ISA projekt

Filtrující DNS resolver

Richard Fiľo (xfilor00)

12. listopadu 2020

Obsah

1 Zadanie

Napište program dns, který bude filtrovat dotazy typu A směřující na domény v rámci dodaného seznamu a jejich poddomény. Ostatní dotazy bude přeposílat v nezměněné podobě specifikovanému resolveru. Odpovědi na dříve přeposlané dotazy bude program předávat původnímu tazateli. Analýza a sestavení DNS zpráv musí být implementována přímo v programu dns. Stačí uvažovat pouze komunikaci pomocí UDP a dotazy typu A. Na jiné typu dotazů a nežádoucí dotazy odpovídejte vhodnou chybovou zprávou.

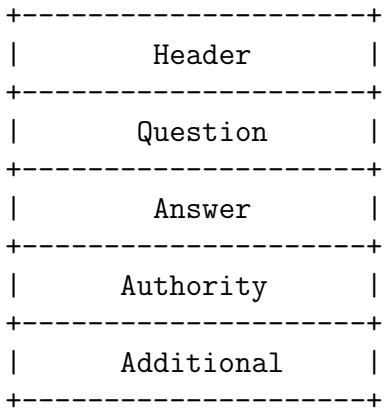
Při vytváření programu je povoleno použít pouze knihovny pro práci se sokety a další obvyklé funkce používané v síťovém prostředí (jako je netinet/*, sys/*, arpa/* apod.), knihovnu pro práci s vlákny (pthread), signály, časem, stejně jako standardní knihovnu jazyka C (varianty ISO/ANSI i POSIX), C++ a STL. Jiné knihovny nejsou povoleny.

2 Systém DNS

Domain Name System prestavuje mechanizmus pre pomenovanie zdrojov, ktorý je použiteľný pre rozličných hostiteľov. Užívateľovi stačí na zistenie informácii o danom serveri jedna informácia - doména. Mapovanie domén na informácie je uložené v databáze, ktorej jednotlivé časti sa nachádzajú na nameservroch. Proces získania záznamov pomocou domény sa nazýva rezolúcia a má ju na starosti resolver. Resolver musí mať prístup k minimálne jednému nameserveru. Poznáme 2 druhy rezolúcie iteratívna a rekurzívna. Pri rekurzívnej si resolver vyžiada odpoveď od práve jedného nameserveru ktorý ak nedisponuje odpoveďou sám sa pýta ďalších až kým nenájde autoritatívnu odpoveď alebo neskončí chybovou hláškou. Pri iteratívnej rezolúcii ak nameserver nepozná odpoveď iba vráti nameserver, ktorý nás môže na odpoveď bližšie nasmerovať. Preferovaný port je 53 a maximálna veľkost paketu je 512B.

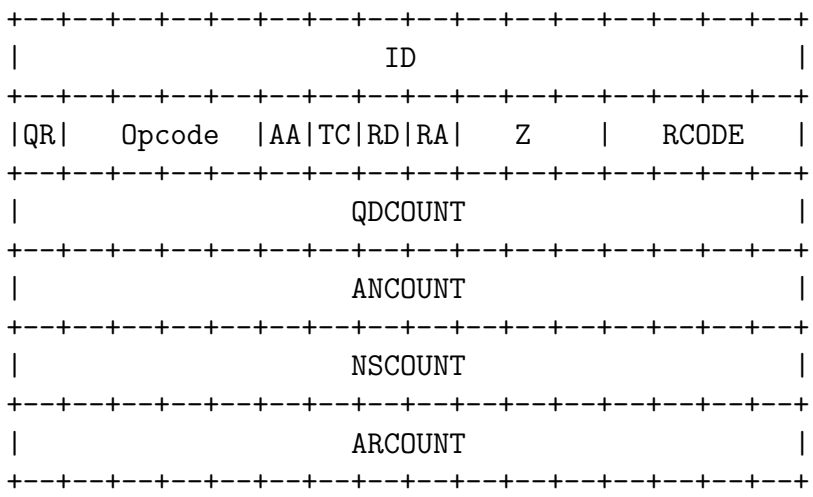
3 Formát DNS požiadavky

3.1 Paket



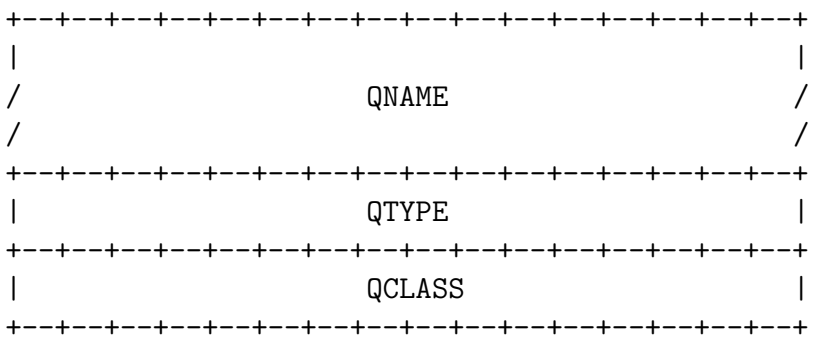
Header = hlavička paketu
Question = otázka na nameserver
Answer = odpoveď z nameservru
Authority = informácie o autoritatívnom nameserveri
Additional = ďalšie informácie

3.2 Hlavička



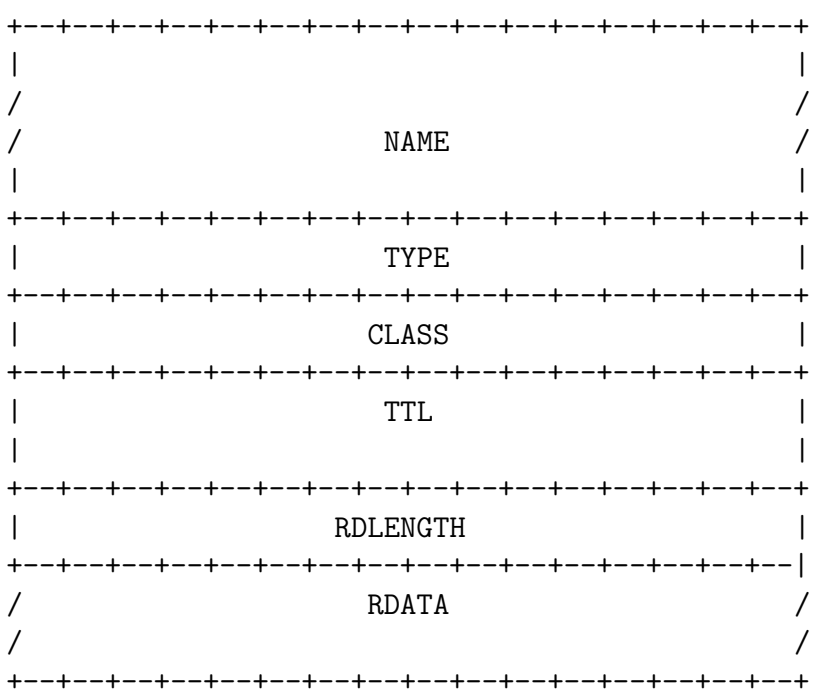
ID = identifikátor požiadavku
QR = 0 pre otázku, 1 pre odpoveď
Opcode = kód správy
AA = 1 značí že odpoveď prišla z autoritatívneho serveru
TC = 1 značí že správa sa nevošla do 512b
RD = 1 značí že je vyžadovaná rekurzívna rezolúcia
RA = 1 značí že server podporuje rekurzívnu rezolúciu
Z = rezervovaný bit, musí mať hodnotu 0
RCODE = návratový kod, 5 znamená, že server odmietol odpoveď na dotaz
QDCOUNT = počet otázok
ANCOUNT = počet odpovedí
NSCOUNT = počet NS záznamov kde sa môže nachádzať odpoveď
ARCOUNT = počet ďalších záznamov

3.3 Požiadavka



QNAME = doménové meno zapísané v DNS formáte (dĺžka časti mena po najbližšiu bodku, časť mena po najbližšiu bodku, posledná časť má dĺžku 0)
QTYPE = označuje typ požiadavky
QCLASS = označuje triedu otázky (väčšinou IN = internet)

3.4 Odpoveď



NAME = doménové meno
TYPE = typ odpovede
CLASS = trieda odpovede
TTL = počet sekúnd po ktorom by záznam mal byť vyradený z cache
RDLENGTH = veľkosť dát
RDATA = dáta odpovede

3.5 Kompresia správ

Reťazec sa v DNS ukladá ako postupnosť dvojíc dĺžka/hodnota. Ukončený je nulovým oktetom. Pri ukladaní doménových mien sa využívajú ukazatele na predchádzajúci výskyt či už celého mena alebo len jeho časti. Rozdiel medzi tým, či sa jedná o reťazec alebo doménové meno spoznáme podľa prvých dvoch bitov. Ak sú nulové, ďalších 6 bitov tohto bajtu obsahuje dĺžku reťazca, ktorý nasleduje počínajúc ďalším oktetom. Ak sú prvé dva bity jednotkové, potom nasledujúce bity obsahujú ukazateľ na predchádzajúci výskyt reťazca v rámci paketu. Je to offset od začiatku paketu. Offset tvorí 8 bitov začínajúcich jednotkami a nasledujúci bajt (spolu 14 bitov).

4 Návrh aplikácie

Tento program spracováva iba DNS dotazy typu A. V inom prípade je klientovi zaslaná RESPONSE REFUSED. Ak sa jedná o dotaz typu A tak sa kontroluje či dotazovaná domená nepatrí do zoznamu nežiadúcich domén. Ak áno, klientovi je opäť zaslaná RESPONSE REFUSED. V opačnom prípade sa DNS dotaz prepošle na vybraný server a odpoveď z neho sa prepošle priamo klientovi.

4.1 Popis implementácie

Aplikácia bola realizovaná pomocou jazyka C a povolených knižníc.

Súbor s zoznamom nežiadúcich domen sa nenačítava do pamäte celý naraz ale postupne sa spracováva po riadkoch. Tuto možnosť som zvolil pretože môžme pracovať aj s velkým počtom nežiadúcich domén a alokovaná pamäť programu bude stále rovnaká.

Kontrola prebieha asi takto. Mame na príklad domenu seznam.cz. Najpr sa skontroluje, či sa doména cz nenachádza v zozname. Ak nie, tak sa zoberie ďalšia poddoména seznam.cz. Ak sa ani tá nenachádza v zozname tak doména nie je nežiadúca a tento dotaz sa môže preposlať zvolenému DNS servru. Odpoveď je následne preposlaná klientovi.

4.2 Testovanie

Testy nespustíte pomocou príkazu "make test", pretože všetky testy boli prevádzané ručne pomocou nástroja dig. Boli odtestované rôzne prípady a všetky dopadli podľa očakávania.

4.3 Návratové hodnoty

- 0 - úspech
- 1 - programové zlihanie napriklad pri alokácii pamäte
- 2 - zlihanie pri nastavení zlých parametrov

4.4 Návod na použitie

dns -s server [-p port] -f filter_file

Povinné parametre:

- -s IPv4 adresa alebo doména DNS servra
- -f názov súboru s nežiadúcimi doménami

Voliteľné parametre:

- -p číslo portu na ktorom bude služba bežať, defaultne 53
- -h výpis nápovedy
- -v výpis nastavených hodnôt servra, portu a súboru

5 Zdroje

- Ing. Petr Matoušek, Ph.D., M.A.- ISA - Systém DNS - prezentácia, prednáška
- `https://tools.ietf.org/html/rfc1035`
- `https://tools.ietf.org/html/rfc1034`