



# Síťové aplikace a správa sítí

Dokumentace k projektu Programování síťové služby

Varianta 2: Export DNS informací pomocí protokolu Syslog

# Obsah

<b>1</b>	<b>Úvod</b>	<b>2</b>
<b>2</b>	<b>Uvedení do problematiky</b>	<b>3</b>
2.1	Model TCP/IP . . . . .	3
2.1.1	Vrstva síťového rozhraní . . . . .	3
2.1.2	Síťová vrstva . . . . .	3
2.1.3	Transportní vrstva . . . . .	3
2.1.4	Aplikační vrstva . . . . .	3
2.2	Domain Name System . . . . .	3
2.2.1	Formát DNS zprávy . . . . .	4
2.3	Syslog protokol . . . . .	4
2.3.1	Formát zpráv . . . . .	4
<b>3</b>	<b>Struktura programu</b>	<b>5</b>
<b>4</b>	<b>Implementace</b>	<b>6</b>
<b>5</b>	<b>Testování</b>	<b>7</b>
<b>6</b>	<b>Použití</b>	<b>8</b>
<b>7</b>	<b>Dodatečné informace</b>	<b>9</b>

# 1 Úvod

Dokumentace popisuje řešení projektu a vysvětluje danou problematiku. Naší úlohou bylo nastudovat si potřebné informace a následně navrhnout, naprogramovat a otestovat síťovou službu, navíc k ní napsat manuálovou stránku. Varianta 2, kterou jsem řešil spočívala ve vytvoření aplikace dns-export. Ta odposlouchává síťový provoz na síťovém rozhraní, případně zpracovává pcap soubor, ve kterém je nějaká síťová komunikace již zaznamenána. Aplikace vyfiltruje DNS provoz a následně zpracovává jednotlivé pakety, konkrétně DNS odpovědi (responses). V každé odpovědi projde skrz všechny odpovědní záznamy (Answer resource records) a vyčte určité informace. Doménové jméno, typ DNS záznamu a data specifická pro každý typ. Dále je zaznamenán výskyt těchto informací, shodné jsou sečteny. Tyto výsledky jsou zasílány na syslog server ve formátu odpovídající syslog protokolu.

## 2 Uvedení do problematiky

### 2.1 Model TCP/IP

Síťová komunikace je kvůli své komplexnosti rozdělena do tzv. vrstev, které znázorňují hierarchii činností. Výměna informací mezi vrstvami je přesně definována. Každá vrstva využívá služeb vrstvy nižší a poskytuje své služby vrstvě vyšší.

#### 2.1.1 Vrstva síťového rozhraní

Nejnižší vrstva, umožňuje přístup k fyzickému médiu. Je specifická pro každou síť v závislosti na její implementaci. (např. Ethernet)

#### 2.1.2 Síťová vrstva

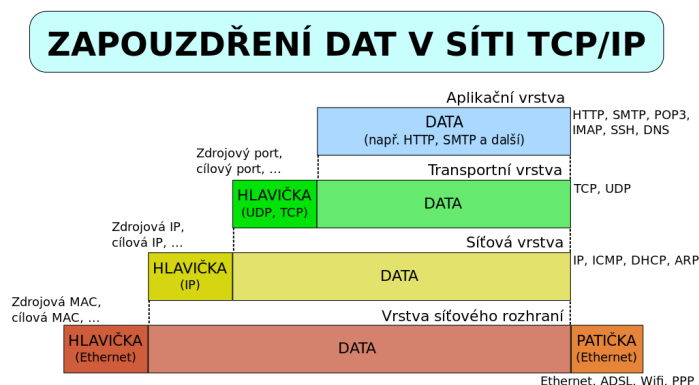
Vrstva zajišťuje síťovou adresaci, směrování a předávání datagramů. Je implementována ve všech prvcích sítě – směrovačích i koncových zařízeních. (např. IPv4, IPv6, ARP, ICMP)

#### 2.1.3 Transportní vrstva

Poskytuje transportní služby pro kontrolu celistvosti dat. Jedná se o spolehlivé spojení (TCP) nebo nespolehlivé spojení (UDP). Je implementována až v koncových zařízeních, proto umožňuje přizpůsobit chování sítě potřebám aplikace.

#### 2.1.4 Aplikační vrstva

Vrstva, která se stará o přenos konkrétních aplikačních dat. (např. SSH, FTP, HTTP, DHCP, DNS)



Obrázek 1: Schéma zapouzdření dat na vrstvách TCP/IP

## 2.2 Domain Name System

DNS (Domain Name System) je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem jsou vzájemné převody doménových jmen a IP adres sítě. Slouží de facto jako distribuovaná databáze síťových informací.

### 2.2.1 Formát DNS zprávy

DNS zpráva má následující formát:

Header
Question
Answer
Authority
Additional

Header (hlavička) blíže specifikuje DNS zprávu. Například zda se jedná o dotaz, či odpověď, zda nastala nějaká chyba, nebo kolik zpráva obsahuje DNS záznamů (resource records) a jakých jsou typů.

V sekci Question (dotaz) jsou informace které chce tázající zjistit. Konkrétně doménové jméno na které se dotazuje, typ a třída záznamu.

Answer, Authority a Additional jsou pak záznamy. Všechny mají shodný formát a obsahují různé odpovědi, případně cestu jak se odpovědi dosáhlo.

## 2.3 Syslog protokol

Syslog protokol je standard pro záznam programových zpráv (logů). Program podle protokolu posílá zprávy napříč sítí ke kolektorům logovacích zpráv – syslog serverům. Jedná se tedy o architekturu klient-server. Komunikace může probíhat přes UDP na portu 514 nebo přes TCP na portu 6541.

### 2.3.1 Formát zpráv

Maximální délka paketu je 1024 bytů. Zpráva má následující formát:

PRI HEADER MSG

Část PRI se skládá ze třech až pěti znaků. Začíná znakem '<', následuje číslo a končí znakem '>'. Číslo uvnitř špičatých závorek se nazývá Priority value a reprezentuje Facility – zařazení podsystému a Severity – míru závažnosti.

PRI = <Priority Value>

Priority value se vypočítá následujícím vzorcem:

Priority Value = Facility \* 8 + Severity

Část HEADER obsahuje časovou značku – TIMESTAMP, tedy kdy byla zpráva odeslána a adresu odesílatele – HOSTNAME, tedy kdo zprávu odeslal.

HEADER = TIMESTAMP HOSTNAME

Poslední část, MSG, se sestává opět ze dvou částí. První z nich je TAG, což je název procesu, který zprávu vygeneroval a druhá je CONTENT, tedy konkrétní obsah zprávy.

MSG = TAG CONTENT

### 3 Struktura programu

Aplikace se snaží držet objektově orientovaného paradigma. Kvůli spravování signálů (signal handler) bylo nutné některé věci definovat na globální úrovni.

Jako první se pracuje s instancí třídy ArgParser, která se stará o zpracování argumentů příkazové řádky a jejich validaci. Argumenty jsou uloženy jako privátní atributy a přístup k nim je definován pomocí příslušných metod.

Třída PcapParser využívá pcap knihovnu pro odchyťávání síťového provozu na síťovém zařízení, případně pro parsování zdrojového pcap souboru. Dále vyfiltruje DNS provoz a zpracuje veškeré hlavičky až k aplikační vrstvě. Poradí si na síťové vrstvě s IPv4 i IPv6 datagramama a na transportní vrstvě s TCP i UDP komunikací.

Třída DnsParser zpracovává data DNS protokolu. Vytrídí pouze odpovědi (responses), které neskončili chybou. Projde všechny záznamy v sekci Answers a vybere data potřebná k vytvoření statistik. Statistiku ukládá do globální datové struktury unordered map jako dvojice klíč->hodnota. Klíč jsou získaná data z DNS záznamu a value je počet výskytů těchto dat za celou dobu odchyťávání, případně za zpracování celého pcap souboru.

Třída Syslog se pak stará o komunikaci se syslog serverem. Poskytuje metody pro připojení, odpojení a odesílání zpráv na syslog.

Ve funkci signal handler jsou pak odchyťávány signály, SIGUSR1 pro výpis statistik na STDOUT, SIGALRM pro odeslání statistik na syslog server a SIGINT pro ukončení aplikace (v případě odposlouchávání na síťovém rozhraní běží aplikace až do obdržení tohoto signálu).

## 4 Implementace

...

## 5 Testování

...



## 6 Použití

...

## 7 Dodatečné informace

...