

TROUBLESHOOTING A BEZPEČNOST IP SÍTÍ



David Tichý



Peter Potrok

AKADEMIE VLÁKNOVÉ OPTIKY A OPTICKÝCH KOMUNIKACÍ[®]

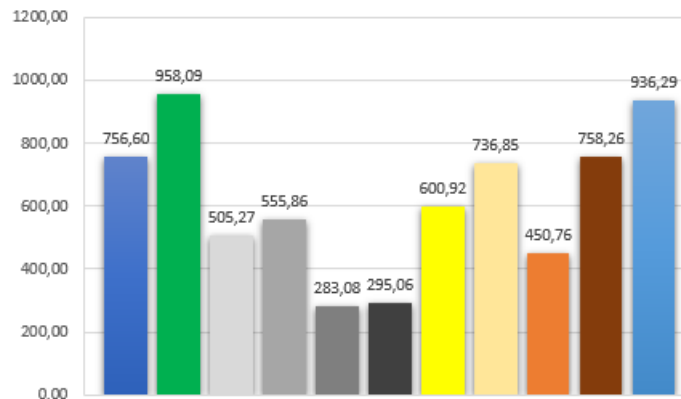
the art of
optical
communication



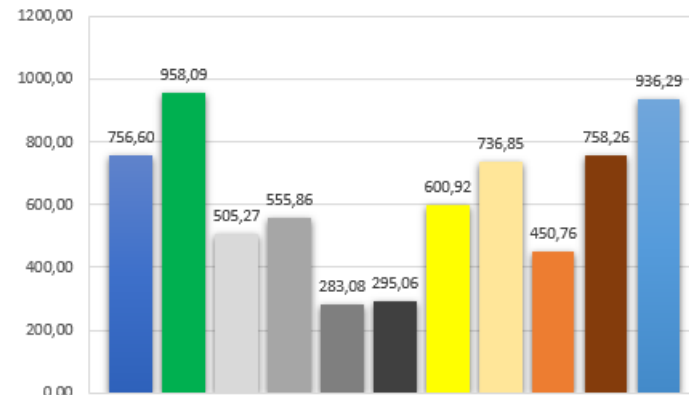
PROFiber[®]
NETWORKING

The logo for PROFiber NETWORKING features a stylized blue and grey graphic above the text. The text 'PROFiber' is in a bold, blue, sans-serif font, with a registered trademark symbol, and 'NETWORKING' is in a smaller, grey, all-caps, sans-serif font below it.

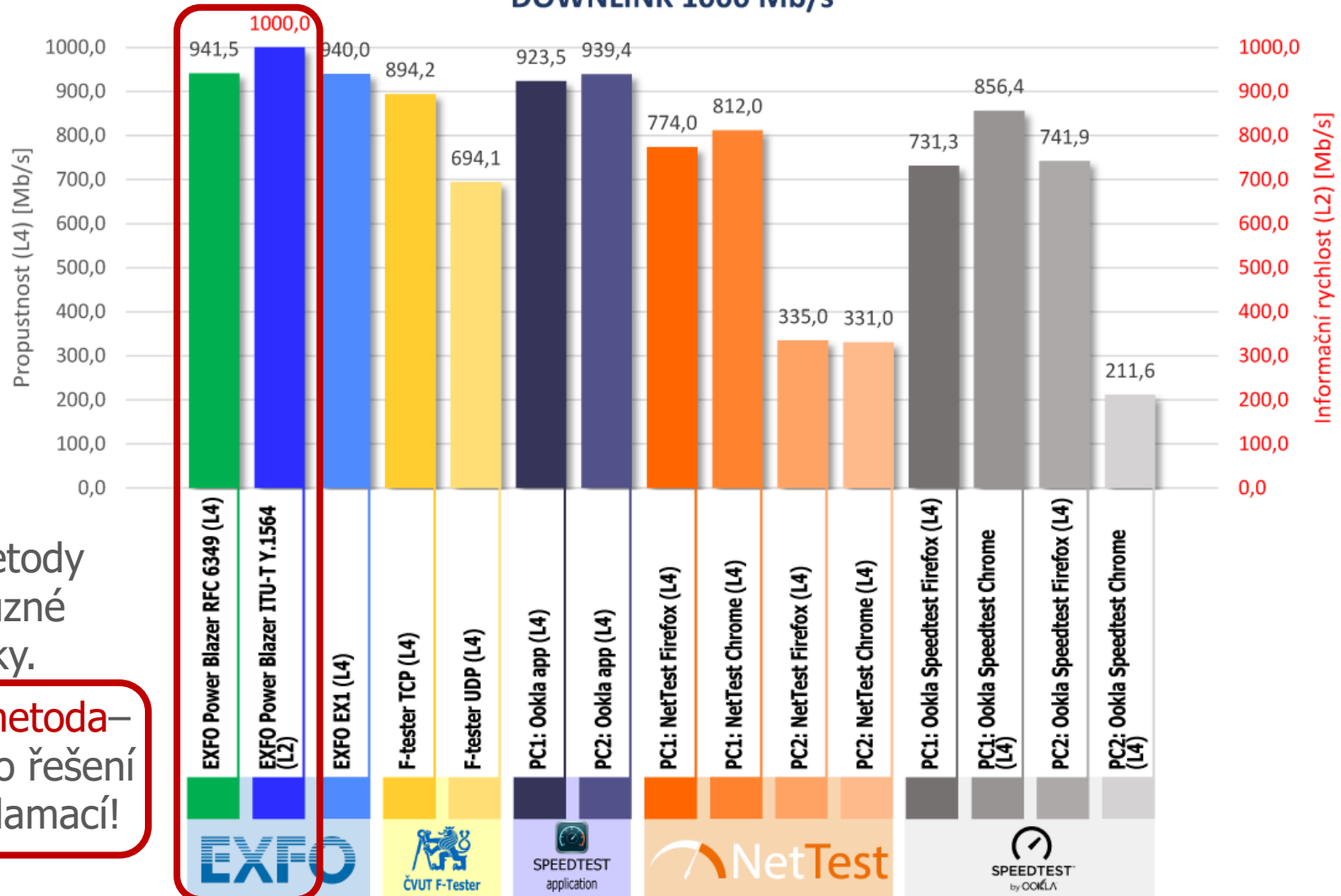
- Změřit rychlost přípojky!
- **Viditelnost v síti!!**
- Změřit QoS parametry poskytované služby
- **Rychlý** a efektivní troubleshooting
- Zajistit bezpečnost dat a účastníků na síti



- Zajištění běžně dostupné rychlosti a kvality připojení
- Dimenzování sítě
- Dohled provozu a služeb
- Měření rychlosti a QoS parametrů



DOWNLINK 1000 Mb/s



Různé metody
dávají různé
výsledky.

referenční metoda –
rozhodná pro řešení
sporů a reklamací!

VÍCE K MĚŘENÍ V APLIKAČNÍ SEKCI SPRÁVNÁ METODA MĚŘENÍ RYCHLOSTI

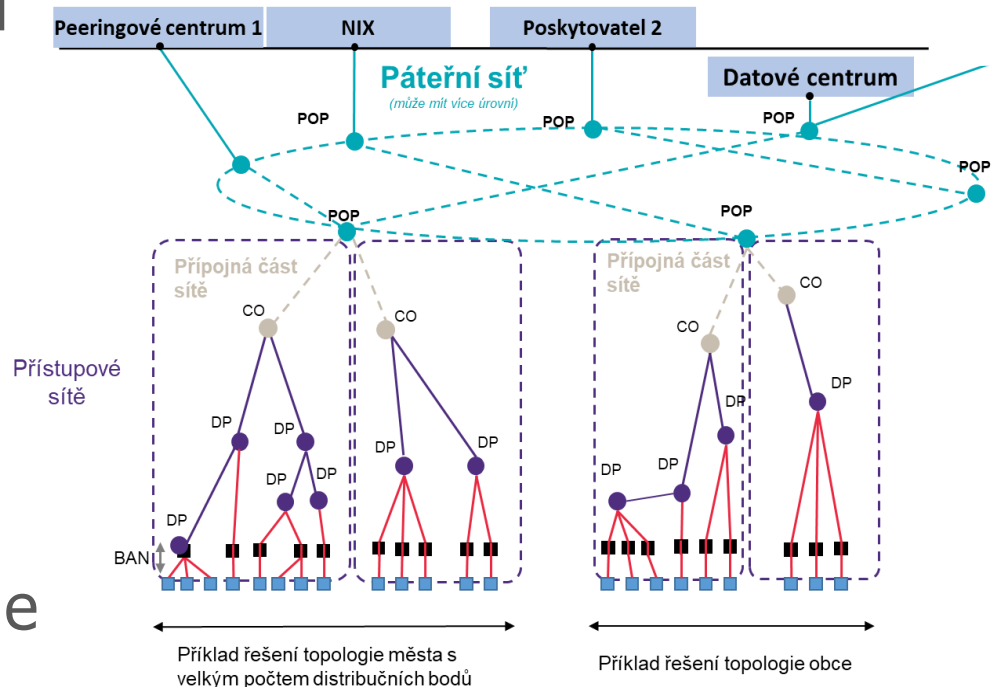


NA SÍTI SE OBJEVÍ PROBLÉM. CO TEĎ?

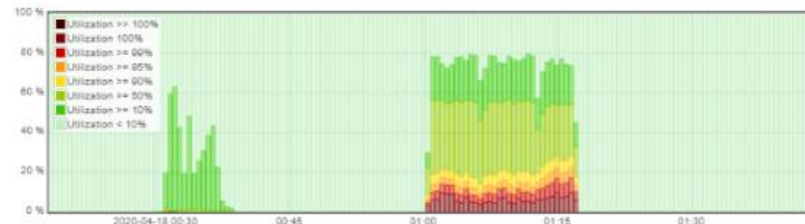
the art of
optical
communication



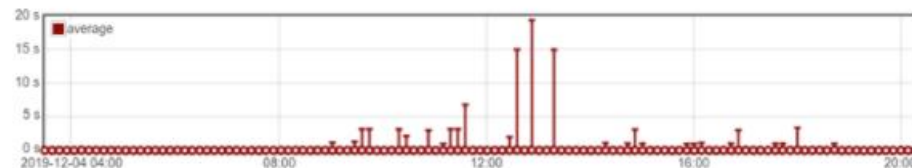
- Zjistíme lokaci poruchy pokud jde o výpadek
- Identifikujeme typ problému
- Zjistíme zda je problém u mě (ISP) na síti, u koncového uživatele nebo u poskytovatele (CAP)



- Vytíženost linky včetně burst analýzy
- TCP retransmise a ztráty
- Účastníky a protokoly
- Jaký typ provozu a aplikací mi na síti chodí a **kam**
- Odezvu na síti
 - TCP handshake
 - SSL handshake a aplikační odezva



Server handshake time



Top sending IPs during the last minute 

IP (name)	Packets/s	Bit/s	PCAP
10.54.0.14	2 pps	3.1 kbit/s	
10.54.0.15	2 pps	1.1 kbit/s	
68.183.161.145	0 pps	0 bit/s	

Zdroj: Allegro Packets

Všechny tyto parametry mohou být indikátory slabých míst na síti nebo v horším případě napadeného místa.

Pokud nemáme dobrou viditelnost, tak tyto místa může být velice obtížné identifikovat nebo dokonce nemožné.



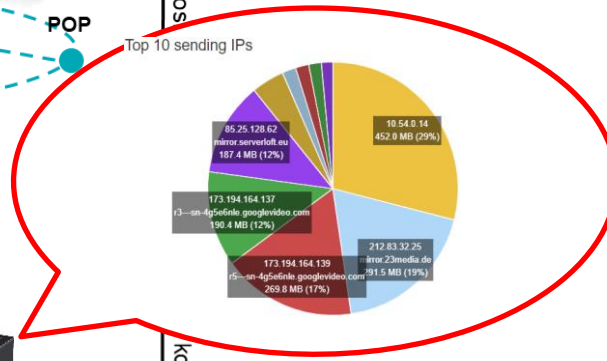
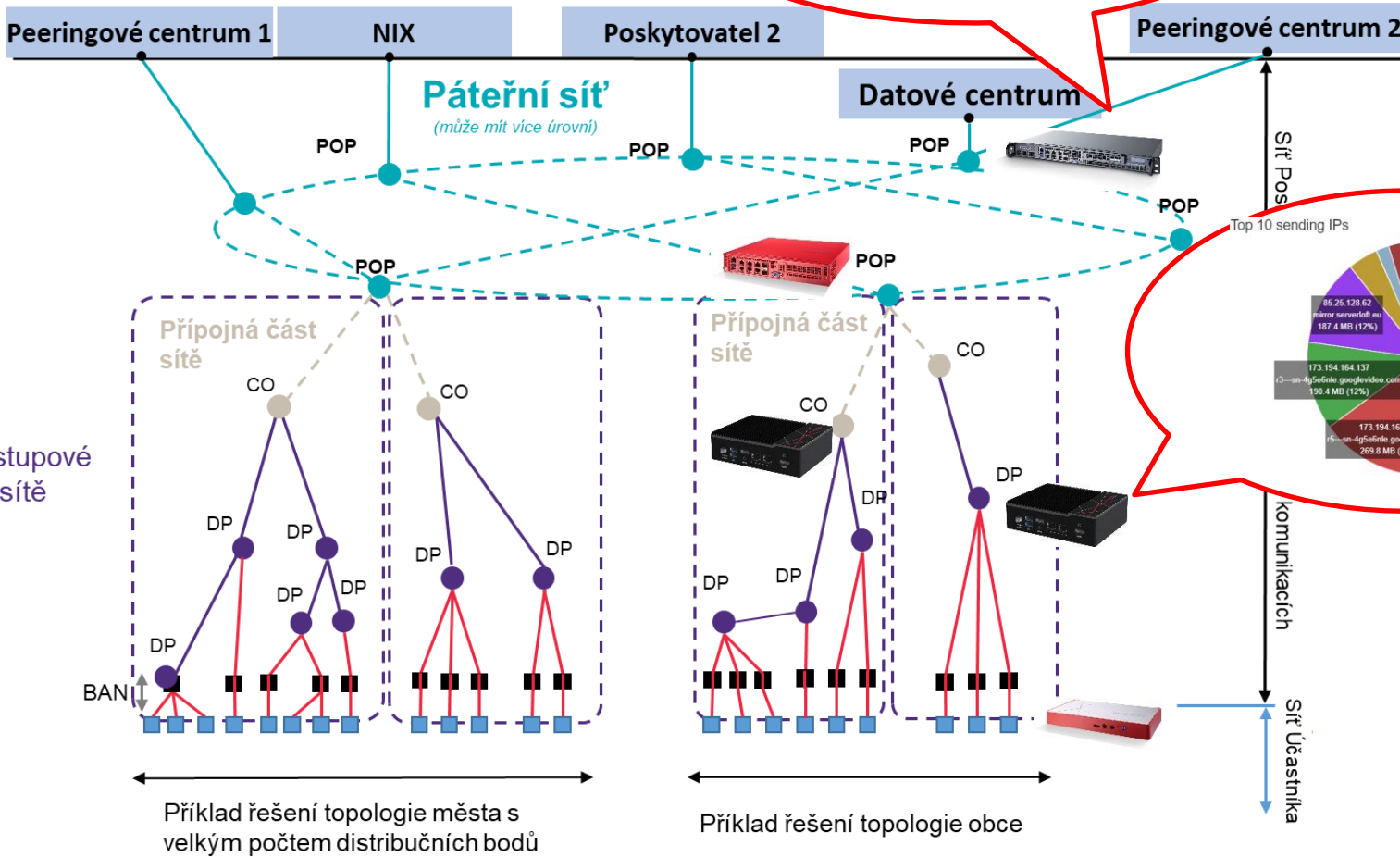
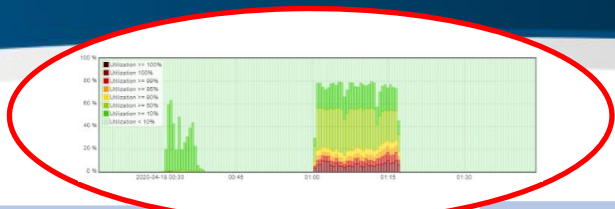
Server handshake time



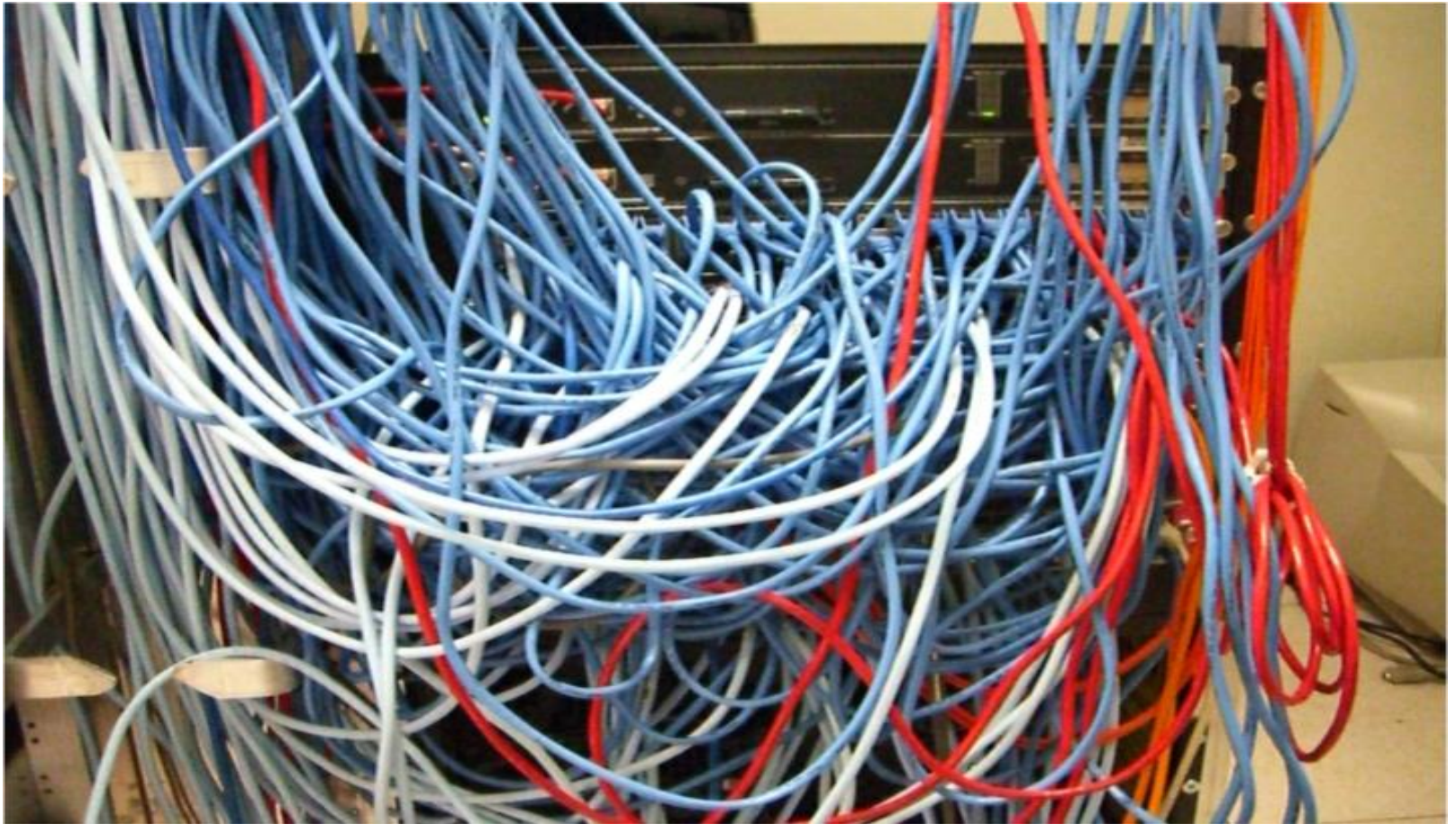
Top sending IPs during the last minute 

IP (name)	Packets/s	Bit/s	PCAP

Zdroj: Allegro Packets

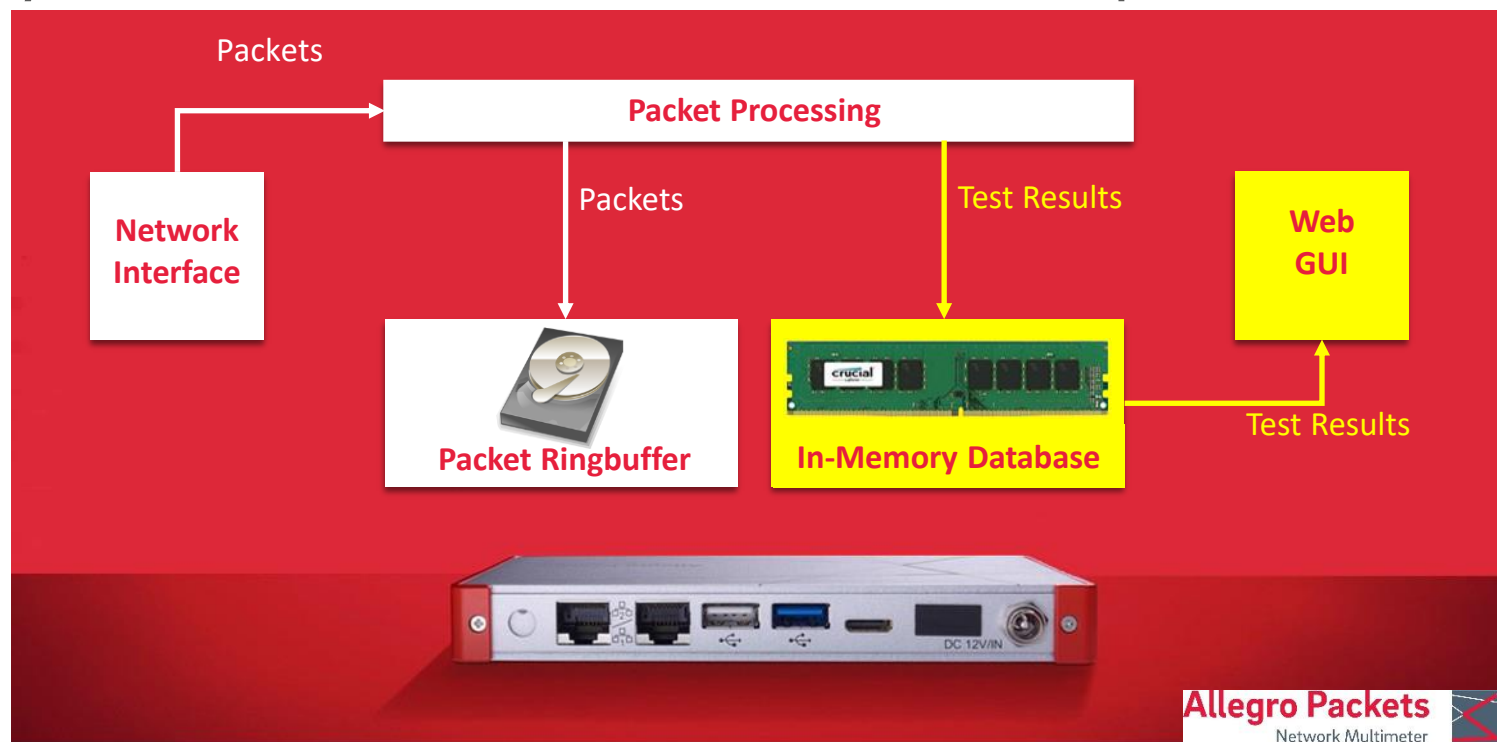


Je potřeba lepší viditelnost v síti!



Zdroj: Allegro Packets

- Multimeter Allegro Packets ukládají raw data jako pcap
- K zobrazení grafů a analýze používají interní paměť a zobrazují zachycená data v reálném čase nebo retrospektivně



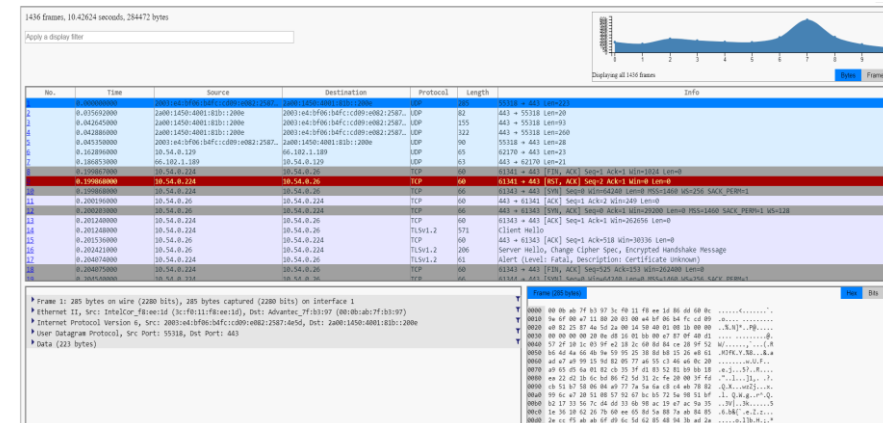
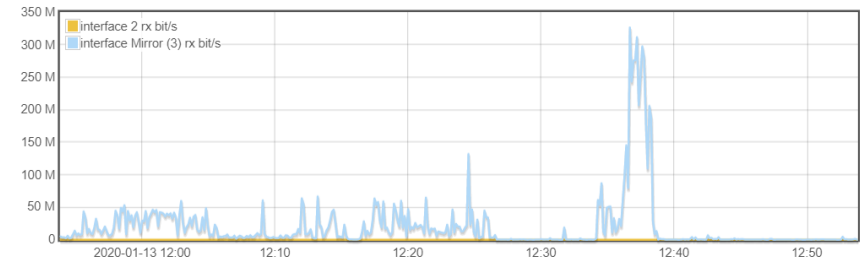
Interní paměť

- metadata
- statistiky
- Prezentováno přes webový interface

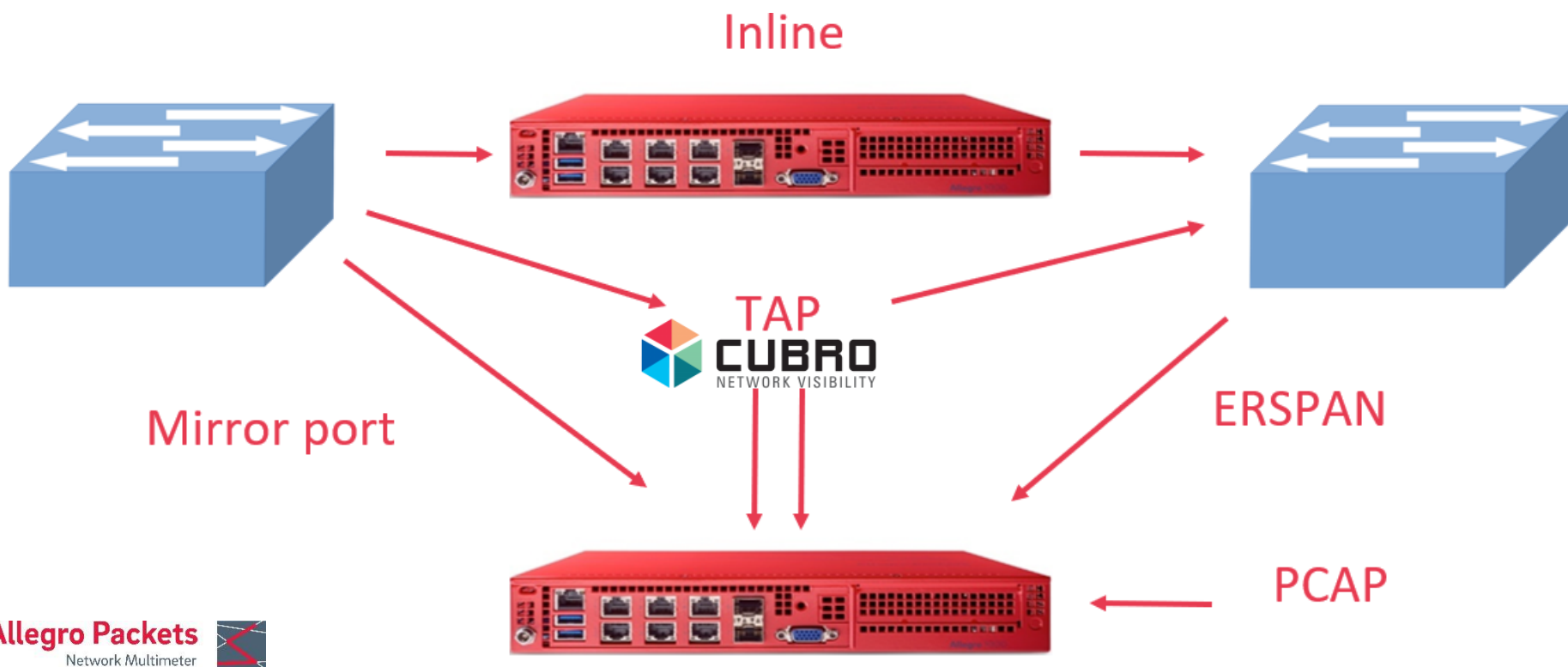


Packet ring buffer

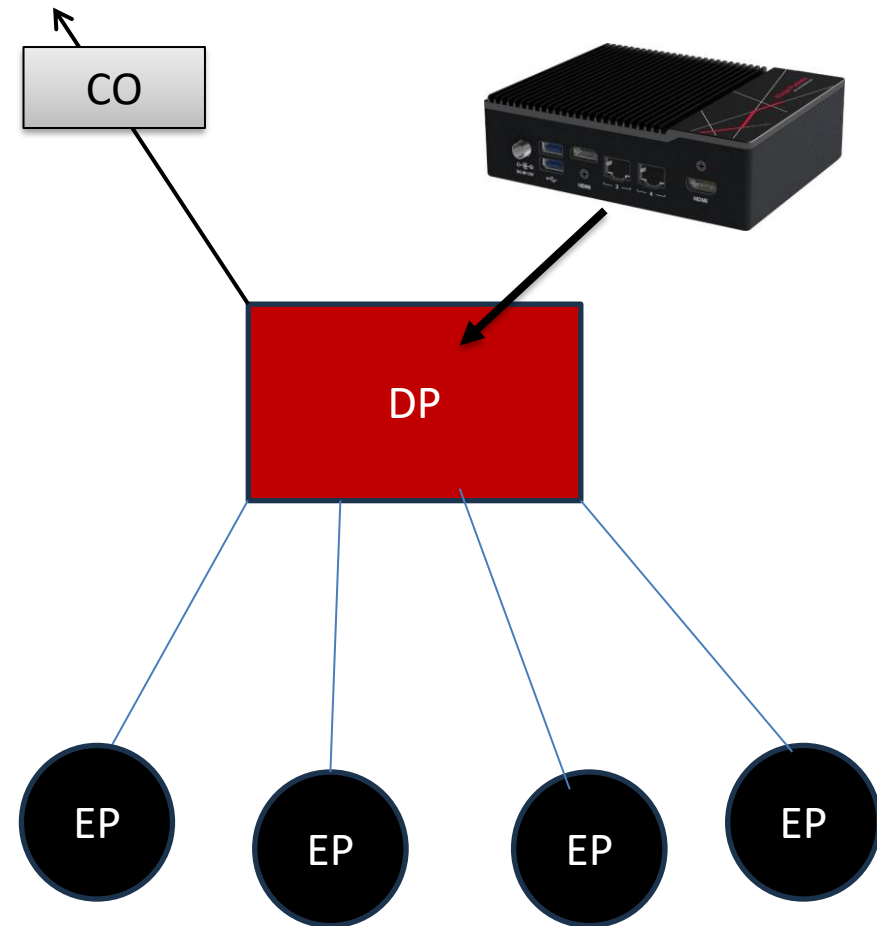
- externí/interní SSD nebo HDD
- Pro přehrání provozu
- Selektivní pcap extrakce
- Může být plně šifrován



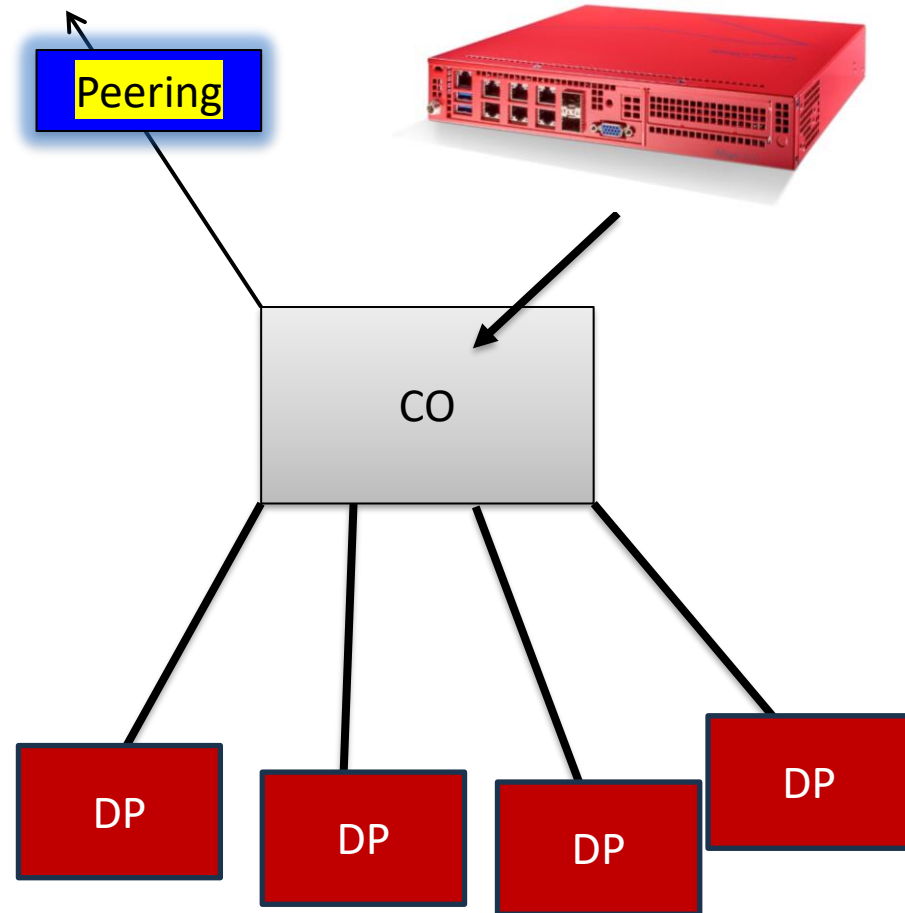
- Multimeter Allegro lze nasadit Inline nebo na mirror port
- Nahrát pcap soubor přímo do Multimetru a analyzovat jej



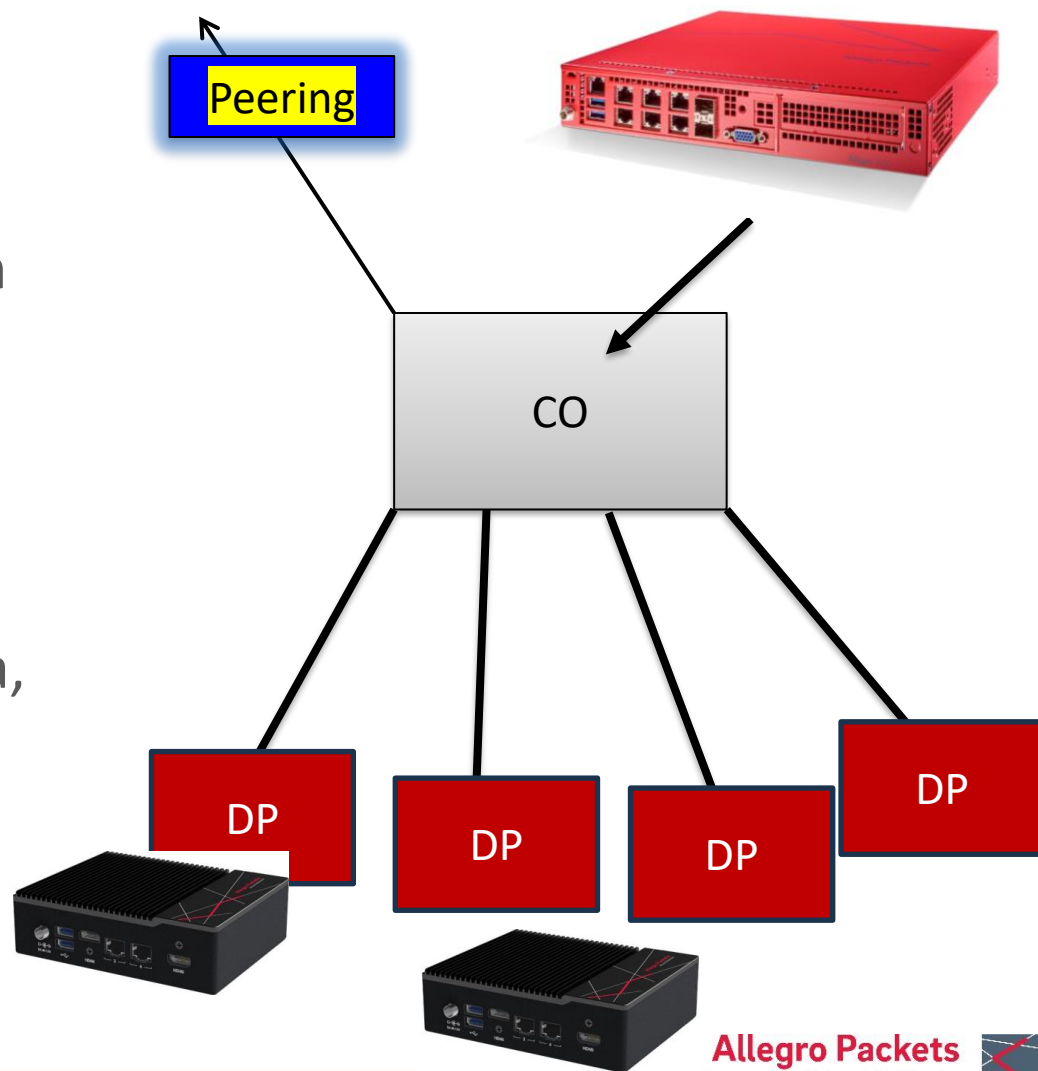
- Nasazení monitorovacího zařízení do distribučního bodu umožní vidět všechny účastníky v tomto bodě, protokoly, spojení odkud kam se co pohybuje a kolik mi jednotliví účastníci posílají v jakém čase dat.
- Distribučních bodů může být ale spousta a tím se toto řešení může stát nákladným.



- Nasazení monitorovacího zařízení do Central Office umožní vidět všechny účastníky ve všech distribučních bodech, spojení odkud kam se co pohybuje a kolik mi jednotlivé distribuční body posílají v jakém čase dat.
- Bohužel tím, že mi data chodí z distribučních bodů ztrácím granularitu dat a nejsem schopný chytat každý detail, který bych mohl potřebovat.



- Nasadím si jednu monitorovací sondu co CO a několik sond do klíčových distribučních bodů odkud mi problémy chodí.
- Tímto způsobem mám přehled o celé síti a nepřicházím o detailní data, která mohou být klíčová pro identifikaci problémů na síti.



- **VÍCE INFORMACÍ O MONITORINGU BUDE PREZENTOVÁNO ZÍTRA NA PŘEDNÁŠCE: K ČEMU JE DOBRÝ MONITORING, ZÁZNAM A ANALÝZA SÍŤOVÝCH PARAMETRŮ A PŘENOSU V 11:20 KTEROU POVEDE PETER POTROK**



Děkujeme za pozornost

david.tichy@profiber.eu
peter.potrok@profiber.eu

AKADEMIE VLÁKNOVÉ OPTIKY A OPTICKÝCH KOMUNIKACÍ[®]

PROFiber Networking CZ s.r.o.
Mezi Vodami 205/29
143 00 Praha 4

PROFiber Networking s.r.o.
Bernolákova 2
917 01 Trnava

the art of
optical
communication

