Internets domännamnssystem (HI1037)

9 juni 2023

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.

---

1. Vad är zonöverföring? (1 p)

   Zonöverföring är kopiering av zonfilen från masterserver till slavserver med DNS-protokollet.

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. 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.

4. 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.

5. Hur kan användning av DNS underlätta adressbyte? (1 p)

   Om ett domännamn används för en tjänst så kan IP-adressen som domännamnet pekar på bytas utan att användarna behöver informeras om adressbytet.

6. Vad innebär det att ett domännamn avslutas med en punkt (".")? (1 p)

   Att domännamnet är ett absolut domännamn alt. ett FQDN.

7. Beskriv formatet på RDATA i en CNAME-post. (1 p)

   RDATA är ett domännamn i FQDN-format.

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 heter den utökning som tillåter tecken bortom ASCII i domännamn och vad heter den teckenuppsättning som dessa baseras på? (2 p)

   Utökningen heter IDN (eller "Internationalized Domain Name"). Tecken-uppsättningen heter Unicode.

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. Var i zonen finns det alltid NS-poster och var i zonen kan det finnas NS-poster? (2 p)

    Det finns alltid minst en NS-post (normalt minst två) i zonens apex, och om det finns delegeringspunkter i zonen så finns det minst en NS-post (normalt minst två) i varje delegeringspunkt. NS-poster finns inte på någon annan plats i zonen.

12. 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.

13. 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.

14. 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).

15. 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.

    ”Answer section” innehåller ingen DNS-post med den efterfrågade posttypen [med ev. en CNAME-post], ”authority section” innehåller SOA-posten för zonen och status är NOERROR.

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

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

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

17. Beskriv hur TSIG kan användas för att styra zonöverföringar. Ge också en övergripande beskrivning av hur konfigurationen görs i master- resp. slavserver. (3 p)

    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.

18. 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.

19. EDNS är en utökning av DNS-protokollet. Beskriv hur EDNS fungerar och vad det tillför enligt följande punkter. (3 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 ett exempel på information som kan signaleras med hjälp av EDNS.

    a. En DNS-post med posttypen OPT används för EDNS.

    b. OPT-posten 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 kan inkluderas i svarspaketet (DO-flaggan).

20. På vilka två sätt kan frågepaketet signalera att frågeställaren önskar få svaret DNSSEC-validerat? Vilken skillnad blir det i svarspaketet i de två fallen om vi antar att efterfrågade datat var signerat och valideringen lyckades? (3 p)

    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.

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)

    - 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.]

22. 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-adress kan ge 3,5 p.)

23. 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 och hur det skulle vara rätt. 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 på fel sätt 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.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
# Mail is outsourced
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 ”ns2.” finns inte.

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

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

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

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

(Det behöver inte vara 7 olika fel för att ge 7 poäng. Om samma fel kan sägas representera mer än en kategori så är det OK, men det måste finnas 7 beskrivningar.)

24. Frågor ställdes till tre namnservrar med programmet "dig" och de tre svarspaketen redovisas nedan. 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 UDP-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.