Slovenská technická univerzita

Fakulta informatiky a informačných technológií

Ilkovičova 3, 842 19 Bratislava 4

Andrej Byrtus

Analyzátor sieťovej komunikácie

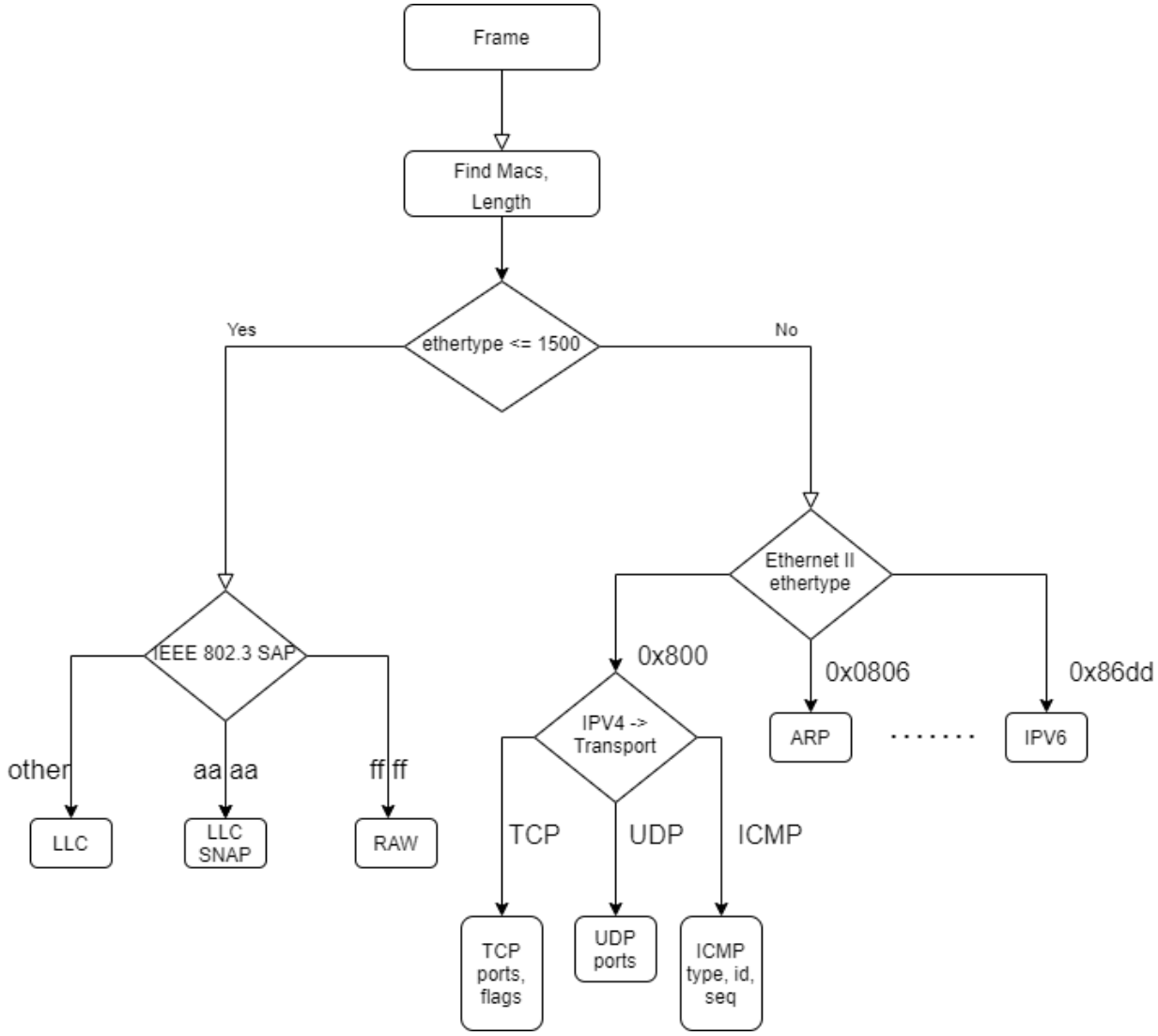
Predmet: **Počítačové a komunikačné siete**

Cvičiaci: Ing. Dominik Macko, PhD.

Ak. rok: 2020/2021

a) **Zadanie** Navrhnite a implementujte programový analyzátor Ethernet siete, ktorý analyzuje komunikácie v sieti zaznamenané v .pcap súbore.

b) **Blokový návrh**



c) **Mechanizmus analýzy vrstiev**

1. Ethernet II / IEEE 802.3 - Rozlišujeme či je pole ethertype v hlavičke menšie ako 1500, v tom prípade analyzujeme podľa SSAP/DSAP o ktoré sa jedná - ff ff = RAW, aa aa = LLC + SNAP, iné = LLC,

2. Pre Ethernet II zisťujeme ethertype, ktorý môže byť 0x800 pre IPV4, 0x0806 pre ARP atď.

3. Transportná vrstvá - podľa dĺžky IP hlavičky posúvame pozície na ktorých sa hľadajú ďalšie hlavičky transportnej vrstvy

a) TCP - pri TCP zisťujeme zdrojové a cieľové porty, flagy ack/s

b) UDP - zisťujeme len zdrojové a cieľové porty

c) ICMP - zaujímajú nás len časti type (echo, echo reply...), Identifier a Sequence pre párovanie dvojíc

Analýza sa vykonáva porovnávaním hexadecimálnych dát na potrebných pozíciách so slovníkom známych hodnôt ktorý načítavame z externého súboru vo formáte .json.

d) **Externý súbor**

formát súboru je nasledovný:

```
{
  "ethertype": {
    "0800": "IPV4",
    "0806": "ARP",
    "86dd": "IPV6",
    "9000": "Loopback"
    ...
  },
  ...
}
```

Pre každý analyzovaný typ existuje kľúč v ktorom je zoznam známych hodnôt.

e) **Používateľské rozhranie**

Analyzátor je konzolová aplikácia, načítava preddefinovaný súbor, ale je možné načítať aj ďalsie pomocou príkazu load <enter> <relatívna_cesta>
Body zadania je možné vypísať číslom + písmenom ak existuje subkategória, napr. “4e”, pre bod 4, e)
Zoznam príkazov sa vypíše na začiatku programu alebo pomocou “help”

f) **Implementačné prostredie**

Program je implementovaný v Python 3.7.

Použité knižnice: Scapy 2.4.4