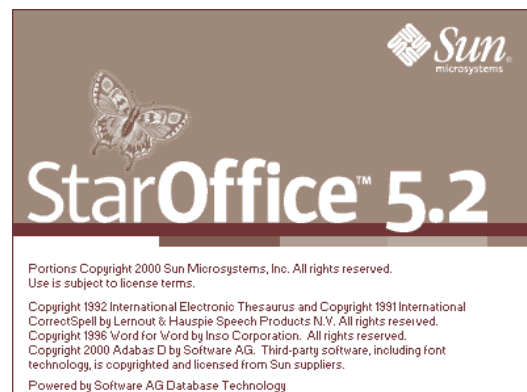
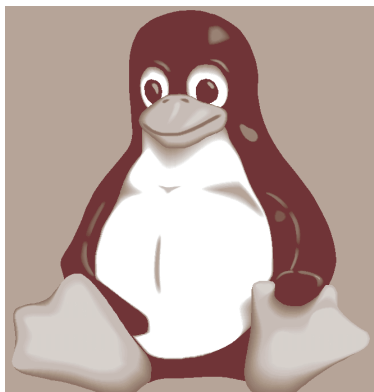


Inhalt

1. Adressierungsverfahren
2. Adreßaufbau und Adreßklassen
3. Adreßregistrierung
4. besondere Adressen und Adreßbereiche
5. Subnetting
6. Verwendung nicht registrierter Adressen
7. Domain Name Service (DNS)

Die Kopiervorlage für dieses Dokument wurde unter Linux mit StarWriter erstellt und gedruckt.



Es existieren die verschiedensten Netzwerktopologien mit entsprechenden Netzwerkprotokollen, die ihre eigene Philosophie entwickelt haben, um die Kommunikation zwischen Netzteilnehmern zu gewährleisten.

Alle diese Philosophien müssen aber eine Bedingung erfüllen: Die Adressierung muss **eindeutig** sein. Jede Netzwerkressource, sei es PC, Workstation oder auch ein Netzwerkdrucker mit eigener Netzwerkkarte muss durch eine eindeutige Adresse identifizierbar sein. Ist das nicht der Fall, kann keine fehlerfreie Kommunikation stattfinden. Vergleichbar ist das mit der Vergabe von Telefonnummern. Für jeden Endteilnehmer kann nur eine Telefonnummer vergeben werden. Welcher Gesprächspartner sollte sich wohl auch melden, wenn eine Telefonnummer doppelt vergeben würde? Das perfekte Chaos. Für Gesprächsteilnehmer mit gleicher Telefonnummer in Orten mit unterschiedlicher Vorwahl (Ortskennzahl) tritt dieses Problem natürlich nicht auf. Bei identischen Telefonnummern ist die Eindeutigkeit durch die unterschiedlichen Ortskennzahlen garantiert. Dieses Prinzip gilt auch für jeden erdenklichen Netzwerktyp, einschließlich der IP-Netze.

1. Adressierungsverfahren

Grundsätzlich unterscheidet man zunächst nach physikalischer und logischer Adressierung. Unter physikalischer Adresse versteht man die sogenannte Hardwareadresse, die jeder Netzwerkressource weltweit eindeutig und unverwechselbar zugeordnet ist. Bei den heute handelsüblichen Ethernet-Karten ist die physikalische Adresse auf der Karte „eingebrennt“ (burnt-in-Address), d.h. sie ist unveränderbar in einem ROM-Baustein abgelegt. Die Eindeutigkeit der physikalischen Adresse wird also bereits durch den Hersteller des Netzwerkinterface realisiert. Die logische Adressierung ist in erster Linie vom Netzwerkprotokoll abhängig. Sie hat zunächst einmal nichts mit der physikalischen Adresse zu tun. Allerdings muss man bei der logischen Adresse nun selbst für die notwendige Eindeutigkeit der Adressierung sorgen. Die logische Adresse wird der physikalischen Adresse „übergestülpt“. Jene logische Adresse ist in TCP/IP-Netzen die IP-Adresse. Die heute noch gültige IP-Version 4 definiert IP-Adressen als eine 32-Bit Zahl, die der besseren Lesbarkeit wegen in vier Oktette (8 Bit) aufgeteilt wird.

Die Oktette werden durch Dezimalpunkte getrennt (**dotted notation**) und in dezimaler Schreibweise angegeben z.B. 192.168.76.254 (Abb. 1).

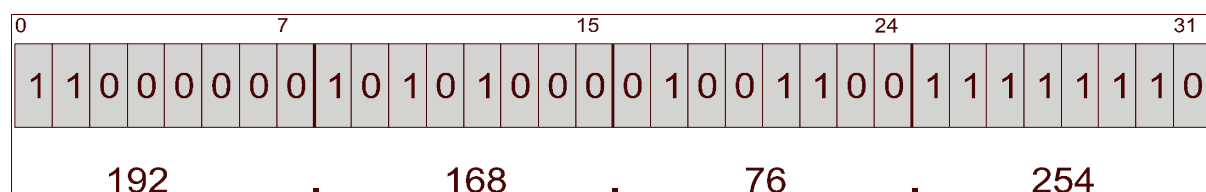


Abbildung 1: IP-Adresse in dualer und (dotted) dezimaler Schreibweise

2. Adreßaufbau und Adreßklassen

Wie schon erwähnt, besteht eine IP-Adresse der Version 4 aus einer 32-Bit Zahl, die in Gruppen zu je 8 Bit aufgeteilt ist. Die IP-Adresse definiert zum einen die Netzwerkressource selbst (Host) und zum anderen das Netzwerk, in dem sich die Netzwerkressource befindet.

Dazu besteht die IP-Adresse aus zwei Teilen.

1. Netzadresse (*Net-ID*)
2. Hostadresse (*Host-ID*)

Auf das Beispiel mit dem Telefonnetz angewendet, bedeutet das, dass die Netz-ID der Ortskennzahl und die Host-ID dem einzelnen Telefonanschluß innerhalb des Ortsbereiches entspricht.

Wie groß die Anteile von Host-ID und Net-ID innerhalb der IP-Adresse sind, ist zunächst prinzipiell variabel. Bei dem Beispiel mit dem Telefonnetz ist das ja ebenso. Die Länge von Ortskennzahl bzw. Telefonnummer kann von Netz zu Netz unterschiedlich sein.

Die für TCP/IP und Internet zuständigen Standardisierungsorganisationen haben den Adressraum in fünf Klassen aufgeteilt, die sich in der Länge von Net-ID und Host-ID unterscheiden. Die so definierten Netzwerkclassen erlauben somit eine verschiedene Anzahl von Netzen mit unterschiedlicher Anzahl von Hosts, die innerhalb der jeweiligen Netzwerkklasse adressiert werden können. Praktische Bedeutung haben vor allem die Klassen A, B und C. Die Klasse D wird für sogenannte Multicast-Adressen verwandt und Klasse E-Adressen werden z.Z. überhaupt nicht verwendet. Die Zugehörigkeit von IP-Adressen zu den verschiedenen Netzclassen läßt sich an Hand des sogenannten **Class-Identifizier** erkennen. Das sind die ersten Bit einer IP-Adresse.

Klasse A-Netze

Bei Klasse A-Netzen wird das erste Oktett der IP-Adresse für die Adressierung des Netzwerkes (*Net-ID*) herangezogen und die restlichen drei Oktette für die Adressierung der Hosts innerhalb des Netzwerkes (*Host-ID*) verwendet (Abb. 2).

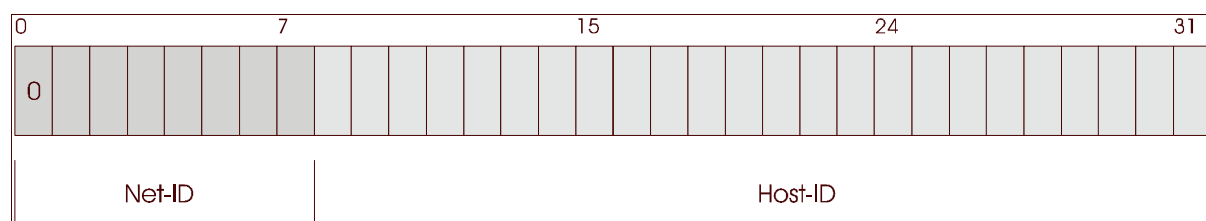


Abbildung 2: Verhältnis von Net-ID und Host-ID bei Klasse A-Netzen

Das erste Bit des ersten Oktetts (Class-Identifizier) besitzt bei Klasse A-Netzen **immer** den Wert „0“. Damit stehen für die eigentliche Adressierung des Netzwerkes nur noch die restlichen 7 Bit zur Verfügung. Das erste Oktett und somit die Net-ID kann bei Klasse A-Netzen also folgende Werte annehmen.

minimal: 00000000₂ bzw. **0**₁₀
maximal: 01111111₂ bzw. **127**₁₀

Es ergibt sich also eine theoretische Anzahl von 128 Netzen. Die Netze **0** und **127** sind für spezielle Anwendungen reserviert und fallen weg. Somit können letztendlich 126 Klasse A-Netze adressiert werden.

Für die Adressierung der Hosts innerhalb eines Klasse A-Netzes stehen 3 Oktette bzw. 24 Bit zur Verfügung. Rein rechnerisch wären damit je Klasse A-Netz $2^{24} = 16.777.216$ Hosts möglich.

Die erste und letzte Hostadresse eines Netzes darf jedoch nicht vergeben werden z.B. 11.0.0.0 und 11.255.255.255.

Die erste Adresse bezeichnet das Netz selbst und die letzte Adresse ist die sogenannte **Broadcastadresse**, die für Rundsendungen an alle Hosts des jeweiligen Netzes benutzt wird.

Somit stehen **16.777.214** adressierbare Host für ein Klasse A-Netz zur Verfügung.

Klasse B-Netze

Bei Klasse B-Netzen werden die ersten beiden Oktette der IP-Adresse für die Adressierung des Netzwerkes (Net-ID) und die anderen beiden Oktette für die Adressierung der Hosts innerhalb des Netzwerkes (Host-ID) verwendet.

Die ersten beiden Bits des ersten Oktetts (Class-Identifizier) besitzen bei Klasse B-Netzen **immer** den Wert „10“.

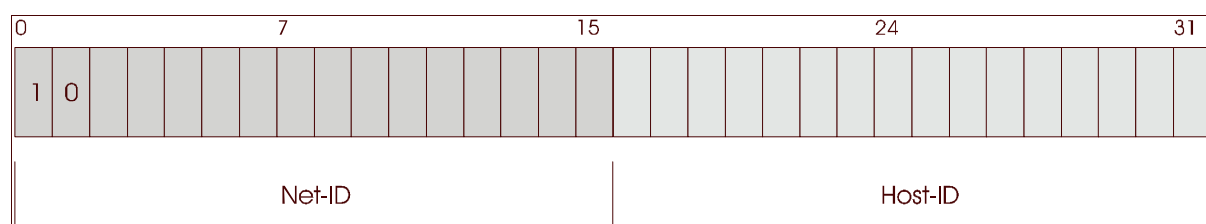


Abbildung 3: Verhältnis von Net-ID und Host-ID bei Klasse B-Netzen

Das erste Oktett kann bei Klasse B-Netzen also folgende Werte annehmen:

minimal: **10000000₂** bzw. **128₁₀**
 maximal: **10111111₂** bzw. **191₁₀**

Man kann hier schon erkennen, dass die Zugehörigkeit eine IP-Adresse zu einer bestimmten Netzklasse bereits durch den Wert des ersten Oktetts festgelegt ist.

Da bei Klasse B-Netzen die Net-ID noch ein weiteres Oktett umfasst, sind theoretisch folgende Net-IDs innerhalb von Klasse B-Netzwerken möglich:

minimal: **10000000.00000000₂** bzw. **128.0.**
 maximal: **10111111.11111111₂** bzw. **191.255**

Damit sind also insgesamt **16384** Klasse B-Netze möglich.

Für die Adressierung der Hosts innerhalb eines Klasse B-Netzes stehen zwei Oktette zu Verfügung. Rein rechnerisch kann man also je Klasse B-Netzwerk 65536 Hosts adressieren. Auch hier entfallen wieder der erste und der letzte Host, so dass **65534** Hosts übrig bleiben.

Klasse C-Netze

Bei Klasse C-Netzen werden die ersten drei Oktette der IP-Adresse für die Adressierung des Netzwerkes (Net-ID) und das letzte Oktett für die Adressierung der Hosts innerhalb des Netzwerkes (Host-ID) verwendet.

Das ersten drei Bits des ersten Oktetts (Class-Identifizier) besitzen bei Klasse C-Netzen *immer* den Wert „110“.

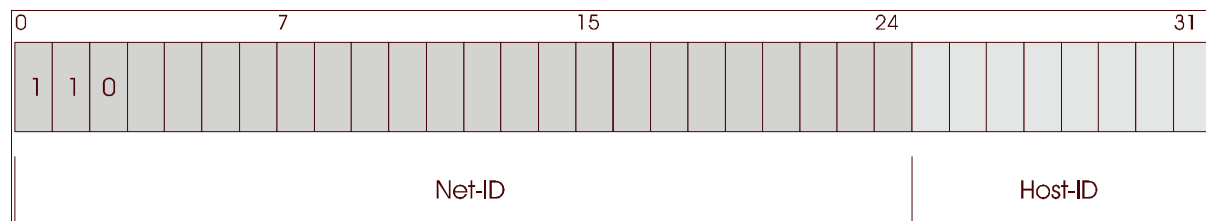


Abbildung 4: Verhältnis von Net-ID und Host-ID bei Klasse C-Netzen

Das erste Oktett kann bei Klasse C-Netzen also folgende Werte annehmen:

minimal: **11000000₂** bzw. **192₁₀**
 maximal: **11011111₂** bzw. **223₁₀**

Die Net-ID umfaßt drei Oktette. Ein Klasse C-Netzwerk kann also im Bereich folgender Net-IDs liegen.

minimal: **11000000.00000000.00000000₂** bzw. **192.0.0**
 maximal: **11011111.11111111.11111111₂** bzw. **223.255.255**

Somit sind **2.097.152** Klasse C-Netze möglich. Allerdings steht für die Adressierung der Hosts innerhalb eines Klasse C-Netztes nur ein Oktett zu Verfügung. Theoretisch sind das **256** Hosts. Da auch hier wieder erster und letzter Host entfallen, bleiben letztendlich 254 adressierbare Hosts übrig.

Klasse D-Netze

Der Class-Identifizier eines Klasse D-Netztes hat den Wert „1110“.

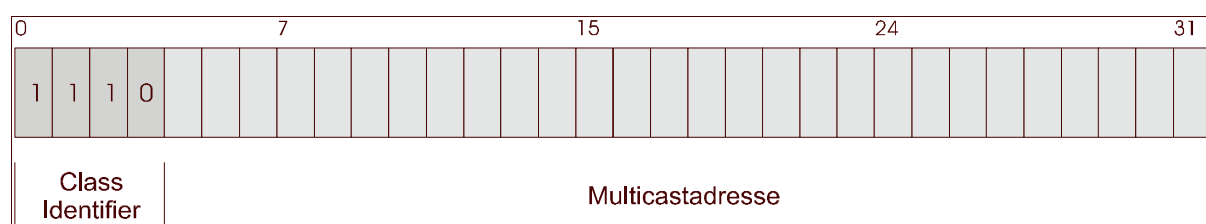


Abbildung 5: Klasse D- Netz

Das erste Oktett kann bei Klasse D-Netzen also folgende Werte annehmen:

minimal: **11100000₂** bzw. **224₁₀**
 maximal: **11101111₂** bzw. **239₁₀**

Es werden keine Bereiche für die Netz-ID oder die Host-ID festgelegt. Die möglichen IP-Adressen liegen im Bereich **224.0.0.0** und **239.255.255.255**.

Diese Adressen besitzen einen Sonderstatus. Es handelt sich dabei um sogenannte **Multicast-Adressen**.

Im Gegensatz zu Broadcastadressen (die ja alle Hosts im Netz ansprechen) dienen Multicast-Adressen dazu, innerhalb eines Netzes eine Gruppe von Hosts zu adressieren.

Klasse E-Netze

Diese Klasse wird momentan nicht verwendet. Die ersten vier Bit sind auf „1111“ gesetzt. Damit lassen sich IP-Adressen im Bereich von **240.0.0.0** bis **255.255.255.254** angeben.

3. Adreßregistrierung

Solange man nur ein privates IP-Netz ohne Anschluß an das Internet betreibt, ist man in der Vergabe der IP-Adressen frei. Es ist jedem selbst überlassen ob er ein Klasse A, Klasse B oder Klasse C-Netz betreiben möchte und welche Adressen er benutzt. Sobald die Adressen aber im Internet sichtbar werden sollen, muss die Adresse registriert sein, um die Eindeutigkeit sicherzustellen. Für die Gewährleistung der weltweiten Eindeutigkeit von IP-Adressen im öffentlichen Datenverkehr über das Internet ist eine zentrale Registrierungsorganisation die **Internet Assigned Number Authority (IANA)** zuständig. Auf nationaler Ebene vergeben im Auftrag der IANA die **Network Information Centre (NIC)** die IP-Adressen. In Deutschland wird diese Aufgabe vom DE-NIC wahrgenommen.

4. Besondere Adressbereiche

Obwohl bei privaten IP-Netzen ohne Zugang zum Internet die Adreßvergabe nach eigenem Ermessen erfolgen kann, hat die IANA für Private Networks spezielle Adreßräume reserviert. Diese Adressen werden im öffentlichen Internet nicht vergeben. Außerdem werden diese IP-Adressen, falls sie doch einmal in unbeabsichtigter Weise in das Internet gelangen sollten, nicht geroutet. Somit sind diese Adressen im Internet nicht sichtbar.

Nachstehende Tabelle listet diese speziellen Adreßbereiche auf:

Netzklasse	Anz.	Netz-Nummer		IP-Adressen	
		von	bis	von	bis
Class A	1	10.0.0.0		10.0.0.1	10.255.255.254
Class B	16	172.16.0.0	172.31.0.0	172.16.0.1	172.31.255.254
Class C	256	192.168.0.0	192.168.255.0	192.168.0.1	192.168.255.254

Wenn man ein privates IP-Netz aufbauen will, verwendet man also am besten Adressen aus diesen Adressbereichen.

5. Subnetting

Es gibt gute Gründe, Netzwerke in einzelne Subnetze zu unterteilen.

Man stelle sich vor, es wäre ein Klasse A-Netz mit seinen ca. 16 Millionen adressierbaren Hosts zu betreiben. Mit welcher Netzwerktechnologie sollte man wohl 16 Millionen Hosts in **einem** Netz verwalten.

Oder man stelle sich eine Firma vor, die verschiedene Standorte miteinander vernetzen will (Abb. 6). Um die Subnetze über Router verbinden zu können, muss jedem Subnetz eine andere Netzwerkadresse zugeordnet sein. Für jeden Standort braucht man somit auch eine eigene Netzwerkadresse. Bei der heutigen explosionsartigen Verbreitung des Internet ist die Vorstellung, drei Netzwerkadressen zu bekommen, absolut illusorisch. Nach außen darf das Firmennetz auch weiterhin nur als ein einziges Netzwerk sichtbar sein, nämlich als dasjenige, welches durch das zuständige NIC zugewiesen wurde.

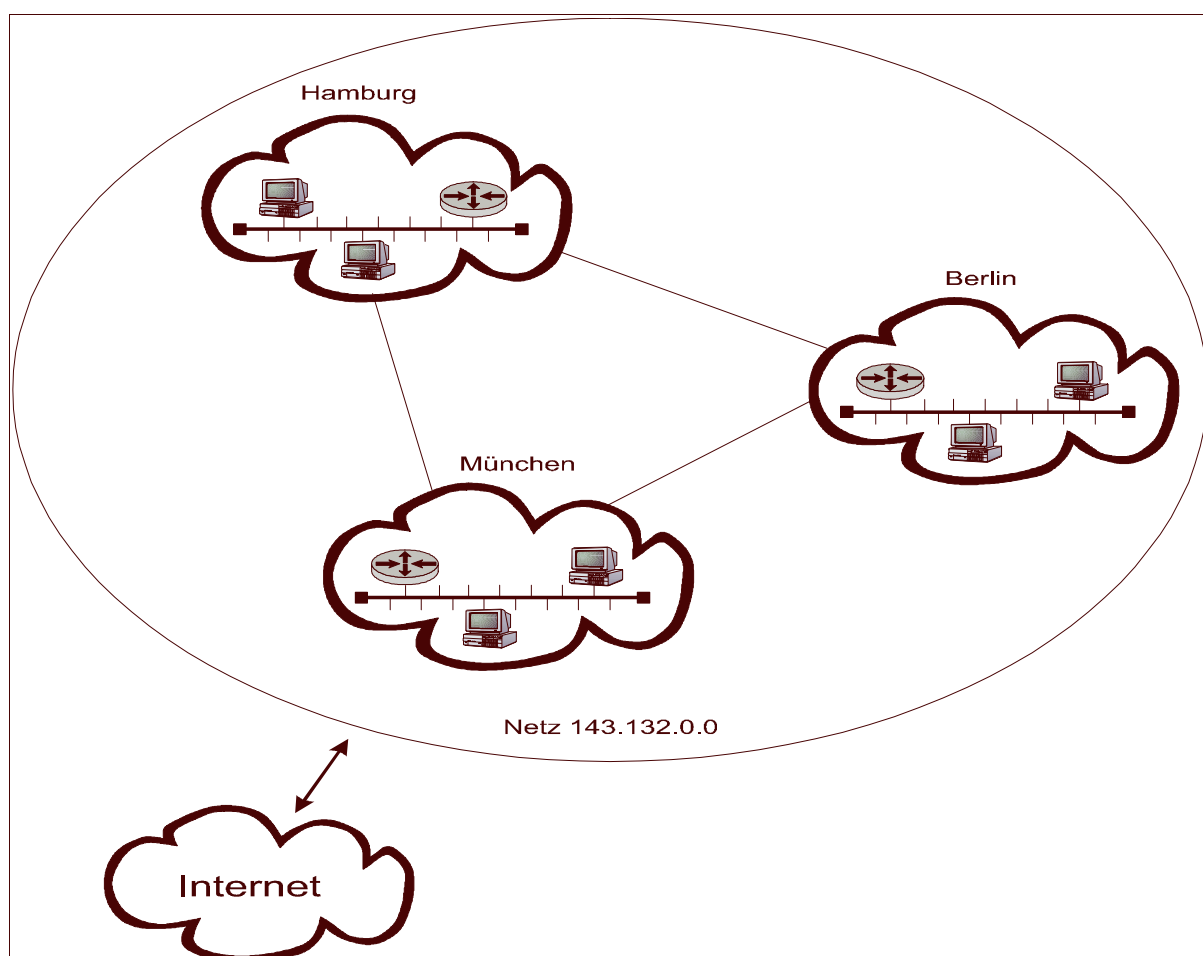


Abbildung 6: Notwendigkeit der Unterteilung eines klassischen Netzes in Subnetze

Um Subnetze innerhalb eines logischen Netzwerkes adressieren zu können, bedient man sich der „*subnetwork mask*“.

Sie stellt ebenso wie die IP-Adresse eine Folge von 32 Bit dar und gibt an, welcher Teil der IP-Adresse zur Netzadresse und welcher Teil zur Hostadresse gehört. Die Schreibweise der subnetwork mask ist an die IP-Adresse angepaßt: *dotted decimal*. Das Rechnen mit der subnetwork mask sollte aber nicht in der dezimalen Schreibweise erfolgen, da die Auswertung der subnetwork mask bitweise geschieht. Um mit subnetwork masks rechnen zu können, sollten Adresse und subnetwork mask in die binäre Schreibweise umgesetzt und dann analysiert werden.

Dabei ist wie folgt an die Auswertung der subnetwork mask heranzugehen.

Wenn die subnetwork mask bei einem Bit den binären Wert „1“ hat, wird das dazugehörige Bit aus der IP-Adresse in die Netzwerkadresse übernommen.

Wenn ein Bit in der subnetwork mask dagegen den binären Wert „0“ hat, wird das dazugehörige Bit aus der IP-Adresse in die Hostadresse übernommen.

Für nicht segmentierte Netzwerke ergeben sich damit je nach Netzwerkkategorie folgende Standard-Subnetmasks (*default subnetwork mask*):

Kategorie	dotted decimal	binary
A	255.0.0.0	1111111100
B	255.255.0.0	111111111111111100000000000000000000000000000000
C	255.255.255.0	111111111111111111111111000000000000000000000000

Abbildung 7: Standard-subnetwork masks für unsegmentierte Netze

Um ein Netz in Subnetze aufzuteilen, werden einfach Bits aus der Host-ID der Net-ID zugeordnet. Das erreicht man, indem die entsprechenden Bits in der subnetwork mask auf „1“ gesetzt werden. Für ein Klasse B-Netz, bei dem zwei Bits aus der Host-ID zur Net-ID wechseln, sieht eine solche *individual subnetwork mask* dann wie folgt aus.

B	255.255.192.0	1111111111111111111111111100000000000000000000000
---	---------------	---

An Hand der Firma aus der Abbildung 6 soll das weitere Herangehen bei der Aufteilung eines Netzes in Subnetze dargestellt werden. Die Aufgabenstellung besteht darin, das Klasse B-Netz 143.132.0.0 in drei Subnetze aufzuteilen.

Zunächst muss an Hand der Anzahl der geforderten Subnetze die Anzahl der Bits bestimmt werden, die der Adressierung der Subnetze dienen sollen. In unserem Beispiel sollen drei Subnetze gebildet werden, d.h. man benötigt zwei Bit ($2^2=4$). Mit zwei Bit lassen sich vier Subnetze erzeugen, rein rechnerisch reicht das für die Lösung unserer Aufgabenstellung zunächst aus.

Damit hat die subnetwork mask folgendes Aussehen:

255.255.192.0	1111111111111111111111111100000000000000000000000
---------------	---

Die ersten beiden Oktette und die zwei Bit aus dem dritten Oktett werden zur Adressierung des Netzes herangezogen. Die restlichen sechs Bit des dritten Oktetts und das gesamte vierte Oktett führen somit zu einer theoretischen Anzahl von 16384 (64 x 256) adressierbaren Hosts pro Subnetz.

255.255.192.0	1111111111111111111111111100000000000000000000000
---------------	---

143.132.0.0	100011111100001000000000000000000000000000000000
-------------	--



Mit dieser subnetwork mask lassen sich nun folgende Teilnetze realisieren:

Nr.	Subnetz	Net-ID	Host-ID
1	143.132.0.0	10001111 10000100 000	00000 00000000
2	143.132.32.0	10001111 10000100 001	00000 00000000
3	143.132.64.0	10001111 10000100 010	00000 00000000
4	143.132.96.0	10001111 10000100 011	00000 00000000
5	143.132.128.0	10001111 10000100 100	00000 00000000
6	143.132.160.0	10001111 10000100 101	00000 00000000
7	143.132.192.0	10001111 10000100 110	00000 00000000
8	143.132.224.0	10001111 10000100 111	00000 00000000

Auch hier werden das erste und das letzte Subnetz gestrichen. Es bleiben somit noch sechs Subnetze übrig. Allerdings hat sich die Anzahl der theoretisch adressierbaren Hosts auf 8192 (32 x 256) verringert.

Bei den Hosts werden allerdings auch wieder zwei Adressen gestrichen, nämlich die erste und die letzte (z.B. 143.132.32.0 und 143.132.63.255). Die erste Host-Adresse ist mit der Subnetzadresse identisch und die letzte Host-Adresse stellt die Broadcastadresse für das jeweilige Subnetz dar.

Somit bleiben je Subnetz 8190 adressierbare Hosts übrig. Das sollte ausreichen.

6. Verwendung nicht registrierter IP-Adressen

Wenn man keine Anbindung an das öffentliche Internet plant, ist man in der Wahl der Netzklasse völlig frei. Eine Umstellung auf öffentliche IP-Adressen ist dann allerdings nur mit großem Aufwand zu realisieren. Da Klasse A- und Klasse B-Netze ohnehin nicht mehr zu haben sind und seit 1996 auch keine kompletten Klasse C-Netze mehr vergeben werden, ist eine vollständige Umstellung des Netzes auf öffentliche IP-Adressen sowieso illusorisch.

Eine Alternative zur Verwendung öffentlicher IP-Adressen stellt die Anbindung des privaten Netzwerkes über einen Proxy-Server/Firewall an das öffentliche Internet dar. Abbildung 8 zeigt ein Beispiel. Eine Firma verfügt über zwei Standorte. Die Überlegungen bei der Wahl der Adressstruktur war von dem Wunsch bestimmt, die organisatorische und geografische Struktur des Unternehmens abzubilden. Dabei lassen sich verschiedene Standorte, Abteilungen und Unterabteilungen in die Adressstruktur integrieren. Die Standorte werden über IP-Router miteinander verbunden. Innerhalb der Standorte existieren Abteilungen mit unterschiedlichen Aufgaben. Jede Abteilung betreibt ihr eigenes Netzwerk und ist über Router mit einem Standort-Backbone verbunden. Aus diesem Backbone heraus erfolgt die WAN-Verbindung über Router zum anderen Standort. Für das private Netzwerk wird das Klasse A-Netz 10.0.0.0 verwendet. Für die Strukturierung in verschiedene Subnetze wird die subnetwork mask 255.255.255.0 verwendet. Pro Abteilung innerhalb eines Standortes stehen also maximal 254 Hostadressen zur Verfügung. Für jeden Standort lassen sich 254 verschiedene Abteilungsnetze einrichten. Einer Erweiterung des Unternehmens steht ebenfalls nichts im Wege, 254 Standorte ließen sich mit einer eigenen Netzadresse versorgen.

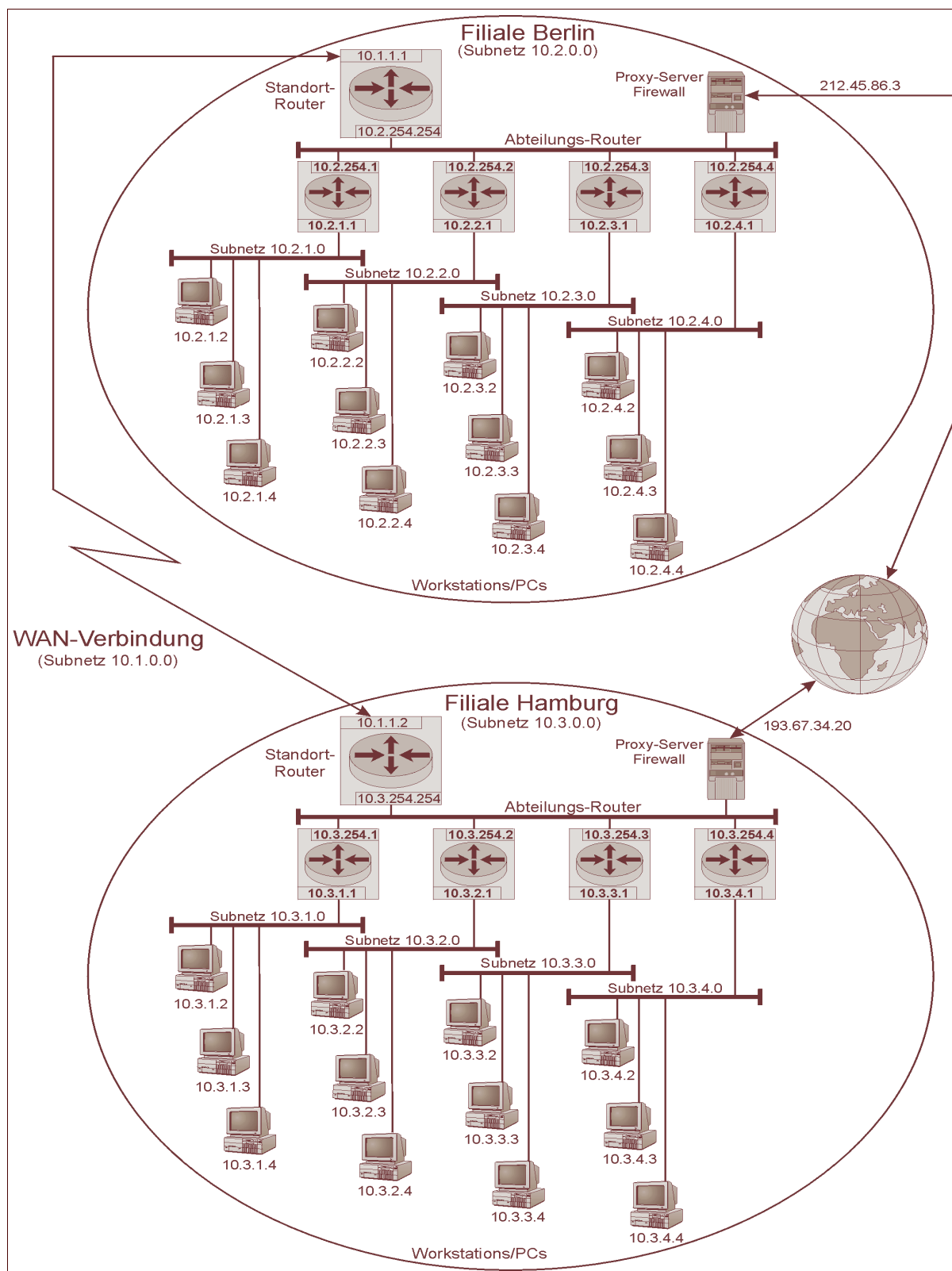


Abbildung 8: Struktur eines Private Network / Anbindung des Private Network über Proxy-Server an das Internet

Standort	Abteilung	Netzadresse
Berlin	Auftragsbearbeitung	10.2.1.0
Berlin	Buchhaltung	10.2.2.0
Berlin	Versand	10.2.3.0
Berlin	Datenverarbeitung	10.2.4.0
Hamburg	Auftragsbearbeitung	10.3.1.0
Hamburg	Buchhaltung	10.3.2.0
Hamburg	Versand	10.3.3.0
Hamburg	Datenverarbeitung	10.3.4.0
WAN-Verbindung der Standorte		10.1.1.0

Eine solche Herangehensweise vereinfacht die Administration des Netzwerkes, da sich aus der IP-Adresse bereits die Zugehörigkeit eines Hosts zu Standort und Abteilung ableiten läßt.

Die Anbindung an das öffentliche Internet erfolgt an jedem Standort über einen Proxy-Server. Dem Proxy wird eine registrierte Adresse aus dem öffentlichen Adreßbereich zugewiesen. Er übersetzt die Anfragen der Clients aus dem Private Network und leitet sie stellvertretend (proxy) in das Internet weiter. Die Antworten aus dem Internet stellt er dann dem Client innerhalb des Private Network wieder zu.

Statt einer (ohnehin nicht realisierbaren) Umstellung des gesamten Netzwerkes auf registrierte Adressen werden in diesem Beispiel lediglich zwei registrierte Adressen benötigt.

7. Domain Name Service

Symbolische Namen

Um in einem TCP/IP-Netz mit einem anderen Host Verbindung aufzunehmen, muss man dessen IP-Adresse kennen, da die Adressierung des Host letztendlich *immer* über die IP-Adresse erfolgt.

Nun ist es der menschlichen Natur fremd, ellenlange Zahlenkolonnen als Adresskonzept zu akzeptieren. Es ist einfacher, sich einen aussagekräftigen Namen zu merken, als eine 32 Bit lange Zahlenkombination.

So ist die IP-Adresse 192.168.2.21 sicherlich schlechter aus dem Stegreif abzurufen als der Rechnername „**dagobert.duck.entenhausen.de**“.

Deshalb wurde schon in der Anfangszeit von TCP/IP und Internet ein Namenssystem entwickelt, das die Zuordnung solcher symbolischer Namen zu den dazugehörigen IP-Adressen erlaubt.

Die Abbildung der symbolischen Rechnernamen auf die dazugehörige IP-Adresse läßt sich auf zwei Arten realisieren. Es gibt eine *statische* sowie eine *dynamische* Methode.

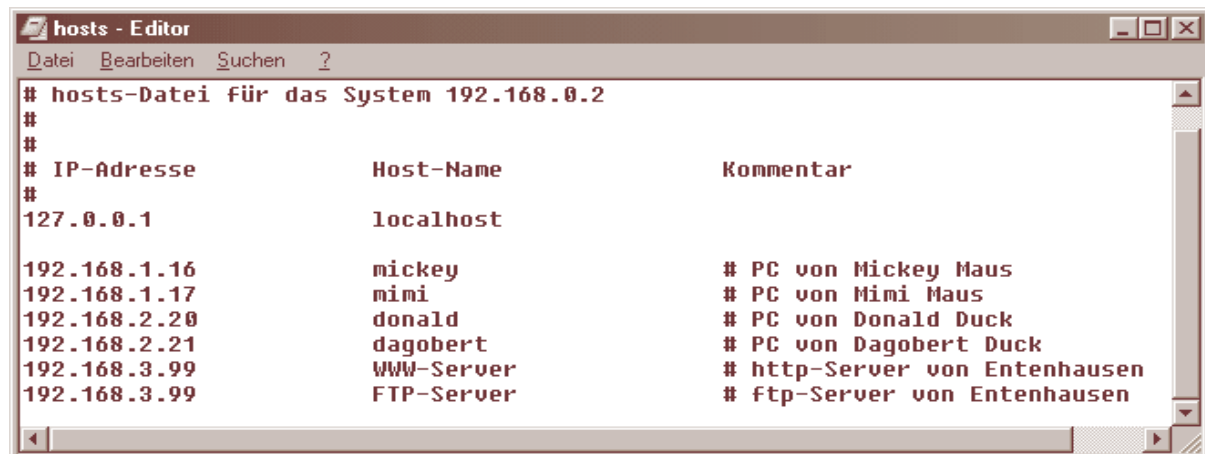
Statische Methode:

Das einfachste Verfahren, symbolische Namen auf IP-Adressen abzubilden, ist der Einsatz der sogenannten „**hosts-Datei**“.

Auf Unix-Systemen befindet sich diese Datei im Verzeichnis „/etc“. Unter Windows 9x befindet sich diese Datei unterhalb von %windir% also zum Beispiel in C:\Windows.

Unter Windows NT 4.0 befindet sie sich unterhalb von %SystemRoot%\system32\drivers\etc.

Die hosts-Datei hat dabei folgenden Aufbau:



```

# hosts-Datei für das System 192.168.0.2
#
#
# IP-Adresse           Host-Name           Kommentar
#
127.0.0.1             localhost

192.168.1.16         mickey              # PC von Mickey Maus
192.168.1.17         mimi                # PC von Mimi Maus
192.168.2.20         donald              # PC von Donald Duck
192.168.2.21         dagobert            # PC von Dagobert Duck
192.168.3.99         WWW-Server          # http-Server von Entenhausen
192.168.3.99         FTP-Server          # ftp-Server von Entenhausen

```

Abbildung 9: Aufbau der hosts-Datei

IP-Adresse und symbolischer Name werden dabei durch Leerzeichen bzw. Tabulatoren von einander getrennt. Kommentare müssen durch ein vorangestelltes „#“ gekennzeichnet werden.

Einer IP-Adresse können dabei auch mehrere symbolische Namen zugeordnet sein. So ist der PC, dessen Netzwerkkarte die IP-Adresse 192.168.3.99 zugeordnet ist, einmal unter dem Host-Namen „**WWW-Server**“ als auch unter dem Host-Namen „**FTP-Server**“ erreichbar. Umgekehrt darf aber ein Host-Name nicht zweimal vergeben werden, d.h. zwei verschiedenen IP-Adressen zugeordnet sein. Das würde das Prinzip der Eindeutigkeit der IP-Adressen verletzen.

Wenn nun der lokale Rechner mit einem hier aufgeführten Netzwerkknoten beispielsweise über eine Telnet-Session Kontakt aufnehmen will, so braucht er das nicht mehr durch die Eingabe des Befehls `telnet 192.168.2.21` zu tun, sondern er gibt `telnet dagobert` ein. Das System sieht nun in der hosts-Datei nach und versucht den Namen an Hand der Datei aufzulösen. Gelingt das, dann wird über die ermittelte IP-Adresse eine Telnet-Session mit dem gewünschten Kommunikationsziel aufgebaut. Gelingt das nicht (das wäre beispielsweise der Fall, wenn eine Telnet-Session mit dem Computer `tweety` aufgenommen werden sollte, der in der hosts-Datei nicht aufgeführt ist), wird der Verbindungsaufbau mit einer entsprechenden Fehlermeldung abgelehnt. Die Namen aus der lokalen hosts-Datei verlassen das eigene System nicht. Es ist immer die IP-Adresse, die für den Verbindungsaufbau verwendet wird.

So einfach wie dieses Namensverfahren auch ist, eine Wartung dieses Systems ist in größeren Netzwerken wie z.B. dem Internet unmöglich. Änderungen in der Netztopologie ziehen dann immer eine Anpassung der lokalen hosts-Datei auf allen Rechnern nach sich. Ab einer bestimmten Anzahl von Hosts ist der Aufwand für die manuelle Pflege der lokalen hosts-

Dateien unvertretbar hoch. Zudem muss wegen der Tabellenform der hosts-Datei jeder Host-Name eindeutig sein, d.h. er kann nicht zweimal vergeben werden. Doppelte Namen wie in einer hierarchischen Struktur sind nicht möglich.

Die Namensauflösung über die hosts-Datei kommt also allenfalls in kleinen Netzen in Frage in allen anderen Fällen benutzt man das dynamische Verfahren zur Auflösung der symbolischen Namen: den **Domain Name Service (DNS)**.

Funktionsweise des DNS

Achtung:

Deutlich muss gesagt werden, dass der Begriff Domain in diesem Zusammenhang nichts (aber auch gar nichts) mit einer Windows-NT Domäne zu tun hat!



Früher wurden alle im Internet angeschlossenen Rechner über die hosts-Datei identifiziert. Mit dem Anwachsen der im Internet vernetzten Computer war das schließlich aus den oben beschriebenen Gründen nicht mehr möglich. 1984 fand daraufhin der Wechsel zum Domain Name Service statt. Über diesen Dienst lassen sich Namen wie „**www.bundeswehr.de**“ in ihre IP-Adressen übersetzen und umgekehrt.

Zur Namensauflösung kommt nur ein System in Frage, das **dezentral** organisiert ist. Zentrale Systeme würden aus allen Bereichen des Netzwerkes sternförmig angesprochen und führen zu einer stark erhöhten Netzbelastung.

Deshalb werden verteilte Namens-Server eingerichtet, die für einen fest definierten Netzwerkbereich (Domain) zuständig sind. Diese Namens-Server (DNS-Server) liegen dabei in unterschiedlichen Schichten einer baumartigen hierarchischen Struktur und verwalten den ihnen zugeordneten Netzwerkbereich.

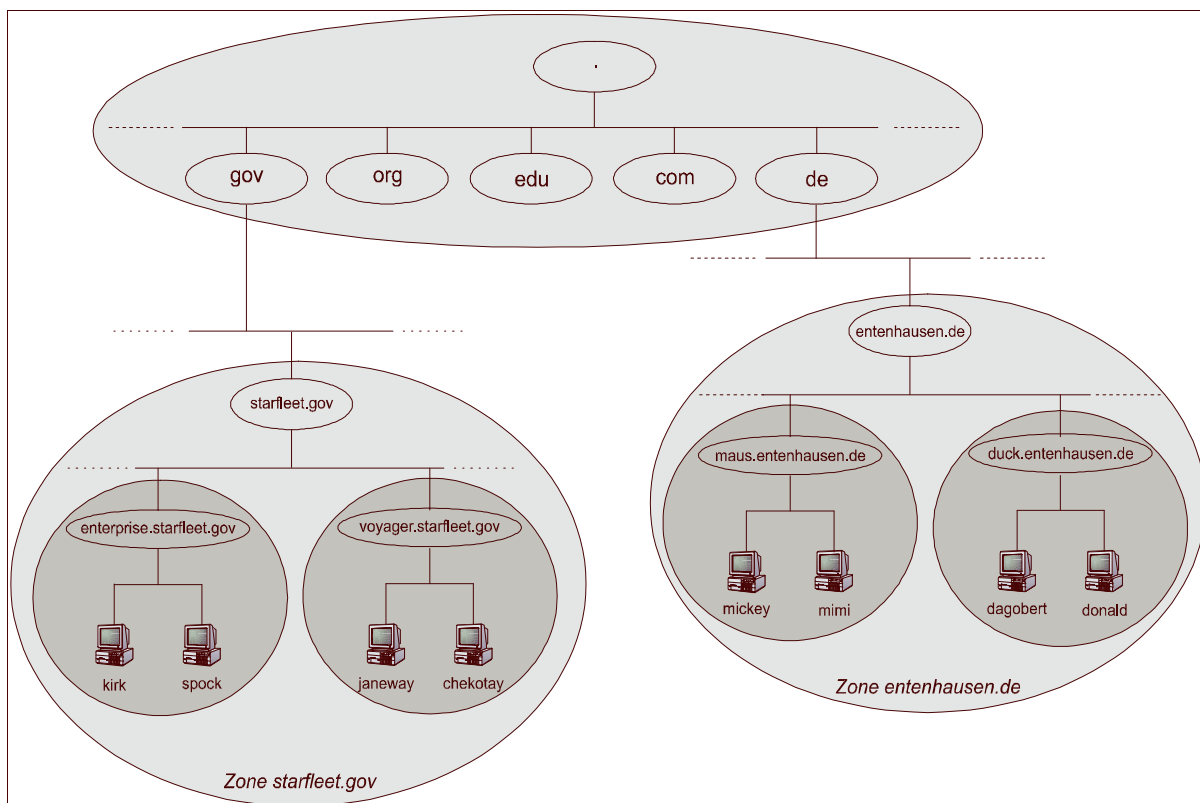


Abbildung 10: DNS-Zonen

Die höchste Hierarchiestufe eines Namensbaumes sind die sogenannten „*toplevel domains*“. Sie wurden bereits in den ersten Jahren der Gründung des Internet festgelegt und in den USA verwaltet. Entgegen den Gepflogenheiten anderer Staaten setzt sich diese oberste Hierarchieebene in den USA aus organisatorischen Strukturbezeichnungen zusammen. Mit zunehmender Internationalisierung des Internet wurden dann die Länderkürzel eingeführt.

Toplevel Domain	Beschreibung / Land
com	kommerzielle Organisationen in den USA
edu	Bildungs- und Forschungseinrichtungen
gov	Amerikanische Bundesbehörden
mil	Amerikanische Militäreinrichtungen
net	Netzwerk-Provider
org	Nichtkommerzielle Organisationen
int	Internationale Organisationen
au	Australien
at	Österreich
ch	Schweiz
de	Deutschland
es	Spanien
fr	Frankreich
se	Schweden
uk	Großbritannien
...	...

Die hierarchische Struktur wird weiter nach unten fortgesetzt und kann mehrere Domains und Subdomains umfassen (Abb. 10). Jede Domain wird mit einem Dezimalpunkt von den anderen Domains getrennt, wobei die Toplevel Domain ganz rechts und der Rechnername ganz links steht.

Im DNS-Namenssystem kann jede Domain unterhalb der Top-Level-Domain aus bis zu 63 Zeichen bestehen (Sonderzeichen und Unterstriche sind nicht erlaubt). Der vollständige Name eines Rechners (Pfad im DNS-Baum) wird als **Fully Qualified Domain Name** bezeichnet und könnte zum Beispiel lauten:

dagobert.duck.entenhausen.de

Für die Verwaltung von DNS-Namen ist der Begriff Zone wichtig. Eine Zone kann aus einer Domain und beliebigen Subdomains bestehen. Jede Zone betreibt normalerweise einen eigenen DNS-Server.

Möchte ein Rechner einen Namen zu einer IP-Adresse auflösen, wendet er sich an seinen DNS-Server. Kann dieser den Namen nicht auflösen, wendet er sich an den nächst höheren Name-Server.

Wenn zu dem Namen eine IP-Adresse ermittelt werden konnte, wird sie dem anfragenden Rechner mitgeteilt. Der adressiert dann den Zielrechner über die IP-Adresse.

Literatur

Gerhard Lienemann
TCP/IP-Grundlagen
Verlag Heinz Heise, 1996

Martin Kuppinger
IP-Adressen im Netz
PC Professionell 06/98