TELTONIKA

USER MANUAL

RUT850 LTE Router

Legal notice

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

Attention

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

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

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

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

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

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

Table of Contents

SAFETY INFORMATION

In this document you will be introduced on how to use a RUT850 router safely. We suggest you to adhere to the following recommendations in order to avoid personal injuries and or property damage.

You have to be familiar with the safety requirements before using the device!

To avoid burning and voltage caused traumas, of the personnel working with the device, please follow these safety requirements.

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

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

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

⚠ Do not mount or service the device during a thunderstorm.

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

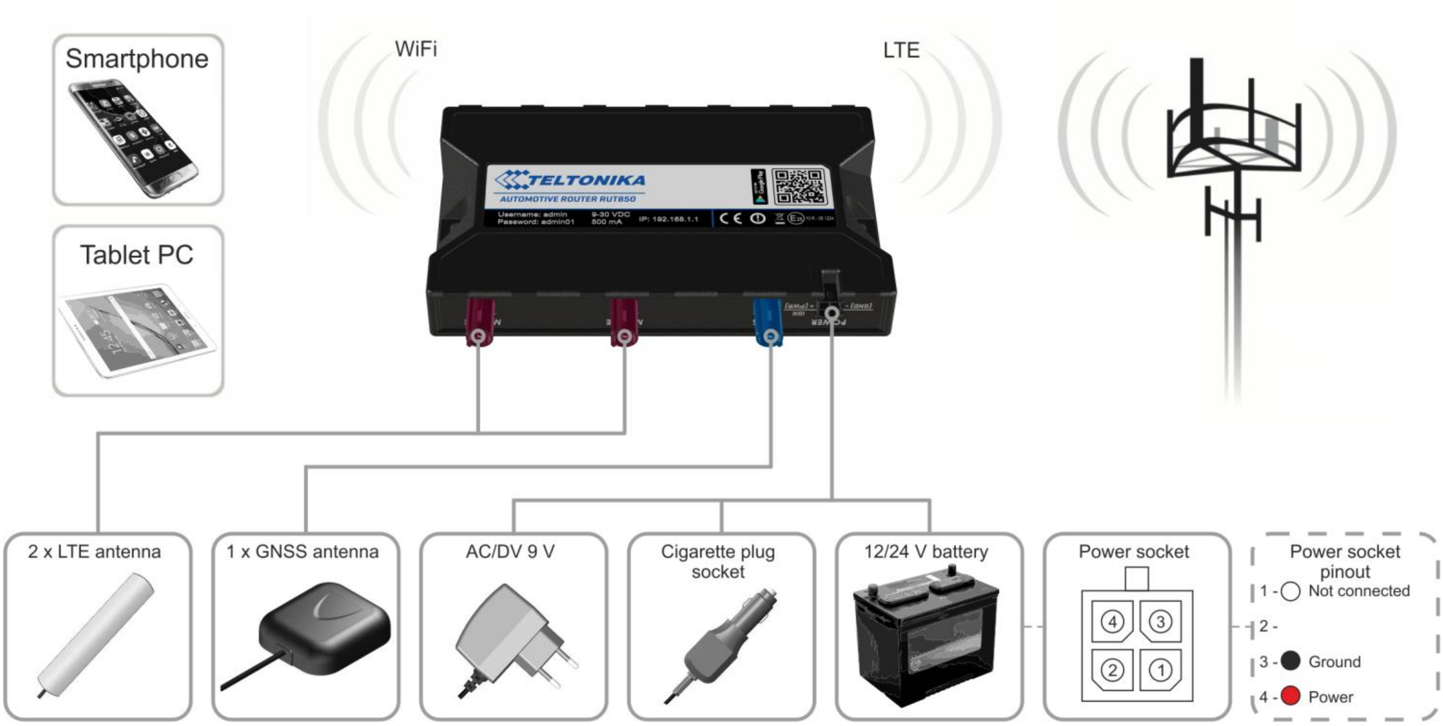
⚠ Protection in primary circuits of associated PC and PSU (LPS) against short circuits and earth faults of associated PC shall be provided as part of the building installation.

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

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

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

Device connection



1 Introduction

Thank you for purchasing a RUT850 LTE router!

RUT850 is compact mobile router with high speed wireless 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.

2 Specifications

2.1 Wi-Fi

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

2.2 Hardware

- LTE
- WiFi
- GNSS**
- 9 - 30 VDC
- Internal WiFi Antenna
- SIM Card Drawer

2.3 Electrical, Mechanical & Environmental

- Dimensions (H x W x D) 131mm x 79mm x 18mm
- Weight 110g
- Input voltage range 9 – 30VDC
- Overvoltage protection up to continuous 60 VDC
- Power consumption < 5W
- Operating temperature -40 °C to 75 °C
- Storage temperature -45 °C to 80 °C
- Operating humidity 10% to 90% Non-condensing
- Storage humidity 5% to 95% Non-condensing

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

***Versions without GNSS are available.*

2.4 Overvoltage protection

RUT850 has TVS diode in it's power input circuit, which protects device from overvoltage. TVS diode completely disconnects device from power if voltage exceeds 34V.

Maximum voltage, which TVS diode can handle is 60 VDC. Voltage up to 60V can be supplied to the router for unlimited amount of time without damaging the device. If voltage is higher than 60V, then it can only be supplied for up to 10us.

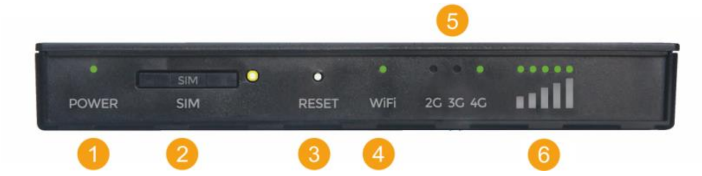
3 Setting up your router

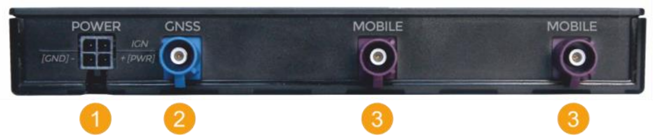
3.1 Installation

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.).

3.1.1 Front Panel and Back Panel





1	**Power led**
2	**SIM card holder**
3	**Reset button**
4	**WiFi status LED**
5	**Network type LEDs**
6	**Mobile signal strength indication LEDs**

1	**Power socket**
2	**LTE antenna connector**
3	**LTE antenna connector**

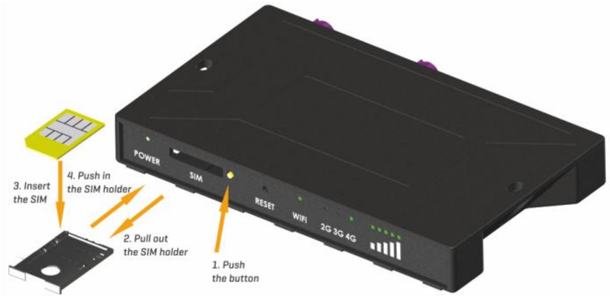
3.1.2 Connection status LED indication

Explanation of connection status LED indication:

1. Signal strength status LED’s constant blinking every 500 ms: router is turning on;
2. WiFi LED turned on/off: WiFI enabled/disabled;
3. 2G, 3G and 4G LED’s constant blinking every 1 sec: no SIM or bad PIN;
4. 2G/3G/4G LED’s blinking every 1 sec: connected 2G/3G/4G, but no data session established;
5. Blinking from 2G LED to 4G LED repeatedly: SIM holder not inserted;
6. 2G/3G/4G LED turned on: connected 2G/3G/4G with data session;
7. 2G/3G/4G LED blinking rapidly: connected 2G/3G/4G with data session and data is being transferred.

3.1.3 Hardware installation

1. Push SIM card holder button, pull out the SIM holder, then insert SIM card which was given by your ISP (Internet Service Provider) and push in the SIM holder. Correct SIM card orientation is shown in the picture.

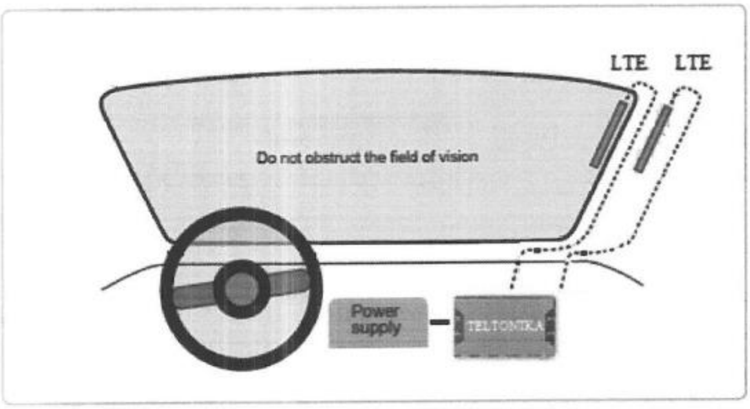


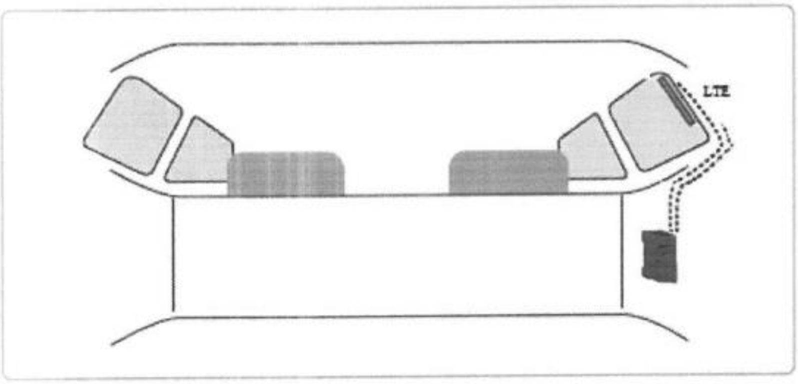
2. Attach LTE antennas.
3. Connect the power adapter to the socket on the front panel of the device. Then plug the other end of the power adapter into power source.
4. Connect to the device wirelessly (SSID: **rut850**).

3.1.4 Product installation

Mounting kit consist of 4 screws and double-side adhevise tape. Select a suitable surface and screw up or use double-side adhevise tape for attaching the product. See examples below:

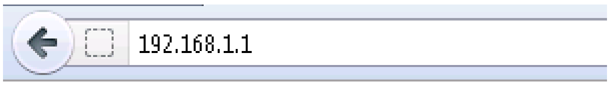
Here are couple examples of location for the installation places in vehicle:



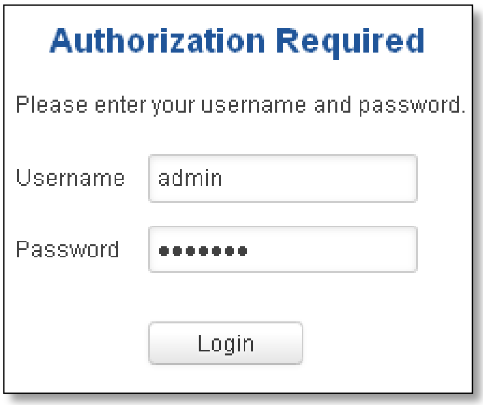


3.2 Logging in

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. Search wireless networks with your device. A list should pop up with all available wireless networks. Select "rut850" and click **connect**. Then we launch our favorite browser and enter the routers IP into the address field:


192.168.1.1

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


Authorization Required

Please enter your username and password.

Username: admin

Password: ●●●●●●●

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 RUT850!

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

4 Operation Modes

The RUT850 router supports various operation modes. It can be connected to the internet (WAN) via mobile or via a wireless network. When connecting to the internet, you may also backup your main WAN connection with backup connection. 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.

WAN	Main WAN	Backup WAN
Mobile	√	√
Wi-Fi	√	√

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

5 Powering the device from higher voltage

If you decide 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.

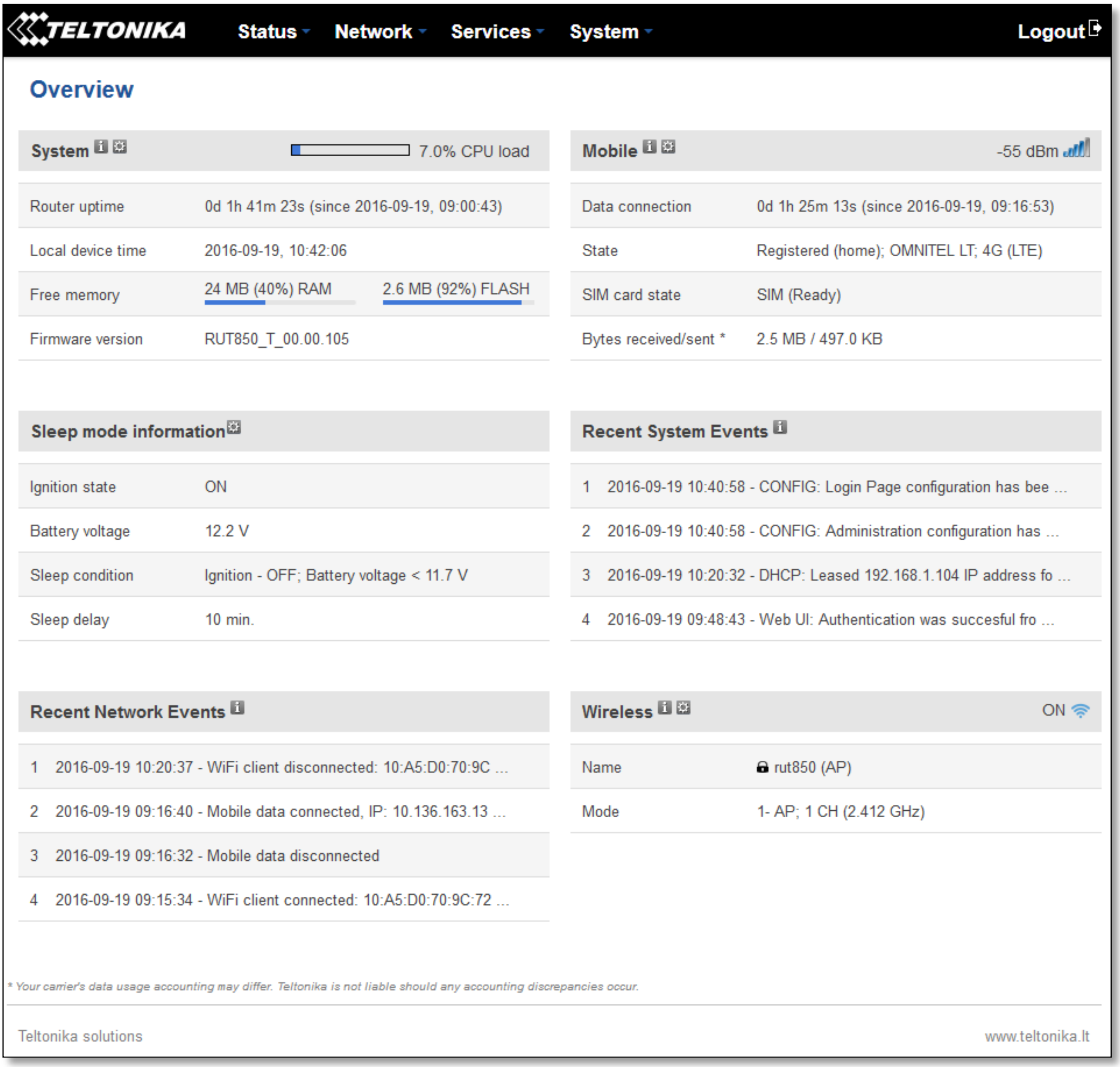
While the device is designed to accept input voltage of up to 30 VDC peaks from high voltage power supplies can harm the device. If you want to use high voltage power supplies it is recommended to also use additional safety equipment to suppress voltage peaks from power supply.

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 information summaries.



Overview

System — 7.0% CPU load

Router uptime	0d 1h 41m 23s (since 2016-09-19, 09:00:43)	
Local device time	2016-09-19, 10:42:06	
Free memory	24 MB (40%) RAM	2.6 MB (92%) FLASH
Firmware version	RUT850_T_00.00.105	

Mobile — -55 dBm

Data connection	0d 1h 25m 13s (since 2016-09-19, 09:16:53)
State	Registered (home); OMNITEL LT; 4G (LTE)
SIM card state	SIM (Ready)
Bytes received/sent *	2.5 MB / 497.0 KB

Sleep mode information

Ignition state	ON
Battery voltage	12.2 V
Sleep condition	Ignition - OFF; Battery voltage < 11.7 V
Sleep delay	10 min.

Recent System Events

```
1  2016-09-19 10:40:58 - CONFIG: Login Page configuration has bee ...
2  2016-09-19 10:40:58 - CONFIG: Administration configuration has ...
3  2016-09-19 10:20:32 - DHCP: Leased 192.168.1.104 IP address fo ...
4  2016-09-19 09:48:43 - Web UI: Authentication was succesful fro ...
```

Recent Network Events

```
1  2016-09-19 10:20:37 - WiFi client disconnected: 10:A5:D0:70:9C ...
2  2016-09-19 09:16:40 - Mobile data connected, IP: 10.136.163.13 ...
3  2016-09-19 09:16:32 - Mobile data disconnected
4  2016-09-19 09:15:34 - WiFi client connected: 10:A5:D0:70:9C:72 ...
```

Wireless — ON

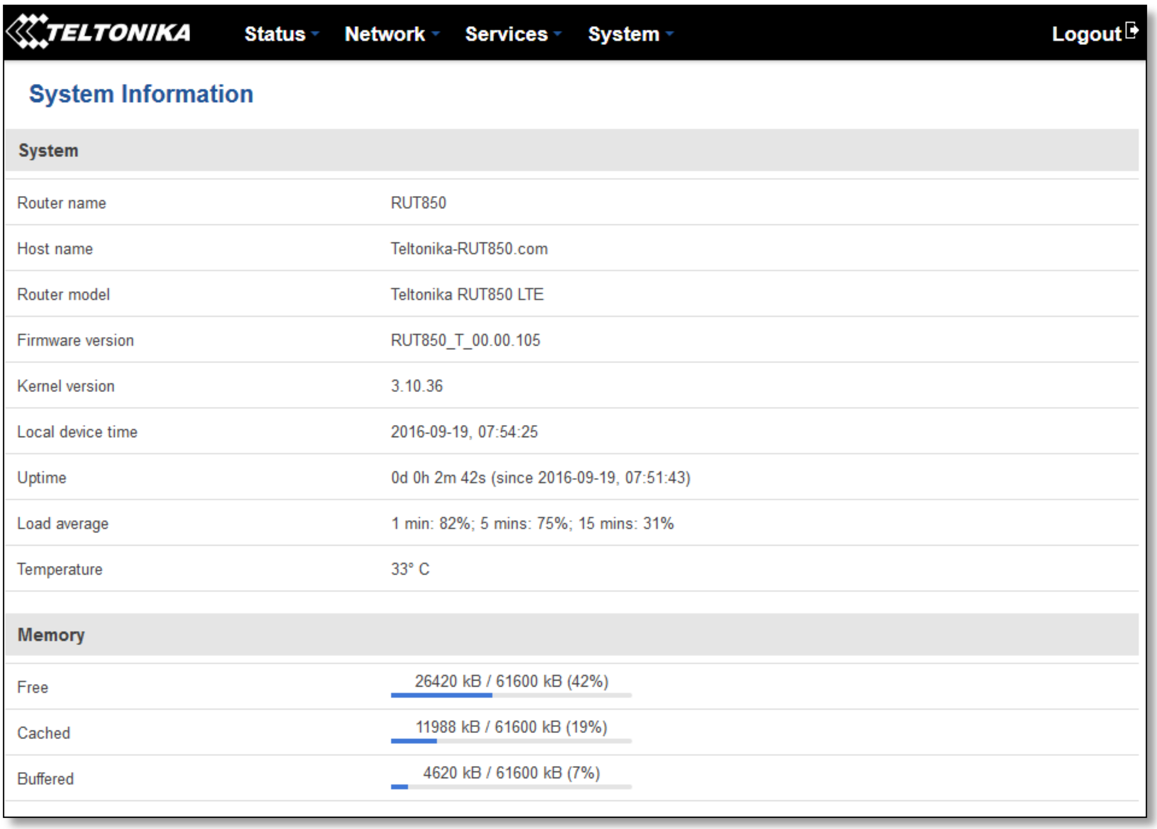
Name	🔒 rut850 (AP)
Mode	1- AP; 1 CH (2.412 GHz)

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

Teltonika solutions www.teltonika.lt

6.2 System Information

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



System Information

System

Router name	RUT850
Host name	Teltonika-RUT850.com
Router model	Teltonika RUT850 LTE
Firmware version	RUT850_T_00.00.105
Kernel version	3.10.36
Local device time	2016-09-19, 07:54:25
Uptime	0d 0h 2m 42s (since 2016-09-19, 07:51:43)
Load average	1 min: 82%; 5 mins: 75%; 15 mins: 31%
Temperature	33° C

Memory

Free	26420 kB / 61600 kB (42%)
Cached	11988 kB / 61600 kB (19%)
Buffered	4620 kB / 61600 kB (7%)

System explanation:

	Field Name	Sample value	Explanation
1.	Router Name	RUT850	Name of the router (hostname of the routers system). Can be changed in System -> Administration.
2.	Host name	Teltonika-RUT850.com	Indicates how router will be seen by other devices on the network. Can be changed in System -> Administration.
3.	Router Model	Teltonika RUT850 LTE	Routers model.
4.	Firmware Version	RUT850_T_00.00.105	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	2016-09-19, 07:55:46	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	0d 0h 4m 7s (since 2016-09-19, 07:51:43)	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: 93%; 5 mins: 79%; 15 mins: 37%	Indicates how busy the router is. Let's examine some sample output: "1 min: 22%, 5 mins: 13%, 15 mins: 20%". The first number mean past minute and second number 22% means that in the past minute there have been, on average, 22% processes running or waiting for a

			resource.
9.	Temperature	33˚ C	Device's temperature

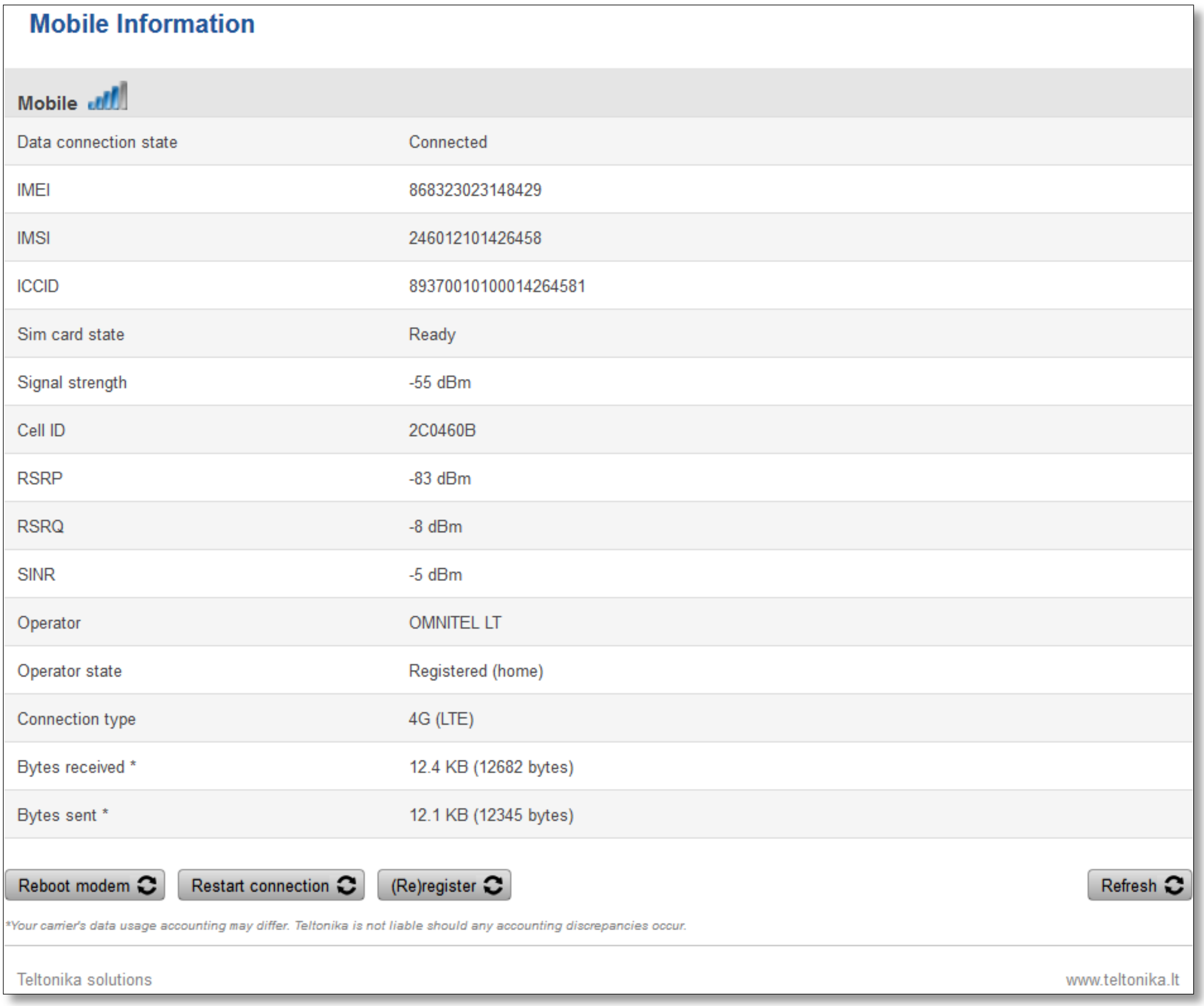
Memory explanation:

	Field Name	Sample Value	Explanation
1.	Free	26216 kB / 61600 kB (42%)	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	11988 kB / 61600 kB (19%)	The size of the area of memory that is dedicated to storing frequently accessed data.
3.	Buffered	4620 kB / 61600 kB (7%)	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

Display information about mobile modem connections.



Mobile Information

Mobile

Data connection state	Connected
IMEI	868323023148429
IMSI	246012101426458
ICCID	89370010100014264581
Sim card state	Ready
Signal strength	-55 dBm
Cell ID	2C0460B
RSRP	-83 dBm
RSRQ	-8 dBm
SINR	-5 dBm
Operator	OMNITEL LT
Operator state	Registered (home)
Connection type	4G (LTE)
Bytes received *	12.4 KB (12682 bytes)
Bytes sent *	12.1 KB (12345 bytes)

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

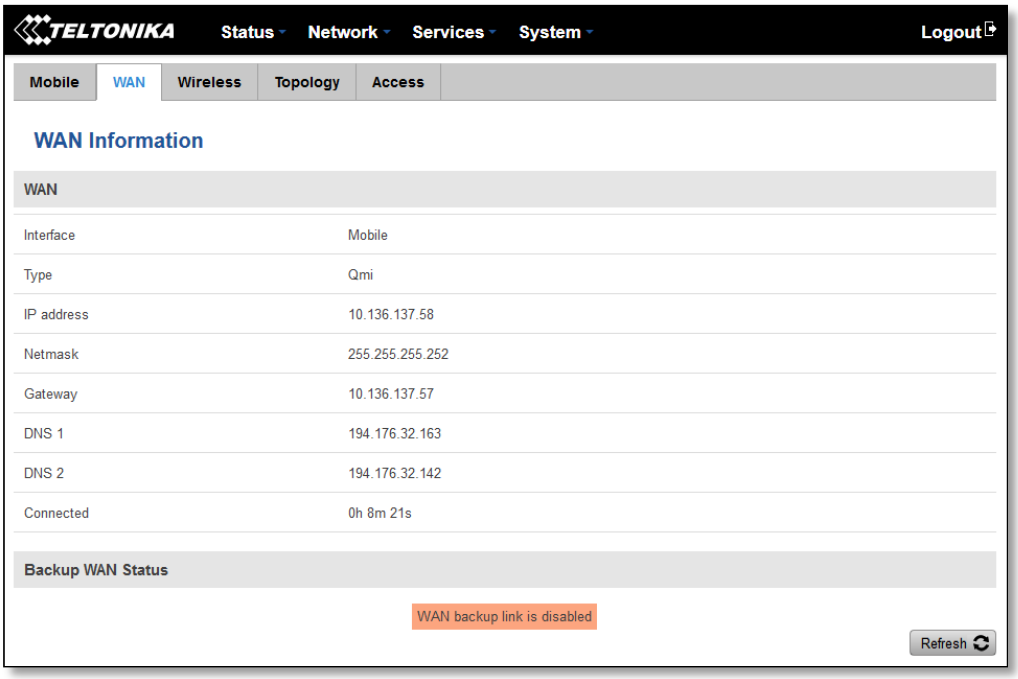
Teltonika solutions www.teltonika.lt

Mobile information:

	Field Name	Sample Value	Explanation
1.	Data connection state	Connected	Mobile data connection status
2.	IMEI	868323023148429	Modem's IMEI (International Mobile Equipment Identity) number
3.	IMSI	246012101426458	IMSI (International Mobile Subscriber Identity) is used to identify the user in a cellular network
3.	ICCID	89370010100014264581	Integrated Circuit Card ID
4.	SIM card state	Ready	Indicates the SIM card's state, e.g. PIN required, Not inserted, etc.
5.	Signal strength	-55 dBm	Received Signal Strength Indicator (RSSI). Signal's strength measured in dBm
6.	Cell ID	2C0460B	ID of operator cell that device is currently connected to
7.	RSRP	-83 dBm	Indicates the Reference Signal Received Power
8.	RSRQ	-8 dBm	Indicates the Reference Signal Received Quality
9.	SINR	-5 dBm	Indicates the Signal to Interference plus Noise Ratio
10.	Operator	OMNITEL LT	Operator's name of the connected GSM network
11.	Operator state	Registered (home)	GSM network's status
12.	Connection type	4G (LTE)	Indicates the GSM network's access technology
13.	Bytes received	12.4 KB (12682 bytes)	How many bytes were received via mobile data connection
14.	Bytes sent	12.1 KB (12345 bytes)	How many bytes were sent via mobile data connection

6.3.1.2 WAN

Display information about WAN connection.



WAN Information

WAN

Interface	Mobile
Type	Qmi
IP address	10.136.137.58
Netmask	255.255.255.252
Gateway	10.136.137.57
DNS 1	194.176.32.163
DNS 2	194.176.32.142
Connected	0h 8m 21s

Backup WAN Status

WAN backup link is disabled

WAN information:

	Field Name	Sample Value	Explanation
1.	Interface	Mobile	Specifies through what medium the router is connecting to the internet. This can either be Wired, Mobile or Wi-Fi.
2.	Type	Qmi	Specifies the type of connection. This can Static, DHCP, Qmi and etc.
3.	IP address	10.136.137.58	The IP address that the routers uses to connect the internet.
4.	WAN MAC**	00:11:22:33:44:55	WAN MAC address
5.	Netmask*	255.255.255.252	Specifies a mask used to define how large the WAN network is
5.	Gateway*	10.136.137.57	Indicates the default gateway, an address where traffic destined for the internet is routed to.
6.	DNS*	194.176.32.163	Domain name server(s).
7.	Connected*	0h 8m 21s	How long the connection has been successfully maintained.

*-These fields show up on other connection modes.

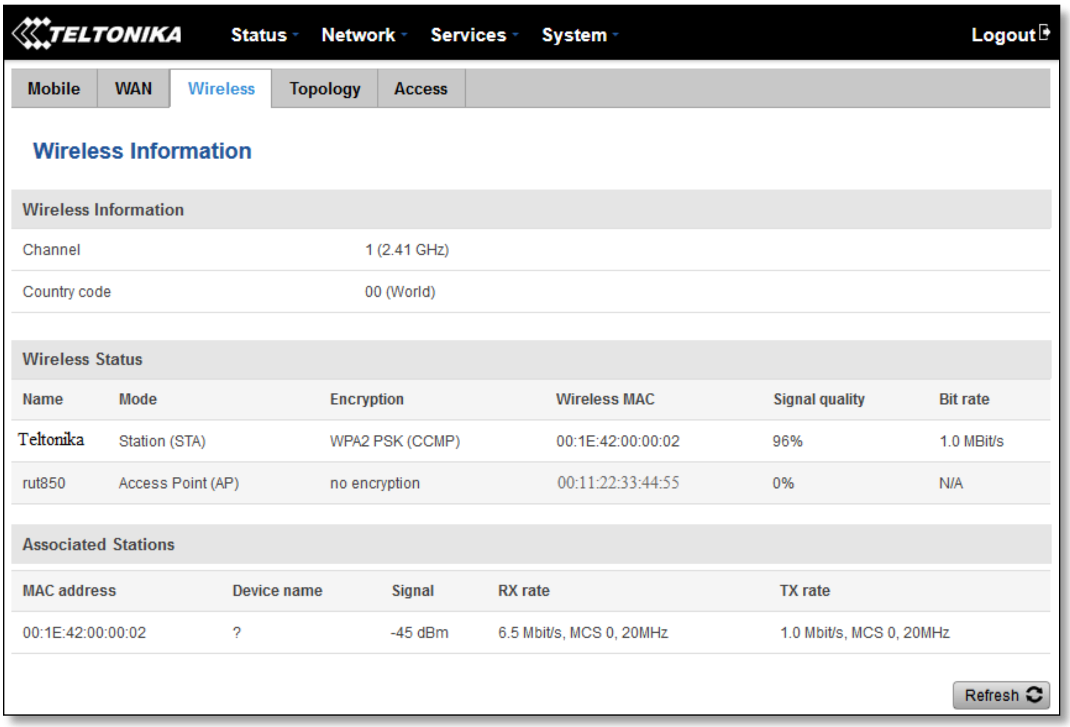
** - Exclusively to Modes with DHCP.

6.3.1.3 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.

6.3.1.3.1 Station

Display information about wireless connection (Station mode).



Wireless Information

Wireless Information

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

Wireless Status

Name	Mode	Encryption	Wireless MAC	Signal quality	Bit rate
Teltonika	Station (STA)	WPA2 PSK (CCMP)	00:1E:42:00:00:02	96%	1.0 MBit/s
rut850	Access Point (AP)	no encryption	00:11:22:33:44:55	0%	N/A

Associated Stations

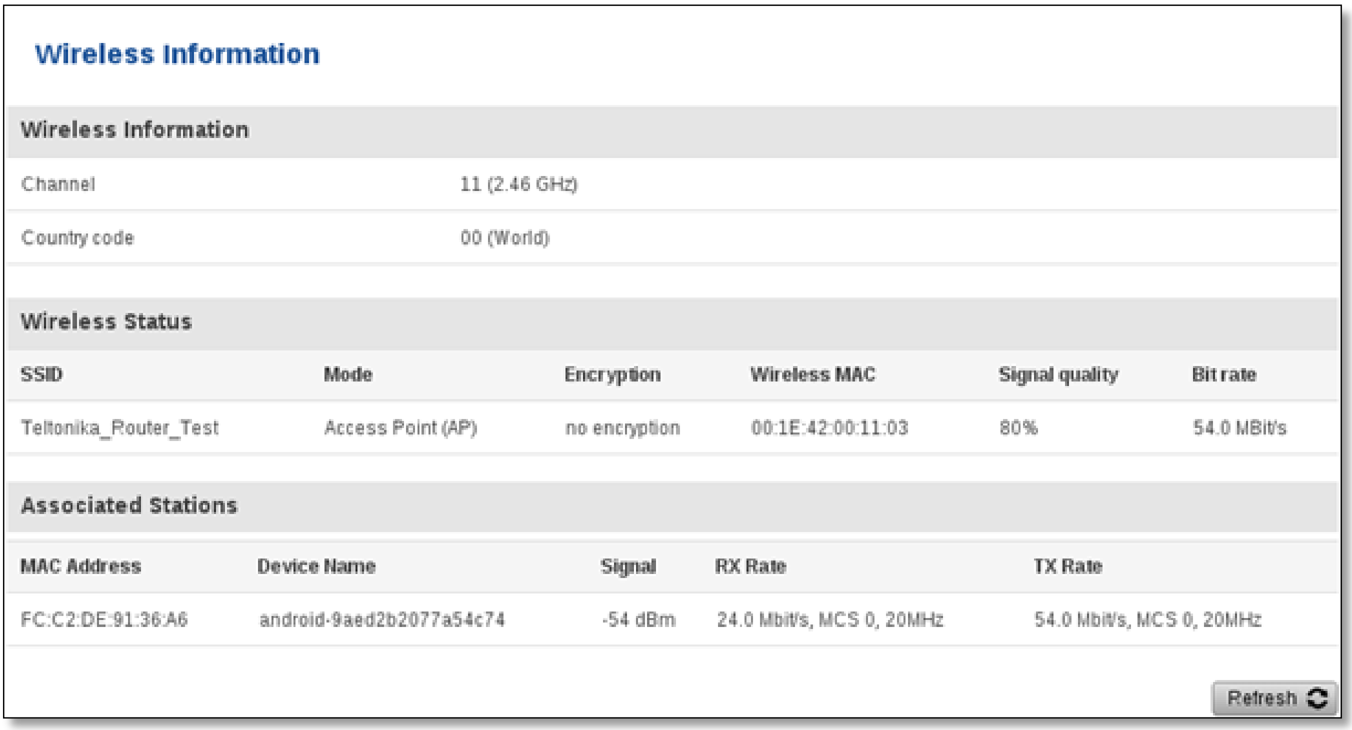
MAC address	Device name	Signal	RX rate	TX rate
00:1E:42:00:00:02	?	-45 dBm	6.5 Mbit/s, MCS 0, 20MHz	1.0 Mbit/s, MCS 0, 20MHz

Client mode information

	Field Name	Sample Value	Explanation
1.	Channel	1 (2.41 GHz)	The channel that the AP, to which the router is connected to, uses. Your wireless radio is forced to work in this channel in order to maintain the connection.
2.	Country code	00 (World)	Country code.
3.	SSID	Teltonika	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:42:00:00:02	The MAC address of the access points radio.
7.	Signal Quality	96%	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	1.0 MBit/s	The physical maximum possible throughput that the routers radio can handle. Keep in mind that this value is cumulative - The bit rate will be shared between the router and other possible devices that connect to the local AP.

6.3.1.3.2 Access Point

Display information about wireless connection (Access Point mode).



Wireless Information

Wireless Information

Channel	11 (2.46 GHz)
Country code	00 (World)

Wireless Status

SSID	Mode	Encryption	Wireless MAC	Signal quality	Bit rate
Teltonika_Router_Test	Access Point (AP)	no encryption	00:1E:42:00:11:03	80%	54.0 MBit/s

Associated Stations

MAC Address	Device Name	Signal	RX Rate	TX Rate
FC:C2:DE:91:36:A6	android-9aed2b2077a54c74	-54 dBm	24.0 Mbit/s, MCS 0, 20MHz	54.0 Mbit/s, MCS 0, 20MHz

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 bit rate will be shared between all devices that connect to the routers wireless network.

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

6.3.1.4 Associated Stations

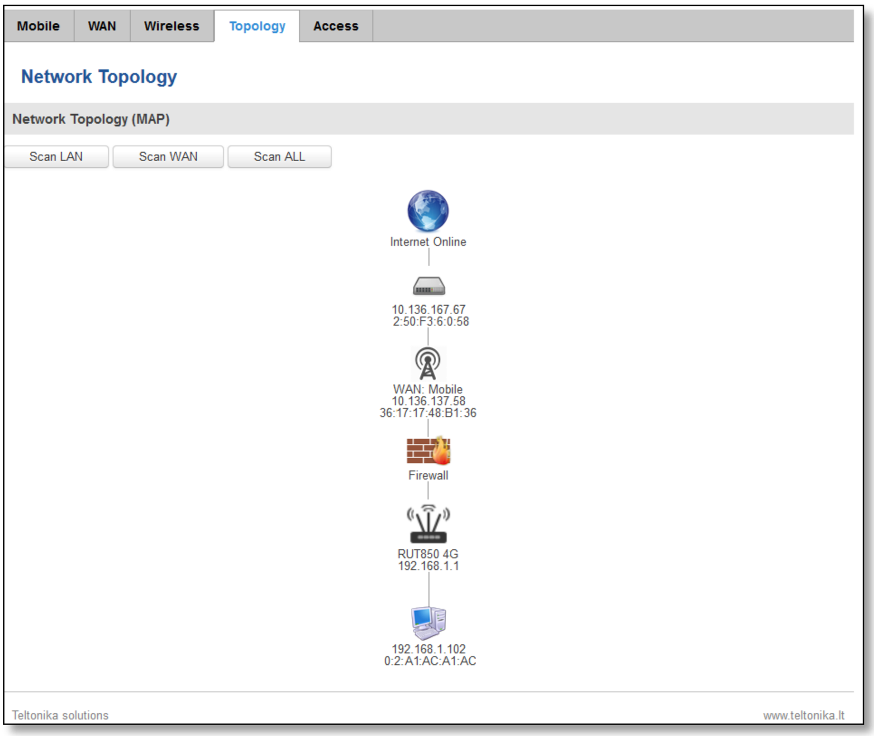
Outputs a list of all devices and their MAC addresses that are maintain a connection with your router right now.

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

	Field Name	Sample Value	Explanation
1.	MAC Address	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

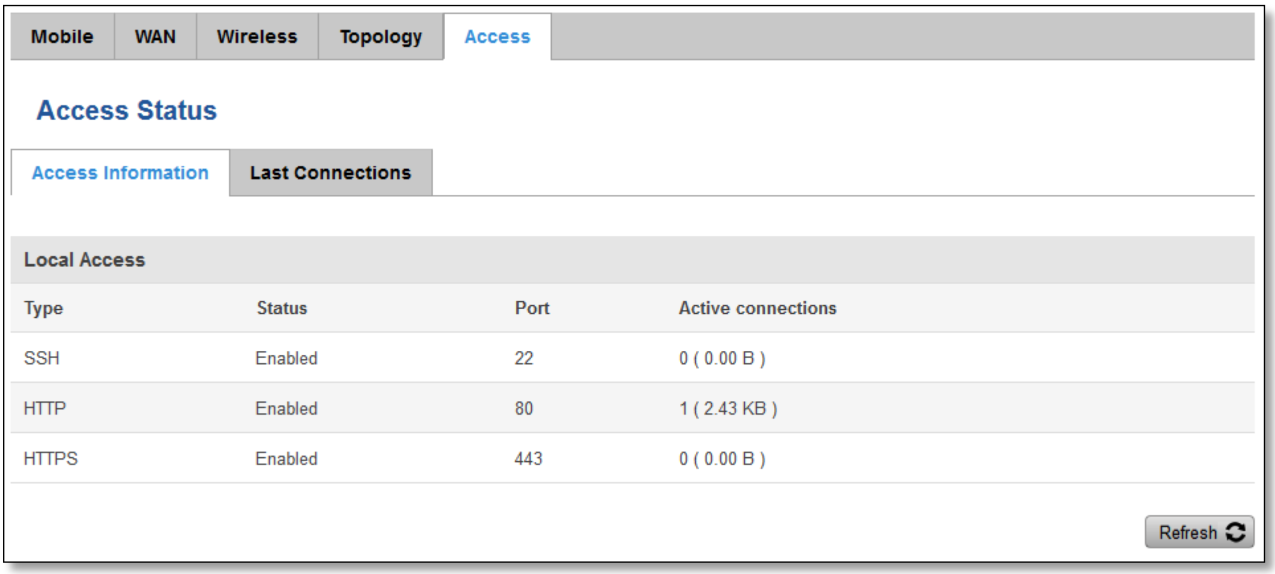
6.3.1.5 Topology

Network scanner allows you to quickly retrieve information about network devices. When router is configured to use Mobile as WAN and Connection type is selected „*PPP*“, then possible to scan only the LAN side.



6.3.1.6 Access

Display information about local and remote active connections status.



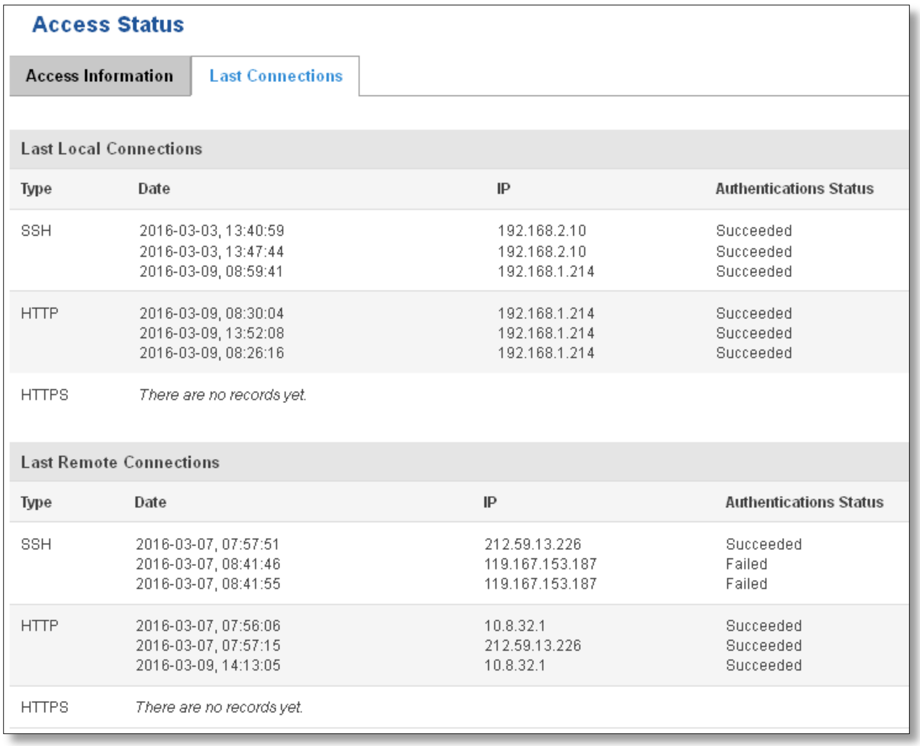
Type	Status	Port	Active connections
SSH	Enabled	22	0 (0.00 B)
HTTP	Enabled	80	1 (2.43 KB)
HTTPS	Enabled	443	0 (0.00 B)

	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.

6.3.1.6.1 Last Connections

Displays information about local and remote last 3 connections status



Last Local Connections

Type	Date	IP	Authentications Status
SSH	2016-03-03, 13:40:59 2016-03-03, 13:47:44 2016-03-09, 08:59:41	192.168.2.10 192.168.2.10 192.168.1.214	Succeeded Succeeded Succeeded
HTTP	2016-03-09, 08:30:04 2016-03-09, 13:52:08 2016-03-09, 08:26:16	192.168.1.214 192.168.1.214 192.168.1.214	Succeeded Succeeded Succeeded
HTTPS	*There are no records yet.*		

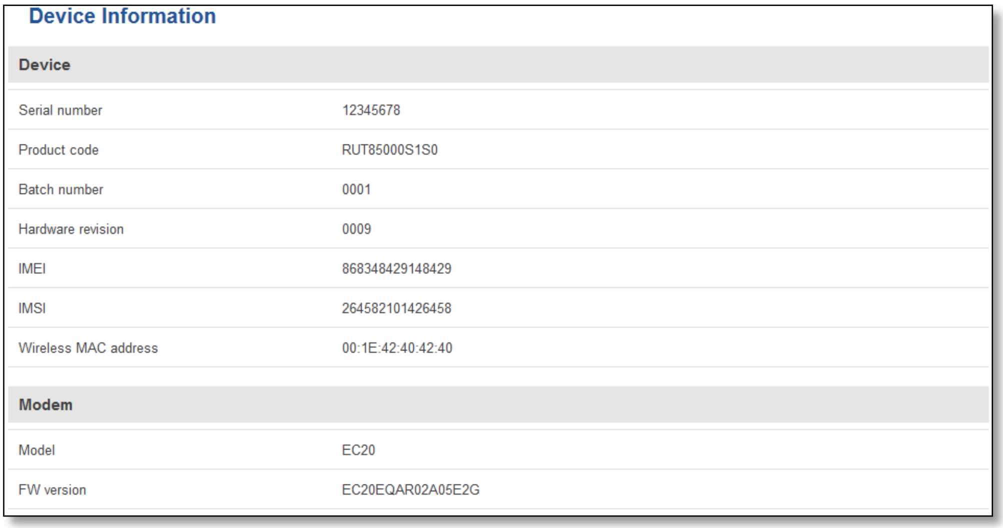
Last Remote Connections

Type	Date	IP	Authentications Status
SSH	2016-03-07, 07:57:51 2016-03-07, 08:41:46 2016-03-07, 08:41:55	212.59.13.226 119.167.153.187 119.167.153.187	Succeeded Failed Failed
HTTP	2016-03-07, 07:56:06 2016-03-07, 07:57:15 2016-03-09, 14:13:05	10.8.32.1 212.59.13.226 10.8.32.1	Succeeded Succeeded Succeeded
HTTPS	*There are no records yet.*		

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

6.4 Device information

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



Device

Serial number	12345678
Product code	RUT85000S1S0
Batch number	0001
Hardware revision	0009
IMEI	868348429148429
IMSI	264582101426458
Wireless MAC address	00:1E:42:40:42:40

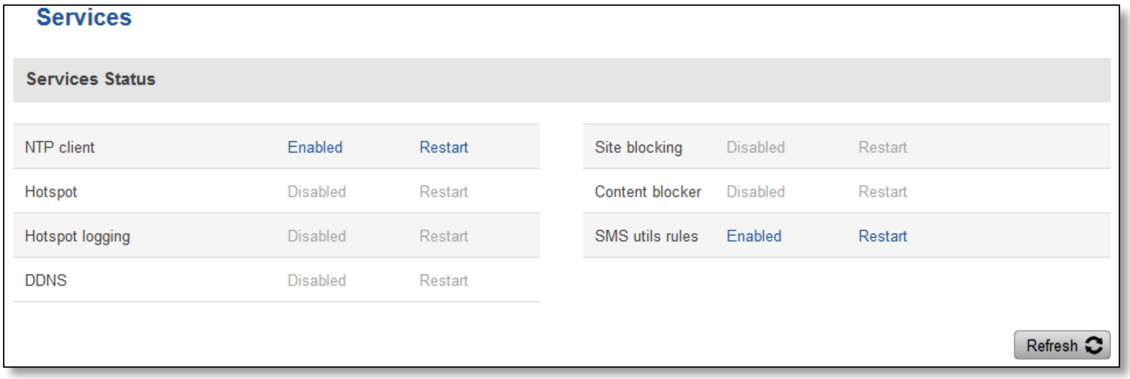
Modem

Model	EC20
FW version	EC20EQAR02A05E2G

	Field Name	Sample Value	Explanation
1.	Serial number	12345678	Serial number of the device
2.	Product code	RUT85000S1S0	Product code of the device
3.	Batch number	0001	Batch number used during device's manufacturing process
4.	Hardware revision	0009	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	00:1E:42:40:42:40	MAC address of the Wi-Fi interface
9.	Model	EC20	Router's modem model
10.	FW version	EC20EQAR02A05E2G	Router's modem firmware version

6.5 Services

The page displays usage of the available services.



Services

Services Status

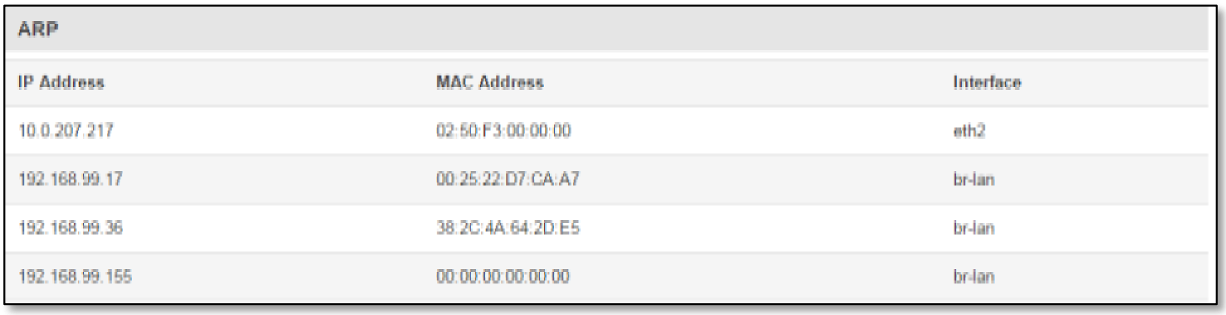
NTP client	Enabled	Restart	Site blocking	Disabled	Restart
Hotspot	Disabled	Restart	Content blocker	Disabled	Restart
Hotspot logging	Disabled	Restart	SMS utils rules	Enabled	Restart
DDNS	Disabled	Restart			

6.6 Routes

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

6.6.1 ARP

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



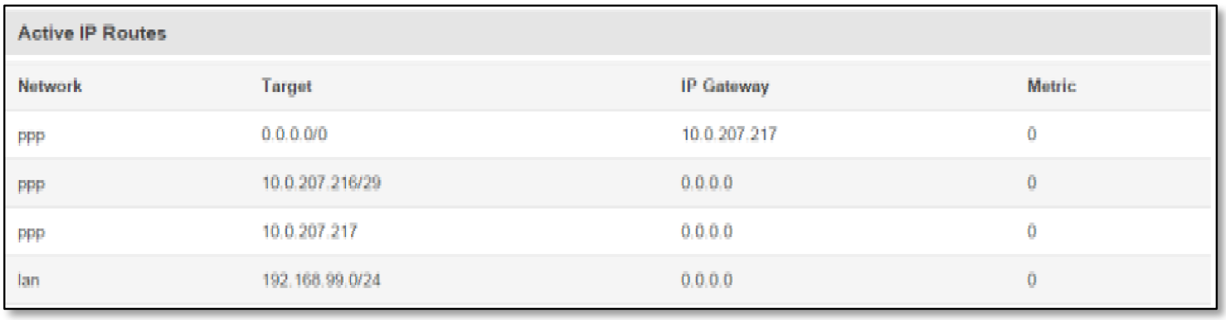
ARP

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 cashed 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

Show 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

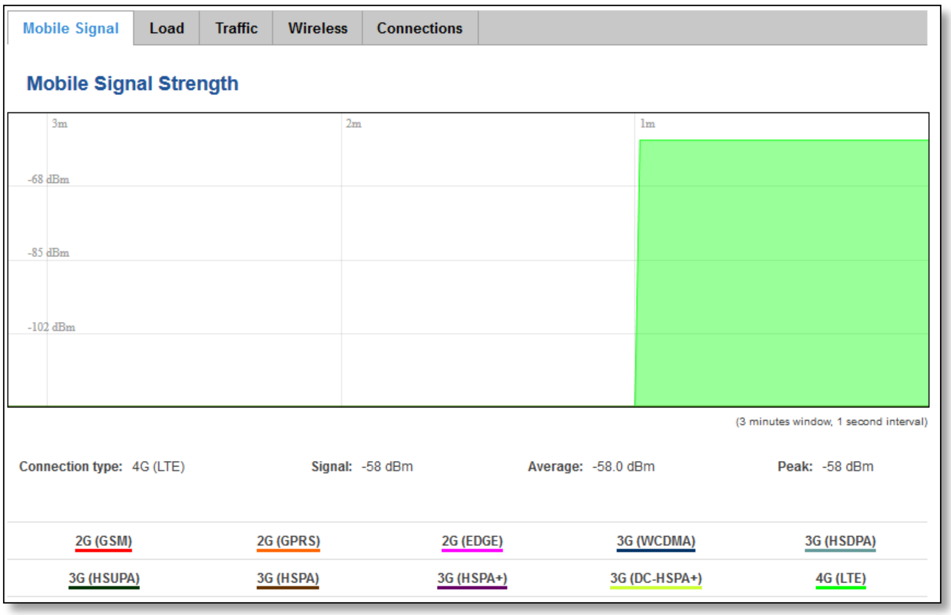
	Field Name	Sample Value	Explanation
1.	Network	ppp	Interface to be used to transmit TCP/IP packets through
2.	Target	192.168.99.0/24	Indicates where a TCP/IP packet, with a specific IP address, should be directed
3.	IP Gateway	0.0.0.0	Indicates through which gateway a TCP/IP packet should be directed
4.	Metric	0	Metric number indicating interface priority of usage

6.7 Graphs

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

6.7.1 Mobile Signal Strength

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



Mobile Signal Strength

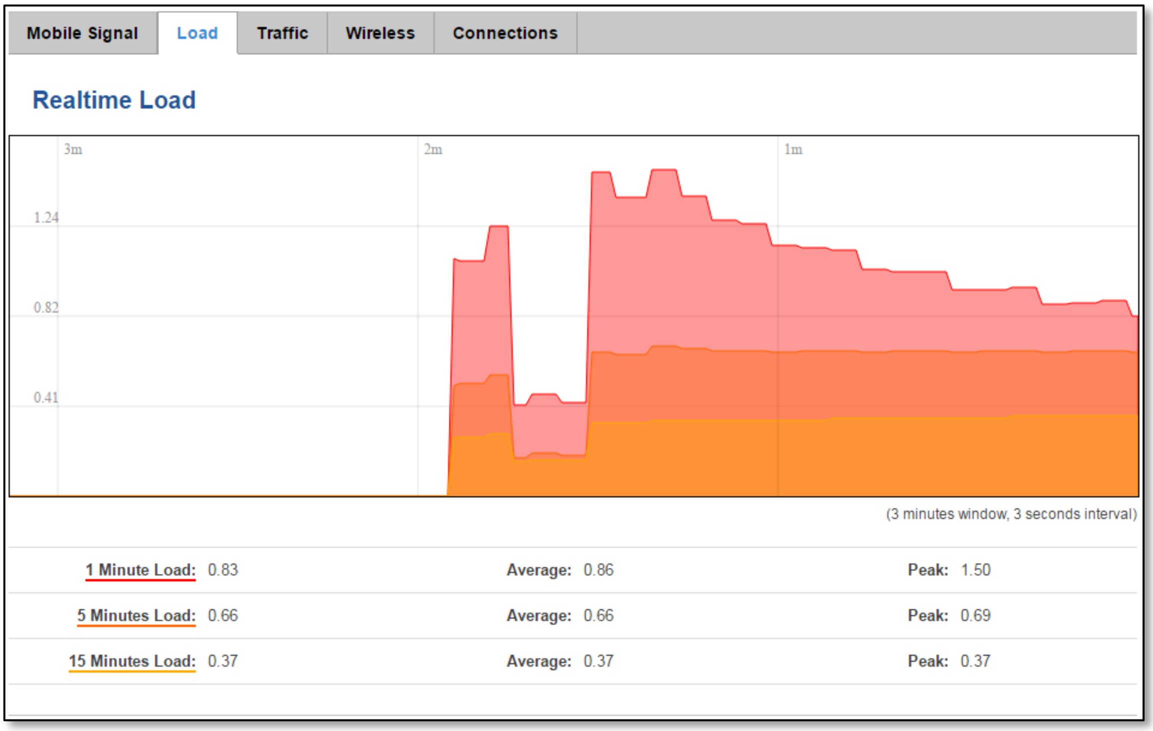
(3 minutes window, 1 second interval)

Connection type: 4G (LTE) Signal: -58 dBm Average: -58.0 dBm Peak: -58 dBm

	Field Name	Sample Value	Explanation
1.	Connection type	4G (LTE)	Type of mobile connection used
2.	Signal	-58 dBm	Current signal strength value
3.	Average	-58.0 dBm	Average signal strength value
4.	Peak	-58 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.



Realtime Load

(3 minutes window, 3 seconds interval)

1 Minute Load: 0.83 Average: 0.86 Peak: 1.50

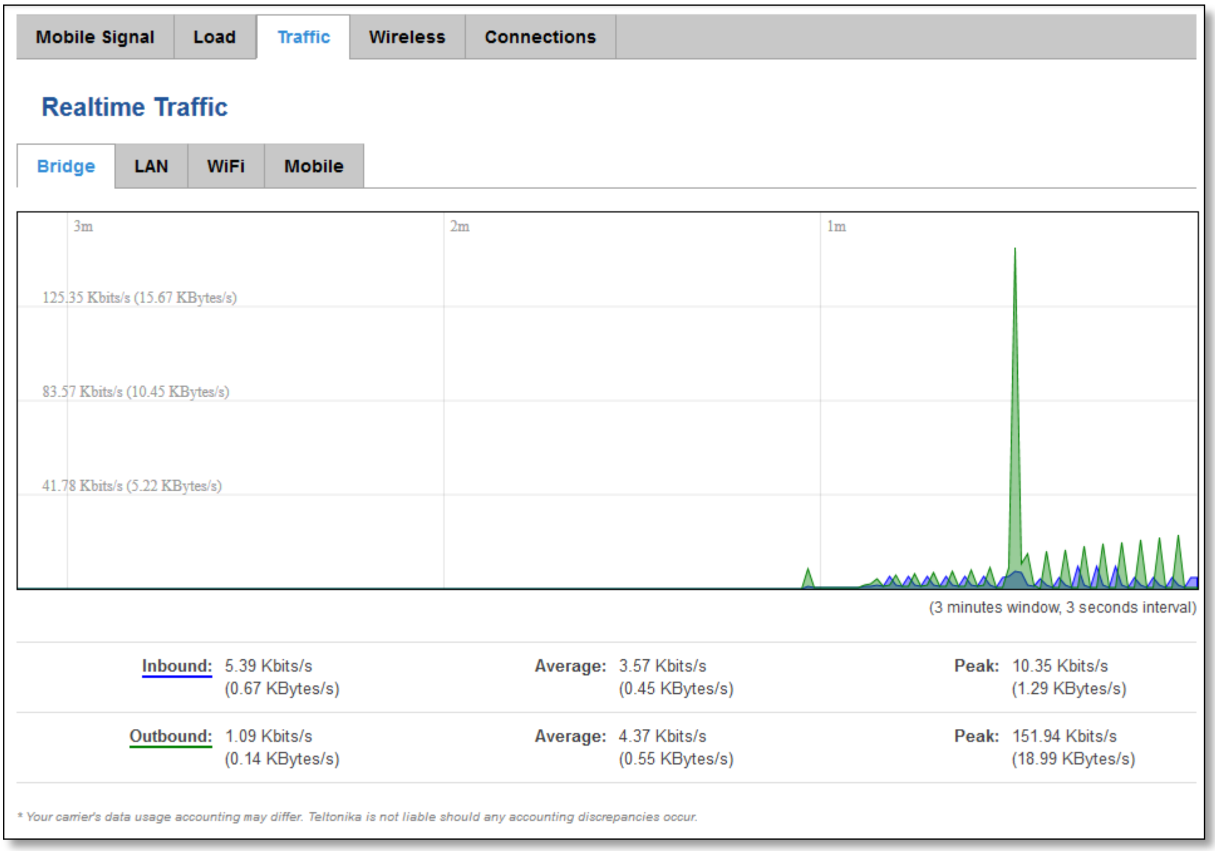
5 Minutes Load: 0.66 Average: 0.66 Peak: 0.69

15 Minutes Load: 0.37 Average: 0.37 Peak: 0.37

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

6.7.3 Realtime Traffic

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


Mobile Signal
Load
Traffic
Wireless
Connections
Realtime Traffic
Bridge
LAN
WiFi
Mobile
3m
2m
1m
125.35 Kbits/s (15.67 KBytes/s)
83.57 Kbits/s (10.45 KBytes/s)
41.78 Kbits/s (5.22 KBytes/s)
(3 minutes window, 3 seconds interval)

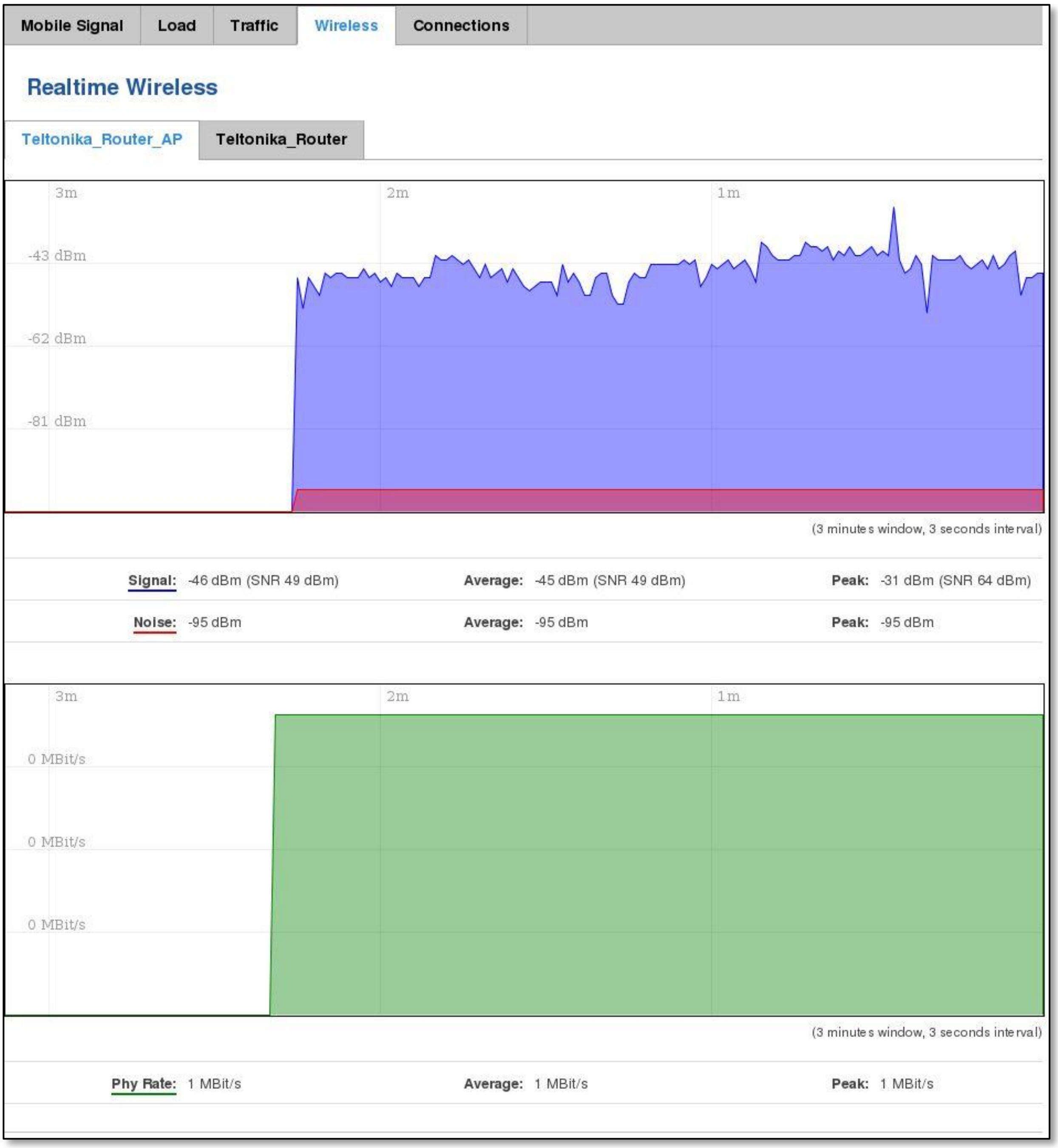
Inbound:	5.39 Kbits/s (0.67 KBytes/s)	Average:	3.57 Kbits/s (0.45 KBytes/s)	Peak:	10.35 Kbits/s (1.29 KBytes/s)
Outbound:	1.09 Kbits/s (0.14 KBytes/s)	Average:	4.37 Kbits/s (0.55 KBytes/s)	Peak:	151.94 Kbits/s (18.99 KBytes/s)

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

	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.
4.	Wi-Fi	Shows the amount of traffic that has been sent and received through the wireless radio.
5.	Mobile	Graphs the amount of traffic which passed through the mobile network connection.

6.7.4 Realtime Wireless

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



Realtime Wireless

(3 minutes window, 3 seconds interval)

Signal: -46 dBm (SNR 49 dBm) **Average:** -45 dBm (SNR 49 dBm) **Peak:** -31 dBm (SNR 64 dBm)

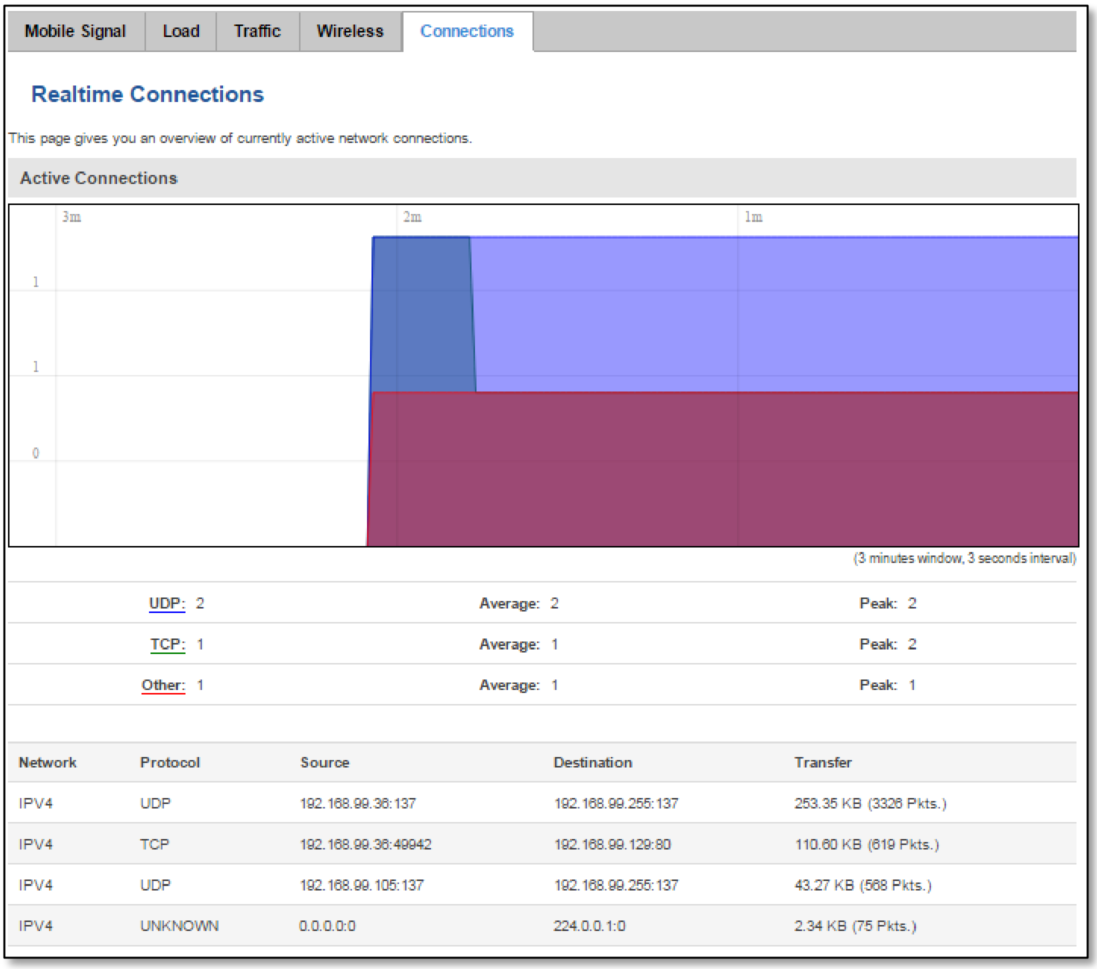
Noise: -95 dBm **Average:** -95 dBm **Peak:** -95 dBm

(3 minutes window, 3 seconds interval)

Phy Rate: 1 MBit/s **Average:** 1 MBit/s **Peak:** 1 MBit/s

6.7.5 Realtime Connections

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



Realtime Connections

This page gives you an overview of currently active network connections.

Active Connections

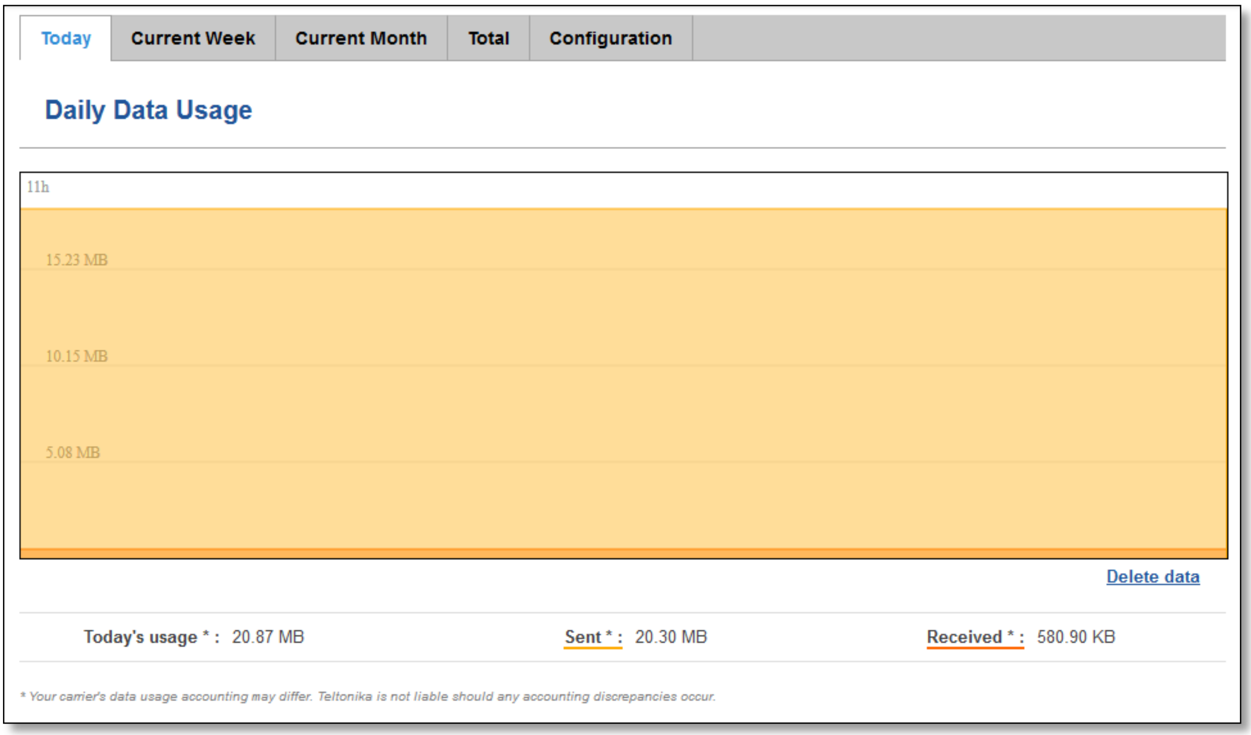
(3 minutes window, 3 seconds interval)

UDP: 2	Average: 2	Peak: 2
TCP: 1	Average: 1	Peak: 2
Other: 1	Average: 1	Peak: 1

Network	Protocol	Source	Destination	Transfer
IPV4	UDP	192.168.99.36:137	192.168.99.255:137	253.35 KB (3326 Pkts.)
IPV4	TCP	192.168.99.36:49942	192.168.99.129:80	110.60 KB (619 Pkts.)
IPV4	UDP	192.168.99.105:137	192.168.99.255:137	43.27 KB (568 Pkts.)
IPV4	UNKNOWN	0.0.0.0:0	224.0.0.1:0	2.34 KB (75 Pkts.)

6.8 Mobile Traffic

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



Daily Data Usage

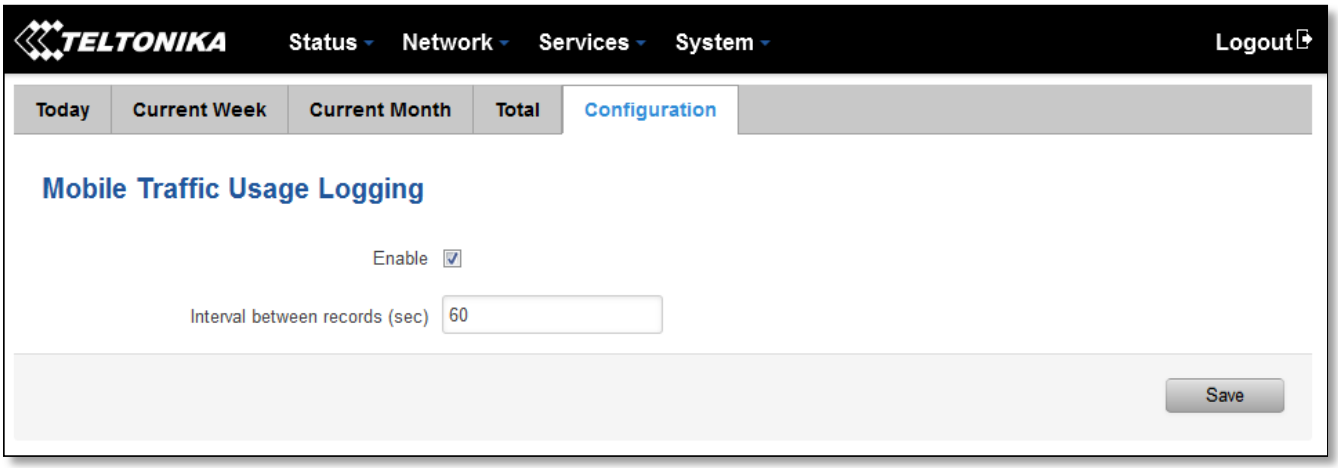
Today's usage * : 20.87 MB

Sent * : 20.30 MB

Received * : 580.90 KB

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

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



Mobile Traffic Usage Logging

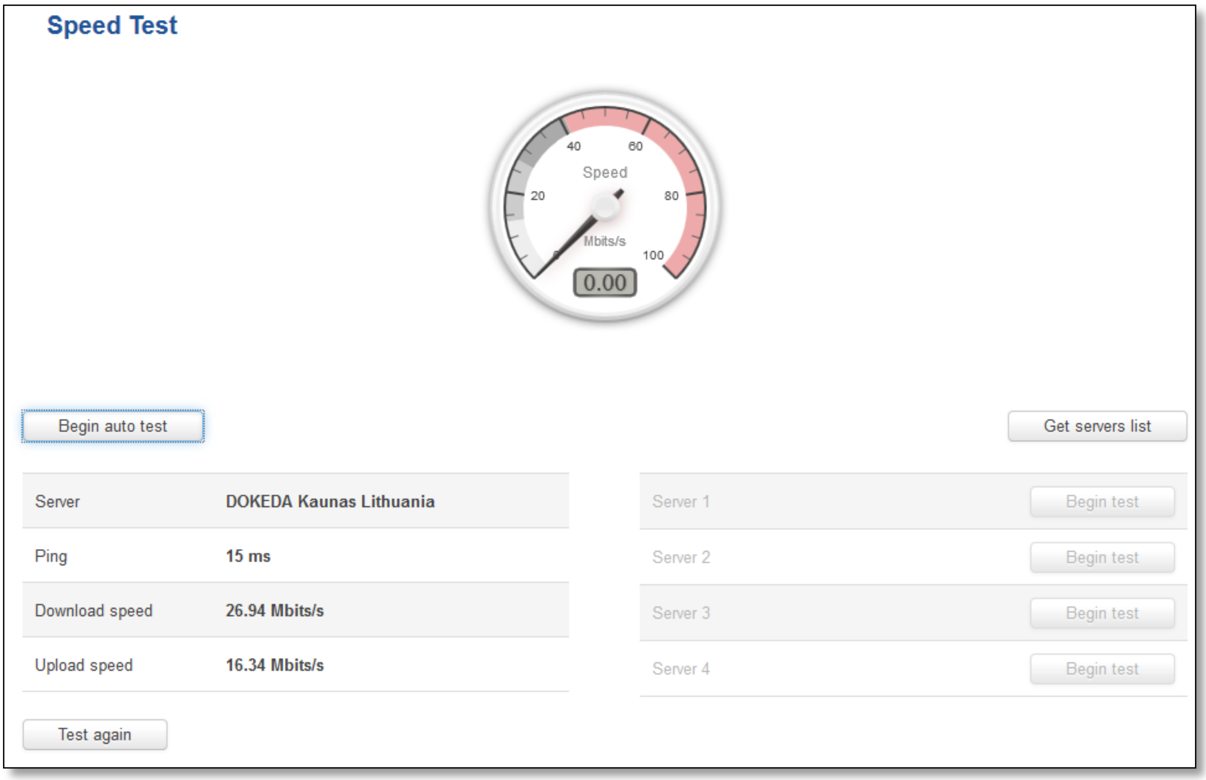
Enable ☑

Interval between records (sec) 60

	Field Name	Sample Value	Explanation
1.	Enable	Enable/Disable	Make a functionality active/inactive
2.	Interval between records (sec)	60	The interval between logging records (minimum 60 sec)

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.



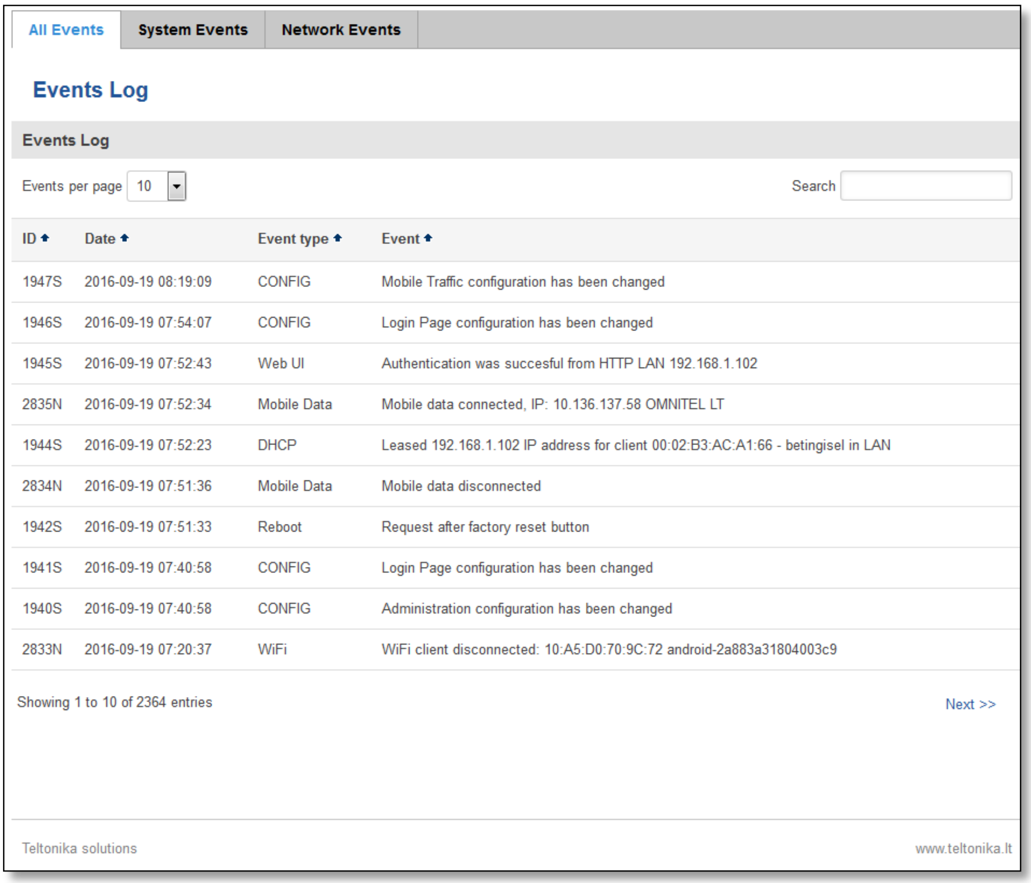
Server	DOKEDA Kaunas Lithuania
Ping	15 ms
Download speed	26.94 Mbits/s
Upload speed	16.34 Mbits/s

6.10 Events Log

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

6.10.1 All Events

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

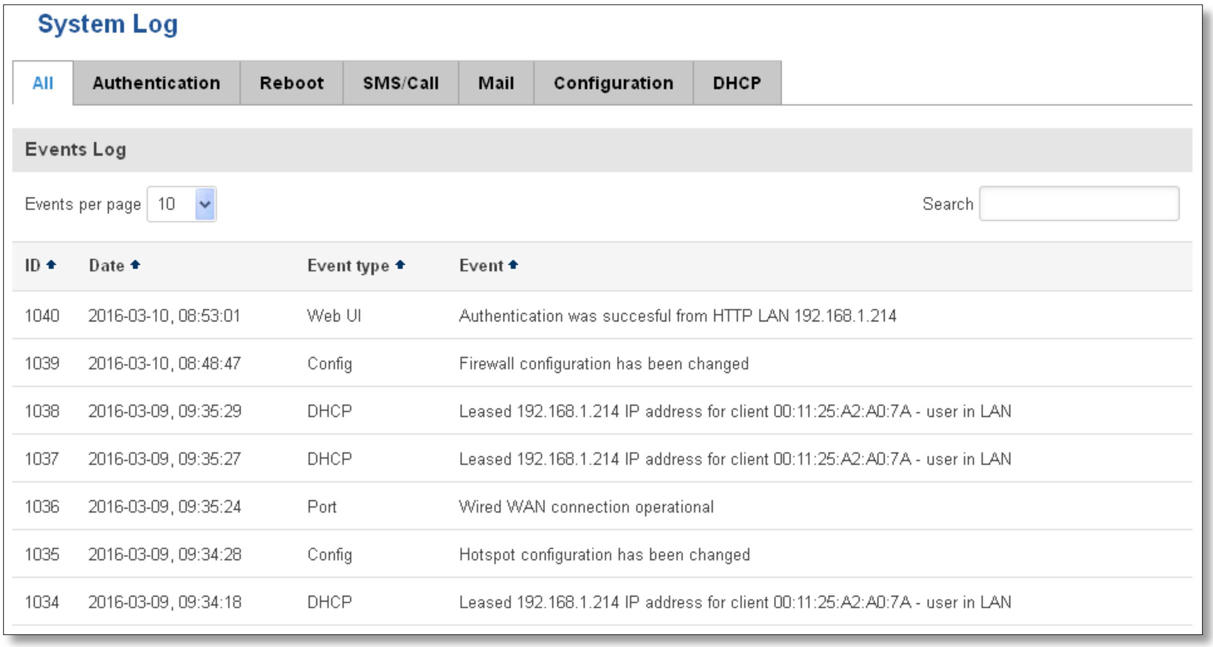


ID	Date	Event type	Event
1947S	2016-09-19 08:19:09	CONFIG	Mobile Traffic configuration has been changed
1946S	2016-09-19 07:54:07	CONFIG	Login Page configuration has been changed
1945S	2016-09-19 07:52:43	Web UI	Authentication was succesful from HTTP LAN 192.168.1.102
2835N	2016-09-19 07:52:34	Mobile Data	Mobile data connected, IP: 10.136.137.58 OMNITEL LT
1944S	2016-09-19 07:52:23	DHCP	Leased 192.168.1.102 IP address for client 00:02:B3:AC:A1:66 - betingisel in LAN
2834N	2016-09-19 07:51:36	Mobile Data	Mobile data disconnected
1942S	2016-09-19 07:51:33	Reboot	Request after factory reset button
1941S	2016-09-19 07:40:58	CONFIG	Login Page configuration has been changed
1940S	2016-09-19 07:40:58	CONFIG	Administration configuration has been changed
2833N	2016-09-19 07:20:37	WiFi	WiFi client disconnected: 10:A5:D0:70:9C:72 android-2a883a31804003c9

Showing 1 to 10 of 2364 entries

6.10.2 System Events

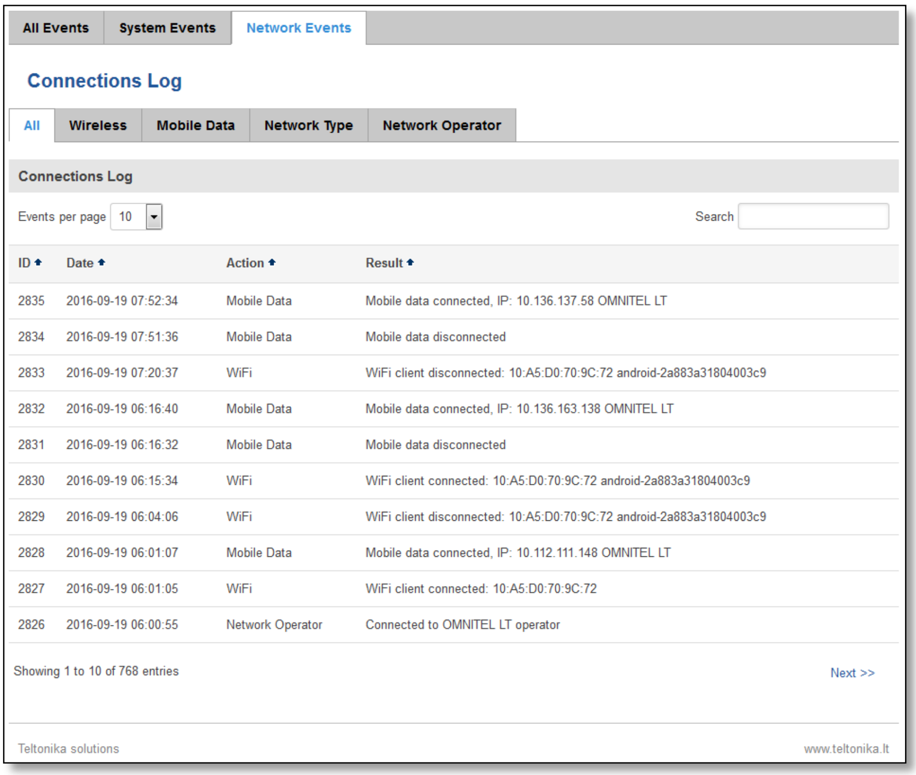
Display all system events, their type and time of occurrence. Events include authentication or reboot requests, incoming and outgoing SMS and calls, Mails, Configuration changes, DHCP events.



ID	Date	Event type	Event
1040	2016-03-10, 08:53:01	Web UI	Authentication was succesful from HTTP LAN 192.168.1.214
1039	2016-03-10, 08:48:47	Config	Firewall configuration has been changed
1038	2016-03-09, 09:35:29	DHCP	Leased 192.168.1.214 IP address for client 00:11:25:A2:A0:7A - user in LAN
1037	2016-03-09, 09:35:27	DHCP	Leased 192.168.1.214 IP address for client 00:11:25:A2:A0:7A - user in LAN
1036	2016-03-09, 09:35:24	Port	Wired WAN connection operational
1035	2016-03-09, 09:34:28	Config	Hotspot configuration has been changed
1034	2016-03-09, 09:34:18	DHCP	Leased 192.168.1.214 IP address for client 00:11:25:A2:A0:7A - user in LAN

6.10.3 Network Events

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



ID	Date	Action	Result
2835	2016-09-19 07:52:34	Mobile Data	Mobile data connected, IP: 10.136.137.58 OMNITEL LT
2834	2016-09-19 07:51:36	Mobile Data	Mobile data disconnected
2833	2016-09-19 07:20:37	WiFi	WiFi client disconnected: 10:A5:D0:70:9C:72 android-2a883a31804003c9
2832	2016-09-19 06:16:40	Mobile Data	Mobile data connected, IP: 10.136.163.138 OMNITEL LT
2831	2016-09-19 06:16:32	Mobile Data	Mobile data disconnected
2830	2016-09-19 06:15:34	WiFi	WiFi client connected: 10:A5:D0:70:9C:72 android-2a883a31804003c9
2829	2016-09-19 06:04:06	WiFi	WiFi client disconnected: 10:A5:D0:70:9C:72 android-2a883a31804003c9
2828	2016-09-19 06:01:07	Mobile Data	Mobile data connected, IP: 10.112.111.148 OMNITEL LT
2827	2016-09-19 06:01:05	WiFi	WiFi client connected: 10:A5:D0:70:9C:72
2826	2016-09-19 06:00:55	Network Operator	Connected to OMNITEL LT operator

Showing 1 to 10 of 768 entries

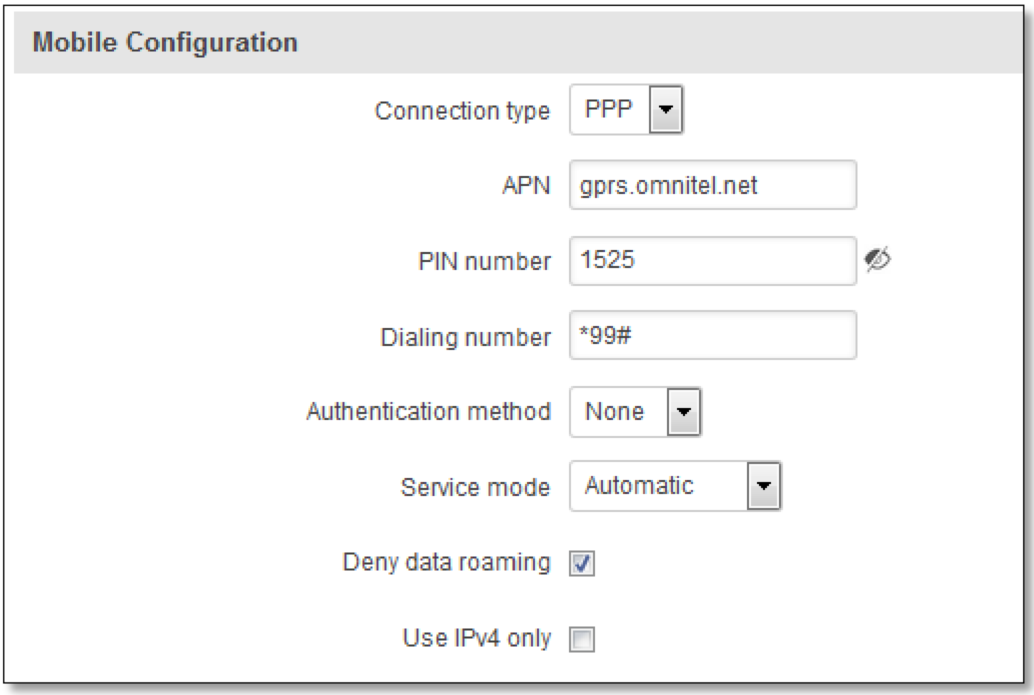
7 Network

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

Connection type: PPP

APN: gprs.omnitel.net

PIN number: 1525

Dialing number: *99#

Authentication method: None

Service mode: Automatic

Deny data roaming ☑

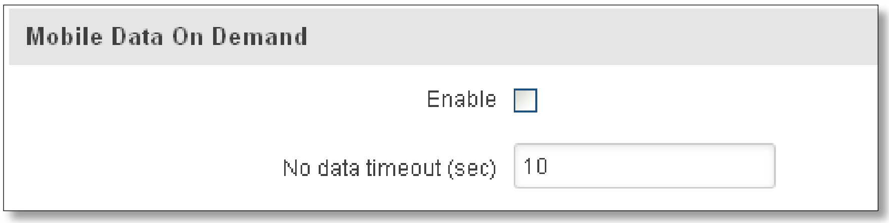
Use IPv4 only □

	Field Name	Sample value	Explanation
1.	Connection type	PPP / QMI	PPP mode uses dialling number to establish data connection. QMI mode (default) does not use dialling and PPP protocol to establish data connection it is usually faster than PPP mode.
2.	APN	gprs.omnitel.net	**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#	Dialling number is used to establish a mobile PPP (Point-to-Point-Protocol) connection.
6.	Authentication method	CHAP, PAP or none	Authentication method, which your carrier uses to authenticate new connections. (This selection is unavailable on the alternate model)
7.	Username	"username"	Your username that you would use to connect to your 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, 3G only, 4G (LTE) only 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 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



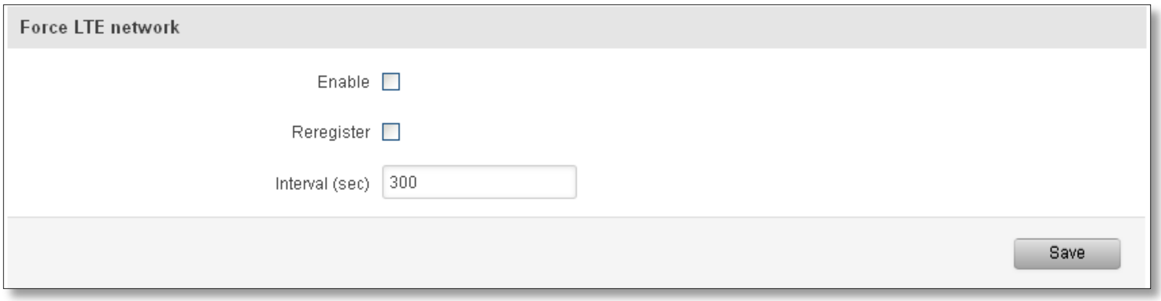
Mobile Data On Demand

Enable ☐

No data timeout (sec) 10

	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 ☐

Reregister ☐

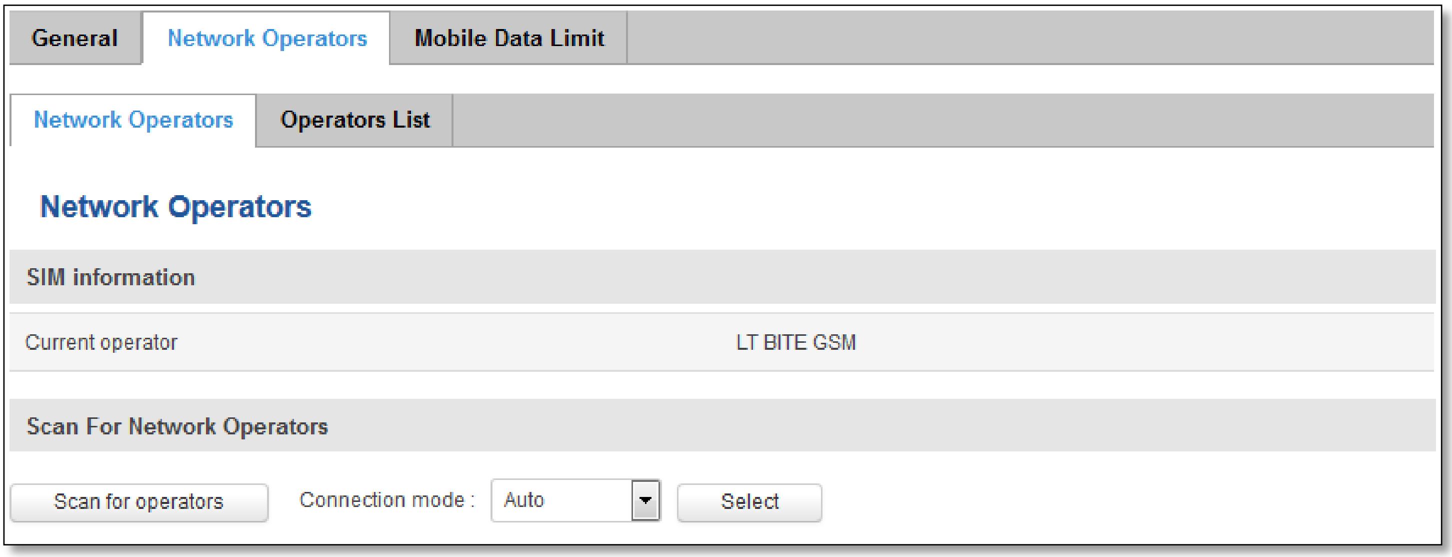
Interval (sec) 300

	Field name	Possible values	Explanation
1.	Enable	Enable/Disable	Enable/disable try to connect to LTE network every x seconds (used only if service mode is set to 4G (LTE) preferred)
2.	Reregister	Enable/Disable	If this enabled, modem will be reregister before try to connect to LTE network
3.	Interval (sec)	180 - 3600	Time in seconds between tries to connect to LTE network. Range [180-3600]

7.1.2 Network Operators

7.1.2.1 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.



Network Operators

SIM information

Current operator LT BITE GSM

Scan For Network Operators

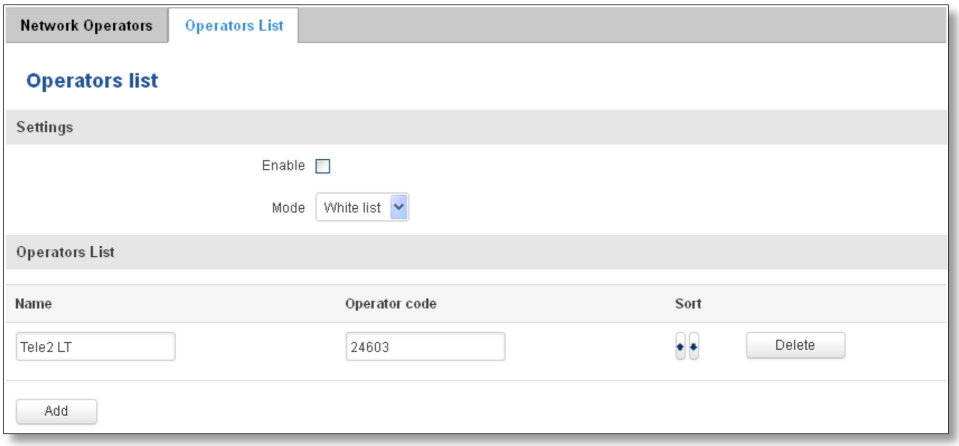
Connection mode : Auto

	Field Name	Sample Value	Explanation
2.	Current operator	LT BITE GSM	Operator's name of the connected GSM network

Note: after clicking Scan for operators' 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.

7.1.2.2 Operator List

This function lets to create white list/black list based on operator's code.



Operators list

Settings

Enable □

Mode White list

Operators List

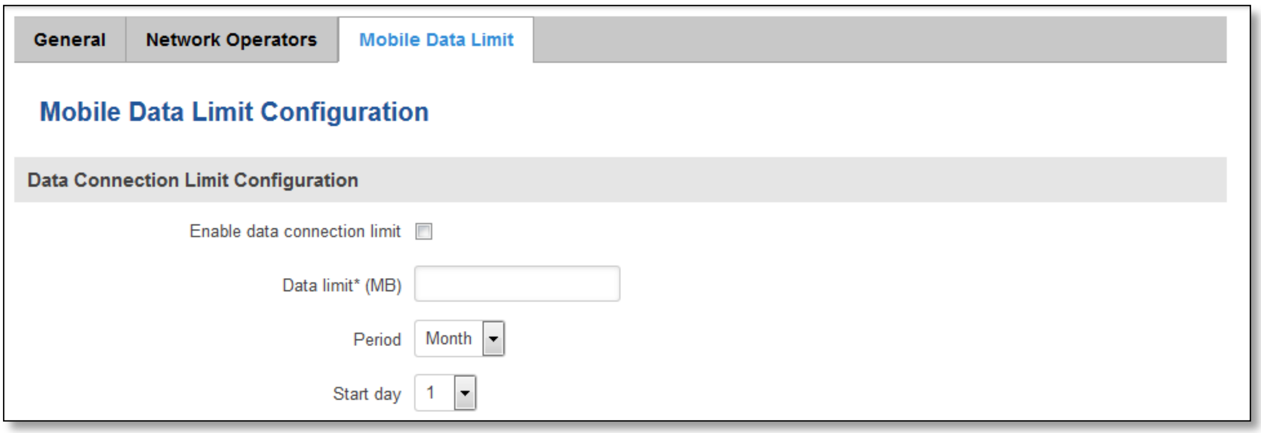
Name	Operator code	Sort
Tele2 LT	24603	

	Field name	Possible values	Explanation
1.	Enable	Enable/Disable	Enable/disable operators blocking
2.	Mode	White list/Black list	White list - allows every operator on the list and blocks everything else. Black list – block every operator on the list and allow everything else
3.	Name	Tele2 LT	Operator's name
4.	Operator code	24603	Operator's code

7.1.3 Mobile Data Limit

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

7.1.3.1 Data Connection Limit Configuration



Mobile Data Limit Configuration

Data Connection Limit Configuration

Enable data connection limit □

Data limit* (MB)

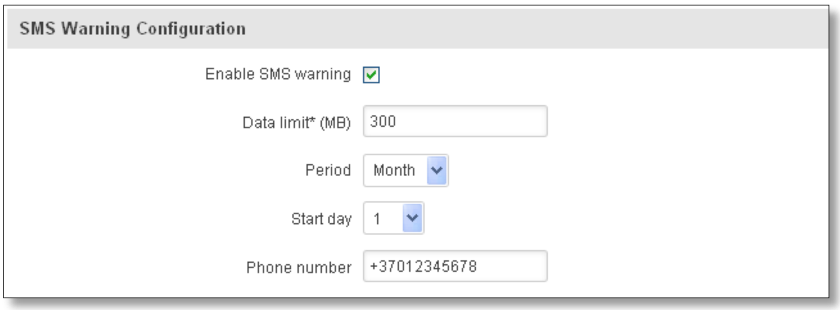
Period Month

Start day 1

	Field Name	Sample value	Explanation
1.	Enable data connection limit	Enable/Disable	Disables mobile data when a limit for 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

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

7.1.3.2 SMS Warning Configuration



SMS Warning Configuration

Enable SMS warning ☑

Data limit* (MB) 300

Period Month

Start day 1

Phone number +37012345678

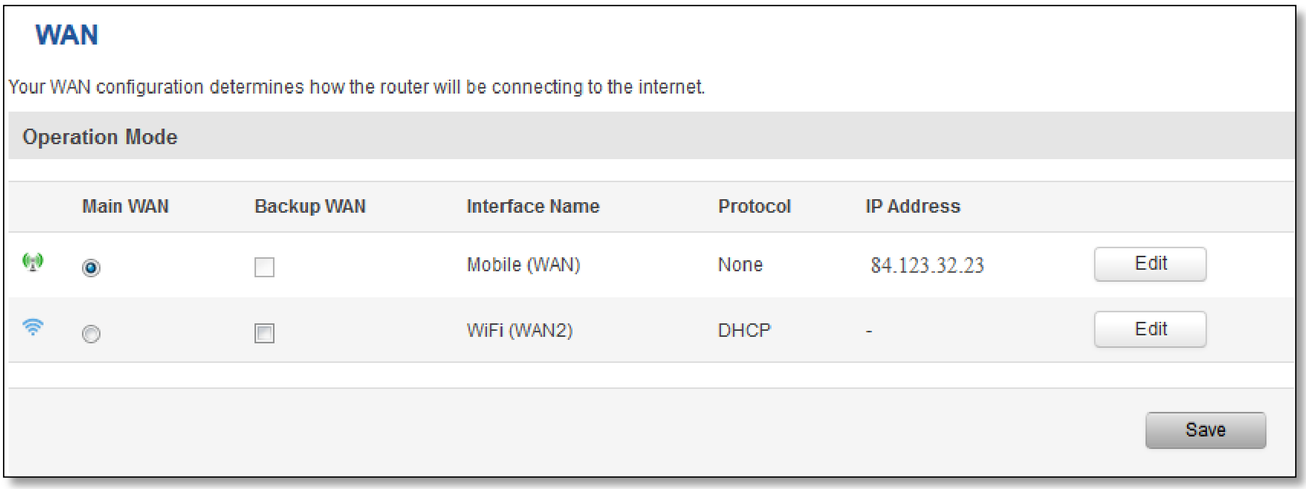
	Field Name	Sample value	Explanation
1.	Enable SMS warning	Enable/Disable	Enables sending of warning SMS message when mobile data limit for current period is reached
2.	Data limit* (MB)	300	Send warning SMS message after limit value in MB is reached
3.	Period	Month/Week/Day	Period for which mobile data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

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

7.2 WAN

7.2.1 Operation Mode

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



WAN

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

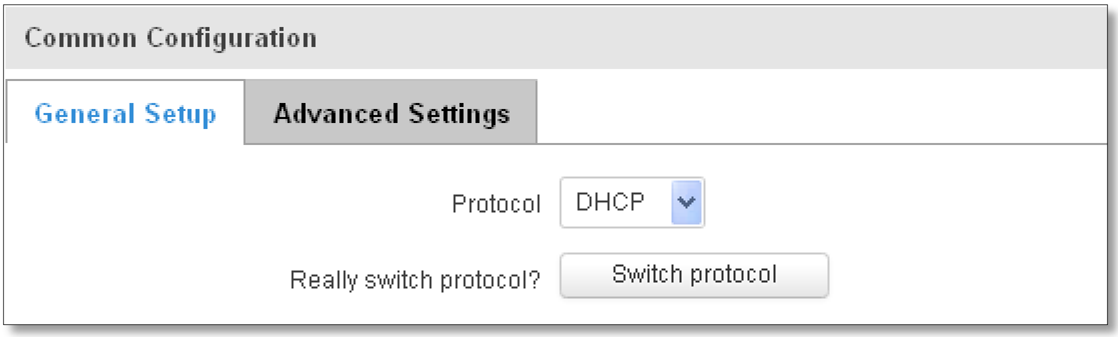
Operation Mode

	Main WAN	Backup WAN	Interface Name	Protocol	IP Address	
	●	□	Mobile (WAN)	None	84.123.32.23	Edit
	○	□	WiFi (WAN2)	DHCP	-	Edit

	Type	Explanation
1.	Main WAN	Switches between Mobile, Wired and Wi-Fi interface for main WAN
2.	Backup WAN	Interface 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

7.2.2 ommon configuration

Common configuration allows you to configure your TCP/IP settings for the wan network (only if Wireless is set as WAN).



Common Configuration

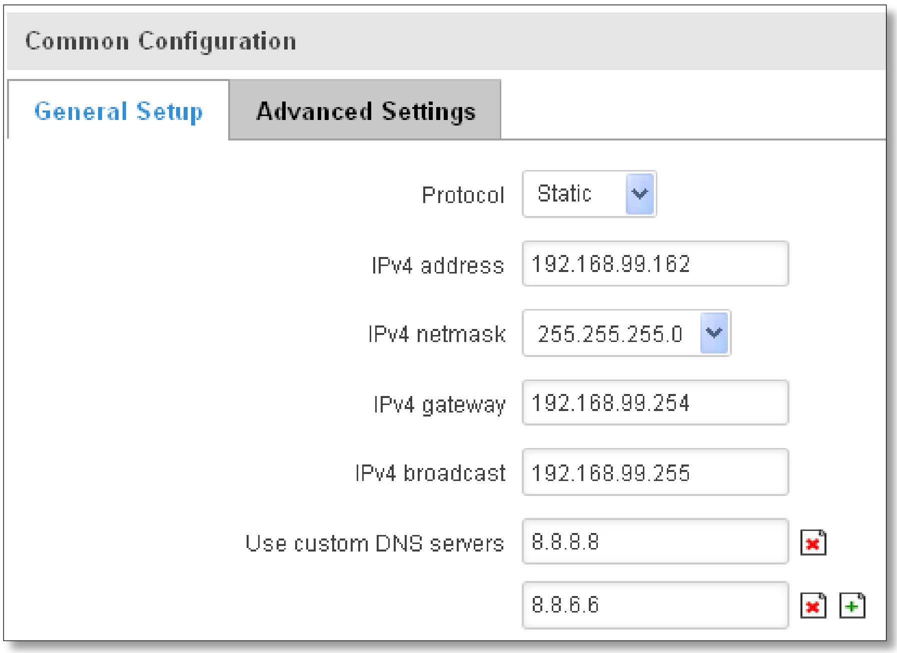
Protocol: DHCP

Really switch protocol? Switch protocol

You can switch between the Static or DHCP 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:



Common Configuration

Protocol: Static

IPv4 address: 192.168.99.162

IPv4 netmask: 255.255.255.0

IPv4 gateway: 192.168.99.254

IPv4 broadcast: 192.168.99.255

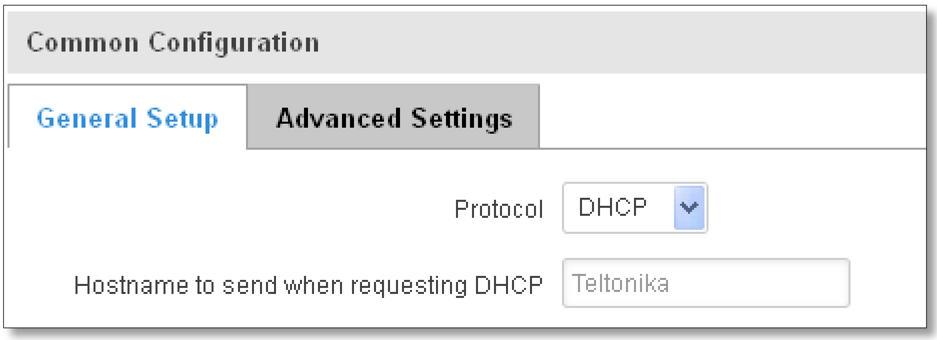
Use custom DNS servers: 8.8.8.8 ☒

8.8.6.6 ☒ ⊞

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 (auto generated if not set). It is best to leave this blank unless you know what you are doing.
5.	Use custom DNS servers	8.8.8.8 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:



Protocol: DHCP

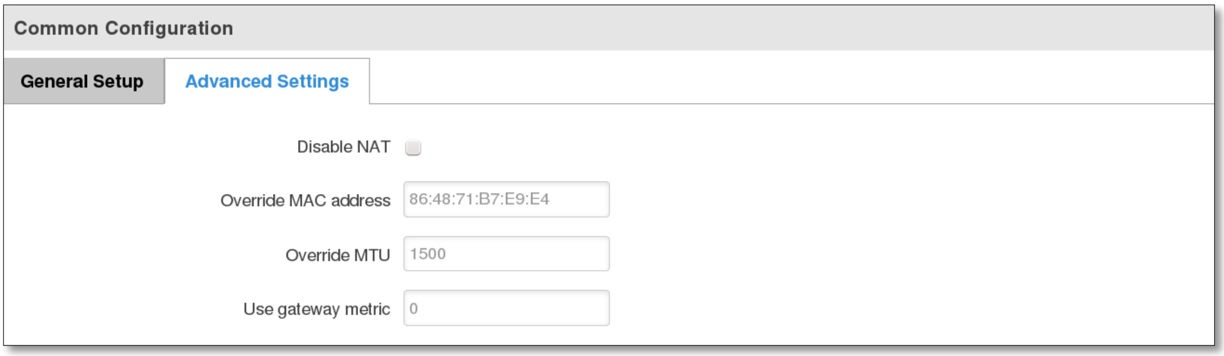
Hostname to send when requesting DHCP: Teltonika

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

7.2.2.2 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



Disable NAT: □

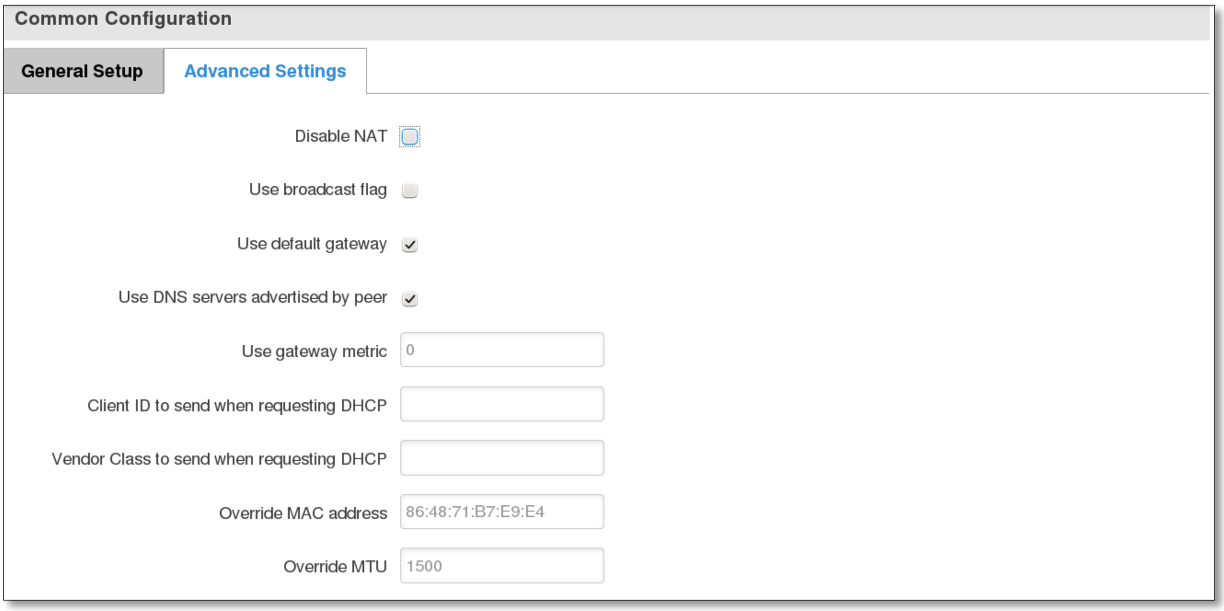
Override MAC address: 86:48:71:B7:E9:E4

Override MTU: 1500

Use gateway metric: 0

	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

Disable NAT □

Use broadcast flag □

Use default gateway ☑

Use DNS servers advertised by peer ☑

Use gateway metric 0

Client ID to send when requesting DHCP

Vendor Class to send when requesting DHCP

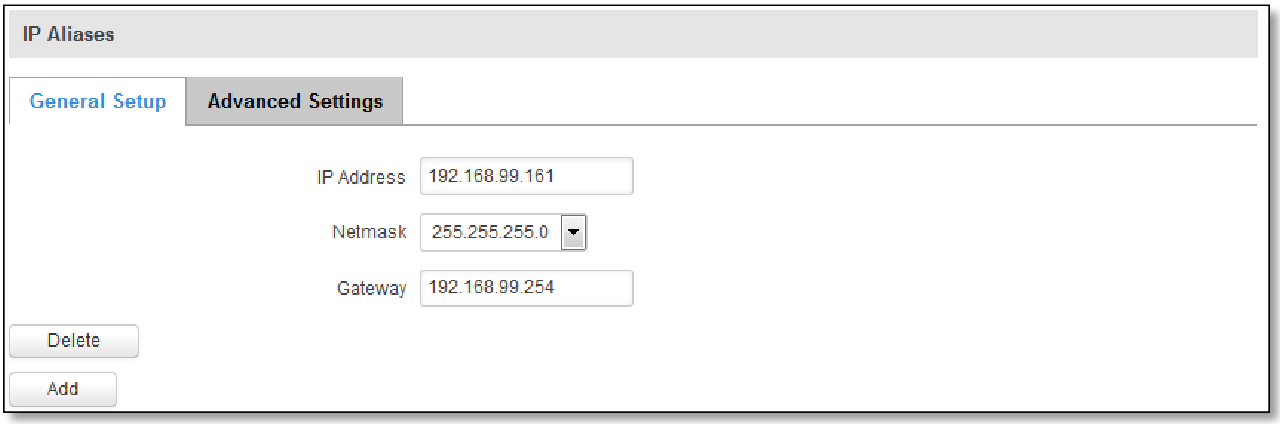
Override MAC address 86:48:71:B7:E9:E4

Override MTU 1500

	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		Specify client ID which will be sent when requesting DHCP (Dynamic Host Configuration Protocol)
7.	Vendor Class to send when requesting DHCP		Specify vendor class which be sent when requesting DHCP (Dynamic Host Configuration Protocol)
8.	Override MAC address	86:48:71:B7:E9:E4	Override MAC address of the WAN interface. If your ISP gives you a static IP address it might also bind it to your 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 IP Aliases

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


IP Aliases

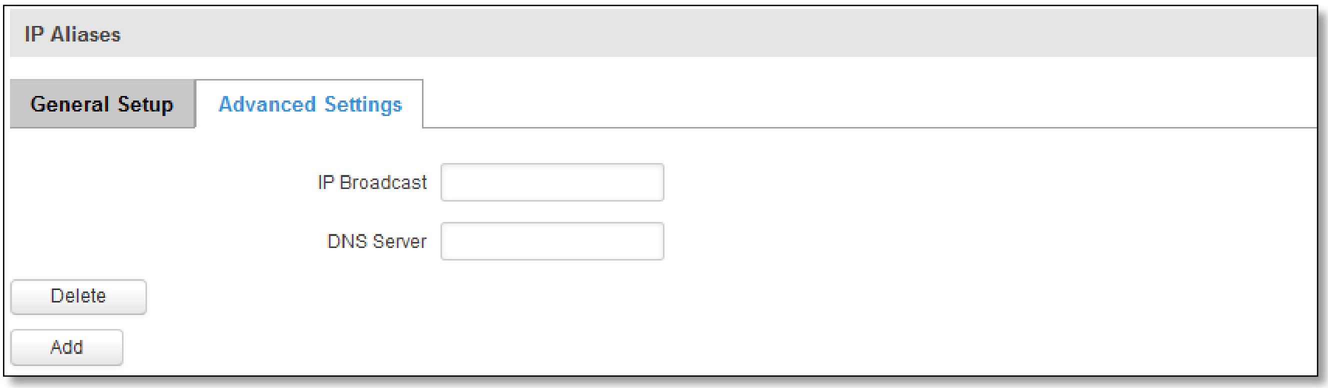
General Setup | Advanced Settings

IP Address: 192.168.99.161

Netmask: 255.255.255.0

Gateway: 192.168.99.254

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.


IP Aliases

General Setup | Advanced Settings

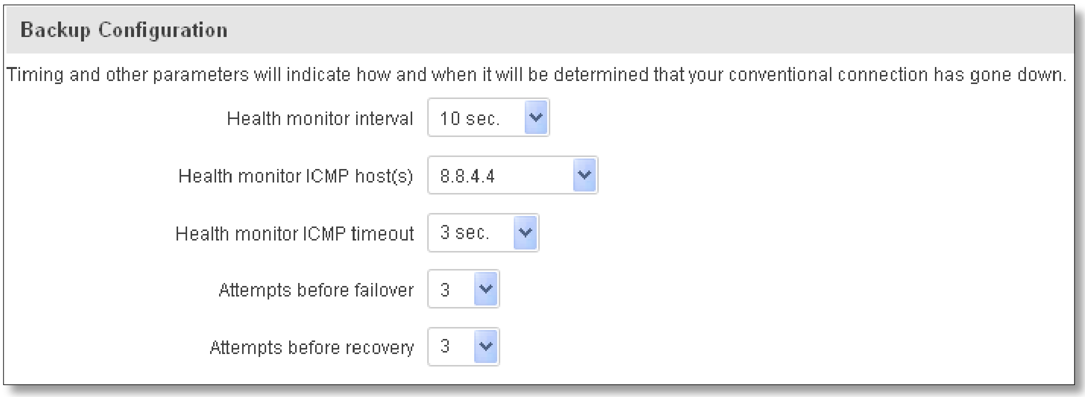
IP Broadcast:

DNS Server:

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

7.2.2.2.4 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.


Backup Configuration

Timing and other parameters will indicate how and when it will be determined that your conventional connection has gone down.

Health monitor interval: 10 sec.

Health monitor ICMP host(s): 8.8.4.4

Health monitor ICMP timeout: 3 sec.

Attempts before failover: 3

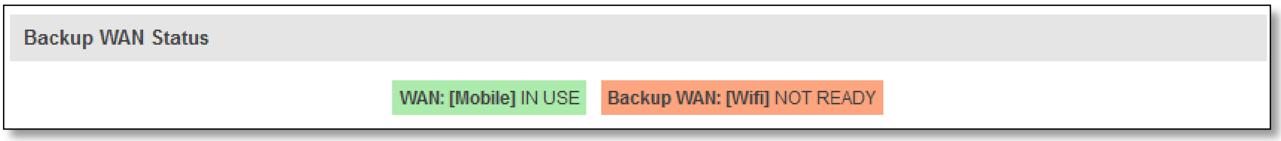
Attempts before recovery: 3

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?

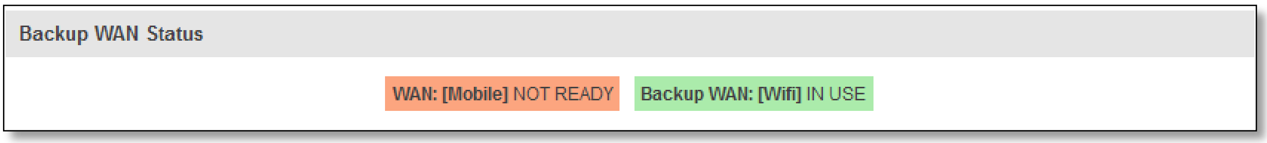
First we must select a main link and choose one or two backup links in WAN section. Then push the “Edit” button and configure your WAN and Backup Wan settings to your liking. Click Save and wait until the settings are applied. Now in the Status -> Network Information -> WAN page there should be a status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



Backup WAN Status

WAN: [Mobile] IN USE   Backup WAN: [Wifi] NOT READY

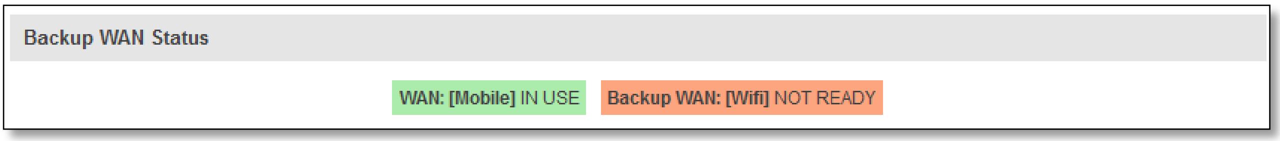
The above picture shows the status for Backup WAN configured on a wired main link. You can now simulate a downed link by simply unplugging your Ethernet WAN cable. When you’ve done so you should see this:



Backup WAN Status

WAN: [Mobile] NOT READY   Backup WAN: [Wifi] IN USE

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



Backup WAN Status

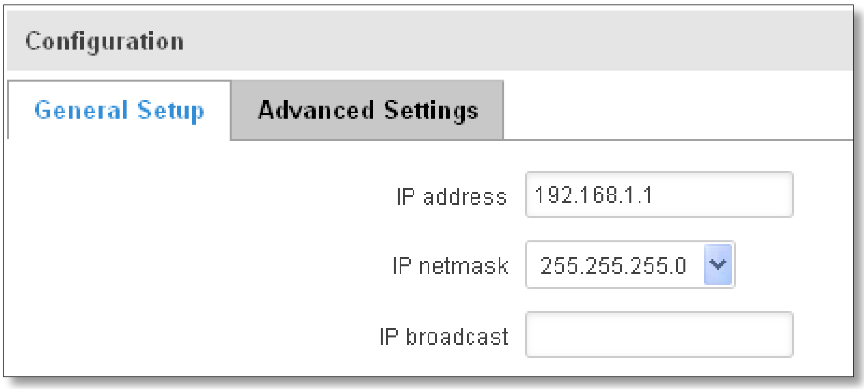
WAN: [Mobile] IN USE   Backup WAN: [Wifi] NOT READY

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



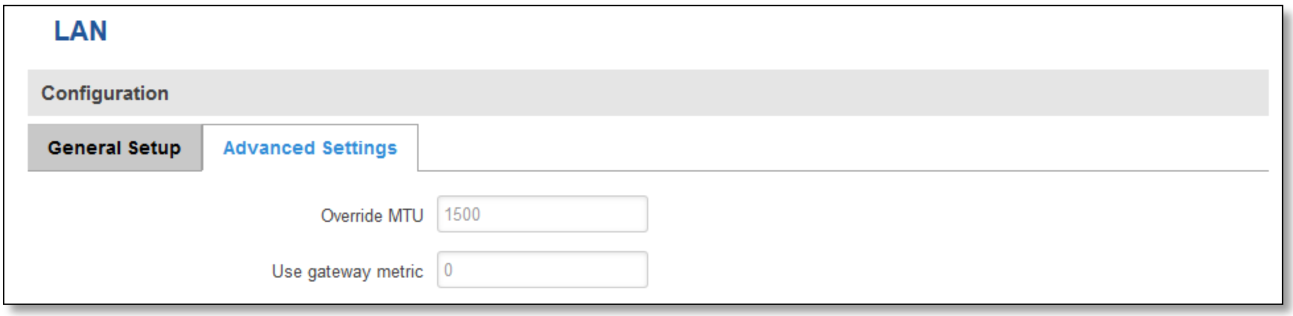
IP address 192.168.1.1

IP netmask 255.255.255.0

IP broadcast

	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		IP broadcasts are used by BOOTP and DHCP clients to find and send requests to their respective servers

7.3.1.2 Advanced settings



Override MTU 1500

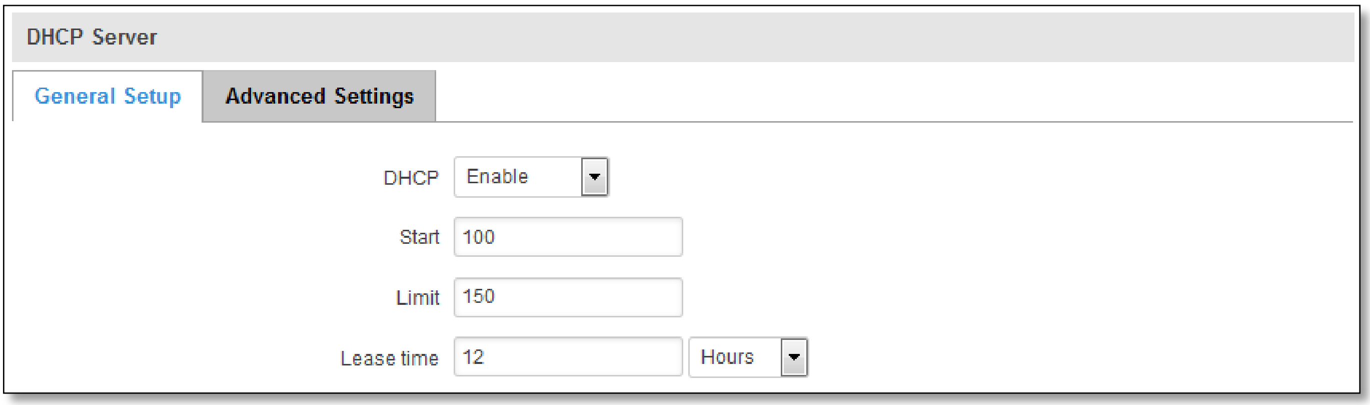
Use gateway metric 0

	Field name	Sample value	Explanation
1.	Override MTU	1500	MTU (Maximum Transmission Unit) specifies the largest possible size of a data packet
2.	Use gateway metric	0	With this field you can alter the metric of that entry

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 IP address and the device will be able to fully communicate with the router.

7.3.2.1 General Setup



DHCP Server

DHCP: Enable

Start: 100

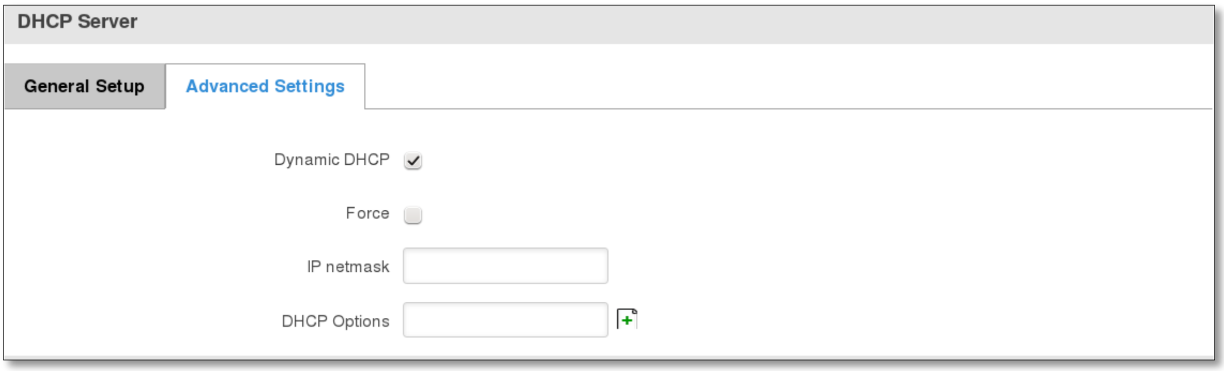
Limit: 150

Lease time: 12 Hours

	Field Name	Sample value	Explanation
1.	DHCP	Enable / Disable/ DHCP Relay	Manage DHCP server
2.	Start	100	The starting address of the range that the DHCP server can use to give out to devices. E.g.: if your LAN IP is 192.168.2.1 and your subnet mask is 255.255.255.0 that means that in your network a valid IP address has to be in the range of [192.168.2.1 – 192.168.2.254](192.168.2.0 and 192.168.2.255 are special unavailable addresses). If the Start value is set to 100 then the DHCP server will only be able to lease out addresses starting from 192.168.2.100
3.	Limit	150	How many addresses the DHCP server gets to lease out. Continuing on the above example: if the start address is 192.168.2.100 then the end address will be 192.168.2.249 [100 + 150 – 1 = 249] (“-1” is needed, because “100” is also included in the limit).
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.



DHCP Server

General Setup | Advanced Settings

Dynamic DHCP ☑

Force □

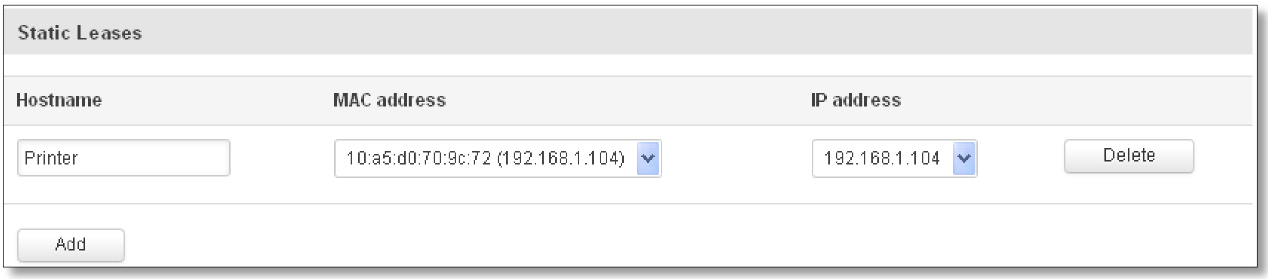
IP netmask

DHCP Options

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

7.3.2.3 Static Leases

This page is used to configure static IP leases.



Static Leases

Hostname	MAC address	IP address	
Printer	10:a5:d0:70:9c:72 (192.168.1.104)	192.168.1.104	Delete

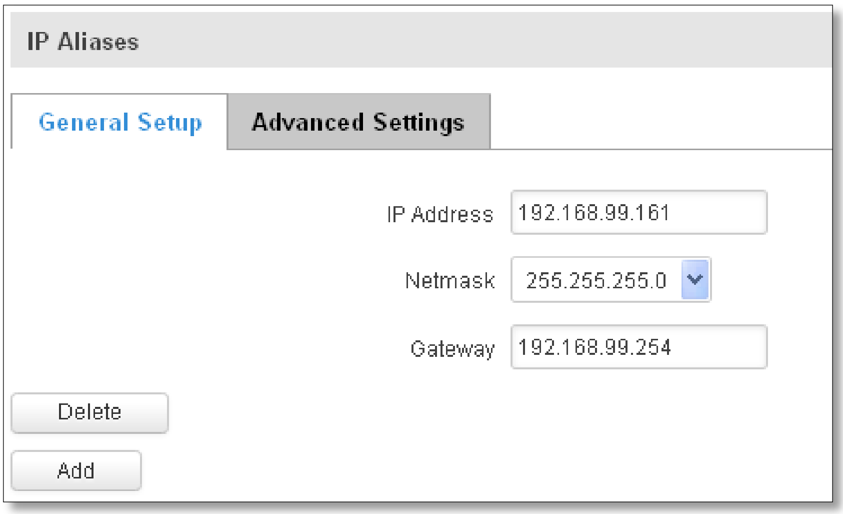
Add

	Field Name	Sample Value	Explanation
1.	Hostname	Printer	Name which will be linked with IP address.
2.	MAC address	10:a5:d0:70:9c:72 (192.168.1.104)	Device MAC address
3.	IP address	192.168.1.104	Device IP address

7.3.2.4 IP Aliases

7.3.2.4.1 General Setup

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



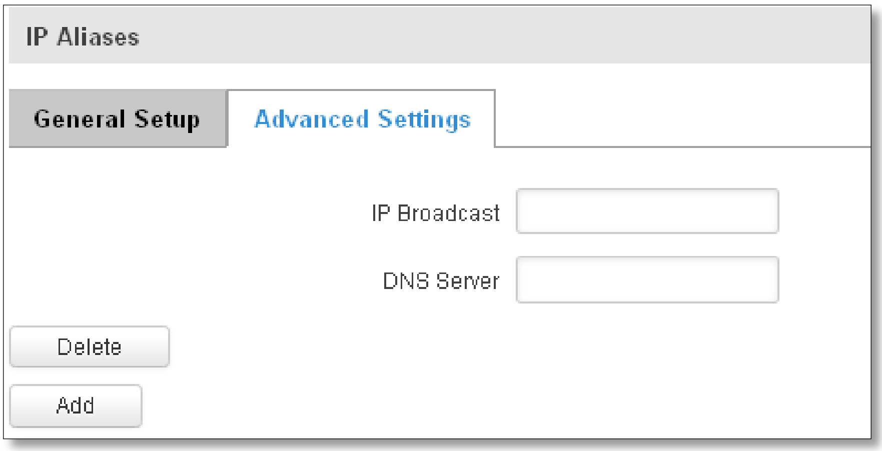
IP Address 192.168.99.161

Netmask 255.255.255.0

Gateway 192.168.99.254

7.3.2.4.2 Advanced Settings

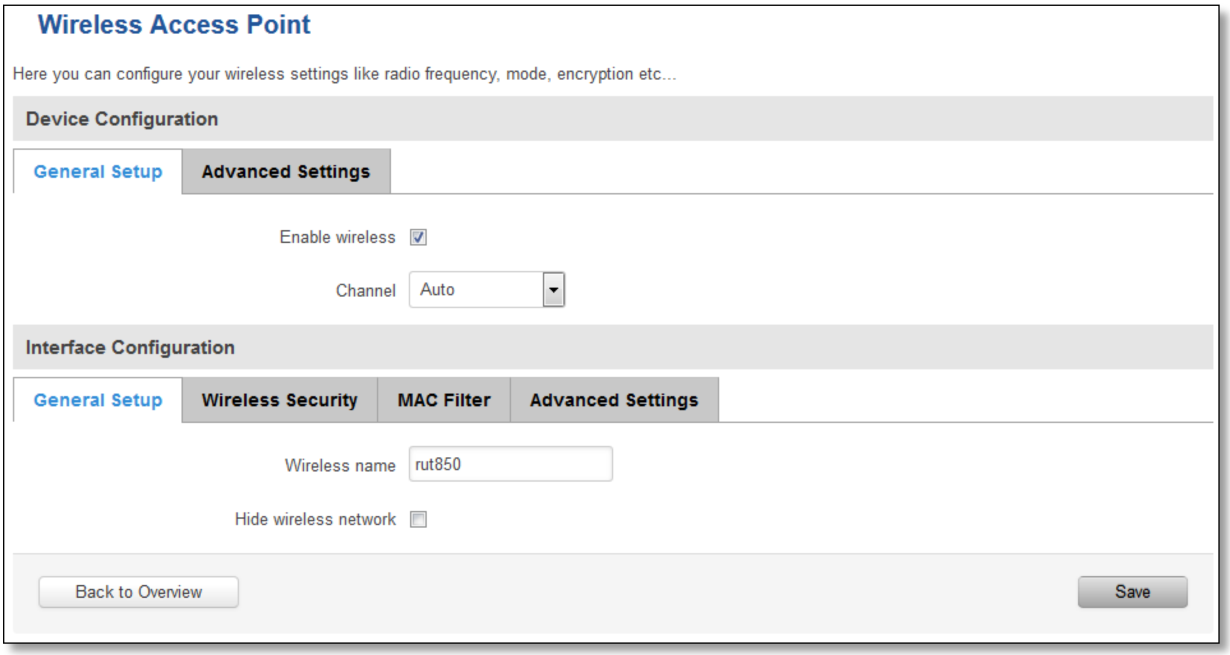
You may also optionally define a broadcast address and a custom DNS server.



7.4 Wireless

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

Access Point:



Wireless Access Point

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

Device Configuration

Enable wireless ☑

Channel: Auto

Interface Configuration

Wireless name: rut850

Hide wireless network □

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.

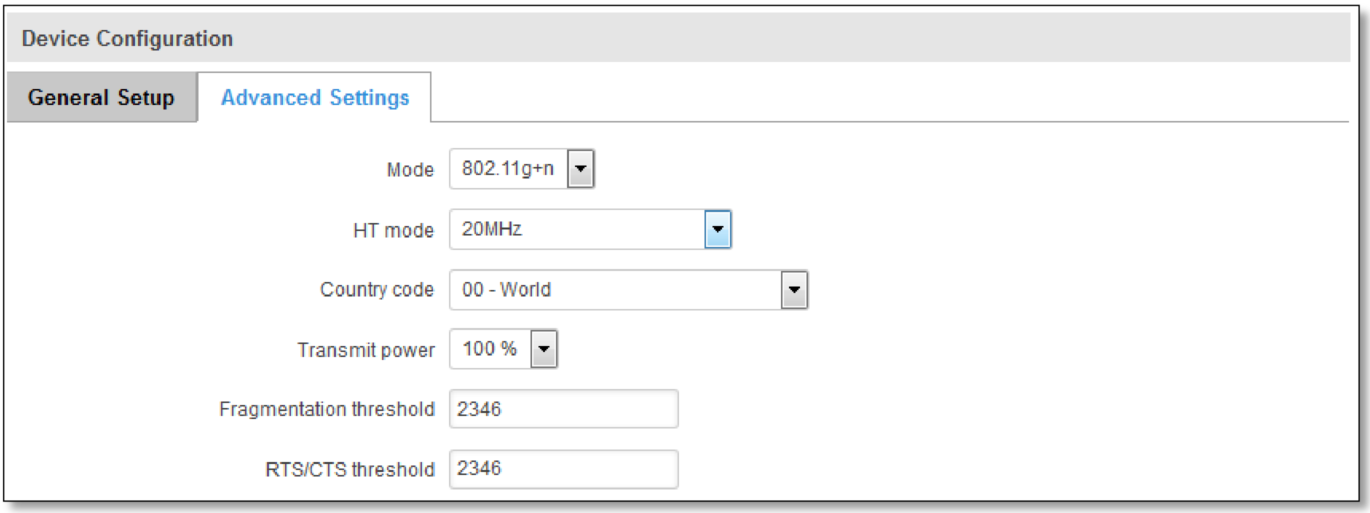
Important note: As seen in the picture you should always **Save** before toggling the radio on and off.

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

7.4.1.1 Device

7.4.1.1.1 Advanced Settings



Mode: 802.11g+n

HT mode: 20MHz

Country code: 00 - World

Transmit power: 100 %

Fragmentation threshold: 2346

RTS/CTS threshold: 2346

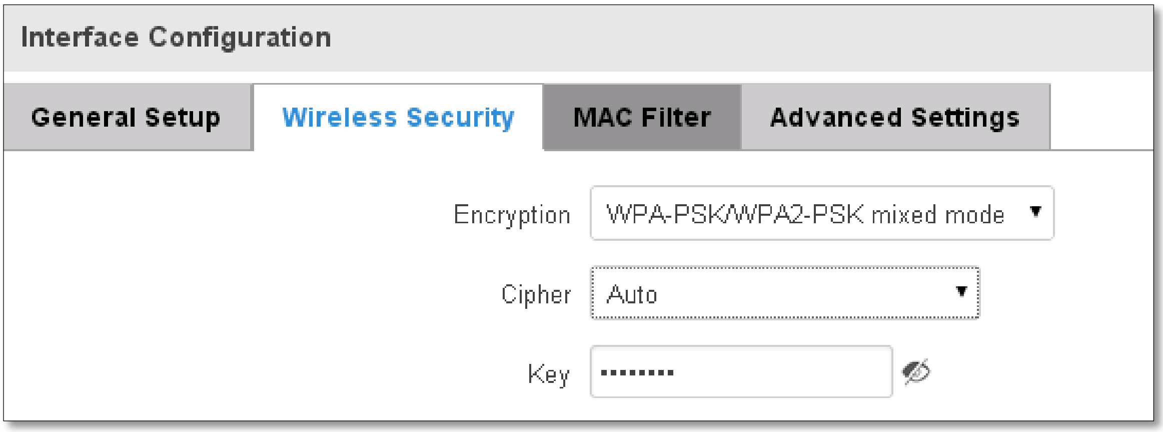
Here you can configure more advanced parameters:

	Field name	Sample value	Explanation
1.	Mode	Auto, b, g, g+n	Different modes provide different throughput and security options.
2.	HT mode	20 MHz/40 Mhz 2nd channel above	HT(High Throughput) mode. 40 MHz bandwidth provides better perfomance
3.	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.
4.	Transmit power	20%/40%/60%/80%/100%	Select Wi-Fi signal power
5.	Fragmentation threshold	2346	The smallest packet size that can be fragmented and transmitted by multiple frames. In areas were interference is a problem, setting a lower fragment threshold might help reduce the probability of unsuccessful packet transfers, thus increasing speed.
6.	RTS/CTS Threshold	2346	Request to send threshold. It can help resolve problems arising when several access points are in the same area, contending.

7.4.1.2 Interface

7.4.1.2.1 Security

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



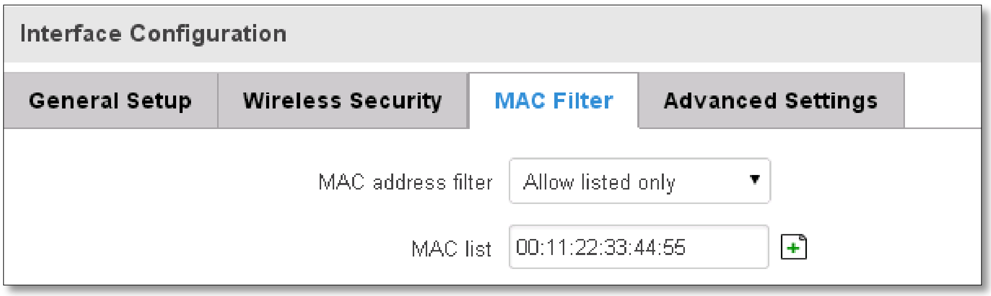
Encryption: WPA-PSK/WPA2-PSK mixed mode

Cipher: Auto

Key: ••••••••

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

7.4.1.2.2 MAC-Filter



MAC address filter: Allow listed only

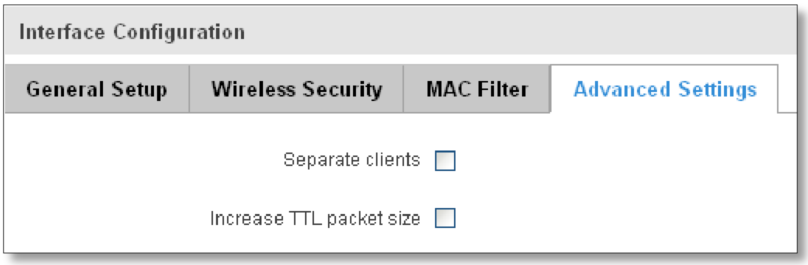
MAC list: 00:11:22:33:44:55

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.

7.4.1.2.3 Advanced settings

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

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



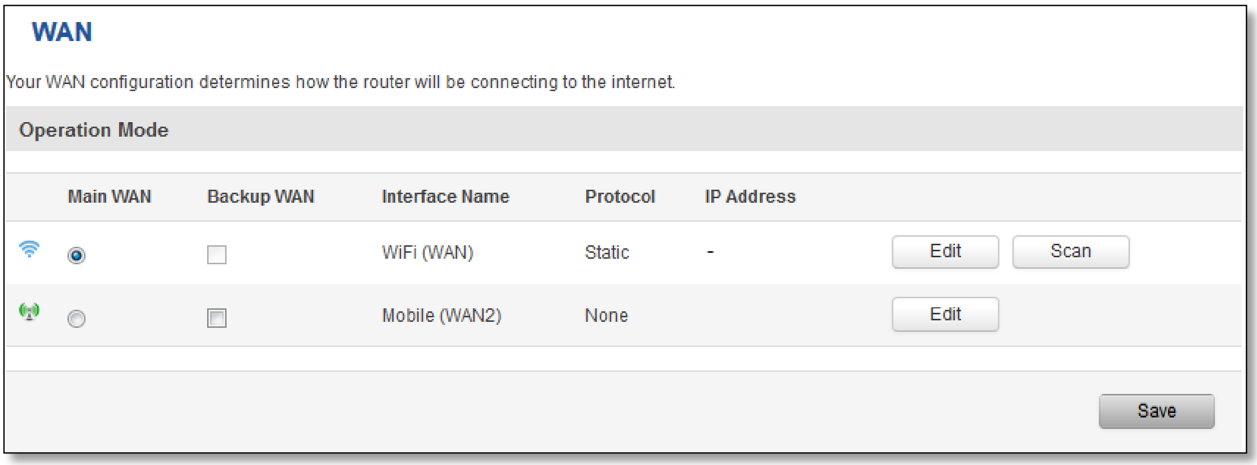
Separate clients □

Increase TTL packet size □

7.4.1.3 Client

RUT850 can work as a Wi-Fi client. Client mode is nearly identical to AP, except for the fact that most for 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.



WAN

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

Operation Mode

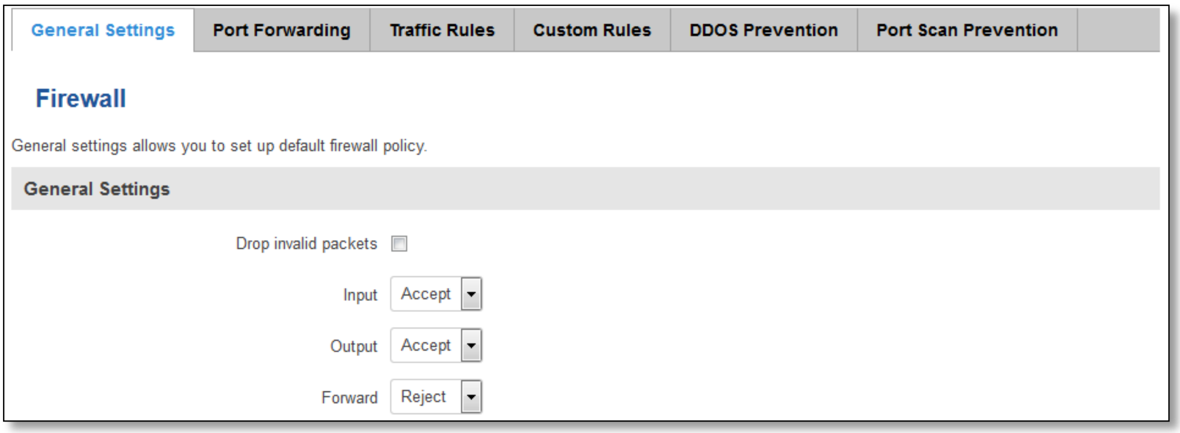
	Main WAN	Backup WAN	Interface Name	Protocol	IP Address		
	●	□	WiFi (WAN)	Static	-	Edit	Scan
	○	□	Mobile (WAN2)	None		Edit	

7.5 Firewall

In this section we will look over the various firewall features that come with RUT9.

7.5.1 General Settings

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



Firewall

General settings allows you to set up default firewall policy.

General Settings

Drop invalid packets □

Input: Accept

Output: Accept

Forward: Reject

	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.

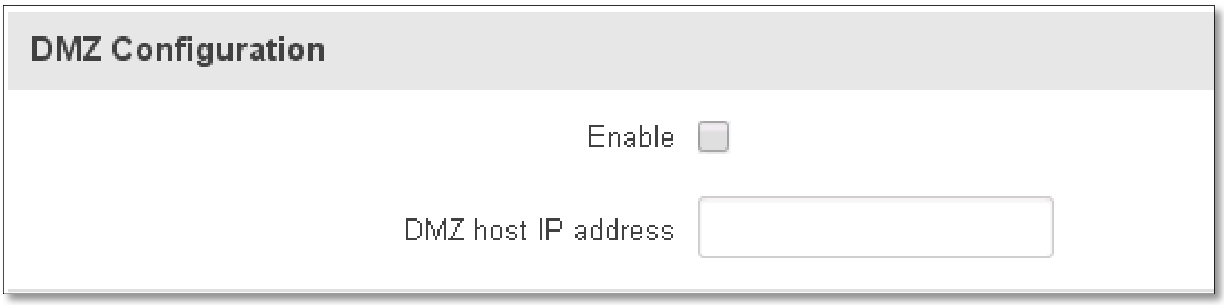
*DEFAULT: When a packet goes through a firewall chain it is matched against all the rules for that specific chain. If no rule matches said packet, an according Action (either Drop or Reject or Accept) is performed.

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.

7.5.2 DMZ



DMZ Configuration

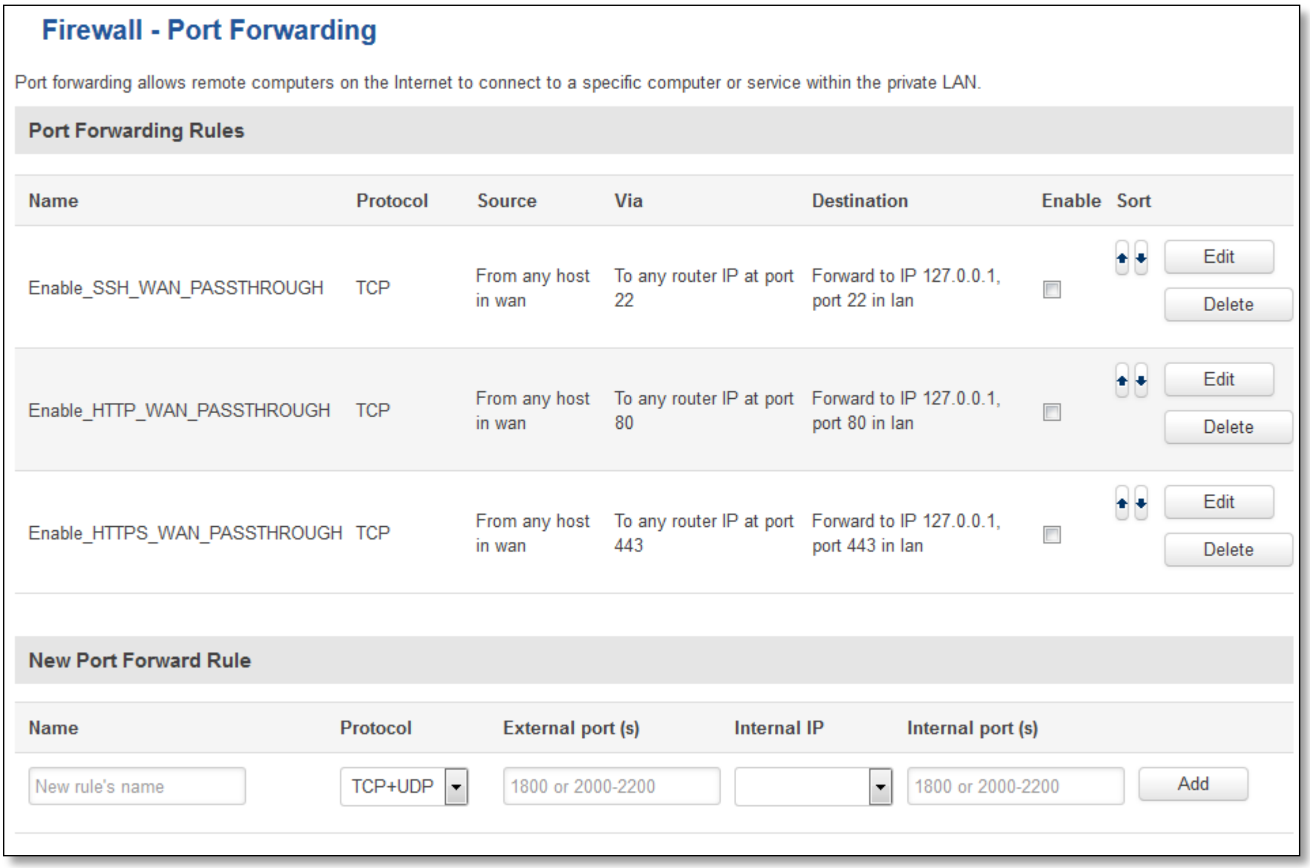
Enable □

DMZ host IP address

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).

7.5.3 Port Forwarding

Here you can define your own port forwarding rules.



Firewall - Port Forwarding

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

Port Forwarding Rules

Name	Protocol	Source	Via	Destination	Enable	Sort
Enable_SSH_WAN_PASSTHROUGH	TCP	From any host in wan	To any router IP at port 22	Forward to IP 127.0.0.1, port 22 in lan	□	Edit Delete
Enable_HTTP_WAN_PASSTHROUGH	TCP	From any host in wan	To any router IP at port 80	Forward to IP 127.0.0.1, port 80 in lan	□	Edit Delete
Enable_HTTPS_WAN_PASSTHROUGH	TCP	From any host in wan	To any router IP at port 443	Forward to IP 127.0.0.1, port 443 in lan	□	Edit Delete

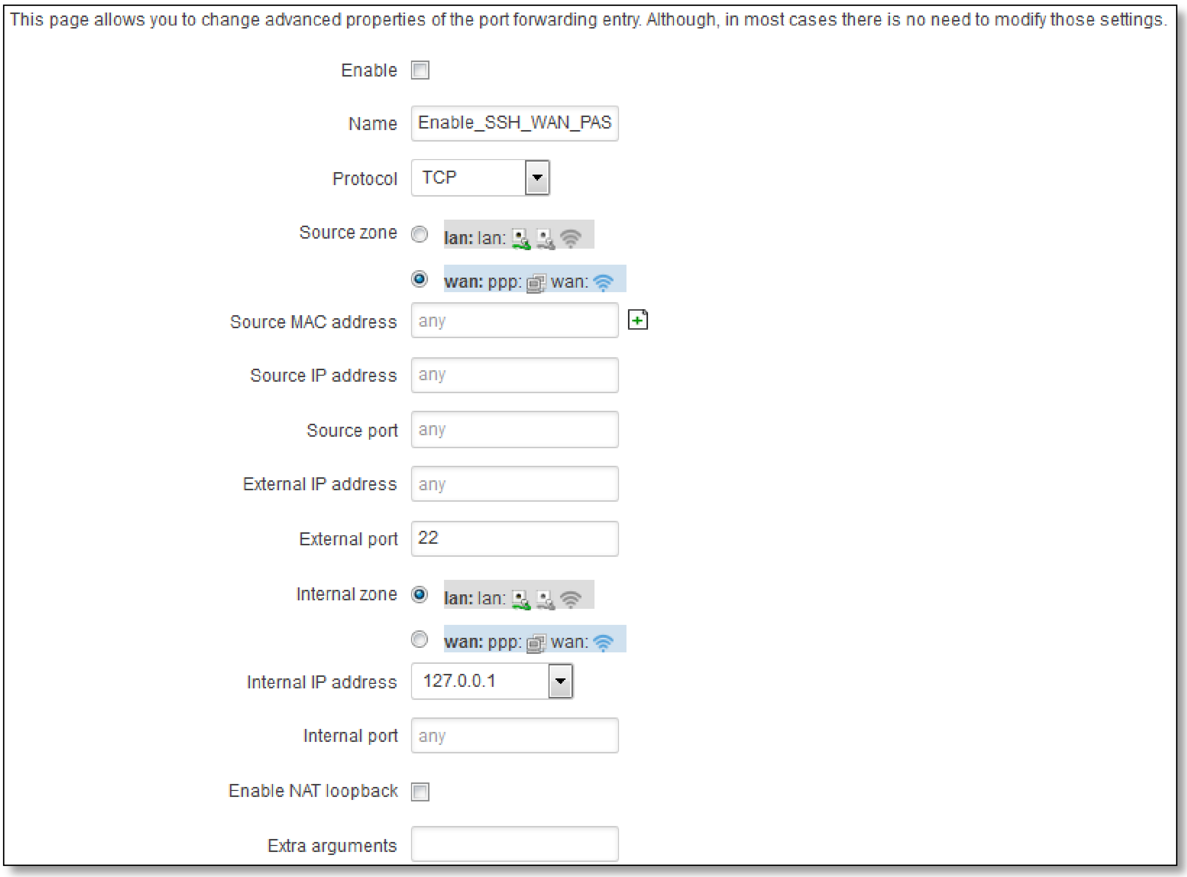
New Port Forward Rule

Name	Protocol	External port (s)	Internal IP	Internal port (s)	
New rule's name	TCP+UDP	1800 or 2000-2200		1800 or 2000-2200	Add

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

	Field Name	Sample value	Explanation
1.	Name	Enable_SSH_WAN_PASSTHROUGH	Name of the rule. Used purely to make it easier to manage rules.
2.	Protocol	TCP/UDP/TCP+UDP/Other	Type of protocol of incoming packet.
3.	External Port	1-65535	From this port on the WAN network the traffic will 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 that port on the internal machine the rule will redirect the traffic.

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



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

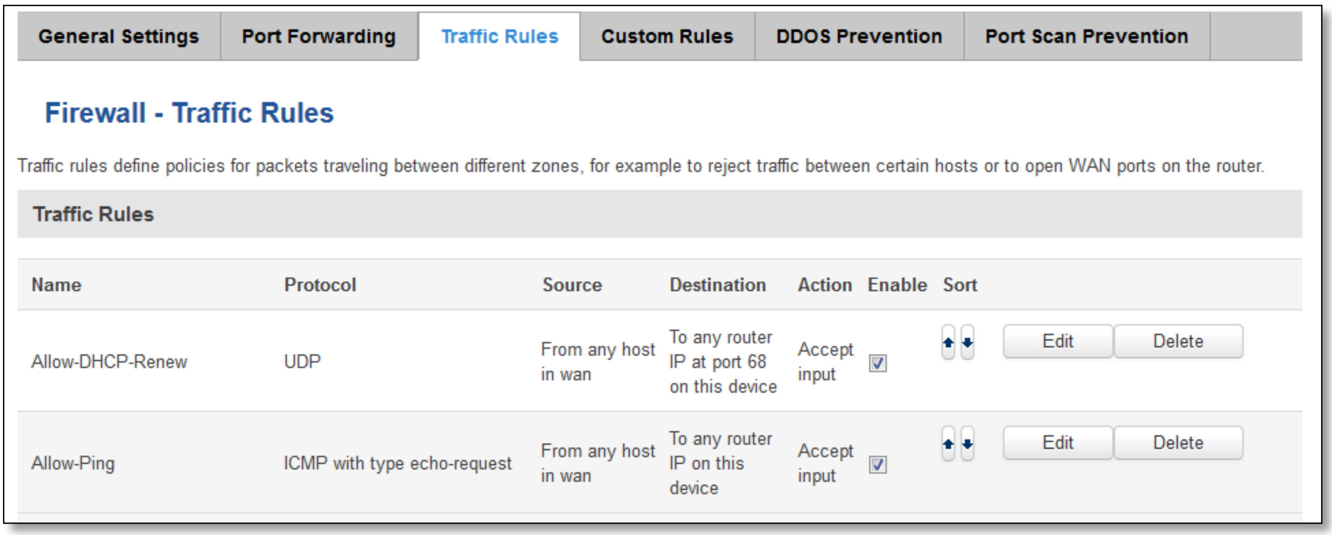
Enable	□
Name	Enable_SSH_WAN_PAS
Protocol	TCP
Source zone	○ lan: lan: ● wan: ppp: wan:
Source MAC address	any
Source IP address	any
Source port	any
External IP address	any
External port	22
Internal zone	● lan: lan: ○ wan: ppp: wan:
Internal IP address	127.0.0.1
Internal port	any
Enable NAT loopback	□
Extra arguments	

	Field Name	Sample value	Explanation
1.	Name	ENABLE_SSH_WAN_PASSTHROUGH	Name of the rule. Used purely to make it easier to manage rules.
2.	Protocol	TCP/UDP/TCP+ UDP/ICMP/Custom	You may specify multiple by selecting (custom) and then entering protocols separated by space

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

7.5.4 Traffic Rules

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



Firewall - Traffic Rules

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

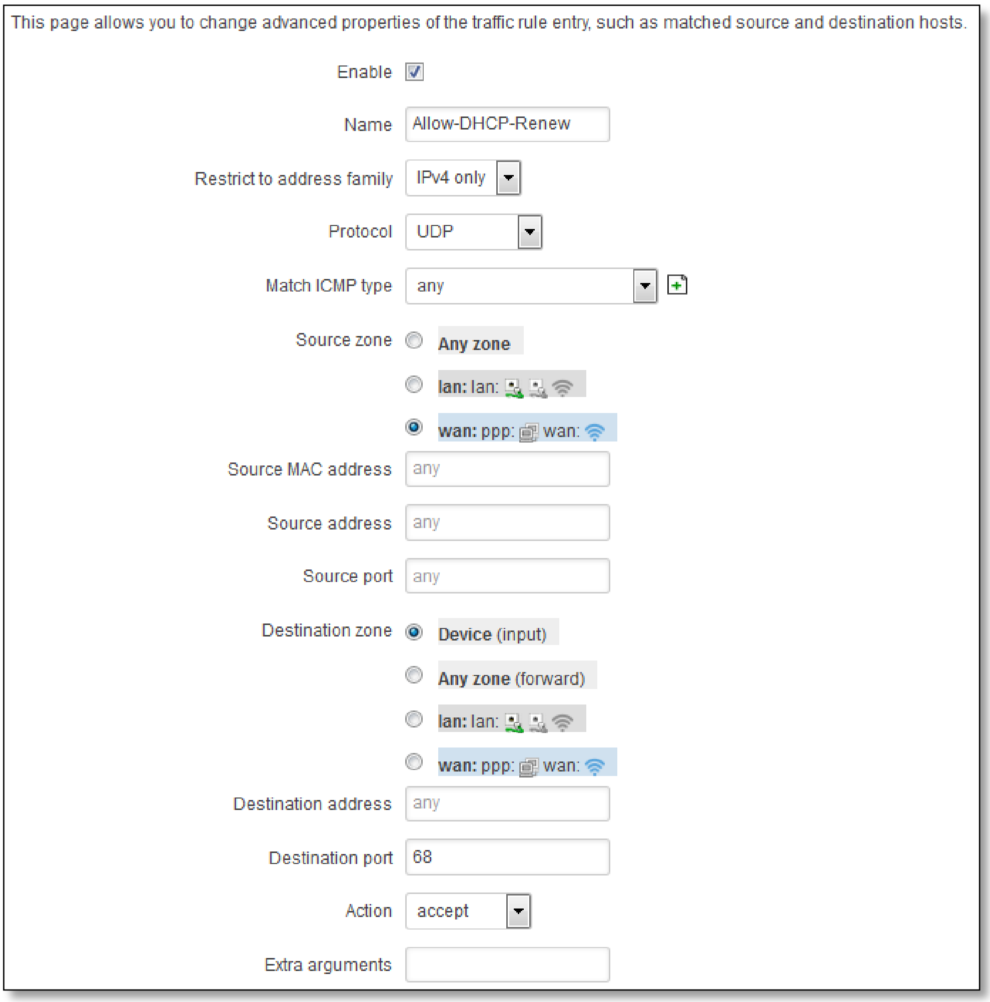
Traffic Rules

Name	Protocol	Source	Destination	Action	Enable	Sort
Allow-DHCP-Renew	UDP	From any host in wan	To any router IP at port 68 on this device	Accept input	☑	↑ ↓
Allow-Ping	ICMP with type echo-request	From any host in wan	To any router IP on this device	Accept input	☑	↑ ↓

	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.



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

Enable ☑

Name: Allow-DHCP-Renew

Restrict to address family: IPv4 only

Protocol: UDP

Match ICMP type: any

Source zone: ○ Any zone ○ lan: lan: ● wan: ppp: wan:

Source MAC address: any

Source address: any

Source port: any

Destination zone: ● Device (input) ○ Any zone (forward) ○ lan: lan: ○ wan: ppp: wan:

Destination address: any

Destination port: 68

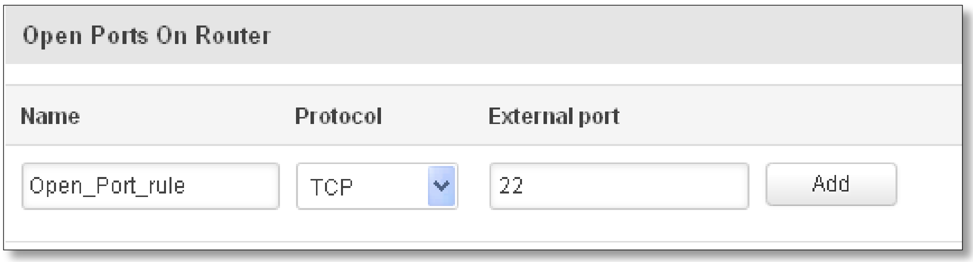
Action: accept

Extra arguments:

	Field Name	Sample value	Explanation
1.	Name	"Allow-DHCP-Renew"	Used to make rule management easier
2.	Restrict to address family	IPv4 and IPV6	Match traffic from selected address family only
3.	Protocol	TCP/UDP/Any/ICMP/Custom	Protocol of the packet that is being matched against traffic rules.
4.	Match ICMP type	any	Match traffic with selected ICMP type only
5.	Source zone	any zone/LAN/WAN	Match incoming traffic from this zone only
6.	Source MAC	any	Match incoming traffic from these MACs only

	address		
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/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 /don't track	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

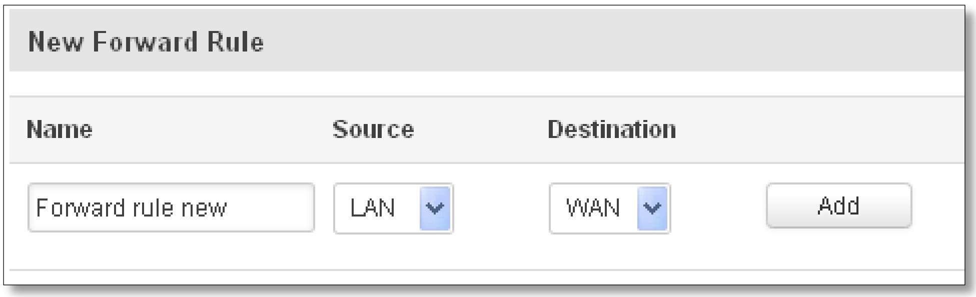
7.5.4.1 Open Ports On the Router


Open Ports On Router

Name: Open_Port_rule
Protocol: TCP
External port: 22

	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.

7.5.4.2 New Forward Rule

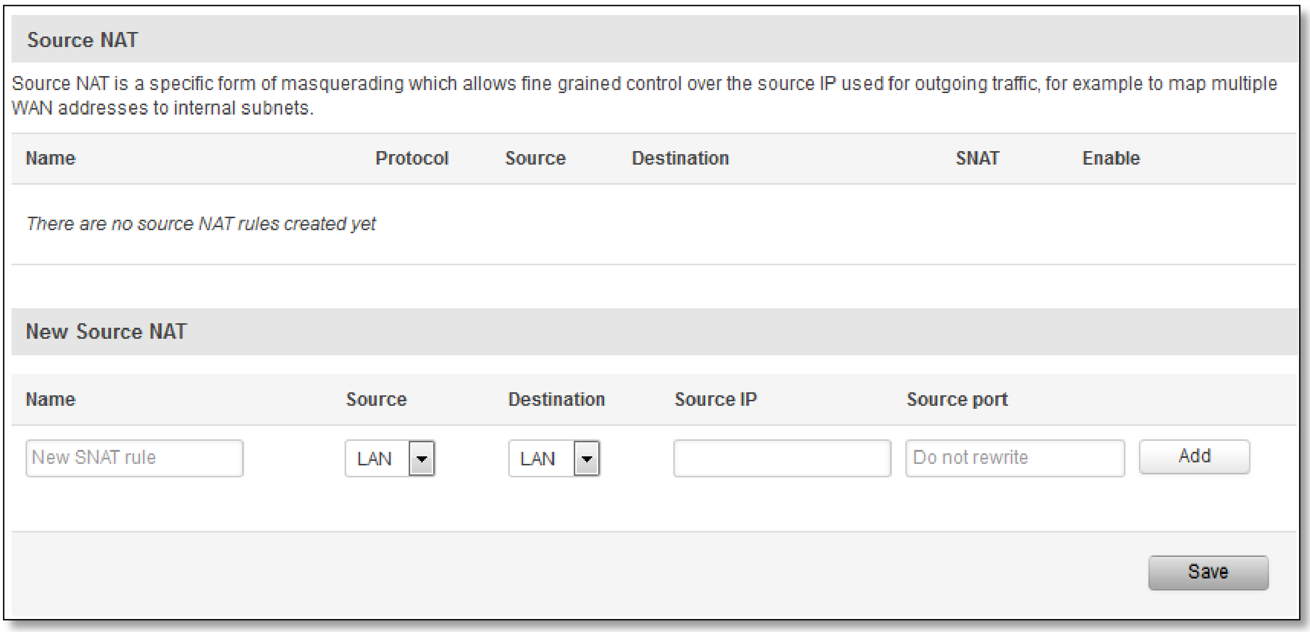

New Forward Rule

Name: Forward rule new
Source: LAN
Destination: WAN

	Field Name	Sample value	Explanation
1.	Name	Forward rule new	Used to make rule management easier
2.	Source	LAN/WAN	Match incoming traffic from selected address family only
3.	Destination	LAN/WAN	The destination of the packet

7.5.4.3 Source NAT

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



Source NAT

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

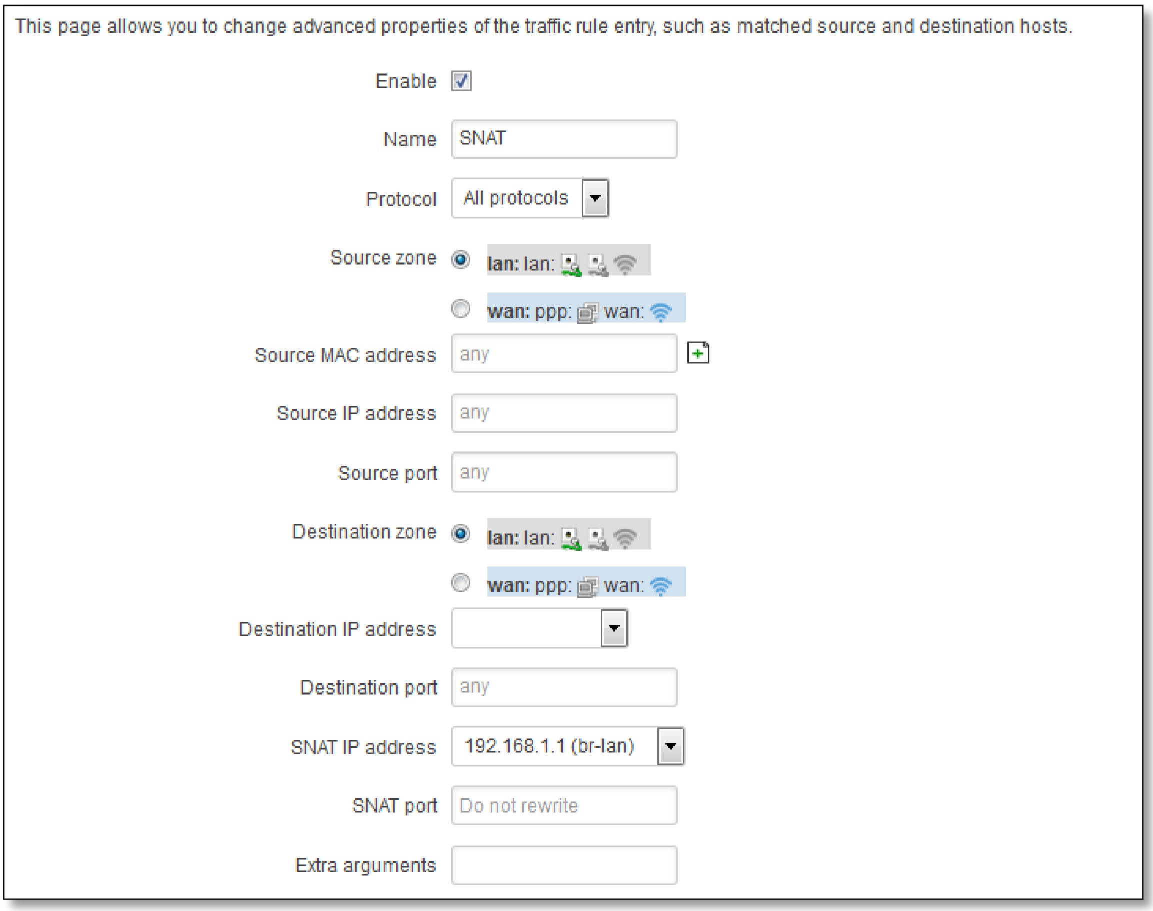
Name	Protocol	Source	Destination	SNAT	Enable
There are no source NAT rules created yet					

New Source NAT

Name	Source	Destination	Source IP	Source port	
New SNAT rule	LAN	LAN		Do not rewrite	Add

	Field Name	Sample value	Explanation
1.	Name	SNAT	Used to make rule management easier
2.	Source	LAN/WAN	Match incoming traffic from selected address family only
4.	Destination	LAN/WAN	Forward incoming traffic to selected address family only
5.	Source IP		Specifies only match incoming traffic from this IP or range
6.	Source port		Specifies only match incoming traffic originating from the given source port or port range on the client host

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



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

Enable ☑

Name SNAT

Protocol All protocols

Source zone ● lan: lan: ○ wan: ppp: wan:

Source MAC address any

Source IP address any

Source port any

Destination zone ● lan: lan: ○ wan: ppp: wan:

Destination IP address

Destination port any

SNAT IP address 192.168.1.1 (br-lan)

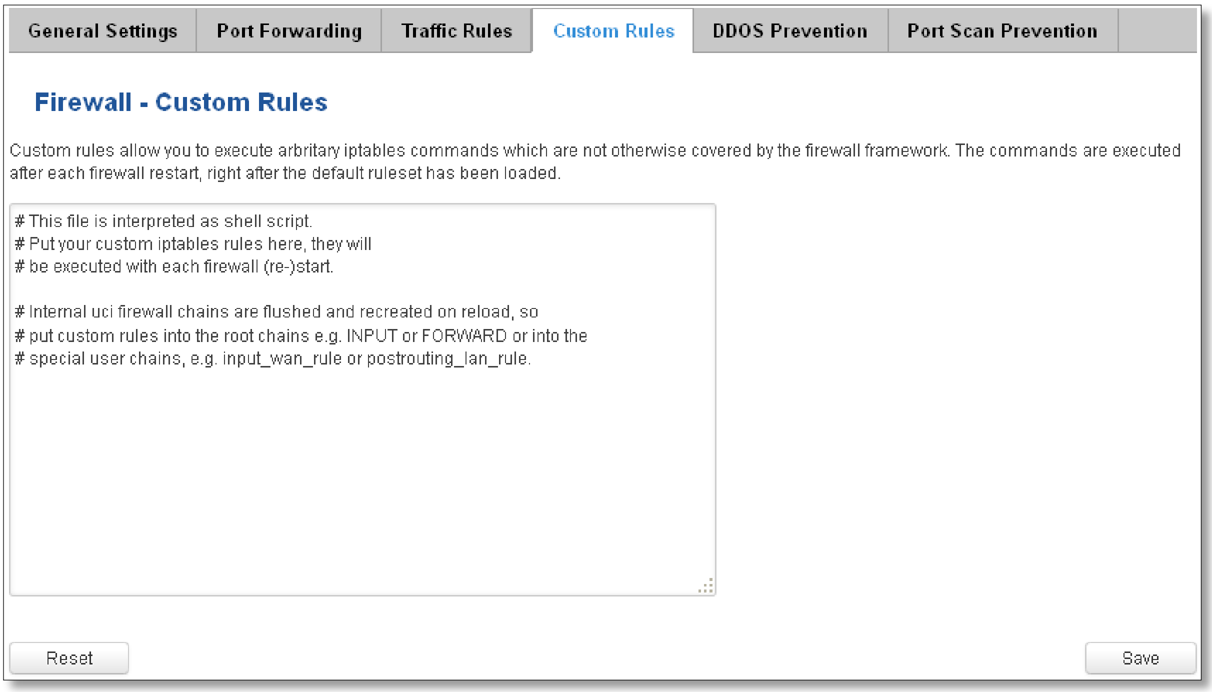
SNAT port Do not rewrite

Extra arguments

	Field Name	Sample value	Explanation
1.	Name	SNAT	Used to make rule management easier
2.	Protocol	All protocols/TCP+UDP/TCP/UDP/ICMP/custom	Protocol of the packet that is being matched against traffic rules.
3.	Source zone	LAN/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/WAN	Match forwarded traffic to the given destination zone only
8.	Destination IP address	Select from the list	Match forwarded traffic to the given destination IP address or IP range only
9.	Destination port	any	Match forwarded traffic to the given destination port or port range only
10.	SNAT IP address	192.168.1.1 (br-lan)	Rewrite matched traffic to the given IP address
11.	SNAT port		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!

7.5.5 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 ant it will get executed as a Linux shell script. If you are unsure of how to use iptables, check out the internet for manuals, examples and explanations.



Firewall - Custom Rules

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

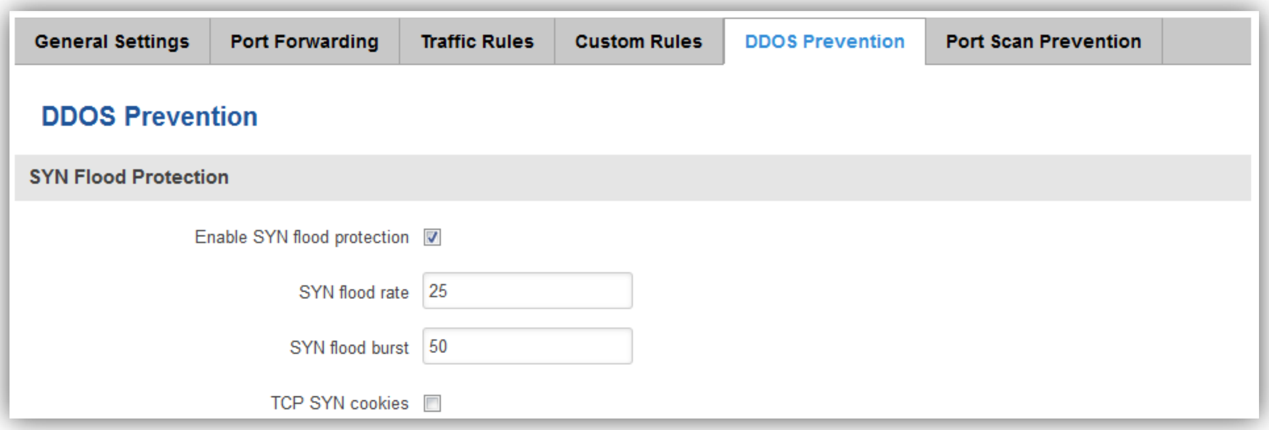
```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

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

7.5.6 DDOS Prevention

7.5.6.1 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.



DDOS Prevention

SYN Flood Protection

Enable SYN flood protection ☑

SYN flood rate 25

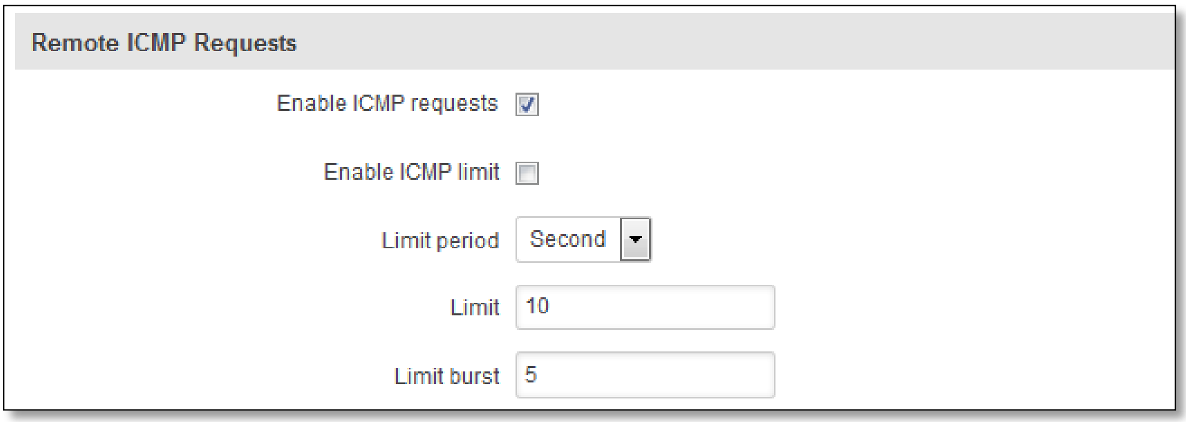
SYN flood burst 50

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).

7.5.6.2 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 Second

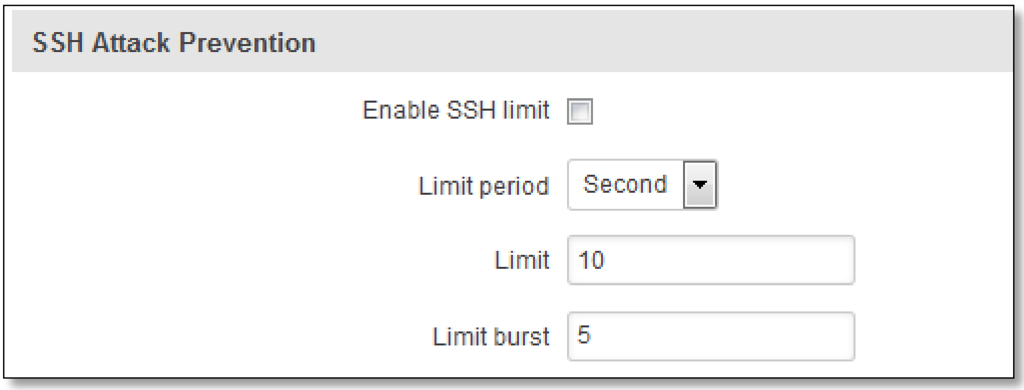
Limit 10

Limit burst 5

	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.

7.5.6.3 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: Second

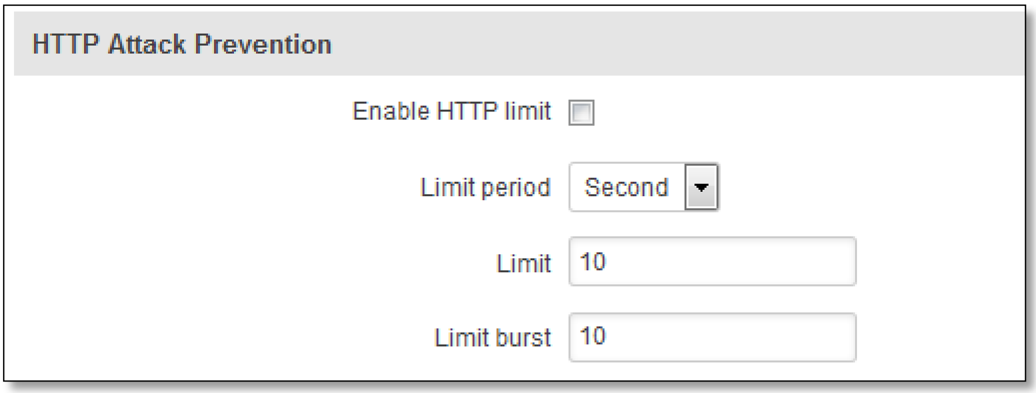
Limit: 10

Limit burst: 5

	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.

7.5.6.4 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 □

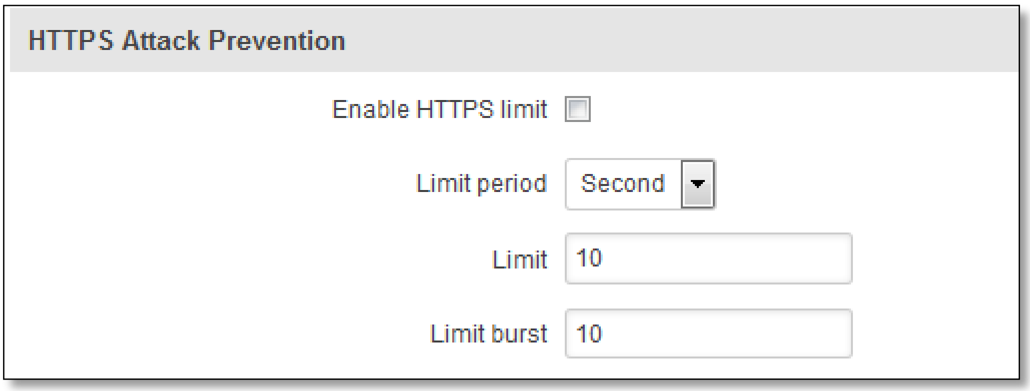
Limit period: Second

Limit: 10

Limit burst: 10

	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.

7.5.6.5 HTTPS Attack Prevention



HTTPS Attack Prevention

Enable HTTPS limit □

Limit period: Second

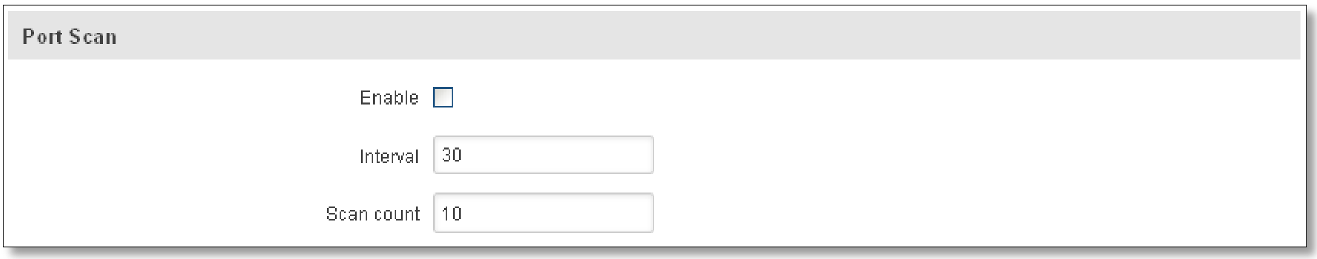
Limit: 10

Limit burst: 10

	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

7.5.7 Port Scan Prevention

7.5.7.1 Port Scan



Port Scan

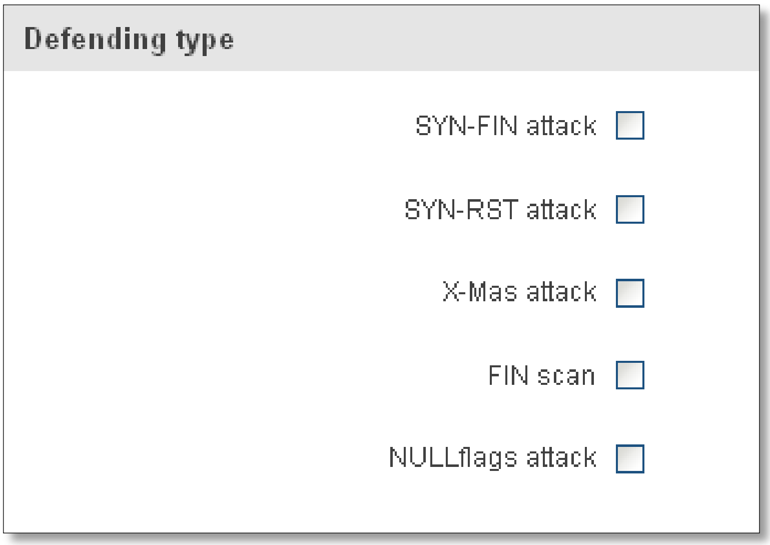
Enable □

Interval: 30

Scan count: 10

	Field Name	Sample value	Explanation
1.	Enable	Enable/Disable	Enable port scan prevention
2.	Interval	30	Time interval in seconds counting how much port scan (10 – 60 sec.)
3.	Scan count	10	How much port scan before blocked

7.5.7.2 Defending type



Defending type

SYN-FIN attack □

SYN-RST attack □

X-Mas attack □

FIN scan □

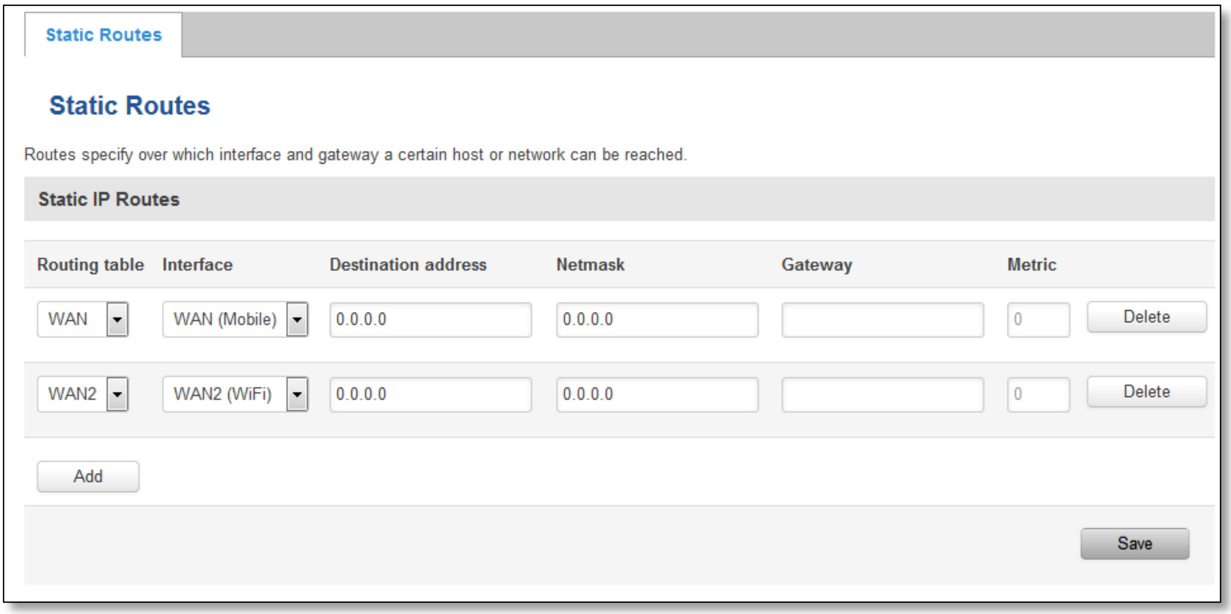
NULLflags attack □

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

7.6 Routing

7.6.1 Static Routes

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



Static Routes

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

Static IP Routes

Routing table	Interface	Destination address	Netmask	Gateway	Metric	
WAN	WAN (Mobile)	0.0.0.0	0.0.0.0		0	Delete
WAN2	WAN2 (WiFi)	0.0.0.0	0.0.0.0		0	Delete

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

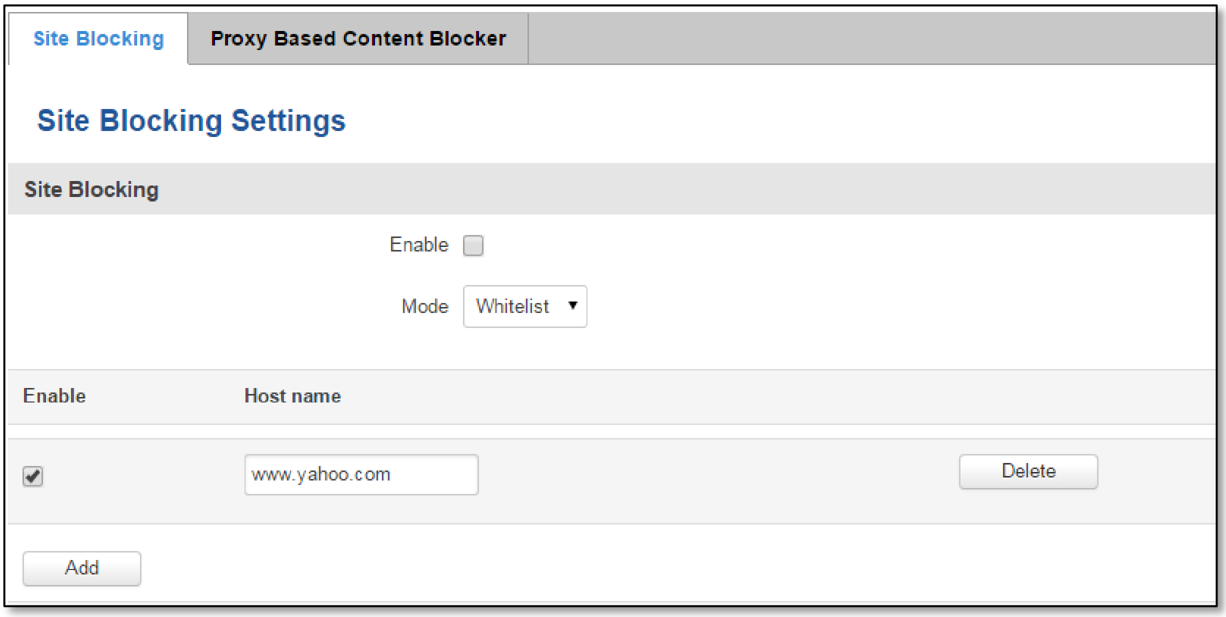
Additional note on Target & Netmask: You can define a rule that applies to a single IP like this: Target - some IP; Netmask - 255.255.255.255. Furthermore you can define a rule that applies to a segment of IPs like this: Target – some IP that STARTS the segment; Netmask – Netmask that defines how large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

8.1.1 Site blocking



Site Blocking | Proxy Based Content Blocker

Site Blocking Settings

Site Blocking

Enable □

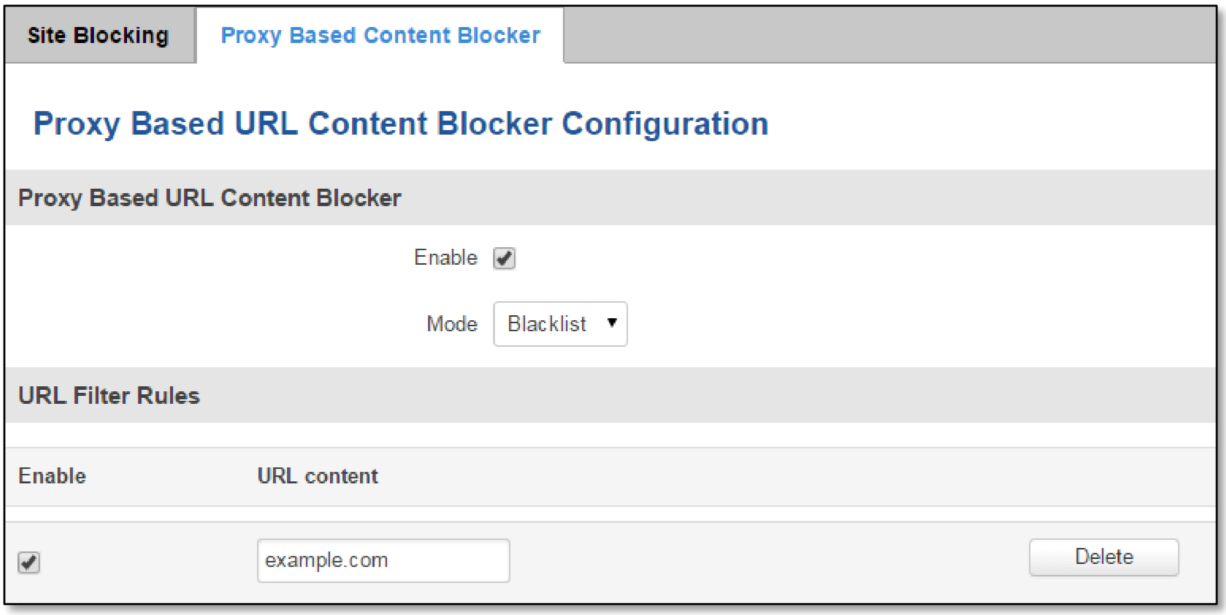
Mode Whitelist ▼

Enable	Host name	
☑	www.yahoo.com	Delete

Add

	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.
3.	Enable	Enable/Disable	Check to enable site blocking
4.	Host name	www.yahoo.com	Block/allow site with this hostname

8.1.2 Proxy Based Content Blocker



Site Blocking | Proxy Based Content Blocker

Proxy Based URL Content Blocker Configuration

Proxy Based URL Content Blocker

Enable ☑

Mode Blacklist ▼

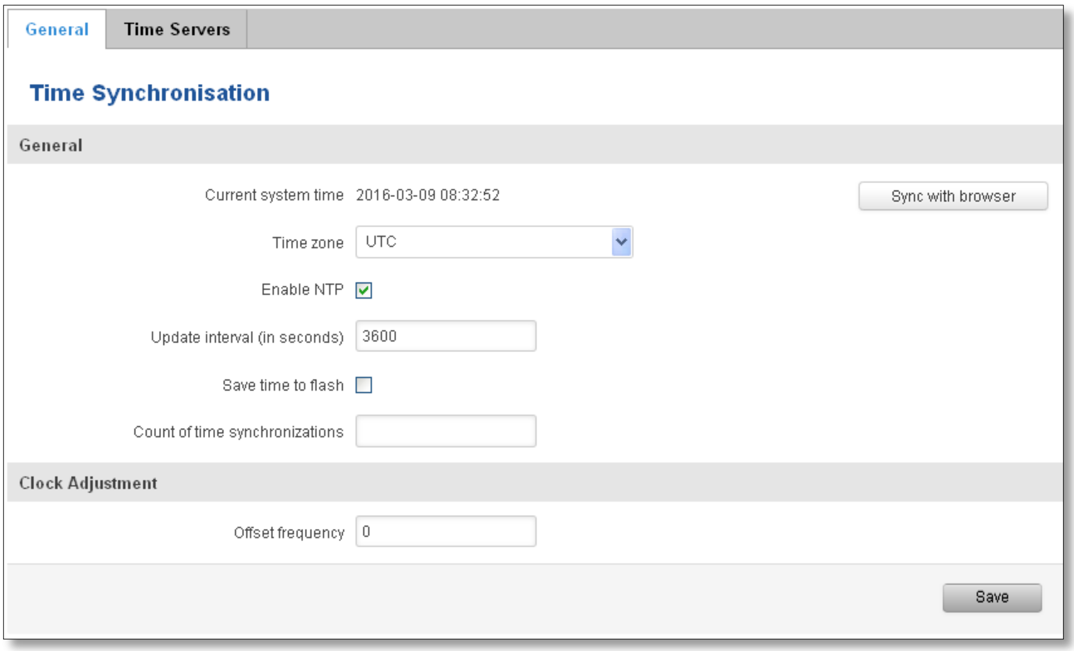
URL Filter Rules

Enable	URL content	
☑	example.com	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
3.	URL content	example.com	Block/allow any URL containing this string. Example.com, example.*, *.example.com

8.2 NTP

NTP configuration lets you setup and synchronize routers time.



Time Synchronisation

General

Current system time 2016-03-09 08:32:52

Time zone UTC

Enable NTP ☑

Update interval (in seconds) 3600

Save time to flash □

Count of time synchronizations

Clock Adjustment

Offset frequency 0

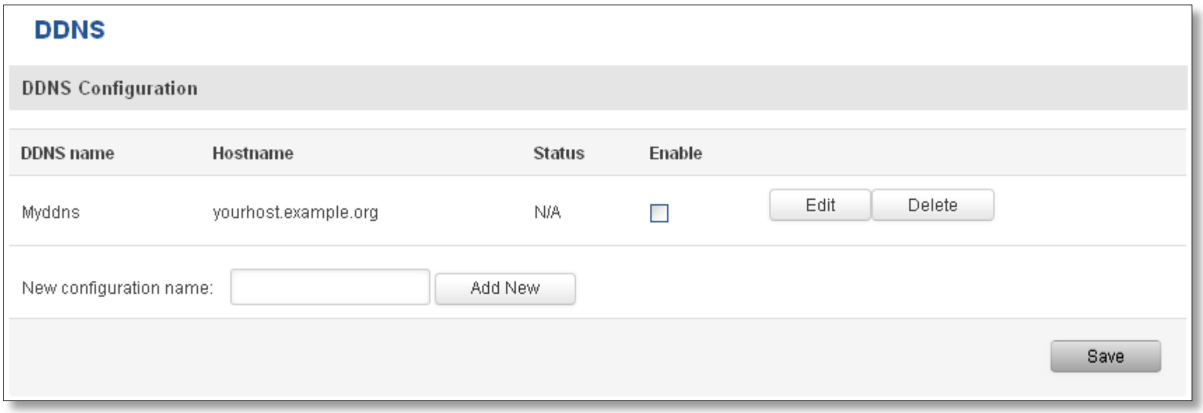
	Field name	Description
1.	Current System time	Local time of router.
2.	Time zone	Time zone of your country.
3.	Enable NTP	Enable system's time synchronization with time server using NTP (Network Time Protocol)
4.	Update interval	How often router updates systems time
5.	Save time to flash	Save last synchronized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

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

8.3 Dynamic DNS

Dynamic DNS (DDNS) is a domain name service allowing to link dynamic IP addresses to static hostname.
To start using this feature firstly you should register to DDNS service provider (example list is given in description).
You are provided with add/delete buttons to manage and use different DDNS configurations at the same time!

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



DDNS

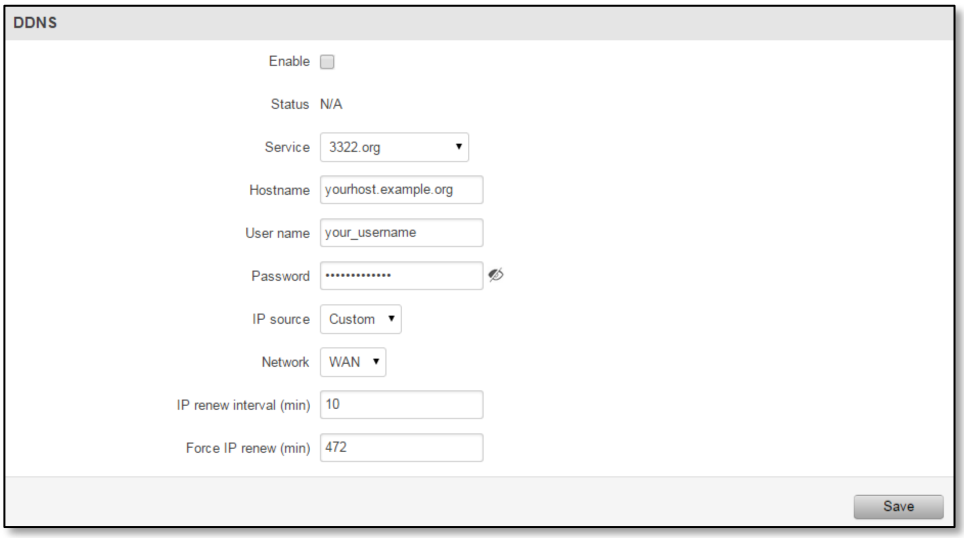
DDNS Configuration

DDNS name	Hostname	Status	Enable	
Myddns	yourhost.example.org	N/A	□	Edit Delete

New configuration name: Add New

Save

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



DDNS

Enable	□
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

Save

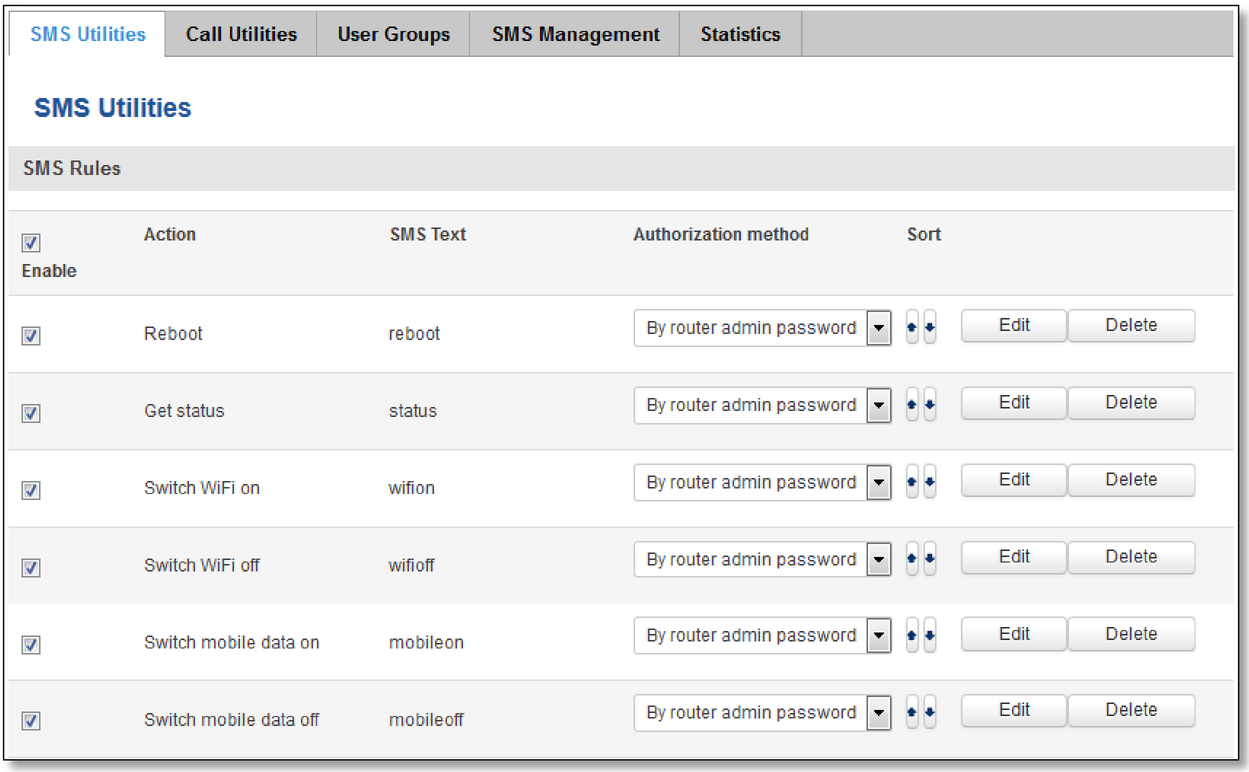
	Field name	Value	Explanation
1.	Enable	Enable/Disable	Enables current DDNS configuration.
2.	Status	N/A	Timestamp of the last IP check or update.
3.	Service	1. dydns.org 2. 3322.org 3. no-ip.com 4. easydns.com 5. zoneedit.com	Your dynamic DNS service provider selected from the list. In case your DDNS 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 interface), then you can send this exact IP to DDNS server by selecting "Private", or by selecting "Custom" and "WAN" interface. The DDNS server will then resolve hostname queries to this specific IP.
8.	Network	WAN	Source network
9.	IP renew interval (min)	10 (minutes)	Time interval (in minutes) to check if the IP address of the device have changed.
10.	Force IP renew	472 (minutes)	Time interval (in minutes) to force IP address renew.

8.4 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 and Statistics.

8.4.1 SMS Utilities



SMS Utilities

SMS Rules

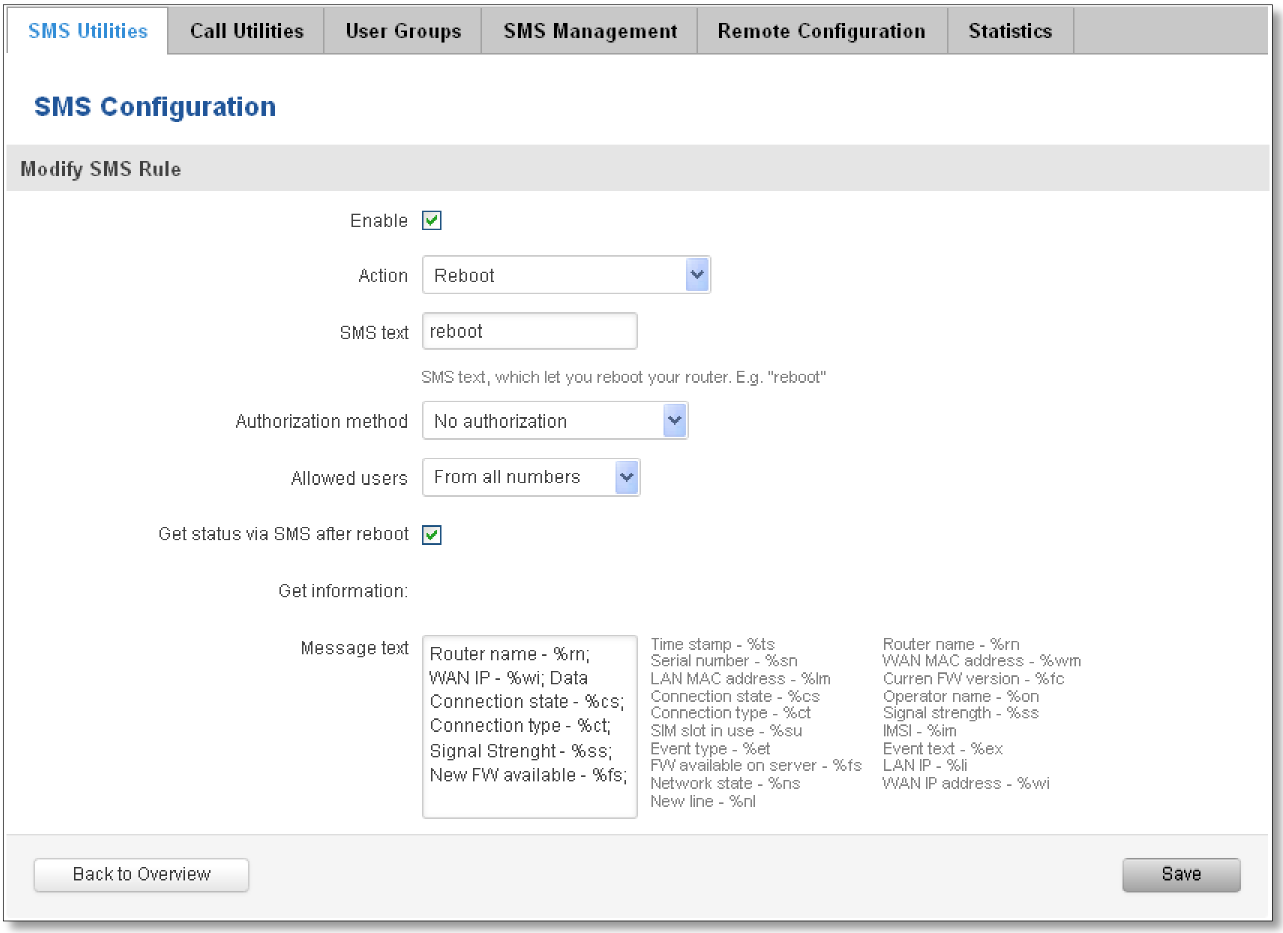
☑ Enable	Action	SMS Text	Authorization method	Sort		
☑	Reboot	reboot	By router admin password		Edit	Delete
☑	Get status	status	By router admin password		Edit	Delete
☑	Switch WiFi on	wifion	By router admin password		Edit	Delete
☑	Switch WiFi off	wifioff	By router admin password		Edit	Delete
☑	Switch mobile data on	mobileon	By router admin password		Edit	Delete
☑	Switch mobile data off	mobileoff	By router admin password		Edit	Delete

All configuration options are listed below:

- Reboot
- Get status
- Switch WiFi on/off
- Switch mobile data on/off
- Change mobile data settings
- Web access control
- Restore to default

- FW upgrade from server
- Config update from server
- Switch monitoring on/off
- Monitoring status

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



SMS Configuration

Modify SMS Rule

Enable ☑

Action: Reboot

SMS text: reboot

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

Authorization method: No authorization

Allowed users: From all numbers

Get status via SMS after reboot ☑

Get information:

Message text: Router name - %rn; WAN IP - %wi; Data Connection state - %cs; Connection type - %ct; Signal Strenght - %ss; New FW available - %fs;

Time stamp - %ts
Serial number - %sn
LAN MAC address - %lm
Connection state - %cs
Connection type - %ct
SIM slot in use - %su
Event type - %et
FW available on server - %fs
Network state - %ns
New line - %nl

Router name - %rn
WAN MAC address - %wm
Curren FW version - %fc
Operator name - %on
Signal strength - %ss
IMSI - %im
Event text - %ex
LAN IP - %li
WAN IP address - %wi

	Field name	Explanation	Notes
1.	**Reboot**		
	Enable	This check box will enable and disable SMS reboot function.	Allows router restart via SMS.
	Action	The action to be performed when this rule is met.	
	SMS text	SMS text which will reboot router.	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.
	Authorization method	What kind of authorization to use for SIM management.	No authorization, by serial or by router admin password.
	Allowed users	Whitelist of allow users	From all numbers, from group or from single number.
	Get status via SMS after reboot	Check this to recieve connection status via SMS after a reboot.	If you select this box, router will send status once it has rebooted and is operational again. This is both separate SMS Rule and an option under

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

	SMS text	SMS text which will turn mobile data ON/OFF.	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.
	Authorization method	What kind of authorization to use for SIM management.	No authorization, by serial or by router admin password.
	Allowed users	Whitelist of allow users	From all numbers, from group or from single number.
	Write to config	Permanently saves mobile network state.	With this setting enabled, router will keep mobile state even after reboot. If it is not selected, router will revert mobile state after reboot.
5.	**Change mobile data settings**		
	Enable	This check box will enable and disable this function.	Allows to change mobile settings via SMS.
	Action	The action to be performed when this rule is met.	
	SMS text	Key word that will precede actual configuration parameters.	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.
	Authorization method	What kind of authorization to use for SIM management.	No authorization, by serial or by router admin password.
	Allowed users	Whitelist of allow users	From all numbers, from group or from single number.

Mobile Settings via SMS parameters:

	Parameter	Value(s)	Explanation
1.	apn=	e.g. internet.gprs	Sets APN. i.e: apn=internet.gprs
2.	dialnumber=	e.g. *99***1#	Sets dial number
3.	auth_mode=	none pap chap	Sets authentication mode
4.	service=	Auto 4gonly 3gonly 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=*991#auth_mode=pap service=3gonly username=user password=user*

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 massages you receiving usually.

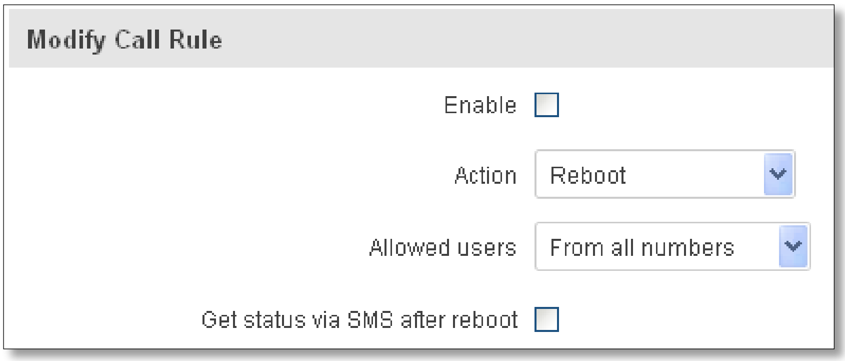
	Field name	Explanation	Notes
7.	**Web access Control**		
	Enable	This check box will enable and disable this function.	Allows Web access control via SMS.
	Action	The action to be performed when this rule is met.	
	SMS text	SMS text which will turn Web access ON/OFF.	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.
	Authorization method	What kind of authorization to use for SIM management.	No authorization, by serial or by router admin password.
	Allowed users	Whitelist of allow users	From all numbers, from group or from single number.
	Enable HTTP access	Enable this to reach router via HTTP from LAN (Local Area Network).	If this box is selected, SMS will enable HTTP access from LAN. If this box is not selected, SMS will disable HTTP access from LAN.
	Enable remote HTTP access	Enable this to reach router via HTTP from WAN (Wide Area Network).	If this box is selected, SMS will enable HTTP access from WAN. If this box is not selected, SMS will disable HTTP access from WAN.
	Enable remote HTTPS access	Enable this to reach router via HTTPS from WAN (Wide Area Network).	If this box is selected, SMS will enable HTTPS access from WAN. If this box is not selected, SMS will disable HTTPS access from WAN.
8.	**Restore to default**		
	Enable	This check box will enable and disable this function.	Allows to restore router to default settings via SMS.
	Action	The action to be performed when this rule is met.	Router will reboot after this rule is executed.
	SMS text	SMS text which will turn Wi-Fi ON/OFF.	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.
	Authorization method	What kind of authorization to use for SIM management.	No authorization, by serial or by router admin password.
	Allowed users	Whitelist of allow users	From all numbers, from group or from single number.
9.	**Switch monitoring on/off**		
	Enable	This check box will enable and disable this function.	Allows monitoring control via SMS.
	Action	The action to be performed when this rule is met.	Turn monitoring ON or OFF.
	SMS text	SMS text which will turn monitoring ON/OFF	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.
	Authorization method	What kind of authorization to use for SIM management.	By serial or by router admin password.
	Allowed users	Whitelist of allow users	From all uers, from group or from single number.

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 massages you receiving usually.

8.4.2 Call Utilities

Allow users to call to the router in order to perform one of the actions: Reboot, Get Status, turn Wi-Fi ON/OFF, turn Mobile data ON/OFF. Only thing that is needed is to call routers SIM card number from allowed phone (user) and RUT9 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 □

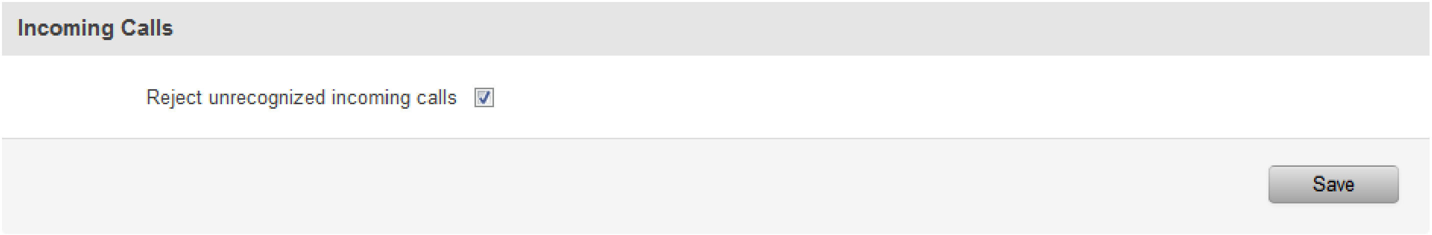
Action: Reboot

Allowed users: From all numbers

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 Wi-Fi, Switch mobile data.
3.	Allowed users	From all numbers	Allows to limit action triggering from all users, to user groups or single user numbers
4.	Get status via SMS after reboot	Enable/Disable	Enables automatic message sending with router status information after reboot

8.4.2.1 Incoming Calls



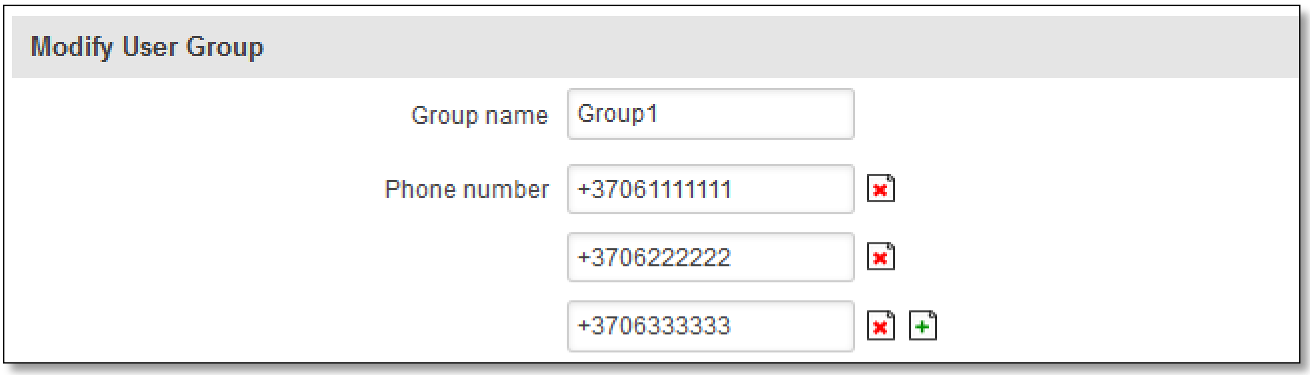
Incoming Calls

Reject unrecognized incoming calls ☑

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

8.4.3 User Groups

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



Modify User Group

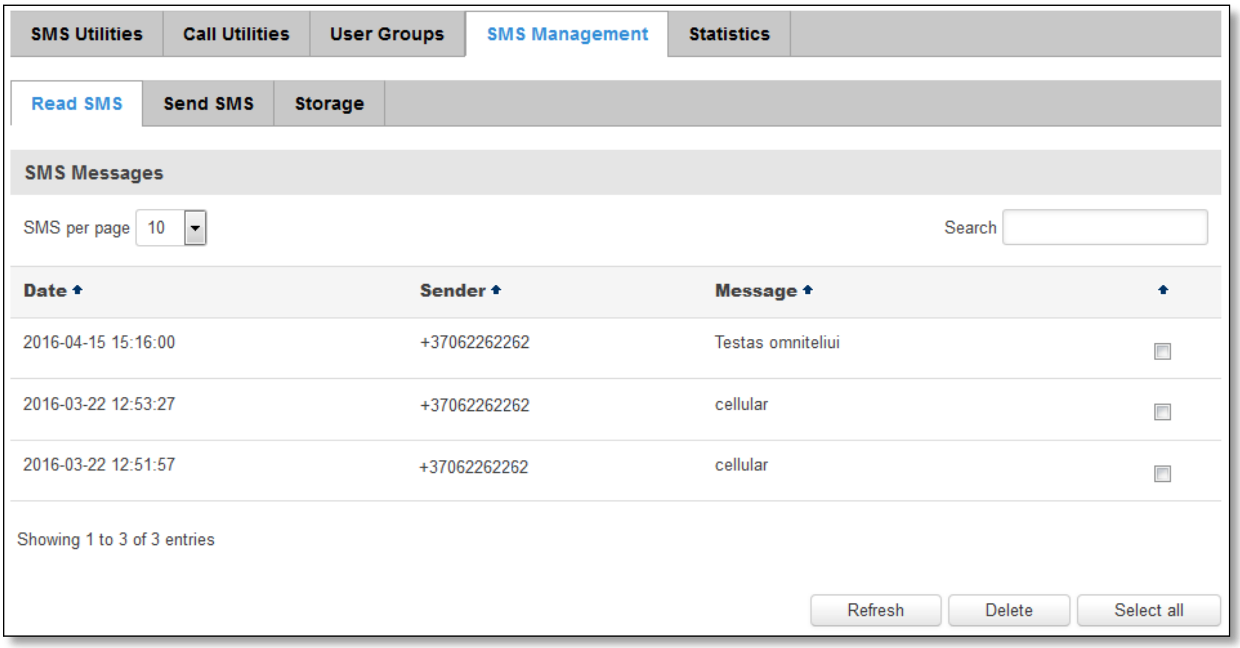
Group name	Group1
Phone number	+37061111111
	+3706222222
	+3706333333

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

8.4.4 SMS Management

8.4.4.1 Read SMS

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



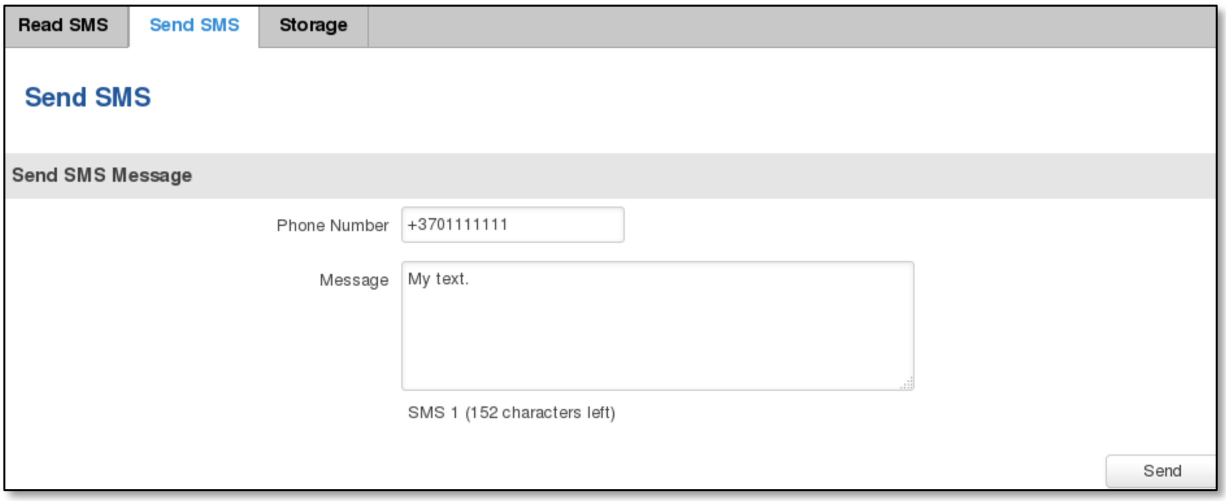
SMS Messages

SMS per page 10 Search

Date	Sender	Message	
2016-04-15 15:16:00	+37062262262	Testas omniteliui	□
2016-03-22 12:53:27	+37062262262	cellular	□
2016-03-22 12:51:57	+37062262262	cellular	□

Showing 1 to 3 of 3 entries

8.4.4.2 Send SMS



Send SMS

Send SMS Message

Phone Number: +3701111111

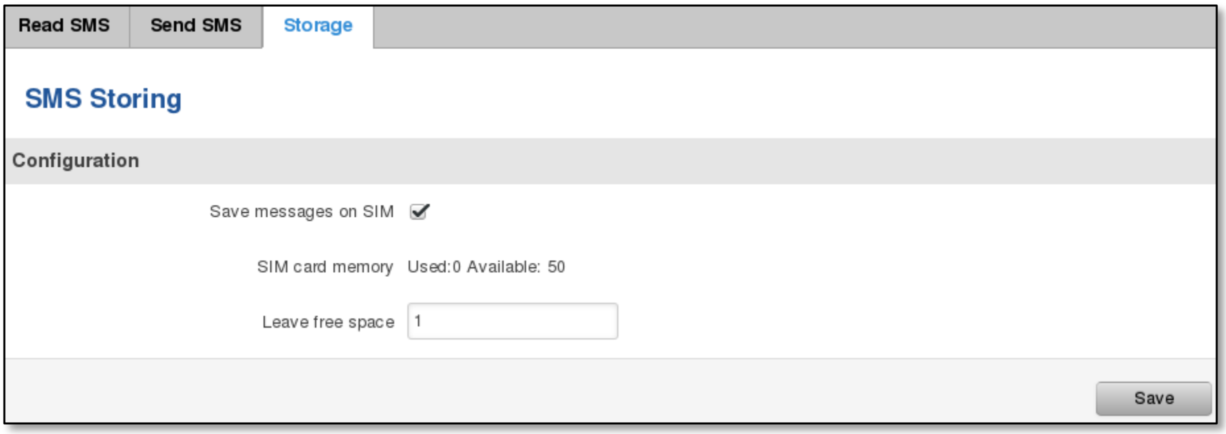
Message: My text.

SMS 1 (152 characters left)

	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.

8.4.4.3 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.



SMS Storing

Configuration

Save messages on SIM ☑

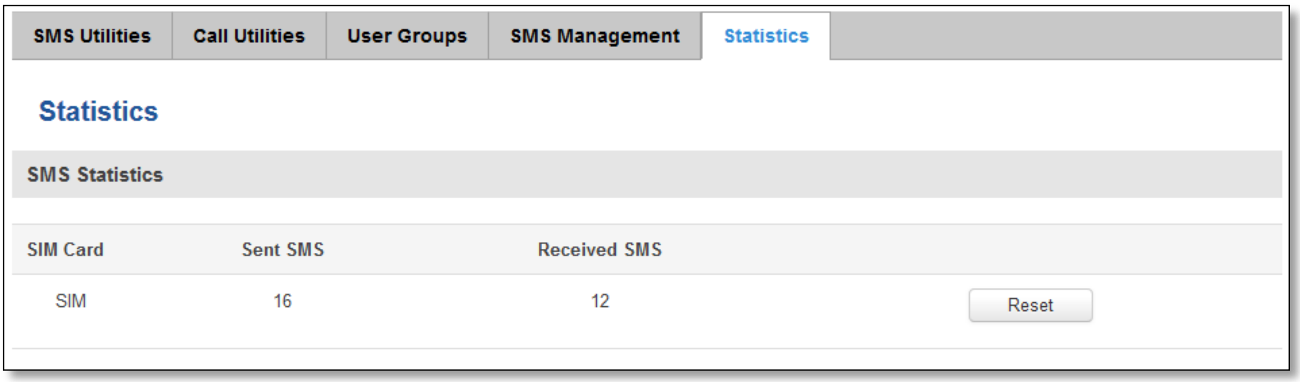
SIM card memory Used:0 Available: 50

Leave free space 1

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

8.4.5 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.



Statistics

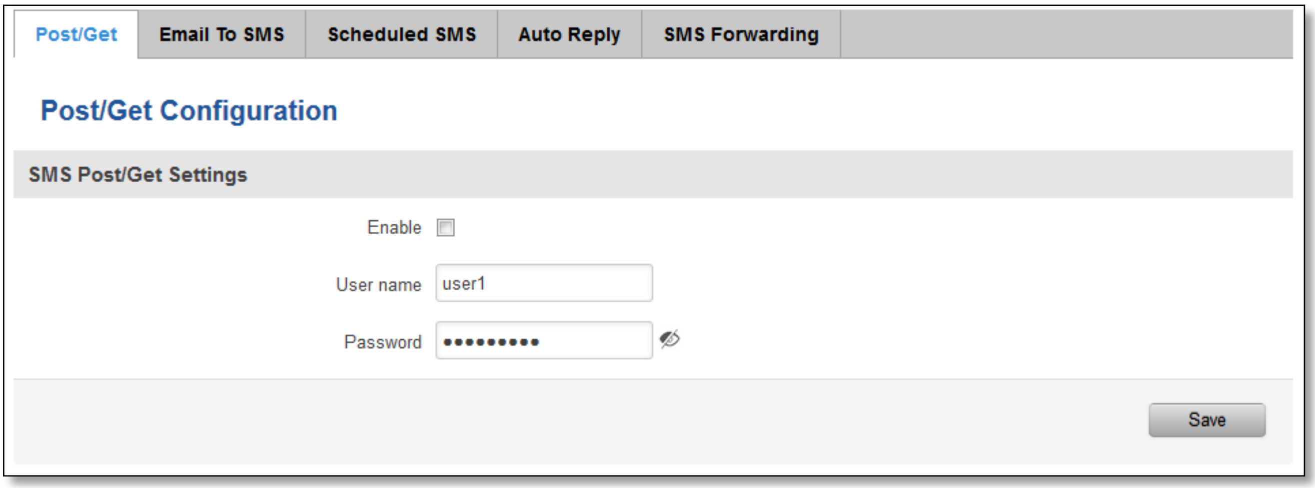
SMS Statistics

SIM Card	Sent SMS	Received SMS	
SIM	16	12	Reset

8.5 SMS Gateway

8.5.1 Post/Get Configuration

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



Post/Get Configuration

SMS Post/Get Settings

Enable □

User name user1

Password ●●●●●●●●●

	Field name	Values	Notes
1.	Enable	Enabled / Disabled	Enable SMS management functionality through POST/GET
2.	User name	user1	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!

8.5.1.1 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=0037060000001&text=testmessage
4.	View mobile messages total	/cgi-bin/sms_total?username=admin&password=admin01
5.	Delete mobile message	/cgi-bin/sms_delete?username=admin&password=admin01&number=1

8.5.1.2 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
	/cgi-bin/sms_send? username={your_user_name}&password={your_password}&number={PHONE_NUMBER}&text={MESSAGE_TEXT}	Send message
	/cgi-bin/sms_delete? username={your_user_name}&password={your_password}&number={MESSAGE_INDEX}	Delete message
	/cgi-bin/ sms_list? username={your_user_name}&password={your_password}	List all messages
	/cgi-bin/sms_ total? username={your_user_name}&password={your_password}	Number of messages in memory

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

8.5.1.3 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.

8.5.1.4 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

8.5.1.5 HTTP POST/GET string examples

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

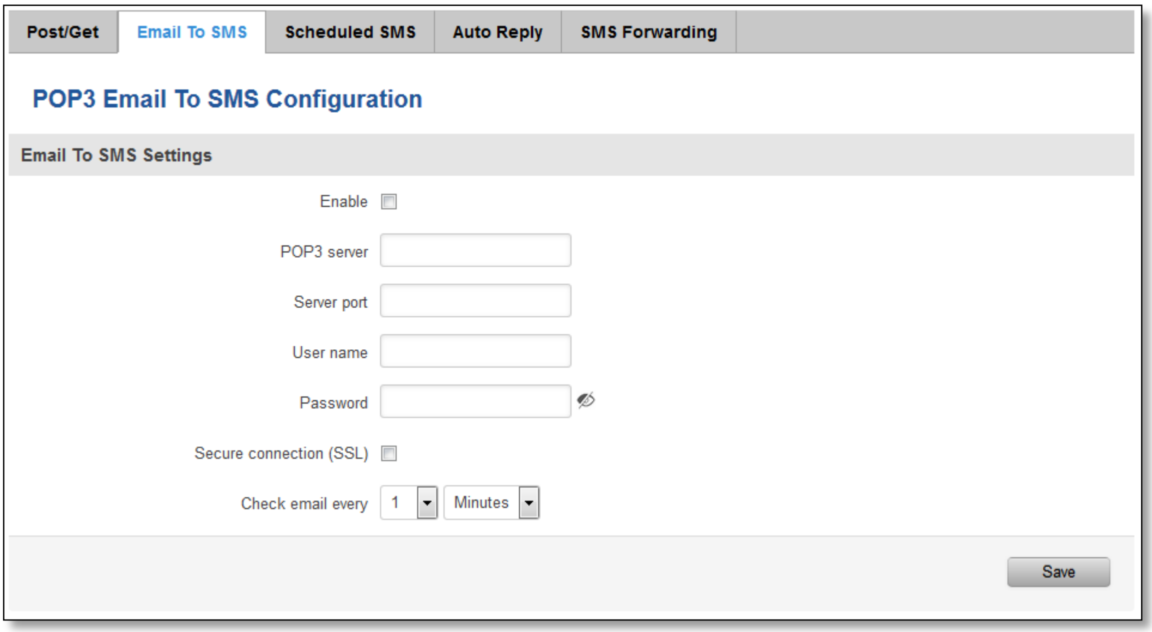
http://192.168.1.1/cgi-bin/sms_send?username=admin&password=admin01&number=0037060000001&text=message

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

http://192.168.1.1 /cgi-bin/sms_list?username=admin&password=admin01

http://192.168.1.1/cgi-bin/sms_total?username=admin&password=admin01

8.5.2 Email to SMS



POP3 Email To SMS Configuration

Email To SMS Settings

Enable □

POP3 server

Server port

User name

Password

Secure connection (SSL) □

Check email every 1 Minutes

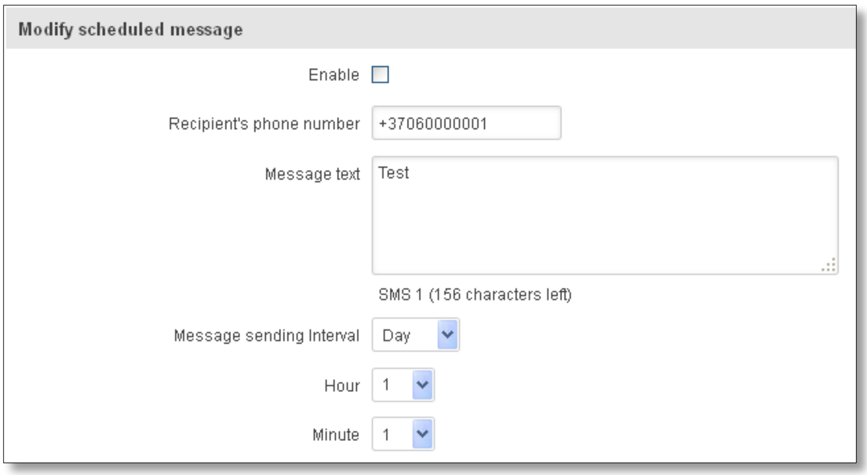
	Field name	Values	Notes
1.	Enable	Enable/Disable	Allows to convert received Email to SMS
2.	POP3 server	"pop.gmail.com"	POP3 server address
3.	Server port	"995"	Server authentication port
4.	User name	"admin"	User name using for server authentication
5.	Password	"admin01"	Password using for server authentication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

8.5.3 Scheduled Messages

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

8.5.3.1 Scheduled Messages Configuration



Modify scheduled message

Enable □

Recipient's phone number +37060000001

Message text Test

SMS 1 (156 characters left)

Message sending Interval Day

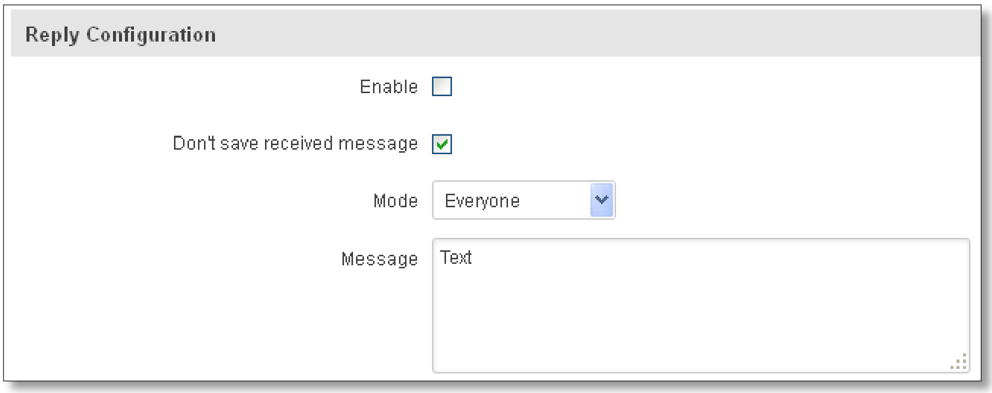
Hour 1

Minute 1

	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.

8.5.4 Auto Reply Configuration

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



Reply Configuration

Enable □

Don't save received message ☑

Mode Everyone

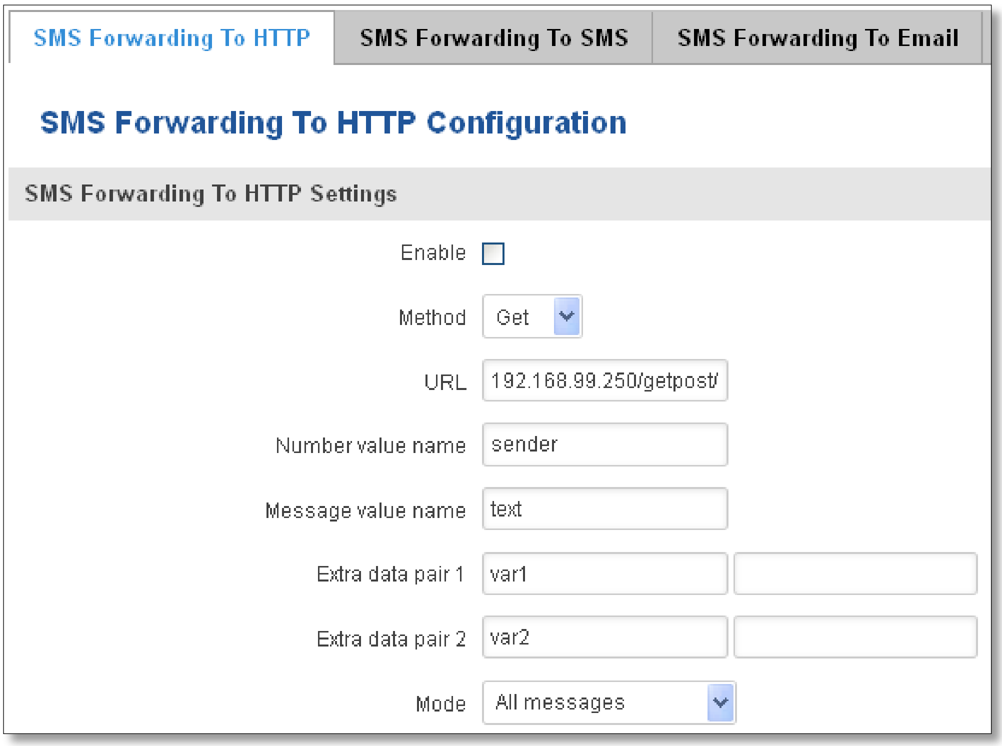
Message Text

	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.

8.5.5 SMS Forwarding

8.5.5.1 SMS Forwarding To HTTP

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



SMS Forwarding To HTTP Configuration

SMS Forwarding To HTTP Settings

Enable □

Method Get

URL 192.168.99.250/getpost/

Number value name sender

Message value name text

Extra data pair 1 var1

Extra data pair 2 var2

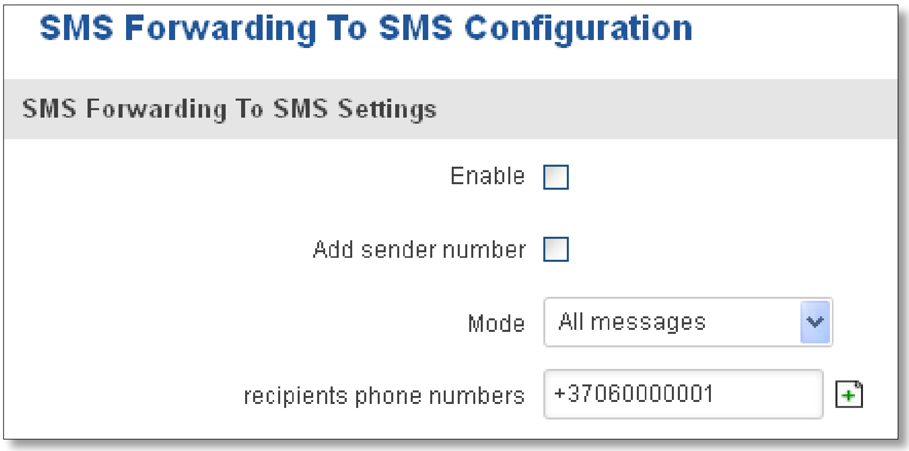
Mode All messages

	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

8.5.5.2 SMS Forwarding to SMS

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



SMS Forwarding To SMS Configuration

SMS Forwarding To SMS Settings

Enable □

Add sender number □

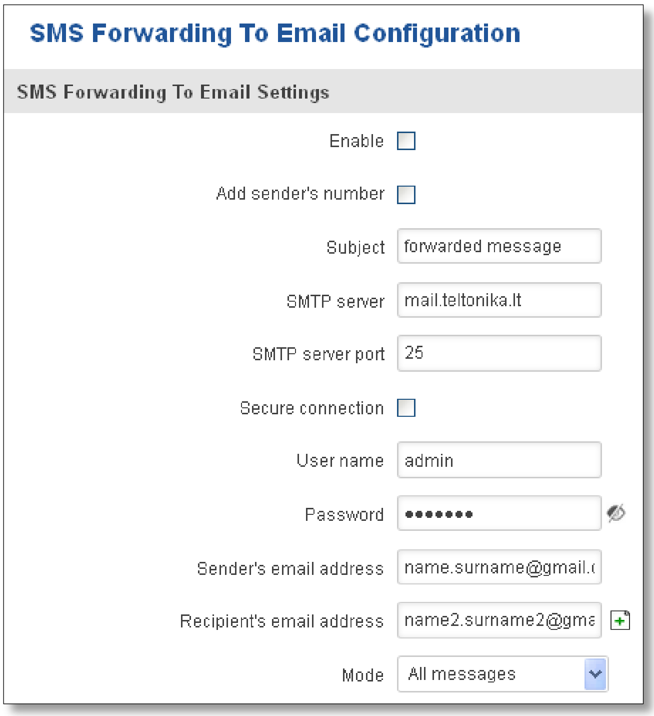
Mode: All messages

recipients phone numbers: +37060000001

	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

8.5.5.3 SMS Forwarding to Email

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



SMS Forwarding To Email Configuration

SMS Forwarding To Email Settings

Enable □

Add sender's number □

Subject: forwarded message

SMTP server: mail.teltonika.lt

SMTP server port: 25

Secure connection □

User name: admin

Password: •••••••

Sender's email address: name.surname@gmail.(

Recipient's email address: name2.surname2@gma

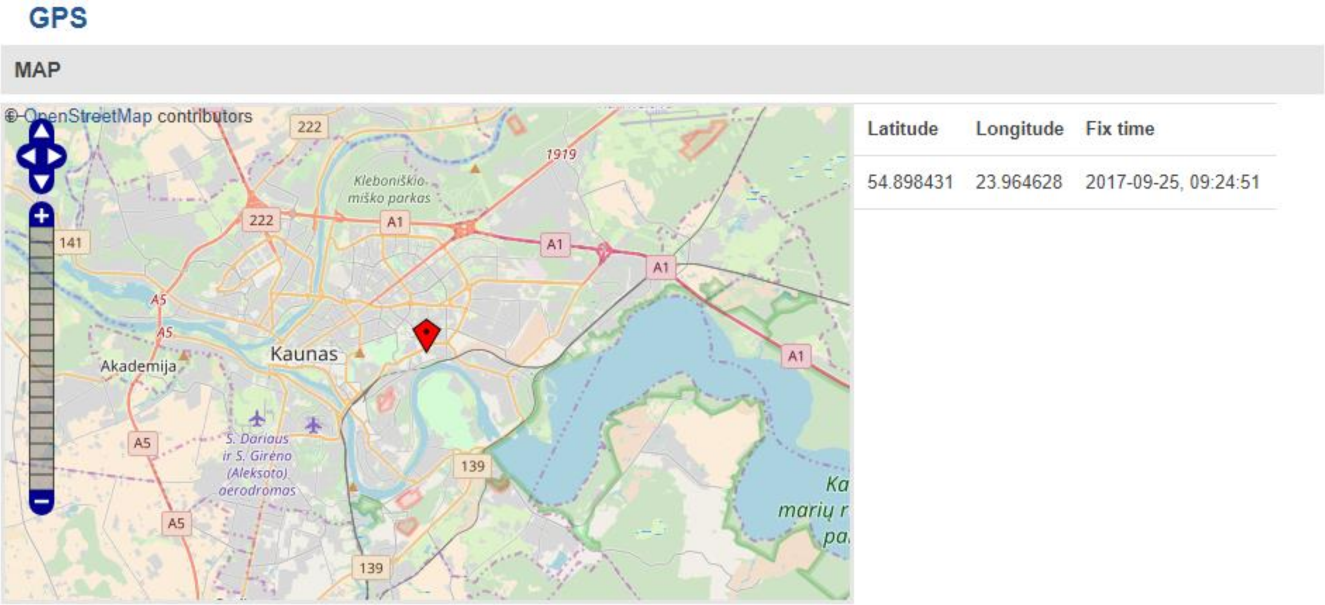
Mode: All messages

	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.lt	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

8.6 GPS

8.6.1 GPS

The GPS window displays your current coordinates and position on the map.



GPS

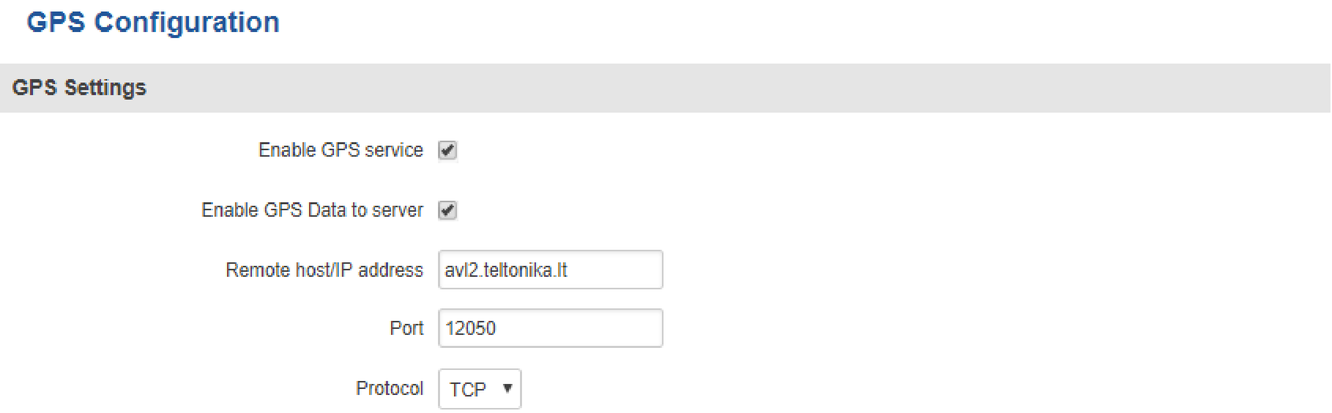
MAP

© OpenStreetMap contributors
Kaunas
Akademija
Kleboniškio miško parkas
S. Dariaus ir S. Girėno (Aleksoto) aerodromas
Kauno marių regioninis parkas
A1
A5
141
222
139
1919

Latitude	Longitude	Fix time
54.898431	23.964628	2017-09-25, 09:24:51

8.6.2 GPS Settings

This is the GPS parameter configuration window.



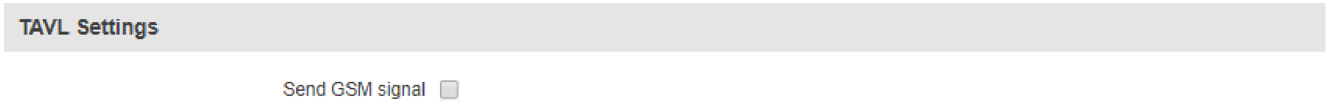
GPS Configuration

GPS Settings

Enable GPS service	☑
Enable GPS Data to server	☑
Remote host/IP address	avl2.teltonika.lt
Port	12050
Protocol	TCP ▾

	Field name	Values	Notes
1.	Enable GPS service	Checked / Unchecked	Enables the GPS function
2.	Enable GPS Data to server	Checked / Unchecked	Enables automatic GPS data transferring to a remote server
3.	Remote host / IP address	Any IP address or hostname	Server IP address or domain name to send the coordinates to
4.	Port	0 - 65535	Server port used for data transfer
5.	Protocol	TCP / UDP	Protocol to be used for data transfer to server

8.6.2.1 TAVL Settings

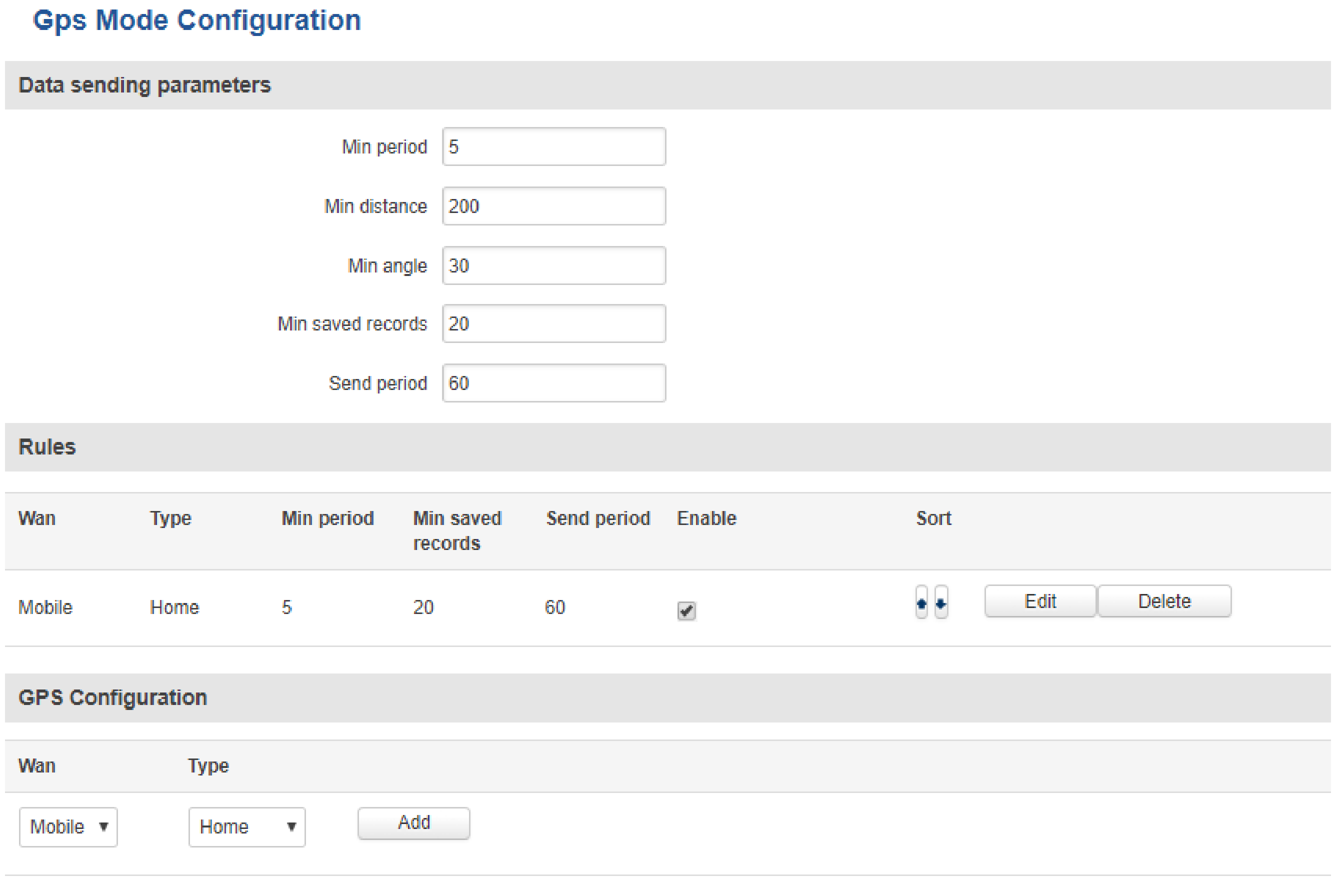


TAVL Settings

Send GSM signal □

	Field name	Values	Notes
1.	Send GSM signal	Checked / Unchecked	Check to include GSM signal strength information in GPS data package to be sent to server

8.6.3 GPS Mode



Gps Mode Configuration

Data sending parameters

Min period: 5

Min distance: 200

Min angle: 30

Min saved records: 20

Send period: 60

Rules

Wan	Type	Min period	Min saved records	Send period	Enable	Sort		
Mobile	Home	5	20	60	☑	↑ ↓	Edit	Delete

GPS Configuration

Wan	Type	
Mobile ▾	Home ▾	Add

Data sending

	Field name	Sample value	Notes
1.	Min period	5	Period (in seconds) for data collection
2.	Min distance	200	Distance difference (in meters) between last registered and current coordinates to collect data (even if Min period has not passed yet)
3.	Min angle	30	Minimal angle difference between last registered and current coordinates to collect data (even if Min period has not passed yet)
4.	Min saved records	20	Minimal amount of coordinates registered to send them to server immediately (even if Send period has not passed yet)
5.	Send period	60	Period for sending collected data to server

Rules

This table shows created GPS rules for data sending.

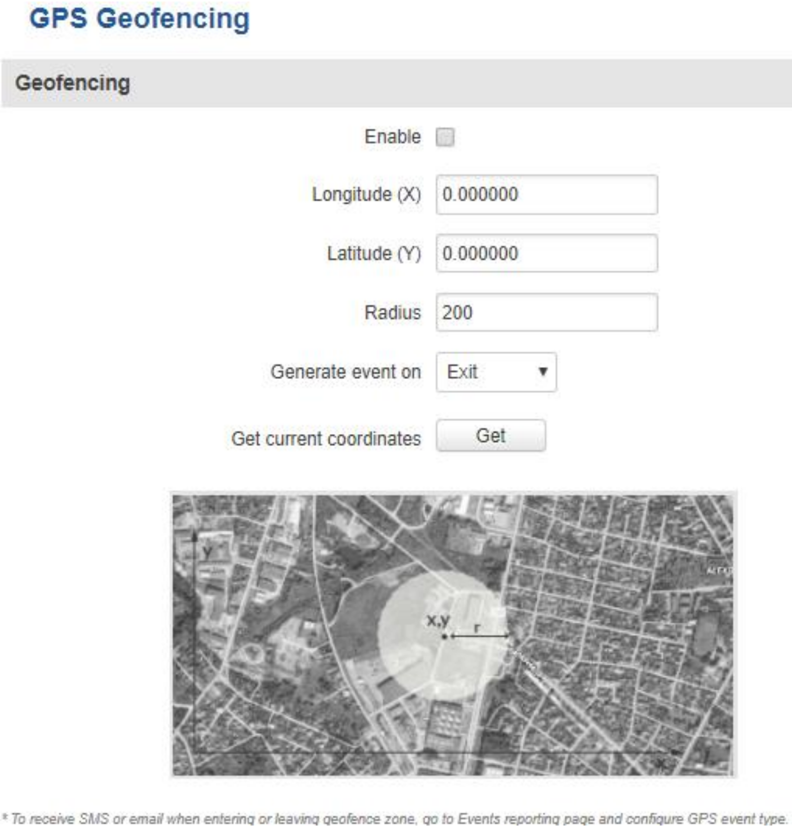
GPS Configuration

GPS configuration section allows to save several different configurations for GPS data collection. Active configuration is automaticaly selected when configured conditions are met.

	Field name	Values	Notes
1.	WAN	Mobile / Wired / WiFi	Interface which needs to be used to activate this configuration
2.	Type	Home / Roaming / Both	Mobile connection state needed to activate this configuration

8.6.4 GPS Geofencing

Geofencing is a feature that lets you define an area on the world map for which you can later customize rules that inform you whenever your device leaves or enters said area.



GPS Geofencing

Geofencing

Enable ☐

Longitude (X) 0.000000

Latitude (Y) 0.000000

Radius 200

Generate event on Exit ▾

Get current coordinates Get

* To receive SMS or email when entering or leaving geofence zone, go to Events reporting page and configure GPS event type.

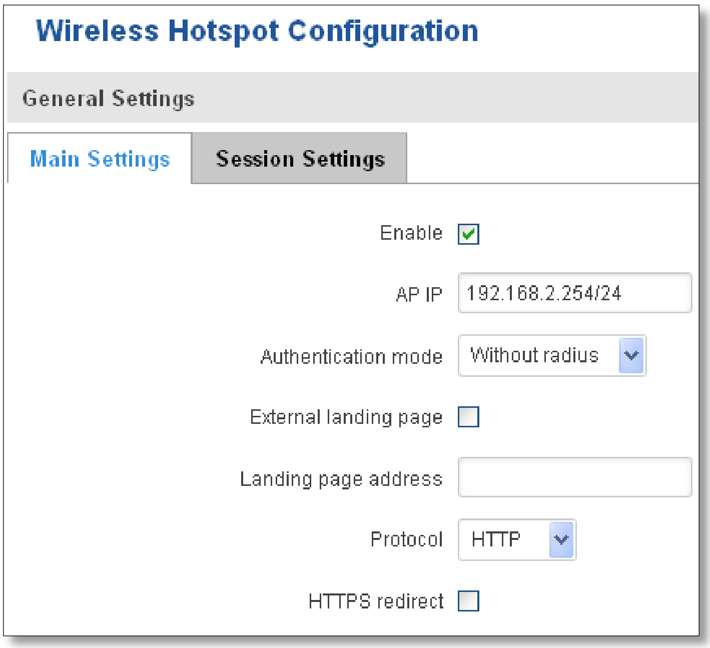
	Field name	Notes
1.	Enable	Enable/Disable GPS Geofencing functionality
2.	Longitude (X)	Longitude of selected point
3.	Latitude (Y)	Latitude of selected point
4.	Radius	Radius of selected area
5.	Generate event on	Generates an event either when the router leaves or enters the defined area
6.	Get current coordinates	Get current device coordinates from GPS

8.7 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.).

8.7.1 General settings

8.7.1.1 Main settings



Wireless Hotspot Configuration

General Settings

Main Settings | Session Settings

Enable ☑

AP IP 192.168.2.254/24

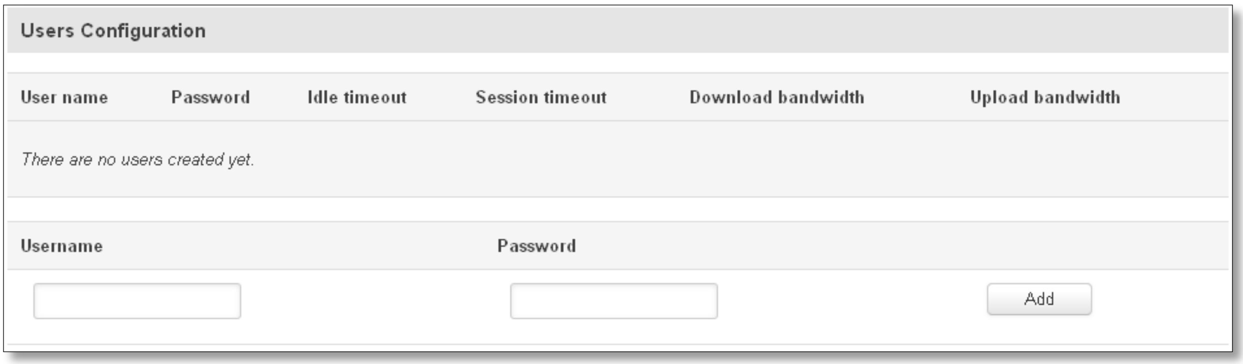
Authentication mode Without radius

External landing page □

Landing page address

Protocol HTTP

HTTPS redirect □



Users Configuration

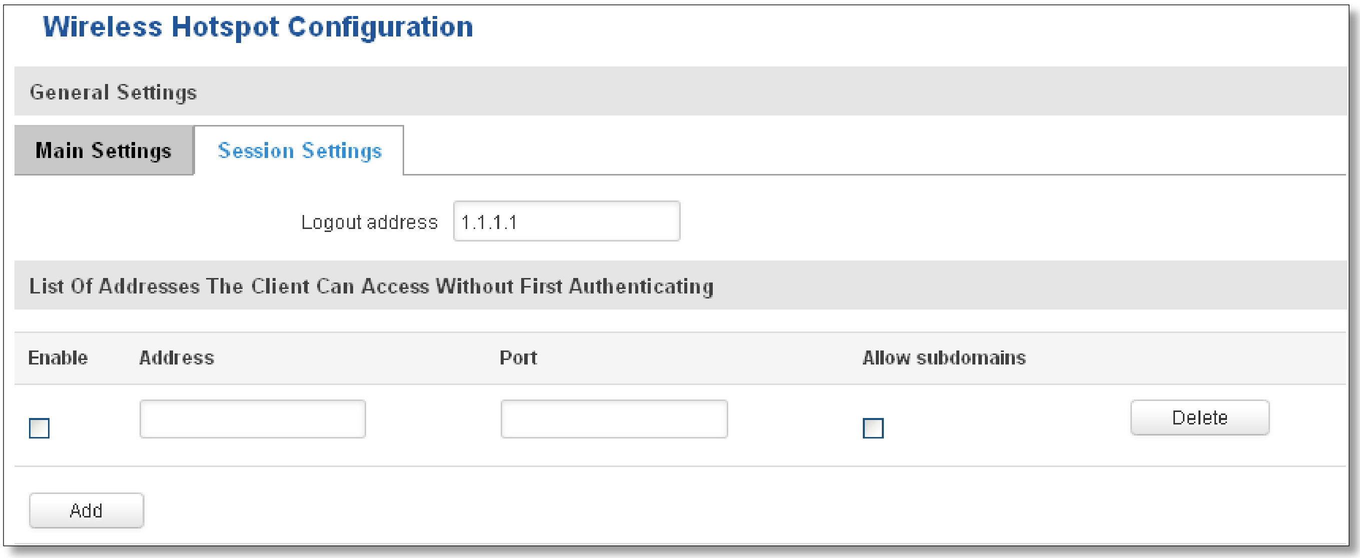
User name	Password	Idle timeout	Session timeout	Download bandwidth	Upload bandwidth
There are no users created yet.					

Username | Password

	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).

<table>
<tr><th colspan="3">Authentication mode: External radius</th></tr>
<tr><td>1.</td><td>Terms of Service</td><td>Client device will be able to access the Internet after agreeing Term of Service (ToS)</td></tr>
<tr><td>2.</td><td>Radius server #1</td><td>The IP address of the RADIUS server that is to be used for Authenticating your wireless clients.</td></tr>
<tr><td>3.</td><td>Radius server #2</td><td>The IP address of the second RADIUS server.</td></tr>
<tr><td>4.</td><td>Authentication port</td><td>RADIUS server authentication port.</td></tr>
<tr><td>5.</td><td>Accounting port</td><td>RADIUS server accounting port.</td></tr>
<tr><td>6.</td><td>Radius secret key</td><td>The secret key is used for authentication with the RADIUS server</td></tr>
<tr><td>7.</td><td>UAM port</td><td>Port to bind for authenticating clients</td></tr>
<tr><td>8.</td><td>UAM UI port</td><td>UAM UI port</td></tr>
<tr><td>9.</td><td>UAM secret</td><td>Shared secret between UAM server an hotspot</td></tr>
<tr><td>10.</td><td>NAS Identifier</td><td>NAS Identifier</td></tr>
<tr><td>11.</td><td>Swap octets</td><td>Swap the meaning of input octets and output as it related to RADIUS attributes</td></tr>
<tr><td>12.</td><td>Location name</td><td>The name of location</td></tr>
<tr><td>13.</td><td>External landing page</td><td>Use external landing page</td></tr>
<tr><td>14.</td><td>Protocol</td><td>Protocol to be used for landing page</td></tr>
<tr><td>15.</td><td>HTTPS redirect</td><td>Redirects HTTP pages to landing page.</td></tr>
<tr><th colspan="3">Authentication mode: Internal radius/Without radius</th></tr>
<tr><td>1.</td><td>Terms of Service</td><td>Client device will be able to access the Internet after agreeing Term of Service (ToS)</td></tr>
<tr><td>1.</td><td>External landing page</td><td>Enables the use of external landing page.</td></tr>
<tr><td>2.</td><td>Protocol</td><td>Protocol to be used for landing page</td></tr>
<tr><td>3.</td><td>HTTPS redirect</td><td>Redirects HTTP pages to landing page.</td></tr>
<tr><th colspan="3">Authentication mode: Advertisement</th></tr>
<tr><td>1.</td><td>Advertisement address</td><td>Advertisement address(http://www.example.com)</td></tr>
<tr><td>2.</td><td>HTTPS redirect</td><td>Redirects HTTP pages to landing page.</td></tr>
<tr><th colspan="3">Authentication mode: MAC auth</th></tr>
<tr><td>1.</td><td>Terms of Service</td><td>Client device will be able to access the Internet after agreeing Term of Service (ToS)</td></tr>
<tr><td>2.</td><td>Password protection</td><td>Client device will be able to access the internet after entering the password</td></tr>
<tr><td>3.</td><td>Website access</td><td>Requested website access mode (Link/Auto redirect)</td></tr>
<tr><td>4.</td><td>Protocol</td><td>Protocol to be used for landing page</td></tr>
<tr><td>5.</td><td>HTTPS redirect</td><td>Redirects HTTP pages to landing page.</td></tr>
<tr><th colspan="3">Authentication mode: SMS OTP</th></tr>
<tr><td>1.</td><td>Protocol</td><td>Protocol to be used for landing page</td></tr>
<tr><td>2.</td><td>HTTPS redirect</td><td>Redirects HTTP pages to landing page.</td></tr>
</table>

8.7.1.2 Session settings



Wireless Hotspot Configuration

General Settings

Logout address: 1.1.1.1

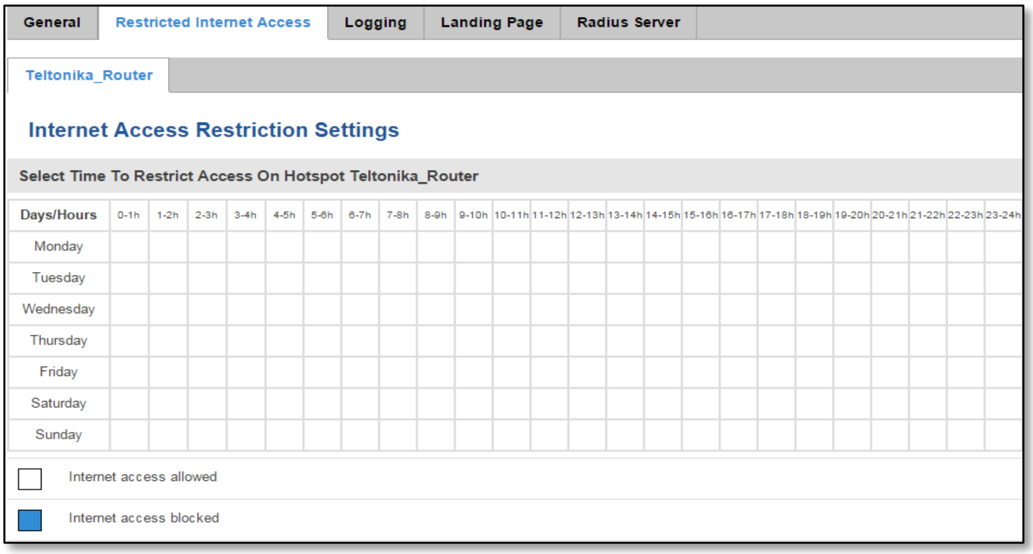
List Of Addresses The Client Can Access Without First Authenticating

Enable	Address	Port	Allow subdomains	
☐			☐	Delete

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

8.7.2 Internet Access Restriction Settings

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



Internet Access Restriction Settings

Select Time To Restrict Access On Hotspot Teltonika_Router

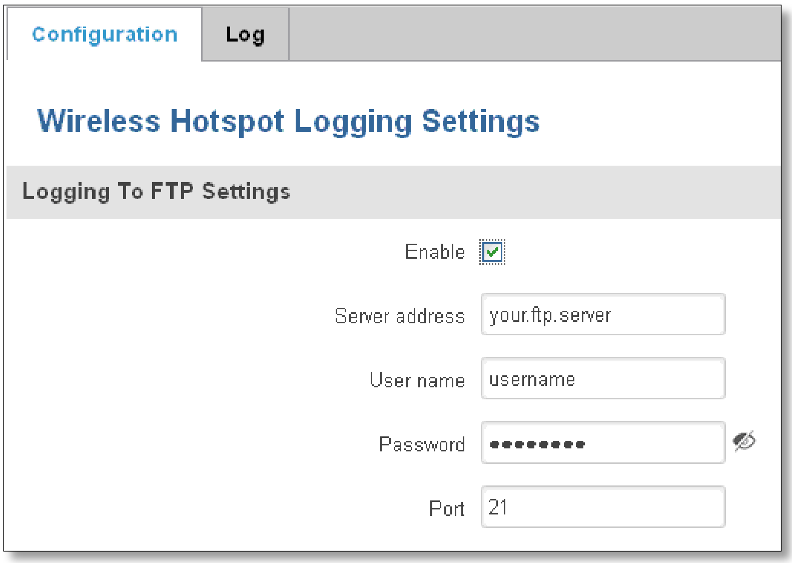
Days/Hours	0-1h	1-2h	2-3h	3-4h	4-5h	5-6h	6-7h	7-8h	8-9h	9-10h	10-11h	11-12h	12-13h	13-14h	14-15h	15-16h	16-17h	17-18h	18-19h	19-20h	20-21h	21-22h	22-23h	23-24h
Monday																								
Tuesday																								
Wednesday																								
Thursday																								
Friday				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

☐ Internet access allowed

🟦 Internet access blocked

8.7.3 Logging

8.7.3.1 Configuration



Wireless Hotspot Logging Settings

Logging To FTP Settings

Enable ☑

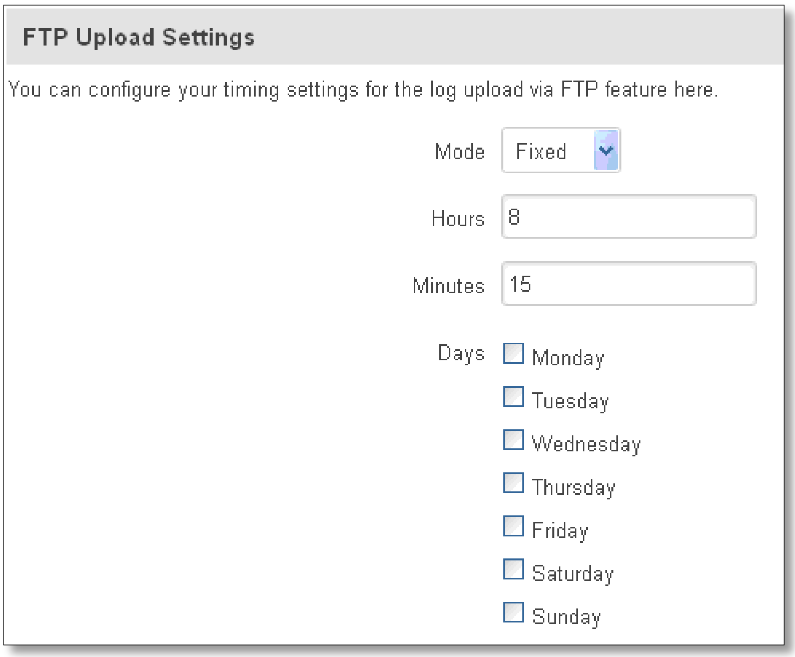
Server address your.ftp.server

User name username

Password ●●●●●●●●●

Port 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 Fixed

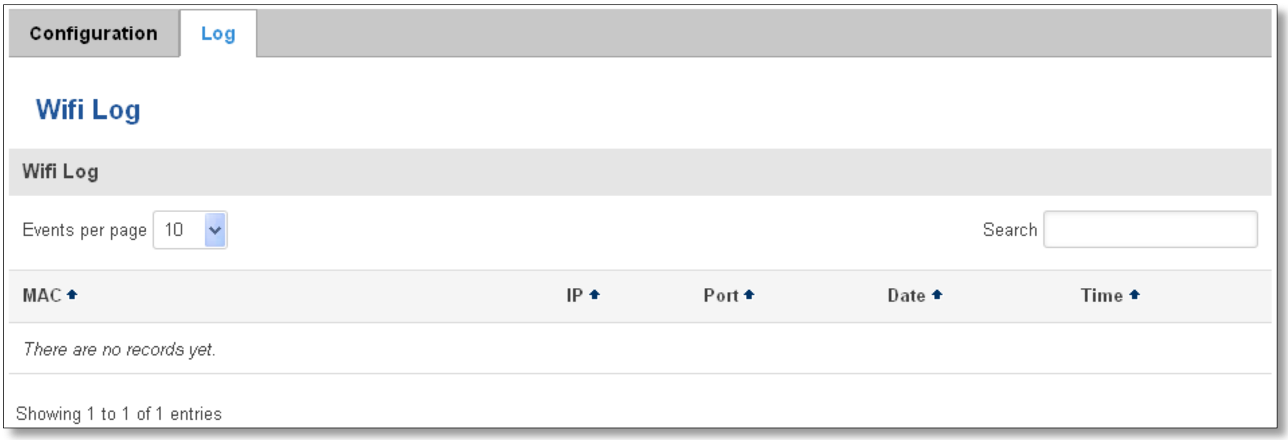
Hours 8

Minutes 15

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

8.7.3.2 Log



Wifi Log

Wifi Log

Events per page 10

Search

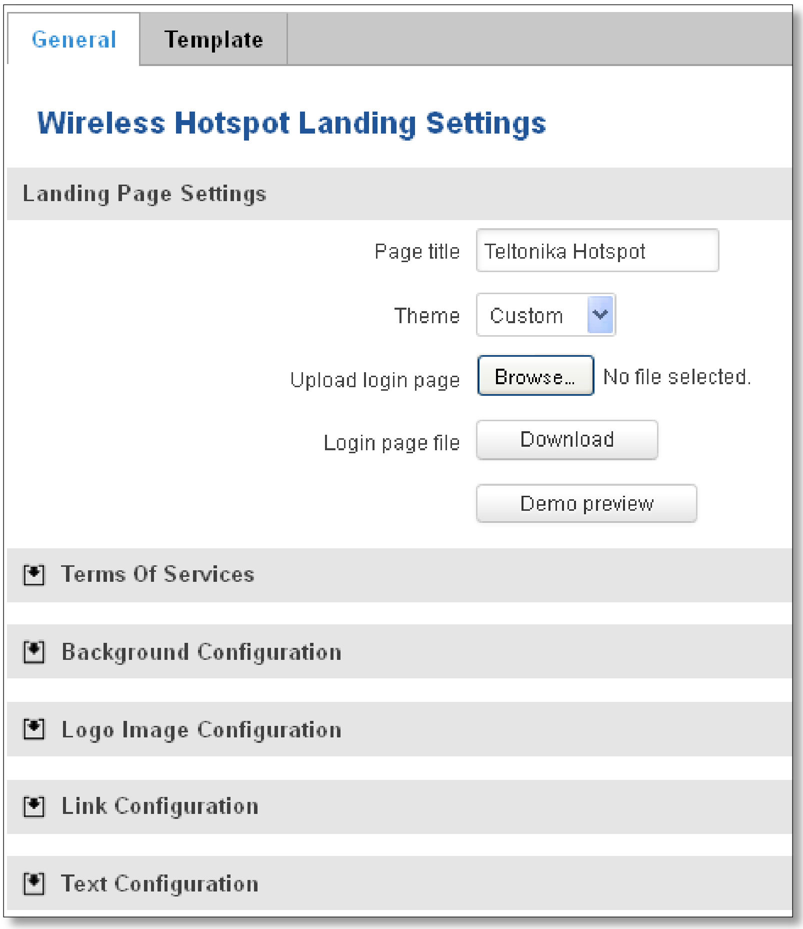
MAC	IP	Port	Date	Time
There are no records yet.				

Showing 1 to 1 of 1 entries

8.7.4 Landing Page

8.7.4.1 General Landing Page Settings

With this functionality you can customize your Hotspot Landing page.



Wireless Hotspot Landing Settings

Landing Page Settings

Page title: Teltonika Hotspot

Theme: Custom

Upload login page: Browse... No file selected.

Login page file: Download

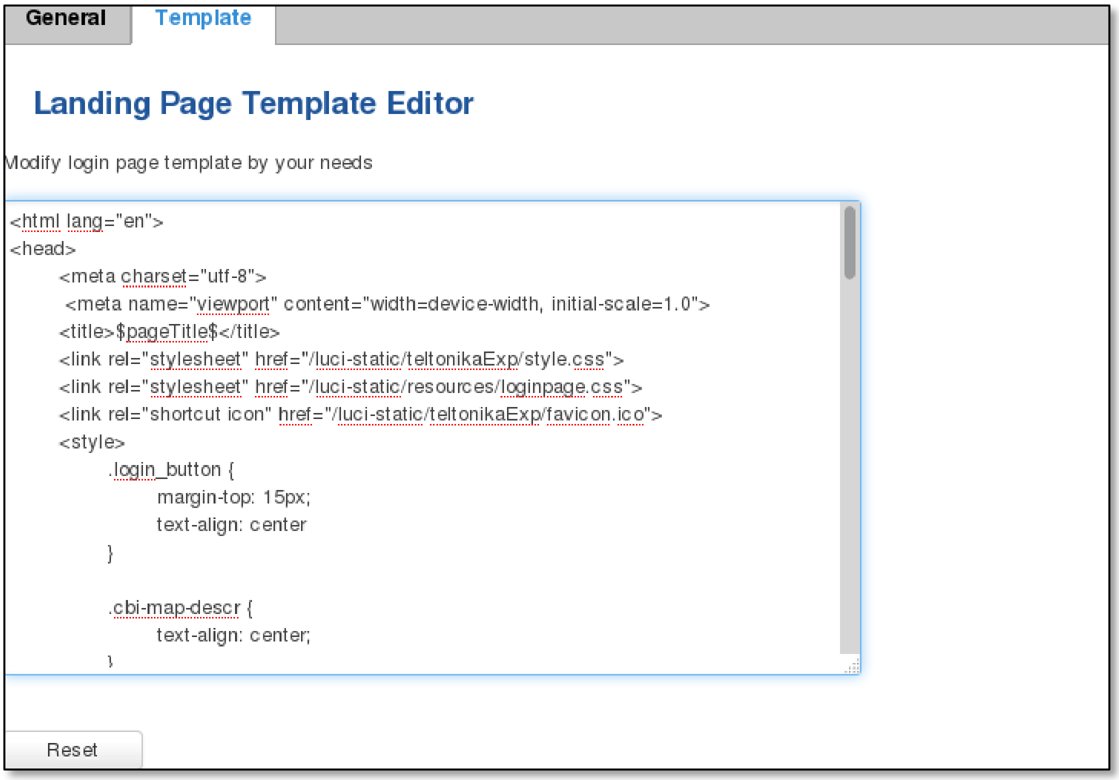
Demo preview

	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.

8.7.4.2 Template

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



Landing Page Template Editor

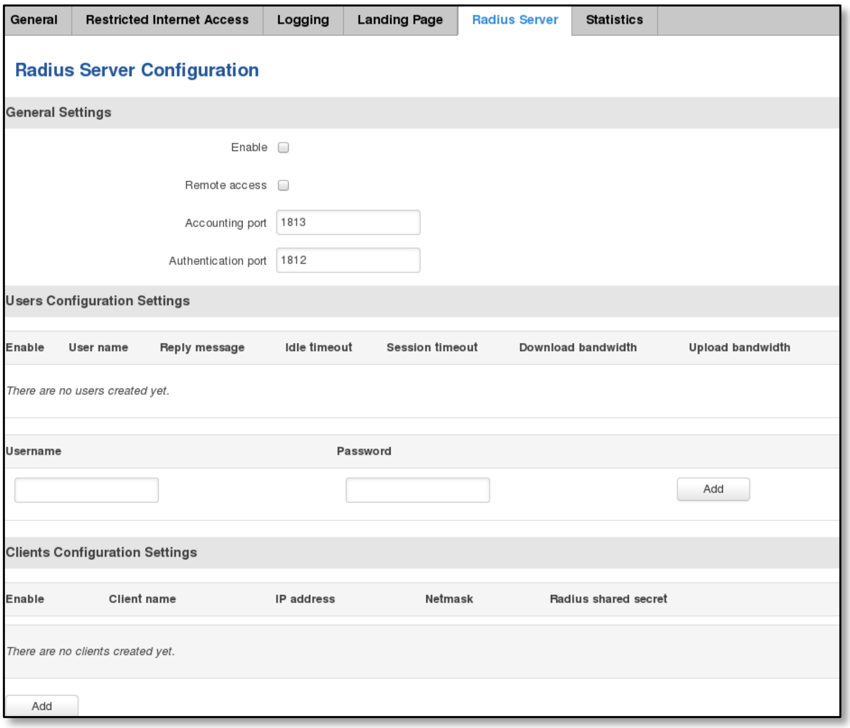
Modify login page template by your needs

```
<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;
                }
```

8.7.5 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 1813

Authentication port 1812

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

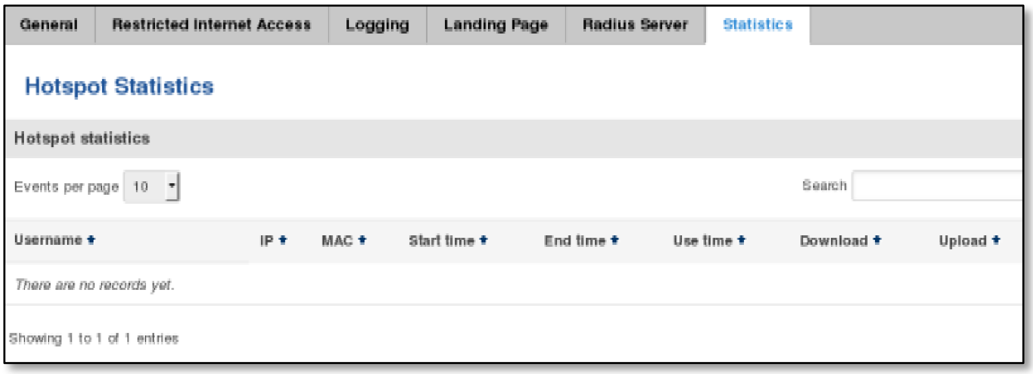
Enable	Client name	IP address	Netmask	Radius shared secret

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

8.7.6 Statistics

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



Hotspot Statistics

Hotspot statistics

Events per page 10

Search

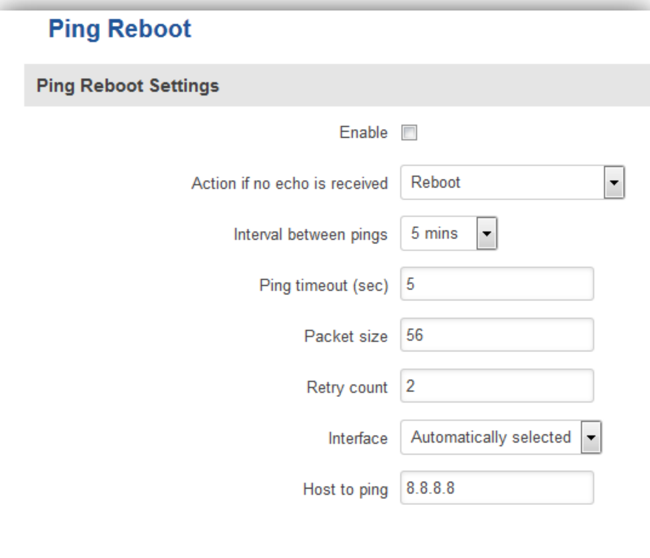
Username	IP	MAC	Start time	End time	Use time	Download	Upload
There are no records yet.							

Showing 1 to 1 of 1 entries

8.8 Auto Reboot

8.8.1 Ping Reboot

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



Ping Reboot

Ping Reboot Settings

Enable □

Action if no echo is received: Reboot

Interval between pings: 5 mins

Ping timeout (sec): 5

Packet size: 56

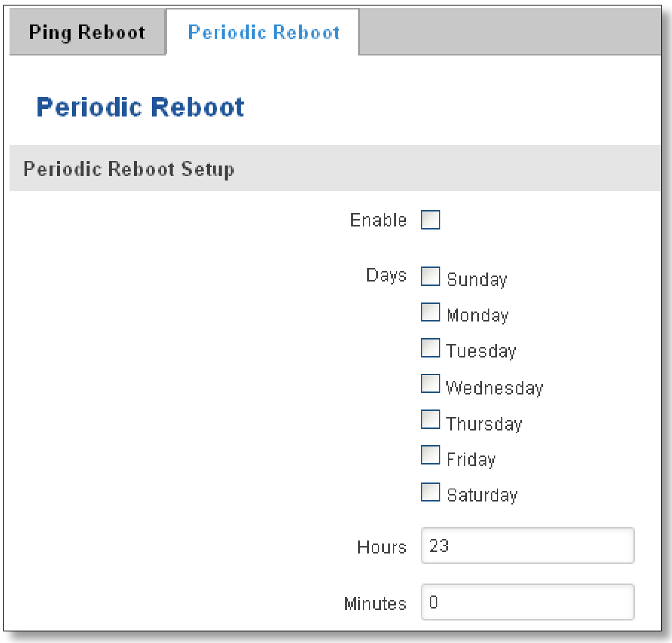
Retry count: 2

Interface: Automatically selected

Host to ping: 8.8.8.8

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

8.8.2 Periodic Reboot



Periodic Reboot

Periodic Reboot Setup

Enable □

Days □ Sunday
□ Monday
□ Tuesday
□ Wednesday
□ Thursday
□ Friday
□ Saturday

Hours 23

Minutes 0

	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

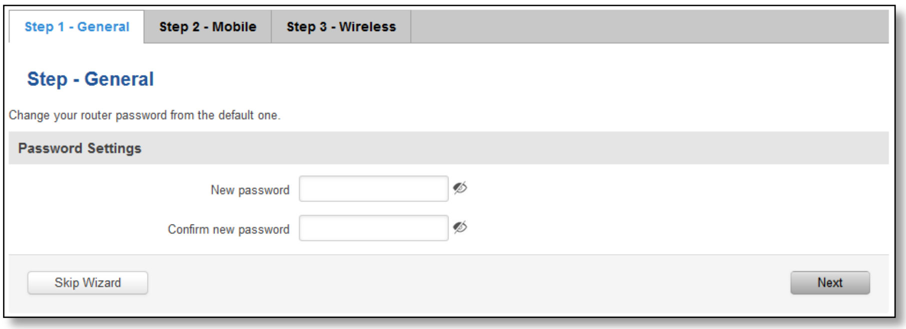
9 System

9.1 Setup Wizard

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

Step 1 (General)

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



Step - General

Change your router password from the default one.

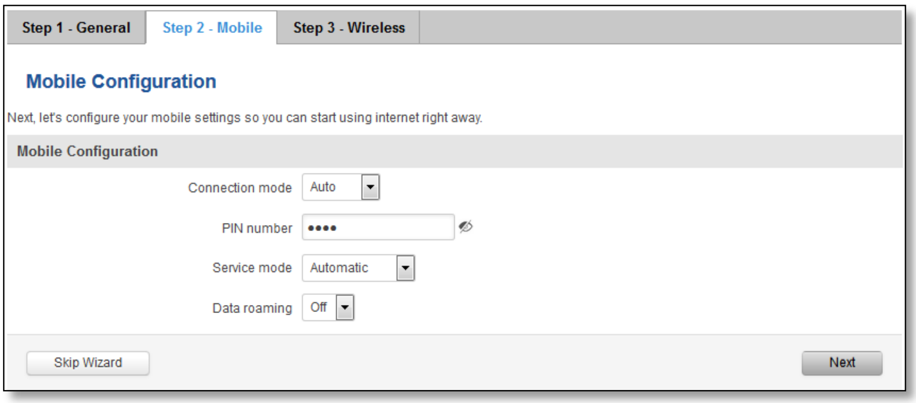
Password Settings

New password

Confirm new password

Step 2 (Mobile Configuration)

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



Mobile Configuration

Next, let's configure your mobile settings so you can start using internet right away.

Mobile Configuration

Connection mode: Auto

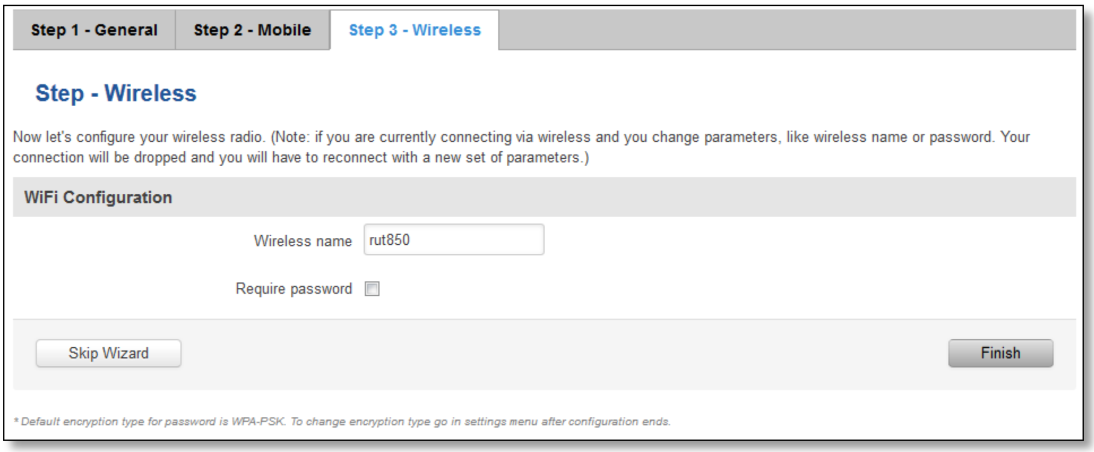
PIN number: ••••

Service mode: Automatic

Data roaming: Off

Step 3 (Wi-Fi)

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



Step - Wireless

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

WiFi Configuration

Wireless name: rut850

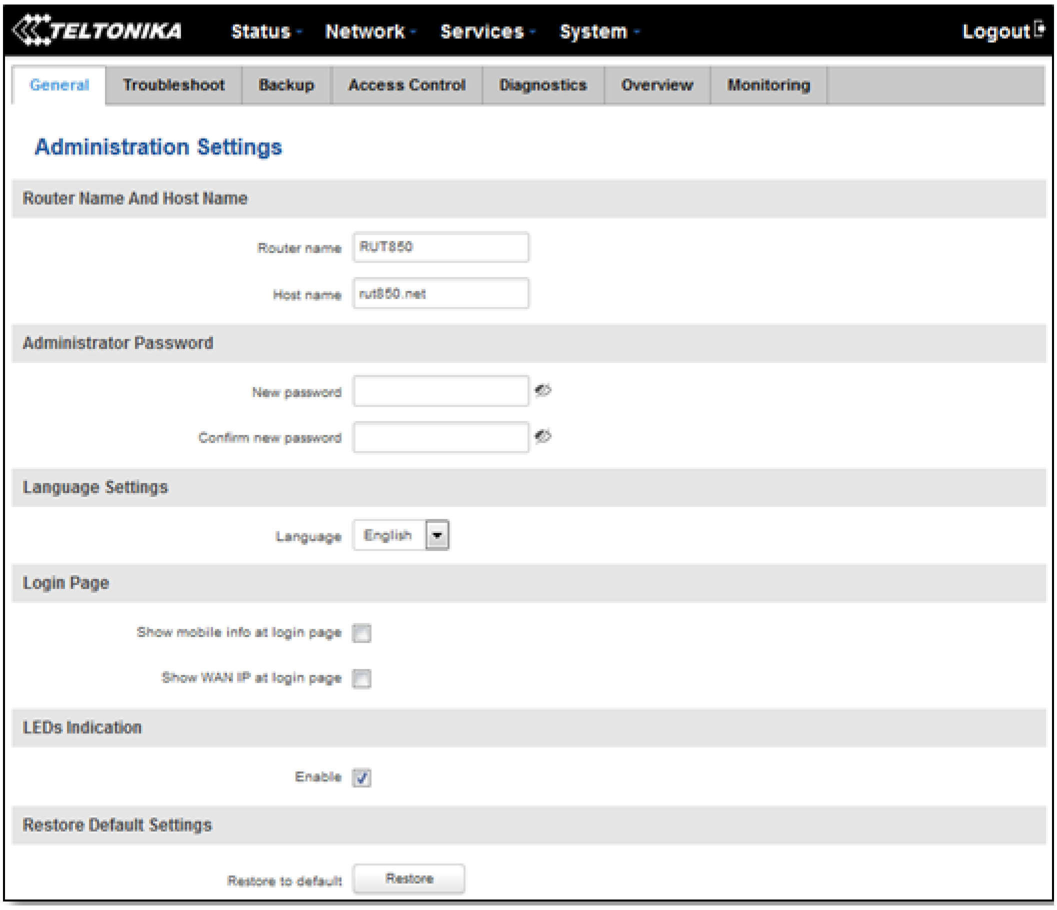
Require password □

* Default encryption type for password is WPA-PSK. To change encryption type go in settings menu after configuration ends.

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

9.2 Administration

9.2.1 General



Administration Settings

Router Name And Host Name

Router name: RUT850

Host name: rut850.net

Administrator Password

New password

Confirm new password

Language Settings

Language: English

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
9.	Show mobile info at login page	Show operator and signal strength at login page.
10.	Show WAN IP at login page	Show WAN IP at login page.
11.	On/Off LEDs	If uncheck, all routers LEDs are off.
12	Restore to default	Router will be set to factory default settings

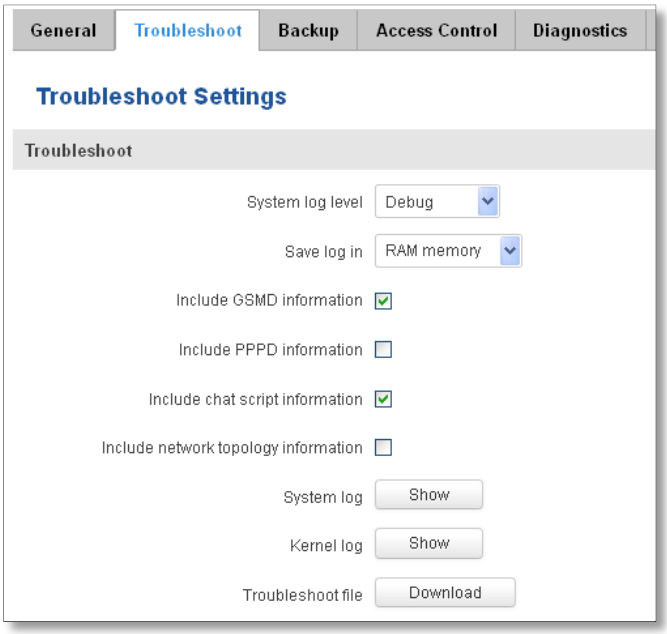
Important notes:

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**

9.2.2 Troubleshoot



Troubleshoot Settings

Troubleshoot

System log level: Debug

Save log in: RAM memory

Include GSMD information ☑

Include PPPD information ☐

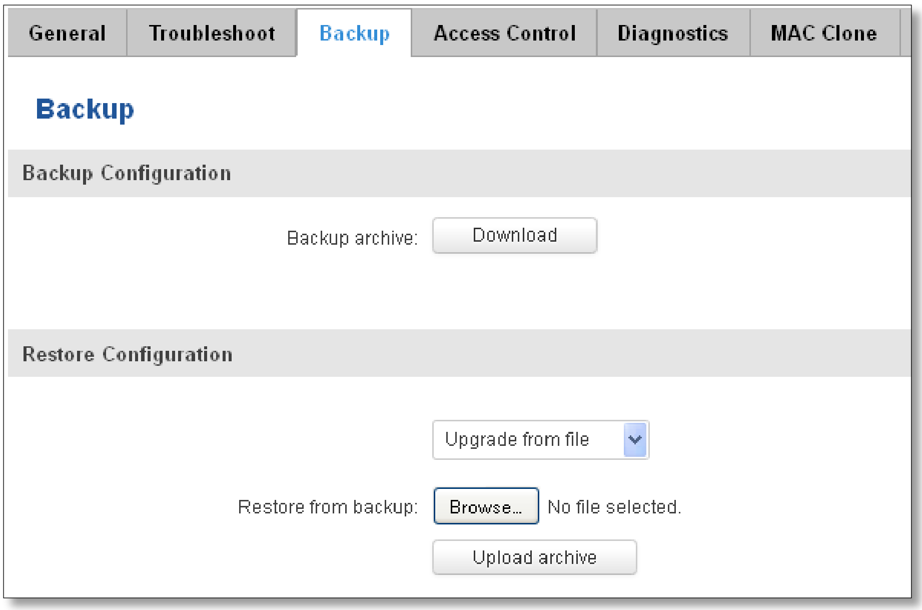
Include chat script information ☑

Include network topology information ☐

	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 file	Downloadable archive, that contains full router configuration and all System log files.

9.2.3 Backup



Backup

Backup Configuration

Backup archive:

Restore Configuration

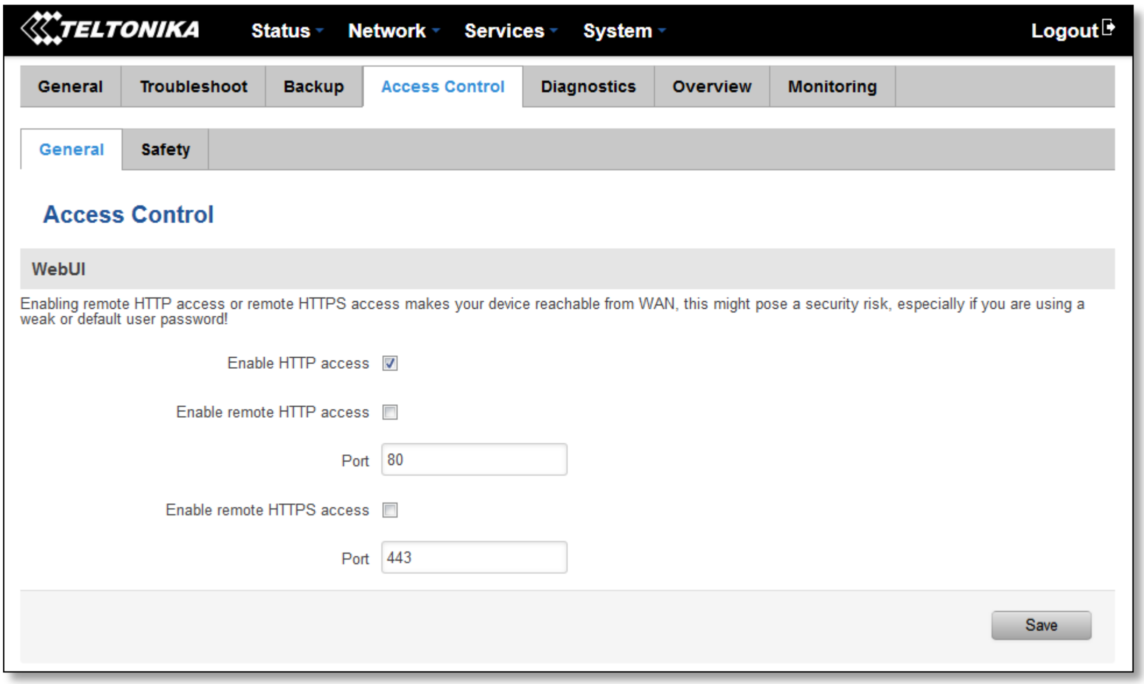
Upgrade from file

Restore from backup: No file selected.

	Field name	Explanation
1.	Backup archive	Download current router settings file to personal computer. This file can be loaded to other RUT950 with same Firmware version in order to quickly configure it.
2.	Restore from backup	Select, upload and restore router settings file from personal computer.

9.2.3.1 Access control

9.2.3.1.1 General



Access Control

WebUI

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

Enable HTTP access ☑

Enable remote HTTP access □

Port 80

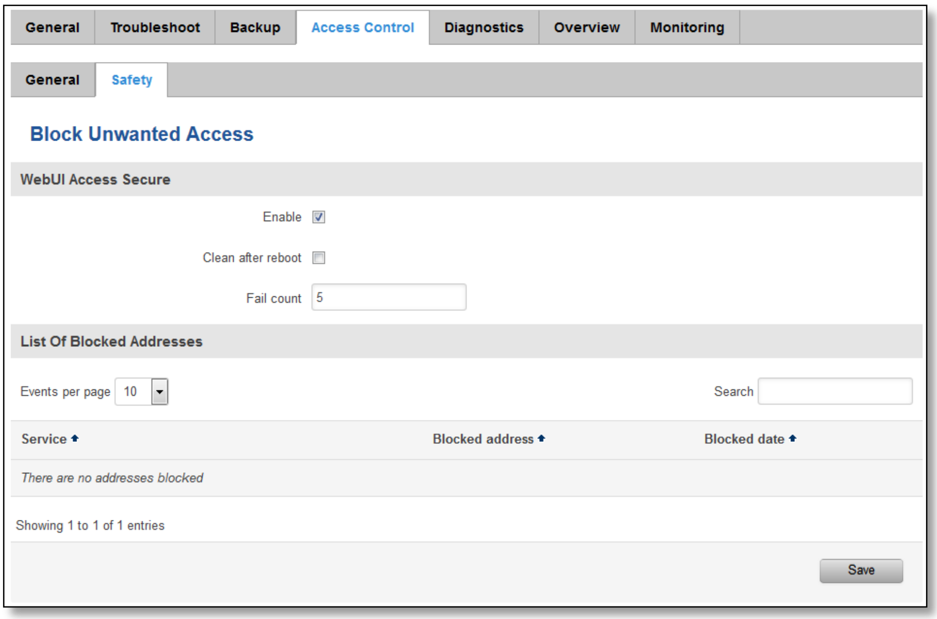
Enable remote HTTPS access □

Port 443

	Field name	Explanation
1.	Enable HTTP access	Enables HTTP access to router
2.	Enable remote HTTP access	Enables remote HTTP access to router
3.	Port	Port to be used for HTTP communication
4.	Enable remote HTTPS access	Enables remote HTTPS access to router
5.	Port	Port to be used for HTTPS communication

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

9.2.3.1.2 Safety



Block Unwanted Access

WebUI Access Secure

Enable ☑

Clean after reboot □

Fail count 5

List Of Blocked Addresses

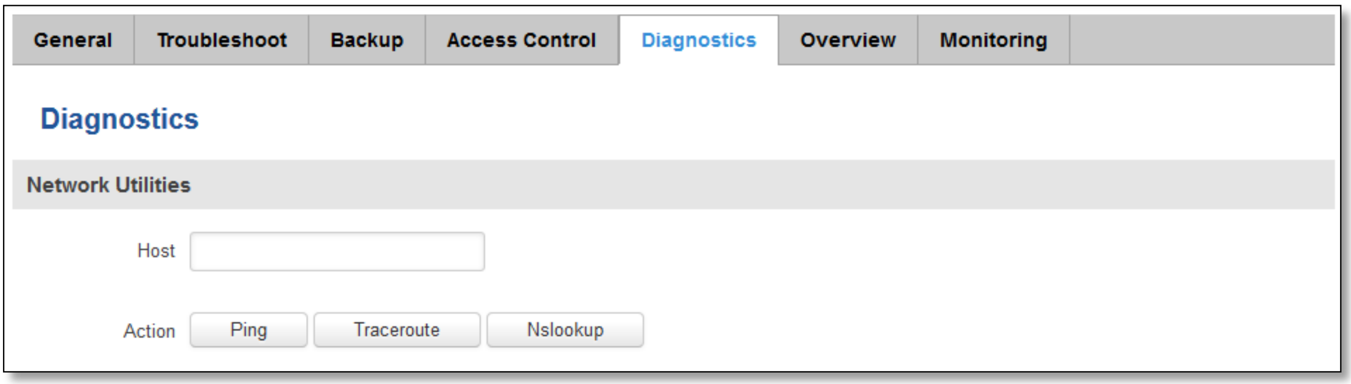
Events per page 10 ▾ Search

Service	Blocked address	Blocked date
There are no addresses blocked		

Showing 1 to 1 of 1 entries

	Field name	Explanation
1.	WebUI access secure enable	Check box to enable secure WebUI access.
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.

9.2.4 Diagnostics



Diagnostics

Network Utilities

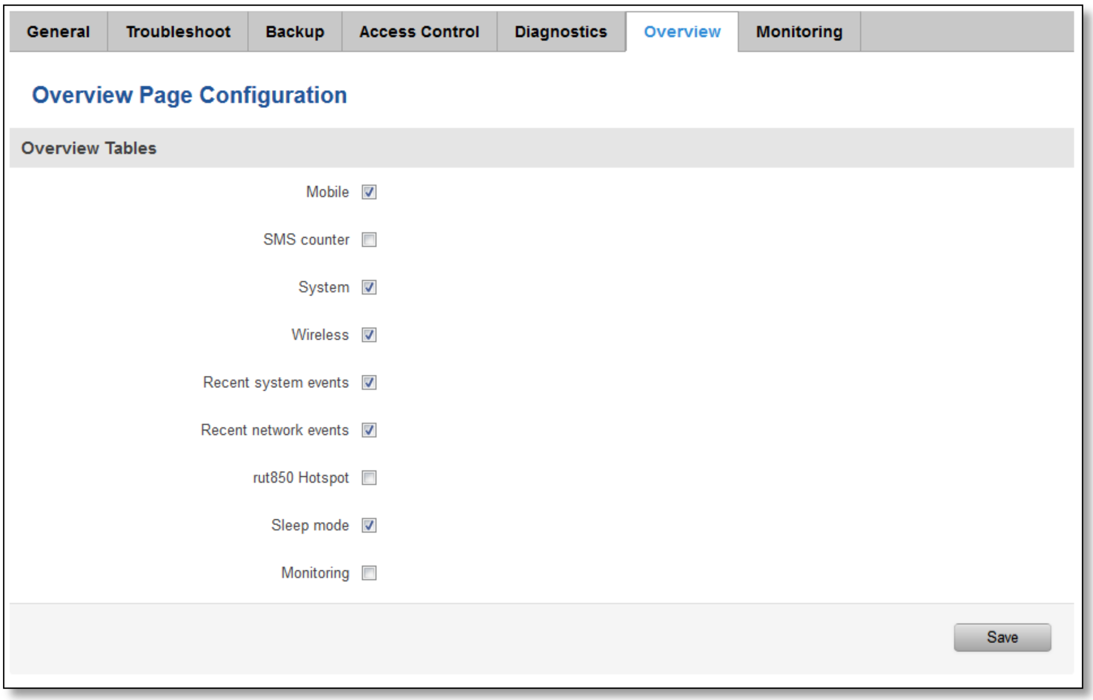
Host

Action

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

9.2.5 Overview

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



Overview Page Configuration

Overview Tables

Mobile ☑

SMS counter □

System ☑

Wireless ☑

Recent system events ☑

Recent network events ☑

rut850 Hotspot □

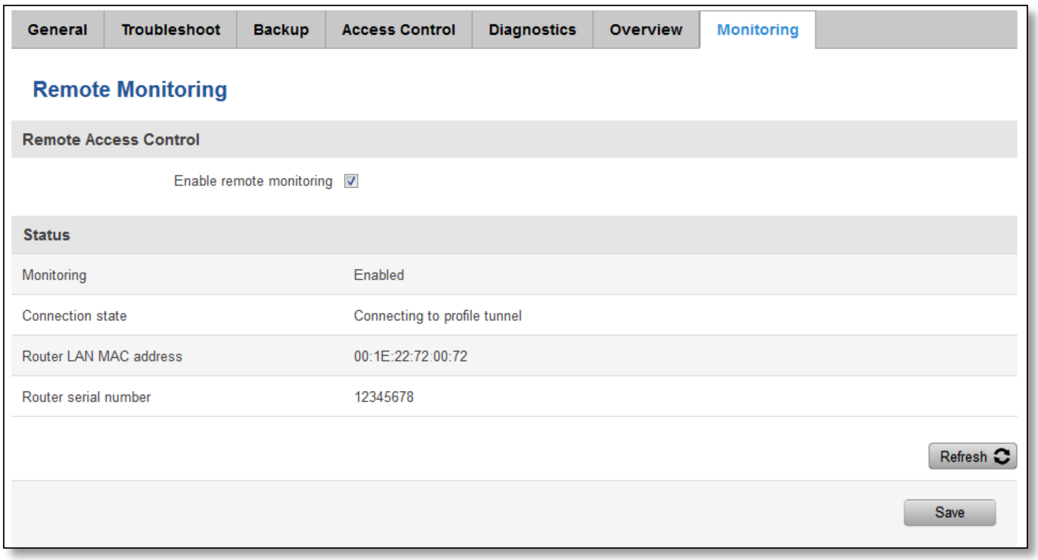
Sleep mode ☑

Monitoring □

	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.	Recent system events	Check box to show Recent system events table in Overview page
6.	Recent network events	Check box to show Recent network events table in Overview page
7.	<Hotspot name> Hotspot	Check box to show Hotspot instance table in Overview page
8.	Sleep mode	Check box to show Sleep mode table in Overview page
9.	Monitoring	Check box to show Monitoring table in Overview page

9.2.6 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 Monitoring

Remote Access Control

Enable remote monitoring ☑

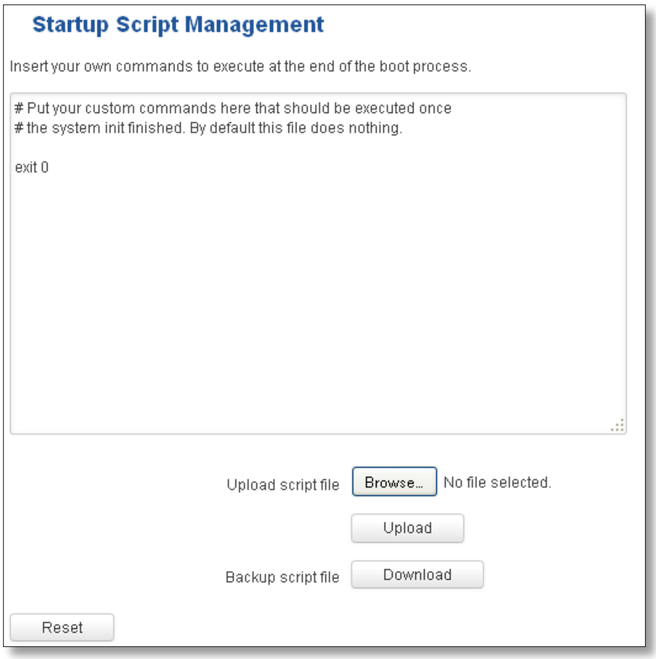
Status

Monitoring	Enabled
Connection state	Connecting to profile tunnel
Router LAN MAC address	00:1E:22:72:00:72
Router serial number	12345678

	Field name	Explanation
1.	Enable remote monitoring	Check box to enable/disable remote monitoring
2.	Monitoring	Shows monitoring status.
3.	Router LAN MAC address	MAC address of the Ethernet LAN ports
4.	Router serial number	Serial number of the device

9.3 User scripts

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


Startup Script Management

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

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

exit 0
```

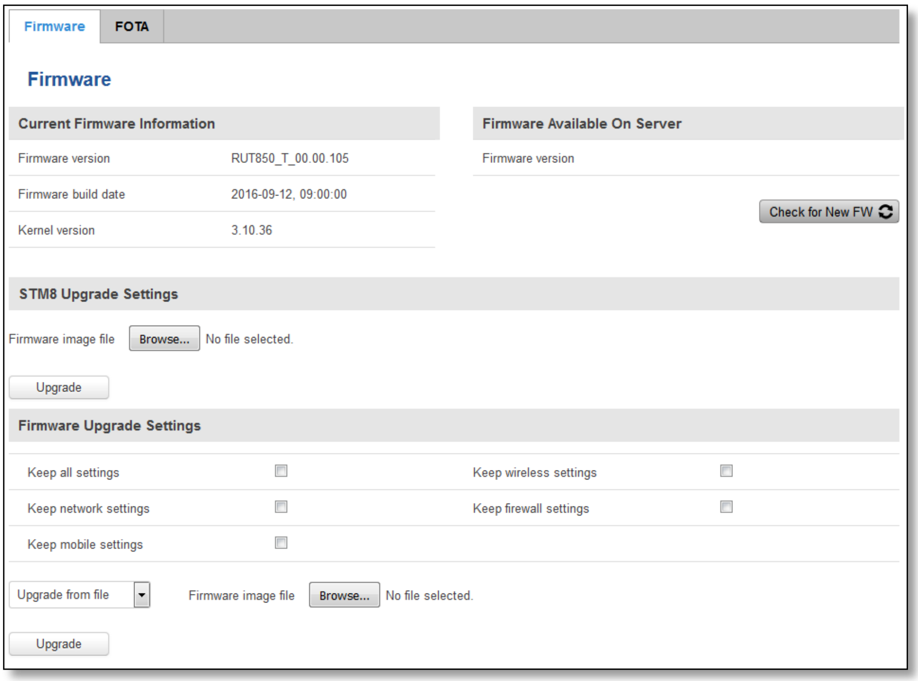
Upload script file Browse... No file selected.

Backup script file

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

9.4 Firmware

9.4.1 Firmware



Firmware

Current Firmware Information	
Firmware version	RUT850_T_00.00.105
Firmware build date	2016-09-12, 09:00:00
Kernel version	3.10.36

Firmware Available On Server

Firmware version

STM8 Upgrade Settings

Firmware image file No file selected.

Firmware Upgrade Settings

Keep all settings	□	Keep wireless settings	□
Keep network settings	□	Keep firewall settings	□
Keep mobile settings	□		

Upgrade from file   Firmware image file No file selected.

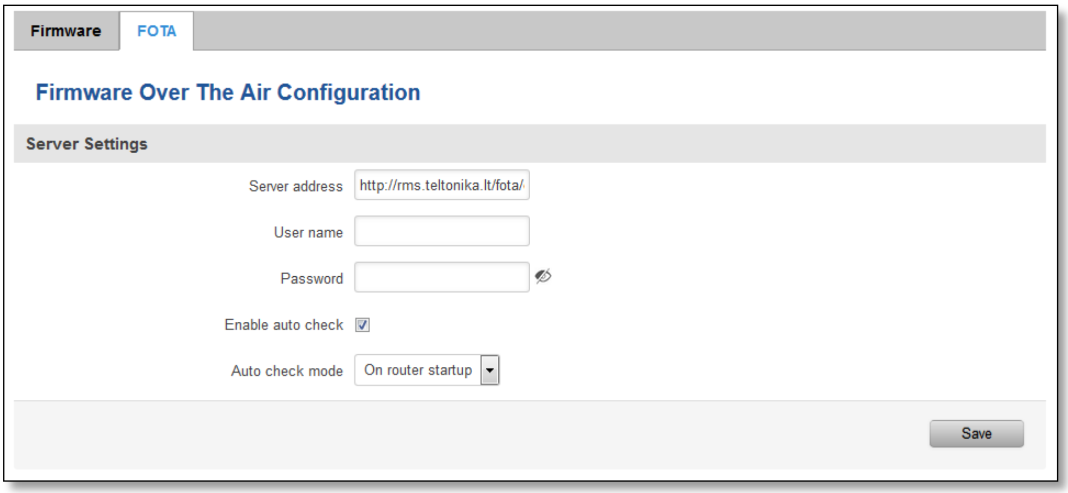
STM8 Firmware –it is responsible for sleep mode functionality and signal strength leds.

Keep all 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.

9.4.2 FOTA



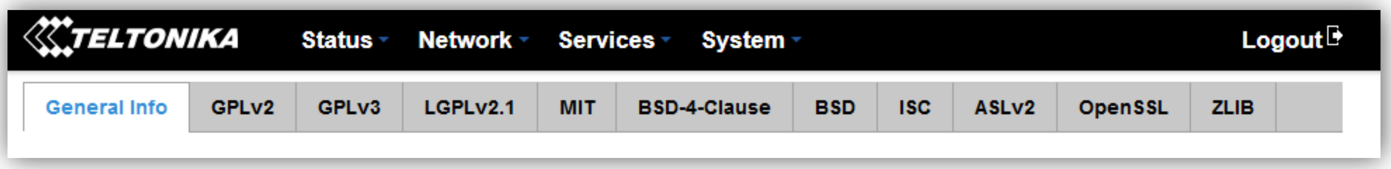
Firmware Over The Air Configuration

Server Settings

Server address	http://rms.teltonika.lt/fota/
User name	
Password	
Enable auto check	☑
Auto check mode	On router startup

	Field name	Explanation
1.	Server address	Specify server address to check for firmware updates. E.g. “http://rms.teltonika.lt/fota/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.

9.5 Licenses



GNU General Public License Notice

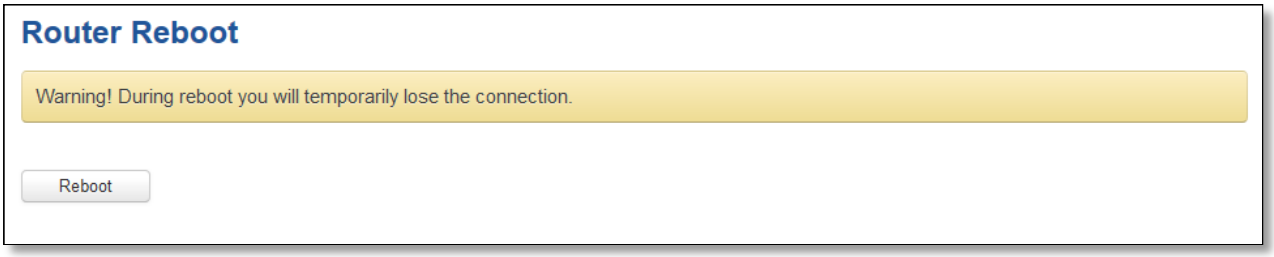
This product includes software code developed by third parties, including software code subject to the GNU General Public License ("GPL"). Teltonika provides mail in service of a machine readable copy of the corresponding GPL source code on CD upon request via email or traditional paper mail. Teltonika reserves the right to charge for shipping and media as allowed under the GPL. This offer will be valid for at least 3 years. For more information, please contact us at gpl@teltonika.lt or Saltoniskiu st. 10C, LT-08105 Vilnius, Lithuania.

Furthermore, under www.teltonika.lt/gpl website, Teltonika provides machine readable copies of the GPL source codes used in Teltonika products, where these copies are available to download for free. Please note, that these machine readable copies may neither offer a full set of source codes used in Teltonika’s products nor always provide for the latest or actual version of such source codes.

The GPL code used in this product is distributed WHITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors.

Please refer to the WebUI System->Licenses page for further information.

9.6 Reboot



Router Reboot

Warning! During reboot you will temporarily lose the connection.

Reboot router by pressing button “Reboot”.

10 Device Recovery

Reset button is located in the front of the device. Reset button has several functions:

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

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

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.

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

DNS – Domain Name System. A server that translates names such as www.google.lt 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 Adress 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.

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 enchanted data cryptographic encapsulation designed for data confidentiality and based upon the Counter Mode with CBC-MAC (CCM) of the AES (Advanced Encryption Standard) standard.

MAC – Media Access Control. Hardware address which uniquely identifies each node of the network. In IEEE 802 networks, the Data Link Control (DCL) layer of the PSO 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.

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

12 Changelog

Nr.	Date	Version	Comments
1	2017-02-01	1.10	
2	2017-05-11	1.11	
3	2017-06-29	1.12	Added information about overvoltage protection (chapter 2.4)