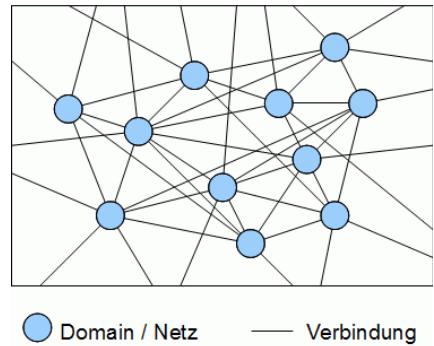


Internet.

Das **Internet ist ein Netz von Netzen**, dh. mehrere Rechner bilden jeweils ein Netzwerk und diese sind untereinander vernetzt. Das Internet ist nicht hierarchisch, sondern dezentral aufgebaut - mit möglichst vielen Verbindungen untereinander.

- Ein Rechner, der einem Netz angehört, wird **Host** genannt.
- Eine **Domain** ist ein **Netz**, dessen Rechner organisatorisch zusammengehören.
- Eine Domain kann sowohl sowohl physikalisch und/oder organisatorisch wiederum in **Subnetze** und/oder **Subdomains** unterteilt werden.
- Zur Datenübertragung zwischen den Hosts gibt es genormte Regeln, die **Protokolle** (engl. Protocol).
- Die werden in Blöcken, den **Pakete** übertragen. Jedes Paket enthält:
 - Den **Header** (Vorspann), in dem die für das Protokoll charakteristischen Informationen stehen.
 - Den **Nutzdaten**. Auf der Empfängerseite werden die Nutzdaten der Pakete wieder zusammengesetzt.



Datenübertragungsprotokolle.

- **TCP/IP** (Transmission Control Protocol)

IP ist für die Adressierung der Daten zuständig, TCP für die Übertragung der Daten. Dabei werden anschaulich die TCP Pakete in IP Pakete eingepackt und beim Empfänger wieder ausgepackt. Sowohl TCP als auch IP erkennen **Fehler in den Paketen**, die bei der Datenübertragung auftreten können. In diesen Fällen wird vom Empfänger das Paket erneut vom Sender angefordert. Die Pakete enthalten eine Nummer mit deren Reihenfolge, damit sie wieder beim Empfänger in der richtigen Reihenfolge zusammengesetzt werden können.

- Der Standard wurde 1984 im ARPANET (Advanced Research Projects Agency, ein Projekt des Verteidigungsministeriums der USA) eingeführt.
- Das ARPANET war der Vorläufer des Internets.
- Die maximale **Paketgröße** (engl. MTU) beträgt 1500 Bytes.
- **Adressierung der Daten** erfolgt über das **IP** Protokoll (Internet Protocol).

Derzeit Version 4 genutzt (IPv4). Zur Zeit beginnende Umstellung auf Version 6 (IPv6), um bei der immer weiter wachsenden Anzahl an angeschlossenen Rechnern genügend Adressen zur Verfügung zu haben.

Weitere Informationen:

- TCP/IP: <http://www.elektronik-kompendium.de/sites/net/0606251.htm>
- IPv4: <http://www.elektronik-kompendium.de/sites/net/0811271.htm>
- TCP: <http://www.elektronik-kompendium.de/sites/net/0812271.htm>

Auf TCP/IP setzen weitere Protokolle auf, wie zum Beispiel **NetBIOS over TCP/IP** (auf die wiederum Protokolle aufsetzen wie **SMB - Server Message Block oder CIFS - Common Internet File System**, die allgemein gesprochen als «**Windows-Netzwerk Umgebung**» bekannt sind). Weitere Informationen:

- NetBIOS: <http://www.elektronik-kompendium.de/sites/net/0907221.htm>

- **UDP (User Datagram Protocol).**

- Verwendung: Übertragung der aktuellen Uhrzeit zur automatischen Einstellung für das Betriebssystem, Audio- und Videoübertragungen.
- **Paketfehler werden erkennen**, aber **im Fehlerfall werden diese Pakete verworfen** und nicht erneut angefordert.
- Weiterhin müssen die UDP Pakete in der richtigen **Reihenfolge beim Empfänger** eintreffen, da diese nicht nummeriert sind.
- Bei UDP Paketen ebenfalls die **IP Adressierung** verwendet.

Weitere Informationen:

- UDP: <http://www.elektronik-kompendium.de/sites/net/0812281.htm>

IP Adressierung.

Ein Host im **Internet (WAN = Wide Area Network)** oder **Intranet (LAN = Local Area Network)**, z. Bsp. internes Firmennetz) muß eine eindeutige IP Adresse besitzen, die aus 32 Bits (IPv4) besteht. Diese wird dem Netzwerkinterface (Netzwerkkarte oder auf dem Motherboard integrierte Netzwerkschnittstelle) zugewiesen. Ein Rechner kann auch mehreren Netzen angehören - einen derartigen Rechner bezeichnet man als **Gateway Rechner**. Zur besseren Übersicht werden die 32 Bit in vier Bytes ($4 \times 8 \text{ Bit} = 32 \text{ Bit}$) dargestellt. Notiert wird eine IP Adresse in der **Dotted Quad Notation**, zum Beispiel 192.168.185.10 in dezimaler Schreibweise. Beispiel:

11000000	10101000	10111001	00001010	Dual
C0	A8	B9	0A	Hexadezimal
192	168	185	10	Dezimal

IP Adressen enthalten einen **Netzwerk Anteil** und den **Host Anteil**. Bei der IP Adresse 192.168.185.10 wären die ersten 24 Bit die Netzwerk-ID, die letzten 8 Bit die Host-ID:

Netzwerk-ID	Host-ID
192	10

IP Adressen werden in **Klassen** aufgeteilt, in denen festgelegt ist, wie viele Bits die Netzwerk ID und wie viele Bits die Host ID bilden:

Klasse	32 Bit IP Adresse	
A	8 Bit Netzwerk-ID	24 Bit Host-ID
B	16 Bit Netzwerk-ID	16 Bit Host ID
C	24 Bit Netzwerk-ID	8 Bit Host ID

Aus der Einteilung ergeben sich für die Klassen sowohl die **Bereiche der Netzwerkadressen** und die maximale Anzahl der Hosts in jeder Klasse:

Klasse	Netzadresse von	Netzadresse bis	Maximale Anzahl der Hosts
A	1.0.0.0	127.0.0.0	Pro Netz ca. 1,6 Mio. Hosts
B	128.0.0.0	191.255.0.0	16320 Netze mit je 65024 Hosts
C	192.0.0.0	223.255.255.0	ca. 2 Mio. Netze mit je 254 Hosts
D, E, F	224.0.0.0	254.0.0.0	Reserviert für spezielle Verwendung

Bei der Vergabe von IP Nummern für ein Intranet gibt es Bereiche, die **im Internet nicht verwendet** werden dürfen. Diese **IP Adressen sind ausschließlich innerhalb eines LAN** zu verwenden:

- **Klasse A** 10.0.0.0 bis 10.255.255.255
- **Klasse B** 172.16.0.0 bis 172.31.255.255
- **Klasse C** 192.168.0.0 bis 192.168.255.255

Die als Beispiel aufgeführte IP Adresse **192.168.185.10** gehört zur Klasse C (**Netzwerkteil** 192.168.185. und **Hostteil** .10) eines lokalen Netzwerkes.

Nicht alle Adressen sind für Hosts reserviert:

- Die **Oktets 0 für den Host-ID Teil** adressieren das Netzwerk - **Netzwerkadresse** (Bsp.: 192.168.185.0).
- Die **Oktets 255 des Host-ID Teiles** dienen als **Broadcast Adresse**. Über die Broadcast Adresse wird an alle Hosts eines Netzwerkes zugleich adressiert (Bsp.: 192.168.185.255).

In den verschiedenen Klassen sind **für spezielle Zwecke Netzwerke reserviert**. So wird zum Beispiel das Netz 169.254.0.0 als Local Link oder **Zeroconf (Apple: Rendezvous Device)** bezeichnet und ist für sogenanntes »Netzwerk Plug & Play« von lokalen Netzwerk-Geräten wie Laptops, Druckern usw. mit Ethernet Interface reserviert. Näheres siehe <<http://www.zeroconf.org>>. Dies ist nicht das einzige Netz, außer der schon erwähnten Unterteilung in Privat/Internet, deren Verwendung festgelegt und reserviert ist:

<u>Adressblock:</u>	<u>Zweck:</u>	<u>Adressblock:</u>	<u>Zweck:</u>
0.0.0.0/8	»This« Network (RFC1700)	192.0.0.0/24	Reserviert
10.0.0.0/8	Private-Use Networks (RFC1918)	192.0.2.0/24	Test-Netz
14.0.0.0/8	Public-Data Networks (RFC1700)	192.88.99.0/24	6to4 Relay Anycast (RFC3068)
24.0.0.0/8	Netzwerke Kabelfernsehen	192.168.0.0/16	Private-Use Networks (RFC1918)
39.0.0.0/8	Reserviert (RFC1797)	198.18.0.0/15	Network Interconnect Device
127.0.0.0/8	Loopback (RFC1700)	223.255.255.0/24	Benchmark Testing (RFC2544)
128.0.0.0/16	Reserviert	224.0.0.0/4	Reserviert
169.254.0.0/16	Zeroconf (RFC3330)	240.0.0.0/4	Multicast (RFC3171)
172.16.0.0/12	Private-Use Networks		Reserviert für zukünftigen Gebrauch (RFC1700)
191.255.0.0/16	Reserviert		

- Als RFC (Request for Commands) werden die festgelegten Normen für das Internet bezeichnet:

<http://tools.ietf.org/html> oder <http://www.rfc-editor.org>

TCP / UDP Ports.

Bei der Adressierung genügt nicht allein die IP Adresse eines Rechners. Jeder Host besitzt **Ports in Form einer ganzen Zahlen zwischen 0 bis 65535**. Diesen Portnummern, Teil der Adressierung, ist jeweils ein bestimmtes Anwendungsprotokoll (und damit auch bestimmte Anwendungsprogramme) zugeordnet bzw. stehen für Clientprogramme zur freien Verfügung, um Verbindungen aufzubauen.

- Port 0 – 1023 von der IANA Organisation (Internet Assigned Numbers Authority) standardisiert.
- Port 1024 – 49151 werden von der IANA auf Anfrage registriert (registrierte Ports).
- Port 49152 – 65535 bei Bedarf frei verfügbar (private dynamische Ports).

Beispiel: Listing der aktuellen Verbindungen mit dem Programm TCPView, frei erhältlich unter <http://www.microsoft.com/technet/sysinternals/default.mspx>

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
[System Process]	0	TCP	andromeda.gate.local	49508	fa-in-f101.1e100.net	http
[System Process]	0	TCP	andromeda.gate.local	49519	lb-v111.net.ke3.speedkom.net	http
[System Process]	0	TCP	andromeda.gate.local	49520	85.183.249.139	https
firefox.exe	3380	TCP	andromeda	49502	localhost	49503
firefox.exe	3380	TCP	andromeda	49503	localhost	49502
firefox.exe	3380	TCP	andromeda	49504	localhost	49505
firefox.exe	3380	TCP	andromeda	49505	localhost	49504
firefox.exe	3380	TCP	andromeda.gate.local	49514	lb-v111.net.ke3.speedkom.net	http
firefox.exe	3380	TCP	andromeda.gate.local	49515	lb-v111.net.ke3.speedkom.net	http
firefox.exe	3380	TCP	andromeda.gate.local	49516	lb-v111.net.ke3.speedkom.net	http
firefox.exe	3380	TCP	andromeda.gate.local	49517	lb-v111.net.ke3.speedkom.net	http
firefox.exe	3380	TCP	andromeda.gate.local	49518	lb-v111.net.ke3.speedkom.net	http
firefox.exe	3380	TCP	andromeda.gate.local	49521	fra07s07-in-f149.1e100.net	http
firefox.exe	3380	TCP	andromeda.gate.local	49522	fra07s07-in-f149.1e100.net	http
firefox.exe	3380	TCP	andromeda.gate.local	49523	fra07s07-in-f149.1e100.net	http
firefox.exe	3380	TCP	andromeda.gate.local	49524	91.215.101.85	http
System	4	TCP	andromeda.gate.local	49525	sirius.gate.local	microsoft-ds

Bekannte Ports werden hier nicht als Nummer, sondern mit Namen angezeigt

- unverschlüsselte Browserverbindung http = Port 80
- SSL verschlüsselte Browserverbindung https = Port 443
- Windows-Netzwerk Freigaben microsoft-ds = Port 445

Netzaufbau.

Router / Gateway Rechner:

Ein **Router** stellt die Verbindung zwischen verschiedenen Netzen her und trennt sie physikalisch voneinander, zum Beispiel als Nahtstelle zwischen dem LAN einer Firma und dem WAN des Internets. Diese Aufgabe kann auch ein Rechner übernehmen: **Gateway Rechner**. Neben der Funktion, die Netze zu trennen, werden diese Aufgaben erfüllt

- NAT (Network Address Translation)**
Übersetzung von privaten IP Adressen in Internet Adressen und umgekehrt.
- Weitere Informationen: <http://www.elektronik-kompendium.de/sites/net/0812111.htm>

• Firewall

Erlaubt oder sperrt Protokolle bzw. Ports für den ausgehenden und eingehenden Datenverkehr.

- <http://www.elektronik-kompendium.de/sites/net/0803051.htm>

• Proxy

- Cache (temporäre Zwischenspeicherung) zur Reduzierung des Datenverkehrs.
- Virenscanner.
- Blacklists zum Sperren für bestimmte Internetadressen, für Dateien mit bestimmten Inhalten. Sperren von Internetdiensten für bestimmte Clients (auch zeitliche Steuerung möglich).
- ... usw.

- Weiter Informationen:

<http://www.elektronik-kompendium.de/sites/net/1101221.htm>

Router und Gateways werden auch in großen Firmennetzen zur Trennung der einzelnen Netze innerhalb der Firma eingesetzt. Die Netze, die der Router verbindet, können auch verschiedener physikalischer Natur oder Topologie sein (Ethernet, Token Ring, ISDN usw.). Ein Router «kennt» die Adressen für die Netze, leitet Signale über die entsprechenden Interface an die Netze weiter. Einem Router wird in der Regel eine Bridge oder ein Switch nachgeschaltet.

- Weitere Informationen: <http://www.elektronik-kompendium.de/sites/net/0810101.htm>

Bridge:

Teilt ein einziges Netz in einige Teilnetze auf, um Kollisionen zwischen dem Datenverkehr zu vermeiden. Wenn zu viele Rechner in einem physikalischen Netz vorhanden sind und sich das Netz teilen müssen, sinkt die Bandbreite. Die Bridge lässt Signale durch, die für die Rechner des anderen Teilnetzes bestimmt sind. Als Broadcast adressierte Signale werden in alle Teilnetze gesendet. Einer Bridge ist in der Regel ein Hub oder Switch nachgeschaltet, da die Bridge nur wenige Anschlüsse für die Teilnetze aufweist.

- Weitere Informationen: <http://www.elektronik-kompendium.de/sites/net/0901101.htm>

Hub:

Wird verwendet, um in einem Netzsegment mehrere Rechner über UTP Kabel sternförmig anschließen zu können. Obwohl es räumlich als Stern Topologie erscheint, liegt einem Hub logisch die Bus Topologie zugrunde. **Ein Hub trennt nicht den Signalweg auf, jeder Rechner am Hub erhält das Signal** und die Bandbreite erniedrigt sich daher, je mehr PC's am Hub angeschlossen sind.

- Weitere Informationen: <http://www.elektronik-kompendium.de/sites/net/1405161.htm>

Switch:

Wird verwendet, um in einem Netzsegment mehrere Rechner über UTP Kabel sternförmig anschließen zu können. **Im Gegensatz zum Hub trennt ein Switch die Signalwege zu den Rechnern auf.** Signale, die nicht für einen PC bestimmt sind, werden auch nicht übertragen.

- Weitere Informationen: <http://www.elektronik-kompendium.de/sites/net/0811021.htm>

Das Netzwerk Interface.

Möglichkeiten der **Zuweisung einer IP Adresse** für eine Netzwerkschnittstelle (es wird also nicht dem Rechner, sondern seinen Schnittstellen zugewiesen):

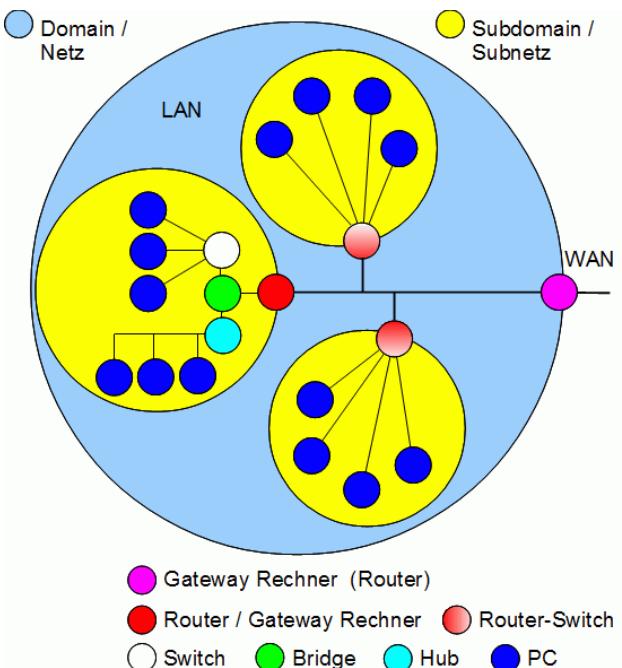
• Statische IP Adresse:

Durch Konfiguration einer festen IP Nummer über das Betriebssystem des Rechners.

• Dynamische IP Adresse:

- Ein Rechner, der online geht, wird vom **ISP (Internet Service Provider)** für sein Netzwerkinterface automatisch eine gerade freie **IP Nummer aus dem Pool der Nummern** durch einen **DHCP Server (Dynamic Host Configuration Protocol)** betrieben vom ISP zugewiesen. *Man kann, gegen höhere Gebühren, bei einem Provider auch immer die gleiche IP zugeteilt bekommen.*

In Firmen mit vielen Rechnern (jeden Rechner eine statische IP zu geben, würde zu viel Arbeit bedeuten) ist es



auch üblich, im LAN einen eigenen DHCP Server zu betreiben.

- IP Nummern lassen sich auch **beim Booten des Rechners** einem Netzwerkinterface zuweisen, das sich eindeutig identifizieren kann. Jede **Netzwerkkarte**, die hergestellt wird, besitzt eine **einige MAC (Media Access Control) Adresse** als Kennung. Beim Booten des Rechners kontaktiert er den sogenannten **BOOTP (Bootstrap Protocol) Server** im Firmennetz, aufgrund der gesendeten MAC Adresse der Netzwerkschnittstelle wird dem Host die dafür vorgesehene IP Nummer zugewiesen. Die MAC Adresse ist eine 6 Byte lange Hardware Adresse der Netzwerkkarte. Jede Netzwerkkarte auf der Welt ist vom Hersteller mit einer einmaligen Hardware Adresse versehen worden.

- Weitere Informationen DHCP: <http://www.elektronik-kompendium.de/sites/net/0812221.htm>
- Weitere Informationen MAC: <http://www.elektronik-kompendium.de/sites/net/1406201.htm>

Nützliche Kommandos.

Mit dem **Konsolenkommando ipconfig** (Windows) **oder ifconfig** (Unix, Linux, Mac OS X) kann u.a. die Schnittstellenkonfiguration überprüft werden. Hat ein Rechner die falsche IP Nummer (zum Beispiel die falsche Netzwerk ID), kann er sich nicht mit anderen Hosts verbinden.

Weitere Informationen: <http://www.elektronik-kompendium.de/sites/net/0901051.htm>

Ob ein Rechner im Netzwerk erreichbar (online) ist, kann mit dem **Konsolenkommando ping** (Windows, Unix, Linux, Mac OS X) getestet werden, auch der eigene Host. Damit ließe sich zum Beispiel klären, warum man nicht ins Internet kommt, weil der Router, Proxy oder das Gateway möglicherweise nicht erreichbar ist, trotz richtig konfigurierter eigener Schnittstelle.

- Eine Zeitüberschreitung der echo Anforderung kann aber auch den Grund haben, daß eine Firewall ICMP Anfragen wie tracert, ping etc. blockiert!
- Weitere Informationen: <http://www.elektronik-kompendium.de/sites/net/0901031.htm>

Das **Konsolenkommando tracert** (Windows) bzw. **traceroute** (Unix / Linux / Mac OS X) verfolgt den Weg durch das Netz zu einem Zielrechner und gibt die Zeiten aus. Damit ließe sich zum Beispiel feststellen, wo auf dem Wege zum Zielrechner besonders viel Zeit vergeht.

- Eine Zeitüberschreitung kann den Grund haben, daß eine Firewall ICMP Anfragen wie tracert, ping etc. blockiert!
- Weitere Informationen: <http://www.elektronik-kompendium.de/sites/net/0901041.htm>

DNS (Domain Name System) Service.

Da der Mensch sich IP Nummern als Adressen von Rechnern schlecht merken kann, benutzt man gerne Namen in der Form eines **FQDN (Full Qualified Domain Name)** für Hosts. Dafür werden im Internet / Intranet DNS Server mit Listen bereit gestellt, die den Namen FQDN in die IP Nummer und zurück übersetzen.

Aufbau Full Qualified Domain Name (FQDN).

Der Name eines Hosts setzt sich aus mehreren Teilen zusammen, die durch Punkte voneinander getrennt sind und deren Gesamtheit als **FQDN** bezeichnet wird. Nicht erlaubt in FQDN's sind Sonderzeichen mit Ausnahme des Bindestrichs (dh. auch Leerzeichen sind nicht erlaubt), erlaubt dagegen sind Buchstaben und Ziffern, wobei zwischen Groß- und Kleinbuchstaben nicht unterschieden wird.

Rechnername.[[Fourth-Level-Domain.]Third-Level-Domain.]Second-Level-Domain.TLD

TLD = Top-Level-Domain (First-Level-Domain)

Als **Beispiel** diene der Web Server der University of Texas in Austin, USA, mit dem FQDN
www1.cc.utexas.edu

- **Hostname:**

Dies ist der eigentliche Name des Rechners. Im Beispiel **www1**

- **3rd, 4th usw. Level Domain (falls verwendet, wahlfrei):**

Subdomains (bzw. auch Zonen genannt). Wird eine Domain in Subdomains unterteilt, folgt deren Bezeichnung. Im Beispiel **cc**

- **2nd Level Domain:**

Dies ist die Bezeichnung des Bereiches, in dem alle Hosts des Betreibers mit eventuellen Subdomains zusam-

mengefasst sind. Im Beispiel **utexas**

- **Top-Level-Domain - TLD oder 1st Level Domain:**

Diese Domain gehört einer übergeordneten Struktur an. Die Top-Level Domain wird nicht willkürlich bei Namensadressen vergeben, sie hat eine feste Bedeutung. Im Beispiel **edu**.

Top Level und 2nd Level Domain sind für Hosts im WAN nicht frei wählbar, sondern müssen registriert werden. Bei einigen TLD's wie zum Beispiel .uk unterliegen auch einige 3rd Level Domains der Registrierungspflicht. Die Registrierung erfolgt beim **NIC (Network Information Center)**.

Die Festlegung der TLD Bezeichnungen obliegt der **ICANN (Internet Corporation for Assigned Names and Numbers)**:

- <http://www.icann.org/tlds/>

Die **IP Nummern Pools** werden regional verwaltet, also auch nicht willkürlich vergeben:

AfriNIC für Afrika: <http://www.afrinic.net>

APNIC für Asien u. Pazifik: <http://www.apnic.net>

ARIN für Nord Amerika: <https://www.arin.net>

LACNIC für Latein Amerika und Karibik: <http://www.lacnic.net>

RIPE NCC für Europa, Nahost und Zentral Asien: <http://www.ripe.net>

Bei einer **TLD** wird unterschieden nach:

- **ccTLD - Country Code Top Level Domain**

TLD's mit zwei Buchstaben, die einem Staat zugeordnet sind (.eu für die Europäische Union gehört zu den Ländercodes).

Beispiel: <http://www.beuth-hochschule.de> (TLD .de für Deutschland).

- **gTLD - Generic Top Level Domain**

Generische TLD's ordnen den Hosts eine bestimmte begriffliche Bedeutung zu, die der Inhaber der Domain erfüllen muß.

Beispiel: <http://www.nuforc.org> (die TLD .org für Organisationen).

Eine vollständige **ccTLD und gTLD Liste** findet sich bei der **Internet Assigned Numbers Authority (IANA)**. Dort sind auch in der Datenbank die für die TLD's zuständigen **NIC's** verzeichnet:

- <http://www.iana.org/domains/root/db>

Kommando nslookup.

Dieses Kommando fragt den **DNS (Domain Name Server)** Server ab. Deshalb muß in der Netzwerkkonfiguration des eigenen Rechners die Adresse des DNS korrekt eingerichtet sein. Dies läßt sich mit dem **Konsolenkommando nslookup** (Windows, Unix, Linux, Mac OS X) überprüfen. Dabei kann entweder eine IP Nummer angegeben werden, um den FQDN des Rechners zu ermitteln oder der FQDN, um ihn in die IP Nummer aufzulösen.

```
> nslookup www.google.de
Server: fxns01.t-d1-wap.de
Address: 10.74.83.22

Nicht autorisierte Antwort:
Name: www.l.google.com
Addresses: 209.85.135.105, 209.85.135.106, 209.85.135.147, 209.85.135.99
          209.85.135.103, 209.85.135.104
Aliases: www.google.de, www.google.com
```

Der Antwort kann man entnehmen, daß der Rechner www.google.de in Wirklichkeit www.l.google.com heißt. Damit sich Menschen es einfacher merken können, gibt es die einfacheren Alias (Schein-) Bezeichnungen www.google.de und www.google.com. Der Rechner www.l.google.com ist aber gar kein einzelner Rechner, sondern es verbergen sich dahinter fünf einzelne Rechner: 209.85.135.105, 209.85.135.106, 209.85.135.147, 209.85.135.99, 209.85.135.103, 209.85.135.104, damit Suchanfragen möglichst schnell beantwortet werden können. Ankommende Verbindungen werden also auf einen der 5 Rechner weitergeleitet. Und wie heißt nun ein bestimmter Rechner, wie 209.85.135.105?

```
> nslookup 209.85.135.105
Server: dodmzns00.t-d1-wap.de
Address: 193.254.160.1

Name: mu-in-f105.1e100.net
Address: 209.85.135.105
```