WiMAX router

User Manual

Suitable for:

RUT423, RUT425, RUT435, RUT438

LEGAL NOTICE

ATTENTION

Before using the device we strongly recommend reading this user manual first.

Do not rip open the device. Do not touch the device if the device block is broken.

All wireless devices for data transferring may be susceptible to interference, which could affect performance.

The device is not water-resistant. Keep it dry.

The device requires high 230V AC voltage.

Table of contents

LEGAL NOTICE **2**

ATTENTION **2**

TABLE OF CONTENTS **3**

SAFETY INFORMATION **4**

PRODUCT OVERVIEW **5**

INTRODUCTION 5
PACKAGE CONTENTS 5
SYSTEM REQUIREMENTS 5
HARDWARE, LED'S AND CONNECTIONS 6

WEBUI OVERVIEW **7**

CONNECTING TO THE WEBUI 7
WEBUI STRUCTURE 8
STATUS 8
NETWORK 9
IP address *9*
DHCP server *9*
Dynamic DNS *10*
OpenVPN *11*
FIREWALL 12
Port forwarding *12*
Mac filtering *13*
IP filtering *14*
Demilitarization zone *15*
ADMINISTRATION 15
Settings *15*
Firmware *16*
Password *16*
Auto Reboot *17*
ABOUT 17

TROUBLESHOOTER: **18**

TECHNICAL SPECIFICATIONS: **20**

ELECTRICAL, MECHANICAL & ENVIRONMENTAL: 20

SAFETY INFORMATION

In this section you will be introduced on how to use a RUT4XX router safely. We suggest you to adhere to the following recommendations in order to avoid personal injuries and or property damage.

You have to be familiar with the safety requirements before using the device!
To avoid burning and voltage caused traumas, of the personnel working with the device, please follow these safety requirements.

⚠ This device requires a power supply that satisfies all safety requirements listed in the LST EN 60950-1 standard. Each power supply should not exceed 15VA.

⚠ The PC to which the device is connected, should satisfy the LST EN 60950-1 standard. The device can be used on first (Personal Computer) or second (Notebook) computer safety class.

⚡ Do not mount or serve device during a thunderstorm.

⚡ Disconnect device from power supply before mounting to avoid voltage effect!

To avoid mechanical damages to the device it is recommended to transport it packed in a damage-proof pack. While using the device, it should be placed so, that its indicating LEDs would be visible as they inform in which working mode the device is and if it has any working problems.

Protection against overcurrents, short-circuiting and earth faults should be provided as a part of the building installation. A two pole protective device is required in order to protect from short-circuiting and earth faults. To disconnect the device plug off the AC/DC power adapter from the wall outlet or power strip. The gap between contacts should be no less than 3mm.

Signal level of the device depends on the working environment. In case the device starts working insufficiently, please refer to qualified personnel in order to repair this product. We recommend to forward it to a repair centre or to the manufacturers. There are no exchangeable parts within the device.

PRODUCT OVERVIEW

Introduction

Teltonika RUT4XX router provides wireless connectivity using WiMAX technology. It supports IEEE 802.16e standard, therefore it is flexible and can be used in a set of different environments.

Package contents

RUT4XX
• WiMAX router
• 2 external WiMAX antennas
• Power adapter
• LAN cable

Note: The provisioning information is provided by your service provider, therefore any questions regarding connectivity problems should be addressed to it.

Note: If any of the components are missing or damaged, please contact the retailer or reseller from which this product was purchased.

Note: Using a power supply with a different voltage rating than the one included with the router will cause damage and void the warranty for this product.

System requirements

- Wired network connection.
- Windows XP, Windows Vista, Windows 7, MAC OS X, or a Linux-based operating system.
- A web browser must have a flash player plug-in (version 10 or higher) in order to access the WebUI for network configuration.

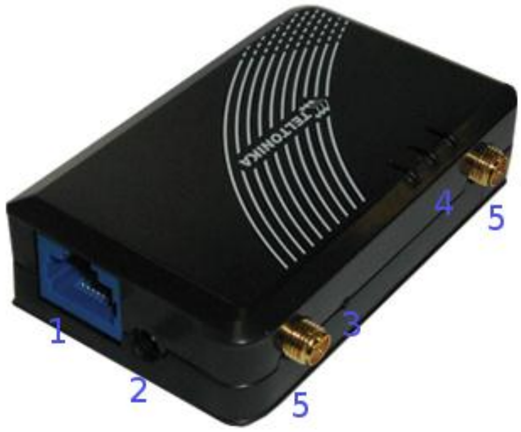
Hardware, LED's and connections

To set up a router do these steps:

- Screw on two antennas provided in the package.

- Plug a power supply and a LAN cable to the router.

RUT4xx explained:



RUT4xx device

1. Ethernet port.
2. Power connection.
3. Reset (Reset to factory defaults – optional).
4. Indication LED (from left to right)
    - Activity.
    - Power plugged in.
    - LAN cable plugged-in.
5. Antenna connectors.
6. Quick start guide.

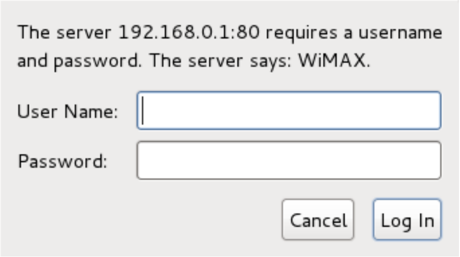
WebUI OVERVIEW

In this section you will be briefly introduced to our user interface.
Note: we use an intuitive tool tip system in our web user interface which displays additional data for the user. To see this data hover your mouse cursor above the field. Also, if the frame of the field becomes red, it usually means that the data in the field is incorrect, in this case look into red tool tip for more information.

Connecting to the WebUI

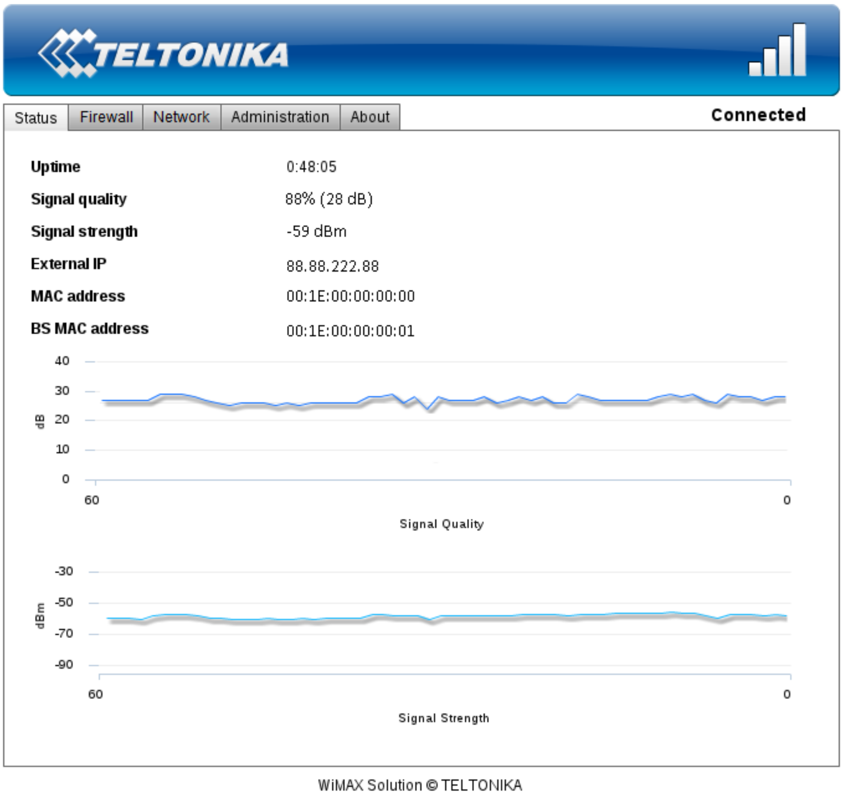
To connect to the configuration web page do the following steps:

1. Type **192.168.0.1** to your favorite internet browser. Skip the step 2 if the password is disabled.
2. Window asking for authentication will pop up. Enter your username and password (default: username: user, password: user) and press enter.



The server 192.168.0.1:80 requires a username and password. The server says: WiMAX.

3. Status window will appear in a few seconds:



Uptime 0:48:05
Signal quality 88% (28 dB)
Signal strength -59 dBm
External IP 88.88.222.88
MAC address 00:1E:00:00:00:00
BS MAC address 00:1E:00:00:00:01

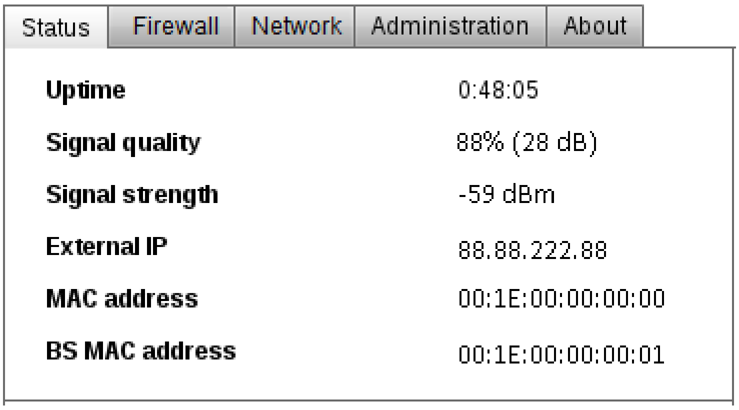
WiMAX Solution © TELTONIKA

First page of WebUI

WebUI structure

Our modern web user interface provides you with all the tools needed within the five main pages: **Status**, **Network**, **Firewall**, **Administration**, **About**.

Status



Uptime	0:48:05
Signal quality	88% (28 dB)
Signal strength	-59 dBm
External IP	88.88.222.88
MAC address	00:1E:00:00:00:00
BS MAC address	00:1E:00:00:00:01

Status page

The status page consists of 6 properties that define the current state of the router:

1. **Uptime** – amount of time since the last reboot (or plug in).
2. **Signal quality** – the quality of a signal in percents (and decibels).

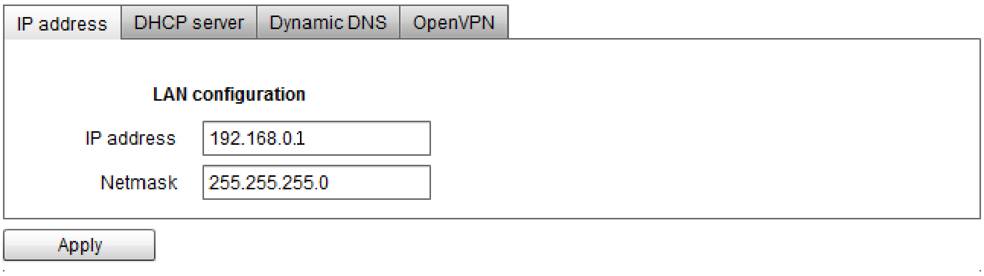
   <30% poor
   >30% <50% decent
   >50% <90% good
   >90% very good

   Note: signal quality depends on the distance between the device and the base station, plus other factors: interference with other devices, etc.
3. **Signal strength** – the strength of the signal in dBm.
4. **External IP** – IP which was assigned by the base station to your device.
5. **MAC address** – physical address of the WiMAX connection module.
6. **BS MAC address** - physical address of the base station.

Network

Network settings page allows the user to change the IP address, net mask and DHCP server settings.

IP address



LAN configuration

IP address: 192.168.0.1

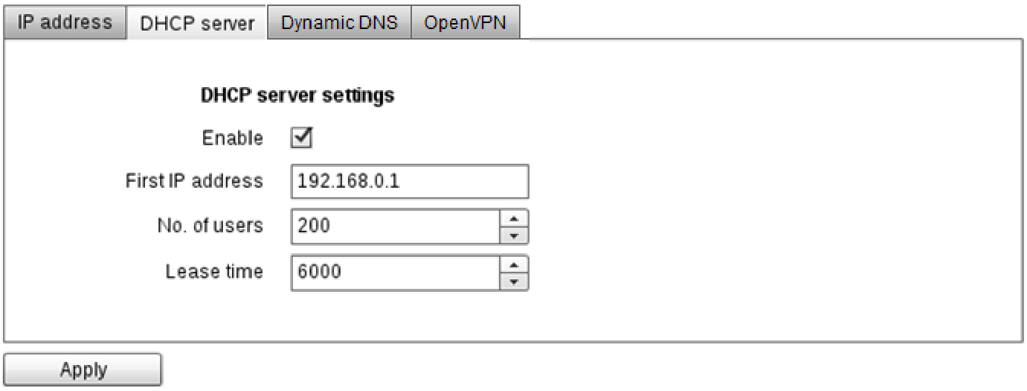
Netmask: 255.255.255.0

IP address settings page

IP address – IP address of the router.
Netmask – mask used to divide IP address into subnets.

DHCP server

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers configured for a given network.



DHCP server settings

Enable: ☑

First IP address: 192.168.0.1

No. of users: 200

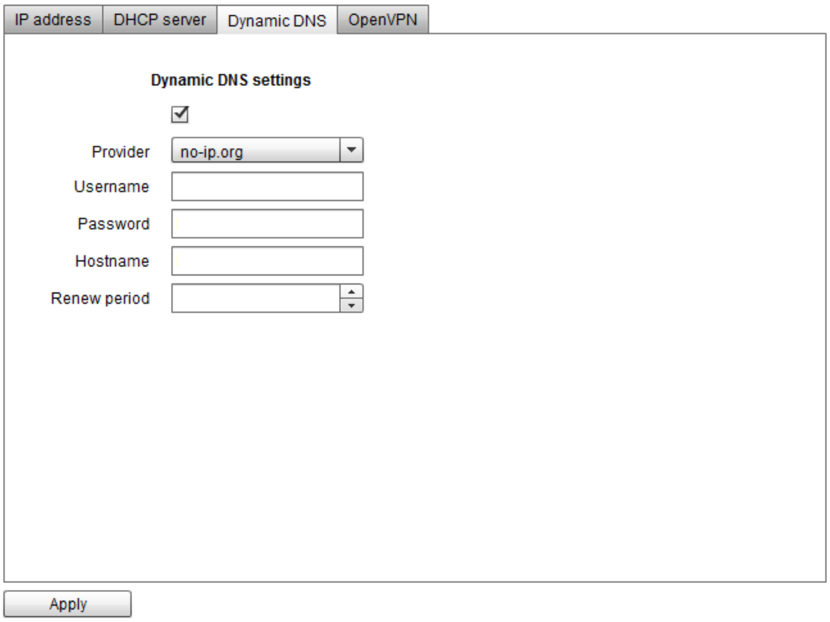
Lease time: 6000

DHCP server form

Enable – check to enable the DHCP server.
First IP address – First IP from the range to be leased.
No. of users – number of IP addresses to be leased.
Lease time – time after the leased IP expires.

Dynamic DNS

Dynamic DNS (DDNS) is a domain name service allowing to link dynamic IP addresses to static hostname. To start using this feature firstly you should register to DDNS service provider.



Dynamic DNS settings

☑

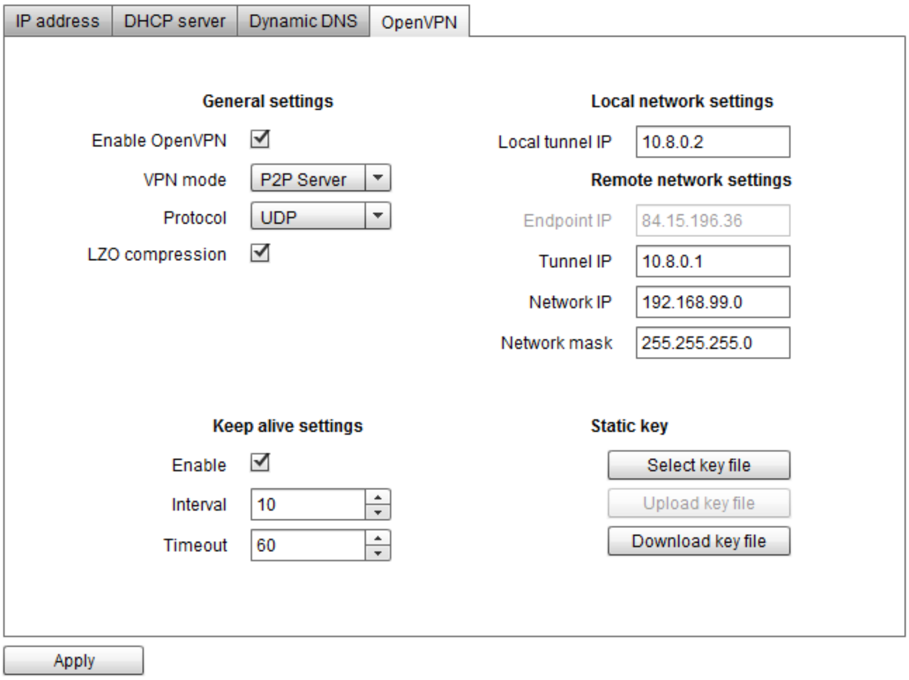
Provider	no-ip.org
Username	
Password	
Hostname	
Renew period	

DDNS form

Provider – your dynamic DNS service provider selected from the list.
Username – name of the user account.
Password – password of the user account.
Hostname – domain name that you will be able to use instead of your IP address.
Renew period – time interval to check if IP address of the device have changed.

OpenVPN

VPN (virtual private network) is a secure network that provides remote offices or traveling users an access to a central organizational network.



General settings

Enable OpenVPN ☑

VPN mode: P2P Server

Protocol: UDP

LZO compression ☑

Local network settings

Local tunnel IP: 10.8.0.2

Remote network settings

Endpoint IP: 84.15.196.36

Tunnel IP: 10.8.0.1

Network IP: 192.168.99.0

Network mask: 255.255.255.0

Keep alive settings

Enable ☑

Interval: 10

Timeout: 60

Static key

OpenVPN form

General:

Enable OpenVPN – enables VPN functionality.

VPN mode – changes VPN mode **Client**/**Server.**

Protocol – use **TCP** or **UDP** for transmitting packets.

LZO compression – check the box to enable fast adaptive LZO compression.

Network:

Local tunnel IP – specifies the IP address of the local VPN tunnel endpoint.

Endpoint IP – specifies server IP address.

Tunnel IP – specifies the IP address of the remote VPN tunnel endpoint.

Network IP – specifies the remote network IP.

Network mask – specifies the remote network subnet mask.

Keep alive:

Enable – turns on “Keep alive” feature.

Interval – specifies time interval to check if VPN connection is still alive.

Timeout – specifies time span for the network to respond.

Firewall

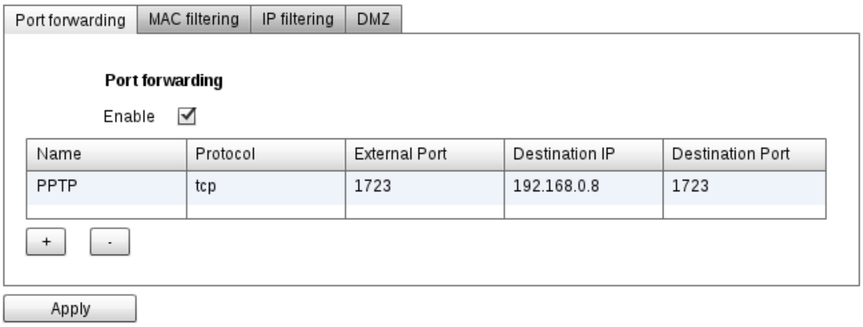
Firewall page lets you configure firewall settings to meet your requirements. It includes port-forwarding, MAC filtering and IP filtering

Port forwarding

Port forwarding is the process of translating the address and port number of a packet to a new destination.

Follow these steps to add a port-forwarding rule:

1. **Enable** – check to enable the Port forwarding.
2. Press the **+** button.



Port forwarding

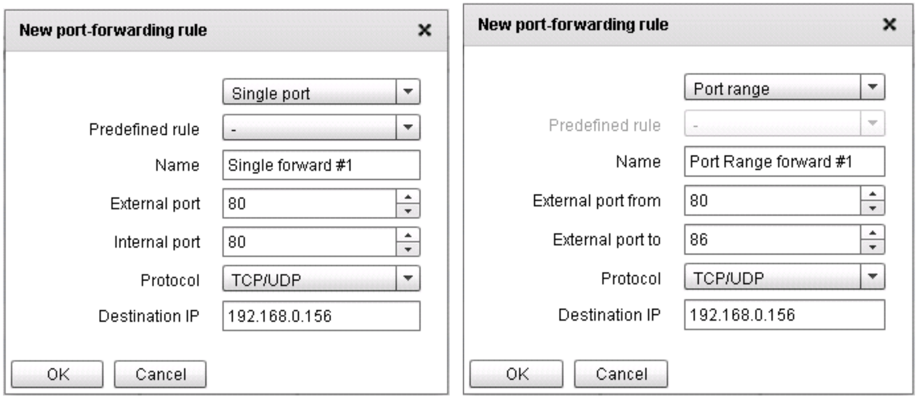
Enable ☑

Name	Protocol	External Port	Destination IP	Destination Port
PPTP	tcp	1723	192.168.0.8	1723

Port forwarding form

The following port-forwarding rule creation window will pop-up. Choose a rule type (single port or port range) and fill the fields in a window to define your rule:

- **Predefined rule** – select from a list of most common rules.
- **Name** – the name of the rule that will be visible in the list of your defined rules.
- **External port from/to** – external port range to be redirected to an identical internal port range.
- **External port** – external port to be redirected to **Internal port.**
- **Internal port** – port used by the destination device to receive data.
- **Protocol** – protocol in which rule operates.
- **Destination IP** – the address of the device to which all the data coming to the selected external ports is forwarded to.



New port-forwarding rule

	Single port
Predefined rule	-
Name	Single forward #1
External port	80
Internal port	80
Protocol	TCP/UDP
Destination IP	192.168.0.156

New port-forwarding rule

	Port range
Predefined rule	-
Name	Port Range forward #1
External port from	80
External port to	86
Protocol	TCP/UDP
Destination IP	192.168.0.156

New port-forwarding rule windows

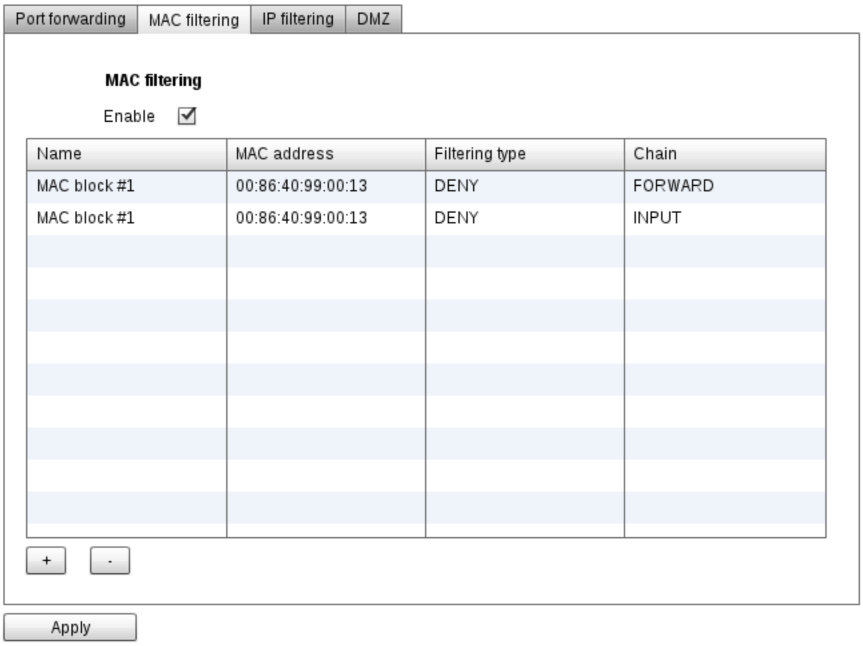
3. Press **OK** button to accept the rule.
4. Press **Apply** to save the rules to the configuration.

Mac filtering

MAC filtering is a security access control method used to determine access to the network by physical address.

Follow these steps to add a MAC filtering rule:

1. **Enable** – check to enable the MAC filtering.
2. Press the **+** button.



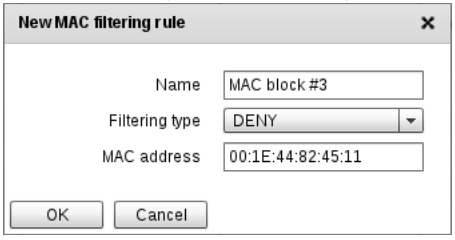
MAC filtering

Enable ☑

Name	MAC address	Filtering type	Chain
MAC block #1	00:86:40:99:00:13	DENY	FORWARD
MAC block #1	00:86:40:99:00:13	DENY	INPUT

Mac filtering form

3. The following MAC filtering rule creation window will pop-up.



New MAC filtering rule

Name	MAC block #3
Filtering type	DENY
MAC address	00:1E:44:82:45:11

New MAC filtering rule window

- **Name** – MAC filtering rule name.
- **MAC address** – physical address that you want to block from connecting to and/or through the router.

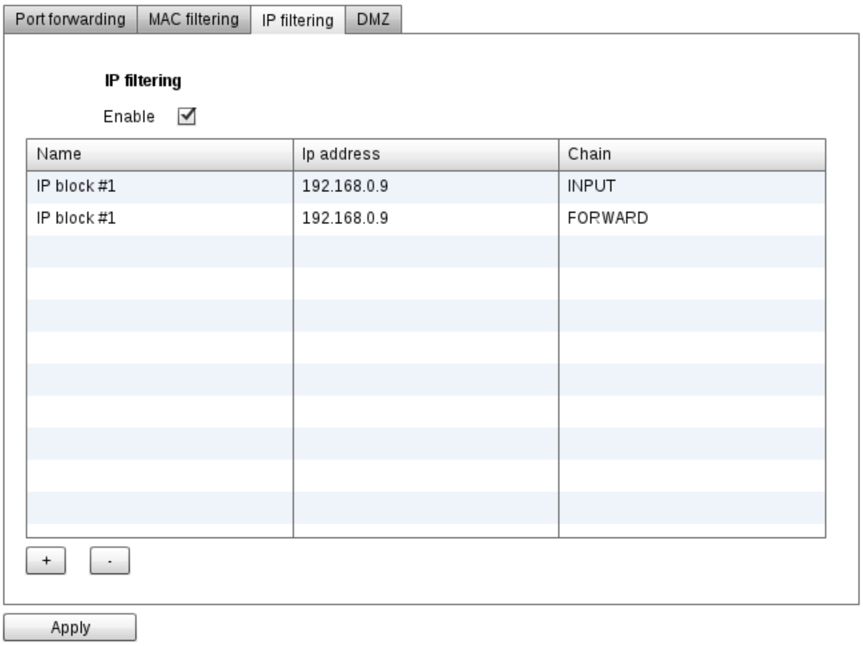
4. Press **OK** to add the rule.
5. After adding all the rules that you needed, press **Apply** to save the rules to the configuration.

IP filtering

IP filtering is a security access control method used to determine access to the network by IP address.

Follow these steps to add an IP filtering rule:

1. **Enable** – check to enable the IP filtering.
2. Press the **+** button.



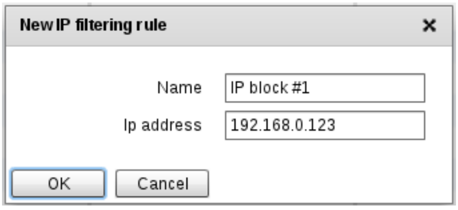
IP filtering

Enable ☑

Name	Ip address	Chain
IP block #1	192.168.0.9	INPUT
IP block #1	192.168.0.9	FORWARD

IP filtering form

3. The following IP filtering rule creation window will pop-up.



New IP filtering rule

Name: IP block #1

Ip address: 192.168.0.123

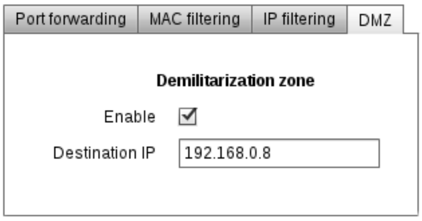
New IP filtering rule window

- **Name** – IP filtering rule name.
- **IP address** – remote IP address that you want to block from connecting to and/or through the router.

4. Press **OK** to add the rule.
5. After adding all the rules that you needed, press **Apply** to save the rules to the configuration.

Demilitarization zone

In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a private network and the outside public network.



Enable ☑

Destination IP 192.168.0.8

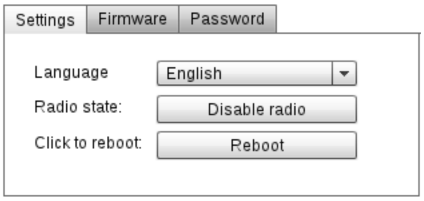
DMZ page

To set up DMZ, click the **Enable** checkbox and put in IP address of your destination in the **Destination IP** text field.

Administration

Administration page allows you to change the language of the WebUI, disable radio connection, reboot the router, save firmware to your computer (in a binary file format) or update it with the newer version. In addition, you can set up a new password for WebUI connection.

Settings



Language English

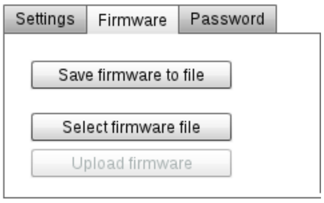
Radio state: Disable radio

Click to reboot: Reboot

Settings page

Language – select a language from the drop down list.
Radio state – disables or enables radio (WiMAX) connection.
Reboot button – click to reboot this device. You will have to wait for a few seconds until it boots up again.

Firmware



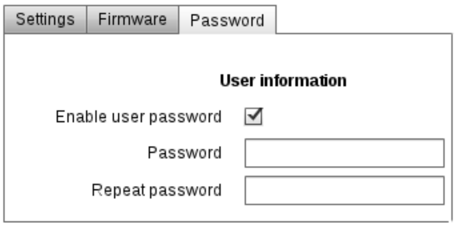
Firmware page

To save firmware: click **Save firmware to file** and at the following dialog browse to the directory you want to place binary file.

To update firmware: click **Select firmware file** and at the following dialog window select firmware file (note: file <u>must</u> be named **firmware.bin**). To start updating click: **Update firmware**. This process usually takes 5 to 10 minutes.

Note: A firmware backup is only suitable for the device from which it was downloaded. If a firmware backup is uploaded to another router, that device will malfunction.

Password



User information

Enable user password ☑

Password

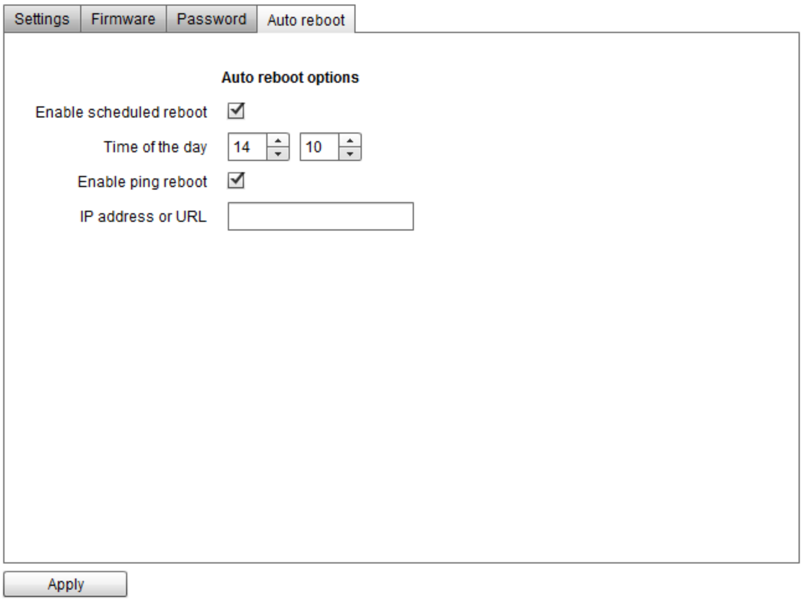
Repeat password

To set up or change a password check **Enable user password** and write a new one into two fields bellow. To disable user password simply uncheck **Enable user password** checkbox. You must click **Apply** if you want to save any of these to configuration.

Note: it is strongly not recommended to disable user password if a router is reachable from Local area network.

Auto Reboot

Auto reboot tab lets you set up scheduled reboot or ping reboot to the URL of your choice.



Auto reboot options

Enable scheduled reboot ☑

Time of the day 14 10

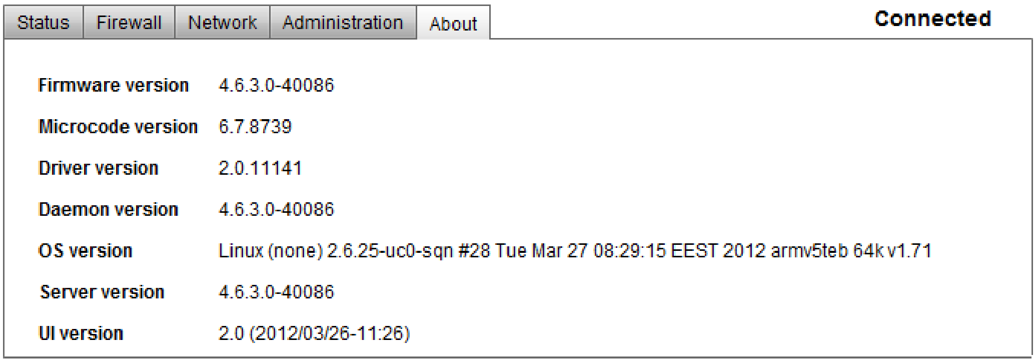
Enable ping reboot ☑

IP address or URL

Auto Reboot form

Enable scheduled reboot – tick to enable scheduled reboot
Time of the day – set the time of the day reboot will begin
Enable ping reboot – tick to enable ping reboot
IP address or URL – ping destination to decide whether to reboot or not

About



Firmware version	4.6.3.0-40086
Microcode version	6.7.8739
Driver version	2.0.11141
Daemon version	4.6.3.0-40086
OS version	Linux (none) 2.6.25-uc0-sqn #28 Tue Mar 27 08:29:15 EEST 2012 armv5teb 64k v1.71
Server version	4.6.3.0-40086
UI version	2.0 (2012/03/26-11:26)

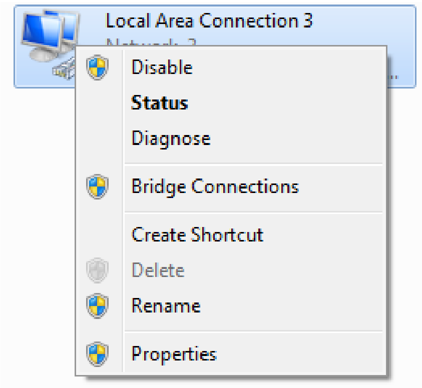
About page

The About page displays the versions of your firmware and software that are currently running on your device. This helps you decide whether or not you need to update your firmware.
Note: The last part in the OS version string refers to the sector size (64 kilobytes in this case) of the flash memory. It is important that the firmware you update is made for the same flash sector size as the flash memory in the device.

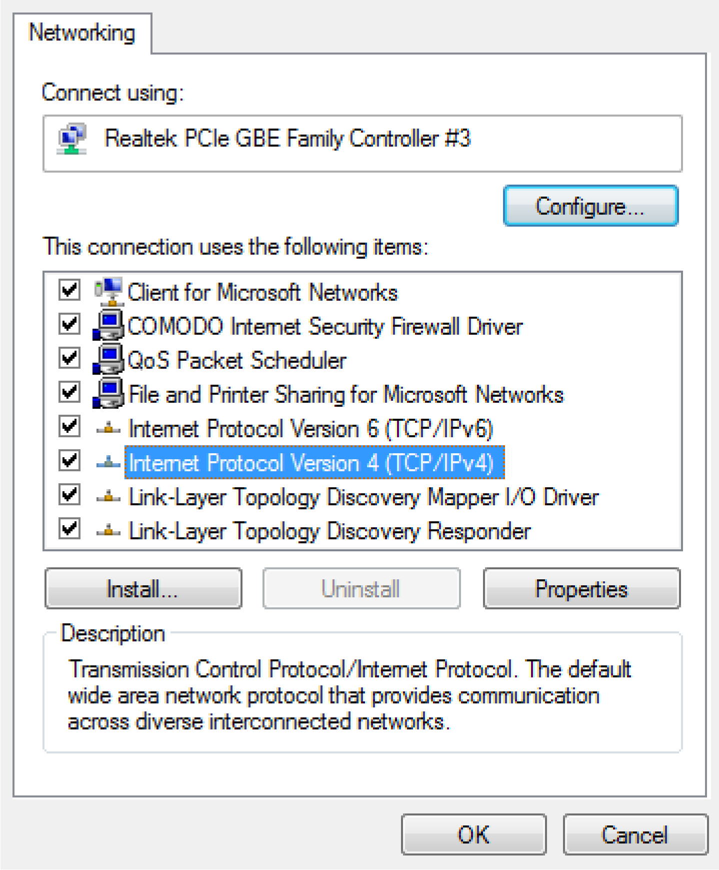
Troubleshooter:

Q: I think my router is not working: can not acquire connection and WebUI is not reachable.
A: Check if IP address is set to obtain automatically via DHCP. Follow these steps:
Windows 7:

- Go to **Control panel -> Network and internet -> Network sharing center -> change adapter settings**.
- Right click on a Local Area Connection which uses RUT4xx for connecting to the internet and click **Properties**.



- Check **Internet Protocol IPv4 (TCP/IP)** and click **Properties**.



Connect using:

Realtek PCIe GBE Family Controller #3

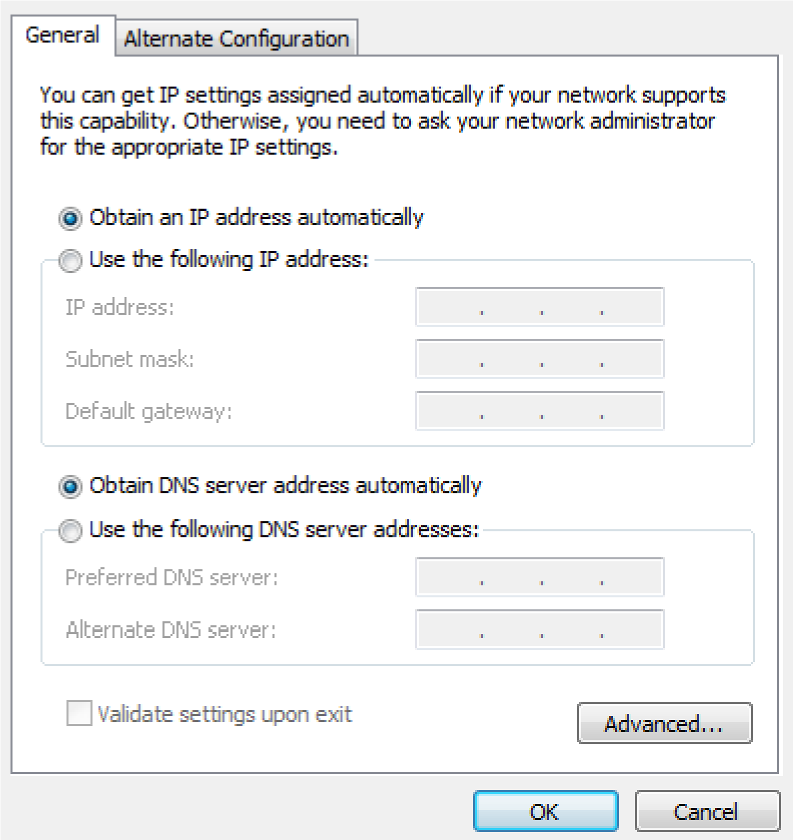
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ COMODO Internet Security Firewall Driver
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

- Make sure that **Obtain IP address automatically** is checked in the **General** settings.



General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

- Click **OK**.

Technical Specifications:

Standard Compliant	IEEE 802.16e-2005
Air Interface	S-OFDMA
Frequency Band	2.3 – 2.4 GHz (RUT423), 2.5 – 2.7 GHz (RUT425), 3.3 – 3.6 GHz (RUT435) or 3.3 – 3.8 GHz (RUT438)
Channel Bandwidth	3 MHz, 3.5 MHz, 5 MHz, 6 MHz, 7 MHz, 8.75 MHz and 10 MHz
Modulation Adaptive	QPSK, 16QAM, 64QAM
MIMO	MRC, Matrix A + MRC, Matrix B
Beamforming	All I/O Beamforming Items
RF Output Power	2x25 dBm @ 2.3 – 2.7GHz; 2x23dBm @ 3.3 – 3.8GHz
RX Sensitivity	RUT435: QPSK1/2: -99 @ 3.5 GHz and 10 MHz BW 16QAM1/2: -93.8 @ 3.5 GHz and 10 MHz BW RUT425: QPSK1/2: -99.5 @ 2.5 GHz and 10 MHz BW 16QAM1/2: -94.29 @ 2.5 GHz and 10 MHz BW
Antenna Gain	Several option available. 2 dBi with standart antenna
Antenna Type	External (2 x RP-SMA connectors)
Handover	Hard / Optimized Handover
QoS Mechanism	UGS, Real-Time-VR, Non Real-Time-VR, Best Effort, ERT-VR
Authentication	EAP-TLS, EAP-TTLS-MSCHAPv2
Encryption	3 CCM-Mode 128-bit AES
Error Handling	HARQ UL and DL, up to Category 7
Throughput	40 Mbps Total DL + UL
LEDs	Power, LAN and WiMAX Activity
LAN	1 x RJ45 10/100 Base-T Ethernet
Reset	Reset button

Electrical, Mechanical & Environmental:

Dimensions (H x W x D)	75mm x 45mm x 23mm
Weight	112g
Power Supply	5VDC
Power Consumption	< 5W
Operating Temperature	0º to 50º C
Storage Temperature	-20º to 70º C
Operating Humidity	10% to 90% Non-condensing
Storage Humidity	5% to 95% Non-condensing