Internets domännamnssystem (HI1037)
4 juni 2020

Hjälpmedel:	Inga.
Observera:	Lösningarna måste vara skrivna med läsbar handstil. Ange namn och personnummer på varje sida. 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. Del 1 är frågor 1—12 (max 29 poäng). Del 2 är frågor 13—24 (max 29 poäng).

---

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

   Klienten ber servern om rekursiv uppslagning.

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

   RD-flaggan var satt i frågepaketet.

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

   Svaret är auktoritativ data.

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

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

5. (5) 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)

6. (6) 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.)

7. (7) 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)

8. (8) 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)

9. (9) 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)

10. (10) Beskriv hur man tar fram DNS-namnet för baklängesuppslagning för IPv4 resp IPv6. Använd adresserna 10.11.12.13 resp abcd::6789 för att illustrera med. (4 p)

    IPv4 (10.11.12.13):

    1. Vänd ordning på oktetterna: 13.12.11.10
    2. Sätt på ”in-addr.arpa” som suffix: 13.12.11.10.in-addr.arpa

    IPv6 (abcd::6789):

    1. Expandera adressen till explicit format:
    abcd:0000:0000:0000:0000:0000:0000:6789
    2. Tag bort ”:” och sätt ”.” mellan alla siffror:
    a.b.c.d.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.7.8.9
    3. Vänd på ordningen på alla siffor:
    9.8.7.6.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.c.b.a
    4. Sätt på ”ip6.arpa” som suffix:
    9.8.7.6.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.c.b.a.ip6.arpa

    (Rätt förutom ”för liten” IPv6-adresse kan ge 3,5 p.)

11. (11) 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)

    a) 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.

    b) Vad är skillnaden mellan en ASCII-label och IDN-label? Beskriv skillnaden med hänsyn till de olika representationerna av IDN-label.

    c) 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.)

12. (12) Kopiera och uppdatera zonfilen nedan så att den är korrekt förutom de listade felaktigheterna. Du ska alltså lägga in dessa felaktigheter, men inga andra, genom att lägga till eller ändra i zonfilen. För varje felaktighet så ska du beskriva vad och hur det är fel. Du får ett poäng för varje korrekt fel. Om du skapar felaktigt fel så får du minuspoäng, men totalsumman på frågan kan aldrig bli mindre än noll. (6 p)

    a) Felaktigt serienummer.

    b) CNAME i otillåten nod.

    c) FQDN som ger fel.

    d) Relativt domännamn som ger fel.

    e) Felaktig RDATA i en AAAA-post.

    f) ”Owner name” som ger fel.

```
$ORIGIN exempel.se.
$TTL 3600
@                       SOA ns1.exempel.se. root.telia.se. (
                                4019060400
                                4400
                                900
                                604800
                                3600
                                )
                        NS          ns1.exempel.se.
                        NS          ns2.exempel.se.
ns1                     A           130.237.72.250
ns2                     A           129.16.253.254
```

Exempel på zonfil med felen ovan:

```
$ORIGIN exempel.se.
$TTL 3600
@                       SOA ns1.exempel.se. root.telia.se. (
                            5019060400
                            4400
                            900
                            604800
                            3600
                            )
                        NS          ns1.exempel.se
                        NS          ns2.
                        CNAME       www.exempel.se.
ns1                     A           130.237.72.250
ns2                     A           129.16.253.254
www                     AAAA        2001::53::80
exempel.com.            MX          10  mail.kth.se.
```

Serienumret i SOA-posten ska vara maximalt 2^32. Talet är större än så.

I första NS-posten så är RDATA relativt, vilket motsvarar FQDN ”ns1.exempel.se.exempel.se.” vilket inte finns.

I andra NS-posten så är RDATA absolut, men FQDN ”ns1.” finns inte.

CANME kan inte finnas med andra DNS-poster i samma ”owner name”.

IPv6-adressen i RDATA för www.exempel.se är felaktigt.

MX-posten har ett ”owner name” som ligger utanför zonen.

(Det behöver inte vara 6 olika fel för att ge 6 poäng. Om samma fel kan sägas representera mer än en kategori så är det OK.)

13. (13) Vad är en ccTLD? (1 p)

    Landstoppdomän.

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

14. (14) 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.

15. (15) Vad står IDN för? (1 p)

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

16. (16) Vad betyder QR-flaggan? När är den satt och när den inte satt? (1 p)

    Satt QR betyder att det är ett svarspaket. I frågepaket är den osatt.

17. (17) Det finns tre A-poster för ”www.exempel.se” och flera klienter gör var sin uppslagning av dessa. I den normala situationen, i vilken ordning kommer posterna? Klienten ska använda en post. Hur väljer klienten vilken post som ska användas? (2 p)

    Posterna kommer i olika ordning för de olika klienterna och vid upprepad förfrågan. Klienten tar normalt den första posten i listan. (Referens till ”round robin” är likvärdigt med ”olika ordning.)

18. (18) Ett svarspaket kan innehålla statuskoden REFUSED. Beskriv två *vanliga* scenarior 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.)

19. (19) Vilken roll har cachning för DNS-resolvning? Vad styr cachningen? Beskriv hur cachningen påverkar svaren vid DNS-resolvning. (2 p)

    Cachningen är tillfällig lagring av svar som har hämtats genom en vanlig DNS-fråga. Tiden för hur länge det lagras styrs av TTL för DNS-posten. När en DNS-resolver har det efterfrågade datat i sin cache så kan den svara direkt utan att ställa egna frågor. Lasten på resolvern och svarstiden minskar. Ändringar i zonen slår inte igenom så länge svaret kommer från cache.

    (Om man missar att cachning kan försena uppdatering, men resten är rätt, så kan man få 1,5 p)

20. (20) En DNS-fråga i ”question section” består av tre delar, varav klass (”class”) är den ena. Vilka är de två andra? (2 p)

    a) Owner name, queryname eller qname

    b) query type eller qtype

21. (21) Hur utförs en delegering i en zonfil och vad krävs för att den ska bli korrekt? Illustrera med ett kommenterat exempel. (3 p)

    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.

22. (22) 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.

23. (23) Utgå ifrån namnet ”www.kth.se” och posttypen A, som finns. Tänk dig att du ställer en DNS-fråga efter det namnet med den posttypen till olika renodlade DNS-hostingservrar på det publika Internet. Beskriv de tre kategorier av servrar som du normalt kommer att stöta på, i förhållande till just denna fråga. Låt beskrivningen utgå ifrån status och vilka DNS-poster som finns, inte finns eller kan finnas med i de olika ”sections” i svarspaketet. Utgå ifrån att servrarna är modernt och korrekt konfigurerade. Bortse ifrån EDNS, klass och TTL. (4 p)

    Alla svarspaket kommer att ha samma innehåll i ”question section”, vilket är kopierat från frågepaketet, ”www.kth.se. A”.

    Kategori 1. Servern har varken kth.se-, se- eller rotzonen. Status i svarspaketet är REFUSED. Förutom ”question section” så innehåller svarspaketet inga DNS-poster.

    Kategori 2. Servern har kth.se-zonen. Status i svarspaketet är NOERROR. ”Answer section” innehåller svaret i form av ”www.kth.se. A x.x.x.x”. ”Authority section” kan innehålla NS-posterna för kth.se-zonen och i så fall kan ”additional section” innehålla A- eller AAAA-poster för namnservernanen från NS-posterna.

    Kategori 3. Servern har se- eller rotzonen (men inte kth.se-zonen). Status är NOERROR. ”Answer section” är tom. ”Authority section” innehåller NS-poster för se-zonen (från rotnamnserver) eller för kht.se-zonen (från .se-server). ”Additional section” innehåller A- eller AAAA-poster om glue-poster är nödvändiga. Ifall glue-poster inte behövs så kan ”additional section” vara tom.

24. (24) Vilka DNS-poster tillkommer i en DNSSEC-signerad zon jämfört med en osignerad? Kopiera zonen nedan och uppdatera den med de nya DNS-posterna. Det ska vara rätt ”owner name” och posttyp. Detaljerna i RDATA för de nya posterna behöver inte finnas med, kan anges som ”(…)”, utan det räcker med att beskriva RDATA. 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. (7 p)

```
$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.
www                     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
                        NSEC        (…) ;
                        RRSIG       (…) ; På NSEC RRSET
www                     A           130.237.28.40
                        RRSIG       (…) ; På www/A RRSET
                        NSEC        (…) ;
                        RRSIG       (…) ; På www/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 **www.exempel.se.**

RDATA för NSEC har dels namnet på nästa namn, dels en lista över alla posttyper med samma ”owner name” som NSEC-posten.