8 Internet Protocol Version 4 (IPv4)

Christian Zahler

Hauptaufgaben des IP-Protokolls:

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

Jeder Rechner auf der ganzen Welt braucht eine eindeutige Adresse, um im Internet oder in einem lokalen TCP/IP-Netzwerk erkannt zu werden, die so genannte IP-Adresse. 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 dezimalen Wert man berechnet. Die "Kurzschreibweise" *(dotted decimal)* der oben angeführten IP-Adresse würde daher zum Beispiel lauten:

```
217.83.207.17
```

8.1 Zuweisung von IP-Adressen

IP-Adressen können einer Netzwerkschnittstelle auf zwei Arten zugewiesen werden:

8.1.1 Statische Konfiguration

Die IP-Konfiguration wird manuell festgelegt und ändert sich nicht; in Windows wird die Konfiguration in den Netzwerkeigenschaften (Systemsteuerung) festgelegt.

Statische Konfiguration von IP-Adressen unter Windows mit GUI

Siehe Bild rechts oben; darunter die dynamische Konfiguration für Windows (siehe 8.1.2).

Konfiguration von IP-Adressen unter Windows über die Command Shell

```
netsh interface ipv4 set address name=LAN-
Verbindung source=static address=10.1.101.108
mask=255.255.255.0 gateway=10.1.101.1

netsh interface ipv4 set dnsserver name=LAN-
Verbindung source=static address=10.1.101.63
```

Es ist auch folgende Kurzschreibweise möglich:

```
netsh interface ipv4 set address LAN-
Verbindung static 10.1.101.108 255.255.255.0
10.1.101.1

netsh interface ipv4 set dnsserver static LAN-
Verbindung 10.1.101.63
```

Hinweise zu netsh

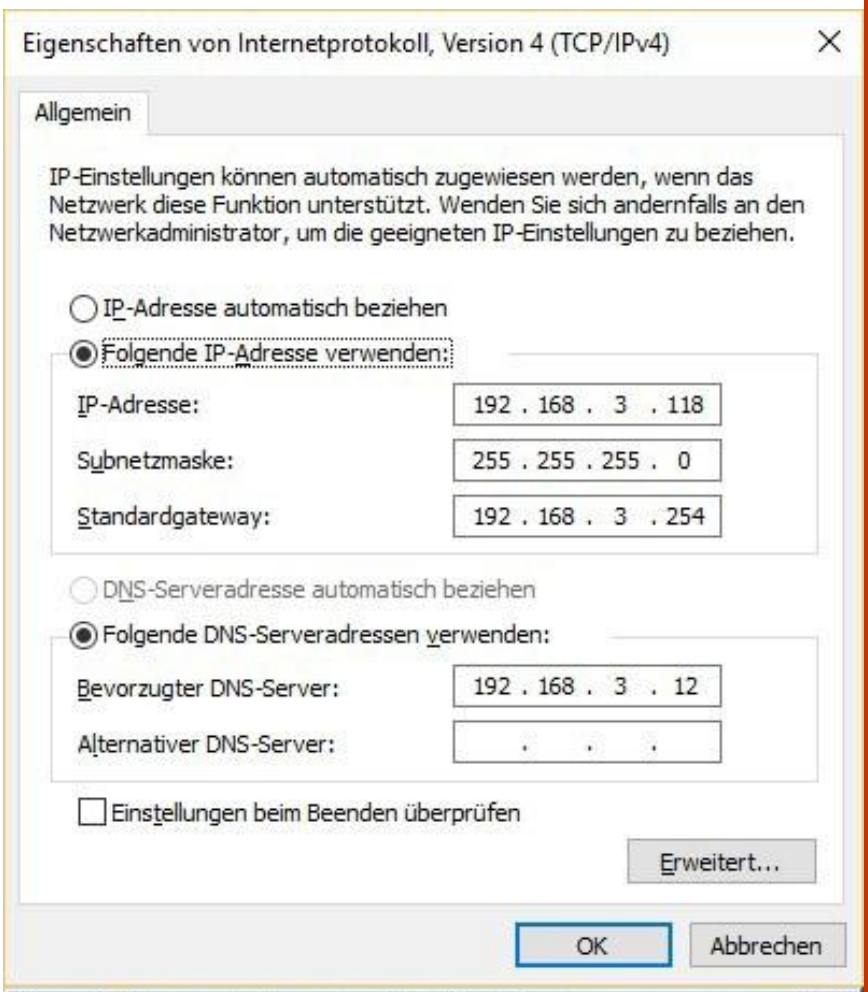
https://technet.microsoft.com/en-us/library/bb490939.aspx

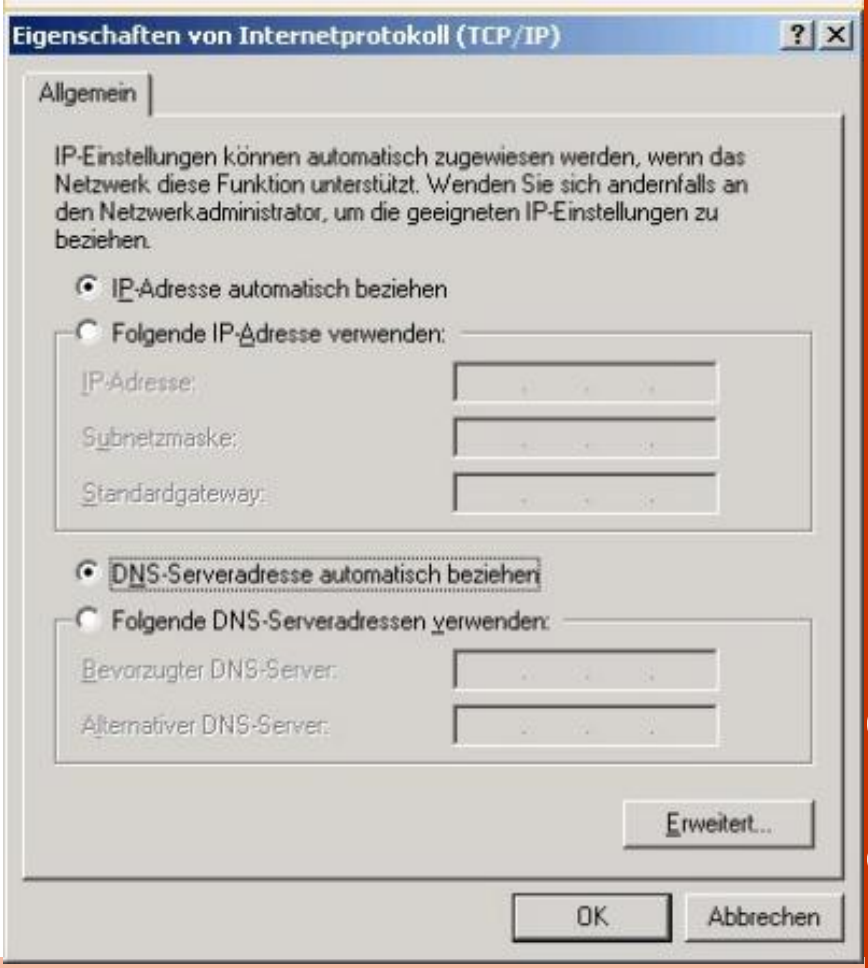
Konfiguration unter Linux

Die IP-Konfiguration befindet sich in der Datei `/etc/network/interfaces` und kann dort mit einem beliebigen Editor bearbeitet werden, etwa wie folgt:

```
iface eth0 inet static
Address 192.168.1.100
Netmask 255.255.255.0
Network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.254
```

Ethernet-Netzwerkschnittstellen unter Linux werden mit `eth0, eth1...` bezeichnet.





Hinweis: Unter Ubuntu Linux muss `vi` als Superuser `sudo` aufgerufen werden (in den meisten anderen Distributionen ist der übliche `root`-User erforderlich):

```
$ sudo vi /etc/network/interfaces
```

Die DNS-Konfiguration befindet sich in `/etc/resolv.conf` und kann dort geändert werden, zum Beispiel:

```
search myisp.com
nameserver 192.168.1.254
nameserver 202.54.1.20
nameserver 202.54.1.30
```

Die Schnittstellenkonfiguration kann auch mit dem Bash-Tool `ifconfig` geändert werden:

Ubuntu-Linux:

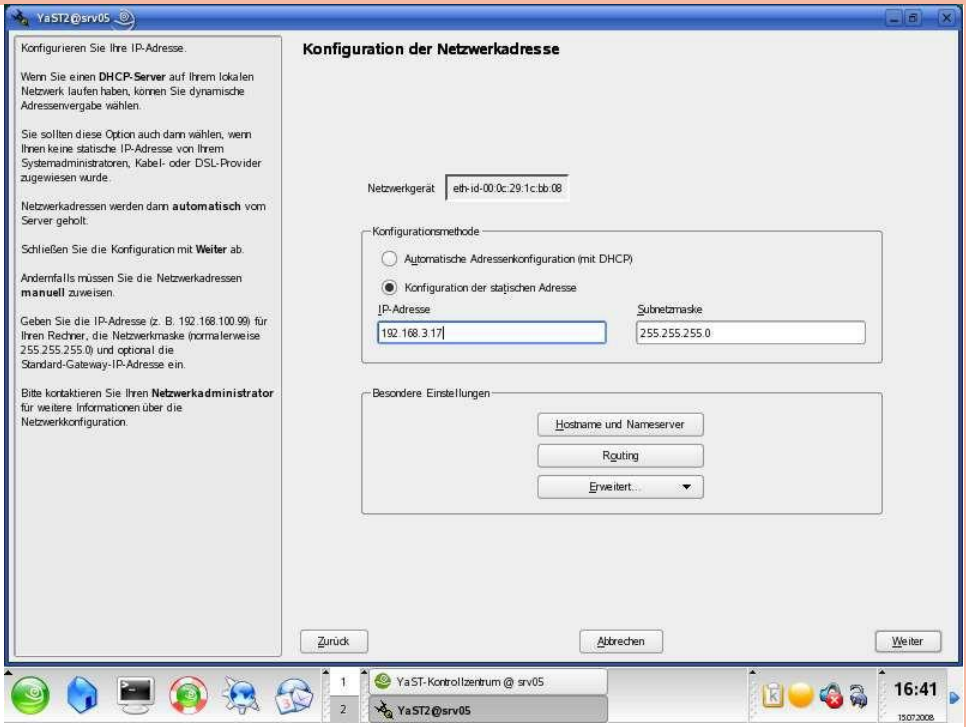
```
$ sudo ifconfig eth0 down
$ sudo ifconfig eth0 192.168.1.50 net-
mask 255.255.255.0 up
```

Unix (FreeBSD, OS-X):

```
ifconfig eth0 192.168.0.254/27
```

Neuere Linux-Distributionen:

```
ip addr add 192.168.0.254/27 brd + dev
eth0
```



Ein GUI-Konfigurationstool kann unter Ubuntu-Linux folgendermaßen gestartet werden:

```
$ network-admin &
```

In SuSE-Linux kann die IP-Konfiguration auch über Yast vorgenommen werden (siehe Bild rechts oben).

8.1.2 Dynamische Konfiguration

Die IP-Konfiguration wird von einem DHCP-Server *(Dynamic Host Configuration Protocol)* bezogen; die konkrete IP-Adresse wird bei jedem Neustart vom DHCP-Server neu zugewiesen und kann sich daher auch ändern. (siehe Bild vorige Seite unten)

Konfiguration unter Linux: Ändern Sie die Datei `/etc/network/interfaces` wie folgt:

```
iface eth0 inet dhcp
```

8.2 ipconfig

Gibt Informationen über die Windows IP-Konfiguration aus. Unter Linux ist stattdessen `ifconfig` oder `ip` zu verwenden.

Syntax für Windows 10:

```
ipconfig [/allcompartments] [/? | /all |
/renew [Adapter] | /release [Adapter] |
/renew6 [Adapter] | /release6 [Adapter] |
/flushdns | /displaydns | /registerdns |
/showclassid Adapter |
/setclassid Adapter [Klassen-ID] |
/showclassid6 Adapter |
/setclassid6 Adapter [Klassen-ID] ]
```

wobei:

`Adapter` Verbindungsname

(Platzhalter * und ? sind zulässig, siehe Beispiele)

Optionen:

```
/? Zeigt diese Hilfe an.
/allZeigt alle Konfigurationsinformationen an.
/release Gibt die IPv4-Adresse für den angegebenen Adapter frei.
/release6 Gibt die IPv6-Adresse für den angegebenen Adapter frei.
/renew Erneuert die IPv4-Adresse für den angegebenen Adapter.
/renew6Erneuert die IPv6-Adresse für den angegebenen Adapter.
/flushdns Leert den DNS-Auflösungscache.
/registerdns Aktualisiert alle DHCP-Leases und registriert DNS-
Namen erneut.
/displaydns  Zeigt den Inhalt des DNS-Auflösungscaches an.
/showclassid Zeigt alle für diesen Adapter zugelassenen DHCP-
Klassen-IDs an.
/setclassid  Ändert die DHCP-Klassen-ID.
/showclassid6 Zeigt alle für diesen Adapter zugelassenen IPv6-
DHCP-Klassen-IDs an.
/setclassid6 Ändert die IPv6-DHCP-Klassen-ID.
```

Standardmäßig werden nur die IP-Adresse, die Subnetzmaske und das Standardgateway für jeden an TCP/IP gebundenen Adapter angezeigt.

Wenn bei `/release` und `/renew` kein Adaptername angegeben wird, werden die IP-Adressenleases für alle an TCP/IP gebundenen Adapter freigegeben oder erneuert.

Wenn bei `/setclassid` und `/setclassid6` keine Klassen-ID angegeben wird, wird die Klassen-ID entfernt.

Beispiele:

`> ipconfig` ... Zeigt Informationen an.

`> ipconfig /all` ... Zeigt detaillierte Informationen an.

`> ipconfig /renew` ... Erneuert alle Adapter.

`> ipconfig /renew EL*` ... Erneuert alle Verbindungen, deren Namen mit `"EL"` beginnen.

`> ipconfig /release *Ver*`... Gibt alle übereinstimmenden Verbindungen frei, z. B. `"Lokale Verbindung 1"` oder `"Lokale Verbindung 2"`

`> ipconfig /allcompartments` ... Zeigt Informationen zu allen Depots an.

`> ipconfig /allcompartments /all`... Zeigt detaillierte Informationen zu allen Depots an.

Beispiel 1: Ausgabe ohne Parameter `/all`

```
C:\>ipconfig
Windows-IP-Konfiguration
Ethernet-Adapter LAN-Verbindung:
  Verbindungsspezifisches DNS-Suffix: zahler.at
  Verbindungslokale IPv6-Adresse . : fe80::b91b:f8f0:ccbe:4723%11
  IPv4-Adresse . . . . . : 192.168.3.117
  Subnetzmaske . . . . . : 255.255.255.0
  Standardgateway . . . . . : 192.168.3.14
Tunneladapter isatap.zahler.at:
  Medienstatus. . . . . : Medium getrennt
  Verbindungsspezifisches DNS-Suffix: zahler.at
```

Beispiel 2: Ausgabe mit Parameter `/all`

```
C:\>ipconfig /all
Windows-IP-Konfiguration
Hostname  . . . . . : pc01
Primäres DNS-Suffix . . . . . : zahler.at
Knotentyp . . . . . : Hybrid
IP-Routing aktiviert  . . . . . : Nein
WINS-Proxy aktiviert  . . . . . : Nein
DNS-Suffixsuchliste . . . . . : zahler.at
```

```
Ethernet-Adapter LAN-Verbindung:
Verbindungsspezifisches DNS-Suffix: zahler.at
Beschreibung. . . . . : Fast-Ethernet-Netzwerkkarte für Realtek R TL8139/810x-Familie
Physikalische Adresse . . . . . : 00-16-17-C4-65-6C
DHCP aktiviert. . . . . : Ja
Autokonfiguration aktiviert . . . : Ja
Verbindungslokale IPv6-Adresse  . : fe80::b91b:f8f0:ccbe:4723%11(Bevorzugt)
IPv4-Adresse  . . . . . : 192.168.3.117(Bevorzugt)
Subnetzmaske  . . . . . : 255.255.255.0
Lease erhalten. . . . . : Mittwoch, 27. Jänner 2010 03:22:04
Lease läuft ab. . . . . : Montag, 08. Februar 2010 03:21:55
Standardgateway . . . . . : 192.168.3.14
DHCP-Server . . . . . : 192.168.3.11
DHCPv6-IAID . . . . . : 201332247
DHCPv6-Client-DUID. . . . . : 00-01-00-01-0D-30-4A-2D-00-16-17-C4-65-6C
DNS-Server  . . . . . : 192.168.3.11
Primärer WINS-Server. . . . . : 192.168.3.11
NetBIOS über TCP/IP . . . . . : Aktiviert

Tunneladapter isatap.zahler.at:
Medienstatus. . . . . : Medium getrennt
Verbindungsspezifisches DNS-Suffix: zahler.at
Beschreibung. . . . . : Microsoft-ISATAP-Adapter
Physikalische Adresse . . . . . : 00-00-00-00-00-00-00-E0
DHCP aktiviert. . . . . : Nein
Autokonfiguration aktiviert . . . : Ja
```

8.3 Vergabe von IPv4-Adressen

Man unterscheidet öffentliche und private IPv4-Adressen.

8.3.1 Öffentliche IPv4-Adressen (Public IPs)

Diese Adressen werden von der *Internet Assigned Numbers Authority* (IANA) vergeben. Diese Adressbereiche sind weltweit eindeutig und werden zur Adressierung von Geräten verwendet, die im Internet erreicht werden sollen. Solche Adressen können Sie über Ihren Internet Service Provider beziehen (nicht direkt bei der IANA).

Die IANA vergibt Adressbereiche an fünf regionale Vergabestellen, die *Regional Internet Registries* (RIR) genannt werden:

- AfriNIC (*African Network Information Centre*) – zuständig für Afrika
- APNIC (*Asia Pacific Network Information Centre*) – zuständig für die Region Asien/Pazifik
- ARIN (*American Registry for Internet Numbers*) – Nordamerika (USA, Kanada, einige Karibikinseln)
- LACNIC (*Regional Latin-American and Caribbean IP Address Registry*) – Lateinamerika und einige Karibikinseln
- RIPE NCC (*Réseaux IP Européens Network Coordination Centre*) – Europa, Naher Osten, Zentralasien.

Die *Local Internet Registries* (LIR) genannten lokalen Vergabestellen vergeben die ihnen von den RIRs zugeteilten Adressen weiter an ihre Kunden. Die Aufgabe der LIR erfüllen in der Regel Internet Service Provider. Kunden der LIR können entweder Endkunden oder weitere (Sub-)Provider sein.

Die Adressen können dem Kunden entweder permanent zugewiesen werden (static IP, feste IP) oder beim Aufbau der Internetverbindung dynamisch zugeteilt werden (dynamic IP, dynamische IP). Fest zugewiesene Adressen werden v. a. bei Standleitungen verwendet oder wenn Server auf der IP-Adresse betrieben werden sollen.

Welchem Endkunden oder welcher *Local Internet Registry* eine IP-Adresse bzw. ein Netz zugewiesen wurde, lässt sich über die Whois-Datenbanken der RIRs ermitteln. Siehe Tabelle auf den folgenden Seiten.

8.3.2 Private IP-Adressbereiche (Private IPs)

Für die Verwendung innerhalb von LANs wurden eigene Adressbereiche festgelegt, die nicht geroutet werden. Diese IP-Adressen sind daher auch nicht weltweit eindeutig, sondern nur im jeweiligen lokalen Netzwerk.

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 (Class A-Bereich)
172.16.0.0  – 172.31.255.255 (Class B-Bereich)
192.168.0.0 – 192.168.255.255 (Class C-Bereich)
```

8.4 Aufbau von IP-Adressen

Beispiel:

```
Adresse         192.168.100.1
Subnetzmaske    255.255.255.0
```


```
   192       168       100         1
11000000  10101000  01100100  00000001
```

Um IPv4-Adressen verstehen zu können, muss man sich vor Augen halten, dass die „reale" Schreibweise von Adressen in binärer Form erfolgt (4 Oktetts a 8 Bit).

Gerechnet wird dann wie folgt:

```
    128  64  32  16   8   4   2   1
192   1   1   0   0   0   0   0   0
168   1   0   1   0   1   0   0   0
100   0   1   1   0   0   1   0   0
  1   0   0   0   0   0   0   0   1
255   1   1   1   1   1   1   1   1

192   =   1100 0000   = 128 + 64
168   =   1010 1000   = 128 + 32 + 8
100   =   0110 0100   = 64 + 32 + 4
1     =   0000 0001   = 1
```

Man hat also mit einer solchen 32 bit-Adresse insgesamt 2^{32} = 4 294 967 296 Möglichkeiten (also mehr als 4 Milliarden), einen PC unverwechselbar zu adressieren.

IP-Adressen bestehen aus zwei Teilen:

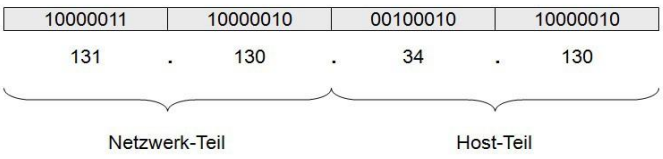
Der erste Teil ist die Netzwerk-Adresse (Net-ID). Da das Internet aus vielen miteinander verbundenen lokalen Netzen (LAN) besteht, ist es sinnvoll, jedem LAN eine eindeutige Adresse zuzuweisen.

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

Wie viele bit zur NetID bzw. zur HostID gehören, wird durch die Subnetz-Maske festgelegt. Dafür gibt es folgende einfache Regel:

- Ist ein bit der Subnetzmaske 1, so gehört das entsprechende bit der IP-Adresse zur Net-ID.
- Ist ein bit der Subnetzmaske 0, so gehört das entsprechende bit der IP-Adresse zur Host-ID.

Im obigen Beispiel würde also die Subnetzmaske 255.255.0.0



lauten.

Grundsätzlich ist die Länge der Net-ID und der Host-ID frei wählbar. Das war aber nicht immer so. In der ursprünglichen Implementierung von IPv4 (1981, RFC 791) verwendete man klassenorientiertes IP-Routing (fixe Länge von Net-ID und Host-ID). Dieses wurde 1993 durch das Verfahren CIDR (*Classless Inter Domain Routing*, Kap. 8.8) ersetzt (RFC 1518 und 1519); bei CIDR ist die Länge von Net-ID und Host-ID frei wählbar.

8.5 Klassenorientierte IP-Adressen

Diese Methode basierte auf fix festgelegten Längen für den Net- und den Host-Anteil der IP-Adressen. Sie wurde durch CIDR (*Classless Inter Domain Routing*, Kap. 8.8) verworfen.

Class-A-Netze: Adresse beginnt mit einer binären 0, 7 bit für Netzwerk-Adresse, 24 bit für Host-Adresse. Damit gibt es welt-

Liste der zugewiesenen IP-Adressen

Quelle: http://www.iana.org , Stand: 10.08.2015

Prefix	Designation	Date	Whois	Status
000/8	IANA—Local Identification	1981-09		RESERVED
001/8	APNIC	2010-01	whois.apnic.net	ALLOCATED
002/8	RIPE NCC	2009-09	whois.ripe.net	ALLOCATED
003/8	General Electric Company	1994-05	whois.arin.net	LEGACY
004/8	Level 3 Communications, Inc.	1992-12	whois.arin.net	LEGACY
005/8	RIPE NCC	2010-11	whois.ripe.net	ALLOCATED
006/8	Army Information Systems Center	1994-02	whois.arin.net	LEGACY
007/8	Administered by ARIN	1995-04	whois.arin.net	LEGACY
008/8	Level 3 Communications, Inc.	1992-12	whois.arin.net	LEGACY
009/8	IBM	1992-08	whois.arin.net	LEGACY
010/8	IANA - Private Use	1995-06		RESERVED
011/8	DoD Intel Information Systems	1993-05	whois.arin.net	LEGACY
012/8	AT&T Bell Laboratories	1995-06	whois.arin.net	LEGACY
013/8	Administered by ARIN	1991-09	whois.arin.net	LEGACY
014/8	APNIC	2010-04	whois.apnic.net	ALLOCATED
015/8	Hewlett-Packard Company	1994-07	whois.arin.net	LEGACY
016/8	Digital Equipment Corporation	1994-11	whois.arin.net	LEGACY
017/8	Apple Computer Inc.	1992-07	whois.arin.net	LEGACY
018/8	MIT	1994-01	whois.arin.net	LEGACY
019/8	Ford Motor Company	1995-05	whois.arin.net	LEGACY
020/8	Computer Sciences Corporation	1994-10	whois.arin.net	LEGACY
021/8	DDN-RVN	1991-07	whois.arin.net	LEGACY
022/8	Defense Information Systems Agency	1993-05	whois.arin.net	LEGACY
023/8	ARIN	2010-11	whois.arin.net	ALLOCATED
024/8	ARIN	2001-05	whois.arin.net	ALLOCATED
025/8	UK Ministry of Defence	1995-01	whois.ripe.net	LEGACY
026/8	Defense Information Systems Agency	1995-05	whois.arin.net	LEGACY
027/8	APNIC	2010-01	whois.apnic.net	ALLOCATED
028/8	DSI-North	1992-07	whois.arin.net	LEGACY
029/8	Defense Information Systems Agency	1991-07	whois.arin.net	LEGACY
030/8	Defense Information Systems Agency	1991-07	whois.arin.net	LEGACY
031/8	RIPE NCC	2010-05	whois.ripe.net	ALLOCATED
032/8	Administered by ARIN	1994-06	whois.arin.net	LEGACY
033/8	DLA Systems Automation Center	1991-01	whois.arin.net	LEGACY
034/8	Halliburton Company	1993-03	whois.arin.net	LEGACY
035/8	Administered by ARIN	1994-04	whois.arin.net	LEGACY
036/8	APNIC	2010-10	whois.apnic.net	ALLOCATED
037/8	RIPE NCC	2010-11	whois.ripe.net	ALLOCATED
038/8	PSINet, Inc.	1994-09	whois.arin.net	LEGACY
039/8	APNIC	2011-01	whois.apnic.net	ALLOCATED
040/8	Administered by ARIN	1994-06	whois.arin.net	LEGACY
041/8	AFRINIC	2005-04	whois.afrinic.net	ALLOCATED
042/8	APNIC	2010-10	whois.apnic.net	ALLOCATED
043/8	Administered by APNIC	1991-01	whois.apnic.net	LEGACY
044/8	Amateur Radio Digital Communications	1992-07	whois.arin.net	LEGACY
045/8	Administered by ARIN	1995-01	whois.arin.net	LEGACY
046/8	RIPE NCC	2009-09	whois.ripe.net	ALLOCATED
047/8	Administered by ARIN	1991-01	whois.arin.net	LEGACY
048/8	Prudential Securities Inc.	1995-05	whois.arin.net	LEGACY
049/8	APNIC	2010-08	whois.apnic.net	ALLOCATED
050/8	ARIN	2010-02	whois.arin.net	ALLOCATED
051/8	Administered by RIPE NCC	1994-08	whois.ripe.net	LEGACY
052/8	Administered by ARIN	1991-12	whois.arin.net	LEGACY
053/8	Daimler AG	1993-10	whois.ripe.net	LEGACY
054/8	Administered by ARIN	1992-03	whois.arin.net	LEGACY
055/8	DoD Network Information Center	1995-04	whois.arin.net	LEGACY
056/8	US Postal Service	1994-06	whois.arin.net	LEGACY
057/8	Aeronautiques S.C.R.L.	1995-05	whois.ripe.net	LEGACY
058/8 – 061/8	APNIC	2004-04	whois.apnic.net	ALLOCATED
062/8	RIPE NCC	1997-04	whois.ripe.net	ALLOCATED
063/8 – 076/8	ARIN	1997-04	whois.arin.net	ALLOCATED

077/8 – 095/8	RIPE NCC	2006-08	whois.ripe.net	ALLOCATED
096/8 – 100/8	ARIN	2006-10	whois.arin.net	ALLOCATED
101/8	APNIC	2010-08	whois.apnic.net	ALLOCATED
102/8	AFRINIC	2011-02	whois.afrinic.net	ALLOCATED
103/8	APNIC	2011-02	whois.apnic.net	ALLOCATED
104/8	ARIN	2011-02	whois.arin.net	ALLOCATED
105/8	AFRINIC	2010-11	whois.afrinic.net	ALLOCATED
106/8	APNIC	2011-01	whois.apnic.net	ALLOCATED
107/8	ARIN	2010-02	whois.arin.net	ALLOCATED
108/8	ARIN	2008-12	whois.arin.net	ALLOCATED
109/8	RIPE NCC	2009-01	whois.ripe.net	ALLOCATED
110/8 – 126/8	APNIC	2008-11	whois.apnic.net	ALLOCATED
127/8	IANA - Loopback	1981-09		RESERVED
128/8 – 132/8	Administered by ARIN	1993-05	whois.arin.net	LEGACY
133/8	Administered by APNIC	1997-03	whois.apnic.net	LEGACY
134/8 – 140/8	Administered by ARIN	1993-05	whois.arin.net	LEGACY
141/8	Administered by RIPE NCC	1993-05	whois.ripe.net	LEGACY
142/8 – 144/8	Administered by ARIN	1993-05	whois.arin.net	LEGACY
145/8	Administered by RIPE NCC	1993-05	whois.ripe.net	LEGACY
146/8 – 149/8	Administered by ARIN	1993-05	whois.arin.net	LEGACY
150/8	Administered by APNIC	1993-05	whois.apnic.net	LEGACY
151/8	Administered by RIPE NCC	1993-05	whois.ripe.net	LEGACY
152/8	Administered by ARIN	1993-05	whois.arin.net	LEGACY
153/8	Administered by APNIC	1993-05	whois.apnic.net	LEGACY
154/8	Administered by AFRINIC	1993-05	whois.afrinic.net	LEGACY
155/8 – 162/8	Administered by ARIN	1993-05	whois.arin.net	LEGACY
163/8	Administered by APNIC	1993-05	whois.apnic.net	LEGACY
164/8 – 170/8	Administered by ARIN	1993-05	whois.arin.net	LEGACY
171/8	Administered by APNIC	1993-05	whois.apnic.net	LEGACY
172/8 – 174/8	Administered by ARIN	1993-05	whois.arin.net	LEGACY
175/8	APNIC	2009-08	whois.apnic.net	ALLOCATED
176/8	RIPE NCC	2010-05	whois.ripe.net	ALLOCATED
177/8	LACNIC	2010-06	whois.lacnic.net	ALLOCATED
178/8	RIPE NCC	2009-01	whois.ripe.net	ALLOCATED
179/8	LACNIC	2011-02	whois.lacnic.net	ALLOCATED
180/8	APNIC	2009-04	whois.apnic.net	ALLOCATED
181/8	LACNIC	2010-06	whois.lacnic.net	ALLOCATED
182/8—183/8	APNIC	2009-08	whois.apnic.net	ALLOCATED
184/8	ARIN	2008-12	whois.arin.net	ALLOCATED
185/8	RIPE NCC	2011-02	whois.ripe.net	ALLOCATED
186/8—187/8	LACNIC	2007-09	whois.lacnic.net	ALLOCATED
188/8	Administered by RIPE NCC	1993-05	whois.ripe.net	LEGACY
189/8—190/8	LACNIC	1995-06	whois.lacnic.net	ALLOCATED
191/8	Administered by LACNIC	1993-05	whois.lacnic.net	LEGACY
192/8	Administered by ARIN	1993-05	whois.arin.net	LEGACY
193/8—195/8	RIPE NCC	1993-05	whois.ripe.net	ALLOCATED
196/8	Administered by AFRINIC	1993-05	whois.afrinic.net	LEGACY
197/8	AFRINIC	2008-10	whois.afrinic.net	ALLOCATED
198/8	Administered by ARIN	1993-05	whois.arin.net	LEGACY
199/8	ARIN	1993-05	whois.arin.net	ALLOCATED
200/8—201/8	LACNIC	2002-11	whois.lacnic.net	ALLOCATED
202/8—203/8	APNIC	1993-05	whois.apnic.net	ALLOCATED
204/8 – 209/8	ARIN	1994-03	whois.arin.net	ALLOCATED
210/8—211/8	APNIC	1996-06	whois.apnic.net	ALLOCATED
212/8—213/8	RIPE NCC	1997-10	whois.ripe.net	ALLOCATED
214/8—215/8	US-DOD	1998-03	whois.arin.net	LEGACY
216/8	ARIN	1998-04	whois.arin.net	ALLOCATED
217/8	RIPE NCC	2000-06	whois.ripe.net	ALLOCATED
218/8	APNIC	2000-12	whois.apnic.net	ALLOCATED
219/8	APNIC	2001-09	whois.apnic.net	ALLOCATED
220/8	APNIC	2001-12	whois.apnic.net	ALLOCATED
221/8	APNIC	2002-07	whois.apnic.net	ALLOCATED
222/8	APNIC	2003-02	whois.apnic.net	ALLOCATED
223/8	APNIC	2010-04	whois.apnic.net	ALLOCATED
224/8 – 239/8	Multicast	1981-09		RESERVED
240/8 – 255/8	Future use	1981-09		RESERVED

weit 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.

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. (Siehe Tabelle „Zusammenfassung“, rechts unten)

8.6 Besondere IP-Adressen

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 ein Filter dar, durch das Rechner entscheiden können, ob sie sich im selben (logischen) Netz befinden.

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.

Nur Rechner mit der gleichen Netzwerkadresse befinden sich im gleichen logischen Netzwerk!

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 für Netzwerkadresse

Hostadresse	192.168.100.1	11000000	10101000	01100100	00000001
UND					
Maske	255.255.255.0	11111111	11111111	11111111	00000000
Subnetz	192.168.100.0	11000000	10101000	01100100	00000000

Beispiel für Broadcastadresse

Subnetz	192.168.100.0	11000000	10101000	01100100	00000000
ODER					
Inv. Maske	0.0.0.255	00000000	00000000	00000000	11111111
Broadcast	192.168.100.255	11000000	10101000	01100100	11111111

Loopback-Adresse

Die Class-A-Netzwerkadresse 127 ist weltweit reserviert für das sogenannte *local loopback* 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 angeschlossenen Netzwerk.

8.7 Subnetting

Internet-Quellen

http://instrumentation.de/5106003d.htm
http://www.zyxel.de/support

Das obige Schema zeigt, dass nur eine begrenzte Anzahl an internationalen IP-Adressen verfügbar ist. Falls die Anzahl der Netzwerke nicht ausreicht, gibt es wie schon erwähnt, die Möglichkeit diese Anzahl durch geschickte Strukturierung von Subnetzen zu erweitern. In der Tabelle unten ist eine mögliche Unterteilung dargestellt.

Wie daraus die möglichen Netze und zugehörigen gültigen IP-Adressen entstehen, soll am Beispiel der Subnetzmasken 255.255.255.192 und 255.255.255.224 erläutert werden. Der Status erlaubt oder nicht ergibt sich daraus, dass die erste und letzte bei der Unterteilung entstehenden Adressen nicht verwendet werden dürfen. (Beispiel siehe Tabelle, nächste Seite, rechts oben)

Subnetting

Subnetzmaske	Anzahl Subnetze (*)	Anzahl Hosts (Rechner, Knoten)
255.255.255.0	1 (1)	254
255.255.255.128	0 (2)	126
255.255.255.192	2 (4)	62
255.255.255.224	6 (8)	30
255.255.255.240	14 (16)	14
255.255.255.248	30 (32)	6
255.255.255.252	62 (64)	2

(*) Die in Klammer stehenden Werte sind zwar rechnerisch möglich, enthalten aber u.U. verbotene Adressen, falls CIDR nicht unterstützt wird.

Zusammenfassung

CLASS	Netzwerk Anteil	Anzahl Netze	Hostanteil	Anzahl Hosts/Netz
A	1 Bit + 7 Bit	128	24 Bit	16.777.214
B	2 Bit + 14 Bit	16.864	16 Bit	65.534
C	3 Bit + 21 Bit	2.097.152	8 Bit	253

Spätestens bei der Einrichtung eines Netzwerkes mit Subnetzen dürfte klar werden, dass hier eine ganze Menge Fehlerquellen schlummern und dass gute Netzwerkadministratoren durchaus Ihre Daseinsberechtigung haben! Man sollte deshalb bei Problemen neuer Rechner/Geräte im Netzwerk die Adressen sehr genau überprüfen.

8.8 CIDR *(Classless Inter-Domain Routing)*, VLSM *(Variable Length Subnet Masks)* und Supernetting

Das CIDR beschreibt ein Verfahren zur effektiveren Nutzung der bestehenden 32 Bit umfassenden IP-Adresse. Bei diesem Verfahren werden IP-Adressen zusammengefasst, wobei ein Block von aufeinander folgenden IP- Adressen der Klasse C als ein Netzwerk behandelt werden.

Möglich wird dies durch "Kürzen" der NetID, die bei klassenorientierter Betrachtung 24 bit lang wäre. Man verwendet daher Netzwerke wie etwa 192.168.4.0/23 mit insgesamt 510 gültigen Host-Adressen.

Das CIDR-Verfahren reduziert die in Routern gespeicherten Routing-Tabellen durch einen Präfix in der IP- Adresse. Mit diesem Präfix kann ein großer Internet Service Provider bzw. ein Betreiber eines großen Teils des Internets gekennzeichnet werden. Dadurch können auch darunter liegende Netze zusammengefasst werden; so genanntes Supernetting. Die Methode wird in RFC 1518 beschrieben.

Um einen Mangel an Netzwerkkennungen zu verhindern, haben Internetinstitutionen ein Schema erarbeitet, das so genannte Supernetting. Im Gegensatz zum Subnetting werden beim Supernetting Bits der Netzwerkkennung verwendet und für effizienteres Routing als Hostkennung maskiert. Statt einer Organisation mit 2.000 Hosts eine Netzwerkkennung der Klasse B zuzuweisen, weist ARIN (*American Registry for Internet Numbers*) beispielsweise einen Bereich von acht Netzwerkkennungen der Klasse C zu. In jeder Netzwerkkennung der Klasse C sind 254 Hosts möglich. Dies ergibt insgesamt 2.032 Hostkennungen.

Beispiel siehe Tabelle rechts.

8.9 IP-Routing

IP unterscheidet nicht zwischen Routern und Endpunkten. Jeder Netzwerkschnittstelle ist eine Routing-Tabelle zugeordnet und kann daher sowohl als Router als auch als Endpunkt agieren.

Abbildung: Cisco 800 (ISDN-Router)

Oft wird zwischen Hardware-Routern (Geräten mit Basisbetriebssystem, deren Hauptaufgabe das IP-Routing darstellt) und Software-Routern (kompletten PCs mit einer Routing-Komponente, die ggf. nachinstalliert werden muss) unterschieden. In Wirklichkeit geht es aber um die entsprechende Software.

Netze und IP-Adressen mit Subnetz-Maske 255.255.255.192

Netzwerkadresse	IP-Adressen	Broadcast	Status
a.b.c.0	1 - 62	63	nicht erlaubt, wenn alte Geräte verwendet werden, die CIDR nicht unterstützen (*)
a.b.c.64	65 -126	127	erlaubt
a.b.c.128	129 -190	191	erlaubt
a.b.c.192	193 -254	255	nicht erlaubt, wenn alte Geräte verwendet werden, die CIDR nicht unterstützen (*)

(*) Anmerkung: Es ist nicht sofort einsichtig, warum das erste und das letzte Subnet „nicht erlaubt“ sind. Der Grund dafür liegt in der Tatsache, dass im vorliegenden Beispiel ein Class C-Netz unterteilt wurde. Class C-Netze haben ohne Subnetting eine Subnetz-Maske 255.255.255.0, wobei sich aus den vorher erwähnten Regeln ergibt, dass die IP-Adresse a.b.c.0 (also alle Bit der HostID auf 0 gesetzt) der Netzwerkadresse entspricht und diese (einzige) Adresse daher nicht verwendet werden darf. Bei der Unterteilung in Subnetze zeigt sich aber, dass beim gesamten Bereich von a.b.c.0 bis a.b.c.63 die SubnetID aus lauter Nullen besteht – daher der ganze Bereich ausfällt. Die Argumentation für das letzte Subnetz ist analog zu sehen. Moderne Netzwerkgeräte unterstützen CIDR und haben deshalb keine Einschränkungen bei der Verwendung dieser Adressbereiche.

Netze und IP-Adressen mit Subnetz-Maske 255.255.255.224

Netzwerkadresse	IP-Adressen	Broadcast	Status
a.b.c.0	1 -30	31	nicht erlaubt, wenn alte Geräte verwendet werden, die CIDR nicht unterstützen (*)
a.b.c.32	33 -62	63	Erlaubt
a.b.c.64	65 -94	95	Erlaubt
a.b.c.96	97 -126	127	Erlaubt
a.b.c.128	129 -158	159	Erlaubt
a.b.c.160	161 -190	191	Erlaubt
a.b.c.192	193 -222	223	Erlaubt
a.b.c.224	225 -254	255	nicht erlaubt, wenn alte Geräte verwendet werden, die CIDR nicht unterstützen (*)

Routingtabelle ohne Supernetting

220.78.168.0	255.255.255.0	220.78.168.1
220.78.169.0	255.255.255.0	220.78.168.1
220.78.170.0	255.255.255.0	220.78.168.1
220.78.171.0	255.255.255.0	220.78.168.1
220.78.172.0	255.255.255.0	220.78.168.1
220.78.173.0	255.255.255.0	220.78.168.1
220.78.174.0	255.255.255.0	220.78.168.1
220.78.175.0	255.255.255.0	220.78.168.1

Routingtabelle mit Supernetting

220.78.168.0	255.255.248.0	220.78.168.1

Anzeige der Routing-Tabelle unter Windows und Linux siehe Kasten rechts.

Begriffserklärungen

- Netzwerkziel, Netzwerkmaske: Unter „Netzwerkziel“ ist gemeint: wenn ein Paket an diese Adresse (meist ein ganzes Netzwerk) gerichtet ist, was soll mit diesem Paket geschehen?
- Gateway: Pakete, die an das in derselben Zeile angegebene Netzwerkziel gerichtet sind, werden an diesen Router (Gateway) weitergeleitet
- Schnittstelle: Über welche Netzwerkschnittstelle sollen Pakete an den Gateway weitergeleitet werden?
- Anzahl (auch: Metrik, Kosten): Prioritätsangabe der Route; je kleiner der Zahlenwert, umso "wichtiger" ist die Route.

```
E:\>route print
===========================================================================
Schnittstellenliste
0x1 ........................... MS TCP Loopback interface
0x1000003 ...00 02 b3 4c 37 d1 ...... Intel(R) PRO PCI Adapter
===========================================================================
===========================================================================
Aktive Routen:
     Netzwerkziel    Netzwerkmaske          Gateway   Schnittstelle  Anzahl
          0.0.0.0          0.0.0.0     172.16.201.2  172.16.201.229       1
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      172.16.50.0    255.255.255.0     172.16.50.229  172.16.201.229       1
    172.16.50.229  255.255.255.255        127.0.0.1       127.0.0.1       1
     172.16.201.0    255.255.255.0   172.16.201.229  172.16.201.229       1
   172.16.201.229  255.255.255.255        127.0.0.1       127.0.0.1       1
   172.16.255.255  255.255.255.255   172.16.201.229  172.16.201.229       1
        224.0.0.0        224.0.0.0   172.16.201.229  172.16.201.229       1
  255.255.255.255  255.255.255.255   172.16.201.229  172.16.201.229       1
Standardgateway:      172.16.201.2
===========================================================================
Ständige Routen:
  Keine
```

Unter Linux kann die Routing-Tabelle wie folgt angezeigt werden:

```
$ /sbin/route        oder
$ /sbin/route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
localnet        *               255.255.255.0   U     0      0        0 ra0
172.16.114.0    *               255.255.255.0   U     0      0        0 eth0
172.16.236.0    *               255.255.255.0   U     0      0        0 eth1
default         192.168.1.254   0.0.0.0         UG    0      0        0 ra0
```

Zeile 1

Netzwerkziel 0.0.0.0
Netzwerkmaske 0.0.0.0
Gateway 172.16.201.2
Schnittstelle 172.16.201.229
Anzahl 1

Was soll mit Paketen geschehen, die an das Netzwerk 0.0.0.0/0 gesendet werden? Diese Route bezeichnet man als Standardroute.

Wir sehen, dass Pakete an den eingetragenen Standardgateway weitergeleitet werden.

Anmerkung: Auf einer typischen Arbeitsstation wird ein Großteil der Pakete zum Standardgateway weitergeleitet werden!

Zeile 2

Netzwerkziel 127.0.0.0
Netzwerkmaske 255.0.0.0
Gateway 127.0.0.0
Schnittstelle 127.0.0.1
Anzahl 1

Hier sehen wir, dass sämtliche Pakete, die an eine Adresse im Netzwerk 127.0.0.0 gerichtet sind, über die Schnittstelle 127.0.0.1 (also den Loopback-Adapter) an den Gateway 127.0.0.1 zurückgeschickt werden. Die Pakete erreichen also weder die Schicht 2 noch verlassen sie den PC.

Zeile 3

Netzwerkziel 172.16.50.0
Netzwerkmaske 255.255.255.0
Gateway 172.16.50.229
Schnittstelle 172.16.201.229
Anzahl 1

Hier sehen wir: Alle Pakete, die ans Netzwerk 172.16.50.0 gerichtet sind, werden über die Schnittstelle 172.16.201.229 an den Gateway 172.16.50.229 geschickt. Dieser Eintrag verbindet also die beiden Netze 172.16.201.x und 172.16.50.x.

Zeile 4 und Zeile 6

Netzwerkziel 172.16.50.229
Netzwerkmaske 255.255.255.255
Gateway 127.0.0.1
Schnittstelle 127.0.0.1
Anzahl 1

Netzwerkziel 172.16.201.229
Netzwerkmaske 255.255.255.255
Gateway 127.0.0.1
Schnittstelle 127.0.0.1
Anzahl 1

Hier wird der PC veranlasst, an sich selbst gerichtete Pakete (als Ziel ist das „Netzwerk“ 172.16.50.229/32, wobei eine Netzwerkmaske von 255.255.255.255 bedeutet, dass nur eine einzige Adresse gemeint ist) an den Loopback-Adapter weiterzusenden.

Zeile 5

Netzwerkziel 172.16.201.0
Netzwerkmaske 255.255.255.0
Gateway 172.16.201.229
Schnittstelle 172.16.201.229
Anzahl 1

Pakete, die an eine Adresse im Netzwerk 172.16.201.x gerichet sind, werden über die Schnittstelle 172.16.201.229 an den Gateway 172.16.201.229 weitergeleitet. Dieser Eintrag entspricht der Umkehrung von Zeile 3.

Zeile 7

Netzwerkziel 172.16.255.255
Netzwerkmaske 224.0.0.0
Gateway 172.16.201.229
Schnittstelle 172.16.201.229
Anzahl 1

Diese Zeile betrifft Broadcasts, die über die 172.16.201.229-Schnittstelle an das lokale Netzwerk weitergeleitet werden.

Zeile 8

Netzwerkziel 224.0.0.0
Netzwerkmaske 224.0.0.0
Gateway 172.16.201.229
Schnittstelle 172.16.201.229
Anzahl 1

Hier wird das Routingverhalten für Multicast-Adressen geregelt.

Zeile 9

Netzwerkziel 255.255.255.255
Netzwerkmaske 255.255.255.255
Gateway 172.16.201.229
Schnittstelle 172.16.201.229
Anzahl 1

Hier finden wir die generische Broadcast-Adresse 255.255.255.255; auch hier werden Broadcasts an PCs im lokalen Netz weitergetragen.

8.10 Der Befehl ROUTE

Manipuliert die Netzwerkroutingtabellen. Anwednung siehe Kasten nächste Seite.

8.11 Aufbau des IP-Headers

Im Internet gibt es die Seite www.protocols.com auf der detailliert eine ganze Reihe von Netzwerkprotokollen beschrieben sind – darunter auch das TCP/IP-Protokoll.

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

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.

IPv4-Header

Die ersten vier Bits stellen das Feld Ver dar (siehe Abbildung nächste Seite unten). 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 Übertra-

gung 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^{16} -1 = 65535 Byte beschränkt. Ein größeres Datagramm kann durch IP nicht vermittelt werden.

Im Zuge der QoS (*Quality of Service*)-Diskussion (Ziel: Qualitätsverbesserung der Internet-Protokolle und Internet-Dienste) am Internet wurde eine Lösung ersonnen, die als „diffserv“ (*differentiated services*) bezeichnet wird. Diffserv (DS) baut am TOS-Feld auf und überträgt in diesem Byte Informationen, die das Routing effizienter machen.

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 repräsentieren 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.

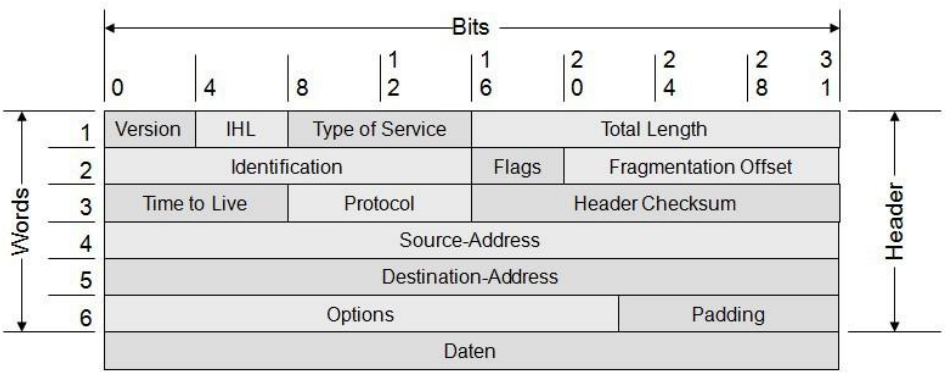
Das Feld Header Checksum beinhaltet eine Prüfsumme. Sie dient zum Erkennen von Verfälschungen bei der Übertragung des Datagramms. Allerdings wird sie nur über die Daten des IP-Headers selbst gebildet. Die zu transportierenden Daten werden nicht berücksichtigt. Soll über diesen Daten auch eine Prüfsumme 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 Data-

```
ROUTE [-f] [-p] [Befehl [Ziel]
                [MASK Netzmaske]  [Gateway] [METRIC Anzahl]
                [IF Schnittstelle]
  -f            Löscht alle Gatewayeinträge in Routingtabellen.
                Wird der Parameter mit einem der Befehle verwendet, werden
                die Tabellen vor der Befehlsausführung gelöscht.
  -p            (persistent) Wird der Parameter mit dem "ADD"-Befehl
                verwendet, wird eine Route unabhängig von Neustarts des
                Systems verwendet.
                Standardmäßig ist diese Funktion deaktiviert, wenn das
                System neu gestartet wird. Dies wird ignoriert für alle
                anderen Befehle, die beständige Routen beeinflussen.
                Diese Funktion wird von Windows 95 nicht unterstützt.
  Befehl        Auswahlmöglichkeiten:
                  PRINT     Druckt eine Route
                  ADD       Fügt eine Route hinzu
                  DELETE    Löscht eine Route
                  CHANGE    Ändert eine bestehende Route
  Ziel          Gibt den Host an.
  MASK          Gibt an, dass der folgende Parameter ein Netzwerkwert ist.
  Netzmaske     Gibt einen Wert für eine Subnetzmaske für den Routeneintrag
                an. Ohne Angabe wird die Standardeinstellung
                255.255.255.255 verwendet.
  Gateway       Gibt ein Gateway an.
  Schnittstelle Schnittstellennummer der angegebenen Route.
  METRIC        Gibt den Anzahl/Kosten-Wert für das Ziel an.

Alle symbolischen Namen, die für das Ziel verwendet werden, werden in
der Datei der Netzwerkdatenbank NETWORKS angezeigt. Symbolische Namen
für Gateway finden Sie in der Datei der Hostnamendatenbank HOSTS.
Bei den Befehlen PRINT und DELETE können Platzhalter für Ziel und
Gateway verwendet werden, (Platzhalter werden durch "*" angegeben),
oder Sie können auf die Angabe des Gatewayparameters verzichten.

Falls Ziel "*" or "?" enthält, wird es als Shellmuster bearbeitet und es
werden nur übereinstimmende Zielrouten gedruckt. Der Platzhalter "*" wird
mit jeder Zeichenkette überprüft, und "?" wird mit jedem Zeichen überprüft.
Beispiele: 157.*.1, 157.*, 127.*, *224*.
Diagnoseanmerkung:
   Eine ungültige MASK erzeugt einen Fehler unter folgender Bedingung :
   (DEST & MASK) != DEST.
   Beispiel> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1
             Die Route konnte nicht hinzugefügt werden: Der angegebene
             Maskenparameter ist ungültig.
(Destination & Mask) != Destination.

Beispiele:
    > route PRINT
    > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
                    Ziel^      ^Maske     ^Gateway     Metric^    ^
                                                     Schnittstelle^
      Sollte "IF" nicht angegeben sein, wird versucht die beste
      Schnittstelle für das angegebene Gateway zu finden.
    > route PRINT
    > route PRINT 157*            .... Zeigt passende Adressen mit 157* an.
    > route DELETE 157.0.0.0
    > route PRINT
```



gramms 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.

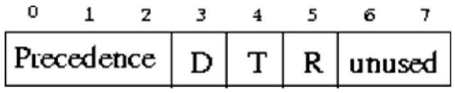


Abbildung: Das Feld TOS des IP-Headers

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.

8.12 IP-Rechner

Auf den folgenden Seiten finden Sie IP-Adressrechner zum Download, aber auch Rechner, die Sie online einsetzen können:

- http://www.chinet.com/html/ip.html
- http://www.tmp-houston.com/subcalc.htm
- http://jodies.de/ipcalc
- http://www.telusplanet.net/public/sparkman/netcalc.htm
- http://www.wildpackets.com/products/ipsubnetcalculator
- http://www.novell.com/coolsolutions/tools/1466.html

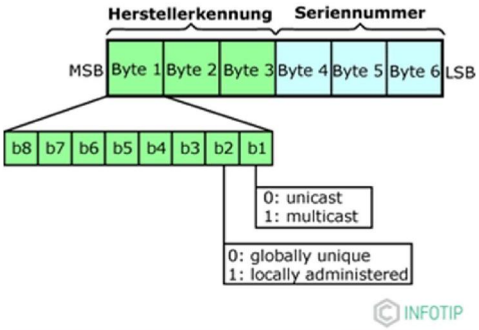
8.13 ARP (Address Resolution Protocol)

Das *Address Resolution Protocol* (ARP) arbeitet auf der Schicht 2, der Sicherungsschicht, des OSI- Schichtenmodells und setzt IP-Adressen in Hardware-und MAC-Adressen um. Alle Netzwerktypen und - topologien benutzen Hardware-Adressen um die Datenpakete zu adressieren. Damit nun ein IP-Paket an sein Ziel findet, muss die Hardware-Adresse des Ziels bekannt sein.

Jede Netzwerkkarte besitzt eine einzigartige und eindeutige Hardware-Adresse, die fest auf der Karte eingebrannt ist und meist nicht änderbar ist, die Media Access Control-Adresse oder kurz MAC-Adresse. In Ethernet-Netzwerken ist diese Adresse meist eine 48 bit-Binärzahl, die als 6 hexadezimal angegebenen Bytes angeschrieben wird.

Bevor nun ein Datenpaket verschickt werden kann, muss durch ARP eine Adressauflösung erfolgen. Dazu benötigt ARP Zugriff auf IP-Adresse und Hardware-Adresse. Um an die Hardware-Adresse einer anderen Station zu kommen verschickt ARP z. B. einen Ethernet-Frame als Broadcast-Meldung mit der MAC-Adresse "FF FF FF

FF FF FF". Diese Meldung wird von jedem Netzwerkinterface entgegengenommen und ausgewertet. Der Ethernet-Frame enthält die IP-Adresse der gesuchten Station. Fühlt sich eine Station mit dieser IP-Adresse angesprochen, schickt sie eine ARP-Antwort an den Sender zurück. Die gemeldete MAC-Adresse wird dann im lokalen ARP-Cache des Senders gespeichert. Dieser Cache dient zur schnelleren ARP-Adressauflösung.



OUI	Hersteller
00-03-93-xx-xx-xx	Apple Computer
00-60-2F-xx-xx-xx	Cisco
00-0B-3B-xx-xx-xx	devolo
00-0F-66-xx-xx-xx	Linksys
00-09-82 -xx-xx-xx	Loewe Opta GmbH
00-1C-EE-xx-xx-xx	Sharp

Ablauf einer ARP-Adressauflösung

Eine ARP-Auflösung unterscheidet zwischen lokalen IP-Adressen und IP-Adressen in einem anderen Subnetz.

Als erstes wird anhand der Subnetzmaske festgestellt, ob sich die IP-Adresse im gleichen Subnetz befindet. Ist das der Fall, wird im ARP-Cache geprüft, ob bereits eine MAC-Adresse für die IP-Adresse hinterlegt ist. Wenn ja, dann wird die MAC-Adresse zur Adressierung verwendet. Wenn nicht, setzt ARP eine Anfrage mit der IP- Adresse nach der Hardware-Adresse in das Netzwerk. Diese Anfrage wird von allen Stationen im selben

Subnetz entgegengenommen und ausgewertet. Die Stationen vergleichen die gesendete IP-Adresse mit ihrer eigenen. Wenn sie nicht übereinstimmt, wird die Anfrage verworfen. Wenn die IP-Adresse übereinstimmt schickt die betreffende Station eine ARP-Antwort direkt an den Sender der ARP-Anfrage. Dieser Speichert die Hardware-Adresse in seinem Cache. Da bei beiden Stationen die Hardware-Adresse bekannt sind, können sie nun miteinander Daten austauschen.

Befindet sich eine IP-Adresse nicht im gleichen Subnetz, geht ARP über das Standard-Gateway. Findet ARP die Hardware-Adresse des Standard-Gateways im Cache nicht, wird eine lokale ARP-Adressauflösung ausgelöst. Ist die Hardware-Adresse des Standard-Gateways bekannt, schickt der Sender bereits sein erstes Datenpaket an die Ziel-Station. Der Router (Standard-Gateway) nimmt das Datenpaket in Empfang und untersucht den IP-Header. Der Router überprüft, ob sich die Ziel-IP-Adresse in einem angeschlossenen Subnetz befindet. Wenn ja, ermittelt er anhand der lokalen ARP-Adressauflösung die MAC-Adresse der Ziel-Station. Anschließend leitet er das Datenpaket weiter. Ist das Ziel in einem entfernten Subnetz, überprüft der Router seine Routing-Tabelle, ob ein Weg zum Ziel bekannt ist. Ist das nicht der Fall steht dem Router auch ein Standard-Gateway zu Verfügung. Der Router führt für sein Standard-Gateway eine ARP-Adressauflösung durch und leitet das Datenpaket an dieses weiter.

Die vorangegangenen Schritte weiderholen sich dann so oft, bis das Datenpaket sein Zeil erreicht oder das IP- Header-Feld TTL auf den Wert 0 springt. Dann wird das Datenpaket vom Netz genommen.

Erreicht dann irgendwann das Datenpaket doch sein Ziel, schreibt die betreffende Station seine Rückantwort in ein ICMP-Paket an den Sender. In dieser Antwort wird falls möglich ein Gateway vermerkt, über das die beiden Stationen miteinander kommunizieren. So werden weitere ARP-Adressauflösungen und dadurch Broadcasts vermieden.

ARP-Cache

Durch den ARP-Cache wird vermieden, dass bei jedem Datenpaket an das selbe Ziel wieder und immer wieder ein ARP-Broadcast ausgelöst wird. Häufig benutzte Hardware-Adressen sind im ARP-Cache gespeichert. Die Einträge im ARP-Cache können statisch oder dynamisch sein. Statische Einträge können manuell hinzugefügt und gelöscht werden. Dynamische Einträge werden durch die ARP-Adressauflösung erzeugt.

Anzeigen des ARP-Caches unter Windows

```
C:\>arp -a
Schnittstelle: 192.168.168.11 ---0x2
Schnittstelle: 192.168.168.11 ---0x2
  Internetadresse   Physikal. Adresse Typ
  192.168.168.8     00-30-ab-0e-d3-6a dynamisch
```

Jeder dynamische Eintrag bekommt einen Zeitstempel. Ist er nach zwei Minuten nicht mehr abgerufen worden, wird der Eintrag gelöscht. Wird eine Adresse auch nach zwei Minuten noch benutzt, wird der Eintrag erst nach zehn Minuten gelöscht. Ist der ARP-Cache für neue Einträge zu klein, werden alte Einträge entfernt.

Wird die Hardware neu gestartet oder ausgeschaltet, wird der ARP-Cache gelöscht. Es gehen dabei auch die statischen Einträge verloren.

Fehler und Probleme mit ARP: Grundsätzlich gibt es keine Probleme oder Fehler mit ARP, solange keine statischen Einträge im ARP-Cache vorgenommen werden oder Hardware-Adressen von Netzwerkkarten verändert werden.

ARP läuft für den Benutzer ganz im Verborgenen.

Den umgekehrten Weg, MAC-Adresse bekannt, IP-Adresse gesucht, definiert RARP (*Reverse Adress Resolution Protocol*).

8.14 Internetanbindung von Firmennetzwerken

Grundsätzlich stehen zwei Möglichkeiten zur Verfügung:

- Verbindung über Router, wobei die im Firmennetzwerk verwendeten privaten IP-Adressen mit NAT (*Network Address Translation*) maskiert werden. Eine spezielle Technologie stellt Microsofts Internet Connection Sharing dar.
- Verbindung über Proxy-Server, wobei nur dieser einer Verbindung zum Internet herstellt und für die Clients als „Vertreter“ handelt. Ein Proxy-Server ist auch in der Lage, einmal heruntergeladene Inhalte zwischenzuspeichern.

8.14.1 Network Address Translation

Network Address Translation (NAT) ist in Rechnernetzen der Sammelbegriff für Verfahren, um automatisiert und transparent Adressinformationen in Datenpaketen durch andere zu ersetzen. Diese kommen typischerweise auf Routern und Firewalls zum Einsatz.

Network Address Port Translation (NAPT) stellt mittlerweile die häufigste Form des NAT dar und wird daher oft als Synonym gebraucht. Da es neben der Umsetzung von IP-Adressen auch eine Umsetzung von Port- Nummern gestattet, wird es oft eingesetzt, um durch sogenanntes „maskieren“ (*masquerading*) eine Reihe von (privaten) IP-Adressen und zugeordneten Port-Nummern zur Nutzung nur einer (öffentlichen) IP-Adresse zu verwenden.

Große Verbreitung fand NA(P)T durch die Knappheit öffentlicher IPv4-Adressen und die Tendenz, private Subnetze über Einwahlverbindungen mit dem Internet zu verbinden. Die einfachste Lösung des Problems beschränkter IP-Adressen war oft die durch NAT mögliche Verwendung mehrerer privater IP-Adressen mit nur einer öffentlichen IP-Adresse.

Üblicherweise wird NAT an einem Übergang zwischen zwei Netzen durchgeführt. Der NAT-Dienst kann auf einem Router, einer Firewall oder einem anderen spezialisierten Gerät laufen. So kann zum Beispiel ein NAT- Gerät mit zwei Netzwerkadaptern das lokale private Netz mit dem Internet verbinden.

Man unterscheidet zwischen Source NAT, bei dem die Quell-IP-Adresse ersetzt wird, und Destination NAT, bei dem die Ziel-IP-Adresse ersetzt wird. (Siehe Tabelle unten).

NAT-Konfiguration auf einem Internet-Gateway/Firewall/Router-Kombigerät

Um interne Geräte vom Internet aus erreichen zu können, ist die Konfiguration von NT-Einträgen notwendig. Dabei werden Anfragen, die sich auf die externe IP-Adresse des Routers beziehen, durch Ersetzen der IP- Adresse an ein internes Gerät weitergeleitet.

-> Tabelle auf der folgenden Seite oben

Beispiel 1: Betreiben eines eigenen Webservers (Zeile 1)

Wenn Sie einen eigenen Webserver betreiben möchten, so sollte dieser übers Internet erreichbar sein. Tragen Sie als Zieladresse (Dest.addr) die public IP ein, die auf der WAN-Schnittstelle Ihres Routers konfiguriert ist. Der Standard-TCP-Zielport für Webserver-Verbindungen über http ist 80. Nun tragen Sie in der Spalte NAT IP die interne Adresse des Zielgeräts ein, auf dem der Webserver läuft; als NAT-Port können Sie den Port 80 belassen.

Beispiel 2: Remotedesktop eines internen Geräts übers Internet ansprechen (Zeile 4).

Hier tragen Sie als Zieladresse (Dest.addr) die public IP ein, die auf der WAN-Schnittstelle Ihres Routers konfiguriert ist. Der Standard-TCP-Zielport für Remotedesktop-Verbindungen ist 3389. Nun tragen Sie in der Spalte NAT IP die interne Adresse des Zielgeräts ein, als NAT-Port können Sie den Port 3389 belassen.

8.14.2 Proxy-Server

Ein Proxy-Server ist eine Software, die auf dem PC installiert ist, der den Internet-Zugang besitzt. Es kann sich hier um einen Wählzugang (Modem, ISDN-Karte) oder um einen Standleitungszugang (ADSL, Kabelmodem, Powerline) handeln.

Diese Software erfüllt verschiedene Aufgaben:

- Sie sammelt die Anfragen von allen PCs im Netz, die auf den Proxy-Server zugreifen, und führt diese Anfragen durch. So wird bei Bedarf die Einwahl durchgeführt und nötige Webdateien heruntergeladen.
- Die heruntergeladenen Dateien werden zwischengespeichert; Vorteil: bei wiederholten Anfragen brauchen die Dateien nicht mehr vom Internet geholt werden, sondern befinden sich bereits lokal auf der Festplatte des Proxy-Servers und werden nur mehr von dort an den Client

Source NAT

```
        lokales Netz (LAN)                          öffentliches Netz (WAN)
     Quell-IP        Ziel-IP                        Quell-IP       Ziel-IP
192.168.0.2:49708 170.0.0.1:80         Router   205.0.0.2:61300 170.0.0.1:80
192.168.0.2:49709 195.58.175.11:80  ========>  205.0.0.2:61301 195.58.175.11:80
192.168.0.3:49708 170.0.0.1:80          NAT     205.0.0.2:61302 170.0.0.1:80

Bei ausgehenden Paketen wird die (private) Quell-IP-Adresse durch eine noch nicht benutzte
(öffentliche) IP-Adresse ersetzt. Dabei merkt sich das NAT-Gerät diese Umsetzung in einer NAT-
Zuordnungstabelle:
*                   192.168.0.2:49708 <-> 205.0.0.2:61300
*                   192.168.0.2:49709 <-> 205.0.0.2:61301
*                   192.168.0.4:49708 <-> 205.0.0.2:61302
```

Destination NAT

```
        lokales Netz (LAN)                          öffentliches Netz (WAN)
     Quell-IP        Ziel-IP                        Quell-IP       Ziel-IP
170.0.0.1:80 192.168.0.2:49708                  170.0.0.1:80     205.0.0.2:61300
170.0.0.1:80 192.168.0.3:49709                  195.58.175.11:80 205.0.0.2:61301
170.0.0.1:80 192.168.0.4:49708                  170.0.0.1:80     205.0.0.2:61302
```

versandt.

- Leistungsfähige Proxy-Server enthalten auch einen Firewall, der vor Angriffen durch Hacker schützt.

Marktüberblick

Beispiele für Proxy Server, oft kombiniert mit NAT-und Firewall-Technologie::

- WinProxy (www.ositis.com)
- WinGate (www.wingate.at)
- JanaServer (www.janaserver.de)
- Microsoft ISA Server (*Internet Security and Access Server*)
- Squid (Linux-Produkt, kostenloser Download unter www.squid-cache.org)

Funktionsweise eines Proxy-Servers

Beim WWW-Caching werden Dokumente, die von einem Browser angefordert werden, nicht direkt beim ursprünglichen Server geholt, sondern über einen so genannten Proxy-Server, der möglichst in der Nähe des Browsers installiert ist. Der Proxy-Server ist im Prinzip ein riesiges Reservoir an (kürzlich) angeforderten Dokumenten, welche vom Server in Bezug auf ihre Aktualität verwaltet werden und allen Browsern zur Verfügung stehen, welche den Proxy-Server benutzen. Falls der Proxy-Server ein Dokument noch nicht kennt, oder die bekannte Version in Bezug auf bestimmte Kriterien veraltet ist, so fordert er die aktuelle Version selbständig beim ursprünglichen Server an und schickt sie an den anfragenden Browser weiter. Damit kann der Netzwerkverkehr wesentlich reduziert werden, insbesondere dann, wenn viele Browser den gleichen Proxy-Server benutzen und/oder wenn dieselben Dokumente immer wieder von weit her geholt werden müssen (z.B. aus den USA). Der Betrieb eines Proxy-Servers ist somit nicht nur aus Kostengründen sehr vorteilhaft, er führt bei „bekannten" Dokumenten auch zu wesentlich kürzeren Antwortzeiten.

Ein Proxy-Server (engl. Proxy: Stellvertreter, Bevollmächtigter), auch Application Level Gateway genannt, erlaubt dem Netzwerk-Administrator die Installation von strengeren Sicherheitsregeln als dies bei einem Paketfilterungs-Router möglich ist. Der Server dient als sicheres Gateway zwischen einem privaten und einem öffentlichen (ungesicherten) Netz. Als Gateway bezeichnet man entweder die Software, die eine Verbindung zwischen zwei Netzwerken herstellt, oder den Computer, auf dem diese Software ausgeführt wird.

Ein Proxy-Server dient nebenbei zur Zwischenspeicherung von Web-Inhalten und kann als erweiterbare Firewall verwendet werden. Das ermöglicht gleichzeitig Datensicherheit und einen schnelleren Zugriff auf Internetinhalte. Der Proxy hat dabei zwei Gesichter: Für den lokalen Client operiert er beim Abruf eines Web-Dokuments wie ein Webserver. Gegenüber dem entfernten Internet-Server tritt er wie ein Webclient auf.

	If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.3.17	80 (HTTP)	HTTP auf SRV04 www.zahler.at
	WAN	TCP	*	*	88.117.246.213	80 (HTTP)	192.168.3.31	80 (HTTP)	HTTP auf EIB-KNX
	WAN	TCP	*	*	88.117.246.211	3390	192.168.3.12	3389 (MS RDP)	RDP auf SRV01
	WAN	TCP	*	*	88.117.246.211	3389 (MS RDP)	192.168.3.118	3389 (MS RDP)	RDP auf PC04
	WAN	TCP	*	*	88.117.246.211	25 (SMTP)	192.168.3.19	25 (SMTP)	SMTP von WAN zu SRV05
	WAN	TCP	*	*	WAN address	443 (HTTPS)	192.168.3.19	443 (HTTPS)	Https von WAN zu SRV05

Proxy-Server sprechen aber nicht nur HTTP, sondern beherrschen auch Dienste wie FTP, POP3 oder IRC - allerdings abhängig vom jeweiligen Produkt. Da sie als einziger Knotenpunkt zwischen lokalem und globalem Netz geschaltet sind, schützen sie zudem die lokalen Clients. Denn nur der Proxy-Server ist Angriffen von außen ausgesetzt. Die Clients liegen "unsichtbar" hinter ihm.

Das Betriebssystem auf Client-Seite spielt prinzipiell keine Rolle. Nur spezielle Funktionen wie beispielsweise eine automatische Konfiguration der Clients oder das Trennen einer Internet-Verbindung vom Client funktionieren lediglich von Windows-Clients aus.

Daneben lässt sich für jeden Dienst wie FTP oder HTTP ein separater Proxy einrichten. Unerwünschte Dienste filtert der Proxy heraus. Zudem findet kein direkter Paketfluss zwischen internen und externen Rechnern statt.

Methode

Ein Proxy-Server hat im Wesentlichen die folgenden Eigenschaften:

- Gegenüber einem Browser (Client) sieht er aus wie ein WWW-Server.
- Gegenüber einem WWW-Server sieht er aus wie ein Client.
- Er besitzt einen riesigen Speicher (*cache*), in dem er Dokumente speichert, die von den mit ihm verbundenen Browsern angefordert worden sind.
- Fordert ein Browser ein Dokument an, so prüft der Proxy-Server zuerst, ob er dieses Dokument bereits im Speicher hat. Falls ja, so prüft er nach, ob das Dokument in Bezug auf bestimmte Kriterien noch aktuell ist. Ist es das, so schickt er es dem Browser direkt zurück, andernfalls schickt er dem ursprünglichen Server eine Anfrage, ob das Dokument in der Zwischenzeit modifiziert worden ist. Falls ja, so fordert er das neue Dokument an und schickt es an den Browser weiter, andernfalls schickt er dem Browser das bereits gespeicherte Dokument.
- Falls der Proxy-Server ein angefordertes Dokument noch nicht kennt, so gibt es mehrere Möglichkeiten:
  1. Er fordert es direkt beim ursprünglichen Server an.
  2. Er fordert es bei einem sog. *parent-proxy* an, einem Proxy-Server des Proxy-Servers.
  3. Er schickt eine Anfrage an einen sog. *sibling-proxy* (ein 'Geschwister'-proxy mit demselben *parent*), ob dieser eine aktuelle Version des Dokumentes hat. Falls ja, so holt er es dort, falls nein, so holt er es direkt beim ursprünglichen Server.
- Ein „reload" des Browsers bewirkt immer, dass eine Rückfrage beim ursprünglichen Server (bzw. bei einem *parent-proxy*) erfolgt. Damit ist gewährleistet, dass der Proxy-Server immer die aktuelle Version des Dokuments an den Browser zurückschickt.