

**POČÍTAČOVÉ A KOMUNIKAČNÉ SIETE**  
**cvičenia**  
**ak. rok 2017/18, zimný semester**

**Zadanie 1: Analyzátor sieťovej komunikácie**

**Zadanie úlohy**

Navrhните a implementujte programový “post” analyzátor Ethernet siete, ktorý analyzuje komunikácie v sieti zaznamenané v súbore a poskytuje nasledujúce informácie o komunikáciách. Vypracované zadanie musí spĺňať nasledujúce body:

- 1) Výpis všetkých komunikácií, t.j. všetkých rámcov v hexadecimálnom tvare postupne tak, ako boli zaznamenané v súbore.

Pre každý rámec uveďte:

- Poradové číslo rámca v analyzovanom súbore.
- Dĺžku rámca v bajtoch poskytnutú pcap API, ako aj dĺžku tohto rámca prenášaného po médiu.
- Typ rámca – Ethernet II, IEEE 802.3 (IEEE 802.3 - LLC, IEEE 802.3- LLC - SNAP, IEEE 802.3 – Raw).
- Zdrojovú a cieľovú fyzickú (MAC) adresu uzlov, medzi ktorými je rámec prenášaný.

Vo výpise jednotlivé bajty rámca usporiadajte po 8, 16 alebo 32 v jednom riadku. Pre prehľadnosť výpisu je vhodné použiť neproporcionálny (monospace) font.

- 2) Študent musí vedieť vysvetliť, aké informácie sú uvedené v jednotlivých rámcoch Ethernet II, t.j. vnáranie protokolov ako aj ozrejmiť dĺžky týchto rámcov.

- 3) Analýzu cez jednotlivé vrstvy vykonajte len pre rámce Ethernet II a protokoly rodiny TCP/IPv4:

Na konci výpisu z bodu 1) uveďte IP adresy všetkých vysielajúcich uzlov, ako aj IP adresu uzla, ktorý sumárne odvysielal (bez ohľadu na príjemcu) najväčší počet bajtov (vypíšte).

V danom súbore analyzujte zadané komunikácie:

- a) HTTP komunikácie
- b) HTTPS komunikácie
- c) TELNET komunikácie
- d) SSH komunikácie
- e) FTP riadiace komunikácie
- f) FTP dátové komunikácie
- g) Všetky TFTP komunikácie
- h) Všetky ICMP komunikácie
- i) Všetky ARP dvojice (request – reply).

Vo všetkých výpisoch treba uviesť aj IP adresy a pri transportných protokoloch aj porty komunikujúcich uzlov.

V prípade výpisu h) uveďte aj typ ICMP správy (pole Type v hlavičke ICMP), napr. Echo request, Echo reply, Time exceeded, a pod.

V prípade výpisu i) uveďte pri ARP-Request IP adresu, ku ktorej sa hľadá MAC (fyzická) adresa a pri ARP-Reply uveďte konkrétny pár - IP adresa a nájdená MAC adresa. V prípade, že bolo poslaných viacero rovnakých rámcov ARP-Request, vypíšte všetky.

Ak počet rámcov danej komunikácie je väčší ako 20, vypíšte iba 10 prvých a 10 posledných rámcov.

Pri všetkých výpisoch musí byť poradové číslo rámca zhodné s číslom rámca v analyzovanom súbore.

- 4) Program musí byť organizovaný tak, aby čísla protokolov v rámci Ethernet II a v IP pakete ako aj čísla portov v transportných protokoloch boli programom určené z externého súboru a pre známe protokoly a porty boli uvedené aj ich názvy.
- 5) V procese analýzy rámcov pri identifikovaní jednotlivých polí rámca ako aj polí hlavičiek vnorených protokolov nie je povolené použiť funkcie poskytované použitým programovacím jazykom. Celý rámec je potrebné spracovať postupne po bajtoch.
- 6) Program musí byť organizovaný tak, aby bolo možné jednoducho rozširovať jeho funkčnosť o výpis rámcov podľa ďalších požiadaviek na protokoly v bode 3) - pri doimplementovaní jednoduchej funkčnosti na cvičení.
- 7) Študent musí byť schopný preložiť a spustiť program v miestnosti, v ktorej má cvičenia!

V danom týždni, podľa harmonogramu cvičení, musí študent priamo na cvičení doimplementovať do funkčného programu (podľa vyššie uvedených požiadaviek) ďalšiu prídavnú funkčnosť.

#### **Program musí mať nasledovné vlastnosti (minimálne):**

- 1) Program musí byť implementovaný v jazyku C/C++ s využitím definovaných knižníc a skompilovateľný a spustiteľný na PC v učebniach. Použité knižnice musia byť schválené cvičiacim
- 2) Poradové číslo rámca vo výpise programu musí byť zhodné s číslom rámca v analyzovanom súbore.
- 3) Pre každý rámec uviesť použitý protokol na 2. - 4. vrstve OSI modelu.
- 4) Pre každý rámec uviesť zdrojovú a cieľovú adresu / port na 2. - 4. vrstve OSI modelu.

#### **Súčasťou riešenia je aj dokumentácia, ktorá má obsahovať najmä:**

- blokový návrh (konceptia) riešenia,
- navrhnutý mechanizmus analyzovania protokolov na jednotlivých vrstvách,
- navrhnutý postup pri analýze komunikácie so spojením (otváranie, ukončovanie spojení),
- príklad obsahu externých súborov pre určenie protokolov a portov,
- opísané používateľské rozhranie,
- voľbu implementačného prostredia.

Súčasťou dokumentácie musí byť aj zadanie úlohy.

## Hodnotenie

Celé riešenie - max. 10 bodov (min. 3), z toho:

- max. 3 body za riešenie úlohy v bode 1); riešenie musí byť prezentované na 3. cvičení;
- max. 1 body za doplnenú funkčnosť (doimplementáciu) priamo na cvičení v požadovanom termíne podľa harmonogramu cvičení; V prípade, ak študent nesplní úlohu zadanú priamo na cvičeniach, nehodnotí sa riešenie úlohy podľa bodu 3);
- max. 6 bodov za výsledné riešenie podľa bodu 3).

Zdrojový kód implementácie študent odovzdáva v elektronickom tvare do AISu v určenom termíne.

## Ukážky výstupu riešenia

V ukážkach ide iba o zobrazenie požadovaného výstupu, obsah rámcov nezodpovedá reálnej komunikácii. Podobne, uvedené IP adresy v desiatkovo-bodkovej notácii nezodpovedajú reálnym hodnotám v rámci.

### **Výpis celej komunikácie – k bodu 1)**

rámec 1

dĺžka rámca poskytnutá pcap API – 68 B

dĺžka rámca prenášaného po médiu – 72 B

Ethernet II

Zdrojová MAC adresa: 00 00 C0 D7 80 C2

Cieľová MAC adresa: 00 04 76 A4 E4 8C

```
00 04 76 A4 E4 8C 00 00    C0 D7 80 C2 08 00 45 00
00 28 0C 36 40 00 80 06    2B 5A 93 AF 62 EE 45 38
87 6A 04 70 00 50 7E 6C    06 32 56 7D 30 A8 50 10
44 70 97 A0 00 00 80 C2    08 0C 36 40 30 A3 23 35
A2 D5 27 81
```

rámec 2

dĺžka rámca poskytnutá pcap API – 494 B

dĺžka rámca prenášaného po médiu – 498 B

IEEE 802.3 – Raw

Zdrojová MAC adresa: 00 04 76 A4 E4 8C

Cieľová MAC adresa: FF FF FF FF FF FF

```
FF FF FF FF FF FF 00 04    76 A4 E4 8C 01 E0 FF FF
01 E0 00 A1 40 00 80 06    05 B0 93 AF 62 EE 93 AF
63 2A 04 4C 00 50 73 78    .....
```

rámec 3

dĺžka rámca poskytnutá pcap API – 62 B

dĺžka rámca prenášaného po médiu – 66 B

Ethernet II

Zdrojová MAC adresa: 00 00 C0 D7 80 C2

Cieľová MAC adresa: 00 04 76 A4 E4 8C

```
00 04 76 A4 E4 8C 00 00    C0 D7 80 C2 08 00 45 00
```

00 30 07 A1 40 00 80 06 05 B0 93 AF 62 EE 93 AF  
63 2A 04 4C 00 50 73 78 17 88 00 00 00 00 70 02  
40 00 C6 0B 00 00 02 04 05 B4 01 01 04 02

rámec 4

dĺžka rámca z poskytnutá pcap API – 60 B

dĺžka rámca prenášaného po médiu – 64 B

Ethernet II

Zdrojová MAC adresa: 00 04 76 A4 E4 8C

Cieľová MAC adresa: 00 00 C0 D7 80 C2

00 00 C0 D7 80 C2 00 04 76 A4 E4 8C 08 00 45 00  
00 2C F0 EA 00 00 3F 06 9D 6A 93 AF 63 2A 93 AF  
62 EE 00 50 04 4C 41 59 C9 42 73 78 17 89 60 12  
40 00 D0 65 00 00 02 04 05 B4 00 00

rámec 5

dĺžka rámca poskytnutá pcap API – 54 B

dĺžka rámca prenášaného po médiu – 64 B

Ethernet II

Zdrojová MAC adresa: 00 00 C0 D7 80 C2

Cieľová MAC adresa: 00 04 76 A4 E4 8C

00 04 76 A4 E4 8C 00 00 C0 D7 80 C2 08 00 45 00  
00 28 0C 36 40 00 80 06 2B 5A 93 AF 62 EE 45 38  
87 6A 04 70 00 50 7E 6C 06 32 56 7D 30 A8 50 10  
44 70 97 A0 00 00

atď.

IP adresy vysielajúcich uzlov:

147.175.10.3

193.45.10.10

.....

27.30.44.12

210.20.66.8

Adresa uzla s najväčším počtom odvysielaných bajtov:

193.45.10.10 984 bajtov

### Výpis HTTP komunikácie – k bodu 3a)

rámec 5

dĺžka rámca poskytnutá pcap API – 62 B

dĺžka rámca prenášaného po médiu – 66 B

Ethernet II

Zdrojová MAC adresa: 00 14 38 06 E0 93

Cieľová MAC adresa: 00 02 CF AB A2 4C

IPv4

zdrojová IP adresa: 192.168.1.33

cieľová IP adresa: 147.175.1.55

TCP

zdrojový port: 1376

cieľový port: 80

```
00 02 CF AB A2 4C 00 14 38 06 E0 93 08 00 45 00
00 30 8D 68 40 00 80 06 16 B0 C0 A8 01 21 93 AF
01 37 05 60 00 50 0A 16 B1 1B 00 00 00 00 70 02
FF FF 6B 8E 00 00 02 04 05 B4 01 01 04 02
```

rámec 8

dĺžka rámca poskytnutá pcap API – 697 B

dĺžka rámca prenášaného po médiu – 701 B

Ethernet II

Zdrojová MAC adresa: 00 14 38 06 E0 93

Cieľová MAC adresa: 00 02 CF AB A2 4C

IPv4

zdrojová IP adresa: 192.168.1.33

cieľová IP adresa: 147.175.1.55

TCP

zdrojový port: 1376

cieľový port: 80

```
00 02 CF AB A2 4C 00 14 38 06 E0 93 08 00 45 00
02 AB 8D 6A 40 00 80 06 14 33 C0 A8 01 21 93 AF
01 37 05 60 00 50 0A 16 B1 1C FC 0E FC 3B 50 18
FF FF DF 73 00 00 47 45 54 20 2F 62 75 78 75 73
2F 67 65 6E 65 72 61 74 65 5F 70 61 67 65 2E 70
68 70 3F 70 61 67 65 5F 69 64 3D 31 20 ....
```

rámec 15

dĺžka rámca poskytnutá pcap API – 60 B

dĺžka rámca prenášaného po médiu – 64 B

Ethernet II

Zdrojová MAC adresa: 00 02 CF AB A2 4C

Cieľová MAC adresa: 00 14 38 06 E0 93

IPv4

zdrojová IP adresa: 147.175.1.55

cieľová IP adresa: 192.168.1.33

TCP

zdrojový port: 80

cieľový port: 1376

```
00 14 38 06 E0 93 00 02 CF AB A2 4C 08 00 45 00
00 28 E6 16 40 00 3A 06 04 0A 93 AF 01 37 C0 A8
01 21 00 50 05 60 FC 0E FD 2F 0A 16 B3 A0 50 10
1B A1 80 DE 00 00 00 00 00 00 00 00
```

atď.

### Výpis ARP dvojíc – k bodu 3i)

Komunikácia č. 1

ARP-Request, IP adresa: 147.175.98.232, MAC adresa: ???

Zdrojová IP: 147.175.98.238, Cieľová IP: 147.175.98.232

rámec 5

dĺžka rámca poskytnutá pcap API – 42 B

dĺžka rámca prenášaného po médiu – 64 B

Ethernet II

Zdrojová MAC adresa: 00 00 c0 d7 80 c2

Cieľová MAC adresa: ff ff ff ff ff ff  
ff ff ff ff ff ff 00 00 c0 d7 80 c2 08 06 00 01  
08 00 06 04 00 01 00 00 c0 d7 80 c2 93 af 62 ee  
00 00 00 00 00 00 93 af 62 e8

ARP-Reply, IP adresa: 147.175.98.232, MAC adresa: 00 04 76 13 97 df  
Zdrojová IP: 147.175.98.232, Cieľová IP: 147.175.98.238  
rámec 6

dĺžka rámca poskytnutá pcap API – 60 B  
dĺžka rámca prenášaného po médiu – 64 B  
Ethernet II

Zdrojová MAC adresa: 00 04 76 13 97 df  
Cieľová MAC adresa: 00 00 c0 d7 80 c2  
00 00 c0 d7 80 c2 00 04 76 13 97 df 08 06 00 01  
08 00 06 04 00 02 00 04 76 13 97 df 93 af 62 e8  
00 00 c0 d7 80 c2 93 af 62 ee 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00

Komunikácia č. 2

ARP-Request, IP adresa: 147.175.98.238, MAC adresa: ???  
Zdrojová IP: 147.175.98.231, Cieľová IP: 147.175.98.238  
rámec 21

dĺžka rámca poskytnutá pcap API – 60 B  
dĺžka rámca prenášaného po médiu – 64 B  
Ethernet II

Zdrojová MAC adresa: 00 00 c0 d7 80 c2  
Cieľová MAC adresa: ff ff ff ff ff ff  
ff ff ff ff ff ff 00 00 c0 d7 80 c2 ...

ARP-Reply IP adresa: 147.175.98.238, MAC adresa: 00 04 76 23 ab ef  
Zdrojová IP: 147.175.98.238, Cieľová IP: 147.175.98.231  
rámec 24

dĺžka rámca poskytnutá pcap API – 60 B  
dĺžka rámca prenášaného po médiu – 64 B  
Ethernet II

Zdrojová MAC adresa: 00 04 76 23 ab ef  
Cieľová MAC adresa: 00 00 c0 d7 80 c2  
00 00 c0 d7 80 c2 00 04 76 23 ab ef ...

..... atď.

-----  
Formát súborov so zaznamenanou komunikáciou je libpcap formát. Obsahuje dáta zachytených rámcov v binárnom tvare. Tento formát je štandardne používaný mnohými sieťovými analyzátorami, napr. Wireshark, tcpdump, WinDump, atď.

Pri riešení použite moduly pcap knižnice. Pcap je voľne dostupný systém pre priame sieťové prístupy pod OS Windows. Pri programovaní v iných programovacích jazykoch než C++ sa tieto knižnice môžu volať inak.

Literatúra (Internet zdroje; Dokumentový server AIS):

<http://www.winpcap.org>

<http://www.wireshark.org/>

RFC dokumenty (pre analyzované protokoly)