Internets domännamnssystem (DVGC28)

29 maj 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: 3-5 från 29 till 58 poäng med intervaller om ungefär 10 poäng. U (underkänt) under 29 poäng.

---

1. Vad är zonöverföring? (1 p)

   Zonöverföring är kopiering av zonfilen från masterserver till slavserver med DNS-protokollet. (Eller mera generellt, kopiering med DNS-protokollet av en zon från en auktoritativ namnserver till en klient.)

2. Beskriv formatet för 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.

3. Vilken roll spelar Message ID i DNS-paketen för DNS-frågor och -svar (”DNS query and response”)? (1 p)

   Med Message ID i svarspaketet så kan klienten para ihop det med rätt frågepaket.

4. 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.

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

   Unicode.

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

   RD-flaggan var satt i frågepaketet.

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. Vad står IDN för? (1 p)

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

9. En klient skickar en DNS-fråga med *www.iis.se* som "query name" till sin resolver. (2 p)
   - Vad blir skillnaden om resolvern följer normal process eller QNAME Minimisation ("query name mininisation") när det gäller ”query name” när resolvern sedan ställer frågan till en rotnamnserver?
   - Vad blir ”query name” till rotnamnservern om "QNAME mininisation" följs?
   - Hur påverkas "query type" av "QNAME minimisation"?

   Normal är QNAME (”query name”) hela ”www.iis.se”, men med QNAME Minimisation så blir det istället bara ”se”. Normalt är QTYPE ("query type") samma som ursprungsfrågan, men med QNAME minimisation så används en fast QTYPE, oftast A, fram till sista frågan, då ursprunglig QTYPE används.

10. Vad innebär frågetyp ANY? Vad förväntas svarsposten innehålla? Kommer svaret att innehålla en ANY-post? (2 p)

    Frågetypen ANY betyder att DNS-klienten (t.ex. "dig") frågar efter alla DNS-poster oavsett posttyp med det "owner name" som anges i frågan. Svaret förväntas innehålla alla dessa i "answer section". ANY är ingen posttyp så någon ANY-post kan inte finnas.

11. 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.

12. 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.

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

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

14. 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).

    [Tydligt beskrivet exempel ska också finnas med.]

15. 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.

16. Det finns en speciell posttyp för email. Vilken är den och hur används den? (2 p)
    - Ange vilken posttypen är.
    - Peka ut vad RDATA består av.
    - Illustrera med ett exempel som skulle kunna gälla för mailadressen info@namn.se.

    Posttypen är MX.

    MX pekar ut mailservern för maildomänen (i fält 2 i RDATA). Om det finns flera MX-poster för samma maildomän så kommer prioritetsfältet (fält 1 i RDATA) att styra vilken MX-post som ska användas.

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

17. TSIG kan användas för att styra möjlighet till zonöverföringar. (4 p)

- Beskriv hur TSIG används i sådant fall.
- Ge en övergripande beskrivning av hur konfigurationen görs i master- resp. slavserver.
- Ge exempel på en fördel att använda TSIG jämfört med med stryrning med "source IP".
- Hur skyddar TSIG mot insyn i zonöverföringen? Förklara

TSIG kan användas för att kontrollera vilka slavservrar som får hämta zonen med zonöverföring. Endast slavar som har den specifika TSIG-nyckeln kommer då att accepteras för zonöverföring.

TSIG-nyckeln läggs in i både masterserverns och slavserverns konfiguration (named.conf) som en delad hemlighet. I masterservern anges att den specifikat TSIG-nyckeln är ett krav för att få zonen med zonöverföring. I slavservern anges att alla anrop till den specifika masterservern ska signeras med den specifika TSIG-nyckeln.

En fördel är att slavservern kan byta IP-adress utan att masterservern behöver konfigureras om jämfört med om restriktion baseras på slavens IP-adress.

En annan fördel är att slavservern får en verifikation på att zonen är komplett och omodifierad när den kommer fram.

TSIG skyddar inte alls mot insyn eftersom zoninnehållet går i klartext. TSIG ger bara en signering av datat.

18. DNS-paketet "on the wire" består av fem huvuddelar. (4 p)

- Ange delarna i den ordning som de kommer i paketet.
- Ange vad det är för type av data som kan finnas i respektive del. Om en del innehåller flera typer av data så räcker det med ett exempel.
  - Header
    - Innehåller flaggor, statuskod, ID m.fl.
  - Question section
    - Frågeposten ("query name, query class and query type")
  - Answer section
    - DNS-poster
  - Authority section
    - DNS-poster
  - Additional section
    - DNS-poster

19. Det finns två sätt som ett frågepaket kan signalera att frågeställaren önskar få veta om ett DNS-svar är DNSSEC-validerat. (4 p)

    - Beskriv de två sätten.
    - Vilken eller vilka skillnader blir det i svarspaketet i de två fallen om vi antar att efterfrågade datat var signerat och valideringen lyckades?
    - Vilken eller vilka likheter blir det med samma antaganden?

    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 (likhet).

20. 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.

    Det som pekas ut är de namnservrar som håller dotterzonen med samma namn som "owner name" till NS-posterna, samt att dotterzonen existerar.

    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:

```
example.se.       NS   ns1.example.se.
example.se.       NS   ns2.example.se.
example.se.       NS   ns.namn.se.
example.se.       NS   dns.example.xa.
ns1.example.se.   A    192.0.2.5
ns1.exemple.se.   AAAA 2001:DB8:A::5
ns2.example.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 motsvaras av en glue-post eftersom den ligger under .se, men måste inte. Den fjärde kan inte ha glue-post eftersom den ligger helt utanför .se.

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

21. Utgå ifrån namnet ”www.kth.se” och posttypen A, som finns. Tänk dig att du ställer en DNS-fråga efter "www.kth.se. A" till olika renodlade DNS-hostingservrar på det publika Internet. (4 p)

    - 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.

    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.

22. 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. Du ska också tydligt beskriva varje felaktighet, vad och hur det är fel. Varje felaktighet ska vara en egen ändring. 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. (7 p)

    - Felaktigt serienummer.
    - CNAME i otillåten nod.
    - FQDN som ger fel.
    - Relativt domännamn som ger fel.
    - Felaktig RDATA i en AAAA-post.
    - ”Owner name” utanför zonen så att det blir fel.
    - Lägg in en kommentar med fel kommentarstecken i zonfilen så att det blir en ”trasig” zonfil.

```
$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.
                        NS          ns2.exempel.se
                        CNAME       www.exempel.se.
ns1                     A           130.237.72.250
ns2                     A           129.16.253.254
www                     AAAA        2001::53::80
# Mail is outsourced
exempel.com.            MX          10  mail.kth.se.
```

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

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

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

I andra NS-posten så är RDATA relativt, vilket motsvarar FQDN ”ns2.exempel.se.exempel.se.” vilket inte finns i zonen.

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

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

”#” är ingen kommentarstecken, utan det ska vara ”;”.

23. Zonerna dnskurs.xa och tenta.nod.dnskurs.xa finns. Noden nod.dnskurs.xa är en "empty non-terminal". Zonen dnskurs.xa har två NS-poster, vars namnserver-namn ligger under dnskurs.xa. Zonen tenta.nod.dnskurs.xa har tre NS-poster, varav exakt en kräver glue-post i delegeringen. Både www.dnskurs.xa och www.tenta.nod.dnskurs.xa finns med adressposter. (7 p)

    - Komponera båda zonerna (zonfilerna) med alla DNS-poster som krävs. Tag inte med några extra DNS-poster.

    Du ska utgå ifrån följande:

    - Använd IP-adresser inom 192.0.2.0/24
    - Alla adressposter ska ha unika IP-adresser.
    - Ingen av zonerna ska vara DNSSEC-signerade.
    - Delegeringar ska matcha dotterzonens DNS-poster.
    - DNS-poster där värdena inte är specificerade i förutsättningarna ges lämpliga värden.
    - Zonerna ska konfigureras rätt och komplett.
    - Om RDATA för en DNS-post har fler än två delfält så kan RDATA förkortas till "(...)".

    Viss data kan väljas annorlunda eftersom allt inte är specificerat eller fullt specificerade i förutsättningarna.

```
$ORIGIN dnskurs.xa.
$TTL 3600
@                   SOA   (...)
                    NS    ns1.dnskurs.xa.
                    NS    ns2.dnskurs.xa.
ns1                 A     192.0.2.20
ns2                 A     192.0.2.30
tenta.nod           NS    ns1.labb.xa.
                    NS    ns2.labb.xa.
                    NS    ns1.tenta.nod
ns1.tenta.nod       A     192.0.2.210
www                 A     192.0.2.50


$ORIGIN tenta.nod.dnskurs.xa.
$TTL 3600
@                   SOA   (...)
                    NS    ns1.labb.xa.
                    NS    ns2.labb.xa.
                    NS    ns1
ns1                 A     192.0.2.210
www                 A     192.0.2.203
```