

Sledování provozu sítě

*Tomáš Košňar
CESNET z.s.p.o.*

kosnar@cesnet.cz

Sledování provozu sítě na základě informací o tocích dat

- „o čem“ sít' je ?
 - ...o přenosu informace z místa A na místo B
- proč sledujeme provoz sítě ?
 - ...bezpečnostní oblast je pouze jedním z důvodů

Sledování provozu sítě na základě informací o tocích dat

- jak nejlépe sledovat provoz sítě ?

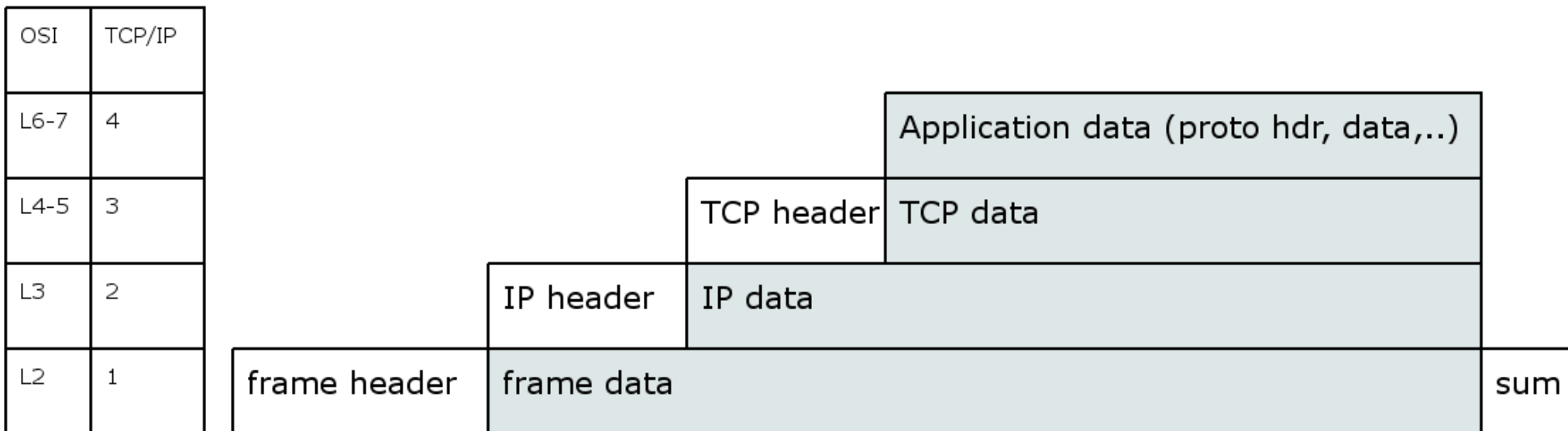
...všechno a neustále ??? 

...snesitelný poměr cena/vypovídací hodnota !!!

...je třeba najít dobrou perspektivu pohledu na síť a její provoz !!!

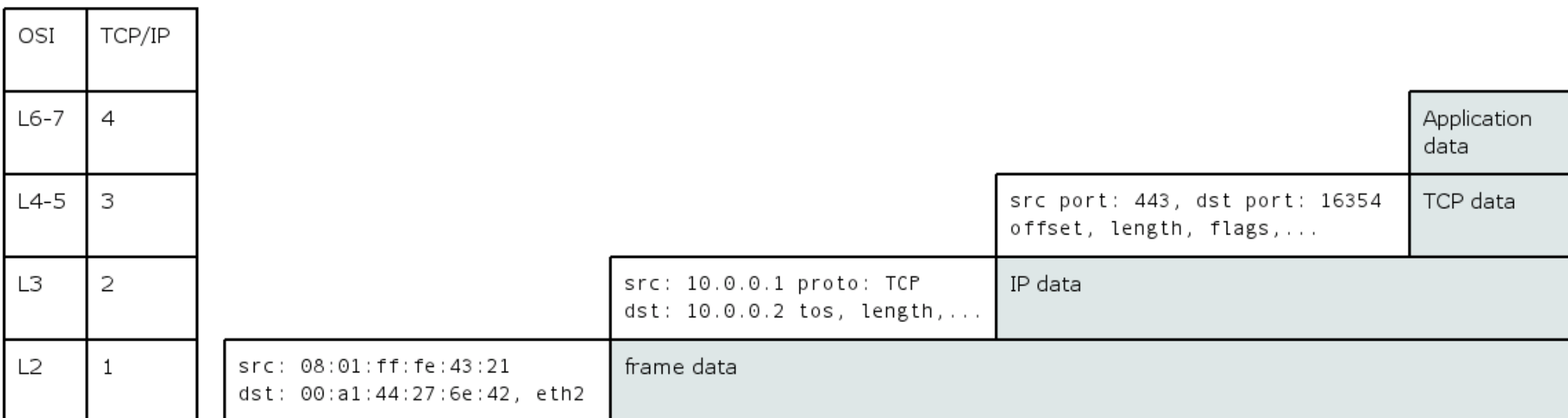
Sledování provozu sítě na základě informací o tocích dat

- vertikální perspektiva



Sledování provozu sítě na základě informací o tocích dat

- vertikální perspektiva



Sledování provozu sítě na základě informací o tocích dat

- vertikální perspektiva
 - samostatná vrstva => nedostatečná
 - směrem k nižším vrstvám
 - klesá vypovídací hodnota (anonymní bity,...)
 - směrem k vyšším vrstvám
 - zpravidla rostou nároky na zdroje

Sledování provozu sítě na základě informací o tocích dat

- horizontální perspektiva
 - síť jako celek
 - část sítě
 - linka/trasa
 - uzlové místo
 - vhodné kombinace
 -

Sledování provozu sítě na základě informací o tocích dat

- nejsou-li k dispozici neomezené zdroje je „*optimální perspektiva*“ **závislá na konkrétních podmínkách**
 - architektura sítě
 - způsob využití sítě (dominantní aplikace, trajektorie významných toků, citlivé oblasti, spektrum a zvyky uživatelů, strategie administrace, ...)

Sledování provozu sítě na základě informací o tocích dat

- koncept **NetFlow** – rozumný kompromis

NetFlow - Cisco Systems Inc. TM

- vybrané informace z hlaviček rodiny TCP/IP protokolů + rozšiřující informace v závislosti podmínkách (autonomní systém, nexthop)
- dočasné uchování v paměti => agregovaný údaj, míra agregace nastavitelná v závislosti na implementaci
- export do míst zpracování (kolektory) – zpravidla UDP, v jednom z exportních formátů (pevné formáty 1/5/7, otevřený 9, ...)

Sledování provozu sítě na základě informací o tocích dat

- informace v NetFlow záznamu
 - a) identifikátory toku => klíč pro doplnění informací z dalších paketů daného toku => NetFlow záznam = **informace o jednom směru toku dat**
 - b) objemové, časové informace => rozsah toku v čase, celkový objem, počet paketů (modifikováno s každým dalším paketem daného toku)
 - c) atributy datagramu (TOS, TCP flags) => agregace (logické OR) v rámci všech paketů příslušných danému toku

Sledování provozu sítě na základě informací o tocích dat

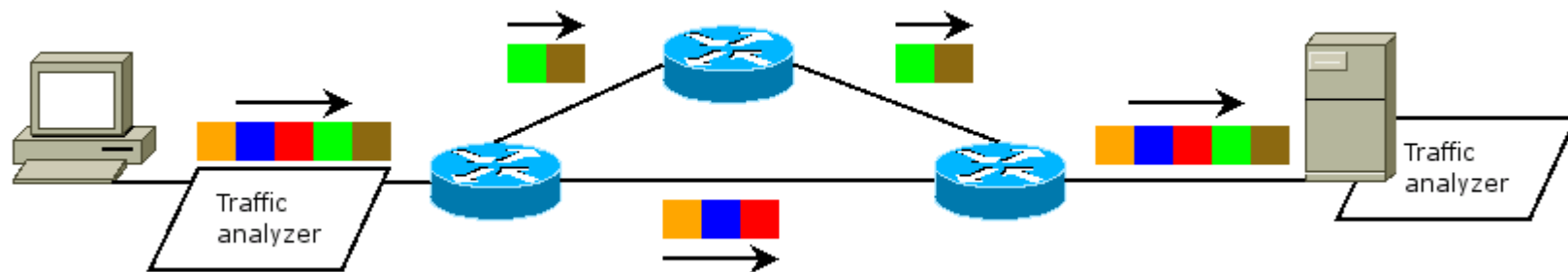
- zdroje NetFlow záznamů
 - přidaná funkčnost směrovačů (např. Cisco, Juniper) za příplatek (v závislosti na výrobcí a architektuře)
 - specializované sondy (např. COMBO FlowMon – CESNET)
 - SW řešení

Sledování provozu sítě na základě informací o tocích dat

- co lze ze sledování na bázi NetFlow „dostat“
 - **co „neteče“ přes zdroj NetFlow záznamů o tom vůbec nic nevíme !!!**
 - ~ *oblasti mimo „horizontální perspektivu“*
- úspěšnost podmiňuje
 - zvolená architektura systému pro sledování
 - vedlejší efekty chování sítě (např. asymetrické směrování, dynamické změny ve směrování)

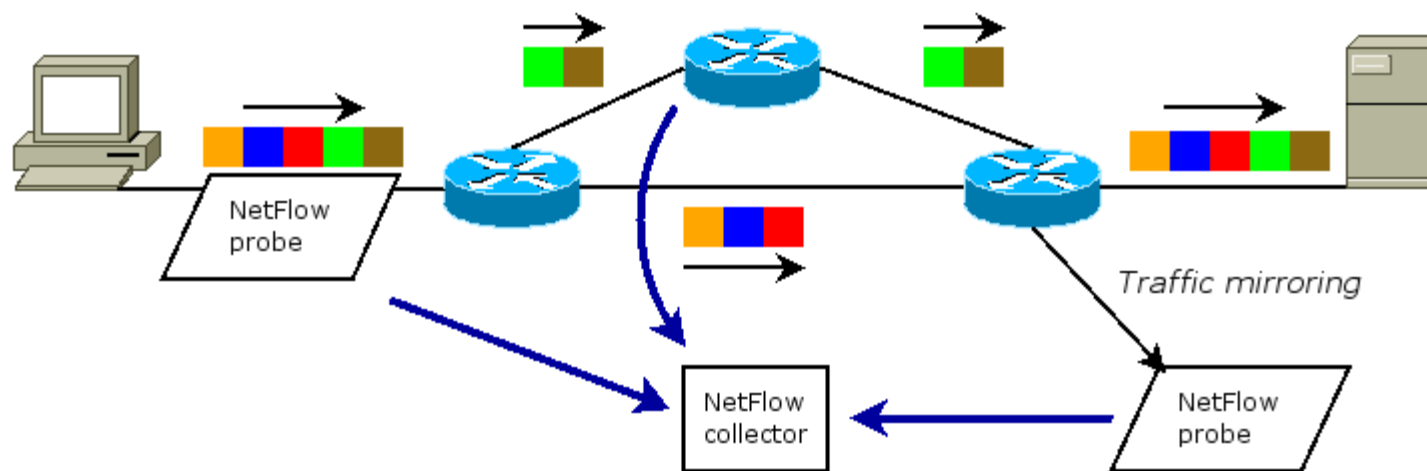
Sledování provozu sítě na základě informací o tocích dat

- efekt změn ve směrování – z pohledu koncových uzlů



Sledování provozu sítě na základě informací o tocích dat

- efekt změn ve směrování – z pohledu různých zdrojů NetFlow záznamů



Sledování provozu sítě na základě informací o tocích dat

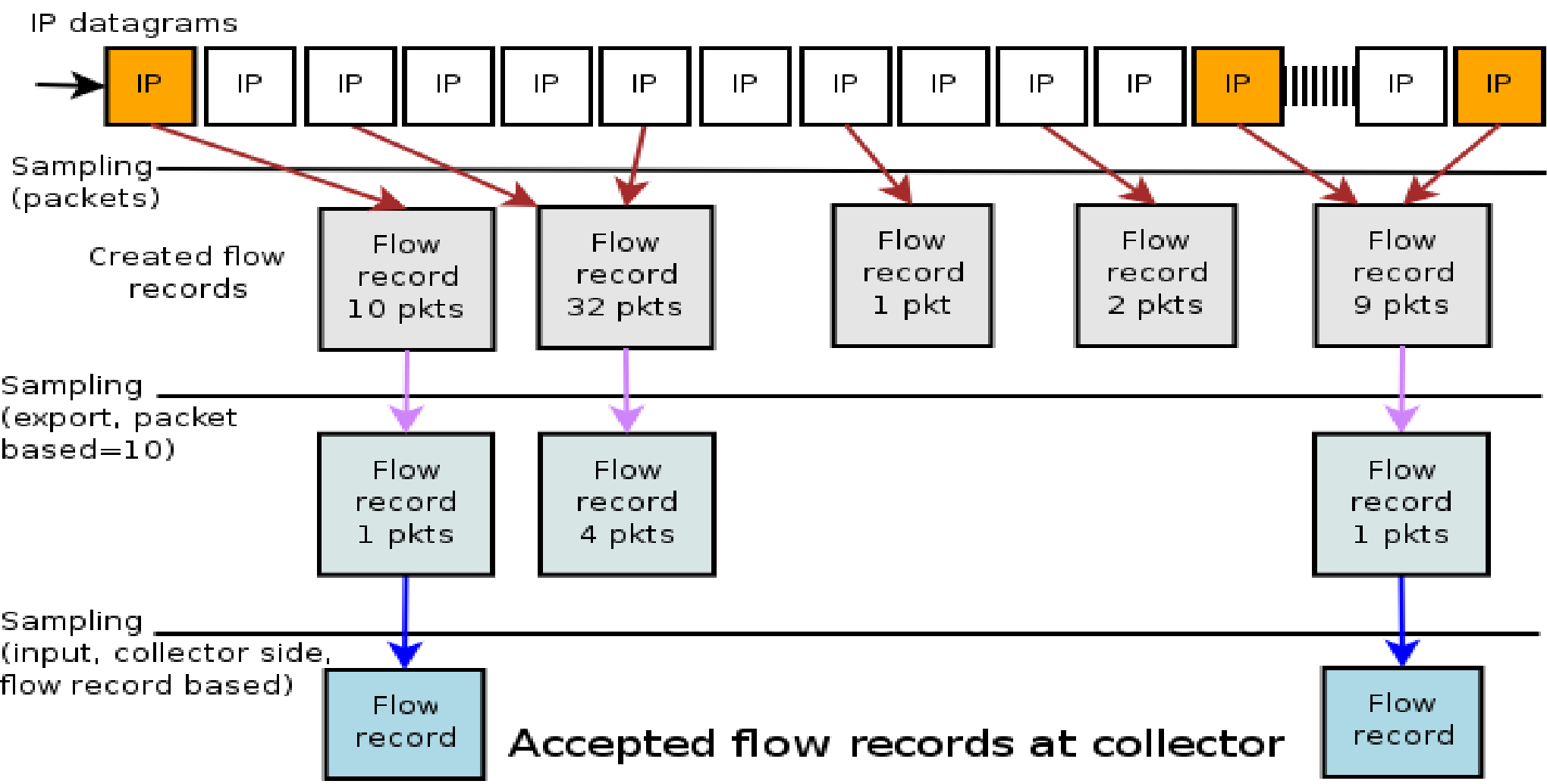
- vzorkování – v některých případech „téměř poznaná nutnost“

principy:

- pakety na „vstupu“ - před mechanismem NetFlow
- při exportu NetFlow záznamů
- na straně kolektorů na úrovni flow záznamů

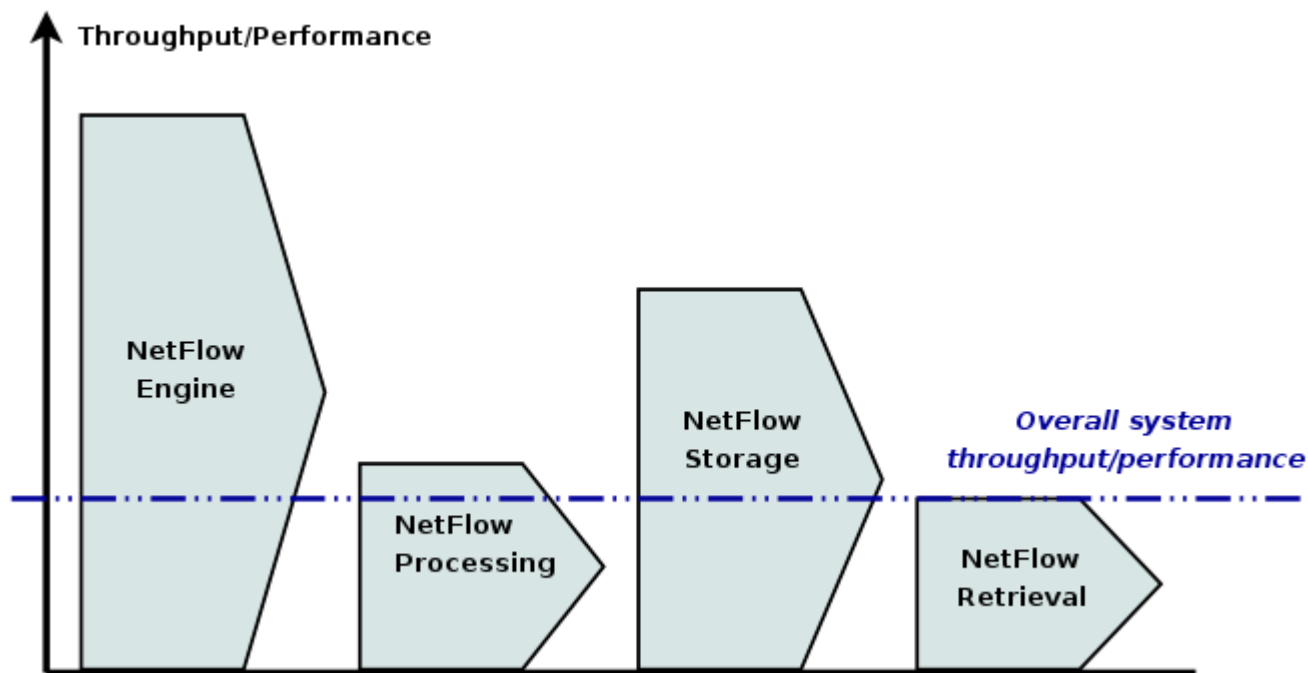
...ztráta vypovídací hodnoty =>

Sledování provozu sítě na základě informací o tocích dat



Sledování provozu sítě na základě informací o tocích dat

- celková principiální výkonnost systému založeného na bázi NetFlow ...*dána nejslabším článkem řetězu*



Sledování provozu sítě na základě informací o tocích dat

- není-li k dispozici 100% obraz provozu sítě, platí při hledání zda byl uskutečněn konkrétní přenos:
 - co jsme našli v NetFlow záznamech - „**jisté jest**“
 - nenalezli jsme-li nic, **neznamená, že se to nestalo**

...potvrzování/vyvracení bezpečnostních incidentů

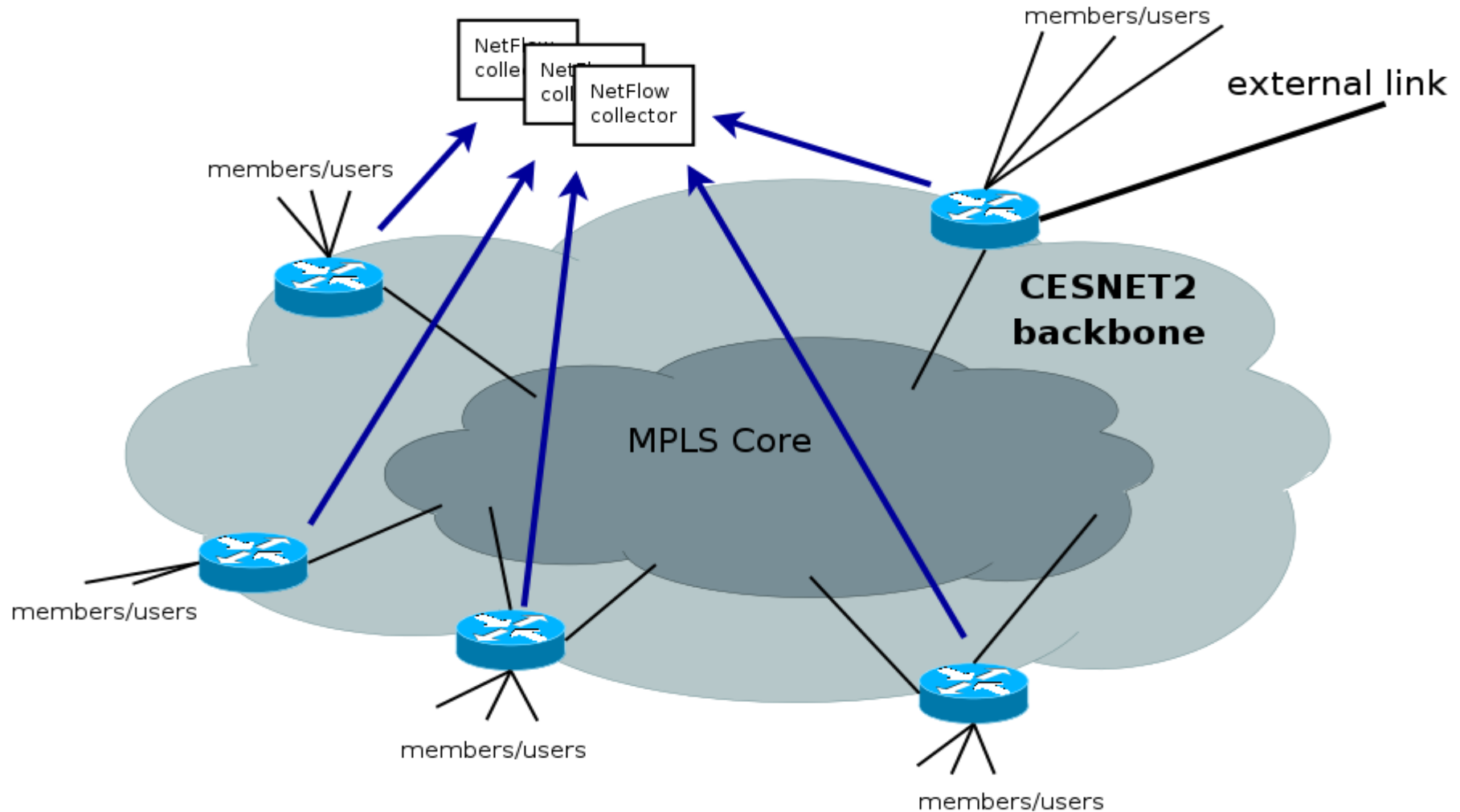
Sledování provozu sítě na základě informací o tocích dat

- co můžeme na základě inspekce NetFlow záznamů s jistotou tvrdit o použitých aplikacích/programech na koncových stanicích ?
 - **nic**, můžeme jenom odhadovat na základě použitých čísel portů a/nebo adres zdrojů/cílů
 - je to informace o **transportu** a ne o obsahu

Systematické, plošné sledování provozu v síti CESNET2

- CESNET2
 - páteřní síť
 - MPLS jádro
- zdroje NetFlow informací
 - směrovače na hraně páteřní sítě

Systematické, plošné sledování provozu v síti CESNET2



Systematické, plošné sledování provozu v síti CESNET2

- systém pro zpracování NetFlow informací - FTAS (Flow-based Traffic Analysis systém)
 - distribuovaná architektura zpracování (aktuálně 8 kolektorů)
 - klasifikační, filtrační mechanismy, post-processing (specifické statistiky)
 - *uchování přijatých NetFlow záznamů v neagregované podobě*

Systematické, plošné sledování provozu v síti CESNET2

- úskalí – množství souvisle exportovaných NetFlow záznamů
 - => vzorkování - aktuálně na úrovni NetFlow záznamů na straně kolektorů
 - podmíněno architekturou směrovačů
 - snahou o maximální vypovídací hodnotu
 - aktuálně cca 1 ze 2 až 1 z 8
 - není synchronní - většina toků prochází přes 2 sledované směrovače – zvýšená pravděpodobnost nalezení konkrétního toku

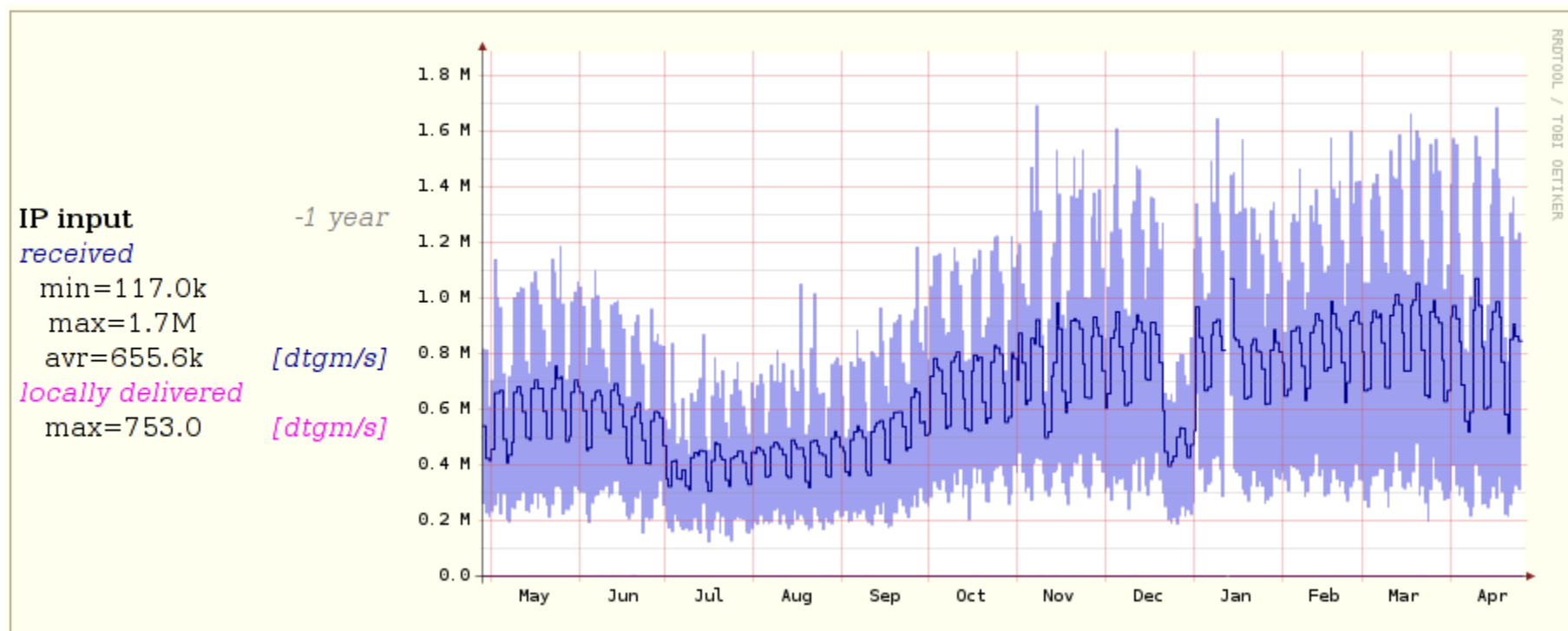
Systematické, plošné sledování provozu v síti CESNET2

- úskalí – množství souvisle exportovaných NetFlow záznamů
 - => omezená doba uchování neagregovaných NetFlow záznamů (ty které prošly vzorkovacím mechanismem)
 - aktuálně 9-14 dní

...parametry se průběžně mění

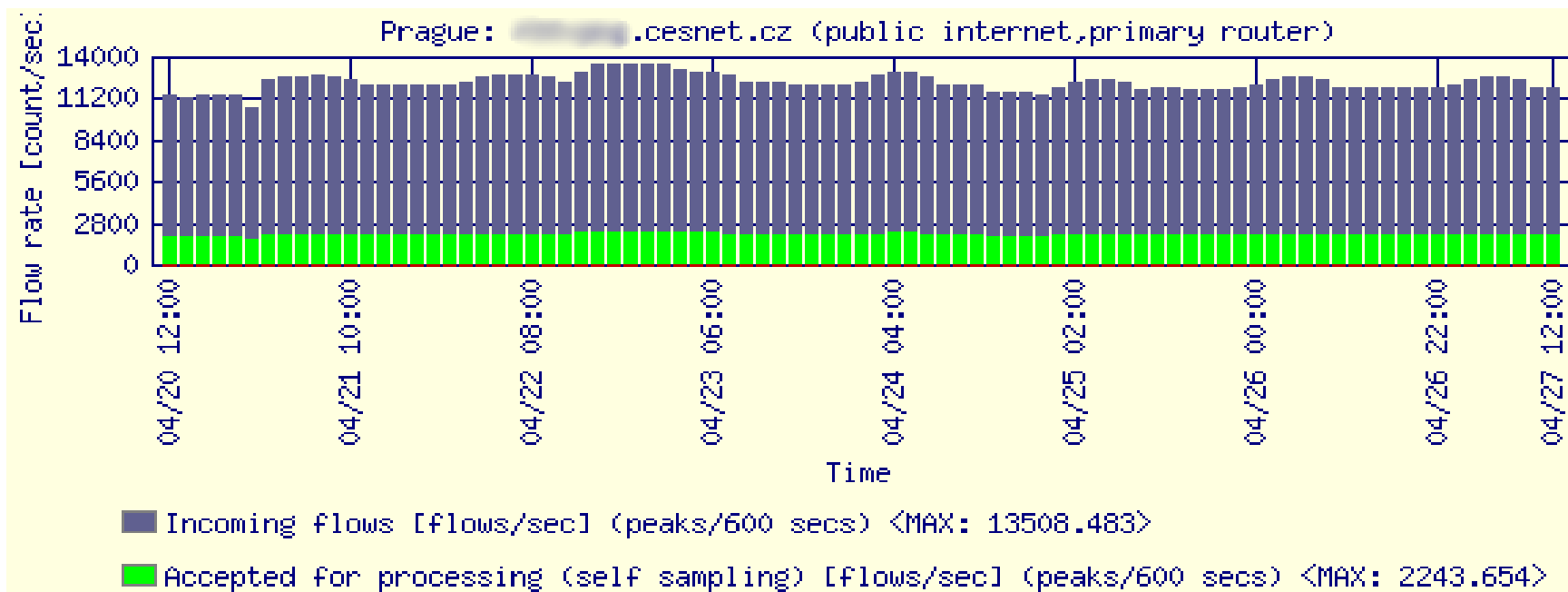
Systematické, plošné sledování provozu v síti CESNET2

- průběh počtu přijatých IP datagramů na jednom z páteřních externích směrovačů sítě CESNET2



Systematické, plošné sledování provozu v síti CESNET2

- průběh počtu příchozích a akceptovaných NetFlow záznamů z jednoho z páteřních externích směrovačů sítě CESNET2 na kolektoru systému FTAS



Systematické, plošné sledování provozu v síti CESNET2

- z předchozího vyplývá průměrně řádově ~100 paketů na jeden NetFlow záznam (oba průběhy ze stejného směrovače)
 - jaké je rozložení paketů v rámci vzorku NetFlow záznamů ?

Systematické, plošné sledování provozu v síti CESNET2

- náhodný výběr – cca 100 000 NetFlow záznamů
- seříděno podle počtu paketů sestupně

o	>	Pkts-measured								
1.		68.370 kp	2001.	0.538 kp	10001.	68.000 p	50001.	5.000 p	74738.	2.000 p
2.		65.545 kp	2002.	0.538 kp	10002.	68.000 p	50002.	5.000 p	74739.	2.000 p
3.		45.681 kp	2003.	0.538 kp	10003.	68.000 p	50003.	5.000 p	74740.	2.000 p
4.		37.465 kp	2004.	0.538 kp	10004.	68.000 p	50004.	5.000 p	74741.	2.000 p
5.		33.555 kp	2005.	0.537 kp	10005.	68.000 p	50005.	5.000 p	74742.	2.000 p
6.		30.893 kp	2006.	0.537 kp	30001.	11.000 p			74743.	1.000 p
7.		30.094 kp	2007.	0.537 kp	30002.	11.000 p			74744.	1.000 p
8.		28.405 kp	2008.	0.537 kp	30003.	11.000 p			74745.	1.000 p
9.		27.068 kp	2009.	0.536 kp	30004.	11.000 p			74746.	1.000 p
10.		25.525 kp	2010.	0.536 kp	30005.	11.000 p			74747.	1.000 p
									74748.	1.000 p
									74749.	1.000 p

- progresivní pokles počtu paketů/záznam
- průměrně 70,4 paketů/flow, 25% záznamů – pouze 1 paket

Systematické, plošné sledování provozu v síti CESNET2

- jaké informace ve vztahu k bezpečnosti je možné získat ?
 - **ad-hoc** detailní/agregované statistiky o komunikaci požadovaných uzlů sítě
 - komplexní podmínky pro výběr např:
`dst_ip=10.0.0.1 and dst_port=2048-65535 and
src_port=4012,35128,41000-43178 and
src_ip=10.4.0.0/16,10.0.1.0/24 and
src_ip<>10.4.0.1-10.4.0.127 and proto=6`
 - musí být „nasbíráno“... (trajektorie, vzorkování, expirace)
 - *bezpečnost: potvrzení komunikace, stěžejní*

Systematické, plošné sledování provozu v síti CESNET2

src_ip=www.google.com and
dst_ip=147.32.192.0/255.255.240.0 and src_port=80

Selected Results

Flow Src. Fields, Flow Dst. Fields			Flow Common Fields	Value Fields	
<input checked="" type="checkbox"/> Src-IP	<input checked="" type="checkbox"/> Src-ifIndex		<input checked="" type="checkbox"/> Protocol	<input checked="" type="checkbox"/> Flow-Start	<input checked="" type="checkbox"/> Pkts-measured
<input checked="" type="checkbox"/> Src-Port	<input checked="" type="checkbox"/> Src-Bitmask		<input checked="" type="checkbox"/> TOS-flags	<input checked="" type="checkbox"/> Flow-End	<input type="checkbox"/> Pkts-estimated
<input type="checkbox"/> Src/Prev-AS			<input type="checkbox"/> TCP-flags	<input checked="" type="checkbox"/> Bytes-measured	<input type="checkbox"/> Average packet length
<input checked="" type="checkbox"/> Dst-IP	<input checked="" type="checkbox"/> Dst-ifIndex		<input type="checkbox"/> Nexthop	<input type="checkbox"/> Bytes-estimated	
<input checked="" type="checkbox"/> Dst-Port	<input checked="" type="checkbox"/> Dst-Bitmask				
<input type="checkbox"/> Dst/Next-AS					

Results

	Src-IP	Dst-IP	Src-ifIndex	Dst-ifIndex	Pkts-measured	Bytes-measured	Flow-Start	Flow-End	Src-Port	Dst-Port	Protocol	TOS-flags	Src-Bitmask	Dst-Bitmask
1.	209.85.129.99	147.32.192.0	85	1	12.000 p	15.867 KB	07/05/02 10:36:49.009	07/05/02 10:36:49.073	www (80)	2420	tcp (6)	high_throughput(16)	23	16
2.	209.85.129.104	147.32.206.0	85	1	6.000 p	2.596 KB	07/05/02 10:38:11.510	07/05/02 10:38:11.958	www (80)	59191	tcp (6)	routine(0)	23	16
3.	209.85.129.99	147.32.192.0	85	1	5.000 p	0.873 KB	07/05/02 10:38:03.841	07/05/02 10:38:06.529	www (80)	1280	tcp (6)	routine(0)	23	16
4.	209.85.129.104	147.32.192.0	85	1	1.000 p	40.000 B	07/05/02 10:35:05.618	07/05/02 10:35:05.618	www (80)	1942	tcp (6)	routine(0)	23	16

Systematické, plošné sledování provozu v síti CESNET2

- jaké informace ve vztahu k bezpečnosti je možné získat ?
 - **ad-hoc** „top listy“ (objem, pakety) požadovaných uzlů sítě
 - časově akceptovatelný rozsah vs. vymezuující podmínka vs. požadované identifikátory komunikace
 - a) `dst_ip=0.0.0.0-255.255.255.255,`
`identifikátor=src_ip`
 - b) `src_ip=147.32.192.0/24,`
`identifikátor=dst_ip,src_port,proto`
 - *bezpečnost: zdroje/cíle „paketových smrští“ (scan,...)*

Systematické, plošné sledování provozu v síti CESNET2

- rozsah 65535 adres, 5 minut, 5 identifikátorů přenosu
- výsledek hledání => 50000 záznamů (při vzorkování: 1 ze 4)

Flow Src. Fields, Flow Dst. Fields

<input checked="" type="checkbox"/> Src-IP	<input checked="" type="checkbox"/> Dst-IP
<input checked="" type="checkbox"/> Src-Port	<input checked="" type="checkbox"/> Dst-Port
<input type="checkbox"/> Src/Prev-AS	<input type="checkbox"/> Dst/Next-AS
<input type="checkbox"/> Src-ifIndex	<input type="checkbox"/> Dst-ifIndex
<input type="checkbox"/> Src-Bitmask	<input type="checkbox"/> Dst-Bitmask

Flow Common Fields

<input checked="" type="checkbox"/> Protocol	<input type="checkbox"/> TCP-flags
<input type="checkbox"/> TOS-flags	<input type="checkbox"/> Nexthop

Value Fields

<input type="checkbox"/> Flow-Start	<input type="checkbox"/> Bytes-estimated
<input type="checkbox"/> Flow-End	<input checked="" type="checkbox"/> Pkts-measured
<input checked="" type="checkbox"/> Bytes-measured	<input type="checkbox"/> Pkts-estimated

Fields Query Conditions - Simple Form ...you may want to work with 'advanced' condition form >>

	Source	relation	Destination
IP address		and	0.0/16
Service Port		and	
AS Number (origin/neighbor)		and	
Interface SNMP Index		and	

Protocol	TCP-flags	TOS-flags
255 ax.25 ddp	ack fin push	critic_ecp flash high_reliability

Time Parameters

current-25m - current-20m

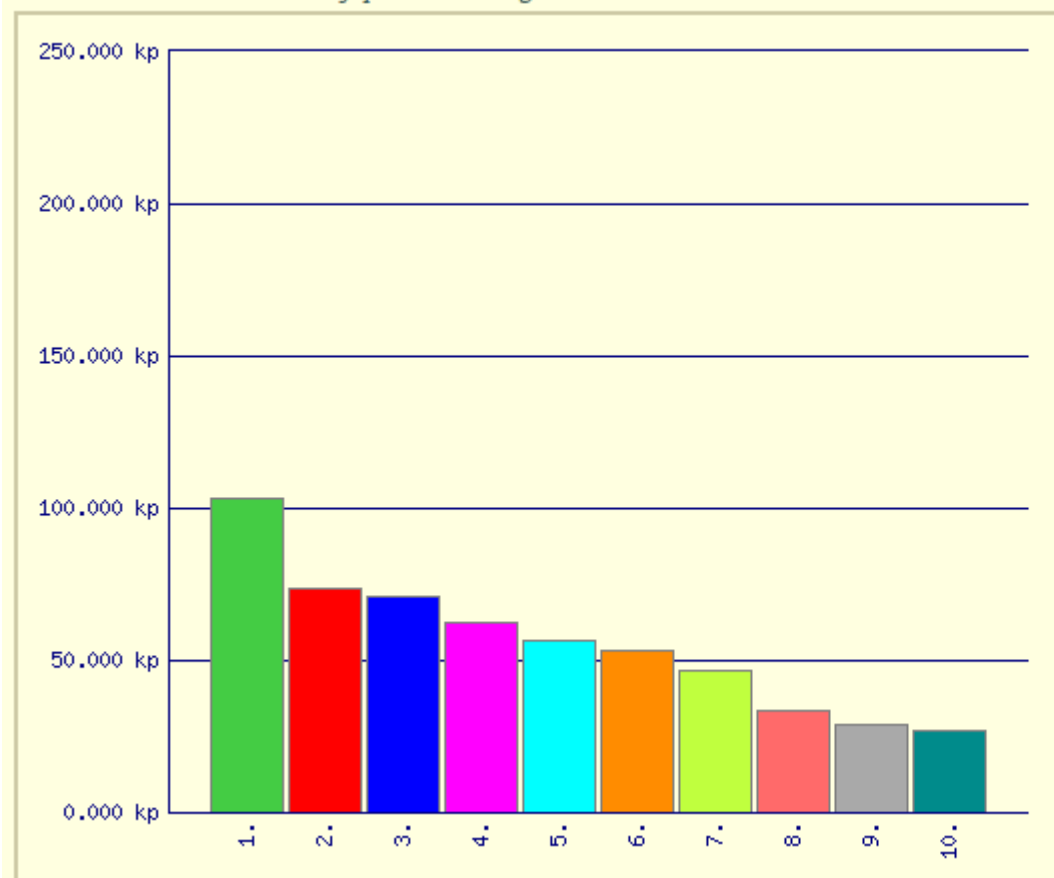
...optional time step: auto

When 'aggregation' set for data (in 'Data Storage Information' box), no available results can be expected within the history specified by that value...

Systematické, plošné sledování provozu v síti CESNET2

- agregace podle cíle, sumární – prvních 10 ~ téměř polovina paketů celé sítě

Pkts-measured: summary per time range



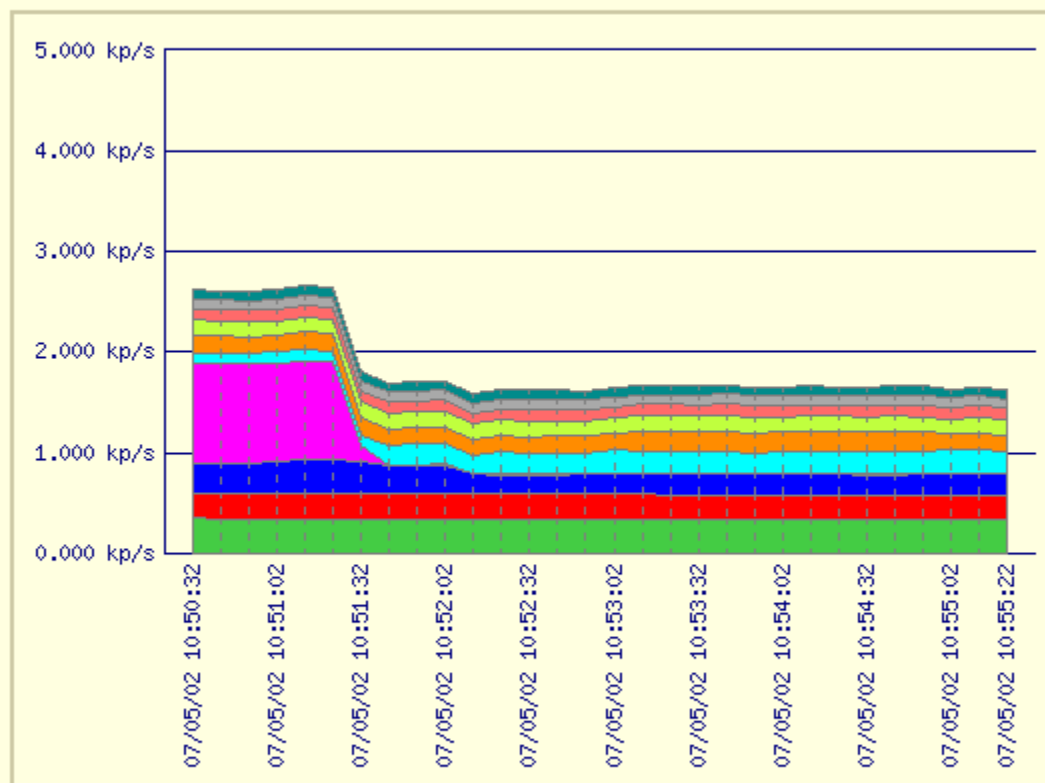
Summary	In graph	0.556 mp	45.27%
	Rest of results	0.672 mp	54.73%
	Total	1.228 mp	100.00%

o	>	Dst-IP	Protocol	Pkts-measured
1.	v	.172.148	tcp (6)	102.926 kp
2.	v	.172.243	tcp (6)	73.790 kp
3.	v	.25.165	tcp (6)	70.639 kp
4.	v	.88.222	tcp (6)	62.605 kp
5.	v	.32.77	tcp (6)	56.540 kp
6.	v	.16.157	tcp (6)	52.925 kp
7.	v	.25.252	tcp (6)	46.715 kp
8.	v	.157.55	udp (17)	33.428 kp
9.	v	.157.219	tcp (6)	29.180 kp
10.	v	.104.152	tcp (6)	27.209 kp

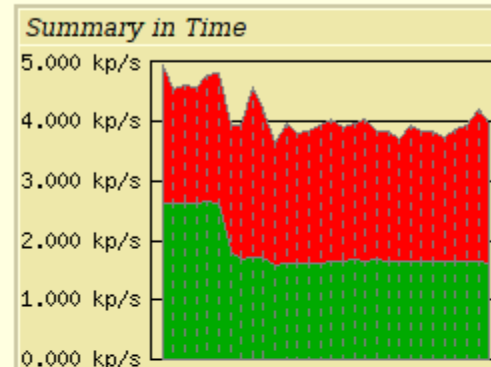
Systematické, plošné sledování provozu v síti CESNET2

- agregace podle cíle, průběh v čase

Pkts-measured: rates



Summary	In graph	0.556 mp	45.27%
	Rest of results	0.672 mp	54.73%
	Total	1.228 mp	100.00%

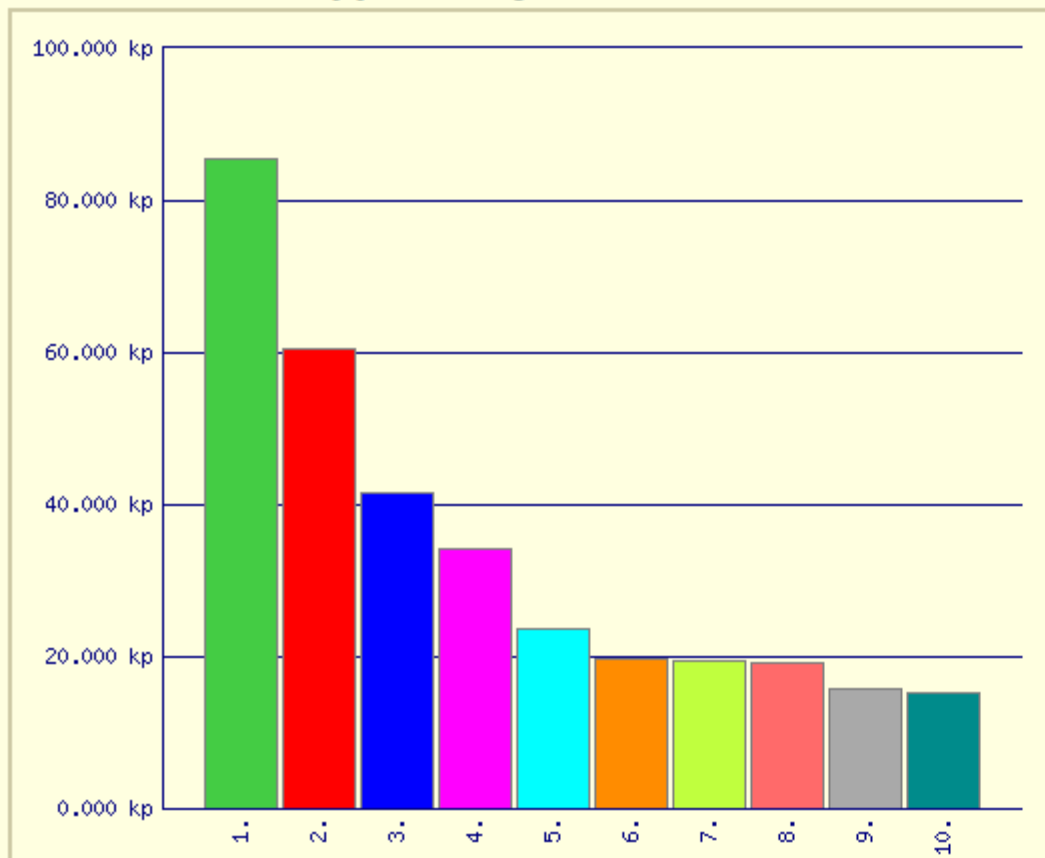


o	>	Dst-IP	Protocol	Pkts-measured
1.	>	172.148	tcp (6)	102.926 kp
2.	>	172.243	tcp (6)	73.790 kp
3.	>	25.165	tcp (6)	70.639 kp
4.	>	88.222	tcp (6)	62.605 kp
5.	>	32.77	tcp (6)	56.540 kp
6.	>	16.157	tcp (6)	52.925 kp
7.	>	25.252	tcp (6)	46.715 kp
8.	>	157.55	udp (17)	33.428 kp

Systematické, plošné sledování provozu v síti CESNET2

- agregace podle **zdroje+cíle**, sumární – prvních 10 ~ pouze 27% paketů celé sítě

Pkts-measured: summary per time range



Summary	In graph	0.335 mp	27.27%
	Rest of results	0.893 mp	72.73%
	Total	1.228 mp	100.00%

o	>	Src-IP	Dst-IP	Protocol	Pkts-measured
1.	>	195.113.125.24	172.148	tcp (6)	85.486 kp
2.	>	147.32.118.220	88.222	tcp (6)	60.453 kp
3.	>	90.225.116.33	32.77	tcp (6)	41.512 kp
4.	>	85.132.166.220	25.165	tcp (6)	34.142 kp
5.	>	82.109.167.130	25.252	tcp (6)	23.753 kp
6.	>	212.20.107.214	25.165	tcp (6)	19.806 kp
7.	>	64.12.201.185	157.80	tcp (6)	19.467 kp
8.	>	205.188.210.217	153.177	tcp (6)	19.209 kp
9.	>	82.228.77.45	172.243	tcp (6)	15.799 kp
10.	>	82.156.231.123	172.243	tcp (6)	15.227 kp

Systematické, plošné sledování provozu v síti CESNET2

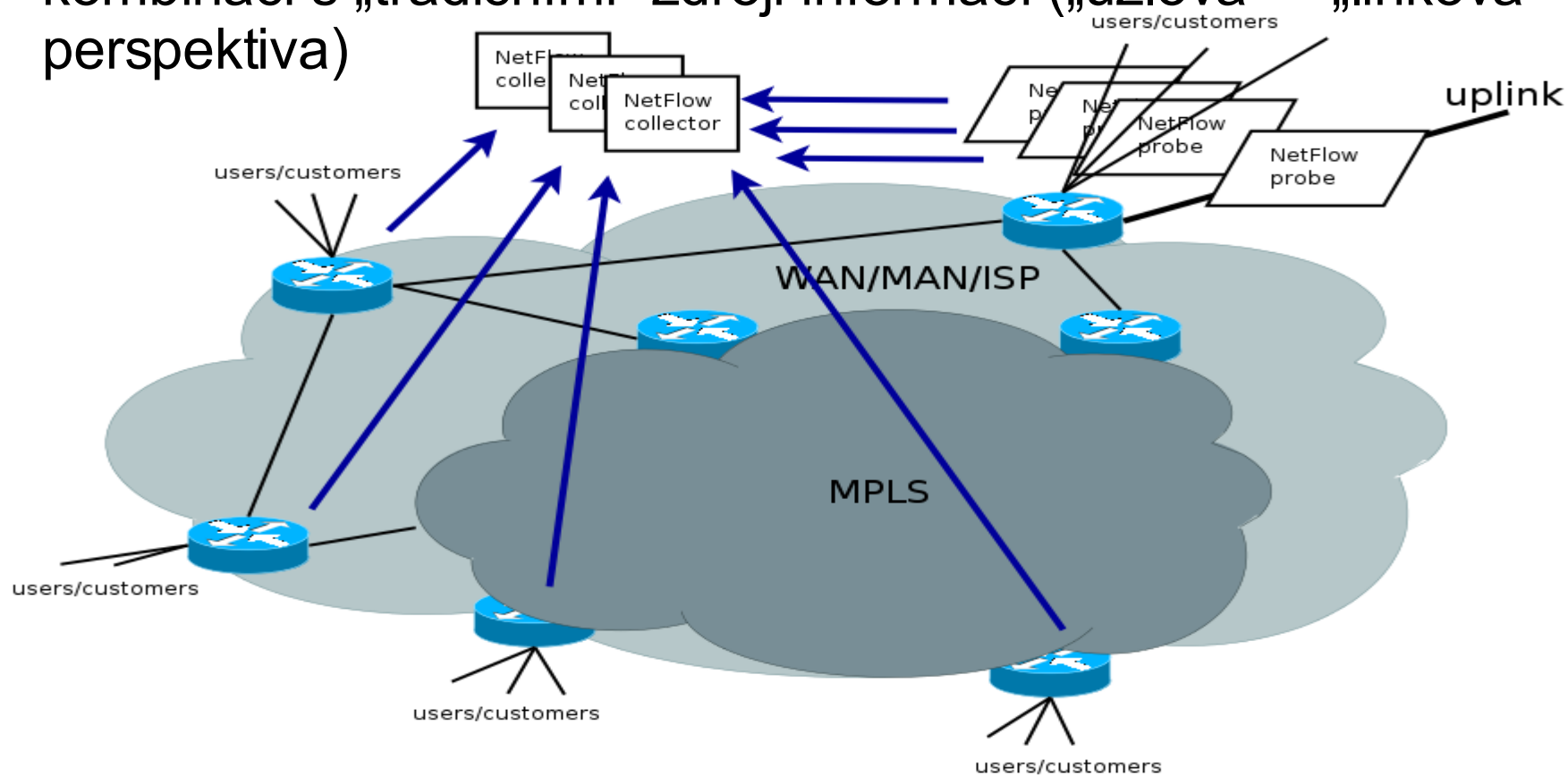
- jaké informace ve vztahu k bezpečnosti je možné získat ?
 - **v závažných případech** je možno nakonfigurovat cílený filtr včetně následného zpracování a specifickou dobou expirace záznamů/výsledků
 - => výsledky až z budoucích nasbíraných dat**
 - *bezpečnost: systematické ověřování indicií*

Systematické, plošné sledování provozu v síti CESNET2

- omezení přístupu k systému
 - velmi úzká skupina – správci páteřní sítě + CSIRT
 - značné nároky na zdroje
 - třída kolektoru ~ 2x Xeon@3+GHz, 2-8GB RAM, HW Raid SCSI/SAS 0,2-0.5TB
 - interaktivní charakter práce
 - step-by-step dohledávání (zpravidla třeba více pokusů/strategií k výsledku), dlouhá vybavovací doba komplexních dotazů (až hodiny)
 - kumulace požadavků v čase
 - když něco ... - tak vše najednou ...

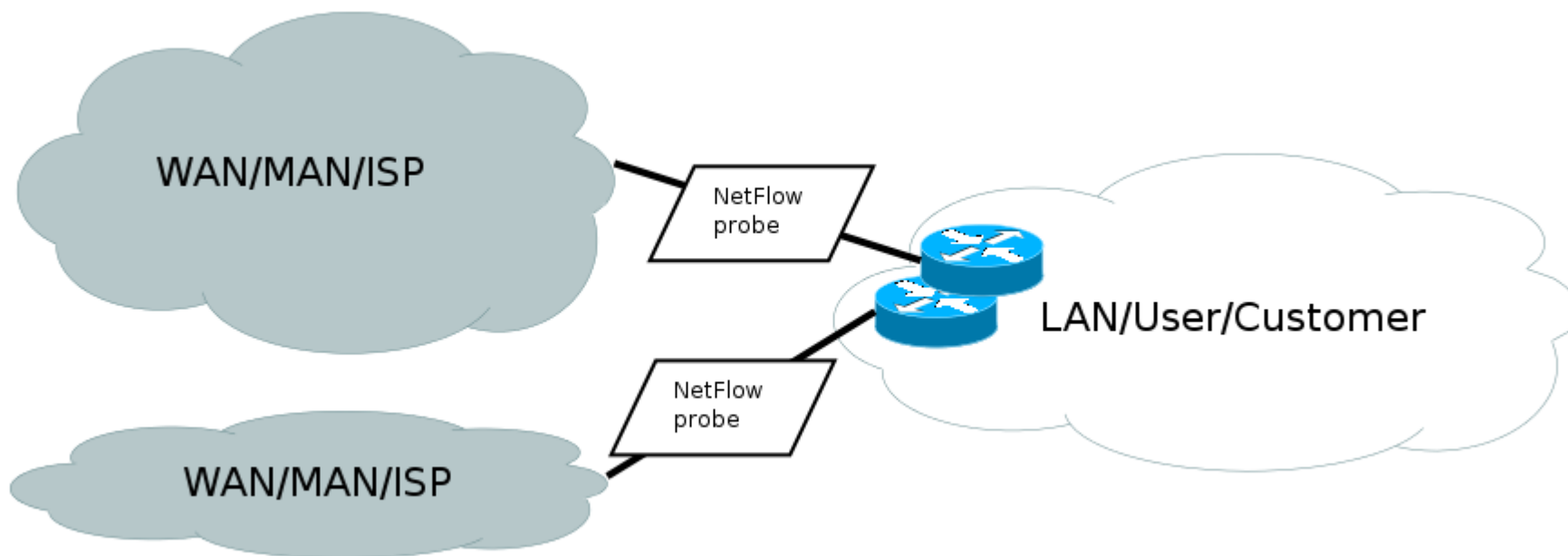
Příklady architektur pro sledování provozu sítě na základě informací o tocích dat

- rozsáhlé sítě - efektivní využití sond (např. FlowMon) v kombinaci s „tradičními“ zdroji informací („uzlová“ + „linková“ perspektiva)



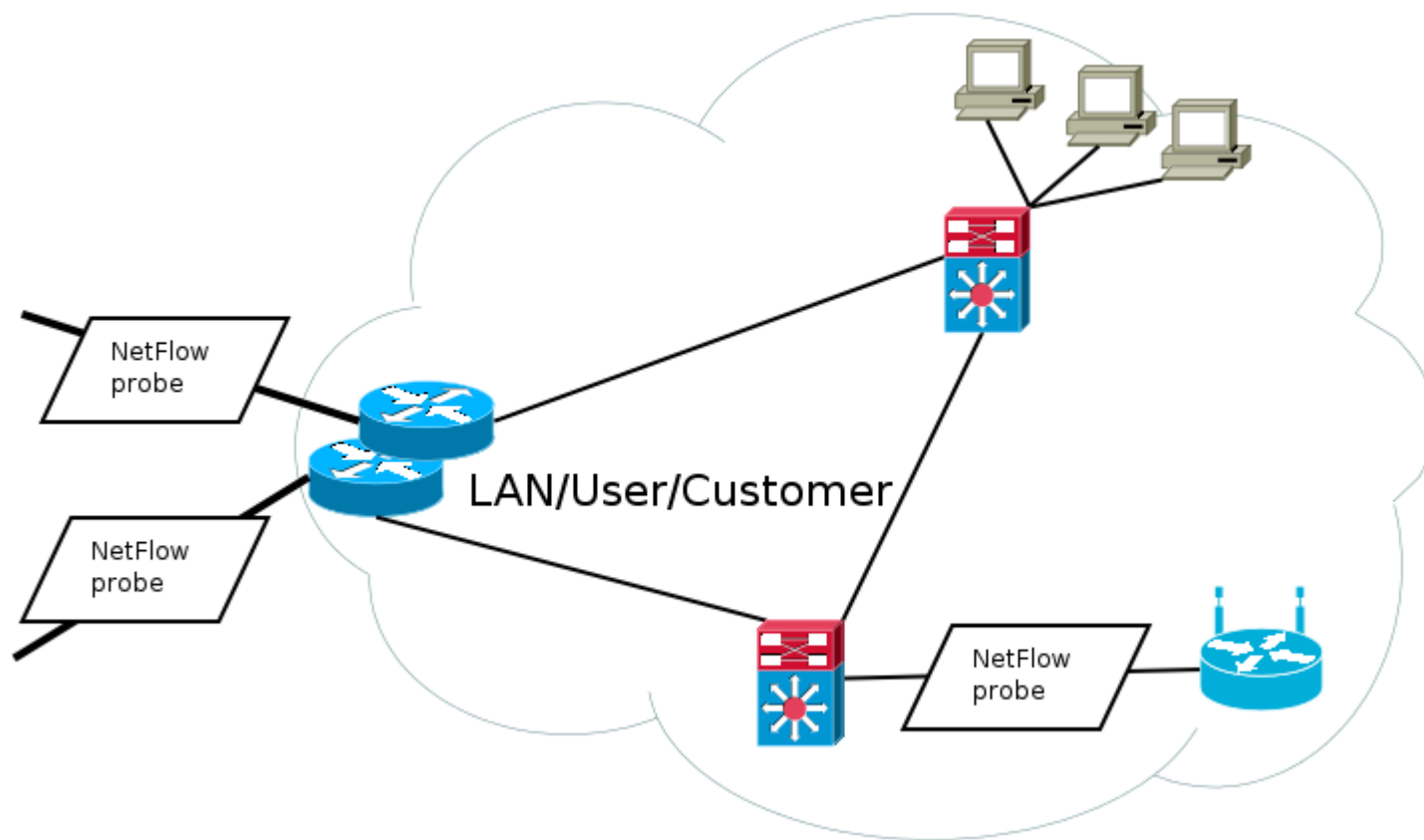
Příklady architektur pro sledování provozu sítě na základě informací o tocích dat

- „uplink“ - velmi vhodné místo, efektivní implementace sond (např. FlowMon) - „linková“ perspektiva



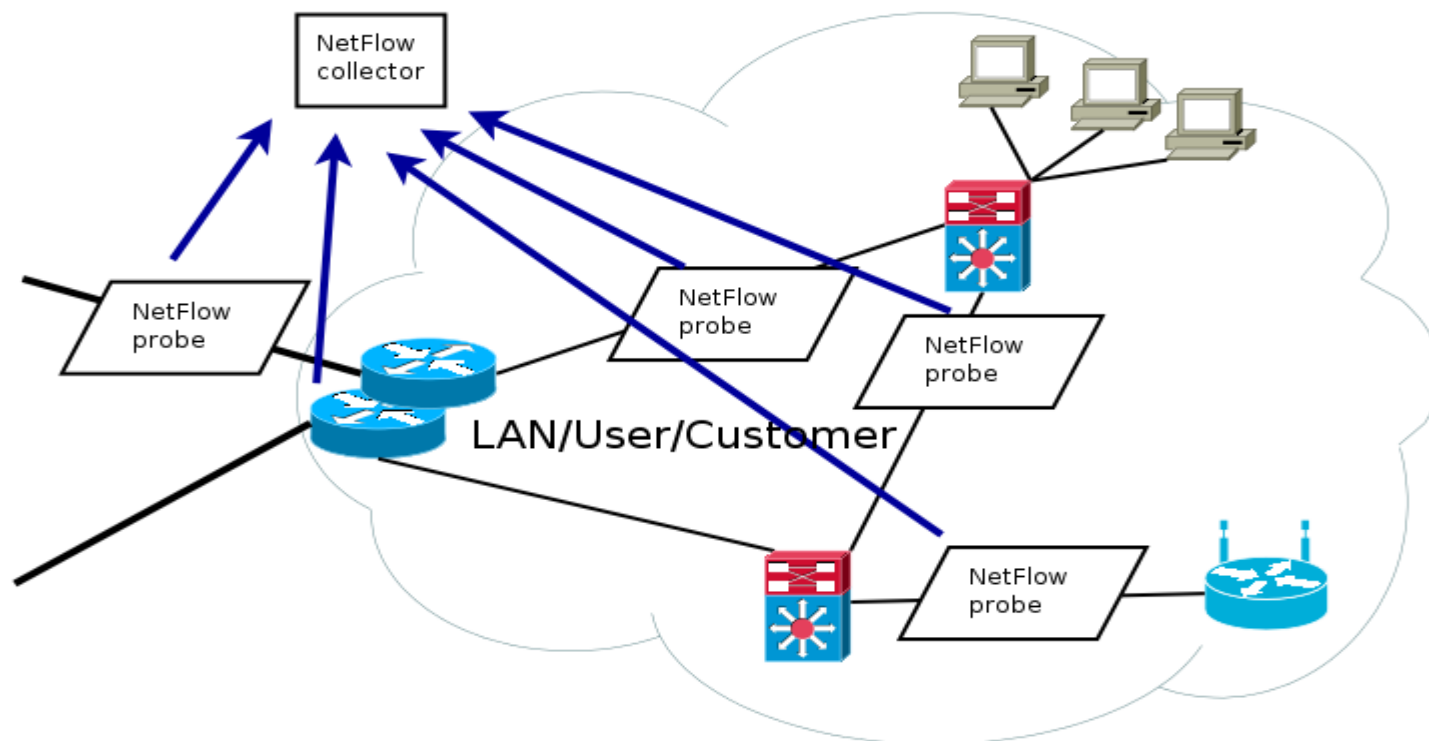
Příklady architektur pro sledování provozu sítě na základě informací o tocích dat

- „uplink“ + „citlivá“ část koncové sítě



Příklady architektur pro sledování provozu sítě na základě informací o tocích dat

- koncové sítě - „linková“ perspektiva, sondy fungují i v L2 infrastruktuře, „tradiční“ zdroje informací nemusí být k dispozici



Uchovávání provozních a lokalizačních údajů

- zák. 127 §97:Právnícká nebo fyzická osoba, zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat provozní a lokalizační údaje a tyto údaje je na požádání povinna poskytnout orgánům oprávněným... Rozsah provozních a lokalizačních údajů, dobu jejich uchovávání, která nesmí být delší než 12 měsíců a formu a způsob jejich předávání ...stanoví prováděcí právní předpis
 - vyhláška 485 (MČR ve spolupráci s MVČR)

Uchovávání provozních a lokalizačních údajů

- zák. 127 §90:
 - Provozními údaji se rozumí jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování
 - uchovávání provozních údajů mimo rámec §97
 - pro vyúčtování ceny a řešení zneužívání
 - marketing nebo služby s přidanou hodnotou – se souhlasem uživatele
 - po nezbytně nutné době smazat

Uchovávání provozních a lokalizačních údajů

- vyhláška 485 (MIČR ve spolupráci s MVČR)
 - týká se: „právnícká nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací“
 - síť CESNET2 je neveřejná
 - doporučení: postupovat přiměřeně k vyhlášce
 - v případě změny předpisů - minimum problémů
 - typy a rozsah uchovávaných vstupních dat (logy) nezbytných pro vypracování provozních údajů a doba jejich uchování zpravidla korespondují s „best-practice“ správců sítí a služeb

Uchovávání provozních a lokalizačních údajů

- **typové skupiny služeb** z hlediska vyhlášky 485 (sítě s přepojováním paketů)
 - služby přístupu k síti
 - především vazba mezi identifikátory uživatele a zařízení v časovém intervalu ~ uživatele od..do u stroje s IP adr.
 - snaha postihnout zejména scénář: inicializace připojení, AA, připojení, přidělení IP adresy, užívání připojení (pošta,.....), odpojení
 - náš případ - spíše prostředí sítí „s pevnou konfigurací“ a „souvislou konektivitou zařízení“ (s výjimkou např. WiFi)
 - jiný úhel pohledu koncových a tranzitních sítí (teoreticky i Flow-based informace)

Uchovávání provozních a lokalizačních údajů

- **typové skupiny služeb** z hlediska vyhlášky 485 (sítě s přepojováním paketů)
 - služby přístupu ke schránkám el. pošty
 - ~ uživatel X z IP adresy Y zpráva ID Z, adresy příjemců a odesílatele, použité protokoly, použití zabezpečení apod. - v závislosti na architektuře služby
 - služby přenosu zpráv el. pošty
 - analogické předchozímu
 - serverové služby
 - identifikátory klientské a serverové strany, URI
 - další služby (chat, usenet, IP telef., ...) - analogicky

Uchovávání provozních a lokalizačních údajů

- **předmětné údaje**

- zpravidla relevantní identifikátory v závislosti na službě ~ provozní informace jsou zjednodušeně výsledkem specificky zpracovaného obsahu logů a jejich kombinací
- rozsah dostupných údajů může záviset na architektuře služby v daném prostředí – množiny dostupných údajů nemusí být vždy identické – princip „*best effort*“

...přímý přístup ke službě vs. vynucené proxy apod.

- doba uchování dle vyhlášky: 6 měsíců s výjimkou URI a souvisejících parametrů (3 měsíce) – vnímám jako minimální dobu

děkuji za pozornost...