

DNS

Einfuehrung
Domain **N**ame **S**ystem

Referent: Lukas Beeler

Mit freundlicher Unterstuetzung von:

Huber+Monsch

Ueber mich

Lukas Beeler

E-Mail: lukas.beeler@projectdream.org

Web: <http://projectdream.org>

Lebenslauf: <http://projectdream.org/cv.html>

Telematikerlehrling 3. LJ bei Huber+Monsch
Systemadministrator auf *nix Betriebssystemen

Ziele

- Aufbau des DNS verstanden
- RR-Typen und deren Verwendung verstanden
- Verstaendnis des Ablaufs einer Namensaufloesung
- Unterschied zwischen Authoritivem Nameserver und Resolver kennen
- Verstaendnis von glued und glueless Delegationen

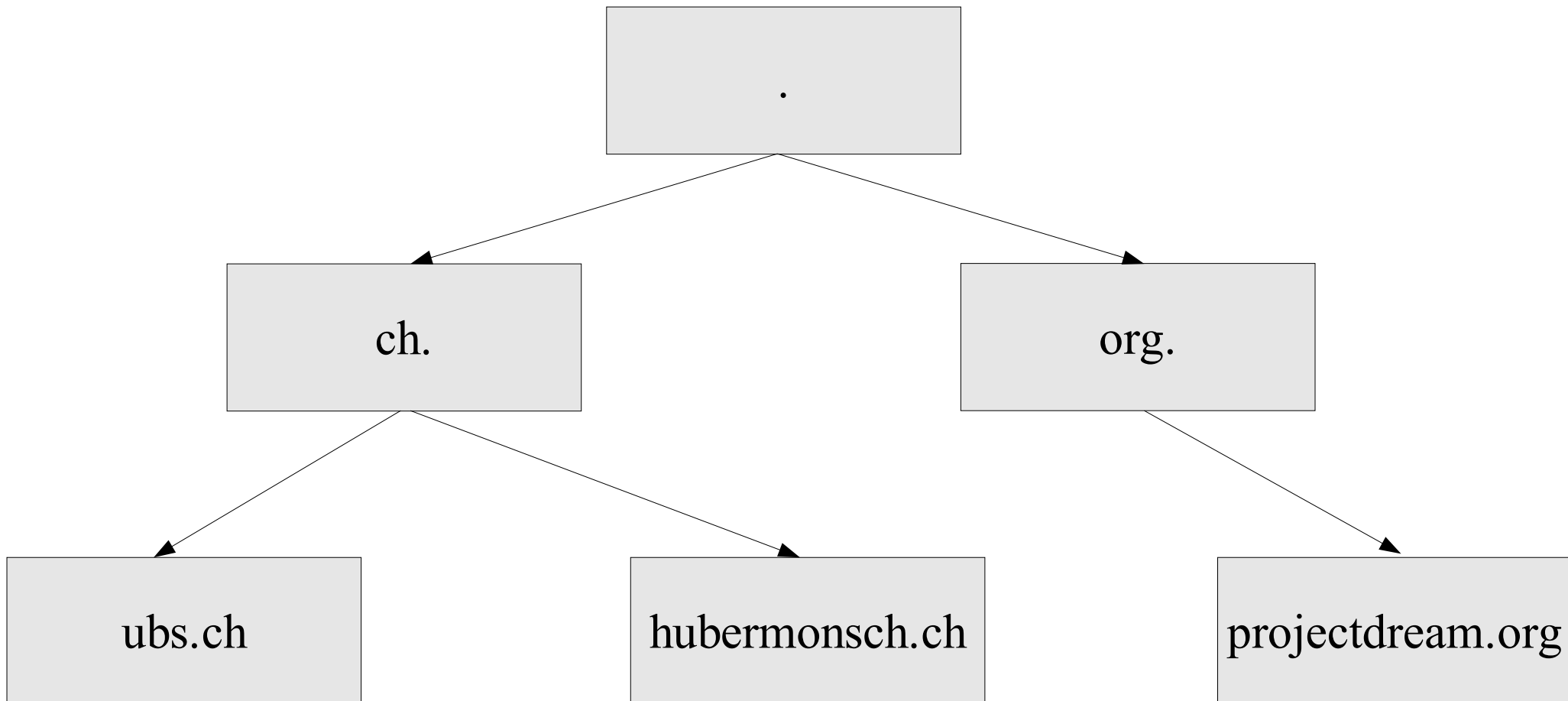
Keine Ziele

- Implementationspezifisches
- Protokoll verstanden
- Mit DNS verwandte Protokolle kennen/verstehen

Geschichtliches

- /etc/hosts
- Neues System
 - Verteilte Datenbank
 - Hierarchisch
- BIND
- DNS Standard

Aufbau



RR's - SOA

```
hubermensch.ch. 86400 IN SOA ns1.v-1.ch. ; Primary
                           webmaster.v-1.ch. ; Hostmaster

                           2002022716 ; Serial
                           10800 ; refresh
                           3600 ; retry
                           604800 ; expire
                           86400 ; minimum TTL
```

RR's PTR

```
113.135.144.213.in-addr.arpa.86400 IN PTR \  
mana.projectdream.org.
```

213.144.135.113

113.135.144.213

113.135.144.213.in-addr.arpa.

Umkehrung der Reihenfolge
Anhaengen von in-addr.arpa.

RR's - NS

```
hubermensch.ch. 86400 IN NS ns1.v-1.ch.
```

RR's - A

```
www.hubermensch.ch. 86400 IN A 157.161.114.120
```

RR's - MX

```
projectdream.org. 86400 IN MX 0 a.mx.projectdream.org.  
projectdream.org. 86400 IN MX 5 b.mx.projectdream.org.  
projectdream.org. 86400 IN MX 10 c.mx.projectdream.org.
```

RR's - SRV

```
_ldap._tcp.pdc._msdcs.hubermensch.ch. 600 IN SRV \
0 100      389      server.hubermensch.ch
```

RR's - CNAME

```
www.hubermensch.ch. 86400 IN CNAME \  
www.grossenbacher.ch.
```

RR's - AAAA

```
may.projectdream.org. 86400 IN AAAA \  
3ffe:202c:ffff:32:230:4fff:fe08:358d
```

RR's - TXT

```
may.projectdream.org. 86400 IN TXT \  
"see http://projectdream.org/nfo/may.html"
```

RR's - LOC

```
projectdream.org. 86400 IN LOC \  
47 0 0.000 N 9 0 0.000 E 779.00m 5m 2m 2m
```

Query-Typen - Iterativ

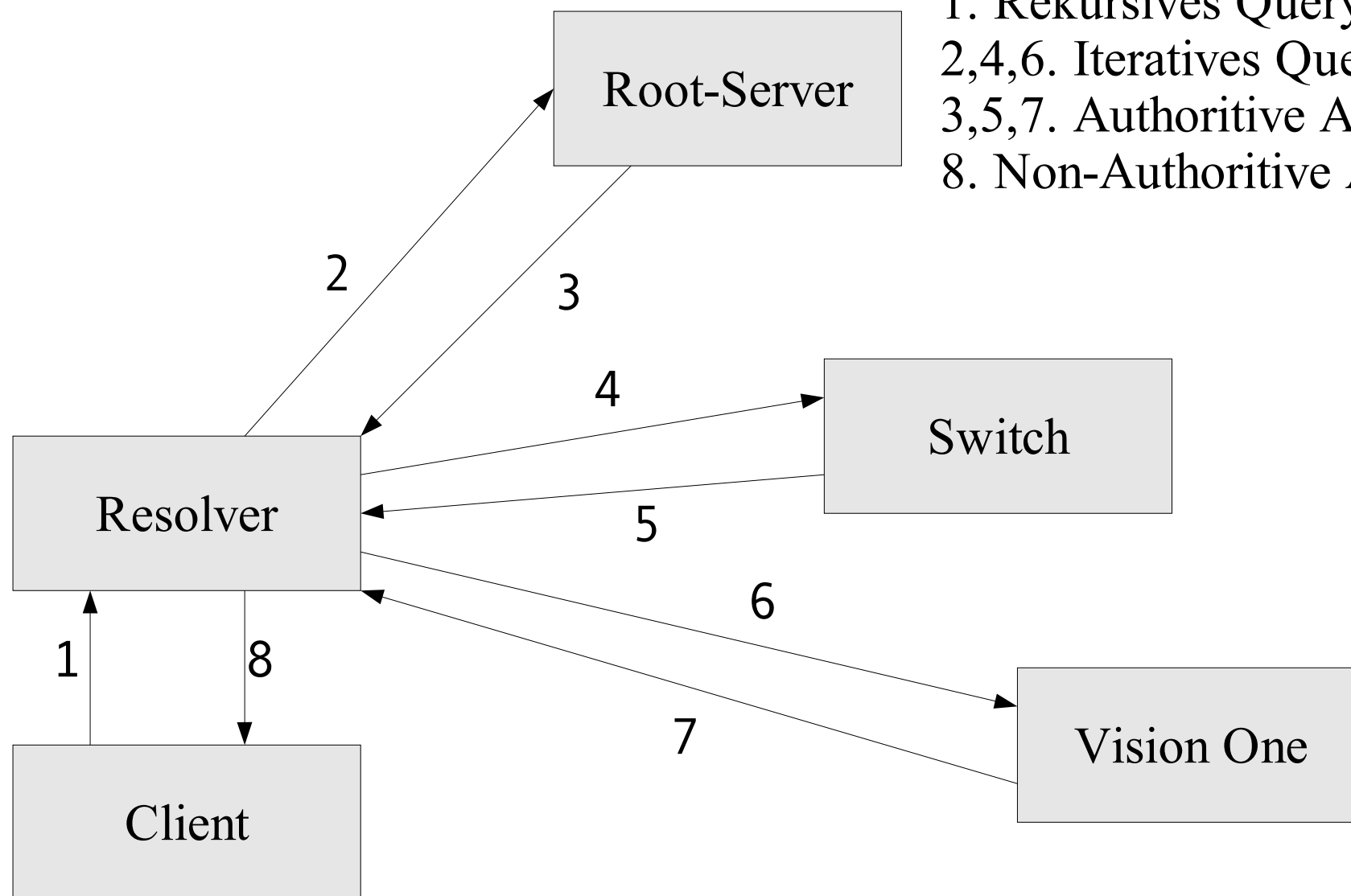
- Wird gestellt von: Resolver, Debugging
- Antwort muss immer authoritativ sein
- Moegliche Antworten
 - Garnicht
 - . Zone
 - NXDOMAIN
 - SERVFAIL
 - NS RR's
 - RR's

Query-Typen - Rekursiv

- Wird gestellt von: Clients, Debugging
- Antwort kann Authoritativ oder Non-Authoritativ sein
- Moegliche Antworten
 - Garkeine
 - SERVFAIL
 - RR's

DNS-Server Typen - Resolver

1. Rekursives Query
- 2,4,6. Iteratives Query
- 3,5,7. Authoritative Antwort
8. Non-Authoritative Antwort



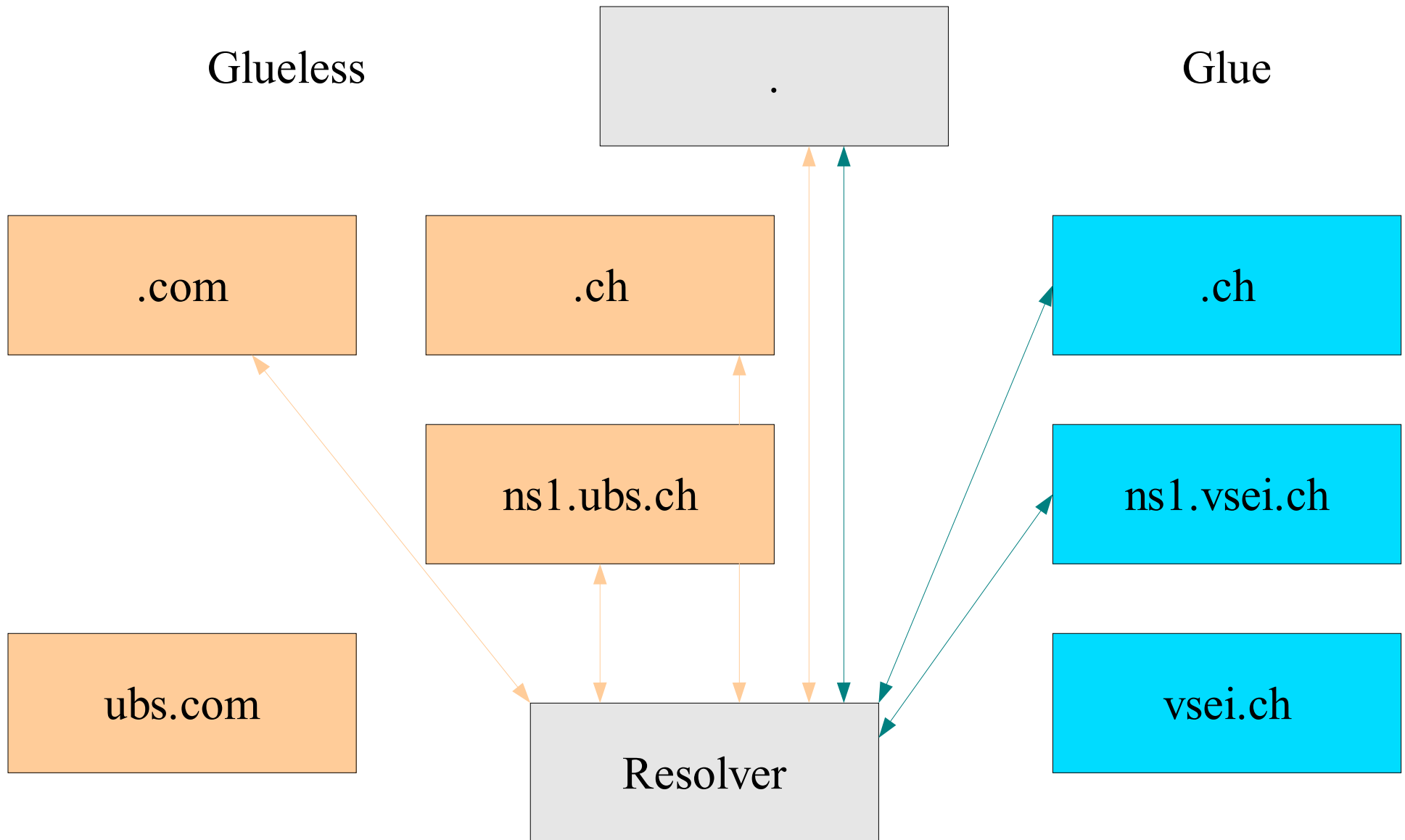
DNS-Server Typen - Autoritativ



Glue

Glueless

Glue



Delegationen

- 2nd Level nur gegen Geld
- 1st Level nur bei ICANN oder anderem Root
- 3rd Level meist Firmenintern

Loadbalancing (z.B. Web)

- Mehrere A RR's fuer einen Namen
- Einfaches, unkontrolliertes Loadbalancing

```
hubermensch.ch. 86400 IN A          157.161.114.120
hubermensch.ch. 86400 IN A          157.161.114.140
```

Loadbalancing (Mail)

- Mehrere MX RR's mit selber Prioritaet
- Einfaches Loadbalancing, aber auch Fallback moeglich

```
hotmail.com. 3600      IN  MX      5  mx1.hotmail.com.  
hotmail.com. 3600      IN  MX      5  mx2.hotmail.com.  
hotmail.com. 3600      IN  MX      5  mx3.hotmail.com.  
hotmail.com. 3600      IN  MX      5  mx4.hotmail.com.
```

TTL

```
hubermensch.ch. 86400 IN SOA ns1.v-1.ch. ; Primary
                    webmaster.v-1.ch. ; Adresse
                    2002022716 ; Serial
                    10800 ; refresh
                    3600 ; retry
                    604800 ; expire
                    86400 ; minimum TTL
```

- Refresh: Gibt an, wie oft der Master gepollt werden soll
- Retry: Gibt an, wie oft ein Refresh erneut versucht werden soll, falls der Master unerreichbar war
- Expire: Gibt an, nach wieviel Zeit der Slave aufhoert auf Anfragen zu Antworten, wenn er den Master nicht mehr erreichen konnte
- Minimum TTL: Gibt die minimale TTL in einer Zone an. Die minimum TTL gilt fuer NXDOMAIN Antworten, die ebenfalls gecached werden.

AXFR

- Zone auf Master wird geaendert, Serial angepasst
- Slaves pollen beim Master periodisch den SOA, und schauen ob sich die Serial geaendert hat. Erweiterung: Notifys
- Slaves laden die Zone mittels AXFR
Erweiterung: IXFR
- Ende der Synchronisation

LDAP

- DNS Daten befinden sich im LDAP
- Updates dank Referrals von ueberall her moeglich

rsync over ssh

- KISS Methode
- Bekannte Tools
- Master pusht zum Slave