VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Dokumentace k projektu do predmetu IPK

DNS Lookup nástroj

9. dubna 2018

Stoika Anastasiia xstoik00@stud.fit.vutbr.cz

Obsah

1 Úvod **2**

2 Teorie **2**
2.1 Systém DNS (Domain Name System) 2
2.1.1 Architektura systému DNS 2
2.2 Přenos dat a komunikace v DNS 3
2.2.1 Formát hlavičky 3
2.2.2 Formát Question 4
2.2.3 Komprese paketů DNS 4
2.3 Záznamy DNS (Resource Records) 4
2.3.1 Formát záznamů 5
2.3.2 Přehled záznamů DNS 5

3 Implementace **5**
3.1 Zpracování vstupních parametrů 6
3.2 Komunikace nad UDP 6
3.3 Vytvoření DNS dotazu 6
3.4 Zpracování odpovědi 6
3.5 Omezení 6

4 Literatura **6**

1 Úvod

Úkolem projektu je nastudovat si detaily protokolu DNS a systému DNS obecně. Na základě nastudovaných informací naprogramovat C/C++ nástroj, který se za pomoci síťové knihovny BSD sockets dotazuje systému DNS a realizuje překlad doménových jmen a IP adres.

2 Teorie

2.1 Systém DNS (Domain Name System)

Základním úkolem služby DNS je mapování (převod) doménových adres (např. www.fit.vutbr.cz) na IP adresy (147.229.9.23). Služba DNS obsahuje databázi všech doménových adres a příslušných IP adres. Definuje také, jak budeme přistupovat k těmto datům. Databáze je distribuovaná na více počítačů, kde běží nameservery. IP adresu zjišťujeme z doménového jména dotazem na server DNS. Proces vyhledávání v systému DNS nazýváme rezoluci (name resolution).

2.1.1 Architektura systému DNS

Architektura systému DNS se skládá z:

- **prostoru doménových jmen** (mapování (nejen) doménových adres na IP adresy)

  Systém DNS tvoří databáze hierarchicky uspořádaná jako kořenový strom doménových jmen. Kořen stromu DNS se nazývá the root. Uzly stromu jsou pojmenovány textovým řetězcem (bez teček) délky max. 63 znaků (někdy se uzlům říká domény). Jednou z funkcí systému je reverzní mapování IP adres na doménové jméno. V datovém prostoru DNS je jedna speciální doména, jejíž uzly jsou pojmenovány čísly reprezentujícími IP adresu ve čtyřbytovém dekadickém formátu odděleným tečkami (například 147.229.8.12). Doména, ve které jsou tyto IP adresy uloženy, se nazývá in-addr.arpa. . Záznam DNS pro IP adresu 147.229.8.12 bude vypadat takhle 12.8.229.147.in-addr.arpa. Pro mapovani IPv6 adres na doménové adresy se používá doména ip6.arpa .

- **serverů DNS**

  Základním úkolem DNS serveru je odpovídat na dotazy směřující na databází DNS. Server DNS uchovává data ve formě množiny záznamů DNS (resource records). Záznamy jsou uloženy v lokálním souboru nebo si je server načte z jiného serveru DNS pomocí přenosu zón.

  Typy serverů DNS: primární (úplně (autoritativní) záznamy o doménách, které spravuje), sekundární (autoritativní kopie dat od primárních serverů), záložní (pouze přijímá dotazy, které předává dalším serverům DNS; ukláda odpovědi do vyrovnávaci paměti; poskytuje neautoritativní odpovědi).

- **resolveru** (přístup k datům, vyhledávání)

  Rezoluce je proces hledání odpovědi v systému DNS. Komunikace typu klient - server. Využívá stromovou strukturu jmen (DNS root server). Dva typy dotazů: rekurzivní a iterativní.

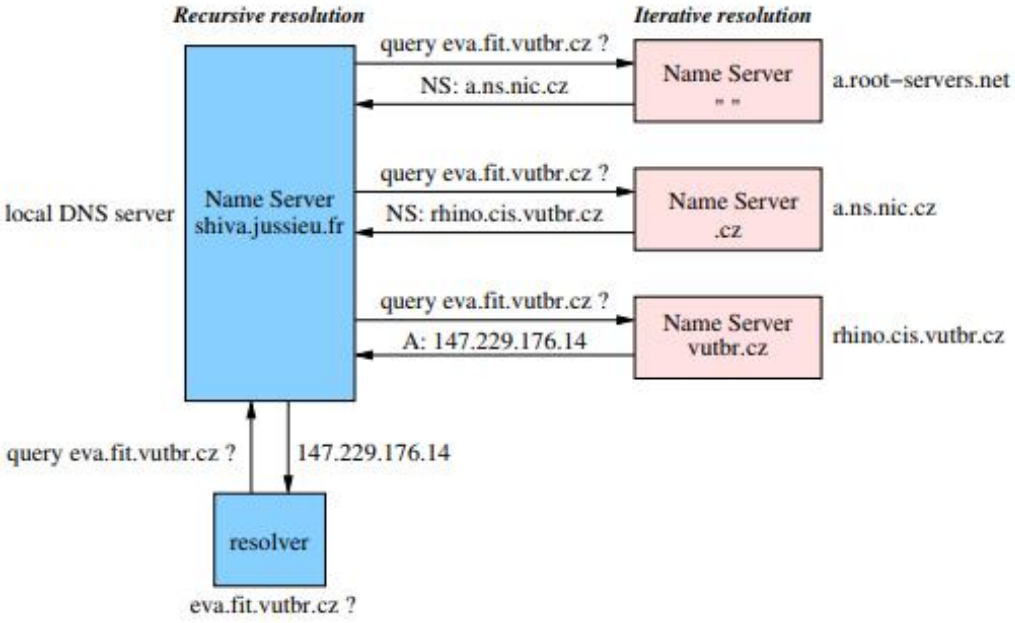
  Rekurzivní dotaz: pokud server nezná odpověď, ptá se dalších serverů. Resolver zašle dotaz na určitý údaj ve stromu DNS konkrétnímu serveru DNS. Server DNS musí odpovědět na dotaz buď požadovanými daty nebo chybovou hláškou, když například nezná odpověď. Pokud server není autoritativní pro hledaná data, musí se zeptat dalších serverů a najít autoritativní odpověď. Může poslat rekurzivní dotaz na některý z autoritativních serverů a čekat na odpověď. Nebo může poslat iterativní dotaz a získat odkaz na jiný server, který zná odpověď. Zda server podporuje rekurzivní či iterativní dotazování záleží na jeho konfiguraci.

  Iterativní dotaz: server vratí nejlepší možnou odpověď. Pokud nezná odpověď, odpoví chybou. Pošle odkaz na server, který může znát odpověď. Iterativní dotazy šetří práci na straně serveru DNS. Při tomto

dotazování vrátí server resolveru nejlepší odpověď, kterou může dát. Více se nedotazuje. Dotazovaný server DNS se podívá do své lokální databáze. Pokud nenajde odpověď, vrátí adresy serverů, které jsou nejblíže hledané adrese.

Příklad vyhledání záznamu v DNS je dobře znazorněn na obrázku 1.

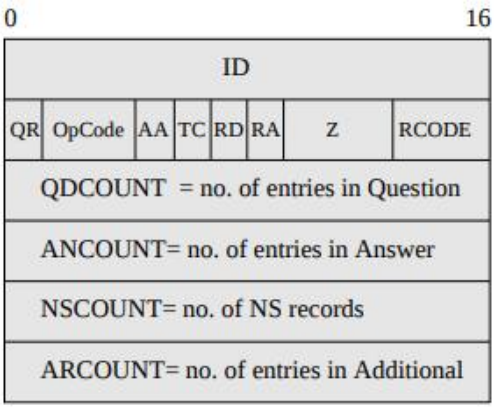
Obrázek 1: Vyhledání záznamu v systému DNS



2.2 Přenos dat a komunikace v DNS

Protokol DNS používá pro posílání dotazů transportní protokol UDP s číslem portu 53. Velikost paketů UDP je standardem DNS omezena na 512 bytů. Delší zprávy je nutné rozdělit do více paketů přenášených nad UDP pomocí bitu TC (TrunCation) v hlavičce protokolu DNS, která je detailně znázorněna na obrázku 2.

Obrázek 2: Hlavička DNS



2.2.1 Formát hlavičky

- ID - 16-bitový identifikátor, přiřazený dotazujícím programem

- QR - 1-bitové pole specifikující typ zprávy: query(0), response(1)
- Opcode - 4-bitové pole specifikující typ dotazu: 0 pro standardní dotáz
- AA - Authoritative Answer
- TC - TrunCation, specifikuje jestli zpáva byla rozdělena na několik částí
- RD - Recursion Desired, je-li nastaven tento bit, server bude dotazovat rekurzivně
- RA - Recursion Available, tento bit je nastaven v odpovědi, pokud server podporuje rekurzivní dotazování
- Z - rezervovaný bit
- RCODE - Response Code, 4-bitové pole je součástí odpovědi, 0 v připadě ze nejsou žádné chyby
- QDCOUNT - počet otázek
- ANCOUNT - počet odpovědí
- NSCOUNT - number of name server resource records
- ARCOUNT - number of resource records in the additional records section

2.2.2 Formát Question

- QNAME - doménové jméno, ukládá se jako posloupnost dvojic délka/hodnota. Každá dvojice obsahuje délku domény a název domény. Tato posloupnost dvojic je ukončena nulovým oktetem.
- QTYPE - specifikuje typ záznamu
- QCLASS - specifikuje třídu záznamu, například IN pro Internet

2.2.3 Komprese paketů DNS

Při vytváření paketů DNS dochází ke komprimování textových dat. Tato činnosti je vhodná, protože některé řetězce se v paketu DNS opakují, například jména doména apod. Proto se místo výskytu jména používá ukazatel na první výskyt řetězce.

Doménové jméno se ukládá jako posloupnost dvojic délka/hodnota. Každá dvojice obsahuje délku domény a název domény. Tato posloupnost dvojic je ukončena nulovým oktetem. Například doménové jméno ”eva.fit.vutbr.cz” se v paketu DNS zapíše jako řetězec znaků ”3 eva 3 fit 5 vutbr 2 cz 0”, kde první byte označuje délku řetězce, který následuje. Posloupnost je ukončena nulovým řetězcem, což je vlastně název kořenového uzlu ve stromu jmen DNS.

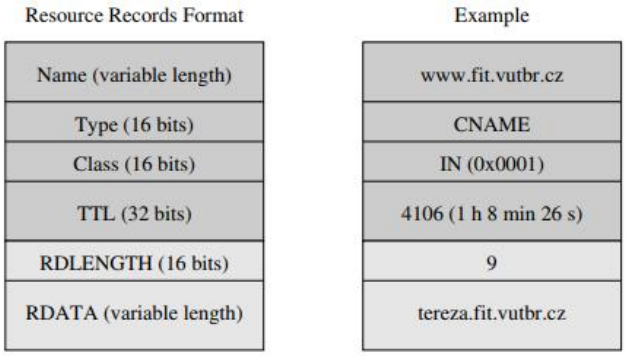
2.3 Záznamy DNS (Resource Records)

Pro ukládání informací v datovém prostoru DNS slouží záznamy DNS (resource records, RR). Záznamy jsou uloženy v textové podobě v zónových souborech na serverech DNS. Nejběžnější jsou záznamy typu A, které mapují doménové jméno na IP adresu (tzv. přímé mapování) a záznamy typu PTR pro opačné (reverzní) mapování.

2.3.1 Formát záznamů

Všechny typy záznamů DNS mají stejný obecný formát definovaný standardem RFC 1035. Formát záznamů obsahuje položky NAME, TYPE, CLASS, TTL, RDLENGTH a RDATA. Každý záznam DNS obsahuje všechny uvedené položky. Položka RDATA se liší podle typy záznamu, kde pro daný typ (např. A či PTR) obsahuje odpovídající informace. Struktura záznamu je s příkladem na obrázku 3. Položka Name obsahuje jméno uzlu ve stromu DNS, kde je daný záznam uložen. Položka Type určuje typ záznamu (např. CNAME), Class definuje třídu záznamu, TTL maximální dobu platnosti záznamu. Pokud je hodnota TTL nastavena na 0, což je běžné například pro záznamy SOA, záznam nesmí být uložen v paměti cache. Pole RDLENGTH a RDATA obsahují hodnotu záznamu, na kterou se obvykle ptáme.

Obrázek 3: Formát záznamu s příkladem.



2.3.2 Přehled záznamů DNS

Každý překlad DNS lze jednoduše popsat jako mapování (funkci), která převádí jeden typ informace na jiný. Pro správné využití systému DNS je nezbytné správně rozlišit jednotlivé typy mapování. Přehled záznamu je uveden na obrázku 4.

Obrázek 4: Příklady záznamů DNS

Záznam	Mapování	Příklad
A	doménové jméno → IP adresa	tereza.fit.vutbr.cz → 147.229.9.22
PTR	IP adresa → doménové jméno	22.9.229.147.in-addr.arpa. → tereza.fit.vutbr.cz.
NS	doména → doménový server	fit.vutbr.cz. → gate.feec.vutbr.cz.
MX	doména → poštovní server	fit.vutbr.cz. → kazi.fit.vutbr.cz.
SOA	doména → identifikace správce	fit.vutbr.cz. →boco.fee.vutbr.cz. michal.fit.vutbr.cz. 200710032 10800 3600 604800 86400
CNAME	doménové jméno → doménové jméno	www.fit.vutbr.cz. → tereza.fit.vutbr.cz.
AAAA	doménové jméno → IPv6 adresa	www.cesnet.cz. → 2001:718:1:101:204:23ff:fe52:221a
PTR	IPv6 adresa → doménové jméno	a.1.2.2.2.5.e.f.f.f.3.2.4.0.2.0.1.0.1.0.1.0.0.0.8.1.7.0.1.0.0.2.ip6.arpa. → www.cesnet.cz.

3 Implementace

V dané sekci budou ukázany vlastní návrh a implementace klientské aplikace realizující dotazování na DNS server a překlad doménových jmén a IP adres. Pro účelu projektu byly vytvořeny pomocné datové struktury pro snazší sestavení dotazu, respektive rozparsování odpovědi: datová struktura realizující hlavičku DNS, struktura pro dotaz a také struktura pro záznam (Resource Record). Parsování přichozích paketů je implementováno pomocí přetypování přichozího paketů na různé struktury a posuvů v obdržených datách.

3.1 Zpracování vstupních parametrů

Pro parsování vstupních parametrů byla vyrvořena funkce **getParams()** využívající funkce getopt(). Funkce **getParams()** vrací naplněnou strukturu typu TParams.

3.2 Komunikace nad UDP

Jelikož úkolem je vytvoit nástroj, který se dotazuje systému DNS za pomoci síťové knihovny BSD sockets, pro vytvoření schránky byla použita funkce socket(). Pro vyměnu dat mezi klientem a serverem jsou použity funkce sendto() a recvfrom(). Pro uzavení schránky je použitá funkce close().

3.3 Vytvoření DNS dotazu

Prvním krokem bylo zaplnění datové struktury DNS hlavičky daty podle rozparsovaného dotazu zadaného uživatelem programu. Data jsou postupně umíštovány do buffru. Nasledujícím krokem je zaplnění struktury pro dotáz. Před vyplněním položky QNAME, doménové jméno je konvertováno podle uvedených výše popisů formátu jména. Dotazuje-li se na záznam typu PTR, je provedená konvertace IPv4/IPv6 adres pomocí vlastních implementovaných funkcí **invertipv4()** a **invertipv6()**. Po následném vyplnění typu záznamu a třídy, paket je odeslan na server DNS pomocí funkce sendto().

3.4 Zpracování odpovědi

Pomocí funkce recvfrom() se dostane příchozí odpověď' od DNS serveru. Odpověď' (paket) je postupně rozparsován pomocí přetypovaní. Na začátku se přetypuje na strukturu DNS hlavičky, ze které zjistime informace, například kolik bylo nalezeno odpovědí. Po analýze přichozí hlavičky, se udělá posuv o velikost datove struktury dns_header. Dalším krokem je získání jména NAME z odpovědi. Pro týto účely byla vztvořena funkce **get_dns_name()** konvertující jméno z formátu pro DNS na uživatelem čitelný formát. Podle uvedených informací v předchozí kapitole, to je bud' jméno, nebo odkáz na jméno kvůli komprese dat. V takovém případě se provede skok na místo, kde je požadované jméno. Dalším krokem je posuv v paketu o delku jména, a přetypování dat na datovou strukturu resourceRecord. Takovým zpusobém se dozvíme typ přichozího záznamu. Posledným krokem je posuv o velikost této struktury a získání samotné odpovědi na uživatelem zadanou otázku. Pro konvertaci odpovědi je také použitá funkce **get_dns_name()**.

3.5 Omezení

V projektu není implementováno iterativní dotazování a timeout. Také vypis sekcí Authority a Additional.

4 Literatura

- P. Mockapetris, RFC 1035: Domain names - implementation and specification, `https://tools.ietf.org/html/rfc1035`.
- Ing. Petr Matoušek, Ph.D., M.A., ISA - přednáška Systém DNS.
- Opora do předmětu ISA - Kapitola 3, Systém DNS.