

Пример настройки роутеров фирмы MikroTik.

Внимание! Перед настройкой роутера рекомендуется обновить прошивку маршрутизатора (роутера) до последней версии. Последние версии прошивок можно найти на сайте производителя.

Подключите устройство к компьютеру (желательно проводом, поставляющимся в комплекте). Откройте "Internet Explorer" или аналогичный браузер, наберите в строке адреса "192.168.88.1" (в некоторых моделях роутеров адрес может быть другим). Подключение по беспроводной связи к устройству или попытка открытия настроек через любой другой Интернет-браузер не всегда могут быть успешными.

Укажите Login и Password (Логин и Пароль) в соответствии с указанными производителем данными по умолчанию. Обычно они нанесены на наклейке снизу, либо на корпусе маршрутизатора (роутера). На некоторых моделях пароль устанавливается при настройке роутера.

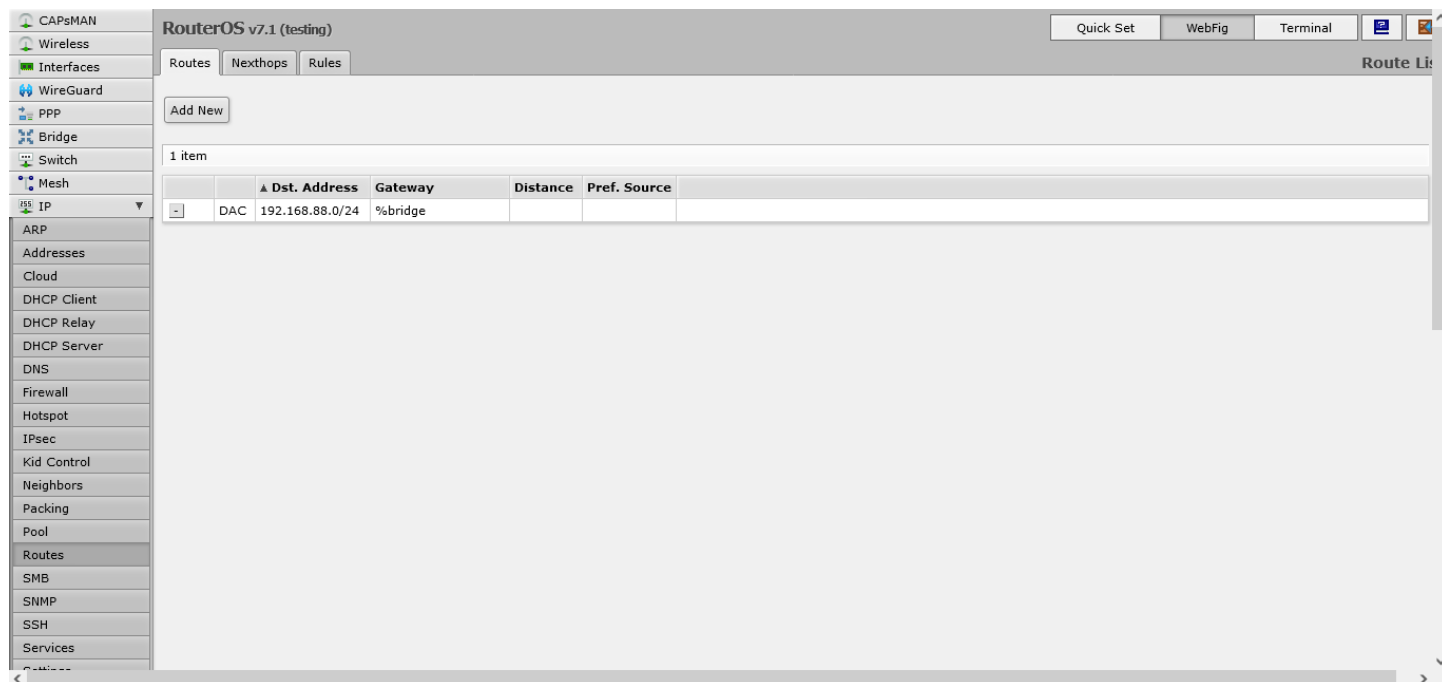
Подключите кабель, и дождитесь пока роутер не получит "IP Adress", в разделе «Internet». Вычислите шлюз (Gateway), по принципу: У IP равном 10.10.1.1 шлюз будет равным 10.0.10.1, у IP равном 10.10.2.1 шлюз будет равным 10.0.10.2 и т.д.

The screenshot displays the RouterOS v7.1 (testing) configuration interface. The top navigation bar includes buttons for 'Quick Set', 'WebFig', 'Terminal', and a language selector. The main interface is divided into several sections:

- Wireless:** Configures 2GHz and 5GHz networks. The 2GHz network is named 'MikroTik-2G' with frequency 'auto' and band '2GHz-B/G/N'. The 5GHz network is named 'MikroTik-5G' with frequency 'auto' and band '5GHz-A/N/AC'. Both are set to country 'etsi'. A 'WIFI Password' is entered and hidden.
- Internet:** Shows 'Address Acquisition' set to 'Automatic'. The 'IP Address' is 192.168.88.1, 'Netmask' is 255.255.255.0 (/24), and 'Gateway' is empty. 'Firewall Router' is checked.
- Local Network:** Shows 'IP Address' as 192.168.88.1 and 'Netmask' as 255.255.255.0 (/24). 'DHCP Server' is checked, and the 'DHCP Server Range' is 192.168.88.10-192.168.88.254. 'NAT' is checked and 'UPnP' is unchecked.
- Guest Wireless Network:** A table shows a single wireless network 'W' with MAC address, last IP (192.168.88.222), uptime (00:07:33), and signal strength (-56).

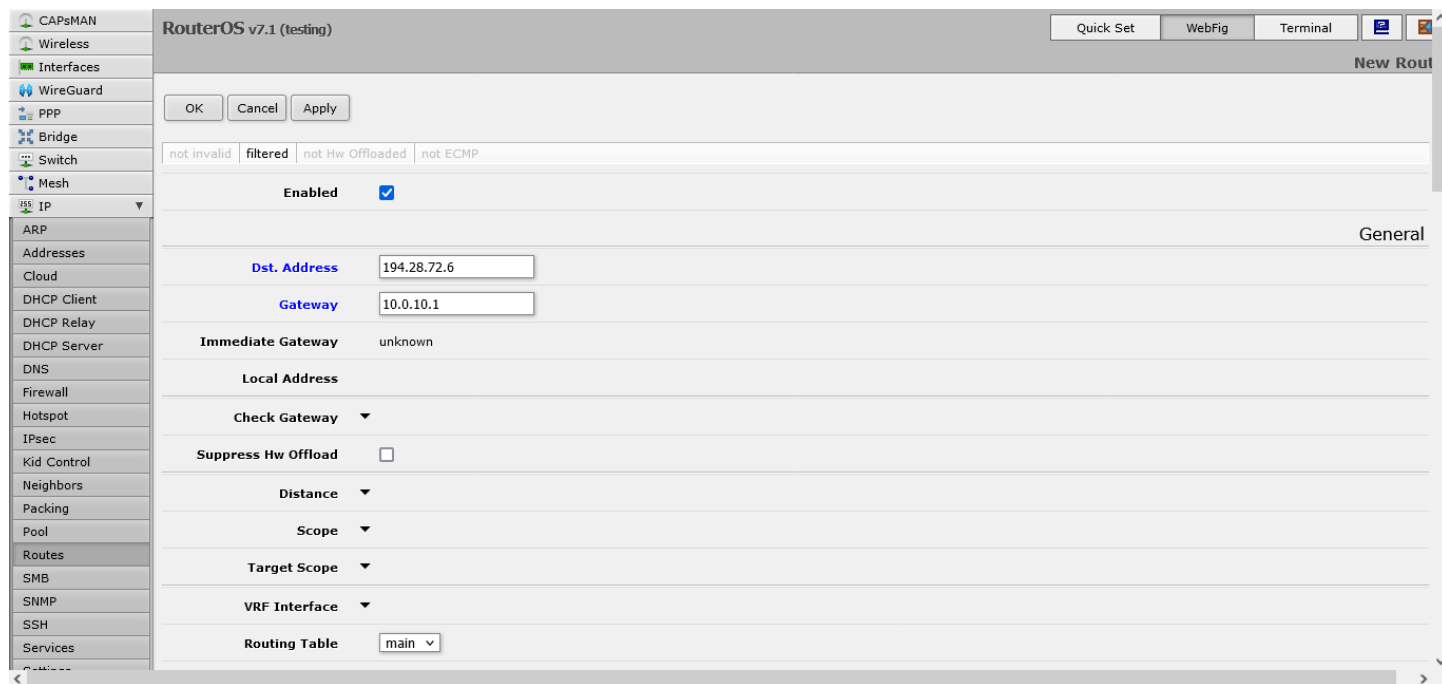
Buttons for 'WPS Accept', 'Port Mapping', 'Check For Updates', 'Reboot', 'Reset Configuration', 'Password...', and 'Apply Configuration' are visible throughout the interface.

Для настройки в правом верхнем углу переключите вид в режим WebFig. Далее открываем вкладку «IP», и выбираем в нём «Routes»:



В появившейся вкладке нажимаете «Add New»:

1. В поле «Dst. Address» указываете «194.28.72.6» .
2. В поле «Gateway» указываете шлюз. На картинке приведён ПРИМЕР, вы должны вписать ВАШ шлюз.
3. Далее нажимаете «OK».
4. Данную процедуру необходимо выполнить два раза, во второй раз указывать «194.28.72.9» .



Далее переходите во вкладку «Interfaces», нажимаете «Add New» и выбираете «L2TP Client»:

	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	
;;: defconf											
D	R	bridge	Bridge	1500	1598	94.6 kbps	7.6 kbps	10	3	0 bps	7.6 kbps
D	S	ether1	Ethernet	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps
D	S	ether2	Ethernet	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps
D	S	ether3	Ethernet	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps
D	S	ether4	Ethernet	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps
D	S	ether5	Ethernet	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps
D	RS	wlan1	Wireless (Atheros AR9130)	1500	1600	95.1 kbps	7.6 kbps	11	3	0 bps	7.6 kbps
D	S	wlan2	Wireless (Atheros AR9130)	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps

В данном окне выставляете как на картинке.

1. В поле «Name» указываете название соединения.
2. В поле «Connect To» указываете адрес сервера для подключения - 194.28.72.6 .
3. В соответствующих полях указываете идентификационные данные (логин и пароль) из Памятки Абонента.
4. Нажмите «OK» чтобы сохранить настройки.

OK Cancel Apply Torch

not invalid not running not slave

Enabled

Name Zelenaya

Type L2TP Client

Actual MTU

Max MTU 1450

Max MRU 1450

MRRU

Connect To 194.28.72.6

User

Password

Profile default-encryption

Dial On Demand

Add Default Route

Default Route Distance 1

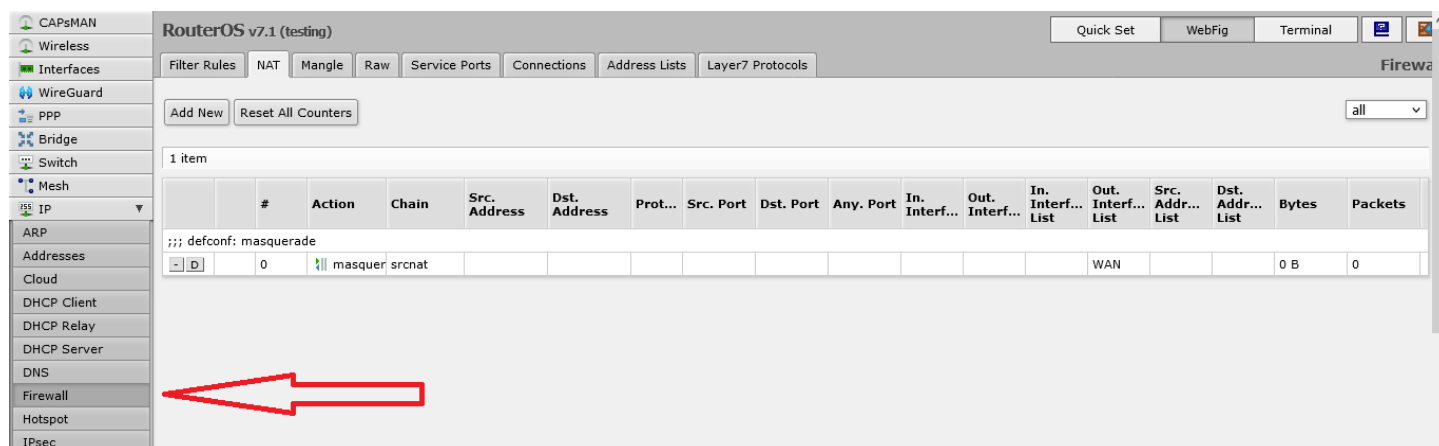
Allow mschap2 mschap1 chap pap

L2TP Protocol Version l2tpv2

Status

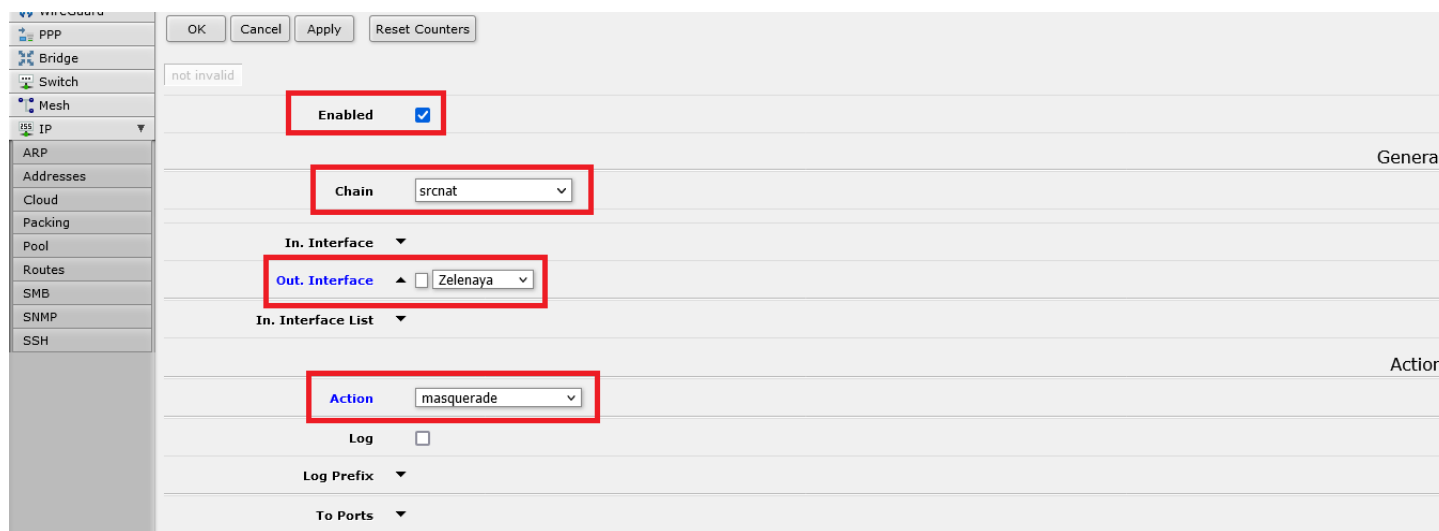
Следующий этап - включаем маскардинг на этом соединении и добавляем правила фильтра.

Для этого в левом столбце «IP» выбираем «Firewall», далее нажимаем на вкладку «NAT». Нажимаем кнопку «Add New».



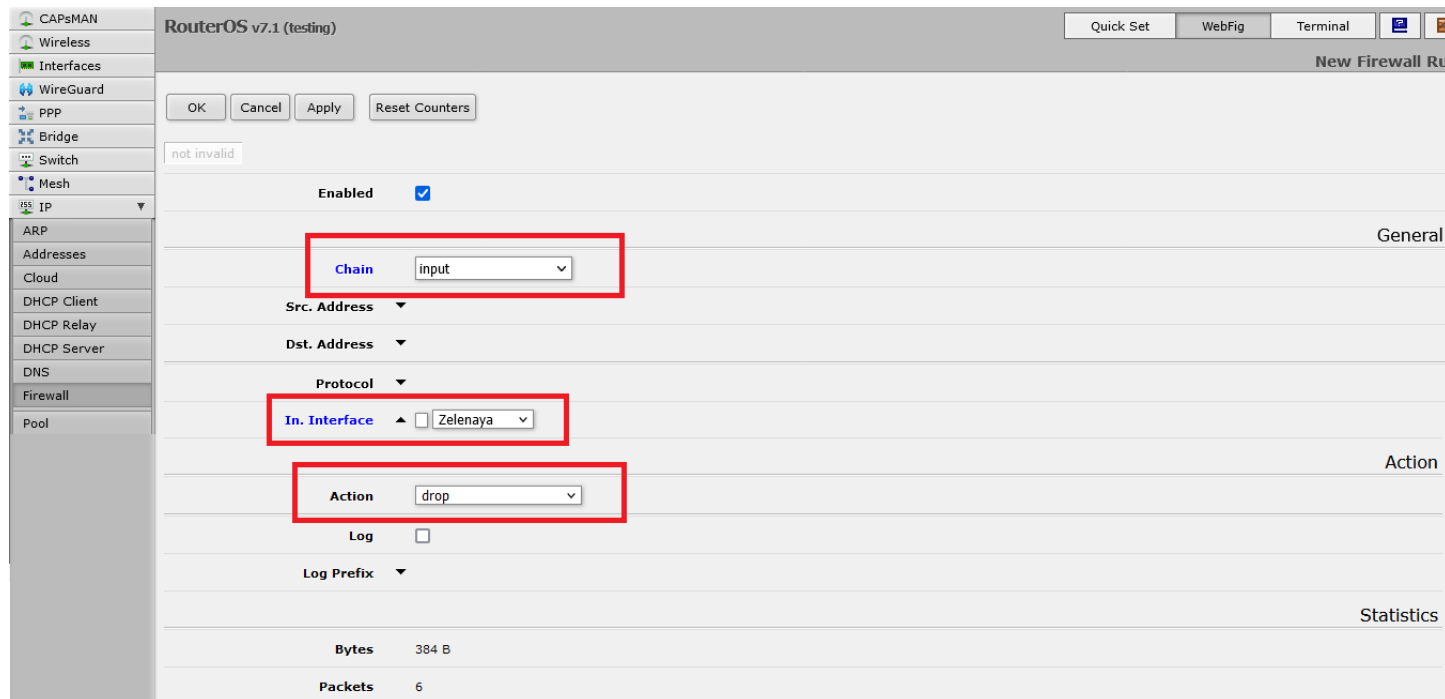
Заполняем в следующем порядке:

1. Для «Chain» выбираем «srcnat».
2. Для «Out-interface» выбираем «Zelenaya» (это имя соединения указанное вами выше).
3. Для «Action» выбираем «masquerade».
4. Нажимаем «OK».



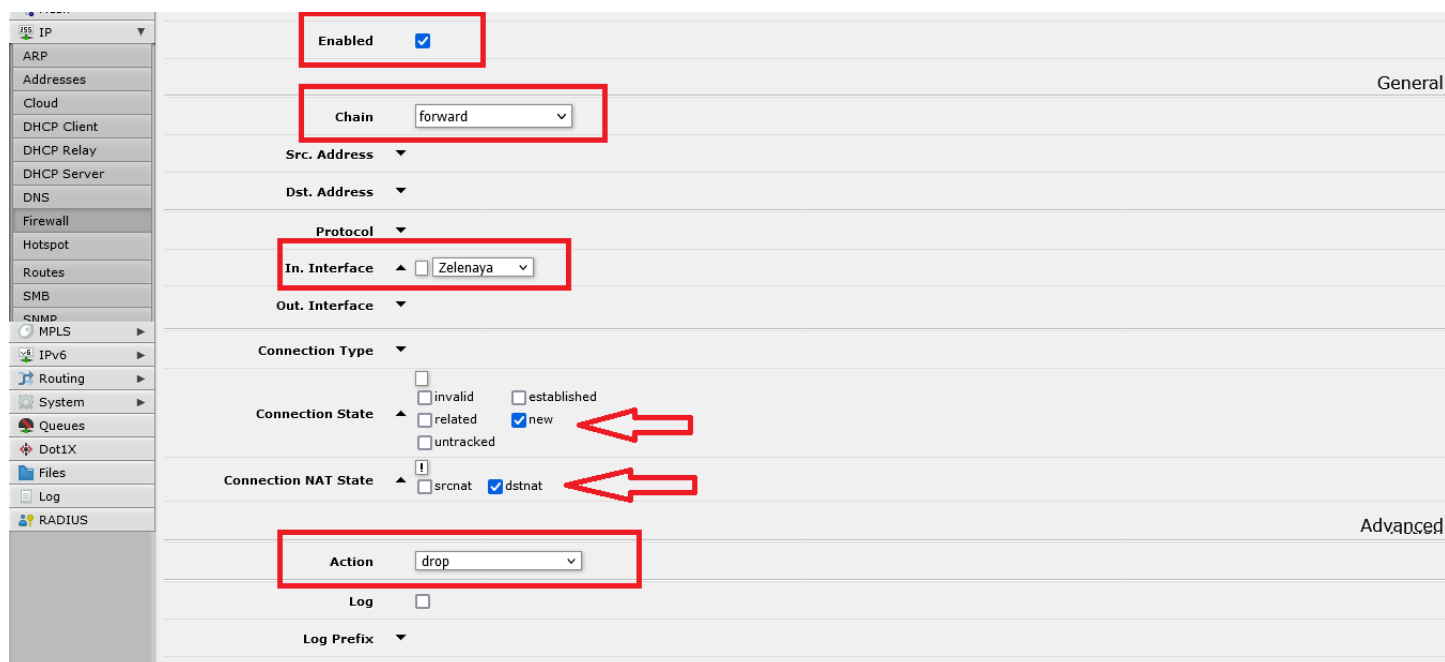
Переходим обратно во вкладку «Filter Rules». Нажимаем «Add New». Заполняем в следующем порядке:

1. Для «Chain» выбираем «input».
2. Для «In-interface» выбираем «Zelenaya» (это имя соединения указанное вами ранее).
3. Для «Action» выбираем «drop».
4. Нажимаем «OK».

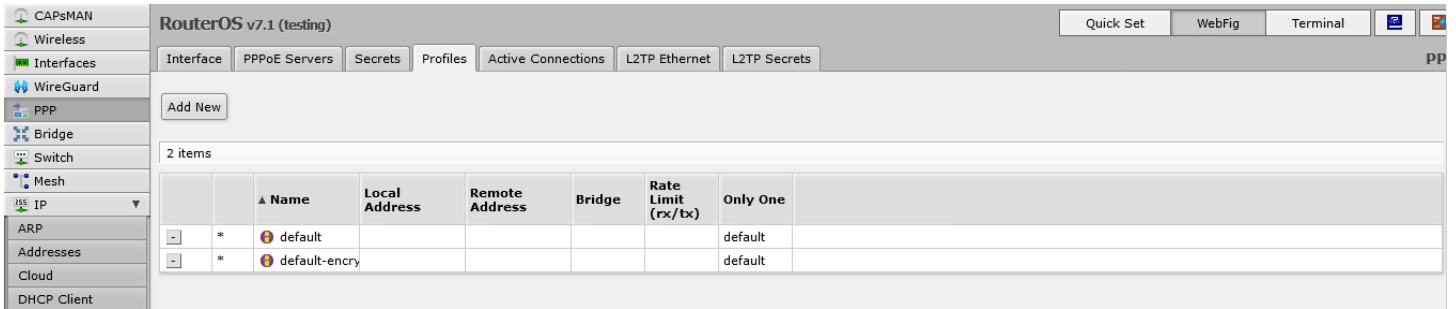


Далее создаём второй фильтр, нажимаем «Add New». Заполняем в следующем порядке:

1. Для «Chain» выбираем «forward».
2. Для «In-interface» выбираем «Zelenaya» (это имя соединения указанное вами ранее).
3. Для «Connection-nat-state» выбираем только «!dstnat».
4. Для «Connection-state» выбираем только «new».
5. Для «Action» выбираем «drop».
6. Нажимаем «OK».

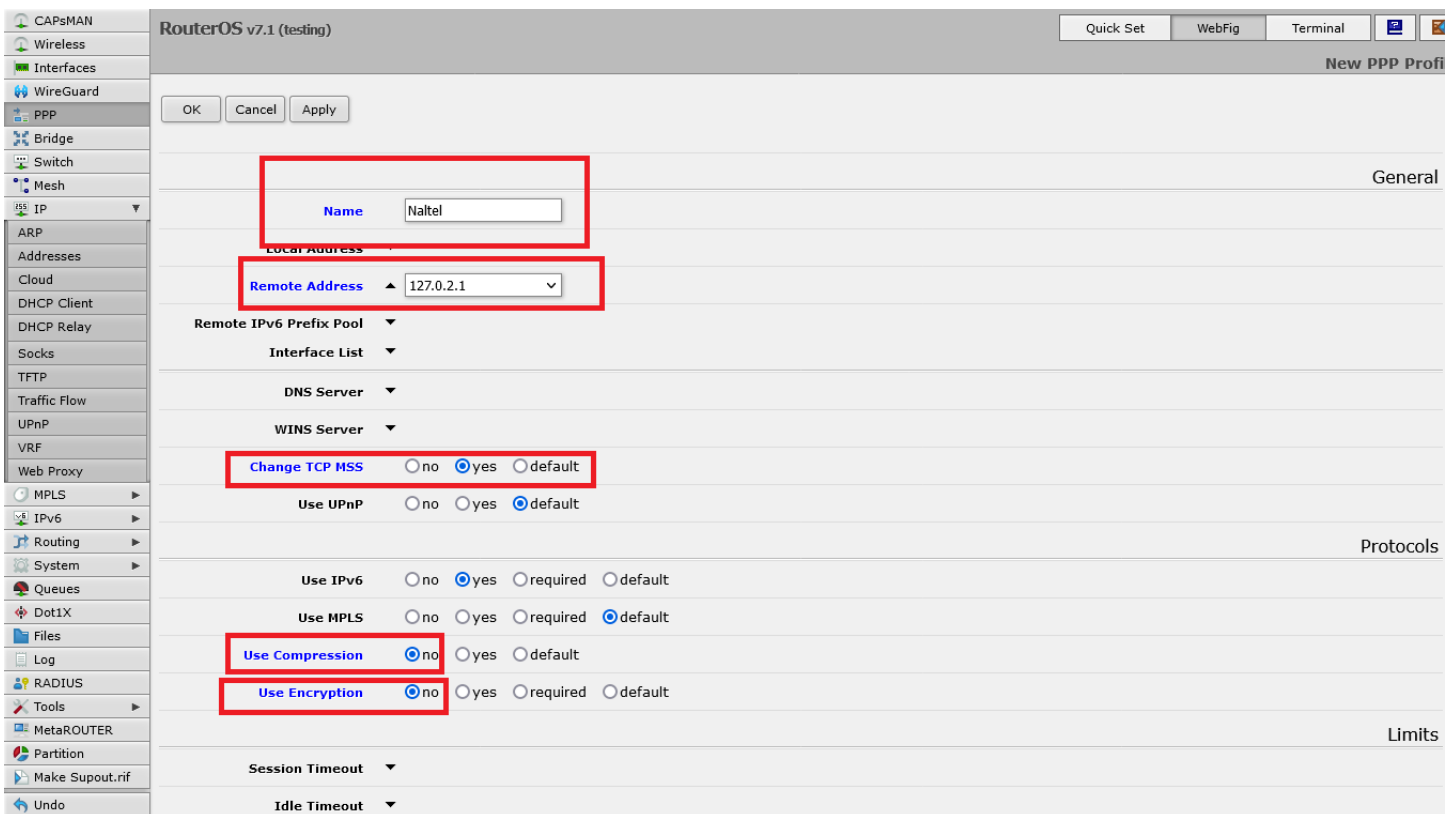


Для избегания нарушений в маршрутизации через тоннель, заменяем Remote Address на адрес из локальной подсети. Для этого в левом столбце выбираем «PPP» и нажимаем на вкладку «Profiles». Нажимаем кнопку «Add New»:



Добавляем новый профиль:

1. В поле «Name» указываем имя, например «Naltel».
2. В поле «Remote adress» вписываем «127.0.2.1».
3. Для «TCP MSS» выбираем только «yes».
4. Для «Use Compression» выбираем только «no».
5. Для «Use Encryption» выбираем только «no».
6. Нажимаем «OK» для сохранения настроек.



Интернет соединение в роутере настроено. Через вкладку «System» выбираем «Reboot» и перезагружаем роутер.