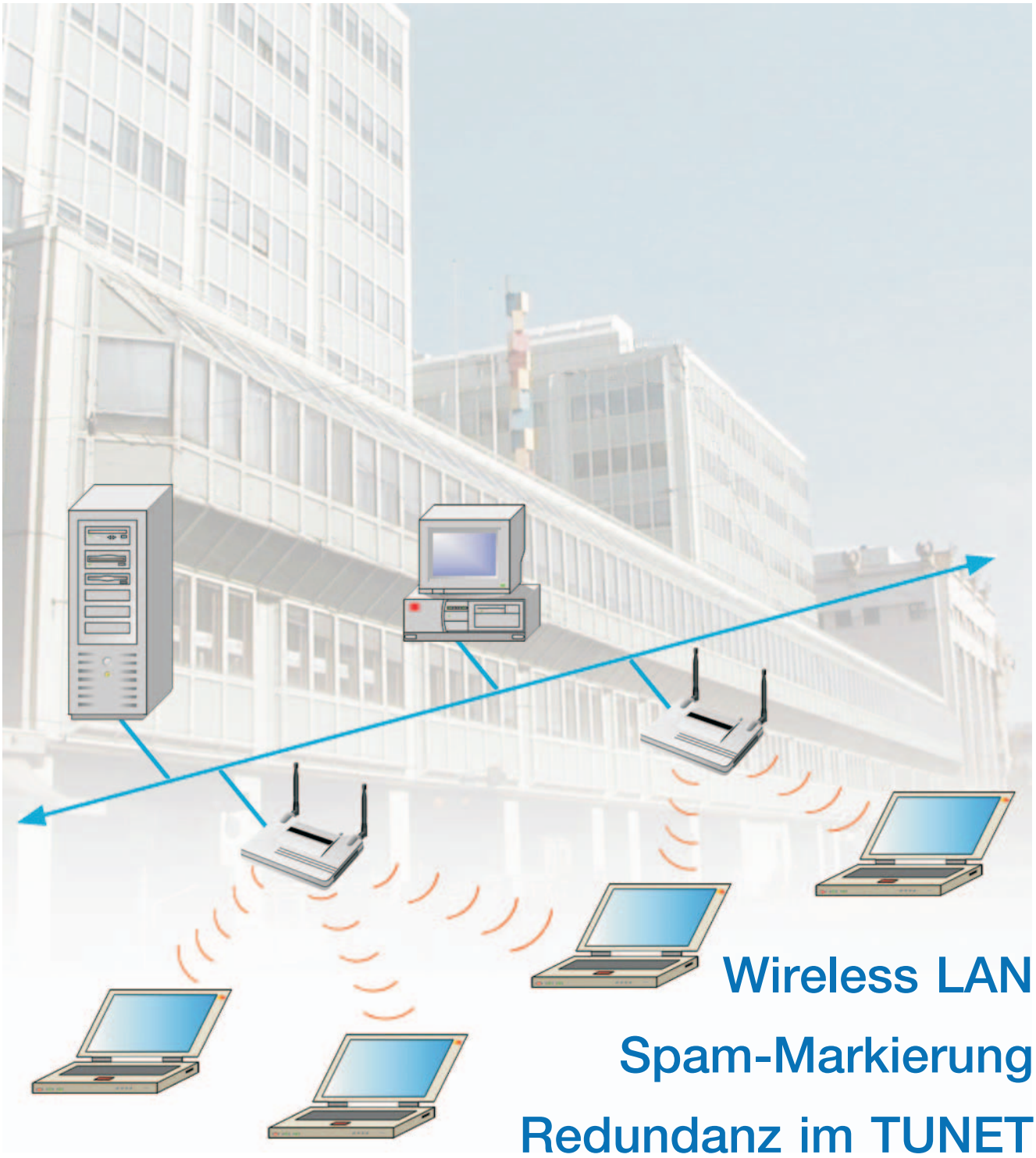
Nr. 8 / Juni 2003

ISSN 1605-475X

ZID line

INFORMATIONEN DES ZENTRALEN INFORMATIKDIENSTES DER TU WIEN



Wireless LAN

Spam-Markierung

Redundanz im TUNET

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.zid.tuwien.ac.at/zidline/

Erstellt mit Corel Ventura
Druck: Grafisches Zentrum an der TU Wien,
1040 Wien, Tel.: (01) 5863316

Editorial

Dass das TUNET, das Netz der TU Wien, 24 Stunden am Tag, 7 Tage in der Woche – obwohl das Personal nur einen Bruchteil davon anwesend ist – reibungslos funktioniert, wird als selbstverständlich angenommen. Jede geringste Störung ist eine Beeinträchtigung der Arbeit der TU-Angehörigen. In dieser ZIDline bekommen Sie einen Einblick, was da alles dahintersteckt, um täglich die Betriebsbereitschaft zu gewährleisten.

Im Gebäude Freihaus und in der Bibliothek wurde begonnen, ein Funknetz für einen kabellosen Netzzugang einzurichten. Hier sind besonders Sicherheitsaspekte bei der Verwendung zu beachten.

Von der Belästigung durch Spam-Mails sind bereits alle betroffen. Diverse Anti-Spam-Maßnahmen werden zurzeit viel diskutiert. Wir bieten als Hilfe eine Markierung von vermutlichen Spam-Mails durch die zentralen Mailserver an, dann kann der Empfänger weitere Entscheidungen treffen.

Die TU Wien bietet als einzige Universität in Österreich ihren Studierenden wichtige Software zu unschlagbar günstigen Preisen an. Lesen Sie ab Seite 24, welche Produkte angeboten werden und wie sie sich verkaufen.

Die PC-Arbeitsplätze in den Internet-Räumen des ZID können in den vorlesungsfreien Zeiten als Internet-Zugang für Teilnehmer von wissenschaftlichen Tagungen benützt werden. Welche Services geboten werden und wie die Reservierung erfolgt, lesen Sie in dieser ZIDline.

An einer Universität sind oft umfangreiche technische Publikationen zu erstellen. Wir bringen dazu einen Kommentar eines Wissenschaftlers zu Scientific WorkPlace und stellen DTP-Programme aus der Campussoftware vor – ganz nach dem Motto „Es muss nicht immer Word sein“.

Ich bedanke mich sehr herzlich bei allen Autoren für ihre Beiträge und die gute Zusammenarbeit.

Allen Lesern wünsche ich, dass auch diesmal wieder etwas Interessantes für Sie dabei ist.

Irmgard Husinsky

---

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

Wireless LAN an der TU Wien

Tilman Linneweh

Mit der zunehmenden Verbreitung von Laptops steigt die Popularität von drahtloser Kommunikation via Wireless LAN, GPRS, Bluetooth etc. Deshalb baut der Zentrale Informatikdienst derzeit auf dem Campus der Technischen Universität Wien ein Wireless LAN auf, das von allen Angehörigen der TU (Mitarbeitern und Studierenden) genutzt werden kann.

Was ist WLAN?

WLAN steht für „*wireless local area network*" – kabelloses Netzwerk. Der Datenaustausch zwischen dem Computer und anderen Netzwerkkomponenten erfolgt über Funk. Die einfachste Form eines WLAN besteht aus zwei Rechnern mit WLAN Netzwerkkarten und wird als „Adhoc Netzwerk" bezeichnet (siehe Abbildung 1).

Für die Verbindung von einem Wireless LAN mit einem drahtgebundenen LAN wird ein so genannter Accesspoint benötigt. Der Accesspoint ist eine Bridge zwischen den beiden Medien. Mit dem LAN ist er über einen Twisted-Pair Anschluss verbunden, mit dem drahtlosen Endsystem kommuniziert er über eine Antenne.

Durch Einsatz mehrerer Accesspoints kann man die gesamte Fläche, auf der der Netzzugang möglich sein soll, mit überlappenden Zellen versorgen. Dadurch können sich die Anwender mit ihren Notebooks frei bewegen, ohne den Kontakt zum LAN zu verlieren (siehe Abbildung 2).

Da ein Endsystem Pakete von verschiedenen Wireless LANs gleichzeitig empfangen kann, ist im Paket-Header eines WLAN Pakets ein eindeutiger Name vorgesehen, die *SSID* („*Service Set Identifier*"). Diese SSID besteht aus maximal 32 Buchstaben. Damit ein Rechner an einem Wireless LAN teilnehmen kann, muss er die zugehörige SSID kennen. Da die SSID im Klartext eines Pakets mitgesendet wird, bietet die SSID aber keinen Schutz vor unberechtigtem Zugriff auf das WLAN.

Abbildung 1: Schon mit zwei oder mehr drahtlosen Netzwerkkarten lässt sich ein einfaches Wireless LAN aufbauen.

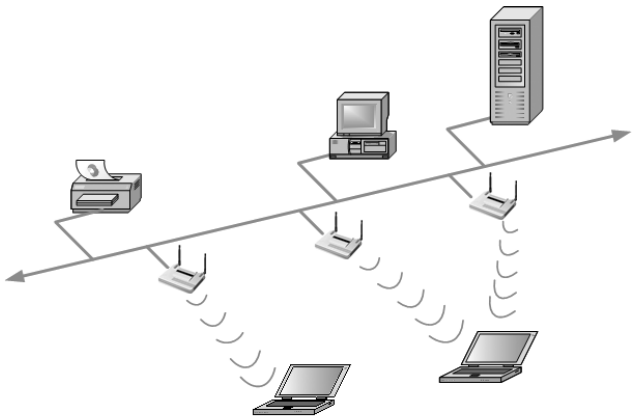


Abbildung 2: Ein Wireless LAN mit Accesspoints

Derzeit gibt es drei verschiedene Standards für Wireless LAN. **802.11b** ist der älteste, verbreitetste Standard und wird derzeit im TUNET Wireless LAN verwendet. 802.11b kompatible Geräte funken mit einer brutto Geschwindigkeit von 11 MBit/s (netto ca. 5.5 MBit/s). Als Frequenz wird das 2,4 GHz Band verwendet, in dem u.a. auch Mikrowellenöfen und Bluetooth funken. Die Abstrahlenergie der Sender ist kleiner als 100mW. Zum Vergleich: Ein Handy sendet mit bis zu 2 Watt. Der Radius des vom Accesspoint abgedeckten Bereichs ist abhängig von den Gebäudestrukturen und schwankt durchschnittlich zwischen 30 und 40 Meter. Mit speziellen Richtantennen und bei Sichtkontakt lassen sich auch größere Reichweiten erzielen.

Der Frequenzbereich (2,400 bis 2,4835 GHz) für 802.11b Wireless LAN ist in Kanäle aufgeteilt. In Europa sind 13 Kanäle zugelassen, in den USA 11.

Diese Kanäle sind allerdings nicht überlappungsfrei, so dass es zu Störungen zwischen Accesspoints auf benachbarten Kanälen kommen kann. Um diese zu vermeiden, werden idealerweise nur 3 Kanäle benutzt, z.B. 1, 6, 11 (siehe Abbildung 3).

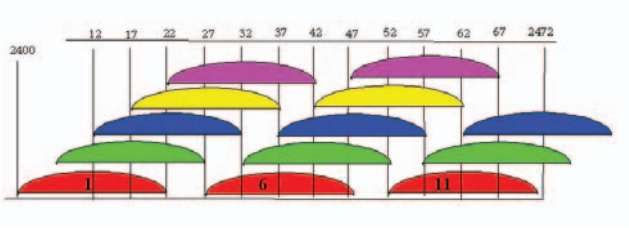


Abbildung 3: Die Kanäle sind überlappend angeordnet

Die Accesspoints sollten nach Möglichkeit so angeordnet sein, dass es keine überlappenden Bereiche zwischen Accesspoints mit gleichem Sendekanal gibt, da dies die maximal verfügbare Bandbreite reduziert.

Durch diese Einschränkungen bezüglich der Platzierung der Accesspoints ist eine vollflächige Versorgung von Gebäuden problematisch (siehe Abbildung 4).

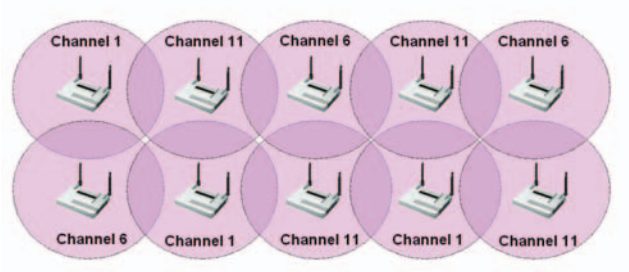


Abbildung 4: Kanalverteilung

Die beiden neueren Standards *802.11a* und *802.11g*, für die jetzt erste Geräte im Handel erhältlich sind, definieren eine höhere Geschwindigkeit von 54 MBit/s brutto (ca. 22 MBit/s netto). 802.11g benutzt ebenfalls das 2.4 GHz Band, 802.11a nutzt hingegen das derzeit noch weitgehend ungenutzte 5 GHz Band.

Der große Nachteil der neuen Standards ist die geringere Reichweite der Accesspoints. Dadurch müssen wesentlich mehr Accesspoints pro Fläche eingesetzt werden, wodurch eine Versorgung mit 54 MBit/s erheblich teurer wird.

Sicherheit im Wireless LAN

Drahtlose Netze sind grundsätzlich leicht abhörbar. Im Gegensatz zum geswitchten Twisted-Pair Netzwerk sind im WLAN die gesendeten Daten im Umkreis des Senders zu empfangen. Die Daten machen so auch nicht vor den Gebäudegrenzen halt und sind somit unter Umständen auch auf der gegenüberliegenden Straßenseite zu empfangen. Neben dem Abhören von Daten im WLAN besteht für einen Angreifer aber auch die Möglichkeit, aktive Angriffe durchzuführen (z.B. Spam versenden, Denial Of Service, Exploits etc.). Angreifer, die von ungesicherten Wireless LANs aus agieren, sind nur schwer identifizierbar !

WEP – Wire Equivalent Security

WEP ist der im Standard 802.11b definierte Sicherheitsmechanismus. Der Accesspoint und alle Rechner im Netzwerk benutzen einen gemeinsamen Schlüssel mit einer Schlüssellänge von 40 bzw. 104 Bit. Dieser Schlüssel wird mit einem 24 Bit Initialisierungsvektor (IV) verlängert. Der Initialisierungsvektor wird im Klartext dem Paket vorangestellt (siehe Abbildung 5).

802.11 Protokoll Header	Initialisierungs-Vektor	Daten	Prüfsumme

Abbildung 5: Aufbau eines 802.11 Pakets

Diese Schlüssellängen sind in der heutigen Zeit zu kurz, alleine mit Brute-Force könnte der gesamte Schlüsselbereich in ca. 45 Tagen von einem herkömmlichen PC berechnet werden.

Durch die Kürze des IV werden außerdem innerhalb kürzester Zeit Pakete mit dem gleichen Schlüssel verschlüsselt. Nutzt ein Angreifer zusätzlich bekannte Schwächen im Schlüsselgenerierungsalgorithmus von herkömmlichen WLAN Karten aus, kann er den Schlüsselbereich auf 21 Bit reduzieren und so innerhalb von 20 – 40 Sekunden den Schlüssel knacken.

Des Weiteren kann ein Angreifer durch Senden von modifizierten Paketen den Accesspoint dazu bringen, Pakete wiederholt zu senden. Dadurch kommt er ohne großen Zeitaufwand an die benötigten Datenmengen, um den Schlüssel zu berechnen.

Ein weiteres Problem neben den Schwächen des WEP Algorithmus ist die Verteilung des WEP Schlüssels. Der gemeinsame Schlüssel muss auf allen Rechnern des Netzwerks installiert werden, was in größeren Netzwerken nicht praktikabel ist.

Verschiedene Hersteller haben zusätzlich proprietäre Protokolle entwickelt, die eine bessere Sicherheit als WEP Verschlüsselung bieten. Diese Protokolle sind in einem heterogenen Umfeld wie beispielsweise in Universitäten nicht geeignet, da sie meist nur mit den Produkten eines Herstellers funktionieren.

VPN – Virtual Private Network

Eine sichere Alternative zur WEP Verschlüsselung ist das Virtual Private Network (VPN). Die genaue Funktionsweise des VPNs wurde ausführlich im Artikel „VPN-Zugang zum TUNET“, ZIDline 7, Oktober 2002 besprochen. Benutzer des TUNET WLANs bekommen automatisch einen separaten VPN-Zugang für das Wireless LAN. Um diesen zu verwenden, ist es notwendig,

sich das entsprechende Profil von der VPN-Webseite `https://nic.tuwien.ac.at/tunet/vpn/download/config/vpn-mobilnetz.zip` im Cisco VPN-Client zu installieren.

Universal Subscriber Gateway

An der TU erfolgt die Authentifizierung der WLAN Benutzer – genauso wie auch die Authentifizierung der TUNET-Anschlüsse in den Hörsälen – über ein Universal Subscriber Gateway (USG).

Das Universal Subscriber Gateway fängt den ersten http-Request ab und leitet den Benutzer auf eine Authentifizierungsseite weiter. Hier kann sich der Benutzer per https authentifizieren, danach wird er für den Verkehr in das TUNET und in das Internet freigeschaltet (siehe Abbildung 6).

Technische Realisierung

Im TUNET WLAN kommen hochwertige Accesspoints der Firma Cisco zum Einsatz. Die ideale Positionierung der Accesspoints im Gebäude wurde von der Fa. Getronics vermessen. Das Wireless LAN ist durch eine eigene Firewall vom TUNET getrennt (siehe Abbildung 6).

Technische Voraussetzungen

Für die Benützung des WLANs wird eine 802.11b kompatible Netzwerkkarte benötigt. Die SSID muss auf „tunet“ eingestellt sein. Im TUNET wird keine WEP Verschlüsselung verwendet, statt dessen wird der VPN-Zugang empfohlen.

Die TCP/IP Konfiguration kann per DHCP bezogen werden. Alternativ kann auch eine beliebige IP-Adresse eingestellt sein. Die Verwendung des VPN-Zugangs erfordert allerdings DHCP.

Administrative Voraussetzungen

Studierende können sich unter `https://nic.tuwien.ac.at/cgi-bin/komvergabe.cgi` anmelden.

Mitarbeiter müssen das notwendige Formular `http://nic.tuwien.ac.at/formulare/ansukom_dialin.pdf` ausfüllen.

Derzeit versorgte Bereiche

Das WLAN ist bereits im Freihaus (Erdgeschoss, 1. und 2. Stock), sowie im Erdgeschoss der Bibliothek verfügbar.

Im Laufe des Jahres ist die Versorgung von weiteren Bereichen geplant: Im Hauptgebäude am Karlsplatz sollen verschiedene Hörsäle und Zeichensäle versorgt werden, darunter auch der Festsaal und der Prechtlsaal. Außerdem ist WLAN-Versorgung in den Hörsälen in der Gußhausstraße, im Audimax sowie im Heinz-Zemanek-Hörsaal in der Favoritenstraße geplant.

Eine flächendeckende Versorgung ist derzeit allerdings aus Kostengründen nicht vorgesehen.

Weitere Informationen:

`http://nic.tuwien.ac.at/tunet/wlan/`

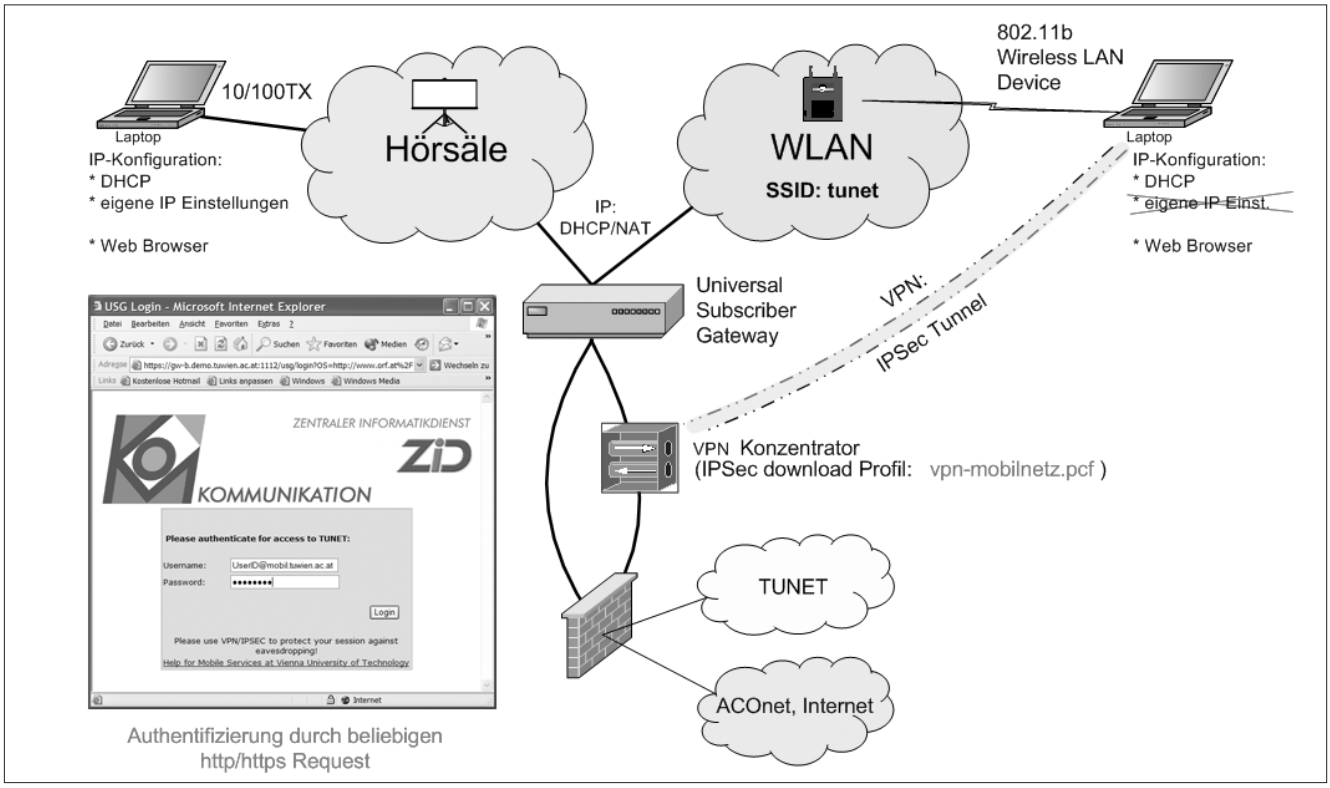


Abbildung 6: Schematische Darstellung des TUNET WLAN

[SPAM?] . . . Markierung von Spam-Mail

Johann Klasek

In Anbetracht des ständig steigenden Aufkommens von Spam-E-Mails stellt der ZID auf den zentralen Mailroutern für den eingehenden Mail-Verkehr ein Markierungsservice zur Verfügung.

Dieses Service erlaubt den Empfängern, Spam-Mails mit einer gewissen Wahrscheinlichkeit als solche zu erkennen und diese gegebenenfalls gesondert zu behandeln. Mit Hilfe von Filtermöglichkeiten des persönlich verwendeten Mailprogramms können z. B. entsprechend bewertete Nachrichten in einen separaten Ordner ablegt werden.

Dieses Service nimmt selbst keinerlei (Aus-)Filterung vor und verändert daher weder den eigentlichen Inhalt noch wird die Weiterleitung (von vermeintlich erkannten Spam-Mails) verhindert oder gestoppt. Lediglich die Markierungsinformation wird den Kontrolldaten der E-Mail hinzugefügt.

Wie wird das Service aktiviert?

Die Markierung der E-Mails in Form einer numerischen Bewertung und gegebenenfalls Auszeichnung der Betreffzeile erfolgt automatisch und erfordert keinerlei Anmeldung oder Freischaltung.

Man profitiert erst von diesem Service, wenn man im verwendeten Mailprogramm entsprechende Filter-Regeln definiert, die die markierten Nachrichten in irgendeiner Weise behandeln. Für diese Einstellungen kann bei aufrechtem Wartungsvertrag des Rechners das Systemunterstützungs-Service der Abt. Standardsoftware in Anspruch genommen werden.

Funktionsweise

Das Mailmarkierungsservice bewertet alle eingehenden E-Mails mit einem *Score* (quasi eine Art „Spam-Faktor"), fügt Header-Zeilen der Mail hinzu bzw. ändert diese, allerdings nur unter ganz speziellen Umständen.

Kern der verwendeten Software ist das Open Source Paket **SpamAssassin**. Dieses ermittelt den *Score* anhand einer umfangreichen und flexiblen (anpassbaren und regelmäßig aktualisierten) Regelbasis. Es werden nicht nur spezifische Anomalitäten im Mail-Header analysiert, sondern es wird auch im Mail-Body auf entsprechende spam-verdächtige Strukturen, Schlüsselwörter und Phrasen untersucht.

Weiters sind auch diverse DNS-basierte Überprüfungen inkludiert, unter anderem auch das kostenpflichtige und von der TU Wien abonnierte RBL+ (Realtime Blackhole List Plus) von mail-abuse.org, wo bekannt offene Mailrelay-Hosts, Dialup-Line-Adressbereiche sowie unzulässige Adressbereiche (Blackholes) registriert sind. Auch eine Reihe von kostenlos verfügbaren DNS-Listen wie dsbl.org, rfc-ignorant.org, dnsbl.njabl.org u.a. werden herangezogen, wo auch offene Proxy-Server, CGI-Scripts und sonstige notorische Spamquellen aufscheinen. Je nach Qualität und Zuverlässigkeit der Eintragungen wirken sich Vorkommnisse auf solchen Listen im *Score*-Wert unterschiedlich aus. Speziell Bewertungen, dass Mails von Dialup- bzw. DSL-Lines stammen, und solche aus jenen Listen, deren Eintragungsmodus nicht sonderlich vertrauenswürdig erscheint, wirken sich auf den *Score*-Wert geringfügiger aus.

Einstellung Ihres Mail-Systems zur Trennung der voridentifizierten Spam-Mails:

einfach durch die Systempflege der Abteilung Standardsoftware
Tel.: 42124 oder Web: sts.tuwien.ac.at/pss/

(bei aufrechtem Wartungsvertrag)

ZID, Abt. Standardsoftware, Systemunterstützung

Einen weiteren Ansatz enthält SpamAssassin in Form des so genannten Auto-Whitelist-Features, wo durch eine Automatik eine Datenbank mit positiven (also nicht als Spam klassifizierten) und negativen (spam-klassifizierten) Absenderadressen gepflegt wird und anhand deren der *Score*-Wert entsprechend korrigiert (erhöht oder reduziert) wird. Im Spam-Report taucht diese Information als „AWL: *Auto-whitelist adjustment*“ auf. Diese Funktion reizt allerdings aufgrund des zentralen Einsatzes prinzipbedingt nicht das Optimum aus und kann so auch nicht mit für kleinere Benutzergruppen zuständigen Spam Assassin-Installationen konkurrieren.

Der Stern am Himmel der Spam-Bekämpfung ist derzeit ein statistisches Verfahren der Mailbewertung nach dem Bayes'schen Prinzip, das auch Bestandteil der Spam Assassin-Installation an der TU Wien ist. Hier sind theoretische Spam-Erkennungsraten von 99,7% bis in den Bereich von 99,9% bei entsprechend geringer False-Positive-Rate (fälschlicherweise als Spam erkannte Nicht-Spam-Mail). Dabei werden Wörter bzw. Teile davon entsprechend ihrer Häufigkeit in Spam- bzw. Nicht-Spam-Mails in einer Datenbank statistisch als „böse“ und „gute“ (gerne auch als „Spam“ bzw. „Ham“ bezeichnet) Wörter erfasst. Hier gilt, dass Wörter nicht unbedingt im klassischen Sinne zu verstehen sind, sondern auch unterschiedliche Schreibweisen in gesperrter Schrift, verfälschte Wörter, Akronyme oder Web-Adressen umfassen. Je nach Wahrscheinlichkeit der Zugehörigkeit der einzelnen Wörter einer neu ankommenden E-Mail, lässt sich eine Aussage ableiten, wie wahrscheinlich eine E-Mail nun als Spam oder Ham einzustufen ist. Dieses Verfahren ist hochadaptiv und ermöglicht die Erkennung von Spam-Mails auch durch nahezu beliebige von den Spam-Versendern erfundene Verfälschungen (die ihre natürlichen Grenzen in der Lesbarkeit durch den menschlichen Betrachter haben, wie etwa die Ziffer „0“ statt des Buchstabens „O“).

Bei all diesen technischen Errungenschaften zeichnet sich eine Tendenz ab, wie die Spam-Mails der Zukunft aussehen. Dem Bayes'schen Ansatz entfliehen lediglich Spam-Mails der Gestalt, die nur eine URL enthalten und ev. einen unverfänglichen Satz mit dem Thema des Treffens und Kennenlernens (ohne spezielle Begriffe) enthalten. Mangels eindeutig zuordenbarer Wörter ist hier eine eindeutige Bewertung schwer. Allerdings gehen Analysten davon aus, dass diese Art des Mail-Marketings aufgrund der schwachen Rücklaufquote bedingt durch die Art selbst kaum eine längerfristige Überlebenschance haben wird und somit zu keiner Bedeutung gelangen wird.

Trotz der nahezu idealen Eigenschaften des Bayes'schen Ansatzes, kann sich auch wie im Falle der obigen AWL-Funktion dieses Verfahren nicht zur Höchstform entfalten. Voraussetzung für den optimalen Einsatz wäre eine empfängerspezifische Optimierung durch Anlernen von Spam-Mails, was auf einem zentral gelegenen Mailgateway wie dem Mailrouter oder der Mailbastion prinzipbedingt nicht umsetzbar ist. Die idealen Voraussetzungen bringen hier nur jene Mailserver mit, die die entsprechenden Mailboxen enthalten (beispielsweise im Wesentlichen jene, die auf den Instituten ihren Dienst verrichten).

Obwohl die zentrale Spam-Markierung mit einigen prinzipbedingten Schwächen zu kämpfen hat, kann man dennoch von einer insgesamt recht guten Erkennungsrate ausgehen.

Eigenschaften

- Die Mail wird im Aufbau (Attachments/Anhänge) nicht geändert und bleibt auf jeden Fall lesbar.
- Mails werden unter allen Umständen weitergeleitet, d.h. nicht blockiert oder nicht (wesentlich) verzögert oder zwischengelagert. Das eigentliche Verwerfen oder Ausfiltern der Mail ist am Instituts-Mailserver oder durch den Mail-Client durchzuführen.
- Für den Fall von technischen Problemen bei der Spamfilterung bzw., wenn E-Mails bestimmte Parameter hinsichtlich Umfang erfüllen, ist es möglich, dass Mails unbewertet passieren.
- Die Regeln, Limits bzw. generell das Verhalten von SpamAssassin können nicht user-spezifisch angepasst werden.

Wen betrifft die Filterung?

Absender	Empfänger	behandelt von
nur außerhalb TUNET	`*@*.tuwien.ac.at`	Mailbastion
überall	`*@tuwien.ac.at`	Incoming Mailrouter
überall	`*@student.tuwien.ac.at`	Incoming Mailrouter

Welche Mails sind von der Markierung ausgenommen?

- Mails, deren Größe mehr als 500.000 Byte beträgt, werden stets unmarkiert weiter geleitet (diese werden auch sonst nicht markiert).
- Nachrichten, deren Analyse ein Zeitlimit überschreiten (man denke nur an die DNS-basierten Überprüfungen) werden schlussendlich ohne weitere Prüfung weiter geleitet.

Wie wird markiert?

Wird eine Mail als Spam erkannt, wird im Betreff zu Beginn die Phrase „[SPAM?]“ eingefügt. Da in seltenen Fällen auch reguläre Mails derart klassifiziert werden, sollte man vermeiden, eine derart markierte Nachricht unmittelbar zu löschen. Weitere – detaillierte – Bewertungsdaten werden der Nachricht als Kontrollinformationen in den Headerzeilen hinzugefügt, abhängig vom ermittelten *Score*-Wert, wobei auf ein gewisses LIMIT, das auf den Wert **6,0** festgelegt ist, Bezug genommen wird. Der LIMIT-Wert dient primär dazu, Mails als Spam zu klassifizieren. Erreicht der *Score* den LIMIT-Wert, werden zusätzliche Informationen in die Nachricht aufgenommen.

Bei allen *Score*-Werten:

```
X-Spam-TU-Processing-Host: HOSTNAME
```

Eine organisationsspezifische Markierung, die zum einen bedeutet, dass die Mail den Spamfilter durchlaufen hat und zum anderen ermöglicht, bei aufeinander folgenden Mailservern die mehrfache Filterung (mit ev. immer gleichem Ergebnis) zu verhindern.

```
X-Spam-Level: ******+++
```

Score-Wert in grafischer Notation: * entsprechen Einer, + Zehntel. In diesem Beispiel entspricht das dem *Score* von 4,3. Es werden nur positive Werte angezeigt, bei negativen Werten bleibt der Wert des Header-Eintrags leer.

```
X-Spam-Status: STATUS ; SCORE
```

Der hier angegebene *Score*-Wert ist der um den Faktor 10 multiplizierte Wert, den SpamAssassin eigentlich berechnet.

Score	Status
< 60	Low
≥ 60 < 100	Medium
≥ 100	High

Bei *Score* ≥ LIMIT:

```
Subject: [SPAM?] ...
```

Eingefügter Subject-Prefix, um den Outlook (Express) Benutzern die Möglichkeit des Filterns zu geben.

```
X-Spam-Flag: YES
```

Man beachte, dass es kein Gegenstück in Form eines „NO“ gibt. In einem solchen Fall wird die Headerzeile überhaupt nicht generiert.

```
X-Spam-Report: Score / LIMIT
```

z.B.:

```
X-Spam-Report: 12.9/6.0
*  2.9 -- BODY: Cable Converter
*  0.4 -- BODY: List removal information
*  0.5 -- BODY: No such thing as a free lunch (1)
*  1.3 -- BODY: Money back guarantee
*  2.9 -- BODY: Bayesian classifier says spam probability
               is 90 to 99% [score: 0.9805]
*  1.5 -- Date: is 3 to 6 hours after Received: date
*  0.6 -- RBL: Received via a blacklisted relay, see
               http://www.mail-abuse.org/
               [RBL check: found 77.46.78.200.rbl-plus.
               mail-abuse.org., type: 127.1.0.2]
*  0.6 -- RBL: Received from dialup,
               see http://www.mail-abuse.org/dul/
*  0.1 -- Message has X-MSMail-Priority, but no X-MimeOLE
*  2.1 -- Forged mail pretending to be from MS Outlook
```

Dieser Report enthält alle Komponenten, aus denen sich die *Score*-Bewertung (additiv) zusammensetzt. Details dazu sind im Allgemeinen unter spamassassin.org/tests.html (umfangreiche Seite) nachzulesen.

Durchführung von Filtermaßnahmen

Das eigentliche Filtern oder Löschen von Spam-Mails obliegt dem Empfänger. Dieser kann seine Mailsoftware, sei es am Mailserver des Instituts oder im Mailclient durch entsprechende Filterfunktionen darauf ausrichten.

Speziell Outlook (Express) Benutzer sind hier auf die Änderung im Subject-Header angewiesen, da sich dort nur ein Subject-Filter definieren lässt. Damit beschränkt sich dort auch die Spam-Erkennung auf den vorgegebenen LIMIT-Wert von 6,0. Die meisten anderen Produkte können sich flexibel am numerischen oder grafischen *Score*-Wert orientieren und damit selbst die Grenze festlegen, wonach eine Mail aus der Sicht verschwinden soll.

An dieser Stelle sei auf die Dokumentation der entsprechenden Mailprogramme hingewiesen bzw. auf das Systemunterstützungsservice der Abt. Standardsoftware oder auf einschlägige Foren im Usenet und WWW.

Vermeidung einer Spam-Klassifizierung bei der Erstellung von E-Mails

Einige Grundregeln sollte man beachten, wenn man in Zukunft mit Personen innerhalb und auch außerhalb der TU Wien kommuniziert (denn auch dort ist SpamAssassin zunehmend im Einsatz) und dabei verhindern möchte, dass die E-Mail beim Empfänger als Spam-Mail eingestuft wird, bzw. sicherstellt, dass die E-Mail im ordentlichen Zustand und für alle lesbar erscheint:

- Das unter Windows sehr gerne betriebene Cut&Paste von Textteilen in eine E-Mail bewirkt das Einschleusen von überflüssigen Carriage-Return-Zeichen (^M), die negativ bewertet werden.
- Die oftmals bei grafisch orientierten Mailprogrammen automatische Umbruchsfunktion (optisch) führt zu extrem langen Zeilen. Auch dass wird negativ bewertet.
- Nur HTML-formatierte (manchmal auch als Rich-Text Format deklarierte) E-Mails sind ein starkes Kriterium für Spam-Mails und sollten grundsätzlich vermieden werden. Nur-Text bzw. Alternate-(Text+HTML) formatierten Nachrichten ist hier den Vorzug zu geben.
- Die Unart, leere Betreffzeilen zuzulassen, bzw. übermäßig viele Interpunktionszeichen wie „!“, „?“ etc. sowie Ziffern und Sonderzeichen („$“) im Betreff wie auch in der Nachricht selbst disqualifizieren eine E-Mail beträchtlich.

Weitere Informationen

Mailrouter/-bastion Dokumentation (Anti-Spam-Maßnahmen): http://nic.tuwien.ac.at/services/mail/

Spam-Markierungsservice: http://nic.tuwien.ac.at/services/mail/spam-markierung/

SpamAssassin Software: http://spamassassin.org/

„A Plan for Spam“. Vorgehensweisen gegen Spam: http://www.paulgraham.com/spam.html

„Forever Spam!? Warum Spam nicht schon längst abgeschafft wurde“. Alexander Talos, Comment 03/1: http://www.univie.ac.at/comment/03-1/031_2.html

Campussoftware Support (Mailprogramme, lokaler Spam Filter *Lyris MailShield Desktop*) und Systemunterstützung-Service des ZID Abt. Standardsoftware: http://sts.tuwien.ac.at/

Firewalls und externe Netze

Georg Gollmann

Um die Betriebssicherheit des TUNET zu erhöhen und den angeschlossenen Rechnern einen Grundschutz zu bieten, sind an den Schnittstellen zu externen Netzen Firewalls installiert.

Zugriffsschutz

Als neue Sicherheitsmaßnahme bietet der ZID seit dem Frühjahr 2003 die Möglichkeit, auf Wunsch Arbeitsplatzrechner und interne Server vor Zugriffen aus dem Internet zu schützen. In diesem Zusammenhang gelten Wählleitungszugänge, TU-ADSL, xDSL@student und VPN als intern (nic.tuwien.ac.at/tunet/extern/). Gründe, diesen Schutz in Anspruch zu nehmen, sind u.a.:

- „*Denial of Service*"-Attacken, d.h. der Rechner wird durch böswillige Zugriffe lahmgelegt.
- Unbeabsichtigt aktivierte Dienste. Diese können durch die Standardinstallation des Betriebssystems oder durch Trojaner gestartet werden.
- Unsicher konfigurierte Dienste. Dies ist bei Standardinstallationen leider oft der Fall.

Es ist zu beachten, dass diese Sperre nur als zusätzliche Vorkehrung zu sehen ist. Sie kann das verantwortungsbewusste Management der einzelnen Rechner nur ergänzen, nicht ersetzen.

Vorzugsweise wird der ganze IP-Adressbereich des Institutes geschützt und nur der Zugriff auf den oder die Server freigegeben. Wenn mehr als etwa vier Server in Betrieb sind, kann alternativ der Adressbereich in eine Zone für geschützte Rechner und eine für aus dem Internet erreichbare Server geteilt werden. Bei einfachen Servern kann statt einer generellen Freischaltung auch nur eine Portgruppe geöffnet werden (z.B. HTTP/HTTPS oder POP3/SPOP3/IMAP/SIMAP). Die Vereinbarung über den zu schützenden Bereich trifft der EDV-Verantwortliche des Instituts bzw. der Abteilung per E-Mail an hostmaster@noc.tuwien.ac.at. Für weitere Einzelheiten zur Durchführung der Anmeldung siehe nic.tuwien.ac.at/nic/tunet/anmeldung.html.

Wie der „*Slammer Worm*" zu Anfang des Jahres wieder gezeigt hat, ist jeder einzelne Rechner für das Funktionieren des gesamten Netzes verantwortlich. Gerade bei aus dem Internet erreichbaren Servern ist daher eine besonders sorgfältige Betriebsführung unerlässlich. Daher sei auf

- die Security Policy der TU Wien (www.zid.tuwien.ac.at/security/policy.php),
- die TUNET Benützungsregelung (nic.tuwien.ac.at/tunet/benutzungsregelung.html) und
- die Hilfestellung durch die Abteilung Standardsoftware (sts.tuwien.ac.at/pss/) hingewiesen.

Portsperren

Basierend auf dem Sicherheitskonzept von BelWü wurde Ende 2001 eine Liste von Services zusammengestellt, die ein Sicherheitsrisiko darstellen und daher zwischen TUNET und Internet gesperrt werden sollten. Diese Liste wird nach Bedarf aktualisiert. Es handelt sich um Services, die entweder

1. nicht über die Grenzen einer Organisation angeboten werden sollten, oder
2. durch sicherere Services ersetzt werden können, oder
3. durch Modifikation (z.B. Tunneling) weiter verwendet werden können.

Behandlung von externen Zugängen zum TUNET (Wählleitungen, TU-ADSL, xDSL@student, VPN, Hörsäle, WLAN):

- Abgehender Verkehr wie in der umseitigen Tabelle.

Überblick über die zwischen dem TUNET und dem Internet gesperrten Ports:

Transport	Port	Protokoll	Beschreibung	Richtung
UDP,TCP	7	echo	Echo	von außen
UDP,TCP	9	discard	Discard Service	von außen
TCP	25	SMTP	Simple Mail Transfer Protocol	von außen *)
UDP,TCP	53	DNS	Nameservice	von außen
UDP	67	bootps	bootp/DHCP Server	beide
UDP	68	bootpc	bootp/DHCP Client	beide
UDP	69	TFTP	Filetransfer ohne PW	von außen
UDP,TCP	111	Portmapper	Portmapper, sunrpc	beide
UDP	123	ntpd	Time Services	von außen
UDP,TCP	135	msrpc	Microsoft Remote Procedure Call	beide
UDP,TCP	136	Profile Name Service	Keine legitime Anwendung mehr	beide
UDP,TCP	137-139	NETBIOS	SMB	beide
UDP,TCP	177	xdmcp	X Display Manager Protocol	beide
UDP,TCP	161-162	SNMP	Netzwerkmgmt	beide
UDP,TCP	445	Microsoft-DS	Microsoft-DS	beide
TCP	512	rexec	R-Kommando	von außen
TCP	513	rlogin	R-Kommando	von außen
TCP	514	rsh, rcp, rdump, rrestore, rdist	R-Kommandos	von außen
UDP	514	syslogd	Logdateien	von außen
TCP	515	lpd	Drucker	von außen
TCP	540	UUCP	Mail (zu Mailhosts)	von außen
TCP	1080	Socks	Anwendungsproxy	von außen
UDP,TCP	1900	SSDP	Simple Service Discovery Protocol	von außen
UDP	1434	SSRS	SQL Server Resolution Service	beide
UDP,TCP	2049	NFS	Filesystem (andere Ports möglich)	beide
TCP	3128	Squid	Web-Proxy	von außen
UDP,TCP	4045	lockd	NFS lock manager	beide
UDP,TCP	5000	UPnP	Universal Plug and Play Service	von außen
TCP	6000-6063	X11	X-Terminal	beide

*) Einkommende Mails werden über den Mailbastionsrechner geleitet.

- Aus dem Internet kommender Verkehr ist gesperrt. Ausgenommen ist – wegen interuniversitär eingerichteter Studien – SSH von den Studentenarbeitsplätzen der Universität Wien.

Funknetze

Funknetze nach dem Standard IEEE 802.11, besser bekannt unter Bezeichnungen wie WLAN oder AirPort, sind zwar einfach zu installieren, stellen aber leider beim derzeitigen Entwicklungsstand ein erhebliches Sicherheitsrisiko dar. Damit ein von einem Institut betriebenes WLAN nicht zur Hintertür wird, durch die Angreifer in das TUNET eindringen können, muss immer eine wirksame Zugangsbeschränkung vom Funkbereich zum TUNET gewährleistet sein.

Zu diesem Zweck plant der ZID, die angebotene Firewall-Lösung auf Linux-Basis (siehe www.zid.tuwien.ac.at/security/firewall2.php) um ein HTTPS-basiertes Authentifizierungsmodul zu erweitern. Für höhere Ansprüche, wenn z. B. auf der Funkstrecke verschlüsselte VPN-Verbindungen gefordert sind, sei auf kommerzielle Produkte wie Nomadix (www.nomadix.com) oder Bluesocket (www.bluesocket.com) verwiesen.

Die von vielen Access Points angebotene Möglichkeit, das Funknetz zu verstecken (*closed mode*) oder nach Geräteadressen zu filtern (*MAC filtering*), bietet keine ausreichende Sicherheit und kann daher nur eine kurzfristige Notlösung darstellen.

Verwendung der Internet-Räume bei Tagungen und Kongressen

Martin Rathmayer

Der Zentrale Informatikdienst bietet Instituten der TU Wien seit einiger Zeit die Möglichkeit, die Internet-Räume FHBR2, FHBR3 und GHBR1 in den Ferialzeiten für Tagungen, Kongresse oder Ähnliches zu reservieren.

In den vorlesungsfreien Zeiten wird die Infrastruktur der Technischen Universität oft für internationale wissenschaftliche Tagungen und Kongresse genutzt. Zur Kongress-Organisation gehört heute auch, dass man den Teilnehmern einen Internet-Zugang über PCs oder Anschlüsse (fest oder Funknetz) für mobile Computer zur Verfügung stellt. Ferner können Vorführungen eigener Software an den PCs durchgeführt werden.

Wenn das organisierende Institut keine entsprechenden Möglichkeiten hat, können einige der vom ZID betriebenen Internet-Räume für Studierende in den vorlesungsfreien Zeiten von Instituten der TU Wien für diese Zwecke benützt werden.

Im Folgenden sind die Möglichkeiten und die Ausrüstung der Räume beschrieben. Wir empfehlen, eine rechtzeitige Reservierung vorzunehmen, da manchmal auch mehrere Tagungen gleichzeitig stattfinden. Sonderwünsche erfüllen wir nach Möglichkeit gerne.

Die Service-Leistung umfasst folgende Punkte:

- Verwendung der PCs nach Bedarf in den jeweiligen Räumen:
  FHBR2: Wiedner Hauptstr. 8-10, 2. OG (28 PCs)
  FHBR3: Wiedner Hauptstr. 8-10, 2. OG (10 PCs)
  GHBR1_A: Gußhausstr 25, 3. Stock (12 PCs)
  GHBR1_C: Gußhausstr. 25, 3. Stock (10 PCs)
- Betrieb innerhalb der Gebäude-Öffnungszeiten
- Voller oder nur TU-interner Internet-Zugang
- Exklusiver PC-Zugang (d.h. kein Studenten-Login möglich) oder ohne Raumreservierung, wenn PC frei ist
- Automatisches Login (keine Validierung notwendig) und automatisches Booten möglich
- Vordefinierte WWW-Startseite
- Druckmöglichkeit über CopyCheck Karte
- Spezielle Features wie Einbindung eines Instituts-Shares, Instituts-Druckers oder andere Vorkonfigurationen nach rechtzeitiger Absprache möglich
- Voller Zugriff auf die gesamte LIZ Software-Umgebung (Linux RedHat plus diverse Standard-Applikationen)
- Zugriff auf MS Office via Citrix Terminal Server
- Alle PCs mit CD-ROM, USB, Floppy und Audio-Anschluss
- Non-Permanent Accounts (d.h. Einstellungen und lokal abgespeicherte Daten gehen nach einem Reboot verloren)
- Permanent Accounts eingeschränkt möglich (z. B. für Kurse)

Eine genaue Beschreibung der Soft- und Hardware-Möglichkeiten der PCs in den Internet-Räumen des ZID befindet sich auf den Internet-Webseiten des ZID unter „Studenten Services“ (student.tuwien.ac.at).

Die Reservierung erfolgt über Herrn Peter Berger (Kl. 42070), bei technischen Fragen stehen Herr Peter Egler (Kl. 42094) und Herr Martin Rathmayer (Kl. 42086) zur Verfügung. Das Institut muss selbst dafür sorgen, dass entsprechende Informationen bzw. Hinweise für den Zeitraum der Veranstaltung angebracht werden. Eventuell ist bei großen Veranstaltungen ein Betreuer vor Ort zu empfehlen.

Die Nutzung der Räume ist derzeit noch kostenlos, sofern für die Tagung von der TU Wien keine Kostenersätze für die Nutzung der Hörsäle oder Seminarräume verrechnet werden.

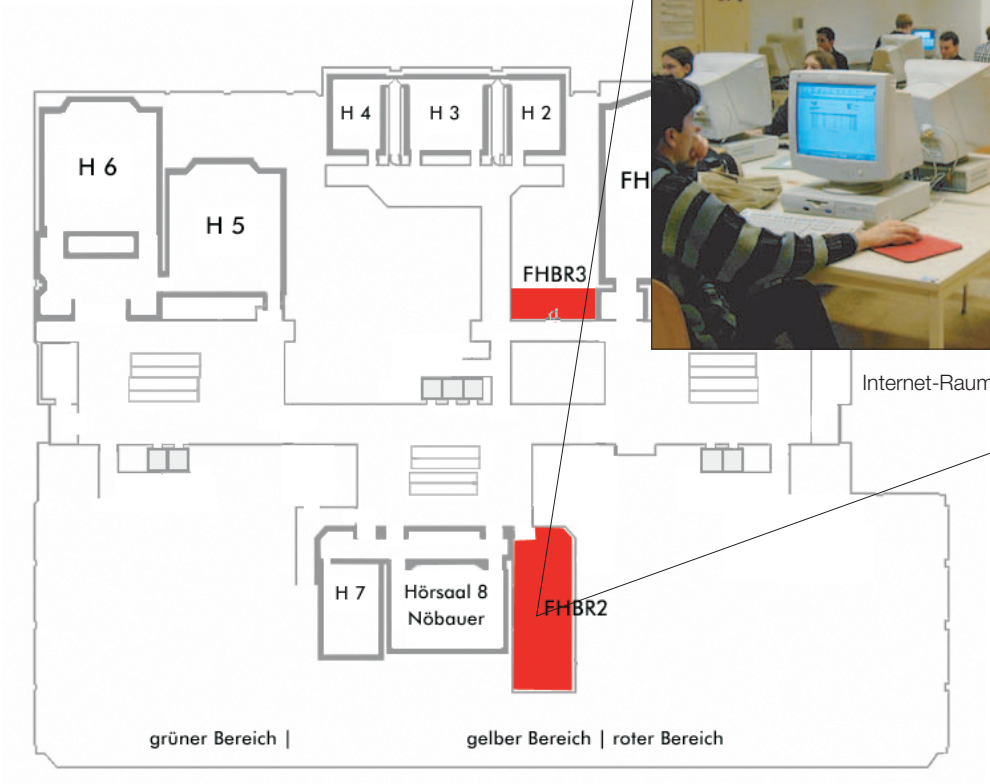
Zusätzlich zu den PCs stehen in den Internet-Räumen so genannte „Datentankstellen“ (Netzwerkanschlüsse für Notebooks) bzw. WLAN (derzeit nur im Freihaus) zur Verfügung. Auf Wunsch können auch in anderen Bereichen vorübergehend Datentankstellen realisiert werden. Falls im Zuge einer Veranstaltung diese Möglichkeit genutzt werden soll, muss diesbezüglich mit Herrn Wolfgang Meyer (Kl. 42050) Kontakt aufgenommen werden.

Für TU-interne Seminare und Schulungen kann in der vorlesungsfreien Zeit der kürzlich neu eingerichtete **Schulungsraum** (FHSR1, Freihaus, Erdgeschoss) reserviert werden. Dort stehen 13 PCs, ein Video-Beamer und auf Wunsch statt LIZ auch lokales Windows 2000 plus MS-Applikationen und Drucker zur Verfügung. Da die Installationen Disk-Image-basiert sind, kann auch kundenspezifische Software eingebunden werden bzw. kann eine zerstörte Installation innerhalb weniger Minuten wieder hergestellt werden.

An der Datentankstelle

Im Schulungsraum

Internet-Raum FHBR2



Lageplan
Internet-Räume des ZID
Wiedner Hauptstr. 8-10
2. Obergeschoss

Ausfallsicherheit und Redundanz im TUNET

Johannes Demel

Das Datennetz der Technischen Universität Wien versorgt derzeit ca. 9000 Endsysteme. Im Tagesschnitt werden von den Mailbastionsrechnern ca. 22000 Mails weitergeleitet, ca. 45000 Mails werden pro Tag auf den zentralen Mailservern auf Viren überprüft. Allein schon aus diesen wenigen Zahlen ist die Bedeutung des Datennetzes für den Betrieb unserer Universität ersichtlich. Die Datenkommunikation und der Zugriff auf Ressourcen im Internet bzw. das Anbieten von Ressourcen im Internet ist aus dem heutigen Leben nicht mehr wegzudenken.

1. Einleitung

Damit die Arbeitsplätze an den Instituten und für Studierende entsprechend versorgt werden, sind derzeit ca. 800 km Kupferkabel (Kabel direkt zum Arbeitsplatz) und ca. 40 km Glasfaserstrecken (im Gebäude und zwischen Gebäuden) erforderlich. Alle diese Kabel werden mit ca. 800 Geräten (von einfachen Repeatern über Switche bis zu komplexen Routern) verbunden. Diese Zahlen lassen schon erahnen, dass das Datennetz der TU Wien bereits ein hochkomplexes Gebilde geworden ist, das es nicht nur gilt, in Betrieb zu halten, sondern auch laufend an neue Anforderungen anzupassen.

Seit einigen Jahren ist daher die Verbesserung der Betriebssicherheit ein wesentlicher Schwerpunkt bei den Erweiterungen im TUNET inklusive der zum TUNET dazugehörigen Server. Anzumerken ist, dass schon alleine die Aufrechterhaltung der gleichen subjektiven Betriebssicherheit große Anstrengungen und Investitionen erfordert.

Alle hier diskutierten Maßnahmen beziehen sich nur auf das IP-Protokoll. Bei eventuell verwendeten anderen Protokollen können ein Teil der Maßnahmen auch greifen, von der Struktur des TUNET wird jedoch die Ausfallsicherheit nur für IP (v4) unterstützt.

2. Grundbegriffe

Bevor wir uns konkret dem TUNET zuwenden, sollen einige Grundbegriffe in Erinnerung gerufen werden:

Ausfallwahrscheinlichkeit

Zur Beurteilung der Wahrscheinlichkeit, dass ein Gesamtsystem funktioniert, sagt uns die Theorie der Wahrscheinlichkeitsrechnung, dass dies das Produkt der Funktionswahrscheinlichkeiten der einzelnen Komponenten ist. Leider sind die Wahrscheinlichkeiten (hoffentlich nur minimal) kleiner als 1, damit ist aber das Produkt dann deutlich kleiner als 1.

Wenn man bedenkt, dass im günstigen Fall und vereinfacht zur Kommunikation von zwei Rechnern in zwei verschiedenen Standorten der TU Wien 4 Glasfaserstrecken, 2 Kupferstrecken, 12 Patchkabel, 2 Switches, 3 Backbone Switche/Router, ein Nameserver (der in einem anderen Gebäude steht und damit wieder 1 Kupferstrecke, 2 Glasfaserstrecken und 6 Patchkabel sowie 2 Switche benötigt) sowie insgesamt 8 230V Stromanschlüsse erforderlich sind, so kommt man unter Vernachlässigung von Komponenten wie Klima auf insgesamt 43 Komponenten.

Wenn nun vereinfacht jede Komponente eine Ausfallwahrscheinlichkeit von 0,1% hätte, so ergibt dies für den gesamten Kommunikationsweg eine Ausfallwahrscheinlichkeit von 4,2%, dies wäre im Schnitt an einem Tag im Monat eine Störung (wie lange dann immer die Fehlerbehebung dauert). Zum Glück sind die Ausfallwahrscheinlichkeiten deutlich geringer, aber bei einem derart großen und komplexen System wie dem TUNET fragt man sich trotzdem manchmal, wieso alles funktioniert (die meiste Zeit sind aber eh irgendwelche Störungen zu beheben und wir kommen auf diese Gedanken gar nicht).

Wichtige Größen zur Beurteilung der Betriebssicherheit sind auch MTBF (*Mean Time Between Failure*) und MTTR (*Mean Time to Repair*).

Betriebsfehler

Unter Betriebsfehlern versteht man ganz einfach Fehler, die im laufenden Betrieb eines Systems auftreten, egal ob sie vorhersehbar sind oder nicht, egal ob sie aufgrund äußerer Einwirkung entstehen oder aufgrund von Verschleiß. Folgende Tabelle soll einen anschaulichen Überblick bieten:

zufällige, physikalische Fehler
Verschleißfehler, z.B. durch Alterung elektrischer Bauteile
Störungsbedingte Fehler aufgrund äußerer physikalischer Einflüsse, z.B. Stromausfall, Wassereinbruch
Bedienungsfehler
Wartungsfehler: fehlerhafte Systemeingriffe während Wartungsintervall
Sabotage, Vandalismus
Umbaumaßnahmen

Neben den eigentlichen Betriebsfehlern gibt es noch die geplanten Unterbrechungen, z.B. infolge von Erweiterungen und Umbauten, Überprüfungen (z.B. der Stromversorgung, Test der Redundanzmaßnahmen, Reproduzieren von Fehlern).

Fehlertoleranz

Fehlertoleranz ist die Fähigkeit eines Systems, auch mit einer begrenzten Zahl fehlerhafter Subsysteme seine spezifizierte Funktion zu erfüllen. Das Verhalten des Systems nach Auftreten von Fehlern kann folgendermaßen klassifiziert werden:

Typ	**Verhalten des Systems**
(go)	System arbeitet sicher und korrekt
(fail-operational)	System fehlertolerant ohne Leistungsverminderung
(fail-soft)	Systembetrieb sicher, aber Leistung vermindert
(fail-safe)	Nur Systemsicherheit gewährleistet
(fail-unsafe)	unvorhersehbares Systemverhalten

Bei der Korrektur von Fehlern unterscheidet man die zwei Prinzipien der Vorwärts- und der Rückwärtsfehlerkorrektur. Bei der **Vorwärtsfehlerkorrektur** versucht das System, so weiterzumachen als ob kein Fehler aufgetreten wäre, indem es z. B. im Moment des Auftretens eines Fehlers sofort mit korrekt funktionierenden Ersatzsystemen weiterarbeitet. Fehler bleiben bei der Vorwärtsfehlerkorrektur normalerweise unsichtbar für Anwender. Bei der **Rückwärtsfehlerkorrektur** versucht das System bei Auftreten eines Fehlers in einen Zustand vor diesem Auftreten zurückzukehren, z. B. in den Zustand direkt vor einer fehlerhaften Berechnung, um diese Berechnung erneut auszuführen. Genauso ist aber auch ein Zustandswechsel in einen Notbetrieb oder z. B. ein Reboot des Systems möglich. Kann eine fehlerhafte Berechnung erfolgreich wiederholt werden, bleibt auch bei der Rückwärtsfehlerkorrektur der Fehler für den Anwender unsichtbar. Oft ist aber nur ein Weiterbetrieb mit Leistungseinbußen oder eingeschränkter Funktionalität möglich und der Fehler somit sichtbar.

Fehlerredundanz

Das häufigste Konzept, um Systeme gegenüber **Betriebsfehlern** tolerant zu machen, ist die Fehlerredundanz, das ist das Vorhandensein von mehr als für die Ausführung der vorgesehenen Aufgaben an sich notwendigen Mittel (nach DIN 40041, Teil 4).

Man unterscheidet dabei verschiedene Stufen der Redundanz.

Aktive-Redundanz (funktionsbeteiligte, heiße Redundanz)	Mehrere Komponenten eines Systems führen dieselbe Funktion simultan aus. Fällt eine Komponente aus, wird dieser Fehler durch die verbleibenden Komponenten direkt kompensiert und führt daher nicht unmittelbar zu einer von außen erkennbaren Reaktion. Normalerweise erfolgt dann zwischen allen aktiven Systemen eine Lastaufteilung.
Standby-Redundanz (passive Redundanz)	Zusätzliche Mittel sind eingeschaltet/bereitgestellt, werden aber erst bei Ausfall/Störung an der Ausführung der vorgesehenen Aufgabe beteiligt.
Kalte Redundanz	Zusätzliche Mittel werden erst bei Ausfall/Störung eingeschaltet/bereitgestellt.

Im Bereich der Vernetzung können die getroffenen Maßnahmen zusätzlich wie folgt klassifiziert werden:

Geräteredundanz	Für eine Funktion gibt es mindestens zwei voneinander unabhängige (wie genau das erreichbar ist, hängt von der jeweiligen Funktion ab) Systeme, die diese Funktion erbringen.
Wegeredundanz	Für eine Verbindung zwischen zwei Systemen gibt es mindestens zwei voneinander unabhängige Wege.
Raumredundanz	Die Funktion kann in zwei verschiedenen Räumen eines Gebäudes erbracht werden.
Gebäuderedundanz	Die Funktion kann in zwei verschiedenen Gebäuden der TU Wien erbracht werden.

3. Der Weg zwischen zwei Rechnern an der TU Wien

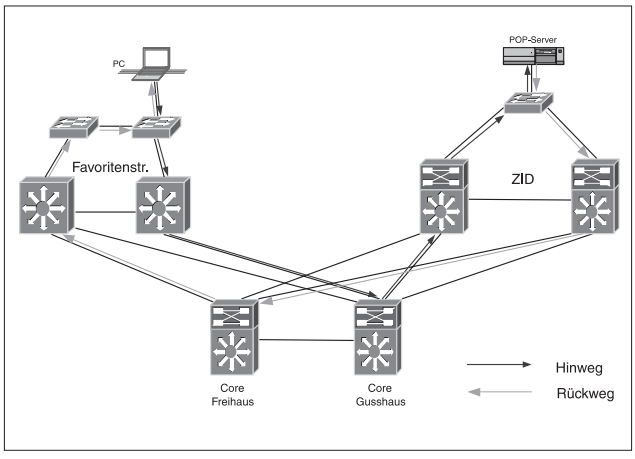
Zur Darstellung der Maßnahmen zur Verbesserung der Ausfallsicherheit bei der Kommunikation zwischen zwei Rechnern soll in diesem Abschnitt der Weg eines Pakets von einem Rechner in einem Gebäude der TU Wien (z.B. Favoritenstraße) und dem POP-Server am ZID dargestellt werden. Es wird dabei davon ausgegangen, dass die beiden Systeme in unterschiedlichen IP-Subnetzen sind und dass damit ein Routing erforderlich ist. Es wird der Einfachheit halber davon ausgegangen, dass die Endrechner schon die Mac-Adresse zur jeweils benötigten IP-Adresse des Default-Gateways wissen und dass daher das ARP Protokoll nicht mehr erforderlich ist. Weiters wird davon

ausgegangen, dass der Rechnername bereits auf eine IP-Adresse aufgelöst wurde (d.h. der Nameserver kontaktiert wurde).

von	nach	via	Maßnahme
PC/Ethernet karte	Etagen Switch Port	TP-Kabel	Keine Ausfall-sicherheit durch TUNET möglich. Siehe 3.1
Etagen Switch	Gebäude Switch	Glasstrecke	Pro Gebäude 2 Backbone Switche. Je ein Weg zu jedem Gebäude Switch. Siehe 3.2
Gebäude Switch	Gebäude Router	Intern oder Glasstrecke	Pro Gebäude 2 Backbone Router. Siehe 3.3
Gebäude Router/Switch	Core-Router	Glasstrecke	2 Core Router auf der TU Wien. Je ein Weg zu jedem Gebäude-Switch. Siehe 3.3
Core Router	Gebäude Router/ Switch	Glasstrecke	Pro Gebäude 2 Backbone Router + Switche. Siehe 3.3
Gebäude Router/Switch	Etagen Switch	Glasstrecke	2 Wege zum Etagen Switch. Siehe 3.2
Etagen Switch	POP-Server	TP-Kabel	Keine Ausfall-sicherheit durch TUNET möglich. Siehe 3.1. Server siehe 5.

Nachdem der POP-Server das Paket verarbeitet hat, muss natürlich ein Antwortpaket (zumindest mit der Information, dass das Paket angekommen ist) zurück zum PC geschickt werden. Dies erfolgt logisch gesehen nach obiger Tabelle von unten nach oben. In Wirklichkeit kann das aber über andere Geräte und Kabelwege laufen, da bei – aus Redundanzgründen vorhandenen – mehreren Wegen die Auswahl des konkreten Weges in jede Richtung eine andere sein kann.

Der Ablauf ist auch in folgender Grafik dargestellt:



3.1 Maßnahmen zwischen Rechner und Etagenswitch

Auf dem Weg zwischen Rechner und Etagenswitch können von TUNET aus keine (aktiven) Redundanzmaßnahmen gesetzt werden. Es wären entsprechende Vorkehrungen im Rechner selber bzw. bei der Verbindung zwischen Rechner und TUNET-Steckdose im Raum notwendig. Konkrete Maßnahmen wären daher vom Institut in Absprache mit dem ZID zu treffen. Solche Maßnahmen könnten sein:

- Für den Rechner sind zwei Anschlussbuchsen reserviert, die zum gleichen oder einem anderen Etagenswitch führen. Bei Störung des Weges zu einem Switch könnte im Sinne einer „kalten Redundanz“ der Rechner auf die andere Buchse umgesteckt werden.

- Der Rechner ist mit zwei Ethernet-Karten ausgestattet, die an zwei Anschlussbuchsen des TUNET hängen, die zu zwei unterschiedlichen Etagenswitchen führen. Dies ist keine triviale Konfiguration, da z. B. bei gleicher Mac-Adresse auf beiden Ethernetkarten (dies würde dem Standard entsprechen!) es zu dauerndem Hin-/Herschalten (*Flapping*) des Weges von Paketen vom Switch zum Rechner auf Basis der Mac-Adresse kommen würde und die Switche dadurch belastet werden (wird in der relativ schwachen CPU des Switches ausgeführt, im Gegensatz zur schnellen Switching-Engine für die Paketweiterleitung) und in der Folge die beteiligten Ports abschalten. Hier sind also zusätzliche Software-Maßnahmen erforderlich, z. B. unterschiedliche Mac-Adressen sowie unterschiedliche IP-Adressen.

- Der Rechner ist mit einer Ethernet-Karte ausgestattet, die an einen so genannten „Twister“ führt, der dann über zwei Wege zu zwei Etagenswitchen eine Verbindung hat. Der Twister stellt sicher, dass zu einem Zeitpunkt nur ein Weg aktiv ist, wodurch die Probleme im vorigen Punkt vermieden werden. Diese Methode wird z.B. bei einigen Services, die nicht leicht auf zwei Server verteilt werden können, im Kommunikationsbereich eingesetzt.

Unabhängig von diesem Maßnahmen sieht der TCP/IP Protokoll Stack in der TCP Transportschicht, deren Aufgabe die Sicherstellung einer fehlerfreien Kommunikation ist, ein nochmaliges Schicken des Pakets vor, wenn die Bestätigung, dass ein abgeschicktes Paket beim Zielrechner angekommen ist, nicht innerhalb einer gewissen Zeit eintrifft. Dies ist beim UDP-Protokoll (z. B. für Nameserverabfragen) nicht gegeben.

Bei den Etagenswitchen handelt es sich normalerweise um nichtmodulare Geräte mit 24, 48 oder 80 Ports, die nur ein Netzteil haben. Es ist daher eine Stromversorgung mit zwei unabhängigen Stromkreisen nicht möglich. Es wird jedoch (zumindest bei Neuerrichtungen) sichergestellt, dass die Stromversorgung durch eine eigene Absicherung mit FI/LS (kombinierter FI Schutzschalter mit Leistungsschalter) erfolgt und nicht mit Licht, Klima,

Staubsaugersteckdosen etc. zusammenhängt. Bei größeren Etagenverteilern wird auch eine eigene USV eingesetzt. Normalerweise ist die Aufrechterhaltung des Betriebes bei Ausfall des Stromes im Etagenverteiler nicht so wichtig, da es sich meistens um Stromausfälle handelt, die auch die Rechner am Institut betreffen (können auf Grund der maximalen TP-Kabellänge von 90 Metern nicht weit entfernt sein).

3.2 Maßnahmen zwischen Etagenswitch und Gebäudeswitch/Router

3.2.1 Physische Maßnahmen

Grundsätzlich sollen an einem Standort bzw. Gebäudekomplex zwei Gebäudeswitche und zwei Gebäuderouter existieren. Dies ist derzeit für die Standorte Freihaus, Favoritenstraße, ZID, Karlsplatz + Resselgasse / Wiedner Hauptstraße 7-9, Getreidemarkt, Gußhausstraße 27-29 der Fall. Die Redundanz für Treitlstraße wird im Zuge der Adaptierung des Perlmooserhauses, die Argentinierstraße im Zuge deren Adaptierung und der Adaptierung Karlsgasse realisiert.

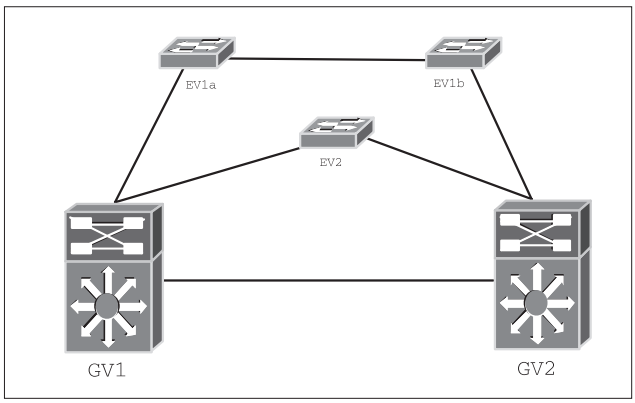
Die Gebäudeswitche / Router sollten in zwei getrennten Räumen aufgestellt sein. Dies ist bei allen Standorten außer Favoritenstraße und ZID der Fall.

In allen Fällen ist der Router im gleichen Gehäuse wie der Switch untergebracht. Je nach verwendetem Modell handelt es sich dabei um eine gemeinsame Switching/Router Engine (ZID, Treitlstraße, Argentinierstraße, Gußhaus, Getreidemarkt) oder im Switch befindet sich ein zusätzliches Routing-Modul. In Falle des eigenen Moduls erfolgt geräteintern dann die Kommunikation über einen Gigabit-Bus. Dies stellt natürlich Kapazitätseinschränkungen dar, gleichzeitig gibt es dadurch aber auch zusätzliche Komponenten, die ausfallen können, und das Management und die Softwareoberfläche (unterschiedliche Betriebssysteme !) wird deutlich komplizierter. Bei manchen Standorten (maximal bei einem Gebäudeswitch pro Standort) gibt es aus Kapazitätsgründen (Anzahl der Ports) für den Switch noch eine Erweiterung mit einem externen Gigabit-Switch.

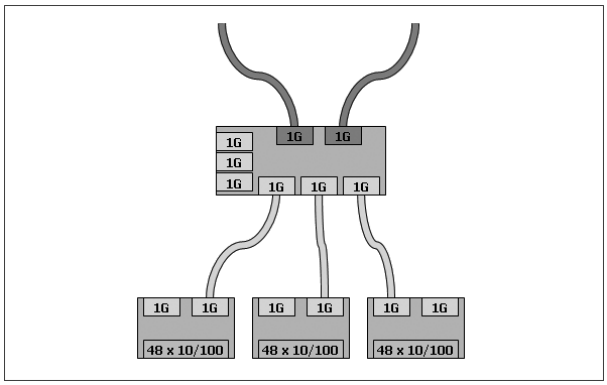
Die beiden Backboneswitche sind mit einem Gigabit Link verbunden. Damit kann z.B. bei den Geräten mit einem eigenen Routing-Modul bei dessen Ausfall das Routing vom zweiten Router übernommen werden. Ein wichtiges Kriterium ist auch, dass Module im Betrieb getauscht bzw. ein-/ausgebaut werden können.

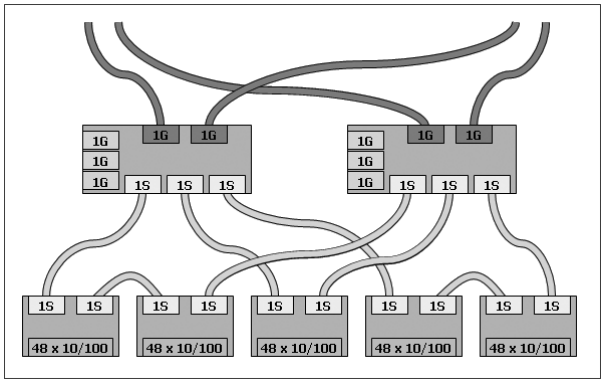
Ein Etagenswitch soll nun mit beiden Gebäudeswitchen über Gigabit verbunden sein, wobei mindestens eine Verbindung direkt erfolgen soll, die zweite kann auch über einen weiteren Etagenswitch erfolgen.

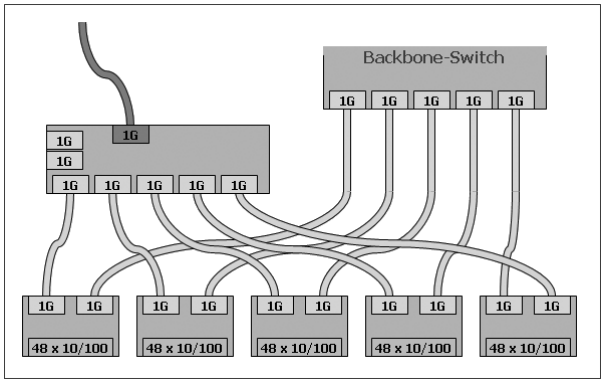
Die typische Struktur im Gebäude hat daher folgendes Aussehen:



Je nach der notwendigen Portanzahl wird die Realisierung aber unterschiedlich kompliziert, wie einige Musterkonfigurationen für den Standort Gußhaus zeigen:







3.2.2 Maßnahmen auf Ebene des ISO Link Layer (2)

Der Link Layer hat im Wesentlichen die Aufgabe, Pakete über eine direkte Kabelverbindung von einem Gerät zum anderen zu schicken. Es muss auch sichergestellt werden, dass das Übertragungsmedium nicht belegt ist (*Collision Detection*). Wenn das Medium nicht frei ist, wird versucht, das Paket verzögert wegzuschicken (*Back-off Algorithmus*). Die Redundanz bei der Verbindung der Etagenswitche mit dem Gebäudeswitch basiert auf folgenden Techniken:

- Es gibt zwei Wege zu den Backbone-Switchen.
- Die Backbone-Switche sind untereinander wieder verbunden.
- Durch diese Verkabelung entsteht eine Masche. Dies ist aber eigentlich vom Ethernet Protokoll her verboten, da ja sonst ein Paket ewig im Kreis laufen würde. Es gibt daher das *Spanning Tree* Protokoll (SPT), das nur zwischen je zwei Switchen abläuft. Der dahinter liegende Algorithmus erkennt nun die Situation der Maschine und schaltet auf Basis von graphentheoretischen Algorithmen mit zu setzenden Gewichten von Verbindungswegen und Prioritäten von Switchen einen Link auf inaktiv, sodass die Masche unterbrochen ist, trotzdem aber die volle Connectivity zwischen allen Switchen gegeben ist.

Bis auf wenige Ausnahmen sind an den Gebäudeswitchen keine Endgeräte angeschlossen (neben strukturellen Überlegungen wäre dann keine Redundanz auf Routing-Ebene etc. möglich).

Durch den *Spanning Tree* Algorithmus gibt es aber Einschränkungen, wie viele Switche maximal zwischen zwei Endgeräten verwendet werden dürfen. Dadurch ist die Flexibilität der Zusammenschaltung von Etagenswitchen eingeschränkt.

Das Umschalten auf einen anderen verfügbaren Weg nach einem Ausfall der aktiven Verbindung dauert ca. 60 Sekunden.

3.2.3 Maßnahmen auf Ebene des ISO Network Layers (3)

Zur Kommunikation mit anderen Subnetzen oder dem Internet muss ein Paket an das „Default Gateway“, das ist die IP-Adresse des Routers im eigenen Subnetz, geschickt werden (an der TU Wien sind das IP-Adressen, die normalerweise 1 oder 129 im letzten Oktett stehen haben). Nun haben wir aber für jedes Gebäude zwei Router, die jeweils eine eigene IP-Adresse benötigen. Die Schwierigkeit besteht nun darin, dass die Endgeräte (Arbeitsplatzrechner, Server) wissen, an welchen der beiden Router das Paket zu schicken ist. Es gibt zwar ein eigenes Protokoll, *ICMP Router Discovery Protocol* (*IRDP*) nach RFC 1256, mit dem Endsysteme feststellen können, welche Router gerade arbeiten. Dies erfordert bei jedem Endsystem eine zusätzliche Software, die für das jeweilige Betriebssystem verfügbar sein muss. Diese Software (üblicherweise ein eigener Dämon) muss dann installiert und gestartet sein, damit alles funktioniert. Weiters müssen alle Router das IRDP Protokoll unterstützen und es muss entsprechend konfiguriert sein. Also relativ viel Aufwand auf allen Seiten. Außerdem dauert die Erkennung, dass ein Router *down* ist, relativ lange (10-30 Minuten !).

Bei uns wird daher das Cisco-proprietäre Protokoll HSRP (*Hot Standby Routing Protocol*, RFC 2281) eingesetzt. Das Prinzip ist im Wesentlichen, dass jeder Router auf seinem Interface eine eigene IP-Adresse hat (bei uns in der Regel endend mit 125/126 bzw. 253/254). Diese Adresse wird vom Router beim Abschicken von Paketen verwendet. Zusätzlich wird von einem der beiden Router die „HSRP-Adresse“ (z.B. 128.130.x.1) mit einer definierten Mac-Adresse (0000.0c07.ac**) emuliert. Welcher Router der aktive ist, machen sich die beiden Router untereinander auf Basis von Prioritäten in der Konfiguration aus. Wenn ein Router den anderen nicht mehr erreichen kann, so aktiviert er sich selber. Dies geschieht innerhalb ca. 10 Sekunden. Natürlich müssen dann die Etagen-Switche lernen, dass die Mac-Adresse des Default-Gateways jetzt über einen anderen Port erreichbar ist.

Ob das HSRP Protokoll für ein konkretes Subnetz eingesetzt wird, ist für den Benutzer nicht sofort ersichtlich. An Hand der Mac-Adresse des Default Gateways und z.B. durch auf den ersten Blick seltsam anmutende Ergebnisse beim Traceroute Befehl ist es erkennbar.

Es gibt in der Zwischenzeit auch ein Standard Protokoll, das *Virtual Router Redundancy Protocol* (*VRRP*) nach RFC 2338, das nach ähnlichen Prinzipien funktioniert, derzeit an der TU Wien im Backbone aber nicht eingesetzt wird.

Durch diese Maßnahmen stellen wir sicher, dass das Default Gateway immer (d.h. zumindest bei einem einfachen Fehler) erreichbar ist. Wenn ein Institut aber hinter einem institutseigenen Firewall liegt, der nicht ebenso redundant ausgeführt ist, bietet diese Redundanz leider nur eine beschränkte Hilfe.

3.3 Maßnahmen im TUNET Backbone

Zum TUNET Backbone im weiteren Sinne gehören alle Gebäude-Switche/Router und die beiden Core Switche/Router. Alle Gebäude-Switche sind mit mindestens einem der beiden Core Switche verbunden.

3.3.1 Physische Maßnahmen

Die Maßnahmen für die Gebäude-Switche/Router wurden bereits unter 3.2.1 besprochen und brauchen daher hier nicht wiederholt werden.

Die beiden Core Switche mit integriertem Routing sind in zwei unterschiedlichen Gebäuden (Freihaus, Gußhaus) aufgestellt. Jeder der beiden Switche verfügt über zwei Netzteile, wobei eines davon über eine USV (Überbrückungszeit je nach Gebäude 30 Minuten bis 8 Stunden) versorgt wird (die im Freihaus im Notfall durch das Notstromaggregat des Hauses versorgt wird). Ein wichtiges Kriterium ist auch, dass Module im Betrieb getauscht bzw. ein-/ausgebaut werden können. Die Räume sind entsprechend klimatisiert und werden auch fernüberwacht (Strom, Temperatur, Feuchte, …). Die beiden Core Switche sind untereinander mit derzeit einer Glasfaserstrecke verbunden.

Jeder Gebäudeswitch ist mit mindestens einem Core Switch verbunden, wobei jedes Gebäude mit jedem der beiden Core Switche mit einer direkten Glasfaserverbindung verbunden sein muss. Ob ein Gebäude mit 2, 3

oder 4 Verbindungen mit dem Core verfügt, hängt von der jeweiligen geografischen Lage und den verfügbaren Glasfaserwegen zwischen den Gebäuden ab. Für die Glasfaserstrecken werden, je nach Möglichkeit der Trassenführung und der Wegerechte, neben selbst verlegten Kabeln Strecken der Telekom Austria sowie der Memorex Telex Communications AG (MTCAG) eingesetzt. Dabei wird darauf geachtet, dass ein Gebäude möglichst über unterschiedliche Trassen zu den beiden Core Switchen geführt wird.

3.3.2 Maßnahmen auf Ebene des ISO Link Layer (2)

Im Gegensatz zu den Jahren 2001/2002 wurde Anfang 2003 der Backbone dahingehend umgebaut, dass keine Layer 2 Techniken, wie der *Spanning Tree* Algorithmus, erforderlich sind. Die Glasfaserstrecke zwischen Gebäude-Switch und Core Switch stellt also ein eigenes VLAN dar, das nur zwischen diesen beiden Punkten existiert. Damit fallen die relativ langen Umschaltzeiten des *Spanning Tree Protocols* (ca. 1-2 Minuten) weg.

Diese Regel gilt naturgemäß nicht für „gebäudeübergreifende“ VLANs, die für Institute benötigt werden, die das gleiche IP-Subnetz in mehreren Gebäuden nutzen wollen. Auch für Appletalk, Novell und DECnet trifft dies zu. In diesen Fällen ist also bei einer Störung mit längeren Auswirkungen zu rechnen.

Übrigens konnte die Umstellung von Layer 2 Core auf ein Layer 3 Core infolge der zu diesem Zeitpunkt existierenden redundanten Gebäuderouter ohne Betriebsunterbrechung durchgeführt werden.

An den Core Switches sind keine Endgeräte und auch keine Etagenswitche angeschlossen.

3.3.3 Maßnahmen auf Ebene des ISO Network Layers (3)

Eine wesentliche Voraussetzung zur Nutzung einer redundanten Konfiguration ist die Verwendung eines geeigneten „*Routingprotocols*“. Es nützt ja schließlich nichts, wenn ein redundanter Weg zur Verfügung steht, aber niemand aktiviert ihn. Die primäre Aufgabe eines *Routingprotocols* ist die Versorgung aller Router mit der Information, über welchen Weg (d.h. Nachbarrouter) ein anderes Subnetz (oder ein IP-Netz im Internet) erreicht werden kann. Jeder Router führt eine eigene Routingtabelle, in der die Subnetze des eigenes Intranets (dem TUNET) enthalten sind, sowie der Weg zu allen anderen Netzen (dem Internet/Extranet) in Form eines „Default-Netzes“. Das Halten sämtlicher Netze des Internet in jedem Router des Intranets macht keinen Sinn, da dies eine viel zu große Menge wäre (die Router des ACOnet Backbones haben derzeit ca. 125.000 Netze mit ca. 260.000 verschiedenen Wegen im Speicher !), die nur sehr leistungsstarke (und damit teure) Router bewältigen können.

Das *Routingprotocol* hat nun einerseits die Aufgabe, mit den Nachbarroutern die vom eigenen Router direkt (*connected*) oder indirekt erreichbaren Subnetze auszutauschen, als auch, die Routingtabellen aufzubauen bzw. zu aktualisieren. Dabei müssen auch mehrere Wege unter Beachtung von Gewichten und Prioritäten berücksichtigt werden. An der TU Wien wird im Backbone das OSPF Protokoll (*Open Shortest Path First*) eingesetzt. Dies ist ein *Routingprotocol*, das hierarchisch basierend auf „Link States“ mittels graphentheoretischer Algorithmen in jedem Router eine Sicht des kompletten Intranets errechnet und damit die Routingtabellen aktualisiert.

Wenn zu einem Ziel zwei Wege mit der gleichen Bewertung existieren, so wird automatisch eine Lastaufteilung erzielt. Gleichzeitig steht bei Ausfall eines der beiden Wege sofort ein zweiter Weg zur Verfügung und damit kann die Unterbrechung minimal gehalten werden. Dies ist auch einer der Gründe, warum die Gebäuderouter mit jeweils einem dedizierten Subnetz mit den Core-Routern verbunden sind. Sobald z.B. ein Interface ausgeschaltet wird (geplant oder wegen einer Störung), werden sofort alle Wege, die über dieses Interface gehen, im Router mit diesem Interface aus der Routingtabelle entfernt. Wenn noch eine zweite Route zu einem Ziel existiert hat, kann diese sofort (und jetzt alleinig) verwendet werden, und es findet praktisch keine Unterbrechung statt.

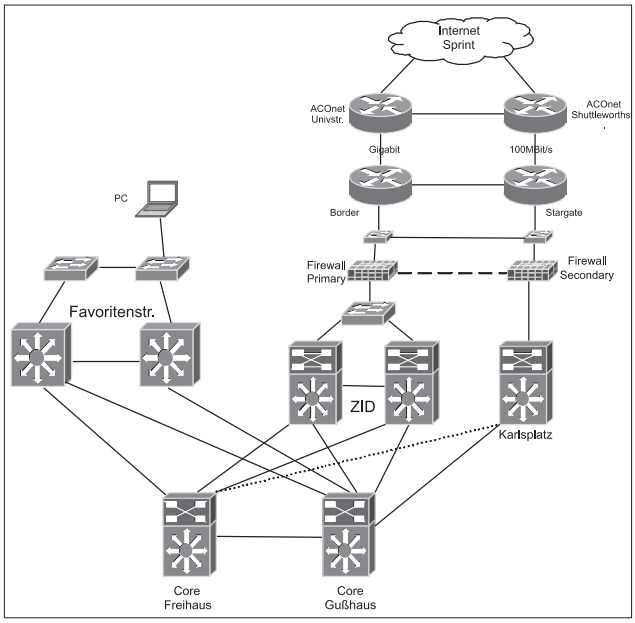
4. Der Weg ins Internet

Zur Darstellung der Maßnahmen zur Verbesserung der Ausfallsicherheit bei der Kommunikation zwischen einem Rechner an der TU Wien und dem Internet soll in diesem Abschnitt der Weg eines Pakets von einem Rechner in einem Gebäude der TU Wien (z. B. Favoritenstraße) bis in das Internet dargestellt werden.

von	nach	via	Maßnahme
PC/ Ethernet karte	Etagen Switch Port	TP-Kabel	Keine Ausfallsicherheit durch TUNET möglich. Siehe 3.1
Etagen Switch	Gebäude Switch	Glas-strecke	Pro Gebäude 2 Backbone Switche. Je ein Weg zu jedem Gebäude Switch. Siehe 3.2
Gebäude Switch	Gebäude router	Intern od. Glas-strecke	Pro Gebäude 2 Backbone Router. Siehe 3.3
Gebäude Router/ Switch	Core-Router	Glas-strecke	2 Core Router auf der TU Wien. Je ein Weg zu jedem Gebäude Switch. Siehe 3.3
Core Router	Gebäude Router/Switch ZID oder Karlsplatz	Glas-strecke	Pro Gebäude 2 Backbone Router + Switche. Siehe 3.3
Gebäude Router/ Switch	Etagen Switch	Glas-strecke	Nur bei Weg über ZID
Gebäude Switch oder Etagen-switch	Firewall	Kupfer	Zum inneren Interface des Firewalls. Jeweils ein Firewall im ZID und am Karlsplatz in einer Active/Standby Konfiguration
Firewall	Anbindungs switch	Kupfer, 100 MBit/s	Je ein Anbindungs-switch pro Gebäude, untereinander verbunden. Kann Verkehr, wenn z.B. gebäudeeigener Firewall ausgefallen ist, zum anderen Gebäude leiten.

Anbindungs switch	Anbindungs router	Glas-patchung	Je ein Anbindungs-router am ZID und am Karlsplatz. Hier wird entschieden, wohin das Paket geschickt werden soll (ACOnet, Internet, Teleweb, Inode)
Anbindungs router	Anbindungs switch	Glas-patchung	
Anbindungs switch	AConet / Teleweb	Glas-strecke	
ACOnet Router	Internet	Glas-strecke	

Wie schon innerhalb der TU Wien dargestellt, kann der Rückweg infolge der Alternativwege ein anderer sein. Der vereinfachte Ablauf ist auch in folgender Grafik dargestellt:



Redundante Server, wie externe Nameserver, Mail-Bastionsrechner sind in einer DMZ, die redundant an beide Firewalls angeschlossen sind, platziert (in der Grafik nicht dargestellt).

Wenn verfügbar, sind die Geräte der externen Anbindung mit zwei Stromversorgungen ausgestattet. Überall sind entsprechende USVs vorhanden (mindestens 4 Stunden Überbrückungszeit). Die Geräte sind alle gebäuderedundant (Freihaus / Karlsplatz) ausgeführt. Die Verbindungswege führen soweit wie möglich über unterschiedliche Trassen und sind zum Teil doppelt (zumindest logisch gesehen) ausgelegt.

Die Firewalls verwenden eine ähnliche Technik, wie bereits beim HSRP-Protokoll beschrieben, um dem aktiven Firewall immer die gleiche Mac-Adresse und IP-Adresse zu geben. Bei den externen Routern wird das BGP Protokoll (*Border Gateway Protocol*) verwendet, das umfangreiche Möglichkeiten der Steuerung von redundanten Wegen zu Destinationen im Internet vorsieht.

Internet-Räume, Wählleitungszugänge, TU-ADSL, xDSL@student, Demonetz und WLAN werden über eine ähnliche Konstruktion mit einem eigenen Firewall-Paar zu den externen Routern geführt.

5. Maßnahmen bei Servern

In Abschnitt 3 sind die Methoden zur ausfallsicheren Übertragung von Paketen von Punkt A nach B, dem „TUNET Transport Dienst“, dargestellt worden. Man hat aber nichts davon, wenn ein Paket erfolgreich zum Server transportiert wurde, der Server ist aber nicht betriebsbereit. Es müssen daher auch eine Reihe von Maßnahmen bei den Servern getroffen werden.

Bei Servern gibt es grundsätzlich 3 Ebenen, auf denen die Betriebssicherheit angegangen werden kann:

- Auf der Ebene der Kommunikationsprotokolle (ISO-Schichten höher als 4) kann bereits die Möglichkeit eines Failovers auf einen anderen Server vorgesehen sein.
- Man kann durch externe Geräte oder Software-Komponenten das Service von einem Server auf einen anderen umschalten.
- Im Server selber werden entsprechende Maßnahmen getroffen.

5.1 Redundanz bei Kommunikations-protokollen

Wenn bereits beim Design der Kommunikationsprotokolle die Nutzung von redundanten Servern vorgesehen wurde, ist dies natürlich die angenehmste Variante. Man braucht einfach nur zwei oder mehr Server aufstellen und sowohl Server und meistens auch Clients müssen richtig konfiguriert werden. Leider ist dies nur bei wenigen Protokollen wirklich der Fall. So gibt es etwas Derartiges bei den wichtigen Protokollen HTTP und FTP leider nicht.

5.1.1 Nameservice http://nic.tuwien.ac.at/services/name/

Eines der grundlegenden Protokolle für den Betrieb des Internet ist das Nameservice. Dessen Aufgabe ist die Umsetzung von Namen auf Adressen (und umgekehrt) und das Liefern von einigen wenigen Zusatzinformationen (wie den richtigen Mailserver).

Vom Design des Nameservice handelt es sich um eine weltweit verteilte Datenbank (vermutlich die größte überhaupt) mit lokaler Cache Funktion. Pro Domain (z.B. tuwien.ac.at) müssen mindestens zwei Nameserver existieren, die möglichst auf Servern, die in unterschiedlichen Gebäuden, wenn möglich sogar Netzen bzw. Providern bzw. Kontinenten aufgestellt sind. Ein Client (Arbeitsplatzrechner) konfiguriert die lokalen Nameserver der jeweiligen Organisation (tunamea und tunameb an der TU Wien) mit deren IP-Adressen (der Name kann ja nicht ohne das Nameservice selber auf eine Adresse umgesetzt werden). Die Anfragen eines Client gehen daher immer zum lokalen Nameserver mittels des DOMAIN Protokolls (in der Regel wird die UDP-Variante verwendet). Dieser kann die Antwort auf Grund der Daten im Cache geben oder fragt einen anderen Nameserver (normalerweise bereits den richtigen Nameserver für die Domain) und gibt dann die Antwort.

Wenn ein Client in einer gewissen Zeit keine Antwort vom Nameserver bekommt, fragt er den nächsten konfigurierten Nameserver. Leider dauert dieser Umschaltvorgang relativ lange (und ist auch vom jeweiligen

Betriebssystem am Client abhängig), sodass das Umschalten meistens vom Anwender bemerkt wird. Verzögerungen treten auch an Stellen auf, wo man es nicht ad hoc erwartet. So erfragen viele Server beim Login-Vorgang den Namen, der zu einer IP-Adresse gehört, um diesen Namen bei Security-Überprüfungen und für das Logging zu verwenden. Da dies auch über den Nameserver abgewickelt wird, treten damit hier Verzögerungen auf.

Für die Domain tuwien.ac.at gibt es innerhalb der TU Wien zwei Server (tunamea und tunameb), die im Freihaus und in der Favoritenstraße aufgestellt sind. Die Generierung der Konfigurationsfiles für den Nameserver aus der TUNET Datenbank erfolgt einmal am Tag auf einem anderen Server, auf dessen lokalen Nameserver die neuen Daten auch aktiviert werden. Von dort holen sich dann obige Nameserver die neuen Daten, Subdomain für Subdomain, über einen längeren Zeitraum. Ein direktes Aktivieren aller Nameserverdaten (da jede Domain ein eigenes File ist, sind diese Daten auf etwa 250 Files verteilt) würde eine Störung von 1-2 Minuten des Nameservice bewirken !

Für die Abfrage nach Daten der TU Wien von Nameservern in der weiten Welt stehen zwei eigene Nameserver (tunamec und tunamed) an den Standorten Freihaus und Karlsplatz (in der DMZ des Firewalls der TU Wien möglichst nahe am Anschluss zum Internet Provider). Auch hier werden die Daten am TUNET Datenbank Server generiert und lokal aktiviert.

Für das Nameservice für Domains der TU Wien ungleich tuwien.ac.at („Fremddomains“) werden zwei eigene Server (tunamee, tunamef) im Freihaus und am Karlsplatz eingesetzt. Hier erfolgt die Generierung nicht aus der TUNET Datenbank sondern wird per Hand in den Text-Files eingetragen. Bei Änderungen erfolgt dann ein *Reload* des jeweiligen Nameservers, da hier wegen der geringen Datenmengen nur eine minimale Unterbrechung auftritt. (Eine Zusammenlegung mit den externen Nameservern würde bei diesen aber eine lange Unterbrechung erfordern.)

Die Nameserver für die Domain ac.at sind neben Wien (mehrere Standorte) auch in Deutschland und den Niederlanden aufgestellt. Für das Nameservice von at kommen noch Standorte in USA und UK dazu.

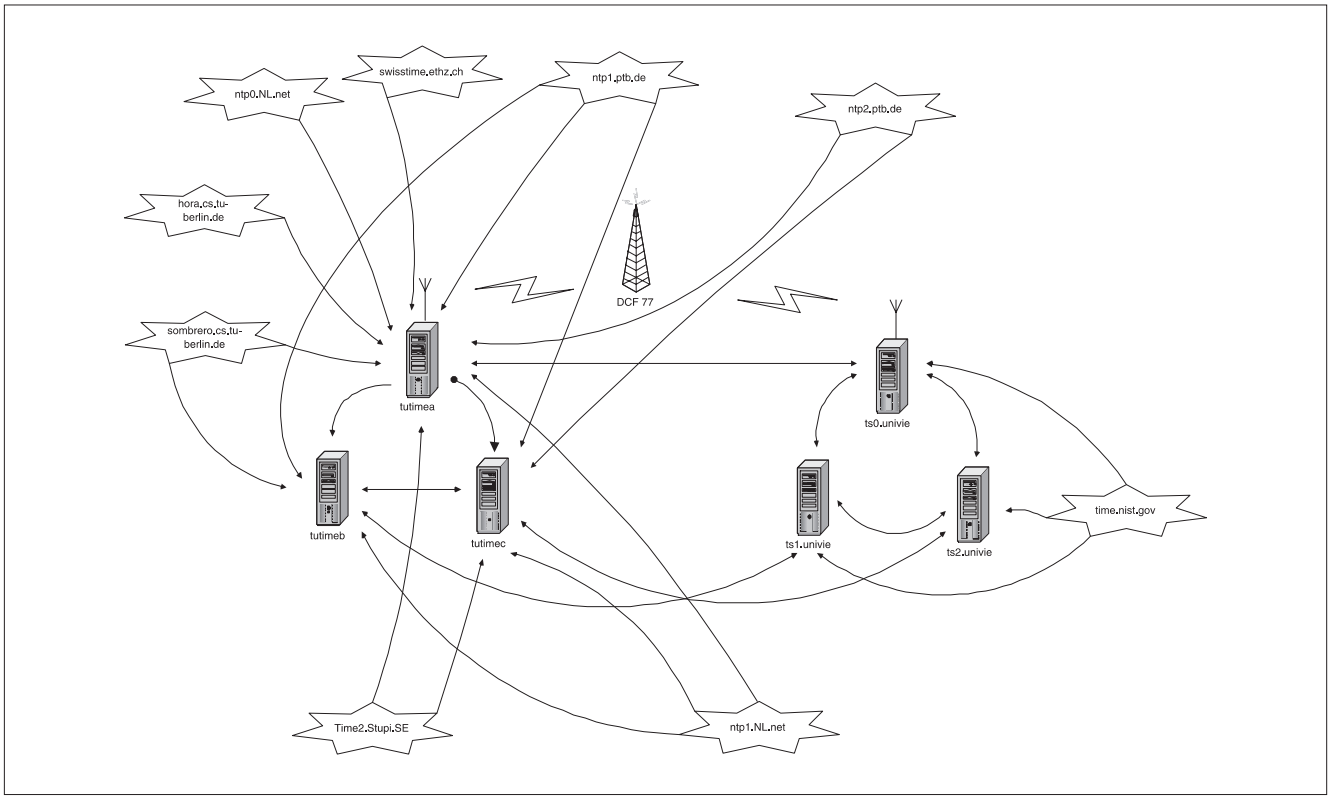
5.1.2 Timeservice

Die Timeserver werden untereinander mit dem NTP Protokoll synchronisiert. Das Konzept sieht einerseits eine Hierarchie der Server vor, die durch den Abstand, dem Stratum (Anzahl der Timeserver), zu einem Referenzserver (einer Atomuhr) bestimmt wird. Ein Server synchronisiert sich normalerweise mit mehreren Servern einer besseren Hierarchie und auch mit Servern der gleichen Hierarchie. Wenn alle Verbindungen zu anderen Servern ausfallen, steht immer noch die lokale Uhr des Rechners im „Freilauf“ zur Überbrückung zur Verfügung.

Auf der TU Wien sind drei Timeserver aufgestellt, zwei im Freihaus, einer in der Favoritenstraße. Einer der Timeserver im Freihaus erhält über eine Funkverbindung (Langwelle) Zeitsignale vom DCF77 Sender in Mainflingen bei Frankfurt, die auf Basis einer Atomuhr erzeugt werden.

Damit ein Client die Redundanz ausnutzen kann, müssen natürlich am Arbeitsplatzrechner mindestens zwei Server konfiguriert werden (siehe http://nic.tuwien.ac.at/services/time/).

Anbei eine Darstellung der derzeitigen Vernetzung unserer Timeserver.



5.1.3 Mailrouting

Beim Weiterleiten von Mails auf Basis des Domainnamens nach dem @ (also nicht des Mailboxnamens !) gibt es die Möglichkeit, mehrere Zielrechner, an die die Mail zugestellt werden soll, mit unterschiedlichen Prioritäten zu definieren. Dies erfolgt mit eigenen Einträgen im Nameserver, den MX-Records. Hierbei werden z.B. für Mailadressen der Form *mailbox@tuwien.ac.at* mehrere MX-Records eingetragen. In diesem konkreten Fall werden als Zielrechner die beiden Systeme *mri1.tuwien.ac.at* und *mri2.tuwien.ac.at* definiert, wobei *mri1* die bessere (numerisch niedrigere Priorität) hat, und damit der Verkehr normalerweise über diesen Rechner geführt wird. Erst bei Ausfall (Nichterreichbarkeit des SMTP-Ports) wird versucht, die Mail an *mri2* zuzustellen. Um eine Lastaufteilung zu bewirken, werden Mails an *mailbox@student.tuwien.ac.at* primär an *mri2* zugestellt, bei Ausfall an *mri1*, d.h. für ankommende Mails an die Adressen *@tuwien.ac.at* und *@student.tuwien.ac.at* stehen zwei Rechner bereit, einer im Freihaus und einer in der Favoritenstraße.

Ähnlich wird bei den Mailbastionsrechnern, über die alle ankommende Mail (außer @tuwien.ac.at und @student.tuwien.ac.at) der TU Wien geführt wird, gearbeitet. Auf den externen (und nur dort) Nameservern ist für Mailrechner auf Basis der Eintragung in der TUNET Datenbank (Attribute MAIL/BASTION) eine Umleitung der Mails auf die beiden Bastionssysteme tuvok.kom.tuwien.ac.at und neelix.kom.tuwien.ac.at mittels MX-Records definiert. Diese Eintragungen haben beide die beste Priorität (0). Damit erfolgt automatisch eine Lastaufteilung (je nachdem, welchen der beiden Einträge der abschickende Rechner verwendet). Als dritter Eintrag sind der/die Rechner innerhalb der TU Wien mit einer schlechteren Priorität eingetragen. Für den Fall, dass beide Bastionsserver über längere Zeit gestört sind, kann daher per Hand auf den Firewalls die Sperre des SMTP-Port aufgehoben werden, und die Mails werden direkt an die Zielrechner an der TU Wien zugestellt. Dadurch entfallen naturgemäß die Schutzmaßnahmen gegen Mail-Relaying und Viren. Die beiden Bastionsrechner stehen im Freihaus und am Karlsplatz und sind in der DMZ der TU Wien angesiedelt.

Neben diesen Möglichkeiten verwenden die *Mail Transfer Agents* (das sind jene Programme, die für die Weiterleitung von Mails im Internet zuständig sind) den Mechanismus, dass eine Mail, die nicht sofort zugestellt werden kann, in einer Queue gehalten wird. Diese Queue wird dann z.B. in regelmäßigen Abständen abgearbeitet. Üblicherweise wird nach 4 Stunden Nichtzustellbarkeit der Absender darüber informiert (Warnung), es wird aber weiter versucht, die Mail zuzustellen. Erst nach 3-5 Tagen (je nach Konfiguration des MTA, an der TU Wien 5 Tage) wird aufgegeben, und die Mail wird als unzustellbar an den Absender zurückgewiesen.

Die Überprüfung auf Viren der Mails erfolgt über insgesamt 4 eigene Virenscanner, die auf drei Standorte der TU Wien verteilt sind. Einem Mailrouter bzw. Bastionsrechner sind ein bis zwei Virenscanner zugeordnet. Wenn keiner dieser Scanner erreichbar ist, wird der Absender mittels eines temporären Fehlercodes darüber informiert, sodass er einen anderen Mailrouter versuchen kann.

Anzumerken ist, dass bei von der TU Wien abgehender Mail (z. B. über die Server mr.tuwien.ac.at, pop.tuwien.ac.at, stud3.tuwien.ac.at) der Mechanismus der MX-Records nicht zur Anwendung kommen kann, da der „*Outgoing SMTP Server*“ fix im Client (z. B. Eudora, Outlook Express, Netscape, …) konfiguriert werden muss. Hier müssen dann Methoden, wie in 5.2 dargestellt, zur Verbesserung der Betriebssicherheit eingesetzt werden.

5.1.4 Validierung Wählleitungen / VPN / ADSL / …

Die Terminalserver, der VPN-Konzentrator, die Router für die Tunnelendpunkte für das TU-ADSL Service und xDSL@student sowie die Gateways zwischen Demo-Netz bzw. WLAN und dem TUNET verwenden zur Abwicklung der Validierung das RADIUS-Protokoll nach RFC2138. Alle Geräte bieten die Möglichkeit zwei (oder mehr) Radius-Server zu konfigurieren, die in einer definierten Reihenfolge versucht werden. An der TU Wien sind zwei Radius-Server installiert, die alle im Freihaus stehen (auch alle Services, die die Validierung benötigen, stehen im Freihaus), jedoch in unterschiedlichen Räumen und Netzbereichen angesiedelt sind.

5.2 Ausfallsicherheit durch Content Switch

Für Protokolle, die ein Umschalten auf Backupsysteme nicht so wie in 5.1 vorsehen, müssen andere Verfahren eingesetzt werden. Erste Voraussetzung ist, dass das Service auf mehr als einem System angeboten wird. Nun geht es darum, bei einem Ausfall des Hauptsystems innerhalb möglichst kurzer Zeit umzuschalten. Im Wesentlichen gibt es drei Verfahren:

- Durch trickreiche Manipulation der Nameserverdaten wird die nun aktive IP-Adresse für das Service von den Nameservern geliefert. Dies setzt voraus, dass ein entsprechender Abgleich der Nameserverdaten (auf den für die Subdomain, in der der Server liegt, zuständigen Nameserver) mit der Verfügbarkeit des Servers über irgendeinen Monitorprozess erfolgt. Weiters muss die Cache-Zeit für den Nameservereintrag sehr kurz (z.B. 1 Minute) gesetzt werden, so dass weltweit alle Nameserver, die diesen Eintrag zwischenspeichern, schnell die neue Adresse mitbekommen. Nachteil dieser Methode ist die hohe Abfragefrequenz auf den Nameservern. Diese Methode kann auch zum Lastausgleich zwischen mehreren Servern verwendet werden (z.B. bei Serverfarmen). Wir hatten so eine Methode vor einigen Jahren einmal eingesetzt, waren im Endeffekt aber damit nicht zufrieden.

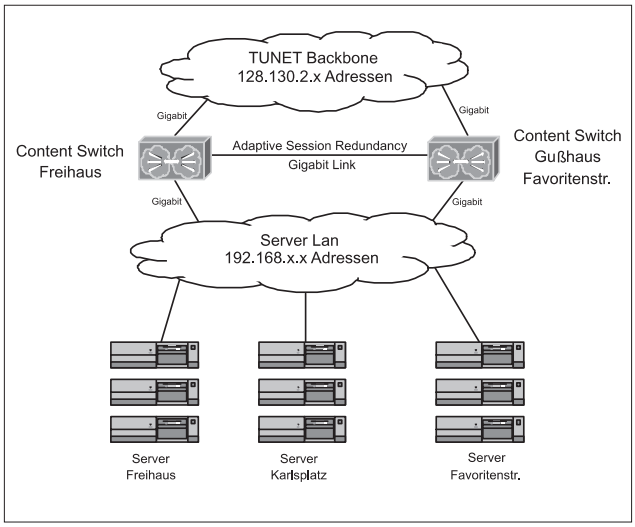
- Die beiden Server überwachen sich gegenseitig (meistens über eine eigene Verbindung) und tauschen unter Umständen auch Statusinformationen (z.B. über aktive Sessions) aus. Ähnlich wie beim HSRP-Protokoll (siehe 3.2.3) ist dem aktiven Server die „virtuelle“ IP-Adresse des Services zugewiesen. Dieses Verfahren wird zum Beispiel beim Software Distribution Server der Abteilung Standardsoftware eingesetzt. Vorteil dieses Verfahren ist, dass keine zusätzliche Hardware notwendig wird. Nachteil ist, dass die dafür notwendige Software meistens plattformspezifisch ist und man sich komplizierte

Abhängigkeiten von dieser Software am jeweiligen System schafft. Meistens ist eine derartige Software auch recht teuer. Ob eine Variante mit Servern mit unterschiedlichen Betriebssystemen unterstützt wird, ist fraglich.

- Es wird ein externes Gerät (*Content Switch*) verwendet, das die „virtuelle" IP-Adresse serviciert und an diese Service-Adresse ankommende Pakete je nach Verfügbarkeit (und Lastsituation oder anderer Kriterien) auf die Server, die das Service anbieten, verteilt. Die entsprechenden Antworten schickt der Server dann wieder an den Content Switch, der im IP-Paket die Adressen umsetzt und an den Client zurückschickt.

Im Frühjahr vorigen Jahres wurden mehrere Firmen zu einer Teststellung für einen Content Switch eingeladen. Dabei wurde an Hand einiger typischer Services (Protokolle) am ZID die Funktionalität der Testsysteme überprüft und entsprechend gegenübergestellt. Im Ergebnis fiel dann, nicht zuletzt auch wegen der Preisrelationen, die Entscheidung zu Gunsten der Content Switche der Firma Cisco Systems, konkret das Modell CSS 11503. Die Geräte wurden Ende 2002 geliefert und dann unterschiedliche Konfigurationen im Detail untersucht. Schrittweise werden nun alle Services der Abteilung Kommunikation mittels dieser Geräte redundant angeboten. Content Switche werden auch als ISO Layer 4-7 Switche bezeichnet.

In der folgenden Abbildung ist die logische Konfiguration des Content Switch dargestellt:



Ein Content Switch bietet eine Reihe von Möglichkeiten, die eine große Flexibilität ermöglichen:

- Nicht alle Services, die unter einer IP-Adresse angeboten werden, müssen von den gleichen Servern erbracht werden. Es sind Unterscheidungen nach der Port-Nummer (also z.B. FTP und http) sowie nach der URL (Prefix, Filetyp) möglich.

- Die Anzahl der Server kann leicht geändert werden.

- Die Aufteilung auf die einzelnen Server kann nach einer Vielzahl von Methoden (Round Robin, Last Used, Prioritäten, Last ,..) erfolgen.

- Ob die einzelnen Server (bzw. genauer Services auf den Servern) verfügbar sind, kann nach verschiedenen Methoden bestimmt werden.

- Bei http (und SSL) werden Sessions (z. B. anhand von Cookies oder SSL-Ids) erkannt, so dass eine begonnene Session immer am gleichen Server bleibt (da ja vielleicht nur dieser sessionspezifische Daten gespeichert hat).

- Zur Performance-Steigerung und Entlastung der Server können HTTPS Verbindungen am Content Switch terminiert werden. Dies ist auch Voraussetzung, dass eine URL-spezifische Weiterleitung zu unterschiedlichen Servern erfolgen kann.

Die beiden Content Switche werden gebäuderedundant im Freihaus und in der Gußhausstraße (oder Favoritenstraße) aufgestellt und direkt an einen Backbone Switch angeschlossen. Untereinander sind die beiden Content Switche über einen dedizierten Gigabit Link verbunden, um „*Adaptive Session Redundancy*" zu erlauben. Damit kann der Backup Switch auch aktive Verbindungen bei einem Ausfall des primären Switches übernehmen. In der Regel wird eine gleichmäßige Lastverteilung (Round Robin) konfiguriert. Mittels des Content Switches werden insbesondere die Services der White Pages (neue Version), Mailrouting, Abteilungsservices unter nic.tuwien.ac.at redundant angeboten.

Die Grenzen der Redundanz durch einen Content Switch und Verdopplung der Server sind bei Services, die Datenbestände im Hintergrund haben, wie z. B. die Web-Seiten beim Info-Server, die Mailboxen beim POP-Server und die TUNET-Datenbank. Hier sind dann wesentlich aufwändigere Konstruktionen zur gemeinsamen (redundanten) Datenhaltung erforderlich.

5.3 Maßnahmen beim Server

Auf den Servern selber werden die üblichen Maßnahmen getroffen:

- Gespiegelte System- und Datenplatten auf unterschiedlichen SCSI-Bussen.

- Möglichst redundante Stromversorgung, wobei mindestens eine Stromversorgung über USV erfolgt.

- Mehrere Speichermodule.

- Mehr als ein Ethernet Interface.

- Bei Geräten, die nur ein Ethernet Interface haben und das Service nur auf einer Maschine erbracht wird (z. B. pop.tuwien.ac.at), Anschluss über „Twister" an zwei Ethernet Switche.

- Tägliche (zumindest inkrementelle) Datensicherung.

- Reserve Systemplatte.

6. Telefonie

Auch wenn sich dieser Artikel hauptsächlich mit der Datenkommunikation beschäftigt, sollen hier kurz die Maßnahmen bei der Telefonie zusammengestellt werden:

- Die 24 Unteranlagen werden über zwei „Group Switche", die redundant im Freihaus und Karlsplatz aufgestellt sind, untereinander verbunden (bis auf die Standorte Atominstitut und Aspanggründe, die nur eine Leitung haben).
- Jede Anlage verfügt über gedoppelte Gleichrichter und einen Batteriesatz, der je nach Standort 4 bis 8 Stunden Stromausfall überbrücken kann.
- Die normalerweise verwendeten Außenanschlüsse (Multianschlüsse mit je 30 Kanälen) sind auf die Standorte Freihaus und Karlsplatz gleichmäßig verteilt und führen zu zwei unterschiedlichen Ortsämtern der Telekom Austria sowie zum alternativen Provider Colt, sodass bei Ausfall eines Standorts oder eines Ortsamts noch immer die Connectivity gegeben ist. Bei Ausfall des Ortsamtes Dreihuf der Telekom Austria müsste aber eine andere Hauptnummer für ankommende Gespräche gewählt werden (50690). Durch *Least Cost Routing* (LCR) wird bei Ausfall einer billigen Leitung auf eine teurere umgeschaltet.
- An jedem Standort existieren zwei bis drei direkte Amtsleitungen zur Telekom Austria (in der Regel POTS), die eine (minimale) Verbindung in die Außenwelt bei Ausfall sämtliche Verbindungen zu den Group Switchen sicherstellen.
- Die Server (z.B. für das Vermittlungstelefonbuch) sind gedoppelt auf die Standorte Freihaus und Karlsplatz und mit USV versorgt.
- Vermittlungsarbeitsplätze sind im Freihaus und am Karlsplatz eingerichtet (haben sich beim Gasunfall im Freihaus vor einigen Jahren sehr bewährt) und sind mit USV versorgt.

Nicht redundant möglich ist der Sprachspeicher (gespiegelte Platten sind aber im Einsatz).

Auch die Chipkarten-Überprüfung ist wegen der komplexen verteilten Konfiguration der Anlage nicht redundant.

7. Management

Ein wesentlicher Aspekt der Betriebssicherheit ist die Überwachung der Komponenten im Netzwerk. Hiezu werden eine Reihe von Tools eingesetzt und bei den Mitarbeitern angezeigt. Folgende Aspekte werden überwacht:

- Mittels *ping* alle Backbone Komponenten in relativ kurzen Abständen (ca. 2-5 Minuten).
- Mittels *ping* werden in größeren Abständen alle Etagenswitche überwacht.
- Mittels *ping* werden in größeren Abständen auch bekannte wichtige Server an Instituten (in der Regel Webserver) überwacht, um einen Indikator zu haben, ob die Erreichbarkeit von Endgeräten im TUNET gegeben ist.
- Die Server und Services werden nach unterschiedlichen Aspekten (Erreichbarkeit, CPU-Last, Plattenplatz, Verfügbarkeit von Service-Ports, Mailqueue, Temperatur) überwacht.
- Mittels SNMP werden bestimmte Parameter von Backbone Routern und Switches überwacht.
- Insbesondere im Backbone und bei der Internet-Anbindung wird das Verkehrsaufkommen überwacht.
- Raumbedingungen (Temperatur, Feuchte, Spannung, Tür) werden laufend überprüft.
- Laufende Auswertung von Logfiles nach kritischen Meldungen.
- Dokumentationssystem von durchgeführten Änderungen.
- Automatische Sicherung von Konfigurationen.
- Die Überwachung erfolgt teilweise von zwei Standorten aus (Freihaus, Favoritenstraße).
- Es existieren eigene interne Management-Netze (für Konsolen aber auch via Ethernet-Verbindungen), um z.B. Backbone Geräte auch dann erreichen und konfigurieren zu können, wenn das Produktionsnetz ausgefallen ist.
- Sicherheitsmaßnahmen unterschiedlicher Stufe bei allen Geräten.

8. Literatur

Betriebsfehler: Fehlertoleranz und Redundanz. Dirk Spöri

RFC 2281. Cisco Hot Standby Router Protocol (HSRP). T. Li, B. Cole, P. Morton, D. Li. (March 1998)

RFC 2338. Virtual Router Redundancy Protocol. S. Knight, D. Weaver, D. Whipple, R. Hinden, D. Mitzel, P. Hunt, P. Higginson, M. Shand, A. Lindem (April 1998)

RFC 2328. OSPF Version 2. J. Moy (April 1998)

DNS Resources Directory: http://www.dns.net/dnsrd

NTP: The Network Time Protocol: http://www.ntp.org/

RFC 2138, Remote Authentication Dial In User Service (RADIUS). C. Rigney, A. Rubens, W. Simpson, S. Willens (April 1997)

Ergänzung zum Entwurf aktive TUNET-Komponenten in den Institutsgebäuden der Technischen Universität Wien, Gußhausstraße 25 und 27-29. Manfred R. Siegl (August 2002).

Cisco LAN Switching. Kennedy Clark, Kevin Hamilton, Cisco Press (1999)

Building Cisco Multilayer Switched Networks. Karen Webb, Cisco Press (2000)

Interconnections: Bridges and Routers. Radia Perlman, Addison Wesley (1993)

Cisco TCP/IP Routing Professional Reference. Chris Lewis, McGraw-Hill (1998)

Routing in the Internet. Christian Huitema, Prentice Hall PTR (1995)

Online-Dokumentationsseiten des Herstellers Cisco System, CCO : http://www.cisco.com/

Studenten Software Service

Bernhard Simon

Die TU Wien ermöglicht ihren Studierenden nun schon das vierte Jahr den Bezug diverser Software zu äußerst günstigen Preisen. Dieses Service, das in der österreichischen Universitätslandschaft hinsichtlich Umfang und Attraktivität weiterhin einzigartig ist, wird vom Zentralen Informatikdienst – mit Unterstützung von HTU und Lehrmittelzentrum – betrieben und von der TU Wien stark subventioniert.

Dieser Beitrag gibt einen Überblick über das aktuelle Softwareangebot und die erzielten Verkaufszahlen, beschreibt die wichtigsten Neuerungen dieses Studienjahres und untersucht Kauf- und Update-Verhalten der Lizenznehmer.

Aktuelles

Das Softwareangebot umfasst derzeit 17 Produkte (16 lizenzpflichtig, davon 8 von Microsoft), die in Tabelle 1 aufgelistet sind. Neue Software des Studienjahres 2002/2003 sowie Updates sind extra gekennzeichnet.

Freeware					
neu	Goodie Domain Software	TU Selection 2003	Windows	Euro 10.-	DVD
Graphik/Visualisierung					
	LabVIEW	6 ***i***	Windows	Euro 4.-	CD
	SigmaPlot	6.1	Windows	Euro 4.-	CD
Mathematik					
upd	Maple	8	Windows, Linux	Euro 5.50	CD
upd	Mathematica	Version 4.2	Windows, Macintosh, Linux	Euro 5.50	CD
Office Automation					
	Lotus SmartSuite	Version 9.5, deutsch	Windows	Euro 4.-	CD
neu	MathType	5, deutsch/englisch	Windows, Macintosh	Euro 4.-	CD
	MS Office 2000	Professional, deutsch	Windows	Euro 6.-	CD
	MS Office XP	Professional, deutsch	Windows	Euro 6.-	CD
neu	ORACLE	9*i*	Windows, Linux	Euro 16.-	DVD
neu	StarOffice	6.0, deutsch/englisch	Windows, Linux	Euro 4.-	CD
PC Systemsoftware					
	MS Windows 98	Second Edition, deutsch		Euro 4.50	CD
	MS Windows Me	Millenium Edition, deutsch		Euro 4.50	CD
	MS Windows 2000	Professional SP2 deutsch		Euro 6.-	CD
	MS Windows XP	Professional, deutsch		Euro 6.-	CD
Programmierung, Utilities					
	MS Visual Studio	6.0, TU Edition, deutsch	Windows	Euro 7.-	CD
neu	MS Visual Studio .NET	Professional, deutsch/englisch	Windows	Euro 18.-	DVD

Tabelle 1: Studentensoftwareangebot

Am 1. 4. 2003 wurden die Lizenzbedingungen insofern vereinheitlicht, dass eine Studentenlizenz ab diesem Zeitpunkt nun bei allen Produkten nach Beendigung des Studiums erlischt.

Aus wirtschaftlichen Gegebenheiten (Aufwand bei der Produktzusammenstellung, hohe Stückzahlen bei der Produktion von Medien) ist es zurzeit nur vertretbar, **ein** Medium pro Produkt auszugeben. Um also den Wünschen der Studierenden nach Sprach- und Betriebssystem-Vielfalt nachzukommen, sollte dieses Medium möglichst viele dieser Anforderungen abdecken.

Seit vergangenem Jahr sind wir in der Lage, Studentensoftware auch auf DVD-ROM (DVD9, double layer, single side) zu verteilen. Diese nur mit professioneller Ausstattung herstell- und duplizierbaren Medien mit einer Kapazität von über 8 GB ermöglichen uns nun, auch umfangreichere Produkte (die uns derzeit von den Herstellern leider noch immer auf vielen CDs ausgeliefert

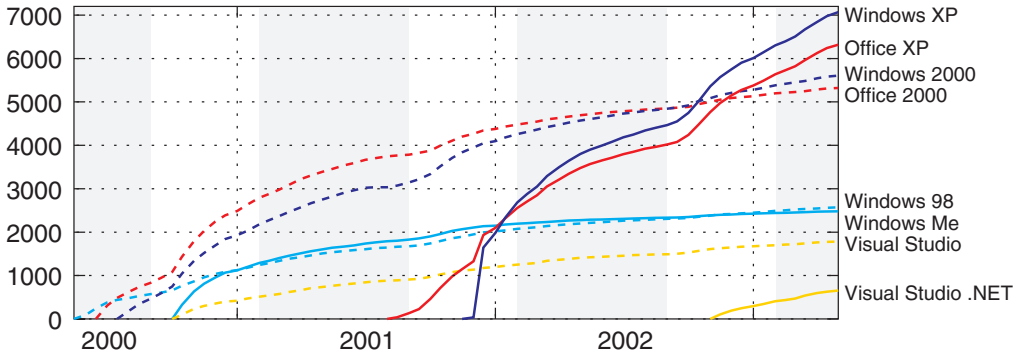


Abb. 1a: Lizenzentwicklung Microsoft Produkte

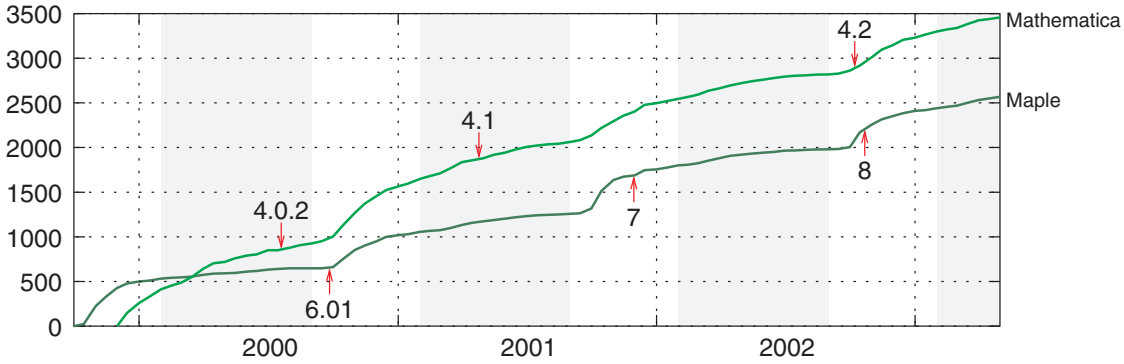


Abb. 1b: Lizenzentwicklung Mathematik Software

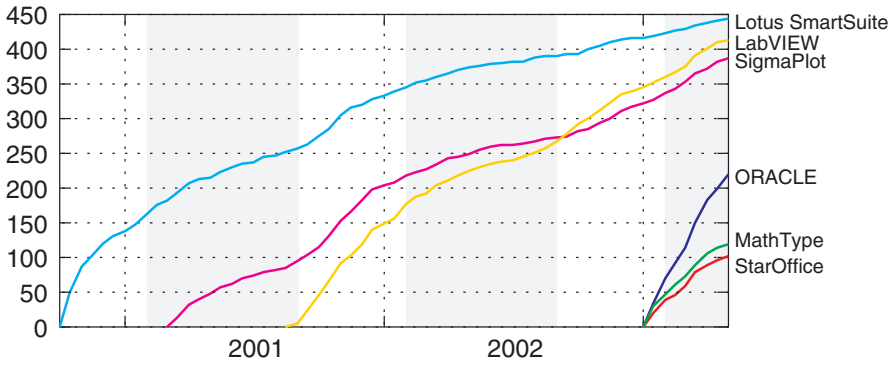


Abb. 1c: Lizenzentwicklung restliches Angebot

werden) nicht nur in vollem Umfang, sondern auch für verschiedene Betriebssysteme oder in mehreren Sprachvarianten zu führen. So enthält beispielsweise die Studenten-DVD mit Visual Studio .NET den Inhalt von 12 CDs (je 6 pro Sprache) und die ORACLE DVD insgesamt 14 CDs (je 7 pro Betriebssystem).

Im Rahmen dieser Qualitätsverbesserung wurde nun auch bei der Zusammenstellung von CDs versucht, dadurch einen Mehrwert zu erzielen, dass mehrere Produkt-CDs des Herstellers (für unterschiedliche Betriebssysteme oder Sprachen) nach Möglichkeit auf einer (Hybrid-) CD zusammengefasst wurden. Das gelang unlängst bei Mathematica, Maple, StarOffice und MathType – die Details sind der Produktaufstellung in Tabelle 1 zu entnehmen.

Ein weiterer Versuch, das Angebotsspektrum zu vergrößern, war die Produktion einer Freeware DVD, die auf ca. 8 GB eine Momentaufnahme der beliebtesten Downloads (primär PC Software) unseres weit bekannten Goodie Domain Servers (gd.tuwien.ac.at) beinhaltet. Nach deren Produkteinführung im Juni dieses Jahres wird sich zeigen, ob auch diese Initiative erfolgreich war, d.h. von den Studierenden genutzt wird.

Die Lizenzentwicklung der vergangenen Jahre ist in Abb. 1a (Microsoft Produkte), Abb. 1b (Mathematik Software) und Abb. 1c (restliches Angebot) grafisch dargestellt.

Diesen Grafiken – aber auch allen nachfolgenden Analysen – liegt das komplette Datenmaterial seit dem Verkauf der allerersten (damals noch selbst gebrannten und handbeschrifteten Maple) CD am 14. 10. 1999 bis zum 30. 4. 2003 zugrunde. In diesem Zeitraum wurden insgesamt 39510 Lizenzen an 12276 verschiedene Studenten vergeben, also im Schnitt etwa 3.2 Lizenzen pro (kaufendem) Studenten. Eingeteilt nach Produktgruppen, hat Microsoft mit 80.5% der Lizenzen den Löwenanteil, gefolgt von Mathematica/Maple mit zusammen immerhin 15.2%, die restlichen 6 Produkte machen nur 4.3% aus. Pro Studienjahr sind jetzt durchschnittlich 18500 Studierende bezugsberechtigt (vor dem WS 01/02 noch etwa 25000), von denen etwa 30% Studentensoftware erwerben, davon ungefähr 2500 – das sind 13.5% – Studienanfänger, von denen etwas mehr als 20% das Angebot nutzen.

Da Erstsemestrige bereits im September bzw. im Februar Software beziehen, werden hier die 5 Monate vom 1. 9. - 31. 1. bzw. die 7 Monate vom 1. 2. - 31. 8. als Winter- bzw. Sommer-(verkaufs-)semester definiert. Diese Intervalle sind in den Lizenzentwicklungs-Grafiken hervorgehoben.

Kaufverhalten

Aus den Lizenzentwicklungskurven lassen sich folgende Gemeinsamkeiten herauslesen:

- starker Anstieg (große Nachfrage) bei Einführung eines Produkts,
- abklingendes Verhalten (Verkaufsrückgänge) im Laufe der Zeit,
- Zuwächse (zum Teil signifikant) am Beginn des Wintersemesters,
- keine Besonderheiten zu Beginn des Sommersemesters.

In der Microsoft-Grafik fällt speziell der explosionsartige Start von Windows XP auf, der Office XP mitzureißen scheint (XP-Effekt). Die Kurven von Mathematica/Maple – Produkte, die am längsten im Angebot sind, – zeigen beide einen gleichmäßig periodischen Verlauf, der auch durch Updates – egal zu welchem Zeitpunkt – nicht gestört wird. Bei Maple sind die starken Zuwächse im Oktober auffällig, die sich dadurch erklären lassen, dass diese Software in einer Massenlehrveranstaltung des Wintersemesters empfohlen wird.

Die Grafiken Abb. 2a und Abb. 2b beziehen sich auf im jeweiligen Verkaufssemester vergebene Lizenzen, wobei WS 99/00 sowie SS 00 (nicht signifikant) und SS 03 (nicht komplett) nur vollständigkeitshalber angeführt sind. Lizenzen der Produktgruppen Microsoft bzw. nicht-Microsoft sind blau bzw. orange dargestellt. Der Anteil von Studienanfängern wurde im unteren Teil der Balken extra hervorgehoben. Schraffiert sind Lizenzen von Studenten, die Software aus beiden Produktgruppen bezogen, wogegen Lizenzen von Studenten, die ausschließlich Software einer Produktgruppe erwarben, nicht schraffiert dargestellt sind.

Die absoluten Verkaufszahlen aus Abb. 2a zeigen, wenn man sich den XP-Effekt im WS 01/02 und SS 02 wegdenkt, ein gleichmäßiges Verhalten: In den 5 Monaten des Wintersemesters werden deutlich mehr Lizenzen vergeben als in den 7 Monaten des Sommersemesters, was nicht besonders verwunderlich ist, werden doch bei manchen Produkten bis zu 30% des Jahresumsatzes im Oktober erzielt.

Aus den dazugehörigen relativen Verkaufszahlen in Abb. 2b lässt sich ablesen, dass mindestens 60% der Lizenzen eines Semesters von Studenten erworben werden, die ausschließlich Microsoft Produkte kaufen und der Anteil der Studienanfänger in Sommersemestern etwa ihrem Anteil von 13.5% an der Gesamtstudentenzahl entspricht, jedoch mit ungefähr 20% in Wintersemestern überdurchschnittlich größer ist. Weiters zeigt sich, dass sich die bei den Höhersemestrigen feststellbaren Relationen bezüglich der Produktgruppen auch im Kleinen (bei den Studienanfängern) widerspiegeln.

Für die Untersuchung des Update-Verhaltens kommen nur Mathematica und Maple in Frage, weil sie die einzigen Produkte im Produktspektrum sind, von denen regelmäßig (jährlich) aktuelle Versionen angeboten werden, allerdings – um die Subventionen optimal zu nutzen – erst dann, wenn die vorherige Version restlos ausverkauft ist, d.h. es wird versucht, gerade so viele Medien zu produzieren, wie in einem Jahr abgesetzt werden können. Die Update-Zeitpunkte sind in Abb. 1b dargestellt. Pro Studienjahr werden durchschnittlich 900 Mathematica Lizenzen (Tendenz fallend) und etwas mehr als 650 Maple Lizenzen (Tendenz gleichbleibend) vergeben.

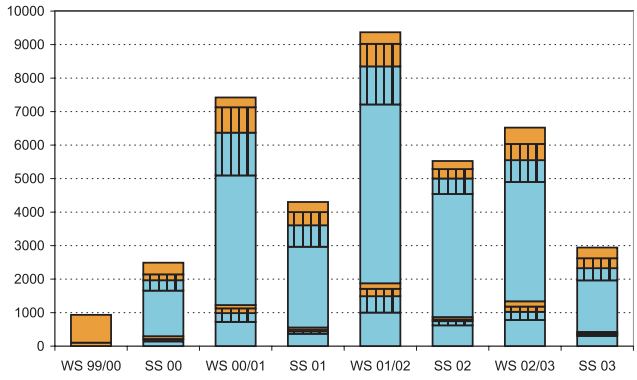


Abb. 2a: Verkaufszahlen pro Semester (absolut)

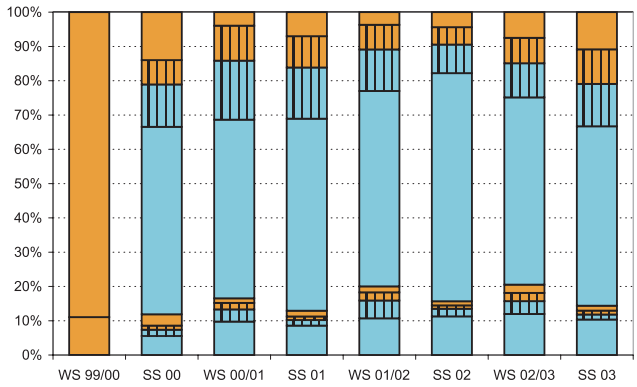


Abb. 2b: Verkaufszahlen pro Semester (relativ)

In den Abbildungen Abb. 3a und Abb. 3b wird das Update-Verhalten bei Mathematica und Maple gegenübergestellt. Ausgangsmaterial sind die Lizenzdaten jeder Version, klassifiziert danach, ob es sich um einen Erstkauf (ganz hell) oder um das erste, zweite, ... Update (immer dunkler werdend) einer bereits existierenden Lizenz einer älteren Version handelt. Zur besseren Vergleichbarkeit sind die prozentuellen Anteile dieser Kategorien dargestellt. Studienanfänger, die ja im allgemeinen nichts zum Update-Verhalten beitragen, sind – wie schon zuvor – im unteren Teil der Balken gekennzeichnet.

Bei Mathematica in Abb. 3a fällt zunächst der beinahe konstante Anteil von 20% der Studienanfänger auf, der Beitrag von Update-Lizenzen nimmt zwar ständig zu, ist aber (noch) nicht signifikant. Im Vergleich dazu ist dieser Update-Beitrag bei Maple in Abb. 3b jedesmal um etwa 10% größer.

Noch auffälliger ist jedoch der mit 40% doppelt so große Anteil der Studienanfänger in den beiden mittleren Balken. Dieser ist einerseits dadurch zu erklären, dass es sich bei der im Zusammenhang mit Maple bereits erwähnten Massenlehrveranstaltung um eine Vorlesung für Erstsemestrige handelt, andererseits auch dadurch bedingt, dass die jährlichen Update-Zeitpunkte – wie in Abb. 1b gut erkennbar ist – im Gegensatz zu Mathematica nicht immer synchron zu den Semester-Perioden (z.B. immer vor dem Oktober) gewählt werden konnten.

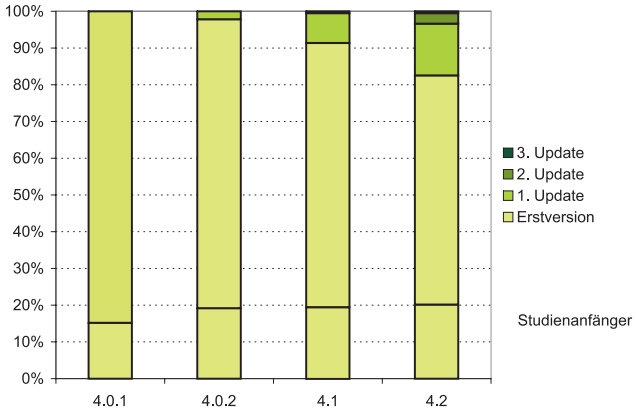


Abb. 3a: Update-Verhalten bei Mathematica

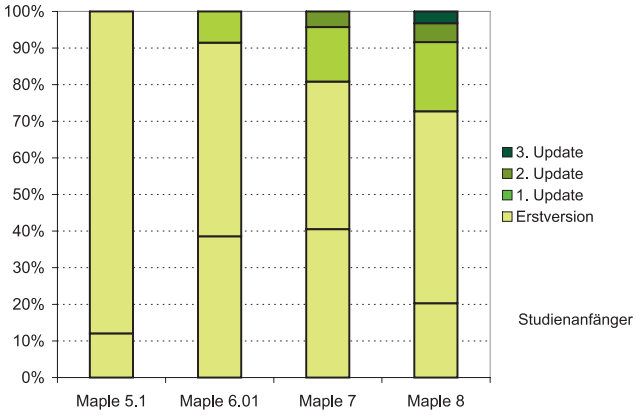


Abb. 3b: Update-Verhalten bei Maple

Vorschau

Für das Studienjahr 2003/2004 sind wieder die gewohnten Updates bei Mathematica und Maple geplant. Weiters ist bereits abzusehen, dass die 2003er Versionen von Office und Visual Studio ins Programm aufgenommen werden. Sollte sich die neue Freeware DVD bewähren, ist auch hier eine regelmäßige Aktualisierung zu erwarten.

Die Einführung einer Chipkarte für Studierende würde zunächst eine Erleichterung in den Bereichen Verkauf und Administration bringen und könnte sogar – bei entsprechender Funktionalität und Infrastruktur – einen Online-Bezug von Studentensoftware ermöglichen.

Jenseits von Word und diesseits von TeX

Gerhard Hanappi
Institut für Volkswirtschaftslehre und Wirtschaftsinformatik, TU Wien
hanappi@pop.tuwien.ac.at

Der Produktionsprozess wissenschaftlicher Artikel unterlag im Zuge der Ausbreitung und Weiterentwicklung von Textverarbeitungssystemen einem tiefgreifenden Wandel. So kritzeln manche alt gebliebene Gelehrte ihre ersten Entwürfe künftiger Artikel immer noch mit Bleistift auf kleine Zettelchen, die dann (nach teilweisem Verlorengehen und Mischen) an Mitarbeiter weitergegeben werden, die den genialen Entwurf ohne Kenntnis seines Inhalts in maschinenlesbare Form bringen. Andere, sich als Publikationslawinen profilierende KollegInnen sitzen selbst am Gerät und produzieren beständig multipel einsetzbare Textblöcke, die dann in der Folge zu einem permanenten Fluss „neuer" Forschungspapiere kombiniert werden – die Möglichkeiten moderner Textverarbeitung, die Unübersichtlichkeiten von Forschungslandschaften und der Druck zur Maximierung der **Anzahl** von Publikationen verführen da zu manchmal fragwürdigen Vorgangsweisen.

Bezogen auf die verwendeten Textverarbeitungssysteme ist zudem ein *Clash of Cultures* ganz besonderer Art zu beobachten: Einerseits ist in den bereits stark mathematisch formulierten Wissenschaftsbereichen ein Produktionsprozess entstanden, der ohnehin zunächst vom Einsatz des Computers als Rechner ausgeht und daher die Versatilität des Autors im Umgang mit dem Gerät rasch zu einer Wahl von Textverarbeitungslösungen mit bestimmten Vorzügen in der Darstellung mathematischer Ausdrücke – auch wenn das ein wenig umständlich ist – führt. Kurz gesagt, die Wahl dieser Wissenschaftskultur fällt auf TeX. Andererseits existiert eine weniger penible, oft auch computerfernere WissenschaftlerInnengemeinde, der das Wald- und Wiesenprogramm MS-Word als Montageinstrument vollauf genügt. Zudem kann Word mit dem Add-on MathType auch noch ein wenig mathematische Notation aufgedrängt werden, wenn es denn sein muss.

Zwischen diesen beiden Kulturen versucht sich nun bereits seit einiger Zeit eine dritte Art von Software zu positionieren: **Scientific WorkPlace** ist dadurch gekennzeichnet, dass es sowohl mittels Maple rechnen kann, als auch (in derselben Anwendung) eine gewöhnliche Textverarbeitung inklusive dynamisch erzeugter Grafiken möglich ist. Diese Integration von Rechnen und in Forschungspapiere Verarbeiten dürfte insbesondere für jene Forscher interessant sein, die ihren Forschungsprozess ohnehin selbst – vom grundlegenden mathematisierten Gedanken bis zur Paperproduktion – selbst in die Hand nehmen. Und diese Gruppe scheint mir in den letzten Jahren stetig zu wachsen. Der Einsatz von Produkten wie Scientific WorkPlace sollte demgemäß künftig stark zunehmen. Schwachstellen, auf deren Beseitigung sich die Produzenten solcher Software hoffentlich konzentrieren werden, bestehen natürlich vor allem im Bereich der Kompatibilität mit anderer Software: Wie bekomme ich Texte, Formeln und Grafiken von einer Umgebung in die andere, ohne Formatierungsmerkmale zu verlieren. Nach wie vor vermischen sich hier die Bemühungen einzelner Hersteller um gewinnmaximierende Inkompatibilität auf benutzerfeindliche Weise mit tatsächlichen Inkompatibilitäten der logischen Herangehensweisen der Programmstrukturen. Es gibt diesbezüglich zwar überall langsame Fortschritte – siehe PDF Format – doch bleiben nach wie vor viele Wege verschlossen.

Der Grund, warum immer noch recht wenig Gebrauch von Software wie Scientific WorkPlace zu verzeichnen ist, dürfte meines Ermessens jedoch nicht so sehr an solchen Schwachstellen liegen. Es ist vielmehr einerseits die nicht unberechtigte prinzipielle Angst davor, dass die Handhabung eines neuen Paketes viel Zeitaufwand bedeutet – was in diesem Fall allerdings eher unberechtigt ist. Andererseits spielt schlicht und einfach auch oft die Unkenntnis der Existenz solcher Lösungen die größte Rolle – und dagegen kann etwas getan werden: Einfach ausprobieren !

Scientific WorkPlace ist als Campussoftware für Institutsangehörige der TU Wien erhältlich (sts.tuwien.ac.at/css/).

Desktop Publishing Programme für umfangreiche und strukturierte Dokumente

Irmgard Husinsky

Zur Erstellung von umfangreichen Berichten (wissenschaftliche Publikationen, technische Dokumentationen, Bücher) von mehreren Hundert Seiten mit vorwiegend strukturiertem Text und vielen integrierten Tabellen und Grafiken kann sich der Einsatz eines DTP (Desktop Publishing)-Programmes lohnen. Hier werden die in der Campussoftware für TU-Institute zu günstigen Preisen erhältlichen DTP-Programme für Windows vorgestellt, vor allem in der Hinsicht, wie sie die Strukturen großer Dokumente unterstützen und wie sie bereits mit XML-Daten umgehen können.

Bei der computerunterstützten Dokumentenerstellung unterscheidet man

- dokumentenorientiertes, eher strukturiertes Arbeiten (textintensiv) und
- seitenorientiertes, eher unstrukturiertes Arbeiten (layout/grafik-intensiv, kreativ).

Für beide Arbeitsweisen können so genannte Desktop Publishing Programme eingesetzt werden. Sie kommen der häufigsten Anforderung in der Praxis nach hoher Flexibilität bei der Kombination von strukturiertem und seitenorientiertem, kreativem Arbeiten entgegen. Im Folgenden wird untersucht, wie DTP-Programme die Erstellung von umfangreichen und/oder strukturierten Dokumenten unterstützen.

Strukturierte Dokumente

Strukturierte Dokumente enthalten Metainformationen über die einzelnen (Text-)Bestandteile, die durch das Layout dargestellt werden können (Überschriften, Zitate, Fußnoten, etc.). Im Idealfall sind Inhalt und Struktur streng getrennt. Beim Layouten werden den einzelnen Elementen (Textabsätzen, Tabellen, Text- und Bild-Rahmen, etc.) Formate (Stile, *Tags*) zugewiesen. Wiederkehrenden Elementen derselben Struktur weist man den selben Stil zu.

Beispiele für strukturierte Dokumente:

- technische Dokumentationen,
- wissenschaftliche Publikationen,
- Diplomarbeiten, Dissertationen,
- Vorlesungsskripten,
- Jahresberichte, Projektberichte,
- Konferenz-Proceedings / Tagungsbände,
- Bücher,
- Kataloge (*Database Publishing*).

Einsatz eines DTP-Programms

Das Werkzeug erster Wahl für strukturierte Dokumente ist für viele sicher das Satzsystem LaTeX, das vor allem durch seine Stabilität und die Schönheit des Layouts (besonders im Zusammenhang mit mathematischen Formeln) besticht. Wer LaTeX nicht lernen möchte, kann *Scientific Word* bzw. *Scientific WorkPlace* verwenden (siehe dazu auch den Kommentar auf Seite 28).

Bei Textverarbeitungsprogrammen muss man – sobald der Anteil an Bildern hoch und das Dokument sehr umfangreich ist – mit einem Verlust an Stabilität rechnen. So erreicht z. B. Microsoft Word beim Aufzählen der Funktionen zwar einen Spitzenplatz in einer Vergleichstabelle, wenn lediglich Funktionen ohne Praxistest gegenübergestellt werden. Bei der Erstellung und Pflege von größeren, strukturierten Dokumenten mit vielen Text-Bild-Kombinationen stößt man jedoch bald an Grenzen. Auch darf man bei Textverarbeitungsprogrammen keine hohen Ansprüche an Typografie und Grafik stellen oder einen professionellen Vierfarbdruck vorbereiten wollen (MS Word arbeitet mit RGB-Farben).

In den letzten Jahren sind immer mehr DTP-Funktionen in die Textverarbeitungsprogramme integriert worden und umgekehrt viele Textfunktionen in die DTP-Programme. Letztere bieten vor allem mehr Kontrolle über Positionierung und Formatierung (punktgenaues Positio-

nieren von Bildern und Texten möglich), sowie komfortable Kombination vieler verschiedener Files (Texte und Bilder) in einem Dokument. Weiters können DTP-Programme Farbseparieren (für den professionellen Vierfarbdruck), sie verwenden Musterseiten und sie bieten zusätzliche wichtige typografische Einstellmöglichkeiten.

Obwohl DTP-Programme Texteditorfunktionen haben, ist es empfehlenswert (und schneller), die Rohtexte in einem Editor zu erstellen. Bilder und Grafiken sollten in entsprechenden Grafikprogrammen vorbereitet werden. DTP-Programme können alle Text- (außer TeX) und Bild-Formate importieren. Sie werden dann in das Dokument eingebettet oder extern verlinkt. Dann wird das Layout gemacht, wobei volle Unterstützung für Modifikationen an Text und Bildern vorhanden ist. Die Aufteilung längerer Dokumente in Teildokumente (Kapitel) ist vorteilhaft bzw. die Verwendung der Buchfunktion. Man erhält ein elektronisches Gesamt-Dokument in einem proprietären Format, das Produkt steht also am Ende Produktionskette, das Originaldokument kann von keiner anderen Anwendung verarbeitet werden.

Eine gewisse Einarbeitungszeit in die Bedienung eines DTP-Programms ist erforderlich – dafür erhält man erweiterte Funktionalität und die Möglichkeit für professionelles Publishing. Die verschiedenen Tools haben jeweils ihre Vor- und Nachteile für verschiedene Anwendungen. Und alle Werkzeuge haben Bugs, mit denen man leben muss.

DTP-Programme aus der Campussoftware

Die Abteilung Standardsoftware des ZID stellt im Rahmen der Campussoftware auch DTP-Programm-Lizenzen zu günstigen Preisen den Institutsangehörigen der TU Wien zur Verfügung: Zur Auswahl stehen Adobe InDesign, Adobe FrameMaker, Adobe PageMaker und Corel Ventura, zum Teil für mehrere Plattformen und Sprachen.

Im Folgenden werden die DTP-Programme aus der Campussoftware kurz charakterisiert und auf ihre Eignung für das Erstellen strukturierter Dokumente untersucht.

Corel Ventura 10

Ventura war das erste DTP-Programm für den PC. Es beeindruckt durch seine Funktionsvielfalt. Strukturiertes Arbeiten wird u.a. durch vielfältige Formatvorlagen (Stile, für Seiten, Rahmen, Absätze, Zeichen und Linien) unterstützt. Ventura ist besonders konsequent in der Anwendung von Stilen.

Die Benutzeroberfläche ist ähnlich wie in Corel Draw, das User-Interface ist anpassbar (bis hin zu selbst definierten Icons und transparenten Pull-Down Menüs). Angenehm beim Arbeiten ist der kontext-sensitive (*modeless*) Cursor.

Ein so genannter Database Publisher dient zum Publizieren von Datenbank-Inhalten.

Ich verwende Ventura seit 1989 (Version 1) zur Erstellung von Zeitschriften, sowie überhaupt für alles, was gedruckt werden soll, von Visitenkarten, allen Arten von Berichten, bis zu großformatigen Plakaten. Es gibt eine kleine, feine User-Gemeinde. Rasche Hilfe ist in den Newsgroups zu bekommen.

Adobe InDesign 2

InDesign ist ein von Adobe neu entwickeltes DTP Programm mit hervorragenden Typografiefähigkeiten und viel Grafikpower. Optischer Randausgleich und eine über mehrere Zeilen vorausschauende Silbentrennung machen ein sehr gleichmäßiges Textbild. Jedoch unterstützt die momentane Version keine Fußzeilen, automatischen Nummerierungen oder Querverweise.

InDesign arbeitet in enger Integration mit anderen Adobe-Produkten, die Benutzeroberfläche wird Photoshop-Anwendern bekannt vorkommen.

Adobe FrameMaker 7

FrameMaker ist schon viele Jahre Standard für technische Dokumentationen, unterstützt SGML und läuft auch unter Unix. FrameMaker unterstützt alle Arten von Automatisierungen für umfangreiche Dokumente und ist stabil in der Performance.

Die Benutzeroberfläche ist jedoch etwas gewöhnungsbedürftig, um nicht zu sagen antiquiert.

DTP-Programme in der Campussoftware

Produkt	Version/Sprache	Plattform	Einstiegspreis Euro	Wartung/Quartal Euro
Adobe InDesign	2, dt., engl.	Windows 98/Me/NT/2000/XP, Mac OS	27.25	5.45
Adobe FrameMaker	7, dt., engl.	Windows 98/Me/NT/2000/XP, Mac OS, Mac OS X AIX, HP-UX, Solaris	22.67 54.40	4.51 10.90
Adobe PageMaker	7, dt., engl.	Windows 98/Me/NT/2000/XP, Mac OS	27.25	5.45
Corel Ventura	8, dt. 10, engl.	Windows 95/98/Me/NT/2000/XP Windows 2000/XP	20.-	4.-
MS Publisher	2002	Windows 9x/NT/2000/XP	18.17	3.63
Scientific WorkPlace	4.1, dt., engl.	Windows 95/98/Me/NT/2000/XP	109.01	10.90

Adobe PageMaker 7

PageMaker hat DTP sozusagen erfunden und das „Seiten-Machen“ durch Zusammenkleben von Text und Bildern auf dem Bildschirm ermöglicht. Für strukturierte Dokumente bietet das Programm jedoch weniger Unterstützung.

Microsoft Publisher

Mit Publisher lassen sich rasch Business-Dokumente oder Party-Einladungen erstellen. Die hier geforderte Unterstützung für umfangreiche technische Dokumentationen ist nicht gegeben.

Anforderungen an das DTP-Programm

Neben dem Import von Texten und Bildern aller möglichen Formate sollen folgende Funktionen für strukturierte Dokumente unterstützt werden:

- Erstellen eines Inhaltsverzeichnisses,
- automatische Nummerierungen (von Seiten, Kapiteln, Überschriften/Absätzen, Abbildungen, Fußnoten),
- Index-Erstellung,
- Fußnoten-Verwaltung (Endnoten/Literatur),
- Querverweise,
- Tabellensatz,
- Formelsatz,
- Scripting
  (Automatisierung diverser Layout-Prozesse möglich).

Die Tabelle zeigt die Funktionsvielfalt der besprochenen Programme. Der Funktionsumfang bezieht sich auf die jeweilige Campuslizenz. Einige Funktionen sind auch mit Plug-Ins zu bewerkstelligen, z. B. wird in der Campussoftware auch MathType angeboten. MathType ist ein interaktives Zusatzprogramm, mit dem mathematische Ausdrücke auch in Textverarbeitungs- und DTP-Dokumenten erzeugt werden können.

	Corel Ventura 10	InDesign 2	FrameMaker 7	PageMaker 7
Inhaltsverzeichnis	✓	✓	✓	✓
automat. Nummerierung Absätze	✓	✗	✓	✗
Index	✓	✓	✓	✓
Fußnoten/Endnoten	✓	✗	✓	✗
Querverweise	✓	✗	✓	✗
Tabellen	✓	✓	✓	✗
Formeln, Gleichungen	✓	✗	✓	✗
Scripting	✓	✓	✓	✓
XML	✓ (Import)	✓	✓	✗

Checkliste Funktionen für strukturierte Dokumente
Der Funktionsumfang bezieht sich auf die Campuslizenz.
Einiges ist mit Plug-Ins zu bewerkstelligen (z.B. MathType für Formeln)

Ich habe sehr gute Erfahrungen mit Ventura gemacht. Längere Texte lassen sich durch konsequentes Verwenden von Formatvorlagen (Stilen) sauber und schnell formatieren. In den Text eingebundene Bilder werden an der entsprechenden Stelle verankert und fließen so mit dem Text immer mit. Fixe Seitenelemente kommen auf die Musterseite. So formatiert sich das gesamte Dokument bei jeder Textänderung automatisch richtig neu, was besonders bei umfangreichen Dokumenten von Vorteil ist.

Auch die Montage von *camera-ready* PDF-Beiträgen zu einem Gesamtdokument (z.B. Tagungsband) ist leicht möglich. Die fertigen Einzelbeiträge werden seitenweise als EPS-Files (über Acrobat erzeugt) wie Bilder in das Ventura Dokument eingebunden. Dann lassen sich automatisierte Aktionen, wie z.B. Fußzeilen mit Seitennummern, Inhaltsverzeichnis und Index vornehmen.

Publishing von XML-Daten

XML (eXtensible Markup Language) ist eine Auszeichnungssprache, die erlaubt, Daten mit Markierungen (Tags) zu versehen und dadurch ihre logische Bedeutung zu definieren. XML Daten enthalten strukturierte Inhalte, auf die sich beliebige Formatierungen automatisch anwenden lassen.

Je mehr Applikationen XML unterstützen, desto leichter wird der Datenaustausch werden. XML hat sicher Zukunft auch im Publishing, vor allem in Hinblick auf die Verwendung derselben Daten für verschiedenen Medien (Stichwort *Cross Media Publishing*: Einsatz von XML-Daten als neutrale Datenquelle für alle Teilnehmer an einem Workflow).

Die neuen Versionen der DTP-Programme haben sich mit diesem Thema bereits auseinander gesetzt: InDesign 2 erlaubt Import, Bearbeitung und Export von XML-Daten. FrameMaker hat einen „*structured*“ Mode: eine vollständig strukturierte Umgebung, die für die Erstellung und Bearbeitung gültiger XML-Dokumente optimiert wurde.

Beispiel Cross Media Publishing

Corel Ventura erlaubt in der Version 10 den Import von XML-Files. Anhand eines Beispiels sei ein einfacher *Cross Media Workflow* demonstriert:

Das Mitteilungsblatt des ZID enthält eine Reihe von aktuellen Mitteilungen, die in bestimmten Zeiträumen gesammelt publiziert werden, sowohl in Papierform als auch im Web (www.zid.tuwien.ac.at/mitteilungsblatt/). Die Daten lassen sich leicht strukturieren: jede Mitteilung (Message) besteht aus Überschrift (Header), Datum, Autor und einem

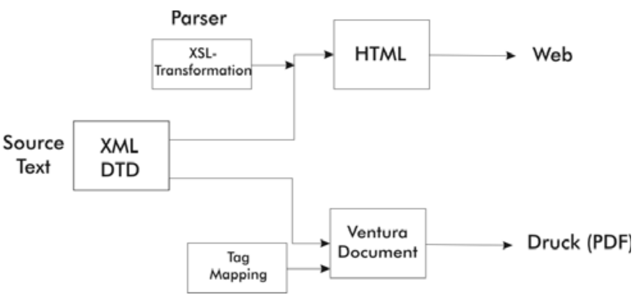
Text. Innerhalb des Message-Textes können noch weitere Strukturen, wie z. B. eine Tabelle auftreten.

Die Daten müssen nun entsprechend strukturiert und markiert vorliegen, also z. B.:

```
<Message>
  <Header>Titel der Mitteilung</Header>
  <Author>
    <Date>Datum</Date>
    <Name>Vorname Nachname</Name>
    <Email>E-Mail Adresse</Email>
  </Author>
  <Text>Text der Mitteilung ... </Text>
</Message>
```

Hat man die Struktur definiert, sind noch folgende Vorbereitungen zu machen:

- Eine DTD (Document Type Definition) zur Definition der XML-Elemente.
- Zuordnung der vorbereiteten Ventura Stile (Tags) zu den XML-Elementen im XML Mapping Editor (in Corel Ventura inkludiert).
- Definition eines Style Sheets in XSL (eXtensible Style Language) zur Formatierung im Web. Da noch nicht alle Browser das darstellen können, wird über einen Parser ein html-File erzeugt.



Cross Media Workflow mit XML-Daten und Corel Ventura

Beim Import des XML-Files in das Ventura Dokument werden nun alle Elemente entsprechend automatisch formatiert. Das XML-File ist nur verlinkt und in Ventura nicht editierbar. Will man noch nachbearbeiten, so kann man das File einbetten und noch Feinheiten am Layout vornehmen, die die automatische Formatierung nicht abdeckt.

Bei der Produktion eines neuen Mitteilungsblattes müssen nun nur die neuen Daten (Mitteilungen) in XML entsprechend vorliegen oder vorbereitet werden. Das Publishing für Web und Druck funktioniert dann wie „auf Knopfdruck“.

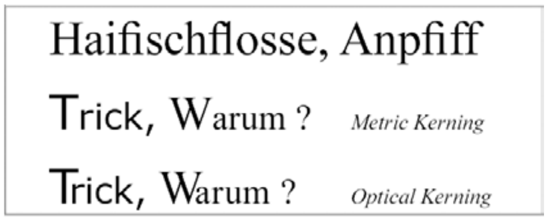
Die Schönheit der Typografie

Zum Schluss ein kleiner Exkurs in die Welt der Typografie. Ziel der Produktion wird ein optisch ansprechendes Dokument sein – der Text soll leicht lesbar sein und ohne hässliche Lücken fließen. Da spielt der Abstand zwischen den Zeichen und Wörtern eine Rolle.

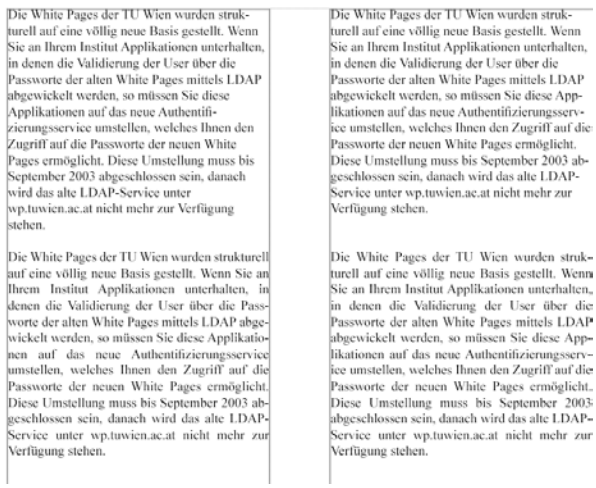
DTP Programme erlauben dem Benutzer eine Reihe von mikrotypografischen Einstellungen: so können z.B. (in Corel Ventura) sogar Punktgröße und Versatz von Hoch/Tiefstellungen und die Linieneinstellung der Unterstreichung verändert werden. Man kann da als Laie auch viel anstellen und die Optik verpatzen. Meist genügt es, die Voreinstellungen des Programms unverändert zu lassen.

Das angenehme Schriftbild von mit TeX gesetzten Texten ist bekannt. **InDesign** geht hier noch weiter und setzt neue Maßstäbe betreffend Typografie im DTP-Bereich:

- InDesign erzeugt automatisch Ligaturen (optische Verschmelzung von zwei aufeinander folgenden Buchstaben, z.B. bei fi, fl und ff) und unterschneidet auch zwischen verschiedenen Schriftgrößen (*Optical Kerning).*

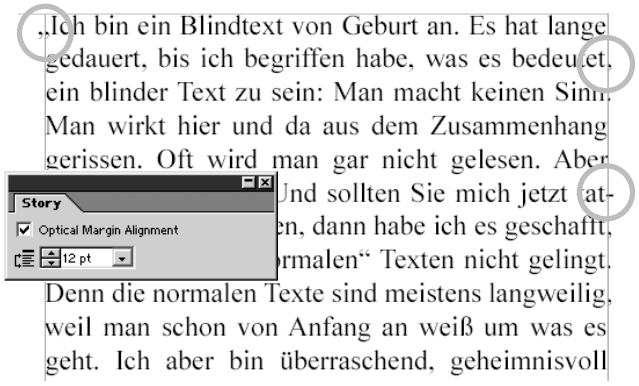


- Der Mehrzeilensetzer (*Paragraph Composer*) berücksichtigt alle Zeilen eines Absatzes beim Berechnen des Zeilenumbruchs. Dadurch entstehen weniger Lücken beim Blocksatz und der Flattersatz wird gleichmäßiger.



Links: Single Line Composer, Rechts: Paragraph Composer

- Beim „Optischen Randausgleich“ setzt InDesign Satzzeichen und Großbuchstaben ein wenig über die Spaltenbegrenzung hinaus. Dadurch erscheinen die Spaltenränder optisch ausgeglichener.



Zusammenfassung

Die große Produktpalette der Campussoftware enthält die meisten wichtigen, auf dem Markt befindlichen Desktop Publishing Programme, außer QuarkXpress. Lizenzen sind für Institutsangehörige der TU Wien zu günstigen Preisen erhältlich.

Wenn es darum geht, einen umfangreichen, gut strukturierten Text, eine technische Dokumentation, für den Druck vorzubereiten, ist der Einsatz eines DTP-Programms überlegenswert. Je nachdem, welche Funktionen man benötigt oder welche Benutzeroberfläche man gewohnt ist, kann man zwischen den Produkten wählen. Die Weiterentwicklung von Ventura, FrameMaker und PageMaker gerät von Firmenseite immer wieder ins Stocken, InDesign sind sicher die besten Zukunftsaussichten beschieden.

Wer sich mit dem Publishing von XML-Daten beschäftigt, findet bei den DTP-Programmen zunehmend Unterstützung.

Links:

Campussoftware der TU Wien:
sts.tuwien.ac.at/css/

Corel Ventura:
www.corel.com
FAQs und Tipps:
www.draw.nu/venturafaq/
www.klartext-verlag.de/ventura/
vpub.publish-net.de
Newsgroups:
corel.graphic_apps.ventura8
corel.graphic_apps.ventura10

Adobe Produkte:
www.adobe.com

MS Publisher 2002:
www.microsoft.com/office/publisher/default.asp

Personelle Veränderungen

Seit Anfang Februar ist Herr Ing. Thomas Mikulka (mikulka@zid.tuwien.ac.at, Nst. 42023) in der Abteilung Standardsoftware halbtags im Bereich Unterstützung Infrastruktur tätig. Herr Gerold Mosinzer hat Ende 2002 den ZID verlassen.

Das Team der Telefon-Vermittlung unterstützen seit November 2002 Frau Simone Klics (Nachfolge Frau Dangel) und Herr Hans Ehrhardt (Karenzvertretung für Frau Helmlinger) seit Mai 2003.

Wir wünschen allen neuen Mitarbeitern viel Erfolg und Freude bei ihrer Tätigkeit am ZID.

Wählleitungen

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

Datenformate:	300 - 56000 Bit/s (V.92) MNP5/V.42bis/V.44 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 (nur innerhalb der TU)
E-Mail: telekom@noc.tuwien.ac.at
Chipkarten, Abrechnung: 58801-42008
TU-ADSL
Hotline 58801-42007
E-Mail: adslhelp@zid.tuwien.ac.at

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

Service-Line Abt. Standardsoftware
Tel.: 58801-42004
E-Mail: sekretariat@sts.tuwien.ac.at

Systemunterstützung
Computer Help Line 42124
E-Mail: pss@zid.tuwien.ac.at
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

Zertifikate des Zentralen Informatikdienstes

Neu:
info.tuwien.ac.at, gültig bis 26. 3. 2006:
`MD5 Fingerprint=FB:70:BD:7B:90:45:7E:19:1D:0B:7D:F1:17:52:C5:49`
nic.tuwien.ac.at, gültig bis 26. 3. 2006:
`MD5 Fingerprint=55:71:4D:4C:A4:D1:98:D7:D7:AB:00:52:A1:71:AC:F4`

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

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: 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

Abteilung Zentrale Services

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
P. Deinlein	42074	deinlein@zid.tuwien.ac.at
P. Egler	42094	egler@zid.tuwien.ac.at
H. Eigenberger	42075	eigenberger@zid.tuwien.ac.at
C. Felber	42083	felber@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
M. Hofbauer	42085	hofbauer@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
D. Sonnleitner	42087	sonnleitner@zid.tuwien.ac.at
E. Srubar	42084	srubar@zid.tuwien.ac.at
Werner Weiss	42077	weisswer@zid.tuwien.ac.at

Abteilung Kommunikation

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
A. Datta	42042	datta@zid.tuwien.ac.at
H. Ehrhardt	42066	ehrhardt@zid.tuwien.ac.at
T. Eigner	42052	eigner@zid.tuwien.ac.at
S. Geringer	42065	geringer@zid.tuwien.ac.at
T. Gonschorowski	42056	gonschorowski@zid.tuwien.ac.at
J. Haider	42043	jhaider@zid.tuwien.ac.at
P. Hasler	42044	hasler@zid.tuwien.ac.at
H. Kainrath	42045	kainrath@zid.tuwien.ac.at
J. Klasek	42049	klasek@zid.tuwien.ac.at
S. Klics	42064	klics@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
M. Markowitsch	42062	markowitsch@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

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
I. Jaitner	42037	jaitner@zid.tuwien.ac.at
N. Kamenik	42034	kamenik@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
T. Mikulka	42023	mikulka@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
W. Steinmann	42036	steinmann@zid.tuwien.ac.at
P. Torzicky	42035	torzicky@zid.tuwien.ac.at