NetFlow

Predmet: Mrežni servisi

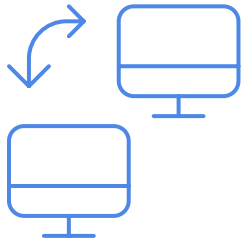
Predavač: dr Dušan Stefanović

Netflow servis

NetFlow je **protokol razvijen od strane Cisco kompanije** koji omogućava prikupljanje i analizu informacija o mrežnom saobraćaju.

Analiza mrežnog saobraćaja

Pruža sumarne statistike o TCP/IP tokovima (flows)



Tok (flow)

Sesija komunikacije između krajnjih tačaka.

DEFINICIJA TOKA

Flow - jednosmerni niz paketa koji imaju iste karakteristike:

- Izvorna IP adresa
- Odredišna IP adresa
- Izvorni port
- Odredišni port
- Protokol
- TOS
- Ulazni interfejs na ruteru

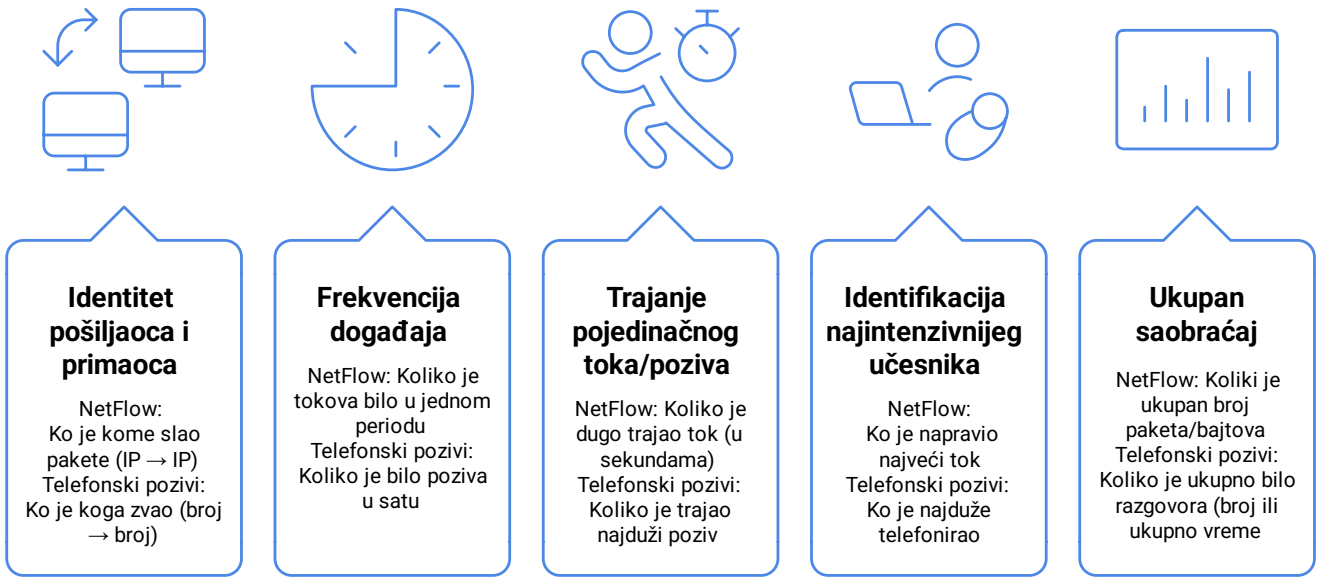
NetFlow agregira pakete iz flow-a

Merenje Toka

- Broj paketa
- Ukupna količina bajtova
- Vreme početka i završetka toka

Analogija netflow servisa i telefonskog poziva

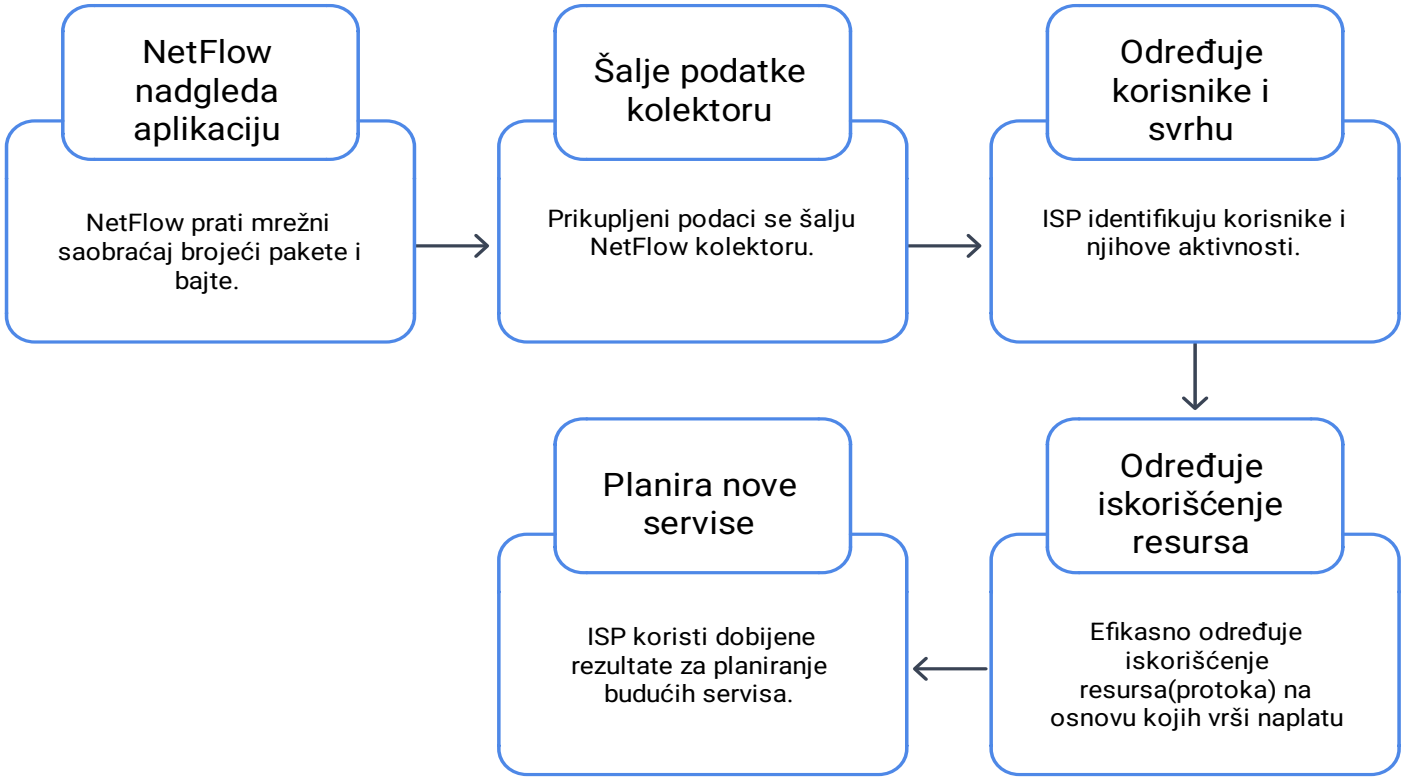
NetFlow ne čita sadržaj komunikacije – **ne "prisluškuje"** – već **beleži metapodatke o komunikaciji**, kao što je:
Ko, **kada**, **koliko dugo**, **koliko podataka**.



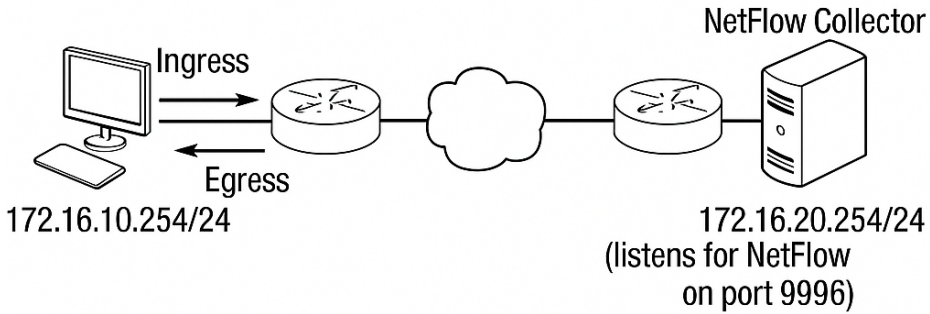
Osobine Netflow servisa

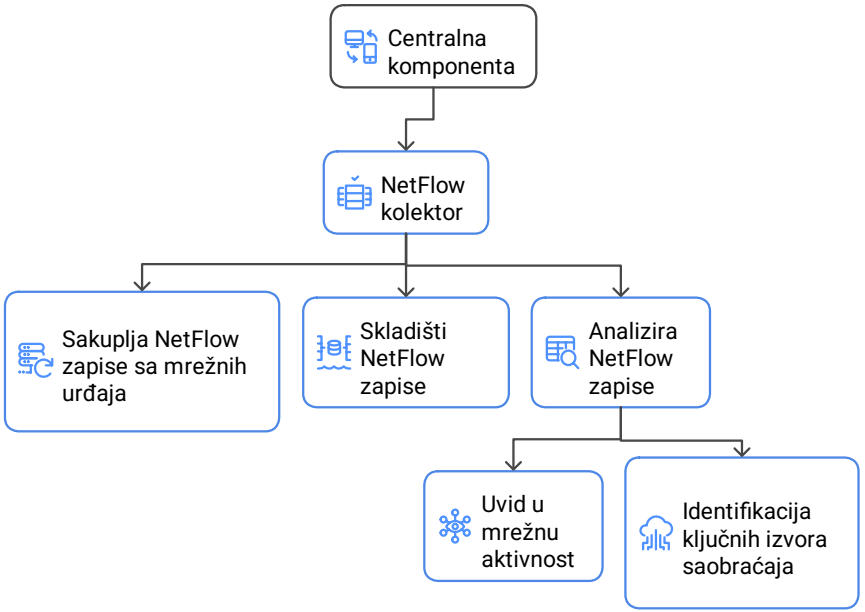
- Paket sniffer (wireshark) je ekvivaletan snimanju poziva na telefonu
- SNMP je protokol za upravljanje mrežom
- Netflow je protokol koji prati TCP/IP tokove (flows)
- Netflow je ekvivaletan praćenju statistike poziva na telefonu
    - Ko je koga zvao
    - Koliko poziva je bilo u jednom satu
    - Koliko je najduži poziv trajao
    - Ko je napravio najduži poziv
    - Koliko je ukupno poziva bilo

Osobine Netflow servisa



Netflow Kolektor





Netflow Kolektor – ključne mogućnosti analize

Identifikacija najaktivnijih korisnika

NetFlow kolektor prikazuje:
Top Talkers / Top Listeners:
Ko najviše šalje saobraćaj (top talkers),
Ko najviše prima podatke (top listeners),
Po kojim protokolima se ostvaruje najveći saobraćaj (top protocols).

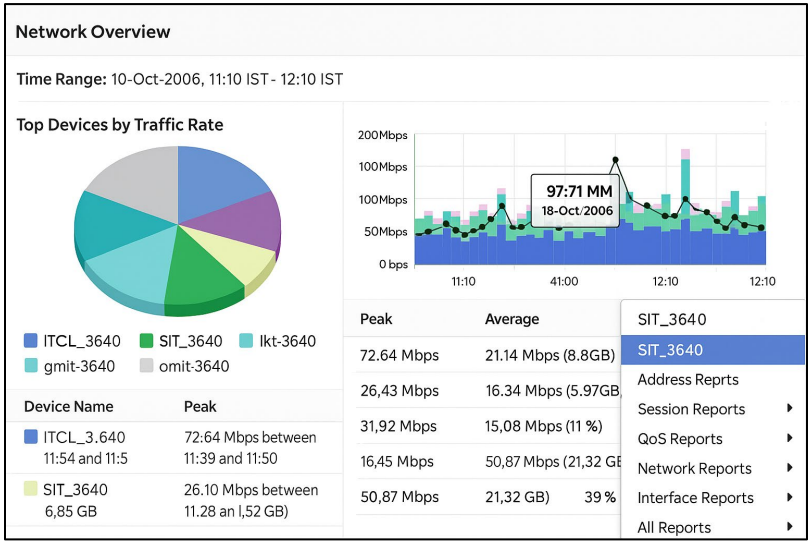
Praćenje web sajtova

Analizom odredišnih IP adresa i domena kolektor može prikazati:
Najčešće posećene web stranice,
Vremenske obrasce pristupa sadržaju,
Tip sadržaja (video, društvene mreže, cloud servisi).

Otkrivanje prekomernog saobraćaja

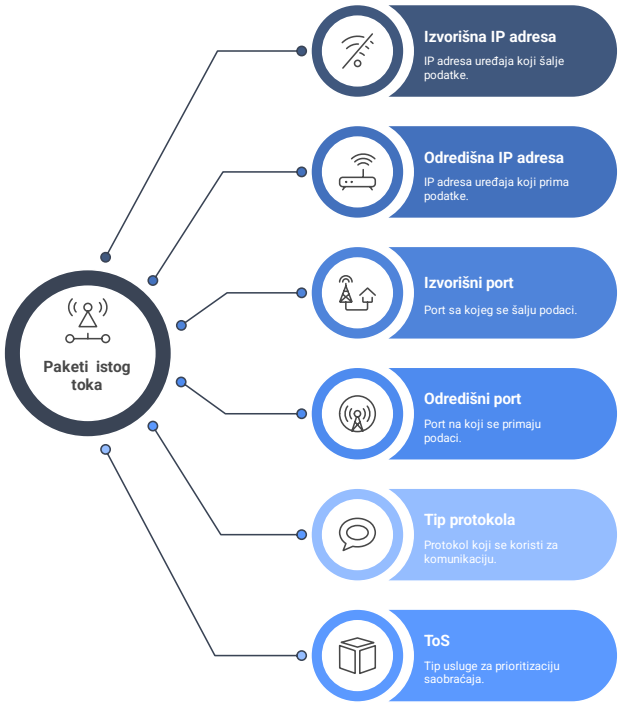
Kolektor identifikuje korisnike koji:
Generišu najveći ukupan saobraćaj,
Prekoračuju zadate limite bandwidth-a,
Učestalo otvaraju mnogobrojne TCP/UDP konekcije.

NetFlow dashboard – pregled protoka po uređajima



Device Name	Peak Traffic (Mbps)	Average Traffic (Mbps / GB)	Traffic Share (%)
ITCL_3640	72.64 (11:46 - 11:47)	21.14 / 8.86	15%
SIT_3640	26.43 (11:39 - 11:50)	16.34 / 6.85	12%
lkt-3640	26.10 (11:20 - 11:25)	15.08 / 5.97	11%
DKIT_3640	21.92 (11:33 - 11:44)	15.06 / 5.96	11%
gmit-3640	16.45 (11:11 - 11:20)	15.09 / 6.43	11%
Others	150.09 (11:54 - 11:55)	50.87 / 21.32	39%

Karakteristike toka (Flow)



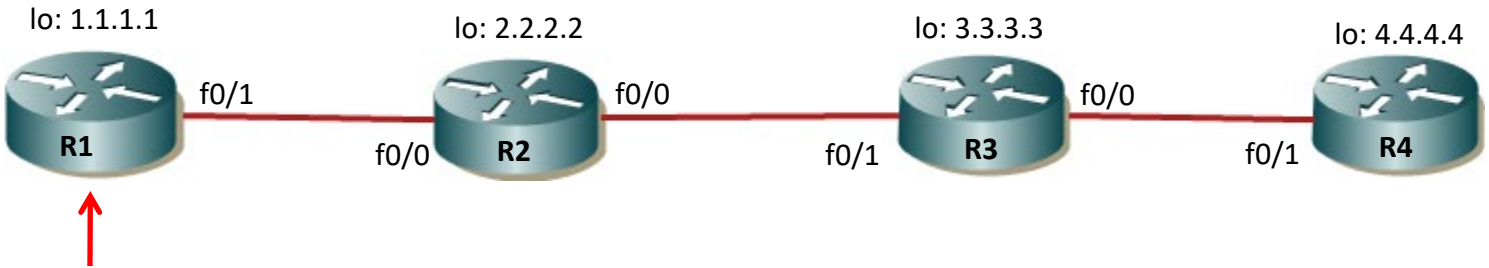
Flow čine paketi ili frejmovi koji imaju zajedničke atribute

Tok (eng. flow) je jednosmerna komunikacija između dva uređaja

Flow je **aktivan** ukoliko se paketi tog toka još uvek šalju

Flow je **neaktivan** ukoliko se slanje paketa istog toka završilo

Karakteristike toka (Flow)



R1# ping 4.4.4.4 source 1.1.1.1 repeat 500 size 1000

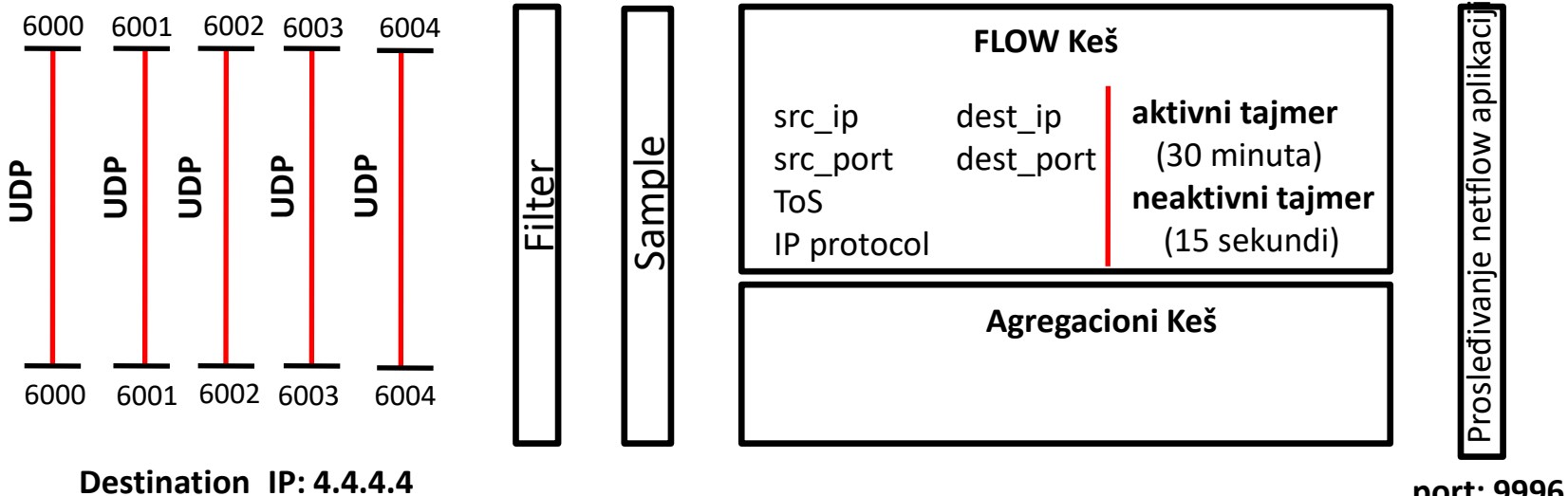
Flow čine paketi ili frejmovi koji imaju zajedničke atribute

Tok (eng. flow) je jednosmera komunikacija između dva uređaja

Kreirali smo dva toka (flow)

- flow od R1 ka R4
- flow od R4 ka R1

Source_IP: 1.1.1.1

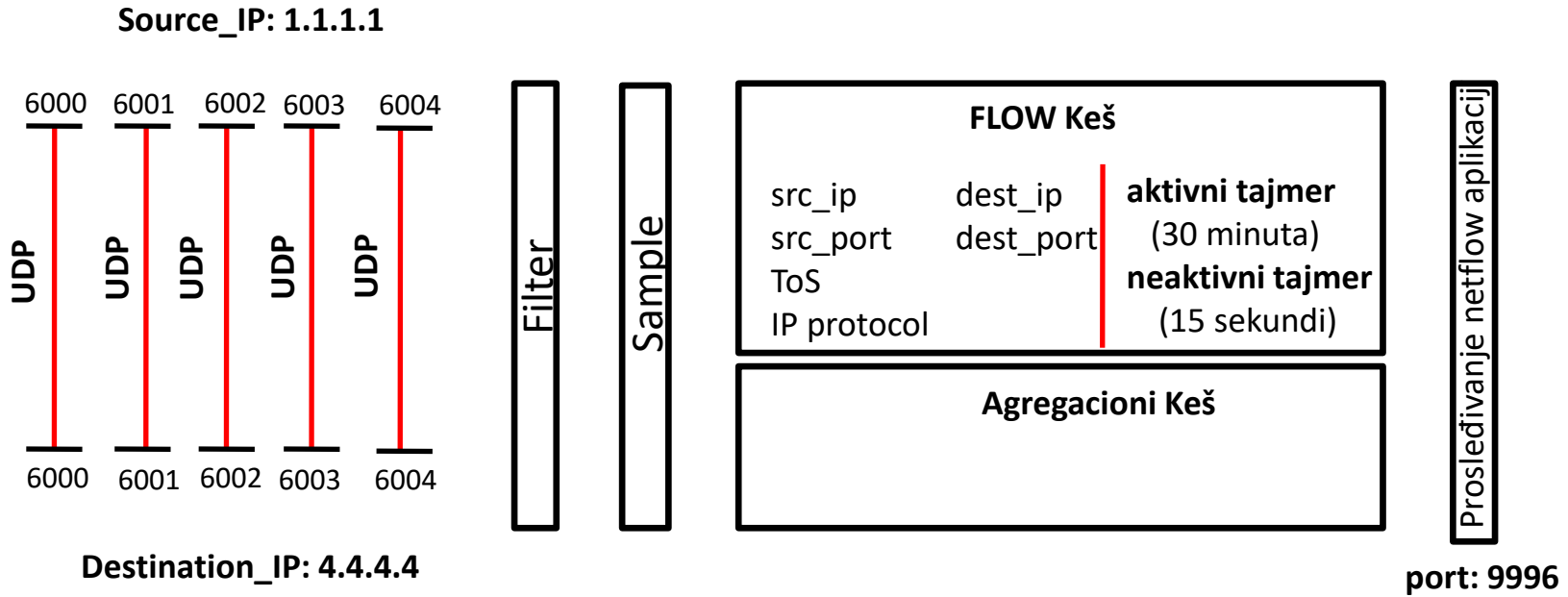


Destination_IP: 4.4.4.4

port: 9996

Na ruteru R1 kreiraju se 5 UDP toka ka ruteru R4

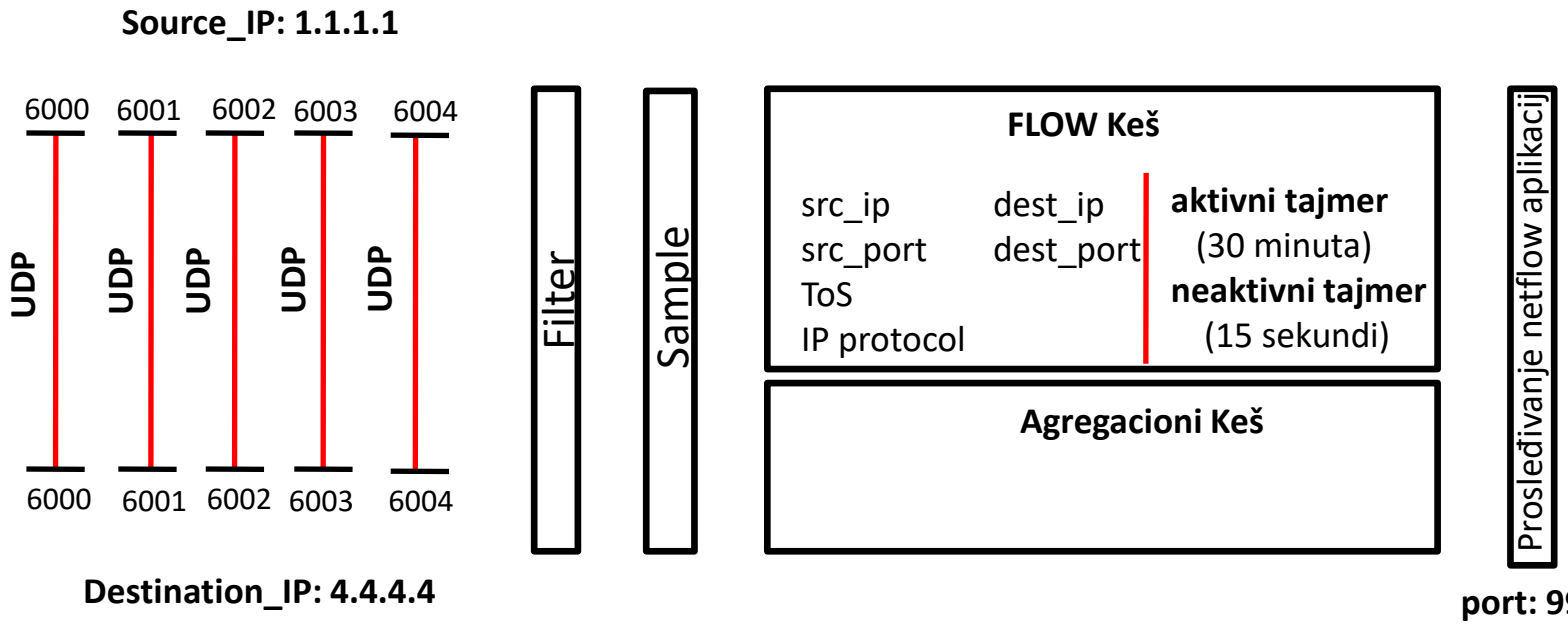
Netflow je konfigurisan na interfejsu f0/0 rutera R2 u dolaznom smeru



Flow keš koji je kreiran na ruteru R2 sadrži svaki flow

Podaci se iz flow keša nakon isteka tajmera (aktivni ili neaktivni) šalju netflow analajzeru

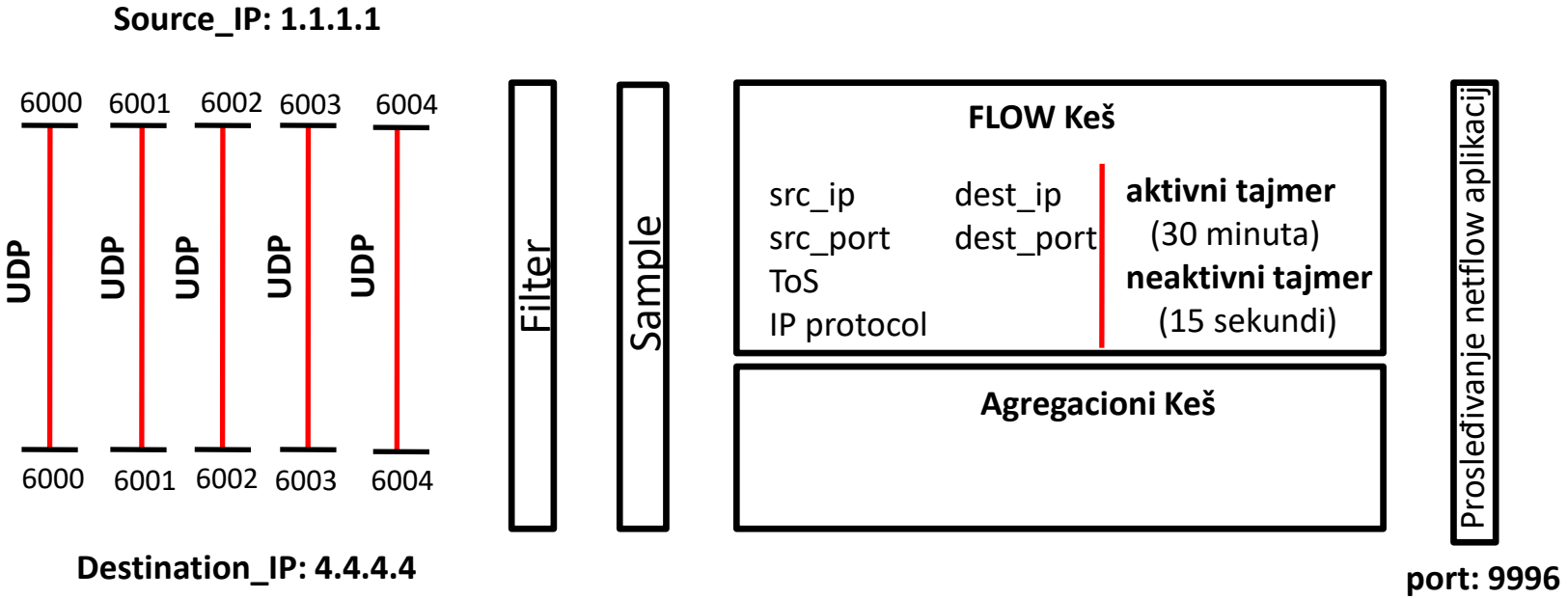
Aktivni tajmer je podešen na 30 minuta, dok je neaktivni tajmer podešen na 15 sekundi



Ukoliko je tok aktivan više sati (replikacija baze), na svakih 30 minuta se podaci za taj tok iz flow keša šalju netflow analajzeru

Tu se nalaze podaci o broju paketa koji su u jednom smeru prošli kroz taj interfejs

To je razlog zbog čega se za neke tokove čeka duže vreme da budu poslati netflow analajzeru



Neaktivni tok je tok koji kratko traje (bursty)

Podaci se 15 sekundi nakon prestanka aktivnosti šalju netflow analajzeru

Konfiguracija

R2(config)# ip flow-export destination 192.168.1.10 9996 udp

R2(config)# ip flow-export version 9

Verzija 9 uključuje sve što i verzija 5 plus MPLS i IPv6 informacije

R2(config)#ip flow-export source loopback 0

R2(config)#interface f0/0

R2(config-if)#ip flow ingress

R2#show ip flow interface

Prikaz interfejsa na kojima je instaliran NetFlow

R2#show ip cache flow

Prikazuje flow keš, lista tokove koji sadrže src interfejs, src ip, dest interfejs, dest ip, src port, dest port i broj paketa

R2#show ip flow export

Prikazuje šta se i gde se eksportuju podaci

Karakteristike toka (Flow)

Pošto je aktivni tajmer podešen na 30 minuta, što je prilično, da bi se podaci kolektoru češće slali, podesićemo tajmer na 1 minut

```
R2(config)# ip flow-cache timeout active 1
```

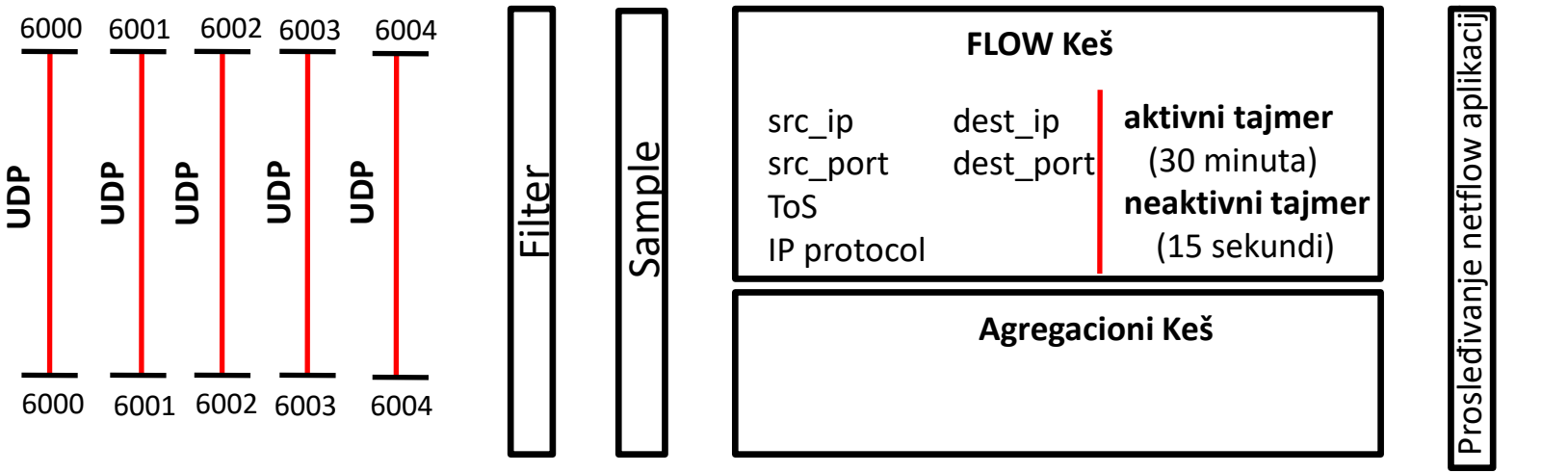
U produkcionoj mreži treba biti oprezan ukoliko aktivni tajmer podesimo na 1 minut jer će se velika količina sobraćaja slati netflow analajzeru

Svaki flow ima svoj aktivni tajmer, neće se svi istovremeno slati netflow analajzeru, što se može proveriti u Wiresharku

U Wiresharku je najlakše da uhvatimo Netflow paket:

Filter: udp.dstport==9996

Filter: cflow

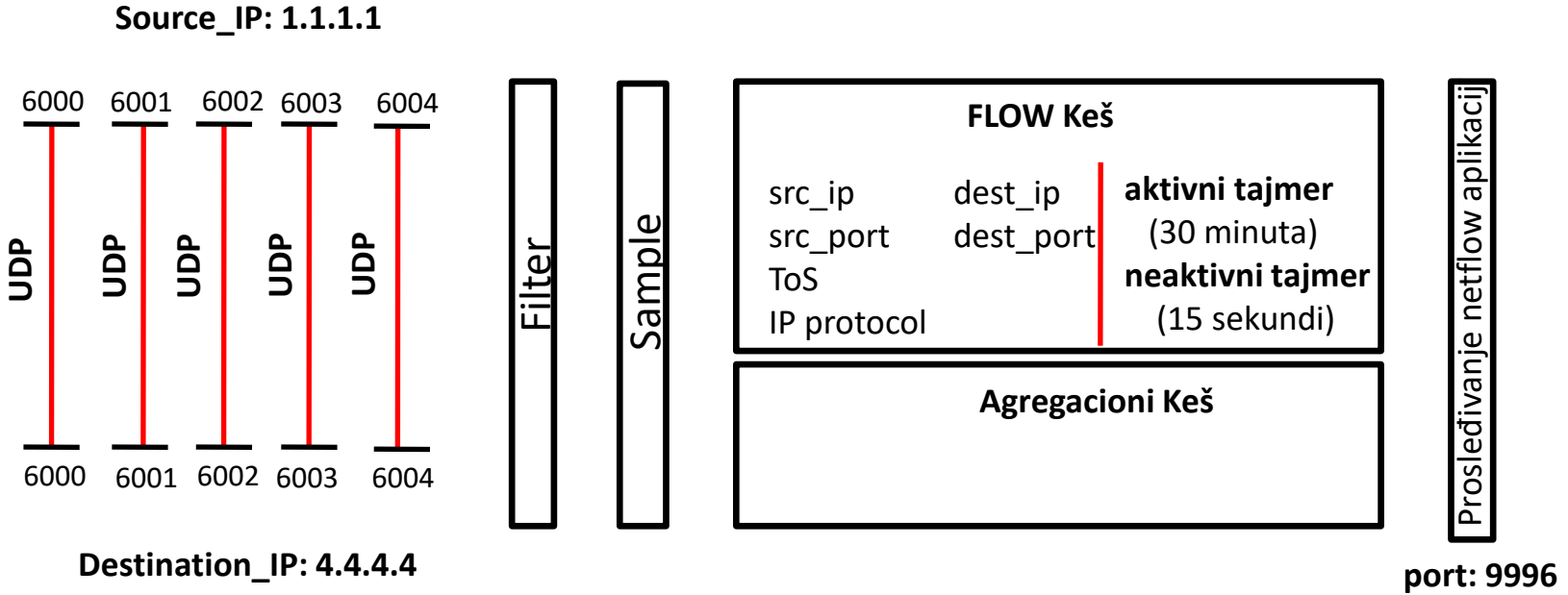


Na Cisco ruteru koristi se još jedan keš koji se zove Agregacioni keš

Agregaciju saobraćaja radi netflow aplikacija

- Agregacija kompletnog UDP saobraćaja
- Agregacija sobraćaja sa određene IP adrese

Agregaciju saobraćaja može da radi i netflow ruter

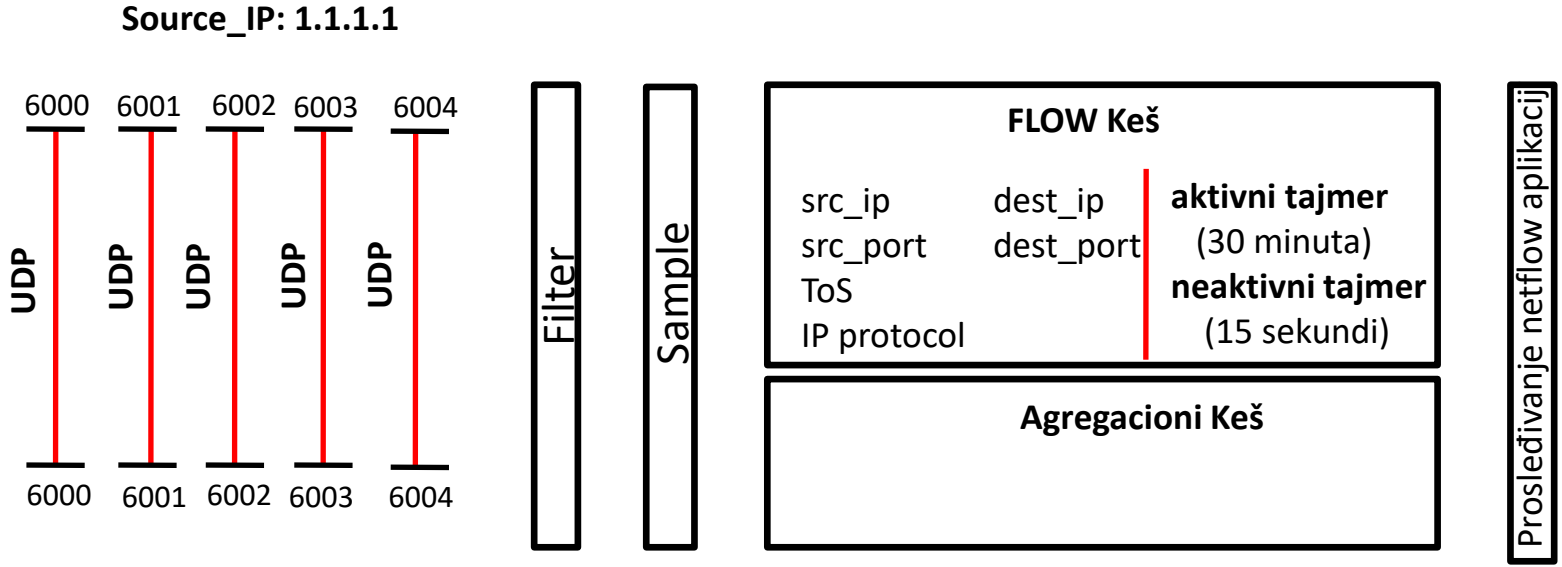


Ukoliko koristimo agregacioni keš, tokovi koji se nalaze u flow kešu nakon isteka aktivnog ili neaktivnog tajmera šalju se u agregacioni keš a odatle netflow aplikaciji

Može se podesiti da se flow iz flow keša prosleđuje i netflow aplikaciji i agregacionom kešu

Agregacioni keš ima svoje aktivne i neaktivne tajmere

Nakon isteka ovih tajmera tok se šalje netflow aplikaciji



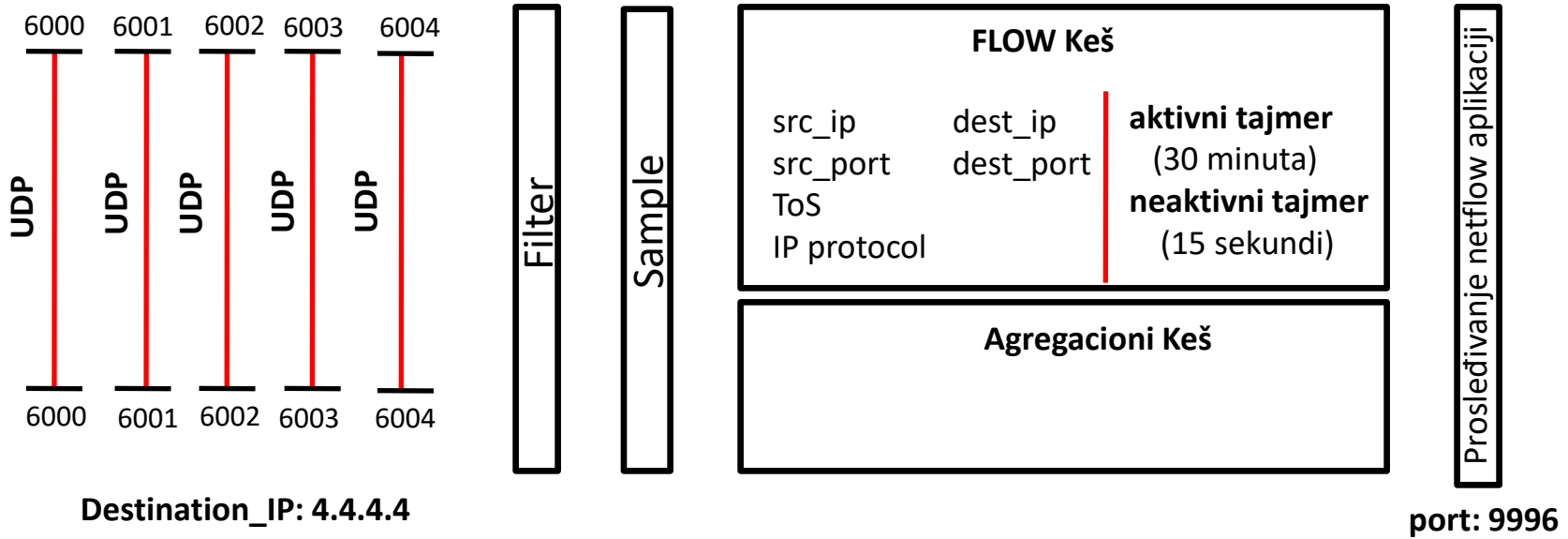

```
R2(config)# ip flow-agreggation cache
R2(config)# ip flow-agreggation cache protocol-port
R2(config-flow-cache)# export destination 192.168.1.10 9996
R2(config-flow-cache)# export version 9
R2(config-flow-cache)# cache timeout active 1
R2(config-flow-cache)# enabled
```

Ukoliko koristimo agregacioni keš, porebno je obrisati komande za kreiranje flow keša

Agregacioni keš

Prikaz agregacionog keša

R2# show ip cache flow agreggation protocol-port



Možemo da prikažemo samo status određenih tokova

Filtriranje tj. način filtriranja zavisi od semplovanja

Konfiguriše se flow sampler koji uzima uzorak, npr. 1 od 100 paketa i stavlja ga u flow keš

Sampler opcija se koristi za paćenje tokova koji su prošli na interfejsu a ne za detaljnu statistiku samog toka

Filter toka

```
R2(config)#ip flow-export destination 192.168.1.10 9996 udp
R2(config)#ip flow-export version 9
R2(config)#ip flow-cache timeout active 1

R2(config)#flow-sampler-map SAMP
R2(config-sampler)# mode random one-out-of 10

R2(config)#interface f0/0
R2(config-if)# flow-sampler SAMP

R2(config-if)#flow-sampler egress

R2# clear ip flow stats
```

Konfiguracija flow-sampler, bira slučajno 1 od 10 paketa

Omogućava semplovanje dolaznog flow na interfejsu

Omogućava semplovanje odlaznog flow na interfejsu

Brišemo flow statistiku