Manual:Initial Configuration

From MikroTik Wiki

Contents

Summary

Congratulations, you have got hold of MikroTik router for your home network. This guide will help you to do initial configuration of the router to make your home network a safe place to be.

The guide is mostly intended in case if default configuration did not get you to the internet right away, however some parts of the guide is still useful.

Connecting wires

Router's initial configuration should be suitable for most of the cases. Description of the configuration is on the back of the box and also described in the online manual.

The best way to connect wires as described on the box:

- Connect ethernet wire from your internet service provider (ISP) to port *ether1*, rest of the ports on the router are for local area network (LAN). At this moment, your router is protected by default firewall configuration so you should not worry about that;
- Connect LAN wires to the rest of the ports.

Configuring router

Initial configuration has DHCP client on WAN interface (ether1), rest of the ports are considered your local network with DHCP server configured for automatic address configuration on client devices. To connect to the router you have to set your computer to accept DHCP settings and plug in the ethernet cable in one of the LAN ports (please check routerboard.com for port numbering of the product you own, or check front panel of the router).

Logging into the router

To access the router enter address *192.168.88.1* in your browser. Main RouterOS page will be shown as in the screen shot below. Click on WebFig from the list.

You will be prompted for login and password to access configuration interface. Default login name is *admin* and blank password (leave empty field as it is already).

Router user accounts

It is good idea to start with password setup or add new user so that router is not accessible by anyone on your network. User configuration is done form **System -> Users** menu.

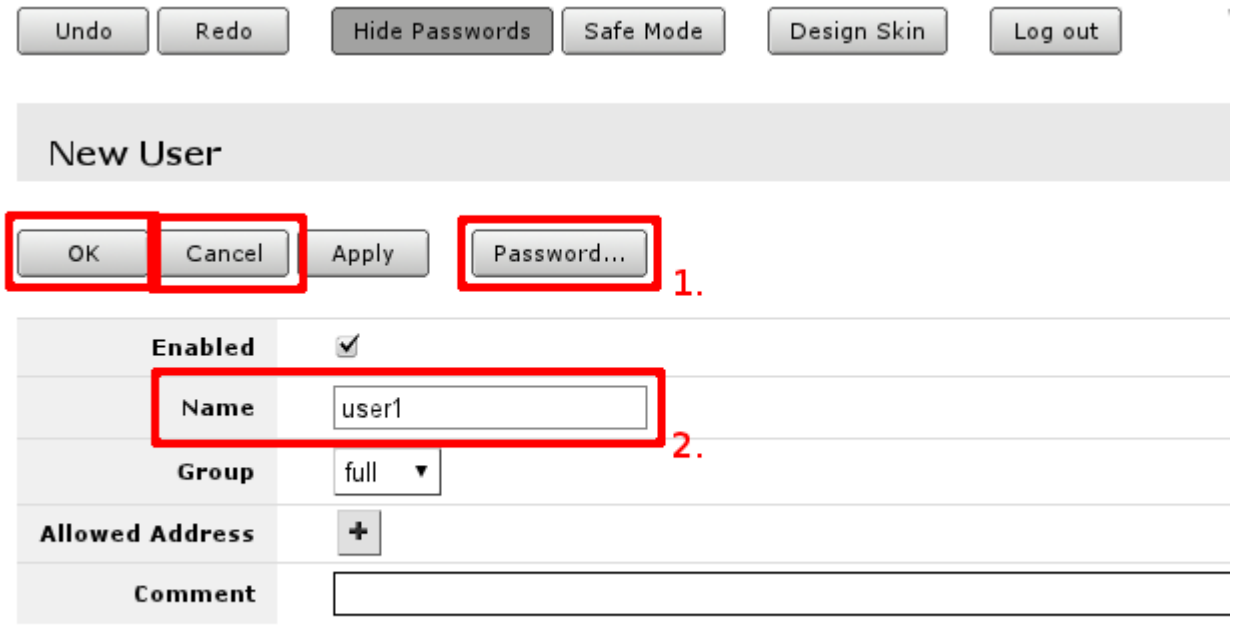
To access this menu, click on **System** on the left panel and from the dropdown menu choose **Users** (as shown in screenshot on the left)

You will see this screen, where you can manage users of the router. In this screen you can edit or add new users:

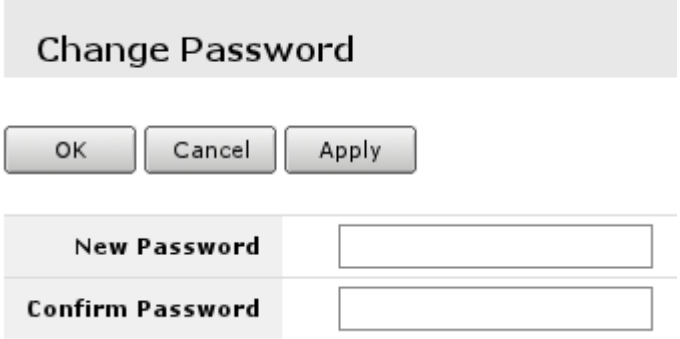
- When you click on account name (in this case *admin*), edit screen for the user will be displayed.

- If you click on **Add new** button, new user creation screen will be displayed.

Both screens are similar as illustrated in screenshot below. After editing user's data click *OK* (to accept changes) or *Cancel*. It will bring you back to initial screen of user management.



In user *edit*/*Add new* screen you can alter existing user or create new. Field marked with *2.* is the user name, field *1.* will open password screen, where old password for the user can be changed or added new one (see screenshot below).



Configure access to internet

If initial configuration did not work (your ISP is not providing DHCP server for automatic configuration) then you will have to have details from your ISP for static configuration of the router. These settings should include

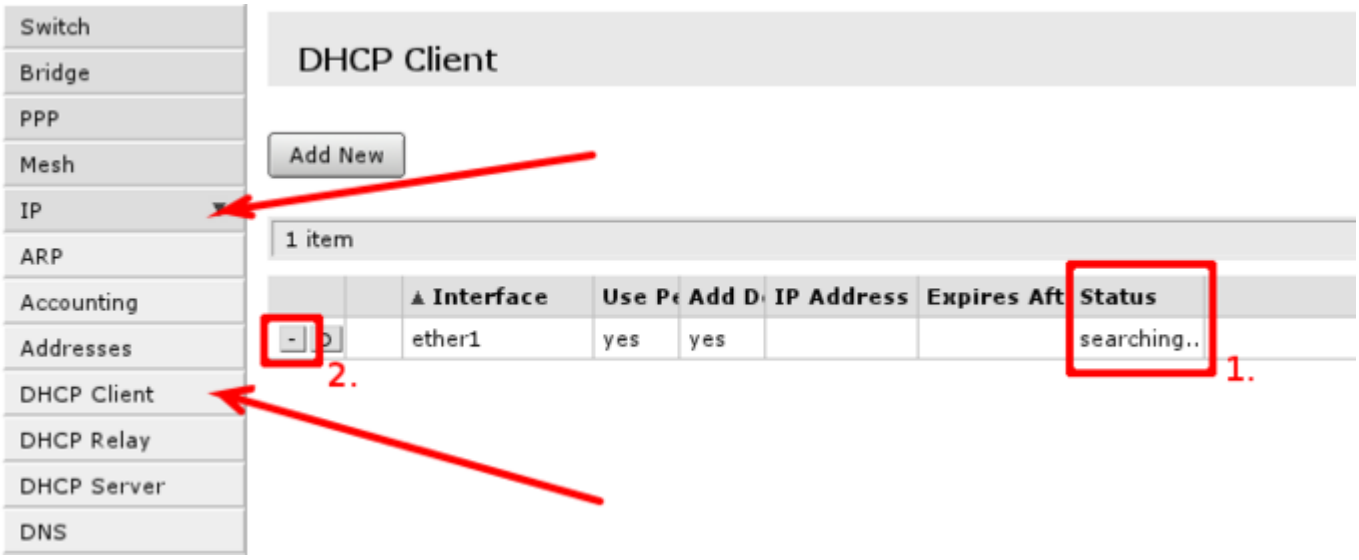
- IP address you can use
- Network mask for the IP address
- Default gateway address

Less important settings regarding router configuration:

- DNS address for name resolution
- NTP server address for time automatic configuration
- Your previous MAC address of the interface facing ISP

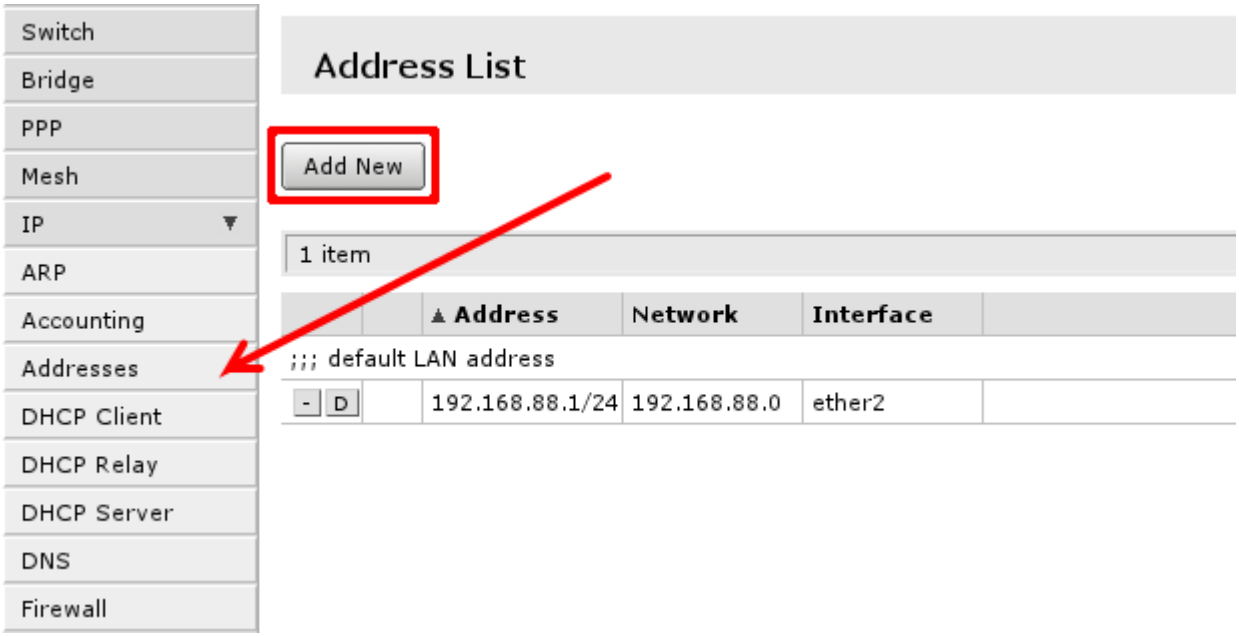
DHCP Client

Default configuration is set up using DHCP-Client on interface facing your ISP or wide area network (WAN). It has to be disabled if your ISP is not providing this service in the network. Open 'IP -> DHCP Client' and inspect field *1.* to see status of DHCP Client, if it is in state as displayed in screenshot, means your ISP is not providing you with automatic configuration and you can use button in selection *2.* to remove DHCP-Client configured on the interface.

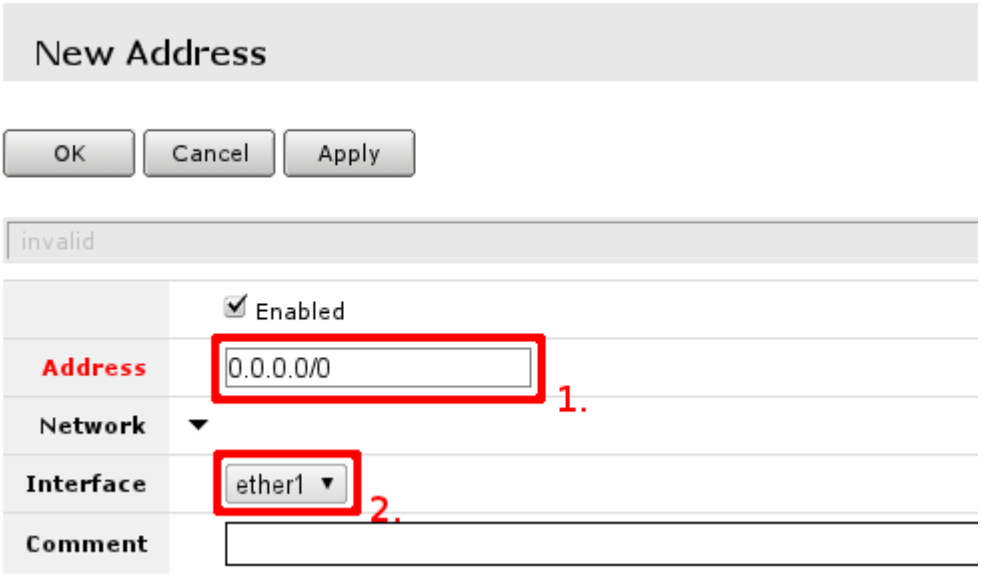


Static IP Address

To manage IP addresses of the router open 'IP -> Address'



You will have one address here - address of your local area network (LAN) *192.168.88.1* one you are connected to router. Select *Add new* to add new static IP address to your router's configuration.



You have to fill only fields that are marked. Field *1.* should contain *IP address* provided by your ISP and *network mask'. Examples:*

```
172.16.88.67/24
```

both of these notations mean the same, if your ISP gave you address in one notation, or in the other, use one provided and router will do the rest of calculation.

Other field of interest is *interface* this address is going to be assigned. This should be interface your ISP is connected to, if you followed this guide - interface contains name - *ether1*

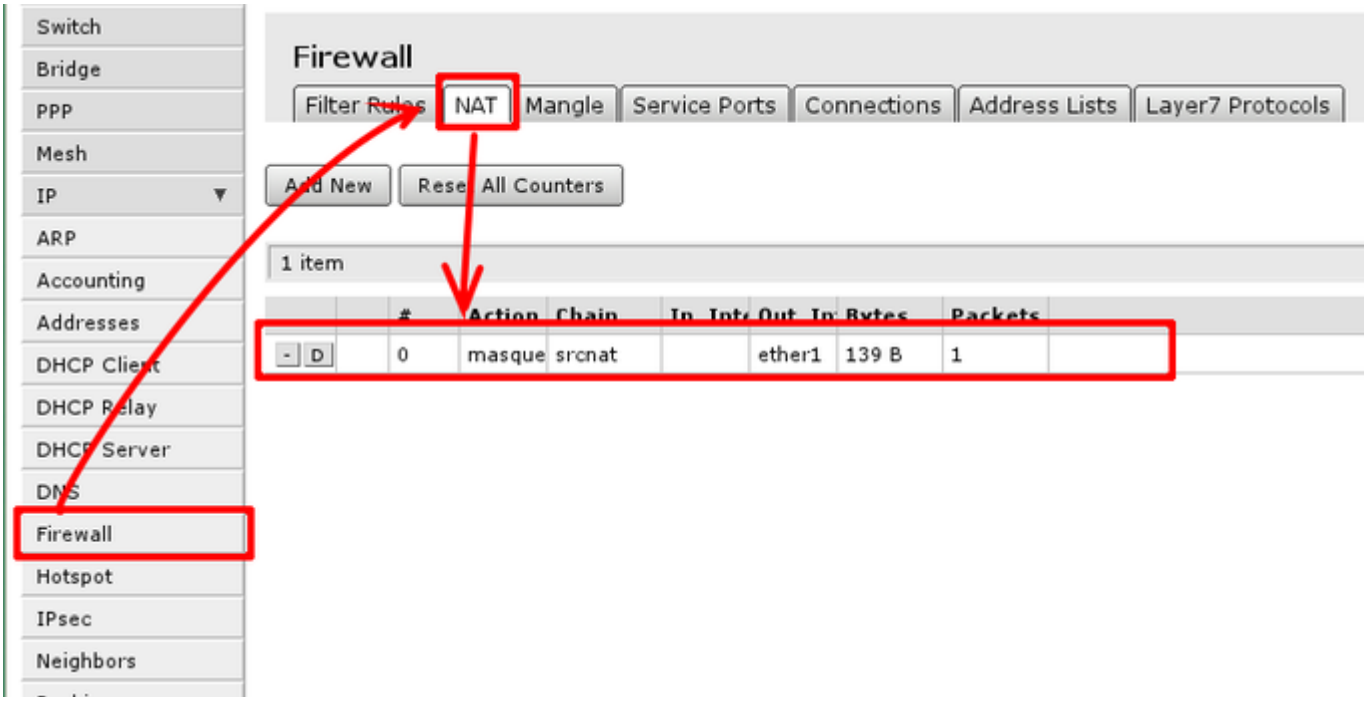
Note: While you type in the address, webfig will calculate if address you have typed is acceptable, if it is not label of the field will turn red, otherwise it will be blue

Note: It is good practice to add comments on the items to give some additional information for the future, but that is not required

Configuring network address translation (NAT)

Since you are using local and global networks, you have to set up network masquerade, so that your LAN is hidden behind IP address provided by your ISP. That should be so, since your ISP does not know what LAN addresses you are going to use and your LAN will not be routed from global network.

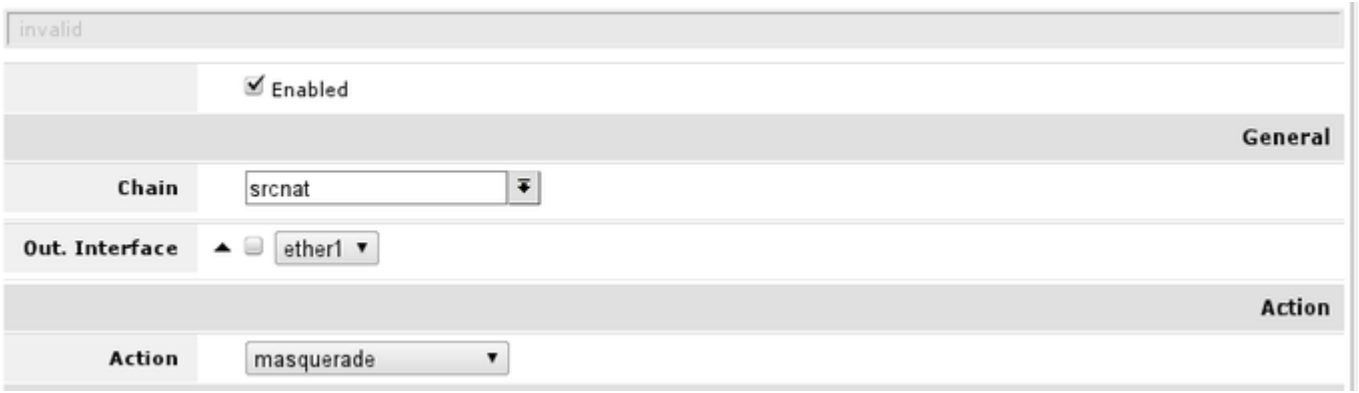
To check if you have the source NAT open 'IP -> Firewall -> tab NAT' and check if item highlighted (or similar) is in your configuration.



Essential fields for masquerade to work:

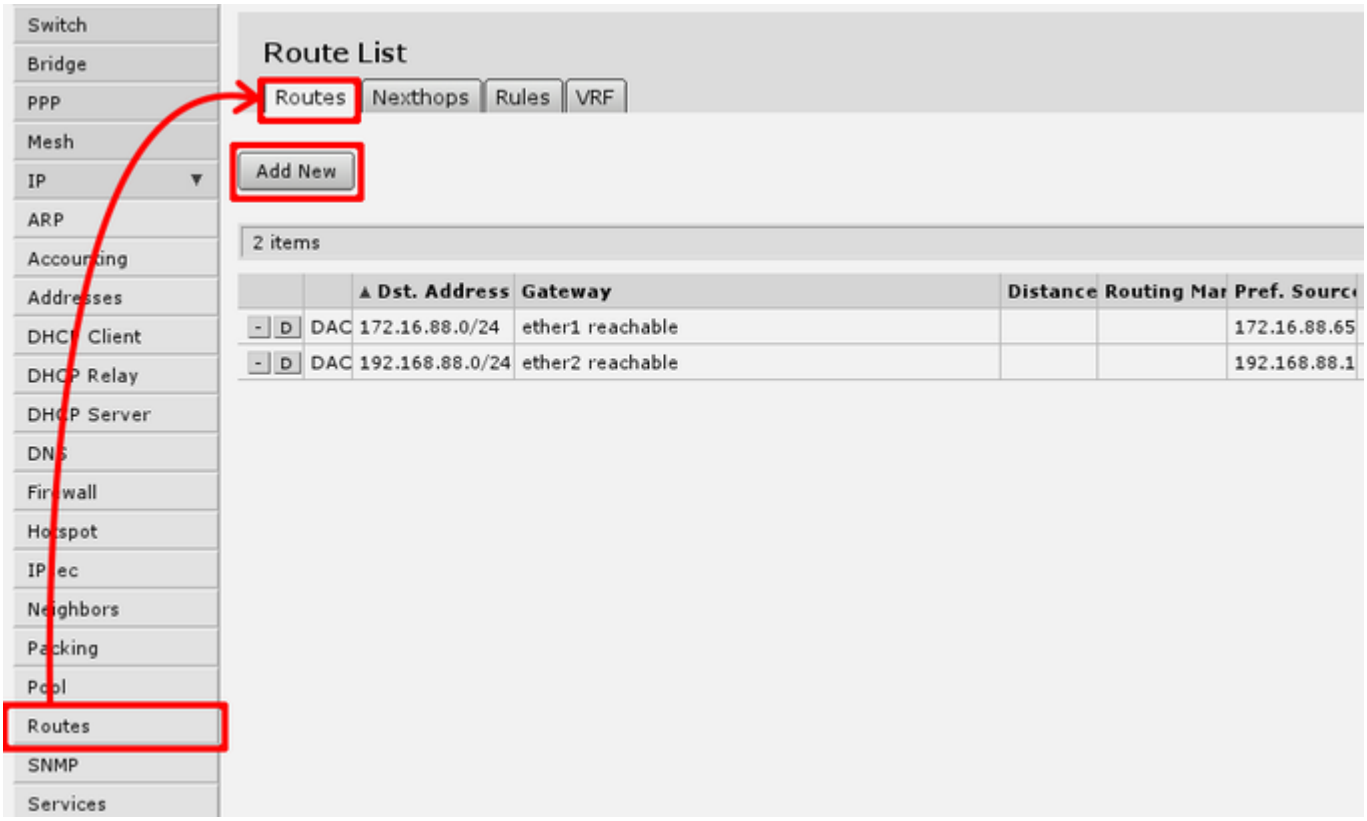
- enabled is checked;
- chain - should be *srcnat*;
- out-interface is set to interface connected to your ISP network, Following this guide *ether1*;
- action should be set to *masquerade*.

In screenshot correct rule is visible, note that irrelevant fields that should not have any value set here are hidden (and can be ignored)

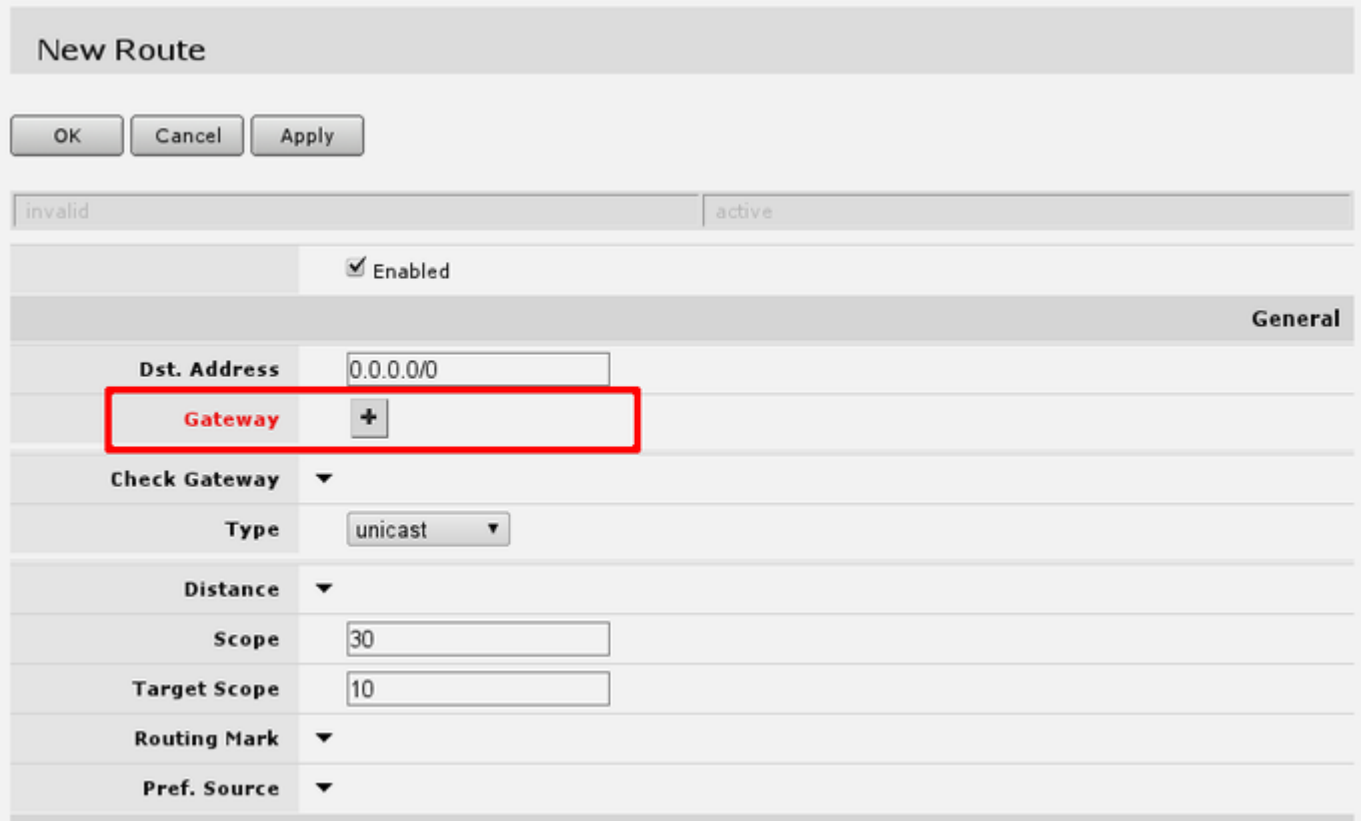


Default gateway

under 'IP -> Routes' menu you have to add routing rule called default route. And select *Add new* to add new route.

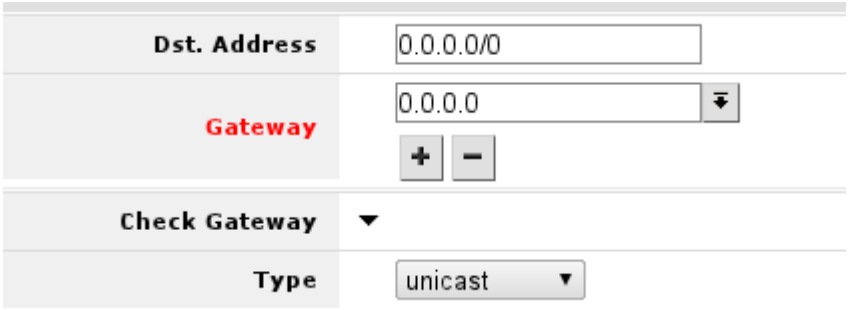


In screen presented you will see the following screen:



here you will have to press button with **+** near red *Gateway* label and enter in the field default gateway, or simply gateway given by your ISP.

This should look like this, when you have pressed the **+** button and enter gateway into the field displayed.



After this, you can press OK button to finish creation of the default route.

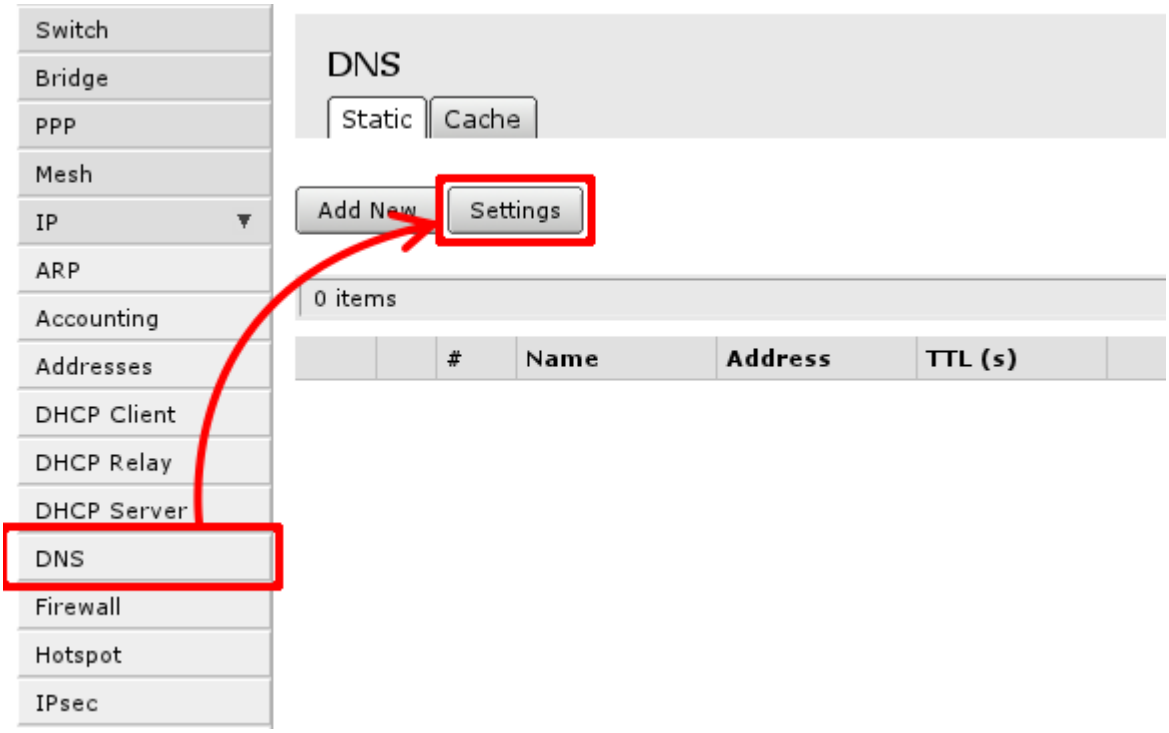
At this moment, you should be able to reach any globally available host on the Internet using IP address.

To check weather addition of default gateway was successful use *Tools -> Ping*

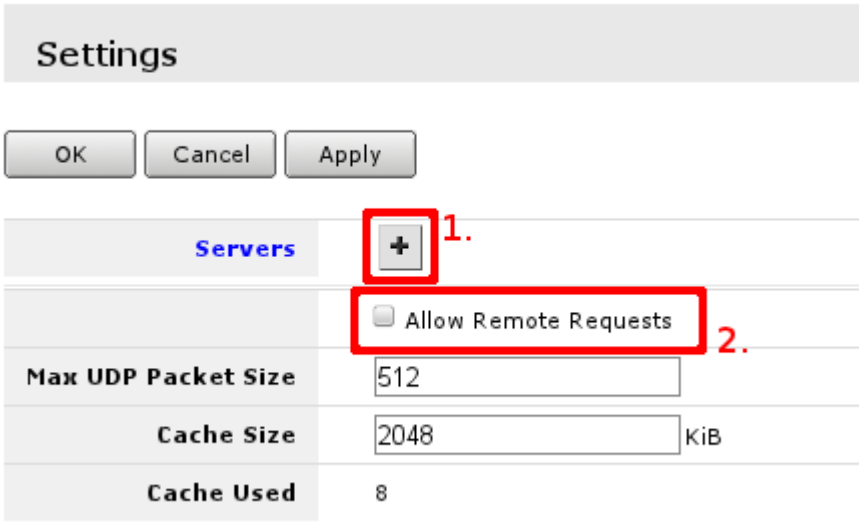
Domain name resolution

To be able to open web pages or access Internet hosts by domain name DNS should be configured, either on your router or your computer. In scope of this guide, i will present only option of router configuration, so that DNS addresses are given out by DHCP-Server that you are already using.

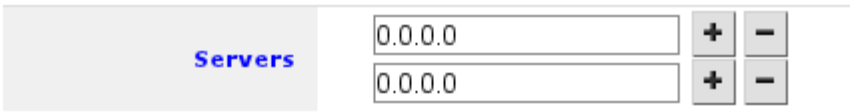
This can be done in 'IP -> DNS ->Settings', first Open 'IP ->DNS':



Then select *Settings* to set up DNS cacher on the router. You have to add field to enter DNS IP address, section *1.* in image below. and check *Allow Remote Requests* marked with *2.*



The result of pressing **+** twice will result in 2 fields for DNS IP addresses:

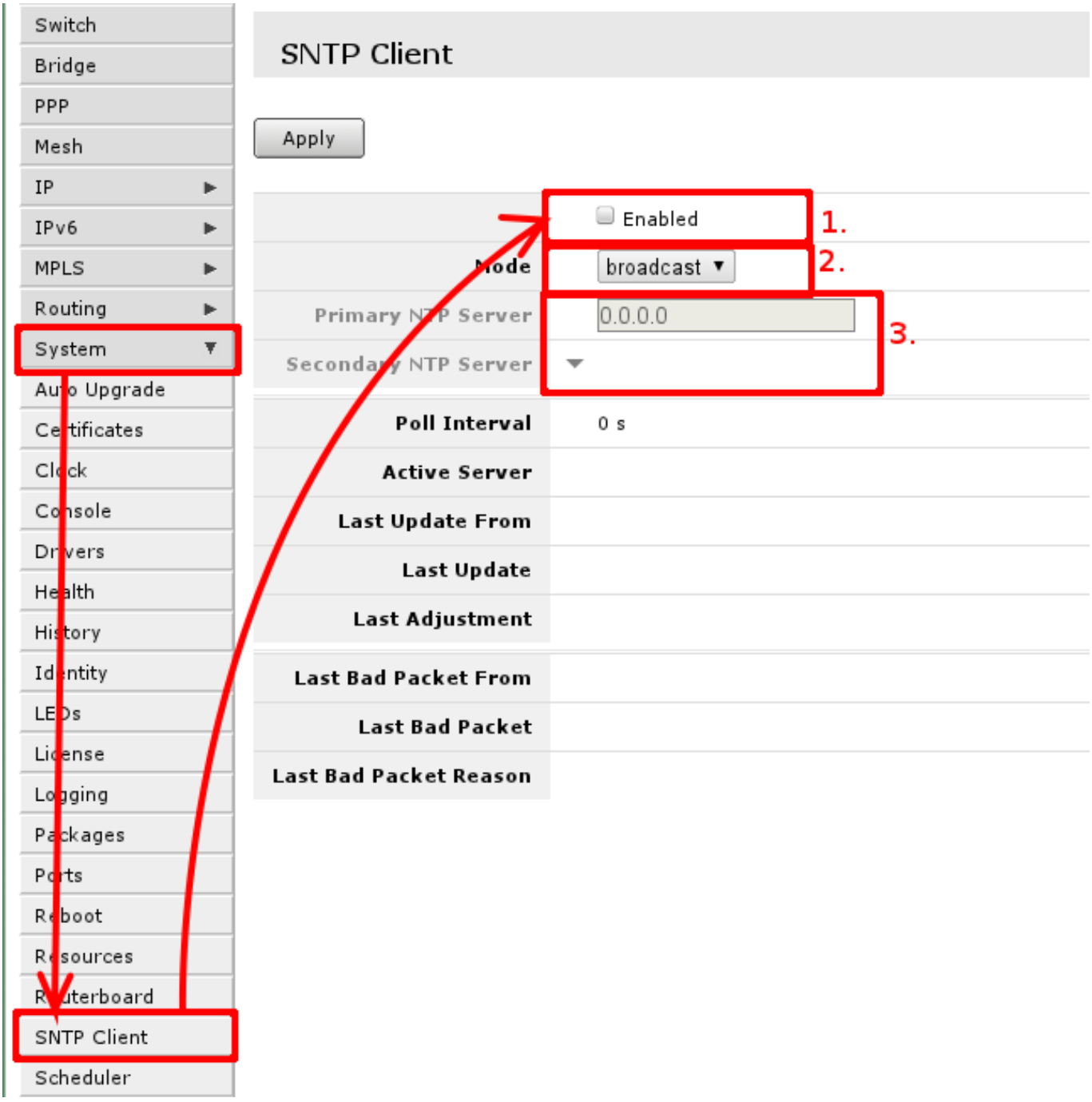


Note: Filling acceptable value in the field will turn field label blue, other way it will be marked red.

SNTP Client

RouterBOARD routers do not keep time between restarts or power failuers. To have correct time on the router set up SNTP client if you require that.

To do that, go to 'System -> SNTP' where you have to enable it, first mark, change mode from broadcast to unicast, so you can use global or ISP provided NTP servers, that will allow to enter NTP server IP addresses in third area.



Setting up Wireless

For ease of use bridged wireless setup will be used, so that your wired hosts will be in same ethernet broadcast domain as wireless clients.

To make this happen several things has to be checked:

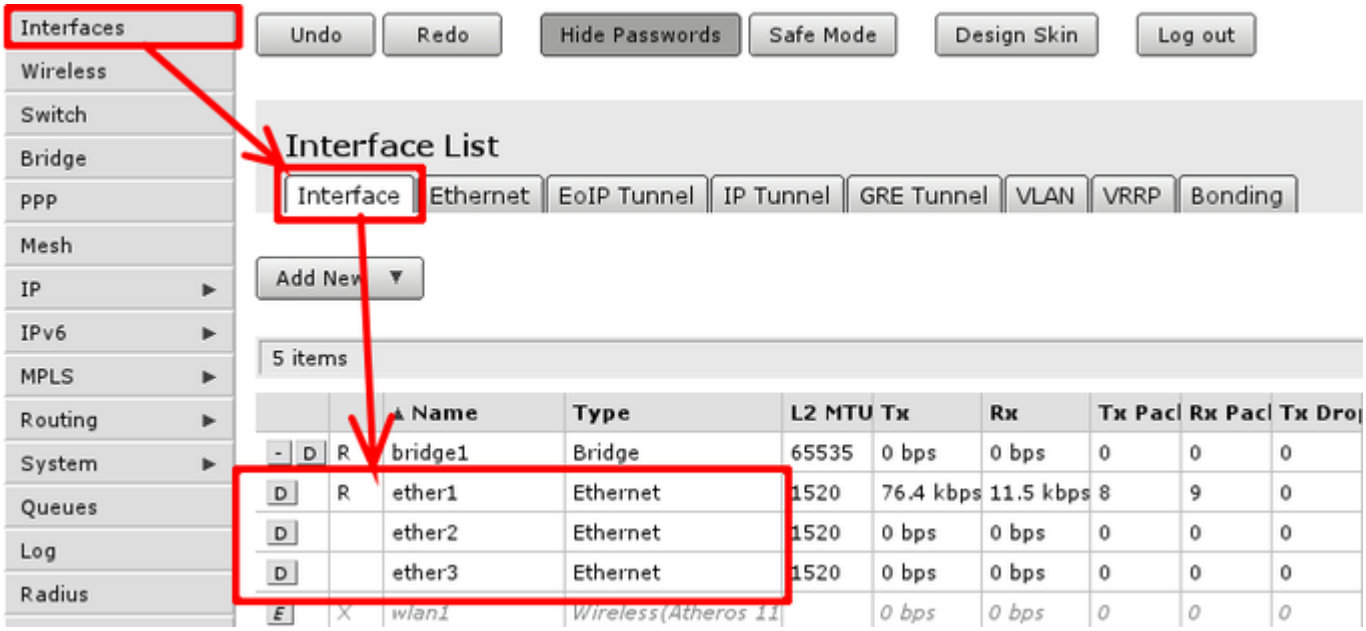
- Ethernet interfaces designated for LAN are swtiched or bridged, or they are separate ports;

- If bridge interface exists;
- Wireless interface *mode* is set to *ap-bridge* (in case, router you have has level 4 or higher license level), if not, then *mode* has to be set to *bridge* and only one client (station) will be able to connect to the router using wireless network;
- There is appropriate security profile created and selected in interface settings.

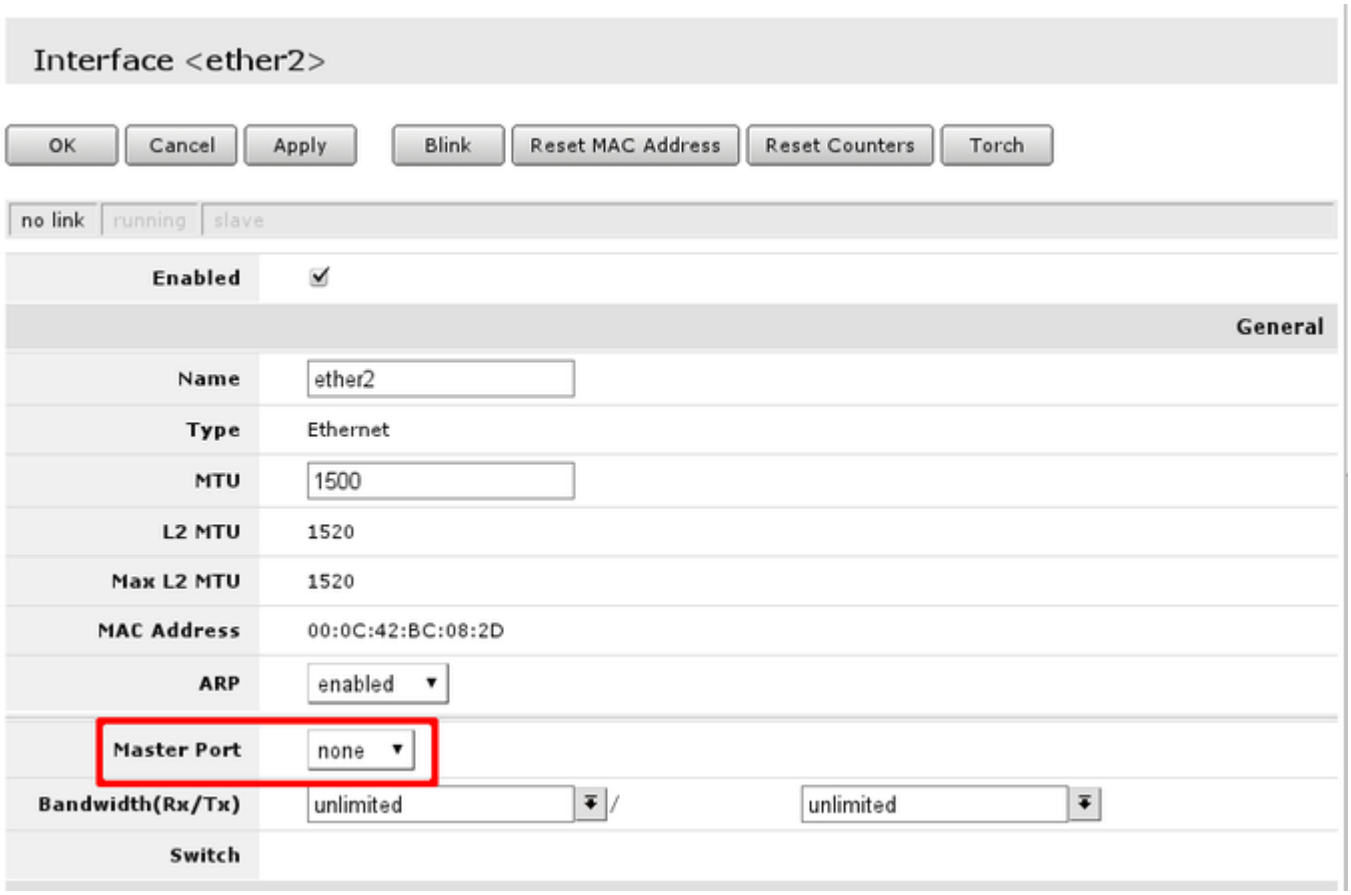
Check Ethernet interface state

Warning: Changing settings may affect connectivity to your router and you can be disconnected from the router. Use *Safe Mode* so in case of disconnection made changes are reverted back to what they where before you entered safe mode

To check if ethernet port is switched, in other words, if ethernet port is set as slave to another port go to 'Interface' menu and open Ethernet interface details. They can be distinguished by Type column displaying *Ethernet*.



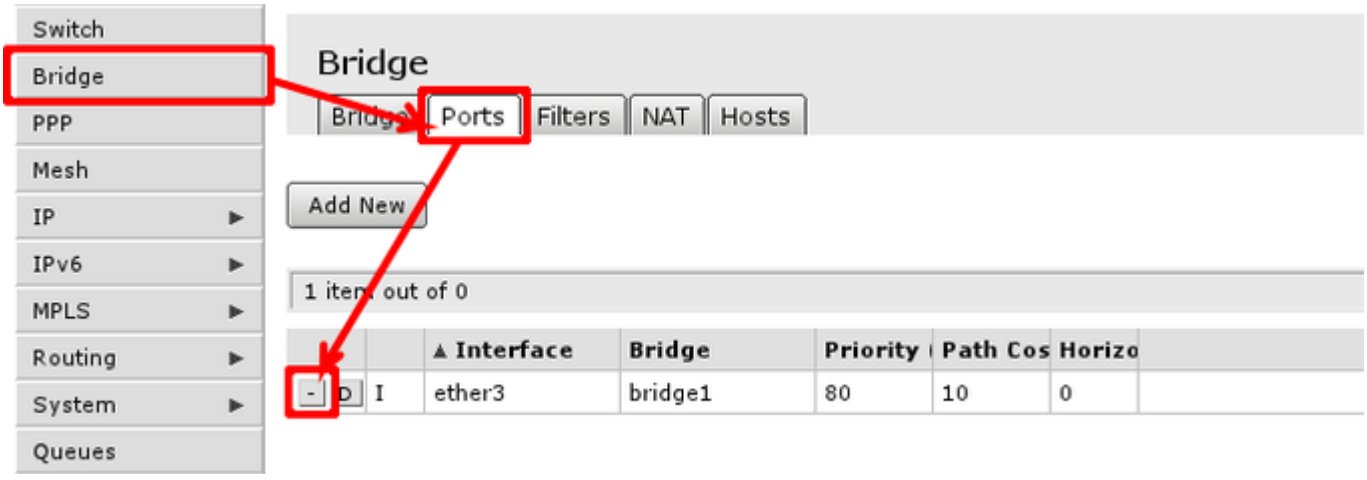
When interface details are opened, look up *Master Port* setting.



Available settings for the attribute are none, or one of Ethernet interface names. If name is set, that mean, that interface is set as slave port. Usually RouterBOARD routers will come with *ether1* as intended WAN port and rest of ports will be set as slave ports of *ether2* for LAN use.

Check if all intended LAN Ethernet ports are set as slave ports of the rest of one of the LAN ports. For example, if *ether2. ether3, ether4* and *ether5* are intended as LAN ports, set on ether3 to ether5 attribute *Master Port* to *ether2*.

In case this operation fails - means that Ethernet interface is used as port in bridge, you have to remove them from bridge to enable hardware packet switching between Ethernet ports. To do this, go to *Bridge -> Ports* and remove slave ports (in example, *ether3* to *ether5*) from the tab.



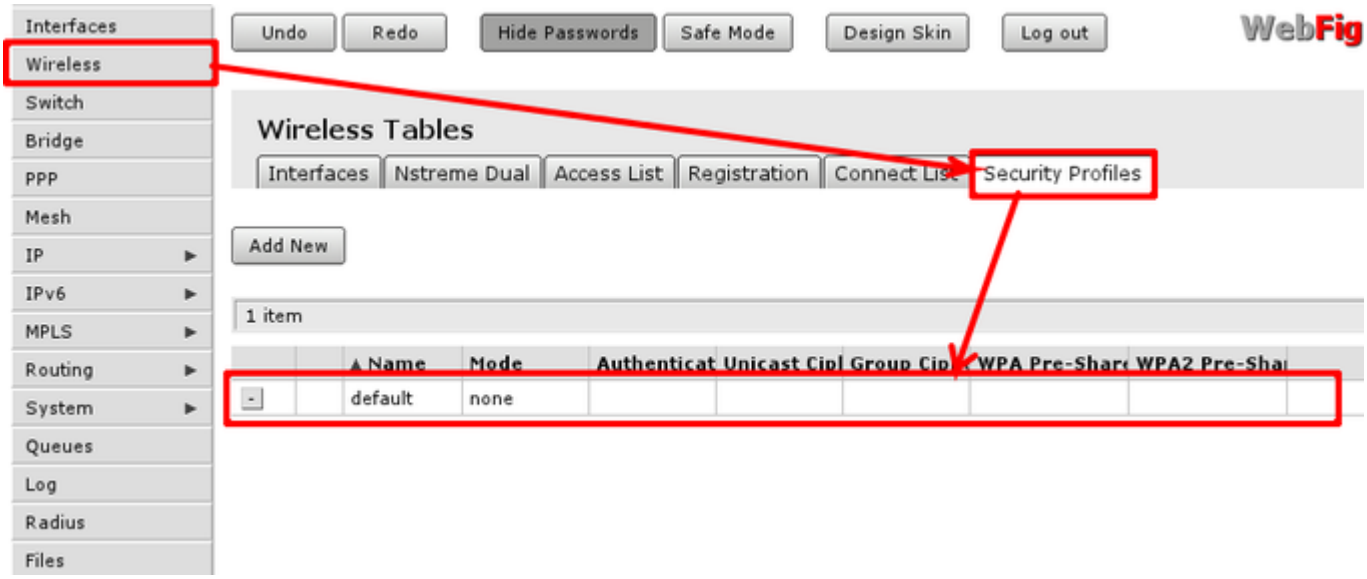
Note: If master port is present as bridge port, that is fine, intended configuration requires it there, same applies to wireless interface (*wlan*)

Security profile

It is important to protect your wireless network, so no malicious acts can be performed by 3rd parties using your wireless access-point.

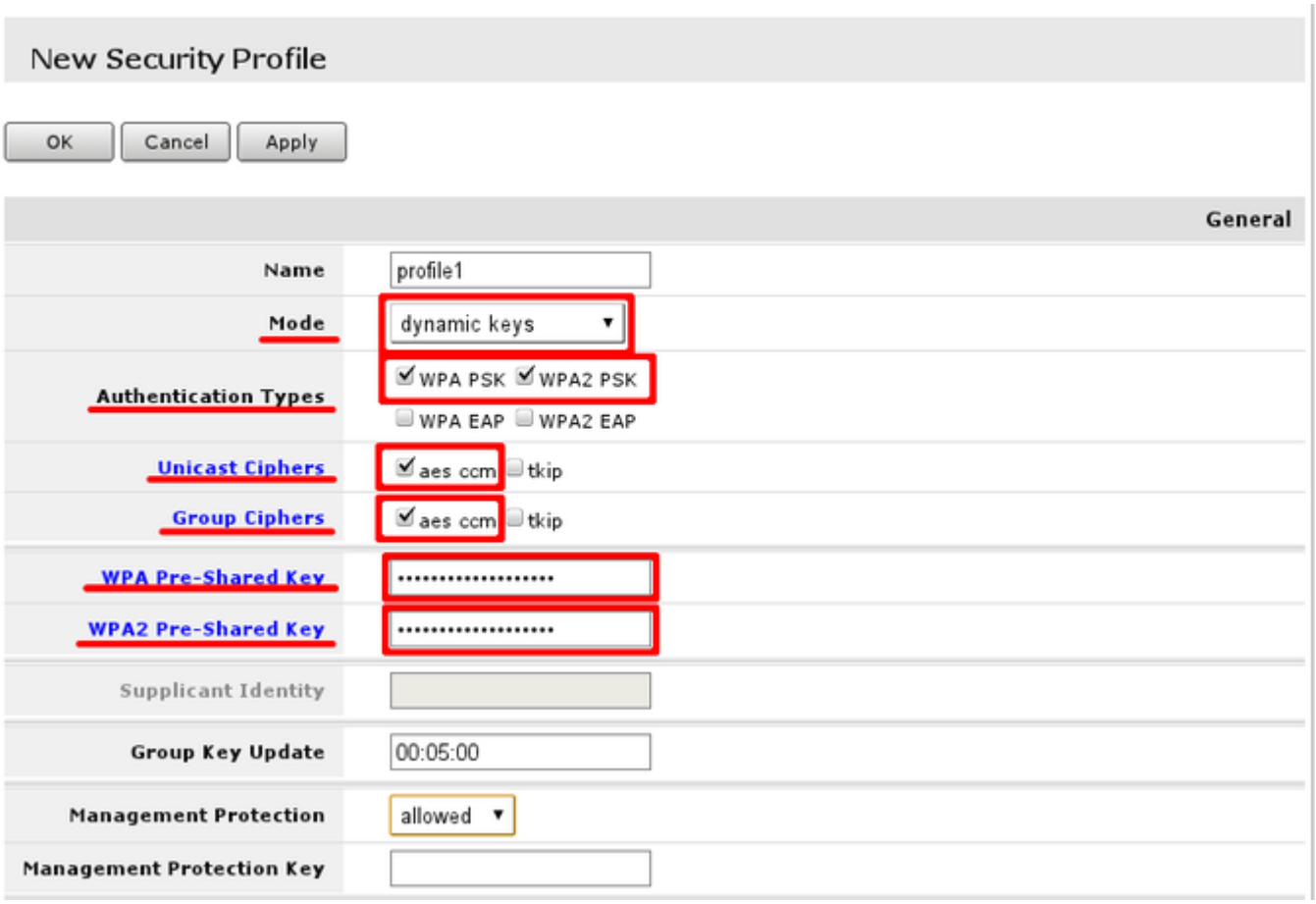
To edit or create new security profile head to 'Wireless -> tab 'Security Prodiles' and choose one of two options:

- Using *Add new* create new profile;
- Using highlighted path in screenshot edit default profile that is already assigned to wireless interface.



In This example i will create new security profile, editing it is quite similar. Options that has to be set are highlighted with read and recommended options are outlined by red boxes and pre-set to recommended values. WPA and WPA2 is used since there are still legacy equipment around (Laptops with Windows XP, that do not support WPA2 etc.)

WPA Pre- shared key and WPA2 Pre- shared key should be entered with sufficient length. If key length is too short field label will indicate that by turning red, when sufficient length is reached it will turn blue.



Note: WPA and WPA2 pre-shared keys should be different

Note: When configuring this, you can deselect *Hide passwords* in page header to see the actual values of the fields, so they can be successfully entered into device configuration that are going to connect to wireless access-point

Wireless settings

Adjusting wireless settings. That can be done here:

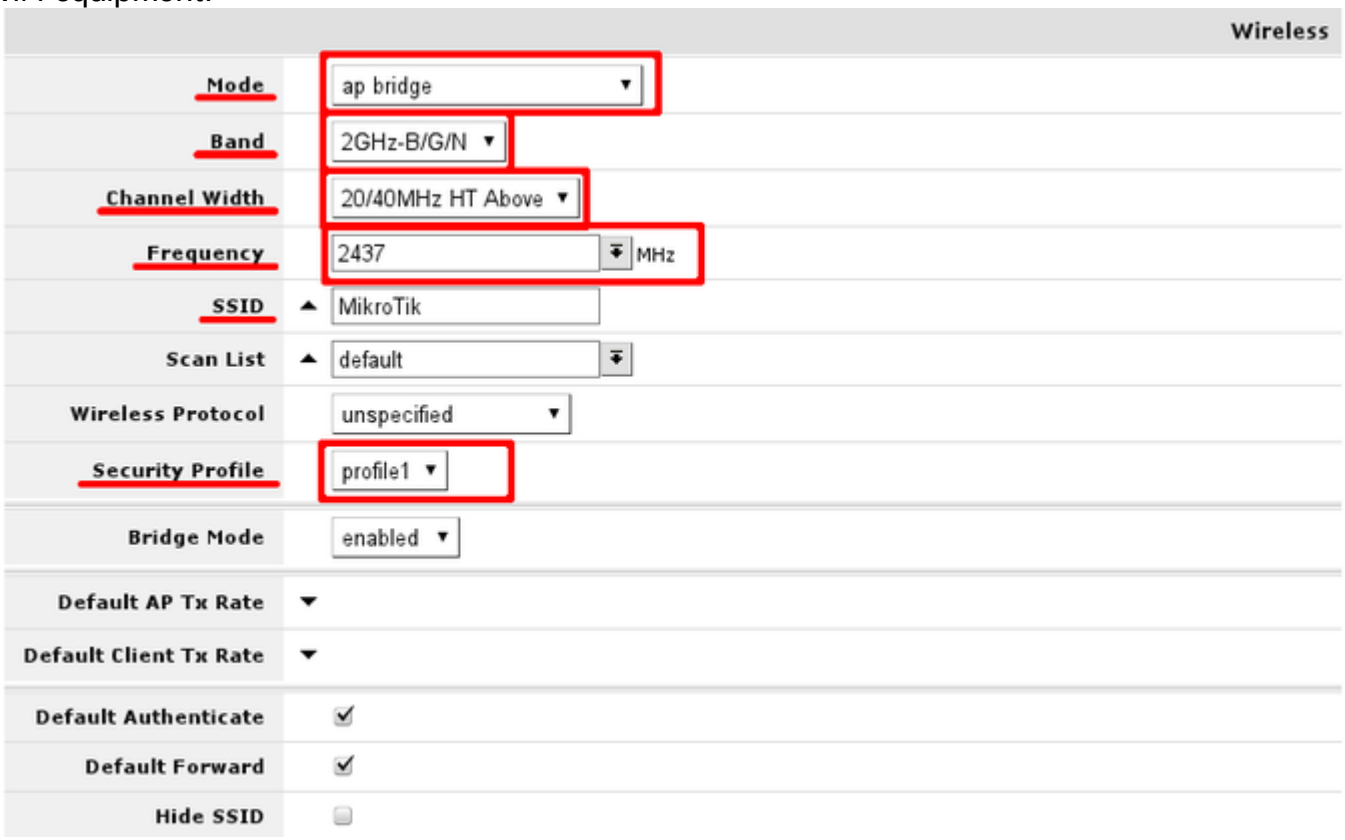
In *General* section adjust settings to settings as shown in screenshot. Consider these safe, however it is possible, that these has to be adjusted slightly.

Interface mode has to be set to *ap-bridge*, if that is not possible (license resctrictions) set to bridge, so one client will be able to connect to device.

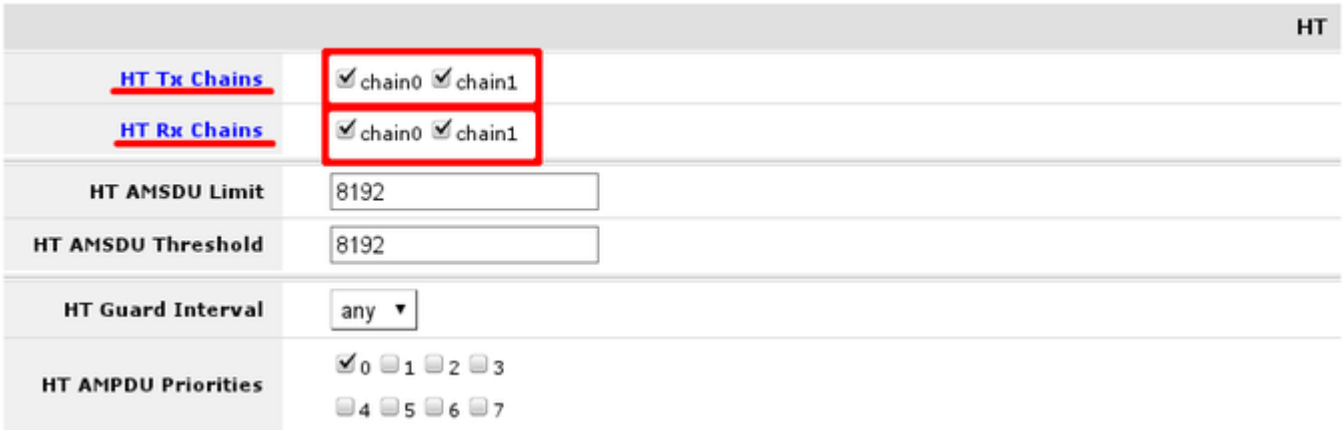
WiFI devices usually are designed with 2.4GHz modes in mind, setting band to 2GHz-b/g/n will enable clients with 802.11b, 802.11g and 802.11n to connect to the access point

Adjust channel width to enable faster data rates for 802.11n clients. In example channel 6 is used, as result, *20/40MHz HT Above* or *20/40 MHz HT Below* can be used. Choose either of them.

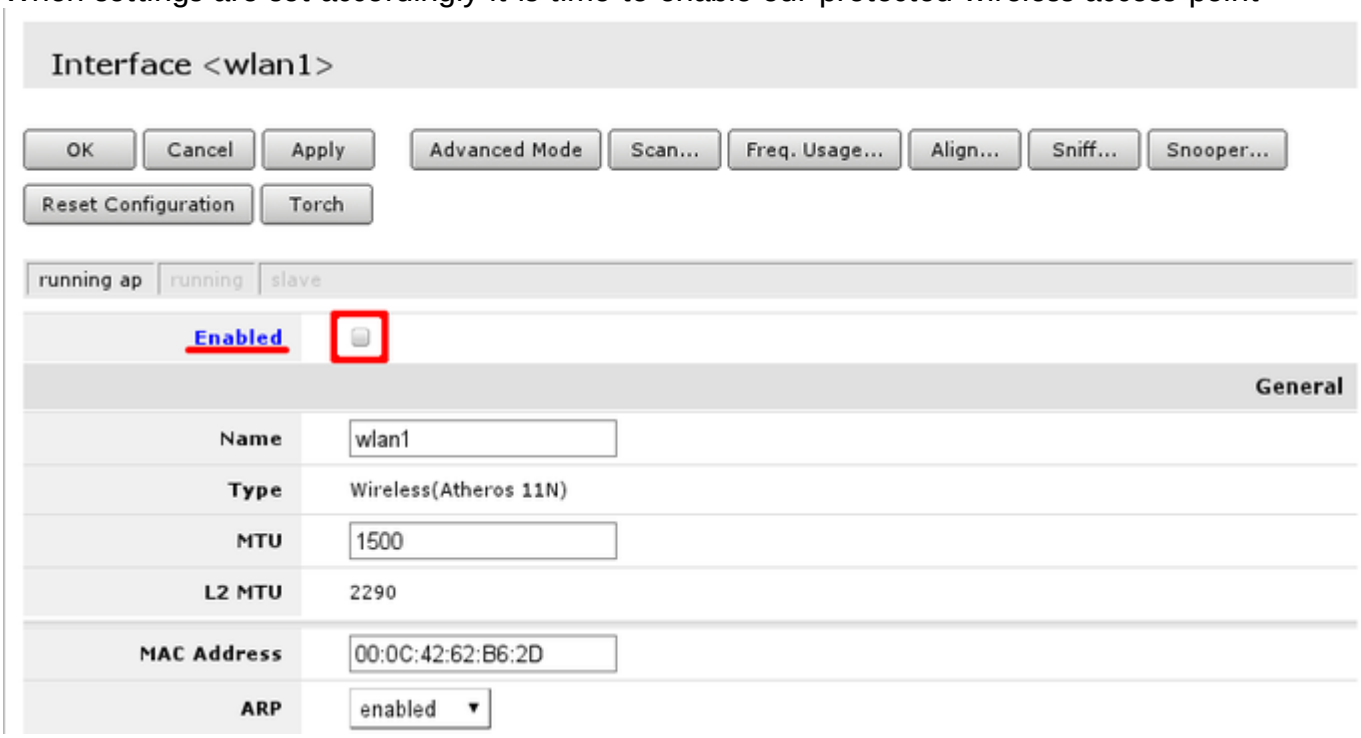
Set SSID - the name of the access point. It will be visible when you scan for networks using your WiFi equipment.



In section *HT* set change HT transmit and receive chains. It is good practice to enable all chains that are available



When settings are set accordingly it is time to enable our protected wireless access-point

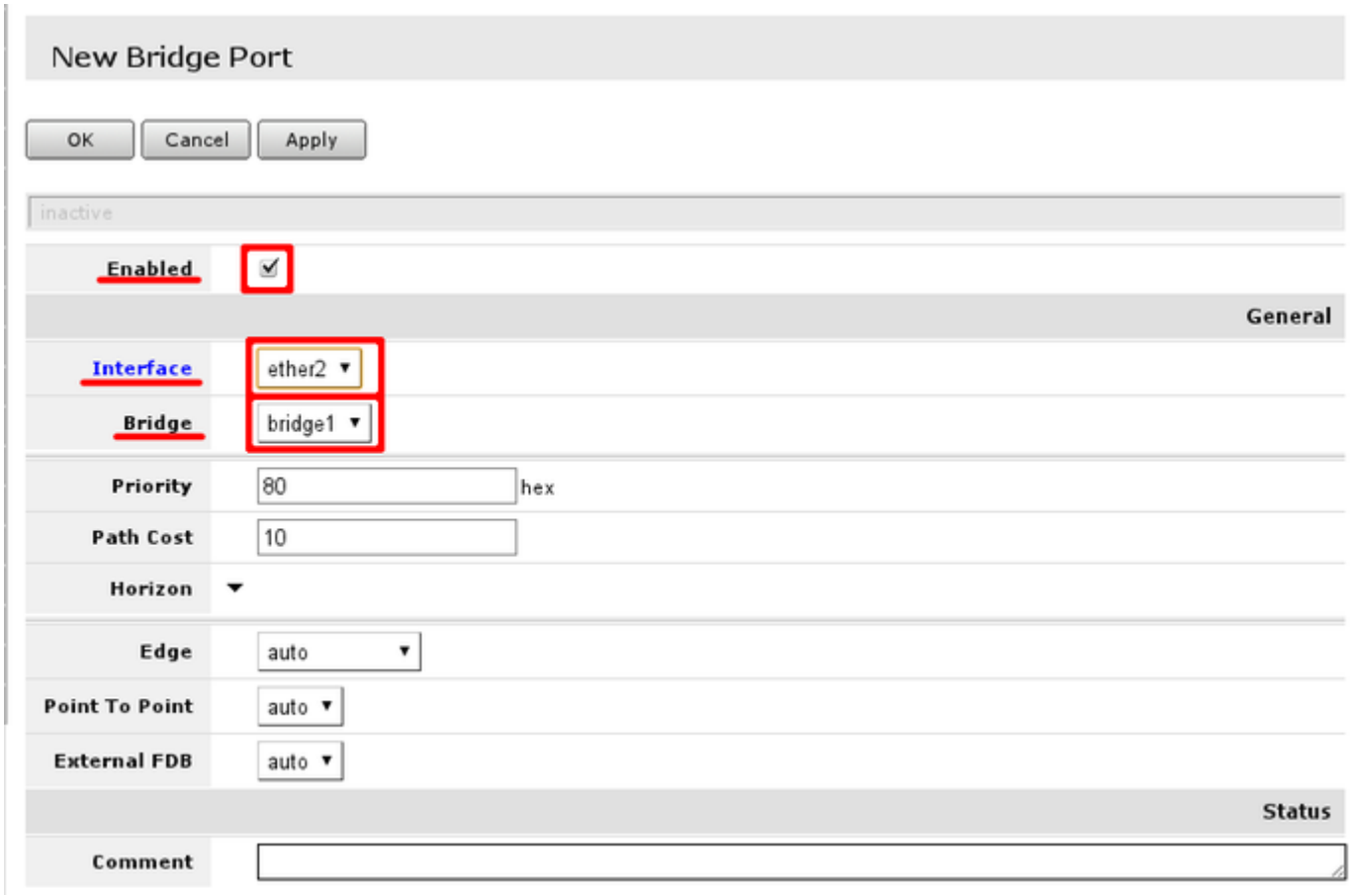


Bridge LAN with Wireless

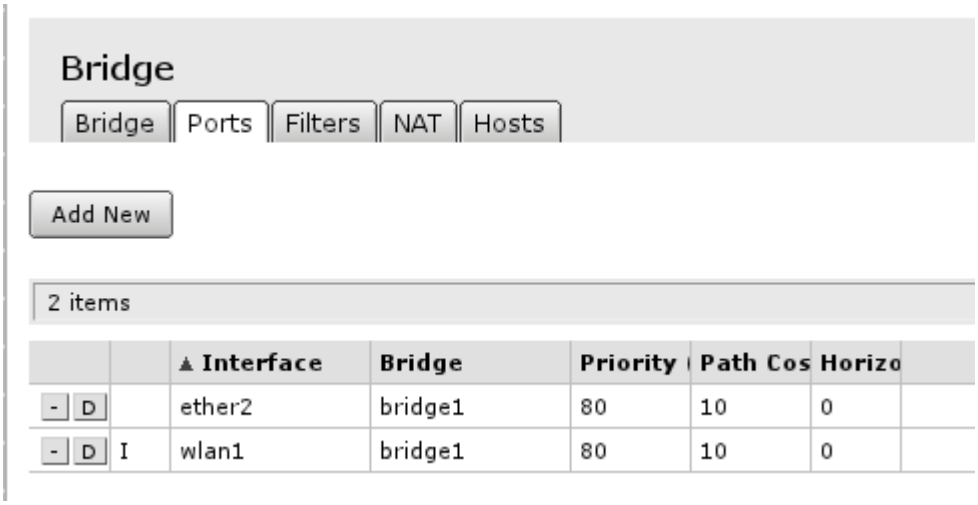
Open *Bridge* menu and check if there are any bridge interface available first mark. If there is not, select *Add New* marked with second mark and in the screen that opens just accept the default settings and create interface. When bridge interface is availbe continue to *Ports* tab where master LAN interface and WiFI interface have to be added.

First marked area is where interfaces that are added as ports to bridge interface are visible. If there are no ports added, choose *Add New* to add new ports to created bridge interfaces.

When new bridge port is added, select that it is enabled (part of active configuration), select correct bridge interface, following this guide - there should be only 1 interface. And select correct port - LAN interface master port and WiFi port



Finished look of bridge configured with all ports required



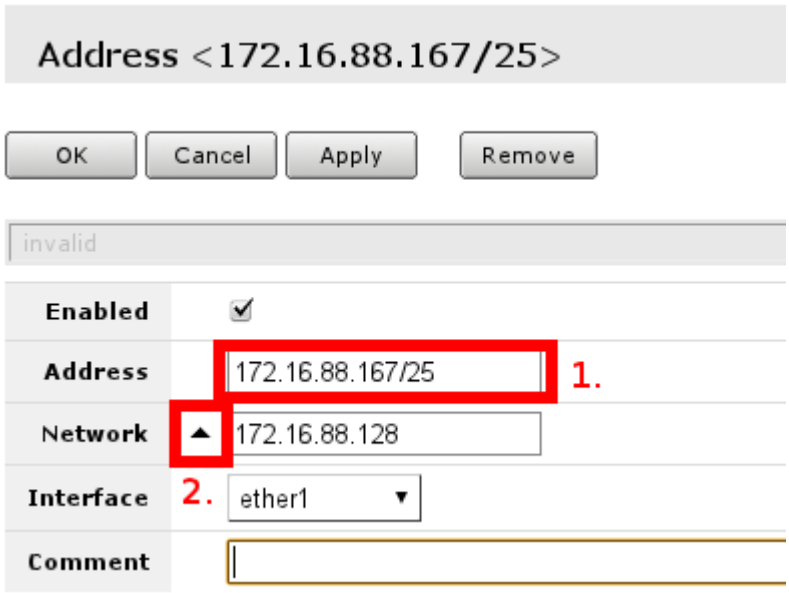
Troubleshooting & Advanced configuration

This section is here to make some deviations from configuration described in the guide itself. It can require more understanding of networking, wireless networks in general.

General

Check IP address

Adding IP address with wrong network mask will result in wrong network setting. To correct that problem it is required to change *address* field, first section, with correct address and network mask and *network* field with correct network, or unset it, so it is going to be recalculated again

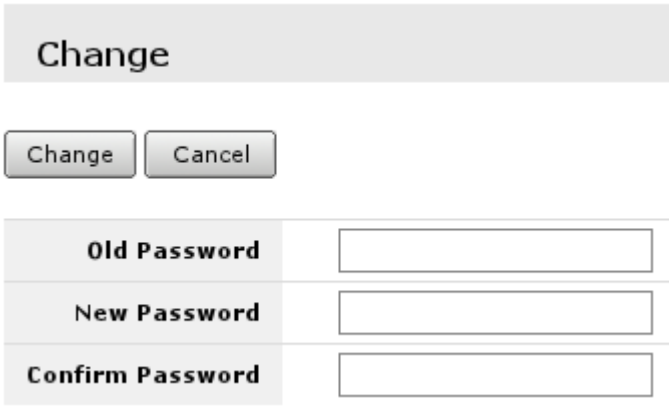


Change password for current user

To change password of the current user, safe place to go is *System -> Password*

Where all the fields has to be filled. There is other place where this can be done in case you have full privileges on the router.

Change password for existing user



If you have full privileges on the router, it is possible to change password for any user without knowledge of current one. That can be done under *System -> Users* menu.

Steps are:

- Select user;
- type in password and re-type it to know it is one you intend to set

No access to the Internet or ISP network

If you have followed this guide to the letter but even then you can only communicate with your local hosts only and every attempt to connect to Internet fails, there are certain things to check:

- If masquerade is configured properly;
- If setting MAC address of previous device on WAN interface changes anything
- ISP has some captive portal in place.

Respectively, there are several ways how to solve the issue, one - check configuration if you are not missing any part of configuration, second - set MAC address. Change of mac address is available only from CLI - *New Terminal* from the left side menu. If new window is not opening check your browser if it is allowing to open popup windows for this place. There you will have to write following command by replacing MAC address to correct one:

```
/interface ethernet set ether1 mac-address=XX:XX:XX:XX:XX:XX
```

Or contact your ISP for details and inform that you have changed device.

Checking link

There are certain things that are required for Ethernet link to work:

- Link activity lights are on when Ethernet wire is plugged into the port
- Correct IP address is set on the interface
- Correct route is set on the router

What to look for using ping tool:

- If all packets are replied;
- If all packets have approximately same round trip time (RTT) on non-congested Ethernet link

It is located here: *Tool -> Ping* menu. Fill in *Ping To* field and press start to initiate sending of

ICMP packets.

Wireless

Wireless unnamed features in the guide that are good to know about. Configuration adjustments.

Channel frequencies and width

It is possible to choose different frequency, here are frequencies that can be used and channel width settings to use 40MHz HT channel (for 802.11n). For example, using *channel 1 or 2412MHz frequency* setting *20/40MHz HT below* will not yield any results, since there are no 20MHz channels available below set frequency.

Channel #	Frequency	Below	Above
1	2412 MHz	no	yes
2	2417 MHz	no	yes
3	2422 MHz	no	yes
4	2427 MHz	no	yes
5	2432 MHz	yes	yes
6	2437 MHz	yes	yes
7	2442 MHz	yes	yes
8	2447 MHz	yes	yes
9	2452 MHz	yes	yes
10	2457 MHz	yes	yes
11	2462 MHz	yes	no
12	2467 MHz	yes	no
13	2472 MHz	yes	no

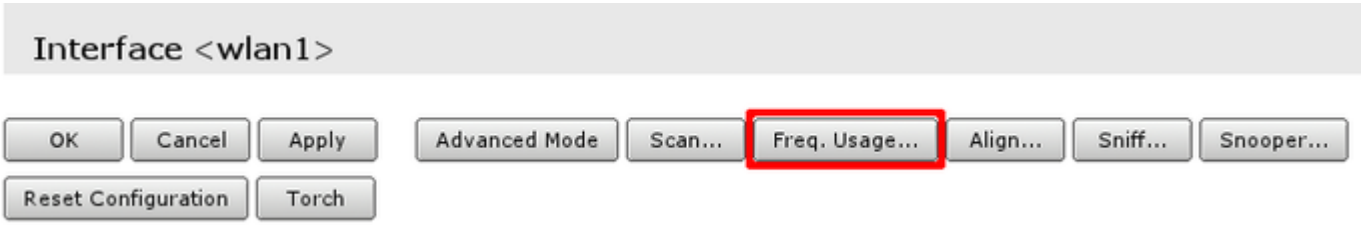
Warning: You should check how many and what frequencies you have in your regulatory domain before. If there are 10 or 11 channels adjust settings accordingly. With only 10 channels, channel #10 will have no sense of setting *20/40MHz HT above* since no full 20MHz channel is available

Wireless frequency usage

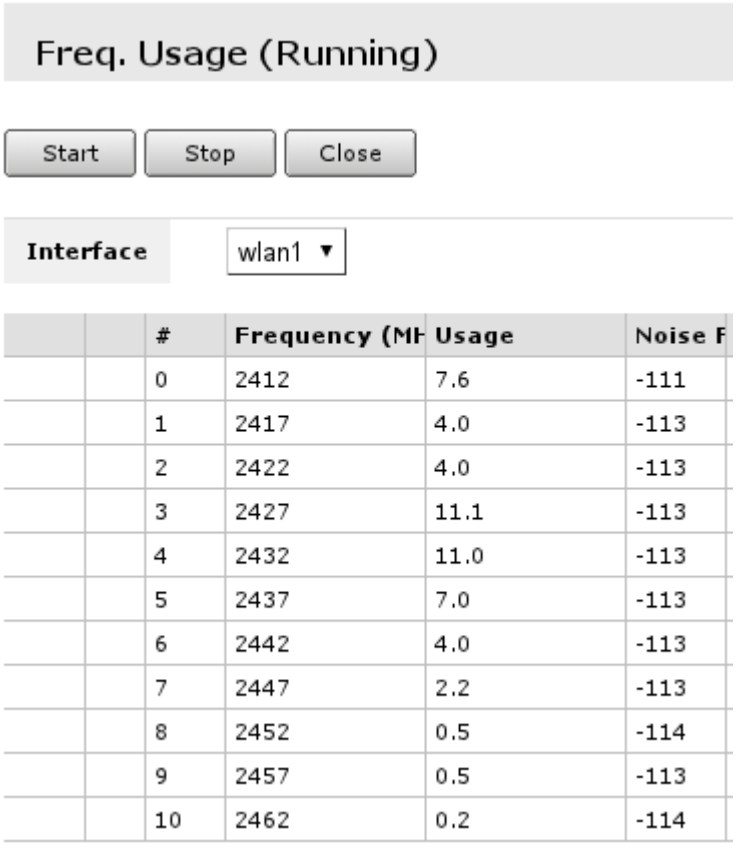
If wireless is not performing very well even when data rates are reported as being good, there

might be that your neighbours are using same wireless channel as you are. To make sure follow these steps:

- Open frequency usage monitoring tool *Freq. Usage...* that is located in wireless interface details;



- Wait for some time as scan results are displayed. Do that for minute or two. Smaller numbers in *Usage* column means that channel is less crowded.



		#	Frequency (MH	Usage	Noise F
		0	2412	7.6	-111
		1	2417	4.0	-113
		2	2422	4.0	-113
		3	2427	11.1	-113
		4	2432	11.0	-113
		5	2437	7.0	-113
		6	2442	4.0	-113
		7	2447	2.2	-113
		8	2452	0.5	-114
		9	2457	0.5	-113
		10	2462	0.2	-114

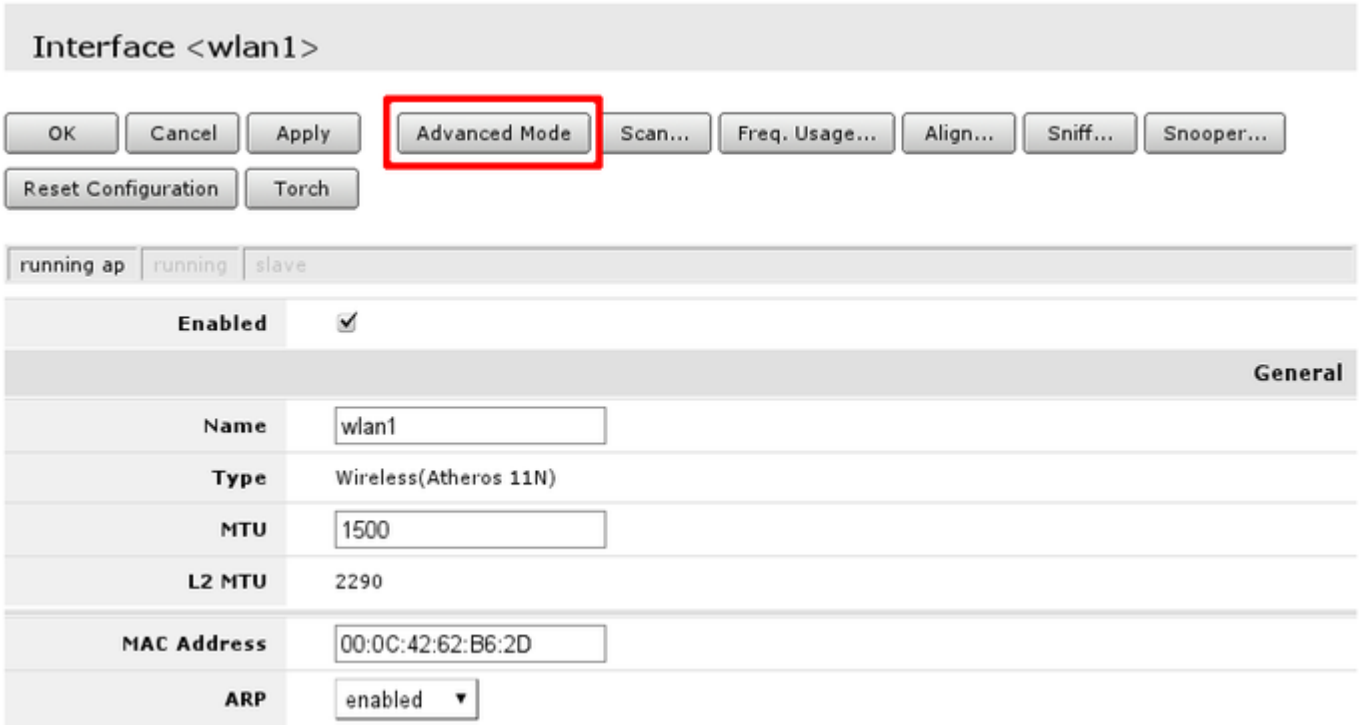
Note: Monitoring is performed on default channels for *Country* selected in configuration. For example, if selected country would be Latvia, there would have been 13 frequencies listed as at that country have 13 channels allowed.

Change Country settings

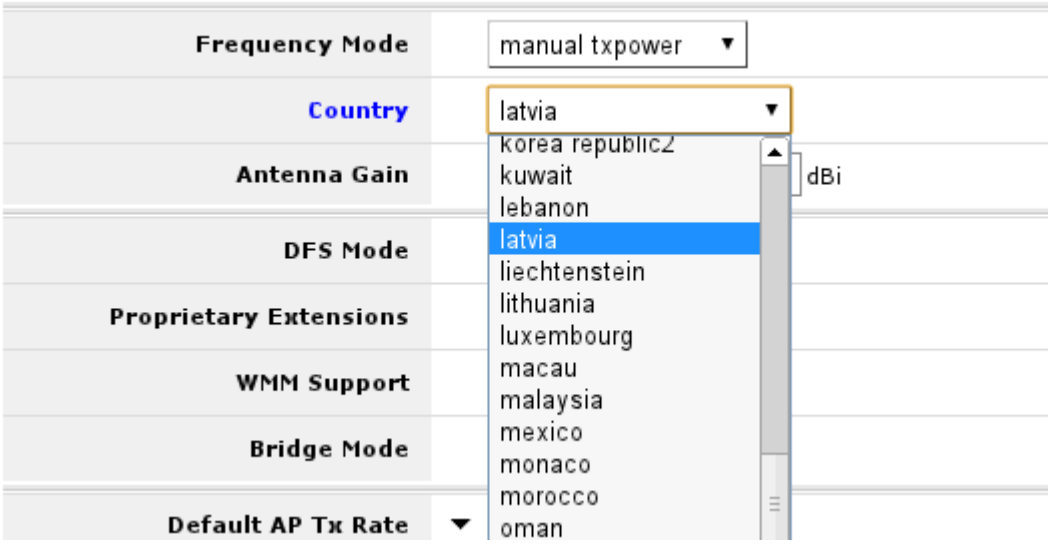
By default *country* attribute in wireless settings is set to *no_country_set*. It is good practice to

change this (if available) to change country you are in. To do that do the following:

- Go to wireless menu and select *Advanced mode*;



- Look up *Country* attribute and from drop-down menu select country



Note: Advanced mode is toggle button that changes from Simple to Advanced mode and back.

Port forwarding

To make services on local servers/hosts available to general public it is possible to forward ports

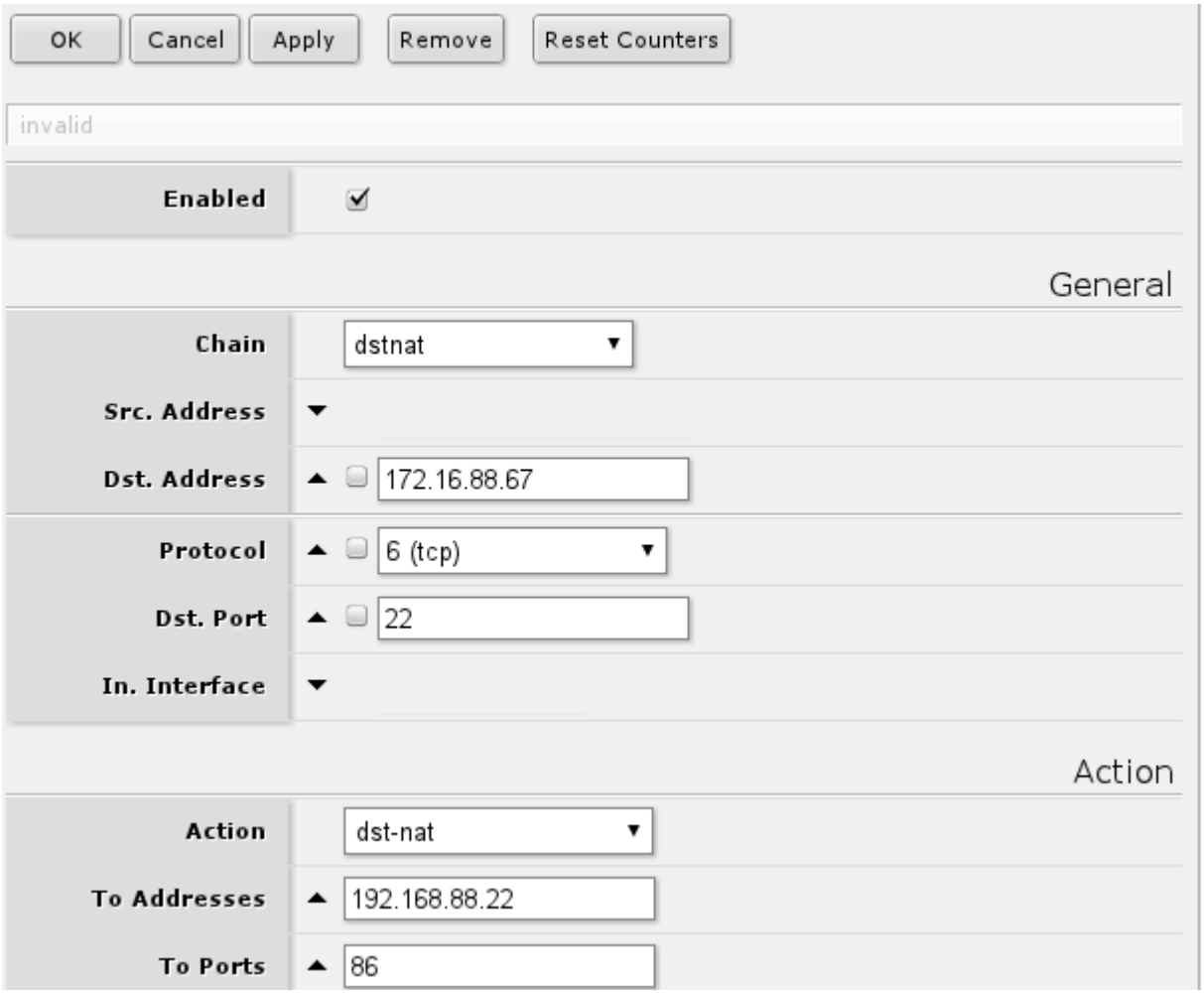
from outside to inside your NATed network, that is done from */ip firewall nat* menu. For example, to make possible for remote helpdesk to connect to your desktop and guide you, make your local file cache available for you when not at location etc.

Static configuration

A lot of users prefer to configure these rules statically, to have more control over what service is reachable from outside and what is not. This also has to be used when service you are using does not support dynamic configuration.

Following rule will forward all connections to port 22 on the router external ip address to port 86 on your local host with set IP address:

if you require other services to be accessible you can change protocol as required, but usually services are running TCP and dst-port. If change of port is not required, eg. remote service is 22 and local is also 22, then to-ports can be left unset.



Comparable command line command:

```
/ip firewall nat add chain=dstnat dst-address=172.16.88.67 protocol=tcp dst-port=22 \
action=dst-nat to-address=192.168.88.22 to-ports=86
```

Note: Screenshot contain only minimal set of settings are left visible

Dynamic configuration

uPnP is used to enable dynamic port forwarding configuration where service you are running can request router using uPnP to forward some ports for it.

Warning: Services you are not aware of can request port forwarding. That can compromise security of your local network, your host running the service and your data

Configuring uPnP service on the router:

- Set up what interfaces should be considered external and what internal;

```
/ip upnp interface add interface=ether1 type=external
/ip upnp interface add interface=ether2 type=internal
```

- Enable service itself

```
/ip upnp set allow-disable-external-interface=no show-dummy-rule=no enabled=yes
```

Limiting access to web pages

Using *IP -> Web Proxy* it is possible to limit access to unwanted web pages. This requires some understanding of use of WebFig interface.

Set up Web Proxy for page filtering

From *IP -> Web Proxy* menu *Access* tab open *Web Proxy Settings* and make sure that these attributes are set follows:

```
Enabled -> checked
Port -> 8080
Max. Cache Size -> none
Cache on disk -> unchecked
Parent proxy -> unset
```

When required alterations are done *apply*settings to return to *Access* tab.

Set up Access rules

This list will contain all the rules that are required to limit access to sites on the Internet.

To add sample rule to deny access to any host that contain example.com do the following when adding new entry:

```
Dst. Host -> .*example\.com.*
Action -> Deny
```

With this rule any host that has example.com will be unaccessible.

Limitation strategies

There are two main approaches to this problem

- deny only pages you know you want to deny *(A)*
- allow only certain pages and deny everything else *(B)*

For approach *A* each site that has to be denied is added with *Action* set to *Deny*

For approach *B* each site that has to be allowed should be added with *Action* set to *Allow* and in the end is rule, that matches everything with *Action* set to *Deny*.

[Top | Back to Content **]**

Category: Manual