DNS Grundlagen

ORR - November 2015

jenslink@quux.de

/me

- Freelancer
- Linux seit es das auf 35 Disketten gab
- IPv6
- DNS und DNSSEC
- Monitoring mit Icinga, LibreNMS, ...
- Netzwerke (Brocade, Cisco, Juniper)

Grundlagen

- Zuweisung
  - Name - Adresse
  - Adresse - Name
- Früher: Textdatei (für einige heute immer noch)
  - /etc/hosts
  - %systemroot%\system32\drivers\etc\hosts
- Verteilte Datenbank
- Jeder kümmert sich um seinen Teil

Aufbau

www.example.com.

- . = Root
- com = TLD
- example = Domain
- www = Hostname

Wer ist zuständig?

- Root: ICANN
- TLD:
  - de - DENIC
  - com - Verisign
  - ...
- Domain: Eigentümer der Domain
- Subdomain: ggf. Abteilungen

DNS ROOT

- 13 ROOT DNS Server [a-m].root-servers.net
- Verschiedene Betreiber, z.B. ICANN, Verisign, ISC, RIPE NCC, NASA, US DOD, US Hochschulen
- Bis auf b per Anycast weltweit verteilt
- Bis auf e und g alle per IPv6 erreichbar
- siehe auch http://www.root-servers.net

Achtung: h.root.servers.net ändert im Dezember seine Adressen

Exkurs: Anycast

- Mehrere Server - eine IP (bzw. ein Netz)
- Server nehmen am dyn. Routing teil
- es wird der “nächste” Server genommen

Und wie geht das nun?

Wie kommt man nun von www.openrheinruhr.de zu 148.251.109.234?

- Frage an .: Wer ist für .de zuständig -> DNS-Server DENIC
- Frage an DENIC: Wer ist für openrheinruhr zuständig? -> DNS-Server von Schlund
- Frage an Schlund: wie ist die IP für www.openrheinruhr.de? -> 148.251.109.234

Resource Records (I)

<name> [<ttl>] [<class>] <type> <rdata>

- Name
- TTL - Gültigkeitsdauer in Sekunden
- Class - Klasse (eigentlich immer **IN** für Internet)
- type - Typ des Records
- rdata Daten

Recource Records (II)

(ohne DNSSEC/DANE)

- A - Address
- AAAA - IPv6 Address
- CNAME - Canonical Name record (Alias)
- MX - Mail eXchange record
- NS - Nameserver
- PTR - Pointer record
- SOA - Start Of Authority
- SRV - Service locator
- TXT - Text Record

Recource Records (III)

(DNSSEC/DANE)

- DNSKEY - DNS Key Record
- DS - Delegation Signer
- NSEC - Next-Secure record
- NSEC3 - NSEC record version 3 or NSEC hashed
- RRSIG - DNSSEC Signature
- TLSA - TLSA certificate association

Recource Records: MX (I)

- Welcher Mailserver ist für die Domain zuständig?
- Wenn kein MX wird versucht an den A-Record der Domain zuzustellen
- Neu: RFC7505 - Null MX für Domains ohne Mailserver

Recource Records: MX (II)

Aufbau: *preference name*

- Es kann mehr als einen Eintrag geben
- Der mit der kleinsten preference wird bevorzugt
- ist dieser nicht erreichbar wird der nächste genommen

```
dig mx openrheinruhr.de +short
10 mx.mylinuxtime.de.
```

Null MX:

- preference = 0
- Name = .

Recource Records: SOA

Start Of Authority - Wer ist überhaup zuständig?

```
openrheinruhr.de.    86378 IN SOA nsa3.schlundtech.de. \
                     michael.gisbers.de. (
                         2015102000 ; serial
                         43200      ; refresh (12 hours)
                         7200       ; retry (2 hours)
                         1209600    ; expire (2 weeks)
                         86400      ; minimum (1 day)
                     )
```

Recource Records: SRV

Beispiel: XMPP

```
_jabber._tcp.example.com.          IN SRV   0 0 5269    \
        jabber.example.com.
_xmpp-server._tcp.example.com.   IN SRV   0 0 5269   \
        jabber.example.com.
_xmpp-client._tcp.example.com.   IN SRV   0 0 5222   \
    jabber.example.com.
```

Beispiel: LDAP

```
_ldap._tcp.example.com. 3600  IN  SRV  10  0  389  \
        ldap01.example.com.
```

PTR (I)

Wie lautet der Name der IP?

```
> dig a mail.quux.de +short
79.140.40.231
> $ dig -x 79.140.40.231 +short
mail.quux.de.
```

PTR (II)

Vorsicht mit IPv6, die IP wird so eingetragen:

5.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.0.1.0.4.1.0.1.0.8.b.d.1.0.0.2.ip6.arpa

Server

Man unterscheidet:

- Rekursive Server
- Authorative Server

Rekursiv

- beantworten Anfragen von Clients
- cachen Daten

Implementierungen:

- Bind
- unbound
- PowerDNS Recusor
- ...

Authorative

- sind für bestimmte Zonen zuständig
- dürfen keine anderen Namen auflösen

Implementierungen:

- Bind
- PowerDNS
- ...

NSentry

Es muss nicht immer ein eigener Namserver sein. Die DENIC bietet z.B. an Daten direkt in die DE Zone einzutragen.

Siehe https://www.denic.de/hintergrund/nameservice/nameserver-und-nsentry-eintraege.html

Multicast DNS

- Ziel: Dienste im lokalen Netz verfügbar machen (z.B. Drucker)
- TLD: .local
- Tool: mdns-scan

DNS Glue

Wenn der Nameserver für eine Domain innerhalb der Domain liegt benötigt man Glue:

```
> dig ns quux.de +short
ns1.quux.de.
ns1.jenslink.net.

> whois quux.de | grep Nserver
Nserver: ns1.jenslink.net
Nserver: ns1.quux.de 2001:4d88:1014:101:0:0:0:53 \
                     79.140.40.227
```

DNS TCP vs. UDP (I)

RFC1123:

> *DNS resolvers and recursive servers MUST support UDP, and SHOULD support TCP, for sending (non-zone-transfer) queries.*

DNS TCP vs. UDP (II)

- 512 Byte Limit zu klein für neue Record-Typen
- EDNS0 (RFC2671) schafft Abhilfe, ist aber nicht überall sauber implementiert
- Wenn die Größe des UDP Paketes die MTU überschreitet muss fragmentiert werden -> Dies kann zu Problemen mit Firewalls führen
- RFC5966 macht aus “SHOULD support TCP” ein “MUST support TCP”

Die häufigsten Probleme

- Seriennummer nicht geändert
- Falsche Daten
- Falscher Glue
- Probleme beim übertragen der Zonen
- Firewall lässt nur UDP durch
- Uralte Filterregeln die man aus dem Internet kopiert hat
- Alle Nameserver in einem AS
- Ein Nameserver reicht auch

Nützliche Tools

- http://www.dnsviz.net
- http://www.zonemaster.net
- http://dane.sys4.de
- http://www.nsupdate.info
- dig
- drill

DNSSEC

Nächster Vortrag ;-)

Fragen?

Danke für die Aufmerksamkeit