Vysoké učení technické v Brně Fakulta informačních technologií

ISA - Sítové aplikace a správa sítí Aplikace pro získání statistik o sítovém provozu

Contents

1	$ m \acute{U}vod$	2
2	Implementace	2
	2.1 Datové struktury	2
	2.2 Vlákna	2
	2.3 Zachytávání paketů (libpcap)	2
	2.4 Správa spojení (hash tabulka)	2
	2.5 Výpočet statistik	2
	2.6 Uživatelské rozhraní (ncurses)	
3	Použití programu	3
	3.1 Kompilace	3
	3.2 Spuštění	3
4	Testování	3
	4.1 Ping a Wireshark	3
	4.2 Iftop	3
5	Literatura	3

1 Úvod

Tento dokument popisuje implementaci programu isa-top, který je využíván k zobrazení statistik o síťovém provozu v terminálu.

2 Implementace

Program je rozdělen do několika hlavních komponent:

2.1 Datové struktury

Program používá následující klíčové datové struktury:

- connection_key_t identifikace spojení (zdrojová/cílová IP, porty, protokol)
- connection_stats_t statistiky spojení (počty bajtů, paketů, rychlosti)
- Hash tabulka pro ukládání aktivních spojení

2.2 Vlákna

Z důvodu optimálního a správného výpisu jsou zde využity 2 vlákna vytvořeny pomocí funkce pthread_create. Tedy jedno vlákno pro výpočet statistik a druhé pro jejich zobrazování pomocí knihovny ncurses.

2.3 Zachytávání paketů (libpcap)

Zde je využívana knihovna libpcap, která umožňuje sledovat pakety v síti. Funkce create_pcap_handle inicializuje zachytávání na specifikovaném sítovém rozhraní a nastavuje potřebné parametry. Funkce packet_handler, která je v nekonečné smyčce pomocí pcap_loop, zpracovává pakety a následně z nich extrahuje informace pro pozdější použití.

2.4 Správa spojení (hash tabulka)

Každé spojení je identifikováno klíčem connection_key_t, který obsahuje zdrojovou a cílovou IP adresu, porty a protokol. Tato struktura umožnuje efektivně pracovat se spojeními, které se zde slučují do jedné v případě obousměrné komunikace. Funkce jako insert_or_update, find a delete jsou použity pro manipulaci se spojeními v hash tabulce. Když je zachycen nový paket, tato část kódu aktualizuje statistiky příslušného spojení nebo vytvoří nové spojení, pokud dosud neexistuje.

2.5 Výpočet statistik

Statistiky zahrnují počet přenesených bajtů a paketů, rychlost přenosu dat a rychlost přenosu paketů. Výpočet statistik se provádí v reálném čase na základě zachycených paketů. Funkce update_speed aktualizuje rychlosti přenosu dat a paketů pro každé spojení. Kód také zajišťuje, že statistiky jsou pravidelně aktualizovány a stará spojení jsou odstraněna, pokud nejsou aktivní.

2.6 Uživatelské rozhraní (ncurses)

Kód zobrazuje seznam aktivních spojení a jejich statistiky v přehledné tabulce. Funkce print_top_connections zobrazuje top 10 spojení s nejvyšší přenosovou rychlostí. Uživatelské rozhraní je pravidelně aktualizováno pomocí vlákna display_loop, aby zobrazovalo aktuální statistiky v reálném čase.

3 Použití programu

3.1 Kompilace

make

3.2 Spuštění

```
./isa-top -i <rozhraní> [-s b/p]
```

Parametry:

- -i síťové rozhraní
- -s b řazení podle bajtů/s (výchozí)
- -s p řazení podle paketů/s

4 Testování

Testování probíhalo 2 způsobmi.

4.1 Ping a Wireshark

Nejdříve jsem využíval nástroje ping, z několika různých terminálů. Komunikace byla odchytávána pomocí nástroje wireshark. Toto mi umožnilo určit zdá je zobrazován správný počet bajtů a paketů za sekundu.

4.2 Iftop

Pomocí nástroje Iftop, který je velmi podobný isa-top jsem mohl statistiky porovnat a určit zda se rychlosti podobají.

5 Literatura

- 1. https://vichargrave.github.io/programming/develop-a-packet-sniffer-with-libpcap/
- 2. Dokumentace knihovny libpcap
- 3. Dokumentace knihovny ncurses