Albert-Ludwigs-Universität Freiburg
Institut für Informatik

WS 2007/08

Seminararbeit

Domain Name System
DNS

Johannes Garimort

5. Februar 2008

Betreut durch Prof. Dr. Christian Schindelhauer

Abstract

Mit dem Siegeszug des Internet Protocol (IP) ist es unumgänglich geworden andere Teilnehmer in Netzwerken über die bekannten 32[1]- oder 128-stelligen Binärzahlen zu adressieren. So sinnvoll und praktisch die Verwendung von IP-Adressen für die Adressierung von Maschinen in Netzwerken auch sein mag, so hat sie doch einen entscheidenden Nachteil: für den Menschen ist diese Darstellungsform nicht geeignet, da er Namen bevorzugt, die leicht auszusprechen und zu merken sind.
Im der folgenden Arbeit wird das Domain Name System beschrieben, das eine solche geforderte effiziente Abbildung von IP-Adressen in abstrakte vom Menschen erfassbare Namen realisiert.

[1] Die Arbeit bezieht sich im Folgenden auf das im europäischen Raum verbreitete IPv4.

Inhaltsverzeichnis

1 Einleitung

In den Anfängen des Internets konnten die Namen für die teilnehmenden Maschinen aufgrund der geringen Teilnehmerzahlen noch relativ frei gewählt werden. 1986 waren nur 3100 offiziell registrierte Hosts und 6500 Aliasse gemeldet[2] - die meisten Teilnehmer waren nicht gemeldet, da dies wegen der geringen Teilnehmerzahlen in Netzwerken nicht erforderlich war. Die Namen wurden verwendet, um die Maschinen direkt zu identifizieren. Ihre Vergabe wurde vom Network Information Center (NIC) verwaltet[2]. Mit der schnell anwachsenden Zahl an Internetnutzern stieß dieses Verfahren jedoch bald an seine administrativen und technischen Grenzen.
1983 schon schlug Mockapetris in den RFCs 882 und 883 eine hierarchische Struktur zur Verwaltung des Namensraum im Internet vor: das Domain Name System (DNS), das 1987 in den RFCs 1038 und 1039 erweitert wurde und bis heute zur Namensauflösung im Internet[3] verwendet wird.

2 Das Domain Name System

Das Domain Name System besteht aus drei Hauptkomponenten, die im Folgenden näher erläutert werden.

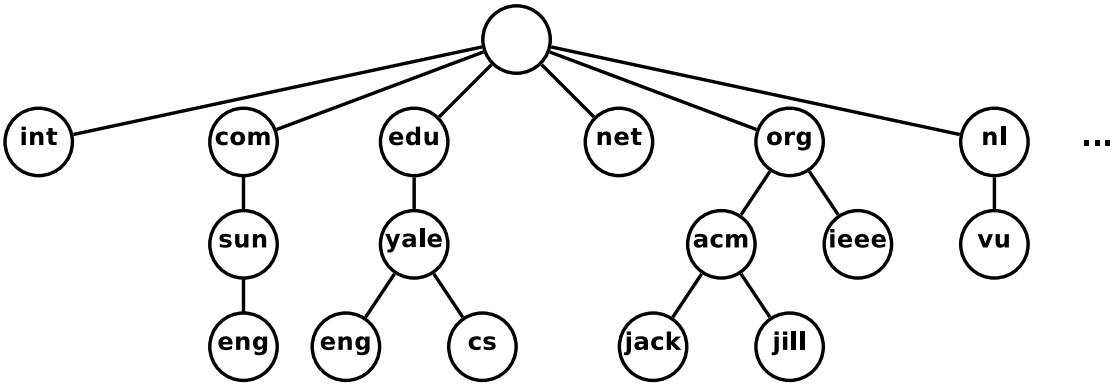

Abbildung 1: Modell des Domain Namensraum

[2] [1], Seite 420.
[3] DNS lässt sich natürlich auch in lokalen Netzen betreiben und funktioniert im Prinzip wie das Internet-DNS, weshalb hier nicht näher auf lokale DNS eingegangen wird.

2.1 Domain Namensraum

Der Domain Namensraum[4] ist ein weitverzweigter, hierarchischer Wurzelbaum. Blätter und Knoten werden als Labels bezeichnet und bestehen aus Zeichenketten von maximal 63 Zeichen. Jeder Pfad des Baumes entspricht einer Domain[5]. Diese haben eine maximale Länge von 255 Zeichen und bestehen aus einer Kombination von Labels.
Die Domain *a.example.com* besteht also aus den Labels *a*, *example*, und *com*. Aufgelöst wird sie von rechts nach links. *com* gehört damit zur obersten Ebene des Baumes und wird auch als *Top-Level Domain* bezeichnet.

Domain Name	Meaning
aero	Air transport industry
arpa	Infrastructure domain
biz	Businesses
com	Commercial associations
edu	Educational government
gov	United States government
info	Information
int	Internation treaty organizations
mil	United States military
museum	Museums
name	Individuals
net	Major network support centers
org	Organizations other than those above
pro	Credentialed professionals
country code	Each country (geographic scheme)

Tabelle 1: Top-Level Internet Domänen erlauben geographische wie auch organisatorische Hierarchisierung. [1], Seite 424.

2.2 Name Server

Name Server sind Programme, die auf Computersystemen arbeiten. Die Name Server bilden das Rückgrat des Domain Namensraumes: Sie speichern Informationen über bestimmte Teile des Namensraumes in - Resource Records genannte - Datensätzen. Anfragen zum Namensraum werden von ihnen bearbeitet oder an andere Name Server zur Bearbeitung weitergeleitet (delegiert). Jeder Name Server kennt mindestens einen weiteren[6] ihm übergeordneten Name Server.

[4] Vgl. Abbildung 1
[5] Domäne
[6] Die Root-Server, die die Wurzel im Namensraum repräsentieren, nicht.

Man unterscheidet zwischen *autoritativen* und *nicht-autoritativen* Name Servern einer Zone im Domain Namensraum. Autoritative Name Server sind verantwortlich für diese Zone, während nicht-autoritative Name Server keine Informationen über diese Zone gespeichert haben, d.h. Anfragen bezüglich der Zone können von ihnen nicht direkt aufgelöst werden.
Als *Zone* bezeichnet man die Teile des Namensraums, die durch gleiche Name Server repräsentiert werden. Sie wird durch die sogenannte Zonendatei definiert, in der alle Resource Records vorliegen. Für jede Zone existiert mindestens ein autoritativer Name Server, der *Primary Name Server*. Weitere Name Server, die aus Gründen der Lastenverteilung mit dem Primary Name Server als Server-Cluster angelegt werden, bezeichnet man als *Secondary Name Server*. Die Zonendatei wird zwischen den Servern per Zonentransfer synchronisiert.

2.3 Resolver

Der Resolver ist die Schnittstelle zwischen den Name Server und Anwendungen. Resolver sind einfach aufgebaute Softwaremodule, die Informationen über *iterative* oder *rekursive* Anfragen von den Domain Servern abrufen.
Programme auf lokalen Rechnern stellen Anfragen an den Resolver um bestimmte Domain Namen aufzulösen. Auch Name Server können die Rolle des Resolvers einnehmen, zum Beispiel bei der rekursiven Auflösung von Anfragen.

3 Datenformate des DNS

3.1 Resource Records

Resource Records (RR) sind die Datensätze des DNS. Alle RRs sind vom selben Format[7]:

```
<NAME> <TYPE> [<CLASS>] [<TTL>] <RDLENGTH> <RDATA>
```

NAME gibt den Domainnamen an, zu dem der RR gehört. *TYPE* bestimmt den RR-Typ. Eine Auswahl an wichtiger Typen ist in der folgenden Tabelle aufgeführt. *RDLENGTH* gibt die Länge des *RDATA*-Feldes an, das abhängig von *TYPE* und *CLASS* RR-spezifische Daten enthält. *CLASS* und *TTL* sind optional. *CLASS* speichert die Zugehörigkeit des RR zum Internet (*IN*). Die anderen Einstellungsmöglichkeiten[8] werden

[7] Format [2] entnommen.
[8] Z.B. *CH* für Chaosnet.

kaum genutzt und können daher vernachlässigt werden. Die *TTL* gibt die Gültigkeitsdauer des RR an.

Typ	Bedeutung	Inhalt (gespeichert in *RDATA*)
A	IPv4 Host Address	32-bit IP-Adresse
NS	Name Server	Name des autoritativen Servers der Domain
SOA	Start of Authority	Bestandteil der Zonendatei; enthält Angaben zur Verwaltung und Zonentransfer
CNAME	Canonical Name	Alias zu einem vorhandenen DNS-Namen
MX	Mail Exchanger	Mailserver der Domain
PTR	Pointer	Domain Name Pointer (vergleichbar mit symbolischem Link)
TXT	Text	frei definierbarer Text
AAAA	IPv6 Host Address	128-bit IP-Adresse

Tabelle 2: Resource Record Typen

3.2 DNS Nachricht

Die Kommunikation zwischen Resolver und Domainserver bzw. unter den Domainservern selbst, läuft über das DNS Message Format. Unterstützt werden TCP und UDP[9] auf Port 53. Eine DNS Nachricht besteht aus einem Header (96 bit) und den Feldern Question, Answer, Authority und Addition Information, deren Länge jeweils im Header angegeben ist.

```
+--------------------+
|        Header      |
+--------------------+
|       Question     | the question for the name server
+--------------------+
|        Answer      | RRs answering the question
+--------------------+
|      Authority     | RRs pointing toward an authority
+--------------------+
|      Additional    | RRs holding additional information
+--------------------+
```

Abbildung 2: Format der DNS Nachricht. [3], Seite 24

[9] Standard

3.2.1 Header Format

Der Header enthält folgende Felder:

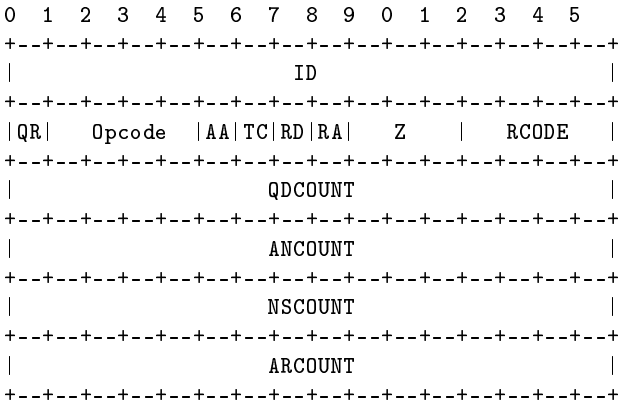

Abbildung 3: [3], Seite 25

Die Felder und ihre Bedeutung sind in Tabelle 3 zu finden. Die wichtigsten sind folgende:

QR Nachricht ist eine Anfrage (0) oder eine Antwort (1) ist
AA Sender ist autoritativ, d.h. Korrektheit der Antwort ist gesichert (1)
RD Resolver wünscht rekursive Bearbeitung (1)
RA rekursive Anfragen werden unterstützt (1)

3.2.2 Query

Pro Anfrage lassen sich mehrere Fragen[10] in eine DNS-Message packen - die Anzahl wird im Header festgelegt. Ein Query beinhaltet den gesuchten Domainnamen (*Query Domain Name*), die Angaben zur gewünschten Rückgabe (*Query Type* (16bit)) und die Klasse der Anfrage (*Query Class* (16bit) - im Normalfall *IN*)

[10] Query

Bit of PARAMETER field	Meaning
0	Operation: 0 Query 1 Response
1-4	Query Type: 0 Standard 1 Inverse 2 Server status request 4 Notify 5 Update
5	Set if answer authoritative
6	Set if message truncated
7	Set if recursion desired
8	Set if recursion available
9	Set if Data is authenticated
10	Set if checking is disabled
11	Reserved
12-15	Response Type 0 No error 1 Format error in query 2 Server failure 3 Name does not exist 5 Refused 6 Name exists when it should not 7 RR set exsist 8 RR set that should exist does not 9 Server not authoritative for the zone 10 Name not contained in zone

Tabelle 3: [1], Seite 433

3.2.3 Reply

In jeder Antwortnachricht[11] eines Name Servers ist im *Question*-Feld die gestellte Anfrage zu finden.

- *Answer Section* enthält - soweit möglich - die RRs, die die gestellte Anfrage beantworten.
- *Authority Section* enthält RRs anderer autoritativer Name Server oder in Spezialfällen die SOA RR des autoritativen Servers.

[11] Reply

- *Additional Section* enthält RRs, die für die RRs der anderen Felder nützlich sein könnten.

4 Funktionen des DNS

4.1 Namensauflösung

Es bietet sich an die Namensauflösung des DNS aus zwei verschiedenen Blickwinkeln zu betrachten: Zum einen wäre da die Arbeitsweise des Resolvers und zum anderen die des Name Servers. Ein Resolver, der eine Anfrage an einen DNS Server stellt oder eine Antwort auf eine Anfrage erhält, befindet sich dabei nie auf demselben Rechnersystem wie der Name Server. Allerdings ist es oft so, dass Name Server bei der Bearbeitung von Anfragen die Rolle des Resolvers einnehmen.
Vereinfachend lässt sich die Namensauflösung folgendermaßen beschreiben:

- Resolver schickt ein Query und fordert die Namensauflösung an.
- Ist der Name Server im Bezug auf die Anfrage autoritativ, so holt er die entsprechenden Daten aus seiner Zonendatei und schickt sie zurück.
- Ist der Name Server nicht-autoritativ gibt es zwei Arten der Auflösung:
  - Bei der rekursiven Namensauflösung[12] wird der Domain Server selbst zum Resolver und schickt Anfragen an Server, die ihm möglicherweise weiterhelfen könnten.
  - Bei der iterativen Namensauflösung sendet der Name Server lediglich Adressen zurück, die dem Resolver bei der weiteren Auflösung nützlich sein könnten. Der Resolver hangelt sich quasi von Name Server zu Name Server zur gesuchten Ressource.

Generell hat ein nicht-autoritativer Name Server folgende Möglichkeiten einen Namen aufzulösen:

- Er deligiert die Anfrage an einen Name Server einer Subdomain.
- Er greift auf gespeicherte Informationen zurück.[13]
- Er löst die Anfrage über den Root-Server auf.[14]

[12] Sofern diese unterstützt und vom Resolver gefordert wird. Siehe Tabelle 3
[13] Siehe Caching.
[14] Root-Server beantworten Anfragen ausschließlich iterativ, da sie sonst mit der Menge an Anfragen überlastet wären.

4.2 Caching

Der Rückgriff auf bereits genutzte oder abgerufene, temporär gespeicherte Daten beschreibt den Begriff des Cachings. Genau wie in anderen Bereichen von Computersystemen, in denen es um eine schnelle Bereitstellung von Daten geht, wird Caching beim DNS genutzt, um wiederholte Anfragen zu ähnlichen oder gleichen Ressourcen zu vermeiden. Nicht-autoritative Name Server können Domain-Anfragen nur über den Domain Namensraum auflösen. Bei jeder Anfrage müsste daher ausgehend von den Root Servern der Domain-Baum bis zum gesuchten Objekt abgelaufen werden. Da sich viele Anfragen an nicht-autoritative Name Server auf denselben Teil des Namensraums beziehen, würde eine ständige Auflösung über die Root Domain Server zum einen ineffizient und zum anderen für die Root Server extrem belastend.
Stattdessen legen nicht-autoritative Name Server Informationen zu Anfragen, die sie bereits gelöst haben, im lokalen Arbeitsspeicher ab. Die autoritativen Name Server der Informationen legen über die TTL[15] fest, wie lange diese gespeichert werden dürfen.
Eine weitere Besonderheit stellt *negatives Caching* dar: Der Server merkt sich, welche Anfragen er nicht auflösen konnte. Erhält er nun weitere Anfragen bezüglich derselben Adresse, so kann er schneller antworten.
Gerade im Bereich des DNS eignet sich Caching sehr, da sich IP-Adressen von Netzwerk-Ressourcen selten ändern. Außerdem kann Caching nicht nur bei den Domain Name Servern angewandt werden, sondern auch lokal bei den Internet-Teilnehmern.

4.3 Inverse Mapping

Manchmal ist es von Nutzen, zu einer gegebenen IP-Adresse den entsprechenden Eintrag im Domain Namensbaum zu kennen. Da ein Absuchen des Namensraums nach der IP-Adresse ineffizient wäre, wurde dafür die Domain *IN-ADDR.ARPA* eingerichtet. Diese Domain besteht nur aus drei Subdomain-Ebenen, von denen alle als Label eine Zahl zwischen 0 und 255 haben. Jede Ebene im *IN-ADDR.ARPA*-Baum repräsentiert eine Komponente einer gegebenen IP-Adresse in umgedrehter Reihenfolge: So wird aus der IP-Adresse *aaa.bbb.ccc.ddd* die Domain *ddd.ccc.bbb.aaa.in-addr.arpa*[16]. Eine Auflösung nach einer IP-Adresse erfolgt nun wie im restlichen DNS.
Die gespeicherten RR im *IN-ADDR.ARPA*-Baum enthalten nur[17] den Typ PTR.

[15] Siehe Resource Record.
[16] [1]
[17] Abgesehen von den für die Zonendatei notwendigen NS-RR und der SOA-RR.

4.4 DNS Security Extensions (DNSSEC)

Die Übersetzung von Domain Namen in IP-Adressen ist eine der Schlüsselfunktionen im Internet und damit besonders gefährdet. So ist es möglich, dass sich Angreifer als DNS Server ausgeben, um den Internetverkehr von Nutzern beobachten oder diese auf falsche Adressen lotsen. Um Missbrauch vorzubeugen entwickelte das *IETF*[18] das *DNS Security*. *DNSSEC* soll die Integrität von DNS Nachrichten und die Authenzität des Versenders gewährleisten. Es verwendet ein assymmetrische Kryptosystem. Autoritative Name Server legen einen geheimen und einen öffentlichen Schlüssel an. Der öffentliche Schlüssel wird im RR-Typ *RRSIG* in der DNS Nachricht versendet. Mit dem privaten Schlüssel unterzeichnet der Name Server die Daten. So kann der Empfänger die Inhalte auf Veränderungen überprüfen und den Absender authentifizieren.

[18] Internet Engineering Task Force

Literatur

[1] Douglas E. Comer. *Internetworking with TCP/IP*. Prentice Hall, 2006.

[2] P. Mockapetris. Domain Names - Concepts And Facilities. http://tools.ietf.org/html/rfc1034, 1987.

[3] P. Mockapetris. Domain Names - Implementation And Specification. http://tools.ietf.org/html/rfc1034, 1987.