Internets domännamnssystem (HI1037)

9 juni 2022

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 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.

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

   Port 53.

3. Vilken roll spelar Message ID i DNS-paketen för DNS-frågor och -svar (”DNS query and response”)? (1 p)

   Med Message ID i svarspaketet så kan klienten para ihop det med rätt frågepaket.

4. 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.

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

   Svaret är auktoritativ data.

8. Vad står IDN för? (1 p)

   Internationalized domain name. [Kortfattad, korrekt beskrivning av IDN är också rätt svar.]

9. Beskriv två tekniker för att begränsa vilka klienter som kan hämta en zon med zonöverföring (och som användes på laborationerna). (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.

10. Beskriv serienumrets (”SOA serial”) roll för zonöverföringen. (2 p)

    Slavservern använder serienumret för att avgöra ifall zonfilen har ändrats. Slavservern hämtar zonfilen från masterservern ifall serienumret hos mastern är högre än hos slaven.

11. Vad är en ”gluepost” i delegeringen? Vad är en nödvändig (strikt) ”gluepost”? Illustrera med ett tydligt exempel. (2 p)

    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
    ```

12. 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.

13. Hur förhåller sig DS till DNSKEY och hur används DS-posten? I vilken zon finns respektive post? Var i zonen finns respektive post? (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 i samma nod som NS-posterna i delegeringen. DS-posten har två uppgifter:

    1. Existensen av DS signalerar att dotterzonen måste vara signerad (med DNSSEC).

    2. DS-posten skapar en tillitskedja (”chain of trust”) från moderzonen till dotterzonen genom att peka ut en giltig DNSKEY i dotterzonen. Om vi kan lita på moderzonen (och därmed DS) så kan vi lita på DNSKEY i dotterzonen (och därmed allt den signerar direkt eller indirekt).

14. 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.
    ```

15. Det finns tre A-poster för ”www.exempel.se” och flera klienter gör var sin uppslagning av dessa. I den normala situationen, i vilken ordning kommer posterna? Klienten ska använda en post. Hur väljer klienten normalt vilken post som ska användas? (2 p)

    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” är likvärdigt med ”olika ordning.)

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. Vissa posttyper har begränsningar när det gäller hur många poster av den posttypen som får finnas i en nod, hur posttypen får kombineras med andra posttyper eller var posttypen får placeras i zonen. Vissa har flera begränsningar. Beskriv tre posttyper med någon begränsning och gör en fullständig beskrivning av respektive posttyps begränsningar. (3 p)

    Tre posttyper med korrekta beskrivningar ger full poäng. Nedan möjliga att välja mellan:

    - SOA – Kan endast förekomma i apex. Aldrig flera SOA med samma "owner name".
    - NS – Kan endast förekomma i två positioner i zonen, i apex eller i en delegeringspunkt.
    - CNAME – Aldrig flera CNAME med samma "owner name". Kan inte kombineras med andra poster utom NSEC och RRSIG.
    - DNSKEY – Kan endast förekomma i apex.
    - NSEC – Aldrig flera NSEC-poster med samma "owner name".
    - DS – Kan endast förekomma i delegeringspunkten.
    - CDS – Kan endast förekomma i apex.
    - CDNSKEY – Kan endast förekomma i apex.

18. 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].

19. En server är master för en zon och en annan server är slav för samma zon. Beskriv skillnader och likheter mellan servrarna. Utgå ifrån en normal situation (t.ex. som det var i labbmiljön). (3p)

    Skillnaderna är att zonfilen skapas på masterservern och sedan kopieras över med zonöverföring (AXFR/IXFR) till slavservern.

    Likheterna är att båda servrar är auktoritativa för zonen (zondatat) och att båda servrar ger samma svar på frågor om namn i zonen.

20. Det finns tre sätt som TTL kan bestämmas för en DNS-post i en zonfil. Ange de tre sätten och ange prioritetsordningen. (3 p)

    1. $TTL på egen rad. 2. Explicit TTL för DNS-posten. 3. Min-TTL i SOA-posten.

    I första hand gäller ev. explicit TTL. I andra hand gäller ev. $TTL som föregår DNS-posten. I tredje hand gäller min-TTL i SOA-posten.

    (Om allt är rätt förutom ofullständigt om vad i SOA-posten kan ge 2,5 p)

21. 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.)

22. 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)

    a) 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.

    b) Vad är skillnaden mellan en ASCII-label och IDN-label? Beskriv skillnaden med hänsyn till de olika representationerna av IDN-label.

    c) 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.)

23. Kopiera och uppdatera zonfilen nedan så att den är korrekt förutom de listade felaktigheterna. Du ska alltså lägga in dessa felaktigheter, men inga andra, genom att lägga till eller ändra i zonfilen. Du ska också beskriva varje felaktighet, vad och hur det är fel och hur det skulle vara rätt. Du får ett poäng för varje korrekt fel. Om du skapar felaktigt fel så får du minuspoäng, men totalsumman på frågan kan aldrig bli mindre än noll. (7 p)

    a) Felaktigt serienummer.

    b) CNAME i otillåten nod.

    c) FQDN som ger fel.

    d) Relativt domännamn som ger fel.

    e) Felaktig RDATA i en AAAA-post.

    f) ”Owner name” som ger fel.

    g) Lägg in en kommentar på fel sätt i zonfilen så att det blir en ”trasig” zonfil.

```
$ORIGIN exempel.se.
$TTL 3600
@                       SOA ns1.exempel.se. root.telia.se. (
                                4019060400
                                4400
                                900
                                604800
                                3600
                                )
                        NS          ns1.exempel.se.
                        NS          ns2.exempel.se.
ns1                     A           130.237.72.250
ns2                     A           129.16.253.254
```

Exempel på zonfil med felen ovan:

```
$ORIGIN exempel.se.
$TTL 3600
@                       SOA ns1.exempel.se. root.telia.se. (
                            5019060400
                            4400
                            900
                            604800
                            3600
                            )
                        NS          ns1.exempel.se
                        NS          ns2.
                        CNAME       www.exempel.se.
ns1                     A           130.237.72.250
ns2                     A           129.16.253.254
www                     AAAA        2001::53::80
# Mail is outsourced
exempel.com.            MX          10  mail.kth.se.
```

Serienumret i SOA-posten ska vara maximalt 2^32. Talet är större än så.

I första NS-posten så är RDATA relativt, vilket motsvarar FQDN ”ns1.exempel.se.exempel.se.” vilket inte finns.

I andra NS-posten så är RDATA absolut, men FQDN ”ns1.” finns inte.

CNAME kan inte finnas med andra DNS-poster i samma ”owner name”.

IPv6-adressen i RDATA för www.exempel.se är felaktigt.

”#” är ingen kommentarstecken, utan det ska vara ”;”.

MX-posten har ett ”owner name” som ligger utanför zonen.

(Det behöver inte vara 7 olika fel för att ge 7 poäng. Om samma fel kan sägas representera mer än en kategori så är det OK, men det måste finnas 7 beskrivningar.)

24. 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)

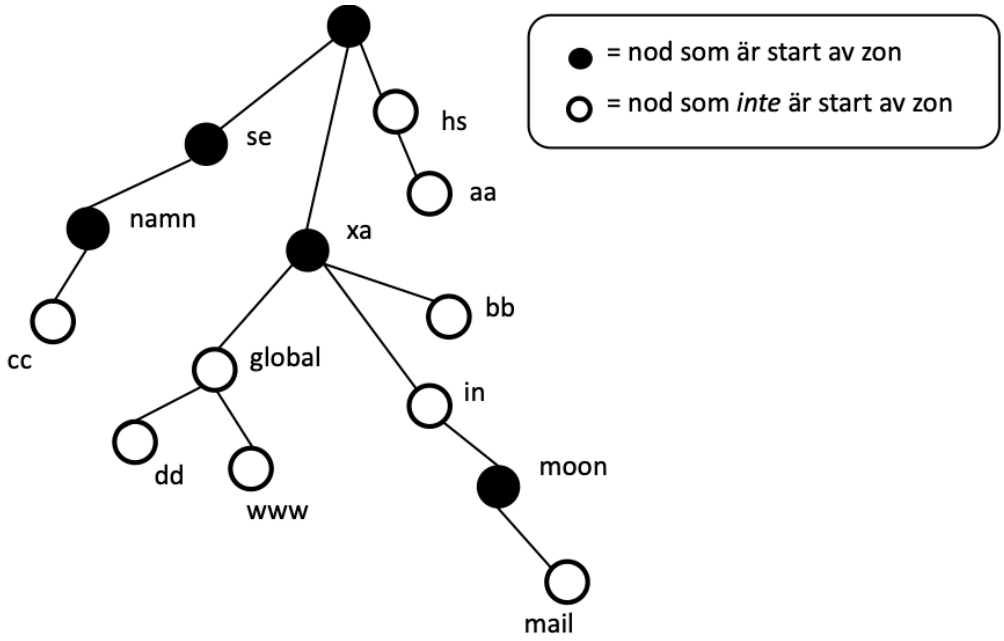
    a) Detaljerna i RDATA behöver inte finnas med om det består av mer än ett delfält. Kan då skrivas som ”(…)”. Om RDATA består av *ett* delfält så ska alla detaljer finnas med och vara korrekta.

    b) Uppsättningen ska vara minimal, men fortfarande korrekt och komplett.

    c) Det finns olika korrekta lösningar, men använd exakt 16 DNS-poster för att lösa uppgiften, varken fler eller färre.

    d) Alla namn ska vara absoluta.

    e) 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”
```