TROUBLESHOOTING A BEZPEČNOST IP SÍTÍ POMOCÍ DEEP PACKET INSPECTION

David Tichý

AKADEMIE VLÁKNOVÉ OPTIKY A OPTICKÝCH KOMUNIKACÍ ®

the art of optical communication

PROFiber® NETWORKING

Úvodní metafora: Pohled na síť jako na dopravní uzel

- Silnice = Přenosová média
  - Dálnice a silnice vedou data sítí.
- Auta = Data
  - Vidíme počet a rychlost, ale co převáží?
- DPI = Nahlédnutí do nákladu
  - Odhaluje, co je uvnitř – nebezpečí i příležitosti.“

Proč potřebuji vidět, co "auta" vezou?

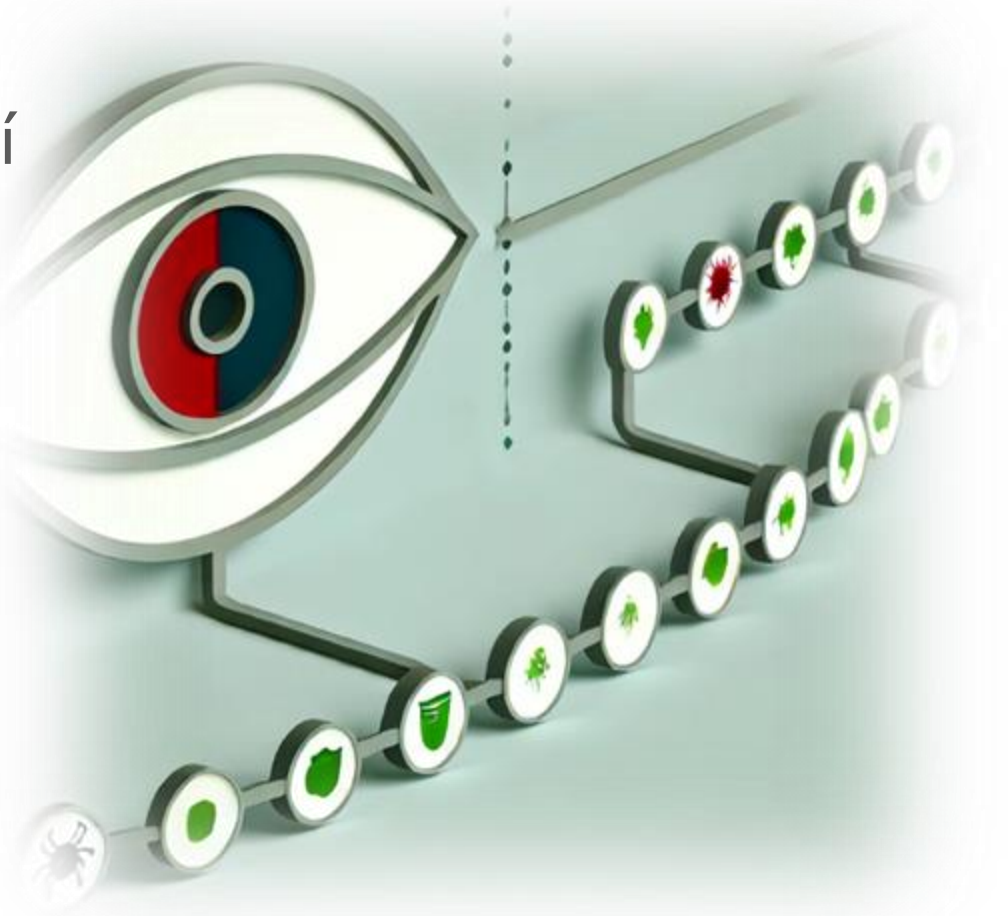
- Skryté hrozby: Nelegální náklad
- Optimalizace provozu
- Rychlejší řešení problémů

DPI jako celní kontrola

- Co DPI dělá?
- Jak DPI funguje?
- Proč je to důležité?

Kde DPI přináší největší výhody?

- Detekce neobvyklého chování
- Řízení priorit provozu
- Prevence šíření hrozeb

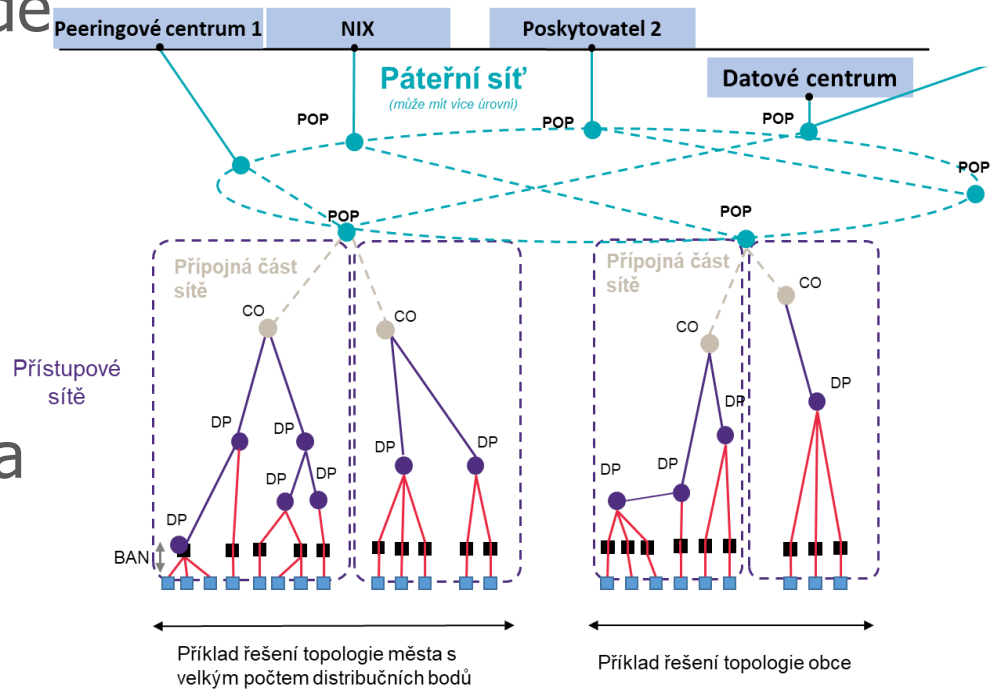


DPI: Co je potřeba zvážit

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

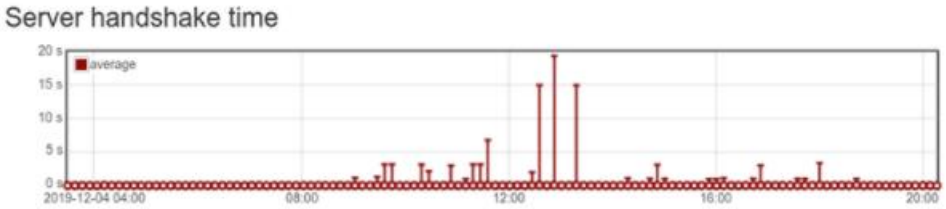
Co nám umožní vidět?

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



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



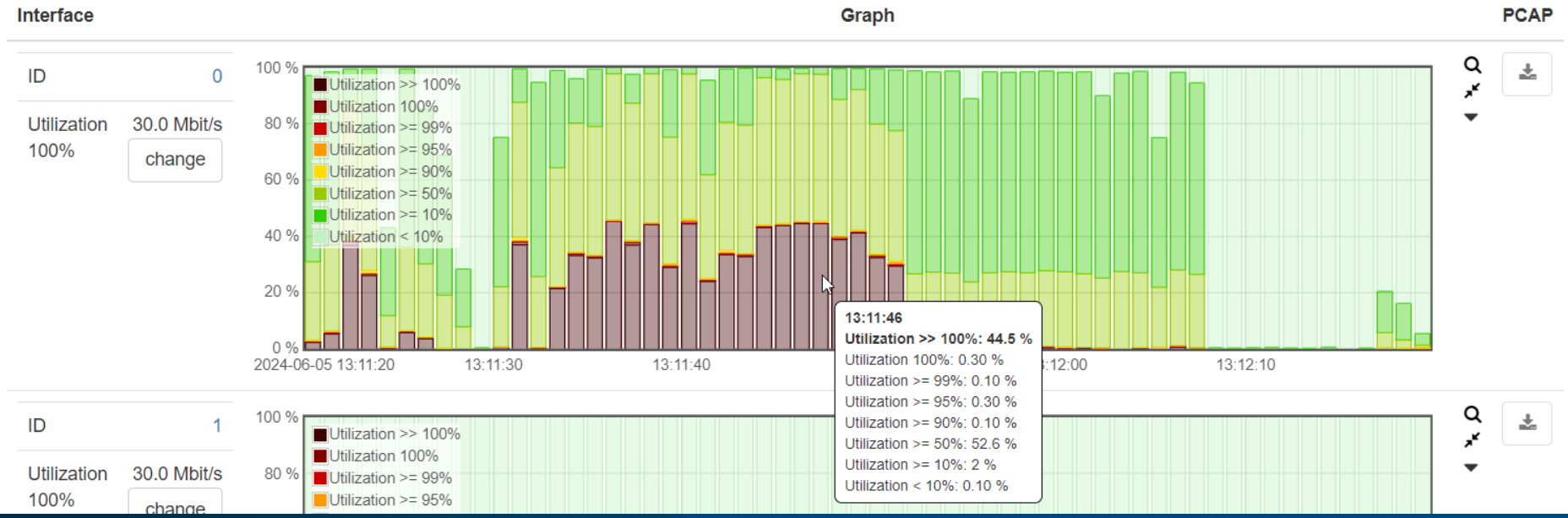
Top sending IPs during the last minute

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 za účelem identifikace krátkodobých zvýšení (burstů) v datovém toku.
- Microbursty: Velmi krátké a intenzivní bursty, trvající jen několik milisekund, které mohou způsobit dočasné zahlcení síťových zařízení a zvýšit latenci.



Příčiny a důsledky microburstů

Příčiny Microburstů

- Aplikace s vysokými nároky na šířku pásma: Video streaming, velké soubory, zálohování dat.
- Špičkové zatížení: Rychlé sekvence přenosů dat.
- Konfigurace sítě: Nesprávné nastavení bufferů v síťových zařízeních.

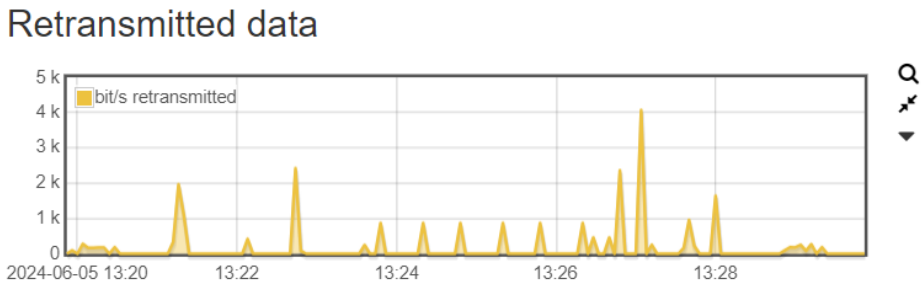
Důsledky Microburstů

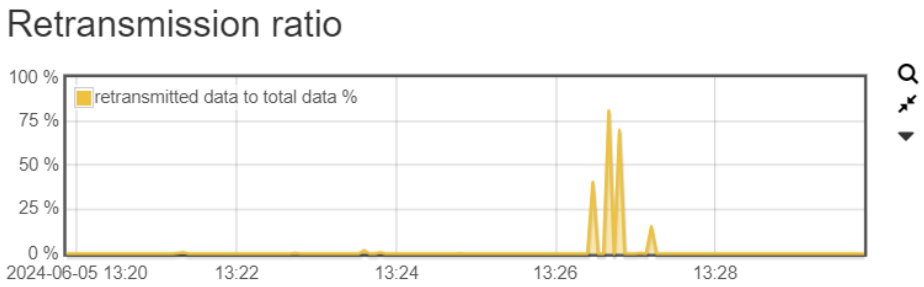
- Ztráta paketů: Přetížení bufferů vede k zahazování paketů.
- Zvýšená latence v důsledku čekání na zpracování přetíženého provozu.
- Snížení kvality služeb: Negativní dopad na aplikace citlivé na latenci, jako jsou VoIP a online hry.

Zdroj: Allegro Packets

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?

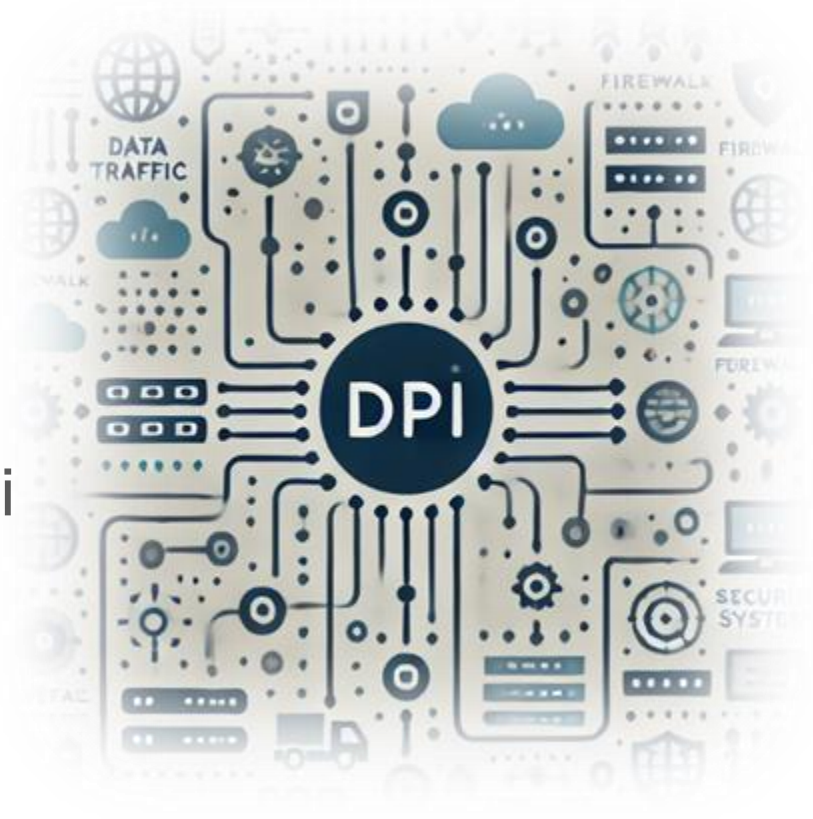
Všechny tyto parametry mohou být indikátory slabých míst na síti nebo v horším případě napadeného místa.

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