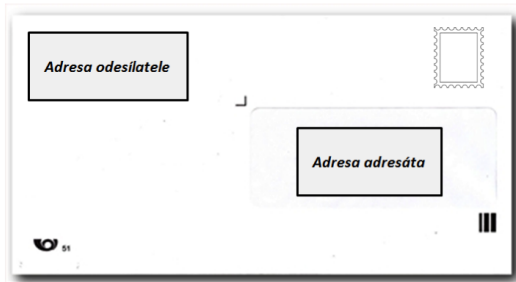


# Quo vadis, ipfixprobe?

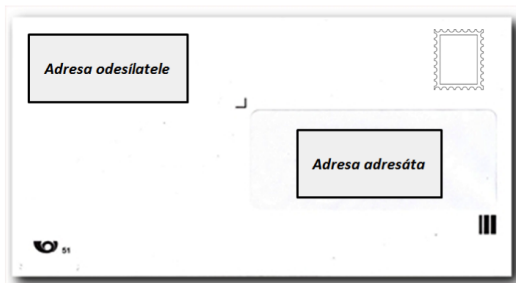
# Úvod

- Zařízení připojená do počítačové sítě přijímají a odesílají tzv. „pakety“
- **Paket**

- Zařízení připojená do počítačové sítě přijímají a odesílají tzv. „pakety“
- **Paket**



- Zařízení připojená do počítačové sítě přijímají a odesílají tzv. „pakety“
- **Paket**



## Síťový provoz (technicky) I

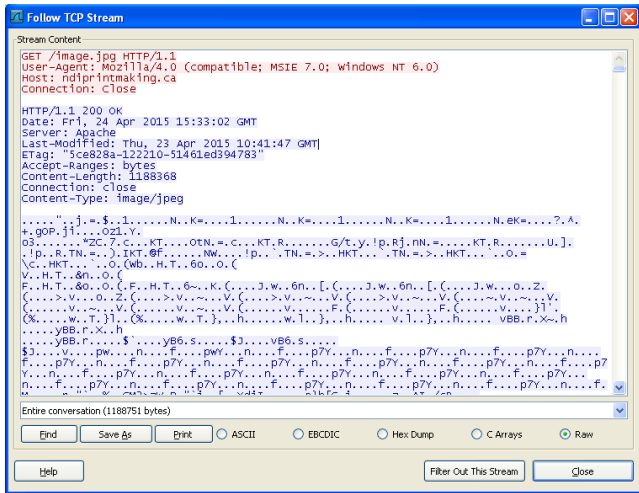
[illegible]

# Síťový provoz (technicky) II

- ▶ Ethernet II, Src: CiscoInc\_2c:f4:c8 (00:26:98:2c:f4:c8), Dst: CiscoInc\_95:d1:03 (f4:4e:05:95:d1:03)
- ▶ Internet Protocol Version 4, Src: 93.115.●● (93.115.●●), Dst: 158.196.●● (158.196.●●)
- ▶ User Datagram Protocol, Src Port: 5071 (5071), Dst Port: 5060 (5060)
- ▶ Session Initiation Protocol (INVITE)

```
0000  f4 4e 05 95 d1 03 00 26 98 2c f4 c8 08 00 45 00  .N.....& ,....E.
0010  03 18 39 ba 00 00 7a 11 21 ef 5d 73 1c b0 9e c4  ..9...z. !.]s....
0020  c9 44 13 cf 13 c4 03 04 c7 76 49 4e 56 49 54 45  .D..... .vINVITE
0030  20 73 69 70 3a 31 36 30 30 35 34 38 35 38 37 33  sip:160 05485873
0040  32 38 33 35 31 40 31 35 38 2e 31 39 36 2e ●● 28351@15 8.196.●●
0050  ●● 2e ●● 20 53 49 50 2f 32 2e 30 0d 0a 54 6f ●● SIP /2.0..To
0060  3a 20 31 36 30 30 35 34 38 35 38 37 33 32 38 33  : 160054 85873283
0070  35 31 36 30 30 35 34 38 35 38 37 33 32 38 33  51...1...6005485873
```

# Síťový provoz (technicky) III





- Monitorování je proces, při kterém sledujeme a sbíráme informace o tom, „zda vše funguje a jestli to funguje správně“ → pakety jsou užitečné
- Detekce bezpečnostních hrozeb, obrana infrastruktury, incident response & forenzní analýza

## Máme k dispozici:

- čítače (SNMP, Network Telemetry)
- síťové toky (NetFlow, IPFIX, případně sFlow)
- pakety (PCAP)

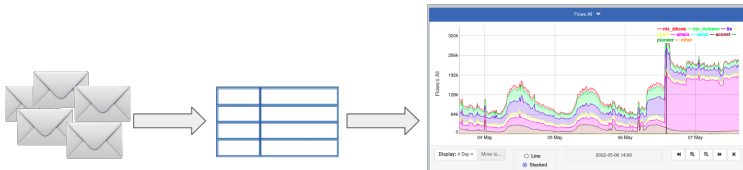
# Monitorování síťového provozu

- Monitorování je proces, při kterém sledujeme a sbíráme informace o tom, „zda vše funguje a jestli to funguje správně“ → pakety jsou užitečné
- Detekce bezpečnostních hrozeb, obrana infrastruktury, incident response & forenzní analýza

## Máme k dispozici:

- čítače (SNMP, Network Telemetry)
- síťové toky (NetFlow, IPFIX, případně sFlow)
- pakety (PCAP)

# ipfixprobe



# Co to je?

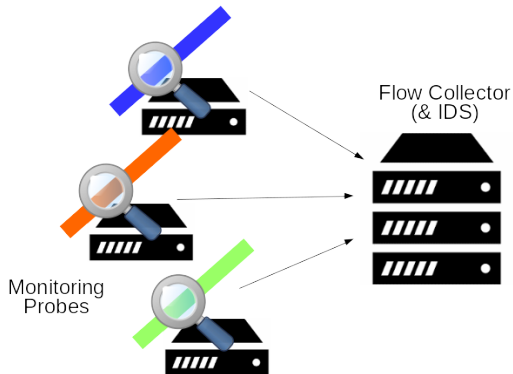
- Exportér síťových toků (IP Flow exporter)
- Monitoruje pakety na síťovém rozhraní (síťové kartě), agreguje a počítá informace o provozu na síti, odesílá získané informace na kolektor (IP Flow collector)
- Lze spustit nad rychlou síťovou kartou / FPGA akcelerační kartou (stovky Gb/s)
- Možnost nasazení i na „SOHO“ routery
- Volně dostupný na github: <https://github.com/CESNET/ipfixprobe>
- Spolupráce sdružení CESNET a českých univerzit

**Hodnoceno jako excelentní výsledek za rok 2022!**

(metodika hodnocení VO, M1)

# Základní použití

Jeden či více exportérů monitoruje provoz a metadata jsou odesílána na kolektor.



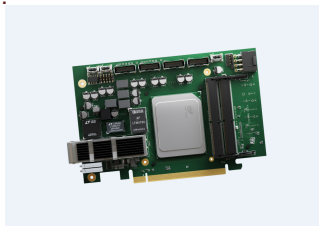
- Implementováno v C++
- Instalace z binárních balíků RPM, repozitář na [COPR - EPEL8 / EPEL9](#)
- Spouštění pomocí systemd
- Možnost vícero instancí exportéru na jednom stroji
- Podpora monitorování 100G linek

**Podle našich měření zvládne ipfixprobe monitorovat 400Gb/s provoz.**

- *2022: měřeno na 200G FPGA kartě (Bittware), NDP vstupní plugin ipfixprobe, 32 CPU jader&DMA kanálů, pozorováno vytížení CPU cca 35 %, replikace “běžného provozu” z linky do NIX pro saturaci 200 Gb/s.*
- *2023: měřeno na 400G FPGA kartě (REFLEX CES) při podobné konfiguraci, ale s DPDK*

# Historie ipfixprobe

- 2016 • `flow_meter`, součást NEMEA (zmíněno na LD2016).
- 2019 • PoC pro P4 generovaný kód.
- 2020 • Jméno `ipfixprobe`.
- 2021 • Produkce na perimetru sítě CESNET,  
„pipeline“ pro V&V: `ipfixprobe` + `IPFIXcol2` + NEMEA.
- 2022 • Použití na komoditní/FPGA kratě: 10/100/200/400G  
(REFLEX CES).
- 2023+ • Důležitý zdroj dat pro náš výzkum  
— vědecko-výzkumné publikace.



Využití v projektech bezpečnostního výzkumu a vývoje, tvorba datových sad...

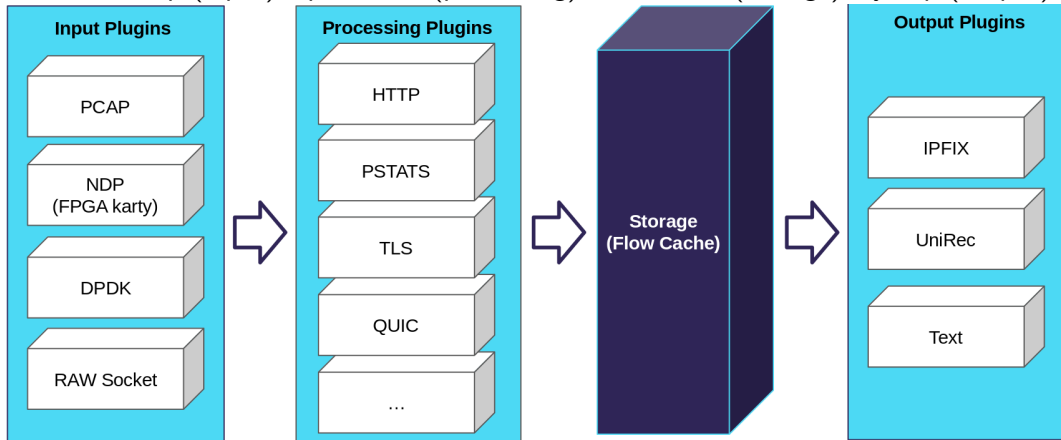
# Ukázka spuštění ipfixprobe

```
1 $ ipfixprobe -i 'raw;ifc=wlo1' -p tls -o "ipfix;h=localhost;p=4739;u"
2 Input stats:
3 # packets parsed bytes dropped qtime status
4 0 108 104 29173 0 0 ok
5 Output stats:
6 # biflows packets bytes dropped status
7 0 8 104 27717 0 ok
```



# Jak vypadá ipfixprobe

4 části: vstup (input), zpracování (processing), flow cache (storage), výstup (output)

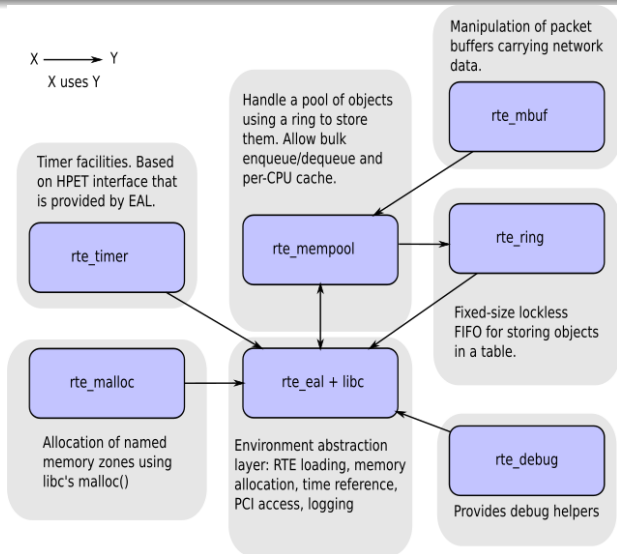


# Vstup ipfixprobe — DPDK

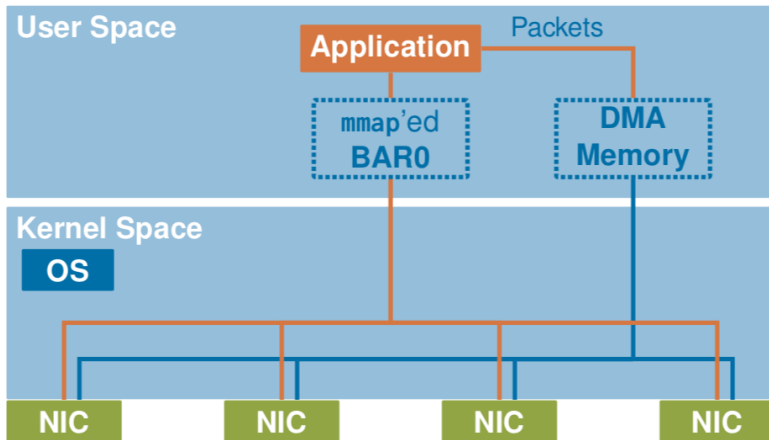
## Data Plane Development Kit (DPDK)

- Vyvíjeno pod Linux Foundation, původně od Intel
- IO framework pro práci s pakety v C
- Reimplementace ovladače síťové karty
- Efektivní řešení, pakety se kopírují z NIC rovnou do user space
- Podpora velkého množství síťových karet
- <https://www.dpdk.org>
- [http://doc.dpdk.org/guides/prog\\_guide/](http://doc.dpdk.org/guides/prog_guide/)
- <http://doc.dpdk.org/api/>

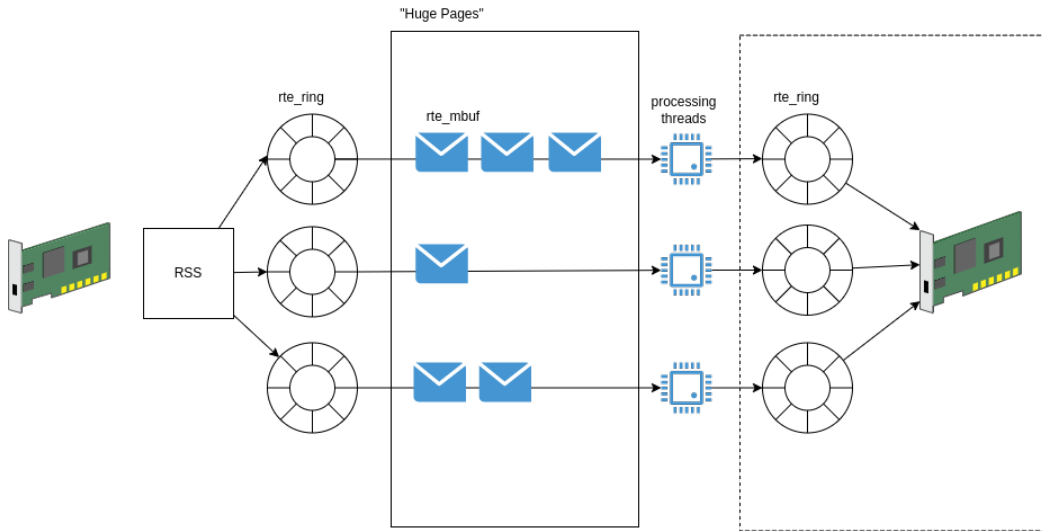
# DPDK architektura podle dokumentace



# DPDK



# Zjednodušené schéma DPDK aplikace



# Ukázka DPDK — Vagrant I

Z předmětu BI-HAM na FIT ČVUT:

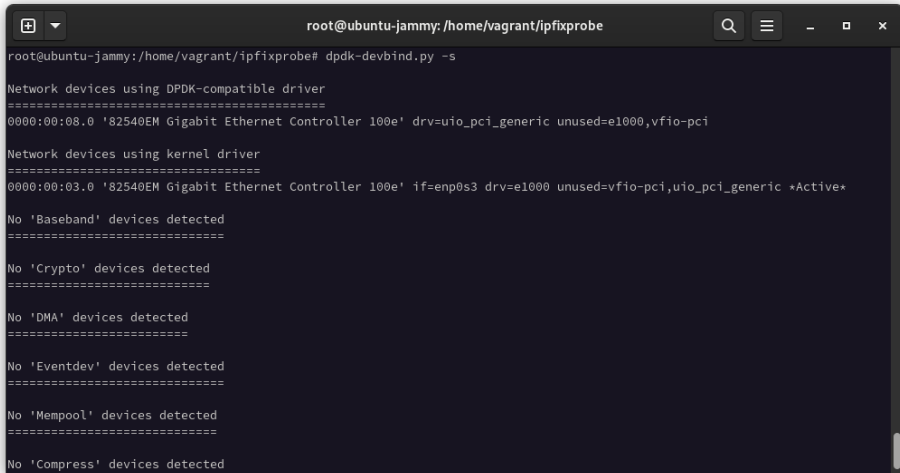
```
1  # -*- mode: ruby -*-
2  Vagrant.configure("2") do |config|
3    config.vm.provider "virtualbox" do |v|
4      v.customize ["setextradata", :id, "VBoxInternal/CPUM/SSE4.1", "1"]
5      v.customize ["setextradata", :id, "VBoxInternal/CPUM/SSE4.2", "1"]
6      v.customize ["modifyvm", :id, "--nic2", "hostonly", "--hostonlyadapter2",
7        "vboxnet0", "--nicpromisc2", "allow-all"]
8      v.memory = "4096"
9      v.cpus = 3
10   end
11   config.vm.define "ubuntu" do |m|
12     m.vm.box = "ubuntu/jammy64"
13
14     m.vm.provision "shell", inline: <<-SHELL
15       apt update
16       apt -y install build-essential autoconf libtool libssl-dev libatomic1 \
17         libxml2-dev libpcap-dev dpdk dpdk-dev linux-image-extra-virtual git
18   end
```

## Ukázka DPDK — Vagrant II

```
19     git clone https://github.com/cesnet/ipfixprobe
20     cd ipfixprobe && autoreconf -i && ./configure -q --with-dpdk && make -j5
21
22     echo "pci 0000:00:08.0 uio_pci_generic" >> /etc/dpdk/interfaces
23     systemctl enable --now dpdk.service
24     dpdk-hugepages.py --setup 2G
25 SHELL
26     end
27 end
```



# Ukázka DPDK — spuštění ipfixprobe I



```
root@ubuntu-jammy: /home/vagrant/ipfixprobe
root@ubuntu-jammy:/home/vagrant/ipfixprobe# dpdk-devbind.py -s

Network devices using DPDK-compatible driver
=====
0000:00:08.0 '82540EM Gigabit Ethernet Controller 100e' drv=uio_pci_generic unused=e1000,vfio-pci

Network devices using kernel driver
=====
0000:00:03.0 '82540EM Gigabit Ethernet Controller 100e' if=enp0s3 drv=e1000 unused=vfio-pci,uio_pci_generic *Active*

No 'Baseband' devices detected
=====

No 'Crypto' devices detected
=====

No 'DMA' devices detected
=====

No 'Eventdev' devices detected
=====

No 'Mempool' devices detected
=====

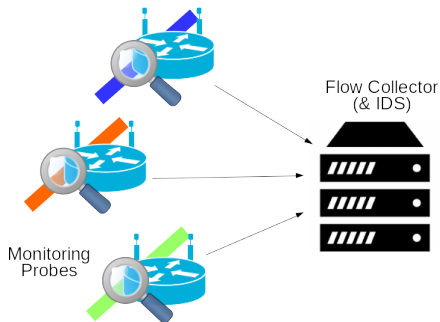
No 'Compress' devices detected
```

# Ukázka DPDK — spuštění ipfixprobe II

```
root@ubuntu-jammy: /home/vagrant/ipfixprobe
root@ubuntu-jammy:/home/vagrant/ipfixprobe# ./ipfixprobe -i 'dpdk;p=0;q=1;e=-a 0000:00:08.0' -p basic -o text
mac conversation packets bytes tcp-flags time extensions
EAL: Detected CPU lcores: 3
EAL: Detected NUMA nodes: 1
EAL: Detected shared linkage of DPDK
EAL: Multi-process socket /var/run/dpdk/rte/mp_socket
EAL: Selected IOVA mode 'PA'
EAL: VFIO support initialized
EAL: Probe PCI driver: net_e1000_em (8086:100e) device: 0000:00:08.0 (socket 0)
TELEMETRY: No legacy callbacks, legacy socket not created
Capabilities of the port 0 with driver net_e1000_em:
    RX offload: 74255
    flow type RSS offloads: 0
    Detected RSS offload capability: no
    Detected HW timestamp capability: no
Skipped RSS hash setting for port 0.
DPDK input at port 0 started.
0a:00:27:00:00:00->33:33:00:00:00:02 58@[fe80::800:27ff:fe00:0]:0->[ff02::2]:0 1->0 56->0 0->0 2023-10-07T21:50:00.895872-
>2023-10-07T21:50:00.895872
^CInput stats:
#      packets      parsed      bytes      dropped      qtime status
0          1          1          70          0          0      ok
SUM        1          1          70          0          0
Output stats:
#      biflows      packets      bytes (L4)      dropped status
0          1          1          56          0      ok
root@ubuntu-jammy:/home/vagrant/ipfixprobe#
```

# Export flow z OpenWrt směrovače

- OpenWrt feed <https://github.com/CESNET/NEMEA-OpenWrt>)
- Testováno na:
  - CZ.NIC Turris/Omnia/MOX, TP-Link



- Zajímavé pluginy:  
pstats (paketová sekvence), bstats („bursts“), **nettisa**
- NetTiSA: Network Time Series Analysis
  - článek v recenzním řízení — univerzální minimalistická sada statistik charakterizujících síťový provoz
  - Zjednodušený (statistický) „popis“ chování síťového spojení

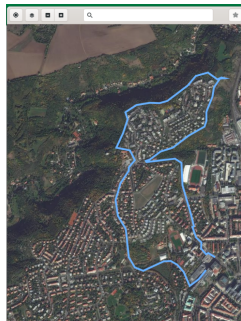
**K čemu je to dobré?**

# K čemu je to dobré? I

## Monitorování, analýza/klasifikace/detekce síťového provozu!

- šifrovaný provoz — obsah je před námi skrytý;
- obecně nás zajímá:
  - zda je komunikace neškodná,
  - zda se něco na síti nechová podezřele;
- úvaha: chytrí útočníci nechtějí být vidět ;-)

→ výstup z ipfixprobe + strojové učení = využití „postranních kanálů“!



### **Náš tým zkoumá možnosti detekce/roznání provozu:**

- Detekce těžby kryptoměn na základě síťové komunikace
- Detekce DNS over HTTPS
- Detekce VPN
- Detekce botnetu/malware (obecně „heartbeat“ komunikace)
- ...

Díky studentům a jejich bakalářským/magisterským/dizertačním pracem dosahujeme celosvětově významných výsledků :-)

(Laboratoř Monitorování síťového provozu, FIT ČVUT v Praze & CESNET)

# Budoucí rozvoj?



# Na co se soustředíme

- Optimalizace pro 400 Gb/s sondu
- Optimalizace/refactoring flow cache
- Podaný projekt na zlepšení odolnosti sondy proti volumetrickým útokům (projekt „AMON“)



# Děkuji za pozornost

E-Mail: [cejkat@cesnet.cz](mailto:cejkat@cesnet.cz) / [cejkato2@fit.cvut.cz](mailto:cejkato2@fit.cvut.cz)

X: [@tomcejka](#)

Mastodon: [fosstodon.org/@tomcejka](https://fosstodon.org/@tomcejka)

## Užitečné odkazy:

- <https://netmon.fit.cvut.cz>
- <https://www.liberouter.org>
- <https://github.com/CESNET/ipfixprobe>
- <https://nemea.liberouter.org>