DNS Lookup nástroj

Počítačové komunikace a sítě – Projekt 2

Fakulta informačních technologií
Vysoké učení technické v Brně

Jiří Furda (xfurda00)
8. dubna 2018

Obsah

Úvod do problematiky

Domain Name System (DNS) jak název napovídá je systém doménových jmen. Tento systém se využívá například při prohlížení webových stránek a umožňuje člověku přístup k těmto stránkam pod jejich lehko zapamatovatelnou doménou (např. *www.google.com*) místo jejich IP adresy (např. *216.58.201.100*). Pro přístup k obsahu dané stránky je ale nutné znát IP adresu jejího serveru, proto je nutné onu doménu nejprve přeložit na IP adresu a až poté ke stránce přistupovat. O tento překlad se stará právě DNS.

DNS dotaz

Pro získání IP adresy je nejprve nutné úspěšně zformulovat a odeslat dotaz na DNS server. Adresy těchto serverů jsou v Unixových systémech uloženy v souboru */etc/resolv.conf*.

Samotný dotaz je sekvence několika bytů odeslána UDP protokolem.

Struktura nastavení

Nastevní dotazu má vždy délku 12 bytů a významově jsou uskupeny po dvojcích.

Byte 1-2 značí identifikaci transakce, v případě tohoto programu je použito ID klientského procesu.

Byte 3-4 určuje nastavení dotazu, tento program neumožňuje iterativní dotazy, proto má nastavení vždy binární hodnotu 0000 0001 0000 0000, značící standarní dotaz vyžádující rekurzi.

Byte 5-6 udává počet dotazů, zde program vždy posílá hodnotu 0 1, protože nepodporuje více jak jeden dotaz.

Byty 7-12 udávají stejným způsobem jako byty 5-6 počty autoritativních a dodatečných serverů, ale tento program tuto položku nevyužívá a vždy odesílá 0 0 0 0.

Struktura dotazu

Samotný dotaz navazuje hned za nastavením dotazu. Jeho délka se odvíjí od dotazovaného doménového jména.

Obsahem jednoho dotazu je přeložené jméno (viz *překlad doménového jména*) a po ní nasledují další 4 byty. Toto celé se může opakovat několikrát, pokud je odesláno více dotazů zároveň. Tento program ale tuto možnost nepodporuje, proto v popisu uvažuje pouze odeslání jednoho dotazu.

Předposlední 2 byty značí typ dotazovaného záznamu. Tento program pracuje pouze s následující typy:

Typ	Hodnota
A	0 1
NS	0 2
CNAME	0 5
PTR	0 12
AAAA	0 28

Poslední 2 byty označují dotazovanou třídu, program ale pracuje pouze s třídou Internet, proto vždy posíla byty s hodnotou 0 1.

Překlad doménového jména

Doménové jméno je rozděleno na úrovně (tečky v doménovém jméně). Před každou úrovní je potřeba vložit byte s hodnotou odpovídající počtu znaků v následující úrovni. Pokud jméno nezačíná tečkou, tak je celé posunuté o jeden znak doprava, aby bylo možné vložit délku první úrovně. Například z doménového jména *www.google.com* se stane *3www6google3com0*. Kdy číselné hodnoty neodpovídají své ASCII hodnotě, ale přímo bytům s danou hodnotou.

Každé doménové jméno končí tečkou, pokud tomu tak ve vstupu nebylo, tečka je doplněna.

DNS odpověd

Odpověd od DNS serveru sebou kromě výsledných IP adres nese i původní DNS dotaz. Až za tímto dotazem následuje obsah odpovědi.

Struktura odpovědi

Samotná odpověď může být buď jedna nebo jich může následovat více za sebou, každá má ale stejný tvar a následují hned za sebou. Jejich délka bývá ale odlišná, jelikož se odvíjí od délky jména a jeho kompresi (viz *komprese zprávy*).

Jako první je obsažen 1 byte či posloupnost bytů nesoucí hodnotu jména. Pro zapsaní tohoto jména mohla být využita komprese, proto je nutné první celé jméno složit a poté provést opačný překlad než je popsán v sekci *překlad doménového jména*. Nalezení nulového bytu značí konec jména.

Následující 4 byty mají stejný význam jako v DNS dotazu. Po nich následují další 4 byty nesoucí hodnotu délky života, nicméně tato informace je pro program irelevantní.

Další 2 byty udávájí počet bytů využitých pro zapsání výsledného jména, to následuje hned po těchto dvou bytech a je zapsáno stejně jako jméno popsané výše.

Komprese zprávy

Za účelem zmenšení délky zprávy se využívají odkazy na opakujícící se data. Odkaz je realizován odskokem od začátku zprávy. Použití odkazu indikuje byte s hodnotou větší než binárně 1100 0000. Pokud tedy zpráva obsahuje byte zapsaný binárně např. 1100 1010, je potřeba od něj odečíst binární číslo 1100 000 a poté k němu připojit i následující byte. Vzniknou nám tedy binární číslo např. 0000 1010 0000 0001. Po převodu do dekacické soustavy nám vzniká číslo 2561. Tudíž data pokračují na 2562. bytu zprávy.

Popis programu

Program realizuje dotaz na systém DNS a následný překlad doménových jmen a IP adres v odpovědi na tento dotaz. To vše bez využití knihovních funkcí k tomu určných.

Použití programu

Programu rozlišuje dvě základní varianty spuštění – klasické a nápovědu.

Spuštění nápovědy

Konvece spuštění programu pro výpis nápovědy programu je následující:

```
./ipk-lookup [-h]
```

Pokud tedy bude program spuštěn bez parametrů nebo pouze s přepínačem *-h*, vypíše se na standartní vstup název programu, jeho autor, krátký popis a konvence klasického spuštění. Pokud je přepínač *-h* kombinován s libovolným dalším parametrem, program končí chybou.

Klasické spuštění

Toto spuštění má v případě úspěšného dotazu za následek vypsání jednodtlivých záznamů. Obecná konvence takového spuštění má tvar:

```
./ipk-lookup -s server [-T timeout] [-t type] [-i] name
```

Přepínač *-s* je povinný a stejně tak i jeho argument, který očekává IPv4 adresu DNS serveru, kam bude dotaz směřován.

Přepínač *-T* je nepovinný, avšak v případě jeho užití je nutné vyplnit i číselný argument, ten udává maximální dobu v sekundách, po kterou program čeká na odpověd z DNS serveru. Pokud v této době odpověd nepřichází, program končí chybou. V případě nevyužití tohoto přepínače je doba automaticky nastavena na 5 sekund.

Přepínač *-t* je nepovinný, ale stejně jako v případě přepínače *-T* je při jeho využití nutno napsat i jeho argument. Povolené argumenty jsou pouze *A*, *AAAA*, *NS*, *PTR* nebo *CNAME*. Ty specifikují typ dotazovaného záznamu. Pokud tento přepínač není použit, dotaz probíhá na typ *A*

Přepínač *-i* je nepovinný. Jeho funkce není implementována, proto běh programu nijak neovliní, avšak jeho existence byla zachována z důvodu dodržení konvece spuštění v zadání projektu.

Parametr *name* je povinný a udává doménové jméno k přeložení, vyjímku tvoří spuštění s dotazem na záznam PTR (*-t PTR*), kdy parametr očekává jako vstup IPv4 nebo IPv6 adresu.

Při úspěšném spuštení programu jsou na standartní výstup vypisovány (dílčí) odpovědi. Každý záznam je zapsán na novém řádku.

Návratové hodnoty

V případě úspěšného běhu programu je navrácena hodnota 0. V opačném případě je program ihned ukončen a vrací se buď hodnota 1 značící chybu za běhu nebo hodnota 2 značící chybu spuštění (nevhodné parametry). Současně se na standartní chybový výstup vypíše hláška ve formátu:

```
ERROR: <popis chyby v anglickém jazyce>
```

Zajimavé pasáže implementace

Timout dotazu

Timeout je řešen pomocí funce *setsockopt()* s parametrem *SO_RCVTIMEO*.

Zpětné dekodování jména

K tomotu účelu program využívá vlastní funkci ntohName(), která nejprve porovná, zda hodnota prvních dvou bytů je větší než 1100 0000 0000 0000. Tím je zjištěno, zda byl nebo nebyl využit odkaz. Pokud ano, je neznaménkové číslo 49152 od těchto bytů odečteno a jeho následná hodnota se uloží jako odskok od začátku zprávy. Pokud ovšem odkaz využit není, pracuje se se jménem úplně stejně, jen hodnota odskoku je nastavena tak, aby odpovídala následujícímu bytu po těchto dvou již přečtených.

Každý následující byte je porovnáván s honotou 0, ta ukončí čtení, a také s hodnoutou větší než 1100 0000, což značí využití odkazu. V tento moment funkce využívá rekurzivní volání sama sebe.

Funkce poté přesouvá znaky z odpovědi do nového řetězce, kde nahrazuje délky doménových úrovní tečkou, samozřejmě vyjma prvního znaku jména (pokud se současně nejedná o poslední).

Zdroj

1. MOCKAPETRIS, Paul. *RFC 135 - Domain names - implementation and specification* [online]. 1987-11 [cit. 2018-04-08]. Dostupné z https://tools.ietf.org/html/rfc1035