Úvod do DNS

CZ.NIC, z. s. p. o.

Zbyněk Michl
<*zbynek.michl@nic.cz*>

Ondřej Surý
<*ondrej.sury@nic.cz*>

9. února 2011

Organizace

- Celková délka školení cca 12 hodin
- Dvě malé přestávky
- Přestávka na oběd
- Otázky rovnou v průběhu školení
- Prosím nenoste do učebny jídlo

Požadavky

- Znalost IP / UDP / TCP
- Obecné povědomí o DNS
- Orientace v GNU/Linux prostředí

Obsah (den první)

- Základní popis DNS
- Správa DNS hierarchie
- RR záznamy
- Rekurzivní server
  - Konfigurace Unbound
  - Konfigurace Bind 9
- Formát zónového souboru
- Autoritativní server
  - Konfigurace NSD 3
  - Konfigurace Bind 9

Obsah (den druhý)

- Rozšířená témata
  - Wireformat DNS zprávy
  - EDNS0
  - TSIG
  - DNS anycast
  - DNSSEC
  - IDN
- Ladění a trasování DNS
  - Problémy s DNS
  - tcpdump / wireshark

Cíle školení

- Pochopit princip DNS
- Umět nakonfigurovat rekurzivní server
- Umět nakonfigurovat autoritativní server
- Umět nakonfigurovat vlastní doménu
- Umět hledat a najít problém v DNS

Obecně

- Všechny materiály ke kurzu jsou dostupné na http://public.nic.cz/files/zmichl/courses/dns/
  - Tato prezentace + cvičení
  - Ukázkové konfigurační příklady
  - Další související materiály
- Přístup na shell uživatele root:

```
$ sudo -s
```

- Startovací skripty:

```
# /etc/init.d/<nazev> start|stop|restart
```

Obecně

- Nastavení repozitářů:

```
# editor /etc/apt/sources.list
# apt-get update
```

- Instalace software:

```
# apt-get install <nazev>
```

Obsah (den první)

- **Základní popis DNS**
- Správa DNS hierarchie
- RR záznamy
- Rekurzivní server
  - Konfigurace Unbound
  - Konfigurace Bind 9
- Formát zónového souboru
- Autoritativní server
  - Konfigurace NSD 3
  - Konfigurace Bind 9

Domain Name System
Základní principy a pojmy

Proč DNS?

- IP adresy
  - Špatně se pamatují
  - Identifikují „počítač“ a nikoli službu
  - Více služeb na jedné IP adrese
  - Malá výpovědní hodnota
  - Nízká flexibilita při změnách
  - Mapování pouze 1:1

Proč DNS?

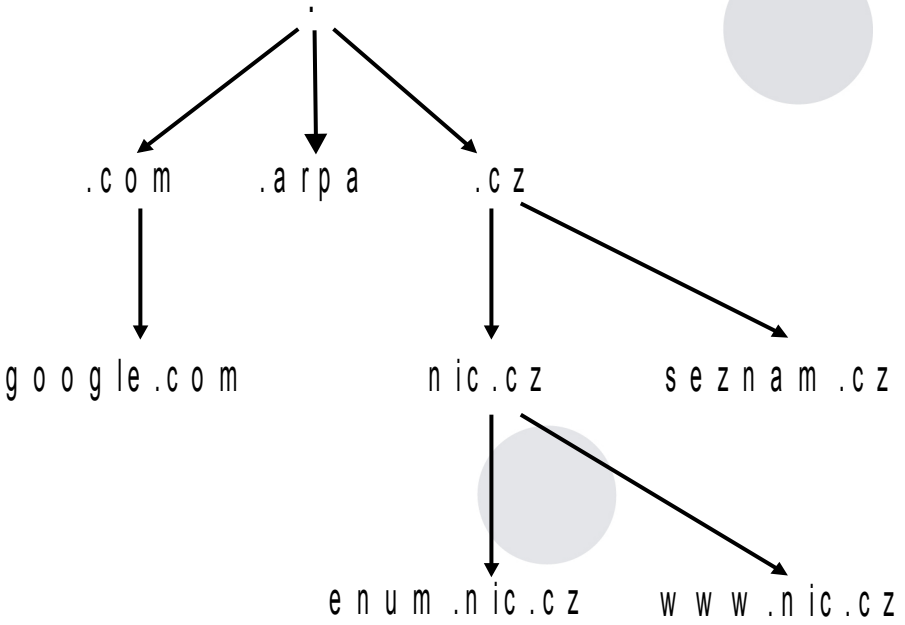
- Mapování jmen na číselné adresy
  - ARPANET (RFC606 – r. 1973)
- Centrální autorita
  - Soubor HOSTS
  - Jednoúrovňové
  - Všechny aktualizace centrálně
  - Nízká (žádná) škálovatelnost
  - Distribuce z jednoho místa
  - Malý počet jmen
  - Malá frekvence změn

Proč DNS?

- Návrh nového řešení (RFC881-883 – r. 1983)
- Vznik DNS (RFC1034 a RFC1035 – r. 1987)
  - Nezávislost na síťových identifikátorech
  - Decentralizované
  - Distribuované
  - Hierarchické
  - Škálovatelné
  - Různé druhy informací
  - Vyrovnávací paměť (blízko koncovému uživateli)

Principy DNS

- Distribuované a decentralizované řešení
  - Technicky
  - Administrativně
- Hierarchické řešení
  - Hierarchie rozdělená tečkou
  - Neviditelná kořenová doména "." (úplně vpravo)



Základní pojmy DNS

- Doména / Doménové jméno
- RR záznam
- Zóna
- Zónový soubor
- Jmenný server / Name server

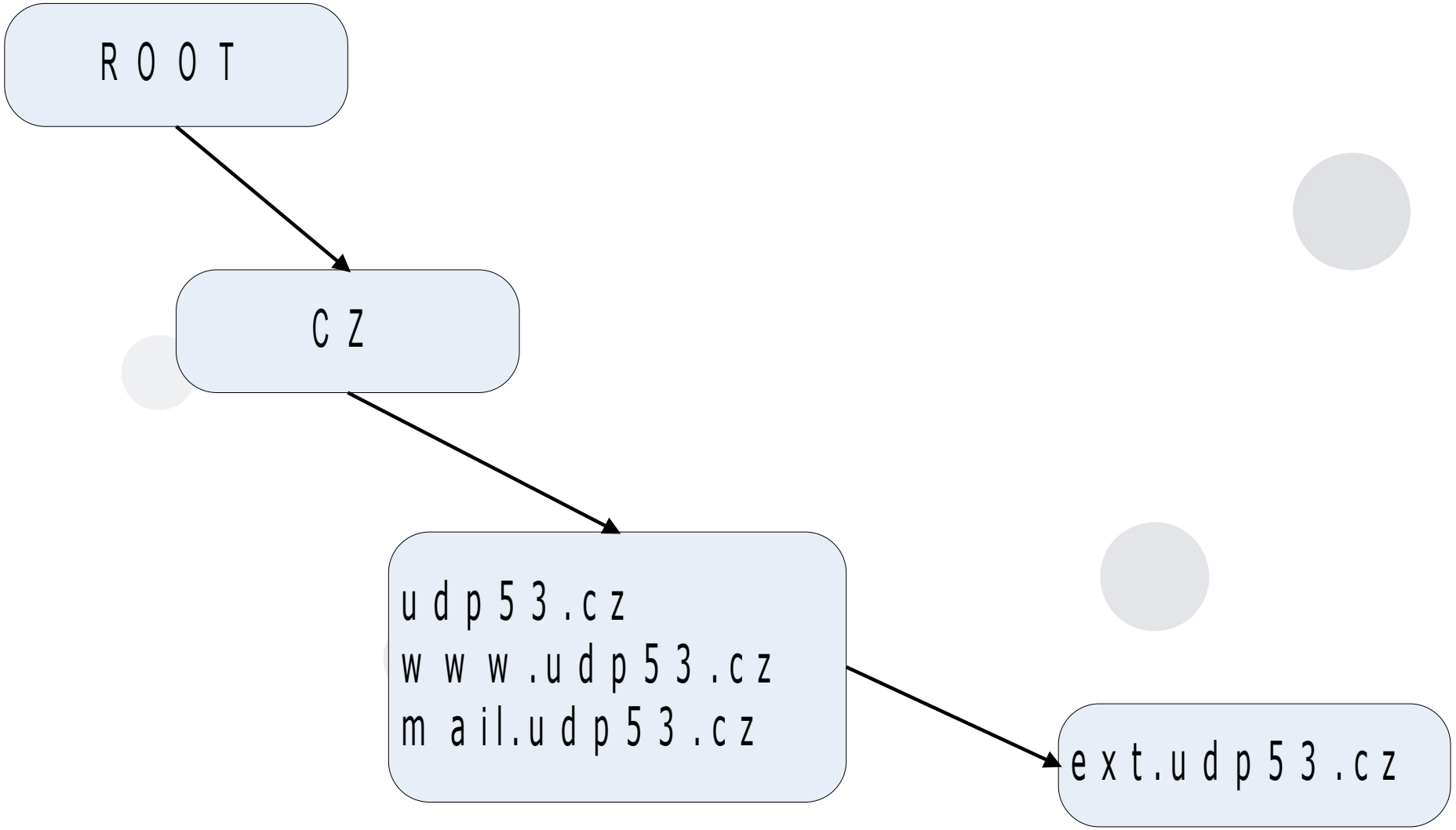
Doménové jméno

- „label“ – část mezi dvěma tečkami (max. 63 oktetů)
- Doménové jméno (max. 255 oktetů)
- Obecně může DNS přenášet libovolné znaky
- Prakticky existují omezení
  - Písmena (US-ASCII)
  - Číslice
  - Pomlčka
  - Potržítko (ve speciálních případech)

Zóna

- Část hierarchie
- Samostatný správce
- Oddělená na úrovni teček v doménové jménu
- Delegovaná „jinam“

Zóna



RR (Resource Record) záznam

- Jednotlivý záznam v DNS databázi
- Obsahuje:
  - Vlastníka záznamu (Owner)
  - Třídu (IN – Internet a CH – Chaos)
  - Typ (A, AAAA, MX, PTR, …)
  - TTL (Time To Live)
  - RData (Resource Data)

Zónový soubor

- RR záznamy zóny
- Na jednom místě
- Speciální formát

```
udp53.cz. 600  IN   SOA  ns.udp53.cz. hm.udp53.cz. (
                           2008101420
                           10800
                           3600
                           1209600
                           7200 )
www.udp53.cz.  600  IN   AAAA 2001:1488:0:3::2
www.udp53.cz.  600  IN   A    217.31.205.50
mail.udp53.cz. 600  IN   AAAA  2001:1488:800:400::400
mail.udp53.cz. 600  IN   A    217.31.204.67
udp53.cz.      600  IN   AAAA 2001:1488:0:3::2
udp53.cz.      600  IN   MX   10 mail.udp53.cz.
udp53.cz.      600  IN   A    217.31.205.50
udp53.cz.      600  IN   NS   a.ns.nic.cz.
udp53.cz.      600  IN   NS   b.ns.nic.cz.
```

Name server

- Má data příslušné zóny (domény)
  - Je pro ni autoritativní
- Každá zóna má vlastní name server
- Name server může obsluhovat <n> zón
  - Lepší využití prostředků
- Zóna může (měla by) mít více name serverů
  - Lepší dostupnost

Domain Name systém
Principy fungování

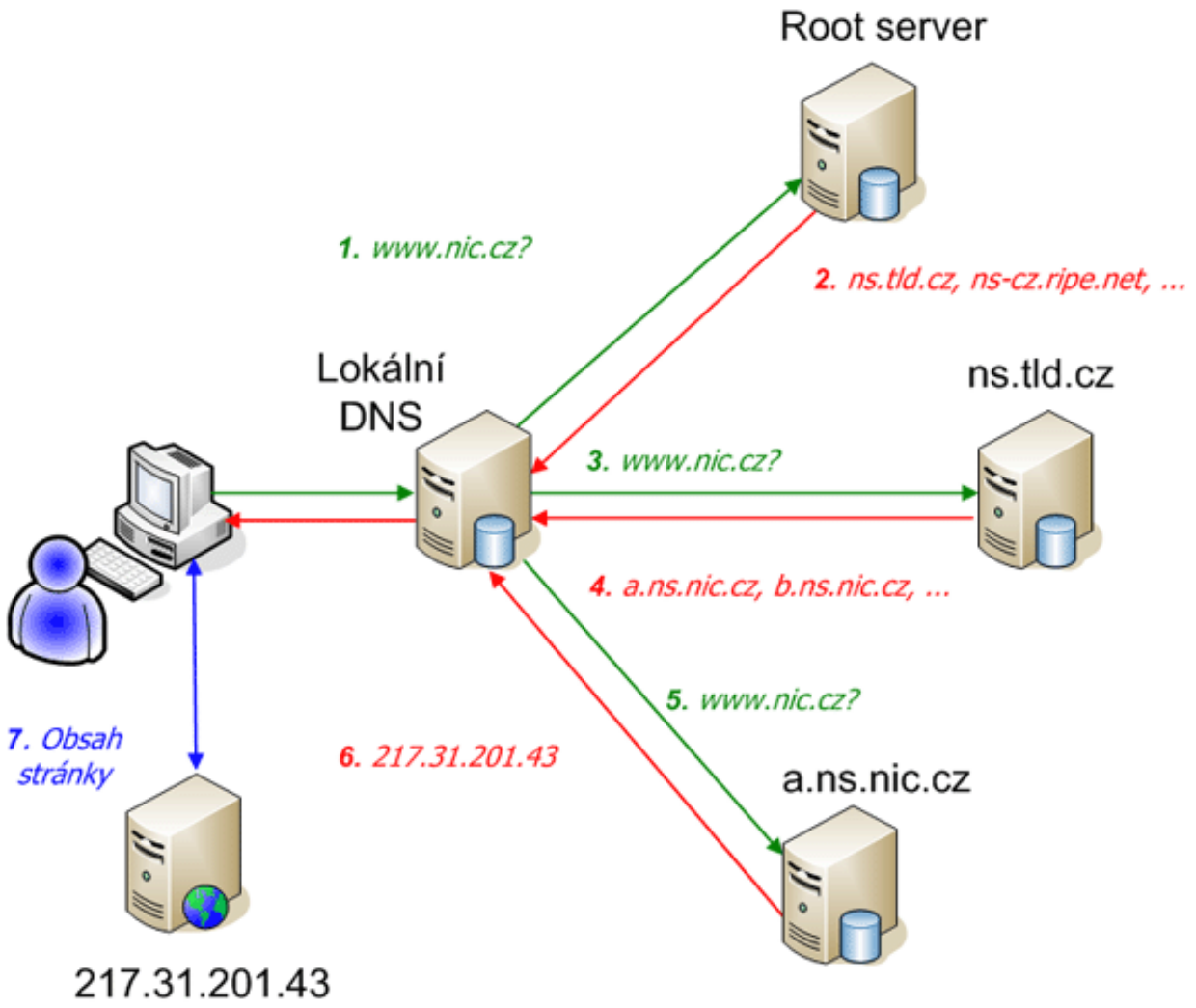
DNS servery a resolvery

- Architektura klient/server
- Klient – rekurzivní name server – resolver
- Server – autoritativní name server
- Komunikace pomocí DNS zpráv
- Resolver se může ptát dalších resolverů
- Vyrovnávací paměť (cache) na resolveru
  - Délku (čas) v cache řídí správce zóny!

Autoritativní server (master→slave)

- Master (primární) server
  - Autoritativní server
  - Data na jednom místě (zónový soubor)
  - Zdroj dat pro ostatní autoritativní servery
  - Může být skrytý
- Slave (sekundární) server(y)
  - Data jsou získávána z master serveru
  - Může jich být více
  - Hierarchie (master → slave → slave … slave)

DNS dotazování



DNS dotazování

- Uživatel → Q(www.nic.cz) → Resolver
  - Resolver → Q(www.nic.cz) → NS(Root)
  - NS(Root) → A(NS pro cz) → Resolver
  - Resolver → Q(www.nic.cz) → NS(cz)
  - NS(cz) → A(NS pro nic.cz) → Resolver
  - Resolver → Q(www.nic.cz) → NS(nic.cz)
  - NS(nic.cz) → A(217.31.205.50) → Resolver
- Resolver → A(217.31.205.50) → Uživatel

DNS dotazování (cache)

- Resolver má data v cache
  - Uživatel → Q(www.nic.cz) → Resolver
  - Resolver → A(217.31.205.50) → Uživatel
- Probíhá na každé úrovni delegace

DNS dotazování

- Stub resolver
  - DNS klient v každém počítači
  - Implementován v systémových knihovnách
  - Malý, jednoduchý
  - Může, ale nemusí, implementovat cache

Autoritativní vs. neautoritativní

- Autoritativní odpověď
  - Od autoritativního NS
  - Dotaz na doménu, která je na NS delegovaná
- Neautoritativní odpověď
  - Od resolveru
- Příznak v DNS zprávě
- „Lame“ delegace
  - Delegace zóny na NS, který není autoritativní

Obsah (den první)

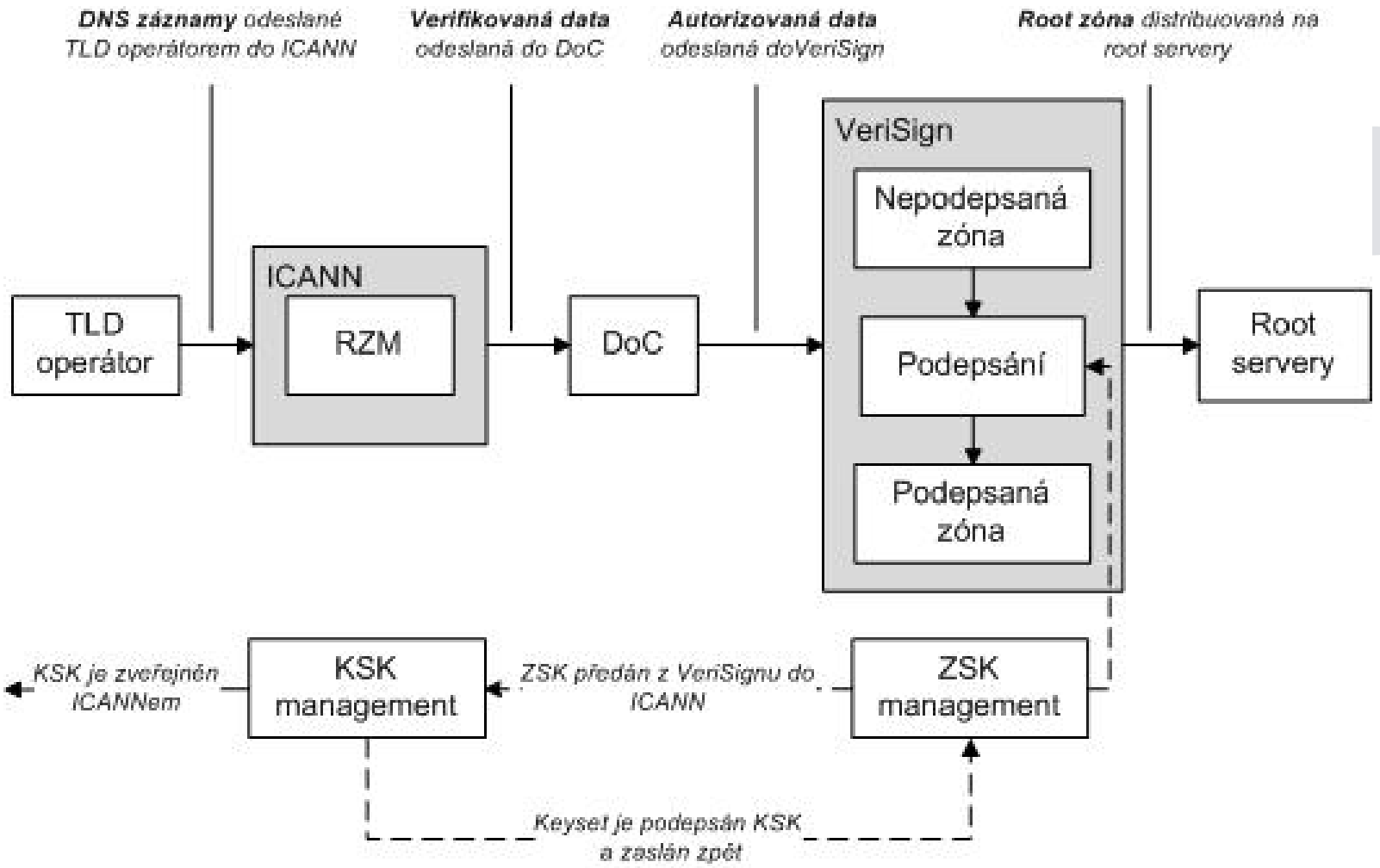
- Základní popis DNS
- **Správa DNS hierarchie**
- RR záznamy
- Rekurzivní server
  - Konfigurace Unbound
  - Konfigurace Bind 9
- Formát zónového souboru
- Autoritativní server
  - Konfigurace NSD 3
  - Konfigurace Bind 9

Internet Governance
Správa DNS hierarchie

Root (kořenová) zóna

- US Department of Commerce
- ICANN / IANA
- VeriSign
- Root Servers Operators

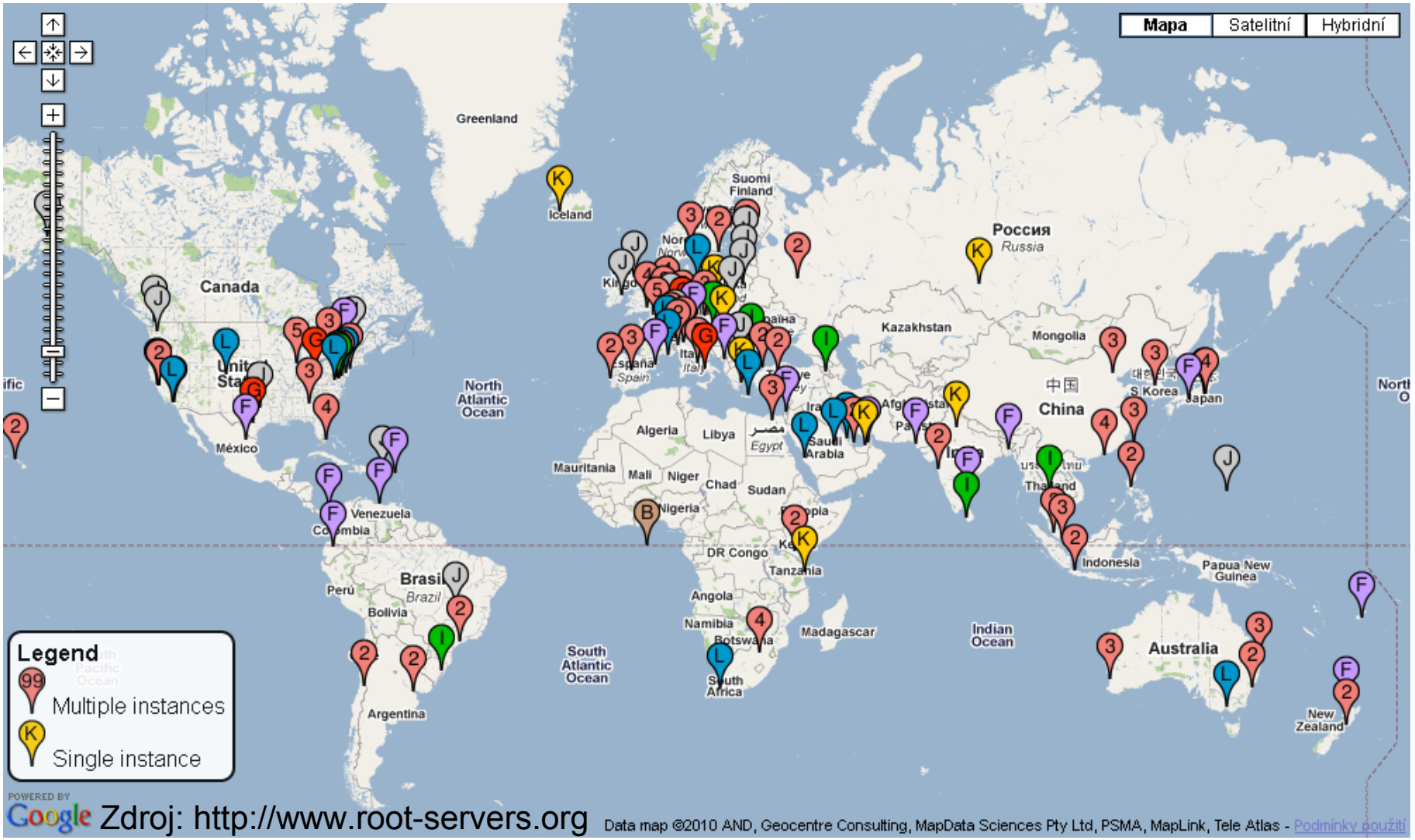
Root (kořenová) zóna



Root servery

- http://www.root-servers.org
- Distribuované po celém světě
- IPv4 i IPv6
- 13 jmen (A – M.root-servers.net)
- 255 serverů
- Česká republika
  - F.root-servers.net (CZ.NIC, op. ISC)
  - J.root-servers.net (NIX, op. VeriSign)
  - L.root-servers.net (CZ.NIC, op. ICANN)

Root servery



Zdroj: http://www.root-servers.org

Top Level Domény

- gTLD – obecné domény
  - .com, .biz, .info, .net, …
- sTLD – sponzorované domény (mají určení)
  - .aero, .gov, .mil, .travel, .museum, …
- ccTLD – národní domény
  - .us, .cz, .de, .sk, …
- Infrastructure
  - .arpa

.cz ccTLD

- Správce CZ.NIC
- Delegováno IANA
- Registr(1) → Registrátor(m) → Držitel(n)
- Name servery
  - 6 jmen → 4 jména (a – d.ns.nic.cz)
  - IPv4 a IPv6
  - 18 serverů
  - Geograficky diverzifikováno
  - Unicast → Anycast (4x)

Obsah (den první)

- Základní popis DNS
- Správa DNS hierarchie
- **RR záznamy**
- Rekurzivní server
  - Konfigurace Unbound
  - Konfigurace Bind 9
- Formát zónového souboru
- Autoritativní server
  - Konfigurace NSD 3
  - Konfigurace Bind 9

RR záznamy

RR záznam

- Vlastník (Owner)
  - Doménové jméno
  - Jeden vlastník → n záznamů
- Třída (Class)
  - IN – Internet
  - CH – Chaos (speciální)
- TTL (Time To Live)
  - Maximální doba uložení v cache resolveru

RR záznam – RDATA

- Resource Data
  - Strukturovaná dle typu RR záznamu
  - Proměnlivá délka dat
  - Maximální délka 65535 oktetů

RR záznam – typy záznamů

Typ	Anglický název	Význam pole RDATA
SOA	Start of Authority	údaje o zóně (více položek)
NS	Name Server	doménové jména autoritativních nameserverů
A	A host address	IPv4 adresa (jméno → IP adresa)
AAAA	IPv6 host address	IPv6 adresa (jméno → IP adresa)
CNAME	Canonical Name	„Alias“ (*jméno → *jiné_jméno)
MX	Mail Exchange	Ukazatel na poštovní servery k doméně
RRSIG	RR Signature	DNSSEC podpis
PTR	Pointer	Reverzní delegace (IP adresa → jméno)
TXT	Text	Obecný text
…		A další speciální...

SOA záznam

- Jeden pro každou zónu
- Na vrcholu zóny
- Řídí master → slave komunikaci
- MINIMUM mělo původně jiný význam

Položka	**Význam**
MNAME	Primární nameserver
RNAME	Email správce zóny
SERIAL	Sériové číslo
REFRESH	Čas obnovy zóny (NS-NS)
RETRY	Nový pokus obnovy (NS-NS)
EXPIRE	Expirace zóny
MINIMUM	Čas pro negativní cache

SOA záznam

```
udp53.cz. 600 IN SOA ns.udp53.cz. hostmaster.udp53.cz. (
                          2008101420 ; serial
                          10800      ; refresh (3 hours)
                          3600       ; retry (1 hour)
                          1209600    ; expire (2 weeks)
                          7200       ; minimum (2 hours)
                          )
```

- MNAME nemusí existovat
- RNAME bez zavináče (první tečka → '@')
- Serial (YYYYMMDDNN) nebo (Unixtime)
- Retry kratší než Refresh
- Expire dostatečně dlouhé

NS záznam

- Záznam o delegaci, obsahuje doménové jméno NS

```
udp53.cz. 3600 IN NS ns.udp53.cz.
```

- Nadřazená zóna obsahuje pouze NS
  - Pro konkrétní doménové jméno
- Podřízená zóna obsahuje minimálně NS, SOA
  - Pro delegované doménové jméno
- Pozor na cyklické závislosti
  - tzv. GLUE záznam (A | AAAA) v nadřazené zóně

```
udp53.cz.    3600 IN NS ns.udp53.cz.
ns.udp53.cz. 3600 IN A  127.0.0.1
```

A a AAAA záznam

- Obsahuje IP adresu
  - A záznam → IPv4 adresu (32 bitů)
  - AAAA záznam → IPv6 adresu (128 bitů)
- Příklad:

```
www.udp53.cz. 3600 IN A    127.0.0.1
www.udp53.cz. 3600 IN AAAA ::1
```

MX záznam

- Ovlivňuje směrování elektronické pošty
- Obsahuje prioritu a kanonické doménové jméno

```
udp53.cz. 3600 IN MX 10 mail.udp53.cz.
udp53.cz. 3600 IN MX 20 mail2.nic.cz.
mail.udp53.cz. 3600 IN A 127.0.0.1
```

- Nesmí (neměl by) směřovat na IP adresu / CNAME

~~`udp53.cz. 3600 IN MX 10 127.0.0.1`~~

~~`udp53.cz. 3600 IN MX 10 mail.udp53.cz.`~~
~~`mail.udp53.cz 3600 IN CNAME web.udp53.cz.`~~

CNAME záznam

- Další jméno, Alias

```
www2.udp53.cz. 600 IN CNAME www.udp53.cz.
```

- Rekurzivně (www3 → www2 → www)
- Přesměruje všechny záznamy

```
udp53.cz. 600 IN A 127.0.0.1
udp53.cz. 600 IN MX 10 mail.udp53.cz.
www.udp53.cz 600 IN CNAME udp53.cz.
```

- `www.udp53.cz. IN MX → 10 mail.udp53.cz.`

CNAME záznam

- CNAME musí být sám
  - Pro konkrétní doménové jméno (vlastníka záznamu)

```
www.udp53.cz. 600 IN CNAME udp53.cz.
www.udp53.cz. 600 IN A 127.0.0.1
www.udp53.cz. 600 IN AAAA ::1
```

- Nesmí na něj ukazovat:
  - MX | NS záznamy
  - Další dle definice konkrétního protokolu
- Resolver dále zpracovává výsledek
  - Může dojít k dalším dotazům

TXT záznam

- Obecná textová data
- Často (zne)užíván k ukládání strukturovaných dat
  - RFC1464 (ukládání atributů do DNS)
  - Sender Policy Framework
  - DomainKeys
  - DNS-SD (Service Discovery)

PTR záznam

- Obecně ukazatel na doménové jméno

```
1.0.0.127.in-addr.arpa. IN PTR udp53.cz.
```

- Porovnej se CNAME
  - Nedochází k dalšímu zpracování na úrovni DNS
  - Může jich být více pro jedno doménové jméno
- Reverzní mapování (IP adresa → doménové jméno)
  - Speciální podstromy v .arpa (in-addr.arpa, ip6.arpa)
  - IP adresa obrácená, rozdělená přes tečky
  - Používáno pro kontrolu nebo správu
    - Poštovní servery, SSH servery
    - Udržení pořádku v síti

Protokol DNS

DNS Protokol

- DNS zpráva
  - Stejný formát pro dotaz i odpověď
- Hlavička
  - ID dotazu
  - Příznaky
  - Návratový kód
  - Počty RR záznamů
- Čtyři sekce s RR záznamy

Název	Anglicky	Popis
Hlavička	Header	Hlavička zprávy
Dotaz	Question	Dotaz (RR záznam)
Odpověď	Answer	Přímá odpověď (RR)
Autorita	Autority	Odkaz na autoritu (RR)
Další	Additional	Další záznamy (RR)

DNS Protokol

- Transportní vrstva
  - UDP
  - TCP (spíše komunikace mezi servery)
- DNS server poslouchá na portu 53
- Dotazy chodí z náhodného portu
  - Kaminsky bug

Nástroje pro práci s DNS

- Nástroje z balíku bind9-host:
  - host – jednodušší, uživatelský přívětivější výstup
- Nástroje z balíku dnsutils:
  - nslookup – k dispozici také v MS Windows
  - dig – pracuje přímo s DNS zprávami
- Alternativní nástroje z balíku unbound-host a ldnsutils:
  - unbound-host – podobný příkazu host
  - drill – podobný příkazu dig

Použití host/unbound-host

```
$ host <adresa> (<server>)
$ unbound-host <adresa>
```

- Výstup je textový:

```
$ host www.nic.cz 127.0.0.1
www.nic.cz has address 217.31.205.50
www.nic.cz has IPv6 address 2001:1488:0:3::2

$ unbound-host -v www.udp53.cz
www.udp53.cz has no address (insecure)
www.udp53.cz has no IPv6 address (insecure)
www.udp53.cz has no mail handler record (insecure)
```

Použití dig/drill

```
# dig [@server] [name] [type] [class] {opt}
# drill {opt} name [@server] [type [class]
```

- Výstup vypisuje DNS zprávu:

```
$ drill @127.0.0.1 IN A www.nic.cz
```

```
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 52314
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 5
;; QUESTION SECTION:
;; www.nic.cz.    IN    A

;; ANSWER SECTION:
www.nic.cz. 1782  IN    A     217.31.205.50

;; AUTHORITY SECTION:
nic.cz.     1782  IN    NS    a.ns.nic.cz.
nic.cz.     1782  IN    NS    e.ns.nic.cz.
nic.cz.     1782  IN    NS    c.ns.nic.cz.

;; ADDITIONAL SECTION:
a.ns.nic.cz.      152953      IN    A     217.31.205.180
a.ns.nic.cz.      152953      IN    AAAA  2001:1488:dada:176::180
c.ns.nic.cz.      152953      IN    A     195.66.241.202
c.ns.nic.cz.      152953      IN    AAAA  2a01:40:1000::2
e.ns.nic.cz.      152953      IN    A     194.146.105.38

;; Query time: 4 msec
;; SERVER: 127.0.0.1
;; WHEN: Tue Jan 13 14:59:34 2009
;; MSG SIZE  rcvd: 199
```

Obsah (den první)

- Základní popis DNS
- Správa DNS hierarchie
- RR záznamy
- **Rekurzivní server**
  - Konfigurace Unbound
  - Konfigurace Bind 9
- Formát zónového souboru
- Autoritativní server
  - Konfigurace NSD 3
  - Konfigurace Bind 9

Konfigurace resolveru

Konfigurace stub resolveru

- Libc6 resolver
  - Konfigurace `/etc/resolv.conf`
- Direktiva `nameserver <ip_adresa>`:

```
nameserver 127.0.0.1
nameserver 10.0.0.101
```

- Direktiva `search <subdomain>`:

```
search int.udp53.cz ext.udp53.cz
```

Konfigurace resolveru – obecně

- Resolver je DNS server, který:
  - Odpovídá na rekurzivní dotazy klientů
  - Ptá se další DNS serverů
- Rekurzivní dotaz
  - V hlavičce zprávy příznak RD (Recursion Desired)
  - V odpovědi zprávy příznak RA (Recursion Available)

Dostupné resolvery

- **Unbound**
- **Bind 9**
- Microsoft DNS
- PowerDNS
- Další (zastaralé, špatné, nepodporující standardy)

http://en.wikipedia.org/wiki/Comparison_of_DNS_server_software

Konfigurace rekurzivního DNS serveru **Unbound**

Unbound

- http://www.unbound.net
- Pouze rekurzivní server
- Napsaný na zelené louce
- Komponentová architektura
- Dynamická knihovna pro resolving
- Používá knihovnu ldns
- Poslední verze 1.4.8

Unbound: Instalace

- Přepneme se na uživatele root

```
$ sudo -s
```

- Nainstalujeme balík unbound

```
# apt-get install unbound
```

- Otevřete si manuálovou stránku

```
$ man unbound.conf
```

- Otevřete si konfiguraci v editoru

```
# editor /etc/unbound/unbound.conf
```

- Zazálohujte si konfiguraci stub resolveru:

```
# cp /etc/resolv.conf
  /etc/resolv.conf.backup
```

Unbound: Konfigurace

- Rozhraní (příchozí)

```
interface: 0.0.0.0
interface: ::0
```

- Port (příchozí)

```
port: 53
```

- Rozhraní (odchozí)

```
outgoing-interface:
```

- Maximální doba v cache

```
cache-max-ttl: 864000
```

- Kontrola přístupu

```
access-control: <net> <action>
```

- Kořenové NS (hints)

```
root-hints:
```

- Stub zóny

```
stub-zone:
    name: "zona"
    stub-addr: 10.0.0.101
```

- Forward zóny

```
forward-zone:
    name: "."
    forward-addr: ::1
```

Unbound: Testování konfigurace

- Před restartem zkontrolujte konfiguraci

```
# unbound-checkconf

unbound-checkconf: no errors in
  /etc/unbound/unbound.conf
```

Unbound: Úkol č. 1

- Zastavte a spusťte Unbound

```
# /etc/init.d/unbound stop
# /etc/init.d/unbound start
```

- Nakonfigurujte stub resolver, aby používal Unbound

```
editor /etc/resolv.conf
    nameserver ::1
    nameserver 127.0.0.1
```

- Otestujte, že vše funguje:

```
# ping <jmenná_adresa>
```

  - Otevřete stránku v prohlížeči

```
$ dig IN ANY www.nic.cz @localhost
```

Unbound: Úkol č. 2

- Nakonfigurujte Unbound, aby používal DNS servery 217.31.204.130 a 217.31.204.131

```
forward-zone:
    name: "."
    forward-addr: 217.31.204.130
    forward-addr: 217.31.204.131
```

- Restartujte Unbound

```
# /etc/init.d/unbound restart
```

Unbound: Úkol č. 3

- Nakonfigurujte Unbound se stub zónou skoleni.udp53.cz na serveru 10.0.0.101

```
stub-zone:
    name: "skoleni.udp53.cz"
    stub-addr: 10.0.0.101
```

- Restartujte Unbound

```
# /etc/init.d/unbound restart
```

- Ověřte doménu www.skoleni.udp53.cz

```
$ ping www.skoleni.udp53.cz
```

Unbound: Úkol č. 4

- Stáhněte aktualizovaný soubor root hints a uložte jej do /etc/unbound/root.hints

```
# wget -O /etc/unbound/root.hints
    http://internic.net/zones/named.root
```

- Nakonfigurujte Unbound, aby používal nový soubor

```
server:
    root-hints: "/etc/unbound/root.hints"
```

- Restartujte Unbound

```
# /etc/init.d/unbound restart
```

- Ověřte funkci

Unbound: Úkol č. 5

- Unbound standardně povoluje přístup jen z localhost
- Nakonfigurujte přístupová práva pro souseda

```
server:
        interface: <ip_vase>
        interface: 127.0.0.1
        interface: ::0
        access-control: <ip_souseda>/32 allow
```

- Restartujte unbound

```
# /etc/init.d/unbound restart
```

- Zkontrolujte, že přístup funguje

```
$ dig www.nic.cz @<ip_souseda>
```

Unbound: Úkol č. 6

- Nakonfigurujte Unbound, aby poslouchal na localhostu

```
server:
        interface: 127.0.0.1
```

- Přidejte na rozhraní eth0 další IP adresu

```
# ip -4 addr add <ip_vase+100> brd 10.0.0.255 dev
  eth0
```

- Nakonfigurujte Unbound, aby posílal dotazy z nově přidané IP adresy

```
server:
        outgoing-interface: <ip_vase+100>
```

- Restartujte Unbound

```
# /etc/init.d/unbound restart
```

Unbound: Vyčištění systému

- Zastavíme Unbound

```
# /etc/init.d/unbound stop
```

- Přesvědčíme se, že neběží:

```
# ps uax | grep unbound
```

- Obnovte konfiguraci stub resolveru

```
# cp /etc/resolv.conf.backup
  /etc/resolv.conf
```

Konfigurace rekurzivního DNS serveru **Bind 9**

Bind 9

- http://www.isc.org/software/bind
- Rekurzivní i autoritativní server
- Poslední verze 9.7.2-P3
- Knihovna pro resolving
- Sada nástrojů (dig, host, dnssec-*)

Bind 9: Instalace

- Přepneme se na uživatele root

```
$ sudo -s
```

- Nainstalujeme balík bind9

```
# apt-get install bind9
```

- Otevřete si konfiguraci v editoru

```
# editor /etc/bind/named.conf
# editor /etc/bind/named.conf.local
# editor /etc/bind/named.conf.options
```

Bind 9: Konfigurace

- Sekce `options {};`

```
listen-on [ port n ] { addr }; // Rozhraní a port
listen-on-v6 { ipv6_addr }; // Rozhraní (ipv6)
port 53; // Port
forwarders { addr1; addr2; ... }; // forward z.
querylog yes/no; // Log dotazů
recursion yes/no; // povolení rekurze
allow-query { addr }; // povolení přístupu
allow-recursion { addr }; // povolení rekurzivních
  dotazů
query-source addr; // zdrojová ipv4 adresa
query-source-v6 ipv6_addr; // zdrojová ipv6 addr
```

Bind 9: Konfigurace

- Sekce `logging {};`

```
channel channel1 {
        file log_file;
        syslog facility;
        null;
        print-time yes/no;
        print-severity yes/no;
        print-category yes/no;
};
category <kategorie> { channel1; channel2; … };
```

- Sekce `acl {};`

```
acl nazev_acl { addr1; addr2; … };
```

Bind 9: Konfigurace

- Sekce `zone {};`

```
type stub | hint | forward | ... ;
file "cesta_k_souboru";
forwarders { addr1; addr2; ... };
masters { addr1; addr2; ... };
```

- Stub zóna

```
zone "udp53.cz." {
      type stub;
      masters { 127.0.0.1; 10.0.0.101; };
}
```

Bind 9: Konfigurace

- Forward zóna

```
zone "udp53.cz." {
        type forward;
        forwarders { 127.0.0.1; 10.0.0.101; };
};
```

- Hint zóna

```
zone "udp53.cz." {
        type hint;
        file "/etc/bind/db.root";
};
```

Bind 9: Testování konfigurace

- Před restartem/načtení konfigurace ji zkontrolujte:

```
# named-checkconf /etc/bind/named.conf
/etc/bind/named.conf:87: unknown option 'chyba'
/etc/bind/named.conf:88: unexpected token near end of file
```

Bind 9: Úkol č. 1

- Zastavte a spusťte Bind 9

```
# /etc/init.d/bind9 stop
# /etc/init.d/bind9 start
```

- Nakonfigurujte stub resolver, aby používal Bind 9

```
editor /etc/resolv.conf
    nameserver ::1
    nameserver 127.0.0.1
```

- Otestujte, že vše funguje:

```
$ ping <jmenna_adresa>
```

  - Otevřete stránku v prohlížeči

```
$ dig IN ANY www.nic.cz @localhost
```

Bind 9: Úkol č. 2

- Nakonfigurujte Bind 9, aby používal DNS servery 217.31.204.130 a 217.31.204.131

```
options {
    forwarders { 217.31.204.130;
                 217.31.204.131; };
};
```

- Načtěte novou konfiguraci

```
# rndc reload
```

- Ověřte, že vše funguje

Bind 9: Úkol č. 3

- Nakonfigurujte Bind 9 se stub zónou skoleni.udp53.cz na serveru 10.0.0.101

```
zone "skoleni.udp53.cz" {
    type stub;
    masters { 10.0.0.101; };
    forwarders { }; };
```

- Načtěte novou konfiguraci

```
# rndc reload
```

- Ověřte doménu www.skoleni.udp53.cz

```
$ ping www.skoleni.udp53.cz
```

Bind 9: Úkol č. 4

- Stáhněte aktualizovaný soubor root hints a uložte jej do /etc/bind/root.hints

```
# wget -O /etc/bind/root.hints
    http://internic.net/zones/named.root
```

- Nakonfigurujte Bind 9, aby používal nový soubor

```
zone "." { type hint;
    file "/etc/bind/root.hints"; };
```

- Načtěte novou konfiguraci

```
# rndc reload
```

- Ověřte funkci

Bind 9: Úkol č. 5

- Nakonfigurujte přístup k dotazům a rekurzi
- Nakonfigurujte přístupová práva pro souseda

```
acl good { 127.0.0.1; ::1; <ip_souseda>; };
options {
        allow-query { good; };
        allow-recursion { good; };
};
```

- Načtěte novou konfiguraci

```
# rndc reload
```

- Zkontrolujte, že přístup funguje

```
# dig www.nic.cz @<ip_souseda>
```

Bind 9: Úkol č. 6

- Nakonfigurujte Bind 9, aby poslouchal na localhostu

```
options {
        listen-on { 127.0.0.1; };
```

- Nakonfigurujte Bind 9, aby posílal dotazy z druhé IP adresy vašeho eth0 rozhraní

```
options {
        query-source <ip_vase+100>; };
```

- Načtěte novou konfiguraci

```
# rndc reload
```

Bind 9: Úkol č. 7

- Nakonfigurujte logování dotazů do samostatného souboru:

```
options { querylog yes; };
logging {
        channel query_log {
                file "/var/cache/bind/query.log";
                print-time yes;
                print-severity yes;
                print-category yes;
        };
        category queries { query_log; };
};
```

Bind 9: Vyčištění systému

- Zastavíme Bind 9

```
# /etc/init.d/bind9 stop
```

- Přesvědčíme se, že neběží:

```
# ps uax | grep named
```

- Obnovte konfiguraci stub resolveru

```
# cp /etc/resolv.conf.backup
  /etc/resolv.conf
```

Obsah (den první)

- Základní popis DNS
- Správa DNS hierarchie
- RR záznamy
- Rekurzivní server
  - Konfigurace Unbound
  - Konfigurace Bind 9
- **Formát zónového souboru**
- Autoritativní server
  - Konfigurace NSD 3
  - Konfigurace Bind 9

Zónový soubor

Zónový soubor: Úkol č. 1

- Stáhněte si šablonu zónového souboru (<**NN**> je číslo vašeho PC):

```
# wget -O /etc/bind/z<NN>.lab.nic.cz
  http://public.nic.cz/files/zmichl/courses/dns/template_zone
```

- Změňte z**<NN>** a pc**<NN>** v souboru:

```
# editor z<NN>.lab.nic.cz
```

- Zkontrolujte správnost zónového souboru:

```
# named-checkzone <zona> <soubor>
```

Zónový soubor: Úkol č. 2

- Přidejte různé typy RR záznamů
  - A
  - AAAA
  - MX
  - TXT
  - CNAME
- Nezapomeňte po každé změně zvýšit sériové číslo v SOA záznamu
- Zkontrolujte validitu zónového souboru

Konfigurace autoritativního serveru

Autoritativní server – obecně

- Autoritativní server
  - Je autoritativní (má data) alespoň k jedné zóně
  - Ideálně nemá zapnutou rekurzi
  - V hlavičce odpovědí vrací 'AA' (Authoritative Answer)
- Master vs. Slave
  - Způsob distribuce zóny: AXFR, IXFR (i jinak)
  - Notifikace (master → slave)
  - Stáhnutí zóny (slave → master)
  - Kromě notify řízeno přes hodnoty v SOA záznamu

Dostupný software

- **NSD 3**
- **Bind 9**
- PowerDNS
- Microsoft DNS
- MyDNS
- další…

http://en.wikipedia.org/wiki/Comparison_of_DNS_server_software

Obsah (den první)

- Základní popis DNS
- Správa DNS hierarchie
- RR záznamy
- Rekurzivní server
  - Konfigurace Unbound
  - Konfigurace Bind 9
- Formát zónového souboru
- **Autoritativní server**
  - Konfigurace NSD 3
  - Konfigurace Bind 9

Konfigurace autoritativního DNS serveru NSD 3

NSD 3: Obecně

- Napsaný na zelené louce
- Statická předkompilovaná databáze RR záznamů
  - Rychlejší start (řádově)
- „Dynamická“ databáze s aktualizacemi
  - Nutno pravidelně slučovat
- Běží na několika Root i TLD name serverech
- Poslední verze 3.2.7

NSD 3: Instalace

- Nainstalujte NSD 3

```
# apt-get install nsd3
```

- Otevřete manuálovou stránku konfigurace

```
$ man nsd.conf
```

- Otevřete konfigurační soubor

```
# editor /etc/nsd3/nsd.conf
```

- Nástroj na ovládání nsd:

```
# nsdc start|stop|reload|rebuild|restart|
  running|update|notify|patch
```

- Kontrola konfigurace

```
# nsd-checkconf
```

NSD 3: Úkol č. 1

- Poslouchá pouze na rozhraní eth0 (IPv4 i IPv6)

```
server:
        ip-address: <ipv4_vase>
        ip-address: <ipv6_vase>
```

- Je autoritativní pro z<NN>.lab.nic.cz
- Má povolený transfer pro lektorský počítač

```
zone:
        name: z<NN>.lab.nic.cz
        zonefile: /etc/bind/z<NN>.lab.nic.cz
        notify: 10.0.0.101 NOKEY
        provide-xfr: 10.0.0.101 NOKEY
```

- Ověřte (dig | drill | host)

```
$ drill @10.0.0.1<NN> z<NN>.lab.nic.cz IN SOA
```

NSD 3: Úkol č. 2

- Nastavte NSD 3, aby dělal master a slave server pro souseda (**<SS>** je číslo sousedova PC):

```
zone:  # zona vaseho souseda
        name: z<SS>.lab.nic.cz
        zonefile: /var/lib/nsd3/z<SS>.lab.nic.cz
        allow-notify: <ip_souseda> NOKEY
        request-xfr: <ip_souseda> NOKEY
zone:   # vase zona
        name: z<NN>.lab.nic.cz
        zonefile: /etc/bind/z<NN>.lab.nic.cz
        notify: <ip_souseda> NOKEY
        provide-xfr: <ip_souseda> NOKEY
```

- Ověřte funkcionalitu:

```
$ drill @<ip_souseda> IN SOA z<NN>.lab.nic.cz
```

NSD 3: Vyčištění

- Zastavte NSD 3

```
# nsdc stop
```

Konfigurace autoritativního DNS serveru Bind 9

Bind 9: Instalace

- Otevřete manuálovou stránku konfigurace

```
$ man named.conf
```

- Otevřete konfigurační soubor

```
# editor /etc/bind/named.conf
# editor /etc/bind/named.conf.local
# editor /etc/bind/named.conf.options
```

- Nástroj na ovládání named:

```
# rndc reload|...
```

- Kontrola konfigurace

```
# named-checkconf
```

Bind 9: Úkol č. 1

- Poslouchá pouze na rozhraní eth0 (IPv4 i IPv6)

```
options {
        listen-on { <ipv4_vase>; };
        listen-on-v6 { <ipv6_vase>; };
```

- Je autoritativní pro z<NN>.lab.nic.cz
- Má povolený transfer pro lektorský počítač

```
zone "z<NN>.lab.nic.cz" {
        type master;
        file "/etc/bind/z<NN>.lab.nic.cz";
        allow-transfer { 10.0.0.101; };
        notify explicit; also-notify { 10.0.0.101; }; };
```

- Ověřte (dig | drill | host)

```
$ dig @10.0.0.1<NN> z<NN>.lab.nic.cz IN SOA
```

Bind 9: Úkol č. 2

- Master i slave server pro souseda:

```
zone "z<SS>.lab.nic.cz" { // zona vaseho souseda
        type slave;
        file "/var/cache/bind/z<SS>.lab.nic.cz";
        masters { <ip_souseda>; };
        notify no; allow-notify { <ip_souseda>; };
};

zone "z<NN>.lab.nic.cz" { // vase zona
        type master;
        file "/etc/bind/z<NN>.lab.nic.cz";
        allow-transfer { <ip_souseda>; };
        notify explicit; also-notify { <ip_souseda>; };
};
```

- Ověřte funkcionalitu:

```
$ dig @<ip_souseda> IN SOA z<NN>.lab.nic.cz
```

Bind 9: Vyčištění

- Zastavte Bind 9

```
# rndc stop
```

Obsah (den druhý)

- Rozšířená témata (?)
  - Wireformat DNS zprávy
  - EDNS0
  - TSIG
  - DNS anycast
  - DNSSEC
  - IDN
- Ladění a trasování DNS (?)
  - Problémy s DNS
  - tcpdump / wireshark

Diskuze