Technische Universität Chemnitz

Zertifikat Internet-Nutzung

– Lehrmaterial –

Chris Hübsch, Karsten Petersen, Marion Riedel, Ralph Sontag

Chris Hübsch, Karsten Petersen, Marion Riedel, Ralph Sontag:
Zertifikat Internet-Nutzung
– Lehrmaterial –
Petra Pönisch Verlag
2. überarbeitete Auflage 2003
ISBN 3-934848-12-5

Petra Pönisch Verlag
2. überarbeitete Auflage 2003

Vorwort zur 2. Auflage

Seit der ersten Auflage sind inzwischen drei Jahre vergangen. Manch einer hat in dieser Zeit gleich mehrere Generationen neuer Programme für seine Arbeit mit dem Internet erlebt. Einige Fachleute setzen ein Internet-Jahr sieben normalen Jahren gleich - es ist also Zeit für eine Überarbeitung.

Obwohl das World Wide Web bunter, die Anbindungen schneller, die Programme intuitiver und E-Mails selbstverständlicher geworden sind, hat sich an den Grundlagen wenig geändert. Die Probleme der Nutzer wandelten sich jedoch. Internetzugänge per Telefon oder ISDN funktionieren klagloser, nur selten noch muss man auf Fehlersuche gehen. Dafür verbreiten sich neue Angebote: Das Schlagwort DSL beherrscht die Anzeigen großer Anbieter, und mit den schnellen Anschlüssen tauchen entsprechende Angebote auf: Selbst Kinofilme finden sich inzwischen im Internet.

Dieses Lehrmaterial versucht, der Entwicklung Rechnung zu tragen. Grundlagenwissen wird weiterhin soweit vermittelt, wie es zur kompetenten Nutzung des Netzes und zur Diagnose einfacher Probleme notwendig ist. Details, um die sich Nutzer heute nicht mehr kümmern müssen, werden nicht mehr erwähnt. Dafür werden neue Begriffe und Entwicklungen berücksichtigt.

Die Grundlagen wurden um moderne Techniken wie DSL oder WaveLan ergänzt. Das separate Kapitel zu den Diskussionsforen des Usenets wurde aufgelöst und aufgeteilt. Während die Netikette nun im Kapitel „Elektronische Post“ behandelt wird, wurden die technischen Grundlagen mit den Konferenzsystemen zum neuen Kapitel „Kommunikation im Internet“ zusammengefasst. Als relativ neuer Netzdienst fanden Peer-to-Peer-Netzwerke Eingang in das entsprechende Kapitel.

Das ZIN-Material wird mittlerweile an mehreren Einrichtungen genutzt. Daher befinden sich Besonderheiten für Nutzer an der TU Chemnitz nun in einem eigenen Kapitel. Alle anderen Abschnitte sind allgemeingültig gehalten, wenn auch die Beispiele oft an Gegebenheiten der Chemnitzer Uni angelehnt sind. Insgesamt konnte der Umfang des Heftes etwa beibehalten werden.

Die TU Chemnitz mit ihrem Universitätsrechenzentrum sowie das Chemnitzer Studentennetz bieten eine hervorragende Umgebung, um auch neueste Entwicklungen im täglichen Einsatz studieren zu können. Das Fachwissen vieler Experten fließt in die tägliche Arbeit und damit auch dieses Material ein. Umgekehrt sind es natürlich auch Fragen der Leser, die uns per E-Mail, Usenet oder über den Nutzerservice des Rechenzentrums erreichen und Lücken oder Fehler offenbaren. Wir sind froh über diese Rückmeldungen und danken allen Helfern für die fruchtbare Unterstützung!

Dank gebührt auch den Korrekturlesern für Hinweise und Vorschläge. Verbleibende Fehler und Unstimmigkeiten sind allein die Schuld der Autoren.

Chemnitz, am 7. November 2002

Vorwort

Vor Ihnen liegt das Lehrmaterial zum „Zertifikat Internet-Nutzung“ (ZIN) der TU Chemnitz. Das ZIN soll helfen, den Netznutzern Grundkompetenzen bei der Nutzung der neuen Medien zu vermitteln. Die TU Chemnitz verfolgt eine sehr offene Politik: Jeder neu immatrikulierte Student erhält automatisch ein Nutzerkennzeichen, kann E-Mail versenden und empfangen und verfügt über ein HOME-Verzeichnis. Das wird einerseits von den Anwendern sehr begrüßt, andererseits erweitern sich auch die Möglichkeiten, durch Missverständnisse, Unwissen oder auch bewusst Schaden anzurichten.

Die Universitäten, aber noch stärker die Wirtschaft verlangen nach geschulten Anwendern, die die Netzdienste mindestens ebenso gut beherrschen wie die klassischen Medien. Einen Hochschulabsolventen, der vom Internet nichts weiter weiß, als dass es einen Mausklick entfernt ist, werden die Firmen binnen kurzem nicht mehr akzeptieren.

Das ZIN soll dazu beitragen, dass die Uni-Absolventen nicht nur Experten auf ihren Fachgebieten sind, sondern sich außerdem in der modernen Informationsgesellschaft souverän bewegen und neue Angebote selbstständig nutzen können.

Das Material wurde für ein selbstständiges Durcharbeiten entwickelt. Es setzt auf Abiturwissen auf und soll längerfristig nutzbare Informationen vermitteln. Es enthält daher keine Bedienungsanleitungen für gerade aktuelle Programme, die möglicherweise in einem halben Jahr bereits veralten und vielleicht nicht einmal unter allen gängigen Betriebssystemen verfügbar sind.

Die verwendeten Fachbegriffe werden beim erstmaligen Auftreten kurz erläutert. Die Stellen sind über das Stichwortverzeichnis schnell zu finden. Der Leser soll keine Definitionen auswendig lernen, wohl aber Vorstellungen von Zusammenhängen und Verständnis für das damit verbundene Vokabular entwickeln.

Die in das Material eingestreuten Fragen sollen das Verständnis des Stoffes vertiefen und Verbindungen zu anderen Gebieten herstellen.

Aktuelle Informationen im Zusammenhang mit dem ZIN stehen auf der WWW-Seite `http://www.tu-chemnitz.de/urz/ZIN` bereit.

In das Material flossen neben der Arbeit der Autoren auch viele weitere Anregungen ein. Besonderer Dank gilt Prof. U. Hübner und dem Chemnitzer Universitätsrechenzentrum für die umfangreiche Beratung und Unterstützung, sowie den aktiven Nutzern des Chemnitzer Studentennetzes (CSN) für viele hilfreiche Fragen und Hinweise.

Chemnitz, am 9. Dezember. 1999

Inhaltsverzeichnis

So, wie Sie in Ihrem bisherigen Leben gelernt haben, wie Briefe zugestellt oder Telefongespräche vermittelt werden, sollen Sie in diesem Kapitel verstehen, wieso Computer miteinander in Verbindung treten können.

1

Internet-Grundlagen

1.1. Vermittlungsverfahren in Netzen

Kanalvermittlung

Sie kennen seit langem das Telefonnetz: Wenn Sie einen Teilnehmer anrufen, wird eine durchgehende Verbindung (ein Kanal) zu Ihrem Kommunikationspartner hergestellt und Sie können diesen Kanal exklusiv nutzen. Weil nur ganze Kanäle vermittelt werden, spricht man von **Kanalvermittlung**.

In unserem Beispiel haben sowohl Hänsel und Gretel als auch Max und Moritz einen Kanal belegt. Ein Verbindungswunsch von Findus zu Pettersson muss nun abgelehnt werden, weil die Kanäle nicht mehr zur Verfügung stehen.

Bei der Kanalvermittlung haben Sie einen Kanal - wenn Sie ihn bekommen - ganz für sich allein. Sie müssen ihn aber dann auch bezahlen, selbst wenn Sie ihn gar nicht nutzen weil Sie z.B. nachdenken.

Wenn sich Computer miteinander unterhalten, ist das Datenaufkommen sehr unregelmäßig: Wenn Sie sich z.B. eine Webseite anschauen wollen, müssen beim Laden sehr viele Daten übermittelt werden. Sobald diese Webseite aber bei Ihnen angekommen ist und Sie sie lesen, werden gar keine Daten mehr übertragen. Ein Kanal wäre in diesem Fall also abwechselnd ganz oder gar nicht ausgelastet.

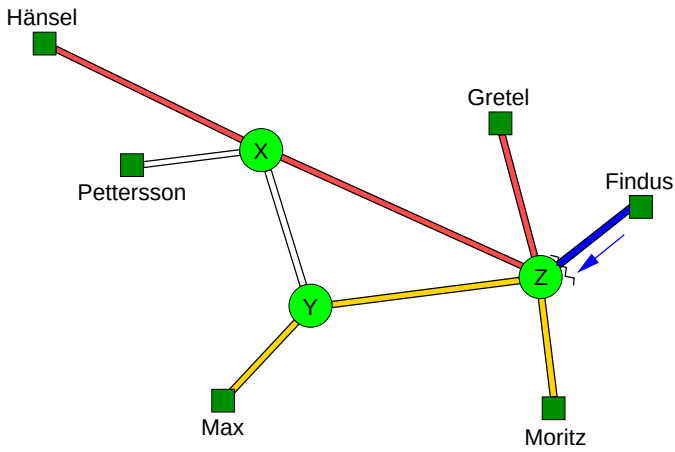


Abbildung 1.1-1.: Beispiel einer Kanalvermittlung

Nachrichtenvermittlung

Wenn nur gelegentlich Daten übertragen werden, brauchen die Rechner zum Kommunizieren gar keine durchgeschalteten Verbindungen. Es reicht völlig aus, wenn einzelne **Nachrichten** transportiert werden können. Damit lassen sich die Probleme der Kanalvermittlung beseitigen, doch taucht sofort ein neues auf: Wenn eine sehr große Nachricht transportiert werden muss, kann es leicht passieren, dass viele kürzere Nachrichten warten müssen. Deswegen ist es günstig, die Nachrichten in kleinere **Pakete** zu zerlegen und diese einzeln zu übertragen.

Paketvermittlung

Bei der **Paketvermittlung** wird jede Nachricht in Pakete zerlegt. Diese erhalten jeweils eine Absender- und Empfängerangabe und gehen einzeln auf die Reise. Die Pakete können unterschiedliche Größen haben, nur eine gewisse Maximalgröße dürfen sie nicht überschreiten.

Wir sehen, dass nun auch Findus seinen Kommunikationswunsch befriedigen kann. Wir sehen aber auch, dass die Leitung zwischen X und Z nicht mehr viele zusätzliche Pakete verkraften kann. Wollen noch mehr Teilnehmer über diese Leitung Daten austauschen, werden sie hin und wieder auf ein Paket etwas warten müssen. Es gibt also zwar keinen Besetztfall wie bei der Kanalvermittlung, die Nutzer müssen sich aber die gemeinsam genutzten Leitungen auch wirklich teilen. So kann ein Nutzer, der sehr viele Pakete überträgt, dadurch die anderen Nutzer behindern.

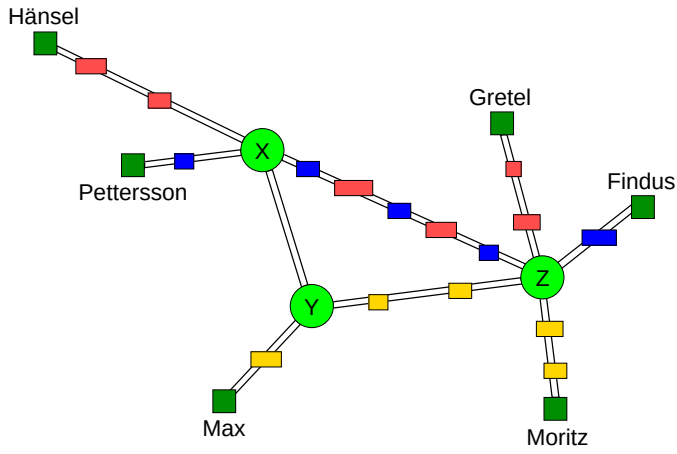


Abbildung 1.1-2.: Beispiel einer Paketvermittlung

Stellen wir uns nun vor, dass die Verbindung zwischen X und Z ausfällt, weil zum Beispiel ein Bagger das Kabel durchgerissen hat. Wenn die Vermittlungen wissen, dass es eine Umleitung über Y gibt, können sie die Pakete über diese alternative Route leiten. Sobald der Schaden beseitigt ist, wird wieder der alte Weg genutzt. Es ist leicht zu verstehen, dass sich dadurch auch Pakete gegenseitig überholen können. Pakete können auch verlorengehen, weil beispielsweise eine Vermittlungsstelle überlastet ist.

Was Sie hier sehen, ist ein Modell des **Internets**. Dort werden die Daten, die Computer miteinander austauschen wollen, in genau solche Pakete zerlegt und auf die Reise geschickt. Nun müssen die Rechner nur noch lernen, wie sie die Pakete ein- und auspacken können.

Wenn vom **Internet-Protokoll (IP)** die Rede ist, ist damit eine Vorschrift gemeint, die den Aufbau der Datenpakete im Internet beschreibt. Auch regelt diese Vorschrift die Art und Weise, wie die Vermittlungsstellen und Endgeräte - das kann z.B. Ihr PC sein - mit den Paketen umgehen müssen.

Das Internet-Protokoll sorgt aber nicht dafür, dass immer alle Pakete ankommen oder dass deren Reihenfolge stimmt. Darum kümmert sich das sogenannte **Transmission Control Protocol (TCP)**, welches die Übertragung der Daten steuert und kontrolliert. Erst beide Protokolle zusammen ermöglichen einen verlustfreien Datenaustauch, weswegen man auch oft von **TCP/IP**-Übertragung spricht.

*Vorschriften, die die Kommunikation mehrerer Teilnehmer regeln, bezeichnet man als **Protokoll**. Das Protokoll, welches die Eröffnung eines Telefongespräches beschreibt, könnte verkürzt so dargestellt werden:*

```
Max läßt es bei Moritz klingeln.
Moritz meldet sich mit "Hallo".
Max stellt sich vor.
...
```

Router und Gateways

Sie können im Bild 1.1-2 sehen, wie die Pakete durch verschiedene Vermittlungsstellen (X, Y, Z) laufen. Diese Vermittlungsstellen heißen **Router** oder auch **Gateways**. Sie kennen ihre Umgebung und entscheiden, welchen weiteren Weg ein Paket nehmen soll. Der Rechner am Ende des Netzes darf daher "dumm" sein, ihm genügt die Adresse des oder der nächsten Router, um alle Rechner im Netz erreichen zu können.

> *Beim Anschluss eines Rechners muss meistens ein **Default-Router** oder **Default-Gateway** angegeben werden, an den alle die Pakete geschickt werden sollen, die nicht direkt zugestellt werden können.*

1.2. Namen und IP-Adressen

IP-Adressen

So wie jeder Telefonanschluss eindeutig über Vorwahl und Nummer identifizierbar ist, besitzt auch jeder Computer im Internet eine eindeutige sogenannte **IP-Adresse**. Eine IP-Adresse besteht aus zwei Teilen, dem **Netz-Teil** und dem **Host-Teil**. Man kann sich den Netz-Teil wie eine Telefon-Vorwahl vorstellen, der Host-Teil ist dann die Telefon-Nummer.

Rechner, deren IP-Adressen sich im Netz-Teil nicht unterscheiden, befinden sich im selben **Subnetz**.

Würde nun ein Rechner auf eine IP-Adresse eingestellt, die im Netz-Teil nicht seinem Standort entspricht, so würden ihn auch keine Datenpakete erreichen. (Wenn Sie die Vorwahl für Hamburg wählen, können Sie schließlich auch nicht erwarten, einen Teilnehmer aus München ans Telefon zu bekommen.)

> *Wenn Sie selber einen Rechner an ein Netz anschließen, dürfen Sie sich nicht einfach eine IP-Adresse aussuchen! Je nach Netz werden IP-Adressen automatisch vergeben oder vom Netz-Verwalter zugewiesen.*

IP-Adressen werden der Einfachheit halber zur Zeit als vier durch Punkte getrennte Zahlen geschrieben, z.B. "134.109.193.89". Da die Menge der IP-Adressen jedoch beschränkt ist und schon knapp wird, forscht man seit einigen Jahren an neuen Netzwerktechnologien, die viel größere IP-Adressen benutzen können, z.B. "3ffe:ffff:100:f101:210:a4ff:fee3:9566". Aber keine Angst, das ist noch Zukunftsmusik und Sie brauchen sich IP-Adressen normalerweise auch nicht zu merken.

Namen

Angenehmer als die komplizierten IP-Adressen sind die heute gebräuchlichen Namen wie `dem.informatik.tu-chemnitz.de`. Wenn Sie so einen Namen in ein Programm eingeben, wird das Programm zuerst versuchen, die zu dem Namen gehörende IP-Adresse herauszufinden, und dann erst den gewünschten Rechner kontaktieren. Dazu fragt es einen sogenannten **Nameserver**. Der Nameserver kennt die Zuordnung von Namen und IP-Adressen oder er weiß zumindest, welchen Nameserver er seinerseits fragen kann.

Beim Anschluss eines eigenen Rechners müssen Sie deshalb eventuell angeben, welche Nameserver benutzt werden sollen. Inzwischen gibt es aber auch Netze, in denen neben der IP-Adresse auch die Adressen von Router und Nameserver automatisch an Ihren Rechner übermittelt werden.

Diese Zuordnung von Namen zu IP-Adresse und umgekehrt funktioniert weltweit. Die Einrichtung, die dies ermöglicht, heißt **Domain Name System (DNS)**.

Es kann auch mehrere Namen für einen Rechner geben. Diese werden dann **Alias** genannt.

Frage 1.2.1:

Können Sie sich denken, warum es sinnvoll ist, den Namen `www.tu-chemnitz.de` als Alias für einen bestimmten Rechner zu vergeben?

Bei den Namen steht ganz rechts die **Toplevel-Domain**, das kann ein Länderkennzeichen oder ein allgemeines Kennzeichen sein. Das ist also anders als bei IP-Adressen, wo der Netz-Teil links steht. Als nächstes (von rechts) folgt die **Domain**. Diese und die evtl. folgenden **Sub-Domains** bestimmen genauer, wozu der Rechner gehört. Ganz links steht dann der **Hostname**.

Kennzeichen	Bedeutung
.com	Firmen (englisch: commercial)
.org	Organisationen
.gov	Regierungseinrichtungen (englisch: governmental)
.edu	Lehreinrichtungen (englisch: educational)
.info	nicht näher spezifizierte Informationen
.aero	Internationale Unternehmen der Luftfahrt-Branche

Tabelle 1.2-1.: Toplevel-Domains: allgemeine Kennzeichen

Dies ist nur eine Auswahl der häufiger vorkommenden allgemeinen Toplevel-Domains. Von Zeit zu Zeit kommen auch weitere hinzu, so dass diese Tabelle niemals vollständig sein kann.

Kennzeichen	Land
.de	Deutschland
.uk	Großbritannien
.nl	Niederlande
.at	Österreich
.jp	Japan
.us	USA (die meisten US-amerikanischen Angebote liegen aus historischen Gründen aber unter den allgemeinen Toplevel-Domains)
.to	Tonga (Inselgruppe im Süd-Pazifik)
.tv	Tuvalu (Inselgruppe im Süd-Pazifik)

Tabelle 1.2-2.: Toplevel-Domains: Länderkennzeichen

```
Beispiel: tan.informatik.tu-chemnitz.de
```

Die Toplevel-Domain ist also `.de` für Deutschland. Als Domain folgt `.tu-chemnitz` für die Uni Chemnitz, die Sub-Domain darin heißt `.informatik` für die Fakultät gleichen Namens. Der Hostname schließlich lautet `tan`.

Sie sollten allerdings nicht versuchen, aus dem Namen auf den Standort eines Rechners zu schließen, denn die Abbildung von Namen auf IP-Adressen erlaubt, die Namen praktisch beliebig zu vergeben.

> *Genau wie bei der IP-Adresse dürfen Sie sich einen Namen für Ihren Rechner nicht einfach aussuchen. Stattdessen wird Ihnen ein Rechnername vom Netz-Verwalter zugewiesen - allerdings dürfen Sie meistens zumindest Vorschläge machen.*

1.3. Bandbreite und Geschwindigkeit

Geschwindigkeit

Als Geschwindigkeit empfindet man üblicherweise die Schnelligkeit des kompletten Vorgangs von der Anforderung bis zur Anzeige des Ergebnisses. Das hängt aber nicht nur von der Geschwindigkeit des Netzes ab, auch die Belastung und Schnelligkeit des Rechners, von dem man Daten anfordert, und die Geschwindigkeit des eigenen Rechners, der die ankommenden Daten erst verarbeiten und anzeigen muss sind wichtig. Auch könnten Datenpakete unterwegs verlorengegangen sein, so dass sie erst neu gesendet werden müssen. All dies kostet Zeit, was den subjektiven Eindruck von der Geschwindigkeit des Netzes senkt.

Durchsatz und Bandbreite

Mit **Durchsatz** wird die Menge an Daten bezeichnet, die wirklich über eine Leitung fließen. Im Gegensatz dazu sagt die **Bandbreite** aus, wieviele Daten in einer bestimmten Zeit durch einen Datenkanal gelangen könnten. Sie können sich die Bandbreite wie die Breite eines Schifffahrtskanals vorstellen: je breiter er ist, desto mehr Schiffe können in einer bestimmten Zeitspanne hindurchfahren. Der Durchsatz ist dann die Anzahl auch wirklich hindurchfahrender Schiffe.

Theoretisch kann der Durchsatz also so groß wie die Bandbreite sein, in der Realität liegt er aber immer mehr oder weniger weit darunter. Das hat verschiedene Gründe: Mitunter entsprechen die Endgeräte nicht den Möglichkeiten der Leitung; ein sehr altes Modem überträgt eben auch über eine gute Telefonleitung nur langsam Daten. Und wenn sich mehrere Nutzer eine Leitung teilen, erleben Sie einen noch geringeren Durchsatz, denn sie teilen sich die Leitung mit den anderen. Je mehr Nutzer aktiv sind, desto geringer erscheint ihnen der Durchsatz der Leitung.

Daten und ihre Größe

Die kleinste Einheit in einem Computer ist das **Bit**, dieses kann genau zwei Zustände speichern: 1 wie "wahr" und 0 wie "falsch". Acht dieser Bits zusammen bilden ein **Byte**, dieses kann sich damit schon 2^8, also 256 Zustände merken. (Man rechnet meistens in Byte und nicht in Bit.) Kommen viele Einheiten zusammen, so kürzt man mit **Kilo (K)** bzw. **Mega (M)** ab. Leider wird die Bedeutung dieser Präfixe nicht einheitlich gehandhabt. Bei der Datenübertragung versteht man darunter 1000 bzw. 1 Million. Bei der Angabe von Hauptspeicherkapazitäten wird dagegen mit den Zweierpotenzen (2^{10}=1024 für Kilo bzw. 2^{20}=1.048.576 für Mega) operiert.

> Beispiel: 10 KByte Speicher sind 10 Kilo-Byte also 10 $*$1024 Byte. In einem Netzwerk entsprechen 10 KByte Bandbreite aber nur 10 $*$1000 Byte.

Buchstaben, Zahlen und andere einfache Zeichen werden normalerweise in einem Byte gespeichert. Eine vollgeschriebene Schreibmaschinenseite enthält ungefähr 4000 Zeichen (auch Leerzeichen und Zeilenumbrüche zählen mit!) und braucht daher auch 4000 Byte (oder gerundet 3,9 KByte) Speicherplatz.

Bei **Bildern** hingegen benötigt jeder Bildpunkt abhängig von der Anzahl von Farben ein oder mehr Byte, und zwar bei Bildern mit 256 Farben ein Byte und bei Bildern mit Echtfarben (16 Millionen Farbtöne) drei Byte.

> Ein 300 mal 200 Bildpunkte großes Bild mit 256 Farben benötigt beispielsweise 300 $*$200 $*$1 Byte = 60000 Byte, also etwa 58,6 KByte Speicher.

Praktisch werden Bilddaten jedoch durch spezielle Methoden meist stark komprimiert.

Ein schon etwas älteres Modem hat eine Bandbreite von 33,6 KBit/s (Kilo-Bit pro Sekunde). Wenn wir jetzt wissen wollen, wie lange eine Datenübertragung dauert, müssen wir zuerst die Einheiten angleichen. Dazu teilen wir die 33,6 KBit/s durch acht (acht Bit sind ein Byte) und erhalten 4,2 KByte/s. Nehmen wir jetzt an, wir würden 100.000 Byte - 100 KByte - übertragen wollen, das würde dann 100 / 4,2 also etwa 23,8 Sekunden dauern.

Frage 1.3.1:

Wie lange dauert es, ein 1024 mal 768 Bildpunkte großes Bild in Echtfarben (3 Byte pro Bildpunkt)

1. mit einem schnellen Modem per Telefonleitung (56 KBit/s)
2. über ein lokales Netzwerk wie das Chemnitzer Studenten-Netz (10 MBit/s)

zu übertragen? Nehmen wir vereinfachend an, dass das Bild nicht in einem komprimierten Format gespeichert wurde, sondern "jeder Bildpunkt einzeln".
(Lösung: 5:37 Min bzw. etwa 1,9 Sekunden.)

1.4. Übertragungstechniken

Manchmal werden Sie gezwungen sein, die physische Verbindung eines Rechners mit dem Netz selbst herzustellen. Deswegen ist es nützlich, die wichtigsten Methoden zu kennen.

Egal wie übertragen wird, die Daten müssen erst einmal aus dem Computer "herauskommen". Außer der Möglichkeit, den Rechner durch interne Steckkarten zu erweitern, gibt es auch sogenannte **Schnittstellen**, über die er mit anderen Geräten verbunden werden kann. Bekannte Beispiele sind der **Universal Serial Bus (USB)** oder die **serielle Schnittstelle**. Meist werden Kabel verwendet, seit einigen Jahren verbreitet sich aber auch drahtlose Technik wie **Bluetooth**.

Modems

Es gibt externe und interne **Modems**.

- *Externe Modems sind kleine Kästen, die neben oder auf den Rechner gestellt werden. Sie werden durch ein Kabel mit dem Rechner verbunden und durch ein zweites Kabel mit der analogen Telefondose. Dank kleiner Lämpchen (Leuchtdioden) kann man ihre Aktivitäten gut verfolgen.*

- *Interne Modems sind Steckkarten, die in einen Steckplatz im Inneren des PCs gesteckt werden. Über ein Kabel werden sie direkt mit der Telefondose verbunden.*

Modems wandeln das digitale Signal des Rechners - die Folge der Bits - in eine Folge von Schwingungen ("Töne") um, die in dem Frequenzbereich liegen, welcher vom Telefonnetz übertragen werden kann. Auf der anderen Seite wird dieses analoge Signal analysiert und in die ursprüngliche Bitfolge zurückverwandelt. Mit dieser Technik sind Datenraten bis zu etwa 33,6 KBit/s möglich. Durch einen Trick können heutzutage auch 56 KBit/s erreicht werden, doch wird dabei eigentlich schon kein analoges Übermittlungsverfahren mehr verwendet.

ISDN

In den sechziger Jahren begann die Digitalisierung des Telefonnetzes, in den siebziger und achtziger Jahren folgte die Vermittlungstechnik. Nur noch auf der Strecke vom Endkunden zur Vermittlungsstelle fand eine analoge Datenübertragung statt. Es lag daher nahe, auch Endkunden digital anzuschließen und damit die gesamte Übertragung digital abzuwickeln. So entstanden **Integrated Services Digital Network (ISDN)**-Anschlüsse, welche die Vorteile digitaler Übertragungen beim Kunden verfügbar machten. Die Umwandlung der analogen Sprachsignale geschieht nun direkt im Telefon.

Der PC kann mit ISDN direkt digitale Signale senden, ein ISDN-Kanal kann 64 kbit/s transportieren. Neben der höheren Datenrate, die durch gleichzeitige Nutzung mehrerer Kanäle ("Bündelung") noch weiter gesteigert werden kann, erhöht sich auch die Geschwindigkeit des Verbindungsaufbaus.

Um einen PC via ISDN anzuschließen, wird ein **ISDN-Adapter** benötigt. Das sind traditionell Steckkarten für den Rechner, inzwischen verbreiten sich aber auch kleine Kästchen, die per USB angeschlossen werden.

> *Der Datenstrom auf einem ISDN-Kanal hat nichts mit einer digitalisierten Schwingung zu tun. Daher kann ein Modem nicht ohne Weiteres mit einer ISDN-Karte kommunizieren.*

DSL

Eine in Deutschland noch recht junge Technik ist **Digital Subscriber Line (DSL)**. Obwohl auch DSL über das Telefonkabel Daten überträgt, ist es doch viel schneller als Modem und ISDN.

Der große Unterschied bei DSL zu den anderen beiden Techniken ist, dass nicht mehr eine Verbindung zu einer vielleicht weit entfernten Gegenstelle bewusst aufgebaut wird. Stattdessen besteht - völlig unabhängig von der normalen Nutzung als Telefonanschluss - praktisch dauerhaft eine zusätzliche Datenverbindung zur nächsten Telefon-Vermittlungsstelle. Aufgrund der kurzen Strecke ist eine höhere Geschwindigkeit möglich.

Allerdings erfordert DSL aus technischen Gründen **Kupferkabel**, wie sie traditionell als Telefonanschluss verlegt werden. In einigen deutschen Städten (vor allem in ostdeutschen Großstädten und im Raum Hannover) wurden jedoch in den letzten Jahren **Glasfaserkabel** bis zu den Kunden verlegt und diese eigentlich modernere Technik erlaubt keinen Betrieb von DSL.

> *Einige Anbieter bewerben "DSL über Satellit" oder "DSL über Glasfaserkabel". Das ist dann nicht wirklich DSL, sondern eine andere Technologie zum Übertragen von Daten. Man wirbt aber immer mit dem Begriff DSL, weil sich das allgemein als Bezeichnung für eine schnelle Internet-Anbindung eingebürgert hat.*

Um einen PC via DSL anzuschließen, wird ein **DSL-Modem** benötigt. Diese auch **DSL-Router** genannten Geräte besitzen dann meist einen Ethernet-Netzwerkanschluss. Beachten Sie dazu bitte den folgenden Abschnitt über lokale Netze.

Allen drei Technologien - analoges Modem, ISDN und DSL - gemein ist die Verwendung des **Point-to-Point-Protokoll (PPP)**. Es hat den Vorteil, dass einige Angaben, die beim Anschluss eines Rechners normalerweise konfiguriert werden müssen (zum Beispiel die Adressen der Nameserver), automatisch übertragen werden können. Daher gestaltet sich der Verbindungsaufbau über die Telefonleitung heutzutage recht einfach.

Lokale Netze

Viele Computer sind in **lokale Netze** eingebunden, von denen es viele Varianten gibt. Man kann die Netze nach der **Netztopologie** unterscheiden (Stern, Ring oder Strang), nach den verwendeten "Leitungen" (**Koaxialkabel**, **Twisted-Pair-Kabel**, **Glasfaserkabel**, Funkwellen, ...) oder nach den Protokollen (ATM, Ethernet, Token Ring, ...).

Derzeit kommt an Arbeitsstationen fast ausschließlich **Ethernet**-Technik zum Einsatz. Die Rechner enthalten dabei einen **Netzadapter**; das ist eine Steckkarte, die eine Buchse für den Anschluss des Ethernet-Kabels zur Verfügung stellt. Bei einem traditionellen Ethernet hängen alle Rechner an einem gemeinsamen Kabel, dem Bus. Irgendwo an diesem Bus befindet sich ein Gerät, das über mehr als eine Schnittstelle verfügt und die Daten in das nächste Segment (das muss nicht zwingend wieder ein Ethernet sein) routen kann - der Router bzw. das Gateway.

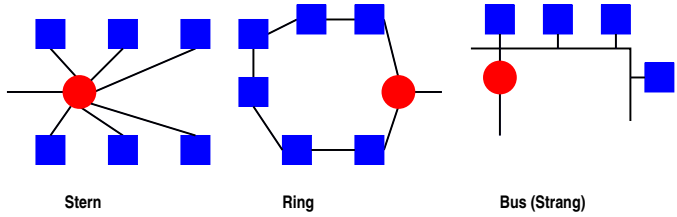


Abbildung 1.4-1.: Es gibt verschiedene Techniken, Rechner in einem lokalen Netz zu verbinden. Das runde Gerät ist jeweils der Router, also die "Vermittlungsstelle" in andere Netze.

Ethernet Netzadapter und Router besitzen dabei immer eine einmalige "Seriennummer", die sogenannte **MAC-Adresse**. Sie wird bereits vom Hersteller der Karte festgelegt und ist für die korrekte Zustellung von Paketen im Ethernet wichtig. Um Probleme zu vermeiden sollten Sie daher niemals die MAC-Adresse verändern, auch wenn Ihnen ein Programm vielleicht die Möglichkeit dazu gibt!

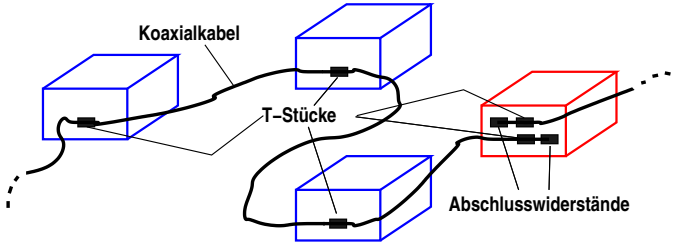


Abbildung 1.4-2.: Mehrere PCs teilen sich ein Koaxialkabel-Segment.

In älteren Netzen finden Sie an den Rechnern **T-Stücke**, von denen jeweils ein Kabel zum vorhergehenden und eines zum nächsten Gerät am Bus führt.

> *Man kann sich das so vorstellen, als ob die Netzadapter durch die T-Stücke auf die vorbeiströmenden Datenpakete schauen und sich die richtigen herausfischen. Ist das Segment offen, weil ein Abschlusswiderstand fehlt oder ein Kabel an einem T-Stück gelöst wurde, funktioniert das gesamte Segment des Netzwerkes nicht mehr. Bitte trennen Sie daher immer nur das T-Stück von Ihrem Rechner, denn sobald sie die Kabel vom T-Stück abziehen, können andere Nutzer das Netzwerk nicht mehr benutzen!*

Abbildung 1.4-3.: Das Bild zeigt ein T-Stück an einem Koaxialkabel mit einem Abschlusswiderstand.

In neueren Netzen wird jeder Rechner mit einem eigenen Kabel angeschlossen. Diese werden dann von einem Verteiler zusammengefasst, der am oben bereits erwähnten Router angeschlossen ist. Erst bei dieser Technik kann ein einzelner Nutzer nicht mehr durch das Abziehen eines Kabels einen ganzen Strang lahmlegen.

Abbildung 1.4-4.: Zwei Kabel an einer Dose.

Solche Netzwerk-Kabel sehen ganz ähnlich aus wie ISDN-Kabel, sie haben sogar die gleichen Stecker. Verwechseln Sie Kabel und Adapterkarten aber bitte nicht, dies könnte Ihren Rechner beschädigen!

Drahtlose Netze

Immer weitere Verbreitung finden auch drahtlose Technologien wie z.B. **IEEE 802.11b** - umgangssprachlich **Wireless LAN** oder auch **WaveLAN** genannt. Hier werden die Daten zwischen einer Basisstation und dem mobilen Klienten per Funk übertragen. (Die Basisstation selbst ist normalerweise mit einer kabelgebundenen Technik angeschlossen.)

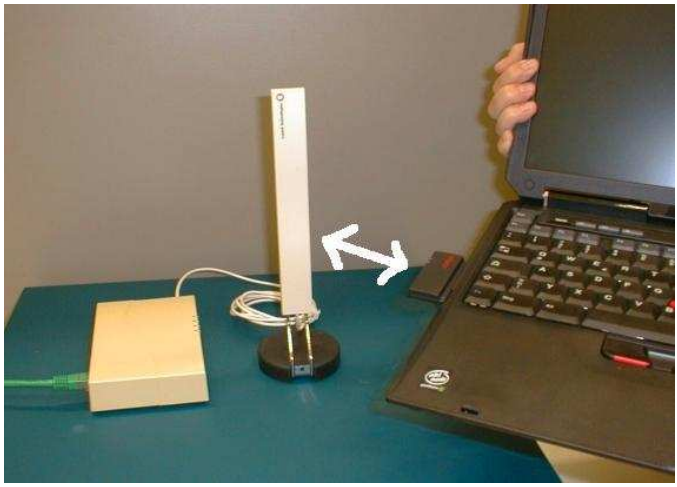


Abbildung 1.4-5.: Wireless LAN: Links ist die Basisstation mit extra Antenne, rechts der Klient.

Vertiefung:
Wenn Sie Ihren Rechner via Modem oder ISDN mit dem Internet verbinden wollen, müssen Sie eine Reihe von Angaben kennen. Die großen Provider verteilen gern CDs, auf denen bereits das meiste vorkonfiguriert ist. Bei kleineren Anbietern müssen Sie die (wenigen) Angaben selbst eintragen. Die Nutzer der TU Chemnitz finden hier die wichtigsten Hinweise zum

> Campusnetzzugang über das öffentliche Telefonnetz.
> [http://www.tu-chemnitz.de/urz/netz/tk.html]

So lange alles klappt, ist das Versenden und Empfangen von E-Mails kinderleicht. Doch manchmal geht etwas schief. Mit ein wenig Hintergrundwissen kann man einen Großteil der Fehler selbst finden und beheben.

2 Elektronische Post

2.1. Aufbau von E-Mails

Heutzutage ist das Versenden von **E-Mails** (oder kurz: **Mails**) nahezu ebenso selbstverständlich wie das Verschicken von Briefen. Genauso, wie es bestimmte Regeln einzuhalten gilt, wenn ein Brief seinen Empfänger erreichen soll (Maße, Gewicht, Adressangabe, Briefmarke ...), müssen auch im elektronischen Postnetz bestimmte Anforderungen erfüllt werden.

Analog zur Briefpost besteht eine E-Mail aus

- Umschlag (*Envelope*)
- Briefkopf (*Header*)
- Inhalt (*Body*)

Schauen wir uns ein (älteres und darum einfacheres) Beispiel an:

Envelope

```
From richter@saturn.hrz.tu-chemnitz.de Wed Oct 30 08:45 MEZ 1991
Received: from saturn.hrz.tu-chemnitz.de
           by obelix.hrz.tu-chemnitz.de with SMTP id AA15137
  (5.65+/IDA-1.3.5 for sontag); Wed, 30 Oct 91 08:45:37 +0100
Return-Path: <richter@saturn.hrz.tu-chemnitz.de>
Received: by saturn.hrz.tu-chemnitz.de id AA07615
  (5.65+/IDA-1.3.5 for sontag@obelix.hrz.tu-chemnitz.de);
  Wed, 30 Oct 91 08:45:35 +0100
```

Header

```
Date: Wed, 30 Oct 91 08:45:35 +0100
From: Frank Richter <frank.richter@hrz.tu-chemnitz.de>
Message-Id: <9110300745.AA07615@saturn.hrz.tu-chemnitz.de>
Subject: Ihr X.500 Directory Eintrag
To: sontag@hrz.tu-chemnitz.de
Status: RO
```

Body

```
Ihre auf dem Einwilligungsformular angegebenen Daten wurden
in das X.500 Directory uebernommen (siehe unten).
Damit zaehlen Sie zu den ersten Nutzern dieses im Aufbau
befindlichen, weltweiten "Telefonbuch-Services". Bitte achten
Sie auf die staendige Aktualitaet ihrer Daten, berichtigen
diese selbst oder teilen Aenderungen dem Directory-
Verantwortlichen mit.
...
```

Die drei Elemente sind für verschiedene Beteiligte bestimmt:

Umschlag (Envelope)

Den **Umschlag (*Envelope*)** benötigt das Mail-System - genauer gesagt der **Mail Transport Agent (MTA)** - für die Zustellung der Mail. Er enthält die Adresse(n) des (der) Empfänger(s), aber auch Hinweise auf die durchlaufenen Zwischenstationen, ähnlich, wie früher Eilbriefe einen Stempel von allen Sortierstellen bekamen.

Abbildung 2.1-1.: Ein klassischer Mail Transport Agent :-)

Genau wie im richtigen Leben mitunter der Umschlag weggeworfen wird, bevor ein Brief auf dem richtigen Schreibtisch liegt, werfen auch die meisten Programme den Envelope weg, wenn sie die Mail an den richtigen Nutzer zugestellt haben.

Auf den Umschlag haben die Nutzer des Mail-Systems kaum einen Einfluss, es genügt, von seiner Existenz zu wissen.

Kopf (Header)

Vom **Kopf (*Header*)** einer E-Mail zeigen die meisten Programme einen Auszug an. Wenn Sie alles sehen wollen, müssen Sie nach einem entsprechenden Knopf oder Schalter bei Ihrem Mail-Programm suchen oder die Mail in eine Datei abspeichern und sich diese mit einem gewöhnlichen Texteditor ansehen.

Kopfzeilen (Headerzeilen) bestehen prinzipiell aus einem Schlüsselwort, gefolgt von einem Doppelpunkt und einem Wert. Es gibt sehr viele mögliche Schlüsselwörter, sowohl international standardisierte als auch spezielle, nur von bestimmten Programmen generierte.

Die wichtigsten Schlüsselwörter sind:

`From:`	Adresse des Absenders
`To:`	Primärempfänger der Nachricht
`Cc:`	Empfänger einer Kopie
`Bcc:`	"Blinde" Empfänger einer Kopie - sie sehen nicht, wer die Mail noch erhielt
`Date:`	Datum und Zeit des Absendens der Nachricht
`Subject:`	Betreff der Nachricht
`Message-Id:`	eindeutiger Identifikator (automatisch vergeben)
`Reply-To:`	Adresse der Person, der zu antworten ist

Die `From`-Zeile setzt Ihr Programm automatisch ein, wenn es korrekt konfiguriert wurde. Um `Date` und `Message-Id` müssen Sie sich ebenfalls nicht weiter kümmern.

Die `To`-Zeile enthält den oder die Empfänger der Mail. Hier können also auch mehrere Adressaten, durch Komma getrennt, stehen. In der `CC`-Zeile werden Empfänger von Kopien (*Carboncopy*) angegeben. Diese erhalten die Mail zur Information, man erwartet keine Reaktion von ihnen. Mittels der `Bcc`-Zeile kann man verhindern, daß die Empfänger den gesamten Verteiler sehen.

Die `Subject`-Zeile muss zwar nicht unbedingt angegeben werden, es empfiehlt sich aber trotzdem, einen aussagekräftigen Betreff zu wählen. Spätestens, wenn sich Ihr Postkorb (Mail-Folder) mit einigen Dutzend Mails gefüllt hat, werden Sie es zu schätzen wissen, wenn Ihre Partner ein wenig Zeit in eine geschickte Wahl des Subjects investiert haben.

Inhalt (Body)

Ursprünglich konnte man in E-Mails nur einfache ASCII-Texte verschicken. **ASCII** heißt ein alter amerikanischer Computer-**Zeichensatz**, der nicht einmal Umlaute und andere Sonderzeichen zulässt. Das war natürlich sehr unbefriedigend. Nutzer aus europäischen oder asiatischen Ländern wollen die in ihrer Sprache üblichen Umlaute und Sonderzeichen verwenden. Auch Bilddateien oder Dokumente von Textverarbeitungsprogrammen bestehen aus einer Folge von Bytes, die bei weitem nicht nur ASCII-Zeichen enthält.

Um derartige Daten zu versenden, müssen sie "verpackt" werden. Ein Nicht-ASCII-Zeichen muss durch ASCII-Zeichen ausgedrückt werden. Bei Verwendung eines fremden Zeichensatzes muss dieser angegeben werden.

Der Standard **Multipurpose Internet Mail Extension (MIME)** ermöglicht es, auch andere Zeichensätze zu verwenden oder die Mails mit sogenannten Anlagen oder Anhängen (**Attachments**) zu versehen. Damit wurde der Versand von Bildern und anderen Dokumenten stark vereinfacht. Die meisten Mailprogramme gestatten es, einfach an-

zugeben, welche Dateien mit einer Mail versandt werden sollen. Office-Pakete selbst können Dokumente per Mail versenden und packen sie dazu MIME-gemäß ein.

Allerdings ist damit nicht gesichert, dass der Empfänger auf der anderen Seite mit den erhaltenen Dateien auch etwas anfangen kann. Bilddateien benötigen einen Bildbetrachter, Dokumente aus Textverarbeitungen müssen mit einem entsprechenden Office-Programm angezeigt werden. Das Mail-System sorgt dafür, dass Ihre Daten unbeschädigt transportiert werden. Ob der Empfänger etwas damit anfangen kann, weiß es nicht.

Der Aufbau von MIME-Mails bleibt im Prinzip so, wie oben dargestellt. Jedoch werden, sobald Sie Attachments versenden wollen oder einen vom Transportsystem nicht akzeptierten Zeichensatz verwenden, weitere Header-Zeilen eingefügt und der eigentliche Inhalt der Mail kodiert. Das sieht dann beispielsweise so aus:

```
MIME-Version: 1.0
Content-Type: TEXT/PLAIN; charset=ISO-8859-15
Content-Transfer-Encoding: QUOTED-PRINTABLE
```

Eine Zeile gibt die Version des Protokolls an. Weitere Zeilen spezifizieren den Inhalt. Hier wurde als Basistyp `TEXT` spezifiziert, es können aber auch `IMAGE` für Bilddaten, `APPLICATION` für bestimmte Anwendungen wie z.B. PDF-Dateien, `MULTIPART` für eine mehrteilige Nachricht oder weitere Schlüsselwörter stehen. Anschließend wird der Subtyp festgelegt, hier also `PLAIN`.

Für den Text wird ein Zeichensatz angegeben. Schließlich versenden Sie nur einfache Bytes, und das Mail-Programm Ihres Empfängers muss entscheiden, ob es z.B. das Zeichen Nr. 233 aus dem bei uns üblichen Zeichensatz **ISO-8859-15** wählen soll und ein "é" darstellt, oder ob ein in kyrillischer Schrift lesender Partner aus dem ISO-8859-5-Zeichensatz ein ъ lesen soll.

Schließlich wird noch festgelegt, welche Art der **Kodierung** verwendet werden soll. Die Quoted-Printable-Kodierung kümmert sich nur um 8-Bit-Zeichen (z.B. Umlaute) und das "=", alles andere lässt sie unangetastet. So wird aus den Worten "Viele Grüße" die Zeichenfolge "Viele Gr=FC=DFe", wobei "FC" und "DF" die hexadezimalen Zeichencodes für die Zeichen ü und ß sind. Dieses Verfahren hat den Vorteil, dass der Text mit etwas gutem Willen auch dann noch lesbar bleibt, wenn das Mail-Programm die Dekodierung verweigert.

Auch innerhalb der Mail können weitere MIME-Zeilen auftauchen. Das passiert, wenn die Mail aus mehreren Teilen mit unterschiedlicher Kodierung oder unterschiedlichem Typ zusammengesetzt wurde.

Im Übrigen wird auf diese Weise nur der Inhalt der Mail kodiert. Für Betreff und andere Headerzeilen sind andere Verfahren nötig, denn ein Mailprogramm muß diese sofort lesen können.

> *Die Umlaute-Situation wird in der nächsten Zeit noch etwas verwickelter. Kurioserweise liegt das in dem Wunsch begründet, das Umlaute-Problem zu vereinfachen: Der neue Zeichensatz **Unicode** soll alle Umlaute und viele weitere Symbole enthalten, also weit mehr als 256 Zei-*

chen. Dann genügt ein Zeichensatz, unabhängig ob man deutsche, französische, tschechische oder gar chinesische Zeichen verwenden möchte. Dafür reicht ein Byte pro Zeichen nicht mehr aus, so daß dann jedes Zeichen zwei Byte Speicherplatz beansprucht. Die ersten Betriebssysteme wurden bereits auf die Verwendung von Unicode-Zeichen umgestellt. Bis sich Unicode allgemein durchgesetzt hat, sind Probleme bei der Darstellung dieser Zeichen nicht auszuschließen.

Sie müssen die Feinheiten der Kodierungen (es gibt viele verschiedene) nicht kennen, doch sollten Sie eine Mail erhalten, mit der Sie nichts anfangen können, muss der Fehler nicht unbedingt nur am Absender liegen. Es kann auch sein, dass Ihr Partner einen Zeichensatz spezifiziert hat, über den Sie nicht verfügen oder dass er ein Attachment gesendet hat, mit dem Sie nichts anfangen können. Mit etwas Übung beim Lesen von Header-Zeilen können Sie die Ursache meist selbst herausfinden.

2.2. E-Mailadressen

Struktur von Mailadressen

Nachdem Mailadressen auf Visitenkarten, Reklametafeln und Plakaten Einzug gehalten haben, ist der prinzipielle Aufbau intuitiv allgemein bekannt. Das liegt daran, dass sich die im Internet verbreitete Schreibweise **Mailbox@Domain** immer weiter durchgesetzt hat. Diese Adressen bestehen aus drei Elementen:

1. In der Mitte steht das Trennzeichen @ (gesprochen wie das englische "at", also etwa "ät"). Auf den deutschen PC-Tastaturen geben Sie es ein, indem Sie die ALT-GR-Taste festhalten und Q drücken.

2. Rechts steht der Domainname, der den Ort der Mailbox spezifiziert. Meist ist das kein konkreter Rechnername, weil ein Rechner auch ausfallen oder aus anderen Gründen nicht erreichbar sein kann. Beispielsweise kann dort der Name eines Bereiches, also etwa `mathematik.tu-chemnitz.de` oder eines Matrikels also `s2003.tu-chemnitz.de` stehen.

3. Links vom @ steht der Mailbox-Name, der üblicherweise eine Person bezeichnet. Oft ist die Zuordnung zur Person aus dem Mailboxnamen ersichtlich, manchmal finden sich aber auch Funktionen (`service`@..., `hilfe`@...) oder kryptische Abkürzungen (`S048215`@...).

Wichtig sind noch folgende Anmerkungen:

- In Mailadressen wird Groß- und Kleinschreibung nicht unterschieden.

- Unter der Adresse `postmaster`@**domain** erreicht man üblicherweise den für das Mailsystem verantwortlichen Administrator einer Domain.

- Der Mailboxname (z.B. **Vorname.Nachname**) wird auch als Alias bezeichnet und über eine Tabelle einem Nutzerkennzeichen, also einem Account zugeordnet. Für diese Tabellen ist der Postmaster verantwortlich. Hier können bei einem Namenswechsel auch neue Alias-Namen eingetragen werden, ohne dass der Account geändert werden muss.

- Zu einer Mailadresse können noch Kommentare hinzugefügt werden. Diese enthalten meist den Namen des Nutzers und werden vom Mailprogramm entsprechend angezeigt. Zwei Formen sind üblich (achten Sie auf die unterschiedlichen Klammern):

  ```
  Alfons.Bitmeister@t-online.de (Alfons Bitmeister)
  Alfons Bitmeister <Alfons.Bitmeister@t-online.de>
  ```

  Umlaute in den Kommentaren erfordern eine Sonderbehandlung. Die meisten Programme beherrschen das. Wenn Ihre Partner jedoch über Probleme damit berichten, sollten Sie Umlaute in Ihrem Namen bei der Konfiguration lieber umschreiben, also ae statt ä usw. verwenden.

Seien Sie sorgfältig beim Notieren von Mailadressen - im Gegensatz zu Briefen werden Mails mit einem falschen Zeichen in der Adresse unbarmherzig zurückgewiesen. Sollte eine Mail nicht zustellbar sein, erhalten Sie im Allgemeinen eine Fehlermeldung. Besteht der Fehler nur zeitweilig, weil beispielsweise die Domain des Empfängers wegen Bauarbeiten nicht erreichbar ist, schicken Ihnen manche Mailsysteme eine Warnung. Sie müssen dann nichts weiter unternehmen.

Hinter manchen Mailadressen verbergen sich Programme, die aufgrund bestimmter Schlüsselwörter aktiv werden. Ein sehr einfaches Beispiel ist das Echo: Unter der Adresse `echo@tu-chemnitz.de` erreichen Sie einen **Auto-Responder**, der Ihnen Ihre E-Mail postwendend zurückschickt. Das ist eine sehr nützliche Einrichtung für Testzwecke: Wenn Ihnen das Echo eine Antwort senden kann, können es sicher auch menschliche Partner.

Mailinglisten

Die `To`-Zeile einer E-Mail muss nicht unbedingt den endgültigen Empfänger enthalten. So kann zum Beispiel in der `To`-Zeile die Adresse einer sogenannten **Mailingliste** stehen. Das bedeutet, dass es eine Sammeladresse gibt, und alle Mitglieder der Mailingliste erhalten Mails an diese Sammeladresse so, als hätten Sie sie einzeln angeschrieben. Bei solchen Listenmails bleibt die `To`-Zeile erhalten. Sie finden dort die Adresse der Mailingliste. Ein Programm hat jedoch aus der einzelnen Mail an die Listenadresse viele neue Mails generiert, die dank unterschiedlicher Envelope-Adressen viele verschiedene Adressaten erreichen. Im täglichen Leben ist das vergleichbar mit einem Leserbrief in einer Zeitung, wo Sie auch an eine einzelne Adresse schreiben, Ihre Zeilen jedoch viele Empfänger erreichen.

Der Umgang mit Mailinglisten birgt einige Tücken in sich, wenn Sie sich nicht unbeliebt machen wollen, denn schließlich wollen Sie mit technischen Fragen ("Wie komme ich auf die Liste?", "Wie kann ich mich löschen?") nicht alle Listenmitglieder nerven. Im Normalfall erhalten Sie mit den Informationen über eine solche Liste auch Hinweise, wie man sich ein- oder austrägt. Lesen Sie sich diese aufmerksam durch, denn diese Hinweise können nicht Gegenstand dieses Materials sein.

Die meisten Provider haben im WWW Informationen abgelegt, wie eigene Mailinglisten eingerichtet und betrieben werden.

2.3. Zugangsmöglichkeiten für Nutzer

Mailversand

Wenn Sie einen gewöhnlichen Brief absenden wollen, werfen Sie ihn irgendwo in einen der gelben Briefkästen. Um den Rest kümmert sich die Post. Nicht anders funktioniert es in der elektronischen Post: Sie müssen Ihre E-Mail bei einem **Mailserver** (manchmal auch als **Mailhost** bezeichnet) einliefern. Im Normalfall kümmert sich darum Ihr Mailprogramm, doch müssen Sie ihm vorher sagen, welchen Mailserver es wählen soll.

> *Als **Server** bezeichnet man ein Programm oder einen Rechner, der eine bestimmte Serviceleistung (Dienst) zur Verfügung stellt. Diese Dienste werden dann von den **Klienten** in Anspruch genommen. Neben Mailservern werden Sie noch weitere Server kennenlernen, z.B. Druckserver, Computeserver, WWW-Server ...*

Der "Einwurf" der Mail geschieht mit einem festgelegten Verfahren, im Sprachgebrauch der Datenkommunikation Protokoll genannt. Das **Simple Mail Transfer Protocol (SMTP)** hat in letzter Zeit noch einige Erweiterungen erfahren, so dass man mitunter auch den Begriff **ESMTP** (E für Extended) findet. Die Mailserver heißen daher auch **SMTP-Server**. SMTP ist also das Regelwerk, nach dem Briefe in elektronische Briefkästen eingeworfen werden.

> *Übrigens ähnelt der Aufbau einer SMTP-Verbindung verblüffend der Eröffnung eines Telefongespräches, wie er in Abschnitt 1.1. dargestellt wurde.*

Leider verleitet dieses einfache und funktionale System zu missbräuchlicher Verwendung. Im Gegensatz zur Briefpost, wo jeder Brief mittels einer Briefmarke bezahlt wird und das Transportsystem in einer Hand liegt, gehören die Mailserver unterschiedlichen Einrichtungen, und die einzelne Mail wird nicht bezahlt. Daher treffen die Administratoren Vorsichtsmaßnahmen, damit nicht ein fremder Nutzer große Mengen von E-Mails auf ihren Mailservern einliefert, die gar nicht für die eigenen Nutzer bestimmt sind. Das Durchleiten fremder Mail - **Relaying** genannt - wird damit unterbunden.

Umgekehrt wird außerdem verhindert, dass Rechner innerhalb des lokalen Netzes direkt Mail auf außerhalb gelegenen Servern einliefern können (Abb.). Nur die Mailhosts

des eigenen Netzes können Mail von außerhalb direkt empfangen oder diese an fremde Mailhosts weiterleiten. Das bedeutet, dass nur "Einlieferungsbriefkästen" beim eigenen Provider genutzt werden können. Sollten Sie Ihr Mailprogramm selbst konfigurieren, müssen Sie also den Mailhost entsprechend angeben.

Wer sich oft bei fremden Providern einwählt, beispielsweise preiswerte call-by-call-Nummern nutzt, müsste also immer neu herausfinden, welche Mailserver er dort nutzen kann. Das wäre mühevoll und umständlich. Wenn man dem heimatlichen Mailserver sagen könnte, dass man eigentlich ein bekannter Nutzer ist, der nur gerade mit der IP-Nummer eines fremden Providers arbeitet, könnte die Annahme der Mail gestattet werden. Dieses Verfahren heißt **SMTP Authentication** und wird von einigen Programmen wie z.B. Netscape Messenger oder Microsoft Outlook unterstützt. Man wird beim Versand der Mail nach Nutzerkennzeichen und Passwort gefragt. Sinnvollerweise schaltet man dazu auch eine verschlüsselte Übertragung (mit TLS/SSL) der Mails ein. Natürlich muss auf der anderen Seite auch der Mailserver diese Protokolle unterstützen, doch darauf hat man als Nutzer nur begrenzten Einfluss.

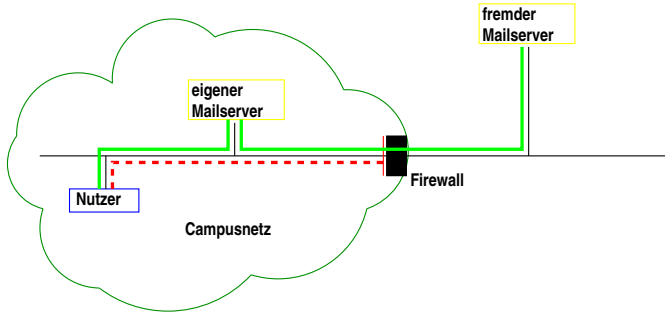


Abbildung 2.3-1.: Direkte SMTP-Verbindungen sind nicht erlaubt.

Der im Bild auftauchende **Firewall** (Brandmauer) hat nicht nur für die E-Mail Bedeutung, sondern schützt die Nutzer des lokalen Netzes auch vor anderen unerwünschten Zugriffen "von außen". Die Rechner des lokalen Netzes sind dadurch nicht für alle Dienste erreichbar: Ein Arbeitsplatzcomputer darf beispielsweise auch nicht als FTP- oder WWW-Server für den Rest der Welt in Erscheinung treten.

Mailempfang

Ihre private Post entnehmen Sie einem Hausbriefkasten, und zwar einem ganz bestimmten, zu dem nur Sie einen Schlüssel besitzen. Nicht anders ist es bei elektronischer Post: Irgendwo befindet sich eine **Mailbox**, in der alle Ihre neuen Mails abgelegt werden. Um Ihre Mail lesen zu können, benötigen Sie ein Mailprogramm, einen sogenannten **Mail User Agent (MUA)**. Der MUA muss auf Ihre Mailbox zugreifen können.

Meist wird sich die Mailbox nicht direkt auf Ihrem Arbeitsplatzrechner befinden, denn dann müsste Ihr Rechner ständig eingeschaltet sein, um neue Mails empfangen zu können - genauso, wie ein Hausbriefkasten auch ständig erreichbar ist. Zudem könnten Sie nur schwer von anderen Plätzen aus darauf zugreifen, und auch die Sicherung gegen technische Ausfälle läge in Ihrer Hand.

Mailboxen befinden sich also auf zentralen Servern, und drei Möglichkeiten des Zugriffs sind weit verbreitet:

1. Die Mailbox wird mittels eines Netzwerkfilesystems auf Ihren Rechner transportiert, und das Mailprogramm greift direkt darauf zu. Es gibt verschiedene Netzwerkfilesysteme, die im Abschnitt 5.3 kurz vorgestellt werden. Dem Vorteil der direkten Sichtbarkeit stehen Probleme bei der Realisierung gegenüber. Zudem werden Sie das "richtige" Netzwerkfilesystem nicht an jedem beliebigen Rechner vorfinden, insbesondere, wenn Sie außerhalb des Campusnetzes arbeiten. Daher verliert diese Methode stark an Bedeutung.

2. Speziell für den Zugriff auf Mailboxen wurden einige Internet-Protokolle geschaffen: Das **Post Office Protocol (POP)** wird allmählich vom moderneren und leistungsfähigeren **Interactive bzw. Internet Mail Access Protocol (IMAP)** abgelöst, welches z.B. auch Such- und Filterfunktionen unterstützt.

   Diese Protokolle sorgen für eine Verständigung zwischen dem Mailprogramm auf Ihrem Computer und dem Mailboxserver. Sie sorgen auch für eine Authentifizierung, damit kein Fremder Ihre E-Mail lesen kann - allerdings wird die Mail dann unverschlüsselt übertragen. Sie ermöglichen es Ihnen auch, von fremden Rechnern aus auf Ihre Mailbox zuzugreifen, wenn Sie dort einen POP- oder IMAP-fähigen Klienten vorfinden und passend konfigurieren.

   Um die Mail auch während der Übertragung zu schützen, wurden neue Varianten von POP und IMAP entwickelt. Bei "POP/IMAP via TLS/SSL" erfolgt eine verschlüsselte Übertragung der E-Mails. Wenn Mailbox-Server und Mailprogramm diese Variante unterstützen, ist das derzeit eine der besten Möglichkeiten, seine Mails zu lesen. Die meisten modernen Mail-Programme sind dazu in der Lage.

3. In jüngster Zeit wird der Zugang zur eigenen Mailbox oft auch über WWW angeboten. In diesem Fall arbeitet Ihr WWW-Browser als Vermittler zur Mailbox. Für Sie als Nutzer sind die Unterschiede möglicherweise gar nicht so offensichtlich. Sie benötigen in diesem Fall zum Lesen Ihrer Mail nur einen WWW-Browser, und den finden Sie mittlerweile fast überall auf der Welt. Vermutlich werden Sie sich freuen, dass viele Einstellungsarbeiten überflüssig werden, weil Ihr Provider das bereits für Sie erledigt hat. Andererseits sind Sie an die Funktionen gebunden, die Ihr Provider bereitstellt und können sich nicht durch die Wahl eines eigenen Programms den Ihnen von Ihnen gewünschten Komfort verschaffen.

Wir orientieren auf einen Zugriff auf die Mailbox mittels **IMAP** via TLS/SSL. Um Ihr Mailprogramm konfigurieren zu können, müssen Sie wissen, wie Ihr Mailbox-

Server heißt. Viele Provider wählen einen gut merkbaren Namen, die TU Chemnitz beispielsweise `mailbox.hrz.tu-chemnitz.de`. Außerdem müssen Sie zumindest Ihr Nutzerkennzeichen angeben und das Passwort eingeben.

> *Wenn Ihr Mailprogramm weiß, wo sich Ihre Mailbox befindet, wie Ihr Name lautet und welchen Schlüssel (Passwort, ...) es verwenden soll, kann es auch Ihre Post für Sie holen.*

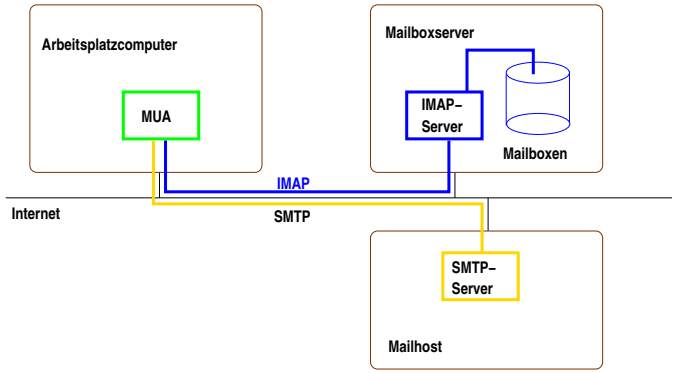


Abbildung 2.3-2.: Das Mailprogramm liest mit IMAP die Mailbox und sendet mit SMTP über den Mailhost.

2.4. Funktionen von Mail-Klienten

Ein Mail-Programm sollte für Sie so etwas wie ein guter Sekretär sein. Es gibt viele Programme mit unterschiedlichen Eigenschaften, und es kann im Rahmen dieses Lehrmaterials keine Bedienungsanleitung für diese Vielfalt gegeben werden. Sie werden jedoch immer wieder auf gewisse Funktionen stoßen, die bei nahezu allen Mailprogrammen vorhanden sind:

Überblick über die eingegangene Post

Gelesene, beantwortete und neue E-Mails müssen deutlich erkennbar sein, Absender, Datum und Subject sollen auf Anhieb sichtbar sein. Auch eine Information über die Größe und eventuelle Anhänge (Attachments) ist wertvoll. Die Sortierreihenfolge (nach Datum, nach Eingang, auf- oder absteigend) können Sie selbst bestimmen.

Zusätzlich gibt es Möglichkeiten, einzelne oder eine ausgewählte Menge von Mails auszudrucken oder zu löschen.

Sinnvoller Umgang mit Anhängen (Attachments)

Keinesfalls sollten ungefragt Anwendungen gestartet werden, die den Inhalt des Attachments ausführen. Es ist wichtig, den Unterschied zwischen Ansehen und Ausführen zu verstehen:

Während ein einfacher Text angezeigt und von Ihnen gelesen wird wie ein beliebiger Zettel, führen Anwendungen wie MS Word ein Dokument wie ein Programm aus. Sie zeigen nicht nur den Text an, sondern arbeiten mitunter auch darin enthaltene Anweisungen ab.

> *So wie Sie ohne Rückfrage und ein wenig Nachdenken nicht irgendwelchen Anweisungen folgen werden, die zufällig in ihrem Hausbriefkasten liegen ("Kaufen Sie ein Haus in Südfrankreich!"), so wenig sollten Sie Ihren Programmen erlauben, Anweisungen zu folgen, die jemand in Ihren elektronischen Briefkasten geworfen hat.*

Das Programm muss rückfragen, ob es ein Attachment einer bestimmten Anwendung übergeben darf!

Verwaltung der Post

Sie sollten Ihre Mail nicht in der Eingangsmailbox liegenlassen. Ihre Mailbox kann ebenso wie Ihr Hausbriefkasten "überlaufen". Speichern Sie gelesene Mails in Ablagen (**Folder**) ab. Sie sollten die Folder geeignet benennen. Einige Programme unterstützen Sie dabei, indem sie den Namen des Absenders der Mail als Folderbezeichnung vorschlagen.

Selbstverständlich sollte es auch einen Folder geben, der die von Ihnen selbst geschriebenen Mails enthält.

In Ihren Foldern sollten Sie suchen können - nach Subjects oder Begriffen aus dem Inhalt der Mail.

Erstellen neuer Nachrichten

Ihr Programm sollte ein Adressbuch besitzen oder auf ein solches zugreifen können, damit Sie die Mailadressen Ihrer Partner nicht immer von neuem eingeben müssen. Es wird die Headerzeilen automatisch erstellen oder sinnvolle Unterstützung geben. Sie können einen oder mehrere Empfänger angeben und `CC`-Zeilen (Copy) hinzufügen. Natürlich werden Sie auch Attachments hinzufügen können.

Wenn Sie eine Mail an mehrere Empfänger schreiben, werden Sie die Adressen in die `TO`- oder `CC`-Zeilen eintragen. Denken Sie daran, dass alle Empfänger alle Adressen sehen können. Das kann gewollt sein, meist wirkt es jedoch unseriös. Die Situation ist vergleichbar mit einem Rundschreiben Ihres Kreditinstitutes, auf dem alle anderen Kunden ebenfalls aufgelistet sind.

Reaktion auf Nachrichten

Sie können E-Mails mittels **Reply** beantworten. Dadurch senden Sie eine Mail an den Absender der Nachricht zurück. Möglicherweise wollen Sie auch Teile der originalen Mail einschließen, um sich darauf zu beziehen. Dies nennt man **quoten**. Lassen Sie nur soviel Text stehen wie nötig, und schreiben Sie Ihre Antwort darunter - das liest sich angenehmer.

War die Mail an mehrere Empfänger gerichtet, sollten Sie überlegen, ob Sie Ihre Antwort an den gleichen Empfängerkreis ("group reply") oder nur an den Absender des Originals ("reply") richten.

Eventuell wollen Sie auch einen anderen Nutzer über die erhaltene Mail in Kenntnis setzen, diese also weiterleiten. Dies wird als **Forwarding** bezeichnet. Denken Sie daran, dass die Weitergabe privater Nachrichten auch ein Vertrauensbruch sein kann.

In jedem Fall sollten Sie die Regeln der Netikette beachten, der wir den nächsten Abschnitt gewidmet haben.

Heutzutage gibt es zwei große Klassen von Mail-Klienten: Einige Pakete verbinden die Mail-Bearbeitung mit vielen anderen Funktionen. Am häufigsten werden aus dieser Klasse der Netscape-Messenger und Outlook von Microsoft genutzt.

Eine andere Klasse von Programmen wurde nur für die Bearbeitung von E-Mail entworfen. Diese Programme nutzen andere Anwendungen, wenn z.B. Bilder dargestellt werden sollen, die per Mail ankamen. Die Beschränkung auf eine Funktion stellt daher keinen Nachteil dar.

Eine andere Möglichkeit ist die Einteilung in Programme mit einer grafischen Oberfläche oder textbasierte Anwendungen. Die auf den ersten Blick altertümlich wirkenden textbasierten Programme verbergen oftmals eine enorme Leistungsfähigkeit. Sie erfordern einen höheren Einarbeitungsaufwand, honorieren diesen aber mit einer hohen Geschwindigkeit bei der Bearbeitung und einem relativ geringen Ressourcenbedarf. Als Beispiel sei hier das auf mehreren Plattformen verfügbare Programm `pine` genannt.

Ein weiterer Vorteil textbasierter MUAs besteht darin, dass sie sich über Secure-Shell- oder Telnet-Verbindungen (siehe Abschnitt 5.1) recht vernünftig aus der Ferne bedienen lassen, auch wenn man nur über eine Verbindung mit verhältnismäßig geringer Kapazität (z.B. eine Modem-Verbindung) verfügt. So kann man z.B. von zu Hause aus die auf den Rechnern der TU Chemnitz bereitgestellten Mail-Agenten nutzen.

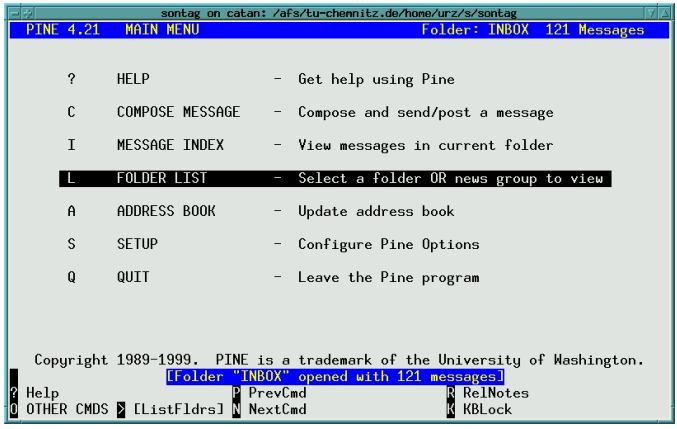


Abbildung 2.4-1.: Das Programm "pine" begrüßt den Nutzer spartanisch, ist aber ein vollwertiges, gut konfigurierbares Mailprogramm.

2.5. Anwendungshinweise und Netikette

Im direkten Umgang mit anderen Menschen sammeln wir seit unserer Geburt Erfahrungen. Inzwischen kennen wir die Gepflogenheiten des Auftretens, wählen unsere Sprache der Umgebung angemessen und verwechseln den Stil eines Einkaufszettels nicht mit dem eines wissenschaftlichen Artikels.

Das Internet als Medium ist relativ jung, die meisten Nutzer schreiben erst seit wenigen Jahren oder gar Monaten E-Mails. Entsprechend groß ist die Unsicherheit bei der Wahl des Stiles. Die wenigen Jahre, die das Internet für die Kommunikation zwischen Menschen genutzt wird, haben jedoch ausgereicht, um eine Reihe von Verhaltensmustern zu entwickeln, die man mit dem Kunstwort **Netikette** bezeichnet. Die Netikette ist kein Gesetz und keine Verordnung, die von irgend einer Institution erlassen wurde. Sie entwickelte sich aus täglichen Beobachtungen der Nutzer selbst. Aus diesem Grund gibt es immer wieder Variationen in dem, was als Netikette bezeichnet und was als ihr zugehörig betrachtet wird. Der grundlegende Gedanke ist dabei, es dem Empfänger so angenehm und so leicht wie möglich zu machen, den verfassten Text zu lesen.

Denken Sie daran, dass Sie nicht wissen, in welcher Umgebung und mit welchen Programmen Ihre Partner arbeiten. Ein aufwendig aufbereiteter Text kann für Ihren Partner wertlos sein, wenn er ein bestimmtes Programm benötigt, um ihn lesen zu können. Beispielsweise sehen in HTML verfasste Artikel auf dem eigenen Bildschirm möglicherweise sehr ansprechend aus. Benutzt der Empfänger jedoch ein Mailprogramm, welches kein HTML darstellen kann, so muss er den eigentlichen Text zwischen den Formatierungsanweisungen herausfinden, was oft sehr mühsam ist. Einfacher Text gilt daher

immer noch als höflichste, sicherste und zudem meist auch effizienteste Variante.

Große Einrichtungen verfügen meist über einen leistungsfähigen Anschluss ans weltweite Netz. Ein Bild als Anhang an eine Mail bereitet hier keinerlei Probleme, kann aber in weniger gut ausgestatteten Einrichtungen oder bei privaten Nutzern, die ihre Mails via Modem holen, Ärger und Kosten verursachen. Erkundigen Sie sich im Zweifelsfall vor dem Absenden bei Ihren Partnern, welche Größe einer Mail noch akzeptabel ist.

Der weniger formelle Umgangston im Netz und das einfache Absenden dürfen nicht zu inhaltlicher Nachlässigkeit führen. Unverständliche Sätze, undurchdachte Aussagen, Häufung von Schreibfehlern kosten die Zeit Ihrer Partner und werden daher als unhöflich empfunden. Besonderer Wert sollte auf eine geeignete Wahl der Betreffzeile (**Subject**) gelegt werden. Das Subject sollte den Inhalt der Mail kurz charakterisieren. Ein schlecht gewähltes Subject kann die Bearbeitung der Mail beim Leser durchaus verzögern, wenn er aufgrund sehr vieler Mails entscheiden muss, in welcher Reihenfolge er die Nachrichten liest. Das heißt natürlich nicht, dass man mit Zusätzen wie *wichtig* oder *dringend lesen* eine Dringlichkeit suggerieren soll, die in Wirklichkeit nicht vorliegt.

Schreiben Sie kurze, durch Leerzeilen getrennte Absätze, denn das erleichtert das Lesen. Beschränken Sie die Zeilenlänge auf unter 75 Zeichen. Denken Sie daran, dass Tabellen in reinen ASCII-Texten nicht als Tabelle erscheinen, wenn Sie eine proportionale Schrift, also Buchstaben mit unterschiedlicher Breite, bei Ihrem Programm verwenden.

Wenn Sie eine E-Mail beantworten, dann ist es üblich, die zu beantwortende Mail in relevanten Ausschnitten zu zitieren und die eigenen Antworten direkt unter die betreffende Textstelle der Originalmail zu setzen. Dies ermöglicht dem Leser, schneller den Zusammenhang wiederzufinden. Auf keinen Fall zitiert werden Anreden, Grußformeln oder automatisch an die Mail angehängte Zusatzinformationen. Gelegentlich ist es auch erwünscht, dass man die komplette Mail an das Ende der eigenen Nachricht anhängt und seine eigenen Bemerkungen vor diesem Zitat anbringt. Wenn das der Fall ist, so sollte man diesem Wunsch entsprechen. Üblich ist dies jedoch nicht, weil der Leser so in die Situation gebracht wird, stets eine große Menge Text nach neuen Informationen zu durchsuchen, obwohl es nichts zu finden gibt.

Neben rein gestalterischen Qualitätsmerkmalen fällt natürlich auch der Inhalt bei einer Mail ins Gewicht. Eine höfliche und passende Anrede sowie ein abschließender Gruß sollten genau so selbstverständlich sein wie der richtige Einsatz von "Du" oder "Sie". Dieser orientiert sich an den normalen Umgangsformen und beim Einsatz von E-Mail gibt es da keine abweichenden Regeln.

Im Gegensatz zum direkten Gespräch werden natürlich keine Gesten und Gesichtsausdrücke übertragen. Ein lustig gemeinter Kommentar kann so leicht falsch verstanden werden und zu Verstimmungen führen. Daher ist es sinnvoll, auf missverständliche Formulierungen zu verzichten oder zumindest entsprechend zu kennzeichnen. Für diesen Zweck wurden die so genannten **Smileys** erfunden.

```
Falls Sie Smileys noch nicht kennen: Neigen Sie
einfach den Kopf nach links und schauen Sie die
folgende Zeile an.

:-)  :-(  :-]  (8-)  ;-D
```

Der Abstand, den man durch die zwischengeschalteten Rechner bekommt, verleitet unter gewissen Umständen, den Empfänger einer Mail unnötig zu beleidigen oder übertrieben stark anzugreifen. Bedenken Sie, dass nicht ausgeschlossen werden kann, dass Sie die betreffende Person einmal persönlich treffen oder die Mail auch andere Personen zu lesen bekommen könnten. Ein gemäßigter Ton hilft, peinliche Situation zu vermeiden.

Im Gegensatz zur Briefpost werden bei der E-Mail-Adresse kleine Schreibfehler nicht stillschweigend korrigiert. Die Adressen haben keine Redundanz - man kann also nicht wie bei der Post aus dem Namen der Stadt und der Straße auf die Postleitzahl schließen. Kontrollieren Sie daher die Adressen aufmerksam, und mehr noch als die fremden sollten Sie den Eintrag für Ihre eigene Adresse überprüfen, wenn Sie Ihr Programm konfigurieren: Eine Mail an eine fehlerhafte, nicht existierende Adresse kommt zurück, aber ein Empfänger kann Ihnen nicht antworten, wenn Ihre `From`-Zeile nicht stimmt.

Hin und wieder werden Sie Mails mit **Fehlermeldungen** erhalten - die möglichen Ursachen sind vielfältig. Sei es, dass Sie sich vertippt haben, dass eine technische Störung vorliegt oder die Mailbox des Empfängers überläuft. Letztendlich ist das ein Zeichen für die Zuverlässigkeit, die etwa dieselbe Größenordnung wie bei der gelben Post erreicht: E-Mail kommt entweder an oder zurück.

Sie werden in Ihrer Mailbox oftmals auch **Werbemails** finden. Mitunter versprechen die Absender, Sie aus dem Verteiler zu löschen, wenn Sie auf eine bestimmte Art und Weise reagieren. Seien Sie vorsichtig: Durch Ihre Antwort zeigen Sie, dass Sie Ihre Mail lesen, und Ihre Mailadresse bekommt bei den Werbestrategen einen viel höheren Wert.

Die einfachste Reaktion ist die Löschung der ungewünschten Mail. Sollten Sie massiv belästigt werden, könnten Sie den Provider des Verursachers informieren, denn Werbung per E-Mail ist nicht zulässig. Leider verschleiern die Urheber oft den Weg der Mail, so dass die Feststellung des Verursachers viel Fachwissen erfordert.

Manche Provider bieten automatische Filter an, um Werbemails soweit möglich herauszufiltern. Die Filter sind wirkungsvoll, können jedoch niemals sämtliche Werbung finden. Je höher der herausgefilterte Anteil Werbung ist, desto höher ist leider auch die Wahrscheinlichkeit, "gute" Mails zu filtern.

Ebenso unangenehm sind **Kettenbriefe**, die als E-Mail leider oft wirkungsvoller als per gelber Post sind. Eine häufige Form ist die Warnung vor Viren, die an "alle Freunde und Bekannten" weiterverteilt werden soll. Die gut gemeinte Weitergabe dieser Warnungen führt zu einer Flut von Mails. Der beschriebene Virus existiert dabei in vielen Fällen gar nicht. Der eigentliche Virus ist die Mail, die andere Anwender verunsichert, Zeit und Geld kostet, sich selbst weiterverbreitet und viel Unruhe stiftet. Eine seriöse Warnung nennt dagegen eine überprüfbare Quelle, ist normalerweise digital signiert und hat einen eindeutigen Absender. Mindestens eine WWW-Seite mit Hintergrundinformationen zum beschriebenen Virus sollte genannt werden.

Oftmals enthalten derartige Hinweismails noch die Adressen sämtlicher Bekannten des Absenders in der To- oder Cc-Zeile. Wer sein Adressenbuch so sorglos weiterverteilt, muß sich nicht wundern, wenn seine Anschrift schließlich auch bei den Werbeversendern landet.

Die technischen Mechanismen des Mailversands bieten nur wenig Sicherheit. Man kann eine "einfache" E-Mail am ehesten mit einer Postkarte vergleichen: So wie dort der Briefträger den Text lesen könnte, könnten auch die beteiligten Administratoren prinzipiell den Inhalt einer Mail erfahren (werden es aber in der Regel nicht tun). Auch die Absenderadresse muss nicht unbedingt stimmen - ebenso wie bei Briefen. Wenn Sie Wert auf Sicherheit und Vertraulichkeit legen, müssen Sie sich mit digitalen Signaturen und Verschlüsselungstechniken beschäftigen.

Vertiefung:
Eine Vielzahl von Hinweisen zu E-Mail, darunter auch eine Suchmöglichkeit nach E-Mailadressen, finden Sie unter

> E-Mail an der TU Chemnitz
> `[http://www.tu-chemnitz.de/urz/mail]`

Die Netikette in ihrer ausführlicheren Version:

> Netikette
> `[http://www.chemie.fu-berlin.de/outerspace/netnews/netiquette.html]`

Eine Übersicht über die Smilies bietet

> The Unofficial Smiley Dictionary
> `[http://www.tu-chemnitz.de/docs/eegtti/eeg_286.html]`

Mit einfachem Klicken der Maus streift der Surfer durch das World Wide Web. Die Einfachheit seiner Bedienung bescherte dem Internet seine rasante Verbreitung. Wer selbst Seiten ins Netz stellt, muss mehr als Surfen können - und deutlich mehr wissen.

3

WWW - Das World Wide Web

3.1. Architekturen und URLs

Wenn heutzutage von "dem Internet" gesprochen wird, ist meist das **World Wide Web (WWW)** gemeint. Die vorangegangenen Kapitel zeigen, dass das Internet viel mehr umfasst. Aber gerade das WWW hat dem Internet einen gewaltigen Boom beschert. Ein Grund ist ohne Zweifel der sehr einfache Zugang mit grafischen Anzeigeprogrammen (Browser). Ein weiterer Vorteil des WWW sind die umfangreichen Gestaltungsmöglichkeiten für Dokumente, die neben einfachem Text auch Tabellen, Grafiken, Querverweise und interaktive Elemente enthalten können. Entwickelt wurde es vor allem am Europäischen CERN im Jahre 1990 von Tim Berners-Lee, der heute der Direktor des **World Wide Web Consortium (W3C)** ist. Er hat das Protokoll HTTP, die Adressierung mit URLs und die Sprache HTML erfunden.

Das Anschauen von Dokumenten im WWW nennt man **surfen**. Dabei fängt man an einer beliebigen **Webseite** an und "hangelt" sich durch Hyperlinks zu anderen Seiten. Der Browser fordert diese Seiten von dem entsprechenden Server an und stellt sie dar. Diese Art der Informationsbeschaffung bewirkt, dass manche Zugriffe sehr schnell gehen und in anderen Situationen die Seite überhaupt nicht geladen wird. Für jeden Klick auf einen Verweis muss nämlich eine Datenverbindung bis zu dem Server aufgebaut werden, der die Seite beherbergt. Das ist anders als beispielsweise bei Mail oder News, wo der Server im lokalen Netz meist schnell erreicht wird.

Rechner, die Webseiten anbieten, nennt man **WWW-Server**. Das **HyperText Transfer Protocol (HTTP)** ist eine Kommunikationsvorschrift für Rechner, um Textdateien (HyperTexte) zu übertragen sowie Daten vom Endnutzer (*User*) zum Server zurück-

zuschicken. HyperTexte sind nichts anderes als Texte, die mit speziellen Einfügungen (**Tags**) versehen sind, damit der Browser zusätzliche Informationen zur Darstellung des Textes erhält. Diese Tags bilden die **HyperText Markup Language (HTML)**.

Um ein WWW-Dokument zu finden, wird eine Adresse benötigt. Diese nennt sich **Uniform Resource Locator (URL)**, was soviel wie "vereinheitlichte Objektadresse" bedeutet.

Die URLs werden als das offensichtliche Merkmal des WWW wahrgenommen. Ein URL besteht aus mehreren Teilen. Die meisten Leser haben einfache URLs bereits gesehen. Typischerweise sieht dieser so aus:

```
protokoll://rechner/verzeichnis/datei
```

Ein vollständiger URL sieht folgendermaßen aus:

```
protokoll://nutzer:passwort@rechner:port/verzeichnis/datei
```

Der Schrägstrich ist immer vorwärtsgerichtet - also / und nicht wie in MS Windows ein Backslash (\)!

`protokoll`

Bestimmt die Art der Übertragung. Mögliche Werte sind: http, ftp, mailto, news, telnet, file oder gopher. Letzteres ist übrigens ein textorientierter Vorläufer des WWW.

`nutzer`

Ist optional und gibt an, wer den entsprechenden Dienst ansprechen möchte.

`passwort`

Ist ebenfalls nicht zwingend notwendig und wird ggf. verwendet, um den Benutzer zu authentifizieren.

`rechner`

Ist der Name oder eine IP-Adresse eines Rechners, auf dem der entsprechende Dienst angesprochen werden soll.

`port`

Wenn mehrere Server-Programme vom gleichen Typ auf einem Rechner laufen, dann kann mit dieser Nummer genauer angegeben werden, welcher der Server gemeint ist. Der Port muss sehr selten angegeben werden, da die meisten Dienste auf standardisierten Ports angesprochen werden, die der Browser schon kennt.

`verzeichnis`

Werden viele Dateien auf einem Server abgelegt, so ordnet man diese thematisch in Verzeichnissen. Dies wird dann natürlich zum Bestandteil der Adresse.

`datei`

Hier wird nun das gesuchte Dokument benannt.

URLs in mehr oder weniger verkürzter Schreibweise sind heutzutage allgemein bekannt. Hier noch ein paar Beispiele:

- `http://www.tu-chemnitz.de/urz/index.html`
  Dies ist die Homepage des Rechenzentrums der TU Chemnitz. Es handelt sich um die Datei `index.html` auf dem WWW-Server `www.tu-chemnitz.de` im Verzeichnis `/urz`.
- `ftp://ftp.tu-chemnitz.de/pub/linux/`
  Dies ist das ftp-Verzeichnis, welches auf dem ftp-Server `ftp.tu-chemnitz.de` eine Reihe von Linux-Software zur Verfügung stellt. (Unter anderem übrigens stets die neuesten Distributionen!)
- `news:de.newusers.infos`
  Hier wird die Newsgruppe `de.newusers.infos` angesprochen. Es wurde kein Host angegeben. In diesem Fall wird der news-Server verwendet, der im Browser als Vorgabe eingetragen ist.

- `mailto:hilfe@hrz.tu-chemnitz.de`
  Bei Mail entfallen die beiden Schrägstriche, denn auch hier kennt der Browser den für ihn zuständigen Mailserver. Diese URL gibt die Hotline des Chemnitzer **Universitätsrechenzentrums (URZ)** an.

Gelegentlich wird man beim Surfen sehr langen URLs begegnen, bei denen der Dateiname höchst seltsam aussieht. Auf diese Art und Weise werden dem Webserver oft Daten übermittelt. Das können beispielsweise Suchbegriffe bei einer Suchmaschine sein. Seiten, welche über solch einen URL angesprochen werden, werden meist von einem Programm, das auf dem WWW-Server läuft, generiert. Es sollten daher keine **Lesezeichen** (**Bookmarks**) oder Querverweise in eigenen Webseiten darauf gelegt werden.

Vertiefung:

WWW-Consortium - die Hüter des WWW
[`http://www.w3c.org`]

Wer das alles mit IP, WWW und so jetzt noch nicht so richtig verstanden hat, dem hilft vielleicht die Maus :-)

Der Datenweg durchs Internet
[http://www.wdrmaus.de/sachgeschichten/internet/]

3.2. HTML - die Sprache des WWW

Die Seiten im WWW werden in einer Sprache geschrieben, der **HyperText Markup Language (HTML)**. Bereits mit wenigen HTML-Anweisungen können Dokumente ansprechend gestaltet werden. Wenn ein WWW-Browser eine solche Seite anfordert, muss er die HTML-Befehle interpretieren und in eine grafische Darstellung umsetzen. Beispielsweise bestimmt der Autor eines HTML-Dokuments, was eine Überschrift ist. Der Browser jedoch legt fest, wie eine Überschrift dargestellt wird: Ob diese Zeile invers oder in einer größeren Schriftart erscheint, ob (bei Vorleseprogrammen) eine andere Sprecherstimme eingesetzt oder die Lautstärke erhöht wird.

Ein einfaches Beispiel für ein HTML-Dokument:

```
<html>
  <head>
    <title> Ein Beispiel zur Illustration </title>
  </head>
  <body>
    <h1>Dokumente im HTML-Format</h1>
    Das Beispiel dient der Illustration. WWW-Autoren
    kennen die wichtigsten Tags auswendig.
    <p>
    Tags werden durch spitze Klammern (<, >) eingeschlossen.
  </body>
</html>
```

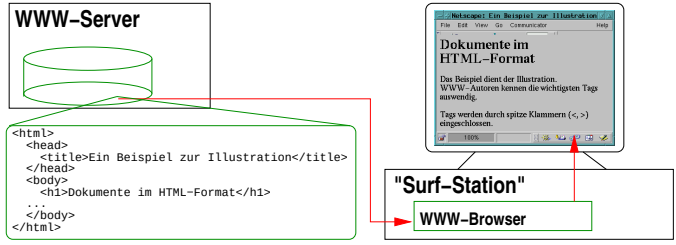


Abbildung 3.2-1.: Erst der Browser legt Zeilenumbrüche und Schriftarten fest.

Die Sprache wird noch immer weiterentwickelt, weshalb die neuesten Features von alten Browsern noch nicht beherrscht werden. Für den Autor heißt das: Neueste Features nur einsetzen wenn nötig!

Einem Autor stehen mehrere Wege offen: Es gibt Softwareprodukte, mit denen die Produktion von WWW-Seiten ohne jede Vorkenntnisse kinderleicht ist. Leider arbeiten die Anwender dadurch oftmals der Philosophie des WWW entgegen und produzieren technisch unkorrekte HTML-Texte. Wer über HTML-Grundkenntnisse verfügt, wird jedoch ansprechende Ergebnisse erzielen. Gute Produkte bieten daher auch einen Blick auf den "reinen" HTML-Text.

> *Das ist wie beim Kochen: Ein Fertiggericht steht zwar schnell auf dem Tisch, doch ein guter Koch kennt Techniken der Verfeinerung und wird sie nutzen.*

Beliebige Textverarbeitung

Am bequemsten arbeitet es sich mit dem gewohnten Textverarbeitungsprogramm. Die meisten Office-Systeme bieten die Möglichkeit, ein Dokument nach HTML zu exportieren. Dabei gibt es aber Nachteile:

Viele Elemente eines gedruckten Textes werden derzeit von HTML nicht unterstützt.

> Aus diesem Grund werden diese entweder weggelassen oder durch Bilder ersetzt. Da ein Bild aber erheblich mehr Bandbreite beim Transport benötigt, lassen sich die Seiten nur sehr langsam laden, und es wird Bandbreite verschwendet.

Formatierungen werden umständlich gesetzt.

> Einige Programme formatieren jedes Wort oder jeden Satz separat. Der HTML-Text vergrößert sich dadurch unnötig und benötigt auf langsamen Systemen länger zum Anzeigen. Bandbreiten- und Speicherplatzbedarf wachsen.

Manche Formatierungen kennt der Browser nicht.

> Obwohl HTML als systemübergreifender Standard entwickelt wurde, legen Textverarbeitungen oft spezielle Schriften im HTML-Code fest, die auf fremden Systemen nicht verfügbar sind. Als Folge sieht das Dokument auf fremden Rechnern ganz anders als erwartet aus.

Spezielle HTML-Editoren

Es gibt spezielle HTML-Editoren, die natürlich nur die Elemente verwenden, die die Sprache auch darstellen kann. Einige Browser enthalten bereits einen solchen Editor. Der damit erzeugte Code ist zwar nicht immer auf dem neuesten Stand und optimal, doch lassen sich die Seiten schnell und einfach erstellen.

Einfache Texteditoren

HTML ist eine Sprache, die man lernen kann. Es gibt hervorragende Anleitungen im Netz. Viele Seiten werden daher von den Autoren "von Hand gesetzt", also mittels eines Text-Editors geschrieben. Solche Editoren sind auf praktisch allen Systemen verfügbar - Notepad unter Windows bzw. vi, emacs oder joe unter Unix. Vom Autor wird dabei verlangt, sich in den sogenannten **Tags** auszukennen: Das sind Anweisungen, die die Darstellung der Seite steuern. Glücklicherweise muss man nicht alle kennen - nur die für den "Eigenbedarf" notwendigen. Sie treten (fast) immer paarweise auf: ein öffnendes und ein schließendes Tag. Im obigen Beispiel ist zu sehen, wie eine Überschrift durch das `h1`-Tag eingefaßt wird und daher vom Browser hervorgehoben werden kann.

Wer seine Seiten mittels anderer Programme produziert, kann nachträglich Fehler beheben oder manuelle Korrekturen vornehmen, wenn er über HTML-Grundkenntnisse verfügt. So lohnt es sich für alle Webautoren, zumindest die Einführungsabschnitte eines HTML-Kurses durchzuarbeiten.

Hier soll und kann jedoch kein HTML-Kurs eingebettet werden, das würde den Rahmen des Materials bei weitem sprengen. Im WWW finden sich ausführliche Informationen in den

Hinweisen für HTML-Autoren.
[http://www.tu-chemnitz.de/urz/www/html-autoren.html]

Dynamische Seiten

Der WWW-Browser verlangt vom Server nichts weiter als eine HTML-Seite. Wie diese entsteht, ist egal. Es muss daher nicht jede Seite als fertige Datei auf der Festplatte des WWW-Servers liegen. Die Seiten können auch dynamisch, im Moment der Anforderung generiert werden.

Beispielsweise kann der WWW-Server im Moment der Auslieferung noch das Datum der letzten Änderung in den Seitenfuß einfügen. Der WWW-Server kann auch ein Programm aufrufen, welches eine Seite produziert. Ein Beispiel für dynamische Seiten ist unser Online-Test: Die Seite, die Sie sehen, wird im Moment der Anforderung erzeugt. Ein weiterer typischer Anwendungsfall sind Datenbankabfragen, beispielsweise im Online-Katalog der Bibliothek.

Als Ergebnis dieser Technik muss eine WWW-Seite nicht immer dieselbe Information liefern - ein Problem bei der Spiegelung oder Abspeicherung von WWW-Angeboten. Suchmaschinen, die eine Seite indizieren, können bei dynamischen Seiten natürlich kaum noch den aktuellen Stand erfassen. Aufmerksame Administratoren schließen Suchroboter daher von der Indizierung derartiger Seiten aus.

Wer dieses Thema vertiefen möchte, sollte unter den Schlagworten **Server side includes (SSI)**, **PHP 4: Hypertext Preprocessor (PHP4)** oder **Common Gateway Interface (CGI)** in den oben genannten Hinweisen für HTML-Autoren nachlesen.

Form und Inhalt

Wie Ihre Webseiten entstehen, ist Ihnen überlassen. Sie sollten jedoch einige Konventionen zu Form und Inhalt beachten, sonst bleiben Sie Ihr einziger Leser. Das Design von WWW-Seiten ist natürlich abhängig vom Inhalt. Der 1. Akademische Faschingsclub Chemnitz wird daher die folgenden Punkte für seine Seiten anders wichten als die Universitätsverwaltung:

- Übersichtlichkeit: Der Nutzer soll sich schnell zurechtfinden können. Ausgeflippte Designs sind zwar ganz nett, fordern jedoch viel Zeit zum Betrachten der Seite.
- Bandbreite sparen: Legen Sie Grafiken in platzsparenden Formaten (JPEG oder PNG sind geeignet). Verwenden Sie bei Bildern die kleinste mögliche Auflösung, weil sonst der Platzverbrauch rasant steigt, und schreiben Sie keine übermäßig langen Dokumente. Nutzer mit langsamen Netzanbindungen oder leistungsärmeren Rechnern werden es Ihnen danken.
- Farben maßvoll einsetzen: Pink auf Hellblau ist schwer zu lesen. Eine schlechte Farbwahl verstößt gegen Grundregeln der Ergonomie. Die Browser unterstützen

auch nicht immer alle Farben, weshalb für HTML eine kleine Menge Farben definiert wurde, die auf jedem System verfügbar sein sollten. Animierte Bilder oder bunte Hintergrundbilder ziehen die Aufmerksamkeit auf sich und lenken leicht vom Hauptthema einer Seite ab.

> Etwa 10 % der Bevölkerung haben eine Rot-Grün-Schwäche. Wer rote Schrift auf grünem Hintergrund verwendet, verliert diesen Teil seiner Leser.

- Aktive Inhalte maßvoll einsetzen: Verwenden Sie Java Applets nur dort, wo es unbedingt notwendig ist. Nicht jeder Browser kann Applets anzeigen, viele Nutzer schalten die Funktion auch aus Sicherheitsgründen ab. Rollende Sternchen gehören sicher nicht zu den sinnvollen Anwendungen. Auf ActiveX-Komponenten sollten Sie verzichten, da gerade im universitären Bereich viele Browser diese nicht anzeigen werden.

- Darstellungsunabhängig gestalten: Nicht jeder Nutzer hat den gleichen Monitor wie Sie. Wer nur für eine bestimmte Auflösung (z.B. 800x600 Pixel) schreibt, produziert für alle anderen meist häßliche Seiten. Es sollten auch niemals absolute Abmessungen bei Tabellen oder Frames angegeben werden.

  "Dieses Buch wurde optimiert für eine Beleuchtung von 60 W mit künstlichem Licht und eine Leseentfernung von 30 cm. Eine passende Glühlampe erhalten Sie hier."

Welches Buch enthält so einen Hinweis? Bei WWW-Seiten kann so etwas schon mal vorkommen ...

Vertiefung:
Weitere Tips für gute Webseiten:
Eine ausführliche Einführung in HTML inklusive Style-Sheets, JavaScript, CGI-Programmierung u.v.a.m. findet sich in Stefan Münz' Dokumentation

> HTML-Dateien selbst erstellen.
> `[http://www.teamone.de/selfhtml.htm]`

Darin werden auch die auf jedem System verfügbaren Farben aufgelistet (die Dokumentation wird an der TU Chemnitz gespiegelt):

> Farbenliste bei Selfhtml
> `[http://www.tu-chemnitz.de/docs/selfhtml/tcaed.htm]`

Eine der besten Sammlungen typischer Fehler sind Stefan Karzauninkats

> Goldene Regeln für schlechtes HTML.
> `[http://www.karzauninkat.com/Goldhtml/goldhtml.htm]`

Hinweise zu einem guten Stil gibt der

> Yale Web Style Guide.
> [http://www.tu-chemnitz.de/docs/yale/contents.html]

3.3. Effektive Suche nach Dokumenten

Das Internet bietet eine gigantische Informationsfülle. Letzte Schätzungen gehen von etwa 3 Milliarden Webseiten und rund 80.000 Newsgroups aus. In dieser Informationsflut findet man sich ohne Hilfen nur schwer zurecht. Man benötigt also eine Art Inhaltsverzeichnis. Derartige Inhaltsverzeichnisse gibt es auch, wobei zwei Formen zu unterscheiden sind: Thematische Kataloge und Volltextsucher.

Die **thematischen Kataloge** entsprechen dem Bild des Inhaltsverzeichnisses am ehesten. Ein Autorenteam beurteilt und katalogisiert eine Menge von Webseiten. Per WWW kann man dann in diesem Katalog blättern und themenbezogene Nachforschungen anstellen. Ein sehr bekanntes System ist Yahoo [1]. Der Nachteil dieser Systeme besteht in der Abhängigkeit von der Einschätzung der Redakteure. Auch wird nicht jede Seite zu dem gewünschten Thema im Katalog eingetragen sein. Dafür werden vorrangig die Startseiten eines Angebotes referenziert, und der Nutzer wird weniger häufig mit aus dem Zusammenhang gerissenen Seiten konfrontiert.

Die thematischen Kataloge führen Sie auf sinnvolle Einstiegsseiten und sind geeignet, um sich zu einem Thema einen Überblick über das Angebot an Dokumenten zu verschaffen.

Volltextsuchsysteme zeichnen sich durch eine andere Herangehensweise aus. Sie versuchen, alle Dokumente des WWW komplett zu erfassen. Eine Suche mit diesen Systemen ist etwa so, als würde man jede Webseite anschauen und dort nach dem entsprechenden Begriff suchen. Um diese Funktionalität zu bieten, werden von diesen Suchsystemen regelmäßig alle erreichbaren Webseiten in einen sehr großen Speicher kopiert. Diese Systeme haben den Nachteil, dass die Suche nicht immer erfolgreich ist, obwohl man glaubt, geeignete Stichworte eingegeben zu haben. Einer der bekannteren Volltextsucher ist Google [2]

Mit Hilfe von Volltextsuchsystemen können Sie sehr gezielt nach spezifischen Informationen suchen, werden aber häufig mit einer Flut von "Treffern" überschüttet und treffen darunter oft auf Seiten, die aus dem Zusammenhang gerissen sind oder scheinbar gar nichts mit Ihrer Anfrage zu tun haben.

Viele Volltextsucher bieten die Möglichkeit, die Suche zu verfeinern. Neben Wörtern, die im gesuchten Dokument vorkommen müssen, kann man beispielsweise auch Wörter gezielt ausschließen.

Die Suchmaschinen versuchen, die Dokumente nach Wichtigkeit zu ordnen. Wenn die Suchbegriffe im Titel oder in Überschriften auftauchen, haben sie eine größere Bedeutung, als wenn sie irgendwo im Text verstreut sind.

Frage 3.3.1:
Kann eine Volltextsuchmaschine ein Dokument finden, in dem der Suchbegriff nur in einem Bild vorkommt?

Neben diesen beiden allgemeinen Kategorien wurde eine ganze Menge anderer Suchsysteme entwickelt. Google [3] ermöglicht auch die Suche in einem Archiv aller wichtigen öffentlichen Newsgroups dieser Welt. Vor einer Frage in einer Newsgroup lohnt sich ein Blick in dieses Archiv. Oft hat man auf diese Art die gesuchte Antwort viel schneller als durch ein Posting.

Für viele Fachgebiete gibt es auch entsprechend spezialisierte Suchsysteme. Diese Stellen sind oft ein geeigneter Einstiegspunkt für die Recherche.

Es gibt noch eine Vielzahl weiterer Such- und Index-Systeme zu(m) finden. Einen guten Einstieg bietet dafür die **Configurable Unified Search Engine (CUSI)** des URZ der TU Chemnitz. [4]

Einige Datenbestände sind ausschließlich durch spezielle Suchsysteme erreichbar. Dazu zählen beispielsweise Literaturdatenbanken wie der **Online Public Access Catalogue (OPAC)** mit Web-Interface, denn eine Volltextsuchmaschine wird die Abfrageseite der Bibliothek nicht mit allen denkbaren Begriffen ausfüllen können...

Viele Webseiten bieten lokale Suchmaschinen an, mit denen innerhalb der Präsentation gesucht werden kann. Das geht oft schneller und ermöglicht präzisere Resultate als ein globaler Suchroboter. Wer sich weiter informieren möchte, dem sei die Suchfibel sehr empfohlen [5].

Wichtig!
Das Lesen der Suchfibel kostet Zeit. Erfolglose Suche kostet mehr Zeit.

Vertiefung:
[1] Yahoo gilt als der Klassiker unter den thematischen Katalogen:

Deutscher Yahoo-Katalog
`[http://de.yahoo.com/]`

[2] Google ist derzeit der Favorit unter den Suchmaschinen.

Google Deutschland
`[http://www.google.de/]`

[3] Google archiviert auch Usenet-Artikel.

Google Groups
`[http://groups.google.com/]`

[4] Einen schnellen Zugriff auf alle möglichen Arten spezieller und allgemeiner Suchmaschinen bietet die

Configurable Unified Search Engine an der TU Chemnitz.
`[http://www.tu-chemnitz.de/misc/cusi.html]`

[5] Nicht nur Tips zur effektiven Suche, sondern auch Hinweise, wie die eigenen Seiten besser von anderen gefunden werden können, gibt

> Die Suchfibel.
> [http://www.suchfibel.de/]

3.4. Verantwortung für Inhalte

Die Verantwortung für den Inhalt von persönliche "Homepages" liegt bei den Autoren. Ein Autor einer Webseite hat die gleiche Verantwortung für den Wahrheitsgehalt der Inhalte wie ein Redakteur einer Zeitung. Damit ist klar, dass derjenige, der eine persönliche Homepage auf einem WWW-Server weltweit zugänglich machen möchte, wissen muss, was erlaubt ist und was nicht.

Der verbreitete Glaube vom Internet als "rechtsfreiem Raum" entbehrt jeder Grundlage. Die meisten rechtlichen Probleme lassen sich mit dem klassischen Gesetzeswerk durchaus lösen, und die Zahl der Präzedenzfälle steigt derzeit rapide an. Es sind keine speziellen "Internet-Gesetze" nötig, um beispielsweise die Verantwortung im Sinne des **Strafrechts** für eine WWW-Seite zu klären.

Natürlich gelten alle Gesetze auch für die Inhalte des Webservers. Das bedeutet insbesondere, dass Material, dessen Verbreitung verboten ist [1], auf einer Webseite nichts zu suchen hat. Dazu gehören beispielsweise rechts- oder linksradikale Propaganda, jugendgefährdende Schriften oder auch Aufforderungen zu gesetzeswidrigen Handlungen.

Halten Sie die Bestimmungen des **Urheberrechts** [2] penibel ein! Bilder von Lieblingsstars, Texte von Liedern oder gar komplette Audiodateien oder Videosequenzen dürfen nicht angeboten werden, wenn nicht zweifelsfrei belegt werden kann, dass die Materialien vom Autor für diesen Zweck freigegeben wurden. Allerdings sollte man, auch wenn man diese Genehmigung besitzt, sparsam mit Speicherplatz umgehen, weil Bandbreite noch immer ein knappes Gut ist. Das Urheberschutzrecht schließt selbstverständlich auch Software ein.

In diesem Rahmen sei auch das **Markenrecht** [3] erwähnt, welches die Verwendung von Produktbezeichnungen im geschäftlichen Verkehr regelt.

Ein weiterer wichtiger Punkt sind **Persönlichkeitsrechte**. Da das WWW ein Medium mit breiter Öffentlichkeit ist, dürfen private Informationen nur mit ausdrücklicher Erlaubnis des Betroffenen verbreitet werden. Beispielsweise ist eine Veröffentlichung privater E-Mails oder von Bildern, welche die Privatsphäre einer Person verletzen, verboten.

Der WWW-Server dient so wie das gesamte Campus-Netz dem Zweck von Forschung und Lehre. Es sollte klar sein, dass kommerzielle Angebote nicht geduldet werden können. Für diese Zwecke gibt es private Anbieter, die mehr oder weniger kostenlos Speicherplatz zur Verfügung stellen. Selbst die positive Erwähnung eines Produktes kann schon als Werbung angesehen werden.

Die Rechtsprechung entwickelt sich, und neue Urteile können Verpflichtungen für Web-Autoren nach sich ziehen. Schon aus diesem Grund bedürften Internet-Präsentationen einer Pflege. Als Beispiel sei ein Urteil des Landgerichts Hamburg vom

12. Mai 1998 (312 O 85/98 - "Haftung für Links") genannt. Demnach hat man durch die Anbringung eines Links die Inhalte der verlinkten Seiten mit zu verantworten, wenn man sich nicht ausdrücklich davon distanziert. Autoren von Linksammlungen, aber auch von anderen Seiten sind daher gut beraten, wenn sie einen entsprechenden Vermerk anbringen.

Ebenso besteht seit Anfang 2002 eine verschärfte Pflicht zur Anbringung eines Impressums, das zudem eine Reihe von Pflichtangaben enthalten muss. Die Gestaltung einer aktuellen WWW-Präsenz erfordert heutzutage mehr als "nur" HTML-Kenntnisse.

Bei Äußerungen zu diesem Thema empfiehlt sich ein "Disclaimer". So sei abschließend darauf hingewiesen, dass dieser Abschnitt weder eine Rechtsberatung darstellen noch vollständig sein kann.

Vertiefung:

[1]

Strafgesetzbuch
[http://dejure.org/gesetze/StGB/]

[2]

Urheberrechtsgesetz
[http://rechtliches.de/info_UrhG.html]

[3]

Das Markengesetz
[http://www.netlaw.de/gesetze/markeng.htm]

[4] Den Inhalt dieses Abschnittes finden Sie im Überblick auch in dem Artikel

Publizieren im WWW: Die rechtliche Seite
[http://www.tu-chemnitz.de/urz/www/recht.html]

Zur effektiven Nutzung des Netzes gehört auch, dass man die geeignetsten Möglichkeiten auswählt, wenn man mit anderen Personen in Kontakt treten möchte.

4

Kommunikation im Internet

4.1. NetNews - das Usenet

Schwarze Bretter des Internets

Über E-Mail verschicken Sie Ihre Texte immer an eine bestimmte Person oder eine begrenzte Personengruppe, wobei jedes Mitglied der Gruppe die Nachricht erhält. Wenn Sie jedoch eine Frage haben oder etwas verkaufen möchten, dann möchten Sie dies allen potentiellen Antwortenden bzw. Interessenten bekannt machen, auch wenn Sie sie gar nicht persönlich kennen. Andererseits möchten Sie Personen aus Ihrem Bekanntenkreis, die an der Frage bzw. dem Verkaufsobjekt möglicherweise kein Interesse haben, auch nicht damit belästigen. Zu diesem Zweck gibt es die **Newsgruppen (*Newsgroups*)**. Der Rechnerverbund, der dies anbietet, heißt **Usenet** und wird meist als Teil des Internets angesehen.

Sie können sich eine Newsgruppe wie ein schwarzes Brett vorstellen. Was Sie auf einen Zettel schreiben und an das Brett heften, kann jeder, der dieses Brett betrachtet, lesen. Er kann dann seine Antwort dazuschreiben, Ihnen persönlich antworten (Telefon, E-Mail, ...) oder natürlich Ihren Zettel einfach ignorieren.

So ein Zettel wird im Usenet **Posting** oder **Artikel** genannt. Die Tätigkeit, ihn zu veröffentlichen, heißt **posten**. Ein Posting sieht fast aus wie eine E-Mail, allerdings fehlt der Umschlag (Envelope), und statt einer "To:"-Zeile enthält es eine "Newsgroups:"-Zeile mit dem (den) Namen der Newsgruppe(n). Man benötigt ein spezielles Programm (**Newsreader**), um Artikel zu lesen und zu schreiben.

Normalerweise gibt es für jedes Thema eine geeignete Gruppe. Daher sollte ein Artikel auch nur in eine einzige Gruppe gepostet werden. Wenn Sie eine Nachricht gleich-

zeitig in mehrere Gruppen posten, spricht man von einem **Cross-Posting (X-Posting)**. Einige Leser werden einem Crossposting in jeder Gruppe erneut begegnen. Sie sollten daher beim Crossposten sehr zurückhaltend sein. In seltenen Fällen kann es gerechtfertigt sein, meist zeigt ein Cross-Posting aber nur, dass der Nutzer nicht in der Lage war, die richtige Gruppe zu finden. Zudem laden manche Newsreader Crosspostings in jeder betroffenen Gruppe erneut, so dass sie neben Unwillen auch noch Netzlast erzeugen.

Ein öffentliches Antwortposting auf einen Artikel wird **Follow-Up** genannt. Durch immer weitere Antworten entsteht eine Diskussion - ein **Thread**.

Gelegentlich kann es vorkommen, dass man nach dem Absenden eines Artikels feststellt, dass man beispielsweise etwas ganz Wichtiges vergessen hat oder das Posting in die falsche Gruppe geschickt wurde. Dafür bieten die meisten Programme eine Funktion zum Löschen (**cancel**) oder Ersetzen (**supersede**) des Artikels. Das ist natürlich kein Freibrief, unüberlegt Dinge zu schreiben, denn nicht jeder News-Server wird die Löschanweisungen auch weiterreichen. Das hat dann zur Folge, dass das falsche Posting noch einige Zeit im Usenet existiert.

Um Newsgruppen zu lesen und Nachrichten zu posten, verwendet man einen **Newsreader**. Das kann ein spezielles Programm sein, doch auch moderne Browser bieten entsprechende Komponenten.

Artikelverbreitung

Die Rechner, die das Usenet bilden und die Newsgruppen anbieten, heißen **News-Server**. Sie sind untereinander verknüpft und stehen in regelmäßiger Kommunikation. Wenn Sie nun ein Posting verfassen und Ihr Newsreader dieses an einen der News-Server schickt, wird Ihr Posting automatisch im Usenet weiterverteilt. Hierbei werden aber lokale Gegebenheiten beachtet, so werden zum Beispiel die Chemnitz-internen Newsgruppen nicht nach außen weitergereicht.

Das Weiterverteilen kann jedoch unter Umständen lange dauern. Die Reihenfolge, mit der Postings auf dem Rechner, von dem Sie Ihre News holen, ankommen, entspricht nicht zwingend der Reihenfolge, in der sie geschrieben wurden.

Die Newsreader sollten den nächstgelegenen News-Server, meist den des eigenen Providers, kontaktieren. Deswegen funktionieren News auch, wenn die Verbindung "nach außen" unterbrochen ist. Für die Nutzer der TU Chemnitz heißt der News-Server beispielsweise `news.tu-chemnitz.de`.

Newsgruppen

Es gibt derzeit vermutlich 50.000 bis 80.000 Newsgruppen weltweit. ("Vermutlich", weil viele Newsgruppen nur lokal in begrenzten Gebieten verfügbar sind und kein Rechner im Usenet alle Gruppen führt.) Würden diese Newsgruppen völlig unsortiert angeboten, fände sich niemand zurecht. Daher existiert eine nach Themen geordnete **Hierarchie der Newsgruppen**. Diese Hierarchie kann man sich wie einen Baum vorstellen. Zuerst kommen die dicken Zweige, also die grobe Auswahl, dann gliedert es sich immer feiner

auf. Man setzt dafür die jeweiligen Bereichsnamen mit Punkt getrennt hintereinander (z.B. `de.newusers.infos` oder `chemnitz.tu.urz`).

> *Im Gegensatz zu den Rechnernamen enthält bei den Newsgruppen also die erste Komponente die globale Information. Allerdings haben die Namen von Rechnern und Newsgruppen überhaupt nichts miteinander zu tun, nur ihre Notation ähnelt sich.*

Eine Auswahl an Bereichen:

Bereich	Beschreibung
comp	Computer- und Technik-Themen (international, englisch)
alt	Alternatives, alles was sonst nirgends hinpasst (international, englisch)
talk	Diskussions-Gruppen (international, englisch)
soc	Gesellschaftliche Themen (international, englisch)
sci	Wissenschaftliche Themen (international, englisch)
rec	Themen aus dem Unterhaltungsbereich (international, englisch)
de	deutschsprachige Newsgruppen (international)
chemnitz	Chemnitz-interne Themen (regional, deutsch)

Exemplarisch sollen nun einige Gruppen vorgestellt werden:

- `de.comp.os.ms-windows.misc` - Speziell für allgemeine Fragen zu Windows.

- `de.newusers.infos` - Diese Gruppe sollte jeder Neuling im deutschen Teil des Usenets zuerst lesen. Hier erscheinen regelmäßig einführende Texte und Erklärungen zum richtigen Verhalten in den Newsgruppen.
- `de.comp.os.unix.linux.newusers` - Für Einsteiger-Fragen zu Linux.
- `de.markt.*` - Hier gibt es mehrere Gruppen, die jeweils auf den An- und Verkauf verschiedener Dinge spezialisiert sind.

Prinzipiell gibt es für jedes Thema eine Gruppe. Das wird durch die Einrichtung von "`misc`"-Gruppen erreicht, die alles das aufnehmen, wofür in den anderen Gruppen der jeweiligen Hierarchieebene kein Platz ist.

Neben `de.comp.os.ms-windows.misc` gibt es z.B. noch `de.comp.os.ms-windows.nt` und `de.comp.os.ms-windows.programmer` für Themen, die sich mit Windows NT oder Programmierung unter Windows beschäftigen.

Für die Gruppen des Usenets existieren sogenannte **Chartas**, die Themengebiet und Aufgabe abgrenzen. In `de.newusers.infos` finden Sie Postings mit den Chartas der `de-`Gruppen. Postings, die nicht zum Thema einer Gruppe passen, werden als **Off-Topic** bezeichnet und rufen den Unwillen der Stammleser hervor.

Gelegentlich kann es vorkommen, dass sich das Thema einer Diskussion immer weiter vom eigentlichen Thema der Gruppe entfernt. In diesem Fall kann man alle weiteren Nachrichten des Threads in eine besser passende Gruppe umlenken. Dies geschieht, indem die `FollowUp-To`-Zeile passend gesetzt wird.

Unter `chemnitz.*` finden Sie Newsgruppen, die speziell für den Raum Chemnitz gedacht sind. Eine Übersicht zu diesem Angebot enthalten die

> Hinweise zur Benutzung der NetNews.
> `[http://www.tu-chemnitz.de/urz/netz/news.html]`

Netikette

Die im Kapitel zu E-Mail angesprochene **Netikette** gilt ebenfalls für die News. Es ist sogar noch viel bedeutsamer, sich an diese Regeln zu halten, weil man aufgrund des größeren Leserkreises schon mit sehr kleinen Fehlern viel mehr Unmut verursachen kann.

Im Gegensatz zu E-Mails ist die Verwendung der Anrede *Du* in den News üblich. Die Verwendung von *Sie* wird fast immer als Beleidigung angesehen. Natürlich gibt es von dieser Regelung auch Ausnahmen, wenn es sich beispielsweise um eine Newsgroup mit sehr begrenzter Leserschaft handelt und man eine Respektsperson ansprechen möchte.

Dieser eher kollegiale Umgangston sollte jedoch nicht mit einem Stammtisch verwechselt werden. Die Verwendung des kompletten Namens als Absender eines Postings ist im deutschsprachigen Usenet ein Muss. Pseudonyme oder Spitznamen werden nur in wenigen Ausnahmen toleriert.

Auch der Inhalt der Postings ist natürlich von Bedeutung. Illegale Inhalte zu verbreiten ist selbstverständlich auch im Usenet unter Strafe gestellt. Aber auch Werbung für Produkte und Dienstleistungen wird nicht gern gesehen, da das Usenet noch in großen Teilen an staatlich finanzierten Universitäten oder von gemeinnützigen Organisationen betrieben wird. Nicht zuletzt bedeutet der Name *News* soviel wie Neuigkeiten bzw. Nachrichten. Nichts ist unangenehmer, als eine Frage zum fünften oder zehnten Mal zu lesen. Daher hat es sich recht schnell etabliert, dass für Newsgruppen, die überwiegend beratende Funktionen haben, so genannte **Frequently Asked Questions (FAQ)**-Listen gepflegt werden, die alle regelmäßig gestellten Fragen beantworten. Die FAQs sind meist im WWW hinterlegt und werden auch in regulären Intervallen als Artikel in die Gruppen gepostet.

Schließlich ist auch die äußere Form entscheidend für die Beurteilung eines Postings durch die Leser. Neben der Anforderung, nur einfachen ASCII-Text zu verwenden, wird auch erwartet, dass eine Zeile nicht mehr als 80 Zeichen enthält. Das heißt, dass man eben auch keine Bilder oder Audio-Dateien per Newsgroup verbreiten sollte.

Oft findet man unter einem Posting oder einer Mail eine **Signatur**. Dort können zum einen persönliche Angaben stehen, soweit sie nicht im Header enthalten sind, zum anderen nutzen die Schreiber den Platz auch gern für ein wenig individuelle Charakterisierung – ein Spruch, eine minimale "‘Grafik"’ aus Buchstaben und Satzzeichen usw. Es ist Vorsicht angebracht: Was beim ersten Mal noch Interesse erweckt, ermüdet den Leser, wenn er es ständig wiedersieht. Eine Signatur soll prinzipiell mit zwei Minuszeichen gefolgt von einem Leerzeichen auf einer einzelnen Zeile vom Rest des Artikels abgetrennt werden, denn dann können sie Newsreader erkennen und beim Antworten auf ein Posting automatisch entfernen. Signaturen werden grundsätzlich nicht zitiert.

Nicht jeder Newsreader verhält sich konform zu diesen Regeln. Die Voreinstellungen von Outlook Express beispielsweise müssen auf jeden Fall angepasst werden, wenn Postings oder Mails nicht Anstoß erregen sollen. Wie man das macht steht auf verschiedenen Seiten im WWW, eine Seite speziell zu Outlook Express finden Sie bei den vertiefenden Links.

Besonderheiten

Einige (wenige) Gruppen sind **moderiert**. Alle dort erscheinenden Artikel werden von einem oder mehreren **Moderatoren** geprüft, bevor sie erscheinen. Das prominenteste Beispiel ist `de.newusers.infos`. Dadurch wird das sogenannte **Rauschen**, das Füllen einer Gruppe mit inhaltsarmen Artikeln, stark reduziert. Natürlich lassen sich so nur schwer Diskussionen durchführen. Wer über Artikel aus `de.newusers.infos` diskutieren möchte, muss das in `de.newusers.questions` tun.

Die Verfahrensweisen zu Anlage und Löschung von Gruppen unterscheiden sich von Hierarchie zu Hierarchie. Über die Gepflogenheiten unterhalb von `de` informieren die Texte in `de.newusers.infos`. Man muss recht lange im Usenet mitlesen, um die Argumente zu verstehen, die für oder gegen die Einrichtung neuer Gruppen sprechen.

Vertiefung:

Einleitende Informationen
`[http://www.boku.ac.at/news/newsd.html]`

Informationen und Ressourcen zu den deutschsprachigen Newsgruppen
`[http://www.rewi.hu-berlin.de/~gerlach/dni/]`

Microsoft Outlook Express: Häufig gestellte Fragen
`[http://oe-faq.de.vu/]`

4.2. Konferenzsysteme

Talk

Unter der Bezeichnung **Konferenzsysteme** wird eine Menge von Diensten zusammengefasst, die einer oder mehreren Personen die Kommunikation in Echtzeit ermöglichen.

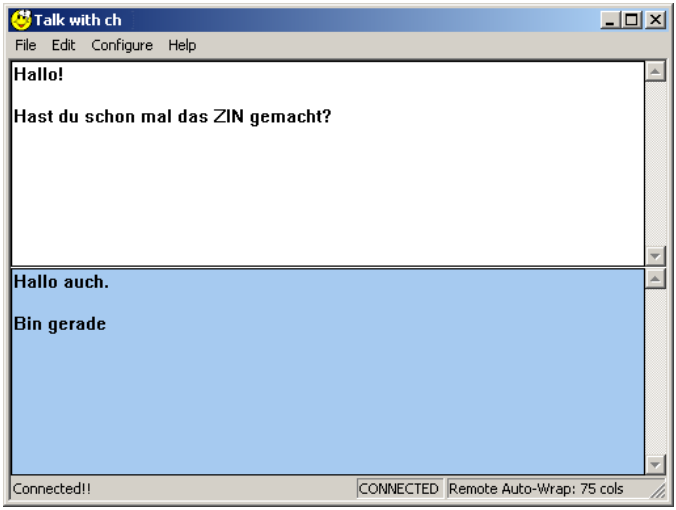
Eines der ersten Systeme war ein textbasiertes System mit dem Namen **talk**. Das Talk-Protokoll verbindet genau zwei Personen miteinander, die auf dem selben Rechner oder auf zwei verschiedenen Rechnern angemeldet sind. Talk ähnelt einem Telefongespräch. Nach dem Aufbau einer Verbindung sieht jeder Gesprächspartner jedes getippte Zeichen des anderen sofort auf seinem Bildschirm. Dazu wird der Bildschirm meistens horizontal geteilt. Im oberen Teil erscheinen die Antworten des Partners und im unteren der eigene Text.

Will man eine Talk-Verbindung starten, so gibt man an einer Kommandozeile den Befehl `talk` **Kennzeichen@Rechner** ein. Das Programm versucht dann, eine Verbindung aufzubauen. Sofern der Nutzer auf dem angegebenen Rechner angemeldet ist, erhält er in einer Kommandozeile eine Nachricht und ein akustisches Signal. Dies entspricht dem Telefonklingeln. Der "Angetalkte" sieht in etwa diese Meldung:

```
$

Message from Talk_Demon@vulkan
talk: connection requested by jtk@janus.hrz.tu-chemnitz.de
talk: respond with: talk jtk@janus.hrz.tu-chemnitz.de
```

Wenn der Partner die Verbindung akzeptiert (also den angegebenen Befehl eingibt), wird das Fenster in zwei Teile geteilt, und man kann miteinander kommunizieren.



Es existieren auch entsprechende grafische Versionen der Talk-Klienten und entsprechende Programme für MS-Windows. Im Bild sehen Sie ein Bildschirmfoto einer solchen Anwendung im Einsatz.

Einige Provider verwenden ein **Firewall**-System, welches bestimmte Datenpakete aus dem Internet nicht in das lokale Netz gelangen lässt. Dazu zählen meist auch die Pakete des Talk-Protokolls. Aus diesem Grund sowie auch wegen der internen Spezifik des Talk-Protokolls ist es aus einigen Netzen heraus nicht möglich, eine Talk-Verbindung zu einem beliebigen Rechner im Internet aufzubauen.

IRC

Ein weiteres Kommunikationssystem stellt der **Internet Relay Chat (IRC)** dar. Der IRC ist ein System, bei dem eine Kommunikation zwischen mehreren Personen gleichzeitig erfolgt. Dazu werden virtuelle Räume eingerichtet - auch Channels genannt. In diesen finden sich die Personen zusammen und führen verschiedenste Gespräche.

Im Gegensatz zum Talk werden beim IRC immer komplette Aussagen (Zeilen) übertragen. Diese werden an alle Mitglieder des Raumes gesendet. Da es bei mehreren Nutzern einer gewissen Ordnung bedarf, haben einige Nutzer erweiterte Rechte. Diese sogenannten **Channel-Operatoren** können beispielsweise Eigenschaften des Raumes festlegen oder auch andere Nutzer aus dem Raum entfernen oder gar aussperren. Da oft mehrere Tausend Nutzer gleichzeitig ein IRC-System verwenden, gibt es mehrere Server, die in einem Verbund arbeiten. Der bekannteste dieser Verbünde ist das **IRCnet**.

Im IRC ist es üblich, sich einen **Spitznamen (*Nickname*)** zu geben. Dieser Name bietet aber keine Anonymität! Es ist jederzeit feststellbar, auf welchem Rechner das Klientenprogramm arbeitet. Nicht zuletzt aus diesem Grund empfiehlt sich ein höflicher Umgangston. Es sollte keiner Erwähnung bedürfen, dass gesetzlich verbotene Inhalte auch im IRC nicht vorkommen dürfen. Viele Anbieter legen auch weitere Richtlinien fest. Dazu gehören beispielsweise die Beschränkung auf die Teilnahme mit nur mit einem Klienten pro Person oder das Verbot automatischer "Roboter". Diese Regeln sollte man sich sehr gründlich anschauen, um einen Ausschluss zu vermeiden, der aus administrativen Gründen schlimmstenfalls alle Nutzer der eigenen Domain trifft.

Es existieren noch mehrere Chat-Systeme mit ähnlicher Funktionalität. Oft findet man diese auch in Form von Java-Applets auf Webseiten. Für diese gelten natürlich die gleichen Hinweise wie für den IRC.

Instant Messengers

Eine weitere Gruppe von Kommunikationstools sind die **Instant Messengers**. Deren Kernfunktionalität besteht im Übertragen von einzelnen Textstückchen zwischen zwei Nutzern. Je nach Einstellung erscheint der Text direkt auf dem Bildschirm des Nutzers oder wird erst zwischengespeichert. Um Instant Messaging nutzen zu können, meldet sich der Nutzer an einer zentralen Datenbank an. Dieser Datenbank gibt er bekannt, ob er gerade vor dem Rechner sitzt oder nicht. Die Informationen aus dieser Datenbank stehen auch allen anderen Nutzern des Instant Messaging Netzwerkes zur Verfügung.

Daraus entsteht einer der Kritikpunkte an diesen Programmen: es können Profile erstellt werden, zu welcher Zeit der Nutzer am Rechner sitzt und wann nicht. Eine oft angebotene Zusatzfunktionalität stellt das Versenden von beliebigen Dateien dar. Auch an dieser Stelle ist Vorsicht geboten, denn es hat sich gezeigt, dass einige Programme Fehler enthielten, die es erlaubten, jede beliebige Datei von einem Nutzerrechner abzurufen.

Es existiert nicht nur ein Instant Messaging Netzwerk, sondern eine ganze Reihe. Zu den bekannteren zählen ICQ, der AOL-Instant-Messaging-Dienst und ein entsprechender Dienst von Microsoft. Für jedes dieser Systeme gibt es eine ganze Reihe von Klienten.

Telefon und Video

Es existieren auch Programme, die eine dem Telefon oder gar Bildtelefon ähnliche Funktionalität realisieren. Die Anforderungen an die Bandbreite übersteigen die für Textnachrichten allerdings um den Faktor 1000 oder gar eine Million. Während man mit in normalem Tempo geschriebenem Text ca. 30 Byte pro Sekunde erzeugen kann, benötigt Sprache zwischen 10 und 60 KByte und Video gar um die 3 MByte pro Sekunde! Üblicherweise sind Netzwerke nicht für eine so starke Belastung ausgelegt, so dass der Einsatz dieser Anwendungen zu einer starken Behinderung der anderen Nutzer führt.

Oft werden Sie gar nicht bemerken, ob ein Vorgang auf dem Prozessor Ihres eigenen Rechners oder ganz woanders abläuft. Um versehentlichen oder absichtlichen Missbrauch zu verhindern und bei Fehlern sinnvoll reagieren zu können, ist jedoch trotzdem ein wenig Hintergrundwissen nötig.

5 Weitere Netzdienste

5.1. Nutzung entfernter Rechner

Textbasiert

Seit es Netzwerke gibt, kann man sich an entfernten Rechnern anmelden (einloggen). Dies bedeutet, dass man mit Hilfe eines speziellen Programms eine Verbindung zu diesem Rechner herstellt und dann dort Programme ausführen kann. Der Grund dafür kann eine höhere Verarbeitungsleistung oder die Verfügbarkeit von speziellen Programmen auf diesem Rechner sein. Man nennt diese Rechner in diesem Fall oft **Compute-Server**. Grundsätzlich kann man sich auf jedem Unix-Rechner aus der Ferne einloggen, sofern dies nicht verboten wurde.

Frage 5.1.1:
Welche Gründe könnte es außer der Rechenleistung noch geben, sich auf einem entfernten Rechner anzumelden?

Zu diesem Zweck benutzt man Programme wie **telnet** oder **ssh** (abgeleitet von **secure shell**). Sie sollten telnet allerdings nur dann benutzen, wenn es sich gar nicht vermeiden lässt, da bei diesem Programm Sicherheitsprobleme bestehen. Wir empfehlen daher, immer ssh zu verwenden.

Beim Start der ssh gibt man den Namen des Zielrechners oder dessen IP-Adresse an, gegebenfalls auch noch das gewünschte Nutzerkennzeichen. Wurde der Rechner gefunden und wird der Dienst unterstützt, so erscheint dann üblicherweise die Frage nach dem Passwort.

```
$  ssh janus.hrz.tu-chemnitz.de
The authenticity of host 'janus.hrz.tu-chemnitz.de (134.109.132.79)' can't
be established.

DSA key fingerprint is 34:90:...:c6:30.
Are you sure you want to continue connecting (yes/no)?
```

In obigem Beispiel sieht man einen Ausnahmefall, der bei der Verwendung von ssh auftritt, sobald man sich das erste Mal auf einem entfernten Rechner einloggt. Der Nutzer wird aufgefordert, den ausgegebenen **key fingerprint** und damit die Identität des Zielrechners zu kontrollieren. Das ist notwendig, weil man im nächsten Schritt sein Passwort eingeben muss, welches nicht in fremde Hände fallen soll.

```
otto@janus.hrz.tu-chemnitz.de's password:
Last login: Tue Jul 30 2002 from herein.hrz.tu-chemnitz.de
[otto@janus otto]#
```

Nach der Eingabe des korrekten Passwortes erhält man eine Eingabeaufforderung, die auf dem entfernten Rechner ausgeführt wird. Darin kann man dann weitere Programme auf dem Rechner starten.

Kostenfreie Implementierungen von ssh-Klienten gibt es sowohl für Unix, als auch für Windows und MacOS.

Grafisch

Mit der Entwicklung grafischer Oberflächen kam auch der Wunsch auf, die Ausgaben grafischer Programme auf einen anderen Rechner weiterzuleiten. Auf Unix-Rechnern wird dazu ein System verwendet, welches von Beginn an auch für diese Zwecke gedacht war. Man nennt es **X**, häufig wird jedoch auch **X11** als Synonym verwendet. (Die 11 steht dabei für die Versionsnummer.)

X11 besteht aus zwei Teilen: dem eigentlichen Anwendungsprogramm und einem Programm, welches die grafische Ausgabe anzeigt. Diese beiden Programme können auf einem einzigen Rechner laufen, und das System unterscheidet sich dann nur wenig von MS Windows oder MacOS. Es ist aber auch möglich, die Anwendung auf einem entfernten Rechner zu starten. X11 sorgt dann dafür, dass die grafische Ausgabe über das Netzwerk zum eigenen Rechner geleitet wird und Eingaben von Maus und Tastatur wieder zurück zur Anwendung geschickt werden.

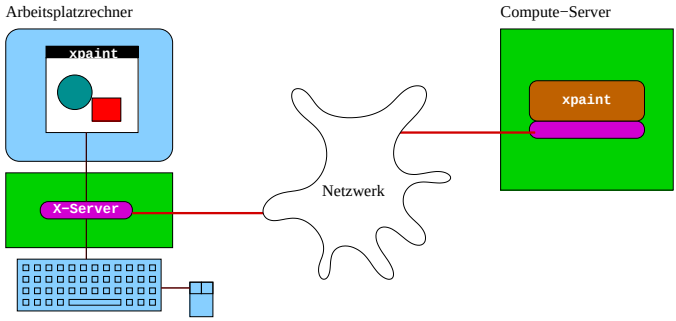


Abbildung 5.1-1.: Der X-Server stellt die Ausgabe eines auf einem entfernten Rechner laufenden Programmes auf dem lokalen Bildschirm dar.

Zwei Dinge sollten Ihnen bei der Verwendung der X-Weiterleitung aber bewusst sein:

1. Das Programm wird auf dem entfernten Rechner ausgeführt und benötigt dort Rechenzeit. Achten Sie darauf, keinen anderen Nutzer dadurch zu behindern.

2. Die Übertragung der Ein- und Ausgaben durch das Netzwerk benötigt Bandbreite. Starten Sie also nur solche Anwendungen auf entfernten Rechnern, die unbedingt notwendig sind.

Noch ein letzter Hinweis: Will man einen Windows-Rechner zur Anzeige von X-Programmen verwenden, so muss man auf diesem Rechner einen X-Server als Zusatzprogramm starten.

5.2. File Transfer Protocol (FTP)

Wenn Sie auf einem entfernten Rechner arbeiten und Ihnen kein Netzwerkfilesystem (siehe nächster Abschnitt) hilft, müssen Sie Ihre Daten mit einer anderen Methode zu diesem fremden Rechner transportieren. Eine Möglichkeit bietet das **File Transfer Protocol (FTP)**, eines der ältesten Protokolle im Internet überhaupt.

Da FTP seit langer Zeit existiert, gibt es eine Vielzahl von Programmen unter allen Betriebssystemen, die es Ihnen mehr oder weniger einfach ermöglichen, Daten zu oder von einem entfernten Rechner zu kopieren.

FTP bietet beispielsweise eine Möglichkeit, um Dateien von Ihrem privaten Rechner zu einem Rechner Ihres Providers zu schaffen. Es ist klar, dass Sie sich dann dort authentifizieren, also Nutzerkennzeichen und Paßwort nennen müssen. Leider wird das Passwort beim FTP nicht verschlüsselt übertragen, so dass auf die besseren Werkzeuge im ssh-Umfeld, hier das **Secure Copy (scp)**, hingewiesen sei.

Andererseits werden auch große Archive freier Software oder anderer allgemein zugänglicher Daten auf **FTP-Servern** abgelegt, auf die alle Nutzer zugreifen können. Dafür ist natürlich kein spezielles Nutzerkennzeichnen notwendig, so dass dieses Angebot

auch als **anonymous FTP** bezeichnet wird. Die meisten WWW-Browser können problemlos auf öffentliche FTP-Server zugreifen.

Es mag etwas verwirren, dass die Abkürzung FTP sowohl für das Protokoll, als auch für den Dienst und ebenfalls noch für das Programm steht. Bei den in den bisherigen Abschnitten behandelten Netzdiensten war das nicht so. Folgende Tabelle soll die Zuordnung von Transportprotokollen und Netzdiensten anhand ausgewählter Protokolle und Programme noch einmal verdeutlichen.

Dienst	**Protokoll**	**Bedeutung**	**Beispiel Programm**	**Pro-**
WWW	HTTP	Hypertext Transfer Protocol	Netscape	
FTP	FTP	File Transfer Protocol	ftp	
E-Mail Versand	SMTP	Simple Mail Transport Prot.	pine	
E-Mail Empfang	IMAP	Internet Mail Access Protocol	pine	
News (Usenet)	NNTP	Network News Transfer Prot.	slrn	

5.3. Netzwerkfilesysteme

In einem Rechnersystem mit vielen hundert Rechnern ist es unpraktisch, wenn die Dateien eines Nutzers nur auf einer Festplatte eines bestimmten Rechners gespeichert und nur von diesem Rechner aus verwendbar wären. Dies würde die Arbeit viel komplizierter machen und eine regelmäßige Datensicherung (Backup) erschweren. Auch ist es aufwändig, wenn Software auf jedem Rechner einzeln installiert werden müsste. Aus diesen Gründen hat man sogenannte **Netzwerkdateisysteme (*network file system*)** entwickelt.

Ziel dieser Entwicklungen war außerdem, dass der Zugriff auf Daten keine speziellen Programme oder Methoden benötigt. Der Nutzer soll von der Existenz von Netzfilesystemen nichts merken. Es gibt verschiedene konkurrierende Systeme. Das **Andrew File System (AFS)**, das **Network File System (NFS)** (welches dieser Gruppe von Diensten auch seinen Namen gab), das **Server Message Block System (SMB)**, sowie Novells **Netware** sind die am Häufigsten verwendeten Systeme.

Dank der Netzwerkfilesysteme finden die Nutzer auf allen Rechnern dasselbe **Homeverzeichnis** vor. Im Homeverzeichnis können die für die Arbeit benötigten Daten gelagert werden.

AFS

Am Beispiel von AFS lassen sich einige für die Nutzer interessante Eigenschaften moderner Filesysteme erläutern. Das Rechenzentrum der TU Chemnitz stellt die Homeverzeichnisse aller Nutzer sowie einen Teil der Anwendungssoftware via AFS bereit.

Das AFS besitzt sehr umfassende Sicherheitsmechanismen. Jedem Verzeichnis ist eine Liste von Nutzern und Gruppen zugeordnet, die verschiedene Operationen mit den

darin enthaltenen Dateien ausführen dürfen. Diese Listen nennt man **Access Control Lists (ACL)**. Außerdem sorgt ein spezieller Mechanismus dafür, dass kein Nutzer mehr Speicherplatz verwendet, als ihm zugeteilt wurde. Man spricht in diesem Zusammenhang von einer **Quota**.

Mit AFS lassen sich unkompliziert weitere Service-Dienste, wie beispielsweise ein tägliches Backup, aufbauen.

Das AFS ist ein sehr hoch entwickeltes System. Statt jede Datei auf genau einem Rechner abzuspeichern, werden mehrere Kopien jeder Datei angelegt. Dies erhöht die Geschwindigkeit und sorgt bei Ausfall eines Servers für schnellen Ersatz. Dieser Vorteil wird jedoch zum Nachteil, wenn sich eine Datei sehr oft ändert. Jede Änderung muss nämlich jedem der beteiligten Rechner mitgeteilt werden. Aus diesem Grund ist das AFS beispielsweise ungeeignet, um Bilder einer Kamera in kurzen Abständen aufzunehmen.

Alle Daten im AFS sind prinzipiell weltweit zugänglich. Im Verzeichnis `/afs/` befinden sich die Zugangspunkte zu allen AFS-Verzeichnisbäumen der Welt. Der Zugriff auf dieses Verzeichnis erfordert besondere Vorsicht, da man leicht erheblichen Netzwerkverkehr auslösen kann. Suchoperationen sind besonders gefährlich.

NFS

Das NFS, ein weiteres verbreitetes Netzwerkdateisystem, hat den Vorteil, dass es sich problemlos in existierende Unix-Dateisysteme eingliedern lässt, ohne den Nutzer etwas davon merken zu lassen.

NFS verfügt jedoch nur über sehr schwache Methoden der Authentifizierung. Dateien, die via NFS bereitgestellt werden, lassen sich also nur schwer gegen unerlaubte Zugriffe schützen. Einige NFS-Versionen besitzen zudem keinen lokalen **Cache** (Zwischenspeicher zum Beschleunigen häufiger Zugriffe).

SMB

Die Betriebssysteme von Microsoft verwenden das gemeinsam mit IBM entwickelte SMB-Filesystem. Um von einem Unix-Rechner auf freigegebene Daten eines Windows-Rechners zugreifen zu können, muss SMB jedoch auch auf dem Unix-Rechner verfügbar sein. Das Softwarepaket **Samba** stellt eine freie SMB-Implementierung für Unix-Rechner dar.

SMB ähnelt dem NFS. Für den Zugriff auf eine Datei muss man die Namen des SMB-Servers, der Freigabe und der Datei kennen. Als Freigabe bezeichnet man unter Windows Verzeichnisse, die im Netz auch für andere Nutzer zur Verfügung stehen. Die Datei wird dann in der Form `\\rechner\freigabe\pfad\dateiname` angesprochen.

Das Chemnitzer Uni-Rechenzentrum verwendet SMB, um Windows-Rechnern Zugriff auf das AFS zu ermöglichen, wenn diese keine AFS-Software installiert haben. Dazu existiert in jedem Subnetz ein Rechner mit dem Namen `sambaXXX`, wobei XXX die Nummer des Subnetzes angibt. Für das Subnetz 96 (V54 im CSN) lautet der Name zum Beispiel samba96.

Passwörter für die Anmeldung an einem Samba-Server werden oft unverschlüsselt übertragen. Dies stellt ein Sicherheitsrisiko dar. Daher sollte man auf SMB-Verzeichnisse nur aus sicheren Umgebungen wie der des Chemnitzer URZ zugreifen. Wenn Ihr SMB-Server die Möglichkeit bietet, ist natürlich eine verschlüsselte Übertragung zu bevorzugen.

Während NFS vorrangig für Unix-Nutzer und SMB vorrangig für Windows-Nutzer interessant ist, hat AFS für beide Welten Bedeutung.

5.4. Drucken im Netz

Werden auf relativ engem Raum sehr viele PC-Arbeitsplätze angeboten, ist es sehr ineffizient, wenn man an jeden Rechner einen eigenen Drucker anschließt. Der Drucker würde nur selten verwendet, Wartungsarbeiten benötigten viel Zeit, Kostenabrechnungen wären schwer möglich und bei Laserdruckern würde ungesundes Ozon den Anwender schädigen. Oft wird auch eine große Anzahl verschiedener Drucker (ein- oder doppelseitig, farbig oder schwarz-weiß, Folie oder Papier, A4 oder A3, ...) benötigt, die es für jeden Arbeitsplatz anzuschaffen oft nicht lohnt.

Die Lösung dieses Problems ist die Einrichtung eines zentralen Drucksystems. Die Druckaufträge werden in eine der Warteschlangen des Systems kopiert. Das Kopieren übers Netz und der Ausdruck von früher eingegangenen Aufträgen anderer Nutzer benötigen etwas Zeit, so dass man auf den eigenen Ausdruck möglicherweise etwas warten muss. Bei dem hier beschriebenen **Druckerspooling** wird jedem Drucker ein Name zugeordnet. Wenn man einen Ausdruck starten will, so muss man den Namen des Druckers angeben, auf dem der Ausdruck erfolgen soll. Das Drucksystem sorgt dann von selbst dafür, dass der Auftrag zum Drucker geschickt wird, die Druckkosten abgebucht werden und bei Fertigstellung des Druckauftrages eine E-Mail an den Auftraggeber gesendet wird, sofern der Nutzer das wünscht.

Drucker müssen die gesendeten Daten in die gewünschte Darstellung auf dem Papier umwandeln. Viele Drucker sprechen eine eigene "Sprache", und wenn man mit diesen Druckern arbeiten möchte, muss man die passenden Programme (Treiber) auf seinem Rechner haben. Glücklicherweise existiert ein Ausweg aus dieser misslichen Situation: Mit **PostScript (PS)** wurde eine Sprache entwickelt, die von einer ganzen Klasse von Druckern beherrscht wird. Damit kann ein einmal produziertes Dokument auf verschiedenen Druckern gedruckt werden, wenn diese postscriptfähig sind.

Wenn Sie sich Postscript-Dokumente auf dem Bildschirm ansehen wollen, benötigen Sie ein Programm, welches einen "Drucker für den Bildschirm" simuliert. Ein solches

Programm für verschiedene Betriebssysteme ist **ghostscript**.

Um nachvollziehen zu können, welcher Nutzer wie viel gedruckt hat und die daraus resultierenden Kosten ihm in Rechnung stellen zu können, wird ein **Druckkonto** geführt. Durch jede Druckausgabe wird das Konto, natürlich je nach Art des Druckers und Umfang des Druckauftrags unterschiedlich, belastet. Die Aufrechterhaltung eines umfangreichen Angebots an Druck-Dienstleistungen setzt allerdings sorgsamen Umgang mit den Ressourcen voraus.

Drucker werden für bestimmte Ausgabemengen konstruiert. Ein im Privatbereich zuverlässiger Tintenstrahldrucker wäre den Anforderungen als Netzwerkdrucker nicht gewachsen. Teure Hochleistungsdrucker würden sich hingegen an einem Privat-Arbeitsplatz nicht rentieren und stehen daher nur an zentralen Plätzen.

5.5. P2P Netzwerke

Peer-to-peer (P2P) Systeme arbeiten ohne zentrale Server, sondern auf der Basis gleichwertiger Partner (engl.: peers). Zu Bekanntheit gelangten die Systeme mit dem Programm namens *Napster*, welches mit dem Ziel entwickelt wurde, Musikdateien zwischen den Nutzern auszutauschen. Dabei stellen die Nutzer sich gegenseitig die Dateien zum Herunterladen zur Verfügung. Solche Systeme nennt man daher auch **Tauschbörse**. Mittlerweile gibt es eine ganze Reihe ähnlicher Projekte, die nicht nur Musikdateien, sondern jedes beliebige Dateiformat unterstützen. Bei der Nutzung dieser Tauschbörsen sind jedoch einige Dinge zu beachten.

Die heruntergeladenen Datenmengen können sehr schnell gewaltige Ausmaße annehmen. Das kann sowohl durch wenige große, als auch durchviele kleine Dateien verursacht werden. Dabei entsteht erheblicher Netzverkehr, der wie jeder andere Datentransfer Kosten verursacht. Da die P2P-Netzwerke auch darauf basieren, dass Nutzer ihrerseits Dateien anbieten, entsteht ein zweiter Datenstrom im Netz. Dieser Datenstrom ist noch schwieriger zu kontrollieren, da er von Dritten ausgelöst wird und nicht vom Nutzer selbst. Eine sorgfältige Konfiguration ist notwendig, damit nicht übermäßig große Datenmengen übertragen werden, die das Netzwerk unbenutzbar machen.

Der kritischste Punkt bei der Verwendung von P2P-Anwendungen ist jedoch das Urheberrecht. Dieses Recht schützt die Autoren von Texten, Bildern, Musik, Software und dergleichen. Es legt fest, dass es allein dem Autor zusteht, über die Verwertung und Verbreitung seines Werkes zu entscheiden. Es ist ebenfalls der Autor, der die Verwertungsrechte an Dritte übertragen kann. Bei Musikstücken ist diese dritte Person beispielsweise ein Musikverlag, der CDs mit den Werken herstellen darf. Das Urheberrechtsgesetz erlaubt für Privatpersonen die Herstellung von Kopien von erworbenen Medien für die private Nutzung. Eine Weiterverbreitung an eine potenziell unbegrenzt große Gruppe - wie den Nutzern von weltweiten P2P-Netzwerken - oder öffentliche Aufführung werden ausdrücklich untersagt. Die Grenzen zwischen privater Nutzung und Weiterverbreitung sind fließend und noch nicht abschließend festgelegt. Man sollte daher vor dem Anbieten von Dateien genau überlegen, ob man dazu auch berechtigt ist.

Bezieht man Programmdateien oder andere Dateien mit aktiven Inhalten aus den

Tauschbörsen, sollte man sich bewusst sein, dass die Dateien unter Umständen nicht das enthalten, was der Name verspricht. Es kann sich durchaus um Schadprogramme handeln, wie sie im Kapitel 6 beschrieben werden.

Als Nutzer sollte man außerdem sehr genau darauf achten, welche Teile des Verzeichnisbaumes für die anderen Nutzer des P2P-Netzes freigibt. Ist man nicht vorsichtig genug, passiert es schnell, dass jeder beliebige Nutzer in persönliche Dateien Einsicht erlangen kann.

Obwohl sich eine Information beliebig vervielfachen lässt, sind die Ressourcen zu ihrer Verbreitung begrenzt und müssen bezahlt werden. Eine effektive Nutzung kommt allen zugute, ohne dass die eigene Arbeit langsamer vonstatten geht.

6

Sinnvolle Ressourcennutzung

6.1. Zielorientierte Kommunikation

Den größten Erfolg erzielt man bei der Kommunikation, wenn man das richtige Medium wählt. Eine eilige Mitteilung an eine bestimmte Person würde man nicht per Anzeige in einer Monatszeitschrift übermitteln, sondern per Telegramm oder Anruf. Natürlich gilt auch im Netz, dass man das Medium wählen sollte, welches am Geeignetsten ist.

Die Entscheidung darüber, welches Medium geeignet ist, lässt sich sehr gut von seiner technischen Funktionsweise ableiten.

- Bei Verwendung von **Echtzeitkommunikation**, wie z.B. Instant-Messaging, Talk oder IRC, wird dem Empfänger die Nachricht unmittelbar und zeitnah zugestellt. Je nachdem, welches Programm der Nutzer verwendet, kann er dabei sogar in seiner aktuellen Arbeit unterbrochen werden, um die Nachricht angezeigt zu bekommen. Die Kommunikation erfolgt dabei üblicherweise zeilenorientiert, so dass keine großen Textmengen übertragen werden können. Diese Form der Kommunikation entspricht in etwa einem Telefonanruf. Folglich sind Themen, die für das Telefon geeignet sind, auch für diese Dienste prädestiniert.

- Eine **E-Mail** hat üblicherweise nur wenige Empfänger und wird relativ schnell zugestellt. Allerdings ist nicht gesichert, dass der Adressat die Mail auch sofort nach Zustellung auf seinem Mailboxserver liest, jedoch wird eine Mail üblicherweise so lange gespeichert, bis der Empfänger sie abruft. Aufgrund der technischen Realisierung ist der Schutz der Vertraulichkeit ohne weitere Vorkehrungen nicht sehr hoch. Aus diesen Merkmalen lässt sich das Einsatzgebiet von E-Mail

ableiten: Terminabsprachen oder Informationsaustausch zwischen wenigen Personen.

- Einen größeren Nutzerkreis spricht man bereits mit **Mailing-Listen** an. Technisch handelt es sich nach wie vor um E-Mails. Der Unterschied besteht jedoch darin, dass man eine viel größere und eventuell sogar anonyme Nutzergruppe ansprechen kann. Die meisten Mailing-Listen werden themenbezogen eingerichtet. Daher sollte man darauf achten, dass man auch nur zu dem entsprechenden Thema schreibt. Alles andere würde die Leser verärgern, weil die an die Liste gestellten Erwartungen nicht erfüllt werden würden.

- Eine nahezu unbegrenzt große Nutzergruppe erreicht man in den **News**. Daraus folgt die Regel, dass nur diejenigen Dinge in den News veröffentlicht werden sollten, die auch einen großen Teil der dort lesenden Menschen betreffen. Technisch bedingt werden die Artikel nur begrenzte Zeit auf dem News-Server bereitgehalten. Man kann sich daher nicht sicher sein, ob alle gewünschten Empfänger die Nachricht auch gelesen haben. Die News sind streng nach Themen geordnet und jede Gruppe hat genau ein ihr zugeordnetes Thema. Der wichtigste Grundsatz bei der Entscheidung für eine Gruppe ist: "Wo erwartet der Leser einen Artikel des von mir gewünschten Themas?". Denn genau diese Frage stellt sich der Leser auch, um nach für ihn interessanten Artikeln zu suchen. Die Gruppe nach der möglichen Leserschaft (z.B. "Da lesen sicher Informatiker. Die frage ich mal wegen meines Computerproblems.") auszuwählen, gilt als überaus unhöflich. Einige Beispiele:

  - Sie möchten wissen, welche Soundkarte in Ihrem Laptop den besten Klang liefert. In `de.sci.informatik.misc` wäre Ihr Posting am falschen Platz. Es bietet sich aber beispielsweise die Gruppe `comp.sys.laptops` an, wenn Sie Englisch schreiben und verstehen können.

- Sie wollen fragen, warum in der Uni bzw. im Wohnheim gerade irgendein Problem auftritt und wann das behoben sein wird. Diese Frage dürfte kaum Personen außerhalb Ihrer Stadt interessieren, geschweige denn von ihnen beantwortet werden können. Also wählen Sie eine lokale Gruppe, in Chemnitz z.B. eine der Hierarchie `chemnitz.*`. Bei Internet-Problemen eignen sich die Gruppen `chemnitz.tu.urz` oder `chemnitz.comp` und bei sonstigen Problemen die Gruppen `chemnitz.general` oder `chemnitz.tu.allgemein`.
- Sie wollen etwas verkaufen, zum Beispiel Ihren alten Rechner oder ein Fahrrad. Wer nicht in der gleichen Stadt lebt, wird kaum daran interessiert sein, wegen Ihres alten Rechners oder Fahrrads sehr weit zu fahren. Sie wenden sich also vorerst nur an Einheimische. Die geeignete Gruppe hierfür ist also eine lokale `markt`-Gruppe, z.B. `chemnitz.markt`. Sollte es aber ein sehr spezieller Rechner oder ein extrem teures und spezielles Fahrrad sein, sind die deutschlandweiten Gruppen in `de.markt.*` besser geeignet.

- **Webseiten** präsentieren Inhalte, die von einem Autor für eine bestimmte Zielgruppe erarbeitet wurden. Dabei schwankt die Veränderungshäufigkeit zwischen sehr selten (z.B. eine Webseite über physikalische Grundsätze) und extrem oft (z.B. aktueller Börsenticker). Gemeinsam ist allen, dass es sich um eine unidirektionale Kommunikation handelt, bei der der Empfänger üblicherweise nicht unmittelbar im Medium Kommentare anbringen kann. Aus diesem Grund hat man auch als Autor eine noch größere Sorgfaltspflicht beim Verfassen von Webseiten.

Natürlich sind die Grenzen fließend und nicht immer ist die Wahl des Mediums einfach. Sollte man unsicher sein, so hilft auch eine zurückhaltende Schreibweise, um mögliche Verstimmungen seitens der unfreiwilligen Leser etwas zu mildern.

6.2. Ressourcenbedarf verschiedener Anwendungen

Auch wenn es auf den ersten Blick nicht so aussieht: Die Ressourcen, die ein Rechenzentrum zur Verfügung stellt, sind knapp. Ein reibungsloser Betrieb setzt sparsamen Umgang voraus. Wichtige Kapazitäten sind Rechenleistung, Speicherplatz im Dateisystem und Netzbandbreite.

Rechenleistung

Auf Rechnern der Unix-Familie können mehrere Nutzer zugleich arbeiten. Sie melden sich dazu von einem anderen Rechner aus auf dem entsprechenden Server an. Der Nutzer kann nun jedes beliebige Programm auf dem entfernten Rechner starten.

Diese Technik macht man sich zunutze, um große Rechenleistung vielen Nutzern zur Verfügung zu stellen. Die dafür eingesetzten Rechner nennt man **Compute-Server**. Seit einiger Zeit gibt es immer wieder ehrgeizige Projekte, die schwierige numerische Aufgaben lösen wollen. Deren Herangehensweise besteht darin, die Aufgabe in kleine Portionen zu teilen, um diese dann von sehr vielen Rechnern rechnen zu lassen. Die Versuchung liegt nahe, die Compute-Server für diese Aufgaben zu verwenden, da diese gelegentlich nicht voll ausgelastet erscheinen. Die Ressource "Rechenzeit" kostet jedoch ebenfalls Geld und kann nicht kostenlos anderen Organisationen oder Personen "geschenkt" werden. Zudem behindert man damit Nutzer, die sich anmelden wollen oder ihrerseits große Rechnungen im Rahmen des Studiums oder der Forschung durchführen müssen. Weiterhin verursacht man höheren Verschleiß bei den betreffenden Systemen. Natürlich steht es jedem Nutzer frei, die Leistung seines privaten Rechners auf diese Weise anderen zur Verfügung zu stellen.

Auch Arbeitsplatzrechner erlauben es, sich per Netz einzuloggen. Dadurch werden kleinere Wartungsarbeiten oder kurze Tests ermöglicht. Keinesfalls dürfen Poolrechner jedoch aus der Entfernung für größere Aufgaben verwendet werden. Sie sind sogar so konfiguriert, dass ab einem gewissen Anteil benötigter Rechenleistung die Prozesse von über das Netz angemeldeten Nutzern automatisch abgebrochen werden.

Falls man Programme auf einem entfernten Rechner startet, so sollte man darauf achten, dass die Programme auch beendet werden, wenn man die Verbindung beendet.

Speicherplatz im Dateisystem

Damit nicht jeder Nutzer unbeschränkt viel Speicherplatz verwendet, wird für die Home-Verzeichnisse eine sogenannte **Quota** festgelegt, die den maximalen Speicherplatz bestimmt, den die Dateien eines Nutzers einnehmen dürfen. Die Höhe und eventuelle Erhöhungsmöglichkeiten legt dabei die jeweilige Institution fest. Es versteht sich von selbst, daß man nicht mehr benötigte Dateien löscht.

Netzbandbreite

Besonders sorgsam muss mit der Netzbandbreite umgegangen werden, da diese von allen Nutzern geteilt wird und auch am Teuersten ist. Ein Netz wird für ein bestimmte Anwendungsszenario ausgelegt. In einer Universität bedeutet das beispielsweise Netzwerkdateisysteme, entfernte Rechnernutzung, Mailversand, gemäßigtes Surfen im Netz und andere Dienste mit geringen Anforderungen. Nicht geeignet ist es zumeist für riesige Datentransfers, Echtzeitübertragungen von Videos oder Klang sowie dem Senden von sehr großen Mengen an Mails. Im Folgenden soll kurz auf die Anforderungen eingegangen werden, die verschiedene Anwendungen stellen.

Zugang zu entfernten Rechnern

Netzbandbreite für den Zugang zu einem entfernten Rechner wird einerseits für die Eingaben des Nutzers auf diesem Rechner und andererseits für die Ausgaben der auf dem Rechner laufenden Programme benötigt. Bei normaler Schreibgeschwindigkeit schafft ein Nutzer etwa 200 Zeichen pro Minute. Um das zu übertragen, ist eine Bandbreite von etwa 30 Bit/s nötig. Wenn es sich bei der Ausgabe um normale Textanwendungen handelt, dann wird auch da eine Kapazität von wenigen Kilobit pro Sekunde ausreichend sein.

Erheblich mehr Daten sind zu übertragen, wenn es sich um grafische Ausgaben handelt, wie sie vom X11-Protokoll erzeugt werden. Schnell werden mehrere hundert KiloBit/s benötigt. Dieses System sollte daher nur sehr sparsam verwendet werden. Unerwünscht ist die Verwendung, wenn ähnliche Dienste auch durch lokal verfügbare Software realisiert werden können.

Mail und News

E-Mails und Postings mit einfachem Text als Inhalt verursachen auch keine große Netzbelastung. Anders verhält es sich, wenn Dateien an die Mails angehängt werden. In diesem Falle können die Mails schnell sehr groß werden. Die meisten Infrastrukturbetreiber legen eine Grenze fest, ab der Mails nicht mehr weitergeleitet werden. Dies sind oft einige MegaByte, allerdings sollten schon Mails ab einer Größe von ca. 250 KByte mit dem Empfänger abgesprochen werden, da man nie weiß, welche Kosten der Empfänger für den Empfang der Daten zu tragen hat.

Etwas anders sieht es bei News aus. Hier sollte ausschließlich Text versendet werden. Dies ist einerseits der andersartigen Verteilungsweise und andererseits der großen Diversität der entsprechenden News-Reader geschuldet. Binär-Dateien - darunter versteht man alle Dateien, die nicht reinen Text im ASCII-Format enthalten, also z.B. Bilder oder Audio-Dateien - dürfen generell nur in extra dafür ausgewiesene Gruppen gepostet werden. Um Bandbreite zu sparen, ist der Zugriff auf News-Server außerhalb des jeweiligen Intranets meist gesperrt oder stark eingeschränkt.

Um das übertragene Datenvolumen möglichst gering zu halten, sollte beim Zitieren (Quoten) von E-Mails bzw. Postings darauf geachtet werden, nur die für das Verständnis

notwendigen Abschnitte in der eigenen Antwort mitzusenden.

WWW und FTP

Diese beiden Anwendungen verursachen einen großen Teil des Datenverkehrs. Aus diesem Grund muss besonders sparsam damit umgegangen werden. Nicht notwendige Datenübertragungen sollten unterlassen werden. Um die Kapazität der Verbindungen zu schonen, kann man mehrere Caches verwenden. Bei sehr langsamen Verbindungen wirkt es oft beschleunigend, wenn man das Laden von Bildern deaktiviert. In diesen Situationen merkt man, wieviel Bandbreite eigentlich für die Bilder benötigt wird.

Bei FTP-Übertragungen sollte vorher überprüft werden, ob vielleicht eine lokale Kopie der gewünschten Daten auf einem Server im Intranet oder zumindest in Deutschland verfügbar ist. Um dies herauszufinden, gibt es entsprechende Suchsysteme.

Filesharing-Anwendungen

Besonders umsichtig muss man bei der Nutzung von Filesharing-Anwendungen vorgehen. Dass bei der Nutzung das Urheberrecht einzuhalten ist, muss nicht extra betont werden. Diese Protokolle können jedoch enorme Mengen an Bandbreite benötigen. Für den Nutzer besteht kaum eine Möglichkeit, Einfluss darauf zu nehmen, woher die Daten bezogen werden. Es ist nicht unwahrscheinlich, dass die Daten von außerhalb des eigenen Netzwerkes angefordert werden und dadurch Kosten verursachen. Da die Dateien oft auch sehr groß sind, sperren oder beschränken einige Rechenzentren deshalb diese Dienste. Für alle Beteiligten vorteilhafter ist jedoch eine sparsame Nutzung, so dass entsprechende beschränkende Maßnahmen nicht notwendig sind.

Konferenzsysteme

Textbasierte Konferenzsysteme wie IRC und Talk verursachen kaum Netzlast. Allerdings ist es in den öffentlichen Pools nicht erwünscht, die Rechner durch "chatten" zu blockieren.

Für Konferenzsysteme, welche auf Audio- oder gar Videobasis arbeiten, ist selbst das Campusnetz einer Uni nur unter Einhaltung bestimmter Rahmenbedingungen geeignet. Die entstehenden Datenmengen sind so groß, daß ein erheblicher Teil der Gesamtkapazität allein für eine einzige Verbindung notwendig wäre. Aus diesem Grund bedarf diese Form der Kommunikation einer vorherigen Absprache mit den zuständigen Netzwerk-Administratoren.

Ähnlich hohe Anforderungen stellen übrigens auch Audio- oder Video-Streaming-Systeme, welche oft nur Unterhaltungsinhalte transportieren. Allerdings setzen immer mehr Anbieter auf eine Technologie namens **Multicast**. Dabei wird der Datenstrom nur ein einziges mal in das lokale Netzwerk geholt und dann dort verteilt. Damit kann erheblich Bandbreite gespart werden, so dass - falls die Übertragung unabdingbar ist - möglichst Multicast verwendet werden sollte.

Vertiefung:

WWW-FTP-Archivbrowser
[http://www.tu-chemnitz.de/urz/netz/ftp.html]

6.3. Caches und Proxies

In einer großen Einrichtung werden viele WWW-Seiten von mehreren Nutzern angeschaut (beispielsweise die aktuelle Tageszeitung im Netz). Da die Bandbreite des Anschlusses an das Internet beschränkt ist und Geld kostet, werden oft angeforderte Seiten im lokalen Netz zwischengespeichert und bei einer Anfrage nicht erneut von außerhalb geholt. Einen Rechner, der diese Aufgabe bewältigt, nennt man **Proxy-Cache**. Es ist ein angenehmer Nebeneffekt, dass der Proxy diese Seiten oft schneller liefern kann, da sie sich bereits im (schnellen) lokalen Netz befinden. Übrigens verwenden auch viele WWW-Browser selbst schon lokale Caches, welche die Cache-Server jedoch nicht ersetzen, da lokale Caches nur von einem Nutzer verwendet werden und der Vorteil des Zugriffes durch viele Nutzer nicht gegeben wäre.

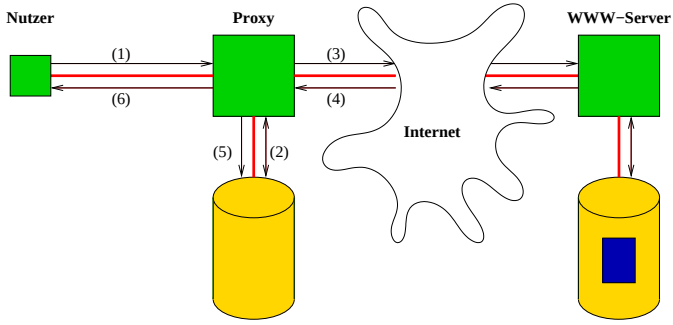


Abbildung 6.3-1.: Proxy bei Cache-Miss

In obiger Abbildung wird der Fall des Cache-Miss dargestellt, d.h. eine Seite wird angefordert (1), die noch nicht im Cache gespeichert ist (2). Der Proxy-Server greift dann auf den WWW-Server zu (3). Nachdem er die Seite erhalten hat (4), legt er eine Kopie in seinem Cache ab (5) und gibt die Seite an den Klient (6) weiter.

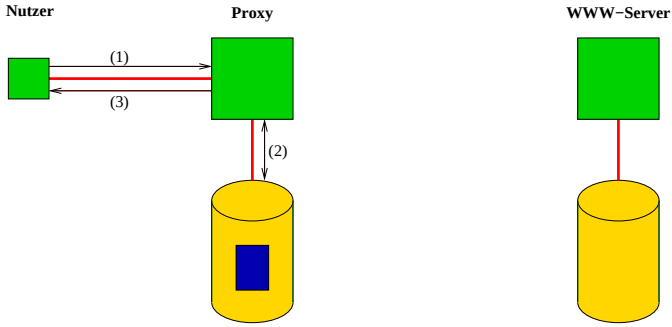


Abbildung 6.3-2.: Proxy bei Cache-Hit

Nun ruft ein zweiter Nutzer dieselbe Seite ab (1). Der Proxy stellt jedoch fest, dass er die Seite bereits im Cache hat (2). Diesen Fall bezeichnet man als Cache-Hit. Anstatt nun noch einmal auf den WWW-Server zuzugreifen, liefert er die Seite direkt aus seinem Cache an den Nutzer aus (3).

Damit dieser Vorteil genutzt werden kann, muss dem WWW-Browser mitgeteilt werden, dass er einen Proxy-Cache verwenden soll. Dies geschieht meistens in einem entsprechenden Konfigurationsdialog. Die Nutzer sollten deshalb die Einstellungen ihres Browsers daraufhin kontrollieren.

Frage 6.3.1:
Manche Seiten werden nicht im Cache gespeichert. Kennen Sie Fälle, in denen eine Zwischenspeicherung nicht sinnvoll ist?

Der Einsatz von Proxy-Cache-Servern kann die Netzbelastung durch WWW-Surfer deutlich senken. Daneben können aber auch die Nutzer selbst durch sinnvolles Verhalten erheblich zur Entspannung beitragen, ohne auf Netzangebote verzichten zu müssen:

Möglichst lokale Dienste nutzen

Die Datenübertragung innerhalb des Intranets ist viel billiger als der Zugriff auf Dienste außerhalb. Häufig genutzte Online-Dokumentationen und FTP-Archive werden deshalb von Rechenzentren als Kopie bereitgestellt (man sagt auch **Spiegel (*Mirror*)** dazu). Wer diese lokalen Kopien nutzt, spart Bandbreite und wird durc kürzere Übertragungszeiten belohnt.

Große Datenübertragungen in Zeiten geringer Netzbelastung auslösen

Nachts wird das Netz weniger interaktiv benutzt. Wird ein größerer Datendurchsatz benötigt, so stört das dann weniger Nutzer. Oft ist die Übertragung wegen der geringeren Auslastung nachts auch schneller. Für die Dateiübertragung per FTP gibt es sogar Roboter, die diese Aufgabe erledigen. (Wer schon einmal

größere Datenmengen von amerikanischen Servern holen wollte, weiß, dass die günstigste Zeit außerhalb der üblichen Arbeitszeit in *beiden* Zeitzonen liegt.)

Kein "wildes Herumklicken"

Auf der Suche nach bestimmten Informationen, hilft zielloses Abrufen beliebiger Seiten kaum. Es erzeugt lediglich nutzlosen Datentransfer, der Kosten verursacht und andere Nutzer behindert. Ein paar Überlegungen, wo man selbst die gesuchte Information unterbringen würde und der gezielte Einsatz entsprechender Suchsysteme führen schneller und mit weniger Aufwand zum Ziel.

Bandbreite sparen

Die heutige Technik eignet sich für Video- und Audioübertragungen nur bedingt. Daher sollte man sich vor jedem Download überlegen, ob die angeforderten Daten wirklich den gewünschten Nutzen bringen. Das gilt besonders für Live-Video- und Live-Audioübertragungen, die eine hohe Bandbreite benötigen.

Vertiefung:

Die Proxy-Konfiguration einiger Browser speziell für Nutzer der TU Chemnitz:
`[http://www.tu-chemnitz.de/urz/www/proxy/]`

6.4. Datensicherheit

Jeder Nutzer möchte seine Daten schützen:

1. *vor versehentlichem Verlust,*
2. *vor unerwünschtem Zugriff (Vertraulichkeit),*
3. *vor unerwünschter Manipulation (Integrität).*

Den ersten Punkt löst man z.B. durch Backups oder Redundanz. Das ist nicht Gegenstand dieses Kurses.

Die anderen beiden Punkte gewinnen enorm an Bedeutung, sobald man nicht mehr auf einem einzeln stehenden Rechner sondern im und mit dem Netz arbeitet. Die Nutzer sind dabei in hohem Maße mit verantwortlich für Integrität und Vertraulichkeit ihrer Daten. Der Betreiber der Infrastruktur kann nur die nötigen Werkzeuge bereitstellen und die Sicherheit der Rechner und Netze überwachen.

Der Provider ist z.B. nicht verantwortlich, wenn ein Nutzer seinen Rechner verlässt, ohne den Bildschirm zu sperren oder sein Passwort weitergibt.

Um gezielt anderen Nutzern auf die eigenen Dateien Zugriff gewähren zu können, muss man diese erst einmal erkennen. Das geschieht durch den Account. Als **Account** bezeichnet man die Zugangsberechtigung zu einem Computer oder Computersystem. Zum Account gehören **Nutzerkennzeichen** - auch **login** genannt - und **Passwort**. Wenn ein Nutzer seine Identität nachweist, also zeigt, dass er "der Richtige" ist (z.B. beim Anmelden an einem Rechner), nennt man das auch **Authentifizieren**.

Der Nutzer kann die **Datensicherheit** auf verschiedenen Stufen beeinflussen.

Im Rechner selbst

Moderne Betriebssysteme erlauben mehreren Nutzern, das **Filesystem** gemeinsam zu nutzen. Bei einem Netzwerkfilesystem haben theoretisch sogar alle Nutzer die Möglichkeit, alle Dateien zu erreichen. Damit nun nicht jeder in den Dateien anderer Personen wahllos lesen und schreiben kann, gibt es **Dateirechte**. Diese legen fest, welcher Nutzer welche Dinge mit welcher Datei tun darf.

Viele aktuelle Unix-Filesysteme kennen drei Arten von Zugriffen: Lesen (r), Schreiben (w) und Ausführen bzw. Betreten (x). Zu jeder Datei und jedem Verzeichnis werden diese Informationen mitgeführt. Diese Rechte kann man sich z.B. durch das Kommando ls mit der Option -l anzeigen lassen.

```
$  ls -l
-rw-r--r--  1 otto  users  4323 Aug 16 14:28 index.html
drwxr-xr-x  2 otto  users  2048 Aug 17 12:10 kap1
$
```

Dieses Beispiel zeigt eine solche Ausgabe. Die erste Spalte macht eine Aussage über den Typ des Objekts, das `d` steht für Directory. Hinter `kap1` verbirgt sich also ein Verzeichnis. Die Dateirechte sind in drei Gruppen eingeteilt. Die nächsten drei Stellen geben an, welche Rechte der Inhaber der Datei (otto) hat. Dann folgen je drei Stellen für die Nutzergruppe (users) und alle übrigen Nutzer. Auf die Details soll hier nicht weiter eingegangen werden. In den URZ-Einführungskursen zu Unix kann man sich gegebenenfalls weiter informieren [2].

Im **AFS** sind von den klassischen Dateirechten nur noch die Angaben für den Besitzer der Datei von Bedeutung. Die Zugriffsbeschränkungen für andere Nutzer werden durch das verteilte Filesystem kontrolliert. Die **Access Control Lists (ACL)** wurden bereits im Abschnitt 5.3 kurz erwähnt. Mit dem Kommando `fs la .` (UNIX) oder mit dem Kontextmenü `AFS: Access Control Lists` (Windows) kann man sich für das aktuelle Verzeichnis die ACLs anzeigen lassen. Die Ausgabe erfolgt als Liste von Nutzern oder Nutzergruppen zusammen mit den entsprechenden Rechten. Die Festlegung der Rechte ist sehr gezielt möglich. Die folgenden Operationen können bei einem Verzeichnis durch ACLs gesteuert werden:

r	Lesen des Inhalts der enthaltenen Dateien
l	Anzeigen der Namen der Dateien
i	Anlegen neuer Dateien
w	Schreiben in existierende Dateien
d	Löschen von Dateien oder Unterverzeichnissen
k	Anfordern von exklusivem Zugriff für ein Programm
a	Ändern der ACL

```
$  fs la .
Access list for . is
Normal rights:
  otto rlidwka
  www-server rl
  system:anyuser rl
  zin-autoren rlidwk
```

Im diesem Beispiel der Ausgabe von "fs la ." besitzt der Nutzer `otto` alle Rechte (die Kombination aller möglichen Operationen - `rlidwka`), die Gruppe aller Nutzer (`system:anyuser`) und der `www-server` dürfen nur lesend zugreifen (Lesen und Dateien auflisten - `rl`), die Gruppe der ZIN-Autoren darf sowohl die Dateien im Verzeichnis lesen als auch schreiben.

Das in Windows NT und seinen Nachfolgern eingesetzte Dateisystem *NTFS* besitzt ebenfalls ACLs, die in ihrer Funktionalität denen des AFS sehr ähnlich sind. Im Gegensatz zum AFS sind sogar pro Datei individuelle Zugriffsrechte einstellbar.

Mancherorts - wie z.B. auch im CSN - kann man seinen Rechner in eine sogenannte **NT-Domäne** einbinden. Damit kann man sich und andere Nutzer innerhalb dieser Gruppen authentifizieren. Ein erhebliches Sicherheitsrisiko entsteht aber dadurch, dass dem Domänen-Administrator per Vorgabeeinstellung uneingeschränkte Zugriffsrechte auf jeden in der Domäne eingetragenen Rechner gewährt werden. Sehr gute Kenntnisse sind erforderlich, um diese Rechte wirksam einschränken zu können. Aus diesem Grund wird das Domänenkonzept oftmals nicht unterstützt. Statt dessen kommt eine abgeschwächte Form mit der Bezeichnung **Arbeitsgruppe** zum Einsatz, die eine ähnliche Funktionalität bietet.

Während der Übertragung

Ein großes Sicherheitsrisiko existiert, wenn man Daten über das Netz überträgt. Es existieren verschiedene Programme, die jeden Datentransfer im Netz "belauschen". Selbstverständlich ist eine Aufzeichnung der übertragenen Daten illegal und wird entsprechend geahndet, jedoch hält eine Strafandrohung nicht alle potentiellen Täter davon ab. Als Anwender sollte man sich stets dessen bewusst sein. Besonders Passwörter sind oft das Ziel

dieser Angriffe, da mit diesen jederzeit die Identität des Nutzers angenommen werden kann. Einige Programme übertragen das Passwort in einer sehr leicht entschlüsselbaren Form. Diese Programme sollte man möglichst nie oder nur sehr selten verwenden. Dazu zählen:

- Personenbezogenes FTP (mit Nutzername und Passwort)
- Entfernte Rechnernutzung mit dem ssh-Vorgänger telnet
- Mailboxzugriff mittels unverschlüsseltem POP oder IMAP
- Die Dateifreigabe von Windows (auch als Samba bezeichnet)

Für die meisten dieser Dienste gibt es Alternativen, welche das Passwort und andere übertragene Daten verschlüsseln.

Die Funktionalität von FTP kann z.T. mit dem Kommando **Secure Copy** erbracht werden [3]. Die meisten Mail-Klienten ermöglichen die Verschlüsselung des IMAP- oder POP-Datenstroms mittels **Secure Sockets Layer (SSL)**.

SSL wird auch immer dann verwendet, wenn es darum geht, die Daten einer HTTP-Verbindung vor Manipulation und Ausspähen zu schützen. Die Verwendung von HTTP mit SSL erkennt man daran, dass der URL mit `https` beginnt. Die meisten Browser zeigen die Verwendung von HTTPS mit einem kleinen Symbol in Form eines Schlüssels oder Schlosses auch stilisiert an. Wann immer WWW-Seiten Kennworte oder sonstige vertrauliche Informationen anfordern, sollte man unbedingt HTTPS verwenden. Beim Verwenden von HTTPS kommt es gelegentlich vor, dass der Browser wegen unbekannter **Zertifikate** Rückfragen stellt. Die Zertifikate stellen wie die Fingerprints bei ssh sicher, dass der Server wirklich derjenige ist, der er behauptet zu sein. Im Gegensatz zu ssh, wo man die Fingerprints aus einer alternativen Quelle beschaffen muss, verwendet man bei SSL eine Hierarchie von Bestätigungen. Ein Zertifikat wird von einem anderen Zertifikat bestätigt, bis eines der Zertifikate von einer *vertrauenswürdigen Institution* ausgestellt wurde. Wem in diesem Sinne Vertrauen ausgesprochen wird, ist in den meisten Browsern fest eingebaut.

Besondere Vorsicht ist geboten, wenn man an "fremden" Internetzugängen arbeiten möchte, beispielsweise auf Tagungen und Konferenzen oder in Internet-Cafés. Der Weg der Datenpakete kann dann kaum kontrolliert werden, und die Verwendung von nicht verschlüsselnden Diensten stellt ein echtes Sicherheitsrisiko dar.

Von vielen Herstellern werden mittlerweile Zusatzprogramme unter dem Schlagwort **Personal Firewall** angeboten. Es handelt sich dabei zumeist um Programme, die den Datenverkehr des eigenen Rechners überwachen und dabei jedes einzelne Datenpaket inspizieren. Dem Nutzer obliegt es nun, bestimmte Regeln festzulegen, welche Datenpakete als gefährlich anzusehen sind und welche nicht. Da diese Einstellungen recht schwierig zu treffen sind, gibt es oft schon vorgefertigte Regeln. In Abhängigkeit dieser Regeln wird dann das Programm den Nutzer über die Sichtung entsprechender Pakete informieren und diese gegebenenfalls nicht weiterleiten. Dieses Verfahren hat aber zwei erhebliche Nachteile. Ein Anwender, der nicht genau weiß, nach welchen Kriterien er die Gefährlichkeit bestimmter Datenpakete bewerten soll, sorgt durch übereifrige

Sperrungen für Störungen im Netzbetrieb. Außerdem können normale Betriebszustände fälschlicherweise als Angriff gewertet werden und dadurch ohne wirkliche Notwendigkeit Beschuldigungen ausgesprochen werden, die sich am Ende als haltlos erweisen.

Meist werden große Netzwerke durch eine richtige Firewall geschützt, die von professionellen Administratoren betrieben wird. Für die Arbeitsplätze der Nutzer gilt dann die Regel, dass der beste Schutz darin besteht, nur die Dienste anzubieten, die wirklich zwingend notwendig sind. Diese Dienste müssen dann sorgfältig konfiguriert und die Programme stets aktuell gehalten werden.

Durch den Nutzer selbst

Generell gilt, dass der Nutzer für alles verantwortlich ist, was unter seinem Account gemacht wird. Um Missbrauch zu vermeiden, sind folgende Regeln einzuhalten:

- Niemals das Passwort weitergeben: Ein Passwort ist wie die PIN einer Kredit-Karte!
- Beim kurzzeitigen Verlassen des Rechners den Bildschirm sperren!
- Beim endgültigen Verlassen des Rechners abmelden!
- Sichere Passwörter wählen und regelmäßig das Passwort ändern, da es Programme gibt, die unsichere Passwörter mittels gewaltiger "Wörterbücher" erraten können. Manche dieser Programme probieren auch alle möglichen Passwörter durch. Aus diesem Grund sollte das Passwort aus nicht zu wenigen Zeichen bestehen und und regelmäßig geändert werden. Meist gibt das jeweilige Rechenzentrum Hinweise oder gar Anweisungen, wie oft das zu erfolgen hat.

Namen, Geburtsdaten oder Wörter aus dem Duden sind natürlich keine guten Passwörter. Statt dessen kann man sich z.B. einen Satz ausdenken und dessen Anfangsbuchstaben verwenden. Ein Beispiel für ein gutes Passwort wäre: "*D7sKtgbM.*" (**D**ie sieben (**7**) **s**chwarzen **K**ätzchen **t**rinken **g**ern **b**laue **M**ilch**.**) Wichtig bei Passwörtern ist, dass sie Sonderzeichen (Punkt, Komma, Ausrufungszeichen, ...), Ziffern und große und kleine Buchstaben enthalten. Kürzer als 8 Zeichen sollte ein Passwort keinesfalls sein. (Obiges Beispiel-Passwort sollte allerdings nicht verwendet werden. Accounts mit diesem Passwort werden gesperrt. :-)

Frage 6.4.1:
Um die Rechner der TU Chemnitz nutzen zu können, muss man sich mit Nutzerkennzeichen und Passwort authentifizieren. Welche anderen Varianten der Authentifizierung kennen Sie? (Z.B. gegen über einem Geldautomaten oder Ihrer Wohnung?)

Natürlich hat ein **Administrator (Admin)**, der sich um Soft- und Hardware kümmert, Fehler behebt, Programme konfigurier usw., eine hohe Verantwortung. Er ist für die Sicherheit des Systems zuständig. Die Administratoren haben die Aufgabe, die Rechner "richtig" zu konfigurieren und neu bekannt gewordene Sicherheitslücken zu beheben.

Wenn Sie Ihren Rechner selbst administrieren (wie z.B. im CSN), obliegt diese Aufgabe Ihnen.

Für die Autoren von WWW-Seiten, die eine Authentifizierung mit Nutzernamen einrichten möchten, gibt es das **HTTPS**-Protokoll, welches eine Erweiterung von HTTP darstellt. Bei diesem Protokoll wird ebenfalls die gesamte Übertragung zwischen Server und Klient verschlüsselt [4].

Hier sei noch der Hinweis gegeben, dass die Verwendung von **Sniffern**, **Portscannern** oder ähnlichen Tools, welche die Daten auf dem Netzwerk abhören, **streng verboten** ist.

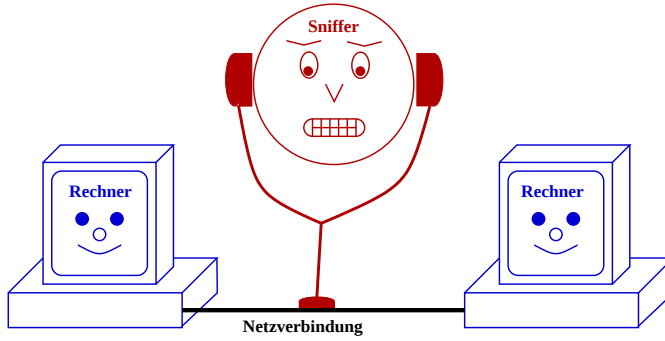


Abbildung 6.4-1.: Sniffer analysieren den Netzverkehr. Sie schreiben sozusagen alles mit, was die Rechner am Netz miteinander bereden.

Vertiefung:

[1] Ausführliche Informationen über das **Andrew File System (AFS)**, darunter auch zur Installation findet man in der Übersicht

> AFS an der TU Chemnitz.
> `[http://www.tu-chemnitz.de/urz/system/afs/]`

[2] Kurse mit vertiefenden Informationen zu einigen hier angerissenen Themen bietet das URZ an:

> URZ - Weiterbildungsangebot
> `[http://www.tu-chemnitz.de/urz/kurse/]`

[3] Mit Themen aus dem Secure-Shell-Umfeld beschäftigt sich Holger Trapp auf seinen Seiten:

> Gesicherte Kommunikation über unsichere Netze
> `[http://www.tu-chemnitz.de/~hot/ssh/]`

[4] WWW-Autoren, die ihre Seiten verschlüsselt übertragen lassen wollen, finden die nötigen Informationen unter dem Titel:

Gesicherter WWW-Zugriff via HTTPS
[http://www.tu-chemnitz.de/urz/www/https.html]

6.5. Schadprogramme

Nicht alle Programmentwickler nutzen ihre Kreativität zum Schreiben von nutzbringenden Programmen.

Die ersten Schadprogramme bezeichnete man als **Würmer**. Sie fanden mit der zunehmenden Vernetzung von Rechnern ihre Verbreitung und nutzten dazu die Schwachstellen in Serverprogrammen aus. Dabei versuchen sie den Rechner dazu zu bringen, bestimmte Aktionen auszuführen, die letzendlich dazu geeignet sind, den Wurm im System einzunisten. Als Administrator von einem Rechner sollte man stets sicherstellen, dass bei Bekanntwerden derartig nutzbarer Sicherheitslücken eine Aktualisierung des jeweiligen Programms vorgenommen wird. Sowohl Softwarehersteller selbst als auch unabhängige Organisationen pflegen Informationsangebote, die über entsprechende Vorfälle und Gegenmaßnahmen berichten.

Mit dem Aufkommen der PCs entstand eine neue Gruppe von Schadprogrammen, die man als **Viren** bezeichnet. Es handelt sich - wie bei den biologischen Namensgebern auch - um kleine Programmfragmente, die nur dann aktiv werden können, wenn sie ein normales Programm infizieren. Die Verbreitung erfolgte über Disketten, die zum Datenaustausch zwischen den Rechnern verwendet wurden. Wann immer ein infiziertes Programm gestartet wurde, hat der enthaltene Virus versucht, andere Programme zu infizieren. Heutzutage ist diese Form der Computerviren eher in den Hintergrund getreten.

Abgelöst wurden sie durch eine neue Generation von Viren, die sich über E-Mail verbreiten. Sie nutzen dabei die Fähigkeit einiger Mailprogramme aus, kleine Textdateien als Befehlsfolge auszuführen. Der Virus nutzt für seine Schadwirkung dazu die Fehler der Entwickler des Mailprogramms aus, um sich im Rechner einzunisten. Die Art der jeweiligen Schadwirkung ist dabei sehr unterschiedlich.

Während früher fast ausschließlich ausführbare Programme der Träger von Viren sein konnten, stellen die neuen Office-Pakete eine weitere Gefahrenquelle dar. So genannte **Makro-Viren** können beispielsweise in Textdateien eingeschleust werden, um beim Öffnen des Dokumentes in der Textverarbeitung automatisch in Aktion treten zu können. Sie nutzen dazu die Möglichkeit, Office-Programme ebenfalls durch kleine Anweisungsfolgen steuern zu können. Aus diesem Grund sollte man sehr vorsichtig sein, wenn man derartige Dokumente von anderen Personen insbesondere per E-Mail erhält. Gleichzeitig sollte man selbst auf den Versand von Office-Dokumenten verzichten, um nicht unabsichtlich die Verbreitung von Makro-Viren zu fördern und im schlimmsten Falle sogar schadensersatzpflichtig zu werden.

Die Schadfunktion der Viren ist sehr unterschiedlich gestaltet. Während einige eher harmlos sind oder beispielsweise "nur" alle Dateien der lokalen Festplatte löschen, stellen andere die Plattform für weitergehende Angriffe bereit. Programme, die dies tun, nennt man **Trojaner**. Ähnlich des mythologischen Namensgebers öffnen sie Zugänge

zum infizierten Rechner, die dann ein Angreifer nutzen kann, um diesem oder anderen Rechnern Schaden zuzufügen.

Ein Programmtyp, der keinen technischen, sondern finanziellen Schaden anrichten kann, sind die so genannten **Dialer**. Ursprünglich wurden sie entwickelt, um im Internet bestimmte gebührenpflichtige Leistungen per Telefonrechnung zu bezahlen. Um einen Bezahlvorgang auszulösen, muss man eine bestimmte Telefonnummer anrufen, die einen erhöhten Tarif verlangt (meist 0190...) und eine gewisse Zeit warten. Mit der Absicht, das Anrufen zu automatisieren, hat man dann Programme geschrieben, die den Anruf tätigen. Wenn nun ein unvorsichtiger Nutzer dazu verleitet wird, ein solches Programm zu installieren, dann ist es nur ein kurzer Weg bis zu dem Punkt, wo Anrufe auch ohne entsprechende Gegenleistung und für hohe Entgelte getätigt werden. Als Konsequenz, sollte man bei der Installation von Programmen grundsätzlich sehr umsichtig vorgehen und nur vertrauenswürdige Quellen nutzen. Ebenso sollte man keine per E-Mail zugeschickten Programme ausführen. Selbst Programme, deren Autoren behaupten, dass diese vor solchen Dialern schützen, haben sich selbst als Dialer entpuppt - als eine Art "Wolf im Schafspelz".

Gefahr besteht übrigens auch beim Download von Bildschirmschonern aus dem Netz, welche ebenfalls Viren enthalten können. Seien Sie also vorsichtig mit solchen kostenlosen Angeboten!

Wenn viele Nutzer ohne große Konflikte miteinander arbeiten sollen, sind einige von allen einzuhaltende Regeln unabdingbar. Praktisch alle Provider verlangen von ihren Nutzern die Einhaltung gewisser Bestimmungen. Am Beispiel der TU Chemnitz werden universitätstypische Regelungen erläutert. Zudem erhalten Nutzer der TU Chemnitz Hinweise zur Arbeit mit den uni-internen Ressourcen.

7 Bestimmungen und Hinweise für die Netz-Nutzung an der TU Chemnitz

7.1. Allgemeines

Schulen und Universitäten stellen Ressourcen und Dienste nahezu kostenfrei zur Verfügung. Diese Möglichkeiten sollen eine möglichst optimale Ausbildung der Studenten gewährleisten. Ein unbeschränkter, freier Zugang ist daher durchaus nicht selbstverständlich.

Jeder Nutzer ist Mitglied einer Gemeinschaft und auf das Funktionieren dieser angewiesen. Man sollte sich also bei jeder Tätigkeit fragen, ob man damit nicht andere Nutzer behindert. Einige Beispiele:

- Die URZ-Pools sind während der Vorlesungszeit stark ausgelastet. Es kommt durchaus vor, dass sich zu Stoßzeiten Schlangen vor den Poolräumen bilden. Wer also am Rechner sitzt und nur zum eigenen Vergnügen surft, behindert möglicherweise einen wartenden Nutzer, der eine dringende Arbeit zu erledigen hat. In diesem Fall ist der Arbeitsplatz zu räumen.

- Jedes Programm (**Job**), das auf einem der Compute-Server gestartet wird, verbraucht Ressourcen und behindert dabei Nutzer bei der Ausführung möglicherweise wichtigerer Aufgaben. Daher sollte man Jobs entsprechend ihrer Wichtigkeit und abhängig von der aktuellen Auslastung des Servers starten.

- Wer im Pool arbeitet, muss sich konzentrieren. Handy-Klingeln oder gar lautstark geführte Telefongespräche wirken sehr störend.

Wichtig!
Alle Ressourcen dürfen nur für Lehre und Forschung genutzt werden!

Die private Nutzung der Rechner und Ressourcen des URZ ist untersagt und kann geahndet werden! Dazu können die eigenen Rechner im Wohnheim genutzt werden! Was bedeutet das genau? Beispiele:

- Private Jobs, die nichts mit dem Studium zu tun haben, nicht auf öffentlichen Rechnern starten.
- Den Druckdienst nur für Belange des Studiums nutzen! Man bezahlt das Drucken zwar selbst, doch diese Preise sind reine Papierpreise und decken nicht die gesamten Material- und Abschreibungskosten. Das Drucken von Stundenplänen, Übungsblättern, Belegarbeiten oder auch Fachliteratur ist problemlos möglich, private Dinge wie Reiseinformationen oder Romane jedoch nicht. Wenn solche "nicht-studienrelevanten" Ausdrucke von URZ-Mitarbeitern an den Druckern gefunden werden, werden sie unverzüglich eingezogen; im Wiederholungsfall kann der Druckservice verwehrt werden.

Persönliche Homepages

Ein immer wieder strittiger Punkt sind persönliche Homepages mit Informationen zum Autor, seinen Interessen usw. Obwohl nicht unmittelbar zu "Lehre und Forschung" gehörig werden sie toleriert, weil sie dazu dienen, den Nutzer in der weltweiten Präsentation im Netz auszubilden.

Man sollte diese Auslegung jedoch nicht überstrapazieren und die private Präsentation in Grenzen halten. Insbesondere sollte man darauf achten, dass man auf den eigenen Seiten keine Copyright-Bestimmungen verletzt (z.B. Fotos von Prominenten, MP3-Dateien ... - da hat es schon großen Ärger gegeben), keine Werbung macht und die Seiten nicht kommerziell nutzt. Eine finanzielle Bereicherung mit Hilfe der Uni-Ressourcen ist verboten und kann zum Entzug der Nutzungsberechtigung führen. Zusätzlich ist natürlich jeder Nutzer für den Inhalt seiner Seiten selbst verantwortlich. Der Nutzer haftet für seine WWW-Seiten!

In den folgenden Abschnitten dieses Kapitels lernen Sie die Rechte und Pflichten kennen, die Sie als Nutzer des Universitätsrechenzentrums (URZ) besitzen. Des weiteren wird noch einmal der Sicherheitsaspekt angesprochen und das Chemnitzer Studentennetz (CSN) vorgestellt.

7.2. Ordnungen

In der TU Chemnitz regelt die Benutzungsordnung des Universitätsrechenzentrums (URZ) die Rahmenbedingungen zur Nutzung der IT-Infrastruktur der TU Chemnitz. Zuständigkeiten und Verfahrensregelungen sind in der Ordnung des URZ festgelegt. Wir empfehlen dringend, nach der Lektüre dieses Kapitels nochmals die

Benutzungsordnungen
[http://www.tu-chemnitz.de/urz/info/ordnungen/]

nachzulesen. Beim Erhalt Ihres Nutzerkennzeichens haben Sie schließlich durch Ihre Unterschrift diese Festlegungen akzeptiert und sich zur Einhaltung verpflichtet.

Im Folgenden werden die einzelnen Ordnungen auszugsweise vorgestellt und teilweise zur besseren Verständlichkeit kommentiert. Die kompletten Ordnungs-Texte finden Sie unter oben genanntem Link.

Auszüge aus der Ordnung des URZ

Das URZ versteht sich als Dienstleister für seine Nutzer, die diese Dienste und die bereitgestellten Ressourcen verantwortungsvoll nutzen dürfen.

Es ist für die Planung, die Verwaltung und den Betrieb der universitätsweiten IT-Infrastruktur zur Nutzung für Aufgaben in Lehre und Forschung verantwortlich. Es berät und unterstützt seine Nutzer und bietet kostenfrei Aus- und Weiterbildungskurse für Mitglieder der Universität an. [1]

Auszüge aus der Benutzungsordnung des URZ

Mitglieder der Universität können die Leistungen des URZ zur Problemlösung im Bereich von Lehre und Forschung in Anspruch nehmen. Sie können jedoch versagt werden, wenn das Mitglied zum Beispiel schon einmal von der Nutzung ausgeschlossen wurde und weitere Verstöße gegen die Nutzungsbestimmungen zu befürchten sind.

Die Nutzer sind verpflichtet:

- die Vorschriften der Benutzungsordnung einzuhalten;
- ausschließlich mit dem ihnen zugewiesenen Nutzerkennzeichen zu arbeiten
- alles zu unterlassen, was den ordnungsgemäßen Betrieb der IT-Systeme stört;
- Störungen, Beschädigungen und Fehler unverzüglich den zuständigen URZ-Mitarbeitern zu melden;
- ihre Daten und Programme so zu sichern, dass keine Schäden durch einen Verlust bei der Verarbeitung im Rechenzentrum entstehen.

Nutzer, die wiederholt oder schwerwiegend gegen die Nutzungsbestimmungen verstoßen oder bei der Benutzung strafbare Handlungen begehen, können zeitweise oder dauernd von der Benutzung ausgeschlossen werden. Rechtswidrige Nutzungen sind zum Beispiel:

- Ausspähen von Daten, Beleidigung, Verleumdung
- Datenveränderung und Computersabotage

- Verbreitung pornographischer Darstellungen sowie von Propagandamitteln verfassungswidriger Organisationen

- Urheberrechtsverletzungen

Der Nutzer haftet selbst für alle Nachteile, die der TU Chemnitz dadurch entstehen, dass er seinen in der Benutzungsordnung festgelegten Pflichten nicht nachkommt. Er haftet auch für Schäden, die durch Nutzung seines Accounts durch unberechtigte Dritte entstanden sind, insbesondere dann, wenn er sein Passwort an Dritte weitergegeben hat. [2]

Die Nutzungserlaubnis zur Nutzung der Dienste des URZ ist in der Regel befristet und kann auf Antrag verlängert werden. Für Studenten wird die Nutzungserlaubnis automatisch um ein Semester verlängert, wenn sie sich rechtzeitig zurückmelden. Sie müssen die Verlängerung also nicht extra beantragen.

Bei der Arbeit an URZ-Rechnern dürfen eigene Disketten zum Datentransport benutzt werden. Gefundene Disketten u.ä. sind im Nutzerservice abzugeben.

Das URZ übernimmt keinerlei Haftung dafür, dass die Hard- und Software fehlerfrei und ohne Unterbrechung läuft und haftet ebenfalls nicht, falls infolge technischer Störungen Daten verloren gehen.[2]

Auszüge aus der Raumordnung

Zum Aufenthalt in den öffentlichen Poolräumen existieren folgende Regelungen:

- Der Aufenthalt ist nur nutzungsberechtigten Personen gestattet. Es ist also nicht erlaubt, mal eben den Freund oder die Freundin (der/die nicht zur TU gehört) ein bisschen surfen zu lassen.

- Auf Verlangen eines URZ-Mitarbeiters haben sich die Nutzer mittels eines gültigen Haus- oder Studentenausweises zu legitimieren. Die Mitarbeiter sind auch weisungsberechtigt.

- Essen, Trinken und Rauchen sind nicht gestattet.

- Das Mitbringen von Haustieren ist nicht erlaubt.

- Untersagt sind Eingriffe in die Gerätetechnik (dazu gehört auch das Betätigen des Reset-Knopfes!), die Benutzung der als defekt ausgewiesenen Geräte sowie das eigenmächtige Anbringen bzw. Entfernen von Defektschildern.

- Jede Betriebsstörung ist umgehend einem Dispatcher mitzuteilen.

- Der Missbrauch bzw. die Weitergabe des eigenen Passworts oder der Magnetkarte sind nicht gestattet.

- Es ist nicht erlaubt, klopfende Nutzer einzulassen, da man nicht wissen kann, ob diese nutzungsberechtigt sind oder nicht. Personen, die nicht nutzungsberechtigt sind, ist der Zutritt nicht gestattet. Nutzungsberechtigte Personen, deren Karte zu Hause liegt bzw. verlorengegangen oder unbrauchbar ist, können sich an den Nutzerservice wenden.
- Wenn der Raum kurzzeitig (maximal 15 Minuten!) verlassen werden muss, ist der Bildschirm zu sperren, so dass während der Abwesenheit ein unbefugter Zugriff auf die Daten nicht möglich ist.
- Wer einen Raum betritt, sollte zuvor einen Blick auf den daneben aushängenden Zeitplan werfen. Sollte der Raum durch einen Kurs, eine Übung, ein Praktikum etc. belegt sein, ist die Arbeit zu diesem Zeitpunkt in diesem Raum nicht möglich. Es ist auch nicht erwünscht, dennoch nachzuschauen, ob vielleicht ein Platz frei ist, und diesen dann zu belegen.

Die Öffnungszeiten der Pool-Räume richten sich nach den Zugangszeiten der jeweiligen Gebäudeteile. Die meisten sind jedoch werktags von 6 bis 2 Uhr, samstags von 6 bis 22 Uhr zugänglich. Werktags ab 22 Uhr und samstags ab 14 Uhr ist zusätzlich eine Zugangsberechtigung notwendig, die Sie bei Ihrem Dekanat beantragen können.[3]

Abbildung 7.2-1.: Netikette für die Pool-Räume

Auszüge aus der Softwarenutzungsordnung

Sofern es sich nicht um freie Software handelt, hat die TU Chemnitz mit den jeweiligen Lizenzgebern Verträge über die Nutzung der auf den Rechnern installierten bzw.

anderweitig vorhandenen Software abgeschlossen. Daraus ergeben sich für alle Nutzer Verpflichtungen:

- Die Programme sind entsprechend dem Urheberrechtsgesetz ausdrücklich gesetzlich geschützt. Die Aneignung von Software durch Kopieren widerspricht den abgeschlossenen Verträgen.
- Die Weitergabe von Software und Dokumentationen an Dritte in jeglicher Form (Verkauf, Vermietung, Überlassung, Leihe ...) ist unzulässig.
- Das Kopieren von Software vom ftp-Server (z.B. Spiele) des URZ ist erlaubt.
- Das Kopieren kostenfreier, lizenzierter Software vom Softwareserver ist erlaubt. Ein Beispiel dafür ist das betriebssystemunabhängige Office-Paket OpenOffice, das sich jeder Interessent auch für den privaten Gebrauch herunterladen kann.
- Das Kopieren kostenpflichtiger, lizenzierter Software - wie beispielsweise MS Word - vom Softwareserver ist nur explizit autorisierten Angehörigen der TU erlaubt.
- Eine Verletzung dieser Bestimmungen macht schadensersatzpflichtig und wird strafrechtlich verfolgt. Wird die auf Datenträgern gespeicherte Software entwendet, kommt eine Anschuldigung wegen Diebstahls, Unterschlagung und Untreue hinzu.
- Jedes Kopieren fremder Software auf Rechner der TU ist untersagt.
- Die Entwicklung und Nutzung von Software, die Datenbestände verfälscht, die Arbeit der Rechentechnik verlangsamt oder andere, die normale Arbeit behindernde Funktionen auslöst, hat Rechtsfolgen. Selbst die Absicht, vorgenanntes zu tun, ist strafbar!

Die Betriebs- und Anwendungssoftware aller TU-Rechner darf nur auf den zugehörigen Rechnern betrieben und nur im Rahmen von Lehre und Forschung eingesetzt werden. [4]

Vertiefung:
[1]

Ordnung des URZ
[http://www.tu-chemnitz.de/urz/info/ordnungen/ordnung_des_urz.html]

[2]

Benutzungssordnung des URZ
[http://www.tu-chemnitz.de/urz/info/ordnungen/benutzungsordnung.html]

[3]

Raumordnung
[http://www.tu-chemnitz.de/urz/info/ordnungen/raumordnung.html]

[4]

Softwarenutzungsordnung
[http://www.tu-chemnitz.de/urz/info/ordnungen/softwareordnung.html]

7.3. Ihr Account an der TU Chemnitz

Als Nutzer der TU Chemnitz stehen Ihnen eine Vielzahl von Ressourcen innerhalb des Campus-Netzes und verschiedene Dienste zur Verfügung [1]. Die wichtigsten sollen an dieser Stelle vorgestellt werden.

Bei der Anmeldung im Nutzerservice des URZ haben Sie ein Nutzerkennzeichen (NKZ) und ein Passwort erhalten. Es sei hier nochmals darauf hingewiesen, dass Sie Ihr Passwort auf gar keinen Fall jemandem mitteilen dürfen. Sie haften für alles, was mit ihrem Account passiert!

Mit Ihrem Account können Sie alle Computer in den Pools, alle Compute-Server und den Chemnitzer Linux-Cluster benutzen (letzteren nur auf Antrag). Eine Übersicht über die verfügbaren Rechner findet sich unter [2].

Homeverzeichnis

Für jeden Nutzer wird im AFS ein Homeverzeichnis angelegt, welches man unter

```
/afs/tu-chemnitz.de/home/urz/x/xyz
```

findet, wobei `x` den Anfangsbuchstaben des Nutzerkennzeichens und `xyz` das Nutzerkennzeichen selbst darstellt. Nach der Anmeldung an einem Uni-Rechner befinden Sie sich automatisch in Ihrem Homeverzeichnis.

Für jeden neuen Nutzer werden in seinem Homeverzeichnis bereits einige Unterverzeichnisse mit vordefinierten AFS-Rechten angelegt:

Beispiel für den Nutzer otto:

```
$  pwd
/afs/tu-chemnitz.de/home/urz/o/otto
$  ls
BACKUP  PRIVAT  PUBLIC  public_html
```

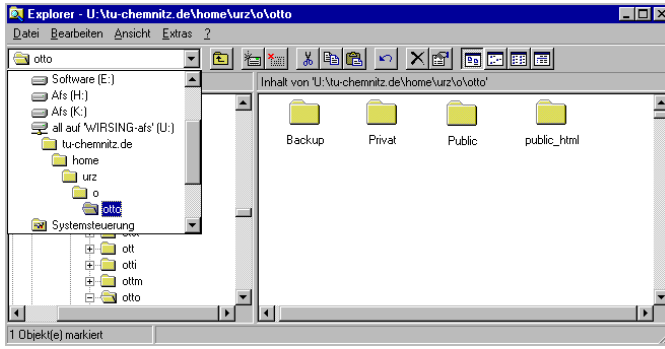


Abbildung 7.3-1.: Homeverzeichnis des Nutzers otto im Windows Explorer

Die Unterverzeichnisse sind für folgende Zwecke gedacht:

- In `PUBLIC` sollten alle die Dateien abgelegt werden, die man allen Nutzern öffentlich zugänglich machen will. In diesem Verzeichnis hat der Besitzer uneingeschränkte Rechte und alle AFS-Nutzer weltweit haben Lesezugriff.

- Das Verzeichnis `PRIVAT` ist - wie der Name schon sagt - für private Dinge gedacht, auf die niemand anders zugreifen können soll. Daher hat dort der Besitzer uneingeschränkten Zugriff, andere Nutzer haben jedoch keinerlei Rechte.

- Auf das Verzeichnis `public_html` hat neben dem Besitzer nur die Gruppe der WWW-Server Zugriff. Dieses Verzeichnis ist nämlich genau das Verzeichnis, in dem Sie Web-Seiten ablegen können, die dann im Webbrowser bei der Eingabe der URL `http://www-user.tu-chemnitz.de/~`**nutzerkennzeichen** angezeigt werden. (Das funktioniert natürlich erst, wenn Sie die ZIN-Prüfung erfolgreich bestanden haben.)

- Das Verzeichnis `BACKUP` ist das einzige, in dem der Eigentümer nur Leserechte besitzt. Es beinhaltet eine Sicherheitskopie des gesamten Homeverzeichnisses, die einmal täglich erstellt wird. Bei Bedarf können somit z.B. fälschlicherweise gelöschte Dateien wiederhergestellt werden.

Sie können natürlich jederzeit weitere Unterverzeichnisse in Ihrem Homeverzeichnis und auch innerhalb der bereits vorhandenen Unterverzeichnisse anlegen und dort die AFS-Rechte nach Bedarf setzen. An den oben erläuterten Voreinstellungen sollten Sie jedoch nur etwas ändern, wenn es unbedingt notwendig ist und Sie genau wissen, was Sie tun.

Die Quota eines jeden neuen Nutzers beträgt 50 MB, das heißt soviel Speicherplatz steht ihm in seinem Homeverzeichnis zur Verfügung. Das BACKUP-Verzeichnis fließt dabei übrigens nicht mit ein. Bei Bedarf kann die Quota durch Anfrage beim Nutzerservice erhöht werden. [3]

E-Mail-Adresse

Zusammen mit Ihrem Account wurde für Sie auch eine Mailbox eingerichtet. Ihre Uni-Mailadresse lautet **Vorname.Nachname@sJahrgang**`.tu-chemnitz.de` (für Studenten) bzw. **Vorname.Nachname@Bereich**`.tu-chemnitz.de` (für Mitarbeiter). Das ist Ihre "Haupt-Adresse" an der TU. Es existieren noch weitere Varianten dieser Adresse (Alias), doch Sie sollten möglichst immer die oben angebene verwenden, da diese im Gegensatz zu den anderen Varianten auch noch existieren wird, wenn Sie kein Nutzer im URZ mehr sind.

Viele neue Nutzer haben heutzutage bereits vor der Immatrikulation an der TU Chemnitz eine E-Mail-Adresse (z.B. bei GMX), die sie verständlicherweise auch weiterhin benutzen wollen. Sie geben deshalb immer ihre alte Adresse an, wenn sie von Kommilitonen oder Dozenten danach gefragt werden. Doch auch wenn Sie Ihre Uni-Adresse kaum zum Schreiben benutzen, sollten Sie Ihre Uni-Mailbox unbedingt in regelmäßigen Abständen (mindestens einmal wöchentlich, besser alle zwei bis drei Tage) überprüfen oder aber in Ihrer Uni-Mailbox eine Weiterleitung auf Ihre andere Mailbox einstellen. Das ist sehr wichtig, da alle offiziellen Mails der Uni, vom CSN oder auch automatisch vom URZ erstellte Mails immer an diese Adresse gehen werden. Auch werden Angehörige der TU, die zwar Sie, aber nicht ihre E-Mail-Adresse kennen, immer anhand Ihres Namens Ihre Uni-Adresse heraussuchen [4] und an diese schreiben.

Für Ihre Uni-Mailbox gibt es übrigens auch eine Quota von 20 MB, die natürlich nicht der Home-Verzeichnis-Quota angerechnet wird. Auf Antrag können Sie Ihre Mail-Quota beim Nutzerservice erhöhen lassen.

Drucken auf URZ-Druckern

Jeder benötigt irgendwann einmal die Dienste eines Druckers. An der TU Chemnitz können Sie zu günstigen Preisen die Drucker des URZ [5] nutzen, welche allesamt Postscript-Drucker sind. Für jeden Nutzer existiert ein sogenanntes Druckkonto, über das die Druckaufträge abgerechnet werden. Dieses Konto ist zu Anfang leer und muss mittels Überweisung oder Abbuchung von der TU-Card aufgestockt werden [5].

> *Zur Orientierung: Bei durchschnittlicher Nutzung der URZ-Drucker sind etwa 5 EUR pro Semester ausreichend.*

Unter Windows werden die Drucker ähnliche wie Verzeichnisse angesprochen. Dazu wird ein System verwendet, welches auf dem SMB-Protokoll basiert. Demzufolge sind sie als `\\sambaXXX\Druckername` verfügbar. XXX gibt dabei wiederum die Nummer des eigenen Subnetzes an. Detaillierte Erläuterungen finden Sie unter [5].

Die Drucker in den öffentlichen Pool-Räumen sind übrigens hauptsächlich für kleinere Aufträge der Nutzer gedacht, die gerade an den Pool-Rechnern sitzen. Daher können Sie auf diesen Druckern nur Aufträge bis maximal 35 Seiten drucken. Für umfangreichere Aufträge sind die leistungsfähigeren Drucker gedacht, die an zentralen Punkten wie dem Nutzerservice stehen.

Einige Fakultäten haben eigene Drucker in den Fakultätsrechenzentren. Die dort angewandte Druckpolitik ist bei den zuständigen Administratoren zu erfahren. Selbstverständlich sollte man auch dort sparsam mit Papier umgehen.

Weitere Dienste

Das URZ bietet für seine Nutzer noch eine ganze Reihe weiterer Dienste an. Eine Übersicht finden Sie unter [1]. Einige wollen wir an dieser Stelle noch kurz anführen:

- Sollten Sie einmal für ein bestimmtes Projekt (z.B. ein Praktikum oder eine Gruppen-Arbeit) Speicherplatz im AFS benötigen, aber die Quota in Ihrem Homeverzeichnis reicht nicht aus, dann können Sie ein Projektverzeichnis beantragen.
- Das URZ bietet auch einen Datenbank-Service an, mit dem sich jeder Nutzer der TU eine MySQL-Datenbank zur eigenen Verwendung anlegen lassen kann, ohne sich um technische Details kümmern zu müssen.
- In allen öffentlichen Pool-Räumen finden Sie je einen Rechner, an den ein Scanner angeschlossen ist, der für alle Nutzer zugänglich ist.
- Über das uni-interne WaveLAN ("Mobiler Campus", siehe [6]) können Sie in einigen Gebäudeteilen ohne lästige Verkabelung Zugang zum Campus-Netz bekommen. Das ist besonders für die Nutzung von Laptops bei Lehrveranstaltungen interessant.
- Das URZ bietet für die Studenten und Mitarbeiter der TUC preisgünstige Handbücher zu Themen wie Computer-Grundlagen, Internet, Programmiersprachen sowie zu verschiedenen Softwareprodukten an. Nähere Informationen finden Sie unter [7]

Vertiefung:
[1]

Übersicht über die Dienste des URZ
`[http://www.tu-chemnitz.de/urz/alle-dienste.html]`

[2]

Übersicht über die nutzbaren URZ-Rechner
[http://www.tu-chemnitz.de/urz/nutzerservice/computer/]

[3]

Speicherplatz im URZ
[http://www.tu-chemnitz.de/urz/system/speicherplatz/]

[4]

Suche nach Email-Adressen der TU Chemnitz
[http://cgi.tu-chemnitz.de/php/mailadr.php3]

[5]

Informationen rund ums Drucken an der TU Chemnitz
[http://www.tu-chemnitz.de/urz/drucken/]

[6]

MoCa - Mobiler Campus
[http://www.tu-chemnitz.de/urz/netz/wlan/]

[7]

Verkauf von Handbüchern durch das URZ
[http://www.tu-chemnitz.de/urz/anwendungen/handbuecher/rrzn.html]

7.4. Richtlinien zur Sicherheit im Campusnetz

Als Nutzer eines Campusnetzes müssen Sie dazu beitragen, dass der Betrieb in hoher Qualität gewährleistet werden kann. Im Vordergrund stehen dabei der Datenschutz und der Schutz der Privatsphäre, die Integrität der Daten sowie der zweckgebundene Einsatz der Ressourcen. Es sei hier nochmals erwähnt, dass das Campusnetz ausschließlich der Lehre und Forschung dient.

Die Nutzer im Campusnetz sind verpflichtet, sich über alle Regelungen zu informieren, diese einzuhalten und sich auf dem laufenden zu halten. Sie haben ihre Ressourcen im Netz sorgfältig zu schützen. Das geschieht z.B. durch die Überwachung des eigenen Accounts (Wurden Daten mysteriös geändert?), Nutzung sicherer Protokolle (ssh statt telnet) usw. Die Weitergabe von Zugangs- und Passwortinformationen ist generell untersagt!

Als Administrator eines Rechners im Campusnetz (z.B. eigener Rechner im Wohnheimzimmer) sind Sie verpflichtet, diesen kooperativ, sachgerecht und zweckgebunden zu administrieren sowie Sicherheitslücken zu verfolgen und zu beseitigen. Für die Sicherheit des Rechners ist der Administrator zuständig!

Frage 7.4.1:
Wissen Sie als Administrator des eigenen Rechners im Wohnheim, wo Sie sich über Änderungen im Netz informieren können?

Sie sollten diese Hinweise und Empfehlungen noch einmal etwas ausführlicher in unten genannten Dokumenten nachlesen. [1,2]

Vertiefung:
[1]

Richtlinien zur Sicherheit im Campusnetz
[http://www.tu-chemnitz.de/urz/info/ordnungen/netz-sicherheit.html]

[2]

Grundregeln zur verantwortungsvollen Nutzung der Datennetze
[http://www.tu-chemnitz.de/urz/netz/alwr-netz/alwr-netz.html]

7.5. Das Chemnitzer Studentennetz (CSN)

Das **Chemnitzer Studentennetz (CSN)** ist eine Initative von Studenten für Studenten, ihre Wohnheime an das Campusnetz der TU Chemnitz anzuschließen. Gleichartige Initiativen gibt es auch in anderen Städten. Mittlerweile sind in Chemnitz alle Wohnheime eingebunden, so dass jeder Student, der im Wohnheim wohnt, die Möglichkeit hat, seinen eigenen Rechner an das Campusnetz anzuschließen sowie dessen Dienste und Ressourcen zu nutzen. Der eigene Rechner ist damit ein Teil des Campusnetzes, und neben den Nutzungsbestimmungen des CSN gelten natürlich auch die des Rechenzentrums. Für die Nutzung des CSN ist pro Jahr ein geringer Beitrag zu zahlen, dessen Höhe Sie unter [2] erfahren. Zusätzliche Telefonkosten wie bei der privaten Internet-Nutzung fallen nicht an.

Vor dem Anschluss des eigenen Rechners an das CSN sollten Sie sich gründlichst über alle Belange, die damit zusammenhängen, informieren. Ausführliche Informationen dazu bietet die Homepage des CSN [1].

Natürlich gibt es auch im CSN Nutzungsbestimmungen, zu deren Einhaltung sich jeder neue Nutzer mit seiner Unterschrift verpflichtet. Auch hier finden sich wieder die Hinweise, dass das Campusnetz nur für Lehre und Forschung zu nutzen ist und dass die Übertragung einer erteilten Nutzungsberechtigung verboten ist. Des weiteren übernimmt das CSN keinerlei Haftung für Hardwareschäden oder Verlust von Daten. Bei Zerstörungen an CSN-Anlagen haftet der Verursacher. Die kompletten Nutzungsbestimmungen finden sich auf den Web-Seiten des CSN [2].

> Wichtig!
> Für die Sicherheit seines Rechnersystems ist jeder Nutzer selbst verantwortlich!

Wer seinen Wohnheim-Rechner ans CSN anschließt, kommt in den Genuss einer sehr guten Anbindung an das Campus-Netz und darüber auch ans Internet. Sie sollten sich dabei allerdings bewusst sein, dass die Campus-Netz-Technologie zwar der Uni gehört, diese jedoch den Internet-Zugang genauso bezahlen muss wie jeder andere Internet-Nutzer auch. Der Uni steht dabei ein bestimmtes monatliches Datenvolumen zur Verfügung, welches über die Internetanbindung aus dem weltweiten Netz in die TU bzw. aus der TU ins Internet fließen kann. Diese Datenmenge darf nicht überschritten werden,

was eine genaue Kalkulation notwendig macht. Die Nutzer des CSN dürfen einen festgelegten Teil des Datenvolumens nutzen. Um diesen Teil effizient zu nutzen und gerecht auf alle Teilnehmer aufzuteilen, wird ein System eingesetzt, welches die Verteilung automatisch reguliert. Detaillierte Informationen zu diesem sogenannten **Traffic-Shaping** finden Sie unter [3].

Die aktiven Mitglieder des CSN üben ihre Tätigkeit ehrenamtlich aus. Sie sind so weit als möglich zu unterstützen und in ihrer Arbeit nicht zu behindern. Sie sollten sich immer vor Augen halten, dass es ohne die Initiative dieser engagierten Studenten kein CSN gäbe! Sollte jemand Interesse an der aktiven ehrenamtlichen Mitarbeit haben, so ist er jederzeit herzlich willkommen.

Vertiefung:

[1]

Homepage des CSN
`[http://www.csn.tu-chemnitz.de/]`

[2]

Nutzungsbestimmungen des CSN
`[http://www.csn.tu-chemnitz.de/info/bestimmungen.html]`

[3]

Beschränkungen des Netzverkehrs
`[http://www.csn.tu-chemnitz.de/info/limits.html]`

A

Abkürzungen

ACL	Access Control Lists
Admin	Administrator
AFS	Andrew File System
CGI	Common Gateway Interface
CSN	Chemnitzer Studentennetz
CUSI	Configurable Unified Search Engine
DNS	Domain Name System
DSL	Digital Subscriber Line
ESMTP	Extended Simple Mail Transfer Protocol
FAQ	Frequently Asked Questions
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HTTP mit Sicherheitsfunktionen
IMAP	Interactive Mail Access Protocol
IP	Internet-Protokoll
IRC	Internet Relay Chat
ISDN	Integrated Services Digital Network
K	Kilo
M	Mega
MIME	Multipurpose Internet Mail Extension
MTA	Mail Transport Agent
MUA	Mail User Agent

NFS	Network File System
OPAC	Online Public Access Catalogue
P2P	peer-to-peer
PHP4	PHP 4: Hypertext Preprocessor
POP	Post Office Protocol
PPP	Point-to-Point-Protokoll
PS	PostScript
scp	Secure Copy
SMB	Server Message Block System
SMTP	Simple Mail Transfer Protocol
SSI	Server side includes
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
URL	Uniform Resource Locator
URZ	Universitätsrechenzentrum
USB	Universal Serial Bus
W3C	World Wide Web Consortium
WWW	World Wide Web
X-Posting	Cross-Posting

B
Index