

# Laboratoare Administarea Retelelor de Calculatoare

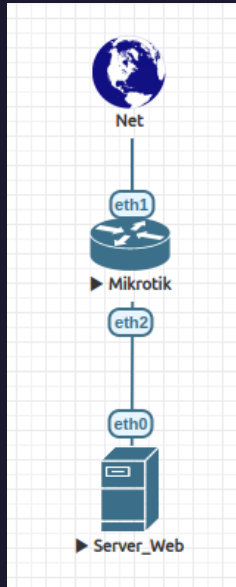
Firewall si Quality of Service



# Port forwarding pe un IP dedicat

- Incepem de la un scenariu in care avem un server web si routerul este conectat la retea 192.168.122.0/24 cu ip-ul lui 192.168.122.60
- Reteaua interna este 10.10.10.0/24 iar serverul web are adresa 10.10.10.254
- Vrem sa ii asignam serverului adresa 192.168.122.61 pentru portul web(80).
- Incepem prin a ii asigna routerului adresa .61 pe portul 80.

Address List			
<div><div></div><div></div><div></div><div></div><div></div><div></div></div>			
	Address	Network	Interface
	<div></div> 10.10.10.1/24	10.10.10.0	ether2
D	<div></div> 192.168.122.60/24	192.168.122.0	ether1
	<div></div> 192.168.122.61/24	192.168.122.0	ether1



- Inainte de a incepe maparea porturilor trebuie sa facem reguli de filtrare.
- Ultima regula fiind mereu drop all input.
- Asa ca incepem sa facem regula de access la porturile routerului pe care vrem sa le folosim (80,8291).

Firewall Rule <192.168.122.61:80>

General

Advanced

Extra

Action

Statistics

Action:

☐ Log

Log Prefix:

Firewall

Filter Rules

NAT

Mangle

Raw

Service Ports

Connections

Address Lists

Layer7 Protocols

+

-

✓

✗

📄

🔍

🔄 Reset Counters

🔄 Reset All Counters

#									
0	✔ Action:	accept	Chain:	input	Dst. Address:	192.168.122.60	Protocol:	6 (tcp)	
	Dst. Port:	80	Hotspot:		Log:	no	Bytes:	1610 B	
	Packets:	26	Rate:	0 bps	Packet Rate:	0			
1	✔ Action:	accept	Chain:	input	Dst. Address:	192.168.122.60	Protocol:	6 (tcp)	
	Dst. Port:	8291	Hotspot:		Log:	no	Bytes:	14.1 KiB	
	Packets:	69	Rate:	0 bps	Packet Rate:	0			
2	✗ Action:	drop	Chain:	input	Hotspot:		Log:	no	
	Bytes:	209.4 KiB	Packets:	2 546	Rate:	2.5 kbps	Packet Rate:	4	

# Regulile de Filtrare

- Pentru ca routerul sa poata comunica avem nevoie de o regula care sa permita noi conexiuni si sa permita celor deja stabilite sa continue comunicarea.
- Atentie acesta ofera un acces general la internet ar routerului si posibil sa nu fie desirabil in orice situatie.
- Apoi mai facem o regula care sa permita acceul din LAN (10.10.10.0/24) la router.
- Si acest lucru trebuie evaulat pentru ca am vrea sa limitam acest acces doar la retea de management.

The image displays three screenshots of the Mikrotik WinBox Firewall Rule configuration interface, showing different stages of rule setup.

**Top Left Screenshot: Firewall Rule <>**

- Chain:
- Src. Address:
- Dst. Address:
- Src. Address List:
- Dst. Address List:
- Protocol:
- Src. Port:
- Dst. Port:
- Any. Port:
- In. Interface:
- Out. Interface:
- In. Interface List:
- Out. Interface List:
- Packet Mark:
- Connection Mark:
- Routing Mark:
- Connection Type:
- Connection State: ☐ invalid ☒ established ☒ related ☐ new ☐ untracked
- Connection NAT State:

**Top Right Screenshot: Firewall Rule <10.10.10.0/24>**

- Chain:
- Src. Address:
- Dst. Address:
- Src. Address List:
- Dst. Address List:
- Protocol:
- Src. Port:
- Dst. Port:
- Any. Port:
- In. Interface:
- Out. Interface:
- In. Interface List:
- Out. Interface List:
- Packet Mark:
- Connection Mark:
- Routing Mark:
- Connection Type:
- Connection State:
- Connection NAT State:

**Bottom Screenshot: Firewall Rule <>**

- Action:
- ☐ Log
- Log Prefix:

# Regulile de NAT

- Prima regula de nat pe care o facem este de a permite serverului accesul la internet printr-o regul de masquerade pe interfeata de iesire ether1 (fiind interfata conectata la internet).
- Dupa instalarea serverului web vom defini si regula care mapeaza portul 80 al serverului pe ip-ul 192.168.122.61.
- Cu actiunea dst-nat catre serverul nostru 10.10.10.254 pe portul 80 de la 192.168.122.61 pe protocolul tcp si portul 80.

NAT Rule <>

General Advanced Extra Action Statistics

Chain: **srcnat**

Src. Address:

Dst. Address:

Src. Address List:

Dst. Address List:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:  ether1

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Connection Type:

NAT Rule <>

General Advanced Extra Action Statistics

Action: **masquerade**

☐ Log

Log Prefix:

To Ports:

NAT Rule <192.168.122.61:80>

General Advanced Extra Action Statistics

Chain: **dstnat**

Src. Address:

Dst. Address:  192.168.122.61

Src. Address List:

Dst. Address List:

Protocol:  6 (tcp)

Src. Port:

Dst. Port:  80

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Connection Type:

NAT Rule <192.168.122.61:80>

General Advanced Extra Action Statistics

Action: **dst-nat**

☐ Log

Log Prefix:

To Addresses:  10.10.10.254

To Ports:  80



# Regulile de NAT

- Acum putem testa conectarea pe cele doua ip-uri pe portul web (80)
- Unde putem observa doua raspunsuri diferite.
- Pe .61 un raspuns default de server apache2 iar pe .60 o pagina complexa care indica pagina de login al routerului.

```
abaddon@abaddon in ~ took 1ms
λ curl http://192.168.122.61
<html><body><h1>It works!</h1></body></html>

abaddon@abaddon in ~ took 7ms
λ curl http://192.168.122.60
<!doctype html>
<html xmlns="http://www.w3.org/1999/xhtml" lang="en">
<head>
<meta charset="utf-8">
<link rel="icon" href="/favicon.png" />
<title>RouterOS router configuration page</title>
<style>
body {
    font-family: Verdana, Geneva, sans-serif;
    font-size: 11px;
}
img {border: none}
img:hover {opacity: 0.8;}
h1 {
    font-size: 1.7em;
    display: inline;
    margin-bottom: 10px;
}
fieldset {
    margin-top: 20px;
    background: #fff;
```

# Regulile de NAT

- Sunt situatii in care si serverul trebuie sa se conecteze la alte servicii pe ip-ul asignat lui ceva ce nu se intampla in mod implicit prin NAT.
- Pornind un listener pe portul 8888 observam ca primim o conexiune de la .60 chiar daca o initializam de pe serverul web
- Asa ca vom adauga o regula noua pe srcnat cu adresa sursa (cel care initializeaza conexiunea) 10.10.10.254 si cu actiunea pe src-nat catre adresa 192.168.122.61.

```
[root@abaddon-82ey abaddon]# nc -vlp 8888
Connection from 192.168.122.60:47326
^CExiting.
[root@abaddon-82ey abaddon]#
```

Server\_Web

```
Docker:/# nc 192.168.122.1 8888
Docker:/#
```

NAT Rule <10.10.10.254>

General Advanced Extra Action Statistics

Chain: **srcnat**

Src. Address: ☐ 10.10.10.254

Dst. Address:

Src. Address List:

Dst. Address List:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Connection Type:

NAT Rule <10.10.10.254>

General Advanced Extra Action Statistics

Action: **src-nat**

☐ Log

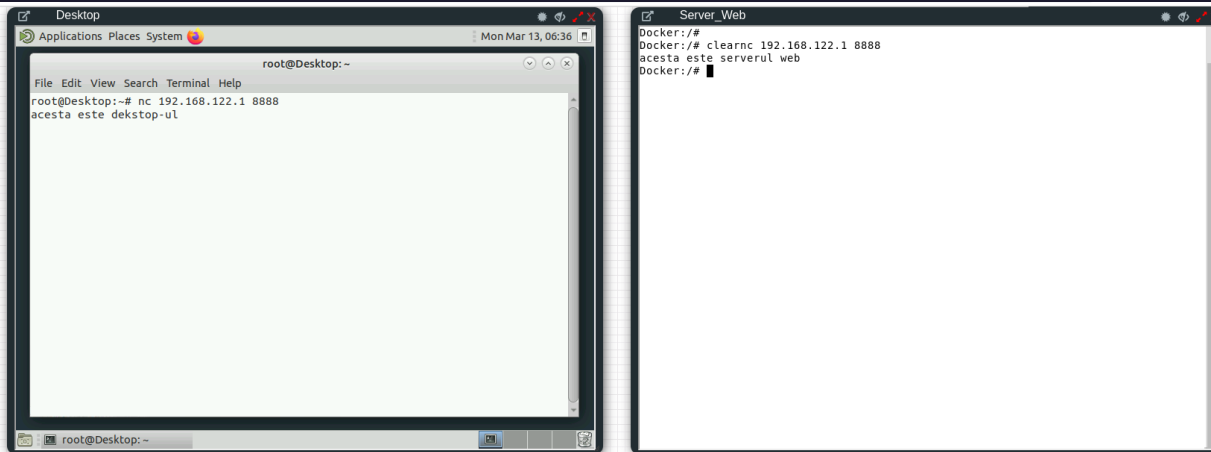
Log Prefix:

To Addresses: 192.168.122.61

To Ports:

# Regulile de NAT

- Si o regula sub ea care sa zica practica toate ip-urile cu exceptia lui 10.10.10.254 sa iasa prin

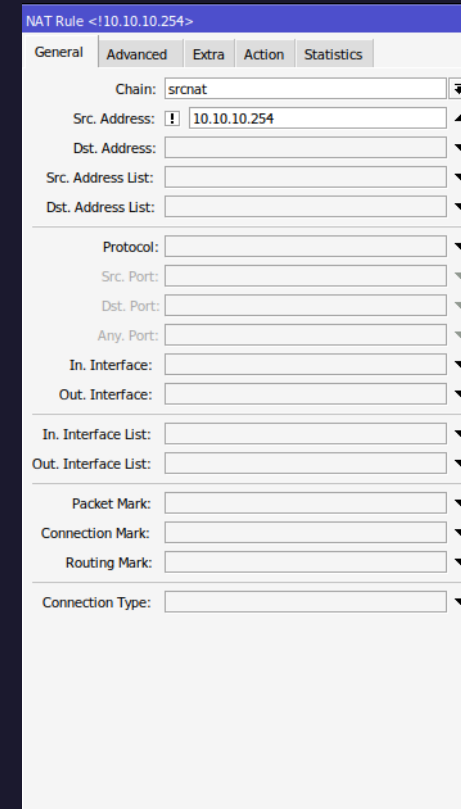


```
root@Desktop:~  
root@Desktop:~# nc 192.168.122.1 8888  
acesta este dektop-ul
```

```
Docker:/#  
Docker:/# clearnc 192.168.122.1 8888  
acesta este serverul web  
Docker:/#
```



```
~ : nc - Konsole  
[~badder@abaddon in ~ took 1ms  
~# nc -lvp 8888  
Connection from 192.168.122.61:36042  
acesta este serverul web  
^CExiting.  
~badder@abaddon in ~ took 10s  
~# nc -lvp 8888  
Connection from 192.168.122.60:43956  
acesta este dektop-ul
```



NAT Rule <10.10.10.254>

General Advanced Extra Action Statistics

Chain: srcnat

Src. Address: 10.10.10.254

Dst. Address:

Src. Address List:

Dst. Address List:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

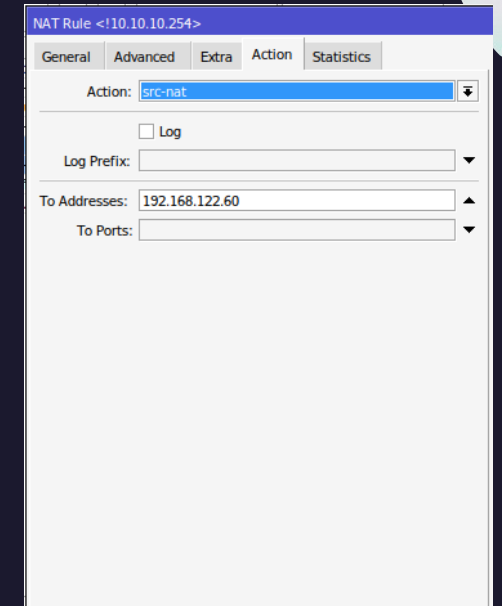
Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Connection Type:



NAT Rule <10.10.10.254>

General Advanced Extra Action Statistics

Action: src-nat

☐ Log

Log Prefix:

To Addresses: 192.168.122.60

To Ports:



# Regulile de NAT

- Avand regulile se NAT astfel:
- Si incercand o noua counexiune catre server obtinem rezultatul dorit.
- Sa nu uitam sa tinem regula generaala de nar ca ultima regula.

Firewall									
Filter Rules		NAT	Mangle	Raw	Service Ports	Connections	Address Lists	Layer7 Protocols	
								Reset Counters  Reset All Counters	
#		Action:		Chain:		Dst. Address:		Protocol:	
0		dst-nat		dstnat		192.168.122.61		6 (tcp)	
		Dst. Port:	80	Hotspot:		no		To Addresses:	10.10.10.254
		To Ports:	80	Bytes:	6.3 KiB	Packets:	107	Rate:	0 bps
		Packet Rate:	0						
1		src-nat		srcnat		10.10.10.254		Hotspot:	
		Log:	no	To Addresses:	192.168.122.61	Src. Address:	60 B	Packets:	1
		Rate:	0 bps	Packet Rate:	0	Bytes:			
2		masquerade		srcnat		ether1		Hotspot:	
		Log:	no	Bytes:	1436 B	Packets:	15	Rate:	0 bps
		Packet Rate:	0						

```
Server_Web
Docker:/# nc 192.168.122.1 8888
Docker:/# nc 192.168.122.1 8888
Docker:/# █

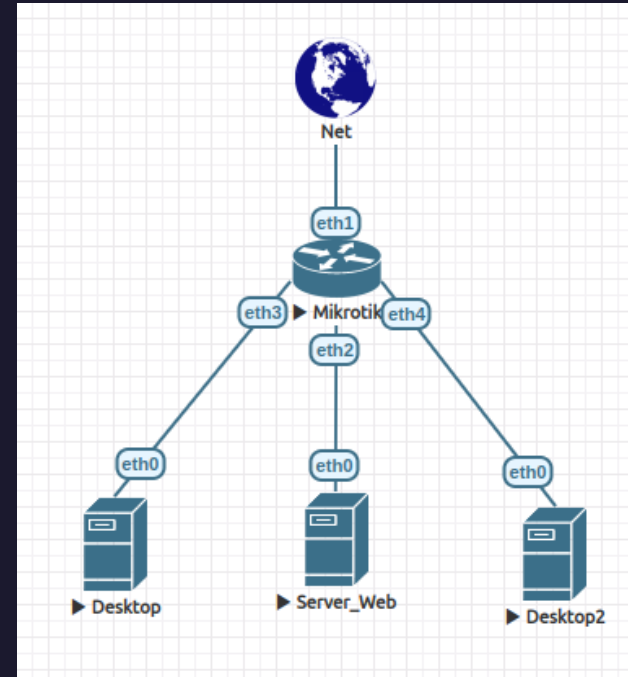
- : bash — Konsole

[root@abaddon-82ey abaddon]# nc -vlp 8888
Connection from 192.168.122.60:47326
^CExiting.
[root@abaddon-82ey abaddon]# nc -vlp 8888
Connection from 192.168.122.60:47450
^CExiting.
[root@abaddon-82ey abaddon]# nc -vlp 8888
Connection from 192.168.122.61:47584
^CExiting.
[root@abaddon-82ey abaddon]# _
```

10

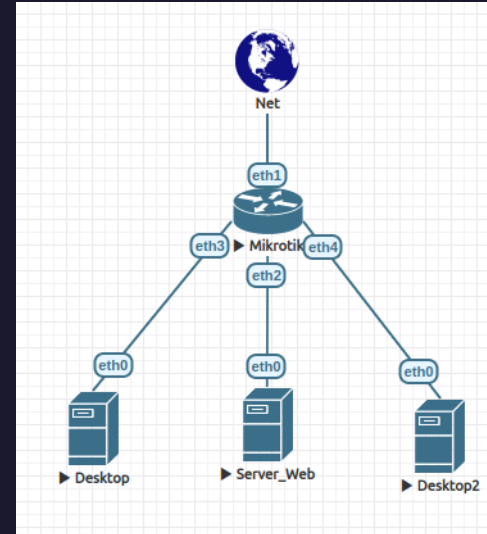
# Reguli de baza QoS

- Am adaugat in infratructura doi clienti desktop bazati pe Ubuntu pentru care vom face regulie de QoS.
- Mikrotik implementeaza un sistem numit Ques care se ocupa de reguli de latime de banda practic si impreuna cu reguli de mangle vom putea face limitari in functie de servicii sau destinatii.



# Reguli de baza QoS

- In primul rand mergem in Queues si adaugam un queue simplu nou.
- La target putem sa punem o clasa, o lista de clase, un ip sau o lista de ip-uri asupta carora sa actioneze regula.
- Max Limit este limita superioara aatat pentru download cat si pentru upload pe care vrem sa o setam.
- In cazul nostru routerul are o legatura de 100Mb dar vrem sa limitam la 10Mb transfer.



New Simple Queue

General Advanced Statistics Traffic Total Total Statistics

Name: queue1

Target: 10.10.10.0/24

Dst.:

Max Limit: 10M

Target Upload: 10M

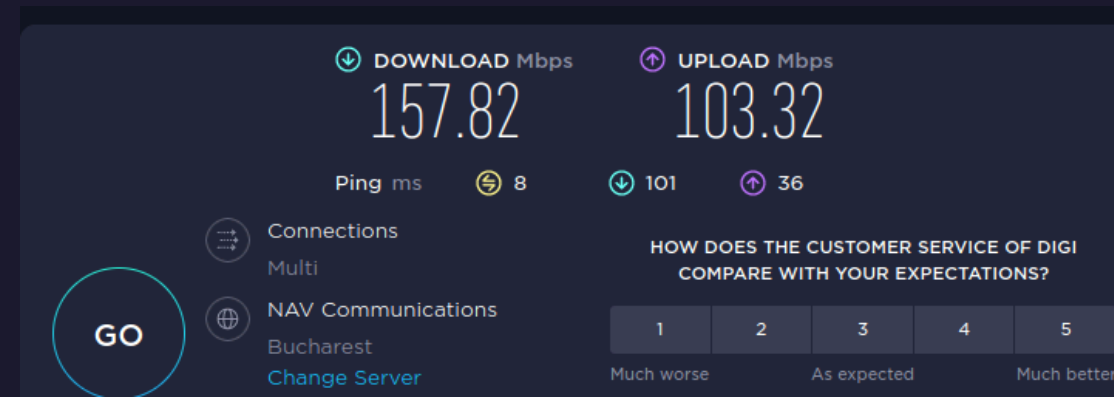
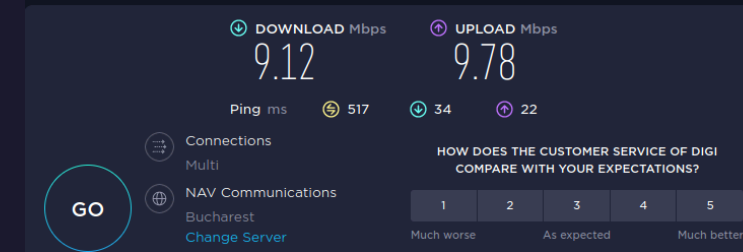
Target Download: 10M

bits/s

Burst

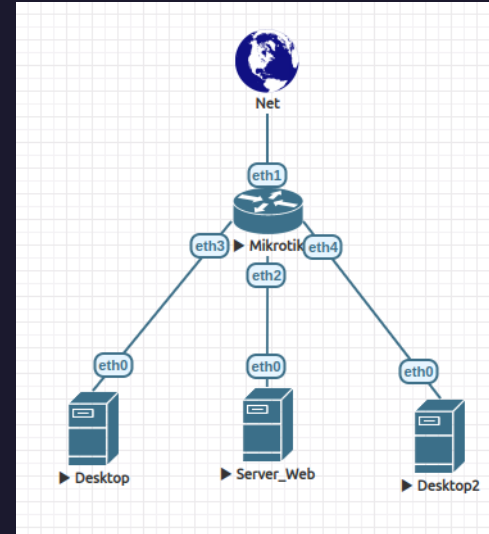
Time

enabled



# Reguli de baza QoS

- In cazul in care vrem sa prioritizam un anumit dispozitiv in retea.
- Acum daca vrem sa prioritizam un client din cei doi putem face un queue pentru fiecare cu un parinte care ar trebuie sa fie de aproape toata lungimea de banda.



New Simple Queue

General Advanced Statistics Traffic Total Total Statistics

Name: queue1

Target: 10.10.10.0/24

Dst.:

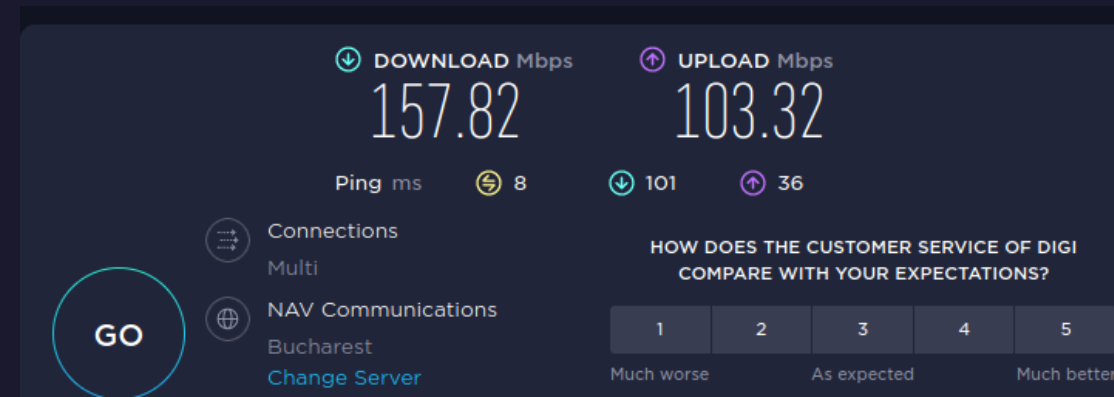
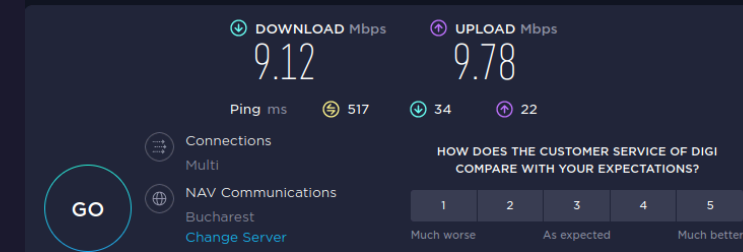
Target Upload Target Download

Max Limit: 10M 10M bits/s

Burst

Time

enabled



# Reguli de baza QoS

- Queue-ul LAN va fi cel parinte la toata retea.
- Acum adaugam unul pentru desktop1 iar la Advanced punem ca parinte queue-ul LAN.
- Repetam acelasi pas si pentru desktop2.
- In situatia actuala latimea de banda va fi impartita egal intre cele doua desktopuri dar vrem ca desktop2 sa aibe prioritate si o latime garantata de 80M.
- In Advanced setam Limit At 80M si punem Priority 1
- Pentru o acuratete mai mare setam si Queue Type ca pcq.
- Pentru a optimiza restrictiile putem sa setam si clientului desktop1 o limita de 10-20M si o prioritate mai mare 2-8.

Sample Footer Text

New Simple Queue

General Advanced Statistics Traffic Total Total Statistics

Name: LAN

Target: 10.10.10.0/24

Dst.:

Max Limit: 100M Target Upload: 100M Target Download: 100M bits/s

Burst Time

New Simple Queue

General Advanced Statistics Traffic Total Total Statistics

Name: desktop1

Target: 10.10.10.252

Dst.:

Max Limit: 100M Target Upload: 100M Target Download: 100M bits/s

Burst Time

Simple Queue <desktop2>

General Advanced Statistics Traffic Total Total Statistics

Name: desktop2

Target: 10.10.10.251

Dst.:

Max Limit: 100M Target Upload: 100M Target Download: 100M bits/s

Burst Time

New Simple Queue

General Advanced Statistics Traffic Total Total Statistics

Packet Marks:

Limit At: 0 Target Upload: 0 Target Download: 0 bits/s

Priority: 8

Bucket Size: 0.100 ratio

Queue Type: default-small default-small

Parent: LAN

Simple Queue <desktop2>

General Advanced Statistics Traffic Total Total Statistics

Packet Marks:

Limit At: 80M Target Upload: 80M Target Download: 80M bits/s

Priority: 1

Bucket Size: 0.100 ratio

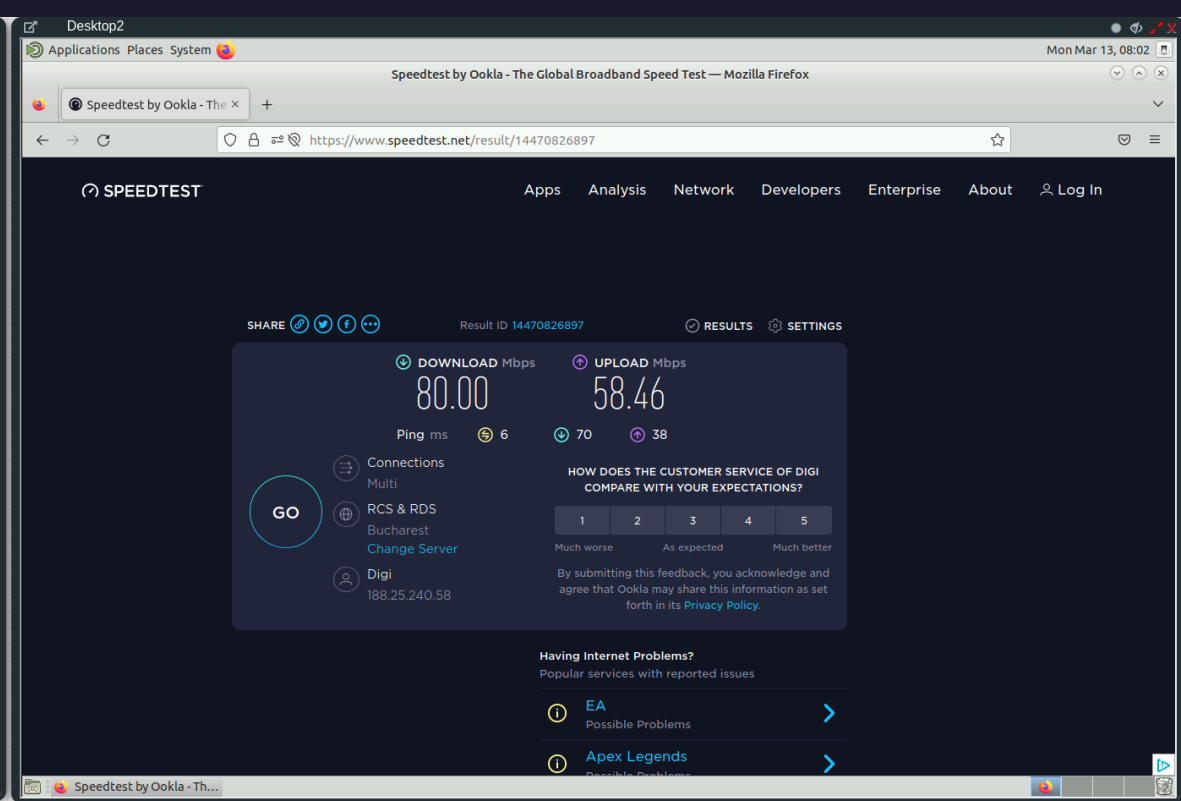
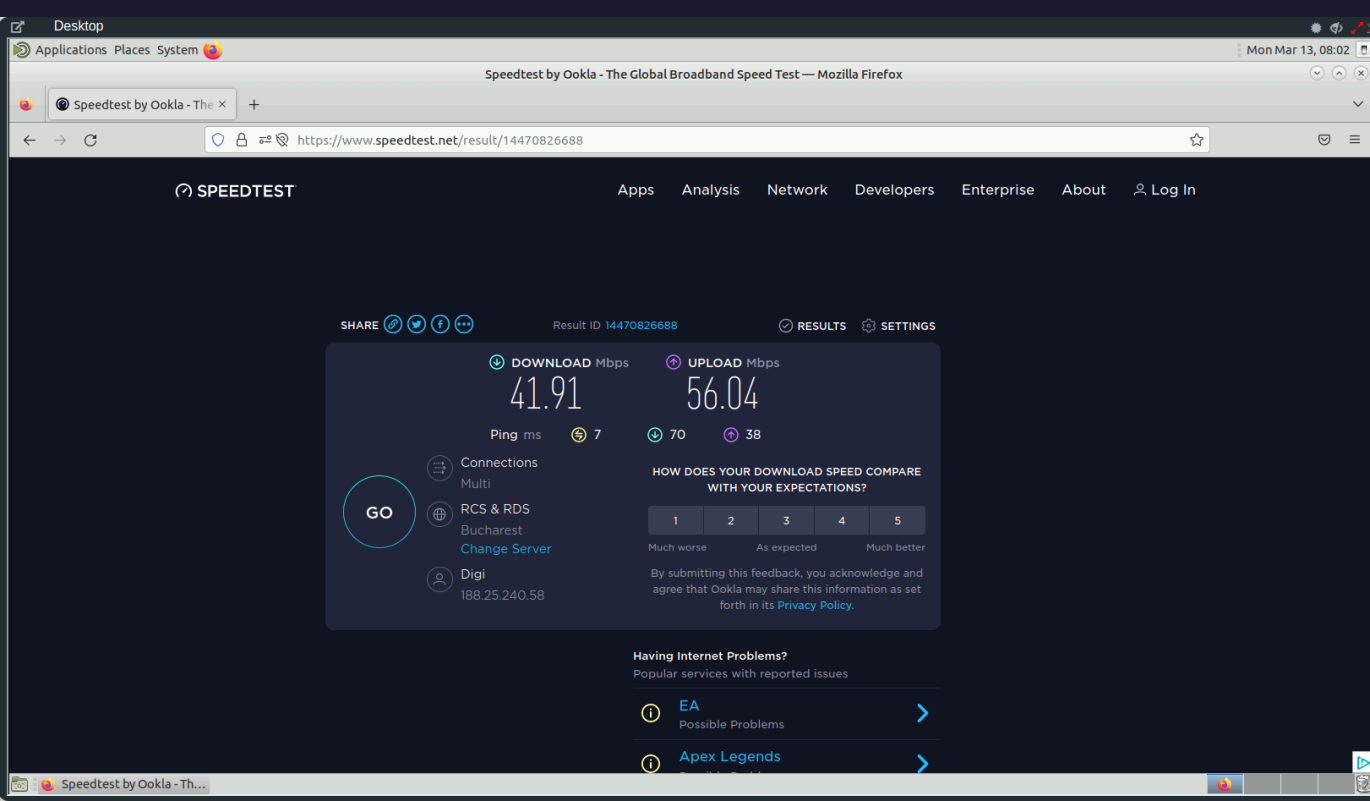
Queue Type: pcq-upload-default pcq-download-default

Parent: LAN



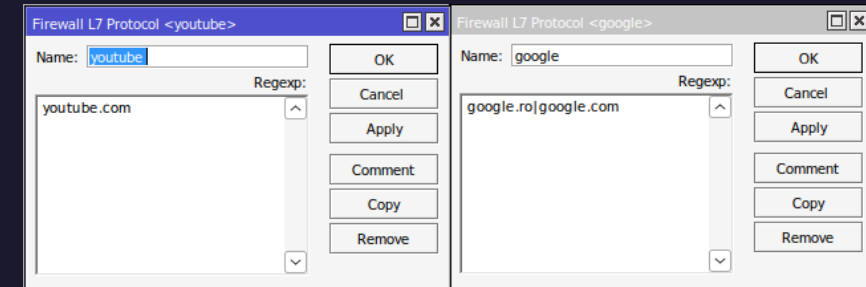
# Reguli de baza QoS

- Dupa ce rulam un test putem vedea rezultatele care reflecta restrictiile impuse de noi.

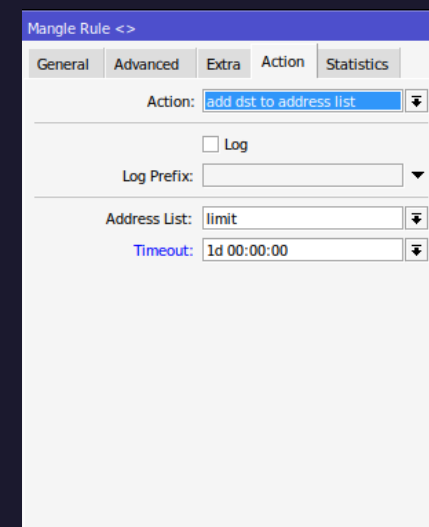
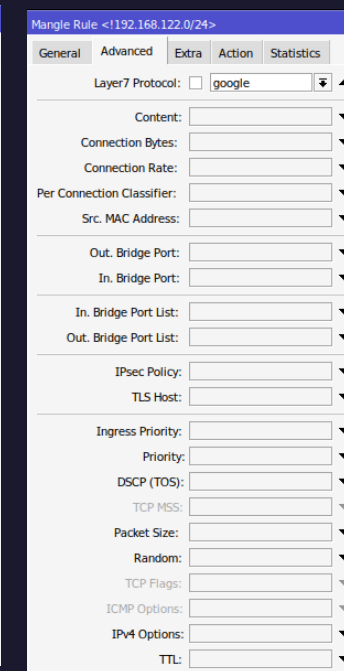
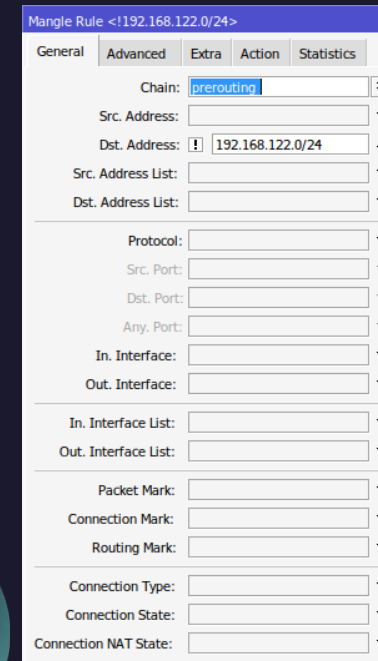


# QoS Avansat

- Sa zicem ca vrem sa limitam viteza pentru site-urile google.com/ro si youtube.com folosind reguli de filtrare si Layer 7.
- In primul rand trebuie sa scoatem o lista dinamica de IP-uri cand utilizatorii acceseaza acele site-uri.
- Mergem in IP→Firewall→Layer7 Protocols unde vom face doua regex-uri.
- Dupa care facem o regula de Mangle in care extragem ip-urile din conexiuni.
- Regula va fi pe prerouting si facem o lista de exceptii a elimina false positive.
- In Advanced selectam unul din regex-uri in Layer7 Protocol.
- Iar la Action setam add dst to address list si dam un nume listei ("limit" in cazul meu), mai putem seta si un timeout pentru a regenera lista.




Name	Address	Timeout	Creation Time
whitelist	192.168.122.0/24		Mar/13/2023 08:50:51
whitelist	10.10.10.0/24		Mar/13/2023 08:50:59



# QoS Avansat

- Acum folosind unul din clienti accesam [google.ro/com](https://google.ro/com) si ne uitem in Address List si vedem o lista de ip-uri adaugate.
- Cautand clasa pe net putem vedea ca apartine Google LLC.
- Repetam aceasi regula si pentru youtube.

Firewall				
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols				
+ - ✓ ✕ [icon] [icon]				
	Name	Address	Timeout	Creation Time
D	limit	142.251.39.35	23:59:33	Mar/13/2023 08:54:26
D	limit	142.251.39.46	23:59:46	Mar/13/2023 08:54:38
D	limit	142.251.39.4	23:59:53	Mar/13/2023 08:54:45
	whitelist	192.168.122.0/24		Mar/13/2023 08:50:51
	whitelist	10.10.10.0/24		Mar/13/2023 08:50:59

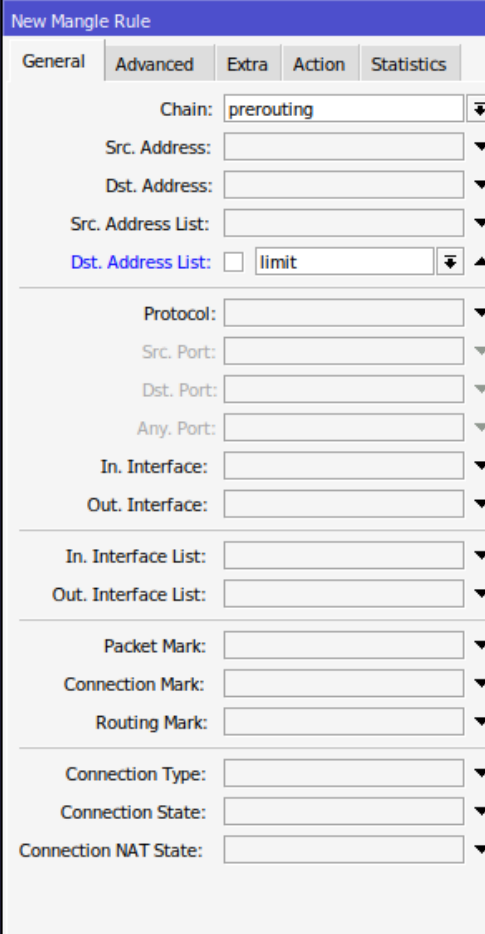
142.250.0.0/15  
AS15169 - GOOGLE - Google LLC, US  
 United States  
GOOGLE - Google LLC

## Summary

NetName	GOOGLE	OrgName	Google LLC
CIDR	142.250.0.0/15	RIR	ARIN
Country		Status	Direct Allocation
Abuse	network-abuse@google.com	Contact	arin-contact@google.com
RegDate	2012-05-24	Updated	2012-05-24

# QoS Avansat

- Si acum trebuie sa marcam pachetele care apartin listei facute de noi.
- Facem o regula noua de mangle la Dst. Address List punem lista dinamica (cazul meu "limit")
- In Action setam "mark packet" si la New Packet Mark setam un nume (In cazul meu mark\_limit).



New Mangle Rule

General Advanced Extra Action Statistics

Chain: prerouting

Src. Address:

Dst. Address:

Src. Address List:

Dst. Address List: ☐ limit

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

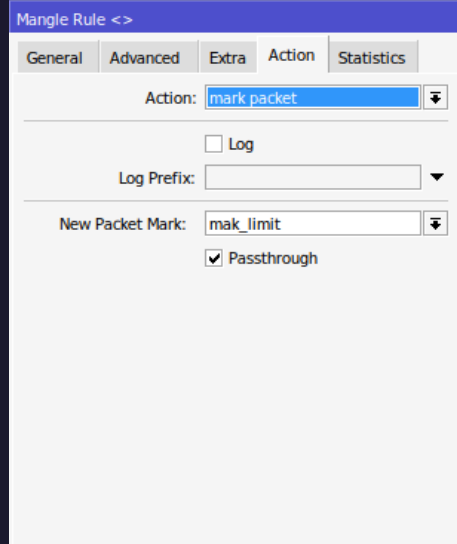
Connection Mark:

Routing Mark:

Connection Type:

Connection State:

Connection NAT State:



Mangle Rule <>

General Advanced Extra Action Statistics

Action: mark packet

☐ Log

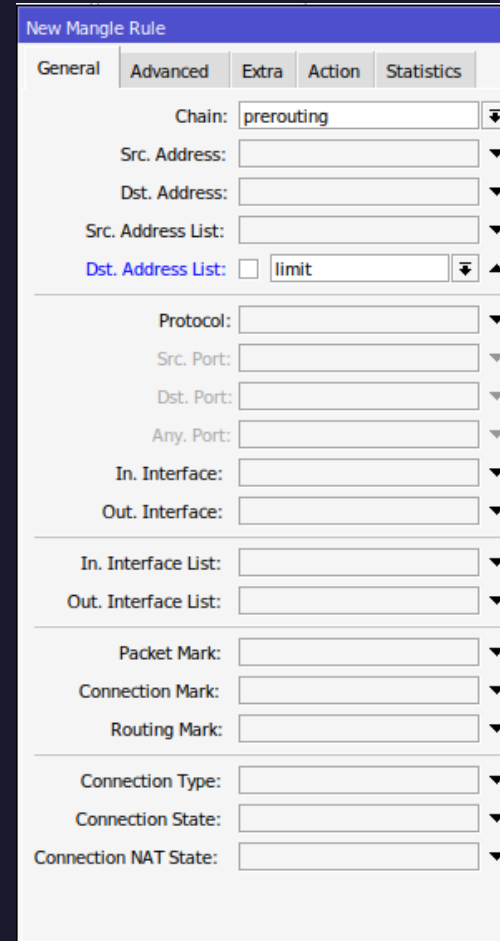
Log Prefix:

New Packet Mark: mak\_limit

☒ Passthrough

# QoS Avansat

- Acum putem face un queue activa pe retea punem limita de 1k pentru teste sa vedem ca se incarca greu.
- La advanced punem Packet Marks mark\_limit si Parent LAN.
- Dupa care mutam cei doi copii sub aceasta regula.



New Mangle Rule

General Advanced Extra Action Statistics

Chain: prerouting

Src. Address:

Dst. Address:

Src. Address List:

Dst. Address List: ☐ limit

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

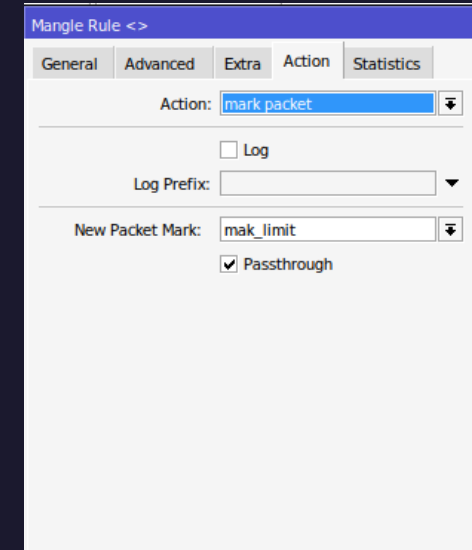
Connection Mark:

Routing Mark:

Connection Type:

Connection State:

Connection NAT State:



Mangle Rule <>

General Advanced Extra Action Statistics

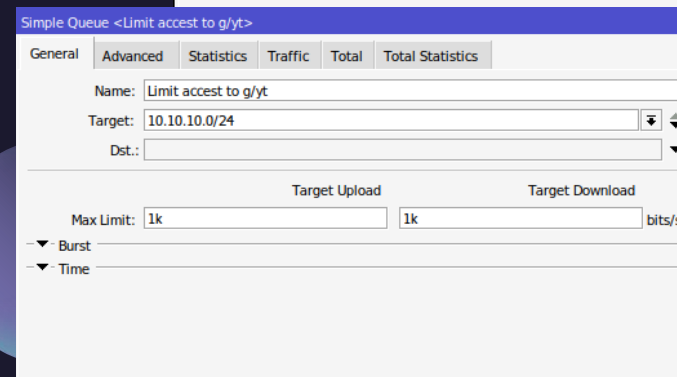
Action: mark packet

☐ Log

Log Prefix:

New Packet Mark: mark\_limit

☒ Passthrough



Simple Queue <Limit access to g/yt>

General Advanced Statistics Traffic Total Total Statistics

Name: Limit access to g/yt

Target: 10.10.10.0/24

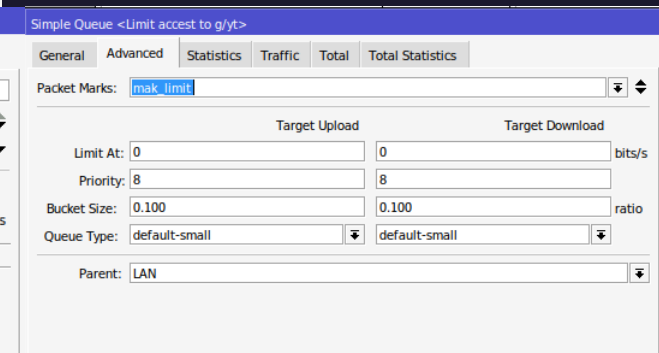
Dst.:

Target Upload Target Download

Max Limit: 1k 1k bits/s

Burst

Time



Simple Queue <Limit access to g/yt>

General Advanced Statistics Traffic Total Total Statistics

Packet Marks: mark\_limit

Limit At: 0 0 bits/s

Priority: 8 8

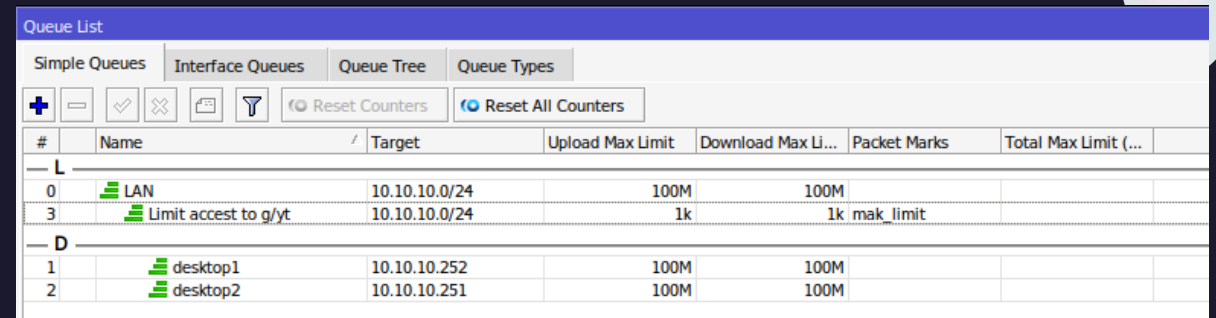
Bucket Size: 0.100 0.100 ratio

Queue Type: default-small default-small

Parent: LAN

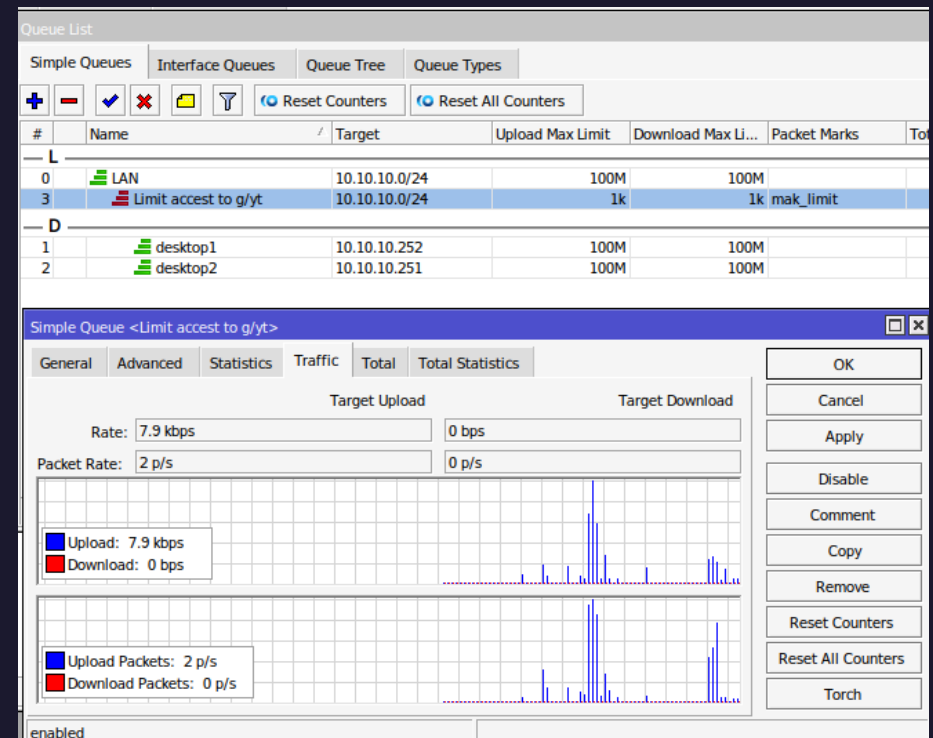
# QoS Avansat

- Avand urmatoarea structura:
- Si vedem ca la simpla accesare a site-ului google sau youtube queue-ul devine rosu insemnand ca a atins limita impusa de noi.



The screenshot shows the 'Queue List' window in Mikrotik WinBox. It displays a table of configured queues. The 'L' (Limit) section contains two entries: 'LAN' (target 10.10.10.0/24, upload/download limits 100M) and 'Limit access to g/yt' (target 10.10.10.0/24, upload/download limits 1k, packet mark 'mak\_limit'). The 'D' (Desktop) section contains two entries: 'desktop1' (target 10.10.10.252, upload/download limits 100M) and 'desktop2' (target 10.10.10.251, upload/download limits 100M).

#	Name	Target	Upload Max Limit	Download Max Li...	Packet Marks	Total Max Limit (...)
<b>L</b>						
0	LAN	10.10.10.0/24	100M	100M		
3	Limit access to g/yt	10.10.10.0/24	1k	1k	mak_limit	
<b>D</b>						
1	desktop1	10.10.10.252	100M	100M		
2	desktop2	10.10.10.251	100M	100M		





# QoS Avansat

- O alta metoda de a adauga domenii este direct in lista routerul facand automat rezoltuia la IP a lor.

New Firewall Address List

Name: limit

Address: bing.com

Timeout:

Creation Time: Mar/13/2023 07:47:06

enabled

	Name	Address	Timeout	Creation Time
D	limit	142.251.39.35	23:31:21	Mar/13/2023 08:54:26
D	limit	142.251.39.46	23:38:05	Mar/13/2023 08:54:38
D	limit	142.251.39.4	23:28:50	Mar/13/2023 08:54:45
D	limit	142.251.39.13	23:36:55	Mar/13/2023 09:02:49
D	limit	142.250.201.196	23:36:56	Mar/13/2023 09:02:51
D	limit	142.251.208.110	23:59:21	Mar/13/2023 09:10:47
D	limit	142.251.208.163	23:46:23	Mar/13/2023 09:11:19
D	limit	142.250.201.206	23:59:10	Mar/13/2023 09:11:19
D	limit	142.250.201.195	23:53:39	Mar/13/2023 09:11:27
D	limit	142.251.208.164	23:47:09	Mar/13/2023 09:13:04
D	limit	142.250.180.238	23:50:02	Mar/13/2023 09:15:57
D	limit	142.251.208.99	23:59:19	Mar/13/2023 09:22:23
D	limit	142.251.39.67	23:59:19	Mar/13/2023 09:22:23
	limit	bing.com		Mar/13/2023 09:25:02
	bing.com			
D	limit	13.107.21.200		Mar/13/2023 09:25:02
	bing.com			
D	limit	204.79.197.200		Mar/13/2023 09:25:02
	whitelist	192.168.122.0/24		Mar/13/2023 08:50:51
	whitelist	10.10.10.0/24		Mar/13/2023 08:50:59