DNS - Geschichte

1982 wird erstmals den Vorschlag für ein hierarchisches System gemacht. Der RFC schlägt auch schon Nameserver und ein System zur Adressauflösung vor.

Dieser Dienst erlaubte bereits die Auflösung von Name zu Adresse und umgekehrt.

Ein Jahr später (1983) erscheint dann das DNS mit Protokoll und Recordtypen in der heute bekannten Form.

Hostname und vollständige Domain bilden den Fully Qualified Domain Name (FQDN). Die FQDN-Länge ist auf 255 Byte limitiert. Die einzelnen Komponenten der Domain dürfen 63 Byte nicht überschreiten.

Erlaubte Zeichen der Domain sind:

- A-Z in Gross und Kleinbuchstaben
- Zahlen
- Bindestrich
- Punkte dienen der Trennung zwischen Domainkomponenten
- Eine Komponente sollte nicht mit einer Zahl beginnen

DNS - Geschichte

TSBE Bern
Höhere Fachschule

DNS - so funktioniert's
- Im gesamten System spielen viele einzelne »Domain Name Server« mit
- Sie sind hierarchisch angeordnet und arbeiten zusammen.
- Kennt ein Server den Namen oder die IP-Adresse nicht, kontaktiert er übergeordnete Server

Praktischerweise verfügt jeder Name-Server über einen Cache, welcher die Auskünfte eine Zeit lang zwischenspeichert

Neben den Informationen zu den Domains selbst muss es Programme geben, welche diese abrufen und auswerten können (so genannte Resolver).

Das lokales Adressbuch - die Datei »**/etc/hosts**«

Zuständig ist auf Linux-Systemen die Datei /etc/hosts - in dieser stehen die IP-Adressen und Rechnernamen der einzelnen Systeme. Eine typische hosts-Datei eines übersichtlichen LANs könnte beispielsweise so aussehen:

```
127.0.0.1 localhost
192.168.2.15 asteroid.hane.org asteroid
```

TSBE Bern
Höhere Fachschule

DNS - Hierarchische Struktur

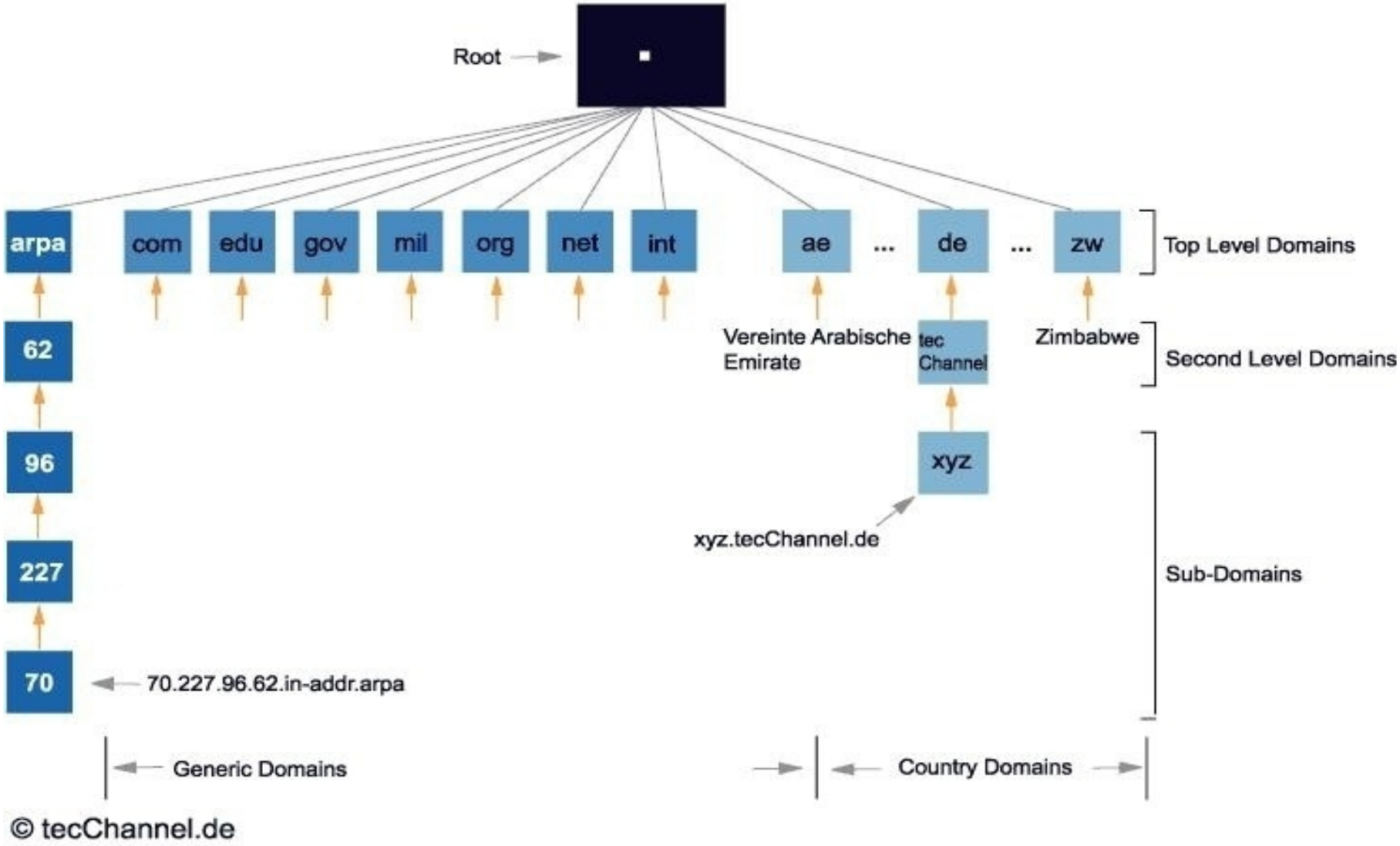
Als verteiltes, hierarchisches System zur Konvertierung von Rechnernamen in IP -Adressen, kennt es keine zentrale Datenbank mit der gesamten Information über die Rechner im Internet.

Die DNS-Datenbank weist eine in Zonen aufgeteilte baumförmige Struktur auf, die Wurzel entspricht dabei dem Root-Verzeichnis.

Direkt unterhalb der Root-Domain befinden sich die Top Level Domains (TLDs). TLDs werden von der ICANN (Internet Corporation for Assigned Names and Numbers) in zwei Hauptgruppen und einen Sonderfall unterteilt:

allgemeine TLDs: generic TLDs (gTLDs)
länderspezifische TLDs: country-code TLDs oder ccTLDs
die Infrastruktur-TLD (iTLD): . arpa

DNS - Hierarchische Struktur



DNS

Die Root-Domain wird als ein einziger Punkt geschrieben und wird in der Regel weggelassen.

Die Vergabe von Domainnamen ist auf zahlreiche Firmen und Institutionen verteilt. Den Ländern selbst überlassen wird die Verwaltung geographischer Top Level Domains.

Ein Antrag für eine Domain muss die Adresse von mindestens zwei Nameservern (Primary/Secondary), enthalten.

Der Primary-Name-Server und die Secondary-Name-Server müssen dabei voneinander unabhängig und redundant ausgelegt sein.

Der Unterschied zwischen den beiden Servern besteht darin, dass der Secondary Name Server alle relevanten Daten vom Primary Name Server bezieht.

DNS

Resolver

Als Resolver bezeichnet man Programme, welche die Informationen zu den Adressbucheinträgen einholen, sie erfüllen also die Funktion einer Vermittlungsstelle zwischen den jeweiligen Anwendungen und dem Name-Server. Der Resolver kann bei seinen Nachforschungen im Wesentlichen zwei Wege beschreiten:

Rekursive Anfrage: Der Resolver sendet seine Frage an einen ihm bekannten Name-Server und erwartet eine eindeutige Antwort von ihm. Dieser meldet sich entweder mit der gewünschten Information zurück oder meldet, dass es keinen passenden Eintrag gibt.

Iterative Anfrage: Der Resolver erhält als Antwort die gesuchte Information oder als Empfehlung die Adresse eines weiteren Name-Servers, den er als Nächstes fragt. Auf diese Weise hangelt sich der Resolver von Name-Server zu Name-Server, bis er die eindeutige Antwort erhält. Domainnamen schreibt man von der untersten Ebene, dem Rechnernamen, zur obersten Ebene, der Top Level Domain.

.

DNS

Nameserver

Ein Name-Server übernimmt die Verantwortung für eine oder mehrere so genannte Zonen, d.h. seine Informationen können als verbindlich, also autoritativ, angesehen werden.

Ganz am oberen Ende stehen so genannte Root Server, welche die volle Autorität besitzen. Diese verteilen als Chef des ganzen Systems allerdings immer nur Informationen zu Anfragen der Art »wer ist für .ch autoritativ?«.

Neben den autoritativen Name-Servern gibt es auch noch solche, welche ihre Informationen zu den Zonen aus **zweiter** oder **dritter** Hand beziehen; diese Server nennt man entsprechend nicht-autoritativ.

DNS

Zonen

Die Zone ist die Datenbank, die den „Teilbaum des Domainraumes" - die Subdomain - beschreibt.

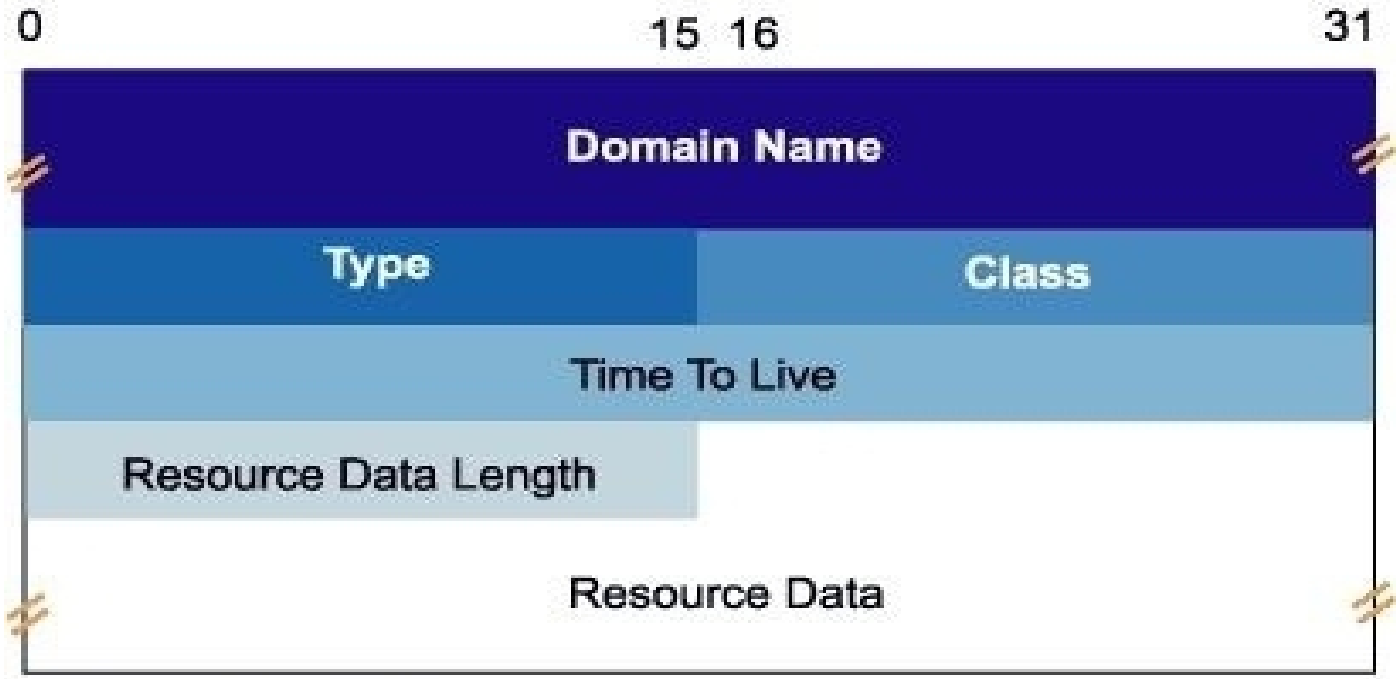
Diese Datenbank liegt auf einem Nameserver. Die Zone ist dabei der Teil, für den der Nameserver zuständig ist.

Eine Zone enthält alle für eine Subdomain relevanten Informationen.

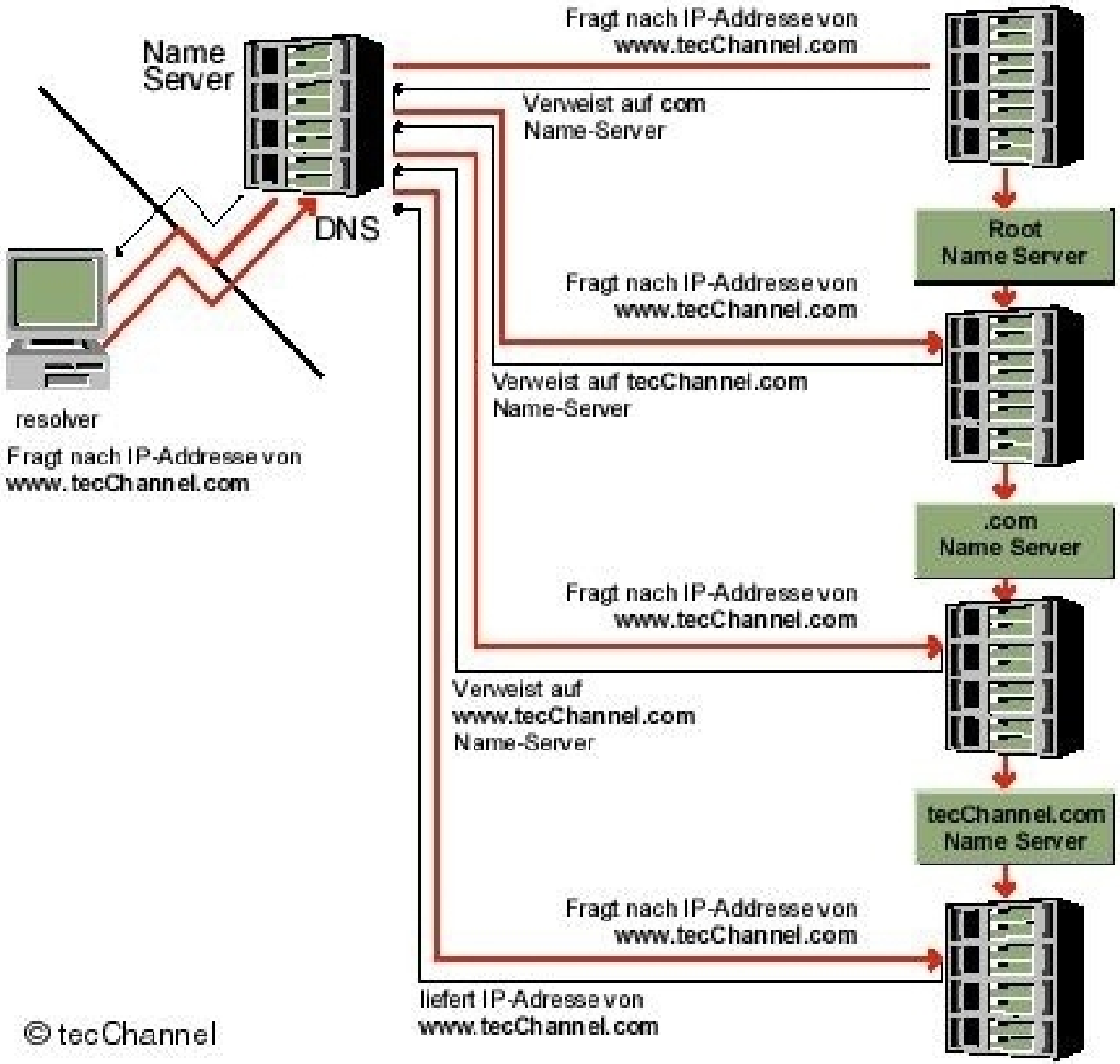
Diese Informationen werden als sogenannte **Resource Records (RR)** hinterlegt. Es gibt über 30 verschiedene RRs, die im Laufe der Zeit entwickelt wurden. Wirklich gebräuchlich sind aber nur wenige.

Es muss nicht zwangsläufig der ganze darunter liegende Teilbaum sein. Tiefer in der Hierarchie liegende Teile können durchaus an andere Server weiter delegiert werden.

DNS



DNS Rekursive Anfrage



DNS

Start of Authority

Im Start of Authority (SOA) Record stehen Verwaltungsinformationen über die Zone, aus denen Timingwerte für die Gültigkeit der Eintäge und zuständige Server und Ansprechpartner und Server und Ansprechpartner hervorgehen. In einer Zonedatei sollte der SOA-Record am Anfang stehen.

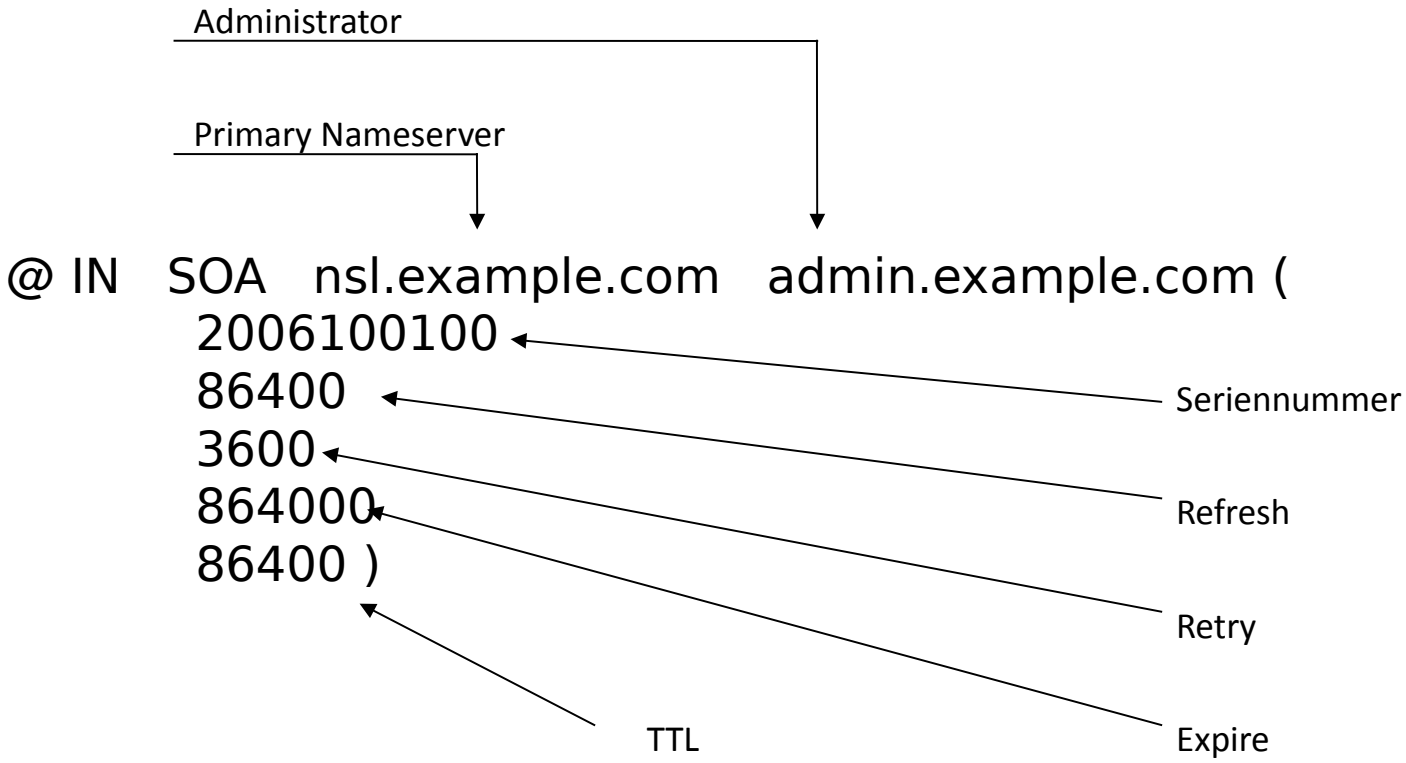
Ein Beispiel für einen SOA-Record in einem Zone-File ist:

```
$TTL 12h
#SOA Resource Record:
@     IN     SOA     ns1.example.net. admin.example.net. (
                        1 ; serial
                        12h ; refresh
                        1h ; retry
                        10d ; expire
                        1h ; minimum (negTTL)
                         )
```

Das @-Zeichen ist in Zonefiles der Platzhalter für die aktuell beschriebene Zone.

DNS

Start of Authority



DNS

Start of Authority

REFRESH
10000-86400 Sekunden, also von ca. 2,75 Stunden bis zu einem Tag.

RETRY
1800-28800 Sekunden, also von einer halben Stunde bis zu acht Stunden

EXPIRE
604800-3600000 Sekunden, also von einer Woche bis zu 41 Tagen und 16 Stunden

TTL
180-345600 Sekunden, entspricht 3 Minuten bis zu 4 Tagen