Internets domännamnssystem (HI1037)
5 juni 2024

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

---

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

   ANY, AXFR, IXFR (en räcker)

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

   Klienten ber servern om rekursiv uppslagning.

6. Hur kan man använda DNS för en enkel lastbalansering av webbservrar? (1 p)

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

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. 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.

10. Beskriv serienumrets (”SOA serial”) roll för zonöverföringen. (2 p)

    Slavservern använder serienumret för att avgöra ifall zonfilen har ändrats. Slavservern hämtar zonfilen från masterservern ifall serienumret hos mastern är högre än hos slaven.

11. Vad innebär tekniken ”anycast”? Utgå ifrån rotnamnservrarna och beskriv hur ”anycast” används för att öka kapacitet, spridning och tillgänglighet för dessa. (2 p)

    ”Anycast” innebär att samma IP-adress annonseras ut från olika platser med olika servrar för ”samma” namnserver (NS). Tekniken ökar kapaciteten för namnservern och ger närhet till den från olika platser.

12. 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”.

13. Delegering är ett viktigt begrepp i DNS. Vad innebär en delegering? (2 p)

    Delegering innebär att en nod i DNS-trädet, och alla underliggande noder, hänvisas till en eller flera namnservrar som har den delegerade zonen (dotterzonen).

14. Du ställer frågan om ”www.exempel.se. A” med ”dig” till masterservern för exempel.se och får ett NODATA-svar. Beskriv vad det innebär och hur svarspaket som ”dig” presenterar ser ut. (2 p)

    NODATA innebär att det efterfrågade namnet, www.exempel.se i detta fall, finns, men inte med det efterfrågade posttypen, ”A” i detta fall.

    I svarspaketet innehåller ”Answer section” inte någon A-post [men ev. CNAME-post], ”authority section” innehåller SOA-posten för zonen och status är NOERROR.

15. Utgå ifrån IPv4-adress 10.20.30.40 och tänk dig att du använder programmet ”dig” med växeln ”-x”. (2 p)
    - 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.

    ”Question section”:

    ```
    40.30.20.10.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 punkter mellan och sedan får suffixet ”.in-addr.arpa.”

16. AD-flaggan används i vissa sammanhang. (2 p)
    - 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?

    I frågepaketet används en satt AD-flagga för att signalera att klienten är beredd på att ta emot ett svarspaket med AD-flaggan satt. Och klienten vill veta ifall svaret är validerat.

    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.

17. Serienumret (”SOA serial”) är ett 32-bitars positivt heltal (har ett värde mellan 0 och 4.294.967.295). (4 p)
    - Beskriv hur jämförelsen görs mellan olika serienummer.
    - Beskrivs vad som räknas som högst och lägst när två serienummer jämförs.
    - Ge två exempel där serienummer A räknas som större än B. I exempel 1 så ska A vara talmässigt större än B. I exempel 2 så ska A vara talmässigt mindre än B.

    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.

    Exempel: Om A är 1000 och B är 10 så är A ett högre serienummer. Om A är 10 och B är 4.000.000.000 så är A ett högre serienummer.

18. EDNS är en utökning av DNS-protokollet. Beskriv hur EDNS fungerar och vad det tillför enligt följande punkter. (4 p)
    - Vad är det för posttyp som används för EDNS-informationen?
    - Var i DNS-paketet transporteras EDNS-informationen?
    - Hur kan man se med ”dig” om DNS-paketet är utökat med EDNS eller inte?
    - Ge två exempel på information som kan signaleras med hjälp av EDNS.

    - En DNS-post med posttypen OPT används för att "transportera" EDNS-informationen.
    - OPT-posten ligger i ”additional section”.
    - “dig” visar EDNS-informationen i ”OPT PSUEDOSECTION” i början av visningen av DNS-paketet.
    - Maximalt storlek (över 512 bytes) på UDP-paket som accepteras signaleras signaleras i EDNS.
    - DO-flaggan för DNSSEC kan sättas i EDNS.

19. 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)
    - Beskriv vad RRSIG används till.
    - 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.]

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

- Redogör för när det måste finnas glue, när det kan finnas glue (men inte nödvändigt) och när det inte får finnas glue.
- Illustrera de tre fallen med exempel, med DNS-poster, med beskrivning.
- 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.

21. 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.)

22. 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.

23. Frågor ställdes till tre namnservrar med programmet "dig" och de tre svarspaketen redovisas nedan. Frågepaketen ("query") var identiska utom ev. skillnad i frågetyp ("query type"). Jämför svaren och identifiera skillnader och likheter. Du kan utgå ifrån att servrar och zoner är korrekt konfigurerade, och och att inget har ändrats i zonen mellan svaren. Du kan bortse från tidsstämplarna. (7 p)

    - Vilka slutsatser kan man dra om namnservrarna och hur de är konfigurerade? Motivera dina slutsatser genom att peka på likheter och skillnader i svarspaketen.
    - Vilka skillnader mellan svarspaketen är inte relevanta för att dra slutsatser om namnservrarna. Motivera.

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13412
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;kth.se.     IN  A

;; ANSWER SECTION:
kth.se.      7200  IN  A  130.237.28.40

;; Query time: 57 msec
;; SERVER: 129.16.253.252#53(129.16.253.252)
;; WHEN: Wed Jun 07 10:27:59 CEST 2023
;; MSG SIZE  rcvd: 51


;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31097
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 3072
;; QUESTION SECTION:
;kth.se.     IN  A

;; ANSWER SECTION:
kth.se.      4571  IN  A  130.237.28.40

;; Query time: 54 msec
;; SERVER: 10.30.7.2#53(10.30.7.2)
;; WHEN: Wed Jun 07 10:28:28 CEST 2023
;; MSG SIZE  rcvd: 51


;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 632
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;kth.se.     IN  AAAA

;; ANSWER SECTION:
kth.se.      7193  IN  AAAA  2001:6b0:1:11c2::82ed:1c28
```

```
;; Query time: 54 msec
;; SERVER: 63.33.59.206#53(63.33.59.206)
;; WHEN: Wed Jun 07 09:06:15 UTC 2023
;; MSG SIZE  rcvd: 51
```

Server 129.16.253.252 är en auktoritativ server för zonen där kth.se ingår (vi kan inte se zonen från svaret, men vi vet av annan erfarenhet att zonen är kth.se) eftersom AA-flaggan är satt. Den är inte en resolver för frågeställaren eftersom RA-flaggan inte är satt.

Servern 10.30.7.2 är en resolver (RA-flaggan är satt) och ger ett icke-auktoritativt svar (AA-flaggan är inte satt). Dessutom så är den en DNSSEC-validerande resolver (AD-flaggan är satt).

Servern 63.33.59.206 är också en resolver (RA-flaggan är satt) och ger också ett icke-auktoritativt svar (AA-flaggan är inte satt). Däremot den inte en validerande resolver eftersom AD-flaggan inte är satt.

Eftersom zonen uppenbarligen är signerad så kan vi anta att även 129.16.253.252 har stöd för DNSSEC.

Skillnader i message ID är inte relevant. Den blir automatiskt olika för varje fråga.

Skillnaden i posttyp (A kontra AAAA) styrs från frågan, och är inte en egenskap i namnservern.

Namnservrarna annonserar olika maximal UPD-storlek i EDNS. Två servrarn annonserar 1232 byte och en 3072 byte. Konfigurering av namnservrarna styr detta.

Skillnaderna i TTL mellan de två namnservrarna som har svarat på A-frågan är inte oväntad där det auktoritiva svaret har längre TTL, och resolverns TTL har hunnit minskas när frågan ställdes. Detta är en effekt av att den ena är en auktoritativ server och den andra en resolver.