Internets domännamnssystem (HI1037)

15 mars 2024

Hjälpmedel:	Inga.
Observera:	Lösningarna måste vara skrivna med läsbar handstil. Ange namn och personnummer på varje sida. Maximalt 58 poäng kan uppnås. Preliminära betygsgränser: E-A från 29 till 58 poäng med intervaller om ungefär 6 poäng. F (underkänt) under 29 poäng.

---

1. Vad är ett RRset? (1 p)

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

2. Vad är en DNS-fråga (”query”) med ”query type” AXFR? (1 p)

   Ett DNS-meddelande till en namnserver med begäran om zonöverföring av en specifik zon.

3. En förfrågan om example.se skickas till en internetoperatörs DNS-resolver, som svarar med REFUSED. Vad är den troliga orsaken? (1 p)

   Klienten sitter inte på ett IP-nät som DNS-resolvern accepterar att svara på frågor från.

4. Det finns några nya DNS-tekniker för att kryptera DNS-kommunikationen. Ge den gängse förkortningen för en sådan och vad den står för. (1 p)

   Alt 1: DoT, DNS över TLS.
   Alt 2: DoH, DNS över HTTPS.
   Alt 3: DoQ, DNS över Quic.

5. Hur kan man använda DNS för en enkel lastbalansering av webbservrar? (1 p)

   Låta samma domännamn peka på två (eller flera) IP-adresser [av samma protokoll (IPv4/IPv6)] till olika servrar som tillhandahåller samma tjänst.

6. Vad är en ccTLD? (1 p)

   Landstoppdomän.

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

7. Vilken är RDATA i följande DNS-post (en rad)? (1 p)

```
kth.se. 1800 IN SOA a.ns.kth.se. hostmaster.kth.se. 2023053061
14400 900 604800 86400
```

Hela uttrycket "a.ns.kth.se. hostmaster.kth.se. 2023053061 14400 900 604800 86400" är RDATA.

8. Hur används QR-flaggan, d.v.s. när är den satt och när är den inte satt? (1 p)

QR-flaggan är satt i ett svarspaket (”response”). I frågepaket (”query”) är den inte satt.

9. Vad heter den utökning som tillåter tecken bortom ASCII i domännamn och vad heter den teckenuppsättning som dessa baseras på? (2 p)

Utökningen heter IDN (eller "Internationalized Domain Name"). Tecken-uppsättningen heter Unicode.

10. Vilken är skillnaden mellan absoluta och relativa domännamn? Illustrera svaret med exempel. (2 p)

I absoluta domännamn så är den sista "label" (längst till höger) en toppdomän (direkt under rot). Det absoluta domännamnet avslutas med en punkt (".") i DNS-sammanhang. "www.kth.se." är ett absolut domänanmn.

Relativa domännamn är relativt något annat domännamn längre ner i domännamnsträdet. "www" är ett relativt domännamn, relativt t.ex. "kth.se.".

11. Var i zonen finns det alltid NS-poster och var i zonen kan det finnas NS-poster? (2 p)

Det finns alltid minst en NS-post (normalt minst två) i zonens apex, och om det finns delegeringspunkter i zonen så finns det minst en NS-post (normalt minst två) i varje delegeringspunkt. NS-poster finns inte på någon annan plats i zonen.

12. Beskriv kort de två tekniker för att begränsa vilka klienter som kan hämta en zon med zonöverföring (och som användes på laborationerna). (2 p)

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

13. "Gluepost" är ett begrepp i DNS. (2 p)
    - Vad är en ”gluepost” i delegeringen?
    - Vad är en nödvändig (strikt) ”gluepost”?
    - Illustrera med ett tydligt exempel.

    En gluepost är en adresspost för det namnservernamn som NS-posten pekar ut.

    En nödvändig gluepost är en adresspost för en namnserver vars namn ligger under delegeringen i fråga.

    Zonen namn.xa är delegerad från zonen xa. Adressposten för ”ns1.namn.xa” är en nödvändig gluepost:

```
namn.xa.       NS  ns1.namn.xa.
namn.xa.       NS  dns1.example.com.
ns1.namn.xa.   A   192.0.2.100
```

14. 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.
    - Namnservern är en resolver som validerar DNSSEC och något DNSSEC-fel gör att valideringen misslyckas, t.ex. DS-posten stämmer inte med DNSKEY i zonen.

15. Ett svarspaket har tom ”answer section” och status NXDOMAIN. Vi tänker oss ett svar utan DNSSEC. (2 p)
    - Vad förväntas finnas i ”authority section”?
    - Vad används informationen i ”authority section” till?

    a) SOA-post. (1 p)

    b) Fastställa cachetiden för det negativa svaret. (1 p)

16. 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".)

17. Vad innebär ”zone walking” med hjälp av NSEC-poster? (4 p)

    - Beskriv begreppet och illustrera det med hjälp av NSEC-poster från en fiktiv zon.
    - Dina NSEC-poster ska skapa en sammanhängande och fullständig kedja bestående av tre kompletta NSEC-poster.
    - Övriga DNS-poster behöver inte ingå.
    - Kommentera NSEC-posterna i ditt svar.

    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. Det går att direkt eller indirekt fråga efter NSEC-posterna i zonen.

    NSEC-poster i en fiktiv zon:

```
namn.se.      NSEC  mail.namn.se.  NS SOA MX RRSIG NSEC DNSKEY
mail.namn.se. NSEC  www.namn.se.   TXT A AAAA RRSIG NSEC
www.namn.se.  NSEC  namn.se.       A AAAA RRSIG NSEC
```

    Första NSEC-posten pekar på nästa namn i zonen (mail.namn.se) och visar vilka posttyper som finns i apex.

    Andra NSEC-posten pekar på sista (tredje) namnet i zonen (www.namn.se) och visar vilka posttyper som finns under mail.namn.se.

    Sista NSEC-posten visar att detta är det sista namnet izonen genom att peka tillbaka på apex och visar vilka posttyper som finns under www.namn.se.

18. En DNS-klient kan påverka storleksbegränsningen av DNS-svarspaketet över UDP. (4 p)
    - Beskriv mekanismen och vad klienten gör för att utnyttja den.
    - 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?
    - Vad är den normal åtgärden från klientens sida om DNS-servern inte har stöd för mekanismen?

    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. Den normala åtgärden från klienten är att ställa om frågan utan EDNS.

19. Tre olika namnservrar är utpekade med NS-poster för en viss zon och alla svarar korrekt. (4 p)
    - Kan någon som **inte har** direkt tillgång till namnservrarna avgöra vilken av namnservrarna som är slavserver resp. masterserver? Motivera ditt svar.
    - Kan någon som kan logga in på namnservrarna med full access avgöra vilken av namnservrarna som är slavserver resp. masterserver? Motivera ditt svar.
    - Spelar det någon roll för den som ställer DNS-frågor om det är en master eller slav som frågorna går till?

    - 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.

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

    - Nej, normalt inte. Både master och slav är auktoritativa för datat och ger normalt samma svar på en viss fråga.

20. Beskriv hur man tar fram DNS-namnet för baklängesuppslagning för IPv4 resp IPv6. Använd adresserna 10.11.12.13 resp abcd::6789 för att illustrera med. (4 p)

IPv4 (10.11.12.13):

1. Vänd ordning på oktetterna: 13.12.11.10
2. Sätt på ”in-addr.arpa” som suffix: 13.12.11.10.in-addr.arpa

IPv6 (abcd::6789):

1. Expandera adressen till explicit format:
abcd:0000:0000:0000:0000:0000:0000:6789
2. Tag bort ”:” och sätt ”.” mellan alla siffror:
a.b.c.d.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.7.8.9
3. Vänd på ordningen på alla siffor:
9.8.7.6.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.c.b.a
4. Sätt på ”ip6.arpa” som suffix:
9.8.7.6.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.c.b.a.ip6.arpa

(Rätt förutom ”för liten” IPv6-adress kan ge 3,5 p.)

21. 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).

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. (
                                20190309
                                4400
                                900
                                604800
                                3600
                                )
                        NS          ns1.exempel.se.
                        NS          ns2.exempel.se.
                        NS          130.237.70.50
                        TXT         "Invalid TXT record"
exempel.com.            MX          10  mail.exempel.se
www                     A           130.237.28.40
                        CNAME       www.example.com.
ns1                     A           130.237.72.250
nameserver              A           130.237.72.250
ns2                     A           129.16.253.356
intrawww                CNAME       intra
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. Tredje NS-posten pekar på något som ser ut som en IP-adress, men som inte kan vara en IP-adress. Lägg till namnet "ns3" i zonen med en A-post med den IP-adressen uppdatera NS-posten så att den pekar på "ns3".

2. ”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.”.

3. 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”.

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. "intrawww" har ett CNAME som pekar på ett namn som inte finns. Tag bort "intrawww" eller lägg till en adresspost under "intra".

7. ”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).

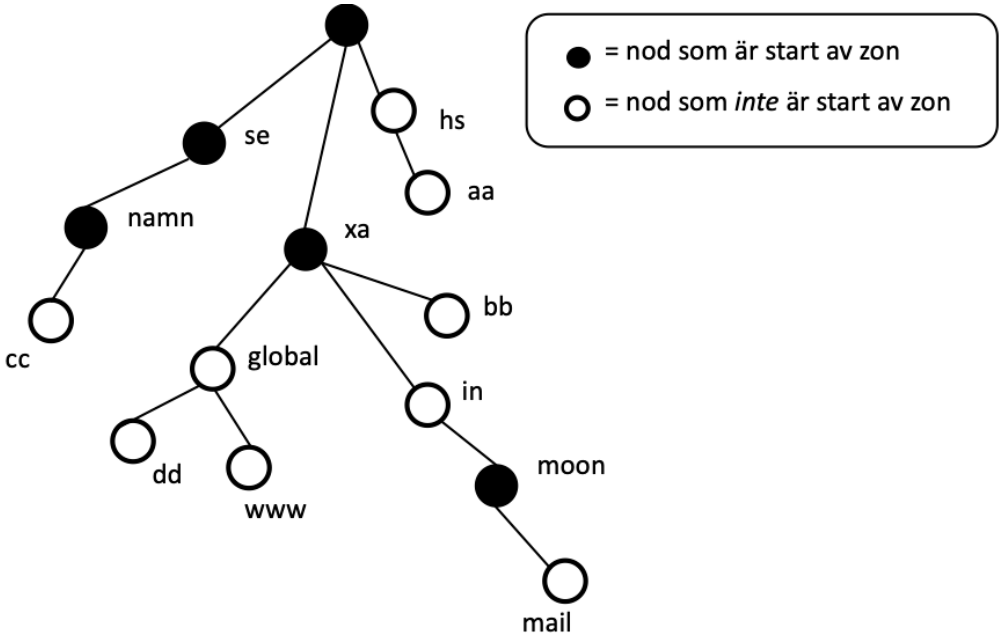
23. I en labbmiljö med en egen rot och bara IPv4 så sätts zoner upp som ger DNS-trädet enligt bilden. Zonerna är korrekt uppsatta utan DNSSEC. IP-adresserna som användas ska plockas valfritt inom 192.0.2.0/24.

    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”
```