

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ FACULTY OF INFORMATION TECHNOLOGY

DNS RESOLVER

PROJEKT - SIEŤOVÉ APLIKÁCIE A SPRÁVA SIETÍ PROJECT - NETWORK APPLICATIONS & NETWORK MANAGEMENT

AUTOR PROJEKTU AUTHOR

MATEJ VADOVIČ, XVADOV01

BRNO 2023

Obsah

1	Úvo	od		3							
2	Popis implementácie										
	2.1	Sprace	ovanie argumentov	5							
	2.2										
		2.2.1	DNS hlavička a dotaz	6							
		2.2.2	Prevod doménového mena na QNAME	6							
		2.2.3	Reverzné dotazovanie	6							
	2.3	Sprace	ovanie odpovede	6							
		2.3.1	Podporované typy záznamov a ich obsah pri výpise	6							
		2.3.2		7							
3	Tes	tovanie		9							
4 Použitie			e								
\mathbf{Li}	terat	túra		11							

Zoznam obrázkov

1.1	DNS resolver aplikujúci iteratívne dotazovanie	4
1.2	DNS resolver aplikujúci rekurzívne dotazovanie	4
2.1	Dotazovanie o AAAA záznam pre doménové meno www.seznam.cz	7
2.2	Reverzné dotazovanie na IPv6 adresu	8
2.3	Ukážka spracovania odpovede, ktorá obsahuje viacero záznamov z rôznych	
	kategórií a tiež veľa kompresných ukazateľov, sekcia 4.1.4. Message compres-	
	sion [2]	8

$\mathbf{\acute{U}vod}$

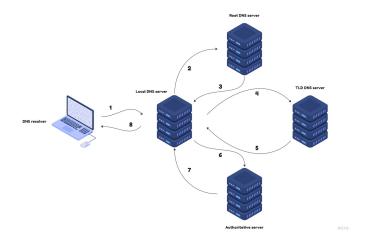
Každé zariadenie v sieti je identifikované pomocou IP adresy. Táto adresa je však pre človeka tažko zapamätateľná a preto sa používajú doménové mená. Je však potrebné mať mechanizmus, ktorý umožní prevod doménového mena na IP adresu a naopak. Tento mechanizmus je DNS(Domain Name System). Pri komunikácií dvoch zaridení je potrebné poznať jeho IP adresu, ktorú odosielateť správy získa od DNS serveru pomocou DNS dotazu. Tieto dotazy klienti posielajú prostredníctvom DNS resolveru.

DNS resolver je lokálny agent, ktorý je zodpovedný za dotazovanie DNS serverov a spracovávanie odpovedí za účelom prekladu doménového mena/IP adresy alebo získavaním iných informácií spojených s doménovým menom. Umožňuje tak užívateľom rýchlešiu a jednoduchšiu navigáciu na internete. [2]

DNS resolver pracuje s distribuovaným, hierarchickým, stromovým doménovým priestorom. Tento priestor je rozdelený na **zóny**. Najvyšší bod hierarchie je **root DNS server**, ktorý obsahuje informácie o serveroch najvyššej úrovni (TLD - Top Level Domain), ktoré sú zodpovedné za správu domén pod nimi. Každá doména najvyššej úrovne má svojho správcu, ktorý je zodpovedný za správu domén pod ňou. Tento proces sa opakuje až na úroveň **autoritatívnych DNS serverov**, ktoré vykonávajú mapovanie názvu domény na adresu pre doménu danej organizácie [3]. Bližší popis doménového priestoru možno nájsť tu [1].

Užívateľské programy interagujú s priestorom doménových mien pomocou resolveru. Resolver odpovedá na užívateľské dopyty informáciami, ktoré získa prostredníctvom dopytov na doménové servery a miestnu vyrovnávaciu pamäť. Na základe metód vyhľadávania možno DNS resolvery rozdeliť:

- Iteratívny dotazuje niekoľko DNS serverov v hierarchickej štruktúre doménového priestoru. Tento proces sa opakuje až kým resolver nedostane záznam z autoritatívneho servera pre danú doménu.
- Ne-rekurzívny dotazuje jeden DNS server, ktorý buď poskytne záznam z autoritatívneho serveru alebo čiastočnú odpoveď, bez toho, aby pokračoval v dotazovaní ďalších DNS serverov.
- Rekurzívny dotazuje jeden DNS server, ktorý môže následne dotazovať ďalšie DNS servery. Tento proces na rozdiel od ne-rekurzívneho poskytuje kompletné riešenie pre danú doménu



Obr. 1.1: DNS resolver aplikujúci iteratívne dotazovanie



Obr. 1.2: DNS resolver aplikujúci rekurzívne dotazovanie

Popis implementácie

Program je implementovaný v jazyku C++ a pozostáva zo súborov dns.cpp(implementácia tried a funkcií) a dns.hpp(deklarácie tried a funkcií).

V rámci projektu som implementoval DNS resolver, ktorý podpuruje dotazovanie a tiež podporuje reverzné dotazovanie, teda preklad IP adresy na doménové meno, obe funkcie pre IPv4 aj IPv6 adresy.

Súčasťou projektu je aj testovací skript, ktorý testuje funkčnosť programu. Testovanie je popísané v kapitole 3.

2.1 Spracovanie argumentov

Pre spacovanie argumentov programu som použil knižnicu **getopt.h**. Táto knižnica umožňuje definovať argumenty programu a ich spracovanie. V prípade, že programu neboli predané argumenty, alebo boli predané argumenty, ktoré nie sú definované, program vypíše nápovedu a ukončí sa. V prípade, že boli predané argumenty, ktoré sú definované, program ich spracuje a uloží do štruktúry **s_Arguments**. Táto štruktúra obsahuje všetky argumenty, ktoré program podporuje.

Argumenty a prepínače, ktoré program podporuje sú:

- -h vypíše nápovedu
- -r rekurzívne dotazovanie
- $-\mathbf{x}$ inverzné dotazovanie¹
- -6 dotazovanie na IPv6 adresy²
- -s server doménové meno/IP adresa DNS servera, na ktorý sa bude dotazovat, povinný argument
- -p port port DNS servera, na ktorý sa bude dotazovať, predvolená hodnota je 53
- adresa doménové meno/IP adresa, o ktorú sa dotazujeme, povinný argument

¹Poznámka ku kombinácií argumentov -x a -6 - v prípade, že sú tieto argumenty kombinované, program vypíše varovnú hlášku o ignorovaní argumentu -6 a pokračuje v spracovaní.

²viď. poznámka pod čiarou č.1

2.2 Komunikácia s DNS serverom

Dotazovanie na DNS server je implementované v main funkcii. Rezolúciu domény DNS servera zabezpečuje funkcia getaddrinfo, ktorá podpuruje aj IPv6 adresy. Následne dochádza k vytvoreniu socketu pre komunikáciu protokolom UDP a vytvorenie dotazu. O zaslanie a prijatie dotazu na DNS server sa starajú funkcia sendto(), resp. recvfrom(). V prípade, že sa nepodarí zaslať dotaz, alebo prijať odpoveď(timeout je 3s), program vypíše chybovú hlášku a ukončí sa. Zostavovaniu jednotlivých častí DNS dotazu sa venujú nasledujúce sekcie.

2.2.1 DNS hlavička a dotaz

Zostavenie DNS hlavičky a nastavenie dotazu je zabezpečené vo funkcii create_DNS_query. Tu dochádza k naplneniu hodnôt v štruktúre hlavičky DNS_header a nastavenie dotazu v štruktúre DNS_question. Štruktúry som vytváral podľa definícií v sekcií 4.1. Format v [2].

2.2.2 Prevod doménového mena na QNAME

Funkcia hostname_to_qname vykonáva prevod doménového mena na QNAME(Query Domain Name). Táto funkcia rozdelí doménové meno na jednotlivé časti, ktoré sú oddelené znakom "" a pridá k nim dĺžku danej časti. Tento postup je opakovaný až kým nie je celé doménové meno prevedené na DNS formát.

www.seznam.cz -> 3www5seznam2cz0

2.2.3 Reverzné dotazovanie

V programe je podpora pre reverzné dotazovanie IPv4 aj IPv6 adries. Dve funkcie, a to reverse_ipv4_address a reverse_ipv6_address, slúžia na prevod IPv4 a IPv6 adries na doménové mená.

Následne už stačí len zavolať funkciu hostname_to_qname a QNAME je pripravené.

2.3 Spracovanie odpovede

Spracovanie odpovede servera raidi funkcia parse_DNS_response. Táto funkcia spracuje DNS hlavičku a následne spracuje odpoveď na dotaz. V prípade, že kód odpovede nie je 0, vypíše sa na stdout aj daný kód a pokračuje spracovanie. Následne sú spracované sekcie Answer, Authority a Additional. Na to slúži funkcia parse_section, ktorá spracuje jednotlivé záznamy v sekcií.

2.3.1 Podporované typy záznamov a ich obsah pri výpise

Tu používam rovnaké označenia ako sú uvedené sekcií 3.2 RR definitions [2], teda v anglickom jazyku, kde možno nájsť aj detailný popis jednotlivých typov záznamov a častí.

Name TYPE CLASS TTL ADDRESS

Tabuľka 2.1: Popis výpisu záznamu A

Name TYPE CLASS TTL ADDRESS

Tabuľka 2.2: Popis výpisu záznamu AAAA

Name TYPE CLASS TTL NSDNAME

Tabuľka 2.3: Popis výpisu záznamu NS

Name	TYPE	CLASS	TTL			
MNAME	RNAME	SERIAL	REFRESH	RETRY	EXPIRE	MINIMUM

Tabuľka 2.4: Popis výpisu záznamu SOA

Name TYPE CLASS TTL CNAME

Tabuľka 2.5: Popis výpisu záznamu CNAME

Name TYPE CLASS TTL PTRDNAME

Tabuľka 2.6: Popis výpisu záznamu PTR

2.3.2 Prevod z QNAME na doménové meno

Prevod z formátu QNAME na doménové meno je implementuje qname_to_hostname. Táto funkcia prechádza jednotlivé časti oddelené značkami. Funckia umožňuje aj prácu s kompresnými ukazateľmi, ktoré sú popísané v sekcií 4.1.4. Message compression [2].

3www5seznam2cz0 -> www.seznam.cz.

./dns -6 -r -s 8.8.8.8 www.seznam.cz Authoritative: No, Recursive: Yes, Truncated: No Question section (1) www.seznam.cz., AAAA, IN Answer section (2) www.seznam.cz., AAAA, IN, 157, 2a02:598:2::1222 www.seznam.cz., AAAA, IN, 157, 2a02:598:a::79:222

Obr. 2.1: Dotazovanie o AAAA záznam pre doménové meno www.seznam.cz.

```
./dns -6 -x -s 8.8.8.8 2a03:2880:f10d:83:face:b00c::25de
Warning: -6 option is ignored when -x is used.
Authoritative: No, Recursive: Yes, Truncated: No
Question section (1)
e.d.5.2.0.0.0.0.0.0.0.0.b.e.c.a.f.3.8.0.0.d.0.1.f.0.8.8.2.3.0.a.2.ip6.arpa., PTR, IN
Answer section (1)
e.d.5.2.0.0.0.0.c.0.0.b.e.c.a.f.3.8.0.0.d.0.1.f.0.8.8.2.3.0.a.2.ip6.arpa., PTR, IN,
3600, edge-star-mini6-shv-01-lax3.facebook.com.
```

Obr. 2.2: Reverzné dotazovanie na IPv6 adresu.

```
./dns -s kazi.fit.vutbr.cz kazi.fit.vutbr.cz
Authoritative: Yes, Recursive: No, Truncated: No
Question section (1)
kazi.fit.vutbr.cz., A, IN
Answer section (1)
kazi.fit.vutbr.cz., A, IN, 14400, 147.229.8.12
Authority section (4)
fit.vutbr.cz., NS, IN, 14400, gate.feec.vutbr.cz.
fit.vutbr.cz., NS, IN, 14400, gate.fit.vutbr.cz.
fit.vutbr.cz., NS, IN, 14400, guta.fit.vutbr.cz.
fit.vutbr.cz., NS, IN, 14400, guta.fit.vutbr.cz.
Additional section (3)
guta.fit.vutbr.cz., A, IN, 14400, 147.229.9.11
guta.fit.vutbr.cz., AAAA, IN, 14400, 2001:67c:1220:809::93e5:90b
kazi.fit.vutbr.cz., AAAA, IN, 14400, 2001:67c:1220:808::93e5:80c
```

Obr. 2.3: Ukážka spracovania odpovede, ktorá obsahuje viacero záznamov z rôznych kategórií a tiež veľa kompresných ukazateľov, sekcia 4.1.4. Message compression [2].

Testovanie

Pzthon skript teest.py sa stará o spustenie programu s rôznymi argumentami a následne porovnáva návratové hodnoty.

Pripravil som sadu testov v zložke tests, ktoré slúžia ako ukážka správneho výstupu. Pri tvorbe testov sade som použil nástroj dig a sledovanie paketov v prostredí Wireshark. Problém s testovaním sú premenlivé hodnoty, ktoré sa môžu vyskytnúť v odpovedi. Či už ide o poradie záznamov v jednotlivých sekciách alebo rozdielne hodnoty TTL alebo hodnôt v SOA zázname. Preto táto predpripravená sada slúži hlavne užívateľom na kontrolu správneho výstupu programu. V skripte je preto iba automatická kontrola návratovej hodnoty.

Použitie

Preklad programu je možné vykonať pomocou príkazu make v koreňovom adresári projektu. Program spustíte príkazom ./dns [-r] [-x] [-6] -s server [-p port] adresa, pre detailný popis argumentov viz. sekcia 2.1.

Testy možno spustiť pomocou príkazu make test v koreňovom adresári projektu.

Literatúra

- [1] MOCKAPETRIS, P. DOMAIN NAMES CONCEPTS AND FACILITIES. Network Working Group, november 1987.
- [2] MOCKAPETRIS, P. DOMAIN NAMES IMPLEMENTATION AND SPECIFICATION. Network Working Group, november 1987.
- [3] WIKIPEDIA CONTRIBUTORS. Domain Name System Wikipedia, The Free Encyclopedia [online]. 2023 [cit. 2023-11-4]. Dostupné z: https://en.wikipedia.org/w/index.php?title=Domain_Name_System&oldid=1182387275.