

Internet-Grundlagen für Anwender

Günter Marxen

Vorwort

Die vorliegende Kurzanleitung versucht, die Funktioneweise des Internets zu erläutern, ergänzt um einige Tipps für Einsteiger. Konstruktive Kritik und Hinweise zu Erweiterungen sind willkommen.

Die „Modification History“ (s. *Änderungen in:*) soll dem Benutzer die Entscheidung erleichtern, ob es sich lohnt, eine neue Version der Anleitung komplett oder ggf. in Teilen zu drucken.

Im universitären und schulischen Bereich darf der Text als Ganzes ausgedruckt und z.B. in Kursen benutzt werden. Ebenso ist die private Nutzung erlaubt. Kommerzielle Nutzung, Textänderungen oder Verteilung der Anleitung ohne Titelblatt und Vorwort sind untersagt!

Textteile dürfen in Mitteilungen o.ä. universitärer oder schulischer Einrichtungen unter Angabe von Autor und Version abgedruckt werden. Wird der Text teilweise nachgedruckt oder in Kursen o.ä. eingesetzt, so bitte ich um eine kurze Mitteilung per E-Mail (Adresse s. *Kontakt*). Im Übrigen verbleiben alle Rechte beim Autor.

Der Text wurde in meiner Freizeit erstellt und ist als Acrobat-Datei bei „Einführungen“ zu finden unter: <http://www.uni-koeln.de/rrzk/kurse/unterlagen/>.

Die Anleitung wurde mit **Sun StarOffice**, die pdf-Datei mit **Adobe Acrobat Distiller** erstellt.

Kontakt für Anregungen, Hinweise und Anfragen: guenter@marxen.de

1. Ausgabe: Version 1.00/12.2001

Änderungen in:

Version 2.00/01.2003: Vollständige Überarbeitung und Ergänzung des Textes.

Inhaltsverzeichnis

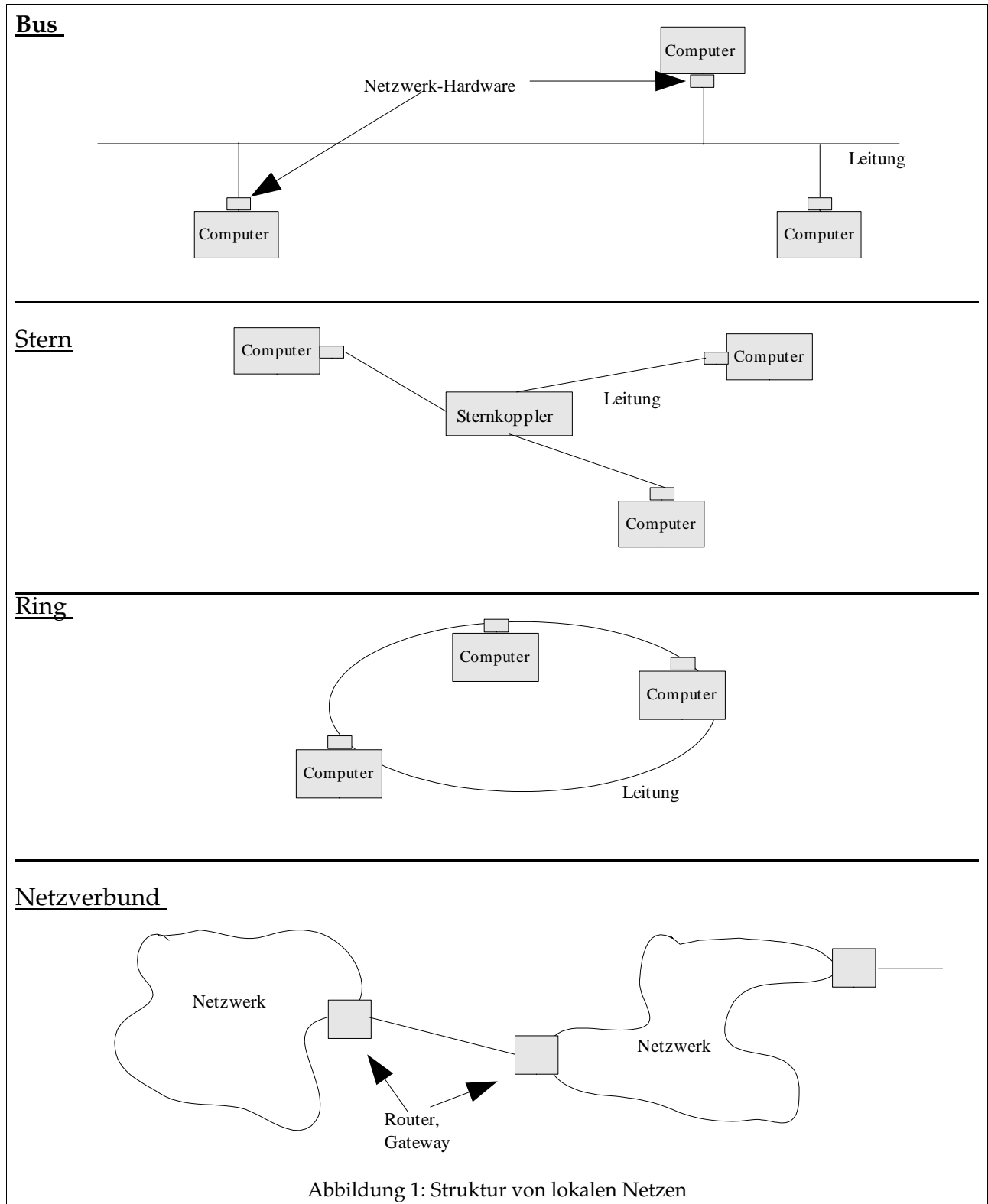
Internet-Technik	1
Netzwerk (Computer-Netz, LAN, WAN)	1
Rechnerkommunikation	2
Schichtenmodell am Beispiel des Internets mit dem TCP/IP-Protokoll (sog. DoD-Schichten)	2
Protokoll	3
Client / Server-Architektur	4
Das Internet	4
Internet- und Host-Adressen (IP-Adressen)	4
Host-Namen und Domain Name Server (DNS)	5
Zugang zum Internet	6
Provider	6
Netiquette – Umgangsformen im Internet	7
Internet-Sicherheit	7
Viren	7
Dialer	7
Trojaner oder Backdoors	7
Schutzmaßnahmen	8
Virens Scanner	8
Personal Firewall	8
Anti-Dialer	8
Allgemeine Sicherheits-Tipps	8
Sicherer surfen mit dem Internet Explorer	9
Sicherer Mailen mit Outlook Express	9
Internet-Dienste	10
E-Mail	10
Aufbau einer E-Mail	10
E-Mail-Adressen	11
POP3 und IMAP	11
Web-Mail	12
E-Mail-Umleitung	12
Mailinglisten	12
Postmaster – der Chef im PostOffice	13
Tipps für E-Mailer	13
Emoticons	13
Abkürzungen	13
WWW - Das World Wide Web	14
HTML-Text	14
URL – WWW-Adressen	15
Suchdienste	15
Browser	15
Net News – Usenet	15
Sonstiges	16
Stichwortverzeichnis.....	17

Internet-Technik

Netzwerk (Computer-Netz, LAN, WAN)

Ein Netzwerk verbindet Computer über (Verbindungs-) Leitungen mit Hilfe von Spezial-Hardware wie Netzwerkkarten, Routern ("Weiterleitungsrechnern") etc. Die passende Software (Computer-Programm) "verpackt" die Nutzdaten (Anfragen, Informationen etc.) in Daten-Pakete und leitet sie (mit Hilfe der Hardware) nach bestimmten Regel von einer (Zwischen-) Station zur nächsten bis zum Empfänger weiter.

Netz-Topologie: Struktur des Netzes, Bus-, Stern-, Ring-Struktur. Netzverbund: Übergang zwischen Netzen.



- **Bus-Struktur:** Jeder Rechner ist an eine „durchgehende“ Leitung angehängt.
- **Stern-Struktur:** Jeder Rechner ist mit einer "Zentrale" (*Hub* oder *Switch*) verbunden.
- **Ring-Struktur:** Ein Rechner ist mit dem nächsten verbunden, der letzte wieder mit dem ersten.
- **Netzverbund:** Einzelne Netze werden über Spezialrechner (Gateways, Router) miteinander verbunden. Das Internet ist ein Verbund vieler unterschiedlicher Netze, die nach bestimmten Regeln, dem *Protokoll* TCP/IP, miteinander kommunizieren, Daten austauschen und transportieren.

Ein Netzwerk umfasst:

- **Rechner,** PCs, Arbeitsplatzrechner und Server für Daten, Programme, Mail, WWW-Seiten.
- **Leitungen** (Koaxkabel, 2-Drahtleitung (Twisted Pair), Lichtleiter, Funkstrecke u.a.)
- **Spezialhardware** (Netzwerkkarte, „Router“, „Gateway“ u.a.)
- **Software** (Steuerung des Datenaustauschs zwischen den Rechnern, „Protokoll“)

Begriffe

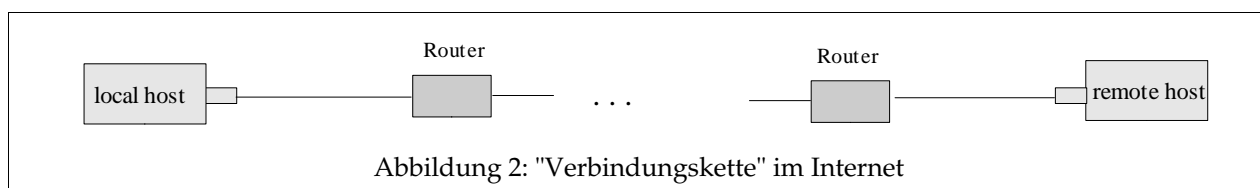
- **LAN:** Local Area Network, Netzwerk mit „lokaler“ Ausdehnung, z.B. Vernetzung von PCs im Büro, oder auch in der Universität zu Köln (UKLAN: Universität zu Köln LAN).
- **WAN:** Wide Area Network. Netzwerk für Fernverbindungen.

Rechnerkommunikation

Zwei Rechner, z.B. Ihr PC und ein WWW-Server im Internet, kommunizieren im Netz bzw. im Netzverbund, indem ein "lokaler" Rechner (*local host*, Ihr Rechner) Daten, z.B. Ihre "Anfrage" durch Klick auf eine Adresse im Netscape Browser, auf die Leitung absetzt, die über viele Zwischenstationen (Router oder Gateways, spezialisierte Rechner etc.) "von Punkt zu Punkt" gehend schließlich beim "entfernten" Rechner (*remote host*, z.B. bei www.uni-koeln.de) ankommen.

Die bei der Kommunikation zu übertragenden Datenmengen werden in kleine Datenpakete aufgeteilt, die durchnummeriert und je nach Netzbelastung über unterschiedliche Wege im Netzverbund übertragen werden. Ein Datenpaket enthält u.a. Absender- und Empfänger-Adresse, die Sequenz- oder Paketnummer und eine (Fehler-) Prüfsumme sowie die zu übertragenden "Nutzdaten". Beim Zielrechner können die Datenpakete wegen der unterschiedlichen Wege in beliebiger Reihenfolge ankommen. Sie werden dort anhand der (Sequenz-) Nummern in die richtige Reihenfolge gebracht und zur übertragenen Information zusammengesetzt. Kommt ein einzelnes Paket nicht fehlerfrei an, so fordert der Zielrechner das Paket unter Angabe seiner Nummer erneut an.

Alle beteiligten Rechner müssen bei der Übertragung der Datenpakete die vereinbarten Regeln (*Protokolle*, im Internet TCP/IP: Transport Control Protocol/Internet Protocol) beachten. Grundsätzlich werden die Datenpakete im gesamten Netzwerk verbreitet und (i.a. nur) vom adressierten *remote host* aufgenommen.



Das „Transportmodell“ (es beschreibt die Transportregeln und -funktionen – die Regeln und Funktionen der Übertragung von Signalen und Daten) ist in „Schichten“ unterteilt, die jeweils einen Teil der „Transportarbeit“ erledigen, wobei höhere Schichten die Dienste (Funktionen) der darunter liegenden benutzen. So wie beim Telefonieren auf der untersten (Hardware-) Ebene Leitungen, Vermittlungsstellen u.a. die elektrischen Signale transportieren und auf der obersten Ebene der Benutzer mit seinem Partner spricht.

Anmerkung: Mit einem „trace route“-Programm, z.B. dem Programm *Ping Plotter*, können die verschlungenen Wege durch's Internet verfolgt werden. Sie geben einen Server, z.B. www.microsoft.com an, und können den Weg der Datenpakete durch's Internet mit „Reisezeit“ auf den einzelnen Etappen auf dem Bildschirm sehen (z.B. um zu prüfen, warum die Antwort auf eine Anforderung an einen Server so lange dauert). Die Version 1.0 können Sie als (kostenlose) freeware von <http://www.pingplotter.com/files.html> herunterladen.

Schichtenmodell am Beispiel des Internets mit dem TCP/IP-Protokoll (sog. DoD-Schichten)

Meist wird zur Darstellung der Funktionsebenen eines Netzwerks das ISO-Schichtenmodell benutzt, das mit 7 Schichten differenzierter ist, als das hier dargestellte „Internet-Schichtenmodell“ (Tabelle 1). Zur

Erläuterung der Internet-Dienste ist das hier benutzte Modell aber ausreichend, bei dem von unten (Hardware) nach oben (Kommunikationsfunktion) die Funktionshierarchie dargestellt ist.

- 1. Netzzugriff:** Auf der untersten „physikalischen“ Ebene (Hardware) werden die Signale (elektromagnetische Wellen, Lichtimpulse etc.) von „Punkt zu Punkt“ (d.h. von einer Station zur nächsten, s. Abb. 2) übertragen. Die physikalische Realisierung der Datenpakete hängt von der Art der benutzten „Leitung“ und der darauf abgestimmten Netzwerk-Hardware (z.B. Netzwerkkarte des PCs) ab: Wellenpakete, Licht-, Funk- oder Laserimpulse etc. Zudem wird auf der untersten Ebene die Fehlerkontrolle - korrekte und vollständige Datenpaketübertragung und Flusskontrolle (Sender darf nicht schneller als Empfänger arbeiten) für die Punkt-zu-Punkt-Verbindung durchgeführt. Damit ist gesichert, dass Daten fehlerfrei von einer Station zur nächsten über den Netzverbund gehen können.

4. Prozess, Applikation	<i>Dienst</i>	Dateitransfer	E-Mail	Terminal	WWW
	<i>Protokoll</i>	ftp	SMTP	Telnet Protocol	HTTP
3. Host-to-Host	TCP (Transmission Control Protocol)				
2. Internet	ARP (Address Resolution)		IP (Internet Protocol)		
1. Netzzugriff, lokales Netzwerk	Spezifische Netzwerktechnik: Ethernet, Token Ring, FDDI etc.				
	"Netzwerkleitung": Doppelader, Koaxkabel, Lichtwellenleiter, Funkstrecke etc.				

Tabelle 1: Internet-Schichtenmodell

- 2. Internet (Netzwerkschicht):** Auf der nächsthöheren Ebene 2, der „Internetschicht“, wird „der Weg durch das Internet“ über alle möglichen Zwischenstationen vom local host zum remote host gewählt, also z.B. von Ihrem Rechner zu dem gewünschten Web-Server, etwa zu www.uni-koeln.de. Damit werden einzelne Datenpakete über viele Stationen weitergeleitet. Hierfür werden die in den Datenpaketen enthaltenen (Netz-) Adressen aufgelöst (ARP: Address Resolution Protocol) und die Pakete von Punkt zu Punkt über die beste Verbindung „zwischen den Netzen“ (Internet) zum Empfänger weitergegeben (Routing und Lastüberwachung).

Rechner- oder Netz-Adressen: Eindeutige Nummern im Netzwerk (-Verbund).

- 3. Host-to-Host oder Transport-Schicht:** "Host" ist ein Rechner im Netz. Diese Schicht überwacht die korrekte Übertragung der Datenpakete zwischen den beiden kommunizierenden End-Rechnern *local host* und *remote host* (Fehler- und Flusskontrolle): Fehlerfreiheit der Pakete (Prüfsumme), Reihenfolge und Vollständigkeit (Sequenznummern). Diese beiden Funktionen entsprechen denen der 1. Schicht *Netzzugriff*, beziehen sich aber nicht auf die jeweilige Punkt-zu-Punkt-Verbindung sondern auf die beiden End-Rechner.

- 4. Applikation (Anwendungsschicht):** Die unteren 3 Schichten sind die „eigentlichen“ Netzwerk-(Transport-) Schichten. Die Internet-Anwendungen (Internet-Dienste) nutzen diese Schichten bzw. deren Transport-Mechanismen für die eigentlichen Informations-Dienste. Für jeden Dienst gilt dabei wieder ein eigenes Regelwerk, ein eigenes Protokoll: Dateiübertragung (**ftp**: File Transfer Protocol), Elektronische Post (**E-Mail**, SMTP Simple Mail Transfer Protocol), Terminal (Telnet) und **WWW** (HTTP: Hyper Text Transfer Protocol), **Network News** (NNTP: Network News Transfer Protocol). (Es gibt weitere Internet-Dienste, die hier nicht erwähnt werden.)

Da die Kommunikation stattfindet zwischen den beiden Hosts, die je nur *eine* eindeutige Adresse haben, wird ein Dienst zusätzlich durch die sogenannte **Portnummer** (oder einfach Port) unterschieden. In Analogie zum Telefon entsprechen die Rechneradressen den Nummern von Nebenstellenanlagen und die Portnummern der Durchwahl. Und wie bei Nebenstellenanlagen, muss ein Anrufer (ein Client, s. Client / Server-Architektur auf Seite 4) die Durchwahl kennen, wenn er eine bestimmte Anfrage stellen will. Für die viel benutzten Dienste sind diese aber „wohlbekannt“ („well known“, s. z.B. bei der *Internet Assigned Numbers Authority*, www.iana.org).

Protokoll

Ein *Protokoll* (Protokolldefinition) ist die Festlegung von Regeln für die Funktionen des Dienstes, Form und Aufbau von Adressen, Datenpaketen usw. im Netzwerk. Jeder „Netzwerktyp“ hat seine eigenen Protokolle: Internet, Windows NT Server Netz, Novell Netware u.a., die i.a. untereinander nicht kompatibel (verträglich) sind. Daher kann beispielsweise ein PC (nur) mit Microsoft-Netzwerksoftware nicht mit einem Internet-Rechner kommunizieren. Es werden deshalb üblicherweise alle notwendigen Netzwerkprogramme

sozusagen parallel auf dem Rechner/PC installiert, also TCP/IP für den Zugriff auf's Internet und ggf. die Microsoft-Netzwerkprogramme für die Kommunikation mit einem NT Server.

Die jeweilige Netzwerksoftware (=Netzwerkprogramm) erledigt die Netzwerkfunktionen mit Hilfe der Hardware entsprechend der definierten Regeln (Protokolle).

Client / Server-Architektur

Die meisten Netzwerk-Dienste sind nach dem Client/Server-Prinzip organisiert: ftp (File Transfer Protocol: Dateiübertragung), E-Mail und WWW. Zwei Rechner (*hosts*) kommunizieren miteinander, wobei der eine, der *Client* (Kunde), Informationen oder Daten anfordert und der andere, der *Server* (Diener), die Informationen oder Daten (bzw. eine Fehlermeldung) liefert.

Die Unterscheidung ist eine funktionale, nicht eine aufgrund der „Rechner-Leistungs“ o.ä. Daher kann jeder Rechner Client oder Server sein. Er benötigt aber für jede der beiden Funktionen spezielle Software, die Client-Software bzw. die Server-Software, um die betreffende Funktion erfüllen zu können. Beim WWW ist z.B. der Netscape Navigator oder der Microsoft Internet Explorer die Client-Software, während z.B. der WWW-Server „Apache“ eine entsprechende Server-Software ist. Üblicherweise wird ein PC mit der betreffenden Software als Client benutzt, während als Server häufig leistungsstarke Unix-Rechner mit der passenden Server-Software eingesetzt werden.

Ist ein Rechner leistungsfähig genug, um gleichzeitig viele unterschiedliche Anfragen erledigen zu können, können auf ihm mehrere Server-Programme laufen, etwa Server-Software für E-Mail, ftp und WWW. Der Rechner ist dann gleichzeitig Mail-, ftp- und WWW-Server.

Das Internet

Das Internet ist ein Verbund von Netzen, die das TCP/IP-Protokoll benutzen und die durch Gateways und Router (Brückenrechner, „Weiterleiter“) und andere Spezialrechner miteinander verbunden sind.

Es entstand etwa 1969 in den USA aus einem ARPA-Projekt (Advanced Research Projects Agency) und hat sich Anfang der 80er Jahre in Europa vor allem an den Universitäten verbreitet. Heute besteht das Internet aus Tausenden von Netzen und Millionen von angeschlossenen Rechnern (Hosts) von denen viele permanent am Netz sind und Server-Aufgaben erledigen.

Internet- und Host-Adressen (IP-Adressen)

Wie beschrieben, gehört zum Protokoll auch die Definition der (Form der Rechner-) Adressen. Im Internet werden sie auch IP-Adressen genannt. IP-Adressen sind Nummern, die im Netz (-Verbund) eindeutig sein müssen. Sie sind wie im Computer üblich Bitkombinationen, im Internet mit 32 Stellen, also 4 Bytes.

Anmerkung: Ein Bit = eine binäre Speicherstelle; es kann wie ein Schalter zwei Werte (0 oder 1) annehmen. Ein Byte besteht aus 8 „parallelen“ Bit und kann die Werte 0 bis 255 annehmen. Statt Byte wird in diesem Zusammenhang auch von *Oktett* gesprochen.

Die **IP-Adressen** werden üblicherweise durch die Werte der 4 Bytes, getrennt durch Punkte, angegeben, z.B. für einen PC im UKLAN (Universität zu Köln LAN):

134.095.202.110, was der Bitkombination
10000110 01011111 11001010 01101110 entspricht.

Jede IP-Adresse besteht aus zwei Teilen, der **Netz-Adresse** und der **Host-Adresse** (Rechner-Nummer) in diesem (Teil-) Netz. Die **vollständige Host-Adresse** entspricht der IP-Adresse. Unterschieden werden mehrere Netz-Klassen, Class A, B und C, die am **ersten Oktett**, am ersten Wert (linke Zahl, im Beispiel 134) zu erkennen sind und sich in der Länge (Größe) der Netznummern unterscheiden. Weitere Klassen für spezielle Zwecke werden hier nicht erwähnt.

- **Class A** Adresse: Wert des 1. Oktetts von 1 bis 126, Länge der Netzadresse 1 Byte (das linke Byte). Insgesamt sind max. 126 Class A Netze möglich, von denen jedes rund 16 Millionen Rechner umfassen kann (2 hoch 24). Die Netznummer 127 ist reserviert.
- **Class B** Adresse: Wert des 1. Oktetts von 128 bis 191, Länge der Netzadresse 2 Byte, max. etwa 16000 Netze möglich, von denen jedes 65535 Rechner (2 hoch 16) umfassen kann. Das UKLAN 134... ist also ein Class B Netz, die Netzadresse ist 134.95.0.0, die Rechneradresse im obigen Beispiel 202.110).

- **Class C** Adresse: Wert des 1. Oktetts von 192 bis 223, Länge der Netzadresse 3 Byte, max. etwa 2 Millionen Netze möglich, von denen jedes 256 Rechner (2 hoch 8) umfassen kann.

Netze können weiter in Sub-Netze unterteilt werden, z.B. das UKLAN als Class-B-Netz durch Benutzung des dritten Wertes. Im Beispiel bezeichnet 202 ein Subnetz (einen PC-Pool) in der EW-Fakultät (110 ist die Rechneradresse im Subnetz 202), 140 ist ein Subnetz im ZAIK/RRZK (Zentrum für Angewandte Informatik/Regionales Rechenzentrum der Universität zu Köln). Subnetze sind „selbstständige“ Teil-Netze, die durch Router verbunden sind und insgesamt das betreffende (im Beispiel Class B-) Netz bilden. Durch diese Strukturierung können Störungen in einem Subnetz (i.a.) andere Subnetze nicht beeinträchtigen.

In der TCP/IP-Software, z.B. im Windows-Netzwerk bei TCP/IP, wird diesem Sachverhalt durch Angabe der Subnetz-Maske 255.255.255.0 Rechnung getragen, aus der zu erkennen ist, dass nur der letzte Wert, im o.a. Beispiel 110, im UKLAN als (eigentliche) Rechneradresse im Subnetz 202 benutzt wird.

Host-Namen und Domain Name Server (DNS)

Da die Internet-Adressen (IP-Nummern) nur schwer zu merken sind, wurden für die Rechner logische Namen (Host-Namen) erfunden. Beispielsweise kann für einen der zentralen Server des ZAIK/RRZK der Universität zu Köln mit der IP-Adresse 134.95.19.27 statt der Nummer der Name *campfire.rrz.uni-koeln.de* angegeben werden, wobei man sich dann leichter merken kann, dass der Rechner *campfire* heisst und zum Regionalen Rechenzentrum der Universität zu Köln (ZAIK/RRZK) gehört.

Dieses Namenssystem ist hierarchisch strukturiert und wird auf der obersten Ebene von der *Internet Corporation of Assigned Names and Numbers* ICANN verwaltet, die die sogenannten **Top Level Domains** (TLD) oder **Zonen** festlegt.

Im Großen und Ganzen entsprechen viele TLDs den einzelnen Staaten:

de	Deutschland,
uk	United Kingdom (Großbritannien)
fr	Frankreich
it	Italien usw.

Für die USA gibt es, wohl aus Gründen, das Internet entstand dort, gleich vier TLDs:

gov	Government
mil	Military
edu	Educational
com	Commercial

Zudem hat die ICANN vor kurzem weitere „allgemeine“ TLDs festgelegt, etwa:

info	Information
biz	Business u.a.

IP-Nummern sind „willkürlich“ vergeben, eine Zuordnung von IP-Nummern und TLDs – etwa 134 = de - existiert nicht.

Unter den TLDs werden die Domains angesetzt, etwa *uni-koeln* oder *spiegel* (*uni-koeln.de* oder *spiegel.de*). Prinzipiell kann man in jeder TLD eine eigene Domain anmelden, etwa *vw.com* für das Volkswagenwerk, für das die USA ein wichtiger Markt sind. **Bei Domain-Namen spielt Groß-/Kleinschreibung keine Rolle!**

Die unter den TLDs angeordneten Domains wie *uni-koeln* oder *spiegel* werden ebenfalls zentral für jede TLD vergeben und verwaltet. Für de, also für Deutschland, macht dies das **DE-NIC** (Network Information Center).

Für jede Domain gibt es wieder eine Verwaltungsstelle, die innerhalb der Domain die Sub-Domains (Namen der Teilnetze) verwaltet. Für *uni-koeln.de* z.B. ist das das ZAIK/RRZK. Analog wird i.a. für eine Sub-Domain, z.B. für die Sub-Domain *rrz.uni-koeln.de* verfahren, die die im Subnetz angesiedelten Rechnernamen und Adressen verwaltet. Die Rechnernamen (Hostnamen), etwa *campfire.rrz.uni-koeln.de*, werden als *vollständiger Domain-Name* (Fully Qualified Domain Name) bezeichnet.

Anmerkung: Umgangssprachlich werden sowohl *uni-koeln*, *uni-koeln.de*, *rrz.uni-koeln.de* (eigentlich Sub-Domain) und Rechner z.B. *campfire.rrz.uni-koeln.de* (eigentlich „fully qualified domain“) einfach nur Domain genannt.

Jede Verwaltungsstelle ist verantwortlich für die (Teil-) Namen und Adressen ihrer Hierarchiestufe. Das ZAIK/RRZK vergibt und verwaltet also beispielsweise die Namen und Adressen der Sub-Domains von *uni-koeln.de* (134.95.x.y), etwa *wiso* (*wiso.uni-koeln.de*). Im Subnetz *wiso.uni-koeln.de* verwaltet dann die

Geschäftsstelle für Datenverarbeitung Namen und Adressen von Rechnern der WiSo-Fakultät, etwa server1.wiso.uni-koeln.de.

Aufgrund dieser Hierarchie ist sichergestellt, dass die Namen eindeutig vergeben und den Internet-weit eindeutigen IP-Nummern zugeordnet werden.

Da die Rechner im Internet nur mit ihren IP-Adressen angesprochen werden können, benötigt man spezialisierte Rechner, auf denen Tabellen (Datenbanken) mit den Namen und IP-Nummern gespeichert sind, um das Namenssystem komfortabel verwenden zu können. Diese dedizierten Server, die **Domain Name Server: DNS** genannt werden, stellen den Internet-Benutzern diese Tabellen automatisch zur Verfügung. Auch die DNS sind hierarchisch strukturiert, um „Overhead“ (überflüssige Verwaltungsarbeit) zu vermeiden.

Es gibt u.a. für jede TLD einen DNS (z.B. für de beim DE-NIC), der alle Domains in dieser TLD in seiner Datenbank notiert hat. Ebenso gibt es in jeder Domain (wenigstens) einen DNS, der alle Sub-Domains und Hosts in dieser Domain enthält. Für die Universität zu Köln ist das zur Zeit u.a. ein Rechner im ZAIK/RRZK mit der IP-Adresse 134.95.100.208.

So kennt jeder DNS nur den seiner Hierarchiestufe entsprechenden Ausschnitt des Internet-„Namensraumes“, zusätzlich aber auch noch den nächst höheren und nächst niedrigeren DNS. So ist die Pflege der Tabellen vereinfacht und trotzdem gewährleistet, dass alle eingetragenen Namen durch „verkettete“ Nachfragen gefunden werden.

Jeder Rechner, der im Internet Informationen finden will, muss „seinen“ DNS kennen (s. *Zugang zum Internet*). Stellt ein Client eine Anfrage an einen Server, so fragt die Client-Software, z.B. der Netscape Navigator, zuerst beim zuständigen DNS nach der IP-Adresse des Servers. Erst wenn die IP-Adresse bekannt ist, kann sich der Client an den Server wenden.

Kennt der erste DNS den Server nicht, fragt er beim über- oder untergeordneten DNS nach, dieser ggf. ebenfalls beim nächsten usw., bis die IP-Adresse gefunden ist. Gibt es den Namen in keiner der DNS-Datenbanken, so wird eine Fehlermeldung „Server nicht gefunden“ o.ä. zurückgegeben.

Zugang zum Internet

Grundsätzlich gibt es zwei Arten des Internetzugangs:

1. Der Rechner (PC) ist direkt an ein lokales Netzwerk (LAN) angeschlossen, das über einen Router oder ein Gateway (einen Brückenrechner) direkt mit dem Internet verbunden ist. In diesem Falle muss der PC-Betreuer vom LAN-Betreuer eine IP-Nummer für den betreffenden PC sowie die IP-Nummer des „lokalen“ DNS und des „Default-Gateways“ (Übergangrechner in's Internet) erhalten. Die IP-Nummern für PC, DNS und Gateway können auch automatisch beim Einschalten des PCs vergeben werden, Stichwort DHCP: Dynamic Host Configuration Protocol.
2. Der Heim-PC wird mit Modem, ISDN-Adapter oder DSL (Digital Subscriber Line, schnelle Internet-Verbindung) über die Telefonleitung mit einem Einwahlrechner eines Providers verbunden. Die Verbindung bis zum Einwahlrechner ist dann eine „Telefonverbindung“, für die Gebühren anfällt. Zudem können Internet-Gebühren des Providers anfallen. Die IP-Nummern für den eigenen PC sowie des DNS werden dem Heim-PC automatisch vom Einwahlrechner mitgeteilt, woraus sich u.a. auch ergibt, dass man bei jeder Einwahl eine andere IP-Adresse für den eigenen PC erhält. Erst „hinter“ dem Einwahlrechner des Providers beginnt das Internet.

Provider

Ein Internet-Provider (Internet-Anbieter) ist eine Organisation oder Firma, die einen Internetzugang (Einwahlrechner) sowie andere Leistungen bereitstellt, etwa die Möglichkeit, eine eigene Homepage (s. WWW weiter hinten) anzulegen, der eine E-Mail-Server (ein PostOffice) und damit E-Mail-Adressen bereitstellt etc. Einige bekannte Provider: AOL, Tiscali, t-online, Universität zu Köln (letztere nur für Angehörige der Universität, die üblichen Telefonkosten sind aber eher höher als die Gesamtkosten mancher Internet-by-Call-Anbieter).

Bei einigen Providern muss zusätzlich zu den Kosten pro Zugangsminute (Telefon- und Internetgebühren) eine monatliche Grundgebühr gezahlt werden. Andere Provider lassen **Internet-by-Call** zu. Die Grundgebühr entfällt, es sind nur die Verbindungsgebühren pro Minute und in einigen Fällen Einwahlgebühren pro Einwahl zu zahlen.

Die Preisunterschiede können beachtlich sein, u.a. auch deswegen, weil einige Provider im Minutentakt (jede angebrochene Minute ist zu zahlen), andere aber im Sekundentakt abrechnen, so dass die Gesamtrechnung trotz höherer Minutenpreise abhängig von den Surf-Gewohnheiten niedriger sein kann (s.

z.B. www.heise.de/itarif/). Bei Internet-by-Call kann es zudem sinnvoll sein, tagsüber einen anderen Provider als abends zu wählen.

Für Vielsurfer kann die von einigen Providern (Arcor, t-online u.a.) angebotene Flatrate günstig sein, die für eine feste Gebühr den Internetzugang ohne Zeitbeschränkung ermöglicht. Bei preiswerteren Flatrates ist aber i.a. eine Beschränkung des Übertragungsvolumens festgelegt.

Zugang zum Internet, E-Mail-Adresse und Homepage können natürlich bei unterschiedlichen Providern in Anspruch genommen werden. Einige Internet-Adressen mit Informationen zu Kosten und Leistungen sind weiter hinten angegeben.

Netiquette – Umgangsformen im Internet

Im Laufe der Zeit haben sich im Internet bestimmte (Höflichkeits-) Formen ausgebildet, die aus Unkenntnis oft missachtet werden, so etwa, wenn Mails immer komplett „zitiert“ werden. Die englischsprachigen Regeln der Netiquette finden Sie unter <http://www.albion.com/netiquette/>, und z.B. unter <http://www.chemie.fu-berlin.de/outerspace/netnews/netiquette.html> eine deutschsprachige Übersicht.

Internet-Sicherheit

Sobald Ihr PC Verbindung mit dem Internet hat, lauern Gefahren wie *Viren*, *Dialer* und *Backdoors* für Ihren PC und (beim Heim-PC) auch für Ihren Geldbeutel auf Sie. (Eine feinere Unterscheidung von Schädlingen, von Malware, wird hier nicht vorgenommen, ebenso wird keine Vollständigkeit in der Aufzählung angestrebt. Die Ausführungen sollen i.w. das Bewusstsein für Gefahren wecken und zur Vorsicht aufrufen.)

Am häufigsten treten Viren auf, die i.a. als Anhang in E-Mails verbreitet werden. Dialer können ebenfalls als Mail-Anhang oder auch über WWW-Seiten verbreitet werden. Backdoors können durch Angriffe aus dem Internet auf Ihrem PC installiert werden. In allen Fällen handelt es sich um Programme, die von Ihnen unbemerkt Aktivitäten auf Ihrem PC entfalten. Mit geeigneten Maßnahmen können die Gefahren aber verringert werden.

Viren

Viren - Viren, Würmer u.a. werden hier nicht unterschieden - sind kleine Programme, die Schaden auf dem lokalen PC anrichten, z.B. die Festplatte formatieren (und damit alle Daten löschen), oder von jedem befallenen PC an jede E-Mail-Adresse im Outlook-Adressbuch eine E-Mail verschicken und damit die „Internet-Leitungen“ so verstopfen, dass niemand mehr Briefe senden oder empfangen kann. Heute werden Viren meist als Anhang von **E-Mails auf Windows-PCs verbreitet**. Sobald eine verseuchte Mail z.B. in Outlook (Express) geöffnet wird, kann das Virenprogramm ausgeführt werden. Dies geschieht i.a. aber spätestens nach einem Doppelklick auf den Anhang. Der Virus (das Virenprogramm) installiert sich dann selbst auf dem befallenen PC und wird bei jedem Einschalten des Rechners gestartet.

Dialer

Dialer sind Programme, die als Anhang oder „Grußkarte“ per Mail versandt oder auch auf Webseiten als Hilfs- oder Schutzprogramme angeboten werden. Werden sie z.B. durch Doppelklick auf den Mail-Anhang gestartet, so installieren sie sich als Internet-Einwahlprogramm, das bei jeder Gelegenheit eine teure 0190er-Nummer anwählt. Kosten bis zu mehreren Hundert oder gar Tausend Euro sind so bei ahnungslosen Internet-Benutzern entstanden. Es scheint, als sei z.Zt. diese Gefahr schon etwas eingedämmt. Durch Dialer sind nur Heim-PCs mit Modem- oder ISDN-Anschluss an das Internet gefährdet.

Trojaner oder Backdoors

Ein Trojaner (auch Hintertür oder Backdoor) ist ein Programm, das für den Angreifer „Serverfunktionen“ auf Ihrem PC bereitstellt, so dass er z.B. Ihren PC für Angriffe auf andere Systeme benutzen kann. Trojaner können über Mail-Anhänge oder aktive Inhalte von WWW-Seiten verbreitet werden. Eine weitere Methode angreifender Hacker ist, mit speziellen Programmen das Internet nach Rechnern zu durchsuchen, die sich im Netz befinden, indem z.B. alle möglichen IP-Nummern in einer Domäne, z.B. 134.95.x.y ausprobiert werden. Ist ein mit dem Internet verbundener Rechner gefunden, so werden alle Ports (s. *Portnummer* auf Seite 3) „gescannt“, d.h. die Hacker-Spezialsoftware „fragt nach“, ob der betreffende (Server-) Dienst installiert ist (Portscan). Steht ein solcher Dienst ungeschützt bereit, so wird er ausgenutzt, um ein Programm (den Trojaner) zu installieren, das alle gewünschten Funktionen für den Eindringling bereit stellt.

Auch Programme großer Hersteller können gefährlich sein! So kam ein gefährlicher Trojaner unbemerkt mit der Microsoft SQL Server Database Engine MSDE (c't 21/2001, Heise Verlag, Seite 142). Bei der vereinfachten Installation der MSDE wird ein Administrator Account (Benutzergenehmigung) ohne Passwort eingerichtet, der den vollen Zugang zum Rechner über das Internet durch andere zulässt! Bei ihren Tests fanden die c't-Redakteure Hunderte von Rechnern mit dieser offenen Hintertür!

Schutzmaßnahmen

Virens Scanner

Virens Scanner sind Programme, die Dateien – etwa E-Mails - auf vorhandene Viren prüfen und diese Schädlinge ggf. beseitigen. Auf jedem Windows-PC sollte unbedingt ein solcher *Virens Scanner* installiert sein. Zudem müssen regelmäßig neue Versionen der *Signaturdateien* für den Scanner aus dem Internet heruntergeladen werden, um einen einigermaßen sicheren Schutz zu gewährleisten. Signaturdateien enthalten „Erkennungsmuster“ der **bekannt**en Viren. Damit ist klar, dass Virens Scanner i.a. **keinen Schutz vor neuen Viren** geben können. **Dagegen hilft aber Vorsicht**, wenn auch nicht 100prozentig, insbesondere bei sogenannten **E-Mail-Anhängen** (Attachments).

Neben im Handel käuflichen Produkten wie McAfee VirusScan oder Norton AntiVirus sind mehrere gute Virens Scanner für die private Nutzung kostenfrei im Internet erhältlich. In PC-Zeitschriften finden Sie regelmäßig Tests von Virenschutzprogrammen, die Anhaltspunkte für die Auswahl geben. Eine kleine Liste ohne Anspruch einer Qualitätseinstufung:

- *McAfee VirusScan*, im Handel erhältlich, Infos unter <http://www.nai.com>.
- *Norton AntiVirus*, im Handel erhältlich, Infos unter <http://www.symantec.com>.
- *H+B AntiVir Personal Edition*, **kostenlos**, <http://www.free-av.com>, mit „Gut“ getestet.
- *Sophos Anti-Virus*, s. <http://www.uni-koeln.de/rrzk/software/campus/sophos.html> (für Einrichtungen und Angehörige der Universität zu Köln kostenlos).

Personal Firewall

Eine Firewall (Brandmauer) ist ein Spezialrechner zwischen LAN und Internet, der mit Hilfe seiner Hard- und Software Angriffe aus dem Internet abwehrt. Eine Personal Firewall ist ein Programm, das diese Funktion z.B. auf Heim-PCs nachbildet. Alle zwischen dem eigenen PC und dem Internet ausgetauschten Datenpakete werden geprüft. Bei Client-Anfragen des eigenen PCs ins Internet wird nachgefragt, ob man den Zugriff auf das Internet zulassen möchte. Bei aus dem Internet kommenden Anfragen wird gemeldet, dass ein Zugriff aus dem Internet abgeblockt wurde.

Bei den verbreiteten Personal Firewalls wie *ZoneAlarm* (<http://www.zonelabs.com/store/content/home.jsp>) kann detailliert eingestellt werden, welche Zugriffe in das oder aus dem Internet erlaubt sind. Somit ergibt sich insgesamt ein Schutz gegen Angriffe aus dem Internet bzw. gegen Backdoors. (Neue Backdoors versuche aber, Firewalls abzuschalten.)

Anti-Dialer

Schutz vor Dialern bieten Programme wie zur Kontrolle der PC-Telefonverbindungen wie 0190Warner, Dialer Control, YAW oder auch ISDNWatch für die FritzCard. Hinweise zur gesamten Problematik finden Sie unter <http://www.dialerundrecht.de/> und <http://www.heise.de/ct/02/10/040/default.shtml>.

Da die Dialer Techniken entwickeln, Einwahlsperren zu deaktivieren, müssen Sie wie bei den Virens Scannern regelmäßig nach neuen Versionen Ausschau halten.

Download von 0190 Warner: <http://www.freewarepage.de/download/831.shtml>

Download von Dialer Control: <http://www.dialer-control.de/>

Download von YAW: <http://www.yaw.at/>

Allgemeine Sicherheits-Tipps

- **Dauer der Verbindung:** Bleiben Sie nur so lange wie nötig im Internet. Auch wenn es „nix kostet“ (Sie eine Flatrate haben), die Gefahr durch Portscans (s. Seite 7) wächst mit der Dauer der Verbindung!
- **Schutzprogramme:** Installieren Sie einen Virens Scanner (regelmäßige Aktualisierung nicht vergessen), Anti-Dialer sowie eine Personal Firewall.
- **Auswahl der Programme:** Die Auswahl der Programme kann die Gefährdung stark verringern. Insbesondere die Microsoft Programme zum Surfen (Internet Explorer) und Mailen (Outlook bzw.

Outlook Express) bergen wegen der engen Verzahnung mit Windows ein großes Gefahrenpotenzial in sich. Die weitaus größte Anzahl von Viren wird z.B. durch Outlook verbreitet. Alternativen für Browser statt Internet Explorer sind Netscape, Opera u.a., für Mail-Programme statt Outlook oder Outlook Express (ebenfalls) Netscape, Mulberry, Eudora u.a.

Wollen Sie absolut nicht auf diese Programme verzichten, sollten Sie unbedingt die **Windows-Sicherheitseinstellungen verschärfen** (s. *Sicherer surfen mit dem Internet Explorer* ff. auf Seite 9).

- **E-Mail-Anhänge** vollkommen fremder Absender **auf keinen Fall** im E-Mail-Programm durch Doppelklick **öffnen!** Auch bei Attachments von Bekannten könnte es sich um „Kettenbrief-Viren“ handeln, da sich diese i.a. automatisch weiterversenden. Falls der Bekannte plötzlich in Englisch schreibt oder der Anhang einen merkwürdigen Namen hat, lieber beim Bekannten nachfragen. Einer der Viren hatte z.B. den Namen AnnaKournikova.jpg.vbs. Das vbs ist in vielen Programmen nicht zu sehen, so dass der unerfahrene Benutzer glaubt, ein tolles Foto erhalten zu haben.
- **Download von Programmen:** Glauben Sie keine „Versprechungen“. Im Internet will man häufig an Ihr Geld! Laden Sie nur bekannte Programme von vertrauenswürdigen Servern wie etwa uni-koeln.de herunter.

Sicherer surfen mit dem Internet Explorer

Die enge Verzahnung von Microsoft Internet Explorer und Outlook bzw. Outlook Express mit Windows birgt großes Gefahrenpotenzial. Wer auf diese Programme nicht verzichten will, sollte unbedingt die **Windows-Sicherheitseinstellungen** (prüfen und ggf.) **verschärfen**. (Die standardmäßig in den Programmen eingestellten Werte sind abhängig von der Windows- und Explorer-Version.)

Zur Einstellung der Sicherheitsoptionen wird der **Internet Explorer** gestartet und der Befehl *Extras -> Internetoptionen...* aufgerufen. Auf der Registerkarte **Sicherheit** können für das **Internet**, d.h. für die „ganze Welt“, sowie für das **Intranet**, das „eigene Firmen-Netzwerk“, etwa das UKLAN, unterschiedliche Sicherheitseinstellungen vorgenommen werden. Zudem können **vertrauenswürdige Sites** (Server im Internet, auf denen man keine Schädlinge erwartet) sowie nicht vertrauenswürdige **eingeschränkte Sites** eingegeben und mit eigenen Sicherheitseinstellungen versehen werden. Eine Site (z.B. ein WWW-Server) wird bei den Einstellungen in der üblichen Form angegeben, z.B. www.uni-koeln.de.

Für jede der 4 Zonen kann durch Anklicken der Schaltfläche [Stufe anpassen...] der Dialog zum individuellen **Einstellen der Sicherheit** aufgerufen werden.

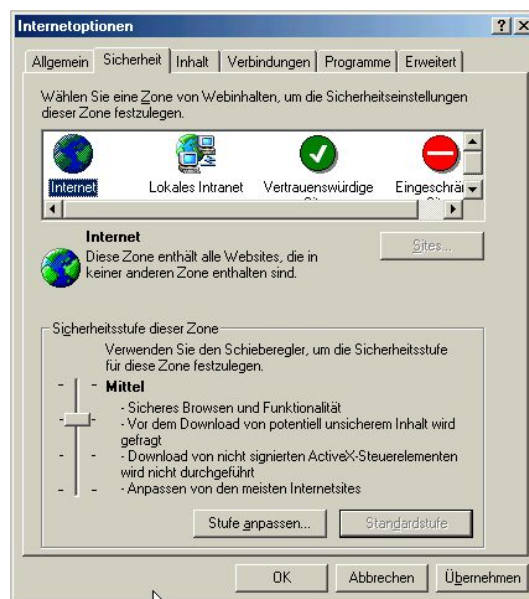
Besonders gefährlich sind aktive Inhalte wie ActiveX, Active Scripting und inzwischen auch Java Script. Am sichersten kann man surfen, wenn für die Zone Internet alle diese „aktiven“ Optionen deaktiviert werden. Dies kann natürlich zur Folge haben, dass manche bunt animierte Seite nicht mehr richtig oder sogar garnicht angeschaut werden kann. In jedem Falle sollte aber ActiveX deaktiviert sein.

Die Sicherheitseinstellungen, etwa für Datei-Download, Java und Active Scripting werden u.U. erst sichtbar, wenn die Optionen mit Hilfe des vertikalen Bildlaufleiste nach oben geschoben werden.

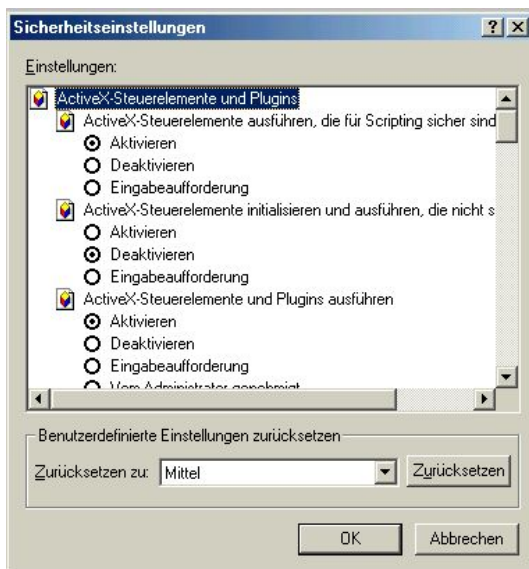
Benutzen Sie den Internet Explorer, so ist es (ähnlich wie bei den Virenschaltern) wichtig, dass regelmäßig auf den Microsoft-Servern nach **Fehlerkorrekturen**, *Patches* oder *Service Releases* (SR) gesucht wird, um neu bekannt gewordene Sicherheitslücken zu schließen.

Sicherer Mailen mit Outlook Express

In (neueren Versionen von) Outlook oder Outlook Express kann man entweder die Zone **Internet** oder die Zone **Eingeschränkte Sites** mit den jeweiligen Einstellungen als



Extras Internetoptionen



Sicherheitseinstellungen für eine Zone

„Sicherheitsstufe“ wählen. Da wenigstens für die Zone *Eingeschränkte Sites* alle ActiveX-Optionen etc. deaktiviert sein sollten, bringt die Wahl dieser Zone für Outlook Express die beste Sicherheit. Zudem sollte die Option „nur Text“ aktiviert sein, damit der Empfänger sicher sein kann, dass keine HTML- oder andere aktive Inhalte mitgesandt wurden. Auch die Wahl eines „einfachen“ Mail-Programms, das weniger Automatismen enthält, kann die Sicherheit auf dem eigenen PC wesentlich erhöhen. Sicherere Alternativen zum Mailen sind etwa Netscape Communicator, Mulberry, The Bat oder auch Eudora.

Internet-Dienste

Wie weiter vorn beim Schichtenmodell (Seite 2) für das Internet angegeben, kann der Benutzer mehrere Dienste im Internet in Anspruch nehmen: E-Mail, WWW, Net News, ftp und Terminal. Beschrieben werden nur die ersten vier. (Bei Terminal handelt es sich um die Möglichkeit, den eigenen PC als Terminal, d.h. als Tastatur und Bildschirm zum Arbeiten auf einem entfernten „Großrechner“ zu benutzen.)

E-Mail

Als Erstes benötigt man eine eigene E-Mail-Adresse, die man auf Wunsch vom Provider erhält, sowie ein eigenes Zugriffs-Passwort, das man nach Einrichtung des „Briefkastens“ durch den Provider selbst festlegt.

E-Mail wird von **PostOffice zu PostOffice** transportiert. Ein **PostOffice** ist ein **Mail-Server** (meist Unix-Rechner mit einer Mail-Server-Software), der immer läuft und immer am Internet ist, also eine feste IP-Nummer und einen Domain-Namen hat, etwa mail.rrz.uni-koeln.de. Der Transport der Mail zwischen den Mail-Servern wird vom Protokoll SMTP (Simple Mail Transfer Protocol) sicher gestellt.

Jeder Mail-Benutzer benötigt im Prinzip zwei „eigene“ Postämter, eines zum Versenden von Post (z.B. mail.rrz.uni-koeln.de, analog zum Versandschalter im Postamt) sowie ein anderes, bei dem er eingegangene Mails abholen kann (z.B. pop.rrz.uni-koeln.de, analog zum Brieffach im Postamt). Beide müssen im Mail-Client (Mail-Programm auf dem PC) eingetragen sein.

Der Sender einer E-Mail gibt seine Mail von seinem PC aus beim für ihn zuständigen Versand-Postamt ab. Dieses sendet die Mail an das Empfänger-Postamt, wo sie vom Empfänger abgeholt werden kann. Im Prinzip ist alles so wie bei der Gelben Post.

Praktisch hat man drei Möglichkeiten, mit dem PC E-Mail-Versand und Empfang zu realisieren: **Web-Mail** mit Hilfe eines Browsers wie Netscape Navigator sowie **POP-** oder **IMAP-Mail** mit einem lokalen (d.h. auf dem eigenen PC installierten) Mail-Client wie dem in den Netscape Communicator integrierten *Messenger*. Bei Webmail genügt zusätzlich zur eigenen E-Mail-Adresse und zum Zugangspasswort die Kenntnis der Provider-Homepage, etwa www.epost.de oder bei der Universität zu Köln die Adresse webmail.uni-koeln.de. Bei POP- und IMAP-Mail benötigt man die Namen des Versand- und des Empfangs-Postamtes (Eingangs- und Ausgangs oder Mail- und SMTP-Server).

Für die Auswahl der Alternativen ist für den Benutzer wichtig, ob er den E-Mail-Dienst auf einem einzigen Rechner, z.B. seinem Heim-PC, auf mehreren Rechnern, etwa seinem persönlichen Dienst-PC und seinem Heim-PC, oder gar weltweit auf beliebigen PCs nutzen will. Bei manchen Providers, z.B. der Universität zu Köln, kann Web-Mail und POP- oder IMAP-Mail auch „parallel“ genutzt werden. Zu beachten ist zudem, dass die viele E-Mail-Programme unter Windows, auch wenn sie mehrere Adressen verwalten können, die jeweiligen vom Mail-Server herunter geladenen Mails (z.B. bei POP-Mail) nicht vor dem Zugriff Dritter schützen, eine Vertraulichkeit von Informationen also nicht gewährleistet ist.

Aufbau einer E-Mail

Eine Mail besteht aus dem *Kopfteil* (Header), dem (Brief-) *Text* (Body) und ggf. noch einem *Anhang* (Attachment). Im Kopf stehen Angaben (Felder), die zur korrekten Auslieferung der Mail notwendig bzw. für den Empfänger hilfreich sind. Folgende Felder sind zu beachten:

- **An** (To): Muss eine oder mehrere, durch Kommata getrennte Empfängeradressen (E-Mail-Adressen) enthalten.
- **Betreff** (Subject): Kann eine kurze Kennzeichnung des Inhalts („Betreff“) enthalten. Dem Empfänger zu Liebe sollte der Betreff immer angegeben werden.
- **Cc** (Carbon Copy): Ein „Durchschlag“ der Mail wird zur Kenntnisnahme an die hier angegebenen Adressen gesendet. Der eigentliche Empfänger der Mail (An:) kann sehen, dass andere die Mail ebenfalls erhalten haben.
- **Bcc** (Blind Carbon Copy): Die hier angegebenen Empfänger erhalten eine Kopie der Mail, dies ist für den eigentlichen Empfänger jedoch nicht erkennbar. Bei Mails an eine große Zahl von Empfängern können

diese i.a. im Bcc-Feld eingetragen werden, so dass die oft lästige lange Adressenliste nicht zu sehen (und nicht zu drucken) ist.

- **Reply-To:** Angabe einer Rückantwortadresse, falls diese von der Absenderadresse abweicht.

Weitere Felder werden beim Absenden automatisch eingefügt und können vom Empfänger gelesen werden:

- **From:** Enthält die Absenderadresse.
- **Date:** Enthält Absendedatum und Uhrzeit.
- **Message-Id:** Enthält eine im Internet eindeutige Identifikationsnummer der betreffenden Mail.
- **Received:** zeigt den Weg der Mail durch das Internet an.

E-Mail-Adressen

E-Mail-Adressen setzen sich zusammen aus dem Benutzer- oder Empfängernamen, etwa *heinz.mueller* oder auch nur *mueller*, gefolgt vom At-Zeichen @, hinter dem der Name der Domain folgt, in der der Mail-Server des Providers angesiedelt ist. Arbeitet beispielsweise Heinz Müller bei der Universität zu Köln und ist diese sein Provider, so könnte seine E-Mail-Adresse *heinz.mueller@uni-koeln.de* lauten. Wichtig ist, dass **nationale Sonderzeichen wie Umlaute in E-Mail-Adressen nicht erlaubt** sind. (Auch im „Betreff“ u.a. Angaben des Mail-Kopfes sollten keine Sonderzeichen benutzt werden.)

POP3 und IMAP

Dienst	Protokoll	Architektur	Adresse	Clients
E-Mail	SMTP, POP3, IMAP	Client/Server	name@domain	Eudora, Netscape Messenger, Outlook, Pegasus u.a.

IMAP: Internet Message Access Protocol, **POP3:** Post Office Protocol Version 3. Beide Protokolle beschreiben und realisieren unterschiedliche Arten, auf Mail-Server (Post Offices) zuzugreifen.

POP3 und IMAP setzen einen Mail-Client (ein Mail-Programm) auf dem PC voraus, der neue Mails vom Empfangs-PostOffice des Providers abrufen. Praktisch alle Mail-Server unterstützen für das Abholen neuer Mails POP3, IMAP hat POP gegenüber einige Vorteile und breitet sich (neben Web-Mail) sehr stark aus. Die wesentlichen, subjektiv mit Plus und Minus bewerteten Unterschiede der beiden Protokolle POP und IMAP:

1. POP3:

Minus: Bei der Abfrage des PostOffice werden i.a. alle neuen Mails sofort übertragen, was bei großen Mails oder großen Anhängen sehr lange dauern kann.

Minus: Man hat die Möglichkeit, alle Mails auch auf dem Server zu belassen oder automatisch nach der Übertragung zum PC zu löschen. Im 1. Fall ist der Aufwand, den Server regelmäßig aufzuräumen, recht groß. Im 2. Fall hat man keine Möglichkeit, die Mails auf anderen als dem benutzten PC (nochmals) zu lesen.

Minus: Will man mit POP Mails auf einem fremden PC lesen, so muss die Konfiguration der Mail-Client-Software geändert oder ergänzt werden für den eigenen E-Mail-Provider. Anschließend muss dies ggf. rückgängig gemacht werden. Es besteht die Gefahr, dass abgerufene E-Mails auf dem fremden PC zurückbleiben. Dies gilt natürlich nicht, falls Sie immer Ihren persönlichen Laptop benutzen, der mit Netzwerkkarte oder Modem mit dem Internet verbunden wird.

Plus: Nach dem Übertragen der Mails kann man *offline* (ohne Telefonverbindung in's Internet) arbeiten, Mails lesen, neue schreiben und diese (nach erneuter Verbindung) schnell versenden. Die Telefon-Kosten bleiben relativ niedrig.

2. IMAP:

Plus: Beim Abrufen der Mails werden zuerst nur die „Header“ übertragen: Absender, Betreff etc. Dies geht relativ schnell, auch bei sehr großen Mails. Erst beim Öffnen (Lesen) einer Mail wird deren Text auf den Bildschirm übertragen, die Mail selbst mit dem eventuell vorhandener Anhang verbleibt aber noch auf dem Server, bis sie (in Eudora z.B. per Ziehen&Fallen-lassen, Drag&Drop) komplett auf den lokalen Rechner übertragen oder aber „gelöscht“ wird. Übertragene oder „gelöschte“ Mails werden auf dem Server nur als gelöscht markiert und müssen ggf. noch mit einem Menü-Befehl explizit „entfernt“ werden. Ggf. kann auch nur die Markierung entfernt werden.

Plus: Das Lesen der Header geschieht online (mit laufender Telefonverbindung). Auf den eigenen PC übertragene Mails können aber offline gelesen, neue Mails offline geschrieben und dann „schnell“ abgeschickt werden.

Plus: Die Verwaltung der eigenen Mails kann in Ordnern auf dem Server vorgenommen werden. Keine Mehrfacharbeit ist nötig.

Plus: Nicht interessierende oder gefährliche Mails (Viren! Der Betreff lässt dies häufig erkennen.) können bereits auf dem Server gelöscht werden ohne dass überhaupt die Möglichkeit zur Schädigung des eigenen PCs besteht.

Plus: Da die Mails auch nach dem Lesen noch auf dem Server verbleiben, kann man prinzipiell von jedem PC in der ganzen Welt mit einem passenden Klienten auf die Mails zugreifen.

Minus/Plus: Wollen Sie Ihre Mails auf einem fremden PC lesen, muss zuerst die Mail-Client-Software neu (mit Ihrer E-Mail-Adresse und den Provider-Daten) konfiguriert werden. Dies ist natürlich dann nicht notwendig, falls es sich um Ihren persönlichen Laptop handelt, und Sie mit Netzwerkkarte oder Modem Zugang zum Internet finden.

Falls Ihr Provider IMAP anbietet und Sie an mehreren persönlichen PCs arbeiten oder einen Laptop benutzen, dürfte IMAP insgesamt vorteilhafter sein.

Web-Mail

Viele Provider wie *ePost* (s. www.epost.de) oder *gmx* (www.gmx.de) bieten kostenlose Mailedienste an, die mit Hilfe eines Browsers wie Netscape Navigator, Microsoft Internet Explorer oder Opera in Anspruch genommen werden können. Mit Hilfe von Programmen (Java, Javascript o.a.), die beim Ansprechen der Provider-Homepage automatisch vom dortigen Server auf den lokalen PC geladen werden, verwandelt sich der Browser in ein Mail-Programm mit direktem Zugang zum PostOffice.

- *Plus:* Es ist kein eigener Mail-Client nötig, die für Anfänger etwas diffizile Konfiguration des Mail-Client entfällt.
- *Plus:* Von jedem PC mit Internetzugang kann Mail gelesen und versandt werden, da die Mails nur auf dem Server gespeichert und erstellt werden.
- *Minus:* Man kann im Prinzip nur online arbeiten, was teuer sein kann.
- *Minus:* Das Versenden und Empfangen von Anhängen ist etwas umständlicher. Manchmal werden die Namen der Anhänge nicht beibehalten, der Empfänger muss u.U. ausprobieren, um welche Art Datei es sich handelt.

Insbesondere, wenn man keinen persönlichen PC oder Laptop besitzt oder häufig „unterwegs“ ist, ist Web-Mail von Vorteil.

E-Mail-Umleitung

Praktisch alle Mail-Server ermöglichen das „Nachsenden“ oder Weiterleiten von Mails an eine andere Adresse. Bei einigen Providern kann dies Menü-gesteuert im Browser auf einer entsprechenden Provider-Seite durchgeführt werden. Bei anderen (etwa bei der Universität zu Köln) muss die Weiterleitungsadresse (die neue Zieladresse) in einer Datei *forward* („Punkt“ forward) auf dem Mail-Server gespeichert werden. Sinnvoll ist Umleitung z.B. nach einem Umzug und Providerwechsel, so dass für eine gewisse Zeit Mails von Absendern, die die neue Adresse noch nicht kennen, dennoch ankommen und man ihnen die neue Adresse mitteilen kann.

Besitzt man eine Web-Mail-Adresse und eine POP- oder IMAP-Adresse, so können die Vorteile der 3 Mail-Varianten kombiniert werden, um jederzeit und ohne Gefahr eigene Mails lesen und versenden zu können. Zu Hause kann man die POP- oder IMAP-Adresse benutzen, bei der Web-Mail wird um Mehraufwand zu vermeiden ggf. eine Umleitung zur POP- oder IMAP-Adresse eingerichtet. Ist man für einige Zeit auf Reisen, benutzt man die Web-Mail und richtet vor der Reise eine Umleitung der POP-/IMAP-Adresse dorthin ein. Natürlich muss man darauf achten, dass nicht beide Adressen auf die andere umleiten, indem man jeweils eine Umleitung rechtzeitig aufhebt.

Mailinglisten

Mailinglisten sind im Prinzip Briefverteiler, für die man sich mit einer E-Mail an den (natürlichen oder softwaremäßigen) Verwalter der Liste anmelden muss. Analog wird die Abmeldung per E-Mail vorgenommen. Listen sind Kommunikationsforen für bestimmte Themen ähnlich wie News-Gruppen (s. weiter hinten).

Unter <http://www.uni-koeln.de/rrzk/maillist/> findet man z.B. Informationen zu Listen an der Universität zu Köln.

Postmaster – der Chef im PostOffice

Haben Sie Probleme mit einem PostOffice, können diese i.a. mit Hilfe des Systembetreuers dieses Mail-Servers gelöst werden. Dieser (bzw. die Systembetreuer-Gruppe) hat praktisch immer die E-Mail-Adresse **postmaster@domain**.

Kommt z.B. eine Mail als „nicht zustellbar“ zurück, obwohl Sie genau wissen, dass der Empfänger eine Adresse in dieser Domain hat, kann eine höfliche Anfrage beim Postmaster das Problem lösen.

Tipps für E-Mailer

Um Ärger, Schäden u.a. z.B. beim Mail-Empfänger zu vermeiden, ist die Beachtung einiger Regeln hilfreich:

- HTML-Mails können aktive Inhalte verbreiten, die großen Schaden anrichten können. Konfigurieren Sie Ihr Mail-Programm so, dass **weder formatierter Text noch HTML-Text** versendet wird.
- Schreiben Sie nur reine Text-Mails (*Nur Text*, englisch *Plain text*)! Die Formatierungen von Texten werden in einigen Mail-Programmen als „merkwürdiger“ Text dargestellt.
- Benutzen Sie vor allem im Kopfteil (Header; Absender, Betreff etc.) auf **keinen Fall Umlaute** o.a. nationale Sonderzeichen. Diese werden in vielen Mailern ebenfalls als „merkwürdiger“ Text dargestellt: =?iso-8859-1?Q?L=FCpsen?=
=?
- **Word-Texte** u.ä. können Viren enthalten. Versenden Sie nie solche „Fremdformate“. Wollen Sie unbedingt ein Worddokument o.ä. versenden, speichern Sie es im RTF-Format und versenden Sie diese Datei.
- Praktisch alle Mail-Clients können vorbereitete Unterschriften (Signatures) automatisch mit der Mail versenden, z.B. die Floskel „Mit freundlichen Grüßen“, darunter Ihr Name. Diese **Signatures** sollten **kurz** sein und etwa vier bis fünf Zeilen nicht übersteigen.
- Die sogenannten *vCards*, die von verschiedenen Mailern automatisch mitgesandt werden können, sind eher lästig. Lassen Sie es sein!
- Antworten Sie auf eine Mail, so können Sie deren Inhalt zusammen mit Ihrer Antwort zurücksenden, d.h. die erhaltene Mail zitieren. Zitieren Sie nur das Notwendige bzw. Wichtige. Alles andere sollten Sie löschen!
- Je nach Mail-Programm sollten Sie darauf achten, dass die Zeilenlänge Ihres Textes eher kurz ist.
- Mailen Sie online, z.B. mit Web-Mail, dann ist es aus Kostengründen sehr sinnvoll, eigene Mails mit dem Windows-Editor *Notepad* vorzuschreiben und nach der Einwahl zum Provider die Texte mit Copy&Paste aus dem Editor-Fenster in das Mail-Fenster einzufügen.
Hierbei sind die Windows-**Tastenkombinationen** <Strg> + <C> für „C“opieren und <Strg> + <V> für ein„V“üßen hilfreich bzw. notwendig.
- Zur Versendung von „binären“ Anhängen wie Grafiken oder Programmen ist das MIME-Format (Multi purpose Internet Mail Extensions) am besten geeignet. Meist ist das auch das standardmäßig benutzte Format, bei einigen Mailern muss dies aber konfiguriert (eingestellt) werden.

Weitere Informationen und Tipps zur E-Mail sowie zu E-Mail-Programmen und ihrer Konfiguration finden Sie z.B. unter <http://www.uni-koeln.de/rrzk/mail/>.

Emoticons

E-Mails haben wohl aufgrund des technischen Mediums einen „kalten“ Character. Um diesen zu mildern und die Bedeutung von Formulierungen klarzustellen, wurden die Emoticons oder Smileys erfunden. Sie sind mit normalen Druckerzeichen dargestellte „Grafiken“, die Stimmungen ausdrücken (sollen). Einige sind immer hilfreich. Eine lange Liste finden Sie unter <http://www.cg.tuwien.ac.at/~helwig/smileys.html>.

:-) ...Freude	:(...Traurigkeit	;-) ...Augenzwinkern
8- ...suspense	:#) ...drunk smiley	:* ...kisses
:~O ...no yelling! (quiet lab)	:-D ...user is laughing (at you!)	:-I ...hmm
:\ ...undecided smiley	:-o ...surprise	:-S ...what you say makes no sense
:-(*) ...that comment made me sick		

Abkürzungen

Da nicht jeder ein Weltmeister im Tippen ist, wurden (vor allem in den USA) Abkürzungen „erfunden“, die oft benutzt werden (und auch hilfreich sind). Eine umfangreiche Liste, aus der fast alle nachfolgenden übernommen wurden, finden Sie z.B. unter <http://www.volker-gringmuth.de/usenet/begriffe.htm>.

MfG	Mit freundlichen Grüßen
CU	See You
AFAIK	As Far As I Know
BTW	By The Way
FYI	For Your Information
GIGO	Garbage In, Garbage Out (Gibt man Müll rein, kommt Müll raus)
IMHO	In My Humble Opinion
ROTFL	Rolling On The Floor Laughing!
RSN	Real Soon Now
RTFM	Read The Fu... Manual!
SNAFU	Situation Normal, All Fouled Up
THANX	Thanks
WT	Without Thinking

WWW - Das World Wide Web

Das World Wide Web, auch Web, WWW oder W3 genannt, ist die z.Zt. wohl wichtigste und meistgenutzte Infrastruktur im Internet. Auf Millionen Web- oder WWW-Servern stehen Informationen, Grafiken, Programmen u.a. zum Abruf bereit.

Die Entwicklung des Web begann 1989 am CERN (Centre Europeenne de Recherche Nucleaire), dem Europäischen Zentrum für Atomphysik in der Nähe von Genf. Im Internet existierten damals bereits Informationssysteme wie Gopher, die den direkten Zugriff auf verteilte Informationen erlaubten. Da diese noch nicht die gewünschte Flexibilität aufwiesen, wurde ein neues, auf Client/Server-Architektur aufbauendes und hypertextbasiertes System entwickelt. Hypertext ist ein strukturierter, mit Querverweisen versehener Text (bzw. eine Menge von Texten), in dem mit Hilfe der Verweise „navigiert“ (hin und her gesprungen) werden kann. Der Benutzer benötigt im Web einen WWW-Client, einen sogenannten **Browser** wie Netscape Navigator, Internet Explorer oder Opera, um ein WWW-Dokument, eine **WWW-Seite** von einem **WWW-Server** (Rechner mit WWW-Server-Software) anzufordern und anzeigen zu lassen.

Auf Basis dieses Modells sind heute auf 100-Tausenden von WWW-Servern Milliarden Dokumente gespeichert, die mit der **HyperText Markup Language (HTML)** aufbereitet sind und neben „Formatierungsangaben“ sogenannte Links, d.h. Querverweise zu anderen Dokumenten oder Textteilen enthalten. Durch Klick auf einen solchen Link wird der betreffende Text von dem im Link angegebenen WWW-Server angefordert und vom Browser angezeigt. Die Übertragung von Anforderung und Dokument wird auf Basis des **HyperText Transfer Protocols (HTTP)** durchgeführt.

HTML-Text

Ein HTML-Text enthält neben dem eigentlichen Text sogenannte *Tags*, das sind Format- und Querverweis-*Bezeichner*. Anders als z.B. in Word wird der Text nicht formatiert z.B. als Überschrift 1, sondern ein „Befehl“ `<H1>` gibt dem Browser an, dass der folgende Text als Header1 (Überschrift 1) darzustellen ist. Ist die Überschrift zu Ende, so gibt dies ein komplementärer Befehl an `</H1>`. Analog gilt dies für andere Tags. Ein kleines Beispiel für einen HTML-Text:

```
<HTML>
<HEAD>
<TITLE>Ein HTML-Text</TITLE>
</HEAD>

<BODY>
<CENTER><H1><B>Beispiel eines HTML-Textes</B></H1> </CENTER>

<h2>Zugänge zum Internet </h2>
<P>
Möchten Sie über Modem auf das Internet zugreifen, so müssen
Sie zuerst die Telefonverbindung zu einem Internet-Provider herstellen und
können dann z.B. einen der folgenden Links wählen:
<P>
<a href="http://www.uni-koeln.de/index.html">Universität zu Köln</a>
<p>
<a href="http://www.heise.de/index.html">Heise Verlag</a>
```

```

<p>
<address>10.01.2003 Günter Marxen</address>
</BODY>
</HTML>

```

Groß-/Kleinschreibung von Tags ist nicht von Bedeutung. Das Dokument beginnt mit dem Tag <HTML> und endet mit </HTML>. <p> erzeugt einen neuen Absatz, <h1> und <h2> definieren Überschriften der 1. und 2. Ebene und legt einen Link, einen Querverweis fest. Bei href= steht die Adresse, die URL des Dokuments, auf das verwiesen wird, danach folgt der Text, der für den Link angezeigt und gekennzeichnet wird und beendet die Kennzeichnung als Link. Das Beispiel sieht in Netscape so aus:



URL – WWW-Adressen

Die URL - Uniform Resource Locator - gibt die Adresse einer Datei im WWW an. Sie hat die Form:

protocol://server/pfad/datei, wobei als *protocol* der Internet-Dienst, i.a. HTTP für WWW-Dokumente, ab und zu auch ftp für Dateiübertragung o.a. anzugeben ist. Die Server-Angabe hat meist die Form *WWW.name.tld*, etwa *WWW.UNI-KOELN.DE*. Nach dem Server folgt der Pfad (die Verzeichnis- oder Ordnerfolge auf dem Server), in dem die gesuchte HTML-Datei gespeichert ist, etwa *rrzk/mail/*. Während bei *protocol* und *server* die Groß-/Kleinschreibung nicht von Bedeutung ist, muss sie bei Pfaden und Dateinamen unbedingt beachtet werden.

Fehlt eine Dateiangabe, so liefert der WWW-Server i.a. automatisch die Datei **index.html** aus dem angegebenen Verzeichnis. Beispiele für URLs finden Sie weiter hinten.

Suchdienste

Die Fülle der Informationen im Internet ist inzwischen so groß, dass man vor lauter Bäumen den Wald nicht mehr sieht. Um dem abzuweichen wurden Suchmaschinen entwickelt und „implementiert“ (eingesetzt). Dies sind Server, die das Web durchsuchen und sozusagen Stichwortverzeichnisse für alle untersuchten Dokumente anlegen. Diese Stichwortverzeichnisse können vom Benutzer abgefragt werden. Der z.Zt. beste Suchdienst ist (meiner Meinung nach) **Google** (www.google.de oder www.google.com).

Gehen Sie z.B. mal zu Google und geben Sie als Suchbegriff *Geschichte des Internet* ein. Sie werden viele gute und ausführliche Dokumente hierzu finden. Vor allem sind die zuerst aufgeführten Dokumente i.a. wirklich die „besten“. Andere Suchdienste haben inzwischen das Verfahren von Google übernommen und sind dann wohl ebenfalls gut.

Browser

Browser sind die Client-Programme, um im Web zu surfen. Der verbreitetste ist der **Microsoft Internet Explorer**, der gute Leistungen bringt aber auch die größten Gefährdungen aufgrund seiner Integration in Windows (s. Internet Sicherheit).

Zurück gefallen ist der früher führende **Netscape Navigator**, der zusammen mit dem Mail-Client Messenger Teil des Netscape Communicators ist. Der Navigator ist weniger anfällig für Schädlinge.

Opera ist ein recht schneller Browser, den ich nicht persönlich kenne, der ebenfalls nicht so gefährdet ist wie der Internet Explorer und in Tests i.a. gute Kritiken bekommt.

Net News – Usenet

NetNews oder kurz News genannt, sind eine Art Konferenzsystem auf Basis von E-Mails. Es entstand Ende der 70er Jahre und wird heute von Tausenden von News-Servern „getragen“. Die Verbreitung erfolgt normalerweise per **NNTP, dem NetNews Transfer Protocol**.

Während normale E-Mails aber personen-bezogen sind, sind die „News-Gruppen“ öffentlich. News-Gruppen sind sozusagen Sammlungen von E-Mails zu einem bestimmten Thema, die auf News-Servern bereitgestellt werden.

Um am Usenet teilzunehmen, muss man die gewünschten Newsgruppen bei einem Server abonnieren, etwa bei news.rrz.uni-koeln.de. Als Client muss ein News-Reader benutzt werden, etwa der Netscape

Messenger, der mit dem Navigator Teil des Netscape Communicators ist.
Die Gruppen sind hierarchisch strukturiert. Die oberste Stufe beschreibt einen Themenkomplex oder ein Herkunftsland (de). Darunter werden Einzelthemen etc. aufgeführt. Einige Beispiele:

alt	alternative	bionet	für Biologen
comp	Computer bezogen...	de	deutsche Gruppen
sci	Natur- und Geisteswiss.		

Sonstiges

URLs von Internet-Organisationen

http://www.icann.com/	Internet Corporation for Assigned Names and Numbers
http://www.iana.org/	Internet Assigned Numbers Authority
http://www.isoc.org/	Internet Society
http://www.eff.org/	Electronic Frontier Foundation
http://www.w3.org/	WWW-Konsortium
http://www.denic.de	Network Information Center für Deutschland

URLs zur Geschichte des Internet

http://ip-service.com/IP/Vortrag/v_arpa.html (Arpanet)
http://www.dfn-expo.de/Geschichte/Geschichte_Internet.html
http://press.web.cern.ch/HSI/HNF-Europe/sem3_2001/HP_Networking/sld007.htm
<http://www.users.comcity.de/~horibo/history.htm>
<http://www.phil-fak.uni-duesseldorf.de/mmedia/web/start.html>
<http://www.michaelkaul.de/Geschichte/geschichte.html>
<http://www.ask.uni-karlsruhe.de/books/inetbuch/all.html> !!!

URLs zur Chemie

Departement of Chemistry der University of Sheffield
<http://www2.shef.ac.uk/chemistry/chemistry-home.html>

Molecular Graphics Software
3-dimensionale Darstellungen von molekularen Objekten sowie verschiedener Previewer
<ftp://stanzi.bchem.washington.edu/pub/raster3d/>

<http://www.uni-koeln.de/rrzk/software/liste.html#Chemie>
<http://www.uni-koeln.de/math-nat-fak/> und dort „Fachgruppe Chemie“

Sonstige URL

<http://www.billiger-surfen.de/>
<http://www.tariftip.de/>
<http://www.heise.de/itarif/>

<http://www.uni-koeln.de/rrzk/kurse/unterlagen/> „Windows für Einsteiger“
<http://www.uni-koeln.de/rrzk/beratung/freeware/index.html> Freeware für jeden PC

http://www.webhostlist.de	Web-Provider
http://www.google.de	Suchdienst
http://www.gmx.de	Provider von kostenlosen Mail-Adressen
http://www.mozilla.org	Mozilla-Projekt, freier „Open Source“ Web-Browser

Stichwortverzeichnis

Address Resolution Protocol	3	Netzklasse, Class A, B und C	4
Anwendungsschicht	3	Netzwerkschicht	3
AOL	6	Netzzugriff	3
Backdoor	7	NNTP	3
Browser	14f	NNTP, NetNews Transfer Protocol	15
Client / Server-Architektur	4	Oktett	4
Client-Software	4	Opera	15
Datenpaket	2	POP3	11
DE-NIC (Network Information Center)	5	Portnummer	3
DHCP: Dynamic Host Configuration Protocol	6	PostOffice	6, 10
Dialer	7	Protokoll	2f
Domain Name Server: DNS	6	Provider	6
Firewall	8	Rechnerkommunikation	2
Flatrate	7	remote host	2
ftp	3	Router, Rechner zur Verbindung 2er Netze	2
Gateway, Rechner zur Verbindung 2er Netze	2	Schichtenmodell	2
Google, Suchdienst	15	Server-Software	4
Hintertür	7	Site	9
host	2	SMTP	3
Host-Adresse	4	Subnetz-Maske	5
Host-Adresse, vollständige	4	TCP/IP: Transport Control Protocol/Internet Protocol	2
Host-Namen	5	Tiscali	6
HTTP	3	TLD, s. Top Level Domain	5
HyperText Markup Language (HTML)	14	t-online	6
HyperText Transfer Protocols (HTTP)	14	Top Level Domain (TLD)	5
ICANN	5	Transport-Schicht	3
IMAP	11	Trojaner	7
Internet-by-Call	6	UKLAN - Universität zu Köln Local Area Network	4
Intranet	9	URL - Uniform Resource Locator	15
IP-Adresse	4	Viren	7
LAN, Local Area Network	1	Virenschanner	8
local host	2	WAN, Wide Area Network	1
Microsoft Internet Explorer	15	WWW - Das World Wide Web	14
Netiquette	7	WWW-Seite	14
Netscape Communicators	15	WWW-Server	14
Netscape Navigator	15	ZAIK/RRZK	5
Netz-Adresse	4	Zone, s. TLD	5
Netz-Klasse	4		