

Monitoring a moderní služby sítě

CESNET z.s.p.o.

Tomáš Košnar
kosnar@cesnet.cz



Monitoring sítě – proč ?

- co nelze měřit a sledovat, to nelze dobře ani efektivně řídit
 - předmět zájmu ?
 - ověřování funkčnosti
 - optimalizace chování
 - míra využití
 - řešení anomálních stavů (havárie, incidenty, útoky)
 - spolehlivostní charakteristiky
 - trendy v chování uživatelské komunity
 - mnoho, mnoho dalších důvodů
-
-

Dlouhodobý trend vývoje sítí a jejich služeb

- historicky byla většina komunikačních a informačních služeb realizována prostřednictvím více či méně nezávislých technických prostředků (strana poskytovatele i uživatelů)
- multifunkční komunikační sítě přinesly koexistenci více služeb ve společném technologickém celku (páteřní infrastruktura) a od toho odvozenou určitou míru vzájemné závislosti (transportní mechanismy, podpora typu DNS apod.)
 - konvergence zřetelnější na straně poskytovatele

Dlouhodobý trend vývoje sítí a jejich služeb

- vývoj technologií spěje od koexistence k integraci služeb
 - další konvergence na straně sítí
 - sjednocování technických prostředků uživatelů
- rozhraní síť – uživatel
 - komplexní integrované prostředí (současné služby ~ komponenty)
 - univerzální a transparentní (rozsah a kvalita)
 - distribuované (mobilita v obecném smyslu slova)
 - *....v praxi vnímám jako schopnost sítě poskytovat libovolnou kombinaci např. hlasových, obrazových, datových, výpočetních, skladových a dalších služeb aktuálně požadovaným způsobem (interaktivně, v reálném čase, off-line apod.), konkrétnímu uživateli a to vždy stejně na základě jeho oprávnění bez ohledu na lokalitu*

Vývoj služeb a oblast monitoringu

- složitost
 - dostatečnou úroveň vypovídací hodnoty již prakticky nelze získat měřením jednotlivých veličin
 - požadované výsledky je nutné často skládat z naměřených hodnot získaných naprosto odlišnými typy měření (např. SNMP, logy, Flow)
 - množství údajů
 - nekoresponduje pouze s nárůstem provozu
 - souvisí s jeho skladbou
 - odvíjí se od vyspělosti zařízení
 - množství a typu poskytovaných služeb
-
-

Vývoj služeb a oblast monitoringu

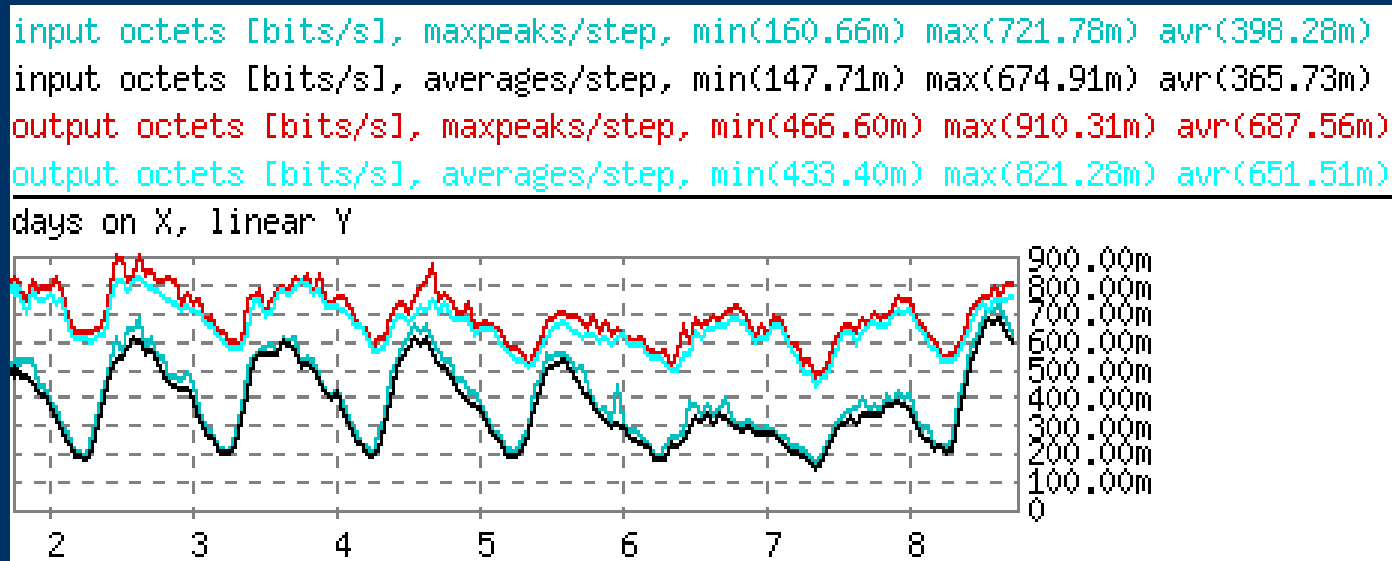
- vývoj služeb od relativně fixní identifikace (transport – čísla portů) k dynamickému chování
- síť TEN-34 CZ, rok 1998 - přibližně 85-95 procent objemu provozu několika málo službami (http, ftp, nntp, smtp apod.)
- síť CESNET2, rok 2004 – skladba provozu – zbývá pouze statistický odhad – zachováno vyjímečné postavení http (rsync, ftp-data), začínají převládat “anonymní” služby (např. pasivní ftp, file-sharing)
- počet exklusivních kombinací zdrojová-cílová IP adresa za jednotku času vzrostl o více než dva řády

Vývoj služeb a oblast monitoringu

- nárůst objemu v oblasti aplikačních logů je analogický
 - vynucené nebo žádoucí zkracování časových kroků měření (např. snmp čítače)
 - různorodost požadavků
 - často protichůdná pro optimální jednopřechodové zpracování (“flow based” systémy)
 - přesnost
 - kritickým parametrem je nutnost stále přesnější časové synchronizace primárních údajů (bezpečnost, incidenty)
-
-

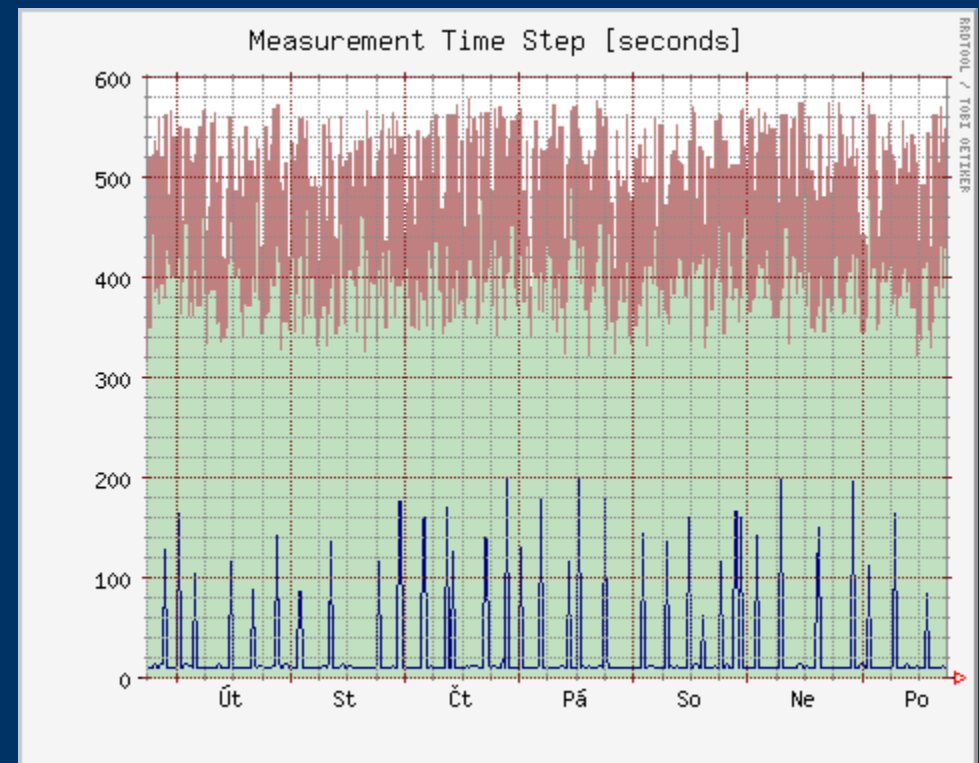
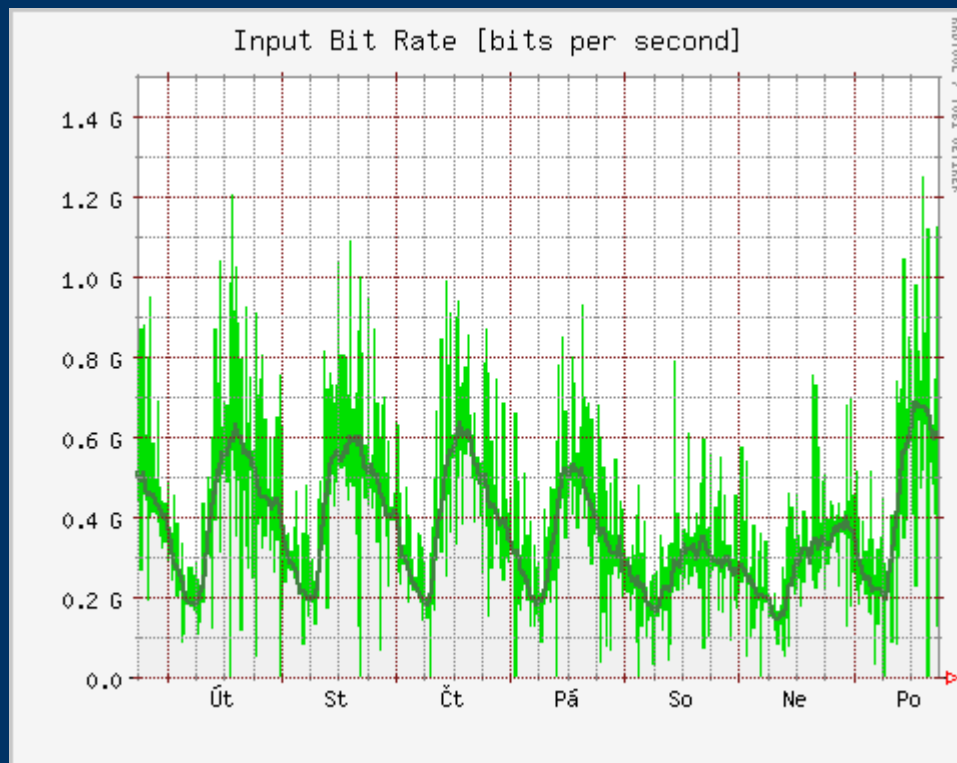
Vývoj služeb a oblast monitoringu

- změna měřítek
 - reálně časové a multimediální služby implikují posun pohledu na problematiku směrem k mikročasovým intervalům, často na možné hranice dané mechanismem (snmp)
 - příklad průběhu zátěže s krokem měření 5 minut



Vývoj služeb a oblast monitoringu

- příklad průběhu zátěže těže linky v příchozím směru s dynamickým krokem měření dle grafu (odchylka špiček až 500Mbps)



Vývoj služeb a oblast monitoringu

- přístup ke sledování dějů směřuje od specifických podmínek k plošnému záběru
- podmíněno například požadavky jako je sledování relací v prostředí dynamických mechanismů řízení směrování nebo nutnost sledovat kromě relací samotných i jejich vliv na okolí
- související trendy v oblasti accountingu a postupné paušalizace při zpoplatňování
 - podstatný je samotný fakt využití (ano/ne) méně míra
 - uživatelé automaticky očekávají dodržení určitých parametrů služby, jejichž zajištění je tak nákladné, že míra využití není podstatná absolutně (“regulační” limitace v rámci paušální platby – např. 10 BG měsíčně apod.)

Vývoj služeb a oblast monitoringu

- zkracování reakční doby “odpovědí na otázky”
 - rychlost reakce rozhoduje v některých případech (DDoS, DoS, konfigurační chyby, jiné provozní anomálie) o udržení parametrů služeb v akceptovatelných mezích, často o stabilitě prostředí jako celku
 - některé pokusy naznačují možný budoucí vývoj směrem k inteligentním automatickým mechanismům na bázi podmíněného výběru strategie chování s vysokou mírou flexibility a variability a případně vysokým stupněm autorizace pro možná automatická regulační opatření
-
-

Vývoj služeb a oblast monitoringu

- zvýšení nároků na zdroje
 - vlastní zdroje primárních informací jsou obvykle technologické celky realizující vlastní funkce komunikačního a informačního prostředí
 - o úspěchu rozhoduje kompromis mezi mírou vypovídací hodnoty informací a mírou agresivitou jejich požadování a sběru
 - významnou roli hraje např. způsob měření (aktivní vs. pasivní) a jeho intenzita (agresivita)
-
-

Vývoj služeb a oblast monitoringu

- transport, zpracování a uskladnění, tedy výpočetní výkon, přenosová a úložná kapacita jsou souvisejícími články řetězce zdrojů
 - specifickou úlohu hrají lidské zdroje - široké pole pro uplatnění vysoké míry přidané intelektuální hodnoty - může řádově ovlivnit nároky na ekonomické zdroje - “chytrá řešení”, schopnost analyzovat a vysvětlit jevy a události...
 - cílem je situace, kdy získané informace mají ještě dostatečnou vypovídací hodnotu vzhledem ke VŠEM požadavkům a zároveň je jejich vytvoření (měření, transport, zpracování, uložení) zvládnutelné vzhledem k dostupným zdrojům
 - je-li problém vůbec v principu zvládnutelný (technologie + know-how) pak obvykle rozhodují ekonomické zdroje
-
-

Vývoj služeb a oblast monitoringu

Dvakrát měř a jednou řež !

Ale než začneš měřit...dlouho, dlouho přemýšlej...

