Úvod do DNS

Petr Špaček • petr.spacek@nic.cz
Petr Černohouz • petr.cernohouz@qtm.cz

Organizace

- Dva dny
  - Dvě malé přestávky
    - 10:15 – 10:30
    - 14:15 – 14:30
  - Přestávka na oběd
    - 12:00 – 12:45
- Otázky rovnou v průběhu školení

Obsah (den první)

- Základní popis DNS
- Správa DNS hierarchie
- RR záznamy
- Rekurzivní server
  - Konfigurace Unbound
- Formát zónového souboru
- Autoritativní server
  - Konfigurace BIND 9
- TSIG (dle času)

Obsah (den druhý)

- Rozšířená témata
  - Wireformat DNS zprávy
  - EDNS0
  - DNSSEC
  - RPZ
  - Knot DNS + DDNS
- 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:

  https://secure.nic.cz/files/akademie/dns/

  - Tato prezentace + cvičení
  - Ukázkové konfigurační příklady
  - Další související materiály
- Přístup na shell uživatele root:

```
$ sudo -s
```

- Startování/vypínání se systemd:

```
# systemctl start|stop|restart <nazev>
```

Domain Name System

Základní principy a pojmy

Proč DNS? – Motivace

- IP adresy
  - Špatně se pamatují: 192.0.2.1, 2001:db8:dead::123
  - Identifikují „počítač“ a nikoli službu
  - Více služeb na jedné IP adrese
  - Malá výpovědní hodnota
  - Nízká flexibilita při změnách
  - Mapování pouze 1:1
    - Chybí obecnost

Proč DNS? – Historie

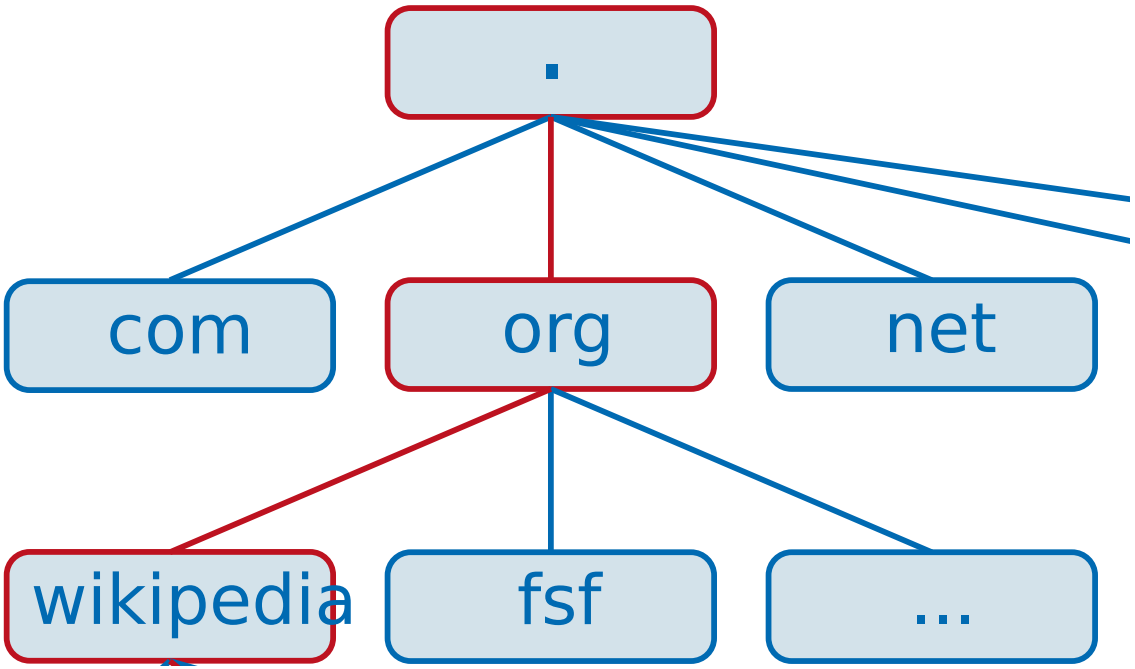
- Mapování jmen na číselné adresy
  - ARPANET (RFC606 – r. 1973)
- Centrální autorita
  - Soubor HOSTS (dodnes: /etc/hosts)
  - Všechny aktualizace se musí dít centrálně
  - Žádná škálovatelnost
  - Distribuce z jednoho místa
  - Malý počet jmen (tehdy)
  - Malá frekvence změn (tehdy)

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
- Decentralizované
  - Technicky
  - Administrativně



- Hierarchické řešení
  - Hierarchie rozdělená tečkou
  - Neviditelná kořenová doména "." (úplně vpravo)

Základní pojmy DNS

- Doména / Doménové jméno

  `www.nic.cz.`

- RR záznam (Resource Record)

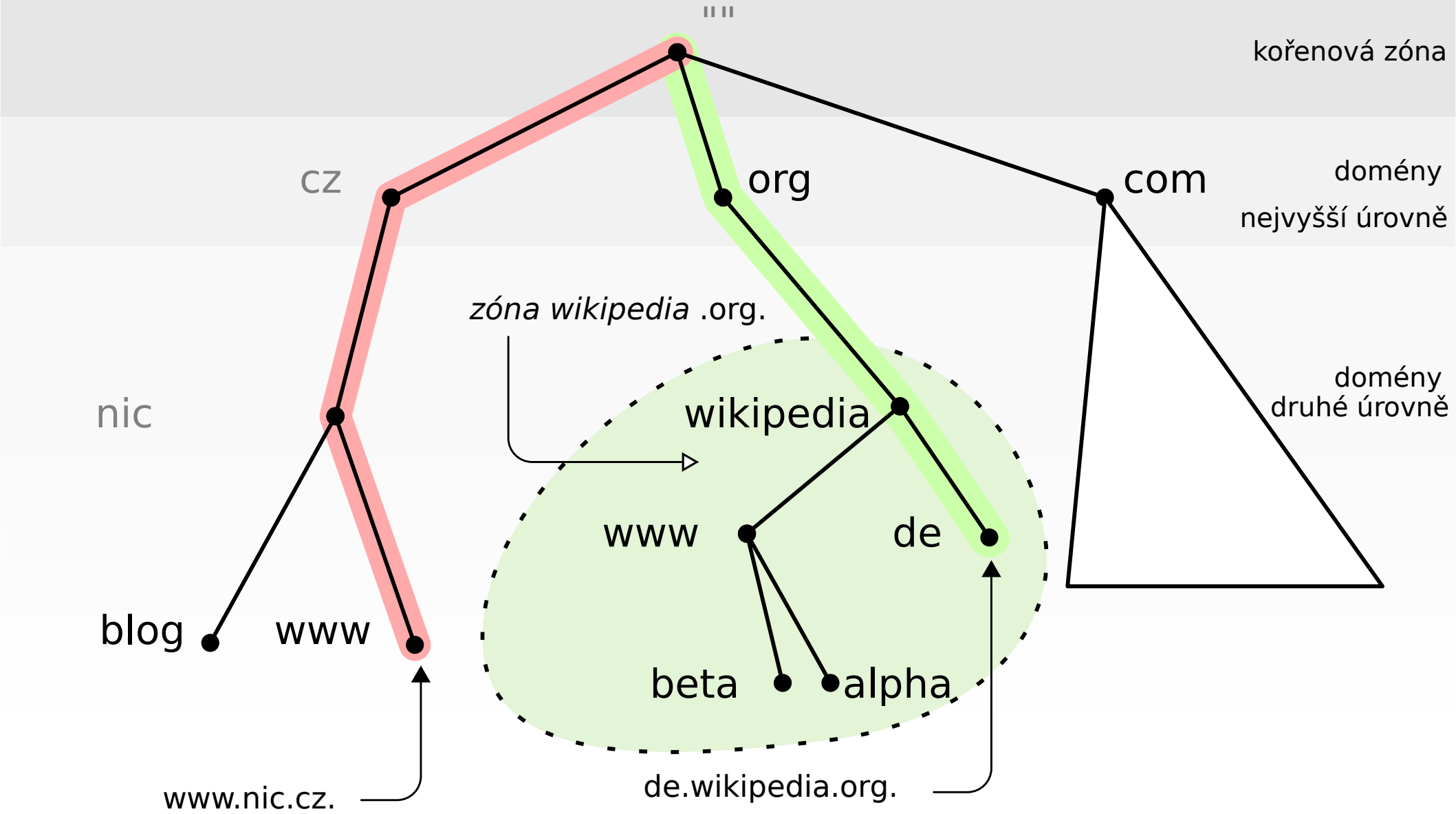
  ```
  www.nic.cz. 3600 IN AAAA 2001:DB8::1
  ```

- Zóna

  `nic.cz.`

- Zónový soubor
- Jmenný server / Name server

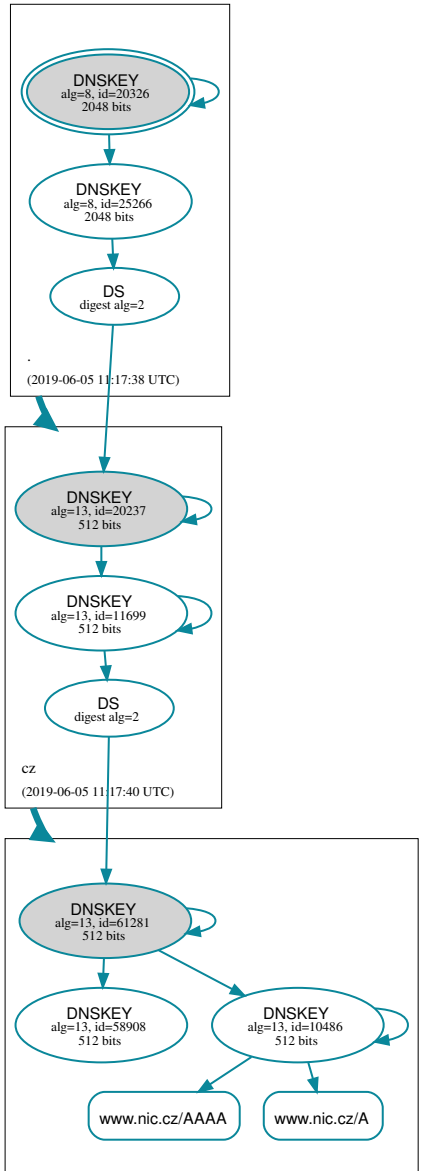
Principy DNS – stromová struktura



Principy DNS – cvičení – stromová struktura

www.dnsviz.net

Principy DNS – cvičení – stromová struktura



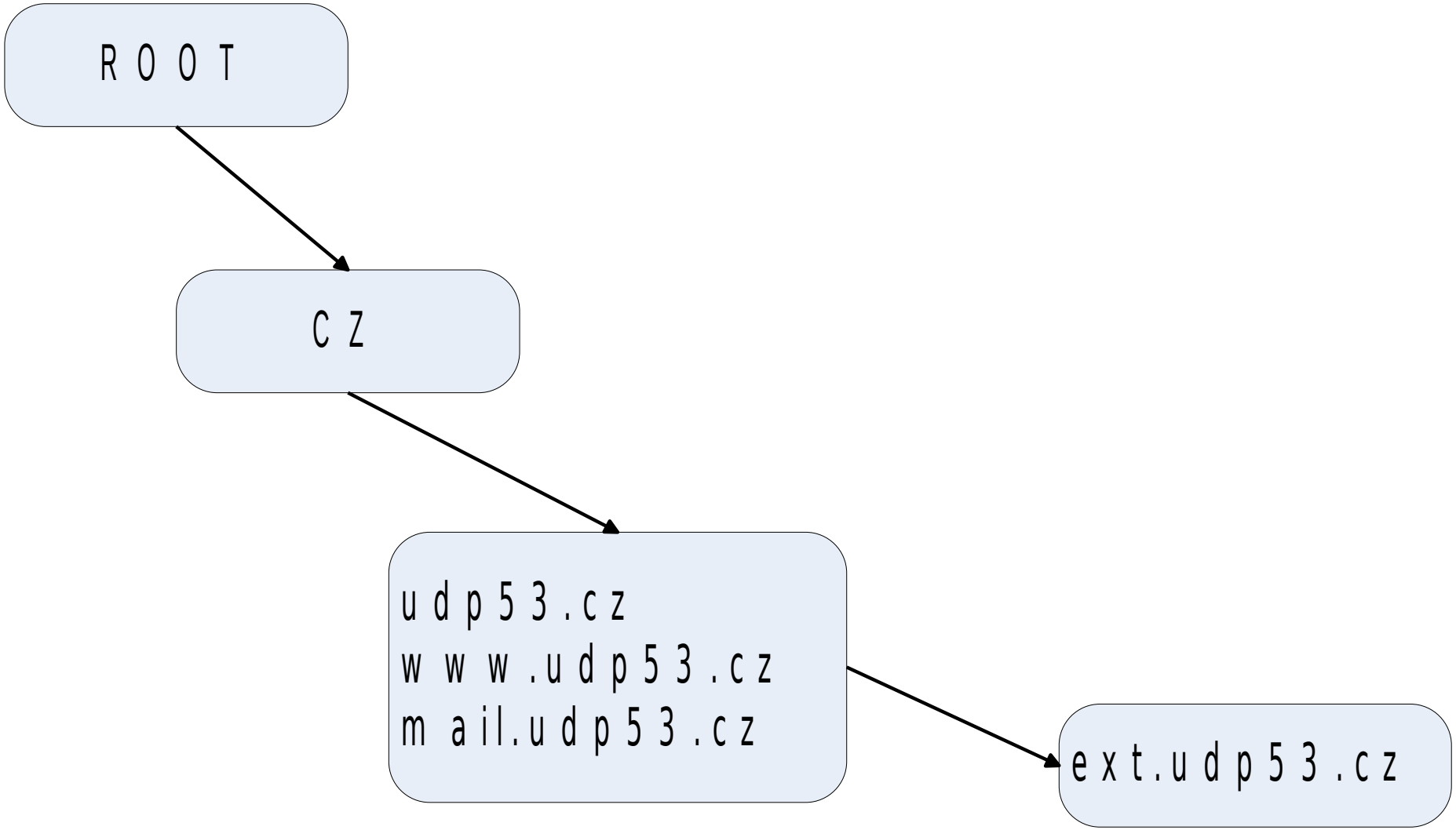
Doménové jméno

- „label“ – část mezi dvěma tečkami (max. 63 bytů)
  `"www"  "nic"  "cz"  ""`
- Doménové jméno (max. 255 bytů)
- Obecně může DNS přenášet libovolné znaky
- Prakticky se omezuje na
  - Písmena (US-ASCII)
  - Číslice
  - Pomlčka
  - Potržítko (ve speciálních případech)

Zóna

- Část hierarchie
- Samostatný správce
- Může být oddělená na úrovni labelů (teček) v doménovém jménu
- Delegovaná výše v nadřazené zóně (kromě '.')

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
- Textový formát, RFC 1035

```
dns53.cz.          600   IN SOA   ns.dns53.cz. hm.dns53.cz.
                   ( 2008101420 10800 3600 1209600 7200 )
www.dns53.cz.      600   IN AAAA  2001:1488:0:3::2
www.dns53.cz.      600   IN A     217.31.205.50
mail.dns53.cz.     600   IN AAAA  2001:1488:800:400::400
mail.dns53.cz.     600   IN A     217.31.204.67
dns53.cz.          600   IN AAAA  2001:1488:0:3::2
dns53.cz.          600   IN MX    10 mail.dns53.cz.
dns53.cz.          600   IN A     217.31.205.50
dns53.cz.          600   IN NS    a.ns.nic.cz.
dns53.cz.          600   IN NS    b.ns.nic.cz.
```

Autoritativní DNS server

- Má data příslušné zóny (domény)
  - Je pro ni autoritativní
- Každá zóna má vlastní DNS server
- Jeden DNS server může obsluhovat více zón
  - Lepší využití prostředků
- Zóna může (měla by) mít více DNS serverů
  - „Nařízeno“ v RFC 1912
  - Lepší dostupnost

Domain Name System

Princip funkce

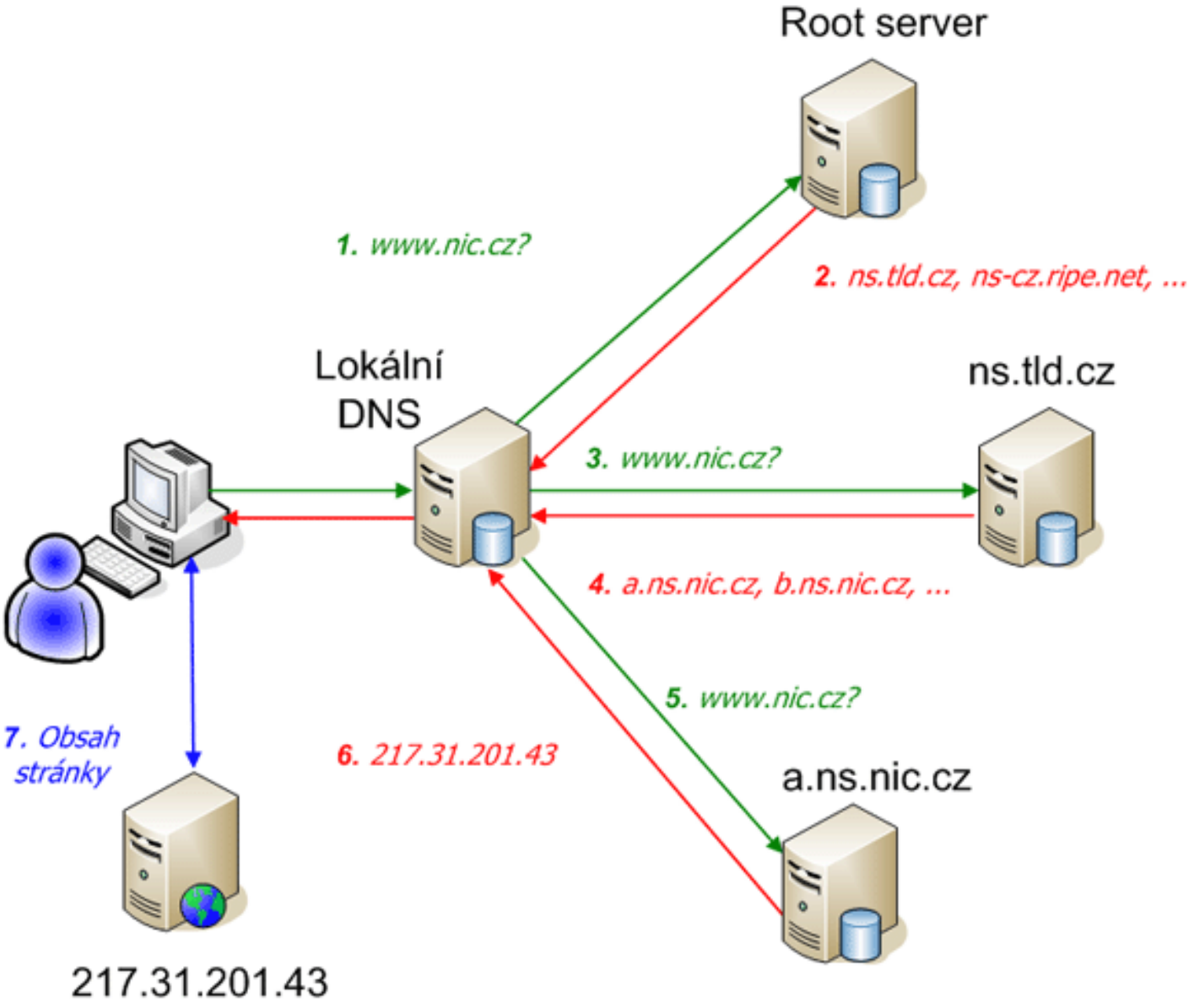
DNS autoritativní servery a resolvery

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

Autoritativní server

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

DNS dotazování – teorie



DNS dotazování – tradičně

- 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 – query name minimization

- Uživatel → Q(www.nic.cz) → Resolver
  - Resolver → Q(cz) → NS(Root)
  - NS(Root) → A(NS pro cz) → Resolver
  - Resolver → Q(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 – cvičení – stub resolver

```
$ dig cs.wikipedia.org

; <<>> DiG 9.14.2 <<>> cs.wikipedia.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64212
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cs.wikipedia.org.      IN  A

;; ANSWER SECTION:
cs.wikipedia.org.   74265  IN  CNAME  dyna.wikimedia.org.
dyna.wikimedia.org. 439 IN  A   91.198.174.192

;; Query time: 12 msec
;; SERVER: 172.20.20.53#53(172.20.20.53)
;; WHEN: St čen 05 13:09:34 CEST 2019
;; MSG SIZE  rcvd: 90
```

DNS dotazování – cvičení – rekurze "ručně"

```
$ dig @198.41.0.4 cs.wikipedia.org

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29128
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 13
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cs.wikipedia.org.      IN  A

;; AUTHORITY SECTION:
org.            172800  IN  NS  d0.org.afilias-nst.org.
org.            172800  IN  NS  a0.org.afilias-nst.info.

;; ADDITIONAL SECTION:
d0.org.afilias-nst.org.    172800  IN  A   199.19.57.1
d0.org.afilias-nst.org.    172800  IN  AAAA   2001:500:f::1
a0.org.afilias-nst.info.  172800   IN  A   199.19.56.1
a0.org.afilias-nst.info.  172800   IN  AAAA   2001:500:e::1
```

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
  - Není potřeba se stále ptát root serverů tak často

DNS dotazování

- Stub resolver
  - DNS klient v každém počítači
  - Implementován v systémových knihovnách
  - Malý, jednoduchý
  - Může, ale nemusí, implementovat cache
- Prohlížeče mají svou cache
  - Někdy ignorují stub resolver
  - Někdy ignorují i lokální rekurzivní resolver
  - DoH!

Autoritativní vs. neautoritativní

- Autoritativní odpověď
  - Od autoritativního nameserveru
  - Dotaz na doménu, pro kterou má server zónu
- Neautoritativní odpověď
  - Od resolveru
- Příznak v DNS zprávě
  - AA bit

Internet Governance

Správa DNS hierarchie

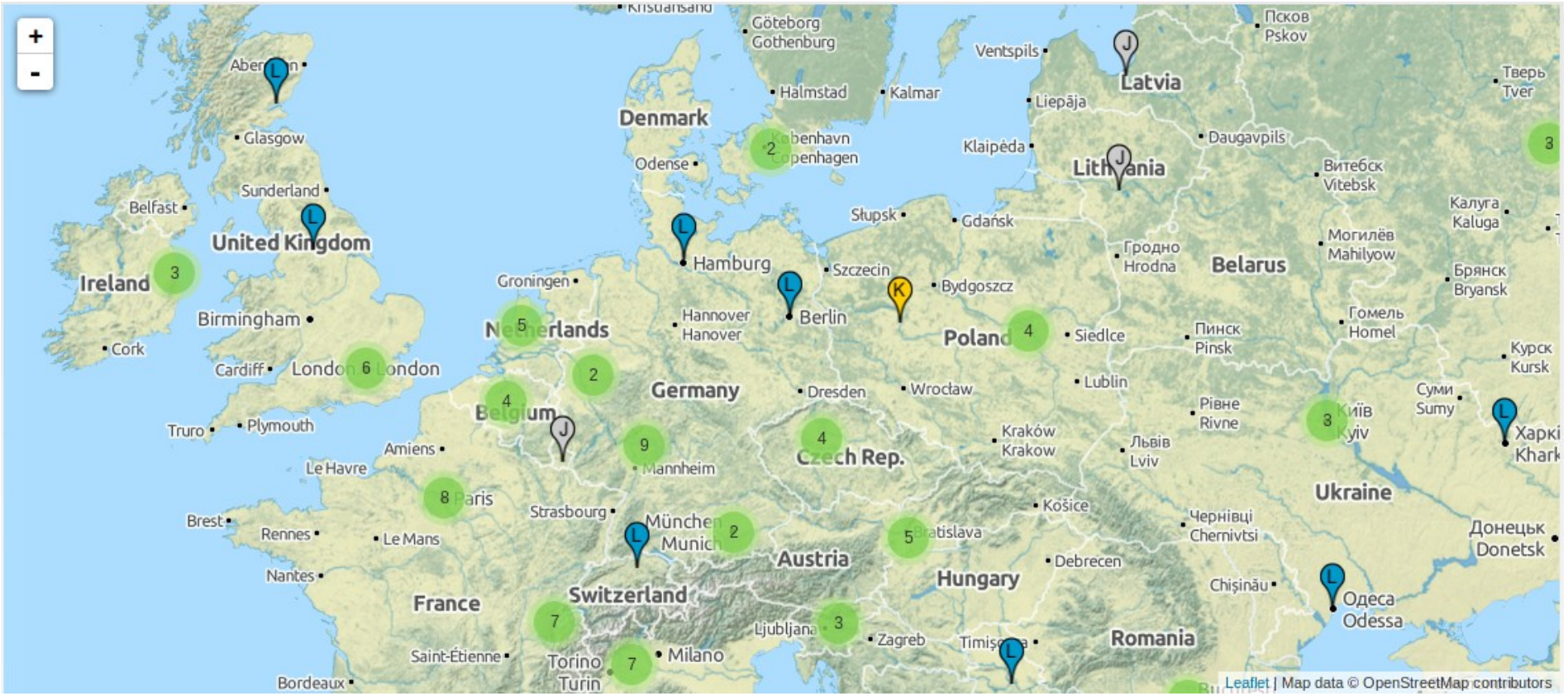
Root (kořenová) zóna

- ICANN
  - Internet Corporation for Assigned Names and Numbers
  - Koordinace DNS globálně
  - Ovlivňuje obsah zóny skrz IANA
- IANA
  - Internet Assigned Numbers Authority
  - Technická správa kořenové zóny
- VeriSign (.com)
  - Vytváří a podepisuje zónové soubory, stará se o distribuci
- Root Servers Operators
  - Zónu poskytují, ale nemohou ji měnit

Root servery

- http://www.root-servers.org
- Distribuované po celém světě
- IPv4 i IPv6
- 13 jmen (A – M.root-servers.net)
- Přibližně 1000 „skutečných“ serverů
- Root servery v České republice:
  - D.root-servers.net (op. University of Maryland)
  - 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, …
  - Nasazeno cca 1000 nových (.space, .rocks)
    - Některé již stihly zaniknout
- sTLD – sponzorované domény (mají určení)
  - .aero, .gov, .mil, .travel, .museum, …
- ccTLD – národní domény
  - .us, .cz, .de, .sk, …
- Infrastructure
  - .arpa

.cz ccTLD - (country code)

- Správce CZ.NIC
- Delegováno IANA
- Registr(1) → Registrátor(m) → Držitel(n)
- Name servery
  - 4 NS (a, b, c, d.ns.nic.cz)
  - IPv4 a IPv6
  - Cca 20 cílových lokalit
  - Geograficky diverzifikováno
  - Unicast → Anycast (4x)

DNS záznamy

Resource Records

RR záznam

```
www.nic.cz. 3600 IN AAAA 2001:DB8::1
```

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

RR záznam – RDATA

```
www.nic.cz. 3600 IN AAAA 2001:DB8::1
```

- Resource Data
  - Strukturovaná dle typu RR záznamu
  - Proměnlivá délka dat
  - Maximální délka 65535 oktetů
    - 2^16 - 1

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
PTR	Pointer	Reverzní delegace (IP adresa → jméno)
TXT	Text	Obecný text
DNSKEY	DNSKEY :-)	DNSSEC klíč
DS	Delegation Signer	hash DNSSEC klíče
RRSIG	RR Signature	DNSSEC podpis
…		A 100 dalších ...

https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-4

SOA záznam

- Jeden pro každou zónu
- Na vrcholu zóny
- Řídí master → slave komunikaci
- MINIMUM bylo původně defaultní TTL

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

```
dns53.cz. 600 IN SOA ns.dns53.cz. hostmaster.dns53.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

```
dns53.cz. 3600 IN NS ns.dns53.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

```
dns53.cz.    3600 IN NS ns.dns53.cz.
ns.dns53.cz. 3600 IN A  127.0.0.1
```

- DS pro DNSSEC, o tom ale příště ...

A a AAAA záznam

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

```
www.dns53.cz. 3600 IN A    127.0.0.1
www.dns53.cz. 3600 IN AAAA ::1
```

MX záznam

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

```
dns53.cz. 3600 IN MX 10 mail.dns53.cz.
dns53.cz. 3600 IN MX 20 mail2.nic.cz.
mail.dns53.cz. 3600 IN A 127.0.0.1
```

CNAME záznam

- Další jméno, Alias

```
www2.dns53.cz. 600 IN CNAME www.dns53.cz.
```

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

```
dns53.cz. 600 IN A 127.0.0.1
dns53.cz. 600 IN MX 10 mail.dns53.cz.
www.dns53.cz 600 IN CNAME dns53.cz.
```

  - Všechna RR pod dns53.cz jsou dostupné přes www.dns53.cz

CNAME záznam

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

    ```
    www.dns53.cz. 600 IN CNAME dns53.cz.
    ```

    ~~`www.dns53.cz. 600 IN A 127.0.0.1`~~

    ~~`www.dns53.cz. 600 IN AAAA ::1`~~
- Nesmí na něj ukazovat:
  - MX | NS záznamy
  - Další dle definice konkrétního protokolu
- Resolver/nameserver dále zpracovává výsledek
  - Může dojít k dalším dotazům

TXT záznam

- Obecná textová data
- Často (zne)užíván k ukládání strukturovaných dat
  - Sender policy framework – SPF (RFC 7208)
    - Povoluje email jen pro některé adresy
    - Existuje i SPF RR typ, ale ten už by se neměl používat

PTR záznam

- Obecně ukazatel na doménové jméno

```
1.0.0.127.in-addr.arpa. IN PTR dns53.cz
1.0.0 .. 0.0.0.ip6.arpa. IN PTR dns53.cz
```

- 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

TYPEXXX záznam

- Obecná data v hexa formátu
- Explicitně uvedená délka
- Důležité pro zpětnou kompatibilitu
- V zónovém souboru:

dns53.cz 3600 IN **TYPE65534 \#5 0883550001**

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 (povinný!)
- DNS server poslouchá na portu 53
- Dotazy chodí z náhodného portu
  - Kaminsky bug

Nástroje pro práci s DNS

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
- Knot DNS má také své utility khost, kdig ...

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

Konfigurace resolveru

Konfigurace **stub** resolveru

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

```
nameserver 127.0.0.1
nameserver 10.10.0.11
```

- Direktiva `search <subdomain>`:

```
search int.dns53.cz ext.dns53.cz
```

  - Nepoužívat!

Konfigurace **rekurzivního** resolveru – obecně

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

Dostupné resolvery

- **Unbound**
- **BIND 9**
- **Knot resolver**
- Microsoft DNS
- PowerDNS
- Další (zastaralé, špatné, nepodporující standardy)

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

Konfigurace rekurzivního resolveru Unbound

Unbound

- http://www.unbound.net
- Pouze rekurzivní server
- Validuje DNSSEC
- Používá knihovnu ldns
- NLnet Labs

Unbound: Seznámení

- Otevřete si manuálovou stránku

```
$ man unbound.conf
```

- Otevřete si konfiguraci v editoru

```
# gunzip /usr/share/doc/unbound/examples/unbound.conf.gz
# cp /usr/share/doc/unbound/examples/unbound.conf /etc/unbound/unbound.conf
# editor /etc/unbound/unbound.conf
```

- Nástroj na ovládání **unbound-control**:

  status, start, stop, reload, stats, dump_cache, load_cache

- 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> <deny,
refuce, allow ...>
```

- Kořenové NS (hints)

```
root-hints:
```

- Stub zóny

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

- Forward zóny

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

Unbound: Testování konfigurace

- Před (re)startem zkontrolujte konfiguraci

```
# unbound-checkconf

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

Unbound: Příprava na úkoly

- Nainstalujte Unbound

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

- Nakonfigurujte Unbound aby fungoval unbound-control

```
editor /unbound/unbound.conf,
```

  - přidat:

```
remote-control:
  control-enable: yes
  control-use-cert: no
```

- Restartujte unbound:

```
# systemctl restart unbound
```

Unbound: Úkol č. 1

- Zkontrolujte zda běží Unbound

```
# systemctl status unbound
```

- Nakonfigurujte stub resolver, aby používal Unbound

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

- Otestujte, že vše funguje:

```
# ping www.nic.cz
```

  - Otevřete stránku v prohlížeči

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

Unbound: Úkol č. 2

- Nakonfigurujte Unbound, aby přeposílal dotazy na DNS server 193.17.47.1

```
forward-zone:
  name: "."
  forward-addr: 193.17.47.1
```

- Reload konfigurace:

```
# unbound-control reload
```

Unbound: Úkol č. 3

- Nakonfigurujte Unbound se stub zónou skoleni.dns53.cz na serveru IP_LEKTOR

```
stub-zone:
  name: "skoleni.dns53.cz"
  stub-addr: IP_LEKTOR
```

- Restartujte Unbound

```
# systemctl restart unbound
```

- Ověřte doménu www.skoleni.dns53.cz

```
$ ping www.skoleni.dns53.cz
```

Unbound: Úkol č. 4

- 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

```
# systemctl restart unbound
```

- Zkontrolujte, že přístup funguje

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

Konfigurace autoritativních serverů

Zónový soubor: Úkol č. 1

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

```
# wget -O /etc/bind/z<NN>.lab.nic.cz
https://secure.nic.cz/files/akademie/dns/template_zone
```

  - **např.** `wget -O /etc/bind/z01.lab.nic.cz https://secure.nic.cz/files/akademie/dns/template_zone`

- Změňte z**<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
  - Nepřidávejte DNSSEC záznamy :)
- Nezapomeňte po každé změně zvýšit sériové číslo v SOA záznamu
- Zkontrolujte validitu zónového souboru

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

- **BIND 9**
- **Knot DNS**
- NSD 4
- PowerDNS
- Microsoft DNS
- MyDNS
- http://en.wikipedia.org/wiki/Comparison_of_DNS_server_software

Zone Transfer

- Master → Slave, Slave → Slave
- AXFR
  - Přenáší se vždy celá zóna
  - Transportní vrstva TCP
- IXFR
  - Inkrementální transfer
  - Přenáší se pouze změny
  - Transportní vrstva TCP

Konfigurace AXFR

- BIND 9

```
options { allow-transfer { acl; <ip_addr>; }; };
zone "dns53.cz" { allow-transfer { acl; ip; };};
view { … };
```

- NSD4

```
provide-xfr: <ip_addr> NOKEY|<tsig_keyname>
request-xfr: <ip_addr> NOKEY|<tsig_keyname>
```

Konfigurace IXFR

- BIND 9

```
provide-ixfr yes/no;
request-ixfr yes/no;
zone "dns53.cz" {
  journal "/var/lib/bind/dns53.cz.jnl";
  ixfr-from-differences yes/no;
};
```

Obsah (den první)

- Základní popis DNS
- Správa DNS hierarchie
- RR záznamy
- Rekurzivní server
  - Konfigurace Unbound
- Formát zónového souboru
- **Autoritativní server**
  - Konfigurace BIND 9
- TSIG (dle času)

Konfigurace autoritativního DNS serveru BIND 9

BIND 9: Seznámení

- 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/refresh/notify/sign ...
```

- Kontrola konfigurace

```
# named-checkconf
# named-checkzone
```

BIND 9: Úkol č. 1

- Poslouchá pouze na rozhraní eth0 (IPv4 i Ipv6)
- V souboru **/etc/bind/named.conf.options**:

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

- Je autoritativní pro z<NN>.lab.nic.cz a má povolený odchozí transfer pro lektorský počítač **/etc/bind/named.conf.local**

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

- Nastartuje BIND 9, pokud už neběží:

```
systemctl start bind9
```

- Ověřte (dig | drill | host)

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

BIND 9: Úkol č. 2

- Master i slave server pro souseda:

/etc/bind/named.conf.local

```
# Přidat
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>; };
};

# Upavit

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
```

TSIG

Secret Key Transaction Authentication for DNS

TSIG

- RFC2845 (r. 2000)
  - Secret Key Transaction Authentication for DNS (TSIG)
  - Obecný podpis DNS zpráv
- Více použití
  - Autentizace transferů zón
  - Autentizace notify zpráv
  - Autentizace dotazů

TSIG

- Symetrická kryptografie
  - ~~HMAC-MD5 [1..512]~~
    - Nepoužívat
  - ~~HMAC-SHA1 [1..160]~~
    - Raději také nepoužívat
  - HMAC-SHA(224|256|384|512)

Vygenerování klíče

- Balík bind9utils

```
$ tsig-keygen -a hmac-sha256 <jméno>.
```

- Generujeme
  - Algoritmem HMAC-SHA256 (-a)
  - Název klíče: <jméno>.

TSIG: Úkol č. 1

- Vygenerujte TSIG klíč
  - Algoritmus HMAC-SHA256

```
#tsig-keygen -a hmac-sha256 >
pc<NN>.lab.nic.cz.key
```

- Podívejte se do vygenerovaného souboru

```
# cat pc<NN>.lab.nic.cz.key
```

TSIG: Úkol č. 2

- Nakopírujte váš klíč k sousedovi
- scp <cesta_ke_klici.key> X.X.X.<SS>:/home/lab/<jmeno_klice.key>
- Heslo bude sděleno lektorem
- Zachovejte jména klíčů (**Jména klíčů jsou součástí autentizace!)**
- Musí odpovídat:
  - Algoritmus
  - Jméno klíče
  - Hodnota klíče

TSIG debug

- Pokud je master dobře nastaven, nepovolí odchozí transfer bez správného klíče. (dig vrátí transfer failed)
- Pokud transfer projde, duplikujte parametry digu v nastavení serveru
- tsig klíč předáme digu jako parametr:

  dig AXFR <zona> -y <algoritmus>:<jmeno-klice>:<digest> @X.X.X.<SS>

  dig AXFR <zona> -y **hmac-sha256**:<jmeno-klice>:<digest> @X.X.X.<SS>

TSIG+BIND: Úkol č. 3 (master)

- Povolte transfer přes TSIG pro souseda

/etc/bind/named.conf.local

```
# Přidat

key "pc<SS>.lab.nic.cz." {
  algorithm hmac-sha256; secret "<klic_souseda>";
};

acl soused { key pc<SS>.lab.nic.cz; };

# Upravit

zone "z<NN>.lab.nic.cz." {
  type master;
  file "/etc/bind/z<NN>.lab.nic.cz";
  allow-transfer { soused; };
  notify explicit;
  also-notify { X.X.X.1<SS>; };
};
```

TSIG+BIND: Úkol č. 3 (slave)

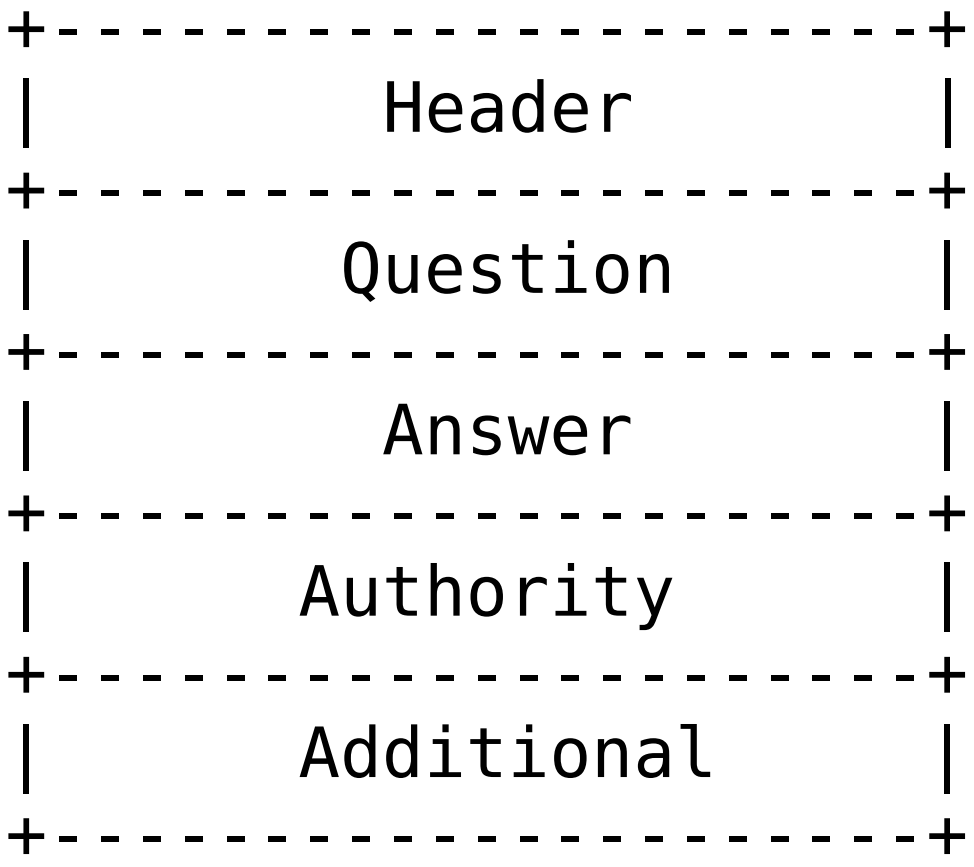
- Nakonfigurujte transfer slave zóny pomocí TSIG

/etc/bind/named.conf.local

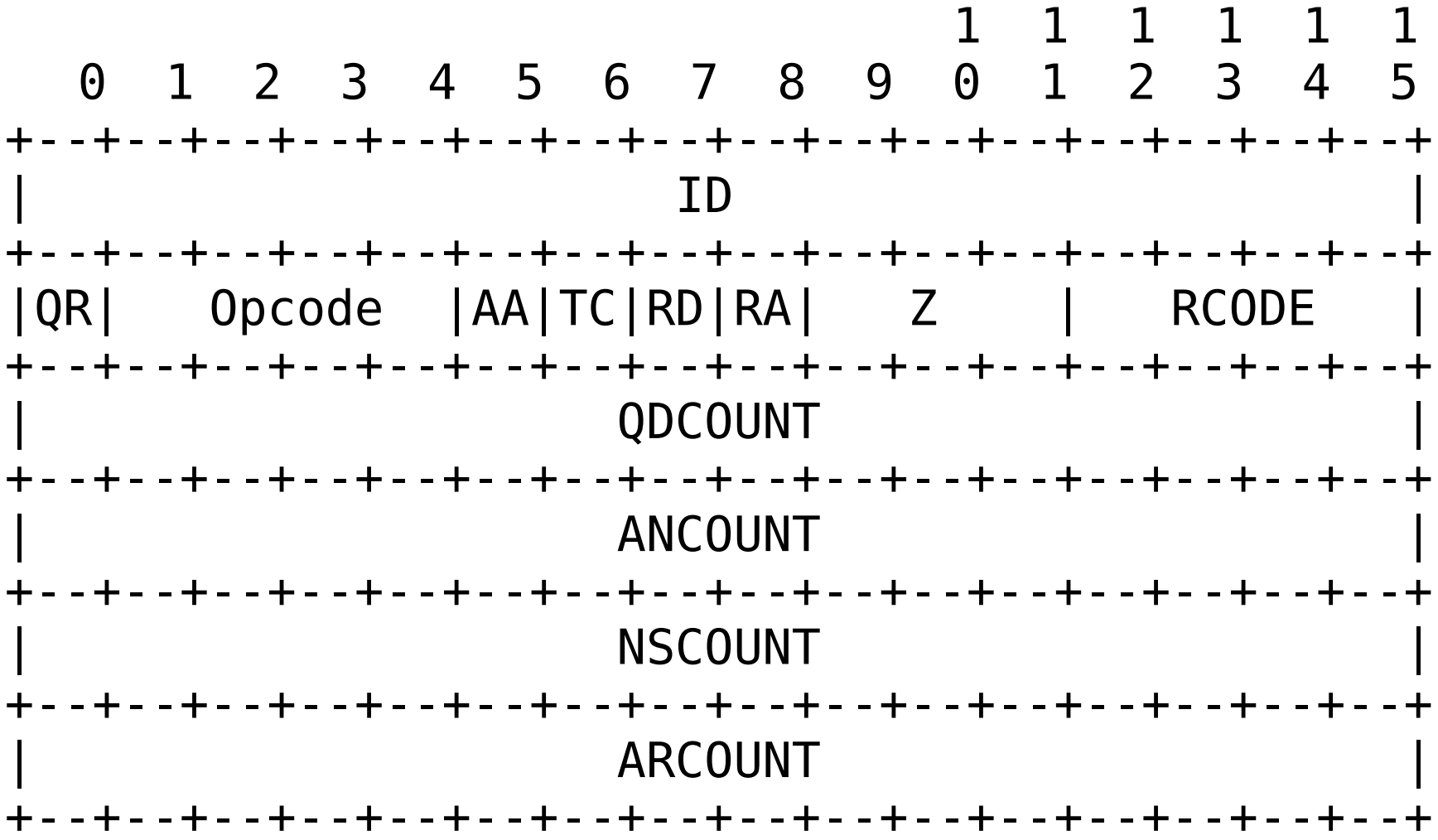
```
# Přidat
key "pc<NN>.lab.nic.cz." {
  algorithm hmac-sha256; secret "<vas_klic>";
};
server X.X.X.1<SS> {keys{pc<NN>.lab.nic.cz;};};
# Ponechat
zone "z<SS>.lab.nic.cz." {
  type slave;
  file "/var/cache/bind/z<SS>.lab.nic.cz";
  masters { X.X.X.1<SS>; };
  notify no; allow-notify { X.X.X.1<SS>; };
};
```

Formát DNS zprávy

Formát DNS zprávy



Hlavička DNS zprávy



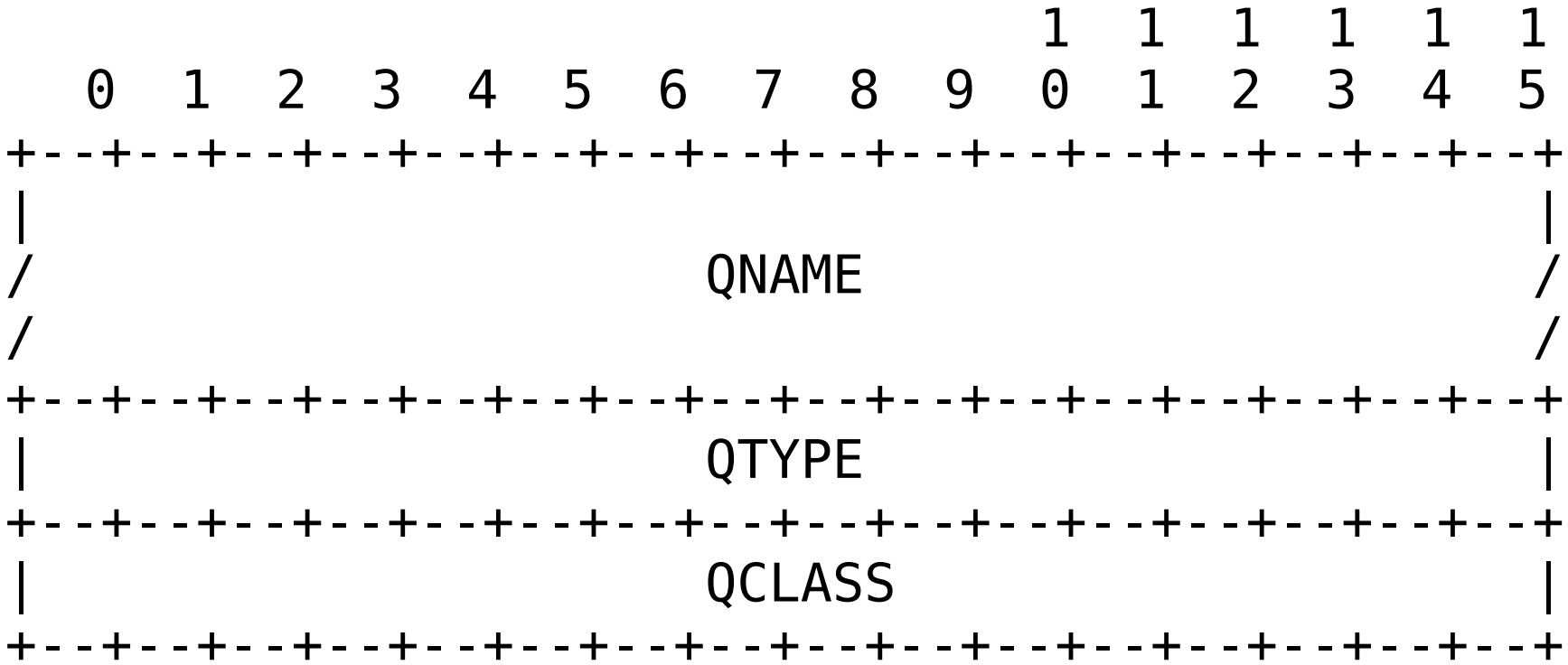
Hlavička DNS zprávy

- ID – 16-bit náhodně generované
  - 16-bit jako ochrana dnes nestačí
  - Pozor na „chytrá“ zařízení, která můžou odstranit náhodnost zdrojových portů
- QR, Opcode
  - QR – dotaz/odpověď
  - Opcode – QUERY/IQUERY/STATUS

Hlavička DNS zprávy

- Příznaky
  - AA – authoritative answer
  - TC – truncation (použij TCP)
  - RD/RA – recursion desired/available
- Z – rezervováno
- RCODE (4-bit) – návratový kód
  - NOERROR
  - FORMERR/SERVFAIL/NOTIMPL/REFUSED
  - NXDOMAIN – neexistence jména

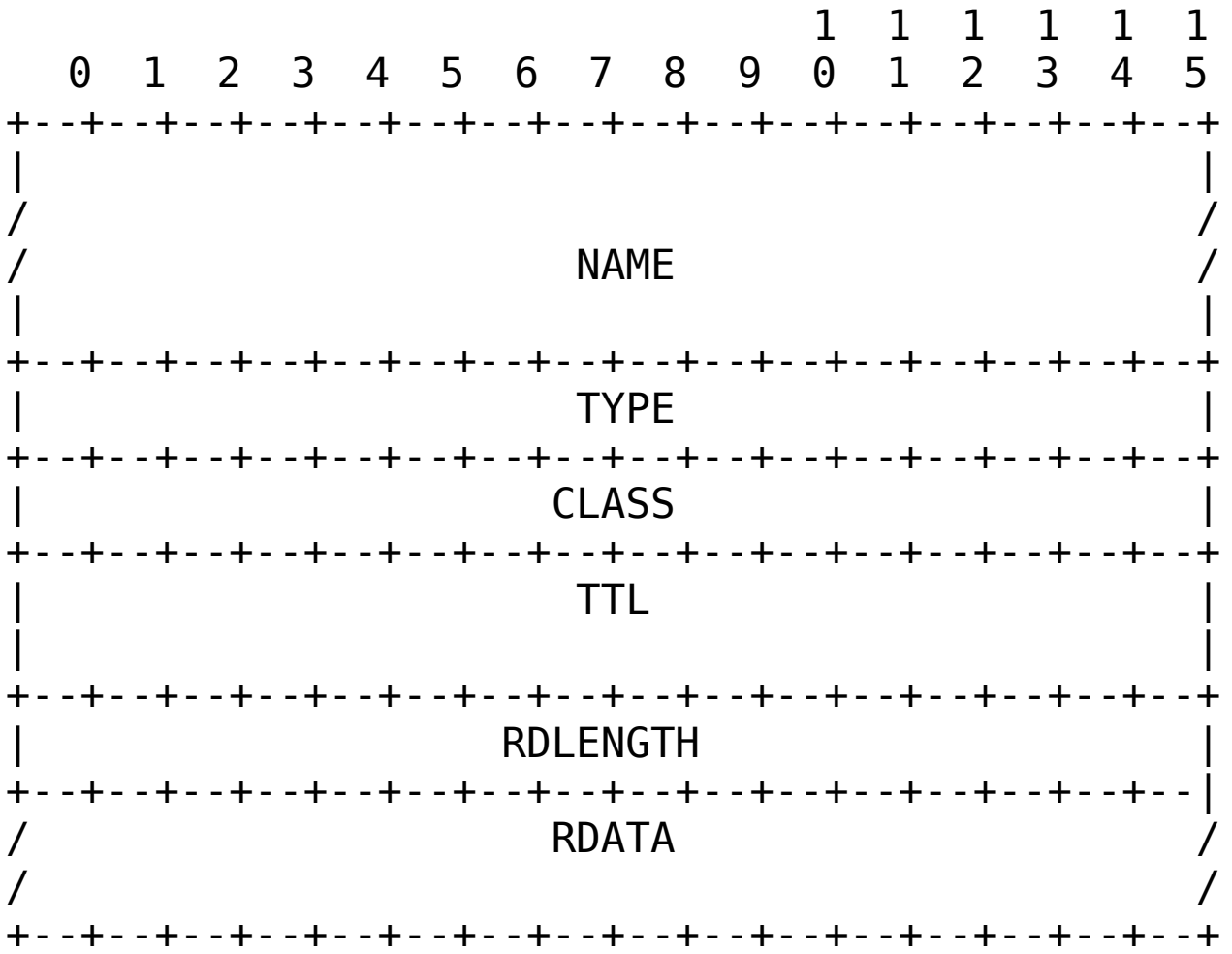
Formát sekce QUESTION



Speciální typy (meta) v dotazech

- Možné použít pouze v dotazu (query)
- Nadmnožina typů
  - Lze použít pro všechny typy
- Speciální položky
  - 252 – AXFR
  - 255 – ANY – nepoužívat
- Obdobně třída:
  - 255 – ANY – nepoužívat

Formát RR záznamu
(Ostatní sekce)



Kódování jména

- Rozkouskováno na labely
- Tečky jsou vynechány
- Label
  - 1 oktet délka (dva bity 0, hodnota na 6 bitech)
  - Až 63 oktetů samotný obsah
- Konec jména
  - Label s nulovou délkou

Komprese

- Pouze u známých typů (CNAME, PTR, …)
- Šetří místo
- Odkazuje se na již použité doménové jméno
- Místo délky labelu – 16 bitů celkem
  - Dva horní bity nastaveny na 1
  - Dolních čtrnáct bitů specifikuje OFFSET od začátku DNS zprávy (ID v hlavičce)

Komprese

- Doménové jméno ve zprávě:
  - Sekvence labelů končící nulovým labelem
    - 00000011www00000011nic00000010cz00000000
  - Odkaz
    - 11<odkaz na www.nic.cz>
  - Sekvence labelů končící odkazem
    - 00000011www11<odkaz na nic.cz>

Úkol č. 1 – pohled na síť

- Spusťe wireshark

```
$ sudo -s
# wireshark
```

- Poslouchejte na rozhraní eth0
- Zapněte filtr na udp port 53

```
udp.port == 53
nebo jen „dns“
```

Úkol č. 1 – pohled na síť

- Zeptejte se na nic.cz

```
$ dig IN NS nic.cz
```

- Prohlédněte si UDP zprávu s dotazem
- Prohlédněte si UDP zprávu s odpovědí

Rozšiřující mechanismy

- Původně maximální velikost zprávy 512 oktetů

```
;; Query time: 22 msec
;; SERVER: 10.0.0.138#53(10.0.0.138)
;; WHEN: Thu Oct 15 01:39:21 2009
;; MSG SIZE  rcvd: 488
```

- 512 oktetů může být často málo

```
$ dig IN ANY nic.cz
;; Truncated, retrying in TCP mode.
```

EDNS0

- Standardizováno v RFC2671
  - Extension Mechanisms for DNS (EDNS0)
- Definuje speciální RR typ **OPT**
  - Přidává se do sekce additional v dotazu i odpovědi
- Rozšiřuje DNS zprávu o
  - Volitelnou maximální velikost
    - Nové problémy s IP fragmetnací!
  - Nové návratové hodnoty RCODE
  - Nové atributy

EDNS0

Field Name	Field Type	Description
NAME	domain name	empty (root domain)
TYPE	u_int16_t	OPT
CLASS	u_int16_t	sender's UDP payload size
TTL	u_int32_t	extended RCODE and flags
RDLEN	u_int16_t	describes RDATA
RDATA	octet stream	{attribute,value} pairs

DNS flag day

- Někdy v roce 2020
- Povinná podpora TCP
- https://dnsflagday.net/

Úkol č. 2 – velké odpovědi

- Ignorujte zkrácení zprávy (truncation)

```
$ dig +noedns +notcp +ignore
    bigtxt.knot-resolver.cz TXT
;; flags: qr tc rd ra;
;; MSG SIZE  rcvd: 41
```

- Použijte EDNS0

```
$ dig +edns=0 +bufsize=8192
    bigtxt.knot-resolver.cz TXT
;; MSG SIZE  rcvd: 4189
```

Úkol č. 3 – dotaz na delegaci

```
$ dig nic.cz NS
```

- Spočítejte počet RR záznamů v sekci Additional

```
a.ns.nic.cz.    212   IN  A      194.0.12.1
a.ns.nic.cz.    212   IN  AAAA   2001:678:f::1
b.ns.nic.cz.    212   IN  A      194.0.13.1
b.ns.nic.cz.    212   IN  AAAA   2001:678:10::1
d.ns.nic.cz.    212   IN  A      193.29.206.1
d.ns.nic.cz.    212   IN  AAAA   2001:678:1::1
```

- Zkontrolujte s hlavičkou

```
ADDITIONAL: 7
```

- Zkontrolujte ve wiresharku

NSID + *.bind CH zóny

- NSID: RFC 5001
- Identifikátor serveru
- Hodí se při anycastu
- CH zóny version.bind, hostname.bind

Úkol č.3

- Nastavte NSID a CH informace BIND serveru

```
options {
    server-id “vaseid“;
    version “verze“;
    hostname “hostname“;
}
```

- Ověřte:

```
dig vasezona +nsid @localhost
dig version.bind CH TXT @localhost
```

Úvod do DNSSEC

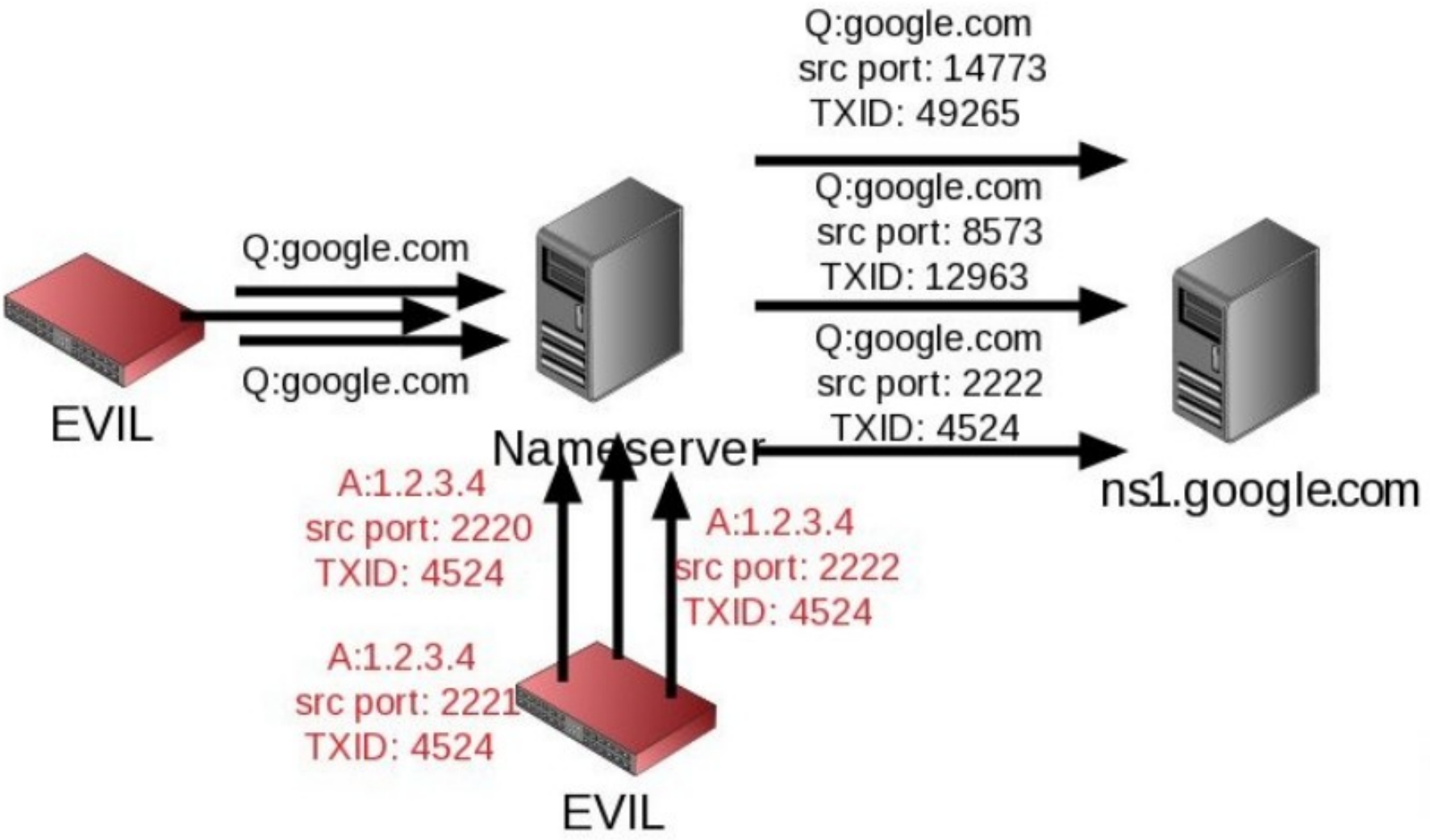
Co se dozvíte

- Proč potřebujeme DNSSEC?
- Jak DNSSEC funguje?
- Jaké jsou s DNSSEC problémy?
- Přehled SW pro práci s DNSSEC.

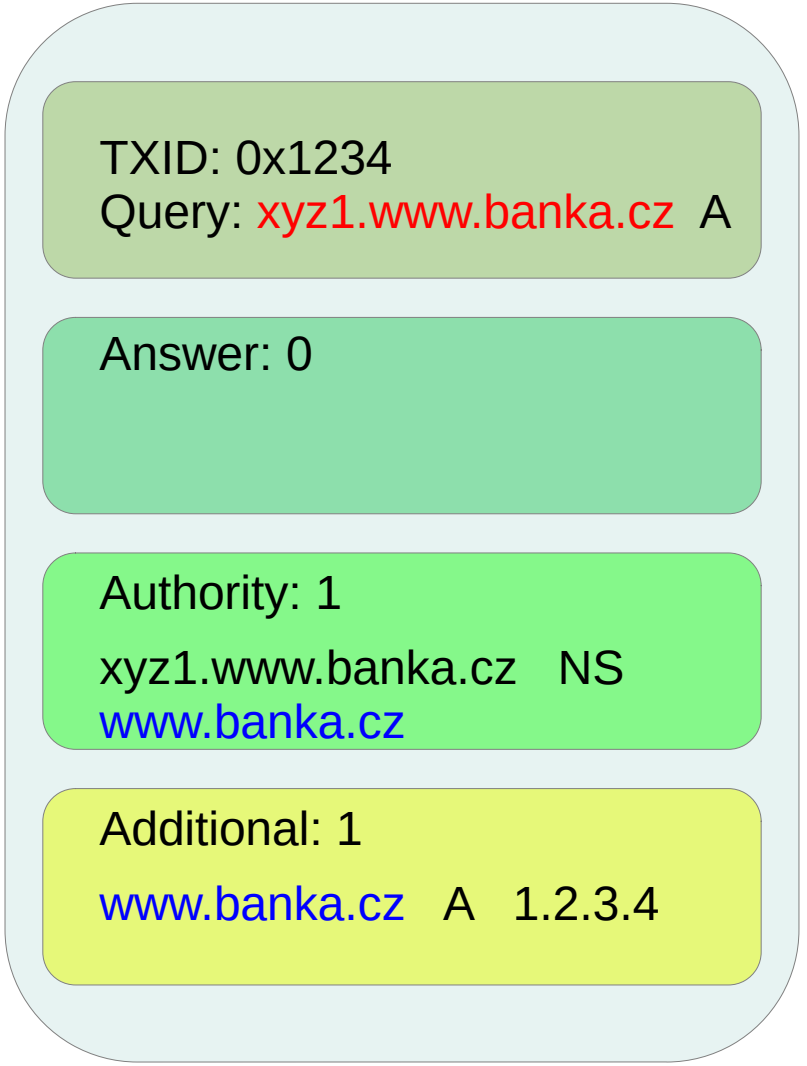
Proč DNSSEC?

- Bez DNSSEC není možné ověřit správnost DNS dat
  - Původní návrh protokolu s bezpečností nepočítá
- Na DNSSEC závisí další protokoly
  - DANE …

Cache poisoning útok



Cache poisoning – Kaminsky



- Nestihl útočník uhodnout TXID/port u dotazu na xyz1.www.banka.cz?
- Nevadí
- Zkusí okamžitě na xyz2.www.banka.cz
- .....

Hezberg & Shulman (2013)

- Útok pomocí fragmentace IP paketů
  - Protokol povoluje fragmentaci velkých paketů kvůli omezení fyzického média (ethernet)
  - Zdroje náhodnosti (UDP port, DNS-ID) zůstávají v prvním fragmentu
  - Zbývá uhodnout IP-ID (16-bit) a UDP checksum
    - Vhodně položený dotaz a zóna generují stejný kontrolní součet
    - Zbývá uhodnout IP-ID
- IP stack složí podvržený paket, pokud se útočník trefí do IP-ID a jeho fragment příjde dřív

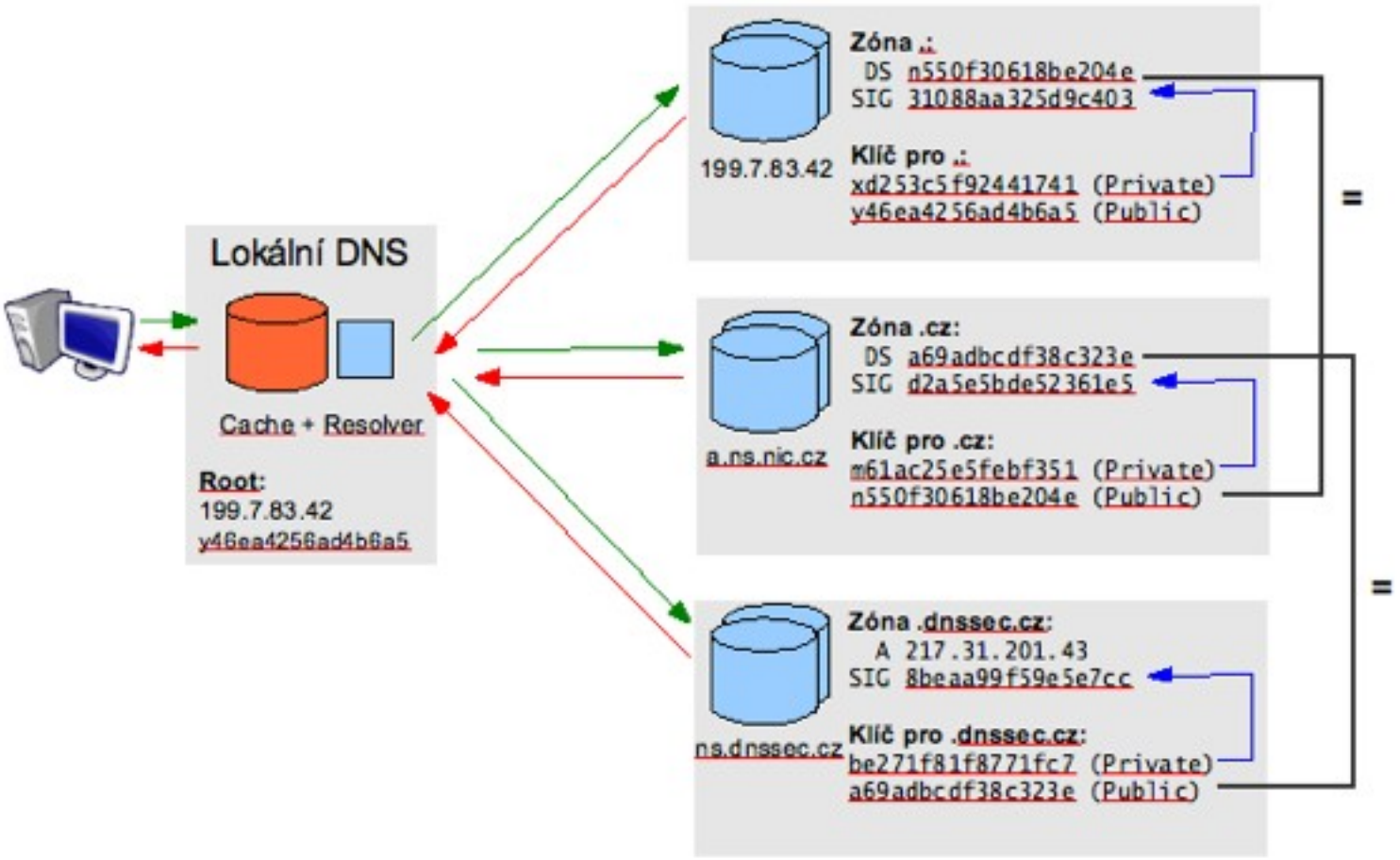
Základní principy DNSSEC

- DNSSEC umožňuje autoritativním serverům poskytovat k „standardním“ DNS datům navíc digitální podpisy RRSetů
- Resolvery ověřující DNSSEC podpisy poskytují potvrzené odpovědi
- Klienti, kteří používají validující resolvery, získávají „správná“ data
- Odpovědi, které nejsou validní, jsou klientovi vráceny z nadřazeného resolveru s chybou „SERVFAIL”

Základní principy DNSSEC

- Dotazy a odpovědi jdou stále po síti nezašifrované!
- Bez DNSSEC validace nechrání
  - Např. pokud vám někdo přenastaví resolver v /etc/resolv.conf nebo na routeru!
  - Řešení je validovat lokálně, použijte forwading.
  - Last-mile zabezpečení (CGA-TSIG)

Základní principy DNSSEC

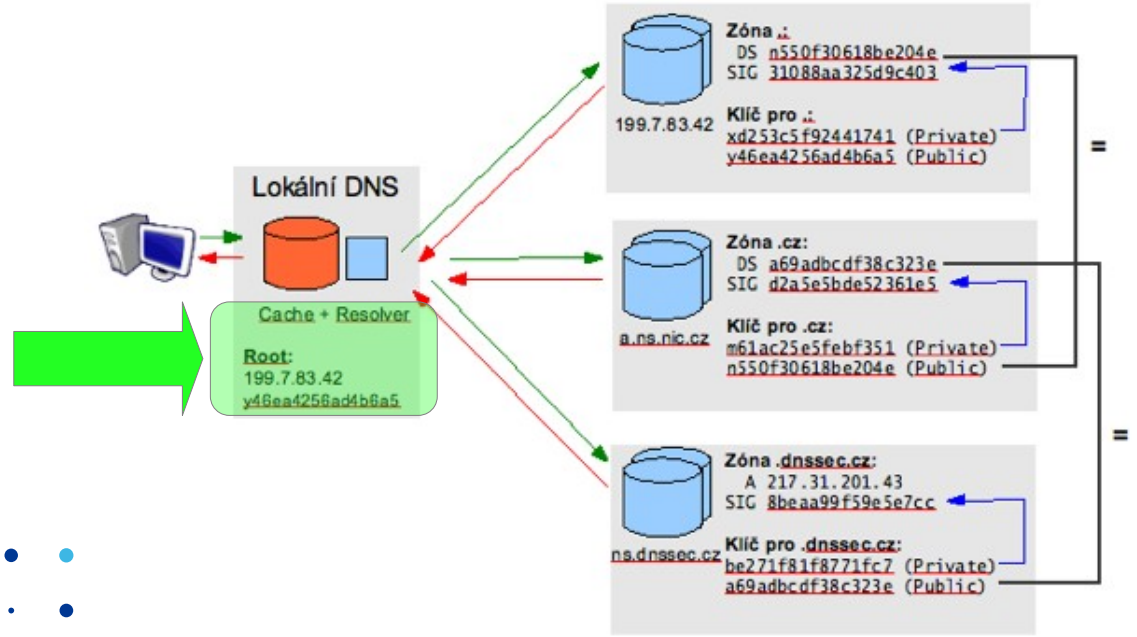


Základní pojmy DNSSEC

- Pevný bod důvěry
- Řetěz důvěry
- Důvěryhodný klíč
- Ostrov důvěry
- Validující Resolver
- Key Signing Key (KSK)
- Zone Signing Key (ZSK)

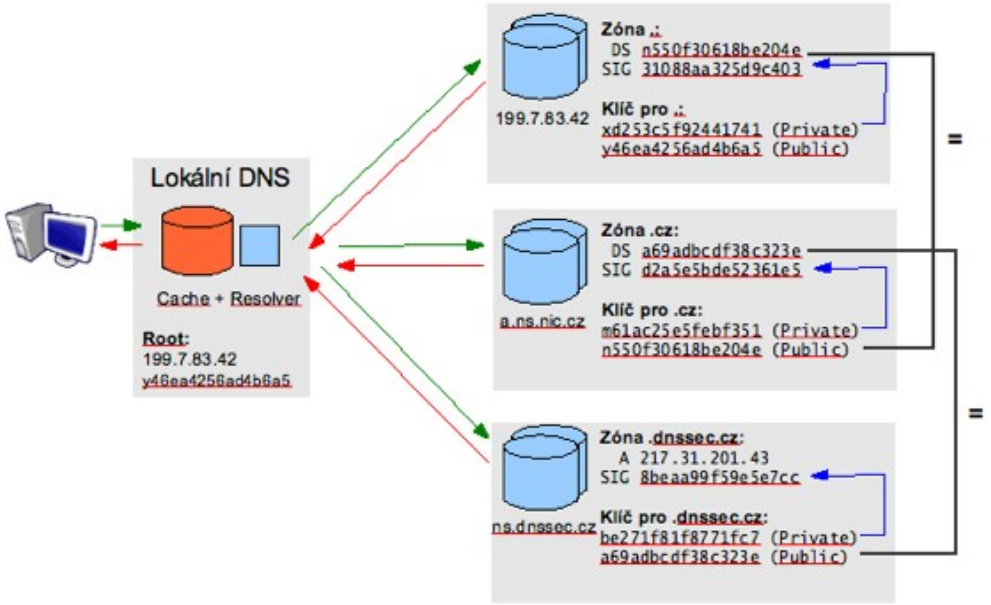
Pevný bod důvěry (Trust Anchor)

- Nakonfigurovaný klíč (nebo jeho hash), kterému důvěřujeme
- Musíme ho získat nějakou bezpečnou cestou
  - (S distribucí, přes TLS, pošta, telefon)



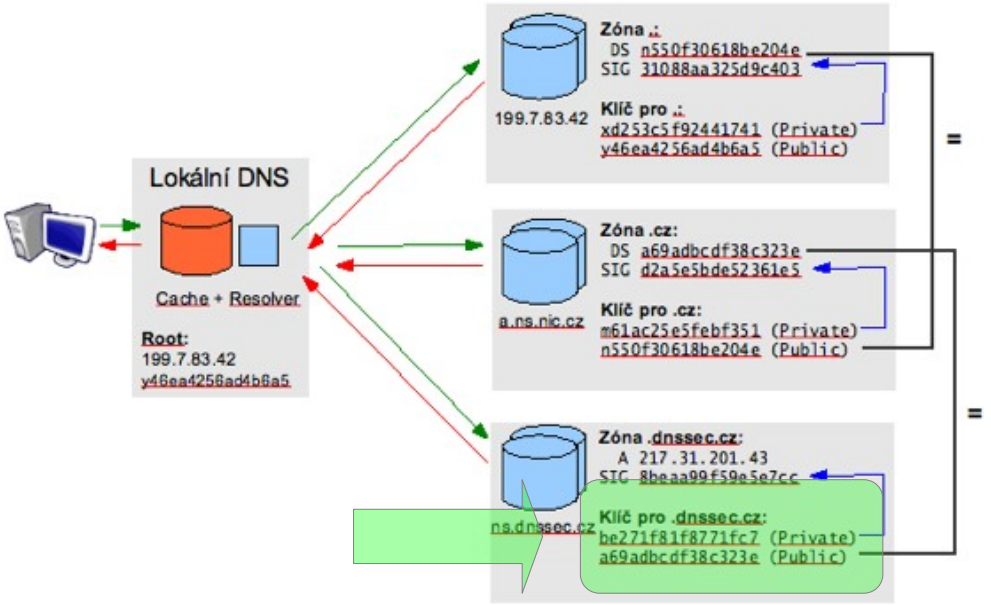
Řetěz důvěry

- Sekvence DNSSEC záznamů (DNSKEY a DS) vedoucí od Pevného bodu důvěry k uzlu v DNS stromu
- V každém uzlu/úrovni máme ověřená data



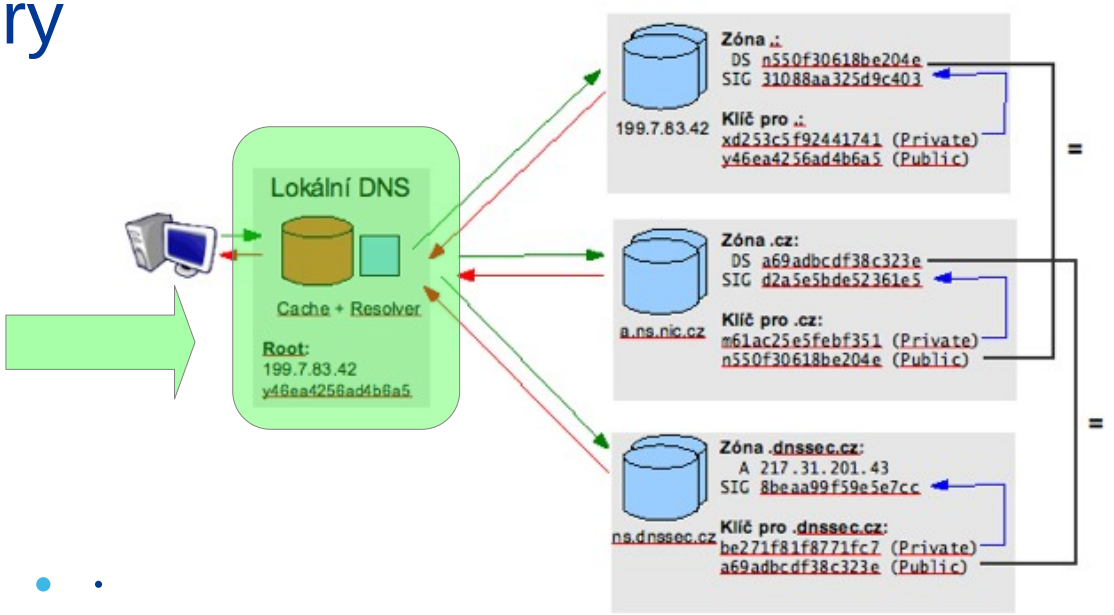
Důvěryhodný klíč

- DNSSEC klíč, který je důvěryhodný (you don't say...)
  1) Pevný bod důvěry
  2) Klíč získaný přes Řetěz důvěry



Validující Resolver

- Posílá DNS dotazy s DNSSEC OK
- Ověřuje validitu DNSSEC podpisů v DNS odpovědích
- Má nakonfigurovaný alespoň jeden Pevný bod důvěry



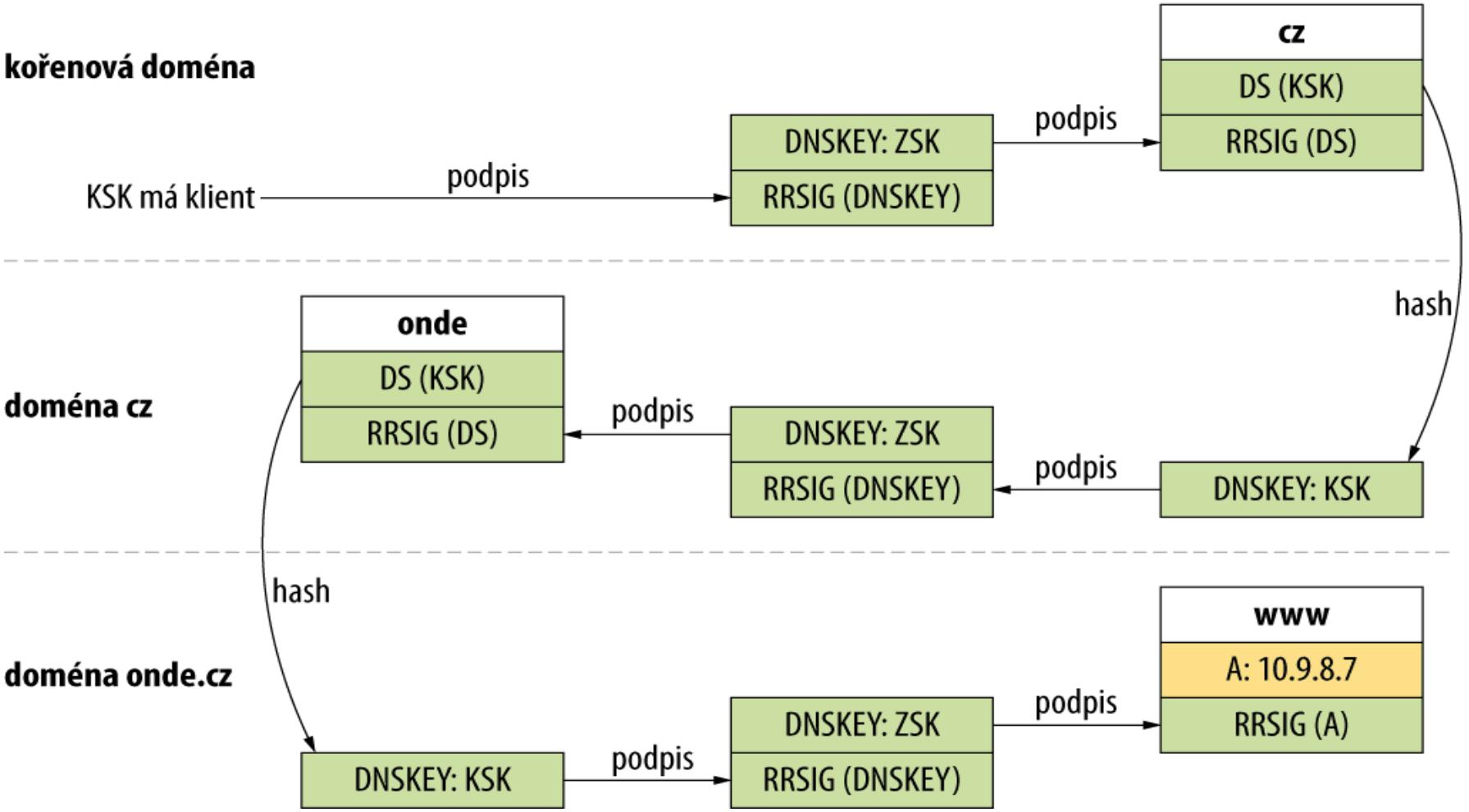
Key Signing Key

- DNSSEC klíč používaný pro podepsání dalších klíčů
  - Silnější
  - Více bitů
  - Výpočetně složitější
  - Více dat
  - Speciální bit (SEP) v příznacích DNSSEC klíče

Zone Signing Key

- DNSSEC klíč používaný pro podepsání vlastního obsahu zóny
  - Slabší
  - Méně bitů
  - Výpočetně jednodušší
  - Rychlejší podpis i ověřování
  - Méně dat

Příklad: doména onde.cz



DNSSEC

Nové RR záznamy

DNSKEY RR záznam

- DNSSEC klíč
- RDATA obsahují
  - Příznaky (Flags)
  - Protocol (vždy 3)
  - Algoritmus
    - 8 – RSASHA256
    - 13 – ECDSAP256SHA256
  - Veřejný klíč
- IN DNSKEY `257 3 8 AwEAAd[...]kNB8Qc=`

RRSIG RR záznam

- Digitální podpis RRSetu
- Obsahuje:
  - Podepsaný RR typ
  - Algoritmus
  - Počet labelů v podpisovaném jméně (kvůli *)
  - Původní TTL
  - Datum platnosti (začátek a konec)
  - Key Tag, Jméno zóny
  - Digitální podpis
- `IN RRSIG A 13 2 1800 20190330173930 20190317114002 46307 dnssec.cz. aD3IV9WM0gPBZfv[...]`

NSEC RR záznam

- Záznam vyznačující neexistenci doménového jména – pomocí vyjmenování dalšího následujícího labelu
- Zóna musí být seřazena (v každé úrovni hierarchie)
- Obsahuje:
  - Další doménové jméno
  - Bitová mapa existujících typů (pro vlastníka)
- `IN  NSEC dns53.cz. NS RRSIG NSEC DS`

NSEC3 RR záznam

- Řeší zone walking problém s NSEC
- NSEC3 jména hashuje
- NSEC3 RR tvoří řetěz v hashovaném pořadí
- NSEC3 RR dokáže existenci hierarchicky „nejbližšího“ jména a neexistenci přesnější zhody
- Zvýšená zátěž jak pro nameserver, tak pro resolver
  - Možnost zahltit nameserver neexistujícími dotazy
- Možnost vypustit z řetězu nepodepsané delegace
  - NSEC3 Opt-out
  - Pouze pro TLD, nepoužívat jinde!

NSEC3PARAM záznam

- Obsahuje kód algoritmu a NSEC3 salt
  - Salt – použit při vytváření NSEC3 záznamů
- TTL může být nulové
  - Dle RFC se nesmí použít na validaci
- Vlastníkem vždy vrchol zóny
- cz. 0 IN NSEC3PARAM 1 0 10 [Hex salt]
  - Obsahuje: algoritmus, flags (0), délku salt, salt
  - Kód algoritmu musí odpovídat tomu v NSEC3 záznamech

DS RR záznam

- Záznam o bezpečné delegaci
- V nadřazené zóne
- RDATA obsahují hash DNSKEY klíče, kterým je zóna podepsaná
- Obsahuje:
  - Key Tag
  - Algoritmus
  - Digest Type
  - Digest
- `IN DS  17398 13 1 BBDDD[...]3502D`

Co je potřeba?

- Aktuální SW
- Podepsaná doména
- DS záznamy v nadřazené doméně
- Automatizace výměny klíčů
  - Ruční výměna možná, ale pravděpodobnost chyb je značná.
- Validující resolver
- Rozumné firewally
  - Omezení UDP > 512B, zahození dotazů s EDNS0

Software pro DNSSEC

- Unbound
- BIND a jeho nástroje
  - Automatické podepisování
  - Ruční podepisování: dnssec-keygen
    dnssec-signzone
- OpenDNSSEC
- Knot DNS
  - Automatické podepisování, nástroje
- PowerDNS

DNSSEC debugging

- dig, dnssec-verify, ldns-verify-zone
- DNSSEC validator plugin
- Online nástroje:
  - DNSViz (dnsviz.net)
  - DNSSEC analyzer (dnssec-debugger.verisignlabs.com)

Problémy s DNSSEC

- Složité nasazení, žádné „ultimate solution“
- Nelze snadno automatizovat, dokud nebude RFC pro mechanismus na výměnu DS záznamů
- Zátež pro DNS infrastrukturu
  - Jak resolvery, tak autoritativní servery
- Možný „únik“ dat (NSEC)
- Značné zvětšení DNS odpovědí
  - Zjednodušuje amplification útoky

Response Policy Zones

Response Policy Zone - RPZ

- Speciální zónový soubor
- Zatím není standardizováno
- Plná podpora jen v DNS serveru BIND
- DNS firewall
  - Narušuje DNSSEC

RPZ – Typy záznamů

Návratová hodnota	typ	syntaxe	příklad
NXDOMAIN	CNAME	.	`example.org CNAME .`
NODATA	CNAME	.*	`example.org CNAME .*`
Nezměněno	CNAME	rpz-passthru.	`example.org CNAME rpz-passthu.`
Zahozeno	CNAME	rpz-drop.	`example.org CNAME rpz-drop.`
Vynucení TCP	CNAME	rpz-tcp-only.	`example.org CNAME rpz-tcp-only.`
změna	jakýkoliv	Cílová data	`example.org CNAME www.example.net.`
wildcard	CNAME	*.cíl	`example.org CNAME *.example.net`

RPZ - příklad

```
$ORIGIN rpz.example.org
skoleni.dns53.cz          CNAME    *.
*.skoleni.dns53.cz        CNAME    .
mail.dns53.cz             CNAME    rpz-passthru.
spam.dns53.cz             CNAME    rpz-drop.
abuse.dns.cz              CNAME    rpz-tcp-only.
www.dns53.cz              A        217.31.192.130
*.dns53.cz                CNAME    *.example.net
```

RPZ - aktivace

```
options {
    response-policy {
        zone: “rpz.example.org“;
    };
}
```

Co se jinam nevešlo

Nameservery (optimalizace)

- Špatně

```
;; ANSWER SECTION:
dns53.cz.          3600    IN   NS   ns.udp53.com.
dns53.cz.          3600    IN   NS   ns.udp53.net.
dns53.cz.          3600    IN   NS   ns.dns53.cz.

;; ADDITIONAL SECTION:
ns.dns53.cz.       1800    IN   A    192.168.1.3
```

Nameservery (optimalizace)

- Dobře

```
;; ANSWER SECTION:
dns53.cz.          3600    IN   NS   a.ns.dns53.cz.
dns53.cz.          3600    IN   NS   c.ns.dns53.cz.
dns53.cz.          3600    IN   NS   b.ns.dns53.cz.

;; ADDITIONAL SECTION:
a.ns.dns53.cz.     1800    IN   A    192.168.1.1
c.ns.dns53.cz.     1800    IN   A    192.168.1.2
b.ns.dns53.cz.     1800    IN   A    192.168.1.3
```

RRSet

- Sada RR záznamů se stejným
  - Vlastníkem, Třídou, Typem a TTL
  - Společný RRSIG

```
aspmx3.googlemail.com.   86400 IN A  209.85.222.4
aspmx3.googlemail.com.   86400 IN A  209.85.222.8
aspmx3.googlemail.com.   3600  IN A  209.85.222.1
aspmx3.googlemail.com.   86400 IN A  209.85.222.2
aspmx3.googlemail.com.   86400 IN A  209.85.222.7
aspmx3.googlemail.com.   86400 IN A  209.85.222.6
aspmx3.googlemail.com.   86400 IN A  209.85.222.5
aspmx3.googlemail.com.   86400 IN A  209.85.222.3
```

Reverse DNS lookup

- Zónu .arpa spravuje IANA
- in-addr.arpa (IPv4) a ip6.arpa (IPv6)
- Resolving přes DNS servery RIRů
- Zkuste pro info.nix.cz:

```
$ dig +trace -x 195.47.235.3
```

Reverse DNS lookup

```
$ dig +trace -x 195.47.235.3
...
195.in-addr.arpa.  86400   IN  NS  SEC3.APNIC.NET.
195.in-addr.arpa.  86400   IN  NS  SUNIC.SUNET.SE.
195.in-addr.arpa.  86400   IN  NS  SNS-PB.ISC.ORG.
195.in-addr.arpa.  86400   IN  NS  SEC1.APNIC.NET.
195.in-addr.arpa.  86400   IN  NS  NS-PRI.RIPE.NET.
195.in-addr.arpa.  86400   IN  NS  TINNIE.ARIN.NET.
195.in-addr.arpa.  86400   IN  NS  NS3.NIC.FR.
;; Received 222 bytes from 128.8.10.90#53(d.root-servers.net) in 110 ms

235.47.195.in-addr.arpa. 172800  IN  NS  info.nix.cz.
235.47.195.in-addr.arpa. 172800  IN  NS  ns1.nixcz.org.
235.47.195.in-addr.arpa. 172800  IN  NS  ns2.ignum.cz.
;; Received 119 bytes from 2001:500:13::c7d4:35#53(TINNIE.ARIN.NET) in
112 ms

3.235.47.195.in-addr.arpa. 21600 IN  PTR info.nix.cz.
235.47.195.in-addr.arpa. 21600   IN  NS  ns1.nixcz.org.
235.47.195.in-addr.arpa. 21600   IN  NS  ns2.ignum.cz.
235.47.195.in-addr.arpa. 21600   IN  NS  info.nix.cz.
;; Received 133 bytes from 2a02:38::1001#53(info.nix.cz) in 1 ms
```

Rotace SERIAL čísla

- Popsáno v RFC1912 sekce 3.1
- Pokud uděláte chybu a číslo zvednete moc
  - 2110061500 místo 2010061500
  - Přechod od YYYYMMDDNN na UNIXTIME

Rotace SERIAL čísla

- Postup
  - Přičtěte max. 2147483647
  - Pokud je větší než 4294967296, odečtěte 4294967296
  - Nechte stáhnout všechny(!) slave servery
  - Změňte na požadovanou hodnotu

IDN

- Internationalized Domain Names
  - Národní znaky v doménových jménech
- Speciální kódování PunyCode
- Doména začíná na xn--
  - háčkyčárky.cz → xn--hkyrky-ptac70bc.cz
- Velmi užitečné pro země nepíšící latinkou!
- Zároveň bezpečnostní problém
  - apple.com vs. apple.com

Knot DNS + DDNS

Knot DNS

- Autoritativní DNS server
- Open source – vývoj v CZ.NIC Labs
- Výkonný, stále odpovídá – bez zámků
- Master / slave – velké zóny, mnoho zón
- Transfery – AXFR, IXFR
- EDNS0, TSIG, DDNS
- Automatický DNSSEC

Významná nasazení Knot DNS

- RIPE NCC – 77 TLD
- .cz, .dk, .fr, .ca, .nl
- CZ.NIC
- forpsi.cz
- gigaserver.cz

Hlavní části Knot DNS

- Serverová část – **knotd**
- Ovládací nástroj – **knotc**
  - lokální i vzdálená správa
- Konfigurační soubor – **/etc/knot/knot.conf**
- Úložný adresář – **/var/lib/knot/**
  - zónové a pomocné soubory

Knot DNS – konfigurační soubor

- Důležité sekce:
  - **server**
  - keys
  - acl
  - **control**
  - **remote**
  - template
  - **zone**
  - log

sekce **server**

- Globální nastavení serveru:

  rundir: "/var/run/knot"

  - pracovní složka pro Knot – dočasné soubory

  [udp|tcp]-workers: 4

  - počet vláken k odpovídání

  background-workers: 4

  - počet vláken na obsluhu událostí (podepisování ...)

sekce key

- Klíče pro zabezpečení DDNS/transferů
- Formát:

```
key:
 - id: jmeno_klice
   algorithm:  hmac-sha256 | hmac-sha384 | hmac-sha512
   secret: BASE64
```

sekce control

- Nastavení komunikace mezi **knotc** a **knotd**
- Buď přes soket, nebo vzdáleně
- Pokud nenastavíme, lze ovládat jen přes signály
- V distribucích neměníme, **knotc** by měl fungovat
- Příklad:

```
control :
  listen: 1.2.3.4
  acl: acl_contol
```

sekce remote

- Vzdálené master/slave servery
- Příklad:

```
remote:
    - id: master
      address: 127.0.0.1@53531
      key: key0.server0;  # (optional)
      via: ipv4;  # (optional)
```

sekce zone

- Obsahuje globální nastavení pro zóny a výčet zón
- Důležitá nastavení:
  - **storage** – složka pro slave zóny, pro žurnál
  - **semantic-checks –** důkladnější kontrola zón
  - **serial-policy** – SOA increment/unixtime/dateserial
  - **dnssec-signing** – automatické DNSSEC podepisování

sekce zone

domain : z<NN>.lab.nic.cz.

file: "/var/lib/knot/z<NN>.lab.nic.cz"

… nastavení vlastností (přepíše globální)

dnssec-signing: off

master: [muj_master1, muj_master2]

notify: muj_slave1

1. příklad: Základní funkčnost

- Přidejte vaši zónu:

```
zone:
  - domain: z<NN>.lab.nic.cz
    file: "/var/lib/knot/z<NN>.lab.nic.cz"
```

- Spuštění serveru:

  systemctl start knot

  /etc/init.d/knot start

- Ověření chodu serveru:

  netstat -lptu

  knotc status

- Dotaz na server:

  dig @127.0.0.1 z<NN>.lab.nic.cz NS

- Status:
  - knotc status, knotc conf-check, knotc zone-status

Možnosti logování

- Umístění:
  - stdout/stderr – pouze pokud neběží jako démon
  - jakýkoliv soubor
  - syslog
- Závažnosti:
  - debug, info, notice, warning, error, critical
- Kategorie:
  - server, zone, control, any

2. příklad: Nastavení logování

- Upravit /etc/knot/knot.conf:

```
log:
    - target: syslog
      any: info
    - target: "/tmp/knot-server.log"
      server: info
```

- Restart serveru:

  /etc/init.d/knot stop

  /etc/init.d/knot start

- Ověření:

  cat /tmp/knot-server.log

3. příklad: Knot jako master a slave

Master: do /etc/knot/knot.conf přidat:

```
server:
   listen: 0.0.0.0@53
   listen: ::@53

remote:
 - id: soused_slave
   address: 10.0.0.<SS>

acl:
 - id: acl_soused_slave
   address: 10.0.0.<SS>
   action: transfer

zone:
 - domain: z<NN>.lab.nic.cz.
   file: "/var/lib/knot/z<NN>.lab.nic.cz"
   notify: soused_slave
   acl: acl_soused_slave
```

3. příklad: Knot jako master a slave

- Slave: do /etc/knot/knot.conf přidat:

```
remote:
 - id :soused_master
   address: soused_ip

acl:
 - id: acl_soused_master
   address: soused_ip
   action: notify
zone:
 - domain: z<SS>.lab.nic.cz.
   file: "/var/lib/knot/z<SS>.lab.nic.cz"
   master: soused_master
   acl: acl_soused_master
```

Generování změn pro IXFR

- Direktiva **zonefile-load: difference**
  - Lze zapnout pro všechny zóny nebo jednotlivě
- Workflow:
  - Ručně editovat zónový soubor
  - Změnit serial v SOA
  - knotc reload nebo knotc zone-reload [jméno zóny]
  - Transfer na slave

4. příklad: IXFR-out z lokálních změn

- Nastavit **zonefile-load: difference** v konfigu:

```
zone:
 - domain: z<NN>.lab.nic.cz.
   file: "...";
   zonefile-load: difference
    ...
```

- Udělat libovolnou změnu do zónového souboru
  - Přidat/odebrat RR, změnit RDATA, změna RRSIG
- **Zvýšit SOA serial** – jinak se nestane nic

4. příklad: IXFR-out z lokálních změn

- Reload serveru

  knotc reload

- Kontrola aktuálního serialu
  - V logu, digem, knotc zone-status
- Oveření, že slave má aktuální zónu
- Nebo ještě lépe:

  dig example.com. IXFR=201211240X @X.X.X.<NN>

5. příklad: Automatický DNSSEC

- Do konfigurace přidejte:

```
dnssec-signing: on
```

- knotc reload
- knotc zone-status

Dynamické updaty - DDNS

- RFC 2136
- Možnost, jak upravit **master** data jinak, než editací zónového souboru
- add/delete
- Prerekvizity
- Pokud je zapnutý DNSSEC, podepisuje online

5. příklad: Změna zóny s DDNS (1)

- Budeme používat nástroj **nsupdate**
- Do /etc/knot/knot.conf přidejte:

```
acl:
 - id: updates
   action: update

zone:
 - domain: z<NN>.lab.nic.cz.
   file: "/var/lib/knot/z<NN>lab.nic.cz"
   acl: [ soused_slave, updates ]
   notify: soused_slave
```

5. příklad: Změna zóny s DDNS (2)

- Spustit **nsupdate -v** (bez zabezpečení)

```
> server localhost
> zone z<NN>.lab.nic.cz.
> update add a.z<NN>.lab.nic.cz 3600 A 1.2.3.5
> show
> send
```

- Ověřit, že se update zdařil
  - digem (zkuste i +dnssec)
  - Kontrola logu

5. příklad: Změna zóny s DDNS (3)

- Spustit **nsupdate -v** (bez zabezpečení)

```
> server localhost
> zone z<NN>.lab.nic.cz.
> update delete nejaky_zaznam A
> show
> send
```

- Ověřit, že se update zdařil
  - dig:

    dig smazany_zaznam A @127.0.0.1

    dig z<NN>.lab.nic.cz SOA @127.0.0.1

Hodnocení

- Zanechte nám prosím zpětnou vazbu
- Odkaz na ploše

  nebo
- http://bit.ly/akademie-hodnoceni

Děkuji za pozornost

Petr Špaček • **petr.spacek@nic.cz**
Petr Černohouz • **petr.cernohouz@qtm.cz**