



Hands on **DNS** Basics part 2



Online for **NOMINET**
20-24 September 2021

The material in these slides is based on Karst Koymans' CIA course material, see: <https://www.os3.nl/2020-2021/courses/cia/start>

Concepts

- **Domain Name Space**

- Organised as a (domain name) tree

- **Resource Records**

- The actual DNS data

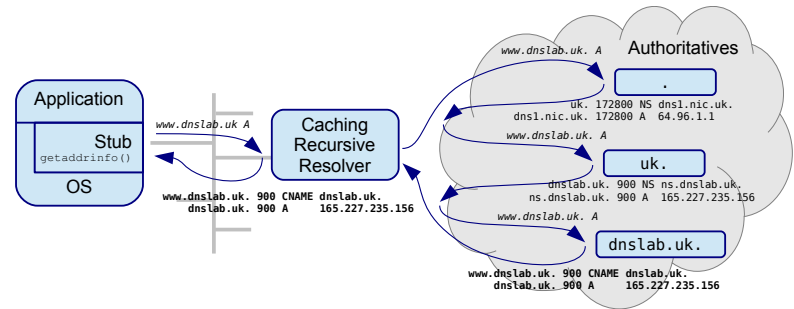
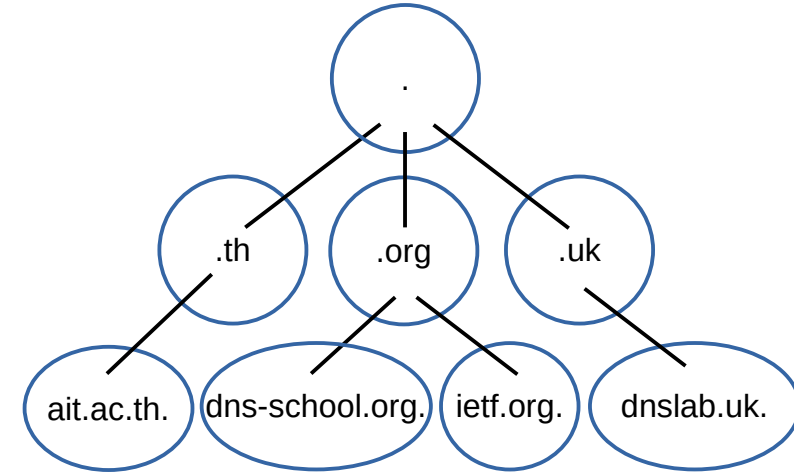
- **Resolvers**

- Send queries to name servers

(Client)

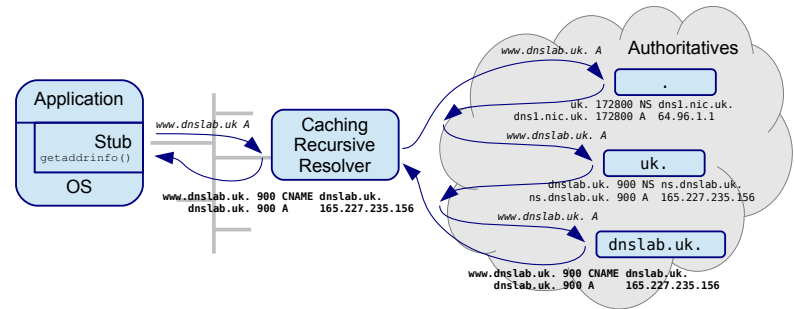
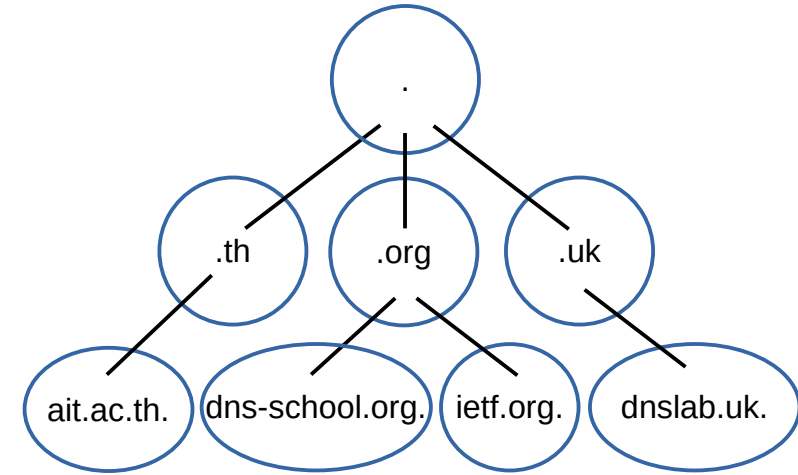
- **Name Servers**

- Send responses to resolvers (Server)



Concepts

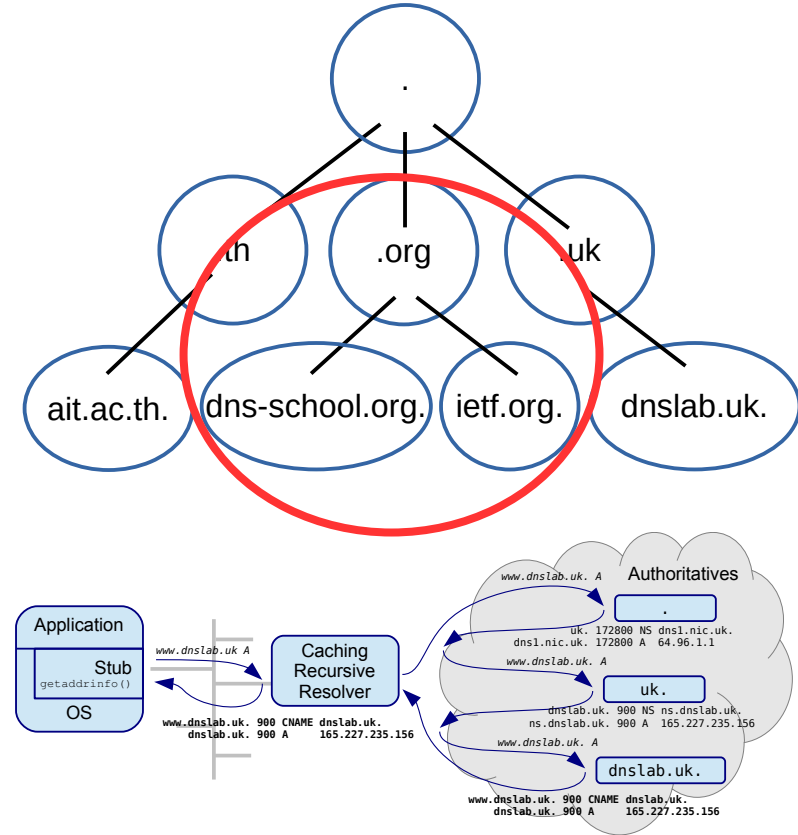
- **Label** – uk
 - the name between the dots
 - root label is empty! “”
- **Domain name** – dnslab.uk
 - A sequence of labels
 - **Fully Qualified Domain Name (fqdn)** – dnslab.uk.
 - Relative Domain Name
 - res-0
 - res-0.do



Concepts

- **Domain**

- A domain name together with all domain names below



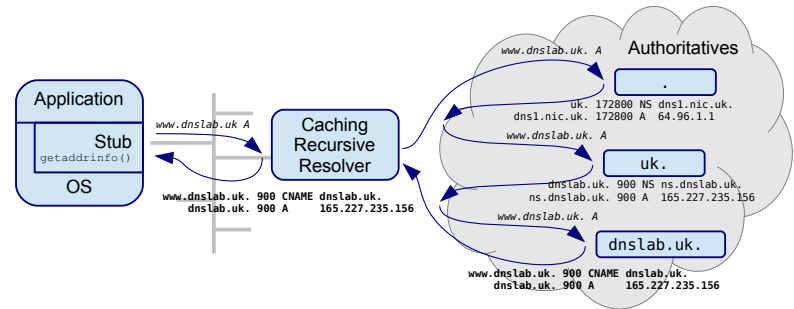
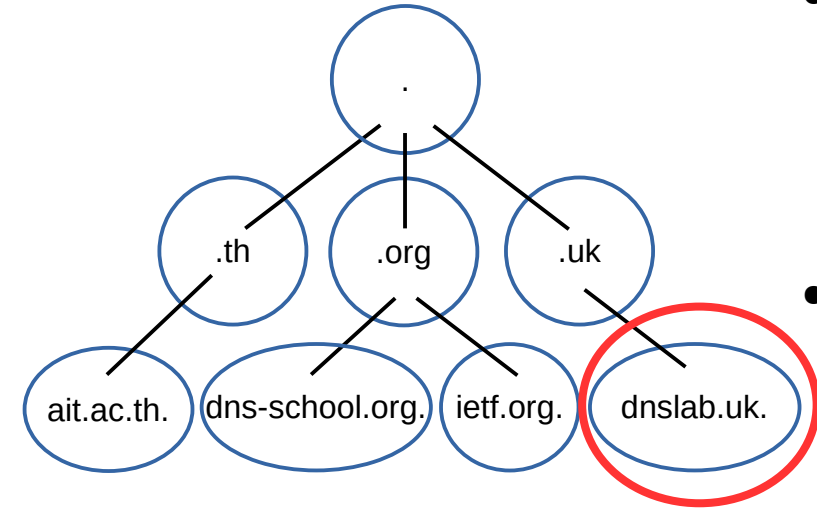
Concepts

- **Domain**

- A domain name together with all domain names below

- **Zone**

- Organization unit of Authoritative Information



Apex → dnslab.uk.
ns.dnslab.uk.
www.dnslab.uk.

Concepts

- **Domain**

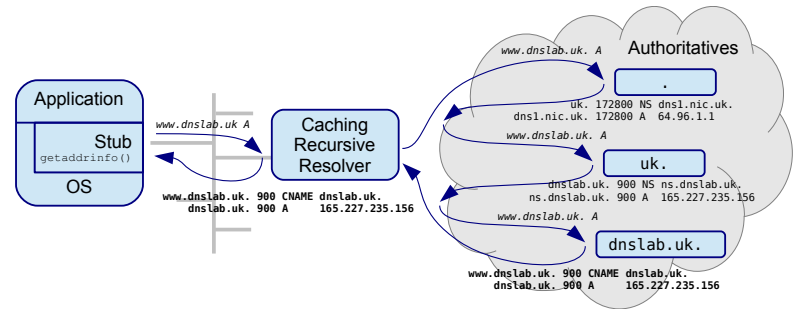
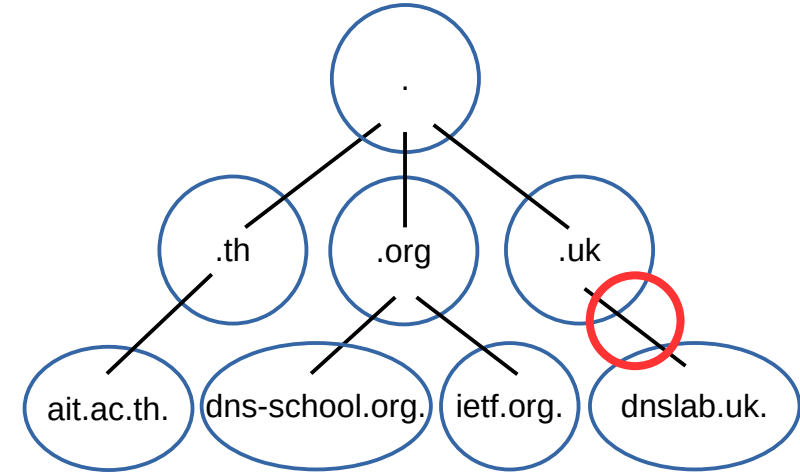
- A domain name together with all domain names below

- **Zone**

- Organization unit of Authoritative Information

- **Delegation**

- Delegation of authority via **Referral** at the **Zone Cut** from a **Parent** to a **Child**



Resource Records (RRs)

- Owner
 - dnslab.uk.
- TTL
- Class
 - IN, CH, HS
- Type
 - A, AAAA, CNAME, etc...
- Resource data (RDATA)
 - depends on type

```
$ drill dnslab.uk A
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 1
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY:
;; QUESTION SECTION:
;; dnslab.uk.IN A

;; ANSWER SECTION:
dnslab.uk. 300 IN A 165.227.235.156

;; Query time: 4 msec
;; SERVER: 2a04:b900:0:100::38
;; WHEN: Sat Sep 18 08:22:13 2021
;; MSG SIZE rcvd: 134
```

Resource Record Set (RRset)

- A set of RRs with same
 - Owner name
 - Class
 - Typebut with different
 - RDATA

```
$ drill dnslab.uk NS
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 4
;; flags: qr rd ra ; QUERY: 1, ANSWER: 2, AUTHORITY:
;; QUESTION SECTION:
;; dnslab.uk.IN  NS

;; ANSWER SECTION:
dnslab.uk. 300 IN  NS  ns.dnslab.uk.
dnslab.uk. 300 IN  NS  ns.nlnetlabs.org.

;; Query time: 17 msec
;; SERVER: 2a04:b900:0:100::38
;; WHEN: Sat Sep 18 08:21:56 2021
;; MSG SIZE  rcvd: 118
```


A record

- Name → IPv4 address
- Can be more than 1

```
$ drill thnic.co.th
;; ->HEADER<- opcode: QUERY, rcode: NOERROR, id: 4
;; flags: qr rd ra ; QUERY: 1, ANSWER: 2, AUTHORITY:
;; QUESTION SECTION:
;; thnic.co.th.   IN   A

;; ANSWER SECTION:
nominet.uk.      300 IN  A    104.16.187.108
nominet.uk.      300 IN  A    104.16.188.108

;; Query time: 10 msec
;; SERVER: 2a04:b900:0:100::38
;; WHEN: Sat Sep 18 08:21:32 2021
;; MSG SIZE  rcvd: 60
```

AAAA record

- Name → IPv6 address
- a.k.a. Quad-A
- Common to be > 1

```
$ drill dnslab.uk AAAA
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 5
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY:
;; QUESTION SECTION:
;; dnslab.uk.IN AAAA

;; ANSWER SECTION:
dnslab.uk. 857 IN AAAA 2a03:b0c0:1:d0::c0b:3001

;; Query time: 2 msec
;; SERVER: 2a04:b900:0:100::38
;; WHEN: Sat Sep 18 08:21:00 2021
;; MSG SIZE rcvd: 146
```

CNAME record

- Name → Canonical Name
- **No other RRs at the same Owner!**
 - Service referrals: SRV SVCB HTTPS
- No subdomains
 - Use DNAME for that

```
$ drill www.dnslab.uk A
;; ->HEADER<- opcode: QUERY, rcode: NOERROR, id: 3
;; flags: qr rd ra ; QUERY: 1, ANSWER: 2, AUTHORITY:
;; QUESTION SECTION:
;; www.dnslab.uk. IN  A

;; ANSWER SECTION:
www.dnslab.uk. 900 IN  CNAME  dnslab.uk.
dnslab.uk.      622 IN  A      165.227.235.156

;; Query time: 28 msec
;; SERVER: 2a04:b900:0:100::38
;; WHEN: Sat Sep 18 08:20:27 2021
;; MSG SIZE rcvd: 152
```

PTR record

- [illegible]

MX record

- Mail Exchange
- 1st RDATA field
 - Priority
- 2nd RDATA field
 - SMTP server for the domain

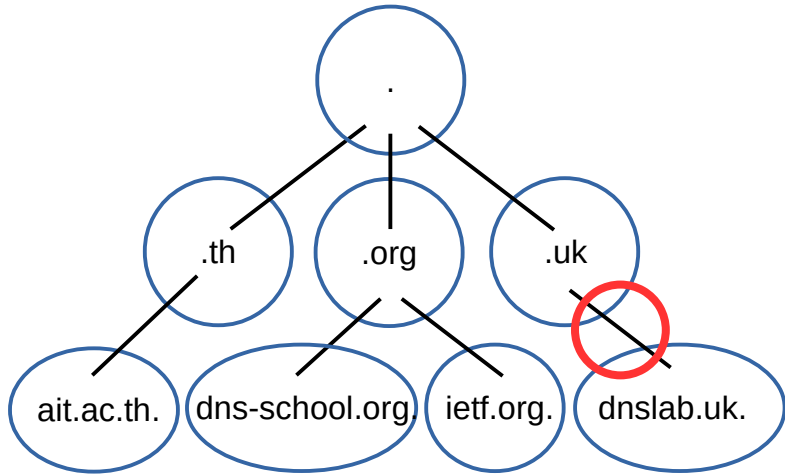
```
$ drill nominet.uk MX
;; ->>HEADER<- opcode: QUERY, rcode: NOERROR, id: 1
;; flags: qr rd ra ; QUERY: 1, ANSWER: 7, AUTHORITY:
;; QUESTION SECTION:
;; mail.in.th.      IN      MX

;; ANSWER SECTION:
nominet.uk.  300 IN      MX      10 mx1.nominet.org.uk.
nominet.uk.  300 IN      MX      10 mx2.nominet.org.uk.

;; Query time: 19 msec
;; SERVER: 2a04:b900:0:100::38
;; WHEN: Sat Sep 18 08:18:55 2021
;; MSG SIZE rcvd: 80
```

NS record

- Name Server
 - Delegates Authority
 - Make DNS Decentralized
- In both Parent & Child!



```
$ drill @213.248.216.1 dnslab.uk NS
;; ->HEADER<- opcode: QUERY, rcode: NOERROR, id:
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY:
;; QUESTION SECTION:
;; dnslab.uk.IN  NS

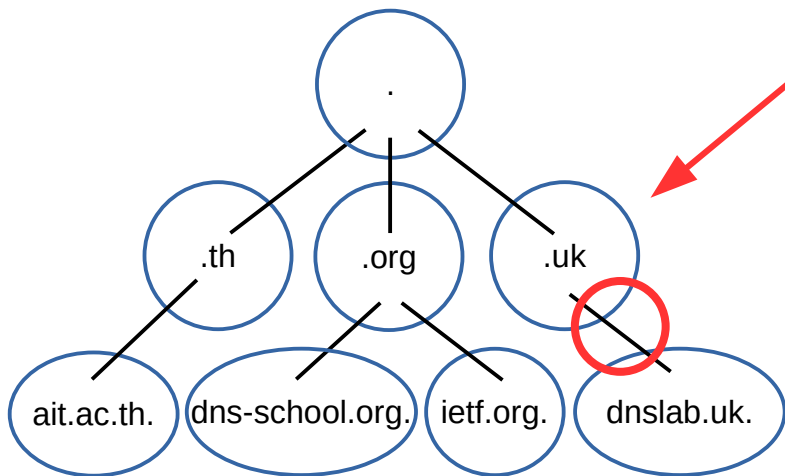
;; ANSWER SECTION:

;; AUTHORITY SECTION:
dnslab.uk. 900 IN      NS  ns.dnslab.uk.
dnslab.uk. 900 IN      NS  ns.nlnetlabs.org.

;; ADDITIONAL SECTION:
ns.dnslab.uk.900 IN  A    165.227.235.156
ns.dnslab.uk.900 IN  AAAA ...
```

NS record

- Name Server
- **Glue**
 - “in bailiwick”
 - Not authoritative



```
$ drill @213.248.216.1 dnslab.uk NS
;; ->HEADER<- opcode: QUERY, rcode: NOERROR, id:
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY:
;; QUESTION SECTION:
;; dnslab.uk.IN NS

;; ANSWER SECTION:

;; AUTHORITY SECTION:
dnslab.uk. 900 IN NS ns.dnslab.uk.
dnslab.uk. 900 IN NS ns.nlnetlabs.org.

;; ADDITIONAL SECTION:
ns.dnslab.uk. 900 IN A 167.227.235.156
ns.dnslab.uk. 900 IN AAAA ...
```

SOA record

- **Start Of Authority**
- Administrates zone parameters
 - Primary server
 - Email address
 - Version of Zone
 - Control Plane parameters for *secondary servers*

```
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 1
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY:
;; QUESTION SECTION:
;; dnslab.uk.IN SOA

;; ANSWER SECTION:
dnslab.uk. 0 IN SOA ns.dnslab.uk. (
                                sysadm.nlnet.nl.
                                2019050418 ; serial
                                28800      ; refresh (8 hours)
                                14400      ; retry (4 hours)
                                604800     ; expire (1 week)
                                86400      ; minimum (1 day)
                                )
```


SOA record

- **Start Of Authority**
- Administrates zone parameters
 - Primary server
 - Email address
 - Version of Zone
 - Control Plane parameters for *secondary servers*

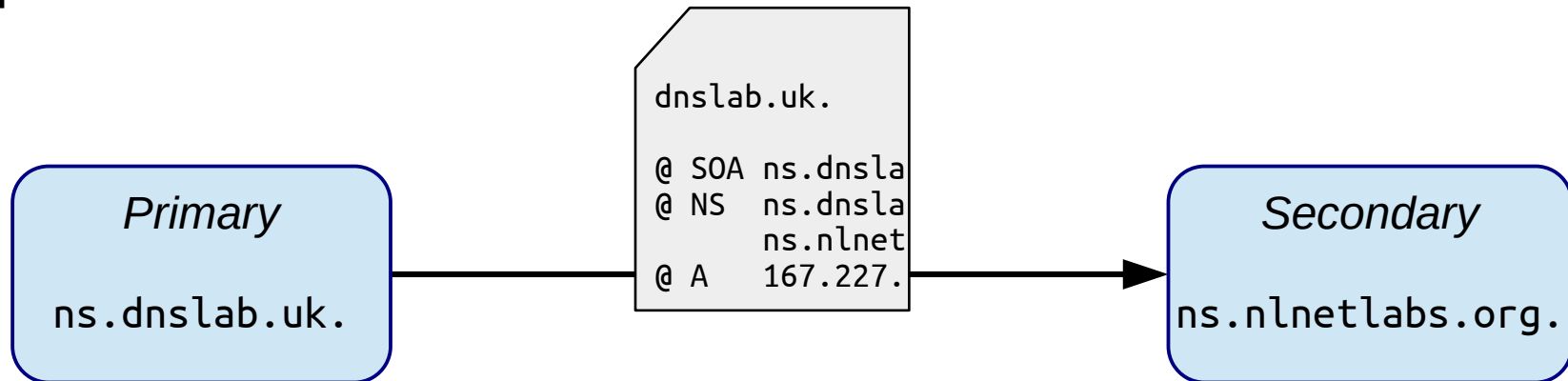
```
$ dig dnslab.uk SOA +multiline
```

```
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 1
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY:
;; QUESTION SECTION:
;; dnslab.uk.IN SOA
```

```
;; ANSWER SECTION:
dnslab.uk. 199 IN SOA ns.dnslab.uk. (
    hostmaster.dnslab.uk.
    2021091602 ; serial
    28800      ; refresh (8 hours)
    14400      ; retry (4 hours)
    604800     ; expire (1 week)
    60         ; minimum (1 minute)
)
```

Name server types

- Master – Primary
- Hidden Primary / Hidden Master
- Secondary
- Stealth
- Lame



Zone file

\$ORIGIN dnslab.uk.

\$TTL 300

@ IN SOA ns hostmaster.dnslab.uk. (
2021091602 ; serial
28800 ; refresh (8 hours)
14400 ; retry (4 hours)
604800 ; expire (1 week)
60 ; minimum (1 minute)
)

IN NS ns

IN NS ns.nlnetlabs.org.

ns IN AAAA 2a03:b0c0:1:d0::c0b:3001

IN A 165.227.235.156

@ IN AAAA 2a03:b0c0:1:d0::c0b:3001

IN A 165.227.235.156

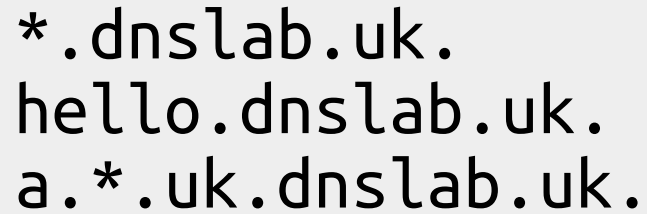
www IN CNAME @

Wildcard records

- RR that can be used for all matching query names
- Leftmost label is '*'
- **Only** matches when wildcard label is directly below longest match

Wildcard records

- welcome.dnslab.uk.
 - Wildcard match
- hello.dnslab.uk.
 - **No** wildcard match
- welcome.hello.dnslab.uk.
 - **No** wildcard match
- something.uk.dnslab.uk.
 - Wildcard match on *.uk.dnslab.uk. (ENT)



```
*.dnslab.uk.  
hello.dnslab.uk.  
a.*.uk.dnslab.uk.
```

Lab time!



- Hands on: <https://dnslab.uk/>
- 2. Set up an Authoritative Name Server