DNS,BIND - jednoduche zaklady

Jiri Kubina

jiri.kubina@osu.cz

Ver. 1.0

unor 2006

Obsah

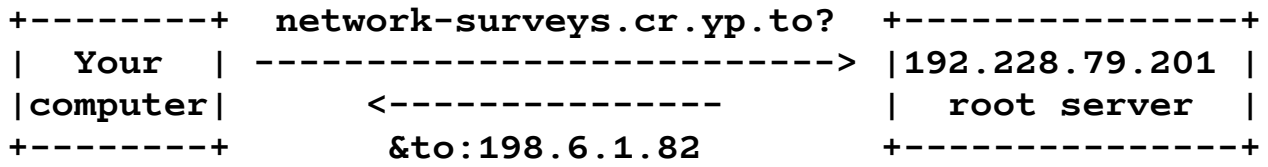
Upozorneni: Vetsina popisovanych principu je zjednodusena, nebo zkracena z vyukovych duvodu. Pro ziskani kompletnich informaci ctete RFC.

1.Jak funguje DNS – zjednoduseny princip

- Protokol DNS pracuje zpusobem **dotaz-odpoved**
- Protokol DNS je protokol **aplikacni** vrstvy, neresi proto otazku vlastniho prenosu paketu
- Pouziva oba transportni protokoly **UDP** i **TCP**
- U dotazu na preklad (zadost o RR) dava prednost UDP. Pokud je odpoved delsi nez **512B** vlozi se do UDP pouze část nepresahujici 512B a nastavi se TC bit ze odpoved je neuplna. Klient si muze kompletni odpoved vyzadat protokolem TCP
- DNS server nasloucha na portu 53

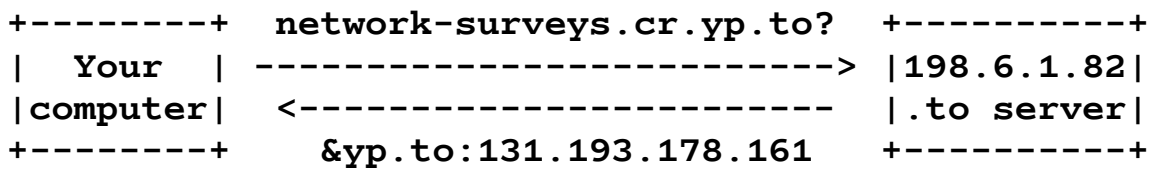
Proces iterace

Predpokladejme ze Vas DNS server chce zjistit IP adresu **network-surveys.cr.yp.to** . Aby ji zjistil bude muset kontaktovat nekolik DNS serveru. Jako prvni kontaktuje **korenovy DNS server** /v mem pripade to byl 192.228.79.201/. Tento server ma ulozenu informaci, ze o zaznamy domeny **.to** se stara DNS server 198.6.1.82 a tuto informaci Vam zasle.



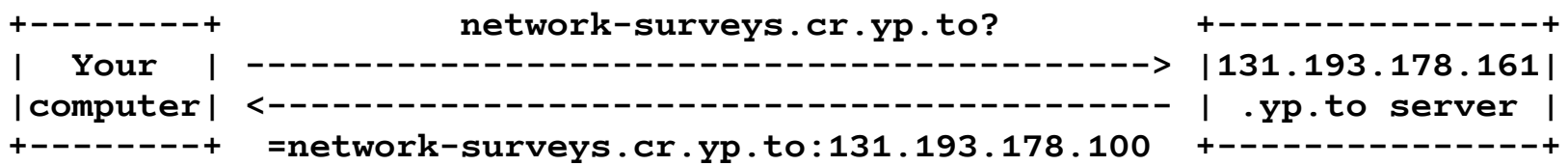
Tato odpoved &to:198.6.1.82 je **delegation** a rika nam ze: Na informace o domene **.to** se ptejte DNS serveru na IP adrese **198.6.1.82**

DNS server 198.6.1.82 ma ulozenu informaci, ze o zaznamy domeny **.yp.to** se stara DNS server 131.193.178.161 . Vas DNS server se ho zepta na stejny dotaz a on mu odpovi.



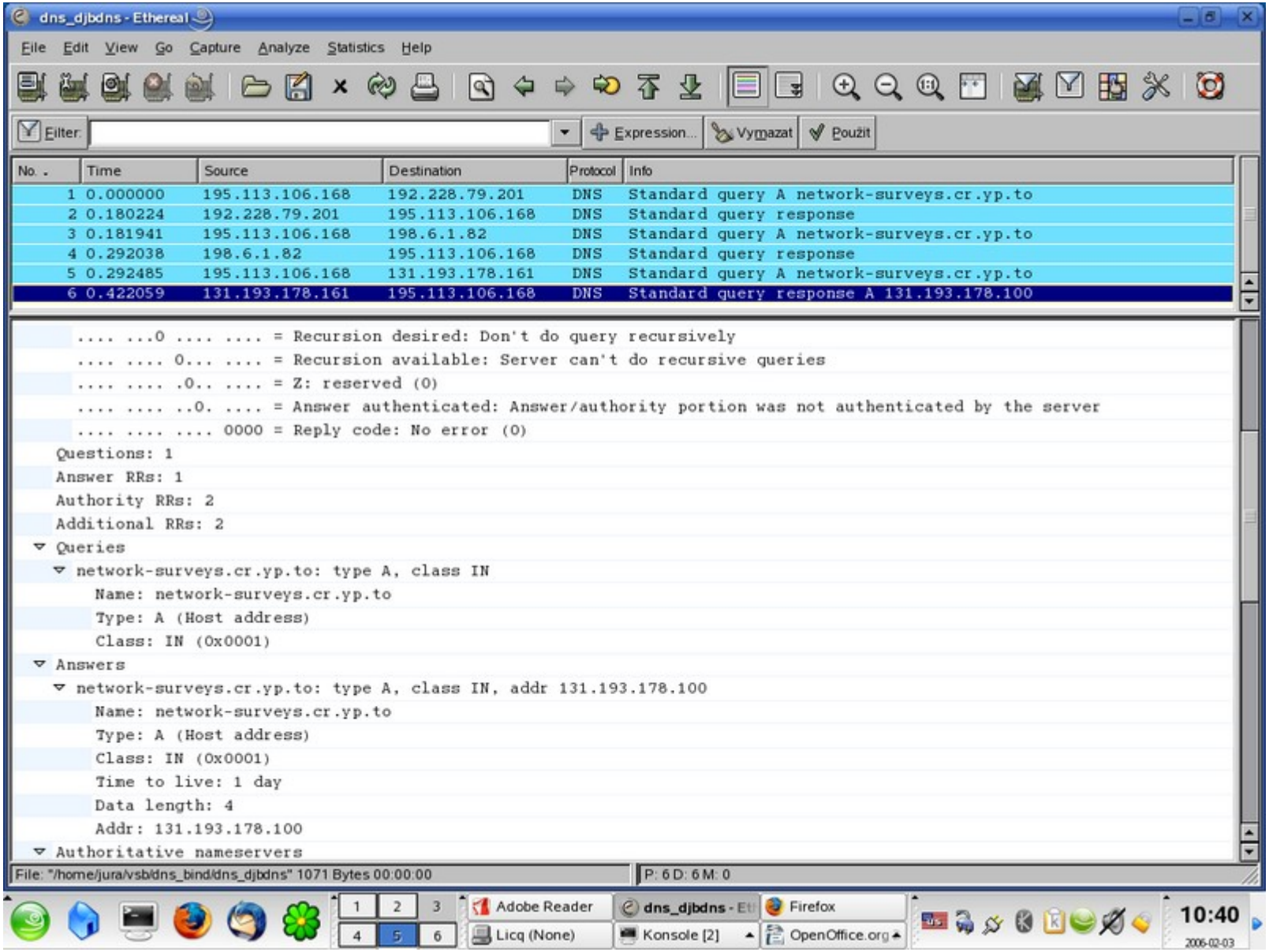
Odpoved &yp.to:131.193.178.160 je dalsi delegation a rika nam ze:
Na informace o domene **.yp.to** se ptejte DNS serveru na IP adrese **131.193.178.161**

DNS server 131.193.178.161 na ulozenu informaci ze **network-surveys.cr.yp.to** ma IP adresu **131.193.178.100** . Vas DNS server se jej zepta na stejny dotaz a obdrzi odpoved.



Odpoved **=network-surveys.cr.yp.to:131.193.178.100** je finalni odpovedi na puvodni dotaz:
IP adresa network-surveys.cr.yp.to je 131.193.178.100

DNS dotaz - iteracni



2.RR – Resouce Records

Informace o domenovych jmenech a jim odpovidajicich IP adresach jsou ulozeny v pameti jmennych serveru ve tvaru zdrojovych vet – **Resource records – RR**

Nejpouzivanejsi typy RR

A	A host address
NS	Authoritative name server
CNAME	Canonical name
SOA	Start Of Autority
PTR	Domain name Pointer
MX	Mail exchange
TXT	Text string
AAAA	Ipv6 address

3.Resolver

- Resolver je cast systemu zabyvajici se prekladem IP adresy
- Resolver neni konkretni program
- Resolver je soustava knihovnich funkci, která se linkuje s aplikacemi, ktere pozaduji tyto sluzby /telnet,ftp,ssh/
- Resolver pozaduje od jmenneho serveru uplnou /rekurzivni/ odpoved na svuj dotaz.

Konfigurace resolveru – Linux/Unix

/etc/resolv.conf

```
domain osu.cz
nameserver 195.113.106.10
search vsb.cz cvut.cz
```

Konfigurace resolveru, ktera urcuje poradi dotazovani /soubor /etc/hosts nebo DNS pripadne jinde/ je ulozena ve starsich verzich v souboru /etc/host.conf v novejsich verzich v komplexnejsim souboru /etc/nsswitch.conf

/etc/host.conf

```
order hosts,bind
```

/etc/nsswitch.conf

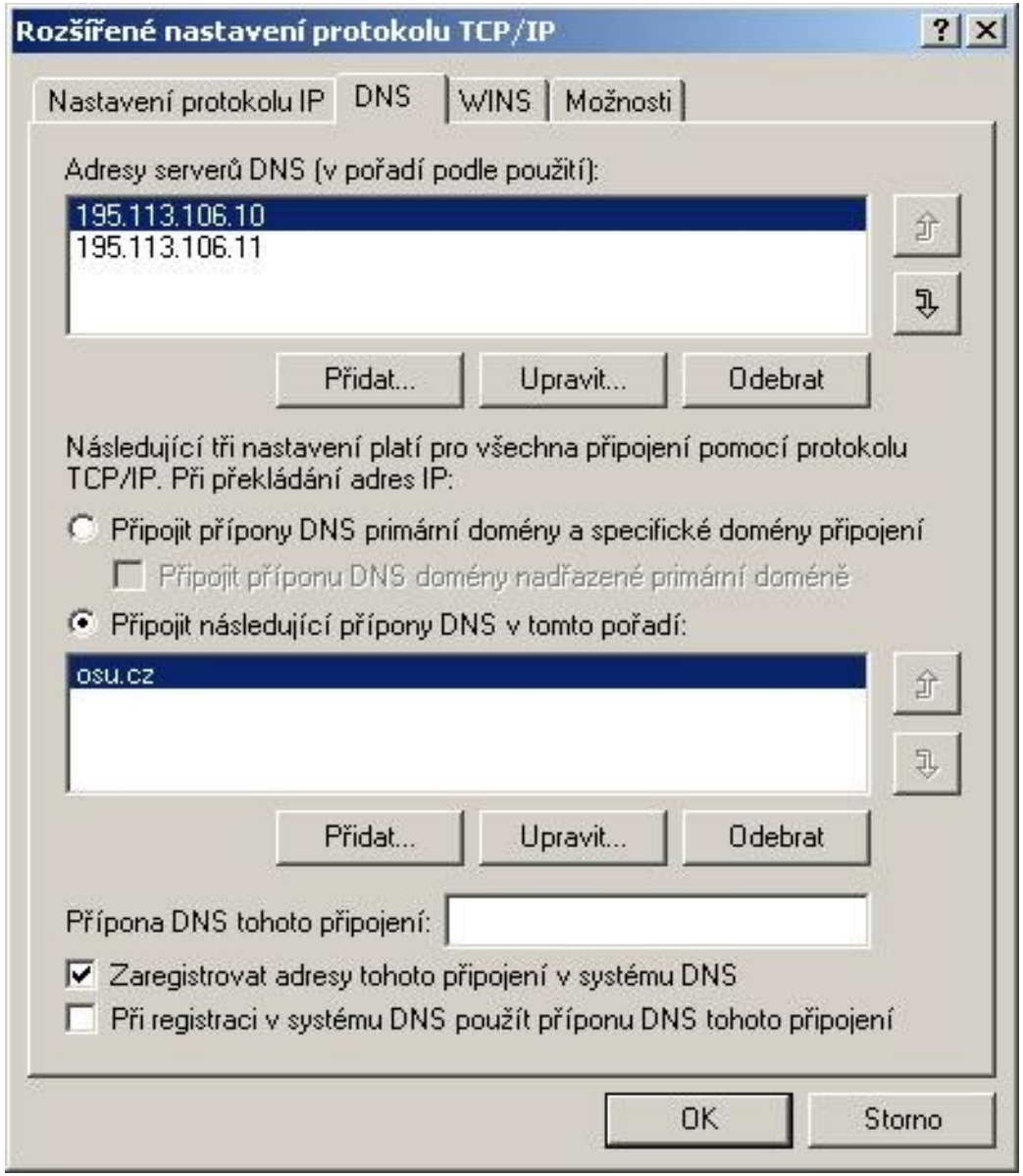
```
hosts:      files dns
```

Konfigurace resolveru – Windows 2000 a vyse

- Standardne spustena sluzba - **Klient DNS**
- Jedna se o cache resolver
- Obsah cache lze zobrazit - **ipconfig /displaydns**
- Obsah cache lze vymazat - **ipconfig /flushdns**
- Parametry cache resolveru lze ovlivnovat zmenou klicu regisru Windows:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters

Priklad konfigurace resolveru Windows 2000 a vyse



4.Typy jmennych serveru

Autoritativni - jsou jmenne servery, ktere uchovavaji vsechny informace o hostitelich prislusne zony. Kazdy dotaz na hostitele uvnitr zony skonci na nejakem autoritativnim serveru /pro jednu zonu jich muze byt i vice/

Autoritativni servery /pokud je jich vice nez jeden/ musí byt velice dobre synchronizovane. Toho dosahneme tim, ze jeden z autoritativnich serveru bude **master /primarni/.** Tento master autoritativni server nacita informace o vsech zonach, ktere spravuje z datovych souboru. Ostatní autoritativni servery budou pracovat jako **slave /sekundarni/** a budou informace o zonach prenaset z master /primarniho/ autoritativniho serveru.

Neautoritativni - vsechny ostatni, ktere neuchovavaji informace o zonach, vcetne caching-only

5.BIND

Pravdepodobne nejrozsirenejsi jmenny server na systemech Linux/Unix je v soucasne dobe program **named** /cti nejmdi/, kteremu se podle mista vzniku také rika BIND /Berkeley Internet Name Domain/.

Vzhledem k dulezitosti sluzby DNS prosel named bourlivym vyvojem. V praktickem nasazeni se pak v dnesni dobe prosazuji nejcasteji verze 8 a 9. Ukazky a konfiguracni volby uvedene nize jsou vybrany z oficialni dokumentace verze 9.

Od verze 8 je konfiguracnim souborem soubor **/etc/named.conf** . Named muze bezet v takzvanem chroot prostredi a taky se toho vetsinou vyuziva /bezpecnost/.

Samozrejme existuji k programu named alternativy. Jako nahradu, ktera dba predevsim na bezpecnost bych doporucoval **djbdns**.

Konfiguracni prikazy souboru /etc/named.conf - vytah

acl	accesslist - definuje seznam IP adres /pristupy/
control	definice rizeni ridici utilitou rndc
include	vklada soubor
key	informace pouzivane pri autentizaci a autorizaci
logging	konfiguruje system logovani
option	celkova konfigurace serveru
zone	definice zony

Priklad jednoduche konfigurace autoritativniho master name serveru /etc/named.conf

```
options {
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
};

include "/etc/rndc.key";

controls {
    inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};

zone "." {
    type hint;
    file "named.ca";
};

zone "localhost" {
    type master;
    file "localhost.hosts";
    allow-update { none; };
};

zone "0.0.127.in-addr.arpa" {
    type master;
    file "localhost.rev";
    allow-update { none; };
```

```
};

zone "firma1" {
    type master;
    file "/var/named/firma1.hosts";
    };

zone "30.152.10.in-addr.arpa" {
    type master;
    file "/var/named/10.152.30.rev";
    };
```

Priklad jednoduche konfigurace autoritativniho slave name serveru /etc/named.conf

V konfiguracnim souboru se meni pouze definice zonovych souboru /bude je stahovat z master name serveru pomoci zone transfer/.

```
zone "firma1" {
    type slave;
    file "/var/named/slaves/firma1.hosts";
    masters {195.113.106.168;};
    };

zone "30.152.10.in-addr.arpa" {
    type slave;
    file "/var/named/slaves/10.152.30.rev";
    masters {195.113.106.168;};
    };
```

Nektere dulezite konfiguracni parametry

recursion no; zakazuje nameserveru odpovidat na rekurzivni dotazy /provadet iteracni dotazovani – rovnou klienta odkaze na nadrizenou autoritu/

allow-recursion {10.0.0.0.24;}; povoli rekurzivni dotazy ze zadaneho rozsahu

allow-query {10.0.0.0/24;}; omezi moznost dotazovat se pouze ze zadaneho rozsahu IP

allow-transfer {10.0.0.3;}; omezi moznost provadet zone transfer

forward (only | first); server bude provadet rekurzivni dotazy na servery uvedene v parametru forwarders /nebude pouzivat iteraci/

forwarders {10.2.3.4;}; seznam serveru, kterych se bude nas server rekurzivne dotazovat

acl {10.2.3.0/24;10.3.4.5/24;}; accesslist pojmenovany seznam rozsahu IP ktery se muze pouzit v predchozich volbach misto IP adres

Priklad hint zony /var/named/named.ca - zkraceno

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:    Jan 29, 2004
;       related version of root zone:   2004012900
;
; formerly NS.INTERNIC.NET
;
.                        3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
;
; formerly NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     192.228.79.201
;
; formerly C.PSI.NET
;
.                        3600000      NS    C.ROOT-SERVERS.NET.
```

Priklad Forward a Reverse localhost zony

Forward - /var/named/localhost.hosts

```
$TTL 1W
@               IN SOA  @   root (
                                42              ; serial
                                2D              ; refresh
                                4H              ; retry
                                6W              ; expiry
                                1W )            ; minimum

                IN NS           @
                IN A            127.0.0.1
```

Reverse - /var/named/localhost.rev

```
$TTL 1W
@               IN SOA          localhost.   root.localhost. (
                                42              ; serial
                                2D              ; refresh
                                4H              ; retry
                                6W              ; expiry
                                1W )            ; minimum

                IN NS           localhost.
1               IN PTR          localhost.
```

Pouzite jednotky:
D - day, H – hour, W – week, bez jednotek – sekundy nebo seriove cislo souboru

Priklad jednoduche forward zony /var/named/firma1.hosts

```
$ttl 38400
firma1. IN      SOA     ns.firma1. jura.firma1. (
                        1139050797  ;serial
                        10800       ;refresh
                        3600        ;retry
                        604800      ;expire
                        38400 )     ;TTL

firma1.             IN       NS       ns.firma1.
ns.firma1.          IN       A        10.152.30.3
pc1.firma1.         IN       A        10.152.30.4


;delegace domeny neco.firma1
neco.firma1.        IN       NS      ns.neco.firma1.
;glue zaznam aby bylo mozno najit ns pro domenu neco.firma1
ns.neco.firma1.     IN       A       10.152.31.5
```

Vysvetleni udaju SOA

firma1.	jmeno zony pro kterou jsou tyto zaznamy autoritativni
IN	typ adresy IN (Internet)
SOA	Start Of Authority
ns.firma1.	jmeno master nameserveru pro tuto zonu
jura.firma1.	mailovy kontakt na spravce zony /@ = ./
1139050797	**serial** - seriove cislo souboru
10800	**refresh** - cas po kolika sek se refreshuji slave servery
3600	**retry** - cas po kolika sek to zkousi slave servery znovu pokud byl predchozi pokus neuspesny
604800	**expire** - cas po kterem prestane poskytovat slave server informace /v pripade ze se nepodari kontaktovat master/
38400	**TTL** – plati pro kazdy zaznam. Je poskytovan nameserverem v kazde odpovedi. Rika jak dlouho mohou neautoritativni servery udrzovat zaznam ve sve cache /0 = no cache/.

Priklad jednoduche reverse zony /var/named/10.152.30.rev

```
$ttl 38400
30.152.10.in-addr.arpa. IN SOA jurasek.firma1. jura.firma1.(
                        1139142009
                        10800
                        3600
                        604800
                        38400 )

30.152.10.in-addr.arpa.    IN       NS    jurasek.firma1.
3.30.152.10.in-addr.arpa.  IN       PTR   jurasek.firma1.
4.30.152.10.in-addr.arpa.  IN       PTR   pc1.firma1.
```

6.BIND – caching-only

Jedna se o specialni typ konfigurace programu **named**. V této konfiguraci **neni** server **autoritativni** pro zadnou domenu. Zpracovava pouze dotazy od ostatnich pocitacu a vsechny **zodpovedne dotazy uklada do vyrovnavaci pameti**. Dalsi dotaz na stejnou adresu jiz zodpovida z vyrovnavaci pameti. Zaznamy ve vyrovnavaci pameti se udrzuji po dobu jejich zivotnosti **TTL**.

Alternativni DNS cache programy:

- **dnscache** – z baliku djbdns
- **pdnsd** – umoznuje udrzet obsah cache po restartu
- **dnsmasq**

Priklad konfigurace named jako caching-only serveru

```
acl "intranet" { 195.113.106.0/24; };

options {
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    allow-query { "intranet"; };
};

include "/etc/rndc.key";

zone "." {
   type hint;
   file "named.ca"; };

zone "0.0.127.in-addr.arpa" {
   type master;
   file "localhost.rev";
   notify no;};
```

7.RNDC – remote name server control

rndc - je utilita umoznujici **zabezpecene vzdalene ovladani** name serveru. Umoznuje spravci provadet na nameserveru nize uvedene akce. Autentizace spojeni se provadi symetrickym klicem. Komunikace probiha na portu TCP 953 /pozor na firewall – prapodivne tuhnuti nameserveru pri shutdown serveru/.

reload	reload konfiguracniho a zone souboru
reconfig	reload konfiguracniho a zmenenych zone souboru
stats	zapis statistik do souboru
querylog	zapne logovani dotazu do souboru
dumpdb	vypis cache nameserveru do dump souboru
stop	stop serveru a zapis zmen ziskanych IXFR
halt	okamzity stop serveru
trace	zvyseni ladici urovne serveru o 1 /logy/
notrace	nastaveni ladici urovne serveru na 0 /logy/
flush	vymazani cache nameserveru
status	vypis stavu serveru

8.Nastroje pro testovani DNS

- nslookup
- host
- dig
- dnswalk

nslookup – dva rezimy /interaktivni a neinteraktivni/

server decsys.vsb.cz	nastavi server ktereho se budeme dotazovat
set q=mx	nastavi typ dotazu /mx,ns,soa,any/
set debug	nastavi uroven vypisu /set d2/
set nosearch	zrusi pridavani domenovych pripon
set norecurse	zrusi rekurzivni dotazovani na jmenne servery / jako nameserver/

nslookup -q=ns vsb.cz	vypise nameservery domeny vsb.cz
nslookup -q=soa vsb.cz	vypise SOA domeny vsb.cz
nslookup -q=mx vsb.cz	vypise mailservery domeny vsb.cz

host

host [-a] [-t typ_zaznamu] jmeno [server]

-a	nastaví filtr pro jakykoliv typ zaznamu
-t typ_zaznamu	nastaví filtr na dany typ záznamu (napr. "-t mx"). Standardne se pouziva typ "A".
-l	vypise celou domenu - zone transfer
jmeno	domenova alebo IP adresa, pro kterou se ma ziskat zaznam
server	adresa DNS serveru, ktery se ma pouzit pro zjisteni zaznamu

host www.osu.cz	zjisti IP adresu pro domenove jmeno
host 10.0.0.2	zjisti domenove jmeno pro IP
host -t mx vsb.cz	zjisti MX zaznamy pro domenu vsb.cz
host www.vsb.cz oudec.osu.cz	pozada server oudec.osu.cz o preklad domenoveho jmena na IP adresu
host -lv -t any osu.cz	vypise vsechny domenove zaznamy pomoci zone transfer

dig

dig -t typ_zaznamu [@server] jmeno

-a	nastaví filtr pro jakykoliv typ zaznamu
-t typ_zaznamu	nastaví filtr na dany typ záznamu (napr. "-t mx"). Standardne se pouziva typ "A".
-x	reverzni preklad
jmeno	domenova alebo IP adresa, pro kterou se ma ziskat zaznam
server	adresa DNS serveru, ktery se ma pouzit pro zjisteni zaznamu

dig www.osu.cz	zjisti IP adresu pro domenove jmeno
dig -x 10.0.0.2	zjisti domenove jmeno pro IP
dig -t mx vsb.cz	zjisti MX zaznamy pro domenu vsb.cz
dig www.vsb.cz @oudec.osu.cz	pozada server oudec.osu.cz o preklad domenoveho jmena na IP adresu
dig osu.cz axfr	vypise vsechny domenove zaznamy pomoci zone transfer

dnswalk

dnswalk osu.cz.

-a kontroluje duplicitu A zaznamu
-d vypis debug informaci
-r projde rekurzivne subdomeny zadane domeny
-i potlaci testovani nestandardnich znaku v domenovych jmenech
-l testuje "lame-delegation". U kazdeho NS zaznamu vyzkousi zda uvedeny nameserver da autoritativni odpoved

9.Pouzite zdroje a nastroje

Zdroje

- Velky pruvodce protokoly TCP/IP a systemem DNS – L.Dostalek A.Kabelova
- http://cr.yp.to/djbdns/intro-dns.html
- http://www.isc.org/index.pl?/sw/bind/
- http://knihy.cpress.cz/DataFiles/Book/00000675/Download/K0819.pdf

Nastroje

- ethereal
- tcpdump
- nslookup, host, dig
- dnswalk

Dekuji za pozornost