



# USER MANUAL

## RUT240 4G Router



## Legal notice

Copyright © 2017 TELTONIKA Ltd. All rights reserved. Reproduction, transfer, distribution or storage of part or all of the contents in this document in any form without the prior written permission of TELTONIKA Ltd is prohibited. The manufacturer reserves the right to modify the product and manual for the purpose of technical improvement without prior notice.

Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

## 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.



Device is powered by low voltage +9V DC power adapter.



Please do not scratch the device. Scratched device is not fully protected.

# Table of Contents

|  |    |
|--|----|
| Legal notice.....                                | 2  |
| Attention.....                                   | 2  |
| SAFETY INFORMATION.....                          | 7  |
| Device connection.....                           | 8  |
| 1 Introduction.....                              | 9  |
| 2 Specifications.....                            | 9  |
| 2.1 Ethernet.....                                | 9  |
| 2.2 Wi-Fi.....                                   | 9  |
| 2.3 Hardware.....                                | 9  |
| 2.4 Electrical, Mechanical & Environmental.....  | 9  |
| 2.5 Applications.....                            | 10 |
| 3 Setting up your router.....                    | 11 |
| 3.1 Installation.....                            | 11 |
| 3.1.1 Front Panel and Back Panel.....            | 11 |
| 3.1.2 Power connector.....                       | 11 |
| 3.1.3 Connection status LED.....                 | 11 |
| 3.1.4 Hardware installation.....                 | 12 |
| 3.2 Logging in.....                              | 12 |
| 4 Operation Modes.....                           | 16 |
| 5 Powering Options.....                          | 16 |
| 5.1 Powering the device from higher voltage..... | 16 |
| 6 Status.....                                    | 17 |
| 6.1 Overview.....                                | 17 |
| 6.2 System Information.....                      | 18 |
| 6.3 Network Information.....                     | 19 |
| 6.4 Device information.....                      | 30 |
| 6.5 Services.....                                | 31 |
| 6.6 Routes.....                                  | 32 |
| 6.6.1 ARP.....                                   | 32 |
| 6.6.2 Active IP-Routes.....                      | 32 |
| 6.6.3 Active IPv6-Routes.....                    | 32 |
| 6.7 Graphs.....                                  | 34 |
| 6.7.1 Mobile Signal Strength.....                | 34 |
| 6.7.2 Realtime Load.....                         | 35 |

|                                 |    |
|---------------------------------|----|
| 6.7.3 Realtime Traffic.....     | 36 |
| 6.7.4 Realtime Wireless.....    | 37 |
| 6.7.5 Realtime Connections..... | 38 |
| 6.8 Mobile Traffic.....         | 39 |
| 6.9 Events Log.....             | 40 |
| 6.9.1 All Events.....           | 40 |
| 6.9.2 System Events.....        | 40 |
| 6.9.3 Network Events.....       | 40 |
| 7 Network.....                  | 41 |
| 7.1 Mobile.....                 | 41 |
| 7.1.1 General.....              | 41 |
| 7.1.2 Mobile Data Limit.....    | 44 |
| 7.2 WAN.....                    | 46 |
| 7.2.1 Operation Mode.....       | 46 |
| 7.2.2 Common configuration..... | 46 |
| 7.3 LAN.....                    | 53 |
| 7.3.1 Configuration.....        | 53 |
| 7.3.2 DHCP Server.....          | 54 |
| 7.4 Wireless.....               | 58 |
| 7.5 VLAN.....                   | 61 |
| 7.5.1 VLAN Networks.....        | 61 |
| 7.5.2 LAN Networks.....         | 61 |
| 7.6 Firewall.....               | 62 |
| 7.6.1 General Settings.....     | 62 |
| 7.6.2 DMZ.....                  | 63 |
| 7.6.3 Port Forwarding.....      | 63 |
| 7.6.4 Traffic Rules.....        | 65 |
| 7.6.5 Custom Rules.....         | 70 |
| 7.6.6 DDOS Prevention.....      | 70 |
| 7.6.7 Port Scan Prevention..... | 73 |
| 7.7 Routing.....                | 74 |
| 7.7.1 Static Routes.....        | 74 |
| 7.7.2 Dynamic Routes.....       | 75 |
| 8 Services.....                 | 78 |
| 8.1 VRRP.....                   | 78 |

|   |     |
|---|-----|
| 8.1.1 VRRP LAN Configuration Settings.....      | 78  |
| 8.1.2 Check Internet connection.....            | 78  |
| 8.2 Web Filter.....                             | 79  |
| 8.2.1 Site blocking.....                        | 79  |
| 8.2.2 Proxy Based Content Blocker.....          | 79  |
| 8.3 NTP.....                                    | 80  |
| 8.4 VPN.....                                    | 81  |
| 8.4.1 OpenVPN.....                              | 81  |
| 8.4.2 IPSec.....                                | 85  |
| 8.4.3 GRE Tunnel.....                           | 88  |
| 8.4.4 PPTP.....                                 | 90  |
| 8.4.5 L2TP.....                                 | 92  |
| 8.5 Dynamic DNS.....                            | 93  |
| 8.6 SMS Utilities.....                          | 95  |
| 8.6.1 SMS Utilities.....                        | 95  |
| 8.6.2 Call Utilities.....                       | 103 |
| 8.6.3 User Groups.....                          | 104 |
| 8.6.4 SMS Management.....                       | 105 |
| 8.6.5 Remote Configuration.....                 | 107 |
| 8.6.6 Statistics.....                           | 110 |
| 8.7 SNMP.....                                   | 111 |
| 8.7.1 SNMP Settings.....                        | 111 |
| 8.7.2 TRAP Settings.....                        | 112 |
| 8.8 SMS Gateway.....                            | 113 |
| 8.8.1 Post/Get Configuration.....               | 113 |
| 8.8.2 Scheduled Messages.....                   | 115 |
| 8.8.3 Auto Reply Configuration.....             | 115 |
| 8.8.4 SMPP.....                                 | 116 |
| 8.9 Hotspot.....                                | 117 |
| 8.9.1 General settings.....                     | 117 |
| 8.9.2 Internet Access Restriction Settings..... | 119 |
| 8.9.3 Logging.....                              | 119 |
| 8.9.4 Landing Page.....                         | 121 |
| 8.9.5 Radius server configuration.....          | 122 |
| 8.9.6 Statistics.....                           | 123 |

|                              |     |
|------------------------------|-----|
| 8.10 CLI.....                | 124 |
| 8.11 Auto Reboot.....        | 125 |
| 8.11.1 Ping Reboot.....      | 125 |
| 8.11.2 Periodic Reboot.....  | 126 |
| 8.12 Input/Output.....       | 127 |
| 8.12.1 Main information..... | 127 |
| 8.12.2 Status.....           | 127 |
| 8.12.3 Input.....            | 129 |
| 8.12.4 Output.....           | 130 |
| 8.13 QoS.....                | 134 |
| 9 System.....                | 135 |
| 9.1 Setup Wizard.....        | 135 |
| 9.2 Profiles.....            | 137 |
| 9.3 Administration.....      | 137 |
| 9.3.1 General.....           | 137 |
| 9.3.2 Troubleshoot.....      | 138 |
| 9.3.3 Backup.....            | 139 |
| 9.3.4 Diagnostics.....       | 141 |
| 9.3.5 MAC Clone.....         | 142 |
| 9.3.6 Overview.....          | 142 |
| 9.3.7 Monitoring.....        | 143 |
| 9.4 User scripts.....        | 144 |
| 9.5 Firmware.....            | 144 |
| 9.5.1 Firmware.....          | 144 |
| 9.5.2 FOTA.....              | 145 |
| 9.6 Reboot.....              | 146 |
| 10 Device Recovery.....      | 146 |
| 10.1 Reset button.....       | 146 |
| 10.2 Bootloader's WebUI..... | 146 |
| 11 FCC Regulations.....      | 147 |
| 12 Glossary.....             | 148 |

## SAFETY INFORMATION

In this document you will be introduced on how to use a RUT240 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.



The device is intended for supply from a Limited Power Source (LPS) that power consumption should not exceed 15VA and current rating of over current protective device should not exceed 2A.



The highest transient over voltage in the output (secondary circuit) of used PSU shall not exceed 36V peak.



The device can be used with the Personal Computer (first safety class) or Notebook (second safety class). Associated equipment: PSU (power supply unit) (LPS) and personal computer (PC) shall comply with the requirements of standard EN 60950-1.



Do not mount or service the device during a thunderstorm.



To avoid mechanical damages to the device it is recommended to transport it packed in a damage-proof pack.



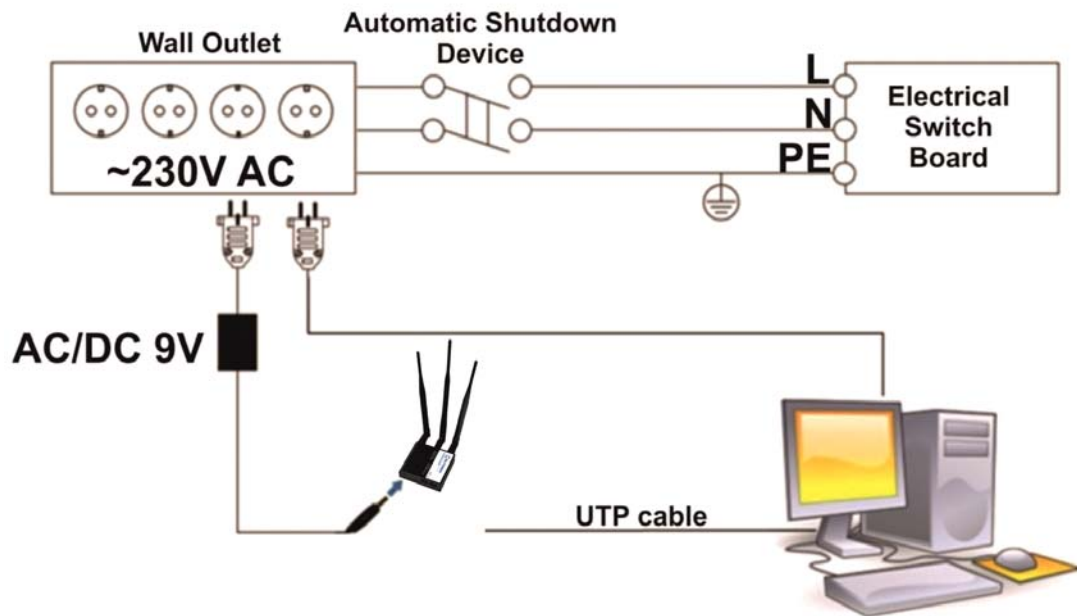
Protection in primary circuits of associated PC and PSU (LPS) against short circuits and earth faults of associated PC shall be provided as part of the building installation.

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 over current, short circuiting and earth faults should be provided as a part of the building installation.

Signal level of the device depends on the environment in which it is working. In case the device starts working insufficiently, please refer to qualified personnel in order to repair this product. We recommend forwarding it to a repair center or the manufacturer. There are no exchangeable parts inside the device.

## Device connection





# 1 Introduction

Thank you for purchasing a RUT240 4G router!

RUT240 is part of the RUT2xx series of compact mobile routers with high speed wireless and Ethernet connections.

This router is ideal for people who would like to share their internet on the go, as it is not restricted by a cumbersome cable connection. Unrestricted, but not forgotten: the router still supports internet distribution via a broadband cable, simply plug it in to the wan port, set the router to a correct mode and you are ready to browse.

# 2 Specifications

## 2.1 Ethernet

- IEEE 802.3, IEEE 802.3u standards
- 1 x LAN 10/100Mbps Ethernet ports
- 1 x WAN 10/100Mbps Ethernet port
- Supports Auto MDI/MDIX

## 2.2 Wi-Fi

- IEEE 802.11b/g/n WiFi standards
- AP and STA modes
- 64/128-bit WEP, WPA, WPA2, WPA&WPA2 encryption methods
- 2.401 – 2.495GHz Wi-Fi frequency range\*
- 20dBm max WiFi TX power
- SSID stealth mode and access control based on MAC address

*\*Supported frequency bands are dependent on geographical location and may not be available in all markets.*

## 2.3 Hardware

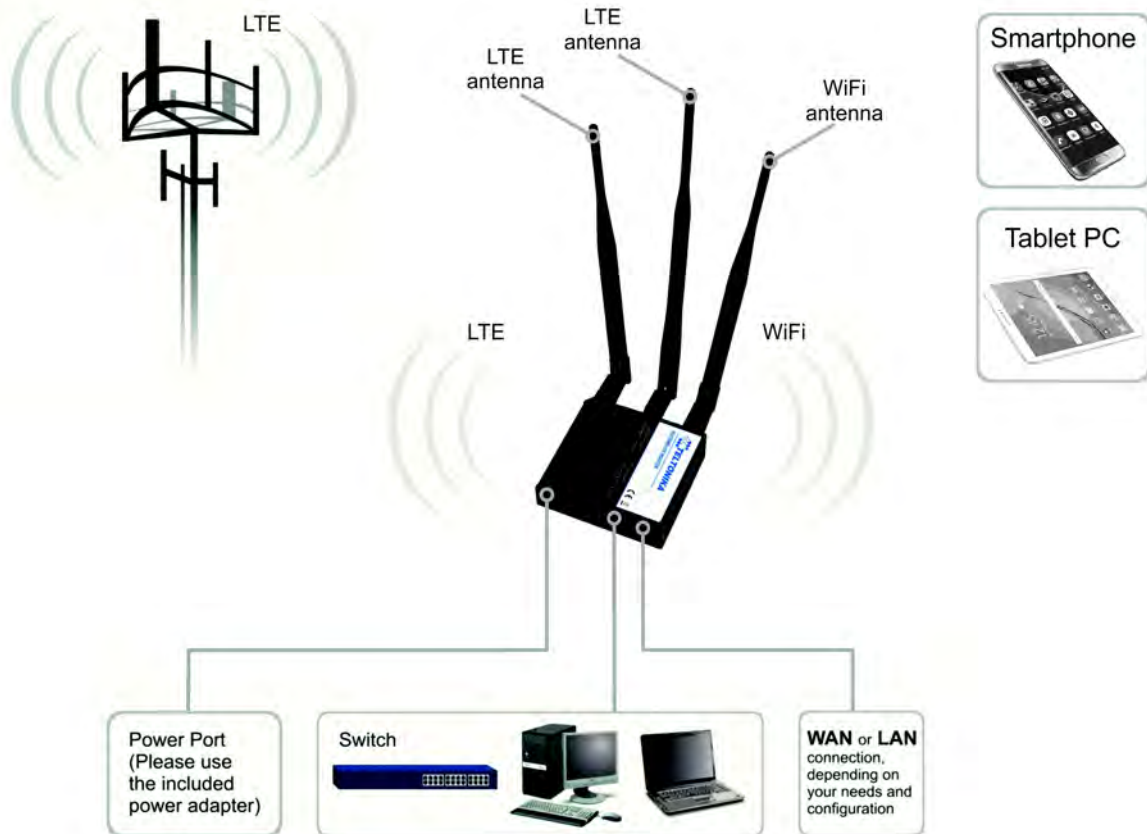
- High performance 400 MHz CPU with 64 Mbytes of DDR2 memory
- External SIM holder
- 4 pin DC connector with 1 x Digital input and 1 x Digital output
- Reset/restore to default button
- 2 x SMA for LTE, 1 x RP-SMA for WiFi antenna connectors
- 2 x Ethernet LEDs, 1 x Power LED
- 5 x signal LEDs, 2 x connection type indication LEDs
- Bottom and sideways DIN rail mounting slits

## 2.4 Electrical, Mechanical & Environmental

- |                          |                                     |
|--------------------------|-------------------------------------|
| • Dimensions (H x W x D) | 83mm x 74mm x 25mm                  |
| • Weight                 | 125g                                |
| • Power supply           | 100 – 240 VAC -> 9 VDC wall adapter |
| • Input voltage range    | 7 – 30VDC                           |
| • Power consumption      | < 5W                                |
| • Operating temperature  | -40° to 75° C                       |
| • Storage temperature    | -45° to 80° C                       |

- Operating humidity 10% to 90% Non-condensing
- Storage humidity 5% to 95% Non-condensing

## 2.5 Applications



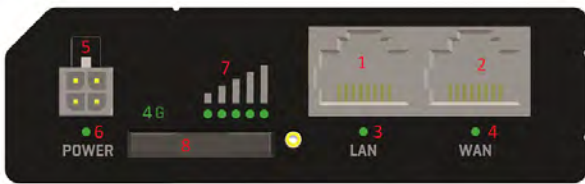
### 3 Setting up your router

#### 3.1 Installation

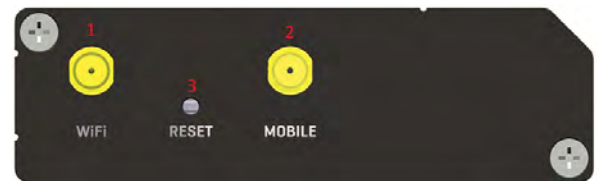
After you unpack the box, follow the steps, documented below, in order to properly connect the device. For better Wi-Fi performance, put the device in clearly visible spot, as obstacles such as walls and door hinder the signal.

1. First assemble your router by attaching the necessary antennas and inserting the SIM card.
2. To power up your router, please use the power adapter included in the box. (IMPORTANT: Using a different power adapter can damage and void the warranty for this product.).
3. If you have a wired broadband connection you will also have to connect it to the WAN port of the router.

##### 3.1.1 Front Panel and Back Panel

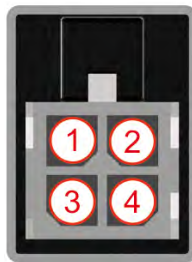


|   |                                 |
|---|---------------------------------|
| 1 | LAN Ethernet ports              |
| 2 | WAN/LAN Ethernet port           |
| 3 | LAN LED                         |
| 4 | WAN LED                         |
| 5 | Power connector                 |
| 6 | Power LED                       |
| 7 | Signal strength indication LEDs |
| 8 | SIM card holder                 |



|   |                            |
|---|----------------------------|
| 1 | Wi-Fi antenna connectors   |
| 2 | LTE main antenna connector |
| 3 | Reset button               |

##### 3.1.2 Power connector



| No. | Description | Wire color |
|-----|-------------|------------|
| 1   | Power       | Red        |
| 2   | Ground      | Black      |
| 3   | Input       | Green      |
| 4   | Output      | White      |

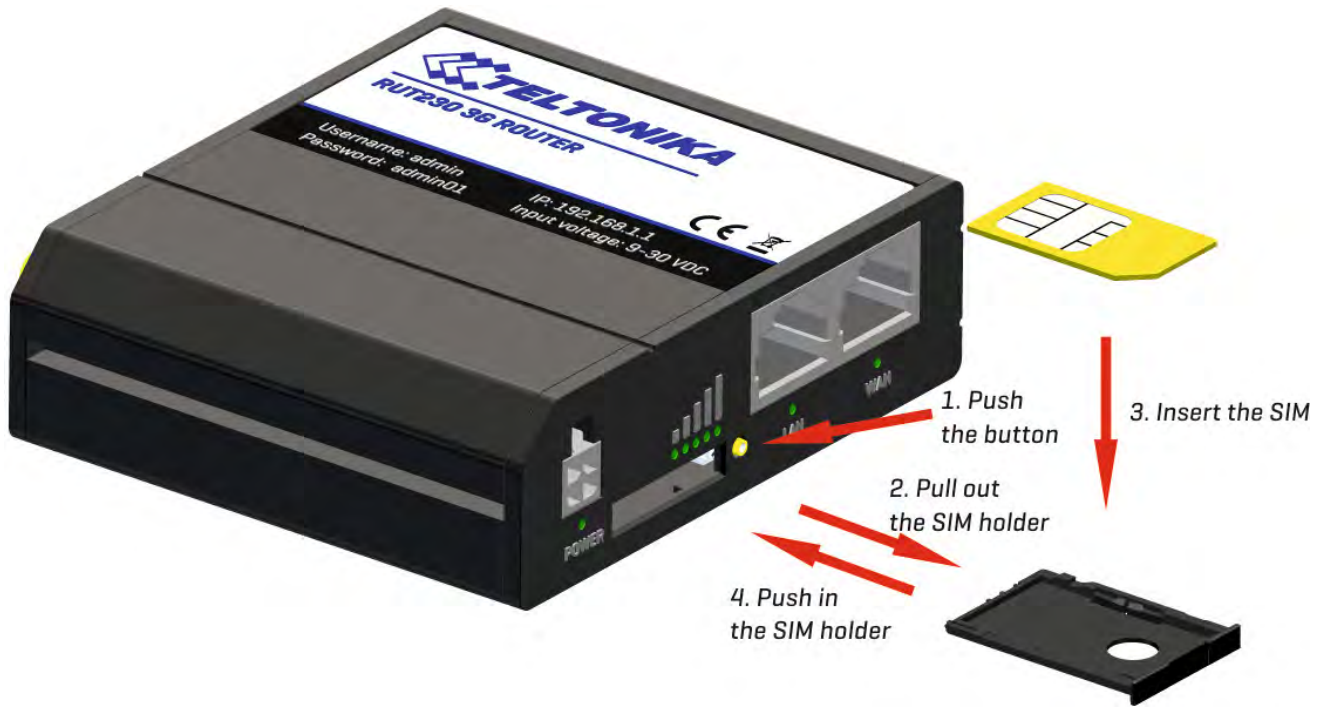
##### 3.1.3 Connection status LED

Explanation of connection status LED indication:

1. Signal strength status LED's turned on: router is turning on;

### 3.1.4 Hardware installation

1. Insert SIM card which was given by your ISP (Internet Service Provider). Correct SIM card orientation is shown in the picture.



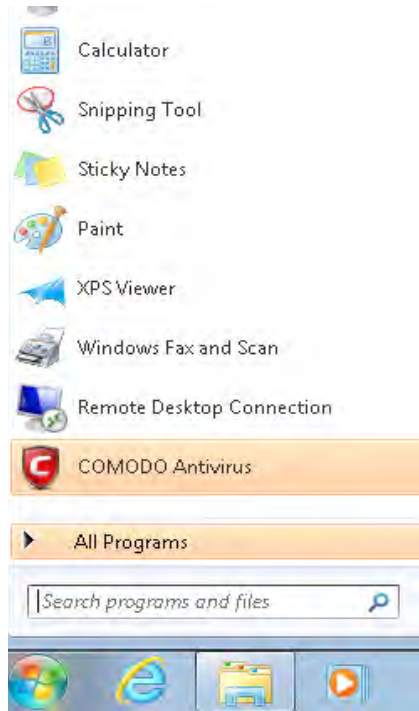
2. Attach 4G and Wi-Fi antennas.
3. Connect the power adapter to the socket on the front panel of the device. Then plug the other end of the power adapter into a wall outlet or power strip.
4. Connect to the device wirelessly (SSID: **Teltonika\_Router**) or use Ethernet cable and plug it into any LAN Ethernet port.

### 3.2 Logging in

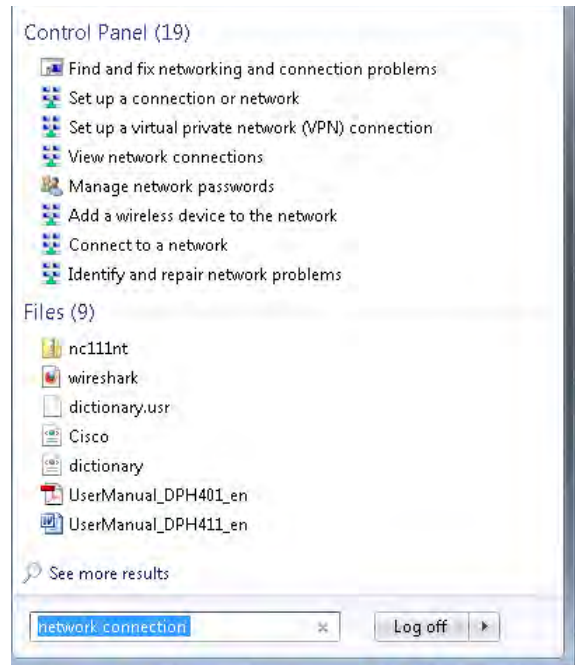
After you're complete with the setting up as described in the section above, you are ready to start logging into your router and start configuring it. This example shows how to connect on Windows 7. On windows Vista: click Start -> Control Panel -> Network and Sharing Center -> Manage network Connections -> (Go to step 4). On Windows XP: Click Start -> Settings -> Network Connections -> (see step 4). You won't see "Internet protocol version 4(TCP/IPv4)", instead you'll have to select "TCP/IP Settings" and click options -> (Go to step 6)

We first must set up our network card so that it could properly communicate with the router.

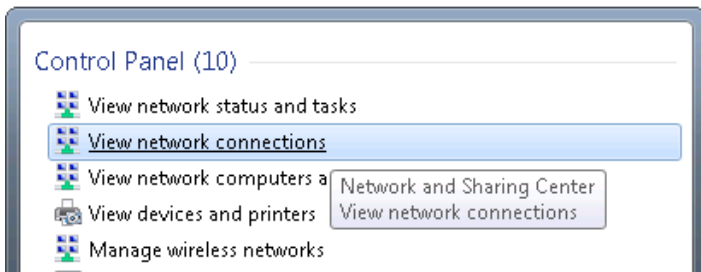
1. Press the start button
2. Type in "network connections", wait for the results to pop up.



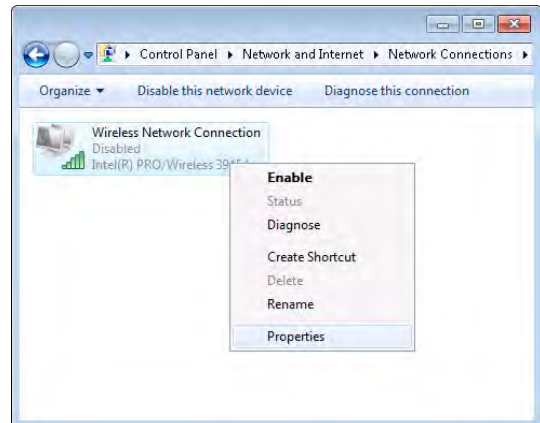
3. Click "View network connections"



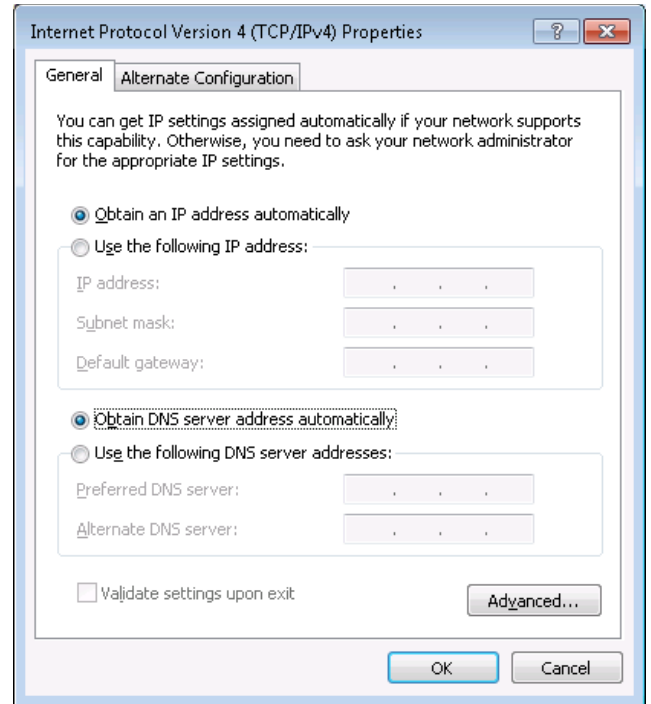
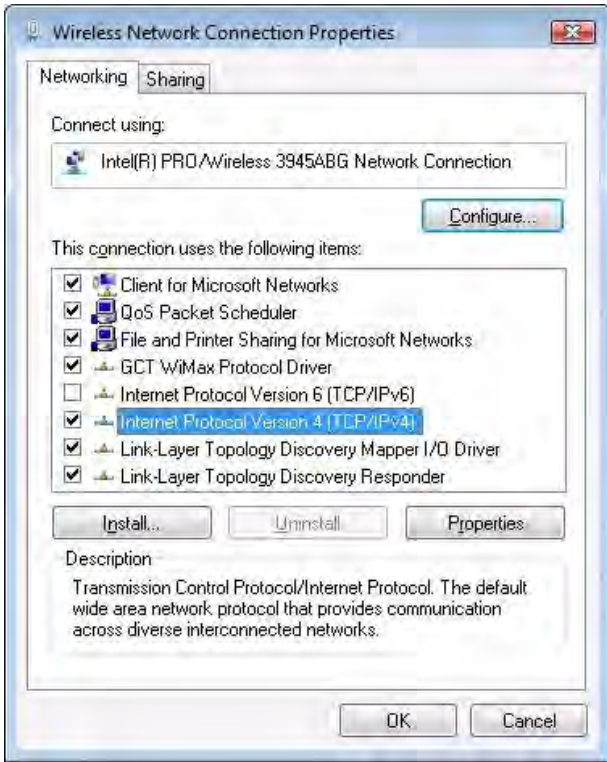
4. Then right click on your wireless device that you use to connect to other access points (It is the one with the name "Wireless Network Connection" and has signal bars on its icon).



5. Select Internet Protocol Version 4 (TCP/IPv4) and then click Properties

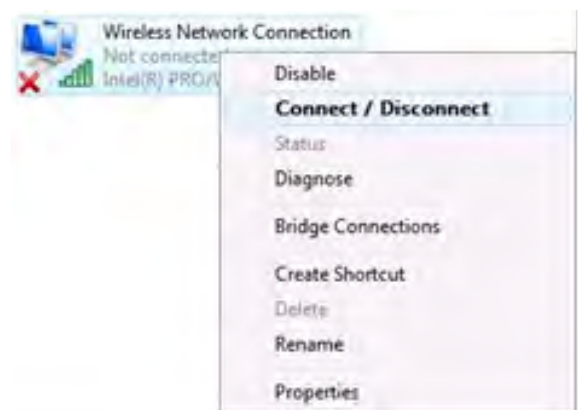
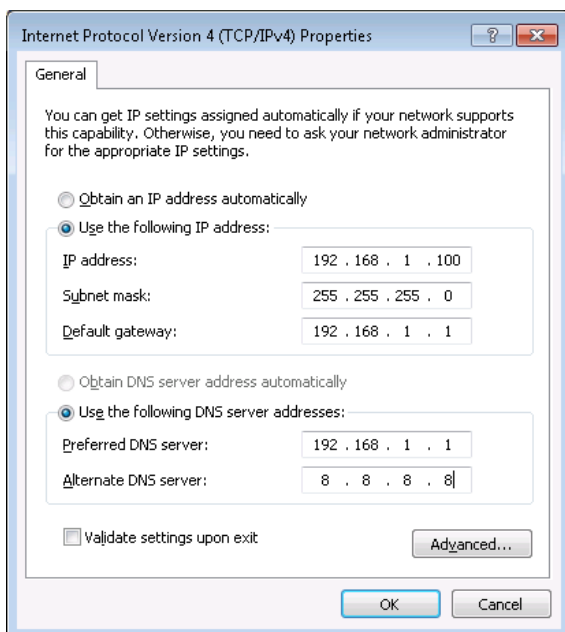


6. By default the router is going to have DHCP enabled, which means that if you select "Obtain an IP address automatically" and "Obtain DNS server address automatically", the router should lease you an IP and you should be ready to login.



7. If you choose to configure manually here's what you have to do:

First select an IP address. Due to the stock settings that your router has arrived in you can only enter an IP in the form of 192.168.1.XXX , where XXX is a number in the range of 2-254 (192.168.1.2 , 192.168.1.254 , 192.168.1.155 and so on... are valid; 192.168.1.0 , 192.168.1.1 , 192.168.1.255 , 192.168.1.699 and so on... are not). Next we enter the subnet mask: this has to be "255.255.255.0". Then we enter the default gateway: this has to be "192.168.1.1". Finally we enter primary and secondary DNS server IP's. One will suffice, though it is good to have a secondary one as well as it will act as a backup if the first should fail. The DNS can be your routers IP (192.168.1.1), but it can also be some external DNS server (like the one Google provides: 8.8.8.8).

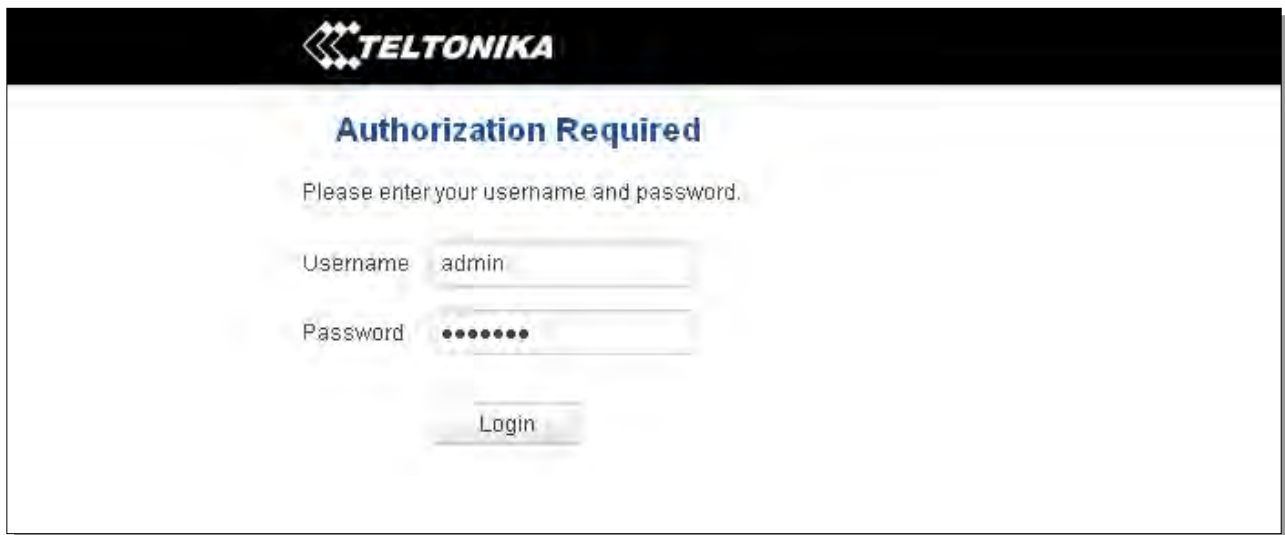




Right click on the Wireless network icon and select **Connect / Disconnect**. A list should pop up with all available wireless networks. Select “Teltonika” and click **connect**. Then we launch our favorite browser and enter the router’s IP into the address field:



Press enter. If there are no problems you should be greeted with a login screen such as this:



Enter the default password, which is “admin01” into the “Password” field and then either click Login with your mouse or press the Enter key. You have now successfully logged into the RUT240!

From here on out you can configure almost any aspect of your router.

## 4 Operation Modes

The RUT2xx series router supports various operation modes. It can be connected to the internet (WAN) via mobile, standard Ethernet cable or via a wireless network. When connecting to the internet, you may also backup your main WAN connection with one or two backup connections. Any interface can act like backup if configured so. At first router uses its main WAN connection, if it is lost then router tries to connect via backup with higher priority and if that fails too, router tries the second backup option.

| Mobile   | √ | √ | x |
|----------|---|---|---|
| Ethernet | √ | √ | √ |
| Wi-Fi    | √ | √ | √ |

In later sections it will be explained, in detail, how to configure your router to work in a desired mode.

## 5 Powering Options

The RUT2xx router can be powered from power socket

### 5.1 Powering the device from higher voltage

If you decide not to use our standard 9 VDC wall adapters and want to power the device from higher voltage (15 – 30 VDC), please make sure that you choose a power supply of high quality. Some power supplies can produce voltage peaks significantly higher than the declared output voltage, especially during connection.

While the device is designed to accept input voltage of up to 30 VDC, peaks from high voltage power supplies can harm the device. If you want to use high voltage power supplies it is recommended to also use additional safety equipment to suppress voltage peaks from the power supply.



## 6 Status

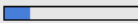

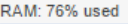
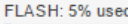
The status section contains various pieces of information, like current IP addresses of various network interfaces; the state of the routers memory; firmware version; DHCP leases; associated wireless stations; graphs indicating load, traffic and much more.



### 6.1 Overview

Overview section contains various information summaries.

**TELTONIKA** Status Network Services System Logout

### Overview

|                   |  |                       |   |
|-------------------|--|-----------------------|---|
| <b>System</b> ⓘ ⓘ |  19.0% CPU load   | <b>Mobile</b> ⓘ ⓘ     | -75 dBm  |
| Router uptime     | 0d 0h 53m 57s (since 2017-04-12, 13:41:36)   | Data connection       | Disconnected  |
| Local device time | 2017-04-12, 14:35:33   | State                 | Registered (home); LT BITE GSM; 3G (HSDPA+HSUPA)  |
| Memory usage      | RAM: 76% used  FLASH: 5% used  | SIM card status       | SIM (Ready)   |
| Firmware version  | RUT2XX_T_00.00.136   | Bytes received/sent * | 0 B / 0 B   |

|                     |  |                   |   |
|---------------------|--|-------------------|---|
| <b>Wireless</b> ⓘ ⓘ | ON  | <b>WAN</b> ⓘ ⓘ    | Wired  |
| SSID                | HAL9000 (AP)   | IP address        | 192.168.1.202   |
| Mode                | 1- AP; 11 CH (2.462 GHz)   | Backup WAN status | Backup link is disabled   |

|                          |                               |                           |                  |
|--------------------------|-------------------------------|---------------------------|------------------|
| <b>Local Network</b> ⓘ ⓘ |                               | <b>Access Control</b> ⓘ ⓘ |                  |
| IP / netmask             | 192.168.200.1 / 255.255.255.0 | LAN                       | SSH; HTTP; HTTPS |
| Clients connected        | 2                             | WAN                       | No access        |

|  |  |  |  |
|--|--|--|--|
| <b>Recent System Events</b> ⓘ ⓘ                                      |  | <b>Recent Network Events</b> ⓘ ⓘ                                     |  |
| 1 2017-04-12 14:23:50 - DHCP: Leased 192.168.200.157 IP address ...  |  | 1 2017-04-12 14:23:53 - WiFi client connected: C0:11:73:94:E8:E5 ... |  |
| 2 2017-04-12 14:13:40 - Web UI: Authentication was succesful fro ... |  | 2 2017-04-12 14:22:51 - WiFi client disconnected: C0:11:73:94:E8 ... |  |
| 3 2017-04-12 14:04:06 - DHCP: Leased 192.168.200.124 IP address ...  |  | 3 2017-04-12 14:06:18 - Connected to LT BITE GSM operator            |  |
| 4 2017-04-12 14:04:00 - DHCP: Leased 192.168.200.157 IP address ...  |  | 4 2017-04-04 09:55:27 - WiFi client connected: C0:11:73:94:E8:E5 ... |  |

\* Your carrier's data usage accounting may differ. Teltonika is not liable should any accounting discrepancies occur.

Teltonika solutions www.teltonika.it

## 6.2 System Information

The System Information tab contains data that pertains to the routers operating system.

### System Information

| System             |  |
|--------------------|--|
| Router name        | RUT240                                     |
| Host name          | Teltonika-RUT240.com                       |
| Router model       | Teltonika RUT240 LTE                       |
| Firmware version   | RUT2XX_R_00.00.20                          |
| Kernel version     | 3.18.44                                    |
| Bootloader version | 2.0.0                                      |
| Local device time  | 2017-05-02, 09:25:05                       |
| Uptime             | 0d 1h 54m 51s (since 2017-05-02, 07:30:14) |
| Load average       | 1 min: 39%; 5 mins: 92%; 15 mins: 90%      |
| Temperature        | 44° C                                      |

| Memory   |                           |
|----------|---------------------------|
| Free     | 17440 kB / 61016 kB (28%) |
| Cached   | 14900 kB / 61016 kB (24%) |
| Buffered | 5884 kB / 61016 kB (9%)   |

### System explanation:

|    | Field Name       | Sample value                               | Explanation   |
|----|------------------|--|---|
| 1. | Router Name      | RUT240                                     | Name of the router (hostname of the router's system). Can be changed in System -> Administration.   |
| 2. | Host name        | Teltonika-RUT240.com                       | Indicates how the router will be seen by other devices on the network. Can be changed in System -> Administration.  |
| 3. | Router Model     | Teltonika RUT240 LTE                       | Router's model.   |
| 4. | Firmware Version | RUT2XX_T_00.00.20                          | Shows the version of the firmware that is currently loaded in the router. Newer versions might become available as new features are added. Use this field to decide whether you need a firmware upgrade or not.   |
| 5. | Kernel Version   | 3.18.44                                    | The version of the Linux kernel that is currently running on the router.  |
| 6. | Local Time       | 2017-04-12, 14:41:18                       | Shows the current system time. Might differ from your computer, because the router synchronizes its time with an NTP server. Format [year-month-day, hours: minutes: seconds].  |
| 7. | Uptime           | 0d 0h 59m 42s (since 2017-04-12, 13:41:36) | Indicates how long it has been since the router booted up. Reboots will reset this timer to 0. Format [days hours minutes seconds (since year-month-day, hours: minutes: seconds)].   |
| 8. | Load Average     | 1 min: 5%; 5 mins: 72%; 15 mins: 76%       | Indicates how busy the router is. Let's examine some sample output: "1 min: 5%, 5 mins: 72%, 15 mins: 76%". The first number means past minute and the second number 5 means that in the past minute there have been, on average, 5% processes running or waiting for a resource. |
| 9. | Temperature      | 40° C                                      | Device's temperature  |

### Memory explanation:

|    | Field Name | Sample Value              | Explanation   |
|----|------------|---------------------------|---|
| 1. | Free       | 14924 kB / 61020 kB (24%) | The amount of memory that is completely free. Should this rapidly decrease or get close to 0, it would indicate that the router is running out of memory, which could cause crashes and unexpected reboots. |
| 2. | Cached     | 16992 kB / 61020 kB (27%) | The size of the area of memory that is dedicated to storing frequently accessed data.   |
| 3. | Buffered   | 6740 kB / 61020 kB (11%)  | The size of the area in which data is temporarily stored before moving it to another location.  |

## 6.3 Network Information

### 6.3.1.1 Mobile

Displays information about mobile modem connections.

- Mobile
- WAN
- LAN
- Wireless
- OpenVPN
- VRRP
- Access

### Mobile Information

| Mobile                |                       |
|-----------------------|-----------------------|
| Data connection state | Connected             |
| IMEI                  | 861075024498503       |
| IMSI                  | 246020100944448       |
| ICCID                 | 8937002160600414481F  |
| Sim card state        | Ready                 |
| Signal strength       | -69 dBm               |
| Cell ID               | 6900156               |
| RSCP                  | N/A                   |
| Ec/fo                 | N/A                   |
| Operator              | LT BITE GSM           |
| Operator state        | Registered (home)     |
| Connection type       | 3G (HSDPA+HSUPA)      |
| Bytes received *      | 58.1 KB (59466 bytes) |
| Bytes sent *          | 47.8 KB (48938 bytes) |

- Reboot modem
- Restart connection
- (Re)register
- Refresh

\*Your carrier's data usage accounting may differ. Teltonika is not liable should any accounting discrepancies occur.

### Mobile information:

|     | Item Name             | Sample Value          | Explanation  |
|-----|-----------------------|-----------------------|--|
| 1.  | Data connection state | Connected             | Mobile data connection status  |
| 2.  | IMEI                  | 861075024498503       | Modem's IMEI (International Mobile Equipment Identity) number                                      |
| 3.  | IMSI                  | 246020100944448       | IMSI (International Mobile Subscriber Identity) is used to identify the user in a cellular network |
| 4.  | ICCID                 | 8937002160600414481F  | Your SIM card's Integrated circuit card identifier number  |
| 5.  | SIM card state        | Ready                 | Indicates the SIM card's state, e.g. PIN required, Not inserted, etc.                              |
| 6.  | Signal strength       | -69 dBm               | Received Signal Strength Indicator (RSSI). Signal's strength measured in dBm                       |
| 7.  | Cell ID               | 6900156               | ID of operator cell that device is currently connected to  |
| 8.  | RSCP                  | N/A                   | Indicates the Reference Signal Received Power  |
| 9.  | Ec/Io                 | N/A                   | Indicates the Reference Signal Received Quality  |
| 10. | Operator              | LT BITE GSM           | Operator's name of the connected GSM network   |
| 11. | Operator state        | Registered (home)     | GSM network's status   |
| 12. | Connection type       | LTE                   | Indicates the GSM network's access technology  |
| 13. | Bytes received        | 58.1 KB (59466 bytes) | How many bytes were received via mobile data connection  |
| 14. | Bytes sent            | 47.8 KB (48939 bytes) | How many bytes were sent via mobile data connection  |

### 6.3.1.2 WAN

Displays information about WAN connection.

The screenshot shows the Teltonika web interface. At the top, there is a navigation bar with the Teltonika logo and menu items: Status, Network, Services, System, and Logout. Below the navigation bar, there are tabs for Mobile, WAN, LAN, Wireless, OpenVPN, VRRP, and Access. The 'WAN' tab is selected, and the 'WAN Information' section is displayed. This section shows the following details:

- Interface: Wired
- Type: DHCP
- IP address: 192.168.1.202
- WAN MAC: 00:1E:42:00:02:1E
- Netmask: 255.255.255.0
- Gateway: 192.168.1.1
- DNS 1: 192.168.1.1
- Connected: 0h 1m 5s

Below the WAN information, there is a 'Ports' section with an image of the device's physical ports, including Power, LAN, and WAN ports.

**WAN information:**

|    | Item Name  | Value             | Description  |
|----|------------|-------------------|--|
| 1. | Interface  | Wired             | Specifies through what medium the router is connecting to the internet. This can either be Wired, Mobile or Wi-Fi. |
| 2. | Type       | DHCP              | Specifies the type of connection. This can either be static or DHCP.   |
| 3. | IP address | 192.168.1.202     | The IP address that the router uses to connect to the internet.  |
| 4. | WAN MAC    | 00:1E:42:00:02:1E | MAC (Media Access Control) address used for communication in an Ethernet WAN (Wide Area Network)                   |
| 5. | Netmask    | 255.255.255.0     | Specifies a mask used to define how large the WAN network is   |
| 6. | Gateway    | 192.168.1.1       | Indicates the default gateway, an address where traffic destined for the internet is routed to.                    |
| 7. | DNS 1      | 192.168.1.1       | Domain name server(s).   |
| 8. | Connected  | 0h 1m 5s          | How long the connection has been successfully maintained.  |

**6.3.1.3 LAN**

Displays information about LAN connections.

The screenshot shows the Teltonika web management interface. At the top, there is a navigation bar with 'Status', 'Network', 'Services', and 'System' menus, and a 'Logout' button. Below this is a sub-menu with 'Mobile', 'WAN', 'LAN', 'Wireless', 'OpenVPN', 'VRRP', and 'Access'. The 'LAN' menu is selected, displaying 'LAN Information'.

**LAN Information**

| Name | IP address    | Netmask       | Ethernet MAC address | Connected for |
|------|---------------|---------------|----------------------|---------------|
| Lan  | 192.168.200.1 | 255.255.255.0 | 00:1E:42:00:02:1D    | 1h 37m 25s    |

**DHCP Leases**

| Hostname                 | IP address      | LAN name | MAC address       | Lease time remaining |
|--------------------------|-----------------|----------|-------------------|----------------------|
| DESKTOP-69EIUGN          | 192.168.200.124 | Lan      | 18:66:DA:28:6A:34 | 11h 52m 58s          |
| android-2450c1993f706ced | 192.168.200.157 | Lan      | C0:11:73:94:E8:E5 | 11h 4m 1s            |

**Ports**

Below the 'Ports' section, there is an image of a Teltonika device with a red 'X' over the LAN port indicator, suggesting a connection issue. A 'Refresh' button is located at the bottom right of the interface.

### LAN information:

|    | Field Name           | Sample Value      | Description   |
|----|----------------------|-------------------|---|
| 1. | Name                 | Lan               | LAN instance name   |
| 2. | IP address           | 192.168.200.1     | Address that the router uses on the LAN network.  |
| 3. | Netmask              | 255.255.255.0     | A mask used to define how large the LAN network is  |
| 4. | Ethernet MAC address | 00:1E:42:00:02:1D | MAC (Media Access Control) address used for communication in an Ethernet LAN (Local Area Network) |
| 5. | Connected for        | 1h 37m 25s        | How long the LAN has been successfully maintained.  |

### DHCP Leases

If you have enabled a DHCP server this field will show how many devices have received an IP address and what those IP addresses are.

|    | Field Name           | Sample Value      | Description   |
|----|----------------------|-------------------|---|
| 1. | Hostname             | DESKTOP69-EIUGN   | DHCP client's hostname  |
| 2. | IP address           | 192.168.200.124   | Each lease declaration includes a single IP address that has been leased to the client  |
| 3. | LAN name             | Lan               | LAN instance name   |
| 4. | MAC address          | 18:66:DA:28:6A:34 | The MAC (Media Access Control) address of the network interface on which the lease will be used. MAC is specified as a series of hexadecimal octets separated by colons |
| 5. | Lease time remaining | 11h 52m 58s       | Remaining lease time for addresses handed out to clients  |

### 6.3.1.4 Wireless

Wireless can work in two modes, Access Point (AP) or Station (STA). AP is when the wireless radio is used to create an Access Point that other devices can connect to. STA is when the radio is used to connect to an Access Point via WAN.

### 6.3.1.4.1 Station

The screenshot shows the Teltonika web interface with the following structure:

- Navigation Bar:** TELTONIKA logo, Status, Network, Services, System, Logout.
- Sub-Menu:** Mobile, WAN, LAN, **Wireless**, OpenVPN, VRRP, Access.
- Section: Wireless Information**
  - Channel: 1 (2.41 GHz)
  - Country code: 00 (World)
- Section: Wireless Status**

| SSID             | Mode              | Encryption                | Wireless MAC      | Signal quality | Bit rate    |
|------------------|-------------------|---------------------------|-------------------|----------------|-------------|
| GG               | Station (STA)     | WPA2 PSK (CCMP)           | C0:11:73:94:E8:E5 | 100%           | 39.0 MBit/s |
| Teltonika_Router | Access Point (AP) | mixed WPA/WPA2 PSK (CCMP) | 02:1E:42:00:02:1F | 0%             | N/A         |
- Section: Associated Stations**

| MAC address       | Device name              | Signal  | RX rate                   | TX rate                   |
|-------------------|--------------------------|---------|---------------------------|---------------------------|
| C0:11:73:94:E8:E5 | android-2450c1993f706ced | -30 dBm | 58.5 Mbit/s, MCS 6, 20MHz | 39.0 Mbit/s, MCS 4, 20MHz |
- Refresh Button:** Refresh

Display information about wireless connection (Station mode).

#### Client mode information

| No. | Parameter      | Value             | Description  |
|-----|----------------|-------------------|--|
| 1.  | Channel        | 1 (2.41 GHz)      | The channel that the AP, to which the router is connected to, uses. Your wireless radio is forced to work in this channel in order to maintain the connection.   |
| 2.  | Country code   | 00 (World)        | Country code.  |
| 3.  | SSID           | GG                | The SSID that the AP, to which the router is connected to, uses.   |
| 4.  | Mode           | Station (STA)     | Connection mode - Station (STA) indicates that the router is a client to some local AP.  |
| 5.  | Encryption     | WPA2 PSK (CCMP)   | The AP, to which the router is connected to, dictates the type of encryption.  |
| 6.  | Wireless MAC   | C0:11:73:94:E8:E5 | The MAC address of the access points radio.  |
| 7.  | Signal Quality | 100%              | The quality between routers radio and some other device that is connecting to the router. Will show 0% if no devices are trying to connect or are currently maintaining a connection.  |
| 8.  | Bit rate       | 39.0 MBit/s       | The physical maximum possible throughput that the routers radio can handle. Keep in mind that this value is cumulative - The bit rate will be shared between the router and other possible devices that connect to the local AP. |



### 6.3.1.4.2 Access Point

Display information about wireless connection (Access Point mode).

The screenshot shows the Teltonika web interface with the 'Wireless' tab selected. The 'Wireless Information' section displays the following details:

- Channel: 1 (2.41 GHz)
- Country code: 00 (World)

The 'Wireless Status' section shows the following configuration:

| SSID        | Mode              | Encryption                | Wireless MAC      | Signal quality | Bit rate    |
|-------------|-------------------|---------------------------|-------------------|----------------|-------------|
| RUT200_test | Access Point (AP) | mixed WPA/WPA2 PSK (CCMP) | 00:1E:42:00:02:1F | 100%           | 52.0 MBit/s |

The 'Associated Stations' section shows the following information:

| MAC address       | Device name              | Signal  | RX rate                   | TX rate                   |
|-------------------|--------------------------|---------|---------------------------|---------------------------|
| C0:11:73:94:E8:E5 | android-2450c1993f706ced | -42 dBm | 72.2 Mbit/s, MCS 7, 20MHz | 52.0 Mbit/s, MCS 5, 20MHz |

A 'Refresh' button is located at the bottom right of the interface.

#### Wireless AP information

| No. | Parameter      | Sample Value              | Description   |
|-----|----------------|---------------------------|---|
| 1.  | Channel        | 1 (2.41 GHz)              | The channel which is used to broadcast the SSID and to establish new connections to devices.  |
| 2.  | Country code   | 00(World)                 | Country code.   |
| 3.  | SSID           | RUT200_test               | The SSID that is being broadcast. Other devices will see this and will be able to use to connect to your wireless network.  |
| 4.  | Mode           | Access Point (AP)         | Connection mode – Access Point (AP) indicates that your router is an access point.  |
| 5.  | Encryption     | Mixed WPA/WPA2 PSK (CCMP) | The type of encryption that the router will use to authenticate, establish and maintain a connection.   |
| 6.  | Wireless MAC   | 00:1E:42:00:02:1F         | MAC address of your wireless radio.   |
| 7.  | Signal Quality | 000%                      | The quality between routers radio and some other device that is connecting to the router. Will show 0% if no devices are trying to connect or are currently maintaining a connection. |
| 8.  | Bit rate       | 52.0 Mbit/s               | The bit rate will be shared between all devices that connect to the routers wireless network.   |

Additional note: MBit/s indicates the bits not bytes. To get the throughput in bytes divide the bit value by 8, for e.g. 54MBit/s would be 6.75MB/s (Mega Bytes per second).

### 6.3.1.5 Associated Stations

Outputs a list of all devices and their MAC addresses that are maintain a connection with your router right now.

This can either be the information of the Access Point that the router is connecting to in STA mode or a list of all devices that are connecting to the router in AP mode:

|    | Field Name  | Sample Value             | Explanation  |
|----|-------------|--------------------------|--|
| 1. | MAC Address | C0:11:73:94:E8:E5        | Associated station's MAC (Media Access Control) address                      |
| 2. | Device Name | android-2450c1993f706ced | DHCP client's hostname   |
| 3. | Signal      | -42dBm                   | Received Signal Strength Indicator (RSSI). Signal's strength measured in dBm |
| 4. | RX Rate     | 72.2Mbit/s, MCS 7, 20MHz | The rate at which packets are received from associated station               |
| 5. | TX Rate     | 52.0Mbit/s, MCS 5, 20MHz | The rate at which packets are sent to associated station                     |

### 6.3.1.6 OpenVPN Client

Displays OpenVPN connection information on client side.

| Mobile                     | WAN | LAN | Wireless | OpenVPN         | VRRP | Topology | Access |
|----------------------------|-----|-----|----------|-----------------|------|----------|--------|
| <b>OpenVPN Information</b> |     |     |          |                 |      |          |        |
| Client_Client              |     |     |          |                 |      |          |        |
| <b>OpenVPN</b>             |     |     |          |                 |      |          |        |
| Enabled                    |     |     |          | Yes             |      |          |        |
| Status                     |     |     |          | Connected       |      |          |        |
| Type                       |     |     |          | Client          |      |          |        |
| IP                         |     |     |          | 10.0.0.2        |      |          |        |
| Mask                       |     |     |          | 255.255.255.255 |      |          |        |
| Time                       |     |     |          | 0h 0m 13s       |      |          |        |

|    | Field Name | Sample Value    | Explanation                                      |
|----|------------|-----------------|--|
| 1. | Enabled    | Yes/No          | OpenVPN status                                   |
| 2. | Status     | Connected       | Connection status                                |
| 3. | Type       | Client          | A type of OpenVPN instance that has been created |
| 4. | IP         | 10.0.0.2        | Remote virtual network's IP address              |
| 5. | Mask       | 255.255.255.255 | Remote virtual network's subnet mask             |
| 6. | Time       | 0h 0m 13s       | For how long the connection has been established |

### 6.3.1.7 OpenVPN Server

Display OpenVPN connection information on server side.

| Mobile                     | WAN | LAN                 | Wireless | OpenVPN                | VRRP | Topology  | Access |
|----------------------------|-----|---------------------|----------|------------------------|------|---|--------|
| <b>OpenVPN Information</b> |     |                     |          |                        |      |   |        |
| Server_Server              |     |                     |          |                        |      |   |        |
| <b>OpenVPN</b>             |     |                     |          |                        |      |   |        |
| Enabled                    |     | Yes                 |          |                        |      |   |        |
| Status                     |     | Connected           |          |                        |      |   |        |
| Type                       |     | Server              |          |                        |      |   |        |
| IP                         |     | 10.0.0.1            |          |                        |      |   |        |
| Mask                       |     | 255.255.255.255     |          |                        |      |   |        |
| Time                       |     | 0h 6m 31s           |          |                        |      |   |        |
| <b>Clients Information</b> |     |                     |          |                        |      |   |        |
| <b>Common Name</b>         |     | <b>Real Address</b> |          | <b>Virtual Address</b> |      | <b>Connection Since</b>                               |        |
| Test001                    |     | 212.59.13.226:52638 |          | 10.0.0.6               |      | Thu May 05 2016 07:46:29 GMT+0300 (FLE Standard Time) |        |

|    | Item Name | Sample Value    | Description                                      |
|----|-----------|-----------------|--|
| 1. | Enabled   | Yes/No          | OpenVPN status                                   |
| 2. | Status    | Connected       | Connection status                                |
| 2. | Type      | Server          | A type of OpenVPN instance that has been created |
| 3. | IP        | 10.0.0.1        | Remote virtual network's IP address              |
| 4. | Mask      | 255.255.255.255 | Remote virtual network's subnet mask             |
| 5. | Time      | 0h 6m 31s       | How long the connection has been established     |

### 6.3.1.8 Clients information

It will show information, when router is configured as OpenVPN TLS server.

|    | Item Name        | Sample Value  | Description   |
|----|------------------|---|---|
| 1. | Common Name      | Test001   | OpenVPN client's name                               |
| 2. | Real Address     | 212.59.13.226:52638                                     | Client's IP address and port number                 |
| 3. | Virtual Address  | 10.0.0.6  | The virtual address that has been given to a client |
| 4. | Connection Since | Thu May 05 2016 07:46:29 GMT + 0300 (FLE Standard Time) | Since when the connection has been established      |

### 6.3.1.9 VRRP

VRRP (Virtual Router Redundancy Protocol) for LAN

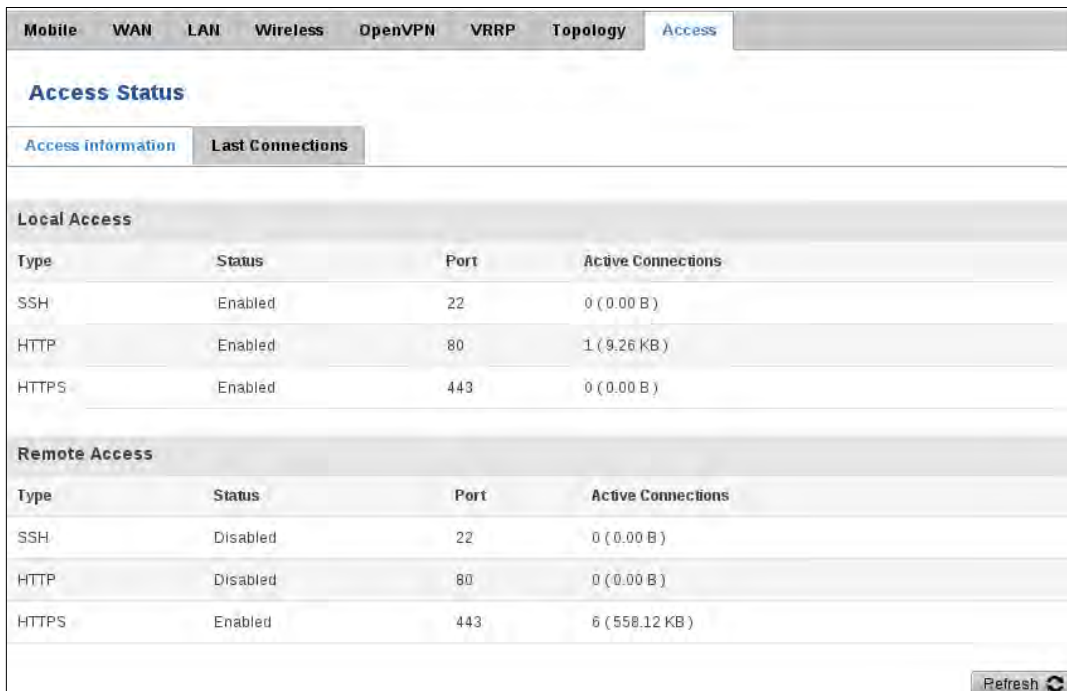


|    | Field Name | Value         | Description   |
|----|------------|---------------|---|
| 1. | Status     | Enabled       | VRRP status   |
| 2. | Virtual IP | 192.168.1.253 | Virtual IP address(-es) for LAN's VRRP (Virtual Router Redundancy Protocol) cluster                   |
| 3. | Priority   | 100           | Router with the highest priority value on the same VRRP cluster will act as a master, range [1 - 255] |
| 4. | Router**   | Master        | Connection mode - Master  |

\*\*-Exclusive to other Modes with Slave.

### 6.3.1.10 Access

Display information about local and remote active connections status.



|    | Field Name         | Sample Value                       | Explanation  |
|----|--------------------|------------------------------------|--|
| 1. | Type               | SSH; HTTP; HTTPS                   | Type of connection protocol  |
| 2. | Status             | Disabled/Enabled                   | Connection status  |
| 3. | Port               | 22; 80; 443                        | Connection port used   |
| 4. | Active Connections | 0(0.00B);0(0.00B);<br>6(558.12 KB) | Count of active connections and the amount of data transmitted in KB |

### 6.3.1.10.1 Last Connections


Displays information about the last 3 local and remote connections

| Access Status                  |                                  |                  |                        |
|--------------------------------|----------------------------------|------------------|------------------------|
| Access Information             |                                  | Last Connections |                        |
| <b>Last Local Connections</b>  |                                  |                  |                        |
| Type                           | Date                             | IP               | Authentications Status |
| SSH                            | 2016-03-03, 13:40:59             | 192.168.2.10     | Succeeded              |
|                                | 2016-03-03, 13:47:44             | 192.168.2.10     | Succeeded              |
|                                | 2016-03-09, 08:59:41             | 192.168.1.214    | Succeeded              |
| HTTP                           | 2016-03-09, 08:30:04             | 192.168.1.214    | Succeeded              |
|                                | 2016-03-09, 13:52:08             | 192.168.1.214    | Succeeded              |
|                                | 2016-03-09, 08:26:16             | 192.168.1.214    | Succeeded              |
| HTTPS                          | <i>There are no records yet.</i> |                  |                        |
| <b>Last Remote Connections</b> |                                  |                  |                        |
| Type                           | Date                             | IP               | Authentications Status |
| SSH                            | 2016-03-07, 07:57:51             | 212.59.13.226    | Succeeded              |
|                                | 2016-03-07, 08:41:46             | 119.167.153.187  | Failed                 |
|                                | 2016-03-07, 08:41:55             | 119.167.153.187  | Failed                 |
| HTTP                           | 2016-03-07, 07:56:06             | 10.8.32.1        | Succeeded              |
|                                | 2016-03-07, 07:57:15             | 212.59.13.226    | Succeeded              |
|                                | 2016-03-09, 14:13:05             | 10.8.32.1        | Succeeded              |
| HTTPS                          | <i>There are no records yet.</i> |                  |                        |

|    | Field Name             | Sample Value         | Explanation                                   |
|----|------------------------|----------------------|---|
| 1. | Type                   | SSH; HTTP; HTTPS     | Type of connection protocol                   |
| 2. | Date                   | 2016-03-03, 13:40:59 | Date and time of connection                   |
| 3. | IP                     | 192.168.2.10         | IP address from which the connection was made |
| 4. | Authentications Status | Failed/Succeed       | Status of authentication attempt              |

## 6.4 Device information

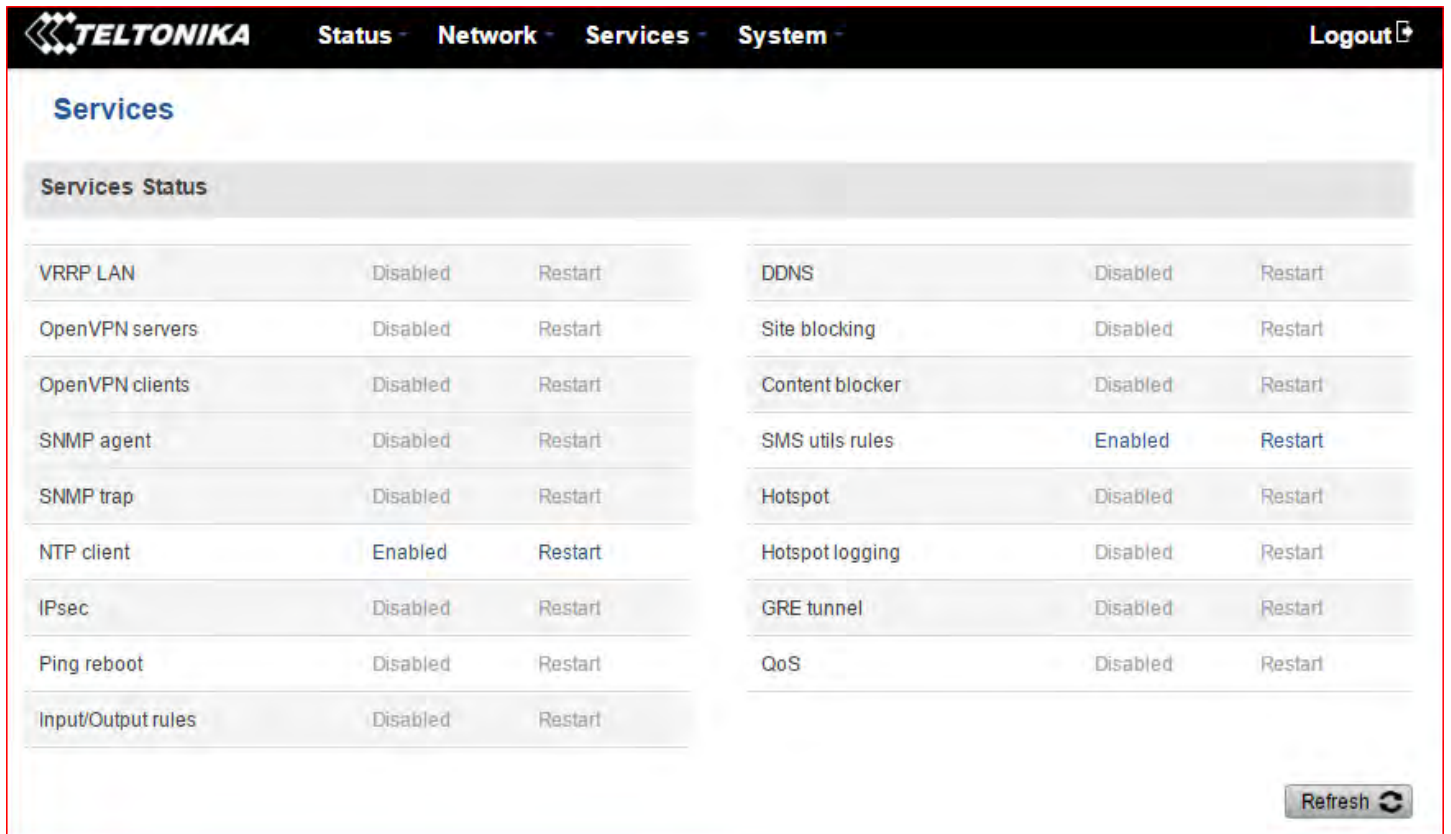
The page displays factory information that was written into the device during manufacturing process.

| TELTONIKA                 |                   | Status ▾ | Network ▾ | Services ▾ | System ▾ | Logout  |
|---------------------------|-------------------|----------|-----------|------------|----------|--|
| <b>Device Information</b> |                   |          |           |            |          |  |
| <b>Device</b>             |                   |          |           |            |          |  |
| Serial number             | 77885555          |          |           |            |          |  |
| Product code              | RUT900001000      |          |           |            |          |  |
| Batch number              | 1000              |          |           |            |          |  |
| Hardware revision         | 0001              |          |           |            |          |  |
| IMEI                      | 351579053257484   |          |           |            |          |  |
| IMSI                      | 246021003515790   |          |           |            |          |  |
| Ethernet LAN MAC address  | 00:1E:42:00:00:1E |          |           |            |          |  |
| Ethernet WAN MAC address  | 00:1E:42:00:00:11 |          |           |            |          |  |
| Wireless MAC address      | 00:1E:42:00:00:12 |          |           |            |          |  |
| <b>Modem</b>              |                   |          |           |            |          |  |
| Model                     | HE910-D           |          |           |            |          |  |
| FW version                | 12.00.027         |          |           |            |          |  |

|     |                   |                   |   |
|-----|-------------------|-------------------|---|
| 1.  | Serial number     | 77885555          | Serial number of the device                                 |
| 2.  | Product code      | RUT900001000      | Product code of the device                                  |
| 3.  | Batch number      | 1000              | Batch number used during the device's manufacturing process |
| 4.  | Hardware revision | 0001              | Hardware revision of the device                             |
| 5.  | IMEI              | 351579053257484   | Identification number of the internal modem                 |
| 6.  | IMSI              | 246021003515790   | Subscriber identification number of the internal modem      |
| 6.  | Ethernet LAN MAC  | 00:1E:42:00:00:1E | MAC address of the Ethernet LAN ports                       |
| 7.  | Ethernet WAN MAC  | 00:1E:42:00:00:11 | MAC address of the Ethernet WAN port                        |
| 8.  | Wireless MAC      | 00:1E:42:00:00:12 | MAC address of the Wi-Fi interface                          |
| 9.  | Model             | HE910-D           | Router's modem model  |
| 10. | FW version        | 12.00.027         | Router's modem firmware version                             |


## 6.5 Services

The page displays the usage of the available services.



The screenshot shows the 'Services' page in the Teltonika web interface. The navigation bar at the top includes 'Status', 'Network', 'Services', and 'System', with 'Services' being the active tab. The 'Services Status' section contains two columns of service entries. Each entry consists of the service name, its current status, and a 'Restart' button. The 'SMS utils rules' service is the only one shown as 'Enabled', while all other services are 'Disabled'. A 'Refresh' button with a circular arrow icon is positioned at the bottom right of the table area.

| Service Name       | Status   | Action  |
|--------------------|----------|---------|
| VRRP LAN           | Disabled | Restart |
| OpenVPN servers    | Disabled | Restart |
| OpenVPN clients    | Disabled | Restart |
| SNMP agent         | Disabled | Restart |
| SNMP trap          | Disabled | Restart |
| NTP client         | Enabled  | Restart |
| IPsec              | Disabled | Restart |
| Ping reboot        | Disabled | Restart |
| Input/Output rules | Disabled | Restart |
| DDNS               | Disabled | Restart |
| Site blocking      | Disabled | Restart |
| Content blocker    | Disabled | Restart |
| SMS utils rules    | Enabled  | Restart |
| Hotspot            | Disabled | Restart |
| Hotspot logging    | Disabled | Restart |
| GRE tunnel         | Disabled | Restart |
| QoS                | Disabled | Restart |

Refresh 

## 6.6 Routes

The page displays ARP table and active IP routes of the device.

### 6.6.1 ARP

Show the router's active ARP table. An ARP table contains recently cached MAC addresses of every immediate device that was communicating with the router.

| IP Address    | MAC Address       | Interface |
|---------------|-------------------|-----------|
| 192.168.99.17 | 02:50:F3:00:00:00 | eth2      |
| 192.168.99.17 | 00:25:22:D7:CA:A7 | br-lan    |

| No. | Field       | Value             | Description  |
|-----|-------------|-------------------|--|
| 1.  | IP Address  | 192.168.99.17     | Recently cached IP addresses of every immediate device that was communicating with the router  |
| 2.  | MAC Address | 00:25:22:D7:CA:A7 | Recently cached MAC addresses of every immediate device that was communicating with the router |
| 3.  | Interface   | br-lan            | Interface used for connection  |

### 6.6.2 Active IP-Routes

Shows the router's routing table. The routing table indicates where a TCP/IP packet, with a specific IP address, should be directed to.

| Destination     | Gateway      | Metric |
|-----------------|--------------|--------|
| 0.0.0.0/0       | 10.0.207.217 | 0      |
| 10.0.207.216/29 | 0.0.0.0      | 0      |
| 10.0.207.217    | 0.0.0.0      | 0      |

| No. | Field      | Value           | Description   |
|-----|------------|-----------------|---|
| 1.  | Network    | ppp             | Interface to be used to transmit TCP/IP packets through                         |
| 2.  | Target     | 192.168.99.0/24 | Indicates where a TCP/IP packet, with a specific IP address, should be directed |
| 3.  | IP Gateway | 0.0.0.0         | Indicates through which gateway a TCP/IP packet should be directed              |
| 4.  | Metric     | 0               | Metric number indicating interface priority of usage                            |

### 6.6.3 Active IPv6-Routes

Display active IPv6 routes for data packet transition.



|                      |                 |          |
|----------------------|-----------------|----------|
| 0:0:0:0:0:0:0:0      | 0:0:0:0:0:0:0:0 | FFFFFFF  |
| 0:0:0:0:0:0:0:0      | 0:0:0:0:0:0:0:0 | FFFFFFF  |
| 0:0:0:0:0:0:0:1      | 0:0:0:0:0:0:0:0 | 0000000  |
| FF00:0:0:0:0:0:0:0/8 | 0:0:0:0:0:0:0:0 | 00000100 |

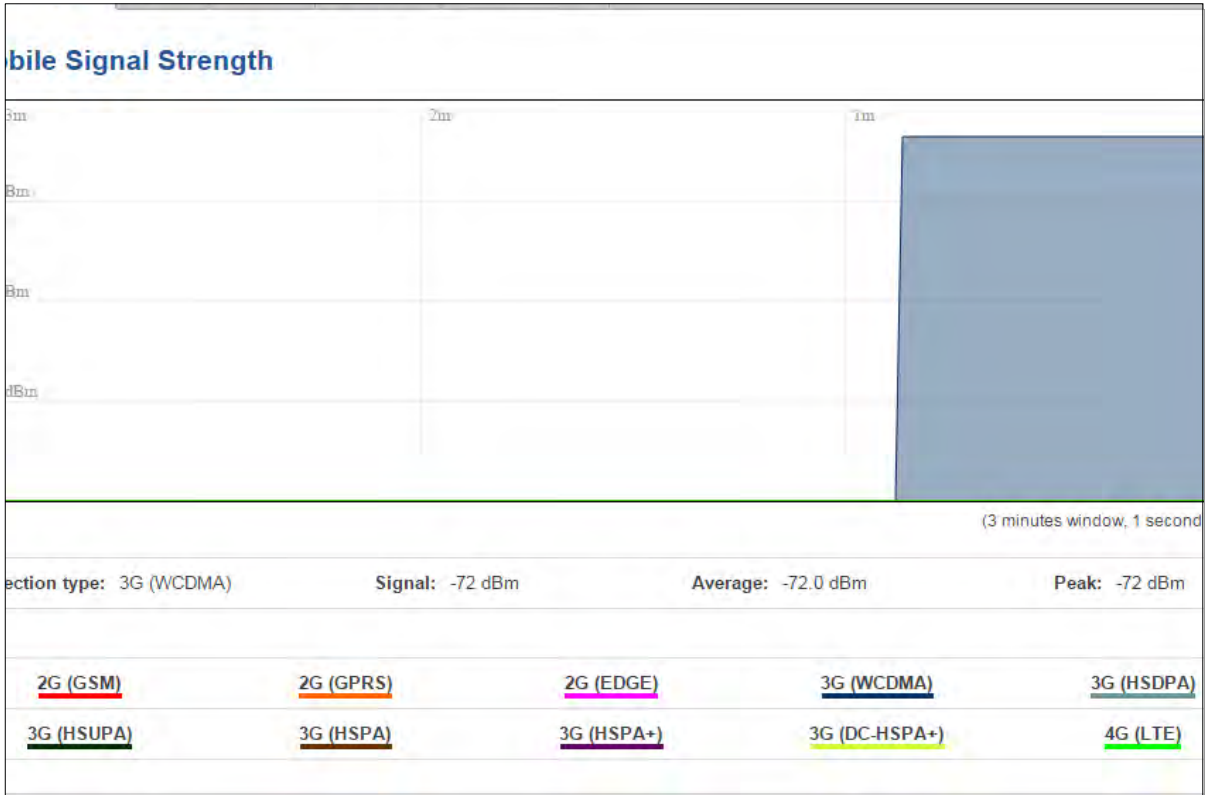
| 1. | Network      | loopback          | Network interface used  |
|----|--------------|-------------------|---|
| 2. | Target       | 0:0:0:0:0:0:0:0/0 | Indicates where a TCP/IP packet, with a specific IP address, should be directed |
| 3. | IPv6-Gateway | 0:0:0:0:0:0:0:0/0 | Indicates through which gateway a TCP/IP packet should be directed              |
| 4. | Metric       | FFFFFFF           | Metric number indicating interface priority of usage                            |

## 6.7 Graphs

Real-time graphs show how various statistical data changes over time.

### 6.7.1 Mobile Signal Strength

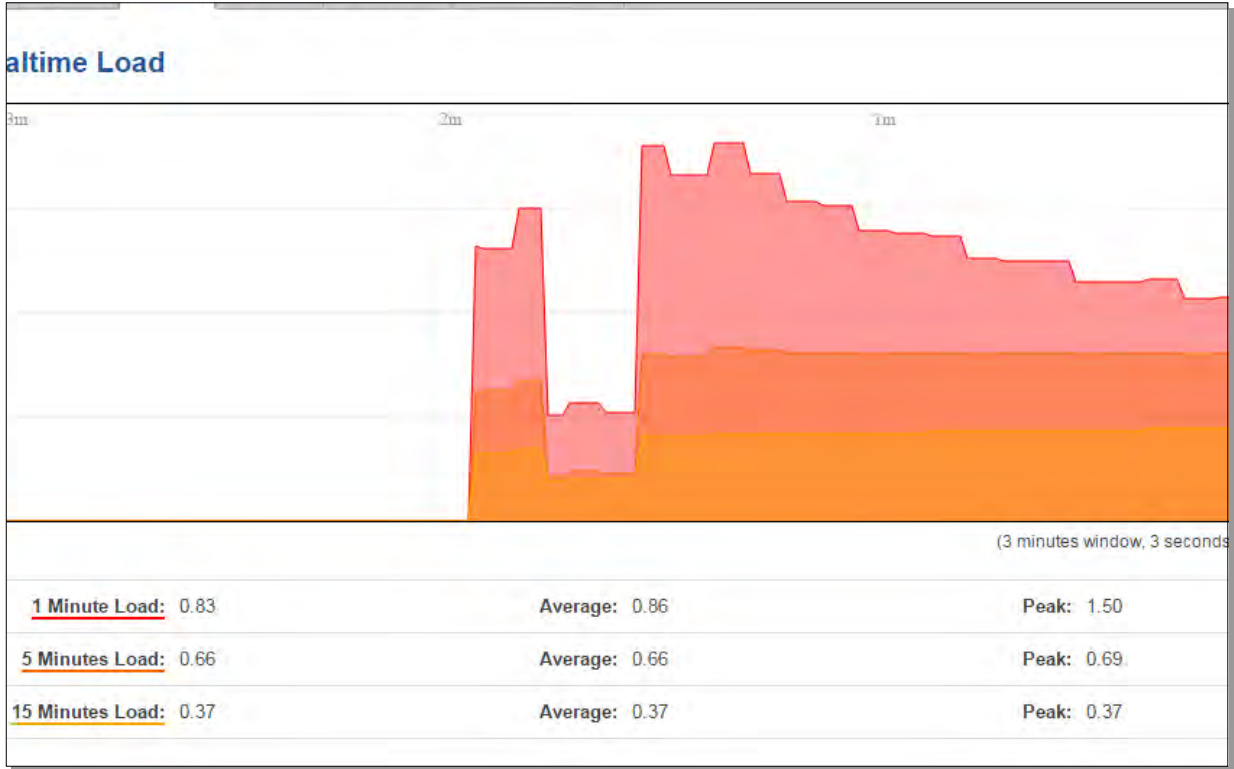
Displays mobile signal strength variation in time (measured in dBm)



| 1. | Connection type | LTE       | Type of mobile connection used |
|----|-----------------|-----------|--------------------------------|
| 2. | Signal          | -72 dBm   | Current signal strength value  |
| 3. | Average         | -72.0 dBm | Average signal strength value  |
| 4. | Peak            | -72 dBm   | Peak signal strength value     |

### 6.7.2 Realtime Load

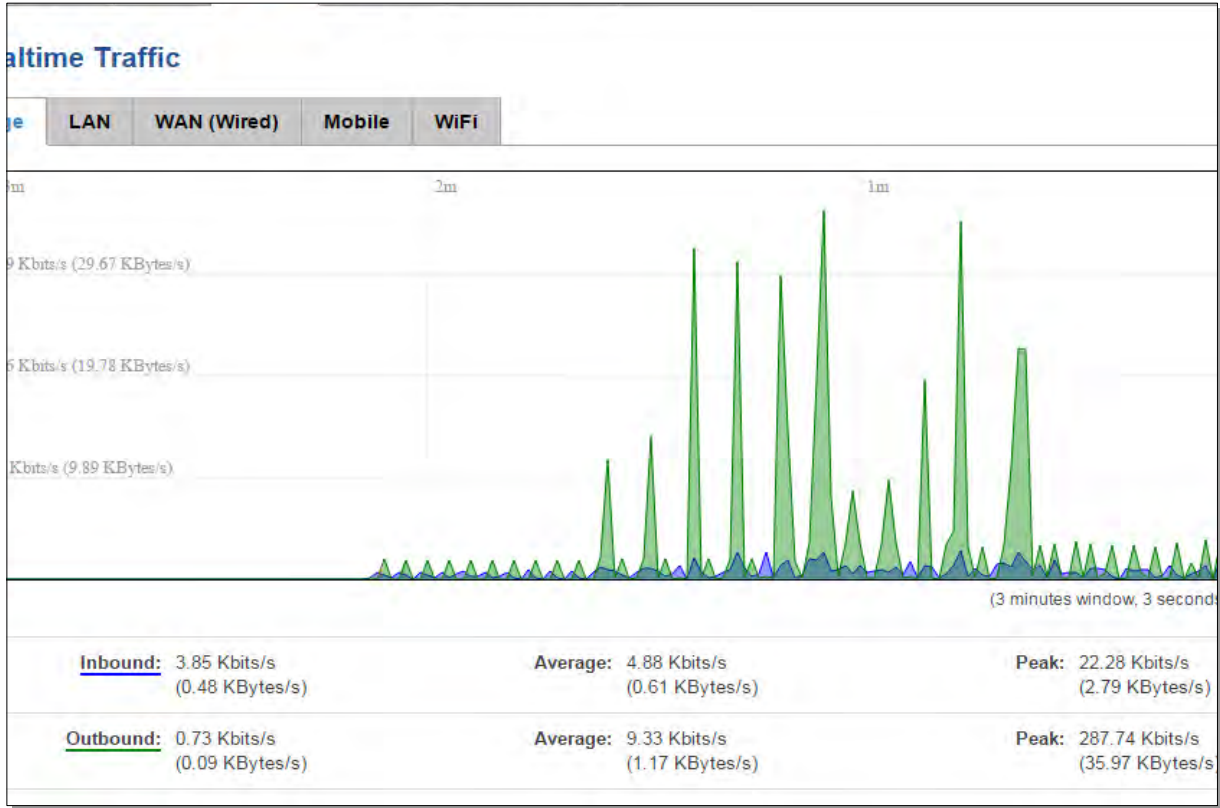
This tri-graph illustrates average CPU load values in real time. The graph consists out of three color coded graphs, each one corresponding to the average CPU load over 1 (red), 5 (orange) and 15 (yellow) most recent minutes.



| 1. | 1/5/15 Minutes Load | 0.83 | Time interval for load averaging, colour of the diagram   |
|----|---------------------|------|---|
| 2. | Average             | 0.86 | Average CPU load value over time interval (1/5/15 Minute) |
| 3. | Peak                | 1.50 | Peak CPU load value of the time interval                  |

### 6.7.3 Realtime Traffic

These graphs illustrate the average system inbound and outbound traffic over the course of 3 minutes; each new measurement is taken every 3 seconds. Each graph consists out of two color coded graphs (green graph shows the outbound traffic, blue graph shows the inbound traffic). Although not graphed, the page also displays peak loads and averages of inbound and outbound traffic.



|    |             |   |
|----|-------------|---|
| 1. | Bridge      | Cumulative graph, which encompasses wired Ethernet LAN and the wireless network.        |
| 2. | LAN         | Graphs the total traffic that passes through both LAN network interfaces.               |
| 3. | WAN (Wired) | Graphs the amount of traffic which passed through the current active WAN connection.    |
| 4. | Mobile      | Graphs the amount of traffic which passed through the mobile network connection.        |
| 5. | Wi-Fi       | Shows the amount of traffic that has been sent and received through the wireless radio. |

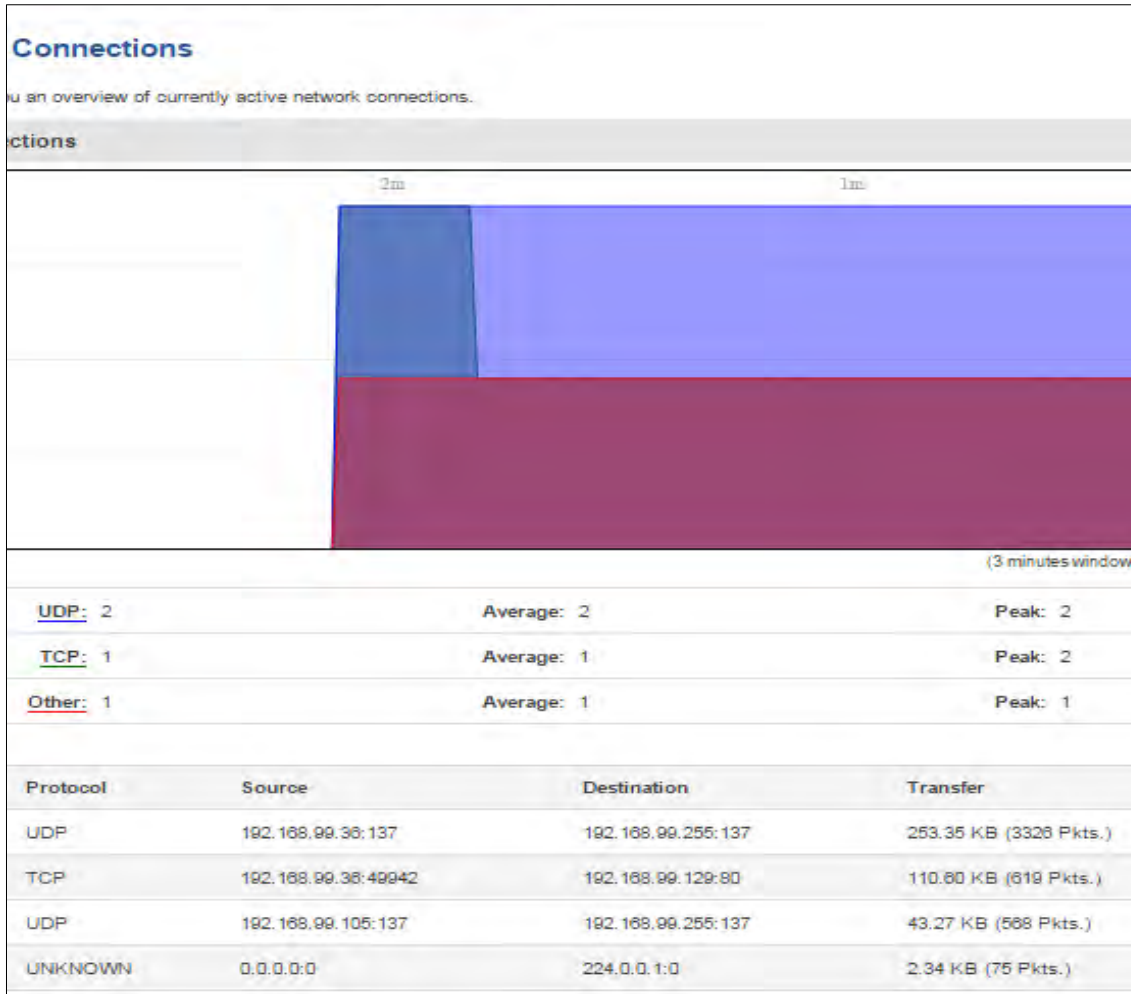
### 6.7.4 Realtime Wireless

Displays the wireless radio signal, signal noise and the theoretical maximum channel permeability. Average and peak signal levels are displayed.



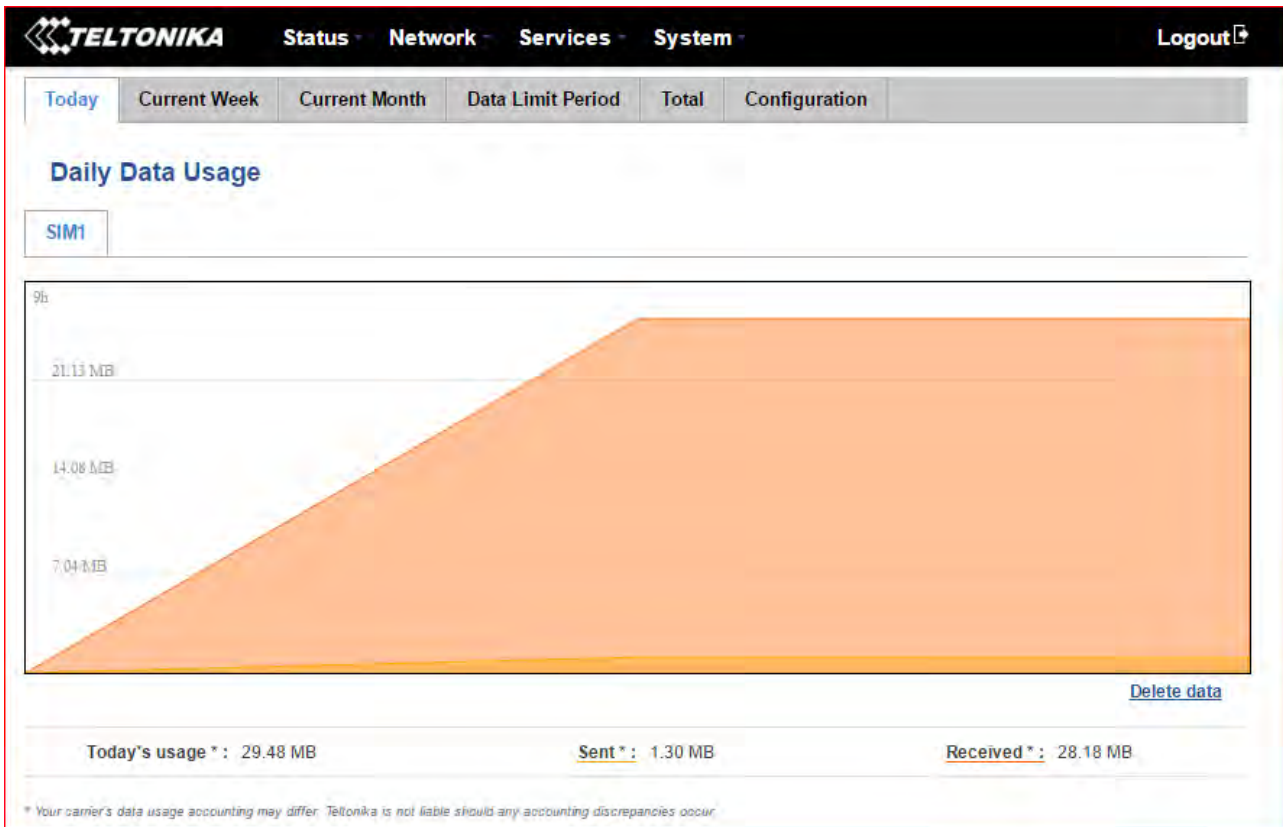
### 6.7.5 Realtime Connections

Displays currently active network connections with the information about network, protocol, source and destination addresses, transfer speed.



## 6.8 Mobile Traffic

Displays mobile connection data sent and received in KB of this day, week and month.



By default mobile traffic usage logging is disabled. To use this functionality is needed to enable it.

The screenshot shows the 'Mobile Traffic Usage Logging' configuration page. It includes a navigation bar with 'Today', 'Current Week', 'Current Month', 'Total', and 'Configuration' (highlighted). The main content area has the title 'Mobile Traffic Usage Logging' and a form with the following elements:
 

- 'Enable' checkbox:
- 'Interval between records (sec)' input field: 60
- 'Save' button

|    |                                |                |   |
|----|--------------------------------|----------------|---|
| 1. | Enable                         | Enable/Disable | Make the functionality active/inactive                |
| 2. | Interval between records (sec) | 60             | The interval between logging records (minimum 60 sec) |

## **6.9 Events Log**

Event log displays such actions as: login, reboot, firmware flashing and reset.

### **6.9.1 All Events**

Displays all router events, their types and time of occurrence.

### **6.9.2 System Events**

Displays all system events, their type and time of occurrence. Events include authentication or reboot requests, incoming and outgoing SMS and Calls, Mails, Configuration changes and DHCP events.

### **6.9.3 Network Events**

Displays information about recent network events like connection status change, lease status change, network type or operator change.



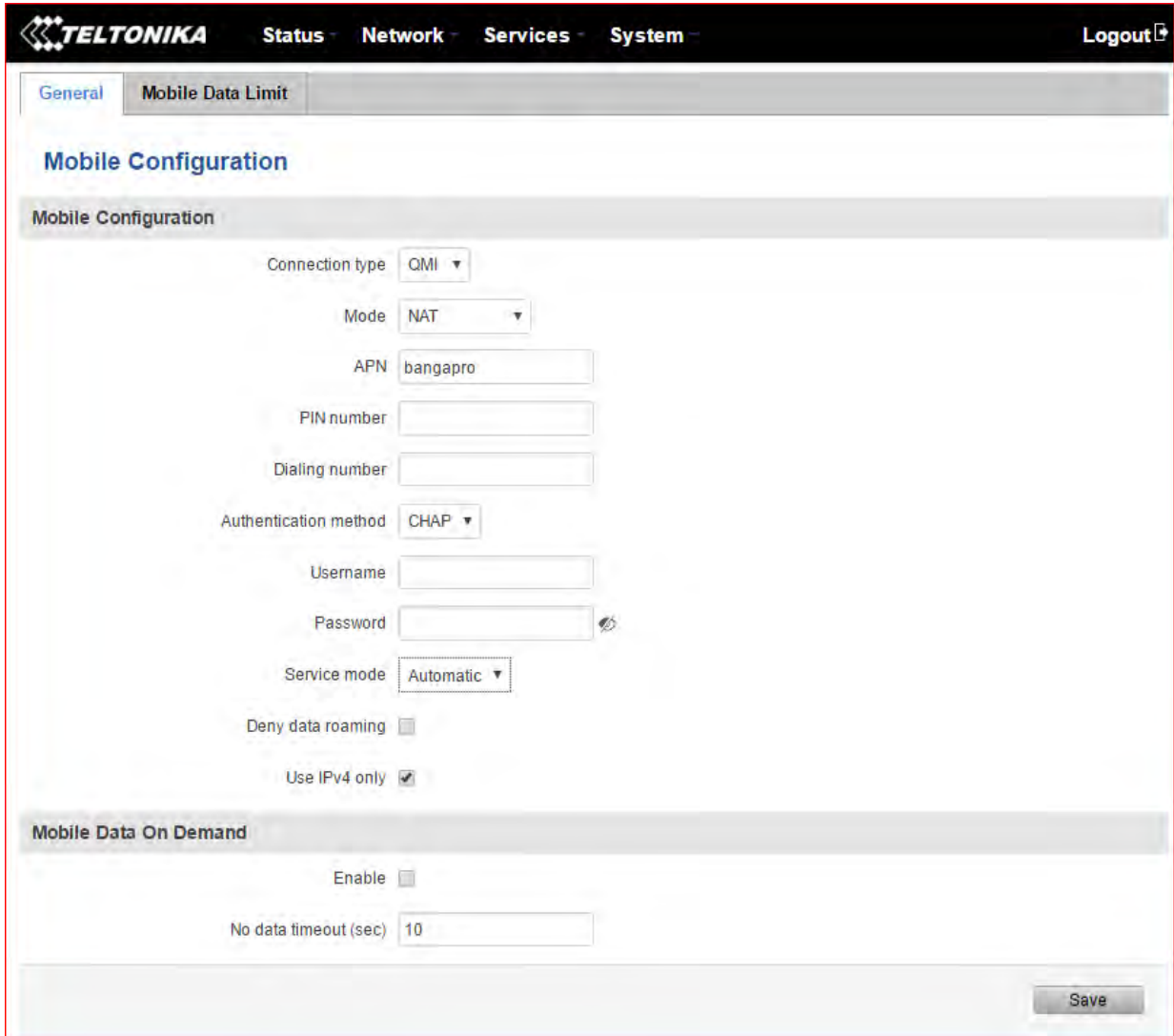
## 7 Network

### 7.1 Mobile

#### 7.1.1 General

##### 7.1.1.1 Mobile configuration

Here you can configure mobile settings which are used when connecting to your local LTE network.



The screenshot displays the Teltonika web management interface. At the top, there is a navigation bar with the Teltonika logo and menu items: Status, Network, Services, and System. A Logout button is located in the top right corner. Below the navigation bar, there are two tabs: 'General' (selected) and 'Mobile Data Limit'. The main content area is titled 'Mobile Configuration' and contains the following settings:

- Connection type: QMI (dropdown)
- Mode: NAT (dropdown)
- APN: bangapro (text input)
- PIN number: (text input)
- Dialing number: (text input)
- Authentication method: CHAP (dropdown)
- Username: (text input)
- Password: (text input with toggle icon)
- Service mode: Automatic (dropdown)
- Deny data roaming:
- Use IPv4 only:

Below the 'Mobile Configuration' section is the 'Mobile Data On Demand' section, which includes:

- Enable:
- No data timeout (sec): 10 (text input)

A 'Save' button is located at the bottom right of the form area.

| 1. | Connection type       | QMI   | The connection type used when connecting to a network. It can either be PPP or QMI. PPP is considerably slower than QMI.   |
|----|-----------------------|---|--|
| 2. | Mode                  | NAT / Passthrough                           | NAT mode enables network address translation on router. Passthrough mode is similar with bridge mode except that in passthrough mode router do have internet connection.   |
| 3. | APN                   | "bangapro"                                  | <b>Access Point Name</b> (APN) is a configurable network identifier used by a mobile device when connecting to a GSM carrier.  |
| 4. | PIN number            | Any number that falls between 0000 and 9999 | A <b>personal identification number</b> is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system. Use this only if your SIM card has PIN enabled. |
| 5. | Dialing number        |   | Dialing number is used to establish a mobile PPP (Point-to-Point-Protocol) connection.   |
| 6. | Authentication method | CHAP, PAP or none                           | Authentication method, which your carrier uses to authenticate new connections. (This selection is unavailable on the alternate model)   |
| 7. | Username              | "username"                                  | Your username that you would use to connect to your carrier's network. This field becomes available when you select an authentication method (i.e. authentication method is not "none").                         |
| 8. | Password              | "password"                                  | Your password that you would use to connect to your carrier's network. This field becomes available when you select an authentication method (i.e. authentication method is not "none").                         |
| 9  | Deny data roaming     | Enable/Disable                              | If enabled this function prevents the device from establishing mobile data connection while not in home network.   |
| 1  | Use IPv4 only         | Enable / Disable                            | If enabled this function makes the device to use only IPv4 settings when connecting to operator.   |

**Warning:** If an invalid PIN number was entered (i.e. the entered PIN does not match the one that was used to protect the SIM card), your SIM card will get blocked. To avoid such mishaps it is highly advised to use an unprotected SIM. If you happen to insert a protected SIM and the PIN number is incorrect, your card won't get blocked immediately, although after a couple of reboots OR configuration saves it will.

### 1.1.1.1.1 Passthrough mode

|                       |                          |         |
|-----------------------|--------------------------|---------|
| Mode                  | Passthrough              | ▼       |
| APN                   | bangapro                 |         |
| PIN number            | 1525                     |         |
| Dialing number        | *99#                     |         |
| Authentication method | None                     | ▼       |
| Service mode          | Automatic                | ▼       |
| Deny data roaming     | <input type="checkbox"/> |         |
| Use IPv4 only         | <input type="checkbox"/> |         |
| DHCP mode             | Static                   | ▼       |
| MAC Address           |                          |         |
| Lease time            | 12                       | Hours ▼ |

**Using Passthrough Mode will disable most of the router capabilities!**

#### DHCP mode: Static

Enter your computer's MAC address (xx:xx:xx:xx:xx:xx) to MAC Address field and select Lease time (expiration time for leased addresses). Device, whose MAC address will be entered, will get IP from the GSM operator. Other connected devices will get IP from the router's DHCP server, but these devices will not have internet access.

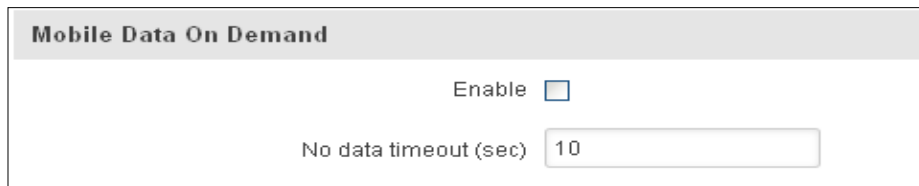
## DHCP mode: Dynamic

When using Dynamic mode, the device will get an IP from the GSM operator, which connects to the router first. When using Passthrough in dynamic mode, the DHCP in LAN configuration will be disabled.

## DHCP mode: No DHCP

Using no DHCP mode, the IP (also subnet, gateway and DNS) should be entered manually on your device which you are trying to connect to the router's LAN. When using Passthrough in no DHCP mode, the DHCP in LAN configuration will be disabled.

### 7.1.1.2 Mobile Data On Demand



**Mobile Data On Demand**

Enable

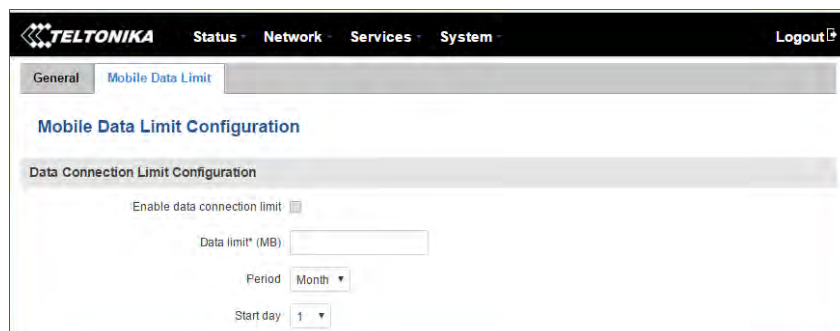
No data timeout (sec)

| 1. | Enable               | Enable/Disable | Mobile Data On Demand function enables you to keep mobile data connection on only when it's in use. |
|----|----------------------|----------------|---|
| 2. | No data timeout(sec) | 10-99999999    | The time it takes for mobile data connection to be terminated if there is no network activity.      |

## 7.1.2 Mobile Data Limit

This function lets you limit maximum amount of data transferred on WAN interface in order to minimize unwanted traffic costs.

### 7.1.2.1 Data Connection Limit Configuration



**TELTONIKA** Status Network Services System Logout

General Mobile Data Limit

**Mobile Data Limit Configuration**

Data Connection Limit Configuration

Enable data connection limit

Data limit\* (MB)

Period Month

Start day 1

|    | Field Name                   | Sample value   | Explanation   |
|----|------------------------------|----------------|---|
| 1. | Enable data connection limit | Enable/Disable | Disables mobile data when a limit for the current period is reached |
| 2. | Data limit* (MB)             | -              | Disable mobile data after limit value in MB is reached              |
| 3. | Period                       | Month/Week/Day | Period for which mobile data limiting should apply                  |
| 4. | Start day/ Start hour        | 1              | A starting time for mobile data limiting period                     |

\*

Your carrier's data usage accounting may differ. Teltonika is not liable should any accounting discrepancies occur.

### 7.1.2.2 SMS Warning Configuration

**SMS Warning Configuration**

Enable SMS warning

Data limit\* (MB)

Period

Start day

Phone number

|    | Field Name            | Sample value   | Explanation   |
|----|-----------------------|----------------|---|
| 1. | Enable SMS warning    | Enable/Disable | Enables the sending of a warning SMS message when mobile data limit for the current period is reached |
| 2. | Data limit* (MB)      | 300            | Send warning SMS message after limit value in MB is reached   |
| 3. | Period                | Month/Week/Day | Period for which the mobile data limiting should apply  |
| 4. | Start day/ Start hour | 1              | A starting time for the mobile data limiting period   |
| 5. | Phone number          | +37012345678   | A phone number to send the warning SMS message to, e.g. +37012345678                                  |

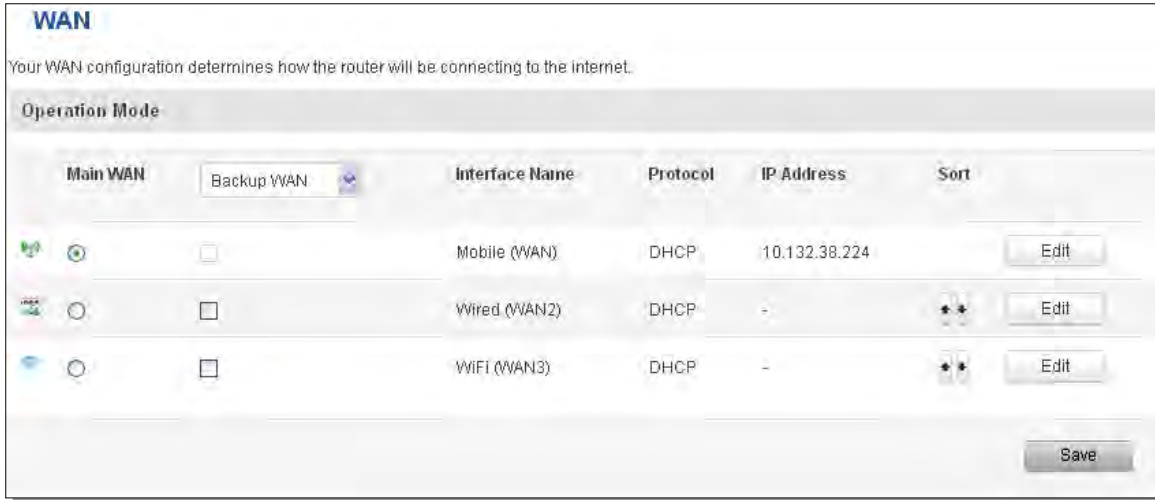
\*

Your carrier's data usage accounting may differ. Teltonika is not liable should any accounting discrepancies occur.

## 7.2 WAN

### 7.2.1 Operation Mode

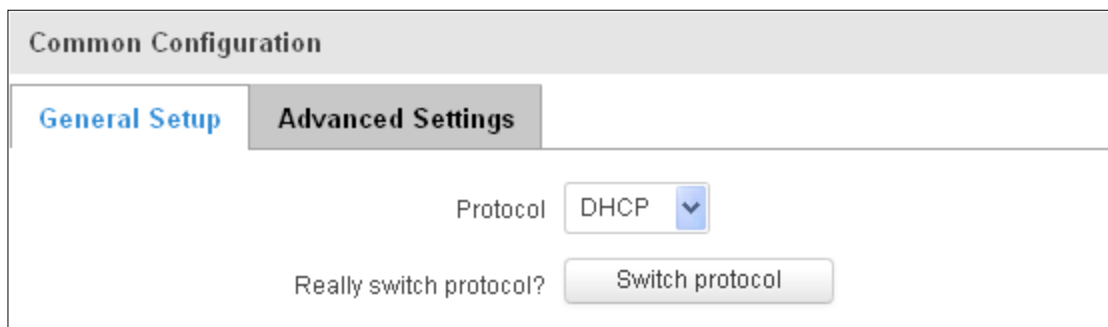
Your WAN configuration determines how the router will be connecting to the internet.



|    |                           |  |
|----|---------------------------|--|
| 1. | Main WAN                  | Switches between Mobile, Wired and Wi-Fi interfaces for main WAN   |
| 2. | Backup WAN/Load balancing | Let's user select one or two interfaces for WAN backup   |
| 3. | Interface Name            | Displays the WAN interface name, and changes interface priority. The interface at the table top has the highest priority |
| 4. | Protocol                  | Displays the protocol used by the WAN interface  |
| 5. | IP Address                | Displays IP address acquired by a specific interface   |
| 6. | Sort                      | Sorts table rows and changes interface priority. The highest interface has the highest priority                          |

### 7.2.2 Common configuration

Common configuration allows you to configure your TCP/IP settings for the wan network.



You can switch between Static, DHCP or PPPoE protocol by selecting the protocol that you want to use and then pressing **Switch Protocol**.

## 7.2.2.1 General Setup

### 7.2.2.1.1 Static:

The screenshot shows the 'Common Configuration' window with the 'General Setup' tab selected. The 'Protocol' is set to 'Static'. The following fields are filled in:

- IPv4 address: 192.168.99.162
- IPv4 netmask: 255.255.255.0
- IPv4 gateway: 192.168.99.254
- IPv4 broadcast: 192.168.99.255
- Use custom DNS servers: 8.8.8.8 and 8.8.6.6

This is the configuration setup for when you select the static protocol.

|    |                        |                    |   |
|----|------------------------|--------------------|---|
| 1. | IPv4 address           | 192.168.99.162     | Your router's address on the WAN network  |
| 2. | IPv4 netmask           | 255.255.255.0      | A mask used to define how "large" the WAN network is  |
| 3. | IPv4 gateway           | 192.168.99.254     | Address where the router will send all the outgoing traffic   |
| 4. | IPv4 broadcast         | 192.168.99.255     | Broadcast address (auto generated if not set). It is best to leave this blank unless you know what you are doing.   |
| 5. | Use custom DNS servers | 8.8.8.8<br>8.8.6.6 | Usually the gateway has some predefined DNS servers. As such the router, when it needs to resolve a hostname ("www.google.com", "www.cnn.com", etc...) to an IP address, it will forward all the DNS requests to the gateway. By entering custom DNS servers the router will take care of host name resolution. You can enter multiple DNS servers to provide redundancy in case the one of the server fails. |

### 7.2.2.1.2 DHCP:

The screenshot shows the 'Common Configuration' window with the 'General Setup' tab selected. The 'Protocol' is set to 'DHCP'. The 'Hostname to send when requesting DHCP' field is filled with 'Teltonika'.

When you select the DHCP protocol you can use it as is, because most networks will not require any additional advanced configuration.

### 7.2.2.1.3 PPPoE

This protocol is mainly used by DSL providers:

The screenshot shows the 'Common Configuration' window with the 'Advanced Settings' tab selected. The 'Protocol' dropdown is set to 'PPPoE'. Below it, there are four input fields: 'PAP/CHAP username' with the value 'test', 'PAP/CHAP password' with masked characters '••••', 'Access Concentrator' with the value 'auto', and 'Service Name' with the value 'auto'.

This is the configuration setup for when you select PPPoE protocol.

| 1. | PAP/CHAP username   | test          | Your username and password that you would use to connect to your carrier's network. |
|----|---------------------|---------------|---|
| 2. | PAP/CHAP password   | your_password | A mask used to define how "large" the WAN network is                                |
| 3. | Access Concentrator | auto          | Specifies the name of the access concentrator. Leave empty to auto detect.          |
| 4. | Service Name        | auto          | Specifies the name of the service. Leave empty to auto detect.                      |

### 7.2.2.2 Advanced

These are the advanced settings for each of the protocols, if you are unsure of how to alter these attributes it is highly recommended to leave them to a trained professional:

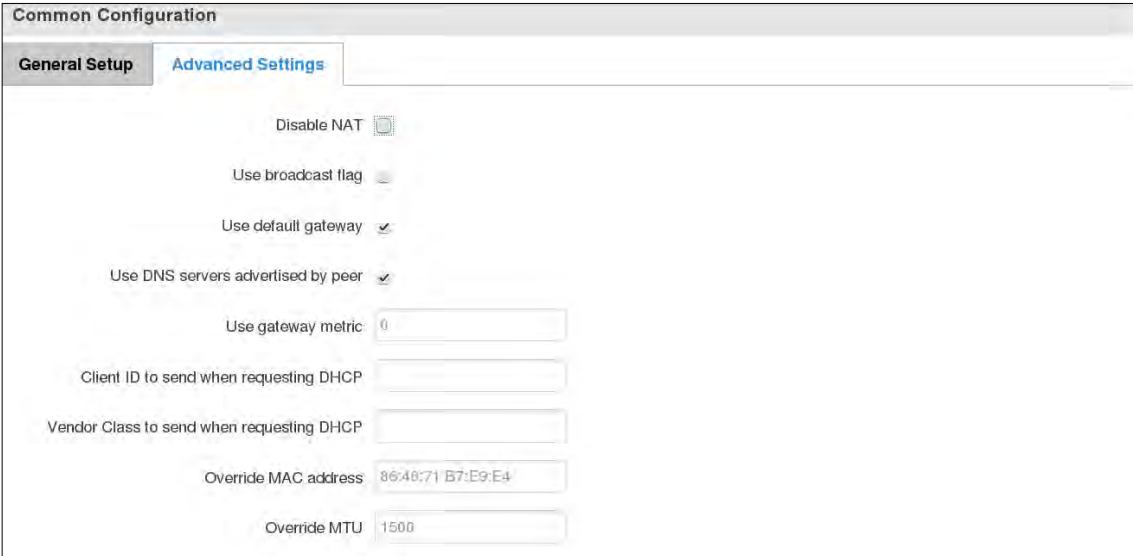
#### 7.2.2.2.1 Static

The screenshot shows the 'Common Configuration' window with the 'Advanced Settings' tab selected. It features several settings: 'Disable NAT' with a toggle switch, 'Override MAC address' with the value '86:48:71:B7:E9:E4', 'Override MTU' with the value '1500', and 'Use gateway metric' with the value '0'.



|    |                      |                   |   |
|----|----------------------|-------------------|---|
| 1. | Disable NAT          | On/Off            | Toggle NAT on and off.  |
| 2. | Override MAC address | 86:48:71:B7:E9:E4 | Override MAC address of the WAN interface. If your ISP gives you a static IP address it might also bind it to your computer's MAC address (i.e. that IP will only work with your computer). In this field you can enter your computer's MAC address and "fool" the gateway in thinking that it is communicating with your computer. |
| 3. | Override MTU         | 1500              | <b>Maximum Transmission Unit</b> – specifies the largest possible size of a data packet.  |
| 4. | Use gateway metric   | 0                 | The WAN configuration by default generates a routing table entry. With this field you can alter the metric of that entry.   |

#### 7.2.2.2.2 DHCP



|    |   |                   |   |
|----|---|-------------------|---|
| 1. | Disable NAT                               | Enable/Disable    | If checked, router will not perform NAT (masquerade) on this interface  |
| 2. | Use broadcast flag                        | Enable/Disable    | Required for certain ISPs, e.g. Charter with DOCSIS 3   |
| 3. | Use default gateway                       | Enable/Disable    | If unchecked, no default route is configured  |
| 4. | Use DNS server advertised by peer         | Enable/Disable    | If unchecked, the advertised DNS server addresses are ignored   |
| 5. | User gateway metric                       | 0                 | The WAN configuration by default generates a routing table entry<br>With this field you can alter the metric of that entry  |
| 6. | Client ID to send when requesting DHCP    |                   | Specify client ID which will be sent when requesting DHCP (Dynamic Host Configuration Protocol)   |
| 7. | Vendor Class to send when requesting DHCP |                   | Specify the vendor class which will be sent when requesting DHCP (Dynamic Host Configuration Protocol)  |
| 8. | Override MAC address                      | 86:48:71:B7:E9:E4 | Override MAC address of the WAN interface. If your ISP gives you a static IP address it might also bind it to your computer's MAC address (i.e. that IP will only work with your computer). In this field you can enter your computer's MAC address and "fool" the gateway in thinking that it is communicating with your computer. |
| 9. | Override MTU                              | 1500              | Maximum transmission unit – specifies the largest possible size of a data packet.   |

### 7.2.2.2.3 PPPoE

**Common Configuration**

**General Setup**   **Advanced Settings**

Disable NAT

Use default gateway

Use gateway metric:

Use DNS servers advertised by peer

LCP echo failure threshold:

LCP echo interval:

Inactivity timeout:

| 1. | Disable NAT                        | Enable/Disable | If checked, the router will not perform NAT (masquerade) on this interface   |
|----|------------------------------------|----------------|--|
| 2. | Use default gateway                | Enable/Disable | If unchecked, no default route is configured   |
| 3. | Use gateway metric                 | 0              | The WAN configuration by default generates a routing table entry. With this field you can alter the metric of that entry |
| 4. | Use DNS servers advertised by peer | Enable/Disable | If unchecked, the advertised DNS server addresses are ignored  |
| 5. | LCP echo failure threshold         | 0              | Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures                                |
| 6. | LCP echo interval                  | 5              | Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold            |
| 7. | Inactivity timeout                 | 0              | Close inactive connection after the given amount of seconds, use 0 to persist connection                                 |

### 7.2.2.2.4 IP Aliases

IP aliases are a way of defining or reaching a subnet that works in the same space as the regular network.



The screenshot shows the 'Advanced Settings' tab for IP Aliases. It features three input fields: 'IP Address' with the value '192.168.99.161', 'Netmask' with a dropdown menu showing '255.255.255.0', and 'Gateway' with the value '192.168.99.254'. On the left side, there are 'Delete' and 'Add' buttons. A 'Save' button is located at the bottom right of the configuration area.

As you can see, the configuration is very similar to the static protocol; only in the example a 99th subnet is defined. Now if some device has an IP in the 99 subnet (192.168.99.xxx) and the subnet's gateway metric is "higher" and the device is trying to reach the internet it will reroute it's traffic not to the gateway that is defined in common configurations but through the one that is specified in IP aliases.

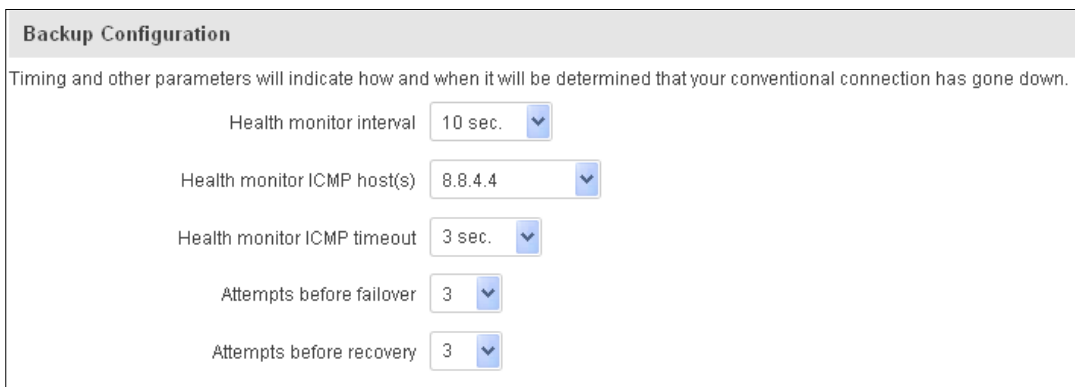


The screenshot shows the 'Advanced Settings' tab for a different configuration. It features two input fields: 'IP Broadcast' and 'DNS Server'. On the left side, there are 'Delete' and 'Add' buttons. A 'Save' button is located at the bottom right of the configuration area.

You may also optionally define a broadcast address and a custom DNS server.

### 7.2.2.2.5 Backup WAN configuration

Backup WAN is a function that allows you to back up your primary connection in case it goes down. There can be two backup connections selected at the same time, in that case, when the primary connection fails, the router tries to use the backup with higher priority and if that is unavailable or fails too, then router tries the backup with the lower priority.



The screenshot shows the 'Backup Configuration' interface. It includes a descriptive text: 'Timing and other parameters will indicate how and when it will be determined that your conventional connection has gone down.' Below this, there are five configuration items, each with a dropdown menu: 'Health monitor interval' set to '10 sec.', 'Health monitor ICMP host(s)' set to '8.8.4.4', 'Health monitor ICMP timeout' set to '3 sec.', 'Attempts before failover' set to '3', and 'Attempts before recovery' set to '3'.

The majority of the options consist of timing and other important parameters that help determine the health of your primary connection. Regular health checks are constantly performed in the form of ICMP packets (Pings) on your primary connection. When the connection's state starts to change (READY->NOT READY and vice versa) a necessary amount of failed or passed health checks has to be reached before the state changes completely. This delay is instituted so as to mitigate "spikes" in connection availability, but it also extends the time before the backup link can be brought up or down.

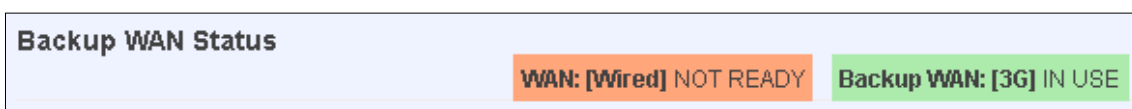
|    |                             |                                      |   |
|----|-----------------------------|--------------------------------------|---|
| 1. | Health monitor Interval     | Disable/5/10/20/30/60/120 Seconds    | The interval at which health checks are performed   |
| 2. | Health monitor ICMP host(s) | Disable/DNS Server(s) /WAN GW/Custom | Indicate where to Ping for a health check. As there is no definitive way to determine when the connection to internet is down for good, you'll have to define a host whose availability is that of the internet as a whole. |
| 3. | Health monitor ICMP timeout | 1/3/4/5/10 Seconds                   | How long to wait for an ICMP request to come back. Set a higher value if your connection has high latency or high jitter (latency spikes).  |
| 4. | Attempts before failover    | 1/3/5/10/15/20                       | How many failed checks before your WAN connection is declared DOWN for good.  |
| 5. | Attempts before recovery    | 1/3/5/10/15/20                       | How many checks before your WAN connection is declared UP.  |

### 7.2.2.3 How do I set up a backup link?

First we must select a main link and choose one or two backup links in WAN section. Then push the "Edit" button and configure your WAN and Backup Wan settings to your liking. Click Save and wait until the settings are applied. Now in the Status -> Network Information -> WAN page there should be a status indication for the backup WAN. If everything is working correctly you should see something like this:



The above picture shows the status for Backup WAN configured on a wired main link. You can now simulate a downed link by simply unplugging your Ethernet WAN cable. When you've done so you should see this:



And, if you plug the cable back in you should, again, see this:



## 7.3 LAN

This page is used to configure the LAN network, where all your devices and computers that you connect to the router will reside.

### 7.3.1 Configuration

#### 7.3.1.1 General Setup

The screenshot shows a configuration window titled "Configuration" with two tabs: "General Setup" (selected) and "Advanced Settings". Under "General Setup", there are three input fields: "IP address" with the value "192.168.1.1", "IP netmask" with a dropdown menu showing "255.255.255.0", and "IP broadcast" which is currently empty.

| 1. | IP address   | 192.168.1.1   | Address that the router uses on the LAN network  |
|----|--------------|---------------|--|
| 2. | IP netmask   | 255.255.255.0 | A mask used to define how "large" the LAN network is   |
| 3. | IP broadcast |               | IP broadcasts are used by BOOTP and DHCP clients to find and send requests to their respective servers |

#### 7.3.1.2 Advanced settings

The screenshot shows the "Advanced Settings" tab in the configuration window. Two settings are visible: "Accept router advertisements" with a checkbox that is currently unchecked, and "Override MTU" with a text input field.

| 1. | Accept router advertisements | Enable/Disable | If enabled allows accepting router advertisements (Disabled by default).  |
|----|------------------------------|----------------|---|
| 2. | Override MTU                 | 1500           | MTU (Maximum Transmission Unit) specifies the largest possible size of a data packet.                                     |
| 3. | Use gateway metric           | 0              | The LAN configuration by default generates a routing table entry. With this field you can alter the metric of that entry. |
| 4. | Use WAN port as LAN          | Enable/Disable | When enabled it allows you to use the WAN port as a LAN port.   |

### 7.3.2 DHCP Server

The DHCP server is the router's side service that can automatically configure the TCP/IP settings of any device that requests such a service. If you connect a device that has been configured to obtain IP address automatically the DHCP server will lease an IP address and the device will be able to fully communicate with the router.

#### 7.3.2.1 General Setup

|    |            |                                 |  |
|----|------------|---------------------------------|--|
| 1. | DHCP       | Enable / Disable/<br>DHCP Relay | Manage DHCP server   |
| 2. | Start      | 100                             | The starting address of the range that the DHCP server can use to give out to devices. E.g.: if your LAN IP is 192.168.2.1 and your subnet mask is 255.255.255.0 that means that in your network a valid IP address has to be in the range of [192.168.2.1 - 192.168.2.254](192.168.2.0 and 192.168.2.255 are special unavailable addresses). If the Start value is set to 100 then the DHCP server will only be able to lease out addresses starting from 192.168.2.100 |
| 3. | Limit      | 150                             | How many addresses the DHCP server gets to lease out. Continuing on the above example: if the start address is 192.168.2.100 then the end address will be 192.168.2.254 (100 + 155 - 1 = 254).   |
| 4. | Lease time | 12                              | How long a leased IP will be considered valid. An IP address after the specified amount of time will expire and the device that leased it out will have to request a new one. Select Hours or Minutes (minimum 2min).  |

#### 7.3.2.2 Advanced settings

You can also define some advanced options that specify how the DHCP server will operate on your LAN network.

|    |              |                   |   |
|----|--------------|-------------------|---|
| 1. | Dynamic DHCP | Checked/Unchecked | Dynamically allocate client addresses, if set to 0 only clients present in the <code>ethers</code> files are served   |
| 2. | Force        | Checked/Unchecked | Forces DHCP serving even if another DHCP server is detected on the same network segment.  |
| 3. | IP netmask   |                   | You can override your LAN netmask here to make the DHCP server think it's serving a larger or a smaller network than it actually is.  |
| 4. | DHCP Options |                   | Additional options to be added for this DHCP server. For example with '26,1470' or 'option:mtu, 1470' you can assign an MTU per DHCP. Your client must accept MTU by DHCP for this to work. |

### 7.3.2.3 Static Leases

This page is used to configure static IP leases.

|    |             |                                   |  |
|----|-------------|-----------------------------------|--|
| 1. | Hostname    | Printer                           | The name which will be linked with IP address. |
| 2. | MAC address | 10:a5:d0:70:9c:72 (192.168.1.104) | Device's MAC address                           |
| 3. | IP address  | 192.168.1.104                     | Device's IP address                            |

### 7.3.2.4 IP Aliases

#### 7.3.2.4.1 General Setup

IP aliases are the way of defining or reaching a subnet that works in the same space as the regular network.

**IP Aliases**

**General Setup** **Advanced Settings**

IP Address

Netmask

Gateway



### 7.3.2.4.2 Advanced Settings

You may also optionally define a broadcast address and a custom DNS server.

**IP Aliases**

**General Setup**   **Advanced Settings**

IP Broadcast

DNS Server

Delete

Add

## 7.4 Wireless

On this page you can configure your wireless settings. Depending on whether your WAN mode is set to Wi-Fi or not, the page will display either the options for configuring an **Access Point** or options for configuring a **connection** to a local access point.

### Access Point:

**Wireless Access Point**

Here you can configure your wireless settings like radio frequency, mode, encryption etc...

**Device Configuration**

**General Setup** **Advanced Settings**

Enable wireless

Channel

**Interface Configuration**

**General Setup** **Wireless Security** **MAC Filter** **Advanced Settings**

SSID

Hide SSID

**WRP100 Configuration**

Connect WRP100 automatically

Here you can see the Overview of the wireless configuration. It is divided into two main sections – device and interface. One is dedicated to configuring hardware parameters, the other – software.

Here you can toggle the availability of the wireless radio and the physical channel frequency.

**Important note:** As seen in the picture you should always **Save** before toggling the radio on and off.

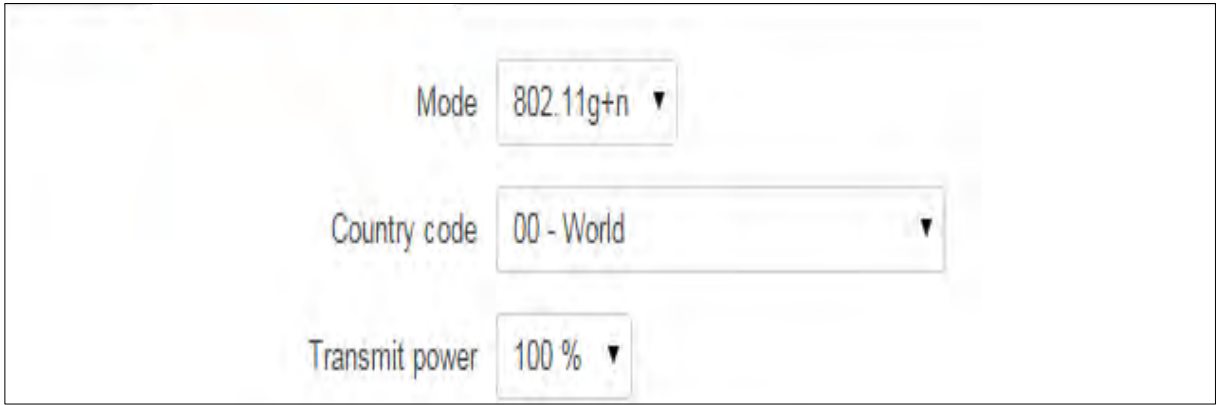
SSID – Your wireless network’s identification string. This is the name of your Wi-Fi network. When other Wi-Fi capable computers or devices scan the area for Wi-Fi networks they will see your network with this name.

Hide SSID – Will render your SSID hidden from other devices that try to scan the area.

Connect to WRP100 automatically – let Teltonika WRP100 wireless repeater connect to this router automatically.

### 7.4.1.1 Device

#### 7.4.1.1.1 Advanced Settings



Mode: 802.11g+n ▼

Country code: 00 - World ▼

Transmit power: 100 % ▼

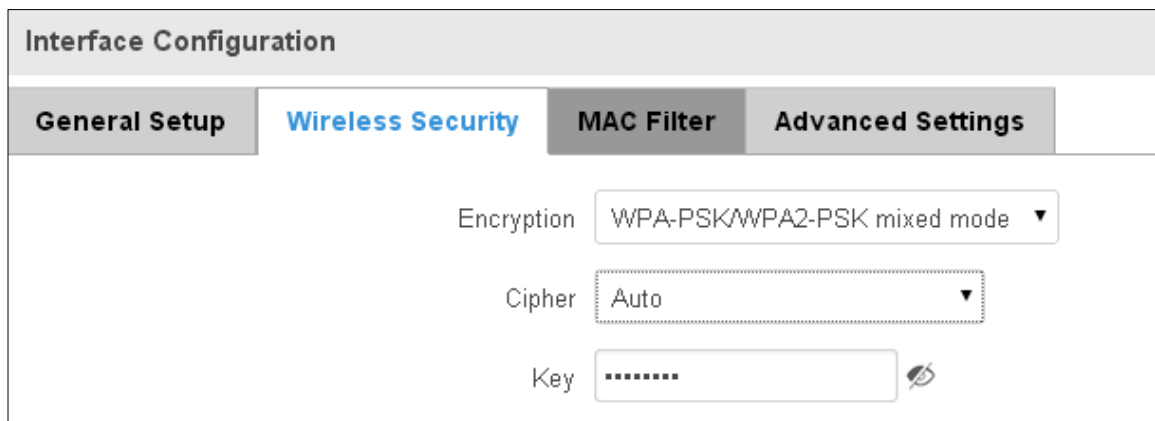
Here you can configure more advanced parameters:

| 1. | Mode                    | Auto, b, g, g+n                      | Different modes provide different throughput and security options.  |
|----|-------------------------|--------------------------------------|---|
| 2. | Country Code            | Any ISO/IEC 3166 alpha2 country code | Selecting this will help the wireless radio configure it's internal parameters to meet your country's wireless regulations.   |
| 3. | Transmit power          | 20%/40%/60%/80%/100%                 | Select Wi-Fi signal power   |
| 4. | Fragmentation threshold | 2346                                 | The smallest packet size that can be fragmented and transmitted by multiple frames. In areas where interference is a problem, setting a lower fragment threshold might help reduce the probability of unsuccessful packet transfers, thus increasing speed. |
| 5. | RTS/CTS Threshold       | 2346                                 | Request to send threshold. It can help resolve problems that arise when several access points are in the same area, contending.   |

### 7.4.1.2 Interface

#### 7.4.1.2.1 Security

Encryption - there are many modes of encryption, a distinctive class is pointed out below.



**Interface Configuration**

General Setup | **Wireless Security** | MAC Filter | Advanced Settings

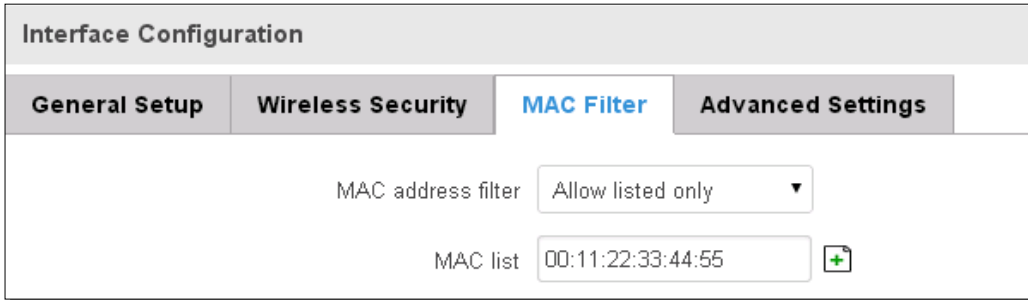
Encryption: WPA-PSK/WPA2-PSK mixed mode ▼

Cipher: Auto ▼

Key: ..... 🔒

First select an encryption method: TKIP, CCMP, TKIP&CCMP and auto. Note: Some authentication methods won't support TKIP (and TKIP&CCMP) encryption. After you've selected your encryption method, you should enter your pass phrase, which must be at least 8 characters long.

#### 7.4.1.2.2 MAC-Filter

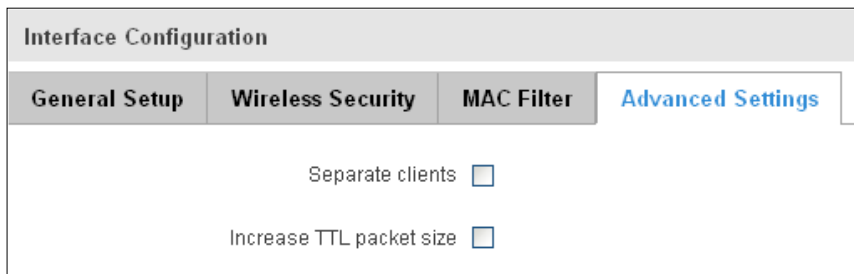


Filter - you can define a rule for what to do with the MAC list you've defined. You can either allow only the listed MACs or allow ALL, but forbid the listed ones.

#### 7.4.1.2.3 Advanced settings

Separate clients - prevents Wi-Fi clients from communicating with each other on the same subnet.

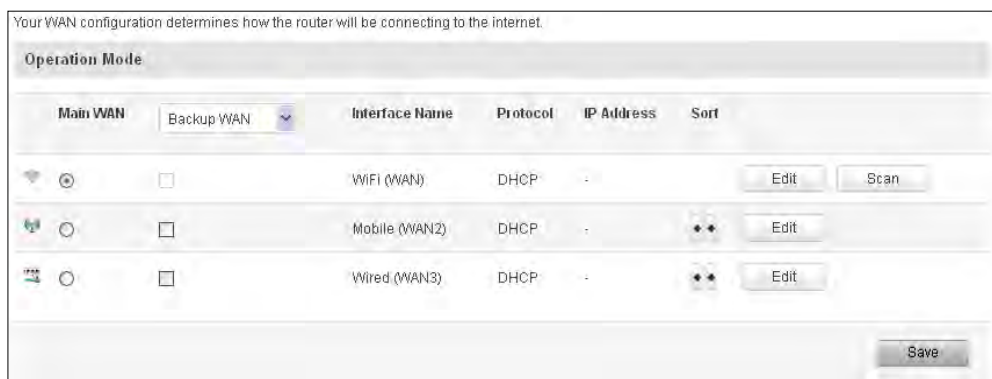
Increase TTL packet size - increase TTL packet size for incoming packets.



#### 7.4.1.3 Client

RUT230 can work as a Wi-Fi client. Client mode is nearly identical to AP, except for the fact that most of the options are dictated by the wireless access point that the router is connecting to. Changing them can result in an interrupted connection to an AP.

In addition to standard options you can also click the **Scan** button to re-scan the surrounding area to attempt to connect to a new wireless access point.



## 7.5 VLAN

On this page you can configure your Virtual LAN settings.

### 7.5.1 VLAN Networks

#### 7.5.1.1 VLAN Functionality

|    |           |                      |   |
|----|-----------|----------------------|---|
| 1. | VLAN mode | Disabled / Tag based | Lets the user choose the VLAN mode or disable VLAN functionality. |
|----|-----------|----------------------|---|

#### 7.5.1.2 VLAN mode – Tag based:

|    |                        |                    |   |
|----|------------------------|--------------------|---|
| 1. | VLAN ID                | 2                  | VLAN Identification number, allowed in range (1-4094)             |
| 3. | Wireless access points | Enabled / Disabled | Assign selected access point(s) to selected LAN.                  |
| 4. | LAN                    | None               | Select to which LAN the wireless access point(s) will be applied. |

### 7.5.2 LAN Networks

In this page you can create extra LAN networks, and assign them with LAN Ports and wireless access points. You can get extra information on how to configure any of your LAN's settings in section – 7.3 LAN

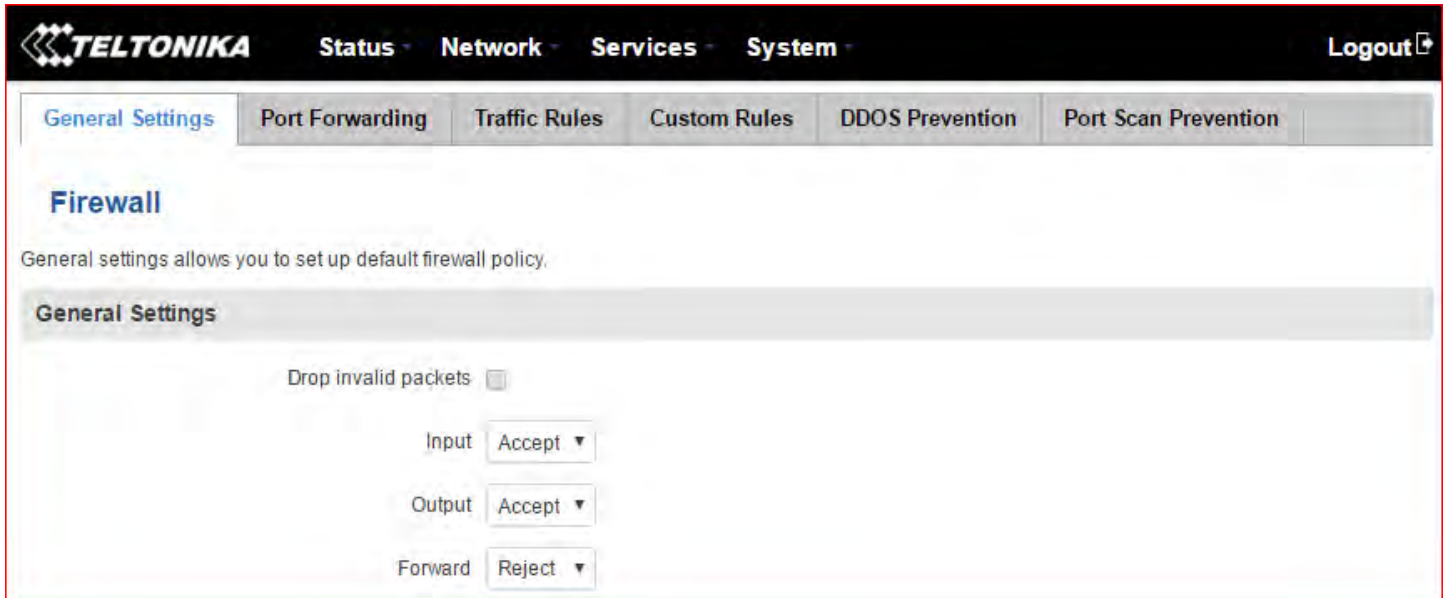
|    |                |           |                              |
|----|----------------|-----------|------------------------------|
| 1. | LAN name       | Lan       | Specifies new LAN name       |
| 2. | Interface name | eth0 tap0 | Specifies LAN interface name |

## 7.6 Firewall

In this section we will look over the various firewall features that come with RUT230.

### 7.6.1 General Settings

The router's firewall is a standard Linux iptables package, which uses routing chains and policies to facilitate control over inbound and outbound traffic.



| 1. | Drop Invalid packets | Checked/Unchecked  | A "Drop" action is performed on a packet that is determined to be invalid                |
|----|----------------------|--------------------|--|
| 2. | Input                | Reject/Drop/Accept | DEFAULT* action that is to be performed for packets that pass through the Input chain.   |
| 3. | Output               | Reject/Drop/Accept | DEFAULT* action that is to be performed for packets that pass through the Output chain.  |
| 4. | Forward              | Reject/Drop/Accept | DEFAULT* action that is to be performed for packets that pass through the Forward chain. |

\*DEFAULT: When a packet goes through a firewall chain it is matched against all the rules for that specific chain. If no rule matches said packet, an according Action (either Drop or Reject or Accept) is performed.

Accept – Packet gets to continue down the next chain.

Drop – Packet is stopped and deleted.

Reject – Packet is stopped, deleted and, differently from Drop, an ICMP packet containing a message of rejection is sent to the **source** of the dropped packet.

### 7.6.2 DMZ

### DMZ Configuration

Enable

DMZ host IP address

By enabling DMZ for a specific internal host (e.g.: your computer), you will expose that host and it's services to the router's WAN network (i.e. - internet).

### 7.6.3 Port Forwarding

Here you can define your own port forwarding rules.

### Firewall - Port Forwarding

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

#### Port Forwarding Rules

| Name                         | Protocol | Source               | Via                           | Destination                               | Enable                   | Sort |                |
|------------------------------|----------|----------------------|-------------------------------|---|--------------------------|------|----------------|
| Enable_SSH_WAN_PASSTHROUGH   | TCP      | From any host in wan | To any router IP at port 22   | Forward to IP 127.0.0.1, port 22 in lan   | <input type="checkbox"/> | ♦♦   | Edit<br>Delete |
| Enable_HTTP_WAN_PASSTHROUGH  | TCP      | From any host in wan | To any router IP at port 80   | Forward to IP 127.0.0.1, port 80 in lan   | <input type="checkbox"/> | ♦♦   | Edit<br>Delete |
| Enable_HTTPS_WAN_PASSTHROUGH | TCP      | From any host in wan | To any router IP at port 443  | Forward to IP 127.0.0.1, port 443 in lan  | <input type="checkbox"/> | ♦♦   | Edit<br>Delete |
| Enable_CLI_WAN_PASSTHROUGH   | TCP      | From any host in wan | To any router IP at port 4200 | Forward to IP 127.0.0.1, port 4200 in lan | <input type="checkbox"/> | ♦♦   | Edit<br>Delete |

#### New Port Forward Rule

| Name  | Protocol | External port (s)                  | Internal IP                                | Internal port (s)                  |                                    |
|---|----------|------------------------------------|--|------------------------------------|------------------------------------|
| <input type="text" value="Enable_Test_Rule"/> | TCP+UDP  | <input type="text" value="12345"/> | <input type="text" value="192.168.1.109"/> | <input type="text" value="12345"/> | <input type="button" value="Add"/> |

You can use port forwarding to set up servers and services on local LAN machines. The above picture shows how you can set up a rule that would allow a website that is being hosted on 192.168.1.109, to be reached from the outside by entering <http://routersExternallp:12345/>.

|    |                     |                                      |  |
|----|---------------------|--------------------------------------|--|
| 1. | Name                | Enable_SSH_WAN_PASSTHROUGH           | Name of the rule. Used purely to make it easier to manage rules.                                     |
| 2. | Protocol            | TCP/UDP/TCP+UDP/Other                | The type of protocol of the incoming packet.   |
| 3. | External Port       | 1-65535                              | The traffic will be forwarded from this port of the WAN network.                                     |
| 4. | Internal IP address | IP address of a computer on your LAN | The IP address of the internal machine that hosts a service that we want to access from the outside. |
| 5. | Internal port       | 1-65535                              | The rule will redirect the traffic to that port of the internal machine.                             |

When you click **edit** you can fine tune a rule to near perfection, if you should desire that.

This page allows you to change advanced properties of the port forwarding entry. Although, in most cases there is no need to modify those settings.

Enable

Name: Enable\_SSH\_WAN\_PAS

Protocol: TCP

Source zone:  lan: lan  vpn: openvpn: gre tunnel  wan: wan: ppp

Source MAC address: any

Source IP address: any

Source port: any

External IP address: any

External port: 22

Internal zone:  lan: lan  vpn: openvpn: gre tunnel  wan: wan: ppp

Internal IP address: 127.0.0.1

Internal port: any

Enable NAT loopback:

Extra arguments:

|    |                     |                                 |   |
|----|---------------------|---------------------------------|---|
| 1. | Name                | ENABLE_SSH_WAN_PASSTHROUGH      | Name of the rule. Used purely to make it easier to manage rules.                                    |
| 2. | Protocol            | TCP/UDP/TCP+<br>UDP/ICMP/Custom | You may specify multiple by selecting (custom) and then entering protocols separated by space       |
| 3. | Source zone         | LAN/VPN/WAN                     | Match incoming traffic from this zone only  |
| 4. | Source MAC address  | any                             | Match incoming traffic from these MACs only   |
| 5. | Source IP address   | any                             | Match incoming traffic from this IP or range only   |
| 7. | Source port         | any                             | Match incoming traffic originating from the given source port or port range on the client host only |
| 8. | External IP address | any                             | Match incoming traffic directed at the given IP   |



|     |                     |                |   |
|-----|---------------------|----------------|---|
|     |                     |                | address only  |
| 9.  | External port       | 22             | Match incoming traffic directed at the given destination port or port range on this host only   |
| 10. | Internal zone       | LAN/VPN/WAN    | Redirect matched incoming traffic to the specified internal zone  |
| 11. | Internal IP address | 127.0.0.1      | Redirect matched incoming traffic to the specified internal host  |
| 12. | Internal port       | any            | Redirect matched incoming traffic to the given port on the internal host  |
| 13. | Enable NAT loopback | Enable/Disable | NAT loopback enables your local network (i.e. behind your router/modem) to connect to a forward-facing IP address (such as 208.112.93.73) of a machine that it also on your local network |
| 14. | Extra arguments     |                | Passes additional arguments to iptables. Use with care!   |

### 7.6.4 Traffic Rules

The traffic rule page contains a more generalized rule definition. With it you can block or open ports, alter how traffic is forwarded between LAN and WAN and many more things.

**TELTONIKA** Status Network Services System Logout

General Settings Port Forwarding **Traffic Rules** Custom Rules DDOS Prevention Port Scan Prevention

### Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

| Name              | Protocol                    | Source               | Destination                                  | Action       | Enable                              | Sort            |
|-------------------|-----------------------------|----------------------|--|--------------|-------------------------------------|-----------------|
| Allow-DHCP-Relay  | UDP                         | From any host in wan | To any router IP at port 67 on this device   | Accept input | <input type="checkbox"/>            | ↑ ↓ Edit Delete |
| Allow-DHCP-Renew  | UDP                         | From any host in wan | To any router IP at port 68 on this device   | Accept input | <input checked="" type="checkbox"/> | ↑ ↓ Edit Delete |
| Allow-Ping        | ICMP with type echo-request | From any host in wan | To any router IP on this device              | Accept input | <input checked="" type="checkbox"/> | ↑ ↓ Edit Delete |
| Allow-vpn-traffic | TCP, UDP                    | From any host in wan | To any router IP at port 1194 on this device | Accept input | <input checked="" type="checkbox"/> | ↑ ↓ Edit Delete |

|    |             |   |
|----|-------------|---|
| 1. | Name        | Name of the rule. Used for easier rules management purpose only   |
| 2. | Protocol    | Protocol type of incoming or outgoing packet  |
| 3. | Source      | Match incoming traffic from this IP or range only   |
| 4. | Destination | Redirect matched traffic to the given IP address and destination port   |
| 5. | Action      | Action to be taken for the packet if it matches the rule  |
| 6. | Enable      | Self-explanatory. Uncheck to make the rule inactive. The rule will not be deleted, but it also will not be loaded into the firewall.  |
| 7. | Sort        | When a packet arrives, it gets checked for a matching rule. If there are several rules that match the rule, the first one is applied i.e. the order of the rule list impacts how your firewall operates, therefore you are given the ability to sort your list as you wish. |

You can configure firewall rule by clicking **edit** button.

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Enable

Name: Allow-DHCP-Relay

Restrict to address family: IPv4 and IPv6

Protocol: UDP

Match ICMP type: any

Source zone:
 Anyzone
 lan: lan:
 vpn: openvpn: gre tunnel:
 wan: wan: ppp:

Source MAC address: any

Source address: any

Source port: any

Destination zone:
 Device (input)
 Anyzone (forward)
 lan: lan:
 vpn: openvpn: gre tunnel:
 wan: wan: ppp:

Destination address: any

Destination port: 67

Action: accept

Extra arguments:

|    |                            |                         |   |
|----|----------------------------|-------------------------|---|
| 1. | Name                       | “Allow-DHCP-Relay”      | Used to make rule management easier                                 |
| 2. | Restrict to address family | IPv4 and IPV6           | Match traffic from selected address family only                     |
| 3. | Protocol                   | TCP/UDP/Any/ICMP/Custom | Protocol of the packet that is being matched against traffic rules. |
| 4. | Match ICMP type            | any                     | Match traffic with selected ICMP type only                          |
| 5. | Source zone                | any zone/LAN/VPN/WAN    | Match incoming traffic from this zone only                          |

|     |                     |   |   |
|-----|---------------------|---|---|
| 6.  | Source MAC address  | any   | Match incoming traffic from these MACs only   |
| 7.  | Source address      | any   | Match incoming traffic from this IP or range only   |
| 8.  | Source port         | any   | Match incoming traffic originating from the given source port or port range on the client host only   |
| 9.  | Destination zone    | Device/Any zone/LAN/VPN/WAN                   | Match forwarded traffic to the given destination zone only  |
| 10. | Destination address | any   | Match forwarded traffic to the given destination IP address or IP range only  |
| 11. | Destination port    | 67  | Match forwarded traffic to the given destination port or port range only  |
| 12. | Action              | Drop/Accept/Reject + chain + additional rules | Action to be taken on the packet if it matches the rule. You can also define additional options like limiting packet volume, and defining to which chain the rule belongs |

#### 7.6.4.1 Open Ports On the Router

**Open Ports On Router**

| Name  | Protocol                                     | External port                   |                                    |
|---|--|---------------------------------|------------------------------------|
| <input type="text" value="Open_Port_rule"/> | TCP <span style="font-size: small;">▼</span> | <input type="text" value="22"/> | <input type="button" value="Add"/> |

| 1. | Name          | Open_Port_rule          | Used to make rule management easier   |
|----|---------------|-------------------------|---|
| 2. | Protocol      | TCP/UDP/Any/ICMP/Custom | Protocol of the packet that is being matched against traffic rules.                       |
| 3. | External port | 1-65535                 | Match incoming traffic directed at the given destination port or port range on this host. |

#### 7.6.4.2 New Forward Rule

**New Forward Rule**

| Name  | Source                                       | Destination                                  |                                    |
|---|--|--|------------------------------------|
| <input type="text" value="Forward rule new"/> | LAN <span style="font-size: small;">▼</span> | WAN <span style="font-size: small;">▼</span> | <input type="button" value="Add"/> |

| 1. | Name     | Forward rule new        | Used to make rule management easier                                 |
|----|----------|-------------------------|---|
| 2. | Source   | LAN/VPN/WAN             | Match incoming traffic from selected address family only            |
| 3. | Protocol | TCP/UDP/Any/ICMP/Custom | Protocol of the packet that is being matched against traffic rules. |

### 7.6.4.3 Source NAT

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

**Source NAT**

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

| Name | Protocol | Source               | Destination                 | SNAT                                      | Enable                              |   |
|------|----------|----------------------|-----------------------------|---|-------------------------------------|---|
| SNAT | TCP+UDP  | From any host in lan | To any host, port 22 in wan | Rewrite to source IP 10.101.1.10, port 22 | <input checked="" type="checkbox"/> | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

---

**New Source NAT**

| Name                                       | Source                               | Destination                          | Source IP            | Source port                                   |                                    |
|--|--------------------------------------|--------------------------------------|----------------------|---|------------------------------------|
| <input type="text" value="New SNAT rule"/> | <input type="button" value="LAN"/> ▾ | <input type="button" value="WAN"/> ▾ | <input type="text"/> | <input type="button" value="Do not rewrite"/> | <input type="button" value="Add"/> |

| #  | Name        | Value                            | Description   |
|----|-------------|----------------------------------|---|
| 1. | Name        | SNAT                             | Used to make rule management easier   |
| 2. | Protocol    | TCP/UDP/Any/ICMP/Custom          | Protocol of the packet that is being matched against traffic rules.                   |
| 3. | Source      | LAN/VPN/WAN                      | Match incoming traffic from selected address family only                              |
| 4. | Destination | LAN/VPN/WAN                      | Forward incoming traffic to selected address family only                              |
| 5. | SNAT        | Rewrite to source IP 10.101.1.10 | SNAT (Source Network Address Translation) rewrite packet's source IP address and port |
| 6. | Enable      | Enable/Disable                   | Make a rule active/inactive   |

You can configure firewall source NAT rule, by clicking **edit** button.

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Enable

Name: SNAT

Protocol: All protocols

Source zone:
 

- lan: lan
- vpn: openvpn gre tunnel
- wan: wan ppp

Source MAC address: any

Source IP address: any

Source port: any

Destination zone:
 

- lan: lan
- vpn: openvpn gre tunnel
- wan: wan ppp

Destination IP address: [dropdown]

Destination port: any

SNAT IP address: 10.101.1.10

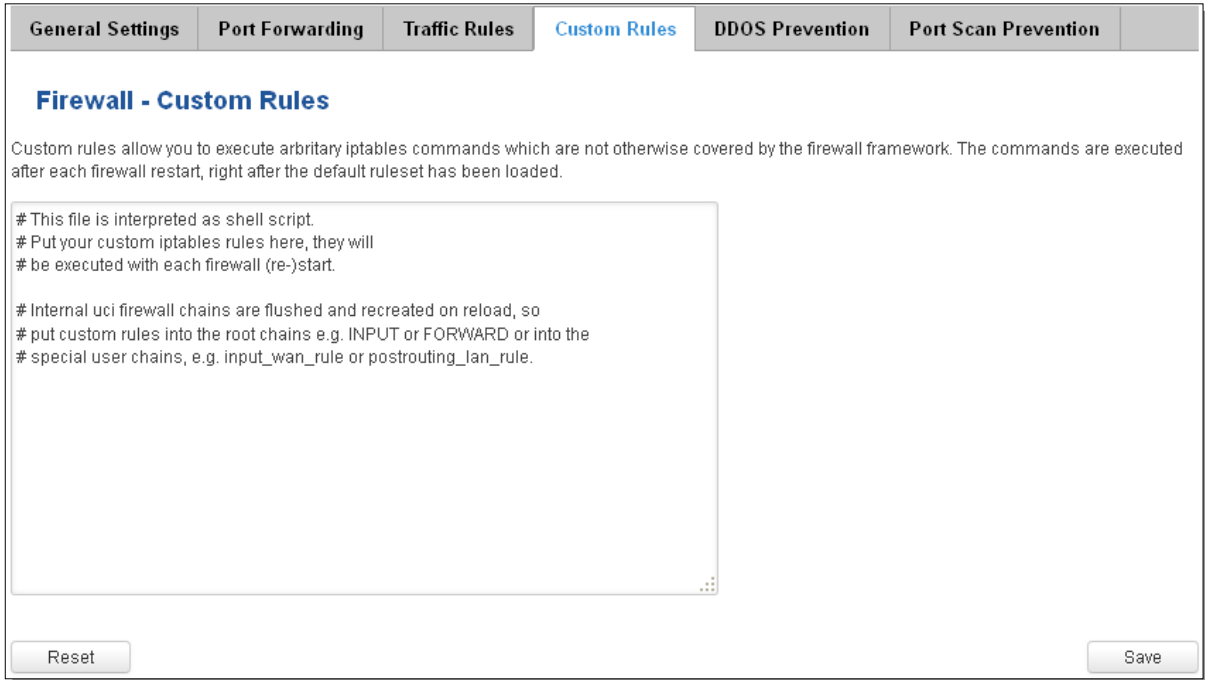
SNAT port: 22

Extra arguments: [text box]

| 1.  | Name                   | SNAT                    | Used to make rule management easier   |
|-----|------------------------|-------------------------|---|
| 2.  | Protocol               | TCP/UDP/Any/ICMP/Custom | Protocol of the packet that is being matched against traffic rules.                                 |
| 3.  | Source zone            | LAN/VPN/WAN             | Match incoming traffic from this zone only  |
| 4.  | Source MAC address     | any                     | Match incoming traffic from these MACs only   |
| 5.  | Source address         | any                     | Match incoming traffic from this IP or range only   |
| 6.  | Source port            | any                     | Match incoming traffic originating from the given source port or port range on the client host only |
| 7.  | Destination zone       | LAN/VPN/WAN             | Match forwarded traffic to the given destination zone only  |
| 8.  | Destination IP address | Select from the list    | Match forwarded traffic to the given destination IP address or IP range only                        |
| 9.  | Destination port       | any                     | Match forwarded traffic to the given destination port or port range only                            |
| 10. | SNAT IP address        | "10.101.1.10"           | Rewrite matched traffic to the given IP address   |
| 11. | SNAT port              | "22"                    | Rewrite matched traffic to the given source port. May be left empty to only rewrite the IP address' |
| 12. | Extra arguments        |                         | Passes additional arguments to iptables. Use with care!   |

## 7.6.5 Custom Rules

Here you have the ultimate freedom in defining your rules – you can enter them straight into the iptables program. Just type them out into the text field and it will get executed as a Linux shell script. If you are unsure of how to use iptables, check out the internet for manuals, examples and explanations.



**Firewall - Custom Rules**

Custom rules allow you to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default ruleset has been loaded.

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

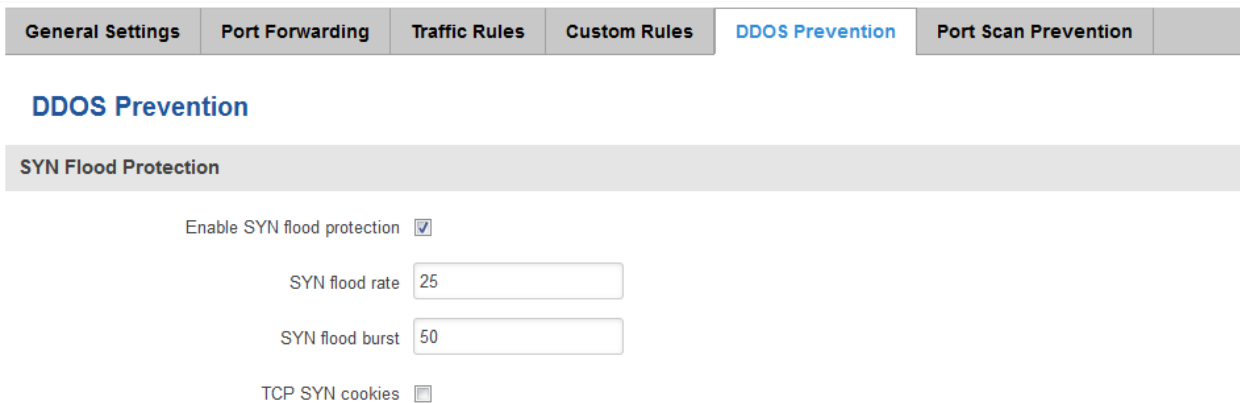
# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.
```

Reset Save

## 7.6.6 DDOS Prevention

### 7.6.6.1 SYN Flood Protection

SYN Flood Protection allows you to protect your router from attacks that exploit part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive. Essentially, with SYN flood DDoS, the offender sends TCP connection requests faster than the targeted machine can process them, causing network saturation.



**DDOS Prevention**

**SYN Flood Protection**

Enable SYN flood protection

SYN flood rate

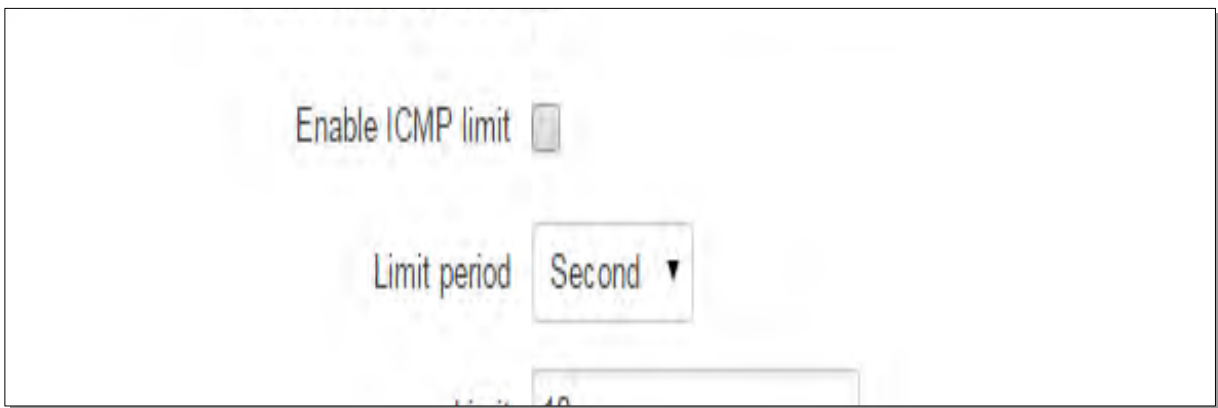
SYN flood burst

TCP SYN cookies

| 1. | Enable SYN flood protection | Enable/Disable | Makes router more resistant to SYN flood attacks.   |
|----|-----------------------------|----------------|---|
| 2. | SYN flood rate              | "25"           | Set rate limit (packets/second) for SYN packets above which the traffic is considered flooded.                |
| 3. | SYN flood burst             | "50"           | Set burst limit for SYN packets above which the traffic is considered flooded if it exceeds the allowed rate. |
| 4. | TCP SYN cookies             | Enable/Disable | Enable the use of SYN cookies (particular choices of initial TCP sequence numbers by TCP servers).            |

### 7.6.6.2 Remote ICMP requests

Attackers are using ICMP echo request packets directed to IP broadcast addresses from remote locations to generate denial-of-service attacks.



| 1. | Enable ICMP requests | Enable/Disable         | Blocks remote ICMP echo-request type                          |
|----|----------------------|------------------------|---|
| 2. | Enable ICMP limit    | Enable/Disable         | Enable ICMP echo-request limit in selected period             |
| 3. | Limit period         | Second/Minute/Hour/Day | Select in what period limit ICMP echo-request                 |
| 4. | Limit                | "10"                   | Maximum ICMP echo-requests during the period                  |
| 5. | Limit burst          | "5"                    | Indicating the maximum burst before the above limit kicks in. |

### 7.6.6.3 SSH Attack Prevention

Prevent SSH (allows a user to run commands on a machine's command prompt without them being physically present near the machine.) attacks by limiting connections in a defined period.



|    |                  |                        |   |
|----|------------------|------------------------|---|
| 1. | Enable SSH limit | Enable/Disable         | Enable SSH connections limit in selected period               |
| 2. | Limit period     | Second/Minute/Hour/Day | Select in what period limit SSH connections                   |
| 3. | Limit            | "10"                   | Maximum SSH connections during the period                     |
| 4. | Limit burst      | "5"                    | Indicating the maximum burst before the above limit kicks in. |

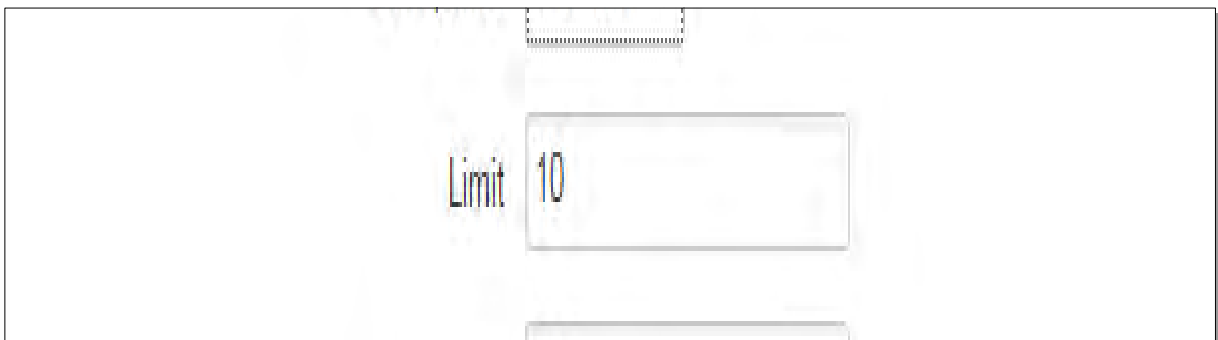
#### 7.6.6.4 HTTP Attack Prevention

HTTP attacks send a complete, legitimate HTTP header, which includes a 'Content-Length' field to specify the size of the message body to follow. However, the attacker then proceeds to send the actual message body at an extremely slow rate (i.e. 1 byte/110 seconds). Due to the entire message being correct and complete, the target server will attempt to obey the 'Content-Length' field in the header, and wait for the entire body of the message to be transmitted, hence slowing it down.



|    |                   |                        |   |
|----|-------------------|------------------------|---|
| 1. | Enable HTTP limit | Enable/Disable         | Limits HTTP connections per period                            |
| 2. | Limit period      | Second/Minute/Hour/Day | Select in what period limit HTTP connections                  |
| 3. | Limit             | "10"                   | Maximum HTTP connections during the period                    |
| 4. | Limit burst       | "10"                   | Indicating the maximum burst before the above limit kicks in. |

#### 7.6.6.5 HTTPS Attack Prevention





|    |                    |                        |  |
|----|--------------------|------------------------|--|
| 1. | Enable HTTPS limit | Enable/Disable         | Limits HTTPS connections per period              |
| 2. | Limit period       | Second/Minute/Hour/Day | Select in what period to limit HTTPS connections |
| 3. | Limit              | "10"                   | Maximum HTTPS connections during the period      |
| 4. | Limit burst        | "10"                   | Indicating the maximum burst                     |

## 7.6.7 Port Scan Prevention

### 7.6.7.1 Port Scan

**Port Scan**

Enable

Interval

Scan count

|    |            |                |   |
|----|------------|----------------|---|
| 1. | Enable     | Enable/Disable | Enable port scan prevention   |
| 2. | Interval   | 30             | Time interval in seconds counting the length of the scan (10 - 60 sec.) |
| 3. | Scan count | 10             | How many port scans before blocked                                      |

### 7.6.7.2 Defending type

**Defending type**

SYN-FIN attack

SYN-RST attack

X-Mas attack

FIN scan

NULLflags attack

|    |                  |                               |
|----|------------------|-------------------------------|
| 1. | SYN-FIN attack   | Protect from SYN-FIN attack   |
| 2. | SYN-RST attack   | Protect from SYN-RST attack   |
| 3. | X-Mas attack     | Protect from X-Mas attack     |
| 4. | FIN scan         | Protect from FIN scan         |
| 5. | NULLflags attack | Protect from NULLflags attack |

## 7.7 Routing

### 7.7.1 Static Routes

Static routes specify over which interface and gateway a certain host or network can be reached.

| 1. | Routing table       | MAIN/WAN/WAN2/WAN3 | Defines the table to use for the route   |
|----|---------------------|--------------------|--|
| 2. | Interface           | MAIN/WAN/WAN2/WAN3 | The zone where the target network resides  |
| 3. | Destination address | IP address         | The address of the destination network   |
| 4. | Netmask             | IP mask            | Mask that is applied to the Target to determine what actual IP addresses the routing rule applies                    |
| 5. | Gateway             | IP address         | Where the router should send all the traffic that applies to the rule  |
| 6. | Metric              | integer            | Used as a sorting measure. If a packet about to be routed fits two rules, the one with the higher metric is applied. |

Additional note on Target & Netmask: You can define a rule that applies to a single IP like this: Target - some IP; Netmask - 255.255.255.255. Furthermore you can define a rule that applies to a segment of IPs like this: Target - an IP that STARTS the segment; Netmask - Netmask that defines how large the segment is. E.g.:

|                       |                        |   |
|-----------------------|------------------------|---|
| <b>192.168.55.161</b> | <b>255.255.255.255</b> | <b>Only applies to 192.168.55.161</b>               |
| 192.168.55.0          | 255.255.255.0          | Applies to IPs in range 192.168.55.0-192.168.55.255 |
| 192.168.55.240        | 255.255.255.240        | Applies 192.168.55.240 - 192.168.55.255             |
| 192.168.55.161        | 255.255.255.0          | 192.168.55.0 - 192.168.55.255                       |
| 192.168.0.0           | 255.255.0.0            | 192.168.0.0 - 192.168.255.255                       |

## 7.7.2 Dynamic Routes

### 7.7.2.1 General

Dynamic routes provide dynamic routing which enables the router to select paths according to real-time logical network layout changes.

The screenshot shows a configuration interface for Dynamic Routes. It has two main tabs: 'Static Routes' and 'Dynamic Routes'. The 'Dynamic Routes' tab is active. Below this, there are three sub-tabs: 'General', 'OSPF Protocol', and 'General Protocols'. The 'General' sub-tab is selected. The main heading is 'Dynamic Routes'. Underneath, there is a section for 'General Settings'. In this section, there is an 'Enable' checkbox which is currently unchecked. Below that is a 'Router ID' field containing the value '192.168.1.1'. At the bottom right of the configuration area, there is a 'Save' button.

|    |           |                |                       |
|----|-----------|----------------|-----------------------|
| 1. | Enable    | Enable/Disable | Enable dynamic routes |
| 2. | Router ID | 192.168.1.1    | Router's ID           |

### 7.7.2.2 OSPF Protocol

#### 7.7.2.2.1 OSPF General Instance

The screenshot shows the 'OSPF Protocol Configuration' page. It has three tabs: 'General', 'OSPF Protocol', and 'General Protocols'. The 'OSPF Protocol' tab is active. The main heading is 'OSPF Protocol Configuration'. Below this, there is a section for 'OSPF General Instance'. In this section, there are several settings: 'Enable' (unchecked checkbox), 'Stub' (unchecked checkbox), 'RFC1583 compatibility' (unchecked checkbox), 'Import' (dropdown menu set to 'All'), and 'Export' (dropdown menu set to 'All').

|    |                       |                 |   |
|----|-----------------------|-----------------|---|
| 1. | Enable                | Enable/Disable  | Enables OSPF protocol                                 |
| 2. | Stub                  | Enable/Disable  | Enable/Disable stub                                   |
| 3. | RFC1583 compatibility | Enable/Disable  | Enables OSPF compatibility with RFC1583 specification |
| 4. | Import                | All/None/custom | Set if the protocol must import routes                |
| 5. | Export                | All/None/custom | Set if the protocol must export routes                |

### 7.7.2.2 OSPF Area

The OSPF network can be divided into sub-domains called areas.

| OSPF Area |        |
|-----------|--------|
| Area name | Enable |
| OSPF_area | No     |

New area name:

|    |           |           |                          |
|----|-----------|-----------|--------------------------|
| 1. | Area name | OSPF_area | OSPF area's name         |
| 2. | Enable    | Yes/No    | Enable/disable OSPF area |

To see at specific configuration settings press **“edit”** button located in newly created OSPF area. A new page with detailed configuration appears, as shown in the picture below.

**Area Instance: OSPF\_area**

**Main Settings**

Enabled

Stub

**OSPF interface**

**Interface**

*There are no interfaces created yet*

Interface:

**OSPF networks**

**IP**

*There are no networks created yet*

New IP:

|    |           |                |   |
|----|-----------|----------------|---|
| 1. | Enabled   | Enable/Disable | Enable specific OSPF area   |
| 2. | Stub      | Enable/Disable | Enable/disable stub   |
| 3. | Interface | br-lan         | The interface that the new instance will have   |
| 4. | New IP    |                | Name of the new OSPF network configuration. Used for easier configuration management purpose only |

### 7.7.2.3 General Protocol

The screenshot shows the 'General Protocols Configuration' window. At the top, there are three tabs: 'General', 'OSPF Protocol', and 'General Protocols'. The 'General Protocols' tab is active. Below the tabs, the title 'General Protocols Configuration' is displayed. The interface is divided into two main sections: 'Kernel Options' and 'Device Options'.  
 In the 'Kernel Options' section, there are three checkboxes: 'Enable', 'Learn', and 'Persist', all of which are currently unchecked. Below these is a 'Scan time' input field with the value '20'. There are also two dropdown menus: 'Import' and 'Export', both of which are currently set to 'All'.  
 In the 'Device Options' section, there is an 'Enable' checkbox which is unchecked, and a 'Scan time' input field with the value '10'.

|    |           |                |  |
|----|-----------|----------------|--|
| 1. | Enable    | Enable/Disable | Enable/Disable settings  |
| 2. | Learn     | Enable/Disable | Enables route learning   |
| 3. | Persist   | Enable/Disable | If checked it allows route storing. After a restart, routes will still be configured |
| 4. | Scan time | 20             | Time between scans   |
| 5. | Import    | All            | Set if the protocol must import routes   |
| 6. | Export    | All            | Set if the protocol must export routes   |
| 7. | Enable    | Enable/Disable | If checked the protocol will not be configured                                       |
| 8. | Scan time | 10             | Time between scans   |

#### 7.7.2.3.1 Static Routes

The screenshot shows the 'Static Routes' configuration window. At the top, the title 'Static Routes' is displayed. Below the title, there is a table with two columns: 'Prefix' and 'Type'. The table is currently empty, and a message below it reads 'There are no static routes created yet'. Below the table, there is a section titled 'New Static Route'. This section contains two input fields: 'Prefix' and 'Type'. The 'Type' dropdown menu is currently set to 'Router'. To the right of these fields is an 'Add' button. At the bottom right of the window, there is a 'Save' button.

|    |        |   |
|----|--------|---|
| 1. | Prefix | Protocol prefix of an incoming or outgoing packet |
| 2. | Type   | Protocol type of an incoming or outgoing packet   |

## 8 Services

### 8.1 VRRP

#### 8.1.1 VRRP LAN Configuration Settings

**VRRP LAN Configuration Settings**

Enable

IP address

Virtual ID

Priority

| 1. | Enable     | Enable/Disable | Enable VRRP (Virtual Router Redundancy Protocol) for LAN   |
|----|------------|----------------|--|
| 2. | IP address | 192.168.1.253  | Virtual IP address for LAN's VRRP (Virtual Router Redundancy Protocol) cluster   |
| 3. | Virtual ID | 1              | Routers with same IDs will be grouped in the same VRRP (Virtual Router Redundancy Protocol) cluster, range [1-255]                   |
| 4. | Priority   | 100            | Router with highest priority value on the same VRRP (Virtual Router Redundancy Protocol) cluster will act as a master, range [1-255] |

#### 8.1.2 Check Internet connection

Ping IP address

Ping interval

Ping timeout (sec)

Ping packet size

Ping retry count

| 1. | Enable             | Enable/Disable | Enable WAN's connection monitoring  |
|----|--------------------|----------------|---|
| 2. | Ping IP address    | 8.8.4.4        | A host to send ICMP (Internet Control Message Protocol) packets to                          |
| 3. | Ping interval      | 10             | Time interval in seconds between two Pings  |
| 4. | Ping timeout (sec) | 1              | Response timeout value, interval [1 - 9999]   |
| 5. | Ping packet size   | 50             | ICMP (Internet Control Message Protocol) packet's size, interval [0 - 1000]                 |
| 6. | Ping retry count   | 100            | Failed Ping attempt's count before determining that connection is lost, interval [1 - 9999] |

## 8.2 Web Filter

### 8.2.1 Site blocking

| 1. | Enable    | Enable/Disable      | Enable host name based websites blocking  |
|----|-----------|---------------------|---|
| 2. | Mode      | Whitelist/Blacklist | Whitelist - allow every site on the list and block everything else. Blacklist - block every site on the list and allow everything else. |
| 3. | Enable    | Enable/Disable      | Check to enable site blocking   |
| 4. | Host name | www.yahoo.com       | Block/allow site with this hostname   |

### 8.2.2 Proxy Based Content Blocker

| 1. | Enable      | Enable/Disable      | Enable proxy server based URL content blocking. Works with HTTP protocol only  |
|----|-------------|---------------------|--|
| 2. | Mode        | Whitelist/Blacklist | Whitelist - allow every part of URL on the list and block everything else. Blacklist - block every part of URL on the list and allow everything else |
| 3. | URL content | example.com         | Block/allow any URL containing this string. Example.com, example.*, *.example.com  |

## 8.3 NTP

NTP configuration lets you setup and synchronize routers time.

The screenshot shows a configuration page for NTP. At the top, there are two tabs: 'General' and 'Time Servers'. The 'Time Servers' tab is active. Below the tabs is the title 'Time Synchronisation'. Underneath is a sub-section 'General' containing the following fields:

- Current system time: 2016-03-09 08:32:52 (with a 'Sync with browser' button to the right)
- Time zone: UTC (dropdown menu)
- Enable NTP:
- Update interval (in seconds): 3600 (text input)
- Save time to flash:
- Count of time synchronizations: (empty text input)

Below the 'General' section is a sub-section 'Clock Adjustment' containing:

- Offset frequency: 0 (text input)

A 'Save' button is located at the bottom right of the configuration area.

|    |                                |   |
|----|--------------------------------|---|
| 1. | Current System time            | Local time of router.   |
| 2. | Time zone                      | Time zone of your country.  |
| 3. | Enable NTP                     | Enable system's time synchronization with time server using NTP (Network Time Protocol)                         |
| 4. | Update interval                | How often router updates systems time   |
| 5. | Save time to flash             | Save last synchronized time to flash memory   |
| 6. | Count of time synchronizations | Total amount of times that router will do the synchronization. Note: If left blank - the count will be infinite |
| 7. | Offset frequency               | Adjust the minor drift of the clock so that it will be more accurate  |

Note, that under **Time Servers** at least one server has to be present, otherwise NTP will not serve its purposes.

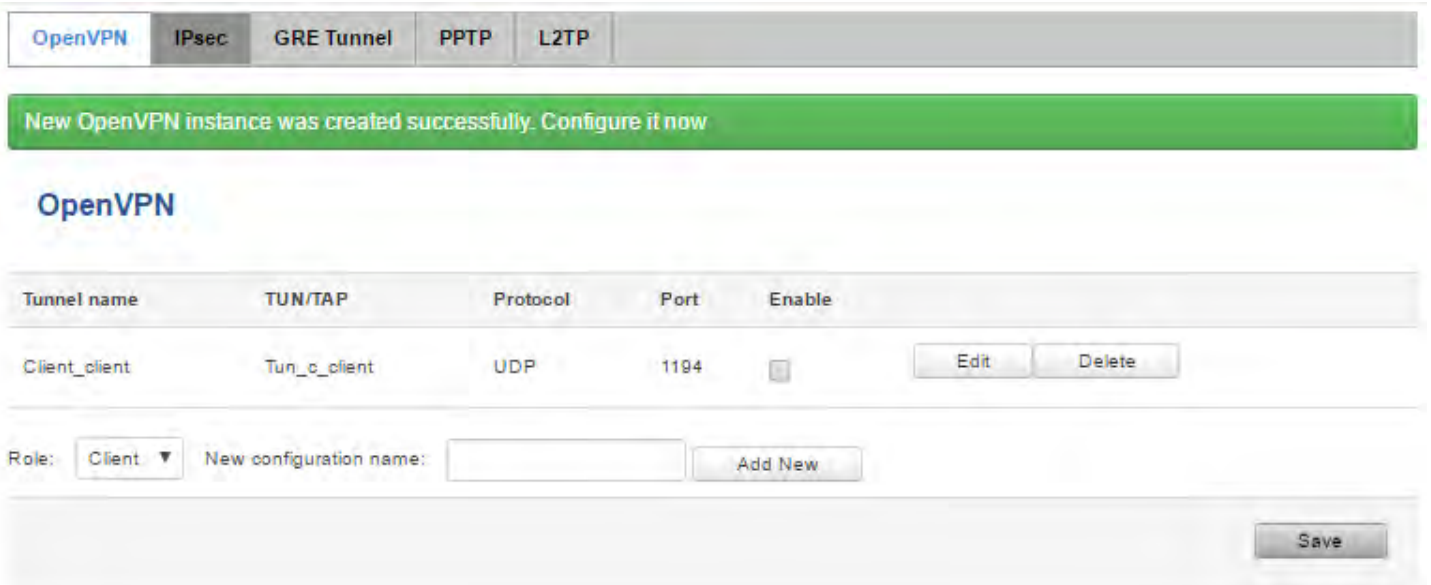


## 8.4 VPN

### 8.4.1 OpenVPN

VPN (Virtual Private Network) is a method for secure data transfer through unsafe public network. This section explains how to configure OpenVPN, which is implementation of VPN supported by the RUT900 router.

A picture below demonstrates default OpenVPN configurations list, which is empty, so you have to define a new configuration to establish any sort of OpenVPN connection. To create it, enter desired configuration name in “**New configuration name**” field, select device role from “**Role**” drop down list. For example, to create an OpenVPN client with configuration name demo, select client role, name it “demo” and press “**Add New**” button as shown in the following picture.



To see at specific configuration settings press “**edit**” button located in newly created configuration entry. A new page with detailed configuration appears, as shown in the picture below (TLS client example).

## OpenVPN Instance: Client\_client

### Main Settings

|                                |   |
|--------------------------------|---|
| Enable                         | <input checked="" type="checkbox"/>                       |
| TUN/TAP                        | TUN (tunnel) ▼  |
| Protocol                       | UDP ▼   |
| Port                           | 1194  |
| LZO                            | <input type="checkbox"/>                                  |
| Encryption                     | BF-CBC 128 (default) ▼                                    |
| Authentication                 | TLS ▼   |
| TLS cipher                     | All ▼   |
| Remote host/IP address         | 84.15.199.20  |
| Resolve retry                  | infinite  |
| Keep alive                     | 10 120  |
| Remote network IP address      | 10.0.0.0  |
| Remote network IP netmask      | 255.255.255.0   |
| Max routes                     | 100   |
| Extra options                  | <input type="text"/>                                      |
| HMAC authentication algorithm  | SHA1 (default) ▼  |
| Additional HMAC authentication | <input type="checkbox"/>                                  |
| Certificate authority          | <input type="button" value="Choose File"/> No file chosen |
| Client certificate             | <input type="button" value="Choose File"/> No file chosen |
| Client key                     | <input type="button" value="Choose File"/> No file chosen |

You can set custom settings here according to your VPN needs. Below is summary of parameters available to set:

| 1.  | Enabled                        | Switches configuration on and off. This must be selected to make configuration active.   |
|-----|--------------------------------|--|
| 2.  | TUN/TAP                        | Selects virtual VPN interface type. TUN is most often used in typical IP-level VPN connections, however, TAP is required to some Ethernet bridging configurations.   |
| 3.  | Protocol                       | Defines a transport protocol used by connection. You can choose here between TCP and UDP.  |
| 4.  | Port                           | Defines TCP or UDP port number (make sure, that this port allowed by firewall).  |
| 5.  | LZO                            | This setting enables LZO compression. With LZO compression, your VPN connection will generate less network traffic; however, this means higher router CPU loads. Use it carefully with high rate traffic or low CPU resources.   |
| 6.  | Encryption                     | Selects Packet encryption algorithm.   |
| 7.  | Authentication                 | Sets authentication mode, used to secure data sessions. Two possibilities you have here: "Static key" means, that OpenVPN client and server will use the same secret key, which must be uploaded to the router using "Static pre-shared key" option. "TLS" authentication mode uses X.509 type certificates. Depending on your selected OpenVPN mode (client or server) you have to upload these certificates to the router:<br>For client: Certificate Authority (CA), Client certificate, Client key.<br>For server: Certificate Authority (CA), Server certificate, Server key and Diffie-Hellman (DH) certificate used to key exchange through unsafe data networks.<br>All mention certificates can be generated using OpenVPN or Open SSL utilities on any type host machine. Certificate generation and theory is out of scope of this user manual. |
| 8.  | TLS cipher                     | Packet encryption algorithm (cipher)   |
| 9.  | Remote host/IP address         | IP address of OpenVPN server (applicable only for client configuration).   |
| 10. | Resolve Retry                  | Sets time in seconds to try resolving server hostname periodically in case of first resolve failure before generating service exception.   |
| 11. | Keep alive                     | Defines two time intervals: one is used to periodically send ICMP request to OpenVPN server, and another one defines a time window, which is used to restart OpenVPN service, if no ICMP request is received during the window time slice. Example Keep Alive "10 60"  |
| 12. | Remote network IP address      | IP address of remote network, an actual LAN network behind another VPN endpoint.   |
| 13. | Remote network IP netmask      | Subnet mask of remote network, an actual LAN network behind another VPN endpoint.  |
| 14. | Max routes                     | Allow a maximum number of routes to be pulled from an OpenVPN server   |
| 15. | HMAC authentication algorithm  | Sets HMAC authentication algorithm   |
| 16. | Additional HMAC authentication | Add an additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks  |
| 17. | Certificate authority          | Certificate authority is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.  |

|     |                    |   |
|-----|--------------------|---|
| 18. | Client certificate | Client certificate is a type of digital certificate that is used by client systems to make authenticated requests to a remote server. Client certificates play a key role in many mutual authentication designs, providing strong assurances of a requester's identity. |
| 19. | Client key         | Authenticating the client to the server and establishing precisely who they are   |

After setting any of these parameters press **“Save”** button. Some of selected parameters will be shown in the configuration list table. You should also be aware of the fact that router will launch separate OpenVPN service for every configuration entry (if it is defined as active, of course) so the router has ability to act as server and client at the same time.

### 8.4.2 IPsec

The IPsec protocol client enables the router to establish a secure connection to an IPsec peer via the Internet. IPsec is supported in two modes - transport and tunnel. Transport mode creates secure point to point channel between two hosts. Tunnel mode can be used to build a secure connection between two remote LANs serving as a VPN solution.

IPsec system maintains two databases: Security Policy Database (SPD) which defines whether to apply IPsec to a packet or not and specify which/how IPsec-SA is applied and Security Association Database (SAD), which contain Key of each IPsec-SA.

The establishment of the Security Association (IPsec-SA) between two peers is needed for IPsec communication. It can be done by using manual or automated configuration.

Note: router starts establishing tunnel when data from router to remote site over tunnel is sent. For automatic tunnel establishment used tunnel Keep Alive feature.

**IPsec Configuration**

|                        |  |
|------------------------|--|
| Enable                 | <input checked="" type="checkbox"/>          |
| IKE version            | <input type="text" value="IKEv1"/>           |
| Mode                   | <input type="text" value="Main"/>            |
| My identifier type     | <input type="text" value="Address"/>         |
| My identifier          | <input type="text" value="100.121.122.123"/> |
| Dead Peer Detection    | <input checked="" type="checkbox"/>          |
| Pre shared key         | <input type="text" value="password"/>        |
| Remote VPN endpoint    | <input type="text" value="215.148.3.15"/>    |
| IP address/Subnet mask | <input type="text" value="192.168.1.0/24"/>  |
| Enable keepalive       | <input checked="" type="checkbox"/>          |
| Host                   | <input type="text" value="192.168.1.125"/>   |
| Ping period (sec)      | <input type="text" value="60"/>              |

|     |                        |                          |  |
|-----|------------------------|--------------------------|--|
| 1.  | Enable                 | Enabled/Disabled         | Check box to enable IPSec.   |
| 2.  | IKE version            | IKEv1 or IKEv2           | Method of key exchange   |
| 3.  | Mode                   | “Main” or “Aggressive”   | ISAKMP (Internet Security Association and Key Management Protocol) phase 1 exchange mode   |
| 4.  | My identifier type     | Address, FQDN, User FQDN | Choose one accordingly to your IPSec configuration   |
| 5.  | My identifier          |                          | Set the device identifier for IPSec tunnel.<br>In case RUT has Private IP, its identifier should be its own LAN network address. In this way, the Road Warrior approach is possible. |
| 6.  | Dead Peer Detection    | Enabled/Disabled         | The values clear, hold and restart all active DPD  |
| 7.  | Pre shared key         |                          | A shared password to authenticate between the peer   |
| 8.  | Remote VPN endpoint    |                          | Domain name or IP address. Leave empty or any  |
| 9.  | IP address/Subnet mask |                          | Remote network secure group IP address and mask used to determine to what subnet an IP address belongs to. Range [0-32]. IP should differ from device LAN IP                         |
| 10. | Enable keep alive      | Enabled/Disabled         | Enable tunnel keep alive function  |
| 11. | Host                   |                          | A host address to which ICMP (Internet Control Message Protocol) echo requests will be send  |
| 12. | Ping period (sec)      |                          | Send ICMP echo request every x seconds. Range [0-999999]   |

**Phase 1** and **Phase 2** must be configured accordingly to the IPSec server configuration, thus algorithms, authentication and lifetimes of each phase must be identical.

**Phase**

The phase must match with another incoming connection to establish IPSec

**Phase 1** **Phase 2**

Encryption algorithm: 3DES

Authentication: SHA1

DH group: MODP1536

Lifetime (h): 8 Minutes

**Phase**

The phase must match with another incoming connection to establish IPSec

**Phase 1** **Phase 2**

Encryption algorithm: 3DES

Hash algorithm: SHA1

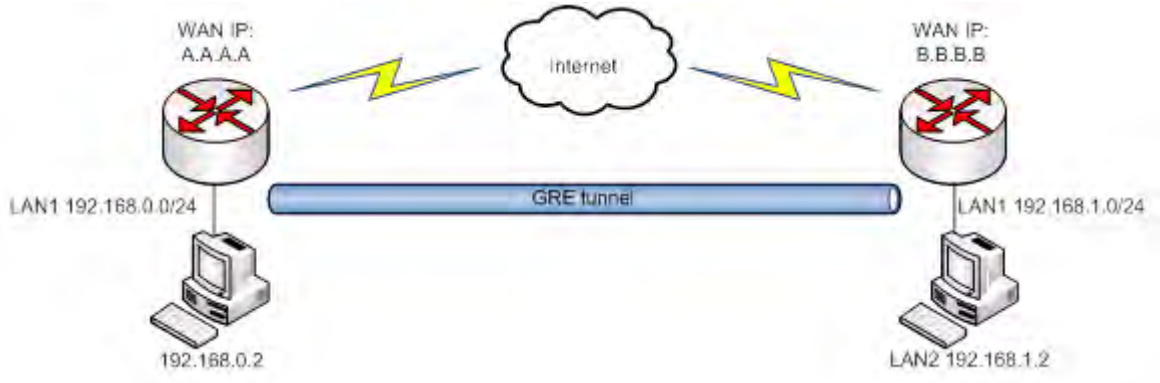
PFS group: MODP1536

Lifetime (h): 8 Hours

| 1. | Encryption algorithm | DES, 3DES, AES 128, AES 192, AES256                               | The encryption algorithm must match with another incoming connection to establish IPsec                |
|----|----------------------|---|--|
| 2. | Authentication       | MD5, SHA1, SHA256, SHA384, SHA512                                 | The authentication algorithm must match with another incoming connection to establish IPsec            |
| 3. | Hash algorithm       | MD5, SHA1, SHA256, SHA384, SHA512                                 | The hash algorithm must match with another incoming connection to establish IPsec                      |
| 4. | DH group             | MODP768, MODP1024, MODP1536, MODP2048, MODP3072, MODP4096         | The DH (Diffie-Helman) group must with another incoming connection to establish IPsec                  |
| 4. | PFS group            | MODP768, MODP1024, MODP1536, MODP2048, MODP3072, MODP4096, No PFS | The PFS (Perfect Forward Secrecy) group must match with another incoming connection to establish IPsec |
| 5. | Lifetime             | Hours, Minutes, Seconds   | The time duration for phase  |

### 8.4.3 GRE Tunnel

GRE (Generic Routing Encapsulation RFC2784) is a solution for tunneling RFC1812 private address-space traffic over an intermediate TCP/IP network such as the Internet. GRE tunneling does not use encryption it simply encapsulates data and sends it over the WAN.



In the example network diagram two distant networks LAN1 and LAN2 are connected.

To create GRE tunnel the user must know the following parameters:

1. Source and destination IP addresses.
2. Tunnel local IP address
3. Distant network IP address and Subnet mask.

**-tunnel Instance: Gre\_tunnel**

**Settings**

Enabled

Remote endpoint IP address

Remote network

Remote network netmask

Local tunnel IP

Local tunnel netmask

MTU

TTL

PMTUD

Enable Keep alive

Keep Alive host

Keep Alive interval



| 1.  | Enabled                    | Check the box to enable the GRE Tunnel function.   |
|-----|----------------------------|--|
| 2.  | Remote endpoint IP address | Specify remote WAN IP address.   |
| 3.  | Remote network             | IP address of LAN network on the remote device.  |
| 4.  | Remote network netmask     | Network of LAN network on the remote device. Range [0-32].   |
| 5.  | Local tunnel IP            | Local virtual IP address. Cannot be in the same subnet as LAN network.   |
| 6.  | Local tunnel netmask       | Network of local virtual IP address. Range [0-32]  |
| 7.  | MTU                        | Specify the maximum transmission unit (MTU) of a communications protocol of a layer in bytes.  |
| 8.  | TTL                        | Specify the fixed time-to-live (TTL) value on tunneled packets [0-255]. The 0 is a special value meaning that packets inherit the TTL value.                         |
| 9.  | PMTUD                      | Check the box to enable the Path Maximum Transmission Unit Discovery (PMTUD) status on this tunnel.  |
| 10. | Enable Keep alive          | It gives the ability for one side to originate and receive keep alive packets to and from a remote router even if the remote router does not support GRE keep alive. |
| 11. | Keep Alive host            | Keep Alive host IP address. Preferably IP address which belongs to the LAN network on the remote device.   |
| 12. | Keep Alive interval        | Time interval for Keep Alive. Range [0 - 255].   |

### 8.4.4 PPTP

Point-to-Point Tunneling Protocol (PPTP) is a protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network. A company no longer needs to lease its own lines for wide-area communication but can securely use the public networks. This kind of interconnection is known as a virtual private network (VPN).

OpenVPN
IPsec
GRE Tunnel
PPTP
L2TP

#### PPTP Server Instance: Server

**Main Settings**

Enable

Local IP

Remote IP range start

Remote IP range end

| User name                                       | Password                               | User IP              |                                       |
|---|--|----------------------|---------------------------------------|
| <input type="text" value="youruser"/>           | <input type="password" value="*****"/> | <input type="text"/> | <input type="button" value="Delete"/> |
| <input type="button" value="Add"/>              |  |                      |                                       |
| <input type="button" value="Back to Overview"/> |  |                      | <input type="button" value="Save"/>   |

|    |                       |  |
|----|-----------------------|--|
| 1. | Enable                | Check the box to enable the PPTP function. |
| 2. | Local IP              | IP Address of this device (RUT)            |
| 3. | Remote IP range begin | IP address leases beginning                |
| 4. | Remote IP range end   | IP address leases end                      |
| 5. | Username              | Username to connect to PPTP (this) server  |
| 6. | Password              | Password to connect to PPTP server         |
| 7. | User IP               | Users IP address                           |

**PPTP Client Instance: Client**

**Main Settings**

Enable

Use as default gateway

Server

User name

Password

[Back to Overview](#)

|    |                        |   |
|----|------------------------|---|
| 1. | Enable                 | Enable current configuration                    |
| 2. | Use as default gateway | Use this PPTP instance as default gateway       |
| 3. | Server                 | The server IP address or hostname               |
| 4. | Username               | The user name for authorization with the server |
| 5. | Password               | The password for authorization with the server  |

### 8.4.5 L2TP

Allows setting up a L2TP server or client. Below is L2TP server configuration example.

OpenVPN IPsec GRE Tunnel PPTP **L2TP**

**L2TP Server Instance: Server**

Main Settings

Enable

Local IP

Remote IP range begin

Remote IP range end

| User name                         | Password                              |                                       |
|-----------------------------------|---------------------------------------|---------------------------------------|
| <input type="text" value="user"/> | <input type="password" value="****"/> | <input type="button" value="Delete"/> |

|    |                       |   |
|----|-----------------------|---|
| 1. | Enable                | Check the box to enable the L2TP Tunnel function. |
| 2. | Local IP              | IP Address of this device (RUT)                   |
| 3. | Remote IP range begin | IP address leases beginning                       |
| 4. | Remote IP range end   | IP address leases end                             |
| 5. | Username              | Username to connect to L2TP (this) server         |
| 6. | Password              | Password to connect to L2TP server                |

Client configuration is even simpler, which requires only **Servers IP**, **Username** and **Password**.

**L2TP Server Instance: Server**

Main Settings

Enable

Local IP

Remote IP range begin

Remote IP range end

| User name                         | Password                              |                                       |
|-----------------------------------|---------------------------------------|---------------------------------------|
| <input type="text" value="user"/> | <input type="password" value="****"/> | <input type="button" value="Delete"/> |

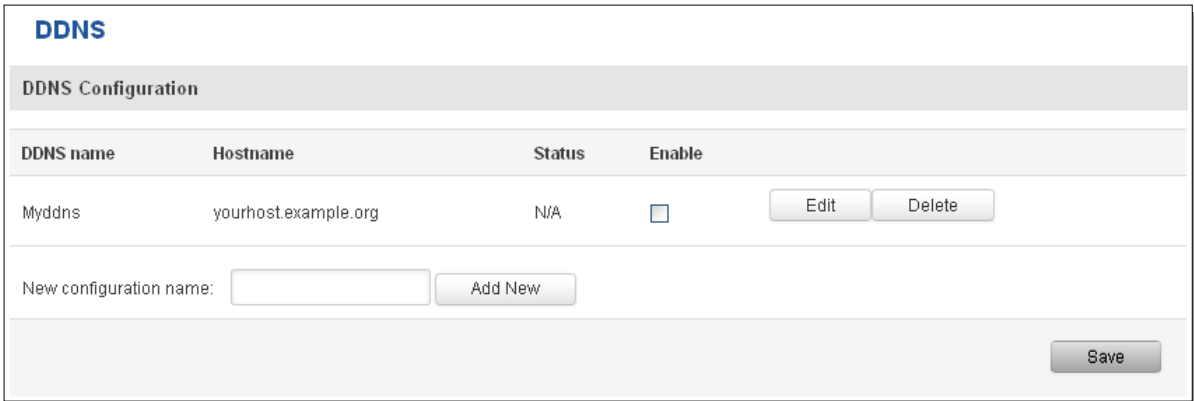
## 8.5 Dynamic DNS

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 (example list is given in description).

You are provided with add/delete buttons to manage and use different DDNS configurations at the same time!

You can configure many different DDNS Hostnames in the main DDNS Configuration section.



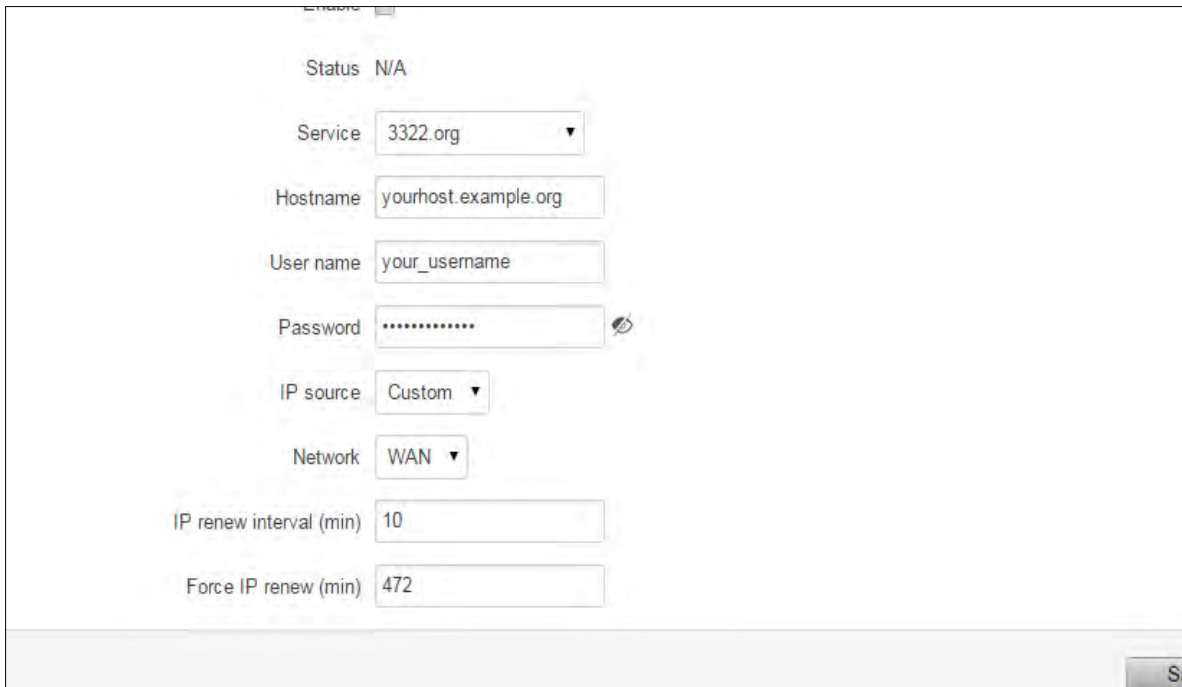
**DDNS**

**DDNS Configuration**

| DDNS name | Hostname             | Status | Enable                   |   |
|-----------|----------------------|--------|--------------------------|---|
| Myddns    | yourhost.example.org | N/A    | <input type="checkbox"/> | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

New configuration name:

To edit your selected configuration, hit **Edit**.



Status N/A

Service

Hostname

User name

Password

IP source

Network

IP renew interval (min)

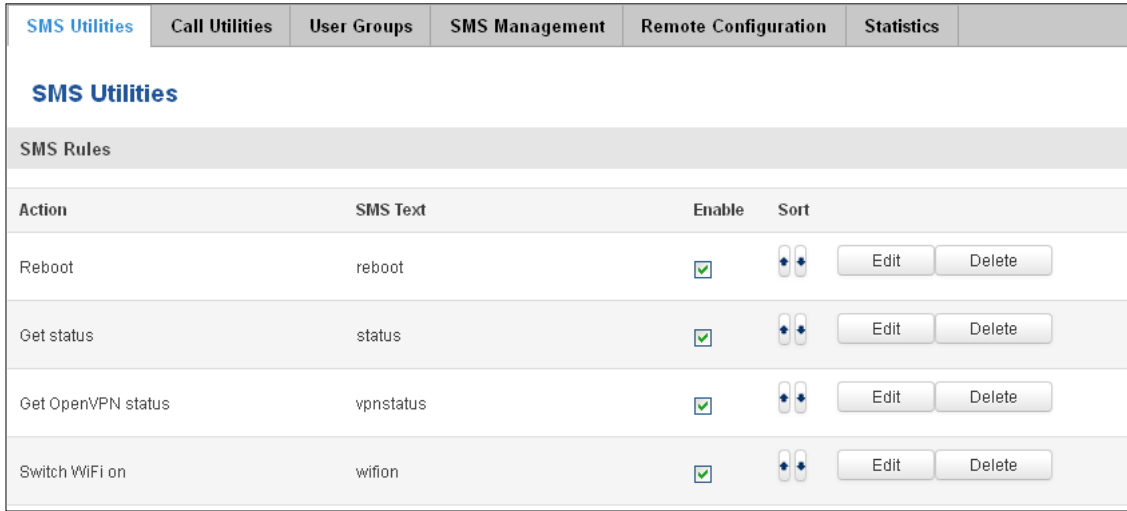
Force IP renew (min)

| 1.  | Enable                  | Enable/Disable   | Enables current DDNS configuration.  |
|-----|-------------------------|--|--|
| 2.  | Status                  |  | Timestamp of the last IP check or update.  |
| 3.  | Service                 | 1. dydns.org<br>2. 3322.org<br>3. no-ip.com<br>4. easydns.com<br>5. zoneedit.com | Your dynamic DNS service provider selected from the list.<br>In case your DDNS provider is not present from the ones provided, please feel free to use "custom" and add hostname of the update URL.  |
| 4.  | Hostname                | yourhost.example.org   | Domain name which will be linked with dynamic IP address.  |
| 5.  | Username                | your_username  | Name of the user account.  |
| 6.  | Password                | your_password  | Password of the user account.  |
| 7.  | IP Source               | Public<br>Private<br>Custom  | This option allows you to select specific RUT interface, and then send the IP address of that interface to DDNS server. So if, for example, your RUT has Private IP (i.e. 10.140.56.57) on its WAN (LTE interface), then you can send this exact IP to DDNS server by selecting "Private", or by selecting "Custom" and "WAN" interface. The DDNS server will then resolve hostname queries to this specific IP. |
| 8.  | Network                 | WAN  | Source network   |
| 9.  | IP renew interval (min) | 10 (minutes)   | Time interval (in minutes) to check if the IP address of the device have changed.  |
| 10. | Force IP renew          | 472 (minutes)  | Time interval (in minutes) to force IP address renew.  |

## 8.6 SMS Utilities

RUT240 has extensive amount of various SMS Utilities. These are subdivided into 6 sections: SMS Utilities, Call Utilities, User Groups, SMS Management, Remote Configuration and Statistics.

### 8.6.1 SMS Utilities



| Action             | SMS Text  | Enable                              | Sort |             |
|--------------------|-----------|-------------------------------------|------|-------------|
| Reboot             | reboot    | <input checked="" type="checkbox"/> | ↑ ↓  | Edit Delete |
| Get status         | status    | <input checked="" type="checkbox"/> | ↑ ↓  | Edit Delete |
| Get OpenVPN status | vpnstatus | <input checked="" type="checkbox"/> | ↑ ↓  | Edit Delete |
| Switch WiFi on     | wifion    | <input checked="" type="checkbox"/> | ↑ ↓  | Edit Delete |

All configuration options are listed below:

- Reboot
- Get status
- Get OpenVPN status
- Switch WiFi on/off
- Switch mobile data on/off
- Switch OpenVPN on/off
- Change mobile data settings
- Get list of profiles
- Change profile
- Manage OpenVPN
- SSH access control
- Web access control
- Restore to default
- Force SIM switch
- FW upgrade from server
- Config update from server
- Switch monitoring on/off
- Get Monitoring status
- UCI parameters

You can choose your SMS Keyword (text to be sent) and authorized phone number in the main menu. You can edit each created rule by hitting **Edit** button.

**SMS Utilities** | Call Utilities | User Groups | **SMS Management** | Remote Configuration | Statistics

## SMS Configuration

### Modify SMS Rule

Enable

Action: Reboot

SMS text: reboot  
SMS text, which let you reboot your router. E.g. "reboot"

Authorization method: No authorization

Allowed users: From all numbers

Get status via SMS after reboot

Get information:

Message text: Router name - %rn; WAN IP - %wj; Data Connection state - %cs; Connection type - %ct; Signal Strength - %ss; New FW available - %fs; Time stamp - %ts; Serial number - %sn; LAN MAC address - %lm; Connection state - %cs; Connection type - %ct; SIM slot in use - %su; Event type - %et; FW available on server - %fs; Network state - %ns; New line - %nl; Router name - %rn; WAN MAC address - %wrm; Curren FW version - %fc; Operator name - %on; Signal strength - %ss; IMSI - %im; Event text - %ex; LAN IP - %li; WAN IP address - %wi

[Back to Overview](#) [Save](#)

| 1. | <b>Reboot</b>                   |  |  |
|----|---------------------------------|--|--|
|    | Enable                          | This check box will enable and disable SMS reboot function.  | Allows router restart via SMS.   |
|    | Action                          | The action to be performed when this rule is met.  |  |
|    | SMS text                        | SMS text which will reboot router.   | SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.   |
|    | Authorization method            | What kind of authorization to use for SIM management.  | No authorization, by serial or by router admin password.   |
|    | Allowed users                   | Whitelist of allow users   | From all numbers, from group or from single number.  |
|    | Get status via SMS after reboot | Check this to receive connection status via SMS after a reboot.  | If you select this box, router will send status once it has rebooted and is operational again. This is both separate SMS Rule and an option under SMS Reboot rule. |
|    | Message text                    | Which status information should be included in SMS: Data state, Operator, Connection type, Signal Strength, Connection State, IP | You can select which status elements to display.   |
| 2. | <b>Get status</b>               |  |  |
|    | Enable                          | Check this to receive connection status via SMS.   | Allows to get router's status via SMS. This is both separate SMS Rule and an option under SMS Reboot rule.   |
|    | Action                          | The action to be performed   |  |



|    |                                  |  |   |
|----|----------------------------------|--|---|
|    |                                  | when this rule is met.   |   |
|    | Enable SMS Status                | This check box will enable and disable SMS status function.  | SMS status is disabled by default.  |
|    | SMS text                         | SMS text which will send routers status.   | SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.  |
|    | Authorization method             | What kind of authorization to use for SIM management.  | No authorization, by serial or by router admin password.  |
|    | Allowed users                    | Whitelist of allow users   | From all numbers, from group or from single number.   |
|    | Message text                     | Which status information should be included in SMS:<br>Data state, Operator,<br>Connection type, Signal Strength, Connection State, IP | You can select which status elements to display.  |
| 3. | <b>Get OpenVPN status</b>        |  |   |
|    | Enable                           | This check box will enable and disable this function.  | Allows to get OpenVPN's status via SMS.   |
|    | Action                           | The action to be performed when this rule is met.  |   |
|    | SMS text                         | SMS text which will send OpenVPN status.   | SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.  |
|    | Authorization method             | What kind of authorization to use for SIM management.  | No authorization, by serial or by router admin password.  |
|    | Allowed users                    | Whitelist of allow users   | From all numbers, from group or from single number.   |
| 4. | <b>Switch WiFi On/Off</b>        |  |   |
|    | Enable                           | This check box will enable and disable this function.  | Allows Wi-Fi control via SMS.   |
|    | Action                           | The action to be performed when this rule is met.  | Turn WiFi ON or OFF.  |
|    | SMS text                         | SMS text which will turn Wi-Fi ON/OFF.   | SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.  |
|    | Authorization method             | What kind of authorization to use for SIM management.  | No authorization, by serial or by router admin password.  |
|    | Allowed users                    | Whitelist of allow users   | From all numbers, from group or from single number.   |
|    | Write to config                  | Permanently saves Wi-Fi state.   | With this setting enabled, router will keep Wi-Fi state even after reboot.<br>If it is not selected, router will revert Wi-Fi state after reboot. |
| 5. | <b>Switch mobile data on/off</b> |  |   |
|    | Enable                           | This check box will enable and disable this function.  | Allows mobile control via SMS.  |
|    | Action                           | The action to be performed when this rule is met.  | Turn mobile ON or OFF.  |
|    | SMS text                         | SMS text which will turn mobile data ON/OFF.   | SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.  |
|    | Authorization method             | What kind of authorization to use for SIM management.  | No authorization, by serial or by router admin password.  |
|    | Allowed users                    | Whitelist of allow users   | From all numbers, from group or from single number.   |
|    | Write to config                  | Permanently saves mobile network state.  | With this setting enabled, router will keep mobile state even after reboot.   |

|    |                                    |   |  |
|----|------------------------------------|---|--|
|    |                                    |   | If it is not selected, router will revert mobile state after reboot.   |
| 6. | <b>Manage OpenVPN</b>              |   |  |
|    | Enable                             | This check box will enable and disable this function.       | Allows OpenVPN control via SMS.  |
|    | Action                             | The action to be performed when this rule is met.           | Turn OpenVPN ON or OFF.  |
|    | SMS text                           | Keyword which will turn OpenVPN ON/OFF.                     | SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters. After Keyword you have to write OpenVPN name. |
|    | Authorization method               | What kind of authorization to use for SIM management.       | No authorization, by serial or by router admin password.   |
|    | Allowed users                      | Whitelist of allow users                                    | From all numbers, from group or from single number.  |
| 7. | <b>Change mobile data settings</b> |   |  |
|    | Enable                             | This check box will enable and disable this function.       | Allows to change mobile settings via SMS.  |
|    | Action                             | The action to be performed when this rule is met.           |  |
|    | SMS text                           | Key word that will precede actual configuration parameters. | SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.   |
|    | Authorization method               | What kind of authorization to use for SIM management.       | No authorization, by serial or by router admin password.   |
|    | Allowed users                      | Whitelist of allow users                                    | From all numbers, from group or from single number.  |

### Mobile Settings via SMS parameters:

| 1. | apn=        | e.g. internet.gprs  | Sets APN. i.e: apn=internet.gprs  |
|----|-------------|---------------------|---|
| 2. | dialnumber= | e.g. *99***1#       | Sets dial number  |
| 3. | auth_mode=  | none<br>pap<br>chap | Sets authentication mode  |
| 4. | service=    | Auto                | You can add as many phone numbers as you need. Dropdown list with additional rows will show up if you click on "add" icon at the end of phone number row. |
| 5. | username=   | user                | Used only if PAP or CHAP authorization is selected  |
| 6. | password=   | user                | Used only if PAP or CHAP authorization is selected  |

All Mobile settings can be changed in one SMS. Between each <parameter=value> pair a space symbol is necessary.

**Example:** `cellular apn=internet.gprs dialnumber=*99***1#auth_mode=pap service=auto username=user password=user`

Important Notes:

- LTE settings must be configured correctly. If SIM card has PIN number you must enter it at “Network” > “LTE” settings. Otherwise SMS reboot function will not work.
- Sender phone number must contain country code. You can check sender phone number format by reading the details of old SMS text messages you receiving usually.

| 8.  | <b>Get list of profiles</b> |  |  |
|-----|-----------------------------|--|--|
|     | Enable                      | This check box will enable and disable this function.              | Allows to get list of profiles via SMS.  |
|     | Action                      | The action to be performed when this rule is met.                  |  |
|     | SMS text                    | SMS text which will send list of profiles.                         | SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.   |
|     | Authorization method        | What kind of authorization to use for SIM management.              | No authorization, by serial or by router admin password.   |
|     | Allowed users               | Whitelist of allow users   | From all numbers, from group or from single number.  |
| 9.  | <b>Change profile</b>       |  |  |
|     | Enable                      | This check box will enable and disable this function.              | Allows profile change via SMS.   |
|     | Action                      | The action to be performed when this rule is met.                  |  |
|     | SMS text                    | Keyword which will change active profile.                          | SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters. After Keyword you have to write profile name. |
|     | Authorization method        | What kind of authorization to use for SIM management.              | No authorization, by serial or by router admin password.   |
|     | Allowed users               | Whitelist of allow users   | From all numbers, from group or from single number.  |
| 10. | <b>SSH access Control</b>   |  |  |
|     | Enable                      | This check box will enable and disable this function.              | Allows SSH access control via SMS.   |
|     | Action                      | The action to be performed when this rule is met.                  |  |
|     | SMS text                    | SMS text which will turn SSH access ON/OFF.                        | SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.   |
|     | Authorization method        | What kind of authorization to use for SIM management.              | No authorization, by serial or by router admin password.   |
|     | Allowed users               | Whitelist of allow users   | From all numbers, from group or from single number.  |
|     | Enable SSH access           | Enable this to reach router via SSH from LAN (Local Area Network). | If this box is selected, SMS will enable SSH access from LAN. If this box is not selected, SMS will disable SSH access from LAN.               |
|     | Enable remote SSH access    | Enable this to reach router via SSH from WAN (Wide Area Network).  | If this box is selected, SMS will enable SSH access from WAN. If this box is not selected, SMS will disable SSH access from WAN.               |
| 11. | <b>Web access Control</b>   |  |  |
|     | Enable                      | This check box will enable and disable this function.              | Allows Web access control via SMS.   |
|     | Action                      | The action to be performed   |  |

|     |                                     |   |   |
|-----|-------------------------------------|---|---|
|     |                                     | when this rule is met.  |   |
|     | SMS text                            | SMS text which will turn Web access ON/OFF.                           | SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.  |
|     | Authorization method                | What kind of authorization to use for SIM management.                 | No authorization, by serial or by router admin password.  |
|     | Allowed users                       | Whitelist of allow users  | From all numbers, from group or from single number.   |
|     | Enable HTTP access                  | Enable this to reach router via HTTP from LAN (Local Area Network).   | If this box is selected, SMS will enable HTTP access from LAN. If this box is not selected, SMS will disable HTTP access from LAN.                        |
|     | Enable remote HTTP access           | Enable this to reach router via HTTP from WAN (Wide Area Network).    | If this box is selected, SMS will enable HTTP access from WAN. If this box is not selected, SMS will disable HTTP access from WAN.                        |
|     | Enable remote HTTPS access          | Enable this to reach router via HTTPS from WAN (Wide Area Network).   | If this box is selected, SMS will enable HTTPS access from WAN. If this box is not selected, SMS will disable HTTPS access from WAN.                      |
| 12. | <b>Restore to default</b>           |   |   |
|     | Enable                              | This check box will enable and disable this function.                 | Allows to restore router to default settings via SMS.   |
|     | Action                              | The action to be performed when this rule is met.                     | Router will reboot after this rule is executed.   |
|     | SMS text                            | SMS text which will turn Wi-Fi ON/OFF.                                | SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.  |
|     | Authorization method                | What kind of authorization to use for SIM management.                 | No authorization, by serial or by router admin password.  |
|     | Allowed users                       | Whitelist of allow users  | From all numbers, from group or from single number.   |
| 13. | <b>Force switch SIM</b>             |   |   |
|     | Enable                              | This check box will enable and disable this function.                 | Allows SIM switch via SMS.  |
|     | Action                              | The action to be performed when this rule is met.                     |   |
|     | SMS text                            | SMS text which will change active SIM card to another one.            | SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.  |
|     | Authorization method                | What kind of authorization to use for SIM management.                 | No authorization, by serial or by router admin password.  |
|     | Allowed users                       | Whitelist of allow users  | From all numbers, from group or from single number.   |
|     | Sender phone number                 | Phone number of person who can receive router status via SMS message. | You can add as many phone numbers as you need. Dropdown list with additional rows will show up if you click on "add" icon at the end of phone number row. |
| 14. | <b>Force FW upgrade from server</b> |   |   |
|     | Enable                              | This check box will enable and disable this function.                 | Allows to upgrade router's FW via SMS.  |
|     | Action                              | The action to be performed when this rule is met.                     | Router will reboot after this rule is executed.   |
|     | SMS text                            | SMS text which will force router to upgrade firmware from server.     | SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.  |
|     | Authorization method                | What kind of authorization to   | No authorization, by serial or by router admin  |

|     |  |  |  |
|-----|--|--|--|
|     |  | use for SIM management.  | password.  |
|     | Allowed users                          | Whitelist of allow users   | From all numbers, from group or from single number.  |
| 15. | <b>Force Config update from server</b> |  |  |
|     | Enable                                 | This check box will enable and disable this function.                  | Allows to upgrade router's Config via SMS.   |
|     | Action                                 | The action to be performed when this rule is met.                      | Router will reboot after this rule is executed.  |
|     | SMS text                               | SMS text which will force router to upgrade configuration from server. | SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters. |
|     | Authorization method                   | What kind of authorization to use for SIM management.                  | No authorization, by serial or by router admin password.   |
|     | Allowed users                          | Whitelist of allow users   | From all numbers, from group or from single number.  |
| 16. | <b>Switch monitoring on/off</b>        |  |  |
|     | Enable                                 | This check box will enable and disable this function.                  | Allows monitoring control via SMS.   |
|     | Action                                 | The action to be performed when this rule is met.                      | Turn monitoring ON or OFF.   |
|     | SMS text                               | SMS text which will turn monitoring ON/OFF                             | SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters. |
|     | Authorization method                   | What kind of authorization to use for SIM management.                  | By serial or by router admin password.   |
|     | Allowed users                          | Whitelist of allow users   | From all uers, from group or from single number.   |
| 17. | <b>Monitoring status</b>               |  |  |
|     | Enable                                 | This check box will enable and disable this function.                  | Allows monitoring control via SMS.   |
|     | Action                                 | The action to be performed when this rule is met.                      | Get monitoring status  |
|     | SMS text                               | SMS text which will turn monitoring ON/OFF                             | SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters. |
|     | Authorization method                   | What kind of authorization to use for SIM management.                  | By serial or by router admin password.   |
| 18. | <b>UCI API</b>                         |  |  |
|     | Enable                                 | This check box will enable and disable this function.                  | Allows monitoring control via SMS.   |
|     | Action                                 | The action to be performed when this rule is met.                      | UCI lets you set or get any parameter from router's configuration files.                         |
|     | SMS text                               | SMS text which will turn monitoring ON/OFF                             | SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters. |
|     | Authorization method                   | What kind of authorization to use for SIM management.                  | By serial or by router admin password.   |
|     |  |  |  |

### UCI via SMS parameters:

UCI lets you set or get any parameter from router's configuration files. Following are syntax examples:

| 1. | uci get config.section.option"       | Get config option value.   |
|----|--------------------------------------|--|
| 2. | uci set config.section.option=value" | Set config option  |
| 3. | uci show config                      | Shows the config file.   |
| 4. | uci show config.section              | Shows the exact part of config file (Eg. uci show network.ppp.apn" ) |

## 8.6.2 Call Utilities

Allow users to call to the router in order to perform one of the actions: Reboot, Get Status, turn Wi-Fi ON/OFF, turn Mobile data ON/OFF. Only thing that is needed is to call routers SIM card number from allowed phone (user) and RUT900 will perform all actions that are assigned for this particular number. To configure new action on call rules you just need to click the Add button in the „New Call rule” section. After that, you get in to the “Modify Call Rule section”.

The screenshot shows the 'Call Configuration' section with the 'Modify Call Rule' sub-section. The 'Enable' checkbox is unchecked. The 'Action' dropdown is set to 'Reboot', and the 'Allowed users' dropdown is set to 'From all numbers'. The 'Get status via SMS after reboot' checkbox is also unchecked. At the bottom, there are 'Back to Overview' and 'Save' buttons.

This screenshot is identical to the one above, but the 'Enable' checkbox is now checked, indicating that the call rule is active.

|    |                                 |                  |  |
|----|---------------------------------|------------------|--|
| 1. | Enable                          | Enable/Disable   | Enables the rule   |
| 2. | Action                          | Reboot           | Action to be taken after receiving a call, you can choose from following actions: Reboot, Send status, Switch Wi-Fi, Switch mobile data. |
| 3. | Allowed users                   | From all numbers | Allows to limit action triggering from all users, to user groups or single user numbers  |
| 4. | Get status via SMS after reboot | Enable/Disable   | Enables automatic message sending with router status information after reboot  |

### 8.6.2.1 Incoming Calls

The screenshot shows the 'Incoming Calls' configuration section. The 'Reject unrecognized incoming calls' checkbox is checked. A 'Save' button is located at the bottom right of the configuration area.

|    |                                    |                |  |
|----|------------------------------------|----------------|--|
| 1. | Reject unrecognized incoming calls | Enable/Disable | If a call is made from number that is not in the active rule list, it can be rejected with this option |
|----|------------------------------------|----------------|--|

### 8.6.3 User Groups

Give possibility to group phone numbers for SMS management purposes. You can then later use these groups in all related SMS functionalities. This option helps if there are several Users who should have same roles when managing router via SMS. You can create new user group by entering group name and clicking on Add button in “Create New User Group” section. After that you get to “Modify User Group” section.



|    |              |              |   |
|----|--------------|--------------|---|
| 1. | Group name   | Group1       | Name of grouped phone numbers   |
| 2. | Phone number | +37061111111 | Number to add to users group, must match international format. You can add phone numbers fields by clicking on the green + symbol |



## 8.6.4 SMS Management

### 8.6.4.1 Read SMS

In SMS Management page Read SMS you can read and delete received/stored SMS.

The screenshot shows the 'Read SMS' interface within the 'SMS Management' section. At the top, there are navigation tabs: 'SMS Utilities', 'Call Utilities', 'User Groups', 'SMS Management' (selected), 'Remote Configuration', and 'Statistics'. Below these are sub-tabs: 'Read SMS', 'Send SMS', and 'Storage'. The main area is titled 'SMS Messages' and includes a 'SMS per page' dropdown set to '10' and a search input field. A table displays one message entry with columns for 'Date', 'Sender', and 'Message'. The entry shows a date of '2016-05-05 13:51:56', a sender of '+370612345678', and a message of 'Labas'. A checkbox is visible to the right of the message. At the bottom, it says 'Showing 1 to 1 of 1 entries' and includes 'Refresh', 'Delete', and 'Select all' buttons.

### 8.6.4.2 Send SMS

The screenshot shows the 'Send SMS' form. It has a header 'SMS' and a sub-header 'Send SMS Message'. The form contains two input fields: 'Phone Number' with the value '+3701111111' and 'Message' with the value 'My text.'.

|    |              |             |  |
|----|--------------|-------------|--|
| 1. | Phone number | +3701111111 | Recipients phone number. Should be preceded with country code, i.e. "+370" |
| 2. | Message      | My text.    | Message text, special characters are allowed.                              |

### 8.6.4.3 Storage

With **storage** option you can choose for router NOT to delete SMS from SIM card. If this option is not used, router will automatically delete all incoming messages after they have been read. Message status “read/unread” is examined every 60 seconds. All “read” messages are deleted.



| 1. | Save messages on SIM | Enabled / Disabled       | Enables received message storing on SIM card           |
|----|----------------------|--------------------------|--|
| 2. | SIM card memory      | Used: 0<br>Available: 50 | Information about used/available SIM card memory       |
| 3. | Leave free space     | 1                        | How much memory (number of message should be left free |

## 8.6.5 Remote Configuration

RUT240 can be configured via SMS from another RUT240. You only have to select which configuration details to send, generate the SMS Text, type in the phone number and Serial number of the router that you wish to configure and Send the SMS.

Total count of SMS is managed automatically. You should be aware of possible number of SMS and use this feature at your own responsibility. It should not, generally, be used if you have high cost per SMS. This is especially relevant if you will try to send whole OpenVPN configuration, which might accumulate ~40 SMS.

### 8.6.5.1 Receive configuration

This section controls how configuration initiation party should identify itself. In this scenario RUT240 itself is being configured.

Receive Configuration

Enable

Authorization method: By router admin password

Allowed users: From all numbers

Save

|    |                      |   |   |
|----|----------------------|---|---|
| 1. | Enable               | Enabled / Disabled  | Enables router to receive configuration   |
| 1. | Authorization method | No authorization /<br>By serial<br>By administration password | Describes what kind of authorization to use for SMS management. Method at Receiving and Sending ends must match |
| 2. | Allowed users        | From all numbers<br>From group<br>From single number          | Gives greater control and security measures   |

**Note, that for safety reasons Authorization method should be configured before deployment of the router.**

### 8.6.5.2 Send configuration

This section lets you configure remote RUT240 devices. The authorization settings must confirm to those that are set on the receiving party.

### Send Configuration

Configuration Message

Network
VPN

Generate SMS New ▼

WAN

Interface Mobile ▼

Primary SIM card SIM1 ▼

Mobile connection Use pppd mode ▼

APN internet.mnc012.mcc34c

Dialing number +37060000001

Authentication method CHAP ▼

User name admin

Password ●●●●●● 👁

Service mode 3G preferred ▼

LAN

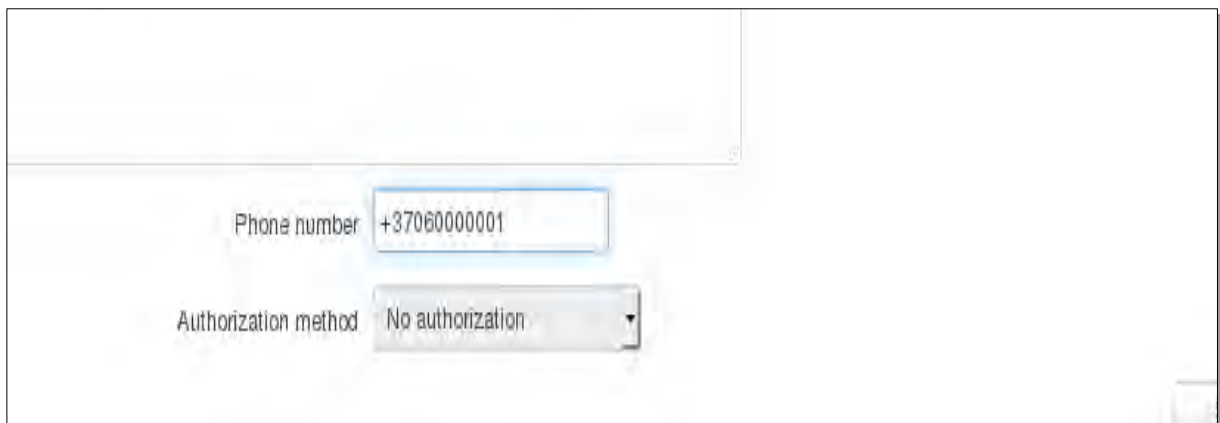
IP address 192.168.1.1

IP netmask 255.255.255.0

IP broadcast 192.168.1.255

|     |              |                                |  |
|-----|--------------|--------------------------------|--|
| 1.  | Generate SMS | New/From current configuration | Generate new SMS settings or use current device configuration  |
| 2.  | Interface    | Mobile/Wired                   | Interface type used for WAN (Wide Area Network) connection   |
| 3.  | WAN          | Enable/Disable                 | Include configuration for WAN (Wide Area Network)  |
| 4.  | LAN          | Enable/Disable                 | Include configuration for LAN (Local Area Network)   |
| 6.  | Protocol     | Static/DHCP                    | Network protocol used for network configuration parameters management  |
| 7.  | IP address   | "217.147.40.44"                | IP address that router will use to connect to the internet   |
| 8.  | IP netmask   | "255.255.255.0"                | That will be used to define how large the WAN (Wide Area Network) network is   |
| 11. | IP gateway   | "217.147.40.44"                | The address where traffic destined for the internet is routed to   |
| 12. | IP broadcast | "217.147.40.255"               | A logical address at which all devices connected to a multiple-access communications network are enabled to receive datagrams. |

|     |                       |                                |   |
|-----|-----------------------|--------------------------------|---|
| 13. | Primary SIM card      | SIM1/SIM2                      | A SIM card that will be used as primary   |
| 14. | Mobile connection     | Use pppd mode<br>Use ndis mode | An underlying agent that will be used for mobile data connection creation and management  |
| 15. | APN                   | "internet.mnc012.mcc345.gprs"  | (APN) is the name of a gateway between LTE mobile networks and another computer network, frequently the public Internet.                                  |
| 16. | Dialing number        | "+37060000001"                 | A phone number that will be used to establish a mobile PPP (Point-to-Point Protocol) connection   |
| 17. | Authentication method | CHAP/PAP/None                  | Select an authentication method that will be used to authenticate new connections on your GSM carrier's network   |
| 18. | User name             | "admin"                        | User name used for authentication on your GSM carrier's network   |
| 19. | Password              | "password"                     | Password used for authentication on your GSM carrier's network  |
| 20. | Service mode          | Auto<br>4G only                | You can add as many phone numbers as you need. Dropdown list with additional rows will show up if you click on "add" icon at the end of phone number row. |
| 21. | IP address            | "192.168.1.1"                  | IP address that router will use on LAN (Local Area Network) network   |
| 22. | IP netmask            | "255.255.255.0"                | A subnet mask that will be used to define how large the LAN (Local Area Network) network is   |
| 23. | IP broadcast          | "192.168.1.255"                | A logical address at which all devices connected to a multiple-access communications network are enabled to receive datagrams                             |



|    |                      |   |  |
|----|----------------------|---|--|
| 1. | Message text field   | Generated configuration message                           | Here you can review and modify configuration message text to be sent |
| 2. | Phone number         | "+37060000001"  | A phone number of router which will receive the configuration        |
| 3. | Authorization method | No authorization<br>By serial<br>By router admin password | What kind of authorization to use for remote configuration           |

### 8.6.6 Statistics

In statistics page you can review how much SMS was sent and received on both SIM card slots. You can also reset the counters.



## 8.7 SNMP

SNMP settings window allows you to remotely monitor and send GSM event information to the server.

### 8.7.1 SNMP Settings

**SNMP Service Settings**

Enable SNMP service

Enable remote access

Port

Community

Location

Contact

Name

| 1. | Enable SNMP service  | Enable/Disable        | Run SNMP (Simple Network Management Protocol) service on system's start up                                  |
|----|----------------------|-----------------------|---|
| 2. | Enable remote access | Enable/Disable        | Open port in firewall so that SNMP (Simple Network Management Protocol) service may be reached from WAN     |
| 3. | Port                 | 161                   | SNMP (Simple Network Management Protocol) service's port  |
| 4. | Community            | Public/Private/Custom | The SNMP (Simple Network Management Protocol) Community is an ID that allows access to a router's SNMP data |
| 5. | Community name       | custom                | Set custom name to access SNMP  |
| 6. | Location             | Location              | Trap named sysLocation  |
| 7. | Contact              | email@example.com     | Trap named sysContact   |
| 8. | Name                 | Name                  | Trap named sysName  |

#### Variables/OID

| 1.  | 1.3.6.1.4.1.99999.1.1.1  | Modem IMEI                         |
|-----|--------------------------|------------------------------------|
| 2.  | 1.3.6.1.4.1.99999.1.1.2  | Modem model                        |
| 3.  | 1.3.6.1.4.1.99999.1.1.3  | Modem manufacturer                 |
| 4.  | 1.3.6.1.4.1.99999.1.1.4  | Modem revision                     |
| 5.  | 1.3.6.1.4.1.99999.1.1.5  | Modem serial number                |
| 6.  | 1.3.6.1.4.1.99999.1.1.6  | SIM status                         |
| 7.  | 1.3.6.1.4.1.99999.1.1.7  | Pin status                         |
| 8.  | 1.3.6.1.4.1.99999.1.1.8  | IMSI                               |
| 9.  | 1.3.6.1.4.1.99999.1.1.9  | Mobile network registration status |
| 10. | 1.3.6.1.4.1.99999.1.1.10 | Signal level                       |
| 11. | 1.3.6.1.4.1.99999.1.1.11 | Operator currently in use          |
| 12. | 1.3.6.1.4.1.99999.1.1.12 | Operator number (MCC+MNC)          |
| 13. | 1.3.6.1.4.1.99999.1.1.13 | Data session connection state      |
| 14. | 1.3.6.1.4.1.99999.1.1.14 | Data session connection type       |
| 15. | 1.3.6.1.4.1.99999.1.1.15 | Signal strength trap               |
| 16. | 1.3.6.1.4.1.99999.1.1.16 | Connection type trap               |

## 8.7.2 TRAP Settings

| 1. | SNMP Trap | Enable/Disable | Enable SNMP (Simple Network Management Protocol) trap functionality   |
|----|-----------|----------------|---|
| 2. | Host/IP   | 192.168.99.155 | Host to transfer SNMP (Simple Network Management Protocol) traffic to                                       |
| 3. | Port      | 162            | Port for trap's host  |
| 4. | Community | Public/Private | The SNMP (Simple Network Management Protocol) Community is an ID that allows access to a router's SNMP data |



## 8.8 SMS Gateway

### 8.8.1 Post/Get Configuration

Post/Get Configuration allows you to perform actions by writing these requests URL after your device IP address.

|    |           |                    |  |
|----|-----------|--------------------|--|
| 1. | Enable    | Enabled / Disabled | Enable SMS management functionality through POST/GET |
| 2. | User name | admin              | User name used for authorization                     |
| 3. | Password  | *****              | Password used for authorization (default- admin01)   |

**Do not forget to change parameters in the url according to your POST/GET Configuration!**

#### 8.8.1.1 SMS by HTTP POST/GET

It is possible to read and send SMS by using valid HTTP POST/GET syntax. Use web browser or any other compatible software to submit HTTP POST/GET string to router. Router must be connected to GSM network when using "SMS send" feature.

|    |                            |   |
|----|----------------------------|---|
| 1. | View mobile messages list  | /cgi-bin/sms_list?username=admin&password=admin01                                       |
| 2. | Read mobile message        | /cgi-bin/sms_read?username=admin&password=admin01&number=1                              |
| 3. | Send mobile messages       | /cgi-bin/sms_send?username=admin&password=admin01&number=0037060000001&text=testmessage |
| 4. | View mobile messages total | /cgi-bin/sms_total?username=admin&password=admin01                                      |
| 5. | Delete mobile message      | /cgi-bin/sms_delete?username=admin&password=admin01&number=1                            |

### 8.8.1.2 Syntax of HTTP POST/GET string

| http://<br>{IP_ADDRESS} | /cgi-bin/sms_read?<br>username={your_user_name}&password={your_password}&number={MESSAGE_INDEX}                    | Read message                 |
|-------------------------|--|------------------------------|
|                         | /cgi-bin/sms_send?<br>username={your_user_name}&password={your_password}&number={PHONE_NUMBER}&text={MESSAGE_TEXT} | Send message                 |
|                         | /cgi-bin/sms_delete?<br>username={your_user_name}&password={your_password}&number={MESSAGE_INDEX}                  | Delete message               |
|                         | /cgi-bin/sms_list? username={your_user_name}&password={your_password}  | List all messages            |
|                         | /cgi-bin/sms_total? username={your_user_name}&password={your_password}   | Number of messages in memory |

Note: parameters of HTTP POST/GET string are in capital letters inside curly brackets. Curly brackets (“{ }”) are not needed when submitting HTTP POST/GET string.

### 8.8.1.3 Parameters of HTTP POST/GET string

| 1. | IP_ADDRESS    | IP address of your router   |
|----|---------------|---|
| 2. | MESSAGE_INDEX | SMS index in memory   |
| 3. | PHONE_NUMBER  | Phone number of the message receiver.<br>Note: Phone number must contain country code. Phone number format is: 00{COUNTRY_CODE} {RECEIVER_NUMBER}.<br>E.g.: 0037062312345 (370 is country code and 62312345 is receiver phone number) |
| 4. | MESSAGE_TEXT  | Text of SMS. Note: Maximum number of characters per SMS is 160. You cannot send longer messages. It is suggested to use alphanumeric characters only.   |

After every executed command router will respond with return status.

### 8.8.1.4 Possible responses after command execution

| 1. | OK           | Command executed successfully  |
|----|--------------|--|
| 2. | ERROR        | An error occurred while executing command                                |
| 3. | TIMEOUT      | No response from the module received                                     |
| 4. | WRONG_NUMBER | SMS receiver number format is incorrect or SMS index number is incorrect |
| 5. | NO MESSAGE   | There is no message in memory by given index                             |
| 6. | NO MESSAGES  | There are no stored messages in memory                                   |

### 8.8.1.5 HTTP POST/GET string examples

http://192.168.1.1/cgi-bin/sms\_read?username=admin&password=admin01&number=2

http://192.168.1.1/cgi-bin/sms\_send?username=admin&password=admin01&number=0037060000001&text=message

http://192.168.1.1/cgi-bin/sms\_delete?username=admin&password=admin01&number=4

http://192.168.1.1/cgi-bin/sms\_list?username=admin&password=admin01

http://192.168.1.1/cgi-bin/sms\_total?username=admin&password=admin01

## 8.8.2 Scheduled Messages

Scheduled messages allow to periodically sending mobile messages to specified number.

### 8.8.2.1 Scheduled Messages Configuration

**Modify scheduled message**

Enable

Recipient's phone number

Message text

SMS 1 (156 characters left)

Message sending Interval

Hour

Minute

| 1. | Enable                   | Enable/Disable      | Activates periodical messages sending.   |
|----|--------------------------|---------------------|--|
| 2. | Recipient's phone number | "+37060000001"      | Phone number that will receive messages. |
| 3. | Message text             | "Test"              | Message that will be send.               |
| 4. | Message sending interval | Day/Week/Month/Year | Message sending period.                  |

## 8.8.3 Auto Reply Configuration

Auto reply allows replying to every message that router receives to everyone or to listed numbers only.

**Reply Configuration**

Enable

Don't save received message

Mode

Message

| 1. | Enable                      | Enable/Disable            | Enable auto reply to every received mobile message.                     |
|----|-----------------------------|---------------------------|---|
| 2. | Don't save received message | Enable/Disable            | If enabled, received messages are not going to be saved                 |
| 3. | Mode                        | Everyone / Listed numbers | Specifies from which senders received messages are going to be replied. |
| 4. | Message                     | "Text"                    | Message text that will be sent in reply.                                |

## 8.8.4 SMPP

Post/Get   Scheduled SMS   Auto Reply   **SMPP**

### SMPP Server Configuration

Transmitter Configuration

Enable

User name

Password

Server port

Save

|    |             |                |  |
|----|-------------|----------------|--|
| 1. | Enable      | Enable/Disable | Enables SMPP server  |
| 2. | User name   | admin          | User name for authentication on SMPP server  |
| 3. | Password    | ●●●●●●         | Password for authentication on SMPP server   |
| 4. | Server port | 7777           | A port will be used for SMPP server communications. Allowed all not used ports [0-65535] |

## 8.9 Hotspot

Wireless hotspot provides essential functionality for managing an open access wireless network. In addition to standard RADIUS server authentication there is also the ability to gather and upload detailed logs on what each device (denoted as a MAC address) was doing on the network (what sites were traversed, etc.).

### 8.9.1 General settings

#### 8.9.1.1 Main settings

**General Settings**

Enable

AP IP

Logout address

Authentication mode

Terms of Service

External landing page

Protocol

HTTPS redirect

Use custom DNS

---

**Session Settings**

| Name      | Download bandwidth | Upload bandwidth | Download limit | Upload limit | Period |                                     |
|-----------|--------------------|------------------|----------------|--------------|--------|-------------------------------------|
| unlimited | Unlimited          | Unlimited        | Unlimited      | Unlimited    | -      | <input type="button" value="Edit"/> |

Template name

---

**Users Configuration**

| User name                              | Password | Idle timeout | Session timeout | Download bandwidth | Upload bandwidth | Session template |
|--|----------|--------------|-----------------|--------------------|------------------|------------------|
| <i>There are no users created yet.</i> |          |              |                 |                    |                  |                  |

| Username                           | Password                               | Session Template                       |                                    |
|------------------------------------|--|--|------------------------------------|
| <input type="text" value="admin"/> | <input type="password" value="*****"/> | <input type="text" value="unlimited"/> | <input type="button" value="Add"/> |

|    |         |  |
|----|---------|--|
| 1. | Enabled | Check this flag to enable hotspot functionality on the router.   |
| 2. | AP IP   | Access Point IP address. This will be the address of the router on the hotspot network. The router will automatically create a network according to its own IP and the CIDR number that you specify after the slash. E.g. "192.168.2.254/24" means that the router will create a network with the IP address 192.168.182.0, netmask 255.255.255.0 for the express purpose of containing all the wireless clients. Such a network will be able to have 253 clients (their IP addresses will be automatically granted to them and will range from 192.168.2.1 to 192.168.2.253). |

|     |                     |  |
|-----|---------------------|--|
| 1.  | Radius server #1    | The IP address of the RADIUS server that is to be used for Authenticating your wireless clients. |
| 2.  | Radius server #2    | The IP address of the second RADIUS server.  |
| 3.  | Authentication port | RADIUS server authentication port.   |
| 4.  | Accounting port     | RADIUS server accounting port.   |
| 5.  | Radius secret key   | The secret key is used for authentication with the RADIUS server                                 |
| 6.  | UAM port            | Port to bind for authenticating clients  |
| 7.  | UAM UI port         | UAM UI port  |
| 8.  | UAM secret          | Shared secret between UAM server an hotspot  |
| 9.  | NAS Identifier      | NAS Identifier   |
| 10. | Swap octets         | Swap the meaning of input octets and output as it related to RADIUS attributes                   |
| 11. | Location name       | The name of location   |

|    |                       |   |
|----|-----------------------|---|
| 1. | External landing page | Enables the use of external landing page. |
| 2. | Landing page address  | The address of external landing page      |
| 3. | HTTPS redirect        | Redirects HTTP pages to landing page.     |

### 8.9.1.2 List Of Addresses The Client Can Access Without First Authenticating

#### Wireless Hotspot Configuration

General Settings

Main Settings

Session Settings

Logout address

List Of Addresses The Client Can Access Without First Authenticating

| Enable                   | Address                                   | Port                                      | Allow subdomains         |                                       |
|--------------------------|---|---|--------------------------|---------------------------------------|
| <input type="checkbox"/> | <input style="width: 100%;" type="text"/> | <input style="width: 100%;" type="text"/> | <input type="checkbox"/> | <input type="button" value="Delete"/> |

|    |                  |   |
|----|------------------|---|
| 1. | Logout address   | IP address to instantly logout a client addressing it |
| 2. | Enable           | Enable address accessing without first authenticating |
| 3. | Address          | Domain name, IP address or network segment            |
| 4. | Port             | Port number   |
| 5. | Allow subdomains | Enable/Disable subdomains                             |

## 8.9.2 Internet Access Restriction Settings

Allows disable internet access on specified day and hour of every week.

RUT200

### Internet Access Restriction Settings

Select Time To Restrict Access On Hotspot RUT200

| Days/Hours | 0-1h | 1-2h | 2-3h | 3-4h | 4-5h | 5-6h | 6-7h | 7-8h | 8-9h | 9-10h | 10-11h | 11-12h | 12-13h | 13-14h | 14-15h | 15-16h | 16-17h | 17-18h | 18-19h | 19-20h | 20-21h | 21-22h | 22-23h | 23-24h |  |
|------------|------|------|------|------|------|------|------|------|------|-------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--|
| Monday     |      |      |      |      |      |      |      |      |      |       |        |        |        |        |        |        |        |        |        |        |        |        |        |        |  |
| Tuesday    |      |      |      |      |      |      |      |      |      |       |        |        |        |        |        |        |        |        |        |        |        |        |        |        |  |
| Wednesday  |      |      |      |      |      |      |      |      |      |       |        |        |        |        |        |        |        |        |        |        |        |        |        |        |  |
| Thursday   |      |      |      |      |      |      |      |      |      |       |        |        |        |        |        |        |        |        |        |        |        |        |        |        |  |
| Friday     |      |      |      |      |      |      |      |      |      |       |        |        |        |        |        |        |        |        |        |        |        |        |        |        |  |
| Saturday   |      |      |      |      |      |      |      |      |      |       |        |        |        |        |        |        |        |        |        |        |        |        |        |        |  |
| Sunday     |      |      |      |      |      |      |      |      |      |       |        |        |        |        |        |        |        |        |        |        |        |        |        |        |  |

Internet access allowed

Internet access blocked

## 8.9.3 Logging

### 8.9.3.1 Configuration

Configuration
Log

### Wireless Hotspot Logging Settings

Logging To FTP Settings

Enable

Server address

User name

Password

Port

|    |                |  |
|----|----------------|--|
| 1. | Enable         | Check this box if you want to enable wireless traffic logging. This feature will produce logs which contain data on what websites each client was visiting during the time he was connected to your hotspot. |
| 2. | Server address | The IP address of the FTP server to which you want the logs uploaded.  |
| 3. | Username       | The username of the user on the aforementioned FTP server.   |
| 4. | Password       | The password of the user.  |
| 5. | Port           | The TCP/IP Port of the FTP server.   |

### FTP Upload Settings

You can configure your timing settings for the log upload via FTP feature here.

Mode

Hours

Minutes

Days  Monday  
 Tuesday  
 Wednesday  
 Thursday  
 Friday  
 Saturday  
 Sunday

|    |                |  |
|----|----------------|--|
| 1. | Mode           | The mode of the schedule. Use "Fixed" if you want the uploading to be done on a specific time of the day. Use "Interval" if you want the uploading to be done at fixed interval.                                     |
| 2. | Interval       | Shows up only when "Mode" is set to Interval. Specifies the interval of regular uploads on one specific day. E.g. If you choose 4 hours, the uploading will be done on midnight, 4:00, 8:00, 12:00, 16:00 and 20:00. |
| 3. | Days           | Uploading will be performed on these days only   |
| 4. | Hours, Minutes | Shows up only when "Mode" is set to Fixed. Uploading will be done on that specific time of the day. E.g. If you want to upload your logs on 6:48 you will have to simply enter hours: 6 and minutes: 48.             |

### 8.9.3.2 Log

**Configuration** | **Log**

## Wifi Log

Wifi Log

Events per page  Search

| MAC ↑                            | IP ↑ | Port ↑ | Date ↑ | Time ↑ |
|----------------------------------|------|--------|--------|--------|
| <i>There are no records yet.</i> |      |        |        |        |

Showing 1 to 1 of 1 entries



## 8.9.4 Landing Page

### 8.9.4.1 General Landing Page Settings

With this functionality you can customize your Hotspot Landing page.

The screenshot shows a web interface for configuring a wireless hotspot landing page. It features a 'General' tab and a 'Template' tab. The main heading is 'Wireless Hotspot Landing Settings'. Under the 'Landing Page Settings' section, there are several fields and buttons: 'Page title' is set to 'Teltonika Hotspot'; 'Theme' is set to 'Custom'; 'Upload login page' has a 'Browse...' button and the text 'No file selected.'; 'Login page file' has a 'Download' button. Below these are several expandable sections: 'Terms Of Services', 'Background Configuration', 'Logo Image Configuration', 'Link Configuration', and 'Text Configuration'.

| 1. | Page title        | Will be seen as landing page title                 |
|----|-------------------|--|
| 2. | Theme             | Landing page theme selection                       |
| 3. | Upload login page | Allows to upload custom landing page theme         |
| 4. | Login page file   | Allows to download and save your landing page file |

In the sections - “Terms Of Services”, “Background Configuration”, “Logo Image Configuration”, “Link Configuration”, “Text Configuration” you can customize various parameters of landing page components.

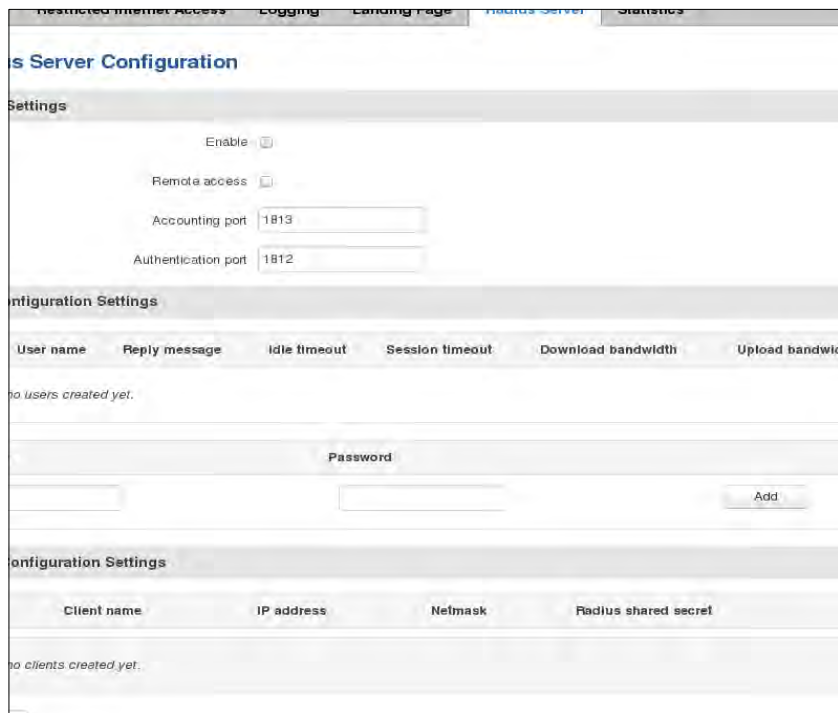
### 8.9.4.2 Template

In this page you can review landing page template HTML code and modify it.



### 8.9.5 Radius server configuration

An authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.



|    |                     |   |
|----|---------------------|---|
|    |                     |   |
| 1. | Enable              | Activates an authentication and accounting system |
| 2. | Remote access       | Activates remote access to radius server          |
| 3. | Accounting port     | Port on which to listen for accounting            |
| 4. | Authentication port | Port on which to listen for authentication        |

### 8.9.6 Statistics

On hotspot statistics page you can review statistical information about hotspot instances.

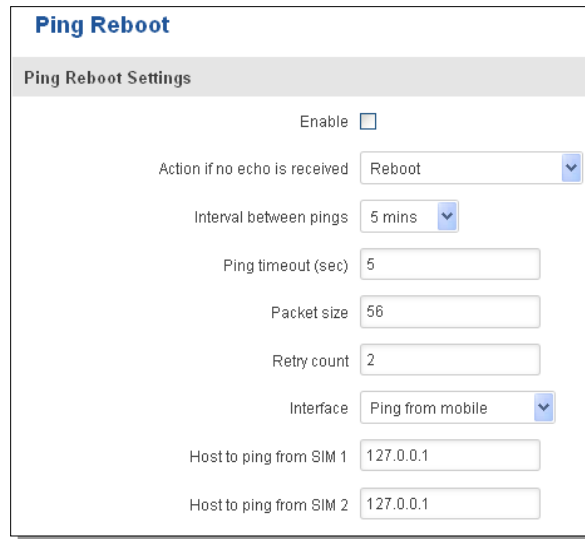




## 8.11 Auto Reboot

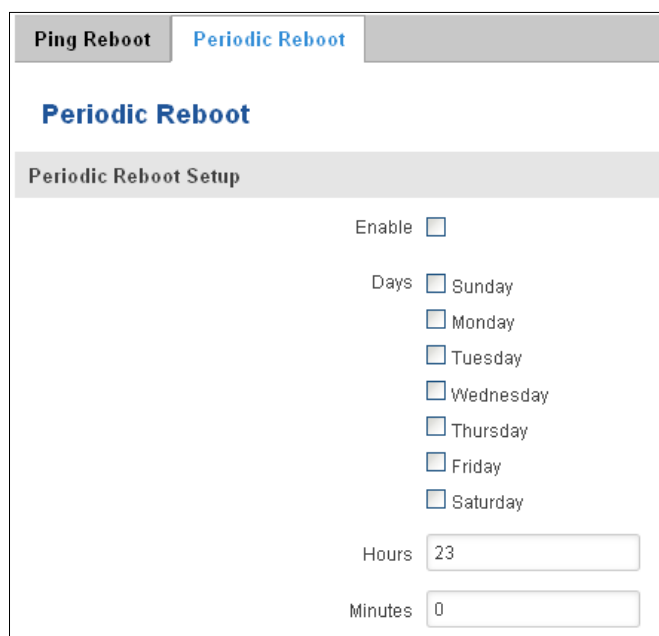
### 8.11.1 Ping Reboot

Ping Reboot function will periodically send Ping command to server and waits for echo receive. If no echo is received router will try again sending Ping command defined number times, after defined time interval. If no echo is received after the defined number of unsuccessful retries, router will reboot. It is possible to turn of the router rebooting after defined unsuccessful retries. Therefore this feature can be used as “Keep Alive” function, when router Pings the host unlimited number of times. Possible actions if no echo is received: Reboot, Modem restart, Restart mobile connection, (Re) register, None.



|    |                               |  |   |
|----|-------------------------------|--|---|
| 1. | Enable                        | This check box will enable or disable Ping reboot feature.   | Ping Reboot is disabled by default.   |
| 2. | Action if no echo is received | Action after the defined number of unsuccessful retries  | No echo reply for sent ICMP (Internet Control Message Protocol) packet received   |
| 3. | Interval between pings        | Time interval in minutes between two Pings.  | Minimum time interval is 5 minutes.   |
| 4. | Ping timeout (sec)            | Time after which consider that Ping has failed.  | Range(1-9999)   |
| 5. | Packet size                   | This box allows to modify sent packet size   | Should be left default, unless necessary otherwise                                |
| 6. | Retry count                   | Number of times to try sending Ping to server after time interval if echo receive was unsuccessful.  | Minimum retry number is 1. Second retry will be done after defined time interval. |
| 8. | Interface                     | Interface used for connection  |   |
| 7. | Host to ping from SIM 1       | IP address or domain name which will be used to send ping packets to. E.g. 127.0.0.1 (or www.host.com if DNS server is configured correctly) | Ping packets will be sending from SIM1.   |
| 8. | Host to ping from SIM 2       | IP address or domain name which will be used to send ping packets to. E.g. 127.0.0.1 (or www.host.com if DNS server is configured correctly) | Ping packets will be sending from SIM2.   |

## 8.11.2 Periodic Reboot



**Periodic Reboot**

Periodic Reboot Setup

Enable

Days  Sunday  
 Monday  
 Tuesday  
 Wednesday  
 Thursday  
 Friday  
 Saturday

Hours

Minutes

| 1. | Enable         | This check box will enable or disable Periodic reboot feature.   |
|----|----------------|--|
| 2. | Days           | This check box will enable router rebooting at the defined days. |
| 3. | Hours, Minutes | Uploading will be done on that specific time of the day          |

## 8.12 Input/Output

### 8.12.1 Main information

Digital OUT: open collector type values, 30V@0.3A.

Digital IN: non-isolated, Logic low 0...+5V, Logic high +8...+40V

### 8.12.2 Status

In this page you can review the current state of router's input and output.

The image shows two screenshots of a web interface for configuring router I/O. The top screenshot, titled "Input/Output Status", features a navigation bar with "Status", "Input", and "Output" tabs. Below the title, there is a table with two columns: "Type" and "State". The first row shows "Digital input" with a state of "1", and the second row shows "Digital output" with a state of "0". Each row has an "Edit" button. A "Restore default" button is located at the top right of the table area. The bottom screenshot, titled "Custom I/O Status Labels", has a navigation bar with "Status", "Input", and "Output" tabs. Below the title, there is a section "Customize Digital input and state fields" containing three input fields: "Digital Input name", "Input shorted state", and "Input open state". At the bottom of this section are two buttons: "Back to Overview" and "Save".

| Type           | State | Restore default |
|----------------|-------|-----------------|
| Digital input  | 1     | Edit            |
| Digital output | 0     | Edit            |

Custom I/O Status Labels

Customize Digital input and state fields

Digital Input name

Input shorted state

Input open state

Back to Overview

|    |                     |                           |
|----|---------------------|---------------------------|
| 1. | Digital Input name  | Digital Input label       |
| 2. | Input shorted state | Input shorted state label |
| 3. | Input open state    | Input open state label    |

## Custom I/O Status Labels

### Customize Digital galvanically isolated input and state fields

Digital Isolated Input name

High logic level state

Low logic level state

[Back to Overview](#)

[Save](#)

| 1. | Digital Isolated Input name | Digital Isolated Input name label |
|----|-----------------------------|-----------------------------------|
| 2. | High logic level state      | High logic level state label      |
| 3. | Low logic level state       | Low logic level state label       |



### 8.12.3 Input

Allows you to set up input parameters and specify what actions should be taken after triggering event of input. In check analog section you can change the analog input checking interval.

Status Input Output

#### Input/Output

Create rules for Input/Output configuration.

##### Input Rules

| Type    | Trigger    | Action   | Enable                              | Sort |   |
|---------|------------|----------|-------------------------------------|------|---|
| Digital | Input open | Send SMS | <input checked="" type="checkbox"/> | ↑ ↓  | <div style="display: flex; justify-content: space-around; width: 100%;"> <span>Edit</span> <span>Delete</span> </div> |

##### Input Configuration

| Input type | Trigger      | Action     |     |
|------------|--------------|------------|-----|
| Digital ▼  | Input open ▼ | Send SMS ▼ | Add |

Save

Status Input Output

#### Input Configuration

Enable

Input type Digital ▼

Triger Input open ▼

Action Send SMS ▼

SMS text open

Digital input - %di  
 Digital isolated input - %ii  
 Analog input - %ai  
 Analog min voltage - %an  
 Analog max voltage - %ax  
 New line - %nl

Recipient's phone number +37063000000 +

Back to Overview
Save

| 1. | Type                      | Digital   | Specifies input type                        |
|----|---------------------------|---|---|
| 2. | Trigger                   | Input open/input shorted/both   | Specifies for which trigger rule is applied |
| 3. | Action                    | Send SMS/Send Email/Change profile/turn WiFi ON or OFF/Reboot/Activate output | Specifies what action is done               |
| 4. | Enable                    | Enable/Disable  | Enable input configuration                  |
| 5. | SMS text                  | Text  | Enter SMS text                              |
| 6. | Recipient's phone numeber | Phone number  | Enter recipient's phone numeber             |

## 8.12.4 Output

### 8.12.4.1 Output configuration

Status Input **Output**

Output Configuration ON/OFF Post/Get Configuration Periodic Control Scheduler

### Output Configuration

Output configuration in active state

Open collector output Low level ▾

Save

|    |                       |                        |   |
|----|-----------------------|------------------------|---|
| 1. | Open collector output | Low level / High level | Choose what open collector output will be in active state |
|----|-----------------------|------------------------|---|

### 8.12.4.2 ON/OFF

Output Configuration **ON/OFF** Post/Get Configuration Periodic Control Scheduler

### Output

Output

Digital OC output Turn on

|    |                   |                    |                                   |
|----|-------------------|--------------------|-----------------------------------|
| 1. | Digital OC output | Turn on / Turn Off | Manually toggle Digital OC output |
|----|-------------------|--------------------|-----------------------------------|

### 8.12.4.3 Post/Get Configuration


Output Configuration ON/OFF **Post/Get Configuration** Periodic Control Scheduler

### Post/Get Configuration

Output Post/Get Settings

Enable

Username

Password  

Save

|    |          |                 |                                      |
|----|----------|-----------------|--------------------------------------|
| 1. | Enable   | Enable /Disable | Enable POST/GET output functionality |
| 2. | Username | User1           | Service user name                    |
| 3. | Password | Pass1           | User password for authentication     |

### Syntax of Output HTTP POST/GET string

With Output post/get you can manage only Output

|    |            |             |  |
|----|------------|-------------|--|
| 1. | IP_ADDRESS | 192.168.1.1 | IP address of your router  |
| 2. | Action     | On and Off  | Specify the action to be taken   |
| 3. | Pin        | Oc          | Specify the output type  |
| 4. | Time (sec) | 10          | Time in seconds after which the output state will go back to usual state |

#### 1. Output HTTP POST/GET string examples

<http://192.168.1.1/cgi-bin/output?username=User1&password=Pass1&action=on&pin=relay>

<http://192.168.1.1/cgi-bin/output?username=User1&password=Pass1&action=on&pin=relay&time=5>

<http://192.168.1.1/cgi-bin/output?username=User1&password=Pass1&action=on&pin=oc>

<http://192.168.1.1/cgi-bin/output?username=User1&password=Pass1&action=off&pin=oc>

### 8.12.4.4 Periodic Control

Periodic control function allows user to set up schedule by which the outputs are either turned ON or OFF at specific time.

|                      |        |                        |                         |           |
|----------------------|--------|------------------------|-------------------------|-----------|
| Output Configuration | ON/OFF | Post/Get Configuration | <b>Periodic Control</b> | Scheduler |
|----------------------|--------|------------------------|-------------------------|-----------|

#### Periodic Output Control

Control Rules

| Action | Mode  | Interval | Hour | Minute | Action timeout | Days | Enable                   |  |
|--------|-------|----------|------|--------|----------------|------|--------------------------|--|
| On     | Fixed | -        | -    | -      | -              | -    | <input type="checkbox"/> | <input type="button" value="Edit"/><br><input type="button" value="Delete"/> |

After clicking on ADD button (Or Edit, if the rule is already created) you get the second periodic output configuration page with extra parameters to set.

#### Edit Output Control Rule

Enable

Output

Action

Action timeout

Timeout (sec)

Mode

Hours

Minutes

Days  Monday  
 Tuesday  
 Wednesday  
 Thursday  
 Friday  
 Saturday  
 Sunday

|    |                |                    |   |
|----|----------------|--------------------|---|
| 1. | Enable         | Enable/Disable     | Enable this output rule                               |
| 2. | Output         | Digital OC output  | Specify the output type                               |
| 3. | Action         | On / Off           | Specify the action to be taken                        |
| 4. | Action timeout | Enabled / Disabled | Enable timeout for this rule                          |
| 5. | Timeout (sec)  | 10                 | Specifies after how much time this action should end. |
| 6. | Mode           | Fixed / Interval   | Specify the mode of output activation                 |
| 7. | Hours          | 15                 | Specify the hour for rule activation                  |
| 8. | Minutes        | 25                 | Specify the minute for rule activation                |
| 9. | Days           | Monday             | Select the week days for rule activation              |

### 8.12.4.5 Scheduler

This function allows you to set up the periodical, hourly schedule for the outputs. You can select on which week days the outputs are going to be on or off.

Output Configuration
ON/OFF
Post/Get Configuration
Periodic Control
Scheduler

## Output Scheduler

### Configure Scheduled Outputs

Output Digital OC output ▼

| Days/Hours | 0-1h | 1-2h | 2-3h | 3-4h | 4-5h | 5-6h | 6-7h | 7-8h | 8-9h | 9-10h | 10-11h | 11-12h | 12-13h | 13-14h | 14-15h | 15-16h | 16-17h | 17-18h | 18-19h | 19-20h | 20-21h | 21-22h | 22-23h | 23-24h |
|------------|------|------|------|------|------|------|------|------|------|-------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| Monday     |      |      |      |      |      |      |      |      |      |       |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| Tuesday    |      |      |      |      |      |      |      |      |      |       |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| Wednesday  |      |      |      |      |      |      |      |      |      |       |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| Thursday   |      |      |      |      |      |      |      |      |      |       |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| Friday     |      |      |      |      |      |      |      |      |      |       |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| Saturday   |      |      |      |      |      |      |      |      |      |       |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| Sunday     |      |      |      |      |      |      |      |      |      |       |        |        |        |        |        |        |        |        |        |        |        |        |        |        |

Digital OC output active

Save

### 8.13 QoS

QoS (Quality of Service) is the idea that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. QoS is of particular concern for the continuous transmission of high-bandwidth video and multimedia information.

QoS can be improved with traffic shaping techniques such as packet, network traffic, and port prioritization.

| Interfaces  |                          |                          |                          |                                   |                                  |                                       |
|---|--------------------------|--------------------------|--------------------------|-----------------------------------|----------------------------------|---------------------------------------|
| Interface   | Enable                   | Calculate overhead       | Half-duplex              | Download speed (kbit/s)           | Upload speed (kbit/s)            |                                       |
| WAN   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="1024"/> | <input type="text" value="128"/> | <input type="button" value="Delete"/> |
| Interface name: <input type="text" value="WAN"/> <input type="button" value="Add"/> |                          |                          |                          |                                   |                                  |                                       |

|    |                         |                |   |
|----|-------------------------|----------------|---|
| 1. | Interface               | WAN/LAN/PPP    |   |
| 2. | Enable                  | Enable/Disable | Enable/disable settings   |
| 3. | Calculate overhead      | Enable/Disable | Check to decrease upload and download ratio to prevent link saturation  |
| 4. | Half-duplex             | Enable/Disable | Check to enable data transmission in both direction on a single carrier |
| 5. | Download speed (kbit/s) | 1024           | Specify maximal download speed  |
| 6. | Upload speed (kbit/s)   | 128            | Specify maximal upload speed  |

| Classification Rules                      |                                      |                                      |                                      |                                      |  |                      |   |
|---|--------------------------------------|--------------------------------------|--------------------------------------|--------------------------------------|--|----------------------|---|
| Target                                    | Source host                          | Destination host                     | Service                              | Protocol                             | Ports  | Number of bytes      | Sort  |
| Priority <input type="button" value="v"/> | All <input type="button" value="v"/> | All <input type="button" value="v"/> | All <input type="button" value="v"/> | All <input type="button" value="v"/> | 22,53 <input type="button" value="v"/>       | <input type="text"/> | <input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="Delete"/> |
| Normal <input type="button" value="v"/>   | All <input type="button" value="v"/> | All <input type="button" value="v"/> | All <input type="button" value="v"/> | TCP <input type="button" value="v"/> | 20,21,25,80 <input type="button" value="v"/> | <input type="text"/> | <input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="Delete"/> |
| Express <input type="button" value="v"/>  | All <input type="button" value="v"/> | All <input type="button" value="v"/> | All <input type="button" value="v"/> | All <input type="button" value="v"/> | 5190 <input type="button" value="v"/>        | <input type="text"/> | <input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="Delete"/> |

## 9 System

### 9.1 Setup Wizard

The configuration wizard provides a simple way of quickly configuring the device in order to bring it up to basic functionality. The wizard is comprised out of 4 steps and they are as follows:

#### Step 1 (General change)

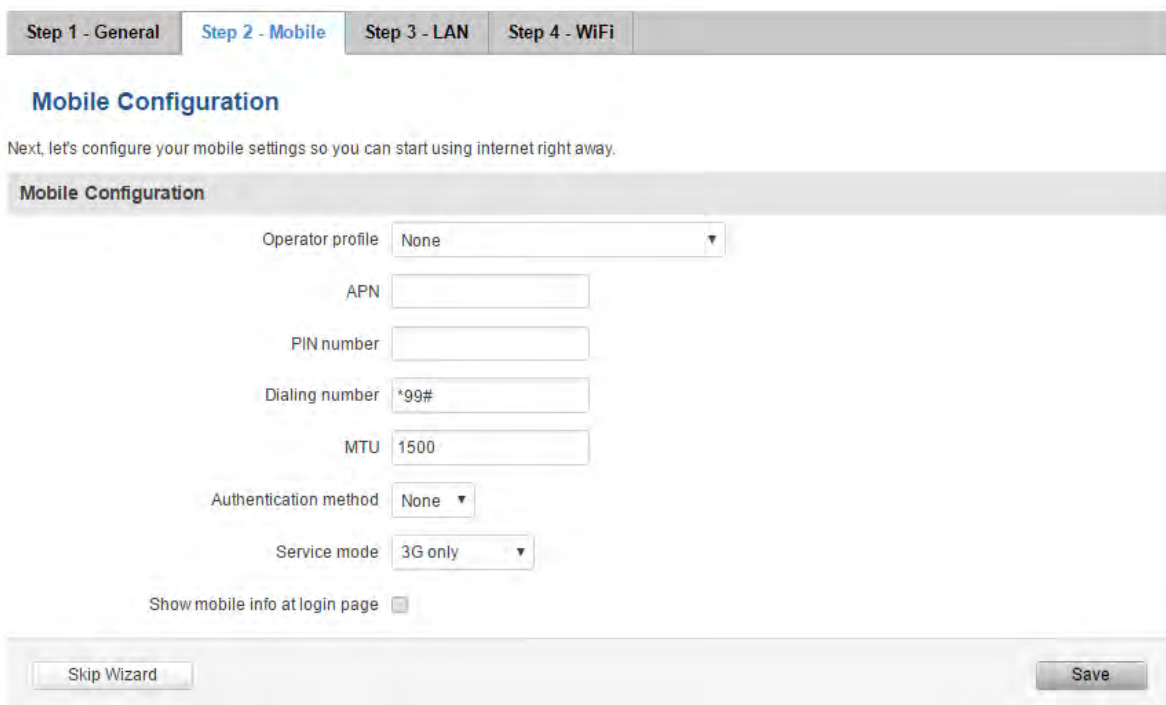
First, the wizard prompts you to change the default password. Simply enter the same password into both Password and Confirmation fields, select time zone and press **Save**.



The screenshot shows the 'Step 1 - General' configuration screen. At the top, there are four tabs: 'Step 1 - General' (selected), 'Step 2 - Mobile', 'Step 3 - LAN', and 'Step 4 - WiFi'. Below the tabs, the title 'Step - General' is displayed. A message reads: 'First, let's change your router password from the default one.' Under the 'Password Settings' section, there are two input fields: 'New password' and 'Confirm new password', both containing six dots. To the right of each field is an eye icon. Below this is the 'Time Zone Settings' section. It shows 'Current system time' as '2016-03-16 09:27:33' and a 'Sync with browser' button. The 'Time zone' is set to 'UTC' with a dropdown arrow.

#### Step 2 (Mobile Configuration)

Next we have to enter your mobile configuration. On a detailed instruction on how this should be done see the Mobile section under Network



The screenshot shows the 'Step 2 - Mobile' configuration screen. At the top, there are four tabs: 'Step 1 - General', 'Step 2 - Mobile' (selected), 'Step 3 - LAN', and 'Step 4 - WiFi'. Below the tabs, the title 'Mobile Configuration' is displayed. A message reads: 'Next, let's configure your mobile settings so you can start using internet right away.' Under the 'Mobile Configuration' section, there are several input fields and dropdown menus: 'Operator profile' (set to 'None'), 'APN' (empty), 'PIN number' (empty), 'Dialing number' (set to '\*99#'), 'MTU' (set to '1500'), 'Authentication method' (set to 'None'), and 'Service mode' (set to '3G only'). At the bottom, there is a checkbox labeled 'Show mobile info at login page' which is unchecked. At the very bottom, there are two buttons: 'Skip Wizard' and 'Save'.

### Step 3 (LAN)

Next, you are given the chance to configure your LAN and DHCP server options. For a detailed explanation see LAN under Network.

Step 1 - General Step 2 - Mobile **Step 3 - LAN** Step 4 - WIFI

#### Step - LAN

Here we will setup the basic settings of a typical LAN configuration. The wizard will cover 2 basic configurations: static IP address LAN and DHCP client.

##### General Configuration

IP address: 192.168.1.1

Netmask: 255.255.255.0

Enable DHCP:

Start: 100

Limit: 150

Lease time: 12h

Skip Wizard Save

### Step 4 (Wi-Fi)

The final step allows you to configure your wireless settings in order to set up a rudimentary Access Point.

Step 1 - General Step 2 - Mobile Step 3 - LAN **Step 4 - WiFi**

#### Step - Wireless

Now let's configure your wireless radio. (Note: if you are currently connecting via wireless and you change parameters, like SSID, encryption, etc. your connection will be dropped and you will have to reconnect with a new set of parameters.)

##### WiFi Configuration

Enable wireless:

SSID: RUT2xx

Mode: 802.11g+n

Channel: Auto

Encryption: No encryption

Country Code: 00 - World

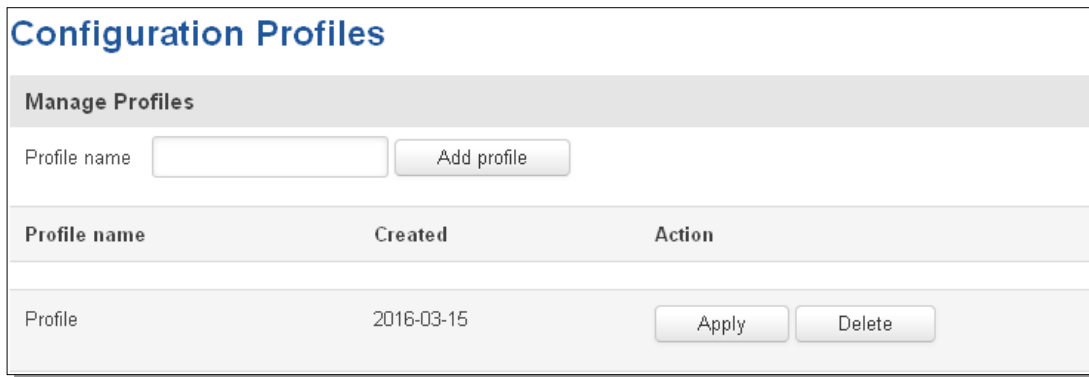
Skip Wizard Save

When you're done with the configuration wizard, press **Save**.



## 9.2 Profiles

Router can have 5 configuration profiles, which you can later apply either via WebUI or via SMS. When you add New Profile, you save **current** full configuration of the router. Note: profile names **cannot** exceed 10 symbols.

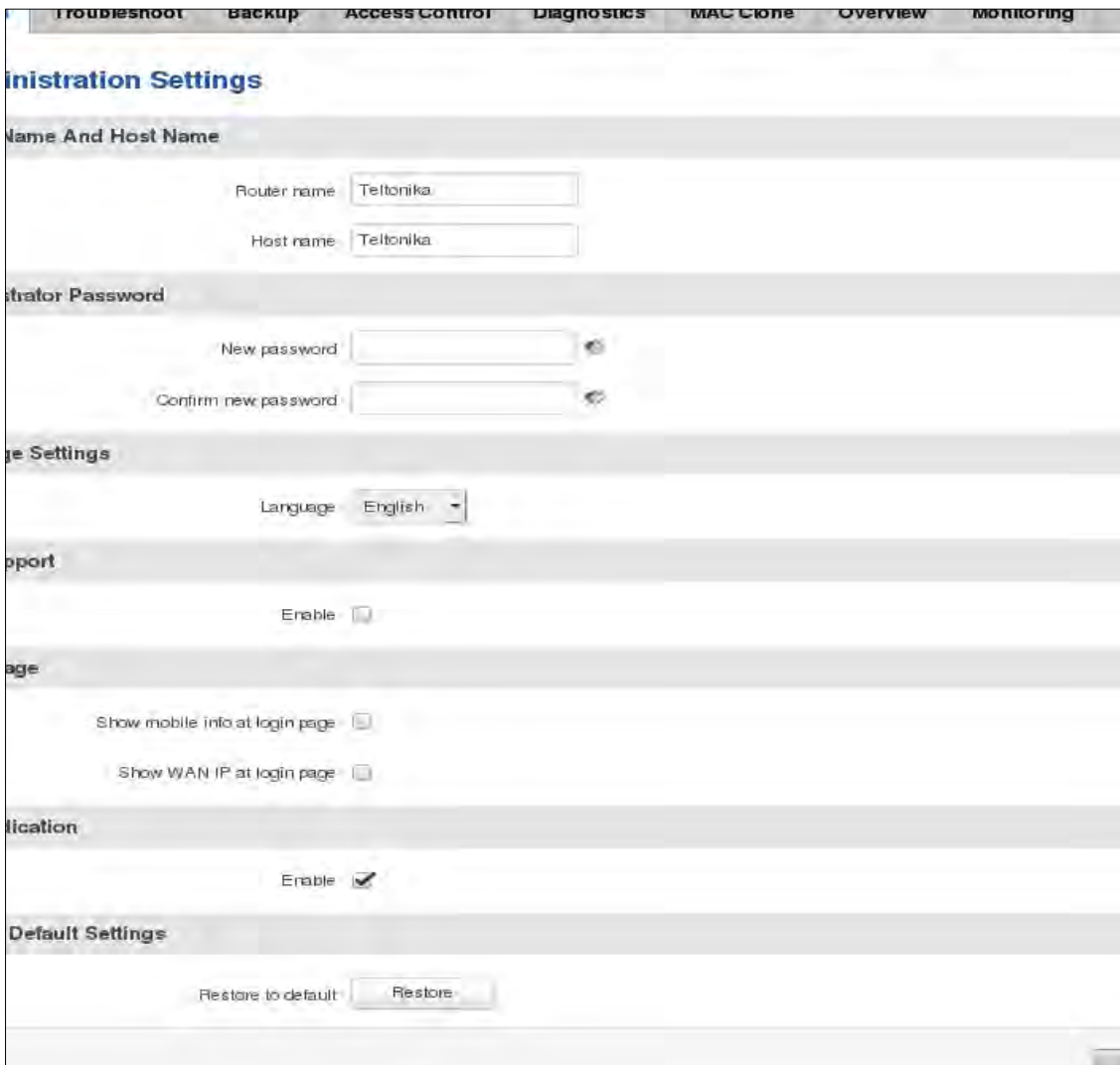


The screenshot shows the 'Configuration Profiles' web interface. At the top, there is a 'Manage Profiles' section with a text input field for 'Profile name' and an 'Add profile' button. Below this is a table with three columns: 'Profile name', 'Created', and 'Action'. The table contains one row with the profile name 'Profile', a creation date of '2016-03-15', and two buttons: 'Apply' and 'Delete'.

| Profile name | Created    | Action   |
|--------------|------------|--|
| Profile      | 2016-03-15 | <input type="button" value="Apply"/> <input type="button" value="Delete"/> |

## 9.3 Administration

### 9.3.1 General



The screenshot shows the 'Administration Settings' web interface. At the top, there is a navigation bar with tabs: 'Troubleshoot', 'Backup', 'Access Control', 'Diagnostics', 'MAC Clone', 'Overview', and 'Monitoring'. The main content area is titled 'Administration Settings' and is divided into several sections:

- Name And Host Name:** Contains two text input fields: 'Router name' (value: Teltonika) and 'Host name' (value: Teltonika).
- Administrator Password:** Contains two text input fields: 'New password' and 'Confirm new password', each with a password strength indicator icon.
- Language Settings:** Contains a dropdown menu for 'Language' (value: English).
- Support:** Contains a checkbox for 'Enable' (unchecked).
- Page:** Contains two checkboxes: 'Show mobile info at login page' (unchecked) and 'Show WAN IP at login page' (unchecked).
- Notification:** Contains a checkbox for 'Enable' (checked).
- Default Settings:** Contains a 'Restore to default' label and a 'Restore' button.

|     |                                |   |
|-----|--------------------------------|---|
| 1.  | Router name                    | Enter your new router name.   |
| 2.  | Host name                      | Enter your new host name  |
| 3.  | New Password                   | Enter your new administration password.<br>Changing this password will change SSH password as well. |
| 4.  | Confirm new password           | Re-enter your new administration password.  |
| 5.  | Language                       | Website will be translated into selected language.  |
| 6.  | IPv6 support                   | Enable IPv6 support on router   |
| 7.  | Show mobile info at login page | Show operator and signal strength at login page.  |
| 8.  | Show WAN IP at login page      | Show WAN IP at login page.  |
| 9.  | On/Off LEDs                    | If uncheck, all routers LEDs are off.   |
| 10. | Restore to default             | Router will be set to factory default settings  |

#### Important notes:

The only way to gain access to the web management if you forget the administrator password is to reset the device factory default settings. Default administrator login settings are:

User Name: **admin**

Password: **admin01**

#### 9.3.2 T

General
Troubleshoot
Backup
Access Control
Diagnostics
MAC Clone
Overview
Monitoring

### Troubleshoot Settings

**Troubleshoot**

System log level Debug ▼

Save log in RAM memory ▼

Include GSMD information

Include PPPD information

Include chat script information

Include network topology information

System log Show

Kernel log Show

Troubleshoot file Download

TCP dump file Download

Enable TCP dump

Select interface any ▼

Select protocol filter All ▼

Select packets direction IN/OUT ▼

Host

Port

Select storage Internal storage ▼

Save

|    |                                      |  |
|----|--------------------------------------|--|
| 1. | System log level                     | Debug level should always be used, unless instructed otherwise.  |
| 2. | Save log in                          | Default RAM memory should always be used unless instructed otherwise.  |
| 3. | Include GSMD information             | Default setting – enabled should be used, unless instructed otherwise.   |
| 4. | Include PPPD information             | Default setting – disabled should be used, unless instructed otherwise.  |
| 5. | Include Chat script information      | Default setting – enabled should be used, unless instructed otherwise.   |
| 6. | Include network topology information | Default setting – disabled should be used, unless instructed otherwise.  |
| 7. | System Log                           | Provides on-screen System logging information. It does not, however, substitute troubleshooting file that can be downloaded from System -> Backup and Firmware menu. |
| 8. | Kernel Log                           | Provides on-screen Kernel logging information. It does not, however, substitute troubleshooting file that can be downloaded from System -> Backup and Firmware       |

9. Tr **General** **Troubleshoot** **Backup** **Access Control** **Diagnostics** **MAC Clone** **Overview** **Monitoring**

10. TC **Backup**

**Backup Configuration**

### 9.3.3 B

Backup archive:

1. Bac **Restore Configuration**

2. Res

Restore from backup:  No file chosen

\*Only configuration file from identical device with same firmware can be uploaded

### 9.3.3.1 Access control

#### 9.3.3.1.1 General

General
Safety

#### Access Control

**SSH**

Enabling remote SSH access makes your device reachable from WAN, this might pose a security risk, especially if you are using a weak or default user password!

Enable SSH access

Remote SSH access

Port

**WebUI**

Enabling remote HTTP access or remote HTTPS access makes your device reachable from WAN, this might pose a security risk, especially if you are using a weak or default user password!

Enable HTTP access

Enable remote HTTP access

Port

Enable remote HTTPS access

Port

Enable JSON RPC

**CLI**

Enabling remote CLI access makes your device reachable from WAN, this might pose a security risk, especially if you are using a weak or default user password!

Enable CLI

Enable remote CLI

Port

|     |                            |   |
|-----|----------------------------|---|
| 1.  | Enable SSH access          | Check box to enable SSH access.         |
| 2.  | Remote SSH access          | Check box to enable remote SSH access.  |
| 3.  | Port                       | Port to be used for SSH connection      |
| 4.  | Enable HTTP access         | Enables HTTP access to router           |
| 5.  | Enable remote HTTP access  | Enables remote HTTP access to router    |
| 6.  | Port                       | Port to be used for HTTP communication  |
| 7.  | Enable remote HTTPS access | Enables remote HTTPS access to router   |
| 8.  | Port                       | Port to be used for HTTPS communication |
| 9.  | Enable JSON RPC            | Enables JSON RPC communication          |
| 10. | Enable CLI                 | Enables Command Line Interface          |
| 11. | Enable remote CLI          | Enables remote Command Line Interface   |
| 12. | Port                       | Port to be used for CLI communication   |

**Note:** The router has 2 users: “admin” for WebUI and “root” for SSH. When logging in via SSH use “root”.

### 9.3.3.1.2 Safety

The screenshot shows the 'Access Control' configuration page with the 'Safety' sub-tab selected. The main heading is 'Block Unwanted Access'. There are two sections: 'SSH Access Secure' and 'WebUI Access Secure'. Each section has an 'Enable' checkbox, a 'Clean after reboot' checkbox, and a 'Fail count' input field set to '5'. Below these is a 'List Of Blocked Addresses' section with a search bar and a table with columns for 'Service', 'Blocked address', and 'Blocked date'. The table is currently empty, showing 'There are no addresses blocked' and 'Showing 1 to 1 of 1 entries'.

|    |                            |  |
|----|----------------------------|--|
| 1. | SSH access secure enable   | Check box to enable SSH access secure functionality.                         |
| 2. | Clean after reboot         | If check box is selected – blocked addresses are removed after every reboot. |
| 3. | Fail count                 | Specifies maximum connection attempts count before access blocking.          |
| 4. | WebUI access secure enable | Check box to enable secure WebUI access.                                     |

### 9.3.4 Diagnostics

The screenshot shows the 'Diagnostics' configuration page with the 'Diagnostics' sub-tab selected. The main heading is 'Diagnostics'. Below it is a section titled 'Network Utilities'. There is a 'Host' input field and an 'Action' section with three buttons: 'Ping', 'Traceroute', and 'Nslookup'.

|    |            |  |
|----|------------|--|
| 1. | Host       | Enter server IP address or hostname.   |
| 2. | Ping       | Utility used to test the reach ability of a host on an Internet IP network and to measure the round-trip time for messages sent from the originating host to a destination server. Server echo response will be shown after few seconds if server is accessible. |
| 3. | Traceroute | Diagnostics tool for displaying the route (path) and measuring transit delays of packets across an Internet IP network. Log containing route information will be shown after few seconds.  |
| 4. | Nslookup   | Network administration command-line tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record. Log containing specified server DNS lookup information will be shown after few seconds.     |

### 9.3.5 MAC Clone

|    |                 |                            |
|----|-----------------|----------------------------|
| 1. | WAN MAC address | Enter new WAN MAC address. |
|----|-----------------|----------------------------|

### 9.3.6 Overview

Select which information you want to get in Overview window (Status -> Overview).

| 1.  | Mobile                | Check box to show Mobile table in Overview page                |
|-----|-----------------------|--|
| 2.  | SMS counter           | Check box to show SMS counter table in Overview page           |
| 3.  | System                | Check box to show System table in Overview page                |
| 4.  | Wireless              | Check box to show Wireless table in Overview page              |
| 5.  | WAN                   | Check box to show WAN table in Overview page                   |
| 6.  | Local network         | Check box to show Local network table in Overview page         |
| 7.  | Access control        | Check box to show Access control table in Overview page        |
| 8.  | Recent system events  | Check box to show Recent system events table in Overview page  |
| 9.  | Recent network events | Check box to show Recent network events table in Overview page |
| 10. | VRRP                  | Check box to show VRRP table in Overview page                  |
| 11. | Monitoring            | Check box to show Monitoring table in Overview page            |

### 9.3.7 Monitoring

Monitoring functionality allows your router to be connected to Remote Monitoring System. Also MAC address and router serial numbers are displayed for convenience in this page, because they are needed when adding device to monitoring system.

| 1. | Enable remote monitoring | Check box to enable/disable remote monitoring     |
|----|--------------------------|---|
| 2. | Hostname                 | The name of the host                              |
| 3. | Port                     | Port number                                       |
| 4. | Monitoring               | Shows monitoring status.                          |
| 5. | Connection state         | Shows if router is connected to monitoring system |
| 6. | Router LAN MAC address   | MAC address of the Ethernet LAN ports             |
| 7. | Router serial number     | Serial number of the device                       |

## 9.4 User scripts

Advanced users can insert their own commands that will be executed at the end of booting process.

**Startup Script Management**

Insert your own commands to execute at the end of the boot process.

```
# Put your custom commands here that should be executed once
# the system init finished. By default this file does nothing.

exit 0
```

Upload script file  No file chosen

Backup script file

In *Script Management* window is shown content of a file `/etc/rc.local`. This file is executed at the end of startup, executing the line: `sh /etc/rc.local` In this script is needed to use `sh` (ash) commands. It should be noted, that this is embedded device and `sh` functionality is not full.

## 9.5 Firmware

### 9.5.1 Firmware

**Firmware** **FOTA**

### Firmware

| Current Firmware Information |                      | Firmware Available On Server  |     |
|------------------------------|----------------------|---|-----|
| Firmware version             | RUT2XX_T_00.00.180   | Firmware version  | N/A |
| Firmware build date          | 2017-04-13, 08:52:16 | <input style="float: right;" type="button" value="Check for New FW"/> |     |
| Kernel version               | 3.18.44              |   |     |
| Bootloader version           | 1.0.0                |   |     |

### Firmware Upgrade Settings

Keep mobile settings

Upgrade from file  No file chosen



**Keep mobile settings** – if the check box is selected router will keep saved user mobile configuration settings after firmware upgrade.

**FW image** – router firmware upgrade file.

**Warning:** Never remove router power supply and do not press reset button during upgrade process! This would seriously damage your router and make it inaccessible. If you have any problems related to firmware upgrade you should always consult with local dealer.

## 9.5.2 FOTA

The screenshot shows the 'Firmware Over The Air Configuration' (FOTA) settings page. At the top, there are two tabs: 'Firmware' and 'FOTA', with 'FOTA' being the active tab. Below the tabs is the title 'Firmware Over The Air Configuration'. Underneath is a section titled 'Server Settings' containing several configuration options:

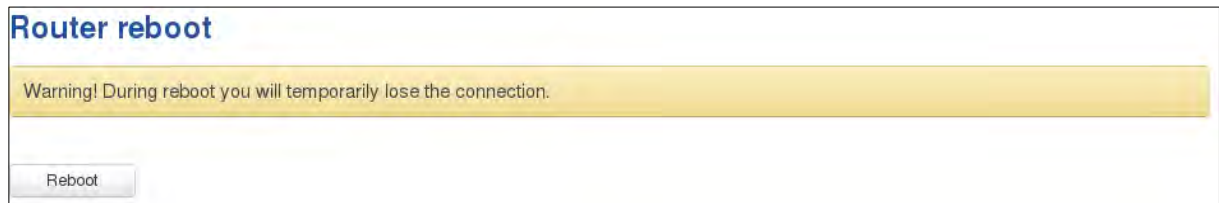
- Server address:** A text input field containing the URL `http://rms.teltonika.it/fota/`.
- User name:** A text input field containing the text `admin`.
- Password:** A password input field with masked characters (dots) and a small eye icon to toggle visibility.
- Enable auto check:** A checkbox that is currently checked.
- Auto check mode:** A dropdown menu set to 'On router startup'.
- WAN wired:** A checkbox that is currently unchecked.

At the bottom right of the configuration area, there is a 'Save' button.

|    |                |  |
|----|----------------|--|
| 1. | Server address | Specify server address to check for firmware updates. E.g. |
|----|----------------|--|

|    |                   |   |
|----|-------------------|---|
|    |                   | "http://teltonika.sritis.lt/rut9xx_auto_update/clients/"                                |
| 2. | User name         | User name for server authorization.   |
| 3. | Password          | Password name for server authorization.   |
| 4. | Enable auto check | Check box to enable automatic checking for new firmware updates.                        |
| 5. | Auto check mode   | Select when to perform auto check function.   |
| 6. | WAN wired         | Allows to update firmware from server only if routers WAN is wired (if box is checked). |

## 9.6 Reboot



Reboot router by pressing button "Reboot".

## 10 Device Recovery

The following section describes available options for recovery of malfunctioning device. Usually device can become unreachable due to power failure during firmware upgrade or if its core files were wrongly modified in the file system. Teltonika's routers offer several options for recovering from these situations.

### 10.1 Reset button

Reset button is located on the back panel of the device. Reset button has several functions:

**Reboot the device.** After the device has started and if the reset button is pressed for up to 4 seconds the device will reboot. Start of the reboot will be indicated by flashing of all 5 signal strength LEDs together with green connection status LED.

**Reset to defaults.** After the device has started if the reset button is pressed for at least 5 seconds the device will reset all user changes to factory defaults and reboot. To help user to determine how long the reset button should be pressed, signal strength LEDs indicates the elapsed time. All 5 lit LEDs means that 5 seconds have passed and reset button can be released. Start of the reset to defaults will be indicated by flashing of all 5 signal strength LEDs together with red connection status LED. SIM PIN on the main SIM card is the only user parameter that is kept after reset to defaults.

### 10.2 Bootloader's WebUI

Bootloader also provides a way to recover the router functionality when the firmware is damaged. To make it easier to use bootloader has its own webserver that can be accessed with any web browser.

Procedure for starting bootloader's webserver:

**Automatically.** It happens when bootloader does not detect master firmware. Flashing all 4 Ethernet LEDs indicate that bootloader's webserver has started.

**Manually.** Bootloader's webserver can be requested by holding reset button for 3 seconds while powering the device on. Flashing all 4 Ethernet LEDs indicates that bootloader's webserver has started.

Bootloader's WebUI can be accessed by typing this address in the web browser: 192.168.1.1/index.html

Note: it may be necessary to clear web browser's cache and to use incognito/anonymous window to access bootloader's WebUI.

## 11 FCC Regulations

FCC ID : 2AET4RUT240V

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution: Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

FCC RF Exposure Information

This device complies with the relevant RF radiation exposure limit set forth for an uncontrolled environment. This device must be installed and operated with the minimum distance 20cm between the radiator and your body. This device must be not co-located or operating in conjunction with any other antenna or transmitter.

## 12 Glossary

WAN – Wide Area Network is a telecommunication network that covers a broad area (i.e., any network that links across metropolitan, regional, or national boundaries). Here we use the term WAN to mean the external network that the router uses to reach the internet.

LAN – A local area network (LAN) is a computer network that interconnects computers in a limited area such as a home, school, computer laboratory, or office building.

DHCP – The Dynamic Host Configuration Protocol (DHCP) is a network configuration protocol for hosts on Internet Protocol (IP) networks. Computers that are connected to IP networks must be configured before they can communicate with other hosts. The most essential information needed is an IP address, and a default route and routing prefix. DHCP eliminates the manual task by a network administrator. It also provides a central database of devices that are connected to the network and eliminates duplicate resource assignments.

ETHERNET CABLE – Refers to the CAT5 UTP cable with an RJ-45 connector.

AP – Access point. An access point is any device that provides wireless connectivity for wireless clients. In this case, when you enable Wi-Fi on your router, your router becomes an access point.

DNS – Domain Name System. A server that translates names such as to their respective IPs. In order for your computer or router to communicate with some external server it needs to know it's IP, its name "" just won't do. There are special servers set in place that perform this specific task of resolving names into IPs, called Domain Name servers. If you have no DNS specified you can still browse the web, provided that you know the IP of the website you are trying to reach.

ARP – Short for Adress Resolution Protocol a used to convert an into a physical address (called a ), such as an address.

PPPoE – Point-to-Point Protocol over Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the internet through a common broadband medium, such as DSL line, wireless device or cable modem.

DSL – digital subscriber line - it is a family of technologies that provide internet access by transmitting digital data using a local telephone network which uses the public switched telephone network.

NAT – network address translation – an internet standard that enables a local-area network (LAN) to use one set of IP addresses for internet traffic and a second set of addresses for external traffic.

LCP – Link Control Protocol – a protocol that is part of the PPP (Point-to-Point Protocol). The LCP checks the identity of the linked device and either accepts or rejects the peer device, determines the acceptable packet size for transmission, searches for errors in configuration and can terminate the link if the parameters are not satisfied.

BOOTP – Bootstrap Protocol – an internet protocol that enables a diskless workstation to discover its own IP address, the IP address of a BOOTP server on the network, and a file to be loaded into memory to boot the machine. This enables the workstation to boot without requiring a hard or floppy disk drive.

TCP – Transmission Control Protocol – one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

TKIP – Temporal Key Integrity Protocol – scrambles the keys using hashing algorithm and, by adding an integrity-checking feature, ensure that the keys haven't been tampered with.

CCMP – Counter Mode Cipher Block Chaining Message Authentication Code Protocol – encryption protocol designed for Wireless LAN products that implement the standards of the IEEE 802.11i amendment to the original IEEE802.11 standard. CCMP is an encrypted data cryptographic encapsulation designed for data confidentiality and based upon the Counter Mode with CBC-MAC (CCM) of the AES (Advanced Encryption Standard) standard.

MAC – Media Access Control. Hardware address which uniquely identifies each node of the network. In IEEE 802 networks, the Data Link Control (DCL) layer of the ISO Reference Model is divided into two sub-layers: the Logical Link Control (LLC) layer and the Media Access Control layer. The MAC layer interfaces directly with the network medium. Consequently, each different type of network medium requires a different MAC layer.

DMZ – Demilitarized Zone – a computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public internet.

UDP – User Datagram Protocol – a connectionless protocol that, like TCP, runs on top of IP networks. Provides very few error recovery services, offering instead a direct way to send and receive datagrams over IP network.

VPN – Virtual Private Network – a network that is constructed by using public wires — usually the Internet — to connect to a private network, such as a company's internal network.

VRRP – Virtual Router Redundancy Protocol – an election protocol that dynamically assigns responsibility for one or more virtual router(s) to the VRRP router(s) on a LAN, allow several routers on a multiaccess link to utilize the same virtual IP address.

GRE Tunnel – Generic Routing Encapsulation – a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork.

PPPD – Point to Point Protocol Daemon – it is used to manage network connections between two nodes on Unix-like operating systems. It is configured using command-line arguments and configuration files.

SSH – Secure Shell – a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels.

VRRPD – Virtual Router Redundancy Protocol – it is designed to eliminate the single point of failure associated with statically routed networks by automatically providing failover using multiple LAN paths through alternate routers.

SNMP – Simple Network Management Protocol - a set of protocols for managing complex networks. SNMP works by sending messages, called *protocol data units (PDUs)*, to different parts of a network.