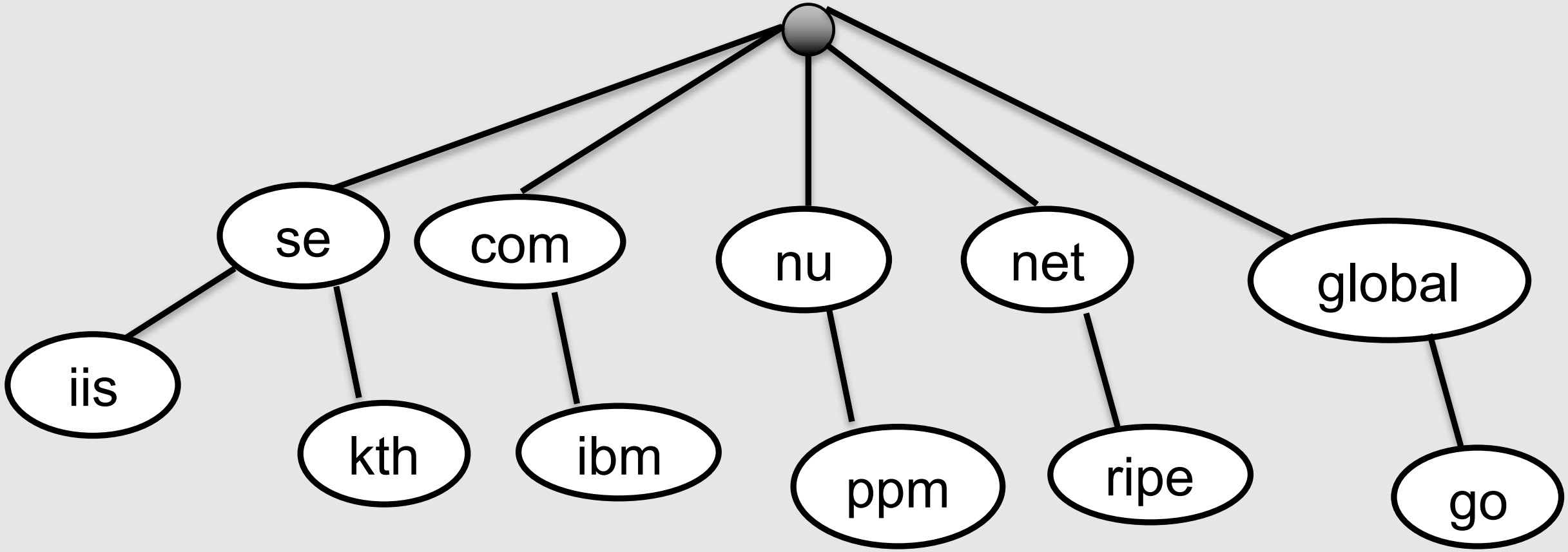

se
com
nu
net
global
iis
kth
ibm
ppm
ripe
go

INTERNET STIFTELSEN

Internets domännamnssystem*

Föreläsning FL09, VT 2024

Mats Dufberg

* Se “Internets domännamnssystem”

Innehåll

▶Begränsningar i NSEC-modellen

[Till Innehåll]

Zone walking

Förra föreläsningen avslutades med en diskussion om ”zone walking”.

Begränsningar i NSEC-modellen

- NSEC skapar en kedja från apex till nästa namn i zonen (med data) och till nästa och nästa till sista namnet i zonen.
- NSEC listar alla posttyper som finns samma ”owner name” som den aktuella NSEC-posten.
- Nu kan vi hämta hela zoninnehållet utan AXFR:
  - Vi kan fråga efter NSEC som vilken annan DNS-posttyp.
  - Vi kan fråga efter de andra posttyperna

Begränsningar i NSEC-modellen

- Vi såg att ”online signing” är en möjlig lösning på problemet med ”zone walking”.
  - Det finns begräningar med ”online signing” som gör att det inte alltid är möjligt eller önskvärt.
    - Den privata nyckeln till DNSKEY måste finnas på alla slavar.
    - Den färdiga zonen finns inte och kan därmed inte valideras.

- Om begränsning av åtkomst av zoninnehållet är viktigt så är NSEC ett problem.

▶NSEC3 och NSEC3PARAM

[Till Innehåll]

NSEC3

För att komma runt problemen med NSEC så skapades en alternativ posttyp med samma grundläggande funktion som NSEC:

- NSEC3

NSEC eller NSEC3

I de fall NSEC3 används så används inte NSEC. Och omvänt.

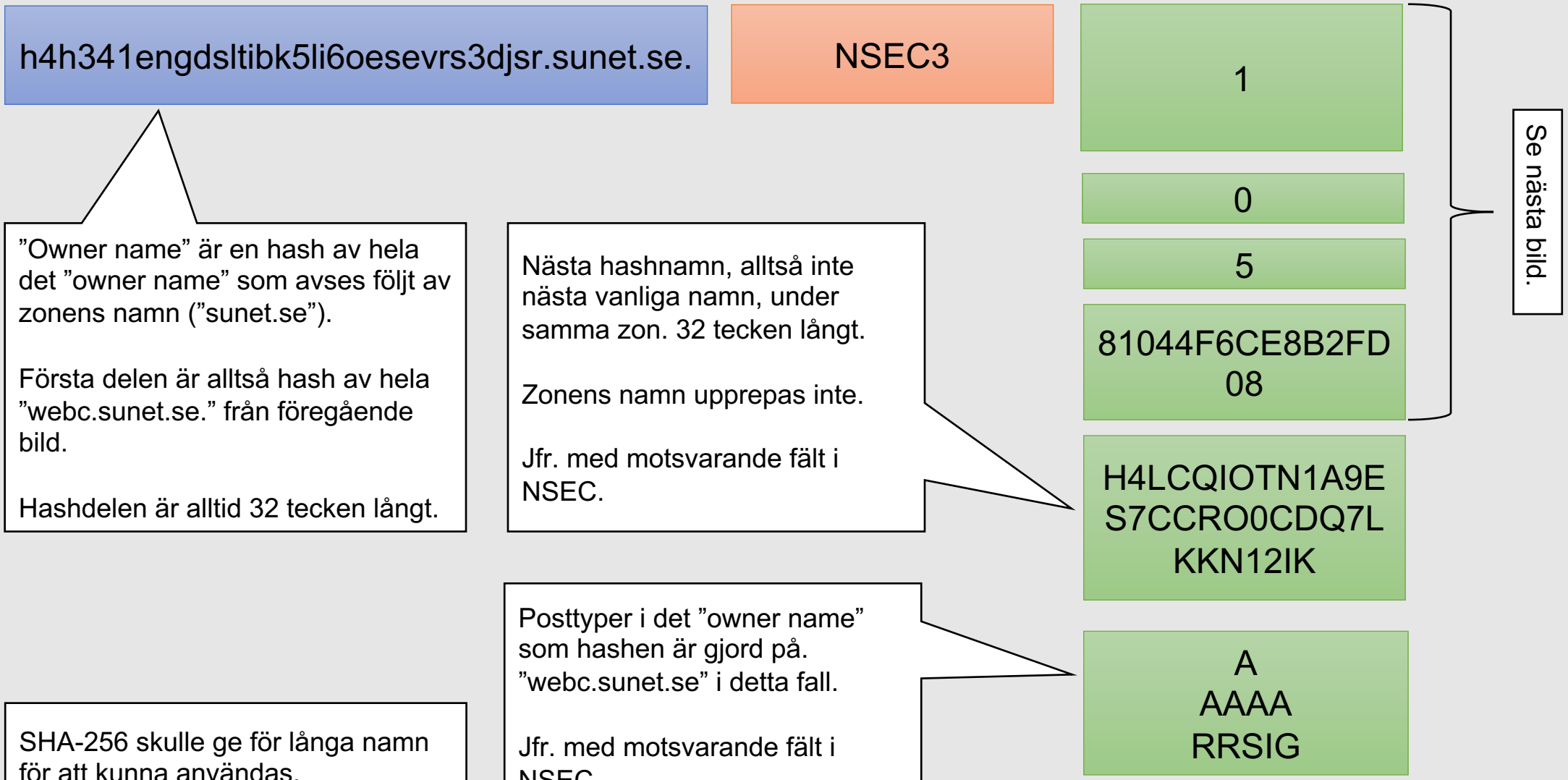
Alla DNSSEC-signerade zoner använder antingen NSEC eller NSEC3. Det finns inget tredje alternativ.

NSEC3

Den sökta posttypen finns inte för det namnet.

```
; <<>> DiG 9.10.6 <<>> webc.sunet.se txt +mult +dns +norec @sunic.sunet.se
(...)
;; QUESTION SECTION:
;webc.sunet.se.          IN TXT

;; AUTHORITY SECTION:
sunet.se.                                   300 IN SOA     (...)
sunet.se.                                   300 IN RRSIG   SOA 8 2 86400 (...)
h4h341engdsltibk5li6oesevrs3djsr.sunet.se.  300 IN NSEC3   1 0 5 (
                                        81044F6CE8B2FD08 H4LCQIOTN1A9ES7CCRO0CDQ7LKKN12IK
                                        A AAAA RRSIG )
h4h341engdsltibk5li6oesevrs3djsr.sunet.se.  300 IN RRSIG   NSEC3 8 3 300 (...)
(...)
```


h4h341engdsltibk5li6oesevrs3djsr.sunet.se.
NSEC3
1
0
5
81044F6CE8B2FD08
Se nästa bild.
”Owner name” är en hash av hela det ”owner name” som avses följt av zonens namn (”sunet.se”).
Första delen är alltså hash av hela ”webc.sunet.se.” från föregående bild.
Hashdelen är alltid 32 tecken långt.
Nästa hashnamn, alltså inte nästa vanliga namn, under samma zon. 32 tecken långt.
Zonens namn upprepas inte.
Jfr. med motsvarande fält i NSEC.
H4LCQIOTN1A9ES7CCRO0CDQ7LKKN12IK
Posttyper i det ”owner name” som hashen är gjord på. ”webc.sunet.se” i detta fall.
Jfr. med motsvarande fält i NSEC.
A
AAAA
RRSIG
SHA-256 skulle ge för långa namn för att kunna användas.

h4h341engdsltibk5li6oesevrs3djsr.sunet.se.

NSEC3

1

Hash-algoritm styr hur hash-namnet skapas. 1 ger SHA-1 som f.n. alltid gäller.

Hash-algoritm, f.n. alltid "1".

0

Flaggor, värde 0 eller 1, normalt 0.

5

Om iterations inte är 0 så görs det hash på hash. Ev. salt stoppas in för att minska risken för kollisioner mellan hashar.

”Iterations”, bör vara 0.

81044F6CE8B2FD08

”Salt” för hash, bör vara tom.

H4LCQIOTN1A9ES7CCRO0CDQ7LKKN12IK

Om flaggan är 1 (opt-out) så hoppas delegeringar utan DS över. Bör inte användas för vanliga zoner. Tänkt för zoner med många delegeringar som en TLD.

A
AAAA
RRSIG

NSEC3

NSEC3 fungerar i princip som NSEC.

- Den anger ett namnintervall där det inte finns någon data.
- I startpunkten finns data, vars posttyper är listade i NSEC3.
- I slutpunkten finns data, men vi vet inte vilken.

Skillnad:

- Vi vet inte vilken slutdomänen är, bara att den finns.
- Vid NXDOMAIN så vet vi heller inte vilken som är startdomänen.

Exempelzon före NSEC3

```
namn.xa.        SOA         (...)
namn.xa.        NS          ns1.namn.xa.
namn.xa.        NS          ns2.namn.xa.
namn.xa.        NSEC3PARAM 1 0 0 -
namn.xa.        DNSKEY      (...)
info.namn.xa.   TXT         "Go to www"
ns1.namn.xa.    A           62.171.158.134
ns2.namn.xa.    AAAA        2a05:d014:4ae:e900:e026:2d09:8d68:2d43
sth.namn.xa.    MX          1 mail.narnia.pp.se.
www.namn.xa.    CNAME       www.narnia.pp.se.
;
```

Zonen namn.xa med NSEC3.

- RDATA i SOA- och DNSKEY har förkortats till "(...)".
- RRSIG visas inte här, men förutsätts skapas för alla RRset, även för NSEC3.

Skapa NSEC3-poster

1. För varje ”owner name”, hela ”owner name”, skapa en hash av ”owner name”.
2. Skapa nya DNS-poster med hash som ”owner name” istället för riktiga ”owner name” men med samma posttyp.
   - Alla DNS-posterna med vanliga namn finns kvar.

Exempelzon på väg mot NSEC3

```
namn.xa.            SOA  (...)
namn.xa.            NS   ns1.namn.xa.
namn.xa.            NS   ns2.namn.xa.
namn.xa.            NSEC3PARAM 1 0 0 -
namn.xa.            DNSKEY    (...)
info.namn.xa.       TXT  "Go to www"
ns1.namn.xa.        A    62.171.158.134
ns2.namn.xa.        AAAA 2a05:d014:4ae:e900:e026:2d09:8d68:2d43
sth.namn.xa.        MX   1 mail.narnia.pp.se.
www.namn.xa.        CNAME     www.narnia.pp.se.
;
; Samma poster som ovan och i samma ordning, men med ”hash owner name”
P1BIM4VNAJIMDI9KDSHOOHOTVHKRG692.namn.xa.    SOA  (...)
P1BIM4VNAJIMDI9KDSHOOHOTVHKRG692.namn.xa.    NS   ns1.namn.xa.
P1BIM4VNAJIMDI9KDSHOOHOTVHKRG692.namn.xa.    NS   ns2.namn.xa.
P1BIM4VNAJIMDI9KDSHOOHOTVHKRG692.namn.xa.    NSEC3PARAM 1 0 0 -
P1BIM4VNAJIMDI9KDSHOOHOTVHKRG692.namn.xa.    DNSKEY    (...)
VOTLAFTBVU3TJ8TI94E5DGKQMFSMEP97.namn.xa.    TXT  "Go to www”
2D3AP5I38BGBEUG3ORH239I5AJ9LR8TF.namn.xa.    A    62.171.158.134
GQ4EIE7D83D7UN53KBEEGEAOK1S0K6HE.namn.xa.    AAAA 2a05:d014:4ae:e900:e026:2d09:8d68:2d43
6J89SBNONU5NIOONN7BJPLJIFSS7AM74.namn.xa.    MX   1 mail.narnia.pp.se.
9P4P242QOQTFIMDV4BE25S3UK6MKG94G.namn.xa.    CNAME     www.narnia.pp.se.
```

Zonen namn.xa med NSEC3.

- RDATA i SOA- och DNSKEY har förkortats till "(...)".
- RRSIG visas inte.

Skapa NSEC3-poster

3. Sortera de nya DNS-posterna efter "hash owner name"

Exempelzon på väg mot NSEC3

```
namn.xa.              SOA  (...)
namn.xa.              NS   ns1.namn.xa.
namn.xa.              NS   ns2.namn.xa.
namn.xa.              NSEC3PARAM 1 0 0 -
namn.xa.              DNSKEY    (...)
info.namn.xa.         TXT  "Go to www"
ns1.namn.xa.          A    62.171.158.134
ns2.namn.xa.          AAAA 2a05:d014:4ae:e900:e026:2d09:8d68:2d43
sth.namn.xa.          MX   1 mail.narnia.pp.se.
www.namn.xa.          CNAME     www.narnia.pp.se.
;
; Samma poster som ovan, men sorterade efter ”hash owner name”
2D3AP5I38BGBEUG3ORH239I5AJ9LR8TF.namn.xa.    A    62.171.158.134
6J89SBNONU5NIOONN7BJPLJIFSS7AM74.namn.xa.    MX   1 mail.narnia.pp.se.
9P4P242QOQTFIMDV4BE25S3UK6MKG94G.namn.xa.    CNAME     www.narnia.pp.se.
GQ4EIE7D83D7UN53KBEEGEAOK1S0K6HE.namn.xa.    AAAA 2a05:d014:4ae:e900:e026:2d09:8d68:2d43
P1BIM4VNAJIMDI9KDSHOOHOTVHKRG692.namn.xa.    SOA  (...)
P1BIM4VNAJIMDI9KDSHOOHOTVHKRG692.namn.xa.    NS   ns1.namn.xa.
P1BIM4VNAJIMDI9KDSHOOHOTVHKRG692.namn.xa.    NS   ns2.namn.xa.
P1BIM4VNAJIMDI9KDSHOOHOTVHKRG692.namn.xa.    NSEC3PARAM 1 0 0 -
P1BIM4VNAJIMDI9KDSHOOHOTVHKRG692.namn.xa.    DNSKEY    (...)
VOTLAFTBVU3TJ8TI94E5DGKQMFSMEP97.namn.xa.    TXT  "Go to www”
```

Zonen namn.xa med NSEC3.

- RDATA i SOA- och DNSKEY har förkortats till "(...)".
- Posterna med ”hash owner name” sorterade efter den.

Skapa NSEC3-poster

3. Skapa NSEC3-poster som har ”hash owner name” och som pekar på nästa ”hash owner name” (utan zonnamnet).
   - De extra DNS-posterna med ”hash owner name” behövs inte längre och tas bort, bara NSEC3 behålls.
4. Posttyperna som NSEC3 pekar ut är samma som de som fanns i ursprungliga ”owner name”.

Exempel med poster och NSEC3

```
namn.xa.            SOA  (...)
namn.xa.            NS   ns1.namn.xa.
namn.xa.            NS   ns2.namn.xa.
namn.xa.            NSEC3PARAM 1 0 0 -
namn.xa.            DNSKEY    (...)
info.namn.xa.       TXT  "Go to www"
ns1.namn.xa.        A    62.171.158.134
ns2.namn.xa.        AAAA 2a05:d014:4ae:e900:e026:2d09:8d68:2d43
sth.namn.xa.        MX   1 mail.narnia.pp.se.
www.namn.xa.        CNAME     www.narnia.pp.se.
;
; NSEC3-posterna kommer i sorteringsordning.
2D3AP5I38BGBEUG3ORH239I5AJ9LR8TF.namn.xa. 300 IN NSEC3 1 0 0 - ( ; hash av ns1.namn.xa.
                    6J89SBNONU5NIOONN7BJPLJIFSS7AM74 A RRSIG)
6J89SBNONU5NIOONN7BJPLJIFSS7AM74.namn.xa. 300 IN NSEC3 1 0 0 - ( ; hash av sth.namn.xa.
                    9P4P242QOQTFIMDV4BE25S3UK6MKG94G MX RRSIG)
9P4P242QOQTFIMDV4BE25S3UK6MKG94G.namn.xa. 300 IN NSEC3 1 0 0 - ( ; hash av www.namn.xa.
                    GQ4EIE7D83D7UN53KBEEGEAOK1S0K6HE CNAME RRSIG)
GQ4EIE7D83D7UN53KBEEGEAOK1S0K6HE.namn.xa. 300 IN NSEC3 1 0 0 - ( ; hash av ns2.namn.xa.
                    P1BIM4VNAJIMDI9KDSHOOHOTVHKRG692 AAAA RRSIG)
P1BIM4VNAJIMDI9KDSHOOHOTVHKRG692.namn.xa. 300 IN NSEC3 1 0 0 - ( ; hash av namn.xa.
                    VOTLAFTBVU3TJ8TI94E5DGKQMFSMEP97 NS SOA RRSIG DNSKEY NSEC3PARAM)
VOTLAFTBVU3TJ8TI94E5DGKQMFSMEP97.namn.xa. 300 IN NSEC3 1 0 0 - ( ; hash av info.namn.xa.
                    2D3AP5I38BGBEUG3ORH239I5AJ9LR8TF TXT RRSIG)
```

Zonen namn.xa med NSEC3.

- RDATA i SOA- och DNSKEY har förkortats till "(...)".
- RRSIG visas inte.
- Varje NSEC3-post motsvarar ett vanligt "owner name" i zonen.

```
; <<>> DiG 9.10.6 <<>> sunet.se hinfo +dns +mult
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2208
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1280
;; QUESTION SECTION:
;sunet.se.      IN HINFO

(...)
```

Fråga efter posttypen HINFO under sunet.se.

Ett NODATA-svar, fortsätter på nästa bild.

```
(...)

;; AUTHORITY SECTION:
sunet.se.       253 IN SOA hidden-master.sunet.se. hostmaster.sunet.se. (
                2020021000 ; serial
                28800      ; refresh (8 hours)
                7200       ; retry (2 hours)
                604800     ; expire (1 week)
                300        ; minimum (5 minutes)
                )
sunet.se.       253 IN RRSIG SOA 8 2 86400 (
                20200220025413 20200210015413 7636 sunet.se.
                C4hbPuPXioKWL1gyU8Xuym/3qAwiMLm4EzqxPOQ0R02P
                1uMe4Fg+EOWMCNn0KILeq9w2EbAlk3sSVP4ebwxar5GG
                CFHkzpKB1Rde0d6T4eqyA5CED0Stsw/yQTt/jzOJt3e9
                Hy/BilbOW4ntHh5SHdzX719GCdHSxuxD6CD7n1E= )
(...)
```

Ett NODATA-svar, från föregående bild och fortsätter på nästa bild.

Hash av ”owner name”, i detta fall ”sunet.se”

Ett NODATA-svar, från föregående bild.

```
(...)
msghfvfp16iq1g3e2nfqo4og6bkgadlu.sunet.se. 253 IN NSEC3 1 0 5 81044F6CE8B2FD08 (
                MSJ08GIJCUISVT1LCLK1RBIS81D9LPQ7
                A NS SOA MX TXT AAAA RRSIG DNSKEY NSEC3PARAM SPF )
msghfvfp16iq1g3e2nfqo4og6bkgadlu.sunet.se. 253 IN RRSIG NSEC3 8 3 300
                20200220025413 20200210015413 7636 sunet.se.
                E6PkTbwxPqODDBaPB9Sf45Ma2mDHAq95OJNSUsbtEimp
                GaYWqMB487vsXr671sLjPW0vqcAUSjEYZ181uDjLlLVo
                cOjrg4INw1XNWYjOy7D8Hic12P0u8aAaRu3JGMgJJi8o
                MkReNG9qLACWwn2t+UoT10fZzUWDBVEgx1dDf34= )
```

Posttyperna som finns i ”hash owner name” vilken är lika med ”sunet.se”. Det finns ingen HINFO där.

NSEC3 listas aldrig här (har annat "owner name"). Jfr med NSEC där posttypen NSEC listas i NSEC.

NSEC3

På servern:

1. Frågan ska besvaras med NODATA eller NXDOMAIN.
2. Servern skapar en hash av det efterfrågade namnet.
3. NXDOMAIN:
   - Servern returnerar en NSEC3-post vars ”hash owner name” är det som kommer precis före den skapade hashen när det gäller ”hash owner name”.
4. NODATA:
   - Servern returnerar en NSEC3-post vars ”hash owner name” är samma som den skapade hashen.

NSEC3

Vid validering:

1. Gör en hash av det aktuella namn enligt samma algoritm som servern har använt.
2. Säkerställ att den skapade hashen ligger inom NSEC3-postens start- och sluthash.

NSEC3

Det går inte att fråga om hash-namnen, vilket förhindrar alla typer av ”zone walking”.

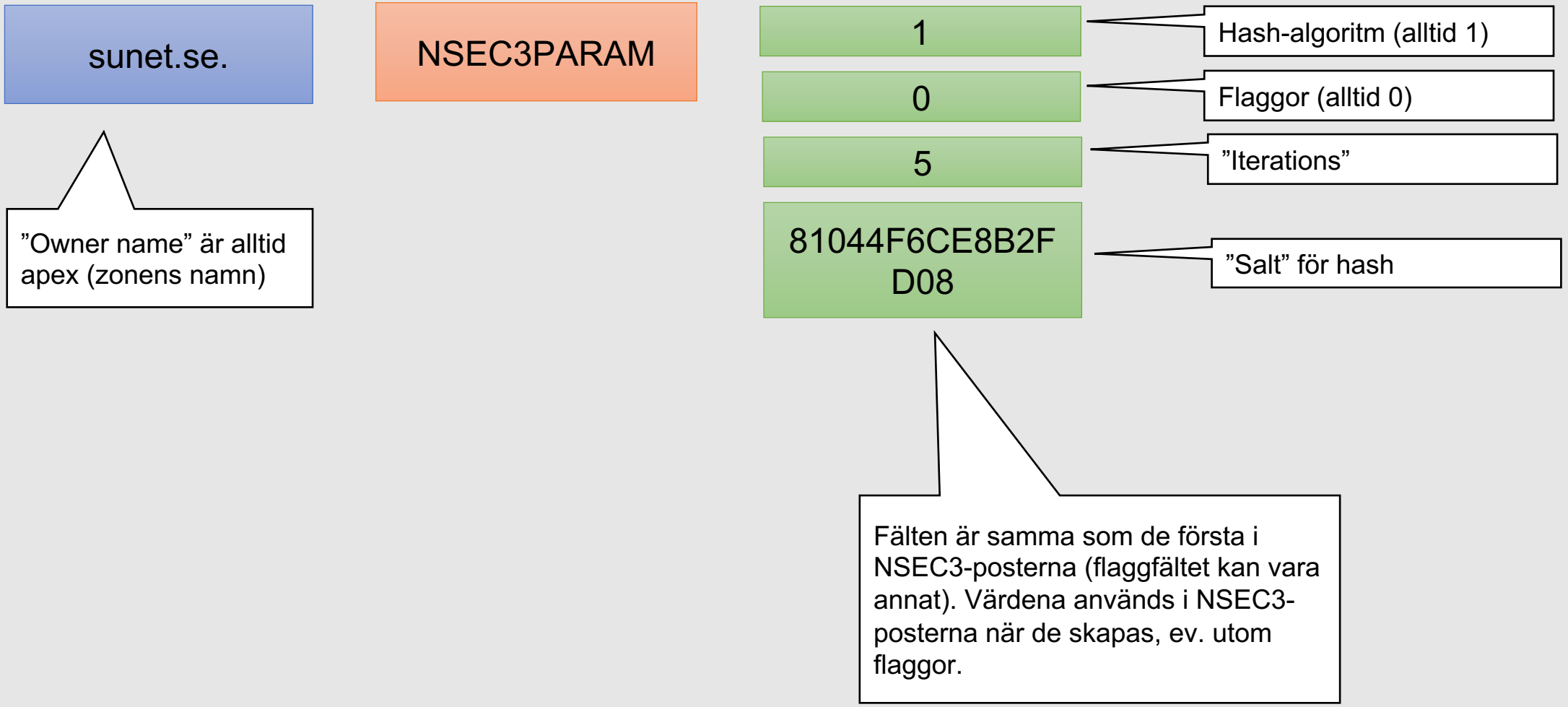
```
; <<>> DiG 9.10.6 <<>> msghfvfp16iq1g3e2nfqo4og6bkgadlu.sunet.se. nsec3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 52598
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;msghfvfp16iq1g3e2nfqo4og6bkgadlu.sunet.se. IN NSEC3
```

Posttyp NSEC3PARAM

```
; <<>> DiG 9.10.6 <<>> sunet.se nsec3param +mult +dns +norec @sunic.sunet.se
(...)
;; ANSWER SECTION:
sunet.se.       0 IN NSEC3PARAM    1 0 5 81044F6CE8B2FD08
sunet.se.       0 IN RRSIG NSEC3PARAM 8 2 0 (
                20190220100902 20190210090902 7636 sunet.se.
                fVxbWlNRR/oi5u2Hpe1LNavXbFZTccoCT7zzRBVo7Cgw
                mcofeTGVJpjA5UzLSTdX+wQUeHDk6p15Uh9R8izgiW4U
                KTKD1tk83P+47AMtSuh+HT6Uz/IAsGLHL5D3/+yoR/SQ
                qbXmQDVTG5y+37QKvMTuUdNZ/hX/MHIEJNODfUA= )

(...)
```


sunet.se.
NSEC3PARAM
1
Hash-algoritm (alltid 1)
0
Flaggor (alltid 0)
5
”Iterations”
81044F6CE8B2F D08
”Salt” för hash
”Owner name” är alltid apex (zonens namn)
Fälten är samma som de första i NSEC3-posterna (flaggfältet kan vara annat). Värdena används i NSEC3-posterna när de skapas, ev. utom flaggor.

NSEC3PARAM

- Används inte vid validering.
- Används vid generering av NSEC3-poster av namnservern.
- Används av auktoritativ server (master och slav) för att avgöra om NSEC3 ska användas eller inte, och vilken NSEC3 post (om det finns flera NSEC3-kedjor).

NSEC3PARAM

- Om NSEC3PARAM finns (i apex) så måste zonen använda NSEC3 istället för NSEC. Ev. NSEC-poster ska ignoreras.
- NSEC3PARAM är alltså obligatoriskt ifall NSEC3 används.
- Om NSEC3PARAM inte finns så ska hostingnamnservern ignorera ev. NSEC3-poster.

NSEC- och NSEC3-poster kan finnas samtidigt, och NSEC3PARAM används för att avgöra vilket som ska användas t.ex. vid byte mellan NSEC och NSEC3.

▶NSEC3 och empty non-terminals

[Till Innehåll]

NSEC3-post för varje namn i zonen

NSEC-poster skapas bara för namn i zonen **med data**.

NSEC3-poster skapas för alla namn i zonen*, även ”empty non-terminals”.

För zoner med namn med många ”labels”, och tomma sådana, så skapas fler NSEC3- än NSEC-poster för samma grundzon.

* Utom för deleringspunkter utan DS om flaggan är satt.

Schematisk exempelzon

```
$ORIGIN namn.se.
namn.se.            SOA     (...)
namn.se.            NS      (...)
www.sth.namn.se.    CNAME   (...)
```

Följande namn finns i zonen:

- namn.se. (SOA, NS)
- sth.namn.se. (”empty non-terminal”)
- www.sth.namn.se. (CNAME)

NSEC kontra NSEC3 om zonen signeras

NSEC:

```
namn.se.           NSEC  www.sth.namn.se. NS SOA DNSKEY NSEC RRSIG
www.sth.namn.se.   NSEC  namn.se.         CNAME NSEC RRSIG
```

NSEC hoppar över sth.namn.se eftersom den är tom. Den går till nästa namn med data.

NSEC3:

```
hash(namn.se)           NSEC3 (...) NS SOA DNSKEY RRSIG
hash(sth.namn.se)       NSEC3 (...)
hash(www.sth.namn.se)   NSEC3 (...) CNAME RRSIG
```

Inga posttyper listas här eftersom namnet sth.namn.se är tom.

NSEC listas alltid som posttyp i NSEC-posten.

NSEC3 listas aldrig som posttyp i NSEC3-posten.

▶NSEC3 och opt-out-flaggan

[Till Innehåll]

Opt-out-flaggan satt

Om opt-out-flaggan är satt så skapas inga NSEC3-poster för delegeringar där DS-posten saknas.

Schematisk exempelzon

```
$ORIGIN namn.se.
namn.se.            SOA     (...)
namn.se.            NS      ns1.namn.se.
alfa.namn.se.       NS      ns1.example.com.
beta.namn.se.       NS      ns1.example.com.
beta.namn.se.       DS      (...)
gamma.namn.se.      NS      ns1.example.com.
ns1.namn.se.        A       192.0.2.100
```

Tre delegeringar, endast beta.namn.se har DS-post.

NSEC3 med och utan opt-out-flaggan

NSEC3 utan opt-out:

```
hash(namn.se)        NSEC3  1 0 (...) NS SOA DNSKEY RRSIG
hash(alfa.namn.se)   NSEC3  1 0 (...) NS
hash(beta.namn.se)   NSEC3  1 0 (...) NS DS RRSIG
hash(gamma.namn.se)  NSEC3  1 0 (...) NS
hash(ns1.namn.se)    NSEC3  1 0 (...) A RRSIG
```

Även för osignerade delegeringar finns NSEC3-post. NS i delegeringen har ingen RRSIG.

NSEC3 med opt-out:

```
hash(namn.se)        NSEC3  1 1 (...) NS SOA DNSKEY RRSIG
hash(beta.namn.se)   NSEC3  1 1 (...) NS DS RRSIG
hash(ns1.namn.se)    NSEC3  1 1 (...) A RRSIG
```

Osignerade delegeringen har ingen NSEC3-post.

Ingen DNSSEC-säkring av osignerade delegeringar om opt-out-flaggan är satt.

▶NSEC eller NSEC3?

[Till Innehåll]

NSEC eller NSEC3?

- NSEC är enklare att generera, validera och felsöka.
- NSEC3 ger en något större zon, NSEC3-poster är normalt något större än NSEC-poster.
  - Om zonen har ”empty non-terminals” så blir det NSEC3-poster men inga NSEC-poster för dem.
  - Om flaggan är satt så kan NSEC3 i vissa fall ge mindre zon.
- Problemet med potentiell ”zone walking” ansågs så stort att NSEC3 var nödvändigt för att få DNSSEC att spridas.
- Om zonen behöver skyddas från fri zonöverföring så bör man välja NSEC3 även om skyddet inte är 100%.

NSEC eller NSEC3

Om NSEC3 väljs så kan flaggan sättas som tillåter att delegeringar utan DS hoppas över.

- Fördel för stora zoner med stor andel delegeringar (TLD:er) som har stor andel delegeringar utan DS (osignerade dotterzoner).
- Mindre lämpligt för vanliga zoner.
- Ger sämre kontroll över icke-existerande namn.

Är NSEC3 säker?

Det finns de som har visat att det går att ”knäcka” NSEC3, i alla fall i vissa fall. Det har gjorts arbete på att göra ett bättre alternativ, men inget som är på väg.

▶CD-flagga

[Till Innehåll]

Flaggor och DNSSEC

Bland de vanlig flaggorna i ”headern” (inte i OPT/EDNS) så finns CD-flaggan.

- I ”query” betyder den ”gör ingen validering utan skicka bara svaret”.
- Resolvern ska skicka med den vid ev. frågor till andra servrar.

Syftet är att den som skickar ”query” ska kunna validera själv men ändå använda en resolver. Kan också användas vid felsökning.

Ingen CD-flagga

```
; <<>> DiG 9.11.5-P1_2 <<>> rhybar.cz soa +mult +qr
;; global options: +cmd
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4376
;; flags: rd ad; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
(...)
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 4376
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; COOKIE: 15d458ddde111d16ea0fb2745c61f9cc8c4b5423c75eda5b (good)
;; QUESTION SECTION:
;rhybar.cz.    IN SOA
```

Med CD-flagga

```
; <<>> DiG 9.11.5-P1_2 <<>> rhybar.cz soa +cd +mult +qr
;; global options: +cmd
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52232
;; flags: rd ad cd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
(...)
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52232
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; COOKIE: e38d66c50f4ef7f4988aaff55c61f970d56ae4fb543905ed (good)
;; QUESTION SECTION:
;rhybar.cz.      IN SOA

;; ANSWER SECTION:
rhybar.cz.      591 IN SOA a.ns.nic.cz. hostmaster.nic.cz. (
                2199091611 ; serial
                10800      ; refresh (3 hours)
                3600       ; retry (1 hour)
                1209600    ; expire (2 weeks)
                7200       ; minimum (2 hours)
                )
```

▶Sammanfattning DNSSEC

[Till Innehåll]

Nya posttyper för DNSSEC

Följande posttyper har lagts till för hanteringen av DNSSEC:

- DNSKEY
- RRSIG
- NSEC
- DS
- CDS
- CDNSKEY
- NSEC3
- NSEC3PARAM

Nya flaggor för DNSSEC

Följande flaggor har lagts till för DNSSEC:

- DO (under EDNS)
- AD (i header)
- CD (i header)

Ändrad delegeringsmekanism med DNSSEC

Utan DNSSEC så innehåller delegeringspunkten (delegeringsnoden) inga auktoritativa DNS-poster i moderzonen.

Med DNSSEC så gör den det, DS, RRSIG och ev. NSEC.

Nya mekanismer för DNSSEC

DNSSEC har tillfört många mekanismer och har förändrat DNS.

För att kunna hantera DNS med DNSSEC så måste man känna till dessa.

▶Rot-zonen och rot-namnservrar

[Till Innehåll]

Hur många rotnamnservrar?

```
; <<>> DiG 9.10.6 <<>> @j.root-servers.net . ns +noedns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9045
;; flags: qr aa rd; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13
;; WARNING: recursion requested but not available

;; 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.

;; ADDITIONAL SECTION:
e.root-servers.net. 518400 IN A 192.203.230.10
e.root-servers.net. 518400 IN AAAA 2001:500:a8::e
h.root-servers.net. 518400 IN A 198.97.190.53
h.root-servers.net. 518400 IN AAAA 2001:500:1::53
l.root-servers.net. 518400 IN A 199.7.83.42
l.root-servers.net. 518400 IN AAAA 2001:500:9f::42
i.root-servers.net. 518400 IN A 192.36.148.17
i.root-servers.net. 518400 IN AAAA 2001:7fe::53
a.root-servers.net. 518400 IN A 198.41.0.4
a.root-servers.net. 518400 IN AAAA 2001:503:ba3e::2:30
d.root-servers.net. 518400 IN A 199.7.91.13
d.root-servers.net. 518400 IN AAAA 2001:500:2d::d
c.root-servers.net. 518400 IN A 192.33.4.12

;; Query time: 52 msec
;; SERVER: 192.58.128.30#53(192.58.128.30)
;; WHEN: Mon Jan 21 22:29:36 CET 2019
;; MSG SIZE  rcvd: 508
```

Hur många rotnamnservrar?

13 NS-poster och 13 adressposter (A/AAAA) får plats i 512 byte om domännamnen väljs så att det går att komprimera.

- Läs om ”compression” i RFC 1035, stycke 4.1.4, s 30-32.
- Antalet NS-poster för rotzonen är satt till 13.

Hur många rotnamnservrar?

- Varje NS-post motsvarar ett domännamn (hostnamn).
- Varje hostnamn har två adressposter:
  - IPv4
  - IPv6
- Totalt 26 IP-adresser.
  - Hur många servrar kan det blir med 26 IP-adresser?
  - På hur många platser kan en IP-adress vara samtidigt?
- Det beror på hur man gör det – anycast.

Anycast

- Unicast – det finns ***en*** målserver (viss IP-adress) som klienten kan kontakta.
- Anycast – det finns ***flera*** likvärdiga målservrar (med samma IP-adress) där routing styr vilken som klienten kommer att kontakta.

Mer nedan.

Hur många rotnamnservrar?

” As of 2023-10-08T11:11:07Z, the root server system consists of **1754** instances operated by the 12 independent root server operators.”

http://www.root-servers.org/

▶Anycast

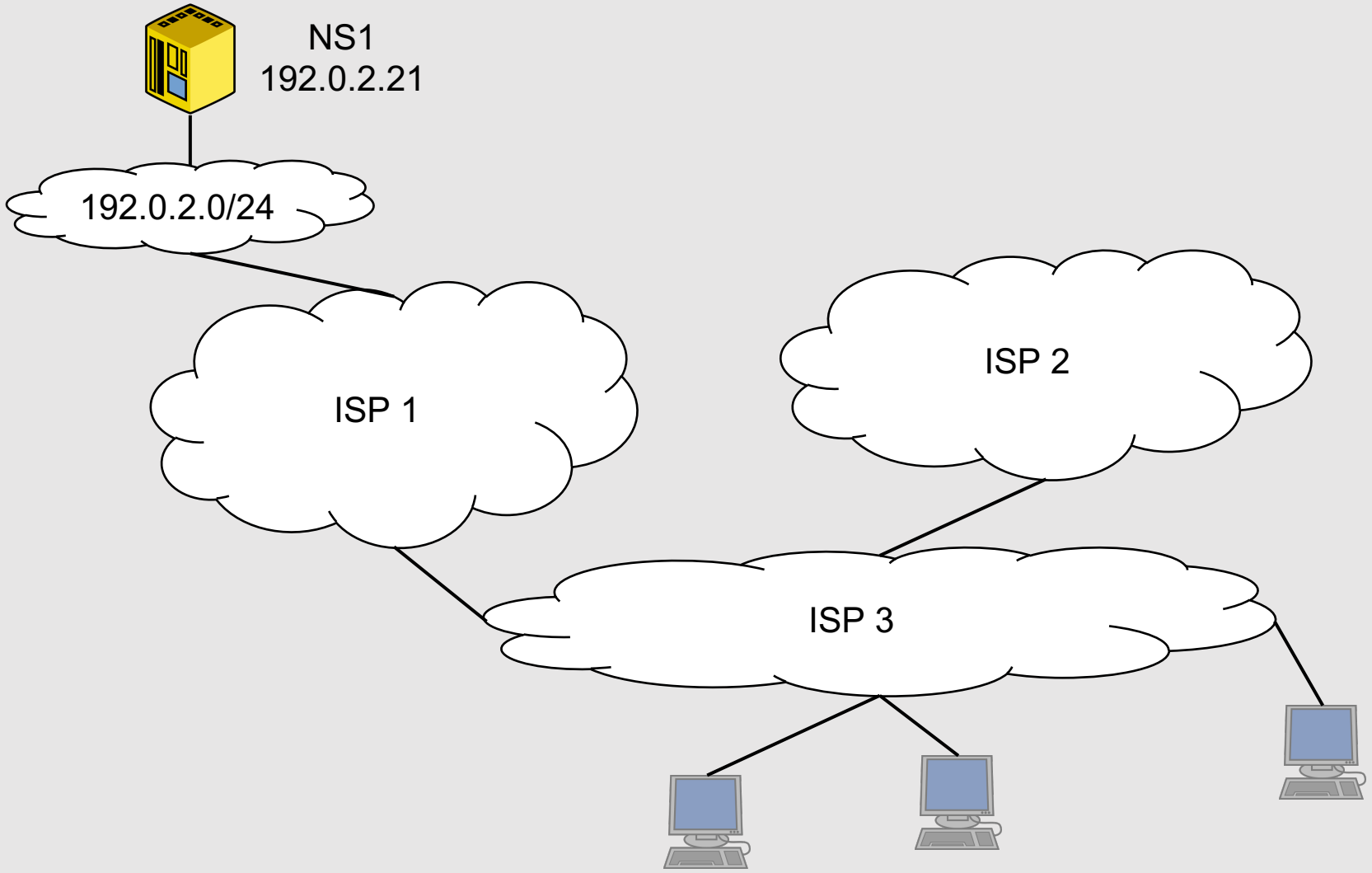
[Innehåll]

Anycast

Anycast är vanligt sätt bland stora zoner och ge bra tillgänglighet.

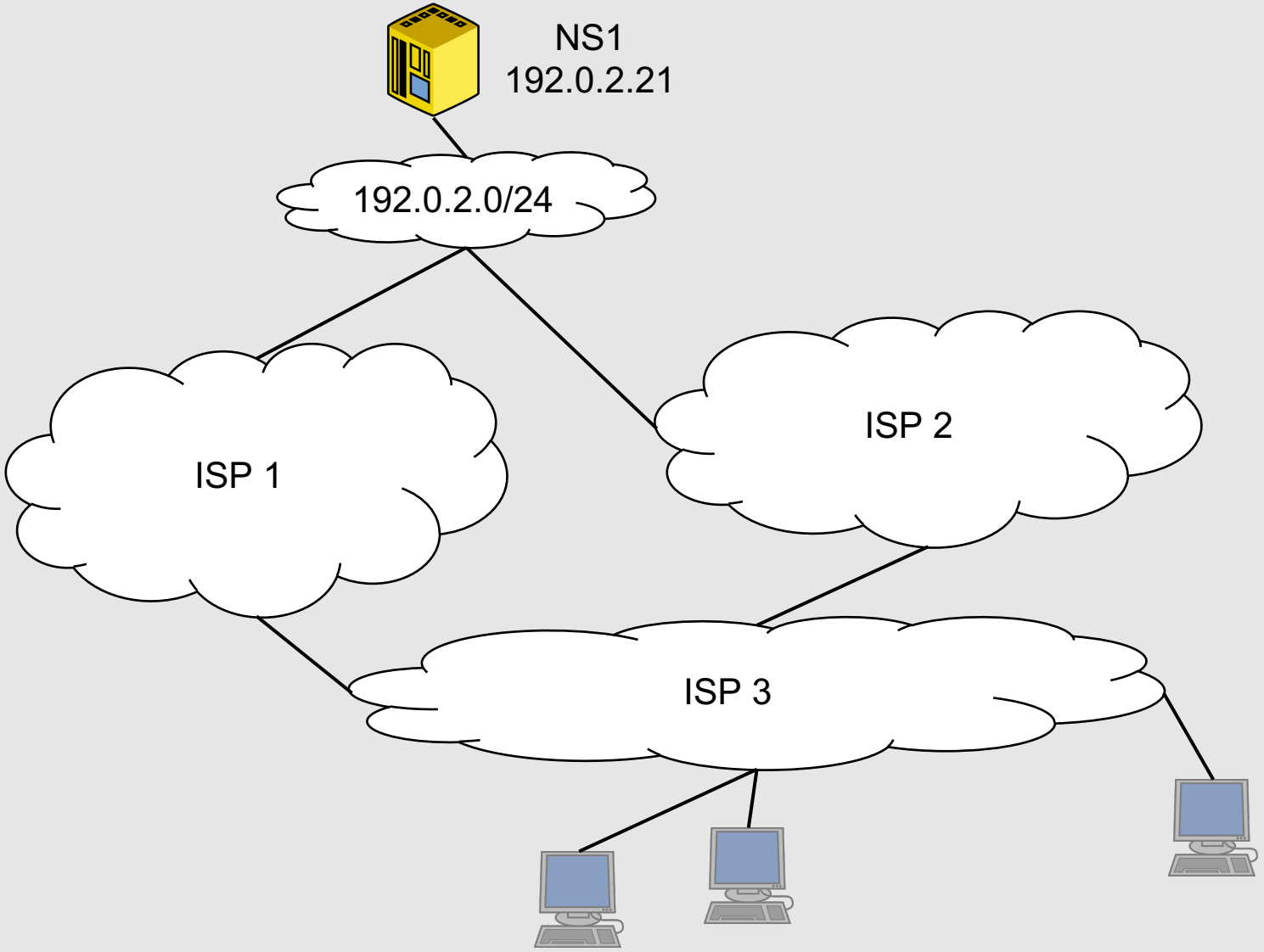
- Rotzonen är ett extremt exempel på användningen av anycast.
- Används också av många andra zoner, t.ex. .se.

Anslutning till en operatör



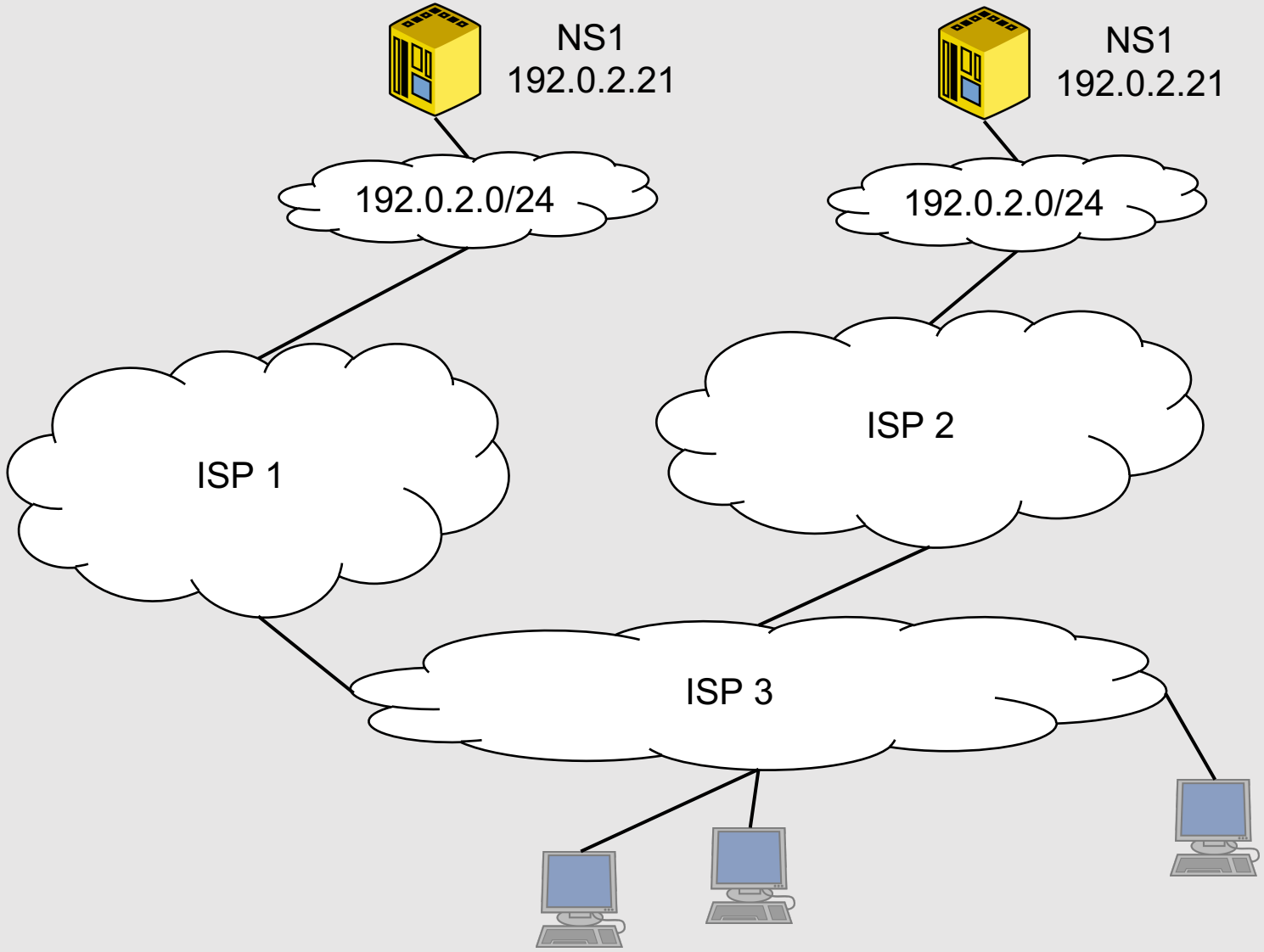
1 routingväg till servern. Det räcker med ett avbrott för att förbindelsen ska brytas.

Multihomed



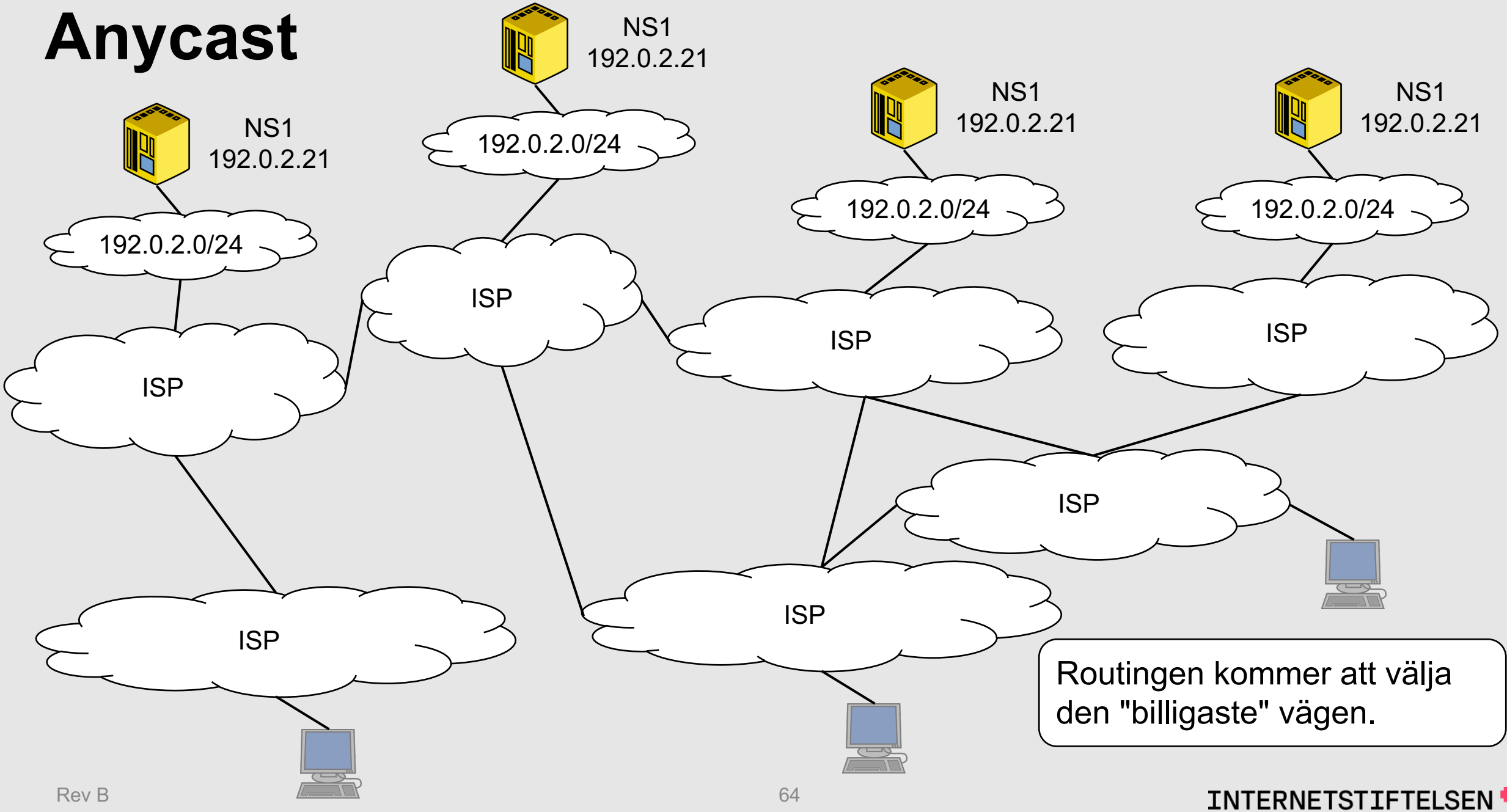
2 routingvägar till servern. Om ena vägen går ner så finns den andra kvar.

Anycast



Samma tjänst på samma IP-adress på två ställen via olika routingvägar.

Anycast



Routingen kommer att välja den "billigaste" vägen.

Unicast och anycast

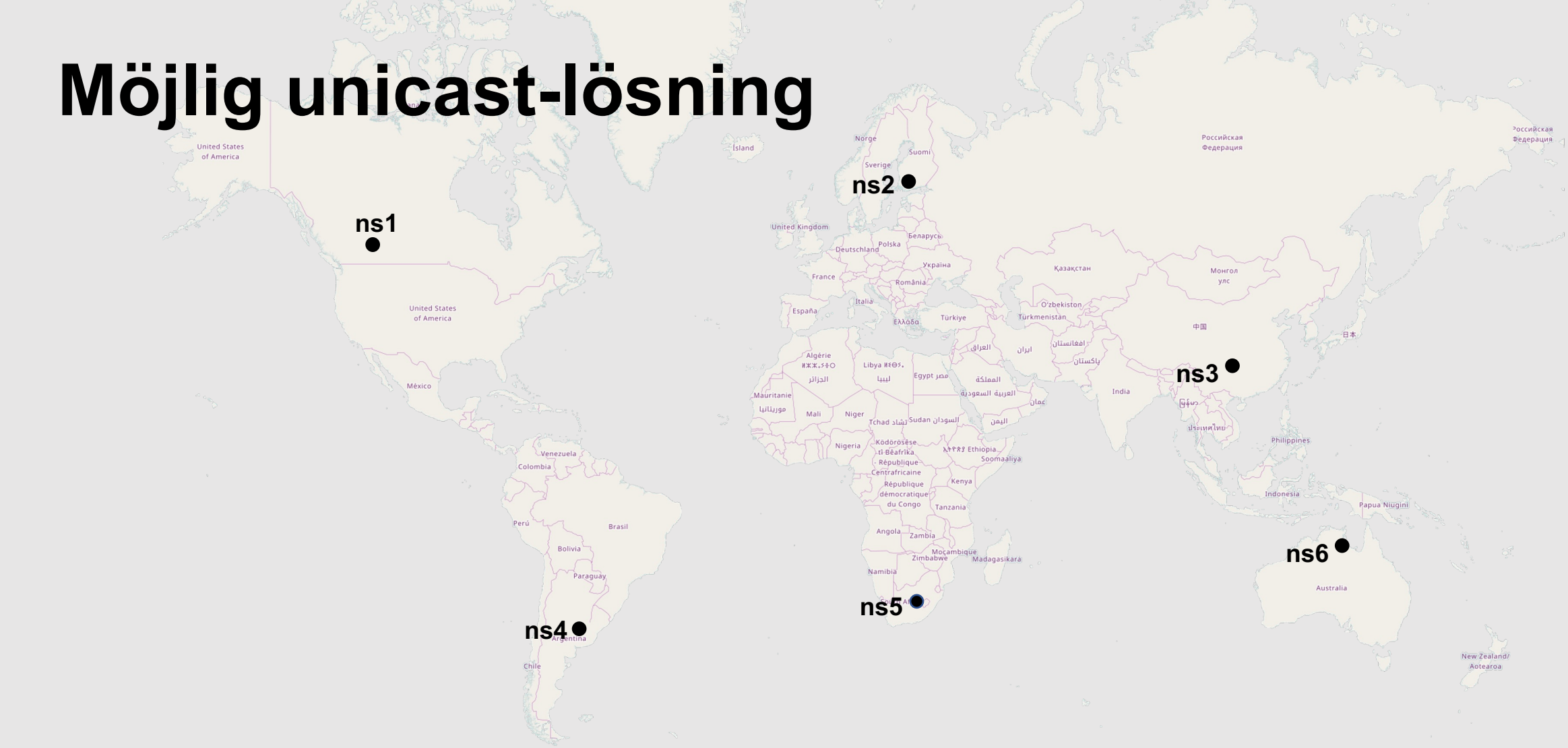
- Unicast är den vanliga lösningen där servern (IP-adressen) finns på ett ställe.
  - Det kan vara så att det finns flera routingvägar dit.
  - Det kan vara så att det är en lokal lastbalanserare och två eller flera servrar på samma plats.
- Anycast är lösningen där flera servrar finns på olika platser med olika routingvägar, men alla delar samma IP-adress.
  - Det kan vara så att det finns flera routingvägar till varje serverinstans.
  - Det kan vara så att varje serverinstans är en lokal lastbalanserare med flera fysiska servrar.

NS kan vara unicast

Om alla NS är unicast, men utspridda i nätet så blir det bara någon NS som är nätmässigt nära klienten.

Om närmsta NS går ner, så får klienten välja annan efter timeout, och sedan fortsätta mot den andra.

Möjlig unicast-lösning



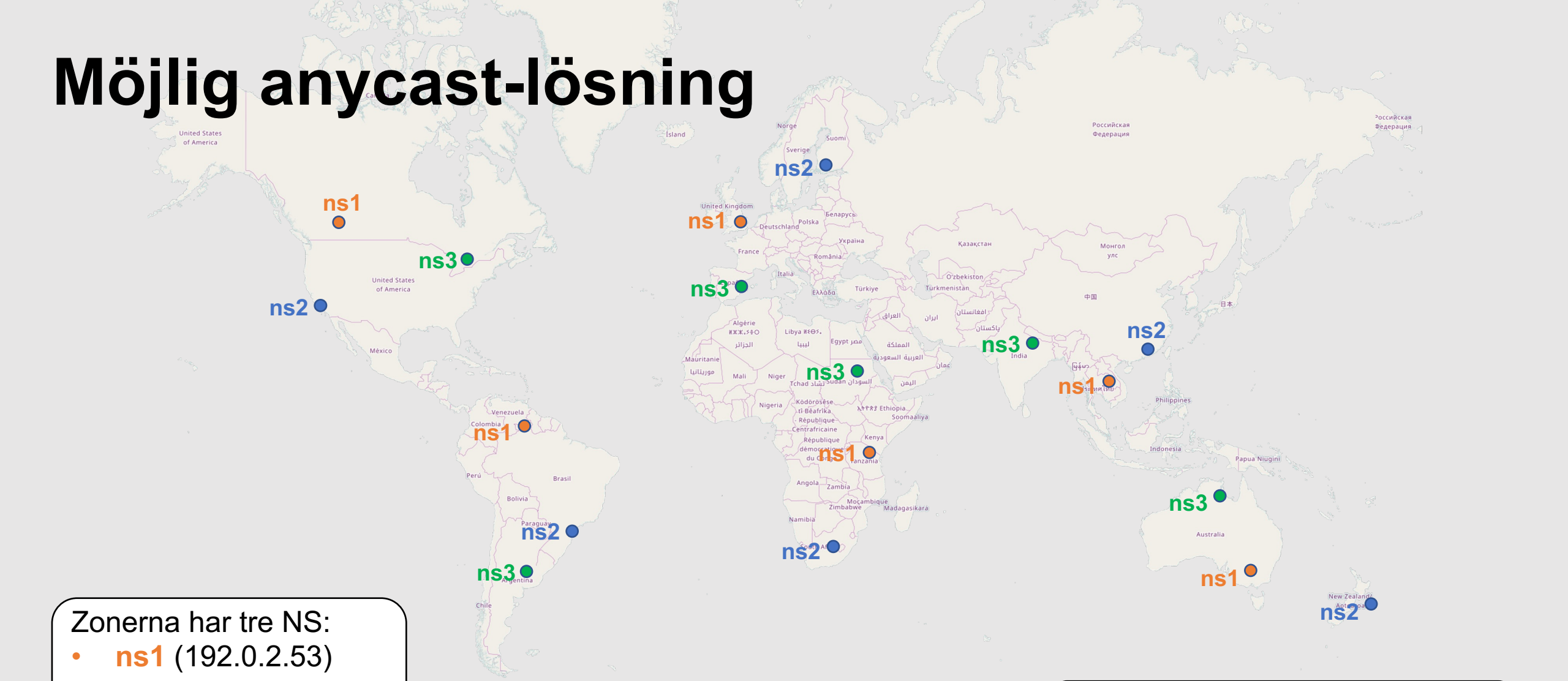
Zonerna har sex NS spridda över världen.

NS kan vara anycast

Om alla NS är anycast, och varje NS är utspridd i nätet så kommer det finns flera NS som är nätmässigt nära klienten, ev. alla.

Om närmsta instans i anycast-klustret går ner så kommer routingen att leda frågan till näst närmsta instans. Klienten kan fortsätta där eller välja annan NS.

Möjlig anycast-lösning



Zonerna har tre NS:

- **ns1** (192.0.2.53)
- **ns2** (198.51.100.53)
- **ns3** (203.0.113.53)

Var klienten än finns så routas den till nätmässigt närmasta ns1, ns2 och ns3.

Anycast

Anycast har vuxit fram som ett rubust sätt att skapa redundans och tillgänglighet för DNS. Anycast bygger på att samma IP-adress finns tillgänglig på många platser samtidigt.

Routingen väljer den närmsta instansen beroende på var klienten finns.

Anycast fungerar väl för protokoll som har korta sessioner, vilket stämmer för DNS.

Synkronisering av anycast

Om alla ns1 har samma IP-adress, hur kan de då hämta zonfilen?

- Varje namnserverinstans har två IP-adresser, dels anycast-adressen, dels en vanlig unicast-adress.
- Masterservern är normalt en dold server, eller kanske flera.
- Masterservern skickar *NOTIFY* till slavens unicast-adress och namnservrarna använder unicast-adressen för *AXFR* och alla annan kommunikation utom att svara på frågor som kommer till anycast-adressen.

Anycast-operatörer

Det finns idag flera stora operatörer som erbjuder anycast-tjänst över stora anycast-nät.

Lösningen kommer i framtiden att bli ännu mer använd för hantering av DNS.

▶Toppdomäner (TLD)

[Till Innehåll]

Rot, toppdomäner och domäner

- Under rot så har vi toppdomäner, TLD (”top-level domain”), t.ex. COM, SE och NU.
- De flesta toppdomänerna erbjuder registrering av domän på nästa nivå för företag och privatpersoner.

ICANN och toppdomänerna

ICANN, Internet Corporation of Assigned Names and Numbers

- Grundades 1999 för att koordinera bl.a. rotzonen.
- Ansvarar för att rotzonen delegerar ut toppdomänerna.
- Har avtal med toppdomänsinnehavarna. Olika avtal med olika kategorier av toppdomäner.

Historik

De ursprungliga TLD:erna var kopplade till USA.

- .com, .org, .net, .gov, .mil m.fl.

Efter det kom landstoppdomäner, t.ex. .se, .nu och .fr.

Runt år 2000 skapades några nya, sponsrade toppdomäner, bl.a. MUSEUM och COOP.

Historik

Den stora ökningen av antalet TLD:er kom efter 2012 när ICANN öppnade för ansökningar om nya TLD:er. Det kom in ca 1900 ansökningar om ca 1400 olika TLD:er.

Från 2013 till 2022 så har drygt 1200 nya generiska TLD:er lagts till.

Exempel på de nya TLD:erna:

- .stockholm
- .blue
- .global
- .adult
- .beer
- .google

▶Katergorier av toppdomäner

[Till Innehåll]

Kategorier av toppdomäner

Toppdomänerna kan delas in i flera kategorier:

- generic, 1200-1300 st
- country-code, ca 300 st
- sponsored, knappt 20 st
- infrastructure, 1 st

Källa där man kan hitta mera information om alla toppdomäner:
https://www.iana.org/domains/root/db

Kategorier och DNS

Ur DNS synpunkt är alla toppdomäner lika. Det finns alltså inget inbyggt i DNS att behandla kategorierna olika. DNS behandlar heller inte toppdomäner speciellt. Kategorin ”toppdomän” finns inte i själva DNS.

Vad skiljer kategorierna åt?

- Syfte
- Innehavare (” Sponsoring Organisation”)
- Avtal med ICANN

Generic, gTLD

De generiska toppdomänerna inkluderar olika typer av toppdomäner:

- Allmänna, t.ex. .com, .xyz
- Geografiska, t.ex. .paris, .stockholm, .cat
- Företagsspecifika, t.ex. .abb, .yahoo

Innehavaren styr över registreringen av domäner under sin TLD. Vissa är restriktiva. Vissa kan vara helt för intern användning, t.ex. .stockholm.

TLD:erna styrs enligt avtal med ICANN, vilket ger finansiering av ICANN.

Country-code, ccTLD

Klassiska ccTLD är TLD:er (landstoppdomäner) för ett specifikt land eller område enligt ISO 3166-1 alpha-2, en lista som upprättas av ISO (International Organization for Standardization).

- Listan består av tvåbokstavsförkortningar (a-z) för alla länder plus vissa geografiska områden.
- Alla dessa kan delas ut som TLD:er, och har så gjorts i de flesta fall.
- Alla toppdomäner på två bokstäver är en ccTLD.

ccTLD

Innehavaren av en ccTLD ska ha en anknytning till landet eller området ifråga, men det behöver inte vara någon myndighet som är innehavaren.

Internetstiftelsen är innehavaren av .se, men Internetstiftelsen är privat (allmännyttig) stiftelse.

Innehavaren av .dk är Dansk Internet Forum, en medlemsorganisation.

ccTLD

En ccTLD behöver inte vara ett land.

- AX är ccTLD för Åland.
- BV är ccTLD för Bouvetön under Norge (men används inte).
- EU är ccTLD för Europeiska unionen

Sponsored

Internationella organisationer: .aero .coop .museum .post .tel .int

Georgrafiska, men inte ccTLD: .asia .cat

Företag: .jobs .travel .xxx

Amerikanska intressen: .edu .gov .mil

Infrastructure (arpa)

Det finns en enda TLD som är "infrastructure", arpa. Det finns inga ”vanliga” domäner under arpa.

Den mest kända användningen är för baklängesuppslagning av IP-adresser, under ”in-addr.arpa” resp. "ip6.arpa" (mer om baklängesuppslagning i kommande föreläsning).

Ytterligare användning och mera information finns under https://www.iana.org/domains/arpa

▶Registry, registrar och registrant

[Till Innehåll]

Registry-registrar-modellen

De flesta TLD:er använder samma modell för registrering av domäner.

Man har tre nivåer:

- Registry – den som driver TLD:n och som publicerar TLD:ns zonfil.
- Registrar – ombud som sköter registreringen och har kundkontakt
- Registrant – den som har registrerat namnet (innehavare)

Exempel SE

Internetstiftelsen är **Registry** för TLD:n .se.

Loopia är en av många **Registrarer** som man kan registrera en .se-domän via. Loopia fakturerar sedan avgiften varje år.

Rigistrant är alla som har en domän, t.ex. KTH, Telia eller en privatperson.

Registrar

Registraren ”äger” registranten som kund. Registranten har bara kontakt med registraren, inte med registry. Registraren sköter debitering av avgiften och ändringar av domänen, t.ex. kontaktinformation och DNS-data.

Det är registraren som sedan uppdaterar databasen hos registry t.ex. med ny DNS-information.

Byte av registrar – transfer

Registranten är normalt inte bunden av registraren, utan kan byta utan att registraren kan stoppa bytet eller flytten.

Enligt reglerna för t.ex. .se så måste en sådan flytt vara konstnadsfri, men under vissa TLD:er så debiteras en avgift.

▶Om presentationen

[Till Innehåll]

Internets domännamnssystem

Denna presentation är framtagen 2019–2024 av Mats Dufberg (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

Dokumenthistorik

- Rev A: Ursprunglig version VT 2024
- Rev B: Förtydligar NSEC3PARAM, bilder 28-31.

Slut.