Upravaljanje mrežama

Uvod

- Životni ciklus mreže
- Praćanje i analiza rada mreže
  - "Tapovanje" mreže
  - SNMP
  - NetFlow
- Optimizacija rada mreže i kvalitet servisa
  - Kvalitet servisa
  - Uvođenje pravila i oblikovanje saobraćaja

Životni ciklus mreže

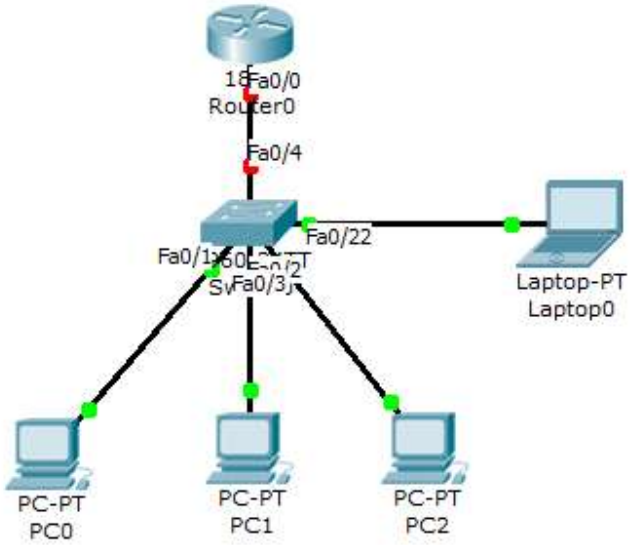
Praćenje i analiza rada mreže

Praćenje i analiza rada mreže

- Zbog **efekta koji stvara konvergercija** različitih tipova saobraća na istoj mreži i različitih zahteva po pogledu propusnog opsega različitih protokola, **subjektivni utisak** rada mreže može biti negativan, čak i u slučaju mreže velikog kapaciteta.
- Zbog toga je **neophodno konstantno pratiti** i analizirati rad mreže, i konstntno unapređivati mrežu kako bi se postigao bolji subjektivni utisak o radu mreže.
- Praćenje rada mreže **podrazumeva**:
  - Merenje realnog protoka na ključnim tačkama u mreži (najčešće izlaznim linkovima ka internetu i drugim mrežama)
  - Merenje parametara pojedinih protokola
  - Praćenje učestalosti eventualnih otkaza
- Analiza podrazumeva:
  - Analizu udela u ukupnom saobraćaju po
    - krajnjim uređajima
    - protokolima
    - tipovima saobraćaja
    - ...

Tapovanje mreže

- Tapovanje mreže je legitiman način za administratore da izvrše analizu saobraćaja tako što se svaki paket koji prođe kroz port koji se prati se kopira i na port swiča sa softverom za snimanje saobraćaja (korisnici ne primećuju promenu).
- "Tap" – eng. ispust
  - "tapuje" se obično izlazni link na svišu na neki uređaj koji može da snima i analizira saobraćaj
  - Na Cisco sviču ovo se postiže sa dve naredbe *monitor session*

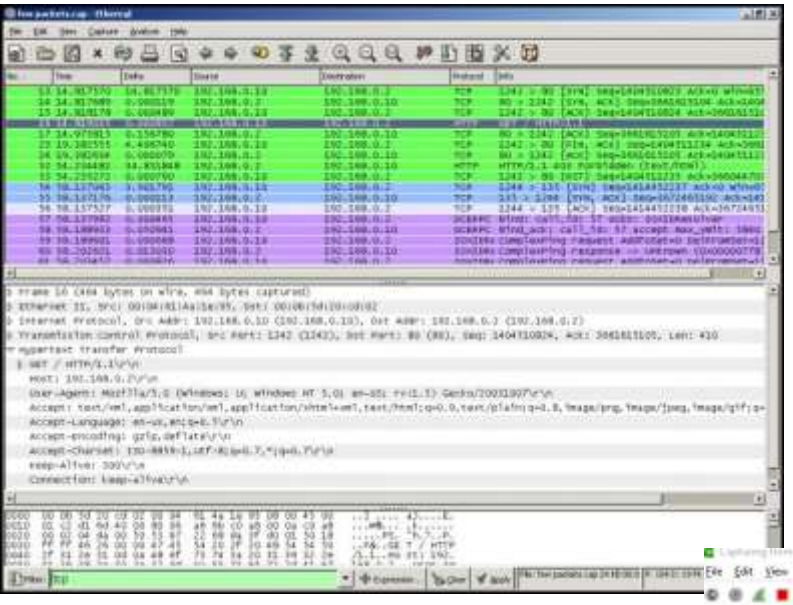


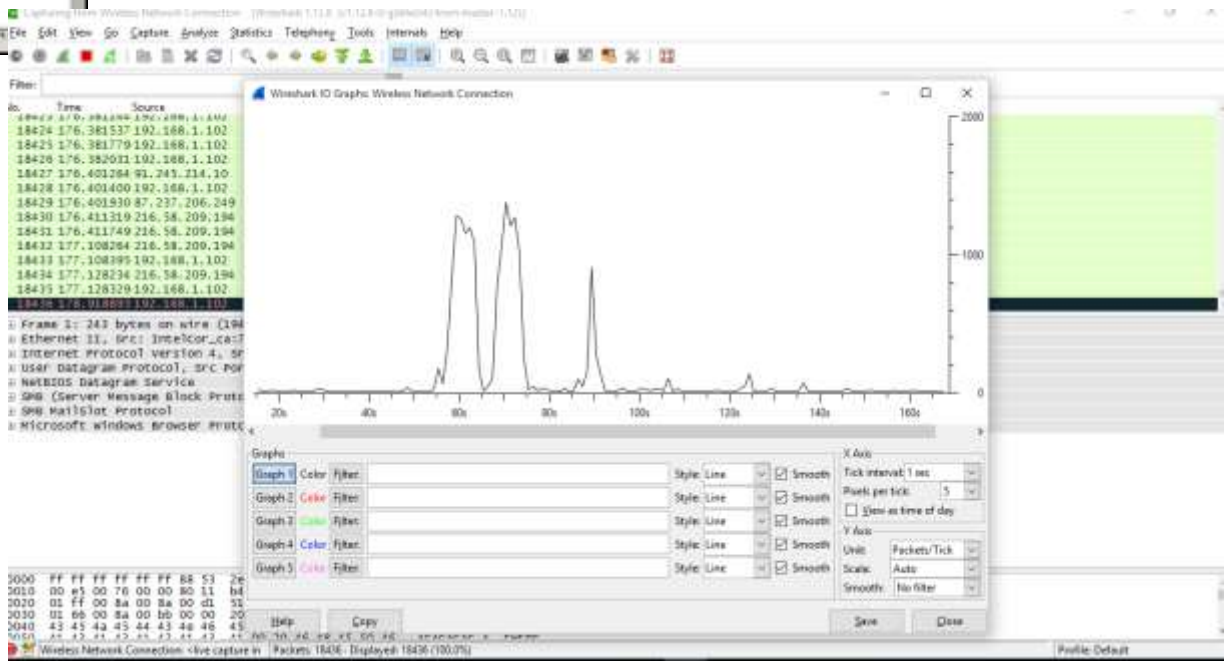

```
CiscoL3(config)#monitor session 1 source interface fastEthernet 0/1
CiscoL3(config)#monitor session 1 destination interface fastEthernet 0/22
```

Wireshark

- Računar (uređaj) na koji se preusmerava “tapovani” saobraćaj treba imati mogućnost snimanja i analize saobraćaja.
- Jedan od poznatijih programa za ovu namenu je Wireshark.
- Wireshark je open source softwer za PC računare koji snima kompletan saobraćaj na zadatoj mrežnoj kartici.
- Snimljeni saobraćaj se naknadno može analiziati iz ovog alata po mnogo osnova.

Wireshark



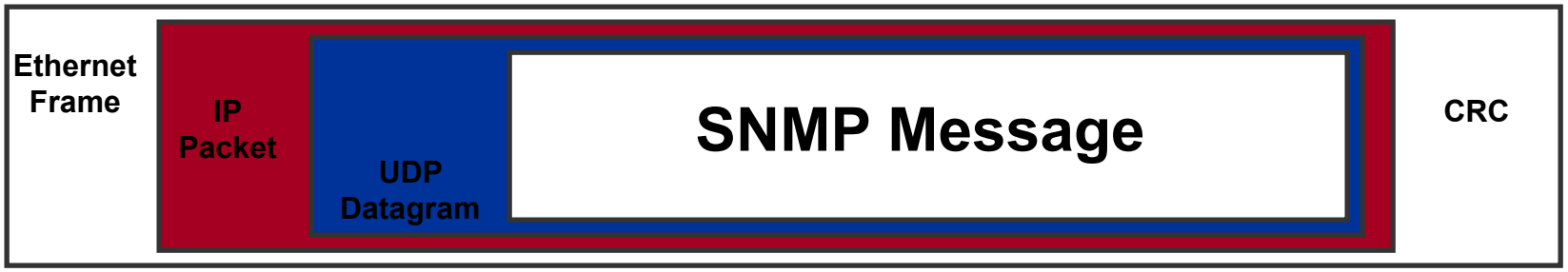


SNMP

- SNMP (Simple Network Management Protocol) je protokol koji omogućava prikupljanje informacija sa mrežnih uređaja i delimično upravljanje radom uređaja.
- SNMP protkolom se mogu prikupljati informacije **sa servera, radnih stanica, rutera, svičeva**, ...
- Za razliku od tapovanja mreže, **SNMP protokolom se salje samo sažetak informacija prikupljenih na uređajima**, a ne kompletan protok.
- **Komponente** SNMP sistema uključiju agente i menadžere
  - Agenti – softverski procesi koji se startuju na uređajima sa kojih se prikupljaju informacije i kojima se upravlja
  - Menadžeri – procesi koji se izršavaju na radnim stanicama pomoću kojih se upravlja mrežom. Uloga im je preriodično prikupljanje informacija.

SNMP

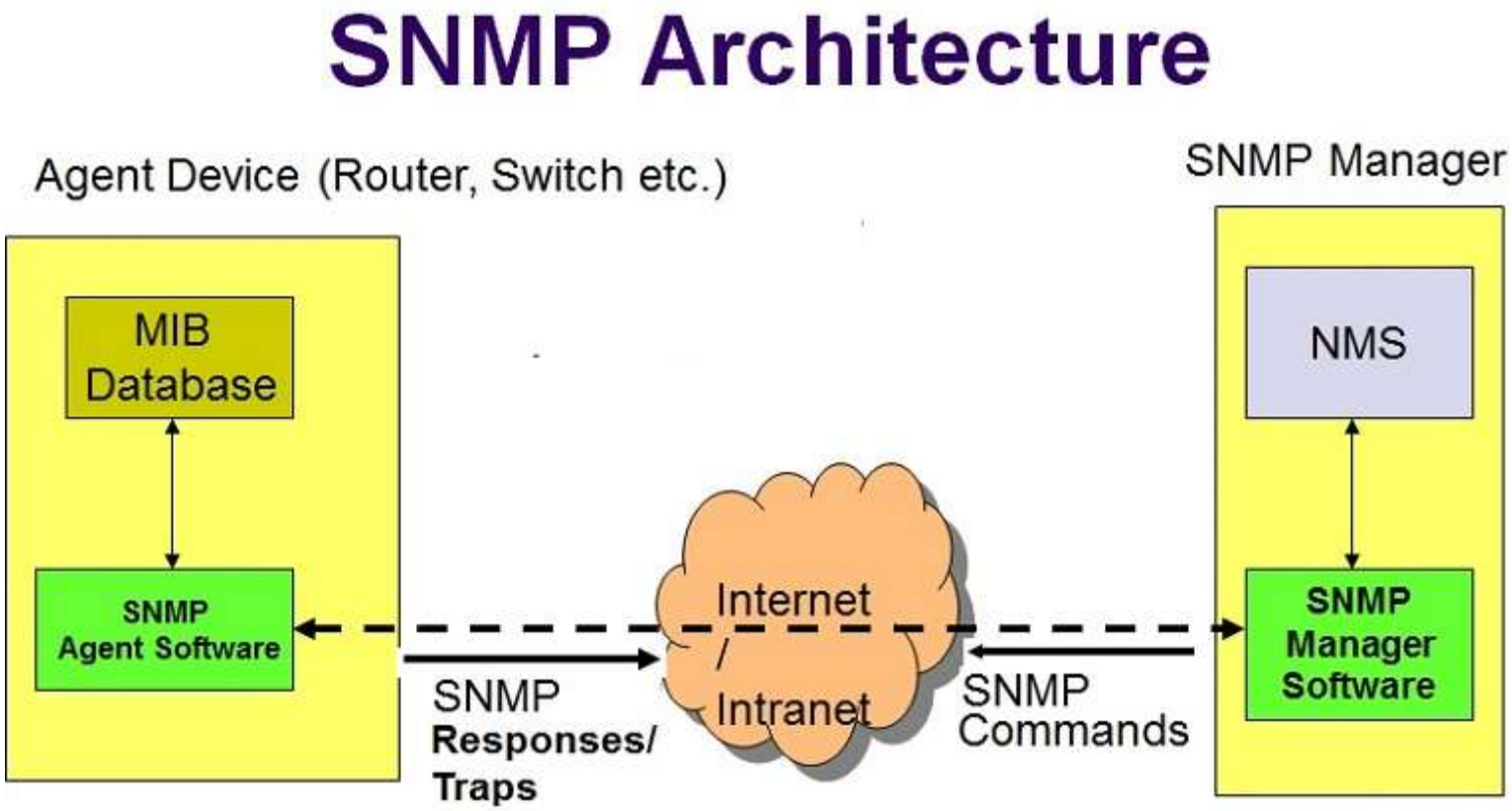
•SNMP koristi User Datagram Protocol (UDP) kao transportni mehanizam



•Portovi:

- **UDP Port 161** - SNMP Messages
- **UDP Port 162** - SNMP Trap Messages

SNMP arhitektura

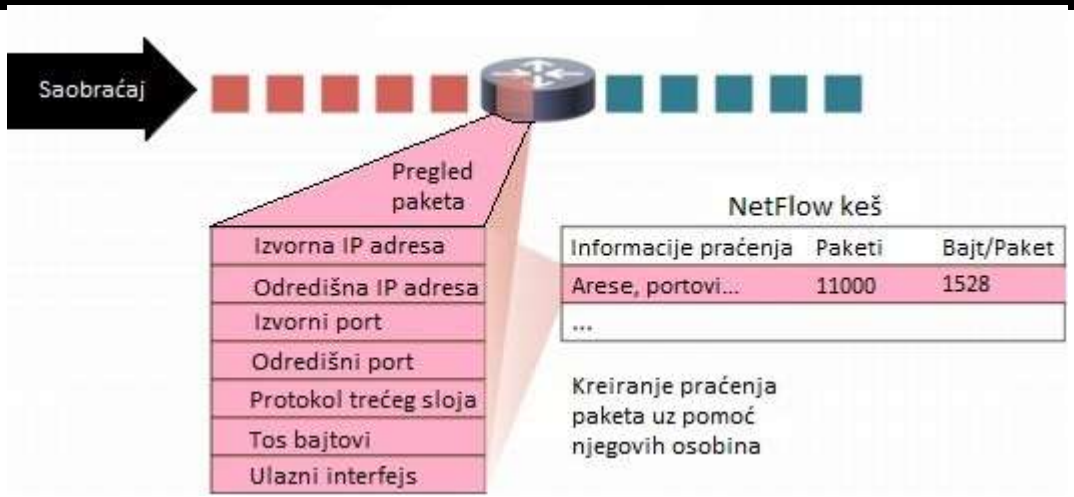


- Pojednostavljeno rečeno, MIB baza je “registar” numeričkih oznaka pojedinih parametara koje je moguće pratiti ovim protokolom.
- Svaka poruka sadrži MIB-oznaku parametra i samu vrednost parametra ili naredbu koju je potrebno izvršiti nad tim parametrom

NetFlow

- NetFlow je protokol aplikativnog nivoa koji za razliku od SNMP-a **nema mogućnost upravljanja mrežom**, već samo nadgledanja rada mreže.
- Svi paketi sa istog izvora ili odredišta, IP adrese, izvornog ili odredišnog porta interfejsa i klase servisa se **grupišu u "tokove"**.
- Tok predstavlja apstraktni pojam o kom se prikupljaju statistički podaci.
- Podaci o toku se pamte u **NetFlow keš**.
- Ceo postupak se obavlja na ruteru.

NetFlow



- Postoje dve glavne metode za pristup *NetFlow* podacima:
  - *show* naredbama iz komandne linije (*CLI*) na ruteru,
    - ***NetFlow CLI*** je veoma pogodan za brz uvid u protok i rešavanje problema.
  - korišćenje posebnih softverskih paketa koji prave izveštaje o podacima NetFlow-a na posebnim računarima.
    - Drugi izbor se naziva **eksportovanje NetFlow-a na server**.
- ***NetFlow* kolektor** je softver koji ima zadatak razumevanja eksportovanih praćenja i kombinovanje ili agregaciju podataka da proizvede važne izveštaje o saobraćaju i izveštaje o sigurnosnim analizama

NetFlow CLI

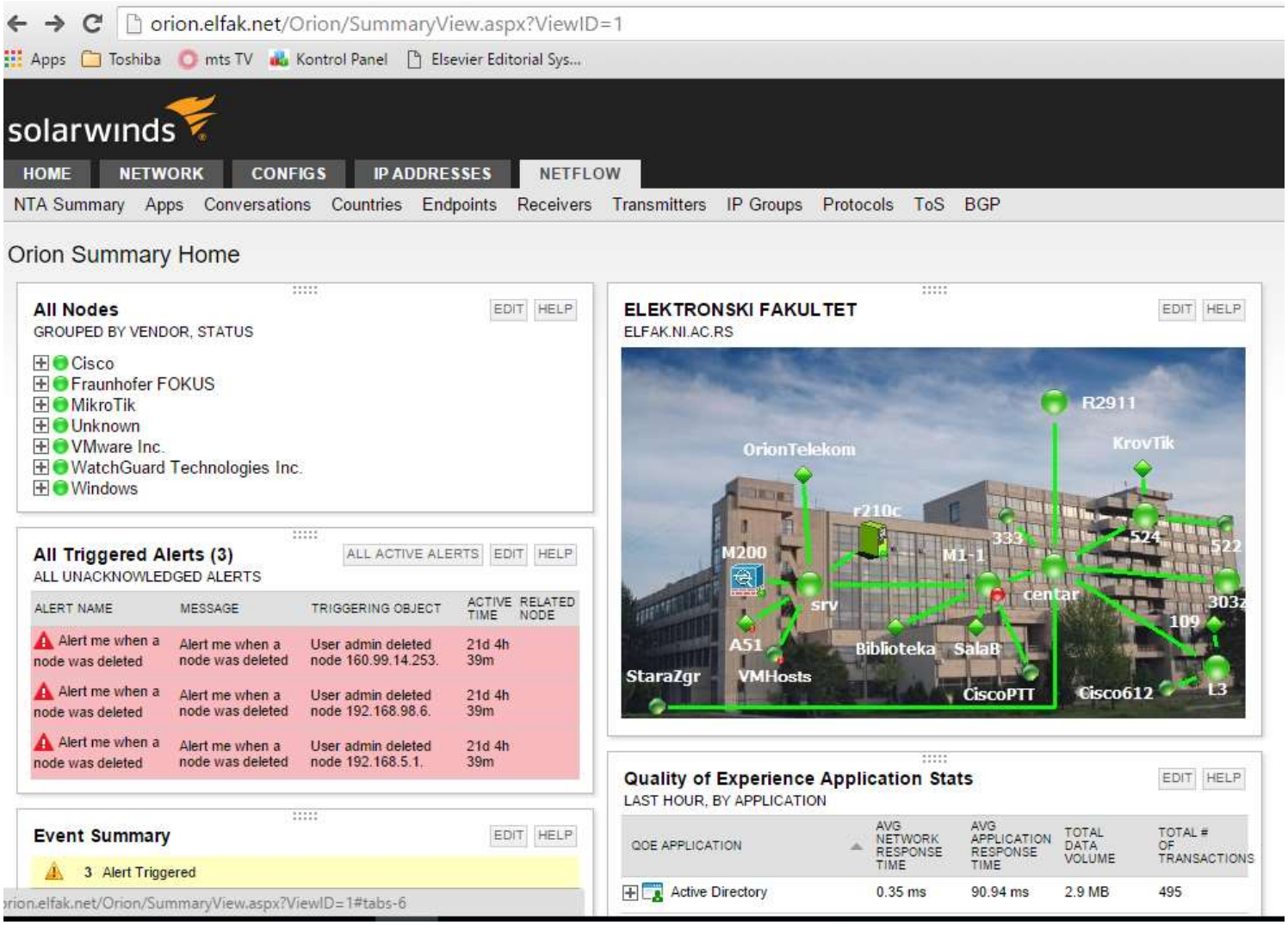
- router# show ip flow top 10 aggregate protocol
  - Ova naredba nam prikazuje 10 protokola koji trenutno teku kroz ruter.
- router# show ip flow top 10 aggregate source-address sorted-by packets
  - prikazuje IP adrese koje šalju najviše paketa.
- router# show ip flow interface
  - Prikazuje da li je saobraćaj na portu rutera ulazni (Ingress), ili izlazni (Egress).
- ...

Eksportovanje NetFlow podataka

- Komanda za podešavanje izvornog porta sa kog se prikuplja statistika o tokovima (zadaje se u interfejsu):
  - **ip flow-export source G0/1**
- Podešva se verzija NetFlow zaglavlja:
  - **ip flow-export version 9**
- Posle podešavanja verzije treba se odrediti odredište kom računaru se šalju NetFlow paketi kako bi se uspostavio monitoring na samom tom računaru
  - **ip flow-export destination {adress} {port}**
- **Eksportovanje NetFlow podataka je poželjno jer se više mrežnih uređaja može pratiti sa jednog računara.**

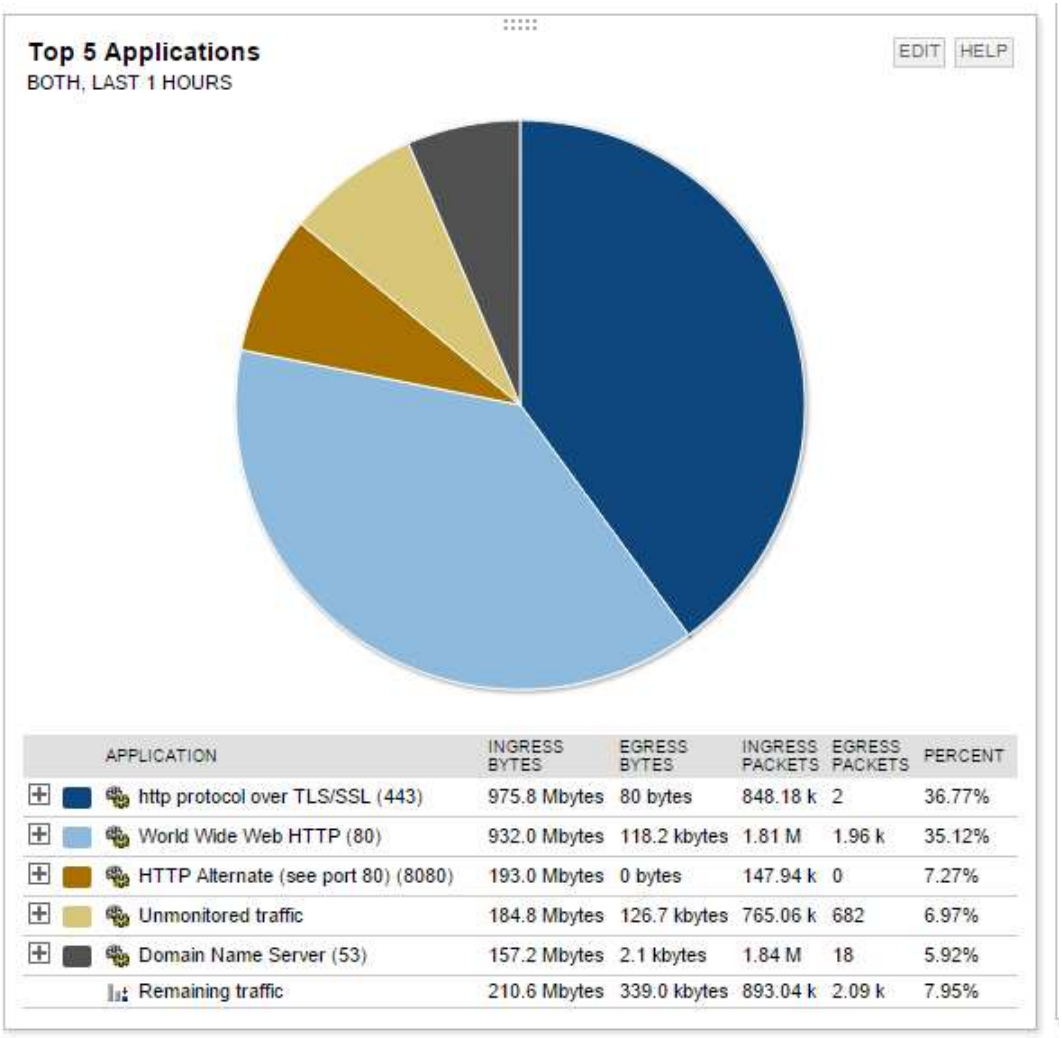
NetFlow serverske aplikacije

- Primer: Orion SolarWinds



NetFlow serverske aplikacije

- Primer: Orion SolarWinds



APPLICATION	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
http protocol over TLS/SSL (443)	975.8 Mbytes	80 bytes	848.18 k	2	36.77%
World Wide Web HTTP (80)	932.0 Mbytes	118.2 kbytes	1.81 M	1.96 k	35.12%
HTTP Alternate (see port 80) (8080)	193.0 Mbytes	0 bytes	147.94 k	0	7.27%
Unmonitored traffic	184.8 Mbytes	126.7 kbytes	765.06 k	682	6.97%
Domain Name Server (53)	157.2 Mbytes	2.1 kbytes	1.84 M	18	5.92%
Remaining traffic	210.6 Mbytes	339.0 kbytes	893.04 k	2.09 k	7.95%

Optimizacija rada mreže i kvalitet servisa

QoS – Quality of Service

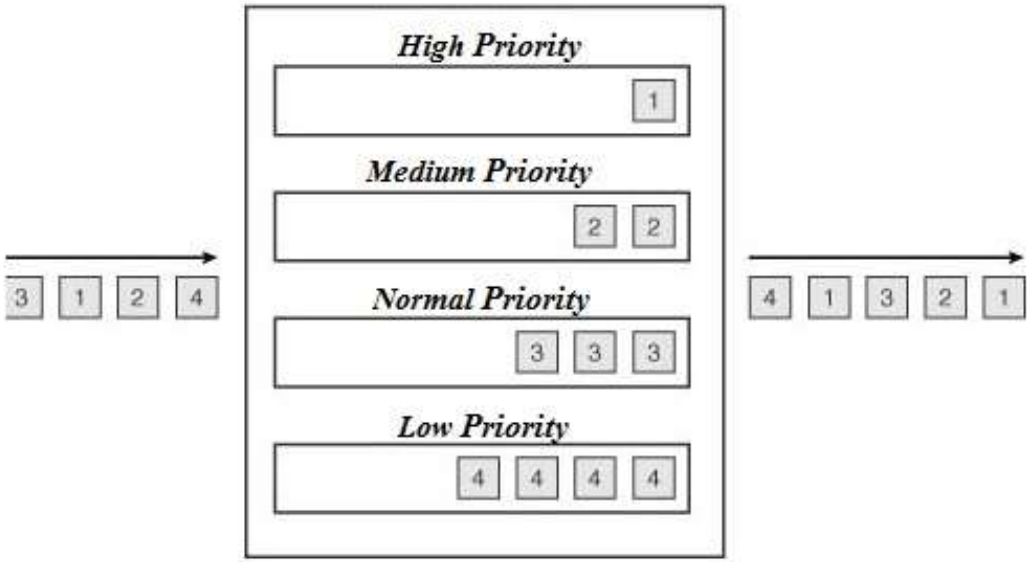
- Pod pojmom "kvalitetet servisa" **podrazumeva se subjektivni utis**ak rada mreže.
- Glavni problem sa subjektivnim utiskom u tome da su današnje mreže zapravo mreže **sa konvergiranim servisima**, odnosno preko iste mreže se prenosi saobraćaj istog tipa.
  - Na primer, na 100 MBps lokalnoj mreži, može da se desi da jedan korisnik downloaduje veliku količinu podataka i zauzima većinu propusnog opsega, pa je korisnicima koji koriste VoIP ili IPTV veza praktično neupotrebljiva.
- Kada se govori o kvalitetu servisa, podrazumeva se mreža čiji **se propusni opseg ne menja**, ali se vrše podešavanja tako da je subjektivni utisak korisnika takav da mreža "radi brže".
- S tim u vezi, u literaturi se obično sreće fraza: "QoS is **zero-sum game**"!
  - Ovo oslikava činjenicu da je propusni opseg konstantan i da bi se povećao kvalitet jednog servisa, mora se narušiti kvalitet nekog drugog servisa.

QoS – Quality of Service

- Načini za obezbeđivanje kvaliteta:
  - Davanje prioriteta različitim tipovima saobraćaja (Priority Queueing).
  - Oblikovanje saobraćaja zadavanjem pravila (Traffic Policing and Shaping)
  - Kombinacija prethodna dva.

Priority Queueing

- PQ se implementira sistemom sa četiri reda čekanja različitog prioriteta (high, medium, normal, low).
- Najpre se opslužuje red najvećeg prioriteta, a nakon toga se prelazi na opsluživanje ostalih, uz konstantnu proveru statusa reda najvišeg prioriteta.
- PQ ima za posledicu veoma malo kašnjenje u redovima većeg priorteta.



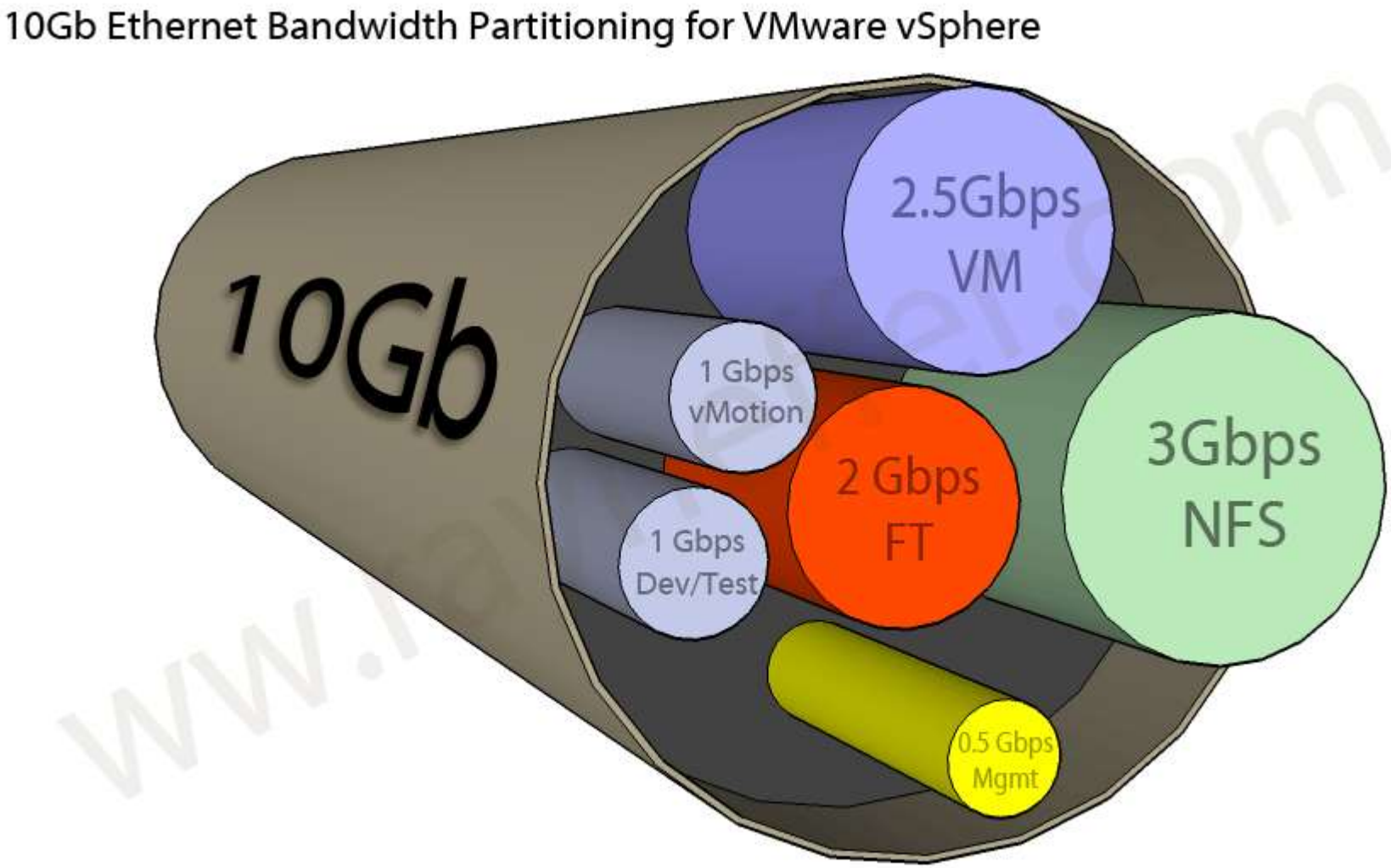
Primer

- Primer bez proiriteta:
  - Kroz 100 Mbps mrežu prolazi intenzivan download fajlova sa interneta od **99.9** Mbps i VoIP poziv od **0.1** Mbps.
  - Ukoliko **nisu zadati prioriteti**, uređaji ravnopravno prenose pakete:
    - na svakih 999 paketa downloada fajlova prenese se 1 paket VoIP-a.
    - Između svaka dva paketa VoIP-a u proseku ima 999 paketa f.transfera, pa je kašnjenje veliko, jer je velika verovatnoća da je bafer pun kada dođe paket VoIP-a, jitter je verovatno neprihvatljiv, pa je subjektivni utisak veoma loš, praktično je nemoguće komunicirati preko VoIP-a.
- Primer sa prioritetom:
  - Isto kao prethodno: kroz 100 Mbps mrežu prolazi intenzivan download fajlova sa interneta od **99.9** Mbps i VoIP poziv od **0.1** Mbps.
  - **Prioriteti su zadati** tako da čim dođe paket VoIP-a, odmah se prenosi, bez obzira da li ima paketa na čekanju drugih protokola
    - Efekat je takav da iz ugla VoIP servisa kašnjenje ne postoji – kao da nema drugog saobraćaja na mreži
    - Iz ugla downloada fajlova takođe nema razlike u subjektivnom utisku, jer je 0.1 Mbps beznačajno i ne može da "ugrozi" 99.9 Mbps koliko je ova aplikacija imala i u ovom i u prethodnom primeru.

Ograničavanje protoka i oblikovanje saobraćaja

- Izbegavanje zagušenja se može rešiti i tako što se određenim tipovima saobraćaja zada tačno definisani propusni opseg.
- To se rešava tako što kad dođe do zadatog maksimuma vrši odbacivanje datagrama koji su prekoračili zadatu kvotu za taj tip saobraćaja.
- Ovaj princip podrazumeva da se najveći deo saobraćaja prenosi preko *TCP* protokola. U tom slučaju će **namerno odbacivanje** paketa prouzrokovati da TCP smanji veličinu prozora, a samim tim i brzinu protoka.
- Datagrami se odbacuju sve dok se TCP ne "natera" da smanji brzinu na zadatu.
- Odbacivanje može biti softificiranije u slučaju kada se vodi računa o tome koji se paketi odbacuju.
- Jedno od rešenja je *WRED* (*Weighted Random Early Detection*).

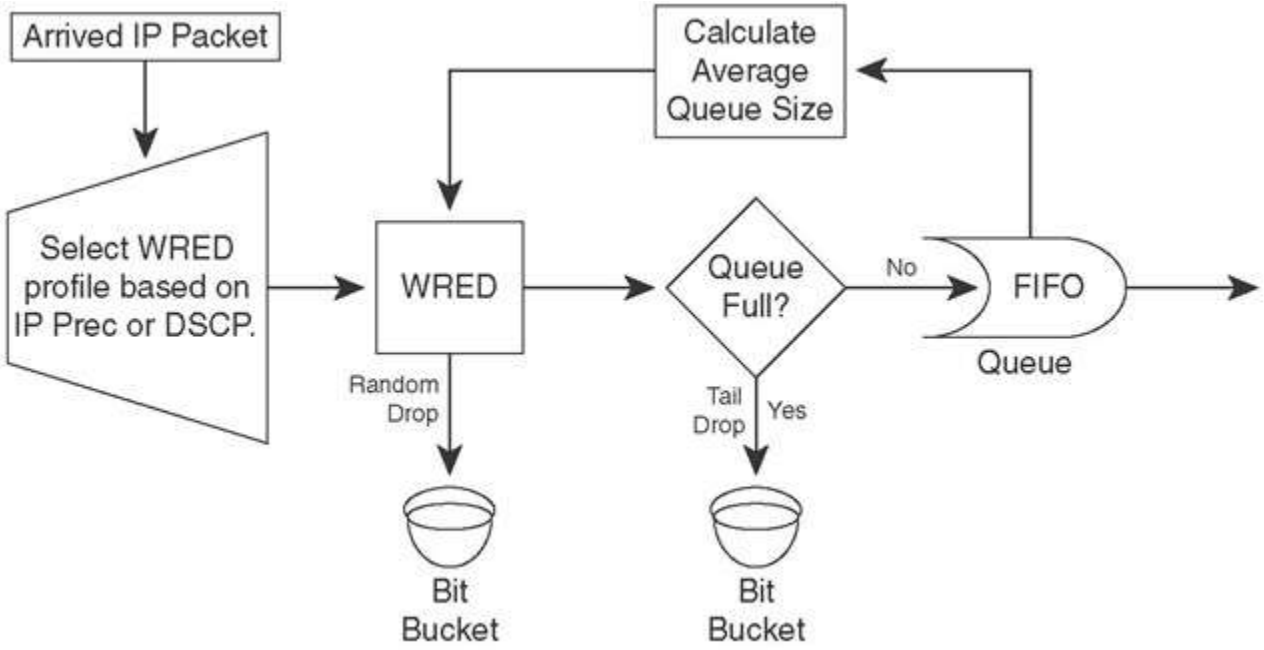
Ograničavanje protoka i oblikovanje saobraćaja

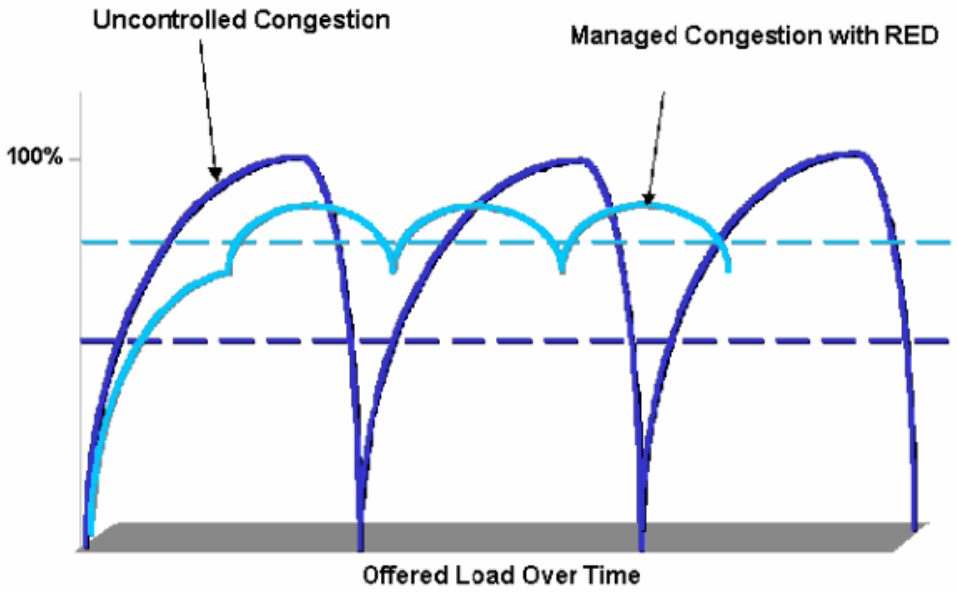


WRED

- WRED (Weighted Random Early Detection) je tehnika kod koje se:
  - Računa prosečna veličinu slobodnog mesta u redu/redovima.
  - Baferuje paket odmah, ako je prosečna veličina ispod minimalnog zadatog threshold-a.
  - Ako je prosečna veličina iznad trešholda paket se odmah odbacuje.
  - Ako je između minimuma i maksimuma, paket se odbacuje ili baferuje u zavisnosti od prethodne verovatnoće odbacivanja paketa tog tipa.
- Prosečna veličina slobodnog mesta u redu se računa po formuli:
  - $avg=o*(1-2^{-n})+c*(2^{-n})$
    - gde je n korisnički definisani težinski faktor, o je stari prosek (old), a c trenutni (current).

WRED


Arrived IP Packet
Calculate Average Queue Size
Select WRED profile based on IP Prec or DSCP.
WRED
Queue Full?
No
FIFO
Queue
Random Drop
Tail Drop
Yes
Bit Bucket
Bit Bucket


Uncontrolled Congestion
Managed Congestion with RED
100%
Offered Load Over Time

Klasifikacija saobraćaja

- Diferencijalni servisi ili DiffServ je mrežna arhitektura koja specifira jednostavan i skalabilan mehanizam za klasifikovanje i upravljanje mrežnim saobraćajem. Koristi:
  - Type of Service (ToS) i
  - Differentiated Services Code Point (DSCP)

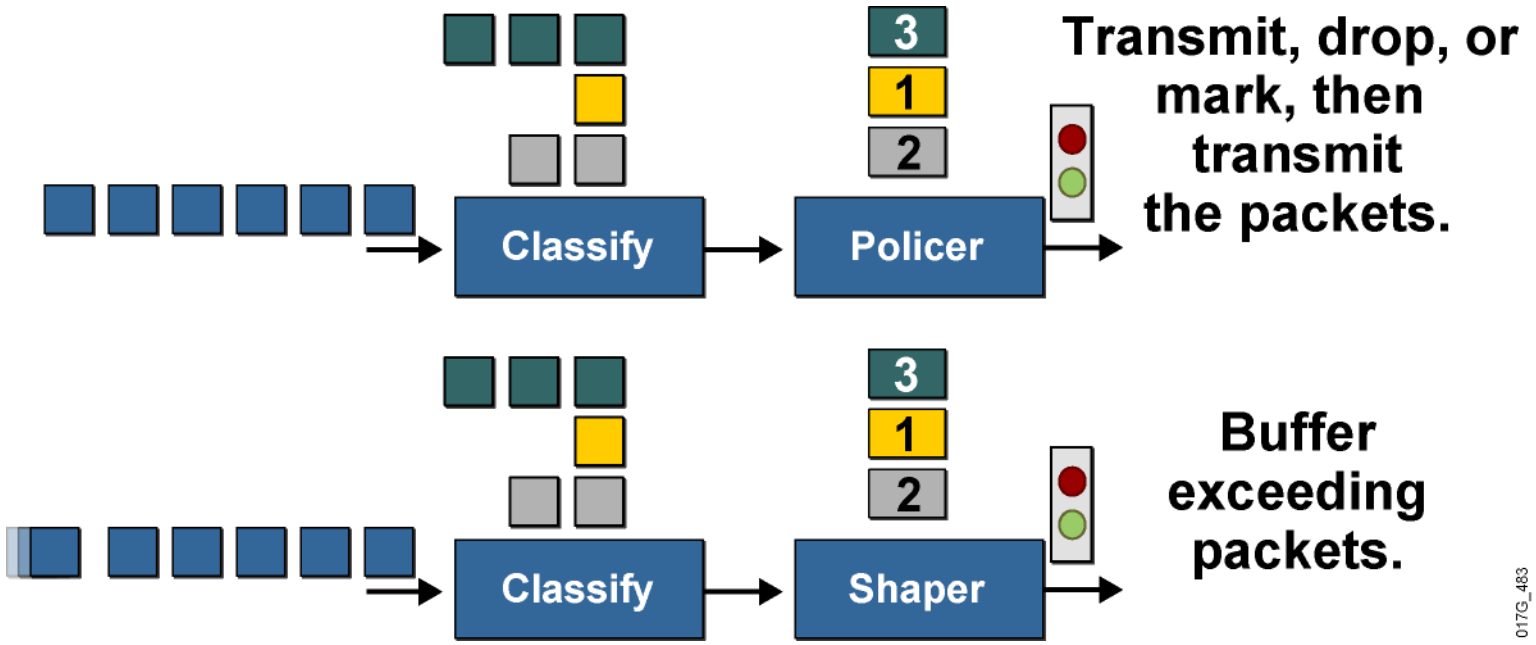
  polja u zaglavlju IP paketa.
- Za svaki tip saobraćaja (npr. web protokoli http, https, webproxy se mogu definisati kao jedan tip) administrator definiše jedan broj za identifikaciju servisa, koji se upisuje u ToS polje.
- Na osnovu ToS polja mrežni uređaji određuju svoje ponašanje prema tom saobraćaju.
- Pojednostavljeno rečeno, klasifikacija ima za cilj upisivanje istog zadatog ToS identifikacionog broja u zaglavlja IP paketa iz iste administratorski definisane grupe protokola.

Traffic Policing and Shaping

Traffic Conditioners

- Policing
  - Limits bandwidth **by discarding** traffic.
  - Can re-mark excess traffic and attempt to send.
  - Should be used on higher-speed interfaces.
  - Can be applied inbound or outbound.
- Shaping
  - Limits excess traffic **by buffering**.
  - Buffering can lead to a delay.
  - Recommended for slower-speed interfaces.
  - Cannot re-mark traffic.
  - Can only be applied in the outbound direction.

Traffic Policing and Shaping Overview



- These mechanisms must classify packets before policing or shaping the traffic rate.
- Traffic policing typically drops or marks excess traffic to stay within a traffic rate limit.
- Traffic shaping queues excess packets to stay within the desired traffic rate.

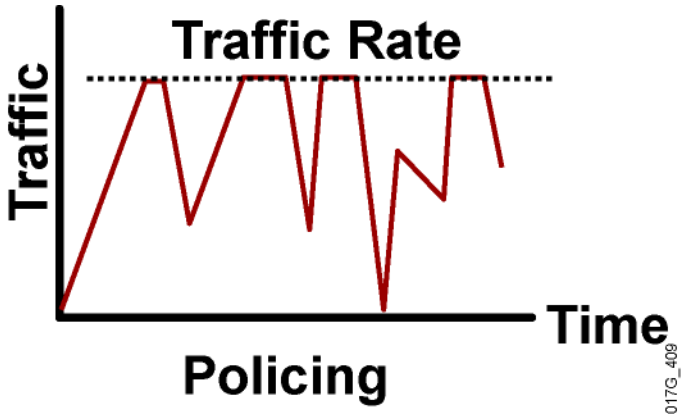
Why Use Policing?

- To limit access to resources when high-speed access is used but not desired (subrate access)
- To limit the traffic rate of certain applications or traffic classes
- To mark down (recolor) exceeding traffic at Layer 2 or Layer 3

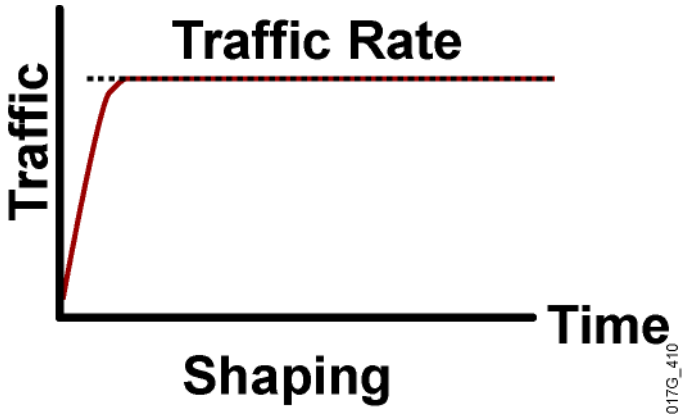
Why Use Shaping?

- To prevent and manage congestion in ATM, Frame Relay, and Metro Ethernet networks, where asymmetric bandwidths are used along the traffic path
- To regulate the sending traffic rate to match the subscribed (committed) rate in ATM, Frame Relay, or Metro Ethernet networks
- To implement shaping at the network edge

Policing Versus Shaping

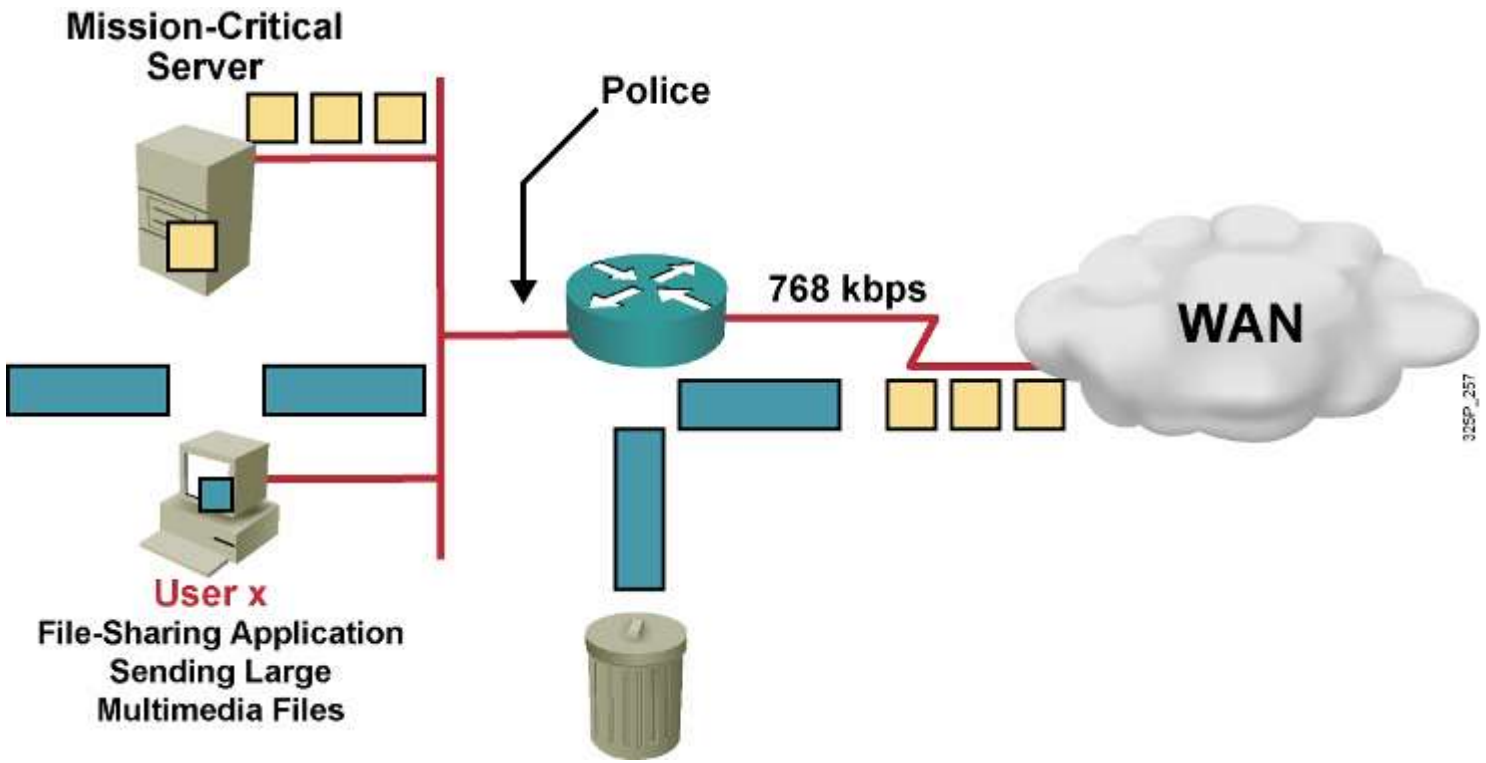


- Incoming and outgoing directions.
- Out-of-profile packets are dropped.
- Dropping causes TCP retransmits.
- Policing supports packet marking or re-marking.



- Outgoing direction only.
- Out-of-profile packets are queued until a buffer gets full.
- Buffering minimizes TCP retransmits.
- Marking or re-marking not supported.
- Shaping supports interaction with Frame Relay congestion indication.

Traffic Policing Example

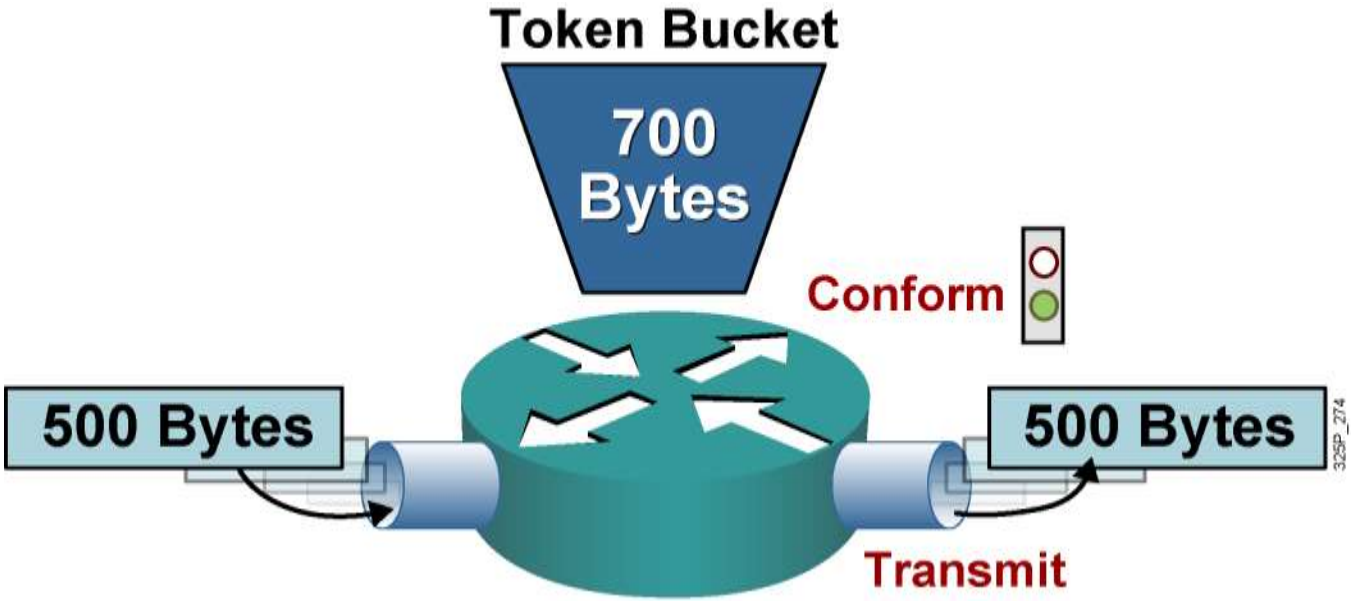


- Do not rate-limit traffic from mission-critical server.
- Rate-limit file-sharing application traffic to 56 kbps.

Token Bucket

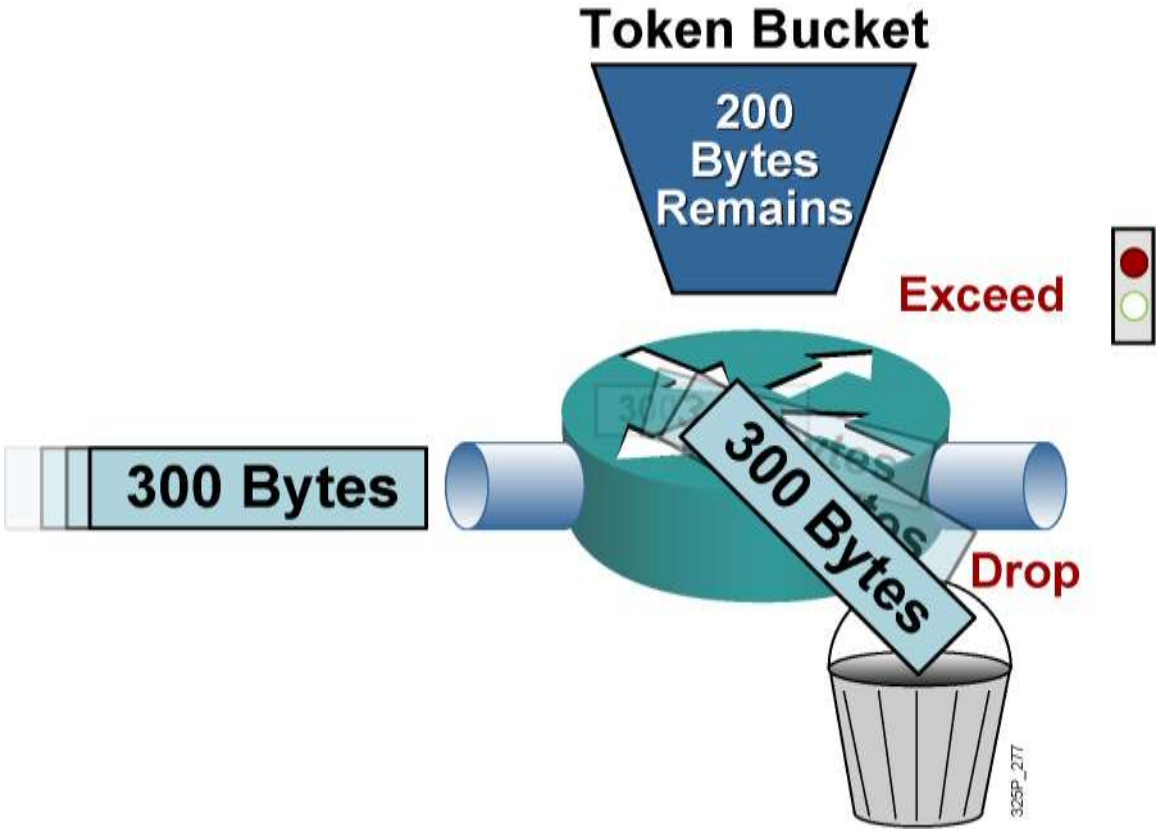
- Mathematical model used by routers and switches to regulate traffic flow.
- Tokens represent **permission to send a number of bits** into the network.
- Tokens **are put into the bucket at a certain rate** by IOS.
- Token bucket holds tokens.
- Tokens are removed from the bucket when packets are forwarded.
- If there are not enough tokens in the bucket to send the packet, traffic conditioning is invoked (shaping or policing).

Single Token Bucket



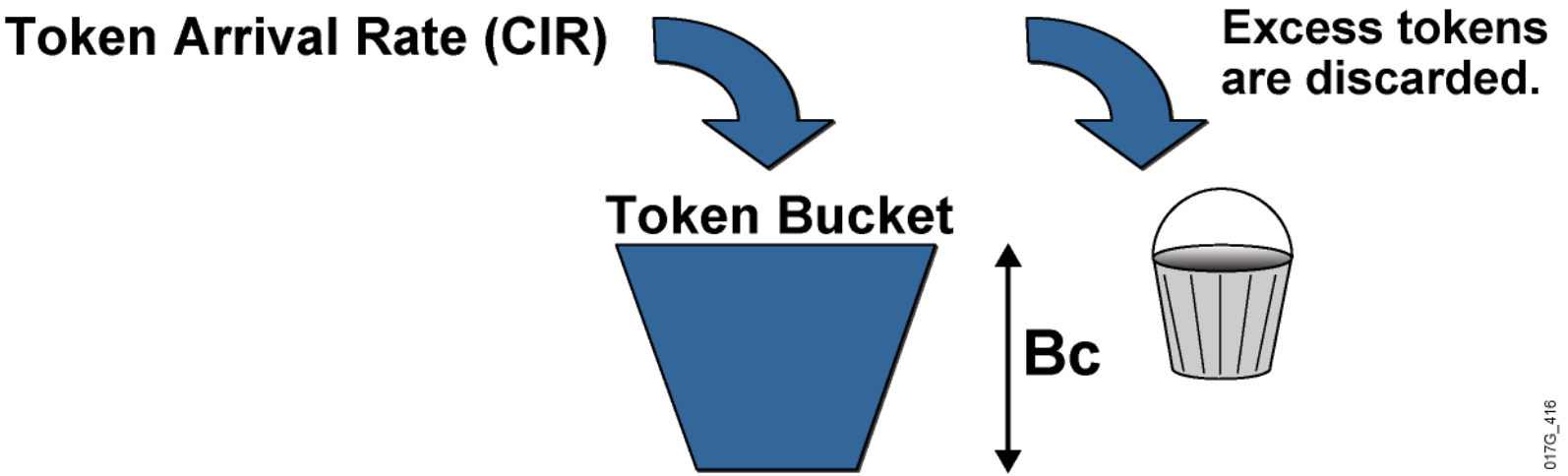
- If sufficient tokens are available (conform action):
  - Tokens equivalent to the packet size are removed from the bucket.
  - The packet is transmitted.

Single Token Bucket Exceed Action



- If sufficient tokens are not available (exceed action):
  - Drop (or mark) the packet.

Single Token Bucket Class-Based Policing



Bc is normal burst size.
Tc is the time interval.
CIR is the committed information rate.
CIR = Bc / Tc

NBAR

- NBAR - Network-Based Application Recognition
- NBAR omogućava
  - Klasifikaciju saobraćaja na
    - Mrežnom,
    - Transportnom, ili
    - Aplikativnom nivou OSI modela (!!!)
      - Ovo omogućava detekciju npr. Torenta bez navođenja portova, već specificiranja specifičnosti formata protokola aplikativnog nivoa
  - Markiranje saobraćaja
  - Policing and shaping

Primer NBAR konfiguracije rutera

- Kreiranje klasa radi klasifikacije različitih tipova saobraćaja u globalnom config modu rutera C2811:

```
class-map match-all KlasaZaEmail
   match protocol pop3
   match protocol imap
   match protocol smtp
class-map match-all KlasaZaVoIP
   match protocol sip
   match protocol h323
   match protocol skinny
   match protocol rtp
class-map match-all KlasaFileDownload
   match protocol ftp
   match protocol BitTorrent
   class-map match-all KlasaZaWeb
   match protocol http
   match protocol https
```

Primer NBAR konfiguracije rutera

- Kreiranje polisa (globalni config mod)

```
policy-map policyIN
  Class KlasaZaEmail
        policy 10 000 000
  class KlasaZaVoIP
        policy 30 000 000
  class ClassWeb
        policy 15 000 000
  class KlasaFileDownload
        policy 15 000 000
  class class-default
        policy 30 000 000
```

- Uključivanje polise na interfejsu (u modu interfejsa)
  - **service-policy input policyIN**