

DNS Monitor Projektová dokumentácia

Jakub Pogádl

November 18, 2024

Vypracoval: Jakub Pogádl
Univerzita: VUT
Fakulta: VUT FIT

Contents

1	Úvod	3
2	Popis problematiky	3
2.1	DNS (Domain name system)	3
2.2	Typy záznamov	3
2.3	Štruktúra DNS paketu	3
3	Návrh a implementácia	4
3.1	Štruktúra programu	4
3.2	Zachytávanie paketov	4
3.3	Spracovanie paketov	4
3.4	Zápis do súborov	4
3.5	Ukážka v kóde	4
3.6	Podporované záznamy	5
4	Závislosti	5
5	Používanie	5
5.1	Kompilácia	5
5.2	Spustenie	6
5.3	Argumenty príkazového riadku	6
5.4	Príklad použitia	6
6	Testovanie	6
6.1	Práca s pamäťou	7
6.2	Testovanie funkčnosti	7
7	Použité zdroje	9

1 Úvod

Tento dokument popisuje implementáciu a funkcionality projektu DNS Monitor. Hlavným cieľom aplikácie je zachytávať a analyzovať DNS pakety, extrahovať relevantné informácie, ako sú doménové mená a IP adresy. Program využíva knižnicu `pcap` na zachytávanie paketov a spracováva DNS správy prenášané prostredníctvom protokolov IPv4 a IPv6 cez UDP.

2 Popis problematiky

2.1 DNS (Domain name system)

DNS je systém, ktorý umožňuje priradiť k číselnej IP adrese meno domény. Používa porty TCP/53 i UDP/53 a je definovaný v RFC1035. Servery DNS sú organizované hierarchicky, rovnako ako sú hierarchicky tvorené názvy domén. Systém DNS umožňuje efektívne udržiavať decentralizované databázy doménových mien a ich preklad na IP adresy.

2.2 Typy záznamov

- **A záznam** mapuje doménu na IPv4 adresu
- **AAAA záznam** mapuje doménu na IPv6 adresu
- **CNAME záznam** zabezpečuje, že jeden názov domény je aliasom pre iný
- **MX záznam** alebo mail exchange záznam mapuje meno domény na zoznam mail exchange serverov pre danú doménu
- **PTR záznam** funguje opačne ako A záznamy. Používajú sa na prepojenie IP adresy s názvom domény, namiesto prepojenia názvu domény s IP adresou.
- **NS záznam** určuje, ktoré servery sú autoritatívne DNS servery pre danú doménu
- **SOA záznam** uchováva dôležité administratívne informácie o doméne. Tieto informácie môžu zahŕňať e-mailovú adresu správcu domény, informácie o aktualizáciách domény a čas, kedy by mal server obnoviť svoje informácie.
- **SRV záznam** je zovšeobecnený záznam o lokalizácii služby.

2.3 Štruktúra DNS paketu

- **Header:**
 - ID (16 bitov)
 - FLAGS (16 bitov)
 - QDCOUNT (16 bitov)
 - ANCOUNT (16 bitov)
 - NSCOUNT (16 bitov)
 - ARCOUNT (16 bitov)
- **Question:**
 - QNAME (variable)
 - QTYPE (16 bitov)
 - QCLASS (16 bitov)
- **Resource record (Answer, Authority, Additional):**
 - NAME (variable)
 - TYPE (16 bitov)
 - CLASS (16 bitov)

- TTL (32 bitov)
- RDLENGTH (16 bitov)
- RDATA (variabilná dĺžka)

3 Návrh a implementácia

3.1 Štruktúra programu

Projekt je štrukturovaný do 2 častí:

- **dns-monitor** - Hlavná časť aplikácie zodpovedná za spracovanie DNS paketov.
- **ArgumentParser** - Modul, ktorý sa zaoberá spracovaním vstupných argumentov a ich uložením do príslušnej štruktúry.

3.2 Zachytávanie paketov

Program zachytáva všetky pakety pomocou funkcie `pcap_loop`, ktorá je volaná na základe toho, či je špecifikovaný súbor alebo sieťové rozhranie.

3.3 Spracovanie paketov

Po zachytení paketu funkcia `packetHandler` vykonáva nasledujúce kroky:

1. **Kontrola protokolu a portu:** Funkcia skontroluje, či je paket UDP a či je cieľový port 53.
2. **Extrahovanie DNS hlavičky:** Funkcia extrahuje DNS hlavičku z paketu.
3. **Spracovanie DNS odpovedí:** Funkcia `parseSection` prechádza cez jednotlivé sekcie paketu a zapisuje domény a IP adresy do súborov.
4. **Ukladanie výsledkov:** Výsledky sú uložené do reťazca `section`.

3.4 Zápis do súborov

Program zapisuje výsledky do súborov, ak sú špecifikované v argumentoch príkazového riadku:

1. **Otvorenie súborov:** Ak sú špecifikované súbory pre domény alebo preklady, program ich otvorí na zápis.
 - Súbor pre doménové mená je špecifikovaný argumentom `-d <domainsfile>`.
 - Súbor pre preklady doménových mien je špecifikovaný argumentom `-t <translationsfile>`.
2. **Uzavretie súborov:** Po spracovaní všetkých paketov program uzavrie všetky otvorené súbory.

3.5 Ukážka v kóde

Štruktúra `dnsAnswer` slúži na ukladanie informácií o DNS odpovedi.

```
#pragma pack(push, 1)
struct dnsAnswer {
    uint16_t type;
    uint16_t answer_class;
    uint32_t ttl;
    uint16_t rdlength;
};
#pragma pack(pop)
```

Funkcia `parseSection` spracováva DNS odpovede na základe typu záznamu a pridáva ich do reťazca `section`. Nasledujúci kód ukazuje, ako sa spracováva záznam typu `CNAME`:

```

case 5: // CNAME
    extractDomainName(packet, offset, result, dns_header_offset);
    offset += calculateDomainLength(packet, offset, dns_header_offset);
    section += domain_name + " " + std::to_string(answer_ttl) + " " + class_str + " " + type
    break;

```

3.6 Podporované záznamy

- **A záznamy:** Extrahuje IPv4 adresu.
- **AAAA záznamy:** Extrahuje IPv6 adresu.
- **NS, CNAME:** Extrahuje doménové meno.
- **MX:** Extrahuje doménové meno a prioritu.
- **SOA:** Extrahuje doménové meno, zodpovednú schránku, sériové číslo, intervaly obnovy, retry, expirácie a minimálny TTL.
- **SRV:** Extrahuje prioritu, váhu, port a doménové meno.

4 Závislosti

Na kompiláciu a spustenie programu `dns-monitor` sú potrebné nasledujúce knižnice a nástroje:

- `libpcap`
- `g++`
- `make`
- `cstring`
- `unistd.h`
- `netinet/ip.h`
- `netinet/udp.h`
- `ctime`
- `arpa/inet.h`
- `netinet/if_ether.h`
- `netinet/ip6.h`
- `fstream`
- `map`
- `set`
- `csignal`
- `iomanip`

5 Používanie

5.1 Kompilácia

Na kompiláciu programu použijete nasledujúci príkaz:

```
make
```

5.2 Spustenie

Spustiť program je možné s nasledujúcimi argumentmi:

```
./dns-monitor (-i <interface> | -p <pcapfile>) [-v] [-d <domainsfile>] [-t <translationsfile>]
```

5.3 Argumenty príkazového riadku

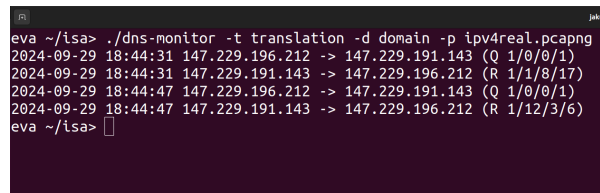
- **-i <interface>**: Špecifikuje sieťové rozhranie, na ktorom sa budú zachytávať pakety v reálnom čase. Tento argument je povinný, ak nie je špecifikovaný pcap súbor.
- **-p <pcapfile>**: Špecifikuje pcap súbor, z ktorého sa budú spracovávať pakety. Tento argument je povinný, ak nie je špecifikované sieťové rozhranie.
- **-v**: Voliteľný argument, ktorý zapne podrobné výpisy (verbose mode). Program bude vypisovať viac informácií o spracovávaní paketov.
- **-d <domainsfile>**: Voliteľný argument, ktorý špecifikuje súbor, do ktorého sa budú zapisovať domény.
- **-t <translationsfile>**: Voliteľný argument, ktorý špecifikuje súbor, do ktorého sa budú zapisovať preklady IP adries.

5.4 Príklad použitia

```
./dns-monitor -d domain -t translation -i eno1 -v
```

6 Testovanie

Program bol vyvíjaný a testovaný na operačnom systéme Ubuntu 22.04.5 LTS. K testovaniu boli použité nástroje Wireshark a dig. Testovanie prebiehalo aj na školských serveroch **eva** a **merlin**, kde bolo možné testovať len čítanie z pcap súborov.



```
eva ~/isa> ./dns-monitor -t translation -d domain -p ipv4real.pcapng
2024-09-29 18:44:31 147.229.196.212 -> 147.229.191.143 (Q 1/0/0/1)
2024-09-29 18:44:31 147.229.191.143 -> 147.229.196.212 (R 1/1/8/17)
2024-09-29 18:44:47 147.229.196.212 -> 147.229.191.143 (Q 1/0/0/1)
2024-09-29 18:44:47 147.229.191.143 -> 147.229.196.212 (R 1/12/3/6)
eva ~/isa>
```

Figure 1: Príklad testovania na serveri **eva**.


```
jakub@jakubpc: ~/VUT/isa2$ sudo ./dns-monitor -d domain -t translation -i eno1 -v
[sudo] password for jakub:
Timestamp: 2024-11-18 19:17:55
SrcIP: 147.229.196.212
DstIP: 147.229.191.143
SrcPort: UDP/56759
DstPort: UDP/53
Identifier: 53b5
Flags: QR=0, Opcode=0, AA=0, TC=0, RD=1, RA=0, AD=0, CD=0, RCODE=0

[Question Section]
www.google.com IN SOA
=====
Timestamp: 2024-11-18 19:17:55
SrcIP: 147.229.191.143
DstIP: 147.229.196.212
SrcPort: UDP/53
DstPort: UDP/56759
Identifier: 53b5
Flags: QR=1, Opcode=0, AA=0, TC=0, RD=1, RA=1, AD=0, CD=0, RCODE=0

[Question Section]
www.google.com IN SOA

[Authority Section]
google.com 60 IN SOA ns1.google.com dns-admin.google.com 696456648 900 900 1800 60
=====
jakub@jakubpc: ~/VUT/isa2$
```

```
jakub@jakubpc: $ dig www.google.com SOA
; <<> DLG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<> www.google.com SOA
;; global options: +cmd
;; Got answer:
;; -->HEADER<< opcode: QUERY, status: NOERROR, id: 38291
;; Flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.com. IN SOA
;; AUTHORITY SECTION:
google.com. 60 IN SOA ns1.google.com. dns-admin.google.com. 696456648 900 900 1800 60
;; Query time: 11 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Nov 18 19:17:55 CET 2024
;; MSG SIZE rcvd: 93
jakub@jakubpc: $
```

Figure 4: Overenie funkčnosti pomocou dig.

7 Použité zdroje

References

- [1] HUAWEI: DNS. [online], [vid. 2024-11-18]. URL <https://info.support.huawei.com/info-finder/encyclopedia/en/DNS.html>
- [2] NIC CZ: O doménách a DNS. [online], [vid. 2024-11-18]. URL <https://www.nic.cz/page/312/o-domenach-a-dns/>
- [3] IBM: DNS Records. [online], [vid. 2024-11-18]. URL <https://www.ibm.com/topics/dns-records>
- [4] HUAWEI: DNS. [online], [vid. 2024-11-18]. URL <https://support.huawei.com/enterprise/en/doc/ED0C1100174721/f917b5d7/dns>
- [5] IETF: RFC 1035 - Domain Names - Implementation and Specification. [online], [vid. 2024-11-18]. URL <https://datatracker.ietf.org/doc/html/rfc1035>