Dokumentace IPK projekt 2

Varianta 3: DNS Lookup nástroj

Autor: Tomáš Kukaň, xkukan00

9. 4. 2018

Obsah

Obecně o DNS

DNS se používá k rezoluci (překladu) doménových jmen na IP adresy. DNS servery jsou uspořádány do stromové struktury a když se pokoušíme získat IP adresu, postupuje se od ko5enových serverů k doménám nižšího řádu o nichž DNS server drží informace.

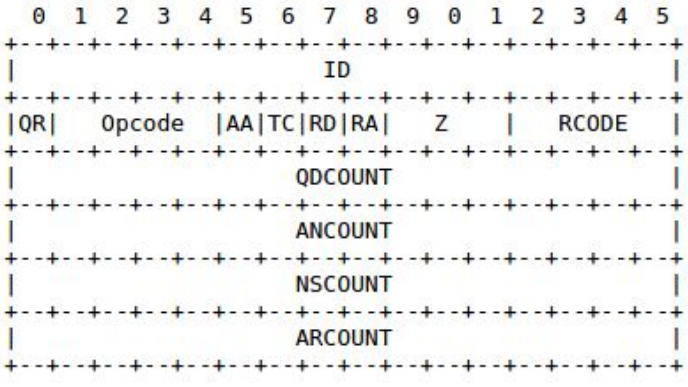
Name servery

Name servery jsou součástí DNS serveru a starají se o data uložené na serveru. Většina serverů si různá data cachuje aby urychlila dotazování.
Name servery které v sobě uchovávají kompletní informace o doménovém stromu nazýváme autoritativní. Záznamy odkazující na jiné name servery autoritatvní nejsou.

Formát DNS dotazu

DNS dotaz se skládá z hlavičky a dotazu nebo více dotazů. Odpověď DNS serveru se skládá z upravené hlavičky, stejného dotazu a pokud bylo vyhledávání úspěšné tak obsahuje několik RR záznamů.

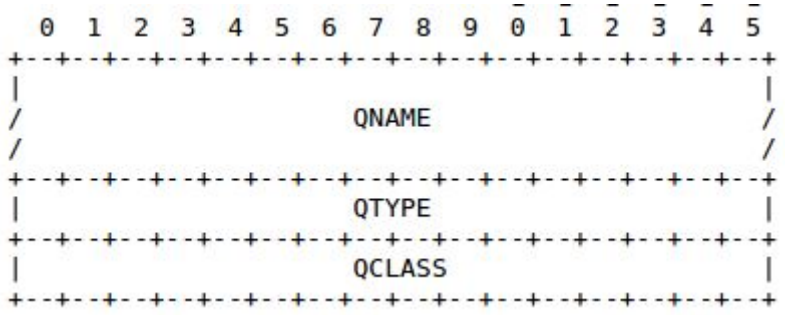
Formát hlavičky:



[1]

Hlavička nese různé informace pevné délky. V tomto projektu je nejzajímavější RD pole, které nastavíme na 1, pokud chceme provést dotaz rekurzivně.
Dále jsou důležité počty RR záznamů a návratový kód RCODE.

Za hlavičkou následuje dotaz v následujícím formátu:



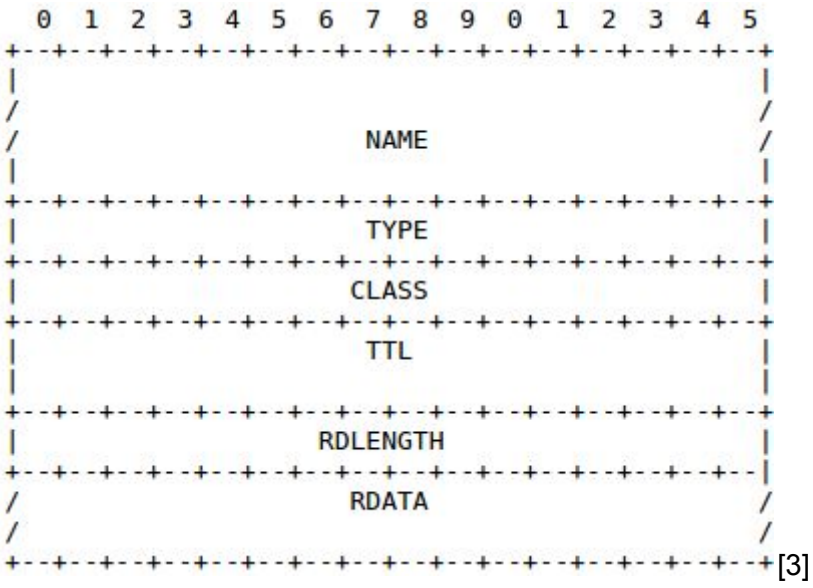
[2]

Kde QNAME je dotaz, který je pole proměnné délky. Poté následuje požadovaný typ odpovědi a její třída (pro nás vždy internet).

Hned za dotazem následují RR záznamy.
Ty dělíme na:

1. Answer RRs
   - Pokud byla resoluce úspěšná, zde najdeme jednu nebo více odpovědí.
2. Authority RRs
   - Tyto záznamy nenesou odpověď ale nesou adresy dalších serverů, které by mohli znát odpověď na náš dotaz.
3. Additional RRs
   - Nepovinné záznamy většinou nesoucí dodatečné informace k Athority RRs, můžou se v nich nacházet IP adresy. Jsou využité ke zmenšení počtu dotazů, neb místo dalšího dotazu na IP adresu danného Authority serveru, odpověď je nám zaslána předem.

Formát RR záznamu:



[3]

Kde pole jsou stejná jako u dotazu a RDATA obsahují odpověď, nebo další adresu. TTL (time to live) je doba po kterou si můžeme data cachovat a považovat je za platná.

Komprese zpráv

DNS dotazování používá jednoduchou kompresi zpráv, která se používá u všech polí proměnné délky, tedy: NAME, RDATA, QNAME.
Adresy se převedou na textovou formu a tečky jenž oddělují jednotlivá čísla, nebo domény se přepíší na znak, jehož hodnota odpovídá počtu znaků za tímto číslem. Adresa končí nulou.

Další kompresní metoda která se tu používá je odkazování zpět do záznamu, čímž se předchází duplikaci dat.

Rekurzivní/iterativní způsob dotazování

Jak už je výše zmíněno, v hlavičce DNS dotazu můžeme nastavit rekurzi. Pokud dotazovaný server rekurzi podporuje, nebude nám vracet jednotlivé autoratitivní servery ale rovnou nám odpoví na dotaz.
V případě iterativního dotazování si tuto rekurzi musíme zajistit sami. Nejdříve se tedy zeptáme na kořenový server a toho se poté ptáme v rekurzi.

Návrh/implementace aplikace

Obecný návrh

Aplikaci jsem se rozhodl implementovat čistě v jazyku C vzhledem k použití knihoven napsaných ve stejném jazyce.
Aplikaci jsem si pro větší přehlednost rozdělil do tří modulů, kde každý odvádí trochu jinou práci.

Nejobtížnější pasáže

Nejobtížnější bylo rozhodně implementovat iterativní dotazování. Musel jsem se nejdřív dotázat na kořenový server a následně vytvořit rekurzivní funkci, která se vrátila IP adresu požadovaného doménového jména a v případě že došla do situace že server neměl IP adresu autoratitivního serveru, funkce se rekurzivně zavolala znova s upravenými parametry.

Citace

1-3. MOCKAPETRIS P., RFC1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION [online]. 2018-9-4 [cit. 1987-11]. Dostupné z: https://www.ietf.org/rfc/rfc1035.txt