Internets domännamnssystem (HI1037)

13 mars 2025

Hjälpmedel:	Inga.
Observera:	Lösningarna måste vara skrivna med läsbar handstil. Ange namn och personnummer på varje sida. Maximalt 58 poäng kan uppnås. Betygsgränser: • 0-26 poäng: F (underkänt) • 27-28 poäng: Fx • 29-34 poäng: E • 35-38 poäng: D • 39-44 poäng: C • 45-50 poäng: B • 51-58 poäng: A

---

1. En DNS-klient skickar en förfrågan till en namnserver över UDP 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”).

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

   Kommunikationen är krypterad.

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

   Unicode.

4. Vad betyder det att AA-flaggan är satt i ett svarspaket? (1 p)

   Svaret är auktoritativ data.

5. Vad är en ccTLD? (1 p)

   Landstoppdomän.

   (Om man svarar ”toppdomän”, men ger exempel med en ccTLD så kan det ge 0,5 p)

6. Vad är nackdelen med höga TTL-värden på DNS-poster i zonen? (1 p)

   Det tar längre tid för förändringar av dessa DNS-poster att få genomslag.

7. Vad betyder FQDN? (1 p)

   "Fully qualified domain name" eller "absolut domännamn".

8. Hur förhåller sig posttyp till RDATA? (1 p)

   Posttypen styr formatet på RDATA och därmed vilken data som får och måste finnas i RDATA.

9. Utgå ifrån IPv4-adress 10.20.30.40 och tänk dig att du använder programmet ”dig” med växeln ”-x”. (2 p)
   - Visa hur ”question section” kommer att se ut i det DNS-paketet som ”dig” skickar.
   - Beskriv hur DNS-namnet (”owner name”) i ”question section” skapas från IP-adressen.

   ”Question section”:

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

   [IP-adressen normaliseras så att den representeras av fyra decimala oktetter utan extra inledande nollor.] DNS-namnet (”owner name”) skapas genom att IPv4-adressens oktetter sätts i omvänd ordning med punkter mellan och sedan får suffixet ”.in-addr.arpa.”

10. Rotzonen har en speciell roll för en DNS-resolver. (2 p)
    - Vilken är denna roll?
    - Vad händer om resolvern inte har tillgång till rotzonen?

    DNS-resolvern måste alltid börja DNS-uppslagningarna i rotzonen och måste därför ha tillgång till den. Om rotzonen är oåtkomlig så kommer all resolvning att misslyckas.

11. RDATA för en MX-post består av två delfält, ett heltal resp. ett domännamn. Hur används delarna av en SMTP-klient? (2 p)

    Om det finns flera MX-poster med samma ”owner name” så ska klienten i första hand använda den MX-post som har det lägsta värdet i första delfältet. I andra hand det med det näst lägsta.

    Domännamnet i delfält två representerar mailservern för maildomänen (= MX-postens ”owner name”). SMTP-klienten slår upp IP-adressen till domännamnet i fält två [och gör en SMTP-uppkoppling mot den].

12. Det finns tre A-poster för ”www.exempel.se” och flera klienter gör flera uppslagningar av ”www.exempel.se. A”. Varje klient ska använda en av posterna. (2 p)
    - I den normala situationen, i vilken ordning kommer posterna?
    - Hur väljer klienten normalt vilken post som den ska använda?

    Posterna kommer i olika ordning för de olika klienterna och vid upprepad förfrågan. Klienten tar normalt den första posten i listan. (Referens till ”round robin” eller "slumpmässig" är likvärdigt med "olika ordning".)

13. En DNS-fråga i ”question section” består av tre delar, varav klass (”class”) är den ena. Vilka är de två andra? (2 p)

    a) Owner name, queryname eller qname

    b) query type eller qtype

14. 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? (2 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.

15. Hur kommer en renodlad och publik DNS-hostingserver hantera olika frågor? (2 p)
    - Kommer frågor om olika domäner att hanteras på lika eller olika sätt? Beskriv hanteringen och kommentera ev. olikhet i hanteringen.
    - Kommer olika klienter att hanteras på lika eller olika sätt? Beskriv hanteringen och kommentera ev. olikhet i hanteringen.
    - Kan man tänka sig en hänvisning i svaret på en vanlig fråga? I så fall, för vilka frågor? Motivera.

    En renodlad DNS-hostingserver kommer bara att svara på DNS-frågor som gäller namn som ligger inom eller under de zoner som är laddade av servern. Om frågan gäller annat namn så kommer den normalt att svara med REFUSED.

    En renodlad, publik DNS-hostingserver kommer normalt att svara på DNS-frågor från alla klienter.

    Om frågan gäller ett namn i en underliggande zon till en zon som finns på servern, men där den underliggande zonen inte finns på servern, så kommer servern att svara med en hänvisning (delegering).

16. 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 ett visst namn att existera med samma DNS-data.

    Begränsningar:

    - Ett ”wildcard” bara kan användas för en hel ”label”, aldrig en del av en ”label”.
    - Det måste vara den först labeln i domännamet som är ett wildcard, t.ex. "*.namn.se" "*.www.namn.se". I "www.*.namn.se" så är "*" inget wildcard.

17. DNS-paketet "on the wire" består av fem huvuddelar. (4 p)
    - Ange delarna i den ordning som de kommer i paketet.
    - Ange vad det är för type av data som kan finnas i respektive del. Om en del innehåller flera typer av data så räcker det med ett exempel.
        - Header
            - Innehåller flaggor, statuskod, ID m.fl.
        - Question section
            - Frågeposten ("query name, query class and query type")
        - Answer section
            - DNS-poster
        - Authority section
            - DNS-poster
        - Additional section
            - DNS-poster

18. Hur skapar man en delegering av en dotterzon från en moderzon? Ge ett sammanhängande svar och illustrera med ett kommenterat exempel. (4 p)

    - Vilka DNS-poster måste läggas in i moderzonen?
    - Vilka DNS-poster kan läggas in?
    - Vad är det som pekas ut med delegeringen?
    - Vad förväntas finnas i dotterzonen som relaterar till delegeringen?

    En eller flera NS-poster med samma ”owner name” infogas i zonfilen. NS-posternas ”owner name” ska vara en subdomän till zonfilens apex.

    Det som pekas ut är de namnservrar som håller dotterzonen med samma namn som "owner name" till NS-posterna, samt att dotterzonen existerar.

    Namnen (namnservrarna) som pekas ut ska vara uppslagbara i DNS (A eller AAAA). Om något namn (namnserver) tillhör den utdelegerade zonen så måste glue-poster (A eller AAAA) tillfogas.

    I se-zonen:

```
example.se.       NS   ns1.example.se.
example.se.       NS   ns2.example.se.
example.se.       NS   ns.namn.se.
example.se.       NS   dns.example.xa.
ns1.example.se.   A    192.0.2.5
ns1.exemple.se.   AAAA 2001:DB8:A::5
ns2.example.se.   A    203.0.113.10
ns2.exemple.se.   AAAA 2001:DB8:B::A
```

    De två fösta NS måste ha motsvarande glue-poster eftersom namnen ligger under den delegeringspunkten. Den tredje kan motsvaras av en glue-post eftersom den ligger under .se, men måste inte. Den fjärde kan inte ha glue-post eftersom den ligger helt utanför .se.

    I dotterzonen (example.se) så ska samma NS poster läggas in. Ev. strikt nödvändiga glue-poster, som i exemplet, ska läggas in som A- och AAAA-posterna i dotterzonen.

19. Ett DNS-paket med förfrågan "www.red.xa. CNAME" skickas till en DNS-resolver. Därefter skickas förfrågan "www.red.xa. A" till samma DNS-resolver. I båda svarspaketen har RCODE värdet NOERROR och inget av svaren är NODATA. (4 p)

    Dessutom så gäller det:

    - DNS-resolvern kan antas bete sig korrekt.
    - I frågepaketen kan DO-flaggan antas vara osatt.
    - I frågepaketen ska RD-flaggan antas var satt.
    - I svarspaketen ska RA-flaggan antas vara satt.
    - Varken klass eller TTL behöver inkluderas.
    - Fält vars värde inte har specificerats i förutsättningarna kan sättas till något rimligt värde i DNS-posterna.

    Att besvara:

    - Vad kommer att finnas i "answer section" i respektive svarspaket?
    - Svara genom att ge fullständiga DNS-poster och motivera dessa.

    I först fallet (CNAME) så kommer "answer section" att innehålla följande DNS-post där RDATA har antagits till ett domännamn för att göra svaret fullständigt.

    ```
    www.red.xa.   CNAME   www.black.xa.
    ```

    Eftersom svarspaketet inte är NODATA så måste det finnas en DNS-post som motsvarar förfrågan. Vid fråga efter CNAME så görs ingen separat hantering av den, utan det är bara CNAME-posten som inkluderas.

    I andra fallet (A) så kommer "answer section" att innehålla följande DNS-poster där RDATA för CNAME har antagits vara samma som ovan och antagits vara "owner name" för A-posten för att skapa en giltig kedja. Det har antagits att det bara finns en A-post. RDATA för A-posten har antagits till ett möjligt värde.

    ```
    www.red.xa.    CNAME   www.black.xa.
    www.black.xa.  A       192.168.9.1
    ```

    Eftersom svarspaketet inte är NODATA så måste det finnas en DNS-post som motsvarar förfrågans "query type" (posttyp). Första fallet visade att det finns en CNAME-post i namnet så därför måste det finnas en A-post i det namn CNAME pekar på (eller ev. via flera CNAME).

20. 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.)

21. DS och DNSKEY. (4 p)

- Hur förhåller sig DS till DNSKEY?
- Hur bidrar DS-posten till tillitskedjan ("chain of trust")?
- I vilken zon finns DS respektive DNSKEY?
- Hur förhåller sig normalt begreppen KSK och ZSK till DNSKEY som förhåller sig till DS-post?
- Var i zonen finns respektive post?

DS-posten innehåller en referens till och en hash av den motsvarande DNSKEY-posten.

DS-posten skapar en tillitskedja (”chain of trust”) från moderzonen till dotterzonen genom att peka ut en giltig DNSKEY i dotterzonen.

DNSKEY ligger i apex i dotterzonen (den delegerade zonen).

DS-posten finns i moderzonen i delegeringspunkten (samma nod som NS-posterna i delegeringen).

Den DNSKEY som DS pekar på har normalt rollen KSK ifall det finns både KSK och ZSK i zonen.

22. Följande zonfil innehåller fel. Identifiera felen. För varje identifierat fel beskriv vad felet är och föreslå en rimlig rättning. Du får ett poäng per fel som du hittar, beskriver korrekt och har en rimlig rättning till. Om du pekar ut något som fel fast det inte är fel så får du ett minuspoäng, men totalsumman på frågan kan aldrig bli mindre än noll. (7 p)

```
$ORIGIN exempel.se.
$TTL 3600
@                       SOA ns1.exempel.se. root.blue.xa. (
                                2019030909060308
                                4400
                                900
                                604800
                                3600
                                )
                        NS          ns1.exempel.se.
                        NS          ns2.exempel.se.
                        TXT         "Invalid TXT record"
exempel.com.            MX          10  mail.exempel.se.
www                     A           130.237.28.40
                        CNAME       www.example.com.
ns1                     CNAME       nameserver
nameserver              A           130.237.72.250
ns2                     A           129.16.253.356
mail.                   A           130.237.72.246
                        AAAA        2001:6b0:1::246
_25._tcp.mail           TLSA 3 1 1 (
                        6F5D10A6DEA882679B6B
                        954BB01F88AB1EA08B434556
                        6B30F0D7E43B7F83981E )
# This is for jabber. Both must be there
_xmpp-client._tcp       SRV 0 0 5222 jabber.example.com.
_xmpp-server._tcp       SRV 0 0 5222 jabber.example.com.
```

1. Serienumret i SOA-posten är för stort för att vara ett 32-bitars heltal, vilket det ska vara. Korta ner det till t.ex. ”2019030909”.

2. Första NS-posten pekar på ett namn som har ett CNAME (ns1). RDATA i en NS-post måste vara ett namn som har en adresspost (A/AAAA). Gör om CNAME till en A-post med adressen som "nameserver" har.

3. ”Owner name” av MX-posten är ”out of zone data”. Zonen heter **exempel.se** och då kan vi inte ha **exempel.com** i zonen. Rätta owner name till ”exempel.se.”.

4. ”www” har två poster, A och CNAME. Man får inte kombinera CNAME med annan post för samma ”owner name”. Rätta genom att plocka bort CNAME eller rätta genom att plocka bort A.

5. ”ns2” har en A-post med ogiltigt IPv4-adress. En oktett kan inte vara 356. Rätta genom att sätta ett värde mellan 0 och 255.

6. ”mail.” är absolut, vilket gör att det är toppdomänen ”mail”, vilket inte kan finnas i vår zon (”out of zone data”). Rätta genom att ta bort

punkten så att det faktiska namnet blir ”mail.exempel.se.” (och matchar vår MX-post efter rättningen).

7. "#" är inte ett kommentarstecken i en zonfil. Ersätt det med ";".

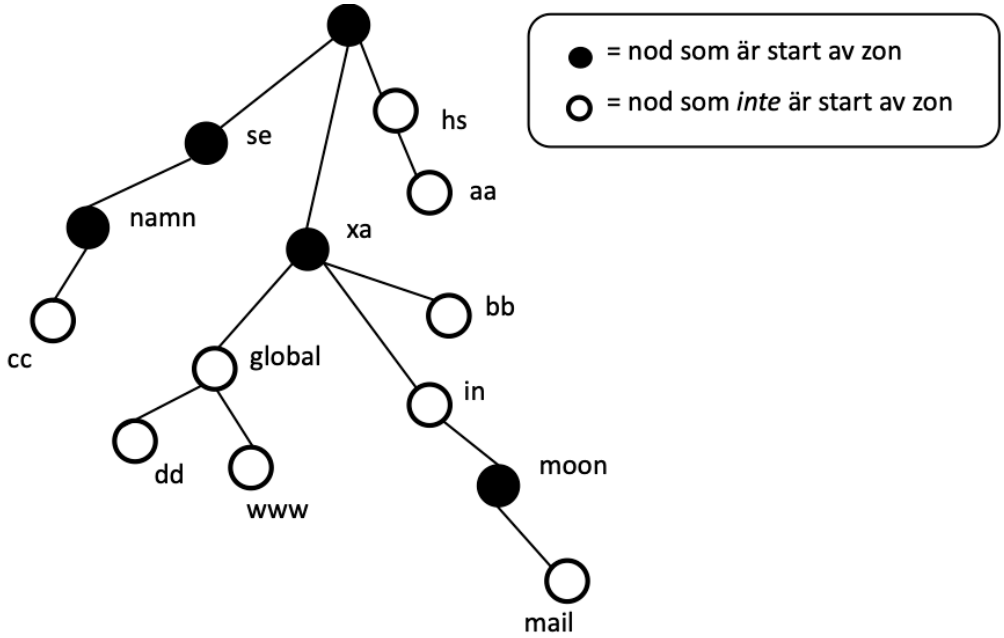
23. I en labbmiljö med en egen rot och bara IPv4 så sätts zoner upp som ger DNS-trädet enligt bilden. Zonerna är korrekt uppsatta utan DNSSEC. IP-adresserna som användas ska plockas valfritt inom 192.0.2.0/24.

    Uppgift:

    - Lista de auktoritativa DNS-poster som måste finnas för att det ska vara korrekt och för att trädet ska skapas.

    Förutsättningar:

    - Detaljerna i RDATA behöver inte finnas med 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 kan 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”
```