Internets domännamnssystem (HI1037)

10 mars 2020

Hjälpmedel:	Inga.
Observera:	Lösningarna måste vara skrivna med läsbar handstil. 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.

---

1. Vad betyder $TTL i en zonfil? (1 p)

   $TTL anger den TTL som ska gälla alla DNS-poster som inte har TTL angiven.

2. Ett svarspaket har tom ”answer section” och status NXDOMAIN.

   - Vad förväntas finnas i ”authority section”? (1 p)

     SOA-post.

   - Vad används informationen i ”authority section” till? (1 p)

     Fastställa cachetiden för det negativa svaret.

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

   Hela svaret (”response”) fick inte plats i ett DNS-paketet och det levereras avkortat.

4. Ge ett exempel på en ccTLD. (1 p)

   .SE, .DK, .DE… (en räcker).

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

   Kommunikationen är krypterad.

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

   Unicode.

7. Hur kan man använda DNS för enkel lastbalansering? (1 p)

   Låta samma domännamn peka på två (eller flera) IP-adresser till olika servrar som tillhandahåller samma tjänst.

8. En förfrågan om exempel.se skickas till en namnserver som inte är DNS-resolver. Namnservern svarar med REFUSED. Vad är den troliga orsaken? (1 p)

   Namnservern har inte zonen exempel.se. [Och dessutom varken se-zonen eller rotzonen.]

9. En DNS-förfrågan om ”www.namn.se” ger ett svarspaket där AA-flaggan har satts. Vilka slutsatser kan vi dra om namnservern som svarspaketet kommer från? (1 p)

   Namnservern har laddat en zonfil där www.namn.se ingår (eller kan ingå). Namnservern är auktoritativ för en zon där www.namn.se ingår.

10. Vad innebär "query name minimalization"? (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.

11. Vilka fem huvuddelar består en DNS-post av? Ge ett exempel på en fullständig DNS-post och beskriv varje del. (2 p)

    Exempel:

    ```
    www.kth.se.  600  IN  A  130.237.28.40
    ```

    - Owner name, ex: “www.kth.se.”
    - TTL , ex: “600”
    - Klass, ex: “IN” (nästan aldrig något annat)
    - Posttyp, ex: “A”
    - RDATA, posttypsberoende, ex för ”A”: ”130.237.28.40”

12. Samma DNS-fråga om en korrekt signerad DNS-post skickas i två olika förfrågningar till en validerande resolver. I det ena fallet sätts AD-flaggan, men inte DO-flaggan. I det andra fallet sätts DO-flaggan, men inte AD-flaggan. Vilka likheter och skillnader kommer det att bli när det gäller flaggor och DNS-poster i svarspaketen? (2 p)

    När DO-flaggan inte är satt, så kommer svarspaketet inte inkludera några DNSSEC-poster. När DO-flaggan är satt så kommer DNSSEC-poster att inkluderas. I båda fallen så kommer AD-flaggan vara satt och samma vanliga DNS-poster kommer att vara inkluderade. [När DO-flaggan är satt i frågepaketet så kommer den också att vara satt i svarspaketet.]

13. 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 ska ”ha” den delegerade zonen (dotterzonen).

    - Vilken information finns i den delegerande zonen för att skapa delegering? (2 p)

      I den delegerande zonen (moderzonen) så finns det i noden (domänen) som delegeras en eller flera NS-poster som pekar ut namnen på namnservrarna för den delegerade zonen (dotterzonen). Om det krävs så finns det glue-poster (A/AAAA) i den delegerande zonen som komplement till NS-posterna. [Glue-posterna behöver bara finnas för NS (RDATA) som tillhör den delegerade zonen.]

14. Utgå ifrån en viss IPv4-adress och tänk dig att du använder programmet ”dig” med växeln ”-x”. Ange vilken IP-adress du har valt. 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. (2 p)

    Vald IP-adress: 130.237.28.40

    ”Question section”:

    ```
    40.28.237.130.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 punkt mellan och sedan får suffixet ”.in-addr.arpa.”

15. Vad är skillnaden mellan en zon och ett domännamn? Hur förhåller sig dessa till domännamnsträdet. (2 p)

    Ett domännamn är en nod (plats) i domännamnsträdet medan en zon är en del av domännamnsträdet. Zonen startar i ett domännamn (nod) och går nedåt. Zonen kan omfatta många domännamn (noder). Zonen slutar där nästa zon tar vid eller där delträdet slutar.

16. Det finns en speciell posttyp för email. Vilken är den och hur används den? Illustrera med ett exempel. (2 p)

    Posttypen är MX.

    MX pekar ut mailservern för maildomänen (i fält 2 i RDATA). Om det finns flera MX-poster för samma maildomän så kommer prioritetsfältet (fält 1 i RDATA) att styra vilken MX-post som ska användas.

    ```
    namn.se.  MX  10 mail.namn.se.
    ```

17. Hur kommer en renodlad DNS-resolverserver resp. en renodlad DNS-hostingserver hantera olika frågor? Hur hanterar servrarna frågor om olika domäner? Hur hanterar servrarna frågor från olika klienter? Ge en sammanhängande beskrivning. (3 p)

    En renodlad DNS-hostingserver kommer normalt att svara på DNS-frågor från alla klienter, men den 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 ett namn i en sådan zon så kan den ge ett auktoritativt svar.] Om frågan gäller ett namn i en underliggande zon så kommer den istället att ge en hänvisning (delegering). Om frågan gäller annat namn så kommer den normalt att svara med REFUSED.

    En renodlad DNS-resolverserver kommer att svara på frågor gällande alla namn i DNS-trädet så vitt det är möjligt genom rekursiv uppslagning. [Svaren till klienten är inte auktoritativa.] Ofta svarar en DNS-resolver bara på frågor från vissa klienter (t.ex. egna nätet). Övriga får REFUSED.

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

    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.

19. Hur kan en DNS-klient påverka storleksbegränsningen av DNS-svarspaketet över UDP? Vad krävs av DNS-servern för att mekanismen ska fungera? Vad händer om DNS-servern inte har stöd för mekanismen, men klienten ändå använder den? (3 p)

    Mekanismen kräver att klient och server har stöd för EDNS. Klienten signalerar genom EDNS vilken maximal storlek på DNS-paket [över UDP] som den kan acceptera. Om servern inte har stöd för EDNS så kommer den att svara med statuskod FORMERR [vilket gör att klienten måste ställa frågan igen utan EDNS].

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

    1. Owner name, queryname eller qname
    2. query type eller qtype

21. Tre olika namnservrar är utpekade med NS-poster för en viss zon och alla svarar korrekt.

    - Kan någon som **inte har** direkt tillgång till namnservrarna avgöra vilken av namnservrarna som är slavserver resp. masterserver? Förklara varför. (2 p)

      Nej, både master och slav är auktoritativa för zonen och det finns ingen skillnad i hur dessa svarar för zonen så utifrån går det inte att skilja dem åt.

    - Kan någon som kan logga in på namnservrarna med full access avgöra vilken av namnservrarna som är slavserver resp. masterserver? Förklara varför. (2 p)

      Ja, det är olika konfigurering för master resp. slav och det går att läsa ut hur zonöverföringar går.

22. Vilken roll har cachning för DNS-resolvning? Vad styr cachningen? Beskriv hur cachningen påverkar svaren vid DNS-resolvning. (2 p)

    Cachningen är tillfällig lagring av svar som har hämtats genom en vanlig DNS-fråga. Tiden för hur länge det lagras styrs av TTL för DNS-posten. När en DNS-resolver har det efterfrågade datat i sin cache så kan den svara direkt utan att ställa egna frågor.

23. DNSKEY används för att verifiera en signerad zon. Vilken posttyp används för att verifiera att det är rätt DNSKEY-post som resolvern har fått? Var återfinns en DNS-post av den posttypen? (2 p)

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

    Medans DNSKEY ligger i apex i dotterzonen (den delegerade zonen) så ligger DS-posten i moderzonen.

24. Hur förhåller sig en A-label till en U-label? Hur kan man se att det är en A-label resp. U-label? (3 p)

    A-label och U-label är två olika kodningar (skepnader) av samma IDN-label. Det går alltid att konvertera från den ena till den andra utan informationsförlust.

    U-label är kodat i Unicodetecken och innehåller minst ett icke-ASCII-tecken [ASCII är ett subset av Unicode].

    En A-label har alltid prefixet ”xn--" och innehåller alltid bara ASCII-tecknen a-z, 0-9 och ”-”. [Det som står efter prefixet kan konverteras till motsvarande U-label.]

25. Följande zonfil innehåller fel. Identifiera felen. För varje identifierat fel beskriv vad felet är och föreslå en rimlig rättning. Du får ett poäng för varje korrekt fel. 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. (5 p)

```
$ORIGIN exempel.se.
$TTL 3600
@                       SOA ns1.exempel.se. root.telia.se. (
                                2019030909060308256677 7
                                4400
                                900
                                604800
                                3600
                                )
                        NS          ns1.exempel.se.
                        NS          ns2.exempel.se.
exempel.com.            MX          10  mail.exempel.se
                        TXT         "Invalid TXT record"
www                     A           130.237.28.40
                        CNAME       www.example.com.
ns1                     A           130.237.72.250
ns2                     A           129.16.253.356
mail.                   A           130.237.72.246
                        AAAA        2001:6b0:1::246
```

- 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”.
- ”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.”.
- Domännamnet i RDATA i MX-posten är relativt (saknar avslutande punkt) vilket gör att zonnamnet läggs på till ”mail.exempel.se.exempel.se.” vilket är fel. Rätta genom att lägga en punkt på slutet eller korta ner till ”mail”.
- ”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.)
- ”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.
- ”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).

26. Vilka DNS-poster tillkommer i en DNSSEC-signerad zon jämfört med en osignerad? Utgå ifrån zonen nedan. Ge ”owner name” och posttyp för de nya posterna. Detaljerna i RDATA behöver inte finnas med utan det räcker med att beskriva RDATA. Förklara vad de nya DNS-posterna har för funktion i den signerade zonen. (7 p)

```
$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.
www                     A       130.237.28.40
```

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

DNSKEY läggs till med owner name **exempel.se.** Det kan vara en eller flera DNSKEY. DNSKEY innehåller de publika DNSSEC-nycklarna för zonen i RDATA.

NSEC läggs till i varje namn i zonen. I detta fall en NSEC-post med owner name **exempel.se.** och en med owner name **www.exempel.se.** NSEC pekar i RDATA ut vilka posttyper som finns under NSEC-postens owner name plus att den pekar ut nästa namn i zonen. Därmed kan man fastställa vad som INTE finns i zonen.

RRSIG läggs till för varje RRset i zonen, d.v.s. för följande namn och posttyper. RRSIG innehåller i RDATA en kryptografisk signatur av innehållet i RRset. RRSIG skapas för följande RRset:

- exempel.se./SOA
- exempel.se./NS
- exempel.se./DNSKEY
- exempel.se./NSEC
- www.exempel.se./A
- www.exempel.se./NSEC

1 p för att lista alla relevanta posttyper. 1 p per posttyp för korrekt angivelse av var posterna kommer att finnas och 1 p per posttyp för korrekt beskrivning av vad varje posttyp har för funktion.