DOHLED NAD KVALITOU IP SÍTĚ NEBO SLUŽBY POMOCÍ DPI

David Tichý

AKADEMIE VLÁKNOVÉ OPTIKY A OPTICKÝCH KOMUNIKACÍ ®

the art of optical communication

PROFiber NETWORKING

Běžné problémy ISP a provozovatelů sítí

- Správa IP sítě není jen o zajištění **dostatečné kapacity**, ale také o **kvalitě poskytované služby.**
- Zákazníci neřeší rychlost linky (např. 1 Gbps), pokud mají problémy s kvalitou služeb:
  - **Netflix laguje** (sekání streamu).
  - VoIP hovory **se sekají** (zhoršená kvalita hlasových hovorů).
  - Herní servery mají **vysoký ping** (zpoždění v online hrách).

Proč vůbec řešit dohled nad kvalitou IP sítě?

Nejčastější problémy:

- **„Zpomalení" internetu** bez jasné příčiny).
- **Výpadky služeb, které nejsou vidět na běžných monitorovacích nástrojích**
- **Zvýšená latence a packet loss**, ale není jasné, kde přesně se ztrácí pakety.
- **Detekce nechtěného provozu**, jako je malware, DDoS, nebo masivní využívání P2P sítí.

Klíčová otázka:
👉 **Jak rychle a přesně identifikovat, co způsobuje degradaci služby?**

Srovnání monitorovacích nástrojů DPI vs. SNMP, NetFlow, ICMP

ICMP (ping, traceroute) – Základní testy dostupnosti

✅ **Výhody:**

- Rychlé testování dostupnosti sítě.
- Dobré pro základní troubleshooting.

❌ **Nevýhody:**

- Mnoho routerů odpovídá na ICMP s nízkou prioritou (někdy je filtrován úplně).
- Neříká nic o skutečné kvalitě služeb (TCP, UDP aplikace).
- Neměří skutečné uživatelské zkušenosti (jen odpověď na ICMP zprávu).

📌 **ICMP řekne, jestli síť „žije“, ale neřekne, jestli funguje dobře.**

Srovnání monitorovacích nástrojů DPI vs. SNMP, NetFlow, ICMP

SNMP – Monitoring infrastruktury

✅ **Výhody:**

- Poskytuje statistiky o stavu zařízení (CPU, RAM, link load).
- Funguje na všech aktivních prvcích (routery, switche, servery).
- Umí reportovat alarmy (např. překročení prahové hodnoty).

❌ **Nevýhody:**

- Měří pouze stav **zařízení**, ne provoz v síti.
- Neumožňuje vidět **konkrétní aplikace** nebo služby, které způsobují problémy.
- Je často omezen na **periodická měření**, takže nemusí zachytit krátkodobé špičky nebo mikrovýpadky.

📌 **SNMP je užitečný pro monitoring HW, ale ne pro detailní analýzu provozu.**

NetFlow – Statistika provozu

✅ **Výhody:**

- Poskytuje agregované informace o tokách v síti (kdo, kam, kolik dat přenesl).
- Umí identifikovat **objem provozu** mezi zdroji a cíli.
- Podporuje různé exportní formáty (sFlow, IPFIX).

❌ **Nevýhody:**

- **Nemá detailní přehled o obsahu paketů** – nepozná např. ztrátovost VoIP hovorů nebo konkrétní HTTP požadavky.
- Funguje na základě vzorkování – **může ztratit detaily** u krátkých přenosů nebo při vysoké zátěži.
- Neposkytuje informace o kvalitě spojení (latence, jitter, ztrátovost).

📌 **NetFlow poskytuje přehled o tocích dat, ale ne o kvalitě přenosu jednotlivých aplikací.**

Srovnání monitorovacích nástrojů DPI vs. SNMP, NetFlow, ICMP

DPI – Hloubková analýza provozu

✅ **Výhody:**

- **Vidí nejen kdo a kam, ale také co přesně se děje v síti.**
- Umí **rozpoznat konkrétní aplikace a služby**, včetně šifrovaných (např. detekce QUIC u YouTube).
- Dokáže **měřit latenci, jitter, packet loss** pro specifické aplikace.
- Umí identifikovat **zneužití sítě, malware a anomálie**.
- Pomáhá při **řešení sporů se zákazníky** („u nás je to v pořádku, problém je u poskytovatele obsahu").

❌ **Nevýhody:**

- Vyšší **nároky na výkon** než SNMP/NetFlow.
- **Nemůže rozpoznat šifrovaný obsah** (ale pozná typ provozu).
- V některých zemích může mít **regulační omezení** na sledování provozu.

📌 **DPI poskytuje detailní vhled do kvality přenosu a konkrétních aplikací, což ostatní nástroje neumí.**

Shrnutí srovnání

📌 **DPI nenahrazuje SNMP, NetFlow ani ICMP – doplňuje je tam, kde ostatní nástroje nestačí.**

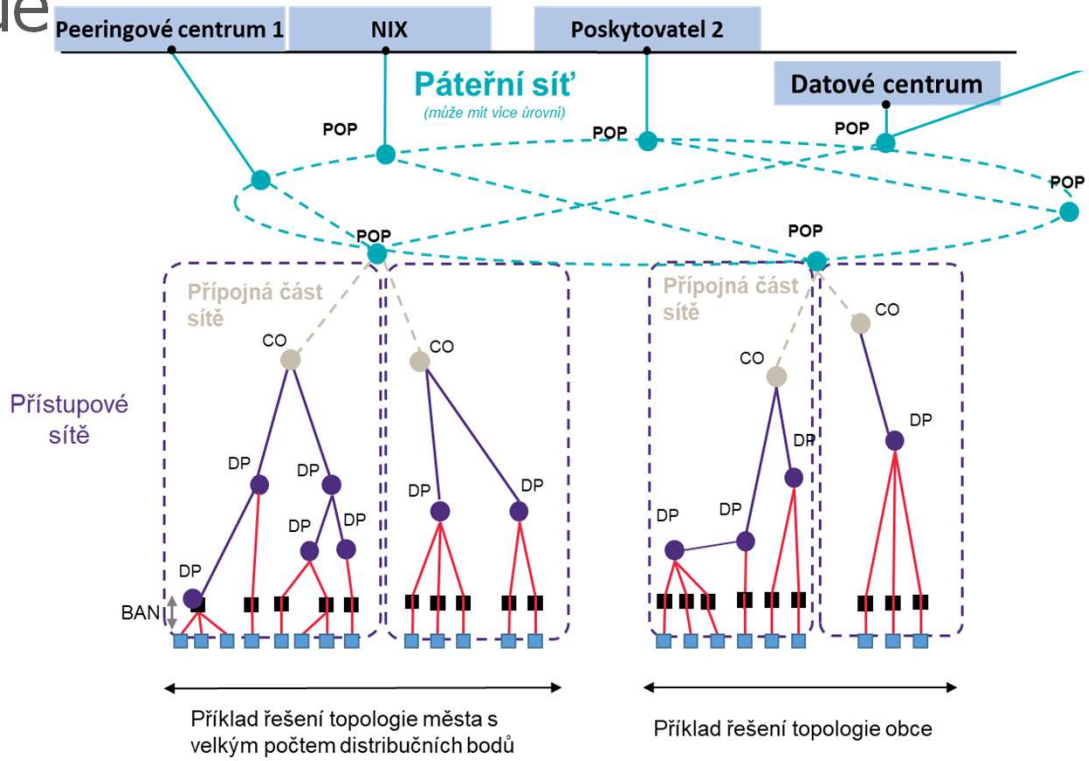
Technologie	Vidí kdo-kam	Vidí co	Měří kvalitu	Detailní analýza	Hlavní výhoda
ICMP	❌	❌	⚠️	❌	Rychlost a dostupnoust
SNMP	❌	❌	❌	❌	Monitoring HW
NETFLOW	✅	⚠️	✅	✅	Agregovaný přehled
DPI	✅	✅	✅	✅	Hloubkový dohled

DPI: Co je potřeba zvážit

- Vysoké náklady na implementaci
- Výkonové nároky
- Šifrovaný provoz
- Soukromí uživatelů

Co nám umožní vidět?

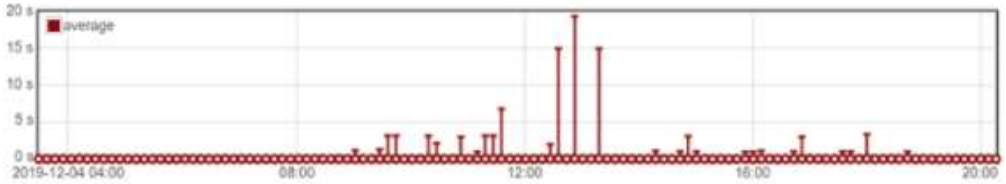
- Zjistit lokaci poruchy pokud jde o výpadek
- Identifikovat typ problému
- Zjistit zda je problém na vaší síti, u koncového uživatele nebo u poskytovatele (CAP)
- Dokazování kvality projektů a zpětné statistiky incidentů



Co potřebujeme vidět?

- 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

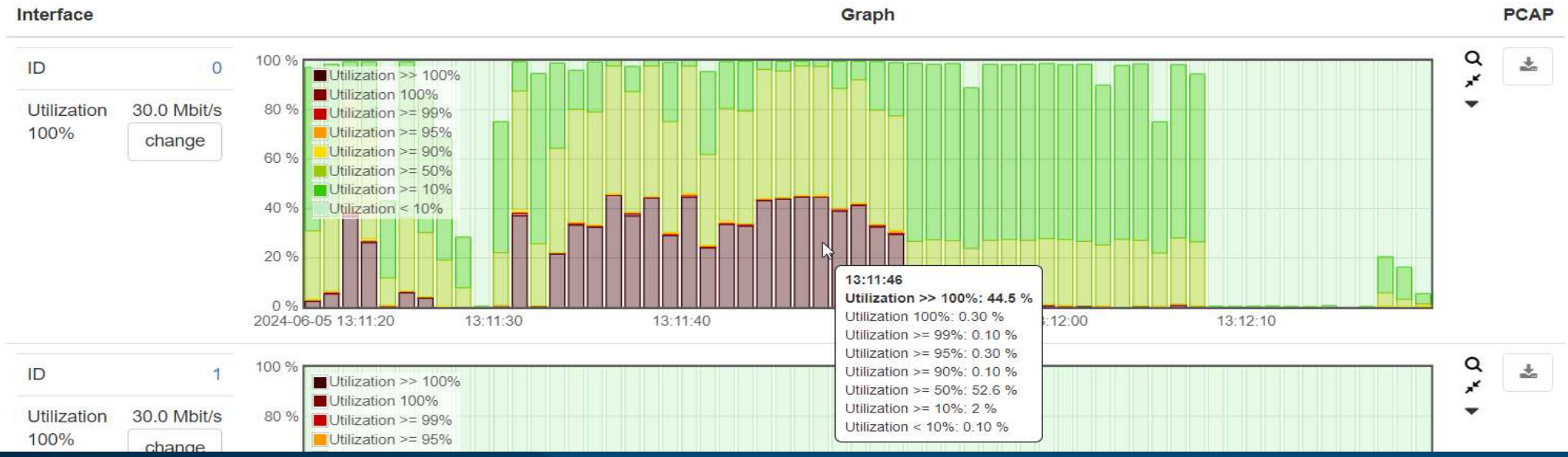
Burst analýza a microbursty

Burst Analýza

- Proces zkoumání datového provozu na síťové lince
- Identifikace krátkodobých zvýšení (burstů) v datovém toku
- Důležité pro detekci přetížení a optimalizaci sítě

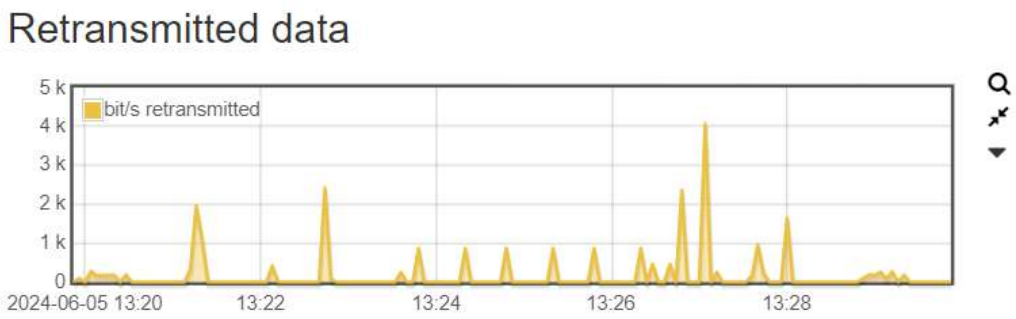
Microbursty

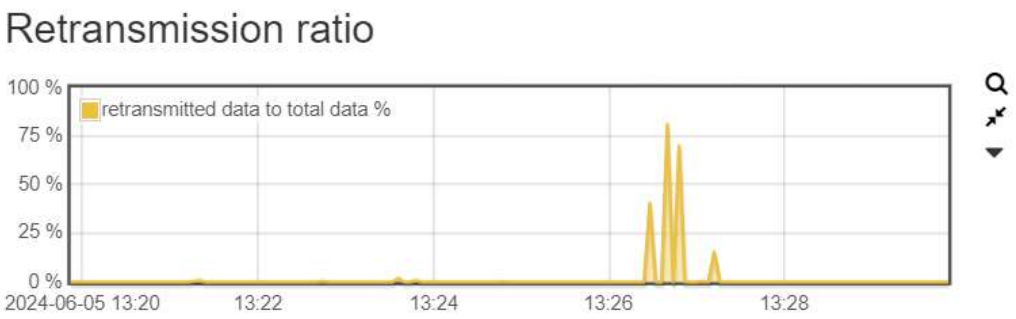
- Velmi krátké a intenzivní bursty (trvají jen několik milisekund)
- Mohou dočasně zahltit síťová zařízení
- Způsobují zvýšenou latenci a ztrátu paketů
- Často nejsou viditelné v běžných měřeních sítě



TCP retransmise a ztráty packetů

- **TCP Retransmise**: Proces, kdy odesilatel znovu pošle paket, který nebyl potvrzen příjemcem v očekávaném čase.
- **Ztráty Paketů**: Situace, kdy paket nedorazí k cíli z důvodu přetížení sítě, chyb v přenosu nebo problému na síťovém zařízení.



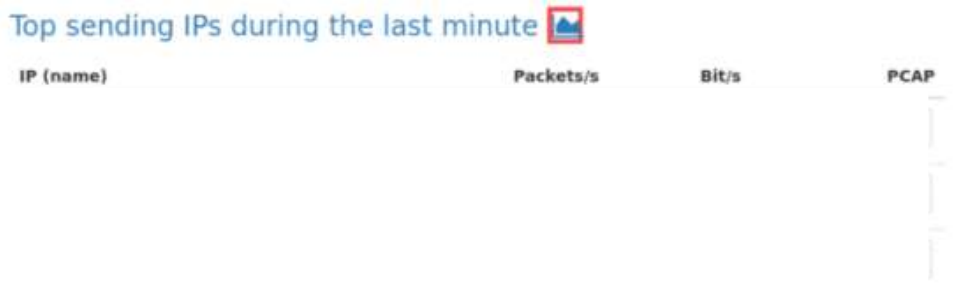


Zdroj: Allegro Packets

Co potřebujeme vidět?

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

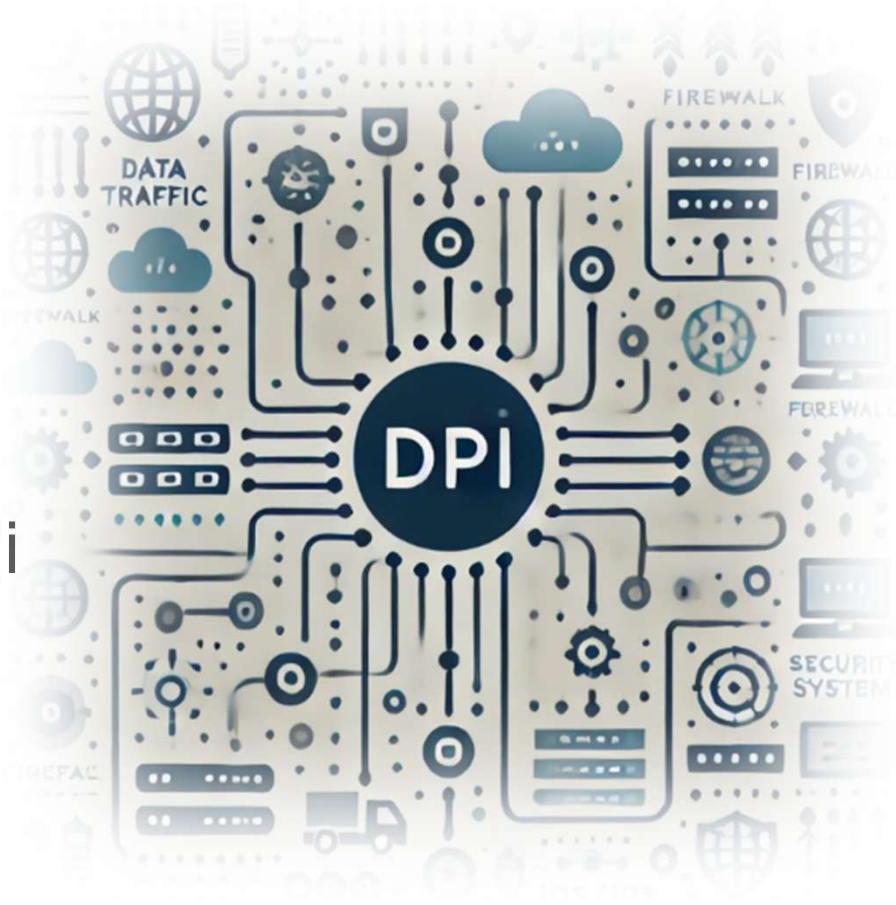
Pokud nemáme dobrou viditelnost, tak tyto místa může být velice obtížné identifikovat nebo dokonce nemožné.



Zdroj: Allegro Packets

Budoucnost správy sítí s DPI

- Zvyšující se nároky na šířku pásma
- Automatizace řízení provozu
- Integrace s bezpečnostními nástroji



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

PROFiber NETWORKING