DNS – Domain Name System

Das Domain Name System,
eine Einführung

Thomas Deutsch <thomas@tuxpeople.org>
20. Oktober 2005
Restaurant Beaulieu, Bern

Inhalt

- Was ist DNS
- Warum ein DNS?
- Geschichte des DNS
- Wie funktioniert DNS
- Konfiguration des Clients
- Konfiguration eines Servers

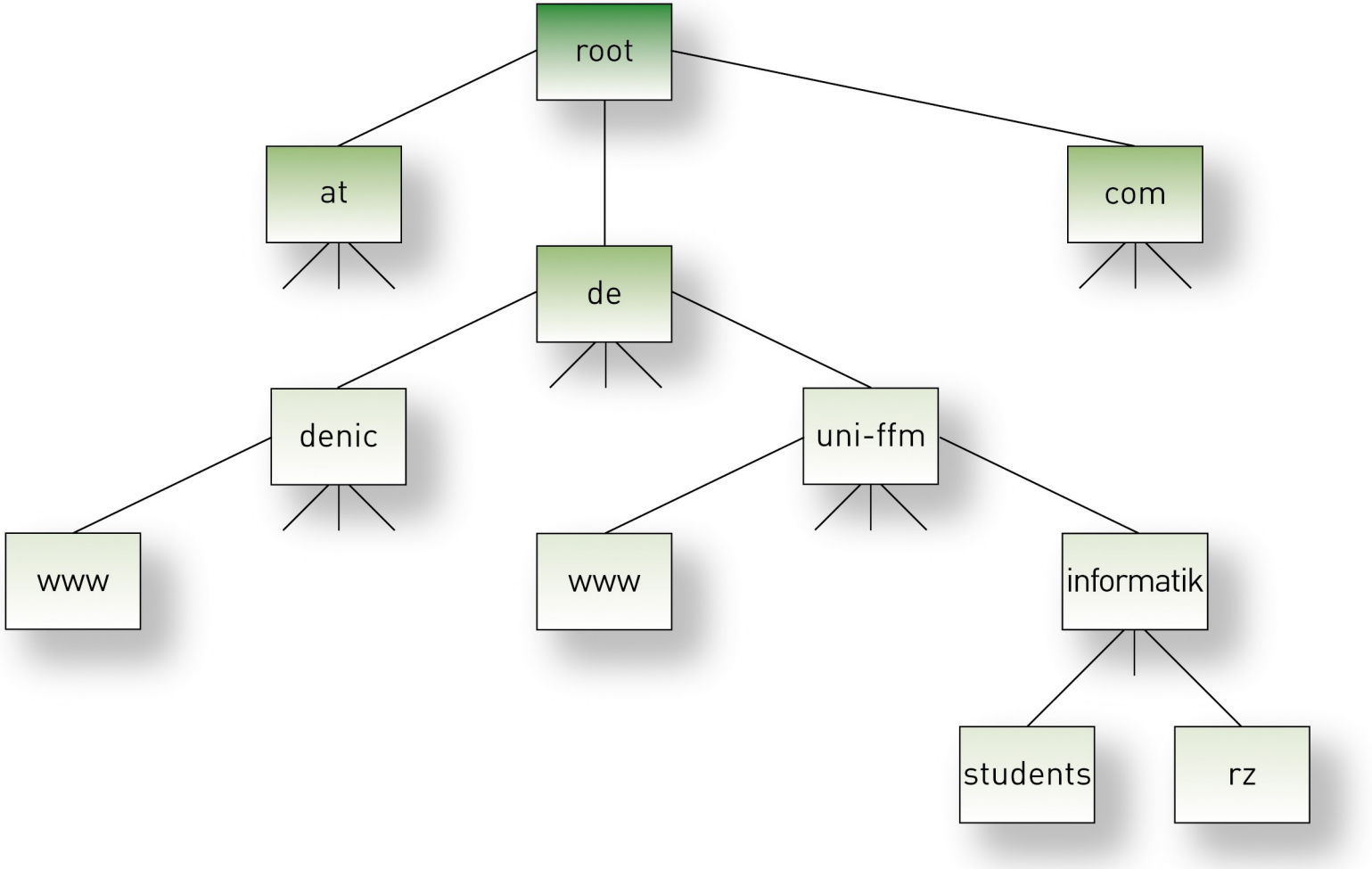
Nicht Inhalt dieses Vortrages:

- Konfiguration eines Servers für rekursive Auflösung

Was ist DNS?

- „unsichtbarer“ Helfer im Hintergrund
- Notwendiger Wegweiser
- Telefonbuch
- Hirarchisch und dezentral
- Unverzichtbar für surfen und mailen

Was ist DNS?



Grafik © Denic.de

Die Domain

students.informatik.uni- ffm.de.

.	Root
de	Top- Level- Domain (TLD)
uni- ffm	Second- Level- Domain
informatik	Third- Level- Domain
students	Hostname

Rootserver

13 Rootserver „A“ - „M“

- Zentrale Rolle: A-Server
  - Datenbasis für alle Rootserver
  - Sync 2x pro Tag
- Aus technischen Gründen nicht mehr möglich
- Trick: Anycast
  - 5 Rootserver nutzen Anycast z.B.
  - F-Server: 19 Server auf 5 Kontinenten
  - K-Server: 16 Server auf 4 Kontinenten
  - Genf: I + K
- 5 alternative Rootserver-Netzwerke

Die Topleveldomains

- Es gibt über 200 TLDs
- Unterschieden werden:
  - Allgemeine Top Level Domains
  - Länderspezifische Top Level Domains
  - Sonderfälle

Allgemeine TLDs

- .aero: aeronautics(weltweit)
- .arpa: Arpanet
- .biz: business (weltweit)
- .com: commercial (weltweit, *)
- .coop: cooperatives (weltweit)
- .edu: educational (*)
- .gov: government (*)
- .info: Informationsanbieter (weltweit)
- .int: Internationale Regierungsorganisationen
- .mil: military (*)
- .museum: Museen (weltweit)
- .name: nur für natürliche Personen oder Familien (Privatpersonen, weltweit)
- .net: Netzverwaltungseinrichtung (weltweit, *)
- .org: organization (weltweit, *)
- .pro: professions (Anwälte, Steuerberater, Ärzte), nur für genannte Berufsgruppen der USA
- .travel: für die Reiseindustrie

*= Ursprüngliche TLDs

Länderspezifische TLDs

- Es gibt über 200 ccTLDs. Jedes Land besitzt genau einen Zwei-Buchstaben Code nach ISO 3166.
- Ausnahmen:
  - das Vereinigte Königreich besitzt die TLDs .uk und .gb
  - Ascension hat eine eigene TLD .ac, obwohl es nicht auf der ISO-Liste steht, sondern zu St. Helena (.sh) gehört.
  - Des weiteren sind noch vier obsolete TLDs aus Gründen der Erreichbarkeit aktiv:
    - Serbien und Montenegro besitzt die TLDs .cs und .yu
    - In der Russischen Föderation wird neben .ru auch noch .su betrieben
    - Ost-Timor wechselt momentan von .tp auf .tl und betreibt für eine Übergangszeit beide TLDs
    - .zr für Zaire wurde 2004 aus den Root-Servern entfernt (jetzt .cd)

Sonderfälle

- .eu
  - Ist weder eine Länderspezifiche Domin (Die EU ist kein Land) noch eine Allgemeine TLD da sie auf ein bestimmtes Gebiet beschränkt ist.
- .arpa
  - Gedacht als Temporäre Lösung bei der Einführung von DNS
  - Subdomain `in-addr.arpa` ist weltweit im Einsatz, um das Auflösen einer IP-Adresse in einen Domainnamen (reverse lookup) zu ermöglichen
  - Subdomain `e164.arpa` wird für ENUM, die Adressierung von Internet-Diensten über Telefonnummern verwendet.

Warum ein DNS?

- Namen kann man besser merken als Zahlen
- Werbewirksammer
- Virtuelle Hosts nur dank DNS möglich

Alternativen:

- IP- Adressen auswendig lernen
- /etc/hosts

Geschichte des DNS

- Ende der 60er:
  - Advanced Research Projects Agency Net
- Beginn der 80er:
  - Entwicklung von TCP/IP
  - SRI-NIC am Stanford Research Institute verwaltet hosts.txt
- Mitte der 80er:
  - DNS wird ins ARPAnet implementiert und wird zum Standard
- Beginn der 90er:
  - Das WWW entsteht (Tim Berners-Lee am CERN (Genf))

Wie funktioniert DNS?

- Zuerst /etc/hosts
- Dann den Nameserver (/etc/resolv.conf)
- Was abgefragt wird und die Reihenfolge regelt die /etc/nsswitch.conf
- Nameserver weiss Antwort falls Cache ist oder Zone verwaltet
- Sonst normale Namensauflösung

Die Datei /etc/resolv.conf

- Beinhaltet die DNS Konfiguration des Clients
- Wird bei DHCP automatisch konfiguriert

Beispiel:

```
search saxsys.de galaxis.de
nameserver 134.109.192.18
nameserver 192.168.85.1
```

Die Datei /etc/nsswitch.conf

- Regelt die Reihenfolge der Namensauflösung

Beispiel:

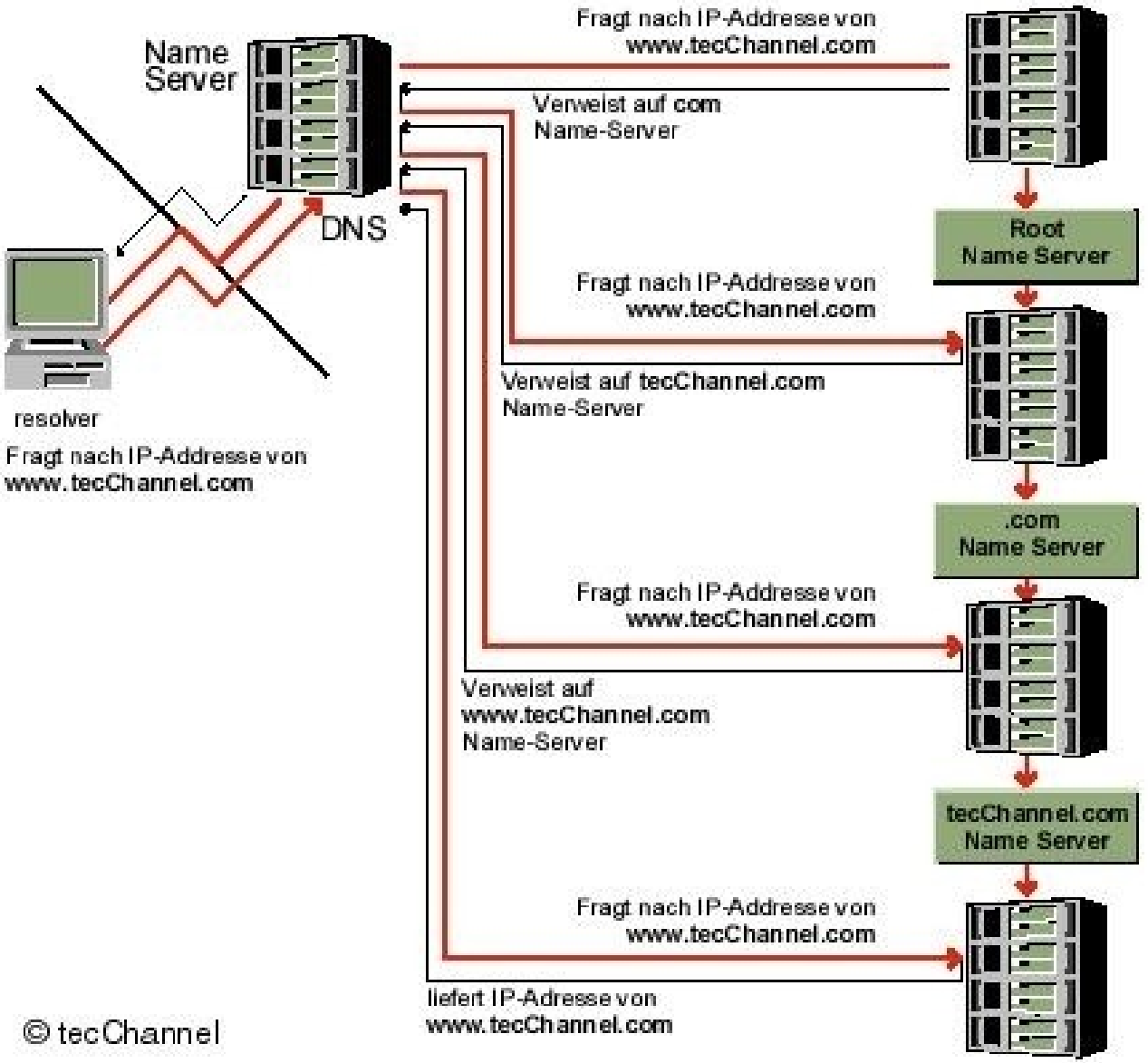
```
hosts:          files dns
```

- Damit werden zuerst die Dateien (files) und dann der Namensdienst (DNS) befragt.

Die Namensauflösung per DNS

- Grundsätzlich werden zwei Arten der Namensauflösung unterschieden:
  - rekursive Namensauflösung
  - iterative Namensauflösung
- Der Client übermittelt in beiden Fällen den Hostnamen und legt den Abfragetyp fest

Die rekursive Namensauflösung



Die iterative Namensauflösung

- Der DNS-Server des Clients teilt dem Client nur mit, welches der nächste Nameserver ist
- Die Abfrage der auf der letzten Folie gezeigten Server muss der Client selbst vornehmen

Eigener Cache- only DNS- Server

- Download der Software von ftp://ftp.isc.org/isc/bind9/
- Eventuell auch Installation über ein Package-Management
- Aktuell bei Bind9 ist zur Zeit die Version 9.2.5. Die unstable Version ist 9.3.1
- Anlegen von
  - named.conf
  - named.root
- Nameserver starten und beim Client eintragen

/ etc/ named.conf

```
options {
        directory "/etc/named";
};


zone "." IN {
        type hint;
        file "named.root";
};
```

/etc/named/named.root

- Download per FTP von ftp://ftp.internic.net/domain/named.root (ftp://192.0.34.27/domain/named.root)
- named.root enthält die IP-Adressen der Root-Server. (Auszug):

```
.                        3600000   NS     B.ROOT-SERVERS.NET.

B.ROOT-SERVERS.NET.      3600000   A      192.228.79.201


.                        3600000   NS     C.ROOT-SERVERS.NET.

C.ROOT-SERVERS.NET.      3600000   A      192.33.4.12
```

Die eigene Domain

- Registrieren einfach
- Kein Luxus mehr
- Man braucht zwei DNS-Server

/etc/named/named.domain.ch

```
@       IN          SOA dns1.domain.ch. root.dns1.domain.ch. (
                                2002012401      ; Serial
                                10800           ; Refresh 3 hours
                                3600            ; Retry   1 hour
                                604800          ; Expire 1000 hours
                                86400)          ; Minimum 24 hours
                IN          NS          dns1.domain.ch.
                IN          NS          dns2.zweiterserver.ch.
;
dns1            IN          A           195.162.162.160
;
domain.ch.      IN          MX 0        mail.domain.ch.
;
www             IN          A           195.162.162.160
ftp             IN          CNAME       www
mail            IN          A           195.162.162.160
smtp            IN          CNAME       mail
pop             IN          CNAME       mail
```

Änderungen an der named.conf

```
allow-transfer {

130.59.1.80;
130.59.211.10;
192.16.202.11;
128.112.129.15;
147.28.0.39;
200.16.97.77;
194.42.48.120;
203.37.255.97;
164.128.36.32/27;
195.162.161.182;  Unser Secondary Nameserver
};


zone ".domain.ch" in {
        type master;
        file "named.domain.ch";
};
```

Die named.conf des Slave Servers

```
zone "domain.ch" {
   type slave;
   file "secondary-domain.ch";
   masters {
           195.162.162.160;
   };
};
```

Uebersicht der gebräuchlichen Record-Typen

• A <IP>	Authoritativ Record IPv4
• AAAA <IPv6>	Authoritativ Record IPv6
• A6 <IPv6>	Authoritativ Record IPv6
• NS <hostname>	Nameserver Record
• MX <prio> <hostname>	Mail Exchanger
• CNAME <hostname>	Canonical Name
• SOA <Domain>	Start Of Authority
• PTR <hostname>	Pointer für Reverse- DNS

Andere Record- Typen

Seltener benutzte Record- Typen

- HINFO <Text> — Host- Info, Angaben zur Hardware, OS, Standort etc
- TXT <Text> — Freier Text
- RP <Text> — Responsible Person, Name der zuständigen Person

Experimentelle oder nicht mehr gebräuchliche Record- Typen

- ISDN <Telnummer> — ISDN Nummer
- MINFO <resp- mbox> — Mailbox oder Mailinglisten Information
- NULL <irgendwas> — Tut nichts

Weitere Infos

- http://de.wikipedia.org/wiki/Anycast
- http://www.linuxfibel.de/dns_cli.htm
- http://www.linuxfibel.de/dns_srv.htm
- http://european.ch.orsn.net/
- http://de.wikipedia.org/wiki/Internet
- http://www.isc.org/index.pl
- http://www.oreilly.de/german/freebooks/linag2/netz1307.htm
- http://de.wikipedia.org/wiki/Top_Level_Domain
- http://www.tecchannel.de/netzwerk/grundlagen/401207/
- http://de.wikipedia.org/wiki/Domain_Name_System
- http://www.denic.de/de/domains/technik/nameserverdienst/