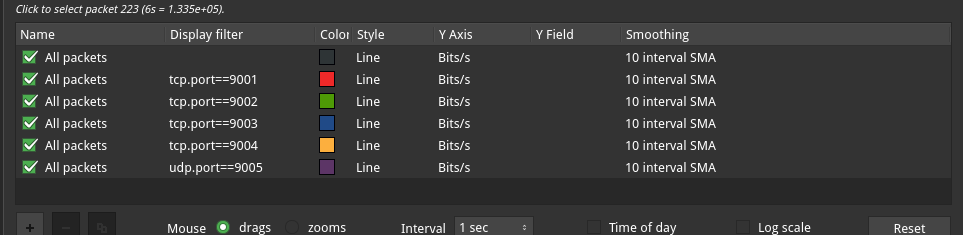
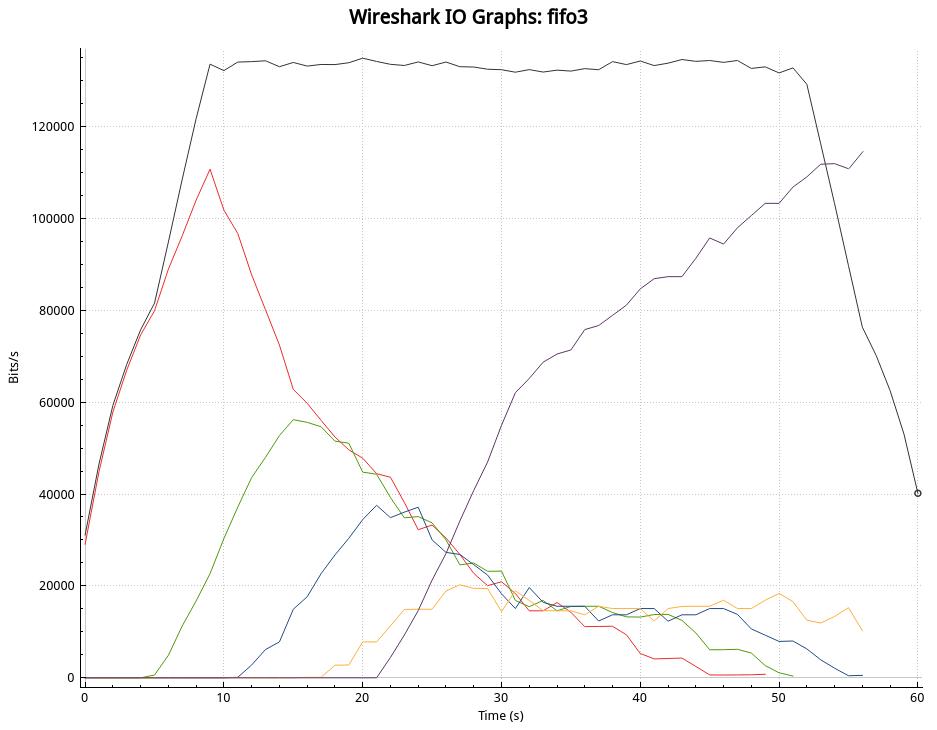
# Laboratórne cvičenie z predmetu Optimalizáia konvergovaných sietí číslo 7

Vypracovali : Bc. Peter Hadač, Bc. Pavol Tuka

## Scenár 1: FIFO

Generovali sme 5 tokov, každý o intenzite 20p/s, jeden z nich bol UDP, zvyšné boli TCP. Pri obrázkoch v tomto výkaze sme použili nasledovné filtre.





\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* TOTAL RESULTS \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Number of flows = 5

Total time = 52.840000 s

Total packets = 1552

Average bitrate = 120.306435 Kbit/s

Average packet rate = 29.371688 pkt/s

**Packets dropped = 0 (0.00 %)**

**Sender#show interface s0/0/0**

**Total output drops: 947**

Najprv sme testovali veľkosti tokov tak, aby v konečnom dôsledku zahltili linku, kvôli nastaveniu rôznych mechanizmov proti zahlteniu. Vo výpise z loggera DITG boli straty nulové, ale na rozhraní smerovača sme videli straty.

# Scenár 2: CBWFQ

**Vytvorili sme 5 x ACL:**

access-list 101 remark TCP\_AF11\_9001

access-list 101 permit tcp any any eq 9001

access-list 102 remark TCP\_AF12\_9002

access-list 102 permit tcp any any eq 9002

access-list 103 remark TCP\_AF31\_9003

access-list 103 permit tcp any any eq 9003

access-list 104 remark TCP\_AF33\_9004

access-list 104 permit tcp any any eq 9004

access-list 105 remark UDP\_AF21\_9005

access-list 105 permit udp any any eq 9005

**Vytvorili sme class-map, ktoré rozlišovali prevádzku na základe vyššie uvedených ACL**

class-map match-all AF11

match access-group 101

class-map match-all AF12

match access-group 102

class-map match-all AF31

match access-group 103

class-map match-all AF33

match access-group 104

class-map match-all AF21

match access-group 105

**Nastavili sme značkovanie**

policy-map Znackovanie

class AF11

set ip dscp af11

class AF12

set ip dscp af12

class AF21

set ip dscp af21

Zvyšná prevádzka (AF31 a AF33) budú v triede *class-default.*

**Nastavili sme QOS politiku na výstupe zo smerovača *Sender***

policy-map CBWFQ

class AF11

bandwidth percent 25

fair-queue

class AF12

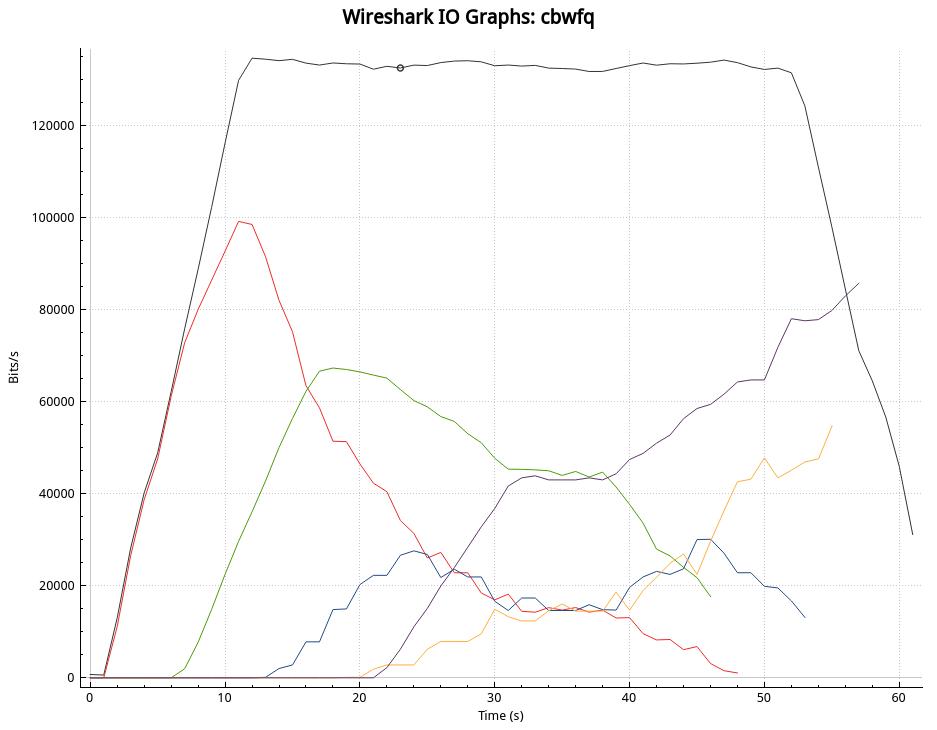
bandwidth percent 25

fair-queue

class AF21

bandwidth percent 25

fair-queue



Flow number: 5

To 10.0.2.2:**9005 (UDP)**

Average bitrate = 52.948590 Kbit/s

Average packet rate = 12.926902 pkt/s

**Packets dropped = 1377 (77.88 %)**

----------------------------------------------------------

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* TOTAL RESULTS \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Number of flows = 5

Average bitrate = 120.072366 Kbit/s

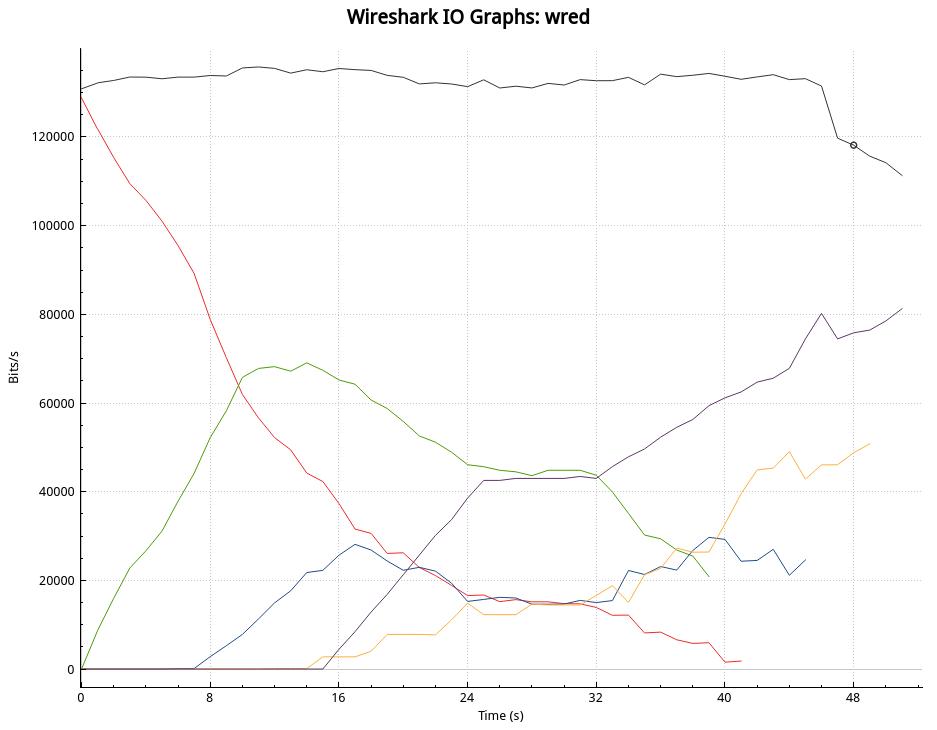
**Packets dropped = 1377 (48.18 %)**

----------------------------------------------------------

Pri použití politiku CBWFQ už došlo k nejakým stratám pri prenose a vidíme, že zahadzované boli iba pakety smerované na port 9005 – teda UDP prevádzka.

# Scenár 3: WRED

V policy-mape CBWFQ sme triedu class-default zmenili na WRED



Flow number: 5

To 10.0.2.2:9005 (**UDP**)

----------------------------------------------------------

Packets dropped = **1375** (77.90 %)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* TOTAL RESULTS \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Packets dropped = **1375** (48.36 %)

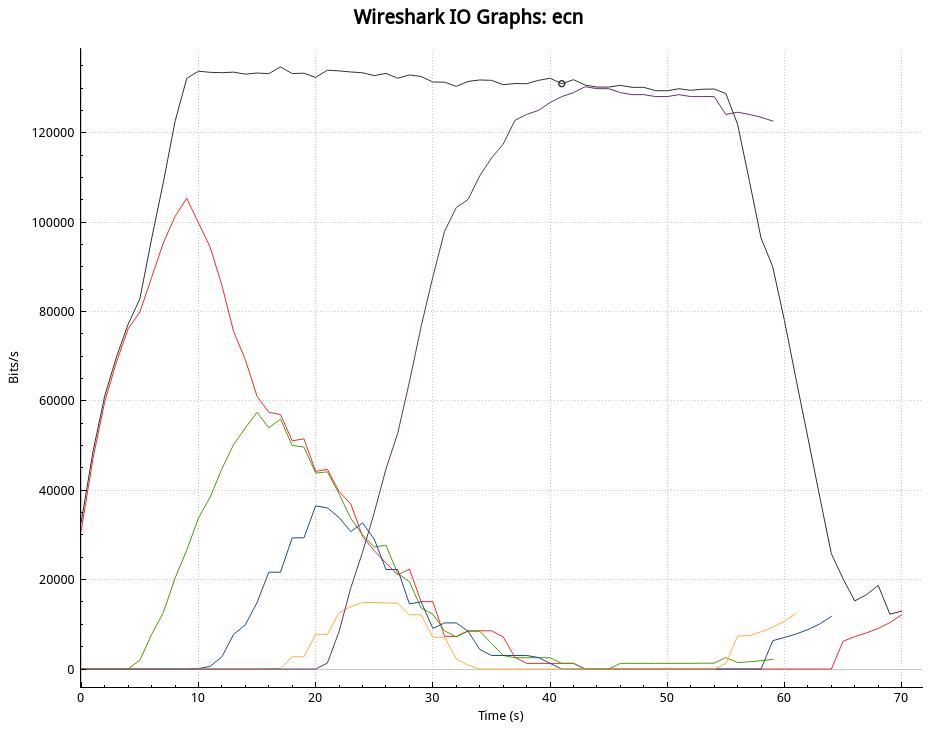
----------------------------------------------------------

Pri použití politiky Weighted Random Early Detection sa nám generovaý tok v sieti správal rovnako ako pri použití CBWFQ – teda boli zahodené len pakety UDP prevádzky.

# Scenár 4: WRED + ECN

V policy-mape CBWFQ sme triedu class-default zmenili na WRED + ECN

netsh int tcp set global ecncapability=enabled



Flow number: 5

To 10.0.2.2:9005 (**UDP**)

Packets dropped = **889** (49.42 %)

----------------------------------------------------------

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* TOTAL RESULTS \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Packets dropped = **889** (34.88 %)

Pri použití politiky WRED + ECN to už dopadlo o niečo lepšie, zahodených paketov bolo o 35% menej ako pri samotnom WRED, prípadne CBWFQ.