Internets domännamnssystem (DVGC28)

31 maj 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 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. 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.

4. 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.

5. Vilken teckenuppsättning baseras IDN-namn på? (1 p)

   Unicode.

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

   Klienten ber servern om rekursiv uppslagning.

7. 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.

8. Vad är en ccTLD? (1 p)

   Landstoppdomän.

   (Om man svarar ”toppdomän”, men ger exempel med en ccTLD så kan det ge 0,5 p)

9. 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.

10. 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”.

11. En förfrågan om kth.se skickas till en namnserver som inte är DNS-resolver. Namnservern svarar med REFUSED. Vad är den troliga orsaken? (2 p)

    Namnservern har inte zonen exempel.se, och dessutom varken se-zonen eller rotzonen. (1p om svaret bara nämner kth.se.)

12. 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)

13. Utgå ifrån en viss IPv4-adress och tänk dig att du använder programmet ”dig” med växeln ”-x”. Ange vilken IP-adress du har valt. Visa hur ”question section” kommer att se ut i det DNS-paketet som ”dig” skickar. Beskriv hur DNS-namnet (”owner name”) i ”question section” skapas från IP-adressen. (2 p)

    Vald IP-adress: 130.237.28.40

    ”Question section”:

    ```
    40.28.237.130.in-addr.arpa.  IN  PTR
    ```

    [IP-adressen normaliseras så att den representeras av fyra decimala oktetter utan extra inledande nollor.] DNS-namnet (”owner name”) skapas genom att IPv4-adressens oktetter sätts i omvänd ordning med punkt mellan och sedan får suffixet ”.in-addr.arpa.”

14. 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.)

15. 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.

16. DNSKEY används för att verifiera en signerad zon. Vilken posttyp används för att verifiera att det är rätt DNSKEY-post som resolvern har fått? Översiktligt, vad innehåller RDATA för en sådan DNS-post? Var återfinns en DNS-post av den posttypen? (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.

17. Vilka begränsningar gäller för antalet CNAME-poster i en nod och hur CNAME-poster får kombineras med andra DNS-poster i en DNSSEC-signerad zon? (3 p)

    En CNAME-post är alltid ensam i sitt RRset. En CNAME-post kan inte kombineras med någon annan DNS-post än RRSIG och NSEC.

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. Hur skapar man en delegering av en dotterzon från en moderzon? Ge ett sammanhängande svar och illustrera med ett kommenterat exempel. (4 p)

    - Vilka DNS-poster måste läggas in i moderzonen?
    - Vilka DNS-poster kan läggas in?
    - Vad är det som pekas ut med delegeringen?
    - Vad förväntas finnas i dotterzonen som relaterar till delegeringen?

    En eller flera NS-poster med samma ”owner name” infogas i zonfilen. NS-posternas ”owner name” ska vara en subdomän till zonfilens apex. Namnen (namnservrarna) som pekas ut ska vara uppslagbara i DNS (A eller AAAA). Om något namn (namnserver) tillhör den utdelegerade zonen så måste glue-poster (A eller AAAA) tillfogas.

    I se-zonen:

```
exempel.se.       NS   ns1.exempel.se.
exempel.se.       NS   ns2.exempel.se.
exempel.se.       NS   dns.example.com.
ns1.exempel.se.   A    192.0.2.5
ns1.exemple.se.   AAAA 2001:DB8:A::5
ns2.exempel.se.   A    203.0.113.10
ns2.exemple.se.   AAAA 2001:DB8:B::A
```

    De två fösta NS måste ha motsvarande glue-poster eftersom namnen ligger under den delegeringspunkten. Den tredje kan inte ha glue-post eftersom den ligger helt utanför .se.

    I dotterzonen (exempel.se) så ska samma NS poster läggas in. Ev. glue-poster, som i exemplet, ska läggas in som A- och AAAA-posterna i dotterzonen.

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 ”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. 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
```

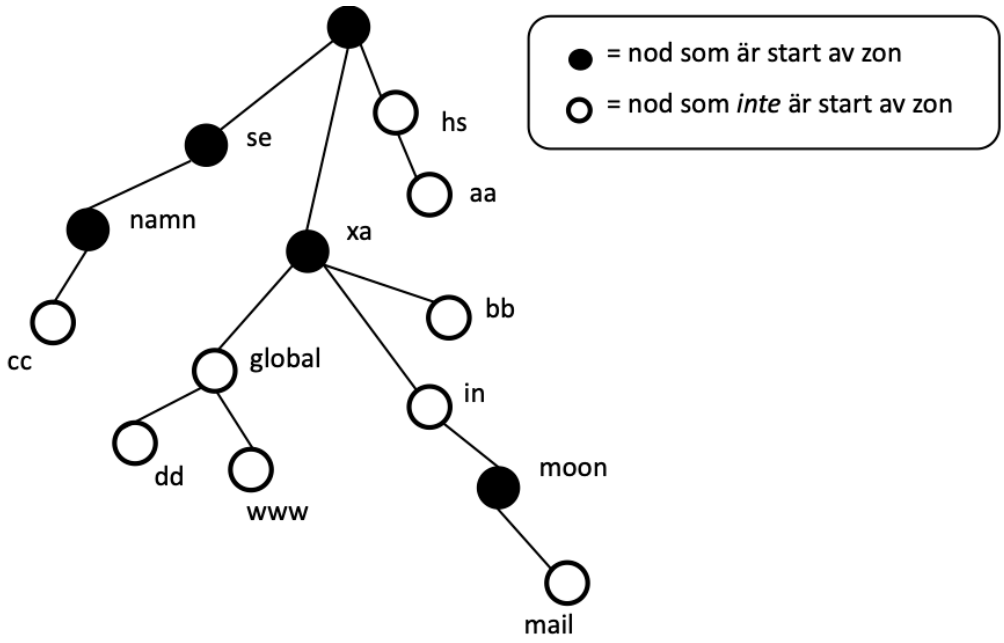
```
            NS          (...)
            RRSIG       (...) ; För NS RRset
            DNSKEY      (...)
            RRSIG       (...) ; För DNSKEY RRset
            NSEC        (...)
            RRSIG       (...) ; För NSEC RRset
*           A           192.0.2.30
            RRSIG       A 13 2 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.

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. IP-adresserna som användas ska plockas valfritt inom 192.0.2.0/24.

    Lista de auktoritativa DNS-poster som måste finnas för att det ska vara korrekt och för att trädet ska skapas. (7 p)

    - 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.
    - Uppsättningen ska vara minimal, men fortfarande korrekt och komplett.
    - Det finns olika korrekta lösningar, men använd exakt 16 DNS-poster för att lösa uppgiften, varken fler eller färre.
    - Alla namn ska vara absoluta.
    - 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”
```