Internets domännamnssystem (HI1037)

14 mars 2023

Hjälpmedel:	Inga.
Observera:	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. 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. En DNS-klient skickar en förfrågan till en namnserver men hela svaret inte får plats i svarspaketet. Vad gör servern? (1 p)

   Servern skickar med så mycket som får plats i paketet och sätter TC-flaggan (”truncated”).

5. 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.

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

   RD-flaggan var satt i frågepaketet.

7. Vad innebär "query name minimisation"? (1 p)

   Istället för att resolvern skickar hela frågan i varje steg (från rotzonen och nedåt) så skickar resolvern bara en minimal fråga tills den har hittat zonen där svaret finns.

8. Ge ett exempel på en ccTLD. (1 p)

   .SE, .DK, .DE… (en räcker).

9. 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.

10. Vad är en ”gluepost” i delegeringen? Vad är en nödvändig (strikt) ”gluepost”? Illustrera med ett tydligt exempel. (2 p)

    En gluepost är en adresspost för det namnservernamn som NS-posten pekar ut.

    En nödvändig gluepost är en adresspost för en namnserver vars namn ligger under delegeringen i fråga.

    Zonen namn.xa är delegerad från zonen xa. Adressposten för ”ns1.namn.xa” är en nödvändig gluepost:

    ```
    namn.xa.      NS  ns1.namn.xa.
    namn.xa.      NS  dns1.example.com.
    ns1.namn.xa.  A   192.0.2.100
    ```

11. 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. Vilka likheter och skillnader kommer det att bli när det gäller flaggor och DNS-poster i svarspaketen? (2 p)

    När DO-flaggan inte är satt, 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.]

12. 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)

13. Vad är en ”zon” i DNS-sammanhang? Beskriv tydligt och illustrera med ett exempel genom att utgå ifrån DNS-trädet. (2 p)

    En zon är data som normalt lagras i en zonfil, och som representerar ett delträd inom DNS-trädet. Zonen börjar i en specifik nod i DNS-trädet och sträcker sig sedan godtyckligt långt nedåt (inom gränserna för hur långa domännamnen får vara). Zonen hostas på en eller flera namnservrar och är en egen administrativ enhet. Zonen är utdelegerad från ovanliggande zon (undantag rotzonen).

    [Ritat, eller tydligt beskrivet exempel ska också finnas med.]

14. Varför måste en DNS-resolver ha en hint-fil och hur används den? (2 p)

    Hintfilen innehåller namn och IP-adresser till rotnamnservrarna. DNS-resolvern måste alltid börja i rotzonen och för att kunna hitta den så måste den ha hintfilen. DNS-resolvern använder alltså informationen för att kunna nå rotzonen och sedan hitta vidare i DNS-trädet.

15. Beskriv RDATA för posttypen MX och beskriv hur MX används. Ge ett exempel på hur en MX-post kan se ut. (2 p)

    RDATA består av två delfält, prioritet som är ett positivt heltal resp. mailservernamn som är ett domännamn.

    ”Owner name” är maildomänen som används i mailadressen. Vid uppslagning så anger mailservernamnet den mailserver som mailet ska skickas till. Prioriteten anger ordningen mellan flera MX-poster med samma ”owner name” där den med lägsta värde ska användas i första hand.

    Exempel:

    ```
    namn.se.  MX  10 mail.namn.se.
    ```

    (Korrekt exempel plus ofullständig beskrivning kan ge 1 p, mindre miss i beskrivningen kan ge 1,5 p)

16. Hur stort kan ett svarspaket över UDP vara? Beskriv också de olika förutsättningarna för storleksgränsen eller -gränserna. (2 p)

    Den grundläggande storleksgränsen är 512 Byte/oktetter. Om både klient och server har stöd för EDNS så kan servern skicka ett svarspaket som är högst så stort som klienten i frågepaketet angav.

    (Rätt på 512 B och ofullständigt om EDNS kan ge 1 p)

17. Vad innebär ”zone walking” med hjälp av NSEC-poster? Beskriv begreppet och illustrera det med hjälp av NSEC-poster från en fiktiv zon. Dina NSEC-poster ska skapa en sammanhängande och fullständig kedja bestående av tre NSEC-poster. Övriga DNS-poster behöver inte ingå. Kommentera NSEC-posterna. (3 p)

    Eftersom en NSEC-post både har information om vilka posttyper som det finns poster av i innevarande nod och information om nästa nod i zonen så är det möjligt att vandra från nod till nod och plocka ut alla DNS-poster även om zonöverföring är avstängd. Det går att direkt eller indirekt fråga efter NSEC-posterna i zonen.

    NSEC-poster i en fiktiv zon:

    ```
    namn.se.      NSEC  mail.namn.se.  NS SOA MX RRSIG NSEC DNSKEY
    mail.namn.se. NSEC  www.namn.se.   TXT A AAAA RRSIG NSEC
    www.namn.se.  NSEC  namn.se.       A AAAA RRSIG NSEC
    ```

    Första NSEC-posten visar vilka posttyper som finns i apex och vilken som är nästa namn i zonen (mail.namn.se). Alla poster i apex kan lätt slås upp.

    Andra NSEC-posten ger samma information om nästa namn, och pekar till sista namnet i zonen (www.namn.se). Alla poster kan lätt slås upp.

    Sista NSEC-posten ger samma information om sista namnet, och visar att det är sista namn genom att peka på apex. Alla poster kan lätt slås upp.

18. 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.

19. 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.

20. Hur kommer en renodlad DNS-resolverserver resp. en renodlad DNS-hostingserver hantera olika frågor? Hur hanterar servrarna frågor om olika domäner? Hur hanterar servrarna frågor från olika klienter? Ge en sammanhängande beskrivning. (3 p)

    En renodlad DNS-hostingserver kommer normalt att svara på DNS-frågor från alla klienter, men den kommer bara att svara på DNS-frågor som gäller namn som ligger inom eller under de zoner som är laddade av servern. [Om frågan gäller ett namn i en sådan zon så kan den ge ett auktoritativt svar.] Om frågan gäller ett namn i en underliggande zon så kommer den istället att ge en hänvisning (delegering). Om frågan gäller annat namn så kommer den normalt att svara med REFUSED.

    En renodlad DNS-resolverserver kommer att svara på frågor gällande alla namn i DNS-trädet så vitt det är möjligt genom rekursiv uppslagning. [Svaren till klienten är inte auktoritativa.] Ofta svarar en DNS-resolver bara på frågor från vissa klienter (t.ex. egna nätet). Övriga får REFUSED.

21. I zonerna för domänerna blue.xa resp. green.xa finns DNS-posterna enligt nedan. När du besvarar denna fråga tänk på hur olika DNS-poster får kombineras, och när DNS-poster av en viss typ måste finnas, kan finnas resp. inte får finnas. (4 p)

```
www.blue.xa.     CNAME   www.iis.se.
www.green.xa.    CNAME   www.iis.se.
```

Dessutom så gäller det:

- Zonerna är korrekt uppsatta.
- Namnet www.blue.xa har ytterligare tre DNS-poster av två olika typer.
- Namnet www.green.xa har inga ytterligare DNS-poster.

Att besvara:

- Beskriv de tre ytterligare DNS-posterna i www.blue.xa och skriv DNS-posterna med så mycket detaljer som det går med tanke på den information som är given. Använd "(...)" för att markera delar där information inte finns.
- Vilken slutsats kan man dra för blue.xa resp. green.xa gällande DNSSEC? Motivera ditt svar.

CNAME kan inte kombineras med några andra DNS-poster än NSEC och RRSIG. NSEC och RRSIG kan bara finnas i signerade zoner och måste finnas i signerade zoner för alla andra DNS-poster.

www.blue.xa har en NSEC-post och två RRSIG-poster, den ena för CNAME-posten och den andra för NSEC-posten. Posterna är

```
www.blue.xa.    NSEC (...)  CNAME NSEC RRSIG
www.blue.xa.    RRSIG NSEC (...)
www.blue.xa.    RRSIG CNAME (...)
```

Eftersom www.blue.xa har RRSIG och NSEC så är blue.xa en signerad zon. Eftersom det inte finns någon RRSIG för www.green.xa så betyder det att green.xa är en osignerad zon.

22. 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. Vad kommer att finnas i "answer section" i respektive svarspaket? Svara genom att ge fullständiga DNS-poster och motivera dessa. (4 p)

    - 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 frågan kan sättas till något rimligt värde i DNS-posterna.

    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).

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. (
                                20190
                                4400
                                900
                                604800
                                3600
                                )
                        NS          ns1.exempel.se.
                        NS          ns2.exempel.se.
                        NS          130.237.70.50
                        TXT         "Invalid TXT record"
exempel.se.             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           129.16.253.156
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. Första NS-posten pekar på ett namn som har ett CNAME (ns1). RDATA i en NS-post måste vara ett namn som har en adresspost (A/AAAA). Gör om CNAME till en A-post med adressen som "nameserver" har.

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. 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”.

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

6. ”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).

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

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.