



USER MANUAL

RUT950 LTE Router



Legal notice

Copyright © 2015 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 adaptor.

Table of Contents

Legal notice.....	2
Attention.....	2
SAFETY INFORMATION	8
Device connection	9
1 Introduction	10
2 Specifications	10
2.1 Ethernet	10
2.2 Wi-Fi.....	10
2.3 Hardware	10
2.4 Electrical, Mechanical & Environmental.....	10
2.5 Applications	11
3 Setting up your router	12
3.1 Installation	12
3.1.1 Front Panel and Back Panel	12
3.1.2 Hardware installation	12
3.2 Logging in.....	13
4 Operation Modes.....	16
5 Powering Options	16
5.1 Powering the device from higher voltage.....	17
6 Status	18
6.1 Overview	18
6.2 System Information	19
6.3 Network Information.....	20
6.4 Device information	31
6.5 Services	32
6.6 Routes	32
6.6.1 ARP.....	32
6.6.2 Active IP-Routes.....	33
6.6.3 Active IPv6-Routes	33
6.7 Realtime Graphs	34
6.7.1 Mobile Signal Strenght.....	34
6.7.2 Realtime Load	35
6.7.3 Traffic.....	36

6.7.4	Realtime Wireless	37
6.7.5	Realtime Connections	38
6.8	Mobile Traffic.....	39
6.9	Speed Test.....	39
6.10	Events Log	40
6.10.1	All Events	40
6.10.2	System Events.....	41
6.10.3	Network Events	42
6.10.4	Events Reporting	43
6.10.5	Reporting Configuration	44
7	Network	46
7.1	Mobile.....	46
7.1.1	General.....	46
7.1.2	SIM Management	48
7.1.3	Network Operators	49
7.1.4	Mobile Data Limit.....	50
7.1.5	Sim Idle protection.....	51
7.2	WAN.....	52
7.2.1	Operation Mode	52
7.2.2	Common configuration	53
7.3	LAN.....	59
7.3.1	Configuration	59
7.3.2	DHCP Server	60
7.4	VLAN.....	61
7.4.1	VLAN Networks	61
7.4.2	LAN Networks	63
7.5	Wireless	63
7.6	Firewall.....	66
7.6.1	General Settings.....	66
7.6.2	DMZ.....	67
7.6.3	Port Forwarding	67
7.6.4	Traffic Rules.....	69
7.6.5	Custom Rules	74
7.6.6	DDOS Prevention	75
7.7	Static Routes	78

8	Services	79
8.1	VRRP.....	79
8.1.1	VRRP LAN Configuration Settings	79
8.1.2	Check Internet connection.....	79
8.2	TR-069	80
8.2.1	TR-069 Parameters Configuration	80
8.3	Web filter	81
8.3.1	Site blocking.....	81
8.3.2	Proxy based URL content blocker	81
8.4	NTP.....	82
8.5	VPN	83
8.5.1	OpenVPN.....	83
8.5.2	IPSec.....	86
8.5.3	GRE Tunnel.....	89
8.5.4	PPTP	91
8.5.5	L2TP.....	92
8.6	Dynamic DNS.....	93
8.7	SNMP	94
8.7.1	SNMP Settings.....	94
8.7.2	TRAP Settings	95
8.8	SMS Utilities	96
8.8.1	SMS Utilities	96
8.8.2	Call Utilities	99
8.8.3	User Groups	99
8.8.4	SMS Management.....	100
8.8.5	Remote Configuration.....	101
8.8.6	Statistics	105
8.9	SMS Gateway	105
8.9.1	Post/Get Configuration.....	105
8.9.2	Email to SMS	107
8.9.3	Scheduled Messages.....	108
8.9.4	Auto Reply Configuration.....	110
8.9.5	SMS Forwarding.....	111
8.9.6	SMPP.....	114
8.10	CLI.....	115

8.11	Hotspot	115
8.11.1	General settings.....	115
8.11.2	Internet Access Restriction Settings.....	117
8.11.3	Logging.....	117
8.11.4	Landing Page.....	119
8.11.5	Radius server configuration.....	121
8.11.6	Statistics.....	122
8.12	Auto Reboot.....	122
8.12.1	Ping Reboot	122
8.12.2	Periodic Reboot	123
8.13	QoS.....	124
9	System.....	125
9.1	Configuration Wizard.....	125
9.2	Profiles	127
9.3	Administration	128
9.3.1	General.....	128
9.3.2	Troubleshoot.....	129
9.3.3	Backup.....	130
9.3.4	Diagnostics	132
9.3.5	MAC Clone	132
9.3.6	Overview	133
9.3.7	Monitoring	134
9.4	User scripts	134
9.5	Safe mode.....	135
9.6	Firmware.....	135
9.6.1	Firmware	135
9.6.2	FOTA.....	136
9.7	Restore point	137
9.7.1	Restore point create	137
9.7.2	Restore point load.....	137
9.8	Reboot.....	137
10	Device Recovery.....	137
10.1	Reset button	138
10.2	Safemode	138
10.3	Bootloader's WebUI.....	138

11 Glossary:.....139

SAFETY INFORMATION

In this document you will be introduced on how to use a RUT950 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 overcurrent protective device should not exceed 2A.



The highest transient overvoltage 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.



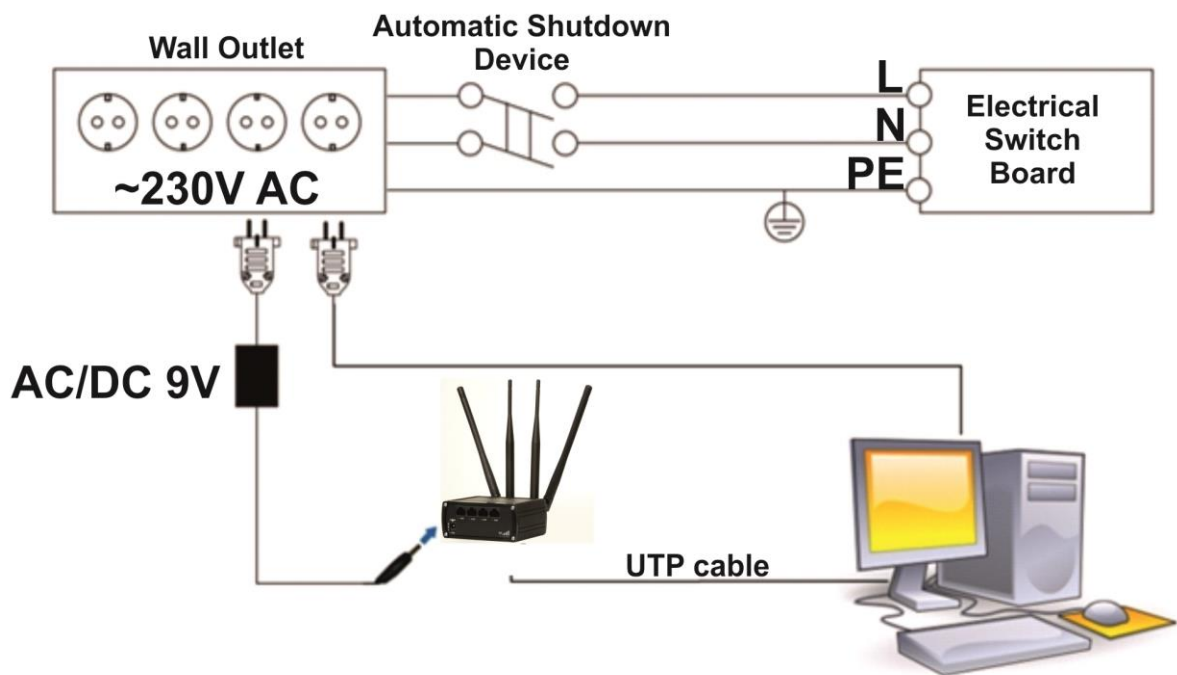
Protection in primary circuits of associated PC and PSU (LPS) against short circuits and earth faults of associated PC shall be provided as part of the building installation.

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 overcurrent, 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 RUT950 LTE router!

RUT950 is part of the RUT9xx series of compact mobile routers with high speed wireless and Ethernet connections.

This router is ideal for people who'd 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
- 3 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
- 2x2 MIMO
- 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

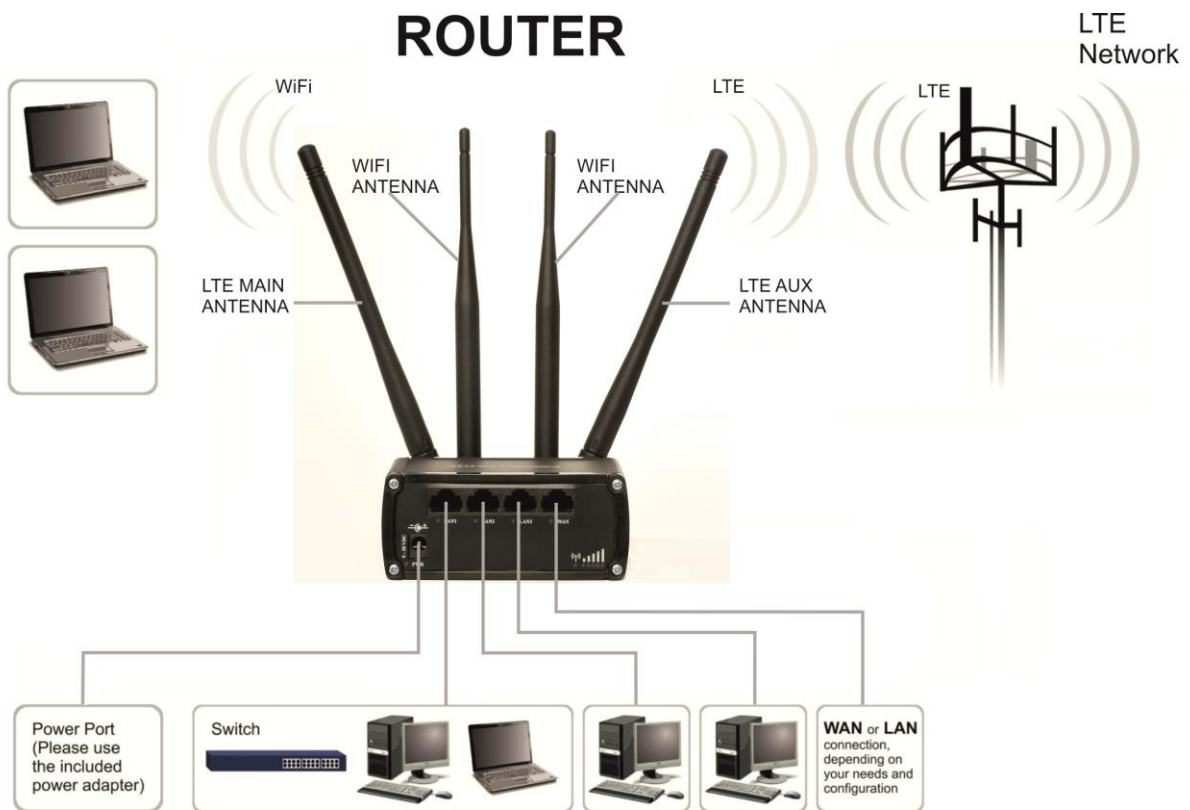
2.3 Hardware

- High performance 560 MHz CPU with 128 Mbytes of DDR2 memory
- 5.5/2.5mm DC power socket
- Reset/restore to default button
- 2 x SMA for LTE , 2 x RP-SMA for WiFi antenna connectors
- 4 x Ethernet LEDs, 1 x Power LED
- 1 x bi-color connection status LED, 5 x connection strength LEDs

2.4 Electrical, Mechanical & Environmental

- | | |
|--------------------------|-------------------------------------|
| • Dimensions (H x W x D) | 80mm x 106mm x 46mm |
| • Weight | 250g |
| • Power supply | 100 – 240 VAC -> 9 VDC wall adapter |
| • Input voltage range | 9 – 30VDC |
| • Power consumption | < 7W |
| • 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



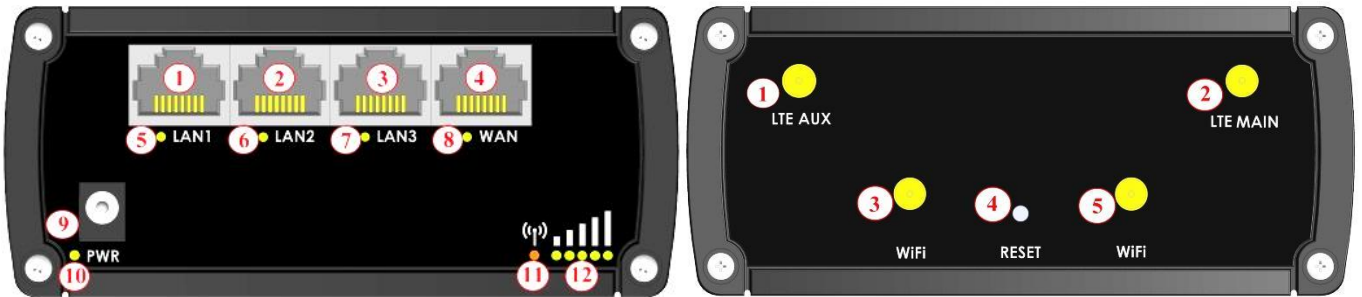
3 Setting up your router

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

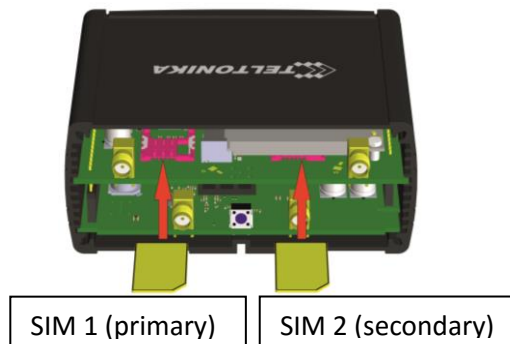


1,2,3	LAN Ethernet ports
4	WAN Ethernet port
5,6,7	LAN LEDs
8	WAN LED
9	Power socket
10	Power LED
11	Connection status LED
12	Signal strength indication LEDs

1	LTE auxiliary antenna connector
2	LTE main antenna connector
3,5	Wi-Fi antenna connectors
4	Reset button

3.1.2 Hardware installation

1. Remove back panel and insert SIM card which was given by your ISP (Internet Service Provider). Correct SIM card orientation is shown in the picture.



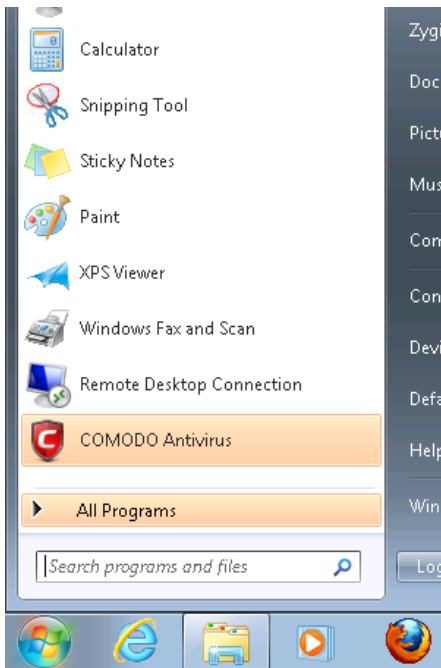
2. Attach LTE main and Wi-Fi antennas.
3. Connect the power adapter to the socket on the front panel of the device. Then plug the other end of the power adapter into a wall outlet or power strip.
4. Connect to the device wirelessly (SSID: **Teltonika_Router**) or use Ethernet cable and plug it into any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

3.2 Logging in

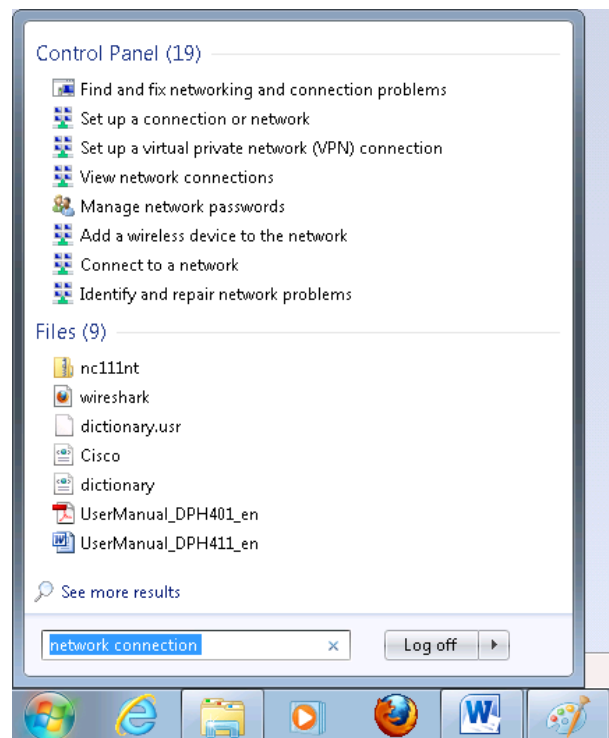
After you're complete with the setting up as described in the section above, you are ready to start logging into your router and start configuring it. This example shows how to connect on Windows 7. On windows Vista: click Start -> Control Panel -> Network and Sharing Centre -> Manage network Connections -> (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.

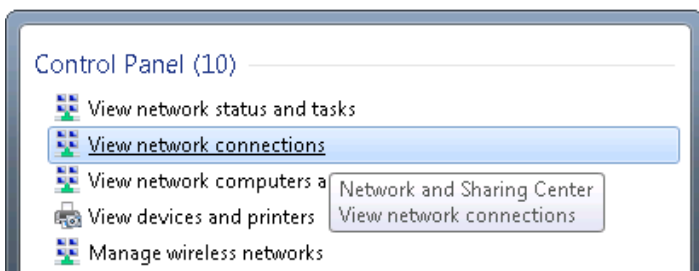
1. Press the start button



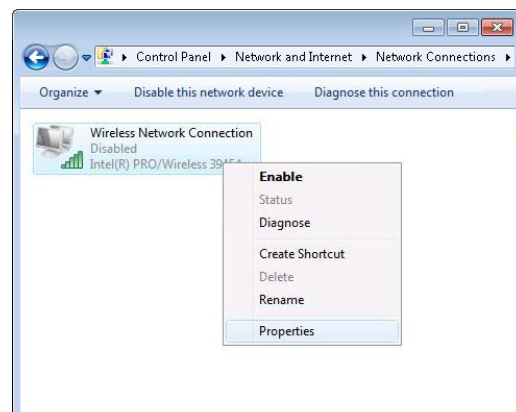
2. Type in "network connections", wait for the results to pop up.



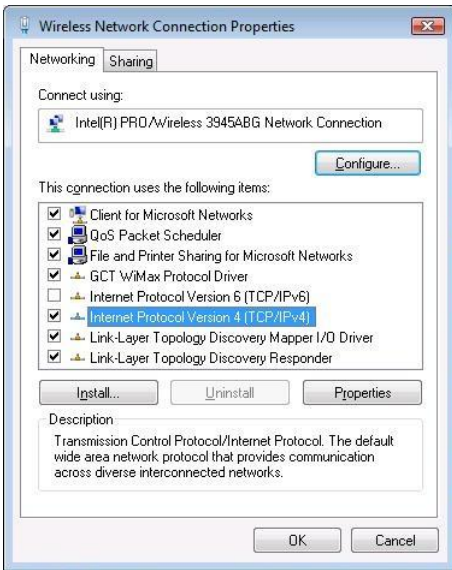
3. Click "View network connections"



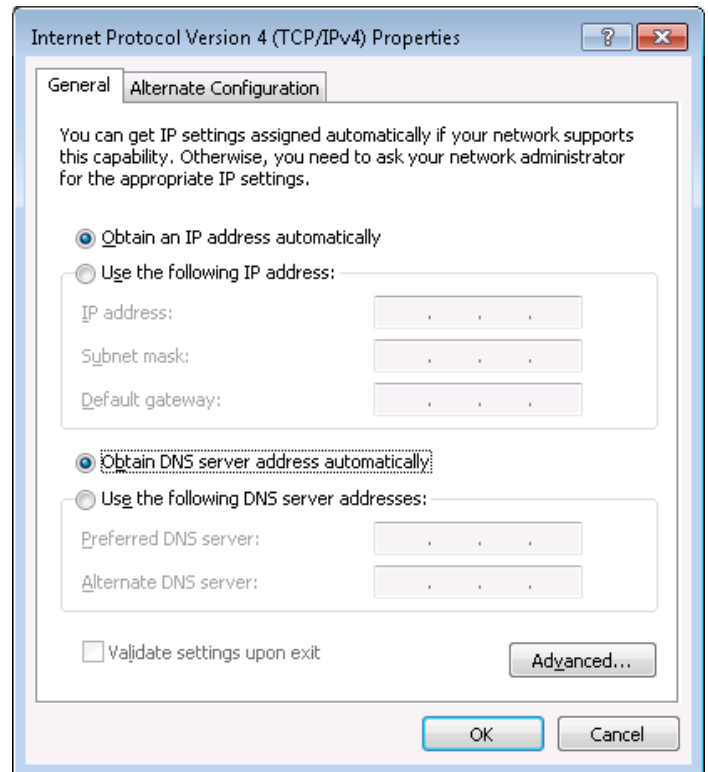
4. Then right click on your wireless device that you use to connect to other access points (It is the one with the name "Wireless Network Connection" and has signal bars on its icon).



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

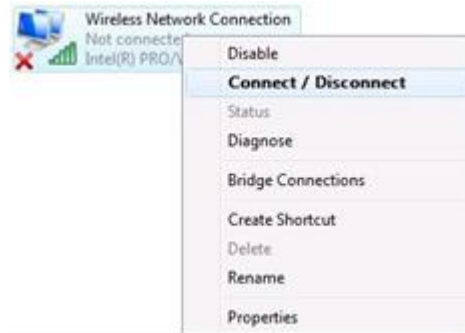
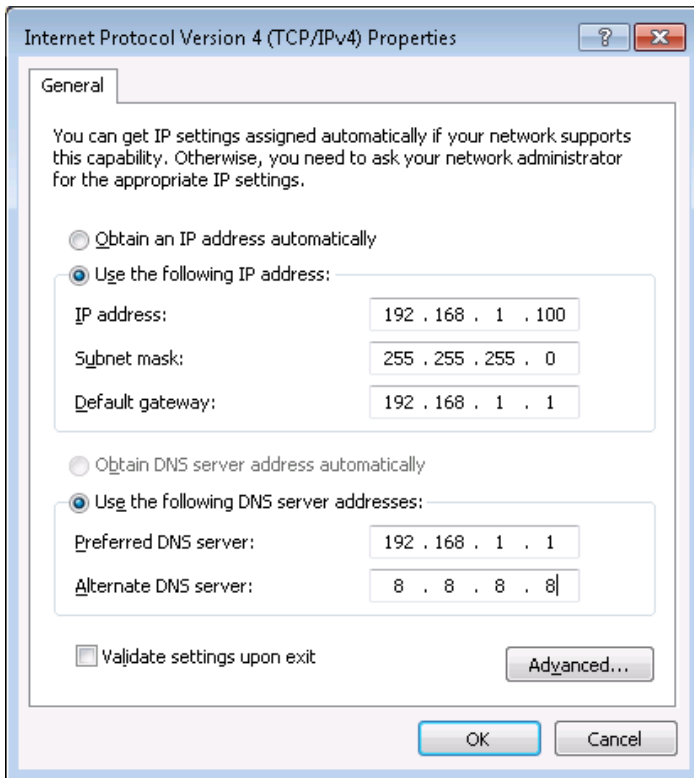


6. By default the router is going to have DHCP enabled, which means that if you select "Obtain an IP address automatically" and "Obtain DNS server address automatically", the router should lease you an IP and you should be ready to login.



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

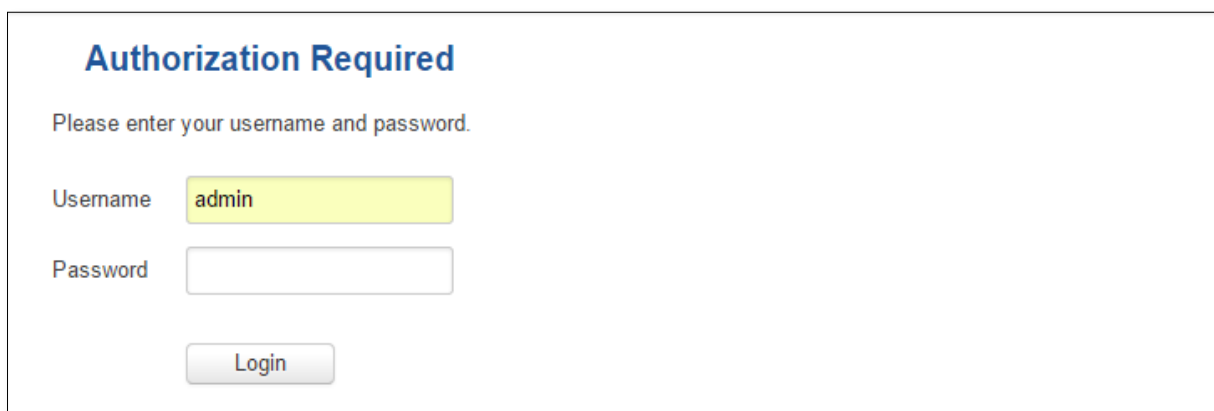
First select an IP address. Due to the stock settings that your router has arrived in you can only enter an IP in the form of 192.168.1.XXX , where XXX is a number in the range of 2-254 (192.168.1.2 , 192.168.1.254 , 192.168.1.155 and so on... are valid; 192.168.1.0 , 192.168.1.1 , 192.168.1.255 , 192.168.1.699 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 IPs. 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 routers 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 RUT950!

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

4 Operation Modes

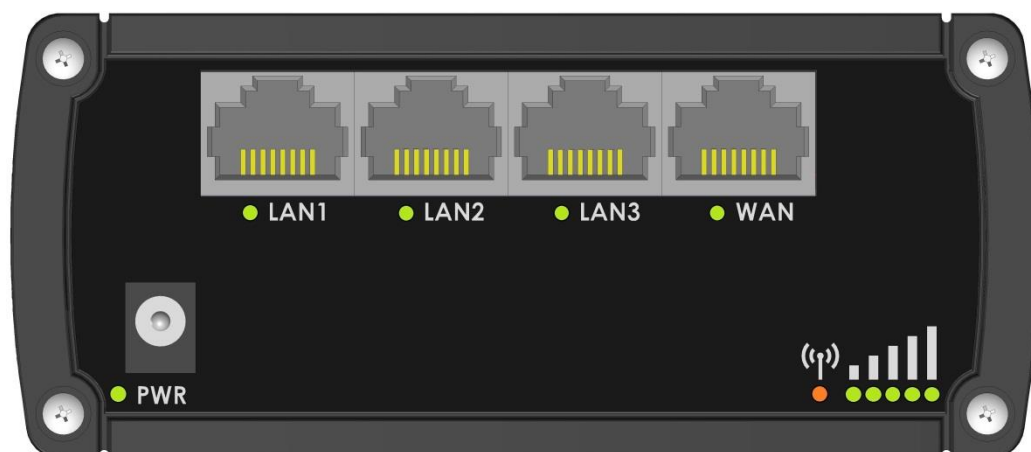
The RUT9xx series router supports various operation modes. It can be connected to the internet (WAN) via mobile, standard Ethernet cable or via a wireless network. When connecting to the internet, you may also backup your main WAN connection with one or two backup connections. Any interface can act like 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.

WAN	Main WAN	Backup WAN	LAN
Mobile	✓	✓	✗
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 RUT9xx router can be powered from power socket or over Ethernet port. Depending on your network architecture you can use LAN 1 port to power the device.



RUT9xx can be powered from power socket and over Ethernet simultaneously. Power socket has higher priority meaning that the device will draw power from power socket as long as it is available.

When RUT9xx is switching from one power source to the other it loses power for a fraction of the second and may reboot. The device will function correctly after the reboot.

Pin	Signal ID	T568A Color	T568B Color	Pins on plug face (socket is reversed)
1	TX+	white/green stripe	white/orange stripe	
2	TX-	green solid	orange solid	
3	RX+	white/orange stripe	white/green stripe	
4		blue solid	blue solid	
5	7 - 30VDC	white/blue stripe	white/blue stripe	
6	RX-	orange solid	green solid	
7	GROUND	white/brown stripe	white/brown stripe	
8	GROUND	brown solid	brown solid	

Though the device can be powered over Ethernet port it is not compliant with IEEE 802.3af-2003 standard. Powering RUT9xx from IEEE 802.3af-2003 power supply **will damage the device** as it is not rated for input voltages of PoE standard.

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 power supply of high quality. Some power supplies can produce voltage peaks significantly higher than the declared output voltage, especially during connecting and disconnecting them.

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 power supply.

6 Status

The status section contains various 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, etc.; and much more.

6.1 Overview

Overview section contains various summary information.

The screenshot displays the Teltonika router's status page. At the top, there is a navigation bar with the Teltonika logo and menu items: Status, Network, Services, System, and Logout. The main content area is titled "Overview" and is divided into several sections:

- System:** Shows a 7.0% CPU load with a progress bar. Other details include Router uptime (0d 2h 21m 28s), Local device time (2015-05-11, 13:56:52), Free memory (87 MB RAM, 0.9 MB FLASH), and Firmware version (RUT9XX_R_00.01.290).
- Mobile:** Shows a signal strength of -79 dBm. Data connection is Disconnected. State is Registered (home); LT BITE GSM; 3G (WCDMA). SIM card slot in use is SIM 1 (Ready). Bytes received/sent are 2.7 KB / 3.1 KB.
- Wireless:** Status is ON. SSID is Teltonika_Router (AP). Mode is 1- AP; 11 CH (2.462 GHz).
- WAN:** Status is Wired. IP address is 192.168.99.110. Backup WAN status is Backup link is disabled.
- Local Network:** IP / netmask is 192.168.1.1/255.255.255.0. Clients connected is 0.
- Access Control:** LAN access is SSH;HTTP;HTTPS; WAN access is HTTP;.
- Recent System Events:**
 - 2015-05-11, 13:52:14 - Port: Wired WAN connection operational
 - 2015-05-11, 13:51:09 - Config: Network configuration has been ...
 - 2015-05-11, 11:56:27 - Config: Access Control configuration ha ...
 - 2015-05-11, 11:56:27 - Config: Firewall configuration has been ...
- Recent Network Events:**
 - 2015-05-11, 13:51:07 - Mobile data disconnected
 - 2015-05-11, 11:36:17 - Mobile data connected, IP: 10.1.12.123 ...
 - 2015-03-18, 16:32:14 - Joined 3G (WCDMA)
 - 2015-03-18, 16:04:26 - Joined 3G (WCDMA)

A footnote at the bottom states: ** Your carrier's data usage accounting may differ. Teltonika is not liable should any accounting discrepancies occur.*

6.2 System Information

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

System Information	
System	
Router name	Teltonika
Host name	Teltonika
Router model	Teltonika RUT9XX
Firmware version	RUT9XX_T_00.00.372
Kernel version	3.10.36
Local device time	2014-11-03, 14:29:09
Uptime	0h 35m 56s (since 2014-11-03, 13:53:13)
Load average	1 min: 10%; 5 mins: 18%; 15 mins: 17%
Temperature	-
Memory	
Free	94556 kB / 126452 kB (74%)
Cached	10828 kB / 126452 kB (8%)
Buffered	4308 kB / 126452 kB (3%)

System explanation:

	Field Name	Sample value	Explanation
1.	Router Name	Teltonika	Name of the router (hostname of the routers system). Can be changed in System -> Administration.
2.	Host name	Teltonika	Indicates how router will be seen by other devices on the network. Can be changed in System -> Administration.
3.	Router Model	Teltonika RUT9xx	Routers model.
4.	Firmware Version	RUT9XX_T_00.00.372	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	3.10.36	The version of the Linux kernel that is currently running on the router.
6.	Local Time	2014-11-03, 14:33:14	Shows the current system time. Might differ from your computer, because the router synchronizes it's time with an NTP server.Format [year-month-day, hours:minutes:seconds].
7.	Uptime	0h 40m 46s (since 2014-11-03, 13:53:13)	Indicates how long it has been since the router booted up. Reboots will reset this timer to 0.Format [day's hours minutes seconds (since year-month-day, hours: minutes: seconds)].
8.	Load Average	1 min: 11%; 5 mins: 18%; 15 mins: 17%	Indicates how busy the router is. Let's examine some sample output: "1 min: 11%, 5 mins: 18%, 15 mins: 17%". The first number mean past minute and second number 11% means that in the past minute there have been, on average, 11% processes running or waiting for a resource.
9.	Temperature		Device's temperature

Memory explanation:

	Field Name	Sample Value	Explanation
1.	Free	94532 kB / 126452 kB (74%)	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	10828 kB / 126452 kB (8%)	The size of the area of memory that is dedicated to storing frequently accessed data.
3.	Buffered	4308 kB / 126452 kB (3%)	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 connection.

The screenshot displays the 'Mobile Information' section of a network management interface. At the top, there are navigation tabs: Mobile (selected), WAN, LAN, Wireless, OpenVPN, VRRP, Topology, and Access. Below the tabs, the 'Mobile Information' title is followed by a status bar indicating 'SIM card slot in use: SIM 1'. The main content area lists various mobile modem parameters in a table-like format:

- Data connection state: Connected
- IMEI: 860461024164561
- IMSI: 246020100070220
- Sim card state: Ready
- Signal strength: -65 dBm
- Cell ID: FD90B
- RSRP: -88 dBm
- RSRQ: -7 dBm
- SINR: -21.4 dBm
- Operator: LT BITE GSM
- Operator state: Registered (home)
- Connection type: 4G (LTE)
- Bytes received *: 3.3 KB (3345 bytes)
- Bytes sent *: 3.4 KB (3487 bytes)

At the bottom of the page, there are two buttons: 'Reset modem' and 'Refresh'.

Mobile information:

	Field Name	Sample Value	Explanation
1.	Data connection state	Connected	Mobile data connection status
2.	IMEI	860461024164561	Modem's IMEI (International Mobile Equipment Identity) number
3.	IMSI	246020100070220	IMSI (International Mobile Subscriber Identity) is used to identify the user in a cellular network
4.	SIM card state	Ready	Indicates the SIM card's state, e.g. PIN required, Not inserted, etc.

5.	Signal strength	-65 dBm	Received Signal Strength Indicator (RSSI). Signal's strength measured in dBm
6.	Cell ID	FD90B	ID of operator cell that device is currently connected to
7.	RSRP	-88dBm	Indicates the Reference Signal Received Power
8.	RSRQ	-7dBm	Indicates the Reference Signal Received Quality
9.	SINR	-21.4dBm	Indicates the Signal to Interference Noise Ratio
10.	Operator state	LT BITE GSM	Operator's name of the connected GSM network
11.	Operator	Registered (home)	GSM network's status
12.	Connection type	4G (LTE)	Indicates the GSM network's access technology
13.	Bytes received	3.3 Kb (3345 bytes)	How many bytes were received via mobile data connection
14.	Bytes sent	3.4 kb (3487 bytes)	How many bytes were sent via mobile data connection

6.3.1.2 WAN

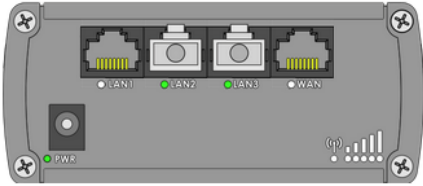
Displays information about WAN connection.

Mobile
WAN
LAN
Wireless
OpenVPN
VRRP
Topology
Access

WAN Information

WAN	
Interface	Wired
Type	Static
IP address	192.168.99.69
WAN MAC	00:1E:42:00:00:01
Netmask	255.255.255.0
Gateway	192.168.99.254
DNS 1	8.8.8.8
Connected	1h 45m 27s

Ports



WAN information:

	Field Name	Sample Value	Explanation
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	Static	Specifies the type of connection. This can either be static or DHCP.
3.	IP address	192.168.99.69	The IP address that the routers uses to connect the internet.
4.	WAN MAC	00:1E:42:00:00:01	MAC (Media Access Control) address used for communication in a 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*	192.168.99.254	Indicates the default gateway, an address where traffic destined for the internet is routed to.
7.	DNS*	8.8.8.8	Domain name server(s).
8.	Connected*	1h 45m 27s	How long the connection has been successfully maintained.

*-These fields show up on other connection modes.

**-Exclusive to other Modes with DHCP.

6.3.1.3 LAN

Displays information about LAN connection.

LAN information:

	Field Name	Sample Value	Explanation
1.	Name	Lan	Lan instance name
2.	IP address	192.168.99.218	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 LAN MAC address	00:1E:42:00:00:00	MAC (Media Access Control) address used for communication in a Ethernet LAN (Local Area Network)
5.	Connected for	1h 53m 56s	How long 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	Explanation
1.	Hostname	?	DHCP client's hostname
2.	IP address	192.168.99.120	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	D4:85:64:65:2B:D4	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	10h 11m 13s	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

Displays information about wireless connection (Station mode).

Mobile	WAN	LAN	Wireless	OpenVPN	VRRP	Topology	Access
Wireless Information							
Wireless Information							
Channel		1 (2.41 GHz)					
Country code		00 (World)					
Wireless Status							
SSID	Mode	Encryption	Wireless MAC	Signal quality	Bit rate		
Teltonika_Router	Station (STA)	no encryption	00:1E:42:10:80:22	61%	43.3 MBit/s		
Teltonika_Router_Test	Access Point (AP)	no encryption	02:1E:42:00:11:03	79%	1.0 MBit/s		
Associated Stations							
MAC Address	Device Name	Signal	RX Rate	TX Rate			
00:1E:42:10:80:22	?	-67 dBm	1.0 Mbit/s, MCS 0, 20MHz	43.3 Mbit/s, MCS 10, 20MHz			
Refresh 							

Client mode information

	Field Name	Sample Value	Explanation
1.	Channel	1 (2.41 GHz)	The channel that the AP, to which the routers is connected to, uses. Your wireless radio is forced to work in this channel in order to maintain the connection.
2.	Country	00	Country code.
3.	SSID	Teltonika_Router	The SSID that the AP, to which the routers is connected to, uses.
4.	Mode	Station (STA)	Connection mode – Client 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	00:1E:42:10:80:22	The MAC address of the access points radio.
7.	Signal Quality	61%	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	43.3 MBit/s	The physical maximum possible throughput that the routers radio can handle. Keep in mind that this value is cumulative - The bitrate will be shared between the router and other possible devices that connect to the local AP.

6.3.1.4.2 Access Point

Displays information about wireless connection (Access Point mode).

Wireless AP information

	Field Name	Sample Value	Explanation
1.	Channel	11 (2.46 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	Teltonika_Router_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 – Master indicates that you router is an access point.
5.	Encryption	No Encryption	The type of encryption that the router will use to authenticate, establish and maintain a connection.
6.	Wireless MAC	00:1E:42:00:00:03	MAC address of your wireless radio.
7.	Signal Quality	80%	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	54.0 MBit/s	The bitrate 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 STAmode or a list of all devices that are connecting to the router in AP mode:

	Field Name	Sample Value	Explanation
1.	MAC Address	FC:C2:DE:91:36:A6	Associated station's MAC (Media Access Control) address
2.	Device Name	Android-9aed2b2077a54c74	DHCP client's hostname
3.	Signal	-54dBm	Received Signal Strength Indicator (RSSI). Signal's strength measured in dBm
4.	RX Rate	24.0Mbit/s, MCS 0, 20MHz	The rate at which packets are received from associated station
5.	TX Rate	54.0Mbit/s, MCS 0, 20MHz	The rate at which packets are sent to associated station

6.3.1.6 OpenVPN Client (must be updated)

Displays openVPN connection client side information.

Field Name	Sample Value	Explanation
Status	Enabled	OpenVPN status
Type	Client	A type of OpenVPN instance that has been created
IP	172.16.1.6	Remote virtual network's IP address
Mask	255.255.255.255	Remote virtual network's subnet mask
Server IP	172.16.1.0	Remote virtual server's IP address
Time	0h 48m 43s	For how long the connection has been established

	Field Name	Sample Value	Explanation
1.	Status	Enabled	OpenVPN status
2.	Type	Client	A type of OpenVPN instance that has been created
3.	IP	172.16.1.6	Remote virtual network's IP address
4.	Mask	255.255.255.255	Remote virtual network's subnet mask
5.	Server IP	172.16.1.0	Remote virtual server's IP address
6.	Time	0h 48m 43s	For how long the connection has been established

6.3.1.7 OpenVPN Server

Displays openVPN connection server side information.

Mobile	WAN	LAN	Wireless	OpenVPN	VRRP	Topology	Access
OpenVPN Information							
Server_Server							
OpenVPN							
Status	Enabled						
Type	Server						
IP	172.16.1.1						
Mask	255.255.255.255						
Time	20h 13m 9s						
Clients Information							
Common Name	Real Address	Virtual Address	Connection Since				
Client1	192.168.99.91:50850	172.16.1.6	2015-05-15 08:07:15				


	Field Name	Sample Value	Explanation
1.	Status	Enabled	OpenVPN status
2.	Type	Server	A type of OpenVPN instance that has been created
3.	IP	172.16.1.1	Remote virtual network's IP address
4.	Mask	255.255.255.255	Remote virtual network's subnet mask
5.	Time	20h 13m 9s	For how long the connection has been established

6.3.1.8 Client information

	Field Name	Sample Value	Explanation
1.	Common Name	Client1	Client connection
2.	Real Address	192.168.99.91:50850	Client's IP address and port number
3.	Virtual Address	172.16.1.6	Virtual address which has been given to a client
4.	Connection Since	2015-05-15 08:07:15	Since when connection has been established

6.3.1.9 VRRP

VRRP (Virtual Router Redundancy Protocol) for LAN

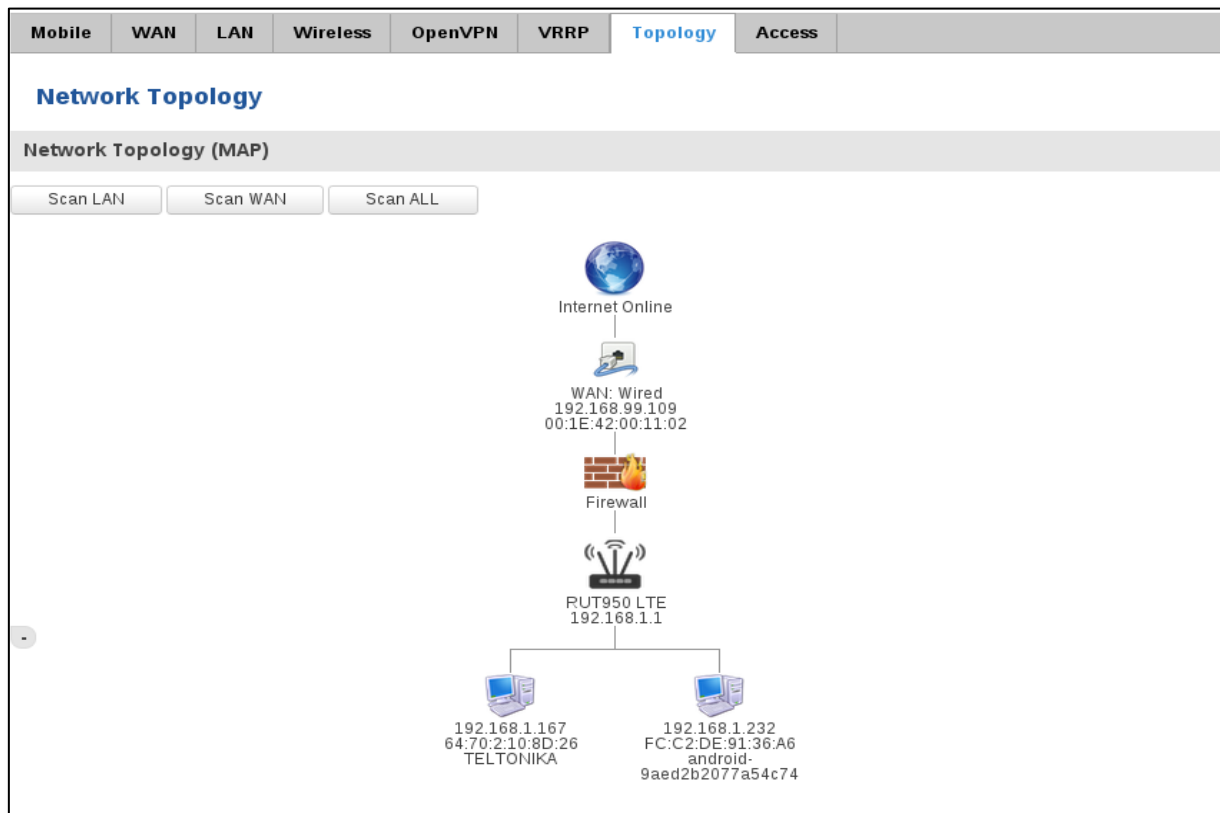
Mobile	WAN	LAN	Wireless	OpenVPN	VRRP	Topology	Access
VRRP Information							
VRRP LAN Status							
Status				Enabled			
Virtual ip				192.168.1.253			
Priority				100			
Router				Master			
<input type="button" value="Refresh"/> 							

	Field Name	Sample Value	Explanation
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 highest priority value on the same VRRP (Virtual Router Redundancy Protocol) cluster will act as a master, range [1 - 255]
4.	Router**	Master	Since when connection has been established

**-Exclusive to other Modes with Slave.


6.3.1.10 Topology

Network scanner allowing you to quickly retrieve information about network devices.



6.3.1.11 Access

Displays information about local and remote active connections status.


Mobile	WAN	LAN	Wireless	OpenVPN	VRRP	Topology	Access
Access Status							
Access information		Last Connections					
Local Access							
Type	Status	Port	Active Connections				
SSH	Enabled	22	0 (0.00 B)				
HTTP	Enabled	80	1 (9.26 KB)				
HTTPS	Enabled	443	0 (0.00 B)				
Remote Access							
Type	Status	Port	Active Connections				
SSH	Disabled	22	0 (0.00 B)				
HTTP	Disabled	80	0 (0.00 B)				
HTTPS	Enabled	443	6 (558.12 KB)				
							Refresh 

	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);1(9.26 KB); 6(558.12 KB)	Count of active connections and amount of data transmitted in KB

**-Exclusive to other Modes with Slave.

6.3.1.11.1 Last Connections

Displays information about local and remote last 3 connections status

Access Status			
Access information		Last Connections	
Last Local Connections			
Type	Date	IP	Authentications Status
SSH	2015-05-11, 10:36:59	192.168.1.167	Succeeded
	2015-05-11, 10:37:54	192.168.1.167	Succeeded
	2015-05-11, 10:38:41	192.168.1.167	Succeeded
HTTP	2015-03-18, 15:56:44	192.168.1.167	Succeeded
	2015-03-18, 16:31:47	192.168.1.167	Succeeded
	2015-05-11, 11:36:23	192.168.1.167	Succeeded
HTTPS	2015-05-07, 09:07:22	192.168.1.167	Succeeded
	2015-05-08, 10:48:52	192.168.1.167	Succeeded
	2015-05-08, 13:39:11	192.168.1.167	Succeeded
Last Remote Connections			
Type	Date	IP	Authentications Status
SSH	2015-05-07, 10:36:01	192.168.99.109	Failed
	2015-05-07, 10:36:13	192.168.99.109	Failed
	2015-05-07, 10:36:16	192.168.99.109	Succeeded
HTTP	2015-05-07, 09:07:17	192.168.99.109	Succeeded
	2015-05-08, 08:44:13	192.168.99.109	Succeeded
	2015-05-08, 09:45:21	192.168.99.109	Succeeded
HTTPS	<i>There are no records yet.</i>		
Refresh 			

	Field Name	Sample Value	Explanation
1.	Type	SSH;HTTP;HTTPS	Type of connection protocol
2.	Date	2015-05-11, 10:36:59	Date and time of connection
3.	IP	192.168.1.167	IP address from which the connection was made
4.	Authentications Status	Failed; Succeeded	Status of authentication attempt

6.4 Device information

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


Device Information	
Device	
Serial number	02345678
Product code	RUT900101010
Batch number	0222
Hardware revision	0321
IMEI	860461024164561
IMSI	246020100070220
Ethernet LAN MAC address	3E:83:6F:84:E1:A4
Ethernet WAN MAC address	AE:F4:F3:5B:9D:CC
Wireless MAC address	N/A
Modem	
Model	ME909u-521
FW version	11.235.07.00.00

	Field Name	Sample Value	Explanation
1.	Serial number	02345678	Serial number of the device
2.	Product code	RUT950 101010	Product code of the device
3.	Batch number	0222	Batch number used during device's manufacturing process
4.	Hardware revision	0321	Hardware revision of the device
5.	IMEI	860461024164561	Identification number of the internal modem
6.	IMSI	246020100070220	Subscriber identification number of the internal modem
6.	Ethernet LAN MAC	3E:83:6F:84:E1:A4	MAC address of the Ethernet LAN ports
7.	Ethernet WAN MAC	AE:F4:F3:5B:9D:CC	MAC address of the Ethernet WAN port
8.	Wireless MAC	N/A	MAC address of the Wi-Fi interface
9.	Model	ME909-521	Router's modem model
10.	FW version	11.235.07.00.00	Router's modem firmware version

6.5 Services

The page displays usage of the available services.

Services			
Services Status			
VRRP LAN	Disabled	DDNS	Disabled
OpenVPN servers	Disabled	Site blocking	Disabled
OpenVPN clients	Disabled	Privoxy	Enabled
SNMP agent	Disabled	SMS utils rules	Enabled
SNMP trap	Disabled	Hotspot	Disabled
NTP client	Enabled	Hotspot logging	Disabled
IPsec	Disabled	GRE tunnel	Disabled
Ping reboot	Disabled	QoS	Disabled

[Refresh](#) 

6.6 Routes

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

6.6.1 ARP

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

ARP		
IP Address	MAC Address	Interface
10.0.207.217	02:50:F3:00:00:00	eth2
192.168.99.17	00:25:22:D7:CA:A7	br-lan
192.168.99.36	38:2C:4A:64:2D:E5	br-lan
192.168.99.155	00:00:00:00:00:00	br-lan

	Field Name	Sample Value	Explanation
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 routers routing table. The routing table indicates where a TCP/IP packet, with a specific IP address, should be directed to.

Active IP Routes			
Network	Target	IP Gateway	Metric
ppp	0.0.0.0/0	10.0.207.217	0
ppp	10.0.207.216/29	0.0.0.0	0
ppp	10.0.207.217	0.0.0.0	0
lan	192.168.99.0/24	0.0.0.0	0

	Field Name	Sample Value	Explanation
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

Displays active IPv6 routes for data packet transmission

Active IPv6-Routes			
Network	Target	IPv6-Gateway	Metric
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF
loopback	0:0:0:0:0:0:0:1	0:0:0:0:0:0:0:0/0	00000000
ppp	FF00:0:0:0:0:0:0:0/8	0:0:0:0:0:0:0:0/0	00000100
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF

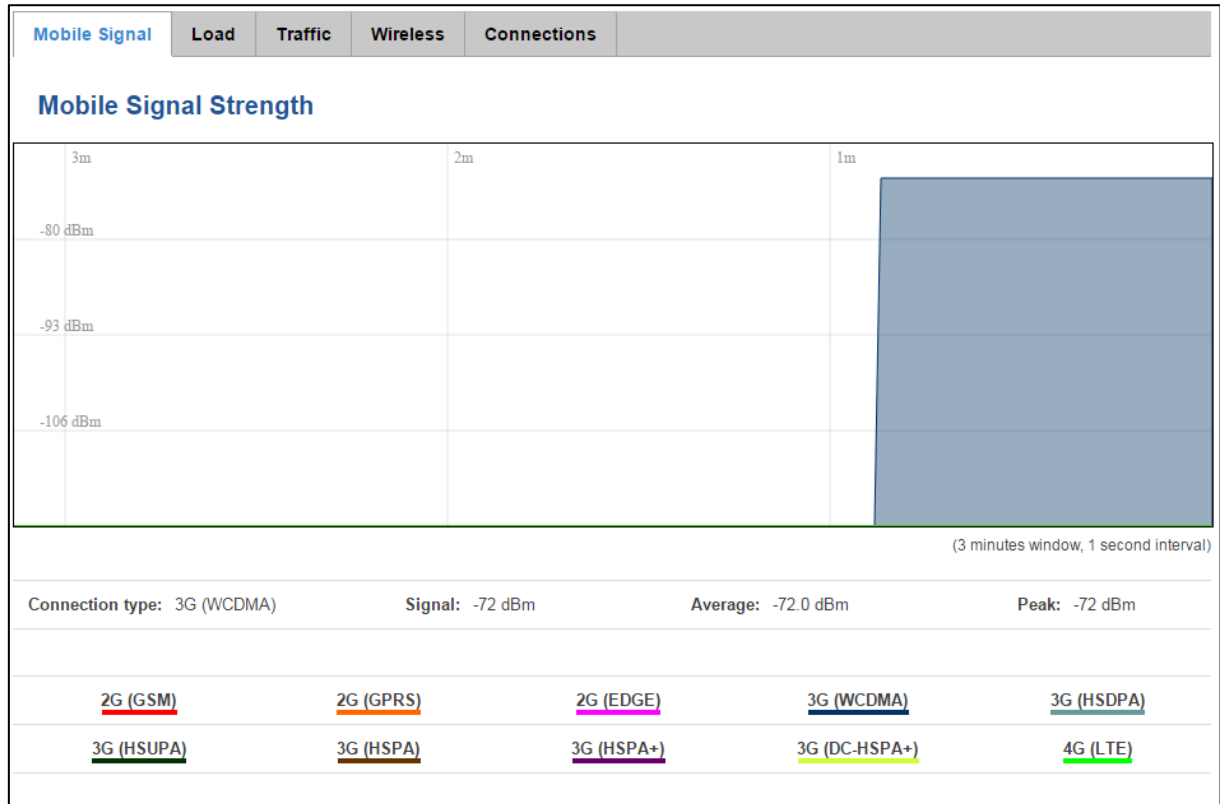
	Field Name	Sample Value	Explanation
1.	Network	loopback	Network interface used
2.	Target	0:0:0:0:0:0:0:0/0	Indicates where a TCP/IP packet, with a specific IP address, should be directed
3.	IPv6-Gateway	0:0:0:0:0:0:0:0/0	Indicates through which gateway a TCP/IP packet should be directed
4.	Metric	FFFFFFFF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

6.7 Realtime Graphs

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

6.7.1 Mobile Signal Strength

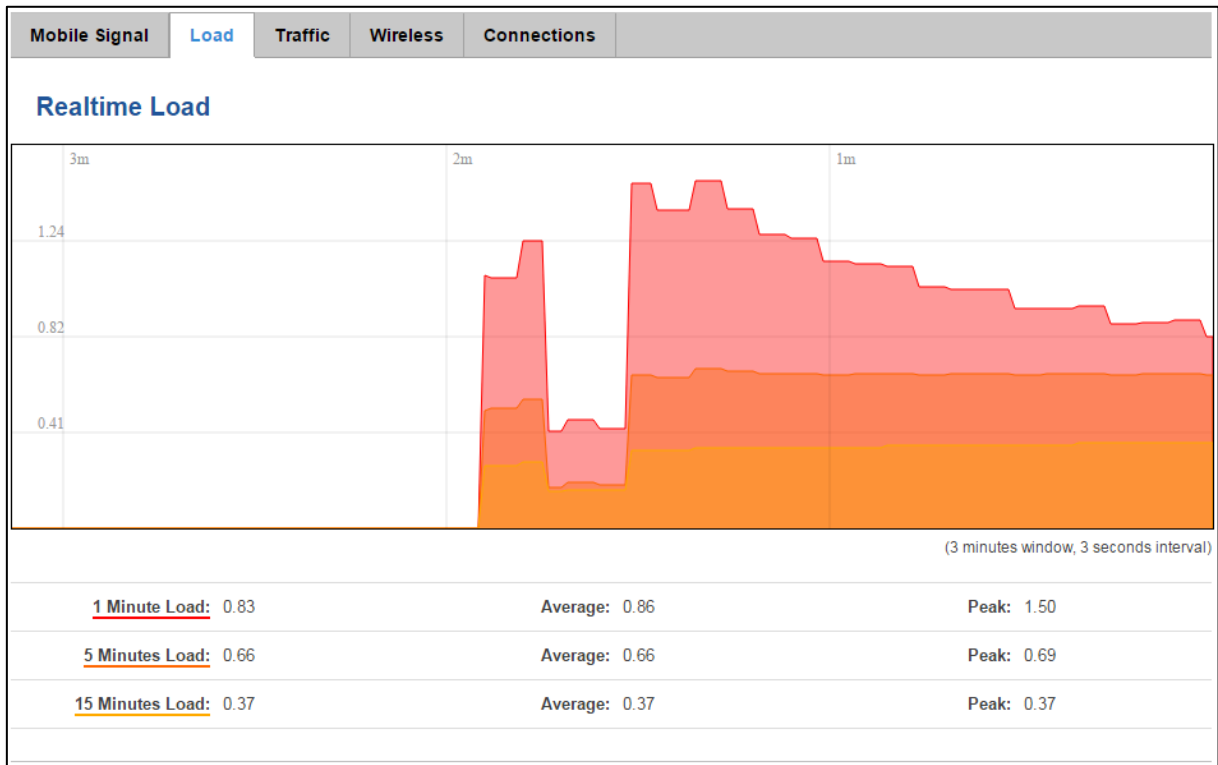
Displays mobile signal strength variation in time (measured in dBm)



	Field Name	Sample Value	Explanation
1.	Connection type	3G (WCDMA)	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

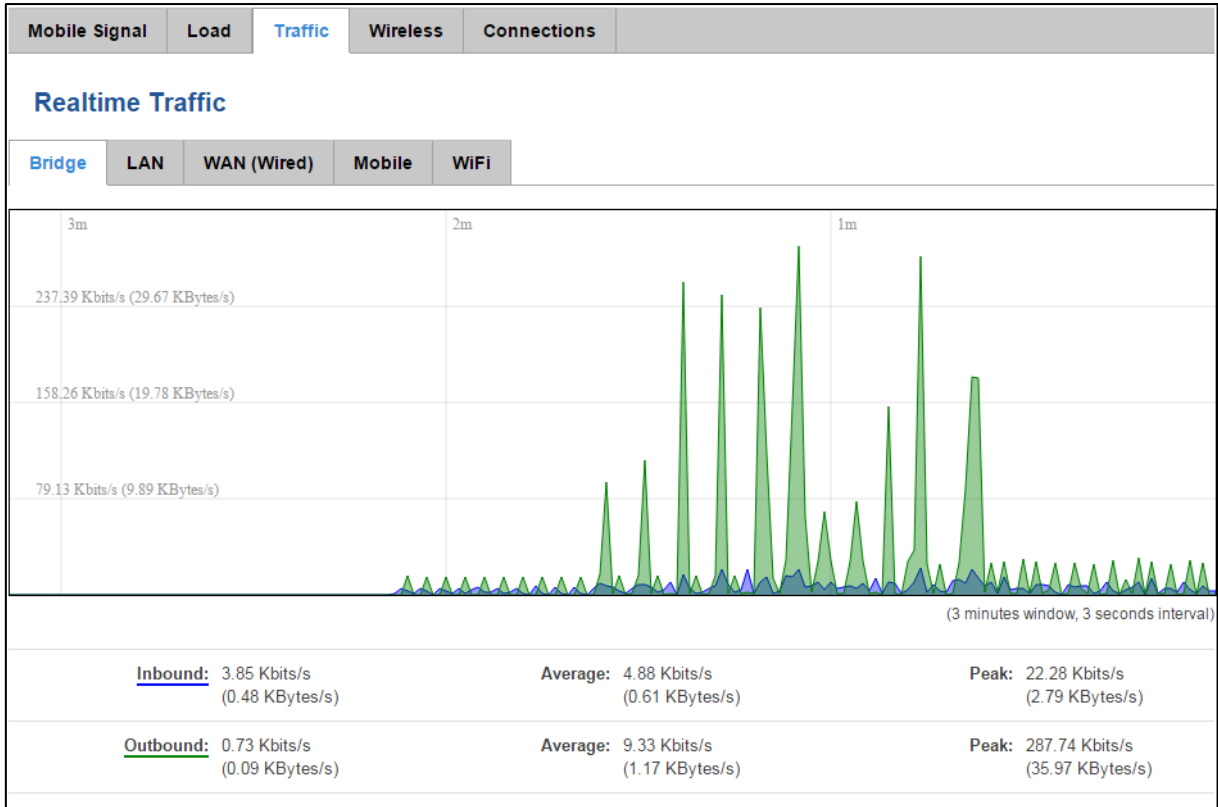
This tri-graph illustrates average CPU load values in real time. The graph consists out of three color coded graphs, each one corresponding to the average CPU load over 1 (red), 5 (orange) and 15 (yellow) most recent minutes.



Field Name	Sample Value	Explanation
1. 1/5/15 Minutes Load	0.83	Time interval for load averaging, color 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 Traffic

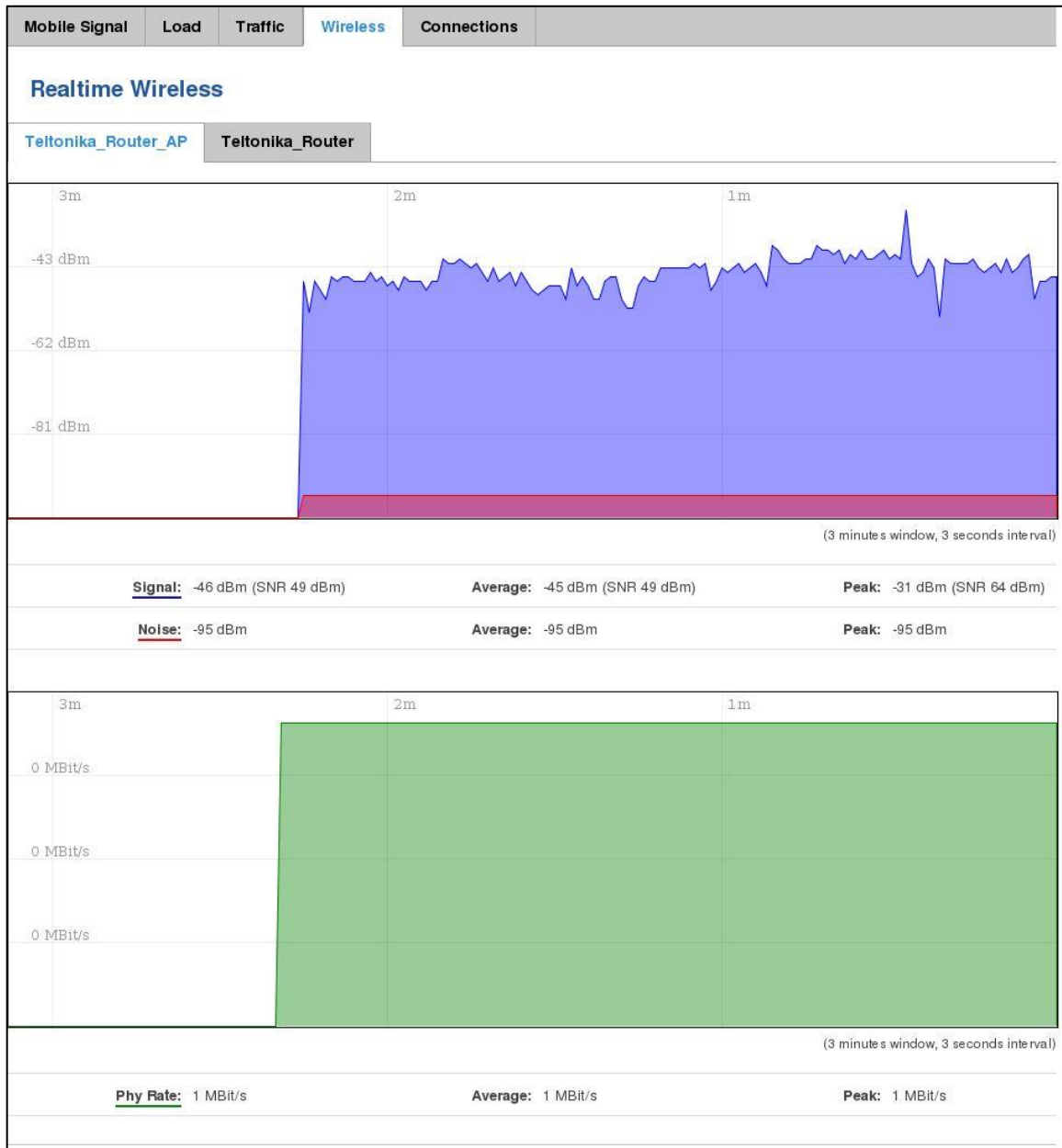
This tri-graph illustrates average system load over the course of ~3 minutes; each new measurement is taken every 3 seconds. The graph consists out of three color coded graphs, each one corresponding to the average system load over 1 (red), 5 (orange) and 15 (yellow) most recent minutes. Although not graphed, the page also displays peak loads over 1, 5 and 15 minutes.



	Field Name	Explanation
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.

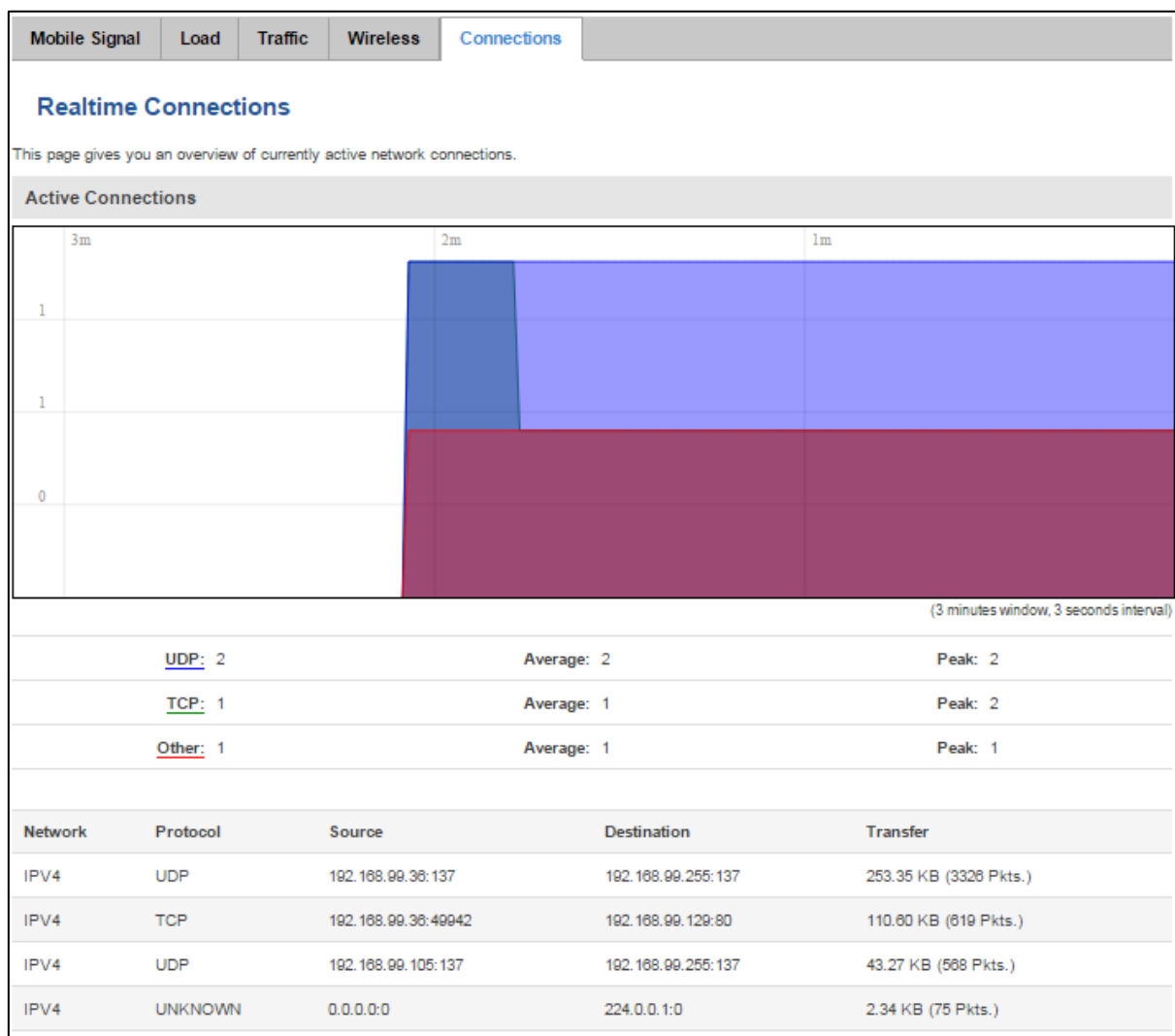
6.7.4 Realtime Wireless

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



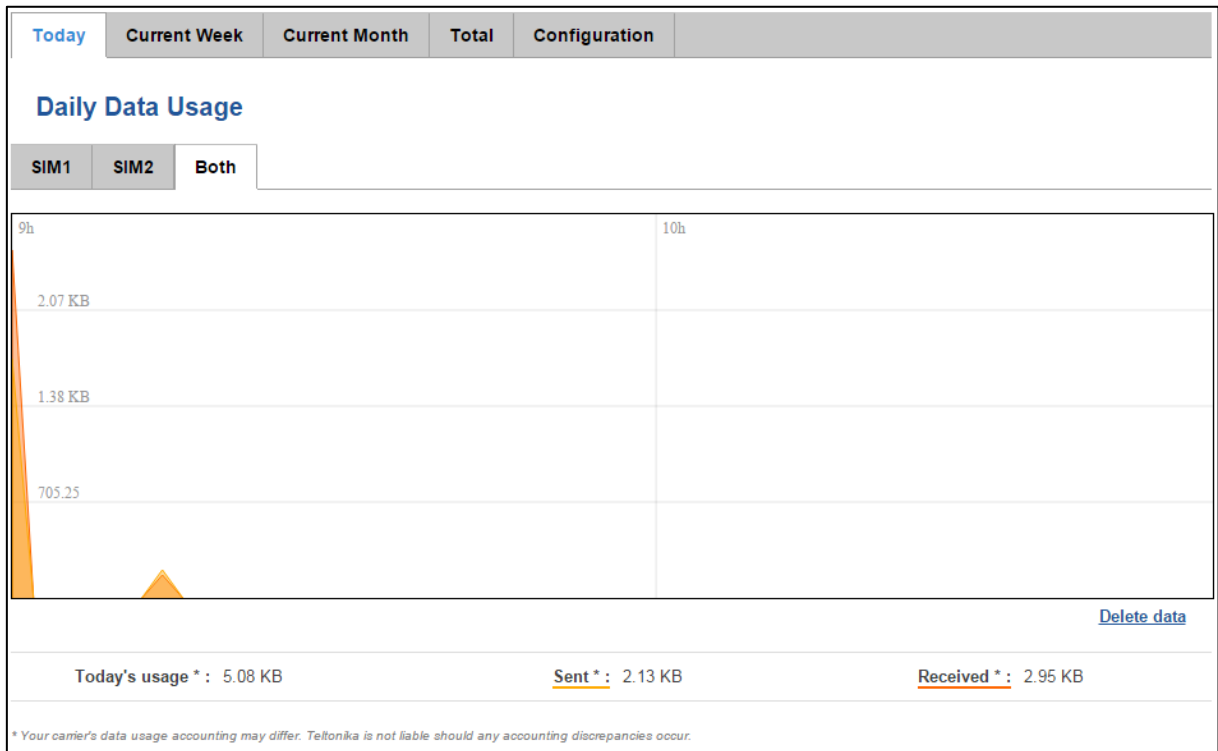
6.7.5 Realtime Connections

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



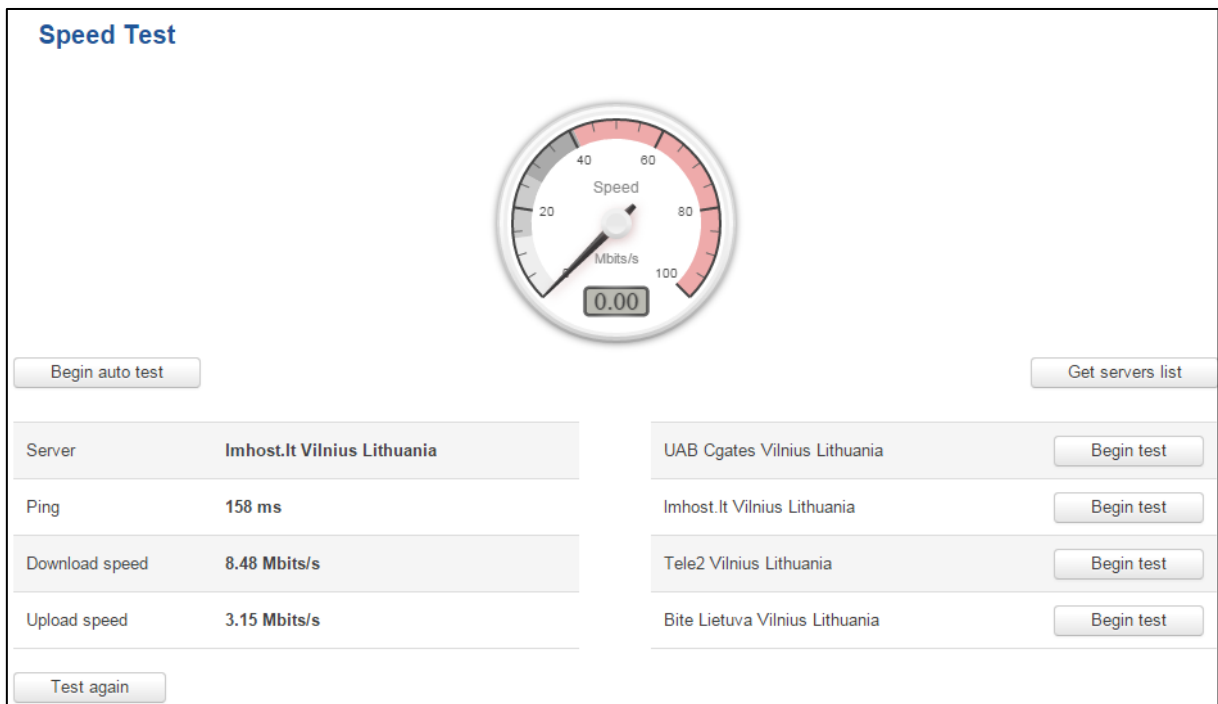
6.8 Mobile Traffic

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



6.9 Speed Test

Speed test is a tool for measuring your internet connection upload and download speeds. You can select servers for manual testing, or use auto test.



6.10 Events Log

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

6.10.1 All Events

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

All Events	System Events	Network Events	Events Reporting	Reporting Configuration
<h3>Events Log</h3>				
Events per page 10		Search <input type="text"/>		
ID	Date	Event type	Event	
3181S	2015-05-11, 16:11:47	Config	Firewall configuration has been changed	
3180S	2015-05-11, 16:09:29	Port	Wired WAN connection operational	
3179S	2015-05-11, 16:05:13	Port	Wired WAN connection non operational	
3178S	2015-05-11, 16:02:39	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi	
3177S	2015-05-11, 16:02:39	Port	Wired WAN connection operational	
3176S	2015-05-11, 16:02:38	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi	
3175S	2015-05-11, 16:02:37	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi	
3174S	2015-05-11, 16:02:36	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi	
3173S	2015-05-11, 16:02:36	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi	
3172S	2015-05-11, 16:02:35	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi	
Showing 1 to 10 of 1912 entries				Next >>

6.10.2 System Events

Displays all system events, their type and time of occurrence. Events include authentication or reboot requests, safemode, incoming and outgoing SMS and calls, configuration changes, DHCP events.

All Events	System Events	Network Events	Events Reporting	Reporting Configuration		
<h3>System Log</h3>						
All	Authentication	Reboot	Safemode	SMS/Call	Configuration	DHCP
Events Log						
Events per page		10				Search <input type="text"/>
ID	Date	Event type	Event			
3181	2015-05-11, 16:11:47	Config	Firewall configuration has been changed			
3180	2015-05-11, 16:09:29	Port	Wired WAN connection operational			
3179	2015-05-11, 16:05:13	Port	Wired WAN connection non operational			
3178	2015-05-11, 16:02:39	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi			
3177	2015-05-11, 16:02:39	Port	Wired WAN connection operational			
3176	2015-05-11, 16:02:38	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi			
3175	2015-05-11, 16:02:37	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi			
3174	2015-05-11, 16:02:36	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi			
3173	2015-05-11, 16:02:36	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi			
3172	2015-05-11, 16:02:35	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi			
Showing 1 to 10 of 1600 entries						Next >>

6.10.3 Network Events

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

All Events **System Events** **Network Events** **Events Reporting** **Reporting Configuration**

Connections Log

All **Wireless** **Mobile Data** **Network Type** **Network Operator**

Events per page Search

ID ↑	Date ↑	Action ↑	Result ↑
312	2015-05-11 15:48:49	WiFi	WiFi client connected: FC:C2:DE:91:36:A6 android-9aed2b2077a54c74
311	2015-05-11 15:48:43	WiFi	WiFi client disconnected: FC:C2:DE:91:36:A6 android-9aed2b2077a54c74
310	2015-05-11 15:48:37	WiFi	WiFi client connected: FC:C2:DE:91:36:A6 android-9aed2b2077a54c74
309	2015-05-11 15:48:31	WiFi	WiFi client disconnected: 20:34:47:41:4B:45
308	2015-05-11 15:36:56	WiFi	WiFi client connected: 20:34:47:41:4B:45
307	2015-05-11 15:36:55	WiFi	WiFi client disconnected: 00:1E:42:10:80:22
306	2015-05-11 15:30:32	WiFi	WiFi client connected: 00:1E:42:10:80:22
305	2015-05-11 15:30:26	WiFi	WiFi client disconnected: 00:1E:42:10:80:22
304	2015-05-11 15:19:58	WiFi	WiFi client connected: 00:1E:42:10:80:22
303	2015-05-11 15:19:52	WiFi	WiFi client disconnected: FC:C2:DE:91:36:A6 android-9aed2b2077a54c74

Showing 1 to 10 of 312 entries [Next >>](#)

6.10.4 Events Reporting

Allows to view, enable, disable or modify created rules for events reporting.

Event type	Event subtype	Action	Enable	Sort
FW upgrade	From file	Send SMS	<input checked="" type="checkbox"/>	↑ ↓ Edit Delete
New DHCP client	Connected from LAN	Send SMS	<input checked="" type="checkbox"/>	↑ ↓ Edit Delete
Config change	All	Send SMS	<input type="checkbox"/>	↑ ↓ Edit Delete

* All rules are executed in current list order.

Events Reporting Configuration

Event type	Event subtype	Action	Add
Config change ▼	All ▼	Send SMS ▼	

6.10.4.1 Events Reporting Configuration

Allows to review created rules details and modify them, so after event occurrence, messages or emails are sent to specified address or phone numbers with information about the event.

Event Reporting Configuration

Modify event reporting rule

Enable

Event type Reboot ▼

Event subtype After unexpected shut down ▼

Action Send SMS ▼

Custom message

Recipient's phone number +123456789 +

	Field Name	Sample Value	Explanation
1.	Enable	Enable/Disable	Make a rule active/inactive
2.	Event type	Reboot	Select event type about which occurrence information will be sent
3.	Event subtype	After unexpected shut down	Specify event subtype to activate the rule
4.	Action	Send SMS	Action to perform when an event occurs
5.	Custom message	Enable/Disable	When action occurs, custom message will be send
6.	Recipient's phone number	+123456789	For whom you want to send a SMS

6.10.5 Reporting Configuration

Displays configured services for event reporting, allows to enable, disable, view and modify the parameters.

All Events
System Events
Network Events
Events Reporting
Reporting Configuration

Events Log Files Report

Create rules for Events Log reporting.

Events Log Report Rules

Events log	Transfer type	Enable	Sort	
System	Email	<input checked="" type="checkbox"/>	↕ ↕	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Network	FTP	<input checked="" type="checkbox"/>	↕ ↕	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

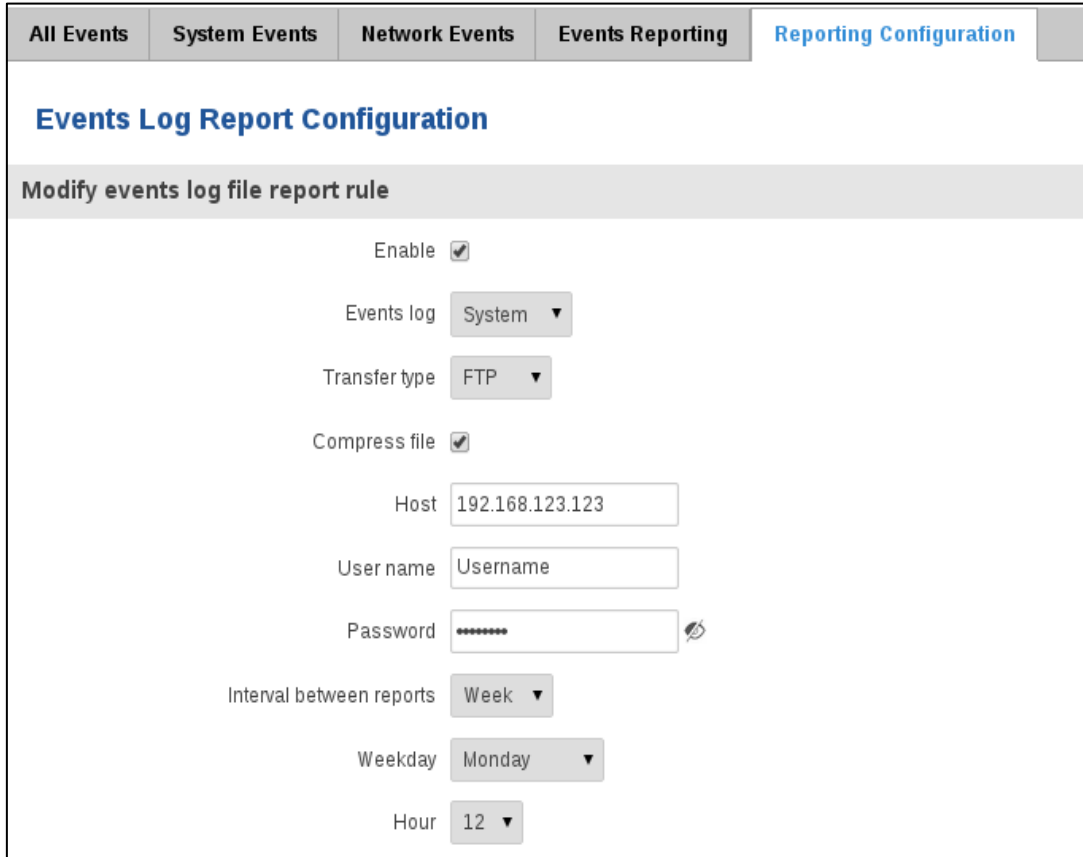
* All rules are executed in current list order.

Events Log Reporting Configuration:

Events log	Transfer type	
System ▼	Email ▼	<input type="button" value="Add"/>

6.10.5.1 Events Log Report Configuration

Allows to change the configuration of periodic events reporting to email or ftp.



	Field Name	Sample Value	Explanation
1.	Enable	Enable/Disable	Make a rule active/inactive
2.	Events log	System	Event type for which the rule is applied
3.	Transfer type	FTP	Event subtype for which the rule is applied: Email/ftp
4.	Compress file	Enable	Action to perform when an event occurs
5.	Host	192.168.123.123	FTP (File transfer Protocol) host name, e.g. ftp.exemple.com , 192.168.123.123. Allowed characters (a-z-A-Z0-9!@#\$\$%^&*+/-=?_`{ }~.)
6.	User name	Username	User name for authentication on SMTP(Simple Mail Transfer Protocol) or FTP (File Transfer Protocol) server. Allowed characters (a-z-A-Z0-9!@#\$\$%^&*+/-=?_`{ }~.)
7.	Password	password	Password for authentication on SMTP(Simple Mail Transfer Protocol) or FTP (File Transfer Protocol) server . Allowed characters (a-z-A-Z0-9!@#\$\$%^&*+/-=?_`{ }~.)
8.	Interval between reports	Week	Send report every select time interval
9.	Weekday	Monday	Day of the week to get events log report
10.	Hour	12	Hour of the day to get events log report

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 3G/LTE network.

Mobile Configuration

Mobile Configuration

SIM 1 **SIM 2**

Connection type

Mode

APN

PIN number

Dialing number

Authentication method

Service mode

Deny data roaming

Use IPv4 only

	Field Name	Sample value	Explanation
1.	Mobile connection	PPP / NDIS	PPP mode uses dialing number to establish data connection. NDIS mode (default) does not use dialing and PPP protocol to establish data connection it is usually faster than PPP mode.
2.	Mode	NAT / Passthrough / Use bridge	NAT mode enables network address translation on router. Bridge mode bridges LTE data connection with LAN. In this mode the router does not have internet connection as ISP provides IP directly to end device (PC, tablet or smartphone). Using Bridge mode will disable most of the router capabilities and you can access your router's settings only by using static IP address on your end device. Passthrough mode is similar with bridge mode except that in passthrough mode router do have internet connection.
3.	APN	"APN"	Access Point Name (APN) is a configurable network identifier used by a mobile device when connecting to a GSM carrier.
4.	PIN number	"1234" or any number that falls between 0000 and 9999	A personal identification number is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system.
5.	Dialing number	*99***1#	Dialing number is used to establish a mobile PPP (Point-to-Point-Protocol) connection.
6.	Authentication	CHAP, PAP or none	Authentication method, which your carrier uses to authenticate new

	method		connections. (This selection is unavailable on the alternate model)
7.	Username	“username”	Your username that you would use to connect to your carriers network. This field becomes available when you select an authentication method (i.e. authentication method is not “none”). These fields are always enabled on the alternate model.
8.	Password	“password”	Your password that you would use to connect to your carriers network. This field becomes available when you select an authentication method (i.e. authentication method is not “none”). These fields are always enabled on the alternate model.
9.	Service mode	2G only, 2G preferred, 3G only, 3G preferred, 4G (LTE) only, 4G (LTE) preferred or automatic.	Your network preference. If your local mobile network supports 2G, 3G and 4G (LTE) you can specify to which network you wish to connect. E.g.: if you choose 2G, the router will connect to a 2G network, so long as it is available, otherwise it will connect to a network that provides better connectivity. If you select auto, then the router will connect to the network that provides better connectivity.
10.	Deny data roaming	Enable/Disable	If enabled this function prevents the device from establishing mobile data connection while not in home network.
11.	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.

7.1.1.2 Mobile Data On Demand

Mobile Data On Demand

Enable

No data timeout (sec)

	Field name	Possible values	Explanation
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)	1-99999999	A mobile data connection will be terminated if no data is transferred during the timeout period

7.1.1.3 Force LTE network

Force LTE network

Enable

Interval (sec)

	Field name	Possible values	Explanation
1.	Enable	Enable/Disable	Force LTE network function periodically disables mobile data connection (for a few seconds) to allow the device to switch to LTE

			network. This could because some operators do not support switching from 3G to LTE networks while data is being transferred.
2.	Interval (sec)	180 - 3600	Interval in seconds the device will use to periodically disable mobile data connection.

7.1.2 SIM Management

	Field name	Possible values	Explanation
1.	Primary SIM card	SIM 1 / SIM 2	SIM card that will be used in the system as a primary SIM card
2.	Enable automatic switching	Enable/Disable	Automatically switch between primary and secondary SIM cards based on the various rules and criterions defined below
3.	Check interval	20-3600	Check interval in seconds
4.	On weak signal	Enable/Disable	Perform a SIM card switch when a signal's strength drops below a certain threshold
5.	On data limit	Enable/Disable	Perform a SIM card switch when mobile data limit for your current SIM card is exceeded
6.	On sms limit	Enable/Disable	Perform a SIM card switch when sms limit for your current SIM card is exceeded
7.	On roaming	Enable/Disable	Perform a SIM card switch when roaming is detected
8.	On data connection fail	Enable/Disable	Perform a SIM card switch when data connection fails
9.	Switch back to primary SIM card after timeout	Enable/Disable	Switch back to primary SIM card after timeout has been reached

7.1.3 Network Operators

This function lets you Scan, Select and enter manual Network Operator to which router should connect. Function will provide great utility when router is in Roaming conditions. Operator is selected only for the active SIM card. In order to specify operator for the other SIM card it must first be selected as primary SIM in “SIM Management”.

Network Operators

Current SIM

SIM card in use	SIM 1
Current operator	TELE2

Scan For Network Operators

Status	Operator name	Short name	Numeric name	Network access type	Connect
Available	Tele2 LT	Tele2 LT	24603	3G/2G	<input type="button" value="Connect"/>
Forbidden	LT BITE GSM	BITE	24602	3G/2G	<input type="button" value="Connect"/>
Available	OMNITEL LT	OMT	24601	2G/3G/4G	<input type="button" value="Connect"/>

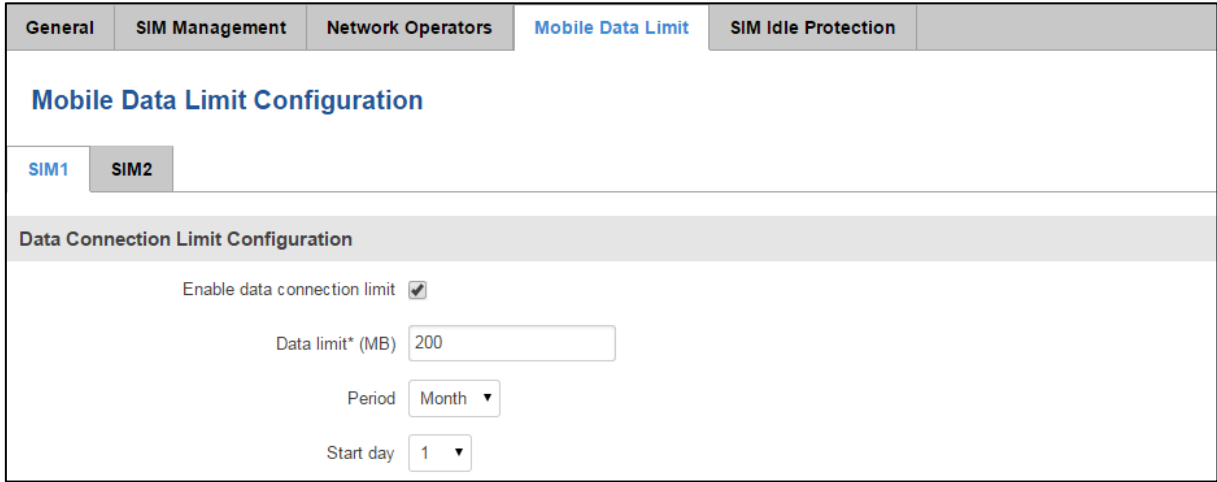
	Field Name	Sample Value	Explanation
1.	SIM card in use	SIM 1 / SIM 2	Shows current SIM card's in use
2.	Current operator	„TELE2“	Operator's name of the connected GSM network

Note: **after clicking Scan button- You will lose current mobile connection!**For changing network operator status have to be available. There is manual connection to network operator, you have to fill numeric name, and it's have to be available.

7.1.4 Mobile Data Limit


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

7.1.4.1 Data Connection Limit Configuration



	Field Name	Sample value	Explanation
1.	Enable data connection limit	Enable/Disable	Disables mobile data when a limit for current period is reached
2.	Data limit (MB)	200	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

7.1.4.2 SMS Warning Configuration



	Field Name	Sample value	Explanation
1.	Enable SMS warning	Enable/Disable	Enables sending of warning SMS message when mobile data limit for current period is reached
2.	Data limit (MB)	200	Send warning SMS message 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		A starting time for mobile data limiting period
5.	Phone number	+37012345678	A phone number to send warning SMS message to, e.g. +37012345678

7.1.5 Sim Idle protection

Some operators block user SIM cards after period of inactivity. This function enables router to periodically switch to secondary SIM card and establish data connection with mobile network in order to prevent sim card blocking.

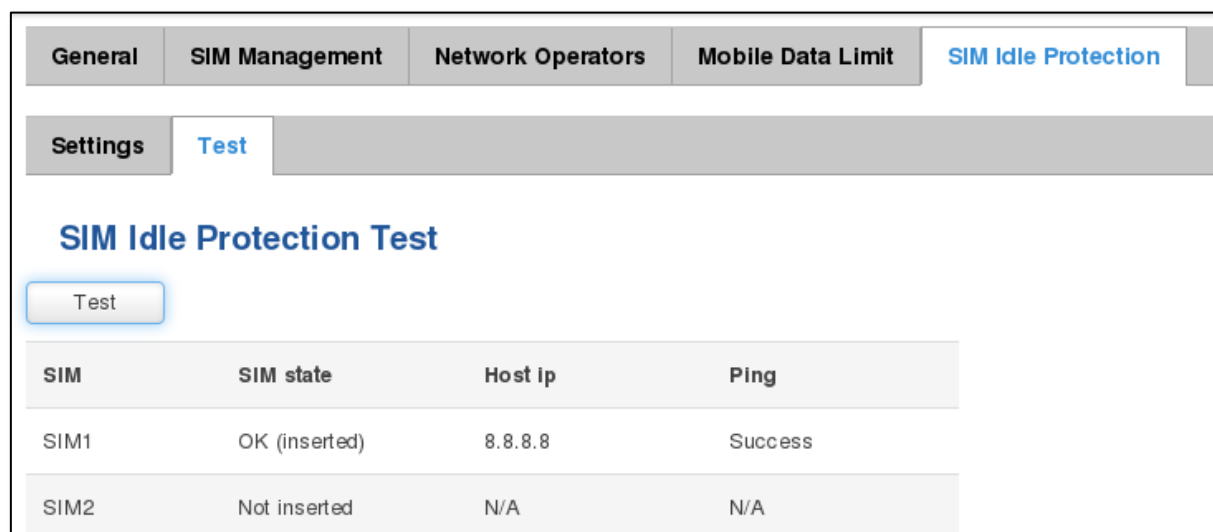
7.1.5.1 Settings

The screenshot shows a web interface for configuring SIM Idle Protection. At the top, there are tabs for 'General', 'SIM Management', 'Network Operators', 'Mobile Data Limit', and 'SIM Idle Protection'. Below these are sub-tabs for 'Settings' and 'Test'. The main heading is 'SIM Idle Protection Configuration'. There are two tabs for 'SIM1' and 'SIM2'. The configuration fields are: 'Enable' (checkbox), 'Period' (dropdown menu set to 'Week'), 'Day' (dropdown menu set to 'Monday'), 'Hour' (dropdown menu set to '1'), 'Minute' (dropdown menu set to '0'), 'Host to ping' (text input field with '8.8.8.8'), 'Ping package size' (text input field with '56'), and 'Ping requests' (text input field with '2').

	Field Name	Sample value	Explanation
1.	Enable	Enable/Disable	Enables SIM idle protection
2.	Period	Month / Week	Switches between monthly and weekly sim activation periods
3.	Day	1-31 / Monday - Sunday	Specifies the day for SIM idle protection activation, 1-31 if Period is Month, and Monday – Sunday if period is week.
4.	Hour	1-24	Specifies the hour for SIM idle protection activation
5.	Minute	1-60	Specifies the minute for SIM idle protection activation
6.	Host to ping	8.8.8.8	Specifies IP address or domain name to send data packages to
7.	Ping package size	56	Specifies ping Package size in bytes
8.	Ping requests	2	Specifies requests to be sent

7.1.5.2 Test

Tests the functioning of idle protection with your parameters entered at settings tab.

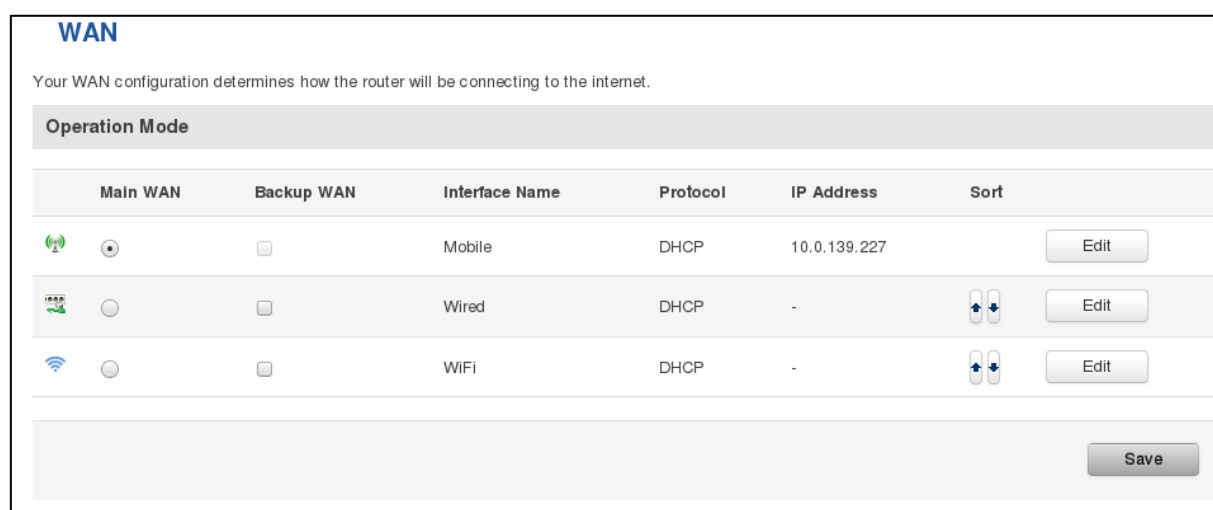


SIM	SIM state	Host ip	Ping
SIM1	OK (inserted)	8.8.8.8	Success
SIM2	Not inserted	N/A	N/A

	Field Name	Sample value	Explanation
1.	SIM	SIM1 / SIM2	Displays SIM number
2.	SIM state	OK (inserted)	Displays status of the SIM card
3.	Host IP	1-31 / Monday - Sunday	Displays the IP of the Host
4.	Ping	Success	Displays status of ping attempt

7.2 WAN

7.2.1 Operation Mode



Main WAN	Backup WAN	Interface Name	Protocol	IP Address	Sort
<input checked="" type="radio"/>	<input type="checkbox"/>	Mobile	DHCP	10.0.139.227	<input type="button" value="Edit"/>
<input type="radio"/>	<input type="checkbox"/>	Wired	DHCP	-	<input type="button" value="Edit"/>
<input type="radio"/>	<input type="checkbox"/>	WiFi	DHCP	-	<input type="button" value="Edit"/>

	Type	Explanation
1.	Main WAN	Switches between Mobile, Wired and WiFi interface for main WAN
2.	Backup WAN	Let's user to select one or two interfaces for WAN backup
3.	Interface Name	Displays Wan interface name, and changes interface priority, the interface at the table top has the highest priority
4.	Protocol	Displays protocol used by Wan interface

5.	IP Address	Displays IP address acquired by specific interface
6.	Sort	Sorts table rows and changes interface priority, the highest interface has highest priority

7.2.2 Common configuration

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

The screenshot shows the 'Common Configuration' window with the 'General Setup' tab selected. The 'Protocol' dropdown menu is set to 'DHCP'. Below it, there is a 'Really switch protocol?' label and a 'Switch protocol' button.

You can switch between the 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' dropdown menu is set to 'Static'. The following fields are visible:

- 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 (with a red 'x' icon)
- 8.8.6.6 (with a red 'x' icon and a green '+' icon)

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

	Filed name	Sample	Explanation
1.	IPv4 address	192.168.99.162	Your routers 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 (autogenerated if not set). It is best to leave this blank unless you know what you are doing.
5.	custom DNS servers	8.8.8.8 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:

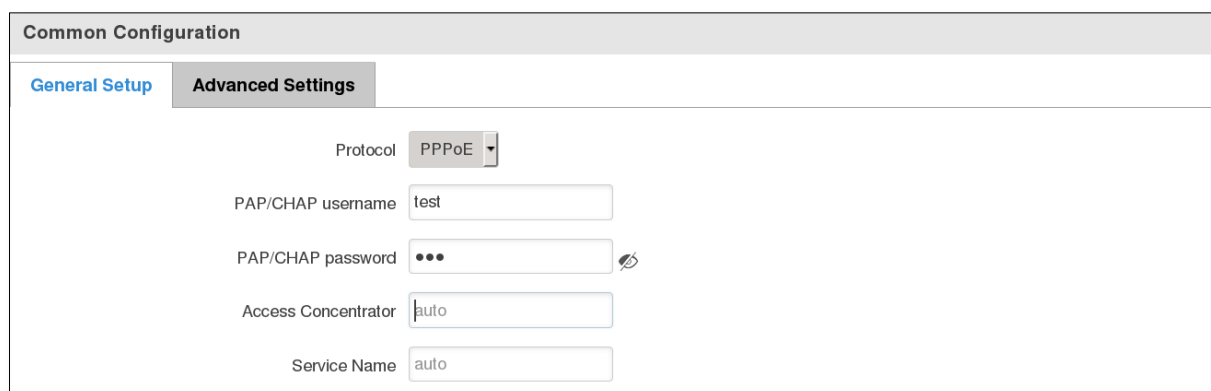


The screenshot shows a configuration interface with two tabs: "General Setup" and "Advanced Settings". The "Advanced Settings" tab is active. It features a "Protocol" dropdown menu set to "DHCP". Below it is a text input field for "Hostname to send when requesting DHCP" containing the value "Teltonika". A section titled "IP Aliases" follows, with a sub-header "IP aliases are a way of defining or reaching a subnet that works in the same space as the regular network". Below this is a message "There are no IP aliases created yet" and an "Add" button. At the bottom right, there is a "Save" button.

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 a configuration interface with two tabs: "General Setup" and "Advanced Settings". The "Advanced Settings" tab is active. It features a "Protocol" dropdown menu set to "PPPoE". Below it are four text input fields: "PAP/CHAP username" with the value "test", "PAP/CHAP password" with masked characters "•••" and a visibility icon, "Access Concentrator" with the value "auto", and "Service Name" with the value "auto".

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

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

Common Configuration

General Setup **Advanced Settings**

Disable NAT

Override MAC address

Override MTU

Use gateway metric

	Field name	Sample value	Explanation
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 computers MAC address (i.e. that IP will only work with your computer). In this field you can enter your computers MAC address and fool the gateway in thinking that it is communicating with your computer.
3.	Override MTU	1500	Maximum transmission unit – 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

Common Configuration

General Setup **Advanced Settings**

Disable NAT

Use broadcast flag

Use default gateway

Use DNS servers advertised by peer

Use gateway metric

Client ID to send when requesting DHCP

Vendor Class to send when requesting DHCP

Override MAC address

Override MTU

	Field name	Sample value	Explanation
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 With this field you can alter the metric of that entry
6.	Client ID to send when requesting DHCP		
7.	Vendor Class to send when requesting DHCP		
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 computers MAC address (i.e. that IP will only work with your computer). In this field you can enter your computers 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

	Field name	Sample value	Explanation
1.	Disable NAT	Enable/Disable	If checked, 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	
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

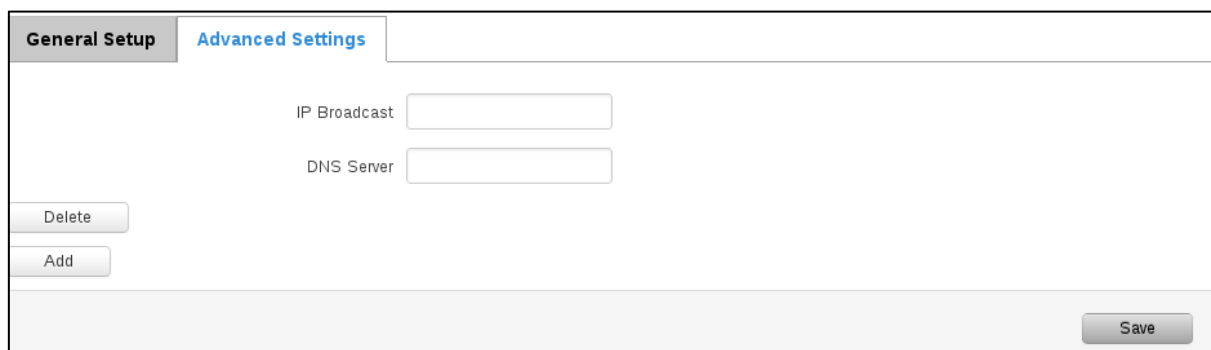
IP aliases are a way of defining or reaching a subnet that works in the same space as the regular network.



The screenshot shows the 'Advanced Settings' tab for an IP alias configuration. It includes the following fields and controls:

- IP Address:** 192.168.99.161
- Netmask:** 255.255.255.0 (dropdown menu)
- Gateway:** 192.168.99.254
- Buttons:** 'Delete', 'Add', and 'Save'.

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 subnets 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.



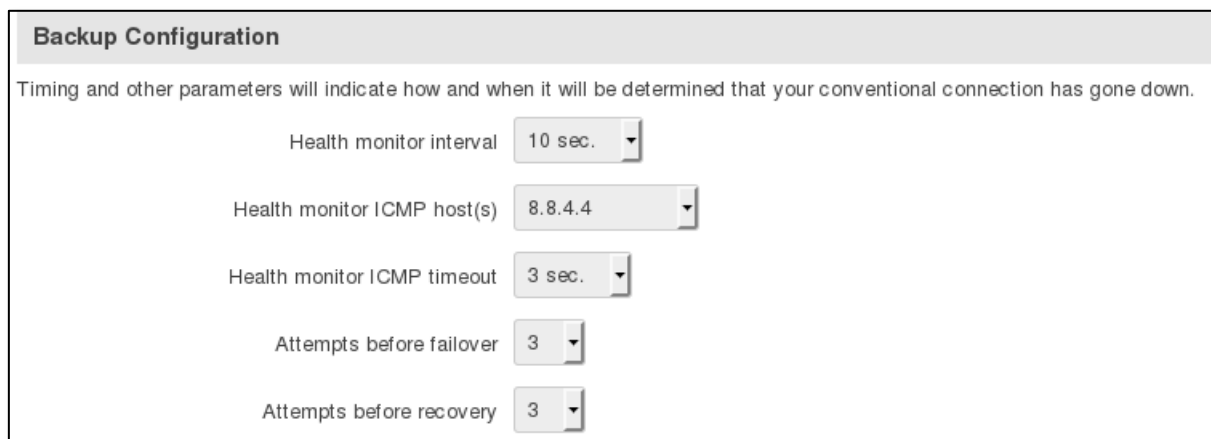
The screenshot shows the 'Advanced Settings' tab for an IP alias configuration. It includes the following fields and controls:

- IP Broadcast:** (empty text field)
- DNS Server:** (empty text field)
- Buttons:** 'Delete', 'Add', and 'Save'.

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

7.2.2.2.5 Backup WAN configuration

Backup WAN is 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 primary connection fails, router tries to use backup with higher priority and if that is unavailable or fails too, then router tries the backup with lower priority.



The screenshot shows the 'Backup Configuration' interface with the following settings:

- Health monitor interval:** 10 sec.
- Health monitor ICMP host(s):** 8.8.4.4
- Health monitor ICMP timeout:** 3 sec.
- Attempts before failover:** 3
- Attempts before recovery:** 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 connections 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.

	Field Name	Sample value	Explanation
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	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 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 checks should fail for your WAN connection to be declared DOWN for good.
5.	Attempts before recovery	1/3/5/10/15/20	How many checks should pass for your WAN connection to be 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 the 'Configuration' page 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.

	Field name	Sample value	Explanation
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	0	IP broadcasts are used by BOOTP and DHCP clients to find and send requests to their respective servers

7.3.1.2 Advanced settings

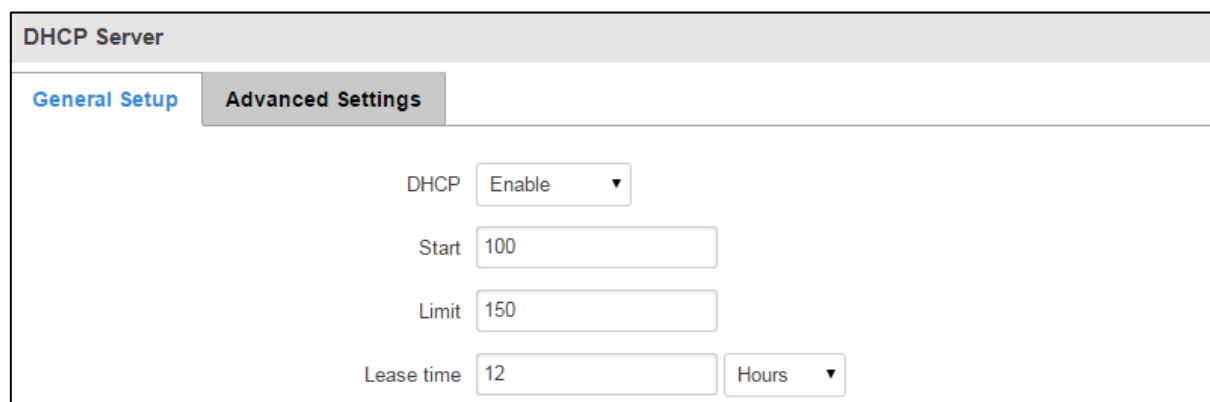
The screenshot shows the 'Configuration' page with two tabs: 'General Setup' and 'Advanced Settings' (selected). Under 'Advanced Settings', there are four configuration options: 'Accept router advertisements' with an unchecked checkbox, 'Override MTU' with a text input field containing '1500', 'Use gateway metric' with a text input field containing '0', and 'Use WAN port as LAN' with an unchecked checkbox.

	Field name	Sample value	Explanation
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	With this field you can alter the metric of that entry
4.	Use WAN port as LAN	Enable/Disable	

7.3.2 DHCP Server

The DHCP server is the router 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 address and the device will be able to fully communicate with the router.

7.3.2.1 General Setup



The screenshot shows the 'DHCP Server' configuration page with the 'General Setup' tab selected. The 'Advanced Settings' tab is also visible. The configuration includes:

- DHCP: Enable (dropdown menu)
- Start: 100 (text input)
- Limit: 150 (text input)
- Lease time: 12 (text input) and Hours (dropdown menu)

	Field Name	Sample value	Explanation
1.	DHCP	Enable/Disable	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 + 150 – 1 = 254).
4.	Lease time	12	How long can a leased IP 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 for a new one. Select Hour or Minute (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.

	Field Name	Sample Value	Explanation
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 <i>DHCP server</i> . 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.

7.4 VLAN

On this page you can configure your virtual LAN settings, either Port based or Tag based.

7.4.1 VLAN Networks

7.4.1.1 VLAN Functionality

	Field Name	Sample Value	Explanation
1.	VLAN mode	Disabled / Port based / Tag based	Lets user to choose the VLAN mode or disable VLAN functionality.

7.4.1.2 VLAN Network List

If VLAN mode – Port based:

VLAN Networks List					
VLAN ID	LAN ports			Wireless access points	LAN
	1	2	3	Teltonika_Router	
1	On	On	On	<input type="checkbox"/>	None <input type="button" value="Delete"/>

	Field Name	Sample Value	Explanation
1.	VLAN ID	1	VLAN Identification number, allowed in range (1-4094)
2.	LAN ports 1 / 2 / 3	on	Switches each LAN port between ON, OFF or tagged state.
3.	Wireless access points	Enabled / Disabled	Assign selected access point(s) to selected LAN.
4.	LAN		Select to which LAN to assign selected LAN ports and wireless access points.

If VLAN mode – Taged based:

VLAN Networks List		
VLAN ID	Wireless access points	LAN
	Teltonika_Router	
2	<input type="checkbox"/>	None <input type="button" value="Delete"/>

	Field Name	Sample Value	Explanation
1.	VLAN ID	1	VLAN Identification number, allowed in range (1-4094)
3.	Wireless access points	Enabled / Disabled	Assign selected access point(s) to selected LAN.
4.	LAN		Select to which LAN to wireless access point(s).

7.4.2 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 – [6.3 LAN](#).

The screenshot shows a web interface titled "LAN". Below the title is a section "LAN Networks List" which contains a table with two columns: "LAN name" and "Interface name". The table has one row with "Lan" in the first column and "eth0 tap0" in the second. To the right of this row is an "Edit" button. Below the table is a form with a label "LAN name:" followed by a text input field containing "LAN2" and an "Add New" button.

	Field Name	Sample Value	Explanation
1.	LAN name	LAN2	Specifies new LAN name

7.5 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 some local access point.

Access Point:

The screenshot shows a web interface for "Wireless Access Point" configuration. It has two main sections: "Device Configuration" and "Interface Configuration".

Device Configuration: This section has two tabs: "General Setup" and "Advanced Settings". Under "Advanced Settings", there is a checkbox for "Enable wireless" which is checked, and a dropdown menu for "Channel" set to "auto".

Interface Configuration: This section has four tabs: "General Setup", "Wireless Security", "MAC Filter", and "Advanced Settings". Under "Advanced Settings", there is a text input field for "SSID" containing "Teltonika_Router" and a checkbox for "Hide SSID" which is unchecked.

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 other – software.

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

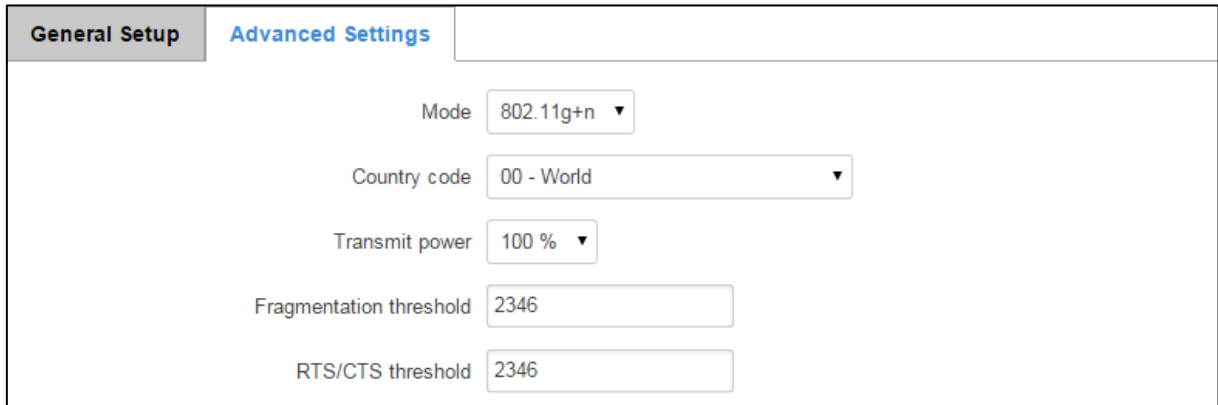
Important note: As seen in the picture you should always **Save** before toggling the radio on and off.

ESSID – Your wireless networks 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 ESSID – Will render your SSID hidden from other devices that try to scan the area.

7.5.1.1 Device

7.5.1.1.1 Advanced Settings



The screenshot shows a configuration window with two tabs: 'General Setup' and 'Advanced Settings'. The 'Advanced Settings' tab is active. It contains the following settings:

- Mode: 802.11g+n
- Country code: 00 - World
- Transmit power: 100 %
- Fragmentation threshold: 2346
- RTS/CTS threshold: 2346

Here you can configure more advanced parameters:

	Field name	Sample value	Explanation
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 its internal parameters to meet your countries wireless regulations.
3.	Transmit power	20%/40%/60%/80%/100%	Select WiFi signal power
4.	Frag. 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 arising when several access points are in the same area, contending.

7.5.1.2 Interface

7.5.1.2.1 Security

Encryption – There are many modes of encryption, a distinctive classis pointed out below.

The screenshot shows the 'Interface Configuration' window with the 'Wireless Security' tab selected. The 'Encryption' dropdown is set to 'WPA-PSK/WPA2-PSK mixed mode'. The 'Cipher' dropdown is set to 'Auto'. The 'Key' field contains a series of dots and has an eye icon to its right.

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 passphrase, which must be at least 8 characters long.

7.5.1.2.2 MAC-Filter

The screenshot shows the 'Interface Configuration' window with the 'MAC Filter' tab selected. The 'MAC address filter' dropdown is set to 'Allow listed only'. The 'MAC list' field contains the address '00:11:22:33:44:55' and has a plus icon to its right.

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 only the listed ones.

7.5.1.2.3 Advanced settings

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

The screenshot shows the 'Interface Configuration' window with the 'Advanced Settings' tab selected. The 'Separate clients' checkbox is currently unchecked.

7.5.1.3 Client

RUT9xx can work as a Wi-Fi client (check **6.5 Chapter** of this manual). 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.

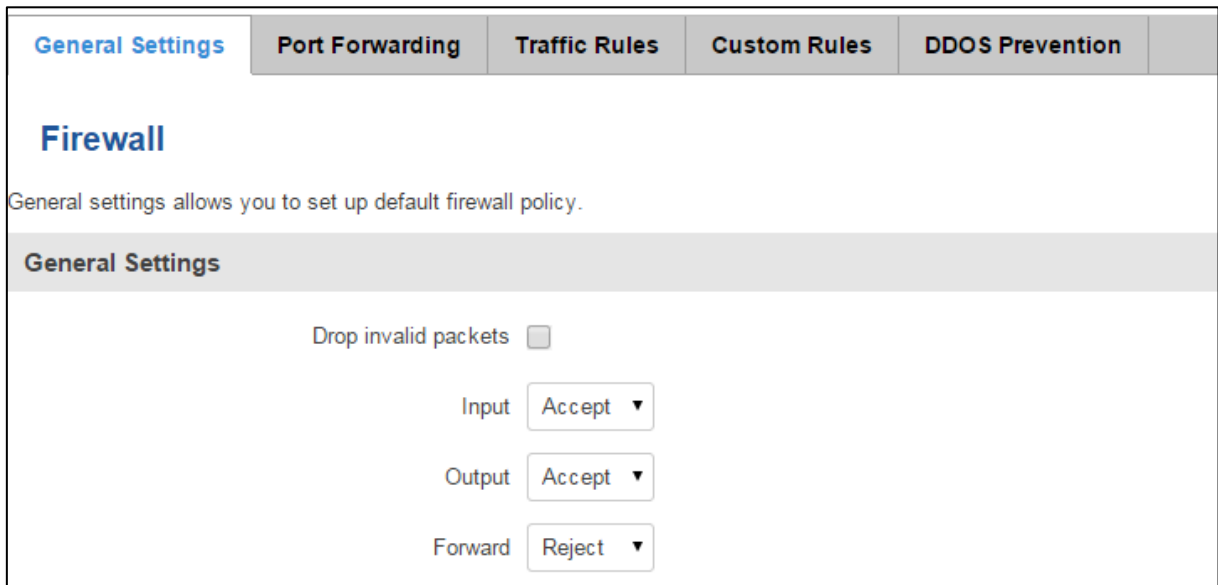
In addition to standard options you can also click the **Scan** button to rescan the surrounding area and attempt to connect to a new wireless access point.

7.6 Firewall

In this section we will look over the various firewall features that come with RUT950.

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.



	Field Name	Sample value	Explanation
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.

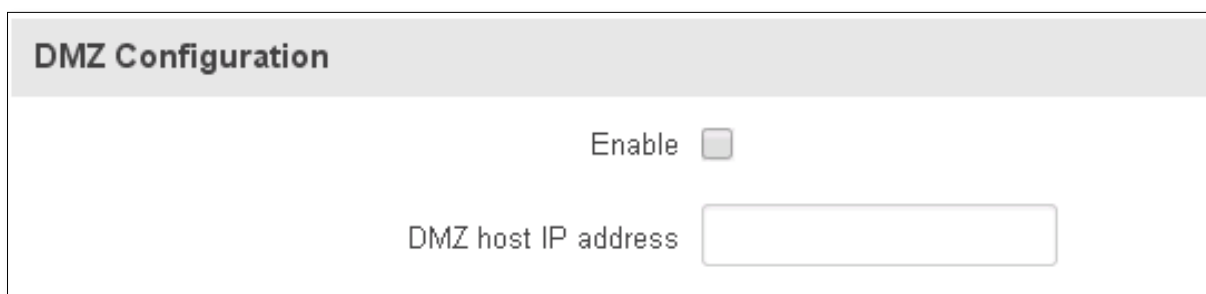
*DEFAULT: When a packet goes through a firewall chain it is matched against all the rules for that specific chain. If no rule matches said packet, an according Action (either Drop or Reject or Accept) is performed.

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

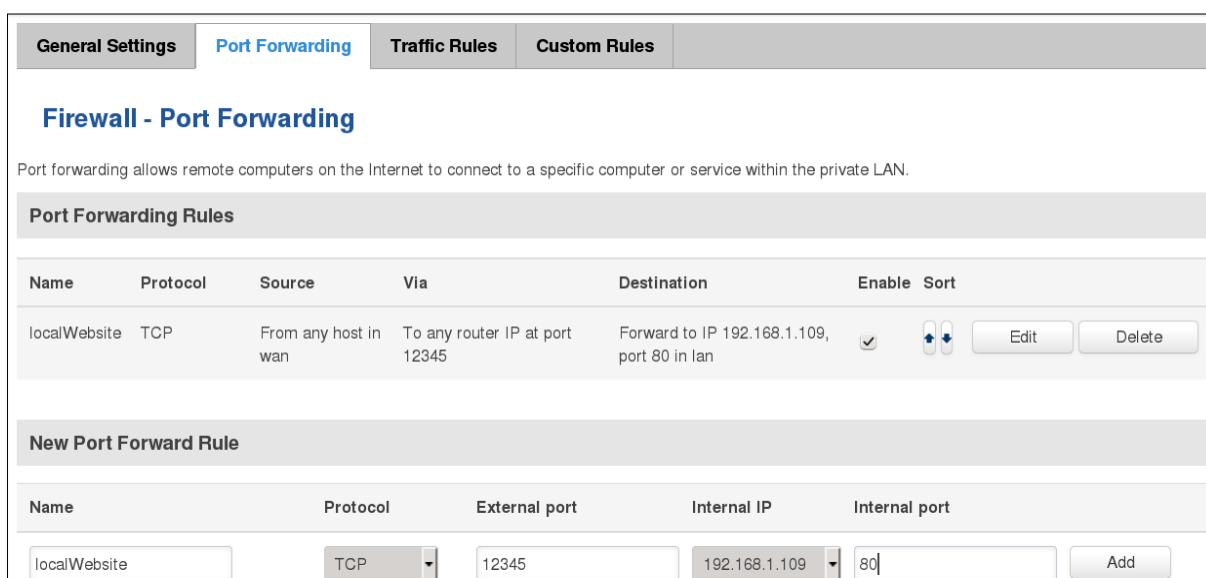


The image shows a 'DMZ Configuration' window. At the top, the title 'DMZ Configuration' is displayed. Below the title, there is an 'Enable' checkbox which is currently unchecked. Underneath the checkbox, there is a text label 'DMZ host IP address' followed by an empty rectangular input field.

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

7.6.3 Port Forwarding

Here you can define your own port forwarding rules.



The image shows a 'Firewall - Port Forwarding' interface. At the top, there are four tabs: 'General Settings', 'Port Forwarding' (which is selected), 'Traffic Rules', and 'Custom Rules'. Below the tabs, the title 'Firewall - Port Forwarding' is displayed. A descriptive text states: 'Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.' Below this, there is a section titled 'Port Forwarding Rules' containing a table with the following columns: Name, Protocol, Source, Via, Destination, Enable, and Sort. One rule is listed: 'localWebsite' with Protocol 'TCP', Source 'From any host in wan', Via 'To any router IP at port 12345', Destination 'Forward to IP 192.168.1.109, port 80 in lan', and an 'Enable' checkbox that is checked. To the right of the 'Enable' checkbox are 'Edit' and 'Delete' buttons. Below the table is a section titled 'New Port Forward Rule' with a form containing fields for Name, Protocol, External port, Internal IP, and Internal port, along with an 'Add' button. The fields are populated with: Name 'localWebsite', Protocol 'TCP', External port '12345', Internal IP '192.168.1.109', and Internal port '80'.

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/`.

	Field Name	Sample value	Explanation
1.	Name	"localWebsite"	Name of the rule. Used purely to make it easier to manage rules.
2.	Protocol	TCP/UDP/TCP+UDP/Other	Type of protocol of incoming packet.
3.	External Port	1-65535	From what port on the WAN network will the traffic be forwarded.
4.	Internal IP address	IP address of some computer on your LAN	The IP address of the internal machine that hosts some service that we want to access from the outside.
5.	Internal port	1-65535	To what port on the internal machine would the rule redirect the traffic.

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

Rule is enabled

Name

Protocol

Source zone lan: lan: vpn: (empty) wan: wan: ppp: wan2:

Source MAC address

Source IP address

Source port

External IP address

External port

Internal zone lan: lan: vpn: (empty) wan: wan: ppp: wan2:

Internal IP address

Internal port

Enable NAT loopback

Extra arguments

	Field Name	Sample value	Explanation
1.	Name	“localWebsite”	Name of the rule. Used purely to make it easier to manage rules.
2.	Protocol	TCP/UDP/TCP+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	12345	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	192.168.1.109	Redirect matched incoming traffic to the specified internal host
12.	Internal port	80	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 generalised rule definition. With it you can block or open ports, alter how traffic is forwarded between LAN and WAN and many more things.

	Field Name	Explanation
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.

Rule is disabled

Name

Restrict to address family

Protocol

Match ICMP type

Source zone

Any zone

lan: lan:

vpn: (empty)

wan: wan: ppp: wan2:

Source MAC address

Source address

Source port

Destination zone

Device (input)

Any zone (forward)

lan: lan:

vpn: (empty)

wan: wan: ppp: wan2:

Destination address

Destination port

Action

Extra arguments

	Field Name	Sample value	Explanation
1.	Name	"Allow-DHCP-Relay"	Used to make rule management easier
2.	Restrict to address family	IPv4-only	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 Router

Open Ports On Router

Name	Protocol	External port	
<input type="text" value="Open_Port_rule"/>	TCP ▾	<input type="text" value="22"/>	<input type="button" value="Add"/>

	Field Name	Sample value	Explanation
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 ▾	WAN ▾	<input type="button" value="Add"/>

	Field Name	Sample value	Explanation
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

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="SNAT"/>	<input type="button" value="LAN"/>	<input type="button" value="WAN"/>	<input type="text" value="10.101.1.10"/>	<input type="text" value="22"/>	<input type="button" value="Add"/>

	Field Name	Sample value	Explanation
1.	Name	Forward_rule_new	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		Redirect matched traffic to the given IP address and destination port
5.	SNAT		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.

Rule is enabled

Name

Protocol

Source zone lan: lan: vpn: (empty) wan: wan: ppp: wan2:

Source MAC address

Source IP address

Source port

Destination zone lan: lan: vpn: (empty) wan: wan: ppp: wan2:

Destination IP address

Destination port

SNAT IP address

SNAT port

Extra arguments

	Field Name	Sample value	Explanation
1.	Name	"Allow-DHCP-Relay"	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 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 the internet out for manuals, examples and explanations.

General Settings
Port Forwarding
Traffic Rules
Custom Rules

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_Jan_rule.
```

Reset
Submit

7.6.6 DDOS Prevention

7.6.6.1 SYN Flood Protection

SYN Flood Protection allows you to protect from attack that exploits 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.

The screenshot shows the configuration page for DDOS Prevention. The 'SYN Flood Protection' section is expanded, showing the following settings:

- Enable SYN flood protection:
- SYN flood rate:
- SYN flood burst:
- TCP SYN cookies:

	Field Name	Sample value	Explanation
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 a flood.
3.	SYN flood burst	"50"	Set burst limit for SYN packets above which the traffic is considered a flood 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.

Remote ICMP requests

Enable ICMP requests

Enable ICMP limit

Limit period

Limit

Limit burst

	Field Name	Sample value	Explanation
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-request 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 defined period

SSH Attack Prevention

Enable SSH limit

Limit period

Limit

Limit burst

	Field Name	Sample value	Explanation
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 attack sends 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 (e.g. 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.

HTTP Attack Prevention

Enable HTTP limit

Limit period

Limit

Limit burst

	Field Name	Sample value	Explanation
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

HTTPS Attack Prevention

Enable HTTPS limit

Limit period

Limit

Limit burst

	Field Name	Sample value	Explanation
1.	Enable HTTPS limit	Enable/Disable	Limits HTTPS connections per period
2.	Limit period	Second/Minute/Hour/Day	Select in what period limit HTTPS connections
3.	Limit	"10"	Maximum HTTPS connections during the period
4.	Limit burst	"10"	Indicating the maximum burst before the above limit kicks in.

7.7 Static Routes

Static routes provide a way of entering custom entries in the internal routing table of the router.

Routes

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

Static IP Routes

Interface	Target	Netmask	Gateway	Metric	
LAN <input type="text" value=""/>	<input type="text" value="192.168.55.0"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="192.168.55.145"/>	<input type="text" value="0"/>	<input type="button" value="Delete"/>
<input type="button" value="Add"/>					
<input type="button" value="Save"/>					

	Field name	Value	Explanation
1.	Interface	LAN/WAN/PPP/WAN2	The zone where the 'Target' resides
2.	Target	IP address	The source of the traffic.
3.	Netmask	IP mask	Mask that is applied to the Target to determine to what actual IP addresses the routing rule applies
4.	Gateway	IP address	To where the router should send all the traffic that applies to the rule
5.	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 – some IP that STARTS the segment; Netmask – Netmask that defines how large the segment is. E.g.:

192.168.55.161	255.255.255.255	Only applies to 192.168.55.161
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


8 Services

8.1 VRRP

8.1.1 VRRP LAN Configuration Settings

VRRP LAN Configuration Settings

Enable

IP address 

Virtual ID

Priority

	Field name	Sample	Explanation
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
4.	Priority	100	Router with highest priority value on the same VRRP (Virtual Router Redundancy Protocol) cluster will act as a master

8.1.2 Check Internet connection

Check internet connection

Enable

Ping IP address

Ping interval

Ping timeout (sec)

Ping packet size

Ping retry count

	Field name	Sample	Explanation
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 minutes 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	10	Failed Ping attempt's count before determining that connection is lost

8.2 TR-069

TR-069 is a standard developed for automatic configuration and management of remote devices by Auto Configuration Servers (ACS).

8.2.1 TR-069 Parameters Configuration


TR-069 Parameters Configuration

Enable

Enable Periodic Transmission

Sending Interval

User name

Password 

URL

	Field name	Sample	Explanation
1.	Enable	Enable/Disable	Enable TR-069 client
2.	Enable Periodic Transmission	Enable / Disable	Enable periodic transmissions of data to server
3.	Sending interval	100	Periodic data transmission to server period
4.	User name	admin	User name for authentication on TR-069 server
5.	Password	*****	Password for authentication on TR-069 server
6.	URL	http://192.168.1.110:8080	TR-069 server URL address

8.3 Web filter

8.3.1 Site blocking

Site Blocking Settings

Site Blocking

Enable

Mode

Enable	Host name	
<input checked="" type="checkbox"/>	<input type="text" value="www.yahoo.com"/>	<input type="button" value="Delete"/>

	Field name	Sample	Explanation
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

8.3.2 Proxy based URL content blocker

Proxy Based URL Content Blocker Configuration

Proxy Based URL Content Blocker

Enable

Mode

URL Filter Rules

Enable	URL content	
<input checked="" type="checkbox"/>	<input type="text" value="example.com"/>	<input type="button" value="Delete"/>

	Field name	Sample	Explanation
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

8.4 NTP

NTP configuration lets you setup and synchronize routers time.

The screenshot shows a web-based configuration interface for NTP. At the top, there are two tabs: 'General' and 'Time Servers', with 'Time Servers' being the active tab. Below the tabs is the title 'Time Synchronisation'. Underneath, there is a sub-section titled 'General'. This section contains the following fields and controls:

- 'Current system time' displayed as '2014-11-24 03:30:49' with a 'Sync with browser' button to its right.
- 'Time zone' set to 'UTC' in a dropdown menu.
- 'Enable NTP' checked with a checkbox.
- 'Update interval (in seconds)' set to '3600' in a text input field.
- 'Save time to flash' unchecked with a checkbox.
- 'Count of time synchronizations' in an empty text input field.

Below the 'General' section is another sub-section titled 'Clock Adjustment', which contains:

- 'Offset frequency' set to '0' in a text input field.

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

	Field name	Description	Notes
1.	Current System time	Local time of router.	---
2.	Time zone	Time zone of your country.	---
3.	Enable NTP	Enables the functionality	---
4.	Update interval	How often router updates systems time	---
5.	Count of time synchronizations	Total amount of times that router will do the synchronization	If left blank - the count will be infinite
6.	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.

8.5 VPN

8.5.1 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 RUT950 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.

The screenshot shows the OpenVPN configuration interface. At the top, there are tabs for 'OpenVPN', 'IPsec', 'GRE Tunnel', 'PPTP', and 'L2TP'. The 'OpenVPN' tab is selected. Below the tabs, the title 'OpenVPN' is displayed. Underneath, there is a section titled 'OpenVPN Configuration'. A table with the following headers is shown: Tunnel name, TUN/TAP, Protocol, Port, and Enabled. Below the table, a message states 'There are no openVPN configurations yet'. At the bottom, there is a form with a 'Role' dropdown menu set to 'Client', a 'New configuration name' input field containing 'demo', and an 'Add New' button.

The screenshot shows the OpenVPN configuration interface after a new configuration has been added. A green notification bar at the top states 'New OpenVPN instance was created successfully. Configure it now'. The 'OpenVPN' tab is selected. Below the tabs, the title 'OpenVPN' is displayed. Underneath, there is a section titled 'OpenVPN Configuration'. A table with the following headers is shown: Tunnel name, TUN/TAP, Protocol, Port, and Enabled. The table contains one entry: 'Client_demo' in the Tunnel name column, 'Tun_c_demo' in the TUN/TAP column, 'UDP' in the Protocol column, '1194' in the Port column, and 'No' in the Enabled column. To the right of this entry are 'Edit' and 'Delete' buttons. At the bottom, there is a form with a 'Role' dropdown menu set to 'Client', an empty 'New configuration name' input field, and an 'Add New' button.

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	IPsec	GRE Tunnel	PPTP	L2TP
<h2>OpenVPN Instance: Client_demo</h2>				
Main Settings				
Enable	<input type="checkbox"/>			
TUN/TAP	TUN (tunnel) ▼			
Protocol	UDP ▼			
Port	1194			
LZO	<input checked="" type="checkbox"/>			
Encryption	BF-CBC 128 (default) ▼			
Authentication	TLS ▼			
Remote host/IP address	215.45.60.66			
Resolve retry	Infinite			
Keep alive	10 60			
Remote network IP address	10.0.0.0			
Remote network IP netmask	255.255.255.0			
Certificate authority	<input type="text"/>			Browse...
Client certificate	<input type="text"/>			Browse...
Client key	<input type="text"/>			Browse...

There can be multiple server/client instances.

OpenVPN	IPsec	GRE Tunnel	PPTP	L2TP
OpenVPN Instance: Client_demo				
Main Settings				
Enable	<input type="checkbox"/>			
TUN/TAP	TUN (tunnel) ▼			
Protocol	UDP ▼			
Port	1194			
LZO	<input checked="" type="checkbox"/>			
Encryption	BF-CBC 128 (default) ▼			
Authentication	TLS ▼			
Remote host/IP address	215.45.60.66			
Resolve retry	Infinite			
Keep alive	10 60			
Remote network IP address	10.0.0.0			
Remote network IP netmask	255.255.255.0			
Certificate authority	<input type="text"/>			Browse...
Client certificate	<input type="text"/>			Browse...
Client key	<input type="text"/>			Browse...

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

	Field name	Explanation
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" 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:

		For client: Certificate Authority (CA), Client certificate, Client key. For server: Certificate Authority (CA), Server certificate, Server key and Diffie-Hellman (DH) certificate used to key exchange through unsafe data networks. All mention certificates can be generated using OpenVPN or OpenSSL utilities on any type host machine. Certificate generation and theory is out of scope of this user manual.
8.	Remote host IP address	IP address of OpenVPN server (applicable only for client configuration).
9.	Resolve Retry	Sets time in seconds to try resolving server hostname periodically in case of first resolve failure before generating service exception.
10.	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"
11.	Remote network IP address	IP address of remote network, an actual LAN network behind another VPN endpoint.
12.	Remote network IP netmask	Subnet mask of remote network, an actual LAN network behind another VPN endpoint.
13.	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.
14.	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.
15.	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.

8.5.2 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.

OpenVPN | **IPsec** | GRE Tunnel | PPTP | L2TP

IPsec

IPsec Configuration

Enable

Mode

Enable NAT traversal

Enable initial contact

My identifier type

My identifier

Pre shared key

Remote VPN endpoint

Enable DPD

Delay (sec)

	Field name	Explanation
1.	Enable	Check box to enable IPsec.
2.	Mode	Select "Main", "Aggressive" or "Base" mode accordingly to your IPsec server configuration.
3.	Enable NAT traversal	Enable this function if client-to-client applications will be used.
4.	Enable initial contact	Enable this to send an INITIAL-CONTACT message.
5.	My identifier type	Set the device identifier for IPsec tunnel. E.g. You can use your IP address
6.	My identifier	Set the device identifier for IPsec tunnel. In case RUT has Private IP, its identifier should be its own LAN network address. In this way, the RoadWarrior approach is possible.
7.	Preshare key	Specify the authentication secret [string]. Secret's length depends on selected algorithm, eg. 128 bit long secret is 16 characters in length, 128 bits / 8 bits (one character) = 16.
8.	Remote VPN endpoint	Set remote IPsec server IP address.
9.	Enable DPD	If the RUT does not receive DPD-ACK message from its IPsec peer, RUT shuts the connection down.
10.	Delay (sec)	Select delay between peer acknowledgement requests

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

Hash algorithm SHA1

DH group MODP768

Lifetime (sec) 28800

Phase

The phase must match with another incoming connection to establish IPsec

Phase 1 **Phase 2**

Encryption algorithm 3DES

PFS group MODP768

Authentication HMAC_SHA1

Life time (sec) 3600

Remote Network Secure Group – Set the remote network (Secure Policy Database) information. It must be LAN network of remote IPsec host.

Remote Network Secure Group

IP address

Subnet mask

Tunnel Keep Alive

Allows sending ICMP echo requests to the remote tunnel network

Enable

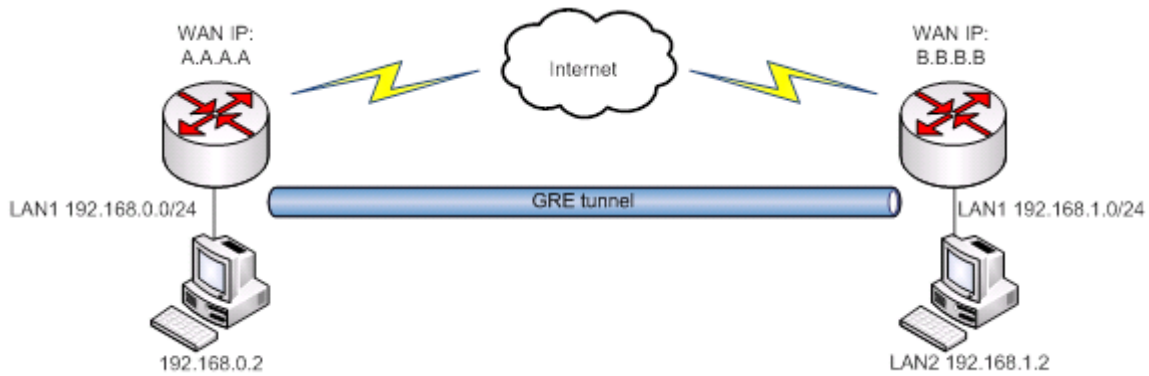
Host

Ping period (sec)

	Field name	Explanation
1.	Tunnel keep alive	Allows sending ICMP echo request (Ping utility) to the remote tunnel network. This function may be used to automatically start the IPsec tunnel. This function should be used every time.
2.	Enable	Allows sending ICMP echo requests to the remote tunnel network
3.	Host	Enter IP address to which ICMP echo requests will be sent.
4.	Ping period (sec)	Set sent ICMP request period in seconds.

8.5.3 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.

OpenVPN	IPsec	GRE Tunnel	PPTP	L2TP
Gre-tunnel Instance: Gre_tunnel				
Main Settings				
Enabled <input checked="" type="checkbox"/>				
Remote endpoint IP address	<input type="text" value="84.148.7.87"/>			
Remote network	<input type="text" value="192.168.2.0"/>			
Remote network netmask	<input type="text" value="24"/>			
Local tunnel IP	<input type="text" value="10.0.0.1"/>			
Local tunnel netmask	<input type="text" value="24"/>			
MTU	<input type="text" value="1500"/>			
TTL	<input type="text" value="255"/>			
PMTUD <input checked="" type="checkbox"/>				
Enable Keep alive <input checked="" type="checkbox"/>				
Keep Alive host	<input type="text"/>			
Keep Alive interval	<input type="text"/>			

	Field name	Explanation
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. Can not 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 keepalive packets to and from a remote router even if the remote router does not support GRE keepalives.
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].

8.5.4 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).

The screenshot displays the configuration page for a PPTP server instance. At the top, there are navigation tabs: OpenVPN, IPsec, GRE Tunnel, PPTP (selected), and L2TP. The main heading is "PPTP Server Instance: Pptpd_server". Under the "Main Settings" section, the "Enable" checkbox is unchecked. The "Local IP" is set to 192.168.0.1, the "Remote IP range start" is 192.168.0.20, and the "Remote IP range end" is 192.168.0.30. Below the settings is a table for user management with columns for "User name", "Password", and "User IP". A single user entry is shown with the name "youruser" and a masked password. There are "Add", "Delete", and "Save" buttons.

	Field name	Explanation
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

8.5.5 L2TP

Allows setting up a L2TP server or client and should it be needed - using it with IPsec (L2TP/IPSec). Below is L2TP server configuration example.

The screenshot shows a web configuration interface for L2TP. At the top, there are tabs for 'OpenVPN', 'IPsec', 'GRE Tunnel', 'PPTP', and 'L2TP'. The current page is titled 'L2TP Server Instance: L2tpd_server'. Under the 'Main Settings' section, there is an 'Enable' checkbox, a 'Local IP' field with the value '192.168.0.1', a 'Remote IP range begin' field with '192.168.0.20', and a 'Remote IP range end' field with '192.168.0.30'. Below this is a table for user management with columns for 'User name' and 'Password'. A table entry shows 'user' as the username and a masked password. There are 'Add', 'Delete', and 'Save' buttons.

	Field name	Explanation
1.	Enable	Check the box to enable the GRE 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**.

8.6 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 Configuration			
DDNS Name	Hostname	Status	Enabled
Myddns	yourhost.example.org	N/A	No
Demo	mypersonaldomain.dyndns.org	N/A	No

New configuration name:

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

DDNS	
Enable	<input type="checkbox"/>
Status	N/A
Service	3322.org
Hostname	yourhost.example.org
User name	your_username
Password
IP source	Custom
Network	WAN
IP renew interval (min)	10
Force IP renew (min)	472

	Field name	Value	Explanation
1.	Enable	-	Enables current DDNS configuration.
2.	Status	-	Timestamp of the last IP check or update.
3.	Service	1. dydns.org 2. 3322.org 3. no-ip.com 4. easydns.com 5. zoneedit.com	Your dynamic DNS service provider selected from the list. 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 Private 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 (3G/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.	IP renew interval (min)	10 (minutes)	Time interval (in minutes) to check if the IP address of the device have changed.
9.	Force IP renew	472 (minutes)	Time interval (in minutes) to force IP address renew.

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 Configuration

SNMP Service Settings

SNMP Settings

TRAP Settings

Enable SNMP service

Enable remote access

Port

Community

Location

Contact

Name

	Field name	Sample	Explanation
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

	OID	Description
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

TRAP Service Settings

SNMP Trap

Host/IP

Port

Community

TRAP Rules

Action	Enable	
Connection type trap	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Signal strength trap	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

New TRAP Rule

Action

	Field name	Sample	Explanation
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 Utilities

RUT950 has extensive amount of various SMS Utilities. These are subdivided into 6 sections: SMS Utilities, Call Utilities, User Groups, SMS Management, Remote Configuration, Statistics.

8.8.1 SMS Utilities

Action	SMS Text	Enable	Sort	
Reboot	reboot	<input checked="" type="checkbox"/>	↑ ↓	Edit Delete
Get status	status	<input checked="" type="checkbox"/>	↑ ↓	Edit Delete
Switch WiFi on	wifion	<input checked="" type="checkbox"/>	↑ ↓	Edit Delete
Switch WiFi off	wifioff	<input checked="" type="checkbox"/>	↑ ↓	Edit Delete
Switch mobile data on	mobileon	<input checked="" type="checkbox"/>	↑ ↓	Edit Delete
Switch mobile data off	mobileoff	<input checked="" type="checkbox"/>	↑ ↓	Edit Delete
Change mobile data settings	cellular	<input checked="" type="checkbox"/>	↑ ↓	Edit Delete
Get list of profiles	profdisp	<input checked="" type="checkbox"/>	↑ ↓	Edit Delete
Change profile	pr	<input checked="" type="checkbox"/>	↑ ↓	Edit Delete
SSH access Control	ssh	<input checked="" type="checkbox"/>	↑ ↓	Edit Delete
Web access Control	web	<input checked="" type="checkbox"/>	↑ ↓	Edit Delete

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. All configuration options are listed below:

	Field name	Explanation	Notes
1.	Enable SMS Reboot	This check box will enable and disable SMS reboot function.	If you select Get Status, it will send routers status once it has rebooted and is operational again. For Get Status description see item No. 4 of this table.
2.	SMS text	SMS text which will reboot router.	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.
3.	Sender phone number	Phone number of person who can reboot router 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.
4.	Get status	Check this to receive connection status via SMS after a reboot.	This is both separate SMS Rule and an option under SMS Reboot rule.
5.	Enable SMS Status	This check box will enable and disable SMS status function.	SMS status is disabled by default.
6.	SMS text	SMS text which will send routers status.	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.
7.	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.
8.	Get Information	Data state Operator Connection type Signal Strength Connection State IP	You can select which status elements to display.
9.	Wireless On/Off via SMS	This check box will enable and disable this function	Allows Wi-Fi control via SMS
10.	Wireless on SMS text	SMS text which will turn Wi-Fi ON	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.
11.	Wireless on SMS text	SMS text which will turn Wi-Fi OFF	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.
12.	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.
13.	Write to config	Permanently saves Wi-Fi state	With this setting enabled, router will keep Wi-Fi state even after reboot. If it is not selected, router will revert Wi-Fi state after reboot.
14.	Mobile Settings via SMS	This check box will enable and disable mobile settings function	Allows cellular control via SMS
15.	SMS text	Key word that will precede actual configuration parameters	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.
16.	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.

Mobile Settings via SMS parameters:

	Parameter	Value(s)	Explanation
1.	apn=	i.e. internet.gprs	Sets APN. i.e: apn=internet.gprs
2.	dialnumber=	i.e. *99***1#	Sets dial number
3.	auth_mode=	none pap chap	Sets authentication mode
4.	service=	auto 3gpreferred 3gonly 2gpreferred 2gonly	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=3gonly username=user password=user*

	Field name	Explanation	Notes
1.	3G On/Off via SMS	This check box will enable and disable this function	Function disabled by default
2.	3G on SMS text	Text to turn 3G connection ON	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.
3.	3G off SMS text	Text to turn 3G connection OFF	
4.	Write to config	Permanently saves 3G network state	With this setting enabled, router will keep 3G state even after reboot. If it is not selected, router will revert 3G state after reboot.
5.	Change profile via SMS	This check box will enable and disable this function	Function disabled by default
6.	SMS text to change profile	Keyword that must precede profile name	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.
7.	SMS text to get list of profiles	Upon receiving this SMS router will send list of created profiles to the sender number	
8.	Sender Phone number	Phone number of person who can control this function	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.

Important Notes:

- 3G settings must be configured correctly. If SIM card has PIN number you must enter it at “Network” > “3G” 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.

8.8.2 Call Utilities

Allows users to Call the router in order to perform one of the actions: Reboot, Get Status, turn WiFi ON/OFF, turn Mobile data ON/OFF. Only thing that is needed is to call routers SIM card number from allowed phone (user) and RUT950 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".

Modify Call Rule

Enable

Action

Allowed users

Get status via SMS after reboot


	Field name	Sample	Explanation
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 WiFi, Switch mobile data, switch output
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


8.8.3 User Groups



Gives 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.

Modify User Group

Group name

Phone number 



	Field name	Sample	Explanation
1.	Group name	Group1	Your name of the phone numbers group
2.	Phone number	+37061111111	Number to add to users group, must match international format. You can add many phone numbers fields by clicking on the green + symbol

8.8.4 SMS Management

8.8.4.1 Read SMS

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

Read SMS | Send SMS | Storage

SMS Messages

SMS per page: 10 | Search:

Date ↑ | Sender ↑ | Message ↑

There are no messages

Showing 1 to 1 of 1 entries

Refresh | Delete | Select all

8.8.4.2 Send SMS

Read SMS | Send SMS | Storage

Send SMS

Send SMS Message

Phone Number: +3701111111

Message: My text.

SMS 1 (152 characters left)

Send

	Field name	Sample	Explanation
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.

8.8.4.3 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.

	Field name	Sample	Explanation
1.	Save messages on SIM	Enabled / Disabled	Enables received message storing on SIM card
2.	Leave free space	1	Specifies how much space for SMS should remain free on SIM at all times.

8.8.5 Remote Configuration

RUT9xx can be configured via SMS from another RUT9xx. You only have to select which configuration details are to be sent, 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.

8.8.5.1 Receive configuration

This section controls how should configuration initiation party should identify itself. In this scenario RUT950 itself is being configured.

	Field name	Values	Notes
1.	Enable	Enabled / Disabled	Enables router to receive configuration

1.	Authorization method	No authorization / By serial By administration password	Method at Receiving and Sending ends must match
2.	Allowed users	From all numbers From group From single number	Gives greater control and security measures

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

8.8.5.2 Send configuration

This section lets you configure remote RUT950 devices. The authorization settings must confirm to those that are set on the receiving party.

Generate SMS New

WAN

Interface Wired

Protocol Static

IP address

IP netmask

IP gateway

IP broadcast

Network VPN

Generate

Wan

Interface

Mobile connection

APN

Dialing number

Authentication method

Username

Password

Service mode

Lan

IP address

IP netmask

IP broadcast

Send Configuration Message

Generate

Phone number

Serial number

Send

	Field name	Values	Notes
1.	Generate SMS	New From current configuration	Generate new SMS settings or use current device configuration
2.	Mobile	Enable/Disable	Include configuration for mobile network
3.	WAN	Enable/Disable	Include configuration for WAN (Wide Area Network)
4.	LAN	Enable/Disable	Include configuration for LAN (Local Area Network)
5.	Interface	Wired Mobile	Interface type used for WAN (Wide Area Network) connection
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
14.	Mobile connection	Use pppd mode 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 a GPRS, 3G or 4G mobile network 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	2G only 2G preferred 3G only 3G preferred 4G (LTE) only 4G (LTE) preferred Automatic	Select network's preference. If your local mobile network supports GSM (2G), UMTS (3G) or LTE (4G) you can specify to which network you prefer to connect to
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

Send Configuration Message

```
network.wan.ifname=eth1, network.ppp.enabled=0, network.wan.proto=static,
network.wan.ipaddr=217.147.40.44, network.wan.netmask=255.255.255.0,
network.wan.gateway=217.147.40.44, network.wan.broadcast=217.147.40.255
```

Phone number

Authorization method

	Field name	Values	Notes
1.	Message text field	Generated configuration	Here you can review and modify configuration

		message	message text to be sent
2.	Phone number	+37060000001	A phone number of router which will receive the configuration
3.	Authorization method	No authorization By serial By router admin password	What kind of authorization to use for remote configuration

8.8.6 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.

SMS Utilities	Call Utilities	User Groups	SMS Management	Remote Configuration	Statistics
Statistics					
SMS Statistics					
SIM Card	Sent SMS	Received SMS			
SIM 1	0	0	Reset		
SIM 2	0	0	Reset		

8.9 SMS Gateway

8.9.1 Post/Get Configuration

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

Post/Get	Email To SMS	Scheduled SMS	Auto Reply	SMS Forwarding	SMPP
Post/Get Configuration					
SMS Post/Get Settings					
Enable <input checked="" type="checkbox"/>					
User name <input type="text" value="admin"/>					
Password <input type="password" value="*****"/>					
Save					

	Field name	Values	Notes
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!

8.9.1.1 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.

	Action	POST/GET url e.g.
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=003706000001&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

8.9.1.2 Syntax of HTTP POST/GET string

HTTP POST/GET string	Explanation
http://{IP_ADDRESS}/cgi-bin/sms_read?username={your_user_name}&password={your_password}&number={MESSAGE_INDEX}	Read message
http://{IP_ADDRESS}/cgi-bin/sms_send?username={your_user_name}&password={your_password}&number={PHONE_NUMBER}&text={MESSAGE_TEXT}	Send message
http://{IP_ADDRESS}/cgi-bin/sms_delete?username={your_user_name}&password={your_password}&number={MESSAGE_INDEX}	Delete message
http://{IP_ADDRESS}/cgi-bin/sms_list?username={your_user_name}&password={your_password}	List all messages
http://{IP_ADDRESS}/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.

8.9.1.3 Parameters of HTTP POST/GET string

	Parameter	Explanation
1.	IP_ADDRESS	IP address of your router
2.	MESSAGE_INDEX	SMS index in memory
3.	PHONE_NUMBER	Phone number of the message receiver. Note: Phone number must contain country code. Phone number format is: 00{COUNTRY_CODE}{RECEIVER_NUMBER}. 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.

8.9.1.4 Possible responses after command execution

	Response	Explanation
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

8.9.1.5 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=003706000001&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

8.9.2 Email to SMS

	Field name	Values	Notes
1.	Enable	Enable/Disable	Allows to convert received Email to SMS
2.	POP3 server	“pop.gmail.com”	POP3 server address
3.	Server port	“995”	Server authentication port
4.	User name	“admin”	User name using for server authentication
5.	Password	“admin01”	Password using for server authentication

6.	Secure connection (SLL)	Enable/Disable	(SSL) is a protocol for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message.
7.	Check mail every	Minutes Hours Days	Mail checking period

8.9.3 Scheduled Messages

Scheduled messages allows to periodically send mobile messages to specified number.

Post/Get Configuration
Email To SMS
Scheduled Messages
Auto Reply

Scheduled Messages

Configure time and text for scheduled messages.

Messages To Send

Recipients number	Sending Interval	Enable	Sort
<i>There are no scheduled messages created yet</i>			

Scheduled messages Configuration:

Phone number	Message sending interval
--------------	--------------------------

▼

8.9.3.1 Scheduled Messages Configuration

	Field name	Values	Notes
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.

8.9.4 Auto Reply Configuration

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

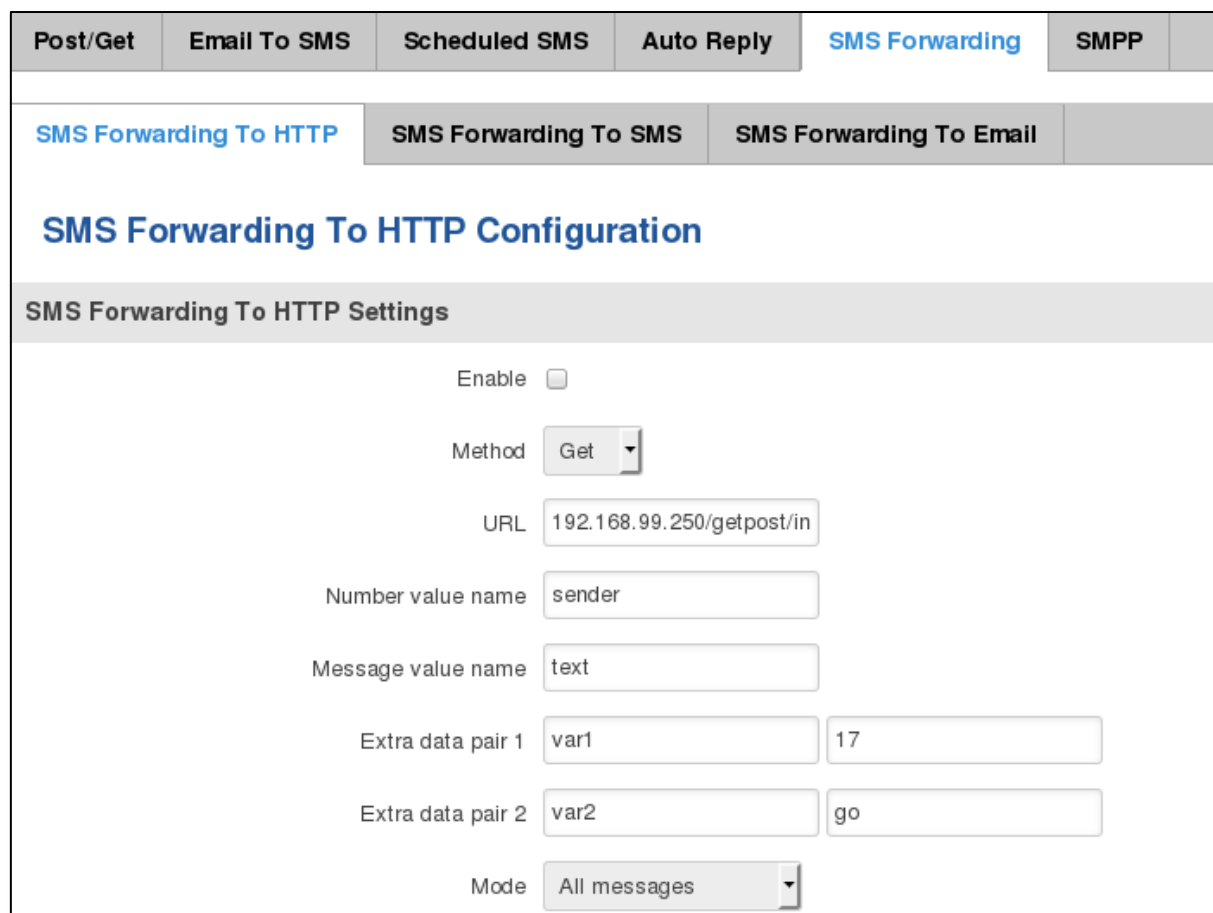
The screenshot shows the 'Auto Reply Configuration' page. At the top, there are five tabs: 'Post/Get Configuration', 'Email To SMS', 'Scheduled Messages', 'Auto Reply' (which is highlighted in blue), and 'SMS Forwarding'. Below the tabs, the page title 'Auto Reply Configuration' is displayed in blue. Underneath the title is a section header 'Reply Configuration'. This section contains four configuration items: 'Enable' with an unchecked checkbox, 'Don't save received message' with a checked checkbox, 'Mode' with a dropdown menu currently showing 'Everyone', and 'Message' with a large, empty text input area.

	Field name	Values	Notes
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.

8.9.5 SMS Forwarding

8.9.5.1 SMS Forwarding To HTTP

This functionality forwards mobile messages from all or only specified senders to HTTP, using either POST or GET methods.



	Field name	Values	Notes
1.	Enable	Enable / Disable	Enable mobile message forwarding to HTTP
2.	Method	POST / GET	Defines the HTTP transfer method
3.	URL	192.168.99.250/getpost/index.php	URL address to forward messages to
4.	Number value name	“sender”	Name to assign for sender’s phone number value in query string
5.	Message value name	“text”	Name to assign for message text value in query string
6.	Extra data pair 1	Var1 - 17	If you want to transfer some extra information through HTTP query, enter variable name on the left field and its value on the right
7.	Extra data pair 2	Var2 – “go”	If you want to transfer some extra information through HTTP query, enter variable name on the left field and its value on the right
8.	Mode	All messages/From listed numbers	Specifies which senders messages to forward

8.9.5.2 SMS Forwarding to SMS

This functionality allows forwarding mobile messages from specified senders to one or several recipients.

SMS Forwarding To HTTP SMS Forwarding To SMS SMS Forwarding To Email

SMS Forwarding To SMS Configuration

SMS Forwarding To SMS Settings

Enable

Add sender number

Mode All messages

recipients phone numbers

	Field name	Values	Notes
1.	Enable	Enable / Disable	Enable mobile message forwarding
2.	Add sender number	Enable / Disable	If enabled, original senders number will be added at the end of the forwarded message
3.	Mode	All message / From listed numbers	Specifies from which senders received messages are going to be forwarded.
4.	Recipients phone numbers	+37060000001	Phone numbers to which message is going to be forwarded to

8.9.5.3 SMS Forwarding To Email

This functionality forwards mobile messages from one or several specified senders to email address.

SMS Forwarding To Email Settings

Enable

Add sender's number


Subject

SMTP server


SMTP server port

Secure connection

User name

Password 

Sender's email address

Recipient's email address 

Mode

	Field name	Values	Notes
1.	Enable	Enable / Disable	Enable mobile message forwarding to email
2.	Add sender number	Enable / Disable	If enabled, original senders number will be added at the end of the forwarded message
3.	Subject	"forwarded message"	Text that will be inserted in email Subject field
4.	SMTP server	mail.teltonika.it	Your SMTP server's address
5.	SMTP server port	25	Your SMTP server's port number
6.	Secure connection	Enable / Disable	Enables the use of cryptographic protocols, enable only if your SMTP server supports SSL or TLS
7.	User name	"admin"	Your full email account user name
8.	Password	*****	Your email account password
9.	Sender's email address	name.surname@gmail.com	Your address that will be used to send emails from
10.	Recipient's email address	name2.surname2@gmail.com	Address that you want to forward your messages to
11.	Mode	All messages / from listed numbers	Choose which senders messages to forward to email

8.9.6 SMPP


SMPP (Short Message Peer to Peer) server allows clients to connect to router using SMPP protocol and then send SMS via mobile network. This SMPP server implementation allows sending messages, but receiving incoming messages is not supported for now.

SMPP Server Configuration

Transmitter Configuration

Enable

User name

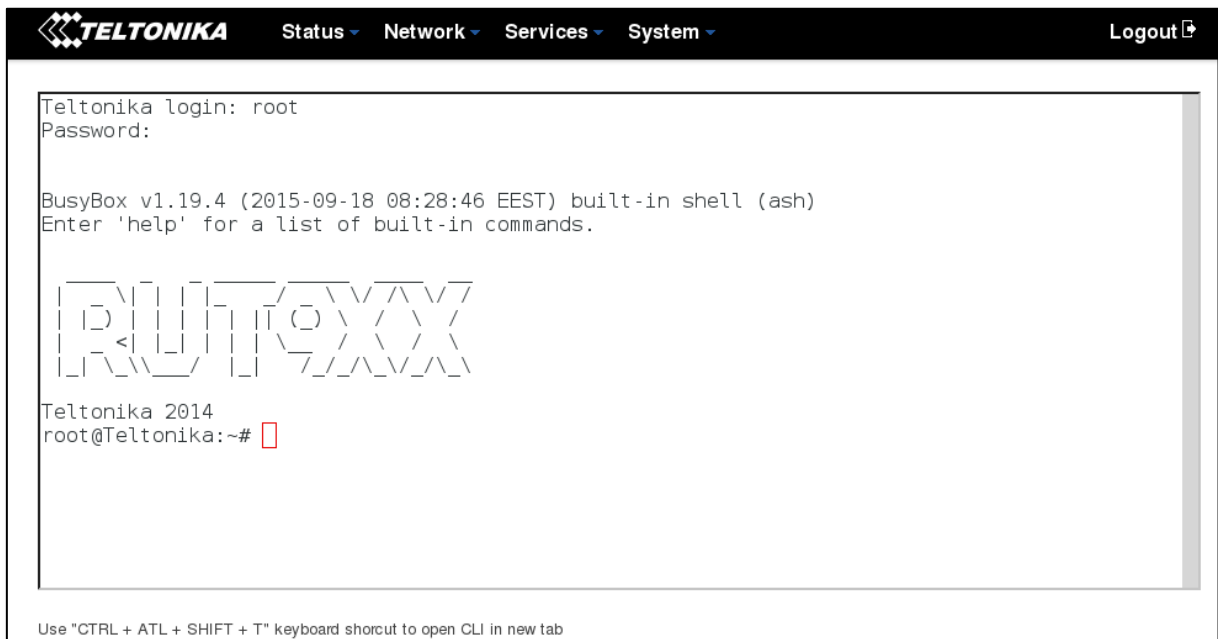
Password 

Server port

	Field name	Values	Notes
1.	Enable	Enable / Disable	Enables SMPP server on router
2.	User name	admin	User name which clients will need to connect to SMPP server
3.	Password	*****	Password which clients will need to connect to SMPP server
4.	Server port	7777	Server port to be used for SMPP communication. You can choose any unused port (0 - 65535)

8.10 CLI

CLI or Comand Line Interface functionality allows you to enter and execute comands into routers terminal.



```
Teltonika login: root
Password:

BusyBox v1.19.4 (2015-09-18 08:28:46 EEST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

      _ _ _ _ _
     / / / / /
    / / / / /
   / / / / /
  / / / / /
 / / / / /
/ / / / /

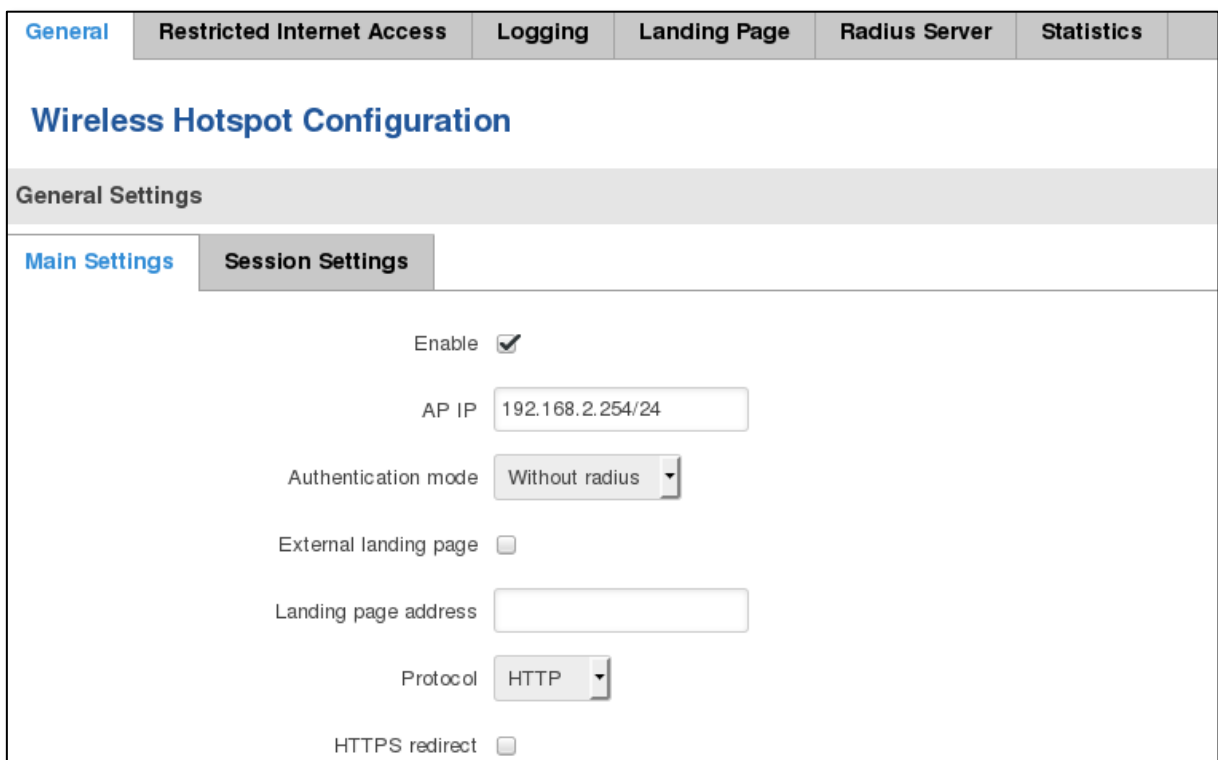
Teltonika 2014
root@Teltonika:~#
```

Use "CTRL + ATL + SHIFT + T" keyboard shorcut to open CLI in new tab

8.11 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.).

8.11.1 General settings



General | Restricted Internet Access | Logging | Landing Page | Radius Server | Statistics

Wireless Hotspot Configuration

General Settings

Main Settings | **Session Settings**

Enable

AP IP

Authentication mode

External landing page

Landing page address

Protocol

HTTPS redirect

Users Configuration	
User name	Password
<i>There are no users created yet.</i>	
<input type="button" value="Add"/>	


	Field name	Explanation
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).
3.	Authentication mode	External radius
4.	Radius server #1	The IP address of the RADIUS server that is to be used for Authenticating your wireless clients.
5.	Radius server #2	The IP address of the second RADIUS server.
6.	Authentication port	RADIUS server authentication port.
7.	Accounting port	RADIUS server accounting port.
8.	Authentication mode	Internal radius
9.	IP address or network of the client	E.g.(192.168.1.1 or 192.168.1.0/24)
10.	Authentication mode	Without radius
11.		Doesn't require any RADIUS configuration. Allows simple user connection based on username/password.
12.	External landing page	Enables the use of external landing page.
13.	Landing page address	The address of external landing page
14.	Protocol	HTTP or HTTPs.
15.	HTTPS redirect	Redirects HTTP pages to landing page.

8.11.2 Internet Access Restriction Settings

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

General	Restricted Internet Access	Logging	Landing Page	Radius Server																				
Teltonika_Router																								
Internet Access Restriction Settings																								
Select Time To Restrict Access On Hotspot Teltonika_Router																								
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																								
<input type="checkbox"/> Internet access allowed <input checked="" type="checkbox"/> Internet access blocked																								

8.11.3 Logging

General	Restricted Internet Access	Logging	Landing Page	Radius Server
Wireless Hotspot Logging Settings				
Logging To FTP Settings				
Enable <input type="checkbox"/>				
Server address <input type="text" value="your.ftp.server"/>				
User name <input type="text" value="username"/>				
Password <input type="password" value="....."/> 				
Port <input type="text" value="21"/>				

	Field name	Explanation
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

	Field name	Explanation
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.	Weekdays	This field specifies on what weekdays the uploading should be done. The entry format is numbers from 1 to 7 separated by only commas. E.g. If you want to upload the logs on Monday, Wednesday and Saturday you should enter "1,3,6".
3.	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.
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.

8.11.4 Landing Page

8.11.4.1 General Landing Page Settings

With this functionality you can customize your Hotspot Landing page.

General Template

Wireless Hotspot Landing Settings

Landing Page Settings

Page title

Theme

Upload login page No file selected.

Login page file

Terms Of Services

Background Configuration

Logo Image Configuration

Link Configuration

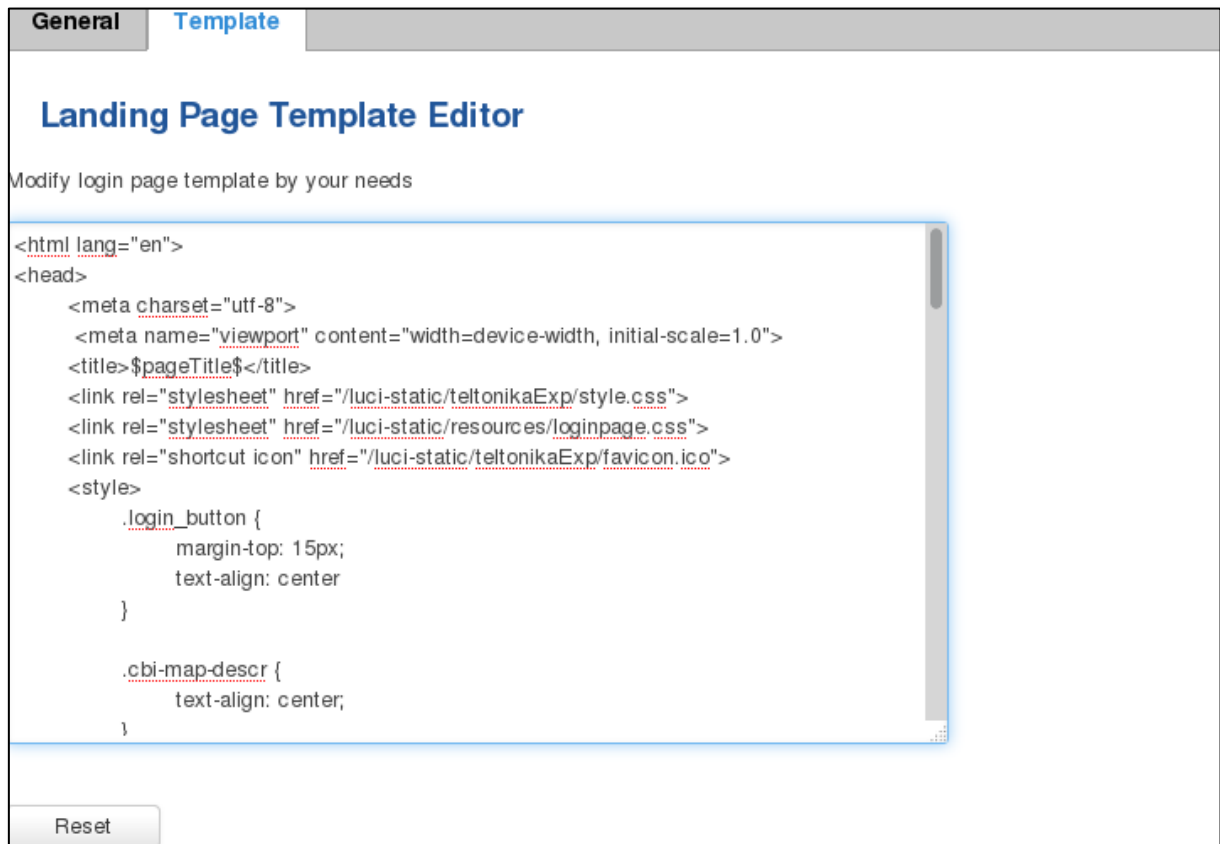
Text Configuration

	Field name	Explanation
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.

8.11.4.2 Template

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



The screenshot shows a web interface for editing the landing page template. At the top, there are two tabs: "General" and "Template", with "Template" being the active tab. Below the tabs is the title "Landing Page Template Editor" and a subtitle "Modify login page template by your needs". The main content area is a text editor containing HTML and CSS code. At the bottom left, there is a "Reset" button.

```
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>${pageTitle}</title>
  <link rel="stylesheet" href="/luci-static/teltonikaExp/style.css">
  <link rel="stylesheet" href="/luci-static/resources/loginpage.css">
  <link rel="shortcut icon" href="/luci-static/teltonikaExp/favicon.ico">
  <style>
    .login_button {
      margin-top: 15px;
      text-align: center
    }

    .cbi-map-descr {
      text-align: center;
    }
  </style>
</head>
<body>
  <div class="login">
    <div class="login-button">
      <button type="button">Login</button>
    </div>
  </div>
</body>
</html>
```


8.11.5 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.

Radius Server Configuration

General Settings

Enable

Remote access

Accounting port

Authentication port

Users Configuration Settings

Enable	User name	Reply message	Idle timeout	Session timeout	Download bandwidth	Upload bandwidth
There are no users created yet.						

Username **Password**

Clients Configuration Settings

Enable	Client name	IP address	Netmask	Radius shared secret
There are no clients created yet.				

	Field name	Explanation
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

8.11.6 Statistics

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

8.12 Auto Reboot

8.12.1 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.

	Field name	Explanation	Notes
1.	Enable	This check box will enable or disable Ping reboot feature.	Ping Reboot is disabled by default.
2.	Reboot router if no echo received	This check box will disable router rebooting after the defined number of unsuccessful retries.	This check box must be unselected if you want to use Ping Reboot feature as “Keep Alive” function.

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.
7.	Host to ping from SIM 1	IP address or domain name which will be used to send ping packets to. E.g. 192.168.1.1 (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. 192.168.1.1 (or www.host.com if DNS server is configured correctly)	Ping packets will be sending from SIM2.

8.12.2 Periodic Reboot

Ping Reboot
Periodic Reboot

Periodic Reboot

Periodic Reboot Setup

Enable

Days

- Sunday
- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday

Hours

Minutes

	Field name	Explanation
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

8.13 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, port prioritization.

Quality of Service

With QoS you can prioritize network traffic selected by addresses, ports or services.

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:

Classification Rules

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

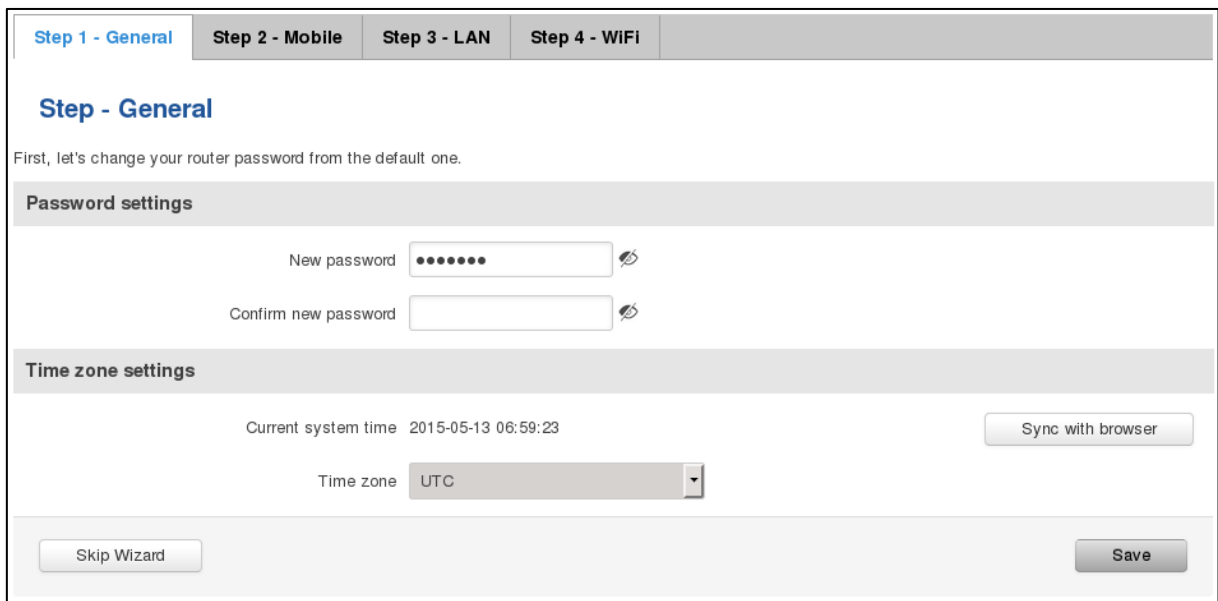
9 System

9.1 Configuration 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)

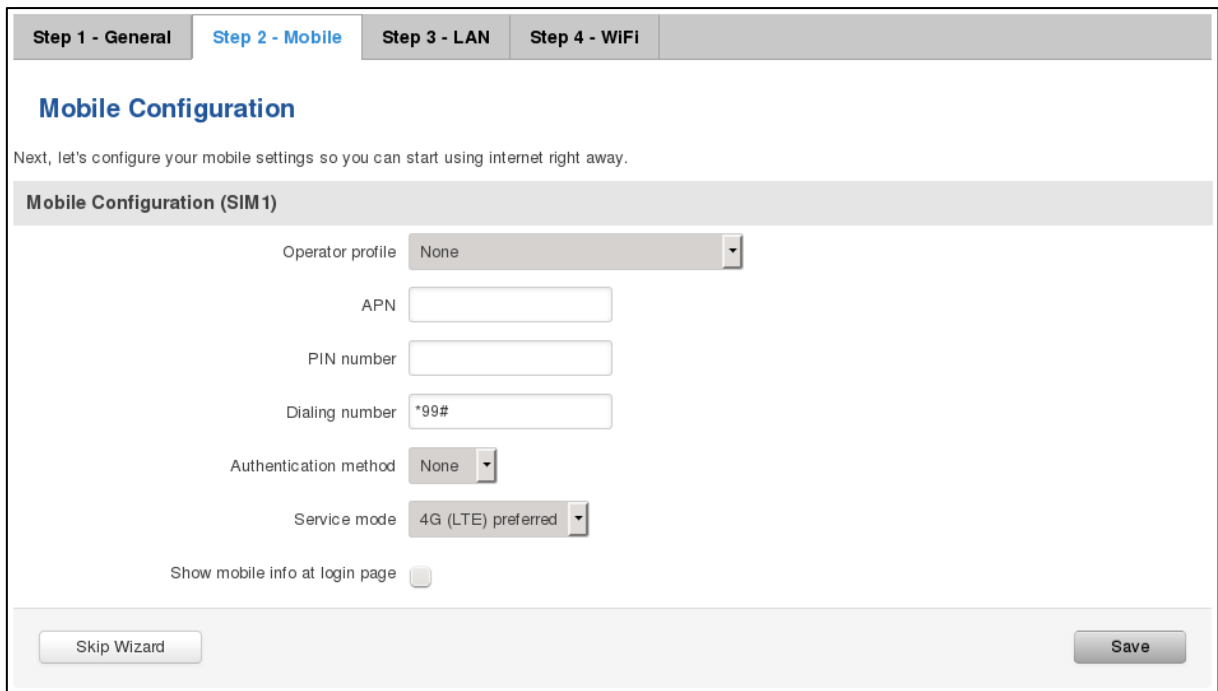
First, the wizard prompts you to change the default password. Simply enter the same password into both Password and Confirmation fields and press **Next**.



The screenshot shows the 'Step 1 - General' configuration screen. At the top, there are four tabs: 'Step 1 - General' (active), '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.' The 'Password settings' section contains two input fields: 'New password' (with a masked password of seven dots) and 'Confirm new password' (empty). Both fields have an eye icon to toggle visibility. The 'Time zone settings' section shows the 'Current system time' as '2015-05-13 06:59:23' and a 'Sync with browser' button. The 'Time zone' is set to 'UTC' in a dropdown menu. At the bottom, there are two buttons: 'Skip Wizard' and 'Save'.

Step 2 (Mobile Configuration)

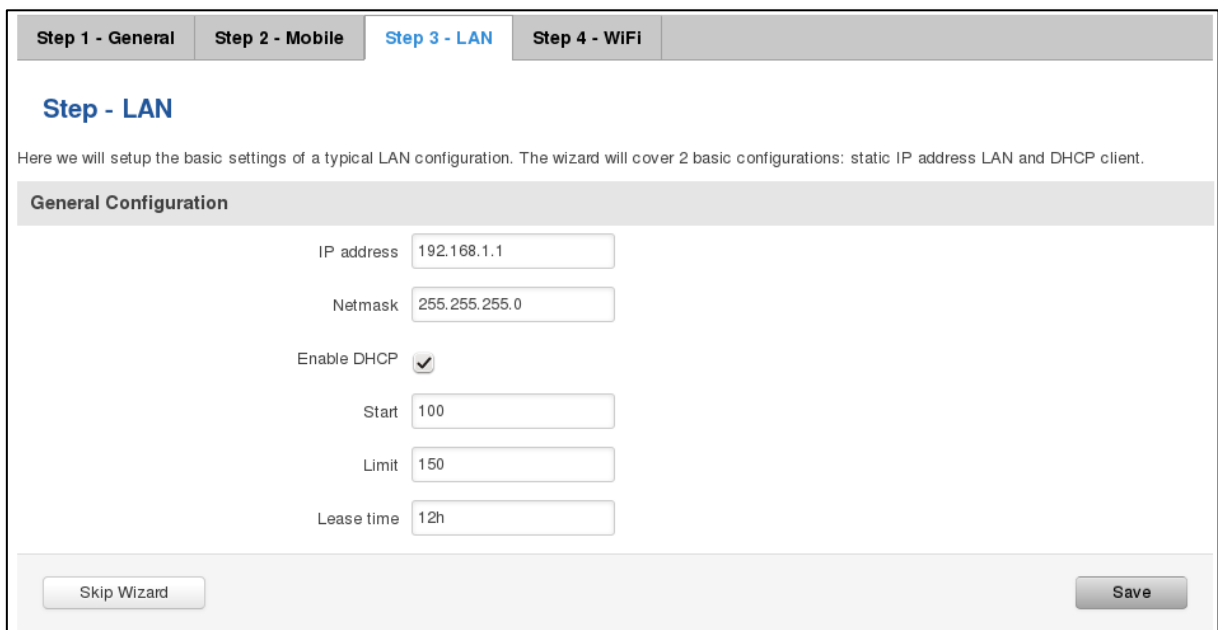
Next we have to enter your mobile configuration. On a detailed instruction on how this should be done see the Mobilesection under Network



The screenshot shows the 'Mobile Configuration' step of a network setup wizard. At the top, there are four tabs: 'Step 1 - General', 'Step 2 - Mobile' (which is active and highlighted in blue), 'Step 3 - LAN', and 'Step 4 - WIFI'. Below the tabs, the title 'Mobile Configuration' is displayed in blue. A sub-header 'Mobile Configuration (SIM1)' is followed by a grey bar. Below this, a message reads: 'Next, let's configure your mobile settings so you can start using internet right away.' The configuration fields include: 'Operator profile' (dropdown menu set to 'None'), 'APN' (text input field), 'PIN number' (text input field), 'Dialing number' (text input field with '*99#' pre-filled), 'Authentication method' (dropdown menu set to 'None'), and 'Service mode' (dropdown menu set to '4G (LTE) preferred'). There is also a checkbox for 'Show mobile info at login page' which is currently unchecked. At the bottom of the form, there are two buttons: 'Skip Wizard' on the left and 'Save' on the right.

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.



The screenshot shows the 'Step - LAN' configuration step of a network setup wizard. At the top, there are four tabs: 'Step 1 - General', 'Step 2 - Mobile', 'Step 3 - LAN' (which is active and highlighted in blue), and 'Step 4 - WIFI'. Below the tabs, the title 'Step - LAN' is displayed in blue. A sub-header 'General Configuration' is followed by a grey bar. Below this, a message reads: '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.' The configuration fields include: 'IP address' (text input field with '192.168.1.1' pre-filled), 'Netmask' (text input field with '255.255.255.0' pre-filled), 'Enable DHCP' (checkbox which is checked), 'Start' (text input field with '100' pre-filled), 'Limit' (text input field with '150' pre-filled), and 'Lease time' (text input field with '12h' pre-filled). At the bottom of the form, there are two buttons: 'Skip Wizard' on the left and 'Save' on the right.

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

Mode

Channel

Encryption

Country Code

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

9.2 Profiles

Router can have virtually unlimited number of 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.

Configuration Profiles

Manage Profiles

Profile name

Profile name	Created	Action
first	2014-12-03	<input type="button" value="Apply"/> <input type="button" value="Delete"/>

9.3 Administration

9.3.1 General

General | Troubleshoot | Backup | Access Control | Diagnostics | MAC Clone | Overview | Monitoring

Administration Settings

Router Name And Host Name

Router name

Host name

Administrator Password

New password

Confirm new password

Language Settings

Language

IPv6 Support

Enable

Login Page

Show mobile info at login page

Show WAN IP at login page

Leds indication

Enable

Restore Default Settings

Restore to default

	Field name	Explanation
1.	Router name	Enter your new router name.
2.	Host name	Enter your new host name
3.	New Password	Enter your new administration password. 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 rounter
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

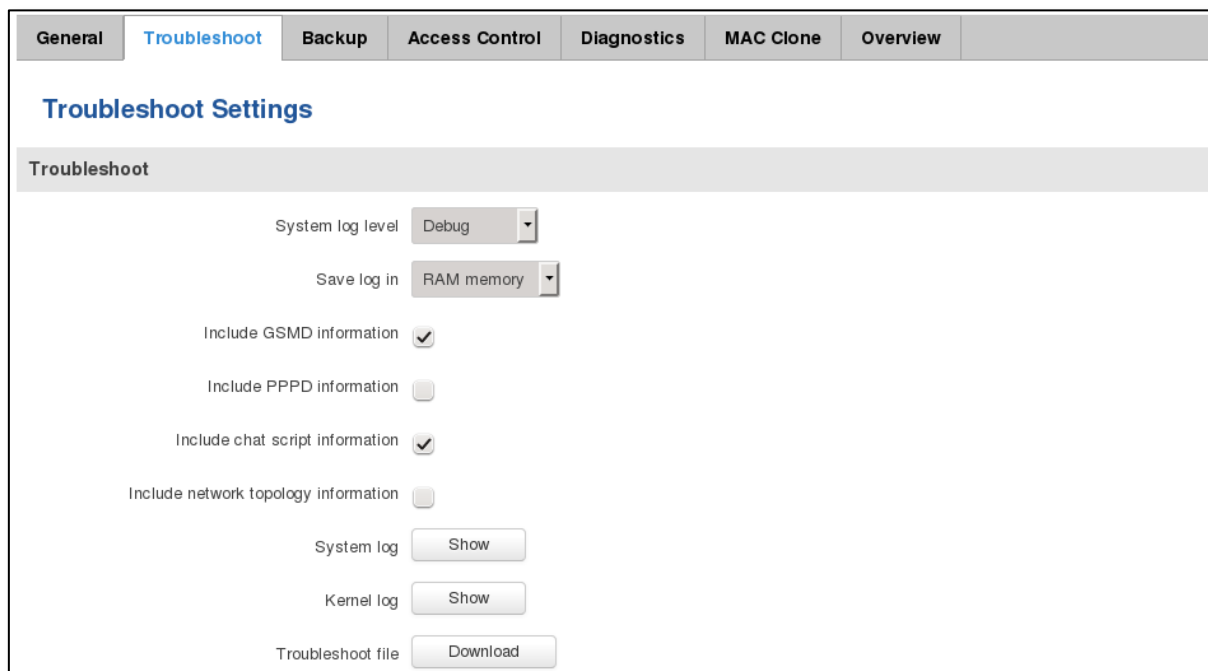
Important notes:

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 Troubleshoot



	Field name	Explanation
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 menu.
9.	Troubleshoot	Downloadable archive, that contains full router configuration and all System log files.

9.3.3 Backup

	Field name	Explanation
1.	Backup archive	Download current router settings file to personal computer. This file can be loaded to other RUT900 with same Firmware version in order to quickly configure it.
2.	Restore from backup	Select, upload and restore router settings file from personal computer.

9.3.3.1 Access Control General

	Field name	Explanation
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 CLI	Enables Command Line Interface
10.	Enable remote CLI	Enables remote Command Line Interface
11.	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”.

9.3.3.2 Access Control Safety

The screenshot shows the 'Access Control' configuration page. Under the 'Block Unwanted Access' section, there are two main areas: 'SSH Access Secure' and 'WebUI Access Secure'. Each area contains three settings: an 'Enable' checkbox (currently unchecked), a 'Clean after reboot' checkbox (unchecked), and a 'Fail count' input field (set to 5). Below these settings is a table titled 'List Of Blocked Addresses' with columns for 'Service' and 'Blocked address'. The table is currently empty, with a message below it stating 'There are no addresses blocked'.

	Field name	Explanation
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.	WebUIaccess secure enable	Check box to enable secure WebUIaccess.

9.3.4 Diagnostics

	Field name	Explanation
1.	Host	Enter server IP address or hostname.
2.	Ping	Utility used to test the reachability 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

	Field name	Explanation
1.	WAN MAC address	Enter new WAN MAC address.

9.3.6 Overview

General	Troubleshoot	Backup	Access Control	Diagnostics	MAC Clone	Overview	Monitoring
Overview Page Configuration							
Overview Tables							
			Mobile	<input checked="" type="checkbox"/>			
			SMS counter	<input type="checkbox"/>			
			System	<input checked="" type="checkbox"/>			
			Wireless	<input checked="" type="checkbox"/>			
			WAN	<input checked="" type="checkbox"/>			
			Local network	<input checked="" type="checkbox"/>			
			Access control	<input checked="" type="checkbox"/>			
			Recent system events	<input checked="" type="checkbox"/>			
			Recent network events	<input checked="" type="checkbox"/>			
			Teltonika_Router Hotspot	<input type="checkbox"/>			
			VRRP	<input type="checkbox"/>			
			Monitoring	<input type="checkbox"/>			

	Field name	Explanation
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.	<Hotspot name> Hotspot	Check box to show Hotspot instance table in Overview page
11.	VRRP	Check box to show VRRP table in Overview page
12.	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.

Remote Access Control	
Enable remote monitoring	<input type="checkbox"/>

Status	
Monitoring	Disabled
Router LAN MAC address	00:1E:42:00:00:00
Router serial number	00000001

	Field name	Explanation
1.	Enable remote monitoring	Enables the device to connect to remote monitoring system

9.4 User scripts

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

Backup script file

9.5 Safe mode

Router contains two firmware images in its internal flash memory. Master firmware image is the default one and is constantly used by the user. Another is safe mode firmware, which is the backup of the master firmware.

Safe mode firmware is similar to the master firmware, but in order to reduce its size, some functions like - Wireless Hotspot, VRRPD, SNMP, Web Filter are removed.

Safe mode firmware can be recognized from different logo and reduced menu in the WebUI. The sole purpose of safe mode firmware is to allow the user to update master firmware and in doing so to remove all previous configuration settings. To make safe mode useful it is strongly recommended to back up configuration of master firmware when the user is satisfied with the setup. After configuration backup is created it can be tested by requesting safe mode.

Safe Mode

Status

Safe mode FW version RUT9XX_SM_00.01.292

Safe mode config backup date 2015-05-12, 12:12:09

Safe Mode Configuration

Write configuration to config partition

Delete configuration from config partition

Request safemode after reboot

9.6 Firmware

9.6.1 Firmware

Firmware **FOTA**

Firmware

Current Firmware Information		Firmware Available On Server	
Firmware version	RUT9XX_R_00.01.299	Firmware version	RUT9XX_R_00.01.50
Firmware build date	2015-05-13, 11:26:59		
Kernel version	3.10.36		

Firmware Upgrade Settings

Keep all settings	<input type="checkbox"/>	Keep dynamic DNS settings	<input type="checkbox"/>
Keep network settings	<input type="checkbox"/>	Keep wireless settings	<input type="checkbox"/>
Keep mobile settings	<input type="checkbox"/>	Keep firewall settings	<input type="checkbox"/>
Keep LAN settings	<input type="checkbox"/>	Keep OpenVPN settings	<input type="checkbox"/>

Upgrade from file
Firmware image file No file selected.

Keep settings – if the check box is selected router will keep saved user configuration settings after firmware upgrade. When check box is not selected all router settings will be restored to factory defaults after firmware upgrade. When upgrading firmware, you can choose settings that you wish to keep after the upgrade. This function is useful when firmware is being upgraded via Internet (remotely) and you must not lose connection to the router afterwards.

FW image – router firmware upgrade file.

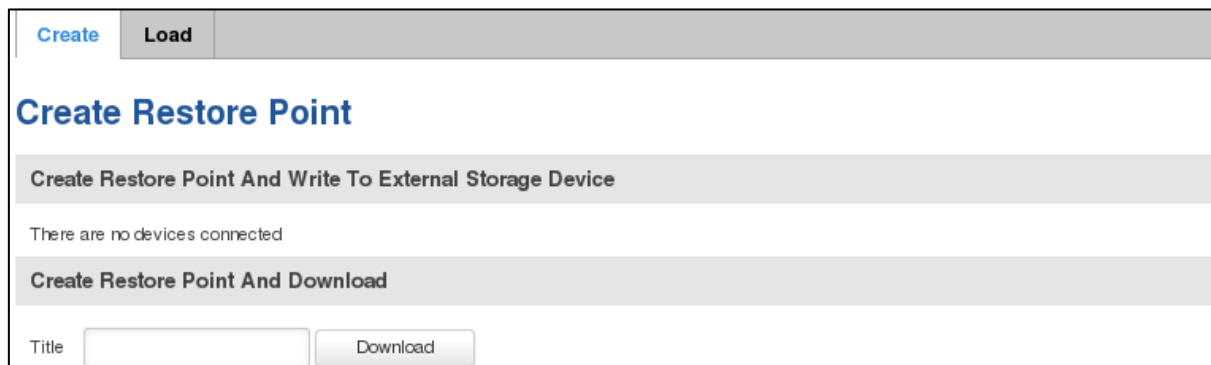
Warning: Never remove router power supply and do not press reset button during upgrade process! This would seriously damage your router and make it inaccessible. If you have any problems related to firmware upgrade you should always consult with local dealer.

9.6.2 FOTA

	Field name	Explanation
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).

9.7 Restore point

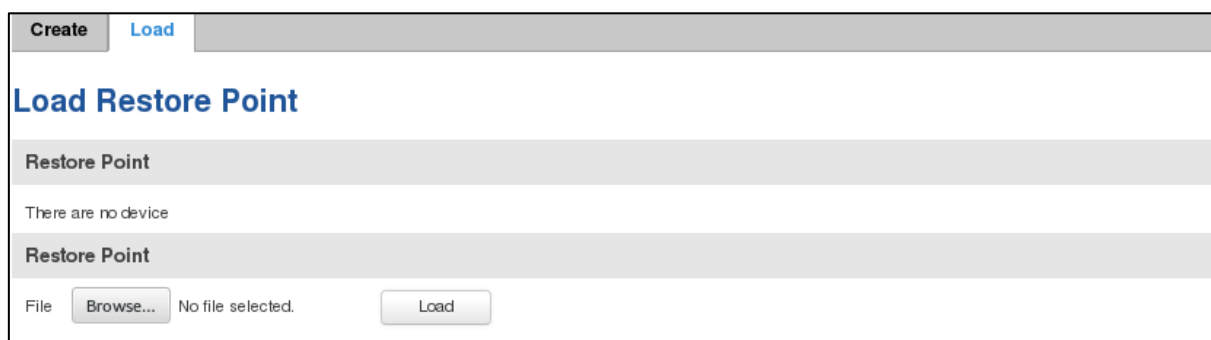
9.7.1 Restore point create



The screenshot shows a web interface with two tabs: 'Create' (active) and 'Load'. The main heading is 'Create Restore Point'. Below it, there are two sections: 'Create Restore Point And Write To External Storage Device' and 'Create Restore Point And Download'. The first section contains the text 'There are no devices connected'. The second section has a 'Title' input field and a 'Download' button.

Allows to create firmware restorepoints with all custom configurations. You can download created restore points to your computer

9.7.2 Restore point load



The screenshot shows a web interface with two tabs: 'Create' and 'Load' (active). The main heading is 'Load Restore Point'. Below it, there are two sections: 'Restore Point' and 'Restore Point'. The first section contains the text 'There are no device'. The second section has a 'File' label, a 'Browse...' button, the text 'No file selected.', and a 'Load' button.

Allows to restore configuration from previously saved restore point. You can upload restore point from your computer.

9.8 Reboot



The screenshot shows a web interface with the heading 'Router reboot'. Below it, there is a yellow warning bar with the text 'Warning! During reboot you will temporarily lose the connection.'. At the bottom, there is a 'Reboot' button.

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 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 indicate 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 Safemode

Router contains two firmware images in its internal flash memory. One is master firmware which is the default firmware on is constantly used by the user. Another is safemode firmware which plays the role of the backup to the master firmware.

Safemode firmware has most function of master firmware but in order to reduce its size Wireless Hotspot, VRRPD, SNMP and Web Filter function were removed. Safemode firmware can be recognized from different logo and reduced menu in the WebUI. The sole purpose of safemode firmware is to allow the user to update master firmware on the router and to reset all previous configuration changes while doing so. To make safemode useful it is strongly recommended to back up configuration of master firmware when the user is satisfied with the setup (described in **Klauda! Nerastas nuorodos šaltinis.** section). After configuration backup is created and it can be tested by requesting safemode.

10.3 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 neither master nor safemode 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:

<http://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 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 Resolver. A server that translates names such as www.google.it 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 "www.something.com" 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 Address Resolution Protocol, a network layer protocol used to convert an IP address into a physical address (called a *DLC address*), such as an Ethernet 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 enhanced 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 that uniquely identifies each node of a 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, allowing 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 network.

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.