Internets domännamnssystem (DVGC28)

23 augusti 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: 3-5 från 29 till 58 poäng med intervaller om ungefär 10 poäng. U (underkänt) under 29 poäng.

---

1. Vad är ett NOTIFY-meddelande? (1 p)

   NOTIFY är ett DNS-meddelande som en masterserver skickar ut till slav-servrarna för en specifik zon om att zonfilen har uppdaterats (eller kan ha uppdaterats).

2. 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.

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

   Svaret är auktoritativ data.

4. Vad står IDN för? (1 p)

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

5. Hur används $ORIGIN i en zonfil? (1 p)

   $ORIGIN ställer in "default domain" i zonfilen som används för att "fylla på" relativa domännamn i zonen.

6. Vad betyder FQDN? (1 p)

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

7. Var i zonen finns SOA-posten och vilket "owner name" har den i förhållande till zonens namn? (1 p)

   SOA-posten finns längst upp i zonen (apex) och har samma "owner name" som zonens namn.

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. Vad innebär "cache poisoning"? (2 p)

   Felaktig data skjuts in med ont syfte i en resolvers cache med syftet att den som ställer en fråga ska få felaktigt data som leder till "ond" kopia av tjänsten eller blockerad tjänst.

10. Ett svarspaket har tom ”answer section” och status NXDOMAIN. (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)

11. 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.

12. Det finns en speciell posttyp för email. Vilken är den och hur används den? (2 p)
    - Beskriv hur posttypen används och fungerar.
    - Illustrera med ett exempel som skulle kunna gälla för mailadressen info@namn.se.
    - Det ska finnas två DNS-poster med den posttypen i ditt exempel.

    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. Lägsta värde har högst prioritet

    ```
    namn.se.   MX   10 mail.namn.se.
    namn.se.   MX   20 mail-sec.namn.se.
    ```

13. Ett svarspaket kan innehålla statuskoden REFUSED. Beskriv två *vanliga* scenarier när detta inträffar. (2 p)

    1. Namnservern har inte zonen som det efterfrågade namnet skulle ingå eller delegeras från.

    2. Namnservern tillåter inte frågor från den IP-adress som klienten har.

    (Full poäng även om man inte nämner ”delegerad från”. *Ett* korrekt scenario kan ge 1 p.)

14. 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. Lasten på resolvern och svarstiden minskar. Ändringar i zonen slår inte igenom så länge svaret kommer från cache.

    (Om man missar att cachning kan försena uppdatering, men resten är rätt, så kan man få 1,5 p)

15. 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

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. 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 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". 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. Vad innebär det att ett svar är auktoritativt och hur kan man se att ett svarspaket är auktoritativt? (3 p)

    Auktoritativt svar innebär att den svarande namnservern har DNS-datat laddat från en zonfil (är master eller slav för zonen).

    I svarspaketet ser man det genom att AA-flaggan är satt.

20. 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 ”-”.

    Olika kodning av samma label och kan konverteras mellan ger 1,5 poäng. Rätt på format på U- resp A-label ger 0,5 poäng vardera. Allt rätt ger 3 poäng.

21. En delegering innehåller ibland glue-poster. (4 p)

- Redogör för när det måste finnas glue, när det kan finnas glue (men inte nödvändigt) och när det inte får finnas glue.
- Illustrera de tre fallen med exempel, med DNS-poster, med beskrivning.
- Det ska också framgå i vilken zon som DNS-posterna finns i för varje exempel.

Glue-poster är adressposter (A eller AAAA) för namnservernamnen i NS-posterna i en delegering. Glue-posterna tillhör den delegerande zonen, moderzonen.

Det som avgör om glue-posten är nödvändig är namnservernamnets förhållande till det delegerade namnet. Om namnservernamnet ligger på eller under det delegerade namnet så är glue-posterna nödvändiga. Exempel:

```
tenta.xa. NS ns1.tenta.xa.
tenta.xa. NS tenta.xa.
```

Första NS-posten har ett namnservernamn under delegeringspunkten (tenta.xa), och den andra en NS-post på delegeringspunkten (tenta.xa). I båda fallen så måste NS-posterna kompletteras med glue-poster (adressposter).

I nästa exempel så antar vi att delegeringen görs från zonen xa:

```
tenta.xa. NS ns1.skrivning.xa.
tenta.xa. NS ns2.kurs.xa.
```

I båda NS-posterna så är det namnservernamn som ligger inom xa-zonen eller inom en dotterzon till xa-zone, men utanför den delegerade zonen (tenta.xa). I detta fall är det möjligt men inte nödvändigt med glue-poster.

I tredje exemplet så antar vi fortfarande att delegeringen görs från zonen xa:

```
tenta.xa. NS  ns1.dns.xb.
tenta.xa. NS ns2.dns.xb.
```

I detta fall så är namnservernamnen inte under xa-zonen, utan sidoordnat xa. Då kan glue-poster inte inkluderas.

1 poäng per rätt beskrivet fall med korrekt exempel. 2 poäng för tre korrekt beskrivna fall utan exempel. 2 poäng för tre korrekta exempel utan beskrivning. 4 poäng om allt är rätt.

22. Utgå ifrån namnet ”www.kth.se” och posttypen A, som finns. Tänk dig att du ställer en DNS-fråga efter det namnet med den posttypen till olika renodlade DNS-hostingservrar på det publika Internet. Beskriv de tre kategorier av servrar som du normalt kommer att stöta på, i förhållande till just denna fråga. Låt beskrivningen utgå ifrån status och vilka DNS-poster som finns, inte finns eller kan finnas med i de olika ”sections” i svarspaketet. Utgå ifrån att servrarna är modernt och korrekt konfigurerade. Bortse ifrån EDNS, klass och TTL. (4 p)

    Alla svarspaket kommer att ha samma innehåll i ”question section”, vilket är kopierat från frågepaketet, ”www.kth.se. A”.

    Kategori 1. Servern har varken kth.se-, se- eller rotzonen. Status i svarspaketet är REFUSED. Förutom ”question section” så innehåller svarspaketet inga DNS-poster.

    Kategori 2. Servern har kth.se-zonen. Status i svarspaketet är NOERROR. ”Answer section” innehåller svaret i form av ”www.kth.se. A x.x.x.x”. ”Authority section” kan innehålla NS-posterna för kth.se-zonen och i så fall kan ”additional section” innehålla A- eller AAAA-poster för namnservernanen från NS-posterna.

    Kategori 3. Servern har se- eller rotzonen (men inte kth.se-zonen). Status är NOERROR. ”Answer section” är tom. ”Authority section” innehåller NS-poster för se-zonen (från rotnamnserver) eller för kht.se-zonen (från .se-server). ”Additional section” innehåller A- eller AAAA-poster om glue-poster är nödvändiga. Ifall glue-poster inte behövs så kan ”additional section” vara tom.

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, 10.13.27.8/29, 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 10.13.27.11 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 10.13.27.8/29 är IPv4-adresserna 10.13.27.8–10.13.27.15 (8 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":

```
8-15.27.13.10.in-addr.arpa. NS ns1.aa.blue.xa.
8-15.27.13.10.in-addr.arpa. NS ns2.aa.blue.xa.
8.27.13.10.in-addr.arpa.    CNAME 8.8-15.27.13.10.in-addr.arpa.
9.27.13.10.in-addr.arpa.    CNAME 9.8-15.27.13.10.in-addr.arpa.
10.27.13.10.in-addr.arpa.   CNAME 10.8-15.27.13.10.in-addr.arpa.
11.27.13.10.in-addr.arpa.   CNAME 11.8-15.27.13.10.in-addr.arpa.
12.27.13.10.in-addr.arpa.   CNAME 12.8-15.27.13.10.in-addr.arpa.
13.27.13.10.in-addr.arpa.   CNAME 13.8-15.27.13.10.in-addr.arpa.
14.27.13.10.in-addr.arpa.   CNAME 14.8-15.27.13.10.in-addr.arpa.
15.27.13.10.in-addr.arpa.   CNAME 15.8-15.27.13.10.in-addr.arpa.
```

Vi antar att ns1.aa.blue.xa har IP-adress 10.13.27.11 som vi ska skapa en revers för (kan vara annat namn). I zonfilen "8-15.27.13.10.in-addr.arpa" ska då följande DNS-post finnas:

```
11.8-15.27.13.10.in-addr.arpa.  PTR  ns1.aa.blue.xa.
```

Om vi frågar efter revers för 10.13.27.11 så finns det nu en obruten kedja som går till PTR-posten.

24. Vilka DNS-poster tillkommer i en DNSSEC-signerad zon jämfört med en osignerad? Komplettera zonen nedan med dessa DNS-poster och förklara vad de har för funktion. (7 p)

    - Kopiera zonen nedan och uppdatera den med DNSSEC-posterna. Det ska vara rätt ”owner name” och posttyp.
    - Detaljerna i RDATA för de nya posterna behöver inte finnas med utan kan anges som ”(…)”.
    - Beskriva RDATA för DNSSEC-posterna.
    - Förklara vad de nya DNS-posterna har för funktion i den signerade zonen och hur de är kopplade till de befintliga posterna och andra nya poster.
    - Dina beskrivningar och kommentarer kan läggas som zonfilskommentarer direkt efter posterna som du ska kommentera. Inled då kommentaren med ”;”.
    - Din uppdaterade zonfil ska vara en giltig zonfil förutom RDATA för DNSSEC-posterna.

```
$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.
                        MX          1 mail
mail                    A           130.237.28.40
```

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

```
$ORIGIN exempel.se.
$TTL 3600
@                       SOA ns1.example.com. root.telia.se. (
                                    2019030909
                                    14400
                                    900
                                    604800
                                    3600
                                    )
                        RRSIG       (…) ; På SOA RRSET
                        NS          ns1.example.com.
                        NS          ns2.example.com.
                        RRSIG       (…) ; På NS RRSET
                        DNSKEY      (…) ; KSK
                        DNSKEY      (…) ; ZSK
                        RRSIG       (…) ; På DNSKEY RRSET
                        MX          1 mail
                        RRSIG       (…) ; På MX RRSET
                        NSEC        (…) ;
                        RRSIG       (…) ; På NSEC RRSET
mail                    A           130.237.28.40
                        RRSIG       (…) ; På mail/A RRSET
                        NSEC        (…) ;
                        RRSIG       (…) ; På mail/NSEC RRSET
```

DNSKEY innehåller de publika DNSSEC-nycklarna för zonen i RDATA och gör det möjligt att validera DNS-posterna via RRSIG.

RRSIG skapas för varje RRSET inkl de nya (exkl sig själv) och gör det möjligt att validera RRSET via DNSKEY.

NSEC läggs till i varje namn (”owner name”) i zonen. I detta fall en NSEC-post med owner name **exempel.se.** och en med owner name **mail.exempel.se.**

RDATA för NSEC har dels namnet på nästa namn, dels en lista över alla posttyper med samma ”owner name” som NSEC-posten.