

CAPsMAN гостевая WiFi сеть

Алгоритм

1. Гостевой bridge
2. Адресация
3. DHCP сервер
4. CAPsMAN
5. IP Rules
6. IP Firewall Tacttrack
7. QoS для гостевой сети

Bridge → New Bridge

The screenshot shows the Mikrotik WinBox interface for configuring a bridge. The main window displays a table of bridges:

Name	Type	L2 MTU	Tx	Rx	Tx F
bridge	Bridge	1598	74.9 Mbps	2.0 Mbps	
bridge-guest	Bridge	65535	0 bps	0 bps	

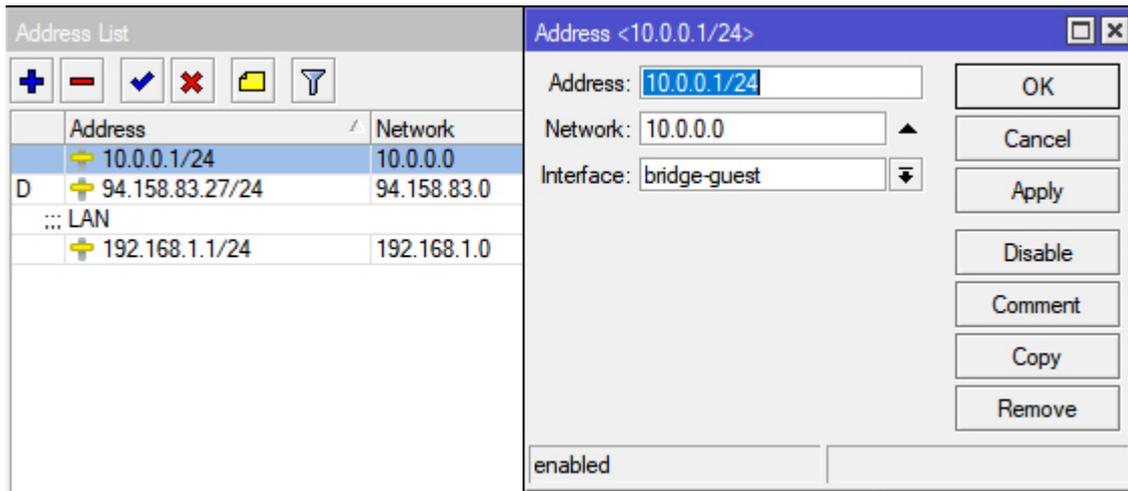
The 'bridge-guest' bridge is selected, and the 'Interface <bridge-guest>' configuration dialog is open. The configuration is as follows:

- Name: bridge-guest
- Type: Bridge
- MTU: (empty)
- Actual MTU: 1500
- L2 MTU: 65535
- MAC Address: C6:D3:69:14:31:32
- ARP: enabled
- ARP Timeout: (empty)
- Admin. MAC Address: (empty)
- Ageing Time: 00:05:00
- IGMP Snooping:
- DHCP Snooping:
- Fast Forward:

Buttons on the right side of the dialog include: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Torch.

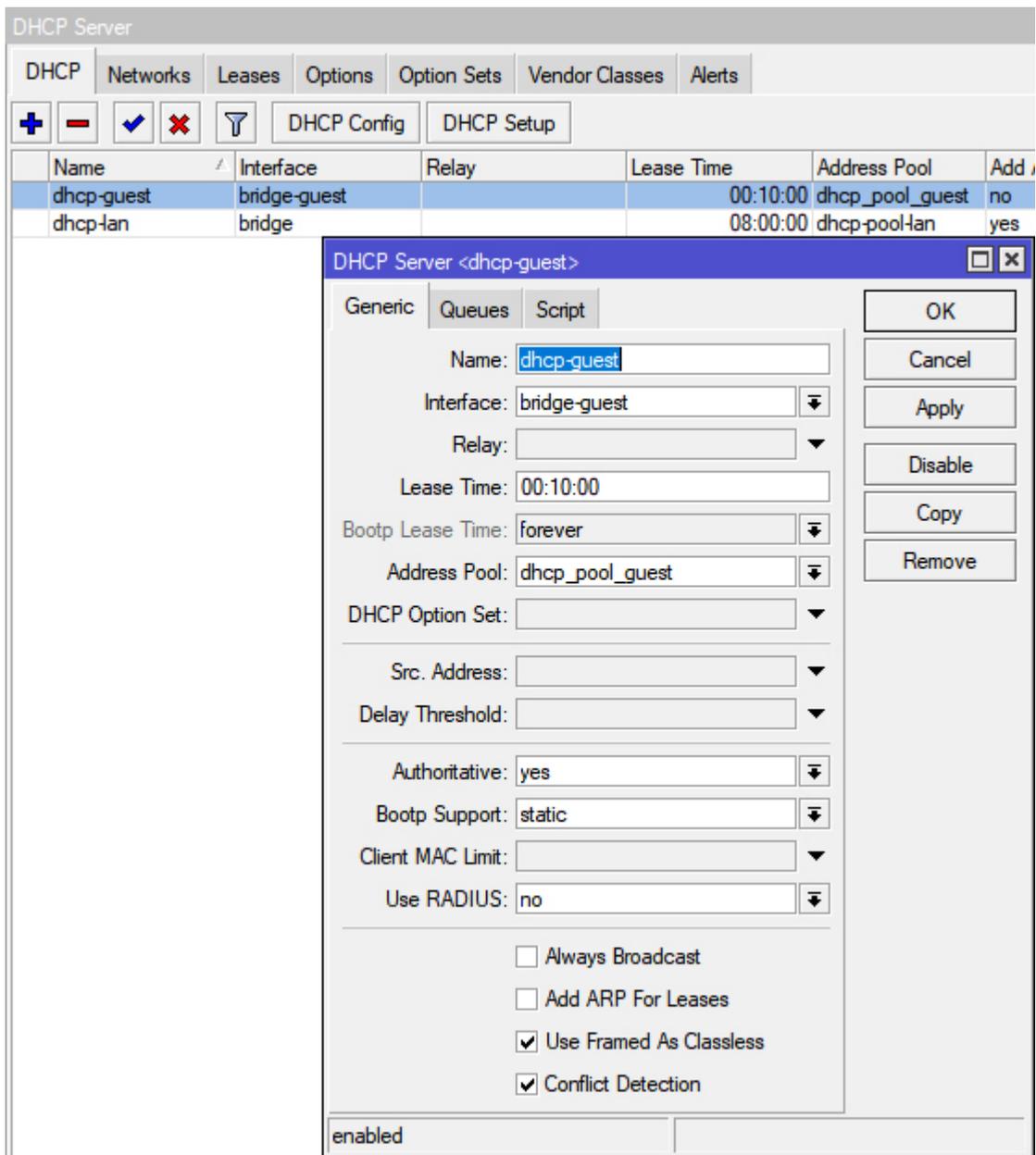
At the bottom of the dialog, the status is shown as: enabled, running, slave.

IP → Addresses → New Address



IP → DHCP Server → DHCP Server Setup

Создаем DHCP сервер для гостевой сети, но в настройках DNS лучше указать google (8.8.8.8; 8.8.4.4)



Можно поставить галочку **Add ARP For Leases**, если нужен контроль этой сети.

Переходим в CAPsMAN. Создаем профиль гостевой сети

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration

+ - [icon] [icon]

Name	Authentication Type	Encryption	Group Encryption	Group Key Update	Passphrase	EAP Methods
security2G	WPA2 PSK	aes ccm	aes ccm	00:20:00	*****	
security2G-guest	WPA2 PSK	aes ccm	aes ccm		*****	
security5G	WPA2 PSK	aes ccm	aes ccm	00:20:00	*****	

3 items (1 selected)

CAPs Security Configuration <security2G-guest>

Name: security2G-guest

Authentication Type: WPA PSK WPA2 PSK WPA EAP WPA2 EAP

Encryption: aes ccm tkip

Group Encryption: aes ccm

Group Key Update:

Passphrase: *****

Disable PMKID:

EAP Methods:

OK Cancel Apply Comment Copy Remove

Выбираем безопасность, если она нужна.

Создаем гостевой Datapath

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio

+ - [icon] [icon]

Name	Bridge	Local For...	Client To ...	VLAN Mo...	VLAN ID
datapath2G	bridge		yes		
datapath2G-guest	bridge-guest				
datapath5G	bridge		yes		

3 items

CAPs Datapath Configuration <datapath2G-guest>

Name: datapath2G-guest

MTU:

L2 MTU:

ARP:

Bridge: bridge-guest

Bridge Cost:

Bridge Horizon:

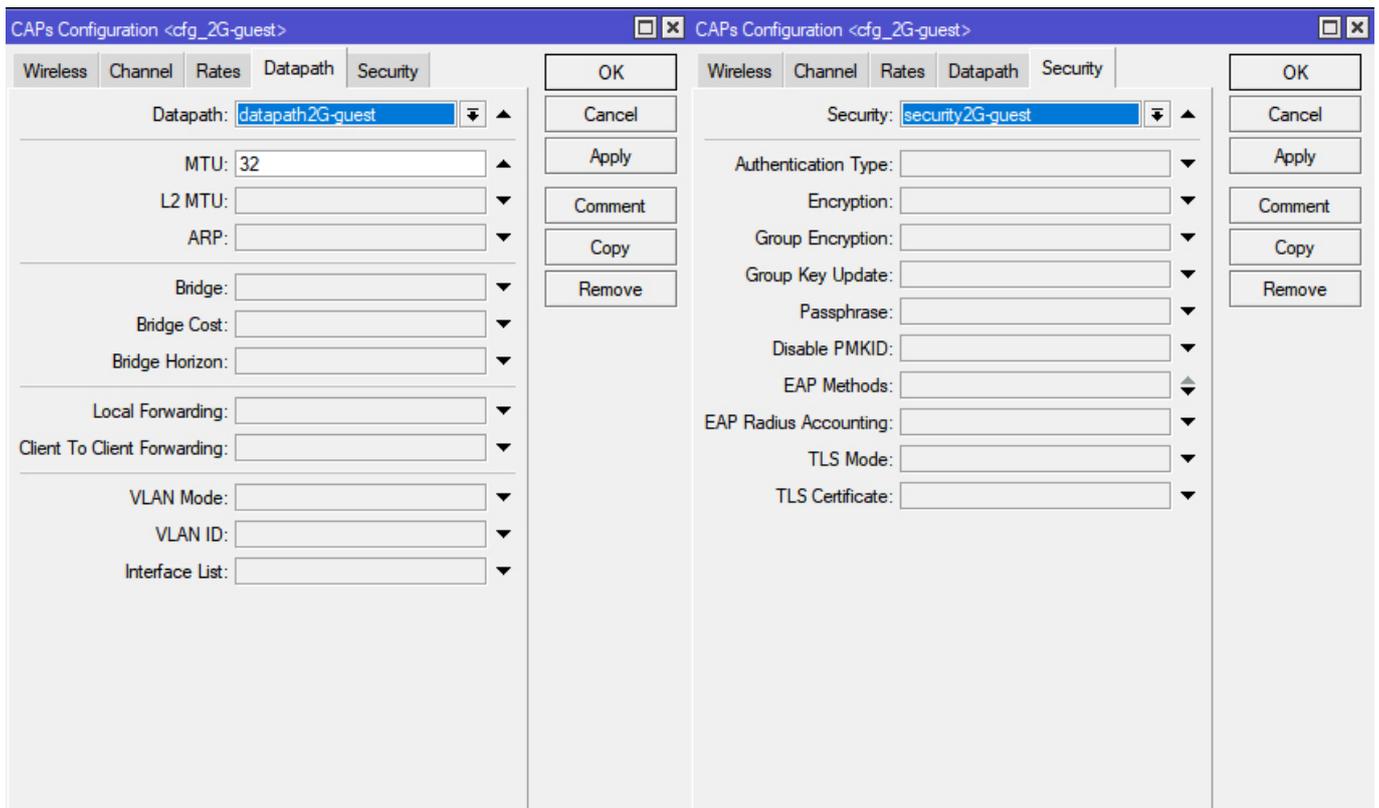
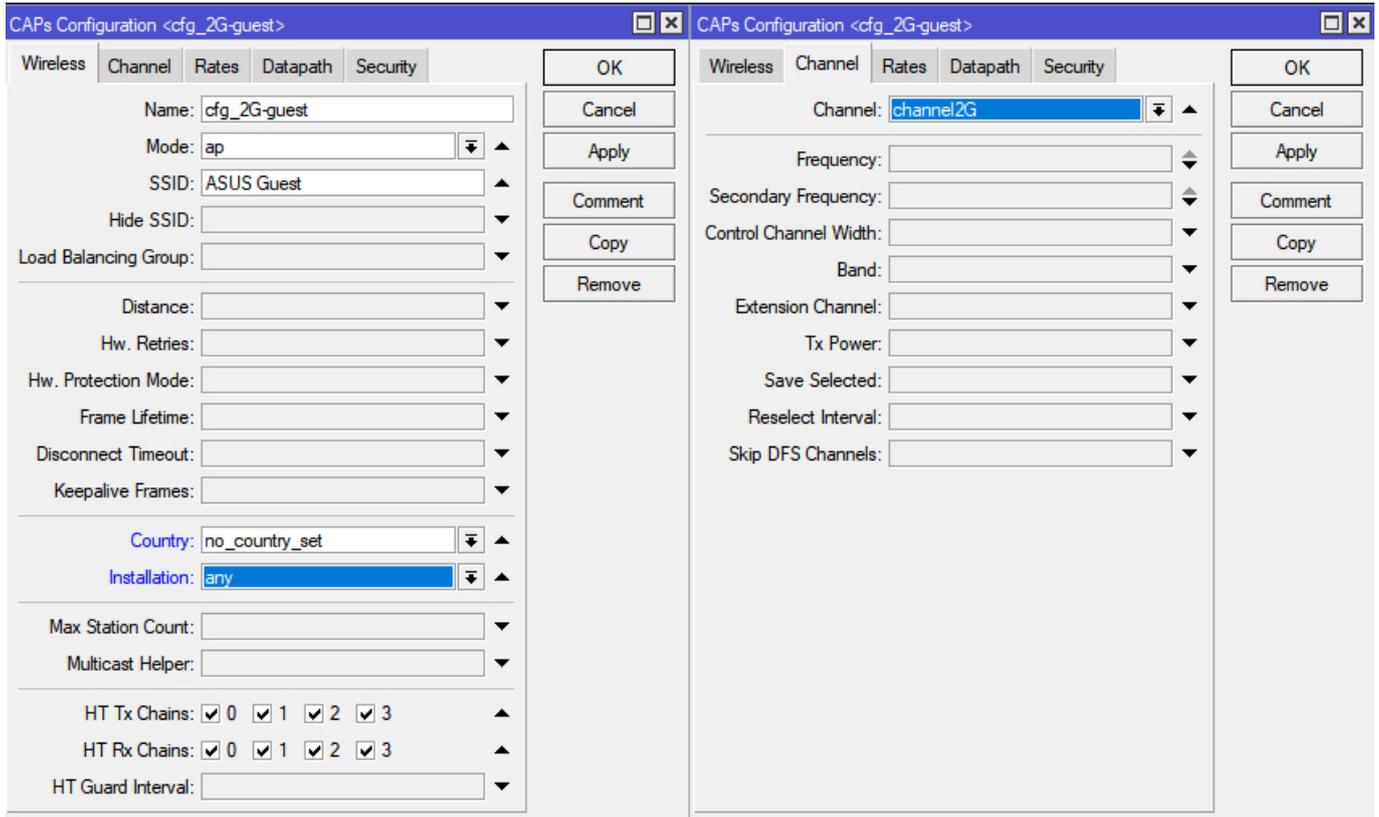
Local Forwarding:

Client To Client Forwarding:

VLAN Mode:

OK Cancel Apply Comment Copy Remove

Создаем конфигурацию



Переходим на вкладку Provisioning и корректируем конфигурацию для 2G добавив slave конфигурацию

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table

+ - ✓ ✗ 📄 🔍

#	Radio MAC	Identity Regexp	Common Nam...	Action	Master Configurati...	Slave Configuration
0	00:00:00:00:00:00			create dy...	cfg_5G	
1	00:00:00:00:00:00			create dy...	cfg_2G	

2 items (1 selected)

CAPs Provisioning <00:00:00:00:00:00>

Radio MAC: 00:00:00:00:00:00

Hw. Supported Modes: [dropdown]

Identity Regexp: [text]

Common Name Regexp: [text]

IP Address Ranges: [dropdown]

Action: create dynamic enabled

Master Configuration: cfg_2G

Slave Configuration: **cfg_2G-guest**

Name Format: prefix identity

Name Prefix: 2G

enabled

OK Cancel Apply Disable Comment Copy Remove

Далее в меню Remote CAP выделяем наши точки и нажимаем кнопку Provision

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table

- 🔍 Provision Upgrade Set Identity

Address	Name	Board	Serial	Version	Identity	Base MAC	State	Radios
127.0.0.1	[DC:2C:6E:...	RBD53IG-5H...	F34E0FA001EF	6.49.6	ASUS	DC:2C:6E:EC:01:B3	Run	2
2C:C8:1B:25:FE:D3	[2C:C8:1B:25:...	RB941-2nD	D1130EE49B...	6.49.6	Divan	2C:C8:1B:25:FE:D3	Run	1

2 items (2 selected)

В меню CAP Interface появится наш гостевой интерфейс как sub интерфейс основной точки. Это же видно и в меню WiFi Intefaces

Wireless Tables

WiFi Interfaces W60G Station Nstreme Dual Access List Registration Connect List Security Profiles Channel

+ - ✓ ✕ 📄 🗑️ CAP WPS Client Setup Repeater Scanner Freq. Usage Alignment

Name	Type	Actual MTU	Tx	Rx	Tx
-- managed by CAPsMAN					
-- channel: 2462/20-eC/gn(15dBm), SSID: ASUS, CAPsMAN forwarding					
XS wlan1	Wireless (IPQ4019)	1500	0 bps	0 bps	
-- managed by CAPsMAN					
-- SSID: ASUS Guest, CAPsMAN forwarding					
DX wlan3	Virtual	1500	0 bps	0 bps	
-- managed by CAPsMAN					
-- channel: 5280/20-eeCe/ac/DP(14dBm), SSID: ASUS-5G, CAPsMAN forwarding					
XS wlan2	Wireless (IPQ4019)	1500	0 bps	0 bps	

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote C

+ - ✓ ✕ 📄 🗑️ Reselect Channel Manager AAA

Name	Type	Actual MTU	L2 MTU	Tx	Rx
DRSMB 2G-ASUS-1	CAP Interface	1500	1600	7.9 kbps	
DSB 2G-ASUS-...	CAP Interface	32	1600	0 bps	
DRSMB 2G-Divan-1	CAP Interface	1500	1600	354.4 kbps	
DSB 2G-Divan-1-1	CAP Interface	32	1600	0 bps	
DRSMB 5G-ASUS-1	CAP Interface	1500	1600	7.9 kbps	

5 items out of 15

Запретим этим сетям общаться между собой.

IP → Route → Rules

Создаем два правила с Action drop

Route List

Routes Nexthops Rules VRF

+ - ✓ ✗ 📄 🗑️

#	Src. Address	Dst. Address	Routing Mark	Interface	Action
0	▶ 10.0.0.0/24	192.168.1.0/24			drop
1	▶ 192.168.1.0/24	10.0.0.0/24			drop

Policy Routing Rule <>

Src. Address: 192.168.1.0/24 ▲

Dst. Address: 10.0.0.0/24 ▲

Routing Mark: ▼

Interface: ▼

Action: drop ▼

Table: ▼

OK

Cancel

Apply

Disable

Comment

Copy

Remove

2 items enabled

Policy Routing Rule <>

Src. Address: 10.0.0.0/24 ▲

Dst. Address: 192.168.1.0/24 ▲

Routing Mark: ▼

Interface: ▼

Action: drop ▼

Table: ▼

OK

Cancel

Apply

Disable

Comment

Copy

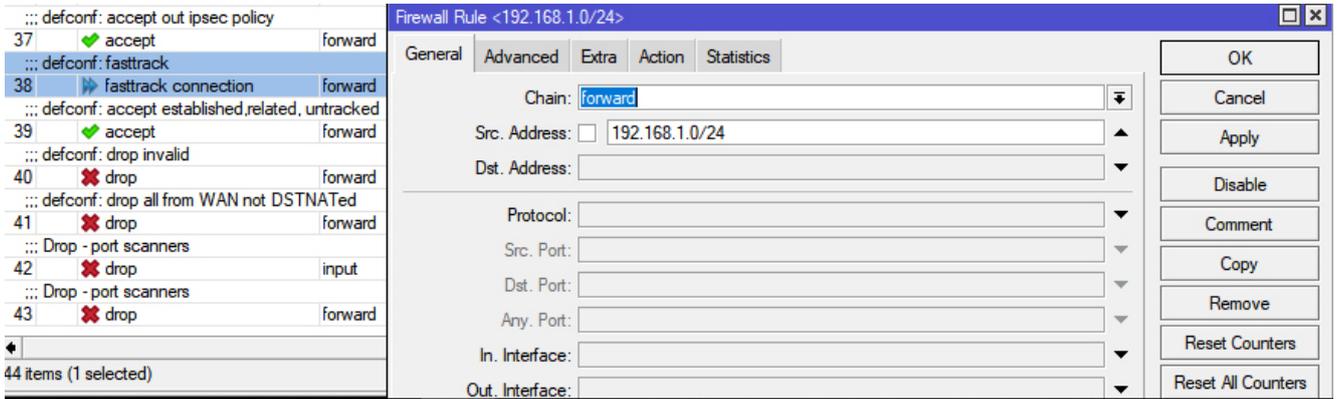
Remove

enabled

Следующий шаг – ограничим скорость гостевой сети. Для этого нужно изменить правило firewall fasttrack

и настроить очереди.

IP → Firewall

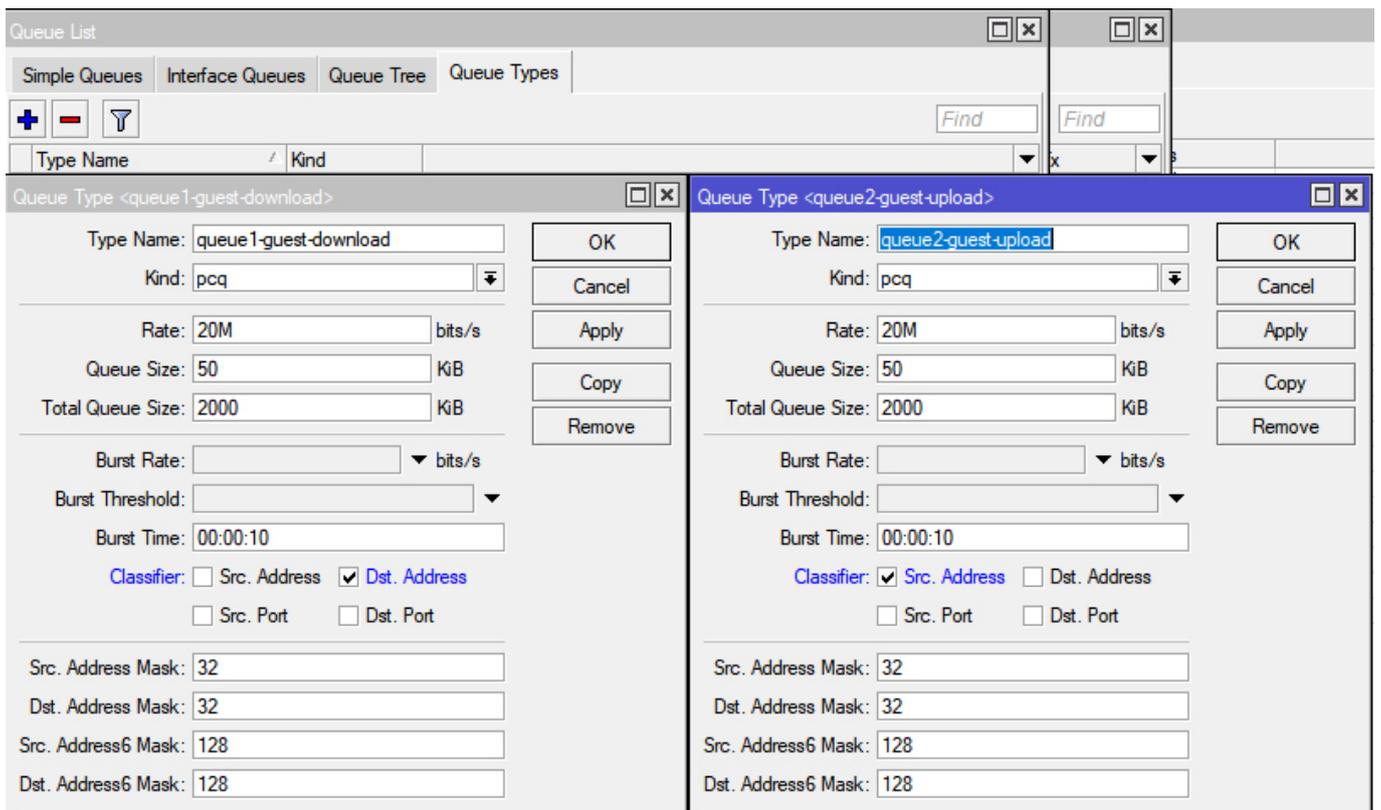


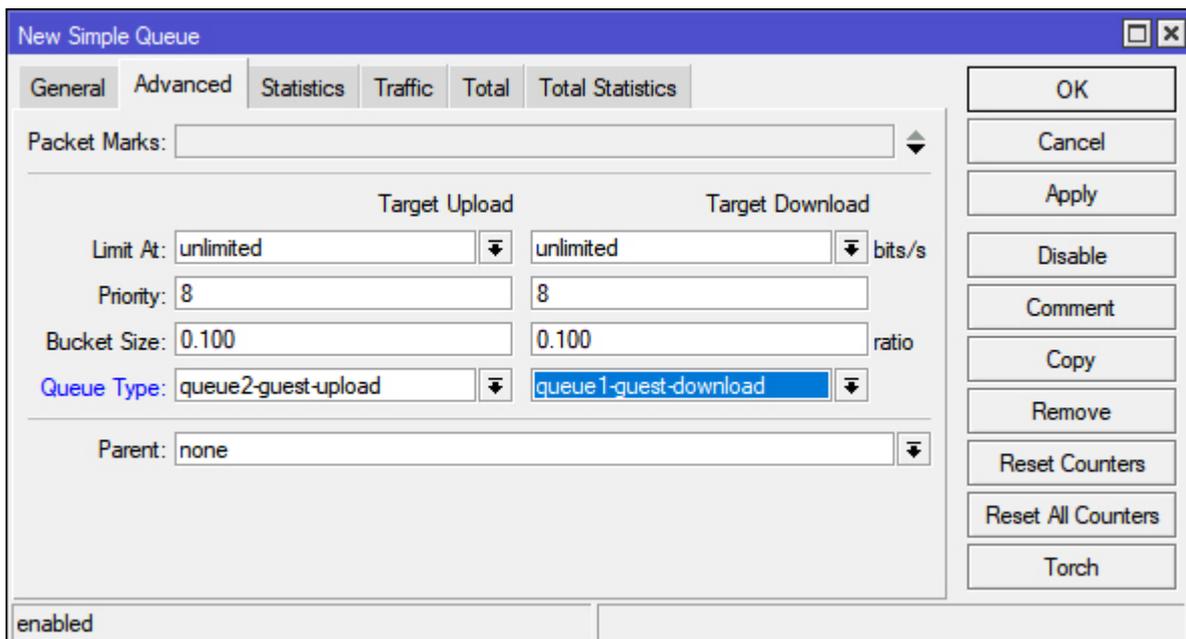
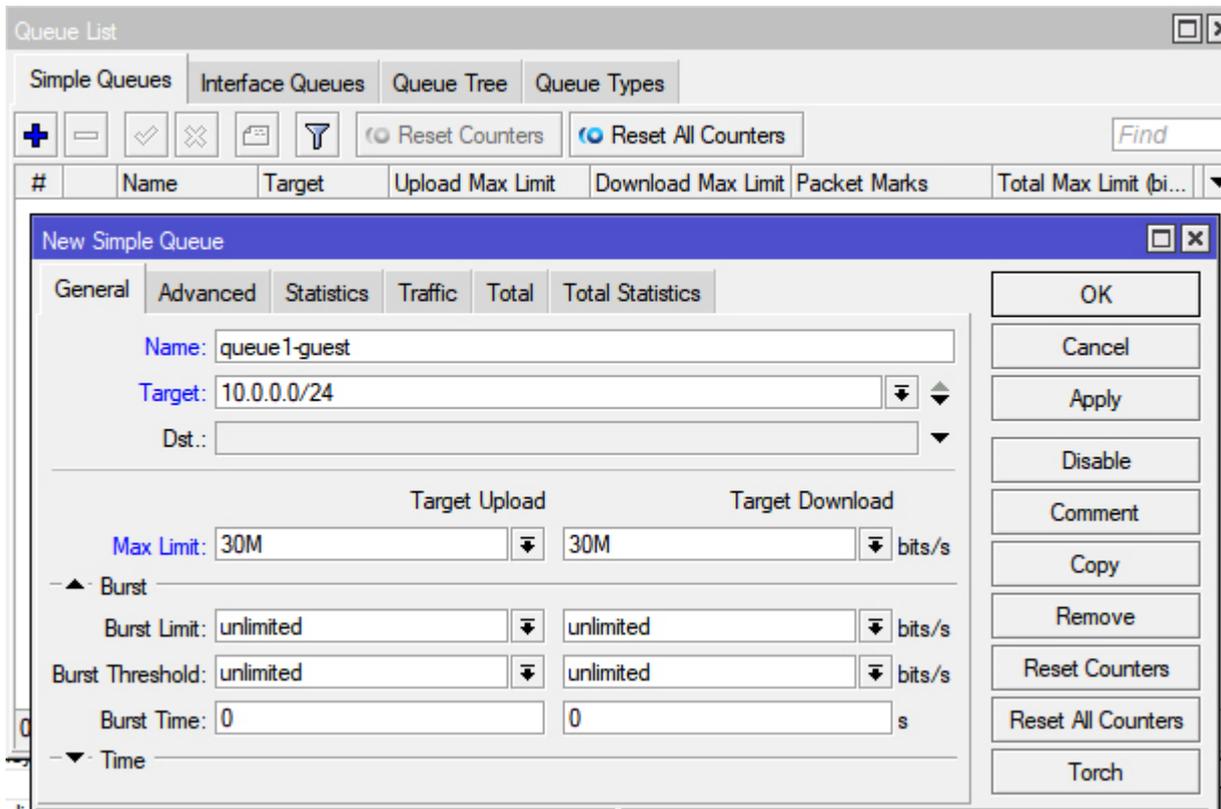
Этим правилом мы говорим, что fasttrack будет работать только в нашей сети, но не в гостевой.

Делаем ограничения.

Queues → Queu Types

Создаем два ограничения на download и upload





Подключаемся и проверяем.