Internet transparent

Christian Zahler

Technische Grundlagen

Jedes Netzwerk braucht Gemeinsamkeiten. Die (einzige!) Gemeinsamkeit im Internet ist die Art der Datenübertragung, das so genannte Protokoll. Im Internet wird das so genannte TCP/IP (*Transfer Control Protocol/Internet Protocol*) verwendet.

Jeder Rechner auf der ganzen Welt braucht eine eindeutige Adresse, um im Internet erkannt zu werden, die so genannte IP-Adresse. (Diese Adresse wird vom *Internet Protocol* IP genutzt). In der derzeit gültigen Version 4 des Internet Protokolls ist die IP-Adresse eine 32-stellige Binärzahl, also etwa:

11011001.01010011.11001111.00010001

Meist fasst man 8 Binärstellen (bits) zu einem Byte zusammen, dessen Wert man berechnet. Die "Kurzschreibweise" der oben angeführten IP-Adresse würde daher zum Beispiel lauten:

217.83.207.17

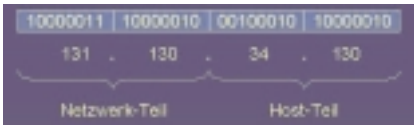
Diese Adressen werden von der *Internet Number Association* (IANE) vergeben.

Man hat also mit einer solchen 32 bit-Adresse insgesamt 2 = 4 294 967 296 Möglichkeiten (also mehr als 4 Milliarden), einen PC unverwechselbar zu adressieren. Man sollte meinen, dass diese große Anzahl für alle PCs der Welt ausreicht. Leider ist das nicht so!

Diese Adressen sind nämlich in zwei Teile geteilt:

Der erste Teil ist die **Netzwerk-Adresse**. Da das Internet aus vielen miteinander verbundenen lokalen Netzen (LAN) besteht, ist es sinnvoll, jedem LAN eine eindeutige Adresse zuzuweisen.

Der zweite Teil gibt die Adresse der einzelnen Rechner im Netz an (**Host-Adresse**). Dieser Teil wird durch das lokale Netzwerkmanagement frei vergeben.



Man hat nun verschiedene Größenklassen von Netzwerken festgelegt:

Class-A-Netze: Adresse beginnt mit einer binären 0, 7 bit für Netzwerk-Adresse, 24 bit für Host-Adresse. Damit gibt es weltweit 127 derartige Netzwerke, ein Class-A-Netz kann bis zu 16 Mio. Teilnehmer haben. Alle derartigen Netzadressen sind bereits belegt.

IP-Adressen von Class-A-Netzen:
0.0.0.0 bis **127.255.255.255**

Class-B-Netze: Adresse beginnt mit der binären Ziffernkombination 10, 14 bit für Netzwerk-Adresse, 16 bit für Host-Adresse. Damit gibt es weltweit 16384 derartige Netzwerke, ein Class-B-Netz kann bis zu 65536 Teilnehmer haben. Alle derartigen Netzadressen sind bereits belegt.

IP-Adressen von Class-B-Netzen:
128.0.0.0 bis **191.255.255.255**

Class-C-Netze: Adresse beginnt mit der binären Ziffernkombination 110, 21 bit für Netzwerk-Adresse, 8 bit für Host-Adresse. Damit gibt es weltweit 2 Mio. derartige Netzwerke, ein Class-C-Netz kann bis zu 256 Teilnehmer haben. Neu zugeteilte Netzadressen sind heute immer vom Typ C. Es ist abzusehen, dass bereits in Kürze alle derartigen Adressen vergeben sein werden. Man arbeitet daher an einem neuen Standard (Version 6 des Internet Protokolls, IPv6 oder IPng für „new generation"), der statt einer Adresslänge von 32 bit eine Länge von 128 bit haben soll. Um die Kompatibilität zu gewährleisten, wird die alte Adresse in der neuen Adresse "enthalten sein".

IP-Adressen von Class-C-Netzen:
192.0.0.0 bis **223.255.255.255**

Class D-Netze haben einen speziellen Anwendungsbereich (Multicast-Anwendungen) und haben für Internet keine Bedeutung.

Laut RFC 1918 sind für „private" Netze folgende IP-Bereiche gestattet (Rechner mit diesen IP-Adressen dürfen keinen direkten Internet-Verkehr haben, d.h. mit dem Internet nur über Proxy-Server in Kontakt treten; sie werden nicht geroutet!):

10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

Für einen Anwender sind derartige Zahlenkombinationen schwer zu merken. Es werden daher statt dieser Zahlendarstellung symbolische Namen verwendet.

So gibt es etwa einen Server mit dem Namen *noe.wifi.at*.

Diesem Servernamen entspricht eine eindeutige IP-Adresse. Dabei setzt sich der Name aus Teilen zusammen, die eine Hierarchie angeben: Das Teilnetzwerk "noe" (fachchinesisch bezeichnet man ein solches Teilnetz als **Domäne**, englisch *domain*) ist ein Teil des Netzwerks "wifi", dieses wiederum ein Teil des Netzwerks "at" (für Österreich). Das "at"-Netzwerk ist ein Teil der Domäne "the world" (die aber nie angegeben zu werden braucht).

Die Länderkennung ist ein Beispiel für eine **Top Level Domain (TLD)**; so werden die „Haupt-Domänen" bezeichnet, die entweder einem Land oder einer „Kategorie" entsprechen.

Die Zuordnung IP-Adressen zu logischen Namen muss von einem eigenen Rechner durchgeführt werden, dem Domain Name System-Server (DNS-Server). Wenn nun ein Anwender einen Server noe.wifi.at anwählt, so "fragt" die Station zunächst beim DNS-Server des Anwenders (der meist beim Provider steht), ob er die IP-Adresse von *noe.wifi.at* kennt. Das wird nicht der Fall sein. In diesem Fall hat der DNS-Server die IP-Adresse des nächstliegenden DNS-Servers gespeichert und fragt bei diesem an, ob er die IP-Adresse kennt. Das geht so lang, bis ein DNS-Server erfolgreich ist, die IP-Adresse wird übermittelt, die Datenübertragung kann beginnen.

Das Internet ist also ein so genanntes **Teilstrecken-Netzwerk**; es genügt, wenn jeder Internet-Knotenrechner mit einem weiteren Knoten verbunden ist. Die physikalische Datenübertragung wird über äußerst leistungsfähige Kabel, so genannte „Backbones" realisiert.

Eine Karte, die die europäische Struktur der Backbones zeigt, findet man unter *www.ebone.net/structure/backbone.html*.

Die zentrale Verwaltung der Domain-Namen mit den Top-Level-Domains .com, .net, .org und .int obliegt der **InterNIC**, einer Kooperation aus dem kommerziellen Unternehmen **NSI** (*Network Solutions Inc.*), der Telefongesellschaft AT&T sowie der US National Science Foundation. Bisher wurden die angegebenen Domains ausschließlich von der NSI im Auftrag der InterNIC verwaltet. Die jährliche „Miete" eines Domännamens kostet ca. 50 US-$. Die Domain-Verwaltung soll jedoch bis 2001 von der NSI an die nichtkommerzielle Organisation **ICANN** (*International Corporation for Assigned Names and Numbers*) übergeben werden. Die Datenbank der NSI ist unter
`www.networksolutions.com/cgi-bin/whois/whois/` zu finden.

Die **IANA** (*Internet Assigned Numbers Authority*, `www.iana.org`) verwaltet die IP-Adressen.

Einen IP-Adressen-Index findet man unter `ipindex.dragonstar.net`.

Die **ISPA** (*Internet Service Provider Association Austria* – `www.ispa.at`) ist die Vereinigung der österreichischen Internet Service Provider, quasi eine „Dachorganisation". Die NIC.AT GmbH, ein Unternehmen der ISPA, ist mit der Verwaltung und Vergabe der Domänennamen mit dem Top Level Domain „.at" beauftragt (`www.nic.at`). Registrierungen und Online-Abfragen von at-Domainen sind unter möglich.

Dabei gibt es zum Beispiel als Länder-Top Level Domain (ISO-Norm 3166):

at	Austria (Österreich)
de	Deutschland
jp	Japan
us	USA (fehlt meist)

Zusätzlich zu den landesspezifischen Erweiterungen gab es folgende Kennzeichnungen, die ursprünglich nur US-amerikanischen Einrichtungen vorbehalten waren:

com	company (Firma)
gov	government (Regierung) – US
edu	education (Universitäten) – US
mil	military (Militär) – US
int	internationale Organisation
org	organization (gemeinnützige Organisation)
net	Provider

Nun werden die Adressen von 28 lizenzierten Firmen vergeben. Diese Firmen werden im CORE (*Council of Registrars*) zusammengefasst. Die neuen TLDs lauten:

firm	Firmen und Unternehmen
arts	Kunst und Kultur
info	Informationsservices
rec	Unterhaltung und Freizeit
web	WWW-Aktivitäten
store	Warenangebote
nom	Restkategorie

MAC-Adresse = weltweit eindeutige Seriennummer, mit der jede Ethernet-Karte identifiziert wird

wird vom Hersteller fest eingebrannt

Unter TCP/IP besitzt jeder Rechner eine **ARP** (*Address-Resolution-Protocol*)-Tabelle, in der die Abbildung der IP-Adressen des lokalen Sub-Netzes auf die MAC-Adresse erfolgt.

Falls MAC-Adresse eines Rechners im Sub-Netz nicht bekannt, wird sie durch Rundfrage (*broadcast*) ermittelt. Rechner mit der gewünschten MAC-Adresse antwortet.

Besondere IP-Adressen

a) Netzwerkmasken

Netzwerkmasken unterscheiden sich in der Länge des Netzwerk- (alle Bit-Stellen auf 1) und Hostanteils (alle Bitstellen auf 0)

abhängig von der Netzwerkklasse

	1.Byte	2.Byte	3.Byte	4.Byte
Class A	255	0	0	0
Class B	255	255	0	0
Class C	255	255	255	0

Netzwerkmasken stellen einen Filter dar, an dem Rechner entscheiden können, ob sie sich im selben (logischen) Netz befinden

b) Netzwerkadressen

die Netzwerkadresse eines Rechners ergibt sich, indem man die IP-Adresse mit der Netzwerkmaske bitweise UND-verknüpft

generell gilt, dass bei Netzwerkadressen alle Bitstellen des Hostanteils 0 sind

Beispiel:

Class C	131	130	34	6	IP-Adresse
AND	255	255	255	0	Class C-Netzwerkmaske
=	131	130	34	0	Netzwerkadresse

nur Rechner mit der gleichen Netzwerkadresse befinden sich im gleichen logischen Netzwerk

c) Broadcast-Adresse

Die Broadcast-Adresse ergibt sich aus der IP-Adresse, bei der alle Bitstellen des Hostanteils auf 1 gesetzt sind. Sie bietet die Möglichkeit, Datenpakete an alle Rechner eines logischen Netzwerkes zu senden. Sie wird ermittelt, indem die Netzwerkadresse mit der invertierten Netzwerkmaske bitweise ODER-verknüpft wird.

Beispiel:

Class C	255	255	255	0	Class C-Netzwerkmaske
	0	0	0	255	invertierte Netzwerkmaske
OR	131	130	34	0	Class C-Netzwerkadresse
=	131	130	34	255	

d) Loopback-Adresse

Die Class-A-Netzwerkadresse 127 ist weltweit reserviert für das sogenannte *local loopback* und dient zu Testzwecken der Netzwerkschnittstelle des eigenen Rechners.

Die IP-Adresse **127.0.0.1** ist standardmäßig dem Loopback-Interface jedes Rechners zugeordnet.

alle an diese Adresse geschickten Datenpakete werden nicht nach außen ins Netzwerk gesendet, sondern an der Netzwerkschnittstelle reflektiert.

Die Datenpakete erscheinen, als kämen sie aus einem angeschlossenem Netzwerk

Datenübertragung im Internet

Bei der Datenübertragung im Internet laufen viele Vorgänge ab, von denen der Anwender nichts merkt. So werden im Internet nicht ganze Dateien übertragen, sondern sogenannte „**Pakete**“, auch „**IP-Datagramme**“ genannt.

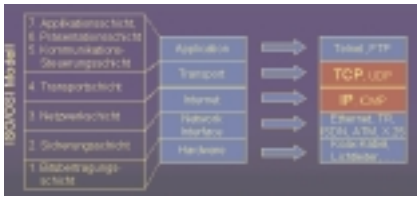
Damit ein Paket auch beim Empfänger ankommt, müssen eine Reihe von Informationen mit diesem Paket mitgeschickt werden.

Da die Datenübertragung in jedem Netzwerk sehr komplex ist, teilt man das Problem in Teilprobleme auf. Man unterscheidet sogenannte „Schichten“, die bestimmte Aufgaben erfüllen; im Internet könnte man folgende Schichten unterscheiden:

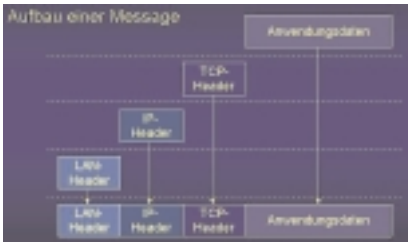
- Application (Anwendung): Benutzerebene (Surfen über WWW, FTP, ...)
- Transportschicht: Transport der Meldungen (verlässlich, ...)
- Netzwerkschicht: Adressierung, Verwaltung
- Network Interface: Daten auf das Medium (Kabel) bringen bzw. vom Medium (abholen)
- Hardware: Lichtwellenleiter, Kupferkabel

Jede Schicht (Teilfunktion) wird durch ein sogenanntes **Protokoll** realisiert; in der Praxis gibt es spezielle Treiber, die die Aufgaben von Protokollen übernehmen (in Windows gibt es etwa die TCP/IP-Treiber).

Man hat für alle Netzwerke ein einheitliches Schichtenmodell entworfen, das **ISO/OSI-7-Schicht-Referenzmodell**. In der folgenden Abbildung sehen Sie, welche Protokolle im Internet welche Aufgaben erfüllen:



Jede Schicht fügt spezielle Adress- und Protokollinformationen (sogenannte „**Header**“) zu den eigentlichen Daten hinzu. Dadurch wird das Datenpaket immer größer. Beim Empfänger durchläuft das Datenpaket die Protokolle in umgekehrter Reihenfolge, wobei die Daten dabei sozusagen „ausgepackt“ werden.



Protokolle niederer Schichten (Schichten 1, 2)

ARP, Address Resolution Protocol

Dieses Protokoll setzt IP-Adressen in MAC-Adressen um. Die meisten Netzwerke sind Ethernet-Netze; in diesen Netzen besitzt jeder Rechner (eigentlich: die Netzwerkkarte jedes Rechners) eine weltweit eindeutige Adresse, die sogenannte MAC-Adresse. Das ARP ordnet daher jeder IP-Adresse die korrekte Netzwerkkarte zu.

DHCP, Dynamic Host Configuration Protocol

Dieses Protokoll dient dazu, um Rechner im Netz bereits beim Booten konfigurieren zu können. So kann zum Beispiel jedem Rechner automatisch eine IP-Adresse zugewiesen werden.

PPP, Point to Point Protocol

Ermöglicht die Verbindung zweier Computer über eine serielle Leitung – wird heute immer bei Modemverbindungen zum Internet-Server verwendet. Das Protokoll arbeitet mit IP zusammen und bildet zusätzlich Prüfsummen zur Fehlerkontrolle. (Ein älteres Protokoll mit derselben Aufgabe war das SLIP = *Serial Line Internet Protocol*, welches heute aber nicht mehr verwendet wird).

Das Internet Protocol (IP) – Schicht 3

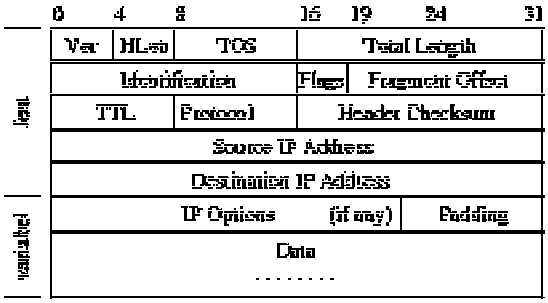
Wir haben bereits erwähnt, dass jedes Protokoll spezielle Informationen (den sogenannten Header) zu den eigentlichen Daten hinzufügt.

Hauptaufgaben des IP-Protokolls:

- **Adressierung** von Netzknoten
- **Routing** (Wegesuche im Netz)
- **Zerlegung** des Datenstroms in **Pakete**; ein **IP-Datenpaket** kann **maximal 65536 Bytes** groß sein.

Wir wollen hier den IP-Header etwas genauer betrachten. Zuerst sollen an dieser Stelle das Aussehen und die Bedeutung der einzelnen Header-Elemente beschrieben werden.

Abbildung: Der IP-Header



Die ersten vier Bits stellen das Feld **Ver** dar (siehe Abbildung). Sie sind für die Version des IP-Protokolls bestimmt, welches das zu sendende Datagramm zusammenstellt. Bei der Benutzung von IPv4 enthält dieses Feld den Wert vier.

Die nächsten vier Bit, die das Feld **HLen** repräsentieren, enthalten die aktuelle Header-Länge. Dabei werden aber nicht die Bytes, sondern die Doppel-Worte (4 Byte) gezählt. Bei einem IP-Standard-Header sollte hier eine fünf stehen. Dieser Standard-Header findet bei der Übertragung normaler Nutzdaten Anwendung. Er umfasst immer 5 Doppel-Worte = 20 Byte.

Danach folgt das Feld **TOS**, Type of Service. Es enthält u.a. Informationen, welcher Art die zu transportierenden Daten sind und welche Qualität die Art der Übertragung besitzen soll.

Das Feld **Total Length** im IP-Header kennzeichnet die totale Länge eines Datagramms einschließlich Header. Da dieses Feld nur eine 16-Bit-Zahl enthalten kann, ist auch die Größe eines IP-Datagramms auf maximal 2 - 1 = 65535 Byte beschränkt. Ein größeres Datagramm kann durch IP nicht vermittelt werden.

Auf die Bedeutung der Felder **Identification**, **Flags** und **Fragment Offset** wird später näher eingegangen. Sie werden benötigt, um eine Datagramm-Übermittlung auch über Netzverbindungen zu garantieren, die die maximale Größe eines IP-Datagramms nicht transportieren können.

Im Feld **TTL** wird die Lebenszeit, Time To Live, eines Datagramms verwaltet. Es dient zur Vorbeugung, dass ein Datagramm im Netz nicht ‚“ewig herumirrt“. Beim Verschicken des Datagramms wird durch den Sender eine Zahl in dieses Feld eingesetzt, die die Lebenszeit dieses Datagramms in Sekunden re-

präsentieren soll. Da aber ein anderer Host nicht weiß, wann dieses Datagramm erzeugt wurde und im Header auch keine Information über die Erzeugung vorhanden ist, repräsentiert diese Zahl in der Praxis etwas anderes. Sie gibt an, wie viele Router dieses Datagramm passieren darf, um den Empfänger zu erreichen. Dazu ist es notwendig, dass jeder benutzte Router den Wert dieses Feld um 1 erniedrigt. Ist irgendwann einmal der Wert des Feldes **TTL** gleich Null, dann wird es von dem Router, der es gerade bearbeitet, verworfen, und er sendet eine Fehlermeldung zurück an den Sender.

Das Feld **Protocol** wird von IP benutzt, um auf der Seite des Senders das Protokoll zu vermerken, welches die Dienste von IP in Anspruch nimmt. Auf der Seite des Empfängers dient es IP dazu, das Datagramm genau an dieses Protokoll zur weiteren Bearbeitung weiterzuleiten.

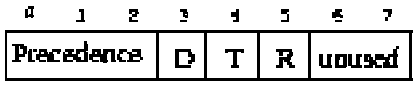
Das Feld **Header Checksum** beinhaltet eine Prüfsumme. Sie dient zum Erkennen von Verfälschungen bei der Übertragung des Datagramms. Allerdings wird sie nur über die Daten des IP-Headers selbst gebildet. Die zu transportierenden Daten werden nicht berücksichtigt. Soll über diesen Daten auch eine Prüfsumme zur Fehlererkennung gebildet werden, muß das ein anderes Protokoll oder die Anwendung selbst übernehmen, die die Dienste von IP in Anspruch nimmt. Die Überprüfung ist einfach zu vollziehen. Der das Datagramm bearbeitende Host, das kann auch ein Router sein, extrahiert den Wert aus dem Feld **Header Checksum** des Datagramms und berechnet diesen neu. Gleichen sich die beiden Werte nicht, wird IP dieses Datagramm verwerfen und eine Fehlermeldung an den Sender schicken. Ansonsten wird das Datagramm an den Empfänger zugestellt. Der Algorithmus zur Erstellung dieser Prüfsumme ist recht simpel. Der Wert dieser Prüfsumme stellt das Einerkomplement der Einerkomplementsumme des Headers dar. Dabei werden die Daten in Einheiten von 16 Bit zerteilt und addiert. Zur Berechnung wird der Header vollständig ausgefüllt. Das Feld **Header Checksum** wird vor der Berechnung mit Null initialisiert. Als Eingabe des Algorithmus bei einem Standard-Header dienen dann diese so vorbereiteten 20 Byte = 10 Worte. Das ermittelte Ergebnis wird zuletzt in das Feld **Header Checksum** übertragen. Der Grund, nur über den IP-Header eine Prüfsumme zu bilden, liegt darin begründet, dass diese Berechnung auf jedem Router durchgeführt werden muss. Dieses Verfahren stellt gegenüber der Berechnung über alle Daten eine erhebliche Beschleunigung der Vermittlung dar.

Zur Adressierung des Datagramms werden unbedingt die zwei Felder **Source IP Address** (Quell-Adresse) und **Destination IP Address** (Ziel-Adresse) benötigt. Die Ziel-Adresse dient zur Adressierung des Empfängers. Das Eintragen einer Quell-Adresse wird einmal zur etwaigen Erzeugung von Fehlermeldungen benötigt und außerdem dient sie dem Empfänger zur Identifizierung des Senders.

Im Feld **Data** können alle möglichen Nutzdaten transportiert werden.

Die Felder **IP Options** und **Padding** hängen direkt miteinander zusammen. Da der IP-Header immer Vielfache von Doppel-Worten enthalten muß, die Optionen aber verschieden lang sein können, wird das **Padding** zur Auffüllung genutzt, um wieder ein volles Doppel-Wort zu erhalten. Wird durch IP festgestellt, daß der Wert im Feld **HLen** größer als 5 ist, muß der Header Optionen enthalten. An Hand dieser Header-Länge ist auch ersichtlich, wo die Optionen enden und von wo ab eventuell Daten im Datagramm enthalten sind. Die Bedeutung der Optionen werden u.a. im RFC 791 beschrieben.

Abbildung: Das Feld TOS des IP-Headers



Die Abbildung zeigt den Aufbau des Feld **TOS**. Die drei Bits des Feldes **Precedence** kennzeichnen die Art des Datagramms. Sie können einen Wert zwischen 0 und 7 annehmen. Der Wert 0 wird bei einem Datagramm eingesetzt, welches normale Nutzdaten transportiert. Der Wert 7 wird für Datagramme zur Netzwerk-Steuerung verwendet. Näheres dazu ist im RFC 791 zu erfahren. Die Felder **D**, **T** und **R** legen fest, welcher Qualität die Art der Übertragung des Datagramms sein soll. Feld **D** macht dabei eine Aussage über die Schnelligkeit, Feld **T** über den Durchsatz und Feld **R** über die Verfügbarkeit der Übertragung. Setzt z.B. ein Sender das Bit in Feld **D** in einem Datagramm, verlangt er, dass dieses so schnell wie möglich an den Empfänger übermittelt wird.

Der Header muss grundsätzlich in der Netzwerk-Byte-Ordnung (*network byte order*) verschickt werden. Diese Ordnung wird auch *Big Endian* genannt.

Das Transfer/Transmission Control Protocol (TCP) – Schicht 4

Das TCP ist ein verbindungsorientiertes Protokoll; es bildet die Verbindung zwischen IP und Anwendung.

Aufgaben

- garantiert den sicheren Transport von Daten im Netz
- gewährleistet, dass kein Datenpaket verlorengeht und dass alle Pakete in der richtigen Reihenfolge ankommen

Merkmale

- vollduplex, bidirektionale (virtuelle) Verbindung
- Benutzer sieht Datenstrom, keine Pakete
- Zustellung der Information der entsprechenden Anwendung
- geregelter Verbindungsauf-/abbau

Der TCP-Header: Natürlich fügt auch das TCP-Protokoll spezielle Daten hinzu – wieder in Form eines Headers – der wie folgt aufgebaut ist:

- Sender/Empfänger-Port (je 16 B): Endpunkte der Verbindung
- Sequ./Quitt.nummer (32 B): Synchronisation der Daten
- Datenabstand (4 B): Länge des Headers in 32 B
- Flags (6 B): Aktionen (Aufbau, Ende, ...)
- Fenstergröße (16 B): Größe des verfügbaren Empfängerbuffers (bei 0 Stop des Senders)
- Prüfsumme (16 B): Korrektheit des Headers
- Urgent-Zeiger (16 B): zur Verarbeitung von wichtigen Daten
- Optionen (24 B), Füllzeichen (6 B)

Protokolle höherer Schichten – 5, 6, 7

Diese Protokolle sind sozusagen die gemeinsame „Sprache“ zwischen Serversoftware und Clientsoftware. Jedem Internet-Dienst ist ein solches Protokoll zugeordnet:

- **HTTP** = Hypertext Transfer Protocol: Surfen im WWW

- **FTP** = File Transfer Protocol: Upload und Download von Dateien
- **SMTP** = Simple Mail Transfer Protocol: Protokoll zum Senden von Mails (funktioniert nur, wenn Online!)
- **POP3** = Post Office Protocol, version 3: Protokoll zum Abholen von Mails (mit User- und Passwortabfrage)
- **NNTP** = Network News Transfer Protocol: Protokoll zum Arbeiten mit Newsgroups
- **Telnet**: Sitzung auf einem Remote Server (Terminal-Modus)

usw.

Well Known Port Numbers (RFC 1340): Fast immer laufen auf einem Internet-Server mehrere Dienste, etwa FTP, Archie, WWW etc. Um die einzelnen Dienste unterscheiden zu können, wurde jedem Dienst eine spezielle Kennung, die sogenannte „Port Number", zugewiesen. Um internationale Einheitlichkeit zu gewährleisten, wurden die „gut bekannten" Port Numbers im RFC 1340 (Request for Comment, „Bitte um Kommentar", de facto eine „Internet-Norm") zusammengestellt.

Ein Auszug folgt hier:

```
ftp-data        20/tcp    File Transfer [Default Data]
ftp             21/tcp    File Transfer [Control]
telnet          23/tcp    Telnet
                24/tcp    any private mail system
smtp            25/tcp    Simple Mail Transfer
                35/tcp    any private printer server
time            37/tcp    Time
rlp             39/tcp    Resource Locatio Protocol
graphics        41/tcp    Graphics
nameserver      42/tcp    Host Name Server
nicname         43/tcp    Who Is
domain          53/tcp    Domain Name Server
xns-auth        56/tcp    XNS Authentication
tftp            69/tcp    Trivial File Transfer
gopher          70/tcp    Gopher
finger          79/tcp    Finger
www             80/tcp    World Wide Web HTTP
hosts2-ns       81/tcp    HOSTS2 Name Server
xfer            82/tcp    XFER Utility
kerberos        88/tcp    Kerberos
su-mit-tg       89/tcp    SU/MIT Telnet Gateway
rtelnet        107/tcp    Remote Telnet Service
pop2           109/tcp    Post Office Protocol - Version 2
pop3           110/tcp    Post Office Protocol - Version 3
auth           113/tcp    Authentication Service
audionews      114/tcp    Audio News Multicast
sftp           115/tcp    Simple File Transfer Protocol
uucp-path      117/tcp    UUCP Path Service
sqlserv        118/tcp    SQL Services
nntp           119/tcp    Network News Transfer Protocol
statsrv        133/tcp    Statistics Service
netbios-ns     137/tcp    NETBIOS Name Service
netbios-dgm    138/tcp    NETBIOS Datagram Service
netbios-ssn    139/tcp    NETBIOS Session Service
imap2          143/tcp    Interim Mail Access Protocol v2
sqlsrv         156/tcp    SQL Service
pcmail-srv     158/tcp    PCMail Server
irc            194/tcp    Internet Relay Chat Protocol
ipx            213/tcp    IPX
imap3          220/tcp    Interactive Mail Access Protocol
conference     531/tcp    chat
netnews        532/tcp    readnews
netwall        533/tcp    for emergency broadcasts
uucp           540/tcp    uucpd
```

Wenn nötig, ist die Portnummer auch anzugeben (mit einem Doppelpunkt nach der eigentlichen Adresse). Ein Beispiel ist der bekannte Ö3-Chat:

Die Syntax in der URL-Zeile lautet allgemein:

```
Servertyp://servername.domain.tld:portnumber
```

Serverinstallation

1. Schritt

NT-Server installieren; kein Domänencontroller, sondern „alleinstehender Server"! CD-Key 040-0033861

2. Schritt

Windows NT Service Pack 3 installieren

3. Schritt

Microsoft Internet Explorer 4.0 installieren

4. Schritt

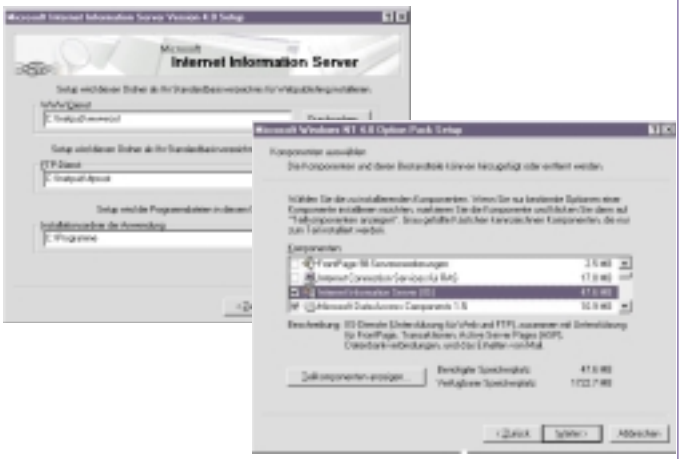
NT 4 Option Pack installieren

Lizenzvertrag annehmen.

Man kann auch die Standard-Variante installieren; wesentlich sind jedoch die Komponenten „Microsoft Script Debugger" und „IIS 4".

An dieser Stelle kann die Entscheidung getroffen werden, ob die Frontpage-Server-Extensions installiert werden sollen oder nicht. Für den Betrieb einer mit Frontpage erstellen Webseite sind diese Erweiterungen - die im wesentlichen aus vorgefertigten Java-Applets bestehen - unbedingt erforderlich. Ein Nachteil dieser Erweiterungen ist, dass unter Umständen Störungen im Betrieb des Servers auftreten können.

Bei den Standardverzeichnissen am besten vorläufig nichts ändern:



Zuordnen von Hostnamen zu IP-Adressen

(a) **Statisch**

Datei HOSTS im Verzeichnis

```
\WINNT\SYSTEM32\DRIVERS\ETC
```

bearbeiten mit Editor.

```
# Copyright (c) 1993-1995 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows NT.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host
127.0.0.1 localhost
192.168.0.1 ilg.at
```

Diese Datei ordnet jeder IP-Adresse einen DNS-Namen ("friendly name") zu.

Im selben Verzeichnis befindet sich auch die LMHOSTS-Datei, die die Zuordnung von IP-Adressen zu NetBIOS-Namen regelt (NetBIOS-Namen werden als "PC-ID" von Win NT standardmäßig verwendet).

Wichtig: Jeder PC im Intranet muss dieselbe HOSTS-Datei bekommen, da sonst der Server nicht mit dem friendly name angesprochen werden kann. (Also: Datei auf jeden PC im Netz kopieren!!!)

(b) **dynamisch**

DHCP-Server nötig (DHCP = dynamic host configuration protocol)

Diagnose- und Konfigurationsprogramme

1. PING

```
C:\WINDOWS>ping 10.0.0.6
```

Ping wird ausgeführt für 10.0.0.6 mit 32 Bytes Daten:

```
Antwort von 10.0.0.6: Bytes=32 Zeit<10ms TTL=128
Antwort von 10.0.0.6: Bytes=32 Zeit<10ms TTL=128
Antwort von 10.0.0.6: Bytes=32 Zeit<10ms TTL=128
Antwort von 10.0.0.6: Bytes=32 Zeit<10ms TTL=128
Ping-Statistik für 10.0.0.6:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0%
Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
```

2. IPCONFIG

```
C:\WINDOWS>ipconfig
Windows 98 IP-Konfiguration
0 Ethernet Adapter :
IP-Adresse. . . . . . . . . : 0.0.0.0
Subnet Mask . . . . . . . . : 0.0.0.0
Standard-Gateway . . . . . . :
1 Ethernet Adapter :
IP-Adresse. . . . . . . . . : 10.0.0.6
Subnet Mask . . . . . . . . : 255.0.0.0
Standard-Gateway . . . . . . : 193.170.244.18
C:\WINDOWS>
```

3. WINIPCFG

Am besten über [Start] – [Ausführen] aufrufen.

4. TRACERT

```
Syntax: TRACERT [-d] [-h Abschnitte max] [-j Host-Liste] [-w
Timeout] Zielname
Options:
-d Adressen nicht zu Hostnamen auswerten.
-h Abschnitte max Max. Anzahl an Abschnitten bei Zielsuche.
-j Host-Liste "Loose Source Route" gemäß Host-Liste.
-w Timeout Timeout in Millisekunden für eine Antwort.
```

5. ARP (Adress Resolution Protocol)

```
C:\WINDOWS>arp
Ändert und zeigt die Übersetzungstabellen für
IP-Adressen/physische
Adressen an, die vom ARP (Address Resolution Protocol)
verwendet werden.
ARP -s IP_Adr Eth_Adr [Schnittst]
ARP -d IP_Adr [Schnittst]
ARP -a [IP_Adr] [-N Schnittst]
-a Zeigt aktuelle ARP-Einträge durch Abfrage der Protokoll-
daten an. Falls IP_Adr angegeben wurde, werden die IP- und
physische Adresse für den angegebenen Computer angezeigt.
Wenn mehr als eine Netzwerkschnittstelle ARP verwendet,
werden die Einträge für jede ARP-Tabelle angezeigt.
-g Gleiche Funktion wie -a.
IP_Adr Gibt eine Internet-Adresse an.
-N Schnittst Zeigt die ARP-Einträge für die angegebene
Netzwerk-
schnittstelle an.
-d Löscht den durch IP_Adr angegebenen Host-Eintrag.
-s Fügt einen Host-Eintrag hinzu und ordnet die
Internet-Adresse
der physischen Adresse zu. Die physische Adresse
wird durch
6 hexadezimale, durch Bindestrich getrennte Bytes angegeben.
Der Eintrag ist permanent.
Eth_Adr Gibt eine physische Adresse (Ethernet-Adresse) an.
Schnittst Gibt, falls vorhanden, die Internet-Adresse der
Schnittstelle
an, deren Übersetzungstabelle geändert werden soll.
Sonst wird die erste geeignete Schnittstelle verwendet.
Beispiel:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Fügt einen
statischen Eintrag
hinzu.
> arp -a .... Zeigt die Arp-Tabelle an.
```

6. NETSTAT

Zeigt bestehende Netzwerkverbindungen an.

Beispiel für netstat:

```
C:\WIN98>netstat
Aktive Verbindungen
Proto Lokale Adresse Remote-Adresse Status
TCP nr:1026 I406:nbsession ESTABLISHED
TCP nr:1037 www.browser.at:80 ESTABLISHED
TCP nr:1045 WWWIFI:80 ESTABLISHED
```

7. ROUTE

Manipulation und Anzeige der Routingtabelle des Betriebssystems.

```
Beispiel für route:
C:\WIN98>route print
Aktive Routen:
Netzwerkadresse Subnet Mask Gateway-Adresse Schnittstelle
Anzahl
0.0.0.0 0.0.0.0 192.168.2.100 192.168.2.104 1
127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1
192.168.2.0 255.255.255.0 192.168.2.104 192.168.2.104 1
192.168.2.104 255.255.255.255 127.0.0.1 127.0.0.1 1
192.168.2.255 255.255.255.255 192.168.2.104 192.168.2.104 1
224.0.0.0 224.0.0.0 192.168.2.104 192.168.2.104 1
255.255.255.255 255.255.255.255 192.168.2.104 0.0.0.0 1
C:\WIN98>
```

FTP-Server einrichten und testen

FTP von der Anwenderseite aus gesehen

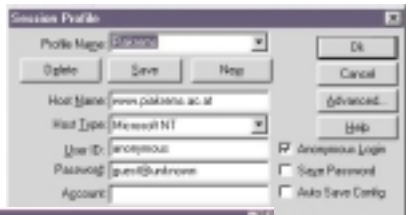
Mit FTP können Sie Dateien von Ihrem Rechner auf einen entfernten Server übertragen (Upload) oder von einem entfernten Server Dateien auf Ihren Rechner laden (Download).

Der FTP-Dienst ist auf verschiedene Art und Weise nutzbar:

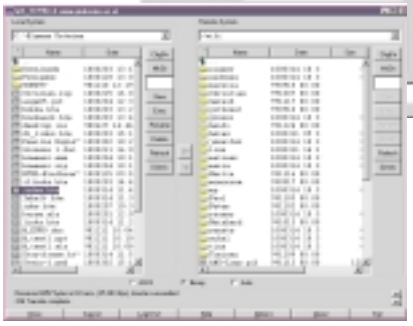
a) FTP-Programm: zum Bsp. WS-FTP

1. Starten Sie das Programm WS-FTP95

2. Legen Sie ein Profil mit folgenden Einträgen an (Klicken Sie auf die Schaltfläche „New“):



3. Mit "OK" verbinden Sie sich zum PIAKREMS-FTP-Server: Links sehen Sie die Verzeichnis-/Laufwerksstruktur Ihres eigenen Rechners, rechts sehen Sie die Verzeichnisstruktur des FTP-Servers, mit dem Sie verbunden sind.



4. Mit den Pfeilen in der Mitte können Sie markierte Dateien von Ihrer Festplatte (links) auf den Server (rechts) kopieren oder umgekehrt!

b) Manuelle FTP-Sitzung:

Aufruf:

ftp *Servername*

FTP-Befehle

```
! delete literal prompt send
? debug ls put status
append dir mdelete pwd trace
ascii disconnect mdir quit type
bell get mget quote user
binary glob mkdir recv verbose
bye hash mls remotehelp
cd help mput rename
close lcd open rmdir
dir remote Verzeichnis auflisten
cd, lcd Verzeichnis wechseln, remote / local
pwd aktuelles Verzeichnis
get, mget Datei/en von remote nach local kopieren
put, mput Datei/en von local nach remote kopieren
binary auf binären Transfer (Programme, Images, ...)
umschalten
prompt Bestätigung abschalten
user als Benutzer einloggen
open, close Verbindung öffnen / schließen
? Hilfe anzeigen
quit, bye Programm beenden
```

Beispiel für eine manuelle FTP-Sitzung (Benutzereingaben sind fett dargestellt)

```
C:\WIN98>ftp off97.noe.wifi.at
Verbindung mit off97.noe.wifi.at.
220 wifi2 Microsoft FTP Service (Version 3.0).
Benutzer (off97.noe.wifi.at:(none)): user401
331 Password required for user401.
Kennwort:****
230-Herzlich Willkommen am Wifi Ftp-Server !
230 User user401 logged in.
Ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
d--------- 1 owner group 0 Aug 19 1999 kids
d--------- 1 owner group 0 Feb 17 1998 kktn
---------- 1 owner group 0 Aug 18 1999 test.txt
---------- 1 owner group 0 Aug 19 1999 test3.txt
226 Transfer complete.
Ftp: 269 Bytes empfangen in 0.16Sekunden 1.68KB/Sek.
Ftp> get test.txt
200 PORT command successful.
150 Opening ASCII mode data connection for test.txt(0 bytes).
226 Transfer complete.
Ftp> put xxx.htm
200 PORT command successful.
150 Opening ASCII mode data connection for xxx.htm.
226 Transfer complete.
Ftp: 1777 Bytes gesendet in 0.00Sekunden 1777000.00KB/Sek.
Ftp> pwd
257 "/" is current directory.
Ftp> quit
221 Auf Wiedersehen !
```

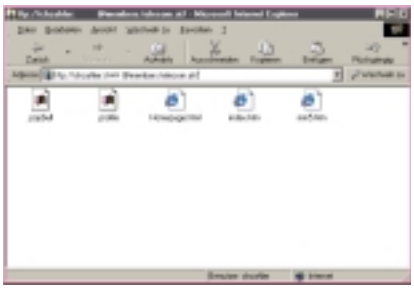
Wenn Sie als anonymer FTP-Nutzer arbeiten wollen, so geben Sie als Benutzername anonymous an, als Kennwort Ihre eigene E-Mail-Adresse. (Es ist kein Passwort nötig, allerdings verlangen die Regeln der Netiquette eine derartige – freiwillige! – Identifizierung.)

c) FTP über den Browser

Auch über Browser-Software ist eingeschränkter FTP-Betrieb möglich: Während Downloads problemlos möglich sind, können Uploads nicht durchgeführt werden!

Wichtig: Sollten Sie für den FTP-Server einen Benutzernamen und ein Kennwort eingeben müssen, dann wählen Sie bitte folgende Syntax für die Adresszeile des Browsers:

ftp://Benutzername:Kennwort@ftpserver.at



(Anmerkung: Das Passwort in der obigen Abbildung wurde abgedeckt bzw. verändert.)**FTP von der Serverseite aus gesehen – Einrichten und Konfigurieren des FTP-Dienstes im Internet Information Server:**