

Jednoduchý DNS server

Petr Nohejl (xnohej00)

24. 4. 2010

Abstrakt

Projekt se zabývá návrhem a implementací jednoduchého DNS serveru pro operační systém GNU/Linux v jazyce C++. Server umí zpracovávat neblokujícím a konkurentním způsobem standardní dotazy typu A a PTR. Server se nastavuje v konfiguračním souboru, který je na vstupu programu. V tomto souboru jsou rovněž uloženy DNS záznamy. Veškeré přístupy na server jsou zaznamenávány do logovacího souboru.

Klíčová slova

DNS server, BSD sockets, konkurentní server, neblokující server, C++.

1. Úvod

V první části dokumentace si krátce popíšeme systém DNS, typy DNS záznamů a strukturu paketu DNS Query. V druhé části je popsán samotný návrh a implementace jednoduchého DNS serveru. Dále je nastíněno testování serveru pomocí klienta. V závěru jsou shrnuty získané dovednosti a zhodnocení projektu.

2. DNS

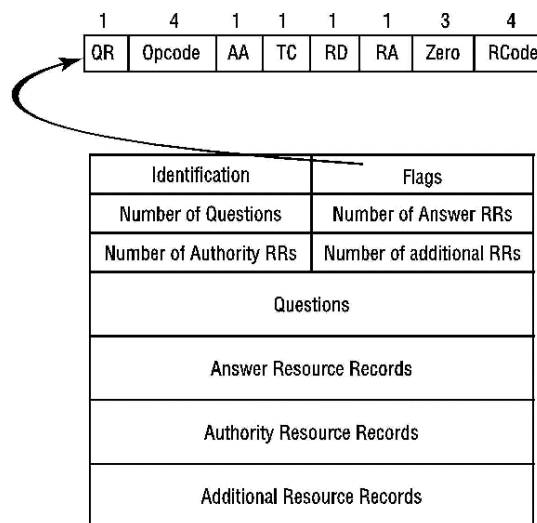
DNS (Domain Name System) je hierarchický systém doménových jmen, který je realizován DNS servery a protokolem DNS, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě. [1]

2.1 Protokol DNS

Protokol DNS pracuje způsobem dotaz – odpověď. Klient pošle dotaz serveru a server na dotaz odpoví. Nejčastější používanou operací je DNS QUERY. Jedná se o dotaz vedoucí k získání vět RR z DNS databáze. Protokol používá porty TCP/53 i UDP/53, je definován v RFC1035. U dotazů typu DNS QUERY se používá protokol UDP. Pokud je odpověď delší než 512B, vloží se do odpovědi pouze část informací a nastaví se příznak TC (Truncated). Klient si pak může kompletní odpověď vyžádat protokolem TCP. Servery DNS jsou organizovány hierarchicky, stejně jako jsou hierarchicky tvořeny názvy domén. Jména domén umožňují lepší orientaci lidem, adresy pro stroje jsou však vyjádřeny pomocí IP adres – A záznam. Systém DNS umožňuje efektivně udržovat decentralizované databáze doménových jmen a jejich překlad na IP adresy. Stejně tak zajišťuje zpětný překlad IP adresy na doménové jméno - PTR záznam. [1] [2]

2.2 Struktura paketu DNS Query

Strukturu paketu znázorňuje následující obrázek.



Obr. 1. Struktura paketu DNS Query [3]

2.3 Typy dotazů DNS Query

Základní typy dotazů DNS Query jsou popsány v následující tabulce.

Typ	Hodnota	Význam
A	1	Požadavek na získání IPv4
NS	2	Požadavek na získání autoritativních jmenných serverů
CNAME	5	Požadavek na získání věty CNAME (aliasy)
SOA	6	Požadavek na získání věty SOA
PTR	12	Požadavek na získání věty PTR (převod na doménové jméno)
MX	15	Požadavek na získání věty MX (pošta)
AAAA	28	Požadavek na získání IPv6

Tab 1. Základní typy dotazů DNS Query [2]

3. Jednoduchý DNS server

3.1 Popis programu

Cílem projektu bylo navrhnout a implementovat jednoduchý DNS server, který naslouchá na UDP portu. Název programu je 'mydns'. Server zpracovává DNS dotazy typu A a PTR neblokujícím a konkurentním způsobem. Na jedno doménové jméno může být více odpovědí. Ostatní typy dotazů nejsou implementovány. Překlad domén a adres funguje obousměrně (dotazy typu A a PTR). Veškeré přístupy na server jsou zaznamenávány do logovacího souboru 'accesslog'.

Nastavení serveru je uloženo v konfiguračním souboru, který je na vstupu programu. Konfigurace se načítá při spuštění serveru. Konfigurační soubor obsahuje seznam rozhraní a IP adres, na kterých bude server naslouchat. Číslo portu, na kterém bude naslouchat. Dále obsahuje DNS tabulku se záznamy (DNS název, IP, TTL) a výchozí hodnoty DNS názvu, IP, TTL. Pokud server nemá odpovídající odpověď na dotaz, odpoví výchozí IP adresou, resp. výchozím DNS názvem. Jednotlivá nastavení v konfiguračním souboru mohou být v různém pořadí. Přesný syntax konfiguračního souboru je popsán přímo v tomto souboru, který je přibalen k projektu (v komentářích).

3.2 Návrh programu

Po spuštění programu se zpracují argumenty a v případě korektního spuštění se zobrazí nápověda k programu, nebo se spustí samotný server. Nejprve se zpracuje konfigurační soubor a načtená data se uloží do proměnných objektu *Mydns*. Poté se zkontrolují všechna rozhraní z konfiguračního souboru a pro každé platné rozhraní či IP adresy se vytvoří vlastní soket na požadovaném portu. Server potom běží v nekonečném cyklu *while*, ve kterém se pomocí funkce *select()* kontrolují všechna rozhraní (sokety) a server čeká na zprávy od klientů. Tímto je zajištěn neblokující způsob zpracování zpráv (neblokují se systémové zdroje).

Po přijetí zprávy od klienta server vytvoří nový proces pomocí funkce *fork()*. Tímto je zajištěno konkurentní (paralelní) zpracování zprávy. V tomto novém procesu (potomku) se zpracuje DNS zpráva a odpověď se odešle zpět klientovi. Nakonec je potřeba nově vytvořený proces řádně ukončit. Hlavní proces serveru běží i nadále.

Přijatá zpráva je nejprve rozkódována. Server zkontroluje, jestli někde nenastala chyba a pokud je dotaz typu *Query* (standardní otázka) *A* nebo *PTR*, server vyhledá ze své databáze odpověď a odešle ji zpět klientovi. Pokud server nezná odpověď, odešle v odpovědi defaultní doménový název či IP. Pokud klient pošle jiný dotaz než *Standard Query* a jiný typ než *A* či *PTR*, server odpoví zprávou 'not implemented'. Pokud někde nastala chyba, server odpoví chybovou zprávou. Na jedno doménové jméno v dotazu typu *A* může být více odpovědí.

Server dále podporuje kompresi DNS dotazu pro snížení velikosti odesílané zprávy. Každé další výskyty doménového jména v zprávě nejsou odesílány celé, ale je na ně pouze ukazováno. Tím se celá zpráva zkrátí.

3.3 Implementace

Server je implementován v jazyce C++. Využívá knihovny BSD sockets a je určen pro operační systémy GNU/Linux. Celý program využívá objektově orientovaný návrh. Samotný server je implementován ve třídě *class Mydns*. Program dále používá knihovnu *pcrcpp* pro práci s regulárními výrazy, které jsou použity ve zpracování konfiguračního souboru a zpracování DNS zprávy.

3.4 Třída Mydns

Třída *Mydns* obsahuje tyto proměnné:

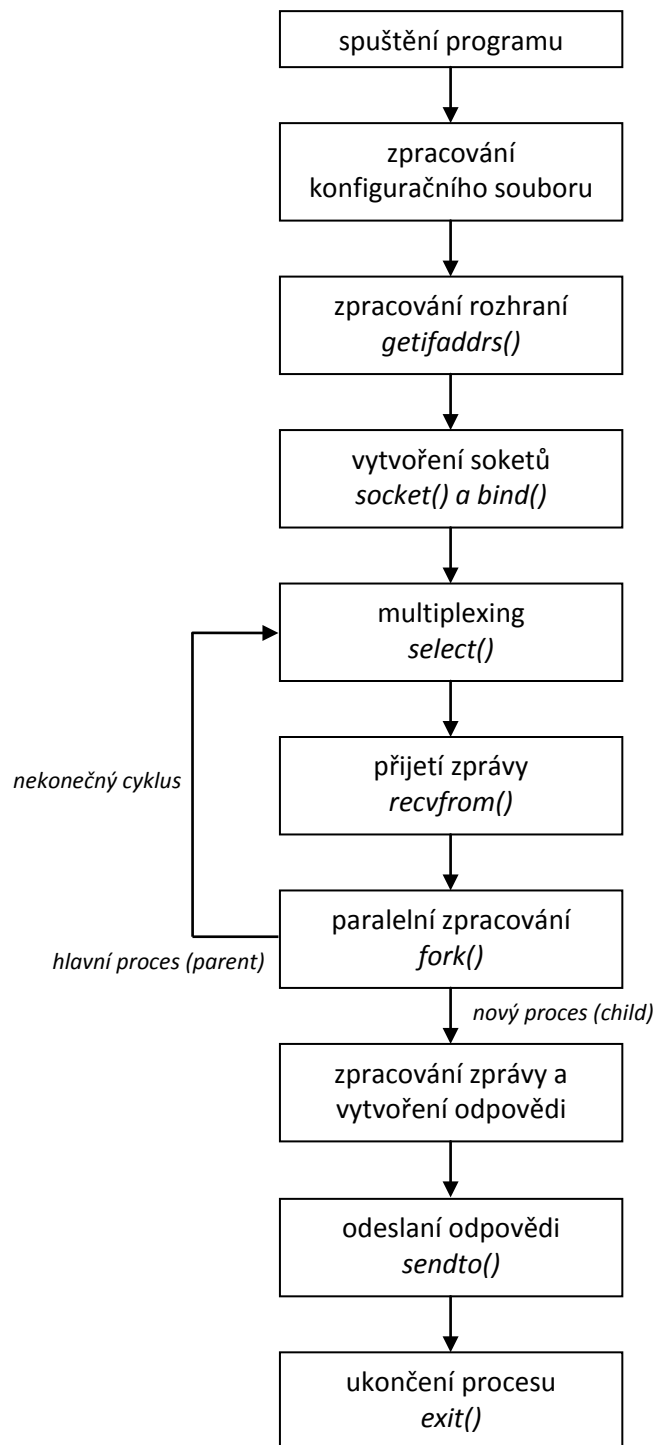
- `int confPort;` číslo portu
- `int confDefaultTTL;` výchozí TTL
- `string confDefaultIP;` výchozí IP
- `string confDefaultDomain;` výchozí doména
- `bool confInterfaceAny;` naslouchání na všech rozhraních
- `vector<string> confInterface;` seznam interfaces
- `vector<string> confInterfaceIP;` seznam IP adres
- `vector<string> confTableName;` DNS tabulka s doménovými jmény
- `vector<string> confTableIP;` DNS tabulka s IP adresami
- `vector<int> confTableTTL;` DNS tabulka s TTL
- `vector<int> sockets;` seznam soketů

Třída *Mydns* obsahuje tyto metody:

- `int help();` vypíše nápovědu
- `int dns();` spustí DNS server
- `int parseConf();` zpracuje konfigurační soubor
- `void parseInterface();` zpracuje seznam interfaces
- `string cutWhitespace();` ořeže bílé znaky v řetězci
- `string removeComment();` odstraní komentáře v konfiguračním souboru
- `int createSockets();` vytvoří sokety
- `int dnsQuery();` zpracuje DNS zprávu
- `void dnsCode();` dekóduje DNS zprávu

3.5 Blokové schéma aplikace

Následující obrázek znázorňuje blokové schéma serveru.



Obr. 2. Blokové schéma DNS serveru

3.6 Použití

Server se spouští z konzole OS GNU/Linux. Pomocí přepínače `-h` lze zobrazit nápovědu. Při spouštění serveru je nutné zadat název konfiguračního souboru (přepínač `-f`), ze kterého se načítají konfigurační data a DNS záznamy při startu serveru. Při změně konfiguračního souboru je nutné server restartovat. Příklady použití:

- `./mydns -f konfiguracni_soubor`
- `./mydns -h`

3.7 Testování

Projekt byl vyvíjen na operačním systému GNU/Linux (server merlin.fit.vutbr.cz). Pro testování projektu slouží testovací skript 'testuj', který zkompile, sestaví, spustí a testuje program MYDNS pomocí příkazů `dig`. Nakonec odstraní všechny vytvořené soubory a vrátí adresář s projektem do původního stavu. Pro testování byl použit Linuxový program `dig`, který zde slouží jako klient a zasílá DNS dotazy na náš server. Příklady použití programu `dig`:

- `dig -p 5729 @127.0.0.1 www.fit.vutbr.cz`
- `dig -p 5729 @127.0.0.1 -x 147.229.9.23`

4. Literatura

- [1] Domain Name System In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2010-04-25]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Domain_Name_System>.
- [2] DOSTÁLEK, Libor; KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. Brno : Computer Press, 2008. 488 s. ISBN 978-80-251-2236-5.
- [3] *Microsoft TechNet* [online]. 2010-04-25 [cit. 2010-04-25]. DNS Query packet. Dostupné z WWW: <http://technet.microsoft.com/en-us/library/Cc723704.socket02_big%28en-us,TechNet.10%29.gif>.