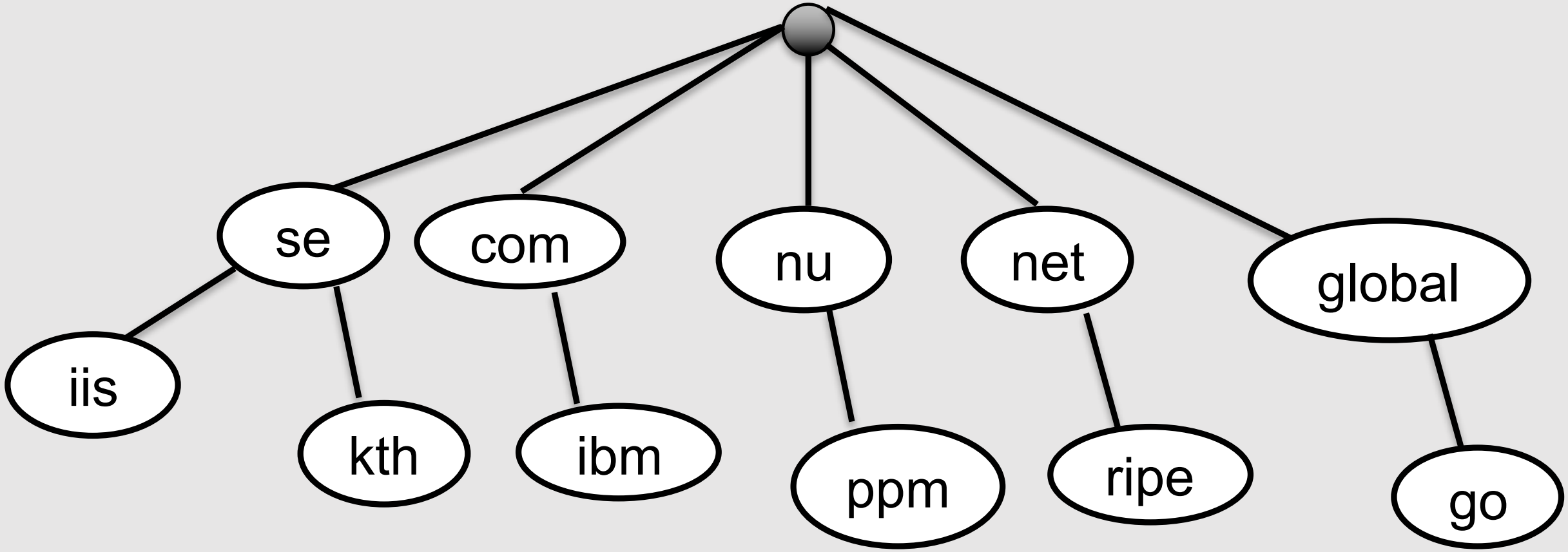

se
com
nu
net
global
iis
kth
ibm
ppm
ripe
go

INTERNET STIFTELSEN

Internets domännamnssystem*

Föreläsning FL03, HT 2023

Mats Dufberg

* Se “Internets domännamnssystem”

Innehåll

▶Domänen startar i noden

[Till Innehåll]

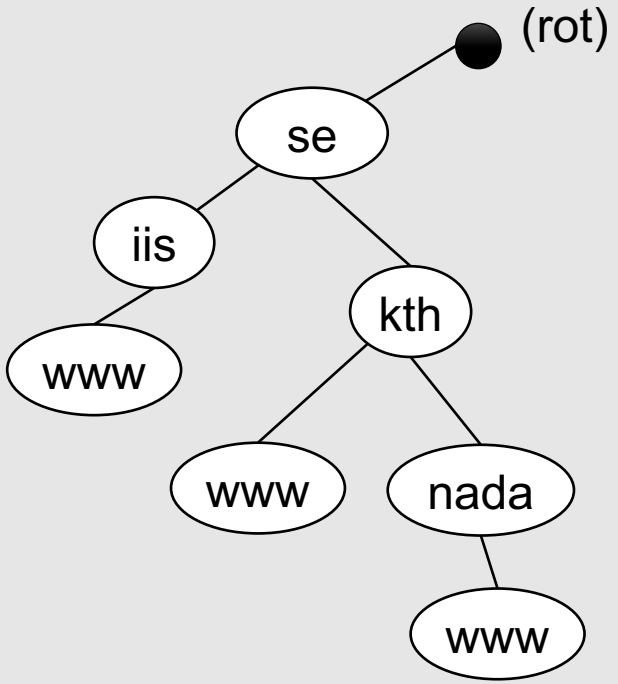
Domänen startar i noden

Är www.kth.se och kth.se samma domän? Domänen startar i noden. De startar i olika noder.

www.kth.se. ≠ kth.se.

DNS-datat (DNS-posterna) är knutna till noden ("owner name").

Om man frågar med fel namn så får man fel data.



Samma domän?

Om man skriver **https://kth.se/** eller **https://www.kth.se/** så hamnar man på samma sida. – Är det samma domän?

Nej, i DNS är det olika domäner.

Omstyrning från **https://kth.se/** till **https://www.kth.se/** är en mekanism inom HTTP, inte inom DNS.

Jämför med att **https://iis.se/** styrs om till **https://internetstiftelsen.se/** med HTTP. Det är olika domäner.

▶Parametrar i DNS-frågan

[Till Innehåll]

Vad frågar du efter och till vem?

Innan du analyserar ett DNS-svar från "dig" se till att du har svar på följande frågor:

Fråga	**Default ifall du inte har angivit något**	**Kommentar**
Vilket domännamn har du frågat efter?	"." (root-noden)	Sällan det vi vill fråga efter
Vilken posttyp har du frågat efter?	A	Ofta användbart, men kan missa AAAA
Vilken server har "dig" skickat frågan till?	Resolver listad i /etc/resolv.conf	Ofta användbart

Svaren finns i svaret

```
; <<>> DiG 9.10.6 <<>> www.sunet.se +noedns @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16576
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
www.sunet.se. 23 IN CNAME webc.sunet.se.
webc.sunet.se. 233 IN A 192.36.171.231

;; Query time: 49 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Jan 18 17:18:39 CET 2019
;; MSG SIZE  rcvd: 65
```

Domännamn och posttyp – *query name* och *query type* – finns det kopierat till svarspaketet.

Servern som "dig" skickade frågan till och fick svaret från.

▶Typer av DNS-svar

[Till Innehåll]

Auktoritativt svar

Auktoritativ server för en zon är master- eller slavserver som har zonen laddad från fil (eller motsvarande). En sådan server kan ge ett **auktoritativt svar** (”authoritative answer”) på fråga om zondata.

Det är viktigt att man kan identifierar sådana svar när man ser det som kommer från ”dig”.

Icke-auktoritativt svar

En resolver ger **icke-auktoritativt svar**. Den tar svaret från data som den har frågat efter eller sin cache.

Även detta ska man kunna identifiera.

Hänvisning

En zon delegerar en subzon till namnservrarna för subzonen genom att lista subzonens NS-poster.

När vi ställer DNS-frågor så kan vi få en ***response*** som motsvarar en delegeringen. Vi får en **hänvisning** (*referral*). Hänvisningen är icke-auktoritativ.

Det är viktigt att kunna skilja mellan hänvisning, å ena sidan, och andra icke-auktoritativa svar som bygger på data från ***cache***, å andra sidan.

Typer av svar

1. Auktoritativt svar (***response***) – Från hostingserver (master eller slav) som är konfigurerad med zonen.
2. Icke-auktoritativt svar (***response***) – Från DNS-resolver som har hämtat svaret från en hostingserver.
3. Svaret (***response***) är hänvisning – Från en hostingserver som pekar vidare till andra hostingservrar för den aktuella zonen, som svaret ev. finns i.

Auktoritativt svar

Auktoritativt svar (***response***) – Från hostingserver (master eller slav) som är konfigurerad med zonen.

Det behöver inte vara en server som delegeringen pekar på (mer om dold master och dold slav i nästa föreläsning).

Typer av svar

Genom att analysera svaret (***response***) som "dig" visar så kan vi se vad som är vad. Vi tittar på flaggor och svarets olika delar (***sections***).

▶Flaggor i DNS-paketet

[Till Innehåll]

Flaggor i ”response”

```
; <<>> DiG 9.10.6 <<>> www.sunet.se +noedns @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16576
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
www.sunet.se. 23 IN CNAME webc.sunet.se.
webc.sunet.se. 233 IN A 192.36.171.231

;; Query time: 49 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Jan 18 17:18:39 CET 2019
;; MSG SIZE  rcvd: 65
```

Frågan skickades till 8.8.8.8, vilket är IP-adressen till Googles öppna resolver.

När en flagga visas så är flaggbiten (***bit***) satt, d.v.s. har värdet 1

Här ”qr”, ”rd”, ”ra” och ”ad” satta (värde 1).

Flaggor i ”response”

```
; <<>> DiG 9.10.6 <<>> www.sunet.se +noedns +norec @sunic.sunet.se
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27643
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 4

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

;; ANSWER SECTION:
www.sunet.se.       300 IN  CNAME   webc.sunet.se.
webc.sunet.se.      300 IN  A   192.36.171.231

(…)
;; Query time: 51 msec
;; SERVER: 2001:6b0:7::2#53(2001:6b0:7::2)
;; WHEN: Fri Jan 18 16:58:01 CET 2019
;; MSG SIZE  rcvd: 244
```

Frågan skickades till sunic.sunet.se som är en auktoritativ server för sunet.se, och finns med i listan av NS.

+norec = sätt inte rd-flaggan i frågan.

När en flagga visas så är flaggbiten satt, d.v.s. har värdet 1

Här ”qr” och ”aa” satta (värde 1).

Flaggor i ”response”

Flagga	Satt (bit-värde = 1)
QR	*response* (0 = *query*)
AA	*authoritative answer*
TC	trunkerat (hela svaret fick inte plats)
RD	*recursion desired* (klienten bad namnservern att agera resolver)
RA	*recursion available* (namnservern kan/skulle kunna agera resolver för klienten)
AD	(DNSSEC)

- Om flaggan o-satt (värde 0) så visas den inte med ”dig”.
- AD-flaggan kommer att behandlas när vi tar upp DNSSEC.

Flagga QR

QR = 0 – ***query***

QR = 1 – ***response***

Flagga AA i "response"

AA = 1 – Svaret kommer från en hostingserver som är auktoritativ för datat in ***answer section*** eller auktoritativ för NXDOMAIN- eller NODATA-svaret.

Om svaret kommer från en resolver eller är en hänvisning så är AA=0.

Flagga TC i "response"

TC = 1 – avkortat ***response*** – kommer senare.

Flagga RD i "response"

Kopierat från ***query***. Ingen speciell betydelse i ***response***, men kan hjälpa oss att förstå om det gjordes rekursion eller inte.

Flagga RA i "response"

Visar vilken policy som servern har för just denna klient:

RA = 0	Servern utför inte rekursion för klienten oavsett värdet på RD-flaggan.
RA = 1	Servern utför (försöker utföra) rekursion för klienten ifall RD-flaggan är satt och rekursion behövs för att hitta svaret.

Om RA-flaggan är satt så ***kan*** servern agera resolver för klienten.

Men kanske inte i just detta fall.

Flagga RD i ”query”

Den flagga vi kan välja att sätta i frågan, eller inte sätta, är RD-flaggan.

Normalt är den satt när man använder ”dig”.

RD = 0	Gör ingen rekursion, svara bara vad du har. Om servern har "cachad" data, och policy säger att den kan svara med "cachad" data, så gör den det.
RD = 1	Gör rekursion, agera resolver. Policy avgör om servern kommer att agera resolver.

”Query” och "response" från "dig"

```
; <<>> DiG 9.10.6 <<>> www2.kth.se +noedns +noad +qr +norecurse
;; global options: +cmd
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45796
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

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

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45796
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 5

;; QUESTION SECTION:
;www2.kth.se.                   IN  A
(…)
```

Query

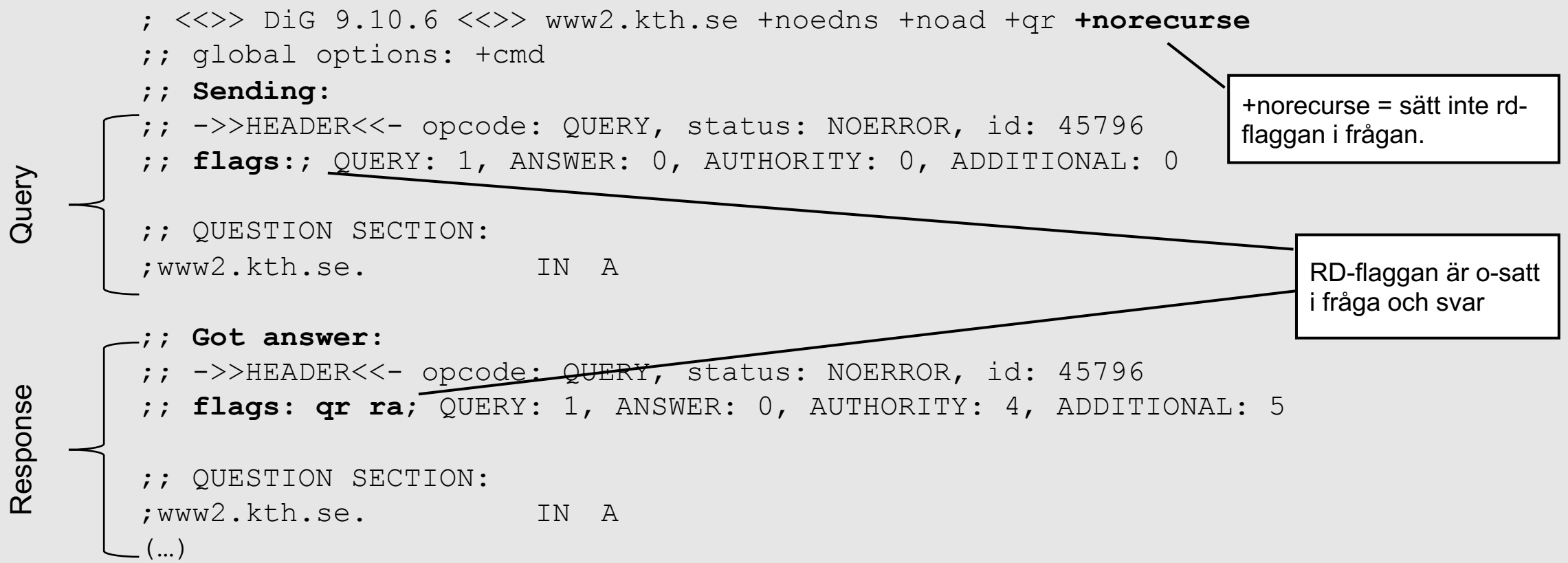
Response

+qr = "dig" visar även ***query*** (efter "sending")

Efter "Got answer" visas ***response***

"dig" skickar ***query*** och får tillbaka ***response***. Normalt visar "dig" bara ***response***, men om man kör "dig" med "+qr" så visas även ***query***.

Flaggor i ”query”



Flaggor i ”response”

```
; <<>> DiG 9.10.6 <<>> www3.kth.se +norec +noedns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62282
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 10, ADDITIONAL: 14

;; QUESTION SECTION:
;www3.kth.se.                   IN  A

;; AUTHORITY SECTION:
se.             97216   IN  NS  f.ns.se.
se.             97216   IN  NS  g.ns.se.
(…)

;; Query time: 87 msec
;; SERVER: 172.17.41.10#53(172.17.41.10)
;; WHEN: Mon Jan 21 11:08:46 CET 2019
;; MSG SIZE  rcvd: 502
```

RA-flaggan sätts (eller inte) av namnservern oberoende om RD-flaggan var satt av klienten eller inte.

RA-flaggan betyder *inte* att namnservern har agerat resolver i detta fall utan bara att den *accepterar* att göra så för klienten.

RD-flaggan är o-satt, vilket betyder att klienten *inte* begärde recursion.

Flaggor från ”query”

```
; <<>> DiG 9.10.6 <<>> www3.kth.se +noedns +mult
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 57375
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;www3.kth.se.      IN A

;; AUTHORITY SECTION:
kth.se.         892 IN SOA a.ns.kth.se. hostmaster.kth.se. (
                2019011674 ; serial
                14400      ; refresh (4 hours)
                900        ; retry (15 minutes)
                604800     ; expire (1 week)
                86400      ; minimum (1 day)
                )
(…)
```

Jfr med föregående bild. Här begär vi rekursion (”agera resolver”) genom att sätta RD-flaggan i frågan. Och får rekursion.

▶Status (RCODE) i DNS-paketet

[Till Innehåll]

Status i ”response”

```
; <<>> DiG 9.10.6 <<>> www3.kth.se +norec +noedns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62282
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 10, ADDITIONAL: 14

;; QUESTION SECTION:
;www3.kth.se.                   IN  A

;; AUTHORITY SECTION:
se.             97216   IN  NS  f.ns.se.
se.             97216   IN  NS  g.ns.se.
(…)

;; Query time: 87 msec
;; SERVER: 172.17.41.10#53(172.17.41.10)
;; WHEN: Mon Jan 21 11:08:46 CET 2019
;; MSG SIZE  rcvd: 502
```

Här sätts status i ***response***. Det kan vara en av flera olika statusvärden. Den är aldrig tom.

Flaggorna är delvis beroende av status.

Status i ”response”

RCODE code	RCODE name	Beskrivning
0	NOERROR	Frågan gick bra, men vi kanske inte fick svaret vi ville ha. Poststypen finns ev. inte. Eller så kanske vi fick en hänvisning istället för det vi frågade efter.
3	NXDOMAIN	Domännamnet vi frågar efter finns inte.
2	SERVFAIL	Servern är felkonfigurerad. Fel på datat eller zonfilen. Problem med att hämta datat som behövs för att kunna svara.
5	REFUSED	Policy hindrar servern att svara på ***query***.
1	FORMERR	Servern kan inte tolka formatet på ***query*** (kanske nyare format).

Lista över alla RCODE: https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dns-parameters-6

NOERROR

Om RCODE är NOERROR så har vi tre möjligheter:

1. Svaret på frågan finns i ***answer section***.
2. Domännamnet finns, men inte med efterfrågad data (***answer*** är tomt). Kallas även ***NODATA***.
3. ***Response*** är en hänvisning (delegering).

Vid alt 1 och 2 så kan flagga AA vara satt eller inte. Vid alt 3 så är den alltid osatt.

NOERROR

Om RD-flaggan är satt och frågan skickas till en resolver som servar klienten (RA är satt) så får vi aldrig en hänvisning (alt 3 i förra bilden).

En resolver kommer alltid att försöka följa delegeringar för att ge det slutgiltiga svaret till klienten.

NXDOMAIN

NXDOMAIN betyder att domännamnet inte finns, d.v.s. det finns ingen sådan nod.

- Om domännamnet finns (noden finns), men inte posttypen så blir det inte NXDOMAIN utan NODATA.

NXDOMAIN

www3.kth.se finns överhuvud taget inte. Om vi frågar efter det, oavsett frågetyp (posttyp) så blir det NXDOMAIN.

”aftonbladet.se. A 13.53.120.82” finns. – Om vi frågar efter ”aftonbladet.se. AAAA” så får vi NODATA, inte NXDOMAIN.

NXDOMAIN gäller bara om namnet finns eller inte.

NODATA

NODATA är ingen RCODE.

- RCODE är NOERROR.
- ***Answer section*** är tom.
- Det är ingen delegering.

Om vi frågar en auktoriativ server så är AA-flaggan satt (auktoritativt svar).

NODATA får vi när domännamnet finns, men inte posttypen under det domännamnet (i den noden).

NOERROR och posttypen finns

```
; <<>> DiG 9.10.6 <<>> @ns04.savvis.net www.telia.net a +norec +noedns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51142
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 3

;; QUESTION SECTION:
;www.telia.net.                 IN  A

;; ANSWER SECTION:
www.telia.net.      1200    IN  A   81.236.63.162

(…)
```

Fråga till hostingserver (auktoritativ server i detta fall).

aa

NXDOMAIN – domännamnet finns inte

```
; <<>> DiG 9.10.6 <<>> @ns04.savvis.net www1.telia.net aaaa +norec +noedns +mult
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 43125
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;www1.telia.net.        IN AAAA

;; AUTHORITY SECTION:
telia.net.      1200 IN SOA dns1.telia.com. backbone.telia.net. (
                2019012100 ; serial
                10800      ; refresh (3 hours)
                3600       ; retry (1 hour)
                604800     ; expire (1 week)
                1200       ; minimum (20 minutes)
                )
(…)
```

Fråga till hostingserver (auktoritativ server i detta fall).

aa

NOERROR/NODATA

```
; <<>> DiG 9.10.6 <<>> @ns04.savvis.net www.telia.net aaaa +norec +noedns +mult
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52442
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;www.telia.net.          IN AAAA

;; AUTHORITY SECTION:
telia.net.      1200 IN SOA dns1.telia.com. backbone.telia.net. (
                2019012100 ; serial
                10800      ; refresh (3 hours)
                3600       ; retry (1 hour)
                604800     ; expire (1 week)
                1200       ; minimum (20 minutes)
                )
(...)
```

Fråga till hostingserver (auktoritativ server i detta fall).

aa

Domännamnet finns, men det finns ingen AAAA-post i den noden.

NOERROR – hänvisning/referral

```
; <<>> DiG 9.10.6 <<>> @ns04.savvis.net www.de.telia.net aaaa +norec +noedns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43004
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.de.telia.net. IN AAAA

;; AUTHORITY SECTION:
de.telia.net.      1200 IN NS dns2.telia.com.
de.telia.net.      1200 IN NS dns1.telia.com.

;; ADDITIONAL SECTION:
dns1.telia.com.         3600 IN A 81.228.11.67
dns2.telia.com.         3600 IN A 81.228.10.67
(…)
```

Fråga till hostingserver.

aa är inte satt

Hänvisning till de namnservrar som via NS-poster listas i ***authority section***.

Domännamnet kanske finns, men inte i den zon som servern ansvarar för utan i så fall i subdomänen.

SERVFAIL

Om namnservern returnerar ***SERVFAIL*** så är det antingen fel på konfigurationen av namnservern eller så kan resolvern inte slutföra uppslagningen.

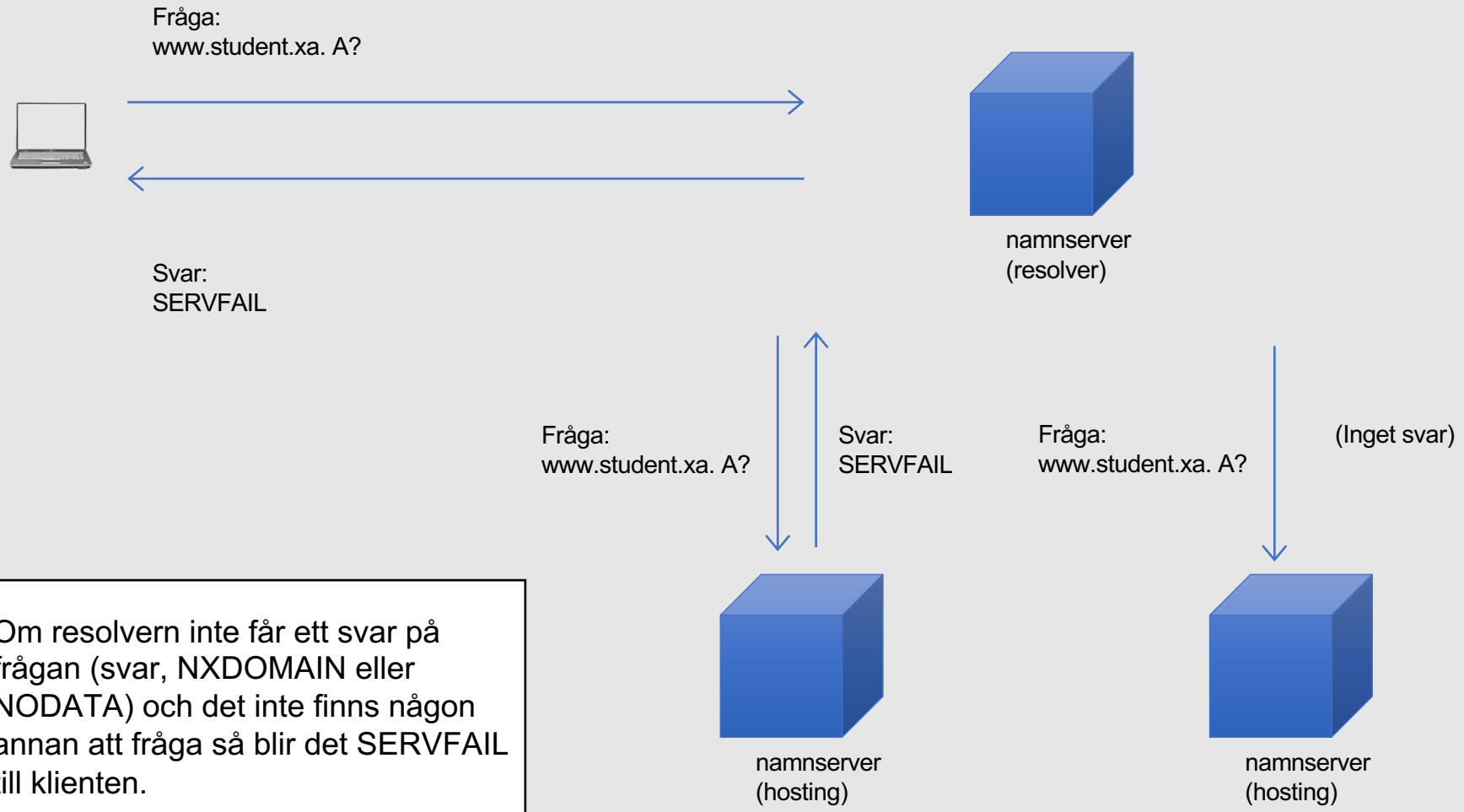
- Zonen har inte kunnat laddas på hostingservern.
- Zonen har löpt ut på slavservern.
- Resolvern kan inte slutföra uppslagningen, t.ex. zonen där datat ligger är oåtkomlig (hostingservrarna svarar inte).
- Datat eller sökvägen kan inte valideras enligt DNSSEC (mer om detta när vi kommer till DNSSEC).

Lame delegation

Om zon inte är åtkomlig på någon av dess servrar, så har vi ”lame delegation”.
T.ex.:

- Servrarna är IP-mässigt oåtkomliga.
- Servrarna är nere eller felkonfigurerade.
- Zonen är felkonfigurerad.
- Delegeringen är felaktig.

Om vi frågar en resolver efter ett domännamn som tillhör en zon som är ”lame” så svarar resolvern med SERVFAIL.



Om resolvern inte får ett svar på frågan (svar, NXDOMAIN eller NODATA) och det inte finns någon annan att fråga så blir det SERVFAIL till klienten.

Alla de auktoritativa servrarna för zonen student.xa

REFUSED

Servern är konfigurerad att inte besvara frågor från klienten eller inte besvara frågor om det specifika domännamn vi frågar efter.

- En namnserver, speciellt en resolver, kan vara konfigurerad att bara hantera vissa klienter (t.ex. på vissa IP-adresser). ***REFUSED*** till andra.
- En hostingnamnserver har vissa domäner (zoner), men inte alla, och kan bara svara för dem den har. ***REFUSED*** vid frågor om andra domännamn.
  - Hänvisning (inte ***REFUSED***) ifall namnet är ett dotternamn (i en eller flera nivåer) till zon som servern har.
  - Hostingservrar med ”gammaldags” konfigurering ger en hänvisning till root istället.

REFUSED – Telias resolvrar för kunder

```
; <<>> DiG 9.10.6 <<>> @195.67.199.15 www.kth.se +noedns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 287
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

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

;; Query time: 50 msec
;; SERVER: 195.67.199.15#53(195.67.199.15)
;; WHEN: Mon Jan 21 16:48:34 CET 2019
;; MSG SIZE  rcvd: 28
```

Klienten måste sitta på Telias nät.

REFUSED

REFUSED är ett svar från namnservern, ett DNS-svar, vilket betyder att frågan går fram till namnservern. I Telias fall så betyder det att namnservern är konfigurerad med en ACL* som anger vilka IP-adresser som släpps fram och vilka som spärras.

Om det är brandväggen som spärrar så blir det inget DNS-svar, vilket leder till att ”dig” gör ”timeout” efter en stund.

*) ACL = Access-control list

REFUSED – Telias hostingserver

```
; <<>> DiG 9.10.6 <<>> @dns2.telia.com www.kth.se +noedns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 33461
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

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

;; Query time: 48 msec
;; SERVER: 81.228.10.67#53(81.228.10.67)
;; WHEN: Mon Jan 21 16:50:54 CET 2019
;; MSG SIZE  rcvd: 28
```

Telia (dns2.telia.com) hostar inte kth.se, men klienten är OK.

NOERROR – Telias hostingserver

```
; <<>> DiG 9.10.6 <<>> @dns2.telia.com www.telia.com +noedns +norec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56931
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 2

;; QUESTION SECTION:
;www.telia.com.                 IN  A

;; ANSWER SECTION:
www.telia.com.      3600    IN  A   81.236.63.162

(…)
```

Telia (dns2.telia.com) hostar telia.com.

Timeout – ingen RCODE

Namnservern svarar inte, och ”dig” gör ***timeout*** (ger upp). Det är inte namnservern som gör ***timeout***.

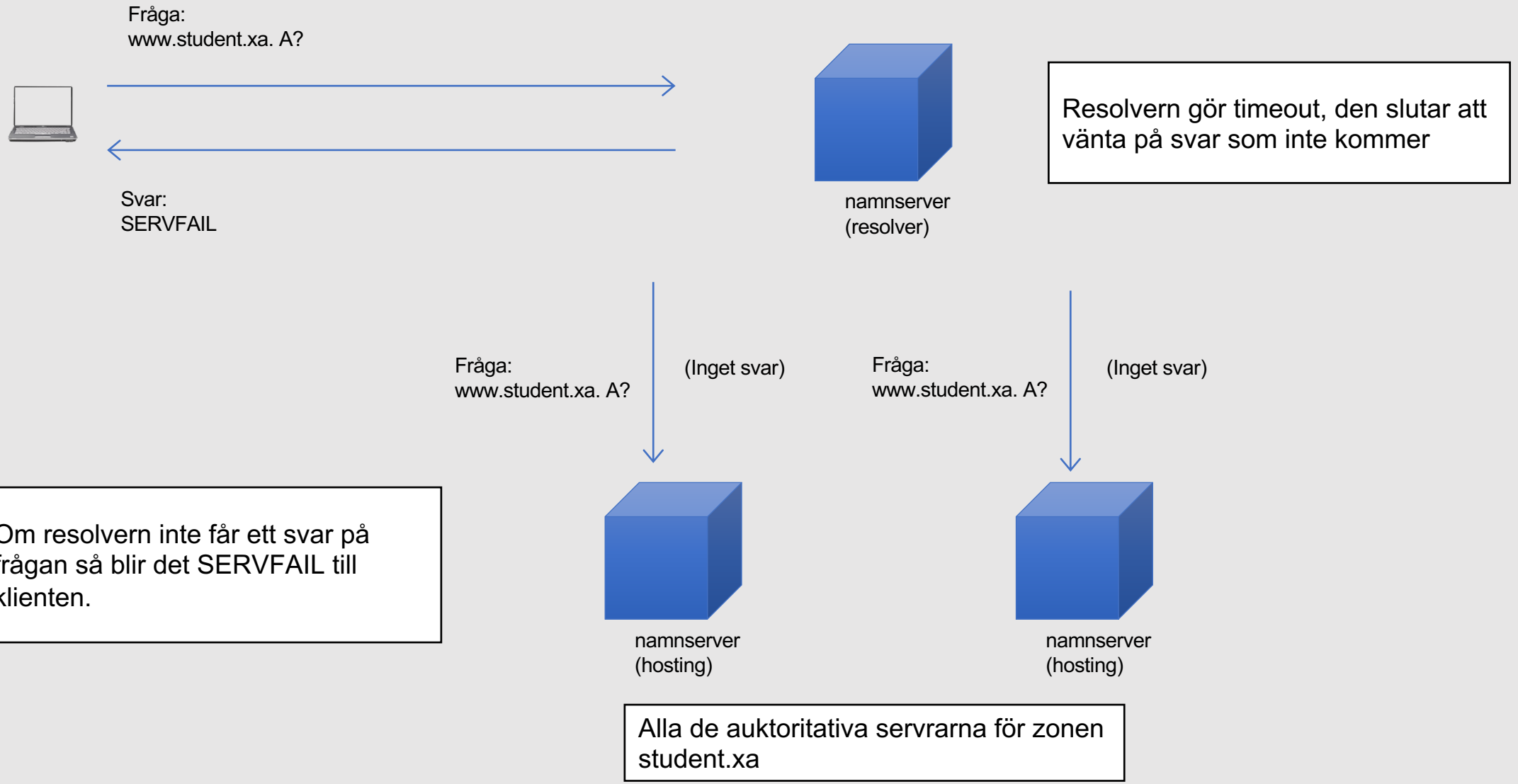
Timeout är ingen RCODE.

```
$ dig @81.228.11.69 www.telia.com

; <<>> DiG 9.10.6 <<>> @81.228.11.69 www.telia.com
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
```

Timeout – ingen RCODE

Om dig skickar en fråga till en resolver, som sedan skickar en fråga till en namnserver som aldrig svarar, så är det resolvern som gör ***timeout*** (ger upp).

- När resolvern har gjort ***timeout*** så skickar den ett DNS-svar tillbaka till "dig".
- När resolvern aldrig får svar så blir RCODE till "dig" ***SERVFAIL***. (Se nästa bild.)


Fråga:
www.student.xa. A?
Svar:
SERVFAIL
namnserver
(resolver)
Resolvern gör timeout, den slutar att vänta på svar som inte kommer
Fråga:
www.student.xa. A?
(Inget svar)
Fråga:
www.student.xa. A?
(Inget svar)
Om resolvern inte får ett svar på frågan så blir det SERVFAIL till klienten.
namnserver
(hosting)
namnserver
(hosting)
Alla de auktoritativa servrarna för zonen student.xa

FORMERR

RCODE ***FORMERR*** är inte så vanlig. Det är en gammal server som inte klarar modern DNS, t.ex. EDNS (kommer senare i denna föreläsning).

▶Message ID i DNS-paketet

[Till Innehåll]

Message ID

Query och ***response*** binds ihop genom ett **message id** som sätts i **query** och sedan tas med i **response**.

Response måste också komma från samma IP och port som ***query*** skickades till.

”Message ID”

```
; <<>> DiG 9.10.6 <<>> nic2.lth.se a +qr +noedns
;; global options: +cmd
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58107
;; flags: rd ad; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;nic2.lth.se. IN A

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58107
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;nic2.lth.se. IN A

;; ANSWER SECTION:
nic2.lth.se. 3389 IN A 130.235.20.5

;; Query time: 54 msec
;; SERVER: 172.17.41.10#53(172.17.41.10)
;; WHEN: Mon Jan 21 23:43:27 CET 2019
;; MSG SIZE  rcvd: 45
```

▶Rotzonen och hint-filen

[Till Innehåll]

Rotzonen

Rotzonen (***root zone***) har en central roll i domännamnsträdet.

- Rotzonen är gemensam för Internet.
- Alla domäner på Internet förenas i en rot (rotzon).
- Rotzonen är startpunkten för domännamnsträdet.

Rotzonen

- Rotzonen har inget namn, men kallas ofta för ”.”
  - ”dig . NS” ger rotzonens NS-poster (NS-posterna i rotnoden).
  - I namnserververns konfiguration (named.conf) så kallas den för ”.”.
  - Rotzonens (och rotnodens) namn är egentligen ”” (tomma strängen).
- Vi måste veta var rotzonen finns innan vi startar en DNS-uppslagning. Allt annat kan vi slå upp genom att starta i rot och söka oss nedåt.

Hint-fil

Alla resolvrar konfigureras med en lista över kända rotnamnservrar, både namn och IP-adress.

- Det kallas för en hint-fil (”hint” = tips).
- Innehåller NS-, A- och AAAA-poster, d.v.s. namn och IP-adress till rotnamnservrarna.
- Innehållet i hint-filen laddas inte auktoritativt, utan som cache.

Rotzonen

```
; <<>> DiG 9.10.6 <<>> . ns +noedns @a.root-servers.net. +norec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64079
;; flags: qr aa; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13


;; QUESTION SECTION:
;. IN NS


;; ANSWER SECTION:
. 518400 IN NS e.root-servers.net.
. 518400 IN NS h.root-servers.net.
. 518400 IN NS l.root-servers.net.
. 518400 IN NS i.root-servers.net.
. 518400 IN NS a.root-servers.net.
. 518400 IN NS d.root-servers.net.
. 518400 IN NS c.root-servers.net.
. 518400 IN NS b.root-servers.net.
. 518400 IN NS j.root-servers.net.
. 518400 IN NS k.root-servers.net.
. 518400 IN NS g.root-servers.net.
. 518400 IN NS m.root-servers.net.
. 518400 IN NS f.root-servers.net.

(...)
```

Vi frågar efter ”. NS” för att få NS-posterna i rotnoden.

Svar från en rotnamnserver om NS-posterna för rot.

Hint-fil

Efter start kommer resolvern att använda hint-filen för att slå upp NS och A/AAAA för rotzonen, d.v.s. bekräfta informationen i hint-filen.

Resolvern använder informationen om rotnamnservrarna för att kunna gå vidare i DNS-trädet.

Hint-fil

```
(...)
.                       3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.     3600000      AAAA  2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                       3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000      A     199.9.14.201
B.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:200::b
;
; FORMERLY C.PSI.NET
;
.                       3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.     3600000      A     192.33.4.12
C.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:2::c
;
; FORMERLY TERP.UMD.EDU
;
.                       3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.     3600000      A     199.7.91.13
D.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:2d::d
;
; FORMERLY NS.NASA.GOV
;
(...)
```

På labbservrarna så finns hela filen som /usr/share/dns/root.hints

Kan det finnas flera rot?

DNS tillåter bara en rot i taget. Varje domännamn måste vara unikt definierat.

- Strikt sett så kan det finnas olika rot för olika grupper även om alla grupper delar samma rymd av IP-adresser.
- I stort sett alla på Internet använder i stort sett samma rot, men det finns säkert modifierade rot, kanske i vissa länder.
  - För roaming på mobilnätet används ett eget DNS-träd för deras slutna del av Internet.

▶Transportprotokoll och paketstorlek

[Till Innehåll]

Transportprotokoll – UDP och TCP

- UDP:
  - Ingen handskakning, ingen bekräftelse och ingen förbindelse.
  - Hela meddelandet i ett (UDP-) paket åt ett håll.
    - För DNS: ”Query” i ett UDP-paket och ”response” i ett annat.
- TCP:
  - Handskakning och bekräftelse. En förbindelse upprättas.
  - Flera (TCP-) paket, åt båda hållen.
    - För DNS: ”Query” och ”response” skickas i samma förbindelse (TCP-ström).

Paketstorlek i DNS

Ett UDP-paket betyder inte nödvändigtvis ett IP-paket.

- Om ett UDP-paket blir större än MTU (***maximum transmission unit***) så kommer UDP-paketet delas upp i två eller flera fragment och skickas som lika många IP-paket.

Paketstorlek i DNS

När DNS standardiserades så ansågs fragmenteringen (av UDP) vara ett problem. För att kunna passa in minsta MTU så maximerades storleken på ett DNS-UDP-paket till 512 bytes (oktetter) plus ”headers”:

> *Messages carried by UDP are restricted to 512 bytes (not counting the IP or UDP headers). Longer messages are truncated and the TC bit is set in the header.*
>
> (RFC 1035)

512 bytes är alltså maximal storlek på ett DNS-paket (om inte EDNS används).

(RFC 1035 ingår i kurslitteraturen.)

Paketstorlek

```
; <<>> DiG 9.10.6 <<>> www.kth.se
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23158
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1


;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.kth.se. IN A


;; ANSWER SECTION:
www.kth.se. 392 IN A 130.237.28.40


;; Query time: 1 msec
;; SERVER: 172.16.43.15#53(172.16.43.15)
;; WHEN: Wed Jan 23 11:14:13 CET 2019
;; MSG SIZE  rcvd: 55
```

Stora DNS-paket

Stora DNS-paket kan skickas över TCP, men det är ***query*** som väljer UDP eller TCP. ***Response*** måste alltid gå tillbaka över samma protokoll som ***query***.

- Om ***query*** går över UDP och full information inte får plats i ***response*** så blir informationen avklippt (***truncated***). Namnservern sätter **TC**-flaggan i ***response***.

Query kan sedan skickas om över TCP så att full information får plats i ***response***.

Trunkerat paket, utan omsändning

```
; <<>> DiG 9.10.6 <<>> kth.se any +noedns +ignore +mult @a.ns.kth.se +norec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34368
;; flags: qr aa tc; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;kth.se.                IN ANY

;; ANSWER SECTION:
kth.se.                1800 IN  SOA a.ns.kth.se. hostmaster.kth.se. (
                       2019012043 ; serial
                       14400      ; refresh (4 hours)
                       900        ; retry (15 minutes)
                       604800     ; expire (1 week)
                       86400      ; minimum (1 day)
                       )
(…)
;; Query time: 49 msec
;; SERVER: 2001:6b0:1::246#53(2001:6b0:1::246)
;; WHEN: Wed Jan 23 11:24:17 CET 2019
;; MSG SIZE  rcvd: 450
```

"dig" ska inte göra någon omförfrågan över TCP vid trunkerat svar.

Trunkerat.

I senare versionen av “dig” (som används på labbarna) så måste man kombinera “+ignore” med “+notcp” om man frågar efter ANY. För säkerhets skull, gör det alltid.

Mer om ANY semare i denna presentation.

Trunkerat paket, med omsändning

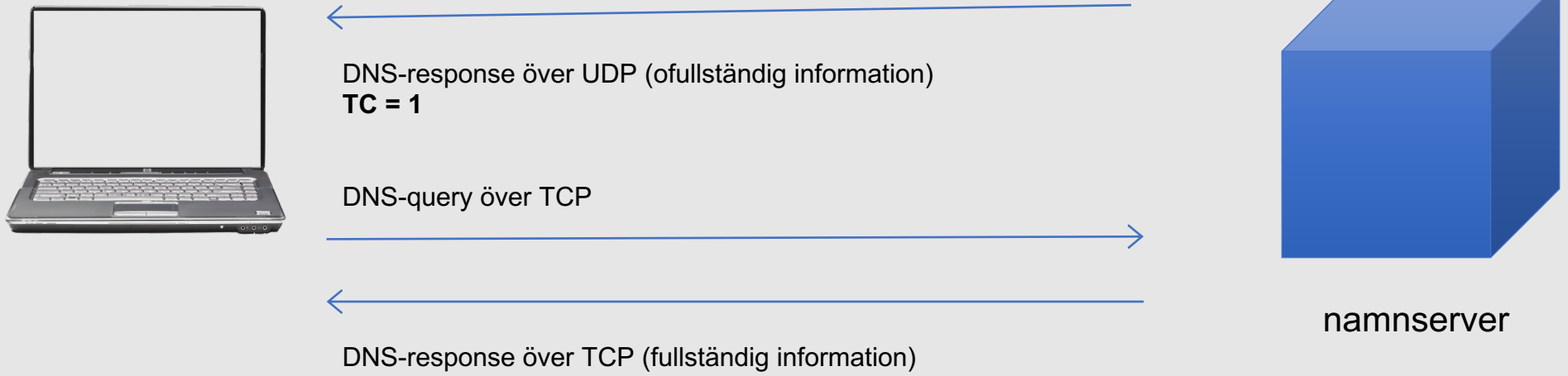
```
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.10.6 <<>> kth.se any +noedns +mult @a.ns.kth.se +norec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9147
;; flags: qr aa; QUERY: 1, ANSWER: 36, AUTHORITY: 0, ADDITIONAL: 15

;; QUESTION SECTION:
;kth.se.                IN ANY

;; ANSWER SECTION:
kth.se.                1800 IN  SOA a.ns.kth.se. hostmaster.kth.se. (
                       2019012043 ; serial
                       14400      ; refresh (4 hours)
                       900        ; retry (15 minutes)
                       604800     ; expire (1 week)
                       86400      ; minimum (1 day)
                       )
(…)
;; Query time: 5 msec
;; SERVER: 2001:6b0:1::246#53(2001:6b0:1::246)
;; WHEN: Wed Jan 23 11:26:14 CET 2019
;; MSG SIZE  rcvd: 4957
```

”dig” rapporterar att svaret var trunkerat. Visar bara svaret över TCP.

I senare versionen av “dig” (som används på labbarna) så måste man ange “+notcp” om man frågar efter ANY och vill ha UDP från början. Om det inte börjar med UDP så för man inte texten “retrying in TCP mode”.

Större än vad som får plats i ett vanligt DNS-paket över UDP.

Omsändning vid trunkering (schematiskt)



Varför inte alltid TCP?

UDP är billigare och går normalt sett snabbare.

- UDP:
  - Två paket, ***query*** och ***response***.
- TCP:
  - Three-way-handshake (tre paket).
  - Två paket, ”query” och ”response”.
  - Två avslutande paket.

UDP används i första hand för normala DNS-frågor.

DNS och brandväggar

Om brandväggen framför en namnserver inte tillåter UDP så kommer det snart att upptäckas. UDP är grundläggande.

Om brandväggen inte tillåter TCP så är det först vid trunkering som tvingar fram TCP som problemet kommer. Kan vara svårfunnet.

Själva synkroniseringen mellan master och slav (zonöverföring) kräver TCP, men initieringen baseras på UDP (mera senare).

TCP/UDP port

En namnserver svarar alltid på port 53.

Undantag? Bara i interna lösningar. Det måste konfigureras speciellt för att hitta andra portar.

(DNS-frågor över krypterad förbindelse använder annan port. Mer om det i senare föreläsning.)

▶EDNS – Utökning av DNS

[Till Innehåll]

EDNS

- EDNS = ”Extension Mechanisms for DNS”

Det dök upp behov av att kunna signalera ny information i DNS-paketet.

Beslutet togs att inte ändra det grundläggande formatet av DNS-paketet.

Utvidgningen görs genom att en speciell posttyp **OPT** placeras i ”additional section”. OPT används inte för egentlig DNS-data.

OPT

Vi visar aldrig **OPT** som en vanligt DNS-post eftersom den hanteras och används på ett speciellt sett. I DNS-paketet skickas den som en vanlig DNS-post, men t.ex. TTL används inte för TTL.

"dig" visar OPT-posten på ett speciellt sätt.

EDNS

Om klienten inte stödjer EDNS (inte inkluderar OPT) så kommer servern inte att inkludera OPT (***response*** utan EDNS).

Om klienten inkluderar EDNS, men servern inte stödjer det så ska servern svara med RCODE **FORMERR**. Klienten skickar då om frågan utan EDNS.

Moderna versioner av DNS-programvaror stödjer EDNS. Vidare utökningar av DNS-protokollet, t.ex, DNSSEC, bygger på EDNS.

Vad tillför EDNS?

- UDP-paketet kan bli större än 512 bytes (oktetter).
- Både klient och server signalerar storleken den stödjer.
  - Med EDNS så kommer alltid maximal storlek för DNS-paket över UDP att signaleras.
- Med EDNS så går det att skicka signaler mellan klient och server som inte är den egentliga DNS-datan. Vi åter kommer till det senare, bland annat när vi kommer till DNSSEC.

UDP-gräns med EDNS

Med EDNS så kan i teorin UDP-paketet bli 64 kB stort. Alltid minst 512 Byte.

Rekommendationen är att hålla sig till maximalt 4 kB, vilket är det som ”dig” och namnservrar normalt håller sig till.

Query med EDNS

```
; <<>> DiG 9.10.6 <<>> nic2.lth.se a +qr
;; global options: +cmd
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59828
;; flags: rd ad; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;nic2.lth.se. IN A
```

OPT finns i ”additional” och räknas med, men visas inte av ”dig” under ”Addition section”

Klienten stödjer 4096 byte (oktetter) i detta fall.

Alltid version 0

Response med EDNS

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59828
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;nic2.lth.se. IN A

;; ANSWER SECTION:
nic2.lth.se. 3599 IN A 130.235.20.5

;; Query time: 54 msec
;; SERVER: 172.17.41.10#53(172.17.41.10)
;; WHEN: Tue Jan 22 00:41:36 CET 2019
;; MSG SIZE  rcvd: 56
```

OPT finns i ”additional” och räknas med.

Servern stödjer 4000 Byte (oktetter) i detta fall.

Stort paket över UDP med EDNS

```
; <<>> DiG 9.10.6 <<>> @a.ns.se se any +mult +norec
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46016
;; flags: qr aa; QUERY: 1, ANSWER: 21, AUTHORITY: 0, ADDITIONAL: 21

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;se.                IN ANY

;; ANSWER SECTION:
se.                172800 IN SOA catcher-in-the-rye.nic.se. registry-default.nic.se. (
                          2019012313 ; serial
                          1800       ; refresh (30 minutes)
                          1800       ; retry (30 minutes)
                          864000     ; expire (1 week 3 days)
                          7200       ; minimum (2 hours)
                          )
(...)
;; Query time: 49 msec
;; SERVER: 2a01:3f0:0:301::53#53(2a01:3f0:0:301::53)
;; WHEN: Wed Jan 23 15:01:58 CET 2019
;; MSG SIZE  rcvd: 3095
```

Det är klientens val av maximalt UDP-paket (som vi inte ser på denna bild) som avgör hur stort svaret kan vara, inte servern val (som vi ser på denna bild).

Avkortat svar för att få plats på bilden. 21 poster i svaret.

▶Paketstorlek och fragmentering

[Till Innehåll]

Paketstorlek i DNS

Om ett UDP-paket blir större än MTU så kommer det att fragmenteras i flera IP-paket.

Fragmentering är inte oproblematiskt.

Fragmentering i IPv4

Fragmentering i IPv4 kan göras var som helst i transportvägen. Om ett paket når ett nätverk med mindre MTU så delas det i fragment.

Fragmentering i IPv6

IPv6-standarden tillåter bara fragmentering i källan. Om ett paket når ett nät med mindre MTU så kastas paketet och ett ICMPv6-paket skickas tillbaka.

Begränsa fragmentering?

Om man får problem med stora ***responses*** så kan man prova att sätta ner maximala UDP-paketet under EDNS till 1232 B för att, med headrar, komma under MTU 1280, vilken är den minsta MTU IPv6 stödjer.

Begränsa fragmentering?

Det finns även de som argumenterar för att alltid hålla storleken under den gräns som gör att det finns risk för fragmentering enligt föregående bild, d.v.s. för att förebygga problem istället för att vänta på dem.

Begränsingen gör man för både klient och server i DNS-resolvern och för server i DNS-hostingservern.

Förslaget är då att sätta gränsen till 1280 Byte.

▶Frågetyp kontra posttyp

[Till Innehåll]

Frågetyp kontra posttyp

I en DNS-fråga så anger man domännamn och frågetyp. Alla posttyper kan användas som frågetyp och då frågar man efter den posttypen, t.ex.

kth.se. A
kth.se. AAAA
kth.se. MX

Det finns dock posttyper som det inte är meningsfullt att fråga efter eftersom sådan post aldrig kommer att svaras på. Ett sådant exempel är ”OPT”. Den hör till EDNS och kommer automatiskt när EDNS är påslaget, men hör inte till någon zon och kan inte frågas efter.

Frågetyp kontra posttyp

Det finns vissa frågetyper som inte kan vara posttyper.

- ANY (”*”) är ett exempel (se nedan).
- På nästa föreläsning kommer AXFR och IXFR.
- Det finns några till, som vi inte tar upp.

▶Frågetyp ANY

[Till Innehåll]

Frågetyp * (ANY)

Om frågetypen sätts till ”ANY” i frågan så kommer servern oftast att skicka alla tillgängliga poster under det domännamnet.

```
dig kth.se. ANY
```

Observera att domännamnet här – som alltid i DNS-sammanhang – betyder den utpekade noden (kth.se ovan), inte inklusive ev. underliggande noder (t.ex. www.kth.se).

Fråga efter ANY

```
; <<>> DiG 9.10.6 <<>> @dns1.telia.com telia.com any +noedns +norec
(...)

;; ANSWER SECTION:
telia.com.        3600 IN   SOA dns1.telia.com. backbone.telia.net. 2020010704 10800 3600 604800 3600
telia.com.        3600 IN   TXT "google-site-verification=N48W5sPvXvxEYWSkDntnCoh-AILPmA-IP56QBvYHAmU"
telia.com.        3600 IN   TXT "v=spf1 ip4:81.236.60.128/26 ip4:81.236.60.192/28 (...)"
telia.com.        3600 IN   A    81.236.63.162
telia.com.        3600 IN   MX   1 mail.telia.com.
telia.com.        3600 IN   NS   dns49.de.telia.net.
telia.com.        3600 IN   NS   dns1.telia.com.
telia.com.        3600 IN   NS   ns02.savvis.net.
telia.com.        3600 IN   NS   dns2.telia.com.
telia.com.        3600 IN   NAPTR    90 50 "s" "SIP+D2U" "" _sip._udp.telia.com.
telia.com.        3600 IN   NAPTR    50 50 "s" "SIP+D2T" "" _sip._tcp.telia.com.

(...)
```

Trunkerad post för visningens skull.

Frågetyp * (ANY)

- En resolver har kanske inte har allt och skickar vad som finns i sin cache. Man får kanske inte det man behöver.
- En auktoritativ server *kan* skicka allt, men behöver inte.
- Vissa servrar skickar så lite som möjligt och det är OK.

Frågetyp * (ANY)

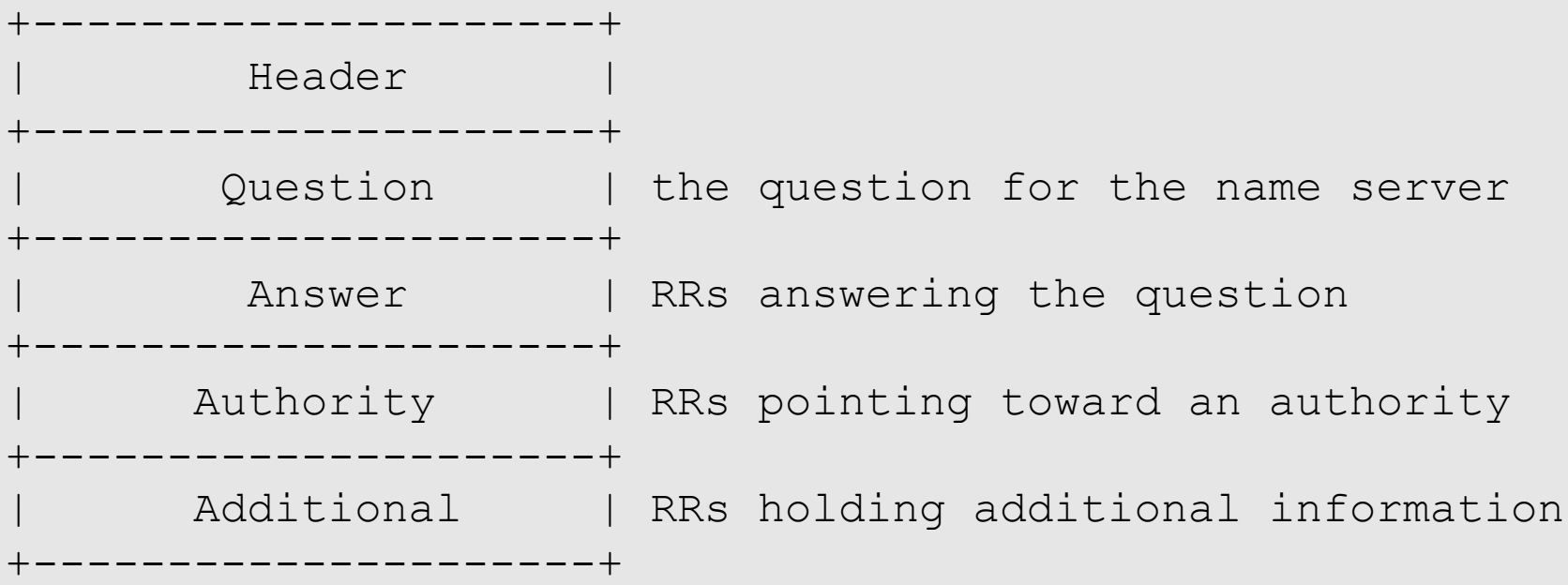
Inga system som t.ex. mail eller webb använder ”ANY”. Används bara för DNS-kontroller.

Använd aldrig ”ANY” för att få en specifik DNS-post. Kan dock användas för att få stora svar om man vill ha det för DNS-tester. Som vi gjorde tidigare i denna presentation.

▶DNS-paketets uppbyggnad

[Till Innehåll]

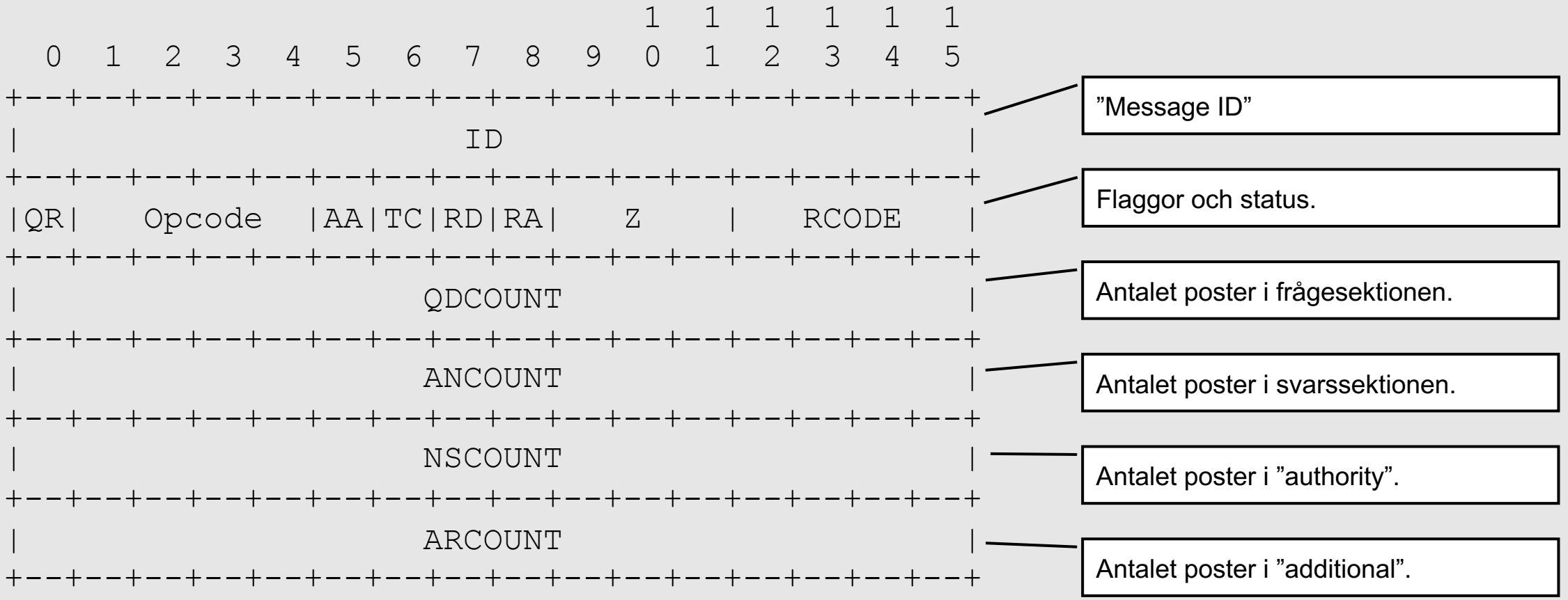
DNS-paketets huvuddelar



Från RFC 1035, 4.1, s 25.

Jfr med ett DNS-svar från ”dig”.

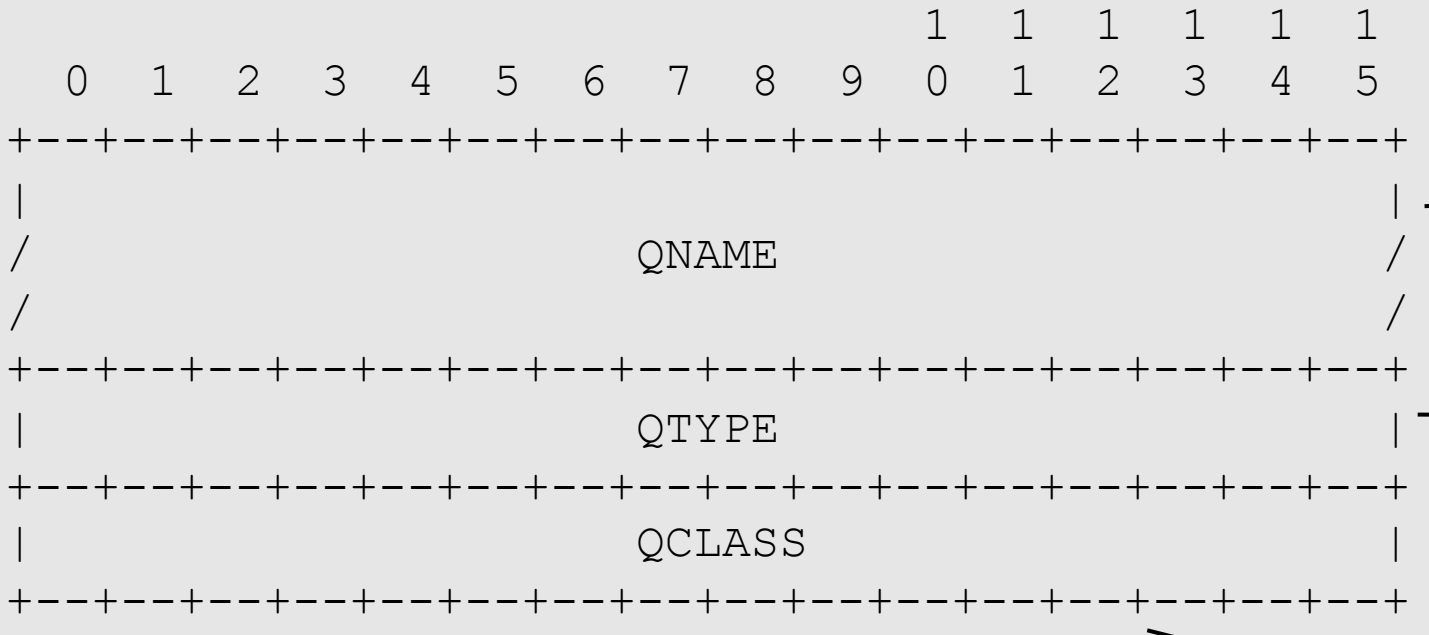
DNS-paketets header



Från RFC 1035, 4.1.1, s 26.

Jfr med ett DNS-svar från ”dig”.

Post i ”Question section”



Namnet, ”owner name”, som frågan gäller.

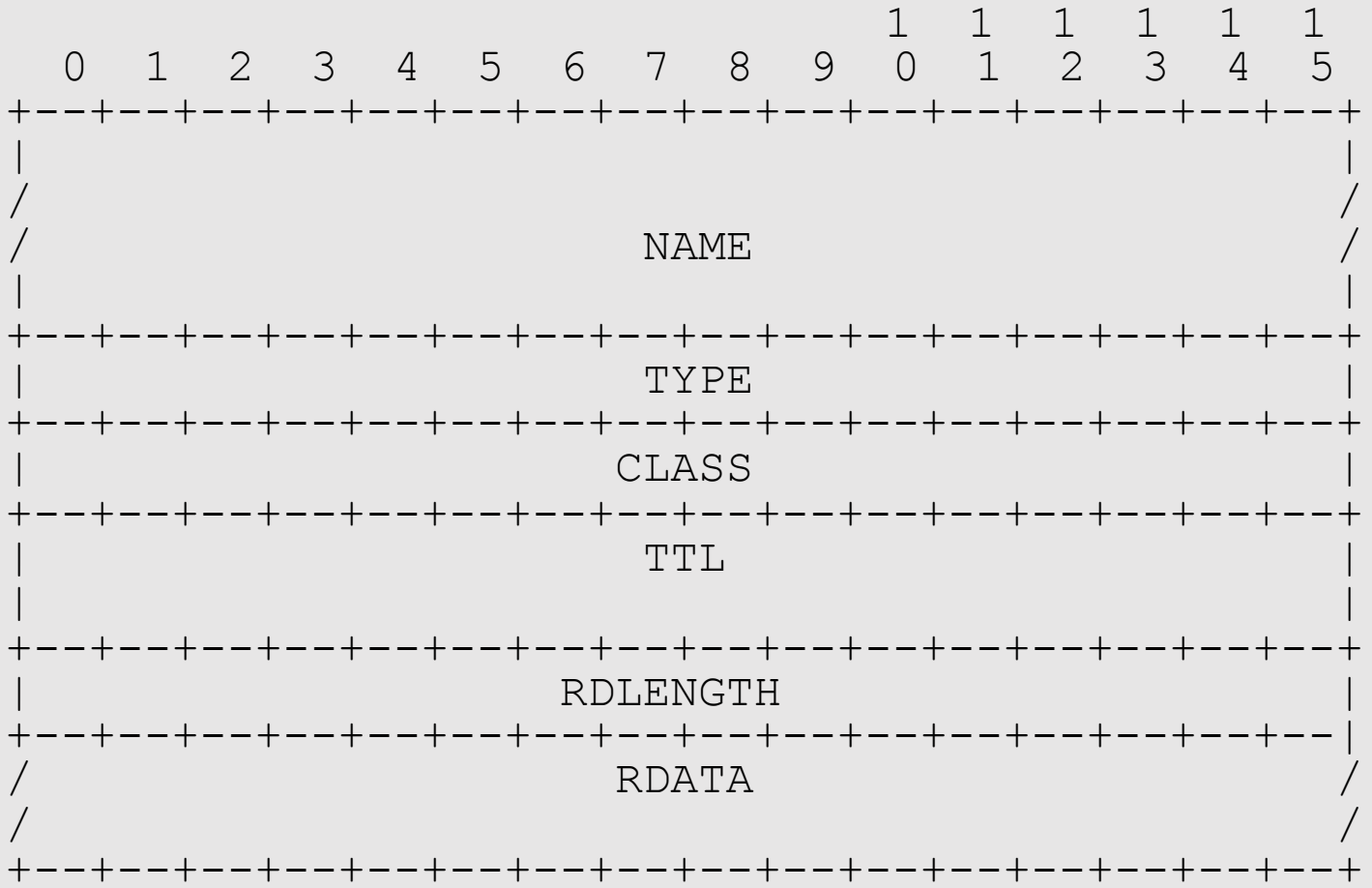
Antingen en posttyp (t.ex. A eller AAAA) som frågan gäller eller en speciell frågetyp som inte motsvarar en poststyp, t.ex. ANY eller AXFR.

Klass är alltid IN i det vi täcker i denna kurs, men måste anges.

Från RFC 1035, 4.1.2, s 28.

Upprepas för varje post i ”question section”. Normal är det 1 (en). Antalet anges i headern.

DNS-post



Från RFC 1035, 4.1.3, s 29.

Samma format på DNS-post i *answer*, *authority* och *additional section*.

Upprepas för varje post i sektionen. Antalet anges i headern för varje sektion.

Samma struktur för ”answer section”, ”authority section” och ”additional section”.

Strukturen på RDATA beror helt på poststypen.

▶Glue-poster

[Till Innehåll]

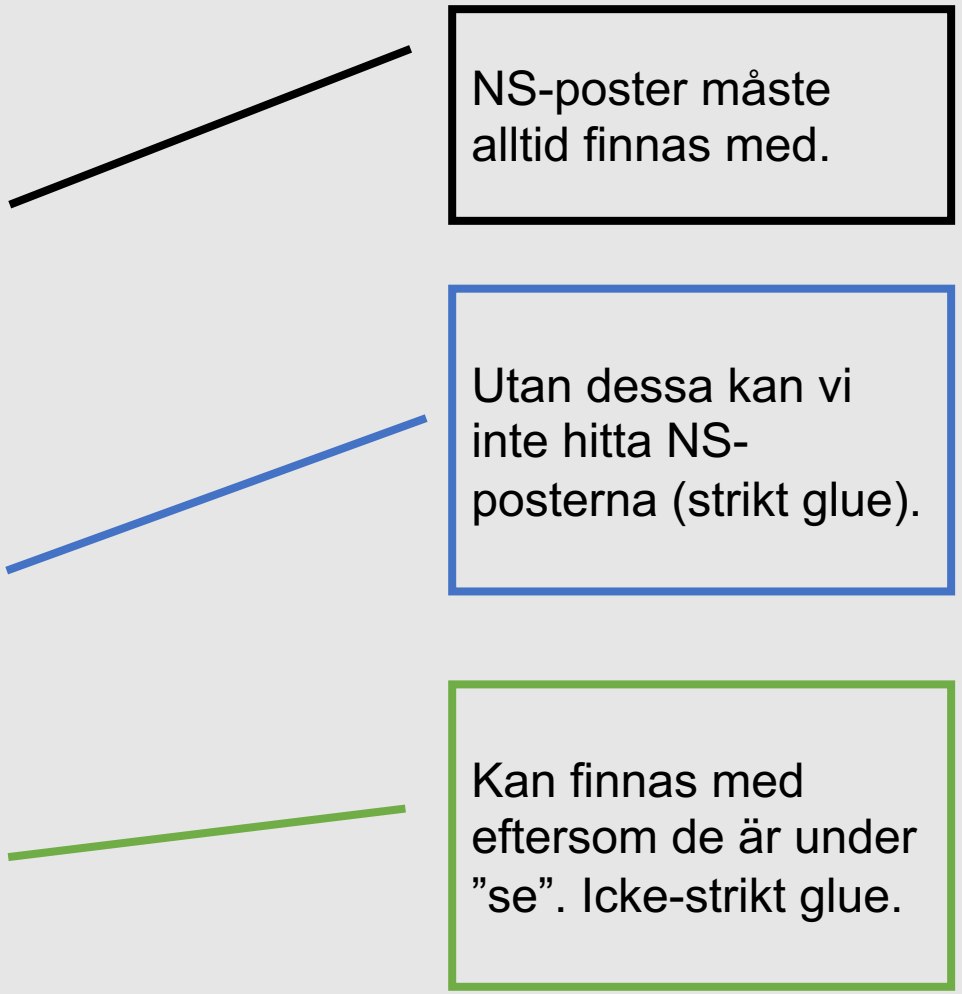
Glue-poster

Delegering av kth.se från se:

```
kth.se.            NS a.ns.kth.se.
kth.se.            NS ns2.chalmers.se.
kth.se.            NS b.ns.kth.se.
kth.se.            NS nic2.lth.se.
```

```
a.ns.kth.se.       A 130.237.72.246
a.ns.kth.se.       AAAA 2001:6b0:1::246
b.ns.kth.se.       A 130.237.72.250
b.ns.kth.se.       AAAA 2001:6b0:1::250
```

```
ns2.chalmers.se. A 129.16.253.252
ns2.chalmers.se. AAAA 2001:6b0:2:20::1
nic2.lth.se.       A 130.235.20.5
```



NS-poster måste alltid finnas med.

Utan dessa kan vi inte hitta NS-posterna (strikt glue).

Kan finnas med eftersom de är under ”se”. Icke-strikt glue.

Glue-poster

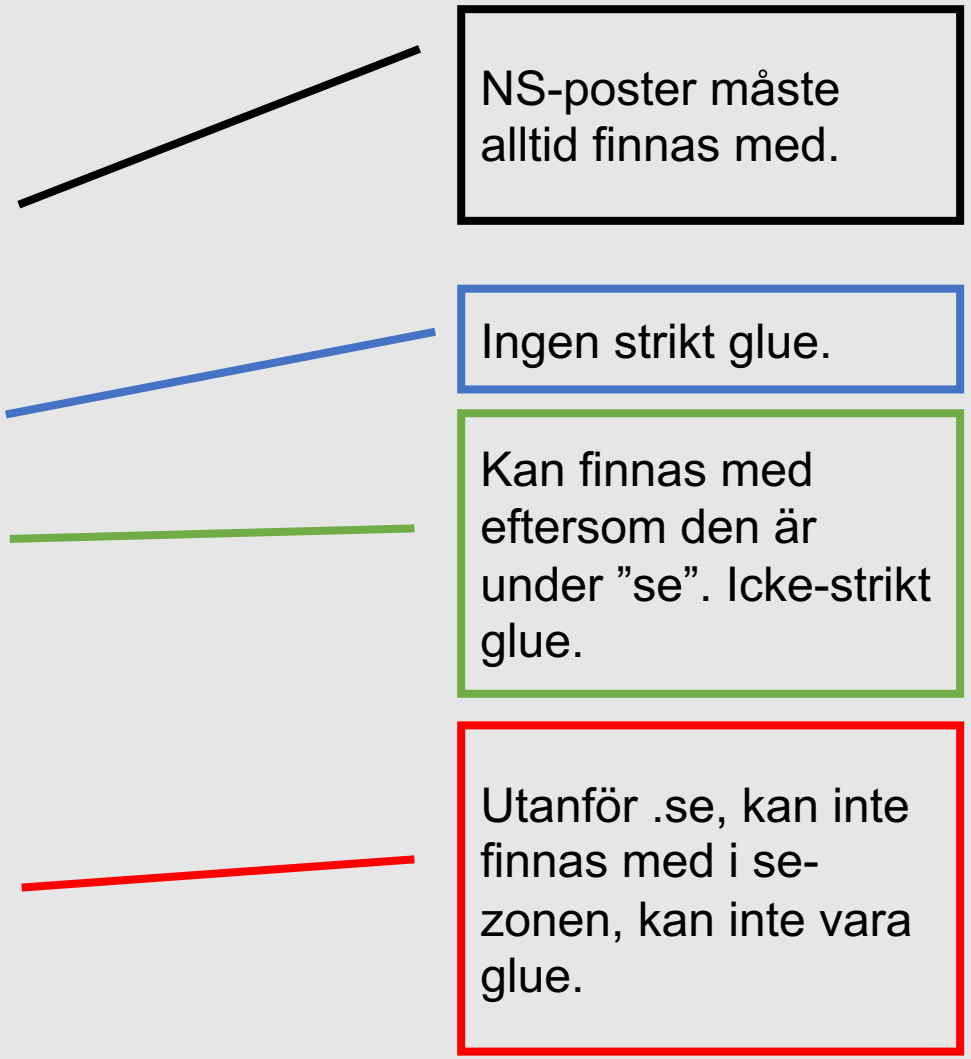
Delegering av wikipedia.se från se:

```
wikipedia.se. NS ns.aname.net.
wikipedia.se. NS ns3.aname.se.
wikipedia.se. NS ns2.aname.net.
```

```
ns3.aname.se. A 195.35.82.105
```

Utanför delegeringen:

```
ns.aname.net. A 195.35.82.101
ns2.aname.net. A 89.221.245.42
```



▶Domännamnsträd och zonindelning

[Till Innehåll]

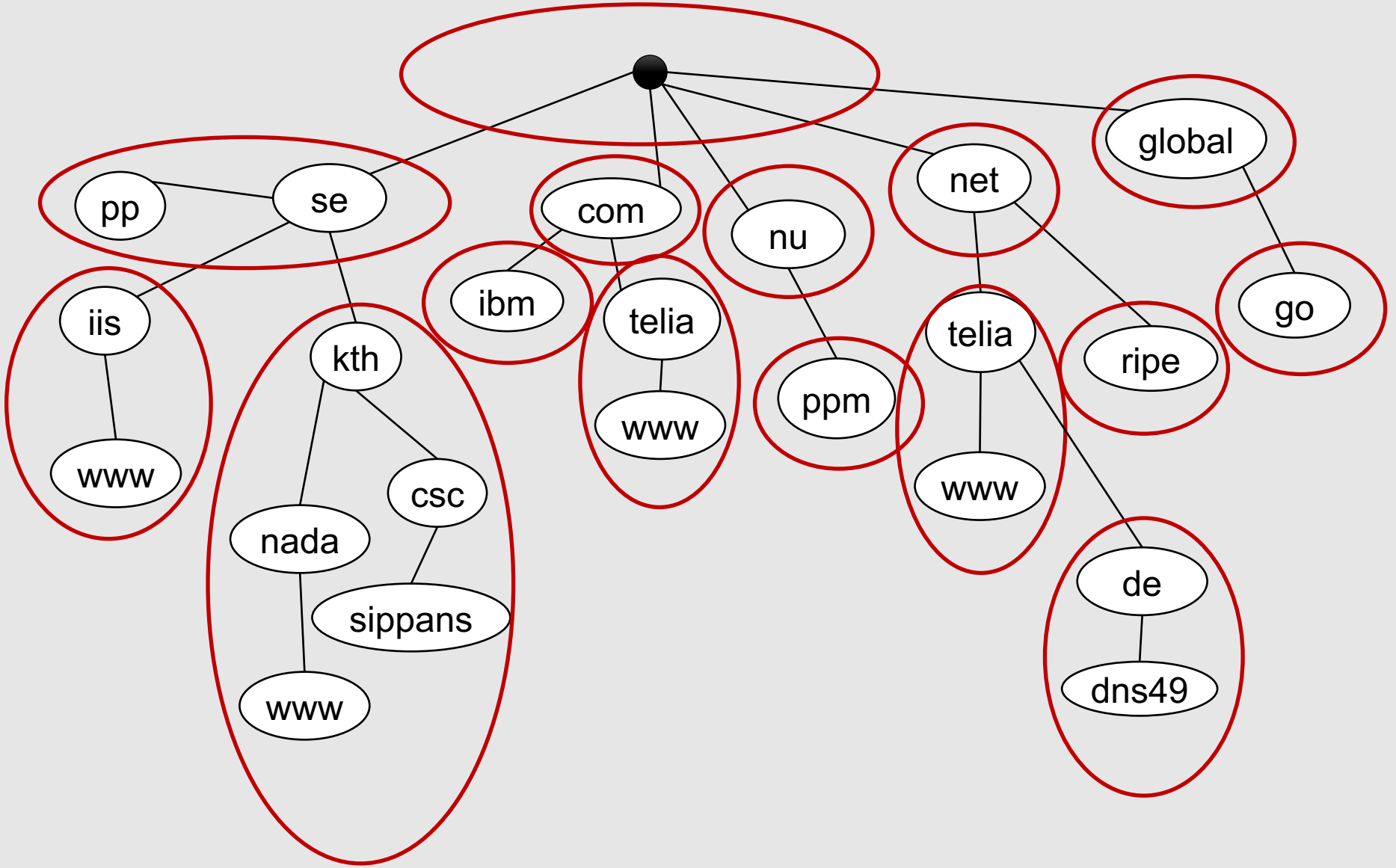
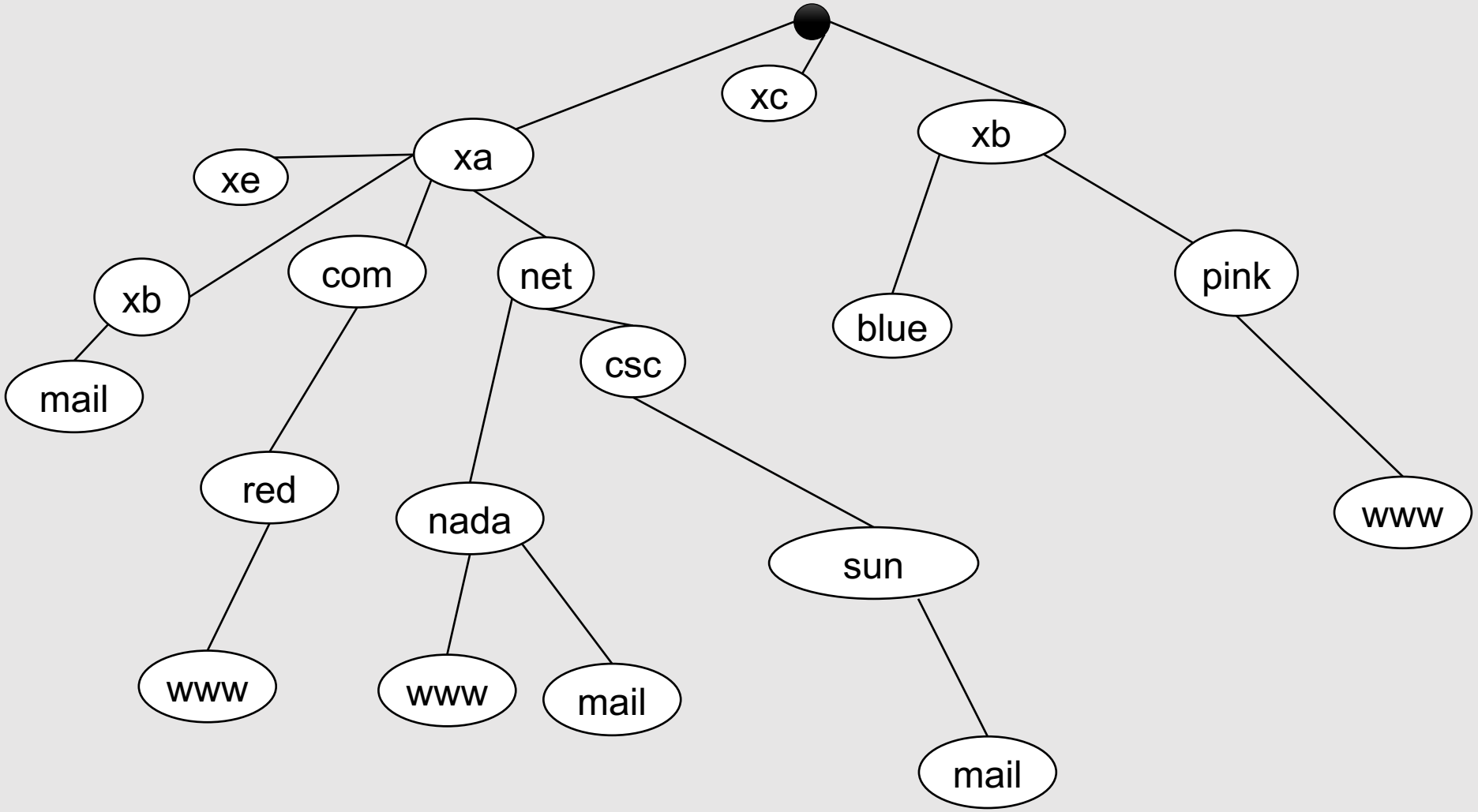
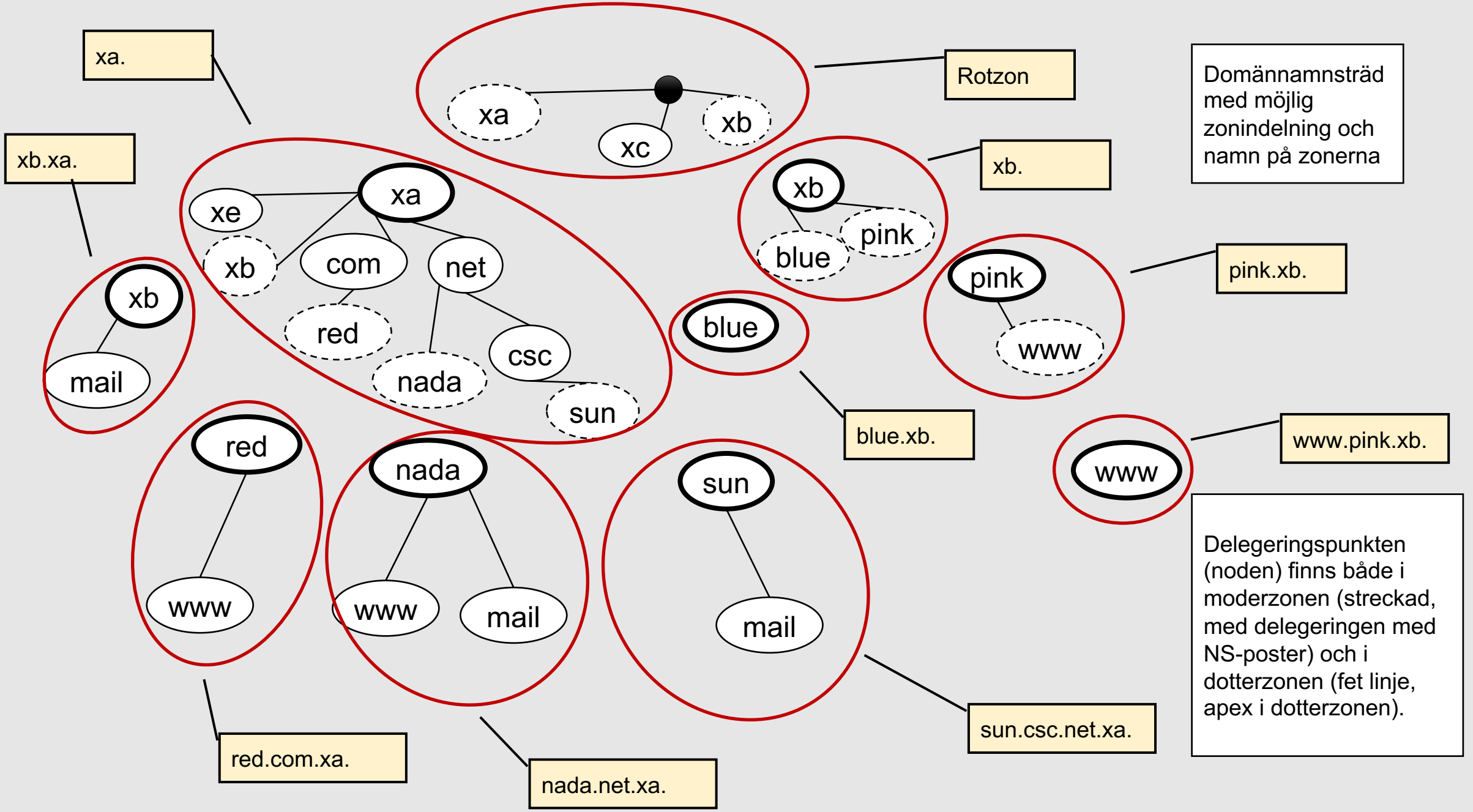


Bild från FL02.

Domännamnsträd




xa.
xb.xa.
xa
xc
xb
Rotzon
Domännamnsträd med möjlig zonindelning och namn på zonerna
xa
xe
xb
com
net
red
nada
csc
sun
xb
mail
xb
pink
blue
xb.
pink
www
pink.xb.
blue
blue.xb.
www
www.pink.xb.
red
www
nada
www
mail
sun
mail
Delegeringspunkten (noden) finns både i moderzonen (streckad, med delegeringen med NS-poster) och i dotterzonen (fet linje, apex i dotterzonen).
red.com.xa.
nada.net.xa.
sun.csc.net.xa.

▶Om presentationen

[Innehåll]

Internets domännamnssystem

Denna presentation är framtagen 2019–2023 av Mats Dufberg på Internetstiftelsen (https://internetstiftelsen.se/). Den är en del av undervisningsmaterialet för kursen ”Internet domännamnssystem” vid Kungliga tekniska högskolan, KTH (kurskod HI1037) resp. Karlstads universitet, KAU (kurskod DVGC28).

Licens

Dokumenthistorik

- Rev A: Ursprunglig version HT 2023
- Rev B: Uppdaterat bild 112

Slut.

[Till Innehåll]