# Materialsammlung Internettechnologien

Prof. Dr. Hans-Jürgen Buhl

Wintersemester 2007/2008

Fachgruppe Mathematik und Informatik
FB C
Bergische Universität Wuppertal

# Inhaltsverzeichnis

# 0 Einleitung

### Internet

In Zeiten der weltweiten Vernetzung, der rapiden Zunahme von Zahlungen und Geschäften via WWW sind Internettechnologien von immer größerer Bedeutung.
Was aber genau bedeutet eigentlich das Wort *internet* bzw. *Internet*? Eine Suche im frei nutzbaren `On-line Dictionary of Computing` gibt Aufschluß.

Auszug aus http://www.nightflight.com/foldoc-bin/foldoc.cgi?query=internet:

Search Home Contents Feedback Random

---

# internet

<networking>(Note: not capitalised) Any set of networks interconnected with routers. The Internet is the biggest example of an internet. (1996-09-17)

Auszug aus http://www.nightflight.com/foldoc-bin/foldoc.cgi?query=Internet:

Search Home Contents Feedback Random

---

# Internet

<networking>(Note: capital "I"). The Internet is the largest internet (with a small "i") in the world. It is a three level hierarchy composed of backbone networks, mid-level networks, and stub networks. These include commercial (.com or .co),

university (.ac or .edu) and other research networks (.org, .net) and military (.mil) networks and span many different physical networks around the world with various protocols, chiefly the Internet Protocol.

Until the advent of the World-Wide Web in 1990, the Internet was almost entirely unknown outside universities and corporate research departments and was accessed mostly via command line interfaces such as telnet and FTP. Since then it has grown to become an almost-ubiquitous aspect of modern information systems, becoming highly commercial and a widely accepted medium for all sort of customer relations such as advertising, brand building, and online sales and services. Its original spirit of cooperation and freedom have, to a great extent, survived this explosive transformation with the result that the vast majority of information available on the Internet is free of charge.

While the web (primarily in the form of HTML and HTTP) is the best known aspect of the Internet, there are many other protocols in use, supporting applications such as electronic mail, Usenet, chat, remote login, and file transfer.

There were 20,242 unique commercial domains registered with InterNIC in September 1994, 10% more than in August 1994. In 1996 there were over 100 Internet access providers in the US and a few in the UK (e.g. the BBC Networking Club, Demon, PIPEX).

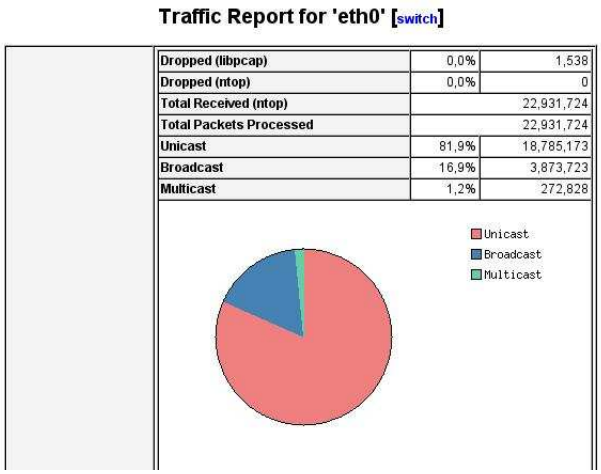
There are several bodies associated with the running of the Internet, including the Internet Architecture Board, the Internet Assigned Numbers Authority, the Internet Engineering and Planning Group, Internet Engineering Steering Group, and the Internet Society.

See also NYsernet, EUNet.

(2000-02-21)

http://www.internetworldstats.com/stats.htm - Statistiken zum Internet.
http://chrisharrison.net/projects/InternetMap/index.html - Der Internet-Verkehr grafisch.

Blick in den Internetverkehr:



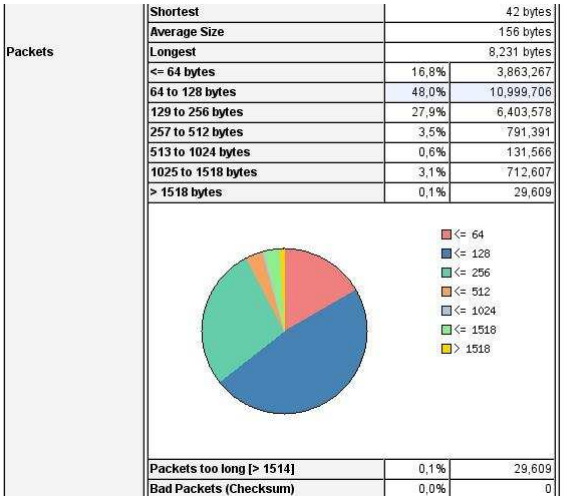
**Traffic Report for 'eth0' [switch]**

| | | | |
|---|---|---|---|
| | Dropped (libpcap) | 0,0% | 1,538 |
| | Dropped (ntop) | 0,0% | 0 |
| | Total Received (ntop) | | 22,931,724 |
| | Total Packets Processed | | 22,931,724 |
| | Unicast | 81,9% | 18,785,173 |
| | Broadcast | 16,9% | 3,873,723 |
| | Multicast | 1,2% | 272,828 |



Abbildung 0.1: An einen, an mehrere oder an alle

http://en.wikipedia.org/wiki/Unicast
http://de.wikipedia.org/wiki/Switch_%28Computertechnik%29



| | | | |
|---|---|---|---|
| Packets | Shortest | | 42 bytes |
| | Average Size | | 156 bytes |
| | Longest | | 8,231 bytes |
| | <= 64 bytes | 16,8% | 3,863,267 |
| | 64 to 128 bytes | 48,0% | 10,999,706 |
| | 129 to 256 bytes | 27,9% | 6,403,578 |
| | 257 to 512 bytes | 3,5% | 791,391 |
| | 513 to 1024 bytes | 0,6% | 131,566 |
| | 1025 to 1518 bytes | 3,1% | 712,607 |
| | > 1518 bytes | 0,1% | 29,609 |
| | Packets too long [> 1514] | 0,1% | 29,609 |
| | Bad Packets (Checksum) | 0,0% | 0 |



Abbildung 0.2: Paketgrößen

http://de.wikipedia.org/wiki/IP-Paket
http://de.wikipedia.org/wiki/Paketvermittlung
http://de.wikipedia.org/wiki/Carrier_Sense_Multiple_Access/Collision_Detection

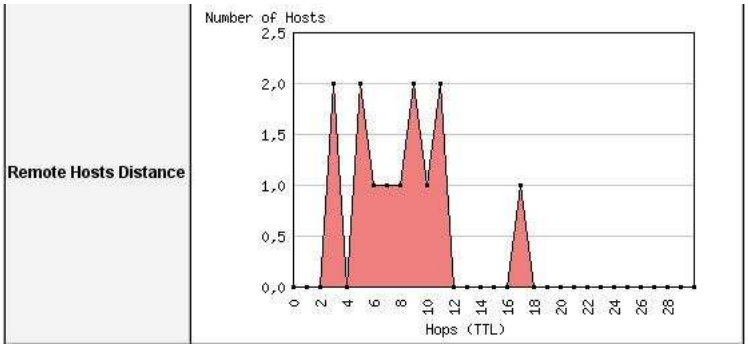



Abbildung 0.3: Wie viele „Netz zu Netz“-Übergänge

http://de.wikipedia.org/wiki/Time-to-live

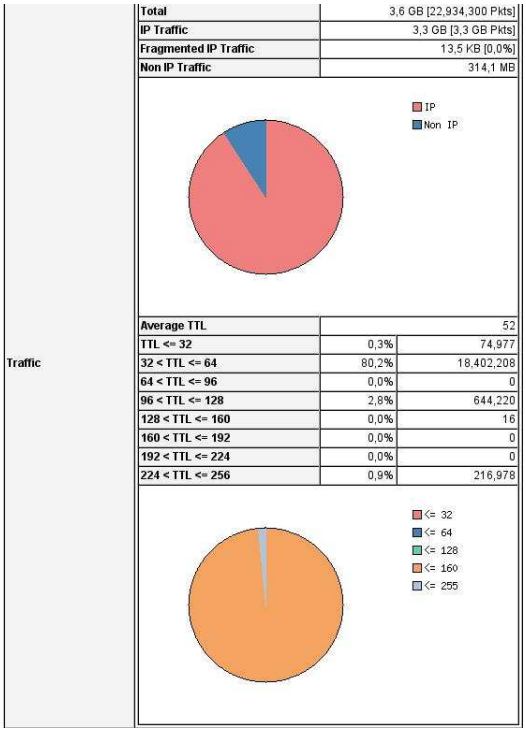



Abbildung 0.4: IP- und andere Pakete — verbliebene „Lebensdauer“ (in Hops)

**Global Protocol Distribution**

| Protocol | Data | Percentage | | | | |
|---|---|---|---|---|---|---|
| IP | 3,3 GB | 91,4% | TCP | 3,1 GB | 95,2% | |
| | | | UDP | 161,3 MB | 4,8% | |
| | | | ICMP | 351,9 KB | 0% | |
| | | | ICMPv6 | 737,8 KB | 0% | |
| | | | IGMP | 4,0 KB | 0% | |
| | | | Other IP | 67,4 KB | 0% | |
| (R)ARP | 120,4 MB | 3,6% | | | | |
| IPX | 12,1 MB | 0% | | | | |
| NetBios | 3,2 MB | 0% | | | | |
| IPv6 | 3,1 MB | 0% | | | | |
| STP | 33,0 MB | 0% | | | | |
| Other | 10,5 MB | 0% | | | | |

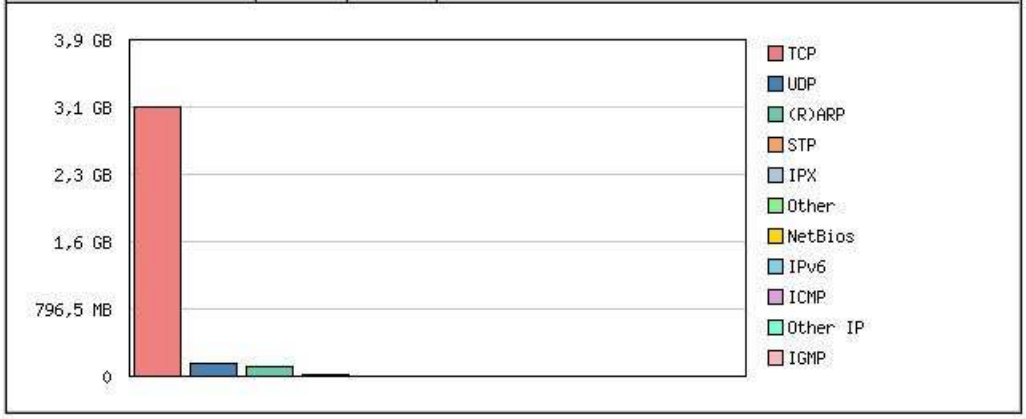



Abbildung 0.5: TCP, UDP und ICMP

http://de.wikipedia.org/wiki/Transmission_Control_Protocol
http://de.wikipedia.org/wiki/User_Datagram_Protocol
http://de.wikipedia.org/wiki/Internet_Control_Message_Protocol
Paket in Paket in Paket ...

**Global TCP/UDP Protocol Distribution**

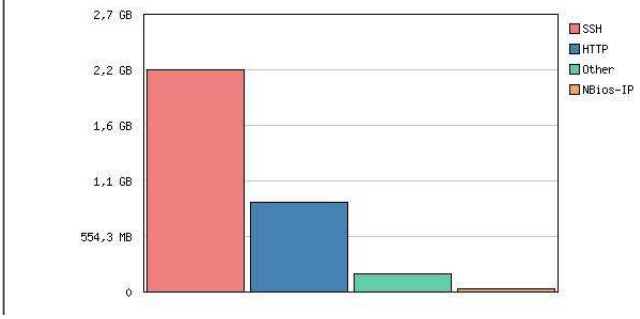
| TCP/UDP Protocol | Data | Flows | Accumulated Percentage / Historical Protocol View | |
|---|---|---|---|---|
| FTP | 1,3 KB | 0 | 0% | |
| HTTP | 903,8 MB | 4,407 | 27,0% | |
| DNS | 18,2 MB | 125,082 | 0% | |
| NBios-IP | 39,8 MB | 235,840 | 1,2% | |
| Mail | 4,1 MB | 854 | 0% | |
| DHCP-BOOTP | 333,4 KB | 966 | 0% | |
| SNMP | 554,1 KB | 4,540 | 0% | |
| NFS/AFS | 22,9 KB | 53 | 0% | |
| VoIP | 0,9 KB | 4 | 0% | |
| SSH | 2,2 GB | 3,521 | 66,3% | |
| Kazaa | 0,3 KB | 1 | 0% | |
| eDonkey | 4,0 KB | 0 | 0% | |
| BitTorrent | 244,4 KB | 6 | 0% | |
| Messenger | 1,8 KB | 9 | 0% | |
| Other TCP/UDP-based Protocols | 161,2 MB | 713,584 | 4,8% | |
| Accumulated View |  | | | |



Abbildung 0.6: Anwendungsdaten

## Dienste (services) im Internet

- E-mail mit MIME bzw. S/MIME (imap/imaps, pop3/pop3s, smtp)
- ssh oder telnet
- Filetransfer/Downloads (ftp)
- Usenet News/Diskussionsforen (nntp)
- Web/WWW (http und https)
- Netzwerkzeit (ntp)
- Adressverzeichnisse, Directories (ldap)

Lese dazu etwa http://de.selfhtml.org/intro/internet/dienste.htm (vgl. auch die Übungsaufgaben).
Von Servern angebotene Dienste können häufig mittels URLs (http://en.wikipedia.org/wiki/Uniform_Resource_Locator) in Browserns wie etwa Firefox/Mozilla/Netscape benutzt werden.

## E-mail

Für Reisen ist etwa der Web-Zugang zum eigenen Mailserver nützlich:

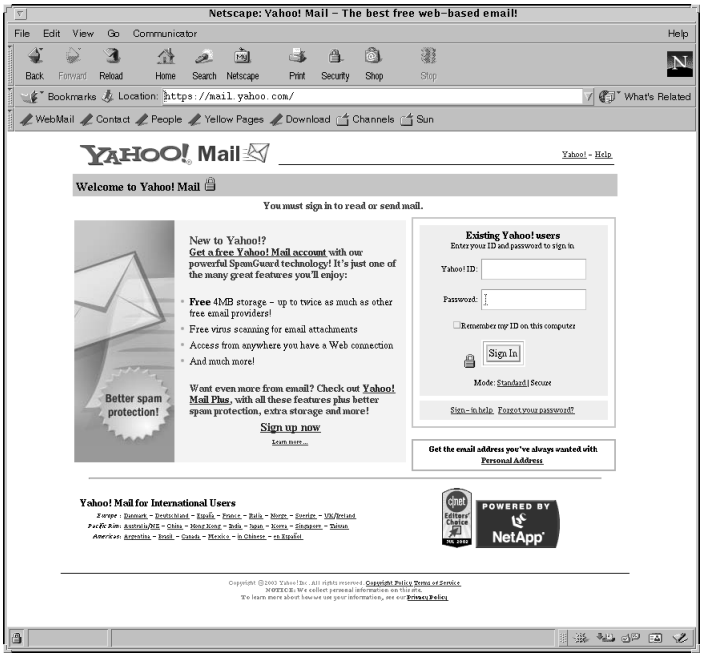



Abbildung 0.7: E-Mail: `http://mail.yahoo.com`

Der E-Mail-Server für Mitglieder der Bergischen Universität: http://www.zim.uni-wuppertal.de/dienste/netz/email/


Abbildung 0.8: Web-Mail an der BUW


Abbildung 0.9: Ändere Mail-Einstellungen

imap-Zugriff auf den Mailserver der BUW

Achten Sie bei Eingabeaufforderungen von Authentifikationsdaten (Usernamen und Paßwörtern (zum Einloggen)) bitte immer darauf, dass diese über eine verschlüsselte (sichere) Verbindung übertragen werden (`https://...`) sowie beim ersten Zugang ein Zertifikatsannahme-Dialog wie folgt durchzuführen ist:

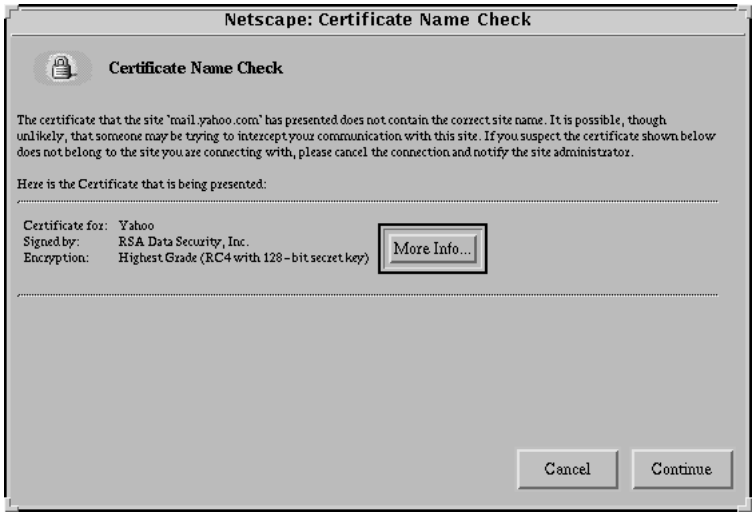



Abbildung 0.10: E-Mail: `https`-Zertifikatsannahme-Dialog

Eine (noch flexibler nutzbare) Alternative ist der Zugriff auf einen IMAP-Server, der etwa in Netscape folgendermaßen eingerichtet werden kann (email-Account einrichten):

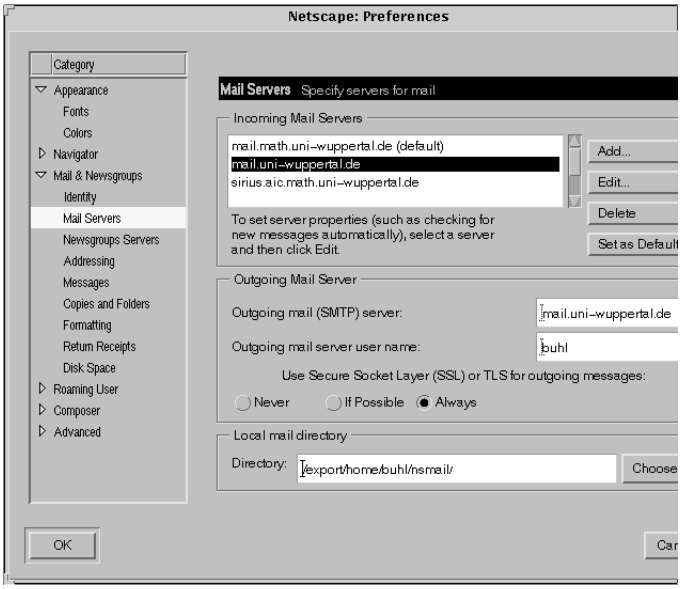



Abbildung 0.11: E-Mail: IMAP-Account-Einrichtung I

Nach Anklicken von `Add` beziehungsweise `Edit`:

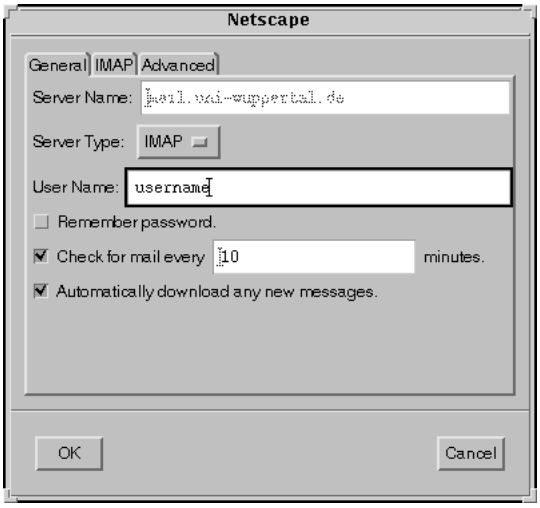



Abbildung 0.12: E-Mail: IMAP-Account-Einrichtung II

Auch hier sollte auf verschlüsselte Datenübertragung unbedingt geachtet werden:

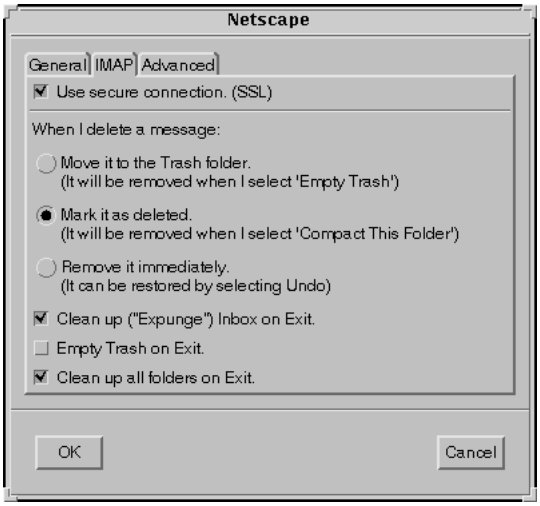
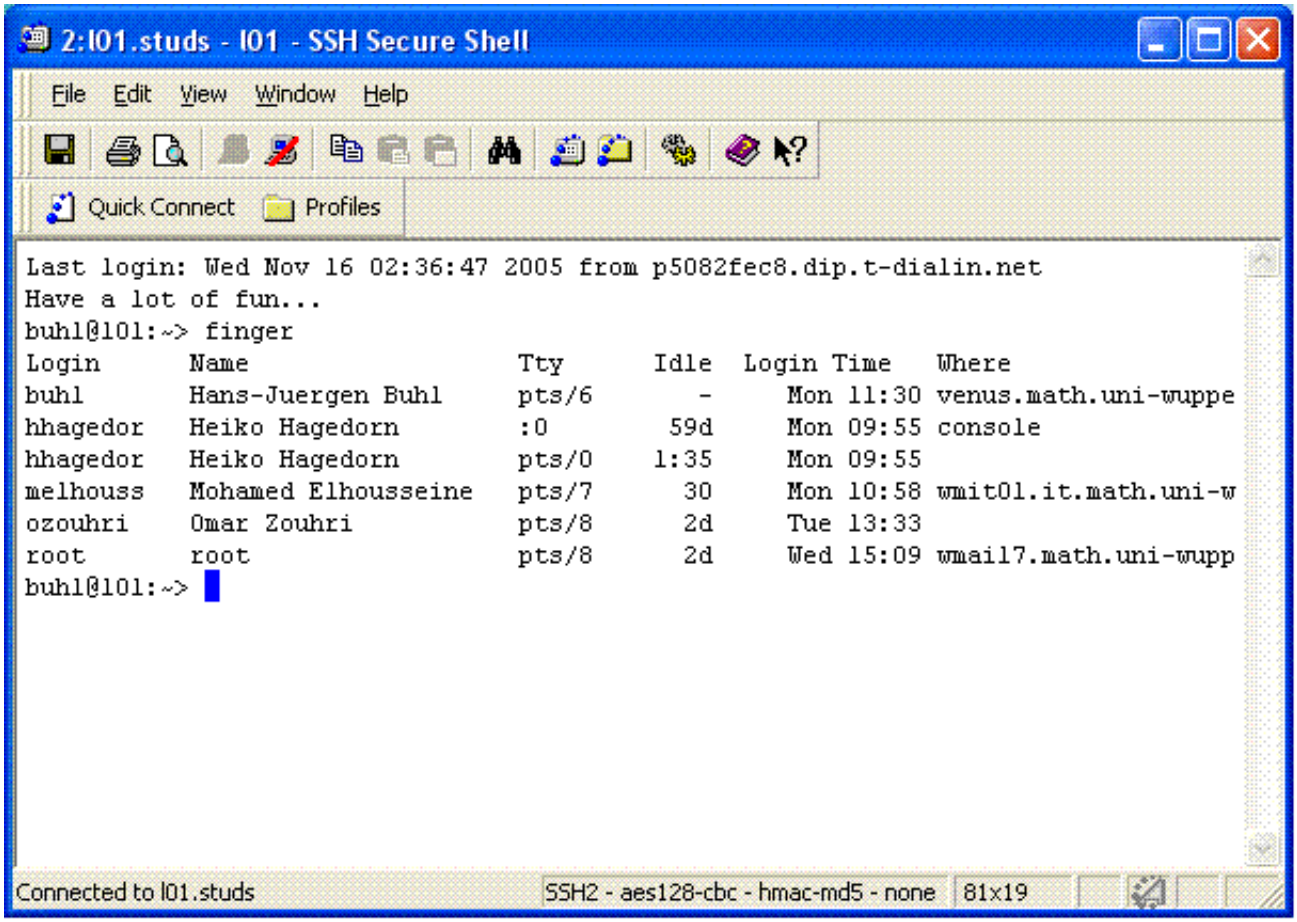
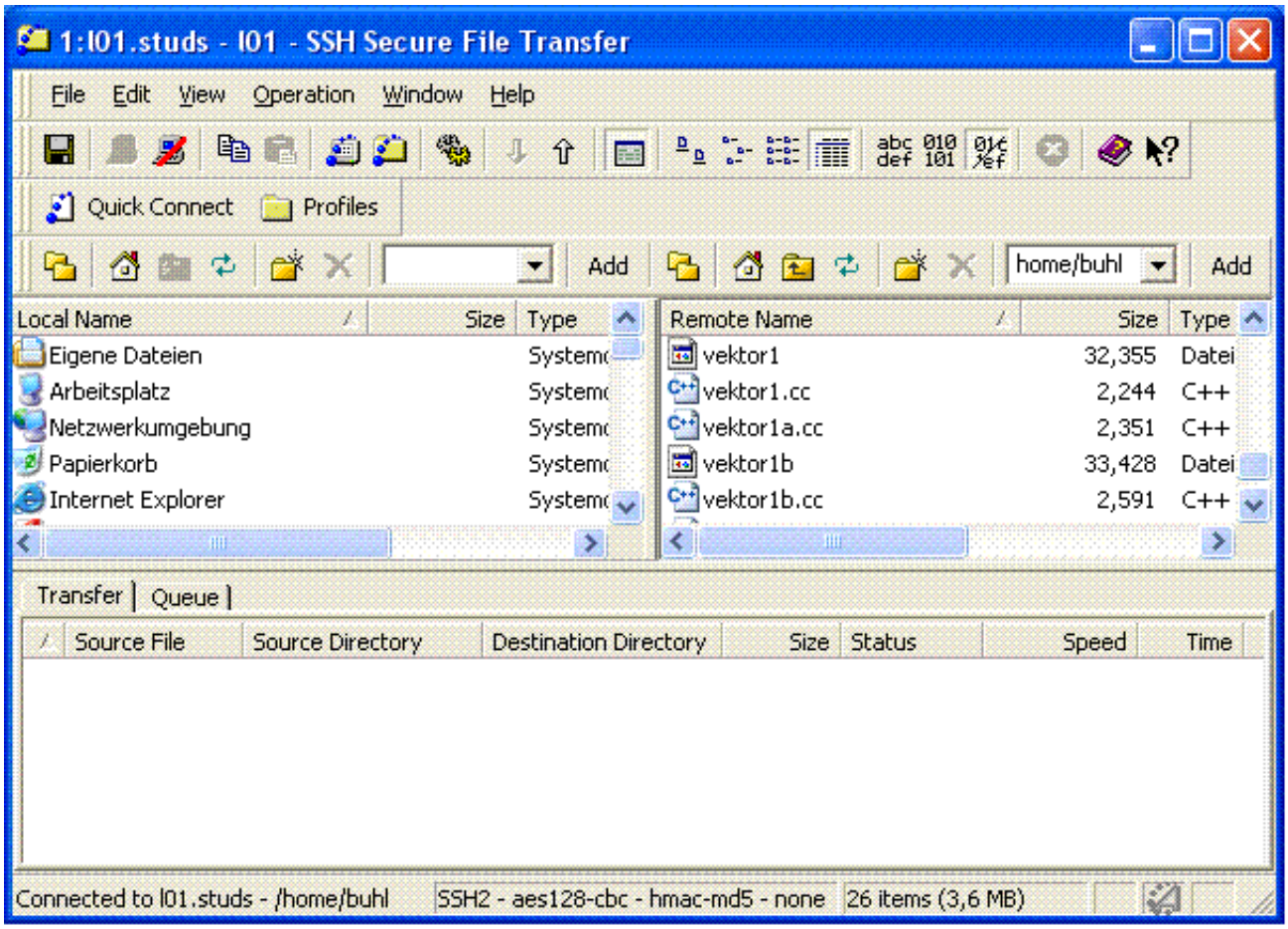



Abbildung 0.13: E-Mail: IMAP-Account-Einrichtung III

Abbildung 0.14: E-Mail: IMAP-Account-Einrichtung IV

## Entfernte Kommandoausführung/Dateitransfer




1:l01.studs - l01 - SSH Secure File Transfer
File Edit View Operation Window Help
Quick Connect
Profiles
Add
home/buhl
Add
Local Name
Size
Type
Eigene Dateien
Arbeitsplatz
Netzwerkumgebung
Papierkorb
Internet Explorer
Remote Name
Size
Type
vektor1 32,355 Datei
vektor1.cc 2,244 C++
vektor1a.cc 2,351 C++
vektor1b 33,428 Datei
vektor1b.cc 2,591 C++
Transfer
Queue
Source File
Source Directory
Destination Directory
Size
Status
Speed
Time
Connected to l01.studs - /home/buhl
SSH2 - aes128-cbc - hmac-md5 - none
26 items (3,6 MB)

### Downloads

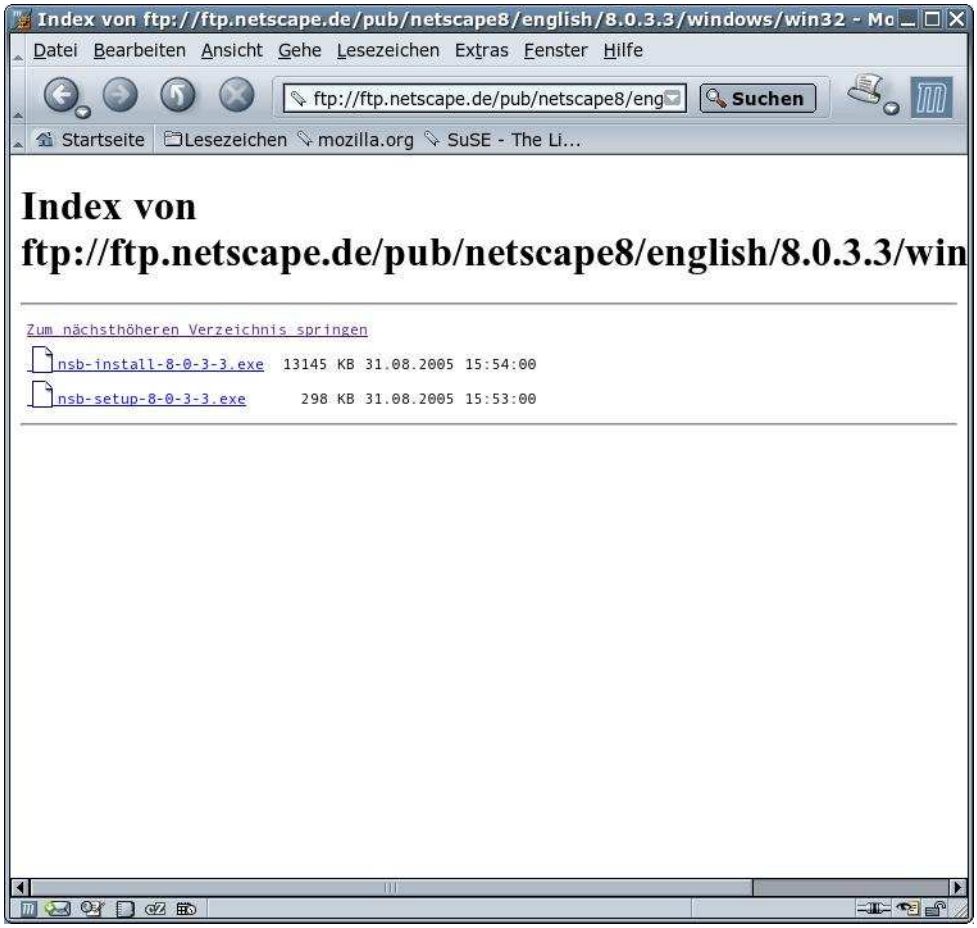



Abbildung 0.15: ftp-Download

Interessant ist unter anderem ftp://localftp.uni-wuppertal.de/pub, ftp://ftp.uni-wuppertal.de/pub und der ftp-Server des Internet-Providers unserer Hochschule ftp://ftp.cert.dfn.de/pub/.

Downloads im GB-Bereich sind für ftp- und http-Server ungeeignet Dazu bieten sich P2P-Server an:

http://de.wikipedia.org/wiki/Peer-to-Peer
http://de.wikipedia.org/wiki/BitTorrent

## Usenet News

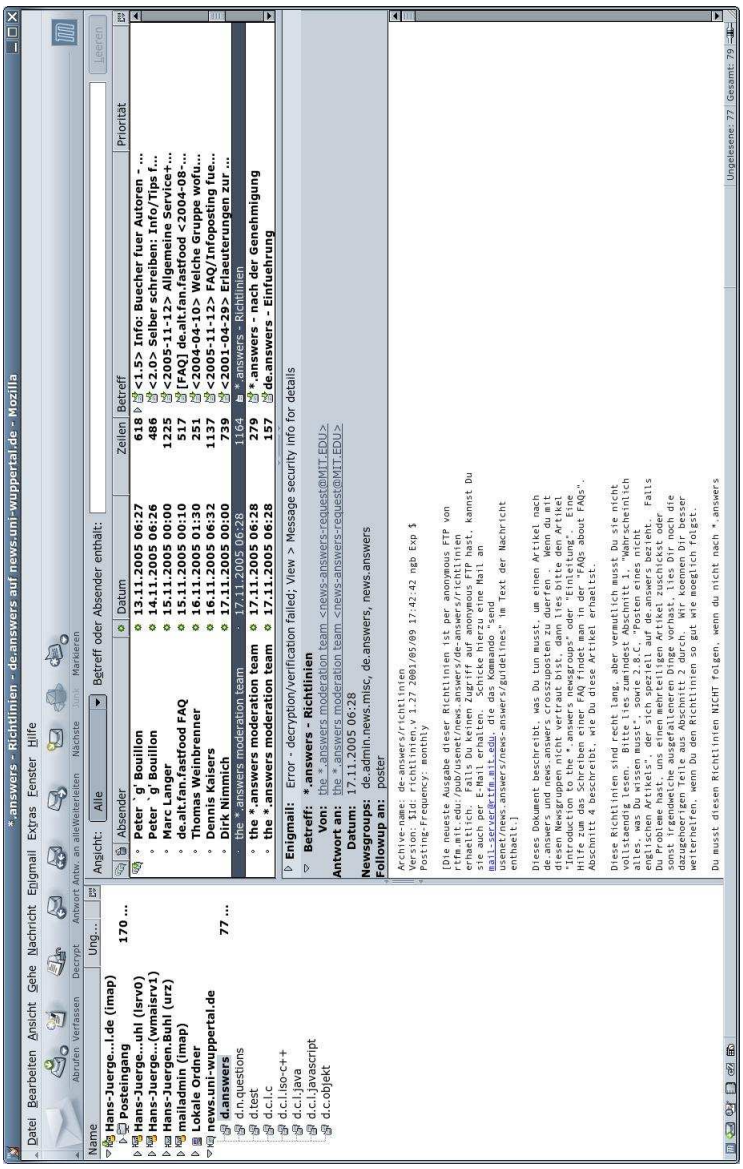



Abbildung 0.16: Usenet News

## Web-Seiten

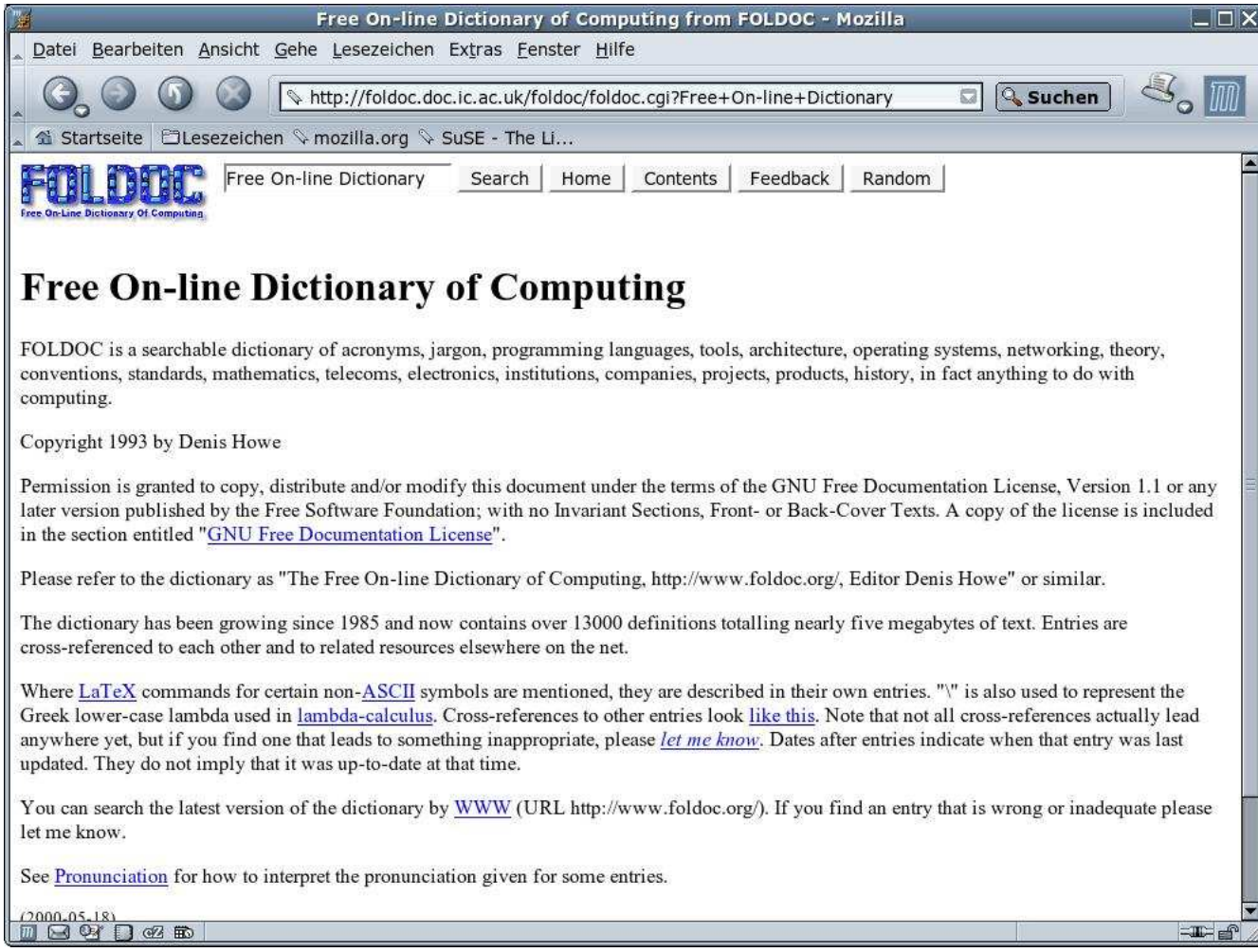
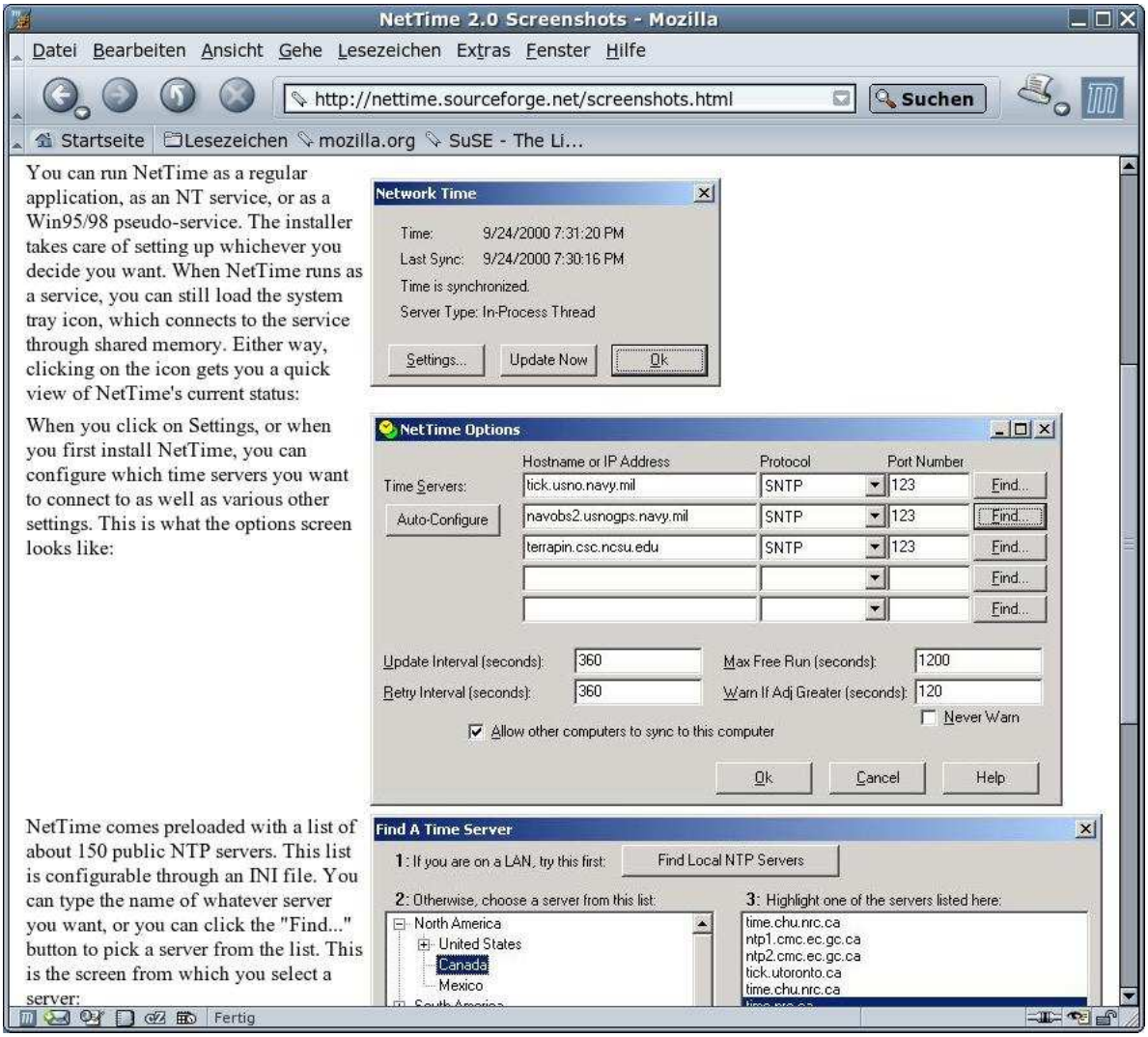


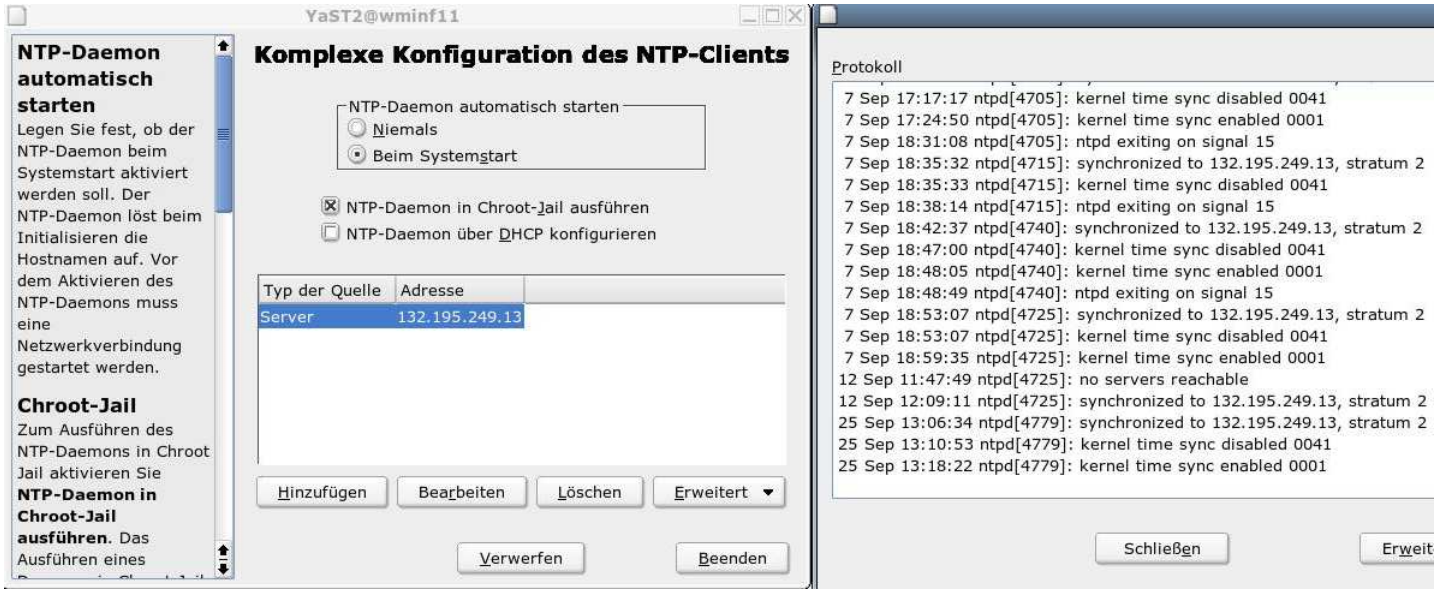

Abbildung 0.17: Web-Seiten

## Zeitsynchronisation

In Windows




und in Linux:


YaST2@wminf11
NTP-Daemon automatisch starten
Legen Sie fest, ob der NTP-Daemon beim Systemstart aktiviert werden soll. Der NTP-Daemon löst beim Initialisieren die Hostnamen auf. Vor dem Aktivieren des NTP-Daemons muss eine Netzwerkverbindung gestartet werden.
Chroot-Jail
Zum Ausführen des NTP-Daemons in Chroot Jail aktivieren Sie NTP-Daemon in Chroot-Jail ausführen. Das Ausführen eines
Komplexe Konfiguration des NTP-Clients
NTP-Daemon automatisch starten
Niemals
Beim Systemstart
NTP-Daemon in Chroot-Jail ausführen
NTP-Daemon über DHCP konfigurieren
Typ der Quelle
Adresse
Server
132.195.249.13
Hinzufügen
Bearbeiten
Löschen
Erweitert
Verwerfen
Beenden
Protokoll
7 Sep 17:17:17 ntpd[4705]: kernel time sync disabled 0041
7 Sep 17:24:50 ntpd[4705]: kernel time sync enabled 0001
7 Sep 18:31:08 ntpd[4705]: ntpd exiting on signal 15
7 Sep 18:35:32 ntpd[4715]: synchronized to 132.195.249.13, stratum 2
7 Sep 18:35:33 ntpd[4715]: kernel time sync disabled 0041
7 Sep 18:38:14 ntpd[4715]: ntpd exiting on signal 15
7 Sep 18:42:37 ntpd[4740]: synchronized to 132.195.249.13, stratum 2
7 Sep 18:47:00 ntpd[4740]: kernel time sync disabled 0041
7 Sep 18:48:05 ntpd[4740]: kernel time sync enabled 0001
7 Sep 18:48:49 ntpd[4740]: ntpd exiting on signal 15
7 Sep 18:53:07 ntpd[4725]: synchronized to 132.195.249.13, stratum 2
7 Sep 18:53:07 ntpd[4725]: kernel time sync disabled 0041
7 Sep 18:59:35 ntpd[4725]: kernel time sync enabled 0001
12 Sep 11:47:49 ntpd[4725]: no servers reachable
12 Sep 12:09:11 ntpd[4725]: synchronized to 132.195.249.13, stratum 2
25 Sep 13:06:34 ntpd[4779]: synchronized to 132.195.249.13, stratum 2
25 Sep 13:10:53 ntpd[4779]: kernel time sync disabled 0041
25 Sep 13:18:22 ntpd[4779]: kernel time sync enabled 0001
Schließen
Erweit

### E-mail Adressverzeichnisse

Nichtlokale Adressbücher können in Form von LDAP-Directory-Servern (Verzeichnisservern) für die automatische Adressergänzung sowohl im Netscape-Messenger als auch in Outlook/Outlook Express genutzt werden:
Dazu wird das Netscape-Adressbuch aufgerufen und z.B. der LDAP[1]-Server der Fachgruppe Mathematik der Bergischen Universität den Verzeichnisdiensten hinzugefügt:

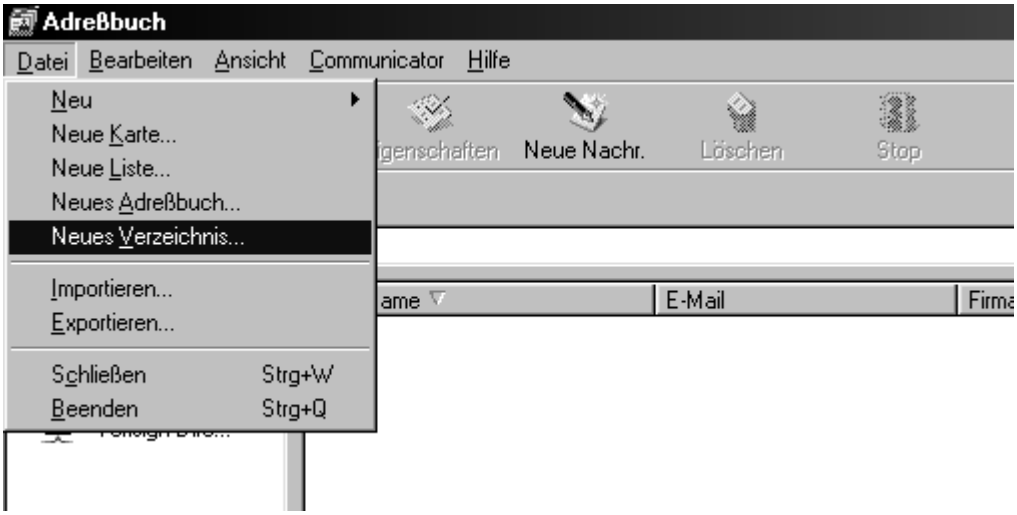



Abbildung 0.18: LDAP-Dienste als Netscape-Adressbuch nutzen

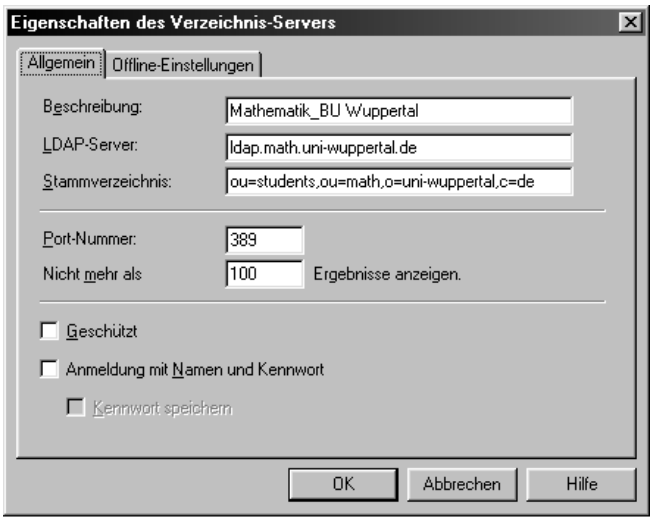



Abbildung 0.19: LDAP-Server Einrichtung in Netscape

[1]LDAP=light weight directory access protocol.
Ein Verzeichnisdienst ist eine Informationsdatenbank, die auf häufige Anfragen optimiert ist, jedoch nicht auf häufige Änderungen/Modifikationen.

Ähnlich kann unter Windows `wab` (windows address book) aufgerufen werden und z.B. der hochschulinterne LDAP-Server des Personals der Bergischen Universität Wuppertal gemäß den folgenden Abbildungen zur Benutzung bereitgestellt werden (aktuelle Zugangsdaten von ldapintern finden Sie unter http://www.hrz.uni-wuppertal.de/dienste/netz/email/ldap_bu.html):

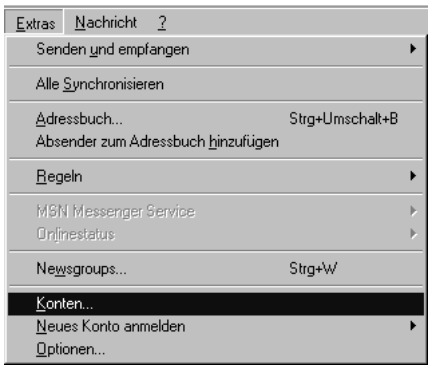



Abbildung 0.20: LDAP-Dienste in Outlook-Express I

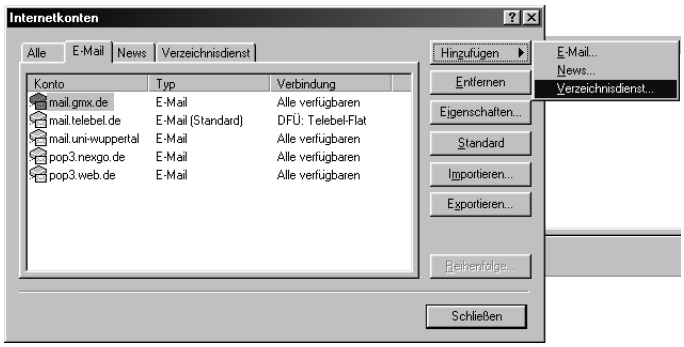



Abbildung 0.21: LDAP-Dienste in Outlook-Express II

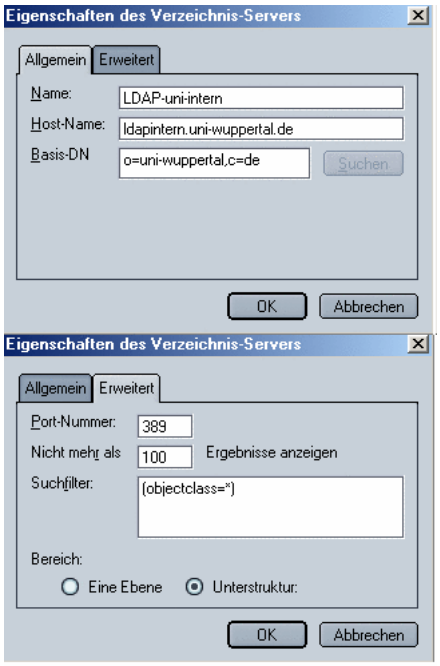



Abbildung 0.22: LDAP-Dienste in Outlook-Express III

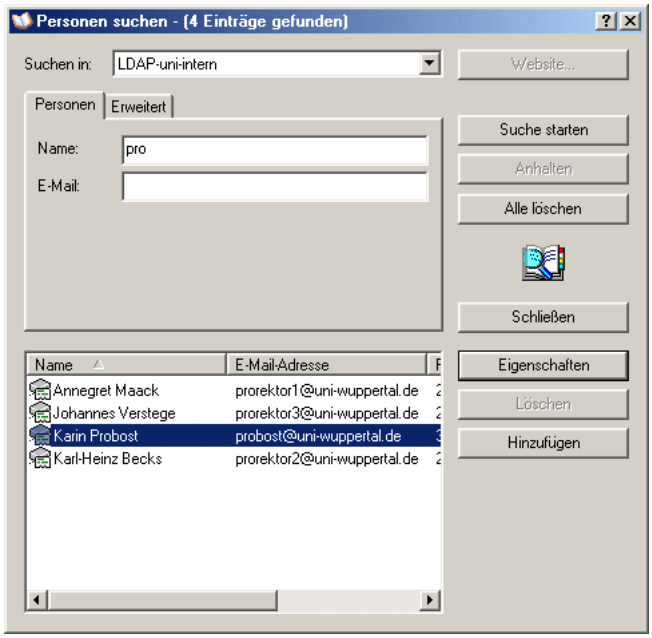



Abbildung 0.23: LDAP-Dienste in Outlook-Express IV

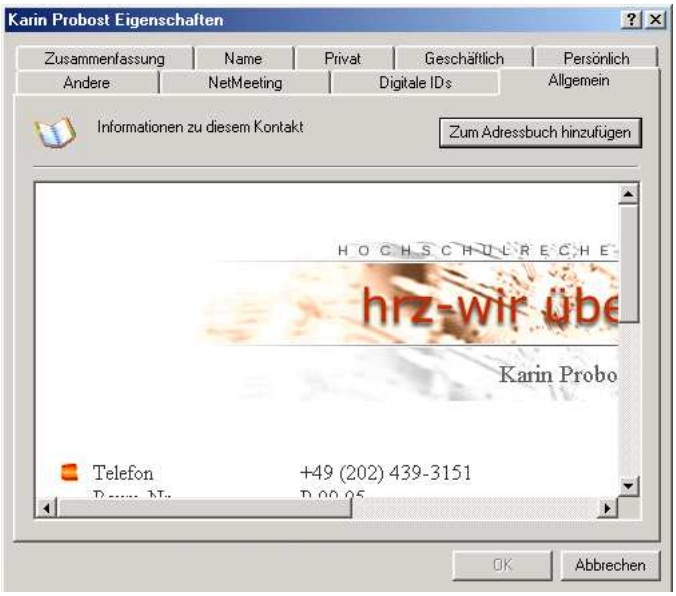



Abbildung 0.24: LDAP-Dienste in Outlook-Express V

Durch die Suchbasis (search root) kann man „Unterabteilungen“ von Organisationen baumartig getrennt ansprechen:

| | |
|---|---|
| Organisationsunit | ou=math |
| Organisation | o=uni-wuppertal |
| Land (country) | c=de |

bzw.

| |
|---|
| ou=groups |
| ou=math |
| o=uni-wuppertal |
| c=de |

usw.

**Daten zur Konfiguration einer Netzwerkkarte**

Reguläre Konfigurationsdaten für den Netzanschluß in der BUW:
http://www.zim.uni-wuppertal.de/zugang/netzanschluss/netzanschluss.html

VPN-Außenzugang zur BUW:
http://www.zim.uni-wuppertal.de/zugang/netzanschluss/vpn/

### Unsicherheit im Internet

Das auf der Basis von Vertrauenswürdigkeit entstandene Internet ist in seinem Grundkonzept unsicher.

Unsicherer E-Mail-Versand per SMTP
Aktuelle und vertrauenswürdigere Mail-Server

## 0.1 S/MIME

Secure MIME bietet die Möglichkeiten, den email-Transfer sicherer zu gestalten. Mittels zertifizierter Codierungsschlüssel wird die

Authentizität

mit Hilfe von „unterschriebener“ E-mail-Nachrichten beziehungsweise die

Geheimhaltung

mittels „codierter“ E-Mails erreicht.

### S/MIME-Zertifikate

Das Versenden von signierten, verschlüsselten bzw. signierten und verschlüsselten E-Mail's sollte mit Hilfe von S/MIME-Zertifikaten (X.509-Zertifikaten) und Mail-Clients wie Thunderbird oder „Windows Mail“ durchgeführt werden.

### Quellen für öffentliche Zertifikate

1. S/MIME-Mail's enthalten den öffentlichen Schlüssel des Absenders.
2. Zertifikat-Verzeichnisse von Zertifikatanbieter:
   Über die WWW-Seite

   `https://www.trustcenter.de/fcgi-bin/Search.cgi?Language=de`

   können in der „öffentliche Gruppe“ S/MIME-Zertifikate eingesehen werden, die das Trustcenter ausgestellt hat. S/MIME-Zertifikate (X.509) können dann mittels des Knopfes „Installieren“ in die Client-Zertifikatdatenbank übernommen werden.
3. LDAP-Verzeichnisse: Trägt man den LDAP-Server von Trustcenter als Verzeichnisdienst in das Adressbuch ein, wie in

   `http://www.trustcenter.de/569.htm`

   beschrieben, so können auch so Zertifikate anderer Trustcenterkunden erfragt werden.

4. Dateien in Form von `.der`-Dateien mit dem MIME-Typ `application/x-x509-email-cert` .

5. Zertifikate auf http-Server:


### 0.1.1 Unterschriften und Zertifikate

**Erwerben eines „kostenlosen“ Class1-Zertifikats für Privatkunden**

Ueber die WWW-Seite http://www.trustcenter.de/products/my_certificate_express.htm kann ein kostenloses Class1-Privatkundenzertifikat oder über

https://www.trustcenter.de:443/fcgi-bin/Request.cgi?Product=TempPriv
&KindOfCert=Client&Customer=Private&Page=SelectCustomer

ein Class3-Privatkundenzertifikat für z.Zt. 31,-Euro/Jahr bezogen werden.

**Versenden von signierten Dateien mittels Netscape (/Explorer)**

Dazu klickt man den Knopf `Signed` bei den Optionen im Compose-Window vor dem Abschicken an.

Als spezielles Attachment wird ein „externe“ `x-pkcs7`-signature mitgeschickt, die auch den öffentlichen S/MIME-Schlüssel enthält.

Ein e-mail Korrespondent kann die Mail auf Authentizität überprüfen (inklusive Datum den Unterzeichnung) und Netscape speichert den öffentlichen Schlüssel automatisch in seiner Zertifikat-Datenbasis (People) ab, so dass der Korrespondent ab sofort verschlüsselte Nachrichten schicken kann (sofern er selbst ein Zertifikat besitzt).

Eine unterschriebene (eigentlich: mit Beglaubigung versehende) email sieht dann in Klatext wie folgt aus:

```
From - Tue Jul  8 18:39:55 2003
Received: from wminf0.math.uni-wuppertal.de by wmwap3.math.uni-
   wuppertal.de
 (Sun Internet Mail Server sims.3.5.1998.08.08.00.06)
 with ESMTP id <0HGX00802RAJQ7@wmwap3.math.uni-wuppertal.de>
    for
 buhl@sims-ms-daemon; Mon, 23 Jun 2003 15:11:08 +0200 (MET DST)
Received: from math.uni-wuppertal.de
 (wmam3.math.uni-wuppertal.de [132.195.95.99]) by wminf0.math.
    uni-wuppertal.de
 (8.9.3+Sun/8.9.3) with ESMTP id PAA29859 for
 <hans-juergen.buhl@math.uni-wuppertal.de>; Mon,
 23 Jun 2003 15:11:06 +0200 (MEST)
Date: Mon, 23 Jun 2003 15:11:01 +0200
From: Peter Feuerstein <fpf@math.uni-wuppertal.de>
Subject: Signierte Mail
Sender: Peter.Feuerstein@math.uni-wuppertal.de
To: "Hans-Juergen Buhl (buhl)" <hans-juergen.buhl@math.uni-
   wuppertal.de>
Message-id: <3EF6FC65.9A5D5862@math.uni-wuppertal.de>
Organization: FB 7 - Mathematik, BUGH Wuppertal
MIME-version: 1.0
X-Mailer: Mozilla 4.77 [en] (X11; U; SunOS 5.5.1 sun4u)
Content-type: multipart/signed; protocol="application/x-pkcs7-
   signature";
 micalg=sha1; boundary="--------------msB24799379B02F5524859EAC5"
X-Accept-Language: de, en

This is a cryptographically signed message in MIME format.

----------------msB24799379B02F5524859EAC5
Content-Type: multipart/mixed;
 boundary="--------------EBB47411FBBBCCA0A1F6F075"

This is a multi-part message in MIME format.
----------------EBB47411FBBBCCA0A1F6F075
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit

Signiert...

--
-- Frank Peter Feuerstein
```

```
    ----------------------------------------
___ University of Wuppertal, FB7-Mathematik
____ mailto:fpf@math.uni-wuppertal.de     Phone:+49 202 439-2818
_____ http://www.math.uni-wuppertal.de/~fpf     Fax: +49 202
   439-2853
----------------EBB47411FBBBCCA0A1F6F075
Content-Type: text/x-vcard; charset=us-ascii;
 name="fpf.vcf"
Content-Transfer-Encoding: 7bit
Content-Description: Card for Peter Feuerstein
Content-Disposition: attachment;
 filename="fpf.vcf"

begin:vcard
n:Feuerstein;Frank Peter
tel;fax:+49 202 439-2853
tel;work:+49 202 439-2818
x-mozilla-html:FALSE
url:http://www.math.uni-wuppertal.de/~fpf
org:BUGH Wuppertal;FB7-Mathematik & IAI
adr:;;Gaussstrasse 20;Wuppertal;;D-42097;Germany
version:2.1
email;internet:fpf@math.uni-wuppertal.de
title:Dr.rer.nat., Dipl.-Math.
note:Angewandte Mathematik & Informatik
x-mozilla-cpt:;23168
fn:Frank Peter Feuerstein
end:vcard

----------------EBB47411FBBBCCA0A1F6F075--

----------------msB24799379B02F5524859EAC5
Content-Type: application/x-pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature

MIIF1gYJKoZIhvcNAQcCoIIFxzCCBcMCAQExCzAJBgUrDgMCGgUAMAsGCS
......
......
----------------msB24799379B02F5524859EAC5--
```

Das `smime.p7s`-Attachment enthält den öffentlichen Schlüssel des Versenders sowie ei-

ne Prüfsumme des Textinhaltes der email. Mit Hilfe des öffentlichen Schlüssels wird die Prüfsumme der angekommenen Mail erneut berechnet und mit der übersendeten Prüfsumme verglichen. Außerdem wird der öffentliche Schlüssel des Absenders auf Gültigkeit überprüft, indem er über die ausstellende Zertifizierungsstelle (zum Beispiel http://www.trustcenter.de) verifiziert wird.

### 0.1.2 Codierte Mail

**Versenden von codierten Mails mittels Netscape (/Explorer)**

Dazu klickt man den Knopf `Encrypted` bei den Optionen im Compose-Window vor dem Abschicken an.

Man muss den (oder die) öffentlichen X.509-Schlüssel des (der) Adressaten besitzen, sonst funktioniert die Verschlüsselung nicht!

Man bittet gegebenenfalls den Adressaten um eine signierte S/MIME-Mail (dann wird bei deren Empfang dessen öffentlicher Schlüssel automatisch für zukünftige Verschlüsselungen gespeichert) oder lädt dessen öffentlichen Schlüssel über „Other People's Certificates“, „Search Directory“ von einer LDAP-Datenbank.

Eine codierte Mail sieht im Klartext folgendermaßen aus:

```
From - Tue Jul  8 18:39:29 2003
Received: from wminf0.math.uni-wuppertal.de by wmwap3.math.uni-
    wuppertal.de
 (Sun Internet Mail Server sims.3.5.1998.08.08.00.06)
 with ESMTP id <0HGX00802R9RQ0@wmwap3.math.uni-wuppertal.de>
     for
 buhl@sims-ms-daemon; Mon, 23 Jun 2003 15:10:39 +0200 (MET DST)
Received: from math.uni-wuppertal.de
 (wmam3.math.uni-wuppertal.de [132.195.95.99]) by wminf0.math.
     uni-wuppertal.de
 (8.9.3+Sun/8.9.3) with ESMTP id PAA29856 for
 <hans-juergen.buhl@math.uni-wuppertal.de>; Mon,
 23 Jun 2003 15:10:37 +0200 (MEST)
Date: Mon, 23 Jun 2003 15:10:36 +0200
From: Peter Feuerstein <fpf@math.uni-wuppertal.de>
Subject: Codierte Mail
Sender: Peter.Feuerstein@math.uni-wuppertal.de
To: "Hans-Juergen Buhl (buhl)" <hans-juergen.buhl@math.uni-
    wuppertal.de>
Message-id: <3EF6FC4C.47240C11@math.uni-wuppertal.de>
Organization: FB 7 - Mathematik, BUGH Wuppertal
MIME-version: 1.0
X-Mailer: Mozilla 4.77 [en] (X11; U; SunOS 5.5.1 sun4u)
Content-type: application/x-pkcs7-mime; name="smime.p7m"
```

```
Content-description: S/MIME Encrypted Message
Content-disposition: attachment; filename="smime.p7m"
Content-transfer-encoding: base64
X-Accept-Language: de, en

MIAGCSqGSIb3DQEHA6CAMIACAQAxggLWMIIBZwIBADCBzzCBvDELMA
 .........
uF8AAAAAAAAAAAA
```

Eine codierte und signierte Mail sieht folgendermaßen aus:

```
From - Tue Jul  8 18:40:21 2003
Received: from wminf0.math.uni-wuppertal.de by wmwap3.math.uni-
    wuppertal.de
 (Sun Internet Mail Server sims.3.5.1998.08.08.00.06)
 with ESMTP id <0HGX00802RBKQG@wmwap3.math.uni-wuppertal.de>
    for
 buhl@sims-ms-daemon; Mon, 23 Jun 2003 15:11:44 +0200 (MET DST)
Received: from math.uni-wuppertal.de
 (wmam3.math.uni-wuppertal.de [132.195.95.99]) by wminf0.math.
    uni-wuppertal.de
 (8.9.3+Sun/8.9.3) with ESMTP id PAA29868 for
 <hans-juergen.buhl@math.uni-wuppertal.de>; Mon,
 23 Jun 2003 15:11:42 +0200 (MEST)
Date: Mon, 23 Jun 2003 15:11:41 +0200
From: Peter Feuerstein <fpf@math.uni-wuppertal.de>
Subject: Codierte und signierte Mail
Sender: Peter.Feuerstein@math.uni-wuppertal.de
To: "Hans-Juergen Buhl (buhl)" <hans-juergen.buhl@math.uni-
    wuppertal.de>
Message-id: <3EF6FC8D.A3677D9A@math.uni-wuppertal.de>
Organization: FB 7 - Mathematik, BUGH Wuppertal
MIME-version: 1.0
X-Mailer: Mozilla 4.77 [en] (X11; U; SunOS 5.5.1 sun4u)
Content-type: application/x-pkcs7-mime; name="smime.p7m"
Content-description: S/MIME Encrypted Message
Content-disposition: attachment; filename="smime.p7m"
Content-transfer-encoding: base64
X-Accept-Language: de, en

MIAGCSqGSIb3DQEHA6CAMIACAQAxggLWMIIBZwIBADCBzzCBvDELMAkGA
 ...........
AAAAAA==
```

### 0.1.3 Dokumentation


- Jalal Feghhi u.a.: Digital Certificates, Addison Wesley, 1999
- http://www.thunderbird-mail.de/wiki/Mailverschl%C3%BCsselung_mit_S/MIME

## 0.2 Gefahren im Internet

http://www.teltarif.de/arch/2004/kw49/s15585.html
http://www.heise.de/newsticker/meldung/42331
http://www.heise.de/newsticker/meldung/52776
http://www.heise.de/newsticker/meldung/52681
http://www.heise.de/newsticker/meldung/print/66308
http://en.wikipedia.org/wiki/Category:Malware
http://www.dfn-cert.de/
http://www.kefk.net/Windows/Update/index.asp

## 0.3 Software zur Absicherung Ihres PCs

ttp://www.uni-koeln.de/rrzk/kompass/99/k99.pdf
http://www.free-av.de/
http://www.download.com/3000-2092_4-10049526.html
http://download.zonelabs.com/bin/free/de/download/trial_zaFamily.html
ftp://ftp.netscape.com/pub/netscape7/german/
http://www.download.com/Ad-Aware-SE-Personal-Edition/3000-8022_4-10045910.html
ftp://ftp.cert.dfn.de/pub/tools/net/ssh/
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
http://prdownloads.sourceforge.net/nettime/NetTime-2b7.exe?download
http://www.xwin32.de
http://www.citrix.com/site/SS/downloads/index.asp
http://www.cygwin.com/mirrors.html
http://sshwindows.sourceforge.net/
http://www.prevx.com/prevxhome.asp

## 0.4 SPAM

- ... als Quelle von übervollen Mailboxen
- ... als Infizierungsherd (Viren, Trojaner)
- ... als Phishing-Versuch
- ...

Unter SPAM versteht man im „elektronischen Post“-Bereich die Versendung unerwünschter, unangeforderter Massenwurfsendungen (meist Werbung zweifelhafter Herkunft und oft auch zweifelhaften Inhalts). http://dict.leo.org?search=spam übersetzt

2 Treffer für 'spam'

| **ENGLISCH** | **DEUTSCH** |
|---|---|
| Spam©[Amer.] | das Frühstücksfleisch |
| spam [comp.] | elektronisches Äquivalent unerwünschter Wurfsendungen |

Abbildung 0.25: Quelle: http://dict.leo.org?search=spam

und http://www.nightflight.com/foldoc-bin/foldoc.cgi?query=spam erläutert

# spam

1. <messaging> (From Hormel's Spiced Ham, via the Monty Python "Spam" song) To post irrelevant or inappropriate messages to one or more Usenet newsgroups, mailing lists, or other messaging system in deliberate or accidental violation of netiquette.

It is possible to spam a newsgroup with one well- (or ill-) planned message, e.g. asking "What do you think of abortion?" on soc.women. This can be done by cross-posting, e.g. any message which is crossposted to alt.rush-limbaugh and alt.politics.homosexuality will almost inevitably spam both groups. (Compare troll and flame bait).

Posting a message to a significant proportion of all newsgroups is a sure way to spam Usenet and become an object of almost universal hatred. Canter and Siegel spammed the net with their Green card post.

If you see an article which you think is a deliberate spam, DO NOT post a follow-up - doing so will only contribute to the general annoyance. Send a polite message to the poster by private e-mail and CC it to "postmaster" at the same address. Bear in mind that the posting's origin might have been forged or the apparent sender's account might have been used by someone else without his permission.

The word was coined as the winning entry in a 1937 competition to choose a name for Hormel Foods Corporation's "spiced meat" (now officially known as "SPAM luncheon meat"). Correspondant Bob White claims the modern use of the term predates Monty Python by at least ten years. He cites an editor for the Dallas Times Herald describing Public Relations as "throwing a can of spam into an electric fan just to see if any of it would stick to the unwary passersby."

Usenet newsgroup: news.admin.net-abuse.

See also http://www.nightflight.com/foldoc-bin/foldoc.cgi?netiquette

2. (A narrowing of sense 1, above) To indiscrimately send large amounts of unsolicited e-mail meant to promote a product or service. Spam in this sense is sort of like the electronic equivalent of junk mail sent to „Occupant".

In the 1990s, with the rise in commercial awareness of the net, there are actually scumbags who offer spamming as a „service" to companies wishing to advertise on the net. They do this by mailing to collections of e-mail addresses, Usenet news, or mailing lists. Such practises have caused outrage and aggressive reaction by many net users against the individuals concerned

Abbildung 0.26: Quelle: http://www.nightflight.com/foldoc-bin/foldoc.cgi?query=spam

SPAM-Nachrichten sehen im allgemeinen folgendermaßen aus:

```
Received: from [217.223.62.15] (helo=web.com)
by mx09.web.de with smtp (WEB.DE(Exim) 4.93 #56)
id 18L4iM-0001M6-00; Sun, 08 Dec 2002 17:55:34 +0100
Message-ID: <000c63e43c8e$1361a2a2$2dd66ac6@dyssus>
From: "Steffi" <steffivf406@web.com>
To: Markus
Subject: Ich habe Dich vermisst!
Date: Mon, 09 Dec 2002 01:27:32 -0900
Sender: steffivf406@web.com

Hallo,
jemand der sich in dich verliebt hat aber sich nicht traut es dir persönlich zu
sagen hat eine Foto Nachricht für dich hinterlassen.

Wenn du wissen willst wer dir eine Nachricht hinterlassen hat, so gehe auf unsere
Seite und wähle die Nachricht mit der Nummer Pt-224885 und benutze das Kennwort:
Pt-224live

Solltest du unsere Livesoftware noch nicht installiert haben, kannst du das jetzt
machen indem du auf folgenden Link klickst:

http://213.76.131.85/?account=dkm-10129&layout=layoutdp4&land=de&exename=live-software

Du wirst dann automatisch in unseren Mitgliederbereich geleitet.

Viel Spaß

SH Partnervermittlung



WERBUNG
==
JETZT NEU: Private Kontakte aus Deiner Stadt
http://66.46.145.36/members/testzugang01/
==
```

Abbildung 0.27: SPAM-Nachrichten: Werbung

```
Return-Path: <m_bundu1@rediffmail.com>
Delivered-To:
Received: (qmail 29004 invoked by uid 4216); 8 Dec 2002 15:07:56 -0000
Received: from unknown (HELO 218.5.135.42) (218.5.135.42)
  by mail.telebel.de with SMTP; 8 Dec 2002 15:07:56 -0000
Received: from rly-xl04.mx.aol.com ([161.143.46.72]) by m10.grp.snv.yahoo.com with QMQP;
          Dec, 08 2002 6:43:00 AM -0700
Received: from 213.54.67.154 ([213.54.67.154]) by sparc.isl.net with esmtp;
Subject: Assistance
Sender: Michael Bundu <m_bundu1@rediffmail.com>

FROM: COL. MICHAEL BUNDU.
DEMOCRATIC REPUBLIC OF CONGO.
Tel No: Your country Intl. access code +8821652098236
email : mik_bundu1@rediffmail.com
Dear Sir/Madam


SEEKING YOUR IMMEDIATE ASSISTANCE.

Please permit me to make your acquaintance in so informal a manner. This is necessitated
by my urgent need to reach a dependable and trust worthy foreign partner. This request may
seem strange and unsolicited but I crave your indulgence and pray that you view it seriously.
My name is COL. MICHAEL BUNDU of the Democratic Republic of Congo and one of the close
aides to the former President of the Democratic Republic of Congo LAURENT KABILA of blessed
memory, may his soul rest in peace.

Due to the military campaign of LAURENT KABILA to force out the rebels in my country, I
and some of my colleagues were instructed by Late President Kabila to go abroad to purchase
arms and ammunition worth of Twenty Million, Five Hundred Thousand United States Dollars
only (US$20,500,000.00) to fight the rebel group. We were then given this money privately by
the then President, LAURENT KABILA, without the knowledge of other Cabinet Members. But
when President Kabila was killed in a bloody shoot-out by one of his bodyguards a day before
we were schedule to travel out of Congo, We immediately decided to put the funds into a private
security company here in Congo for safe keeping. The security of the said amount is presently
being threatened here following the arrest and seizure of properties of Col. Rasheidi Karesava
(One of the aides to Laurent Kabila) a tribesman, and some other Military Personnel from our
same tribe, by the new President of the Democratic Republic of Congo, the son of late President
Laurent Kabila, Joseph Kabila.
...
```

Abbildung 0.28: SPAM-Nachrichten: Bitte um Unterstützung

Häufig sind sie noch darüber hinaus falsch codiert oder aber mit unsinnigen Zeitangaben der Versendung versehen. Auf jeden Fall stimmt die Absendeadresse nicht.

```
Return-Path: <Marshamaxi@id.ru>
Delivered-To:
Received: (qmail 1197 invoked by uid 4216); 8 Dec 2002 16:11:46 -0000
Received: from unknown (HELO yuwpd) (200.160.248.74)
  by mail.telebel.de with SMTP; 8 Dec 2002 16:11:46 -0000
From: Elena Palik <Marshamaxi@id.ru>
To:
Subject: Information sven.b1
Date: Sun, 08 Dec 2002 07:10:44 -0500
Mime-Version: 1.0
Message-Id: <aounwrravnxv@id.ru>

PEhUTUw+PFAgQUxJRO49QOVOVEVSPjxGTO5UICBTSVpFPTYgUFRTSVpFPTIOPjxCPnN2ZW4u
YjEsPEJSPgOKPC9GTO5UPjxGTO5UICBDTOxPUj0iI2ZmMDAwMCIgQkFDSzOiI2ZmZmZmZiIg
c3R5bGU9IkJBQOtHUk9VTkQtQO9MT1I6ICNmZmZmZmYiIFNJWkU9NiBQVFNJWkU9MjQgRkFN
SUxZPSJTQU5TUOVSSUYiIEZBQOU9IkFyaWFsIiBMQU5HPSIwIj48VT5Zb3UgaGF2ZSBiZWVu
IGFwcHJvdmVkLjxCUj4NCjwvRk9OVD48Rk9OVCAgQO9MT1I9IiNmZjAwMDAiIEJBQOs9IiNm
ZmZmZmYiIHNOeWxlPSJCQUNLR1JPVU5ELUNPTE9SOiAjZmZmZmZmIiBTSVpFPTUgUFRTSVpF
PTE4IEZBTUlMWTOiUOFOU1NFUklGIiBGQUNFPSJBcmlhbCIgTEFORzOiMCI+PC9VPkNhc2gg
R3JhbnQgQW1vdW50OjxCUj4NCjwvRk9OVD48Rk9OVCAgQO9MT1I9IiMwMDAwZmYiIEJBQOs9
IiNmZmZmZmYiIHNOeWxlPSJCQUNLR1JPVU5ELUNPTE9SOiAjZmZmZmZmIiBTSVpFPTcgUFRT
SVpFPTM2IEZBTUlMWTOiUOFOU1NFUklGIiBGQUNFPSJBcmlhbCIgTEFORzOiMCI+JDEwLDAw
MCOkNSwwMDAsMDAwPEJSPgOKPC9GTO5UPjxGTO5UICBDTOxPUj0iIzAwMDAwMCIgQkFDSzOi
I2ZmZmZmZiIgc3R5bGU9IkJBQOtHUk9VTkQtQO9MT1I6ICNmZmZmZmYiIFNJWkU9NiBQVFNJ
WkU9MjQgRkFNSUxZPSJTQU5TUOVSSUYiIEZBQOU9IkFyaWFsIiBMQU5HPSIwIj48ST48VT5E
aWQgWW91IEtub3c/PEJSPgOKPC9GTO5UPjxGTO5UICBDTOxPUj0iIzAwMDAwMCIgQkFDSzOi
I2ZmZmZmZiIgc3R5bGU9IkJBQOtHUk9VTkQtQO9MT1I6ICNmZmZmZmYiIFNJWkU9NSBQVFNJ
WkU9MTggRkFNSUxZPSJTQU5TUOVSSUYiIEZBQOU9IkFyaWFsIiBMQU5HPSIwIj48LOI+PC9J
```

Abbildung 0.29: SPAM-Nachrichten: unbrauchbar, falsch codiert

Leider wird erst jetzt sehr zögerlich etwas vom Gesetzgeber und der Rechtssprechung gegen SPAM unternommen:

# US-Urteil gegen Spam-Versender

Über 98.000 US-Dollar soll der US-Amerikaner Jason Heckel für das Versenden von Spam-Mails bezahlen. Er verlor
das Berufungsverfahren vor dem obersten Gericht des Staates Washington. Zuvor hatte ein Richter eine einzige E-Mail als ausreichenden Beweis für Heckels illegale Spam-Aktivitäten gewertet. Die Anklage warf Heckel vor, seit 1998 zwischen 100.000 und einer Million unerwünschte Werbesendungen pro Woche verschickt zu haben.

Die eigentliche Strafe von 2000 US-Dollar dürfte Heckel dabei kalt lassen. Schließlich soll er jahrelang pro Monat dreißig bis fünfzig Exemplare seiner 46-seitigen Online-Broschüre "How to Profit from the Internet" verkauft haben, für die er in den Mails geworben hat. Doch zusätzlich muss er nun auch Gerichtskosten von über 96.000 US-Dollar tragen. Heckels Anwalt kündigte an, das Urteil anzufechten. Gelingt ihm dies nicht, dürfte es in den USA als Präzedenzfall eine ganze Welle von Klagen gegen Spam-Versender nach sich ziehen.

Washington erließ 1998 als erster US-Bundesstaat ein E-Mail-Gesetz. Es stellt Werbe-Mails mit irreführendem Inhalt oder einer Absenderadresse, auf die man nicht antworten kann, unter Strafe. Inzwischen haben aber auch andere US-Staaten ähnliche Gesetze erlassen. Das nährt die Hoffnung, dass in den USA, von wo auch sehr viele Spam-Mails nach Deutschland kommen, bald gegen die Verursacher der Plage vorgegangen wird.

Mit der Internet-Seuche Spam befasst sich c't in der aktuellen Ausgabe 22/02 unter anderem mit Artikeln über Anwender- und Administrationstools gegen unerwünschte Werbe-Mails und einem Report darüber, wer hinter deutschsprachigem Spam steckt. (ad/c't)

Abbildung 0.30: Quelle: heise online
`http://www.heise.de/newsticker/data/ad-20.10.02-002/`

Man beachte dabei, dass viele SPAM-Nachrichten auch HTML-Code verwenden. Dieser HTML-Code ist aber unter umständen recht unsicher und liefert i.a. eine Rückmeldung an den Absender, der diesen darüber informieren kann, eine Opfer-email-Adresse gefunden zu haben.
Gerade Newsreader wie Microsoft Outlook (Express) sind dabei besonders anfällig, da sie sich in den neueren Versionen nur noch schwer sicher konfigurieren lassen.
Bei diesen Newsreadern ist es wichtig,

1. die Vorschau zu deaktivieren (denn auch diese führt Skripte aus),
2. kein Öffnen von Nachrichten zweifelhaften Inhalts durchführen.

Im Zusammenhang mit Windows-Systemen ergeben sich daneben immer häufiger Probleme mit sogenannten Dialern, d.h. Programmen, welche im Hintergrund teure 0190-Telefonnummern anwählen:

## Bundesregierung will besseren Dialer- und Spam-Schutz

Das Verbraucherschutzministerium dringt auf ein schärferes Vorgehen gegen die Dialer-Mafia. „Wir sehen die 0190-Problematik als einen Schwerpunkt dieser Legislaturperiode“, erklärte Georg Starke, Leiter des Referats für den wirtschaftlichen Schutz der Verbraucher im Hause von Ministerin Renate Künast, am heutigen Donnerstag am Rande einer Konferenz zur europaweiten Harmonisierung des Wettbewerbsrechts in Berlin. Die zweite Änderung der Telekommunikations-Verbraucherschutzverordnung, die Netzbetreiber zum Einrichten kostenloser Service-Nummern verpflichtet und von vielen Seiten als unzweckmäßig kritisiert wurde, sei nur „ein erster Schritt“ gewesen. Weiter gehende Schutzmaßnahmen sollen laut Starke in die anstehende und von der Branche mit Spannung erwartete Novelle des Telekommunikationsgesetzes (TKG) einfließen, für die das Wirtschaftsministerium federführend verantwortlich ist.

Wie groß das Problem mit der Abzocke über 0190-Dialer im Internet oder der Werbespam für 0190-Nummern per SMS und E-Mail ist, erfährt das Verbraucherministerium ständig am eigenen Leib. „Wir erhalten täglich unzählige Eingaben und Beschwerden zu diesem Thema“, sagte Starke. „Sie pflastern uns den Schreibtisch zu.“ Momentan prüfe sein Haus noch zusammen mit dem Wirtschafts- und Justizressort, wie der Missbrauch effektiv einzudämmen ist. Konkret kann sich der Ministerialbeamte vorstellen, „verstärkt die Regulierungsbehörde für Telekommunikation und Post in die Verantwortung zu nehmen“ und so den schwarzen Schafen unter den Anbietern zu Leibe zu rücken. Bisher sind diese von den Netzbetreibern oft nur schwer zu ermitteln; eine effektive Datenbank mit einer Übersicht überdie einzelnen 0190-Dienstleister existiert nicht.

Auch im Bereich E-Mail-Spam sieht Starke Handlungsbedarf. „Bisher sind die ungewünschten Werbezusendungen nicht im Telekommunikationsgesetz erfasst“, bemängelt der Regierungsvertreter. Auch hier will das Verbraucherschutzministerium im Laufe der TKG-Novelle nachbessern. Ein großes Problem sieht Ursula Pachl vom Bureau Européen des Unions de Consommateurs, dem Dachverband der europäischen Verbraucherschutzorganisationen, allerdings nach wie vor bei internationalen Spam-Versendern, hauptsächlich aus den USA. Mit den Partnerschaftsverbänden jenseits des Atlantiks arbeite ihre Institution an einer Lösung. Über „Selbstregulierungsmaßnahmen“ der Wirtschaft gehen die Überlegungen bislang aber nicht hinaus.

Für die deutschen Wahrer der Konsumentenrechte ist die gesamte Thematik Spam und 0190-Nummern im vergangenen Jahr zum Dauerärgernis geworden. „Wir erleben einen zunehmenden Wildwuchs in der Werbung, der sich vor allem durch die Neuen Medien ergibt“, sagt Edda Müller, Vorstand Verbraucherzentrale Bundesverband (VZBV). Immer mehr Firmen würden teure 0190-Nummern verwenden, um bei den Verbrauchern „in wettbewerbswidriger Weise abzukassieren“. Zahlreiche Fälle seien aus der Gewinnspielwerbung bekannt oder im Zusammenhang des vermeintlichen „Abbestellens“ von unerwünschten kommerziellen Faxen.



Abbildung 0.31: Quelle: heise online
http://www.heise.de/newsticker/data/jk-31.10.02-006/

Der Konsument sei dagegen größtenteils machtlos, da sich die Möglichkeiten für Abmahnungen und Unterlassungserklärungen im Gesetz gegen den unlauteren Wettbewerb (UWG) als „zahnlos“ erweisen hätten. Selbst wenn eine Firma eindeutig eines Verstoßes gegen das UWG überführt worden sei, könnten die betroffenen Verbraucher keine Schadensersatzansprüche einklagen. Eine entsprechende Vorkehrung wollen die Verbraucherschützer nun aber im Rahmen der in Brüssel in den nächsten Wochen anstehenden Verhandlungen zur Harmonisierung des europäischen Wettbewerbrechts und des Grundbuchs zum Verbraucherschutz für alle Mitgliedsländer fordern. Eine „Strohmannklausel“ soll ferner verhindern, dass zwielichtige Anbieter unter Postfachadressen auf dem Markt auftreten können.

Mit der Internet-Seuche Spam befasst sich c’t in der Ausgabe 22/2002 unter anderem mit Artikeln über Anwender- und Administrationstools gegen unerwünschte Werbe-Mails und einem Report darüber, wer hinter deutschsprachigem Spam steckt. (Stefan Krempl) / (jk/c’t)

Abbildung 0.32: Quelle: heise online Fortsetzung
`http://www.heise.de/newsticker/data/jk-31.10.02-006/`

## Regierung legt Gesetzentwurf gegen 0190-Missbrauch vor

Die Bundesregierung hat einen ersten Referentenentwurf für das neue „Gesetz zur Bekämpfung des Missbrauchs von Mehrwertdiensterufnummern“ vorgelegt. Kernstück ist die geplante Änderung des Telekommunikationsgesetzes (TKG). Ein neuer Paragraf 43a soll jeden Anbieter, der eine 0190- oder 0136-0138-Nummer zur Nutzung überlassen bekommen hat, dazu verpflichten, eine ladungsfähige Anschrift bei der Regulierungsbehörde für Telekommunikation und Post (RegTP) zu hinterlegen.

Die RegTP selbst soll diese Angaben in Form einer Datenbank im Internet der Öffentlichkeit zugänglich machen. Außerdem soll jedermann einen Anspruch darauf haben, die Daten telefonisch erfragen zu können. Bei Verstoß gegen die Meldepflicht „kann die Zuteilung der Rufnummer durch die Regulierungsbehörde widerrufen werden“, heißt es im Gesetzentwurf. Von weiteren Sanktionierungsmaßnahmen wie etwa der Verhängung eines Bußgeldes findet sich, anders als noch im Konzeptpapier, nichts mehr im Gesetzentwurf.

Bei der Preiskappungsgrenze ist das Bundesministerium für Wirtschaft und Arbeit (BMWA) dagegen sogar noch weiter gegangen: Die Kosten für eine über frei tarifierbare Rufnummern abgerechnete Einwahl sollen demnach 30 Euro künftig nicht überschreiten dürfen. Vorgesehen waren hier zunächst 120 Euro pro Anruf. Wird entsprechend der Länge der Verbindung abgerechnet, soll das Entgelt auf zwei Euro pro Minute begrenzt werden. Abgerechnet werden soll mit einem Takt von einer Länge von maximal 60 Sekunden.

Hintergründe, erste Reaktionen und Einschätzungen zu dem Gesetzentwurf gegen 0190-Missbrauch finden sich im Artikel auf c’t aktuell:

Erster Gesetzentwurf gegen 0190-Missbrauch
`http://www.heise.de/ct/aktuell/data/hob-18.12.02-000/`

(hob/c’t)

Abbildung 0.33: Quelle: heise online
`http://www.heise.de/newsticker/data/hob-18.12.02-001/`

**Spam auf dem gerichtlichen Prüfstand**

Der Heise-Zeitschriften-Verlag, der die Zeitschriften iX und c't, das Online-Magazin Telepolis und den Newsdienst auf heise online herausgibt, klagt vor dem Amtsgericht Hannover gegen die Firma Online-Marketing Albrecht, nachdem diese Verlagsmitarbeiter trotz einer Unterlassungsaufforderung weiterhin mit Spam-E-Mails bombardiert hatte. Dabei beruft sich der Verlag unter anderem auf die neue EU-Datenschutzrichtlinie, in der für E-Mail-Werbung ein klares „Opt-in" bestimmt wird. Diese Richtlinie ist bis zum 31. Oktober 2003 in nationale Gesetzgebung umzusetzen, sollte aber bereits jetzt Einfluss auf die deutsche Rechtsprechung haben.

Unter dem Namen „emailfuchs" versendet Bernd Albrecht in Wellen unverlangt Werbe-E-Mails an deutsche Adressen. In den Newslettern wird für Webshops, beispielsweise einen Berufsbekleider und einen Uhrenhändler, geworben. ...

Der überzeugte Spammer hält es für rechtmäßig, unverlangte Werbe-E-Mails zuzusenden. Und: „Sie werden es nicht schaffen, unseren kostengüstigen und schnellen Newsletter-Versand an Millionen Leser zu blockieren", gab er sich kampfbereit. „Denken Sie daran, dass unsere Auflage weit höher ist als ihre", schrieb Albrecht und sprach von einer Pressekampagne mehrerer Verlage gegen ihn. Albrecht rechtfertigte sein Tun unter anderem unter ökologischen Gesichtspunkten: „Im Gegensatz zu den Printmedien müssen für unsere Informationen keine Bäume vernichtet werden, um eine Zeitung mit viel Werbung drucken zu müssen."

Nach Ansicht von Joerg Heidrich, Justiziar des Heise-Verlags, hat Albrecht freilich wenig Chancen, sein zweifelhaftes Anliegen vor Gericht durchzusetzen. Bis auf wenige Ausnahmen sei man inzwischen in Rechtssprechung und juristischer Literatur einhellig der Meinung, dass die unerwünschte und unaufgeforderte Zusendung von E-Mails rechtswidrig sei. Das Versenden solcher Nachrichten gegenüber Privatpersonen gilt dabei meist als Verletzung des allgemeinen Persönlichkeitsrechts des Betroffenen.

Unternehmen und Gewerbetreibende können sich auf einen Eingriff in den sogenannten „eingerichteten und ausgeübten Gewerbebetrieb" nach §§823, 1004 BGB berufen und ebenfalls Unterlassung verlangen. Ist der Empfänger der Spam-Mail darüber hinaus noch in einem ähnlichen Bereich gewerblich tätig wie der Versender, so steht ihm zusätzlich ein wettbewerbsrechtlicher Unterlassungsanspruch aus §1 UWG zu. Ein Anspruch auf Schadensersatz bei den Empfängern besteht dagegen nach bisheriger Rechtsprechung nicht. Insbesondere aufgrund der neuen EU-Richtlinie, die hinsichtlich unverlangter Werbezusendungen erstmals ein klares Verbot ausspricht, sieht Heidrich sehr gute Aussichten für die eingereichte Klage. (hob/c't)

Abbildung 0.34: Quelle: heise online
`http://www.heise.de/newsticker/data/hob-04.12.02-000/`

# EU-Richtlinie zum Datenschutz in Kraft

*[01.11.2003 10:40 ]*

Seit dem gestrigen Freitag haben Spammer es in Europa mit einer neuen Rechtslage zu tun: Nunmehr ist das Versenden von unverlangten E-Mails oder SMS-Botschaften in der gesamten **Europäischen Union[1]** illegal.

Die seit gestern geltende **Datenschutzrichtlinie[2]** für elektronische Kommunikation legt europäische Normen für den Schutz personenbezogener Daten und der Privatsphäre in der elektronischen Kommunikation fest. Sie enthält grundlegende Verpflichtungen, die die Sicherheit und Vertraulichkeit der Kommunikation über elektronische Netze in der EU gewährleisten sollen. Dies betrifft auch das Internet und mobile Dienste.

Insbesondere führt die Richtlinie ein EU-weites Spam-Verbot ein: Sofern sie nicht der Aufrechterhaltung einer bestehenden Kundenbeziehung dient, ist E-Mail-Werbung nur mit vorheriger Einwilligung der Adressaten gestattet. Vorgetäuschte Absender und ungültige Rückadressen, wie Spam-Versender sie häufig verwenden, sind verboten. Das Erfordernis einer verbindlichen vorherigen Einwilligung ("Opt-in") gilt ebenfalls für SMS-Botschaften und andere elektronische Nachrichten, die an ein mobiles oder festes Endgerät gesendet werden. Die EU-Mitgliedstaaten können auch unerbetene elektronische Werbepost an Unternehmen verbieten.

Des weiteren dürfen unsichtbare Verfahren der Nachverfolgung, mit denen Informationen über Internetnutzer gesammelt werden können, nur verwendet werden, wenn der Nutzer deutliche Informationen über den Zweck einer solchen unsichtbaren Aktivität und das Recht erhält, diese abzulehnen. Das betrifft etwa sogenannte Spyware, aber auch den Einsatz von Cookies.

Standortdaten, die von Mobiltelefonen erzeugt werden, dürfen vom Netzbetreiber nur mit ausdrücklicher Einwilligung des Nutzers weiterverwendet oder weitergegeben werden. Einzige Ausnahmen betreffen die Übermittlung der Standortdaten an Notdienste sowie an Strafverfolgungsbehörden. Für letztere gelten strenge Voraussetzungen - sie dürfen solche Daten nur anfordern, sofern dies Zwecken der nationalen Sicherheit oder Ermittlungen in Strafrechtssachen dient.

Ab heute müssen die Mitgliedstaaten diese Regeln anwenden und wirksam durchsetzen. Die Richtlinie enthält jedoch keine rechtsverbindlichen Bestimmungen, die Maßnahmen der Mitgliedstaaten gestatten oder verhindern würden, welche die Speicherung von Verkehrs- oder Standortdaten für Strafverfolgungszwecke erfordern, da dies außerhalb ihres Geltungsbereichs liegt. Doch müssten solche Maßnahmen mit Vorkehrungen zum Schutz der Menschenrechte einhergehen, die in der Richtlinie ausgeführt werden.

Eine unmittelbare Rechtwirkung für die betroffenen Unternehmen und Bürger ergibt sich allerdings aus der EU-Richtlinie nicht. Diese richtet sich zunächst nur an die Mitgliedsstaaten, welche die Regelungen in nationales Recht umzusetzen haben. Dies hat die Bundesregierung bis zum gestrigen Stichtag allerdings versäumt. Geplant ist eine nationale Umsetzung der Richtlinie im Rahmen der Reform des Wettbewerbsrechts (UWG), welche jedoch nicht vor dem nächsten Frühjahr zu erwarten ist. Nach der derzeitigen **Planung[3]** enthält jedoch auch das neue UWG keine direkte

Abbildung 0.35: E-Mail: Maßnahmen gegen SPAM in der EU

**Was tun gegen Spam (`http://spam.trash.net/was.shtml`)?**

Unter http://spam.trash.net/tun.shtml ist erläutert, wie Sie Spam in Zukunft vermeiden können, was Sie tun können, wenn Sie bereits spam erhalten haben, ...

- Auf keine Fall sollten Sie den Aufforderungen der Spam-Nachrichten nachkommen.
- Die Spam-Nachrichten sollten sofort gelöscht werden. Bei nur wenigen Nachrichten reicht oft noch das manuelle Löschen.
- Da die Spam-Mails immer mit neuen Absenderadressen auftauchen, helfen Einträge in lokale Filterlisten oft sehr wenig. Bei der Filterung nach Stichworten (z.B. Sex, Porno, etc.) werden leider auch gerne reguläre e-mails ausgefiltert. ...

**Filtern im Netscape-Communicator:**

- Eine Netscape Filterbeschreibung finden Sie unter

  `http://www.thunderbird-mail.de/wiki/Junk-Filter_verwenden,_um_Spam_zu_filte`
- Für Outlook Express vergleiche http://www.inboxprotector.com/.

**Weitere Informationen finden Sie zum Beispiel unter:**

- SPAM-Klassifikator der Uni-Wuppertal:

  http://www.hrz.uni-wuppertal.de/dienste/netz/email/spam/spam-filter.html
- http://www.antispam.de/
- Information zum Thema Spam

  (`http://spam.trash.net/index.shtml`)
- DFN-CERT Informationsbulletin Spam

  (`http://www.cert.dfn.de/infoserv/dib/dib-9901.html`)
- Ratgeber Kampf gegen Spam

  (`http://www.wienerzeitung.at/aktuell/2001/antispam/default.htm`)
- HRZ-Anti-Spam an der BU Wuppertal

  (`http://w3.uni-wuppertal.de/hrz/infos/hrz-info/hrz-info-9806/node16.html`)
- Spam (Auflistung von anderen Spam-Seiten)

  (`http://directory.google.com/Top/Computers/Internet/Abuse/Spam/`)
- Reading Email Headers (`http://www.stopspam.org/email/headers.html`)

- Uni Bremen: Maßnahmen gegen SPAM
  (http://www.zfn.uni-bremen.de/zfn/dienste/mail/anti-spam.php3 )
- http://www.schnappmatik.de/TFFFFF/
- Uni Köln: Electronix Mail am RRZK: Spam
  (http://www.uni-koeln.de/rrzk/mail/spam/)
- Uni Köln: Spamassassin am RRZK
  (http://www.uni-koeln.de/rrzk/mail/spam/spamassassin.html)

## Gericht untersagt den Versand unverlangter Newsletter-Aktivierungsmails

Nach den Anbietern von Grußkarten könnte es nun auch den Versendern von Online-Newslettern an den Kragen gehen. Nach Auffassung des Landgerichts Berlin stellt die unerwünschte Übersendung einer Newsletter-Anmeldung per E-Mail eine unzulässige Werbung dar.

Der Antragsteller des Beschlusses vom 19. September 2002 hatte eine E-Mail erhalten, in der er aufgefordert wurde, einen Aktivierungslink anzuklicken, um in einen Newsletter-Verteiler aufgenommen zu werden. Sofern er dies nicht wolle, solle er die Mail einfach löschen. Hierin sah der Antragsteller unerwünschte Werbung und beantragte den Erlass einer einstweiligen Verfügung gegen den Betreiber des Informationsservices.

Das Landgericht bestätigte in seiner Entscheidung nochmals die mittlerweile herrschende Auffassung, dass es sich bei dem unaufgeforderten Zusenden einer E-Mail mit Werbeinhalten gegenüber Gewerbetreibenden um einen unzulässigen Eingriff in den Gewerbebetrieb handelt. Privatpersonen steht unter den Gesichtspunkten des allgemeinen Persönlichkeitsrechts gegen den Versender der Mail ebenfalls ein Unterlassungsanspruch nach §§1004, 823 Abs. 1 BGB zu.

Die Einwendung des Newsletter-Betreibers, der Antragsteller hätte die Eintragung für die Mailingliste selbst vorgenommen, ließ das Gericht nicht gelten. Nachweispflichtig für die Eintragung in eine Liste sei stets der Betreiber des Angebotes. Diesen Beweis konnte der Anbieter jedoch nicht führen. Der Beschluss ist unter Juristen umstritten. Die der Entscheidung zugrundeliegende Art des Opt-In-Verfahrens bei der Anmeldung zum Bezug eines Newsletters ist im Internet weit verbreitet und galt bisher als rechtlich unbedenklich. (Joerg Heidrich) / (em/c't)

Abbildung 0.36: Quelle: heise online
`http://www.heise.de/newsticker/data/em-02.11.02-000`

## Spam-Versender muss sieben Millionen Dollar zahlen

**AOL ist vor einem Gericht in Virginia ein wegweisendes Kunststück gelungen: Erfolgreich klagte das Unternehmen einen pornografischen Spam-Versender in den Bankrott. Das Urteil, hoffen Millionen, könnte Schule machen.**

CN Productions kennt niemand, und doch haben Millionen Internet-Nutzer schon Post des Unternehmens im E-Mail-Empfangsordner gehabt. CN machte seine Profite mit Spam, unverlangt zugesandten Werbebotschaften. Das Unternehmen des bereits 1999 einschlägig verurteilten Jay Nelson gehörte zu den Pionieren des wohl meistgehassten Geschäftszweiges im Internet: pornografische Massenmailings.

Zum wohl endgültigen Verhängnis wurde Nelsons Firma nun ein Gesetz des US-Staates Virginia, das als Muster für den zunehmend härter geführten juristischen Kampf gegen die Müllversender gilt: Wegen Verstoßes gegen Auflagen des ersten Urteils wurde CN Productions zur Zahlung von sieben Millionen Dollar an AOL als geschädigtes Unternehmen verurteilt. Für den Pornowerber ist das der Ruin, und doch ist es fast ein mildes Urteil: Das Gesetz des Staates Virginia sieht Geldstrafen von bis zu 25.000 Dollar für einen Spambrief vor. Davon verschickte CN Productions allein an AOL-Adressen mehrere Milliarden.

Für AOL ist das ein wichtiger Sieg, von dem das Unternehmen erhofft, dass er Signalwirkung haben möge. AOL litt über Jahre unter dem Ruf, einerseits Heimat von Spam-Versendern zu sein, anderseits die eigenen User nicht davor schützen zu können.

Das Problem sind die E-Mail-Verzeichnisse von AOL, die von Spamern immer wieder gern „abgefischt“ werden: Mehr verifiziert gültige Adressen lassen sich kaum auf einen Schlag besorgen. Nutzer von AOL oder auch des Instant Messenger AIM konnten ein Lied davon singen: Es rappelte im Postfach. Heute dagegen liegt das AOL-Spam-Aufkommen sogar unter dem Durchschnitt. Der liegt - je nach Schätzung - mittlerweile bei 25 bis 50 Prozent.

AOL geht seit spätestens 1998 vehement gegen Spamer und ihre Aussendungen vor: „Wir haben die Schnauze so voll davon wie unsere Kunden“, sagte damals AOL-Chef Steve Case - und topfte ein Programm von Gegenmaßnahmen ein, die von Filtern über Rausschmisse und gerichtliche Klagen bis hin zu öffentlichen Prangern reichte. Schon 1998 landete CN Productions auf der AOL-Liste der zehn „meistgesuchten Spamer“. Vier Jahre später hat AOL seinen Peiniger erlegt, das Kopfgeld kassiert.

Abbildung 0.37: Quelle: Spiegel Online
`http://www.spiegel.de`

## IETF gründet Anti-Spam-Arbeitsgruppe

Die Internet Engineering Task Force (IETF), eine der bedeutendsten Organisationen für Internet-Standards, will das Problem der immer größer werdenden Flut an unerwünschten E-Mails jetzt an der Wurzel packen: Im Rahmen des Forschungszweigs der IETF wurde eine Arbeitsgruppe namens Anti-Spam Research Group (ASRG) gegründet.

Bestehende Anti-Spam-Lösungen setzen nach Ansicht der ASRG-Mitglieder zu spät an, nämlich erst dann, wenn eine unerwünschte Nachricht bereits auf dem Server des Empfängers angekommen ist. Ziel der jetzt begonnenen Forschungen ist zunächst eine Machbarkeitsstudie, in der geprüft werden soll, ob man solche Nachrichten nicht bereits im Vorfeld unterdrücken und so auch die Netzwerk-Belastung verringern kann. Erreichen will man das mit einem Satz an Protokollen und Frameworks unter dem Stichwort „consent-based communication“ (zustimmungsbasierte Kommunikation). So sollen potenzielle Nachrichtenempfänger in die Lage versetzt werden festzulegen, welche Art von Mitteilungen sie überhaupt empfangen wollen. Dazu soll auch eine Möglichkeit gehören, Absender von Nachrichten zu identifizieren, die sich solchen Übereinkünften widersetzen.

Die Mitglieder der ASRG wollen sich zum ersten Mal im Rahmen des 56. IETF-Meetings zusammensetzen, das vom 16. bis zum 21. März dieses Jahres in San Francisco stattfindet. Wann mit ersten Ergebnissen zu rechnen ist und ob die Arbeit in einem offiziellen Standard münden wird, ist noch völlig offen. (hos/c't)

Abbildung 0.38: Quelle: heise online
`http://www.heise.de/newsticker/data/hos-01.03.03-000/`

## Künast: Schärferes Gesetz gegen Spam im Herbst

Eine Art große Koalition bildet sich gegen unverlangt eingesandte Werbe-Mail und ihre Versender heraus: Nachdem CDU/CSU bereits forderte, Spammer zur Kasse zu bitten und die SPD am vergangenen Freitag „Wege aus der Vermüllung“ suchte, geht Verbraucherschutzministerin Renate Künast (Grüne) mit Ankündigungen neuer Gesetzesinitativen in die Öffentlichkeit. Die Versender unerwünschter Werbe-Mails im Internet müssen sich auf drastische Gegenmaßnahmen einstellen, verspricht Künast. Im Herbst werde der Bundestag eine Gesetzesverschärfung beschließen, wonach E-Mail-Werbung nur noch mit vorheriger Zustimmung des Empfängers verschickt werden darf, sagte der Berliner Zeitung. Gewinne, die unter Verstoß gegen diese Bestimmung erzielt werden, könnten dann bei dem betroffenen Unternehmen eingezogen werden.

Künast setzte sich ebenfalls für internationale Vereinbarungen gegen so genannte Spam-E-Mails ein. „Das könnten zum Beispiel Mindeststandards für Provider sein“, sagte Künast. „Es ist ein klassischer Dienst am Kunden, unverlangte E-Mails auszufiltern.“ Nur Anbieter mit einem solchen Service würden sich langfristig am Markt halten können. Künast reagiert mit der Ankündigung des neuen Gesetzes allerdings nur auf bereits beschlossene EU-Regelungen: Die Europäische Union hat bereits vor einem Jahr eine Richtlinie gegen Spam erlassen. Darin wird eine Opt-in-Regelung verlangt. „Die Bekämpfung des Spammings geht uns alle an und ist mittlerweile zu einem Hauptaspekt des Internet geworden“, hatte Erkki Liikanen, EU-Kommissar für die Informationsgesellschaft, betont, als er die EU-Staaten daran erinnerte, dass sie bis Ende Oktober die Richtlinie in nationales Recht umzusetzen müssten. (jk[7]/c't)

Abbildung 0.39: Quelle: heise online
`http://www.heise.de/newsticker/data/jk-21.07.03-000/`

### Aktuelle Vertiefung

http://www.heise.de/newsticker/meldung/65358
http://www.heise.de/newsticker/meldung/62780
http://www.heise.de/newsticker/meldung/65896
Gray Lists

## 0.5 Konfiguration einer Netzwerkkarte

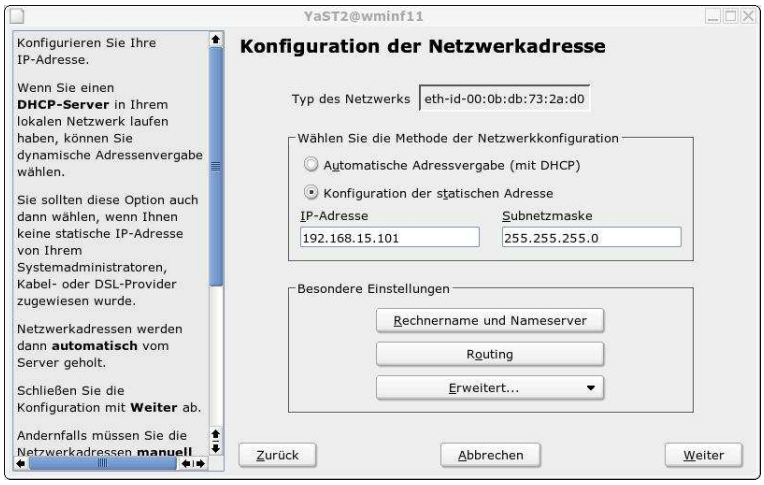



Abbildung 0.40: Konfiguration einer Netzwerkkarte 1

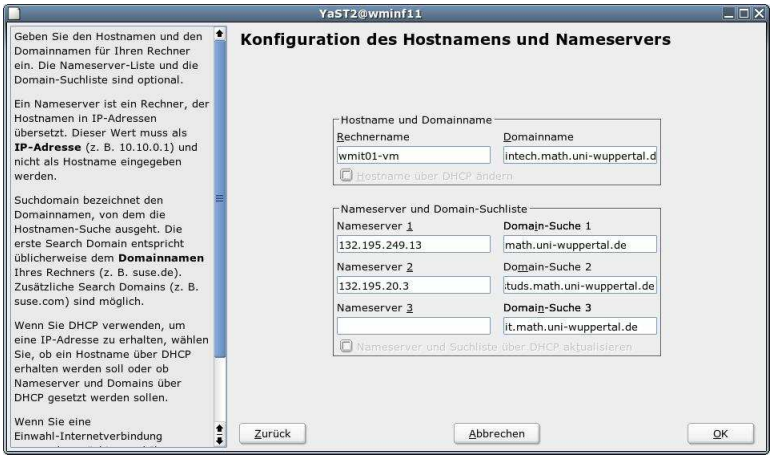



Abbildung 0.41: Konfiguration einer Netzwerkkarte 2

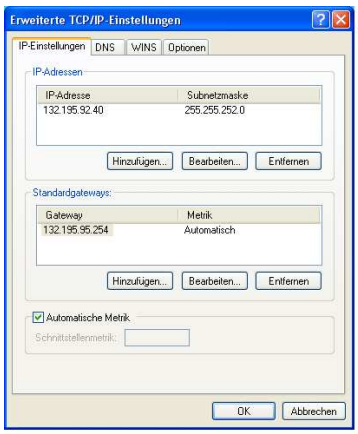



Abbildung 0.42: Windows-Konfiguration einer Netzwerkkarte 1

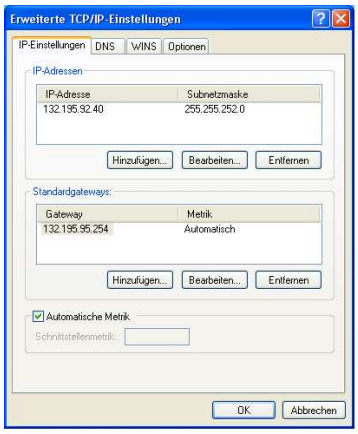



Abbildung 0.43: Windows-Konfiguration einer Netzwerkkarte 2

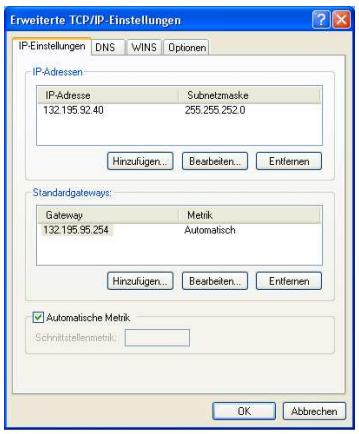



Abbildung 0.44: Windows-Konfiguration einer Netzwerkkarte 3


Abbildung 0.45: Windows-Konfiguration einer Netzwerkkarte 4

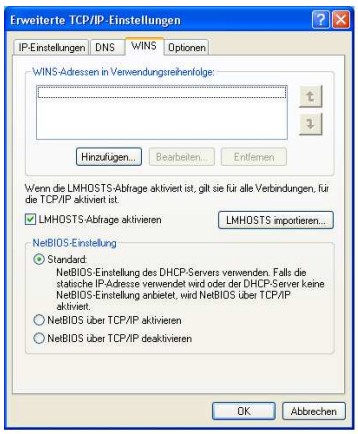



Abbildung 0.46: Windows-Konfiguration einer Netzwerkkarte 5

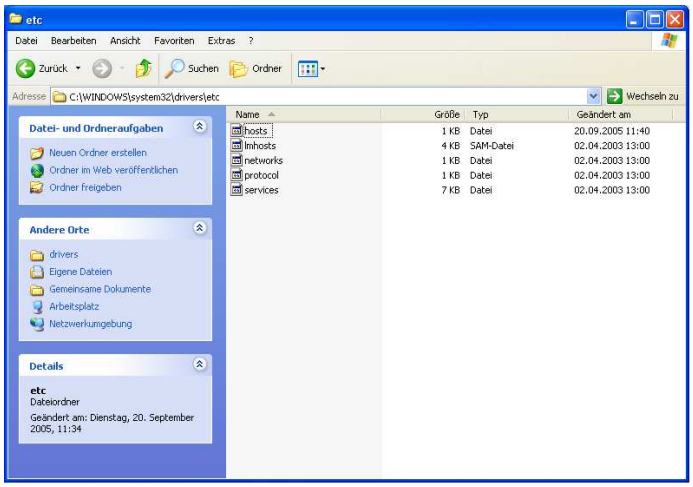
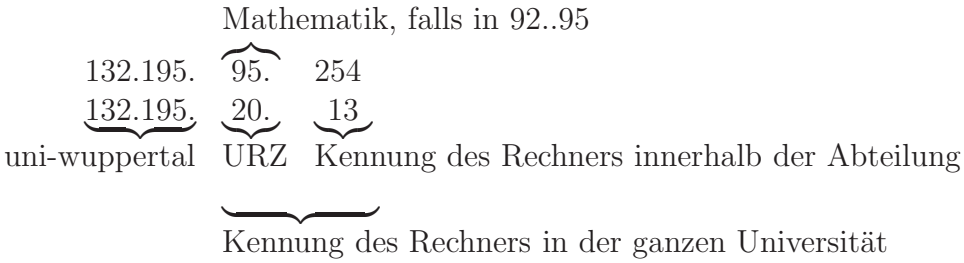


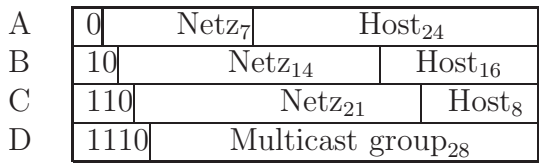

Abbildung 0.47: Windows etc-Dateien

## 0.6 IP-Adressen und Subnetze

Beispiele von IP-Adressen:




IP-Adressen gemäß IPv4 werden mit 4*8 Bit (je 0..255) angegeben. Man unterscheidet dabei 4 verschiedene Netztypen:




Damit ergeben sich dann folgende IP-Adressen in den verschiedenen Netzen

| | |
|---|---|
| A | 0.0.0.0 .. 127.255.255.255 |
| B | 128.0.0.0 .. 191.255.255.255 |
| C | 192.0.0.0 .. 223.255.255.255 |
| D | 224.0.0.0 .. 239.255.255.255 |

132.195.x.x ist also ein Class B Netz mit bis zu $2^{16} = 65.536$ verschiedenen Host-Adressen. Zwei Hostadressen dienen dabei für Sonderzwecke:

| | |
|---|---|
| 132.195.0.0 | Netzwerkadresse für das gesamte Netzwerk |
| 132.195.255.255 | Broadcast (Damit kann ein Datenpaket an alle Rechner dieses Netzes gesendet werden.) |

Weiter Sonderadressen:

Es gibt zusätzliche Adressen, die nicht international eindeutig sind. Sie werden für weitere Sonderzwecke (loopback_interface), automatische „private“ Adressvergabe auf Windows XP-Rechnern, HP-Netzwerkdruckern,... verwendet:

| | | |
|---|---|---|
| A | 127.0.0.1 | das sogenannte loopback interface, damit wird also nur der eigene Rechner angesprochen (auch `localhost`) |
| B | 169.254.x.x | private Netze für Apple/Microsoft (APIPA=automatic private IP addressing) |
| | 172.16.x.x<br>...<br>172.31.x.x | für 16 private Netze reserviert, z.B. Intranet (keine Kommunikation ins Internet über diese Internetadressen) |
| C | 192.168.0.x<br>...<br>192.168.255.x | 256 private Netze |

### IPv6 oder auch IPng

Dieser Standard benutzt 128 Bit lange Adressen. Dies behebt den großen Mangel an IP-Adressen im Internet. Z.B.

47CD:12AB:CDEF:1234:000A:000B:000C:ABCD

Dies sind 8*16 Bit = 128 Bit = 16 Byte
Weitere Beispiele entnehmen Sie der folgenden Datei

```
#
# hosts         This file describes a number of hostname-to-address
#               mappings for the TCP/IP subsystem.  It is mostly
#               used at boot time, when no name servers are running.
#               On small systems, this file can be used instead of a
#               "named" name server.
# Syntax:
#
# IP-Address  Full-Qualified-Hostname  Short-Hostname
#

127.0.0.1 localhost

# special IPv6 addresses
::1             localhost ipv6-localhost ipv6-loopback

fe00::0         ipv6-localnet

ff00::0         ipv6-mcastprefix
ff02::1         ipv6-allnodes
ff02::2         ipv6-allrouters
ff02::3         ipv6-allhosts

127.0.0.2       linux.local  linux
```

### 0.6.1 Netzwerkmasken und Subnetze

Subnetze werden zur Unterteilung etwa eines Class B-Netzwerkes in kleinere Unternetze benutzt:

132.195.92.0 ... 132.195.95.255

ist ein IP-Adressbereich, der für die Rechner der Fachgruppe Mathematik benutzt wird. der Netzverkehr (inklusive Broadcasts) dieser Rechner untereinander bleibt auf diesen Teilbereich beschränkt.

Rechner z.B. im Subnetz der Fachgruppe Physik können diesen Netzverkehr nicht „mithören“. Damit wird eine höhere Netzwerksicherheit erreicht. Zusätzlich belasten Datentransfers innerhalb des Mathematik-Subnetzes nicht die Netzwerkkapazität der anderen Subnetzwerke.

Zur Erzeugung von solchen Subnetzen dienen sogenannte Netzmasken:

| Class | default Netzmaske |
|---|---|
| A | 255.0.0.0 |
| B | 255.255.0.0 |
| C | 255.255.255.0 |

Die Netzmaske hat denselben Aufbau wie eine IP-Adresse. Bei ihr bedeutet jede binäre Bitstelle, ob das stellengleiche Bit der IP-Adresse zur Netzwerkkennung (wenn 1) oder zur Hostkennung gehört.

Um also 132.195.92 ... 132.195.95 im selben (Sub-)Netzwerk zu platzieren, muss die Netzmaske

| | | |
|---|---|---|
| $92_{10}$ | = | $0101\ 1100_2$ |
| $93_{10}$ | = | $0101\ 1101_2$ |
| $94_{10}$ | = | $0101\ 1110_2$ |
| $95_{10}$ | = | $0101\ 1111_2$ |
| Maske | | $1111\ 1100_2 = 252_{10}$ |

zu 255.255.252.0 gewählt werden.

Wenn Sie einen Rechner

132.195.83.1

mit der Netzmaske 255.255.248.0 installieren, heißt das also, dass ein Subnetzwerk mit der Netzkennung

$$132.195.83.1\ \mathrm{AND}_{\mathrm{bitweise}}\ 255.255.248.0{=}132.195.80.0$$

und der Broadcastadresse

$$132.195.83.1\ \mathrm{OR}_{\mathrm{bitweise}}\ 0.0.7.255{=}132.195.87.255$$

im Fachbereich Elektrotechnik benutzt wird. (Dabei geht 0.0.7.255 durch bitweises Komplement aus 255.255.248.0 hervor.)

Einen Ausschnitt der innerhalb der Universität Wuppertal benutzten Subnetze kann unter

http://www.hrz.uni-wuppertal.de/dienste/netz/subnetze/

gefunden werden:

**Vertiefung:**
http://en.wikipedia.org/wiki/Subnetwork
http://en.wikipedia.org/wiki/Classes_of_IP_addresses
http://en.wikipedia.org/wiki/Classless_inter-domain_routing
http://en.wikipedia.org/wiki/IPv4
http://en.wikipedia.org/wiki/IPv6

| **Fachbereich** | **Domain/ Subnetze** | **Gateway** | **Netzmaske** |
|---|---|---|---|
| FB 1<br>Gesellschafts-<br>wissenschaften | gewil<br>132.195.1 | 132.195.20.201 | 255.255.192.0 |
| FB 2<br>Geschichte, Philo-<br>sophie, Theologie | geistwi<br>132.195.2 | 132.195.20.201 | 255.255.192.0 |
| FB 3<br>Erziehungswissen-<br>schaften | erziwi<br>132.195.3 | 132.195.20.201 | 255.255.192.0 |
| FB 4<br>Sprach- und<br>Literaturwissen-<br>schaften | lingu<br>132.195.4 | 132.195.20.201 | 255.255.192.0 |
| FB 5<br>Design, Kunst, Druck<br>(Gaußstr. | kunst<br>132.195.5 | 132.195.20.201 | 255.255.192.0 |
| FB 5<br>Computational Design<br>(Hofaue) | kunst<br>132.195.65 | 132.195.65.254 | 255.255.255.0 |
| FB 5<br>Design, Kunst, Druck<br>(PKS) | kunst<br>132.195.68 | 132.195.71.253 | 255.255.252.0 |
| FB 5<br>Kommunikations-<br>technologie Druck<br>(Campus Freudenberg) | kommtech<br>132.195.88 | 132.195.89.254 | 255.255.254.0 |
| FB 6<br>Wirtschaftswissen-<br>schaft | wiwi<br>132.195.6<br>132.195.38 | 132.195.20.201 | 255.255.192.0 |
| FB 7<br>Mathematik | math<br>132.195.92<br>⋮<br>132.195.95 | 132.195.95.254 | 255.255.252.0 |
| | ⋮ | | |

Abbildung 0.48: Subnetzstruktur an der BU Wuppertal

## 0.7 Domain Name Services

<networking> (DNS) A general-purpose distributed, replicated, data query service chiefly used on Internet for translating hostnames into Internet addresses. Also, the style of hostname used on the Internet, though such a name is properly called a fully qualified domain name. DNS can be configured to use a sequence of name servers, based on the domains in the name being looked for, until a match is found.

The name resolution client (e.g. Unix's gethostbyname() library function) can be configured to search for host information in the following order: first in the local /etc/hosts file, second in NIS and third in DNS. This sequencing of Naming Services is sometimes called *name service switching*. Under Solaris is configured in the file /etc/nsswitch.conf.

DNS can be queried interactively using the command nslookup. It is defined in STD 13, RFC 1034, RFC 1035, RFC 1591.

BIND is a common DNS server.
(Zitat: FOLDOC)

Siehe auch http://en.wikipedia.org/wiki/Domain_Name_System.

*/etc/nsswitch.conf:*

```
# /etc/nsswitch.conf
#
# An example Name Service Switch config file. This file should
# sorted with the most-used services at the beginning.
#
# The entry '[NOTFOUND=return]' means that the search for an
# entry should stop if the search in the previous entry turned
# up nothing. Note that if the search failed due to some other reason
# (like no NIS server responding) then the search continues with the
# next entry.
passwd: compat
group:  compat
hosts:          files lwres dns
networks:       files dns
services:       files
protocols:      files
rpc:            files
ethers:         files
netmasks:       files
netgroup:       files
publickey:      files
```

```
 bootparams:     files
automount:      files nis
aliases:        files
```

*/etc/resolv.conf:*

```
nameserver 132.195.249.13
domain studs.math.uni-wuppertal.de
nameserver 132.195.20.3
search studs.math.uni-wuppertal.de math.uni-wuppertal.de uni-wuppertal.de
```

*Der Vorgang der Namensauflösung:*

```
> nslookup ftp.netscae.com
Server:         132.195.249.13
Address:        132.195.249.13#53

Non-authoritative answer:
ftp.netscape.com        canonical name = ftp.gftp.netscape.com.
Name:   ftp.gftp.netscape.com
Address: 64.12.204.22

> nslookup www.uni-wuppertal.de
Server:         132.195.249.13
Address:        132.195.249.13#53

www.uni-wuppertal.de    canonical name = w4.urz.uni-wuppertal.de.
Name:   w4.urz.uni-wuppertal.de
Address: 132.195.129.2
```

Now our application is presented with www.cranzgot.co.za. The following sequence of lookups takes place to resolve this name into an IP address. This procedure is called host name resolution and the algorithm that performs this operation is called the resolver.

- The application checks certain special databases on the local machine. If it can get an answer directly from them, it proceeds no further.
- The application looks up a geographically close name server from the local machine's configuration file. Let's say this machine is called ns.
- The application queries ns with www.cranzgot.co.za?.
- ns determines whether that IP has been recently looked up. If it has, there is no need to ask further, since the result would be stored in a local cache.
- ns checks whether the domain is local. That is, whether it is a computer about which it has direct information. In this case, this would only be true if the ns were cranzgot.co.za's very own name server.
- ns strips out the TLD (top level domain) .za. It queries a root name server, asking what name server is responsible for .za. The answer will be ucthpx.uct.ac.za of IP address 137.158.128.1.
- ns strips out the next highest domain co.za. It queries 137.158.128.1, asking what name server is responsible for .co.za. The answer will be secdns1.posix.co.za of IP address 160.124.112.10.

- ns strips out the next highest domain cranzgot.co.za. It queries 160.124.112.10, asking what name server is responsible for cranzgot.co.za. The answer will be pizza.cranzgot.co.za of IP address 196.28.123.1.

- ns queries 196.28.123.1 asking for the IP address of www.cranzgot.co.za. The answer will be 160.123.176.1.

- ns returns the result to the application.

- ns stores each of these results in a local cache with an expiration date, to avoid having to look them up a second time.

(Zitat: http://www.math.mcgill.ca/lebaron/rute/rute/node30.html)

Ländercodes als TLDs: http://www.unc.edu/~rowlett/units/codes/country.htm

Vermietete Länder-Domains: http://www.heise.de/newsticker/meldung/37604 und http://www.nic.de.vu/

Neue TLDs: http://www.heise.de/newsticker/meldung/43122

.eu:
http://www.heise.de/newsticker/meldung/43302
...
http://www.heise.de/newsticker/meldung/67050

Internationale Domain-Namen:
http://www.heise.de/newsticker/meldung/32001,
http://www.heise.de/newsticker/meldung/45057,
http://en.wikipedia.org/wiki/Puny_code

... und ihre Gefahren:
http://en.wikipedia.org/wiki/Phishing#Phishing_techniques,
http://www.heise.de/newsticker/meldung/56110

Internationale Zeichensätze auch in E-Mail-Adressen:
http://www.heise.de/newsticker/meldung/42296,
http://www.heise.de/newsticker/meldung/66099

*Handel* mit Domain-Namen:
http://www.heise.de/newsticker/meldung/43784,
http://www.heise.de/newsticker/meldung/67059

Ein symbolischer Name für *wechselnde* IP-Adressen: dynDNS
http://en.wikipedia.org/wiki/Dynamic_dns

Vertiefung: Ein eigener DNS-Server im privaten Netz
http://www-uxsup.csx.cam.ac.uk/pub/doc/suse/suse9.3/suselinux-adminguide_en/cha.dns.html

Informationstypen:

```
> nslookup
> www.uni-wuppertal.de
Server:         132.195.249.13
Address:        132.195.249.13#53

www.uni-wuppertal.de    canonical name = w4.urz.uni-wuppertal.de.
Name:   w4.urz.uni-wuppertal.de
Address: 132.195.129.2
```

```
> 132.195.95.1
Server:         132.195.249.13
Address:        132.195.249.13#53

1.95.195.132.in-addr.arpa       name = wmai01.math.uni-wuppertal.de.
```

```
> set type=mx
> uni-wuppertal.de
Server:         132.195.249.13
Address:        132.195.249.13#53

uni-wuppertal.de        mail exchanger = 20 mail2.urz.uni-wuppertal.de.
uni-wuppertal.de        mail exchanger = 20 mail1.urz.uni-wuppertal.de.
```

```
> set type=ns
> uni-koeln.de
Server:         132.195.249.13
Address:        132.195.249.13#53

Non-authoritative answer:
uni-koeln.de    nameserver = mail1.rrz.uni-koeln.de.
uni-koeln.de    nameserver = ws-lei1.win-ip.DFN.de.
uni-koeln.de    nameserver = ns2.netcologne.de.
uni-koeln.de    nameserver = noc2.rrz.uni-koeln.de.

Authoritative answers can be found from:
noc2.rrz.uni-koeln.de   internet address = 134.95.129.23
mail1.rrz.uni-koeln.de  internet address = 134.95.100.208
ws-lei1.win-ip.DFN.de   internet address = 193.174.75.162
```

# 1 Das Internet: Dienste und Informationen

Das Internet stellt vielfältige Dienste und Informationen bereit:

- E-Mail (pop, imap, smtp, MIME)
- (E-Mail-)Adressbücher (ldap)
- WWW (http)
- Usenet-News (nntp)
- Dateiendownload (ftp)
- Zeitsynchronisation (ntp)
- entferntes Arbeiten (ssh, telnet)
- ...

```
Jeder Dienst hat eine eigene ihn adressierende
ganze Zahl,die Portnummer, die man z.B. in folgender Datei
nachlesen kann:\\

cat /etc/services

#
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, most entries here have two entries
# even if the protocol doesn't support UDP operations.
#
# This list could be found on:
#            http://www.iana.org/assignments/port-numbers
#
# (last updated 2004-02-12)
#
```

```
# The port numbers are divided into three ranges: the Well Known Ports,
# the Registered Ports, and the Dynamic and/or Private Ports.
#
# The Well Known Ports are those from 0 through 1023.
#
# The Registered Ports are those from 1024 through 49151
#
# The Dynamic and/or Private Ports are those from 49152 through 65535
#
#
### UNASSIGNED PORT NUMBERS SHOULD NOT BE USED.  THE IANA WILL ASSIGN
# THE NUMBER FOR THE PORT AFTER YOUR APPLICATION HAS BEEN APPROVED ###
#
#
# WELL KNOWN PORT NUMBERS
#
# The Well Known Ports are assigned by the IANA and on most systems can
# only be used by system (or root) processes or by programs executed by
# privileged users.
#
# Ports are used in the TCP [RFC793] to name the ends of logical
# connections which carry long term conversations.  For the purpose of
# providing services to unknown callers, a service contact port is
# defined.  This list specifies the port used by the server process as
# its contact port.  The contact port is sometimes called the
# "well-known port".
#
# To the extent possible, these same port assignments are used with the
# UDP [RFC768].
#
# The range for assigned ports managed by the IANA is 0-1023.
#
# Port Assignments:
#
# Keyword         Decimal    Description                     References
# -------         -------    -----------                     ----------
#                 0/tcp    Reserved
#                 0/udp    Reserved
#                          Jon Postel <postel@isi.edu>
tcpmux            1/tcp    # TCP Port Service Multiplexer
tcpmux            1/udp    # TCP Port Service Multiplexer
#                          Mark Lottor <MKL@nisc.sri.com>
compressnet       2/tcp    # Management Utility
compressnet       2/udp    # Management Utility
```

```
compressnet       3/tcp    # Compression Process
compressnet       3/udp    # Compression Process
#                          Bernie Volz <VOLZ@PROCESS.COM>
#                 4/tcp    # Unassigned
#                 4/udp    # Unassigned
rje               5/tcp    # Remote Job Entry
rje               5/udp    # Remote Job Entry
#                          Jon Postel <postel@isi.edu>
#                 6/tcp    # Unassigned
#                 6/udp    # Unassigned
echo              7/tcp    Echo
echo              7/udp    Echo
#                          Jon Postel <postel@isi.edu>
#                 8/tcp    # Unassigned
#                 8/udp    # Unassigned
discard           9/tcp    # Discard
discard           9/udp    # Discard
#                          Jon Postel <postel@isi.edu>
#                10/tcp    # Unassigned
#                10/udp    # Unassigned
systat           11/tcp    users        # Active Users
systat           11/udp    users        # Active Users
#                          Jon Postel <postel@isi.edu>
#                12/tcp    # Unassigned
#                12/udp    # Unassigned
daytime          13/tcp    # Daytime (RFC 867)
daytime          13/udp    # Daytime (RFC 867)
#                          Jon Postel <postel@isi.edu>
#                14/tcp    # Unassigned
#                14/udp    # Unassigned
netstat          15/tcp    # Unassigned [was netstat]
#                15/udp    # Unassigned
...
ssh              22/tcp    # SSH Remote Login Protocol
ssh              22/udp    # SSH Remote Login Protocol
#                          Tatu Ylonen <ylo@cs.hut.fi>
telnet           23/tcp    # Telnet
telnet           23/udp    # Telnet
#                          Jon Postel <postel@isi.edu>
#                24/tcp    any private mail system
#                24/udp    any private mail system
#                          Rick Adams <rick@UUNET.UU.NET>
smtp             25/tcp    mail         # Simple Mail Transfer
smtp             25/udp    mail         # Simple Mail Transfer
```

```
#                               Jon Postel <postel@isi.edu>
#                  26/tcp       # Unassigned
...
```

## 1.1 Historie: Uucp und das Internet

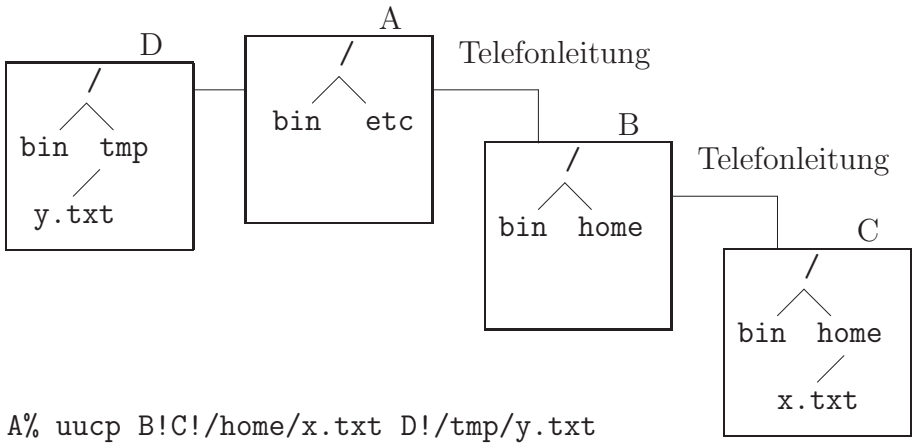
Topologie des Wissenschaftsnetzes in Europa:

- Geant
- Geant2
- G-WiN

```
traceroute to ftp.gftp.netscape.com (207.200.66.55), 30 hops max, 40 byte packets
 1  math-gw (132.195.95.254)  0.939 ms  0.749 ms  0.534 ms
 2  transfer0.lan.uni-wuppertal.de (132.195.254.254)  1.480 ms  1.217 ms  1.175 ms
 3  cr-essen1.x-win.dfn.de (188.1.17.97)  2.830 ms  2.745 ms  3.607 ms
 4  cr-leipzig1-po11-0.x-win.dfn.de (188.1.18.106)  18.622 ms  18.736 ms  18.728 ms
 5  cr-frankfurt1-po10-0.x-win.dfn.de (188.1.18.189)  27.243 ms  26.953 ms  26.416 ms
 6  so-6-0-0.ar2.FRA2.gblx.net (208.48.23.141)  26.932 ms  26.885 ms  26.927 ms
 7  so6-0-0-2488M.ar1.FRA2.gblx.net (67.17.74.150)  26.864 ms  27.483 ms  27.009 ms
 8  pop2-frr-S7-0-1.atdn.net (66.185.149.225)  27.112 ms  27.062 ms  27.117 ms
 9  bb2-frr-S0-0-0.atdn.net (66.185.139.18)  27.448 ms  27.570 ms  26.960 ms
10  bb1-new-P4-0.atdn.net (66.185.152.146)  158.953 ms  116.518 ms  116.697 ms
11  bb1-ash-P13-0.atdn.net (66.185.152.48)  118.351 ms  118.281 ms  118.387 ms
12  bb1-sjg-P7-0.atdn.net (66.185.153.59)  176.113 ms  176.064 ms  176.089 ms
13  bb1-ntc-P5-0.atdn.net (66.185.152.62)  177.019 ms  176.729 ms  176.619 ms
14  pop1-ntc-P0-0.atdn.net (66.185.142.113)  176.593 ms  176.856 ms  176.619 ms
15  cor1-nc1-P2-1.atdn.net (66.185.142.158)  178.131 ms  177.829 ms  176.452 ms
16  *
```

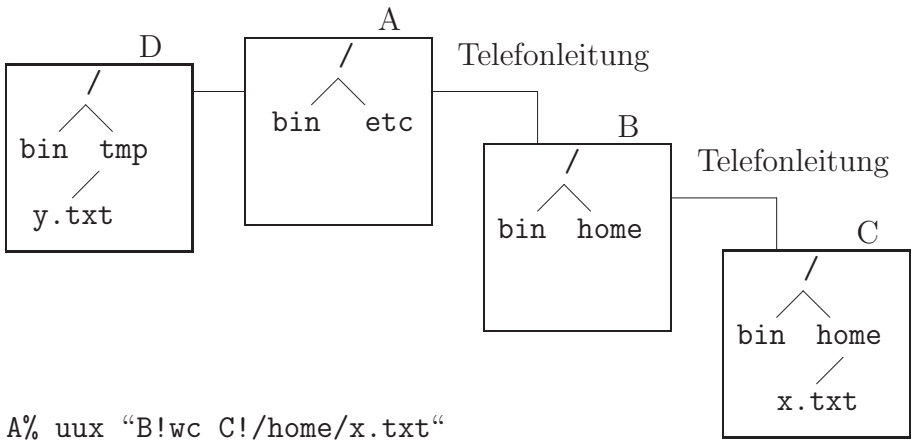
Vorläufer des Internets (http://www.internetworldstats.com/stats.htm) war die Verbindung verschiedener Universitäts- und Militärrechner mit Hilfe von Einwahlverbindungen über Telefonleitungen: das UUCP-Netz. Er stellte folgende Dienste bereit:

- uucp



(unix to unix copy: zum Kopieren von Dateien zwischen zwei (entfernten) Rechnern)

- uux




(unix to unix execute: zum Ausführen von Kommandos auf fremden Rechnern mit Dateien auf (nochmals) fremden Rechnern)

- E-Mail

  wird relyed (stationsweise weitergereicht), benutzt uucp

- Usenet Netnews

  Diskussionsforen werden ebenfalls relyed (2001 mit einem Datendurchsatz von ca. 1,1 GB/Tag)

Die Lage eines Rechners (relativ zum eigenen Rechner) wird als Rechnername benutzt, dieser ist also topologieabhängig:

Jeder Zielrechner wird auf unterschiedlichen Rechnern durch einen anderen “Pfad“ angesprochen. Nach einem Ausfall von nur einem Rechner, kann derselber Rechner vielleicht über einen anderen Pfad immer noch angesprochen werden, aber diesen Pfad muss man erst erfragen. Das ist im Internet nicht praktikabel, weshalb dort internetweite eindeutige Rechnernamen eingeführt wurden: die IP-Adressen.

## 1.2 Secure by Default

- http://en.wikipedia.org/wiki/Secure_by_default
- http://www.windowsitpro.com/Windows/Article/ArticleID/39808/39808.html
- http://opensolaris.org/os/community/security/projects/sbd/sbd_toi.pdf

## 1.3 Firewall-geschützte Dienste von extern nutzen / Dienstzugangspunktverlegung

Mittels *Port-Forwarding* kann man auch nur auf Subnetze beschränkte Dienste von außen nutzen, sofern man sich auf einem Subnetzrechner mittels **ssh** (secure shell) anmelden kann:

```
ssh -L 10000:ldapintern.uni-wuppertal.de:389 \
       username@l01.studs.math.uni-wuppertal.de
```

erlaubt so vom Internet aus das (geschützte) universitätsinterne E-Mail-Adressverzeichnis
http://www.hrz.uni-wuppertal.de/dienste/netz/email/ldap_bu.html
zu erreichen.

Weitere Beispiele:

```
ssh -L 8888:lsrv0.studs.math.uni-wuppertal.de:443 l01.studs.math.uni-wuppertal.de
...
ssh -R 8120:192.168.15.120:80 username@wmit16v
```

**Vertiefung:**

http://www.ssh.com/support/documentation/online/ssh/adminguide/32/Port_Forwarding.html

## 1.4 Dynamic host configuration protocol

Siehe: http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

**Vertiefung:**

- dhcp FAQ
- Die Ausleiehe einer Internetadresse
- rfc2131

## 1.5 Internet protocol version 6

Siehe: http://en.wikipedia.org/wiki/Internet_Protocol_Version_6
Die Vorteile von IPv6:

größerer Adressraum (128 Bit je Adresse)]

Autokonfiguration (nearest neighbourhood discovery, plug-and-play)

Roaming

QoS

IPsec intrinsisch

Multicasting/Anycast intrinsisch

Kompatibilität zu IPv4

...

## 1.6 Publizieren des x-x509-email-cert's

http://www.vpas.fsnet.co.uk/wot/publish_cert.html oder „Die Benutzung von `openssl` zur Extrahierung des E-Mail-Zertifikats aus der Sicherheitsdatenbank".

**Links:**

- S/MIME mit OpenPGP
- http://www.kes.info/archiv/online/01-01-60-SMIMEvsOpenPGP.htm
- http://www.trustcenter.de/569.htm

## 1.7 Firewalls

- http://en.wikipedia.org/wiki/Firewall_%28networking%29
- SuSEfirewall2
- SuSEfirewall2 Manual
- http://www.mtiweb.com/isp/ciscoacc.html

## 1.8 NAT

- NAT beispielhaft erklärt
- http://de.wikipedia.org/wiki/Network_Address_Translation
- NAT Traversal
- IPsec and NAT
- ISO/OSI 7-Schicht-Modell
- ARP, IP, TCP, ...

## 1.9 VPN / IPsec

- Cisco VPN Client FAQ
- Remote Access VPN
- Site to Site VPN
- VPN-Funktionalität
- SSL
- Microsoft und SSL-VPNs
- OpenVPN
- Openswan

# 2 Mehr Sicherheit auf dem Computer

## 2.1 uuencode und uudecode

uuencode

http://foldoc.org/?uuencode

## 2.2 base64

http://foldoc.org/?Base+64

base64

OpenSSL Tricks

Text-Codierungen von Binärdateien

base64-Verfahren

## 2.3 md5

Message Digest

openssl dgst -md5

one-way hash function

md5-Algorithmus

md5sum

## 2.4 GPG/PGP und die Dateicodierung/ -Signierung

GPG-Tutorial

### 2.4.1 Lokales (symmetrisches) Verschlüsseln

GPG

OpenSSL

### 2.4.2 Schlüssel für die asymmetrische Verschlüsselung/Signierung

Schlüsselerzeugung

Web of Trust

Keyserver

### 2.4.3 Signieren (Beglaubigen) von Dateien

Signatur

### 2.4.4 Verschlüsseln einer Datei für ...

Vertraulichkeit

### 2.4.5 Sicherung eines Schlüsselpaars, ...

Key Backup

gpgme-Bibliothek

kgpg

PGP S/MIME

gpgsm - S/MIME mit gpg

gpg: Aegypten

kde kleopatra-Handbuch

X.509 und kleopatra

# 3 (Semi-)Professionelle Benutzung des Internets

## 3.1 Internet-Radio — Web-Radio

http://de.wikipedia.org/wiki/Internetradio

## 3.2 VoIP / Internet-Telefonie

IP-Telefonie

### 3.2.1 Der Rechner als Telefon / das Telefon als Rechner

VoIP

IP-Telefonie

SIP

Session Initiation Protocol

Real Time Transport Protocol

### 3.2.2 VoIP-Provider

Übersicht

Konfigurationsdaten (am Beispiel von `twinkle`)

Partnernetze von VoIP-Anbietern

### 3.2.3 SIP-Servertypen — die Technik

prinzipieller SIP-Protokollverlauf

IP Telephony Cookbook (nur die Abschnitte ber SIP relevant)

### 3.2.4 Gateways Festnetz zu den VoIP-Inseln

Rufnummern im Festnetz

032-Rufnummern

032 Auskunft

### 3.2.5 ENUM-Lookup

Verfahren

Telefonnummern-Abbildung

denic-Registratur für ENUM-Domains

Was ist ENUM

ENUM center.de

ENUM on snom phones

ökonomische Notwendigkeit von ENUM-Datenbanken

### 3.2.6 Ein SIP Software-Telefon: twinkle

Twinkle Homepage

### 3.2.7 VoIP-Sicherheit

Sicherheit?

RTSP FAQ

TLS und RTSP

STUN, TURN und ICE

ICE in Windows

IAX

## 3.3 ssh mit Schlüsseln: ssh-keygen, ssh-agent, ssh-add,...

### 3.3.1 pubkey Authentifizierung

http://www.rrze.uni-erlangen.de/ausbildung/kolloquien/ssh-13-05-2002.pdf

### 3.3.2 ssh-agent

http://www.arches.uga.edu/ pkeck/ssh/
http://www-106.ibm.com/developerworks/library/l-keyc2/

### 3.3.3 hostbased Authentifizierung für cron-Jobs

http://www.snailbook.com/faq/trusted-host-howto.auto.html

### 3.3.4 Ausblick: ssh mit VPN-Funktionalität

http://www.heise.de/newsticker/meldung/69122

## 3.4 Ausblick: Web-Services

### 3.4.1 RPC-Middleware

http://www.ipd.uka.de/ dyngeb/topics/versys.html
http://www.vs.inf.ethz.ch/edu/WS0304/VS/slides/Vorl.VertSys03_04_8a.pdf
http://www.cs.wustl.edu/ schmidt/PDF/docwc.pdf

### 3.4.2 Web-Services

http://www.w3schools.com/xml/xml_whatis.asp
http://www.w3schools.com/xsl/
http://en.wikipedia.org/wiki/Web_Services

### 3.4.3 RESTFUL Web-Services

http://java.sun.com/developer/technicalArticles/WebServices/restful/