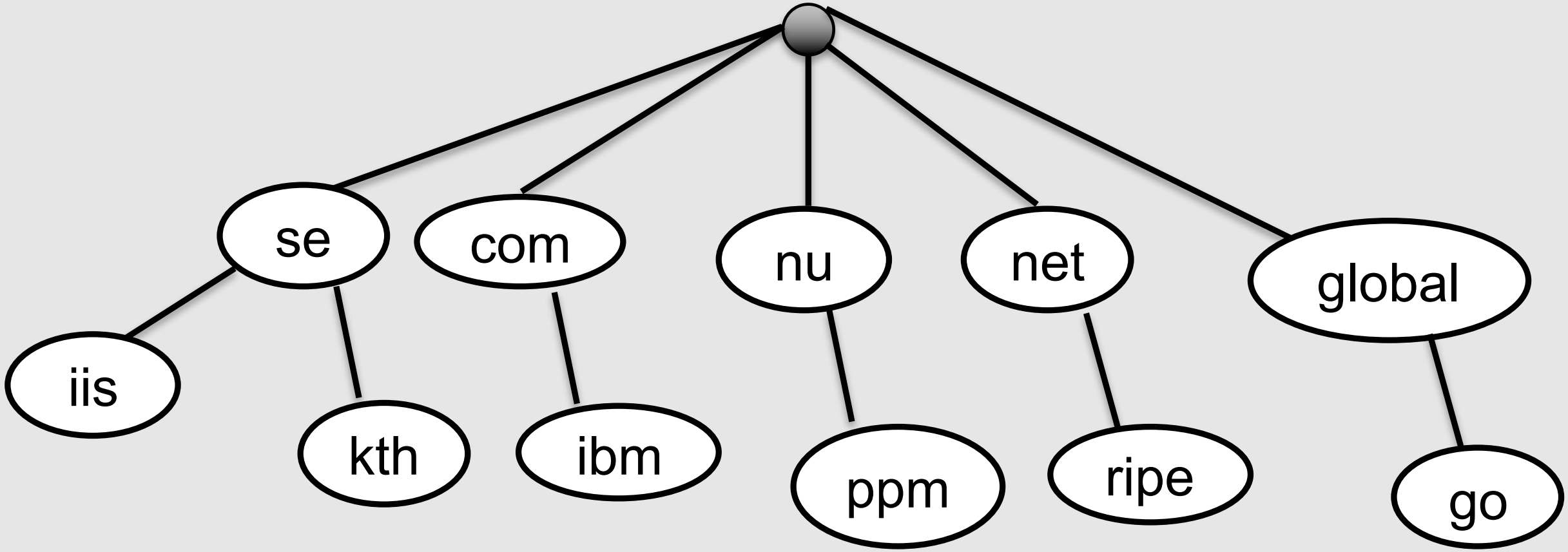
se
com
nu
net
global
iis
kth
ibm
ppm
ripe
go

INTERNET STIFTELSEN

Internets domännamnssystem*

Föreläsning FL14, VT 2024

Mats Dufberg

* Se “Internets domännamnssystem”

Innehåll

- ▶Genomgång av tenta 2023-06-09
- ▶Sammanfattning av kursen
- ▶Utvärdering av kursen
- ▶Om presentationen

▶Genomgång av tenta 2023-06-09

[Innehåll]

Fråga 1 (1p)

Vad är zonöverföring?

Facit

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.)

Fråga 2 (1 p)

Beskriv formatet för RDATA för posttyp A som det presenteras av t.ex. programmet "dig", och ge ett exempel.

Facit

RDATA för A-post är en IPv4-adress skrivet med fyra decimala oktetter med punkt mellan, t.ex. 192.0.2.190.

Fråga 3 (1 p)

En förfrågan om example.se skickas till en internetoperatörs DNS-resolver, som svarar med REFUSED.

- Vad är den troliga orsaken?

Facit

Klienten sitter inte på ett IP-nät som DNS-resolvern accepterar att svara på frågor från.

Fråga 4 (1 p)

Hur kan man använda DNS för en enkel lastbalansering av webbservrar?

Facit

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

Fråga 5 (1 p)

Hur kan användning av DNS underlätta adressbyte?

Facit

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

Fråga 6 (1 p)

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

Facit

Att domännamnet är ett absolut domännamn alt. ett FQDN.

Fråga 7 (1 p)

Beskriv formatet på RDATA i en CNAME-post.

Facit

RDATA är ett domännamn i FQDN-format.

Fråga 8 (1 p)

Hur används QR-flaggan, d.v.s.

- när är den satt och
- när är den inte satt?

Facit

- QR-flaggan är satt i ett svarspaket (”response”).
- I frågepaket (”query”) är den inte satt.

Fråga 9 (2 p)

- Vad heter den utökning som tillåter tecken bortom ASCII i domännamn och
- vad heter den teckenuppsättning som dessa baseras på?

Facit

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

Fråga 10 (2 p)

- Vad innebär frågetyp ANY?
- Vad förväntas svarsposten innehålla?
- Kommer svaret att innehålla en ANY-post?

Facit

- 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.

Fråga 11 (2 p)

- Var i zonen finns det alltid NS-poster och
- var i zonen kan det finnas NS-poster?

Facit

- Det finns alltid minst en NS-post (normalt minst två) i zonens apex.
- 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.

Fråga 12 (2 p)

Beskriv serienumrets (”SOA serial”) roll för zonöverföringen

Facit

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

Fråga 13 (2 p)

- Vad är en ”stub resolver” och
- vad har den för funktion för resolvning?

Facit

- 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.

Fråga 14 (2 p)

Delegering är ett viktigt begrepp i DNS.

- Vad innebär en delegering?

Facit

Delegering innebär att en

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

Fråga 15 (2 p)

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.

Facit

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.

Fråga 16 (2 p)

- Vad innebär begreppet "dold master"?
- Vilka fördelar finns det med att använda en dold master?

Facit

"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.

Fråga 17 (3 p)

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

Facit (1/2)

- 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.

Facit (2/2)

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.

Fråga 18 (3 p)

Serienumret (”SOA serial”) är ett 32-bitars positivt heltal (har ett värde mellan 0 och 4.294.967.295).

- Beskriv hur jämförelsen görs mellan olika serienummer, d.v.s.
  - vad som räknas som högst och
  - lägst när två serienummer jämförs.

Facit

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.

Fråga 19 (3 p)

EDNS är en utökning av DNS-protokollet. Beskriv hur EDNS fungerar och vad det tillför enligt följande punkter.

- 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.

Facit (1/2)

- En DNS-post med posttypen OPT används för EDNS.
- OPT-posten ligger i ”additional section”.
- “dig” visar EDNS-informationen i ”OPT PSUEDOSECTION” i början av visningen av DNS-paketet.

Facit (2/2)

- Två exempel på information, ett räcker:
  - Maximalt storlek (över 512 bytes) på UDP-paket som accepteras signaleras.
  - Flagga för om DNSSEC-poster kan inkluderas i svarspaketet (DO-flaggan).

Fråga 20 (3 p)

- 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?

Facit (1/2)

(På vilka två sätt...?)

Alternativ 1: AD-flaggan sätts i frågepaketet

Alternativ 2: DO-flaggan sätts i frågepaketet.

Facit (2/2)

(Vilken skillnad...?)

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).

Fråga 21 (4 p)

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.

- Beskriv vad RRSIG används till.
- Lista den information och de DNS-poster som måste finnas tillgängliga.

Facit (1/2)

RRSIG används för att validera det RRset som RRSIG hör till, d.v.s. verifiera att det inte har förvanskats under transporten.

Facit (2/2)

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.

Fråga 22 (4 p)

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.

Facit (1/2)

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

Facit (2/2)

IPv6 (abcd::6789):

1. Expandera adressen till explicit format (32 hexadecimala siffror):
   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

Fråga 23 (7 p) – (1/3)

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.

Fråga 23 (7 p) – (2/3)

- 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.

Fråga 23 (7 p) – (3/3)

```
$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
```

Facit (exempel på zonfil) – (1/2)

```
$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.
```

Facit (enl exempel på zonfil) – (2/2)

- 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.

Fråga 24 (7 p) – (1/5)

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"). [Tillagt jämfört med tentan.]
- 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.

Fråga 24 (7 p) – (2/5)

- 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.

Fråga 24 (7 p) – (3/5)

```
;; ->>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
```

Fråga 24 (7 p) – (4/5)

```
;; ->>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
```

Fråga 24 (7 p) – (5/5)

```
;; ->>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
```

Analys

```
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
(...)
;; ANSWER SECTION:
kth.se. 7200  IN  A  130.237.28.40


;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
(...)
;; ANSWER SECTION:
kth.se. 4571  IN  A  130.237.28.40

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
(...)
;; ANSWER SECTION:
kth.se. 7193  IN  AAAA  2001:6b0:1:11c2::82ed:1c28
```

Facit – (1/7)

- Server 129.16.253.252 är en auktoritativ server för zonen där kth.se ingår eftersom AA-flaggan är satt.
- Den är inte en resolver för frågeställaren eftersom RA-flaggan inte är satt.

Facit – (2/7)

- 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).

Facit – (3/7)

- 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.

Facit – (4/7)

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

Facit – (5/7)

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.

Facit – (6/7)

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

Facit – (7/7)

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.

▶Sammanfattning av kursen

[Innehåll]

Sammanfattning av kursen (FL01)

- Domännamn och DNS
  - Domännamn som address
  - Abstrahering
    - Domännamn istället för IP-adress
    - Igenkänning
    - Gruppering
    - Beteckna tjänst
    - Varumärke

Sammanfattning av kursen (FL01)

- Inte bara peka ut IP-adresser
  - Annan data
- Adressbyten
- Lastdelning
- Domännamnsträdet
- Domännamnets form
- Var finns domännamnet
- Var finns datat

Sammanfattning av kursen (FL01)

- Visningsformatet på DNS-datat
  - Owner name
  - TTL
  - Class
  - Record type
  - RDATA
- Relativa och absoluta namn
- Posttyp A, AAAA, TXT

Sammanfattning av kursen (FL02)

- Domännamn och tecken
  - FQDN
  - ASCII
  - Hostname
- DNS-data
  - På hostingserver
  - Via resolver

Sammanfattning av kursen (FL02)

- Zoner
  - Domännamn kontra zon
- DNS-anrop och DNS-paket
  - Nätverkslager
    - UDP, TCP, port 53
  - DNS-frågor från program
  - Stub-resolver
  - DNS-frågor med "dig"

Sammanfattning av kursen (FL02)

- DNS-pakets delar
- Query och response
  - Question och answer
  - Response utan answer
- Posttyp MX
  - Mail och DNS
- Posttyp CNAME
  - Alias

Sammanfattning av kursen (FL02)

- Posttyp NS och delegering
  - Posttyp NS
  - Delegering
- SOA
  - Posttyp SOA
    - RDATA med många delfält

Sammanfattning av kursen (FL02)

- Posttyper och begränsningar
  - A, AAAA, TXT – ger data direkt
  - CNAME, MX – pekar helt eller delvis vidare
  - NS, SOA – bara inom DNS
  - Begränsningar hos CNAME, SOA, NS
- Zonfiler

Sammanfattning av kursen (FL02)

- Roller hos namnservrar
  - Hosting
  - Resolver

Sammanfattning av kursen (FL03)

- Typer av DNS-svar
  - Auktoritativt svar
  - Icke-auktoritativt svar
  - Hänvisning (referral)
- Flaggor i DNS-paketet
  - QR, AA, TC, RD, RA, AD

Sammanfattning av kursen (FL03)

- Status i DNS-paketet (response)
  - NOERROR, FORMERR, SERVFAIL, NXDOMAIN, NOTIMP, REFUSED
  - NODATA (psuedo-status)
  - Timeout (ingen status)
  - Lame delegation
- Message ID i DNS-paketet

Sammanfattning av kursen (FL 3)

- Rot-zonen
  - Toppen av DNS-trädet
  - Hint-fil, namnservrar för root
  - Flera rot?
- Transportprotokoll och paketstorlek
  - UDP och TCP
  - 512 byte i UDP
  - Trunkering, TC och omsändning

Sammanfattning av kursen (FL03)

- Port 53
- Utökning av DNS – EDNS
  - OPT
  - FORMERR vid icke-stöd
  - Vad tillför EDNS?
    - Bl.a. höjd UDP-gräns
  - Query och response med EDNS

Sammanfattning av kursen (FL03)

- Paketstorlek och fragmentering
  - Fragmentering i IPv4 och IPv6
  - Begränsa fragmentering
- Frågetype kontra posttyp
  - * (ANY)
- DNS-paketets uppbyggnad
  - RFC 1035, 4.1, s 25
  - Återspeglas väl i output från "dig"

Sammanfattning av kursen (FL03)

- Glueposter
  - Används i delegeringen
  - Strikt glue
  - Icke-strikt glue

Sammanfattning av kursen (FL04)

- Zonfil och zonfilsformat
  - Zonfilsformat
  - $TTL
  - $ORIGIN, @ och default domän
  - Apex
  - Relativa och absoluta namn
  - Kommentarer

Sammanfattning av kursen (FL04)

- Master och slav
  - Roller
  - Kan sättas upp olika
  - Dold master, dold slav
  - Hitta mastern, hitta slavarna
- Konfigurering av master och slav i bind
- Zonöverföring och synkronisering
  - SOA-postens roll för synkronisering

Sammanfattning av kursen (FL04)

- Serienummer
- AXFR, IXFR
- NOTIFY
- Begränsa zonåtkomst
  - Med IP-adress
  - Med TSIG
  - Konfigurera begränsning i bind

Sammanfattning av kursen (FL05)

- Svar från namnserver i olika scenarior
  - Resolver öppen för oss
  - Resolver stängd för oss
  - Hosting av aktuell zon
  - Hosting av överliggande zon till aktuell zon
  - Hosting av andra zoner
  - Flaggor och status
- RRset

Sammanfattning av kursen (FL05)

- Cachning och TTL
  - Resolvning och cachning
  - För- och nackdelar med cachning
  - Hur bestäms och sätts TTL?
- Cachning av negativa svar
  - NODATA, NXDOMAIN
  - Hur bestäms och sätts TTL?

Sammanfattning av kursen (FL05)

- Resolvning
  - Detaljerat för www.dn.se
- CNAME
  - Som query type
  - I answer section
  - Med NODATA, NXDOMAIN och referral

Sammanfattning av kursen (FL06)

- Moderzon, dotterzon och delegering
- Ordning i ett RRset
  - Vilket ordning har DNS-posterna?
  - Vilken DNS-post ska klienten välja?
  - Fixed, random, cyclic
- Cache poisoning
  - Man-in-the-middle
- Falsk resolver eller modifierande resolver

Sammanfattning av kursen (FL06)

- Bortglömd NS
- Öppen zonfil
- Öppen resolver
  - DOS- och DDOS-attack
- Amplification
  - Resolvrar som redskap för DOS -attacker
  - DOS-attack via resolver

Sammanfattning av kursen (FL06)

- Är UDP ett problem
- DNS-trafik i klartext
  - Query name minimisation
  - Måste DNS-frågan visas överallt?

Sammanfattning av kursen (FL07)

- DNSSEC
  - Verifiering av innehåll
- Krypto
  - Asymmetriskt, symmetriskt
- Hash eller checksumma
- Signaturer
  - Krypterad hash

Sammanfattning av kursen (FL07)

- Posttyper för DNSSEC
  - DNSSEC -- nyckel för DNSSEC
  - RRSIG – signaturer
  - NSEC -- Existerar eller inte
  - DS – tillitskedjan
- CNAME, RRSIG och NSEC

Sammanfattning av kursen (FL07)

- Domännamn utan data
  - Empty non-terminals
  - Aldrig "empty terminals"
  - NODATA, inte NXDOMAIN
  - Ingen NSEC-post

Sammanfattning av kursen (FL07-08)

- Validering
  - DS, DNSKEY, RRSIG
  - Valideing av RRset
- KSK och ZSK
  - Roller för DNSKEY
- Delegering och validering
  - DS i deleringen

Sammanfattning av kursen (FL08)

- DNSSEC frågor med "dig"
  - AD-flagga
  - DO-flagga
  - Validerat eller inte?

Sammanfattning av kursen (FL08)

- Delegering och DS
  - Delegering och DS
  - Byte av KSK
  - Byte av DS

Sammanfattning av kursen (FL08)

- CDS och CDNSKEY
  - Posttyper för att signalera byte av DS
  - CDS samma format som DS, olika funktioner och placering
  - CDNSKEY samma format som DNSKEY, olika funktioner men samma placering
- Zone walking
  - Zone walking med NSEC
    - Ibland går det att lösa

Sammanfattning av kursen (FL09)

- NSEC3
  - Alternativ till NSEC, samma funtion
  - NSEC3PARAM för NSEC3
  - Mera komplext
- CD-flagga
  - I "query"
  - Stäng av validering

Sammanfattning av kursen (FL09)

- Rotzonen och rotnamnservrar (FL09)
  - Hur många? 13 NS, men mer än 1000 servrar m.h.a. anycast

Sammanfattning av kursen (FL09)

- Toppdomäner (TLD)
  - Generiska, gTLD
  - Country-code, ccTLD
  - Infrastructure (endast arpa)
  - IDN ccTLD
- Registry, registrar och registrant
  - Roller för registrerat domännamn

Sammanfattning av kursen (FL10)

- Hitta namn från IP-adress
- Baklängesuppslagning
  - in-addr.arpa
  - ip6.arpa
  - Mest signifikant, minst signifikant
- Posttyp PTR

Sammanfattning av kursen (FL10)

- Användning av baklängesdata
- Uppslagning av in-addr.arpa
  - Som en vanlig domän
  - Revers speciell, speciellt format på namnet
    - IPv4 – label per decimal oktett i normalt format
    - IPv6 – label per hexadecimal siffra i explicit IPv6-format
  - Indirekt data via CNAME vid nät mindre än 256 addresser

Sammanfattning av kursen (FL10)

- Revers följer IP-adressen
  - IP-adresstilldelning styr delegeringen
- Hur in-addr.arpa-domäner delegeras
- Baklängesuppslagning av IPv6-adresser
- DNS-poster i reverszoner
- Låt "dig" konvertera
- Privata adresser och baklängesuppslagning

Sammanfattning av kursen (FL11)

- Tillgänglighet
  - Tillgänglighet till resolver
  - Tillgänglighet till zondata
- Anycast – ger bättre tillgänglighet för zondata

Sammanfattning av kursen (FL11)

- Krypterad DNS
  - DNS över TLS, DoT
    - TLS med ceritifikat
    - Port 853 över TCP
  - DNS över HTTPS, DoH
    - TLS med ceritifikat, som vanlig HTTPS, port 443
  - DNS över Quic, DoQ
    - TLS med certificat, över Quic (HTTPS över UDP), port 853

Sammanfattning av kursen (FL11)

- TXT-poster för mailkontroll
  - SPF
  - DKIM
  - DMARC

Sammanfattning av kursen (FL11)

- Posttyp SRV
  - Servicenamn och transportprotokoll bakas in i "owner name"
  - Liknar MX, men fler fält
- DANE
  - Lagra TLS certifikat
    - Förutsätter DNSSEC
  - Posttyp TLSA
  - Owner name som RSV

Sammanfattning av kursen (FL12)

- Nya domännamn
  - Krav på utökad teckenuppsättning
  - IDN = Internationalized domain name, IDNA2008
  - Unicode
  - Begränsat till "ordtecken"
    - Bokstäver och motsvarande tecken för olika språk
    - Siffror
    - Vissa skiljetecken

Sammanfattning av kursen (FL12)

- Inte versaler
- Unicode-tecken får inte plats i DNS-paketet utan omkodning
- Kompatibelt med DNS och domännamn

- IDN – label inte hela domännamnet
  - A-label – omkodat till ASCII med inledande xn--
  - U-label – samma IDN-label med avsedda tecken
  - Vanlig ASCII-label är varken A-label eller U-label

Sammanfattning av kursen (FL12)

- Använd modern "dig" eller annat verktyg för omkodning
  - Omkodningen är vändbar

Sammanfattning av kursen (FL13)

- Wildcard-label (*)
  - Sätts i zonfilen
  - Måste vara hel label
  - Måste vara första label
  - Matchar alla namn som inte är definierade

Sammanfattning av kursen (FL13)

- Olika vyer av DNS-trädet
  - Skapa olika vyer av samma domän
  - Som virtuella namnservrar.

▶Utvärdering av kursen

[Innehåll]

Utvärdering

Har dina förväntningar på kursen uppfyllts?

Kommentarer eller synpunkter?

▶Om presentationen

[Innehåll]

Internets domännamnssystem

Denna presentation är framtagen 2019–2024 av Mats Dufberg (mats.dufberg@internetstiftelsen.se) på Internetstiftelsen (https://internetstiftelsen.se/). Den är en del av undervisningsmaterialet för kursen ”Internets domännamnssystem” vid Kungliga tekniska högskolan, KTH (kurskod HI1037) resp. Karlstads universitet, KAU (kurskod DVGC28).

Licens

Dokumenthistorik

- Rev A: Ursprunglig version VT 2024
- Rev B: Några rättelser i facit.

Slut.