Introduction to MikroTik

● What is MikroTik?

MikroTik is a Latvian company that develops hardware and software for Internet connectivity and network management. Its most popular products are **RouterOS** (an operating system) and **RouterBOARD** (hardware). MikroTik routers are widely used in small to large organizations for configuring and managing networks including tasks like firewall, bandwidth control, VPN, hotspot, and routing.

● Introduction to RouterOS and RouterBOARD

▪ RouterOS:

RouterOS is MikroTik's proprietary operating system based on the Linux kernel. It is installed on MikroTik routers and provides a wide range of features for network configuration and management. Key functions include:

- IP Routing
- Firewall
- Bandwidth Management
- VPN
- DHCP Server
- Hotspot
- Wireless Configuration

▪ RouterBOARD:

RouterBOARD is the hardware product line from MikroTik. These are purpose-built router boards that come pre-installed with RouterOS. Various models are available depending on the use case, such as hAP, RB750, CCR, etc.

● Using Winbox, WebFig, CLI, and Mobile App

▪ Winbox:

Winbox is a Windows-based graphical configuration utility for MikroTik routers. It allows users to view and manage all settings of the router through a user-friendly interface. It can be downloaded from MikroTik's official website.

▪ WebFig:

WebFig is a web browser-based configuration interface. You can access it by entering the MikroTik router's IP address into a browser and logging in. It offers a full set of configuration options.

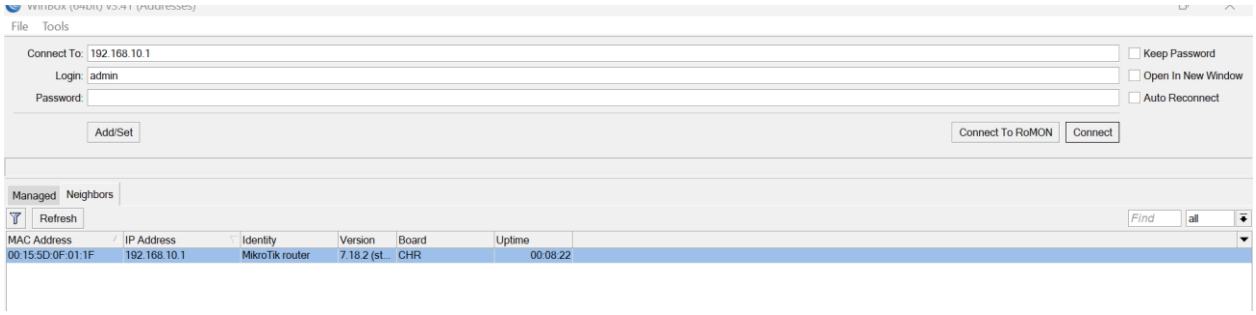
▪ **CLI (Command Line Interface):**

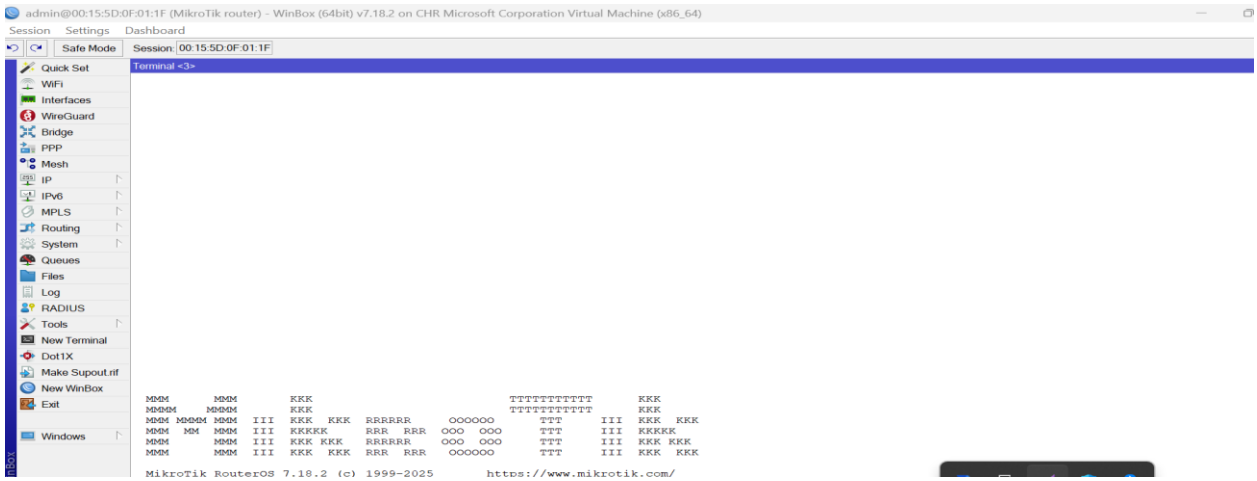
The CLI is a text-based interface accessed through the terminal or SSH. It is used for faster configuration and scripting, especially useful for advanced users.

Basic Configuration

Step 1: Login to MikroTik

- Open **Winbox** or a web browser and connect to the MikroTik router using **MAC address** or **IP**.
- Default login:
    - Username: admin
    - Password: *(blank)*

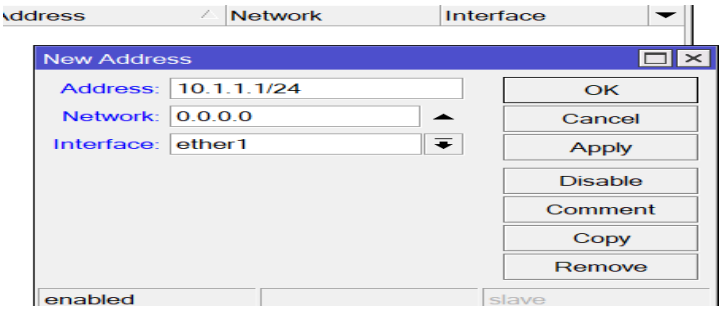




IP Address Configuration (LAN & WAN)

1. **Go to IP in the menu.**
2. **Click on Addresses.**
3. **In the Addresses window, click the + button at the top to add a new address.**
4. **Fill in the details as follows:**
    - **Address: 10.1.1.1/24**
    - **Interface: Select ether1 from the dropdown list.**
5. **Click OK to apply the settings.**

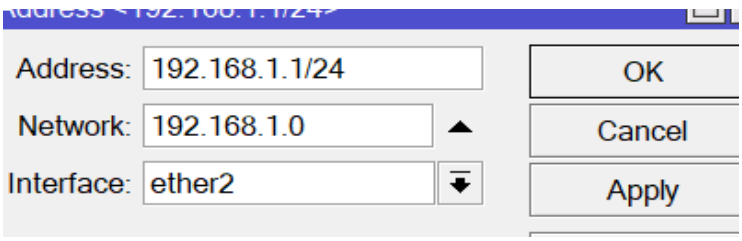
This will assign the IP address 10.1.1.1/24 to the WAN interface ether1

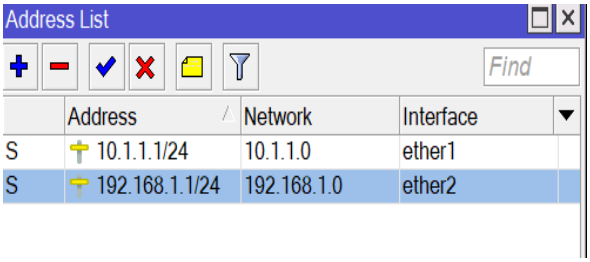


LAN Interface (ether2) IP

1. Enter the following details:
    - **Address**: 192.168.1.1/24
    - **Interface**: Select **ether2** from the dropdown list.
2. Click **Apply** and then **OK** to save the settings.

This will assign the IP address 192.168.1.1/24 to the LAN interface **ether2**.

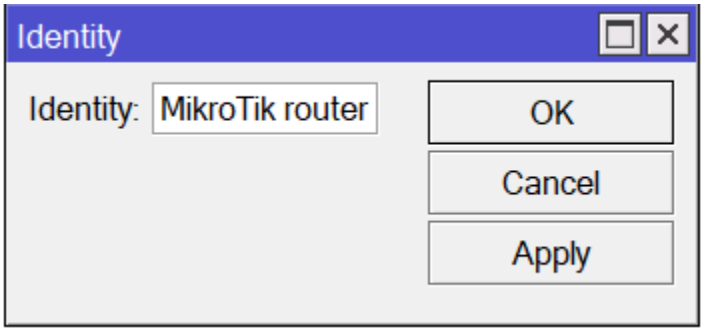




Router Identity ؛ Password Change

1. **Go to System in the menu.**
2. **Click on Identity.**
3. **In the Name field, enter the desired name for the router, such as MyRouter (or any name you prefer).**
4. **Click Apply and then OK to save the changes.**

This will change the router's name to MyRouter or the name you provided.

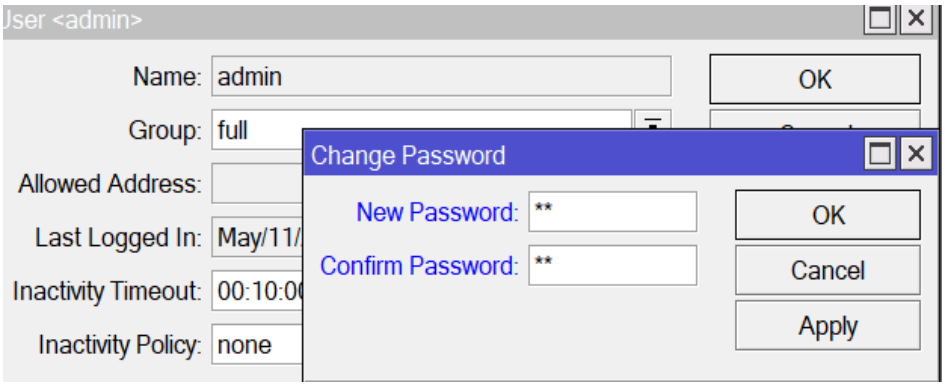


8.٢ -

To change the password for the admin user on MikroTik, follow these steps:

1. **Go to System in the menu.**
2. **Click on Users.**
3. **Double-click on the admin user to open the settings.**
4. **In the New Password field, enter the new password.**
5. **In the Confirm Password field, re-enter the same new password.**
6. **Click Apply and then OK to save the changes.**

This will update the password for the admin user.

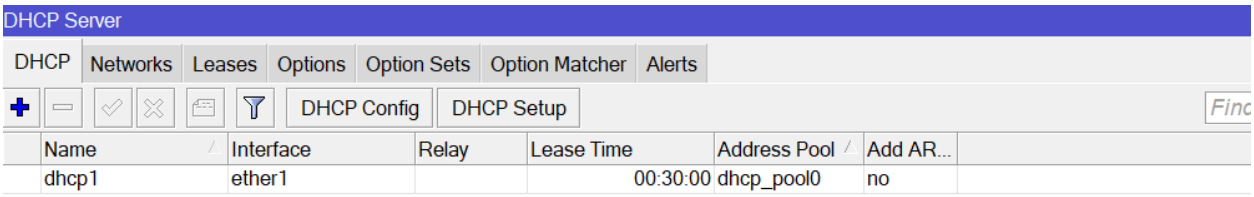


DHCP Server Setup (LAN Interface)

To set up DHCP for automatically assigning IP addresses to LAN devices (on ether2 with IP 192.168.1.1/24), follow these steps:

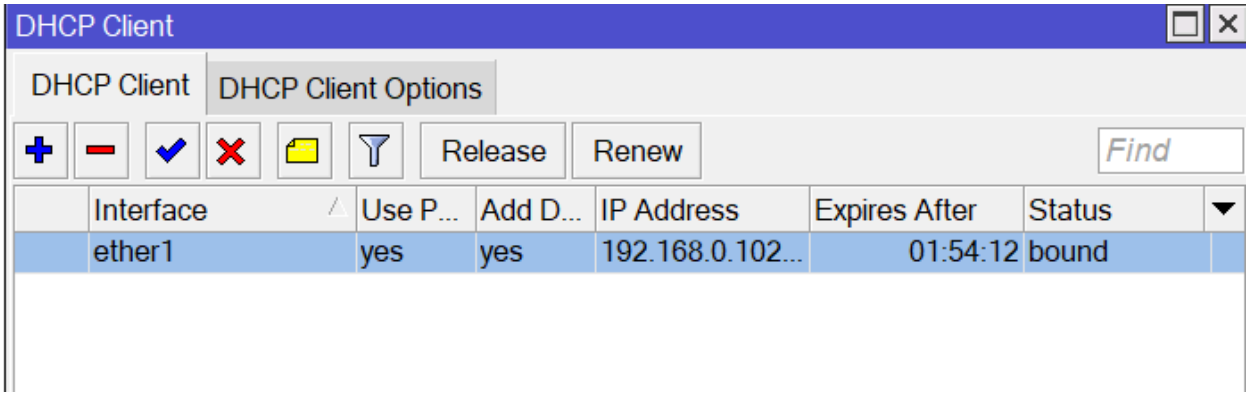
1. **Go to IP in the menu, then click on DHCP Server.**
2. **Click on DHCP Setup to start the configuration.**
3. **Select ether2 as the Interface and click Next.**
4. **For DHCP Address Space, enter 192.168.1.0/24 and click Next.**
5. **For Gateway, enter 192.168.1.1 (this is the LAN IP address of the router) and click Next.**
6. **For Address to Give Out, enter the range 192.168.1.10 - 192.168.1.254 to define the IP range for DHCP allocation, then click Next.**
7. **For DNS Server, enter 8.8.8.8 or 192.168.1.1 (depending on your preference) and click Next.**
8. **For Lease Time, you can leave it at the default (10 minutes or 1 hour), then click Next.**
9. **Click Apply to apply the settings.**

Now, the router will automatically assign IP addresses to LAN devices in the range 192.168.1.10 - 192.168.1.254.



DHCP Client Setup (WAN Interface)

- **To set up the MikroTik Router to automatically receive an IP address from the WAN (ether1), follow these steps:**
- **Go to IP in the menu, then click on DHCP Client.**
- **Click the + (Add) button to add a new DHCP client.**
- **In the Interface field, select ether1 (the WAN interface).**
- **Below, make sure the following options are checked:**
- ✅ **Add Default Route**
- ✅ **Use Peer DNS**
- **Click Apply, and then OK to save the settings.**
- **Now, the MikroTik router will automatically receive an IP address from the WAN network via the DHCP client on ether1.**



NAT . **Static Lease Bind (নির্**

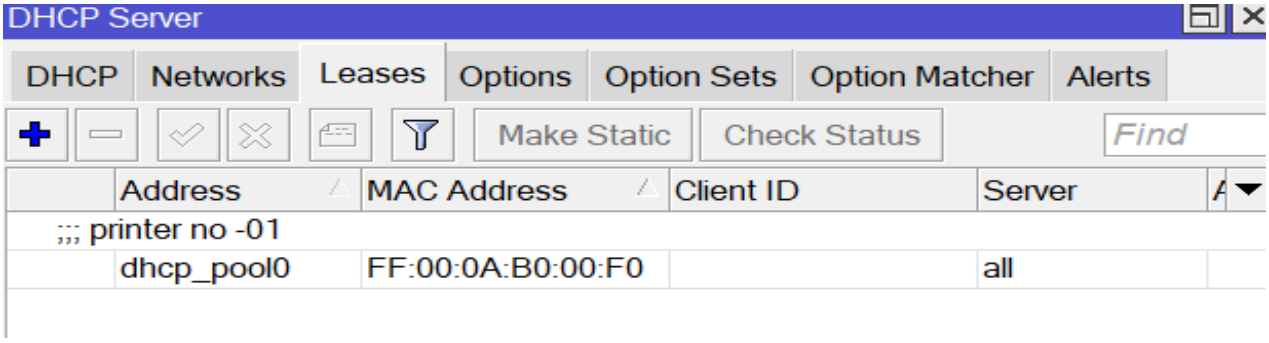
To make a DHCP lease static on MikroTik, follow these steps:

1. Go to **IP** in the menu and then click on **DHCP Server**.

2. Click on the **Leases** tab to view the devices that have received IP addresses via DHCP.
3. Right-click on the lease for the device you want to make static, then click **Make Static**.
4. Optionally, double-click on the static lease entry to edit the following details:
    - **Address**: Enter the IP address you want to assign (e.g., 192.168.1.100).
    - **MAC Address**: This will auto-populate.
    - **Comment**: Enter a descriptive name for the device, such as "Printer", "PC-1", etc.
5. Click **Apply** and then **OK** to save the changes.

This will make the DHCP lease static, ensuring that the device always gets the same IP address.

1. **Apply > OK**



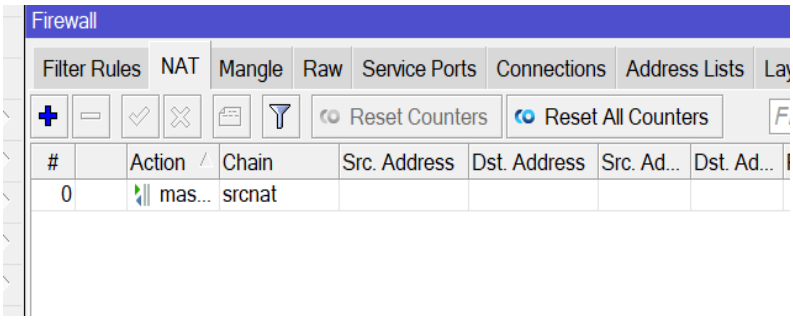
NAT Configuration in MikroTik:

To set up NAT (Network Address Translation) for outgoing traffic through the WAN interface (ether1) on MikroTik, follow these steps:

1. Go to **IP** in the menu, then click on **Firewall**.
2. Navigate to the **NAT** tab.

3. Click on the **+** (Add New Rule) button to add a new NAT rule.
4. In the **General** tab:
    - **Chain**: Select **srcnat**.
    - **Out Interface**: Select **ether1** (the WAN interface).
5. Go to the **Action** tab:
    - **Action**: Select **masquerade**.
6. Click **Apply** and then **OK** to save the rule.

This will enable NAT and allow devices on the LAN to access the internet through the WAN interface (ether1) by masquerading the source IP address.



Destination NAT (Port Forwarding):

To set up port forwarding (redirecting port 80 from the public IP to a local device), follow these steps:

Example:

- **Public IP (WAN): 10.1.1.1**
- **Local Device IP: 192.168.1.100**
- **Port to Forward: 80 (HTTP)**

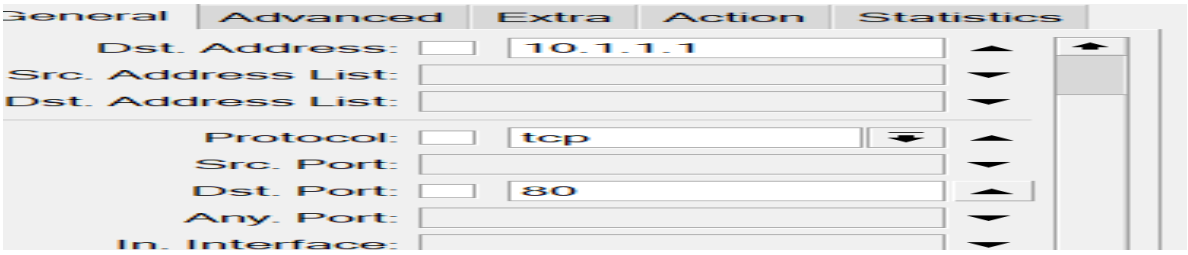
Step-by-Step:

1. **Go to IP in the menu, then click on Firewall.**
2. **Navigate to the NAT tab.**
3. **Click on the + (Add New Rule) button to create a new NAT rule.**

4. **In the General tab:**
    - **Chain: Select dstnat.**
    - **Dst. Address: Enter 10.1.1.1 (the public IP address).**
    - **Protocol: Select tcp.**
    - **Dst. Port: Enter 80 (the port to forward).**
5. **Go to the Action tab:**
    - **Action: Select dst-nat.**
    - **To Addresses: Enter 192.168.1.100 (the local device IP).**
    - **To Ports: Enter 80 (the local port on the device).**
6. **Click Apply and then OK to save the rule.**

Result:

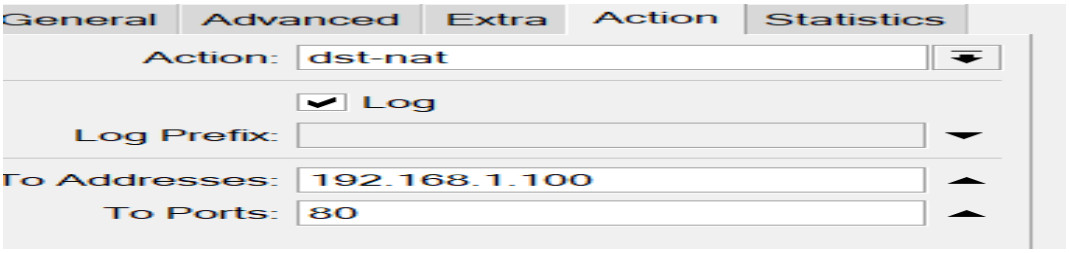
Now, any incoming traffic to 10.1.1.1:80 will be redirected to 192.168.1.100:80 (the local device), enabling access to the internal web server.



Action tab:

- **Action: dst-nat**
- **To Addresses: 192.168.1.100**
- **To Ports:** 80

2. **Apply > OK**



Hairpin NAT

To allow LAN devices to access a local server via the public IP, you'll need to set up a Source NAT (srcnat) rule. This will ensure that when LAN devices access the server through the public IP, it is properly routed to the internal IP address.

Example:

- **Server IP: 192.168.1.100**
- **Public IP: 10.1.1.1**
- **LAN Network: 192.168.1.0/24**

Step-by-Step:

A. Source NAT (For LAN to Public IP access)

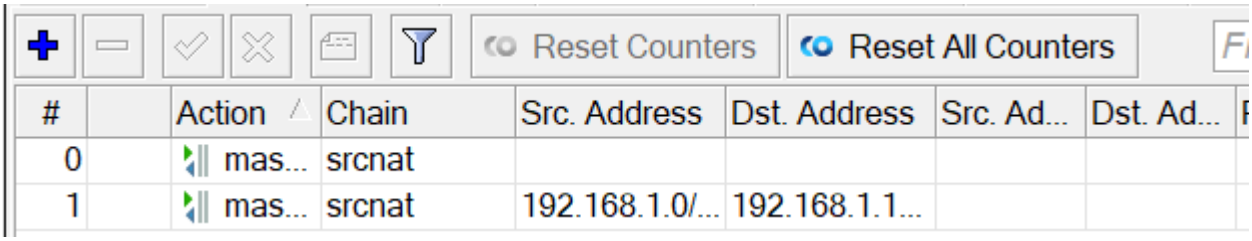
1. **Go to IP in the menu, then click on Firewall.**
2. **Go to the NAT tab and click on the + (Add New Rule) button.**
3. **In the General tab:**
    - **Chain: Select srcnat.**
    - **Src. Address: Enter 192.168.1.0/24 (this is the LAN subnet).**
    - **Dst. Address: Enter 192.168.1.100 (the local server IP).**
4. **In the Action tab:**
    - **Action: Select masquerade (to hide the LAN IP and use the router's public IP for outbound traffic).**
5. **Click Apply, then OK to save the rule.**

Result:

This rule ensures that when LAN devices access the server with 192.168.1.100, the source address is masqueraded to the router's public IP.

After this, you can proceed with the destination NAT (dstnat) rule to complete the redirection from public IP to local server.

1. **Apply > OK**



To configure filter rules for controlling access and blocking ICMP (ping) from the WAN interface (ether1) to the router, follow these steps:

Example:

- Objective: Block ICMP (ping) requests coming from the WAN (ether1) to the router.

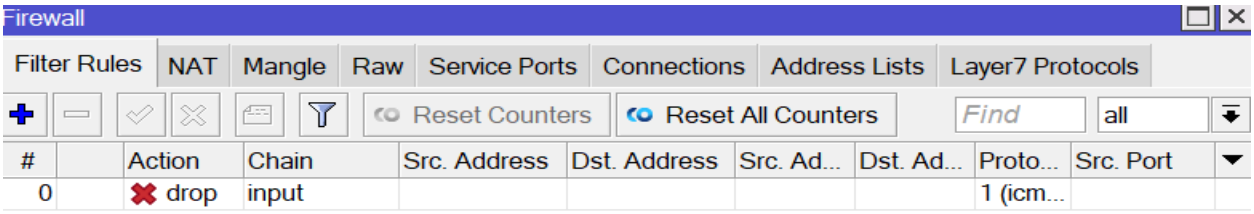
Step-by-Step:

A. Block ICMP (Ping) from WAN to Router:

1. Go to IP in the menu, then click on Firewall.
2. Click on the Filter Rules tab and then click the + (Add New Rule) button.
3. In the General tab:
    - Chain: Select input (to filter traffic destined for the router).
    - Protocol: Select icmp (this specifies that you want to block ping requests).
    - In Interface: Select ether1 (the WAN interface).
4. In the Action tab:
    - Action: Select drop (to drop the ping requests).
5. Click Apply, then OK to save the rule.

Result:

This rule will block ICMP (ping) requests from the WAN (ether1) interface to the MikroTik router, effectively preventing external users from pinging the router.



To create an **Address List** to block or allow a specific IP address (for example, 192.168.1.100), follow these steps:

Example:

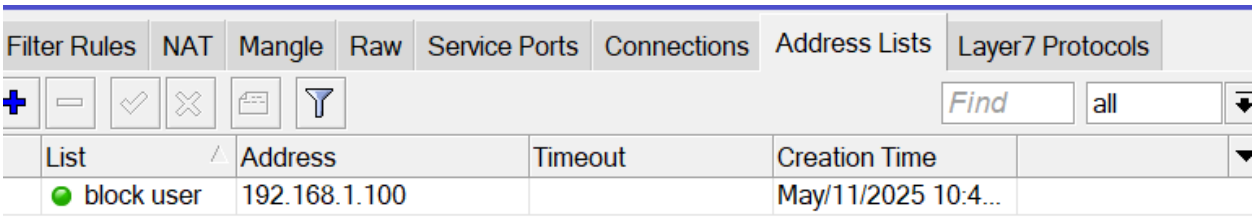
- **IP to Block or Allow**: 192.168.1.100
- **List Name**: blocked-users (you can name it as you like)

Step-by-Step:

1. Go to **IP** in the menu, then click on **Firewall**.
2. Click on the **Address Lists** tab.
3. Click the **+** (Add New) button to add a new entry.
4. In the **Address** field, enter the IP address you want to block or allow (e.g., 192.168.1.100).
5. In the **List Name** field, give a descriptive name for the list, such as blocked-users.
6. Click **Apply**, then **OK** to save the address list.

Result:

Now, the IP 192.168.1.100 will be added to the blocked-users address list, and you can



use this list in firewall rules to block or allow traffic from this IP.

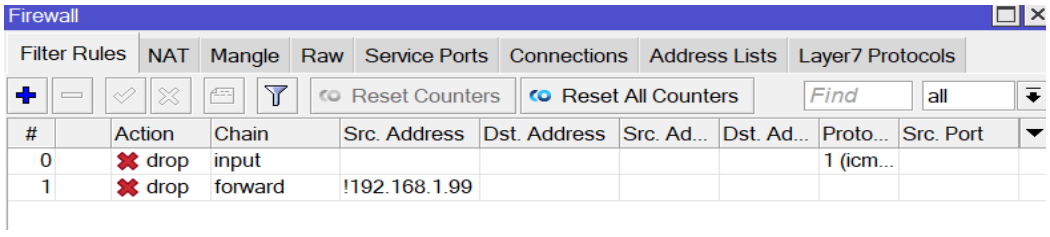
Block Traffic Using Address List (Filter Rule)

Step-by-step:

1. Go to **IP > Firewall > Filter Rules**.
2. Click **+** to add a new rule.
3. In the **General** tab:
   - **Chain**: Select forward
   - **Src. Address List**: Enter the name of the list (e.g., blocked-users)
4. Go to the **Action** tab:
   - **Action**: Select drop
5. Click **Apply**, then **OK**.

Result:

Now, any device with an IP in the blocked-users address list will have its traffic dropped — it won't be able to reach the internet or other networks through the router.

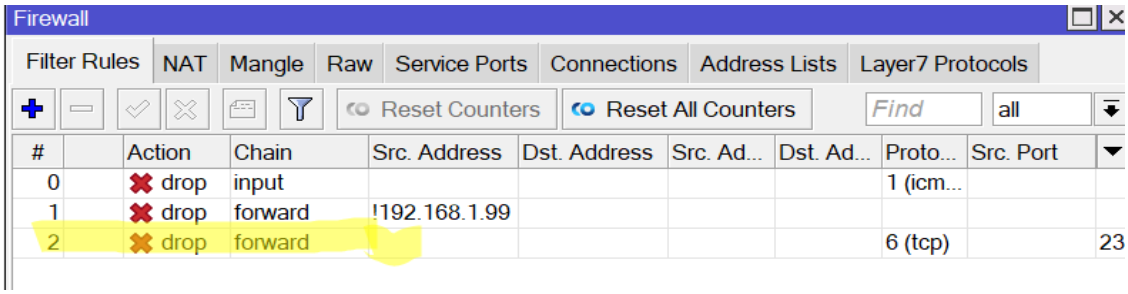


To **block a specific port** (like TCP port 23 for Telnet) using MikroTik's **firewall filter rules**, follow this step-by-step guide:

✅ Block TCP Port 23 (Telnet)

Step-by-Step:

1. Go to **IP > Firewall > Filter Rules**
2. Click **+** (Add) to create a new rule
3. In the **General** tab:
   - **Chain**: `forward`
   - **Protocol**: `tcp`
   - **Dst. Port**: `23`
4. Go to the **Action** tab:
   - **Action**: `drop`
5. Click **Apply**, then **OK**



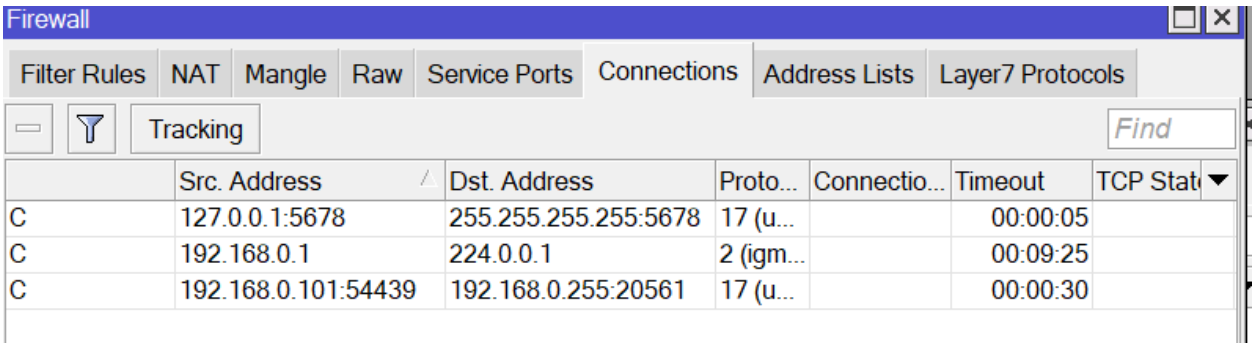
Connection

View Active Connections (Tracking)

Step-by-step:

1. **Go to IP > Firewall**
2. **Click on the Connections tab**

Active Connection



. Routing

- Static Routing
- Gateway configuration
- Distance, Routing mark

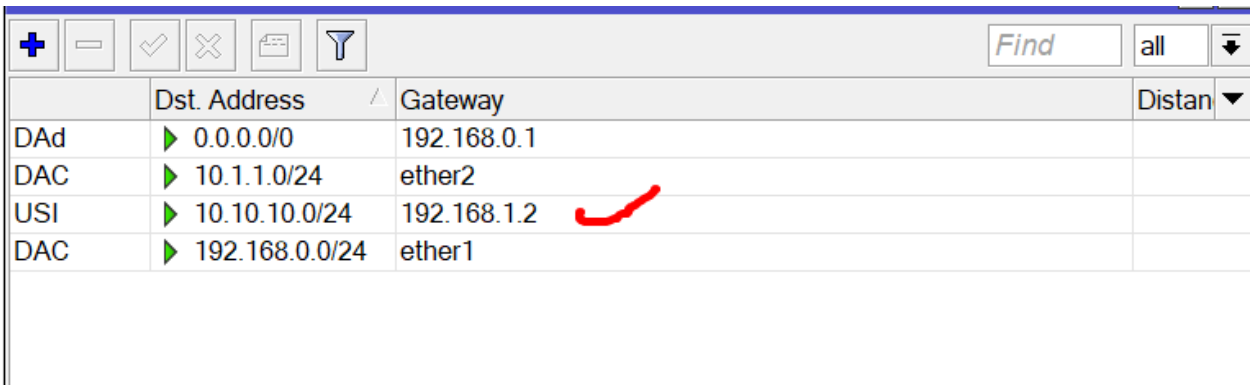
Static Routing Configuration

Static Route Configuration Example

Objective: Allow LAN (192.168.1.0/24) to reach network 10.10.10.0/24 via gateway 192.168.1.2

- Step-by-Step:
  1. Go to IP > Routes
  2. Click the + button to add a new route
  3. In the General tab:
     - Dst. Address: 10.10.10.0/24
     - Gateway: 192.168.1.2
  4. Click Apply, then OK

✅ Now, whenever a packet is destined for the 10.10.10.0/24 network, it will be routed through the gateway 192.168.1.2



Gateway Configuration (Default Route)

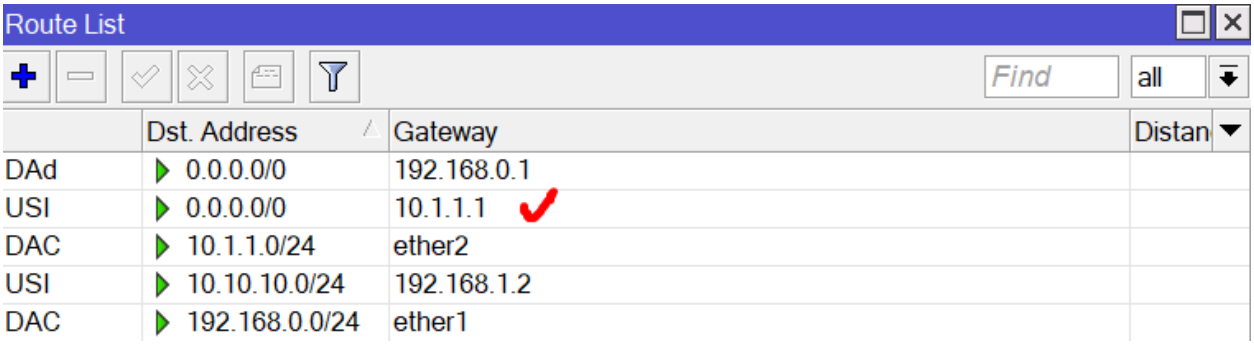
- Step-by-Step (Default Route Setup):

1. Go to IP > Routes
2. Click + (to add a new route)
3. In the General tab:
    - Dst. Address: 0.0.0.0/0

This means "any unknown destination"

- Gateway: 10.1.1.1

4. Click Apply, then OK



✅ **What is Distance?**

- **Distance = route preference (priority)**
- **Lower distance = higher priority**
- **Default value is 1**
- **If you want a backup route, assign it a higher distance**

🔹 **Example: Failover Routing**

Route Type	Gateway IP	Distance	Purpose
Primary	10.1.1.1	1	Main internet route
Secondary	10.1.1.2	2	Backup (used if primary fails)

💡 **How It Works:**

- **The router will use the gateway 10.1.1.1 as long as it's reachable.**
- **If 10.1.1.1 fails (e.g., cable unplugged or interface down), the router will automatically switch to 10.1.1.2.**

✅ **To Configure (Step-by-Step):**

1. **Go to IP > Routes > +**
2. **Dst. Address: 0.0.0.0/0**
3. **Gateway: 10.1.1.1**
4. **Distance: 1**
5. **Apply > OK**

Repeat for the second route:

1. **Again go to IP > Routes > +**
2. **Dst. Address: 0.0.0.0/0**
3. **Gateway: 10.1.1.2**
4. **Distance: 2**
5. **Apply > OK**

Routing Mark (Policy-Based Routing)

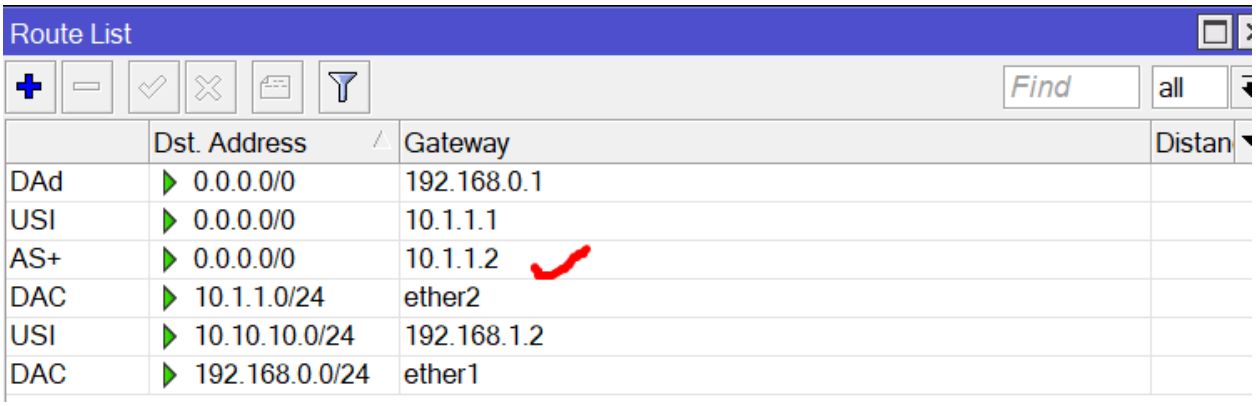
Reason for Using Routing Mark:

- Route different users/groups through different gateways (Policy-Based Routing).
    - Step-by-Step (Brief):

1. Go to IP > Firewall > Mangle > +
2. Set the following:
    - Chain: prerouting
    - Src. Address: 192.168.1.100 (or the address of the user/group you want to route differently)
    - Action: mark routing
    - New Routing Mark: via-isp2 (name it according to the gateway you want to use)
3. Click Apply, then OK

1. **IP > Routes > +**
    - Dst Address: 0.0.0.0/0
    - Gateway: 10.1.1.2
    - Routing Mark: via-isp2

✅ users with the IP **192.168.1.100** will route their internet traffic through the gateway



10.1.1.2, as we created a **Routing Mark** via-isp2 and configured it with a specific **Routing Rule**

Bridge & VLAN Configuration:

.

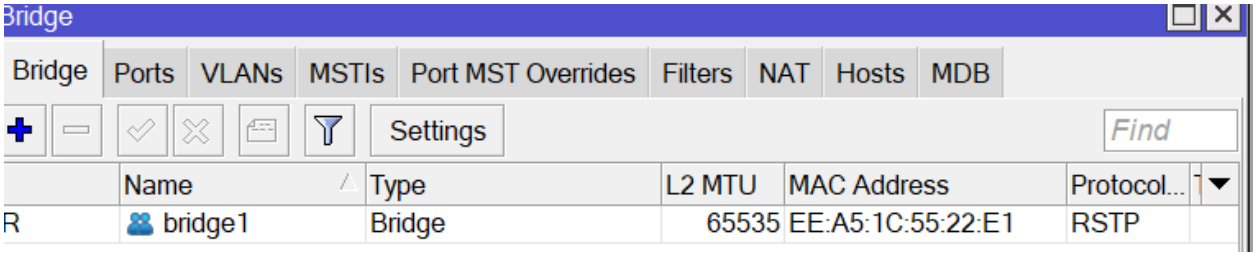
Bridge Creation in MikroTik:

A Bridge allows you to combine multiple network interfaces into a single logical interface, enabling communication between devices on those interfaces as if they are part of the same network.

- **Step-by-Step:**
  1. **Go to Interfaces > Bridge**
  2. **Click + (to add a new bridge)**
  3. **In the Name field, type: bridge1 (or your preferred name)**
  4. **Click Apply, then OK**

Now you've successfully created a bridge! You can add interfaces (like ether1, ether2) to this bridge to allow devices on those interfaces to communicate with each other.

✅ **Now, you have created a Bridge, where multiple physical interfaces can be grouped together. This allows devices on those interfaces to communicate as if they are on the same**

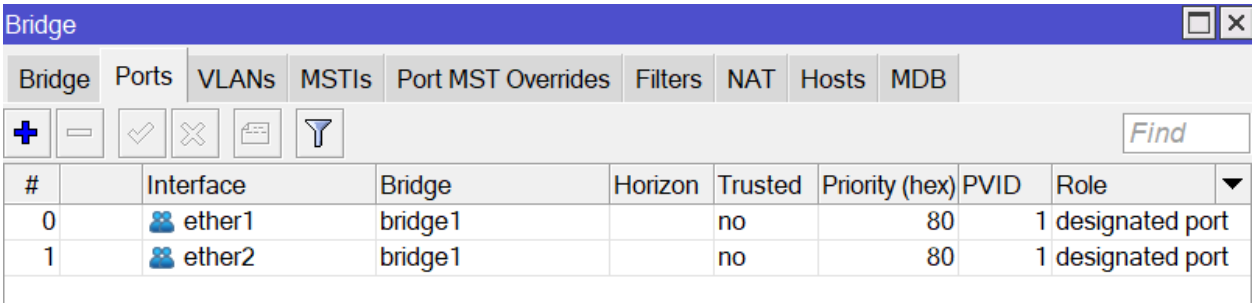


Adding Network Ports to the Bridge:

✅ **Example: Adding ether2 and ether3 to the Bridge.**

1. **Go to Interfaces > Bridge > Ports tab and click +.**
2. **In the Interface field, select ether2, and in the Bridge field, select bridge1.**
3. **Click Apply, then OK.**
4. **Click + again, this time select ether3 as the interface, and bridge1 as the bridge.**
5. **Click Apply, then OK.**

✅ **Now, ether2 and ether3 are both added to the same bridge, meaning they will be in the same Broadcast Domain**



Creating VLAN and Routing:

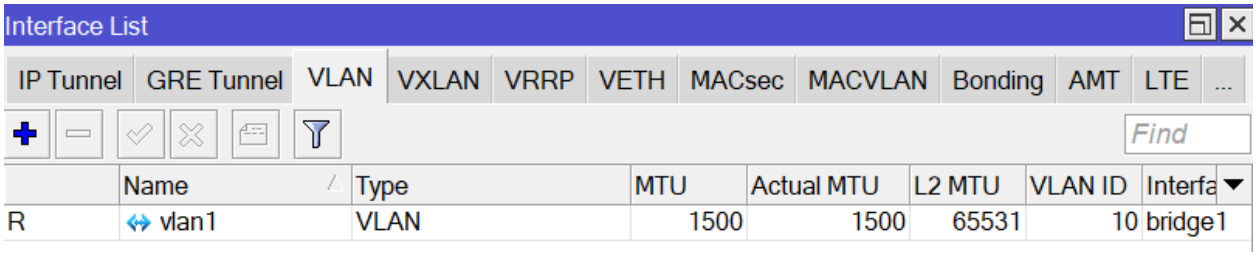
✅ **Step-by-Step to create VLAN10 (ID: 10) and assign an IP:**

1. **Go to Interfaces > VLAN and click +.**
2. **Enter the following details:**
   - **Name: vlan10**
   - **VLAN ID: 10**

- **Interface: Select bridge1 (or the interface where you want the VLAN to be configured)**

3. **Click Apply, then OK.**

This will create VLAN10. Now, you can assign an IP address to this VLAN interface for routing purposes



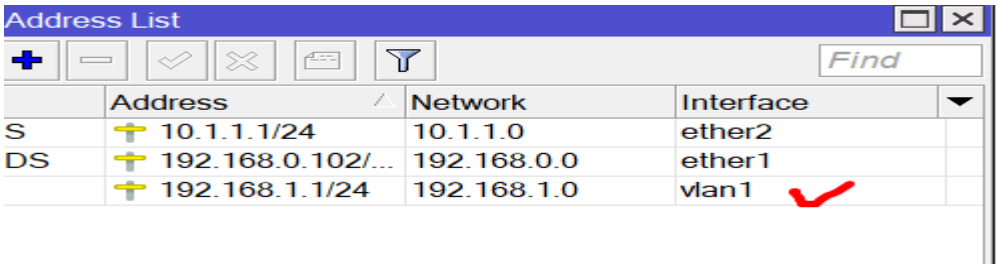
Assigning IP to VLAN10:

✅ Step-by-Step to assign an IP address to VLAN10:

1. Go to IP > Addresses and click +.
2. Enter the following details:
   - Address: 192.168.10.1/24
   - Interface: vlan10
3. Click Apply, then OK.

✅ Routing for VLAN10:

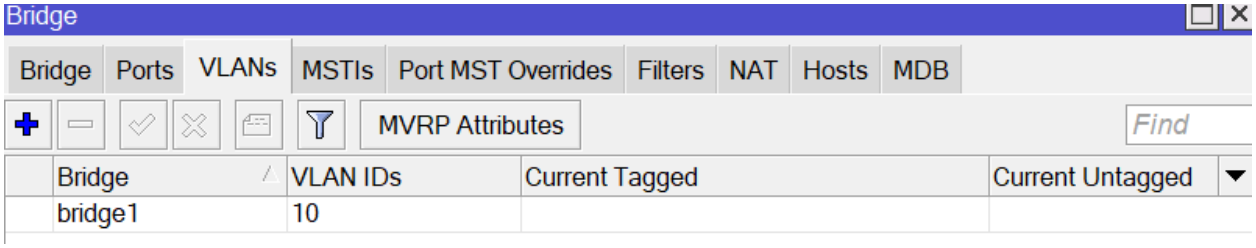
- If you want to route between VLANs, assign an IP to each VLAN (as you've done for VLAN10), and then add Static Routes for inter-VLAN communication.



Trunk Port Configuration (Where different VLAN tags will go):

1. **Go to Interfaces > Bridge > VLANs and click +.**
2. **Bridge: bridge1**
3. **VLAN ID: For example, 10 (the VLAN ID you want to use)**
4. **Tagged: ether1 (the port where the trunk connection will be, such as a switch/router)**
5. **Untagged: Leave it blank**

Now, ether1 is configured as a trunk port, allowing traffic from multiple VLANs with VLAN tags.

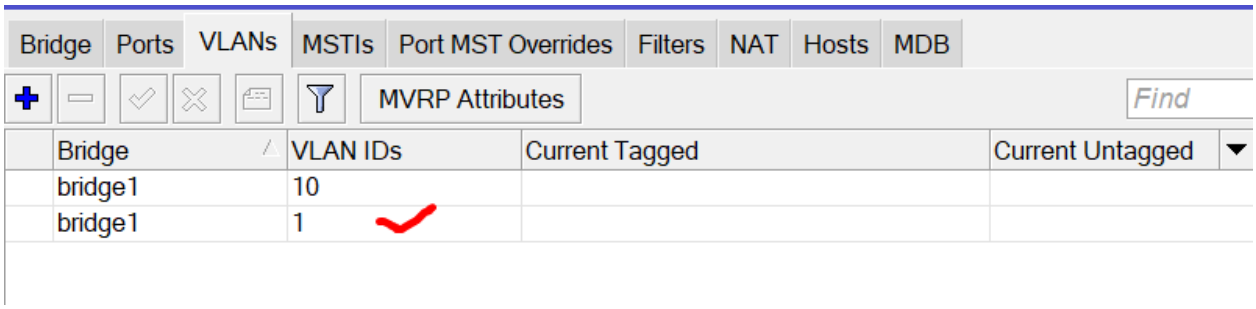


Access Port Configuration (For a specific VLAN):

✅ **Step-by-Step:**

1. **Go to the VLAN tab and click +.**
2. **VLAN ID: 10 (the VLAN ID you want to assign)**
3. **Tagged: Leave it blank.**
4. **Untagged: Select ether2 (the port where the user/PC will be connected)**
5. **Click Apply, then OK.**

Now, ether2 is configured as an Access Port for VLAN 10, meaning devices connected to this port will be in VLAN 10.



Bandwidth Management

- **Simple Queue**
- **PCQ (Per Connection Queue)**

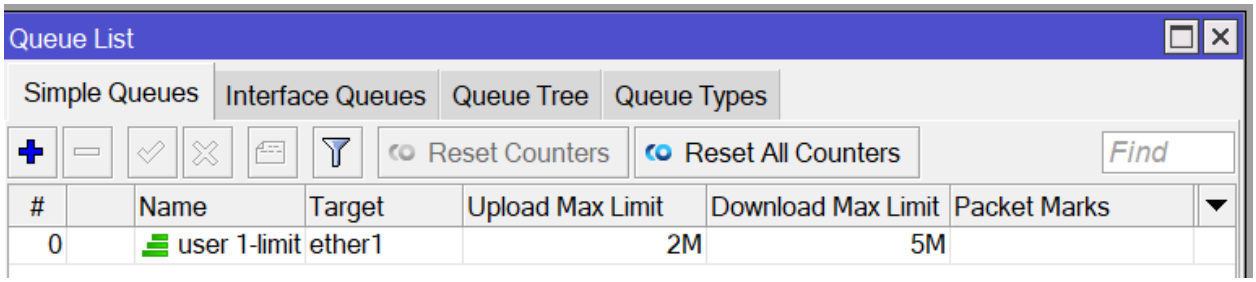
Creating a Simple Queue (Using GUI):

✅ **Example:**

- **For IP 192.168.1.100, set Download = 5Mbps and Upload = 2Mbps.**

Step-by-Step:

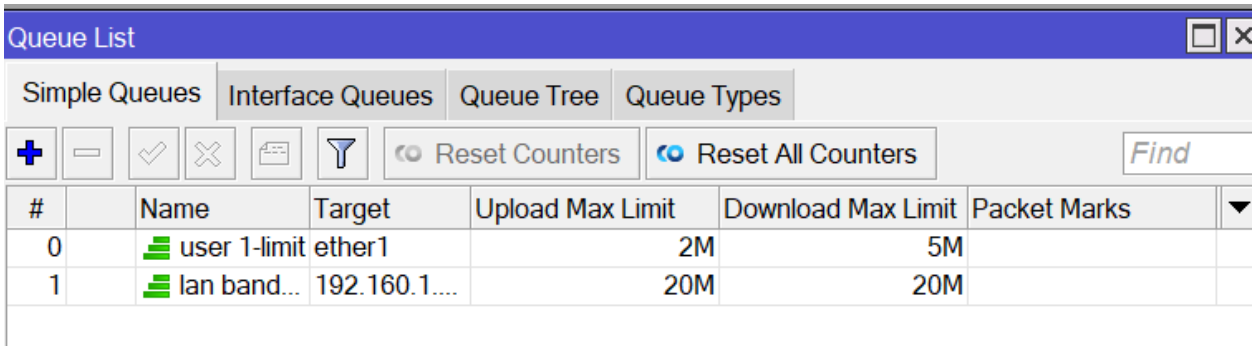
1. **Go to Queues > Simple Queues and click +.**
2. **In the Name field, enter: user1-limit (or any name you prefer).**
3. **For Target, select: ether1 (the interface you want to apply the queue to).**
4. **In the Max Limit section:**
    - **Target Upload: 2M**
    - **Target Download: 5M**
5. **Click Apply, then OK.**



6. **Using Simple Queue with PCQ:**
7. ✅ **Step-by-Step:**

8. **Go to Queues > Simple Queue and click +.**
9. **In the Name field, enter: LAN-Bandwidth.**
10. **For Target, enter: 192.168.1.0/24 (the IP range for your LAN).**
11. **In the Max Limit section:**
12. **Upload: 20M**
13. **Download: 20M**
14. **Go to the Advanced Tab > Queue Type:**
15. **Upload: Select pcq-upload.**
16. **Download: Select pcq-download.**
17. **Click Apply, then OK.**
18. ---
19. ✅ **Result:**

Now, each user (based on their IP) will receive up to 2 Mbps individually, with the total 20 Mbps shared across the users.



s