KRATKA POVIJEST DNS-a

Kako je sve počelo. Američko Ministarstvo odbrane (Department of Defense, DoD) odlučilo je uložiti novac u razvoj svoje nove mreže. On je povjeren organizaciji Advanced Research Projects Agency (ARPA). Zanimljivo je reći kako je uopće nastala sama ARPA: Amerikanci su osnovali tu agenciju za "napredna istraživanja" nakon što je 1957. Sovjetski Savez lansirao Sputnika, nadajući se da će im ta agencija pomoći da dostignu Ruse u svemirskoj utrci. Tako je 1968. nastala mreža ARPAnet, koja se smatra prethodnicom današnjeg Interneta. ARPAnet je bio eksperimentalni projekt, na kojemu je trebalo provjeriti mnoge stvari vezane uz mreže.

Sama mreža bila je zasnovana na tada novoj, a danas opće prihvaćenoj tehnologiji paketnog prespajanja. Smatra se da je Internet nastao onoga dana kada je Ministarstvo obrane odlučilo svoj ARPAnet povezati s nekim drugim javnim mrežama, sveučilištima i znanstvenim institucijama. Stvoren je protokol kojim se paketi prenose mrežom i nazvan je IP - Internet Protocol. "Internet" u tom trenutku još nije bilo ime mreže. Razvojem takvog protokola omogućeno je da međusobno komuniciraju različiti tipovi računala: bilo je samo važno da se međusobno dobro "razumiju". U početku, ARPAnet je spajao samo četiri institucije (uglavnom sveučilišne).

Kako se broj računala koji se povezuju preko mreže povećavao, bilo je potrebno ustanoviti jedinstven komunikacijski sistem koji bi regulirao promet na mreži. Tako je 1972. godine ustanovljena organizacija IANA (Internet Assigned Numbers Authority - www.iana.org) čiji je zadatak bio da dodjeljuje jedinstvene adrese svim računalima koja su na mreži. Tada je već 20 sveučilišta bilo u mreži. U početku su te adrese bile numeričke, tj. svako računalo je imalo svoj IP (Internet Protocol) broj - nešto kao kućni broj - na osnovu kog je svako računalo na mreži moglo biti locirano, tj. primati i slati pakete informacije.

Kako su mreža i broj korisnika rasli, bilo je sve teže pamtiti IP brojeve. Zbog toga je 1984. godine razvijen prvi Domain Name System (DNS), tj. distributivna baza podataka koja u osnovi sadrži sva imena svih računala i opreme koja su spojena na Internet, čime su Internet adrese dobile današnji oblik.

Sljedeći bitan događaj se dogodio 1991. godine kada se pojavio prvi komercijalni ISP i tako je, pored obrazovnih, naučnih i vojnih institucija, svaki korisnik mogao registrirati adresu na Internetu, čime je Internet ušao u javnu upotrebu. 1992. godine je oformljen InterNIC (www.internic.net), kvazi-vladina organizacija koja je organizirala i održavala registraciju domena.

Na početku su domene bile besplatne, ali kada je NSFNet (National Science Foundation Network) prestao sponzorirati registriranje novih domena, InterNIC je tražio 100.000 US$ za dvogodišnju registraciju domene. Zato je američko Ministarstvo trgovine tražilo da se raspodjela i upravljanje domenama prebaci na privatne organizacije. Veća konkurencija je automatski značila i sniženje cjena.

Godine 1998. je formiran ICANN (International Corporation for Assigned Names and Numbers - www.icann.org) - neprofitna, privatna korporacija, koja na principu konsenzusa koordinira tehničkim upravljanjem Internet Domain Name Sistema, raspodjelom IP adresa, parametara Internet protokola i brojeva portova, odnosno svih onih činioca čija jedinstvenost je preduslov za globalno funkcioniranje Interneta. ICANN je akreditirao veliki broj kompanija - registranata širom svijeta koje Internet korisnicima omogućavaju registraciju domena i tako je nastao Shared Registration System koji se i danas primjenjuje.

UVOD

Danas je na Internetu tzv. DNS jedan od osnovnih servisa, te je za to bitno njegovo shvaćanje i uporaba - čije ćemo temelje objasniti u ovom seminaru.

DNS (Domain Name System) je strogo hijerarhijski distribuirani sustav u kojem se mogu nalaziti različite informacije, no prvenstveno one o IP adresama i slovnim nazivima za računala. **Slovni naziv računala** (engl. hostname) je jedinstveno simboličko ime unutar pojedine mreže kojim se koriste neki protokoli (SMTP, NNTP) za elektroničku identifikaciju nekog računala. Takvi slovni nazivi mogu biti samo jedna riječ, ako se recimo radi o lokalnoj mreži; ili nekoliko riječi odvojenih točkama. Klijentima DNS informacije pružaju DNS **poslužitelji** (DNS servers), koristeći DNS protokol za komunikaciju kako sa klijentima tako i međusobno.

Svrha DNS sustava je pojednostavljivanje komunikacije među računalima u smislu olakšanog pamćenja slovnih naziva kao i mogućnosti tematskih i sličnih grupiranja računala koja nisu nužno logički blizu (logički blizu u smislu slijednih IP adresa). Jasno je, da je u svakodnevnom radu daleko lakše koristiti i pamtiti slovna i smislena imena umjesto odgovarajućih IP adresa.

DNS sustav je naravno puno širi, te obuhvaća tri osnovne funkcije sa različitim segmentima koje ćemo objasniti u daljnjem tekstu:

1. DNS imenički prostor, problematiku imenovanja i pravila: karakteristike su hijerarhijska struktura, imenička struktura i pravila imenovanja te specifikacije domena
2. registraciju domena i ostale administrativne probleme: hijerarhijsku strukturu nadležnih tijela, hijerarhiju vršnih nadležnih tijela (TLD), procedure registracije sekundarnih domena, administraciju DNS zona i administraciju hijerarhije
3. poslužitelje i proces rezolucije: DNS zapisi i zone, tipovi DNS poslužitelja sa različitim ulogama, procesi rezolucije, DNS poruke, formati i zapisi

DOMENSKO IME

Domensko ime je simboličko ime računala na Internetu koje ga uglavnom (postoji mogućnost da više računala dijeli jedno domensko ime) jedinstveno označuje. DNS sustav vrši preslikavanje domenskog imena u jednu ili više IP adresa te obrnuto, preslikavanje jedne ili više IP adrese u jedno domensko ime. Na većini modernih operacijskih sustava se DNS sustav koristi implicitno, pa je moguće nekom računalu na Internetu pristupiti kako kroz odgovarajuću IP adresu, tako i kroz domensko ime - ako ono postoji.

Domensko ime se često naziva i **labela** (engl. label), iako je po definiciji pojedina labela alfanumerički niz znakova sa maksimalno 63 znaka unutar pojedine labele. Više takvih labela se međusobno odvaja točkama, a tek zajedno one tvore domensko ime, koje se u takvoj potpunoj formi (navedene su sve labele) zove i **FQDN** (Fully Qualified Domain Name). Takvo ime je maksimalne dužine od 255 znakova, a različito od običnog domenskog imena (koje može biti i kratkog oblika, sadržavajući svega dio labela) po tome što predstavlja apsolutnu stazu unutar DNS hijerarhije.

Primjer 1: Domenska imena, FQDN, labele

```
FQDN: sirius.phy.hr, 12tesla.phy.hr
labele: sirius, 12tesla, phy, hr
```

```
ime računala: sirius, 12tesla, www
domensko ime: sirius.phy
```

Napomenimo još jednom - svaka labela se sastoji od isključivo alfanumeričkih znakova i znaka "-" (dakle ASCII znakovi od A do Z i znak "-"), pri čemu se labele ne razlikuju po velikim i malim slovima. Danas je u procesu prihvaćanja novi sustav koji bi trebao dozvoliti i ne-ASCII znakove u labelama, tzv. IDNA (engl. Internationalizing Domain Names in Applications). Da bi se FQDN dodatno razlikovao od labela odnosno standardnih (ne nužno potpunih) domenskih imena, česta je konvencija dodavanja **dodatne točke** (znaka ".") na kraj domenskog imena.

Da ponovimo: domensko ime se sastoji od dvije ili više labela odvojenih točkama. Krajnje desna labela je TLD (Top-Level Domain), a svaka druga labela lijevo je **poddomena** - domena koja je hijerarhijski ispod prethodne. Ukupno maksimalno podjela može biti 127, dok se držimo zadane granice od 255 znakova za FQDN. Na kraju, labela koja je krajnje lijeva je kratko ime računala (već spomenuti slovni naziv računala, dakle bez domene).

DOMENE

Domenska imena su obično grupirana; ona završavaju pojedinom grupom labela za koje postoje točno definirana pravila. Takve završne labele se nazivaju **TLD** (Top-Level Domain) imena, kojih postoje dva tipa:

- geografski bazirane domene, tzv. **ccTLD** (engl. country code TLD) domene koje predstavljaju državni dvoznakovni kod temeljen oko ISO-3166 standarda, a danas ih ima preko 240 u upotrebi
- generičke domene, tzv. **gTLD** (engl. generic TLD) domene koje se obično sastoje od 3 ili više znakova

U pojedinoj domeni, odnosno **domenskom prostoru** ne mogu postojati dvije iste labele - što znači niti dvije poddomene niti dva računala.

Primjer 2: TLD-ovi

```
gTLD: .com, .net, .org, .biz, .info, .museum, .travel, .xxx
ccTLD: .hr, .us, .eu, .fr, .es, .de, .it, .jp, ...
```

Za dodjelu i upravljanje problematikom domena, zaduženo je **ICANN** (Internet Corporation for Assigned Names and Numbers) neprofitno tijelo. Ova relativno mlada organizacija je preuzela poslove koje je nekad obavljala **IANA** (Internet Assigned Numbers Authority). Specifično, riječ je o upravljanju dodjeljivanjem domena i IP adresa, pri čemu se lokalna registracija IP adresa predaje pojedinačnim RIR-ovima (Regional Internet Registries). Svaki RIR alocira adrese za različiti dio svijeta.

DOMENSKI REGISTRI

Slično kao i za IP adrese, postoje **domenski registri**, baze podataka o domenama i odgovarajućim IP adresama, po jedan za svaku TLD. Oni kao uslugu daju domenska imena za vlastitu TLD te omogućavaju ostatku svijeta pregled informacija o registracijama pojedinih

domena. Domenski registri se inače nazivaju **NIC** (Network Information Centre), te su najčešće neprofitne ili državne organizacije. Informacije o registracijama su dostupne kroz **Whois** sustav, pa je tako za Europu nadležan whois.ripe.net poslužitelj (primjer dobrog Whois klijenta je **Jwhois**, sa ugrađenim bazama lokalnih registara). Svaki registar upravlja DNS poslužiteljima za specifični TLD, pa je to za Hrvatsku (.HR) dns.srce.hr kojim upravlja HR-DNS služba za CARNet. Dakle, za ccTLD-ove su obično nadležne vlade pojedine države, dok je za gTLD nadležan isključivo ICANN.

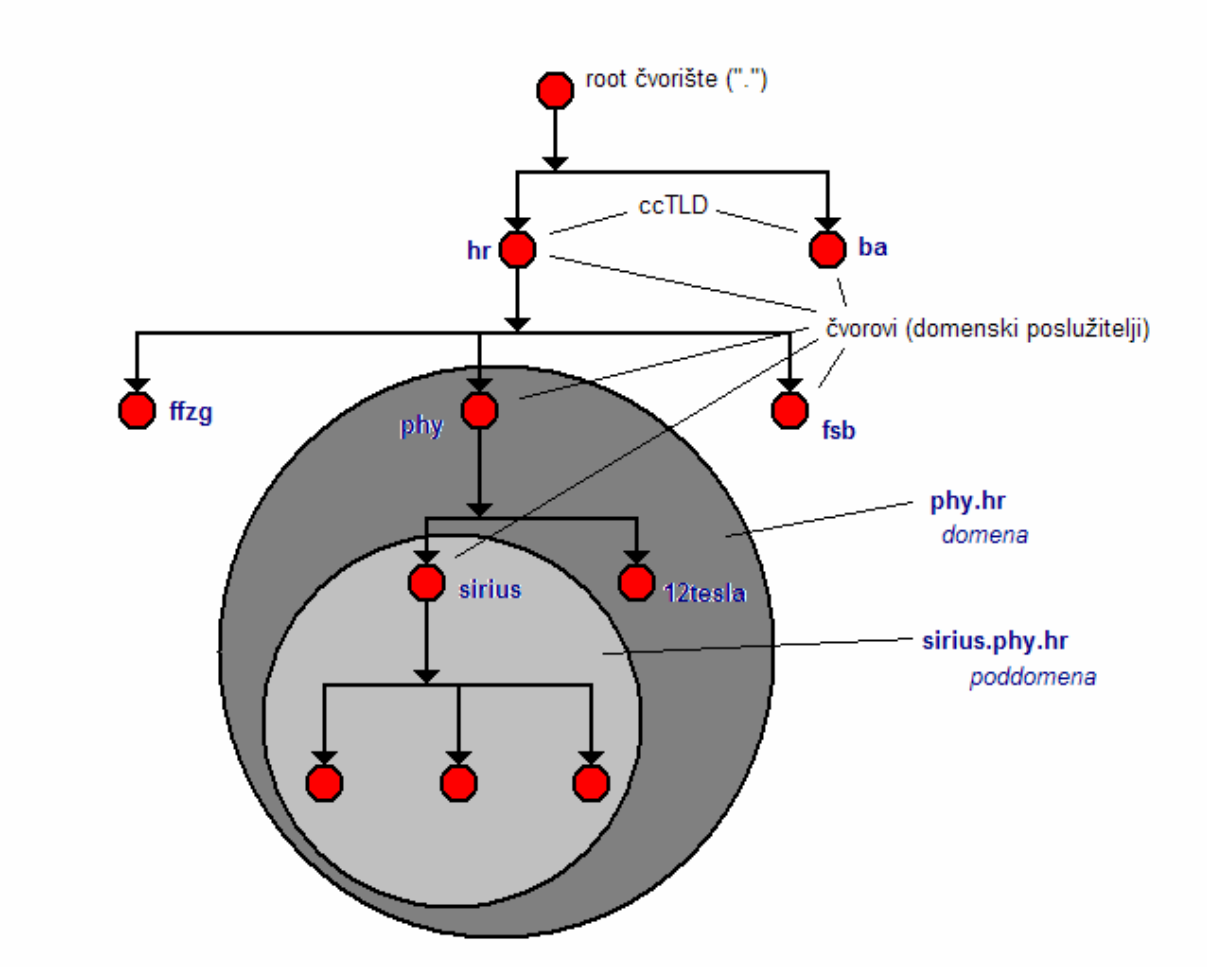
Naravno, za osnovnu domenu je također nadležan ICANN, koji regulira upravljanjem 13 **vršnih DNS poslužitelja** (engl. root servers).

Ovdje dajemo pregled svih 13 root servera, njihovih imena i IP adresa.

```
[dominis] 15:30 [~] > dig @a.root-servers.net

; <<>> DiG 9.2.4 <<>> @a.root-servers.net
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17278
;; flags: qr aa rd; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13

;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       518400  IN      NS      D.ROOT-SERVERS.NET.
.                       518400  IN      NS      A.ROOT-SERVERS.NET.
.                       518400  IN      NS      H.ROOT-SERVERS.NET.
.                       518400  IN      NS      C.ROOT-SERVERS.NET.
.                       518400  IN      NS      G.ROOT-SERVERS.NET.
.                       518400  IN      NS      F.ROOT-SERVERS.NET.
.                       518400  IN      NS      B.ROOT-SERVERS.NET.
.                       518400  IN      NS      J.ROOT-SERVERS.NET.
.                       518400  IN      NS      K.ROOT-SERVERS.NET.
.                       518400  IN      NS      L.ROOT-SERVERS.NET.
.                       518400  IN      NS      M.ROOT-SERVERS.NET.
.                       518400  IN      NS      I.ROOT-SERVERS.NET.
.                       518400  IN      NS      E.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
D.ROOT-SERVERS.NET.     3600000 IN      A       128.8.10.90
A.ROOT-SERVERS.NET.     3600000 IN      A       198.41.0.4
H.ROOT-SERVERS.NET.     3600000 IN      A       128.63.2.53
C.ROOT-SERVERS.NET.     3600000 IN      A       192.33.4.12
G.ROOT-SERVERS.NET.     3600000 IN      A       192.112.36.4
F.ROOT-SERVERS.NET.     3600000 IN      A       192.5.5.241
B.ROOT-SERVERS.NET.     3600000 IN      A       192.228.79.201
J.ROOT-SERVERS.NET.     3600000 IN      A       192.58.128.30
K.ROOT-SERVERS.NET.     3600000 IN      A       193.0.14.129
L.ROOT-SERVERS.NET.     3600000 IN      A       198.32.64.12
M.ROOT-SERVERS.NET.     3600000 IN      A       202.12.27.33
I.ROOT-SERVERS.NET.     3600000 IN      A       192.36.148.17
E.ROOT-SERVERS.NET.     3600000 IN      A       192.203.230.10

;; Query time: 138 msec
;; SERVER: 198.41.0.4#53(a.root-servers.net)
;; WHEN: Thu Mar  2 15:32:08 2006
;; MSG SIZE  rcvd: 436
```

Postoje i različite organizacije koje nude alternativne vršne DNS poslužitelje, nudeći najčešće i vlastiti skup TLD-eva, nekompatibilan sa ICANN-ovom listom, npr. ORSC (Open Root Server Confederation), OpenNIC, Pacific Root, New.Net; i najorganiziraniji **ORSN** (Open Root Server Network) koji ima direktnu kompatibilnost sa ICANN-ovom bazom.

Slika 1: DNS hijerarhija



DNS REZOLUCIJA

Svaki se funkcionalni DNS sustav nužno sastoji se od tri dijela:

- DNS **klijent** (engl. resolver), program koji se izvršava na klijentskom računalu i koji formira određeni DNS zahtjev. Takav program je najčešće ugrađen u standardnoj biblioteci u formi sistemskih poziva koje pozivaju različiti korisnički programi
- **Rekurzivni** (engl. recursive) DNS **poslužitelj**, koji nakon dobivenih upita za klijenta obavlja pretraživanje kroz DNS stablo i vraća nazad odgovore klijentima
- **Autoritativni** (engl. authoritative) DNS **poslužitelj**, koji odgovara na upite rekurzivnih poslužitelja te vraća ili završni odgovor ili zbog delegiranja vraća referencu na neki drugi autoritativni DNS poslužitelj

Sam proces primanja zahtjeva i njihove obrade te vraćanja odgovora se naziva DNS **rezolucija** (engl. name resolution). Pojednostavljeno, osnovna rezolucija je proces pretvorbe domenskog imena u IP adresu: prvo tražimo DNS poslužitelj, a zatim mu šaljemo upit za adresom, na koji on odgovara sa traženom adresom. Budući da je DNS strogo distribuirana

baza, ona je raspodijeljena po mnogo različitih poslužitelja. No, očigledno je da zbog raspodijeljenosti rezolucija obično ne može biti obavljena kroz samo jedan upit i odgovor, već najčešće zahtijeva dužu komunikaciju i niz upita i odgovora. Najčešća je situacija da klijent šalje zahtjeve **lokalnom** DNS **poslužitelju** (nadležan za klijentsko računalo, obično dodijeljen od ISP-a ili ustanove u kojoj se nalazi klijentsko računalo), koji predstavlja rekurzivni poslužitelj i obavlja upite te zatim vraća odgovor klijentu. Dakle, najveći i najkompliciraniji dio procedure predstavlja traženje autoritativnog poslužitelja u složenoj DNS hijerarhiji.

Što se samih tipova DNS rezolucije tiče, postoje dva osnovna tipa prolaska kroz DNS hijerarhiju da bi se otkrio točan zapis. Oni se razlikuju po tome tko obavlja većinu posla oko saznavanja podataka i njihove obrade, a prvenstveno se pojavljuju kad obrada određenog DNS upita zahtijeva nekoliko koraka (dakle, lokalni DNS poslužitelj nema sve informacije):

- **Iterativni** - kada klijent šalje dotične upite, poslužitelj mora odgovoriti jednim od dva moguća odgovora: odgovorom na zahtjev ili imenom drugog DNS poslužitelja koji ima više podataka traženom o upitu. U ovakvom tipu upita najveći dio posla obavlja klijent iterirajući akcije upit-odgovor i prolazeći kroz DNS hijerarhiju.
- **Rekurzivni** - kada klijent šalje rekurzivni upit, poslužitelj preuzima posao pronalaženja informacija o traženom upitu. Dakle, ono što je u iterativnom obavljao klijent, kod rekurzivnih upita obavlja poslužitelj - obrađuje informacije i šalje nove upite drugim poslužiteljima sve dok ne pronađe traženo. Dakle, klijent šalje svega jedan zahtjev te dobiva ili točnu informaciju koju je tražio ili poruku o grešci.

Očigledno je rekurzivan način pretraživanja vrlo povoljan za klijente, ali može znatno opteretiti DNS poslužitelje, pa se takve forme upita obično eksplicitno dozvoljavaju samo iz lokalne mreže, dakle računalima kojima je dotični DNS poslužitelj nadležan.

Već smo spomenuli da je DNS vrlo strogo hijerarhijski baziran - praktički svaka pretraga za nekom DNS informacijom počinje od čvornog DNS računala, od vrha DNS **stabla**. Prolazak kroz DNS stablo je silazak po granama stabla, gdje je svaki čvor jedan DNS poslužitelj, nadležan za svoj dio DNS prostora. Osnovni preduvjet pronalaženja čvora stabla je lokalna lista 13 vršnih DNS poslužitelja, koji dalje delegiraju pretragu po zapisima. DNS stablo je dakle hijerarhijski složen skup DNS poslužitelja, gdje svaka domena i poddomena ima jednog ili više autoritativnih DNS poslužitelja. Dotični poslužitelji (čvorovi stabla) su nadležni (ili mogu delegirati dalje) za "sve" domene ispod njih, servirajući podatke drugima na upit. Hijerarhijski raspored poslužitelja upravo mora odgovarati rasporedu domena i odgovarajućeg domenskog prostora.

U svakodnevnoj upotrebi, osim domena i labela pojavljuje se i pojam **zona**. Zona kao takva predstavlja dio ukupnog domenskog prostora, te se prostire od jedne točke - jednog DNS poslužitelja zaduženog za tu zonu, odnosno autoritativnog za tu zonu - dalje do krajnjih čvorova ili do početaka neke druge zone. Tehnički zona je dakle dio domene, iako se može prostirati i na cijelu domenu.

DNS MEĐUSPREMNICI

DNS je sustav sa ovim osnovnim načinima pretraživanja (iterativni i rekurzivni silazak kroz DNS stablo) vrlo neefikasan, budući da svaki upit implicitno znači novi prolazak po stablu, počevši od vršnih DNS poslužitelja. Jasno, kada bi se u stvarnom svijetu nužno svaki put prolazilo od početka DNS stabla do kraja, do traženog zapisa - proces DNS rezolucije bi trajao i trajao, a opterećenje DNS poslužitelja bi postalo pretjerano veliko, sve veće i veće sa

porastom broja računala na Internetu. No, eskalaciju ovog problema prilično je smanjio jednostavan princip spremanja kako pozitivnih (uspješnih) tako i negativnih (neuspješnih) rezultata DNS upita na DNS poslužiteljima. Naime, formiranje međuspremnika (engl. cache) DNS rezultata je odgovor na dva jednostavna fenomena prisutnim u računalnim mrežama i računalima općenito:

- Veće su šanse da se će pristupati nekom resursu ako se nedavno pristupalo nekom drugom (prostorno) bliskom resursu - što je tzv. prostorna lokalnost reference
- Ako se samom tom resursu nedavno pristupalo, to su veće šanse da će mu se ponovno pristupati - što je tzv. vremenska lokalnost reference

Praksa pokazuje da se vrlo često šalju slični ili isti DNS upiti u vremenski bliskim periodima. Stoga svi moderni DNS poslužitelji imaju interne međuspremnike o nedavnim DNS upitima koji im omogućavaju da pribave odgovor ili dio odgovora iz međuspremnika (obično u privremenoj memoriji). DNS spremnici se nalaze i na većini DNS klijenata, obavljajući isti posao kao i na DNS poslužiteljima. Na taj način se spremaju rezultati već obavljenih upita i na klijentskim računalima, smanjujući na taj način promet prema poslužiteljima i njihovo opterećenje. Tako spremljeni odgovori će biti "duže" spremljeni kod klijenata, budući da je svaki spremnik ograničene veličine i dovoljan broj upita "istiskuje" stare ili nekorištene odgovore. Međuspremnici kao takvi više poboljšavaju performanse što su bliže klijentu, ali daju bolju pokrivenost što su dalje od klijenta. Podaci spremljeni u spremnicima imaju svoja vremena života, TTL (Time To Live), pa se time osigurava da zastarjeli podaci nužno nestaju iz spremnika. Današnji moderni DNS poslužitelji će pri prihvatu DNS upita obaviti pretraživanje vlastitih spremnika kao i lokalne DNS baze, pokušavajući što više skratiti vremenski "skup" prolazak kroz DNS stablo.

REVERZNA REZOLUCIJA

Do sada smo samo spominjali standardnu unaprijednu (engl. forward) rezoluciju kod koje se DNS imena pretvaraju u IP adrese. U standardnoj komunikaciji na Internetu nužno je moći vršiti rezoluciju u oba smjera, što će reći i u unazadnom obliku (engl. reverse) - primjerice za provjeru spada li određena adresa u kakvu domenu i sl. No, problem kod **reverzne** DNS **rezolucije** je da se poslužitelji razlikuju prvenstveno po labelama odnosno po domenama za koje su nadležni, a ovdje imamo samo IP adresu kao početnu informaciju. Kako bi se pojednostavio i uopće omogućio ovaj proces, formirana je dodatna hijerarhija u vidu **IN-ADDR.ARPA** domene. Riječ je o domenskom prostoru koji se sastoji od četiri nivoa poddomena, a svaki nivo odgovara jednom dijelu IP adrese. Reverznom DNS rezolucijom odnosno prolaskom kroz dotična četiri nivoa, dolazi se do čvora za traženu IP adresu koji pokazuje na odgovarajuće domensko ime.

Svaki nivo unutar in-addr.arpa domene se sastoji od 256 poddomena (0, 1, ..., 255). **Reverzna** DNS **adresa** se formira od čvorova unutar reverzne domene, a identična je obrnuto zapisanoj IP adresi sa in-addr.arpa sufiksom, pa upiti nad takvom adresom daju kao povratnu informaciju "standardnu" DNS adresu:

Primjer 5: Standardne i reverzne adrese

```
12tesla.phy.hr A 161.53.7.81
81.7.53.161.in-addr.arpa PTR 12tesla.phy.hr
```

DNS PROTOKOL I KOMUNIKACIJA

DNS protokol se nalazi na najvišem aplikacijskom sloju TCP/IP modela, te je preko sušelja povezan sa TCP protokolom i UDP protokolom nižeg prijenosnog sloja. DNS poslužitelj koristi standardne portove dodijeljene od IANA-e: TCP/53 i UDP/53. Na njima osluškuje zahtjeve, te može bilo sa dotičnih bilo sa nekog visokog porta (port veći od 1024, ovisno o konfiguraciji poslužitelja) poslati odgovor u vidu traženih zapisa odnosno RR-ova (engl. resource record). Standardno se uvijek koristi UDP za upite, a komunikacija se uglavnom svodi na jedan UDP upit i jedan UDP odgovor. TCP komunikacije se koristi jedino kad veličina odgovora prelazi 512 bajtova ili za grupne prijenose DNS informacija, tzv. prijenos zone (engl. zone transfer). Standardni DNS upit je obično vrlo jednostavan, sadrži uglavnom samo adresu koja se želi razriješiti - no odgovori su vrlo komplicirani budući da sadrže sve adrese i zamjenske adrese koje su rezultat upita. Stoga se odgovori obično sažimaju posebnim algoritmima, eliminirajući nepotrebne podatke i smanjujući samu veličinu UDP datagrama. U slučaju da i dalje veličina paketa prelazi 512 bajtova, šalje se parcijalna poruka u obliku UDP paketa sa posebnim bitom postavljenim (TC=1), koji označuje da se upit mora ponoviti koristeći TCP.

Za DNS upite i odgovore se koristi tzv. opći oblik poruke, koji se sastoji od 5 odjeljaka. Dotični se popunjavaju kako upitom od klijenta, tako i odgovorom od poslužitelja i u oba slučaja i podacima u zaglavlju koji su nužni da se proces obavi ispravno i uspješno. Dotični odjeljci sa sadržajem su:

- Zaglavlje (engl. header) - nužna polja koja definiraju tip poruke i pružaju klijentu ili poslužitelju važne informacije o poruci. Također, u zaglavlju se nalaze i brojači zapisa u drugim odjeljcima poruke. Zaglavlje je prisutno u svim porukama i fiksne je veličine od 12 bajtova. Jedna od važnijih zastavica u zaglavlju je i QR koja označava da li je poruka upit ili odgovor
- Pitanje (engl. question) - jedan ili više upita klijenta prema DNS poslužitelju
- Odgovor (engl. answer) - jedan ili više RR-ova koji su odgovor na klijentov upit
- Autoritet (engl. authority) - jedan ili više RR-ova koji predstavljaju delegaciju na autoritativne poslužitelje, odnosno pokazuju na autoritativne DNS poslužitelje koji se mogu koristiti za nastavak DNS rezolucije
- Dodatno (engl. additional) - jedan ili više RR-ova koji sadrže različite dodatne informacije vezane uz upit, ali dotične nisu nužne za potpunost odgovora ili upita; primjerice IP adresa DNS poslužitelja spomenutog u polju za autoritet

Neke od mogućih zastavica u zaglavlju DNS poruke su sljedeće:

- ID (engl. identifier) - riječ je o 16-bitnom identifikacijskom broju koje stvara računalo ili uređaj koji šalje DNS upit. Poslužitelj u poruci mora odgovoriti sa istim takvim brojem, što omogućava klijentu da prepozna par upit-odgovor
- QR (engl. query/response flag) - služi za razlikovanje upita i odgovora. Postavljena je na 0 za upit od klijenta, a 1 za odgovor od poslužitelja
- AA (engl. authoritative answer flag) - zastavica će biti postavljena na 1 ako je poslužitelj koji šalje odgovor autoritativan za zonu koja je dana u odjeljku pitanja, a u suprotnom će biti 0
- TC (engl. truncation flag) - zastavica koja kad je postavljena na 1 označava da je poruka nepotpuna budući da je bi ukupna veličina UDP poruke bila veća od 512 bajtova. Klijent tada može poslati novi zahtjev da bi dobio potpun odgovor, pa se najčešće ostvaruje novi zahtjev-odgovor koristeći TCP

- RD (engl. recursion desired) - kada je dotična zastavica postavljena, označava da bi bilo poželjno da poslužitelj obavi rekurzivnu rezoluciju, ako to poslužitelj podržava. Odgovor koji poslužitelj šalje će zadržati isto stanje zastavice kao i u upitu,
- RA (engl. recursion available) - kada je postavljena zastavica, znači da poslužitelj koji šalje odgovor podržava rekurzivne upite, što klijenti najčešće "zapamte" za buduću komunikaciju sa dotičnim poslužiteljem
- Rcode (engl. response code) - zastavica koja je u upitima uvijek na 0, ali u odgovorima indicira na tip greške koji se desio, odnosno da li je uspješno došlo do odgovora
- QDCount (engl. question count) je brojač upita u odjeljku pitanja poruke
- ANCount (engl. answer record count) je brojač RR-ova u odjeljku odgovora poruke
- NSCount (engl. authority record count) je brojač RR-ova u odjeljku autoriteta poruke
- ARCount (engl. additional record count) je brojač RR-ova u dodatnom odjeljku poruke

Poruka od DNS klijenta je primjerice sljedećeg oblika: klijent šalje UDP upit (QR=0, što označava upit, a ne odgovor) kao standardni upit (OPCODE=0) sa jednim zapisom u upitu (QDCOUNT=1). Upit uglavnom ne sadrži dodatne zapise niti u polju za odgovor, niti za autoritativni dio niti u polju za dodatne zapise (ANCOUNT=0, NSCOUNT=0, ARCOUNT=0). QNAME zapis označava primjerice domenu za kojom klijent pretražuje (QNAME = www.google.com.). Tip i klasa zapisa za kojom klijent pretražuje su QTYPE=1 (adresa računala) i QCLASS=1 (Internet adresa). Budući da veličina odgovora unutar 512 bajtova, TC=0.

Odgovor (QR=1) od poslužitelja na standardni upit (OPCODE=0) je primjerice sljedeći: poslužitelj je autoritativan za traženu domenu (AA=1), a podržava i rekurzivne upite (RA=1). Tijekom pretrage nisu utvrđene nikakve greške u upitu (RCODE=0) koji je sadržavao samo jedan zapis (QDCOUNT=1). Odgovor sadržava 3 RR-a (ANCOUNT=3) u polju odgovora, 6 zapisa u odjeljku za autoritet (ARCOUNT=6). Očigledno je da se originalni upit koristi za formiranje odgovora, pa se polje zaglavlja i polje pitanja kopiraju iz originalnog upita u odgovor, sa već navedenim promjenama.

DNS KLASE I ZAPISI

Kao što je već spomenuto, RR je jedan zapis, jedna jedinica u DNS sustavu. Svaki RR sadrži određene atribute, odgovarajuće za vlastiti tip; to mogu biti IP adresa, adresa za isporuku elektroničke pošte, niz teksta, DNS labela ili nešto treće. Svaki RR se sastoji od sljedećih komponenti, redom kojim se pojavljuju:

- Ime domene - uglavnom se koristi FQDN, a ako je zapisano kratko ime onda se automatski dodaje ime zone na kraj imena
- TTL u sekundama, standardna vrijednost je minimalna vrijednost navedena u SOA zapisu (o ovome kasnije)
- **klasa zapisa** koji može biti Internet, Hesiod i Chaos
- Tip zapisa: CNAME, PTR, A, MX, TXT, AAAA, A6, itd.
- Podaci za dotični tip zapisa - odgovaraju određenom tipu, ako sadržavaju ime domene koje nije FQDN, automatski se dodaje ime zone na kraj imena
- Opcionalni komentar (dodan u ovisnosti o vrsti poslužiteljskog softvera)

Klase zapisa (engl. resource record classes) su u osnovi povijesna ostavština, bez stvarne koristi danas. Budući da je DNS inicijalno vrlo generički oformljen, ideja je bila da će se kroz DNS nuditi imeničke usluge za više od jednog protokola (dakle, osim IP-a). Stoga svaki RR zapis ima i klasu, te općenito rečeno ona mora biti specificirana za svaki RR unutar lokalne zone. Danas se u praksi koristi jedino Internet klasa, pa se ona implicitno podrazumijeva kad u lokalnoj zoni nije eksplicitno navedena IN klasa.

Što se pak tiče tipova zapisa, postoji nekoliko osnovnih tipova, navedimo neke koji se češće sreću u praksi:

- **A** (engl. address) - povezuje odgovarajuće domensko ime (labelu ili niz labela) sa IPv4 adresom (32bitna adresa). Danas je često moguće naći da više A zapisa pokazuje na istu IP adresu, što je sasvim legalno.
- **CNAME** (engl. canonical name) - omogućava da jedno domensko ime bude zamjensko ime za drugo. Takvo zamjensko ime dobiva sve osobine originala, uključujući i IP adrese i poddomene. No, ilegalno je u zoni imati ijedan zapis koji dijeli isto ime kao i CNAME zapis. Također, niti jedan tip zapisa osim CNAME ne smije pokazivati na zamjensku adresu (odnosno na CNAME), budući da bi to omogućilo petlje i neispravne zapise u zoni.
- **MX** (engl. mail exchange) - označava koji su sve e-mail poslužitelji nadležni za dotičnu domenu. U slučaju da ovaj zapis ne postoji, e-mail se isporučuje koristeći A zapis dobiven rezolucijom iz odredišne domene. Osnovna funkcionalnost ovog mehanizma je pružiti mogućnost da postoji više e-mail poslužitelja za jednu domenu i da se definira točan redoslijed prema kojem ih se mora kontaktirati. Time se na jednostavan način omogućava usmjerivanje maila (engl. mail routing) kao i mogućnost raspodjele opterećenja između više poslužitelja.
- **PTR** (engl. pointer record) - povezuje IPv4 adresu sa odgovarajućim domenskim imenom (FQDN). Obično PTR zapisi trebaju pokazivati na ime koje se može nazad razriješiti u polaznu IPv4 adresu. Naravno, PTR zapis kao takav nije IPv4 adresa, već obrnuto zapisana 4 okteta adrese sa dodatnom IN-ADDR.ARPA. domenom.
- **NS** (engl. name server record) - označava da je za dotičnu zonu treba posluživati upravo dotični DNS poslužitelj. Svaki NS zapis je ili oznaka autoriteta ili oznaka za delegaciju: naime, ako je naziv NS zapisa jednak zoni u kojoj se NS zapis pojavljuje, onda je riječ o autoritativnom zapisu; ako je pak riječ o nazivu koji sadrži neku od poddomena, onda je riječ o delegaciji.
- **SOA** (engl. start of authority) - između ostaloga označava koji je DNS poslužitelj autoritativan za dotičnu domenu, kao i dodatne informacije o zoni. Svaka ispravna zona mora imati SOA zapis.
- **AAAA** i **A6** - povezuju odgovarajuće domensko ime sa IPv6 adresom (128bitna adresa). Moguće je naći i AAAA i A6 zapis, pri čemu se oni razlikuju u nekim detaljima: A6 omogućava da labela bude definirana kao binarni niz, itd. Danas se A6 smatra još uvijek eksperimentalnom, te se preporuča koristiti AAAA u produkciji.
- **TXT** (engl. text string) - pojednostavljeno, omogućava proizvoljan tekstualan zapis do 255 bajtova.
- **DS** (engl. delegation signer) - dodaje se na mjestu prekida zone (mjesta gdje se vrši delegacija) da bi se pokazalo kako je delegirana zona digitalno potpisana i da dotična prepoznaje određeni ključ kao ispravni vlastiti ključ. Ovime se eksplicitno definira delegacija, umjesto implicitno kao do sada.
- **KEY** (engl. public key) - javni ključ koji je autoriziran od SIG zapisa, a omogućava spremanje i DNSSEC ključeva i proizvoljnih ključeva za aplikacije.

- **LOC** (engl. location information) - zapis u koji je moguće spremiti geolokacijske odnosno GPS podatke o određenom čvoru ili domeni.
- **SIG** (engl. cryptographic public key signature) - predstavlja potpis radi autentifikacije podataka u DNSSEC-u.
- **TSIG** (engl. transaction signature) - omogućava jednostavnu autentifikaciju koristeći dijeljene tajne ključeve i hashiranje za DNS transakcije.
- **RP** (engl. responsible person) - zapis o odgovornoj osobi za domenu ili čvorove.

DNS DODACI I NEKI DETALJI

Naposljetku, spomenimo i **dinamički DNS** (engl. dynamic DNS) na klasični DNS sustav. DNS u početku osmišljen s idejom da se promjene u zonama neće prečesto odvijati - što smo već vidjeli kod problematike razmjene i sinkronizacije zona. Za unos u DNS sustav su uglavnom predviđene statičke adrese koje se ne mijenjaju, budući da bi ručno mijenjanje svaki put predstavljalo noćnu moru za održavanje. Moderni DNS i DHCP poslužitelji stoga omogućavaju međusobno povezivanje sustava dodjeljivanja IP adresa sa DNS sustavom, tako da se svako DHCP-registrirano računalo registrira u DNS sustavu kroz automatizirani proces.

Specifično, DHCP klijent šalje DNS UPDATE poruku koja indicira DNS poslužitelju što treba obaviti sa odgovarajućim RR-ovima. Naravno, dinamički DNS kao takav nije ograničen nužno na DHCP, već u praksi svaki autorizirani DDNS (dinamički DNS) klijent može upravljati odgovarajućim zapisima u zoni.

DNS SIGURNOST

Nažalost, uz DNS sustav su vezani i različiti sigurnosni problemi. Postoji niz trikova pomoću kojih se može odredišni DNS poslužitelj natjerati da prihvati lažne zapise. Takvom metodom lažiranja DNS zapisa (engl. DNS forgery) nesvjesni se klijenti preusmjeruju na lažne adrese i time postaju laka meta napadača. Standardno su takvi napadi u formi trovanja DNS međuspremnika (engl. cache poisoning), napada kod kojeg se utiče na DNS poslužitelj da povjeruje da je dobio autoritativne informacije o nekim RR-ovima. Time se utiče na sve klijente koji koriste dotični DNS poslužitelj da također koriste lažiranu informaciju, koja može omogućiti daljnje različite napade na klijentska računala.

Postoje tri osnovna tipa ovakvog napada:

- Preusmjeravanje poslužitelja za odredišnu domenu - gdje se za neku domenu na zloćudnom poslužitelju specificira vlastiti NS za traženu domenu u autoritativnom odjeljku i još u dodatnom odjeljku daje vlastiti A zapis sa lažnim NS-om koji se nazivno nalazi u napadnutoj domeni. Zatrovani poslužitelj pamti IP adresu NS poslužitelja koji je sada napadačev DNS poslužitelj i time napadač dobiva mogućnost proizvoljnog baratanja sa cijelom napadnutom zonom.
- Preusmjeravanje NS zapisa odredišne domene - omogućava preusmjeravanje DNS poslužitelja neke druge domene (nevezane uz originalni upit) na proizvoljnu napadačevu IP adresu. Napadačev DNS poslužitelj odgovara u autoritativnom odjeljku za napadnutu domenu (nevezanu uz originalni upit) sa NS zapisom u traženoj domeni, a u dodatnom odgovoru daje A zapis sa IP adresom dotičnog DNS poslužitelja. Time dolazi do iste funkcionalnosti kao i u prošlom napadu.

- Treći tip napada je napad identifikacijom - kod kojeg je osnovna ideja predviđanje 16-bitnog identifikacijskog broja u DNS komunikaciji. Ako napadač uspješno pogodi isti i bude prvi koji vraća odgovor sa ispravnim brojem, poslužitelj/klijent će tretirati njegov odgovor kao ispravan i autoritativan. Nažalost, sa što većim brojem istovremenih DNS upita koje poslužitelj obrađuje, vjerojatnost uspješnog pogađanja (odnosno vjerojatnost kolizije) jedinstvenog broja upita se povećava. Danas moderni softver uglavnom taj problem rješava kvalitetnijim pseudo-slučajnim generatorima kao i slučajnim izborom visokih izvorišnih portova za upite (budući da odgovor mora biti poslan na isti izvorišni port).

Većina ovih napada danas je riješena promjenama u DNS softveru (dakle noviji Bind9 i DJBDNS softver) koji uglavnom ignorira dobivene DNS odgovore koji nisu striktno vezani uz prvotni zadani upit. Alternativni i sve popularniji pristup sigurnosti je uvođenje sigurnog DNS-a, tzv. **DNSSEC** sustava. Pojednostavljeno, riječ je o korištenju odgovarajućih RR-ova za potpisivanje dijelova zona ili čak cijele komunikacije koristeći digitalne potpise i digitalne certifikate kako bi se potvrdila izvornost, integritet i autentičnost DNS podataka. Na taj način (provjeravajući potpis i podatke u zoni) DNS klijent može provjeriti podatke i za sigurnošću znati jesu li oni zaista potekli od traženog autoritativnog DNS poslužitelja.

DDOS NAPADI

DDOS je skraćenica od Distributed Denial of Service, a to je naziv za relativno sofisticirani napad na poslužitelje na Internetu, u kojem se koriste brojna računala da bi se napadnuti poslužitelj preopteretio poslom i tako stavio izvan funkcije. Napadač ne pokušava provaliti u računalo koje napada, nego samo koristi tisuće drugih računala kako bi napadnuti poslužitelj imao previše zahtjeva za uslugama, koje onda ne može ispuniti, čime poslužitelj postaje neupotrebljiv za rad. Računala koja sudjeluju u napadu pojedinačno najčešće nemaju izravne veze s napadačem, nego je riječ o računarima koji su "provaljeni" i koriste se bez znanja svojih vlasnika. DDOS je neugodan jer ga je teško spriječiti bez velikog utjecaja na ostatak prometa preko Interneta.

Važno je spomenuti kako cijeli sistem domena ne funkcionira ako ne postoji korijenski ili "root" poslužitelj na kojem je zapisano koja je adresa svakoga pojedinog poslužitelja odgovornog za pojedinu domenu. Izraz korijenski dolazi od toga što je to svojevrsni korijen stabla koje se širi i ima pojedinačna računala na Internetu.

Važnost postojanja "root" poslužitelja nametnula je potrebu da takvih računala ima više. Trenutačno ih je službeno 13 i raspodijeljeni su po cijelom svijetu kako bi se minimizirao utjecaj bilo kakve lokalne katastrofe na funkcioniranje ostatka Interneta. Računala na kojima se nalaze poslužitelji rade i na različitim operativnim sistemima i sa različitim verzijama aplikacija koje se brinu o podacima važnima za funkcioniranje DNS sistema, čime je osigurano da niti jedna pojedinačna pogreška unutar nekog sistema ne može utjecati na sve poslužitelje istodobno.

No ono što se ne može dogoditi slučajno, može se dogoditi namjerno pa je posljednji najozbiljniji napad, koji se dogodio u Studenom 2002. godine, bio usmjeren upravo prema tih 13 poslužitelja i trajao je punih šest sati. Napad je za posljedicu imao da je čak 9 od 13 poslužitelja ipak prestalo ispravno funkcionirati usprkos svim sistemima zaštite, no zahvaljujući načinu na koji radi DNS sistem, preostala računala bila su dovoljna da se ne osjete posljedice ovog napada. Iz svakog incidenta potrebno je izvući i pouku, tako je i s ovim događajem, pa se već uvelike priča o potrebi za dodatnim sigurnosnim mehanizmima i još

većom redundancijom unutar DNS sistema kako bi nesmetano funkcionirao bez obzira na sve moguće incidente.

PRIMJER ZA phy.hr DOMENU

Pokažimo za kraj kako to izgleda na našem fakultetu.

```
[dominis] 17:09 [~] > host -l -a phy.hr
Trying "phy.hr"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24795
;; flags: qr aa ra; QUERY: 1, ANSWER: 318, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;phy.hr.                                IN      AXFR

;; ANSWER SECTION:
phy.hr.                 86400   IN      SOA     sirius.phy.hr. postmaster.siri
us.phy.hr. 20050539 3600 300 3600000 3600
phy.hr.                 86400   IN      NS      sirius.phy.hr.
phy.hr.                 86400   IN      NS      bjesomar.srce.hr.
phy.hr.                 86400   IN      MX      10 sirius.phy.hr.
12tesla.phy.hr.         86400   IN      A       161.53.7.81
18tesla.phy.hr.         86400   IN      A       161.53.7.144
abydos.phy.hr.          86400   IN      A       161.53.132.86
act.phy.hr.             86400   IN      A       161.53.7.108
agram.phy.hr.           86400   IN      A       161.53.7.66
aldebaran.phy.hr.       86400   IN      A       161.53.7.133
alf.phy.hr.             86400   IN      A       161.53.6.158
alien.phy.hr.           86400   IN      A       161.53.7.245
alka.phy.hr.            86400   IN      A       161.53.6.154
altair.phy.hr.          86400   IN      A       161.53.132.90
.
.
.
sinapsa.phy.hr.         86400   IN      A       161.53.7.52
sirius.phy.hr.          86400   IN      A       161.53.6.130
sirius.phy.hr.          86400   IN      A       161.53.7.130
sirius.phy.hr.          86400   IN      A       161.53.132.130
soliton.phy.hr.         86400   IN      A       161.53.6.188
.
.
.
Received 7134 bytes from 161.53.7.130#53 in 28314 ms
```

ZAKLJUČAK

Dakle, mogli smo vidjeti kako je nastao, što je i čemu služi Domain Name System. Vidimo da je to strogo hijerarhijski sistem koji je osmišljen da bi se olakšao rad kako korisnicima, tako i administratorima računalnih mreža. Funkcija DNS-a zvuči jednostavno, međutim mogli smo vidjeti da je to vrlo kompleksan sustav, čak je mnogo kompleksniji nego što smo mi ovdje izložili. Zbog stalnog porasta broja računala na Internetu i zbog razloga prikazanih pretkraj seminara, mislimo da je vrlo važno posebnu pažnju posvetiti sigurnosti sustava i njegovom razvoju.

LITERATURA

http://en.wikipedia.org/wiki/Dns
http://www.linux.ie/articles/dns.php
http://www.dns.hr/domain.html
Damir Kirasić: Unix mreže i komunikacije, Zagreb 1994.

Dinko Korunić: DNS Priručnik, Zagreb 2005.
Ermin Hromadžić: DNS - Domain Name Server, Zenica 2003.
Andrew S. Tanenbaum: Computer networks, New Jersey 2003.