DNS

Proč DNS

- IP adresy
  - Špatně se pamatují
  - Identifikují „počítač" a nikoli službu
  - Malá výpovědní hodnota
  - Nízká flexibilita při změnách
  - Mapování pouze 1:1
    - Chybí obecnost
  - Mapování jmne na číselné adresy
    - ARPANET (RFC606)
  - Centrální autorita
    - Soubor HOSTS (dodnes: /etc/hosts)
    - Všechny aktualizace se musí dít centrálně
    - Žádná škálovatelsnost
    - Distribuce z jednoho místa
    - Malý počet jmen (tehdy)
    - Malá frekvence změn (tehdy)

Princip DNS

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 (Resource Record)
- Zóna
- Zónový soubor
- Jmenný server / Name server

Doménové jméno

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

Zóna

- Ščást hierarchie
- Samostatný správce
- Oddělená na úrovni teček v doménovém jménu
- Delegovaná výe v nadřazené zóně (kromě '.')

Resource Record

RR (Resource Record) zázanm

- 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
- Textový formát
  - RFC 1035

Name server

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

Autoritativní a rekurzivní DNS server

DNS servery a resolvery

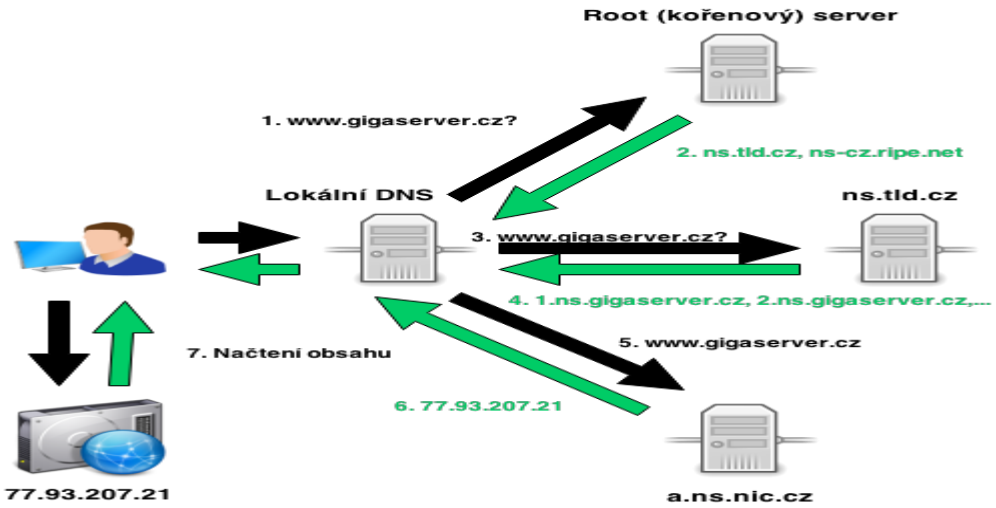
- Architektura klient/server
- Klient – rekurzivní name server – resolver
- Server – autoritativní name server
- Komunikace pomocí DNS zpráv

- Resolver se může ptát dalších resolverů
- Vyrovnávací paměť (cache) na resolveru
    - Délka (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) servery
    - Také autoritativní
    - Data jsou získávána z master serveru
    - Může jich být více
    - Hierarchie (master – slave – slave …. Slave)

DNS dotazování



DNS dotazování – pokr.

- 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) – NS(nic.cz)
    - 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
    - Není oitřeba se stále ptát root serverů

DNS dotazování - Stub resolver

- Stub resolver
    - DNS klient v každém počítači
    - Implemtován v systémových knihovnách
    - Malý, jednoduchý
    - Může, ale nemusí, implementovat cache
- Prohlížeče mají svou cache
    - S DNS nemá nic společné

Autorativní vs. Neautorativní

- Autorativní odpověď
    - Od autorativního nameserveru
    - Dotaz na doménu, pro kterou má server zónu
- Neautorativní odpověd
    - Od resolveru
- Příznak v DNS zprávě
    - AA bit

Typy záznamů v DNS

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

Resource Record záznamy – RDATA

RR záznam – RDATA

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

Typy záznamů

RR záznam – typy záznamů

Typ	Anglický název	Význam pole RDATA
SOA	Start of Authority	Údaje o zóně (více položek)
NS	Name Server	Doménové jména autorativních nameserverů
A	A host address	IPv4 adresa (jména – IP adresa)
AAAA	IPv6 host address	IPv6 adresa (jména – IP adresa)
CNAME	Canonical Name	„Alias" (*jméno -*jiné_jmeno)
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 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 – pokr-

```
Udp53.cz.       600     IN      SOA     ns.udp53.cz.    hostmaster.udp53.cz.  (
2008101420      ; seriál
10800           ;refresh  (3 hourse)
3600            ;retry  (1 hour)
1209600         ;expire (2 weeks)
7200            ; minimum (2 hourse)
)
```

- MNAME nemusí existovat
- RNAME bez zavináče (první tečka – '@')
- Seriál (YYYYMMDDNN) nebo (Unixtime)
- Retry kratší než Refresh
- Expirace 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 bitú)
  - 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.Nnic.cz
  Mail.udp53.cz.  3600  IN  A       127.0.0.1
  ```

CNAME záznam

- Další jméno, Alias

  ```
  www2.udp53.cz.  600  IN  CNAME   ww.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.
- Všechna RR pod upd53.cz jsou dostupné přes www.udp53.cz

CNAME záznam pokr.

CNAME záznam

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

~~www.udp53.cz. 600 IN CNAME 127.0.0.1.~~
~~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/nameserver dále zpracovává výsledek
  - Může dojít k dalším dotazům

TXT záznam

- Obecné 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
  1.0.0.128.in-addr.arpa. IN PTR udp53.cz
  1.0.0 .. 0.0.0.ip6.arpa. IN PTR upd53.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:
  Udp53.cz 3600 IN TYPE65534 \#5 0883550001