Standards

Das Domain Name System bildet ein verteiltes Verzeichnis zur Umwandlung von Namen und Adressen.

Der Internet Standard 13 (DOMAIN) umfaßt

- **RFC1034** Domain Names - Concepts and Facilities
- **RFC1035** Domain Names - Implementation and Specification

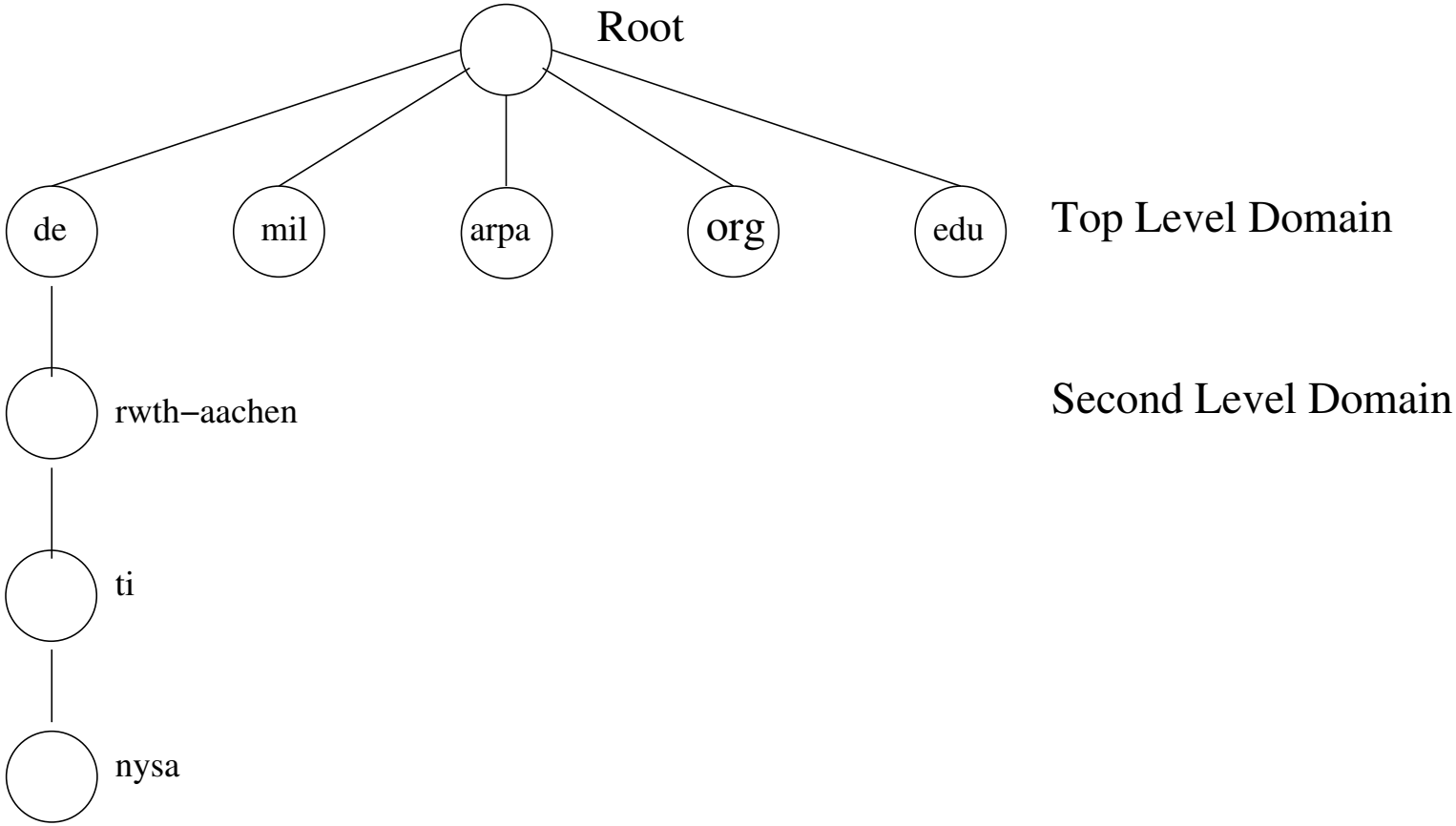
Eine Vielzahl von Erweiterungen finden sich in jüngeren RFCs (vgl. `http://www.dns.net/dnsrd/rfc/`) und sind zum Teil in aktuellen DNS Servern implementiert.

Syntax für Namen

Die dem DNS zugrunde liegende Datenbank hat einen hierarchischen Aufbau, der sich in den Namen widerspiegelt:

- Namen bestehen aus Folgen von Bezeichnern (Label), die maximal 63 Zeichen lang sind.
- Die Bezeichner werden durch einen Punkt (’.’) voneinander getrennt.
- Zwischen Groß- oder Kleinschreibung wird nicht unterschieden.
- RFC1035 empfiehlt für Label, mit einem Buchstaben (a-z oder A-Z) zu beginnen, dann Buchstaben, Ziffern oder ’-’ und nicht mit einem ’-’ zu enden.
- Namen, die mit einem Punkt (’.’) enden, werden als vollständig angenommen, andernfalls ist eine Erweiterung nötig, um zum **Fully Qualified Domain Name, FQDN** zu kommen.

Verzeichnisaufbau



Verzeichnisaufbau

Namen werden in umgekehrter Reihenfolge des Labels geschrieben, d.h. die Top Level Domain (TLD) zuletzt.

Beispiele:

- **nysa** oder **RWTH-Aachen**: Bezeichner gemäß RFC1035
- **nysa.ti.rwth-aachen.de.**: FQDN
- **nysa.ti**: Unvollständiger Name
- **182.35.130.134.in-addr.arpa.**: FQDN

Top Level Domains

- **Country Coded TLD**: ISO 3166 Ländercode, Administrativer Kontakt unter `http://www.iana.org/root-whois/index.html`
- **Generic TLD**: Namen, die einer bestimmten Organisation/Verwendung zugeordnet sind, z.B. `.com`, `.edu`, Administrativer Kontakt unter `http://www.iana.org/gtld/gtld.html`
- **Infrastucture TLD**: TLD für Namen, die aus technischen Gründen benutzt werden, `.arpa` erzeugt eine separaten Baum, `.root` wird nur als Marker der Rootzone verwendet.

```
$host -t TXT \
  vrsn-end-of-zone-marker-dummy-record.root
```

DNS Zonen

- Zonen sind separat administrierbare Unterbäume des Verzeichnisses
- Der Administrator einer Zone ist dafür verantwortlich, DNS Server für diese Zone bereitzustellen
- Der Administrator einer Zone kann die Verwaltung von Unterbäumen an andere Administratoren delegieren.
- Primary DNS Server einer Zone ist der (ggfs. redundant aufgebaute) Server, auf dem die Konfigurationsdaten der Zone administriert werden.
- Eine Zone kann weitere Secondary DNS Server haben, die die Konfigurationsdaten vom Primary DNS Server herunterladen (sog. Zone Transfer).
- Ein DNS Server ist Authoritative, wenn er eine aktuelle Kopie der Zone hat.

DNS Rahmen

Identification	Flags
Number of Questions	Number of RRs
Number of Authority RRs	Number of Additional RRs
Questions	
Answer RRs	
Authority RRs	
Additional RRs	

Felder im DNS Rahmen

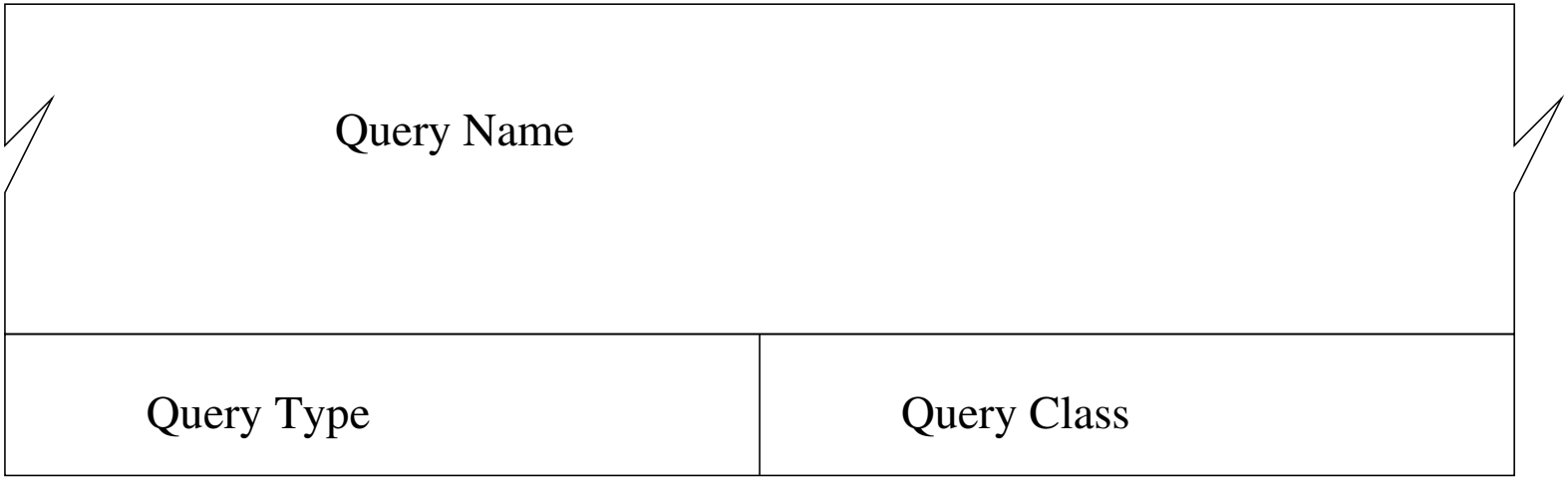
- **Identification**: 16 Bit Code, mit dem die Antwort einem Request zugeordnet werden kann.
- **Flags**: 16 Bit, beschreibt Art der Antwort, Fehlerstatus, ...
- **Number of Questions**: 1 für DNS Anfragen, 0 für Antworten
- **Number of RRs**: Anzahl Resource Records (Antworten auf eine Anfrage)
- **Number of Authority RRs**: Anzahl Authority Records (DNS Server, die die gesuchte Information sicher haben)
- **Number of Additional RRs**: Anzahl Additional Records (Zusatzinformation, z.B. die Adressen der DNS Server aus den Authority Records)

Flags

QR	opcode	AA	TC	RD	RA	empty (0)	RCode

- **QR**: 0: Anfrage, 1: Antwort
- **opcode**: 0: Default, 1: Inverse Abfrage, 2: Server Status
- **AA**: Antwort ist “authoritative”
- **TC**: (Truncated) Paket enthält nur 512 Bytes der Antwort
- **RD**: 1: Server soll Anfrage rekursiv bearbeiten
- **RA**: 1: Server bietet Rekursion an
- **RCode**: Fehlerstatus, 0: Kein Fehler, 3: Name nicht gefunden

Question Datensatz



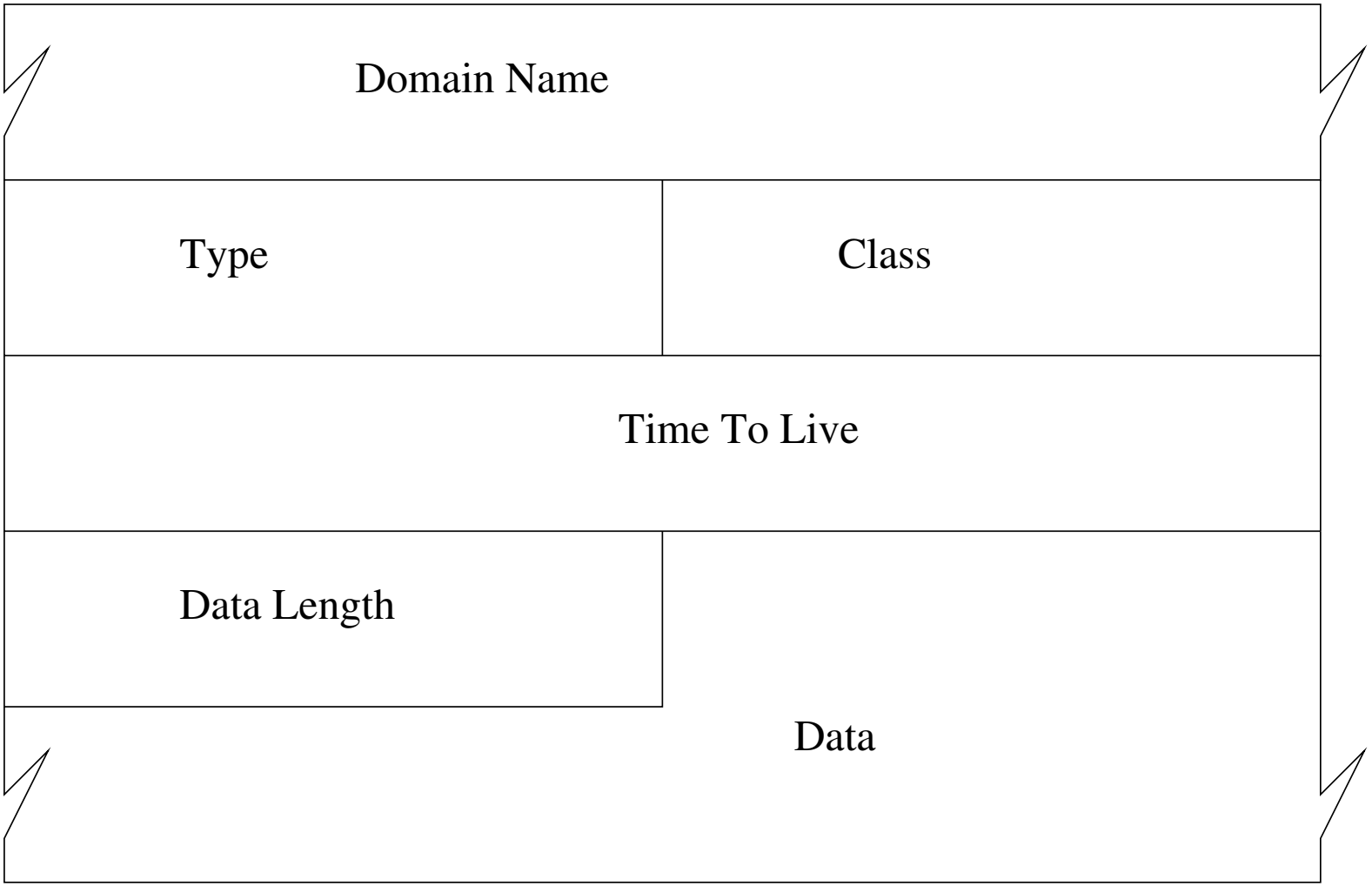
- **Query Name**: Name, der abgefragt wird
- **Query Type**: Typ der Anfrage, entweder Standardtyp oder
  - **ANY**: Jeder Standardtyp
  - **AXFR**: Zonentransfer
- **Query Class**: 1 für Internet (IN)

Standardtypen

Hier ist eine Auswahl der gebräuchlichsten Datensätze

Typ	Wert	Name
A	1	IPv4 Adresse
NS	2	Name Server Name
CNAME	5	Canonical Name (Alias)
SOA	6	Start of Authority, Administrative Daten einer Dom
PTR	12	Pointer Record (Verweis)
HINFO	13	Host Info (Informationen über den Rechner)
MX	15	Mail Exchange (Zuständiger E-Mailserver)
AAAA	28	IPv6 Adresse (RFC1933)
SRV	32	Server Record (Host:Port des Servers)
NAPTR	35	Naming Authority Pointer (RFC2915)

Resource Records



Felder eines Resource Records

- **Domain Name**: Name, zu dem die Daten gehören
- **Type**: Standardtyp der Daten
- **Class**: 1 für IN
- **Time To Live**: Zeit in Sekunden, die der Eintrag von einem DNS Server oder Client aus dem Cache verwendet werden darf.
- **Data Length** Länge in Byte der folgenden Daten
- **Data**: Daten und Kodierung abhängig vom Typ.

Transport

- Üblicherweise werden DNS Anfragen per UDP gestellt
- Zeitüberschreitungen und Wiederholungen werden von den Clients gesteuert.
- Zonentransfers finden über TCP statt (aber nur zu den Secondary DNS Servern)
- DNS Server binden sich üblicherweise auf Port 53
- Der Quellport bei Anfragen ist beliebig.
- Sind mehr als 512 Byte zu übertragen, muß der Client via TCP erneut nachfragen (TC Flags ist in der Antwort gesetzt).

Beispiel

Abfrage eines SRV Records (TTL und Query Class):

```
$ dig -t SRV _xmpp-client._tcp.jabber.org
;; QUESTION SECTION:
;_xmpp-client._tcp.jabber.org.   SRV
;; ANSWER SECTION:
_xmpp-client._tcp.jabber.org.    SRV  5222 jabber.org.
;; AUTHORITY SECTION:
jabber.org.                       NS   ns2.jeremie.com.
jabber.org.                       NS   ns1.jeremie.com.
;; ADDITIONAL SECTION:
jabber.org.                        A   208.245.212.98
ns1.jeremie.com.                   A   208.245.212.29
```

Auflösung von Namen

- Ein Host stellt die Anfrage bei den (bis zu 3) konfigurierten Nameservern (RD ist üblicherweise 1)
- Hat ein DNS Server die Antwort im Cache, sendet er die zugehörigen Daten
- Kann er die Anfrage nicht lokal beantworten, fragt er (nicht rekursiv) einen der konfigurierten ROOT Server.
- Antwort ist eine Liste der Authoritative DNS Server der zugehörigen Zone in den Authority RRs.
- Eine Anfrage bei einem dieser DNS Server führt entweder zum Ergebnis, oder zu einer weiteren Liste von DNS Servern einer untergeordneten Zone.
- Dies wird fortgesetzt, bis ein Server die Anfrage beantworten kann.

Beispiel mit Rekursion

```
$ dig www.heise.de
;; QUESTION SECTION:
;www.heise.de.                  IN   A
;; ANSWER SECTION:
www.heise.de.           74272   IN   A   193.99.144.85
;; AUTHORITY SECTION:
heise.de.               74272   IN   NS  ns.pop-hannover.d
heise.de.               74272   IN   NS  ns.heise.de.
heise.de.               74272   IN   NS  ns2.pop-hannover.
;; ADDITIONAL SECTION:
ns.pop-hannover.de.     10562   IN   A   193.98.1.200
ns2.pop-hannover.net.   75522   IN   A   62.48.67.66
ns.heise.de.            85574   IN   A   193.99.145.37
```

Beispiel ohne Rekursion

```
$ dig +norec www.heise.de @198.41.0.4
;; QUESTION SECTION:
;www.heise.de.                  IN    A
;; AUTHORITY SECTION:
de.                   172800   IN    NS    Z.NIC.de.
de.                   172800   IN    NS    A.NIC.de.
de.                   172800   IN    NS    C.DE.NET.
;; ADDITIONAL SECTION:
A.NIC.de.             172800   IN    A     194.0.0.53
C.DE.NET.             172800   IN    A     208.48.81.43
Z.NIC.de.             172800   IN    A     194.246.96.1
Z.NIC.de.             172800   IN    AAAA  2001:628:453:4905::53
```

Beispiel ohne Rekursion (2)

```
$ dig +norec www.heise.de @194.246.96.1
;; QUESTION SECTION:
;www.heise.de.                  IN   A
;; AUTHORITY SECTION:
heise.de.               86400   IN   NS   ns.heise.de.
heise.de.               86400   IN   NS   ns.pop-hannover.de.
heise.de.               86400   IN   NS   ns2.pop-hannover.ne
;; ADDITIONAL SECTION:
ns.heise.de.            86400   IN   A    193.99.145.37
ns.pop-hannover.de.     86400   IN   A    193.98.1.200
```

Beispiel ohne Rekursion (3)

```
$ dig +norec www.heise.de @193.99.145.37
;; QUESTION SECTION:
;www.heise.de.          IN   A
;; QUESTION SECTION:
;www.heise.de.  IN      A
;; ANSWER SECTION:
www.heise.de.   86400  IN   A   193.99.144.85
;; AUTHORITY SECTION:
heise.de.       86400  IN  NS   ns.pop-hannover.de.
heise.de.       86400  IN  NS   ns2.pop-hannover.net.
heise.de.       86400  IN  NS   ns.heise.de.
;; ADDITIONAL SECTION:
ns.heise.de.    86400  IN   A   193.99.145.37
```

Reverse Lookup

- IP Adressen in Dotted Notation bilden Namen im DNS Verzeichnis
- Die TLD ist arpa, die Second Level Domain ist in-addr.
- Eine IP Adresse a.b.c.d wird in der Zone administriert als **d.c.b.a.in-addr.arpa**
- Der Typ eines in-addr.arpa Eintrages ist PTR, der Wert ist der FQDN des Hosts mit der entsprechenden Adresse.
- Die Auflösung des Namens **d.c.b.a.in-addr.arpa** erfolgt wie für alle FQDN

Beispiel

Der Host `www.heise.de` hat die IP Adresse `193.99.144.85`

```
$ dig -t PTR 85.144.99.193.in-addr.arpa
;; QUESTION SECTION:
;85.144.99.193.in-addr.arpa.          PTR
;; ANSWER SECTION:
85.144.99.193.in-addr.arpa.   PTR   www.heise.de.
;; AUTHORITY SECTION:
144.99.193.in-addr.arpa.      NS    ns.s.plusline.de.
144.99.193.in-addr.arpa.      NS    ns.heise.de.
144.99.193.in-addr.arpa.      NS    ns.plusline.de.
;; ADDITIONAL SECTION:
ns.heise.de.                  A     193.99.145.37
ns.s.plusline.de.             A     212.19.40.14
ns.plusline.de.               A     212.19.48.14
```

Reverse Lookups und CIDR

- Die Segmente eines FQDN geben die Ebenen der Administrativen Kontrolle an.
- Dieser Mechanismus funktioniert nicht beim Reverse Lookup, wenn Netze eine Netzmaske haben, die nicht auf einer Bytegrenze endet.
- RFC2317 beschreibt eine mögliche Konfiguration des Parent DNS Servers, der die Kontrolle an untergeordnete Server weiterleitet.
- Einige DNS Server haben eigene Lösungen, die Delegation zu implementieren (z.B. BIND9 $GENERATE).

Beispiel

Unterhalb der Domain `test.net` mit Adressbereich `1.2.3.0/24` wird eine Domain `sub.test.net` mit Adressen `1.2.3.128/25` angelegt.
Auszug aus dem Zonenfile der `test.net` Domain (RFC1035):

```
$ORIGIN test.net
@     NS      ns.test.net.
ns    A       1.2.3.1
sub   NS      ns.sub.test.net.
```

```
$ORIGIN 3.2.1.in-addr.arpa
1     PTR     ns.test.net.
128   CNAME   128.3.2.1.sub.test.net.
129   CNAME   129.3.2.1.sub.test.net.
```

Beispiel Fortsetzung

Das Zonenfile der `sub.test.net` Domain:

```
$ORIGIN sub.test.net
@       NS    ns.sub.test.net.
ns      A     1.2.3.129
host2   A     1.2.3.130
129     PTR   ns
130     PTR   host2
```

DNS Load Balancing

- Server können nur eine begrenzte Anzahl paraleller Verbindungen bedienen.
- Viele Dienste erfordern/erlauben, daß Verbindungen lange geöffnet bleiben (z.B. IMAP IDLE, vgl. RFC2177).

Die Lösung besteht darin, auf den Clients den Namen (nicht die IP) des Servers zu konfigurieren. Bei jedem Verbindungsaufbau wird der Name in eine Adresse umgewandelt, wobei die TTL des Eintrages beachtet wird. Dadurch kann der Administrator später weitere Server hinzuschalten.

Beispiel: Round Robin DNS

```
$ host www.google.de
 www.google.de      CNAME  www.google.com
 !!! www.google.de CNAME record has zero ttl
 www.google.com     CNAME  www.l.google.com
 !!! www.google.com CNAME record has zero ttl
 www.l.google.com     A    209.85.135.104
 www.l.google.com     A    209.85.135.147
 www.l.google.com     A    209.85.135.99
 www.l.google.com     A    209.85.135.103
```

Bei weiteren Anfragen ist die Reihenfolge der Resource Record möglicherweise anders.