Internets domännamnssystem (DVGC28)

4 juni 2025

Hjälpmedel:	Inga.
Observera:	Lösningarna måste vara skrivna med läsbar handstil. Ange namn och personnummer på varje sida. Maximalt 58 poäng kan uppnås. Betygsgränser: • 0-28 poäng: U (underkänt) • 29-38 poäng: 3 • 39-48 poäng: 4 • 49-58 poäng: 5

---

1. Vad är ett RRset? (1 p)

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

2. 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).

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

   ANY, AXFR, IXFR (en räcker)

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

   Port 53.

5. 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.

6. 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.

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. Vad är det för typ av "label" som är andra från vänster i följande domännamn? Vad signalerar "xn--"? (1 p)

   - www.xn--rvc1e0am3e.xa

   Det är en IDN-label av typen A-label. "xn--" signalerar att det är en A-label.

9. En klient skickar en DNS-fråga med *www.iis.se* som "query name" till sin resolver. (2 p)

   - Vad blir skillnaden om resolvern följer normal process eller QNAME Minimisation ("query name mininisation") när det gäller ”query name” när resolvern sedan ställer frågan till en rotnamnserver?
   - Vad blir ”query name” till rotnamnservern om "QNAME mininisation" följs?
   - Hur påverkas "query type" av "QNAME minimisation"?

   Normal är QNAME (”query name”) hela ”www.iis.se”, men med QNAME Minimisation så blir det istället bara ”se”. Normalt är QTYPE ("query type") samma som ursprungsfrågan, men med QNAME minimisation så används en fast QTYPE, oftast A, fram till sista frågan, då ursprunglig QTYPE används.

10. Vad innebär frågetyp ANY? Vad förväntas svarsposten innehålla? Kommer svaret att innehålla en ANY-post? (2 p)

    Frågetypen ANY betyder att DNS-klienten (t.ex. "dig") frågar efter alla DNS-poster oavsett posttyp med det "owner name" som anges i frågan. Svaret förväntas innehålla alla dessa i "answer section". ANY är ingen posttyp så någon ANY-post kan inte finnas.

11. 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.

12. Vilka begränsningar gäller för tecknen i ett domännamn av typen ”hostname”? (2 p)

    Endast ”a-z”, ”A-Z”, “0-9” och “-“ får användas i en ”label” i ett ”hostname”. ”-” får varken inleda eller avsluta en ”label”. Mellan ”labels” används ”.” Tecknen ”A-Z” hanteras som identiska med ”a-z”.

13. 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.]

14. 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. (2 p)

    - Vilka likheter och skillnader kommer det att bli när det gäller flaggor och DNS-poster i svarspaketen?

    När DO-flaggan inte är satt i förfrågan, 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 i detta fall.]

15. Zon och domännamn. (2 p)

    - Vad är skillnaden mellan en zon och ett domännamn?
    - Hur förhåller sig zon och domännamn till domännamnsträdet?

    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. 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.)

17. TSIG kan användas för att styra möjlighet till zonöverföringar. (4 p)

- Beskriv hur TSIG används i sådant fall.
- Ge en övergripande beskrivning av hur konfigurationen görs i master- resp. slavserver.
- Ge exempel på en fördel att använda TSIG jämfört med med stryrning med "source IP".
- Hur skyddar TSIG mot insyn i zonöverföringen? Förklara

TSIG kan användas för att kontrollera vilka slavservrar som får hämta zonen med zonöverföring. Endast slavar som har den specifika TSIG-nyckeln kommer då att accepteras för zonöverföring.

TSIG-nyckeln läggs in i både masterserverns och slavserverns konfiguration (named.conf) som en delad hemlighet. I masterservern anges att den specifikat TSIG-nyckeln är ett krav för att få zonen med zonöverföring. I slavservern anges att alla anrop till den specifika masterservern ska signeras med den specifika TSIG-nyckeln.

En fördel är att slavservern kan byta IP-adress utan att masterservern behöver konfigureras om jämfört med om restriktion baseras på slavens IP-adress.

En annan fördel är att slavservern får en verifikation på att zonen är komplett och omodifierad när den kommer fram.

TSIG skyddar inte alls mot insyn eftersom zoninnehållet går i klartext. TSIG ger bara en signering av datat.

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. Ange fyra posttyper med någon sådan begränsning och gör en fullständig beskrivning av respektive posttyps begränsningar. (4 p)

    Fyra 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. 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.

20. 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.

21. DS och DNSKEY. (4 p)

    - Hur förhåller sig DS till DNSKEY?
    - Hur bidrar DS-posten till tillitskedjan ("chain of trust")?
    - I vilken zon finns DS respektive DNSKEY?
    - Hur förhåller sig normalt begreppen KSK och ZSK till DNSKEY som förhåller sig till DS-post?
    - Var i zonen finns respektive post?

    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).

    Den DNSKEY som DS pekar på har normalt rollen KSK ifall det finns både KSK och ZSK i zonen.

22. 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.

    Ert vanliga domännamn är tenta.xa. Använd det för namn som krävs, men som inte ges av förutsättningarna.

    Avdelning AA inom ditt företag har egna namnservrar och ska förvalta en del av blocket, 10.13.27.8/30 (d.v.s. 10.13.27.8-10.13.27.11), 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 antas fungerar korrekt. Lista den eller de DNS-poster som kommer att finnas i svaret i "answer section" från en resolver när man har frågat efter reversuppslagningen för 10.13.27.9.
    - Avgränsningar:
        a. Skapa delegeringarna så att det inte behöver finnas några glue-poster.
        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.

    Delfråga a:

    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.

Delfråga b:

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.

Delfråga c:

"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.
```

Delfråga d:

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.
```

Delfråga e:

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:

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

23. 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. (
                                2019030909060308
                                4400
                                900
                                604800
                                3600
                                )
                        NS          ns1.exempel.xa.
                        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                     CNAME       nameserver
nameserver              A           130.237.72.250
ns2                     A           129.16.253.356
intrawww                CNAME       intra.exempel.xa.
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. 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”.

2. 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".

3. ”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.”.

4. 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”.

5. ”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.

6. ”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.

7. "#" är inte ett kommentarstecken i en zonfil. Ersätt det med ";".