Internets domännamnssystem (HI1037)

11 mars 2026

Hjälpmedel:	Inga.
Observera:	Lösningarna måste vara skrivna med läsbar handstil. Ange namn och personnummer på varje sida. Maximalt 58 poäng kan uppnås. Betygsgränser: • 0-26 poäng: F (underkänt) • 27-28 poäng: Fx • 29-34 poäng: E • 35-38 poäng: D • 39-44 poäng: C • 45-50 poäng: B • 51-58 poäng: A

---

1. Vad är zonöverföring? (1 p)

   Zonöverföring är kopiering av zonfilen från masterserver till slavserver med DNS-protokollet. (Eller mera generellt, kopiering med DNS-protokollet av en zon från en auktoritativ namnserver till en klient.)

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

   ANY, AXFR, IXFR (en räcker)

3. Beskriv formatet för RDATA för posttyp A som det presenteras av t.ex. programmet "dig", och ge ett exempel. (1 p)

   RDATA för A-post är en IPv4-adress skrivet med fyra decimala oktetter med punkt mellan, t.ex. 192.0.2.190.

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

   Klienten ber servern om rekursiv uppslagning.

5. Ge två exempel på ccTLD:er. (1 p)

   .SE, .DK, .DE, .FR, .NU, .FI… (två räcker).

6. Vad står IDN för? (1 p)

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

7. Vad betyder FQDN? (1 p)

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

8. I en DNSSEC-signerad zon utan delegeringar, vilka RRset är signerade med RRsig? (1 p)

   Alla.

9. Trots att DNS-trädet i grunden är publikt och gemensamt så finns det många fall av intern och extern vy av DNS-data. Om privata adresser används på ett nätverkt, förklara varför det kan vara nödvändigt med intern och extern vy, speciellt när det gäller revers. Beskriv schematiskt hur man skulle göra med reversen. (2 p)

   Om samma tjänst (med samma domännamn) ska vara åtkomlig via privat IP-adress (t.ex. ur 10.0.0.0/8) internt, men via publik IP-adress externt så måste namnet ge olika upplösning internt och externt. Revers av privata IP-adresser, t.ex. 10.0.0.0/8 finns inte på det publika Internet och kan inte finnas där. Skapa en reverszon för det privata nätet, t.ex. för 10.0.0.0/8 och lägg i en namnserver som kan hosta zoner (förslagsvis gör zonen bara åtkomlig internt). Se till att den lokala resolvern skickar reversfrågor om de relevanta privata IP-adresserna till den servern.

10. För DANE-protokollet används TLSA-poster som en möjlighet att säkra kommunikationen till tjänster som använder TLS. Hur bidrar TLSA-poster till säkerheten för TLS-kommunikationen och hur förhåller sig DANE till DNSSEC? (2 p)

    TLSA-posten kopplad till tjänsten har RDATA som gör det möjligt att verifiera att det certifikat som TLS-tjänsten skickar vid uppkoppling. En förutsättning för att en klient med DANE-stöd ska använda informationen i TLSA-posten är att den korrekt signerad med DNSSEC.

11. Vad är det för typ av "label" som är andra från vänster i domännamnet under frågan? Den typen av "label" förekommer i två former. Vilken form är det i detta fall? Förklara hur du kom fram till svaret. Vad heter den andra formen? (2 p)

    - www.malmö.se

    Det är en IDN-label i formen U-label. Att den bara innehåller tecken som är tillåtna av IDN, och att en bokstaväverna ligger utanför ASCII visar att det är en U-label och IDN-label. Den andra formen heter A-label.

12. 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 ställer frågorna till en namnserverarna?
    - 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 kommer QNAME att kortas ner till det nödvändiga för att få hänvisningar till nästa zon med dess namnservrar.

    I detta fall 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.

13. 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.

14. Det finns två tidsvärden i SOA-posten som styr zonöverföring. Beskriv deras roll för zonöverföringen. (2 p)

    ”SOA refresh” specificerar hur ofta slavservern ska kontrollera om zonöverföring är nödvändig. ”SOA retry” specificerar hur ofta slavservern ska försöka igen om kontrollen eller zonöverföringen misslyckades.

15. 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.

16. Delegering är ett viktigt begrepp i DNS. Vilken information finns i den delegerande zonen för att skapa en delegering? Tänk på olika scenarior. Ge ett exempel där det framgår i vilken zon som är den delegerande och där posterna kommenteras. Exemplet kan vara fiktivt. (2 p)

    I den delegerande zonen (moderzonen) så finns det i noden (domänen) som delegeras en eller flera NS-poster som pekar ut namnen på namnservrarna för den delegerade zonen (dotterzonen). Om det krävs så finns det glue-poster (A/AAAA) i den delegerande zonen som komplement till NS-posterna. [Glue-posterna behöver bara finnas för NS (RDATA) som tillhör den delegerade zonen.]

    I zonen dnskurs.xa lägger vi in följande DNS-poster för att delegera ut zonen student13.kth.dnskurs.xa:

    ```
    student13.kth.dnskurs.xa.      NS   ns1.dnskurs.xb.
    student13.kth.dnskurs.xa.      NS   ns1.student13.kth.dnskurs.xa.
    ns1.student13.kth.dnskurs.xa.  A    192.0.2.53
    ns1.student13.kth.dnskurs.xa.  AAAA 2001:db8::53
    ```

    Den andra NS-postens namn (i RDATA) tillhör en delegerade zonen så det måste finnas glue-poster, A- och AAAA-posterna. Den första NS-postens namn (i RDATA) tillåter inte glue-poster.

17. Traditionellt skickas DNS-meddelanden direkt på UDP eller TCP, standardiserat i RFC 1035. Det finns tre nya standardiserade transportsätt för DNS-frågor. (4 p)

    1. Vad kallas de nya transportsätten? Det räcker med förkortningen för dem.
    2. För varje transportsätt, vilket eller vilka protokoll, mellan IP och DNS-meddelande, använder transportsättet?

    Det finns tre nya transportsätten är:

    - DoT (DNS over TLS) som går ovanpå TLS ovanpå TCP.
    - DoH (DNS over HTTPS) som går ovanpå HTTP ovanpå TLS ovanpå TCP.
    - DoQ (DNS over QUIC) som går ovanpå HTTP ovanpå TLS ovanpå UDP.

18. En DNSSEC-signerad zon måste innehålla vissa DNS-poster som inte används i en osignerad zon. Det är flera posttyper som tillkommer, och det gäller här bara de som **måste** tillkomma. (4 p)

    - Det finns två alternativa och delvis överlappande listor med posttyper. Svara med de två listorna som delsvar.
    - Hur förhåller sig de två alternativen till "zone walking"? Utgå ifrån zoner som är signerade med "offline signing" (signerad i förväg).

    Alternativ 1: DNSKEY, NSEC och RRSIG.

    Alternativ 2: DNSKEY, NSEC3, NSEC3PRAM och RRSIG.

    Zoner signerade med NSEC kan hämtas med "zone walking" men det går inte med zoner signerade med NSEC3.

19. 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".
- Skyddar TSIG mot insyn i zonöverföringen? Motivera ditt svar.

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.

20. 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).

21. DS och DNSKEY. (4 p)

- Hur förhåller sig DS till DNSKEY?
- Hur bidrar DS-posten till tillitskedjan ("chain of trust")?
- I vilken zon och var i zonen finns DNSKEY-posten eller -posterna?
- I vilken zon och var i zonen finns DS-posten eller -posterna?
- Hur förhåller sig normalt begreppen KSK och ZSK till DNSKEY resp. DS?

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. I de fallet används KSK för att signera DNSKEY RRset. DNSKEY med rollen ZSK används för att signera alla RRset i zonen, möjligen med undantag för DNSKEY RRset. (Det är den privata nyckeln, inte själva DNSKEY som signerar.)

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

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

    Avdelning Rosor 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 Rosor.

    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:ens zon? Förklara också hur namnet har skapats.
        b. Vilket namn har den zon som ditt företag får delegerat från RIR:en? Förklara också hur namnet har skapats.
        c. Lista den delegering som finns i RIR:ens zonfil av er zon.
        d. Lista de DNS-poster som ska finnas i företagets zonfil för att delegeringen av baklängesdatat till avdelning Rosors 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:en 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 Rosors namnservrar och CNAME som pekar dit. Vi låter Rosors namnservrar heta ns1.rosor.blue.xa och ns2.rosor.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.rosor.blue.xa.
8-11.27.13.10.in-addr.arpa. NS ns2.rosor.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.rosor.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.rosor.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.rosor.blue.xa.
```

23. Vi har ställt en DNS-fråga med "dig" till en auktoritativ namnserver för wildcard.xa och har fått svaret ("response") enligt nedan. Lista de DNS-poster som måste finnas i zonen wildcard.xa. Utgå ifrån de DNS-poster som måste finnas i en zonfil av denna typ, och ifrån DNS-svaret nedan. (7 p)

    - Zonen antas vara korrekt uppsatt och servern antas svara korrekt.
    - Klass behöver inte anges och TTL antas vara samma för alla poster.
    - När exakt RDATA för en DNS-post inte är känd så kan RDATA anges som "(...)".
    - När det gäller signaturer så ska det alltid framgå vilket RRset som signaturen avser.
    - Inkludera inga DNS-poster som inte måste finnas enligt materialet.

```
; <<>> DiG 9.16.25 <<>> @localhost web.wildcard.xa +dns +mult
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39838
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1300
; COOKIE: ce01d77c3a82fa9b01000000621611ba1353614ddc9165af (good)
;; QUESTION SECTION:
;web.wildcard.xa.         IN A

;; ANSWER SECTION:
web.wildcard.xa.          3600 IN A 192.0.2.30
web.wildcard.xa.          3600 IN RRSIG A 13 2 3600 (
                                   20220307185732 20220223095041 51609
                                   wildcard.xa.
                                   NeaC9+IdGDhvdwhqCCM+5JV
                                   FXnW4E9YdwtDFUcDWQmAu
                                   pn9vtIxLMRNLzSDTMBs+uTF
                                   h6rYzyLoOR+LmJrDueA== )

;; AUTHORITY SECTION:
*.wildcard.xa.            3600 IN NSEC wildcard.xa. A RRSIG NSEC
*.wildcard.xa.            3600 IN RRSIG NSEC 13 2 3600 (
                                   20220307185732 20220223095041 51609
                                   wildcard.xa.
                                   axJuhricGBqzhgjeGeK3j4i
                                   ZV8qVNb0sxoJdzYy788WR
                                   cLo2RmTN7IwSVcJxb3Fnw+a
                                   7FJAp4zKcX11nJTxSJA== )

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
;; WHEN: Wed Feb 23 11:51:38 CET 2022
;; MSG SIZE  rcvd: 341
```

Följande DNS-poster finns i zonen:

```
$TTL 3600
$ORIGIN wildcard.xa.
@        SOA         (...)
         RRSIG       (...) ; För SOA RRset
```

```
            NS          (...)
            RRSIG       (...) ; För NS RRset
            DNSKEY      (...)
            RRSIG       (...) ; För DNSKEY RRset
            NSEC        (...)
            RRSIG       (...) ; För NSEC RRset
*           A           192.0.2.30
            RRSIG       A 13 2 3600 (
                        20220307185732 20220223095041 51609
                        wildcard.xa.
                        NeaC9+IdGDhvdwhqCCM+5JV
                        FXnW4E9YdwtDFUcDWQmAu
                        pn9vtIxLMRNLzSDTMBs+uT
                        Fh6rYzyLoOR+LmJrDueA== )
            NSEC        wildcard.xa. A RRSIG NSEC
            RRSIG       NSEC 13 2 300 (
                        20220307185732 20220223095041 51609
                        wildcard.xa.
                        axJuhricGBqzhgjeGeK3j
                        4iZV8qVNb0sxoJdzYy788WR
                        cLo2RmTN7IwSVcJxb3Fnw+
                        a7FJAp4zKcX11nJTxSJA== )
```

Utifrån förutsättningarna så kan vi inte identifiera några ytterligare DNS-poster, men det kan finnas fler.