ISA 2019

DNS resolver

Martin Litwora

Datum: 10.11.2019

1. Úvod

Cílem projektu bylo vytvořit program, který zašle dns dotaz na server a vypíše na standartní výstup informace, které od serveru obdržel. Uživatel zadá adresu serveru, na který se bude posílat dotaz, zda-li chce aby byl dotaz rekurzivní. Aplikace také umožňuje zasílat reverzní dotazy a podporuje IPv6. Je také možné specifikovat port, na který se dotaz zašle.

2. Základní informace o DNS

DNS slouží k mapovaní serverových jmén na jejich odpovídající IP adresy. Základní požadavek, jež se zasílá, obsahuje doménové jméno, u kterého chceme zjistit IP adresu. DNS server následně prochází svoji databázi jmén a pokud najde shodu vrátí hledanou IP adresu, pokud ne zasílá požadavek na další server, ve kterém se proces hledání opakuje.
Samotné DNS dotazy se posílají formou UDP paketu.

3. Struktura DNS paketu

Každý DNS paket obsahuje hlavičku (Header), ve které se mimo jiné nachází sekce s Flagy, díky kterým můžeme říci například aby dotaz byl rekurzivní, nebo můžeme zjistit, zda byla odpověď zkrácena. Dále se z hlavičky můžeme dozvědět počet odpovědí ze serveru a také server může nastavit Response code, což je 4bitové číslo, které nám může už na začátku určit, zda nedošlo k nějaké chybě.
Další sekce je pro samotný dotaz (Question), která obsahuje samotný doménový název, typ dotazu, tedy v našem případě buď, že se jedná o klasický A dotaz (IPv4) nebo AAAA (IPv6). Dále se tam nachází třída, kterou máme nastavenou jako IN, tedy internet.
V samotné odpovědi (Answer) je nejdůležitější část s daty jež jsme dostali od serveru a typ odpovědi. Aplikace podporuje tyto typy odpovědí: A, AAAA, CNAME, dále SOA a NS pro autoritativní odpovědi.

4. Implementace

Při samotné implementaci byly nejnáročnější pasáže, kdy bylo potřeba převést samotnou dotazovanou adresu do odpovídající formy. Tedy, například URL example.com se skládá ze dvou částí, oddělených tečkou. První byte tedy obsahuje počet znaků, než se má objevit další tečka. Výraz je pak ukončen nulovým bytem.
Výsledný dotaz má tedy tuhle formu: 7example3com0
Další obtíž nastala v momentě čtení a parsovaní samotné odpovědi. Především, kdy odpověď obsahovala CNAME záznam. Samotná sekce může obsahovat ukazatel (hodnota c0 hexadecimálně), která odkazuje na jinou část DNS sekce. Na tuhle část jsem využil funkci, kterou jsem našel na této stránce.
Inverzní dotaz taky má svoji vlastní formu, jež je nutné dodržet. Například IPv4 adresu 77.21.134.9 je nutné převést na: 9.134.21.77.in-addr.arpa a teprve je možné zaslat dotaz.
Aplikace má také zakomponován timeout, při čekání na odpověď na dvě sekundy. Při úspěchu program skončí s návratovou hodnotou 0, nastane-li chyba vrací se hodnota 1 včetně chybového hlášení na standartní errorový výstup. Fungování bylo několikrát ručně otestováno.

5. Bibliografie a studijní materiály

www.binarytides.com, 18.12.2012 [online]. Dostupné z: *https://www.binarytides.com/dns-query-code-in-c-with-winsock/*
www.tcpipguide.com, 20.9.2005 [online]. Dostupné z: http://www.tcpipguide.com/free/t_TCPIPDomainNameSystemDNS.htm
wikipeda.org, 27.10.2019 [online]. Dostupné z: *https://en.wikipedia.org/wiki/List_of_DNS_record_types*
www.gta.ufrj.br, [online]. Dostupné z: *https://www.gta.ufrj.br/ensino/eel878/sockets/sockaddr_inman.html*
www.networksorcery.com, 2018 [online]. Dostupné z: *http://www.networksorcery.com/enp/protocol/dns.htm#Opcode*
tools.ietf.org, 4.8.2008 [online]. Dostupné z: *https://tools.ietf.org/id/draft-ietf-dnsop-no-response-issue-12.html*
www.ripe.net, 1.12.2007 [online]. Dostupné z: https://www.ripe.net/manage-ips-and-asns/db/support/configuring-reverse-dns
amriunix.com, 2.8.2018 [online]. Dostupné z: https://amriunix.com/post/deep-dive-into-dns-messages/