

# Internets domännamnssystem\*

Föreläsning FL02, VT 2024

Mats Dufberg

\* Se [“Internets domännamnssystem”](#)

# Innehåll

- [▶ Kort sammanfattning av FL01](#)
- [▶ Fullständigt domännamn \(FQDN\)](#)
- [▶ Tecken i domännamn](#)
- [▶ Var finns DNS-datat?](#)
- [▶ DNS-zoner](#)
- [▶ Domännamn kontra zon](#)
- [▶ DNS-anrop och DNS-paket](#)
- [▶ Stub resolver](#)
- [▶ Manuella DNS-frågor och "dig"](#)
- [▶ Posttyp MX](#)
- [▶ Posttyp CNAME](#)
- [▶ Posttyp NS och delegering](#)
- [▶ Posttyp SOA](#)
- [▶ Posttyper och begränsningar](#)
- [▶ Zonfiler med DNS-poster](#)
- [▶ Roller hos namnservrar](#)
- [▶ Uppslagning via resolver](#)
- [▶ Om presentationen](#)

# ▶ Kort sammanfattning av FL01

[\[ Till innehåll \]](#)

# Sammanfattning så här långt

- DNS används bl.a. för att slå upp IP-adresser för domännamn.
- Domännamnet är mer än bara en IP-adress.
- Domännamnet är en del av ett namnträd.
- DNS-datat, som vi kan slå upp, kopplas till en viss punkt i domänträdet.
- Det finns olika posttyper för olika data, bl.a. A, AAAA och TXT.

# ► Fullständigt domännamn (FQDN)

[\[ Till innehåll \]](#)

# Fullständiga och relativa domännamn

I DNS och namnservrar:

`www.iis.se.` – fullständigt namn (med avslutande punkt)

`www.iis.se` – relativt namn (utan avslutande punkt)

I URI:er så är namnet fullständigt utan avslutande punkt:

`mailto:nisse@kth.se` (mailadressen `nisse@kth.se`)

`https://www.kth.se/`

`sip:nisse@kth.se` (sip-adress för IP-telefoni)

I konfigurationsfiler för olika program (utom DNS) så är fullständiga domännamn normalt utan avslutande punkt.

Vi kommer att se att den avslutande punkten är viktig i DNS.

# FQDN

FQDN = Fully qualified domain name

Fullständigt domännamn upp till rot, med eller utan avslutande punkt (beroende på kontext).



# ► Tecken i domännamn

[\[ Till innehåll \]](#)

# Tecken i domännamn

DNS-paketerna har oktetter (koder om 8 bitar) i namnsträngarna, men som tecken är det bara ASCII (7 bitar).

Vi kommer bara att beröra namnsträngar med tecken, vilket är det normala.

Teckenjämförelsen är skiftlägesokänslig ("case insensitive"), d.v.s. "a" == "A", "b" == "B".

# Teckenuppsättningen ASCII (decimalt)

0 nul	1 soh	2 stx	3 etx	4 eot	5 enq	6 ack	7 bel
8 bs	9 ht	10 nl	11 vt	12 np	13 cr	14 so	15 si
16 dle	17 dc1	18 dc2	19 dc3	20 dc4	21 nak	22 syn	23 etb
24 can	25 em	26 sub	27 esc	28 fs	29 gs	30 rs	31 us
32 sp	33 !	34 "	35 #	36 \$	37 %	38 &	39 '
40 (	41 )	42 *	43 +	44 ,	45 -	46 .	47 /
48 0	49 1	50 2	51 3	52 4	53 5	54 6	55 7
56 8	57 9	58 :	59 ;	60 <	61 =	62 >	63 ?
64 @	65 A	66 B	67 C	68 D	69 E	70 F	71 G
72 H	73 I	74 J	75 K	76 L	77 M	78 N	79 O
80 P	81 Q	82 R	83 S	84 T	85 U	86 V	87 W
88 X	89 Y	90 Z	91 [	92 \	93 ]	94 ^	95 _
96 `	97 a	98 b	99 c	100 d	101 e	102 f	103 g
104 h	105 i	106 j	107 k	108 l	109 m	110 n	111 o
112 p	113 q	114 r	115 s	116 t	117 u	118 v	119 w
120 x	121 y	122 z	123 {	124	125 }	126 ~	127 del

0-31: Styrkoder (inga skrivbara tecken)

32: Mellanslag (skrivbart tecken)

33-126: Skrivbara tecken

127: Styrkod (inget skrivbart tecken)

128-255: Odefinierade, ingår inte i ASCII (åttonde biten satt)

# Hostname

I DNS så är **hostname** ett domännamn som har minst en adresspost, A eller AAAA. Alltså nod med A eller AAAA eller båda.

T.ex.

– www.kth.se

som har både AAAA och A.

För en systemadministratör så är **hostname** kanske namnet på datorn, och då är det oftast första "label", d.v.s. "www" i detta fall.

# Tecken i domännamn

**Hostname** är begränsat till a-z, A-Z, 0-9, -

- Begränsningen gäller **label**, alltså namnet på noderna i DNS-trädet.
- Mellan två **label** har vi en punkt som markerar gränsen mellan noderna (**labels**).
- Rot är en specialnod med tom **label**

I **label** får ”-” inte stå varken först eller sist.

-aaa.kth.se	–	ej OK
aaa-.kth.se	–	ej OK
-aaa-.kth.se	–	ej OK
a-a-a.kth.se	–	OK

# Tecken i domännamn

- När man registrerar ett domännamn under t.ex. .se eller .com så gäller normalt samma begränsning som **hostname**.
- Detta gäller i praktiken även generellt för domännamn (alla noder/**labels**) som används
  - Några undantag kommer senare under kursen.

*Föreläsningen om IDN kommer att modifiera vissa påståenden om tecken i domännamn. Kommer senare i kursen.*

# ▶ Var finns DNS-datat?

[\[ Till innehåll \]](#)

# Var finns DNS-datat?

DNS är en nättjänst som är gemensam för Internet och tillgänglig för alla på Internet.

DNS är idag ett måste för Internet och TCP/IP. Innan DNS så fanns det en lista över alla datorer på Internet med namn och IP-adress. Det fungerar inte idag.

DNS är en gemensam databas över domännamn och dess data för hela Internet.

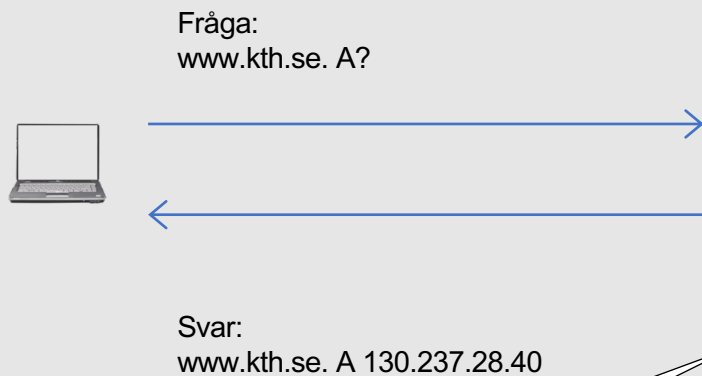


# Var finns DNS-datat?

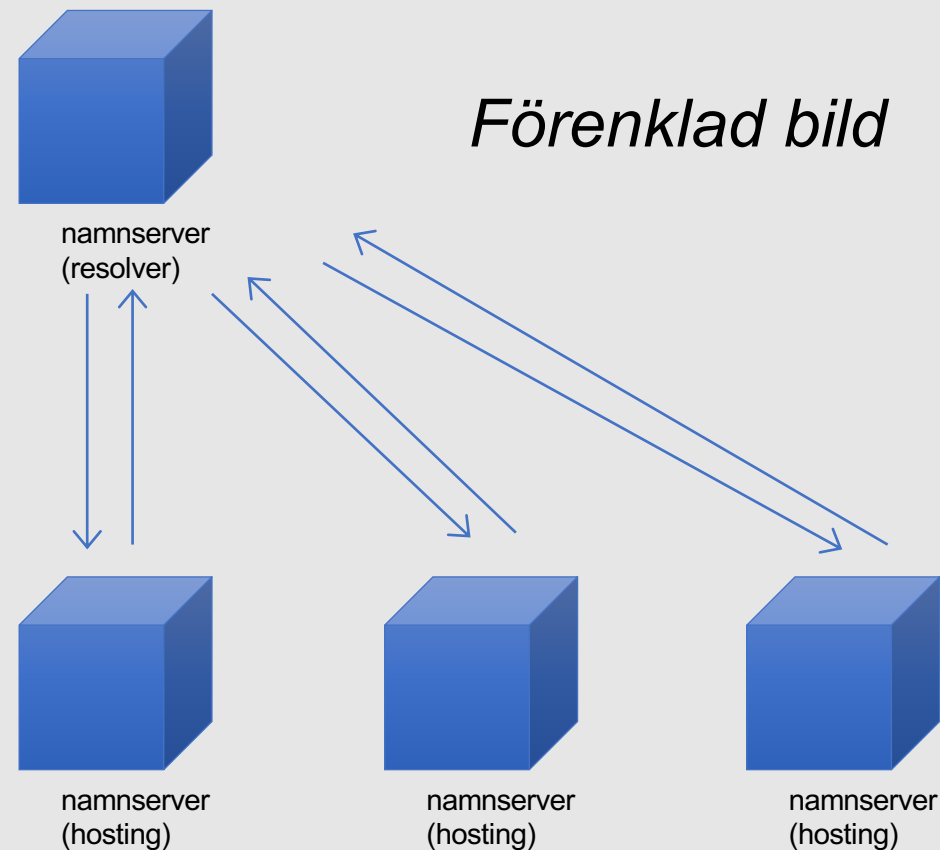
Den server som håller DNS-datat kallar vi en namnserver (***name server***) eller DNS-server.

Det finns två huvudtyper av namnservrar:

1. Hostingserver där vi publicerar datat
2. Resolver som hittar datat åt oss



Resolvern har inte datan från början utan hämtar den åt klienten



# ▶ DNS-zoner

[\[ Till innehåll \]](#)

# Zoner

Domännamnsträdet delas in i delar. En sådan del kallas zon (**zone**) och består av en nod i trädet och ev. underliggande noder. Zonen går ner till ev. underliggande zon.

Om det inte finns någon underliggande zon så är det resten av delträdet, d.v.s. allt som ligger i eller under zonens startnod.

Startnoden i t.ex. kth.se-zonen är noden "kth.se".

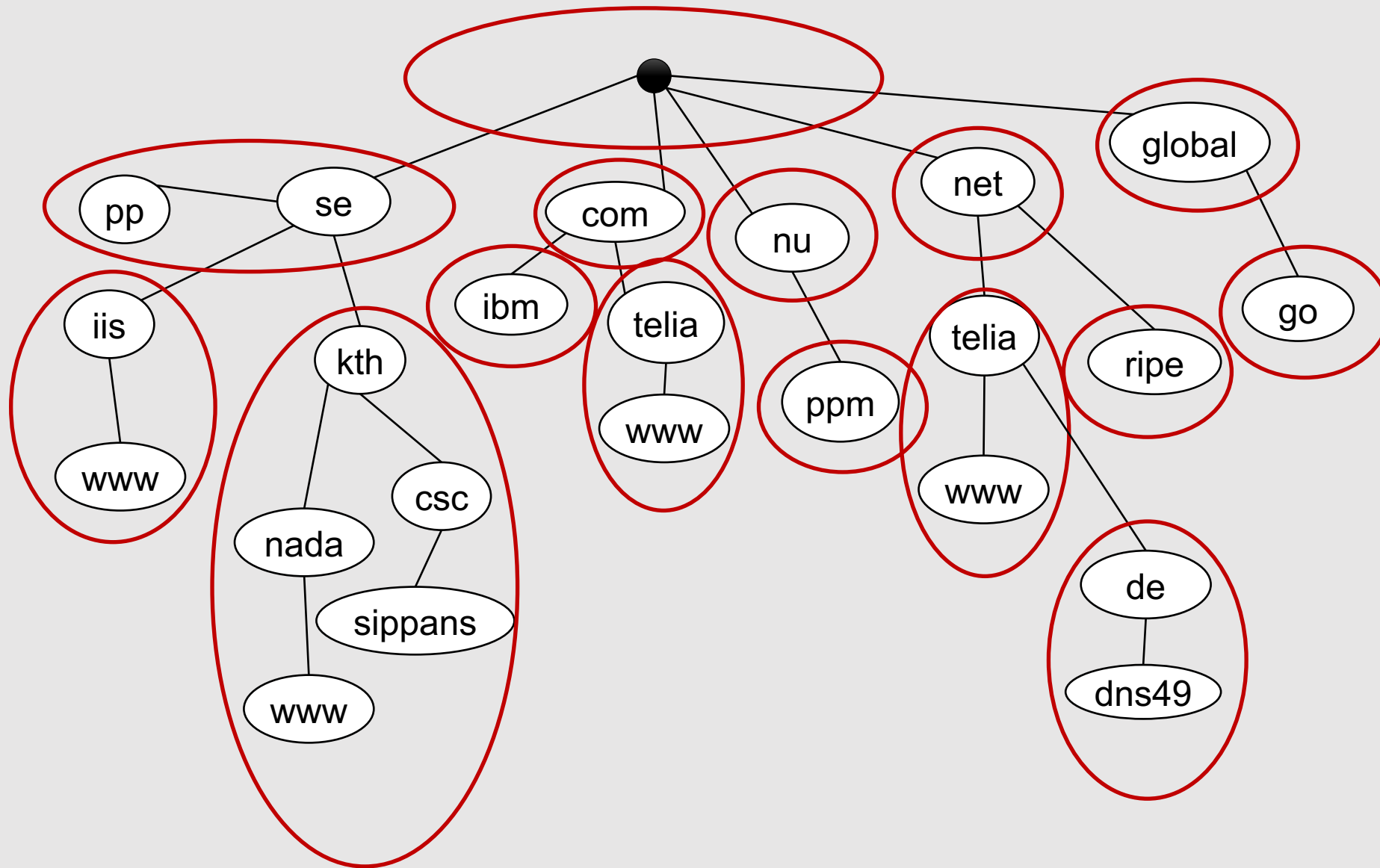
En zon skapas av en zonfil (konfigurationsfil) med det DNS-data som tillhör den zonen.

# Zoner

En zon är en administrative enhet. Var och en kan sköta sin zon (sin zonfil) för sitt domännamn.

Olika zoner kan ligga på olika namnservrar och kontrolleras av olika organisationer.

Två olika zoner kräver normalt två olika zonfiler.



# Zoner

För varje zon så finns det utpekade namnservrar (DNS-servrar) som håller innehållet i zonen (zonfilen).

Rot-zonen (***root zone***) är speciell för den är startpunkten för hela trädet.

# ► Domännamn kontra zon

[\[ Till innehåll \]](#)



# Olika betydelser av ”domännamn”

Varje namn i domännamnsträdet är ett domännamn (*domain name*).

Ofta används domän eller domännamn för att avse ett registrerat (domän-) namn, t.ex. kth.se. Med den vinkeln så är www.kth.se en del av kth.se-domänen.

*I DNS så är kth.se och www.kth.se två olika namn, olika domännamn, olika domäner.*

# Skillnad mellan domännamn och zon

Oftast så skapas en zon för varje registrerat domännamn, men det behöver inte vara så.

När man har ett eget domännamn så kan man välja att ha alla namn (noder) i samma zon. Eller så kan man skapa underliggande zoner som hanterar delar av namnrymden.

Ett domännamn är ett namn (en nod) i domännamnsträdet. En zon är en *administrativ del* – en avgränsad del av domännamnsträdet som administreras med en egen zonfil.

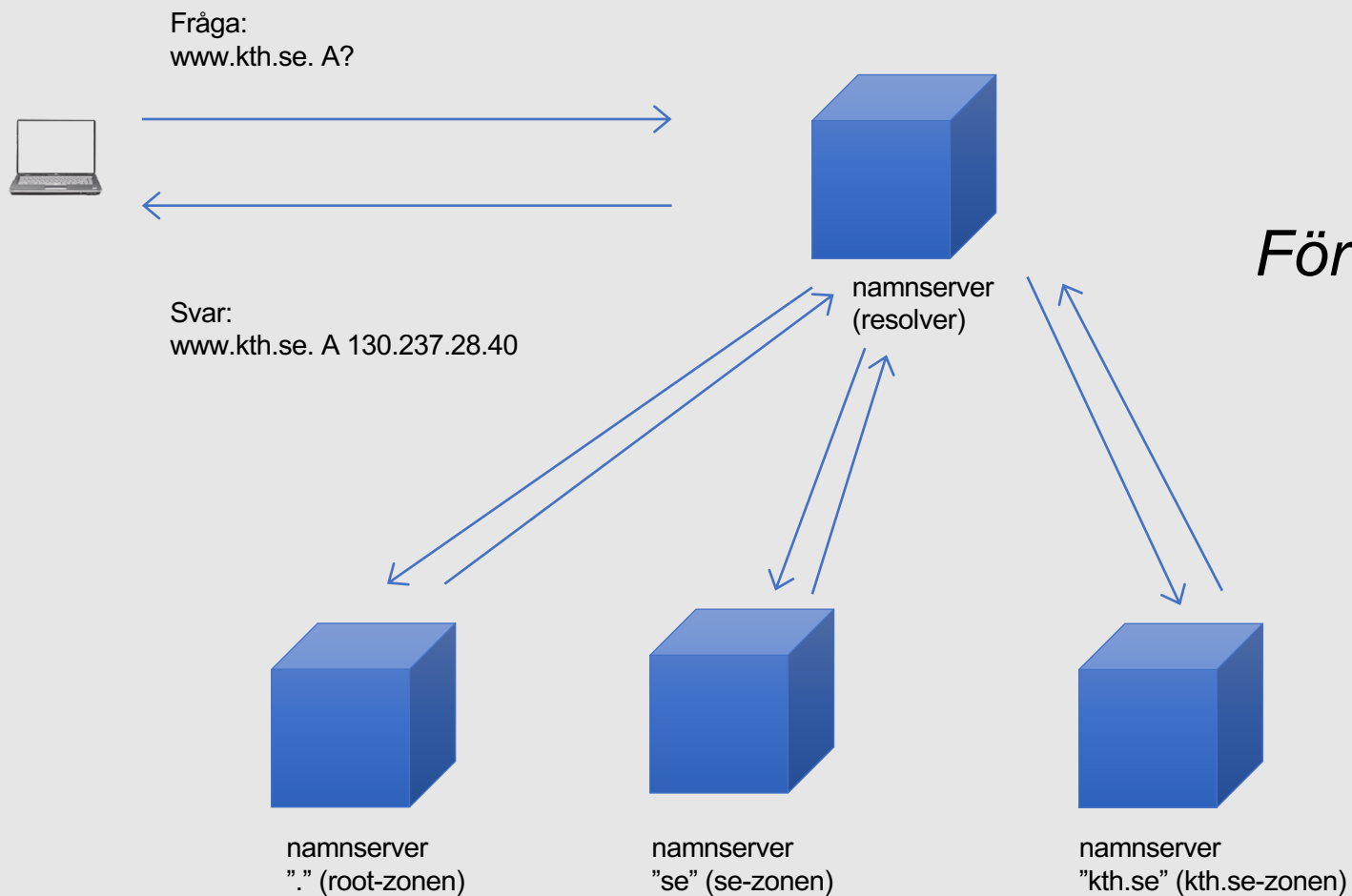
# ▶ DNS-anrop och DNS-paket

[\[ Till innehåll \]](#)

# Nätverkslager

Anrop till en namnserver görs över UDP eller TCP till port 53.

- Det vanligaste är att skicka DNS-frågor över UDP.
- En namnserver måste lyssna på både UDP och TCP.



*Förenklad bild*

# DNS-frågor från program

DNS-frågor initieras av alla möjliga program, nästan alla program som vill göra uppkoppling mot nätet. T.ex.

- webbläsare
- mailklient
- mailserver
- chatklient
- chatserver
- ping

Vart skickas dessa DNS-frågor?

# ▶ Stub resolver

[\[ Till innehåll \]](#)

# DNS-frågor från program

Program utnyttjar normalt biblioteksrutiner för att ställa DNS-frågor till vald namnserver (resolver). Biblioteksrutinerna kallas ofta för ***stub resolver***.

Valet av resolver blir då normalt gemensam för datorn och bestäms av konfiguration av ***stub resolver***.

Det är sedan denna som skickar frågorna vidare till en full DNS-resolver, och returnerar relevant information till programmet (applikationen).



# Program till *stub resolver*

Kommunikationen mellan program och *stub resolver* är inte egentlig DNS-kommunikation, utan intern kommunikation i programmet (*stub resolver* är inlänkad i programmet).

Kommunikationen är viktig för DNS-frågorna som skapas från ett program.

# Konfiguration av *stub resolver*

Alla system har filen "resolv.conf" under katalogen "etc" med inställningar för *stub resolver*.

I vissa system så är det den primära konfigurationen av *stub resolver*, i andra system så innehåller "resolv.conf" en kopia av vissa parametrar.

Alla system har möjlighet att ställa in hur *stub resolver* ska bete sig.

# Konfiguration av *stub resolver*

Exempel från traditionell Unix, men alla har motsvarande funktioner (och fler än vad som visas här).

```
$ cat /etc/resolv.conf
search iis.se prod.iis.se stage.iis.se
nameserver 172.17.41.10
nameserver 172.16.43.15
```

Datorn är konfigurerad att använder två namnservrar (full DNS-resolver) med IP-adresserna 172.17.41.10 resp. 172.16.43.15.

# Relativa namn och *search*

```
search iis.se prod.iis.se stage.iis.se
```

Search-listan styr hur stub resolver ska hantera relativa namn.

Programmet körs med ett namn som bara består av en "label", t.ex.:

```
$ ssh db3
```

"db3" troligen en lokal server, men det finns ingen absolut domän

"db3." utan det är ett relativt namn.

# Relativa namn och *search*

***stub resolver*** använder *search*-konfigurationen och skapar namn och skickar frågor om dem till resolvern (se *search*-listan på förra bilden). Frågorna skickas i följande ordning tills det blir ett positivt svar, eller sökalternativen tar slut. Vi antar IPv4 här.

1. db3.iis.se. A?
2. db3.prod.iis.se. A?
3. db3.stage.iis.se. A?
4. db3. A?

← Default när *search*-listan är uttömd.

# Relativa namn

Relativa namn kan fungera på ett lokalt nätverk. Allra bäst fungerar det om man bara har en sträng i search-listan. Om search-listan är lång så kan det bli många frågor. Om man skriver fel, så tar det längre tid innan man får svar.

Om det finns både "www.prod.iis.se" och "www.stage.iis.se" så kommer det relativa namnet "www" att vara beroende på ordningen i search-listan.

Vid felsökning, prova alltid med det absoluta namnet, både med och utan det avslutande punkt ".".

# Absoluta namn och *search*

Search-listan används inte om namnet avslutas med ".".

Search-listan används:

```
$ ssh db3
```

Search-listan används inte:

```
$ ssh db3.
```

# ***stub resolver***-information i Windows och MacOS

I Windows, starta "cmd.exe"

- I den, kör "ipconfig /all | more"
- I det som kommer upp, leta efter "DNS Servers".

I MacOS, så finns det hänvisning till kommandot "scutil --dns" från "/etc/resolv.conf".



# ▶ Manuella DNS-frågor och "dig"

[\[ Till innehåll \]](#)

# DNS-frågor från program

Ett program behöver inte använda den gemensamma ***stub resolver*** utan det kan använda annat bibliotek eller annan inställning för DNS-frågor.

Programmet "dig" som vi kommer att använda utnyttjar informationen i "resolv.conf", men väljer själv vilken DNS-server som den ska skicka frågorna till.

# Manuella DNS-frågor

Med verktyget "dig" så kan man ställa DNS-frågor och se hela svars paketet. Med "option" så kan man också se frågepaketet.

- Man kan välja vilken namnserver som man ska ställa DNS-frågan till.
- Man kan välja vad man frågar efter.
- Det finns olika flaggor att ställa in.

På labbarna så kommer vi att använda "dig" hela tiden. Och föreläsningarna kommer visa körningar av "dig" många gånger.

# Ställa DNS-frågor med "dig"

```
$ dig www.kth.se A

; <<>> DiG 9.10.6 <<>> www.kth.se
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11673
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.kth.se. IN A

;; ANSWER SECTION:
www.kth.se. 365 IN A 130.237.28.40

;; Query time: 109 msec
;; SERVER: 172.17.41.10#53(172.17.41.10)
;; WHEN: Mon Jan 14 17:04:21 CET 2019
;; MSG SIZE rcvd: 44
```

Fråga med "dig"

- Alltid "owner name" (default ".") och posttyp (default "A").
- Ev. dig-flaggor
- "dig" tolkar normalt "owner name" som absolut oavsett om den avslutas med punkt eller inte.

Frågan upprepad i svars paketet. Namnet är alltid absolut och avslutas alltid med punkt.

Svaret (om det finns ett svar)

Server IP + port (namnservern som svarade)

# Query, response, question och answer

**Query** är det som skickas till namnservern. I den finns alltid en **question** (i **question section**) plus flaggor m.m.

**Response** är det som kommer tillbaka från namnservern. I den upprepas **question** (i **question section**).

I **response** så *kan* det finns **answer** (i **answer section**), men det kan också vara tomt.

På svenska så blir det tyvärr ofta "fråga" för både **query** och **question** resp. "svar" för både **response** och **answer**.

# Response utan answer

```
$ dig www2.kth.se +mult
```

```
; <<>> DiG 9.10.6 <<>> www2.kth.se +mult  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 31963  
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
```

```
;; QUESTION SECTION:  
;www2.kth.se. IN A
```

```
;; AUTHORITY SECTION:  
kth.se. 891 IN SOA a.ns.kth.se. hostmaster.kth.se. (  
    2019011529 ; serial  
    14400      ; refresh (4 hours)  
    900       ; retry (15 minutes)  
    604800    ; expire (1 week)  
    86400     ; minimum (1 day)  
)
```

```
;; Query time: 115 msec  
;; SERVER: 172.17.41.10#53(172.17.41.10)  
;; WHEN: Wed Jan 16 10:39:20 CET 2019  
;; MSG SIZE rcvd: 81
```

"+mult" är en flagga till "dig" för att poster med mycket RDATA att visas på flera rader, t.ex. SOA.

Frågan, men det finns inget "answer" eftersom namnet www2.kth.se inte finns. ANSWER = 0

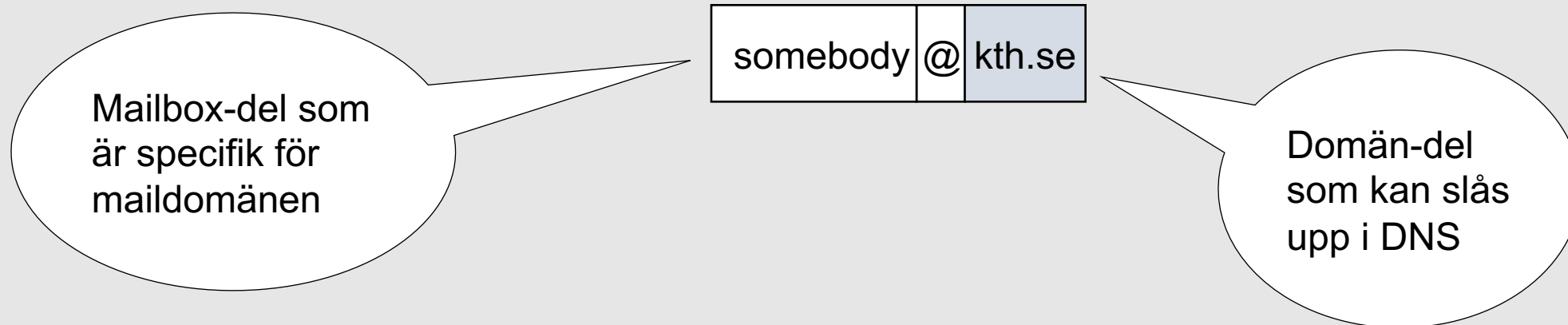
Kommandot "dig -h" ger en lista över flaggor till "dig".

# ► Posttyp MX

[\[ Till innehåll \]](#)

# Mail och DNS

Domändelen slås upp i DNS. Normalt med en speciell posttyp, MX.





# Posttyp MX

MX = "Mail Exchange"

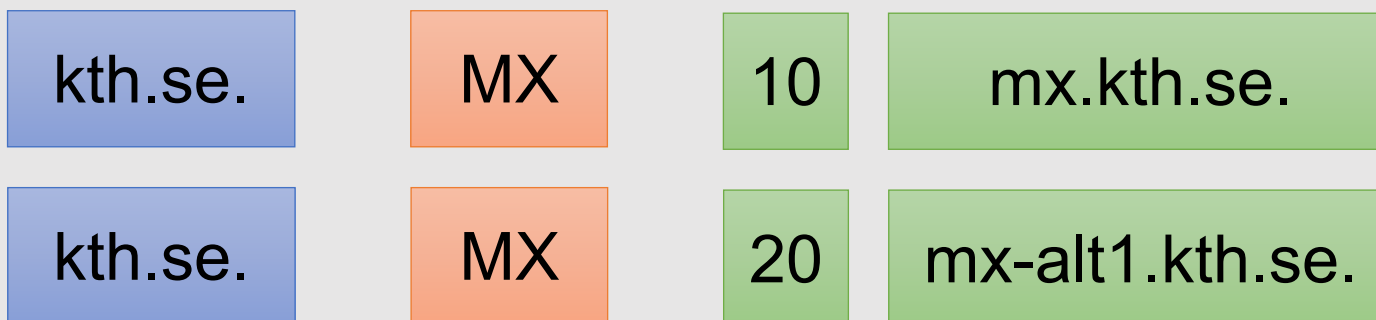
kth.se. MX 10 mx.kth.se.

kth.se. MX 20 mx-alt1.kth.se.

Owner name

Resource record type

Resource record data



Två delfält i "resource record data" för denna poststyp ("resource record type").

# Posttyp MX

Hur används MX?

- Ska skicka mail till nisse@kth.se
- Slå upp MX för kth.se.
- Hitta mailservern att skicka mailet till.

Ifall MX saknas för domändelen så görs en uppslagning av A och AAAA för samma namn för att hitta mottagande mailserver. Används sällan.

- Prioritet.
- Använd i första hand posten med **lägsta** värdet (i detta fall 10).

- Mailserver ("mail exchange").
- Slå upp A och AAAA för det angivna namnet för att hitta servern att skicka mail adresserad till "@kth.se".
- Måste vara ett "hostname" (ha A och/eller AAAA).

kth.se.	MX	10	mx.kth.se.
kth.se.	MX	20	mx-alt1.kth.se.

Alltid två delfält för MX.

# ► Posttyp CNAME

[\[ Till innehåll \]](#)

# Posttyp CNAME

Namn1 (d.v.s. *owner name*) är ett alias för namn2 (d.v.s. RDATA).

```
www.nada.kth.se. CNAME sippans.csc.kth.se.
```

”www.nada.kth.se” är ett alias för ”sippans.csc.kth.se”.

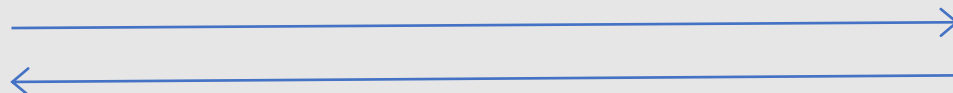
```
www.aftonbladet.se. CNAME www.aftonbladet.se.cdn.cloudflare.net.
```

”www.aftonbladet.se” är ett alias för  
”www.aftonbladet.se.cdn.cloudflare.net”.

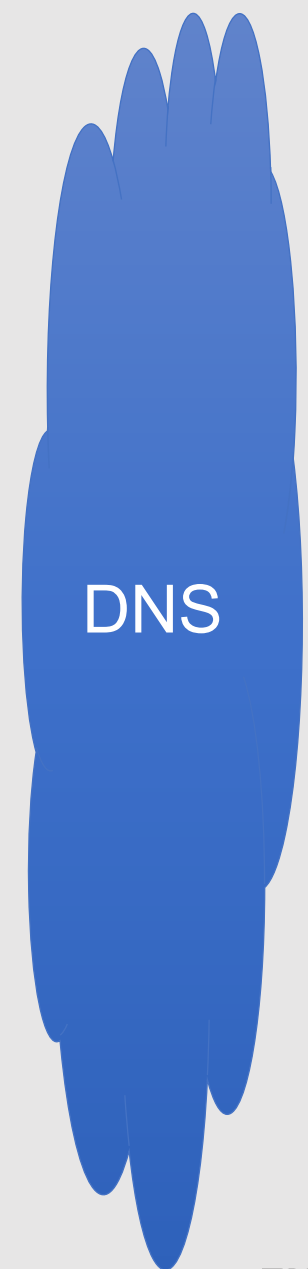
Med en fråga (allt i första svaret).  
CNAME och A finns i samma zon.



Fråga:  
www.nada.kth.se. A?



Svar:  
www.nada.kth.se. CNAME sippans.csc.kth.se.  
sippans.csc.kth.se. A 130.237.227.116



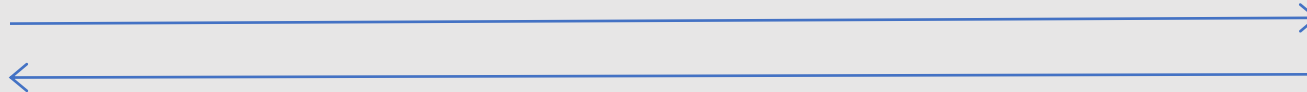
Med flera frågor.



1

Frågorna ställs till hosting-servrarna.  
CNAME och A finns i olika zoner.

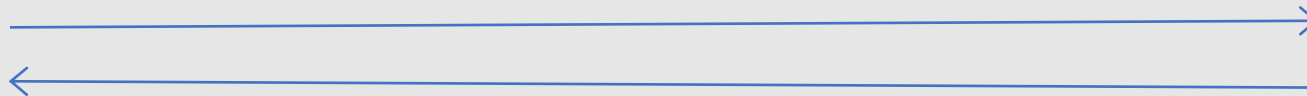
Fråga:  
www.aftonbladet.se. A?



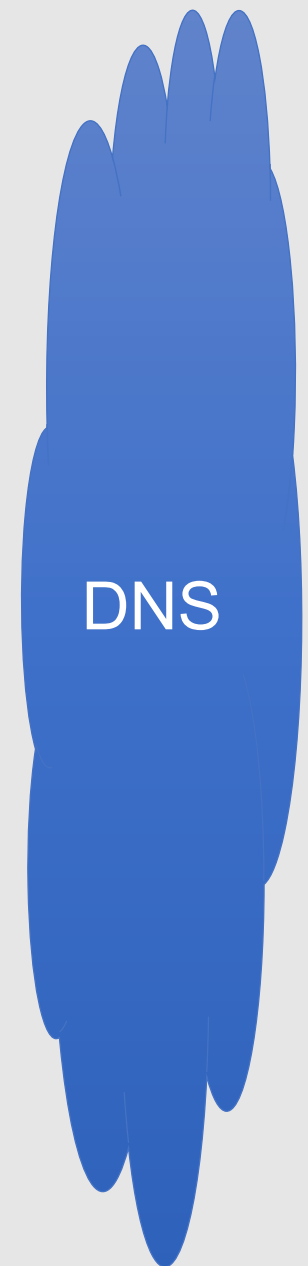
Svar:  
www.aftonbladet.se. CNAME www.aftonbladet.se.cdn.cloudflare.net.

2

Fråga:  
www.aftonbladet.se.cdn.cloudflare.net. A?



Svar:  
www.aftonbladet.se.cdn.cloudflare.net. A 104.20.54.70  
www.aftonbladet.se.cdn.cloudflare.net. A 104.20.55.70

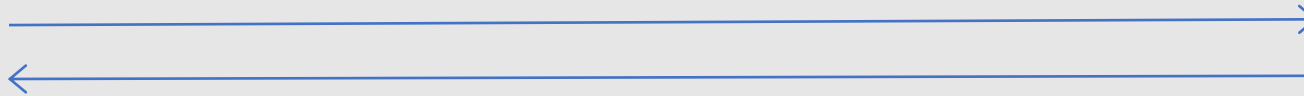


Med en fråga (allt i första svaret).



Frågorna ställs till resolver. Det spelar ingen roll att CNAME och A finns i olika zoner för resolvern samlar ihop svaren.

Fråga:  
www.aftonbladet.se. A?



Svar:

www.aftonbladet.se.	CNAME	www.aftonbladet.se.cdn.cloudflare.net.
www.aftonbladet.se.cdn.cloudflare.net.	A	104.20.54.70
www.aftonbladet.se.cdn.cloudflare.net.	A	104.20.55.70

DNS



Namnet vi vill ha svar på

www.nada.kth.se.

CNAME

Namnet vi hänvisas till

sippans.csc.kth.se.

# CNAME är speciellt 1

När DNS-frågan kommer till namnservern så kontrollerar den

1. Vilket namn gäller frågan?
2. Vilken posttyp gäller det?

*Normalt blir svaret tomt ifall namnservern inte har en DNS-post med samma namn och posttyp.*

**CNAME är ett undantag.** Ifall namnservern har en CNAME-post med rätt namn så finns den med i svaret.

Om namnet har CNAME så har namnet ingen annan data.

# CNAME är speciellt 2

Normalt returnerar namnservern svaret (DNS-posterna man frågat efter) utan vidare behandling.

Om frågan gäller t.ex. A, men svaret blir ett CNAME, så kommer namnservern att försöka lägga med en A-post med samma "owner name" som CNAME pekar på.

Se exemplet ovan med [www.aftonbladet.se](http://www.aftonbladet.se).

# ► Posttyp NS och delegering

[\[ Till innehåll \]](#)

# Posttyp NS

Anger namnservern (DNS-servern) för en **zon**.

kth.se. NS b.ns.kth.se.

kth.se. NS a.ns.kth.se.

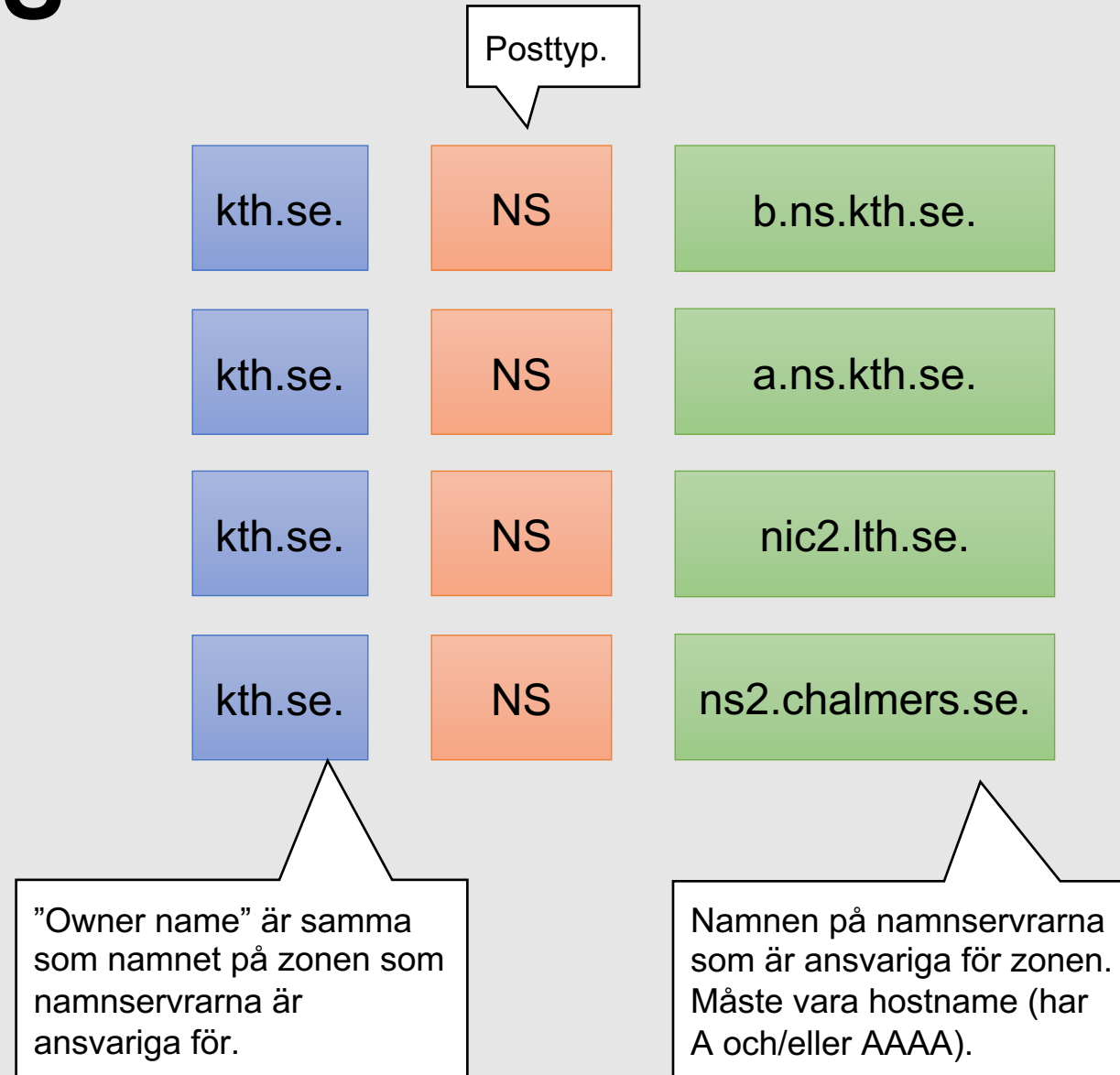
kth.se. NS nic2.lth.se.

kth.se. NS ns2.chalmers.se.

NS-posterna finns längst upp i zonen (apex) och anger zonens namnservrar.

"Längst upp" (apex) betyder namnmässigt längst upp, *inte nödvändigtvis i början av zonfilen*, även om det är det vanligaste.

# Posttyp NS



# Delegering

En moderzon pekar ut en dotterzon genom att ha NS-posterna för dotterzonen. I .se-zonen finns följande NS-poster

kth.se. NS b.ns.kth.se.

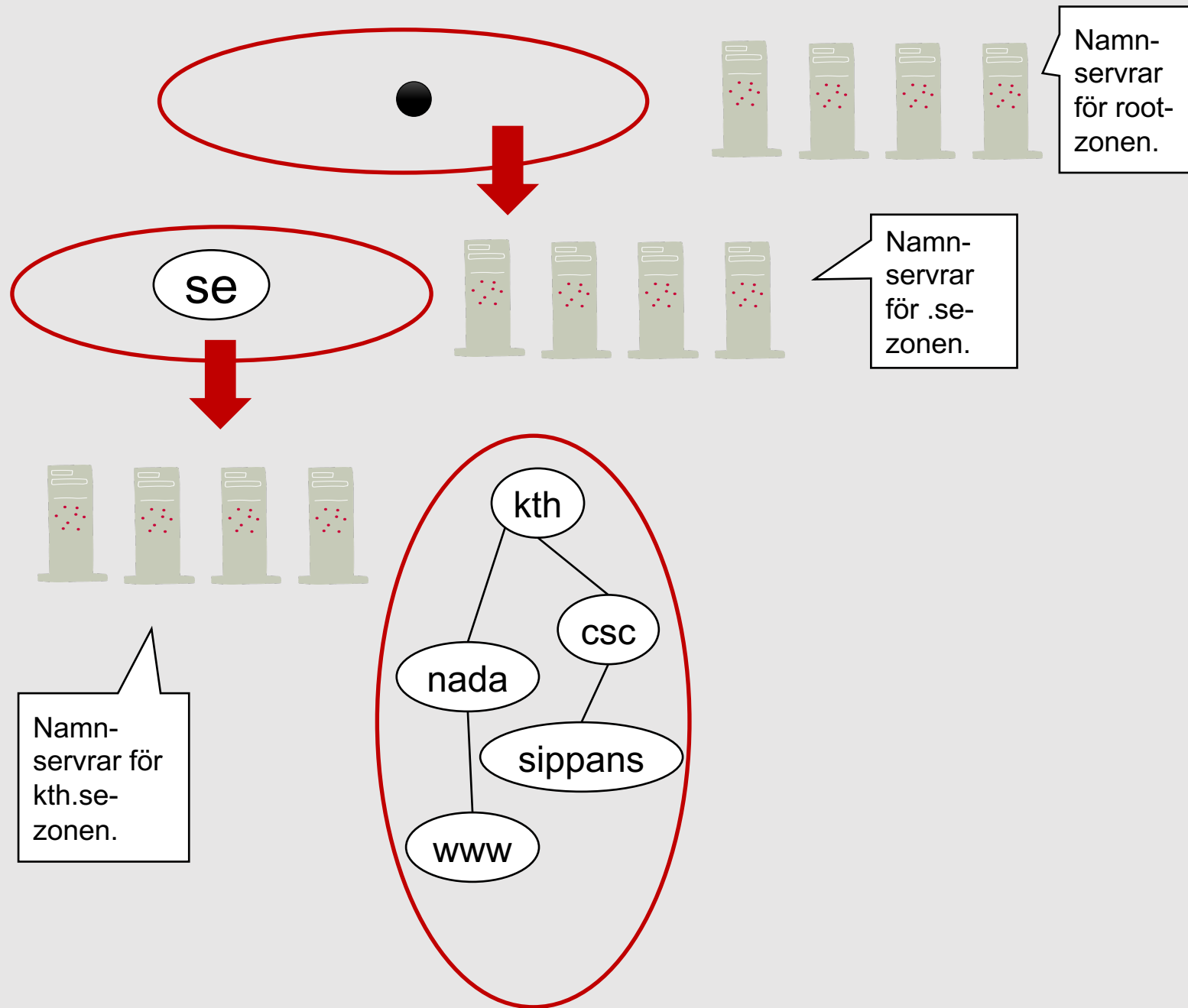
kth.se. NS a.ns.kth.se.

kth.se. NS nic2.lth.se.

kth.se. NS ns2.chalmers.se.

som pekar ut namnservrarna för kth.se. Detta kallas **delegering**.

- Det är (eller ska vara) samma NS-poster som återfinns i kth.se-zonen.
- Det finns alltid NS-poster i apex (se två bilder upp). Vid delegering till underliggande zon (dotterzon) så finns det NS-poster i delegeringspunkten





# Hänvisning av kth.se från se-zonen

```
; <<>> DiG 9.10.6 <<>> @a.ns.se www.kth.se +noedns +norec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56880
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 7
```

Fråga efter namn under  
kth.se (som är en egen zon)  
till en namnserver för .se

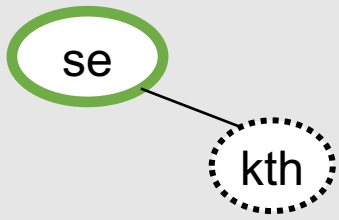
```
;; QUESTION SECTION:
;www.kth.se. IN A
```

```
;; AUTHORITY SECTION:
kth.se. 86400 IN NS a.ns.kth.se.
kth.se. 86400 IN NS nic2.lth.se.
kth.se. 86400 IN NS ns2.chalmers.se.
kth.se. 86400 IN NS b.ns.kth.se.
```

Hänvisning till  
namnservrarna för kth.se  
(se kommande bilder).

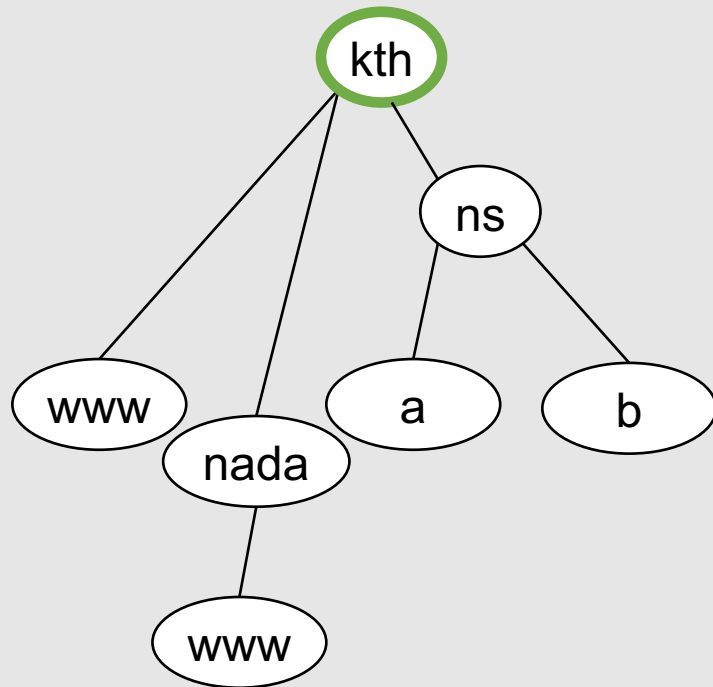
```
;; ADDITIONAL SECTION:
nic2.lth.se.      86400 IN A 130.235.20.5
ns2.chalmers.se. 86400 IN A 129.16.253.252
b.ns.kth.se.     86400 IN A 130.237.72.250
a.ns.kth.se.     86400 IN A 130.237.72.246
ns2.chalmers.se. 86400 IN AAAA 2001:6b0:2:20::1
b.ns.kth.se.     86400 IN AAAA 2001:6b0:1::250
a.ns.kth.se.     86400 IN AAAA 2001:6b0:1::246
```

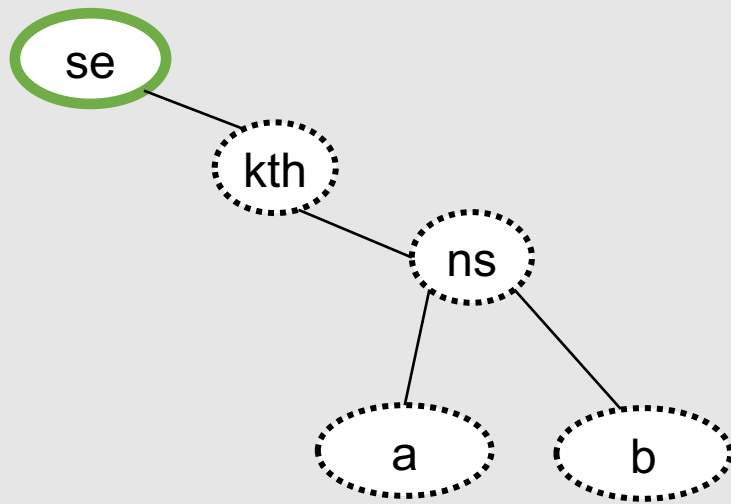
```
;; Query time: 54 msec
;; SERVER: 192.36.144.107#53(192.36.144.107)
;; WHEN: Sun Jan 21 14:49:41 CET 2024
;; MSG SIZE rcvd: 271
```



Delegering av kth.se från se:

```
;; AUTHORITY SECTION:  
kth.se. 86400 IN NS a.ns.kth.se.  
kth.se. 86400 IN NS ns2.chalmers.se.  
kth.se. 86400 IN NS nic2.lth.se.  
kth.se. 86400 IN NS b.ns.kth.se.
```

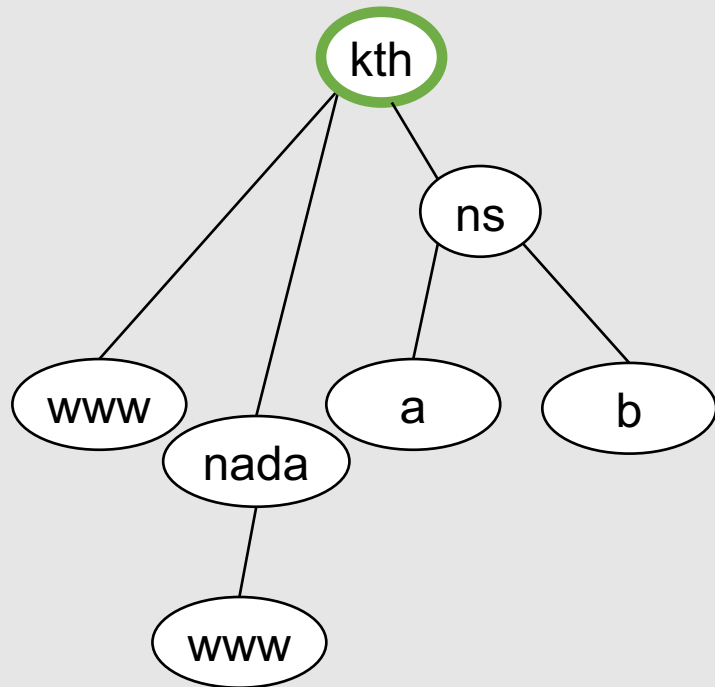




Delegering av kth.se från se:

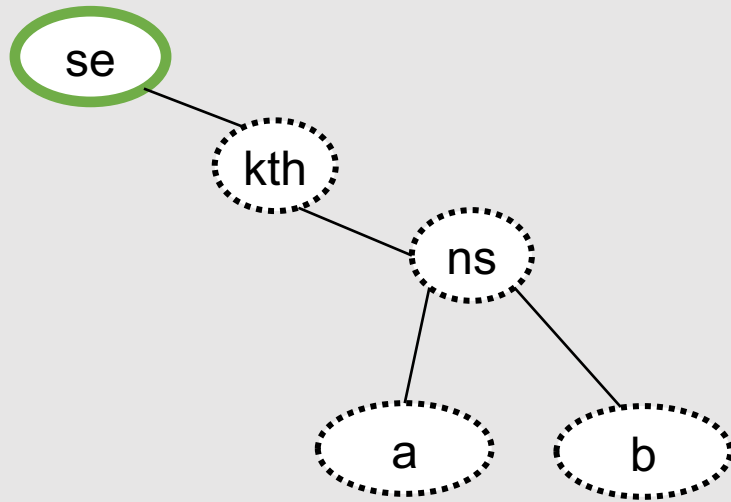
```

;; AUTHORITY SECTION:
kth.se. 86400 IN NS a.ns.kth.se.
kth.se. 86400 IN NS ns2.chalmers.se.
kth.se. 86400 IN NS nic2.lth.se.
kth.se. 86400 IN NS b.ns.kth.se.
  
```



```

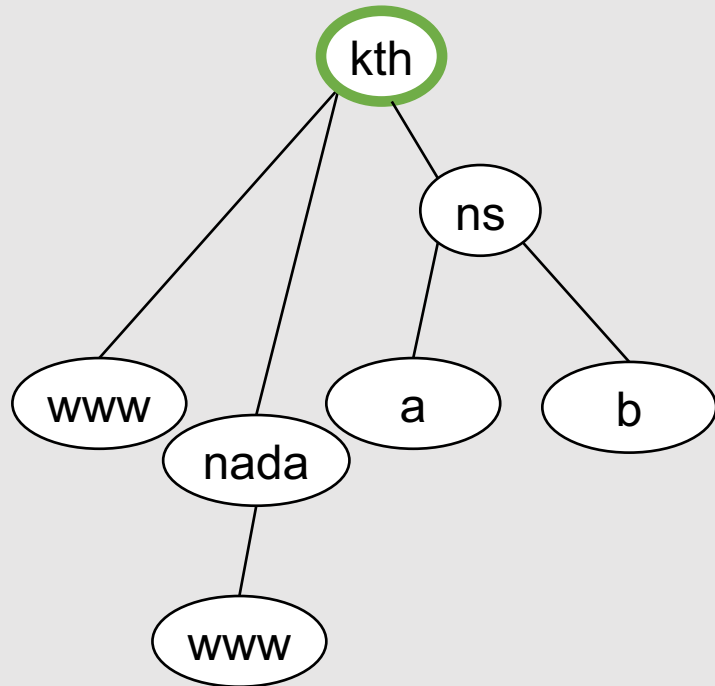
;; ADDITIONAL SECTION:
a.ns.kth.se.      86400 IN A 130.237.72.246
a.ns.kth.se.      86400 IN AAAA 2001:6b0:1::246
b.ns.kth.se.      86400 IN A 130.237.72.250
b.ns.kth.se.      86400 IN AAAA 2001:6b0:1::250
ns2.chalmers.se.  86400 IN A 129.16.253.252
ns2.chalmers.se.  86400 IN AAAA 2001:6b0:2:20::1
nic2.lth.se.      86400 IN A 130.235.20.5
  
```



Delegering av kth.se från se:

```
;; AUTHORITY SECTION:
kth.se. 86400 IN NS a.ns.kth.se.
kth.se. 86400 IN NS ns2.chalmers.se.
kth.se. 86400 IN NS nic2.lth.se.
kth.se. 86400 IN NS b.ns.kth.se.
```

```
;; ADDITIONAL SECTION:
a.ns.kth.se.      86400 IN A 130.237.72.246      ←
a.ns.kth.se.      86400 IN AAAA 2001:6b0:1::246  ← Nödvändiga
b.ns.kth.se.      86400 IN A 130.237.72.250      ← glue-poster
b.ns.kth.se.      86400 IN AAAA 2001:6b0:1::250  ←
ns2.chalmers.se.  86400 IN A 129.16.253.252
ns2.chalmers.se.  86400 IN AAAA 2001:6b0:2:20::1
nic2.lth.se.      86400 IN A 130.235.20.5
```



En glue-post är en adresspost (A, AAAA) för namnservernamnet i en NS-post i en hänvisning (*referral*).

En **nödvändig glue-post** är en adresspost för ett namnservernamn som ligger i eller under delegeringspunkten.

NS-posterna och ev. glue-poster är "inlånade" från dotterzonen.

# ► Posttyp SOA

[\[ Till innehåll \]](#)

# Posttyp SOA

SOA = "Start Of Authority"

Finns längst upp i zonen (apex) tillsammans med NS-posterna.

```
kth.se. SOA a.ns.kth.se. hostmaster.kth.se. 2017020159 14400 900 604800 86400
```

"Längst upp" (apex) betyder namnmässigt längst upp, inte nödvändigtvis i början av zonfilen.

# Posttyp SOA

Mera lättläst sätt att skriva samma SOA-post som förra bilden:

```
kth.se.      SOA      a.ns.kth.se. hostmaster.kth.se. (  
                2017020159 ; serial  
                14400      ; refresh (4 hours)  
                900       ; retry (15 minutes)  
                604800    ; expire (1 week)  
                86400    ; minimum (1 day)  
                )
```

”dig” ger det lättlästa sättet inkl. förtydligande kommentarer om man anger ”+mult”.

Normalt använder man det lättlästa sättet i zonfiler.

kth.se.

SOA

a.ns.kth.se.

hostmaster.kth.se.

2017020159

14400

900

604800

86400

"Owner name" är samma som namnet på zonen.

"MNAME". Primär server för zon-datat. Ska vara "hostname" (med A och/eller AAAA).

"RNAME". Mailadress till ansvarig för zonen. Fungerar ofta inte.

7 delfält i RDATA.



# RNAME

RNAME är en mailadress som har konverterats till ett domännamn. För att konvertera tillbaka till mailadress:

Ersätt punkten mellan första och andra *label* med "@".

- Första *label* blir mailboxnamnet.
- Resten blir maildomänen.

Exempel "hostmaster.kth.se" från SOA-posten för kth.se:

"hostmaster.kth.se" → hostmaster@kth.se

# RNAME

När vi skapar en RNAME från en mailadress så går vi åt andra hållet och ersätter "@" med punkt ".".

hostname@namn.se → hostname.namn.se

Om mailadressen innehåller en punkt i mailboxdelen, t.ex. mats.dufberg@internetstiftelsen.se, så blir det trassligt att använda den i RNAME. Lämpligt är att använda funktionsadresser som t.ex. hostmaster@kth.se.

Mailadressen från RNAME användes mycket förr, men har minskat mycket i betydelse.

kth.se.

SOA

a.ns.kth.se.

hostmaster.kth.se.

2017020159

14400

900

604800

86400

Mera detaljer i senare föreläsning.

Serienumret måste ökas varje gång zonfilen uppdateras.

Vanligt är att ta datumet (ÅÅÅÅMMDD) och lägga till 2 siffor.

Annars ett löpnummer som uppdateras.

Det är ett 32-bitars heltal.

kth.se.

SOA

a.ns.kth.se.

hostmaster.kth.se.

2017020159

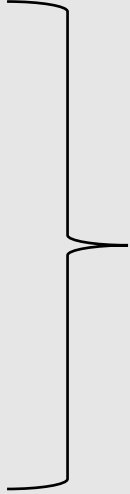
14400

900

604800

86400

Mera detaljer i senare föreläsning.



Tre numeriska värden som används vid synkroniseringen mellan namnservrar för samma zon.

Alla tre är tid i sekunder.

Alla tre är 32-bitars heltal.

kth.se.

SOA

a.ns.kth.se.

hostmaster.kth.se.

2017020159

14400

900

604800

86400

Mera detaljer i senare föreläsning.

Sekunder. Det är ett 32-bitars heltal.

Det anger TTL för svar på frågor där datat inte finns.

Även för TTL för andra poster om annan specificering saknas.

# ► Posttyper och begränsningar

[\[ Till innehåll \]](#)

# Posttyper ("resource record type")

## Ger data direkt:

- A: a.ns.kth.se. A 130.237.72.246
- AAAA: a.ns.kth.se. AAAA 2001:6b0:1::246
- TXT: kth.se. TXT "1 - Royal Inst of Technology"

## Pekar (helt eller delvis) vidare i DNS:

- CNAME: www.nada.kth.se. CNAME sippans.csc.kth.se.
- MX: kth.se. MX 10 mx.kth.se.

## Används bara inom DNS:

- NS: kth.se. NS a.ns.kth.se.
- SOA: kth.se. SOA a.ns.kth.se. hostmaster.kth.se. 2019011549 (...)

# Posttyper ("resource record type")

Det finns många posttyper. Vissa är väldigt ovanliga eller används aldrig.

De som vi hittills tagit upp är grundläggande och vanliga. Dem måste man kunna utantill (utom varje fält i SOA-posten).

Vi återkommer till fler posttyper.



# Posttyper ("resource record type")

En komplett lista över alla posttyper för DNS finns på <https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-4>

# Posttyper ("resource record type")

Varje posttyp har både en textkod och en numerisk kod. Den numeriska koden är den som används i DNS-paketet. Kan slås upp i tabellen hos IANA enligt länken på förra bilden vid behov.

Type	Value
A	1
NS	2
CNAME	5
SOA	6
MX	15
TXT	16
AAAA	28

# Posttyper och domännamnsträdet

De flesta posttyperna kan **kombineras fritt**.

De flesta posttyperna kan **placeras** **vi vilken nod som helst**.

De flesta posttyper **kan upprepas** (med olika RDATA) flera gånger i samma nod.

iis.se. MX 5 mx1.iis.se.

iis.se. MX 5 mx2.iis.se.

# Begränsningar i rot

- De flesta posttyper är inte meningsfulla i den tomma toppnoden i rotzonen eftersom den inte har något namn.

# Begränsningar hos CNAME

- CNAME får inte upprepas i samma nod.
- En nod med CNAME får inte innehålla någon annan DNS-post.

När vi kommer till DNSSEC så kommer påståendet två att modifieras något.

# Begränsningar hos SOA

- SOA måste finnas i toppen ("apex") av zonen.
- Det ska finnas exakt en SOA.
- SOA får inte finnas i någon annan nod.

# Begränsningar hos NS

- Det måste finnas minst en NS i toppen ("apex") av zonen, men det kan finnas många, normalt minst två.
- NS kan finnas i annan nod, och läggs då till för att skapa en delegering.
  - Om det finns en delegering (NS) så slutar grenen där, utom att det kan finnas glue-poster.
  - Nästa zon tar över (delegerar).
- NS får inte finnas i andra noder i zonen.

# ▶ Zonfiler med DNS-poster

[\[ Till innehåll \]](#)



# Zonfiler

Varje zon har en zonfil.

1. Det finns alltid en SOA-post och NS-poster i zonens "start".
2. Normalt så finns det egentliga dataposter, t.ex. A och MX. Vissa toppdomäner (TLD\*) saknar egentliga dataposter.
3. Många zoner, speciellt toppdomäner, har delegeringar med NS-poster till dotterzoner.

\*) TLD = Top Level Domain, nivån direkt under root.

# Enkel zonfil

```
$TTL      3600
$ORIGIN   namn.se.

@          SOA ns1 info (
                2020011700
                7200
                900
                604800
                3600
                )

NS ns1
NS dns5.telia.com.
mx 10 mail

www      A      192.0.2.20
ns1     A      192.0.2.25
```

Default TTL för posterna i zonen (zonfilen).

Normalt zonens namn. Lägggs på alla relativa namn.

Parentes "()" för att kunna visa posten med radbrytning.

"@" representerar med det som anges med \$ORIGIN.

"ns1" är relativt namn (ingen punkt på slutet) och blir "ns1.namn.se." (\$ORIGIN läggs på). Motsvarande för andra relativa namn.

# Delegering från root till se

I root-zonen:

```
.      SOA      a.root-servers.net. nstld.verisign-grs.com. (...)  
.      NS       a.root-servers.net.  
.      NS       b.root-servers.net.  
.      NS       l.root-servers.net.  
.      NS       m.root-servers.net.
```

(...)

```
se.      NS       x.ns.se.  
se.      NS       i.ns.se.  
se.      NS       f.ns.se.  
se.      NS       g.ns.se.  
x.ns.se. A       213.108.25.4  
x.ns.se. AAAA    2001:67c:124c:e000::4  
i.ns.se. A       194.146.106.22  
i.ns.se. AAAA    2001:67c:1010:5::53  
f.ns.se. A       192.71.53.53  
g.ns.se. A       130.239.5.114
```

Delegering av .se (förkortad).

# Delegering från se till kth.se

I .se-zonen:

```
se.          SOA  catcher-in-the-rye.nic.se. registry-default.nic.se. (...)
```

```
se.          NS    x.ns.se.
se.          NS    i.ns.se.
se.          NS    f.ns.se.
se.          NS    g.ns.se.
x.ns.se.     A      213.108.25.4
x.ns.se.     AAAA   2001:67c:124c:e000::4
i.ns.se.     A      194.146.106.22
i.ns.se.     AAAA   2001:67c:1010:5::53
f.ns.se.     A      192.71.53.53
g.ns.se.     A      130.239.5.114
```

Ska  
motsvara  
delegeringen  
från "root".

(...)

```
kth.se.      NS    nic2.lth.se.
kth.se.      NS    ns2.chalmers.se.
kth.se.      NS    a.ns.kth.se.
kth.se.      NS    b.ns.kth.se.
a.ns.kth.se. A      130.237.72.246
a.ns.kth.se. AAAA   2001:6b0:1::246
b.ns.kth.se. AAAA   2001:6b0:1::250
```

Delegering av kth.se (förkortad).

# kth.se

I kth.se-zonen:

```
kth.se.          SOA      a.ns.kth.se. hostmaster.kth.se. 2017020160 (...)
```

```
kth.se.          NS       nic2.lth.se.
kth.se.          NS       ns2.chalmers.se.
kth.se.          NS       a.ns.kth.se.
kth.se.          NS       b.ns.kth.se.
a.ns.kth.se.     A        130.237.72.246
a.ns.kth.se.     AAAA     2001:6b0:1::246
```

```
kth.se.          MX       20      mx-alt1.kth.se.
kth.se.          MX       10      mx.kth.se.
kth.se.          A        130.237.28.40
kth.se.          AAAA     2001:6b0:1:11c2::82ed:1c28
www.kth.se.     A        130.237.28.40
www.kth.se.     AAAA     2001:6b0:1:11c2::82ed:1c28
www.nada.kth.se. CNAME    sippans.csc.kth.se.
(...)
```

Ska  
motsvara  
delegeringen  
från .se.

Inga delegeringar i  
detta exempel, men  
det kan finnas i kth.se-  
zonen.

# ► Roller hos namnservrar

[\[ Till innehåll \]](#)

# Roller hos namnserver

Namnserverar (DNS-serverar) kan ha två olika roller:

- **Hostingsserver.** Auktoritativ DNS-server. Håller zonfilen för en zon, och svarar på frågor om zonen. T.ex. för .se eller kth.se.
- **DNS-resolver.** Letar fram DNS-datat åt vanliga klienter, t.ex. bärbara datorer, mobiler, men även åt t.ex. mailservrar.

# DNS-resolver

DNS-resolvern konfigureras ofta automatiskt samtidigt som IP-adressen sätts. "resolv.conf" uppdateras med informationen om resolver.

I en vanlig PC eller mobil så är "DNS-server" samma sak som DNS-resolver.

DNS-resolvern lagrar svaren i en s.k. cache ett tag för att kunna svara snabbare.



# DNS-hosting och DNS-resolver

- Oftast olika servrar – den rekommenderade lösningen.
- DNS-hosting är normalt åtkomlig från hela Internet.
  - Det finns även intern hosting, speciellt på stora företag.
- DNS-resolvrar är normalt bara åtkomliga för de avsedda användarna.

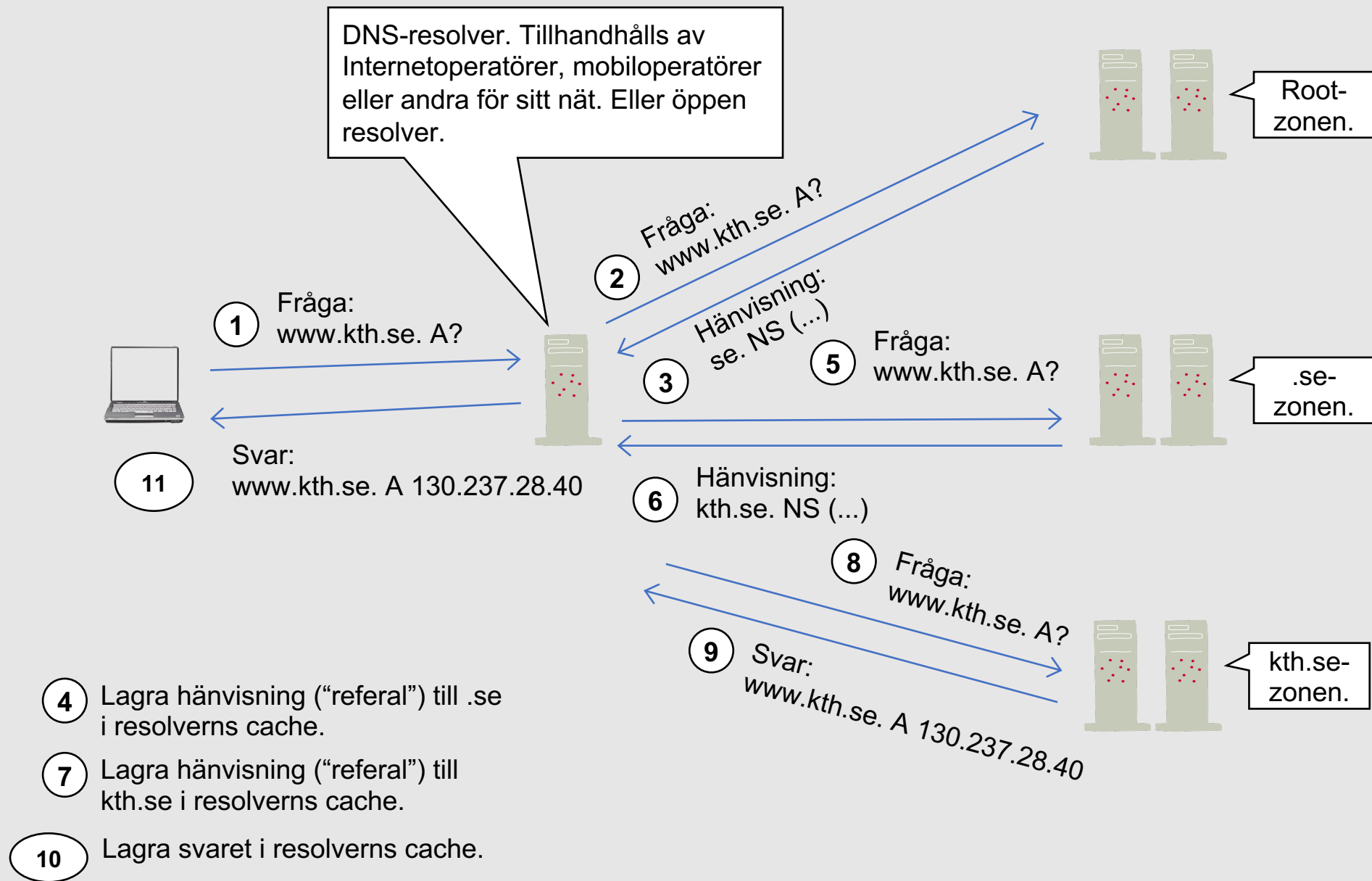
# Öppna resolvrar

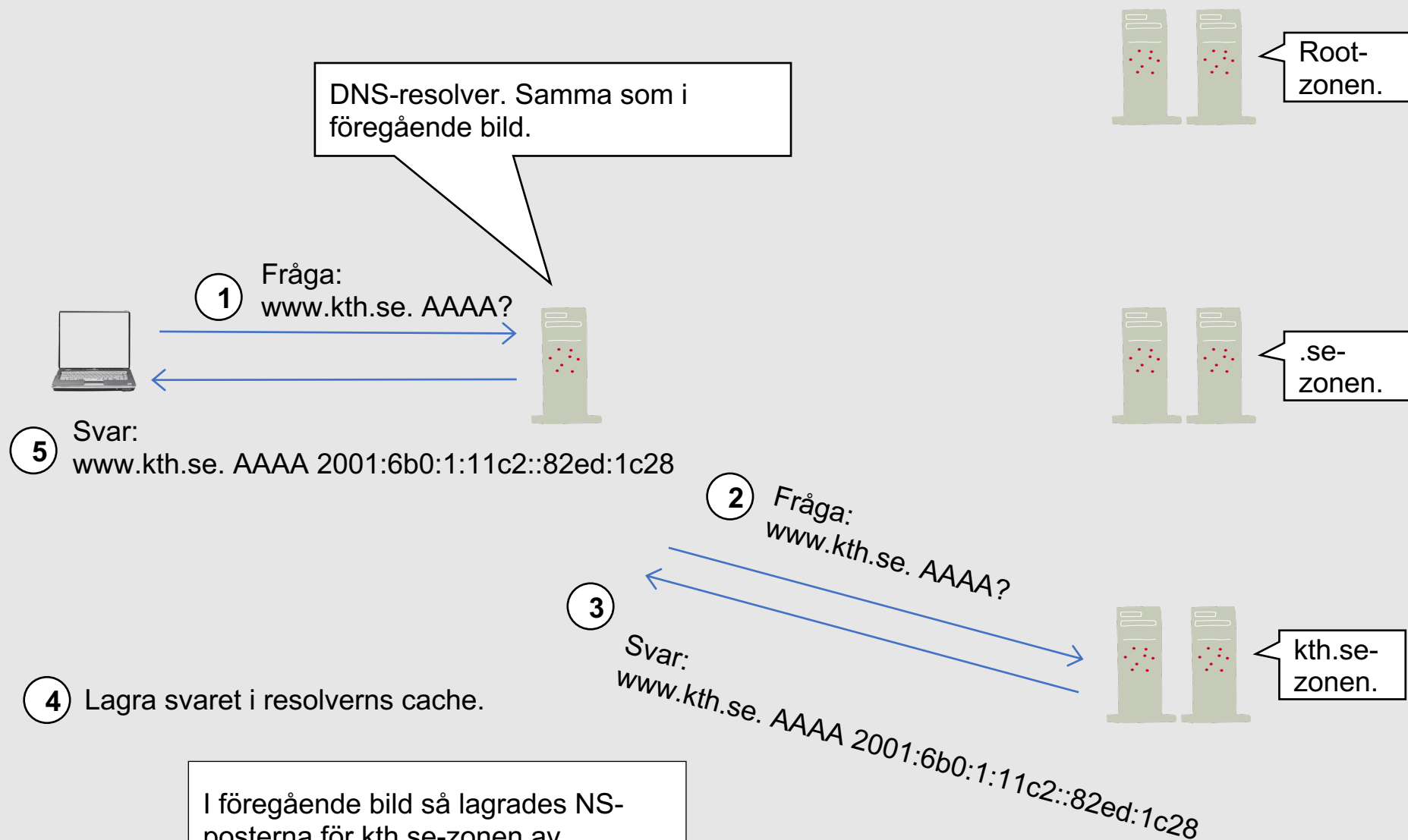
- Det finns resolvrar som är öppna och avsedda för alla användare på Internet, t.ex.:
  - 8.8.8.8 (Google)
  - 9.9.9.9 (Quad9)
  - 1.1.1.1 (Cloudflare och APNIC)

Det finns även IPv6-adresser till resolvrar.

# ▶ Uppslagning via resolver

[\[ Till innehåll \]](#)





I föregående bild så lagrades NS-posterna för kth.se-zonen av resolvern vilket gör att den kan gå direkt till dess servrar och ställa frågan.

# Uppslagning via resolver

Senare kommer vi att återkomma till hur uppslagningen går till med en något modifierad modell.

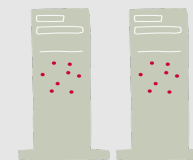
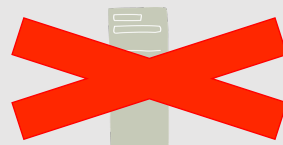
Vad händer om DNS-resolvern inte svarar eller inte är tillgänglig?



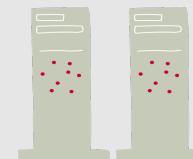
1 Fråga: www.kth.se. AAAA?

2 Fråga: www.kth.se. AAAA?

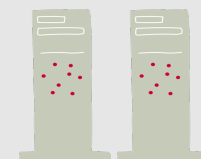
3 Fråga: www.kth.se. AAAA?



Root-zonen.



.se-zonen.



kth.se-zonen.

# ► Om presentationen

[\[ Till innehåll \]](#)



# Internets domännamnssystem

Denna presentation är framtagen 2019–2024 av Mats Dufberg ([mats.dufberg@internetstiftelsen.se](mailto:mats.dufberg@internetstiftelsen.se)) på Internetstiftelsen (<https://internetstiftelsen.se/>). Den är en del av undervisningsmaterialet för kursen ”Internets domännamnssystem” vid Kungliga tekniska högskolan, KTH (kurskod HI1037) resp. Karlstads universitet, KAU (kurskod DVGC28).

# Licens

Detta undervisningsmaterial tillhandahålls med licens BY 4.0 enligt Creative Commons (<https://creativecommons.org/licenses/by/4.0/deed.sv>) och får användas i enlighet med de villkoren.

# Dokumenthistorik

- Rev A: Ursprünglich version VT 2024

# Slut.

[\[ Till innehåll \]](#)