Technická analýza kyberútoků z března 2013

..útoky na některé zdroje českého Internetu od 4. do 7. března 2013..

Tomáš Košňar

CESNET z.s.p.o.

kosnar@cesnet.cz

Obsah

- Cíle časování, schémata, síla, důsledky, dopad zdroje
  - Technický rozbor variant útoků
  - Ukázky provozních záznamů útoků z perspektivy e-infrastruktury CESNET
- Možnosti eliminace útoků tohoto typu
  - Rámcové shrnutí identifikace a eliminace útoků tohoto typu na úrovni transportu a v koncové síti

Typ a cíle útoků

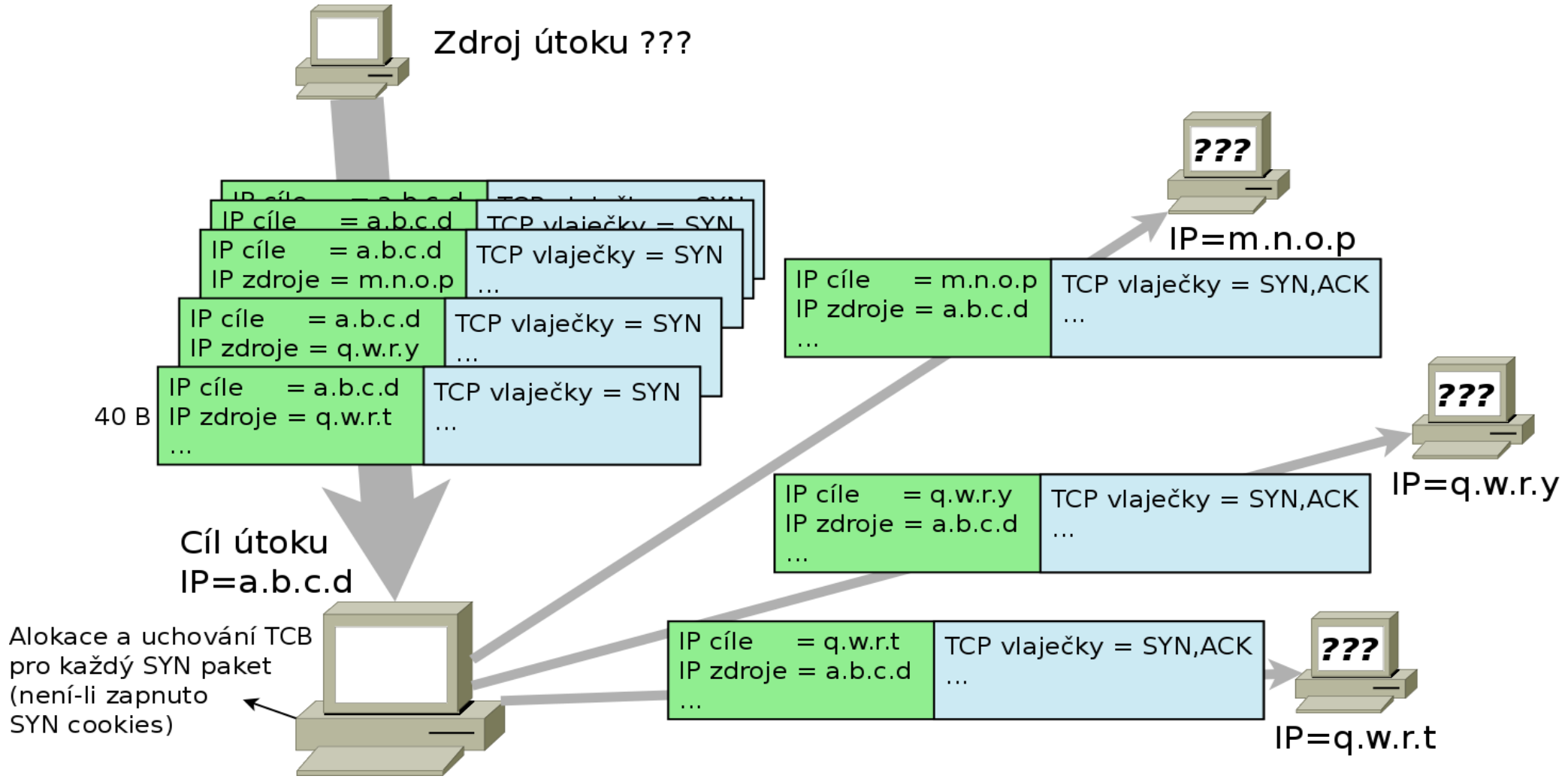
- Typ útoku
  - DoS (Denial of Service)
- Cíle útoků - uživatelsky viditelné, hojně navštěvované zdroje
  - **www** služby
  - Uživatelsky velmi viditelné → mediálně „atraktivní“
  - Posloupnost nejvýznamnějších cílů
    - Mediální servery
    - Seznam.cz
    - Banky
    - Mobilní operátoři

Schémata a časování útoků

- Časování útoků
  - Pondělí a úterý
    - TCP SYN FLOOD, podvržené zdrojové IP adresy
  - Středa a čtvrtek
    - BOUNCE TRAFFIC TCP SYN FLOOD, podvržené zdrojové IP adresy
  - Zpravidla dvě vlny „v pracovní době“ ;-)
    - 9-11
    - 14-16

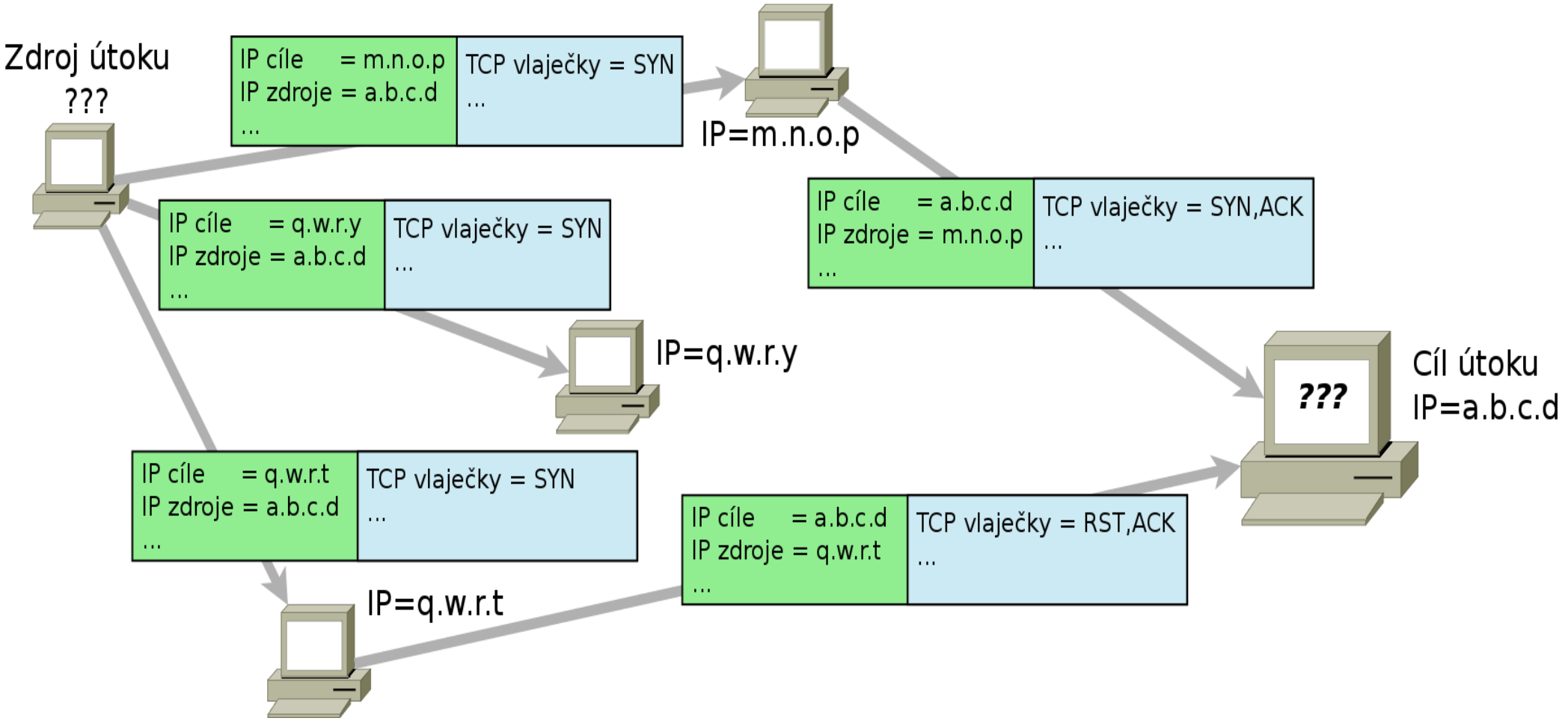
Schémata útoků

- a) přímý TCP SYN Flood s podvrženými zdrojovými IP adresami ~ velké množství „požadavků na otevření spojení“



Schémata útoků

- b) Bounce traffic (technika odražení) s podvrženou zdrojovou IP adresou (→ **adresa cíle útoku**) a odesláním na jiné místo, které odpoví podvržené zdrojové IP adrese, neobvyklé RWIN

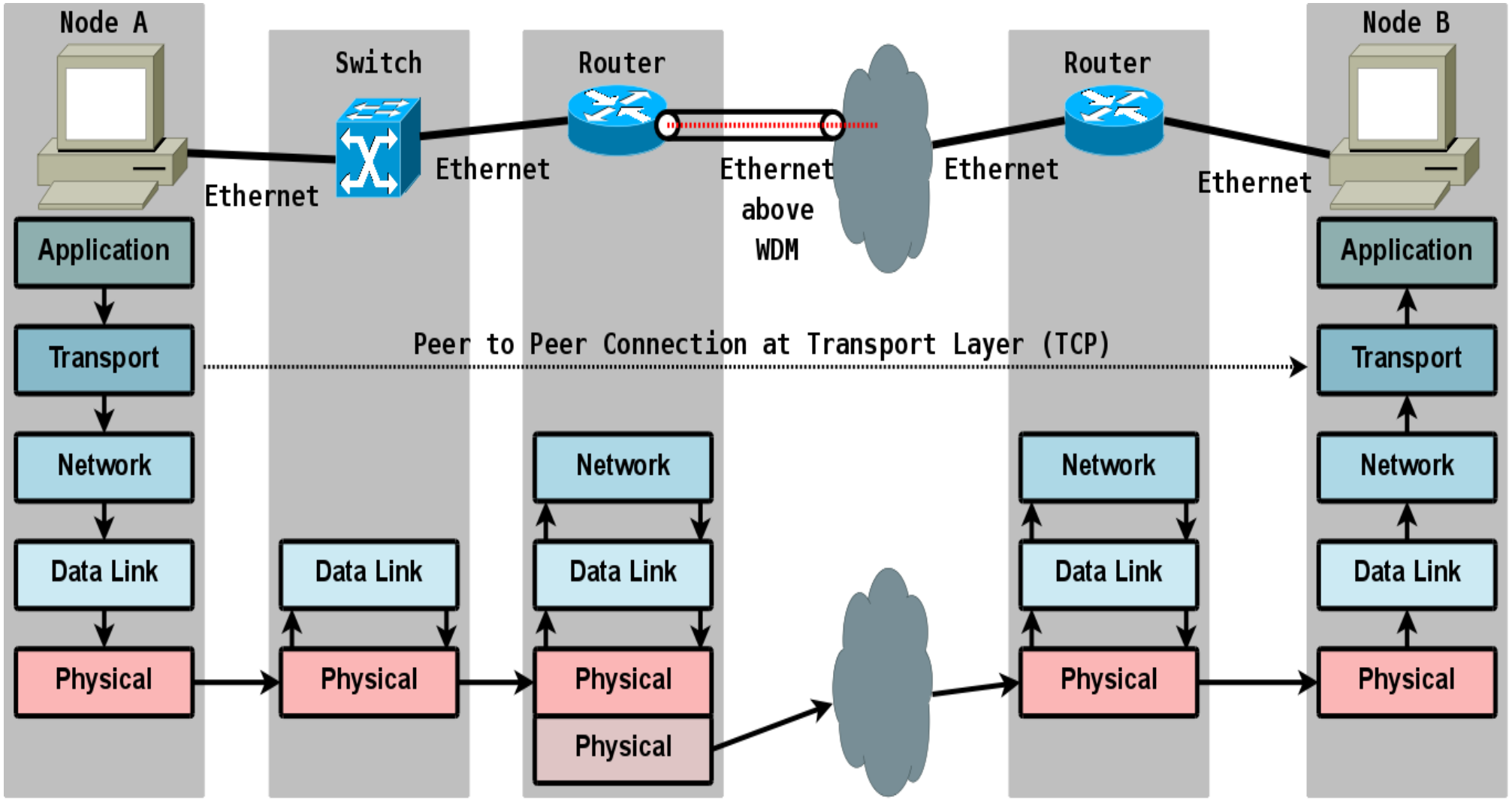


Síla a důsledky útoků

- Z pohledu síťového operátora
  - Objemově → TCP handshaking ~ 40Bpp
  - Paketově → 1-1.5 Mpps → „neohrožující“, ale detekovatelné
- Z pohledu poskytovatele obsahu, služby
  - Případ od případu, ale obecně významná
    - koncentrace provozu do jednoho místa
    - zatížení zdrojů o vrstvu výše ~ TCP

Síla a důsledky útoků

- Nároky na zdoje v kontextu síťového transportu a TCP negociace
  - k zamyšlení (*pozn.: TCP/IP model*)



Síla a důsledky útoků

- Z pohledu poskytovatele obsahu, služby
  - V některých případech impakt na předřazená zařízení (FW, balancery)
    - *Dává smysl budovat infrastrukturu schopnou odbavit řádově vyšší počet požadavků než je smysluplné vzhledem k účelu aplikace ?*
    - *Splnilo předřadné zařízení svoji úlohu, když nevydrželo nápor a „odpojilo“ cíl ?*
  - V závislost na architektuře koncové sítě, vedlejší efekty (s cílem útoku nesouvisející, ale postižené služby apod.)

Ukázky provozních záznamů reprezentujících útok s odražením

- Z pohledu e-infrastruktury CESNET (v roli odrazné sítě)
  - Agregace, příchozího provozu z IP rozsahu cíle útoku; mj. počet disjunktních čísel cílových portů a porovnání s „běžným“ provozem

Results *(time values in CEST)*

	Src-IP	Pkts-measured	Bytes-measured	Flow-Start [CEST]	Flow-End [CEST]	Protocol	Dst-Port-Cnt
1.	[redacted]40.198	1.951 mp	86.307 MB	13/03/06 14:29:37.483	13/03/06 14:44:59.995	tcp (6)	65531
2.	[redacted]40.70	1.950 mp	85.981 MB	13/03/06 14:29:33.045	13/03/06 14:44:59.999	tcp (6)	65531
3.	[redacted]40.71	5.737 kp	4.273 MB	13/03/06 14:29:17.765	13/03/06 14:40:24.455	tcp (6)	153
4.	[redacted]40.199	3.306 kp	2.489 MB	13/03/06 14:29:38.933	13/03/06 14:44:45.656	tcp (6)	116
5.	[redacted]40.161	1.954 kp	99.377 KB	13/03/06 14:43:54.880	13/03/06 14:43:55.456	tcp (6)	1
6.	[redacted]40.205	79.000 p	52.107 KB	13/03/06 14:39:37.735	13/03/06 14:43:27.276	tcp (6)	3
7.	[redacted]40.44	93.000 p	43.390 KB	13/03/06 14:31:46.493	13/03/06 14:32:11.837	tcp (6)	1
8.	[redacted]40.43	38.000 p	5.410 KB	13/03/06 14:34:50.631	13/03/06 14:40:24.404	tcp (6)	1
9.	[redacted]40.77	1.000 p	1.465 KB	13/03/06 14:30:45.956	13/03/06 14:30:45.956	tcp (6)	1
10.	[redacted]40.192	13.000 p	1.089 KB	13/03/06 14:31:25.605	13/03/06 14:44:57.223	udp (17)	13
11.	[redacted]40.65	7.000 p	1.038 KB	13/03/06 14:31:56.353	13/03/06 14:44:58.009	udp (17)	7
12.	[redacted]40.64	9.000 p	0.798 KB	13/03/06 14:30:32.778	13/03/06 14:40:37.237	udp (17)	9
13.	[redacted]40.193	4.000 p	0.512 KB	13/03/06 14:37:51.668	13/03/06 14:44:57.286	udp (17)	4
14.	[redacted]40.170	5.000 p	0.225 KB	13/03/06 14:31:24.331	13/03/06 14:31:28.811	tcp (6)	1

Ukázky provozních záznamů reprezentujících útok s odražením

- Z pohledu e-infrastruktury CESNET (v roli odrazné sítě)
  - Neagregovaný příchozí provoz, podle cílové IP adresy

	Src-IP	Dst-IP	Pkts-measured	Bytes-measured	Flow-Start [CEST]	Src-Port	Dst-Port	Protocol
1.	[redacted]40.70	[redacted].22.0	1.000 p	46.000 B	13/03/06 14:36:35.228	www (80)	47837	tcp (6)
2.	[redacted]40.70	[redacted].22.0	1.000 p	46.000 B	13/03/06 14:38:55.370	www (80)	47290	tcp (6)
3.	[redacted]40.198	[redacted].22.0	1.000 p	46.000 B	13/03/06 14:39:23.168	www (80)	28536	tcp (6)
4.	[redacted]40.198	[redacted].22.0	1.000 p	46.000 B	13/03/06 14:36:40.152	www (80)	3794	tcp (6)
5.	[redacted]40.198	[redacted].22.0	1.000 p	46.000 B	13/03/06 14:30:35.313	www (80)	3874	tcp (6)
6.	[redacted]40.198	[redacted].22.0	1.000 p	46.000 B	13/03/06 14:35:07.400	www (80)	35670	tcp (6)
7.	[redacted]40.198	[redacted].22.0	1.000 p	46.000 B	13/03/06 14:39:09.937	www (80)	22666	tcp (6)
8.	[redacted]40.198	[redacted].22.0	1.000 p	46.000 B	13/03/06 14:32:21.419	www (80)	8302	tcp (6)
9.	[redacted]40.198	[redacted].22.0	1.000 p	46.000 B	13/03/06 14:34:33.438	www (80)	31342	tcp (6)
10.	[redacted]40.198	[redacted].22.0	1.000 p	46.000 B	13/03/06 14:32:15.758	www (80)	52733	tcp (6)
11.	[redacted]40.70	[redacted].22.1	1.000 p	46.000 B	13/03/06 14:35:15.660	www (80)	12989	tcp (6)
12.	[redacted]40.70	[redacted].22.1	1.000 p	46.000 B	13/03/06 14:36:17.312	www (80)	699	tcp (6)
13.	[redacted]40.198	[redacted].22.1	1.000 p	46.000 B	13/03/06 14:30:26.879	www (80)	14087	tcp (6)
14.	[redacted]40.70	[redacted].22.1	1.000 p	46.000 B	13/03/06 14:30:26.040	www (80)	11257	tcp (6)
15.	[redacted]40.198	[redacted].22.1	1.000 p	46.000 B	13/03/06 14:32:17.353	www (80)	29593	tcp (6)
16.	[redacted]40.70	[redacted].22.1	1.000 p	46.000 B	13/03/06 14:30:33.279	www (80)	61987	tcp (6)
17.	[redacted]40.198	[redacted].22.1	1.000 p	46.000 B	13/03/06 14:34:03.519	www (80)	22245	tcp (6)
18.	[redacted]40.70	[redacted].22.1	1.000 p	46.000 B	13/03/06 14:35:02.907	www (80)	17879	tcp (6)
19.	[redacted]40.70	[redacted].22.1	1.000 p	46.000 B	13/03/06 14:37:20.721	www (80)	4984	tcp (6)
20.	[redacted]40.70	[redacted].22.1	1.000 p	46.000 B	13/03/06 14:33:53.181	www (80)	44741	tcp (6)
21.	[redacted]40.198	[redacted].22.1	1.000 p	46.000 B	13/03/06 14:33:16.128	www (80)	26372	tcp (6)

Ukázky provozních záznamů reprezentujících útok s odražením

- Z pohledu e-infrastruktury CESNET (v roli odrazné sítě)
  - Agregovaný příchozí provoz, počet pokusů vůči jednomu místu potenciálního odrazu

Results *(time values in **CEST**)*

	Src-IP	Dst-IP	Pkts-measured	Bytes-measured	Protocol	Avr-Pkt-Length	Src-Port-Cnt	Dst-Port-Cnt
1.	[redacted]0.198	[redacted]2.0	8.000 p	0.359 KB	tcp (6)	46	1	8
2.	[redacted]0.70	[redacted]2.0	2.000 p	92.000 B	tcp (6)	46	1	2
3.	[redacted]0.198	[redacted]2.1	7.000 p	0.314 KB	tcp (6)	46	1	7
4.	[redacted]0.70	[redacted]2.1	8.000 p	0.359 KB	tcp (6)	46	1	8
5.	[redacted]0.198	[redacted]2.2	7.000 p	0.314 KB	tcp (6)	46	1	7
6.	[redacted]0.70	[redacted]2.2	4.000 p	184.000 B	tcp (6)	46	1	4
7.	[redacted]0.198	[redacted]2.3	8.000 p	0.359 KB	tcp (6)	46	1	8
8.	[redacted]0.70	[redacted]2.3	6.000 p	0.270 KB	tcp (6)	46	1	6
9.	[redacted]0.198	[redacted]2.4	6.000 p	0.270 KB	tcp (6)	46	1	6
10.	[redacted]0.70	[redacted]2.4	4.000 p	184.000 B	tcp (6)	46	1	4
11.	[redacted]0.198	[redacted]2.5	5.000 p	0.225 KB	tcp (6)	46	1	5
12.	[redacted]0.70	[redacted]2.5	6.000 p	0.270 KB	tcp (6)	46	1	6
13.	[redacted]0.198	[redacted]2.6	4.000 p	184.000 B	tcp (6)	46	1	4
14.	[redacted]0.70	[redacted]2.6	6.000 p	0.270 KB	tcp (6)	46	1	6
15.	[redacted]0.70	[redacted]2.7	3.000 p	138.000 B	tcp (6)	46	1	3
16.	[redacted]0.198	[redacted]2.7	5.000 p	0.225 KB	tcp (6)	46	1	5
17.	[redacted]0.198	[redacted]2.8	5.000 p	0.225 KB	tcp (6)	46	1	5
18.	[redacted]0.70	[redacted]2.8	4.000 p	184.000 B	tcp (6)	46	1	4
19.	[redacted]0.198	[redacted]2.9	9.000 p	0.404 KB	tcp (6)	46	1	9
20.	[redacted]0.70	[redacted]2.9	4.000 p	184.000 B	tcp (6)	46	1	4
21.	[redacted]0.198	[redacted]2.10	3.000 p	138.000 B	tcp (6)	46	1	3

Ukázky provozních záznamů reprezentujících útok s odražením

- Z pohledu e-infrastruktury CESNET (v roli odrazné sítě)
  - Odraz, akceptace „požadavků na spojení“

.235.114	[redacted]	40.198	2.000 p	88.000 B	13/03/06 15:25:53.606	13/03/06 15:26:02.602	63677	www (80)	syn(2), ack(16)
.229.22		40.70	2.000 p	88.000 B	13/03/06 15:25:53.082	13/03/06 15:26:02.081	47363	www (80)	syn(2), ack(16)
.237.110		40.198	2.000 p	88.000 B	13/03/06 15:25:44.085	13/03/06 15:26:02.069	63302	www (80)	syn(2), ack(16)
.230.109		40.70	2.000 p	88.000 B	13/03/06 15:25:53.055	13/03/06 15:26:02.057	22167	www (80)	syn(2), ack(16)
.226.10		40.198	2.000 p	88.000 B	13/03/06 15:25:49.751	13/03/06 15:26:01.753	27309	www (80)	syn(2), ack(16)
.224.168		40.198	2.000 p	88.000 B	13/03/06 15:25:52.522	13/03/06 15:26:01.524	57738	www (80)	syn(2), ack(16)
.231.212		40.198	2.000 p	88.000 B	13/03/06 15:25:48.367	13/03/06 15:26:00.369	6067	www (80)	syn(2), ack(16)
.232.218		40.70	2.000 p	88.000 B	13/03/06 15:25:51.234	13/03/06 15:26:00.236	16882	www (80)	syn(2), ack(16)
.230.167		40.198	2.000 p	88.000 B	13/03/06 15:25:50.968	13/03/06 15:26:02.971	27248	www (80)	syn(2), ack(16)
.232.68		40.198	2.000 p	88.000 B	13/03/06 15:25:53.154	13/03/06 15:26:02.156	52978	www (80)	syn(2), ack(16)
.238.112		40.70	2.000 p	88.000 B	13/03/06 15:25:53.007	13/03/06 15:26:02.009	342	www (80)	syn(2), ack(16)
.234.67		40.70	2.000 p	88.000 B	13/03/06 15:25:52.989	13/03/06 15:26:01.988	7837	www (80)	syn(2), ack(16)
.228.35		40.70	2.000 p	88.000 B	13/03/06 15:25:43.518	13/03/06 15:26:01.509	16219	www (80)	syn(2), ack(16)
.235.87		40.198	2.000 p	88.000 B	13/03/06 15:25:49.471	13/03/06 15:26:01.473	62665	www (80)	syn(2), ack(16)
.231.175		40.70	2.000 p	88.000 B	13/03/06 15:25:48.321	13/03/06 15:26:00.320	39842	www (80)	syn(2), ack(16)
.225.50		40.70	2.000 p	88.000 B	13/03/06 15:25:47.694	13/03/06 15:25:59.696	38620	www (80)	syn(2), ack(16)
.236.199		40.70	2.000 p	88.000 B	13/03/06 15:25:47.691	13/03/06 15:25:59.693	19954	www (80)	syn(2), ack(16)
.229.40		40.198	2.000 p	88.000 B	13/03/06 15:25:53.592	13/03/06 15:25:59.594	64889	www (80)	syn(2), ack(16)
.239.145		40.198	2.000 p	88.000 B	13/03/06 15:25:53.564	13/03/06 15:25:59.561	47067	www (80)	syn(2), ack(16)
.224.70		40.198	2.000 p	88.000 B	13/03/06 15:25:50.508	13/03/06 15:25:59.507	45598	www (80)	syn(2), ack(16)
.232.77		40.70	2.000 p	88.000 B	13/03/06 15:25:52.892	13/03/06 15:25:58.894	53899	www (80)	syn(2), ack(16)
.236.129		40.198	2.000 p	88.000 B	13/03/06 15:25:46.878	13/03/06 15:25:58.879	31461	www (80)	syn(2), ack(16)
.230.213		40.70	2.000 p	88.000 B	13/03/06 15:25:52.543	13/03/06 15:25:58.542	15140	www (80)	syn(2), ack(16)
.231.145		40.70	2.000 p	88.000 B	13/03/06 15:25:46.484	13/03/06 15:25:58.382	32972	www (80)	syn(2), ack(16)
.227.188		40.70	2.000 p	88.000 B	13/03/06 15:25:51.842	13/03/06 15:25:57.841	54540	www (80)	syn(2), ack(16)
.232.162		40.70	2.000 p	88.000 B	13/03/06 15:25:48.526	13/03/06 15:25:57.528	30980	www (80)	syn(2), ack(16)
.229.11		40.198	2.000 p	88.000 B	13/03/06 15:25:45.469	13/03/06 15:25:57.470	17408	www (80)	syn(2), ack(16)

Ukázky provozních záznamů reprezentujících útok s odražením

- Z pohledu e-infrastruktury CESNET (v roli odrazné sítě)
  - Odraz, odmítnutí „požadavků na spojení“

.48.2	[redacted]	40.198	1.000 p	40.000 B	13/03/06 15:25:00.423	13/03/06 15:25:00.423	33438	www (80)	rst(4), ack(16)
.150.41		40.198	1.000 p	40.000 B	13/03/06 15:25:01.447	13/03/06 15:25:01.447	10976	www (80)	rst(4), ack(16)
.86.113		40.198	1.000 p	40.000 B	13/03/06 15:25:01.447	13/03/06 15:25:01.447	50501	www (80)	rst(4), ack(16)
.11.248		40.70	1.000 p	40.000 B	13/03/06 15:25:01.133	13/03/06 15:25:01.133	45600	www (80)	rst(4)
.20.129		40.70	1.000 p	40.000 B	13/03/06 15:25:00.673	13/03/06 15:25:00.673	59886	www (80)	rst(4), ack(16)
.250.75		40.70	1.000 p	40.000 B	13/03/06 15:25:00.482	13/03/06 15:25:00.482	8966	www (80)	rst(4), ack(16)
.105.21		40.198	1.000 p	40.000 B	13/03/06 15:25:00.409	13/03/06 15:25:00.409	48194	www (80)	rst(4), ack(16)
.68.167		40.198	1.000 p	40.000 B	13/03/06 15:25:01.540	13/03/06 15:25:01.540	36493	www (80)	rst(4), ack(16)
.251.39		40.198	1.000 p	40.000 B	13/03/06 15:25:00.914	13/03/06 15:25:00.914	3438	www (80)	rst(4), ack(16)
.77.136		40.70	1.000 p	40.000 B	13/03/06 15:25:00.914	13/03/06 15:25:00.914	59889	www (80)	rst(4), ack(16)
.39.1		40.198	1.000 p	40.000 B	13/03/06 15:25:01.429	13/03/06 15:25:01.429	30708	www (80)	rst(4), ack(16)
.53.33		40.198	1.000 p	40.000 B	13/03/06 15:25:00.841	13/03/06 15:25:00.841	59489	www (80)	rst(4), ack(16)
2.197		40.198	1.000 p	40.000 B	13/03/06 15:25:00.616	13/03/06 15:25:00.616	5704	www (80)	rst(4), ack(16)
.3.27		40.198	1.000 p	40.000 B	13/03/06 15:25:00.546	13/03/06 15:25:00.546	8047	www (80)	rst(4), ack(16)
.64.65		40.70	1.000 p	40.000 B	13/03/06 15:25:04.692	13/03/06 15:25:04.692	30410	www (80)	rst(4), ack(16)
.212.1		40.198	1.000 p	40.000 B	13/03/06 15:25:04.758	13/03/06 15:25:04.758	19802	www (80)	rst(4), ack(16)
.64.68		40.70	1.000 p	40.000 B	13/03/06 15:25:04.527	13/03/06 15:25:04.527	9068	www (80)	rst(4), ack(16)
.64.68		40.70	1.000 p	40.000 B	13/03/06 15:25:02.592	13/03/06 15:25:02.592	63110	www (80)	rst(4), ack(16)
.25.206		40.70	1.000 p	40.000 B	13/03/06 15:25:01.942	13/03/06 15:25:01.942	29185	www (80)	rst(4), ack(16)
.147.10		40.198	1.000 p	40.000 B	13/03/06 15:25:01.955	13/03/06 15:25:01.955	19923	www (80)	rst(4), ack(16)
.117.179		40.70	1.000 p	40.000 B	13/03/06 15:25:01.933	13/03/06 15:25:01.933	58983	www (80)	rst(4), ack(16)
.208.193		40.70	1.000 p	40.000 B	13/03/06 15:25:01.936	13/03/06 15:25:01.936	57336	www (80)	rst(4), ack(16)
.87.37		40.198	1.000 p	40.000 B	13/03/06 15:25:01.945	13/03/06 15:25:01.945	52971	www (80)	rst(4), ack(16)
.173.8		40.70	1.000 p	40.000 B	13/03/06 15:25:01.939	13/03/06 15:25:01.939	63778	www (80)	rst(4), ack(16)
.113.129		40.198	1.000 p	40.000 B	13/03/06 15:25:01.952	13/03/06 15:25:01.952	43354	www (80)	rst(4), ack(16)
.225.1		40.70	1.000 p	40.000 B	13/03/06 15:25:01.969	13/03/06 15:25:01.969	40144	www (80)	rst(4), ack(16)
.81.178		40.198	1.000 p	40.000 B	13/03/06 15:25:01.974	13/03/06 15:25:01.974	43418	www (80)	rst(4), ack(16)
.193.3		40.198	1.000 p	40.000 B	13/03/06 15:25:01.974	13/03/06 15:25:01.974	53695	www (80)	rst(4), ack(16)
.199.105		40.70	1.000 p	40.000 B	13/03/06 15:25:01.974	13/03/06 15:25:01.974	65387	www (80)	rst(4), ack(16)
.180.94		40.70	1.000 p	40.000 B	13/03/06 15:25:01.980	13/03/06 15:25:01.980	26824	www (80)	rst(4), ack(16)

Ukázky provozních záznamů reprezentujících útok s odražením

- Efektivita odrazu přes e-infrastrukturu CESNET ???

- Příklad náhodně vybraného útoku - vzorek provozních dat z **hraničního směrovače** e-infrastruktury CESNET, provoz do/z NIX

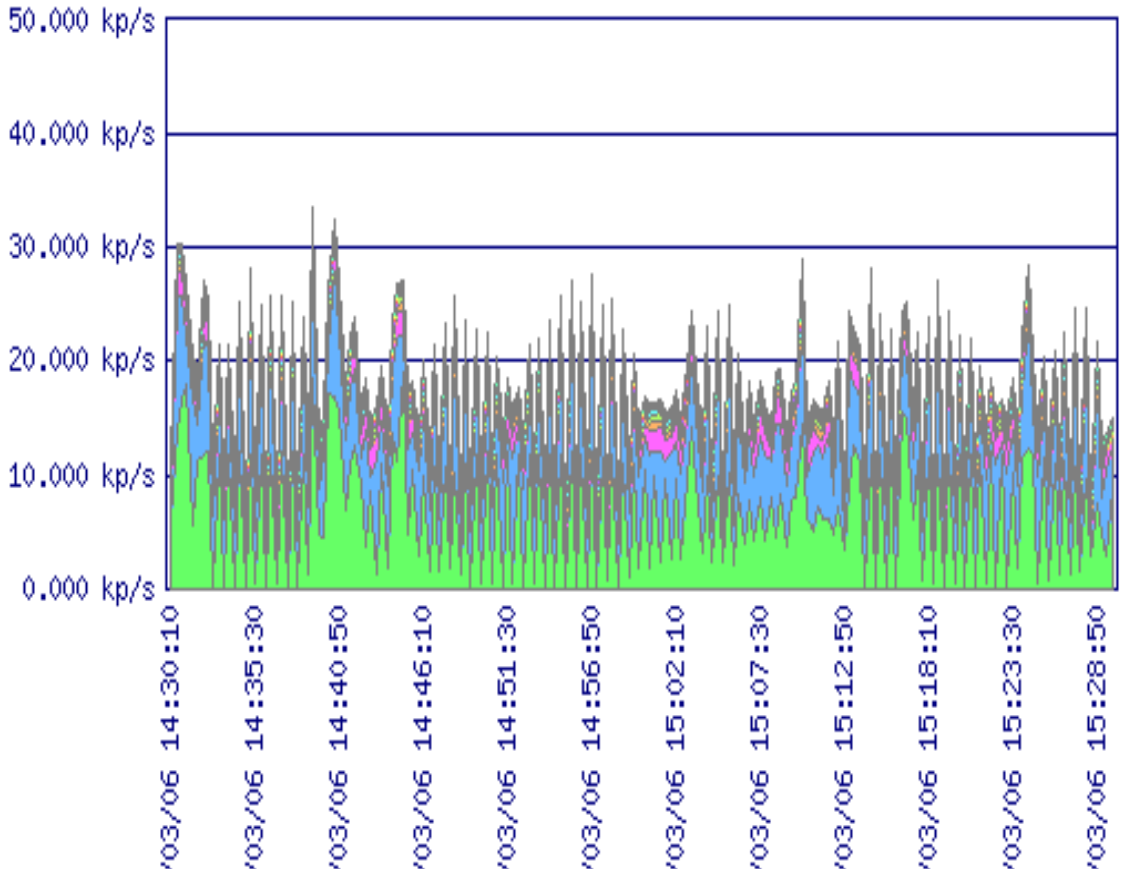
- Počet SYN: 61.444 Mpkt
- Počet odrazů jako SYN+ACK: 4.190 Mpkt ~ **6.81%**
- Počet odrazů jako RST/RST+ACK: 2.070 Mpkt ~ **3.37%**

→ **efektivita odrazu ~ 10%**

- ICMP side efekty < 1Mpkt (oba směry)

Ukázky provozních záznamů reprezentujících útok s odražením

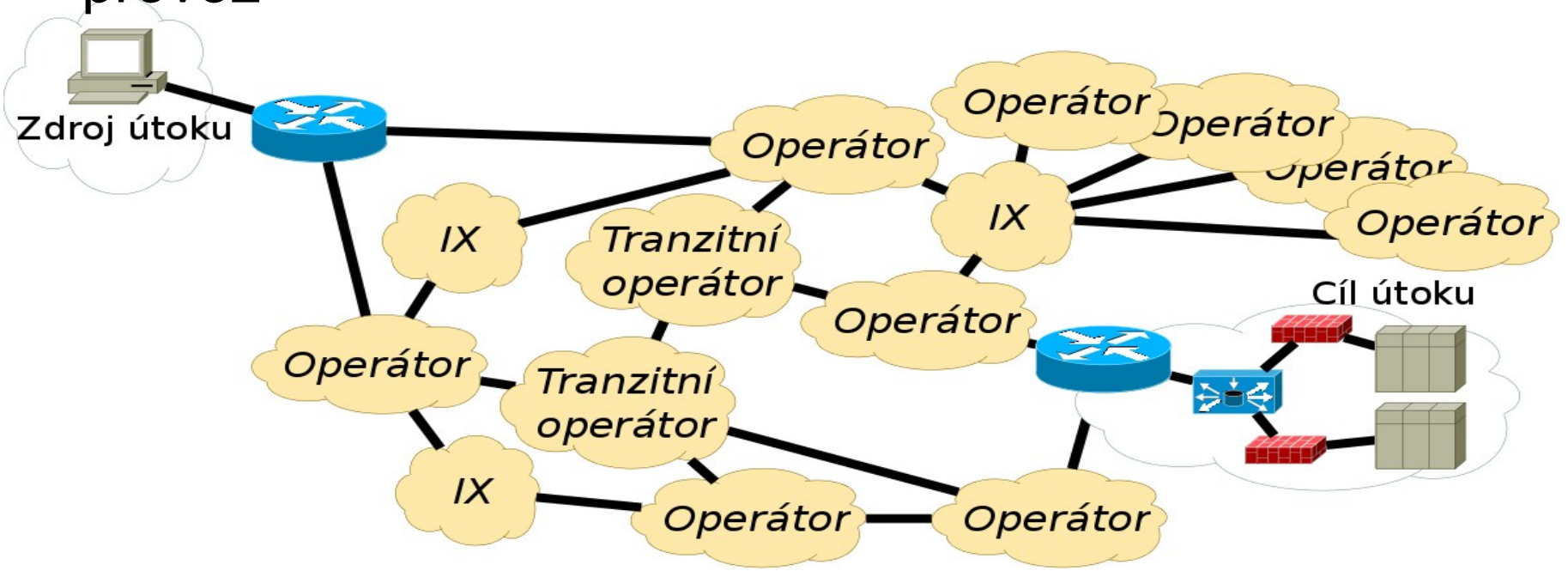
- Rozložení v čase ???
- Vzorek provozu z některých regionálních směrováčů e-infrastruktury CESNET – prakticky rovnoměrné rozložení vzhledem k vzorkování vstupních dat



	Pkts-estimated	Bytes-estimated	Protocol	
1.	25.559 mp ~ 40.169%	1.103 GB ~ 37.181%	tcp (6)	P
2.	22.252 mp ~ 34.971%	0.964 GB ~ 32.470%	tcp (6)	L
3.	6.764 mp ~ 10.631%	0.308 GB ~ 10.384%	tcp (6)	Z
4.	2.323 mp ~ 3.651%	143.542 MB ~ 4.724%	tcp (6)	C
5.	2.087 mp ~ 3.280%	114.597 MB ~ 3.771%	tcp (6)	H
6.	1.533 mp ~ 2.409%	95.237 MB ~ 3.134%	tcp (6)	J
7.	0.954 mp ~ 1.499%	83.030 MB ~ 2.732%	tcp (6)	Ji
8.	0.910 mp ~ 1.430%	64.337 MB ~ 2.117%	tcp (6)	U
9.	0.677 mp ~ 1.064%	46.381 MB ~ 1.526%	tcp (6)	P
10.	0.570 mp ~ 0.895%	59.555 MB ~ 1.960%	tcp (6)	C

Rámcové možnosti eliminace útoků s podvrženou IP na úrovni transportu

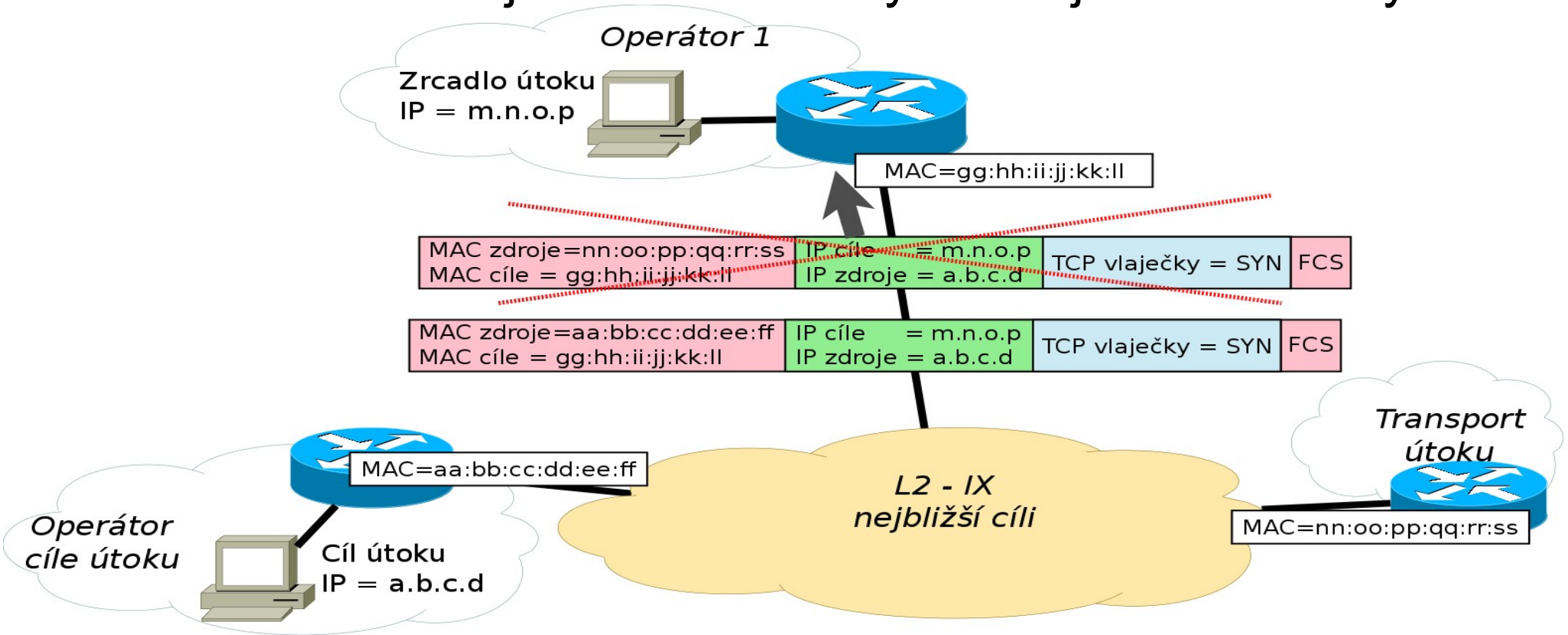
- Možnosti efektivní eliminace útoku tohoto typu na úrovni transportu souvisí se schopností identifikovat příslušný provoz



Pravděpodobnost přesného určení provozu s podvrženými zdrojovými adresami zpravidla klesá se vzdáleností (topologoickou ~ hop count) od zdroje dat...

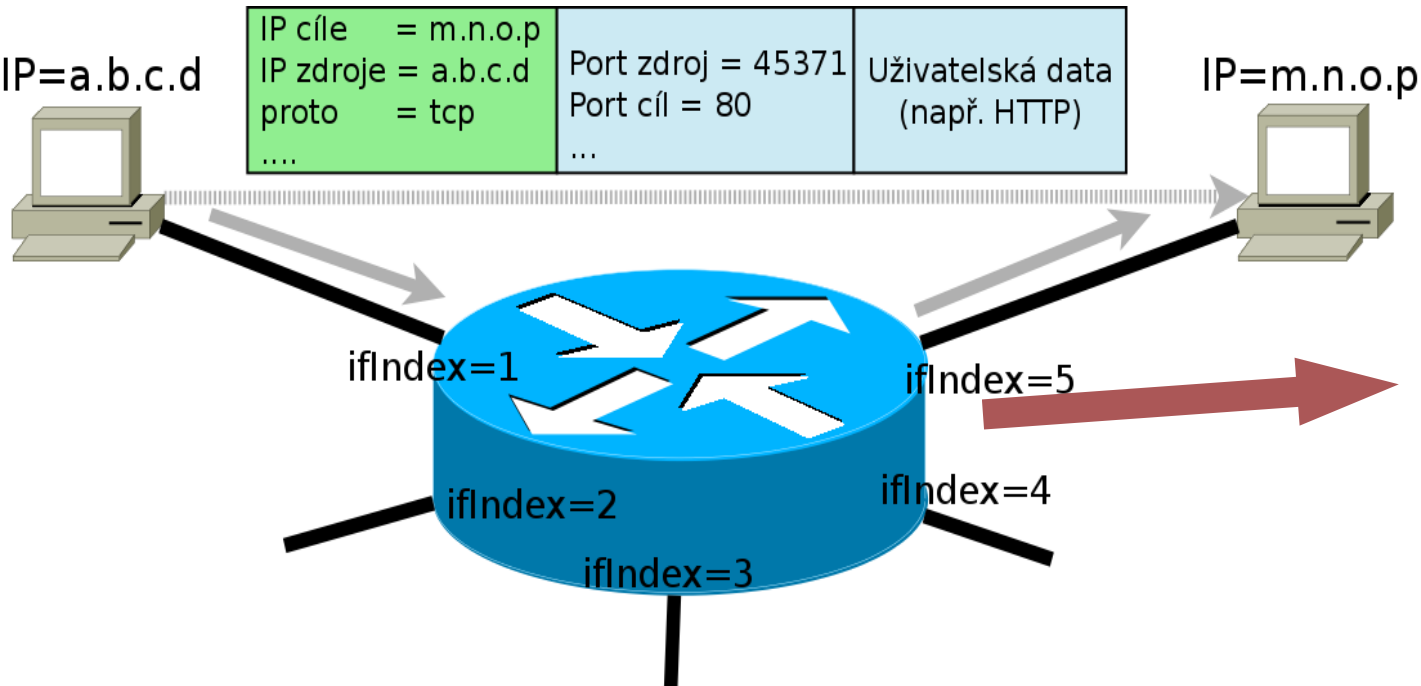
Rámcové možnosti identifikace útoků s podvrženou IP na úrovni transportu

- Příklad ad-hoc identifikace podvržené zdrojové IP adresy na základě znalosti zařízení, které datagram odeslalo v rámci L2 infrastruktury (IX)
- Podmínka - operátor 1 musí vědět, kdo (MAC adresa) je operátorem „a.b.c.d“ (cíl útoku) – podvrh lze určit na základě kombinace zdrojové MAC adresy a zdrojové IP adresy



Rámcové možnosti identifikace útoků s podvrženou IP na úrovni transportu

- Příklad ad-hoc identifikace podvržené zdrojové IP adresy na základě znalosti směru, ze kterého datagram do infrastruktury vstoupil pomocí provozních informací typu „NetFlow“
  - Daným rozhraním nemůže být příslušná IP síť dostupná
  - V rámci aktuálního provozního stavu je velmi nízká pravděpodobnost, že by daným rozhraním měla z dané IP sítě přicházet data



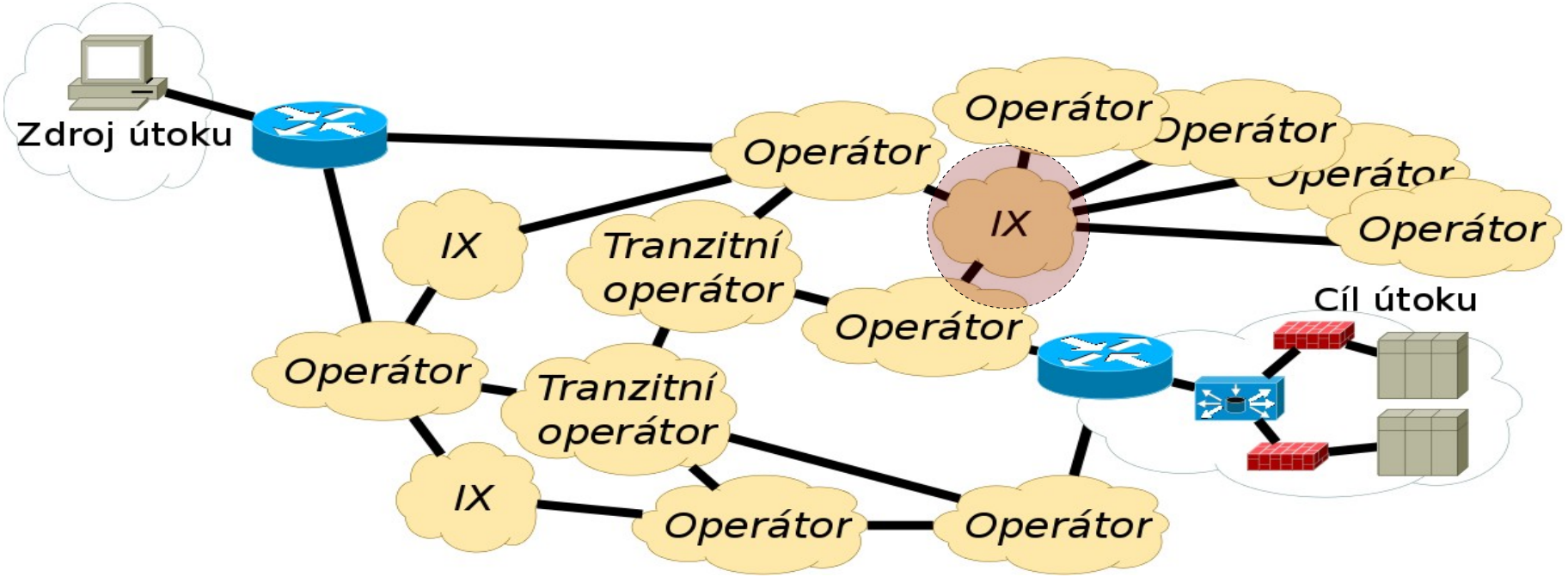

```
SrcIP   = a.b.c.d
DstIP   = m.n.o.p
Proto   = tcp
SrcPort = 45371
DstPort = 80
SrcIf   = 1
DstIf   = 5
...
Octets  = 12252
Pkts    = 12
```

Rámcové možnosti eliminace útoků s podvrženou IP na úrovni transportu

- Systematická provozní eliminace příchozích datagramů s podvrženou zdrojovou IP adresou
  - Standardní mechanismy založené na kontrole zdrojové IP adresy (BCP 38, revese path check)
  - V závislosti na tom, co je oznamováno/přiděleno v příslušném směru
  - Obecně žádoucí → „net-etický standard“ ;-)
- Ad-hoc filtrace
  - Možnosti zařízení, která jsou k dispozici v daném místě
  - Principiální mantinely → „policy“ - neutralita, zásah do provozu třetích stran !!!
- Rozumná zásada - „nevytlačit“ takový provoz změnou směrování tam, kde už je naprosto neidentifikovatelný; řešit mechanismy „black hole“, „silent drop“, ...

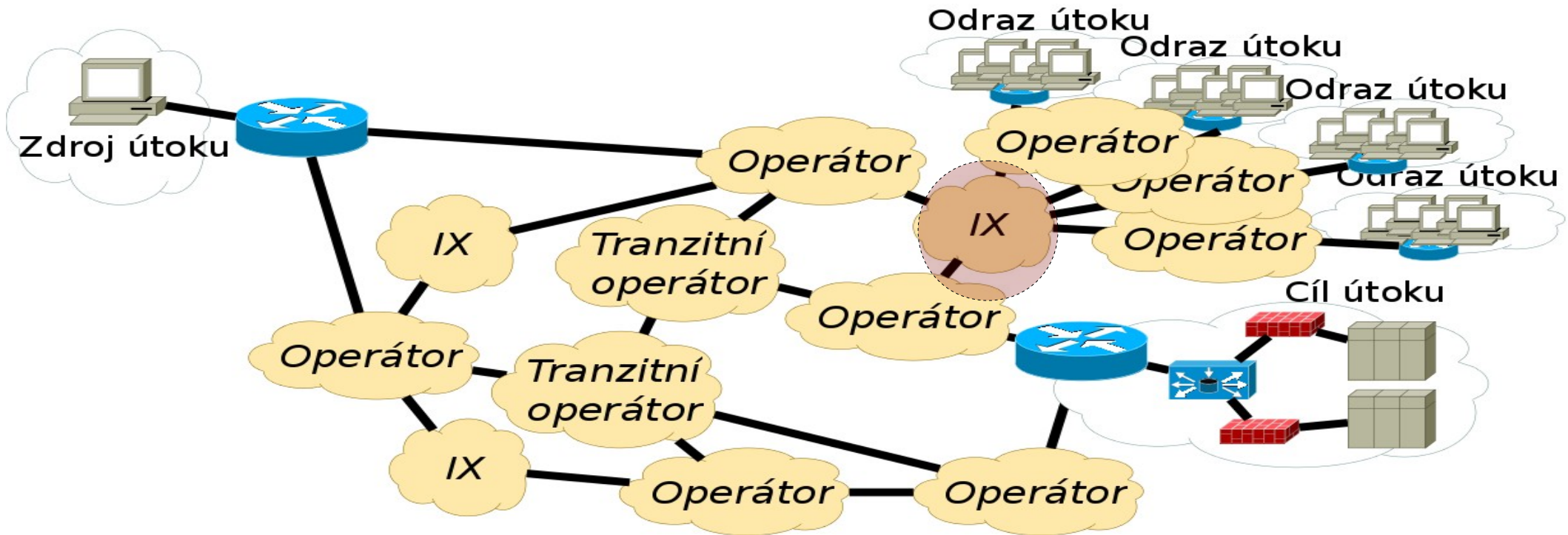
Rámcové možnosti eliminace útoků s podvrženou IP v koncové síti

- Přímý SYN flood s podvrženými zdrojovými adresami
  - Spolupráce se síťovým operátorem
  - Selektivní metody filtrace (technologické ~ adresace, významové ~ tuzemská služba), statistické metody filtrace ~ QoS, posouvání cíle útoku po adresovém prostoru (preventivně nízké ttl na DNS záznam), IPS, pračky provozu, předřadná zařízení s TCP synchronizací (bez okamžitých alokací v TCP stacku ;-)), SYN cookies,...



Rámcové možnosti eliminace útoků podvrženou IP v koncové síti

- „Bounce traffic“ primárně s podvrženými zdrojovými adresami
  - Spolupráce s operátorem sítě a s operátory odrážejících sítí - odraz TCP SYN požadavku je málo efektivní, ale po odrazu se obecně jedná z hlediska transportu o naprosto legitimní provoz (validní identifikátory, autentické ttl)
  - Účinná obrana v odrážejících sítích, pouze některé metody efektivně použitelné v síti cíle útoku



???