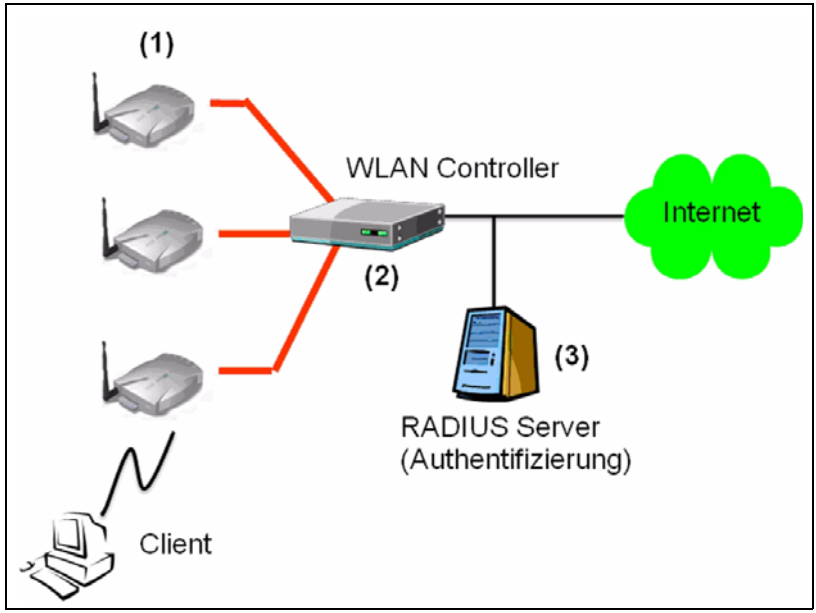


Abb. 2: Schematische Darstellung eines Controller-basierten Funk-LANs

3.3.1 Aufgaben der einzelnen Komponenten

1. Accesspoints

Die Accesspoints sind direkt mit dem Controller verbunden. Die Kommunikation zwischen Accesspoint und Controller erfolgt meist verschlüsselt, wobei die Hersteller dazu unterschiedliche und teilweise auch proprietäre Protokolle verwenden. Moderne Lösungen beinhalten häufig Accesspoints, die mit zwei parallel arbeitenden „Radios“ die bisherigen Standards 802.11a sowie 802.11b/g bedienen. Ein weiteres Merkmal kann die Möglichkeit zum Anschluss externer Antennen sein. Für die einfache Installation von Accesspoints ist auch die Stromversorgung ganz entscheidend. Dabei ist es sinnvoll, Geräte einzusetzen, welche PoE[8] nach dem Standard 802.3af

8. Power over Ethernet (Standard: 802.3af)

beherrschen. Die WLAN-Controller mit RJ45-Ethernetanschluss sind meistens in der Lage, nach diesem Standard die Accesspoints mit Strom zu versorgen. Werden 802.3af-fähige Accesspoints über fremde Switches an die Controller angebunden, so sind Switches mit PoE zu verwenden.

2. WLAN-Controller

Der WLAN-Controller übernimmt das Management der Accesspoints. Das kann zum einen ein dynamisches Radio-Management sein, wodurch die Höhe der jeweiligen Sendeleistungen sowie die Kanalwahl auf den Accesspoints automatisch den örtlichen Bedürfnissen angepasst werden. Bei etwaigem Ausfall einzelner Accesspoints kann der Controller die Sendeleistung der umliegenden Accesspoints entsprechend erhöhen, damit die „Funk-Lücke“ wieder geschlossen werden kann. Durch die Trennung in verteilte Accesspoints und zentrale Controller besteht die Möglichkeit der Skalierung des Funk-LANs, um wachsenden Anforderungen besser gerecht werden zu können. Häufig können mehrere Controller als „Verbund“ eingesetzt werden, wenn höhere Leistungen gefordert sind. Überdies wäre der Einsatz von mindestens zwei Controllern allein schon aus Redundanzgesichtspunkten unerlässlich, da die Controller einen klassischen „Single Point Of Failure“ darstellen.

3. Authentifizierung (RADIUS)

Letztlich ist eine Authentifizierung der Benutzer in Funk-LAN-Umgebungen unerlässlich. Bei vielen Lösungen ist ein RADIUS-Server die zentrale Authentifizierungsinstanz. Der RADIUS-Server kann seinerseits Benutzerdatenbanken via LDAP, Active Directory oder weitere Verzeichnisdienste als Datenbasis abfragen, sodass als Kommunikationspartner für den Controller immer der RADIUS-Server die entscheidende Instanz darstellt. Einige Produkte erlauben überdies auch die Übertragung spezifischer Attribute wie VLAN und Security-Policies vom RADIUS an den Controller, sodass benutzer- und gruppenabhängig bestimmte Eigenschaften für den Anwender nutzbar sind.

3.3.2 Anbindung von Fremd-Accesspoints

Allen Controller-basierten Lösungen gemein ist die Tatsache, dass die Accesspoints des jeweils eigenen Herstellers in Verbindung mit dem Controller natürlich die meisten Funktionalitäten bieten. Dennoch können bei vielen Systemen auch Accesspoints fremder Hersteller integriert werden, wobei dieses oft mit einem Verlust wesentlicher Merkmale einhergeht. Dieser Gesichtspunkt ist nicht unwichtig, wenn eine bereits installierte Funk-LAN-Umgebung durch neue Controller-basierte Systeme ersetzt werden

soll. Hierbei erleichtert auch die teilweise Integrationsfähigkeit fremder Accesspoints den Migrationsprozess.

3.3.3 Verschlüsselung, Authentifizierung und Zugang

Typisch für Controller-basierte Lösungen ist die Eigenschaft, eine ganze Reihe möglicher Zugangswege zu bieten. Die drei wesentlichen sind hier aufgeführt:

1. Web-basierte Anmeldung

Die einfachste Variante stellt die Web-basierte Anmeldung am Funk-LAN dar. Hier ist auf Seiten des Benutzers lediglich ein Webbrowser erforderlich. Eine spezielle Webseite erfragt hierbei Benutzername und Passwort und erlaubt bei korrekter Eingabe anschließend den Zugang zum Netz. Abhängig von der Installation kann oder muss dieser Prozess in gewissen Abständen wiederholt werden. Diese Zugangsvariante ermöglicht hierbei keinerlei Verschlüsselung, sodass die Benutzer selbst für ausreichende Verschlüsselung bei der Kommunikation sorgen müssen (https, IMAPs, POP3s etc.). Dieses Verfahren ist häufig auch für Geräte geeignet, bei denen keine speziellen Clients installiert werden können (PDA).

2. 802.1X und ähnliche Varianten

Nahezu alle Controller erlauben den Zugang über den Standard 802.1x. 802.1x beschreibt den Zugang zum Netzwerk. Die Verschlüsselung selbst ist optional. Häufig aber wird 802.1x mit den Verschlüsselungsvarianten im EAP[9] verwendet. Hierbei können EAP-TLS, EAP-TTLS, PEAP sowie LEAP eingesetzt werden. Insbesondere PEAP findet weite Verbreitung, da es ohne größeren Aufwand von neueren Microsoft-Betriebssystemen unterstützt wird. Bei den EAP-Varianten ist überdies die Nutzung von Zertifikaten eine weitere Möglichkeit, die Username/Password-Kombinationen zu erset-

9. EAP, Extensible Authentication Protocol

zen. Allerdings erfordert dieses Verfahren eine CA-Umgebung, die nicht immer vorhanden ist.

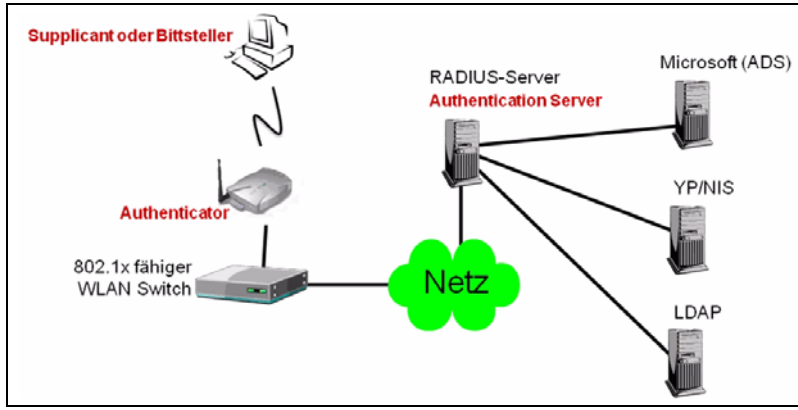


Abb. 3: Prinzip des 802.1x

Bei 802.1x erfolgt zunächst die Anfrage des „Supplicant“ an den „Authenticator“. Dieser kommuniziert mit dem WLAN-Controller, der wiederum beim RADIUS-Server nachfragt, ob der Benutzer/Rechner authentifiziert wird. Dieser Vorgang ist nicht immer trivial, weshalb die controller-basierten Lösungen wesentliche Teile dieses Verfahrens im eigenen System integriert haben, sodass meist nur noch ein externer RADIUS-Server angebunden werden muss.

3.3.4 Management

Funk-LAN-Lösungen, die auf Controllern basieren, werden mit zentralen Managementlösungen installiert. Mit solchen speziellen Lösungen sind Gruppierungen und die Einrichtung von diversen Richtlinien möglich. Auch Gästezugänge sind meist Bestandteil eines controller-basierten Systems. Eine weitere Stärke ist die Überwachung und das Accounting der gesamten Funk-LAN-Umgebung. Einige Lösungen besitzen Schnittstellen für verbreitete Netzwerkmanagementsysteme wie z. B. HP OpenView. Dennoch empfiehlt sich meist die Nutzung des mitgelieferten Managements, da nur hiermit die teilweise komplexen Abläufe beherrscht werden können.

Einige Lösungen liefern ein eigenes Programm für die Planung und Ausleuchtung von Funk-LAN-Standorten mit. Dabei können Gebäudegrundrisse integriert werden und durch Angabe der Dämpfungswerte der Wände

ergänzt können diese Programme eine bessere Positionierung der Accesspoints bestimmen.

3.3.5 Voice over WLAN, Roaming

Entscheidend für eine moderne Funk-LAN-Lösung ist natürlich die Möglichkeit, den Standort zu wechseln, ohne dass Verbindungsabbrüche, Wechsel der IP-Adresse oder Unterbrechungen in der Kommunikation die Folge sind. Bei controller-basierten Lösungen ist die Fähigkeit zum „Roaming" meistens gegeben. Allerdings unterscheiden sich die Systeme in der Umschaltzeit, in der ein Wechsel des Accesspoints erkannt und die Kommunikation entsprechend übernommen wird. Gerade für Voice- und Videoverbindungen sind schnelle Umschaltzeiten essentiell. Im Bereich VoIP werden Unterbrechungen von bis zu 100 ms noch toleriert. Größere Unterbrechungen machen Voice over WLAN unbrauchbar.

4. Zukünftige Entwicklungen im Bereich Funk-LAN

Die Entscheidung für eine geeignete Funk-LAN-Lösung ist nicht immer einfach. Gerade im Zeitraum 2007/2008 stehen Entwicklungen bevor, die eine Auswahl der richtigen Komponenten beeinflussen.

Ende 2007 ist mit der Übernahme von 802.11n als Standard zu rechnen, sodass spätestens 2008 die Geräte der Hersteller verfügbar sein werden. Wichtig ist bei derzeit installierten oder kurzfristig zu installierenden Lösungen die Aussage des Herstellers, ob die Systeme kostengünstig auf 802.11n umgesteckt werden können. Accesspoints nach dem Standard 802.11a/b/g werden in jedem Fall nicht in der Lage sein, nach dem Standard 802.11n zu funktionieren, weshalb ein späterer Austausch der Komponenten immer erforderlich wird. Bei controller-basierten Lösungen muss überdies geklärt werden, ob die Controller selbst den höheren Anforderungen hinsichtlich Bandbreite und Latenz des 802.11n-Standards genügen. Immerhin ist mit einer sieben- bis zehnfachen Erhöhung der Bandbreite zu rechnen. Von den beiden angefragten Herstellern Trapeze und Aruba haben wir diesbezüglich eine positive Antwort bekommen. Beide Hersteller versichern, dass deren zentrale Controller sowie die Managementsoftware den neuen Anforderungen nach einem kostenfreien/kostengünstigen Upgrade genügen werden. Der Austausch der Accesspoints ist natürlich auch hier obligatorisch.

5. Schlussbetrachtung

Werden die bisherigen Standards und die zur Verfügung stehenden Varianten hinsichtlich Verschlüsselung und Authentifizierung berücksichtigt, so ist

nach derzeitigem Stand eine controller-basierte Lösung die richtige Wahl. Hierbei werden integriertes Management und die Möglichkeit diverser Zugangsverfahren sowie unterschiedliche Gruppierungen und Benutzerregeln in eine homogene Lösung integriert.

Da mittlerweile fast alle namhaften Hersteller zu controller-basierten Funk-LAN-Lösungen übergegangen sind, ist die Auswahl entsprechend groß. Eklatante Unterschiede sind zumindest bei den großen Herstellern nicht mehr zu finden (Trapeze, Aruba und CISCO). Unterschiede im Bereich „Roaming“ sind entsprechend den Anforderungen im eigenen Netz und dem Wunsch nach Voice over WLAN verknüpft und dominieren möglicherweise die Produktauswahl.

In der Reihe GWDG-Berichte sind zuletzt erschienen:

Nähere Informationen finden Sie im Internet unter
`http://www.gwdg.de/forschung/publikationen/gwdg-berichte`

Nr. 40 *Plesser, Theo und Peter Wittenburg* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1994
1995

Nr. 41 *Brinkmeier, Fritz* (Hrsg.):
Rechner, Netze, Spezialisten. Vom Maschinenzentrum zum Kompetenzzentrum - Vorträge des Kolloquiums zum 25jährigen Bestehen der GWDG
1996

Nr. 42 *Plesser, Theo und Peter Wittenburg* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1995
1996

Nr. 43 *Wall, Dieter* (Hrsg.):
Kostenrechnung im wissenschaftlichen Rechenzentrum - Das Göttinger Modell
1996

Nr. 44 *Plesser, Theo und Peter Wittenburg* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1996
1997

Nr. 45 *Koke, Hartmut und Engelbert Ziegler* (Hrsg.):
13. DV-Treffen der Max-Planck-Institute - 21.-22. November 1996 in Göttingen
1997

Nr. 46 **Jahresberichte 1994 bis 1996**
1997

Nr. 47 *Heuer, Konrad, Eberhard Mönkeberg und Ulrich Schwardmann*:
Server-Betrieb mit Standard-PC-Hardware unter freien UNIX-Betriebssystemen
1998

Nr. 48 *Haan, Oswald* (Hrsg.):
Göttinger Informatik Kolloquium - Vorträge aus den Jahren 1996/97
1998

Nr. 49 *Koke, Hartmut und Engelbert Ziegler* (Hrsg.):
IT-Infrastruktur im wissenschaftlichen Umfeld - 14. DV-Treffen der Max-Planck-Institute, 20. - 21. November 1997 in Göttingen
1998

Nr. 50 *Gerling, Rainer W.* (Hrsg.):
Datenschutz und neue Medien - Datenschutzschulung am 25./26. Mai 1998
1998

Nr. 51 *Plesser, Theo und Peter Wittenburg* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1997
1998

Nr. 52 *Heinzel, Stefan und Theo Plesser* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1998
1999

Nr. 53 *Kaspar, Friedbert und Hans-Ulrich Zimmermann* (Hrsg.):
Internet- und Intranet-Technologien in der wissenschaftlichen Datenverarbeitung - 15. DV-Treffen der Max-Planck-Institute, 18. - 20. November 1998 in Göttingen
1999

Nr. 54 *Plesser, Theo und Helmut Hayd* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1999
2000

Nr. 55 *Kaspar, Friedbert und Hans-Ulrich Zimmermann* (Hrsg.):
Neue Technologien zur Nutzung von Netzdiensten - 16. DV-Treffen der Max-Planck-Institute, 17. - 19. November 1999 in Göttingen
2000

Nr. 56 *Plesser, Theo und Helmut Hayd* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2000
2001

Nr. 57 *Hayd, Helmut und Rainer Kleinrensing* (Hrsg.):
17. und 18. DV-Treffen der Max-Planck-Institute
22. - 24. November 2000 in Göttingen
21. - 23. November 2001 in Göttingen
2002

Nr. 58 *Plesser, Theo und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2001
2003

Nr. 59 *Suchodoletz, Dirk von*:
Effizienter Betrieb großer Rechnerpools - Implementierung am Beispiel des Studierendennetzes an der Universität Göttingen
2003

Nr. 60 *Haan, Oswald* (Hrsg.):
Erfahrungen mit den IBM-Parallelrechnersystemen RS/6000 SP und pSeries690
2003

Nr. 61 *Rieger, Sebastian:*
Streaming-Media und Multicasting in drahtlosen Netzwerken - Untersuchung von Realisierungs- und Anwendungsmöglichkeiten
2003

Nr. 62 *Kremer, Kurt und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2002
2003

Nr. 63 *Kremer, Kurt und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2003
2004

Nr. 64 *Koke, Hartmut* (Hrsg.):
GÖ* – Integriertes Informationsmanagement im heterogenen eScience-Umfeld: GÖ*-Vorantrag für die DFG-Förderinitiative „Leistungszentren für Forschungsinformation“
2004

Nr. 65 *Koke, Hartmut* (Hrsg.):
GÖ* – Integriertes Informationsmanagement im heterogenen eScience-Umfeld: GÖ*-Hauptantrag für die DFG-Förderinitiative „Leistungszentren für Forschungsinformation“
2004

Nr. 66 *Bussmann, Dietmar und Andreas Oberreuter* (Hrsg.):
19. und 20. DV-Treffen der Max-Planck-Institute
20. - 22. November 2002 in Göttingen
19. - 21. November 2003 in Göttingen
2004

Nr. 67 *Gartmann, Christoph und Jochen Jähnke* (Hrsg.):
21. DV-Treffen der Max-Planck-Institute
17. - 19. November 2004 in Göttingen
2005

Nr. 68 *Kremer, Kurt und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2004
2005

Nr. 69 *Kremer, Kurt und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2005
2006

Nr. 70 *Gartmann, Christoph und Jochen Jähnke* (Hrsg.):
22. DV-Treffen der Max-Planck-Institute
16. - 18. November 2005 in Göttingen
2006

Nr. 71 *Hermann, Klaus und Jörg Kantel* (Hrsg.):
23. DV-Treffen der Max-Planck-Institute
15. - 17. November 2006 in Berlin
2007

Nr. 72 *Kremer, Kurt und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2006
2007

Nr. 73 *Baumann, Thomas, Dieter Ruder und Bertram Smolny* (Hrsg.):
24. DV-Treffen der Max-Planck-Institute
6. - 8. November 2007 in Jena
2008