VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Počítačové komunikace a sítě

2. projekt – Varianta 3

DNS Lookup nástroj

Dokumentace

6. dubna 2018 Petr Marek

Obsah

1 Zadání

Cílem projektu bylo naprogramovat C/C++ nástroj, který se za pomoci síťové knihovny BSD sockets dotazuje systému DNS a realizuje překlad doménových jmen a IP adres.

2 Úvod do problematiky DNS

Jelikož počítače pracují na úrovni binárních dat, i přenos dat po síti musí probíhat touto cestou. Nicméně pro člověka je náročné zapamatovat si sekvenci několika číslic pro každou stránku, kterou chce navštívit. Těmto sekvencím se říká IP adresy a identifikují každé zařízení v internetu. Vznikla proto potřeba mapovat IP adresy na lehce zapamatovatelná doménová jména.

3 Historický podtext

Na základě informací z RFC 1034[1] jsem zjistil, že jedna z prních implementací doménového systému byla udržována v Network Information Centru (NIC) v jednom souboru HOSTS.TXT. Tento se FTP protokolem přenášel mezi všemi hosty. To působilo velkou zátěž na síti a to v době, kdy počet hostů velmi rychle rostl. Z tohoto důvodu a mnoha dalších vznikl DNS systém, jaký známe dnes.

4 Formát DNS zpráv

Všechna komunikace v rámci doménového protokolu je přenášena formou zpráv. Tyto zprávy jsou dle RFC 1035[2] děleny na pět hlavních částí: Header, Question, Answer, Authority a Additional. V překladu tedy Hlavička, Otázka, Odpověď, Autorita a Další. Header musí být vyplněn vždy. Pokud se dotazujeme DNS serveru, musí být navíc vyplněna část Question. Ve zprávě, kterou server odpovídá může být kromě Headeru vyplněno cokoliv dalšího kromě části Question.

4.1 Formát DNS Otázky

Otázka se skládá ze tří následujících částí:

QNAME sekvence návěští, kde každé návěští se skládá z čísla udávající počet následujících znaků. Doménové jméno se skládá ze sekvence těchto návěští a je ukončeno nulou značící návěští kořene. Tedy například doménové jméno *www.seznam.cz* je zapsáno jako *3www6seznam2cz0*.

QTYPE číselný kód specifikující typ otázky. Těchto typů je mnoho, nicméně zadání vyžaduje implemetovat jen následující:

- **A** IPv4 adresa hosta
- **AAAA** IPv6 adresa hosta[3]
- **NS** Jméno autoritativního serveru
- **PTR** Ukazatel na doménové jméno
- **CNAME** Kanonické jméno pro alias

QCLASS číselný kód specifikující třídu otázky. Dle zadání je třída vždy IN (Internet).

4.2 Formát DNS Odpovědi

Sekce Answer, Authority a Additional sdílejí stejný formát. Je to proměnný počet záznamů, jejichž počet je specifikován v sekci Header. Odpověď se skládá z:

NAME Doménové jméno

TYPE Typ dat RDATA

CLASS Třída dat RDATA

TTL Časový interval specifikující životnost zprávy

RDLENGTH Délka dat RDATA

RDATA Samotná data specifikovaná předchozími částmi

5 Způsob komprese zpráv

Za účelem snížení velikost zprávy doménový systém implentuje ukazatele, které zamezují zbytečnému opakování stejným doménových jmen ve zprávě[2]. Tento ukazatel má velikost dvou oktetů (osmibitové hodnoty). Od návěští se rozpozná tak, že má první dva bity jedničky. Návěští má velikost maximálně 63 oktetů, tedy musí začínat dvěma nulovými bity.

Komprese dovoluje DNS systému reprezentovat doménové jméno jako:

- sekvenci návěští končící nulovým oktetem
- ukazatel
- sekvenci návěští končící ukazatelem

6 Rekurzivní způsob dotazování

Při rekurzivním způsobu dotazování (tedy dotazování bez použití parametru -i) se odešle otázka (Query) serveru uvedenému v parametrech. Pokud tento server nezná odpověď, zeptá se na tento dotaz kořenovému serveru. Pokud ten odpověď nezná, zašle v odpovědi jméno autoritativního serveru nejvyšší úrovně a jeho adresu. Na tuto adresu opět původně dotázaný server zašle původní dotaz. Pokud ani tento server odpověď nezná, opět zašle jméno autoritativního serveru a jeho adresu. Tento postup probíhá do té doby, než původně dotázaný server neobdrží od daného serveru autoritativní odpověď na jeho dotaz. Tuto odpověď poté přepošle původnímu tazateli a dotaz je vyřízen.

7 Iterativní způsob dotazování

Podstata tohotu způsobu spočívá v tom, že dotazem se původně dotázaný server vůbec nezabývá, ale ihned odpovídá jménem kořenovéhu serveru a jeho adresou. Tazatel tedy musí položit další dotaz danému kořenovému serveru. Ten opět odpovídá jménem a adresou autoritativního serveru nejvyšší úrovně. Takto se tazatel ptá, dokud neobrží odpověď na svůj dotaz.

8 Návrh aplikace

Nejdůležitější při návrhu aplikace bylo dobře zvolit struktury a typy jejich hodnot tak, aby byly s DNS kompatibilní. Strukturu dotazu jsem rozdělil na tři oddělené části. První je hlavička (Header). Další je jméno dotazu. Není předem známá jeho délka, tedy kdyby bylo ve struktuře, nebylo by možné jednoduše zjistit velikost této struktury. Poslední částí je struktura Quest_info obsahující typ a třídu. Odpovědi jsou ukládány do struktury Res_record. Její implementace odpovídá popisu ve standardu RFC 1035[2].

9 Implementace

Timeout je řešený na úrovni nastavení možností socketu funkce setsockopt. Je nastaven jak pro odesílané, tak pro přijímané zprávy. Implementováno je vše kromě typu dotazu PTR v kombinaci s iterativním dotazováním.

10 Příklady použití

```
./ipk-lookup -s 8.8.8.8 www.fit.vutbr.cz.
www.fit.vutbr.cz. IN A 147.229.9.23
(exit code 0)

./ipk-lookup -s 8.8.8.8 www4.fit.vutbr.cz.
www4.fit.vutbr.cz. IN CNAME tereza.fit.vutbr.cz.
tereza.fit.vutbr.cz. IN A 147.229.9.22
(exit code 0)

./ipk-lookup -s 8.8.8.8 -t AAAA www4.fit.vutbr.cz.
www4.fit.vutbr.cz. IN CNAME tereza.fit.vutbr.cz.
(exit code 1)

./ipk-lookup -s 8.8.8.8 -t PTR 172.217.23.238
238.23.217.172.in-addr.arpa. IN PTR prg03s06-in-f14.1e100.net.
238.23.217.172.in-addr.arpa. IN PTR prg03s06-in-f238.1e100.net.
(exit code 0)

./ipk-lookup -s 8.8.8.8 -t AAAA -i www.fit.vutbr.cz.
. IN NS a.root-servers.net.
a.root-servers.net. IN A 198.41.0.4
cz. IN NS b.ns.nic.cz
b.ns.nic.cz. IN A 194.0.13.1
vutbr.cz. IN NS pipit.cis.vutbr.cz
pipit.cis.vutbr.cz. IN A 77.93.219.110
fit.vutbr.cz. IN NS rhino.cis.vutbr.cz
gate.feec.vutbr.cz. IN A 147.229.71.10
www.fit.vutbr.cz. IN AAAA 7777:772e:6669:742e:7675:7462:722e:637a
(exit code 0)
```

Reference

[1] MOCKAPETRIS, P. *RFC 1034: Domain names - concepts and facilities*. Dostupné na: <https://tools.ietf.org/html/rfc1034>.

[2] MOCKAPETRIS, P. *RFC 1035: Domain names - implementation and specification*. Dostupné na: <https://tools.ietf.org/html/rfc1035>.

[3] S. THOMSON, e. a. *RFC 3596: DNS Extensions to Support IP Version 6*. Dostupné na: <https://tools.ietf.org/html/3596>.