Počítačové komunikace a sítě 2019/2020

Sniffer paketů

Daša Nosková (xnosko05)

Obsah

Kapitola 1

Úvod

Cieľom projektu je vytvoriť sieťový analyzátor, ktorý na danom porte zachytáva a filtruje pakety. Program zachytáva každý paket vyhovujúci filtrom na danom sieťovom rozhraní.

1.1 Paket

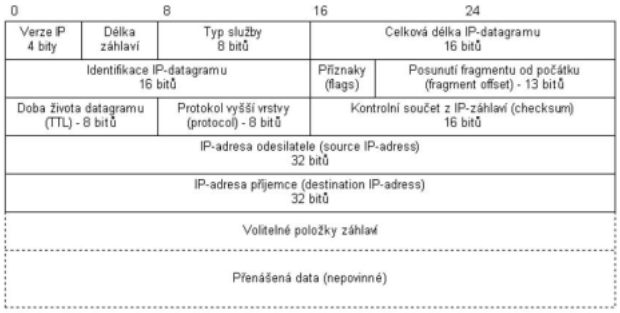
Pakety prenášajú dáta rôznej dĺžky z jedného počítača na druhý. Dáta sú prenašané cez viac vrstiev, pričom pri každej vrstve sa pripoja k paketu nové informácie. Internet využíva na prenos paketov protokol TCP/IP, ktorý sa skladá zo 4 vrstiev: linková a fyzická vrstva, IP, TCP/UDP, aplikačná vrstva.[1]

1.1.1 Fyzická a linková úroveň

Ethernet obsahuje 6 bajtovú linkovú adresu príjemcu a adresu odosielatela, pole špecifikujúce protokol sieťovej vrstvy a špecifikáciu protokolu. [1]

1.1.2 Sieťová úroveň

Internet protokol, IP, reprezentuje sieťovú vrstvu. Prenáša IP-datagramy, ktoré sa skladajú zo záhlavia a prenášaných dát. Záhlavie má spravidla 20 B a obsahuje informácie napríklad o IP adresách príjemcu a odosielateľa.[1]



Obr. 1.1: IP datagram
[1]

1.1.3 Transportná úroveň

Transportná vrstva sa skladá z protokolov TCP a UDP zaistujúcich spojenie medzi aplikáciami na 2 počítačoch. TCP potvrdzuje príjmané dáta, UDP nie.[1] Každý protokol má priradené číslo, tj. pre TCP = 6 a pre UDP = 17. Adresou je port.

Kapitola 2

Implementácia

Program je zložený zo súborov `ipk-sniffer.c, ipk-sniffer.h, filter.c, filter.h, error.h`.

Program začína parsovaním argumentov pomocou knižnice `argp.h`. Implicitne sú nastavené hodnoty parametrov ako na obrázku 2.

```
// default values of arguments
arguments.interface = NULL;
arguments.port = -1;
arguments.tcp = false;
arguments.udp = false;
arguments.num = 1;
```

Po dokončení spracovania argumentov sa zavolá funkcia sniff s priloženými argumentami a prípadnými filtrami. Vo funkcii `sniff()` sa otvorí rozhranie na ktorom sa budú zachytávať pakety, nastaví sa prípadný filter a začne sa zbierať určený počet paketov.

Vo funkcii `process_paket()` sa rozdelí paket na hlavičky jednotlivých vrstiev z ktorých sa extrahujú informácie, ktoré sú následne ako aj celý obsah paketu vypísané.

Funkcia `check_protocol()` skontroluje či ide o protokol TCP alebo UDP a daný typ predá ako parameter funkcii `get_port()`, ktorá vracia čísla portov príjmateľa a odosielateľa. V prípade ak protokol nie je TCP ani UDP, program vypíše upozornenie, a pokračuje ďalej.

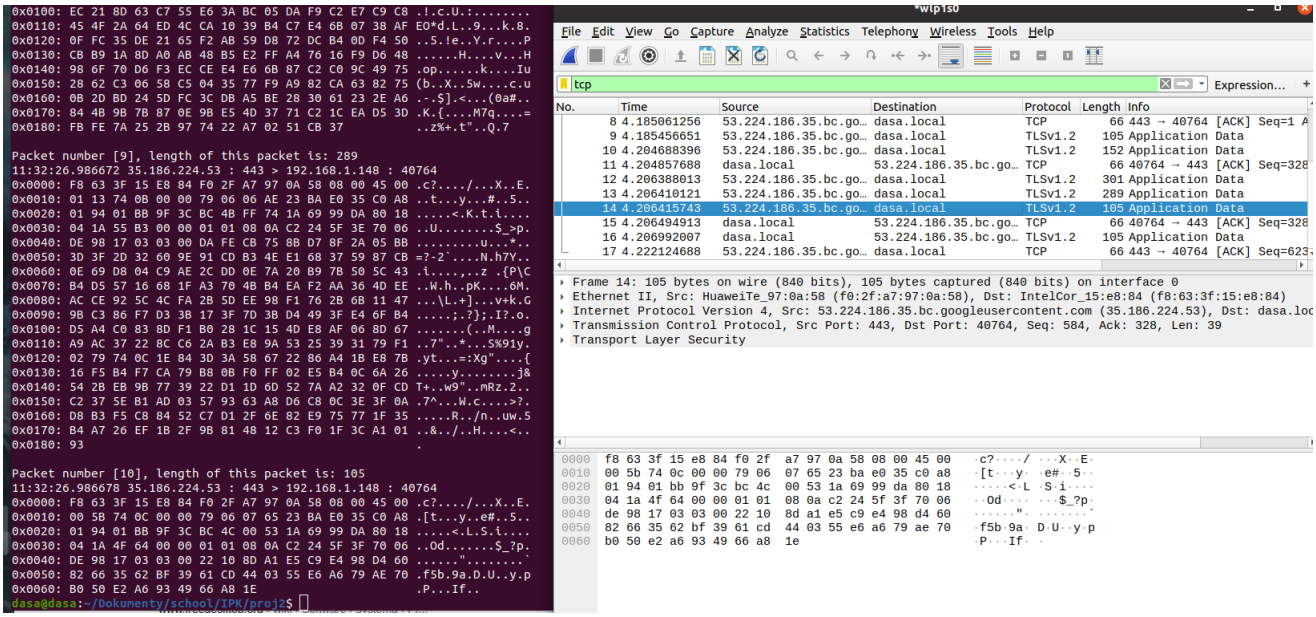
Funkcia `check_src_dst_addr()` vracia IP adresu príjmateľa a odosielateľa. V programe nie je implementovaný prevod IP adresy na doménové meno.

Celý obsah paketu sa vypisuje pomocou funkcie `print_packet()`, ktorá pri každom zavolaní vypíše 16 B z daného paketu a 16 znakov v ASCII. Konverzia hexadecimálneho čísla na ascii hodnotu zabezpečuje funkcia `convert_ascii()`.

Kapitola 3

Testovanie

Testovanie bolo vykonané porovnaním výpisom paketov s paketmi z programu `Wireshark`.



Obr. 3.1: Porovnanie paketov

Literatúra

[1] Klement, M.: *Technologie počítačových sítí – úvod do problematiky počítačových sítí.* Olomouc: Univerzita Palackého v Olomouci, druhé vydání, 2019, ISBN 978-80-244-5580-8.