Internets domännamnssystem (HI1037)

14 mars 2022

Hjälpmedel:	Inga.
Observera:	Lösningarna måste lämnas direkt i Canvas eller vara skrivna med läsbar handstil. Ange namn och personnummer på varje sida (om svar på papper). Maximalt 58 poäng kan uppnås. Preliminära betygsgränser: A-E från 29 till 58 poäng med intervaller om ungefär 6 poäng. F (underkänt) under 29 poäng.

---

1. Beskriv 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.

2. En förfrågan om example.se skickas till en internetoperatörs DNS-resolver, som svarar med REFUSED. Vad är den troliga orsaken? (1 p)

   Klienten sitter inte på ett IP-nät som DNS-resolvern accepterar att svara på frågor från.

3. 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.

4. 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.

5. Hur kan man använda DNS för en enkel lastbalansering? (1 p)

   Låta samma domännamn peka på två (eller flera) IP-adresser [av samma protokoll (IPv4/IPv6)] till olika servrar som tillhandahåller samma tjänst.

6. En klient skickar en DNS-fråga om ”www.exempel.se” till en rotnamnserver. Vad blir skillnaden om klienten följer normal process eller "query name minimisation" när det gäller ”query name”? (1 p)

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

7. Vad är en ccTLD? (1 p)

   Landstoppdomän.

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

8. Hur används QR-flaggan, d.v.s. när är den satt och när är den inte satt? (1 p)

   QR-flaggan är satt i ett svarspaket (”response”). I frågepaket (”query”) är den inte satt.

9. Vad är en ”stub resolver” och vad har den för funktion för resolvning? (2 p)

   En ”stub resolver” är programbiblioteksrutiner som används av en vanlig applikation (ett vanligt program) för DNS-uppslagning. Det är ”stub resolver” som sedan skickar DNS-frågan enligt DNS-protokollet till en DNS-resolver. Oftast är ”stub resolver” gemensamma biblioteksrutiner för alla applikationer i ett operativsystem.

10. 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 masterserver och sedan vara master gentemot andra slavar.]

11. Delegering är ett viktigt begrepp i DNS. Vilken information finns i den delegerande zonen för att skapa delegering? (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.]

12. Ett svarspaket har tom ”answer section” och status NXDOMAIN. (2 p)

    a) Vad förväntas finnas i ”authority section”?

    b) Vad används informationen i ”authority section” till?

    a) SOA-post. (1 p)

    b) Fastställa cachetiden för det negativa svaret. (1 p)

13. 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)

14. Om du vill göra en baklängesuppslagning av en viss IPv4-adress, hur kommer då frågan se ut i frågesektionen av DNS-paketet? Välj en IP-adress att utgå ifrån. Du ska både beskriva DNS-frågan och dess delar, samt ge ett exempel. (2 p)

    Exempel på baklängesuppslagning av 130.237.28.40:

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

    - Owner name skapas genom att IPv4-adressens oktetter sätts i omvänd ordning och sedan får suffixet ”.in-addr.arpa.”
    - Klassen är alltid ”IN”.
    - Frågetypen (vilket i detta fall är posttypen vi frågar efter) är alltid ”PTR”.

    Korrekt exempel ger 0,5 poäng, korrekta beskrivningar ger ytterligare 1,5 poäng.

15. 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.)

16. Vad innebär begreppen "dold master"? Vilka fördelar finns det med att använda en dold master? (2 p)

    "Dold master" betyder att masterservern varken finns med som NS-post (i zonen eller i delegeringen) eller som SOA MNAME.

Genom att den inte är avsedd för publika frågor så kan accessen till den begränsas, och därmed skydda den från attacker.

Full poäng även om SOA MNAME inte nämns.

17. Serienumret (”SOA serial”) är ett 32-bitars positivt heltal (har ett värde mellan 0 och 4.294.967.295). Beskriv hur jämförelse görs mellan olika serienummer, d.v.s. vad som räknas som högst och lägst när två serienummer jämförs. (3 p)

    Serienumren är som en klocka där 0 är kl 12 och talet efter första fjärdedelen kl 3 o.s.v. När två serienummer jämförs så finns det två vägar, medurs och moturs. Om moturs är den kortaste vägen från första till andra serienumret så är det en minskning. Om medurs är den kortaste vägen så är det en ökning.

18. EDNS är en utökning av DNS-protokollet. Beskriv hur EDNS fungerar och vad det tillför enligt följande punkter. (3 p)
    a) Vad är det för posttyp som används för EDNS-informationen?
    b) Var i DNS-paketet transporteras EDNS-informationen?
    c) Hur kan man se med ”dig” om DNS-paketet är utökat med EDNS eller inte?
    d) Ge ett exempel på information som kan signaleras med hjälp av EDNS.

    a. Posttypen OPT används för EDNS.

    b. OPT ligger i ”additional section”.

    c. “dig” visar EDNS-informationen i ”OPT PSUEDOSECTION” i början av visningen av DNS-paketet.

    d. Två exempel, ett räcker:

        1. Maximalt storlek (över 512 bytes) på UDP-paket som accepteras signaleras.

        2. Flagga för om DNSSEC-poster ska skickas i svarspaketet skickas (DO-flaggan).

19. På vilka två sätt kan frågepaketet signalera att frågeställaren önskar få svaret DNSSEC-validerat? Vilken skillnad blir det i svarspaketet i de två fallen? (3 p)

    Svaret får utgå ifrån att valideringen lyckas.

    Alternativ 1: AD-flaggan sätts i frågepaketet

    Alternativ 2: DO-flaggan sätts i frågepaketet.

    Skillnad: Om DO-flaggan sätts så kommer svarspaketet att innehålla relevanta DNSSEC-poster (t.ex. RRSIG) och DO-flaggan kommer att vara satt.

DNSSEC-posterna inkluderas inte och DO-flaggan sätts inte i svarspaketet ifall bara AD-flaggan har satts.

I båda fallen kommer AD-flaggan att vara satt (ingen skillnad).

Svar som korrekt anger båda flaggorna, men inte mer, får 1,5 poäng. Svar som också anger att DNSSEC-posterna inkluderas i det ena fallet får 3 poäng även om det utelämnas att DO-flaggan är satt i svarspaketet i det fallet.

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. RRSIG spelar en viktig roll i DNSSEC. När RRSIG används så måste vissa andra DNS-poster och viss annan information finnas tillgänglig, förutom själva RRSIG. (4 p)
    a) Beskriv vad RRSIG används till.
    b) Lista den information och de DNS-poster som måste finnas tillgängliga.

RRSIG används för att validera det RRset som RRSIG hör till, d.v.s. verifiera att det inte har förvanskats under transporten. För valideringen krävs följande information förutom själva RRSIG:

- RRset att validera.
- Aktuell tid för att verifiera att RRSIG är giltig.
- DNSKEY som RRSIG refererar till.

[DNSKEY antas vara validerad i annan process.]

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

a) Redogör för när det måste finnas glue, när det kan finnas glue (men inte nödvändigt) och när det inte får finnas glue.

b) Illustrera de tre fallen med exempel, med DNS-poster, med beskrivning.

c) 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.

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.
$ORIGIN exempel.se.
$TTL 3600
@                       SOA ns1.exempel.se. root.blue.xa. (
                                2019030909060308
                                4400
                                900
                                604800
                                3600
                                )
                        NS          ns1.exempel.se.
                        NS          ns2.exempel.se.
                        TXT         "Invalid TXT record"
exempel.com.            MX          10  mail.exempel.se.
www                     A           130.237.28.40
                        CNAME       www.example.com.
ns1                     A           130.237.72.250
nameserver              A           130.237.72.250
ns2                     A           129.16.253.356
intrawww                CNAME       intra
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. Dubbla $ORIGIN är inget formellt fel och ger ingen skillnad, men är olämpligt och berodde på misstag. Om det tas upp så ger det varken plus eller minus.

2. 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”.

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. ”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.

5. ”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.

6. "intrawww" har ett CNAME som pekar på ett namn som inte finns. Tag bort "intrawww" eller lägg till en adresspost under "intra".

7. ”mail.” är absolut, vilket gör att det är toppdomänen ”mail”, vilket inte kan finnas i vår zon (”out of zone data”). Rätta genom att ta bort punkten så att det faktiska namnet blir ”mail.exempel.se.” (och matchar vår MX-post efter rättningen).

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

24. 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)

    a) Zonen antas vara korrekt uppsatt och servern antas svara korrekt.

    b) Klass behöver inte anges och TTL antas vara samma för alla poster.

    c) När exakt RDATA för en DNS-post inte är känd så kan RDATA anges som "(...)".

    d) När det gäller signaturer så ska det alltid framgå vilket RRset som signaturen avser.

    e) 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.