**VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ**

**BRNO UNIVERSITY OF TECHNOLOGY**

**FAKULTA INFORMAČNÍCH TECHNOLOGIÍ**

**FACULTY OF INFORMATION TECHNOLOGY**

**ÚSTAV INFORMAČNÍCH SYSTÉMŮ**

**DEPARTMENT OF INFORMATION SYSTEMS**

**ANALYZÁTOR PAKETŮ**

**PACKET ANALYZER**

**PROJEKTOVÁ DOKUMENTACE**

**PROJECT DOCUMENTATION**

**AUTOR PRÁCE PETR BUCHAL**

**AUTHOR**

**BRNO 2017**

**Obsah**

[Úvod 0](#_Toc498940138)

[1.1 Motivace 0](#_Toc498940139)

[1.2 Cíl práce 0](#_Toc498940140)

[Návrh Aplikace 1](#_Toc498940141)

[Popis implementace 0](#_Toc498940142)

[Základní informace o programu 1](#_Toc498940143)

[4.1 Co to je normovaná stránka? 2](#_Toc498940144)

[Návod na použití 4](#_Toc498940145)

[Parametry programu 4](#_Toc498940146)

[Závěr 5](#_Toc498940147)

[Metriky kódu 5](#_Toc498940148)

[Literatura 6](#_Toc498940149)

**Kapitola 1**

# Úvod

V dnešní době prostupuje internet napříč téměř všemi sférami každodenního života a je tedy důležité, zabývat se tím, co sebou tato skutečnost nese. Běžného člověk většina věcí týkající se této záležitosti zajímat nemusí, stačí mu, aby to prostě fungovalo. Poté jsou zde ale lidé, jejichž prací je, zařídit právě, aby nebyla ohrožena efektivita, bezpečnost a obecně funkčnost internetu a potažmo všech sítí. Správa sítí je složitá disciplína, ale existuje spousta prostředků, které tuto činnost usnadňují. Každý informatik nicméně využívá ke své práci odlišné nástroje podle toho, které se na danou práci hodí nejlépe. Je tedy nápomocné, když tito lidé mají co největší počet kvalitních prostředků a mohou si vybrat opravdu ten, který je pro danou činnost nejlepší.

## 1.1 Motivace

Klíčový prvek sítí jako takových je skutečnost, že zařízení mezi sebou vzájemně komunikují. Posílají si zprávy různých typů a ty poté interpretují. Co ale když nastane nějaký problém v síti a je třeba zjistit jeho příčinu? Jednou z variant při pátrání po chybě je právě analýza paketů, tedy zpráv, které směřují přes síťovou kartu do zařízení a ze zařízení. Jenže bez nějakého podpůrného prostředku se jedná pouze o binární informace, které člověk nepřečte. Zde se nabízí možnost vytvoření programu, který bude binární formu transformovat do podoby, kterou nebude mít člověk problém přečíst.

## 1.2 Cíl práce

Vytvořený prostředek bude pracovat offline, tedy bude zpracovávat soubory se zachycenou síťovou komunikací. Vytvoření programu na analýzu paketů chci docílit s pomocí knihovny libpcap, která tento proces značně usnadňuje. Vytváří totiž nad daty jakousi abstraktní vrstvu s jejíž pomocí se s nimi lépe pracuje. Tato knihovna ovšem neusnadní problematiku sítí jako takových. Nachází se zde příliš mnoho protokolů, abych je zvládl ve školní práci analyzovat všechny, a tudíž dělám analýzu pouze několika základních protokolů. Z vrstvy síťového rozhraní analyzuji Ethernet a IEEE 802.1Q (včetně IEEE 802.1ad), z vrstvy síťové analyzuji IPv4, IPv6, ICMPv4 a ICMPv6 a z vrstvy transportní TCP a UDP. Uživatel programu si rovněž bude moci nechat agregovat, filtrovat nebo seřadit analyzovaná data podle různých parametrů.

**Kapitola 2**

# Návrh Aplikace

L2 vrstva

L3 vrstva

L4 vrstva

**Kapitola 3**

# Popis implementace

Struktury

Implementace analýzy paketů

**Kapitola 4**

# Základní informace o programu

**Kapitola 5**

# Návod na použití

Program je nutné spouštět alespoň s jedním analyzovatelným souborem (pokud nechceme vypsat nápovědu). Analyzovaný soubor musí být čitelný knihovnou libcap.

## Parametry programu

**-h** **—** Vypíše nápovědu a ukončí program. Tento parametr nelze kombinovat s žádným jiným.

**-a aggr-key** **—** Zapnutí agregace podle klíče aggr-key, což může být *srcmac* značící zdrojovou MAC adresu, *dstmac* značící cílovou MAC adresu, *srcip* značící zdrojovou IP adresu, *dstip* značící cílovou IP adresu, *srcport* značící číslo zdrojového transportního portu nebo *dstport* značící číslo cílového transportního portu.

**-s sort-key** **—** Zapnutí řazení podle klíče sort-key, což může být packets (počet paketů) nebo bytes (počet bajtů). Řadit lze jak agregované, tak i neagregované položky. Řadí se vždy sestupně.

**-l limit** **—** Nezáporné celé číslo v desítkové soustavě udávající limit počtu vypsaných položek.

**-f filter-expression** **—** Program zpracuje pouze pakety, které vyhovují filtru danému řetězcem filter-expression.

**file** **—** Cesta k souboru ve formátu pcap (čitelný knihovnou libpcap). Možné je zadat jeden a více souborů.

**Kapitola 6**

# Závěr

Program úspěšně provádí offline analýzu pcap souborů. Pro překlad slouží soubor Makefile, program je překládán překladačem g++. Prostředek byl otestován na referenčním serveru Merlin (CentOS/Linux).

## Metriky kódu

**Počet souborů:** 1 soubor

**Počet řádků zdrojového textu:** textu

**Velikost spustitelného souboru**

# Literatura

[1] Hlavsa, Z.; aj.: *Pravidla českého pravopisu*. Academia, 2005, ISBN 80-200-1327-X.