

Sledování provozu sítě

...vzhledem k řešení bezpečnostních incidentů...

Tomáš Košňar
CESNET z.s.p.o.

kosnar@cesnet.cz

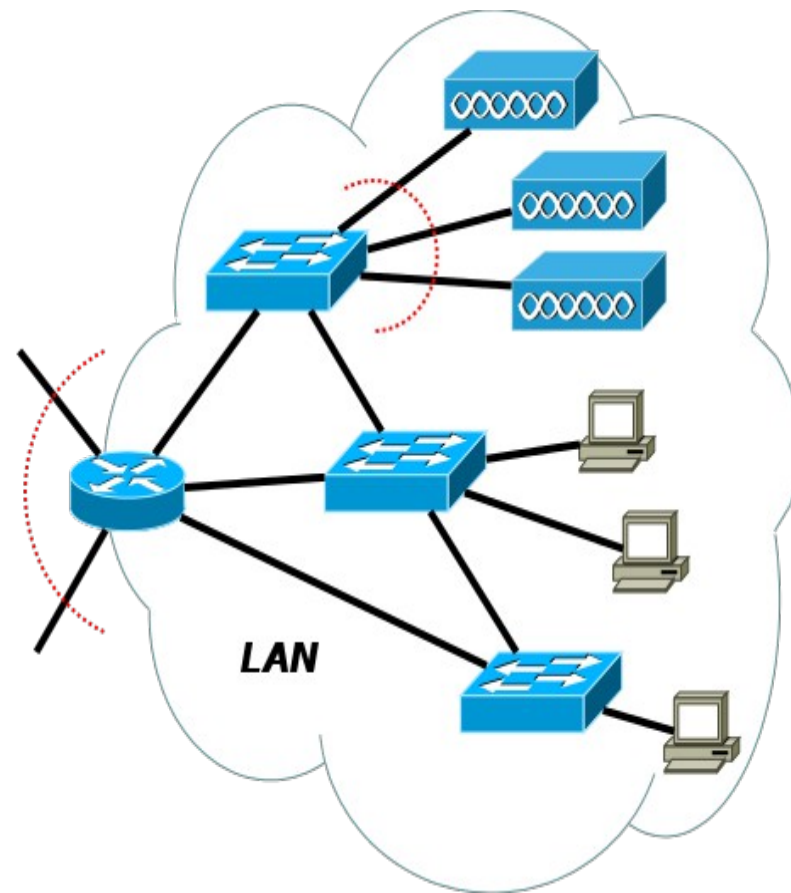
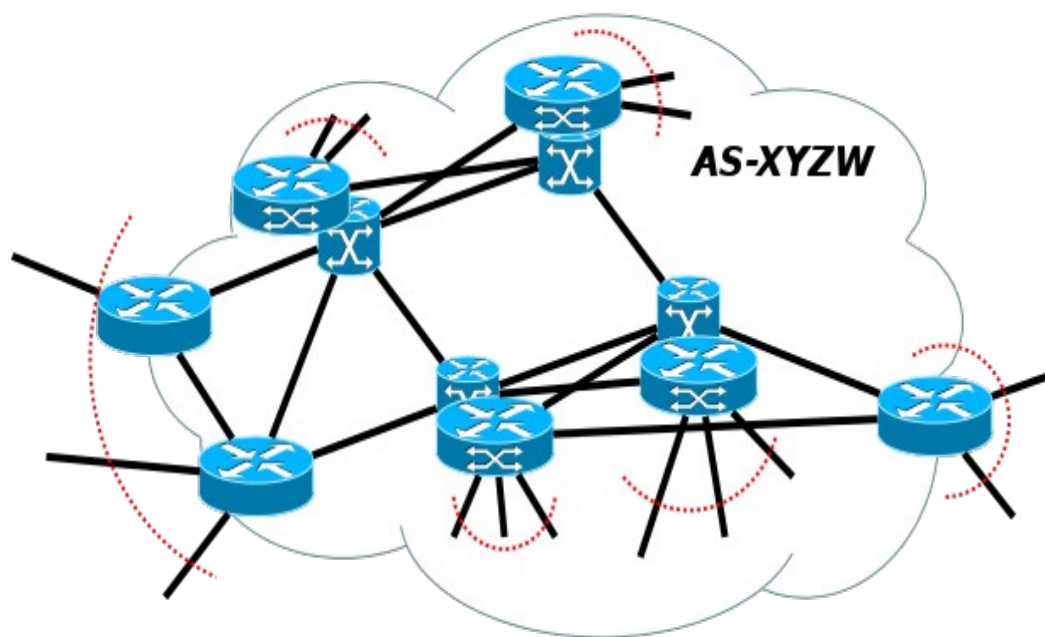
- Základní principy sledování provozu sítí
- Mechanismy a možnosti sledování provozu sítí
- Co je dobré sledovat, uchovávat
- K čemu je možné takto získané informace využít

- **Proč to vůbec děláme – důvody !!!**

- ...manažerské, profesní uspokojení
- ...
- ...aby mě šéfové „neprudili“...
- ...chci vědět, co dělá kolega ;-)
- ...
- ...
- ...potřebuji zajistit optimální využití sítě a jejích zdrojů
- ...
- ...
- ...potřebuji jistě a spolehlivě řídit chod sítě, mít schopnost efektivně řešit anomální situace a dokonce je být schopen predikovat...

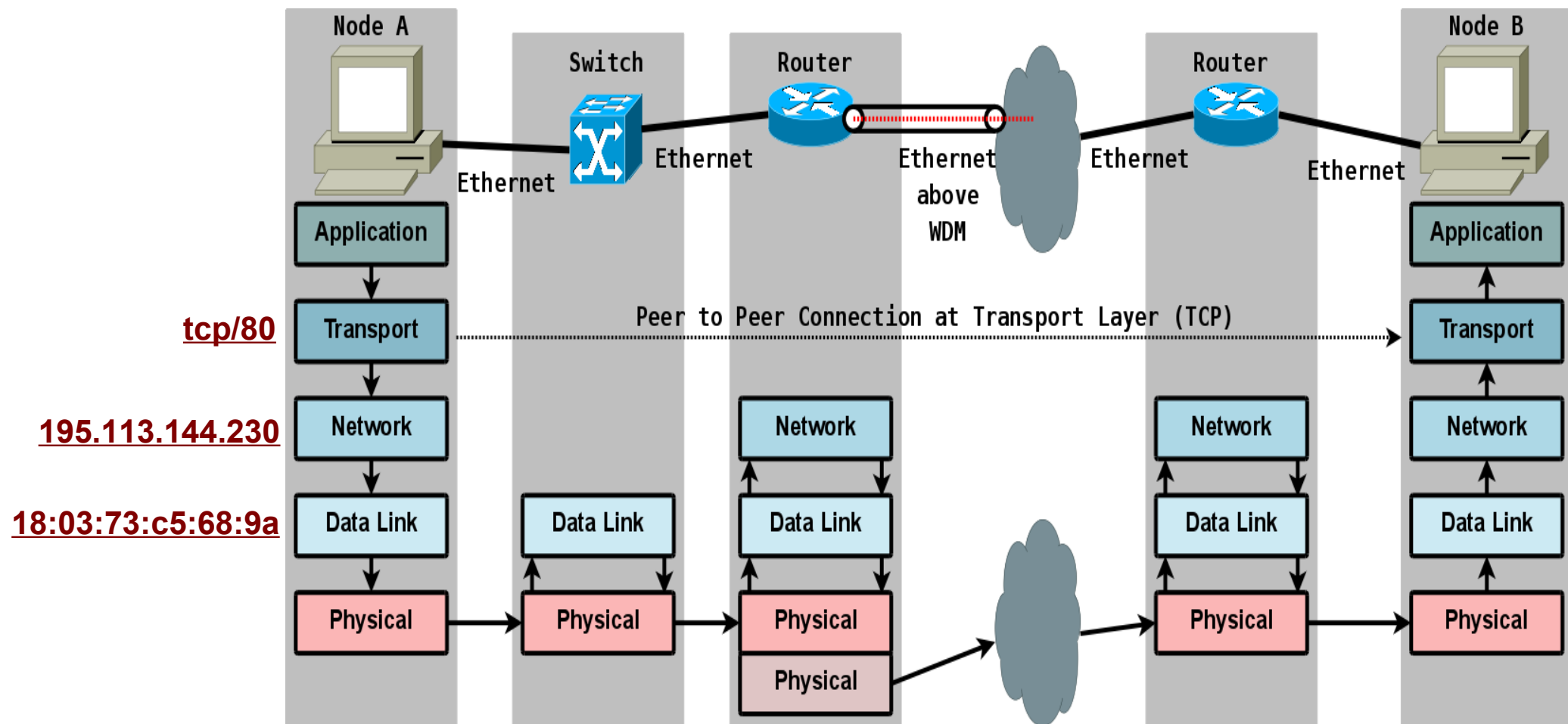
- Sledujeme-li - tedy pozorujeme → zaznamenat můžeme pouze to, co vidíme → „**místa**“ **pozorování**

– Architektura sítě a její topologie

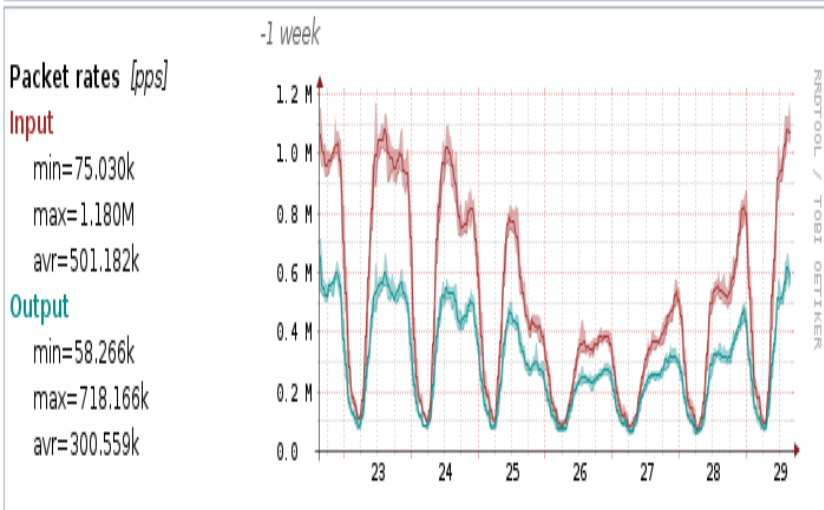
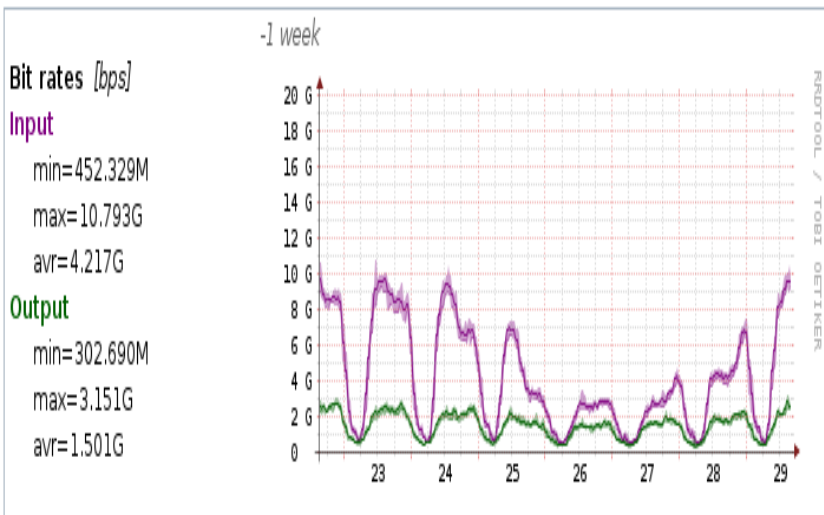


- Sledujeme-li - tedy pozorujeme → zaznamenat můžeme pouze to, co vidíme → „**místa**“ pozorování

- Hierarchie ~ vrstvy



- Detailnost pozorování → vypovídací informační hodnota → **využitelnost**



VS.

No.	Time	Source	Destination	Protocol	Length	Info
42	2.785591000	Cisco_03:bf:90	Spanning-tree-(for-bridg	STP	60	RST, Root = 32768/2/00:0d:ed:ac
43	3.004830000	2001:718:1:100:195:178:6	2001:718:1:101::3	DNS	93	Standard query 0xe14 A gc8.ce
44	3.005281000	2001:718:1:101::3	2001:718:1:100:195:178:6	DNS	309	Standard query response 0xe14
45	3.005553000	195.178.64.169	195.113.187.27	TCP	74	39898 > nrpe [SYN] Seq=0 Win=14
46	3.005878000	195.113.187.27	195.178.64.169	TCP	74	nrpe > 39898 [SYN, ACK] Seq=0 A
47	3.005914000	195.178.64.169	195.113.187.27	TCP	66	39898 > nrpe [ACK] Seq=1 Ack=1
48	3.006101000	195.178.64.169	195.113.187.27	TCP	194	39898 > nrpe [PSH, ACK] Seq=1 A
49	3.006421000	195.113.187.27	195.178.64.169	TCP	66	nrpe > 39898 [ACK] Seq=1 Ack=12
50	3.036732000	195.113.187.27	195.178.64.169	TCP	282	nrpe > 39898 [PSH, ACK] Seq=1 A
51	3.036798000	195.178.64.169	195.113.187.27	TCP	66	39898 > nrpe [ACK] Seq=129 Ack=
52	3.037801000	195.178.64.169	195.113.187.27	TCP	201	39898 > nrpe [PSH, ACK] Seq=129
53	3.038986000	195.113.187.27	195.178.64.169	TCP	301	nrpe > 39898 [PSH, ACK] Seq=217
54	3.039403000	195.178.64.169	195.113.187.27	TCP	143	39898 > nrpe [PSH, ACK] Seq=264

Frame 45: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Interface id: 0
WTAP_ENCAP: 1
Arrival Time: Oct 29, 2013 14:54:04.127993000 CET
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1383054844.127993000 seconds
[Time delta from previous captured frame: 0.000272000 seconds]
[Time delta from previous displayed frame: 0.000272000 seconds]
[Time since reference or first frame: 3.005553000 seconds]
Frame Number: 45
Frame Length: 74 bytes (592 bits)
Capture Length: 74 bytes (592 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ip:tcp]
[Coloring Rule Name: TCP SYN/FIN]
[Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]

Ethernet II, Src: Dell_c5:68:9c (18:03:73:c5:68:9c), Dst: Cisco_ac:91:40 (00:0d:ed:ac:91:40)

- Destination: Cisco_ac:91:40 (00:0d:ed:ac:91:40)
- Source: Dell_c5:68:9c (18:03:73:c5:68:9c)
- Type: IP (0x0800)

Internet Protocol Version 4, Src: 195.178.64.169 (195.178.64.169), Dst: 195.113.187.27 (195.113.187.27)

- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
- Total Length: 60
- Identification: 0xbf41 (48961)
- Flags: 0x02 (Don't Fragment)
- Fragment offset: 0
- Time to live: 64
- Protocol: TCP (6)
- Header checksum: 0xf891 [correct]
- Source: 195.178.64.169 (195.178.64.169)
- Destination: 195.113.187.27 (195.113.187.27)
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]

Transmission Control Protocol, Src Port: 39898 (39898), Dst Port: nrpe (5666), Seq: 0, Len: 0

- Source port: 39898 (39898)
- Destination port: nrpe (5666)
- [Stream index: 1]
- Sequence number: 0 (relative sequence number)
- Header length: 40 bytes
- Flags: 0x002 (SYN)

0000 00 0d ed ac 91 40 18 03 73 c5 68 9c 08 00 45 00@..s.h...E.
0010 00 3c bf 41 40 00 40 06 f8 91 c3 b2 40 a9 c3 71 ...<.A@.@...@.g
0020 bb 1b 9b da 16 22 18 a6 4e e2 00 00 00 00 a0 02N.....
0030 39 08 83 17 00 00 02 04 05 b4 04 02 08 0a 00 17 9.....
0040 f1 a3 00 00 00 00 01 03 03 07
● Transmission Control Protocol (tcp...) Packets: 59 Displayed: 59 Marked: 0 Dropped: 0 Profile: Default

- Detailnost pozorování → vypovídací informační hodnota → **využitelnost**
 - Časové aspekty ? ...nahodile, periodicky, souvisle...
- Smysluplnost
 - Obsahová (*~ statistický podíl výskytu ethernet rámců s lichým FCS je zajímavá úloha, ale pro praxi patrně nikoli nejpotřebnější*)
 - Ekonomická (poměr cena:výkon)
 - Ne sledování pro sledování, ale opět kvůli účelu !!!

- Téma uchopeno spekulativně účelově
 - Pravděpodobně většina zde reprezentovaných sítí → **IP nad Ethernet infrastrukturou** (fyzickou, logickou)

; -)

- Spekulativně se zaměřím na rutinní systematický monitoring provozu (nikoli detekční systémy ala IDS apod.)

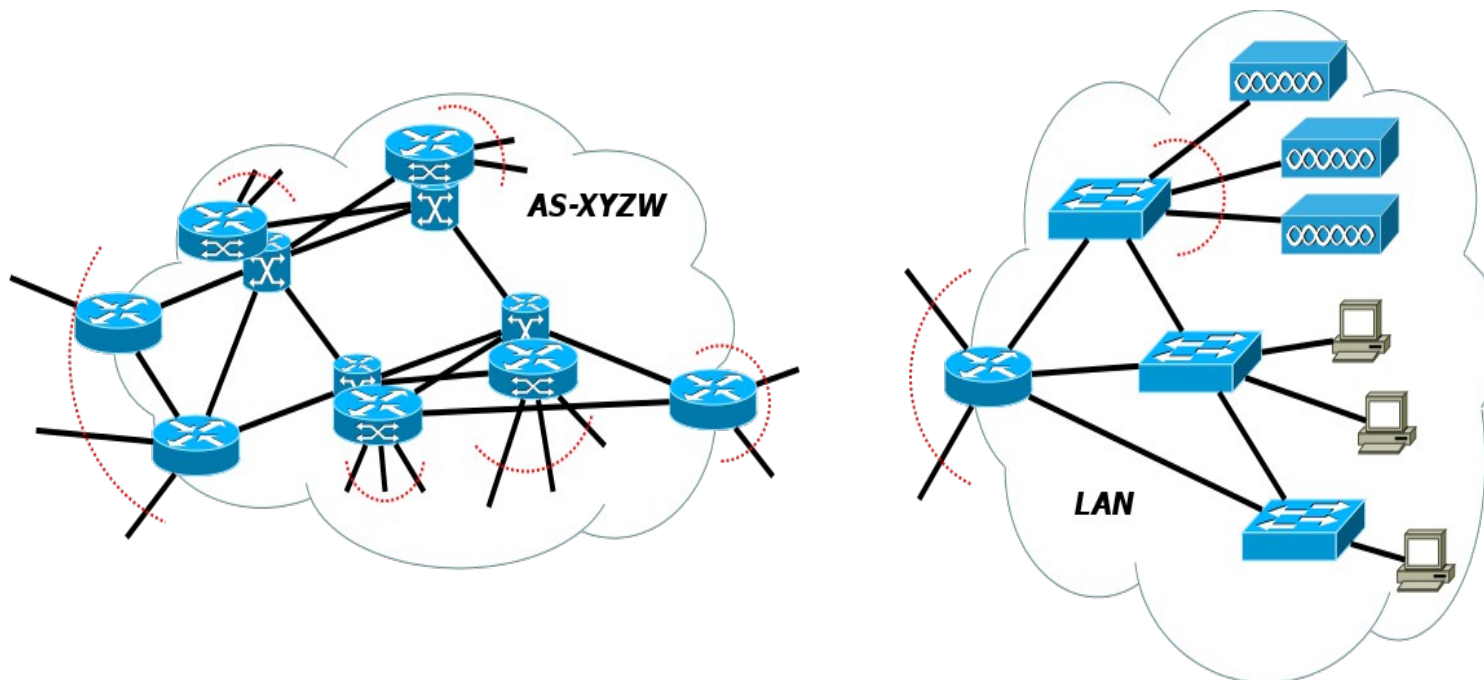
- **Pro běžnou praxi**

- **I.** Permanentní přehled o IP komunikaci alespoň na hraně/perimetru sítě
- **II.** Schopnost nalézt MAC adresu k dané IP adrese (i v real-time)
- **III.** Schopnost dohledat uživatele, který seděl na dané MAC adrese

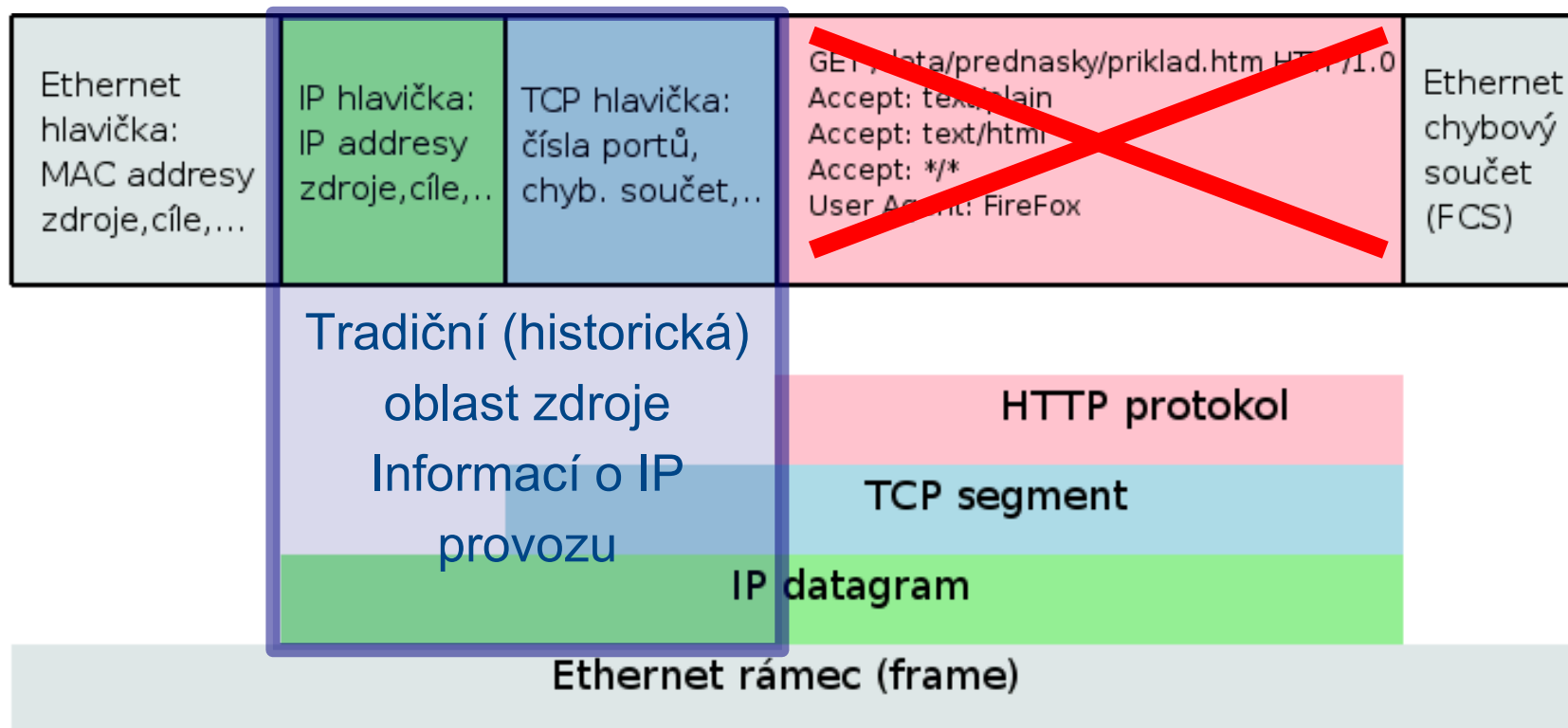
- I. pro běžnou praxi
 - **Permanentní přehled o IP komunikaci alespoň na hraně/perimetru sítě**

...co nám do/z/v sítě teče ???
 - K úvaze při řešení...
 - Operují koncovou vs. tranzitní sít' ?
 - Mohu aplikovat „reverse path checks“ ?
 - Je sít' nebo její část „galvanicky“ oddělena (FW, DMZ, NAT) ?
 - ...provozují data-centrum (perimetr dílčích větví interní infrastruktury) ?
 - ...

- I. pro běžnou praxi
 - **Permanentní přehled o IP komunikaci alespoň na hraně/perimetru sítě**
 - Mechanismy sledování
 - Informace o IP provozu na bázi toků (*~flow-based~*) – rozumný kompromis



- I. pro běžnou praxi - **permanentní přehled o IP komunikaci alespoň na hraně/perimetru sítě**
- Informace o IP provozu na bázi toků (*~flow-based~*)
 - Informace vybrané z hlaviček paketů transportních protokolů (TCP/IP)



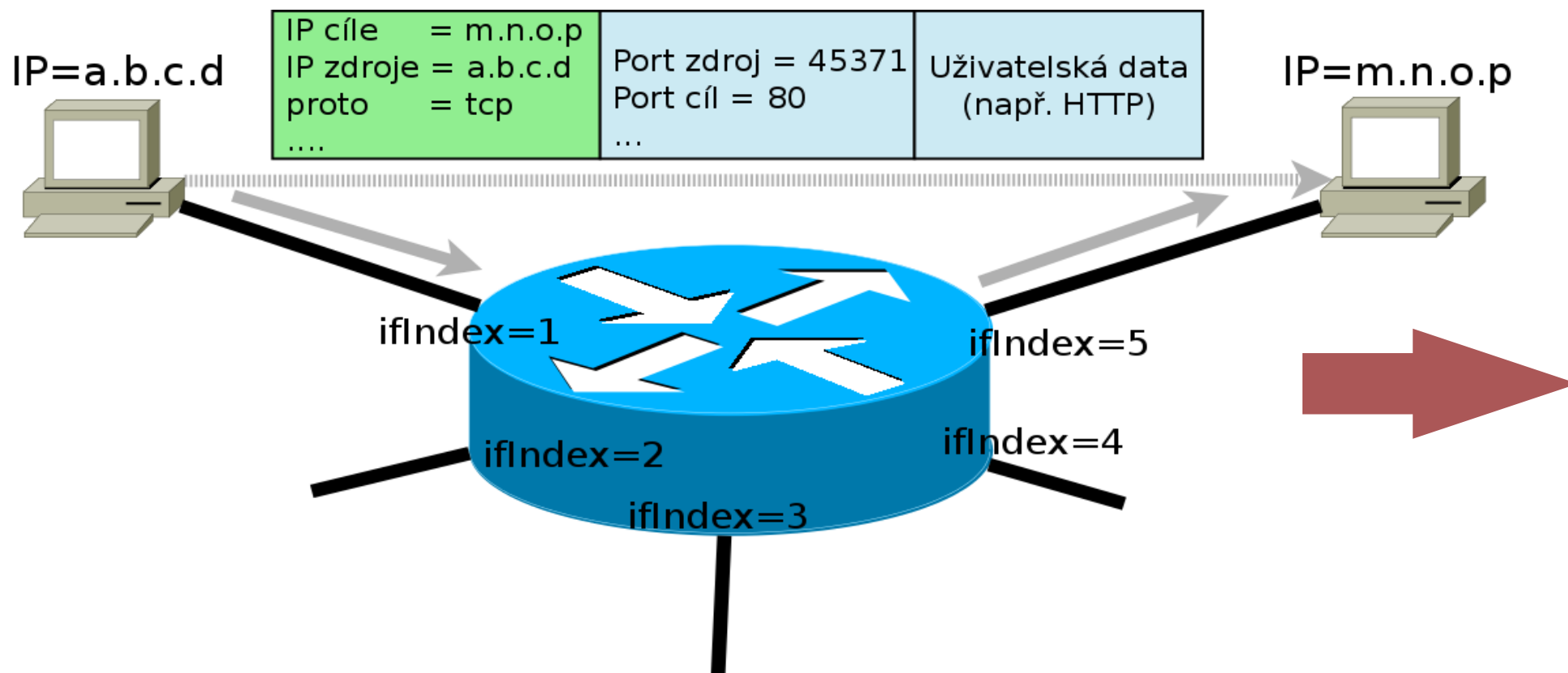
- I. pro běžnou praxi - **permanentní přehled o IP komunikaci alespoň na hraně/perimetru sítě**
- Informace o IP provozu na bázi toků (*~flow-based~*)
 - Zachování soukromí koncových uživatelů
 - Dostatečná vypovídací hodnota informací o IP provozu
 - „Přijatelné“ množství dat ke zpracování
 - Možnost plošného zpracování v rozsáhlých sítích

- I. pro běžnou praxi - **permanentní přehled o IP komunikaci alespoň na hraně/perimetru sítě**
- Informace o IP provozu na bázi toků (*~flow-based~*)
 - ..z hlavičky přenášeného datového bloku
 - => informace o jednosměrném přenosu**
 - Informace v místě vzniku **dočasně držena v paměti ~ provozní záznam**
 - Záznam průběžně modifikován informacemi (objem, čas, TCP flags, DSCP bity,..) z každého IP datagramu, který přísluší danému toku (stejně klíčové informace – IP adresy, protokol, čísla portů, rozhraní)
 - => agregovaná informace o provozu**

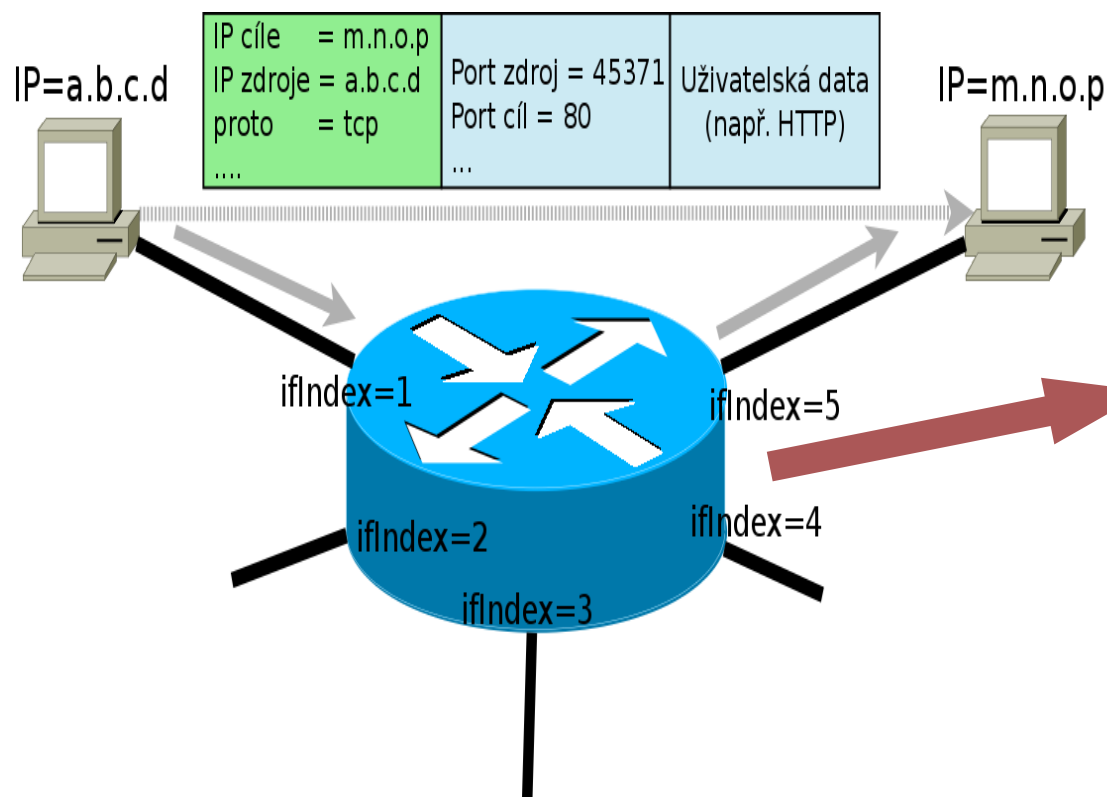
- I. pro běžnou praxi - **permanentní přehled o IP komunikaci alespoň na hraně/perimetru sítě**
- Informace o IP provozu na bázi toků (*~flow-based~*)
 - **Po expiraci** (přirozená [*konfigurace*] nebo vynucená)
 - **Záznam o provozu** zpravidla odeslán ke zpracování na tzv. **Kolektory** (UDP, několik exportních formátů)
 - Zdroje záznamů o provozu
 - **Směrovače** (v závislosti na výrobci)
 - **Sondy**
 - **HW sondy** (např. FlowMon, Endace)
 - **SW** (např. FlowMon, flow-tools,...)

- I. pro běžnou praxi - **permanentní přehled o IP komunikaci alespoň na hraně/perimetru sítě**
- Informace o IP provozu na bázi toků (*~flow-based~*)
 - **Typický informační obsah provozního záznamu (běžné implementace)**
 - IP adresy, čísla portů, protokol
 - Identifikátory rozhraní (ifIndex), kterým tok vstoupil (vystoupil) z/do zařízení – u sond informace o směru přenosu na lince, u směrovačů informace o vstupním a výstupním rozhraní (informace i o zahození paketu)
 - IP nexthop – následující IP uzel pro přenos
 - Čísla AS (je-li k dispozici BGP), sousední nebo cílové
 - Atributy – TCP vlaječky, DSCP bity (logické OR přes všechny pakety vytvářející záznam)
 - Objemové informace – rozsah toku v čase, objem, počet paketů

- I. pro běžnou praxi - **permanentní přehled o IP komunikaci alespoň na hraně/perimetru sítě**
- Informace o IP provozu na bázi toků (*~flow-based~*)



- I. pro běžnou praxi - **permanentní přehled o IP komunikaci alespoň na hraně/perimetru sítě**
- Informace o IP provozu na bázi toků (*~flow-based~*)
- V závislosti na implementaci a typu zdroje dostupnost informací o „fyzické“ trase přenosu



SrcIP	=	a . b . c . d
DstIP	=	m . n . o . p
Proto	=	tcp
SrcPort	=	45371
DstPort	=	80
SrcIf	=	1
DstIf	=	5
...		
Octets	=	12252
Pkts	=	12

- I. pro běžnou praxi - permanentní přehled o IP komunikaci alespoň na hraně/perimetru sítě
- Informace o IP provozu na bázi toků (~flow-based~)
 - Typický informační obsah provozního záznamu (běžné implementace) – částečná anonymizace

Results (time values in CET)

#	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Src-ifindex	Dst-ifindex	Src/Prev-AS	Dst/Next-AS	TOS-flags	TCP-flags	Nexthop	Flow-Start [CET]	Flow-End [CET]	Bytes-measured	Pkts-measured
1.	2a02:598:1:0:0:x:x:x	2001:718:2:b2:1d08:x:x:x	tcp (6)	http (80)	63236	58	25			00000000	push(8), ack(16)	0:0:0:0:ffff:c371:9c06	13/10/30 10:13:02.238	13/10/30 10:13:02.610	95.000 KB	76.000 p
2.	77.75.76.x	146.102.149.x	tcp (6)	http (80)	55732	58	25	AS43037	AS65001	00000000	push(8), ack(16)	195.113.156.8	13/10/30 10:19:32.645	13/10/30 10:19:35.891	77.500 KB	62.000 p
3.	2a02:598:1:0:0:x:x:x	2001:718:1e03:5176:d55f:x:x:x	tcp (6)	http (80)	52827	58	25			00000000	push(8), ack(16)	0:0:0:0:ffff:c371:9c08	13/10/30 10:14:08.713	13/10/30 10:14:09.079	62.500 KB	50.000 p
4.	77.75.76.x	147.229.174.x	tcp (6)	http (80)	60838	58	25	AS43037	AS197451	00000000	push(8), ack(16)	195.113.156.26	13/10/30 10:15:16.408	13/10/30 10:15:22.923	61.250 KB	49.000 p
5.	77.75.76.x	146.102.117.x	tcp (6)	http (80)	59547	58	25	AS43037	AS65001	00000000	push(8), ack(16)	195.113.156.8	13/10/30 10:20:30.269	13/10/30 10:20:31.044	61.250 KB	49.000 p
6.	2a02:598:1:0:0:x:x:x	2001:718:2:2905:6236:x:x:x	tcp (6)	http (80)	42986	58	25			00000000	ack(16)	0:0:0:0:ffff:c371:9c06	13/10/30 10:22:01.927	13/10/30 10:22:06.421	53.750 KB	43.000 p
7.	2a02:598:1:0:0:x:x:x	2001:718:2:31:4c58:x:x:x	tcp (6)	http (80)	49377	58	25			00000000	push(8), ack(16)	0:0:0:0:ffff:c371:9c06	13/10/30 10:20:58.109	13/10/30 10:21:01.927	52.500 KB	42.000 p
8.	77.75.76.x	193.84.36.x	tcp (6)	http (80)	30220	58	25	AS43037	AS65004	00000000	push(8), ack(16)	195.113.156.3	13/10/30 10:18:34.186	13/10/30 10:18:39.354	52.500 KB	42.000 p
9.	2a02:598:1:0:0:x:x:x	2001:718:1e02:8144:0:x:x:x	tcp (6)	http (80)	55743	58	25			00000000	push(8), ack(16)	0:0:0:0:ffff:c371:9c08	13/10/30 10:19:34.436	13/10/30 10:19:35.015	51.250 KB	41.000 p
10.	2a02:598:1:0:0:x:x:x	2001:718:1e02:9100:f112:x:x:x	tcp (6)	http (80)	50259	58	25			00000000	push(8), ack(16)	0:0:0:0:ffff:c371:9c08	13/10/30 10:18:52.044	13/10/30 10:18:52.248	50.000 KB	40.000 p
11.	2a02:598:1:0:0:x:x:x	2001:718:1800:1804:0:x:x:x	tcp (6)	http (80)	42560	58	25			00000000	ack(16)	0:0:0:0:ffff:c371:9c0d	13/10/30 10:19:11.640	13/10/30 10:19:13.400	41.250 KB	33.000 p
12.	77.75.76.x	147.229.172.x	tcp (6)	http (80)	59198	58	25	AS43037	AS197451	00000000	push(8), ack(16)	195.113.156.26	13/10/30 10:15:15.651	13/10/30 10:15:16.355	38.750 KB	31.000 p
13.	2a02:598:1:0:0:x:x:x	2001:718:1e02:8144:0:x:x:x	tcp (6)	http (80)	62354	58	25			00000000	push(8), ack(16)	0:0:0:0:ffff:c371:9c08	13/10/30 10:14:08.752	13/10/30 10:14:09.151	37.500 KB	30.000 p
14.	2a02:598:1:0:0:x:x:x	2001:718:1c01:164:8171:x:x:x	tcp (6)	http (80)	49491	58	25			00000000	push(8), ack(16)	0:0:0:0:ffff:c371:9c07	13/10/30 10:17:18.583	13/10/30 10:17:18.685	36.292 KB	30.000 p
15.	2a02:598:1:0:0:x:x:x	2001:718:1e03:deee:0:x:x:x	tcp (6)	http (80)	53279	58	25			00000000	push(8), ack(16)	0:0:0:0:ffff:c371:9c08	13/10/30 10:18:25.694	13/10/30 10:18:26.297	34.759 KB	28.000 p
16.	77.75.76.x	147.229.174.x	tcp (6)	http (80)	42643	58	25	AS43037	AS197451	00000000	push(8), ack(16)	195.113.156.26	13/10/30 10:14:29.369	13/10/30 10:14:32.633	33.580 KB	27.000 p
17.	2a02:598:1:0:0:x:x:x	2001:718:1e02:8144:0:x:x:x	tcp (6)	http (80)	49205	58	25			00000000	push(8), ack(16)	0:0:0:0:ffff:c371:9c08	13/10/30 10:15:00.550	13/10/30 10:15:06.204	32.500 KB	26.000 p
18.	77.75.76.x	147.228.209.x	tcp (6)	http (80)	50156	58	25	AS43037	AS65090	00000000	syn(2), push(8), ack(16)	195.113.156.13	13/10/30 10:20:36.840	13/10/30 10:20:37.974	32.249 KB	27.000 p
19.	2a02:598:1:0:0:x:x:x	2001:67c:1220:c1a3:d0f9:x:x:x	tcp (6)	http (80)	60303	58	25			00000000	push(8), ack(16)	0:0:0:0:ffff:c371:9c1a	13/10/30 10:13:51.227	13/10/30 10:13:51.299	31.250 KB	25.000 p
20.	77.75.76.x	147.229.174.x	tcp (6)	http (80)	56182	58	25	AS43037	AS197451	00000000	push(8), ack(16)	195.113.156.26	13/10/30 10:17:51.780	13/10/30 10:17:55.000	31.250 KB	25.000 p

- I. pro běžnou praxi - **permanentní přehled o IP komunikaci alespoň na hraně/perimetru sítě**
- Informace o IP provozu na bázi toků (*~flow-based~*)
 - Rozšířený informační obsah provozního záznamu (ukázka NetFlow security event logging - NSEL) – částečná anonymizace, možné řešení problematiky v případě NAT apod.

	NAT-Event	Src-IP	Dst-IP	Src-PostNAT-IP	Dst-PostNAT-IP	Protocol	Src-Port	Dst-Port	Src-PostNAPTPort	Dst-PostNAPTPort	Ingress-VRfid	Flow-Start [CET]
1.	delete	10.10.x.x	193.85.x.x	213.29.x.x	193.85.x.x	udp (17)	55384	domain (53)	19899	domain (53)	3	13/10/30 10:04:11.0
2.	delete	10.11.x.x	173.194.x.x	213.29.x.x	173.194.x.x	tcp (6)	36364	https (443)	36164	https (443)	3	13/10/30 10:04:11.1
3.	create	10.10.x.x	173.194.x.x	213.29.x.x	173.194.x.x	tcp (6)	41544	https (443)	36164	https (443)	3	13/10/30 10:04:11.1
4.	create	10.10.x.x	173.194.x.x	213.29.x.x	173.194.x.x	tcp (6)	60368	https (443)	36181	https (443)	3	13/10/30 10:04:11.1
5.	delete	10.10.x.x	134.170.x.x	213.29.x.x	134.170.x.x	tcp (6)	58708	https (443)	44033	https (443)	3	13/10/30 10:04:11.1
6.	delete	10.10.x.x	31.13.x.x	213.29.x.x	31.13.x.x	tcp (6)	37940	https (443)	42759	https (443)	3	13/10/30 10:04:11.1
7.	delete	10.11.x.x	74.217.x.x	213.29.x.x	74.217.x.x	tcp (6)	38460	https (443)	44730	https (443)	3	13/10/30 10:04:11.1
8.	create	10.10.x.x	77.93.x.x	213.29.x.x	77.93.x.x	tcp (6)	42778	https (443)	44718	https (443)	3	13/10/30 10:04:11.2
9.	delete	10.10.x.x	92.122.x.x	213.29.x.x	92.122.x.x	tcp (6)	53002	https (443)	44134	https (443)	3	13/10/30 10:04:11.2
10.	delete	10.11.x.x	173.194.x.x	213.29.x.x	173.194.x.x	tcp (6)	34759	http (80)	44590	http (80)	3	13/10/30 10:04:11.2
	NAT-Event	Src-IP	Dst-IP	Src-PostNAT-IP	Dst-PostNAT-IP	Protocol	Src-Port	Dst-Port	Src-PostNAPTPort	Dst-PostNAPTPort	Ingress-VRfid	Flow-Start

- II. pro běžnou praxi
 - **Schopnost nalézt MAC adresu k dané IP adrese**
...co nám tento IP provoz do sítě posílá ???
 - Koncová zařízení
 - Za určitých okolností i v „real-time“
 - K úvaze při řešení
 - Technická/logická architektura LAN
 - Řízení datových toků v LAN
 - ...

- II. pro běžnou praxi - **schopnost nalézt MAC adresu k dané IP adrese**
 - Mechanismy sledování
 - Log mechanismů přidělujících IP adresy v případě dynamické konfigurace
 - Neřeší dohledání v případě ad-hoc podvržené zdrojové IP

- II. pro běžnou praxi - **schopnost nalézt MAC adresu k dané IP adrese**
 - Mechanismy sledování
 - Systematický ARP „watch“ (pouze IPv4)
 - Sběr dat ze síťových prvků (SNMP; IPV6-MIB::ipv6NetToMediaPhysAddress,...)
 - *Dohledání v případě ad-hoc podvržené zdrojové IP ???*
 - Dump provozu
 - Vhodná architektura LAN infrastruktury pro mirror/rozdvojení provozu ?
 - Obtížné jako systematická činnost s uchováním dat, zpravidla nasazeno ad-hoc na základě potřeby – což dává smysl

- II. pro běžnou praxi - **schopnost nalézt MAC adresu k dané IP adrese**

- Mechanismy sledování

- Flow-based sledování v rozšířené implementaci (~flexible NetFlow, IPFIX)
- V principu řeší IPv6 i podvržené zdrojové IP adresy, ale závisí na úrovni implementace v daném zařízení

	FWD-Status	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Src-ifIndex	Dst-ifIndex	Ingress-VRFID	Src-MAC-Addr	Dst-MAC-Addr	TOS
1.	Terminate For us	134.94.115.x	195.113.250.x	icmp (1)	Echo Reply (0)	Echo Reply (0)	21	0	1	00:00:00:00:00:00	00:00:00:00:00:00	0000
2.	Terminate For us	10.31.2.x	10.31.2.x	icmp (1)	Echo Reply (0)	Echo Reply (0)	21	0	1	00:00:00:00:00:00	00:00:00:00:00:00	0000
3.	Terminate For us	188.1.144.x	195.113.250.x	icmp (1)	Echo Reply (0)	Echo Reply (0)	1	0	0	e0:2f:6d:2b:76:80	00:00:00:00:00:00	0000
4.	Terminate For us	195.113.250.x	195.113.250.x	icmp (1)	Echo Reply (0)	Echo Reply (0)	2	0	1	00:60:dd:44:b9:70	00:00:00:00:00:00	0000
5.	Terminate For us	195.113.250.x	195.113.250.x	icmp (1)	Echo Reply (0)	Echo Reply (0)	2	0	1	00:50:56:8d:0d:2d	00:00:00:00:00:00	0000
6.	Terminate For us	195.113.250.x	195.113.250.x	icmp (1)	Echo Reply (0)	Echo Reply (0)	2	0	1	00:60:dd:44:b8:ec	00:00:00:00:00:00	0000
7.	Terminate For us	195.113.250.x	195.113.250.x	icmp (1)	Echo Reply (0)	Echo Reply (0)	2	0	1	00:60:dd:44:b9:6d	00:00:00:00:00:00	0000
8.	Forwarded	134.94.115.x	195.113.250.x	icmp (1)	Echo Reply (0)	Echo (2048)	21	2	1	00:00:00:00:00:00	00:50:56:8d:0d:2d	0000
9.	Forwarded	195.113.250.x	134.94.115.x	icmp (1)	Echo Reply (0)	Echo Reply (0)	2	21	1	00:50:56:8d:0d:2d	00:00:00:00:00:00	0000

- III. pro běžnou praxi

- **Schopnost dohledat identitu uživatele, který „používal“ dané MAC/IP adresy**

..elektronická v lepším případě i fyzická identita uživatele, který byl „přítomen“ u zařízení, které generovalo/přijímalo daný provoz..

- K úvaze při řešení

- Technická/logická architektura autentizace, autorizace pro přístup k síti
- Síla ověření identity uživatele
- ...

- I. Sledování provozu v nadřazené síti: automatická detekce potenciálních provozních anomálií z/do sítí uživatelů, s uchováním „důkazního materiálu“ a statistickou nadstavbou

**...z důvodu ochrany soukromí uživatelů
nezveřejněno...**

II. Sledování provozu v nadřazené síti jako služba pro uživatele

**...z důvodu ochrany soukromí uživatelů
nezveřejněno...**

III. Interaktivní traffic browser provozu v nadřazené síti jako služba pro uživatele

**...z důvodu ochrany soukromí uživatelů
nezveřejněno...**

- **Etické otázky**

- Transparentně deklarovat způsob míru sledování provozu
- Hlídat limity zásahu do soukromí uživatelů
- Transparentní podmínky, za jakých je možné takové limity překročit ~ *standardní systém vs. zvlá*
- Výsledné informace propojovat z dílčích zdrojů až na základě odůvodněné potřeby (nikoli systematicky a automaticky), dílčí zdroje informací držet odděleně a s disjunktivními přístupovými právy (je-li možné; v zájmu vlastní ochrany administrátorů)

???