


DNS (T-Mobile)

Dinko Korunić, InfoMAR
v1.0, veljača 2009.



Tijekom prezentacije

- ako što nije jasno - **pitajte!**
- ako što nije točno - **ispravite!**
- **diskusija** je poželjna i produktivna
- monolog je zamoran i dosadan, kako polaznicima tako i predavaču

Sadržaj

1. uvod, hijerarhija, komunikacija, klijent
2. oznake, domene, rezolucija, zone, upiti
3. reverzna rezolucija, paket, zaglavlja, polja
4. rr, osnovni zapisi, točke
5. kružno posluživanje, dodatni zapisi
6. tipovi poslužitelja, praksa, prijenos zone
7. delegacija, delegacija pod mreže
8. dinamički dns, alati, sigurnost, analizatori
9. trovanje, zagađenje, istraživanje, kraj

O predavaču

- 1999-, SRCE: Debian Linux paketi, sigurnosne forenzike, istraživanja, predavanja i seminari vezani uz Unix/Linux, sistemsko programiranje, konzalting
- 2004-, CARNet: isto...
- 2000-, BUG/Mreža: Linux radionica, testovi mrežne opreme i poslužitelja, specijalizirani članci
- 2004-, InfoMAR: Linux/Unix sigurnosni specijalist
- 15ak različitih produkcijskih DNS poslužitelja, različitih veličina, DNS predavanja diljem HR (ECS, Končar, SRCE/CARNet, itd.), vlastita DNS knjiga/priručnik, DNS IDS, ...

Uvod u DNS

- hijerhijski, imenički i distribuirani sustav
- jedan od osnovnih protokola na Internetu
- tri osnovne funkcije:
 - DNS imenički prostor, specifikacije domena
 - registracija domena i administracija: struktura nadležnih tijela, procedura registracije domena, administracija zona i hijerarhije,
 - poslužitelji i rezolucija: DNS zapisi i zone, tipovi i uloge DNS poslužitelja, proces rezolucije, DNS poruke, formati i zapisi

Uvod u DNS (2)

- skriven u pozadini većine aplikativnih protokola (HTTP, SSH, FTP, POP3, IMAP4, ...) - pamtimo slovne labele umjesto adresa
- slovni naziv = host name
 - koristi se za adresiranje računala
 - jedna riječ ili više riječi odvojeno točkama
 - nije nužno jedinstveno (npr. DNS load-balancing)
- sufiks, domensko ime = domain name
 - više računala dijeli isto domensko ime

DNS komunikacija općenito

- DNS poslužitelji
 - koriste DNS protokol međusobno i prema DNS klijentima
 - standardno: 1 upit, 1 odgovor, max 512 bajtova UDP
 - moguće više upita u 1 paketu (rijetko), veći odgovori od 512 bajtova (EDNS0), TCP (kad je preko 512 ili prijenos zone)
 - moguće prenositi grupe podataka (prijenos zone)
 - u prosjeku 10ak tisuća upita u sekundi (QPS)

DNS klijent

- resolver
 - klijent koji pristupa DNS poslužitelju
 - libc rutine: `gethostbyname()`, `gethostbyaddr()`, `getnameinfo()`, `getaddrinfo()`
 - dns biblioteke: `adns`, itd.
 - dns helper proces: `Netscape`, `nscd`, itd.
- lokalna konfiguracija:
 - `/etc/nsswitch.conf`
 - `/etc/resolv.conf`
 - `/etc/hosts`

DNS klijent (2)

- konfiguracija informira sustav o lokaciji DNS poslužitelja (nužno koristiti IP adrese)
- /etc/resolv.conf
 - search LISTA_DOMENA
 - domain DOMENA
 - nameserver ADRESA
 - sortlist LISTA_DOMENA
- ako je DNS lokalno:
 - nameserver 127.0.0.1

Oznake, puna imena

- DNS oznaka / label:
 - maksimalno 63 znaka ukupno (pojedina oznaka)
 - slova A-Z te a-z, brojevi 0-9 i znak -
 - postoji lokalizacija, ali se ne primjenjuje globalno
- više oznaka (labela):
 - odvojene su međusobno točkama
 - tvore zajedno puno ime (FQDN)
 - puno ime je maksimalno 255 znakova ukupno
 - apsolutna staza unutar hijerarhije

Oznake, puna imena (2)

- ne razlikujemo velika i mala slova!
 - DNS.SRCE.HR = dns.srce.hr
- primjeri:
 - oznake: www, dns, smtp, t-mobile, srce, hr, com
 - FQDN: www.srce.hr, www.carnet.hr, mili.t-mobile.hr, vanili.t-mobile.hr, dns1.t-com.hr
- domena (TLD, krajnja desna oznaka): hr
- poddomena (SLD, predzadnja): t-mobile.hr
- kratko ime: www; FQDN: www.t-mobile.hr

Domene

- kratko ime je jedinstveno u domeni
- vršne domene - TLD:
 - gTLD: generičke tipa .com, .net, .org, .biz, itd.
 - ccTLD: geografski, ISO3166, oko 243 u upotrebi
- ICANN:
 - upravlja dodjelom i problematikom domena
 - neprofitno tijelo, locirano u Americi
 - nadležan za gTLD, dok su pojedine države za ccTLD
 - upravlja vršnim DNS poslužiteljima (13 komada)

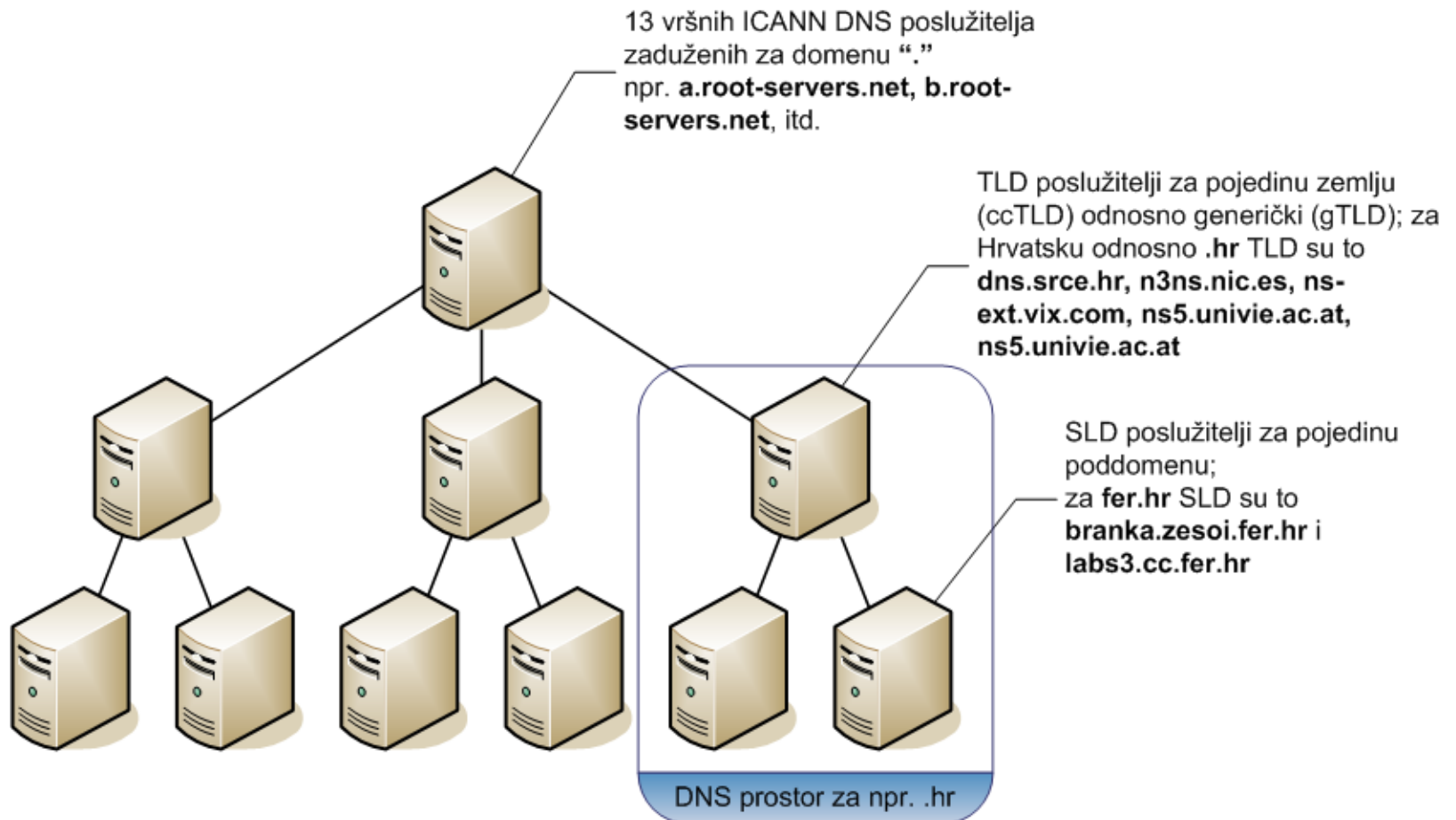
Domene (2)

- 13 vršnih poslužitelja:
 - a, b, c, ...
 - anycast i BGP, razmješteni po svijetu, fizički oko 150ak poslužitelja, prosječno 10ak tisuća QPS, nejednolika geografska distribucija
 - 98% prometa neispravan/pogrešan promet!
 - u prosjeku 10000-15000 QPS vršno
 - uglavnom Bind 9 poslužitelji
- TLD (.hr), SLD (.fer.hr), 3LD (.esa.fer.hr)

Domene (3)

- domenski registri
 - baze informacija o domenama i IP adresama
 - NIC, Network Information Centre
 - neprofitne, državne organizacije
 - WHOIS servis (za Europu: whois.ripe.net)
 - HR-DNS služba, CARNet, za .HR ccTLD, 28 tisuća domena u 2004., dns.srce.hr
 - ccTLD - obično pojedine države, 2-slovni zapis
 - gTLD - ICANN isključivo
 - alternative ICANN-u slabe/nepostojeće (ORSN)

Domene i hijerarhija



Rezolucija / razrješenje

- DNS sustav:
 - klijent: resolver, zadaje upite, nije nužno samostojeći
 - poslužitelj: odgovara na zadane upite ili prosljeđuje upit dalje
 - rekurzivni: prima (rekurzivni) upit od klijenta, umjesto njega obavlja iterativne upite prema drugim poslužiteljima i vraća finalni odgovor (ili grešku)
 - autoritativni/iterativni: prima (iterativni) upit i vraća odgovarajući odgovor iz lokalne baze ako su autoritativni za pitanje ili imenom nadležnog poslužitelja (delegiranje)

Rezolucija / razrješenje (2)

- DNS rezolucija:
 - razrješenje slovne labele u IP adresu
 - slanje DNS upita nadležnom DNS poslužitelju (rekurzivan)
 - traženje autoritativnog poslužitelja kroz DNS hijerarhiju
 - dobivanje odgovora ili greške od autoritativnog poslužitelja
 - prosljeđivanje tog odgovora ili greške klijentu, zajedno s originalnim upitom

DNS zona

- zona:
 - dio domene ili cijela domena
 - nalazi se na jednom poslužitelju (autoritativan za zonu!)
 - ne mora biti cijela domena zbog tehnike delegacije
 - npr. fer.hr poslužitelj vrši delegacije za svoje esa.fer.hr, zemris.fer.hr, itd. poddomene na pojedine poslužitelje iz poddomene
 - bitni su glue zapisi pri tome (NS i odgovarajući A)

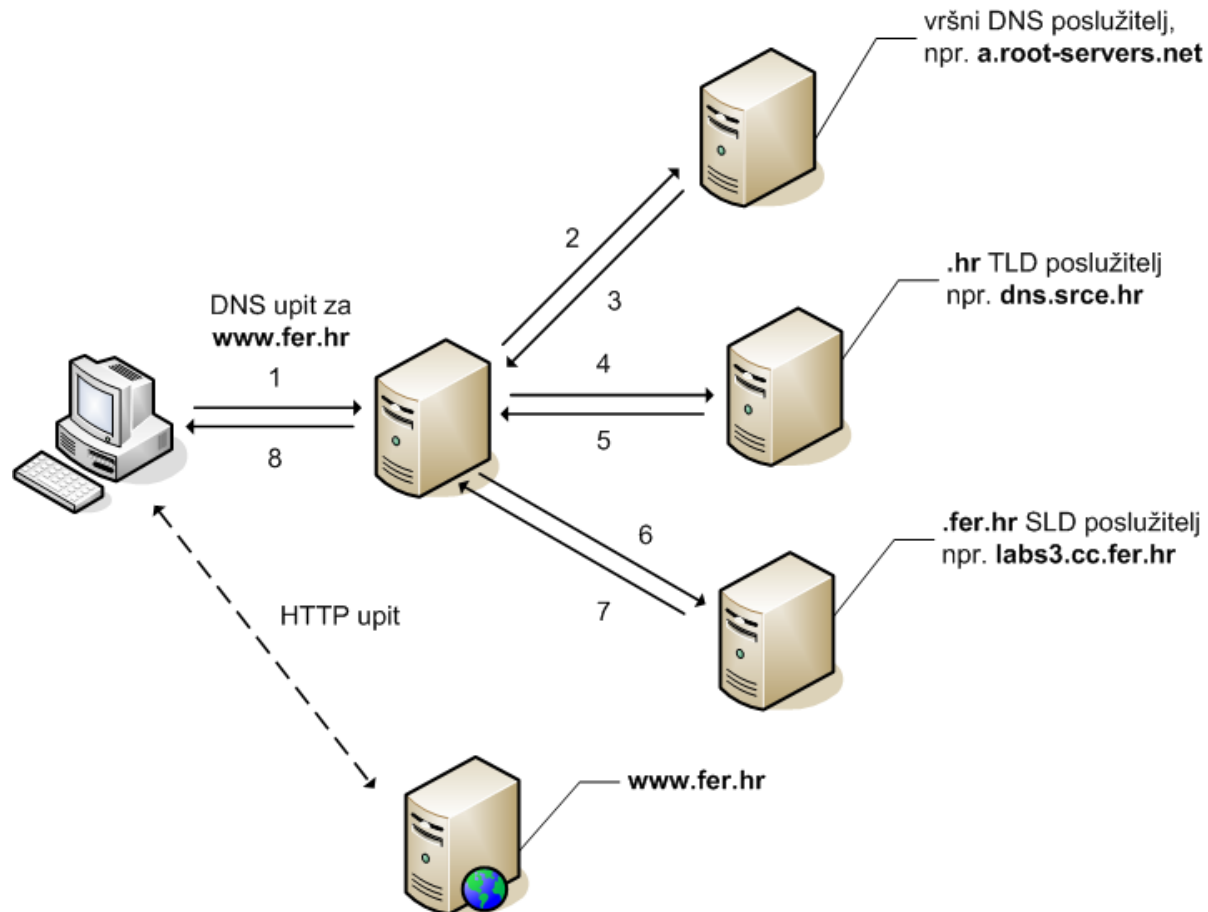
Prolazak kroz hijerarhiju

- iterativni:
 - na svaki upit se odgovara ili autoritativnim odgovorom ili odgovorom sa statusom greške
 - najviše posla obavlja klijent iterirajući kroz strukturu
- rekurzivni:
 - klijent šalje rekurzivni upit
 - poslužitelj obavlja niz iterativnih upita do pronalaženja zadane informacije
 - poslužitelj vraća klijentu odgovor ili grešku

Prolazak kroz hijerarhiju (2)

- iterativni:
 - minimalno opterećenje na poslužitelju
- rekurzivni:
 - minimalno opterećenje na poslužitelju
 - opasno ako je otvoren prema cijelom svijetu - DoS/DDoS opasnost!
 - nužno ograničiti pristupnim listama - obično samo za LAN ili barem poznate/vlastite IP raspone
 - zadajući posebno formulirane upite - moguće trovanje DNS poslužitelja!

Prolazak kroz hijerarhiju (3)



Prolazak kroz hijerarhiju (4)

```
$ dig +trace www.srce.hr
.                7829    IN      NS      L.ROOT-SERVERS.NET.
...
;; Received 484 bytes from 161.53.72.21#53(161.53.72.21) in 3 ms
hr.              172800  IN      NS      ns.uu.net.
...
;; Received 233 bytes from 199.7.83.42#53(L.ROOT-SERVERS.NET) in 138
ms
srce.hr.         86400   IN      NS      regoc.srce.hr.
srce.hr.         86400   IN      NS      bjesomar.srce.hr.
;; Received 104 bytes from 137.39.1.3#53(ns.uu.net) in 126 ms
www.srce.hr.    86400   IN      CNAME   regoc.srce.hr.
regoc.srce.hr.  86400   IN      A       161.53.2.69
srce.hr.        86400   IN      NS      regoc.srce.hr.
srce.hr.        86400   IN      NS      bjesomar.srce.hr.
;; Received 118 bytes from 161.53.2.69#53(regoc.srce.hr) in 0 ms
```

Prolazak kroz hijerarhiju (5)

- pretraživanje - uvijek od vrha, neefikasno, vrlo veliko opterećenje na vršne poslužitelje
- uvode se međuspremnicima:
 - prostorna lokalnost, vremenska lokalnost
 - pozitivni: pamte uspješne rezultate
 - negativni: pamte negativne rezultate
 - svaki zapis ima svoje vrijeme života (TTL)
 - implementiraju ih i klijenti i poslužitelji
 - minus: povećava se vrijeme propagacije promjena u DNS podacima! oprez!

Prolazak kroz hijerarhiju (6)

- svaki rekurzivni DNS poslužitelj ima popis vršnih DNS čvorova!
 - izmjene u adresama vršnih poslužitelja iznimno rijetke
 - root zona, nužna za normalan rad!
 - distribucija poslužitelja: <http://www.root-servers.org/>
 - službeno: <http://www.internic.net/zones/named.cache>

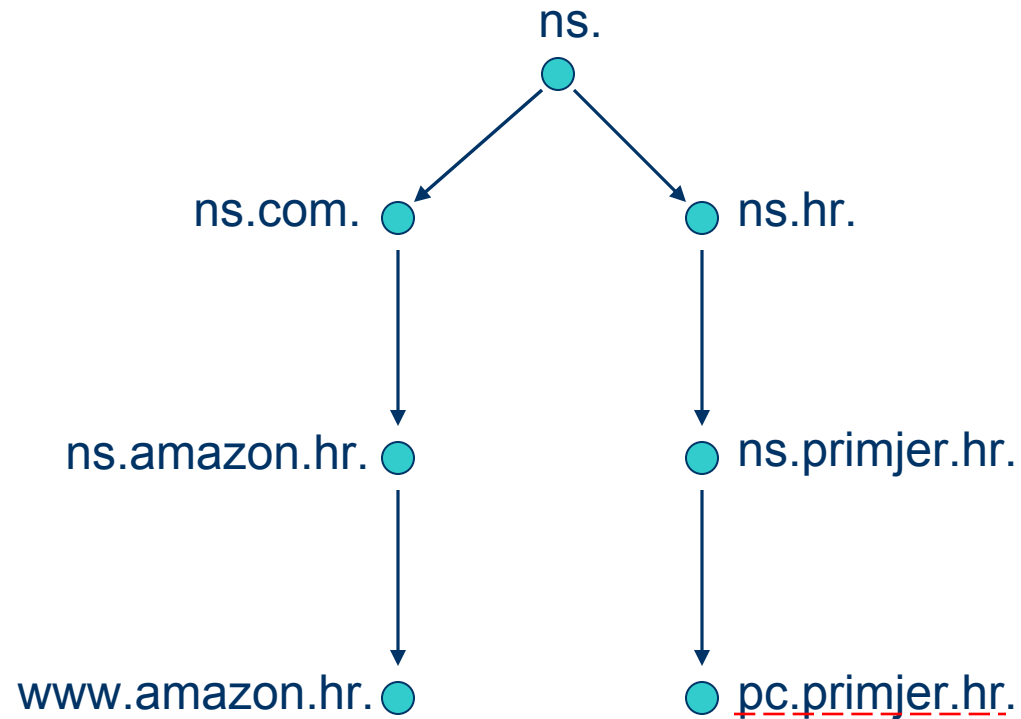
Rekurzivni i iterativni upiti

- upit također može biti rekurzivan ili iterativan:
 - rekurzivan: RD=1, označavamo da želimo od poslužitelja da obavlja rekurzivnu funkciju što on može odbiti
 - iterativan: RD=0, poslužitelj će dati konačan odgovor, delegaciju ili pak grešku
 - forsirajući npr. iterativni upit možemo lako doznati da li poslužitelj vrši delegaciju i ima li glue zapise za poddomenu

Vježba - rekurzivni, iterativni

- Slika prikazuje hijerarhiju DNS imena i DNS poslužitelje svake domene
- Uz pretpostavku da isključivo DNS poslužitelj **ns.primjer.hr** rekurzivno razrješava imena, prikazati tok razrješavanja imena **www.amazon.com** koje zahtijeva klijent **pc.primjer.hr**

Vježba - rekurzivni, iterativni (2)



Vježba - rekurzivni, iterativni (3)

1. **pc.primjer.hr** šalje rekurzivni (RD=1) upit za **www.amazon.com** na **ns.primjer.hr**
2. **ns.primjer.hr** od sad nadalje obavlja iterativne (!) upite, te počinje s **ns.** poslužiteljem (vršni) kojem šalje iterativni upit za **www.amazon.com** i od kojeg dobiva delegaciju na **ns.com** kao nadležni server za **.com** domenu

Vježba - rekurzivni, iterativni (4)

1. **ns.primjer.hr** šalje upit **ns.com** za **www.amazon.com** i dobiva delegaciju na **ns.amazon.com** kao nadležni za **amazon.com** domenu
2. **ns.primjer.hr** šalje upit **ns.amazon.com** i dobiva autoritativni (!) i konačan odgovor za **www.amazon.com**, te se rekurzija zaustavlja

Vježba - rekurzivni, iterativni (5)

- **ns.primjer.hr** salje neautoritativni (!) odgovor prema **pc.primjer.hr** sa adresom za **www.amazon.com**
- kraj upita, klijent je dobio odgovor ...
- s obzirom na količinu posla koju je obavio poslužitelj, sasvim je jasno i zašto je poželjno ograničiti pristup rekurzorima

Reverzna rezolucija

- IP adresa iz DNS imena
- dodatna hijerarhija: in-addr.arpa domena
- obrne se IP adresa (okteti su zapisani unazad) - 4 upita do razrješenja:
 - `t-mobile.hr A 195.29.178.175`
 - `175.178.29.195.in-addr.arpa PTR www.htmobile.com`
 - `175.178.29.195.in-addr.arpa PTR www.htmobile.hr`

DNS komunikacija

- portovi (IANA): tcp/53 i udp/53
- prvenstveno UDP, paketi do 512 bajtova
- jedan upit (uglavnom jedan QR u jednom paketu) - jedan odgovor (jedan ili više RR-ova)
- TCP se uglavnom ne koristi, osim:
 - kad odgovor prelazi 512 bajtova (TC=1)
 - kad se ne koristi EDNS0 tj. dogovor o veličini
 - kad je riječ o prijenosu zone (AXFR, IXFR)

DNS paket

- labele u odgovoru se sažimaju posebnim algoritmima
- lista od 13 poslužitelja - 512 bajtova, 1 paket
- odgovor uvijek sadrži i originalni upit!
- svaki paket ima 5 odjeljaka



DNS paket (2)

- zaglavlje: tip poruke, brojači zapisa, upit ili odgovor
- pitanje: QR (najčešće samo jedan)
- odgovor: RR (nula ili više)
- autoritet: RR (nula ili više), za delegaciju na nadležne DNS poslužitelje i nastavak komunikacije
- dodatno: RR (nula ili više), dodatne informacije npr. IP adrese auth. DNS-ova

Zaglavlje DNS paketa

- ID - identifier
- QR - query/response
- OPCODE - query, iquery, status, notify, update
- AA - authoritative answer
- TC - truncation flag
- RD - recursion desired
- RA - recursion available
- Z - 0
- RCODE - response code
- QDCOUNT - question count
- ANCOUNT - answer record count
- NSCOUNT - authority record count
- ARCOUNT - additional record count

Polje upita

- QNAME:
 - objekt, domena ili zona koja je predmet upita
- QTYPE:
 - tip RR koji se očekuje ili poseban tip (IXFR, AXFR, ANY)
- QCLASS:
 - klasa RR - tipično IN (Internet), podrazumijeva se
 - ostale klase (Chaos, Hesiod) se danas ne koriste

RR - Resource Record

- osnovna jedinica u DNS zoni (dio domene ili cijela domena na poslužitelju)
- sadrži grupu atributa: IP adresa, DNS oznaka, tekst, itd.
- sastoji se od:
 - imena domene: mora biti FQDN
 - TTL - u sekundama
 - klase zapisa: Internet, Chaos, Hesiod (podrazumijevano Internet, tipično se ne specificira)

RR - Resource Record (2)

- tip zapisa: CNAME, PTR, A, MX, TXT, AAAA, A6, NS, SOA, itd.
 - podaci za zapis - odgovaraju tipu zapisa, ako sadržavaju ime domene koje nije FQDN (nema točke na kraju), dodaje se cijelo ime domene
 - opcionalni komentar (ovisi o vrsti poslužiteljskog softvera)
- primjeri:
 - `t-mobile.hr. 57814 IN A 195.29.178.175`
 - `t-mobile.hr. 62187 IN NS mili.t-mobile.hr.`

Tipovi zapisa

- A - address
- CNAME - canonical name
- MX - mail exchanger
- PTR - pointer record
- NS - name server record
- SOA - start of authority
- DNAME - delegation name
- AAAA, A6
- SRV - server selection
- TXT - text string
- DS - delegation signer
- KEY - public key
- KX - key exchanger
- SIG - public key sign.
- TSIG - transaction sign.
- ...

Osnovni zapisi - SOA

- SOA (start of authority):
 - `srk.fer.hr. IN SOA fly.srk.fer.hr.
postmaster.fly.srk.fer.hr. (
200201071 28800 7200 604800 86400)`
 - serijski broj, vrijeme osvježavanja, vrijeme za ponovni upit, vrijeme trajanja zone, minimalni TTL
- server dokazuje da je autoritativan - ako ga nema, to je "lame" server (greška!)
- serijski broj - važan zbog odluke o prijenosu zone, najčešća greška

Osnovni zapisi - SOA (2)

- serijski broj: verzija podataka u zoni, mora se ručno ili automatski povećavati
- vrijeme osvježavanja: koliko sekundarni čeka između pojedinih osvježavanja zone
- vrijeme ponovnog pokušaja: čekanje nakon neuspješnog prijenosa zone, eliminacija masovnih prijenosa
- vrijeme isteka: nakon kojeg sekundarni proglasi svoje informacije zastarjelima

Osnovni zapisi - SOA (3)

- tipične greške u SOA:
 - zaboravi se povećati serijski broj nakon promjene
 - krivi serijski broj; tipično se koriste dva oblika:
 - `YYYYMMDDnn`
 - `YYYYMMDDn`
 - e-mail adresa u krivom obliku; tipično je dozvoljeno samo:
 - `korisnik.posluzitelj.domena.`
 - zaboravljene točke na kraju zapisa u SOA - automatski se dodaje ime domene na kraj!
 - SOA mora biti prvi zapis u zoni, pa slijede NS

Osnovni zapisi - SOA (4)

- krivi serijski broj u SOA... što sad?
 - problem: prenese se i na sekundarne poslužitelje, te eventualno ometa prijenos zone!
 - Bind 9: na originalni krivi se dodaje 2147483647 ($2^{31}-1$) i ponovno učitava zona
 - nakon toga se prenese takva zona na sekundarne poslužitelje

Osnovni zapisi - NS

- NS (nameserver):
 - poslužitelji za zadanu domenu
 - oznaka autoriteta (oznake s lijeve strane jednake domeni) ili delegacija (oznake sadrže poddomene)
 - poslužitelj se koristi NS listom kad šalje NOTIFY nakon što je promijenjena zona i povećan serijski broj u SOA
 - `srk.fer.hr. NS fly.srk.fer.hr.`
 - `srk.fer.hr. NS burek.srk.fer.hr.`

Osnovni zapisi - A

- A (address):
 - povezuje DNS oznaku sa IPv4 adresom
 - može više istih A zapisa pokazivati na različite IPv4 adrese
 - moguće primitivno razdjeljivanje opterećenja, bez detekcije pada poslužitelja (round-robin)
 - **fly.srk.fer.hr. A 161.53.70.130**
 - **fly.srk.fer.hr. A 161.53.70.131**
 - **burek.srk.fer.hr. A 161.53.70.132**

Osnovni zapisi - MX

- MX (mail exchanger):
 - nadležni SMTP/SMTSPS poslužitelji za oznaku ili cijelu domenu - ako ne postoji, koristi se A zapis
 - omogućava definiranje "cijene" i jednostavno (primitivno) raspodjeljivanje opterećenja - kreće se sa nižim cijenama dok se ne uspije isporučiti
 - naspram SRV: nema alternativnih portova
 - ne smije biti CNAME (potencijalno neispravni)
 - `srk.fer.hr. MX 5 fly.srk.fer.hr.`
 - `srk.fer.hr. MX 10 burek.srk.fer.hr.`

Osnovni zapisi - PTR

- PTR (pointer):
 - povezuje IPv4 adresu sa DNS oznakom
 - isključivo in-addr.arpa oblik sa obrnuto zapisanim oktetima
 - problem - samo 4 razine u hijerarhiji! što kad je potrebno dijeliti segment na manje od /24 raspona?
 - **130 PTR fly.srk.fer.hr.**
 - **132 PTR burek.srk.fer.hr.**

Osnovni zapisi - CNAME

- CNAME (canonical name):
 - omogućava da jedna oznaka bude zamjensko ime za drugu, ne nužno iz iste domene
 - takvo zamjensko ime ima sve osobine originala (na koji pokazuje), ali mu treba dodatni DNS upit (!) za razrješenje - smanjena efikasnost
 - postoje restrikcije na upotrebu: ne smije koegzistirati niti s jednim drugim zapisom za pojedinu DNS oznaku!
 - `www.srk.fer.hr. CNAME fly.srk.fer.hr.`

Osnovni zapisi - TXT

- TXT (text):
 - unos teksta kao opisa neke DNS oznake
 - danas se koristi i u druge svrhe tipa SPF, odnosno sprečavanje neželjene pošte
 - `igh.hr. TXT "v=spf1 mx -all"`
 - `www.igh.hr. TXT "Web poslužitelj"`

Osnovni zapisi - *

- jedan zajednički zapis umjesto više
- ograničenja:
 - istog su tipa (A, CNAME, PTR)
 - pokazuju na isti podatak (adresu, IP)
 - u istoj su zoni (važno!)
- primjer:
 - `ns2 A 192.168.0.2`
 - `* A 192.168.0.1`
 - `lists MX 10 mail`

Osnovni zapisi - * (2)

- primjenjuje se ako nema preciznijih (boljih, odgovarajućih) zapisa (!)
- omogućava da se upiti za "nepostojećim" oznakama preusmjere na neku koja postoji
- tipična upotreba:
 - vhostovi kod ISP-va, nije potrebno mijenjati DNS zapise a mogu se definirati novi virtualhostovi u Web poslužitelju

Točke u oznakama

- DNS oznaka može sadržavati točku:
 - pri tome je to i dalje normalna oznaka u svojoj uobičajenoj domeni (nije riječ o delegaciji!)
 - `burek.sir A 192.168.1.1`
- ako ne završava s točkom, dodaje se ime domene na kraj:
 - `www.t-mobile.hr. A 192.168.1.1`
 - `www A 192.168.1.1`

Kružno posluživanje

- round robin
 - jednostavno, jeftino, primitivno - load balancing
 - svaka n-torka (!) za istu oznaku se naizmjenično rotira pri odgovoru klijentima
 - slučajan odabir, statistički podjednako
- primjer:
 - `www A 10.0.0.1`
 - `www A 10.0.0.2`
 - `www A 10.0.0.3`

Kružno posluživanje (2)

- shemu odabira nije uvijek moguće mijenjati (ovisi po poslužitelju)
- nije moguće određivati cijene (usporedi sa SRV zapisom) i prioritete
- nema detekcije da li je npr. poslužitelj nedostupan ili preopterećen
- forward-reverse-forward provjera - ne vodi nužno do istog zapisa...

Ostali DNS zapisi - AAAA i SRV

- AAAA - IPv6 adresa:
 - `www.carnet.hr. AAAA`
`2001:B68:E160:0:20B:DBFF:FEE6:A4F0`
- SRV (service):
 - pametnija alternativa MX
 - definiraju se poslužitelji, težine, prioriteti i portovi za pojedini mrežni servis
 - Microsoft Active Directory / DNS: `_udp`, `_tcp`, `_msdcs`, `_sites`
 - OpenLDAP: `_ldap`

Ostali DNS zapisi - SRV

- SRV:
 - Web sa različitim težinama (omjer koliko se često koristi koji zapis) za isti prioritet:
 - `_http._tcp SRV 0 1 80 www1`
 - `_http._tcp SRV 0 3 80 www2`
 - MS AD:
 - `_ldap._tcp.dc._msdcs SRV 0 0 389 msad`
 - `_ldap._tcp SRV 0 0 389 msad`
 - zabranimo ostale servise:
 - `*._tcp SRV 0 0 0 .`
 - `*._udp SRV 0 0 0 .`

Tipovi DNS poslužitelja

- autoritativni (authoritative):
 - ima kopiju cijele zone - nema potrebe za daljnjom rezolucijom kad dobije upit za objektom iz te zone
 - poslužitelj može biti autoritativan za više zona
 - serviraju se vlastiti podaci klijentima (i drugim poslužiteljima)
 - greška u SOA i NS poljima - poslužitelj može imati cijelu zonu, a smatrati da nije autoritativan (AA=0)
 - poželjno je imati više autoritativnih za jednu zonu

Tipovi DNS poslužitelja (2)

- autoritativni:
 - tipično se koriste 2 poslužitelja: primarni i sekundarni - oba imaju cijelu kopiju zone za koju su autoritativni
 - u slučaju da jedan ne radi - drugi svejedno odgovara na upite (nakon što klijentov upit prema prvome timeouta ili biva odbijen)
 - sekundarni nekom tehnikom (AXFR, IXFR, SSH, rsync, itd.) prenosi zonu od primarnog nakon promjene: povećava se serijski broj u SOA i pošalje NOTIFY paket

Tipovi DNS poslužitelja (3)

- autoritativni:
 - ako nema sekundarnog - nakon isteka TTL-a po klijentima, svi zapisi o zoni nestaju!
 - upiti se dijele statistički podjednako između više autoritativnih poslužitelja po round-robin principu
 - postoje isključivo autoritativni poslužitelji:
 - nemaju omogućenu rekurziju (PowerDNS, NSD, TinyDNS, Bind9 tek uz posebne zahvate)
 - razlog je sigurnost (rekurzija je potencijalno opasna), te pojednostavljenje koda poslužitelja

Tipovi DNS poslužitelja (4)

- međuspremnički (caching):
 - drže do isteka TTL
 - svi rekurzivni poslužitelji imaju i međuspremnike (pozitivni i negativni), neki autoritativni
 - razlog: smanjenje opterećenja na autoritativnim
- prosljeđivački (forwarding)
 - međuspremnički + prosljeđuje upite nekim daljnjim rekurzivnim poslužiteljima (ne prema krajnjim autoritativnim, već npr. ISP-ovim rekurzorima)

Tipovi DNS poslužitelja (5)

- skriveni poslužitelji (steath):
 - dio poslužitelja vidljiv izvana, a dio ne
 - poslužuje se tek dio informacija vanjskim klijentima (split view DNS)
 - mogući razdvojeni DNS poslužitelji: jedni za vanjske autoritativne odgovore, jedni za unutrašnje autoritativne odgovore

Popularni DNS poslužitelji

- BIND 4, 8, 9
- PowerDNS: pdns, pdns-recursor
- Djbdns: tinydns, dnscache, axfrdns
- NSD
- MaraDNS
- Unbound
- DNSmasq

Poslužitelji - dobra praksa

- razdvojiti autoritativni (vanjsko posluživanje zone) od rekurzivnog:
 - autoritativni: sluša na javno (cijeli svijet) dostupnoj IP adresi + eventualni split-view
 - rekurzivni: sluša na lokalnoj (LAN i/ili lokalni korisnici) adresi + strogo definirane pristupne liste (ACL)
- 2x svaki DNS poslužitelj
- autoritativni: PowerDNS, BIND, NSD
- rekurzivni: PowerDNS recursor, dnscache

Prijenos zone

- započinje UDP AXFR upitom
- vrši se provjera SOA polja (serijski broj)
- ostvaruje se TCP veza (isključivo) preko koje se u komadu prenosi cijela tražena zona
- česti prijenosi opterećuju poslužitelj
- varijante:
 - poruka obavijesti: NOTIFY
 - SQL baza i odgovarajuća replikacija
 - drugi modeli sinkronizacije: rsync, DRBD, SAN

Prijenos zone (2)

- AXFR: zona se prenosi u jednom, svaki put ispočetka
- IXFR: Bind 9, inkrementalni prijenos
 - poslužitelj vodi računa o promjenama i prenosi samo razlike (RR-ove)
 - potrebna podrška sa obje strane, inače se prebacuje na AXFR
- važno:
 - ograničiti kome je dozvoljen AXFR sa ACL-ovima
 - paziti na serial i refresh

Delegacija zapisa

- domena se dijeli u zone
 - koristeći NS zapise
 - delegiraju se dijelovi prema hijerarhijski podređenim DNS poslužiteljima
- ako su poslužitelji unutar zone (FQDN završava s rečenom domenom):
 - za normalno funkcioniranje potrebni povezujući (glue) zapisi, uzrok je "chicken and egg" problem
 - poslužitelji se prozivaju po DNS oznakama, a ne svojim IP adresama

Delegacija zapisa (2)

- primjer:
 - dns.srce.hr je ccTLD za hr
 - fer.hr poslužitelj mora imati povezujući zapis za fer.hr (barem jedan NS i barem jedan A) na dns.srce.hr
 - `$ dig +norecurse any fer.hr @dns.srce.hr`
 - `fer.hr. NS branka.zesoi.fer.hr.`
 - `fer.hr. NS labs3.cc.fer.hr.`
 - `labs3.cc.fer.hr. A 161.53.72.21`
 - `branka.zesoi.fer.hr. A 161.53.64.4`

Delegacija zapisa (3)

- konzistentnost delegacije:
 - zapisi na podposlužiteljima mora odgovarati onome na poslužitelju koji vrši delegaciju!
 - najčešća greška: korisnici mijenjaju NS zapise kod sebe i ne jave nadležnom DNS-u (HR DNS ili vlastiti ISP, itd.)
- lame delegation:
 - delegira se na poslužitelj koji smatra da nije autoritativan
 - nema NS i/ili SOA

Delegacija zapisa (4)

- lame delegation:
 - podaci istekli (sekundarni), a prijenos zone ne radi
 - uopće ne radi poslužitelj (refused ili uvijek vraća grešku)
- kružna ovisnost:
 - cyclic dependancy
 - dio jedne zone ovisi o drugoj koja vrši delegaciju na prvu

Delegacija pod mreže

- delegacija pod mreže bez upotrebe klasa:
 - popularna i česta!
 - uvedena zbog problema dijeljenja IP segmenata
 - reverzno razrješavanje nepraktično zbog /24 segmenata (256 adresa najčešće previše ...)
 - NS: poslužitelj za pod mrežu
 - PTR: povezuje kanonička imena prema reverznim adresama
 - CNAME: zamjenska imena radi pojednostavljivanja procesa

Delegacija pod mreže (2)

- varijante:
 - delegira se svaka IP adresa kao D klasa sa barem jednim NS zapisom za svaku (!) IP adresu; tko prima delegaciju mora imati zonu za svaku adresu (SOA, NS i PTR)
 - jednostavnija i popularnija varijanta: koristi se proizvoljan CNAME za svaku reverznu adresu (IP) u zoni, zamjenjujući PTR; labela se po konvenciji formira iz IP adrese, sufiks je domena kojoj se prosljeđuje; tko prima delegaciju treba imati samo PTR zapis

Delegacija pod mreže (3)

- primjer:
 - ns2.fpz.hr ima zonu 1-62.46.198.193.in-addr.arpa, odnosno 193.198.46.0/26 (1-62)
 - dns.srce.hr je nadležan za 198.193.in-addr.arpa, te direktno vrši delegaciju za 1-62.46 prema ns2.fpz.hr
 - adresa: 1.1-62.46.198.193.in-addr.arpa
 - 1-62.46.198.193.in-addr.arpa NS ns2.fpz.hr
 - 1 PTR r3-siget.fpz.hr.
 - 2 PTR sw1-siget.fpz.hr.
 - 3 PTR fw1-siget.fpz.hr.

Delegacija pod mreže (4)

- primjer 2:
 - vsa.hr, 193.198.50.0/25 raspon
 - reverzna zona: 0/25.50.198.193.in-addr.arpa.
 - 198.193.in-addr.arpa. - nadležan dns.srce.hr
 - 50.198.193.in-addr.arpa. - nadležan dns.carnet.hr
 - na nadležnom:
 - 9.50.198.193.in-addr.arpa. CNAME
9.0/25.50.198.193.in-addr.arpa.
 - 0/25.50.198.193.in-addr.arpa. NS ahil.vsa.hr.
 - na podposlužitelju (ahil):
 - 9 PTR ...

Dinamički DNS

- autorizirano udaljeno upravljanje (dodavanje, brisanje, izmjena) DNS zapisima
- dyndns, itd.
- najčešće: DHCP + DNS
- UPDATE poruka
- zone: jnl datoteke, oprez pri ručnom mijenjanju!

Tipični DNS alati

- upiti i detaljni odgovori: dig, host
- verzija poslužitelja: fpdns
- provjera zone: nslint, dnswalk, zonecheck
- statistike upita: dnstop
- prislušivanje: tcpdump, tshark, wireshark
- WHOIS informacije: whois, jwhois
- Web: MrDNS, IntoDNS, ...

DNS sigurnost

- kritičan servis sa brojnim problemima:
 - izvana: trovanje DNS-a (utiče na sve klijente!), napadi koristeći otvorene rekurzivne poslužitelje (npr. FER-ovi DNS poslužitelji) za DDoS svrhe
 - iznutra: trovanje (malware ili napadači), neispravne DNS konfiguracije (RFC1918 upiti, A-za-A upiti, upiti za krivim TLD-ovima, dinamički DNS, paketi neispravnog oblika, ...)
 - neispravni klijenti (Windows, stari Un*x)
 - neispravni/ranjivi poslužitelji (Bind4, Bind8, ...)
 - problemi u mreži se koncentriraju na DNS-ovima

DNS analizatori

- postojeći alati:
 - Snort IDS, dnstop, dnspktflow, Wireshark, dnscap
 - bilježenje DNS prometa, grafički prikaz, eventualni prikaz top DNS upita
 - **nisu specijalizirani**, nedostaje:
 - detekcija anomalija/incidenata/napada
 - bilježenje podataka u prezentiranom zapisu iz svih razina (Ethernet, IP, DNS, DNS upit, DNS odgovor)
 - distribuiranost + samostojeći rad
 - dobro skaliranje s opterećenjem, odgovarajuće performanse, itd.

DNS trovanje

- trikovi da DNS poslužitelj prihvati lažne zapise (DNS forgery)
- uzrokuje trovanje (poisoning) međuspremnik:
 - DNS poslužitelj smatra da je dobio autoritativne informacije
 - utiče na sve klijente (rekurzivni poslužitelj!)
 - DNS bailiwick (putanja) za detekciju suvišnih informacija
 - metode čišćenja "stabla" dobivenih informacija

DNS trovanje (2)

- `$ dig www.domain.nasty.foo @ns.nasty.foo`
- `;; ANSWER SECTION`
- `; prazno`
- `;; AUTHORITY SECTION`
- `domain.nasty.foo. NS www.google.com.`
- `domain.nasty.foo. NS www.cnn.com.`
- `;; ADDITIONAL SECTION`
- `www.google.com. A 10.1.2.3`
- `www.cnn.com. A 10.1.2.4`

DNS trovanje (3)

- `$ dig www.domain.nasty.foo @ns.nasty.foo`
- `;; ANSWER SECTION`
- `; prazno`
- `;; AUTHORITY SECTION`
- `com. NS ns1.domain.nasty.foo.`
- `domain.nasty.foo. NS ns2.domain.nasty.foo.`
- `domain.nasty.foo. NS ns3.domain.nasty.foo.`
- `;; ADDITIONAL SECTION`
- `ns1.domain.nasty.foo. A 10.1.2.1`
- `ns2.domain.nasty.foo. A 10.1.2.2`
- `ns3.domain.nasty.foo. A 10.1.2.3`

DNS trovanje (4)

- preusmjeravanje na zloćudnu domenu:
 - neki upit rezultira pretragom na zloćudnom, modificiranom poslužitelju
 - za neku domenu na modificiranom poslužitelju se u odgovoru daje vlastiti NS kao autoritativni
 - u dodatnom odjeljku istog odgovora se daje vlastiti A sa lažnim NS-om koji je nazivno u domeni koju trujemo (!)
 - napadnuti poslužitelj pamti IP adresu lažiranog NS poslužitelja i time se preusmjerava sav promet za tu domenu (microsoft.com na primjer ...)

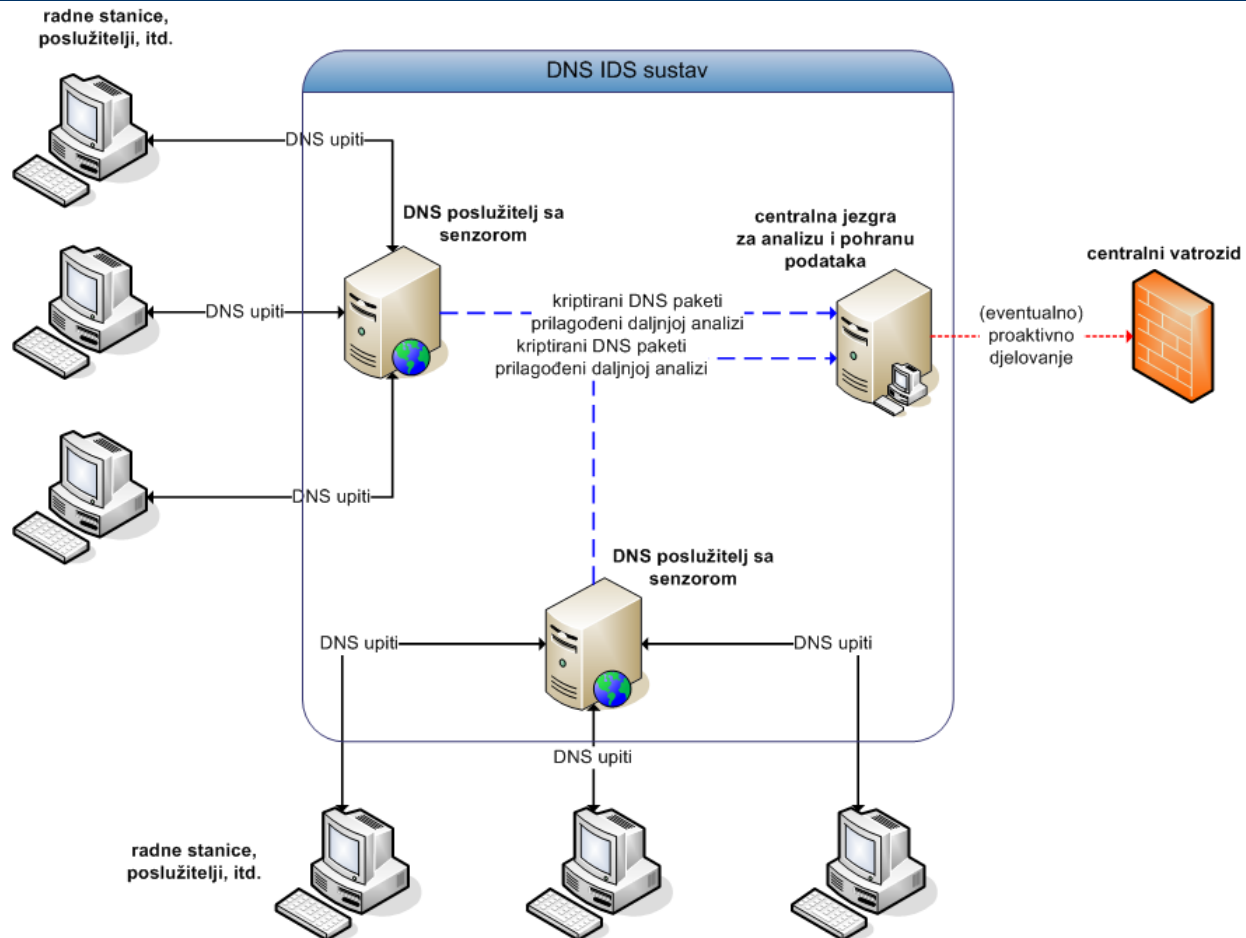
DNS trovanje (5)

- preusmjeravanje NS zapisa odredišne domene:
 - preusmjerava neku drugu domenu, nevezanu uz originalni upit
 - odgovara se u autoritativnom odjeljku sa NS zapisom u napadnutoj domeni
 - u dodatnom A zapis sa IP adresom tog NS
- napad identifikacijom:
 - predviđanje ID (pseudoslučajno), ako se pogodi broj tretira se kao ispravan odgovor

DNS zagađenje

- uzrok: raznorazne softverske greške i neispravna konfiguracija DNS klijenata
- neispravne DNS oznake u upitima (npr. dodan port na kraj oznake u upitu)
- nepostojeći TLD-ovi (local, localdomain, wpad, itd..)
- A-za-A upiti
- upiti za RFC1918/3330 adresama (privatne)
 - izrazito mnogo takvih upita, AS112 infrastruktura

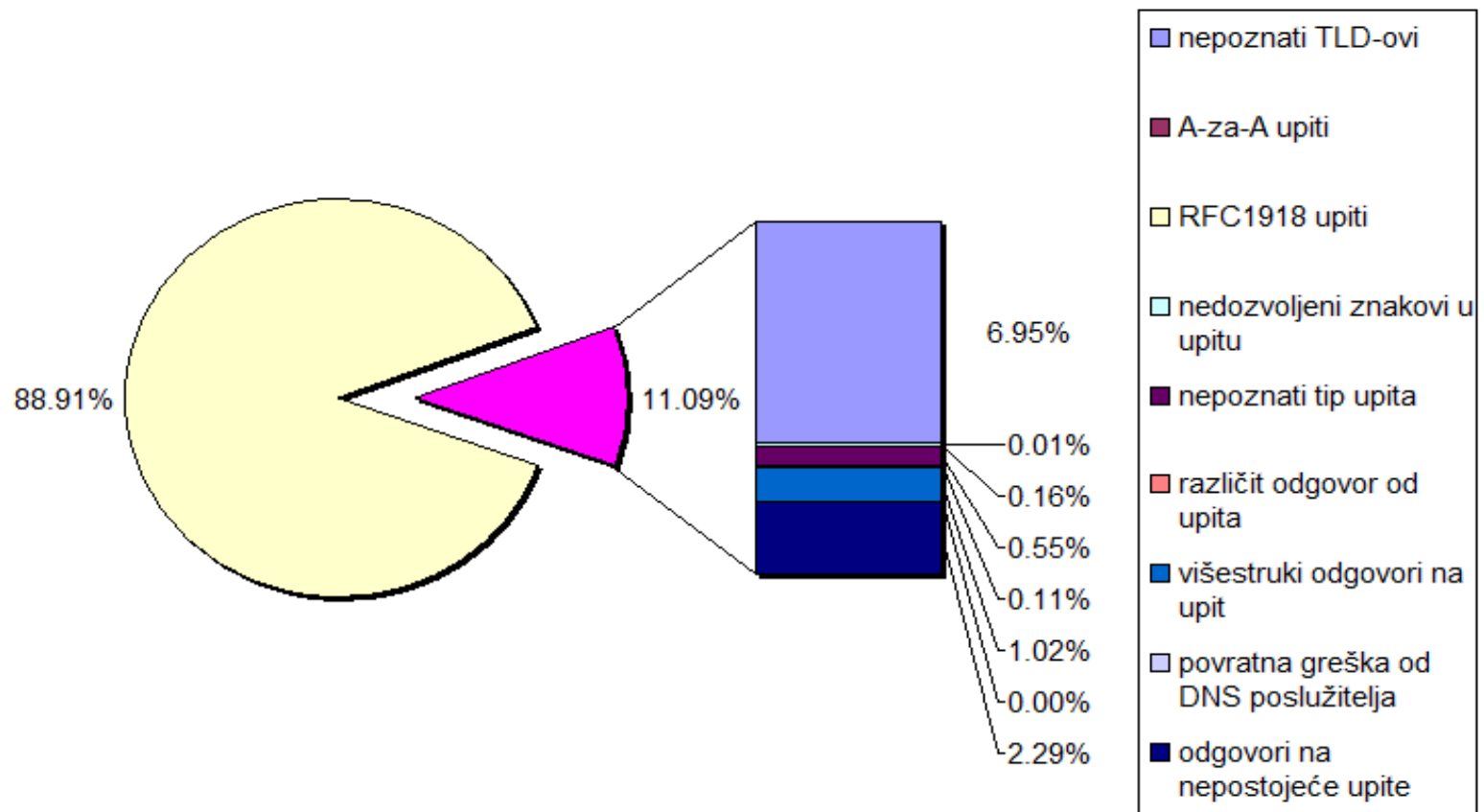
DNS IDS



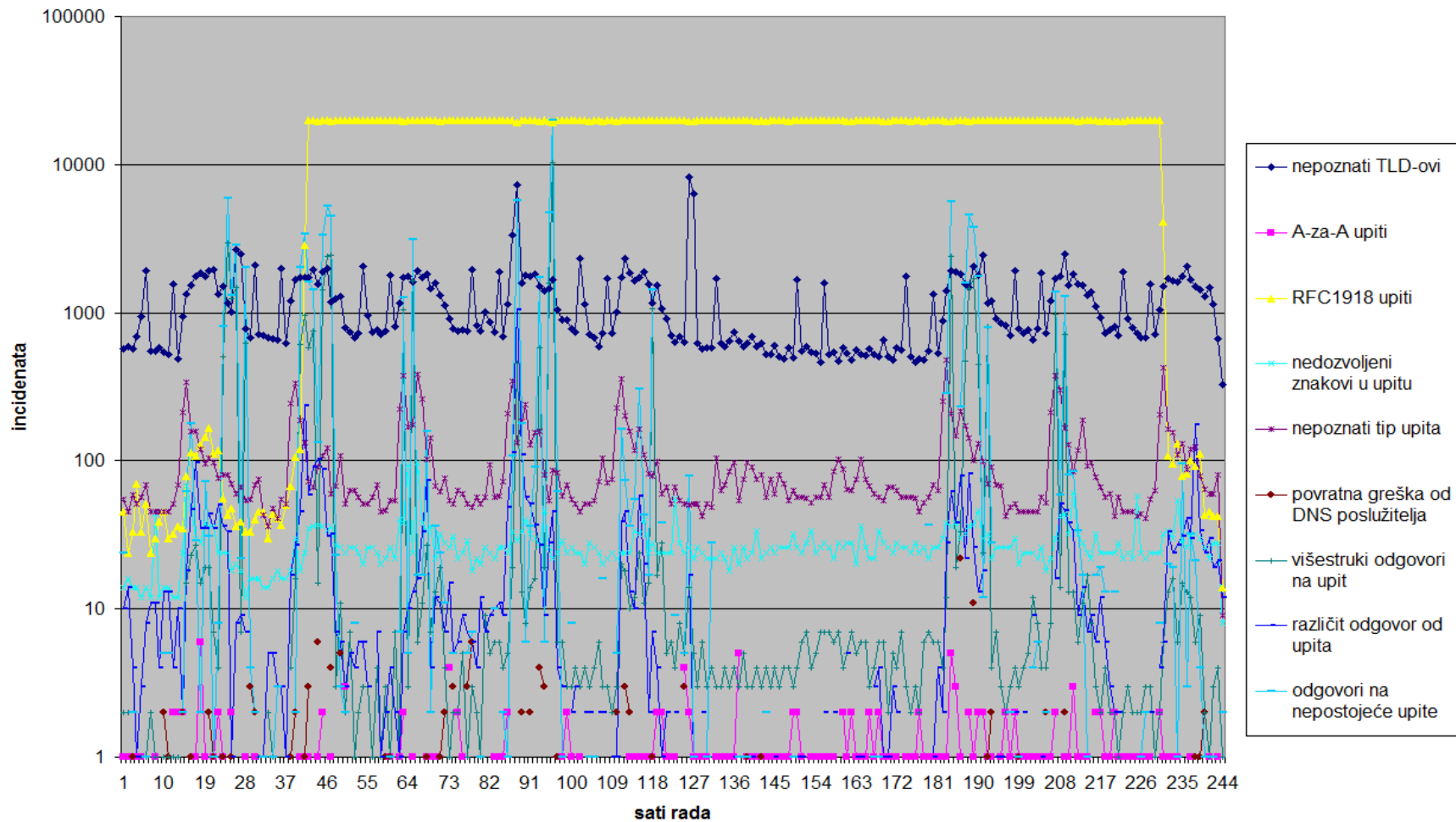
Rezultati - FSB

- mjerenje na centralnom FSB poslužitelju
 - 2000+ računala, različiti OS-ovi i okruženja
 - 243 radnih sati
 - 39 milijuna dolaznih i odlaznih DNS paketa
 - **4 milijuna** različitih incidenata: prosječno **170 tisuća** po satu, 11% ukupnog prometa
 - 7 tisuća pogrešaka u komunikaciji (neispravni paketi)
 - incidenti svih tipova i oblika ...

Raspodjela incidenata - FSB



Vremenski prikaz - FSB



Kraj

- pitanja, nejasnoće, diskusija?
- uočeni problemi u t-mobile DNS zoni:
 - dns1.t-com.hr naveden na T-Mobile DNS-ovima (mili, vanili) - stealth DNS
 - nije naveden na ccTLD HR DNS-ovima (samo mili i vanili jesu)
 - mili ne daje glue za dns1.t-com.hr, dok vanili daje
 - vanili je Bind 8... aktualna verzija je Bind 9.4