

ISC Bind9

Pripremio: Dinko Korunić
Verzija: 1.1, listopad 2002.

Tijekom prezentacije

- ako što **nije jasno** - pitajte!
- ako što **nije točno** - ispravite!
- diskusija je **poželjna** i **produktivna**
- ako je **prebrzo** - tražite da se uspori!
- ako je pak **presporo** i **uspavljuje** vas - lako se ubrza sa sadržajem
- vremena je malo, sadržaja mnogo - zato su neki sadržaji samo ukratko objašnjeni

Ciljevi prezentacije

- osnovne značajke Bind9 paketa:
 - sadržaj paketa
 - upotreba programa
 - konfiguracija programa
 - novosti naspram Bind4 i Bind8
- uspješno korištenje Bind softvera
- detekcija i otklanjanje pogrešaka i problema
- prostor za diskusiju i iskustva

Potrebno predznanje

- **apsolutno obavezno** - osnovna računalna pismenost:
 - datoteke, direktoriji, hijerarhija programa na Solaris 7/8 ili Debian Linux sistemima
 - pokretanje, zaustavljanje servisa
- **nužno** - poznavanje rada DNS poslužitelja, konfiguriranje, upravljanje
- **opcionalno** - iskustva u radu sa više zona i delegaciji, djbdns, DNSSEC, etc.

Sadržaj (1)

- **I - uvod, osnove i početnica**
 - izvršne datoteke i upotreba
 - bind4, bind8, bind9
 - named.conf, rndc.conf, rndc.key
 - A, PTR, MX, CNAME
 - zone, primjeri
 - obavezna pravila
 - malo teorije
- **II - korišćenje i upravljanje**
 - nslookup, dig, host
 - rndc upravljanje
 - nslint, dswalk
 - master/slave
 - MX i pravila
 - forward, rekurzije, iteracije, cache
 - česte greške
 - TXT, HINFO, NXT, WKS, AAAA, LOC, RP, SRV

Sadržaj (2)

- **III - napredno korišćenje**
 - teorija, sigurnost, itd.
 - dinamički dns, SOA, TTL
 - potpisivanje zona
 - pozitivni/negativni cache
 - wildchars
 - neobičnosti (točke u nazivima, \$ORIGIN i sl)
- **IV - otvorena diskusija**
 - iskustva, problemi

Uvod u Bind

ponešto teorije, osnovna upotreba
izvedba paketa i razlike..
brzo konfiguriranje i postavljanje

Bind DNS softver

- URL: <http://www.isc.org/products/BIND/>
- činjenice:
 - brzo zastarijeva
 - previše major i minor verzija: bind4, bind8, bind9, alpha, beta, itd.
 - mnogo rupa i problema u prošlosti: uz sendmail jedan od "zloglasnijih" softvera
 - složeno konfiguriranje i upravljanje
 - teško otkrivanje grešaka - kobno

CARNet bind9 paket (1)

- *izvršne* datoteke:
 - **osnovne:**
 - `named`, `rndc`, `rndc-confgen`, `named-checkconf`, `named-checkconf`
 - **sigurnost:**
 - `dnssec-keygen`, `dnssec-makekeyset`, `dnssec-signkey`, `dnssec-signzone`
- *konfiguracijske* datoteke:
 - `/etc/named.conf`, `/etc/rndc.conf` (+ `/etc/rndc.key`)
 - `/etc/namedb/*` (`db.0`, `db.255`, `db.127`, itd.)

CARNet bind9 paket (2)

- *opcionalni* programi:
 - u Debian Linux inačici postoje kao **zasebni** paketi
 - u Solaris inačici dolaze u bind paketu
 - nslookup, dig, host
- *dokumentacija*:
 - /usr/local/doc/bind/* ili /usr/share/doc/bind-doc/*
 - ARM html dokumentacija - BIND u detalje!
 - RFC-ovi

CARNet bind9 paket (3)

- posebne značajke:
 - named/bind proces nema root ovlasti, već se koristi pod korisnikom named
 - rndc i rndc.conf
 - **neinteraktivno** popravljjanje postojeće konfiguracije bind4 i bind8 na bind9-kompatibilne
 - nema više chroot() okoline uvedene u CARNet bind8 - nema potrebe za sada
 - uveden **setuid** na **named** grupu

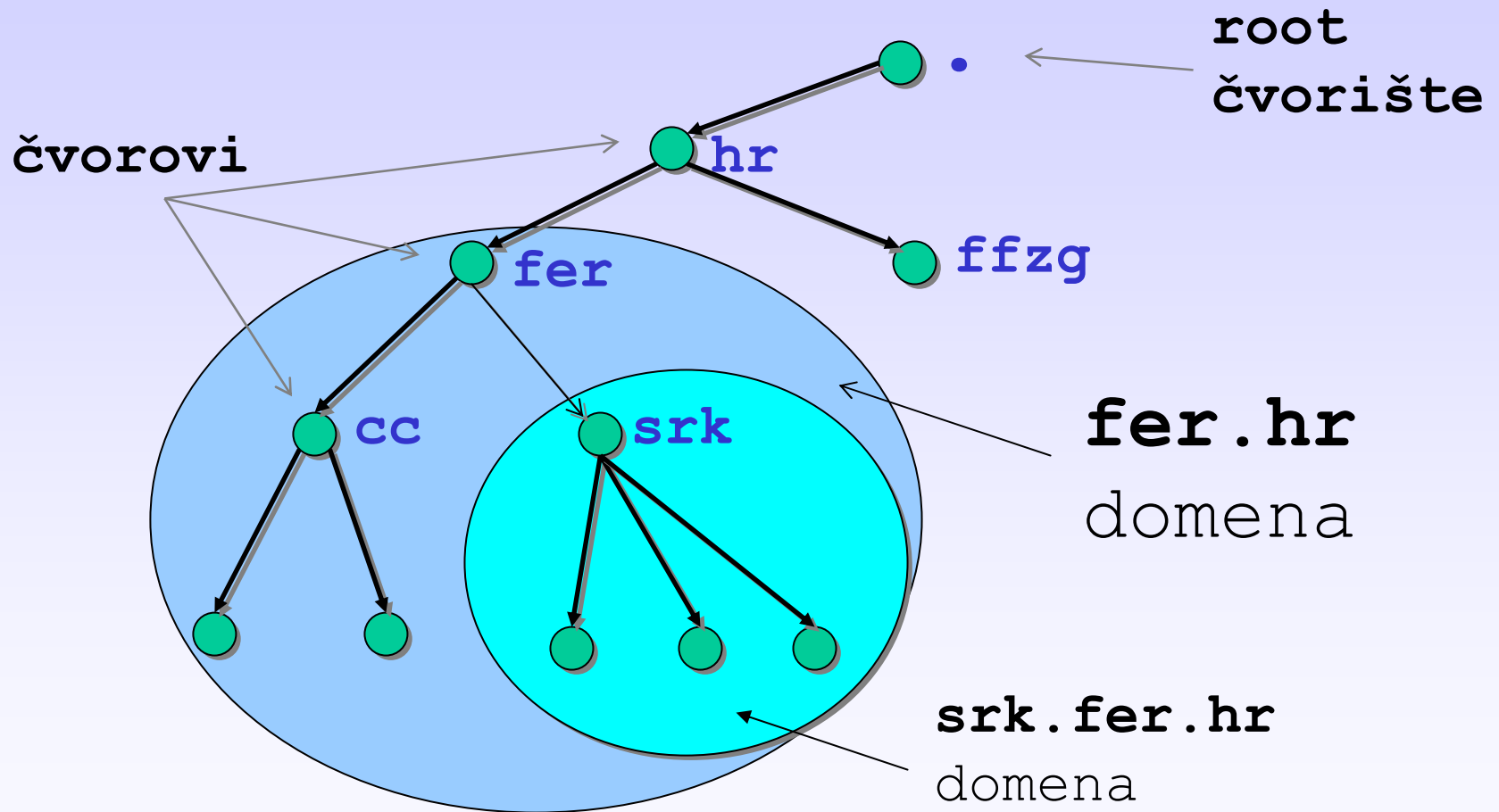
Bind9 vs. BindX, X = {8, 4} (1)

- **bind4** (4.9.8):
 - iznimno poznata (proširenost, rupe, itd.)
 - ne prijavljuje greške u zonama, ili vrlo rijetko
 - postoje OW patchevi - navodno sigurnije
 - named.boot + zone
- **bind8** (8.3.1):
 - recentniji, svejedno mnogo rupa
 - uvodi se named.conf i DNSSEC
 - danas najrašireniji

Bind9 vs. BindX, X = {8, 4} (2)

- kod identičan verziji 4 uz popravke grešaka
- bind8 i bind4 imaju vrlo, vrlo mnogo poznatih rupa
- **bind9 (9.2.0):**
 - posljednja inačica - niz novih vidljivih i nevidljivih mogućnosti
 - sigurnost, kvaliteta, kvalitetniji multithread - uz možda sporiji rad, za sada **nema** poznatih rupa
 - identične zone (dodati **\$TTL!**) i konfiguracija
 - **pogreške u zonama se ne toleriraju**

Domain Name Space



Kratka opća teorija (1)

- stroga hijerarhija sa **glavnim čvorom** ("") = .
- **distribuirana** indeksirana (po imenu) baza
- dužina imena (labela) - maks. 63 znaka
- **FQDN** = kompletno ime sa svim **labelama**, apsolutno prema glavnom čvoru
- u **istom** prostoru **nema dvije iste** labela
- **domena** = podstablo cjelokupnog stabla, ime domene je ime glavnog (najvišeg = **TLD**) čvora u toj domeni

Kratka opća teorija (2)

- podaci o domenama - nalaze se u **RR**
- klase RR: Hesiod, **Internet**, Chaosnet
- TLD: com, edu, gov, mil, net, org, int, arpa + ISO 3166.* domene (2-slovni zapis zemlje)
- **delegacija** = čvorovi/DNS poslužitelji odgovorni za dotičnu zonu (pružanje informacija) (fer.hr domena → labs3.cc.fer.hr poslužitelj)
- **nameserver** = autoritativan za domenu (1+)

Kratka opća teorija (3)

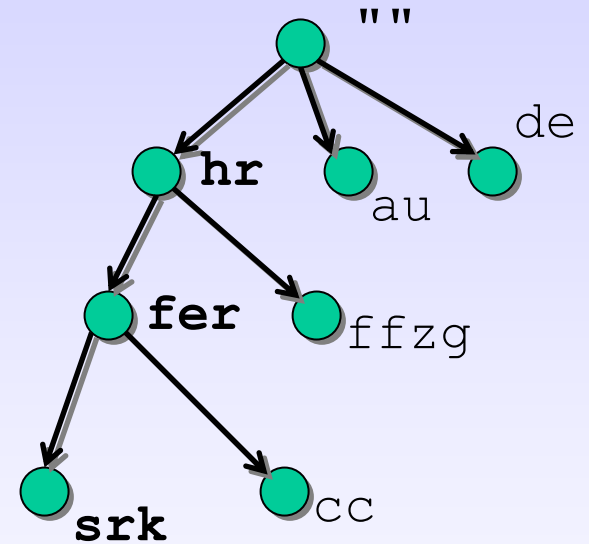
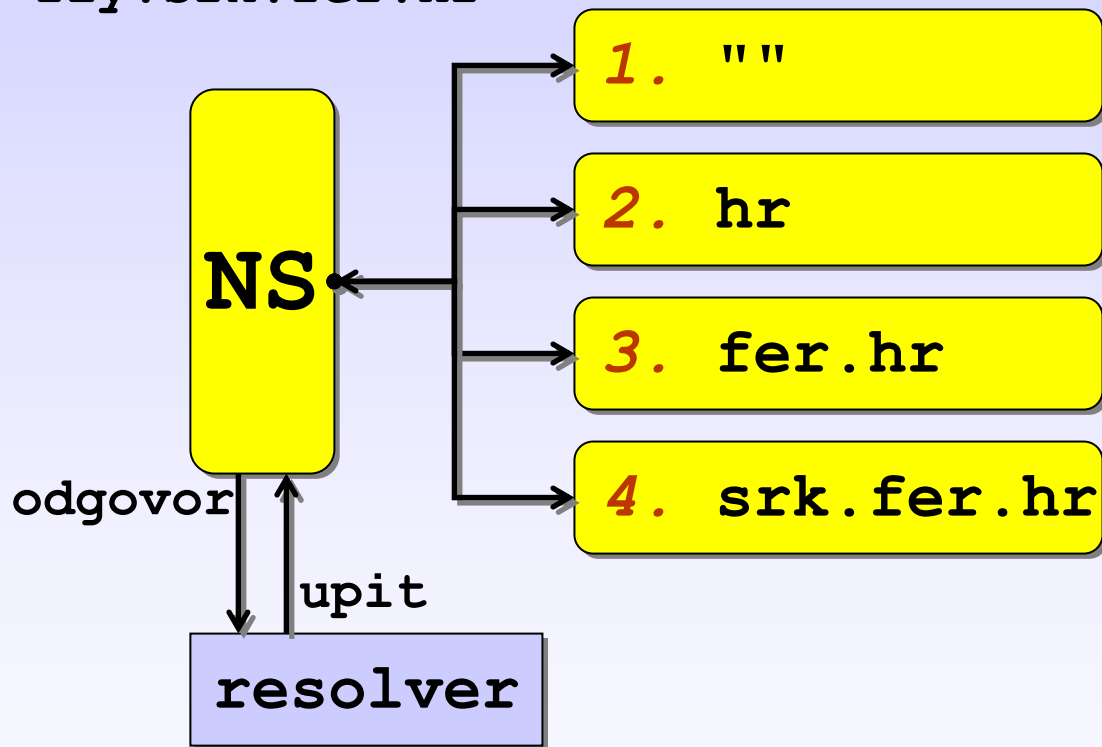
- P: zašto **zona** umjesto domene?
O: zona = samo relevantne informacije za dotični NS u toj domeni
- tipovi DNS poslužitelja:
 - **primarni** - zone čita iz lokalnih datoteka
 - **sekundarni** - kupi zone sa primarnih
 - **cache** - kupi sve podatke iz autoritativnih NS i drži u memoriji do isteka **TTL**
 - **forwarder** - samo prosljeđuje upite dalje
- nužno: **1 primarni i 1 sekundarni po zoni!**

Kratka opća teorija (4)

- **resolver** = klijent koji pristupa NS:
 - libc rutine (gethostbyname() ili gethostbyaddr())
 - adns biblioteka
 - dns helper proces (Netscape itd.)
 - /etc/nsswitch.conf i /etc/resolv.conf (*)
 - nscd, /etc/hosts
- **name resolution** = proces dobivanja podataka od NS
 - ponešto jednostavniji kod cacheiranja podataka!

Kratka opća teorija (5)

traži se:
fly.srk.fer.hr



primjer procesa rezolucije

Kratka opća teorija (6)

- vrste upita:
 - **rekurzivni** - rekurzivni upiti, želimo dozvoliti lokalnim klijentima, ali ne i stranim
 - **iterativni** - NS pogleda i odgovori najbliže što zna
- mapiranje adrese imenima (unazadno):
 - koristi se **in-addr.arpa** domena
 - 32bitni broj (točkasti zapis) + in-addr.arpa
 - inverzni upiti (**inverse query**)
 - nema prosljeđivanja

Konfiguriranje poslužitelja

- osnovna konfiguracija DNS procesa:
 - nekada named.boot - danas **named.conf**
 - niz ključnih riječi, počesto vrlo složeno određivanje
 - potrebno navesti **zone** i master/slave opciju
 - kod slave poslužitelja potrebno je navesti tko je master
 - **master** mora imati čitljive navedene zone
 - **slave** ne treba imati pripremljene zone, one će ionako biti obrisane nakon uspješnog prijenosa
 - ključ za rndc i **rndc.conf** (ili može u rndc.key..)

Osnovno konfiguriranje zona (1)

- 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
- obično su vrijednosti dobro postavljene
- **serijski broj** - važan zbog odluke o retransferu

Osnovno konfiguriranje zona (2)

- **NS** (nameserver):

- poslužitelji za zadanu domenu + SOA!

- ```
srk.fer.hr. IN NS fly.srk.fer.hr.
```

- ```
srk.fer.hr. IN NS burek.srk.fer.hr.
```

- **A** (address):

- ```
fly.srk.fer.hr. IN A 161.53.70.130
```

- ```
burek.srk.fer.hr. IN A 161.53.70.132
```

- **PTR** (pointer):

- ```
130 IN PTR fly.srk.fer.hr.
```

# Osnovno konfiguriranje zona (3)

- **CNAME** (canonical name):
  - alias za stvarno ime hosta
  - postoje restrikcije na upotrebu

```
www CNAME fly
```
- **MX** (mail exchanger):
  - ne smije biti CNAME
  - može biti i za zone i za pojedine hostove
  - pažljivo koristiti!
  - `srk.fer.hr. IN MX 5 fly.srk.fer.hr.`

# Konfiguriranje resolvera

- sistem informirati o raspoloživosti DNS-a
- `/etc/resolv.conf`:
  - `search LISTA_DOMENA`
  - `domain DOMENA`
  - `nameserver ADRESA`
  - `sortlist LISTA_DOMENA`
- ako nam je DNS lokalno:
  - `nameserver 127.0.0.1`
  - ovime se dobivaju značajna ubrzanja

# Potpuno konfiguriran

- potrebne zone:
  - root zona (master)
  - localhost zona (master)
  - 127, 255 i 0 zone (master)
  - naše hostane domene kao i reverse za njih (master/slave)
- podesiti serijski broj, provjeriti \$TTL direktivu na vrhu svake zone (obično 1D)

# Naredba dig

- rijetko korištena
- najčešća sintaksa:
  - `dig @poslužitelj naziv tip`
  - naziv = zapis koji tražimo
  - tip = NS, SOA, AA, CNAME, PTR, itd.
- pomoću njega lako možemo napuniti root zonu:
  - `dig @dns.carnet.hr > named.ca`

# Naredba host

- novijeg datuma
- niz opcija, jedan od moćnijih i jednostavnijih alata
- najčešće:
  - `host -a burek.srk.fer.hr`
  - `host -t NS srk.fer.hr dns.hinet.hr`
- niz opcija, podešavanja, itd.
- može služiti i kao alat za detekciju pogreški
- razumije više podataka u DNS-u od ostalih

# Naredba nslookup

- nekad osnovna naredba
- danas se **izbacuje** iz upotrebe
- naredbe unutar:
  - root, finger, ls
  - set (+ mnogobrojni parametri)
- nespretnan za korištenje, itd.
  - nslookup, set debug type=soa, srce.hr
  - nslookup jagor.srce.hr

# Osnovne razlike 4 vs. 9 (1)

- `named.boot` - `named.conf`
- eksplicitni `$TTL`
- nema višestrukih CNAME sa istim originalom:
  - `www.ex.com. CNAME host1.ex.com.`
  - `www.ex.com. CNAME host2.ex.com.`
- nema miksanja CNAME + nešto:
  - `www.ex.com. CNAME host1.ex.com.`
  - `www.ex.com. MX 10 host2.ex.com.`

## Osnovne razlike 4/8 vs. 9 (2)

- nema toleriranja grešaka u zonama:
  - potrebno koristiti `named-checkzone`
- problemi komunikacije `bind4` - `bind9`:
  - `transfer-format many-answers;`
  - odnosno promijeniti u
  - `transfer-format one-answer;`
- nešto drukčije kategorije logiranja
- `notify-source` i `transfer-source` (bivši `query-source`)

## Osnovne razlike 4/8 vs. 9 (3)

- točke u SOA serijskom broju nedozvoljene:
  - 3.00, SCCS podrška i sl.
- nedozvoljeni nezatvoreni navodnici:
  - host TXT "foo
- nema prenošenja ( u više redova, ( započinje blok i mora biti u prvoj liniji):
  - @ IN SOA ns.ex. hostmaster.ex.  
( 1 3600 1800 1814400 3600 )
- \\$ za umetanje "\$" u zonu umjesto \$\$

# Osnovne razlike 4/8 vs. 9 (4)

- set znakova za imena - 8bit clean
- ndc postao rndc
- bind8 postavljao umask na 022, bind9 to ne radi
- bug u Win2k DNS prilikom transfera zona - rješenje:
  - `transfer-format one-answer;`

# Korištenje Binda

rndc, česte greške, master/slave,  
provjera grešaka, klase hostova,  
MX i problemi..

# Naredba rndc

- umjesto stare **ndc** naredbe
- upravljanje procesom bind
- komunicira preko TCP veze, autentificira se lozinkom iz [rndc.key/rndc.conf](#)
- opcije:
  - startanje, stopanje, debugiranje (querylog), verbose, itd.
- primjer:
  - `rndc querylog`

# Master/slave

- slave sam prima podatke (zone transfer)
- master pri promjeni serijskog broja i reload (rndc reload) obavijesti (notify) sve slave poslužitelje (iz NS polja)

```
- zone "eng.example.com" {
 type slave;
 file "eng.example.com.bk";
 masters { 192.168.4.12; };
};
```

# Provjera konfiguracija/zona

- programi iz paketa:
  - `named-bootconf.sh < /etc/named.boot > /etc/named.conf`
  - **named-checkconf**
  - **named-checkzone**
- vanjski programi:
  - `host`, `dig`, `nslookup`
  - `dnswalk`, `nslint`
  - `nessus`

# Program nslint

- radi **lokalno** na DNS poslužitelju
- detektira najčešće greške u zonama:
  - krivo definirane zapise
  - krivo postavljene točke (nedostaje na kraju i sl)
  - imena sa nedozvoljenim znakovima
  - imena bez potrebnog reverse i obrnuto, itd. itd.
- upotreba:
  - `nslint -c /etc/named.conf`

# Program dnswalk

- radi udaljeno, samo na poslužiteljima koji nam dozvole transfer zone
- opcija -F = vrlo važno, provjera back-forward za imena i reverse (lame host i sl)
- opcija -l = provjera za lame delegacijama
- upotreba:
  - `dnswalk srk.fer.hr.`
  - `dnswalk 70.53.161.in-addr.arpa.`

# Saznavanje verzije

- starije verzije - exploiti, rupe, itd.
- zašto dozvoliti interne podatke poslužitelja?
- dva rješenja:
  - redefinirati chaos/txt klasu
  - definirati version "TEKST" opciju u named.conf
- kako doznati tuđu verziju:
  - `nslookup -query=txt -class=chaos version.bind fly.srk.fer.hr`
  - `host -t txt -c chaos version.bind labs3.cc.fer.hr`

# Klase hostova u konfiguraciji

- mnogo hostova za dozvole - prevelika i nespretna konfiguracija
- moguće definirati vlastite klase
- ključna riječ je "acl":
  - `acl "xfer", acl "trusted", acl "bogon"`
  - koristimo kasnije umjesto listi hostova
  - `allow-recursion { trusted; };`
  - `allow-query { trusted; };`
  - `blackhole { bogon; };`

# Forwardanje / rekurzija

- DNS neće sam raditi rezoluciju, već proslijedi dalje - najčešće za ISP-ove
- primjer:
  - `forward only;` ili `forward first;`
  - `forwarders { 195.29.150.3;  
161.53.123.3; };`
- rekurzija - zabraniti za vanjske hostove zbog cache-poisoning napada:
  - `allow-recursion { trusted; };`

# MX zapisi

- moguće definirati:
  - više MX za pojedini host
  - više MX za cijelu domenu
- kamo će prvo poslati - odlučuje MX cost, numeričko polje u MX zapisu:
  - `MX 5 fly`
  - `MX 10 burek`
  - nižem se šalje prvo
  - pripaziti na relay (Cw i sl.) i mail-loopback (MX list)

# Veća sigurnost

- obavezno:
  - zabraniti **rekurzije** izvana
  - zabraniti **nedozvoljene** mreže
  - dozvoliti transfer **samo** željenim NS
  - ugasiti verziju
  - zone i conf nečitljivi običnim korisnicima
- opcionalno:
  - **chroot** okolina
  - svaki bind na **unutrašnji** i **vanjski** daemon

# Najčešće greške

- **komentari** - mora biti isključivo ";" u zonama, a u conf mora biti "#"
- **točka** - završava ime, ako ne postoji dodaje se domena
- **krivi NS ili SOA** = lame server
- **nedostajući/krivi PTR** = fwd-bwrđ provjera
- razno: nema \$TTL, krivi \$ORIGIN, dupliciranje, krive datoteke za slave, itd.

# Opcionalna polja (1)

- **AAAA** = IPv6 adresa - prešlo u **A6**:
  - burek.ip6 A6 3ffe:b80:3c0:3::2
- **HINFO** (host information):
  - burek HINFO "SS2" "Linux 2.2.x"
- **TXT** (text):
  - burek TXT "FER IRC server"
- **RP** (responsible person)
- **DNAME** - delegacija reverse adresa

## Opcionalna polja (2)

- **WKS** (well known services) - prešao u **SRV**:
  - `_http._tcp.example.com. SRV 10 5 80. www.example.com`
- **KEY, NXT, SIG** = DNSSEC
- eksperimentalno:
  - **AFSDB** - za AFS baze podataka
  - **ISDN** - reprezentiranje ISDN adresa
  - **LOC** - za GPS podatke
  - **RT** - routing informacije za non-WAN strojeve
  - **X25** - X.25 mrežne adrese

# Napredno korištenje

potpisivanje zona, load balancing,  
dinamičke adrese, wildchars,  
točke u nazivima

# DNSSEC (1)

- kriptografsko autentificiranje
- stvaranje vlastitog ključa
  - `dnssec-keygen -a DSA -b 512 -n ZONE srk.fer.hr`
- rezultat:
  - `Ksrk.fer.hr.[BROJ].private`
  - `Ksrk.fer.hr.[BROJ].key`
- stvaranje seta ključeva:
  - `dnssec-makekeyset srk.fer.hr.[BROJ]`

# DNSSEC (2)

- potpisati keyset vlastitim ključem:
  - `dnssec-signkey keyset-srk.fer.hr`  
`Ksrk.fer.hr.[BROJ]`
- uključiti ključ u samu zonu:
  - `$INCLUDE Ksrk.fer.hr.+001+32322.key`
- potpisati samu zonu:
  - `dnssec-signzone srk.fer.hr`  
`Ksrk.fer.hr.[BROJ]`
- dobivenu zonu "srk.fer.hr.zone.signed" staviti u `named.conf`

# DNS spoofing - cache poisoning

- zbuniti DNS dajući krive informacije
- napadač pošalje rekurzivni upit poslužitelju
- odgovor na takav upit se nalazi u zoni koju kontrolira napadač
- odgovor sadržava autoritativni (lažni!) zapis za domenu koji kontrolira netko treći
- naš DNS sada ima lažnu adresu koju može cacheirati - čime naš DNS postaje "rupa"

# Load balancing

- jeftini load balancing - round robin tipa

- primjer:

```
- www 600 IN A 10.0.0.1
 600 IN A 10.0.0.2
 600 IN A 10.0.0.3
```

- slučajnim odabirom se vrte mogućnosti
- shemu odabira u Bind9 nije moguće mijenjati
- nepravilna raspodjela - vidjeti bolji SRV

# Signali

- signali koje named proces razumije:
  - SIGHUP - ponovno iščitavanje konfiguracija (zone, conf)
  - SIGTERM - završi i izađi
  - SIGKILL :-)
  - SIGINT - završi i izađi

# TSIG (1)

- Transaction SIGnatures - za dodatnu sigurnost u razmjeni podataka između servera - npr. dinamički update
- stvorimo 128 bit base64 kodirani ključ:
  - `dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2.`
- dobijemo "Khost1-host2.+157+00000.private." sa sadržajem:
  - Key: `La/E5CjG90+os1jq0a2jdA==`

# TSIG (2)

- u svaki named.conf dodamo:
  - `key host1-host2. { algorithm hmac-md5; secret "La/E5CjG90+os1jq0a2jdA==" ; };`
- u host1 dodamo (a host2 ima IP 10.1.2.3):
  - `server 10.1.2.3 { keys { host1-host2. ; } ; };`
- ili recimo:
  - `allow-update { key host1-host2. ; };`

# Dinamički update

- specifikacije RFC 2136
- pojedine zone moguće updateati izvana - npr. klijent pošalje promjene glavnom poslužitelju
- ključne riječi **allow-update** i **update-policy**
- pri tome se stvara log promjena (.jnl):
  - `rndc stop; rm *jnl; vi hosts.db; /etc/init.d/bind start`
- primjeri:
  - DHCP + DNS
  - [dyndns.org](http://dyndns.org)

# Wildcard

- zapis od znaka "\*" (samo jedan znak)
- omogućava jedan zapis umjesto više:
  - 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
```

# Točke u nazivlju

- dozvoljeno je imati ime (label) poslužitelja sa točkom u imenu
- primjer:
  - mali.pero IN A 161.53.70.121
- primjedba:
  - u većini slučajeva resolv.conf postavke i pretraživanje po kratkom imenu za ovakav naziv neće raditi