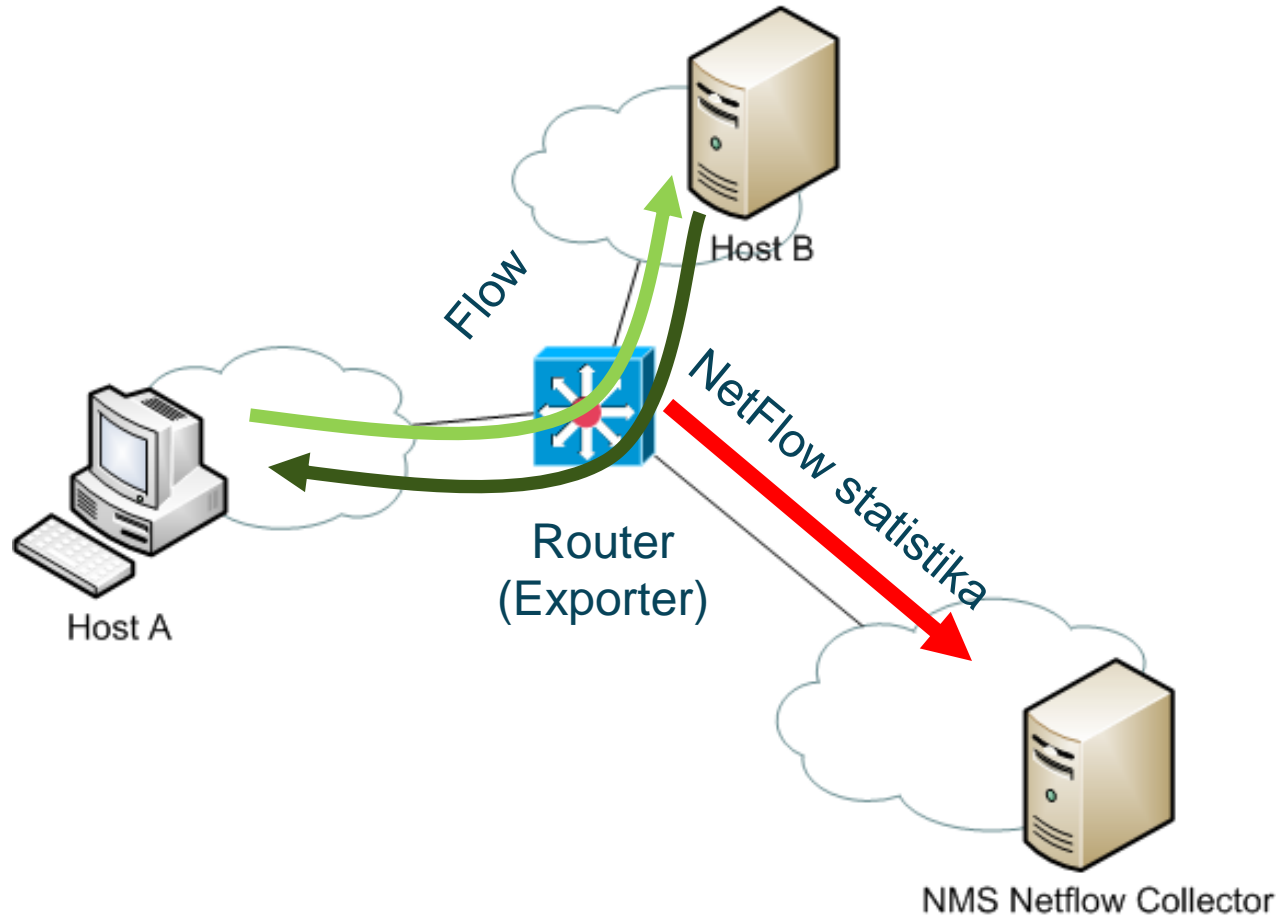


Praktična primena NetFlow protokola

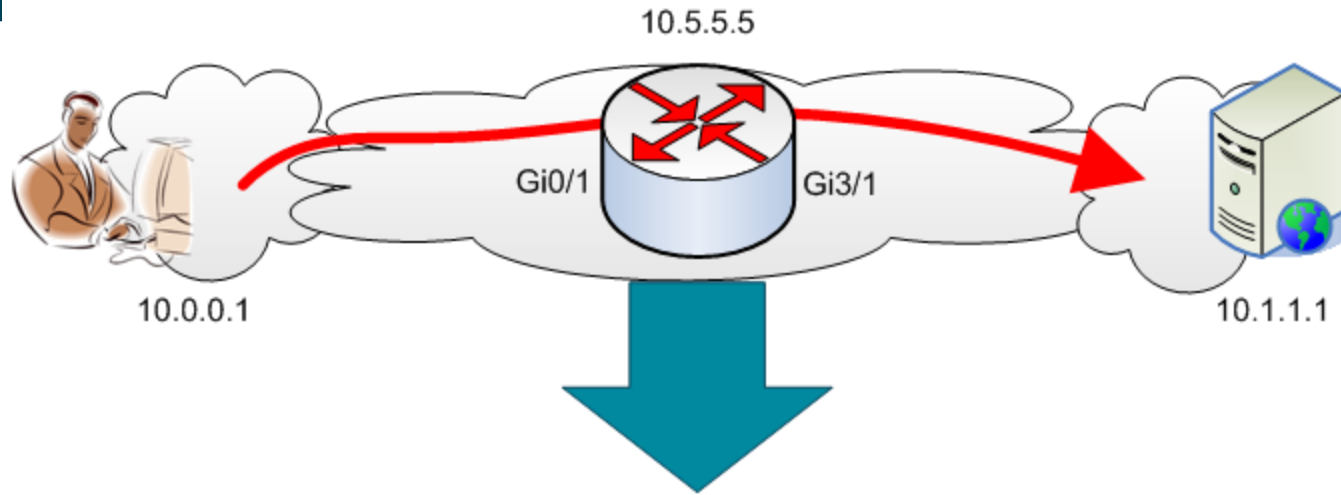
Ivan Ivanović, RCUB
Žabljak, februar 2013.

Šta je NetFlow tehnologija



- Razvijena od strane Cisco kompanije
- Standardizovana od strane IETF – novi naziv je IPFIX.
- Netflow V5 i V9 se danas najčešće koriste
- IPFIX (Netflow V9) – Fleksibilni NetFlow.
- Postoji definisano više od 100 NetFlow rekorda (većina se još uvek ne koristi)
- Pruža nam uvid u informacije o statistici sa L3-L4 sloja.
- Netflow V9 podržava i IPV6, MPLS, MAC....
- U AMRESu se samo NetFlow koristi za monitoring IPV6 protokola
- Drugi proizvođači takođe podržavaju NetFlow (Netstream, Jflow...).
- Empirijski je pokazano da čini manje od 1% od ukupnog saobraćaja umreži

Primer NetFlow statistike



Start time	End time	Src IP	Dst IP	Src port	Dst port	Protocol	tos	Packet	Bytes
01:00	01:01	10.0.0.1	10.1.1.1	9733	80	TCP	0	7	376

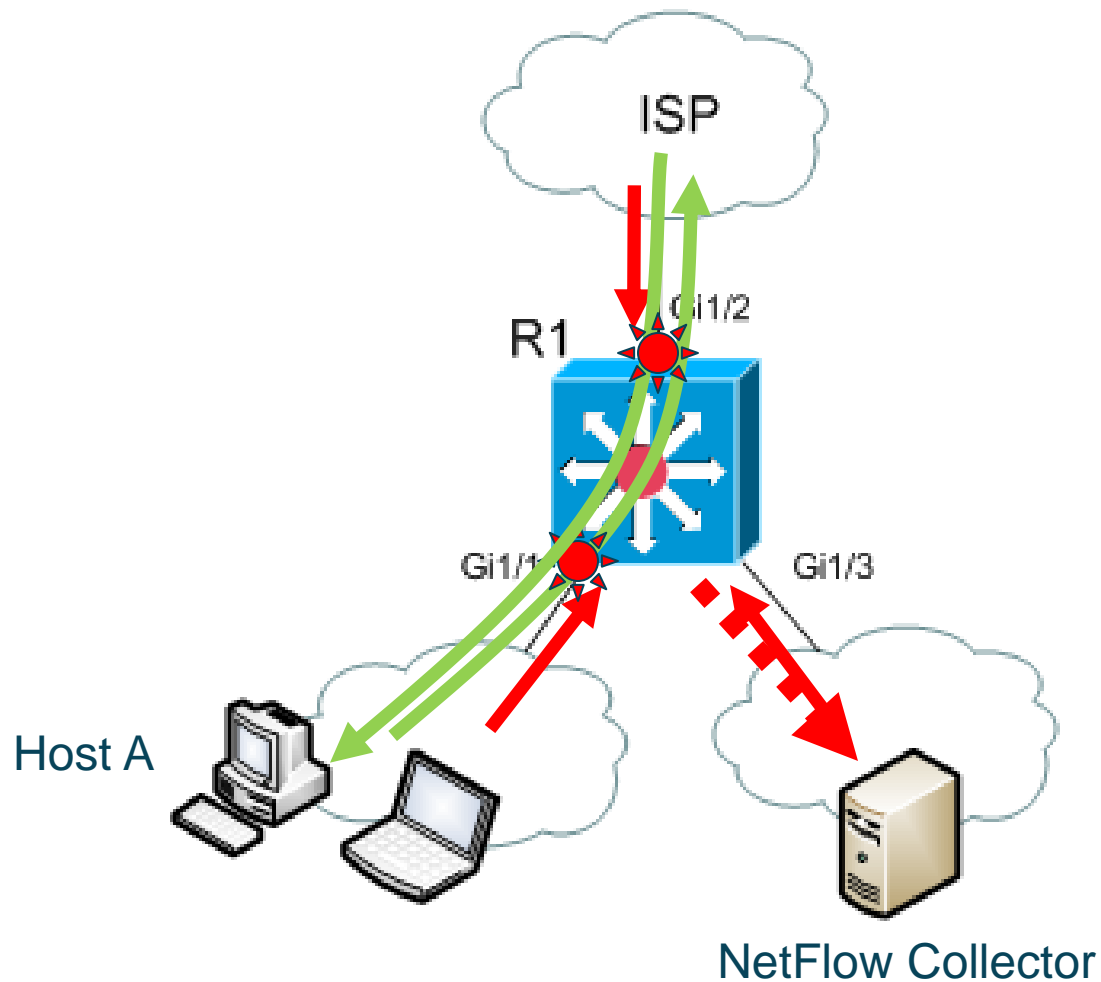
Tcp flags	Exporter	Interface IN	Interface OUT	Nex hop	Src AS	Dst AS
S	10.5.5.5	Gi0/1	Gi3/4	10.9.9.9	8756	6985

Kako pokrenuti prikupljanje NetFlow statistike?

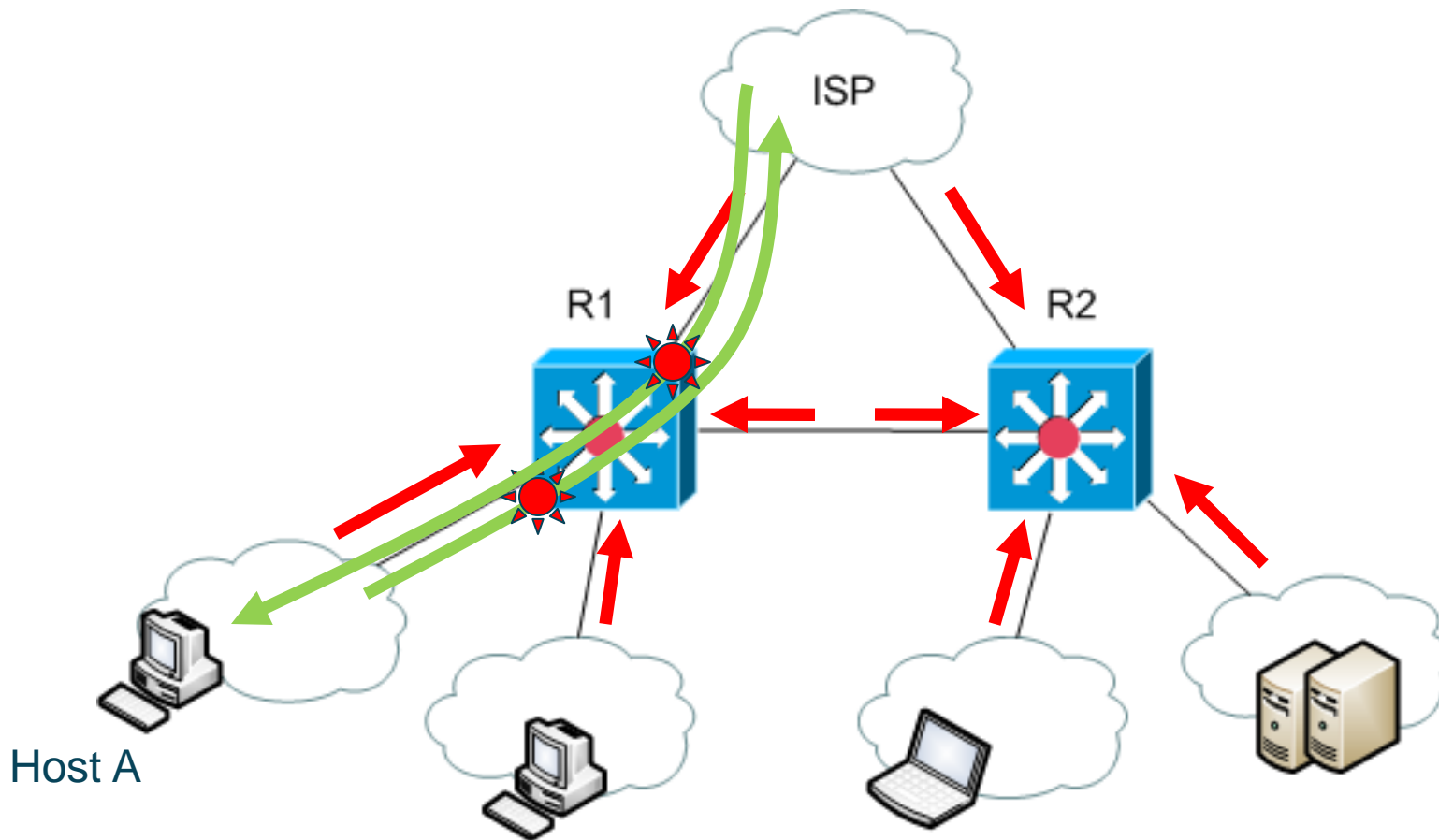


- Dosta rutera koji prosleđuju pakete u “softveru” podržavaju NetFlow
- Neki od L3 svičeva takođe podržavaju NetFlow (dodatni moduli)
- Dva tipa podešavanja NetFlowa
 - Globalno
 - Na nivou interfejsa
- Globalno podešavanje dopušta prikupljanje statistike jedino na svim interfejsima i to najčešće u jednom smeru (in/ingress)
- Podešavanje na nivou interfejsa nam daje veću fleksibilnost i najčešće je moguće birati smer in/ingress ili out/outgress

NetFlow podešavanje- IN smer

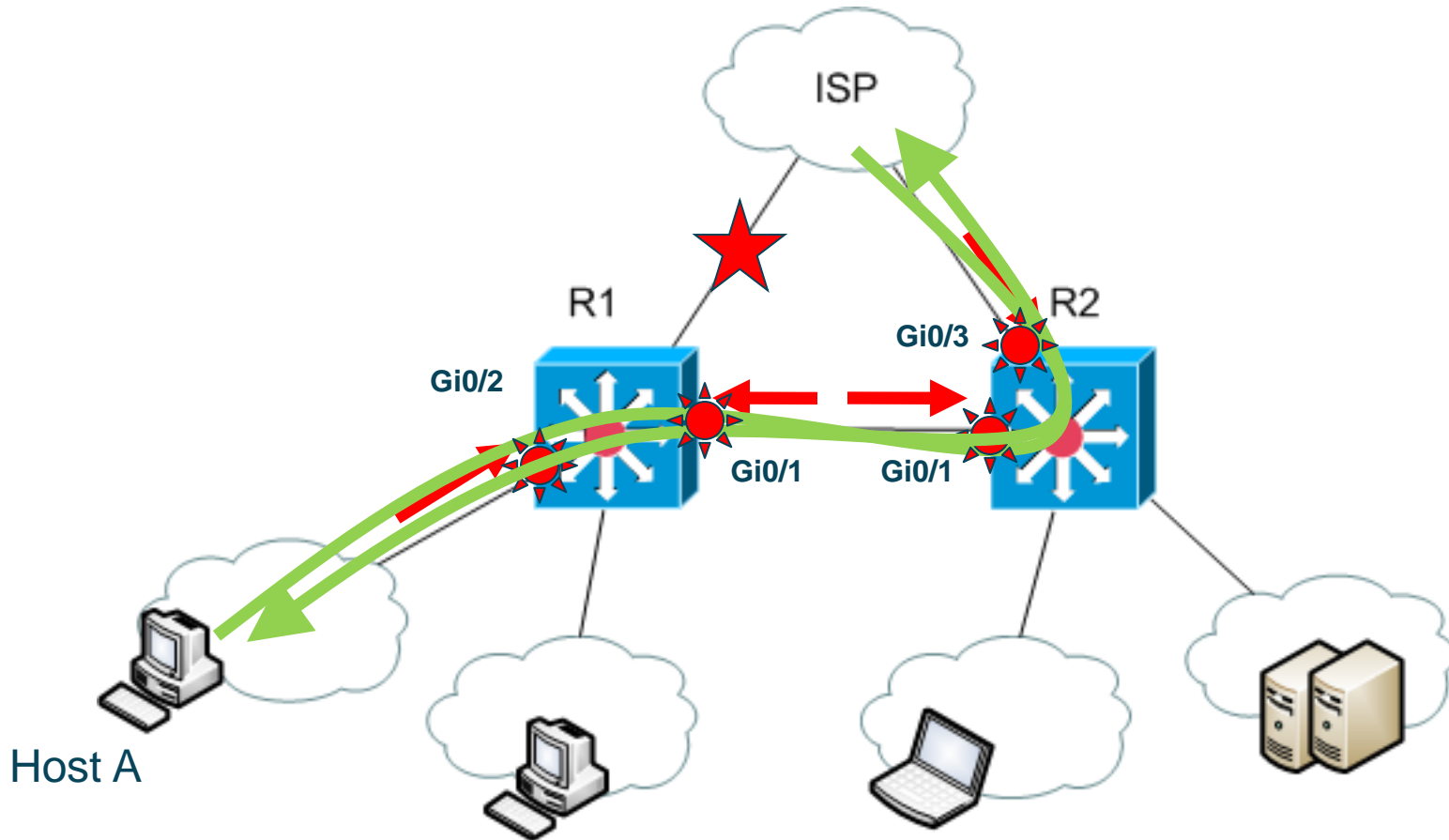


NetFlow podešavanje- IN smer

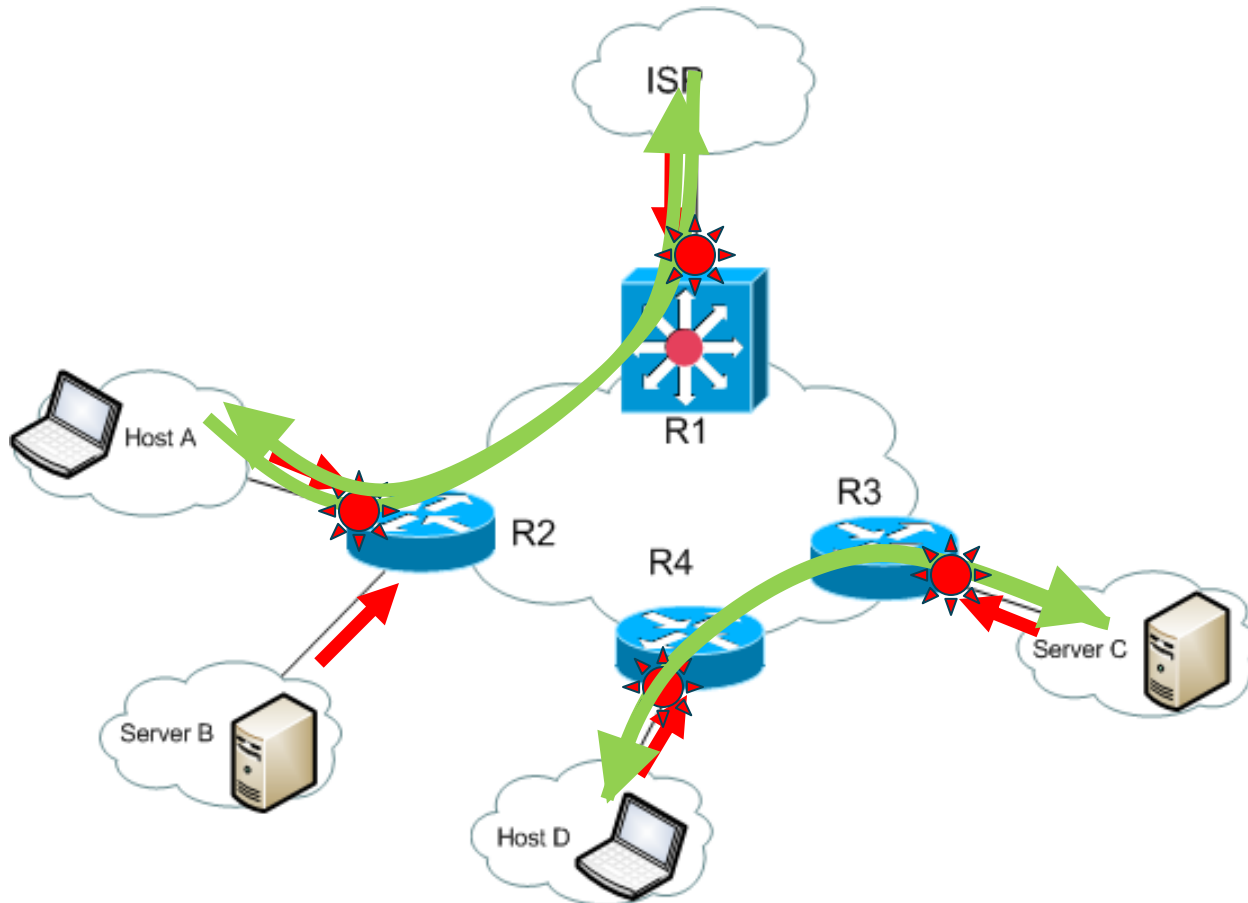


Host A

NetFlow dupliranje statistike- IN smer



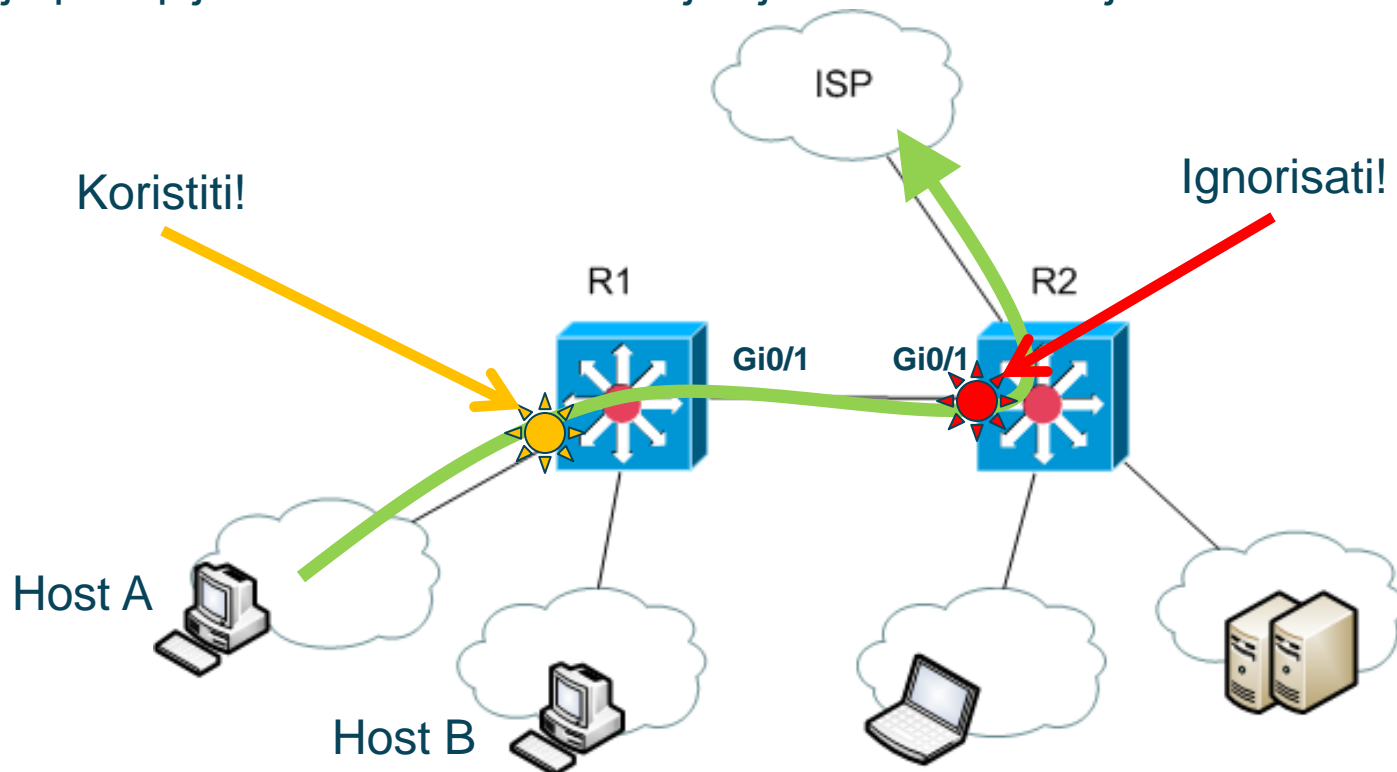
NetFlow dupliranje statistike



- Problem se lako može rešiti ako uređaj ima kontrolu eksporta NetFlow statistike na nivou svako pojedinačnog interfejsa.
- Korišćenjem Ingress/Egress komande možemo kontrolisati prikupljanje NetFlow statistike.
- Neke aplikacije koje prikupljaju NetFlow statistiku imaju mogućnost da provere da li dolazi do dupliranja prikupljene statistike. (src ip, dst ip , src port, dst port, in/out interfaces, next hop...).
- Veoma dobro rešenje predstavljaju kolektori NetFlow statistike koji imaju mogućnost filtriranja na osnovu NetFlow rekorda (polja)

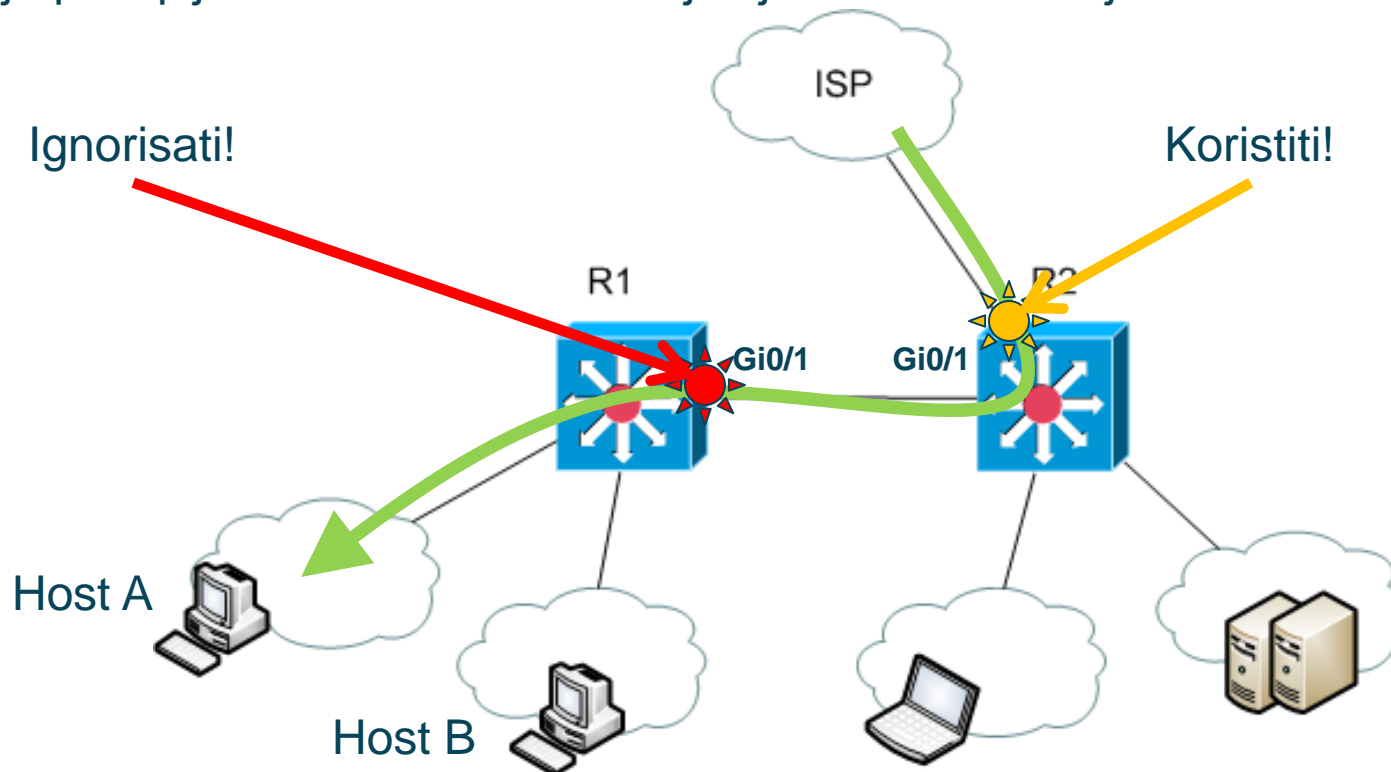
Dupliranje NetFlow statistike- Rešenje

- Nećemo koristiti NetFlow statistiku koja ima IP adresu eksportera R2 i koja je prikupljena koristeći saobraćaj koji ulazi na interfejs Gi0/1 uređaja R2!



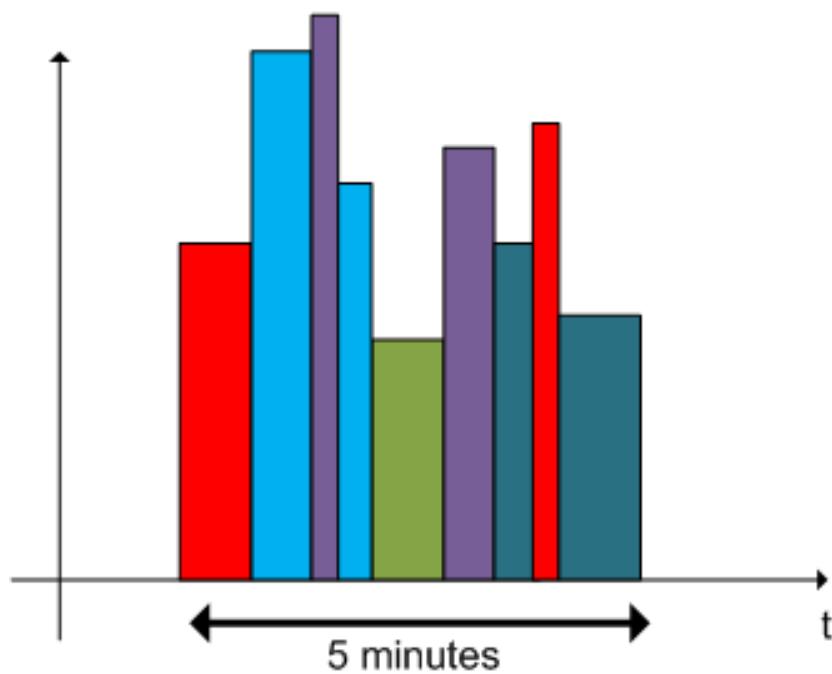
Dupliranje NetFlow statistike- Rešenje

- Nećemo koristiti NetFlow statistiku koja ima IP adresu eksportera R1 i koja je prikupljena koristeći saobraćaj koji ulazi na interfejs Gi0/1 uređaja R1!



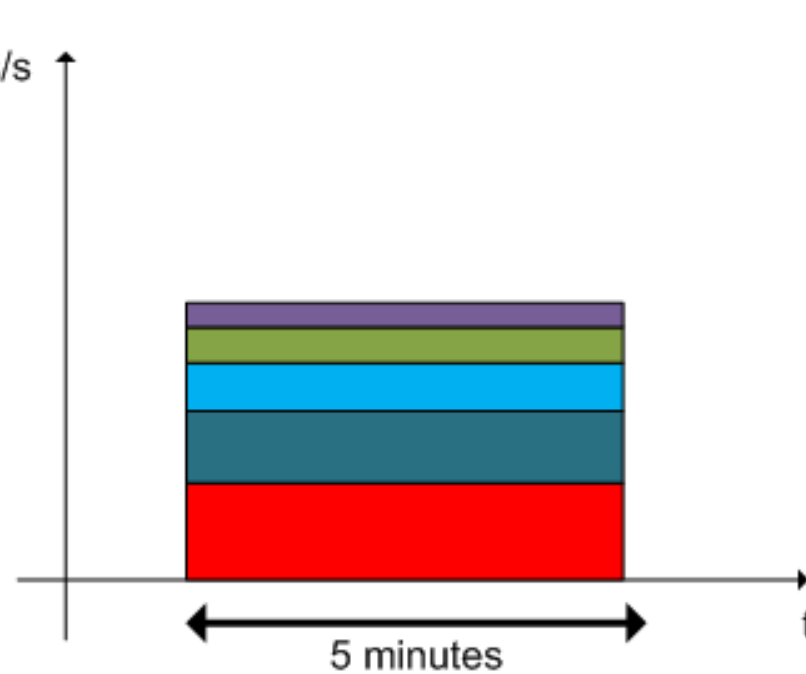
- Većina administratora ih ne koristi
- Neke od aplikacija koje prikupljaju NetFlow statistiku ne koriste timestap polje koje NetFlow eksportuje
 - Problem se javlja kod velike količine NetFlow podataka
 - Rešenje je agregacija podataka
- Prednosti agregacije su manje baze i brži rad aplikacija
- Mana agregacije je nedostatak detalja
- Šta su NetFlow tajmeri (aging)?
- Npr. Cisco
 - Normal
 - Long
 - Short (threshold ~100packets)

Multiple samples per host



≈

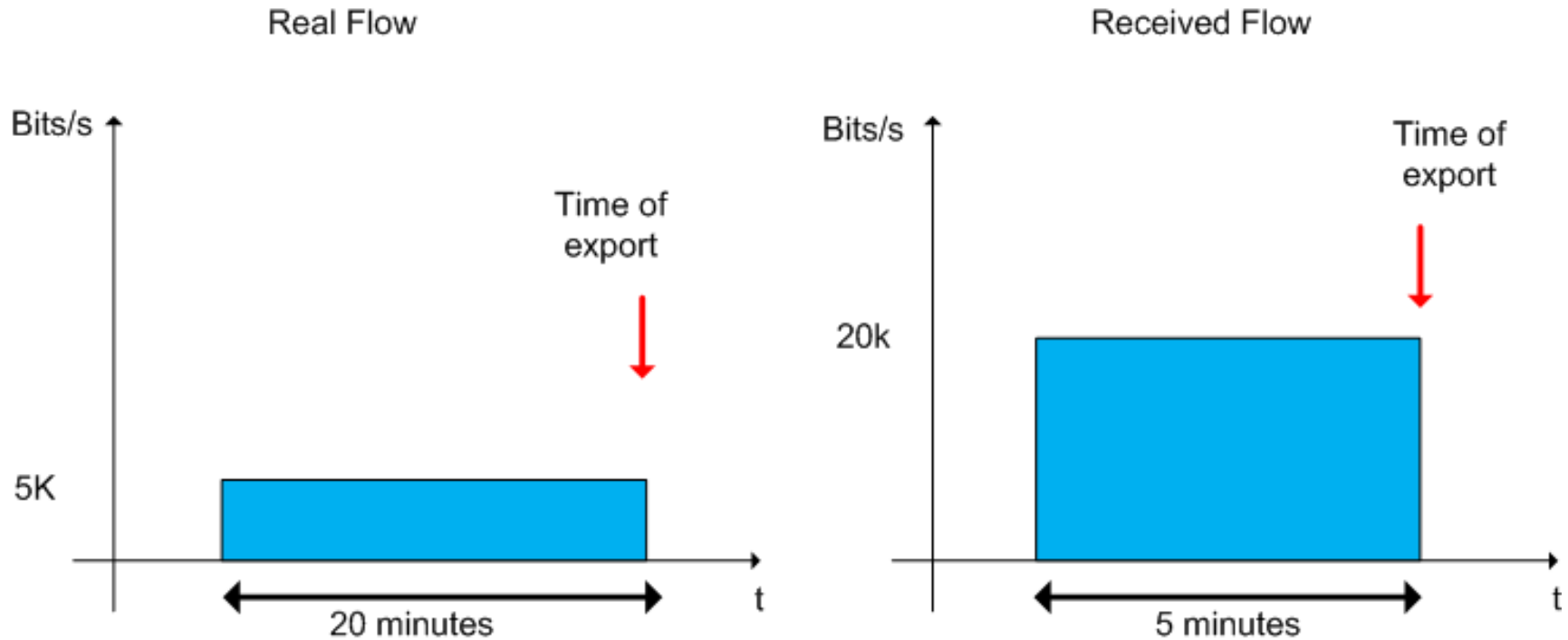
One sample per host



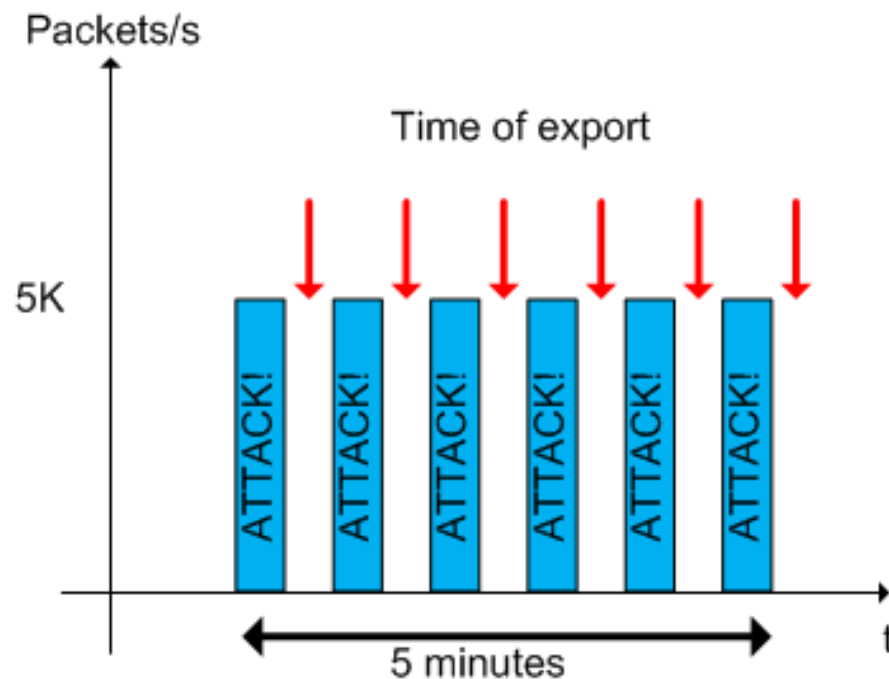
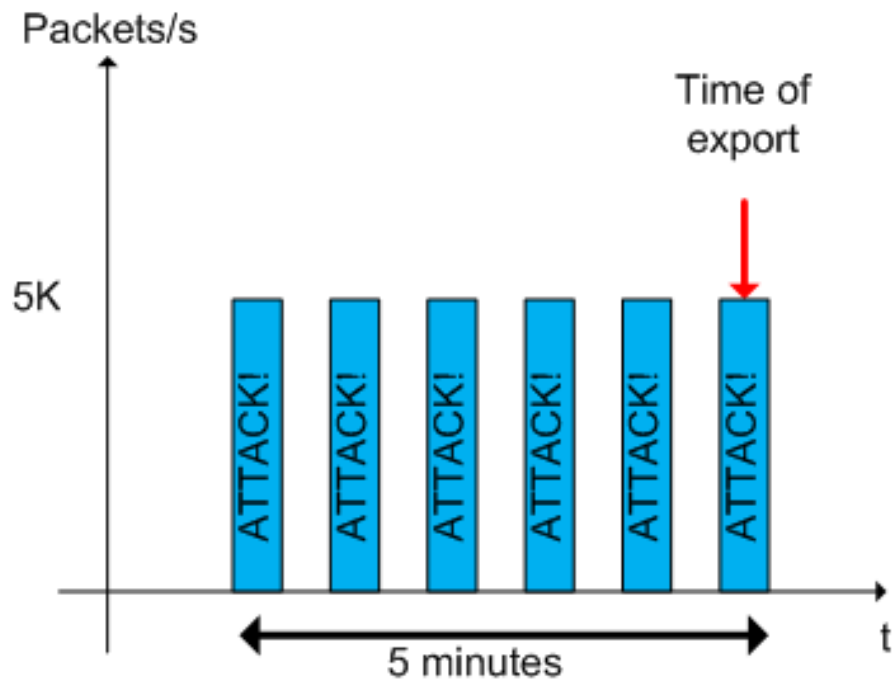
NetFlow Tajmeri– Long aging



- Receiving application is using 5 minute aggregation



NetFlow Tajmeri– Fast aging (Detekcija napada!)



NetFlow tajmeri i popunjavanje lokalne memorije eksportera



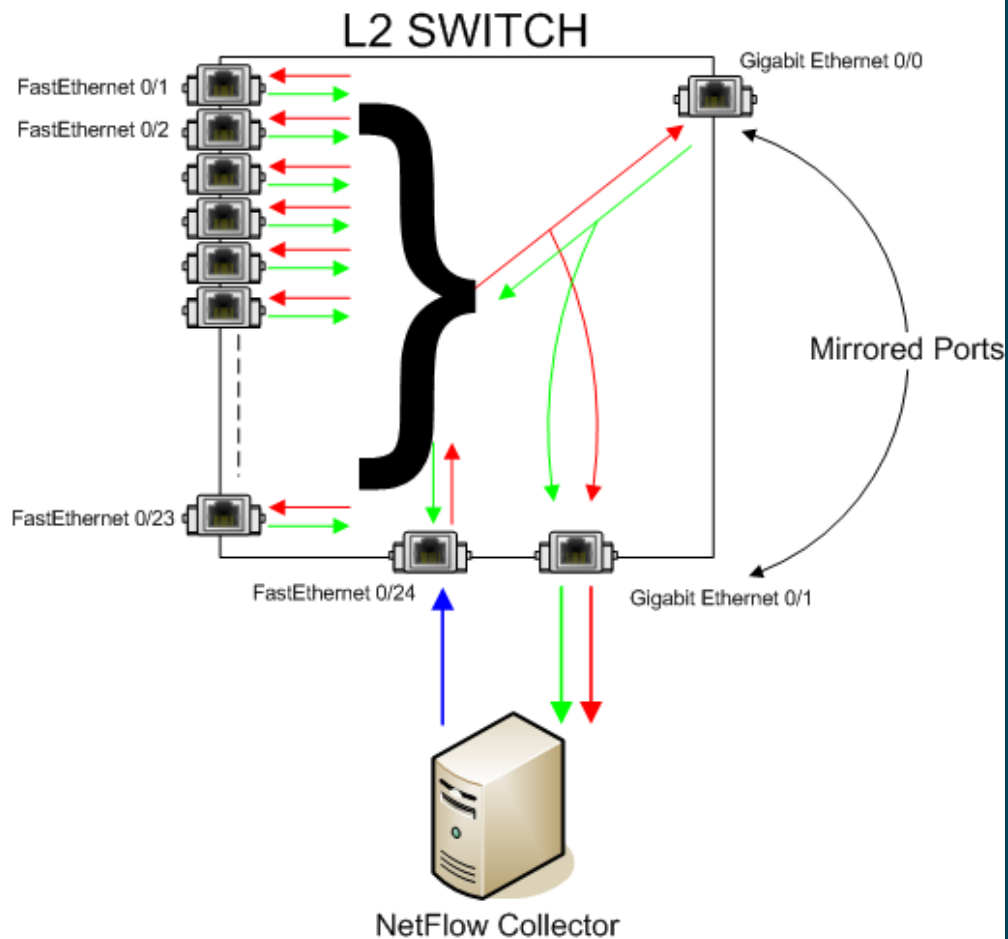
- Eksporter prikuplja statistiku lokalno u svojoj memoriji
- Kada se memorija prepuni kolektor označi sve prikupljene podatke kao zastarele i eksportuje. Zatim se lokalna memorija oslobađa.
- Specijalni slučajevi mogu dovesti do zauzimanja memorije
 - Ping sweep
 - DNS lookups
- Kod protokola koji uspostavljaju sesiju postoji mehanizam otkrivanja kraja sesije – TCP flegovi
- Kod protokoli koji ne uspostavljaju sesiju ne postoji mogućnost detekcije kraja sesije - UDP
- Preterano zauzimanje memorije može dovesti do opterećenja eksportera
- Tajmeri su jedini način da se “zastari” i eksportuje NetFlow statistika

- Veoma koristan alat!
- Dosta korisnih informacija se može naći na web stranici SWITCH NRENa
 - <http://www.switch.ch/network/projects/completed/TF-NGN/floma/software.html>
- Šta je NetFlow sonda?
- Kako se koristi?
- Gde se koristi?
- Šta se dobija sa tim?
- Šta se gubi ako je koristimo?
- Problemi?

Netflow Sonda- L2 segment mreže!



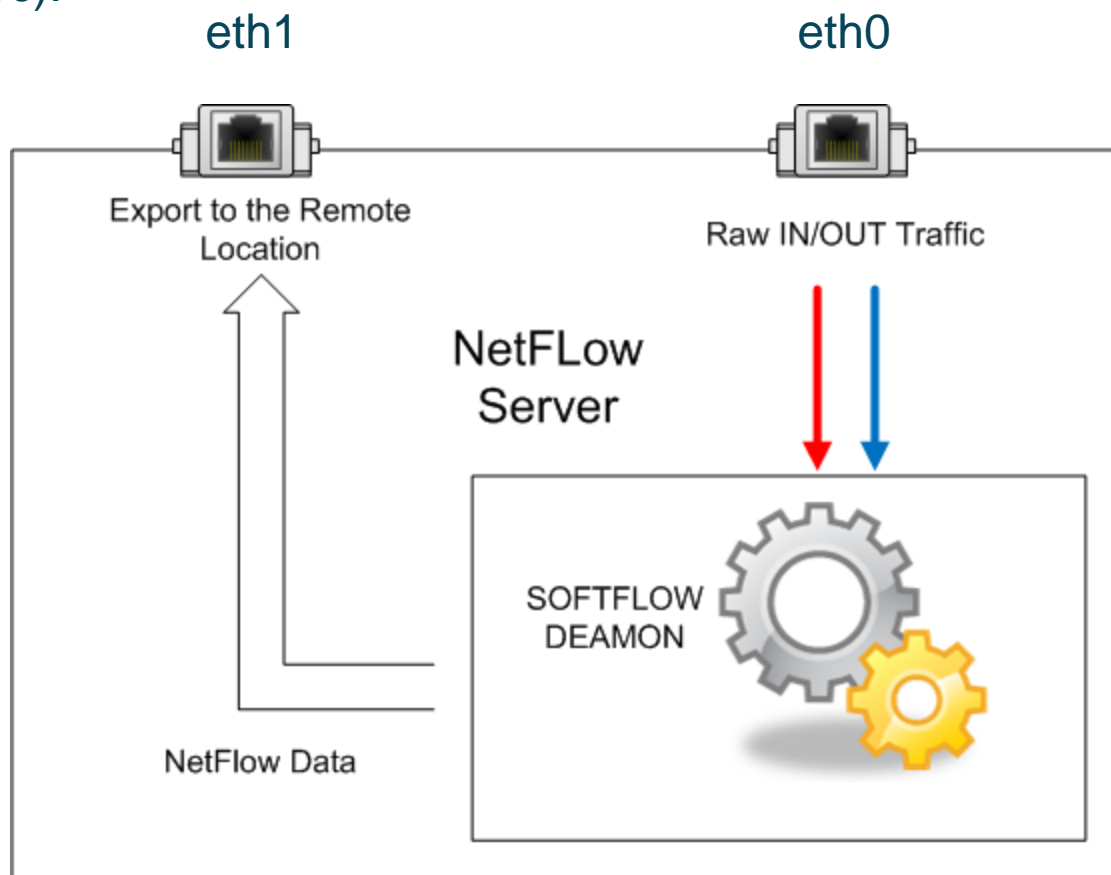
- L2 Svičevi ne podržavaju NetFlow protokol
- L2 Svičevi obično podržavaju port mirroring (SPAN)!
- E.g. softflowd
 - <http://www.mindrot.org/projects/softflowd/>
 - <http://code.google.com/p/softflowd/>



Netflow Sonda– Port mirroring zahtevi!



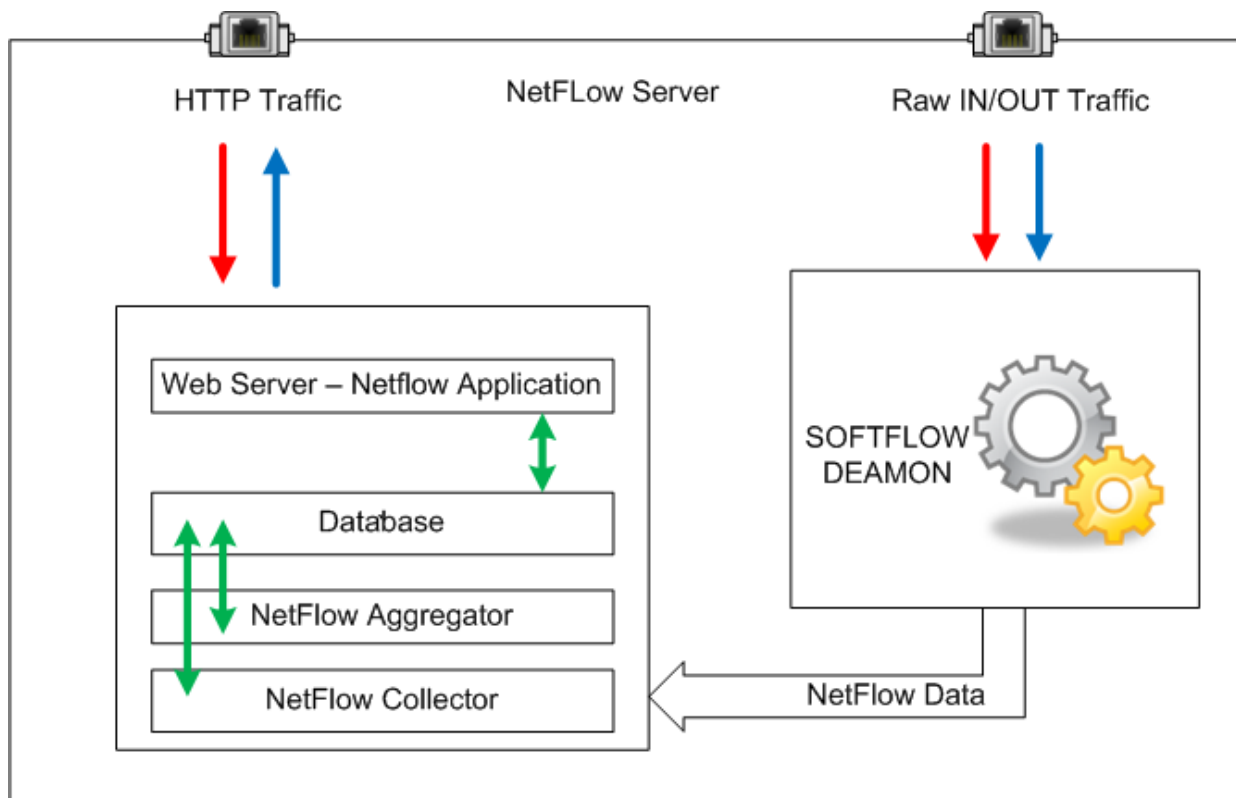
- Dodatni server (desktop pc).
- Dve NIC kartice.
- Dva porta na sviču.
- Gubi se informacija o IN/OUT portovima.



Netflow Sonda – Port mirroring zahtevi!

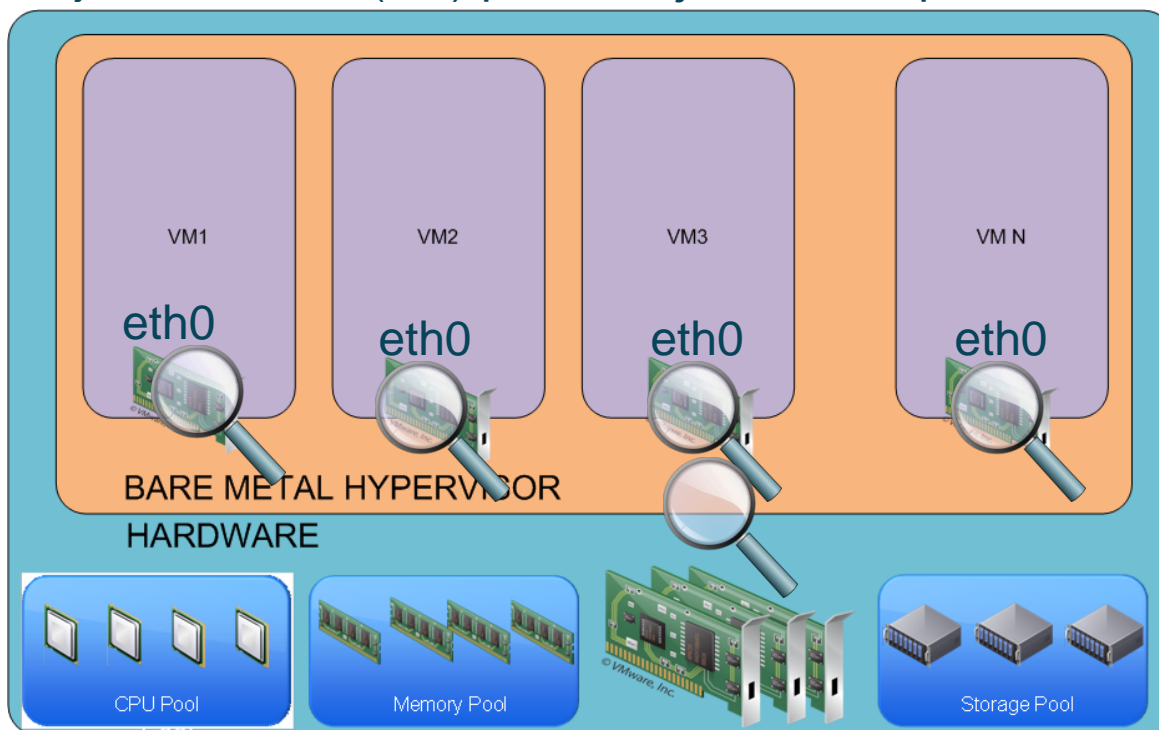


- Institucija koja je na L2 segmentu.

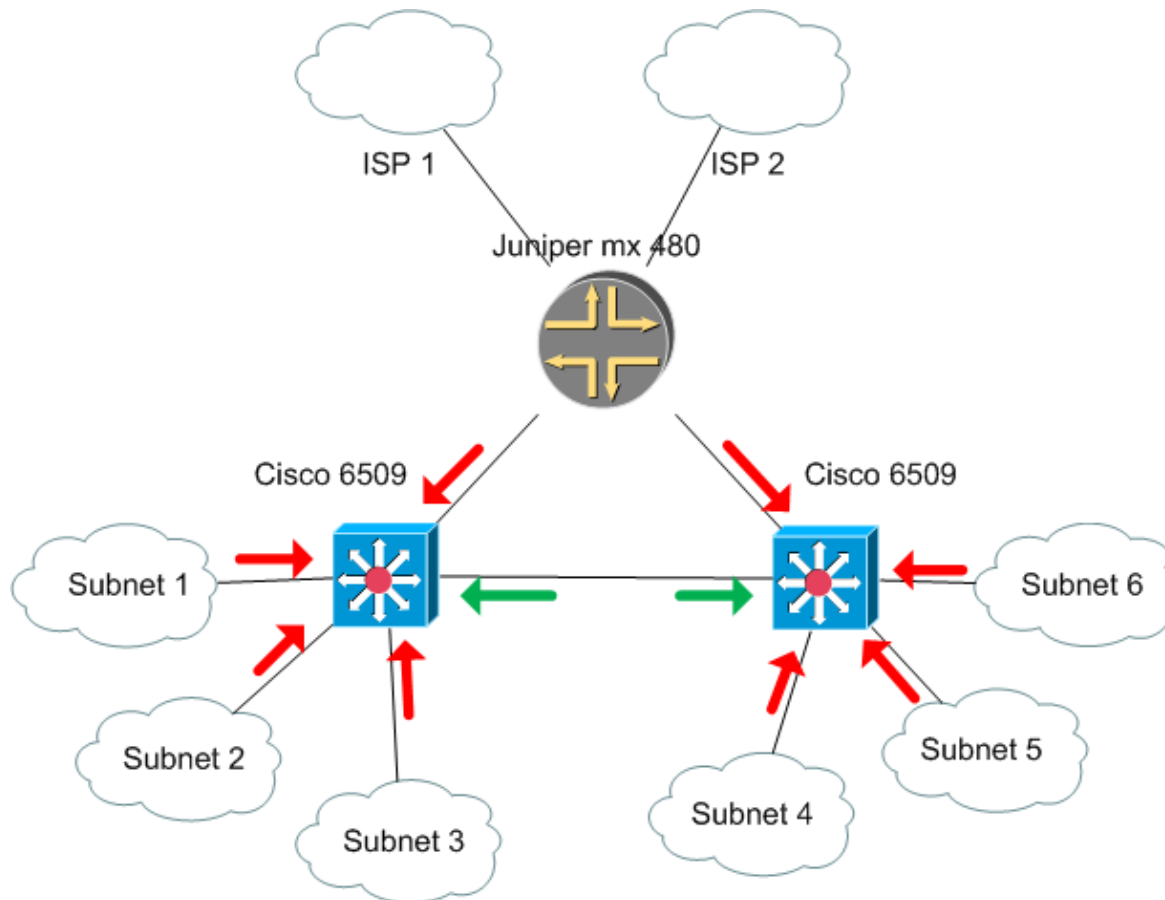


NetFlow Sonde – Virtuelizacija

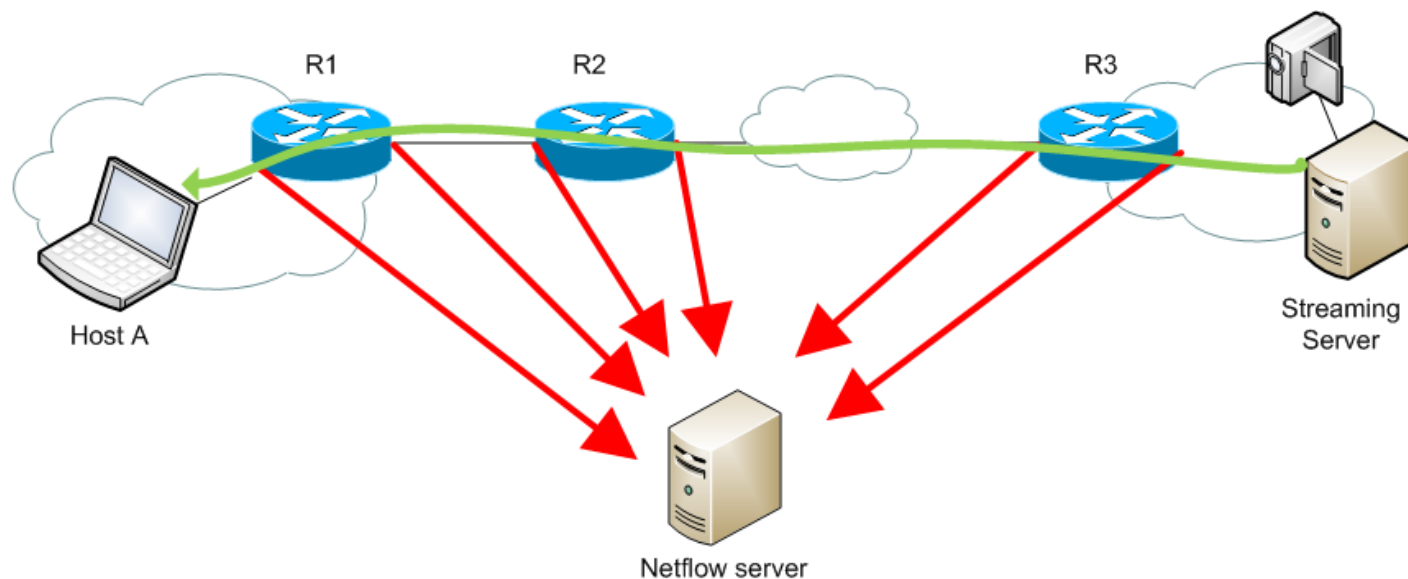
- Testirano na Citrix XenServeru
- Starije verzije VmWare-a (3.5) podržavaju NetFlow protokol.



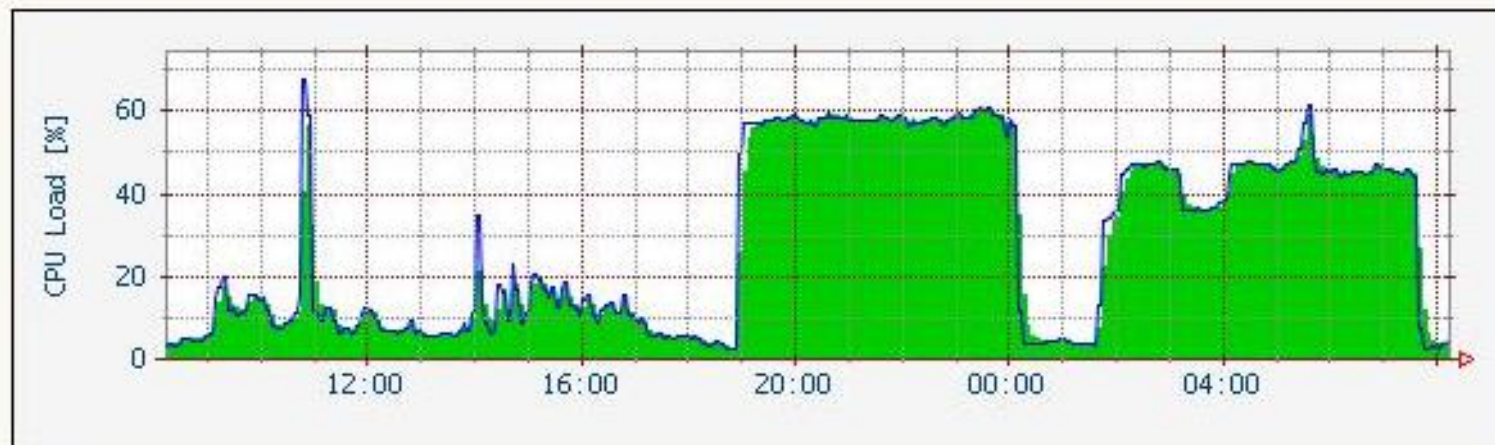
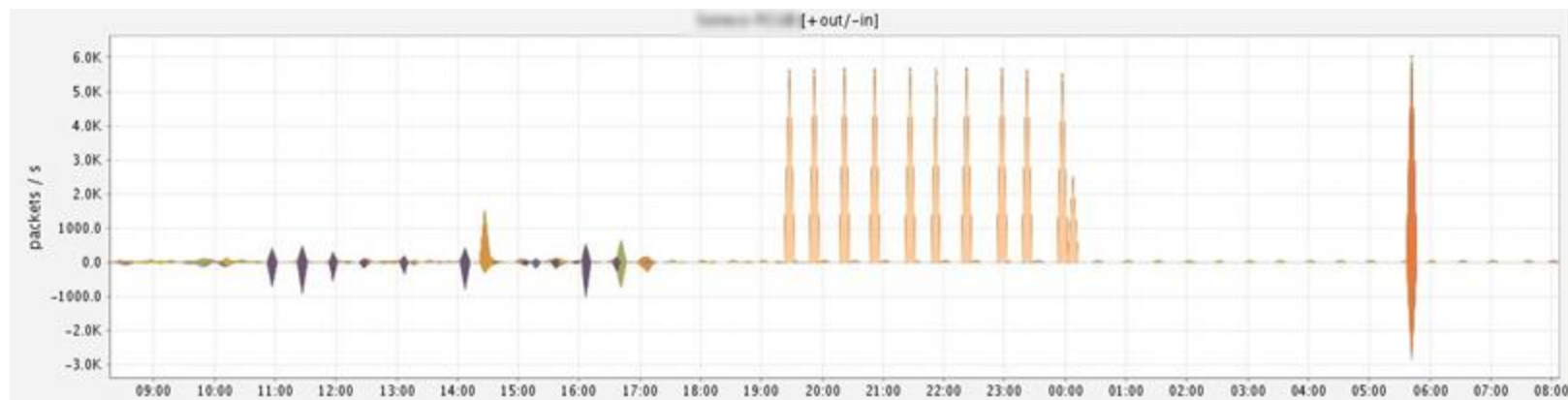
AMRES konfiguracija



- Raste popularnost novih NetFlow rekorda
- Cisco je počeo da koristi dodatna NetFlow polja za media saobraćaj
 - (Cisco -Medianet)
- NetFlow media rekordi: packet delay, packet loss, jitter...



Analiza sigurnosti u mreži - I



Analiza sigurnosti u mreži - I



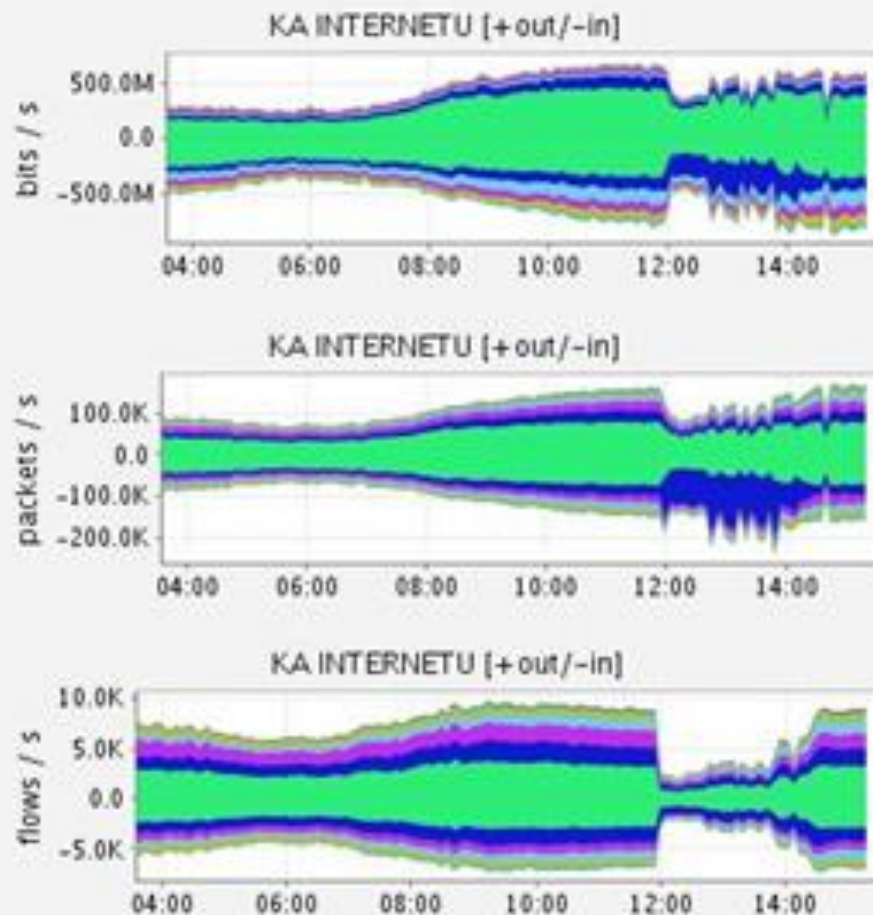
ICmyNet.Flow Home Page | My Account | About | Logout x
Ivan Ivanovic (vkrzee)

request previous next close

No.	Date / Time		Source		Destination		Protocol			Counters					
			<input type="checkbox"/> Bi-direct <input type="checkbox"/> IP	Port	IP	Port	Number	TOS	Flags	Flows	Packets	Bytes	Throughput	Seconds	IP
1	11-11-2010	23:31:45	172.16.14.19	---	172.16.0.4	POP3	TCP	0	---	14	1,682,893	87,509,916	388.9 Kbps	2331	
2	11-11-2010	23:57:50	172.16.14.19	SIP	172.16.0.4	POP3	TCP	0	A	24	62	44,755	1.4 Kbps	782	
3	11-11-2010	23:58:10	172.16.14.19	---	172.16.0.4	---	---	0	---	9	222	15,896	4.2 Kbps	601	
4	12-11-2010	00:03:24	172.16.14.19	NFS-or-IIS	172.16.0.12	SNMP	UDP	0	A	1	4	424	188.4 bps	18	
5	12-11-2010	00:03:46	172.16.14.19	NFS-or-IIS	172.16.12.100	SNMP	UDP	0	A	2	2	212	-	0	

previous next close 1 - 5 of 5

Analiza sigurnosti u mreži - II



Analiza sigurnosti u mreži - II



Analiza sigurnosti u mreži - II



ICmyNet.Flow Home Page | My Account | About | Logout x
Ivan Ivanovic (ivkree)

request previous next close

No.	Date / Time		Source		Destination		Protocol			Counters					
			<input type="checkbox"/> Bi-direct <input checked="" type="checkbox"/> IP	Port	IP	Port	Number	TOS	Flags	Flows	Packets	Bytes	Throughput	Seconds	
1	08-02-2010	13:45:02		---		Half-Life	UDP	0	none	23,072	16,602,429	4,266,824,253	57.5 Mbps	594	195
2	08-02-2010	13:45:02		---		Half-Life	UDP	0	none				26.0 Mbps	597	195
3	08-02-2010	13:50:42		7130		Half-Life	UDP	0	none	1	69	3,174	423.0 bps	60	195
4	08-02-2010	13:50:24		---		Half-Life	UDP	0	none	6	8	368	98.0 bps	30	195
5	08-02-2010	13:53:39		32330		Half-Life	UDP	0	none	2	6	276	368.0 bps	6	195
6	08-02-2010	13:50:02		7130		Half-Life	UDP	0	none	1	2	92	-	0	195
7	08-02-2010	13:52:50		---		Half-Life	UDP	0	none	2	2	92	184.0 bps	4	195
8	08-02-2010	13:51:10		50177		Half-Life	UDP	0	none	2	2	92	36.0 bps	20	195
9	08-02-2010	13:54:32		3139		Half-Life	UDP	0	none	1	1	53	-	0	195
10	08-02-2010	13:50:10		1454		Half-Life	UDP	0	none	1	1	46	-	0	195

KRAJ