ISSN 1866-4954 JUNI 2010 / 2

Steinbuch Centre for Computing

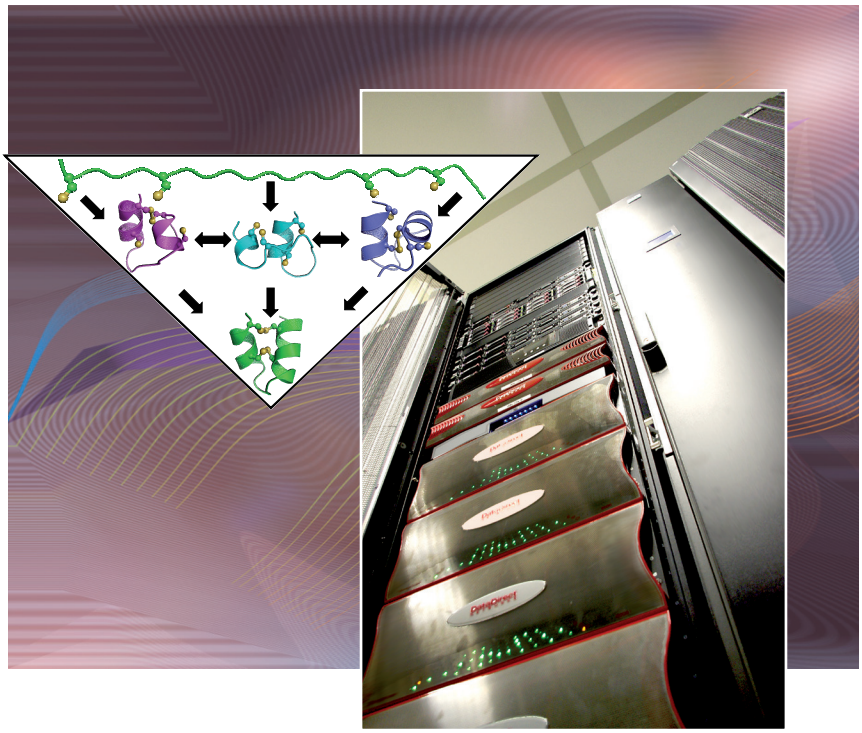
NEWS SCC

Erster Spatenstich für neues Institutsgebäude

Neuartiges Speicherkonzept für die Wissenschaft

Large Scale Data Facility am SCC stellt systembiologische Daten weltweit zur Verfügung

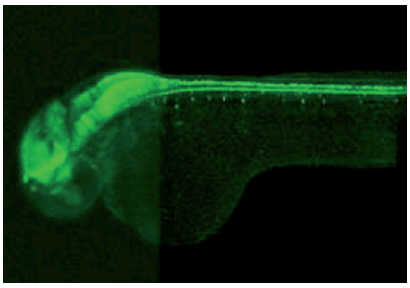
Schnell und stabil – der neue Hochleistungsrechner am SCC



KIT – Universität des Landes Baden-Württemberg und nationales Forschungszentrum in der Helmholtz-Gemeinschaft

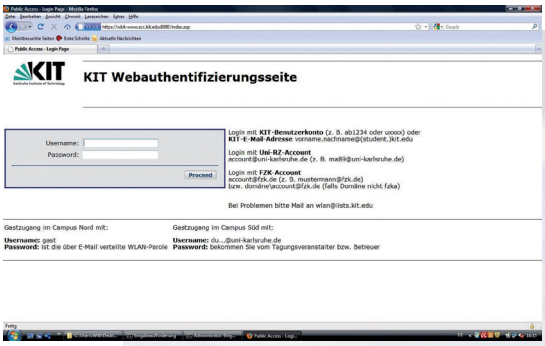
INHALT

4

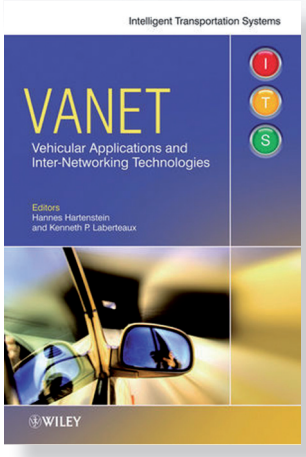


5

10



19



21

EDITORIAL

Liebe Leserinnen und Leser,

lange Jahre der Planung gingen voraus, nun erfolgte im April auf dem Campus Nord der erste Spatenstich für das neue gemeinsame Institutsgebäude des SCC und des Instituts für Angewandte Informatik (IAI). Der Neubau, dessen Gesamtkosten mit 7 Millionen Euro veranschlagt sind, soll bis Ende 2011 fertig gestellt sein. Auf über 3.000 Quadratmetern sieht das dreigeschossige Gebäude eine Technikumshalle, Büroflächen, Besprechungsräume, einen Hörsaal sowie einen Seminarraum vor. Das SCC benötigt den Platz insbesondere für die Erweiterung des Grid Computing Centre Karlsruhe (GridKa), da es neben seiner Funktion als international operierendes Tier1-Zentrum für den Large Hadron Collider am CERN für die Anforderungen weiterer Wissenschaftszweige zu einem führenden nationalen Grid-Rechenzentrum ausgebaut werden soll.

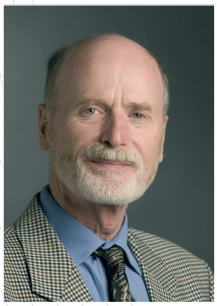
Eine führende Position will das SCC auch im Bereich der Speicherung und Verwaltung von großen Datenmengen einnehmen. Mit einem neuartigen Speicherkonzept und dem Aufbau einer Large Scale Data Facility, die riesige Mengen an Datenspeicher und Compute-Ressourcen bereitstellen wird, sollen den verschiedensten wissenschaftlichen Disziplinen neue Forschungsmöglichkeiten eröffnet werden. Für die Systembiologie steht die Anlage bereits weltweit zur Verfügung.

Um darüber hinaus den Wissenschaftlern am KIT eine optimale Rechnerversorgung im Bereich des High Performance Computing (HPC) anzubieten, hat das SCC Mitte Februar einen neuen Hochleistungsrechner vom Typ HP XC3000 in Betrieb genommen. Für viele Institute ist HPC bereits seit langem aus der Forschung nicht mehr wegzudenken und immer mehr Wissenschaftszweige nutzen zunehmend die Möglichkeiten der numerischen Simulation. Inzwischen rechnen mehr als 250 Wissenschaftler auf dem neuen KIT-Hochleistungsrechner, der seit seiner Inbetriebnahme äußerst stabil und ohne technische Probleme läuft.

Viel Vergnügen bei der Lektüre wünschen Ihnen
Hannes Hartenstein, Wilfried Juling und Klaus-Peter Mickel

Prof. Dr. Hannes Hartenstein
Foto: Privat

Prof. Dr. Wilfried Juling
Foto: Privat



Klaus-Peter Mickel
Foto: Privat

IMPRESSUM

Juni 2010
Herausgegeben im Auftrag des Direktoriums des Steinbuch Centre for Computing (SCC) von der Stabsstelle Öffentlichkeitsarbeit und Kommunikation
Anschrift: Steinbuch Centre for Computing (SCC)
Redaktion SCC-News
Zirkel 2
76128 Karlsruhe bzw.
Hermann-von-Helmholtz-Platz 1
76344 Eggenstein-Leopoldshafen
Fax: 0721/32550
http://www.scc.kit.edu/publikationen/80.php

Redaktion:
Ursula Scheller (verantwortlich)
Telefon: 0721/608-4865
E-Mail: ursula.scheller@kit.edu
Layout und Bildredaktion: John Atkinson

Erster Spatenstich für neues Institutsgebäude

Für das Institut für Angewandte Informatik (IAI) und das Steinbuch Centre for Computing (SCC) wird bis Ende 2011 auf dem Campus Nord ein neues Gebäude errichtet, dessen Gesamtkosten mit 7 Millionen Euro veranschlagt sind. Der erste Spatenstich fand am 26. April statt.

Prof. Dr. Georg Bretthauer, Leiter des Instituts für Angewandte Informatik, Prof. Dr. Detlev Löhe, KIT-Vizepräsident für Forschung und Information, und Klaus-Peter Mickel, Technisch-Wissenschaftlicher Direktor des SCC (von links), beim gemeinsamen Spatenstich für das neue Institutsgebäude.
Foto: Markus Breig

Mit Mitteln des Bundes werde auf über 3.000 Quadratmetern für die vielfältigen Aktivitäten des SCC und IAI ein geeignetes Umfeld bereitgestellt, das Raum für neue Ideen in Forschung und Infrastruktur bietet, erklärte Professor Detlev Löhe, KIT-Vizepräsident für Forschung und Information. Das dreigeschossige Gebäude sieht Büroflächen für insgesamt 140 Mitarbeiter der beiden Institute, Besprechungsräume, einen Hörsaal für 100 Personen sowie einen Seminarraum für 50 Personen vor.

„Das SCC wird das neue Gebäude insbesondere für den dringend erforderlichen Ausbau des zugehörigen Grid Computing Centre Karlsruhe nutzen“, sagte Klaus-Peter Mickel, Technisch-Wissenschaftlicher Direktor des SCC. Etwa 50 neue Mitarbeiter sollen dort Platz finden. Das Grid Computing Centre Karlsruhe (GridKa) ist als einer der elf weltweiten Hauptknotenpunkte maßgeblich an der Speicherung und Analyse der Daten aus den Experimenten des Large Hadron Collider (LHC) am europäischen Forschungzentrum CERN in Genf beteiligt. Darüber hinaus soll GridKa für die Anforderungen weiterer Wissenschaftszweige, wie beispielsweise der Systembiologie, zu einem führenden nationalen Grid-Rechenzentrum ausgebaut werden.

Für das Institut für Angewandte Informatik ist neben der dringend erforderlichen Erweiterung des Institutsgebäudes vor allem die 250 Quadratmeter große Technikumshalle von Bedeutung. „Dort werden wir im Rahmen unserer Forschungsarbeiten zur Nutzung regenerativer Energien, Energiespeicher und prototypische Automatisierungslösungen im Bereich Geothermie aufbauen und testen“, so Professor Georg Bretthauer, Leiter des IAI.

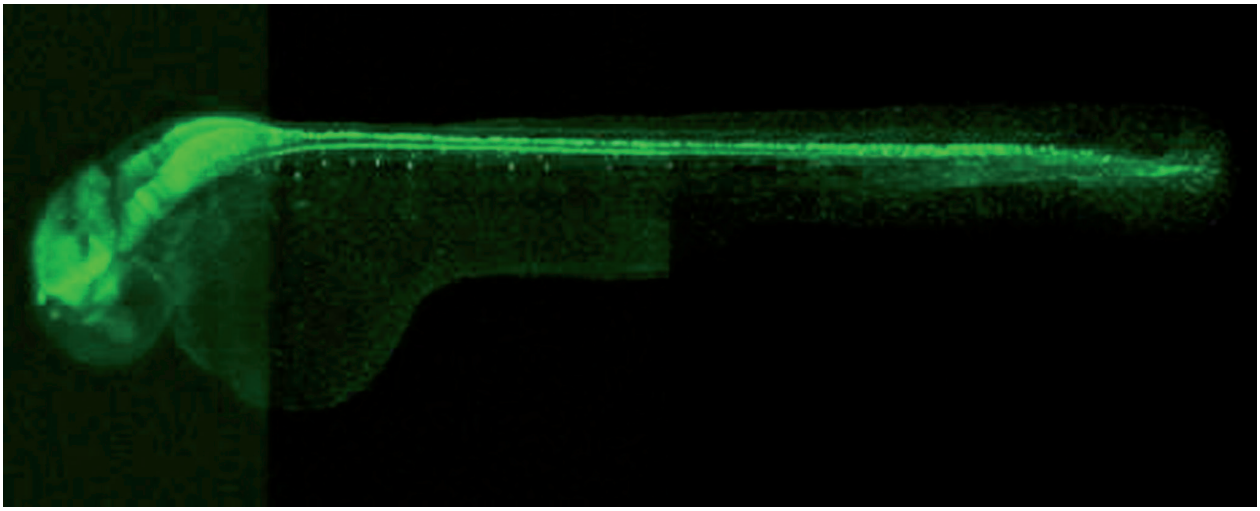
Das Energiekonzept des Institutsgebäudes basiert auf der Nutzung oberflächennaher Geothermie in Verbindung mit einer Bauteilaktivierung, die sowohl zu Heiz- als auch Kühlzwecken verwendet wird. Wasserführende Rohrleitungen in den Betondecken nutzen den Speichereffekt des Betons und sorgen für eine angenehme Temperierung der Räume. Die Energieversorgung erfolgt über eine Wärmepumpe, die das ganzjährig mit nahezu gleicher Temperatur zur Verfügung stehende Grundwasser nutzt.

(red)

Das neue Institutsgebäude: Mehr Raum für das Grid Computing Centre Karlsruhe und das Institut für Angewandte Informatik.
Quelle: Obermeyer Planen + Beraten GmbH

Neuartiges Speicherkonzept für die Wissenschaft

Large Scale Data Facility am SCC stellt systembiologische Daten weltweit zur Verfügung



Embryo des Zebrabärblings.
Foto: Institut für Toxikologie und Genetik

In enger Kooperation mit dem Institut für Toxikologie und Genetik (ITG) und dem Institut für angewandte Informatik (IAI) entwickelt das SCC eine neuartige Large Scale Data Facility (LSDF) für die Speicherung von wissenschaftlichen Daten. Die Anlage wird in den nächsten Jahren mit vielen Petabyte an Platten- und Bandspeicher-Volumen ausgebaut und steht weltweit für die Systembiologie zur Verfügung.

Im ITG entstehen im Forschungsfeld „Rekonstruktion der embryonalen Entwicklung von Zebrafischen unter Einsatz der Hochdurchsatzmikroskopie“ in einem Zeitintervall von 36 Stunden etwa 300.000 Bilder, was einer Datenmenge von 2 bis 3 Terabyte entspricht. „Das SCC ist für unsere Anforderung bezüglich der Speicherung und Verwaltung von großen Datenmengen mit seiner langjährigen Erfahrung auf diesem Gebiet der ideale Partner“, so Prof. Dr. Uwe Strähle, Institutsleiter am ITG.

Der Aufbau der LSDF-Infrastruktur umfasst nicht nur die Bereitstellung von großen Mengen an Datenspeicher- und Computer-Ressourcen, sondern liefert auch neue Forschungsaspekte, die das SCC zusammen mit den Instituten für Prozessdatenverarbeitung und Elektronik (IPE) sowie für Angewandte Informatik (IAI) bearbeiten wird.

Im Fokus von Forschung und Entwicklung stehen der hochperformante und sichere Zugriff auf die Facility, automatisierte Workflows zur Verschiebung der Daten in unterschiedliche Speicherklassen, die Langzeitarchivierung unter Wahrung der Integrität, die Analyse der Daten sowie die Entwicklung von komplexen Bildverarbeitungsalgorithmen und Schnittstellen zur LSDF. „Wir sehen in dem Thema LSDF ein langfristig tragfähiges Forschungsgebiet für das SCC, mit dem wir neben der Systembiologie auch andere Wissenschaften effektiv unterstützen wollen“, beschreibt Prof. Dr. Wilfried Juling, Geschäftsführender Direktor, den neuen Forschungs- und Entwicklungsschwerpunkt am SCC.

Das ITG, das sich mit der Identifizierung und Charakterisierung von Molekülen beschäftigt, die das Zellverhalten steuern, benutzt die Süßwasserfische Zebrabärbling und Medaka als Tiermodelle. Dazu betreibt das ITG eine der größten experimentellen Anlagen zur Haltung dieser Fische. Geplant ist, diese Anlage zum europäischen Ressourcenzentrum auszubauen. Die Verknüpfung dieses Ressourcenzentrums mit der LSDF eröffnet völlig neue Möglichkeiten der Erforschung von Entwicklungsmechanismen und wird in dieser Form eine weltweit einzigartige Anlage darstellen. Ein Ziel ist es, durch Einbindung der LSDF und Verwendung großer Datensätze Modelle zu erstellen, mit denen man die Organentwicklung und -regeneration simulieren kann. „Wir wollen langfristig durch Computersimulation virtuelle Embryonen und Organe erstellen, um somit die Natur besser verstehen zu können“, so die beiden ITG-Professoren Strähle und Wittbrodt.

Das SCC blickt auf zehn Jahre Erfahrung beim Management von großen Datenmengen zurück. Beim Worldwide Large Hadron Collider Computing Grid (WLCG)-Projekt hat das SCC mit seinem Grid Computing Centre Karlsruhe (GridKa) - eines der elf weltweiten Tier1-Zentren für den Large Hadron Collider (LHC), das die Daten direkt vom Europäischen Forschungszentrum CERN in Genf erhält - die Rolle eines führenden Datenproviders für die Experimente der Hochenergiephysik übernommen. Zurzeit sind 10 Petabyte an Platten- und Bandspeicher aufgebaut.

(red)

Protein folding simulation at the SimLab NanoMikro meets new HPC challenges

Complementing experiment and theory, computer simulation gains increasing importance in materials research and life sciences. Simulations help to understand observed phenomena and even predict properties and scenarios in complex systems. Especially challenging is the quest for new materials and phenomena for which an experimental exploration without the knowledge from simulations would be prohibitive.

The development of methods for the quantitative prediction of the three dimensional structure of proteins and their complexes belongs to the grand computational challenges of the 21th century. After the completion of diverse genome projects the blueprint of human and other organisms is now available for research. However, to understand and to predict the interplay between the nanoscale protein machines encoded in the genes it is essential to analyze the three-dimensional structure of proteins (see figure 1), the structure of the protein in its biologically active state. Experimental approaches for determination of the three-dimensional structure are very expensive and for important protein families, e.g. membrane proteins, only of limited applicability. In recent years, computer based approaches have made substantial progress in predicting protein structures on the basis of sequence comparisons with databases of proteins with known structure. The search using these methods is, however, restricted to protein families for which at least one member has already a known structure.

The problem of finding the tertiary structure of a protein is a well-known mathematical problem of non-polynomial complexity (NP) described already in the 1960-ies as the Levinthal paradox. The paradox arises because the number of possible conformations of a protein increases exponentially with the number of amino-acid residues. If one residue had only 2 folding states, there would be for a chain of N residues 2^N possible folding conformations. If we assume a folding time of 1 femtosecond (10^{-15} seconds) then a protein of 100 residues would need about 4 million years to visit all its possible conformations. In nature, such a protein finds its natural conformation in the range from several seconds up to several minutes. This "paradox" led to the hypothesis that the folding of a protein into its biologically active state must be steered by natural mechanisms rather than by a purely combinatorial search. Also in the 1960-ies, Christian Anfinsen formulated a theory (that he verified experimentally) stating that the folded structure of many proteins in their native environment is thermodynamically the most stable one (with lowest free energy) and determined completely by the amino-acid sequence and the interactions with the environment.

Traditionally, phenomenological models have been applied to describe and understand the folding process of proteins. These models require the knowledge of native protein structures in their definition. Alternatively, molecular dynamics (MD) methods with atomic resolution have been applied. The latter reconstruct the protein structure formation in a resolution of femtoseconds. Because the overall folding process often takes place on the micro or millisecond timescale the simulation of even small proteins on the nanosecond scale is often at the limit of existing computational capabilities. The low granularity of the methods (synchronisation after every energy calculation) makes the usage of distributed computing resources difficult. Recent implementations of force fields on GPGPUs can significantly accelerate single energy computations, however, cannot influence the overall scaling behaviour of the simulation method due to the granularity issue.

Presently, the protein structure prediction is dominated by heuristic approaches that produce models on the basis of sequence similarities with proteins with resolved structure. The predictive strength of these methods is reviewed every two years in the Critical Assessment of Techniques for Protein Structure Prediction (CASP, see predictioncenter.org). Thereby it has been found that for experimentally relevant proteins with sequence similarity of over 40% compared with a known protein these knowledge-based methods are successful within almost experimental resolution. In some cases, also the prediction of novel folding motives has been successful. Among the major drawbacks of these methods are the often insufficient fidelity of the prediction and the lack of quality assessment for the proposed structures. For the most recent CASP competition the independent reviewers have found no visible improvements in the results of "template-free" target proteins comparing to earlier competitions. This is why the development of novel methods is necessary. Because of the high numerical expenses the physics-based methods have not contributed much to predicting protein structures. This motivates the development of high performance implementations in order to close these methodological gaps in protein structure prediction.

The great challenge for the coming years, being currently addressed to the SimLab NanoMikro, is the development of high-throughput approaches of high prediction quality for proteins with low sequence similarity compared to already resolved proteins. In cooperation with the Institute of Nanotechnology (INT) at Karlsruhe Institute of Technology novel massively parallel algorithms have been developed basing on physical models. With these methods, over twenty smaller proteins could be folded into their biologically active structure utilizing up to 10,000 processors simultaneously. Due to the high computational demand these methods and codes are still restricted to relatively small proteins. In

the running project HPC-5, funded by the Landesstiftung Baden-Württemberg that has started in the fourth quarter of 2009, we combine our models and algorithms with established techniques from bioinformatics in order to address larger proteins of biological and practical relevance.

The deployment of efficient algorithms on HPC architectures can help in the accomplishment of these challenging tasks. In particular, adoption of state-of-the-art multi-core processors as well as next-generation HPC processor architectures, such as GPGPU (General Purpose Graphical Processing Units) will be a significant part of our code development in the next years.

Since many years, the development of biophysical methods with atomic resolution has been pursued in close and continuous cooperation with the SCC (F. Schmitz, A. Verma, and I. Kondov) and the group of W. Wenzel at the Institute of Nanotechnology. Currently, the activities are continued within the SimLab NanoMikro (K. Klenin, M. Brieg, and I. Kondov). The combination of physics-based simulation approaches with sequence-based (knowledge-based) modelling enables the treatment of proteins of low sequence similarity with known structures and thus promises high-impact applications in the field of life sciences and capability computing. The developed tools will be made available for interested biologists, pharmacists and medics directly for employment in life sciences.

Development of a universal force field for protein folding und structure prediction

Together we develop the code POEM (Protein Optimization with Energy Methods) to meet the challenges in the field of protein folding on high-performance architectures. In this method the INT group has implemented the Protein Force Fields PFF01 and PFF02 for the free energy of proteins in their physiological environment. Using these force fields a number of small proteins could be folded reproducibly and atomically resolved. Today, over 27 proteins with up to 72 amino-acid residues of all structure classes could be folded with an average deviation of 2.8 Å from their experimental resolution. Because the direct folding of proteins from completely disordered conformations is computationally demanding, new efficient optimization methods have been developed and implemented and the force field was validated against the ROSETTA test datasets. Thereby was shown that PFF02 recognized all proteins from the dataset to be in their native conformations and even was able to filter out the correct structures from incomplete test datasets in 80% of the cases.

Our biophysical model requires the use of a so called implicit solvent model in which the aqueous environment of the protein is described by an effective model. The main bottleneck of the calculation is the computation of the surface elements of the protein interfacing with the solvent, which results in about 60% of the total simulation numerical effort. We have recently developed a very efficient analytical method for these calculations that is also very suitable for special architectures with low memory bandwidth like GPGPUs.

Development of efficient folding algorithms for distributed computer architectures

To speed up the simulations an efficient evolutionary algorithm has been implemented that partitions the overall folding simulation into many thousands partial simulations. With this algorithm, a protein with 60 amino-acid residues could be reproducibly folded. On one of the first large Blue Gene installations (4096 processors) at the IBM Capacity on Demand Center (Rochester, USA) we could test the scalability of the method and demonstrated the folding of a protein with 40 amino-acid residues on one single day. Later the algorithm was deployed on other supercomputing facilities, e.g. at the Supercomputing Center MareNostrum in Barcelona. Motivated by this positive experience, we began implementing the distributed computing network POEM@HOME (http://boinc.fzk.de). With POEM@HOME a protein simulation using the methods in POEM can be distributed over resources worldwide. Currently, other stochastic optimization algorithms such as particle swarm optimization are being developed and tested in the group with special focus on parallelization.

Using this technology we participated in the CASP8 competition and submitted blind predictions for 150 proteins, achieving a respectable rank 5 in the template-free modelling area in a field of 298 groups. At that time, only physics-based models and no knowledge of homology were used for the prediction. Thus, for proteins with high sequence similarity the results were not satisfactory. In the coming competition CASP9 (beginning in April 2010) novel knowledge-based techniques will also be employed for the prediction.

Dr. Ivan Kondov

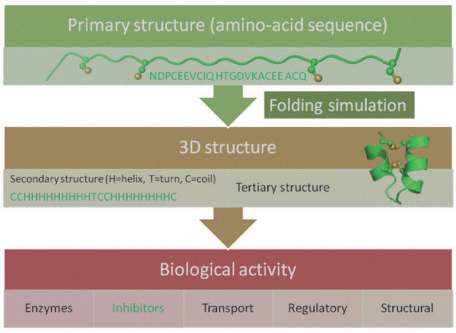


Figure 1: A diagram showing the role of protein folding simulations for understanding the relation between structure and function. The amino-acid sequence (primary structure), shown in one letter code, the secondary structure, cartoons and the biological function of the potassium channel blocker 1WQE are indicated in green colour.

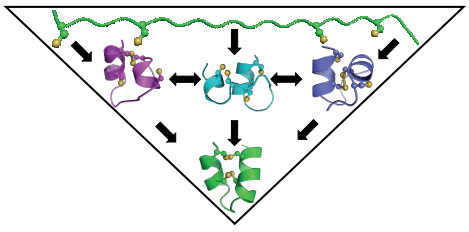


Figure 2: Folding paths for potassium channel blocker 1WQE, a toxin isolated from the scorpion Opisthacanthus madagascariensis. On the top the extended conformation, at the bottom the native folded conformation are shown. Source: I. Kondov, A. Verma, and W. Wenzel, Biochemistry 48, 8195-8205 (2009).

Konsistenz identitätsbezogener Informationen in verteilten Systemen

In verteilten IT-Umgebungen werden Informationen oftmals redundant gespeichert, beispielsweise um die Ausfallsicherheit oder Performanz eines Systems zu verbessern. Insbesondere bei Identitätsinformationen von Benutzern, die für einen gesicherten Zugriff auf IT-Dienste verwendet werden, ist häufig eine verteilte Vorhaltung anzutreffen. Da sich identitätsbezogene Informationen ändern, gilt es geeignete Mechanismen einzusetzen, um Inkonsistenzen in diesen Daten zu vermeiden. Eine aktuelle Forschungsarbeit mit Bezug auf die Realisierung eines föderativen Identitätsmanagements am KIT schlägt hierbei einen Mechanismus zur Sicherstellung der Informationskonsistenz in verteilten Systemen vor [1]. Die Arbeit wurde auf der Fifth International Conference on Availability, Reliability and Security (ARES 2010) veröffentlicht und diskutiert.

Organisationsübergreifende Kooperationen, beispielsweise mit dem Ziel neue Funktionalitäten oder einen vereinfachten Zugriff auf angebotene Dienste bereit zu stellen, sind heutzutage ein wichtiges Instrument, um im Wettbewerb mit konkurrierenden Organisationen bestehen zu können. Zum Beispiel erlaubt die Kooperation des KIT und der ReDi (Regionale Datenbank-Information) KIT-Benutzern, über ihr bestehendes Benutzerkonto bibliographische Volltext- und Faktendatenbanken zu nutzen, die von der ReDi zur Verfügung gestellt wurden. Um diese organisationsübergreifende Dienstnutzung zu ermöglichen, müssen identitätsbezogene Informationen, wie ein Authentifikationsstatus, zwischen den beteiligten Diensten ausgetauscht werden, was durch ein so genanntes föderatives Identitätsmanagement (FIM) ermöglicht wird.

Hierbei ist zu beachten, dass die Weitergabe identitätsbezogener Informationen über Organisationsgrenzen hinaus einer strengen Prüfung des Datenschutzes unterliegen muss. Aktuelle FIM-Technologien führen diesen Informationsaustausch während der Dienstnutzung durch, was eine verteilte Speicherung identitätsbezogener Daten nicht zwingend notwendig macht. Jedoch ist diese „on-the-fly"-Informationsbereitstellung nicht in jedem Fall einsetzbar; es gibt sowohl organisatorische als auch technische Gründe, die eine Replikation identitätsbezogener Informationen motivieren. Beispielsweise stärkt die Informationsreplikation die Autonomie eines Systems auf der organisatorischen Ebene, genauso wie die Fehlertoleranz auf der technischen Ebene. Darüber hinaus machen es Legacy-Systeme oftmals notwendig, dass Identitätsinformationen lokal vorgehalten werden, da diese Systeme typischerweise nicht dazu konzipiert sind, mit externen Datenspeichern zu kommunizieren. Da sich identitätsbezogene Daten jedoch mit der Zeit ändern können, besteht die Gefahr, dass Replikate voneinander differieren. Resultierende Inkonsistenzen in identitätsbezogenen Informationen können zu einer unautorisierten und inkorrekten Dienstnutzung führen. Folglich können Inkonsistenzen sowohl dazu führen, dass Benutzer einen Dienst in Anspruch nehmen können, ohne hierzu berechtigt zu sein, ebenso kann ihnen ein Dienstzugriff verweigert werden, obwohl sie die Berechtigung zur Dienstnutzung besitzen. Demnach gilt es der Herausforderung zu begegnen, Inkonsistenzen in Identitätsinformationen in verteilten Systemen zu vermeiden.

Informationskonsistenz in verteilten Systemen kann nur dann erreicht werden, wenn sichergestellt ist, dass sobald Informationen sich ändern, alle Replikate ebenfalls aktualisiert werden. Hierzu ist es notwendig, die betroffenen Systeme in einem angemessenen Maße zu integrieren. Es müssen also die Herausforderungen bezüglich der Integration heterogener Systeme in verteilten Umgebungen gemeistert werden, so zum Beispiel die Überwindung eventuell differierender Informationsschemata. Hierbei sollte jedoch stets auch die Effizienz Berücksichtigung finden, d.h. die Systeme sollten mit einem möglichst geringen Aufwand integriert werden. Dies gilt sowohl für den initialen Aufwand, um neue Systeme zu integrieren, als auch für den Betriebsaufwand der Integrationslösung. Beispielsweise sollten während des Betriebs des Gesamtsystems die beteiligten Systeme nicht von der Erreichbarkeit anderer Systeme abhängig sein oder Änderungen an einem System sollten sich nicht maßgeblich auf die restlichen Systeme auswirken.

Analyse bestehender Technologien und Standards

Das föderative Identitätsmanagement bzw. die diesem Bereich zugesprochenen Standards und Technologien, wurde für den organisationsübergreifenden Austausch identitätsbezogener Informationen in verteilten Systemen konzipiert. Daher ist es naheliegend, für die Wahrung der Informationskonsistenz in verteilten Systemen, bestehende Standards und Technologien zu analysieren, nicht zuletzt, um zu ermitteln, ob existierende Bausteine wieder verwendet werden können. Eine Analyse der relevantesten FIM-Standards und -Technologien, so eines der wichtigsten Standards im Bereich der Kommunikation identitätsbezogener Informationen, der Security Assertion Markup Language, und der zwei am weitestet verbreiteten SSO-Softwares, Shibboleth und OpenID, hat ergeben, dass einige Konzepte existierender Standards als Basis für eine angemessene Integrationslösung eingesetzt werden können, eine „Komplettlösung" jedoch derzeit nicht zur Verfügung steht. Neben den Ergebnissen der Analyse kann auf Erfahrungen bei der Konzeption und Realisierung eines KIT-weiten Identitätsmanagements zurückgegriffen werden [2], [3]. Insbesondere auf die Erfahrungen mit Werkzeugen, die eingesetzt werden, um innerhalb des KIT Informationskonsistenz zu gewährleisten, auch wenn hierbei berücksichtigt werden muss, dass eine Integrationslösung in einem organisationsübergreifenden Szenario beteiligte Systeme weniger stark koppeln sollte als in einem organisationsinternen Szenario.

Middleware für die Sicherstellung der Konsistenz in verteilten Systemen

Ziel der Forschung ist es somit, existierende „Puzzleteile“ zu einem Gesamtsystem zusammenzuführen und hierdurch die Konsistenz identitätsbezogener Informationen in verteilten Systemen sicherstellen zu können. Um die Lösung in organisationsübergreifenden Szenarien einsetzbar zu machen, galt es hierbei die beteiligten Systeme zu integrieren und gleichzeitig möglichst wenige Abhängigkeiten zwischen den Systemen zu erzeugen. Um dies zu erreichen, wird eine auf dem Publish/Subscribe-Paradigma basierte Middleware eingesetzt. Die Middleware stellt hierbei einen „Vermittler“ dar, der auftretende Änderungen zwischen den Systemen so verteilt, dass Heterogenität, beispielsweise unterschiedliche Informationsschemata, für die Systeme verborgen bleibt. Eine Reduktion der Abhängigkeiten wird durch das Publish/Subscribe-Paradigma erreicht, das es dem so genannten „Publisher“ erlaubt, Nachrichten an eine bestimmte Interessengruppe, den „Subscriber“, zu übermitteln, ohne die Subscriber direkt adressieren zu müssen. Durch diese Entkopplung der Systeme wird es möglich, dass der Aufwand während des Betriebs der Integrationslösung reduziert wird und somit die Erreichbarkeit oder auch Änderungen an integrierten Systemen keinen Einfluss auf andere Systeme nehmen. Des Weiteren hat eine prototypische Implementierung gezeigt, dass durch den Einsatz wiederverwendbarer Dienste, wie ein Dienst zur Korrelation der unterschiedlichen Identitäten eines Benutzers, der initiale Aufwand für die Integration neuer Systeme reduziert werden kann. Insgesamt konnte durch die Kombination bestehender Konzepte des föderativen und des organisationsinternen Identitätsmanagement eine Integrationslösung zur Sicherstellung der Konsistenz identitätsbezogener Informationen geschaffen werden, welche die zu integrierenden Systeme weitestgehend entkoppelt und somit ideal für den Einsatz in verteilten Systemen geeignet ist.

Thorsten Höllrigl

[1] T. Höllrigl, J. Dinger, H. Hartenstein: FedWare: Middleware Services to Cope with Information Consistency in Federated Identity Management, Proceedings of the Fifth International Conference on Availability, Reliability and Security (ARES 2010), Krakau, Polen, Februar 2010
[2] T. Höllrigl, S. Labitzke, F. Schell, J. Dinger, A. Maurer, H. Hartenstein: Identitätsmanagement am KIT – Kurzbeschreibung (Stand: August 2009), Technischer Bericht SCC-TB-2009-2, Steinbuch Centre for Computing (SCC), Karlsruhe Institute of Technology (KIT), August 2009
[3] T. Höllrigl, S. Labitzke, F. Schell, J. Dinger, A. Maurer, H. Hartenstein: KIM-Identitätsmanagement – Projektdokumentation, Technischer Bericht SCC-TB-2009-1, Steinbuch Centre for Computing (SCC), Karlsruhe Institute of Technology (KIT), August 2009

Schnell und stabil – der neue Hochleistungsrechner am SCC

Um den Wissenschaftlern am KIT eine optimale Rechnerversorgung - insbesondere im Bereich des High Performance Computing (HPC) anzubieten, wurde Mitte Februar am SCC der neue Hochleistungsrechner HP XC3000 (HC3) in Betrieb genommen. Dabei handelt es sich um ein Parallelrechnersystem der Firma Hewlett Packard mit fast 2.700 Rechenkernen und einer theoretischen Spitzenleistung von mehr als 27 TeraFlops pro Sekunde. Dies entspricht der Rechenleistung von ca. 1.000 modernen PCs. Der Hauptspeicher umfasst mehr als 10 TeraBytes – vergleichbar mit der Speicherkapazität von ca. 2.500 PCs.

Der Bereich des Hochleistungsrechnens ist für viele Institute des KIT schon lange von essentieller Bedeutung. Als klassische Anwendungen seien hier nur die numerische Strömungsmechanik und die Strukturmechanik genannt. Aber auch viele weitere Forschungsbereiche machen zunehmend von der numerischen Simulation Gebrauch, so dass der Bedarf an Hochleistungsrechnerkapazität am KIT stetig wächst.

Um diesem Bedarf gerecht zu werden, hat das SCC in den vergangenen Monaten einen neuen Hochleistungsrechner installiert, der nun bereits seit Mitte Februar den Wissenschaftlern des KIT zur Verfügung steht und auch schon sehr intensiv genutzt wird. Die HC3 läuft seit Betriebsbeginn sehr stabil und ohne technische Probleme. Mehr als 250 Wissenschaftler am KIT simulieren bereits auf der Maschine realitätsnahe technisch-wissenschaftliche Vorgänge. Dieser neue Rechner dokumentiert in gewisser Weise auch das Zusammenwachsen des KIT, da er gemeinsam mit Mitteln des Campus-Nord und -Süd beschafft wurde und somit von allen Wissenschaftlern des KIT in gleichem Maße genutzt werden kann.

Der neue Hochleistungsrechner ersetzt einerseits die inzwischen fünf Jahre alte, mit Intel Itanium-Prozessoren ausgestattete XC1, die bisher den Campus Süd versorgte und bereits seit Anfang April endgültig stillgelegt ist. Andererseits ist er Nachfolger für die HPC-Nutzung des OPUSIB-Clusters am Campus Nord. Nach der XC1 und dem Landeshöchstleistungsrechner XC2 ist dies der dritte Hochleistungscluster am Campus Süd, daher der Name HC3.

Kostenfreie Nutzung für alle KIT-Wissenschaftler

Die Nutzung der HC3 ist kostenfrei für die Wissenschaftler des KIT sowohl im Hinblick auf die Rechenzeit als auch auf den lokalen Speicher. Da es sich bei einem Hochleistungsrechner wie diesem um eine teure Spezialinvestition handelt, sollte gewährleistet sein, dass er auch sinnvoll genutzt wird, d.h. dass dort vorwiegend rechenintensive, parallele Anwendungen laufen. Der Zugang zur HC3 ist deshalb beim ServiceDesk des SCC zu beantragen. Das Formular hierfür kann von folgender Webseite heruntergeladen werden: http://www.scc.kit.edu/hotline/3268.php.

Wie die XC1 und XC2 stammt auch die HC3 von der Firma HP. Im Rahmen des Cloud Computing-Forschungsprojekts OpenCirrus™, an dem das SCC zusammen mit HP, Intel, Yahoo! und anderen internationalen Partnern beteiligt ist, wird die HC3 zu Teilen auch in diesem Projekt eingesetzt.

Neueste Technologie

Die neue Maschine ist Intel Xeon-basiert. Dabei wird neueste Technologie vom Feinsten eingesetzt. Die erst seit kurzer Zeit erhältlichen Intel Nehalem-Prozessoren mit vier Rechenkernen bieten im Vergleich zu deren Vorgängern eine enorme Steigerung der Speicherbandbreite und der Kommunikationsleistung zwischen den CPUs in einem Knoten. Mit einer Taktfrequenz von 2,53 Ghz wird ein guter Kompromiss zwischen Rechenleistung und Stromverbrauch erreicht.

Das Kommunikationsnetzwerk zwischen den Knoten der Anlage ist als Infiniband 4x QDR der Firma Voltaire realisiert. Diese Interconnect-Technologie besitzt die enorme Bandbreite von 40 Gbit pro Sekunde (jeweils Senden und Empfangen gleichzeitig) bei einer gleichzeitig sehr geringen Latenz von nur wenig mehr als einer Mikrosekunde.

Auch kommen neueste Server von HP zum Einsatz, die innerhalb eines Gehäuses von zwei Höheneinheiten jeweils vier unabhängige Server enthalten. Diese sind preislich günstiger als Blades, haben aber eine höhere Packungsdichte als klassische Rack Server.

Die Gesamtkonfiguration des neuen Clusters sieht wie folgt aus:

- 2 Login-Knoten mit jeweils 8 Cores mit einer theoretischen Spitzenleistung von 81,0 GFLOPS und 48 GB Hauptspeicher pro Knoten
- 288 Rechenknoten mit jeweils 8 Cores mit einer theoretischen Spitzenleistung von 81,0 GFLOPS und 24 GB Hauptspeicher pro Knoten
- 32 Rechenknoten mit jeweils 8 Cores mit einer theoretischen Spitzenleistung von 81,0 GFLOPS und 48 GB Hauptspeicher pro Knoten
- 12 Rechenknoten mit jeweils 8 Cores mit einer theoretischen Spitzenleistung von 81,0 GFLOPS und 144 GB Hauptspeicher pro Knoten und
- InfiniBand 4X QDR Interconnect mit ConnectX Dual Port QDR HCAs.

Die 12 'fetten' Knoten mit je 144 GB Hauptspeicher sind für sehr Hauptspeicher-intensive Shared-Memory-Anwendungen bestens geeignet (wie zum Beispiel für CAE-Anwendungen) und sind für diesen Zweck zusätzlich noch jeweils mit einer lokalen Plattenkapazität von ca. 0,5 TB in schneller RAID-Konfiguration ausgestattet. Insgesamt acht weitere Server sind für die Infrastruktur und das Management des Clusters vorhanden.

Für sehr schnelle File-I/O, insbesondere von parallelen Jobs, verfügt das System über ein lokales, paralleles Lustre-File-System von über 200 TB Kapazität und einem Durchsatz von bis zu 4,5 GB/s. Dieses File-System auf Basis von DDN-Technologie dient für temporäre und sehr große Scratch-Daten.

Die permanent verfügbaren HOME-Verzeichnisse der Nutzer liegen in dem schon vor zwei Jahren aufgebauten parallelen Lustre-File-System, an das auch der Institutscluster IC1 angeschlossen ist. Erwähnenswert ist in diesem Zusammenhang die wohl weltweit einmalige Konfiguration des Infiniband-Netzwerks. Es ist den Mitarbeitern des SCC gelungen, die Inifiniband-Infrastrukturen des Institutsclusters IC1, des globalen parallelen File-Systems PFS, des neuen Clusters HC3 und dessen lokales File-System von DDN in einer gemeinsamen Infiniband-Fabric zu integrieren. Trotz der Tatsache, dass dabei Komponenten unterschiedlichster Hersteller in einer Fabric zusammengeschlossen sind (HP, Transtec, DDN, Voltaire, Mellanox, Flextronics), arbeitet diese Konfiguration sehr zuverlässig und ermöglicht eine gemeinsame Nutzung des HOME-Verzeichnisses für die Anwender von verschiedenen Clustern aus.

Software

Auf der HC3 stehen die unterschiedlichsten CAE-Softwarepakete (CAE steht für Computer Aided Engineering) aus den Bereichen Strukturmechanik und Strömungsdynamik zur Verfügung. Namentlich sind das im Bereich Strukturmechanik die CAE-Pakete ABAQUS, MD Nastran, Permas und LS-Dyna; aus dem Bereich Strömungsmechanik die CAE-Pakete Fluent, ANSYS CFX, Star-CD und Star CCM+.

Weitere installierte Programmpakete sind COMSOL Multiphysics sowie Matlab und aus den Bereichen Pre- und Post-Processing bzw. Visualisierung die Programmpakete EnSight, Gambit, HyperWorks und ICEM CFD. Es stehen auch verschiedene Unterprogrammbibliotheken wie die MKL (Math Kernel Library) von Intel, CPLEX zur Lösung von Optimierungsproblemen und LINSOL zur Lösung von linearen Gleichungen bereit.

Zum Übersetzen und Linken eigener Programmpakete stehen Compiler von Intel, PGI, Sun und GNU für die Programmiersprachen C/C++, Fortran95 (Fortran 2003) und Java zur Verfügung. Hinzu kommen Werkzeuge zum Debuggen und zur grafischen Analyse eigener Programme.

Prof. Dr. Rudolf Lohner, Hartmut Häfner

Weitere Informationen
http://www.scc.kit.edu/dienste/hc3.php

Mehr als 250 Wissenschaftler nutzen bereits den neuen KIT-Hochleistungsrechner für numerische Simulationen.
Foto: Rolf Mayer

Das SCC stellt sich vor

In dieser Ausgabe: Die Abteilung Netze und Telekommunikation (NET)

Foto: Privat

Reinhard Strebler ist Leiter der Abteilung Netze und Telekommunikation (NET). Er studierte Elektrotechnik an der Universität Karlsruhe und nahm 1978 seine Tätigkeit als Wissenschaftlicher Mitarbeiter am ehemaligen Rechenzentrum der Universität Karlsruhe in der Abteilung für Analog- und Hybridrechnen auf. Im Jahr 1987 übernahm er die Leitung der Abteilung Technik und war hier für die Campus- und Gebäudevernetzung zuständig. Ab 1998 leitete er die Abteilung Netze und Kommunikation. Mit der Gründung des SCC übernahm er die Leitung der neuen Abteilung Netze und Telekommunikation.

Foto: Privat

Bruno Hoeft ist stellvertretender Leiter der Abteilung NET. Er studierte Informatik an der FH Darmstadt und begann 1989 als Ingenieur am ehemaligen Kernforschungszentrum Karlsruhe am Institut für Datenverarbeitung in der Technik (IDT), später Institut für Angewandte Informatik (IAI), zu arbeiten. Von 1994 bis 2002 war er für diakonische/soziale Zwecke beurlaubt und unterstützte die Verwaltung einer medizinischen Hilfsorganisation in Nepal beim Aufbau ihrer IT-Infrastruktur. Anschließend unterrichtete er an der Yanbian University of Science and Technology Yanji in Nordost-China. Nach seiner Rückkehr im August 2002 übernahm er im damaligen Institut für Wissenschaftliches Rechnen (IWR) den Aufbau der Netzwerkinfrastruktur des Projektes GridKa. Mit der Gründung des SCC übernahm er die stellvertretende Leitung der neuen Abteilung für Netze und Telekommunikation.

Die Abteilung Netze und Telekommunikation (von links nach rechts): Bruno Hoeft, Reinhard Strebler, Rainer Steinmüller, Elena Huck, Thomas Geldmacher, Aurélie Reymund, Manfred Altinger, Andreas Bullinger, Helmut Inhoff, Walter Schneider, Julia Rohlfing, Klara Mall, Wilhelm Fries, Norbert Lehmann, Daniel Thomé, Tim Subbert, Jürgen Deutschmeyer. Nicht im Bild: Petra Spanger, Dieter Gottschalk, Gerd Halbeis.
Foto: Mirko Hoffmann

Der Zugang zum Netz ist heutzutage eine der wichtigsten Eintrittskarten zu Information und Kommunikation. Eine stabile, funktionale und komfortable Netzinfrastruktur bildet die Basis für effektives Arbeiten von Wissenschaftlern, Mitarbeitern, Studierenden, externen und internen Nutzern. Die Abteilung NET unter der Leitung von Reinhard Strebler versorgt das gesamte KIT mit IP-Konnektivität, betreibt die komplette Netzinfrastruktur mit aktiven Komponenten wie Routern und Switches, aber auch die passiven Komponenten der Kupfer- und Glasfaserinfrastruktur. Neben dem Festnetz betreibt NET auch das Wireless Netzwerk des KIT und bietet den Benutzern einen hohen Grad an Mobilität. Für den Zugriff aus dem Internet oder von zu Hause über DSL werden passende Remote Access Lösungen angeboten.

Darüber hinaus werden zahlreiche netznahe Dienste wie DNS, NTP, DHCP, RADIUS etc. bereitgestellt. Einen weiteren Schwerpunkt der Abteilung bilden Telekommunikationsdienste. NET entwickelt eine multicasting- und streamingfähige Netzinfrastruktur, etabliert integrierte Mehrwertdienste zur zukünftigen Integration von Sprach- und Datendiensten und stellt einen Class-of-Service im Netz bereit. Damit wird Verkehr in Abhängigkeit von Anwendungen im Hinblick auf Background, Best Effort, Video, Voice und Management priorisiert. Der Rund-um-die-Uhr-Betrieb der Abteilung sorgt 24 Stunden an 7 Tagen in der Woche für die technische Redundanz und Bereitschaft.

Die Abteilung NET hat von Anfang an bewusst auf eine Gruppenbildung verzichtet, um die Kommunikation zwischen den Personen flach und effizient zu gestalten. Stattdessen war der gemeinsame Konsens, Funktionsgruppen in Form von Dienste-Teams zu bilden. Dabei wird durch regelmäßige Campus-Nord/Campus-Süd-Rotationen der Mitarbeiter gewährleistet, dass sie sich sowohl auf dem Campus-Süd als auch -Nord zurechtfinden. Die Mitarbeiter von CN und CS arbeiten also eng im Team zusammen.

Für einen reibungslosen Betrieb des Kernnetzes rund um die Uhr betreibt NET eigene Überwachungssysteme, um sofort über Ausfälle und Störungen in den Netzbereichen bzw. den bereitgestellten Diensten alarmiert zu werden. Außerhalb der regulären Arbeitszeit leistet NET eine Rufbereitschaft für das Kernnetz.

Insgesamt betreibt NET 27 Router, ca. 1450 Switches mit über 47.000 Interfaces in über 500 Datenverteilern, 8 zentrale VPN-Konzentratoren, verteilte zentrale Nameserver (DNS) und eine Vielzahl weiterer Server für dedizierte Aufgaben wie DHCP, RADIUS und Netzwerkmanagement.

Betriebsteam

Die Mitarbeiterinnen und Mitarbeiter des Betriebsteams haben die Aufgabe, für den reibungslosen Ablauf des Datenverkehrs innerhalb des KIT (Intranet) und zum Internet zu sorgen. Zum Aufgabenumfang zählen das gesamte Life Cycle Management der aktiven Netzkomponenten, d.h. Beschaffung, Konfiguration, Einbau, Wartung, Upgrade und Ausbau/Entsorgung. Ebenso wichtig ist die Aktivierung von Datenanschlussdosen und die technische Unterstützung der Netzwerkadministration. Weitere Säulen sind die permanente Pflege der Management- und Sicherheitssysteme.

Darüber hinaus bieten die Mitarbeiter den Instituten kompetente und qualifizierte Beratung über moderne Netzwerkstrukturen sowie -erneuerungen und versuchen flexibel auf die jeweiligen Kundenbedürfnisse einzugehen. Neben einer Vielzahl von Standardlösungen werden auch individuelle Wünsche der Kunden erfüllt mit dem Ziel, eine hohe Verfügbarkeit und Leistungsfähigkeit der Netzinfrastruktur zu gewährleisten.

Der Teil des Betriebsteams, der am Campus Nord seinen Hauptarbeitsplatz hat, löste die Fremdfirma „Telematis“ Ende September 2009 vollständig ab. Die bis zu diesem Zeitpunkt von der Firma erbrachten Leistungen sind jetzt zusätzlich am SCC angesiedelt.

Netzausbau-Team

Die Abteilung Netze und Telekommunikation ist Betreiber der kompletten, offiziellen Datennetzinfrastruktur (KITnet) mit seinen aktiven Komponenten (Router, Switches) und den passiven Komponenten (Kupfer- und Glasfaserverkabelungsanlage). Veränderungen an der Verkabelungsanlage innerhalb der Gebäude (Institute/Organisationseinheiten) sind nur in direkter Absprache mit dem Betreiber des Datennetzes möglich.

Bauunterhaltung des Datennetzes

Auch eine vorhandene Verkabelungsanlage des Datennetzes innerhalb eines Gebäudes unterliegt ständig wachsenden Anforderungen. Oft reicht die Anzahl der installierten Datenanschlüsse nicht mehr aus, und eine Nachverkabelung von zusätzlichen Datenanschlüssen wird notwendig. Oder der vorhandene Datenverteiler ist zu klein geworden und muss erneuert werden, damit er die neue Technik aufnehmen kann.

An anderer Stelle ist eine Migration der Übertragungsgeschwindigkeit angeraten, weil das Datenaufkommen durch neue Anwendungen oder Projekte rasant wächst. Hier wird eine Überprüfung der passiven Infrastruktur sowie der Aktivkomponenten auf Tauglichkeit im Zusammenhang mit den neuen Anforderungen die Entscheidungshilfe für die notwendigen Investitionen liefern. Ein Redesign von aktiven Netzwerkkomponenten (Switches) steht spätestens dann an, wenn die vorhandenen Aktivkomponenten technisch veraltet sind, die Abkündigung vom Hersteller schon viele Jahre zurück liegt oder die Störanfälligkeit der Aktivkomponenten zunimmt.

Wenn Sie als Verantwortlicher eines Institutes die oben beschriebenen Maßnahmen in ihrem Bereich beabsichtigen, wenden Sie sich bitte vorab am Campus Nord an die Herren Halbeis (Tel. -5259) oder Deutschmeyer (Tel. -5249), am Campus Süd an die Herren Altinger (Tel. -7385) oder Geldmacher (Tel. -6438). Sie erfahren dort kompetente Unterstützung von der Planung über die Realisierung bis zur Freigabe. Auf Grund der unterschiedlichen Finanzierung an den Standorten des KIT gelten hier abweichende Regeln zur Kostenbeteiligung.

Komplettverkabelung/-sanierung von Gebäuden

Bei größeren Baumaßnahmen, die eine festgelegte Wertgrenze überschreiten, schreibt die Vergabeordnung des KIT eine andere Vorgehensweise vor. In diesen Fällen ist eine Ausschreibung der Datennetzarbeiten notwendig. Am Campus Nord ist das SCC in der Lage, alle Leistungsphasen der Honorarordnung für Architekten und Ingenieure (HOAI) selbst zu erbringen. Diese reicht von der Kostenberechnung über die Erstellung einer Ausschreibungsunterlage bis hin zur Bauüberwachung und schließt die Abrechnung und Erstellung der Dokumentation mit ein. Am Campus Süd werden derartige Leistungen stellvertretend vom Staatlichen Vermögens- und Bauamt, Abteilung Universitätsbau, erbracht.

GridKa

Das Grid Computing Centre Karlsruhe (GridKa), deutsches Tier1- Zentrum, stellt für den am Europäischen Forschungszentrum CERN betriebenen Large Hadron Collider (LHC) Compute- und Storage-Ressourcen zur Verfügung. Dafür wurde ein redundant ausgelegtes und weitgehend blockungsfreies Netzwerk installiert. Die internationalen Verbindungen stehen im LHCOPN zur Verfügung. Das maßgeblich durch die Mitarbeiter von NET geprägte LHCOPN (LHC Optical Private Network) ist ein sternförmiges, breitbandiges (10Gbps) Netzwerk mit der Datenquelle CERN (Tier0) als Zentrum und teilweisen Vermaschungen der Tier1-Zentren. Die GridKa betreffenden Vermaschungen sind in Kooperation mit dem DFN über sogenannte CrossBorderFiber-Verbindungen zu drei europäischen Tier1-Zentren (FR-IN2P3, IT-INFN-CNAF, NL-T1) aufgebaut. Darüber hinaus sind direkte Verbindungen zu den Tier2-Zentren Desy (10Gbps), FZU (Tschechien/Prag) (1Gbps) sowie zu den drei polnischen Zentren Warschau, Poznan und Krakau (1Gbps) hergestellt (s. Abbildung 1). Das Routing innerhalb der Tier 1-Zentren wurde mit BGP (Border Gateway Protocol) realisiert, daher ist es möglich, sehr schnell und dynamisch auf Veränderungen zum Beispiel beim Ausfall einer Verbindung eines Tier1-Zentrums zum CERN zu reagieren.

Die interne Netzwerkinfrastruktur für GridKa ist ebenso breitbandig und dynamisch aufgebaut. Sechs Backbone Router nehmen die Daten von den zwei redundant aufgebauten Border Routern entgegen und verteilen sie auf die Endgeräte. Die Backbone Router sind als eigenständige Inseln konzipiert, die über die Routingprotokolle OSPF (Open Shortest Path First) und das Redundanzprotokoll VRRP (Virtual Router Redundancy Protocol) eine redundante und weitgehend blockungsfreie Backbone-Infrastruktur für GridKa bereitstellen. Die Worker Nodes sowie die File Server sind logisch über VLAN-Strukturen eingebunden.

Dante (europaweiter Interconnect der Wissenschaftsnetze) betreibt für LHCOPN ein Perfsonar-Monitoringsystem, das zusätzlich zur Überwachung durch die NET-Systeme die ständige Erreichbarkeit aller Tier1- Zentren untereinander über die LHCOPN-Infrastruktur überwacht.

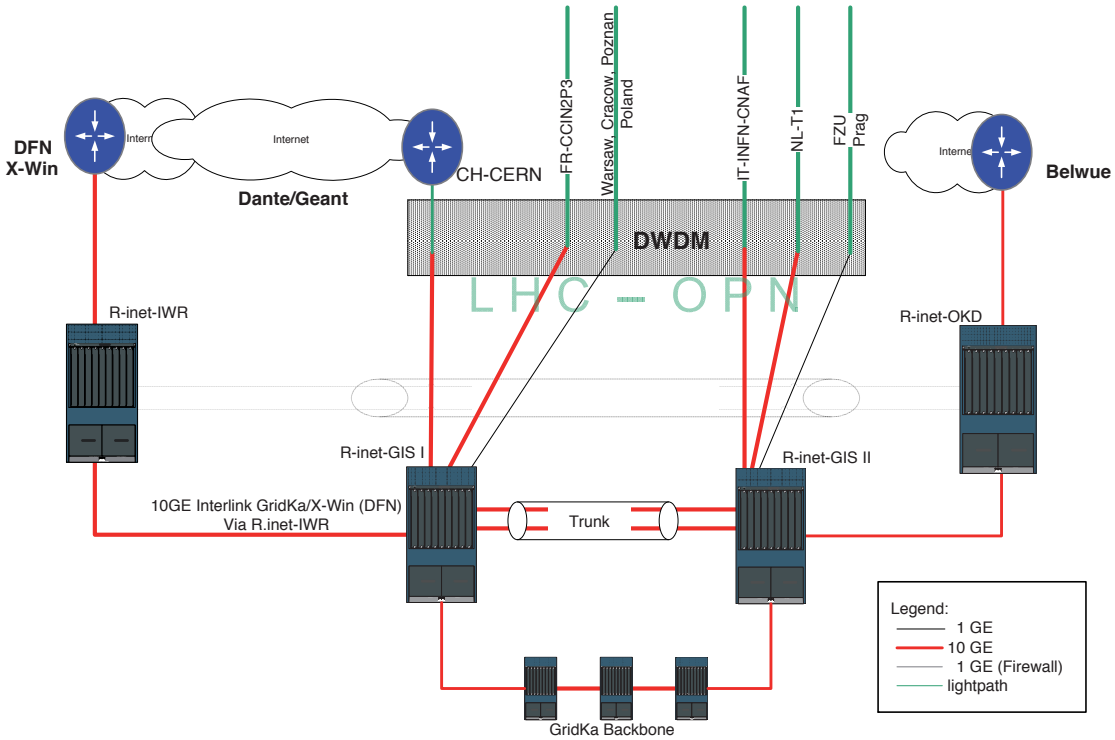


Abbildung 1: LHC-OPN am KIT.

Zentrale Netzwerk-Dienste

Aufbauend auf der Netz-Infrastruktur (KIT-Backbone mit zentralen Komponenten und Netz-Anbindung aller Gebäude) bietet NET zentrale Netzwerk-Dienste an, die es dem Benutzer ermöglichen, seine Endgeräte effektiv ans Netz anzuschließen und die Angebote im Intranet und Internet zu nutzen.

Zu den zentralen Netzwerk-Diensten, ohne die eine Kommunikation der Endgeräte im Netz nicht möglich ist, zählen:

- die Verwaltung von IP-Adressen
- die Netzwerk-Konfiguration für Endgeräte (manuell oder dynamisch)
- der Namens-Dienst (DNS)

IP-Adressverwaltung

Jedes Endgerät am Netz benötigt eine eindeutige Adresse, die IP-Adresse. Diese Adressen sind in Subnetzen gegliedert, ein Subnetz vereinigt dabei alle Endgeräte einer OE (Organisationseinheit) eines Gebäudes oder eines Anwendungsbereiches. Alle Subnetze sind an die zentralen Backbone-Router angebunden, somit ist die Kommunikation im gesamten KITnet oder ins Internet möglich.

Die Verwaltung von Subnetzen und IP-Adressen realisiert NET über zentrale Datenbanken. Die bisherigen Datenbestände am CS und CN sind miteinander gekoppelt.

Netzwerk-Konfiguration für Endgeräte

Jedes Endgerät benötigt neben der IP-Adresse weitere Konfigurations-Parameter, damit die Kommunikation im Netz funktioniert (Hostname, Namens-Domäne, Subnetzmaske, Standard-Gateway). Diese Parameter müssen manuell auf dem Endgerät eingetragen werden, wenn dieses eine statische IP-Adresse zugeteilt bekommt. Sie können aber auch automatisch vergeben und eingetragen werden, wenn das Endgerät beim Netzzugang den DHCP-Dienst (Dynamic Host Configuration Protocol) nutzt.

NET bietet einen zentralen DHCP-Dienst an. Im KITnet sind inzwischen mehr als 10.000 Endgeräte über diesen Dienst ans Netz angeschlossen. DHCP bietet gegenüber dem manuellen Verfahren vielerlei Vorteile, weniger Verwaltungsaufwand, weniger Fehlermöglichkeiten und eine bessere Ausnutzung der vorhandenen IP-Adressbereiche (Budgetierungsproblematik am CN). Selbstverständlich sind im DHCP-Betrieb auch verschiedene Zugangskontrollen möglich.

Namensdienst (DNS, Domain Name System)

Wie bei einer Telefonauskunft bietet dieser Dienst die Zuordnung von Namen (Hostnamen, Servernamen, Mail-Adressen, Web-Adressen) zu IP-Adressen. Die Kommunikation zwischen Clients (Endbenutzer) und Servern (zum Beispiel Web-Server) basiert im Netz immer auf IP-Adressen. Für den Menschen sind aber naturgemäß Namen leichter zu behalten und einzugeben als IP-Adressen.

DNS ist ein weltweit hierarchisch aufgebauter Verzeichnis-Dienst für den Namensraum des Internets. Dieser Namensraum ist in Domänen unterteilt. Die zentralen DNS Server von NET sind in diese Hierarchie eingebunden und übernehmen u.a. die Namensauflösung für die KIT-Domäne kit.edu, die CS-Domäne uni-karlsruhe.de oder die CN-Domäne fzk.de. Außer diesen Haupt-Domänen sind die Name Server zuständig für zurzeit ca. 200 DNS-Domänen; weitere Unter-Domänen sind an KIT-Einrichtungen delegiert.

In Anlehnung an die Trennung Internet/Intranet gibt es eine Trennung zwischen internem und externem DNS-Dienst. Der externe DNS-Dienst beantwortet Anfragen aus dem Internet, der interne DNS-Dienst steht allen Clients im KIT-Intranet zur Verfügung. Im internen DNS-Dienst gibt es derzeit ca. 75.000 Einträge für Hostnamen, die auf IP-Adressen zeigen, und ca. 50.000 Einträge für das Mail-Routing (Zustellung von E-Mails). Der DNS-Dienst wird intern durch vier auf die beiden Campus verteilten DNS Server bereitgestellt. Für den externen DNS-Dienst stehen zwei Server zur Verfügung.

Die Einträge für den DNS-Dienst werden entweder manuell über ein Web-Interface oder automatisch über die Verknüpfung der IP-Datenbank mit dem DNS-Dienst durchgeführt. So werden die Hostnamen aller Endgeräte, die per DHCP ans Netz gehen, vom DHCP-Server automatisch in die IP-Datenbank eingetragen und von dort unmittelbar auf die internen DNS Server verteilt. Änderungen (beispielsweise der Rechnername wird geändert oder ein Laptop geht in einem anderen Subnetz ans Netz) werden also unmittelbar an den DNS-Dienst weitergegeben. Dieses Verfahren wird auch als dynamisches DNS bezeichnet. Dynamisches DNS ist auch eine stringente Empfehlung für den Betrieb von Active-Directory-Domänen.

Dienst Netzsicherheitssysteme

Zum Schutz vor unerlaubten Zugriffen auf Ressourcen im Datennetz des KIT betreibt NET Netzsicherheitssysteme („Firewalls“). Mit diesen Systemen wird die Kommunikation ganzer Netzsegmente mit anderen Netzen (Campusnetz, Internet) über diverse Regeln gesteuert. Hierbei gibt es je nach Sicherheitsbedarf unterschiedliche Sicherheitsstufen, die in einer Art Baukastensystem vom SCC angeboten werden.

Die Netzsicherheit ist historisch bedingt am Campus-Nord und -Süd noch unterschiedlich implementiert. Ziel von NET ist eine Vereinheitlichung, an der bereits gearbeitet wird.

Campus Nord

Als Netzsicherheitssysteme werden eine so genannte „Zentrale Firewall“ und dezentrale Firewalls betrieben. In beiden Fällen kommen spezielle Firewall-Module in den Routern

zum Einsatz. Diese Module sind redundant ausgelegt, wobei zu jedem Zeitpunkt stets nur ein Gerät aktiv ist (hot/standby-Redundanz). Jede Konfigurationsänderung wird jedoch automatisch auf beiden Geräten durchgeführt, und im Falle einer Störung übernimmt das zweite Modul unterbrechungsfrei den Dienst.

Zentrale Firewall
Die zentrale Firewall regelt die Verbindung zwischen dem Netzwerk des Campus Nord und dem Internet. Die Firewall wirkt dabei in beide Richtungen: Sie begrenzt die Möglichkeiten von Rechnern im Internet, auf Ressourcen im Campus-Nord zuzugreifen. Sie schränkt den Zugang interner Rechner zu Diensten im Internet ein. Die Firewall wird „zentral" genannt, weil sie für alle am Intranet angeschlossenen Geräte wirkt. In begründeten Einzelfällen können in der Firewall Freischaltungen eingerichtet werden, um ausgesuchte Rechner für spezielle Dienste erreichbar zu machen. Der direkte Zugriff auf das WWW oder auf externe FTP-Server über die Firewall ist gesperrt. Hierzu müssen der WWW-Proxy bzw. FTP-Proxy verwendet werden.

Dezentrale Firewall
Organisationseinheiten mit erhöhtem Sicherheitsbedarf können zusätzlich den Dienst „Dezentrale Firewall" nutzen. Eine dezentrale Firewall reglementiert die Kommunikation zwischen dem Netzsegment eines Instituts/einer OE und dem übrigen KITnet.

Anträge für Änderungen in der zentralen oder dezentralen Firewall können vom zuständigen LAN-Koordinator per E-Mail an firewall@iwr.fzk.de gestellt werden.

Campus Süd

Als Grundschutz sind auf den Router-Systemen Standard-Sicherheitseinstellungen aktiv, die in Abhängigkeit einer Klassifizierung konfiguriert werden:

· Internet Uplink
· Benutzernetze
· Servernetze am SCC

Am Internet Uplink ist eine White List konfiguriert, die nur die global geforderten Protokolle in Richtung des KITnet durchlässt. Es gibt hier eine Vielzahl von spezifischen Freischaltungen, die nach schriftlichem Antrag und Gutbefund konfiguriert werden. Diese Freischaltungen werden in zeitlichen Abständen revalidiert. Inbound- und Outbound sind Antispoofing-Regeln nach RFC 2827 implementiert. An den Router Interfaces der Benutzernetze sind Standardregeln konfiguriert, die Netzwerkmanagementprotokolle aus den Benutzernetzen ausfiltern. Außerdem ist grundsätzlich Antispoofing konfiguriert. An den Router-Interfaces der Servernetze sind dienstspezifische Filterlisten eingetragen.

Sicherheitsstufe 0
Die Stufe 0 sieht öffentliche IP-Adressen vor. Die Sicherheitsregeln leiten sich aus den Grundschutzregeln ab.

Sicherheitsstufe 1
Ziel der Stufe 1 ist die Abschottung von Systemen gegenüber dem Internet. Als Grundsatz gilt: Auf von innen initiierte Verbindungen darf von außen geantwortet werden. Ein Verbindungsaufbau von außen ist nicht möglich. Hier finden private IP-Adressen nach RFC 1918 Verwendung. Da private Adressen nur innerhalb einer Einrichtung Gültigkeit haben, ist für die Kommunikation dieser Systeme mit dem Internet der Einsatz von Application Gateways oder einer Adressumsetzung erforderlich. Im Bereich der Application Gateways wird dies durch SCC-Web-Proxies und Mail-Server realisiert. Für alle anderen Protokolle und Anwendungen findet im Bereich des Internet Uplinks eine Adressumsetzung (PAT/NAT, Port/Network Address Translation) statt. Dieser Dienst wird zentralisiert durch den Einsatz eines Firewall-Moduls im Router realisiert. Die Administration erfolgt über NATVS, eine Eigenentwicklung des SCC. NATVS verfügt über ein User Interface, das den IT-Beauftragten der Einrichtungen eine selbständige Verwaltung ihrer Freischaltungen bietet. Über NATVS erfolgt automatisiert ein Download der konfigurierten Freischaltungen auf das NAT-System. Voraussetzung für den NATVS-Zugang ist die Registrierung als DNSVS-Betreuer.

Sicherheitsstufe 2
Stufe 2 entspricht im Ansatz der Implementierung von Stufe 1 mit dem Unterschied, dass hier Gruppen von Systemen innerhalb des Universitätsnetzes gegeneinander und gegen das Internet geschützt werden. Die zu schützende Gruppe von Systemen muss sich jeweils in einem eigenen VLAN befinden.

WLAN

Mit dem Begriff WLAN (Wireless Local Area Network) bezeichnet man ein lokales Netzwerk, das die Daten per Funk im Netzwerk über so genannte Access Points überträgt. Rechner (Notebook, PDA, mobile Phone, Desktop-PC), die auf das WLAN zugreifen, die so genannten Clients, sind dabei örtlich flexibel und können sich je nach Wahl des Netzwerknamens (die SSID) in unterschiedliche Umgebungen verbinden.

WLAN hat sich prinzipiell von einem zusätzlichen (nice to have) Netzwerk-Angebot zu einer grundlegenden und unverzichtbaren Dienstleistung gewandelt. Die rasche technische Entwicklung in diesem Bereich sowie die steigenden Übertragungsraten sorgten dafür, dass heute die meisten mobilen Clients WLAN-fähig sind. So überrascht es nicht, dass schon vor Jahren sowohl am Campus-Nord als auch -Süd eine Wireless-Infrastruktur entstanden ist.

Im Süden sind derzeit mehr als 400 Access Points installiert. Die meisten dieser mit IEEE 802.11 b/g Radio-Modulen ausgestatteten Access Points sind in Gebäuden und Hörsälen vorhanden. Über Dachantennen wird das WLAN weit über das Campusgelände abgestrahlt. Damit wird durchschnittlich mehr als 1.000 Benutzern pro Tag der Netzzugang ermöglicht. Die hohe Anzahl der gleichzeitigen Nutzer führte zur

Notwendigkeit einer Segmentierung der WLAN-Bereiche im Süden. Im Norden wurden von den einzelnen Instituten mehr als 100 Access Points (a,b,g Radio) angefordert und in den Gebäuden angebracht. Ein spezieller unverschlüsselter Zugang über die SSID *VPN/WEB* mit 14-tägig wechselnder Parole (Zugangspasswort) für Gäste wurde implementiert, um Besuchern den einfachen Zugang zum Internet zu ermöglichen. Mitarbeiter kommen mit der SSID *fzk-intra-1x* mittels 802.1x verschlüsselt ins Intranet.

Im Norden sind die SSIDs überall einheitlich (keine Segmentierung) und täglich wird die Infrastruktur von ca. 300 Mitarbeitern oder Gästen genutzt.

Trotz unterschiedlicher Ausgangslagen bei der Implementierung des WLAN versucht das WLAN-Team eine möglichst einheitliche Lösung für das KIT zu realisieren. Derzeit ist das Management der Access Points im Norden und Süden identisch. An einer einheitlichen Zugangsmöglichkeit für Mitarbeiter, Gäste und Studierende wird bereits gearbeitet. So wurden beispielsweise neue Server (Radius-Instanzen) zur Authentifizierung aufgesetzt, die für VPN und WLAN im Norden und Süden genutzt werden.

Zukünftig wird am gesamten KIT identische Hardware (802.11n Access Points) und eine redundante WLAN-Controller-Lösung eingesetzt. Dadurch wird eine noch leistungsfähigere gemeinsame Infrastruktur entstehen, die mit ca. 300Mbit /s auch hinsichtlich der Performance neue Maßstäbe setzen wird.

VPN

Um die gesicherten (verschlüsselten) Datenverbindungen (Tunnel) durch das Internet in das interne KITnet aufbauen zu können, bietet NET den KIT-weiten VPN-Dienst auf Basis des Produkts SA-6500 der Firma „Juniper Networks, Inc." an, der die alten Cisco-basierenden VPN-Lösungen ablösen wird. Der VPN-Dienst ist unter der URL https://vpn.kit.edu erreichbar.

Die Nutzung des VPN-Dienstes setzt die Installation einer Client-Software auf den Endgeräten voraus. Mit Hilfe dieser Software wird von dem Endgerät ein „virtuelles privates Netzwerk" (Virtual Private Network, VPN) zu einer Gegenstelle, dem VPN-Gateway im KITnet, aufgebaut. Über diese Verbindung, den so genannten Tunnel, wird der gesamte Verkehr verschlüsselt übertragen. Zudem erhält das Endgerät eine IP-Adresse aus dem KITnet.

Somit stehen Dienste zur Verfügung, die sonst nur KIT-intern genutzt werden können (Bibliothekrecherchen, Suche nach internen Telefonnummern, SAP, etc.).

Der Juniper-VPN-Dienst unterstützt alle gängigen Betriebssysteme und Internet Browser. Derzeit erfolgt die Authentifizierung über FZKA-AD-Accounts, RZ-Accounts und KIT-AD-Accounts.

Netzwerkmanagement

Das Netzwerkmanagement im KITnet basiert auf einer speziell für diese Zwecke aufgebauten Netzwerkinfrastruktur. Diese orientiert sich in den wesentlichen Punkten am ITU-T-Standard M.3200 (TMN, Telecommunication Management Network). Demnach erfolgt das Management der zentralen Komponenten des KITnet über eine dedizierte Netzwerkumgebung, damit die Administration der Netzkomponenten auch bei Störungen des Betriebsnetzes möglich bleibt. Für die verteilt auf dem Gelände des KIT

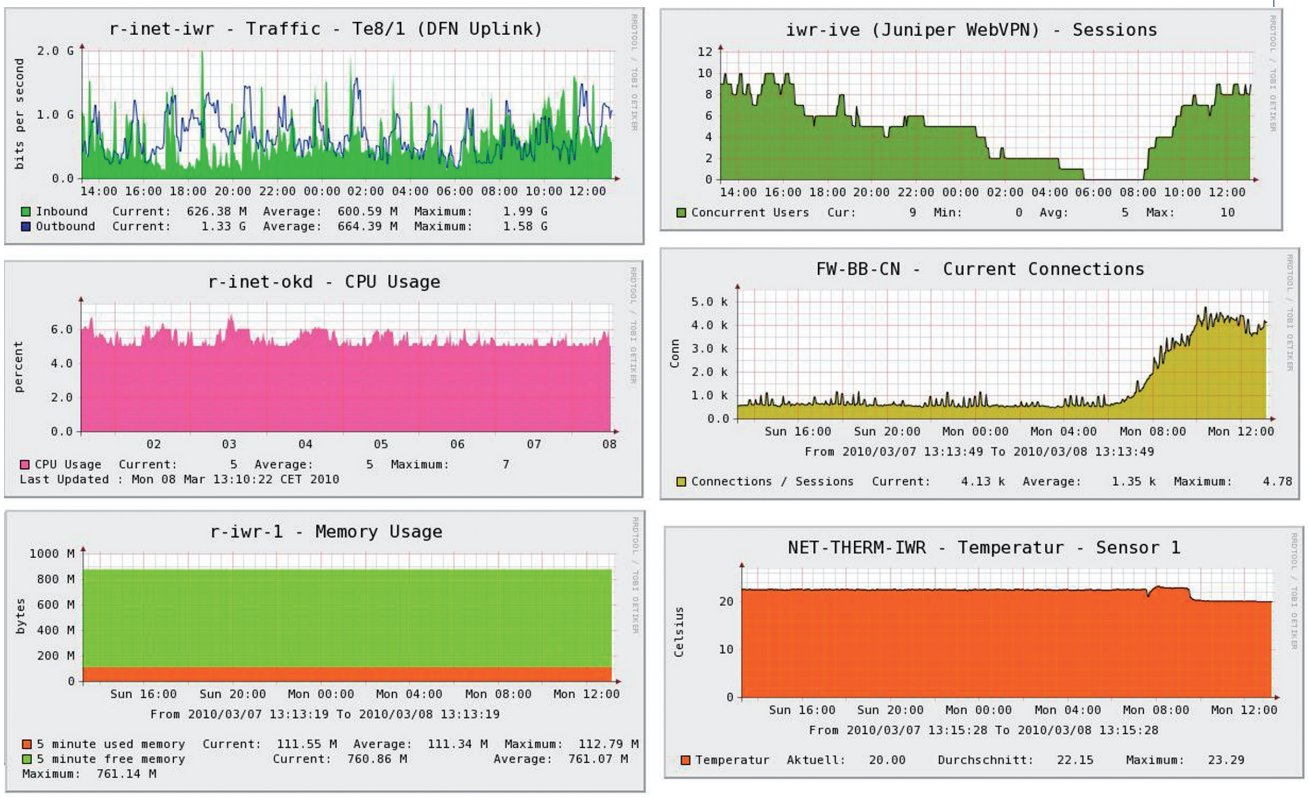


Abbildung 2: Auslastungsstatistiken.

installierten Netzkomponenten erfolgt die Administration logisch out-of-band, nutzt aber dieselben physikalischen Verbindungen wie das Produktionsnetz. Über dieses Managementnetz erfolgen neben der Administration der Komponenten auch die Überwachung der Komponenten sowie das Erfassen von statistischen Daten der Komponenten und all ihrer Interfaces.

Für die Überwachung des Netzes und der betriebenen Netzkomponenten werden eine Vielzahl von kommerziellen und selbst entwickelten Tools eingesetzt. Diese sind überwiegend eng gekoppelt, wobei einige Systeme auch noch separat administriert werden müssen. Hier steht die enge Anbindung an die Zentralsysteme mit hoher Priorität auf der Zeitachse.

LanKo

Die LanKo (Koordination für Vernetzungsfragen und Netzanträge der Hochschulen in Baden-Württemberg) ist seit 2003 dem SCC-Süd angegliedert und ist neben der BelWü-IP-Koordination und dem BelWü-SDH-Management eine weitere vom Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg (MWK) initiierte Einrichtung. Wird von einer Einrichtung eine HU-Geräte (Haushaltsunterlage Geräte) zur Beschaffung von aktiven Netzkomponenten gestellt, so wird diese von der LanKo überprüft und bei Unklarheiten Rücksprache mit der stellenden Einrichtung genommen. Eine abgeschlossene Überprüfung wird mit einer Stellungnahme, gegebenenfalls auch mit Empfehlungen und Auflagen, an das Ministerium für Wissenschaft, Forschung und Kunst weitergeleitet. Bei der HU-Geräte wird besonderes Augenmerk auf die technischen Aspekte gelegt. Vor Eingang eines HU-Geräte-Antrags ist ein Nachweis über die Verwendung der letzten Mittelzuweisung erforderlich.

Die LanKo informiert sich intensiv über aktuelle Netzwerktrends, unterhält diverse Kontakte zu einer Vielzahl von Herstellern und Vertriebsorganisationen und verfolgt die Arbeiten der Standardisierungsgremien.

SDH-Management in BelWü

Das SDH-Netz (SDH: Synchrone Digitale Hierarchie) besteht aus SDH-Knoten der Firma Marconi vom Typ MSH64 und SMA16 und wird vom SCC betreut. Die Backbone-Karten der SDH-Geräte sind direkt auf die DWDM-Transponder des BelWü-Netzes geschaltet. Die SDH-Knoten dienen dem Daten-Multiplexing und der Bereitstellung von QoS-Diensten.

Das SDH-Management in Karlsruhe verwaltet das SDH-Netz. Dabei fallen folgende Aufgaben an:

- Überwachung des SDH-Netzes
- Konfiguration der Komponenten
- Kontaktpflege mit den Firmen Tesion und Marconi
- Bereitstellung von SDH-Verbindungen für Projekte und Betrieb
- Verteilung von Wartungs- und Fehlermeldungen
- Ansprechpartner für die Rechenzentren der Universitäten in Baden-Württemberg
- Weiterentwicklung des SDH-Netzes

Quellen:
http://www.belwue.de/ueberuns/netz/sdh-betrieb.html
http://www.belwue.de/produkte/sonstdienste/sonstdienste-lanko.html

Reinhard Strebler, Bruno Hoeft

Neues Wireless LAN am KIT

Ab Juni 2010 beginnt das SCC mit dem Aufbau eines neuen KIT-weiten Wireless LAN (WLAN). Dabei kommt der neue WLAN-Standard 802.11n im 5 GHz-Bereich zum Einsatz.

Selbstverständlich werden aber auch die bisherigen WLAN-Standards 802.11a/b/g weiterhin unterstützt. Dies erfolgt durch so genannte Dual Radio Access Points, die auf einem Radio die Standards 802.11b/g im 2,4 GHz-Frequenzbereich ausstrahlen und auf dem zweiten Radio die 802.11a/n Standards im 5 GHz-Frequenzbereich zur Verfügung stellen. Ob der neue Standard genutzt werden kann, hängt von der Hardware im mobilen Gerät ab. Diese sollte die Verfügbarkeit des neuen Standards automatisch erkennen und anwenden.

Die Authentifizierungsmethoden bleiben unverändert, die Zugangs-Credentials (Benutzername/Passwort) werden aber vereinheitlicht und genau so geregelt wie beim neuen VPN-Zugang. Als Default-Zugang wird der KIT-Account gesetzt (Kürzel, Mail-Adresse oder Mail-Alias), bei den alten UNI-RZ- und FZK-Accounts muss wie beim EDUROAMing der Zusatz „@uni-karlsruhe.de“ bzw. „@fzk.de“ angehängt werden.

Auch die Webauthentifizierungsseite wird vereinheitlicht. Hier gelten ebenfalls die gleichen Zugangs-Credentials (s. Abbildung 1).

Bei dieser Gelegenheit werden auch die WLAN-Namen (SSIDs) der alten Access Points wie folgt vereinheitlicht:

wkit-/VPN/WEB/belwue**

(Ungesichertes Netzwerk entspricht der bisherigen SSID *VPN/WEB* am Campus Nord und den SSIDs *dukath-**, *belwue, VPN/WEB, INKA* am Campus Süd.)

Diese SSID verbindet Sie mit einem ungesicherten Netzwerk. Um Internet-Konnektivität zu erhalten, können Sie:

1. Einen VPN-Tunnel aufbauen (entweder zu dem KIT-Juniper-Konzentrator *vpn.kit.edu* oder zu einem anderen Konzentrator einer Hochschule, die am BELWÜ-Roaming teilnimmt. (s. http://www.belwue.de/produkte/sonstdienste/sonstdienste-roaming.html).

2. Ein Browserfenster öffnen und sich auf der automatisch erscheinenden Webseite mit Benutzerkennung und Passwort authentifizieren. Achtung, bei dieser Methode wird der Datenverkehr „durch die Luft“ nicht verschlüsselt und ist von dritten problemlos abhörbar (die Authentifizierung ist durch SSL verschlüsselt). Sie sollten daher nur sichere Protokolle wie https, ssh usw. nutzen.

Für ** bleiben die bisherigen Bereichskürzel (rz, ph, ch, ub, mv, usw.) erhalten. Das Kürzel „cn“ wird dabei für Campus Nord stehen.

eduroam

(802.1x und WPA-gesichertes Netzwerk, entspricht der bisherigen SSID *eduroam* am Campus Nord und den SSIDs *eduroam* und *802.1X* am Campus Süd.)

Diese SSID ist ausschließlich für unsere Gäste gedacht (s. http://www.dfn.de/dienstleistungen/dfnroaming/). Mitarbeiter und Studierende des KIT sollten diese SSID nicht benutzen. Nach erfolgter Authentifizierung werden die Besucher des KIT mit dem Gästenetz des KIT verbunden und haben von da aus einen vollständigen Zugriff auf das Internet. Der Zugriff auf KIT-Ressourcen unterliegt dabei den gleichen Bedingungen wie denen im Internet.

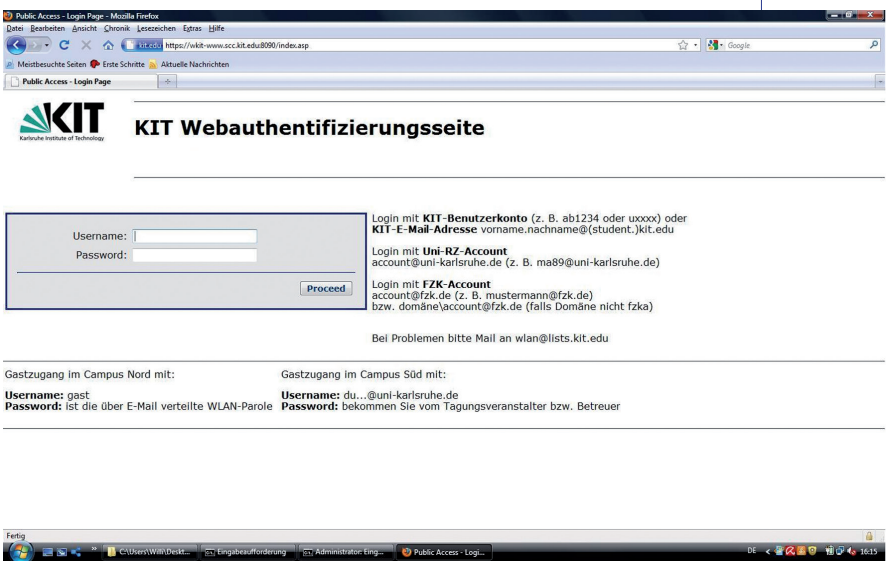


Abbildung 1: Webauthentifizierungsseite.

wkit-x**

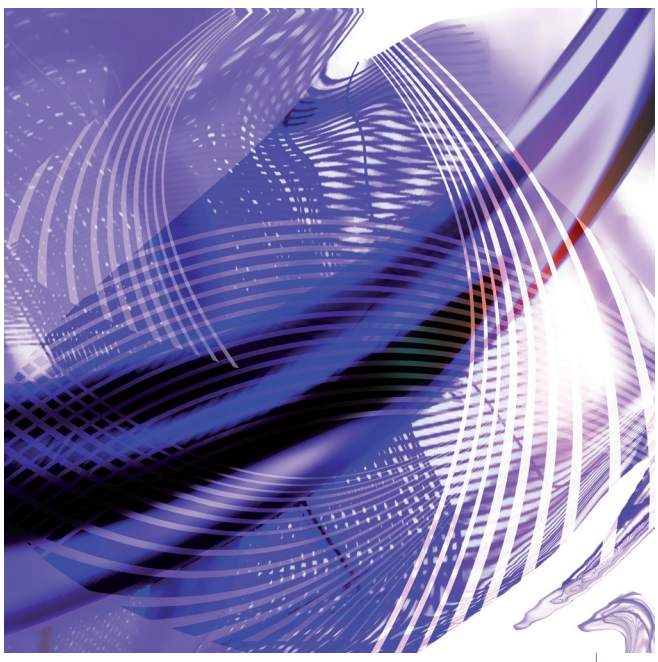
(802.1x und WPA-gesichertes Netzwerk, entspricht der bisherigen SSID *fzk-intra1x* am Campus Nord und den SSIDs *dukath-**x* am Campus Süd.)

Diese SSID ist für Angehörige (Mitarbeiter und Studierende) des KIT gedacht. Dafür ist ein KIT-Account, RZ-Account oder FZK-Account erforderlich (s.o.).

Klara Mall, Helmut Inhoff, Willi Fries

Präsidium verabschiedet Leitlinie zur IT-Sicherheit am KIT

Die Leistungsfähigkeit des KIT hängt maßgeblich von der Verfügbarkeit und Qualität der Dienste der Informationstechnik (IT) ab. Gleichwohl ist die IT-Infrastruktur immer stärkeren Gefahren ausgesetzt. Die Ergreifung von Schutzmaßnahmen zur Sicherstellung aller IT-gestützten Dienste in Forschung, Innovation, Studium und Lehre, Weiterbildung und Verwaltung am KIT besitzt daher höchste Priorität.



Das Präsidium hat eine Leitlinie zur IT-Sicherheit verabschiedet, die den Informationssicherheitsprozess für das KIT beschreibt und als Grundlage für ein IT-Sicherheitskonzept dient. Die daraus resultierenden Maßnahmen sollen eine größtmögliche Sicherheit im Bereich der Informationstechnik gewährleisten. Diese Sicherheit ist unabdingbare Voraussetzung für Datenschutzmaßnahmen, die insbesondere bei der Verarbeitung personenbezogener Daten zu garantieren sind. Eine erfolgreiche Umsetzung des IT-Sicherheitsprozesses setzt geregelte Verantwortungsstrukturen sowie die Unterstützung aller Mitglieder des KIT voraus.

Die IT-Sicherheitspolitik am KIT folgt dem Grundsatz, dass der Aufwand für die Schutzmaßnahmen stets in Relation zum erzielten Sicherheitsgewinn und dem Wert der zu schützenden Güter zu setzen ist, weil sich nur so auf Dauer das Bedürfnis nach Sicherheit und die Freiheit der Forschung miteinander vereinbaren lassen.

Die Sicherheitsleitlinie kann auf der Webseite des CIO (http://www.cio.kit.edu/downloads/KIT-Sicherheits-leitlinie.pdf) eingesehen werden.

Andreas Lorenz

New book: VANET

Vehicular Applications and Inter-Networking Technologies

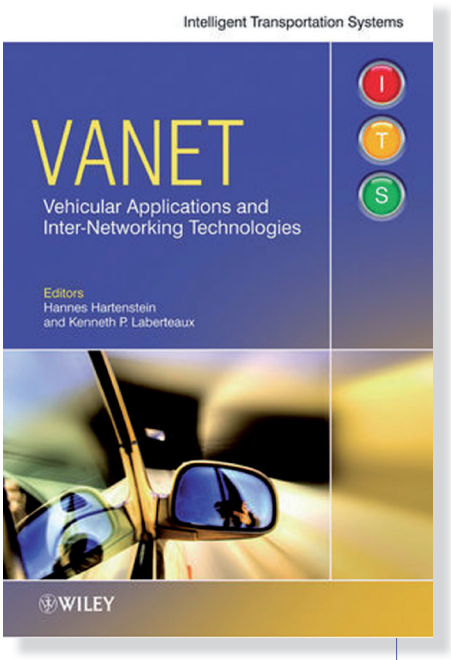
This book addresses the applications and technical aspects of radio-based vehicle-to-vehicle and vehicle-to-infrastructure communication that can be established by short- and medium range communication based on wireless local area network technology (primarily IEEE 802.11). It contains a coherent treatment of the important topics and technologies contributed by leading experts in the field, covering the potential applications for and their requirements on the communications system. The authors cover physical and medium access control layer issues with focus on IEEE 802.11-based systems, and show how many of the applications benefit when information is efficiently disseminated, and the techniques that provide attractive data aggregation (also includes design of the corresponding middleware). The book also considers issues such as IT-security (means and fundamental trade-off between security and privacy), current standardization activities such as IEEE 802.11p, and the IEEE 1609 standard series.

Key Features:

- Covers the state-of-the-art in the field of vehicular inter-networks such as safety and efficiency applications, physical and medium access control layer issues, middleware, and security
- Shows how vehicular networks differ from other mobile networks and illustrates the idea of vehicle-to-vehicle communications with application scenarios and with current proofs of concept worldwide
- Addresses current standardization activities such as IEEE 802.11p and the IEEE 1609 standard series
- Offers a chapter on mobility models and their use for simulation of vehicular inter-networks
- Provides a coherent treatment of the important topics and technologies contributed by leading academic and industry experts in the field

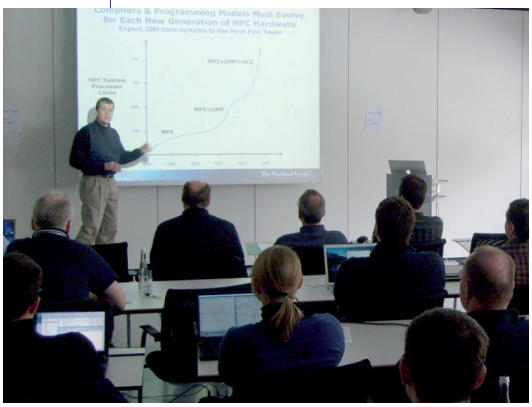
This book provides a reference for professional automotive technologists (OEMS and suppliers), professionals in the area of Intelligent Transportation Systems, and researchers attracted to the field of wireless vehicular communications. Third and fourth year undergraduate and graduate students will also find this book of interest.

(red)



VANET
Vehicular Applications and
Inter-Networking Technologies
Hannes Hartenstein (Editor),
Kenneth Laberteaux (Editor)
Publisher: John Wiley & Sons
ISBN: 978-0-470-74056-9
Hardcover
472 pages
January 2010

Workshop zu PGI Compiler und GPUs



Douglas Miles von der Firma The Portland Group stellte die wichtigsten Neuerungen zur PGI Compiler Suite vor.
Foto: Frank Schmitz

Im Februar fand im Gebäude des SCC-Süd ein Workshop zum Thema PGI Compiler und GPUs statt. Referent war Douglas Miles von der Firma The Portland Group, der von der Firma SMB, Vertriebspartner in Deutschland, unterstützt wurde.

In diesem Workshop wurden die Neuerungen der PGI Compiler Suite vorgestellt. Ein besonderes Augenmerk der Veranstaltung lag dabei auf dem PGI CUDA Fortran Compiler und dem erweiterten PGI Accelerator-Modell für CUDA. Der Compiler liefert GPU-Performance-Daten und Statistiken. Dabei ist die Analyse des Quellcodes durch die Anzeige des Compiler-Feedbacks im Quellcode-Browser des Profilers wesentlich vereinfacht.

Alle Teilnehmer des Workshops konnten die vorgestellten Neuerungen des PGI-Compilers an kleinen Beispielprogrammen praktisch ausprobieren.

Teilnehmer mit einem Notebook mit CUDA-fähiger NVIDIA-Grafikkarte konnten die Software direkt auf ihrem Notebook testen. Die Software und entsprechende Lizenzen wurden frühzeitig zur Verfügung gestellt.

Zu dem ganztägigen Workshop, der auf Englisch gehalten wurde, waren auch Interessenten von der RWTH Aachen angereist.

Der Compiler ist am gesamten KIT verfügbar. Ansprechpartner sind Hartmut.Haefner@kit.edu und Karl-Heinz.Schmidmeier@kit.edu.

Frank Schmitz

Block-Kurs Fortran 95/2003

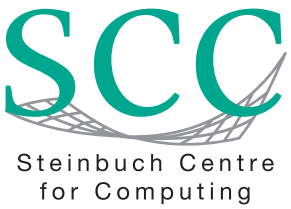
Im Februar fand am SCC-Süd ein dreitägiger Block-Kurs zu Fortran 95 und zu Fortran 2003 statt. Insgesamt unterteilte sich der Kurs in 6 Blöcke mit je 3 Stunden, wobei in jedem Block in einer Hälfte vorgetragen und in der anderen Hälfte das Vorgetragene an Hand von Programmieraufgaben eingeübt wurde. Referenten waren Hartmut Häfner und Torsten Adolph aus der Abteilung SCL (Scientific Computing Labs) des SCC.

Zweieinhalb Tage drehten sich die Vorträge und Übungen um die Grundlagen von Fortran 95. Die wichtigsten Themen waren: Syntax, (abgeleitete) Datentypen, Operatoren, Kontrollstrukturen, Module, Prozeduren, dynamische Daten, I/O und intrinsische Funktionen. Zuletzt wurden wichtige, bereits in die Compiler integrierte Merkmale von Fortran 2003 behandelt wie die Erweiterung des Modulkonzepts, Interoperabilität mit C sowie Unterstützung für Gleitkomma-Arithmetik und -Ausnahmebehandlung unter IEEE.

Bei den ca. 35 Teilnehmern handelte es sich um Mitarbeiterinnen und Mitarbeiter des KIT mit guten Programmierkenntnissen; sie haben drei Tage lang konzentriert mitgearbeitet und nahezu alle Programmieraufgaben erfolgreich implementiert. Der nächste Fortran-Kurs ist für den Herbst 2011 geplant.

Hinweis: Der Fortran-Compiler der Firma Intel wird nach Aussage von Intel ab Sommer 2010 Fortran 2003 vollständig unterstützen.

Hartmut Häfner



Steinbuch Centre for Computing (SCC)
76128 Karlsruhe
Tel: 0721/608-3754 oder 07247/82-5601
E-Mail: scc@kit.edu

www.scc.kit.edu