

## MỤC LỤC

MỤC LỤC .....	1
BÀI 1. CÁC LỆNH CLI VÀ MỘT SỐ THAO TÁC THƯỜNG DÙNG .....	4
BÀI 2. ĐỊA CHỈ IP VÀ MỘT SỐ CÀI ĐẶT CƠ BẢN.....	5
BÀI 3. ĐIỀU HƯỚNG MẠNG LAN RA WAN TUỖ Ý .....	6
1. Mô hình mạng: .....	6
2. Thực hành: .....	6
2.1. Cách 1: sử dụng phương pháp danh sách Address List .....	6
2.2. Cách 2: sử dụng phương pháp In. Interface .....	9
BÀI 4. VLAN VÀ TRUNKING .....	10
1. Mô hình mạng: .....	10
2. Thực hành: .....	10
2.1. Trên Router: .....	10
2.2. Trên Switch: .....	13
3. Kiểm tra: .....	17
BÀI 5. LINK AGGREGATION CONTROL PROTOCOL 802.3ad.....	18
1. Lý thuyết: .....	18
2. Mô hình mạng: .....	19
3. Thực hành: .....	19
3.1. Trên Router .....	19
3.2. Trên Switch: .....	22
BÀI 6. VLAN MANAGEMENT .....	27
1. Giới thiệu: .....	27
2. Mô hình mạng: .....	27
3. Thực hành: .....	27
3.1. Trên router:.....	27

3.2. Trên switch:.....	28
<b>BÀI 7. FIREWAL CƠ BẢN .....</b>	<b>31</b>
1. Yêu cầu: .....	31
2. Thực hiện trên router.....	31
<b>BÀI 8. CÂN BẰNG TẢI VỚI PHƯƠNG PHÁP PER CONNECTION CLASSIFIER VÀ FAIL OVER.....</b>	<b>35</b>
1. Giới thiệu: .....	35
2. Mô hình mạng .....	35
3. Thực hành .....	35
3.1. Cấu hình cân bằng tải và fail over bằng dòng lệnh.....	35
3.2. Cấu hình cân bằng tải bằng giao diện .....	38
3.3. Cho phép một lớp mạng không qua cân bằng tải:.....	40
3.4. NAT một địa chỉ IP/dịch vụ đi vào/ra đường internet được chỉ định	<b>Error!</b>
<b>Bookmark not defined.</b>	
<b>BÀI 9. NAT .....</b>	<b>42</b>
1. Giới thiệu: .....	42
2. Mô hình mạng .....	42
3. Thực hành .....	43
3.1. NAT để truy cập internet.....	43
3.2. NAT port .....	45
3.3. Hairpin NAT .....	47
<b>BÀI 10. DHCP SNOOPING .....</b>	<b>48</b>
1. Mô hình mạng .....	48
2. Thực hành .....	48
<b>BÀI 11. CÀI ĐẶT QOS .....</b>	<b>Error! Bookmark not defined.</b>
1. Giới thiệu .....	49
2. Mô hình mạng:.....	49

3.	Thực hành .....	49
3.1.	Giới hạn băng thông cho một địa chỉ IP .....	49
3.2.	Giới hạn băng thông cho một lớp mạng.....	50
3.3.	Giới hạn băng thông bằng script .....	52
BÀI 12.	VPN L2TP/IPSec.....	54
1.	Giới thiệu: .....	54
2.	Mô hình mạng:.....	54
3.	Thực hành: .....	54

## **BÀI 1. CÁC LỆNH CLI VÀ MỘT SỐ THAO TÁC THƯỜNG DÙNG**

- Bật romon: `tool romon set enabled=yes`
- Đặt tên cho router: `system identity set name=CoreRouter`
- In địa chỉ IP: `ip add print`
- Cho phép nhận DHCP: `ip dhcp-client add interface=ether1 disable=no`
- Set địa chỉ IP: `ip address add address=192.168.10.1/24 interface=ether1`
- Trích xuất file script: `export file=myconfig`
- Cập nhật firmware: `IP >> Package >> Check For Updates`

## **BÀI 2. ĐỊA CHỈ IP VÀ MỘT SỐ CÀI ĐẶT CƠ BẢN**

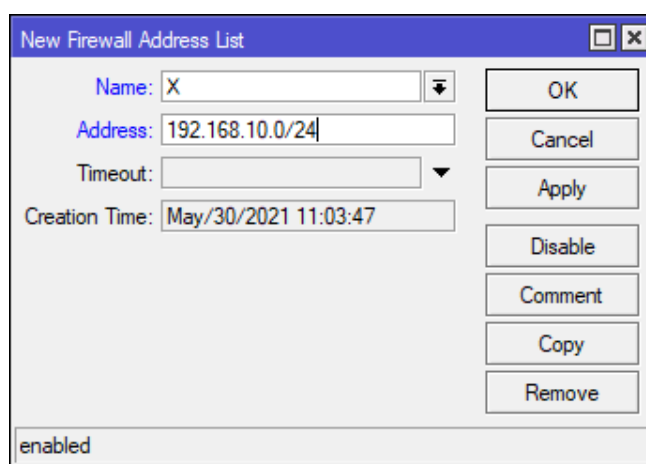
## BÀI 3. ĐIỀU HƯỚNG MẠNG LAN RA WAN TỰ Ý

### 1. Mô hình mạng:

### 2. Thực hành:

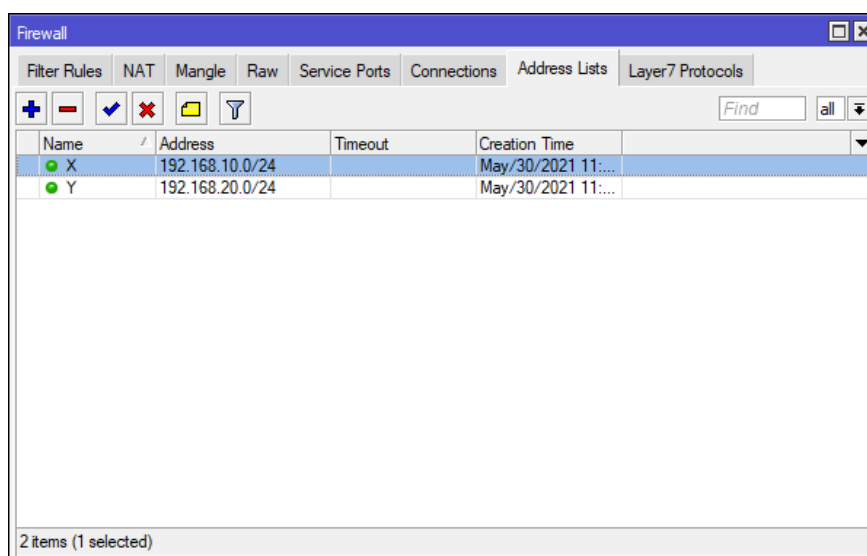
#### 2.1. Cách 1: sử dụng phương pháp danh sách Address List

- **Bước 1:** Vào IP >> Firewall, tại tab Address Lists bấm dấu + để bắt đầu thêm danh sách địa chỉ mới.
  - o Name: đặt tên cho danh sách.
  - o Address: có thể là 1 địa chỉ IP, một đoạn, hoặc một lớp mạng.



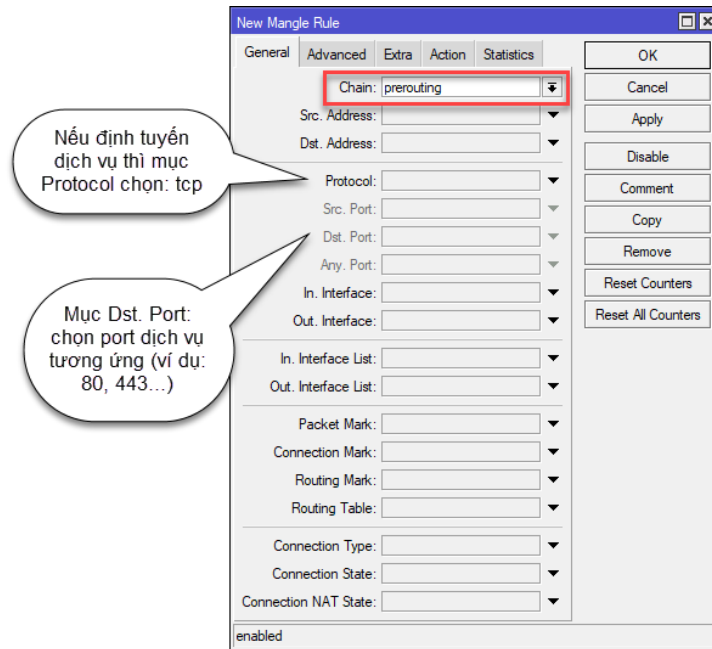
**Hình 3.1.** Cửa sổ tạo Address List

Sau khi tạo xong, tab Address List có dạng như sau:



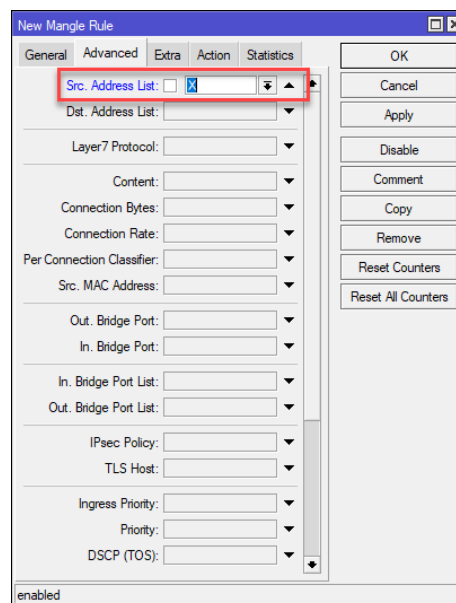
**Hình 3.2.** Tab address list sau khi tạo xong danh sách địa chỉ.

- **Bước 2:** vẫn trong cửa sổ Firewall, vào tab Mangle, bấm dấu + để thêm luật Mangle mới.
- **Bước 3:** tại màn hình New Mangle Rule, tab General, mục Chain: chọn prerouting. Ta còn có thể định tuyến cho dịch vụ mạng bằng cách chọn mục Protocol và chọn Dst. Port là port dịch vụ tương ứng.



Hình 3.3. Tab general của New Mangle Rule

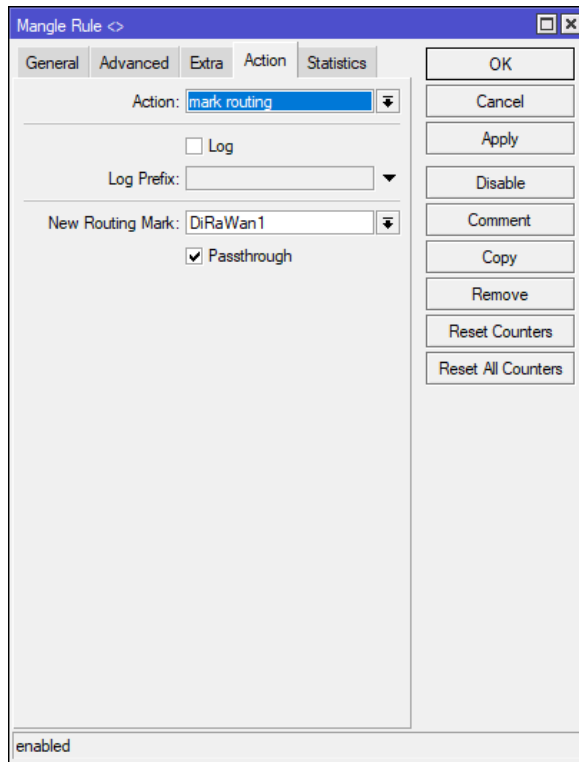
- **Bước 4:** trong tab Advanced, mục Src. Address List: chọn tên của danh sách địa chỉ đã tạo ở bước 1.



Hình 3.4. Tab advanced của New Mangle Rule

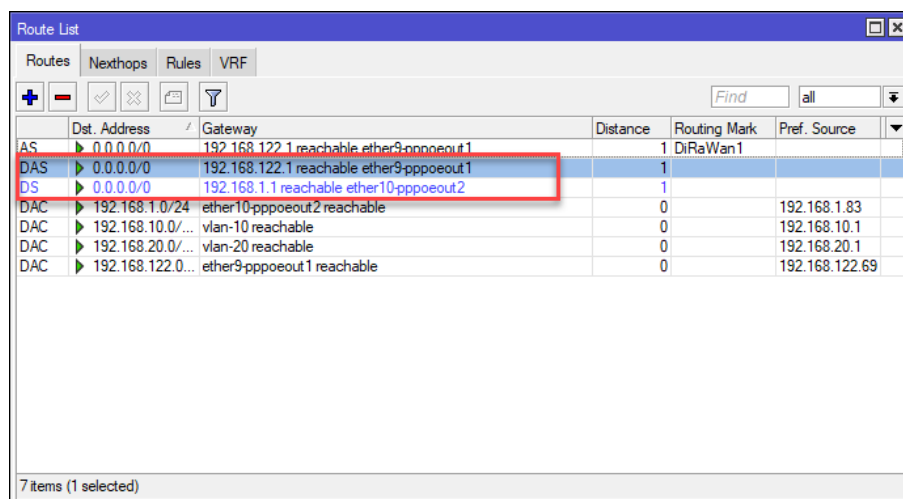
- **Bước 5:** trong tab Action,

- Mục Action: chọn mark routing.
- Mục New Routing Mark: đánh dấu đường đi ra WAN mong muốn (đặt tên là “DiRaWan1”)
- Check vào ô Passthrough



**Hình 3.5.** Tab action của cửa sổ Mangle Rule

- **Bước 6:** vào IP >> Route, bấm kép vào đường WAN mong muốn cho danh sách đánh dấu đi ra, chọn copy.

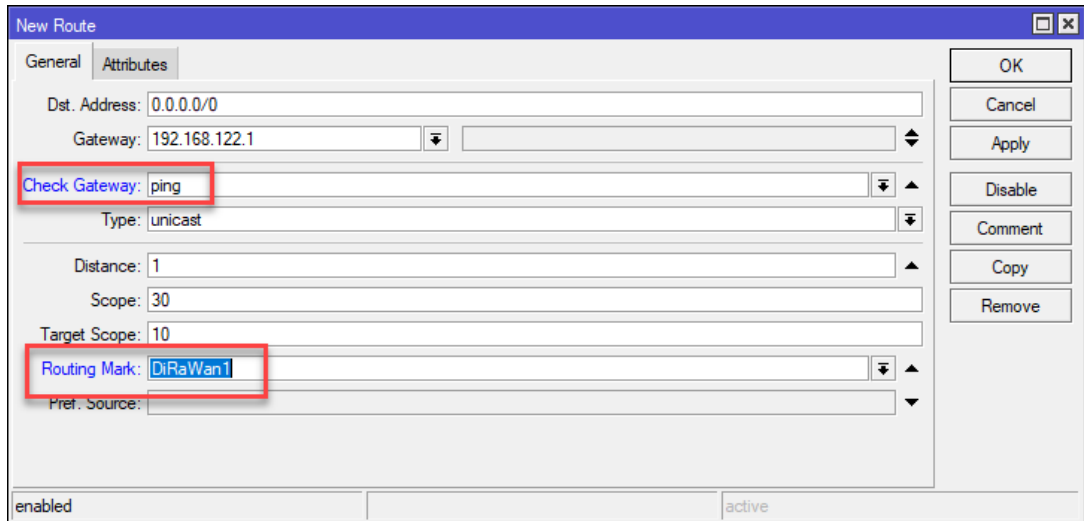


**Hình 3.6.** Cửa sổ Route List

- **Bước 7:** trong cửa sổ New Route,
  - Check Gateway: chọn mục ping



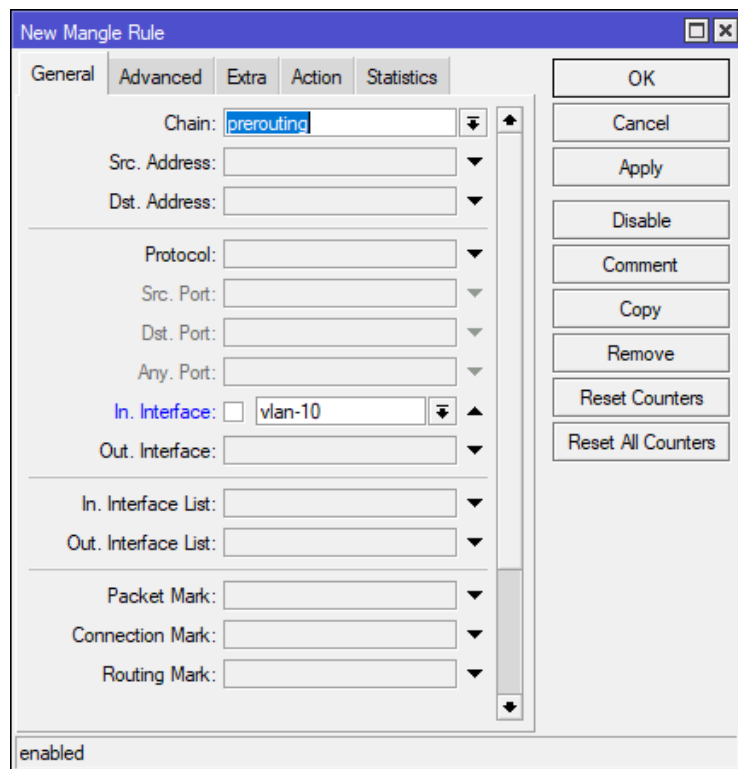
- Routing Mark: chọn đường đánh dấu đã đặt tên ở bước 5 (DiRaWan1)



**Hình 3.7.** Màn hình New Route

## 2.2. Cách 2: sử dụng phương pháp In. Interface

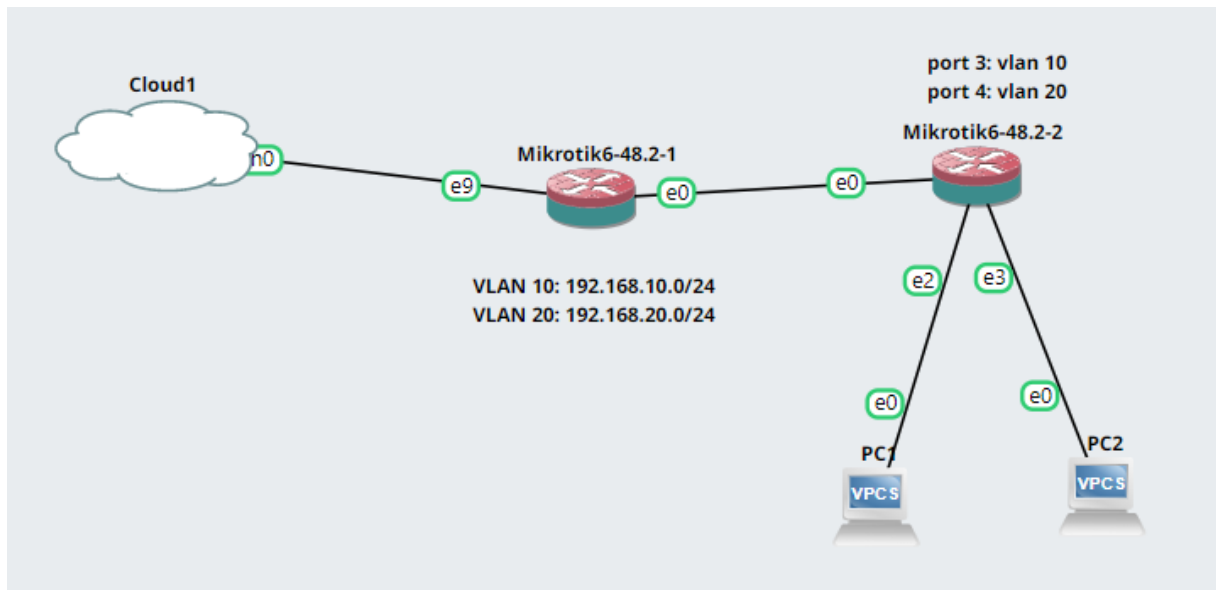
- Trong cửa sổ New Mangle Rule, tab General,
  - Mục Chain: chọn prerouting
  - Mục In. Interface: chọn interface mong muốn.



**Hình 3.8.** Sử dụng In. Interface để điều hướng mạng lan

## BÀI 4. VLAN VÀ TRUNKING

### 1. Mô hình mạng:

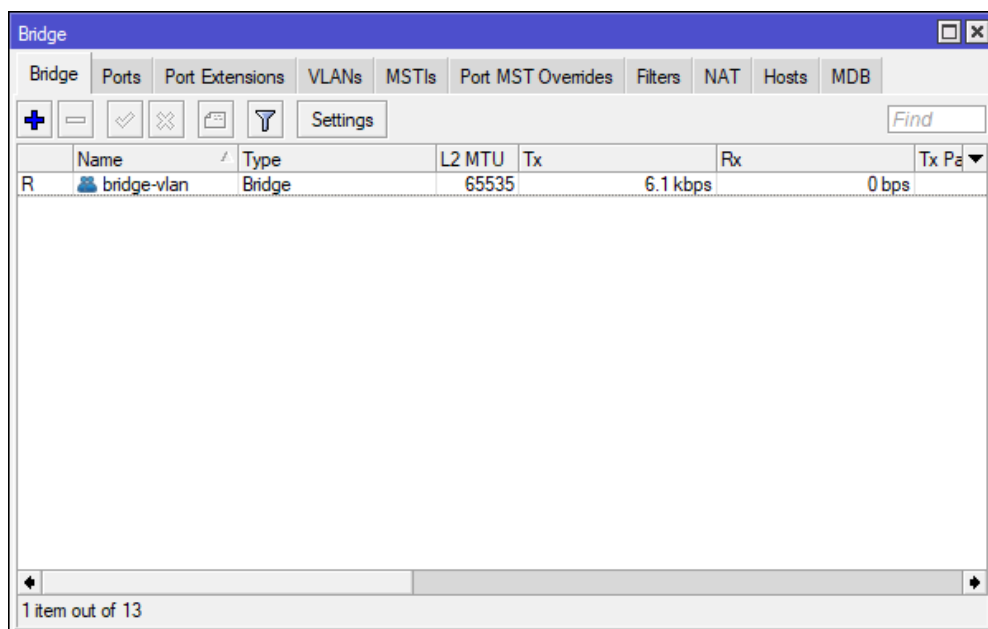


Hình 4.1. Mô hình mạng vlan và trunking trên mikrotik

### 2. Thực hành:

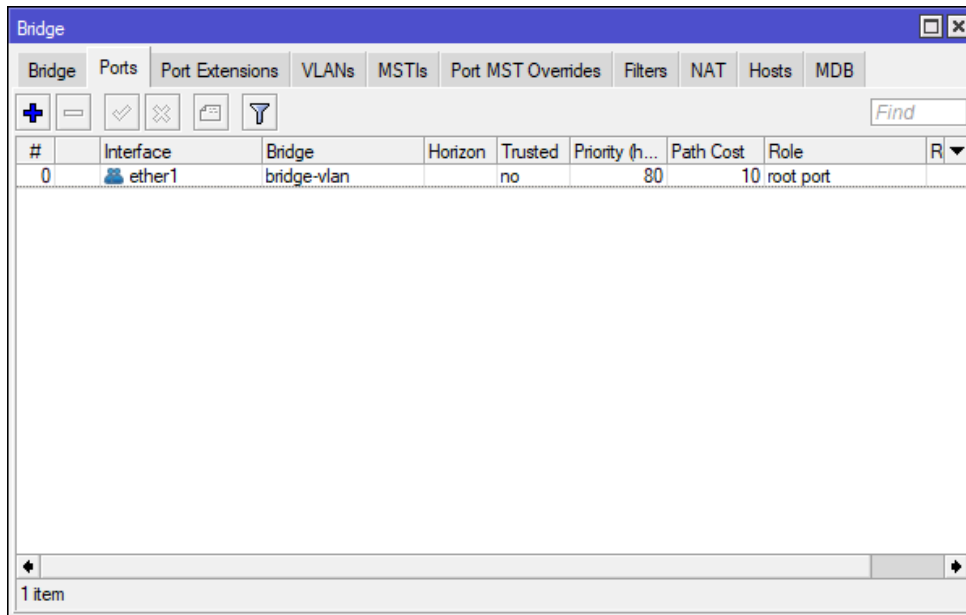
#### 2.1. Trên Router:

- **Bước 1:** Vào Bridge, tạo bridge-vlan



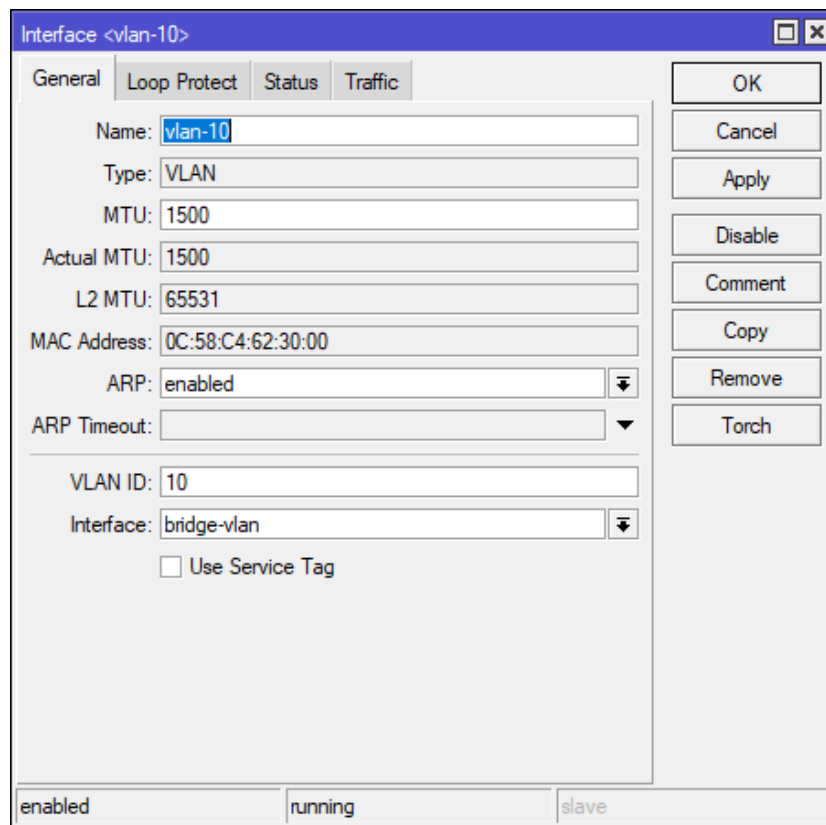
Hình 4.2. Tạo bridge-vlan

- **Bước 2:** Trong cửa sổ Bridge, vào tab Ports, thêm port ether 1 làm port trunk vào bridge-vlan.



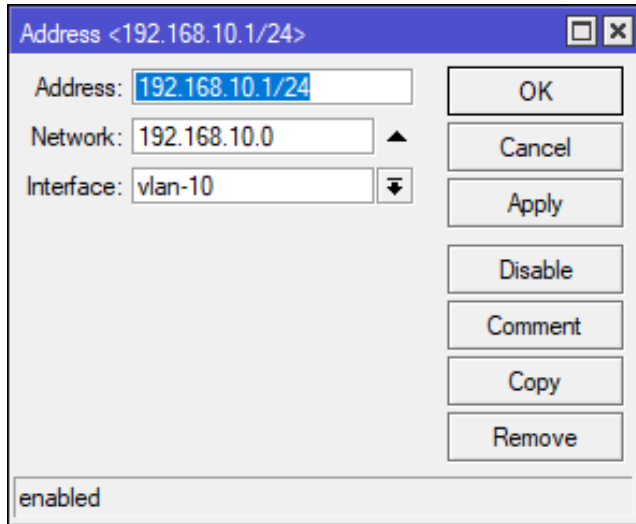
**Hình 4.3.** Thêm port ether1 làm port trunk vào bridge-vlan

- **Bước 3:** Vào Interfaces >> VLAN, tạo ra các VLAN và gán các VLAN này vào Interface bridge-vlan đã tạo ở bước 1.
  - o Name: nhập tên đại diện vlan
  - o VLAN ID: nhập số ID của vlan
  - o Interface: bridge-vlan



**Hình 4.4.** Tạo ra các vlan và gán vào Interface bridge-vlan

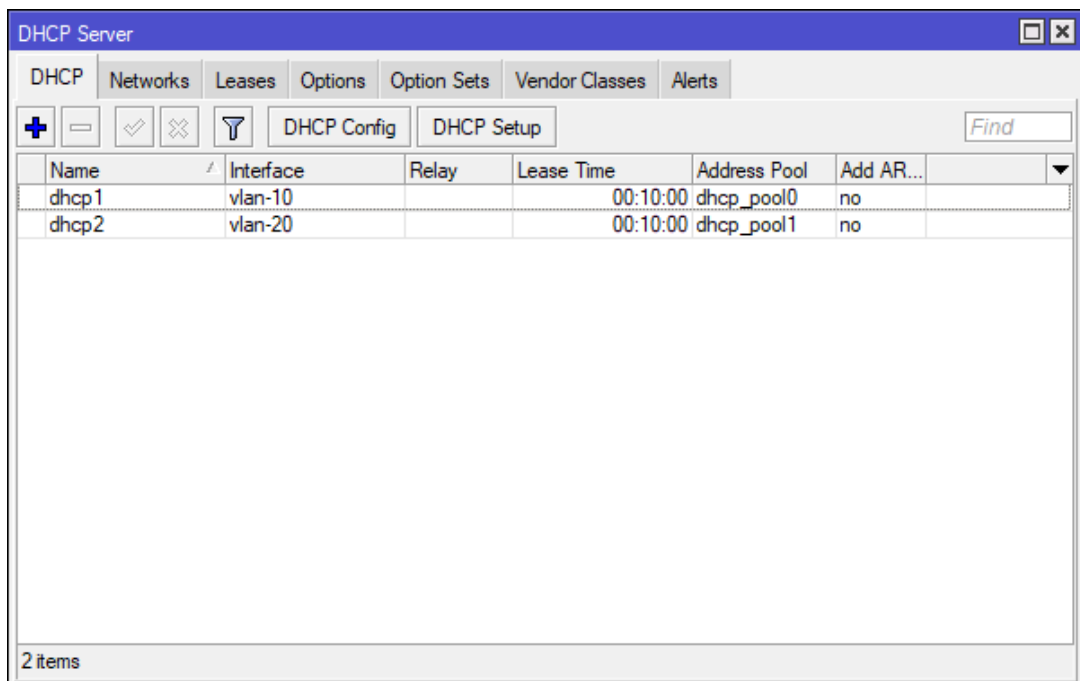
- **Bước 4:** Vào IP >> Address, gán địa chỉ IP cho các VLAN vừa tạo.
  - o Address: địa chỉ ip của vlan
  - o Network: lớp mạng
  - o Interface: chọn vlan



**Hình 4.5.** Gán địa chỉ IP cho VLAN

**Hình 4.6.** Tạo địa chỉ ip của vlan và gán vào interface vlan tương ứng.

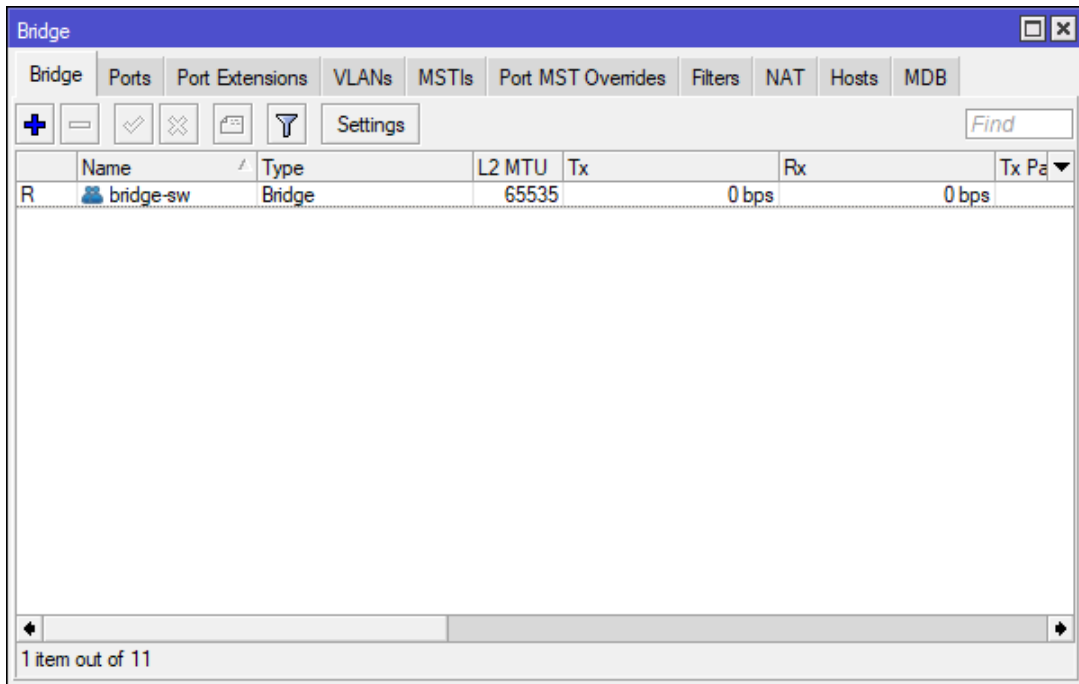
- **Bước 5:** Vào IP >> DHCP Server, bấm vào nút DHCP Setup, lần lượt tạo DHCP Server cấp địa chỉ IP cho các vlan.



**Hình 4.7.** Tạo DHCP Server cấp địa chỉ IP cho các vlan

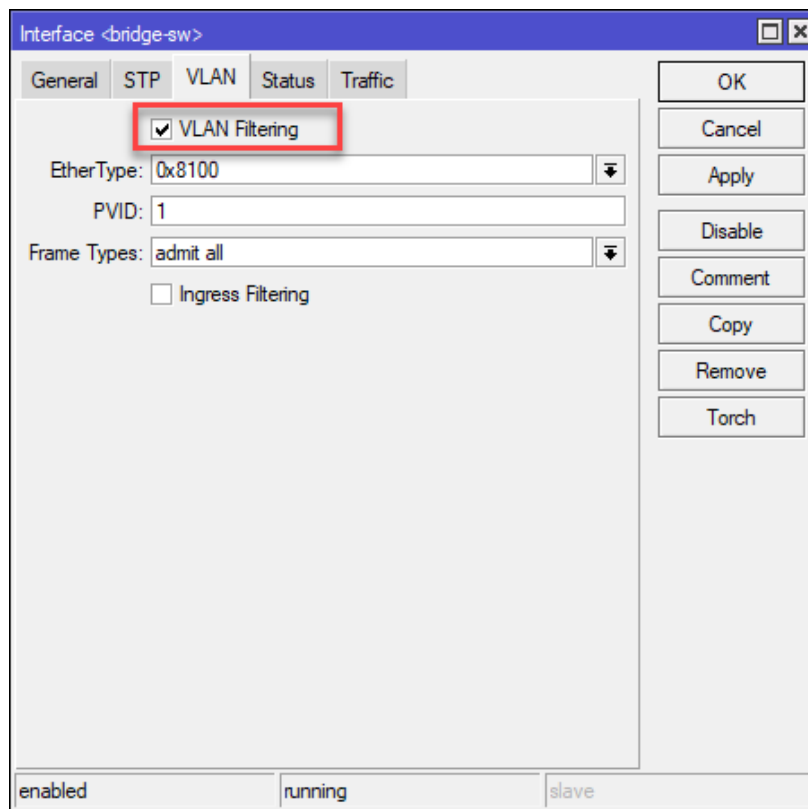
## 2.2. Trên Switch:

- **Bước 1:** Vào Bridge, tạo bridge-sw.



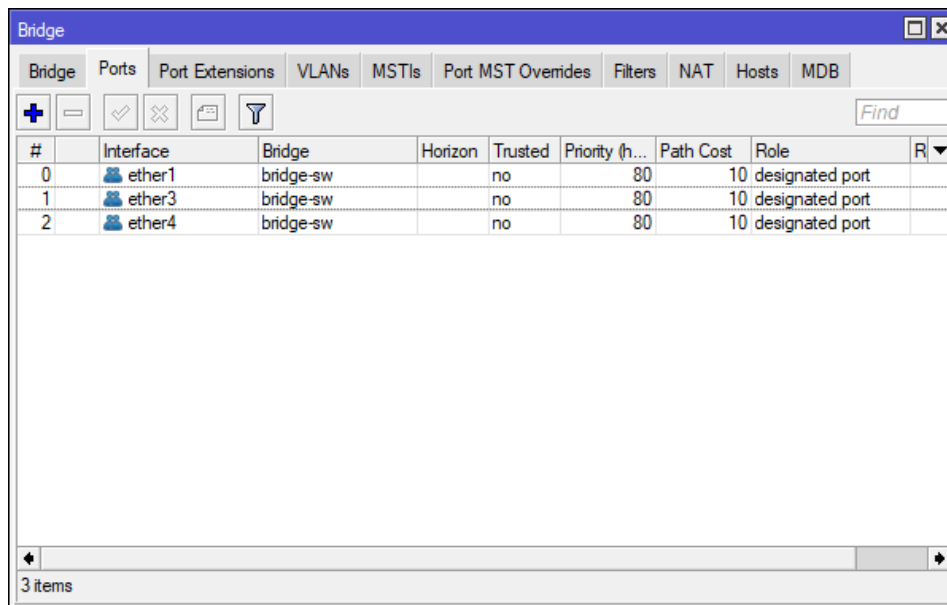
**Hình 4.8.** Tạo bridge-sw

- **Bước 2:** Bấm kép vào bridge-sw vừa tạo, vào tab VLAN, check vào ô “VLAN Filtering”. Các mục còn lại để mặc định.



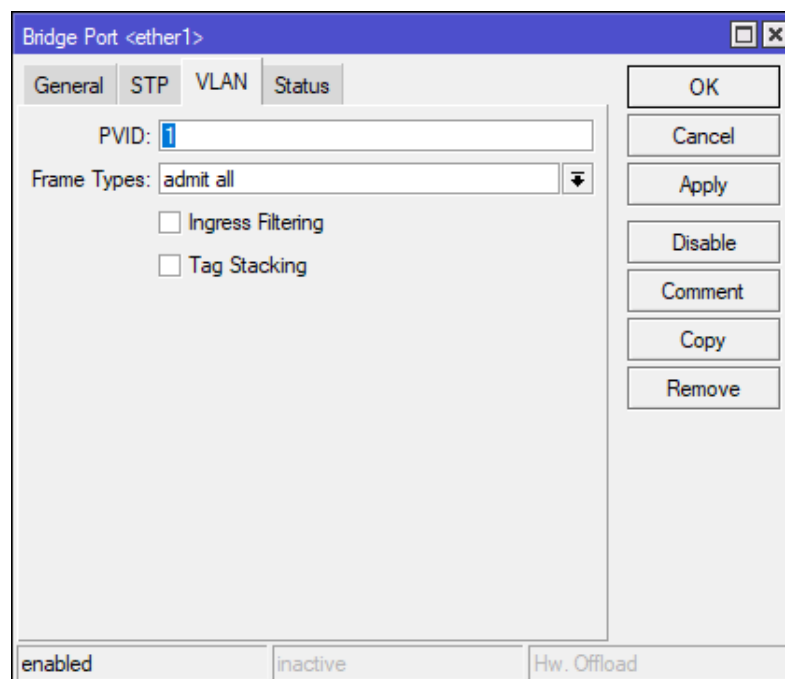
**Hình 4.9.** Check vào ô “VLAN Filtering”

- **Bước 3:** Trong cửa sổ Bridge, vào tab Ports, thêm vào các port có liên quan đến VLAN, kể cả port ether1 là port trunk



**Hình 4.10.** Thêm các port có liên quan đến vlan

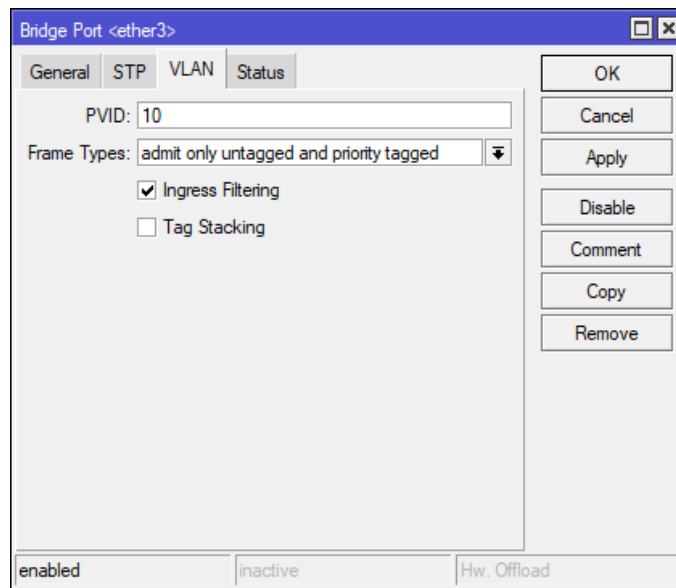
- **Bước 4:** Vẫn trong tab Ports, gán vlan vào port bằng cách bấm kép vào từng port. Đối với port ether 1 là port trunk, tại tab VLAN của port này, ta để mặc định và không chỉnh sửa.



**Hình 4.11.** Port trunk ether1, trong tab VLAN để mặc định.

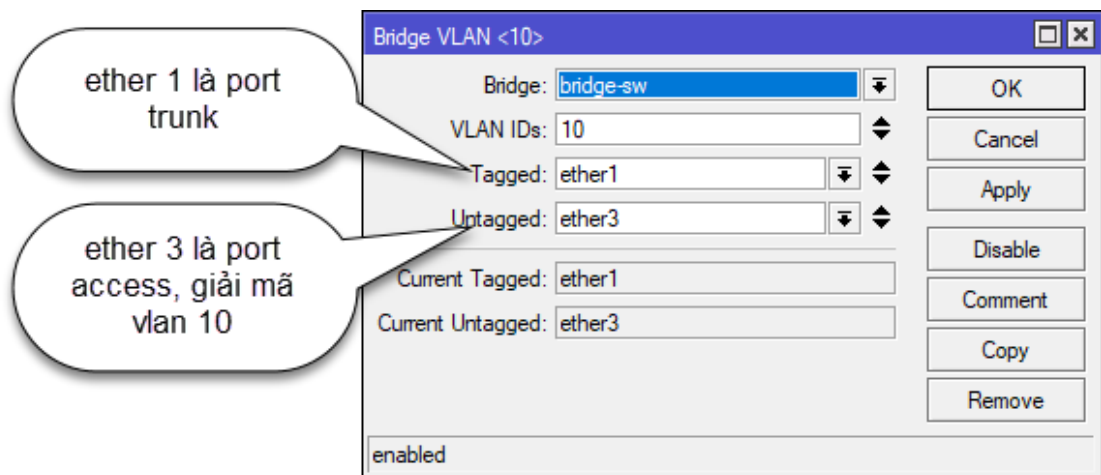
- **Bước 5:** Vẫn trong tab Ports, tiếp tục bấm kép vào các port còn lại, vào tab VLAN của port đó:

- Mục PVID: gán vlan tương ứng.
- Mục Frame Types: chọn admit only untagged and priority tagged.
- Check vào ô Ingress Filtering



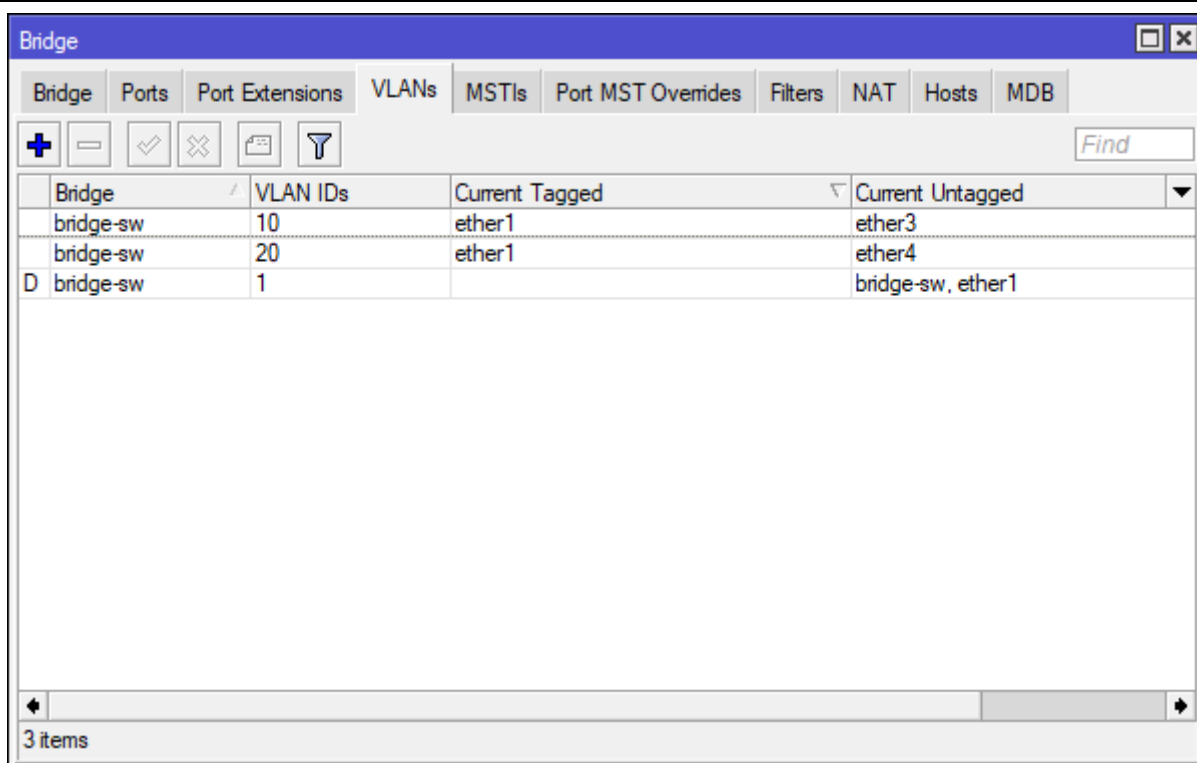
**Hình 4.12.** Cấu hình cho port access (port giải mã vlan)

- **Bước 6:** Trong cửa sổ Bridge, vào tab VLANs,
  - Bridge: bridge-sw
  - VLAN IDs: nhập vào ID của vlan
  - Tagged: port làm port trunk
  - Untagged: port giải mã vlan



**Hình 4.13.** Cấu hình cho vlan đi qua port trunk và port access

Tiếp tục thực hiện với các vlan còn lại. Sau khi làm xong ta có bảng VLANs như sau:



The screenshot shows the Mikrotik WinBox interface for the Bridge VLANs configuration. The 'VLANs' tab is selected, and a table displays the current configuration. The table has four columns: Bridge, VLAN IDs, Current Tagged, and Current Untagged. There are three entries in the table.

Bridge	VLAN IDs	Current Tagged	Current Untagged
bridge-sw	10	ether1	ether3
bridge-sw	20	ether1	ether4
D bridge-sw	1		bridge-sw, ether1

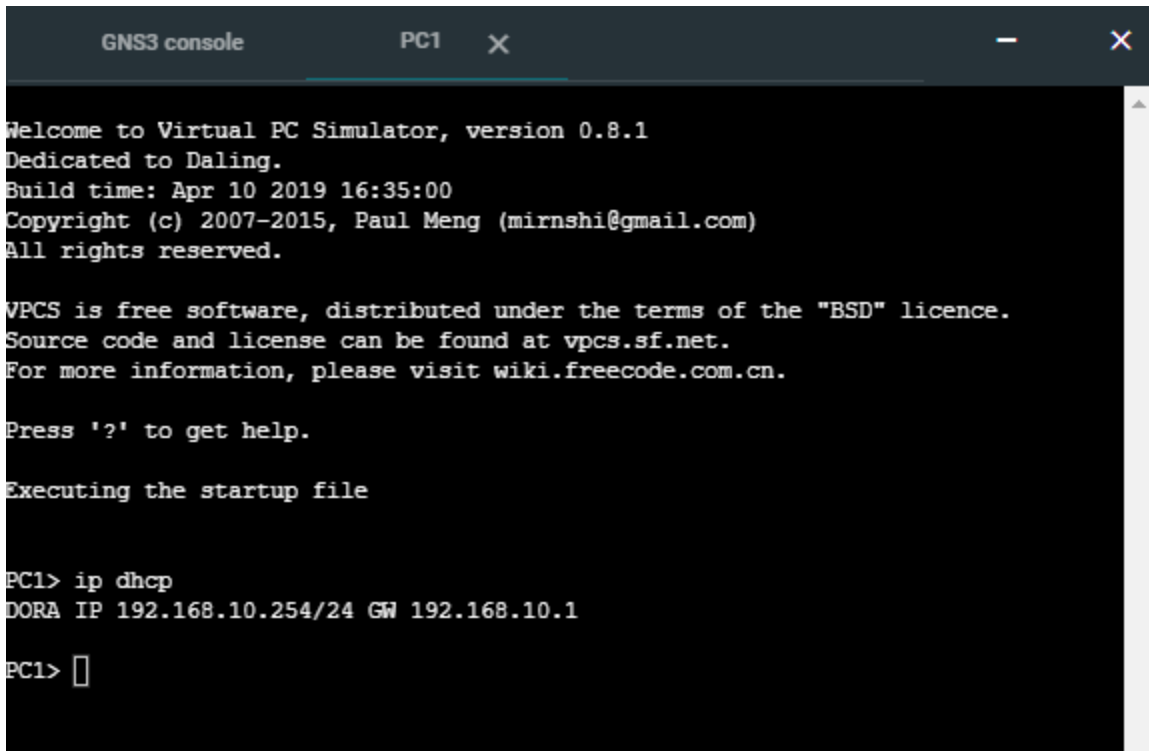
3 items

**Hình 4.14.** Bảng VLANs



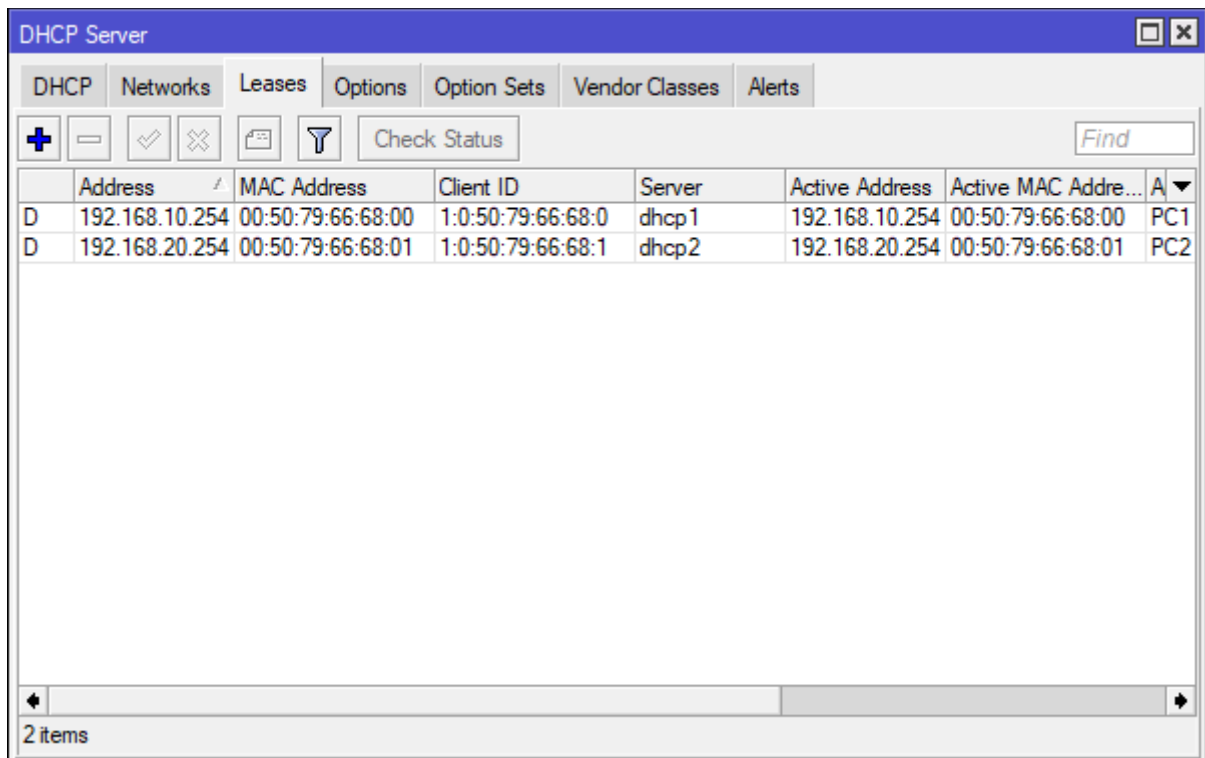
### 3. Kiểm tra:

Trên Pc1, vào web console gõ lệnh ip dhcp, nếu nhận được ip thì thành công.



**Hình 4.15.** Kiểm tra trên Pc1

Trong Core Router, cửa sổ DHCP Server tại tab Leases, sẽ thấy có IP cấp cho PC1.



**Hình 4.16.** IP cấp cho Pc1

## **BÀI 5. LINK AGGREGATION CONTROL PROTOCOL 802.3ad**

### **1. Lý thuyết:**

Khi mà dữ liệu truyền tải quá lớn đến nỗi đường truyền không đáp ứng được thì thay vì ta phải nâng cấp hay mua thiết bị mới thì ta sẽ nghĩ tới việc mở thêm nhiều kết nối dây giữa các Switch để cân bằng tải dữ liệu.

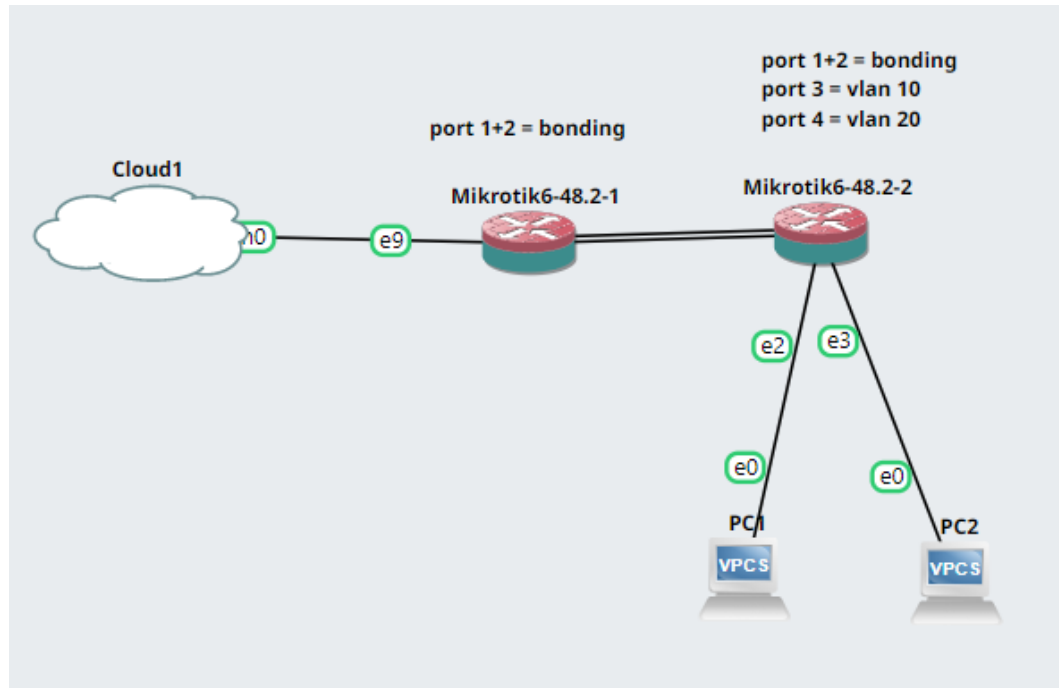
Ví dụ: Ta có hai Switch đang kết nối với nhau bằng cổng Fast Ethernet 100 Mbit trong khi các PC Host kết nối Switch thì dùng cổng Fast với băng thông 1000 Mbit. Hiển nhiên khi mà PC muốn truyền tải một lượng lớn dữ liệu hơn 100 Mbit đi thì tại Switch sẽ xảy ra hiện tượng nghẽn Traffic, các gói tin trong hàng đợi khi quá ngưỡng Cache thì sẽ bị Drop bỏ.

LACP (Link Aggregation Control Protocol): là giao thức cấu hình EtherChannel chuẩn quốc tế IEEE 802.3ad và có thể dùng được cho hầu hết các thiết bị thuộc các hãng khác nhau, LACP hỗ trợ ghép tối đa 16 Link vật lý thành một Link luận lý (8 Port Active – 8 Port Passive).

LACP có 3 chế độ:

- On: Chế độ cấu hình EtherChannel tĩnh, chế độ này thường không được dùng vì các Switch cấu hình EtherChannel có thể hoạt động được và cũng có thể không hoạt động được vì các Switch được cấu hình bằng tay phục thuộc vào con người nên hoàn toàn không có bước thương lượng trao đổi chính sách giữa bên dẫn đến khả năng Loop cao và bị STP Block.
- Active: Chế độ tự động – Tự động thương lượng với đối tác
- Passive: Chế độ bị động – Chờ được thương lượng

## 2. Mô hình mạng:

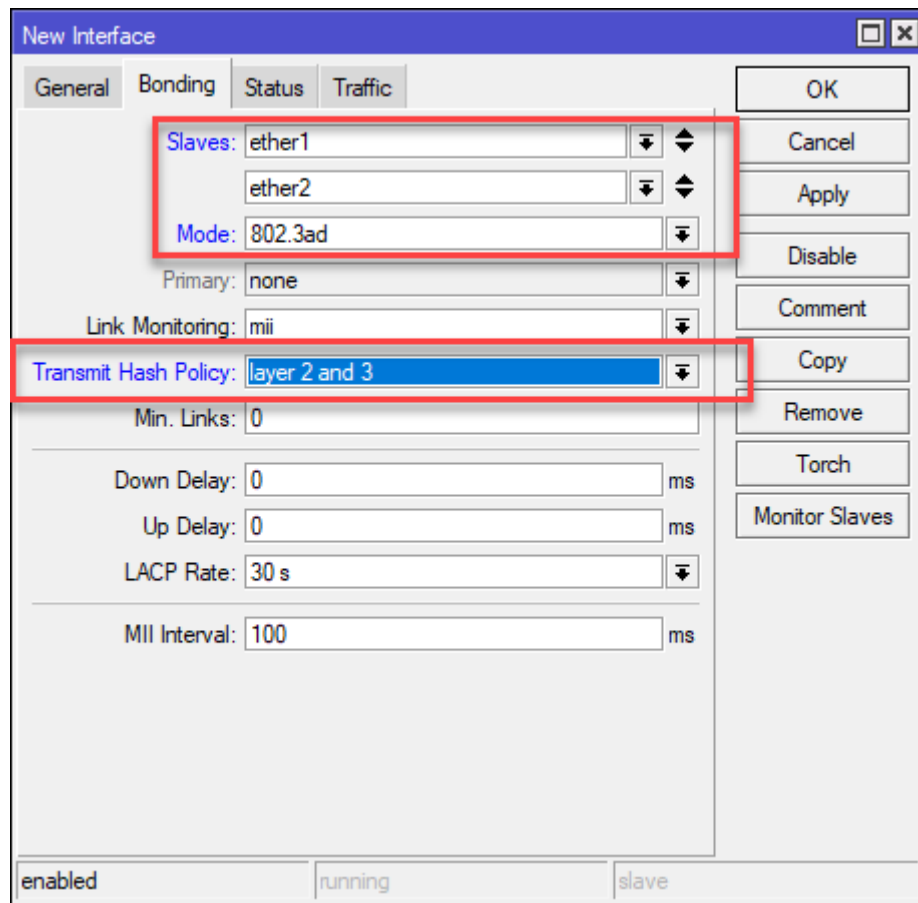


**Hình 5.1.** Mô hình mạng kết hợp bonding và vlan trunking trên mikrotik

## 3. Thực hành:

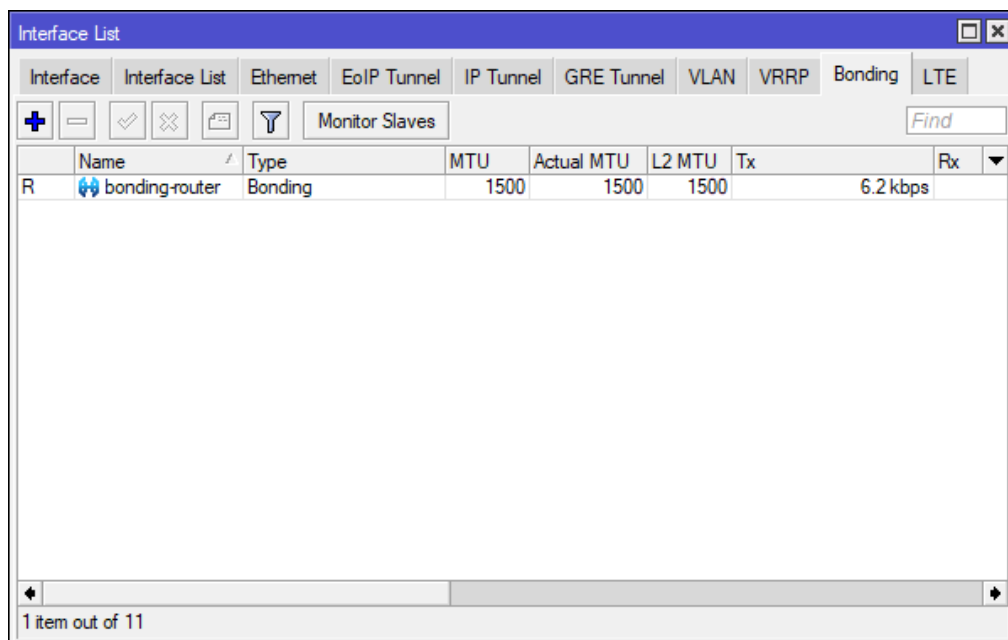
### 3.1. Trên Router

- **Bước 1:** Vào Interfaces >> Bonding, tạo bonding-router, thêm port ether1 và ether 2 vào bonding-router.
  - o Slaves: ether1 và ether 2
  - o Mode: 802.3ad
  - o Transmit Hash Policy: layer 2 and 3



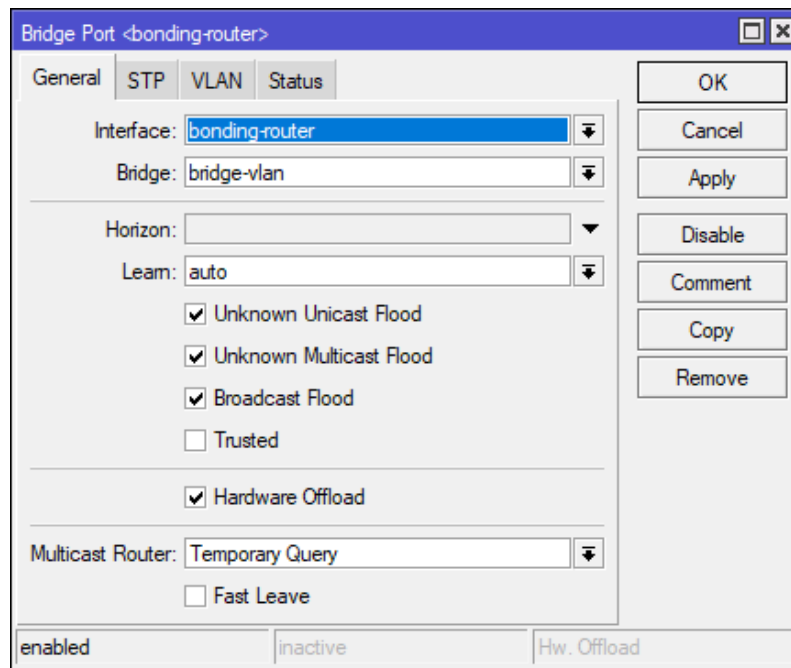
**Hình 5.2.** Thêm port vào bonding

Kết quả sau khi tạo bonding-router:



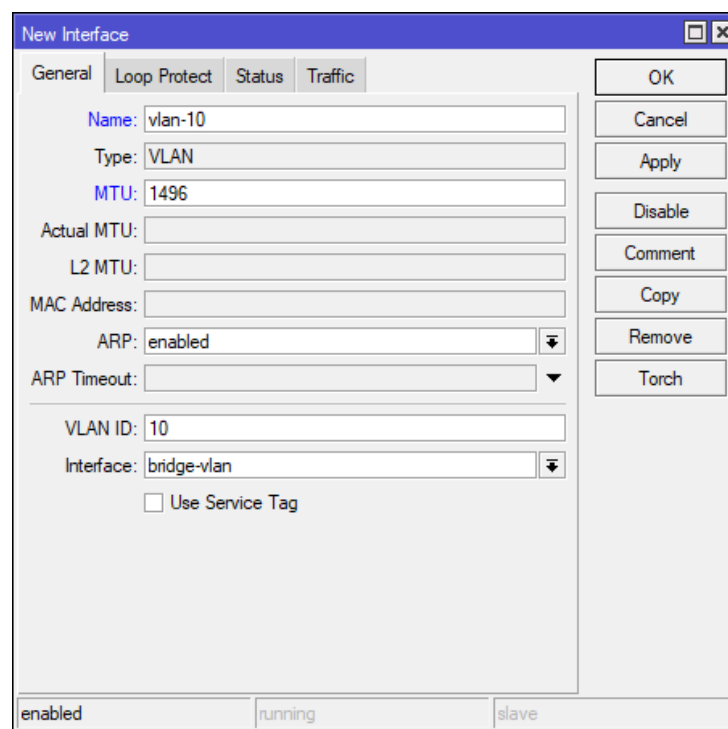
**Hình 5.3.** Bảng bonding

- **Bước 2:** Trong cửa sổ Bridge, tạo bridge-vlan. Vào tab Ports, thêm port bonding-router làm port trunk vào bridge-vlan.



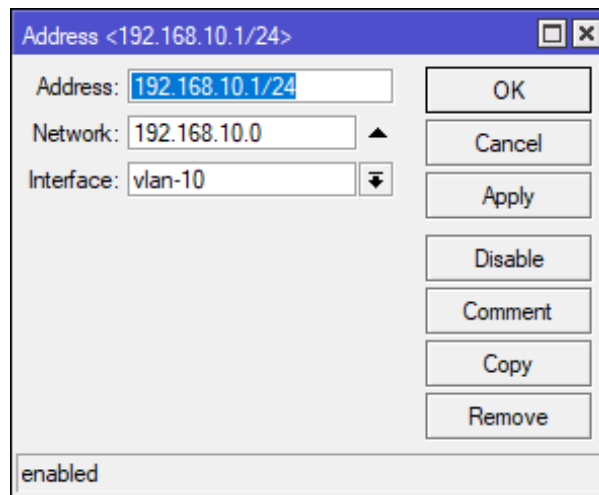
**Hình 5.4.** Thêm port bonding-trunk làm port trunk vào bridge-vlan

- **Bước 3:** Vào Interfaces >> VLAN, tạo ra các VLAN và gán các VLAN này vào Interface bridge-vlan đã tạo ở bước 1.
  - o Name: nhập tên đại diện vlan
  - o MTU: 1496 (đối với GNS3)
  - o VLAN ID: nhập số ID của vlan
  - o Interface: bridge-vlan



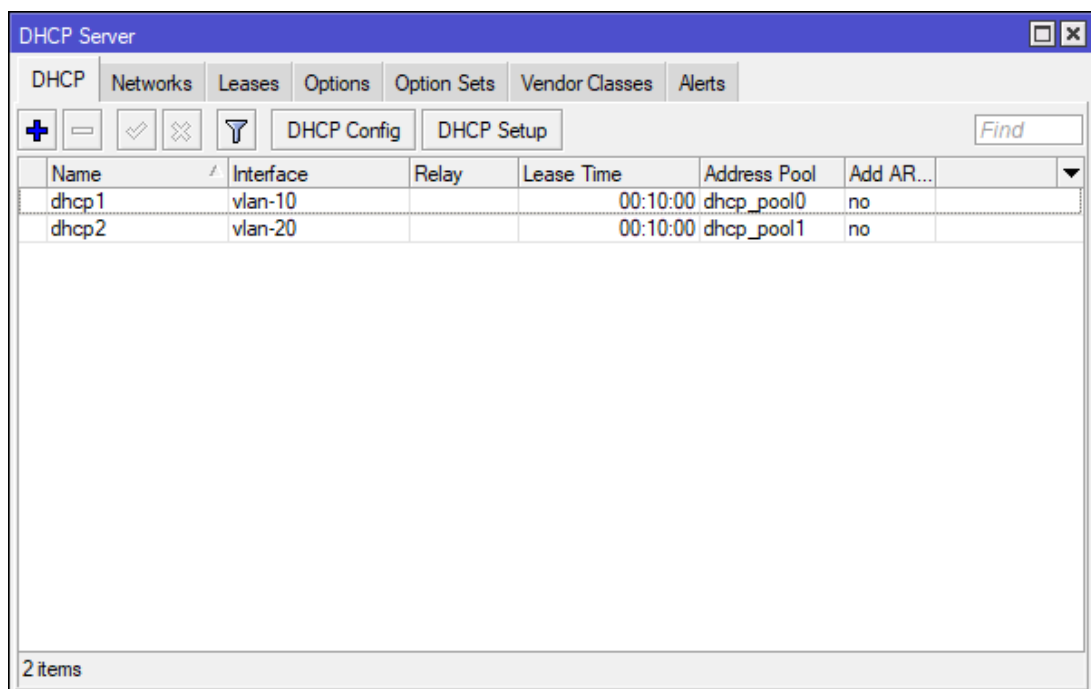
**Hình 5.5.** Tạo ra các vlan và gán vào Interface bridge-vlan

- **Bước 4:** Vào IP >> Address, tạo địa chỉ IP cho các VLAN. Gán địa chỉ IP này cho Interface vlan tương ứng.



**Hình 5.6.** Tạo địa chỉ ip của vlan và gán vào interface vlan tương ứng.

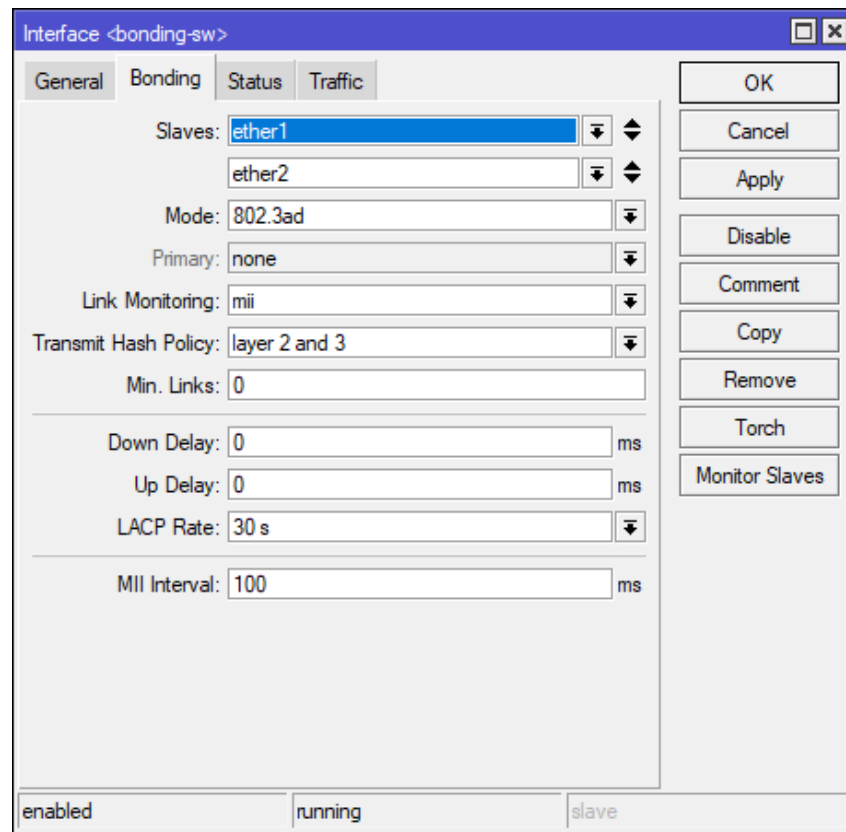
- **Bước 5:** Vào IP >> DHCP Server, bấm vào nút DHCP Setup, lần lượt tạo DHCP Server cấp địa chỉ IP cho các vlan.



**Hình 5.7.** Tạo DHCP Server cấp địa chỉ IP cho các vlan

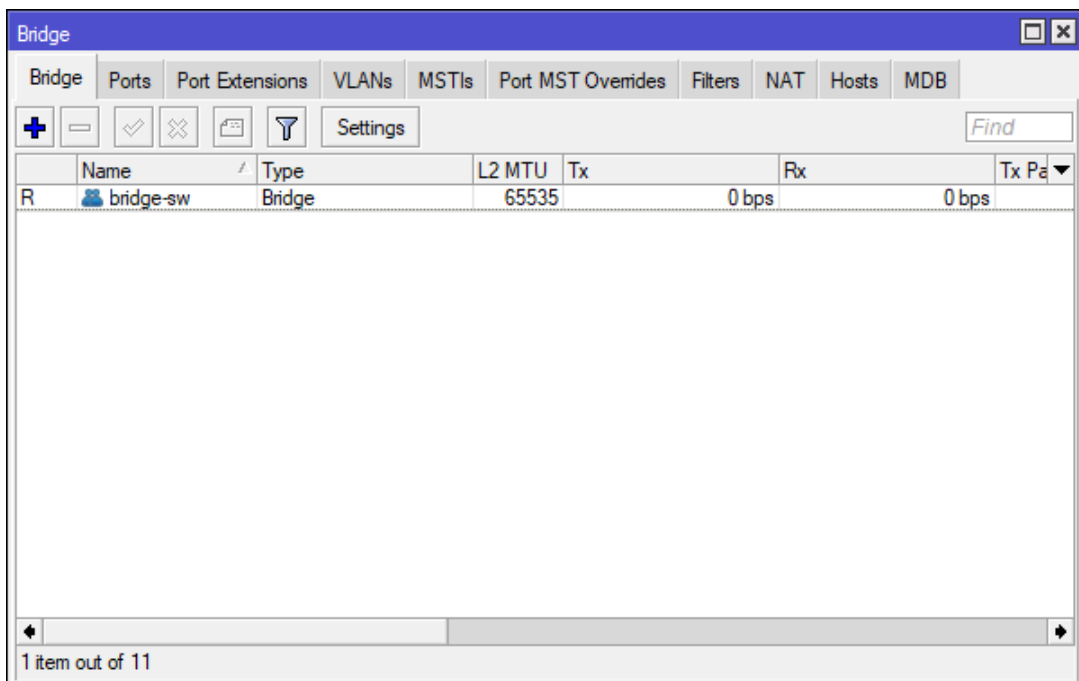
### 3.2. Trên Switch:

- **Bước 1:** tạo bonding: tương tự như trên router, tạo bonding-sw chứa port ether1 và ether2.



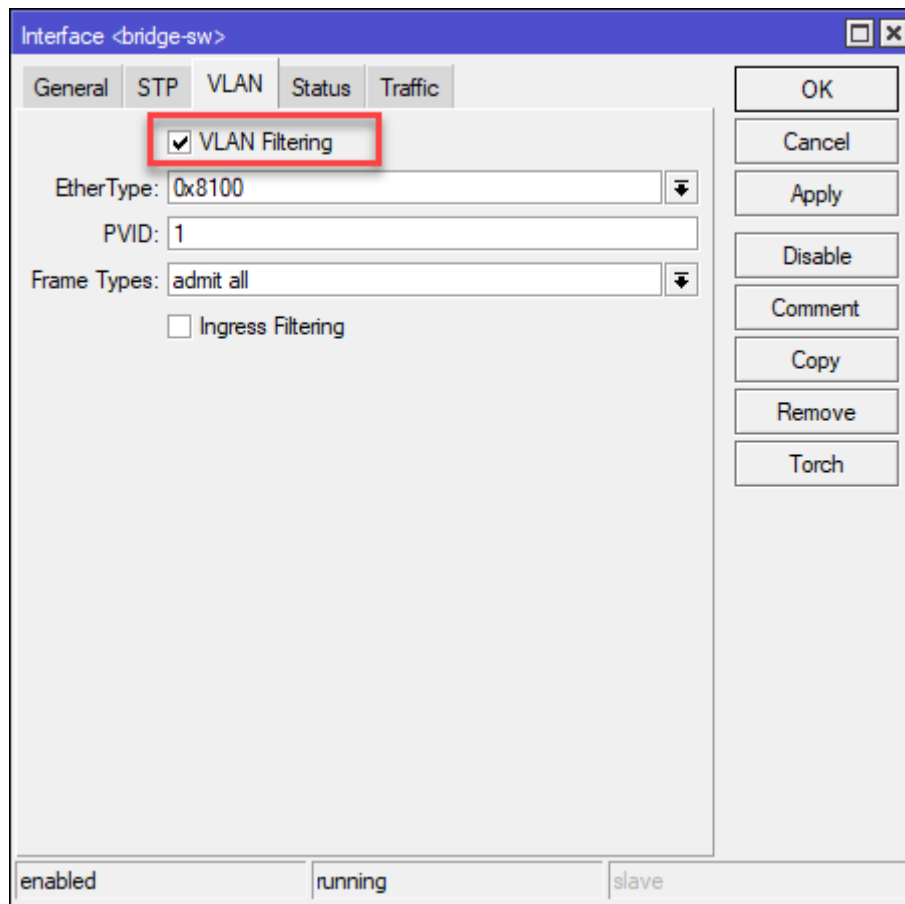
**Hình 5.8.** Bonding trên switch

- Bước 2: Vào Bridge, tạo bridge-sw.



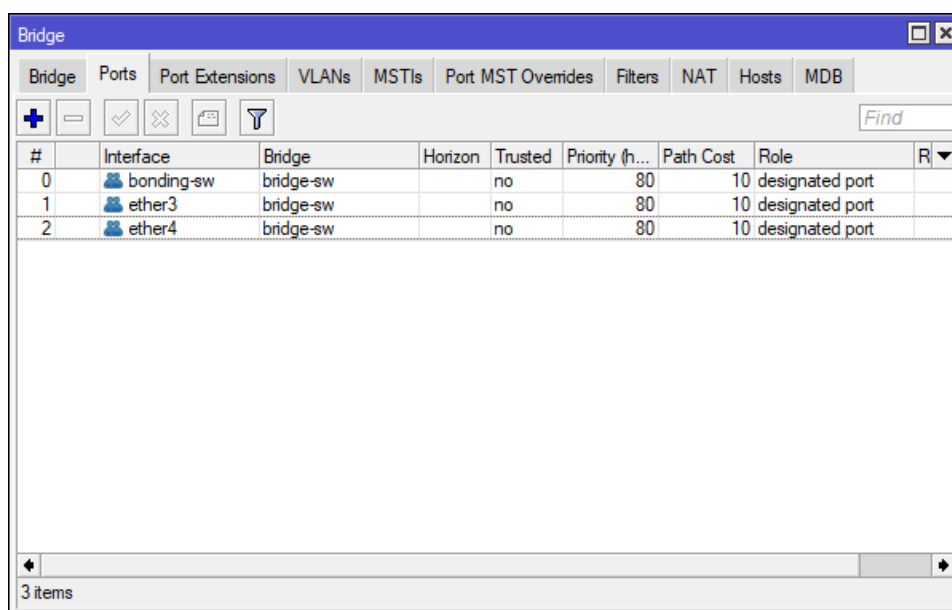
**Hình 5.9.** Tạo bridge-sw

- **Bước 2:** Bấm kép vào bridge-sw vừa tạo, vào tab VLAN, check vào ô “VLAN Filtering”. Các mục còn lại để mặc định.



**Hình 5.10.** Check vào ô “VLAN Filtering”

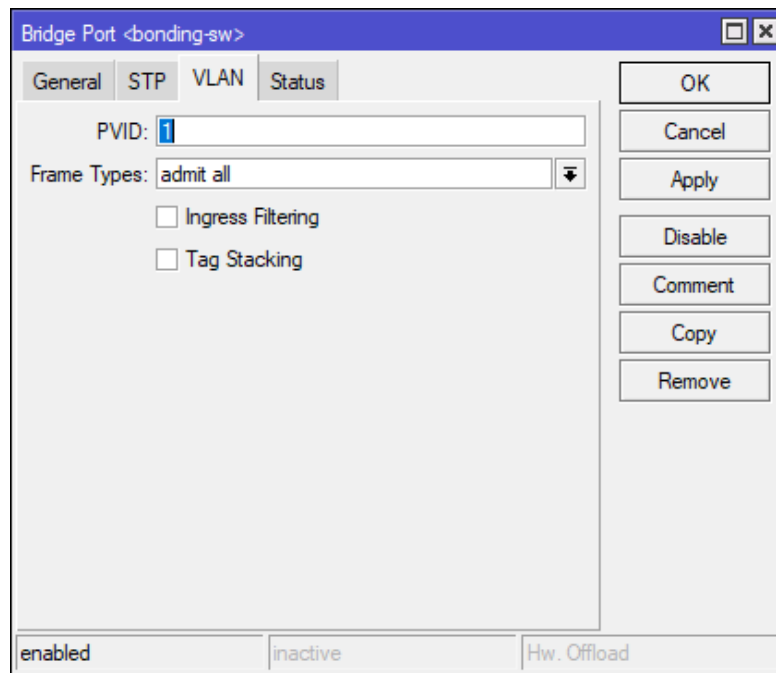
- **Bước 3:** Trong cửa sổ Bridge, vào tab Ports, thêm vào các port có liên quan đến VLAN, kể cả port bonding-sw là port trunk



**Hình 5.11.** Thêm các port có liên quan đến vlan vào bridge-sw

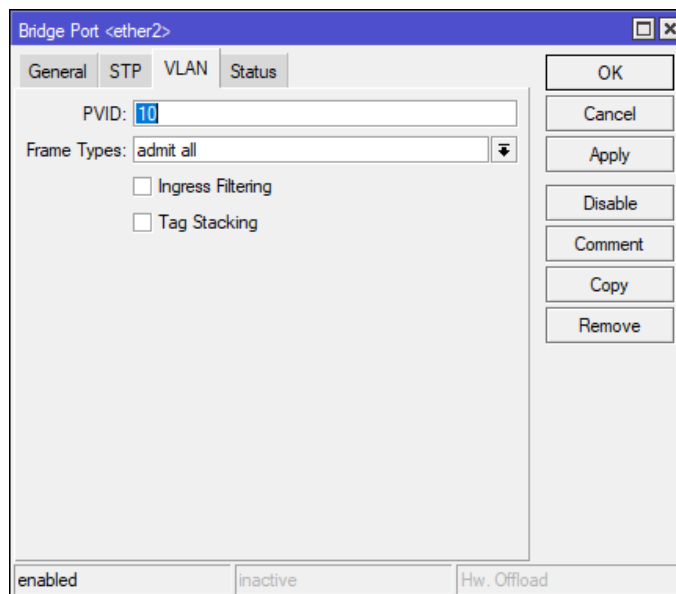


- **Bước 4:** Vẫn trong tab Ports, gán vlan vào port bằng cách bấm kép vào từng port. Đối với port bonding-sw là port trunk, tại tab VLAN của port này, ta để mặc định và không chỉnh sửa.



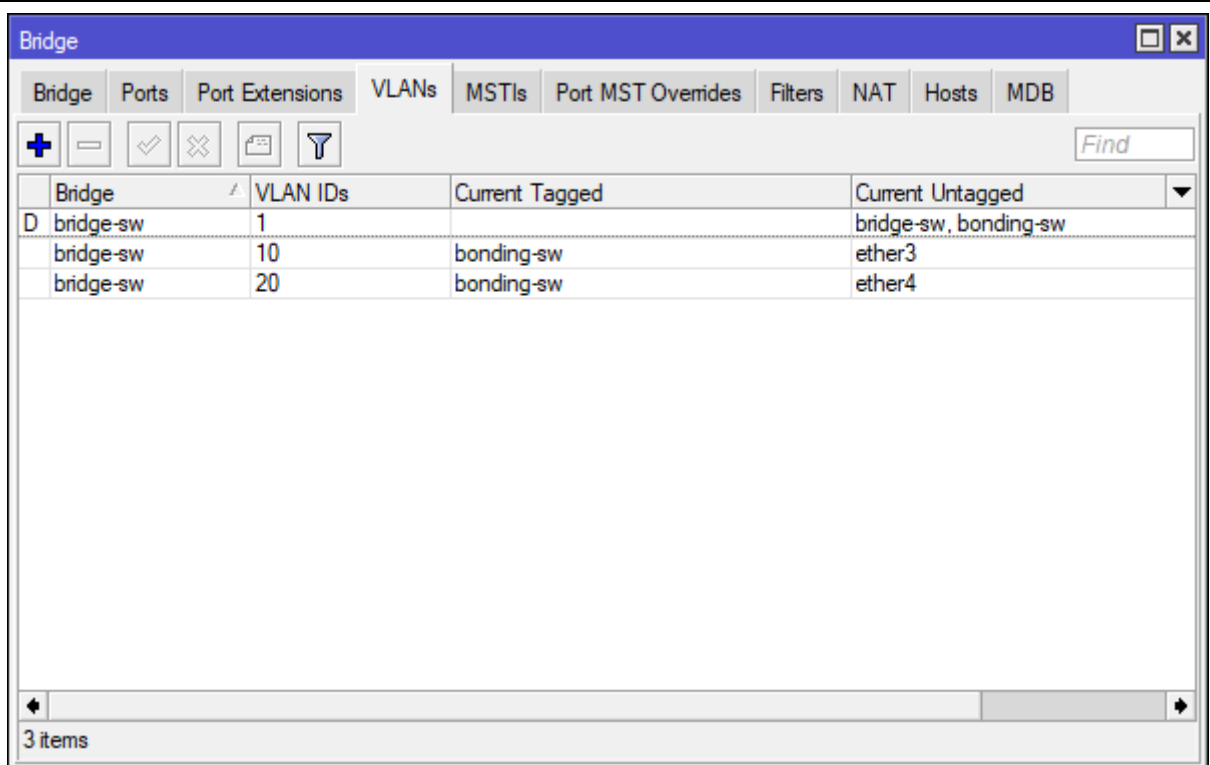
**Hình 5.12.** Port trunk ether1, trong tab VLAN để mặc định.

- **Bước 5:** Vẫn trong tab Ports, tiếp tục bấm kép vào các port còn lại, vào tab VLAN của port đó:
  - o Mục PVID: gán vlan tương ứng.
  - o Mục Frame Types: admit all.



**Hình 5.13.** Cấu hình cho port access (port giải mã vlan)

- **Bước 6:** Sau cùng ta có bảng VLANs như sau:



The screenshot shows the Mikrotik WinBox interface for configuring Bridge VLANs. The 'VLANs' tab is selected. The table below displays the current configuration for three VLANs.

Bridge	VLAN IDs	Current Tagged	Current Untagged
bridge-sw	1		bridge-sw, bonding-sw
bridge-sw	10	bonding-sw	ether3
bridge-sw	20	bonding-sw	ether4

3 items

**Hình 5.14.** Bảng VLANs

## BÀI 6. VLAN MANAGEMENT

### 1. Giới thiệu:

...

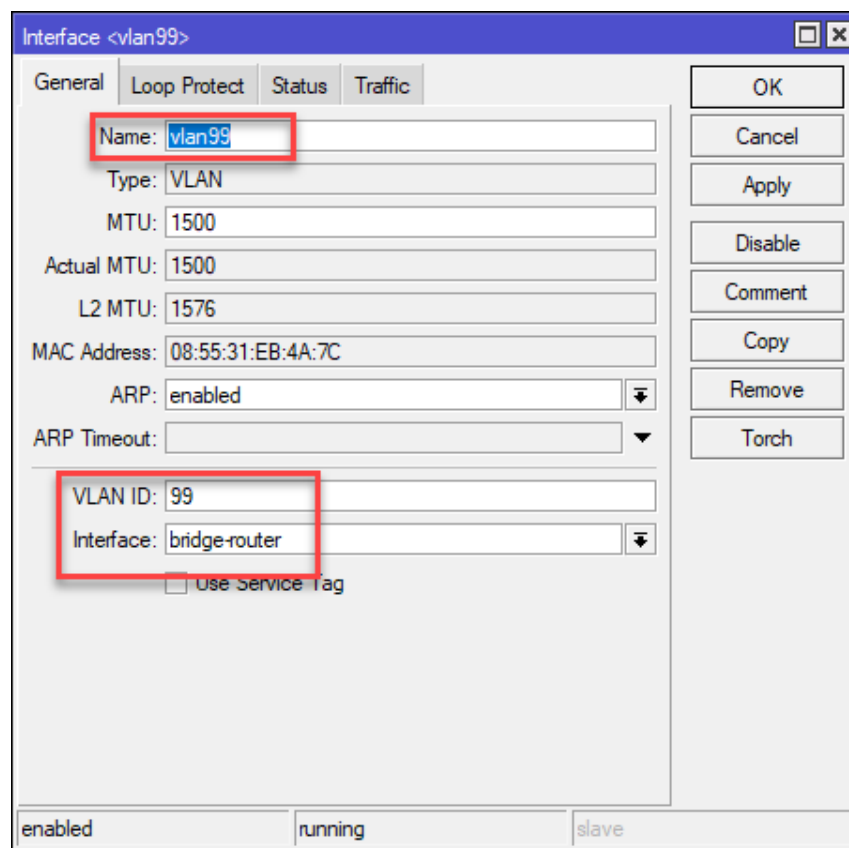
### 2. Mô hình mạng:

...

### 3. Thực hành:

#### 3.1. Trên router:

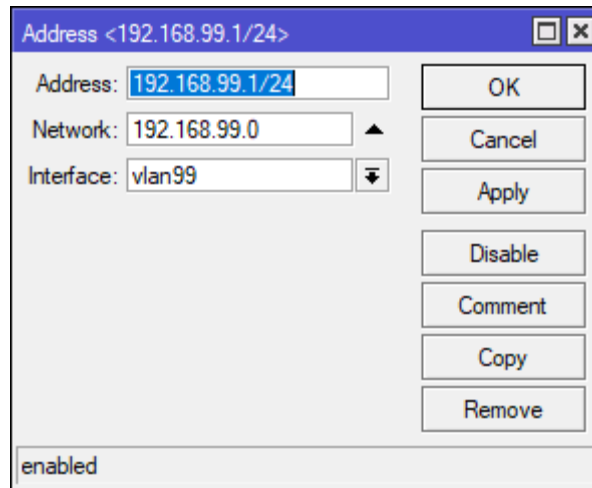
- **Bước 1:** khởi tạo vlan99 (vlan management). Vào Interface chọn VLAN. Bấm dấu + để tạo vlan mới.
  - o **Name:** vlan99 (tên đại diện, bạn có thể thay đổi tùy ý)
  - o **VLAN ID:** 99
  - o **Interface:** bridge-router



Hình 6.1. Tạo vlan quản lý

- **Bước 2:** đặt địa chỉ IP cho vlan quản lý. Vào IP, chọn address, bấm dấu + để tạo địa chỉ mới.
  - o **Mục Address:** 192.168.99.1/24
  - o **Network:** 192.168.99.0

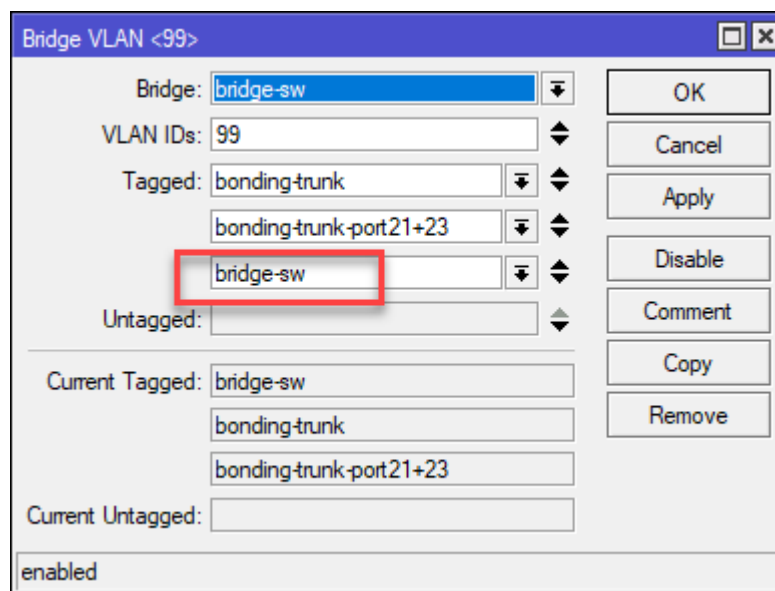
- **Interface:** vlan99



**Hình 6.2.** Gán địa chỉ IP cho vlan99

### 3.2. Trên switch:

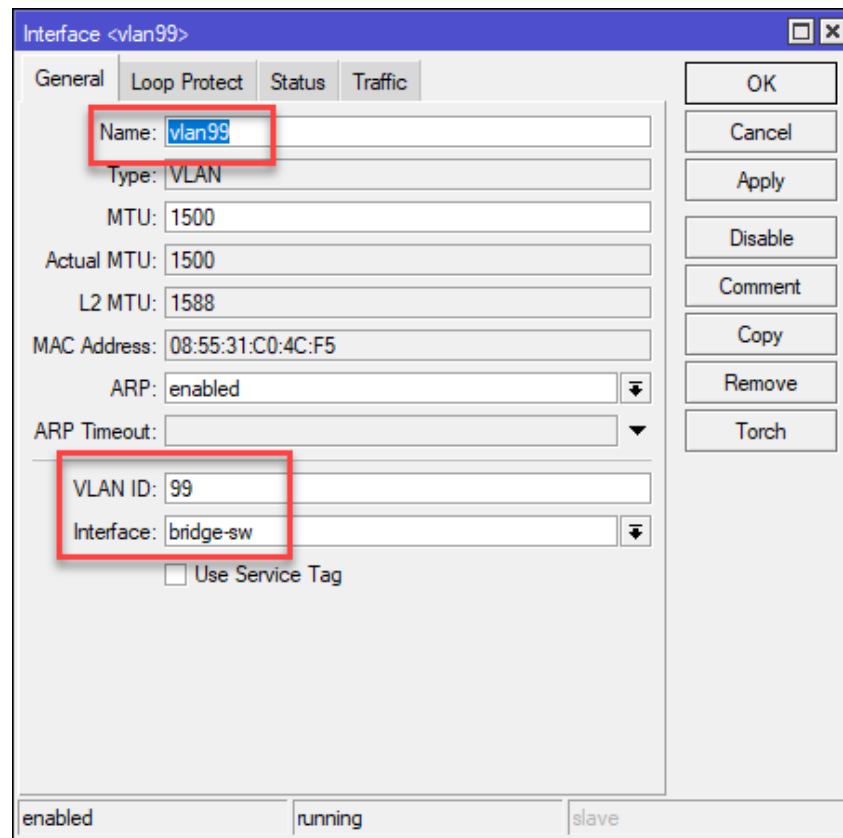
- **Bước 1:** gán vlan99 vào bridge-sw. Vào Bridge chọn VLANs, bấm dấu + để thêm VLAN mới.
  - **VLAN IDs:** 99
  - **Tagged:** chọn interface kết nối trực tiếp với router, có thể chọn tiếp interface mà muốn chuyển vlan này đi tiếp, chọn interface bridge-sw.



**Hình 6.3.** Thêm vlan quản lý vào bridge-sw

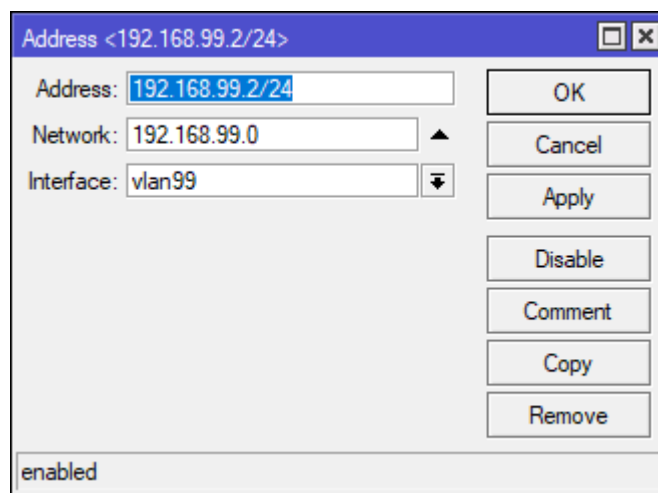
- **Bước 2:** Tạo vlan 99 và gán vlan id 99 vào interface bridge-sw. Vào Interface, chọn VLAN, bấm dấu + để thêm vlan mới.
  - **Name:** vlan99

- **VLAN ID:** 99
- **Interface:** bridge-sw



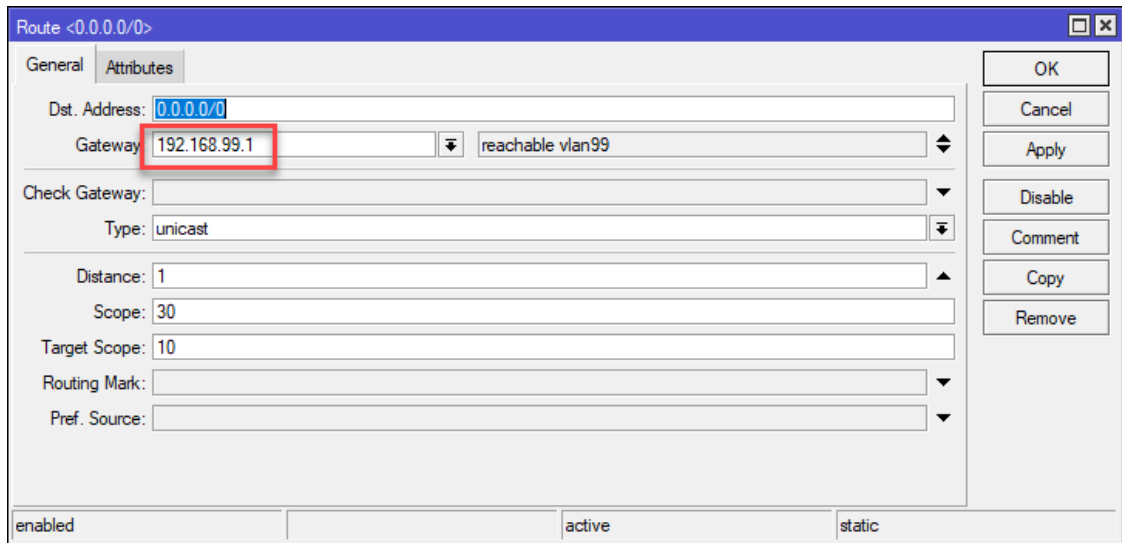
**Hình 6.4.** Gán vlan id 99 cho interface bridge-sw

- **Bước 3:** gán địa chỉ IP cho vlan 99. Vào IP >> Address. Bấm dấu + để thêm địa chỉ IP mới.
  - **Address:** 192.168.99.2/24
  - **Network:** 192.168.99.0
  - **Interface:** vlan99



**Hình 6.5.** Gán địa chỉ IP cho vlan 99

- **Bước 4:** tạo route đến gateway của vlan 99. Vào IP >> Route, bấm dấu + để tạo route mới. Mục gateway: nhập vào địa chỉ IP của vlan 99 ở router: 192.168.99.1.



**Hình 6.6.** Tạo route đến gateway vlan 99 ở router.

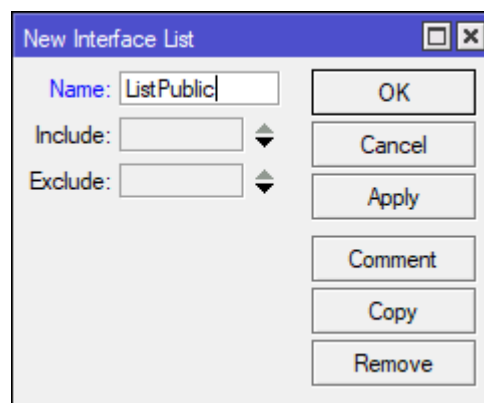
## BÀI 7. FIREWAL CƠ BẢN

### 1. Yêu cầu:

- Mặc định các vlan trên Mikrotik đều là intervlan. Do đó, ta phải điều chỉnh lại để cho một số vlan không nhìn thấy nhau. Yêu cầu:
- Không cho các địa chỉ trong vlan public thấy các địa chỉ trong vlan private và gateway của các vlan khác, chỉ được phép thấy gateway của vlan chính nó.
- Không cho địa chỉ ip giữa các vlan public thấy lẫn nhau.

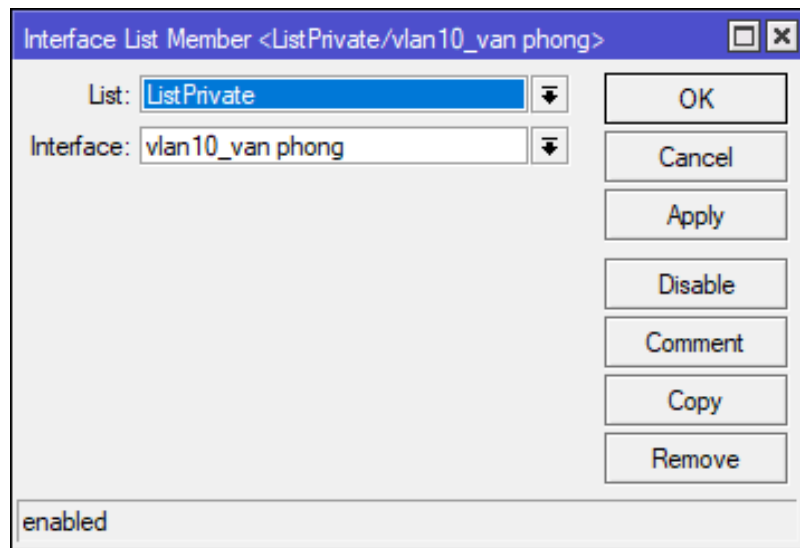
### 2. Thực hiện trên router

- Tóm tắt các bước:
  - o Tạo hai danh sách interface dành cho các vlan private và public, sau đó thêm các vlan interface vào hai danh sách.
  - o Tạo một danh sách địa chỉ (address list) và thêm các gateway của vlan vào danh sách.
  - o Sử dụng
- **Bước 1:** vào Interface >> Interface List, bấm dấu vào nút Lists để bắt đầu thêm danh sách mới. Bấm Ok sau khi tạo xong danh sách.
  - o **Danh sách 1:** ListPublic
  - o **Danh sách 2:** ListPrivate



Hình 7.1. New interface list

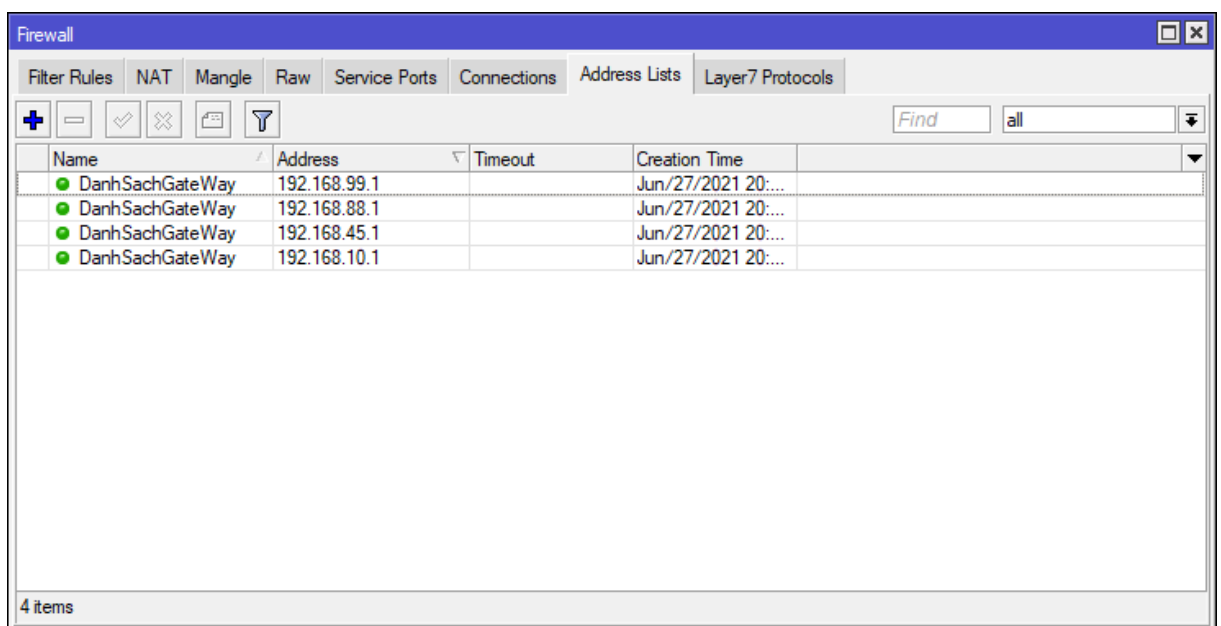
- **Bước 2:** trở lại màn hình Interface List, bấm dấu + để thêm member vào danh sách. Tiếp tục thêm các member khác cho đến hết.



**Hình 7.2.** Thêm member vào Interface List

Tương tự, thực hiện tiếp với danh sách ListPublic.

- **Bước 3:** vào IP >> Firewall, Address Lists, tạo danh sách các gateway của các vlan thuộc ListPrivate:



**Hình 7.3.** Danh sách các gateway các vlan của ListPrivate

- **Bước 4:** vào IP >> Firewall, tab Filter Rules, bấm dấu + để thêm luật mới.

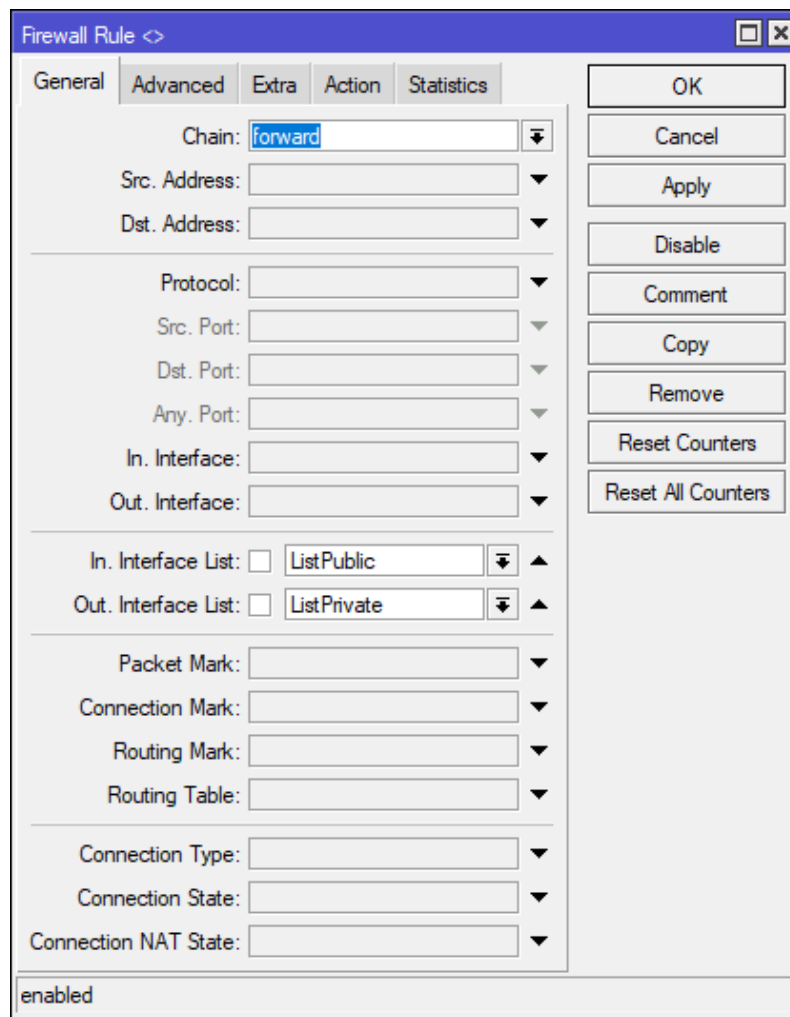
Ý nghĩa các chain forward và input:

- o Chain forward: dữ liệu đi qua router
- o Chain input: dữ liệu đi vào router.



Không cho các vlan trong danh sách public thấy các vlan trong danh sách private. Để làm được điều này, ta tạo một chain forward với action là drop.

- Chain: **forward**,
- In. Interface List: **ListPublic**,
- Out. Interface List: **ListPrivate**,
- Action: **drop**



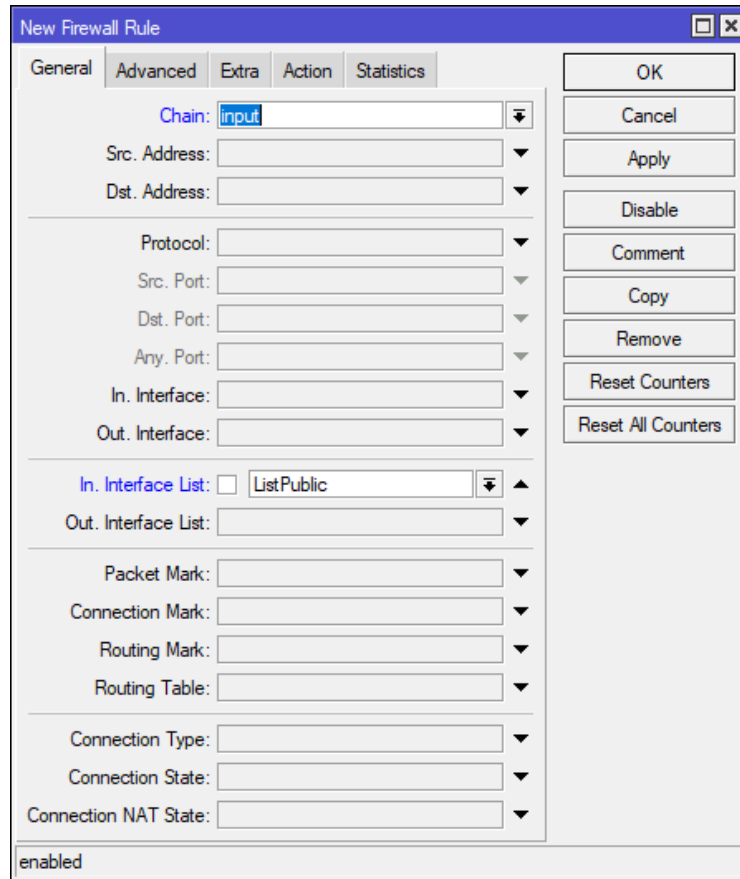
**Hình 7.4.** Không cho danh sách public thấy danh sách private

Không cho các địa chỉ ip trong danh sách public thấy nhau.

- Chain: **forward**,
- In. Interface List: **ListPublic**,
- Out. Interface List: **ListPublic**,
- Action: **drop**

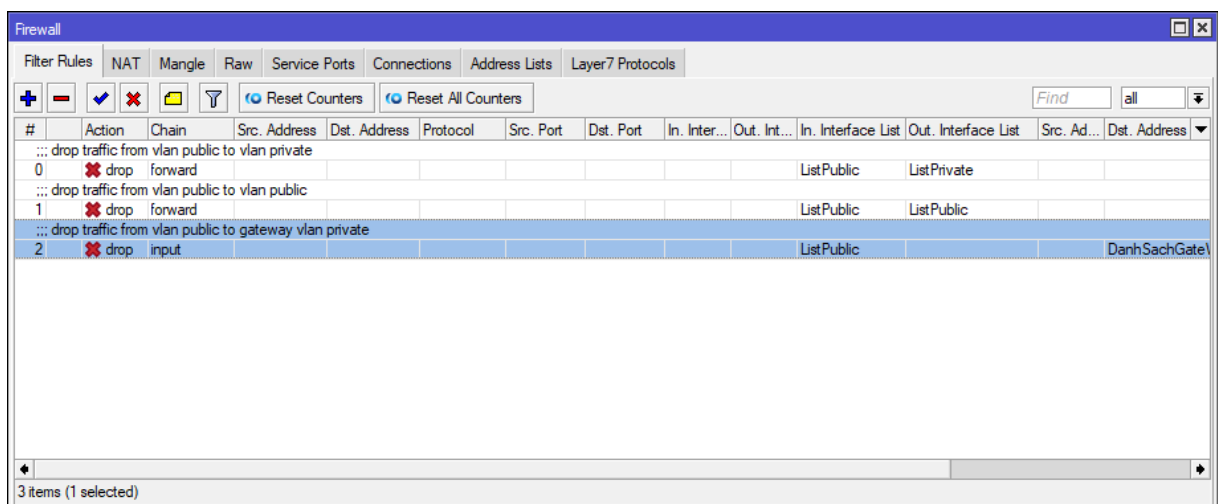
Không cho vlan thuộc ListPublic ping tới gateway của các vlan thuộc ListPrivate. Để làm được điều này, ta tạo một luật với chain input và action là drop.

- Chain: **input**
- In. Interface List: **ListPublic**
- Dst. Address List: **DanhSachGateWay**
- Action: **drop**



**Hình 7.5.** Không cho ListPublic ping tới gateway của ListPrivate

Kết quả sau khi làm xong:



**Hình 7.6.** Filter Rules

## BÀI 8. CÂN BẰNG TẢI VÀ FAIL OVER

### 1. Giới thiệu:

MikroTik hỗ trợ cân bằng tải nhiều đường WAN dựa trên tính năng gọi là “PCC – Per Connection Classifier”. Dữ liệu trong mạng nội bộ đi ra Internet sẽ được chia đều các gói tin ra ngoài theo các đường WAN ngẫu nhiên.

Để làm được điều này, ta phải “mark” (đánh dấu) kết nối và đường đi gói tin hợp lý để một gói tin khi đi ra ngoài internet bằng đường WAN với IP Local nào thì khi quay lại nó sẽ phải đi vào đúng đường WAN nó đã đi ra. Cùng với đó là việc kết hợp thêm “PCC” và chỉnh lại Routes để đặt đường đi, cài đặt độ ưu tiên cho đường WAN (Failover).

Công thức của PCC rất đơn giản, sử dụng thuật toán băm theo tỷ lệ. Ví dụ hai đường WAN có cùng tốc độ: WAN1: 100Mb/s và WAN2: 100Mb/s, lúc này tỉ lệ sẽ là 1:1. Do đó tỉ lệ PCC sẽ là 2/0 và 2/1.

Trường hợp hai đường WAN có tốc độ khác nhau, giả sử WAN1: 100Mb/s, WAN2: 50Mb/s, tỉ lệ lúc này sẽ là 2:1. Do đó tỉ lệ PCC cho WAN1(100Mb/s) là hai phần 3/0 và 3/1, của WAN2 (50Mb/s) là một phần 3/2

### 2. Mô hình mạng

Các bước thực hiện:

- Tạo prerouting chấp nhận cho các lớp mạng bên trong nội bộ không cần đi qua cân bằng tải.
- Đánh dấu các kết nối đi vào từ internet.
- Đánh dấu các kết nối đi ra internet từ trong mạng lan.
- Cân bằng tải
- Kết nối đi vào từ wan nào thì chỉ đường đi ra lại đúng wan đó.
- Tạo route cho các kết nối đánh dấu đi ra đúng wan tương ứng

### 3. Thực hành

#### 3.1. Cấu hình cân bằng tải và fail over bằng dòng lệnh

Giả sử ta cần cấu hình cân bằng tải trên hai đường WAN VNPT\_1 và VNPT\_2 kiểu **both-addresses-and-ports** và dự phòng (failover)

- **Bước 1:** tạo luật mangle chấp nhận lưu lượng trong mạng nội bộ sẽ không bị ảnh hưởng bởi các luật mangle của firewall.

- `dst-address`: là lớp mạng sẽ chấp nhận không đi qua cân bằng tải.
- `In-interface`: là interface trong mạng nội bộ

Luật mangle này kiểm tra mọi traffic có đích đến (`dst-address`) là mạng LAN (192.168.10.0/24) và interface tiếp nhận traffic là BridgeLAN. Action "accept" với mục đích dừng không xử lý traffic này với các rule kế tiếp sau. Để bắt traffic đi qua các rule bên dưới tiếp theo, cần khai báo trường "`passthrough=yes`".

```
/ ip firewall mangle
add chain=prerouting dst-address=192.168.10.0/24
action=accept in-interface=BridgeLAN
```

- **Bước 2:** đánh dấu kết nối khởi tạo từ bên ngoài đi vào mạng nội bộ (interface `pppoe-out1` và `pppoe-out 2`). Những kết nối chưa được đánh dấu (`no-mark`) sẽ được đánh dấu (`mark`) là "`danhdauVNPT1`" và "`danhdauVNPT2`"

```
add chain=prerouting in-interface=pppoe-out1 connection-
mark=no-mark action=mark-connection new-connection-
mark=danhdauVNPT1
add chain=prerouting in-interface=pppoe-out2 connection-
mark=no-mark action=mark-connection new-connection-
mark=danhdauVNPT2
```

- **Bước 3:** đánh dấu kết nối khởi tạo bên trong mạng nội bộ đi ra internet, sử dụng thuật toán `pcc` (`per-connection-classifier`). Trong đó:
  - `both-address`: chỉ cân bằng tải
  - `both-address-and-ports`: cân bằng tải và gộp băng thông

```
add chain=prerouting in-interface=BridgeLAN connection-
mark=no-mark dst-address-type=!local per-connection-
classifier=both-addresses-and-ports:2/0 action=mark-
connection new-connection-mark=danhdauVNPT1
add chain=prerouting in-interface=BridgeLAN connection-
mark=no-mark dst-address-type=!local per-connection-
```

```
classifier=both-addresses-and-ports:2/1 action=mark-connection new-connection-mark=danhdauVNPT2
```

- **Bước 4:** những traffic khởi tạo từ interface **BridgeLAN** sẽ đánh dấu là “**diraVNPT1**” hoặc “**diraVNPT2**”.

```
add chain=prerouting connection-mark=danhdauVNPT1 in-interface=BridgeLAN action=mark-routing new-routing-mark=diraVNPT1
```

```
add chain=prerouting connection-mark=danhdauVNPT2 in-interface=BridgeLAN action=mark-routing new-routing-mark=diraVNPT2
```

- **Bước 5:** đối với những traffic đi ra ngoài (output) được đánh dấu là “**danhdauVNPT1**” hoặc “**danhdauVNPT2**”, ta sẽ đánh dấu đường đi cho nó là “**diraVNPT1**” hoặc “**diraVNPT2**”

```
add chain=output connection-mark=danhdauVNPT1 action=mark-routing new-routing-mark=diraVNPT1
```

```
add chain=output connection-mark=danhdauVNPT2 action=mark-routing new-routing-mark=diraVNPT2
```

- **Bước 6:** cấu hình cho bảng định tuyến, gán gateway **pppoe-out1** cho đánh dấu “**diraVNPT1**” và **pppoe-out2** cho đánh dấu “**diraVNPT2**”

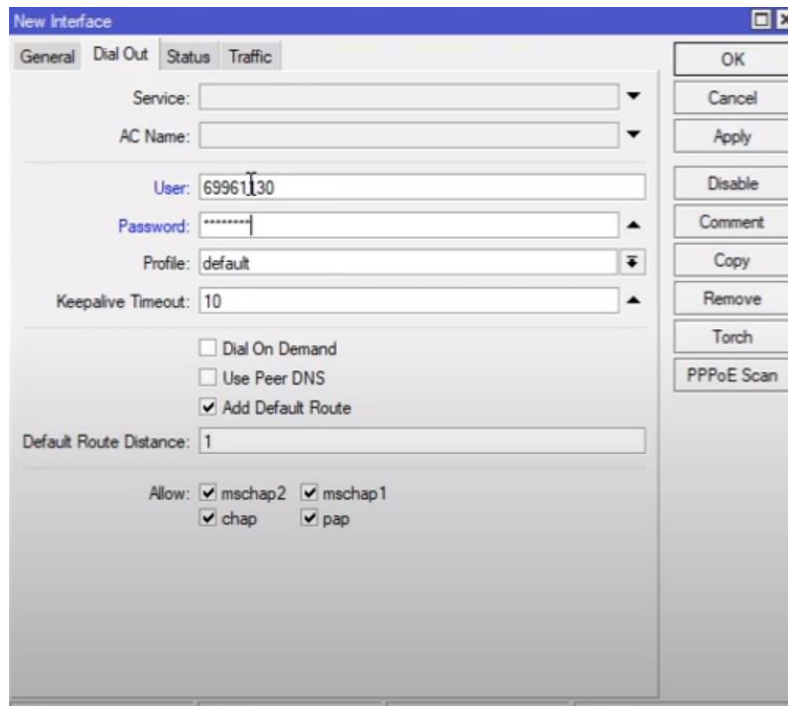
```
/ ip route  
add check-gateway=ping distance=1 gateway=pppoe-out1  
routing-mark=diraVNPT1  
add check-gateway=ping distance=1 gateway=pppoe-out2  
routing-mark=diraVNPT2
```

- **Bước 7:** cấu hình failover

```
/ip route  
add check-gateway=ping distance=1 gateway=pppoe-out1  
add check-gateway=ping distance=2 gateway=pppoe-out2
```

### 3.2. Cấu hình cân bằng tải bằng giao diện

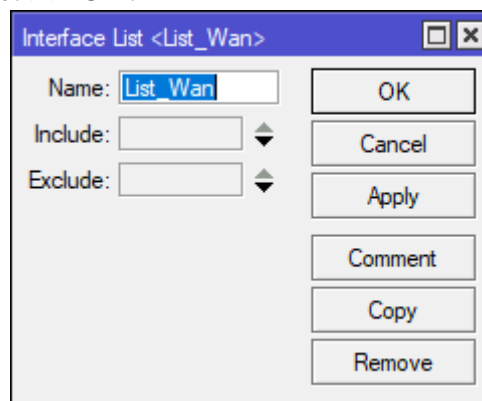
- **Bước 1:** khai báo pppoe cho pppoe-out 1: vào Interface >> Bấm dấu +, chọn New Interface. Tại tab Dial Out:
  - o User: điền vào username pppoe
  - o Password: nhập mật khẩu
  - o Tích chọn Add Default Route
  - o Default Route Distance: 1+n với n là số đường truyền kế tiếp



**Hình 8.1.** Tab dial out của màn hình New Interface

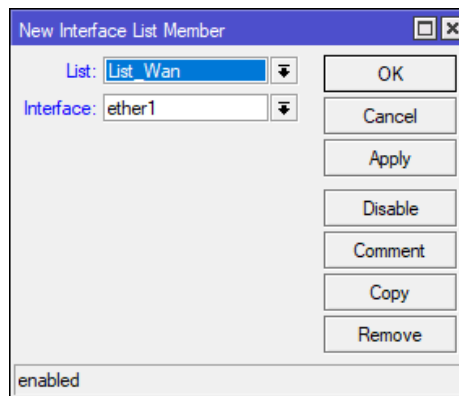
Lặp lại bước 1 cho các đường Wan tiếp theo.

- **Bước 2:** tạo Interface List đưa các đường WAN vào danh sách. Vào Interface >> tab Interface List >> bấm nút List để thêm danh sách. Name: đặt tên cho danh sách Interface. >> OK.



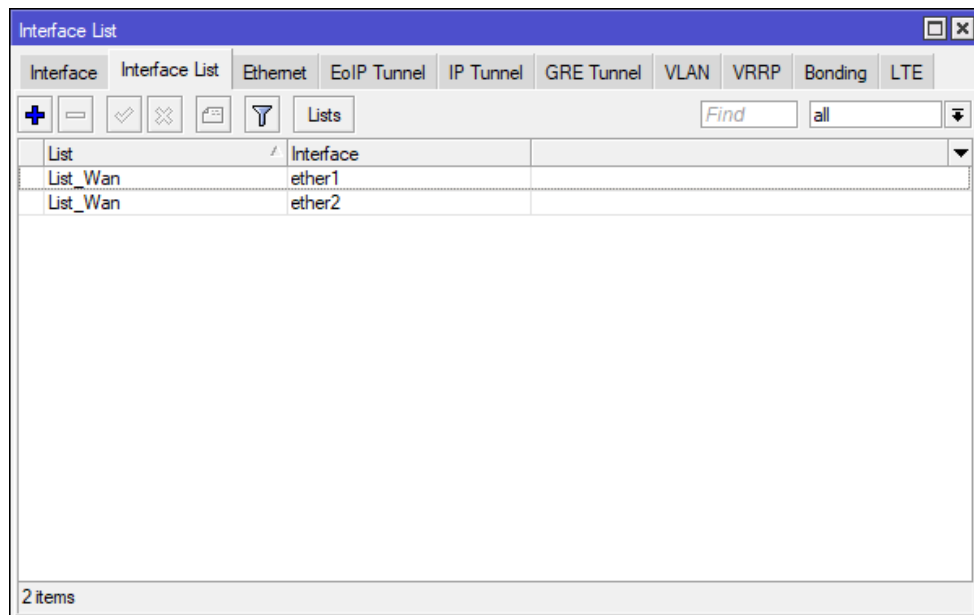
**Hình 8.2.** New Interface List

- **Bước 3:** quay lại tab Interface List, bấm dấu +,
  - o List: chọn tên danh sách interface vừa tạo ở bước 2.
  - o Interface: thêm vào các interface pppoe



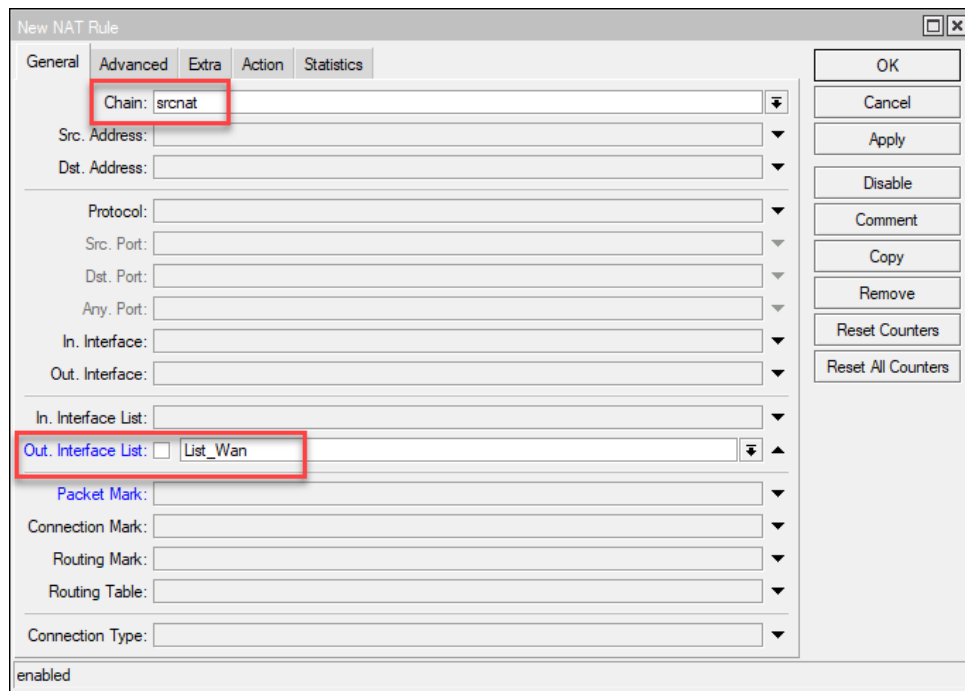
**Hình 8.3.** Thêm interface vào danh sách

Sau khi thêm xong, màn hình Interface List như sau:



**Hình 8.4.** Màn hình Interface List sau khi thêm interface

- **Bước 4:** tạo luật NAT để truy cập được internet: vào IP >> Firewall >> tab NAT. Bấm dấu + để thêm luật NAT mới. Tại tab General:
  - o Chain: srcnat
  - o Out. Interface List: chọn danh sách interface đã tạo



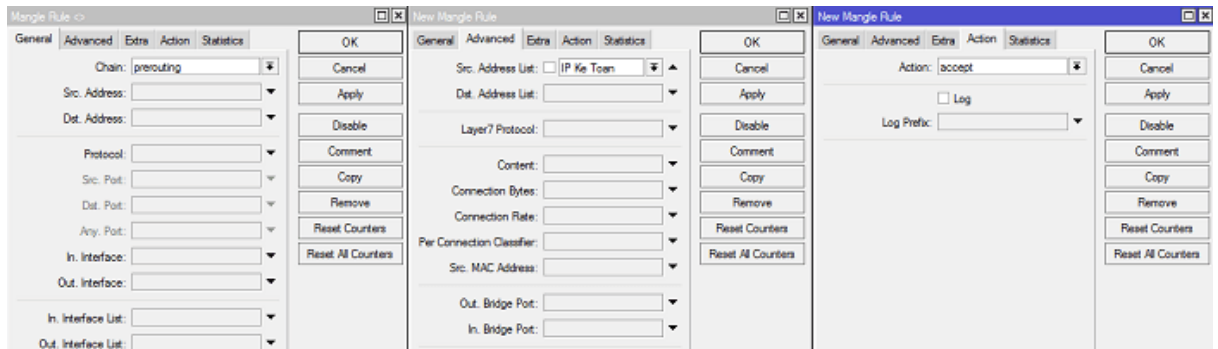
**Hình 8.5.** Tab general của màn hình New Nat Rule

- Bước 5: cũng trong màn hình New Nat Rule, chọn tab Action, mục Action: chọn masquerade

### 3.3. Tạo danh sách địa chỉ IP bỏ qua cân bằng tải:

Khi cấu hình cân bằng tải, một số trang thanh toán trực tuyến sẽ không cho phép thao tác hoặc bị lỗi vì chúng chỉ chấp nhận một địa chỉ IP WAN trong suốt quá trình giao dịch. Để sửa lỗi này, ta có thể định tuyến các máy tính cần sử dụng dịch vụ trên theo đường WAN cụ thể, hoặc đơn giản là loại bỏ các máy này ra khỏi cân bằng tải.

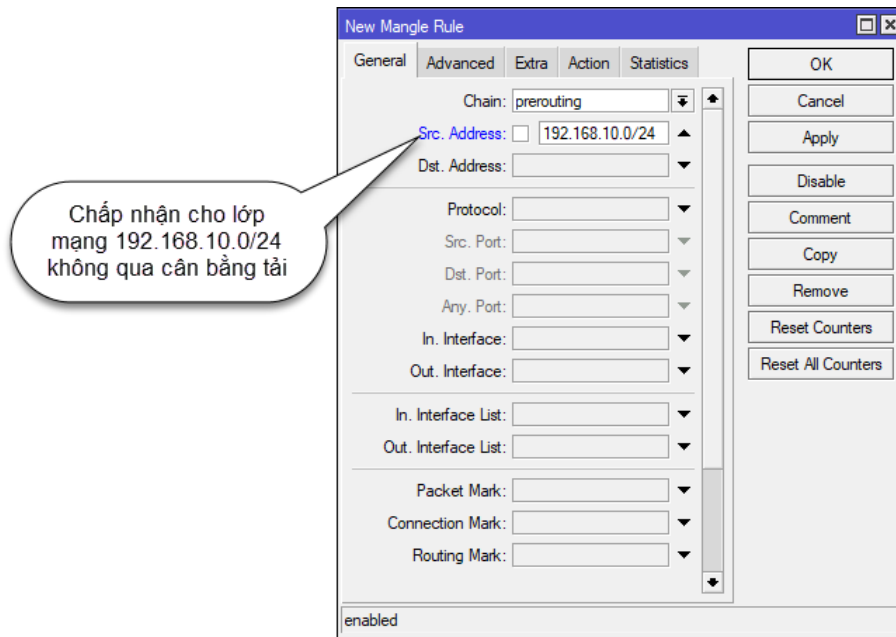
- **Bước 1:** tạo danh sách địa chỉ IP (Address List) bỏ qua cân bằng tải. Vào IP >> Firewall >> Address Lists. Thêm IP các máy tính cần loại ra khỏi cân bằng tải và đặt tên cho danh sách, ví dụ “List\_Khong\_CBT”.
- **Bước 2:** trong Mangle Rule, ta thêm vào rule như hình sau và kéo lên vị trí trên cùng:





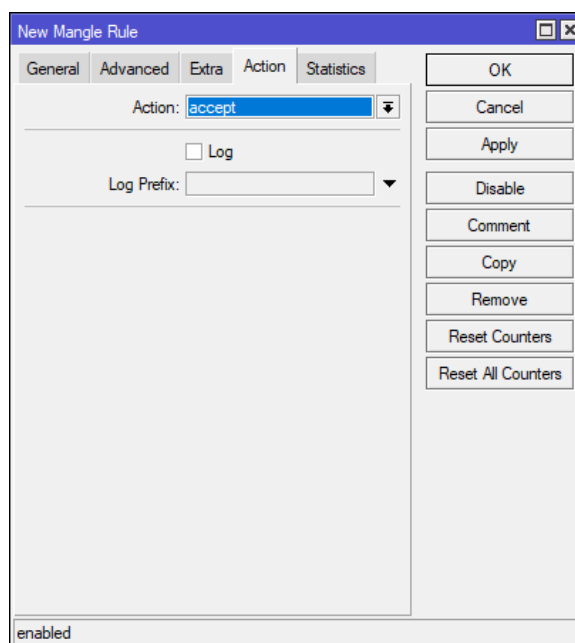
**Hình 8.6.** Rule mangle chấp nhận cho danh sách địa chỉ IP không qua cân bằng tải  
Ngoài cách tạo danh sách địa chỉ IP như trên, ta còn có thể dùng cách gán Src. Address.

- **Bước 1:** vào IP >> Firewall >> Tab Mangle, bấm nút + để thêm luật mới
- **Bước 2:** trong New Mangle Rule, tab General
  - o **Chain:** chọn prerouting
  - o **Src. Address:** nhập vào lớp mạng hoặc một địa chỉ IP, một port dịch vụ cho phép bỏ qua qua cân bằng tải.



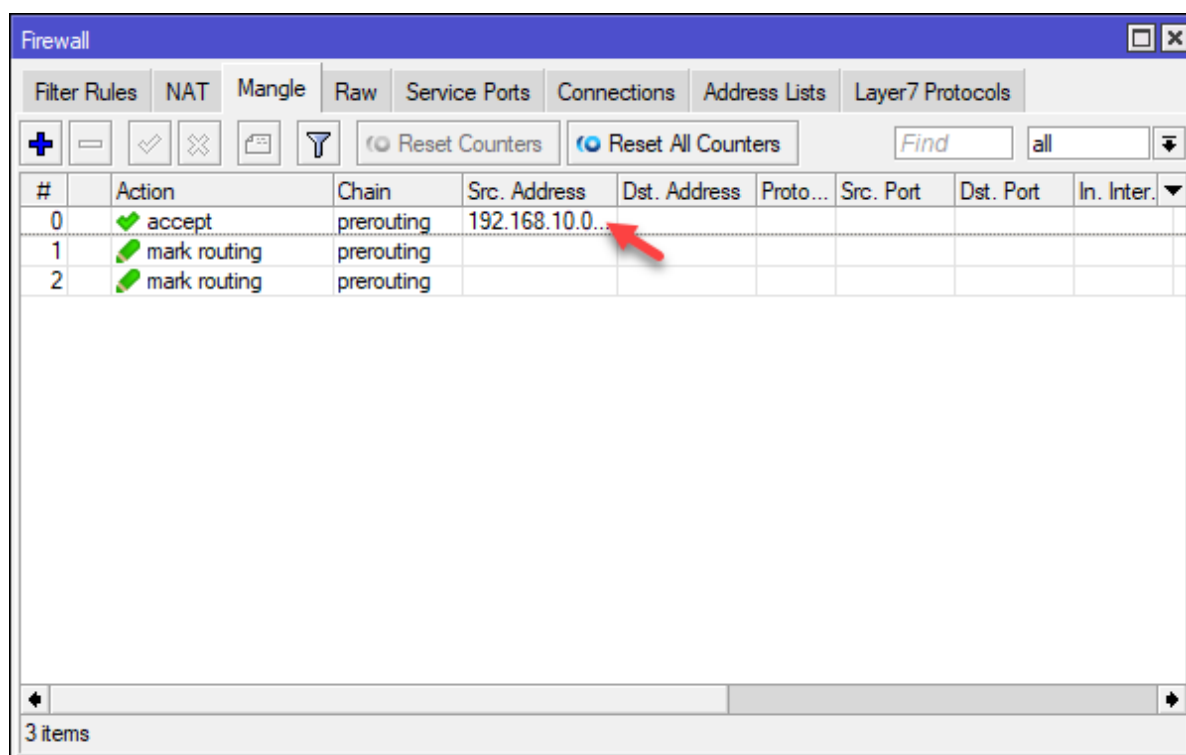
**Hình 8.7.** Tab general của màn hình New Mangle Rule

- **Bước 3:** tại tab Action, mục Action: chọn accept



**Hình 8.8.** Tab action của màn hình New Mangle Rule

- **Bước 4:** kéo lệnh prerouting vừa tạo lên đầu danh sách Mangle.

**Hình 8.9.** Màn hình tab Mangle của cửa sổ Firewall**BÀI 9. NAT****1. Giới thiệu:**

NAT (Network Address Translation) là kỹ thuật cho phép một hay nhiều địa chỉ IP nội bộ được ánh xạ với một hay nhiều địa chỉ IP mạng ngoài. Các địa chỉ IP nội bộ có thể chạy các dịch vụ như web, mail hay đầu ghi lưu trữ camera,... hoặc chỉ đơn giản sử dụng Internet bình thường. NAT được thực hiện ở router biên, nơi kết nối giữa mạng LAN nội bộ và mạng Internet.

NAT giúp tiết kiệm được địa chỉ IP public IPv4 (với tổng địa chỉ khả dụng là hơn 4 tỉ) nhờ cơ chế xử lý của mình. Với NAT, hàng chục đến hàng trăm người dùng trong mạng có thể dùng “chung” một địa chỉ IP public.

Với router Mikrotik, ta cần quan tâm đến các hình thức NAT đó là NAT port, Hairpin NAT và NAT ra Internet

**2. Mô hình mạng.**

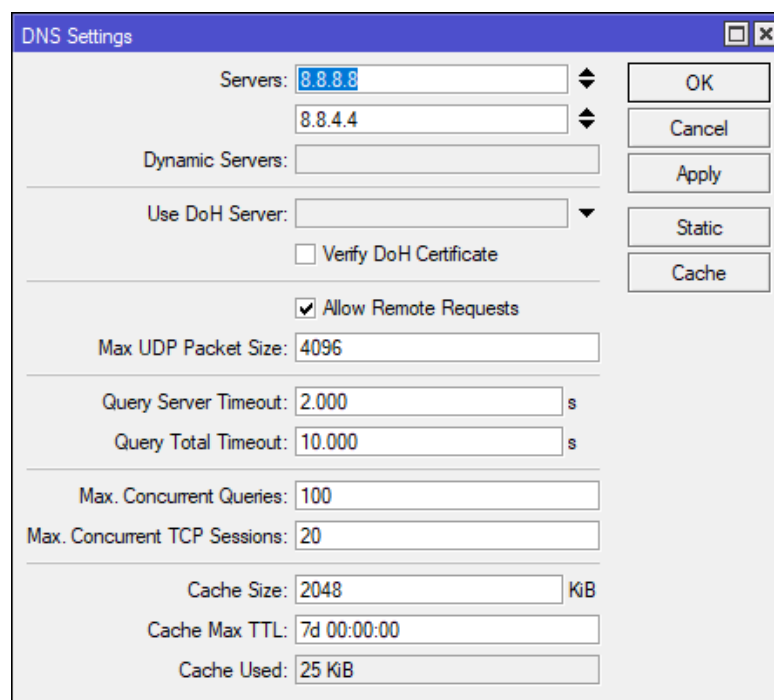
...

### 3. Thực hành

#### 3.1. NAT để truy cập internet

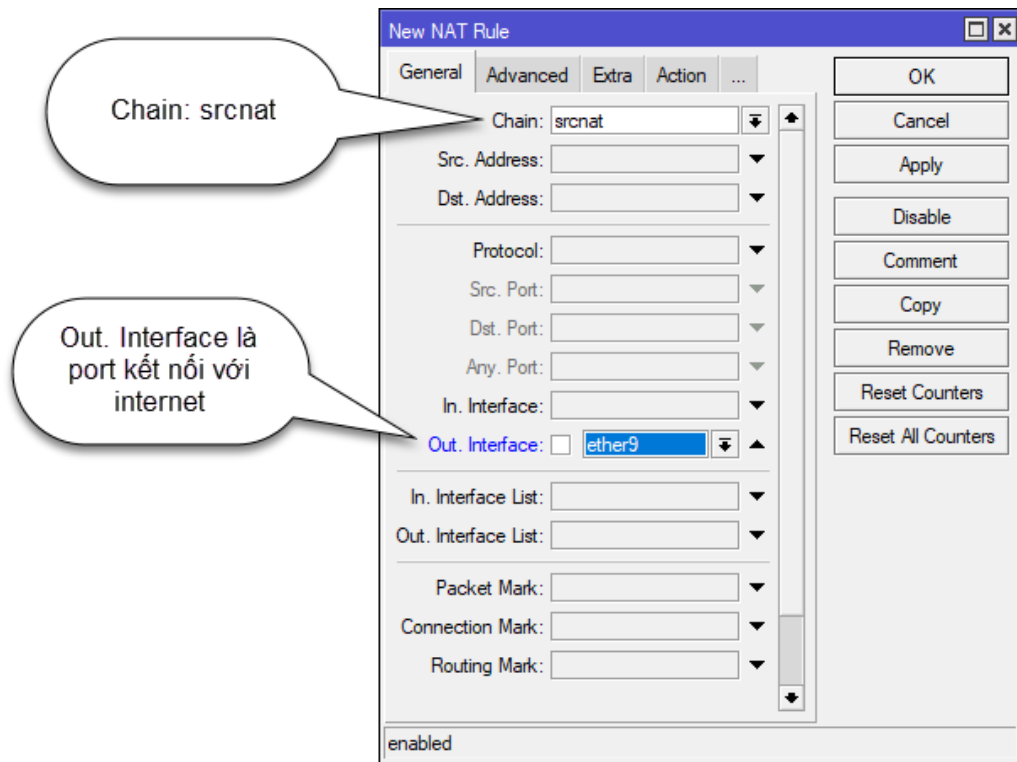
Hay còn gọi là Source NAT, nghĩa là đổi địa chỉ nguồn (source) từ local thành địa chỉ ip public trên cổng WAN để đi ra ngoài Internet. Hình thức NAT phổ biến và đơn giản nhất là NAT động masquerade. Gói tin sẽ được đổi địa chỉ nguồn và router sẽ đánh port nguồn ra ngoài theo một cổng “mặt nạ” nào đó mà router chưa được dùng đến. Khi gói tin đi vào thì router cũng sẽ theo cổng này để đưa đúng gói tin trở lại IP local như cũ.

- **Bước 1:** vào IP >> DNS, nhập DNS là 8.8.8.8 và 8.8.4.4 hoặc 1.1.1.1. Check vào ô Allow Remote Request.



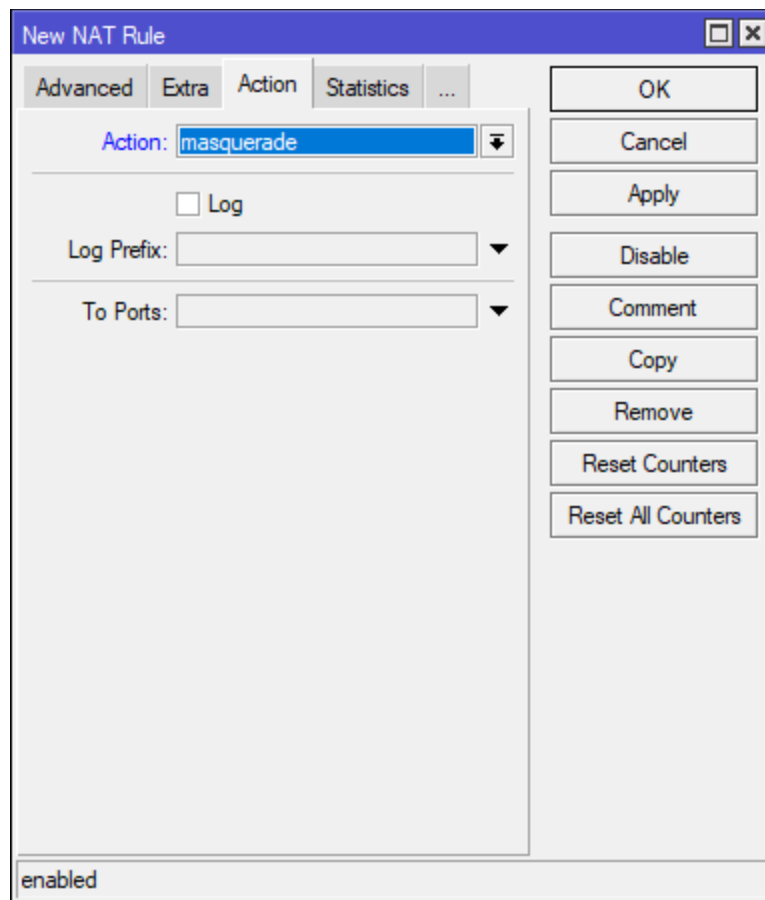
**Hình 9.1.** Cửa sổ DNS Settings

- **Bước 2:** vào IP >> Firewall >> NAT. Bấm dấu + để thêm NAT mới.
- **Bước 3:** trong cửa sổ New NAT Rule, tại tab General
  - o Chain: srcnat
  - o Out. Interface: interface đi ra internet



**Hình 9.2.** Tab general của cửa sổ New NAT Rule

- **Bước 4:** tại tab Action, chọn Action là masquerade



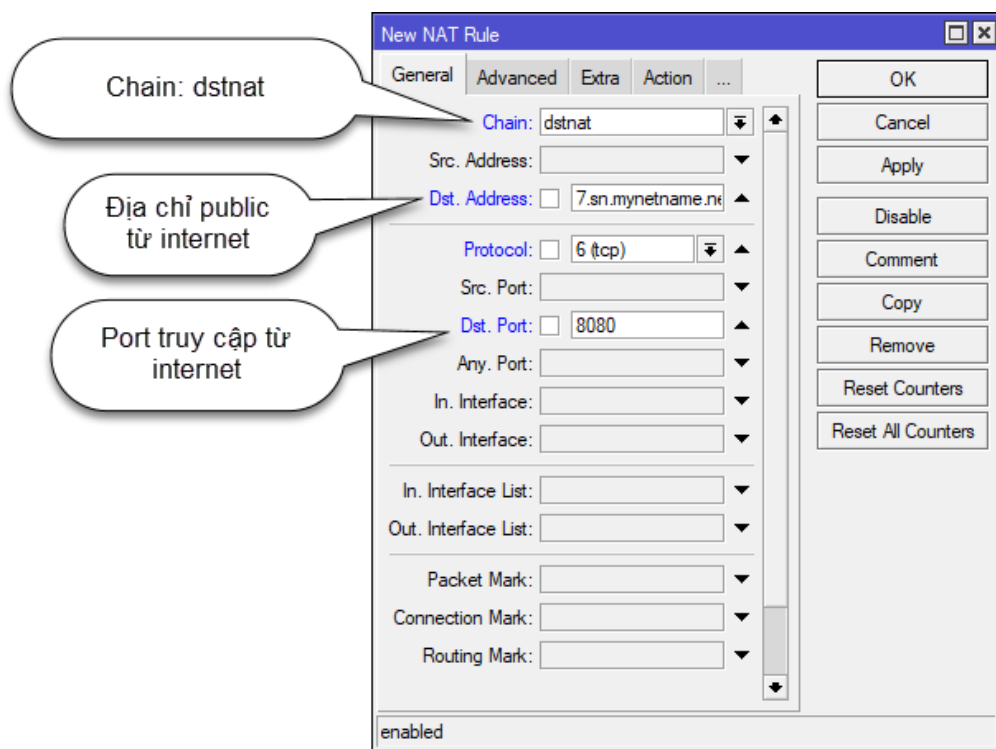
**Hình 9.3.** Chọn Action cho NAT rule

### 3.2. NAT port

NAT port là hình thức phổ biến để truy cập dịch vụ nội bộ từ bên ngoài Internet qua địa chỉ IP Public. Ta cần xác định địa chỉ IP public cần NAT trên cổng WAN, Địa chỉ IP local và port/protocol cần để NAT.

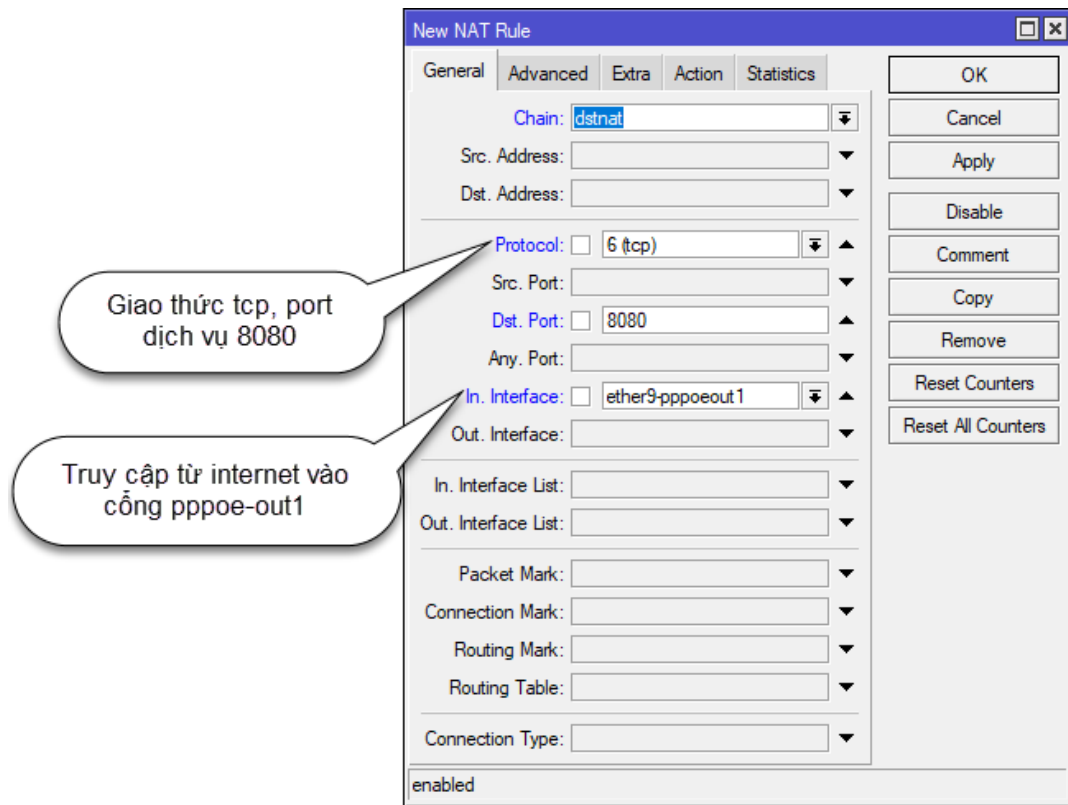
Giả sử cần NAT đầu ghi camera IP có địa chỉ 192.168.68.22, port là 8022 để có thể xem được từ bên ngoài Internet.

- **Bước 1:** vào IP >> Firewall >> NAT, bấm dấu + để thêm luật NAT mới. Trong màn hình NAT Rule, tab General.
  - o Chain: dstnat
  - o Dst. Address là địa chỉ IP tĩnh của đường WAN (trong trường hợp không có IP tĩnh có thể tham khảo cấu hình DDNS trong phần IP >> Cloud)
  - o Protocol: 6 (tcp)
  - o Dst. Port: port cần NAT từ internet (8080)



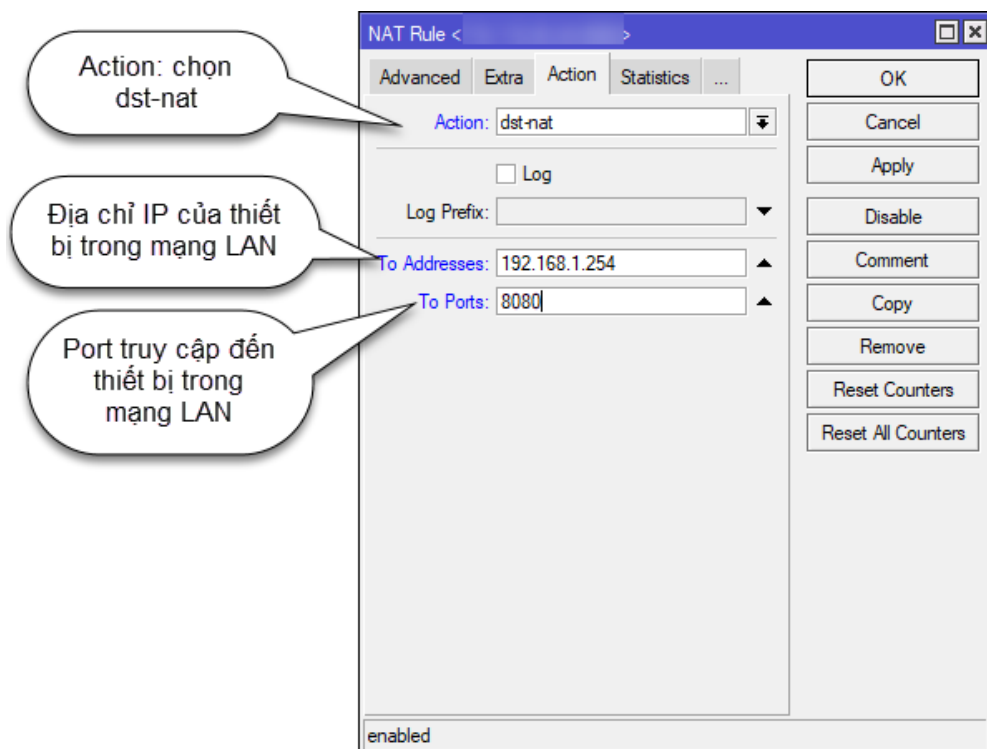
**Hình 9.4.** Tab general của cửa sổ New NAT Rule

Ngoài cách gán địa chỉ IP Public vào mục Dst. Address như trên, ta còn có thể dùng In. Interface để gán. Mục In. Interface chọn Interface kết nối với internet (pppoe-out1)



**Hình 9.5.** Tab general của sổ New NAT rule cách NAT bằng In. Interface

- **Bước 2:** cũng trong cửa sổ NAT Rule, chọn tab Action
  - o Action: dst-nat
  - o To Addresses: 192.168.1.254 (địa chỉ IP của đầu ghi)
  - o To Ports: 8080

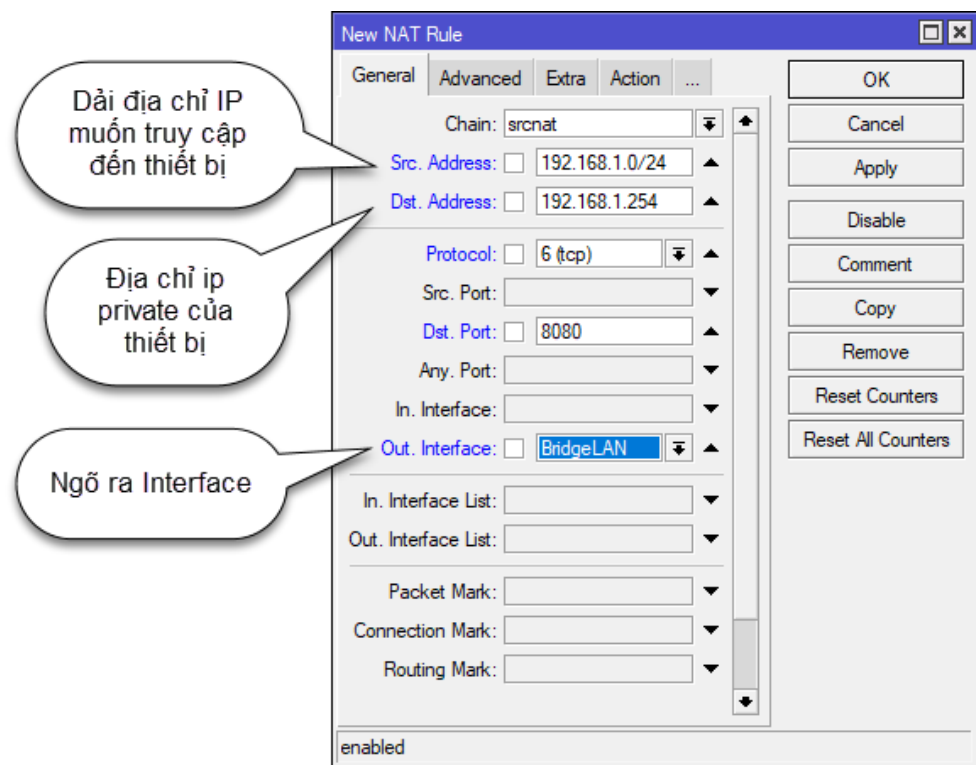


**Hình 9.6.** Tab action của màn hình NAT Rule

### 3.3. Hairpin NAT

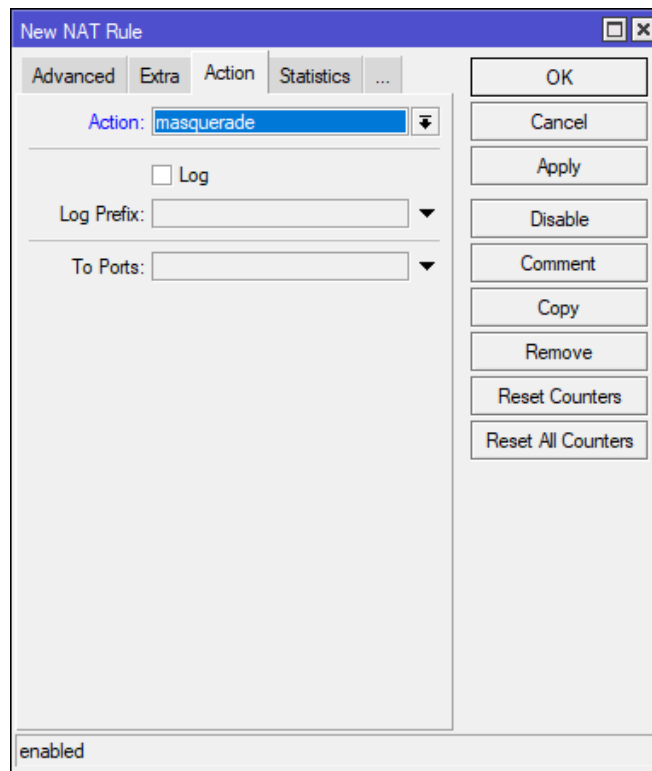
Hairpin NAT được sử dụng khi người dùng muốn truy cập đến thiết bị bên trong mạng nội bộ bằng IP public.

- **Bước 1:** vào IP >> Firewall >> NAT, bấm dấu + để thêm rule NAT mới. Tại tab General,
  - o Chain: srcnat
  - o Src. Address: dải địa chỉ IP local cần truy cập đến thiết bị
  - o Dst. Address: địa chỉ IP của thiết bị
  - o Protocol: 6(tcp)
  - o Dst. Port: port muốn truy cập đến
  - o Out. Interface: Interface mà traffic đi ra.



**Hình 9.7.** Tab general của màn hình New NAT Rule

- **Bước 2:** vẫn trong cửa sổ New NAT Rule, tại tab Action, mục Action: chọn masquerade



**Hình 9.8.** Tab action trong màn hình New NAT Rule

## BÀI 10. DHCP SNOOPING

### 1. Mô hình mạng

....

### 2. Thực hành



## BÀI 11. Simple Queues

### 1. Giới thiệu

There are a lot of articles on the Internet devoted to speed limits and traffic dividing on MikroTik equipment, but almost all of them consider only Queue Tree, which requires deep understanding and are redundant in many tasks and can be replaced by Simple Queues.

Simplified queues - the mechanism of dividing the bandwidth of the channel and prioritizing traffic associated with a specific goal (target). Incoming and outgoing traffic is calculated relative to the target.

### 2. Mô hình mạng:

...

### 3. Thực hành

#### 3.1. Giới hạn băng thông cố định cho một địa chỉ IP

- Vào Queue, chọn tab Simple Queues. Bấm dấu + để thêm simple queue mới.
  - o Name: đặt tên cho simple queue
  - o Target: mục tiêu muốn giới hạn băng thông
  - o Max Limit: giới hạn băng thông tối đa cho phép sử dụng.
  - o Burst Limit: băng thông ban đầu khi chưa bị giới hạn
  - o Burst threshold: băng thông khi người dùng cố tình sử dụng quá mức giới hạn sẽ bị giới hạn tiếp.
  - o Burst time: thời gian bắt đầu giới hạn băng thông.

The screenshot shows the 'Simple Queue <Giới hạn băng thông>' configuration window. The 'General' tab is active, showing the following settings:

- Name: Giới hạn băng thông
- Target: 192.168.1.120
- Max Limit: 10M (Target Upload) / 10M (Target Download) bits/s
- Burst Limit: 40M (Target Upload) / 40M (Target Download) bits/s
- Burst Threshold: 2M (Target Upload) / 2M (Target Download) bits/s
- Burst Time: 2 (Target Upload) / 2 (Target Download) s

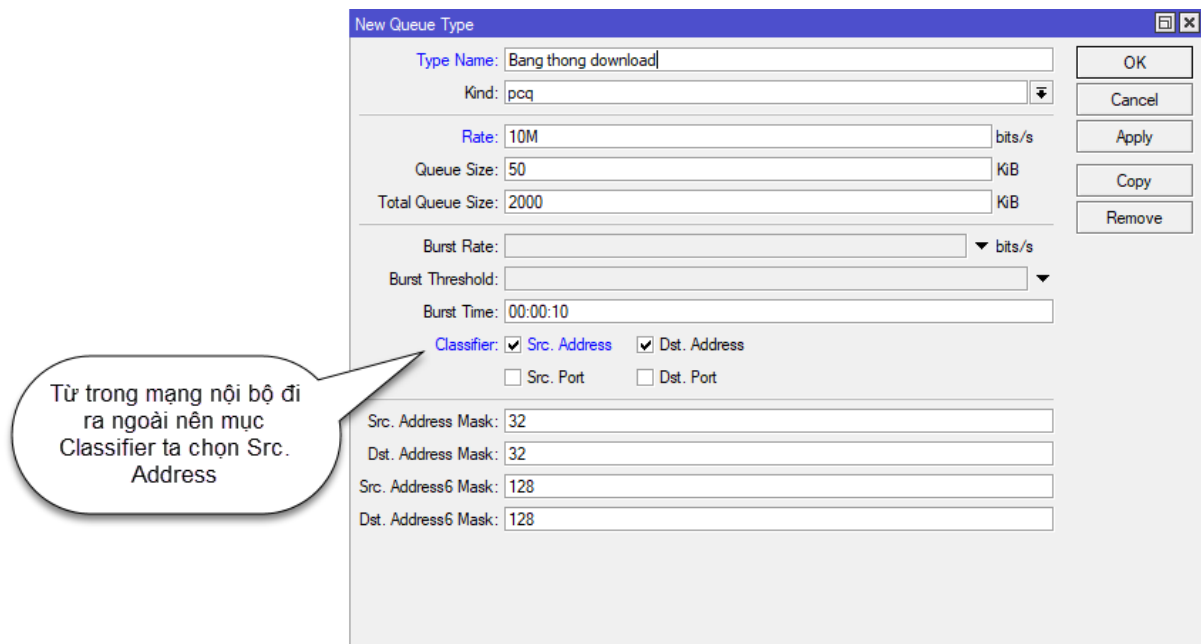
Callouts explain the fields:

- Địa chỉ IP hoặc lớp mạng muốn giới hạn băng thông (Target)
- Băng thông giới hạn tối đa là 10M (Max Limit)
- Băng thông cho phép trước 2s là 40M (Burst Limit)
- Ngưỡng bóp băng thông nếu người dùng sử dụng quá nhiều băng thông là 2M (Burst Threshold)
- Thời gian để bóp băng thông xuống là 2s (Burst Time)

**Hình 11.1.** Tab general của bảng Simple Queue

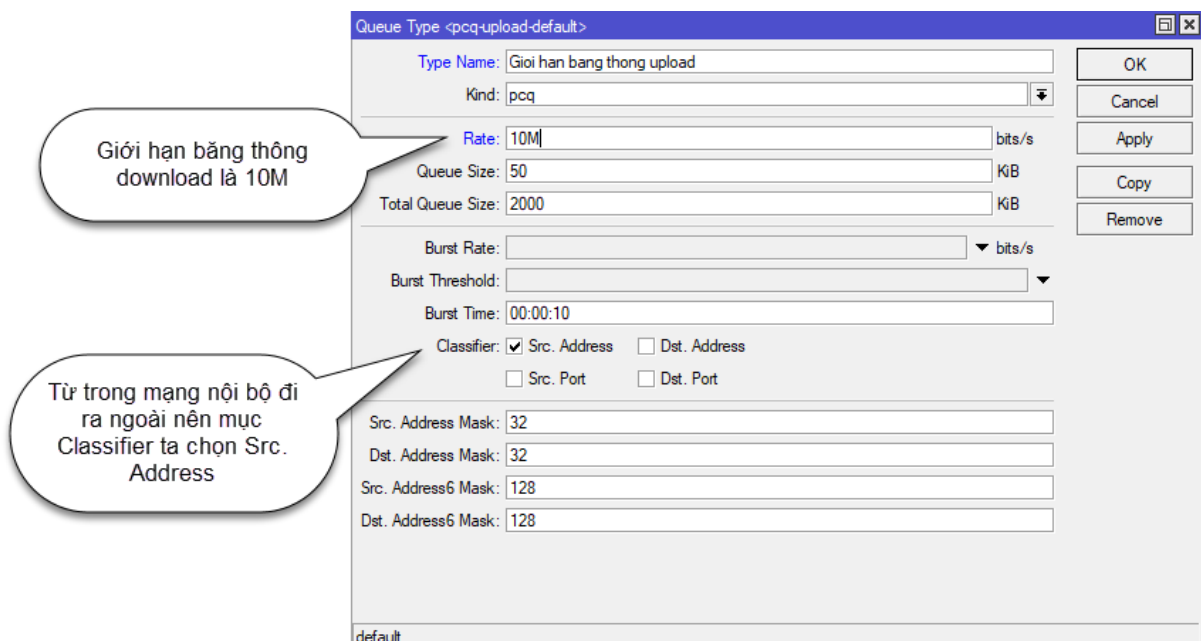
### 3.2. Giới hạn băng thông cố định cho một lớp mạng

- **Bước 1:** vào Queues, chọn tab Queue Types. Trong danh sách, bấm kép vào mục pcq-download-default. Bấm nút copy để tạo Queue Type mới.
  - o **Type Name:** đặt tên
  - o **Classifier:** chọn Src. Address



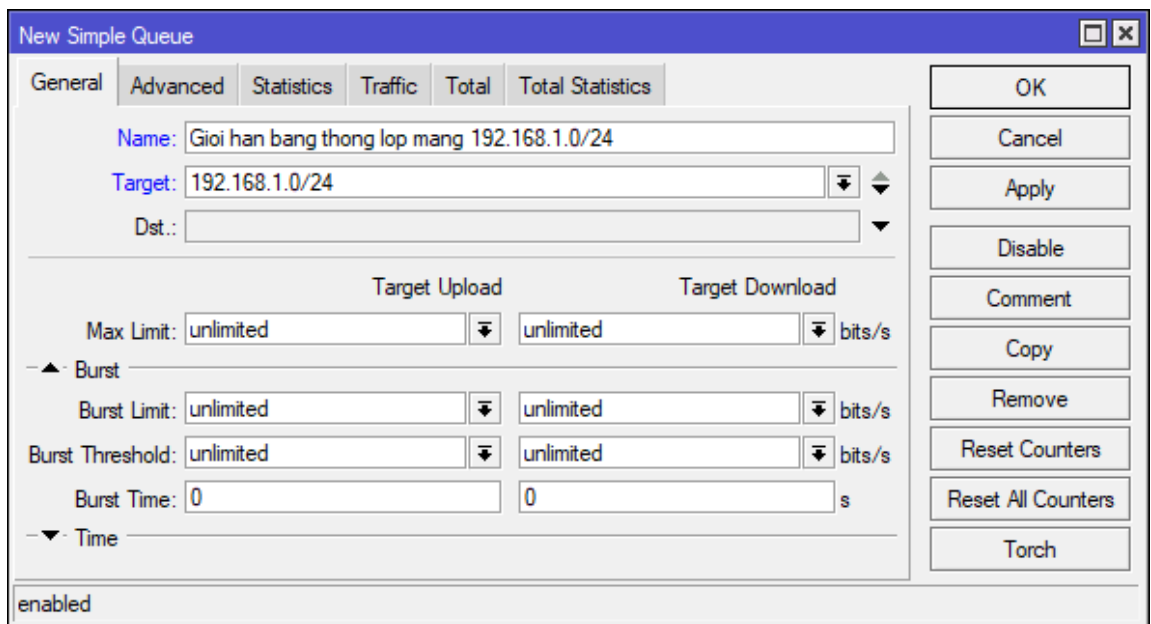
**Hình 11.2.** New queue type giới hạn băng thông download

- **Bước 2:** vẫn trong danh sách queue type, bấm kép vào mục pcq-upload-default. Bấm nút copy để tạo Queue Type mới.



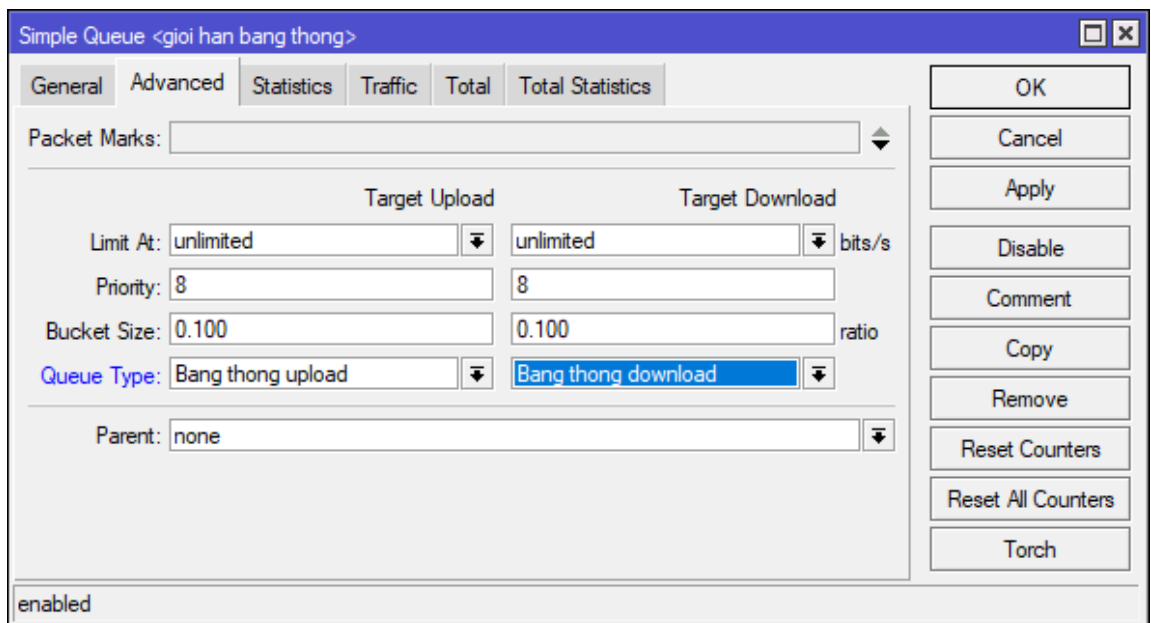
**Hình 11.3.** New queue type giới hạn băng thông upload

- **Bước 3:**



**Hình 11.4.** Tab general màn hình New simple queue

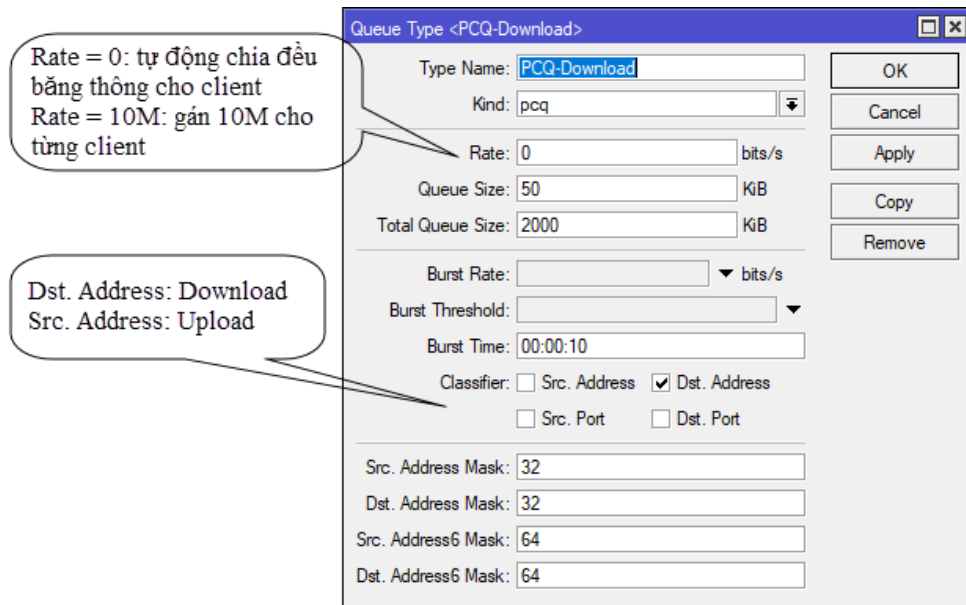
- **Bước 4:** vào tab Advance



**Hình 11.5.** Tab advanced của màn hình Simple queue

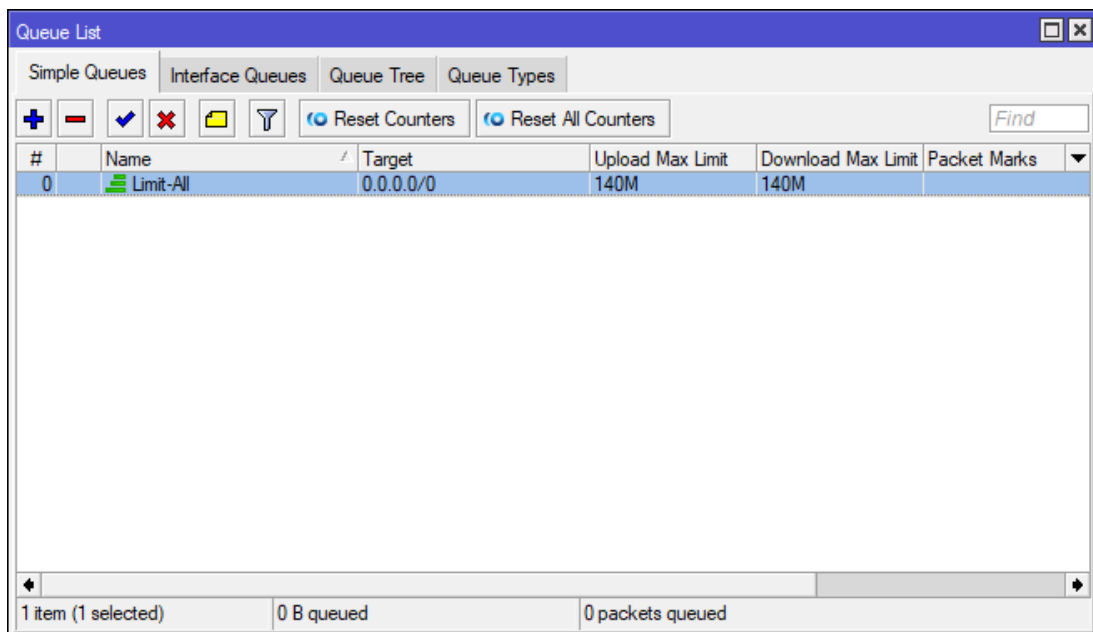
### 3.3. Giới hạn băng thông linh hoạt

- **Bước 1:** vào Queue → Queue Type → bấm kép vào pcq-download-default → copy.
- **Bước 2:** tạo queue có tên “PCQ-Download”. Cài đặt như hình bên dưới và làm tương tự cho “PCQ-Upload”



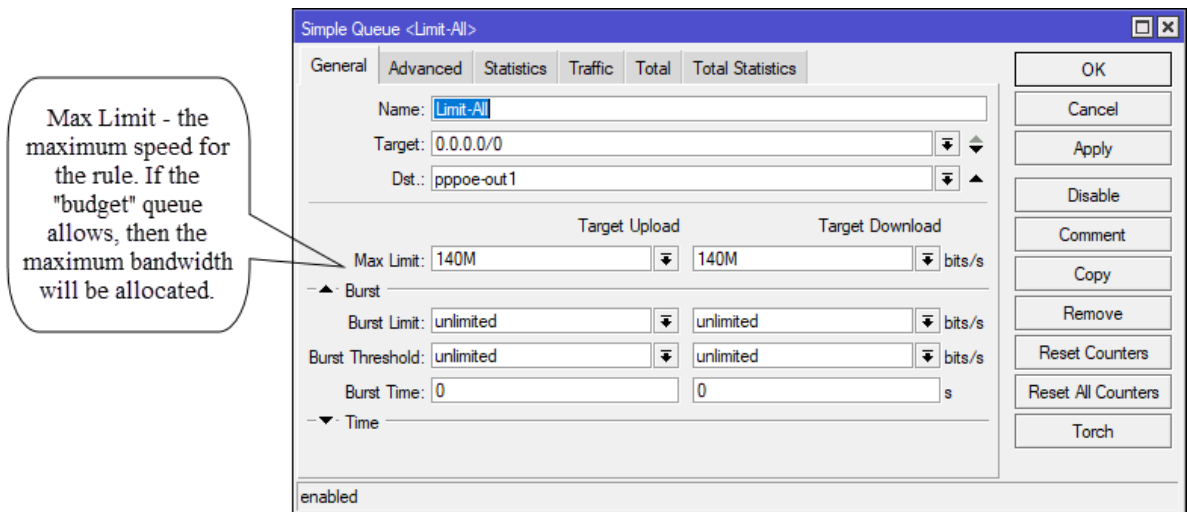
Hình 11.6. Queue Type: “PCQ-Download”

- **Bước 3:** bấm vào tab Simple Queues, bấm dấu + để tạo luật “Limit-All” như sau:

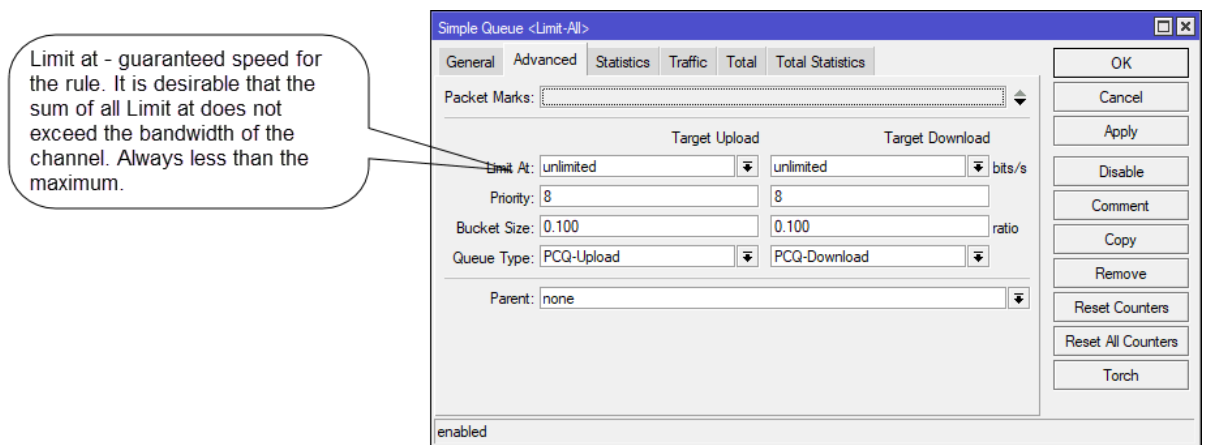


Hình 11.7. Tab Simple Queues

Max Limit: tổng băng thông cho phép của đường truyền



Hình 11.8. Tab general



Hình 11.9. Tab advanced

**3.4. Giới hạn băng thông bằng script**

- Sử dụng script sau để giới hạn băng thông cho một lớp mạng.

```
for e from 2 to 254 do={ /queue simple add name="IP- $\$e$ "
target="192.168.1. $\$e$ " max-limit=3M/3M burst-limit=40M/40M
burst-threshold=1M/1M burst-time=2/2s}
```

## BÀI 12. VPN L2TP/IPSec

### 1. Giới thiệu:

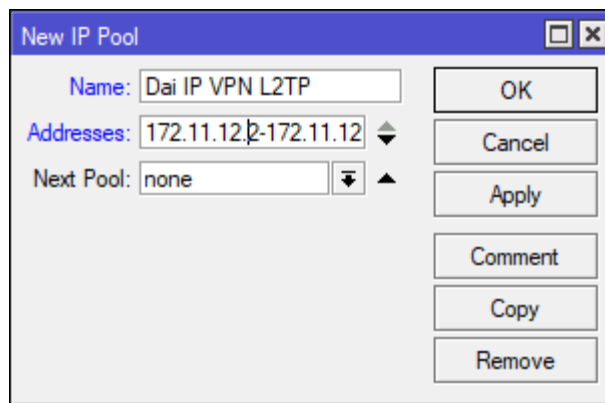
...

### 2. Mô hình mạng:

...

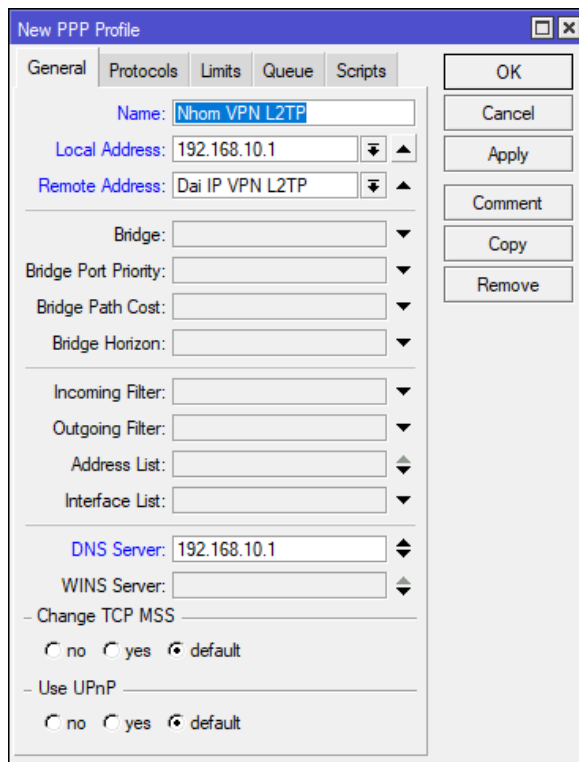
### 3. Thực hành:

- **Bước 1:** khởi tạo dải IP cho VPN user. Vào IP >> Pool. Trong tab Pools, bấm dấu + để thêm pool mới.
  - o **Name:** đặt tên cho dải IP
  - o **Address:** 172.11.12.2-172.11.12.100



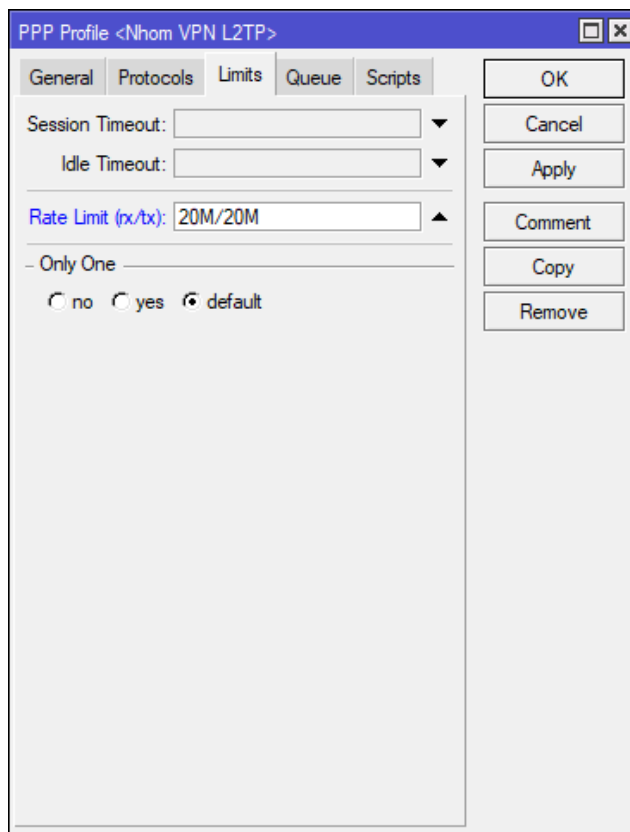
**Hình 12.1.** New IP Pool cho dải IP VPN

- **Bước 2:** khởi tạo nhóm người dùng kết nối L2TP. Nhóm người dùng này chứa các thông tin về băng thông kết nối, loại IP ... Vào PPP, chọn Profiles, bấm dấu + để thêm profiles mới.
  - o **Name:** tên nhóm
  - o **Local Address:** địa chỉ IP gateway
  - o **Remote Address:** pool đã tạo ở bước 1



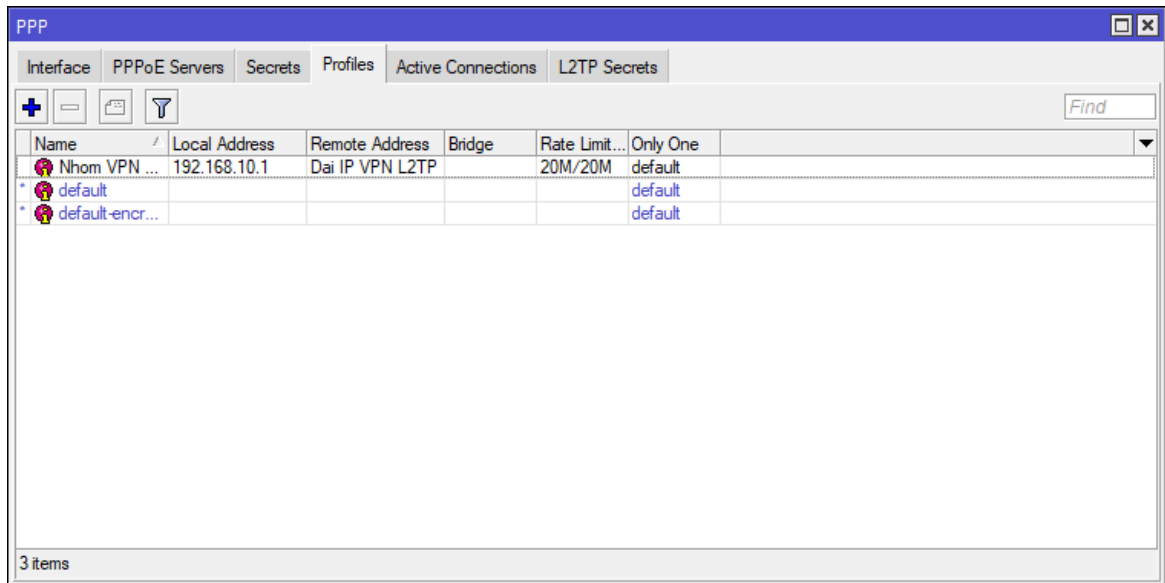
**Hình 12.2.** Tab general của màn hình New PPP Profile

- **Bước 3:** giới hạn băng thông cho user VPN. Vào tab Limits, mục Rate Limit: nhập 20M/20M



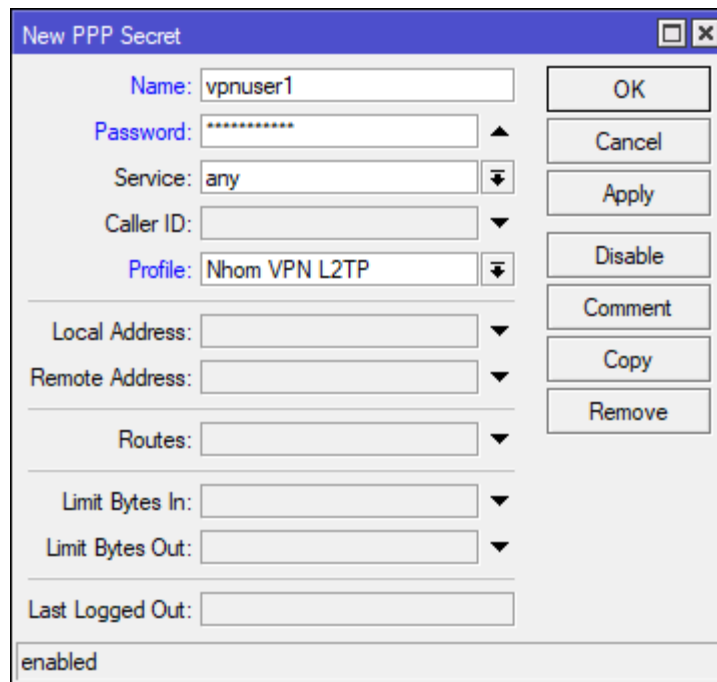
**Hình 12.3.** Tab Limits của màn hình New PPP Profile

- Sau khi thực hiện xong, tab Profiles của màn hình PPP như sau:



**Hình 12.4.** Tab profiles của màn hình PPP

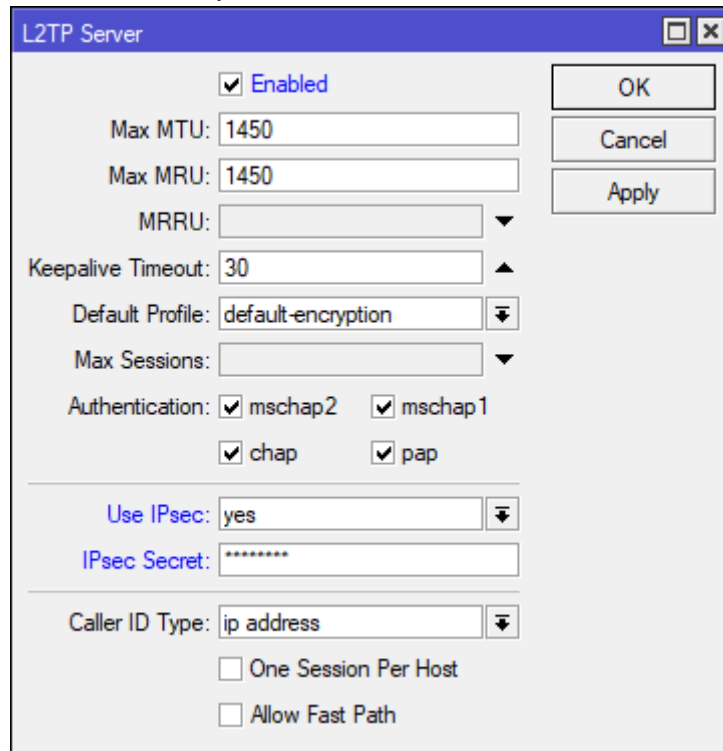
- **Bước 4:** tạo user VPN. Vẫn trong màn hình PPP, vào tab Secrets. Bấm dấu + để thêm user mới.
  - o **Name:** tên đăng nhập
  - o **Password:** mật khẩu
  - o **Profile:** chọn nhóm VPN L2TP đã tạo trước.



**Hình 12.5.** Màn hình New PPP Secret



- **Bước 5:** bật dịch vụ L2TP. Vẫn trong màn hình PPP, vào tab Interface, bấm nút L2TP Server,
  - o check vào ô Enabled.
  - o Use Ipsec: yes
  - o Ipsec Secret: mã bí mật của IPsec



**Hình 12.6.** Bật dịch vụ L2TP