Nr. 5 / Juni 2001

ISSN 1605-475X

ZID line

INFORMATIONEN DES ZENTRALEN INFORMATIKDIENSTES DER TU WIEN

Studenten Software Service

Neu: IBM RS/6000 SP

Gigabit Ethernet

Inhalt

Impressum / Offenlegung gemäß § 25 Mediengesetz:

Herausgeber, Medieninhaber:
Zentraler Informatikdienst
der Technischen Universität Wien
ISSN 1605-475X

Grundlegende Richtung: Mitteilungen des Zentralen Informatikdienstes der Technischen Universität Wien

Redaktion: Irmgard Husinsky

Adresse: Technische Universität Wien,
Wiedner Hauptstraße 8-10, A-1040 Wien
Tel.: (01) 58801-42014, 42001
Fax: (01) 58801-42099
E-Mail: zidline@zid.tuwien.ac.at
WWW: http://www.zid.tuwien.ac.at/zidline/

Erstellt mit Corel Ventura
Druck: HTU Wirtschaftsbetriebe GmbH,
1040 Wien, Tel.: (01) 5863316

Editorial

Hier eine kurze Zusammenfassung des Inhalts der Sommer-Ausgabe der ZIDline. Wir hoffen, dass etwas Interessantes für Sie dabei ist.

Wir stellen unseren neuen Applikationsserver für Freie Programmierung vor, ein System IBM RS/6000 SP 9070-550, es ist auch auf dem Titelblatt zu sehen.

Studierende der TU Wien können Software zu äußerst günstigen Preisen erwerben. Dieses „Studenten Software Service“ der Abt. Standardsoftware wird im Detail präsentiert. Ein Bericht befasst sich mit Erfahrungen und Analysen zur Systemunterstützung der Arbeitsplatzrechner und Server der Institute.

Gigabit Ethernet hält Einzug im TUNET, siehe dazu ab Seite 13. Zum Thema Security finden Sie in dieser Ausgabe Tipps „wie kann ich mein Linux-System sicher machen“ und den Erfahrungsbericht eines Instituts über den Aufbau eines geschützten Subnetzes im TUNET.

Die momentanen Arbeiten und Diskussionen rund um eine neue Web-Präsenz für die TU sind der Anlass für den Artikel auf Seite 27.

Die Einsatzmöglichkeiten des auf einem zentralen Applikationsserver des ZID installierten Software-Pakets CFX-TASCflow werden aus der Sicht eines Anwenders aufgezeigt.

Wir drucken die Betriebs- und Benutzungsordnung des Zentralen Informatikdienstes (ZID) der Technischen Universität Wien. Sie wurde am 25. April 2001 vom Akademischen Senat beschlossen und tritt in Kraft, sobald sie vom Bundesministerium für Bildung, Wissenschaft und Kultur genehmigt und im Mitteilungsblatt der TU Wien veröffentlicht wurde.

Mein besonderer Dank gilt allen Autoren dieser Ausgabe für ihre Beiträge und die gute Zusammenarbeit.

Irmgard Husinsky

www.zid.tuwien.ac.at/zidline/

Der neue Applikationsserver Freie Programmierung

IBM RS/6000 SP Hochleistungsserver

Peter Berger

Im Sommer 2000 wurde mit den Vorbereitungsarbeiten für eine Ausschreibung eines neuen Applikationsservers „Freie Programmierung“ als Ersatz für den über 4 Jahre alten NEC-Vektorrechner (Applikationsserver „Lineare Algebra“) begonnen. Eine Arbeitsgruppe unter der Leitung des ZID, bestehend aus Vertretern der Hauptbenutzer der Applikationsserver „Freie Programmierung“ und „Lineare Algebra“, erarbeitete die Spezifikationen und stellte Benchmarkprogramme zur Verfügung.

Am 3. Oktober 2000 wurde eine EU-weite öffentliche Ausschreibung für dieses Hochleistungs-Serversystem veröffentlicht. Als maximaler Finanzrahmen standen ATS 8,5 Mio (aufgeteilt auf zwei Teilzahlungen, 2001 und 2002) zur Verfügung. Die Ausschreibung wurde von 21 Firmen abgeholt, von 5 Firmen wurden Angebote bis zur Anbotseröffnung am 23. 11. 2000 abgegeben.

Nach einer intensiven Evaluierungsphase wurde am 15. 2. 2001 der Zuschlag der Firma IBM für ein System ***IBM RS/6000 SP 9070-550,*** bestehend aus 3 Knoten SMP High Node (je 16 Prozessoren Power3, 375 MHz, Nighthawk2), erteilt.

Ein Blick in die Vergangenheit der SP-Systeme

In den späten 80er-Jahren gründete IBM ein Labor, *The High Performance Supercomputer System Development Laboratory* (HPSSDL), um eine Supercomputer-Technologie zu entwickeln, die möglichst auf weit verbreitete, nicht exotische Architekturen aufsetzt und skalierbar in Leistung und Preis war.

1990 veröffentlichte die IBM Advanced Workstation Division in Austin, Texas, die RISC-Systemfamilie (RS/6000) auf UNIX-Basis (Betriebssystem AIX). Diese RISC-Workstations wurden von HPSSDL in „Nodes“ gepackt und in „Frames“ zusammengefasst.

Zur gleichen Zeit wurde ein *High-Speed Switch* (Code-Name *Vulcan*) entwickelt, der die Zusammenschaltung von 16 Stück RS/6000 Systemen in einem Frame ermöglichte. Verbunden über ESCON-Adapter und eine entsprechende Management-Software war dieses System der erste Schritt zur SP-Serie.

1993 kam dieses System als SP1 (*Scalable Parallel System*) auf den Markt, die Anzahl von Knoten betrug max. 512 (gleichzusetzen mit max. 512 Prozessoren), als Management-Software wurde PSSP (*Parallel System Support Program*) entwickelt und eingesetzt.

1994 wurde die SP2 vorgestellt, ausgestattet mit unterschiedlichen Knoten und Prozessoren (Power2 und Power PC).

1996 wurde die SP-Serie als Top-End der RS/6000 Produktserie angekündigt, die Knoten unterstützen SMP-Architektur (*Symmetric Multiprocessor*), die Kopplung der Knoten erfolgt entweder über den Hochleistungs-Switch oder über einen Gigabit Ethernet Switch.

Die Architektur des neuen Systems IBM RS/6000 SP 9070-550

Das System besteht aus 3 SMP-Knoten (Nighthawk2), die in einem SP-Frame installiert sind. Jeder Knoten verfügt über 16 Prozesssoren, 16 GB Hauptspeicher und 2 lokale 36 GB Platten. Das Massenspeicher-Subsystem besteht aus einem externen SSA-System (IBM 7133/D40 SSA) mit insgesamt 10 SSA-Platten mit je 36 GB, die über SSA-Kabel mit dem ersten und zweiten Knoten verbunden sind. Zur Datensicherung ist ein LTO Ultrium Tape (IBM 3581/H17 LTO, 100/200 GB Speicherkapazität) installiert. Die Kopplung der Knoten erfolgt über Gigabit Ethernet und einen GBit-Switch mit 6 Ports.

Das Management der SP erfolgt über eine Control-Workstation (RS/6000 F50), die über RS232 und einen getrennten Management-LAN (100 MBit/s, Switch) mit den SP-Knoten verbunden ist.

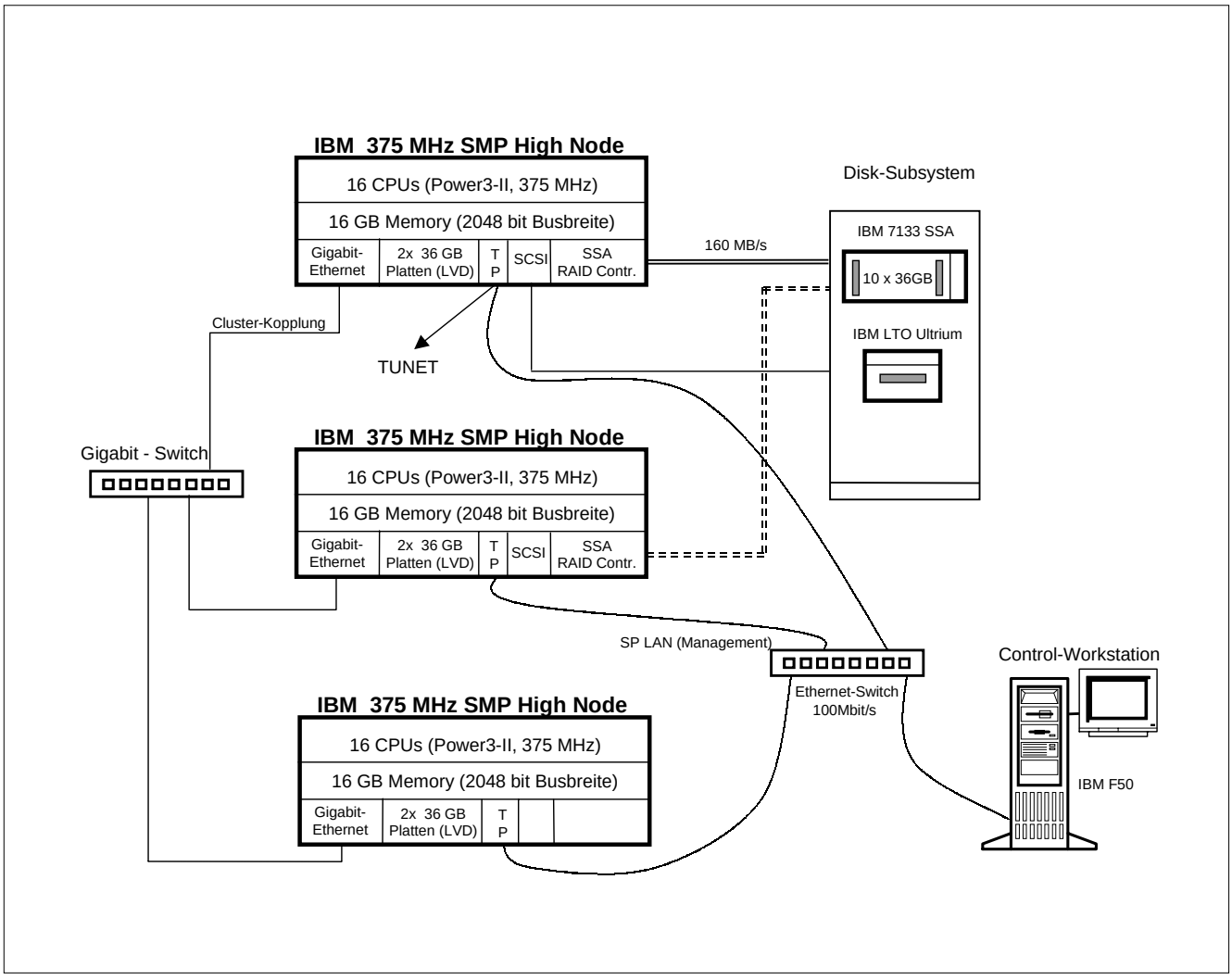
Der Anschluss an das lokale Netz der TU Wien ist mit 2x 100 MBit/s realisiert.

Bei der Erstellung der Spezifikationen für die Ausschreibung wurde von der Arbeitsgruppe gemeinsam mit dem ZID festgelegt, dass bei Clustersystemen die Knoten über mindestens 4 Prozessoren, die auf ein gemeinsames Memory zugreifen (SMP-Architektur), verfügen müssen.

Es war gefordert, dass die Kopplung dieser Knoten für eine Prozessoranzahl von 4 pro Knoten über ein Kopplungsmedium mit einer Bandbreite deutlich größer 1 GBit/s erfolgen muss. Bei Knoten mit mehr als 4 Prozessoren wurde die Bandbreite mit mindestens 1 GBit/s festgelegt.

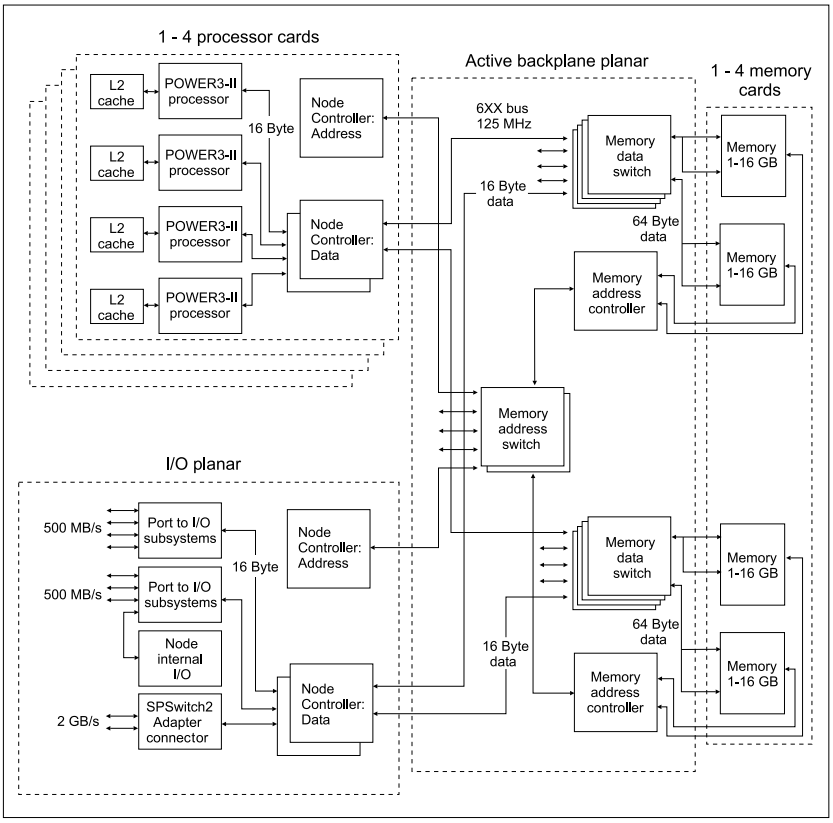
Der Grund dieser Abstufung ist die Tatsache, dass von Seiten der Institute für die großen Produktionsjobs kein hoher Grad an Parallelisierung verwendet wird. Die Nutzung von CPU-Ressourcen über Knotengrenzen hinaus ist von untergeordneter Bedeutung, wenn eine ausreichende Anzahl von CPUs innerhalb eines Knotens zur Verfügung steht.

Die Kopplung der Knoten über Gigabit-Ethernet ermöglicht (z. B. über MPI) die Nutzung von Ressourcen über Knotengrenzen hinweg, ist aber wesentlich preisgünstiger als die Kopplung über einen Hochleistungs-Switch.



Architektur IBM RS/6000 SP 9070-550

Blockdiagramm des 375 MHz Power3 SMP High Node (Nighthawk2)



Hardware:

IBM RS/6000 SP 9070-550 mit
3x Knoten 375 MHz SMP High Node (Nighthawk2), pro Knoten mit
- 16x CPU (Power3-II, 375 MHz, 8 MB Cache) 16 GB Hauptspeicher
- 2x 36 GB interne Platten (LVD)
- 1x Gigabit-Ethernet
- 1x 10/100 Ethernet (Management)
- 4x 10/100 Ethernet (nur Knoten 1)
- 1x SSA RAID Controller (nur Knoten 1 und 2)
- 1x SCSI (FWD, nur Knoten 1 und 2)

Disk-Subsystem IBM 7133/D40 SSA, 10x 36 GB SSA-Platten
Backup-Subsystem IBM 3581/H17 LTO Ultrium
Gigabit-Switch zur Kopplung der Knoten
100 MBit Switch zur Kopplung des Management-LAN
Control-Workstation IBM 7025/F50

Einige Leistungszahlen:

SPECint95	23.5
SPECfp95	51.3
SPECint2000	252
SPECfp2000	337
Linpack 1000x1000	1208 Mflops (1 Prozessor)

Das Kernstück der SP – der 375 MHz Power3 SMP High Node (Nighthawk2)

Prozessoren:
- 16 Prozessoren (Power3-II, 375 MHz, CMOS 7S Kupfertechnik)
- Superskalar-Architektur mit 8 Execution Units
- 32 KB Instruction Cache, 64 KB Data Cache, 8MB L2 Cache
- SMP-Architektur

Hauptspeicher:
- 16 GB, 4 Memory-Cards mit je 4 GB (max. 64 GB möglich)
- 4 Banks mit je 8 DIMM-Slots pro Memory-Card
- 4 GB/sec Bandbreite pro CPU-Card, 16 GB/sec Gesamtbandbreite

I/O-Subsystem:
- 2 getrennte PCI-Controller, SP-Switch Adapter (500 MB/sec)
- PCI 0: 1x 32-Bit, 2x 64-Bit, Ultra-SCSI, 10/100 Ethernet
- PCI 1: 2x 64-Bit

Disk-Subsystem:
- 2x interne 36 GB Platten, Ultra-SCSI, 10.000 rpm (Spiegelung)

Das externe Platten-Subsystem

Als externes Storage-Subsystem kommt ein IBM 7133 D40 (SSA-Subsystem), bestehend aus 10x 36 GB SSA-Platten, zum Einsatz. Dieses Subsystem ist über zwei

SSA-Loops mit zwei SSA-Adaptern (*FC 6230 Advanced SerialRAID Plus Adapter*) mit den Knoten verbunden. Mit diesem *Controller* können die Platten in *RAID-Sets* (RAID 0, 1, 5) zusammengefasst werden, *hot-spare Disks* werden natürlich unterstützt.

***Serial Storage Architecture* (SSA)**
ist eine schnelle, hochverfügbare, serielle Verkabelungstechnologie zur Verbindung von Platten und Hostadaptern auf Kupferbasis. SSA ist ein offener Standard (ANSI X3T10.1), der von der *SSA Industry Association* entwickelt wurde.

Die Basis der SSA-Technologie bildet die *Loop*, eine bidirektionale, im *full-duplex Mode* arbeitende serielle Verbindung zwischen den Hostadaptern und den Platten. Zwei unabhängige physikalische Pfade zum Lesen und zwei zum Schreiben zu jeder Platte in der *Loop* ermöglichen den Zugriff auf das Plattensystem auch dann, wenn die *Loop* an einer Stelle unterbrochen ist (z.B. Ausfall einer Platte oder defektes Kabel). Die maximale Transfer-Rate für jeden Schreib- oder Lesevorgang beträgt 40 MB/s, für die *Loop* ergibt das eine Bandbreite von maximal 160 MB/s.

Jeder Hostadapter verfügt über 2 *Loops*, die unabhängig und gleichzeitig lesen und schreiben können. Dadurch können sowohl Konfigurationen mit hoher Verfügbarkeit als auch mit hoher Durchsatzleistung realisiert werden. Die Kabel und Platten sind *hot-pluggable*, die *Loop* ist im Fehlerfall *self-configuring* und *self-repairing*, maximal 48 Platten sind pro *Loop* zulässig.

SSA ermöglicht ein *Mapping* der SCSI-2 Funktionen, aus der Sicht der Hostsoftware ist das Plattensystem ein SCSI-System mit allen Funktionalitäten.

Das *Storage-Subsystem* IBM 7133 / D40
besteht aus einem Gehäuse (Rackversion) mit 2 unabhängigen Netzteilen, 16 Steckplätzen für SSA-Platten und einer internen Verkabelung, die jeweils 4 Platten in eine *Loop* zusammenschaltet. Diese *Loops* sind nach außen geführt und können über SSA-Kabel (max. 25 m Kupfer, max. 10 km Glasfaser) an die Hostadapter angeschlossen werden.

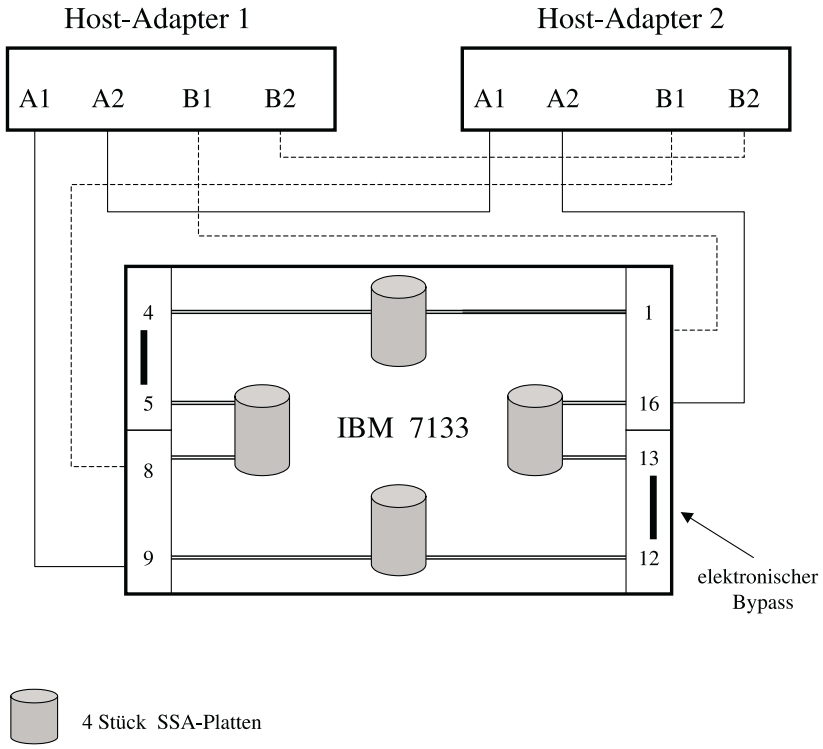
Die Konfiguration am ZID besteht aus 10 SSA-Platten mit je 36 GB, die über 2 *Loop*s mit den RAID-Controllern verbunden sind. Die Platten bilden zwei *RAID5-Sets*, die über die beiden *Loops* gleichzeitig angesprochen werden können. Um die Ausfallssicherheit zu erhöhen, wurde in einem anderen Knoten ein zweiter RAID-Controller installiert, der im Normalbetrieb nicht verwendet wird.

Auf dem externen Storage-Subsystem befinden sich die Home-Verzeichnisse der Benutzer, die über NFS an den Knoten zur Verfügung stehen.

Backup-System – IBM 3581 Ultrium Tape Autoloader

Im Jahr 1997 entwickelten die Firmen IBM, HP und Seagate gemeinsam einen neuen Standard – das *Linear Tape-Open* (LTO) *Program*. Ziel von LTO war, offene Spezifikationen für Bandspeichersysteme mit hoher Kapazität und Geschwindigkeit zu entwickeln (http://www.lto-technology.com/).

Zwei unterschiedliche Bandformate wurden definiert, LTO Accelis und Ultrium, wobei das Accelis-Format (Doppelspule, 8 mm Band) für hohe Zugriffsgeschwindigkeit optimiert wurde, das Ultrium-Format (*single-reel*, ½ Zoll Band) für hohe Speicherkapazitäten gedacht ist.



Die Basistechnologie von LTO wird als „*multi-channel linear serpentine recording*“ bezeichnet. Die Daten werden auf 384 Spuren geschrieben, die auf 4 *Data-Bands* zu je 96 *Tracks* aufgeteilt werden. Ein Schreib/Lesekopf schreibt 8 Spuren gleichzeitig, beginnend vom Bandbeginn zum Bandende. Dann wird die Position innerhalb des Bandes gewechselt und die nächsten 8 Spuren vom Bandende zum Anfang geschrieben. Für die richtige Positionierung des Kopfes sorgen 5 *Servo-Bands*, die sich zwischen den 4 *Data-Bands* befinden.

Der LTO Ultrium Tape Autoloader IBM 3581 speichert bis zu 100 GB (200 GB mit 2:1 Komprimierung) auf ein Ultrium-Medium. Die Host-Schnittstelle ist SCSI, die Transferrate beträgt 15 MB/s. Der *Autoloader* kann 7 Kassetten aufnehmen, das ergibt eine maximale Speicherkapazität von 700 GB (ohne Komprimierung).

Betriebssystem und Applikationssoftware

Software:
- AIX 4.3 (SP-Version und alle Komponenten des TU Campusvertrages)
- PSSP V2.4
- Parallel Environment for AIX V2.3
- C und C++ Compiler
- Fortran77 und Fortran90 Compiler
- HPF V1.3
- PD-Software (tcsh, ssh, …)
- LoadLeveler V2.2

Applikationssoftware:
- ESSL und OSL
- Parallel ESSL und Parallel OSL
- LaPack und ScaLaPack
- NAG Library Mark 19

Die Installation weiterer Softwarekomponenten erfolgt dem Bedarf entsprechend, vor allem der Einsatz von Software, die diese Rechnerarchitektur optimal nützen, ist erforderlich (sowohl *scalar* wie auch zur Parallelisierung).

Zugang über das TUNET

Der Systemzugang erfolgt ausschließlich über den Knoten 1 (sp01), nur dieser ist an das lokale Netz der TU Wien angeschlossen (Fast Ethernet, 100 MBit/s). Die anderen Knoten und die Control-Workstation sind direkt nicht erreichbar, können aber vom „Zugangsknoten“ aus angesprochen werden. Aus Sicherheitsgründen ist der Zugang nur über Secure Shell möglich (telnet und ftp sind nicht offen), ebenso können die Berkeley *r-Commands* (rlogin, rcp, ...) nicht verwendet werden.

Der Hostname (des Zugangsknotens) ist

```
hal.zserv.tuwien.ac.at
```

Betriebskonzept und Betriebsmittelvergabe

Die Abnahme des Gesamtsystems wurde erfolgreich am 27. April 2001 durchgeführt. Das System läuft im Testbetrieb, Anträge für eine Usernummer bitte wie üblich an das Sekretariat des ZID senden. Ein Betriebskonzept mit entsprechenden Batch-Queues wird demnächst zur Verfügung stehen.

Das neue System steht allen Instituten der TU Wien für selbstentwickelte Applikationen (freie Programmierung) mit relativ geringem Parallelisierungsgrad aber mit hohem Ressourcenbedarf (CPU und Speicherzugriffe) zur Verfügung.

Die Systemadministration und die Projektberatung wird von Herrn Dr. Ernst Haunschmid übernommen, für Fragen stehen wir jederzeit gerne zur Verfügung.

Studenten Software Service

Bernhard Simon

Seit dem Wintersemester 1999/2000 ermöglicht der Zentrale Informatikdienst den Studierenden an der TU Wien – als erster Universität in Österreich – den Bezug diverser Software zu äußerst günstigen Preisen. Dieses Service, das von der TU Wien stark subventioniert wird, hat großen Zuspruch gefunden. Im Folgenden werden die Voruntersuchungen, die Realisierung, das Angebot und die Erfahrungen zu diesem Service ausgeführt.

Evaluierung

Zum Zeitpunkt, als im Jahr 1999 ernsthaft an die Einführung eines „Studenten Software Service“ (SSS) gedacht wurde, stellte die Abteilung Standardsoftware im Bereich der Distribution kostenpflichtiger Software mit den beiden Diensten „Campus Software Service“ (CSS) und „Plattform Software Service“ (PSS) ihre Leistungen hauptsächlich den Instituten und Verwaltungseinrichtungen der TU Wien zur Verfügung. Im Laufe der letzten Jahre hat sich dabei ein gut funktionierendes System etabliert, das Bestellung, Bezug, Wartung und Verrechnung der verschiedensten Produkte zum Großteil automatisiert und servergestützt (Datenbank, Softwaremedien) abwickelt.

Um einerseits dem Auftrag des ZID nachzukommen, seine Leistungen nicht nur für Forschung und Administration zur Verfügung zu stellen, sondern auch im Bereich der Lehre den Studenten zugänglich zu machen, andererseits dem Interesse der Studenten nach kostengünstiger Software, die im Rahmen der Ausbildung sinnvoll eingesetzt werden kann, zu entsprechen, wurde – weil auch von einzelnen Firmen die Bereitschaft zur Unterstützung dieses Vorhabens vorhanden war – von der Abteilung Standardsoftware das Projekt „Studenten Software Service“ ins Leben gerufen, mit dem Ziel – nach Klärung der dafür notwendigen Voraussetzungen und Schaffung der entsprechenden Rahmenbedingungen – ab dem Wintersemester 1999/2000 Campussoftware in den Softwarekategorien Graphik/Visualisierung, Mathematik, Office Automation und PC Systemsoftware für Studenten anzubieten.

Unter Berücksichtigung der Vorgaben

1. Jeder Student der TU Wien soll berechtigt sein, Campus Software für Studenten zu beziehen.
2. Die Studentensoftware sollte (möglichst in vollem Leistungsumfang) zu einem attraktiven Preis angeboten werden.
3. Der Administrationsaufwand sollte minimal sein (kein zusätzliches Personal).
4. Bereits bestehende Infrastruktur und Verteilungsmechanismen sollten nach Möglichkeit genutzt werden.

stellte sich sehr bald heraus, dass existierende Mechanismen zur Abwicklung von Geschäftsfällen, wie sie – abgestimmt auf die vorhandenen Strukturen einer Universität (Institute, Personal) – eingerichtet wurden, für die Verteilung der Studentensoftware nur in geringem Maße anwendbar sind. Die wichtigsten Unterschiede in den Problembereichen

- Personen – Erfassung aller Studenten, Identifikation, Erreichbarkeit
- Verteilung – Zugangsmöglichkeit zum Server (Netzanbindung erforderlich, Accounts), Zugang von außerhalb des TUNET (Einschränkungen, Protokolle, Bandbreite)
- Verrechnung – Infrastruktur müsste komplett neu aufgebaut werden

zeigten auf, dass eine servergestützte Verteilung der Studentensoftware unter den derzeitigen Voraussetzungen an der TU nicht durchführbar ist.

Der traditionelle Ansatz für die Verteilung von Software (Produktion und Verkauf der Medien) kann – weil eine entsprechende Verkaufsstelle im ZID nicht eingerichtet ist – nur mit externer Unterstützung realisiert werden. In Gesprächen mit der Hochschülerschaft der TU Wien (HTU) stellte sich heraus, dass nicht nur die Bereitschaft zur Zusammenarbeit vorhanden ist, sondern auch mit dem Lehrmittelzentrum (LMZ) die Voraussetzungen und Kapazitäten existieren, Studentensoftware allen Bezugsberechtigten zu verkaufen.

Im Zusammenhang mit der Produktion der Medien wurde untersucht, ob die Produktion – nach Anschaffung entsprechender Geräte – im Haus erfolgen kann, oder besser einer externen Firma übertragen werden soll. Unter Berücksichtigung der zu erwartenden Stückzahlen und der erforderlichen Qualität stellte sich – nachdem eine

Firma gefunden wurde, die auch Kleinserien prompt liefern kann – die zweite Variante als sinnvoller heraus.

Wegen der Kosten, die bei der externen Produktion der CDs anfallen, muss sich das Angebot auf jene Produkte beschränken, bei denen der Absatz von großen Stückzahlen (mindestens 1000 pro Version) zu erwarten ist und zu deren Verteilung eine CD ausreicht. In Sonderfällen – wenn ein Produkt, das aus mehreren CDs besteht, auf eine CD zusammengeschnitten werden muss – wird auch eine eingeschränkte Funktionalität in Kauf genommen, jedoch explizit darauf hingewiesen.

Unter Berücksichtigung der angegebenen Bedingungen ergab sich letztendlich folgende Arbeitsteilung als Grundlage für die Realisierung des „Studenten Software Service“:

ZID, Abteilung Standardsoftware:
- Abschluss der Campusverträge
- Bereitstellung der Medien (Produktion extern)
- Ankündigungen, (Lizenz-)Informationen
- Logistik, Lizenzkontrollen

HTU, Lehrmittelzentrum:
- Überprüfung der Identität (Studentenausweis)
- Unterzeichnung der Lizenzbedingungen durch den Studenten
- Verkauf der Software
- Rückmeldung der Verkaufsdaten an den ZID
- Public Relations

Realisierung

Dieser Abschnitt stellt das Studenten Software Service – wie es seit Oktober 1999 läuft – vor, gibt einen Überblick über das aktuelle Softwareangebot und beleuchtet das Service aus der Sicht der Studenten, des Lehrmittelzentrums und des ZID.

Das Studenten Software Service, das vom Zentralen Informatikdienst, Abt. Standardsoftware in Zusammenarbeit mit der Hochschülerschaft der Technischen Universität Wien (HTU) und zum Teil mit dem Institut für Analysis und Technische Mathematik, Abt. Regelungsmathematik und Simulation angeboten wird, soll den Studenten eine legale Möglichkeit zum Einsatz wichtiger Software bieten und wird von der Technischen Universität entsprechend subventioniert. Die Software hat zumeist den normalen Leistungsumfang und wird den Studenten stark verbilligt für ihren privaten Heimgebrauch zur Verfügung gestellt. Sie beinhaltet keine gedruckte Dokumentation und darf nur für nicht kommerzielle Anwendungen eingesetzt werden.

Jeder Student der Technischen Universität Wien ist berechtigt, Campus Software für Studenten zu beziehen. Die Verteilung erfolgt über die Buchhandlungen des Lehrmittelzentrums (Bibliotheksgebäude der TU bzw. am Rilkeplatz 3). Der Student unterschreibt eine Erklärung, dass er sich an die Lizenzbedingungen hält und erhält eine CD mit der Software, wobei ein geringer Kostenbeitrag (für jedes Produkt weniger als ATS 100.-) verrechnet wird. Neue Versionen dieser Software sind in gleicher Weise beziehbar.

Berechtigt sind alle Studierenden, die an der TU Wien gültig rückgemeldet sind und dies im Lehrmittelzentrum beim Kauf der Software durch Vorlage eines gültigen Studentenausweises oder einer Inskriptionsbestätigung nachweisen können.

Die von den Studenten unterzeichneten Lizenzbedingungen garantieren, dass die Studentensoftware nicht zweckentfremdet verwendet wird:

1. Die Lizenz für die Campus Software für Studenten berechtigt nur Studenten der Technischen Universität Wien zur Nutzung (Speichern, Laden, Ausführen) der Software auf genau einem Personal Computer unter genau einer Version genau eines Betriebssystems und gilt solange die Bedingung „Student der Technischen Universität Wien“ erfüllt ist.

2. Es darf maximal eine Software-Kopie zu Backup- bzw. Archivierungs-Zwecken angelegt werden und die Software (bzw. Kopien davon) darf nicht an Dritte weitergegeben werden.

3. Die Software darf nur zu Zwecken der eigenen Ausbildung genutzt werden. Jede – wie auch immer geartete – kommerzielle Nutzung ist nicht gestattet.

4. Der Lizenznehmer verpflichtet sich, keine Versuche (wie z.B. durch Reverse Engineering oder Disassembling) zu unternehmen, geheime bzw. vertrauliche Informationen über die Funktionalität der Software und deren interne und externe Schnittstellen herauszufinden.

5. Wenn die Bedingungen (Student der Technischen Universität Wien) für die Verwendung der Software nicht mehr erfüllt sind, darf die Software nicht mehr weiterverwendet werden und muss vom Rechner entfernt werden. Medien und Kopien davon müssen unbrauchbar gemacht werden.

Microsoft Produkte dürfen (nach den derzeit gültigen Bestimmungen) auch nach Beendigung des Studiums weiter verwendet werden, dann allerdings nur für den privaten Gebrauch.

Alle Lizenzen gelten jeweils für den vollen Produktumfang, selbst wenn aus Kostengründen nur ein Teil der Software auf der im Lehrmittelzentrum verteilten CD untergebracht werden konnte. Bei Microsoft Produkten berechtigt die Studentenlizenz auch zum Einsatz einer anderssprachigen Variante des lizenzierten Produkts, das allerdings nur anstelle der erworbenen deutschen Version.

Nachfolgende Aufstellung gibt einen Überblick über das aktuelle Softwareangebot für Studenten und listet vollständigkeitshalber auch ältere – längst ausverkaufte – Versionen aus dem Bereich Mathematik.

Für die ursprünglich zur Verteilung vorgesehenen Produkte MS Visio 2000, MATLAB und Adobe Photoshop konnten mit den Firmen keine akzeptablen Verträge ausverhandelt werden, sodass es derzeit keine Möglichkeit einer Studentenlizenz gibt.

Informationen zum Studenten Software Service werden den Studenten über verschiedene Kanäle angeboten:

Produkt	Version	Plattform	seit	bis	Code	Auflage
Maple	5.1	Win/Mac/Linux	14.10.1999	27.07.2000	MAP9901	650
	6.01	Win/Mac/Linux	26.09.2000		**MAP**0002	1000
Mathematica	4.0.1	Win/Mac/Linux	06.12.1999	01.07.2000	MAT9901	850
	4.0.2	Win/Mac/Linux	20.07.2000	20.04.2001	MAT0002	1000
	4.1	Win/Mac/Linux	25.04.2001		**MAT**0103	1000
MS Windows 98	Second Ed., deutsch	Win	24.05.2000		**W98**0001	2000
MS Office 2000	Prof., deutsch	Win	27.06.2000		**OFF**0001	4000
MS Windows 2000	Prof., deutsch	Win	20.07.2000		**W2K**0001	3000
Lotus SmartSuite	9.5, deutsch	Win	28.09.2000		**LSS**0001	1000
MS Windows Me	deutsch	Win	03.10.2000		**WME**0001	2000
MS Visual Studio	6.0 TU Ed., deutsch	Win	05.10.2000		**VST**0001	1000
SigmaPlot 2000	6.1	Win	01.03.2001		**SPL**0101	500

- SSS Homepage als primärer Einstiegspunkt zu Informationen: http://sts.tuwien.ac.at/sss.html
  Sie beschreibt ganz allgemein das Studenten Software Service, gibt Hinweise zum Bezug der Software und zu den Lizenzbedingungen und enthält die so genannten Produktpages mit Kurzinformationen zum jeweiligen Produkt, Versionsangaben, Preis, spezielle Lizenzbedingungen, technische Anforderungen und Links zu weiterführenden Informationen (des Herstellers).

- Newsgroup at.tuwien.student
  (und at.tuwien.zid.neuigkeiten)
  Hier wird punktuell über neue Produkte bzw. Updates informiert und einmal pro Semester ein Überblick über das aktuelle Software-Angebot gegeben. Dieses Medium wird auch genutzt, um Fragen von allgemeinem Interesse (z.B. über Produktumfang oder spezielle Lizenzangelegenheiten) zu klären.

- Schaukasten im Freihaus 2. Stock, gelber Bereich, beim Internet Raum FHBR2

- Plakate des Lehrmittelzentrums
  Besonders wirksam sind die Plakate in den Verkaufsräumen des LMZ oder die Plakatständer, die gelegentlich vor dem Geschäft aufgestellt werden.

- Aussendungen und Zeitschriften der HTU (z. B. zu Semesterbeginn)

Neben seinen Verkaufs- und Kontrolltätigkeiten erfasst das Lehrmittelzentrum (derzeit noch manuell) alle zur Lizenzkontrolle relevanten Verkaufsdaten und gibt sie an den ZID weiter. Auch die von den Studenten unterzeichneten Lizenzbedingungen werden – als Beleg den Firmen gegenüber – im ZID archiviert.

Von der Entscheidung, ein bestimmtes Produkt als Studentensoftware anzubieten, bis hin zu dessen Verteilung und Wartung ist ein langer Weg, der nur dann erfolgreich ist, wenn alle daran Beteiligten gut zusammenarbeiten:

- Vertragsverhandlungen
- Abkommen mit der HTU
- Erstellen einer Master CD, falls erforderlich
- Testen, Prüfsummenerstellung, CD-Beschriftung
- Produktion der CDs durch externe Firma
- Überprüfung der Lieferung (Stichproben)
- Erstellen von Informationsmaterial (Beiblatt etc.)
- Ankündigungen (Web, Newsgroups, Schaukasten, Plakate)
- Verkauf durch LMZ
- Bearbeitung von Anfragen, Problemen, Nachbestellungen, neue Versionen
- Erfassung, Kontrolle und Verrechnung der Verkaufsdaten, in Abteilungsdatenbank

Statistik

Den folgenden Untersuchungen über Anzahl der Lizenzen pro Student und Verteilung nach Studienjahrgängen liegt das gesamte vorhandene Datenmaterial (vom Start des Service am 14. 10. 1999 bis zum zuletzt erfassten Wert am 4. 5. 2001) zugrunde. Bis zu diesem Stichtag – dem Zeitpunkt der Fertigstellung dieses Berichtes – wurden insgesamt 13379 Lizenzen an 5783 Studenten vergeben.

Diese Lizenzen teilen sich folgendermaßen auf die 9 derzeit angebotenen Produkte auf, wobei bereits 70% der Lizenzen durch die 4 gängigen Microsoft Produkte Office und Windows 98/Me/2000 abgedeckt sind (Abb. 1).

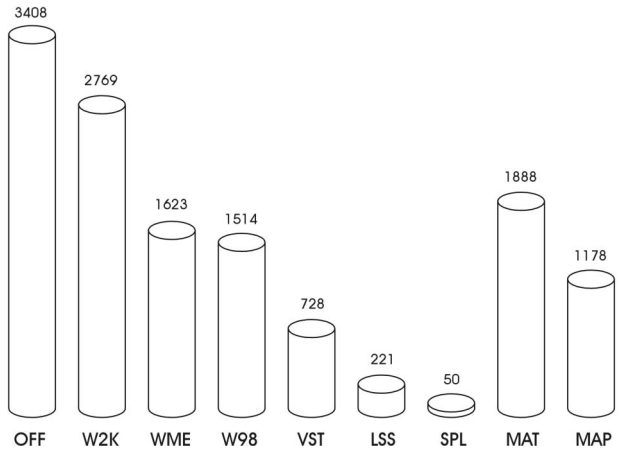


Abb. 1: Verteilung der Lizenzen nach Produkten

Bei Klassifizierung der 13379 Lizenzen nach Studienjahrgang (erste und zweite Stelle der Matrikelnummer) des Käufers zeigt sich die erwartete Abnahme an Lizenzen bei Studenten höheren Semesters (Abb. 2). Auffallend ist der relativ hohe Anteil älterer Semester.

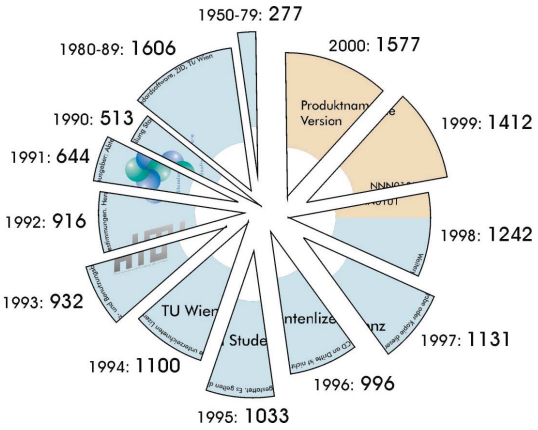


Abb. 2: Verteilung der Lizenzen
nach Studienjahrgang des Käufers

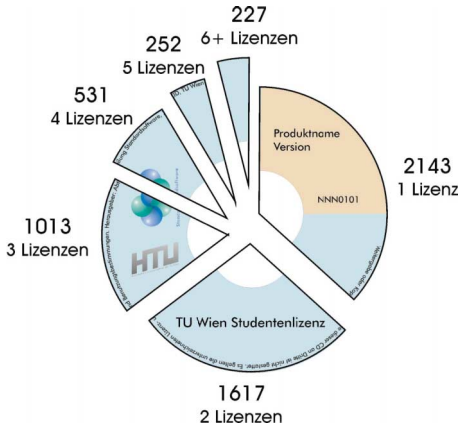


Abb. 3: Verteilung der Studenten
nach Anzahl der Lizenzen

Zwischen den einzelnen Studienjahrgängen gibt es so geringe Abweichungen beim Verhältnis der einzelnen Produkte zueinander, dass es sogar auffällt, wenn Erstsemestrige vermehrt Windows Me (18% statt durchschnittlich 12%) kaufen und die Studienjahrgänge 1950-79 sich weniger für Office und Windows (57% statt 70%) interessieren.

Abbildung 3 zeigt, wie viele CDs jeder einzelne der 5783 Studenten erworben hat. Auch hier gibt es wieder eine gute Übereinstimmung zwischen den einzelnen Studienjahrgängen. Bemerkenswert ist einzig, dass die Studienjahrgänge 1950-79 zu einem hohen Anteil (18% statt durchschnittlich 4%) 6 und mehr CDs kaufen.

Die Lizenzentwicklung für die einzelnen Produkte seit dem Bestehen des Studenten Software Service ist in Abbildung 4 dargestellt. Neben den erwarteten steilen Anstiegen in den Wochen unmittelbar nach der Einführung eines neuen Produkts sind die beachtlichen Zuwächse zu Beginn des Wintersemesters 2000/2001 besonders auffällig und lassen sich mit folgenden Zahlen belegen.

In den vier Wochen zu Semesterbeginn (das waren auch die einzigen Wochen des Jahres 2000 mit einem Wochenumsatz von mehr als 500 Lizenzen, Spitzenwerte: zweite Oktoberwoche mit insgesamt 858 Lizenzen, 9. Oktober mit 209 Stück Tagesumsatz), wurde – bezogen auf die Stückzahlen – fast ein Drittel (29.7%) des Jahresumsatzes abgewickelt. In diesem Zeitraum erreichten auch die einzelnen Produkte – was die täglichen Verkaufszahlen betrifft – ihr relatives Maximum. Den absoluten Rekord hält bislang Office mit den 3 Spitzenwerten 104, 63 bzw. 80 – aufgestellt zwischen dem 28. und 30. Juni, also den drei Tagen nach der Freigabe des Produkts.

Wie die Auswertung der Web-Zugriffsdaten des Jahres 2000 zeigt, wurden die Informationsseiten über das Studentensoftware Angebot (nicht nur von Rechnern an der TU Wien) häufig frequentiert, wobei alle Informationen *public* waren und Zugriffe von Teleweb, Chello, ... bei „nicht TU“ gezählt wurden.

2000	hosts	requests	kbytes	%transfer
nur TU	1337	28923	61337	28.2
nicht TU	13298	75249	156235	71.8
Summe	14635	104172	217572	100

Dabei fanden die Informationen über Mathematica, die Lizenzbestimmungen, und in weiterer Folge über die Produkte Maple, Windows 98 und Office 2000 besonderes Interesse.

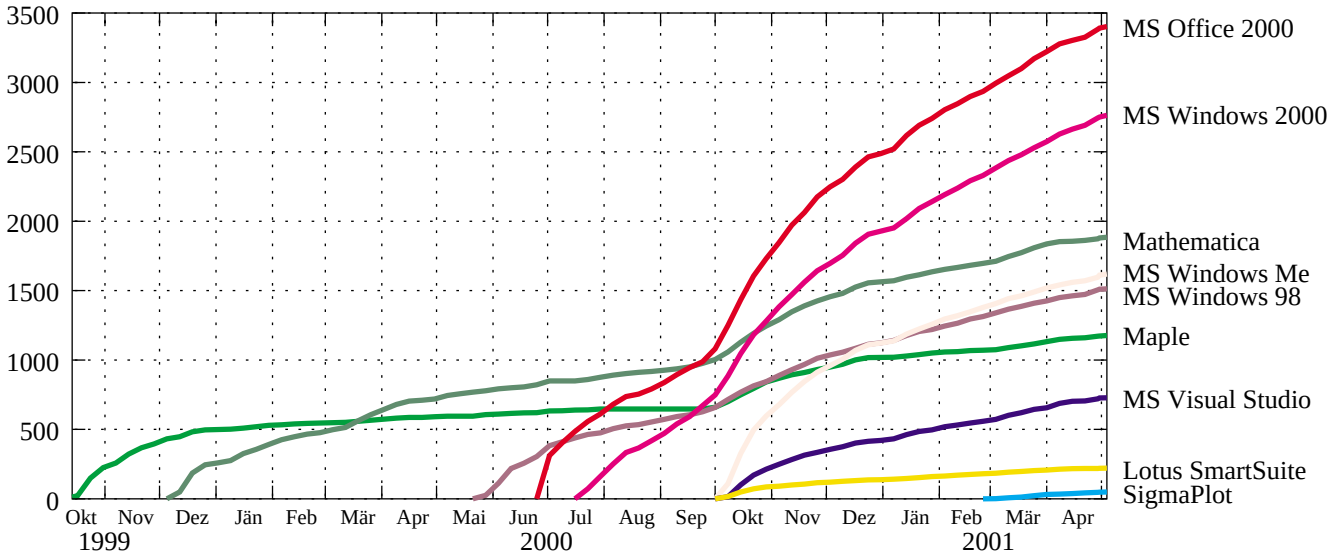


Abb. 4: Lizenzentwicklung gesamt

Erfahrungen

Die Erfahrungen seit dem Beginn der Verteilung im Herbst 1999 zeigen nicht nur eine erfolgreiche Umsetzung der konzipierten Distributionsmechanismen und eine ausgezeichnete Zusammenarbeit mit den Partnern, sondern auch, dass dieses Service bei den Studenten gut ankommt und stärker als ursprünglich vermutet genutzt wird.

Aufgrund der ersten Verkaufszahlen konnte davon ausgegangen werden, dass von den meisten Produkten zumindest 1000 Stück verkauft werden. Somit war es möglich, die Produktionskosten pro CD durch entsprechend große Serien – wodurch erst ein billigeres Produktionsverfahren angewendet werden konnte – auf ungefähr ein Drittel des bei Kleinserien erzielbaren Preises zu reduzieren.

Da im Vorhinein nicht abzuschätzen war, wie groß der Bedarf bei den einzelnen Produkten sein wird, wurden alle neuen Produkte zunächst mit einer Auflage von 1000 Stück eingeführt, und erst später – der Nachfrage entsprechend – in 1000er Schritten nachproduziert.

Die mit der Produktion der CDs beauftragte Firma FANCY-MEDIA erwies sich als sehr zuverlässig und arbeitet mit hoher Qualität, was sich daran zeigte, dass die wenigen als unlesbar reklamierten CDs zumeist in Ordnung waren und der Fehler vielmehr an defekten CD Laufwerken der Studenten lag. Trotzdem kam es (durch eher untypische Produktionsfehler) zur Lieferung von zwei Serien mit jeweils 1000 defekten CDs, die aufgrund der bestehenden Kontrollmechanismen im ZID rechtzeitig vor deren Verteilung als solche erkannt wurden. Nachdem bewiesen werden konnte, dass die Ursache des Problems nicht eine fehlerhafte Vorlage (Master CD) war, wurde die Lieferung ohne zusätzliche Kosten prompt ausgetauscht. Ab diesem Zeitpunkt wurde verstärkt daran gearbeitet, mögliche Fehlerquellen bei der Erstellung der Master CD durch zusätzliche Tests zu vermeiden und die Identität von Kopie(n) und Master durch Prüfsummen zu verifizieren.

In einer im Dezember 1999 mit der Verteilung von Mathematica gestarteten Umfrage wurden Richtwerte über den Einsatz der von den Studenten verwendeten Plattformen Windows, Linux bzw. Macintosh gesammelt, um bei Bedarf die Produktion plattformspezifischer CDs besser steuern zu können. Dabei stellte sich heraus, dass die Studenten zum überwiegenden Teil Windows verwenden und dass eine Produktion von eigenen, plattformspezifischen CDs wegen der zu geringen Stückzahlen wohl kaum in Frage kommt.

Von Studentenseite wurde unter anderem angeregt, auch Linux-Distributionen ins Programm aufzunehmen und einige Produkte zusätzlich in anderen Sprachvarianten (z. B. in Englisch) anzubieten. Ersteres erwies sich nach internen Diskussionen allein schon produktionstechnisch als nicht zielführend (relativ billige kommerzielle Angebote, Vielfalt der Distributionen, Häufigkeit der Updates). Aufgrund der erforderlichen hohen Stückzahlen ist die Verteilung einer zusätzlichen Sprachvariante eines Produkts kostenbedingt nicht durchführbar, eine Umstellung des gesamten Angebotes z. B. von deutsch auf englisch – allein schon vom Bedarf her – unrealistisch.

Schon von Anbeginn war klar, dass aufgrund der zu erwartenden großen Studenten- und Lizenzzahlen das Service so aufgezogen werden muss, dass kein direkter Kontakt des ZID mit den Studenten erforderlich wird und nur in Ausnahmefällen auf administrative bzw. Lizenzfragen – jedoch nicht auf Supportwünsche – persönlich eingegangen werden muss. In diesem Zusammenhang stellten sich vom Hersteller 1:1 übernommene und vom ZID nicht weiter modifizierte CDs rein argumentativ als vorteilhaft heraus, wenn Beschwerden über angeblich nicht installierbare Software vorgebracht wurden. Um das Produkt Mathematica verwenden zu können, muss sich jeder Lizenznehmer bei der Firma Wolfram Research registrieren und ein Passwort anfordern, das nach ca. einem Jahr abläuft. Dadurch ergibt sich ein nicht kalkulierbarer externer Faktor, der (verständlicherweise) verstärkt zu Anfragen und Beschwerden führt, wenn es Probleme bei dieser Registrierung gibt – egal, wer der Verursacher dafür ist. In den bisher zwei Fällen, als die Registrierungsstelle über mehrere Tage hindurch nicht erreichbar war, oder – noch unangenehmer – nicht funktionierende Passwörter ausstellte, zeigte sich, dass solche Ausnahmesituationen einen Mitarbeiter in seinen sonstigen Tätigkeiten mehr oder weniger lahmlegen.

Ausblick

Für die nächsten Jahre ist eine Weiterführung dieses Services und ein kontinuierlicher Ausbau des Angebots vorgesehen.

Konkret geplant sind die Verteilung der neuen Microsoft XP Produkte sowie laufende Updates von bereits etablierter Software wie Mathematica oder Maple.

Es bleibt abzuwarten, ob bzw. welche Auswirkung die Einführung von Studiengebühren auf das Studenten Software Service haben wird.

Mit flächendeckenden und einheitlichen Mechanismen zur Identifikation und Authentifikation aller TU Studenten (z. B. Student-Card, Accounts für alle Studenten) könnte die Administration der Studentensoftware effizienter gestaltet und die Lizenzkontrolle verbessert werden.

Vortragende, die in ihren Lehrveranstaltungen Studentensoftware als Hilfsmittel empfehlen oder verwenden, sollten mit dem ZID Kontakt aufnehmen, damit einerseits sichergestellt ist, dass zu Beginn der jeweiligen Veranstaltung im Lehrmittelzentrum ausreichend Medien lagernd sind, andererseits sie selbst über geplante Veränderungen (Updates, neue Produkte) vorab informiert werden können.

Wir sind überzeugt, dass dem ZID mit der Einführung des Studenten Software Service ein weiterer Beitrag zum legalen Einsatz von Standardsoftware gelungen ist und hoffen, dass die angebotenen Produkte von den Studenten widmungsgemäß als wertvolle Unterstützung im Rahmen ihrer Ausbildung genutzt werden.

Webpage

`sts.tuwien.ac.at/sss.html`

TUNET Backbone & Gigabit

Johann Kainrath

Neben der ATM-Technologie, die sich nicht so schnell aus dem TUNET verabschieden wird, hält Gigabit Ethernet Einzug, eine Technologie, die neben 1000 MBit/s Bandbreite auch Stabilität und Flexibilität für das High-Speed Backbone der TU Wien verspricht.

Backbone an der TU Wien

Die bereits 1996 begonnene Umstrukturierung des Backbone auf ein ATM-Netz konnte im Jahr 1999 weitgehend abgeschlossen werden. Die Infrastruktur für die Datenkommunikation zur Verbindung der Gebäudekomplexe am Campusbereich basierte damit zu diesem Zeitpunkt fast ausschließlich auf Asynchronous Transfer Mode (ATM) über Glasfaserkabeln. ATM bot neben anderen Vorteilen wie Skalierbarkeit auch im Bereich Sprachdienste in einem Netzwerk Möglichkeiten zur Realisierung. Durch die Flexibilität von ATM war die Integration des neuen über die TU-Standorte verteilten und redundant aufgebauten Telekommunikationssystems in das TUNET-Daten-Backbone möglich.

Mit der gewählten ATM Implementierung stand und steht allen Benutzern der TU Wien mittels TUNET eine moderne und leistungsstarke Infrastruktur zur Verfügung, die sich auf stabile Art und Weise bereits bewährt hat.

Hauptanforderungen an das Backbone, nämlich ausreichend Bandbreite zur Übertragung von Daten und Sprache auf sämtlichen Verbindungen sowie Redundanz in höchstem Maße, sind garantiert, erfordern jedoch einen stetig vorangetriebenen Ausbauprozess.

Kernstück bisheriger Planungen war nach wie vor die Verbindung der zentralen Gebäudekomplexe Freihaus, Karlsplatz und Gußhaus mit ausreichender Kapazität, nämlich 622 MBit/s. 1999 wurde in dieses Dreieck der vierte Eckpfeiler, nämlich der Gebäudekomplex Favoritenstraße integriert. Damit verfügte die TU Wien über genug Bandbreite am Campusbereich, in Summe also über 7 OC12 (622 MBit/s) Verbindungen zwischen oben erwähnten Standorten.

Bisher gelang es durch geeignete Infrastruktur-Anpassungen immer, diesen steigenden Bedarf der Datenkommunikation sowohl im Backbone als auch bei der Anbindung im Institutsbereich zu befriedigen. Die Bandbreite auf einem ATM Link im TUNET beträgt jedoch maximal 622 MBit/s (entspricht OC12). Gigabit Ethernet bietet hier von Beginn weg höhere Bandbreiten, außerdem ist eine mögliche Skalierbarkeit durch so genannte Gigabit Ethernet Channels gegeben.

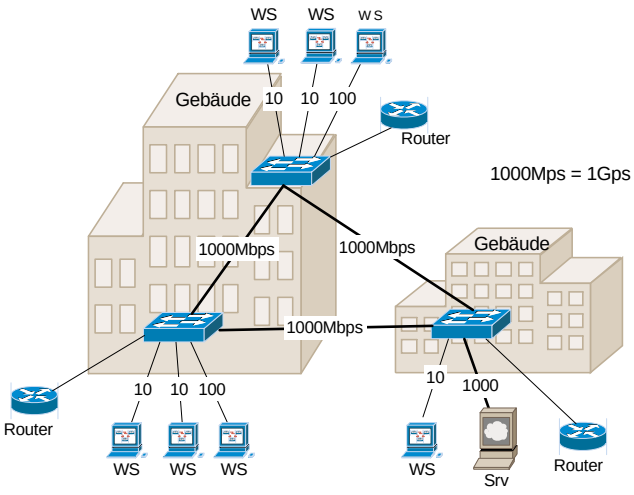
1999 erstmals Gigabit

Als neue Technologie wurde daher bereits 1999 erstmals Gigabit Ethernet bei Uplinks vom Backbone zum Distribution/Access-Bereich ins Spiel gebracht. Im Freihaus und in der Favoritenstraße wurden erste sehr positive Erfahrungen gesammelt. Bereits damals wurde daran gedacht, die zur Datenkommunikation eingesetzte Technologie (ATM LAN Emulation = Emulieren eines Ethernet LANs auf ATM Zellen Technologie) zu Gunsten von Gigabit Ethernet zu reduzieren. In diese Richtung gingen und gehen auch die Entwicklungen und Trends am Netzwerksektor.

Gigabit Ethernet (GE) – Die Technologie

100 MBit/s oder Fast Ethernet reichte vielen bereits bei seiner Einführung nicht aus, somit wurde im Juni 1998 eine neue höhere Bandbreitentechnologie auf die Industrie losgelassen. Gigabit Ethernet (IEEE 802.3z) spezifiziert Datenübertragung im Bereich 1000 MBit/s, also wieder eine zehnfache Steigerung der Bandbreite. Wozu ist diese erneute Steigerung eigentlich notwendig ? Manchmal scheint es schon schwierig zu sein, eine 100 MBit/s Full Duplex Verbindung voll auszulasten. Was also mit 1000 MBit/s tun ? Befürworter der Gigabit Ethernet-Technologie sehen Haupteinsatzgebiete einerseits im Backbone-Bereich (Verbindungen zwischen Gebäuden bzw. als Uplink im Gebäude) als auch im Bereich Anschluss von High Speed Fileservern. Es ist nicht zu erwarten, dass normale Netzwerkclients (PCs, Workstations) demnächst flächendeckend direkt via Gigabit Ethernet angeschlossen werden. Diverse Studien belegen, dass bei Workstations in der „Pentium PC Klasse“, in denen ein Gigabit Ethernet Interface eingebaut wird, die

(Netzwerk-) Performance eher sinkt und die CPU bei hohem Netzverkehr überlastet ist (eine erreichte Datenrate von 400 MBit/s scheint hier zum heutigen Zeitpunkt realistisch zu sein). Hier werden wohl auch Netzwerk-Karten Abhilfe bringen, die den TCP/IP-Stack bereits *on-board* implementiert haben. Andererseits können UNIX Hochleistungsworkstations durchaus von einer Gigabit Ethernet Pipe zum Netzwerk profitieren.



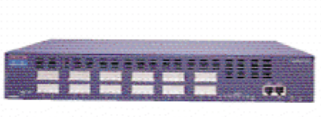
Gigabit Ethernet Backbone Architektur

Die Gigabit Ethernet Spezifikation mixt Eigenschaften von 802.3 Ethernet und Fiber Channel (eine Gigabit Technologie als LAN-Ersatz zum direkten High Speed Zusammenschluss zwischen Fileservern). Die beiden untersten Ebenen der Fiber Channel Architektur werden mit den Ethernet 802.3 MAC und LLC Layers zum Gigabit Ethernet Standard formiert. Wie Fast Ethernet (100 MBit/s) unterstützt Gigabit Ethernet ebenfalls sowohl Half Duplex als auch Full Duplex Modi. Der Full Duplex Modus bedeutet somit eine Kapazität von 2 GBit/s auf einem Link.

Die 802.3z Gigabit Ethernet Spezifikationen definieren für unterschiedliche Typen von Medien (Glas, Kupfer) verschiedene Distanzen, die in nachfolgender Tabelle zusammengefasst sind.

Standard	**Kabelkategorie**	**Kabellänge** (geswitcht) [Minimum: 2 Meter]
1000BaseCX	Kupfer, Twisted Pair geschirmt (150 Ohm)	bis 25 Meter
1000BaseT	Kupfer, Kategorie 5 UTP (ungeschirmt 4 Paare)	bis 100 Meter
1000BaseSX	Glas, Multimode (50µm,62,5µm; 850nm)	220 bis 550 Meter
1000BaseLX	Glas, Multimode, Singlemode, (1300nm)	bis 550 Meter bis 5 Kilometer
1000BaseLH	Glas, Singlemode (9µm,10µm)	bis 10 Kilometer
1000BaseZX	Glas, Singlemode (9µm,10µm)	bis 90 Kilometer

Um beim Einsatz von Gigabit Verbindungen flexibel zu sein, sind die Gigabit Ethernet Einschübe in den Switches meistens nicht fix konfiguriert, sondern erlauben den Einsatz von so genannten GBICs. Diese Gigabit Ethernet Interface Converter werden einfach in das betreffende Gigabit Ethernet Device eingesteckt und erlauben somit je nach Bedarf den Einsatz des richtigen Connectors (1000BaseSX, LX). Diese Variante ist zudem noch kostengünstig.



Cisco 4912G – 12Port Gigabit Switch

Gigabit & ATM TUNET 2000

Zunächst waren im Zuge des Telekommunikationsprojektes die Umbauten im ATM Backbone nach wie vor nicht abgeschlossen. Das an der TU Wien eingesetzte und über alle Standorte verteilte Ericsson Telekommunikationssystem MD110 setzt ein synchron laufendes ATM Netz mit all seinen Knoten voraus. Durch die schrittweise installierten neuen ATM Module konnte die erforderliche Genauigkeit (Präzision) schließlich erfüllt werden.

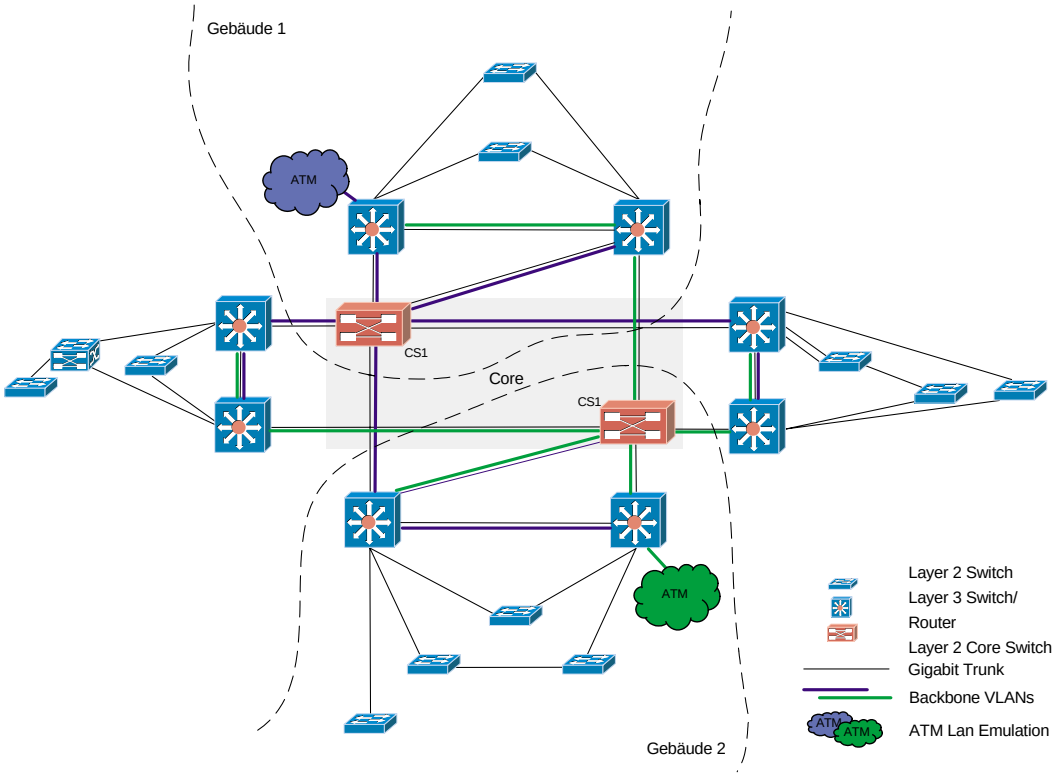
Alle Wartungen bzw. Erweiterungen standen im Zeichen, die hohe Verfügbarkeit des TUNET aufrecht zu erhalten. In einem so großen ATM LAN Emulation Netz wie dem an der TU Wien implementierten (übrigens eines der größten in Österreich neben anderen wie etwa bei Steyr Fahrzeugtechnik) ist dies freilich mit hohem Managementaufwand bei Konfigurationsänderungen verbunden.

Im Hintergrund der Umbauten zeichnete sich bereits seit einiger Zeit Gigabit Ethernet als neue Backbone-Technologie in der IT-Branche ab, die wesentlich billigere Technik (nämlich pures Ethernet) als die Overlay-Technik von ATM (Ethernet LAN Emulation über ATM) verwendet. Diese Technik verspricht eine kostengünstige Investition in Bandbreite (billigere Geräte, einfachere Technologie – kommt aus der bekannten und bewährten 10Base und 100Base Ethernet Entwicklungsschiene). Zudem bietet diese Technologie den Vorteil, einerseits im Backbone als auch im Distribution- bzw. Access-Bereich eingesetzt werden zu können. Weniger Komplexität bei der Konfiguration und damit weniger Fehleranfälligkeit schlagen sich in weniger Aufwand beim Troubleshooting nieder.

Implementierung von Gigabit im TUNET

Gigabit Ethernet Technologie soll einerseits im TUNET Backbone zur Verbindung der Gebäudekomplexe eingesetzt werden. Andererseits sollen Etagenverteiler im Gebäude optional (wenn die Notwendigkeit und Möglichkeit von der Infrastruktur her gegeben ist) redundant an zwei Backbone Switche mit Gigabit Ethernet Uplinks angebunden werden, um Ausfallssicherheit zu garantieren.

Die Gebäude selbst sollen auf alle Fälle redundant an die Core Switche angebunden werden, um hier größtmögliche Ausfallssicherheit zu bieten. Vor allem aber sollen dadurch geplante Eingriffe in das Backbone Netz im Rahmen der Netzwartung unproblematisch erfolgen



Implementierungsvarianten von Gigabit im TUNET Backbone und Distribution/Access-Bereich

können. Aus Sicht der Benutzer sollen dann Störungen durch Wartungsarbeiten weitgehend vermieden werden.

Im größten Vernetzungsprojekt im Jahr 1999, der Inbetriebnahme des neuen Gebäudes in der Favoritenstraße, wurden mit diesen beiden Varianten bereits erste Gehversuche unternommen. Allerdings sind die Etagenverteiler im gesamten Gebäudekomplex nicht in redundanter Weise angebunden. Die Erfahrungen waren trotzdem äußerst positiv, somit konnte der nächste Schritt in Richtung Gigabit Ethernet im gesamten Backbone getan werden.

Aufgrund der aktuellen ATM Backbone Struktur und der eingesetzten Switch-Modelle bot sich als Übergangslösung die Implementierung eines Gigabit Ethernet Ringes parallel zum ATM Netz an. Durch die Beschaffung weiterer Einschübe für die freien Steckplätze in den Backbone Switches und der Verwendung freier Glasfaser Infrastruktur konnte die Implementierung relativ rasch erfolgen und erste Erfahrungen konnten gesammelt werden. Die Ringtopologie ist jedoch nicht die Struktur, die einen optimalen Einsatz der Gigabit Ethernet Technologie garantiert.

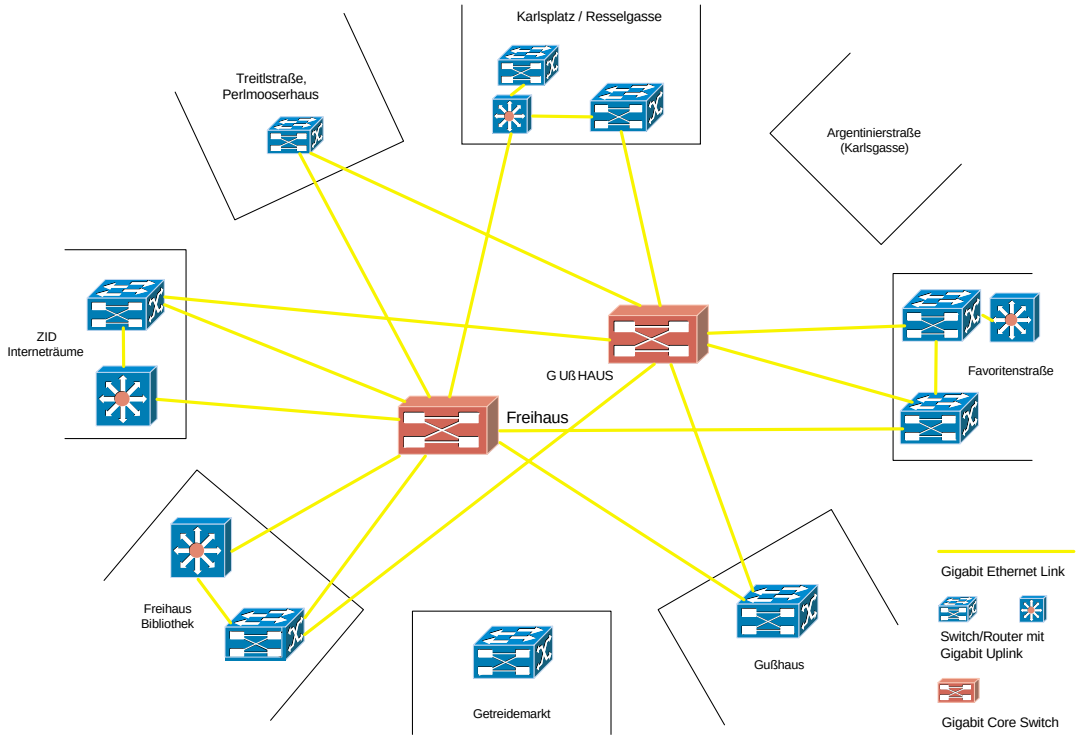
Erste Besprechungen zum Thema Gigabit Ethernet im TUNET Backbone fanden im Juni 2000 statt. Nach Klarheit über die ersten Schritte der Implementierung erfolgten im November 2000 letzte Teillieferungen von Modulen. Nach einem nochmaligen Feinschliff des Konzeptes wurde von uns mit dem Einbau der Gigabit Ethernet Komponenten noch im November 2000 begonnen. Schließlich erfolgte die „Inbetriebnahme“ von Gigabit Ethernet im TUNET Backbone im Dezember 2000. Leider funktionierte die in Zusammenarbeit mit dem Lieferanten ausgearbeitete Lösung nicht in gewünschter Weise und führte zu mehreren längeren Ausfällen des TUNET Backbones im Zeitraum Dezember 2000 bis Jänner 2001. Erst durch ein Abweichen vom ursprünglichen Implementierungskonzept und daraus resultierende Umkonfigurationen (nur je ein Übergang zwischen ATM LAN Emulation und Gigabit Ethernet für das betroffene Backbone LAN) gelang es, die Instabilitäten in den Griff zu bekommen und den gewohnten Servicelevel wieder herzustellen.

Gigabit im TUNET 2001

Von der bis jetzt zwischenzeitlich aus Kostengründen implementierten Ringtopologie soll auf eine Sterntopologie übergegangen werden. Die Realisierung soll noch im Sommer 2001 erfolgen.

Der Core Bereich (innerster Backbone Bereich) soll vorerst ausschließlich auf Layer 2 des ISO/OSI Sieben-Schichtenmodels realisiert werden. Wie in der Grafik angeführt, sollen die wichtigsten Gebäudekomplexe an die beiden redundant ausgeführten Core Switche angeschlossen werden.

Mit dem Einsatz von Gigabit Ethernet im TUNET Backbone wird auch die Reduktion der bisherigen Protokollvielfalt umgesetzt. Bisher konnte neben dem Hauptprotokoll TCP/IP je nach Standort auch eine teilweise Ausfallssicherheit anderer Protokolle wie Novell (IPX/SPX), AppleTalk und Decnet Phase IV implementiert werden. Die Redundanz im Gigabit Ethernet bedeutet IP-Only. Die vorgesehenen Geräte auf diesem Gebiet sind kombinierte Switch(Layer 2)/Router(Layer3) in einer fixen (nicht modularen) Konfiguration. Dies schlägt sich in deutlich niedrigeren Anschaffungskosten nieder. Redundanz für die anderen erwähnten Protokolle im Gigabit



TUNET Gigabit Backbone
Plan 2001

Bereich implementieren zu wollen, würde die Anschaffung hochmodularer und extrem teurer Geräte (im Millionen Schilling Bereich) bedeuten und wäre nicht vertretbar.

Hardware-Ausstattung des Backbones

Derzeit umfasst das Backbone 17 Core Switche, das sind 11 kombinierte ATM/Ethernet Switche (Cisco Catalyst 5500) sowie 5 reine ATM Switche (Cisco LS1010). 2 ATM Routeserver (Cisco 7507) sowie 5 Routeswitch-Module und einige kleinere Router erledigen das Routing der Datenpakete über das Backbone. Insgesamt verbinden derzeit sieben Gigabit Ethernet Verbindungen (Trunks) ausgewählte Backbone Switche untereinander.

Backbone & Telekommunikation

Die in den zentralen Bereichen Freihaus, Karlsplatz, Gußhaus und Favoritenstraße sowie an den Standorten Treitlstraße, Resselgasse, Karlsgasse und Argentinierstraße installierten ATM- bzw. kombinierten ATM-Ethernet-Switche ermöglichen die Integration von Daten und Sprache an der TU Wien. Immerhin beansprucht die Telekommunikation permanent ca. 70 MBit/s auf den einzelnen Backbone-Verbindungen. Das entspricht den 35 CES Verbindungen (CES = Circuit Emulation Service über ATM entspricht 2 MBit/s CBR Constant Bitrate Traffic), die quer durch das ATM Backbone gespannt sind.

Da zurzeit VOIP (Voice over IP = Telefonie über IP) an der TU Wien kein Thema ist und Gigabit Ethernet sonst keine Möglichkeit zur Integration von Sprache bietet, wird die ATM Technologie nicht so schnell aus dem TUNET verschwinden.

Backbone & Internet-Anbindung

Die geplante Gigabit Ethernet Topologie unterstützt in hohem Ausmaß die Möglichkeit, die redundante Internet-Anbindung der TU Wien über zwei unabhängige Serviceprovider wie bisher zu implementieren. Weiters ist sie geeignet, die Firewall für die TU Wien optimal zu integrieren.

Backbone & externe Standorte

Die ATM-Technologie wird auch dazu eingesetzt, um sowohl Daten- als auch Telefonverbindungen zu abgesetzten Standorten zu realisieren. Die bereits im Jahre 1999 realisierten 2 MBit/s ATM-Strecken zu Theresianumgasse, Aspanggründe und Atominstitut zeichnen sich durch hervorragende Stabilität aus. Die Kapazität der Anbindung reichte zwar im Jahr 2000 für alle Standorte aus, dennoch wird an eine Migration auf die Ethernet Technologie gedacht. Voraussetzung ist jedoch, entsprechende Glasfaserstrecken zu diesen Standorten zu errichten – eine nicht ganz billige Angelegenheit (dieses Problem besteht derzeit auch für den Standort Getreidemarkt).

Konklusion

ATM wird im TUNET erhalten bleiben. In der Telekommunikation führt kein Weg daran vorbei, aber auch in der Datenkommunikation ist ATM zur Realisierung externer Verbindungen nicht wegzudenken. Die Zukunft wird jedoch mit Sicherheit verstärkt Gigabit Ethernet bringen. Am Horizont schimmert aber schon der – wegen der eingesetzten Wellenlänge nicht sichtbare – 10 Gigabit Ethernet Lichtstrahl, siehe http://www.10gea.org/.

Sicherheit unter Linux

16 Schritte zu einem sicheren Linux-System

Walter Selos

Linux findet, vor allem als zuverlässiges Server-Betriebssystem, immer mehr Verbreitung. Die meisten dieser Linux-Installationen sind, insbesondere an der TU, ständig mit dem Internet verbunden. Aus diesem Grund ist es besonders wichtig, über die Sicherheit der Installation Überlegungen anzustellen.

Das Gerücht, Linux sei ein „Hacker-Betriebssystem“, geht einerseits auf die große Verbreitung und gute Dokumentation zurück, bewahrheitet sich bezüglich Netzwerksicherheit aber nur dann, wenn das entsprechende Fachwissen, das zum Betrieb eines Servers nötig wäre, fehlt (das gilt nicht nur für Linux). Da die Installation von Linux jetzt schon sehr bequem und menügeführt vonstatten geht, ist dafür ein solches Wissen nicht nötig, um zu einem lauffähigen Linux zu kommen, was sich im Betrieb allerdings rächen kann. Um sich dieses Wissen gezielter aneignen zu können, möchte ich in Form einer Checkliste die mir am wichtigsten erscheinenden Punkte zusammenfassen. So haben Sie einerseits eine grobe Konfigurations-Richtlinie zur Verfügung, andererseits können Sie Ihr Wissen gezielter vertiefen, wenn Sie beim Durchlesen der Checkliste auf Wissenslücken stoßen.

Es ist für ein komplexes Server-Betriebssystem, welches noch dazu in verschiedensten Distributionen und Versionen verfügbar ist, evident, dass diese Liste keinen Anspruch auf Vollständigkeit hat.

Checkliste

Tipp 1 Starten Sie nur die benötigten Services (Daemons)

a Start über Startupscripts

Die folgenden Daemons werden über Startupscripts gestartet, welche sich in einem für den jeweiligen Runlevel relevanten Verzeichnis befinden.

Wie weiß ich den Standard Runlevel ?

```
grep default /etc/inittab
```

Als Ergebnis sehen Sie eine Zeile, z.B:

```
id:3:initdefault:
```

Die 3 entspricht dem eingestellten Runlevel.

Wenn Sie z.B. den unten angegebenen `dhcp`-Server deaktivieren wollen, gehen Sie in das dem Runlevel entsprechende Verzeichnis z.B. `/etc/rc.d/rc3.d` (kann je nach Distribution variieren) und nennen Sie die Datei `S35dhcpd` auf `s35dhcpd` um.

Beim nächsten Reboot wird dieser Daemon nicht mehr gestartet.

Die Nummer hinter dem „S“ gibt die Startreihenfolge an und kann je nach Distribution variieren.

Einige Beispiele von Startupscripts:

```
S05apmd           You only need this for laptops
S10xntpd          Network time protocol
S11portmap        Required if you have any rpc services, such as NIS or NFS
S15sound          Saves sound cared settings
S15netfs          This is the nfs client, used for mounting filesystems from a nfs server
S20rstatd         Try to avoid running any r services,
S20rusersd              they provide too much information to remote users
S20rwhod
S20rwalld
S20bootparamd     Used for diskless clients, you probably don't need this vulnerable service
S25squid          Proxy server
S34yppasswdd      Required if you are a NIS server, this is an extremely vulnerable service
S35ypserv         Required if you are a NIS server, this is an extremely vulnerable service
S35dhcpd          Starts dhcp server daemon
S40atd            Used for the at service, similar to cron, by not required by the system
S45pcmcia         You only need this script for laptops
S50snmpd          SNMP daemon, can give remote users detailed information about your system
S55named          DNS server. If you are setting up DNS, upgrade to the latest version of BIND
                  http://www.isc.org/bind.html
S55routed         RIP, don't run this unless you REALLY need it
S60lpd            Printing services
S60mars-nwe       Netware file and print server
S60nfs            Use for NFS server, do not run unless you absolutely have to
S72amd            AutoMount daemon, used to mount remote file systems
S75gated          used to run other routing protocols, such as OSPF
S80sendmail       You can still send email if you turn this script off, you just will not
                  be able to receive or relay
S85httpd          Apache webserver, I recommend you upgrade to the latest version
                  http://www.apache.org/
S87ypbind         Required if you are a NIS client
S90xfs            X font server
S95innd           News server
S99linuxconf      Used to remotely configure Linux systems via browser,
                  every black-hat's dream :)
```

b Start über `inetd.conf` -> TCP-Wrapper einbauen

Beispiel: Hier ist z.B. nur ftp und swat (Samba Configuration Tool) erlaubt, ftp und swat werden über den TCP-Wrapper (`tcpd`) umgeleitet. Das System läuft auch noch, wenn man alles auskommentiert, also keine falsche Scheu, besser man dreht ein Service ab, das man nachher wieder aktivieren muss, als man wird Opfer einer Hackerattacke!

```
#
# inetd.conf      This file describes the services that will be available
#                 through the INETD TCP/IP super server.  To re-configure
#                 the running INETD process, edit this file, then send the
#                 INETD process a SIGHUP signal.
#
# Version:        @(#)/etc/inetd.conf 3.10 05/27/93
#
# Authors:        Original taken from BSD UNIX 4.3/TAHOE.
#                 Fred N. van Kempen, <waltje@uwalt.nl.mugnet.org>
#
# Modified for Debian Linux by Ian A. Murdock <imurdock@shell.portal.com>
#
# Modified for RHS Linux by Marc Ewing <marc@redhat.com>
#
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
#
# Echo, discard, daytime, and chargen are used primarily for testing.
#
# To re-read this file after changes, just do a 'killall -HUP inetd'
#
#echo stream       tcp          nowait       root           internal
#echo dgram        udp          wait         root           internal
#discard          stream       tcp          nowait         root           internal
#discard          dgram        udp          wait           root           internal
#daytime          stream       tcp          nowait         root           internal
#daytime          dgram        udp          wait           root           internal
#chargen          stream       tcp          nowait         root           internal
#chargen          dgram        udp          wait           root           internal
#time stream       tcp          nowait       root           internal
#time dgram        udp          wait         root           internal
#
# These are standard services.
#

ftp               stream       tcp          nowait         root           /usr/sbin/tcpd     in.ftpd -l -a

#telnet           stream       tcp          nowait         root           /usr/sbin/tcpd     in.telnetd
#
# Shell, login, exec, comsat and talk are BSD protocols.
#
#shell            stream       tcp          nowait         root           /usr/sbin/tcpd     in.rshd
#login            stream       tcp          nowait         root           /usr/sbin/tcpd     in.rlogind
#exec             stream       tcp          nowait         root           /usr/sbin/tcpd     in.rexecd
#comsat           dgram        udp          wait           root           /usr/sbin/tcpd     in.comsat
#talk             dgram        udp          wait           nobody.tty     /usr/sbin/tcpd     in.talkd
#ntalk            dgram        udp          wait           nobody.tty     /usr/sbin/tcpd     in.ntalkd
#dtalk            stream       tcp          wait           nobody.tty     /usr/sbin/tcpd     in.dtalkd
#
# Pop and imap mail services et al
#
```

```
#pop-2             stream       tcp          nowait         root           /usr/sbin/tcpd     ipop2d
#pop-3             stream       tcp          nowait         root           /usr/sbin/tcpd     ipop3d
#imap              stream       tcp          nowait         root           /usr/sbin/tcpd     imapd
#
# The Internet UUCP service.
#
#uucp              stream       tcp          nowait         uucp           /usr/sbin/tcpd     /usr/lib/uucp/uucico -l
#
# Tftp service is provided primarily for booting.  Most sites
# run this only on machines acting as "boot servers." Do not uncomment
# this unless you *need* it.
#
#tftp              dgram        udp          wait           root           /usr/sbin/tcpd     in.tftpd
#bootps            dgram        udp          wait           root           /usr/sbin/tcpd     bootpd
#
# Finger, systat and netstat give out user information which may be
# valuable to potential "system crackers."  Many sites choose to disable
# some or all of these services to improve security.
#
#finger            stream       tcp          nowait         nobody         /usr/sbin/tcpd     in.fingerd
#cfinger           stream       tcp          nowait         root           /usr/sbin/tcpd     in.cfingerd
#systat            stream       tcp          nowait         guest          /usr/sbin/tcpd     /bin/ps -auwwx
#netstat           stream       tcp          nowait         guest          /usr/sbin/tcpd     /bin/netstat -f inet
#
# Authentication
#
#auth              stream       tcp          wait           root           /usr/sbin/in.identd in.identd -e -o
#
# End of inetd.conf
#linuxconf         stream       tcp          wait           root /bin/linuxconf linuxconf –http

swat               stream       tcp          nowait.400     root /usr/sbin/tcpd /usr/sbin/swat swat
```

Nicht vergessen:

Nach Editieren `inetd.conf`: `killall -HUP inetd` (`inetd` liest das `conf`-File neu ein!)

Achtung:

Neue Versionen haben oft statt des `inetd` den **`xinetd`** laufen, dann ist die Konfigurationsdatei meist in mehrere, für jedes Service eine, aufgeteilt, die sich in einem eigenen Verzeichnis, meist `/etc/xinetd.conf` befinden. Dieser neue `xinetd` hat die TCP-Wrapper-Funktion bereits eingebaut und ist flexibler zu konfigurieren. Die Syntax ist etwas anders, siehe „`man xinetd`“ und „`man xinetd.conf`“.

Tipp 2 Zugriffsrechte über TCP-Wrapper einschränken

Der TCP-Wrapper wird über 2 `config`-Dateien konfiguriert. Außerdem müssen die Einträge in `/etc/inetd.conf` modifiziert werden. Z.B.:

```
/etc/hosts.deny:
ALL: ALL
```

```
/etc/hosts.allow:
ALL EXCEPT swat: .mysubnet.tuwien.ac.at
swat: localhost mycomputer.mysubnet.tuwien.ac.at
```

Funktion testen !

Das heißt: alle Dienste, die über `tcpd` gestartet werden, sind für „`mysubnet` ...“ erlaubt, jedoch `swat` nur für die eine Maschine „`mycomputer.mysubnet`“ und für die lokale Maschine.

Siehe auch: `man 5 hosts_access`

Auch den Portmapper-Zugriff kann man bei Linux über `host.allow/deny` konfigurieren.

Achten Sie natürlich auch auf **spezielle Services**, die Sie selbst gestartet haben: z.B. appletalk, mars-nwe (Novell-Server) etc.

Tipp 3 Shadow Password verwenden, auf sinnvolle Passwörter achten

Bei RedHat: Wenn Sie die Option „shadow-passwords“ beim Installieren vergessen haben, hilft: `pwconv`

Tipp 4 Auf File Permissions achten beim Einrichten von Usern, Gruppen

Da kann man nicht viel dazu sagen, hängt von der Struktur ab, die man abbilden will.
Siehe: `man chmod, man chgrp, man chown`

Bei RedHat: gute graphische Konfigurationshilfe: `linuxconf`
(damit kann man relativ leicht User und Gruppen verwalten)

Tipp 5 Womöglich nur `ssh` verwenden (oder onetime-passwd)

Um sich von Windows oder Mac einzuloggen: Teraterm bzw. nifty-telnet
Teraterm (für Windows): http://hp.vector.co.jp/authors/VA002416/teraterm.html
Nifty-Telnet (für Mac): http://www.lysator.liu.se/~jonasw/freeware/niftyssh/

Tipp 6 Wenn User für Samba oder pop u.dgl. eingerichtet werden:

keine Shell (`/bin/false` im `/etc/passwd`) und eigenes Passwort, welches in keinem Shell-Account verwendet wird.

Auch für ftp-User, dann muss man aber `/bin/false` in `/etc/shells` eintragen.

Sollte sich dann jemand das Passwort mittels eines Sniffers aneignen, kann er zwar Dateien transferieren, jedoch keine Kommandos absetzen bzw. Programme starten.

Tipp 7 Achten Sie auf offene X-Verbindungen

(also remote X-Server: X-Terminal, andere Unix/Linux-Maschine, Windows mit X-Server, z. B. HCL-Exceed)

Wenn X-Windows-Sessions nicht über `ssh` getunnelt werden, kann
a.) im Netz mitgesnifft werden,
b.) eine Verbindung zum X-Server von anderswo hergestellt und jeder Tastendruck abgefragt werden.

Punkt b.) ist nur möglich, wenn der X-Server für alle zugänglich ist.
Mit dem Befehl `xhost` Einträge überprüfen/ändern !
Zusammengefasst: Vorsicht mit X11 übers Netz !

Tipp 8 Samba Server absichern

- Für Samba: (Fileserver für Windows-Maschinen)
- Passwort-Encryption verwenden (mit Win98 oder NT SP ≥ 4)
- `hosts_allow` Liste in den Shares verwenden
- wenn SWAT verwendet wird, nur so verwenden, dass keine Sniffingmöglichkeit vorhanden, womöglich nur für localhost erlauben (`/etc/hosts.allow`).

Tipp 9 Achten auf Netzwerktopologie: große Collisiondomain ?

Sind andere schwach gesicherte Maschinen im Netz ? -> Gefahr durch potentielle Passwort-Sniffer !

Abhilfe: Bessere Sicherung der Maschinen durch strukturierte Verkabelung, Switches, Bridges etc.

Tipp 10 Eventuell zusätzliche Filterung mit Packetfilter (`ipchains`)

Logging für die Rules aktivieren ? (option `-l`)
Siehe: http://gd.tuwien.ac.at/opsys/linux/LDP/HOWTO/IPCHAINS-HOWTO.html

Verwenden Sie `ipchains` und andere Firewall-Lösungen nur, wenn Sie wirklich wissen, was Sie tun, und testen Sie die Konfiguration auf ihre gewünschte Funktion, damit Sie sicher gehen, dass hier nicht nur Sicherheit vorgetäuscht wird.
Im Rahmen der Wartungsabkommen können Sie hier Hilfe vom ZID beanspruchen (sts.tuwien.ac.at/pss/).

Tipp 11 Eventuell einfache Firewall-Lösungen

mit packetfilter in forward-chain, Masquerading,
siehe http://linux.tuwien.ac.at/firewall.html

Tipp 12 Bei Kernel ≥ 2.2.x -> Spoofing Protection möglich

Spoofing Protection verhindert das Vortäuschen falscher IP-Adressen.

```
echo 1 > /proc/sys/net/ipv4/conf/ethx/rp_filter
```

Tipp 13 Achten Sie auf Veröffentlichungen von Securitybugs, Patches ...

Siehe Homepages der diversen Distributionen.

Tipp 14 Erkennen von Hackerattacken I

evtl. cronscripts, welche potentielle Attacken erkennen, wie z.B.: `logcheck` ...

Achten Sie in den Logfiles auf „`connect from unknown`“: könnte Portscanner-Aktivitäten anzeigen.

Tipp 15 Erkennen von Hackerattacken II

Kopieren Sie Programme, die Sie zum Aufspüren von Hackern brauchen, wie `ps`, `ls`, `ifconfig`, `top`, `find`, `grep`, `cksum`, `md5sum` usw., unter einem anderen Namen auf ein anderes Verzeichnis.

Machen Sie nach der Erstinstallation von diesen (oder vom ganzen `/bin/* /sbin/*`) ein `cksum` oder `md5sum` und notieren Sie sich die Checksummen (ausdrucken, auf anderer Maschine speichern).
z.B:

```
md5sum /bin/* >md5_datei
md5sum /sbin/* >>md5_datei
```

Heben Sie jetzt die `md5_datei` gut auf (z.B. auf einem anderen Computer).

Wenn Sie den Verdacht hegen, dass ein Hacker auf Ihrer Maschine sich versteckt hält, machen Sie den oben beschriebenen Vorgang nochmals in eine andere Datei und vergleichen Sie die beiden Dateien mit „`diff`“. Wenn Unterschiede gemeldet werden, wurde etwas verändert (könnte natürlich auch von Ihnen durch irgendwelche Updates verursacht sein, daher nach einem Update den Vorgang wiederholen.)

So können Sie feststellen, ob ein Eindringling einige Ihrer wichtigen Systemprogramme ausgetauscht hat, um Spuren zu verschleiern.

Tipp 16 Allgemeine Hinweise

Wenn Sie einfach eine Standardinstallation durchführen, sollten Sie daran denken, dass, je nach Distribution, der Bequemlichkeit halber viele Komponenten und Dienste mitinstalliert werden, die Sie meist nicht brauchen.

Informieren Sie sich bitte, was das für Komponenten sind, die da laufen.

Machen Sie einen Portscan (dieser wird auf Wunsch vom ZID für Sie durchgeführt: E-Mail an security@tuwien.ac.at mit dem Betreff „Systemcheck“.)

Tipp 1 soll Ihnen dabei als Anhaltspunkt und Hilfe dienen, allerdings ohne einen Anspruch auf Vollständigkeit.

Vorsicht bei fertig installierten Firmenlösungen: Erfahrungsgemäß sind die Leute, die das System installieren, nicht mit so großen Netzwerken, wie auf der TU vorhanden, konfrontiert. Daher fehlt auch oft eine gewisse Erfahrung; wieder laufen einige nicht benötige Dienste.

Weitere Informationen können Sie durch die „HOWTOs“ des LDP (Linux Documentation Project) bekommen, siehe: http://gd.tuwien.ac.at/opsys/Linux/LDP/.

Sollte Ihnen das alles zu viel sein, können Sie für Ihren Server auch einen Wartungsvertrag bei uns (Zentraler Informatikdienst, Abteilung Standardsoftware) abschließen, siehe:

`sts.tuwien.ac.at/pss/`

Systemunterstützung der Arbeitsplatzrechner und Server

Statistiken und Analysen

Albert Blauensteiner

Der folgende Artikel gibt einen Überblick über den Verlauf der Systemunterstützung seit Einführung des Services Ende 1999 bis zum Ende des ersten Quartals 2001. Die Verteilung der Unterstützung nach Fakultäten, Plattformen und Aufwand wird kurz analysiert.

Einleitung

Ein Aufgabengebiet der Abt. Standardsoftware liegt in der Betreuung und Unterstützung der Server und Arbeitsplatzrechner an den einzelnen Instituten der TU Wien. Diese Leistungen werden auf allen gängigen Plattformen, wie den Unix-Systemen von SGI, HP, Compaq, IBM, SUN sowie LINUX und im PC Bereich Windows, WindowsNT, W2K sowie auch für Mac erbracht.

Die Einsatzgebiete reichen dabei von der Analyse bei Neuanschaffungen, über die Unterstützung und Beratung in Fehlerfällen und bei Ausbauplänen bis hin zu Fragen von Betriebs- und Sicherheitsaspekten sowie der Planung des Einsatzes von Systemkomponenten und der Anwendungssoftware. Nicht zu vergessen sind dabei die Fragen, die im Zusammenhang mit der lokalen und überregionalen Vernetzung auftreten.

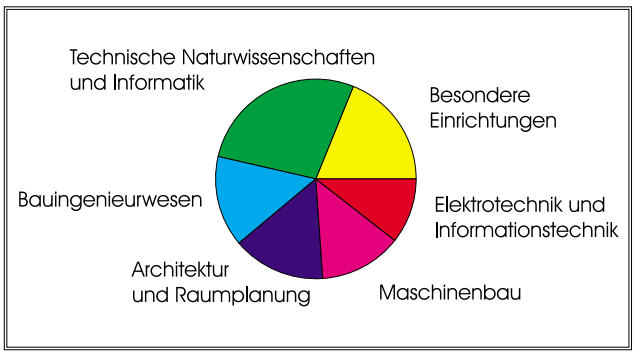
Seit Jahren wird von der Abteilung Standardsoftware diese Systemunterstützung, der so genannte Plattformsupport, für alle UNIX Systeme sowie VMS angeboten. Dafür waren bisher speziell geschulte Mitarbeiter auch vor Ort im Einsatz. Seit letztem Jahr trägt die Abteilung Standardsoftware mit einer neuen Form der Systemunterstützung den veränderten Gegebenheiten in der Rechnerlandschaft Rechnung.

Seit Beginn des Jahres 2000 besteht die Möglichkeit für PCs, Workstations und Server an der Technischen Universität Wartungsvereinbarungen mit der Abteilung Standardsoftware des Zentralen Informatikdienstes abzuschließen. Diese Wartungsvereinbarungen bieten besondere Leistungen der Systempflege für die spezifizierten Rechnersysteme an, und zwar in zwei grundsätzlichen Kategorien: Einerseits eine Systempflege, die auch einen Einsatz vor Ort umfasst, andererseits eine Fernunterstützung, die nur über Netzwerk und Telefon erfolgt. In beiden Kategorien wird zwischen „normalen“ Arbeitsplatzrechnern und Serversystemen unterschieden. Bei den Arbeitsplatzrechnern wiederum gibt es noch eine Unterscheidung zwischen wartungsfreundlichen und wartungsintensiveren Arbeitsplätzen.

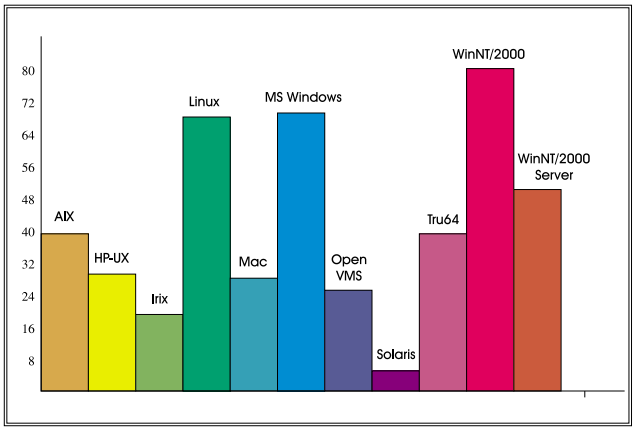
Wenn ein derartiges Rechnersystem mit einer entsprechenden Wartungsvereinbarung ausgestattet ist, so können für dieses System Anforderungen zur Hilfestellung über ein dafür errichtetes Call Center im Zentralen Informatikdienst in Anspruch genommen werden. Es wird eine entsprechende Antwortzeit garantiert und die Anfrage entweder mit Mitarbeitern des Zentralen Informatikdienstes oder mit Mitarbeitern von externen Firmen einer Untersuchung bzw. einer Lösung zugeführt.

Statistisches

Bis zum Ende des ersten Quartals 2001 wurden 455 Unterstützungsfälle gezählt, die sich, wie in den beiden folgenden Abbildungen dargestellt, auf die unterstützten Plattformen sowie die unterstützten Fakultäten verteilen.



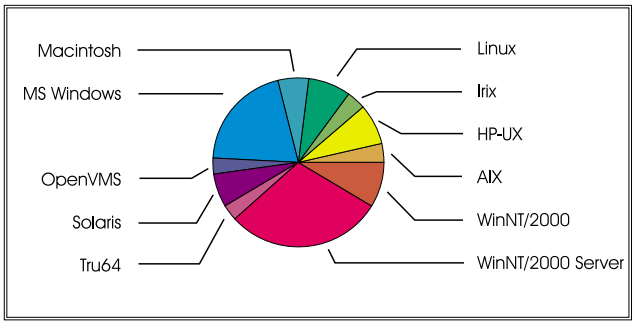
Unterstützungsfälle nach Fakultäten



Unterstützungsfälle nach Plattformen

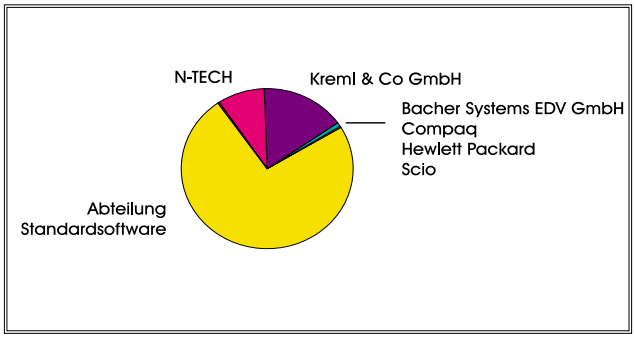
Die meisten Unterstützungsfälle wurden für Windows NT gezählt, dann für Win 9x sowie Linux, die wenigsten für Solaris. Es gab mit dem Stichtag insgesamt 345 abgeschlossene Verträge, davon 270 Systempflegeverträge und 75 Fernunterstützungsverträge. Die meisten Verträge, nämlich 132, wurden für Windows NT abgeschlossen, die wenigsten für die Plattform Open VMS, nämlich 10.

Die niedrige Unterstützungsquote bei Solaris ist vermutlich darauf zurückzuführen, dass zuletzt diese Plattform vom ZID nach dem Abgang des zuständigen Mitarbeiters und der Nichtnachbesetzung nicht mehr unterstützt werden konnte und dadurch eine Servicelücke entstand.



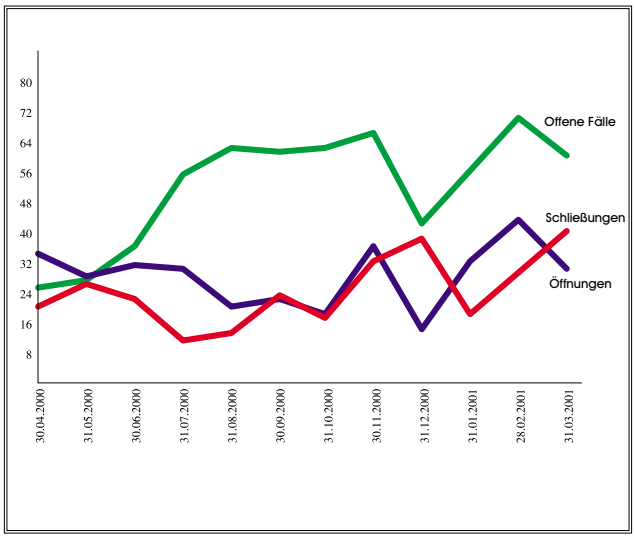
Abgeschlossene Verträge nach Plattformen

Es zeigt sich, dass die Verträge zur Plattformunterstützung nach wie vor und zwar im verstärktem Maße zunehmen, was vermutlich auf den nun einsetzenden Bekanntheitsgrad, die Budgetsituation an den Instituten und nicht zuletzt auf den tatsächlichen Bedarf zurückgehen dürfte. Über 1300 Stunden wurden dabei für die Unterstützungsfälle aufgewendet, die meisten, nämlich 363, für die Fakultät für Technische Naturwissenschaften und Informatik, die wenigsten, nämlich 136, für die Fakultät für Elektrotechnik und Informationstechnik. Bezüglich der Plattformen ging der größte Aufwand, nämlich 216 Stunden, in den Bereich HP-UX, der geringste an Solaris. Interessant ist dabei vielleicht die Tatsache, dass etwa drei Viertel der erbrachten Unterstützungsstunden durch die Abteilung Standardsoftware selbst erbracht wurde, der Rest durch externe Firmen, wobei nur zwei Firmen wesentlichen Anteil am restlichen Viertel haben.

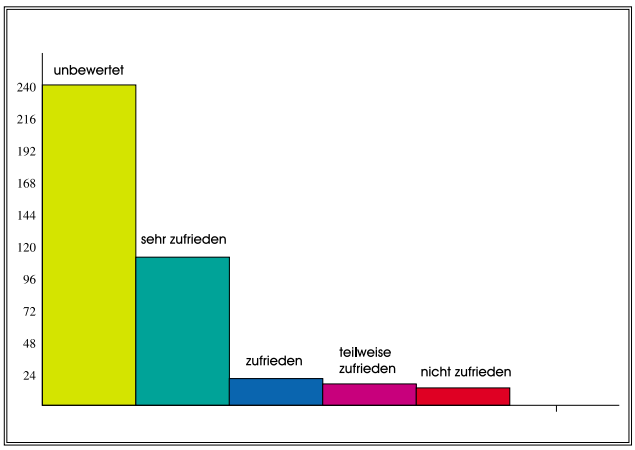


Erbrachte Unterstützungsstunden

Bei der monatlichen Bilanz der Öffnungen und Schließungen der Bearbeitungsfälle zeigt sich ein etwa gleichförmiges Bild. Die Gesamtzahl der offenen Fälle bleibt nun etwa konstant bei etwa 60.



Status Unterstützungsfälle



Qualitätsbewertung

Ein Wort noch zur Qualität der bereits beendeten Leistungen: Von 400 Fällen wurden 240 nicht bewertet, bei 111 Fällen waren die Kunden „sehr zufrieden“ (Bestnote), bei 13 Fällen äußerten sie sich als „nicht zufrieden“.

Es gibt einen eindeutigen Qualitätsunterschied zwischen den Eigenleistungen und den Fremdleistungen. Die zukünftige Konzeption und Weiterentwicklung des Plattformservices wird gerade in Hinblick auf die externen Ressourcen und die externe Qualität überprüft und überarbeitet. Im Großen und Ganzen läuft aber das Service sowohl logistisch als auch technisch zufriedenstellend und kann so, falls keine besonderen Einschränkungen in den Ressourcen bzw. signifikante Zunahmen in den Verträgen bzw. in den Unterstützungsanforderungen stattfinden, prinzipiell in der bisher erbrachten Form weiter geführt werden.

Erfahrungen mit der Systemunterstützung

Rudolf Sedlaczek

Aus über einem Jahr Erfahrungen mit der neuen Systemunterstützung lässt sich schon ein statistisch signifikanter Überblick über die Stärken und auch verbesserungswürdigen Aspekte ziehen, die im nachfolgenden Artikel detailliert behandelt werden.

Überblick

In den Web-Seiten der Systemunterstützung

sts.tuwien.ac.at/pss/

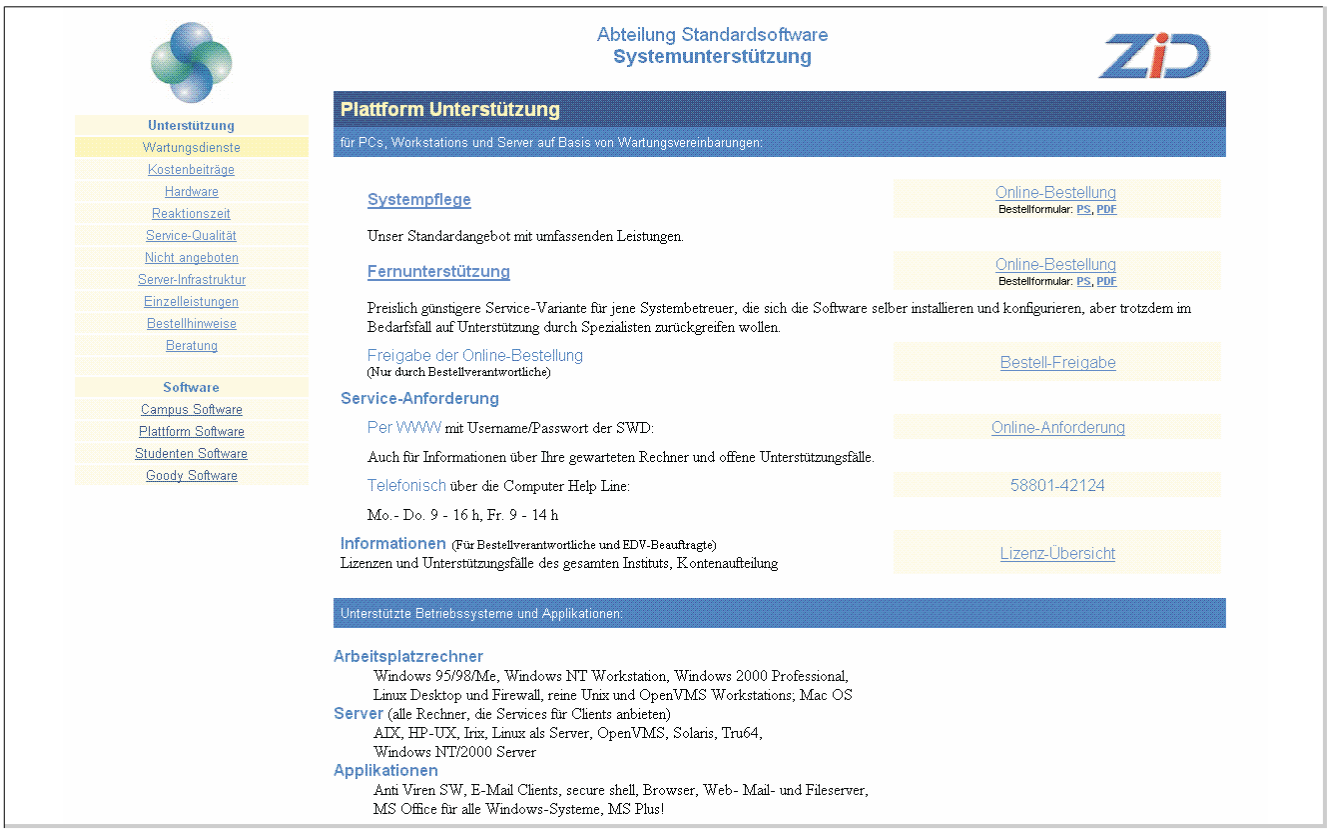
sind die Leistungen, Kosten und Randbedingungen der angebotenen Dienstleistungen spezifiziert, weshalb hier nicht nochmals darauf eingegangen wird.

Eine erste Anpassung der Dienstleistungen wurde schon Mitte vorigen Jahres durchgeführt. Auf vielfachen Benutzerwunsch wurde der Dienstleistungsumfang ohne Kostensteigerung ausgedehnt und umfasst nun auch die Installation und Unterstützung für MS Office auf den Windows Plattformen.

Konzeptionelles

Das System der Unterstützung basiert auf Wartungsvereinbarungen für einzelne Rechner, nicht pauschal für alle Rechner einer Organisationseinheit. Das minimiert den Administrationsaufwand gegenüber einer Verrechnung von Einzelleistungen und erleichtert die Abschätzung des Unterstützungsbedarfs. Daraus ergibt sich die Notwendigkeit, alle Rechner identifizieren zu können. Wurden früher nur die Rechner der proprietären Server- und Workstation-Familien in der Abteilungs-Datenbank aufgenommen und verwaltet, so werden in der neuen Systemunterstützung auch alle Rechner mit Wartungsabkommen eingetragen. Zur Identifikation dient primär der (eindeutige) TCP/IP-Hostname, da bis auf einzelne Ausnahmen alle Rechner per LAN am TUNET angeschlossen sind. Als weitere Identifikationsmöglichkeit wird optional auch die Ethernet-Adresse in der Datenbank gespeichert. Weitere wesentliche Daten eines Rechners sind die Plattform, der Einsatztyp (Server oder Arbeitsplatz), der Rechner-Typ (z. B. Pentium PC, Sun Ultra 60, ...), der Eigentümer (Institut) und die Kontaktperson. Erst für bekannte bzw. durch die Kontaktperson online selbst registrierbare Rechner kann dann schriftlich oder online ein Wartungsabkommen für **Systempflege** oder **Fernunterstützung** bestellt werden.

Alle diese Daten werden entweder bei der Online-Registrierung durch die Kontaktperson oder bei schriftlicher Anmeldung durch die Mitarbeiter der Gruppe Systemun-



sts.tuwien.ac.at/pss/

terstützung eingetragen. Ist die Kontaktperson noch nicht durch Software-Bestellungen oder als Server-Betreuer in der Datenbank bekannt und autorisiert, kann die Wartungsvereinbarung nur schriftlich erfolgen. Dann wird diese Person auch in die Datenbank aufgenommen und erhält einen Usernamen und ein generiertes Passwort.

Diese Daten bilden die notwendige Grundlage für die Abwicklung und Verwaltung der einzelnen Unterstützungsanforderungen, die jeweils bei den Abkommen in der Abteilungs-Datenbank gespeichert werden. Jeder Unterstützungsfall wird nach erfolgter technischer Bearbeitung dann auch noch in der Datenbank geschlossen und ein Arbeitsbericht und die aufgewendete Zeit werden eingetragen.

Die Leistungen werden durch die Mitarbeiter der Gruppe Systemunterstützung und/oder durch externe Firmen erbracht, mit denen entsprechende Serviceverträge abgeschlossen wurden. In mindestens einmal jährlich stattfindenden Besprechungen mit den verantwortlichen Firmenvertretern werden diese Vereinbarungen und die Erfahrungen mit der Firma einem Review unterzogen und bei Bedarf angepasst. Im Jahre 2000 bestanden Verträge mit 9 externen Firmen.

Zur Qualitätssicherung werden besonders die negativ bewerteten Fälle, aber auch das Feedback und Beschwerden über die Qualität externer Firmen und interner Betreuung aufgearbeitet. Hier ergibt sich ein sehr differenziertes Bild, nicht nur im Vergleich zwischen den verschiedenen Dienstleistern, sondern auch im Vergleich der Abwicklung verschiedener Calls bei einzelnen Firmen. Oft werden Calls zur vollen Zufriedenheit der Kunden abgewickelt, manchmal werden aber von den gleichen Bearbeitern Calls wieder nicht entsprechend behandelt, versprochene Rückrufe und Kontaktaufnahmen bleiben aus. Ein eher negatives Gesamtbild bietet das nur für telefonische Unterstützung eingesetzte Call-Center der Fa. SCIO. Hier reichten die Beurteilungen von „völlig inkompetent“ über „bemüht, aber trotzdem unfähig, das Problem zu lösen“ bis zur Zufriedenheit mit der Lösungskompetenz. Dem muss man fairerweise zugute halten, dass die nur telefonische Unterstützung bei Windows oft wirklich nicht leicht möglich ist und manche Probleme oder Wünsche prinzipiell nicht lösbar oder erfüllbar sind (ohne das Betriebssystem umzuschreiben).

Plattform-Differenzierung

Die Systemunterstützung lässt sich in drei unterschiedlich zu handhabende Bereiche gliedern.

1. **Traditionelle proprietäre (Unix-)Plattformen**
   Hierzu sind auch OpenVMS und Macintosh zu rechnen. Bei diesen Systemen gibt es (bis auf die Solaris-Plattform) kompetente Betreuungsspezialisten in der Abteilung, für die zur Unterstützung und Eskalation von Calls Support-Verträge mit den Herstellerfirmen abgeschlossen wurden (mit IBM für AIX, mit Hewlett Packard für HP-UX, mit Unisys für IRIX, mit Bacher Systems für Solaris und mit Compaq für OpenVMS und Tru64). Hier werden die meisten Calls durch interne Bearbeiter abgehandelt und gelöst.
   Interessant ist hierbei, dass für die zahlenmäßig stärks-

te Unix-Plattform Solaris relativ zur Gesamtzahl die wenigsten Wartungsabkommen abgeschlossen wurden (19%). Dies kann auf die fehlende interne Betreuungskapazität zurückgeführt werden. Die relativ meisten Wartungsverträge gibt es bei HP-UX und OpenVMS (je 38%), gefolgt von AIX (29%), Irix (28%) und Tru64 (24%).

2. **Linux**
   Dieser Bereich ist im Gegensatz zum proprietären Unix-Bereich sehr dynamisch wachsend, vor allem im Einsatzgebiet als Server für vielfältigste Dienste. Hier werden die Unterstützungsleistungen hauptsächlich durch kompetente interne Spezialisten erbracht und das Unterstützungsteam durch freiwerdende Kapazitäten aus dem zurückgehenden proprietären Unix-Bereich verstärkt.
   Die Anzahl der Linux-Server ist nicht bekannt, es gibt aber mit 28 Wartungsabkommen fast so viele wie bei Windows NT/2000 Server.

3. **Windows**
   Die hier zu unterstützenden Plattformen reichen von den relativ einfachen (aber fehleranfälligen) Windows 95/98/Me Systemen über die komplexeren, aber stabileren Windows NT Workstations und Windows 2000 Professional bis zu komplexen Serversystemen mit Windows NT Server und Windows 2000 Server, dessen Mächtigkeit und Komplexität die von Windows NT Server noch um ein Mehrfaches übersteigt.
   Der gesamte Windows-Bereich ist mit 204 Wartungsabkommen der zahlenmäßig Größte und auch am schwierigsten zu behandeln. Das liegt an der breiten Streuung der Aufgaben, der eingesetzten Hardware verschiedenster Firmen und Qualitäten und des Know-hows der Systembetreuer (wo es solche im eigentlichen Sinn des Wortes überhaupt gibt). Hier gibt es derzeit mehrere externe Unterstützer und aus auch historischen Personalgründen nur relativ geringe interne Betreuungskräfte.
   Besonders in diesem Bereich kommt der Funktion des Call-Dispatchers eine kritische Aufgabe zu, indem er die einlangenden Fälle zu klassifizieren hat und nach den Kriterien der bestmöglichen Unterstützung zu den geringst möglichen Gesamtkosten einem internen oder externen Bearbeiter zuweisen muss. Einfache Aufgaben (Basisversorgung wie Software-Installation, Updates, Drucker- und Netzwerkkonfiguration, ...) werden in diesem System von anderen Firmen bzw. Mitarbeitern abgewickelt als komplexe Problemstellungen eines oftmals erfahrenen Systembetreuers, den man nicht zu jemandem mit weniger Know-how, als er selber hat, weiterleiten sollte.
   Bei den Server-Versionen von Windows NT und Windows 2000 besteht nur für 14% der 203 registrierten Serversysteme ein Wartungsabkommen. Bei den anderen unterstützten Plattformen ist die Anzahl der Rechner nicht erfasst, weshalb man keine vergleichbaren Prozentzahlen angeben kann. Bezogen auf die Anzahl der lizenzierten Betriebssysteme kann nur eine Obergrenze für den tatsächlichen Anteil an Wartungsabkommen genannt werden: 6% bei Windows 95/98/Me und 12% bei Windows NT/2000.

Ausblick

Aus den Erfahrungen von über einem Jahr mit der neuen beitragsorientierten Systemunterstützung und eingehender interner Diskussion darüber werden folgende Maßnahmen für die weitere Verbesserung der Unterstützungsqualität gesetzt:

1. Reduzierung der Anzahl der externen Firmen auf das nötigste Minimum. Jede weitere Firma bewirkt zusätzlichen Administrations- und Koordinationsaufwand. In der ersten Phase wurden bewusst mehrere Firmen auch für eine Plattform ausgewählt, um Erfahrungen mit der Qualität der versprochenen Dienstleistungen in der Praxis zu sammeln.
2. Interne Betreuungskapazitäten und Know-how werden verstärkt. Ein Vergleich der Problemlösungskompetenz der internen und externen Unterstützer auf Grund von Feedback, Beschwerden und Fallbewertungen fällt positiv zugunsten der internen Betreuer aus. Besonders bei den proprietären UNIX Plattformen und Linux wird das Know-how sehr geschätzt.
3. Für die Windows-Plattformen wird ein angepasstes differenziertes Unterstützungsportfolio angeboten:
   - Telefon-Support über ein Call Center, das in Zukunft vermehrt durch interne Fachkräfte besetzt werden wird.
   - Breitenwirksamer Basis Support an den Instituten durch 1 bis max. 2 Firmen, wobei sich die Fa. Kreml als zuverlässiger Partner bisher am besten bewährt hat.
   - Abdeckung von Spezialfragen und komplexen Problemen durch interne und komplementär durch unvermeidbar teure, aber ihren Preis werte externe Spezialisten. Hier wurden mit der Fa. HP gute Erfahrungen gemacht.

Bestellungen von Wartungsvereinbarungen und Unterstützungsanforderungen für gewartete Systeme online rund um die Uhr unter

sts.tuwien.ac.at/pss/

Telefonische Computer Help Line: 42124
Mo-Do 9-16 Uhr, Fr 9-14 Uhr

www.tuwien.ac.at

Werner F. Sommer
Abteilung für Öffentlichkeitsarbeit und Information der Zentralen Verwaltung der TU Wien
wsommer@zv.tuwien.ac.at

„Der 26.2. wird an der TU als geschmacklosester Tag in die Geschichtsbücher eingehen. Dieses Webdesign ist eine Schande für eine technische Hochschule unseren Niveaus."
Was war geschehen? An jenem Tag wurde das Aussehen von www.tuwien.ac.at demonstrativ geändert. Die Reaktionen (www.tuwien.ac.at/redesign) – positiv wie negativ – waren heftig. Allein: Es handelt sich NICHT um die neue Webpräsenz der TU. Die lässt noch auf sich warten.

Nachdem die „Briefmarken" also Ende Februar ausgedient hatten, gingen die Emotionen hoch. Die zahlreichen „zweckdienlichen Hinweise" ließen die Hoffnung aufkeimen, dass beim Ende Jänner ausgeschriebenen Wettbewerb (www.tuwien.ac.at/pr/wettbewerb/) zahlreiche Vorschläge, wie es besser zu machen wäre, über uns hereinbrechen würden. Nun ist der Wettbewerb vorbei, und die quantitative Ausbeute eher bescheiden.

Mag sein, dass die 100.000 Schilling zu wenig Anreiz darstellen. Mag sein, dass Unzufriedenheit nicht zwangsläufig zum Aufzeigen von Alternativen führt. Sei es, wie es sei. Wir werden versuchen, das gesteckte Ziel trotzdem zu erreichen: Nämlich im Herbst einen neuen Web-Auftritt der TU präsentieren zu können.

Was bisher geschah

In Zeiten, da die „Killer-Websites" wie Schwammerln aus dem Boden schießen, regte sich letztes Jahr an zentralen Stellen (nämlich dem Zentralen Informatikdienst und der Zentralen Verwaltung) zusehends Unbehagen hinsichtlich der Webpräsenz der TU. Zwar war die TU schon früh online, seitdem wucherte die Site aber eher, anstatt planvoll zu wachsen. Selbst die vehementesten AnhängerInnen der Philatelie werden nicht bestreiten, dass Inhalt, Design und Technik der TU-Site nicht zeitgemäß sind. Einige Problempunkte und Optionen:

Inhalt

Strukturell orientiert sich die TU-Site an der Aufbauorganisation. Im Vordergrund stehen Informationen über Institute, Einrichtungen, Personen usw. Noch nicht durchgesetzt hat sich die Orientierung an den Bedürfnissen unserer „KundInnen". Künftig sollte die Fragestellung „Was können wir für wen tun?" aus dem Schatten der wenig nutzenstiftenden Abbildung der Hierarchie treten. Außerdem würde sich das Medium hervorragend anbieten, die interne Kommunikation durch mehr aktuellen Content anzukurbeln.

Design

Die „Trademark" der Briefmarken klang bereits an. Wiewohl sie uns gute Dienste geleistet haben, kann – bei aller Liebe zur Kontinuität – dies nicht für alle Zeiten die optische Repräsentanz sein. Zwar entwickelt sich ein Corporate Design (CD) an der TU – bösen Gerüchten zufolge – immer nur dann, wenn ein Architekt Rektor ist. Trotzdem sollten die wenigen Versatzstücke eines TU-CD´s (Logo, Farbe, ...) durchgängig Niederschlag in den Webseiten finden. Andernfalls ist ein Wiedererkennungseffekt schwer zu realisieren.

Technik

Die Palette an EDV ist an der TU denkbar breit. Alle Plattformen und Clients sind vertreten. Das macht es per se nicht einfacher, funktionale Elemente zu implementieren. Proprietäre Lösungen sind verpönt. Allein die Vielfalt der datenbankgetriebenen Web-Infosysteme an der TU ist beeindruckend. Um nur die wichtigsten zu nennen:

- Zentrale Verwaltung: *TUWIS, HISTU*
- ZID: *White Pages*
- Außeninstitut: *Forschungsdokumentation*
- Bibliothek: *Aleph 500*
-)|(unikat: *Lehrzielkatalog, Wegweiser*

Diese – gut gemeinte, aber wenig reflektierte und koordinierte – Entwicklung führt zu Redundanzen und Inkonsistenzen. Freilich wäre es unvertretbar, all diese etablierten Systeme über Bord zu werfen und den großen Wurf in Angriff zu nehmen. Auch ein Warten auf einen evolutionären Bereinigungsprozess erscheint nicht angebracht. Allerdings würde das Fokussieren auf EINE Darstellung nach außen den UserInnen wohl einiges an Verwirrung ersparen.

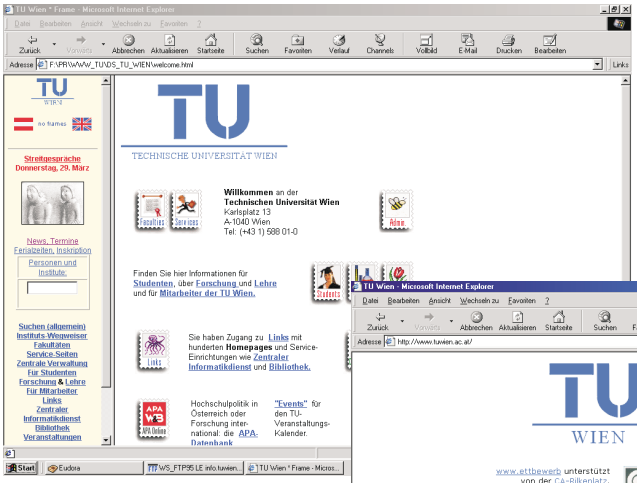
Von www.bhutan.at lernen

Jüngst heimste das Institut für Softwaretechnik einen internationalen Preis für die Site www.bhutan.at ein. Eine komplexe Site mit allem, was das SurferInnen-Herz höher schlagen lässt. Gut zu wissen, dass „wir“ das können.

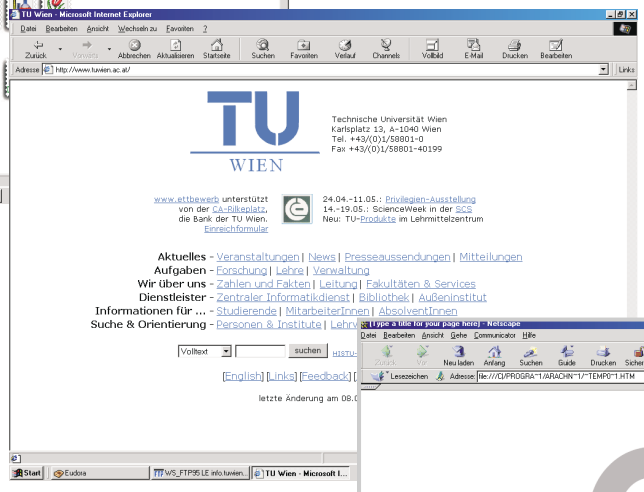
Wiewohl sich aus den Ergebnissen des Wettbewerbs wohl kein neues Look-And-Feel für die TU-Site aufdrängt, werden wir an der Implementierung weiterarbeiten. Die Verwendung eines Content Management Systems (CMS), was ein schnelles „Befüllen“ der Site mit aktuellen Inhalten ermöglichen soll, ist ebenso fix eingeplant wie effektivere Suchmöglichkeiten.

Es stünde der *Technischen* Universität gut zu Gesicht, eine Website auf der Höhe der Zeit zu haben. Bleibt zu hoffen, dass die bisherigen Bemühungen von Erfolg gekrönt sind. Das kann aber nur funktionieren, wenn wir beim „Bauen“ von Websites dieselben Maßstäbe zur Anwendung bringen, wie wir das beim Bauen von Häusern gewohnheitsmäßig tun. Schließlich gibt es an der TU nicht „nur“ ArchitektInnen, sondern auch InformatikerInnen.

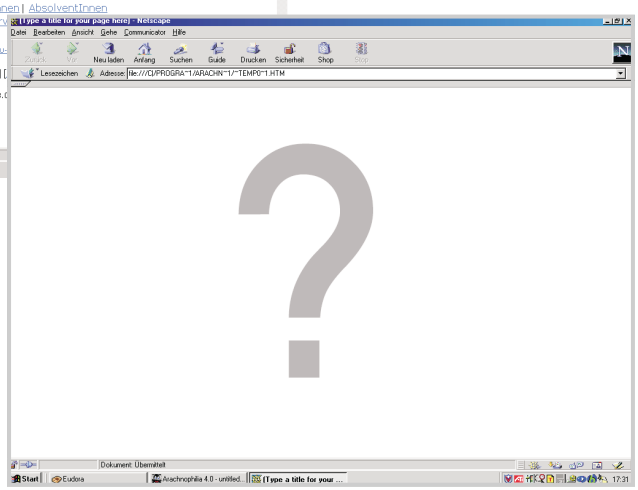
Allerdings handelt es sich auch um eine Glaubensfrage. Glauben wir daran, dass sich ein professionellerer Webauftritt amortisiert, weil „bessere“ StudentInnen zu uns kommen, weil potentere Wirtschaftspartner mit uns kooperieren und weil wir uns selbst Zeit und Ärger sparen?



„Gestern“ ...



... „Heute“ ...



... „Morgen“

Aufbau eines geschützten Subnetzes im TUNET

Werner Scholz, Thomas Schrefl und Josef Fidler
Institut für Angewandte und Technische Physik
werner.scholz@tuwien.ac.at, thomas.schrefl@tuwien.ac.at, fidler@tuwien.ac.at
http://magnet.atp.tuwien.ac.at/

Die Vergrößerung der Arbeitsgruppe und besondere Anforderungen an die Netzwerk-Infrastruktur haben uns veranlasst, ein geschütztes Subnetz innerhalb des TUNET aufzubauen. Über die dabei gemachten Erfahrungen soll im Folgenden berichtet werden.

1 Motivation

Im Lauf der letzten Jahre hat sich die Arbeitsgruppe von Prof. Fidler und Doz. Schrefl kontinuierlich vergrößert. Mittlerweile ist sie auf knapp ein Dutzend Mitarbeiter und rund 20 Computer (Arbeitsplatz-Rechner und Hochleistungs-Workstations) angewachsen.

Damit ist auch der Aufwand für Wartung und Administration gewachsen, ohne jedoch eine grundlegende Verbesserung z.B. auf dem Gebiet der Datensicherheit zu bringen. Die Umstellung auf twisted-pair-Verkabelung und die Erneuerung einiger Computer machte ein grundsätzlich neues Konzept notwendig.

Die wichtigsten Aspekte bei der Planung der neuen Netzwerk-Lösung waren Einbruchsicherheit, Datensicherheit und optimale Ausnützung der Netzwerk und Rechenkapazitäten bei vereinfachter Administration.

Einbruchsicherheit sollte vor Angriffen von Hackern aus dem Internet bewahren und damit vor den leidvollen Erfahrungen, die andere Institute bereits machen mussten. Datensicherheit bedeutet für uns nicht nur Schutz vor Datenverlust, sondern auch einen vereinfachten Zugriff auf die Daten innerhalb des heterogenen Netzwerks. Die vorhandenen und neu anzuschaffenden Rechner sollten dabei optimal ausgenützt werden und ein leistungsfähiges Umfeld zur Durchführung der mikromagnetischen Simulationen bereitstellen [1].

Wie sind die einzelnen Anforderungen zu erreichen? Wir wollen (und können) nicht alle Möglichkeiten aufzeigen und vergleichen, sondern beschränken uns auf die Beschreibung der Lösung, die wir für unsere Arbeitsgruppe gefunden haben.

Von Anfang an war klar, dass die Einbruchsicherheit nur durch eine Firewall-Lösung gewährleistet werden kann. Dazu ist es notwendig, das Netzwerk so aufzubauen, dass es genau eine Verbindung zwischen unserem Subnetz und dem Rest des TUNET gibt. Dazu kann man entweder ein „virtuelles LAN“ einrichten oder die Netze einfach physisch trennen. An die Schnittstelle der beiden Netze wird die Firewall gesetzt, die die Verbindung zwischen den beiden herstellt.

Datensicherheit wollten wir durch einen zentralen Fileserver erreichen. Über NFS können Unix und Linux Clients auf die Daten zugreifen, während Windows PCs über Samba [2] die zentralen Daten erreichen. Dadurch müssen sich die Benutzer nicht mehr mit „verteilten“ Daten auf einer Vielzahl von Rechnern herumschlagen, sondern haben alles an einem Ort vereint und können doch von allen Rechnern darauf zugreifen. Außerdem werden regelmäßige zentrale Backups möglich, die alle wichtigen Daten sichern.

Trotz der „bunten“ Mischung aus DEC Alpha Workstations, Linux/Alpha Workstations, Linux/Intel PCs und Windows PCs, wollten wir möglichst viele Verwaltungsaufgaben zentral auf einem Server erledigen und die Clients mit einer einfachen „Standardinstallation“ ins Netz einbinden. Vor allem die Benutzer- und Ressourcenverwaltung sollten zentral erfolgen. Für die Benutzerverwaltung bietet sich unter Unix/Linux NIS/yellow pages an, das eine zentrale Verwaltung ermöglicht und den Benutzern erlaubt, sich am nächsten freien Rechner anzumelden und die gewohnte Umgebung mit allen persönlichen Einstellungen vorzufinden. Ressourcenverwaltung bedeutet für uns die Verteilung der Computersimulationen auf die verschiedenen Rechner. Ein zentrales Queueing-System für Batch-Jobs sollte diese Anforderung auch in einer heterogenen Netzlandschaft erfüllen.

Letzteres ist auch das eigentliche Ziel unseres Entwurfs: Der Aufbau eines leistungsfähigen Netzwerks für CPU- und speicher-intensive Computersimulationen. Beim Entwurf hat uns Dr. Robert Lorenz (Institut für Materialphysik der Universität Wien) mit seiner langjährigen Erfahrung ausgezeichnet beraten. Die Firma init.at [3] hat die neuen Maschinen vorinstalliert geliefert und konfiguriert. Wartungsverträge sichern uns dabei den reibungslosen Betrieb und entlasten uns von Fehlersuche und Problembehebung. Das wichtigste Argument war (neben dem Preis) vor allem der Komfort, alles aus einer Hand zu erhalten, und damit bei Problemen nur einen Ansprechpartner zu haben.

2 Entwurf

Zuerst stellte sich die Frage, ob wir weiterhin die Infrastruktur des TUNET benützen oder unser Subnetz auch physisch vom TUNET trennen. Da wir eine NFS-Anbindung der Clients (auf denen die Computersimulationen durchgeführt werden) an einen zentralen Fileserver planten, war klar, dass die Verbindung der Rechner über die Switches des ZID mit 10 MBit nicht ausreichen würde. Vor allem das letzte Teilstück zum Fileserver (auch wenn es mit 100 MBit angebunden würde) könnte zum Flaschenhals werden. Daher haben wir uns entschlossen, die Rechner mit eigenen Switches zu verbinden und physisch vollkommen vom TUNET zu trennen. In Anbetracht der möglichen Netzwerkbelastung haben wir uns schließlich für eine 100 MBit full-duplex Anbindung der Clients und ein 1 GBit full-duplex Netzwerkinterface zum Fileserver entschieden.

Die physische Trennung vereinfacht auch den Einbau einer Firewall, da man ohne Einrichtung eines „virtuellen LANs“ auskommt. Für Firewalls bieten sich verschiedene Lösungen an. Eine einfache und ausfallssichere Firewall wird vom ZID angeboten [4]. Wir haben uns für eine Lösung von init.at entschieden und damit alle neuen Geräte aus einer Hand. Diese Firewall erlaubt auch den Aufbau eines „virtual private network (VPN)“ und damit die Einbindung entfernter Rechner (auch außerhalb des TUNET z. B. über chello StudentConnect, Teleweb), für die ein VLAN nicht mehr möglich ist (siehe Kap. 5.2). Außerdem verstecken wir durch IP-Masquerading unser gesamtes Subnetz hinter einer einzigen IP-Adresse. Dadurch haben wir hinter der Firewall die Freiheit, in einem Class-C-Netz bis zu 254 IP-Adressen selbst zu vergeben.

Der Fileserver ist das „Herzstück“ unseres Subnetzes. Er sollte mehrere Aufgaben übernehmen:

- Datenspeicherung, für die wir rund 200 GB vorgesehen haben. Der Zugriff auf die Daten muss über NFS und Samba ermöglicht werden.
- Benutzerverwaltung und Authentifizierung mittels NIS/ yellow pages.
- Nameserver für unser Subnetz
- Master für das Queueing-System
- zentrale Installation verschiedener Applikationen

Als Clients haben wir leistungsstarke PCs vorgesehen, die einerseits als Arbeitsplatzrechner dienen und gleichzeitig im Hintergrund die Computersimulationen durchführen. Dafür benötigen sie eine schnelle CPU und ausreichend Hauptspeicher. Als Betriebssystem haben wir uns für Linux entschieden, da es

- stabil genug ist, um eine gleichzeitige Nutzung der Computer als Arbeitsplatzrechner und „Rechenknecht“ zu ermöglichen,
- die gewünschte Client/Server-Architektur optimal unterstützt,
- von den von uns verwendeten Programmpaketen unterstützt wird,
- ein ausgezeichnetes Preis/Leistungsverhältnis hat
- und wir das Know-how haben, um die notwendigen Administrationsaufgaben selbst zu erledigen.

3 Implementierung

Bevor wir uns an die Umsetzung unserer Pläne machten, besprachen wir sie noch ausführlich mit dem ZID. Dabei wurde uns erlaubt, die bestehende twisted-pair-Verkabelung zu benützen und an unseren eigenen Switch, der in das Rack des ZID eingebaut wurde, anzuschließen.

3.1 Das Netzwerk

In Abbildung 1 ist die Struktur unseres Netzwerks skizziert. Die Firewall stellt die Verbindung zwischen dem TUNET und dem internen Subnetz über Switch 2 her. An Switch 2 sind einige Simulationsrechner (Linux/ Alphas) mit 100 MB und der Fileserver mit 1 GB angeschlossen. Eine zweite Glasfaserleitung stellt die Verbindung zu Switch 1 her, an den die bestehende twisted-pair Verkabelung mit den Arbeitsplatzrechnern angeschlossen ist. Der Mail- und Webserver ist außerhalb unseres Subnetzes direkt an das TUNET angeschlossen.

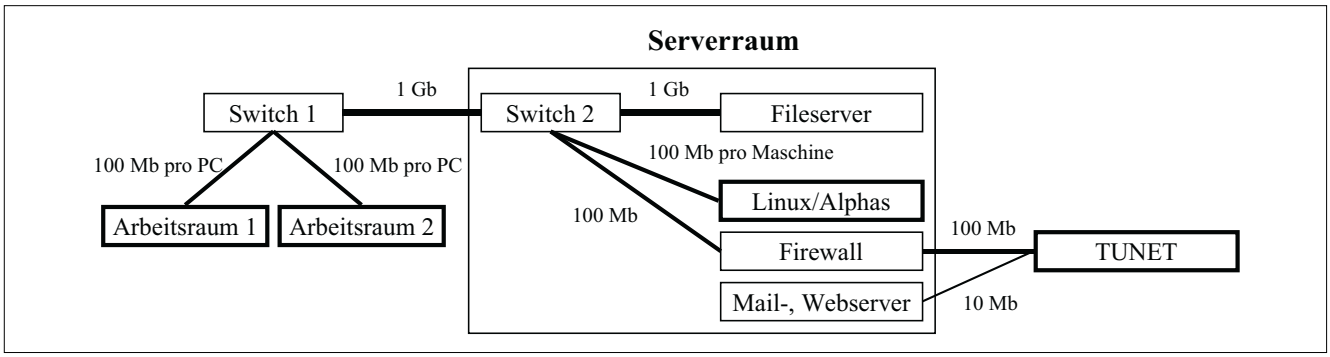


Abbildung 1

3.2 Die Switches

Da unsere Server in einem anderen Raum stehen als das Rack, in dem die twisted-pair-Kabel der Arbeitsplätze zusammenlaufen, mussten wir zwei Switches (hp procurve 2512 und 2324) kaufen und mittels Glasfaserstrecke (1 GBit) verbinden. Die Anschlüsse der Arbeitsplätze wurden einfach von den Switches des ZID auf unseren verlegt, sodass wir hier eine „saubere“ physikalische Trennung des TUNET von unserem Subnetz erreichen. Solange das private Netz relativ klein und überschaubar ist und damit keine spezielle Konfiguration (VLANs etc.) erfordert, kann auf Management- und Fernwartungsfähigkeiten (SNMP) der Switches verzichtet werden. Dem zweiten (zentralen) Switch, an den die Firewall und der Fileserver angeschlossen sind, haben wir diese Fähigkeiten spendiert, um einfachere Möglichkeiten zur Fehlerdiagnose zu haben. Unbedingt notwendig ist SNMP für uns, wie sich gezeigt hat, jedoch nicht.

3.3 Der Fileserver

Wir haben einen Dual Pentium III 733 MHz mit 256 MB ECC RAM ausgewählt, der unter SuSE Linux 7.0 [5] betrieben wird. Die geforderte Datensicherheit wird dabei durch mehrere Maßnahmen erreicht: Ein Hardware-RAID-Controller verbindet 4 SCSI Festplatten zu einem RAID Level 5 System mit einer Kapazität von 80 GB, auf dem das Betriebssystem und die Home-Verzeichnisse der Benutzer abgelegt sind. Der Einsatz des „journaling filesystem“ „ReiserFS“ [6] beschleunigt die Rekonstruktion des Filesystems in einen konsistenten Zustand auch bei Absturz des Fileservers. Zwei große IDE-Festplatten werden als Software-RAID mit einer Kapazität von 110 GB ebenfalls unter ReiserFS betrieben.

Zur Datensicherung haben wir einen Sony TDL-11000 Bandwechsler für 8 Backup-Bänder mit einem eingebauten SDL-11000 DDS4 Bandlaufwerk, das komprimiert bis zu 40 GB pro Band speichern kann. Ein Bandwechsler ist zwar eine teure aber sehr komfortable Investition, die durch vollautomatische tägliche Backups die Datensicherheit garantiert.

3.4 Die Clients

3.4.1 Reine Arbeitsplatzrechner

Die vorhandenen Arbeitsplatzrechner wurden natürlich an die neue Infrastruktur angeschlossen und profitieren von der schnellen 100 MB full-duplex Anbindung, sofern die jeweilige Netzwerkkarte das unterstützt.

3.4.2 Kombinierte Arbeitsplatz/Simulationsrechner

Fünf neue Athlon PCs mit 900 MHz und 512 MB RAM wurden als Arbeitsplatzrechner, die gleichzeitig im Hintergrund Simulationen durchführen, angeschafft und die Linux-Distribution von RedHat [7] in der Version 6.2 installiert. Schnelle 100 MB Netzwerkkarten und schnelle IDE-Festplatten, die im UDMA-Modus betrieben werden, erlauben diesen kombinierten Betrieb. Solange der Hauptspeicher ausreicht, ist kaum zu merken, dass die CPU im Hintergrund mit einer Simulation beschäftigt ist. Erst wenn auf den virtuellen Speicher auf der Festplatte ausgelagert wird, ist ein Performance-Einbruch spürbar.

3.4.3 Simulationsrechner

Sechs Alpha-Clones (Alpha EV56 Prozessoren mit 533 MHz auf AlphaPC 164 LX und SX Boards) wurden ebenfalls in unser Netzwerk eingebunden. Da wir mit RedHat 5.2 (Linux Kernel 2.0.25), das bisher installiert war, immer wieder Probleme mit NFS hatten, wurde ein Update auf RedHat 6.2 durchgeführt. Der Standard-Kernel wurde auch hier durch einen selbst kompilierten (2.2.18) ersetzt.

Außerdem wurde ein Hochleistungsrechner (UP2000: 2x Alpha EV67 666 MHz mit 1 GB ECC RAM auf einem AlphaPC 264 DP Board mit Tsunami Chipsatz [8]) gekauft, um besonders große Probleme rechnen zu können. Als Betriebssystem kommt wieder SuSE 7.0 mit selbstkompiliertem Kernel 2.2.17 SMP zum Einsatz.

4 Konfiguration und Administration

4.1 Netzwerkkonfiguration

Da wir so eine „saubere“ Trennung unseres Subnetzes vom TUNET vorgesehen hatten, wurden unserer Pläne vom ZID ohne Änderungen akzeptiert. Bei der Besprechung wurden im Wesentlichen nur die IP-Adresse der externen Netzwerkkarte unserer Firewall im TUNET und der Adressraum unseres Subnetzes festgelegt. Dabei wurde uns das Class-C-Netz 192.168.45.0/24 mit 254 freien IP-Adressen zugewiesen. Da auch Class-C-Adressen innerhalb des TUNET voll geroutet werden (!), ist eine entsprechende Koordinierung unbedingt notwendig. Dies ist vor allem im Falle eines „Lecks“ der Firewall, bei dem interne Pakte nach außen gelangen, wichtig, um den Urheber schnell ausfindig machen zu können.

Durch die Aktivierung der Firewall mit IP-Masquerading sind natürlich einige Rechner aus dem TUNET „verschwunden“, sodass wir sie in der TUNET-Datenbank [9] abmelden und die entsprechenden IP-Adressen freigeben konnten. In unserem Subnetz 128.130.45.0 wäre es gar nicht mehr möglich gewesen, alle neuen Rechner anzumelden, da der freie Adressraum bereits ausgeschöpft ist.

Will man sich die Administration von IP-Adressen ersparen, so kann man auch einen DHCP-Server installieren. Den Clients wird dann beim Booten automatisch eine IP-Adresse vom Server zugewiesen. Meist gibt es aber einige Geräte, die diese Funktionalität nicht unterstützen, und denen ohnedies eine IP-Adresse fix zugewiesen werden muss. Den wichtigen Servern werden auch meist fixe Adressen zugewiesen. Daher haben wir uns entschlossen, gleich alle IP-Adressen händisch zu vergeben.

Die Konfiguration der Firewall und des Fileservers wurde von init.at durchgeführt. Diese beiden Rechner übernehmen mehrere (zentrale) Funktionen in unserem Netzwerk und sollen daher im Folgenden näher beschrieben werden.

4.2 Firewall-Konfiguration

Die Firewall ist ein einfacher PC (Intel Celeron 633 MHz mit 64 MB RAM und 10 GB Festplatte), der mit einer von init.at modifizierten Linux-Distribution von Debian läuft. Eine einzige Datei enthält alle Informationen und Regeln zur Konfiguration der Firewall.

Die Firewall ist damit genauso sicher und unsicher wie der Linux-Kernel, der darauf läuft, aber sie ist für uns ein großer Fortschritt im Vergleich zur früheren Situation, als alle Rechner „direkt“ von der ganzen Welt aus erreichbar waren und damit ein potentielles Ziel für Angriffe aller Art.

Auch eine Sicherheitsüberprüfung durch den ZID [10], die die gängigsten Sicherheitsmängel aufdecken kann, hat uns diesbezüglich beruhigt.

Von außen ist (im Prinzip) ein einziger Port erreichbar, damit wir uns überhaupt in unser Netz einloggen können (siehe Kap. 5.1). Auch der Zugriff von innen nach außen ist auf die notwendigen Dienste (z. B. telnet, ftp, ssh, http, https, news, ntp, pop2, pop3, smtp, domain, ping, finger etc.) eingeschränkt.

Auf der Firewall laufen aus Sicherheitsgründen keine weiteren Dienste wie WWW-Proxies, E-Mail-Server, WWW-Server oder Ähnliches. Diese laufen alle auf anderen Maschinen. Öffentlich zugängliche Dienste wie WWW-Server oder E-Mail-Server kann man in einer „DMZ“ (demilitarized zone), die zwar durch die Firewall überwacht wird, in der aber bestimmte Dienste von außen zugänglich sind, unterbringen. Wir haben vorerst darauf verzichtet und den E-Mail- und WWW-Server der Arbeitsgruppe in die „freie Wildbahn“ gestellt, können aber bei Bedarf jederzeit eine DMZ einrichten.

4.3 Netzwerkoptimierung

Die Firewall erfüllt auch noch einen zweiten Zweck: Sie hält unerwünschten Netzwerkverkehr fern und entlastet damit die Anbindung unserer Arbeitsplatzrechner. Beispielsweise die „Fluten“ an Broadcast-Messages, die sich bei jedem Öffnen der Netzwerkumgebung auf einem Windows-PC ins Netz ergießen, werden von der Firewall gefiltert und nicht nach innen weitergeleitet. Natürlich sind unsere Windows-PCs damit von außen nicht mehr sichtbar, aber erstens liegen unsere wichtigen Daten ohnedies nur noch am Fileserver und zweitens soll auch sonst niemand auf unsere Windows-PCs zugreifen. (Wie wir von außen auf unsere Daten zugreifen können, ist in Kap. 5.1 beschrieben.)

Da wir mit unseren eigenen Switches alle Rechner mit 100 MB full-duplex anschließen können, wurde bei jenen Rechnern, die das nicht automatisch mit dem Switch „ausgehandelt“ haben, händisch nachgeholfen. Sehr hilfreich waren dabei die LEDs auf unseren Switches, die die eingestellte Geschwindigkeit für jeden Port anzeigen. Natürlich haben wir auch ein paar ältere Modelle, die nur 10 MBit unterstützen, wobei diese alle im half-duplex Modus betrieben werden. Die Umstellung einer DEC AlphaStation in den 10 MBit full-duplex Modus, der theoretisch von unseren Switches unterstützt wird, war beispielsweise nicht möglich.

Schließlich haben wir auch den Netzwerk-Verkehr, der durch NFS-Verbindungen erzeugt wird, reduziert, indem wir „automount“ verwenden. Dazu mehr in Kapitel 4.4.3 über unsere NFS Konfiguration.

4.4 Fileserver-Konfiguration

Der Fileserver spielt eine zentrale Rolle in unserem Subnetz. Daher haben wir für ihn auch einen Wartungsvertrag abgeschlossen. Natürlich ist es gefährlich, einer einzigen Maschine alle im Folgenden beschriebenen Aufgaben zu übertragen, für uns hat es aber mehrere Vorteile. Erstens haben wir die Maschine fertig konfiguriert gekauft und mit dem Wartungsvertrag dem Lieferanten die Verantwortung für den reibungslosen Betrieb übertragen. Zweitens sind fast alle diese Dienste notwendig, um überhaupt in unserem Netz arbeiten zu können. Würden wir diese Dienste einer anderen Maschine übertragen, müssten wir für diese ebenfalls einen Wartungsvertrag abschließen. Dies kommt wieder nur bei einem neuen Gerät in Frage, was weitere Investitionen notwendig gemacht hätte. Schließlich war es unser Ziel, die Daten nur noch zentral am Fileserver abzulegen. Sollte dieser ausfallen, können wir ohnedies nicht auf unsere Daten zugreifen und sind in unserer Arbeit stark behindert, sodass er möglichst schnell wieder in Betrieb genommen werden muss.

4.4.1 NIS/yellow pages

Die zentrale Verwaltung der Benutzeraccounts erfolgt am Fileserver. Dieser stellt über NIS/yellow pages allen Clients die Benutzerdaten zur Verfügung. Ein neuer Benutzer muss damit nur ein Mal am Fileserver angelegt werden und kann sich sofort auf jedem beliebigen Unix/Linux-Rechner anmelden. Die home-Verzeichnisse liegen natürlich auch am Fileserver und werden über NFS exportiert, sodass jeder Benutzer seine gewohnte Umgebung und seine persönlichen Einstellungen vorfindet, egal an welchem Rechner er arbeitet. Dies funktioniert bei uns sogar im Mischbetrieb von Athlons und Alphas unter RedHat und SuSE Linux und einer DEC AlphaStation, die unter Compaq Tru64 4.0F läuft, reibungslos.

Wenn man viele Windows NT Rechner in einem heterogenen Netz mit Unix/Linux Rechnern zu administrieren hat, lohnt es sich sicher, diese in die zentrale Benutzerauthentifizierung über NIS/yellow pages einzubinden. Dies konnte bei uns unterbleiben und unter Windows 95 und Windows 98 kann sich ohnedies „jeder selbst“ seinen Benutzeraccount anlegen, wobei es jedoch vorteilhaft ist, die selben Usernamen zu verwenden (siehe Kap. 4.4.4).

4.4.2 DNS

Der Fileserver hat bei uns auch die Aufgaben eines Nameservers für die internen IP-Adressen übernommen. Dieser Dienst könnte noch durch einen zweiten Nameserver abgesichert werden. Diese Sicherheit bietet uns aber auch die Verteilung der IP-Adressen und Namen in statischen „hosts“-Dateien. Bei der Größe unseres Subnetzes

ist die Verwaltung dieser statischen Tabellen noch möglich und es reduziert nebenbei wieder den Netzwerkverkehr durch Einsparung von Anfragen an den Nameserver.

4.4.3 NFS

Die wichtigsten Verzeichnisse werden über NFS exportiert und so den Unix/Linux Clients zur Verfügung gestellt. Mit der 2.2.x Serie des Linux-Kernels wurde die NFS-Implementierung stark verbessert und hat sich als sehr stabil und zuverlässig erwiesen. Da NFS-Verbindungen auch dann (geringen) Netzwerkverkehr erzeugen, wenn keine Daten übertragen werden, wird auf allen Clients „automount" verwendet. Dabei laufen auf den Unix/Linux-Clients Dämonen im Hintergrund, die erst dann eine NFS-Verbindung herstellen (das gewünschte Verzeichnis mounten), wenn ein Zugriff darauf erfolgt. Nach einer (konfigurierbaren) Zeitspanne, in der keine Daten übertragen wurden, wird die Verbindung automatisch wieder abgebaut (umount des jeweiligen Verzeichnisses).

Auch die meisten Anwendungen haben wir nicht auf den Clients, sondern nur zentral am Fileserver installiert (siehe Kap. 4.4.6). Dies vereinfacht und verkürzt die Installation enorm.

NFS Dienste sind ein beliebtes Ziel für Angriffe. Unsere Firewall schützt uns vor derartigen Gefahren, da NFS-Verbindungen über die Firewall (in beiden Richtungen) unterbunden sind. Welche Probleme das (und die Verwendung von IP-Masquerading) mit sich bringt, ist in Kap. 5.6 beschrieben.

4.4.4 Samba

Damit auch Windows-PCs von der zentralen Speicherung der Daten profitieren, wurde am Fileserver ein Samba-Server installiert [2]. Bei der Einrichtung eines neuen Benutzers wird auch gleich ein Samba-User angelegt und ein entsprechendes Passwort festgelegt.

In unserem Netzwerk hat damit jeder Benutzer nur zwei Accounts und zwei Passworte, die aber problemlos ident gewählt werden können: Ein Unix/Linux-Account mit Passwort, mit dem er sich auf den Unix/Linux-Rechnern authentifiziert, und ein Benutzername mit entsprechendem Passwort für den Zugriff auf den Fileserver über Samba. Werden der Benutzername und das Passwort auf den Windows-Rechnern ident mit jenen für den Samba-Zugriff gewählt, erhält der Benutzer nach erfolgter Anmeldung an einem Windows-PC ohne weitere Passworteingabe Zugriff auf seine Daten am Fileserver. Damit die Samba-Passworte nicht im Klartext übertragen werden, muss unter Windows die Übertragung unverschlüsselter Passworte deaktiviert sein. Bei Windows 95 erfolgt dies mit einem Patch von Microsoft, bei Windows 98 und Windows NT 4.0 ab SP3 werden die Passworte standardmäßig nur verschlüsselt übertragen [11]. Letzteres kann durch einen Registry-Eintrag wieder aufgehoben werden, ist aber natürlich nicht zu empfehlen.

Für Windows-Rechner sind vier Samba-Shares eingerichtet. Unter [home] finden unsere Benutzer alle home-Verzeichnisse, von denen täglich ein Backup gezogen wird, wobei sie nur im eigenen Verzeichnis Schreibrechte haben. Unter [scr] erhält jeder Benutzer Schreib- und Lesezugriff auf seine Daten im Scratch-Bereich des Fileservers und Lesezugriff auf die Daten aller anderen. Zusätzlich wurde [groups] eingerichtet, das zwar physikalisch im Home-Directory des Fileservers liegt, jedoch mit speziellen Optionen in der Samba-Konfiguration versehen wurde. Diese führen dazu, dass die Dateien und Verzeichnisse, die unter Windows unter [groups] erstellt werden, von allen Benutzern gelesen und beschrieben/ modifiziert/gelöscht werden können. Damit wird unter Windows der gemeinsame Zugriff auf bestimmte Daten und beispielsweise das Erstellen und Bearbeiten von Dokumenten in der Gruppe vereinfacht. Schließlich gibt es noch einen [temp] Bereich (der physikalisch auf der Scratch-Partition am Fileserver liegt), in dem ebenfalls jeder alle Rechte hat.

4.4.5 DQS

Als Queueing-System, das die Jobs automatisch an die verfügbaren Rechner verteilt, verwenden wir DQS [12] in der Version 3.3.2. Wir haben in unserem Netz zwei binär-inkompatible Architekturen, nämlich Intel-kompatible Rechner (AMD Athlons) und Alphas. Diese haben wir trotzdem in einem Queueing-System zusammengefasst und verwalten dieses mit nur einem „Queue-Master". Dieser läuft am Fileserver und überwacht die einzelnen Queues und verteilt die Jobs.

DQS ermöglicht die Konfiguration mehrerer Zellen, die von mehreren Queue-Mastern verwaltet werden. Die Trennung der beiden Architekturen erfolgt aber einfacher durch die Definition von sog. „complexes". Diese sind im Wesentlichen Schlüsselworte, die bei verschiedenen Queues, die aus bestimmten Gründen zusammengefasst werden sollen, definiert sind. In unserem Fall wurde für die Intel-kompatiblen Rechner das Schlüsselwort „intel" definiert und den Queues der entsprechenden Rechner zugeordnet. Analog erhielten die sechs Queues der Alpha-Clones das Schlüsselwort „alpha". Zusätzlich wurden diese „complexes" als „required" konfiguriert, sodass der Benutzer beim Abschicken seines Jobs eines der beiden Schlüsselworte angeben muss. Damit ist der Benutzer gezwungen, sich für eine Architektur zu entscheiden, und es kann nicht vorkommen, dass ein Job unvorhergesehen auf der falschen Architektur (erfolglos) zur Ausführung kommt.

Spezielle Rechner, die für bestimmte Aufgaben reserviert sind, wurden nicht in obiges Schema aufgenommen, sondern wurden im „complex" „reserved" zusammengefasst. Dazu gehören unsere DEC AlphaStation, die hauptsächlich zum Kompilieren verwendet wird, die UP2000, die für besonders große Probleme verwendet wird, oder der Fileserver, auf dem keine Simulationen ausgeführt werden, sondern der z. B. große Datenmengen in einem Batch-Job komprimieren kann. Letzteres ist natürlich doppelt sinnvoll, da die Daten dann nicht zweimal über das Netz laufen, sondern direkt am Fileserver komprimiert werden.

4.4.6 Anwendungen

Alle Anwendungen, die zusätzlich zur RedHat-Standardinstallation benötigt werden, werden ebenfalls zentral am Fileserver installiert.

Unsere Strategie soll am Beispiel des wissenschaftlichen 2D-Plotprogramms Grace [13] demonstriert werden:

Nach dem Kompilieren des Quellcodes oder dem Auspacken aus dem tar.gz- oder RPM-Archiv wird auf der Partition „/pd“ des Fileservers ein Unterverzeichnis „grace-5.1.3“ angelegt. Darin werden die Unterverzeichnisse „bin“, „doc“, „include“, „lib“ etc. angelegt und die notwendigen Dateien in das entsprechende Unterverzeichnis kopiert. (Wenn man den Quellcode selbst kompiliert, kann man als Option für „configure“ oder im „Makefile“ das gewünschte Installationsverzeichnis meist frei wählen. In unserem Fall wäre dies „/pd/grace-5.1.3“.) Um die Installation späterer Updates zu erleichtern, wird noch ein symbolischer Link, der nur den Namen, aber keine Versionsnummer enthält, auf das aktuelle Installationsverzeichnis angelegt: „ln -s /pd/grace-5.1.3 /pd/grace“. Zuletzt wird die Anwendung in „/usr/local“ installiert, indem symbolische Links auf die entsprechenden Dateien angelegt werden: z. B. „ln -s /pd/grace/bin/grace /usr/local/bin/grace“.

Die Verzeichnisse „/pd“ und „/usr/local“ werden vom Fileserver mit NFS exportiert und von allen (Intel-kompatiblen) Clients gemountet. Die Umgebungsvariable „$PATH“ muss natürlich den Pfad „/usr/local/bin“ enthalten und der dynamische Linker für „shared libraries“ auch den Pfad „/usr/local/lib“ berücksichtigen (in „/etc/ld.so.conf“).

Die beschriebene Strategie hat mehrere Vorteile:

a) Anwendungen müssen nur ein Mal am Fileserver installiert werden und stehen danach sofort allen Clients zur Verfügung.

b) Saubere Trennung von Standardinstallation und selbst installierten Anwendungen.

c) Dadurch einfache Installation und Einbindung neuer Clients bzw. Neuinstallation oder Update des Betriebssystems der Clients, da nur eine Standardinstallation mit „ein bisschen“ Anpassung der Konfiguration notwendig ist.

d) Einfaches Update der Anwendungen durch Installation in ein neues Verzeichnis und Umsetzen des symbolischen Links (z. B. „/pd/grace -> /pd/grace-5.1.4“).

e) Schneller Überblick über alle installierten Anwendungen durch ein zentrales Verzeichnis („/pd“).

4.4.7 Beowulf Tools

Wie lässt sich nun die Konfiguration und Administration vieler gleichartiger Clients am einfachsten bewerkstelligen?

Im Rahmen des Beowulf-Projekts [14] wurden einige Werkzeuge entwickelt, die diese Aufgaben wesentlich vereinfachen. Wir verwenden vor allem „brsh“ [15], die „Beowulf remote shell“, die wir zu einer „bssh“, „Beowulf secure shell“, umgeschrieben haben. Damit lässt sich der Reihe nach auf allen gewünschten Maschinen ein Kommandozeilenbefehl ausführen, ohne sich auf jeder Maschine einzeln einzuloggen und den Befehl ausführen zu müssen.

Die Clients müssen auf diese Art des Zugriffs vorbereitet sein, indem eine entsprechende „.rlogin“-Datei im Home-Verzeichnis von root angelegt wird, oder der öffentliche Schlüssel des Benutzers, der bssh aufruft, den „authorized_keys“ der Clients hinzugefügt wird. „brsh“ ist nur ein einfaches Shell-Skript, das sich mittels rsh oder ssh auf jeder Maschine einloggt, den gewünschten Befehl ausführt und die Verbindung wieder beendet, ehe mit der nächsten Maschine fortgesetzt wird.

Die Konfiguration und Administration der Clients besteht meist in einem Editieren entsprechender Dateien. Von den Konfigurationsdateien (z. B. /etc/bashrc) haben wir beispielsweise eine Kopie auf dem Fileserver (z. B. /pd/Athlon.config/etc/bashrc). Ist nun eine Änderung notwendig, so wird die gewünschte Datei am Fileserver editiert und mit dem einfachen Befehl „bssh cp /pd/Athlon.config/etc/bashrc /etc/“ auf alle Clients kopiert.

Damit lässt sich ein Großteil der Administrationsaufgaben für alle Clients „gleichzeitig“ durchführen und der Aufwand ist unabhängig (!) von der Anzahl der Clients.

Natürlich ist die beschriebene Konfiguration nur in einem (von einer Firewall) geschützten Netzwerk empfehlenswert. Andernfalls wird es einem Angreifer sehr leicht gemacht, nach einer kompromittierten Maschine auch noch die Kontrolle über alle anderen zu übernehmen.

5 Probleme und Lösungen

5.1 Zugriff von außen

Hat man einmal so ein durch eine Firewall gesichertes Netzwerk aufgebaut, so war man bestrebt, alle Lücken, durch die ein Einbrecher in das Netzwerk eindringen kann, zu schließen. Hat man es wirklich gründlich gemacht, dann sollte man auch selbst nicht mehr von außen in sein Netzwerk hineingelangen. Da es aber meist doch erwünscht ist, authorisierten Personen den Zugang zu ermöglichen, muss man wohl oder übel wieder einen Weg öffnen.

Dafür gibt es wieder mehrere Möglichkeiten, die stark von den jeweiligen Erfordernissen abhängen. Auf keinen Fall sollte man ein Login direkt auf der Firewall erlauben. Die Firewall sollte vielmehr die Verbindung auf eine bestimmte Maschine im Netz weiterleiten (z. B. durch Port-Forwarding), die dann die Authentifizierung durchführt. Es ist damit sehr einfach und auch sehr empfehlenswert, die Anmeldungen im Netz zu protokollieren und zu überwachen.

In jedem Fall sollten nur verschlüsselte Verbindungen zugelassen werden, da sonst die Gefahr, dass Passworte belauscht (gesnifft) werden, zu groß ist. Heute ist das Standardwerkzeug für verschlüsselte Verbindungen „ssh“

[16]. Im Gegensatz zu telnet, ftp und pop werden alle übertragenen Daten (vor allem auch die Passworte!) verschlüsselt. Damit wird die Übertragung vertraulicher Daten über ein unsicheres Netzwerk möglich. Natürlich muss die Verbindung vom Anfang bis zum Ende verschlüsselt sein. Die in der Praxis immer wieder verwendete Methode „*Ich-hab-auf-Rechner-A-gerade-kein-ssh-darum-log-ich-mich-auf-Rechner-B-mit-telnet-ein-und-mach-dann-ein-ssh-auf-Rechner-C*“ führt natürlich alle Sicherheitsmaßnahmen ad absurdum, da die Verbindung von Rechner A zu Rechner B nicht verschlüsselt ist und damit alle Informationen auf dieser Verbindungsstrecke belauscht werden können. Um solchen Situationen vorzubeugen, sind Werkzeuge wie Mindterm's Java-Implementierung eines ssh Clients [17] hilfreich, da, auch wenn kein ssh installiert ist, fast immer ein Webbrowser mit Java-Unterstützung zur Verfügung steht.

Es gibt mehrere (auch freie) Implementierungen des ssh-Protokolls (z. B. OpenSSH [18]), und in den meisten Linux-Distributionen ist die eine oder andere enthalten.

Wie bereits erwähnt, ist auch ftp ein unsicheres Protokoll, bei dem Passworte im Klartext übertragen werden, und damit relativ einfach belauscht werden können. Als Ersatz bietet sich „scp“, „secure copy“, an, das Dateien über einen verschlüsselten Kanal kopieren kann. Es bietet die selbe Sicherheit und die selben Authentifizierungsmechanismen wie ssh und ist in den meisten ssh-Paketen enthalten.

Natürlich gibt es auch für Windows-Rechner entsprechende Programme. Wir verwenden als ssh-Client für Windows Putty [19] und als ftp-Ersatz WinSCP [20] oder den iXplorer [21]. Weitere Implementierungen auch für andere Plattformen findet man im WWW [22].

Idealerweise sollten für die Anmeldung von außen andere Benutzernamen und Passworte verwendet werden als innerhalb des geschützten Netzes. Diese sollten vom Administrator vorgegeben und so gewählt sein, dass sie nicht leicht erraten werden können. Es sollten keine „normalen“ Wörter sein, sondern auch Ziffern und Sonderzeichen enthalten. Damit ist man beispielsweise vor „brute force“ Angriffen, die einfach ganze Wörterbücher durchprobieren, sicher. Eine regelmäßige Änderung der Passworte ist ein weiterer bedeutender Sicherheitsfaktor.

Will man trotzdem auch den unverschlüsselten Zugang ermöglichen, so bietet sich beispielsweise telnet mit (maschinengenerierten) Einmal-Passworten an. Jeder Benutzer kann dann eine Liste mit solchen Einmal-Passworten anfordern, die innerhalb eines bestimmten Zeitraums gültig sind und nur einmal verwendet werden können.

5.2 VPN

Ist ein einfacher ssh/telnet-Zugang von außen, wie im vorigen Kapitel beschrieben, nicht ausreichend, so kann durch „virtual private networking“ eine sichere, verschlüsselte Verbindung aufgebaut werden, die eine völlig transparente Einbindung in das lokale Subnetz ermöglicht. Beim Aufbau eines VPN wird eine verschlüsselte Punkt-zu-Punkt Verbindung hergestellt, die einen Client über ein unsicheres (öffentliches) Netzwerk (z. B. dem Internet) mit einem VPN-Server und dem angeschlossenen privaten Netz verbindet.

Wir verwenden VPN für Fernwartung und „Teleworking“. Im ersteren Fall erleichtert ein VPN unserem Lieferanten notwendige Konfigurations- und Administrationsarbeiten und damit die Erfüllung des Wartungsvertrags. Durch die Einrichtung eines VPN kann man auch von zu Hause über Modem-Dialin oder Teleweb in unserem Subnetz arbeiten, als wäre man direkt angeschlossen. Damit ist beispielsweise der direkte Zugriff auf unseren Fileserver möglich.

In welcher Form VPN unterstützt wird, hängt von der Firewall und dem VPN-Server ab, der verwendet wird. Will man Windows-Rechner über VPN einbinden, so kann man dazu den „Microsoft Windows VPN Adapter“ verwenden [23]. Abhängig von der Windows-Version werden verschiedene Verschlüsselungsalgorithmen mit verschiedenen Schlüssellängen unterstützt.

5.3 E-Mail

Sind die Standardprotokolle SMTP (zum Versenden) und POP bzw. IMAP (zum Abholen von E-Mails) auf der Firewall freigegeben, so kann man mit entsprechenden Client-Programmen ganz normal auf E-Mail-Server zugreifen. Probleme ergeben sich, wenn innerhalb des Subnetzes ein E-Mail-Server läuft, der E-Mails über die Firewall nach außen senden will. Dieser verwendet als Domain des Absenders nämlich die interne, die ja willkürlich gewählt wurde. Eine vom Benutzer „scholz“ am Fileserver weggeschickte E-Mail wird in unserem Netz mit dem Absender „scholz@fs.lan“ versehen. Die Domain des Absenders wird von den meisten E-Mail-Servern auf ihre Gültigkeit überprüft. Da es die Domain „lan“ natürlich nicht als offiziell registrierte Domain gibt, wird die E-Mail abgelehnt und kann nicht zugestellt werden. Dieses Problem kann durch Domain-Masquerading umgangen werden [24]. Dabei wird die Domain des Absenders ersetzt (sinnvollerweise durch den offiziellen E-Mail-Server der Benutzer), sodass die E-Mails erfolgreich zugestellt werden können.

5.4 WWW

Beim Zugriff auf das World Wide Web ergibt sich ein anderes Problem. Der Standard-Port für das http-Protokoll ist der Port 80. Ist dieser auf der Firewall geöffnet, so kann man problemlos auf das WWW zugreifen. Dokumente, die nur über eine verschlüsselte https-Verbindung erreicht werden können, erfordern das Öffnen des Port 443 für das https-Protokoll.

Zu allem Überfluss gibt es aber viele Dienste im WWW, die über andere Ports aufgerufen werden. Dazu zählen z. B. der Online-Katalog des Österreichischen Bibliothekenverbundes (Port 4505) [25], das „Hypertext Webster Gateway at UCSD“ (Port 5141) [26] und der Mirror von „Scientific Applications on Linux“ am Goodie Domain Service der TU Wien (Port 8050) [27]. Die entsprechenden Ports für die gewünschten Rechner ein-

zeln auf der Firewall freizugeben, ist natürlich nicht praktikabel.

Eine elegante Lösung ist die Installation eines Proxy-Servers außerhalb des privaten Subnetzes. Für diesen muss nur ein bestimmter Port auf der Firewall geöffnet werden. Alle Anfragen des WWW-Browsers werden an den Proxy geschickt, der sie seinerseits an die gewünschte Maschine und an den gewünschten Port weiterleitet. Squid [28] ist so ein Proxy-Server, der auch noch als Cache fungieren kann, und die Protokolle http, https und ftp unterstützt.

Ist ein Proxy für das http-Protokoll ausreichend, so kann man auch den „webwasher“ [29] einsetzen. Dieser wurde eigentlich zum Filtern von Web-Inhalten entwickelt und kann mit oder ohne diese Funktionalität betrieben werden. Mit sehr feinen Einstellungsmöglichkeiten kann man definieren, welche Web-Inhalte nicht weitergeleitet werden sollen (z. B. Werbebanner, bestimmte URLs, Scripts, Animationen) bzw. welche Informationen an die Webserver weitergeleitet werden sollen („referers“, „cookies“).

5.5 Lizenzserver

Ein weiterer Dienst, der bei der Konfiguration der Firewall berücksichtigt werden muss, ist die Anforderung von Lizenzen bei Lizenzservern außerhalb des Subnetzes.

Einige Anwendungsprogramme (z. B. AVS, Patran), die im Rahmen von Campusverträgen vom ZID zur Verfügung gestellt werden, fragen die Lizenzen bei einem zentralen Lizenzserver im ZID ab. Damit diese Abfrage funktioniert, müssen die entsprechenden Ports auf der Firewall geöffnet werden. Dies ist kein Problem, solange die Kommunikation über fest vorgegebene Ports läuft. Der oft verwendete Lizenzmanager FLEXlm [30] erlaubt diese fixe Einstellung.

Trotzdem ist es uns passiert, dass AVS eines Tages nicht mehr laufen wollte, da es keine Lizenz mehr erhielt. Patran hingegen funktionierte weiter klaglos. Was war passiert? Eine Stromabschaltung im gesamten Freihaus der TU und damit auch im ZID erforderte die Abschaltung des Lizenzservers. Nach dem erneuten Hochfahren wurden auch die Lizenzserver mit den vorgegebenen Ports neu gestartet. AVS und Patran verwenden zur Abfrage der Lizenz aber nicht nur einen Port (der bei FLEXlm vorgegeben werden kann), sondern zwei. Der zweite hat sich bei Patran (zufällig?) nicht geändert, bei AVS aber sehr wohl, wie eine Analyse mit tcpdump [31] gezeigt hat. Nachdem der neue Port geöffnet war, konnte AVS auch wieder gestartet werden.

Auch wenn die Firewall sonst die problemloseste Maschine in unserem Subnetz ist, solche Schwierigkeiten sind nur mit einiger Erfahrung (zu der vielleicht auch dieser Artikel ein wenig beitragen kann) und mit Hilfe geeigneter Tools (wie tcpdump) zu lösen.

5.6 Campus- und Plattform-Software

Die Verteilung von Campus-Software erfolgt zumeist auf zwei Arten:

Windows-Software wird über den swd-Server verteilt, indem man unter Windows das entsprechende Netzlaufwerk verbindet und dann Zugriff auf sämtliche lizenzierte Software hat. Da beim Verbinden des Netzlaufwerks eine Benutzer-Authentifizierung mit Name und Passwort erforderlich ist, ist sichergestellt, dass nur autorisierte Personen Zugriff haben. Damit das funktioniert, müssen auf der Firewall einfach die entsprechenden Ports für SMB/ NetBIOS-Verbindungen geöffnet werden.

Unix-Software wird meist durch NFS-Export der Verzeichnisse auf den entsprechenden Servern zur Verfügung gestellt. Da eine Benutzerauthentifizierung fehlt, muss genau festgelegt werden, welche Rechner die Verzeichnisse mounten dürfen. Da sich alle unsere Rechner mittels Masquerading hinter der Firewall verstecken, müsste als berechtigter Rechner die Firewall in den exports-Listen eingetragen werden. Damit kann aber nicht sichergestellt werden, dass nur berechtigte Maschinen die NFS-Verzeichnisse mounten. Damit ist es auch nicht mehr möglich, etwa Betriebssystemdokumentation auf den Installationsservern zu belassen und nur bei Bedarf mittels automount verfügbar zu machen. Da es für diese Problematik im Moment noch keine universelle Lösung gibt, ist bei jedem Zugriff auf die gewünschte Software Rücksprache mit den Verantwortlichen im ZID notwendig.

6 Zusammenfassung

Unser Netzwerk ist seit vier Monaten im Vollbetrieb und hat unsere Erwartungen bestens erfüllt. Die Firewall und der Fileserver laufen seit Beginn ohne Absturz und auch die Arbeitsplatzrechner verrichten trotz der Doppelbelastung (die vorhandene Rechnerkapazität wird mittlerweile voll genützt) sehr stabil ihren Dienst. Durch die zentrale Speicherung ist die Organisation der Daten stark vereinfacht worden und die regelmäßigen Backups haben die Gefahr von Datenverlust minimiert. Auch das dritte Ziel, die Einbruchsicherheit, haben wir durch die sehr restriktiv konfigurierte Firewall erreicht. Dabei ist es natürlich wichtig, regelmäßig die Sicherheitsbulletins zu lesen (z. B. [32], [33]) und notwendige Patches einzuspielen. Trotz einer starken Erweiterung der Rechnerkapazität hat sich der Administrationsaufwand vereinfacht und ein ausgezeichnetes Umfeld für unsere wissenschaftliche Arbeit geschaffen.

7 Referenzen

[1] W. Scholz, D. Suess, T. Schrefl, J. Fidler, „Micromagnetic simulation of structure-property relations in hard and soft magnets“, Computational Materials Science, 18 (2000) 1-6.

[2] samba - opening windows to a wider world
http://www.samba.org/
http://at.samba.org/samba/samba.html

[3] init.at informationstechnologie GmbH
http://www.init.at/

[4] W. Selos, „Eine einfache Firewall-Lösung“,
ZIDline Nr. 4, Dezember 2000
http://linux.tuwien.ac.at/Firewall.html

[5] SuSE Linux AG
http://www.suse.de/
Mirror: http://gd.tuwien.ac.at/linux/suse.com/

[6] Reiserfs
http://www.namesys.com/

[7] Red Hat, Inc.
http://www.redhat.com/
Mirror: http://gd.tuwien.ac.at/linux/redhat/

[8] API NetWorks Inc.
http://www.alpha-processor.com/
products/up2000-board.shtml

[9] TUNET-Datenbank
http://nic.tuwien.ac.at/tunetdb/

[10] ZID / DI Udo Linauer
http://www.zid.tuwien.ac.at/
mitteilungsblatt/mb02-2001.html#4

[11] Microsoft Support
http://support.microsoft.com/support/kb/articles/
q165/4/03.asp
http://support.microsoft.com/support/kb/articles/
Q166/7/30.asp

[12] DQS - Distributed Queueing System
http://www.scri.fsu.edu/~pasko/dqs.html

[13] Grace
http://plasma-gate.weizmann.ac.il/Grace/

[14] The Beowulf Project
http://www.beowulf.org/
http://buweb.parl.clemson.edu/software.html

[15] The Beowulf Underground
http://buweb.parl.clemson.edu/
http://buweb.parl.clemson.edu/software.html

[16] SSH Communications Security
http://www.ssh.fi/

[17] MindTerm - pure java ssh Client
http://www.mindbright.se/

[18] OpenSSH
http://www.openssh.org/

[19] PuTTY: A Free Win32 Telnet/SSH Client
http://www.chiark.greenend.org.uk/~sgtatham/
putty.html

[20] WinSCP - secure data transmission
http://winscp.vse.cz/

[21] Secure iXplorer - Windows Front End for PSCP
http://www.i-tree.org/ixplorer.htm

[22] SSH Clients für andere Betriebssysteme
http://www.openssh.org/windows.html
http://www.openssh.org/unix.html
http://www.at.openbsd.org/openssh/java.html
http://www.at.openbsd.org/openssh/palmos.html
http://opensores.thebunker.net/pub/mirrors/ssh-faq/
ssh-faq-2.html#ss2.1

[23] Virtual Private Networking
http://www.microsoft.com/technet/win2000/
win2ksrv/reskit/intch09.asp

[24] sendmail.org - Masquerading and Relaying
http://www.sendmail.org/m4/masquerading.html

[25] Online-Katalog des Österreichischen Bibliothekenverbundes
http://bvzr.bibvb.ac.at:4505/ALEPH

[26] Hypertext Webster Gateway at UCSD
http://work.ucsd.edu:5141/cgi-bin/http_webster

[27] „Scientific Applications on Linux“ am Goodie Domain Service der TU Wien
http://gd.tuwien.ac.at:8050/

[28] Squid Web Proxy Cache
http://www.squid-cache.org/

[29] webwasher.com
http://www.webwasher.com/

[30] GLOBEtrotter Software
http://www.globetrotter.com/

[31] tcpdump
ftp://ftp.ee.lbl.gov/tcpdump.tar.Z

[32] CERT Coordination Center
http://www.cert.org/

[33] SANS Global Incident Analysis Center
http://www.sans.org/

CFX-TASCflow Version 2.10 und CFX-TurboGrid Version 1.5

Franz Wingelhofer
Institut für Thermische Turbomaschinen und Energieanlagen
franz.wingelhofer+e313@tuwien.ac.at

Neben den General Purpose CFD-Codes CFX, FIDAP und FLUENT steht seit Ende 2000 auf dem FE-CFD-Cluster (Applikationsserver für Strömungsdynamik und Finite Elemente) auch das leistungsfähige Software-Paket CFX-TASCflow zur Verfügung.

Die beiden auf dem Finite-Volumen-Verfahren basierenden CFD-Codes *CFX* und *FLUENT* finden auf Grund ihrer implementierten Modelle für chemische Reaktionen in erster Linie in der Verfahrenstechnik Verwendung. *FIDAP* hingegen, welches mit Hilfe der Finite-Elemente-Methode das Strömungsfeld berechnet, wird oft eingesetzt, wenn freie Oberflächen auftreten. Das auf dem Finite-Volumen-Verfahren basierende *CFX-TASCflow* wird dagegen oft im allgemeinen Maschinenbau angewendet.

Der Preprocessor *CFX-TurboGrid* und der Postprocessor *CFX-TurboVisualizer* sind speziell auf die Simulation der Strömung durch thermische bzw. hydraulische Turbomaschinen zugeschnitten. Mit diesem Pre- und Postprocessor stellt *CFX-TASCflow* ein umfassendes Werkzeug für die Berechnung und Visualisierung der Strömung durch stillstehende und/oder rotierende dreidimensionale Reihen von Turbomaschinen dar.

Vernetzung des Strömungsgebietes: *CFX-TurboGrid*

Der Preprocessor *CFX-TurboGrid* ist ein auf Turbomaschinen zugeschnittenes Werkzeug zur raschen und qualitativ hochwertigen Vernetzung des zu untersuchenden Strömungsgebietes durch eine Reihe. Für die Netztopologie muss entsprechend dem zu vernetzenden Profil ein vordefiniertes Template ausgewählt werden, dessen Parameter den jeweiligen Profilquerschnitten angepasst werden können. Auch die Vernetzung von Radialspalten ist mit diesem Werkzeug auf einfache Weise möglich. Abbildung 1 zeigt eine Blade-To-Blade-Ansicht einer axialen Turbinenbeschaufelung.

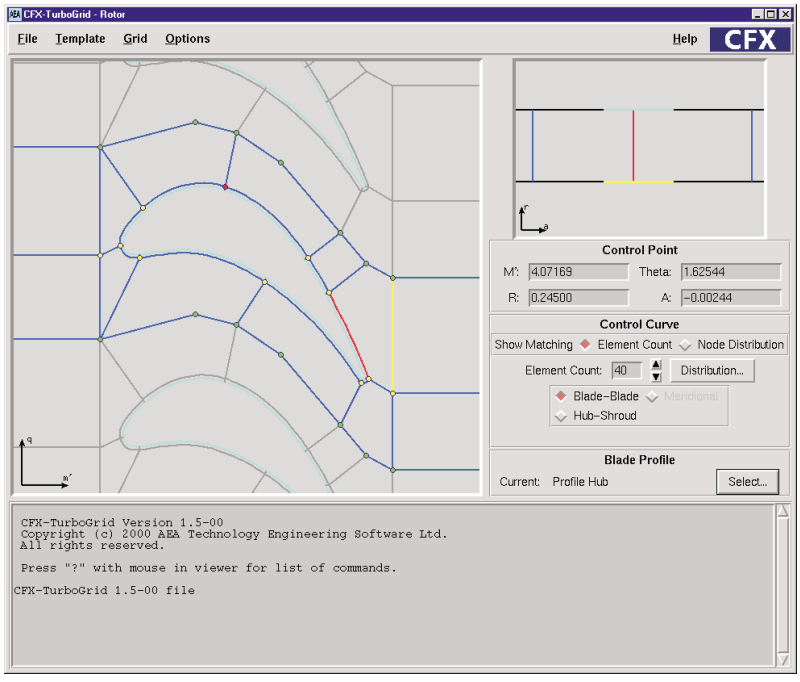


Abbildung 1:
Blade-To-Blade-Ansicht
einer axialen Turbinenbeschaufelung
(*CFX-TurboGrid*)

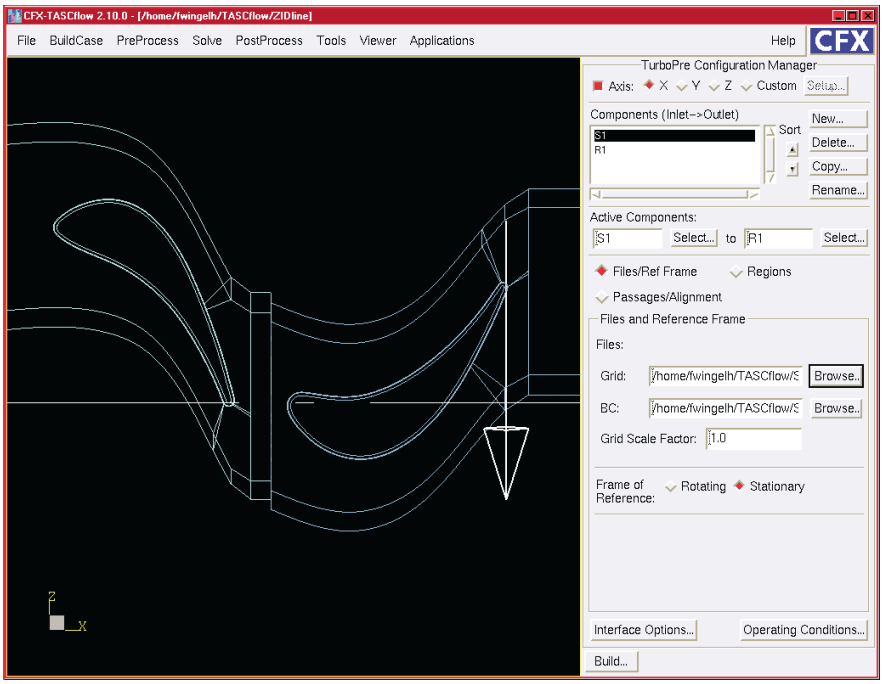


Abbildung 2:
Gesamtnetz für eine Leit- und eine Laufreihe einer axialen Turbinenstufe (*CFX-TASCflow – BuildCase TurboPre*)

Zusammenstellen des gesamten Strömungsbereiches: *CFX-TASCflow - BuildCase TurboPre*

Mit *CFX-TASCflow – BuildCase TurboPre* können die mit *CFX-TurboGrid* erstellten Rechennetze zu einem Gesamtnetz zusammengefasst und die Randbedingungen an den Wänden, am Ein- und Austritt vorgegeben werden. Die Kopplung der zusammengefügten Rechennetze erfolgt problemspezifisch, wobei mehrere Interfaces zur Auswahl stehen. Abbildung 2 zeigt das Gesamtnetz für eine Leit- und eine Laufreihe einer axialen Turbinenstufe.

Solver von *CFX-TASCflow*

Der Solver von *CFX-TASCflow* löst mit Hilfe der Finite-Volumen-Methode die instationäre, dreidimensionale Massen-, Impuls- und nötigenfalls Energiebilanz. Für die Berücksichtigung des turbulenten Charakters der Strömung werden außerdem noch die die Turbulenz beschreibenden instationären, dreidimensionalen Bilanzgleichungen gelöst. Auf Grund der Nichtlinearität der Bilanzgleichungen wird das Strömungsfeld iterativ berechnet. Im Gegensatz zu den meisten anderen CFD-Solvern werden hier die Massen- und Impulsbilanzen simultan gelöst. Dies hat zur Folge, dass eine geringere Anzahl von Iterationsschritten bis zum Erreichen eines Konvergenzkriteriums nötig und die Rechenzeit bei gleicher Genauigkeit kürzer ist.

Für eine hohe Robustheit der Rechnung sorgt die Verwendung eines *algebraic multigrid*-Algorithmus, bei dem das Rechennetz während der Rechnung automatisiert verfeinert bzw. vergröbert wird.

Der Solver kann sowohl inkompressibles als auch kompressibles Fluid simulieren. Durch die optionale Verwendung von Stoffwertdatenbanken können auch Realgase wie zum Beispiel Wasserdampf als Fluid verwendet werden. Ebenso ist die Berechnung von mit dem Strömungsfeld gekoppeltem Wärmeübergang an den Wänden möglich.

Wegen des hohen Stellenwertes der Turbulenz bei der Strömung durch Turbomaschinen wird ein breites Spektrum von Turbulenzmodellen angeboten. Bewährte Turbulenzmodelle wie das Standard-k-ε-Turbulenzmodell sind ebenso verfügbar wie jüngere Turbulenzmodelle wie das RNG-k-ε-Modell, k-ω-Modelle oder Reynolds-Stress-Modelle.

Durch die gleichzeitige Verwendung von ruhenden (Statoren) und rotierenden (Rotoren) Koordinatensystemen, so genannte *multiple frames of reference*, kann eine Stator-Rotor-Interaktion modelliert werden. Die zeitliche Diskretisierung kann wahlweise erster oder zweiter Ordnung genau erfolgen.

Postprocessing: *CFX-TurboVisualizer und CFX-TASCtool*

Der Postprocessor *CFX-TurboVisualizer* ist wie der Preprocessor *CFX-TurboGrid* ein auf Turbomaschinen zugeschnittenes Werkzeug für die Darstellung der Berechnungsergebnisse. Mit *CFX-TurboVisualizer* können dreidimensionale Ansichten, Blade-To-Blade-Ansichten und Meridianansichten interaktiv über ein GUI erstellt werden.

Neben dem interaktiven Postprocessing über ein GUI kann das Postprocessing auch zeilenorientiert mit *CFX-TASCtool* durchgeführt werden. Im zeilenorientierten Postprocessing können auf einfache Weise neue Größen berechnet, oft verwendete Befehlssequenzen in Macros zusammengefasst und Teile des Postprocessings automatisiert abgearbeitet werden. Abbildung 3 zeigt die Verteilung des statischen Druckes an der Nabe, an der Leit- und der Laufreihe einer axialen Turbinenstufe.

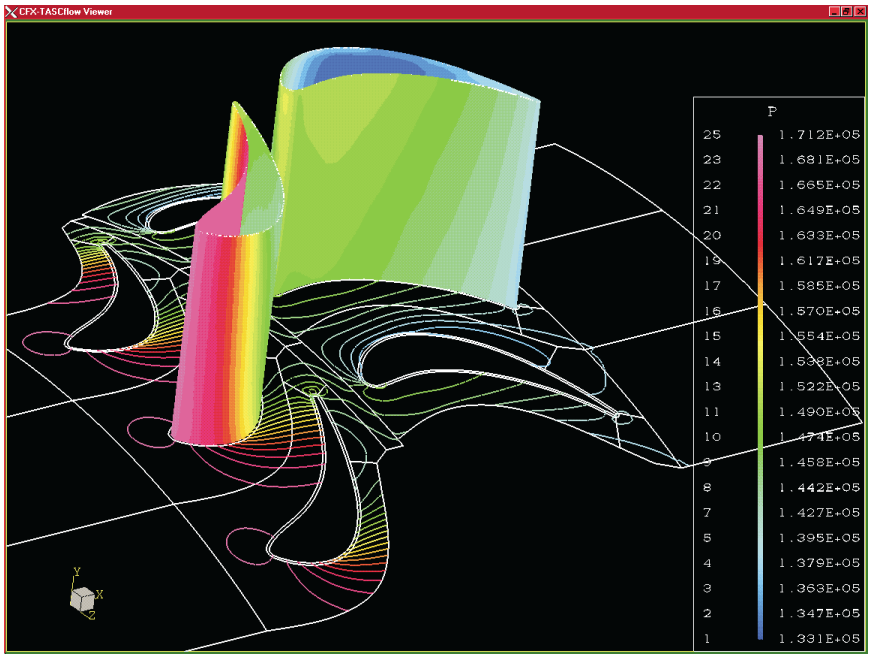


Abbildung 3:
Verteilung des statischen Druckes
in einer axialen Turbinenstufe
(*CFX-TASCtool*)

Fazit

Gemeinsam mit dem Preprocessor *CFX-TurboGrid* und dem Postprocessor *CFX-TurboVisualizer* stellt *CFX-TASCflow* ein umfassendes Werkzeug für die Berechnung und Visualisierung der Strömung durch stillstehende und/ oder rotierende dreidimensionale Reihen von thermischen bzw. hydraulischen Turbomaschinen dar. Auf Grund der Verwendung eines *algebraic multigrid*-Algorithmus und des simultanen Lösens von Massen- und Impulsbilanzen kann das Strömungsfeld in im Vergleich zu anderen CFD-Codes kurzer Rechenzeit mit ausreichender Genauigkeit berechnet werden.

Referenzen

AEA Technology:
http://www.software.aeat.com/cfx/

Online-Dokumentation am FE-CFD-Cluster:
CFX-TASCflow:
/appl/local/tascflow/TASCflow/Doc

CFX-TurboGrid:
/appl/local/turbogrid/Doc

Betriebs- und Benutzungsordnung des Zentralen Informatikdienstes (ZID) der Technischen Universität Wien

Senatsbeschluss vom 25. April 2001

Aufgaben

§ 1. (1) Der ZID ist eine Dienstleistungseinrichtung gemäß § 75 UOG 1993. Die Aufgaben des ZID sind im § 77 UOG 1993 und in der Satzung der Technischen Universität Wien festgelegt.

Funktionen

§ 2. (1) Zur Koordinierung der Angelegenheiten der Informationstechnologie hat der ZID insbesondere folgende Funktionen wahrzunehmen:

- Erfassung des zukünftigen Informatikbedarfes;
- Erstellung mittelfristiger Konzepte und Vorhabensplanungen für den Bereich der Informationstechnologie einschließlich der Netz- und Systemsicherheit;
- Festlegung von Standards und Prozeduren zur Sicherstellung von Kompatibilität, Konnektivität, Interoperabilität, Netz- und Systemsicherheit.

(2) Die Planung, Schaffung und Sicherstellung einer leistungsfähigen Infrastruktur für die Informations- und Datenverarbeitung der Universitätseinrichtungen umfasst insbesondere folgende Informatikeinrichtungen:

- Rechnersysteme und Software im zentralen Bereich;
- Datennetz- und Telekommunikationseinrichtungen bis zur Anschlussdose;
- das zentrale Telefonsystem inklusive Endgeräte;
- zentrale Interneträume für Studierende;
- Campuslizenzen.

(3) Der ZID hat insbesondere folgende Dienste zu erfüllen:

- Beratung und Unterstützung aller Universitätseinrichtungen bei Planung, Beschaffung und Betrieb von Informatikeinrichtungen für Forschung, Lehre und Verwaltung;
- Beratung der Universitätsangehörigen in allen Belangen der Informationstechnologie;
- Erteilung von Benutzungsbewilligungen und Zuteilung von Informatikressourcen an zentralen Servern des ZID;
- Software-Verteilung;
- Unterstützung von dezentralen Systemen;
- Netzdienste;
- Telekommunikationsdienste;
- Internetzugang.

(4) Der ZID hat als Dienstleistungseinrichtung entsprechend den zur Verfügung gestellten personellen und wirtschaftlichen Ressourcen die Anforderungen und Bedürfnisse aller Kunden nach zeitgemäßen Servicestandards zu befriedigen.

Kunden

§ 3. (1) Kunden des ZID sind die Universitätsangehörigen gemäß § 19 UOG 1993 und weitere Angehörige von Universitätseinrichtungen, soweit sie Informatikeinrichtungen und Dienste des ZID verwenden, sowie jene Personen außerhalb der Technischen Universität Wien, für die ein Benutzungsverhältnis über Informatikeinrichtungen oder Dienste des ZID aufgrund gesonderter Vereinbarungen nach § 3 (2) besteht.

(2) Nach Maßgabe vorhandener Kapazität können entsprechend vom Rektor getroffener Vereinbarungen auch Mitarbeiter anderer Universitäten, Hochschulen, Ministerien und der Akademie der Wissenschaften sowie deren Einrichtungen Informatikeinrichtungen und Dienste des ZID in Anspruch nehmen.

(3) Vereinbarungen über die Inanspruchnahme von Informatikeinrichtungen und Diensten des ZID werden für Angehörige von Universitätseinrichtungen mit dem Leiter der betreffenden Universitätseinrichtung getroffen.

Benutzungsbewilligung

§ 4. (1) Angehörige der Technischen Universität Wien gemäß § 19 UOG 1993 haben zur Erfüllung ihrer Aufgaben gemäß § 1 UOG 1993 Anspruch auf die Benützung der Informatikeinrichtungen und der Dienste des ZID.

(2) Für bestimmte Leistungsbereiche oder für abgrenzbare Projekte benötigen alle Kunden des ZID eine vom ZID erteilte Benutzungsbewilligung, die auf schriftliche Anmeldung erteilt wird. Ressourcenbedarf in einem besonderen qualitativen oder quantitativen Ausmaß ist angemessen zu begründen.

(3) Eine Benutzungsbewilligung endet mit Abschluss des entsprechenden Projektes, durch Beendigung der Universitätszugehörigkeit, durch Abmeldung oder Entzug der Benutzungsbewilligung oder durch Ruhen der Nutzung von Services über einen Zeitraum von mindestens einem halben Jahr. Mit Ende der Benutzungsbewilligung werden alle gespeicherten Daten des Kunden gelöscht. Die Universitätseinrichtung des jeweiligen Kunden ist vor der beabsichtigten Löschung zu benachrichtigen.

(4) Eine Benutzungsbewilligung kann mit Begründung eingeschränkt, verweigert oder vom Nachweis spezieller Fachkenntnisse abhängig gemacht werden.

(5) Kunden, die ihnen zugeteilte Ressourcen für andere als die in der Benutzungsanmeldung beschriebenen Aufgaben verwenden oder eine projektfremde Verwendung verursachen, wird die Benützungsbewilligung durch den Leiter des ZID entzogen. Dies kann auch dann erfolgen, wenn ein Kunde Informatikressourcen in einer störenden Weise beansprucht oder Betriebsmittel nicht nach den Grundsätzen der Wirtschaftlichkeit, Sparsamkeit und Zweckmäßigkeit verwendet.

(6) Über Einsprüche gegen die Beschränkung, Verweigerung oder Entziehung der Benutzungsbewilligung entscheidet der Rektor nach Anhörung des Leiters des ZID.

Rechte und Pflichten

§ 5. (1) Die Kunden und die Mitarbeiter des ZID sind zur Einhaltung der Bestimmungen dieser Betriebs- und Benutzungsordnung und der gemäß § 11 veröffentlichten ergänzenden Richtlinien und Benutzungsregelungen verpflichtet. Dienstverrichtungen zum Zweck der Sicherheit und des Datenschutzes haben Vorrang vor anderen Aufgaben.

(2) Der Kunde trägt die volle Verantwortung für die Verwendung der Benutzungsbewilligung. Eine Weitergabe an andere Personen ist nicht zulässig.

(3) Werden Kopien von Programmen und Daten, die der ZID dem Kunden zur Verfügung stellt, widerrechtlich angefertigt, haftet der Kunde gegenüber dem Lizenzgeber oder Eigentümer.

(4) Die Kunden haben die Einrichtungen des ZID jeweils so zu hinterlassen, dass danach eine weitere ordnungsgemäße Benützung durch andere möglich ist.

(5) Der Kunde erklärt sich bereit, bei der Untersuchung von unzulässigen Verwendungen oder Schäden an Informatikeinrichtungen, den ZID und Organisationen, die dabei mit dem ZID zusammenarbeiten, zu unterstützen.

(6) Beim Anschluss von Informatikeinrichtungen an die zentrale Kommunikationsinfrastruktur durch den Kunden sind die technischen Spezifikationen und Vorgaben des ZID zu erfüllen.

(7) Die Öffnung des Netzzuganges für andere als die in § 3 genannten Kunden („Dritte“) ist nicht gestattet. Eine Nutzung des Netzes durch Dritte liegt im allgemeinen dann vor, wenn diese über die vom ZID bereitgestellten Informatikeinrichtungen nationale und internationale Netze und Netzdienste erreichen, bzw. wenn auf Informatikeinrichtungen der Universität Informationsdienste für Dritte betrieben werden.

(8) Der ZID hat die Kunden regelmäßig ausreichend zu informieren. Abweichungen vom Normalbetrieb (wie z. B. Abschaltungen, Umstellungen, Wartungsarbeiten) sind den Kunden möglichst frühzeitig mitzuteilen.

Verwaltungsübertragung von Informatikeinrichtungen

§ 6. (1) Der ZID kann Informatikeinrichtungen einem Kunden vorübergehend zur Verwaltung übertragen. Der ZID kann Informatikeinrichtungen von Kunden auf deren Antrag zur Verwaltung übernehmen. Voraussetzung für eine Verwaltungsübertragung ist die Gewährleistung der Erfüllung der Aufgaben des ZID. Die Übernahme bedarf der Schriftform und hat die genaue Gerätebezeichnung, den Aufstellungsort, den Umfang der Betreuung und die Dauer der Übernahme zu enthalten.

Zuteilung von Informatikressourcen

§ 7. (1) Die Informatikeinrichtungen und Betriebsmittel werden vom ZID nach Maßgabe der bewilligten Budgetmittel zur Verfügung gestellt.

Verrechnung von Leistungen

§ 8. (1) Der ZID kann für Dienstleistungen im Rahmen einschlägiger Benutzungsregelungen (§ 11) eine Kostenbeteiligung verrechnen. Die Höhe der Kostenersätze ist in geeigneter Form bekanntzumachen. Die Verrechnung erfolgt auf die jeweiligen Kostenstellen des ZID.

Datensicherung

§ 9. (1) Der ZID führt in periodischen Abständen Datensicherungsläufe für die auf seinen zentralen Servern gespeicherten Daten durch. Diese Form der Datensicherung beinhaltet, dass nach aufgetretenen Fehlern die Informationen (Dateien) von den Sicherungsbeständen des ZID rekonstruiert werden können. Darüber hinausgehende Sicherungen und Archivierungen sind von den Kunden selbst in eigener Verantwortung durchzuführen.

Beratendes Gremium für IT-Angelegenheiten und IT-Kontaktpersonen

§ 10. (1) Zur Unterstützung der notwendigen Kommunikation zwischen den Fakuläten und dem ZID wird ein beratendes Gremium für IT-Angelegenheiten eingerichtet. Es besteht aus zwei vom Senat entsandten Mitgliedern und je einem Mitglied aus den einzelnen Fakultäten, das vom Dekan entsandt wird. Aus dem Senat ist je ein Mitglied aus dem Kreis der Studierenden und eines aus der Fakultät für Technische Naturwissenschaften und Informatik zu entsenden. Dieses Gremium ist mindestens viermal im Jahr vom Vorsitzenden des Beirates einzuberufen.

(2) Die Leiter der Universitätseinrichtungen benennen zur Unterstützung der notwendigen Kommunikation mit dem ZID eine Mitarbeiterin oder einen Mitarbeiter als IT-Kontaktperson.

Ergänzende Richtlinien und Benutzungsregelungen

§ 11. (1) Einschlägige Benutzungsregelungen (Policies) für spezielle Informatikeinrichtungen des ZID (z. B. Datennetzinfrastruktur, Telefonanlage, Security Policy, ...) sowie spezielle Richtlinien für Dienstleistungen des ZID und für Datensicherheitsmaßnahmen werden nach Vorschlag des Leiters des ZID vom Rektor erlassen und im Mitteilungsblatt der Technischen Universität Wien veröffentlicht.

Personelle Veränderungen

In Memoriam Günter Vollmann

Völlig unerwartet ist unser Freund und Kollege **Günter Vollmann** am 19. Dezember 2000 im 57. Lebensjahr verstorben.

Geboren am 13. 10. 1944 in Wien, begann er 1966 als Operator der Rechenanlage IBM 7040 am Institut für Numerische Mathematik der TU Wien bei Prof. Stetter.

Unser „Gundi“, wie wir ihn alle nannten, hat die Entwicklung der EDV an der TU Wien von den ersten Anfängen aus mitverfolgt und begleitet.

In den Jahren der „Lochkarten-EDV“ stand er den Studenten sowie den Kolleginnen und Kollegen der TU Wien mit Rat und Tat zur Seite, wenn es galt, einen Locher zu reparieren, den Papiersalat im Drucker zu beheben oder einige hundert Lochkarten neu zu sortieren.

In diese Zeit fallen auch seine sportlichen Höhepunkte: Faustball war sein Leben, Meisterschaftsspiele im In- und Ausland, Spiele in der österreichischen Nationalmannschaft bestimmten nachhaltig sein Leben.

1975 wurde Günter Vollmann Chefoperator an den neuen Rechenanlagen von CDC und wurde zusammen mit einigen Kollegen und mir Mitte 1976 in den Personalstand des neuen IEZ übernommen.

Im Herbst 1988 feierten wir die Vollendung des 25. Dienstjahres im öffentlichen Dienst, Anfang 1991 wurde Günter Vollmann nach der Reorganisation und Zusammenlegung der Abteilungen Digital-, Hybrid- und Prozeßrechenanlage sowie des IEZ in den Personalstand des neuen EDV-Zentrums der TU Wien übernommen.

In einer stillen Feier im Krematorium am Zentralfriedhof haben wir ihm am 28. 12. 2000 das letzte Geleit gegeben.

Lieber Günter, wir werden Dich immer in Erinnerung behalten.

Peter Berger

Veränderungen im Referat Internet-Räume

Am 15. April 2001 wechselte Herr **Dipl.-Ing. Gerhard Schmitt** an die Universität für Angewandte Kunst und übernahm dort den Posten des Leiters des Zentralen Informatikdienstes.

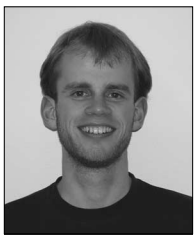
Herr Gerhard Schmitt war über 25 Jahre an der TU Wien beschäftigt und leitete ab 1992 das Referat Internet-Räume (vormals Benutzerräume).

Wir wünschen ihm auf seinem weiteren Weg viel Erfolg und alles Gute.

Herr **Dipl.-Ing. Martin Rathmayer** wechselt aus dem Bereich der Systemadministration in dieses Referat und übernimmt die Referatsleitung (E-Mail: rathmayer@zid.tuwien.ac.at, Nebenstelle 42086).

Herr **Michael Roth** arbeitet seit 6. Dezember 2000 halbtags als PC-Techniker am ZID (E-Mail: roth@zid.tuwien.ac.at, Nebenstelle 42091). Er ist im Bereich Internet-Räume vor allem für die Hardwarebetreuung der PC-Arbeitsplätze zuständig.

Herr **Philipp Kolmann** unterstützt seit Anfang Mai halbtags die Abteilung Zentrale Services im Bereich der zentralen Applikationsserver.



Seit Anfang April 2001 ist Herr **Tilman Linneweh** in der Abteilung Kommunikation tätig. Sein Hauptaufgabengebiet ist der Bereich Hardware-Wartung und -Fehlersuche sowie Installation im Access-Bereich des TUNET.

Wir wünschen allen neuen Mitarbeitern viel Erfolg und Freude bei ihrer Tätigkeit!

Frau **Dipl.-Ing. Elisabeth Donnaberger** verlässt nach mehr als 3 Jahren Tätigkeit leider den Zentralen Informatikdienst mit Anfang Juni. Frau Donnaberger war in ihrer Tätigkeit für die Abteilung Standardsoftware unter anderem für den Software Server verantwortlich und hat in dieser Aufgabe erfolgreich dazu beigetragen, dass das Campus Software Service hochverfügbar den Kunden zur Verfügung steht. In der Abteilung Kommunikation war sie für die White Pages und den Mailrouter zuständig und von dieser Tätigkeit her sicher vielen bekannt.
Alle Mitarbeiter wünschen ihr weiterhin alles Gute.

Server-Zertifikate des Zentralen Informatikdienstes

TU Testzertifizierungsstelle:
`http://www.zid.tuwien.ac.at/security/testca/`

Fingerprints der Test-CAs und der von ihnen ausgegebenen Serverzertifikate:

Zertifikat der Root-Test-CA (PCA)
gültig von Dec 30 1999 bis Dec 26 2014
`0D:D9:02:9C:24:61:85:9E:72:59:93:28:68:3D:B3:7C`

Zertifikat der Server-Test-CA (SCA)
gültig von Dec 30 1999 bis Dec 27 2009
`03:2F:CB:C6:B6:5B:FC:00:C0:56:41:DF:CD:E9:AF:98`

Zertifikat der User-Test-CA (UCA)
gültig von Dec 30 1999 bis Dec 27 2009
`3C:B3:AC:1F:83:D0:C9:1E:3E:11:31:53:A0:F3:C9:88`

Server-Zertifikat von stud3.tuwien.ac.at
gültig von Nov 20 2000 bis Nov 20 2001
`MD5 Fingerprint=`
`04:CE:1E:67:57:EB:80:A0:C1:EB:0D:11:05:12:52:99`

Server-Zertifikat von stud4.tuwien.ac.at
gültig von Nov 20 2000 bis Nov 20 2001
`MD5 Fingerprint=`
`DB:47:20:4A:A7:90:DE:5D:D5:2B:6C:BD:CF:02:D2:21`

Server-Zertifikat von fbma.zserv.tuwien.ac.at
gültig von Dec 5 2000 bis Dec 5 2001
`MD5 Fingerprint=`
`13:4C:C2:ED:7E:6A:F7:1D:24:48:D6:FB:5D:9E:00:DA`

Server-Zertifikat von mail.zserv.tuwien.ac.at
gültig von Dec 5 2000 bis Dec 5 2001
`MD5 Fingerprint=`
`89:10:25:A0:C1:5C:E7:30:D2:38:7C:5E:9C:40:ED:E2`

Server-Zertifikat von studman.ben.tuwien.ac.at
gültig von Jan 18 2001 bis Jan 18 2002
`MD5 Fingerprint=`
`9F:DD:07:6D:73:5E:9C:E6:51:62:4E:D7:53:4B:46:E6`

Server-Zertifikat von swd.tuwien.ac.at
gültig von May 10 2001 bis May 25 2002
`MD5 Fingerprint=`
`88:08:46:AB:A8:B9:78:AA:35:EE:6B:AA:6A:CC:B4:20`

Fingerprints von „TC TrustCenter Class 2 CA“:

Server-Zertifikat von
info.tuwien.ac.at (Informationsserver für die TU Wien)
gültig von Mar 27 2001 bis Mar 27 2002
`MD5 Fingerprint=`
`90:F4:99:B5:6B:DC:71:D8:81:EE:CB:24:0E:03:19:4C`

Fingerprints der „self signed“ Serverzertifikate:

Server-Zertifikat von
iu.zid.tuwien.ac.at (Campussoftware Verwaltung)
gültig bis Mar 1 2002

`A0:FF:97:E3:25:5D:07:B9:20:CC:84:D6:88:05:EB:0F`

Öffnungszeiten

Sekretariat

Freihaus, 2. Stock, gelber Bereich

Montag bis Freitag, 8 Uhr bis 13 Uhr

- Ausgabe und Entgegennahme von Formularen für Benutzungsbewilligungen für Rechner des ZID,
- Internet-Service für Studierende: Vergabe von Benutzungsbewilligungen, die nicht automatisch erteilt werden können,
- allgemeine Beantwortung von Benutzeranfragen, Weiterleitung an fachkundige Mitarbeiter.

Telefonische Anfragen: 58801-42001

Internet-Räume

Die Internet-Räume (in den Gebäuden Karlsplatz, Freihaus, Gußhausstraße, Treitlstraße, Gumpendorferstraße, Bibliothek, Favoritenstraße) sind im Regelfall entsprechend den Öffnungszeiten des jeweiligen Gebäudes geöffnet. An Sonn- und Feiertagen ist kein Betrieb. Siehe auch
`http://www.ben.tuwien.ac.at/InternetRaeume/`

Operator-Ausgabe

Freihaus, 2. Stock, roter Bereich
Montag bis Freitag, 7 Uhr 30 bis 20 Uhr

- Ausgabe für Farbdrucker.
- Passwortvergabe für das Internet-Service für Studierende.
- Ausgabe diverser Informationen für Studierende, Weiterleitung von Anfragen an fachkundige Mitarbeiter.

Wählleitungen

01 / 589 32	**Normaltarif**
07189 15893	**Online-Tarif** (50 km um Wien)

Datenformate:
300 - 56000 Bit/s (V.90)
MNP5/V.42bis
PPP
ISDN Synchronous PPP

Auskünfte, Störungsmeldungen

Sekretariat
Tel.: 58801-42001
E-Mail: sekretariat@zid.tuwien.ac.at

TUNET

Störungen
Tel.: 58801-42003
E-Mail: trouble@noc.tuwien.ac.at

Rechneranmeldung
E-Mail: hostmaster@noc.tuwien.ac.at

Telekom
Hotline: 08
(8.00-12.00 und 13.00-15.00 Uhr, nur innerhalb der TU)
E-Mail: telekom@noc.tuwien.ac.at
Chipkarten, Abrechnung: 58801-42008

Netz- und Systemsicherheit
E-Mail: security@tuwien.ac.at

Service-Line Abt. Standardsoftware
Tel.: 58801-42004

Systemunterstützung
Computer Help Line 42124
Web: sts.tuwien.ac.at/pss/

Campussoftware
E-Mail: campus@zid.tuwien.ac.at
gd@zid.tuwien.ac.at

Zentrale Server, Operating
Tel.: 58801-42005
E-Mail: operator@zid.tuwien.ac.at

Internet-Räume
Tel.: 58801-42006
E-Mail: studhelp@zid.tuwien.ac.at

Personalverzeichnis

Telefonliste, E-Mail-Adressen

Zentraler Informatikdienst (ZID)
der Technischen Universität Wien
Wiedner Hauptstraße 8-10 / E020
A - 1040 Wien
Tel.: (01) 58801-42000 (Leitung)
Tel.: (01) 58801-42001 (Sekretariat)
Fax: (01) 58801-42099
Web: http://www.zid.tuwien.ac.at/

Leiter des Zentralen Informatikdienstes:

W. Kleinert	42010	kleinert@zid.tuwien.ac.at

Administration:

A. Müller	42015	mueller@zid.tuwien.ac.at
M. Grebhann-Haas	42018	grebhann-haas@zid.tuwien.ac.at

Öffentlichkeitsarbeit

I. Husinsky	42014	husinsky@zid.tuwien.ac.at

Netz- und Systemsicherheit

U. Linauer	42026	linauer@zid.tuwien.ac.at

Abteilung Zentrale Services

http://www.zid.tuwien.ac.at/zserv/

Leitung

P. Berger	42070	berger@zid.tuwien.ac.at
W. Altfahrt	42072	altfahrt@zid.tuwien.ac.at
J. Beiglböck	42071	beiglboeck@zid.tuwien.ac.at
C. Bojer	42083	bojer@zid.tuwien.ac.at
P. Deinlein	42074	deinlein@zid.tuwien.ac.at
P. Egler	42094	egler@zid.tuwien.ac.at
H. Eigenberger	42075	eigenberger@zid.tuwien.ac.at
H. Flamm	42092	flamm@zid.tuwien.ac.at
W. Haider	42078	haider@zid.tuwien.ac.at
E. Haunschmid	42080	haunschmid@zid.tuwien.ac.at
P. Kolmann	42095	kolmann@zid.tuwien.ac.at
F. Mayer	42082	fmayer@zid.tuwien.ac.at
J. Pfennig	42076	pfennig@zid.tuwien.ac.at
M. Rathmayer	42086	rathmayer@zid.tuwien.ac.at
M. Roth	42091	roth@zid.tuwien.ac.at
J. Sadovsky	42073	sadovsky@zid.tuwien.ac.at
A. Schulz	42081	schulz@zid.tuwien.ac.at
E. Srubar	42084	srubar@zid.tuwien.ac.at
Werner Weiss	42077	weisswer@zid.tuwien.ac.at

Abteilung Kommunikation

http://nic.tuwien.ac.at/

Leitung

J. Demel	42040	demel@zid.tuwien.ac.at
S. Beer	42061	beer@zid.tuwien.ac.at
F. Blöser	42041	bloeser@zid.tuwien.ac.at
G. Bruckner	42046	bruckner@zid.tuwien.ac.at
S. Dangel	42066	dangel@zid.tuwien.ac.at
T. Eigner	42052	eigner@zid.tuwien.ac.at
S. Geringer	42065	geringer@zid.tuwien.ac.at
J. Haider	42043	jhaider@zid.tuwien.ac.at
M. Hanold	42062	hanold@zid.tuwien.ac.at
P. Hasler	42044	hasler@zid.tuwien.ac.at
S. Helmlinger	42063	helmlinger@zid.tuwien.ac.at
H. Kainrath	42045	kainrath@zid.tuwien.ac.at
J. Klasek	42049	klasek@zid.tuwien.ac.at
W. Koch	42053	koch@zid.tuwien.ac.at
T. Linneweh	42055	linneweh@zid.tuwien.ac.at
I. Macsek	42047	macsek@zid.tuwien.ac.at
F. Matasovic	42048	matasovic@zid.tuwien.ac.at
W. Meyer	42050	meyer@zid.tuwien.ac.at
R. Vojta	42054	vojta@zid.tuwien.ac.at
Walter Weiss	42051	weiss@zid.tuwien.ac.at

Abteilung Standardsoftware

http://sts.tuwien.ac.at/

Leitung

A. Blauensteiner	42020	blauensteiner@zid.tuwien.ac.at
C. Beisteiner	42021	beisteiner@zid.tuwien.ac.at
J. Donatowicz	42028	donatowicz@zid.tuwien.ac.at
G. Gollmann	42022	gollmann@zid.tuwien.ac.at
M. Holzinger	42025	holzinger@zid.tuwien.ac.at
A. Klauda	42024	klauda@zid.tuwien.ac.at
H. Mastal	42079	mastal@zid.tuwien.ac.at
H. Mayer	42027	mayer@zid.tuwien.ac.at
E. Schörg	42029	schoerg@zid.tuwien.ac.at
R. Sedlaczek	42030	sedlaczek@zid.tuwien.ac.at
W. Selos	42031	selos@zid.tuwien.ac.at
B. Simon	42032	simon@zid.tuwien.ac.at
A. Sprinzl	42033	sprinzl@zid.tuwien.ac.at
P. Torzicky	42035	torzicky@zid.tuwien.ac.at