Internets domännamnssystem (HI1037)

18 december 2023

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. 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”).

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

   Kommunikationen är krypterad.

3. Vad har $TTL för funktion i en zonfil? (1 p)

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

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

   Klienten ber servern om rekursiv uppslagning.

5. 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 ifrån? (1 p)

   Namnservern är auktoritativ för zonen där www.namn.se ingår.

6. En klient skickar en DNS-fråga om ”www.iis.se” till sin resolver. Vad blir skillnaden om resolvern följer normal process eller "query name mininisation" när det gäller ”query name” när resolvern sedan ställer frågan till en rotnamnserver? (1 p)

   Normal är ”query name” hela ”www.iis.se”, men med "query name minimisation" så blir det istället bara ”se”.

7. Ge ett exempel på en ccTLD. (1 p)

   .SE, .DK, .DE… (en räcker).

8. Ge exempel på en ”query type” som inte är en posttyp. (1 p)

   ANY, AXFR, IXFR (en räcker)

9. Vilka är skillnaderna mellan en slavserver och en masterserver för en viss zon? (2 p)

   En slavserver hämtar zonfilen (zondatat) med AXFR/IXFR (zonöverföring) från den utpekade masterservern. På en slavserver editeras inte datat.

   På en ren masterserver uppdateras zondatat normalt genom att zonfilen redigeras på plats.

   [En server kan ha båda rollerna, d.v.s. hämta zonen från en annan master-server och sedan vara master gentemot andra slavar.]

10. Jämför följande två fall och ange vad det blir för status i svarspaketet. (2 p)
    - Det efterfrågade ”owner name” finns, men inte den efterfrågade posttypen i det namnet.
    - Det efterfrågade ”owner name” finns inte.

    a) Status blir NOERROR. (1 p)

    b) Status blir NXDOMAIN. (1 p)

11. Vilka fem huvuddelar består en DNS-post av? Ge ett exempel på en fullständig DNS-post och beskriv varje del i exemplet. (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”

    (Allt utom ett fullständigt exempel ger 1,5 p)

12. Vad innebär det att AD-flaggan sätts i ett frågepaket? När får AD-flaggan sättas i ett svarspaket? Vad betyder satt AD-flagga i svarspaketet? (2 p)

    I frågepaketet används en satt AD-flagga för att signalera att klienten är beredd på att ta emot ett svarspaket med AD-flaggan satt.

    I svarspaketet används en satt AD-flagga för att signalera att svaret (”response”) är validerat med DNSSEC. Flaggan får bara sättas om AD-flaggan eller DO-flaggan är satt i frågepaketet.

    (Om första delen är rätt, men andra ofullständig så kan det ge 1 p.)

13. 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.

14. 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.

    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).

15. RDATA för en MX-post består av två delfält, ett tal 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 (hel-) talet i första fältet. I andra hand det med det näst lägsta.

    Domännamnet i fält 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].

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

17. 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.

18. 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 är möjliga posttyper med beskrivning att välja mellan, men det finns fler:

    - 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". Alltid tillsammans med annan posttyp (aldrig ensam DNS-post i en specifik nod).
    - DS – Kan endast förekomma i delegeringspunkten i moderzonen.
    - CDS – Kan endast förekomma i apex.
    - CDNSKEY – Kan endast förekomma i apex.

19. 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.

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.

21. I zonerna för domänerna blue.xa resp. green.xa finns bla. DNS-posterna enligt nedan. När du besvarar denna fråga tänk på hur olika DNS-poster får kombineras, och när DNS-poster av en viss typ måste finnas, kan finnas resp. inte får finnas. (4 p)

```
www.blue.xa.     CNAME   www.iis.se.
www.green.xa.    CNAME   www.iis.se.
```

    Dessutom så gäller det:

    - Zonerna är korrekt uppsatta.
    - Namnet www.blue.xa har ytterligare tre DNS-poster av två olika typer.
    - Namnet www.green.xa har inga ytterligare DNS-poster.

    Att besvara:

    - Beskriv de tre ytterligare DNS-posterna i www.blue.xa och skriv DNS-posterna med så mycket detaljer som det går med tanke på den information som är given. Använd "(...)" för att markera delar där information inte finns.
    - Vilken slutsats kan man dra för blue.xa resp. green.xa gällande DNSSEC? Motivera ditt svar.

    CNAME kan inte kombineras med några andra DNS-poster än NSEC och RRSIG. NSEC och RRSIG kan bara finnas i signerade zoner. I zon med NSEC så måste NSEC finns i noder där det finns andra DNS-poster. I signerad zon så måste RRSIG för alla RRset.

    www.blue.xa har en NSEC-post och två RRSIG-poster, den ena för CNAME-posten och den andra för NSEC-posten. Vi vet inte vad nästa namn i zonen är. Posterna är

```
www.blue.xa.    NSEC (...)  CNAME NSEC RRSIG
www.blue.xa.    RRSIG NSEC (...)
www.blue.xa.    RRSIG CNAME (...)
```

    Eftersom www.blue.xa har RRSIG och NSEC så är blue.xa en signerad zon. Eftersom det inte finns någon RRSIG för www.green.xa så betyder det att green.xa är en osignerad zon.

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)

- 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 ”labels”.

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. Du och ditt företag har fått tilldelat IP-blocket 10.13.27.0/24 från RIR N, och får nu en baklängeszon delegerat till era namnservrar enligt normala principer. RIR N:s zon täcker blocket 10.0.0.0/8.

    Avdelning AA inom ditt företag har egna namnservrar och ska förvalta en del av blocket, 10.13.27.8/30, både IP-mässigt och baklängesdata. Ni gör en intern delegering av baklängesdatat enligt CNAME-modellen till avdelning AA.

    Skriv ett sammanhängande svar. Det ska besvara frågorna och uppgifterna nedan. Det ska följa avgränsningarna nedan. Det ska följa förutsättningarna ovan. Det ska innehålla förklaringar som gör svaret begripligt. (7 p)

    - Frågor och uppgifter att besvara:
        a. Vilket namn har RIR N:s zon? Förklara också hur namnet har skapats.
        b. Vilket namn har den zon som ditt företag får delegerat från RIR N? Förklara också hur namnet har skapats.
        c. Lista den delegering som finns i RIR N:s zonfil av er zon.
        d. Lista de DNS-poster som ska finnas i företagets zonfil för att delegeringen av baklängesdatat till avdelning AA:s namnservrar ska fungera.
        e. Reversuppslagningen för 10.13.27.9 ska fungerar fullt ut. Lista den eller de DNS-poster som ska finnas i zonfilen hos AA som gör att uppslagningen kommer att fungera.
    - Avgränsningar:
        a. Skapa delegeringarna så att det inte behöver finnas några glueposter.
        b. Bortse från DNSSEC och förutsätt att övrig DNS är korrekt uppsatt.
        c. DNS-poster utanför de tre zonfilerna ska inte listas, t.ex. namn och IP-adresser på namnservrar.
        d. Utelämna TTL och klass i alla DNS-poster som listas.

    Zonen som RIR N har är "10.in-addr.arpa" vilket motsvarar 10.0.0.0/8. Alla reverszoner för IPv4 slutar på "in-addr.arpa" varje label före motsvarar en oktett i IPv4-adressen eller nätet. Oktetterna tas från vänster i IP-adressen och läggs i omvänd ordning i reversnamnet före "in-addr.arpa". Varje oktett är 8 bitar. I detta fall ska reverszonen bara täcka 8 bitar, d.v.s. en oktett.

    Zonen som är delegerad till företaget är "27.13.10.in-addr.arpa" vilket motsvarar 10.12.27.0/24. 24 bitar täcker de tre första oktetterna som läggs in före "in-addr.arpa", i omvänd ordning.

"27.13.10.in-addr.arpa" delegeras till namnservrar, vars namn normalt ligger under vanliga domännamn. Vi väljer här ns1.blue.xa och ns2.blue.xa (valfria namn):

```
27.13.10.in-addr.arpa.  NS  ns1.blue.xa.
27.13.10.in-addr.arpa.  NS  ns2.blue.xa.
```

Blocket 10.13.27.8/30 är IPv4-adresserna 10.13.27.8–10.13.27.11 (4 adresser). Det kan inte delegeras med en label som motsvarar en oktett. Istället lägger vi in ett specialnamn som vi delegerar till AA:s namnservrar och CNAME som pekar dit. Vi låter AA:s namnservrar heta ns1.aa.blue.xa och ns2.aa.blue.xa (valfria namn). Följande läggs in i zonen "27.13.10.in-addr.arpa":

```
8-11.27.13.10.in-addr.arpa. NS ns1.aa.blue.xa.
8-11.27.13.10.in-addr.arpa. NS ns2.aa.blue.xa.
8.27.13.10.in-addr.arpa.    CNAME 8.8-11.27.13.10.in-addr.arpa.
9.27.13.10.in-addr.arpa.    CNAME 9.8-11.27.13.10.in-addr.arpa.
10.27.13.10.in-addr.arpa.   CNAME 10.8-11.27.13.10.in-addr.arpa.
11.27.13.10.in-addr.arpa.   CNAME 11.8-11.27.13.10.in-addr.arpa.
```

Vi antar att ns1.aa.blue.xa har IP-adress 10.13.27.9 som vi ska skapa en revers för (kan vara annat namn). I zonfilen "8-11.27.13.10.in-addr.arpa" ska då följande DNS-post finnas:

```
9.8-11.27.13.10.in-addr.arpa.  PTR  ns1.aa.blue.xa.
```

Om vi frågar efter revers för 10.13.27.9 så finns det nu en obruten kedja som går till PTR-posten.

24. Zonerna dnskurs.xa och tenta.nod.dnskurs.xa finns. Noden nod.dnskurs.xa är en "empty non-terminal". Zonen dnskurs.xa har två namnservrar och NS-poster, vars namnservernamn ligger under dnskurs.se. Zonen tenta.nod.dnskurs.xa har tre namnservrar och NS-poster, varav exakt en kräver glue-post i delegeringen. Både www.dnskurs.xa och www.tenta.nod.dnskurs.xa finns som A-poster. (7 p)

    - Komponera båda zonerna (zonfilerna) med alla DNS-poster som krävs. Tag inte med några extra DNS-poster.

    Du ska utgå ifrån följande:

    - Namnservrar för zonerna ska endast ha IPv4, inte IPv6.
    - Ingen av zonerna ska vara DNSSEC-signerade.
    - Delegeringar ska matcha dotterzonens DNS-poster.
    - DNS-poster där värdena inte är specificerade i förutsättningarna ges lämpliga värden.
    - Zonerna ska konfigureras rätt och komplett.
    - Om RDATA för en DNS-post har fler än två delfält så kan RDATA förkortas till "(...)".

    Följande data kan väljas annorlunda eftersom de inte är specificerade eller fullt specificerade i förutsättningarna:

    - IP-adresser
    - Värden i SOA-poster
    - Namn på namnservrarna för dnskurs.xa och tenta.nod.dnskurs.xa.

```
$ORIGIN dnskurs.xa.
$TTL 3600
@                   SOA ns1 root (...)
                    NS   ns1.dnskurs.se.
                    NS   ns2.dnskurs.se.
tenta.nod           NS   ns1.labb.xa.
                    NS   ns2.labb.xa.
                    NS   ns1.tenta.nod
ns1.tenta.nod       A    192.0.2.210
www                 A    192.0.2.50


$ORIGIN tenta.nod.dnskurs.xa.
$TTL 3600
@                   SOA ns1 root (...)
                    NS   ns1.labb.xa.
                    NS   ns2.labb.xa.
                    NS   ns1
ns1                 A    192.0.2.210
www                 A    192.0.2.203
```