VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ


Síťové aplikace a správa sítí – Dokumentace k projektu

# Aplikace pro získání statistik o síťovém provozu

Peter Stáhl (xstahl01)

# Kapitola 1 Úvod

Táto dokumentácia slúži ako komplexný popis návrhu, implementácie a funkcionality programu ISA-TOP. ISA-TOP je nástroj na monitorovanie siete, ktorý je určený na sledovanie a vizualizáciu prenosových rýchlostí pre jednotlivé IP adresy komunikujúce so zariadením, na ktorom je tento nástroj spustený. Cieľom aplikácie je poskytnúť užívateľom prehľad o aktuálnych sieťových aktivitách a umožniť im analyzovať výkon siete v reálnom čase.

# Kapitola 2  Obsah uvedenia do problematiky

Cieľom projektu ISA-TOP je vytvoriť efektívny nástroj, ktorý zobrazuje prenosové rýchlosti pre jednotlivé IP adresy komunikujúce so zariadením. Tento nástroj využíva knižnicu ‘libpcap’ na zachytávanie sieťového prevádzku a následne počíta prenosovú rýchlosť pre jednotlivé zachytené spojenia. Program funguje ako konzolová aplikácia, čo znamená, že štatistiky sú zobrazené priamo v termináli a pravidelne sa aktualizujú, čím poskytujú užívateľom aktuálne informácie o sieťovej prevádzke.

## 2.1  Zadanie projektu

Vytvorte nástroj ISA-TOP, ktorý zobrazuje aktuálne prenosové rýchlosti pre jednotlivé IP adresy komunikujúce so zariadením. Program po spustení začne zachytávať prevádzku na vybranom sieťovom rozhraní pomocou knižnice libpcap a počíta prenosovú rýchlosť pre každé zachytené spojenie. Aplikácia ponúka intuitívne používateľské rozhranie, ktoré umožňuje jednoduchú interakciu s užívateľom a poskytuje prehľadné zobrazenie štatistík.í.

# Kapitola 3 Návrh programu

Program má slúžiť na zobrazenie rýchlosti komunikácie v termináli medzi zariadením, na ktorom je spustení a ostatnými komunikujúcimi zariadeniami, v špecifikovanom rozhraní. Po spustení programu, je potrebné zachytiť prevádzku na špecifikovanom sieťovom rozhraní a vypočítať prenosovú rýchlosť pre každé zachytené pripojenie.

Pre dosiahnutie tejto funkcionality je potrebné problematiku atomizovať. Najvyššia abstrakcia programu pozostáva z 3 logických celkov. Odchytenie komunikácie, vytvorenie štatistiky komunikácie a zobrazenie štatistiky komunikácie. Tieto základné celky sú každé osobitné reprezentované prislúchajúcim model.

## 3.1 Odchytávanie komunikácie

Na úspešné odchytenie komunikácie je potrebné implementovať knižnicu špecializovanú na sieťovehé sniffera. Úlohou špecifikovaného sniffera je pasívne monitorovať špecifikované sieťové rozhranie a zachytávať výlučne pakety s potokolmi Transmission Control Protocol (TCP), User Datagram Protocol (UDP) a Internet Control Message Protocol (ICMP). Modul bude extrahovať kľúčové informácie z hlavičiek monitorovaných paketov , vrátane typu protokolov, zdrojovej IP adresy, cieľovej IP adresy a k nim prislúchajúce porty. Tento proces zabezpečí, že všetky relevantné dáta sú presne zaznamenané na ďalšie spracovanie

## 3.2 Vytvorenie štatistiky

Pre vytvorenie korektnej štatistiky je potrebné zvoliť jednotný formát, do ktorého bude modul zychátania komunikácie vedieť zapisovať informácie a modul zobrazenie tieto informácie zobraziť v správnom poradí. Tento formát musí umožniť rýchly prístup k potrebným údajom, aby ich zobrazenie na obrazovke bolo efektívne. Pre dosiahnutie tejto flexibility bude vhodné vytvoriť jedinečný kľúč pre každú konkrétnu komunikáciu, ktorá bude uložená v hash tabuľke. Takáto štruktúra zabezpečí rýchlu dostupnosť a efektívne vyhľadávanie štatistík, čím sa zlepší celková výkonnosť aplikácie pri spracovaní veľkého množstva dát.

## 3.3 Zobrazenie štatistiky

Očakávané zobrazenie štatistiky by malo byť prehľadné a intuitívne, aby užívateľ mohol jednoznačne vyčítať kľúčové informácie o komunikácii. Zobrazenie bude realizované konkrétnou knižnicou pre dynamické zobrazenie dát v termináli.

Úlohou tohto modulu bude vytvoriť grafické rozhranie organizované do prehľadnej tabuľky, ktorá jasne oddelí jednotlivé atribúty sieťovej komunikácie. Každý záznam v tabuľke bude obsahovať stĺpec pre zdrojovu adresu, cieľovú adresu, protokol, rýchlosť prijatých dát a rýchlosť odoslaných dát.

Na zabezpečenie dynamického a interaktívneho zobrazenia týchto štatistík bude použitá knižnica ncurses, ktorá umožní efektívne vykresľovanie tabuliek v termináli. Obrazovka sa bude pravidelne aktualizovať na základe nastaveného intervalu, pričom sa zabezpečí, že všetky zmeny v štatistikách budú okamžite viditeľné. Týmto spôsobom budú mať používatelia neustály prehľad o aktuálnych sieťových aktivitách a môžu rýchlo reagovať na akékoľvek nezrovnalosti alebo problémy v komunikácii.

# Kapitola 4 Popis implementácie

Implementácia systému na monitorovanie sieťovej komunikácie v programe ISA-TOP sa zameriava na efektívne zachytávanie a analýzu paketov, pričom kladie dôraz na modularitu a prehľadnosť kódu. Cieľom je atomizovať jednotlivé komponenty programu tak, aby sa zjednodušila ich údržba a rozšírenie. Využitie objektovo orientovaného programovania prostredníctvom tried prináša významné výhody, ako je enkapsulácia dát a metód, čo zvyšuje prehľadnosť a znižuje riziko vzniku chýb. Modularita umožňuje jednoduché pridávanie nových funkcií, ako sú podpora pre rôzne protokoly alebo filtre, bez nutnosti zásahov do existujúceho kódu.

## 4.1 Základná implementácia

Na začiatku implementácie je potrebné nastaviť základný rámec pre program. Program je spustený spolu so vstupnými argumentmi z príkazového riadka, pričom najdôležitejším argumentom, ktorý je vyžadovaný od užívateľa je názov sieťového rozhrania, ktoré bude monitorované. V prípade nesprávne zadaných argumentov aplikácia poskytne krátku nápovedu opisujúcu správne volanie programu a krátke objasnenie jednotlivých argumentov.

Pre zjednodušenie procesu výberu sieťového rozhrania som vytvoril funkciu ‘list_interfaces()’, ktorej úlohou je vypísať list dostupných sieťových rozhraní, ak nebolo zadané sieťové rozhranie. Táto funkcia silno inšpirovaná podľa internetového fórumu, spomenutého v zdrojoch. Implementuje systémové volanie ‘getifaddrs()’ importovaného knižnicou ‘ifaddrs.h’ . Toto volanie načítava zoznam všetkých dostupných sieťových zdrojov, ktoré sa nasledovne uložia do štruktúry ifaddrs. Podmienkou uloženia do štruktúry je aby rozhranie malo priradenú adresu typu IPv4.

## 4.2 Odchytávanie komunikácie

Odchytávanie komunikácii je implementované triedou ‘PacketCapture’ reprezentujúca navrhovaný sniffer. Ako už spomenuté úlohou tejto triedy je pasívne zachytávať pakety prichádzajúce a odchádzajúce cez zvolené sieťové rozhranie.

Na implementácia odchytávania komunikácie sa využíva knižnica ‘libpcap’, ktorá poskytuje rozhranie pre prístup k paketom na rôznych operačných systémoch.

### 4.2.1 Inicializácia odchytávania komunikácie

Pri vytváraní inštancie triedy ‘PacketCapture’ je potrebné, aby si trieda prevzala názov sieťového rozhrania a objekt triedy štatistík pre zápis odchytených informácií, prípadne ich aktualizáciu. Počas inicializácii inštancie trieda volá funkciu ‘pcap_open_live()’ z knižnice ‘libpcap’, ktorá otvára vybrané sieťové rozhranie na monitorovanie.

### 4.2.2 Zachytenie komunikácie

Zatiaľ čo predom spomenutá funkcia ‘pcap_open_live()’ otvára komunikáciu, jej zaznamenávanie začne až pri spustení cyklu ‘PacketCapture::start_capture()’. Počas vykonávania tohto cyklu začína spracovanie samotných paketov a pakety sa analyzujú. Táto činnosť sa vykonáva pomocou funkcie ‘PacketCapture::packet_handler()’, ktorá zisťuje podstatné informácie o pakete pre jeho správne definovanie. Kľúčovým aspektom definície paketu je rozpoznanie lokálnej IPv4 adresy v porovnaní s adresou komunikovaného zariadenia. Zásadným faktorom pre správne komunikovanie je, že každé sieťové rozhranie má odlišne definovanú lokálnu adresu a teda bolo nutné vytvoriť funkciu, ktorá dokáže zistiť lokálnu IPv4 adresu zo zadaného rozhrania.

Pri každom spracovaní paketu sa následne volá metóda ‘Stats::update()’, ktorá aktualizuje počty prenesených bajtov a počet paketov pre dané pripojenie.

## 4.3 Vytvorenie štatistiky

Vytvorenie štatistiky je kľúčovou spojovaciou zložkou programu. Reprezentuje ho trieda ‘Stats’, ktorá zodpovedá za zhromažďovanie a spracovanie údajov o prenose paketov, pričom sa využíva mutex multithreading metóda na zabezpečenie efektívneho a bezpečného prístupu k údajom.

Štatistiky sa uchovávajú do mapy štatistík, pričom každá obsahuje jedinečný kľúč pre pripojenie reprezentovaný dátovou štruktúrou, ktorá pozostáva zo zdrojovej IP adresy, cieľovej IP adresy a protokolu. V rámci mapy sa k jednoznačnému kľúču ‘ConnectionKey’ priradzujú samostatné metriky prenesených údajov. Tie sú reprezentované v dátovej štruktúre ‘ConnectionStats’ a uchovávajú metriky pre prichádzajúce a odchádzajúce rýchlosti. Implementácie teda využíva základný princíp hash tabuľky pomocou C++ konceptu unordered_map.

Keďže trieda štatistiky reprezentuje úložisko, do ktorého sniffer zapisuje a displej čítá údaje v reálnom čase, bolo potrebné zabezpečiť bezpečnú synchronizáciu prístupu k štatistikám, čím sa prechdáza proti problémom s race conditions. Vlákna teda zamykajú prístup k štatistikám v danom čase pomocou funkcie ‘Stats::lock_guard<mutex>’ počas zápisu alebo čítania štatistík. Vďaka tejto implementácii sa minimalizuje riziko nekonzistentných údajov pri súbežnej aktualizácii.

## 4.4 Zobrazenie štatistiky

Zobrazenie štatistiky ako posledná časť implementácia programu ISA-TOP zobrazuje a interaguje so samotným užívateľom. Logický celok je reprezentovaný triedou ‘Display’, ktorá zodpovedá za samotnú vizualizáciu a čítanie údajov v reálnom čase, pričom využíva knižnicu ‘ncurses’ na prehľadné zobrazenie informácii v terminálovom prostredí.

### 4.4.1 Inicializácia zobrazenia

Trieda ‘Display’ sa inicializuje s referenciou na objektu ‘Stats’, ktorý obsahuje aktuálne štatistiky, voliteľné argumenty ovplyvňujúce zobrazenie štatistiky ako je interval obnovenia, typ komunikácie a flag pre kontrolu behu aplikácie

### 4.4.2 Zobrazenie

Pre spustenie zobrazenia sa používa funkcia ‘Display::run()’ , ktora inicializuje prostredie vytvorené pomocou knižnice ‘ncurses’ a spúšťa displejové vlákno, ktorom beží zobrazovací cyklus ‘Display::display_loop()’. Jeho úlohou je nepretržite aktualizovať zobrazenie štatistík, predvoleným intervalom obnovenia. Vždy pri novom behu cyklu si funkcia zamkne prístup k štatistikám. Vďaka tejto mechanike sú zobrazené dáta konzistentné.

V rámci zobrazenie štatistiky sa implementuje zobrazenie maximálne 10 najrýchlejších komunikácii, pričom v rámci tejto komunikácia bolo potrebné zlúčiť kľúče, kde sa zhodujú prevrátené hodnoty cieľovej a zdrojovej IP adresy.

Ak si užívateľ želá opustiť program dokáže stlačiť klávesu q, ktorá nastaví flag pre beh programu na false a začne ukončenie programu.

# Kapitola 5 Základné informácie o programe

Program ISA-TOP je nástroj určený na monitorovanie a analýzu sieťovej komunikácie. Jeho hlavnou funkciou je pasívne zachytávať pakety prenášané cez zvolení sieťové rozhranie a zhromažďovať štatistiky o prenose dát. Program je napísaný v jazyku C++ a využíva knižnice ‘libpcap’ na zachytávanie paketov a ‘ncurses’ na vizualizáciu údajov v terminálovom prostredí pomimo iných systémových knižníc C++.

# Kapitola 6 Návod na použitie

Program ISA-TOP je možné spustiť z príkazového riadka. Tu sú základné kroky na jeho použitie:

## 6.1 Rekvizity

Pre správnu kompiláciu programu je potrebné mať nainštalované spomínané knižnice ‘libpcap’, ‘ncurses’ a nástroj cmake

## 6.2 Kompilácia programu

Program je možné skompilovať pomocou príkazu “make”, ktorý vykoná všetky potrebné kroky pre vytvorene build adresáru, samotného skompilovania kodu

Počas tohto kroku si môže vypýtať program heslo k adminovi. Čo záleží od prístupu a užívateľa. Je to z dôvodu, že Makefile vykonáva príkaz :

```
sudo setcap cap_net_raw=eip ./isa-top
```

Tento príkaz poskytuje možnosť používať surové sockety, čo umožňuje progamu priamo odosielať a prímať sieťové pakety.

## 6.3 spustenie programu

Po úspešnej kompilácii sa program dokáže nasledovne spustiť :

```
./isa-top -i <názov_rozhrania> [-s <b|p>] [-t <čas>]
```

Kde -i parameter špecifikuje rozhranie, -s špecifikuje zoradenie podľa bytov alebo paketov, pričom predvolene bez zadania zoraďuje podľa bytov a -t špecifikuje interval v sekundách pre monitorovanie.

Po spustení programu sa začne monitorovanie vybraného sieťového rozhrania a zobrazovanie štatistík v reálnom čase. Program je možné ukončiť stlačením klávesy ‘q’.

# Kapitola 7 Testovanie

## 7.1 Popis testovania aplikácie

Testovanie aplikácie ISA-TOP bolo navrhnuté s cieľom zabezpečiť, že všetky komponenty fungujú správne a efektívne. Testy sa zamerali na kľúčové funkcie tried Stats, Display a vstupných argumentov, pričom každá trieda bola podrobená jednotkovým testom na overenie ich funkčnosti.

### 7.1.1 Testovanie triedy Stats

**UpdateAndRetrieveStats**: Testuje správnosť aktualizácie a načítania štatistík pre prenosové rýchlosti. Overuje, či sú hodnoty prenesených bajtov a paketov správne uložené a načítané.

**NoStatsInitially**: Overuje, že pri inicializácii triedy `Stats` nie sú k dispozícii žiadne štatistiky

### 7.1.2 Parsing argumentov

**alidArguments**: Testuje, či funkcia správne spracováva platné argumenty príkazového riadka.

**MissingInterface**: Overuje, že funkcia vyhodí výnimku, ak chýba argument pre sieťové rozhranie.

**InvalidSortOption**: Testuje, že funkcia vyhodí výnimku pri neplatnej možnosti triedenia.

**InvalidInterval**: Overuje, že funkcia vyhodí výnimku pri neplatnom intervale.

**NoArguments**: Testuje, že funkcia vyhodí výnimku, ak nie sú zadané žiadne argumenty.

### 7.1.3 Display

Triedu display bola testovaná čisto vizuálne, či zobrazuje dáta a či pri stlačení klávesy ‘q’ správne ukončí program.

## 7.2 Výsledky testov

Výsledky testovania potvrdili správnosť implementácie a stabilitu aplikácie ISA-TOP pre jednotlivé testy. Pre komponent Display po spustení aplikácie sa štatistiky zobrazovali v terminálovom prostredí. Hlavným cieľom bolo overiť, či sa údaje zobrazujú správne a či aplikácia reaguje na klávesové vstupy. Hoci neexistujú automatizované testy pre vizualizáciu, manuálne testovanie zabezpečilo, že užívateľské rozhranie je intuitívne a prehľadné.

ZDROJE

https://dev.to/fmtweisszwerg/cc-how-to-get-all-interface-addresses-on-the-local-device-3pki

https://www.tcpdump.org/manpages/

https://www.tcpdump.org/pcap.html

https://man7.org/linux/man-pages/man8/setcap.8.html

využitie ncruses bolo inšpirované mojím starším projektom, kde táto knižnica bola využívaná