

DNSSEC - DNS 1x1

Patrick Koetter und Carsten Strotmann, sys4 AG

Agenda

1. Domain Name System Grundlagen
2. Der DNS Namensraum
3. DNS Namens-Auflösung
4. Komponenten eines DNS-Systems
5. DNS als Protokoll
6. DNS-Delegation
7. der SOA-Record
8. der NS-Record

DNS - Das Domain Name System

DNS is like chess

the rules are simple

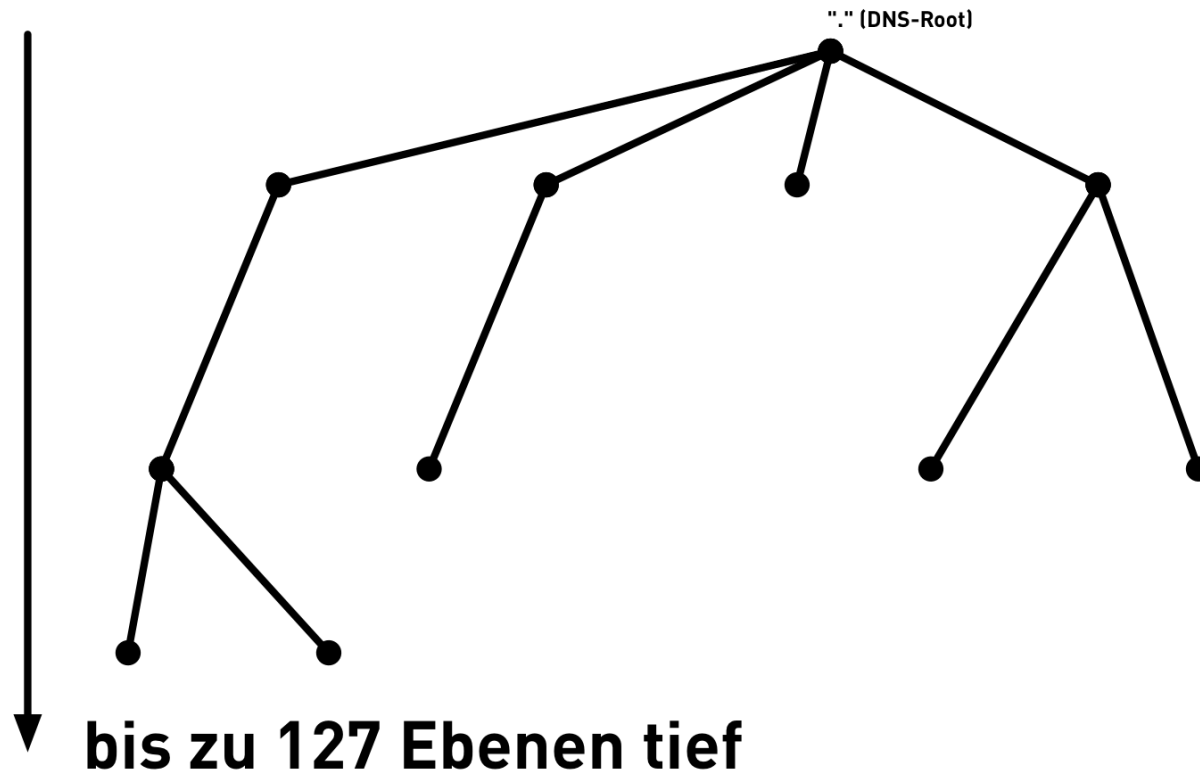
but the chances to loose the game

are endless

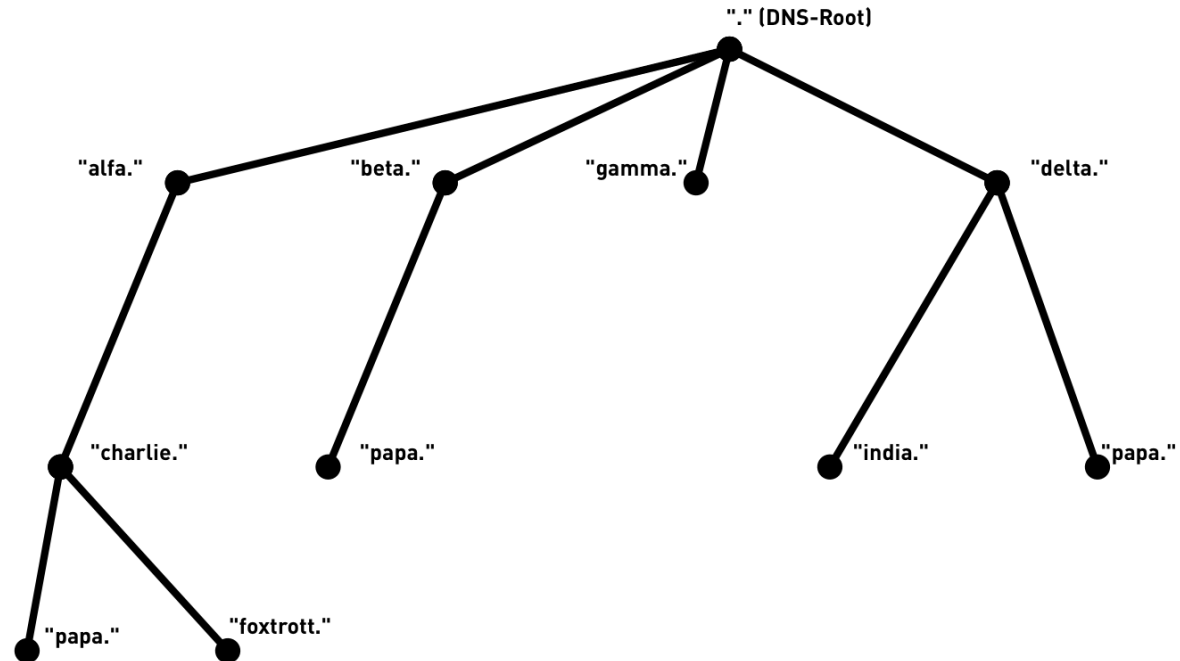
DNS - Das Domain Name System

- Erste Grundlagen 1981-1983
- Einführung im Internet von 1983 bis 1988
- Ersatz für die statische "hosts.txt" Datei
- Bis heute immer erneuert/erweitert
- Skaliert mit dem Wachstum des Internet
- Keine eigenen Sicherheits-Mechanismen

DNS Namensraum

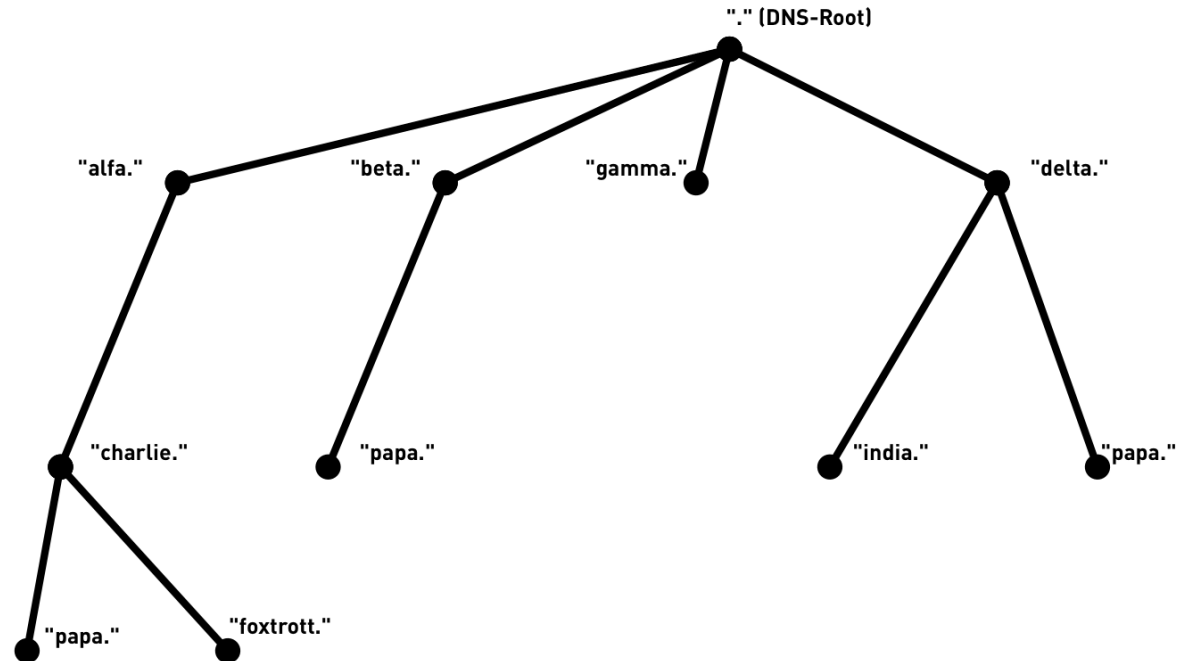


DNS Namensraum - "Label"



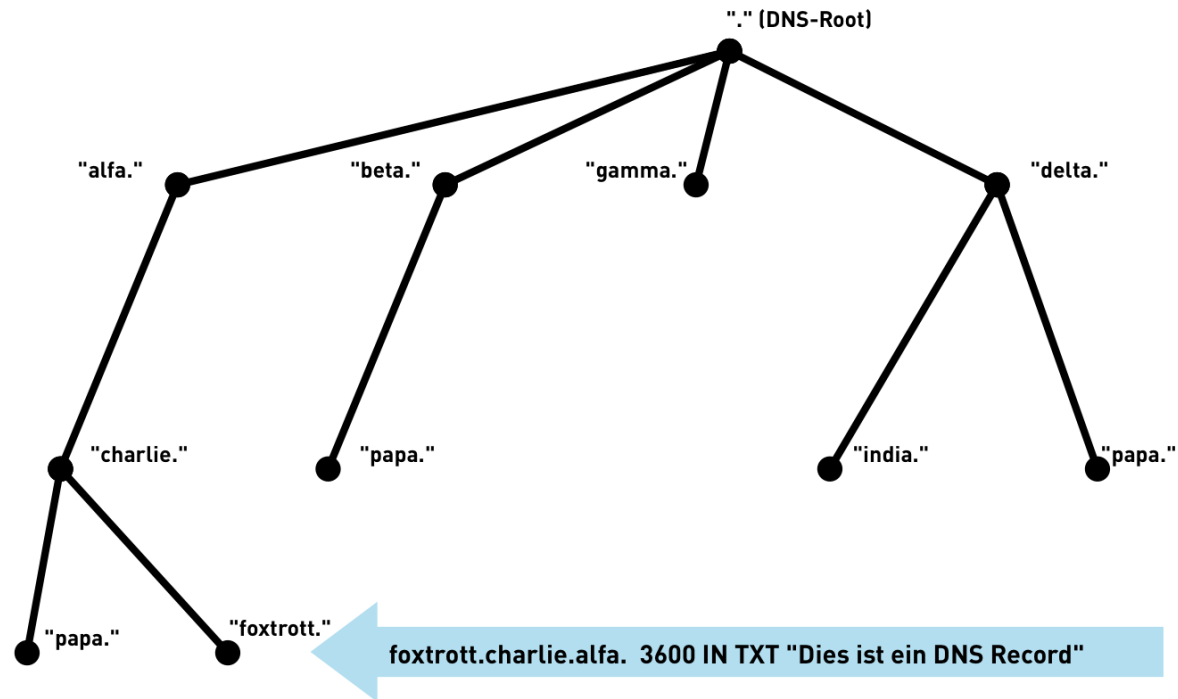
Knoten haben Namen, 0-63 Byte

DNS Namensraum - "Label"



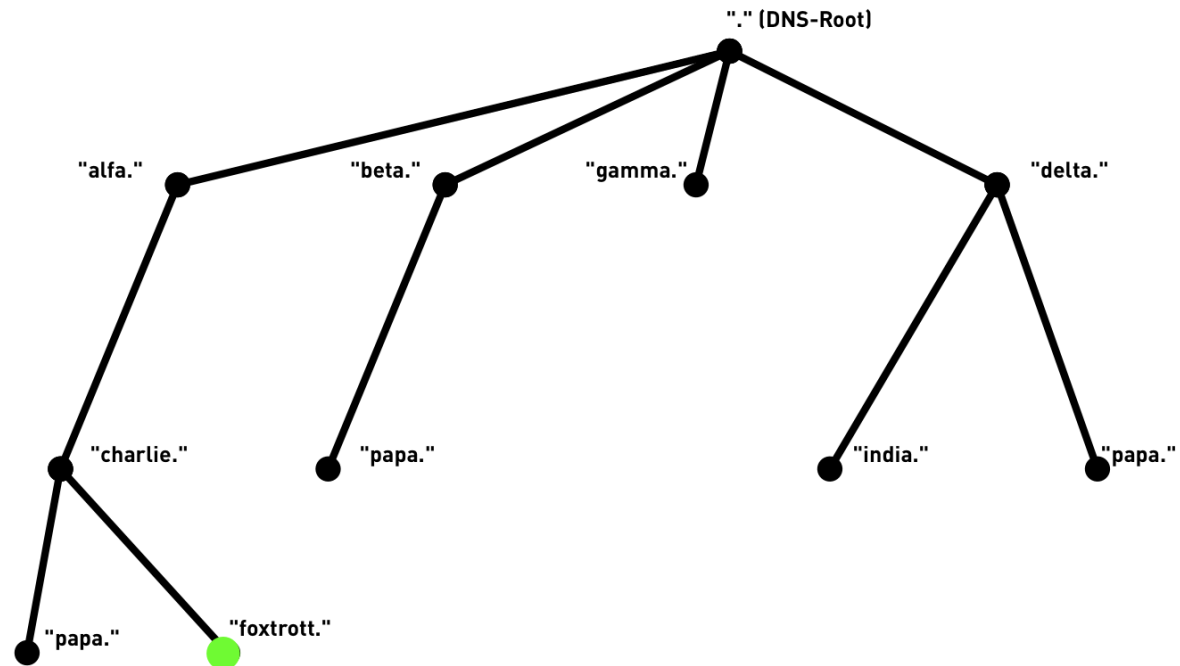
**Namen unter dem gleichen Elternknoten
müssen eindeutig sein**

DNS Namensraum - "Label"



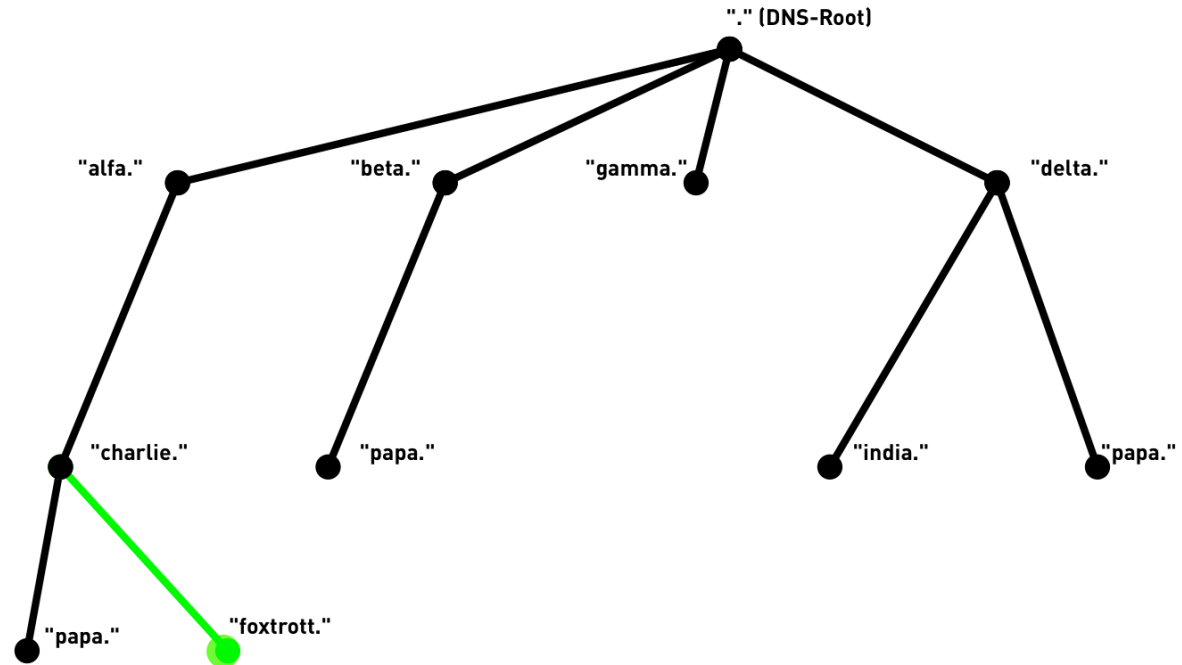
Knoten "besitzen" Daten

DNS Namensraum



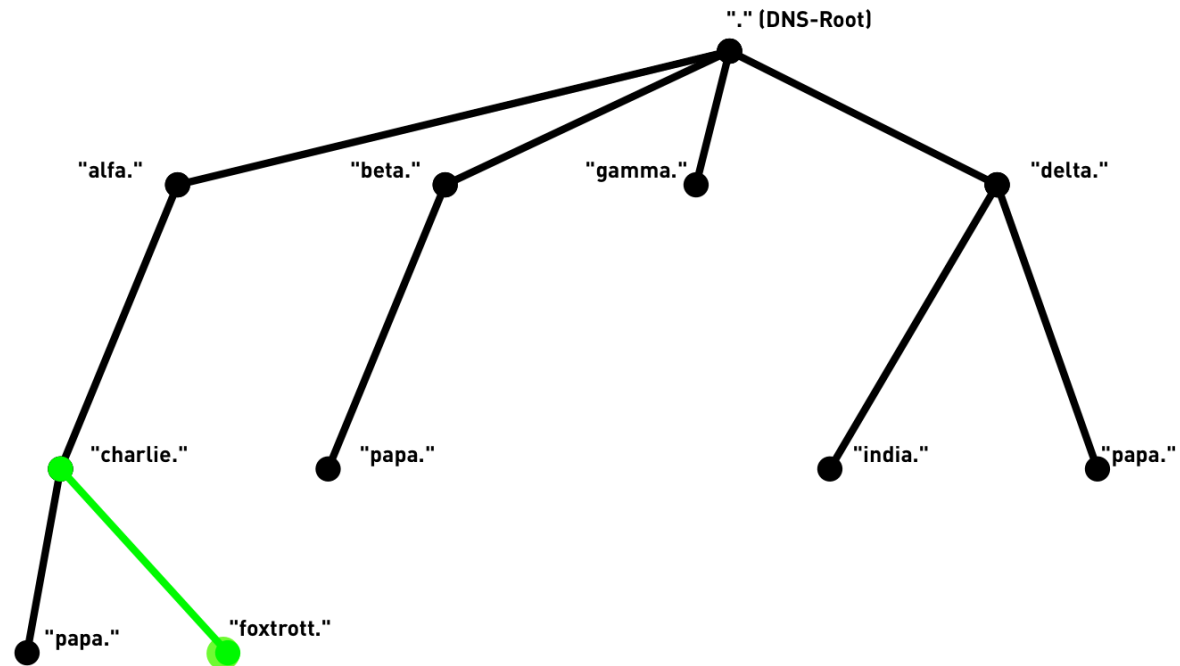
foxtrott

DNS Namensraum



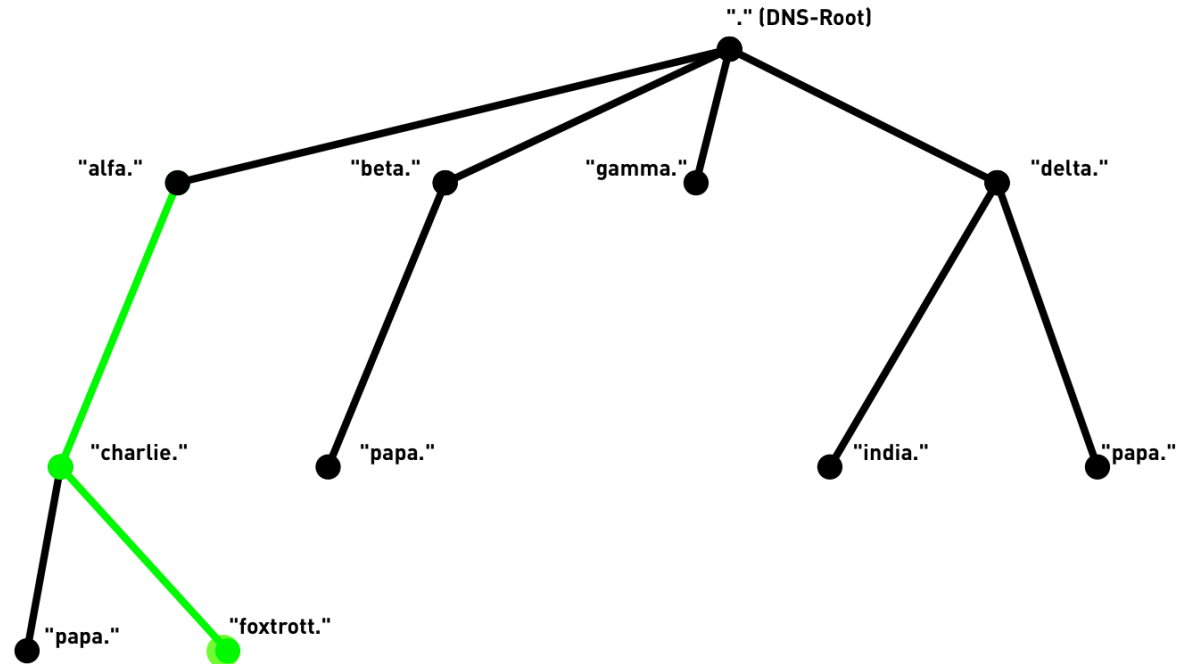
foxtrott.

DNS Namensraum



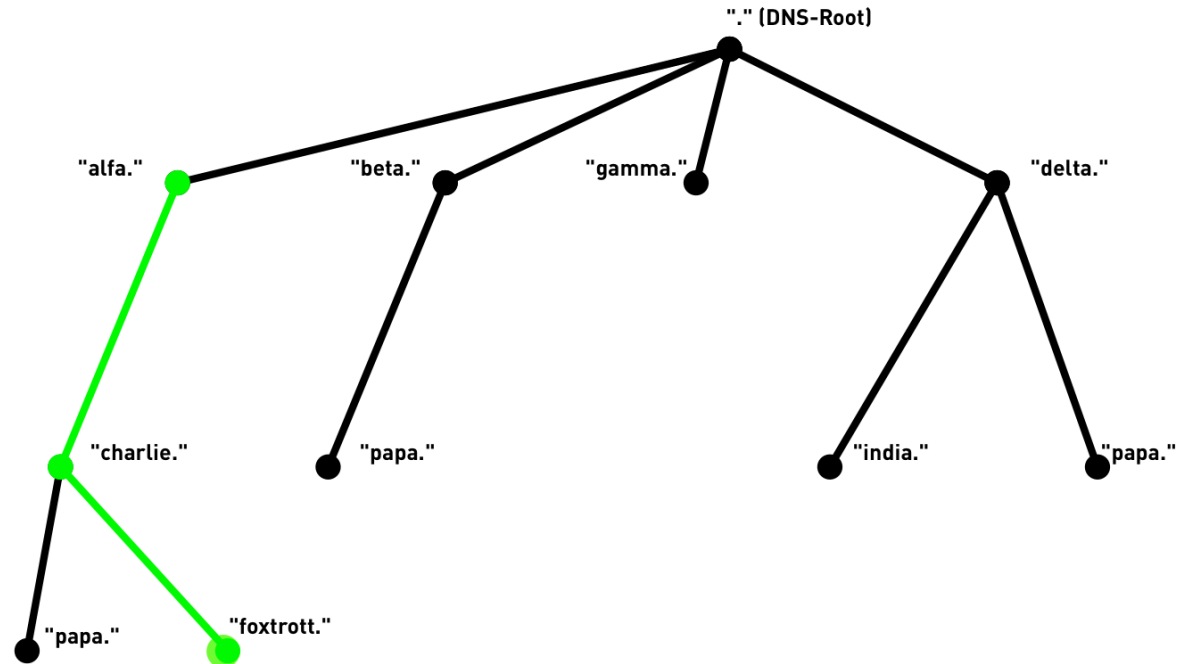
foxtrott.charlie

DNS Namensraum



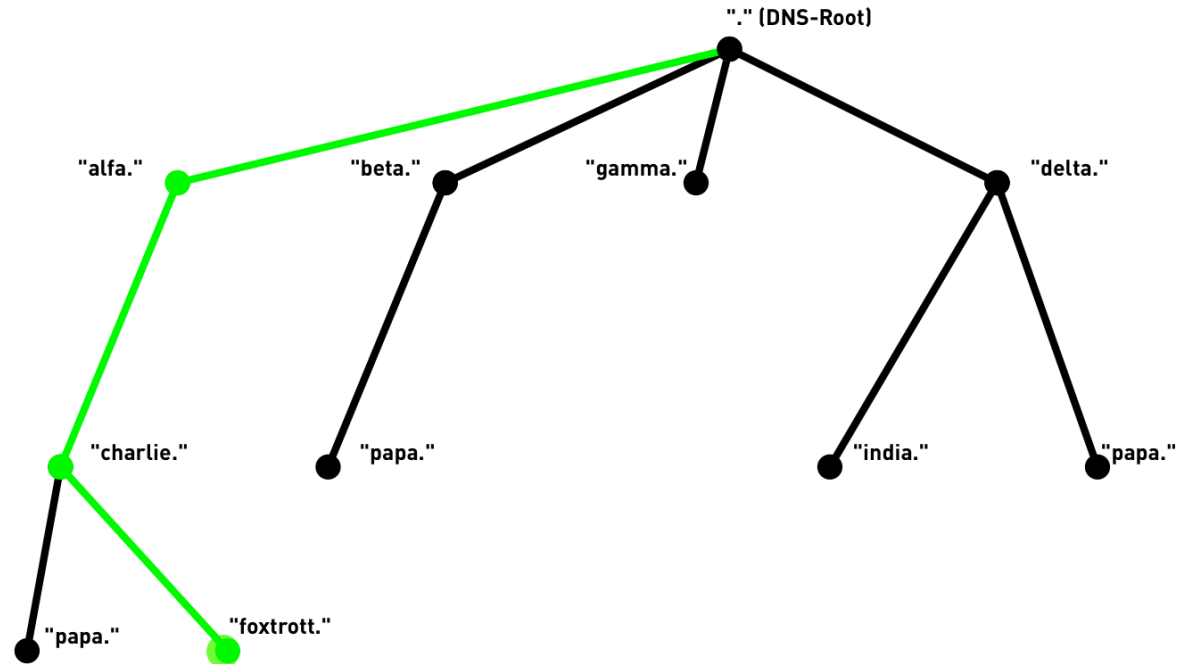
foxtrott.charlie.

DNS Namensraum



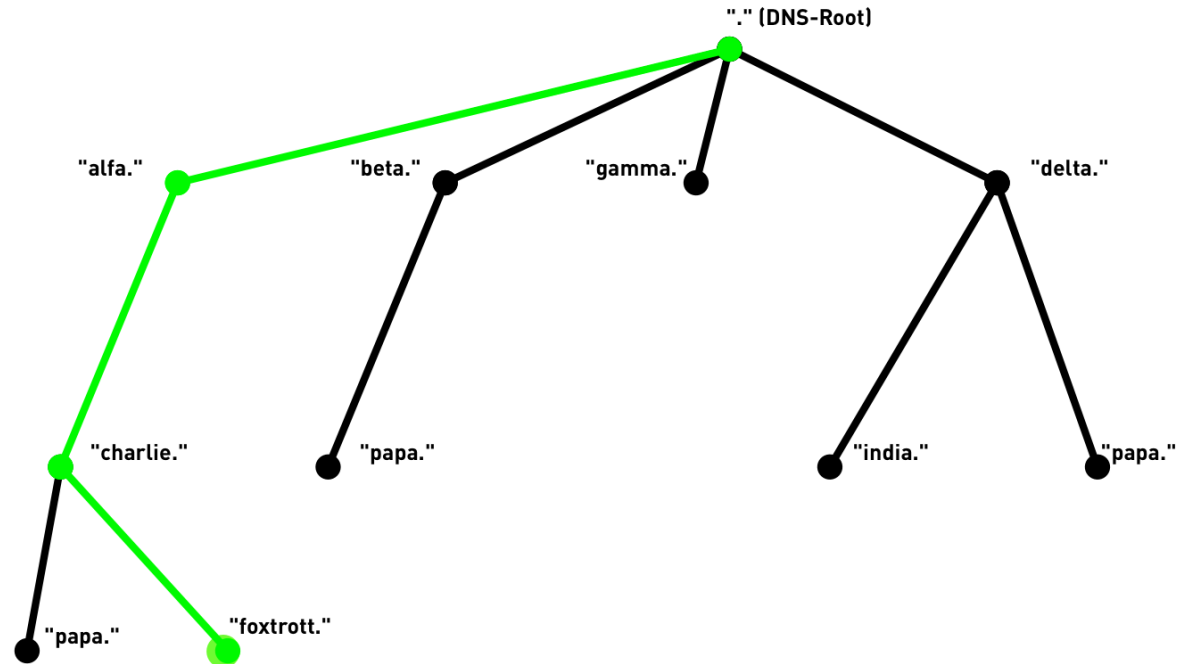
foxtrott.charlie.alfa

DNS Namensraum



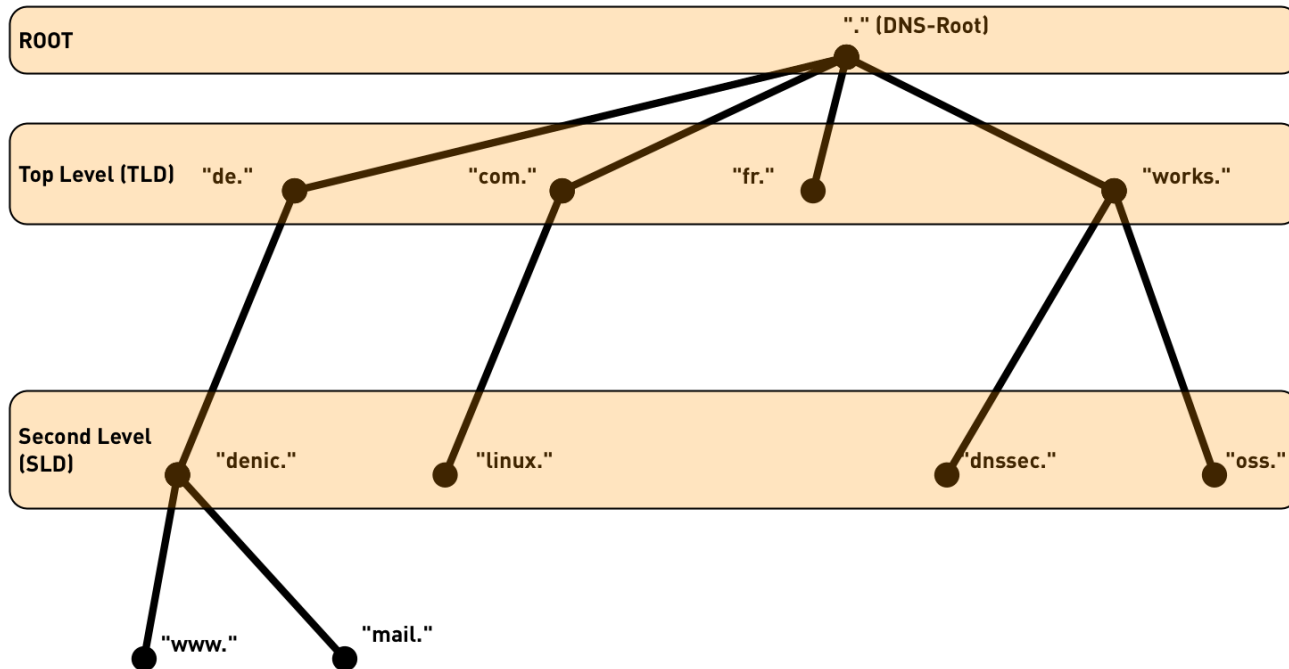
foxtrott.charlie.alfa.

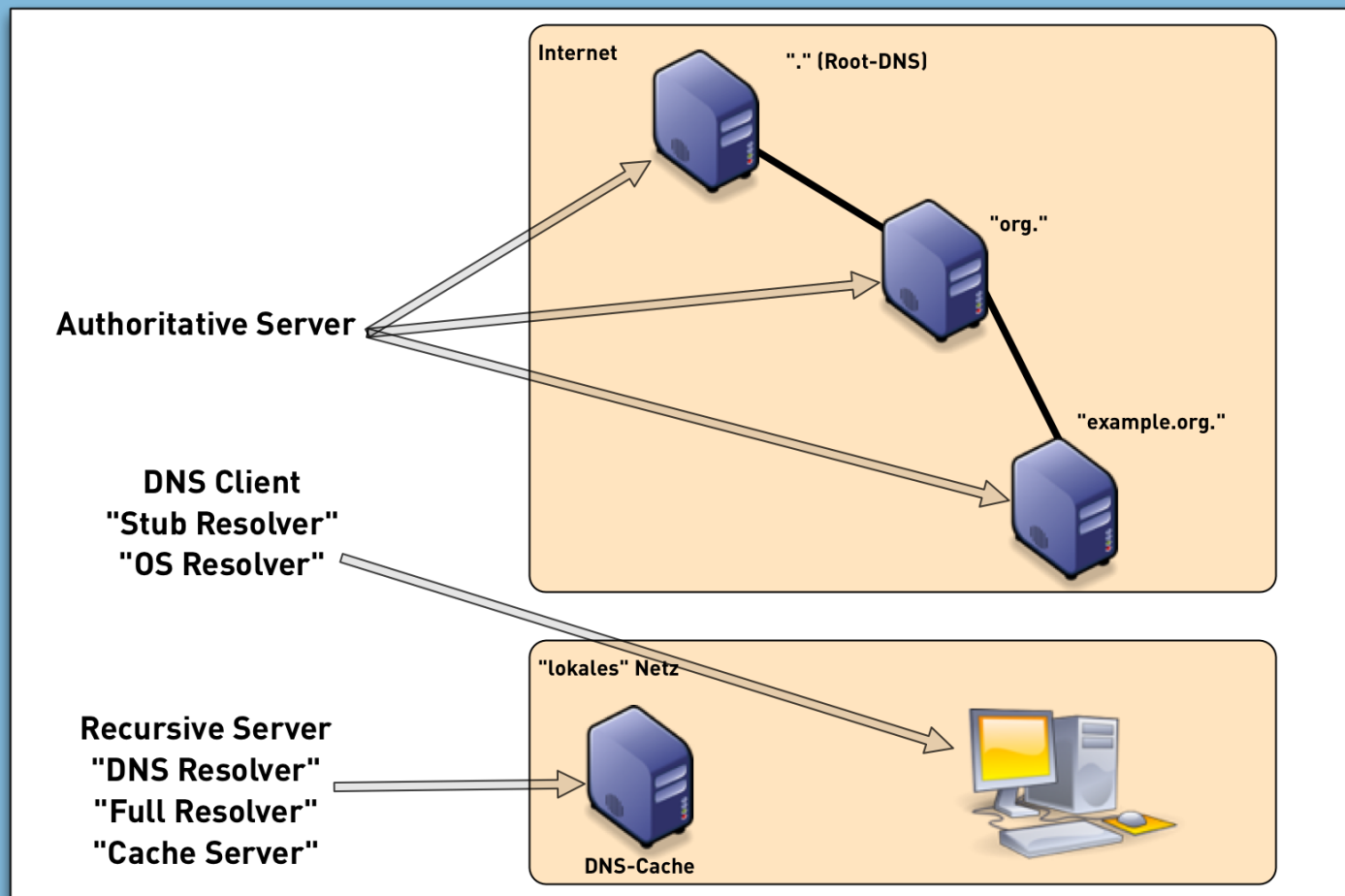
DNS Namensraum



foxtrott.charlie.alfa.

Internet Namensraum





DNS Komponenten - Hybrid-DNS

BIND 4 (End of Life)
BIND 8 (End of Life)
BIND 9
Windows DNS

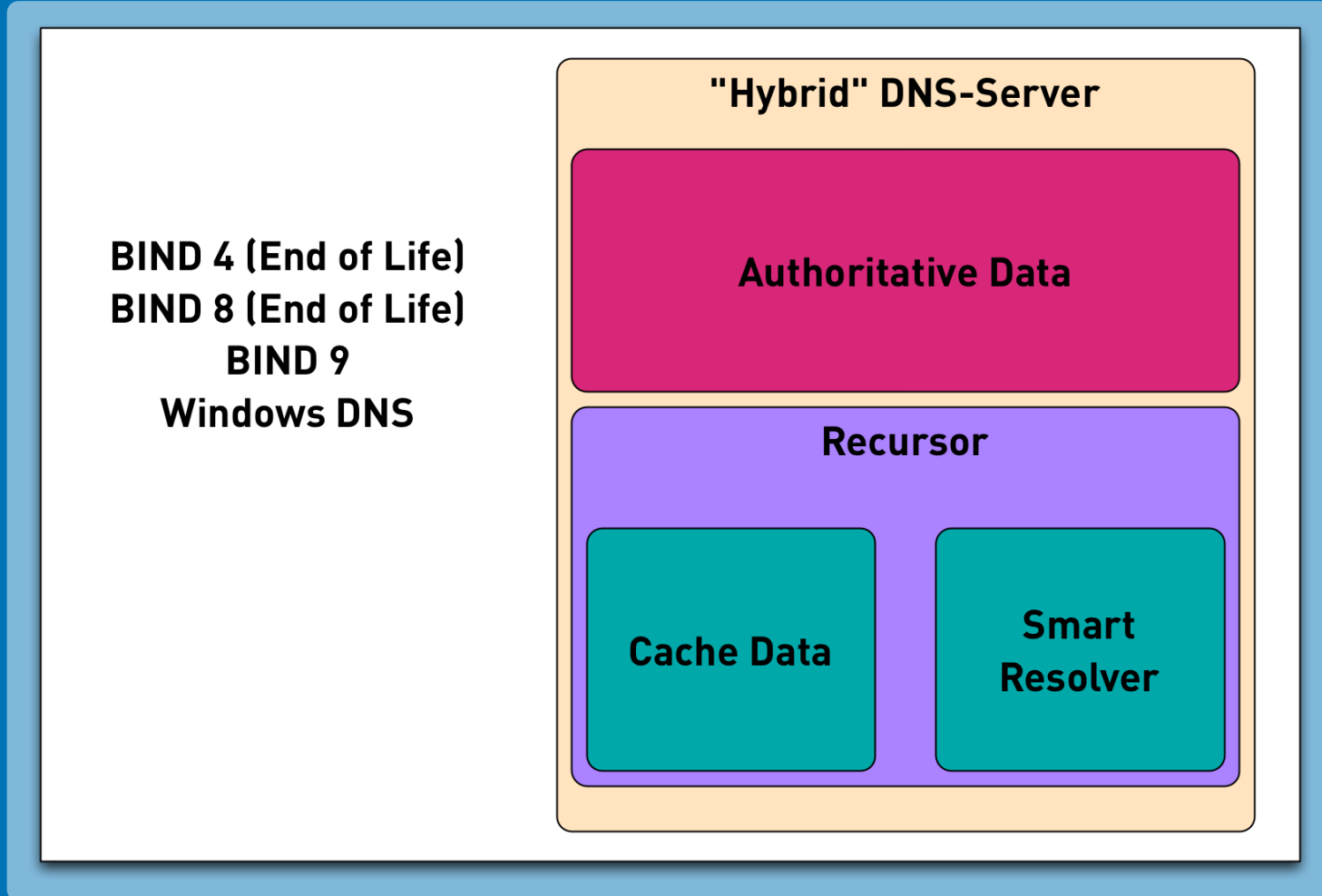
"Hybrid" DNS-Server

Authoritative Data

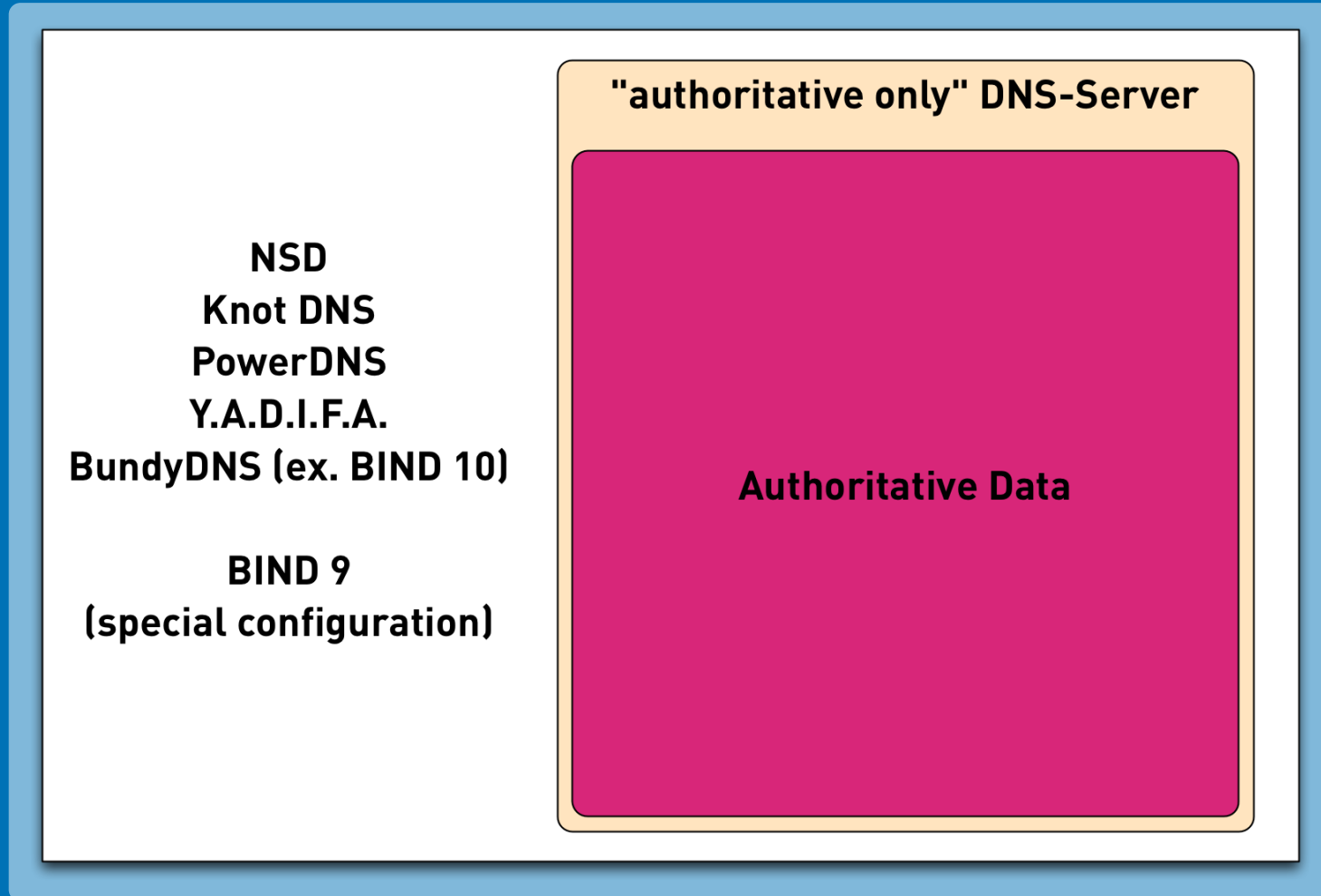
Recursor

Cache Data

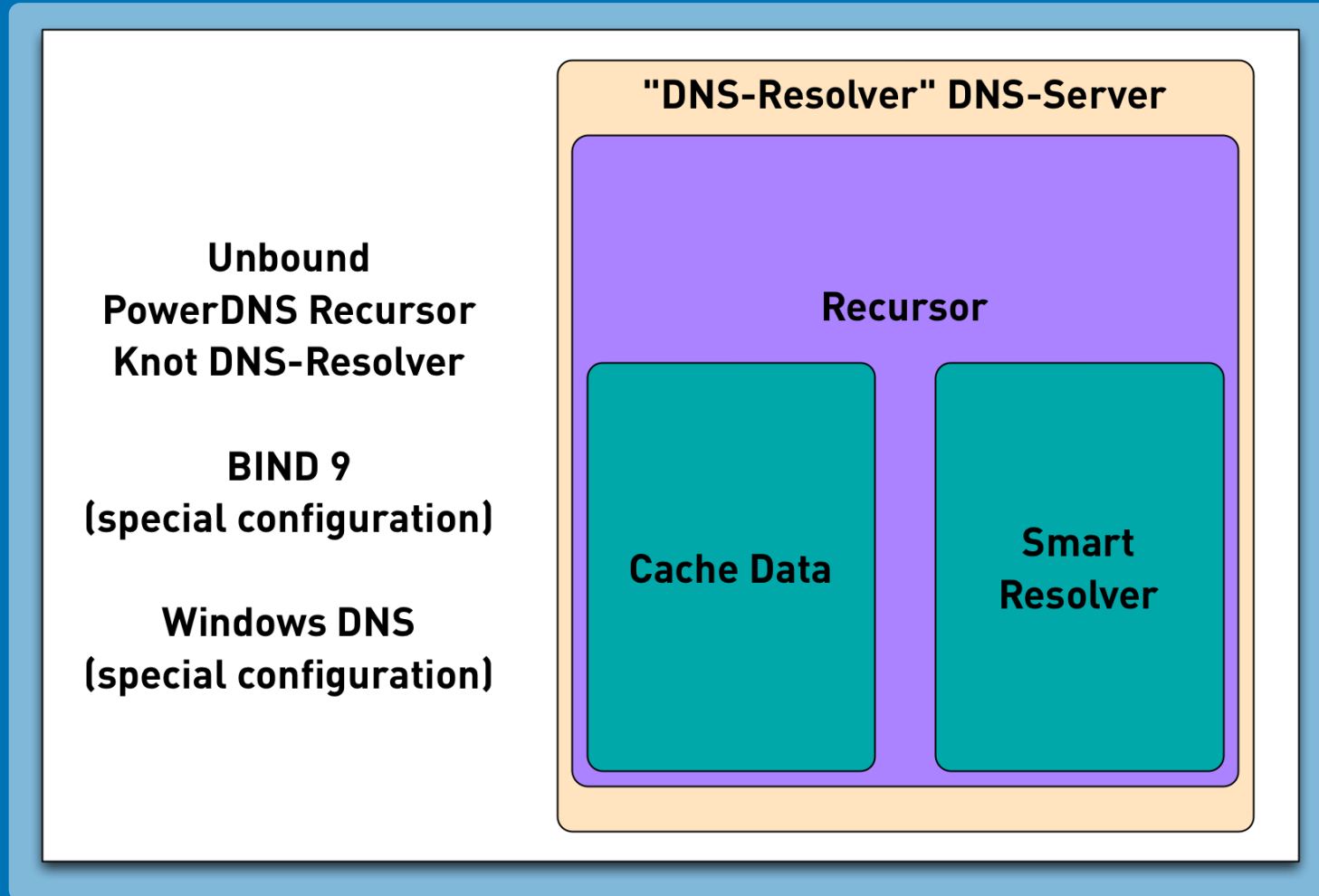
**Smart
Resolver**



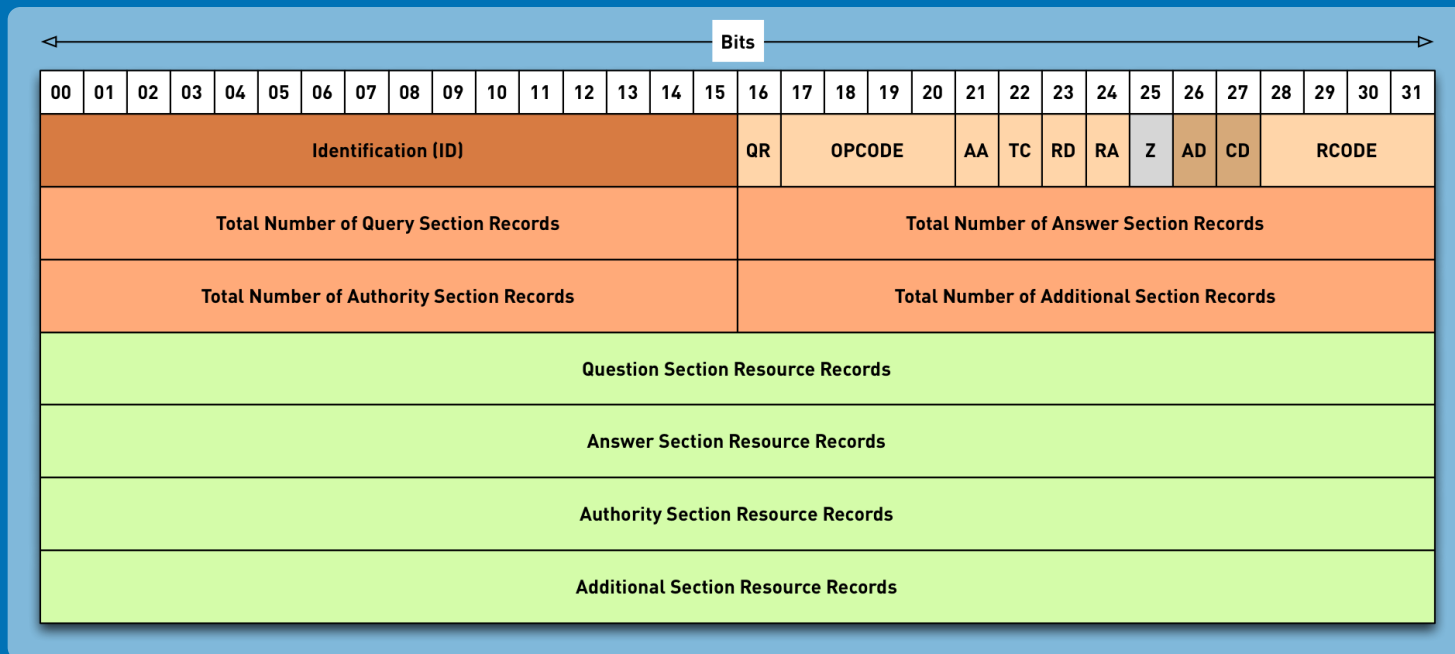
DNS Komponenten - Authoritative Only



DNS Komponenten - DNS Resolver



DNS Paketformat



DNS Resource Records

SOA Record

```
example.com. 3600 IN SOA dns1.example.org. (  
    hostmaster.example.com.  
    2016012504 ; serial  
    86400      ; refresh  
    7200       ; retry  
    3600000    ; expire  
    3600 )     ; negTTL
```

Negatives Caching

- Der letzte Wert im SOA-Record bestimmt (zusammen mit dem TTL-Wert des SOA-Records, kleinster Wert wird benutzt), wie lange negative DNS-Antworten im Cache gehalten werden
- Negative DNS-Antworten sind NXDOMAIN und NXRRSET/NODATA
- Fehlerzustände (SERVFAIL, FORMERR, REFUSED ...) werden nicht im DNS-Cache gespeichert

NS-Record

```
example.com. 3600 IN NS dns1.example.org.  
example.com. 3600 IN NS dns2.example.info.  
example.com. 3600 IN NS dns3.example.com.
```

NS-Record

- NS-Records erzeugen die DNS-Delegation
- Die NS-Records in der Eltern-Zone müssen mit den NS-Records in der delegierten "Kind" Zone übereinstimmen
- Liegt der Name eines delegierten DNS-Servers innerhalb der delegierten Zone, so müssen in der Eltern-Zone "Glue-Records" eingefügt werden

Glue (1)

```
example.com. 3600 IN NS dns1.example.org.  
example.com. 3600 IN NS dns2.example.info.  
example.com. 3600 IN NS dns3.example.com.
```

Glue (2)

```
example.com. 3600 IN NS dns1.example.org.  
example.com. 3600 IN NS dns2.example.info.  
example.com. 3600 IN NS dns3.example.com.
```

```
dns3.example.com. 3600 IN AAAA 2001:db8::53  
dns3.example.com. 3600 IN A 192.0.2.53
```

Ende DNS 1x1 - Fragen?
