

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Síťové aplikace a správa sítí –
Filtrující DNS resolver

Obsah

1	IPV4 a IPV6	2
2	DNS	2
3	DNS packet	2
3.1	Hlavička	2
3.2	Dotaz	3
3.3	Odpověď	3
3.4	Authority	3
3.5	Additional	3
4	Návrh a implementace aplikace	4
4.1	Překlad programu	4
4.2	Ukázka spouštění	4
4.3	Parametry programu	4
4.4	Tělo programu	4
4.5	Child proces	4
4.6	Návratové kódy	5
5	Testování	5
5.1	Testování typu dotazu	5
5.2	Testování blacklistových domén	5

1 IPV4 a IPV6

Tento filtrující DNS resolver funguje jen pro ipv4 QTYPE 1, tedy dotazy typu A.

2 DNS

DNS je hierarchický systém doménových jmen. Ten realizují právě DNS servery spolu s protokolem stejného jména, který využívají k výměně informací. DNS je v praxi překladová služba, která číselnou IP adresu přeloží do podoby zvolené domény. Na IP se ptá DNS serveru[1].

3 DNS packet

Veškerá komunikace v domain protokolu je přenášena pomocí zpráv, které mají následující podobu[2].

Header	hlavička
Question	dotaz
Answer	odpověď
Authority	autorita(autorizovaná odpověď)
Additional	dodatečné informace

3.1 Hlavička

Hlavička paketu je přítomna vždy. Hlavička zahrnuje pole, které značí, z jakých dalších částí se paket skládá a dále také, jestli je paket dotaz, nebo odpověď a další[2]. Podoba hlavičky je následující:

- ID - 16 bitový identifikátor paketu
- QR - 1 bit značí, jestli je paket typu 0 (dotaz), nebo 1 (odpověď)
- Opcode - 4 bity pro označení typu dotazu
- AA - 1bit Odpověď autority, tedy serveru odpovědného serveru
- TC - 1 bit Indikuje zda byl paket zmenšen
- RD - 1 bit Indikuje, zda-li je vyžadována rekurze
- RA - 1 bit Podpora rekurze
- Z - 4 bity Rezerva pro budoucí použití
- RCODE - 4 bity Response code

- QDCOUNT - 16 bitů Specifikující počet vstupů v dotazu
- ANCOUNT - 16 bitů Specifikující počet zdrojových záznamů v odpovědi
- NSCOUNT - 16 bitů Počet zdrojových záznamů
- ARCOUNT - 16 bitů Počet zdrojových záznamů v přídatné sekci

3.2 Dotaz

Část paketu používaná pro přenos dotazu a parametrů s ním spojených[2].

- QNAME - 16 bitů Název domény
- QTYPE - 16 bitů Typ dotazu
- QCLASS - 16 bitů Třída dotazu

3.3 Odpověď

Část paketu používaná pro přenos odpovědi a parametrů s ní spojených[2].

- NAME - 16 bitů Název domény spojené se zdrojovým záznamem
- TYPE - 16 bitů Typ dotazu
- CLASS - 16 bitů Specifikuje význam dat v RDATA
- TTL - 16 bitů Čas po jakou dobu má být zaznam zachován před vymazáním
- RDLENGTH - 16 bitů Délka oktetů v RDATA
- RDATA - Proměnná délka oktetových stringů popisujících zdroj

3.4 Authority

Sekce obsahuje zdrojové záznamy odkazující na autoritativní server[2].

3.5 Additional

Obsahuje zdrojové záznamy, které jsou spjaté s dotazem, ale nejsou odpovědí na tento dotaz[2].

4 Návrh a implementace aplikace

4.1 Překlad programu

Zdrojové kódy k programu se nachází ve složce `src`. V souboru, nad složkou `src`, se nachází `makefile`, pomocí kterého lze pracovat s aplikací. Příkazem `make` se přeloží projekt a vygeneruje se program `dns`. Příkazem `make clean` se program `dns` smaže. `Makefile` také zná příkaz `make docu`, který vytvoří doxygen dokumentaci k projektu.

4.2 Ukázka spouštění

Program se spouští následujícím způsobem:

```
./dns -s 1.1.1.1 -p 8080 -f blacklist
```

```
./dns -s 8.8.4.4 -f blacklist.txt
```

4.3 Parametry programu

Program umí zpracovat 3 parametry. Jsou jimi:

- `-s`: IP adresa nebo doménové jméno DNS serveru (resolveru), kam se má zaslat dotaz.
- `-p port`: Číslo portu, na kterém bude program očekávat dotazy. Výchozí je port 53. (volitelný parametr)
- `-f filter_file`: Jméno souboru obsahující nežádoucí domény.

Parametry zpracovává funkce `getArguments()`

4.4 Tělo programu

Aplikace `dns` běží jako server. Po spuštění programu se vytvoří funkcí `socket()` komunikační soket, přiřadí se mu adresa pomocí funkce `bind()` a následně se v cyklu čeká na přijetí paketu na adrese `localhost` na portu zadaném parametrem programu `-p`.

Jakmile je zachycen paket na dané adrese a portu, tak se hlavní aplikační proces rozdělí funkcí `fork()`. Zatímco child proces získává doménové jméno z paketu a další informace, hlavní proces se vrátí a čeká na přijetí dalšího paketu.

4.5 Child proces

Jakmile je paket přijat, zpracovává se v child procesu. V tomto procesu program získá dotazované doménové jméno `QTYPE` z paketu, aby si ověřil, zda se opravdu jedná o dotaz typu `A`.

Dále program prochází zadaný soubor domén a hledá, zda-li dotazovaná doména není na tomto seznamu nebo jestli není poddoménou na tomto seznamu.

Případnou zakázanou doménu vrací klientovi jako původní paket s nastaveným `rcode` flagem na 5 a flagem `qr` na 1. Obdobně je to pro případ jiného typu dotazu než je typ `A`, resp. s `rcode` nastaveným na 4.

V případě, že tyto kontroly proběhnou v pořádku, je paket přeměřován na DNS server zadaný parametrem programu `-s`. Parametr `-s` se předává funkci `getDnsIp()`, která vrací ip adresu DNS serveru. Po získání ip adresy je paket funkcí `sendto()` poslán na port 53 DNS serveru. Příchod odpovědi je očekáván funkcí `recvfrom()` a jakmile tento paket dorazí, je poslán nazpět klientovi.

4.6 Návratové kódy

- 9 - Chyba soubor neexistuje
- 10 - Chyba vstupních parametrů
- 11 - Chyba získávání ip adresy DNS serveru
- 12 - Chyba vytvoření socketu
- 13 - Chyba přidělování adresy socketu

5 Testování

Korektní funkčnost aplikace jsem testoval pomocí nástroje `nslookup`. Testy fungovaly následovně. V jednom okně terminálu jsem pustil svůj program a ve 2. okně terminálu jsem pustil `nslookup` takto: `"nslookup -port=8080 -type=a doména localhost"` a pak jsem porovnával ip adresu, která přišla zpět `nslookupu` s online resolv nástrojem DNS Checker. Případně jsem zadal ip adresu do prohlížeče. Takto jsem iteroval přes různé domény.

5.1 Testování typu dotazu

Korektnost ošetření dns dotazu typu A jsem testoval tak, že jsem pustil `nslookup` bez parametru `-type=a`. Tím pádem se pošle první ipv4 paket a následně i ipv6 paket. V tomto případě nebyl `QTYPE` z hlavičky paketu nastaven na 1 ale na 28. V situaci kdy přišel ipv6 paket, dns program reagoval korektně a poslal zpět paket s nastaveným `rcode` a `qr` a dále neposílal paket na dns resolver. Toto jsem kontroloval programem Wireshark, který celou komunikaci odchytával.

5.2 Testování blacklistových domén

Testování blacklistových domén probíhalo tak, že jsem si do souboru zapsal několik domén. Doménami byly kupříkladu `facebook.com`, `docs.google.com` a `wis.fit.vutbr.cz` a na běžící program dns jsem pomocí `nslookup` posílal domény, které jsem čekal, že projdou, tedy například `face.com`, `google.com`, `google.cz`, `vutbr.cz`, `docs.google.cz` apod. Následně jsem posílal domény, u kterých jsem čekal, že neprojdou, tedy domény jako `google.com`, `wis.wis.fit.vutbr.cz` atd. Celou síťovou komunikaci jsem sledoval programem Wireshark. A pro každou zaslanou doménu na server, jsem kontroloval odchozí paket na klienta a díval se na `rcode` a `qr` flagy v hlavičce.

Reference

- [1] info@best-hosting.cz BEST-HOSTING s.r.o. Co je to dns server?, 2020.
- [2] P.v. Mockapetrís. Domain names - implementation and specification. page 1–55, Nov 1987.