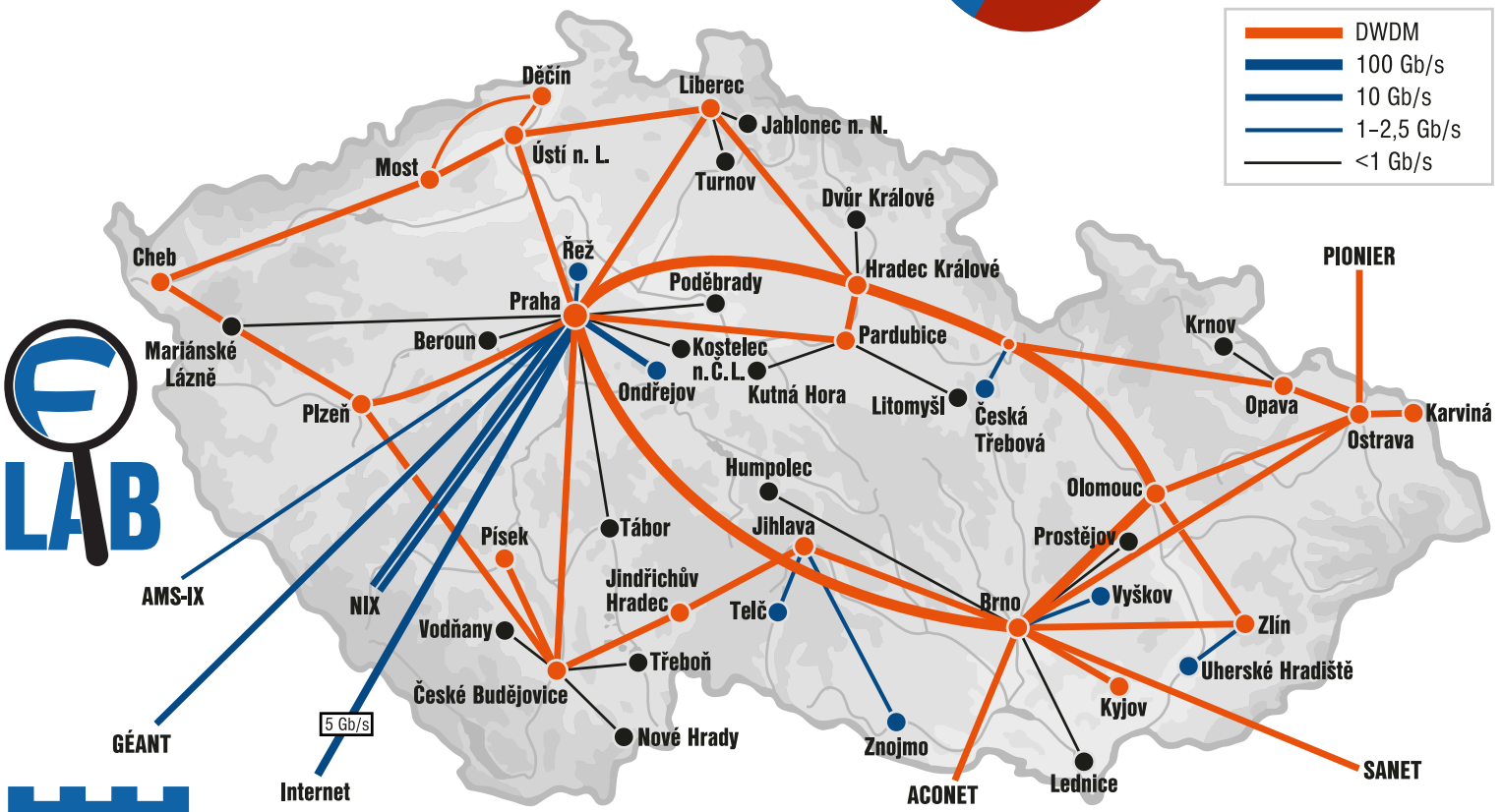
DNS, jak ho (možná) neznáte

Ondřej Caletka

11. listopadu 2014

Uvedené dílo podléhá licenci Creative Commons Uveďte autora 3.0 Česko.

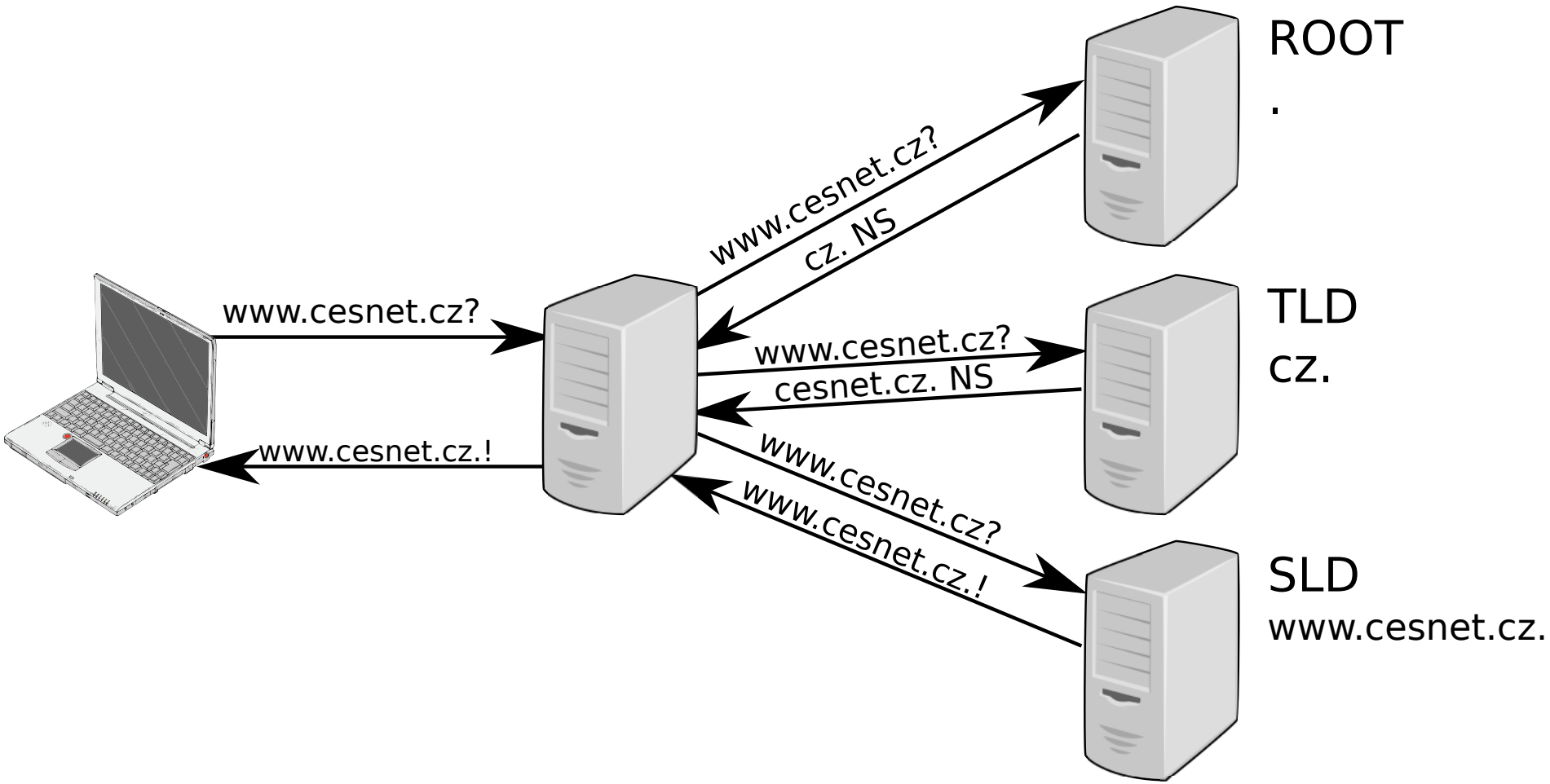
O sdružení CESNET



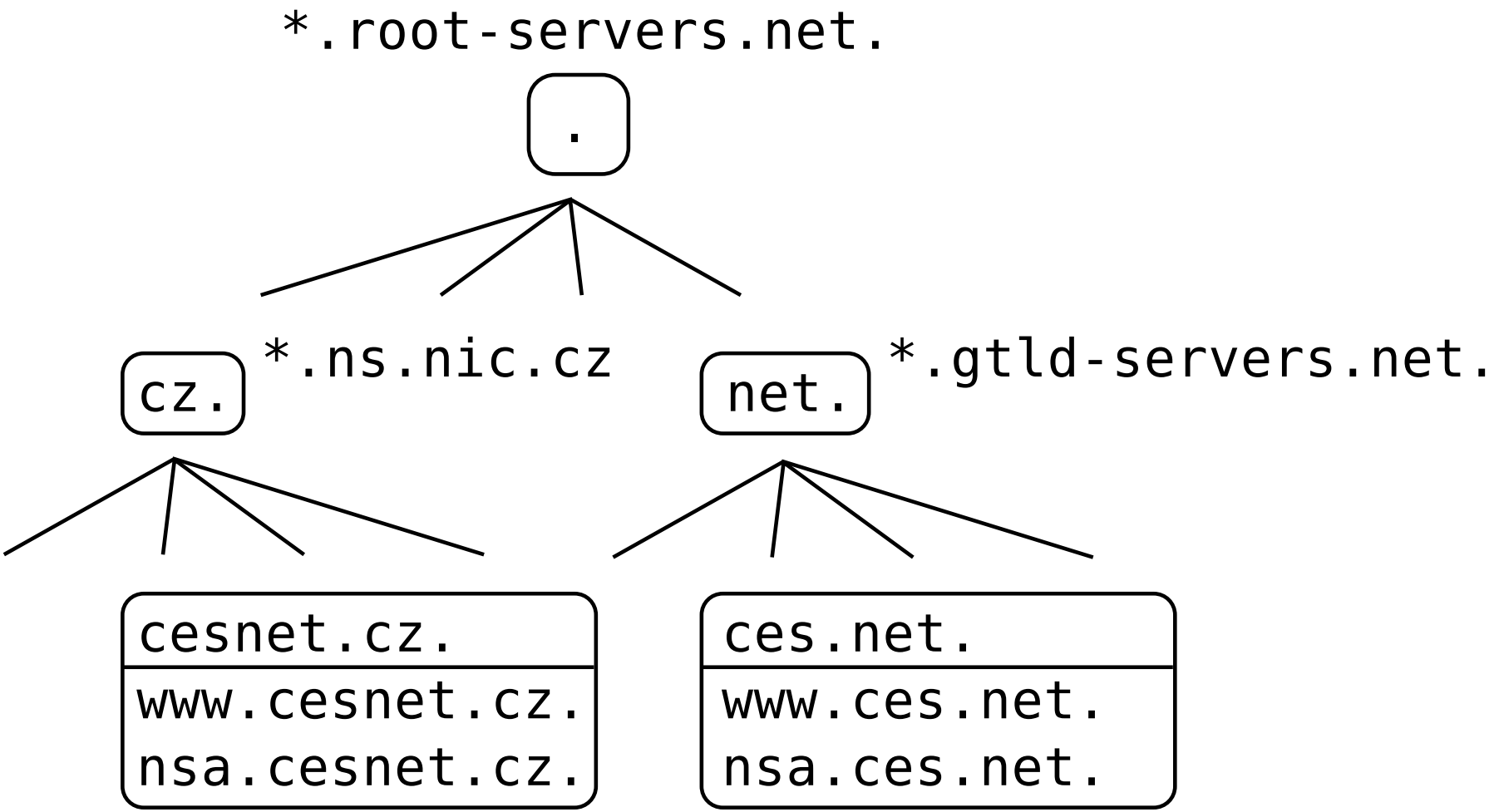
Obsah

1. Letem světem DNS
2. DNSSEC jako bezpečné uložiště
3. Dynamické DNS
4. Passive DNS

O službě DNS


ROOT
.
TLD
cz.
SLD
www.cesnet.cz.
www.cesnet.cz?
cz. NS
www.cesnet.cz?
www.cesnet.cz?
cesnet.cz. NS
www.cesnet.cz?
www.cesnet.cz.!
www.cesnet.cz.!
stub resolver
rekurzivní resolver
autoritativní server

Hierarchická struktura DNS zón



Pojmy z DNS

zóna Část globální databáze, samostatně spravovaná
Např.: zóna `cz.` spravovaná CZ.NIC

autoritativní server Server poskytující odpovědi ze zón, které drží
Např.: `a.ns.nic.cz.`

rekurzivní server/resolver Server, který dokáže postupnými dotazy zjistit odpověď na libovolný DNS dotaz
Např.: Google Public DNS `8.8.8.8`

stub resolver Knihovní funkce, tvoří rozhraní mezi aplikací a rekurzivním serverem
Např.: glibc

DNS zpráva

- Binární formát
- Společné záhlaví
  - ID transakce
  - Stavový kód
  - Příznaky

`AA`	Authoritative Answer
`RD`	Recursion Desired
`RA`	Recursion Available
`TC`	TrunCated message

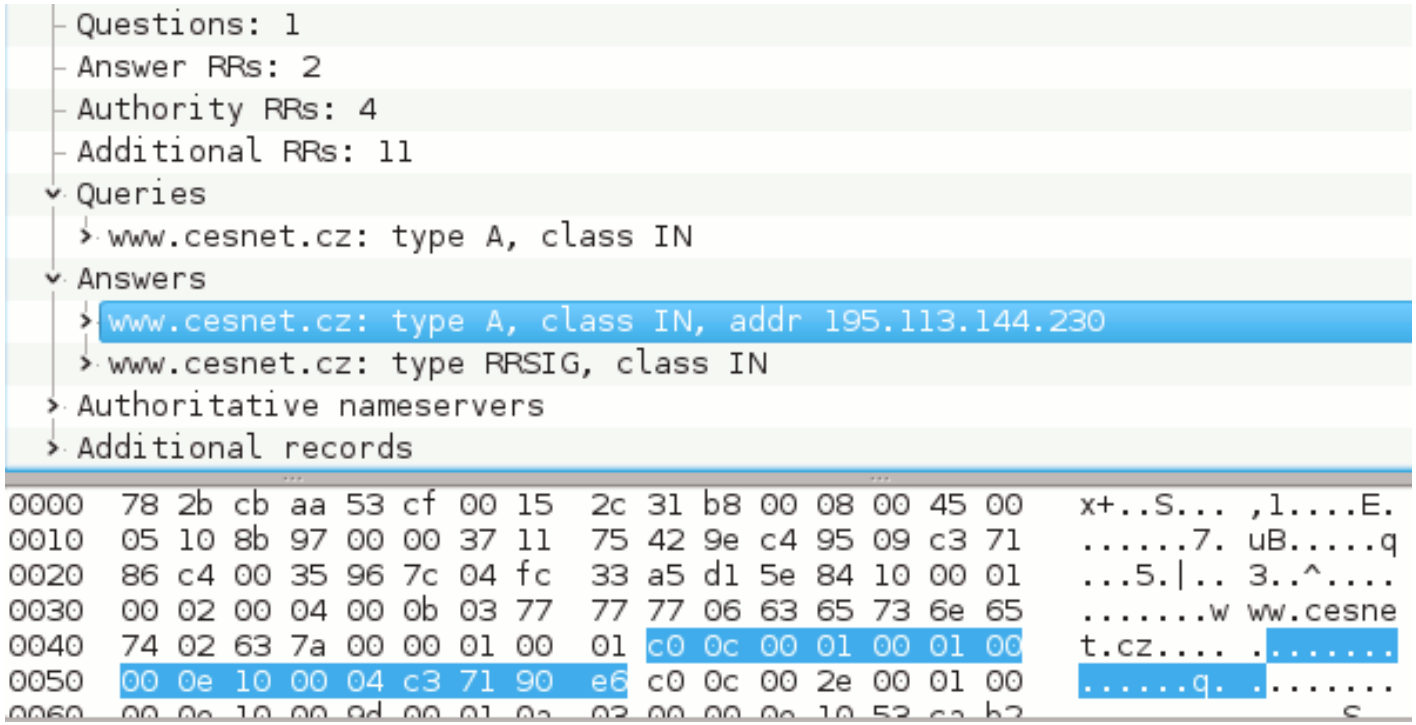
- Čtyři sekce s *resource records*

`QUERY`	dotaz
`ANSWER`	konečná odpověď
`AUTHORITY`	odkaz (referral)
`ADDITIONAL`	doplňující informace

DNS Resource Record

- Udržován v cache po dobu TTL
- Názvy domén jako spojový seznam *labels*
- Komprese opakujících se názvů

```
www.cesnet.cz. 3600 IN A 195.113.144.230
```



Typy záznamů

A	IPv4 adresa
AAAA	IPv6 adresa
PTR	Reverzní záznam Adresa se převrátí a připojí pod strom `in-addr.arpa.`, nebo `ip6.arpa.`
MX	Mail eXchange - SMTP server
CNAME	Canonical Name - alias Nelze kombinovat s jiným typem RR pro stejné jméno. Neměl by se řetězit.
SRV	Hledání služeb (SIP, XMPP, atd.)
SSHFP	SSH finger print
TLSA	TLS certifikát (DANE)

EDNS0

- Historický limit UDP DNS paketu 512 B
- Později přidána rozšiřující hlavička jako záznam typu `EDNS0` v poli `ADDITIONAL`
  - Inzeruje podporovanou délku UDP paketu (např. 4096 B)
  - Obsahuje další příznak `DO` -- DNSSEC OK
- Větší UDP zpráva šetří používání TCP, zhoršuje ale následky zesilujících útoků
- EDNS0 může další volby:
  - Informaci o klienské podsíti (problém CDN vs. 8.8.8.8)
  - Informaci o podporovaných DNSSEC algoritmech

DNSSEC

- Rozšíření zajišťující autenticitu DNS dat
- Využívá princip elektronického podpisu
- Nepoužívá PKI model, důvěra je delegována hierarchicky
- Validaci provádějí obvykle rekurzivní resolvery
- K validaci je potřeba nakonfigurovat pevný bod důvěry (obvykle otisk klíče kořenové zóny)

Reverzní delegace

Adresa se převrátí (IPv4 po oktetech, IPv6 po nibblech) a připojí pod strom `in-addr.arpa.`, nebo `ip6.arpa.`

IPv4

```
server.example.com.      IN A   192.0.2.1
1.2.0.192.in-addr.arpa.  IN PTR server.example.com.
```

IPv6

```
server.example.com.      IN AAAA 2001:db8:123:456::1
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.\
6.5.4.0.3.2.1.0.8.b.d.0.1.0.0.2.ip6.arpa.
                         IN PTR server.example.com.
```

Delegace a subdelegace

- Způsob, jak je sestaven DNS strom
- Nadřazená zóna obsahuje NS záznam s adresou serveru s zónou nižší úrovně
  Např.: `cz. IN NS a.ns.nic.cz.`
- Pokud server pro zónu leží uvnitř stejné zóny, je třeba navíc GLUE záznam
  Např.: `a.ns.nic.cz. IN A 194.0.12.1`
- Tyto informace se použijí pouze pro prvotní nasměrování (*priming*). Po spojení s delegovaným serverem jsou v cache přepsány informacemi z cílové zóny.
- Záznamy patřící do subdelegace DNS server ignoruje

Subdelegace – příklad

```
$ORIGIN example.cz
$TTL    3600
@         IN  SOA  …
          IN  NS   ns1         ; toto není delegace
ns1       IN  A    192.0.2.1


sub       IN  NS   ns.sub      ; toto je delegace
          IN  NS   server.nekde.cz.
; GLUE záznam - nutný
ns.sub    IN  A    192.0.2.2
; nonsens - out-of-zone data
server.nekde.cz. IN A 192.0.2.3
; nonsens -  data v delegované zóně, která nejsou GLUE
server.sub IN A    192.0.2.4
```

Reverzní classless delegace

Problém: Rozsahy IPv4 adres jsou menší, než celá třída.

Zóna 2.0.192.in-addr.arpa.

```
128/25  IN NS server.example.com.
        IN NS secondary.example.com.
128     IN CNAME 128.128/25
129     IN CNAME 129.128/25
…
255     IN CNAME 255.128/25
```

Zóna 128/25.2.0.192.in-addr.arpa

```
129     IN PTR server.example.com
```

Zónové přenosy

- Synchronizace autoritativních serverů
- Slave servery periodicky dotazují SOA master serveru
- Došlo-li ke zvýšení sériového čísla, požádají pomocí TCP o záznam typu AXFR, nebo IXFR
- Master server odpoví kompletním obsahem zóny (AXFR), nebo změnou proti předchozímu sériovému číslu (IXFR)
- Není-li master dlouho dostupný, zóna expiruje
- Master může upozornit slave servery zprávou NOTIFY

Zabezpečení přenosu pomocí TSIG

- Zabezpečení DNS dotazu elektronickým podpisem
- Využívá sdílené tajemství a algoritmus HMAC
- Lze použít např. místo omezování IP adres pro zónové přenosy

Vygenerování sdíleného tajemství

```
$ openssl rand -base64 32
UKoj75Qy5BOGbOKxRDJhtKRQkdYXmrsIPcdy2nBchJI=
```

Časování a synchronizace

- odpovědi serverů kešovány po TTL daného záznamu
- negativní odpovědi kešovány podle hodnoty `SOA minimum`
- nesynchronnost serverů vede ke *split-brain*:
  o odpovědi rozhoduje náhoda

Za jak dlouho se změna nejpozději projeví?

	s `NOTIFY`	bez `NOTIFY`
nový záznam	`SOA minimum`	`SOA minimum + SOA refresh`
změna	`TTL starého`	`TTL starého + SOA refresh`

DNSSEC jako bezpečné uložiště

SSHFP záznamy

Umístění otisku serverového klíče do DNS

vygenerování klíče

```
$ ssh-keygen -r server
server IN SSHFP 1 1 b2…16
server IN SSHFP 1 2 e9…a307881a26da5961f41ef41ccc
server IN SSHFP 2 1 6c…57
server IN SSHFP 2 2 1e…44963ffbf82b1c028d365b859e
server IN SSHFP 3 1 3f…a3
server IN SSHFP 3 2 a9…9d7dd752bea56ff505281c7ed1
```

validace

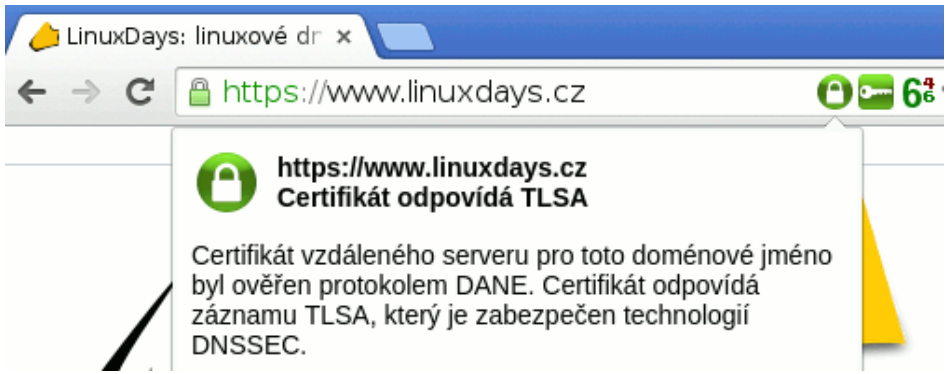
```
$ echo "VerifyHostKeyDNS yes" >> ~/.ssh/config
```

http://www.root.cz/clanky/dnssec-jako-bezpecne-uloziste-ssh-klicu/

CESNET

TLSA záznamy (DANE)

- generujte pomocí utility swede
- zvolte usage podle vašeho vztahu s CA:
  - 0 připíchnutí CA
  - 1 připíchnutí koncového certifikátu
  - 2 vložení nové CA
  - 3 vložení koncového certifikátu bez ohledu na PKI
- pro free DV certifikáty se nejvíc hodí typ 3



http://www.root.cz/clanky/pripichnete-si-ssl-certifikat-k-domene/

Dynamické DNS

Dynamické IPv6 záznamy

- Běžná praxe v IPv4 spočívá ve vygenerování všech možných DNS záznamů
- Pro IPv6 nemožné, soubor pro jednu podsíť /64 by zabíral stovky EiB (2^{60})
- Řešením je dynamické generování, podporované v Knot DNS 1.5+

Příklad

```
example.cz {
    file "/etc/knot/empty.zone";
    query_module {
        synth_record "forward dyn- 60 2001:db8:1::/64";
        synth_record "forward dyn- 60 192.0.2.0/24";
    }
}
```

Dynamické DNS

- Tradiční DNS servery načítají zónový soubor
- Změna dat vyžaduje změnu zónového souboru a reload serveru
- Dynamické DNS je rozšíření DNS protokolu o možnost aktualizace dat
- Server změny aplikuje automaticky a zvyšuje sériové číslo
- Po zapnutí DDNS není již nadále možné editovat zónové soubory

Zprovoznění DDNS

1. Nastavíme TSIG klíč
2. Povolíme dynamické aktualizace
3. Aktualizujeme utilitou nsupdate

Příklad nsupdate

```
> server n72.nebula.cesnet.cz
> update delete test.example.com.
> update add test.example.com. 60 IN TXT "test"
> send
```

Nsdiff

- Nevýhodou DDNS je ztráta formátování a komentářů ve zdrojových souborech
- Není možné kombinovat DDNS a editaci zónového souboru na jedné zóně
- Možným řešením je utilita `nsdiff`. Ta porovná starou zónu s novou a vygeneruje skript pro `nsupdate`, který změny aplikuje

```
$ nsdiff example.com example.com.zone | nsupdate
```

Passive DNS

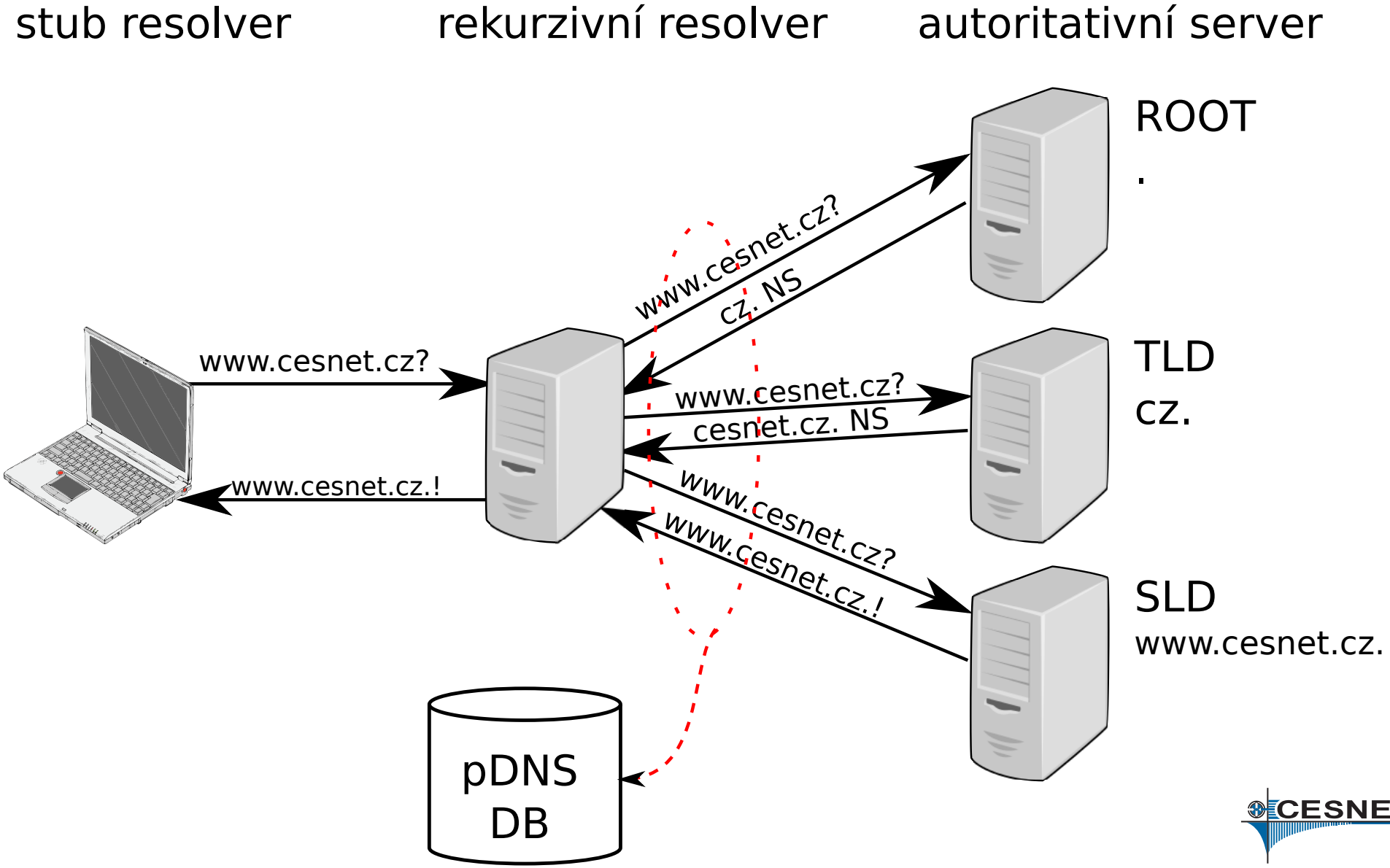
Myšlenka passive DNS

- sbírat veřejná DNS data na rekurzivních DNS serverech
- zjišťovat, na co se lidé ptají
- nezjišťovat, kdo se ptá (ochrana soukromí)
- ukládat do databáze spolu s časovou značkou
- získat tak informace o **historii DNS dat**
- mít možnost pokládat **inverzní DNS dotazy**

Dva přístupy k passive DNS

1. zachytávání před rekurzivním serverem
   - zaznamenávání každé uživatelské aktivity
   - přesné sledování četnosti dotazů
2. zachytávání za rekurzivním serverem
   - menší objem dat díky cache
   - implicitní ochrana soukromí

Passive DNS za rekurzivním serverem

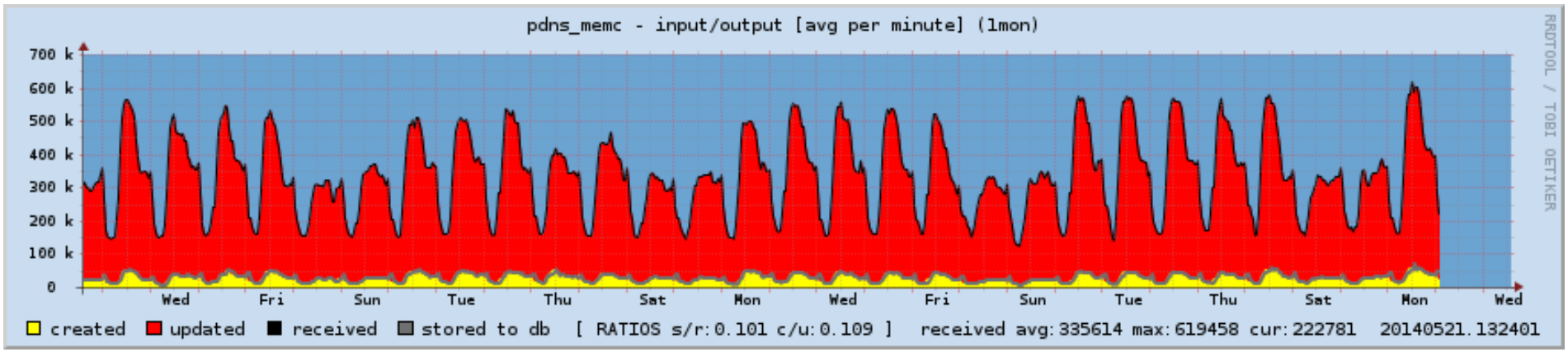


Technické provedení

- senzor sbírá DNS provoz pomocí PCAP knihovny v blízkosti DNS serveru
- je možné jej buď spustit na stejném stroji jako DNS server, nebo klonovat data switchi
- data se zapisují do binárních souborů po minutách
- soubory jsou posílány pomocí SCP do databáze

Databáze pDNS

1. ISC/Farsight DNSDB.info
2. BFK
3. CERT.at
   - založeno na PosgreSQL
   - miliarda položek v databázi
   - 100 GB RAM, data na SSD discích



Webové rozhraní pDNS@CERT.at

CERT.at / ACOnet
DNS History

www.google.at | Go | Reset [X]

Format: Whois csv HTML
Options: Sensor info Exact domain
List only: NXDOMAIN A NS CNAME SOA PTR MX TXT AAAA
First seen: >= <=
Last seen: >= <=
Sort: desc , desc , desc

```
% CERT.at / ACOnet DNS replicator WHOIS server, version 2.0.
% (C) 2011 All rights reserved.
% Authors: L. Aaron Kaplan <kaplan AT cert.at>
%          Achim Adam      <achim.adam AT univie.ac.at>
%
% 419 elements, 0.1437s
```

LEFT	RTYPE	RIGHT	FIRST-SEEN	LAST-SEEN	COUNT-SEEN
www.google.at	A	74.125.232.223	2012-09-21 06:05:39	2012-09-21 06:05:39	48
www.google.at	A	74.125.232.215	2012-09-21 06:05:39	2012-09-21 06:05:39	48
www.google.at	A	74.125.232.216	2012-09-21 06:05:39	2012-09-21 06:05:39	48
www.google.at	A	74.125.232.248	2012-09-21 12:39:39	2012-09-21 12:39:39	349
www.google.at	A	74.125.232.247	2012-09-21 12:39:39	2012-09-21 12:39:39	349
www.google.at	A	209.85.148.94	2012-09-11 17:27:31	2012-09-27 11:11:29	5
www.google.at	A	74.125.135.94	2012-09-10 13:06:35	2012-10-17 18:16:55	5
www.google.at	A	74.125.232.56	2012-11-22 18:40:04	2012-11-22 18:40:04	2
www.google.at	A	74.125.232.55	2012-11-22 18:40:04	2012-11-22 18:40:04	2
www.google.at	A	74.125.232.63	2012-11-22 18:40:04	2012-11-22 18:40:04	2
www.google.at	A	74.125.227.56	2012-11-22 18:40:31	2012-11-22 18:40:31	1
www.google.at	A	74.125.227.63	2012-11-22 18:40:31	2012-11-22 18:40:31	1
www.google.at	A	74.125.227.55	2012-11-22 18:40:31	2012-11-22 18:40:31	1
www.google.at	A	74.125.129.94	2012-11-22 18:40:36	2012-11-22 18:40:36	1
www.google.at	A	74.125.224.120	2012-11-22 18:40:41	2012-11-22 18:40:41	1
www.google.at	A	74.125.224.119	2012-11-22 18:40:41	2012-11-22 18:40:41	1
www.google.at	A	74.125.224.127	2012-11-22 18:40:41	2012-11-22 18:40:41	1
www.google.at	A	74.125.230.215	2012-10-23 08:26:04	2012-11-28 11:41:30	3
www.google.at	A	74.125.230.216	2012-10-23 08:26:04	2012-11-28 11:41:30	3
www.google.at	A	74.125.230.223	2012-10-23 08:26:04	2012-11-28 11:41:30	3

CESNET

Příklady použití

- odhalení řídicích serverů botnetů, ve spolupráci s NetFlow také odhalení infikovaných stanic
- odpověď na otázky:
  - jde o zneužití legitimní služby, nebo o cílený hosting škodlivého obsahu?
  - jaké další weby jsou hostovány na stejné IP adrese?
- kontrola neoprávněného využití adresního prostoru (například sítě CESNET2)
- výzkum nad globálními DNS daty
  - které domény jsou hostovány pouze na území jednoho státu?
  - jak často se mění data v různých doménách?

Konec

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
http://Ondřej.Caletka.cz

CESNET