Internets domännamnssystem (HI1037)

12 mars 2021

Hjälpmedel:	Inga.
Observera:	Lösningarna måste vara skrivna med läsbar skrift. Ange namn och personnummer på varje sida. Maximalt 58 poäng kan uppnås. Preliminära betygsgränser: A-E från 29 till 58 poäng med intervaller om ungefär 6 poäng. F (underkänt) under 29 poäng. Del 1 är frågor 1—13 (max 29 poäng). Del 2 är frågor 14—25 (max 29 poäng).

Del 1

1. (1) Vad är ditt telefonnummer och mailadress? (0 p)

2. (2) Vad är ett RRset? (1 p)

   En eller flera DNS-poster med samma owner name och posttyp.

3. (3) Vad är zonöverföring? (1 p)

   Zonöverföring är kopiering av zonfilen från masterserver till slavserver med DNS-protokollet.

4. (4) Vilken TCP/UDP-port måste en namnserver lyssna/svara på? (1 p)

   Port 53.

5. (5) En DNS-klient skickar en förfrågan till en namnserver men hela svaret inte får plats i svarspaketet. Vad gör servern? (1 p)

   Servern skickar med så mycket som får plats i paketet och sätter TC-flaggan (”truncated”).

6. (6) Vilka begränsningar gäller för tecknen i ett domännamn av typen ”hostname”? (2 p)

   Endast ”a-z”, ”A-Z”, “0-9” och “-“ får användas i en ”label” i ett ”hostname”. ”-” får varken inleda eller avsluta en ”label”. Mellan ”labels” används ”.” Tecknen ”A-Z” hanteras som identiska med ”a-z”.

7. (7) Delegering är ett viktigt begrepp i DNS. Vad innebär en delegering? (2 p)

   Delegering innebär att en nod i DNS-trädet, och alla underliggande noder, hänvisas till en eller flera namnservrar som har den delegerade zonen (dot-terzonen).

8. (8) Om du vill göra en baklängesuppslagning av en viss IPv4-adress, hur kommer då frågan se ut i frågesektionen av DNS-paketet? Beskriv DNS-frågan och ge ett exempel. (2 p)

   Exempel på baklängesuppslagning av 130.237.28.40:

   ```
   40.28.237.130.in-addr.arpa.  IN  PTR
   ```

   - Owner name skapas genom att IPv4-adressens oktetter sätts i omvänd ordning och sedan får suffixet ”.in-addr.arpa.”
   - Klassen är alltid ”IN”.
   - Frågetypen (vilket i detta fall är posttypen vi frågar efter) är alltid ”PTR”.

9. (9) Vad kan man uppnå med att stoppa in ”wildcard”, ”*”, i en zonfil? Vilka begränsningar finns det i användningen av ”wildcard”? (2 p)

   Man kan få alla namn under zonen att existera med samma DNS-data.

   Begränsningen är att ”wildcard” bara kan användas för en hel ”label”, aldrig en del av en ”label”, och att det måste vara den första labeln DNS-posten i zonfilen som är ett ”wildcard”, ”*”.

10. (10) Vad innebär ”zone walking” med hjälp av NSEC-poster? (3 p)

    Eftersom en NSEC-post både har information om vilka posttyper som det finns poster av i innevarande nod och information om nästa nod i zonen så är det möjligt att vandra från nod till nod och plocka ut alla DNS-poster även om zonöverföring är avstängd.

11. (11) Vilka begränsningar gäller för antalet CNAME-poster i en nod och hur CNAME-poster får kombineras med andra DNS-poster i en DNSSEC-signerad zon? (3 p)

    En CNAME-post är alltid ensam i sitt RRset. En CNAME-post kan inte kombineras med någon annan DNS-post än RRSIG och NSEC.

12. (12) En ”label” i ett vanligt domännamn kan vara en ASCII-label eller en IDN-label. En IDN-label kan dessutom representeras på olika sätt. (4 p)

    - På vilka olika sätt kan en och samma IDN-label representeras? Ge namnet på dessa olika representationer och beskriv hur de skiljer sig åt och hur de förhåller sig till varandra.
    - Vad är skillnaden mellan en ASCII-label och IDN-label? Beskriv skillnaden med hänsyn till de olika representationerna av IDN-label.
    - Illustrera svaret med relevanta domännamn, riktiga eller påhittade, och kommentera vad det är för ”lablar”.

    A-label och U-label är två representationerna av samma IDN-label. U-label är en ”label” med minst ett icke-ASCII-tecken inom Unicode. A-label är ASCII-representation av U-label. A-label börjar alltid på prefixet ”xn--" och består sedan av kodningen av U-label. Det går alltid att konvertera från den ena till den andra utan informationsförlust.

    En ASCII-label består bara av ASCII-tecken och respresenterar bara dessa tecken. En IDN-label består av något icke-ASCII-tecken, direkt (U-label) eller via omkodning (A-label).

    Exempel: ”malmo.se”, ”malmö.se”, ” xn--malm-8qa.se”. ”se” och ”malmo” är ASCII-lablar. ”malmö” och ” xn--malm-8qa” är IDN-lablar, varav den första är en U-label och den andra är en A-label.

    (Om A-label och U-label är rätt beskrivet och exempel på dem, men vanlig ASCII-label inte beskrivs så kan det ge 3 p. Om A-label och U-label är någorlunda beskrivet, men resten är fel så kan det ge 1p.)

13. (13) Vilka DNS-poster tillkommer i en DNSSEC-signerad zon jämfört med en osignerad? Komplettera zonen nedan med dessa DNS-poster och förklara vad de har för funktion. (7 p)

    - Kopiera zonen nedan och uppdatera den med DNSSEC-posterna. Det ska vara rätt ”owner name” och posttyp.
    - Detaljerna i RDATA för de nya posterna behöver inte finnas med utan kan anges som ”(…)”.
    - Beskriva RDATA för DNSSEC-posterna.
    - Förklara vad de nya DNS-posterna har för funktion i den signerade zonen och hur de är kopplade till de befintliga posterna och andra nya poster.
    - Dina beskrivningar och kommentarer kan läggas som zonfilskommentarer direkt efter posterna som du ska kommentera. Inled då raden med ”;”.
    - Din uppdaterade zonfil ska vara en giltig zonfil förutom RDATA för DNSSEC-posterna.

```
$ORIGIN exempel.se.
$TTL 3600
@                       SOA ns1.example.com. root.telia.se. (
                                2019030909
                                14400
                                900
                                604800
                                3600
                                )
                        NS      ns1.example.com.
                        NS      ns2.example.com.
                        MX      1 mail
mail                    A       130.237.28.40
```

Posttyper DNSKEY, RRSIG och NSEC tillkommer. (NSEC3 och NSEC3PARAM stället för NSEC om man vill).

```
$ORIGIN exempel.se.
$TTL 3600
@                       SOA ns1.example.com. root.telia.se. (
                                2019030909
                                14400
                                900
                                604800
                                3600
                                )
                        RRSIG   (…) ; På SOA RRSET
                        NS      ns1.example.com.
                        NS      ns2.example.com.
                        RRSIG   (…) ; På NS RRSET
                        DNSKEY  (…) ; KSK
                        DNSKEY  (…) ; ZSK
                        RRSIG   (…) ; På DNSKEY RRSET
                        MX      1 mail
                        RRSIG   (…) ; På MX RRSET
                        NSEC    (…) ;
                        RRSIG   (…) ; På NSEC RRSET
mail                    A       130.237.28.40
                        RRSIG   (…) ; På mail/A RRSET
                        NSEC    (…) ;
                        RRSIG   (…) ; På mail/NSEC RRSET
```

DNSKEY innehåller de publika DNSSEC-nycklarna för zonen i RDATA och gör det möjligt att validera DNS-posterna via RRSIG.

RRSIG skapas för varje RRSET inkl de nya (exkl sig själv) och gör det möjligt att validera RRSET via DNSKEY.

NSEC läggs till i varje namn (”owner name”) i zonen. I detta fall en NSEC-post med owner name **exempel.se.** och en med owner name **mail.exempel.se.**

RDATA för NSEC har dels namnet på nästa namn, dels en lista över alla posttyper med samma ”owner name” som NSEC-posten.

Del 2

14. (14) Hur skiljer sig DoT (”DNS over TLS”) från vanlig DNS? (1 p)

    Kommunikationen är krypterad.

15. (15) Vilken teckenuppsättning baseras IDN-namn på? (1 p)

    Unicode.

16. (16) Vad innebär "query name minimisation"? (1 p)

    Istället för att resolvern skickar hela frågan i varje steg (från rotzonen och nedåt) så skickar resolvern bara en minimal fråga tills den har hittat zonen där svaret finns.

17. (17) Ge ett exempel på en ccTLD. (1 p)

    .SE, .DK, .DE… (en räcker).

18. (18) Beskriv två tekniker för att begränsa vilka klienter som kan hämta en zon med zonöverföring, (2 p)

    1. Lista över vilka IP-adresser som zonöverföring tillåts till.
    2. Att kräva att en specifik TSIG-nyckel ska användas vid begäran om zonöverföring.

19. (19) Det finns två tidsvärden i SOA-posten som styr zonöverföring. Beskriv deras roll för zonöverföringen. (2 p)

    ”SOA refresh” specificerar hur ofta slavservern ska kontrollera om zonöverföring är nödvändig. ”SOA retry” specificerar hur ofta slavservern ska försöka igen om kontrollen eller zonöverföringen misslyckades.

20. (20) Vad innebär tekniken ”anycast”? Utgå ifrån rotnamnservrarna och beskriv hur ”anycast” används för att öka kapacitet, spridning och tillgänglighet för dessa. (2 p)

    ”Anycast” innebär att samma IP-adress annonseras ut från olika platser med olika servrar för ”samma” namnserver (NS). Tekniken ökar kapaciteten för namnservern och ger närhet till den från olika platser.

21. (21) Du ställer en fråga med ”dig” till en namnserver och får tillbaka ett svar (”response”) med status SERVFAIL. Beskriv två scenarier där detta skulle ske. (2 p)

    Två beskrivningar räcker.

    - Namnservern ska, enligt dess konfiguration, vara auktoritativ för ”query name”. Servern är masterserver för zonen i fråga, men servern kan p.g.a. fel inte ladda zonen.
    - Namnservern ska, enligt dess konfiguration, vara auktoritativ för ”query name”. Servern är slavserver för zonen i fråga, men servern har p.g.a. något fel inte kunnat verifiera mot eller uppdatera från dess masterserver under så lång tid att ”expire” från SOA-posten har inträtt.
    - Namnservern är en resolverserver som misslyckas med att genomföra uppslagningen av ”query name” p.g.a. fel utanför resolvern, t.ex. nätverksfel eller fel i hostingen av aktuell zon.

22. (22) Vilka är DNS-paketets fem huvuddelar? Ange delarna i den ordning som de kommer i paketet. (3 p)

    - Header
    - Question section
    - Answer section
    - Authority section
    - Additional section

    5 korrekta delar i fel ordning ger 2,5 p. 0,5 p/korrekt del vid färre korrekta delar.

23. (23) EDNS är en utökning av DNS-protokollet. Beskriv hur EDNS fungerar och vad det tillför enligt följande punkter. (3 p)
    - Vad är det för posttyp som används för EDNS-informationen?
    - Var i DNS-paketet transporteras EDNS-informationen?
    - Hur kan man se med ”dig” om DNS-paketet är utökat med EDNS eller inte?
    - Ge ett exempel på information som kan signaleras med hjälp av EDNS.

    - Posttypen OPT används för EDNS.
    - OPT ligger i ”additional section”.
    - “dig” visar EDNS-informationen i ”OPT PSUEDOSECTION” i början av visningen av DNS-paketet.
    - Två exempel, ett räcker:
        1. Maximalt storlek (över 512 bytes) på UDP-paket som accepteras signaleras.
        2. Flagga för om DNSSEC-poster ska skickas i svarspaketet skickas.

24. (24) Utgå ifrån namnet ”www.kth.se” och posttypen A, som finns. Tänk dig att du ställer en DNS-fråga efter det namnet med den posttypen till olika renodlade DNS-hostingservrar på det publika Internet. Beskriv de tre kategorier av servrar som du normalt kommer att stöta på, i förhållande till just denna fråga. Låt beskrivningen utgå ifrån status och vilka DNS-poster som finns, inte finns eller kan finnas med i de olika ”sections” i svarspaketet. Utgå ifrån att servrarna är modernt och korrekt konfigurerade. Bortse ifrån EDNS, klass och TTL. (4 p)

    Alla svarspaket kommer att ha samma innehåll i ”question section”, vilket är kopierat från frågepaketet, ”www.kth.se. A”.

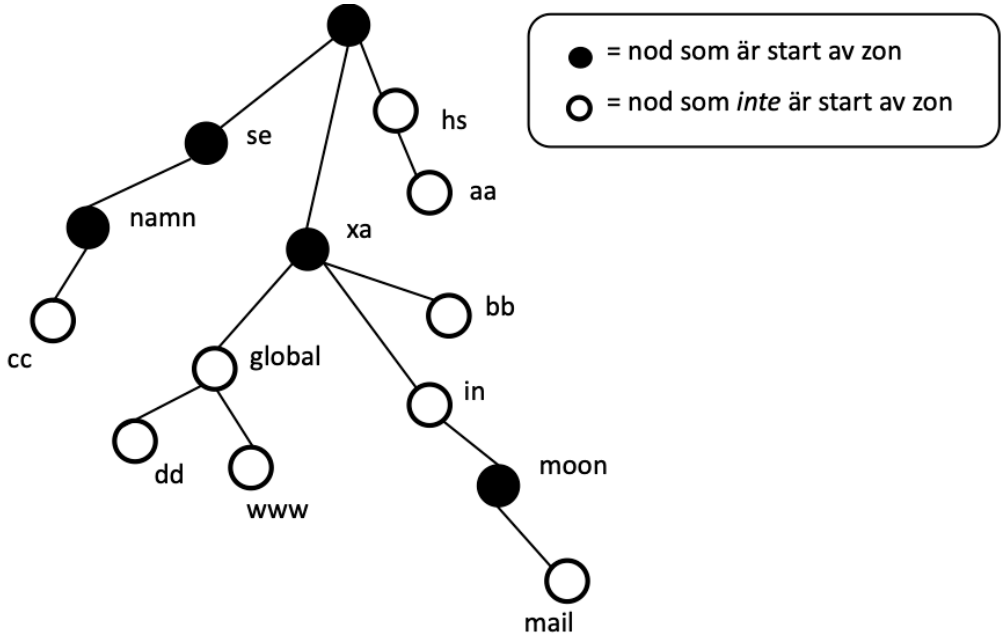
    Kategori 1. Servern har varken kth.se-, se- eller rotzonen. Status i svarspaketet är REFUSED. Förutom ”question section” så innehåller svarspaketet inga DNS-poster.

    Kategori 2. Servern har kth.se-zonen. Status i svarspaketet är NOERROR. ”Answer section” innehåller svaret i form av ”www.kth.se. A x.x.x.x”. ”Authority section” kan innehålla NS-posterna för kth.se-zonen och i så fall kan ”additional section” innehålla A- eller AAAA-poster för namnservernanen från NS-posterna.

    Kategori 3. Servern har se- eller rotzonen (men inte kth.se-zonen). Status är NOERROR. ”Answer section” är tom. ”Authority section” innehåller NS-poster för se-zonen (från rotnamnserver) eller för kht.se-zonen (från .se-server). ”Additional section” innehåller A- eller AAAA-poster om glue-poster är nödvändiga. Ifall glue-poster inte behövs så kan ”additional section” vara tom.

25. (25) I en labbmiljö med en egen rot och bara IPv4 så sätts zoner upp som ger DNS-trädet enligt bilden. Zonerna är korrekt uppsatta utan DNSSEC. Lista de auktoritativa DNS-poster som måste finnas för att det ska vara korrekt och för att trädet ska skapas. (7 p)

    - Detaljerna i RDATA behöver inte finnas med detaljer om det består av mer än ett delfält. Kan då skrivas som ”(…)”. Om RDATA består av *ett* delfält så ska alla detaljer finnas med och vara korrekta.
    - Uppsättningen ska vara minimal, men fortfarande korrekt och komplett.
    - Det finns olika korrekta lösningar, men använd exakt 16 DNS-poster för att lösa uppgiften, varken fler eller färre.
    - Alla namn ska vara absoluta.
    - Om du inkluderar DNS-poster som är förenliga med trädet, men inte behövs eller om du inkluderar DNS-poster som inte är förenliga med trädet så får du också minuspoäng. Totalsumman på frågan kan aldrig bli mindre än noll.



Svaret ska innehålla SOA- och NS-post för alla noder som startar zon. NS-posten ska peka ut ett namn i trädet, där det ska finnas en A-post, men namnet är valfritt. Mellanliggande noder utan zonstart ska inte ha någon DNS-post (för att hålla antalet minimalt). Terminala noder ska innehålla en DNS-post. De exakta DNS-posterna vara olika, men antalet är 16 DNS-poster.

```
.                   SOA         (…)
.                   NS          aa.hs.
aa.hs.              A           192.0.2.1
se.                 SOA         (…)
se.                 NS          bb.xa.
namn.se.            SOA         (…)
namn.se.            NS          cc.namn.se.
cc.namn.se.         A           192.0.2.30
xa.                 SOA         (…)
```

```
xa.                 NS          bb.xa.
bb.xa.              A           192.0.2.40
dd.global.xa.       A           192.0.2.50
www.global.xa.      TXT         ”tenta”
moon.in.xa.         SOA         (…)
moon.in.xa.         NS          dd.global.xa.
mail.moon.in.xa.    TXT         ”tenta”
```