TELTONIKA

Remove back panel to insert SIM
TELTONIKA
RUT955
To restore default settings:
1. Power on and wait for 1 min
2. Press reset button for 5 sec
3. Wait for 3 min
Default settings
IP: 192.168.1.1
User name: admin
Password: admin01
LAN1
LAN2
LAN3
WAN
RS485
9 - 30 VDC
PWR
RS232
I/O

Legal notice

Copyright © 2015 TELTONIKA Ltd. All rights reserved. Reproduction, transfer, distribution or storage of part or all of the contents in this document in any form without the prior written permission of TELTONIKA Ltd is prohibited. The manufacturer reserves the right to modify the product and manual for the purpose of technical improvement without prior notice.

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

Attention

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

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

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

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

The device is powered by low voltage +9V DC power adaptor.

Table of Contents

Legal notice 2
Attention 2
SAFETY INFORMATION 9
Device connection 10
1 Introduction 11
2 Specifications 11
2.1 Ethernet 11
2.2 Wi-Fi 11
2.3 Hardware 11
2.4 Electrical, Mechanical & Environmental 12
2.5 Applications 12
3 Setting up your router 13
3.1 Installation 13
3.1.1 Front Panel and Back Panel 13
3.1.2 Connection status LED indication 14
3.1.3 Hardware installation 14
3.2 Logging in 15
4 Operation Modes 18
5 Powering Options 19
5.1 Powering the device from higher voltage 19
6 Status 20
6.1 Overview 20
6.2 System Information 21
6.3 Network Information 22
6.4 Device information 34
6.5 Services 35
6.6 Routes 36
6.6.1 ARP 36
6.6.2 Active IP Routes 36
6.6.3 Active IPv6-Routes 37
6.7 Graphs 38

6.7.1 Mobile Signal Strength 38
6.7.2 Realtime Load 39
6.7.3 Realtime Traffic 40
6.7.4 Realtime Wireless 41
6.7.5 Realtime Connections 42
6.8 Mobile Traffic 43
6.9 Events Log 44
6.9.1 All Events 44
6.9.2 System Events 45
6.9.3 Network Events 46
6.9.4 Events Reporting 47
6.9.5 Reporting Configuration 52
7 Network 57
7.1 Mobile 57
7.1.1 General 57
7.1.2 SIM Management 60
7.1.3 Network Operators 61
7.1.4 Mobile Data Limit 63
7.1.5 SIM Idle Protection 64
7.2 WAN 66
7.2.1 Operation Mode 66
7.2.2 Common Configuration 66
7.2.3 How do I set up a backup link? 74
7.3 LAN 75
7.3.1 Configuration 75
7.3.2 DHCP Server 76
7.3.3 Static Leases 77
7.3.4 IP Aliases 78
7.4 VLAN 79
7.4.1 VLAN Networks 79
7.4.2 LAN Networks 80
7.5 Wireless 81
7.5.1 Wireless Access Point 81
7.5.2 Wireless Station 85

7.6 Firewall 86
7.6.1 General Settings 86
7.6.2 DMZ 87
7.6.3 Zone Forwarding 87
7.6.4 Port Forwarding 88
7.6.5 Traffic Rules 91
7.6.6 Custom Rules 97
7.6.7 DDOS Prevention 98
7.6.8 Port Scan Prevention 101
7.7 Routing 102
7.7.1 Static Routes 102
7.7.2 Dynamic Routes 103
7.7.1 105
7.7.2 105
7.8 Load Balancing 112
8 Remote monitoring and administration 113
9 Services 115
9.1 VRRP 115
9.1.1 VRRP LAN Configuration Settings 115
9.1.2 Check Internet connection 115
9.2 TR-069 116
9.2.1 TR-069 Parameters Configuration 116
9.3 Web filter 117
9.3.1 Site Blocking 117
9.3.2 Proxy Based Content Blocker 117
9.4 MQTT 118
9.4.1 MQTT Broker 118
9.4.2 MQTT Publisher 121
9.5 NTP 123
9.6 RS232/RS485 124
9.6.1 RS232 124
9.6.2 RS485 126
9.6.3 Modes of different serial types in RS232 and RS485 130
9.7 VPN 133

9.7.1 OpenVPN 133
9.7.1 136
9.7.2 IPSec 139
9.7.3 GRE Tunnel 142
9.7.4 PPTP 144
9.7.5 L2TP 146
9.8 Dynamic DNS 148
9.9 SMS Utilities 149
9.9.1 SMS Utilities 149
9.9.1 150
9.9.2 Call Utilities 159
9.9.3 User Groups 160
9.9.4 SMS Management 161
9.9.5 Remote Configuration 163
9.9.6 Statistics 166
9.10 SNMP 167
9.10.1 SNMP Settings 167
9.10.2 TRAP Settings 168
9.11 SMS Gateway 169
9.11.1 Post/Get Configuration 169
9.11.2 Email to SMS 171
9.11.3 Scheduled Messages 172
9.11.4 Auto Reply 173
9.11.5 SMS Forwarding 174
9.11.6 SMPP 177
9.12 GPS 178
9.12.1 GPS 178
9.12.2 GPS Settings 178
9.12.1 179
9.12.2 179
9.12.3 GPS Mode 180
9.12.4 GPS I/O 181
9.12.5 GPS Geofencing 182
9.13 Hotspot 183

9.13.1 General settings 183
9.13.2 Internet Access Restriction Settings 185
9.13.3 Logging 185
9.13.4 Landing Page 186
9.13.5 Radius server configuration 188
9.13.6 Statistics 189
9.14 CLI 189
9.15 Auto Reboot 190
9.15.1 Ping Reboot 190
9.15.2 Periodic Reboot 191
9.16 Network Shares 191
9.16.1 Mounted File Systems 191
9.16.2 Samba 192
9.16.3 Samba User 192
9.17 Modbus TCP interface 194
9.18 UPNP 195
9.18.1 General Settings 195
9.18.2 Advanced Settings 195
9.18.3 UPnP ACLs 196
9.18.4 Active UPnP Redirects 196
9.19 QoS 196
9.20 Input/Output 197
9.20.1 Status 197
9.20.2 Input 198
9.20.3 Output 201
9.20.4 Input/Output hardware information 204
10 System 210
10.1 Configuration Wizard 210
10.2 Profiles 212
10.3 Administration 213
10.3.1 General 213
10.3.2 Troubleshoot 214
10.3.3 Backup 215
10.3.4 Diagnostics 217

10.3.5 MAC Clone 218
10.3.6 Overview 218
10.3.7 Monitoring 219
10.4 User scripts 219
10.5 Restore point 220
10.5.1 Restore point create 220
10.5.2 Restore point load 220
10.6 Firmware 221
10.6.1 Firmware 221
10.6.2 FOTA 222
10.7 Reboot 222
11 Device Recovery 222
11.1 Reset button 223
11.2 Bootloader's WebUI 223
12 Glossary: 223
13 Changelog 226

SAFETY INFORMATION

In this document you will be introduced on how to use a 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 to draw power from a Limited Power Source (LPS) whose power consumption should not exceed 15VA and the current rating of the overcurrent protective device should not exceed 2A.

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

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

Do not mount or service the device during a thunderstorm.

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

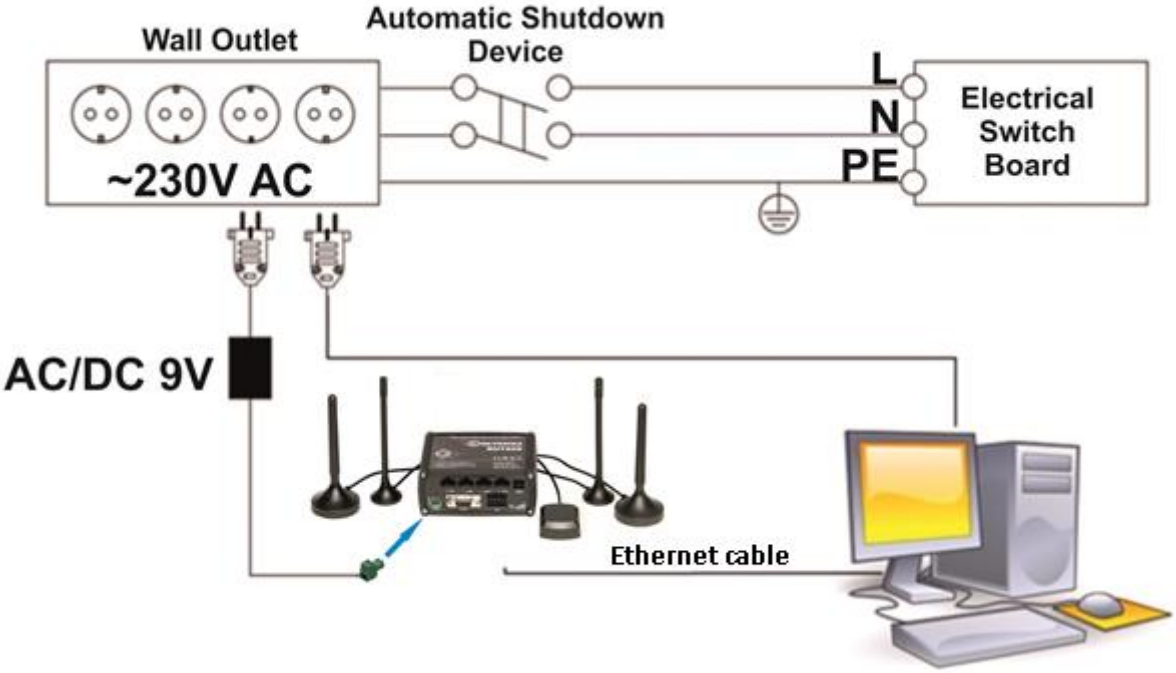
Protection of the primary circuits of the associated PC and PSU (LPS) against short circuits and earth faults of the associated PC will be provided as part of the building installation.

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

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

Signal level of the device depends on the environment in which it is working in. 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 RUT955 LTE router!

RUT955 is part of the RUT9xx series of compact mobile routers with high speed wireless and Ethernet connections.

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

2 Specifications

2.1 Ethernet

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

2.2 Wi-Fi

- IEEE 802.11b/g/n WiFi standards
- 2x2 MIMO
- AP and STA modes
- 64/128-bit WEP, WPA, WPA2, WPA&WPA2 encryption methods
- 2.401 – 2.495GHz Wi-Fi frequency range
- 20dBm max WiFi TX power
- SSID stealth mode and access control based on MAC address

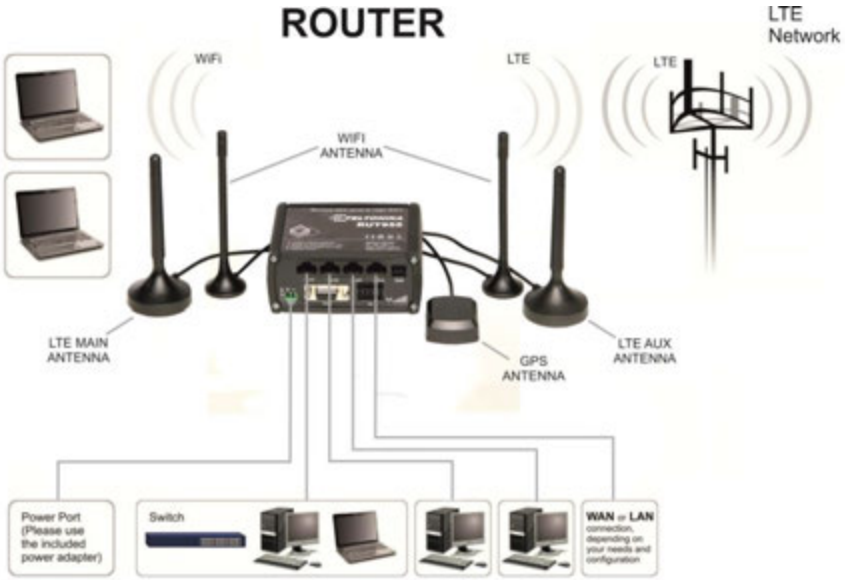
2.3 Hardware

- High performance 560 MHz CPU with 128 Mbytes of DDR2 memory
- 2 pin industrial DC power socket
- Attachable DIN rail adapter
- 4 pin industrial socket for 2/4 wire RS485
- DB9 socket for full-featured RS232
- USB A socket for external devices
- 4 pin industrial socket for 2/4 wire RS485
- Reset/restore to default button
- 2 x SMA for LTE , 2 x RP-SMA for WiFi antenna connectors
- 4 x Ethernet LEDs, 1 x Power LED
- 1 x bi-color connection status LED, 5 x connection strength LEDs
- 10 pin industrial socket for inputs/outputs:
  - 0 - 3 V digital input
  - 0 - 30 V digital galvanically isolated input
  - 0 - 24 V analog input 30 V, 250 mA digital open collector output
  - 40 V, 4 A SPST relay output

2.4 Electrical, Mechanical & Environmental

- Dimensions (H x W x D) 80mm x 106mm x 46mm
- Weight 250g
- Power supply 100 – 240 VAC -> 9 VDC wall adapter
- Input voltage range 9 – 30VDC
- Power consumption < 7W
- Operating temperature -40° to 75° C
- Storage temperature -45° to 80° C
- Operating humidity 10% to 90% Non-condensing
- Storage humidity 5% to 95% Non-condensing

2.5 Applications



3 Setting up your router

3.1 Installation

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

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

3.1.1 Front Panel and Back Panel

1,2,3	LAN Ethernet ports
4	WAN Ethernet port
5,6,7	LAN LEDs
8	WAN LED
9	RS485 connector
10	Power socket
11	RS232 connector
12	Inputs and outputs connector
13	Power LED
14	Connection LED
15	Signal strength LED

1	LTE auxiliary antenna connector*
2	GPS antenna connector
3	LTE main antenna connector*
4	USB connector
5,7	WiFi antenna connectors
6	Reset button

***LTE main/aux antenna connector positions depend on the router's modem:**
Quectel: 1 – MAIN; 3 - AUX
Huawei: 1 – AUX; 3 - MAIN
Telit: 1 – AUX; 3 – MAIN

To find out your router's modem brand, check the bottom of your router. You should find a sticker containing information about the router (Serial, IMEI, LAN MAC, etc.). The first line is the router's product code. The seventh symbol of the code indicates the router's modem:

- Quectel: **A, H, J, K, L, M, P**
- Huawei: **1, 3, 5, 7, 9, B, F**
- Telit: **0, 2, G**

Below is an example of a sticker with a **Huawei** modem (the modem symbol is highlighted in yellow)

3.1.2 Connection status LED indication

Constant blinking (~ 2Hz) – router is turning on.
LED turned off – it has no 4G data connection
LED turned on – it has 4G data connection.

Explanation of connection status LED indication:

1. Green and red blinking alternatively every 500 ms: no SIM or bad PIN;
2. Green, red and yellow blinking alternatively every 500 ms: connecting to GSM;
3. Red blinking every 1 sec: connected 2G, but no data session established;
4. Yellow blinking every 1 sec: connected 3G, no data session established;
5. Green blinking every 1 sec: connected 4G, no data session established;
6. Red lit and blinking rapidly while data is being transferred: connected 2G with data session;
7. Yellow lit and blinking rapidly while data is being transferred: connected 3G with data session;
8. Green lit and blinking rapidly while data is being transferred: connected 4G with data session;

3.1.3 Hardware installation

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

SIM 1 (primary)	SIM 2 (secondary)

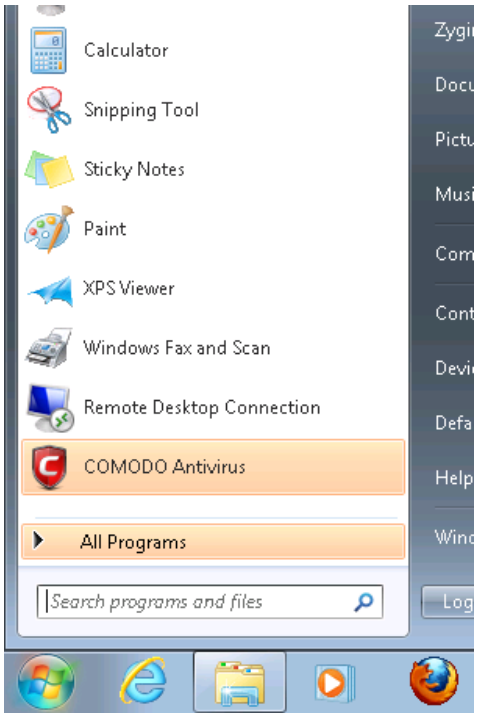
2. Attach LTE main and Wi-Fi antennas.
3. Connect the power adapter to the socket on the front panel of the device. Then plug the other end of the power adapter into a wall outlet or power strip.
4. Connect to the device wirelessly (SSID: **Teltonika_Router**) or use an Ethernet cable and plug it into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

3.2 Logging in

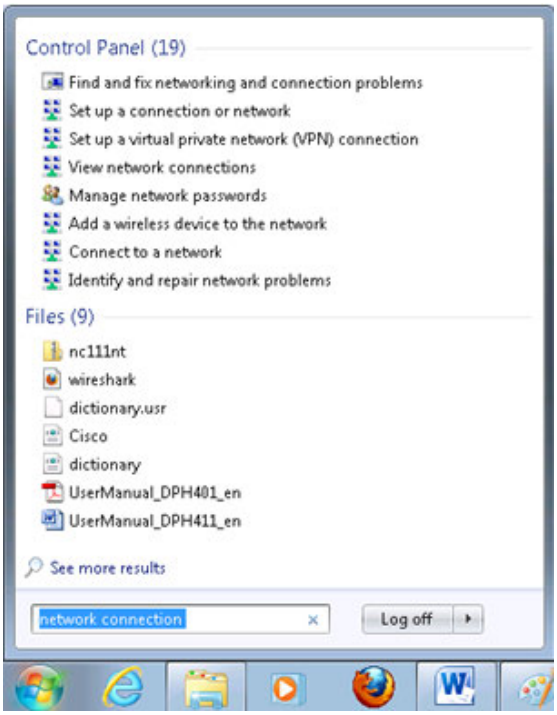
After you're complete with the setting up as described in the section above, you are ready to start logging into your router and start configuring it. This example shows how to connect on Windows 7. On windows Vista: click Start -> Control Panel -> Network and Sharing Centre -> Manage network Connections -> (go to step 4). On Windows XP: Click Start -> Settings -> Network Connections -> (see step 4). You wont's see "Internet protocol version 4(TCP/IPv4)", instead you'll have to select "TCP/IP Settings" and click options -> (go to step 6). On Windows 10 type "Network and Sharing Center" into the search bar and go there. In the navigation bar on the left side of the window click "Change adapter settings" -> (go to step 4).

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

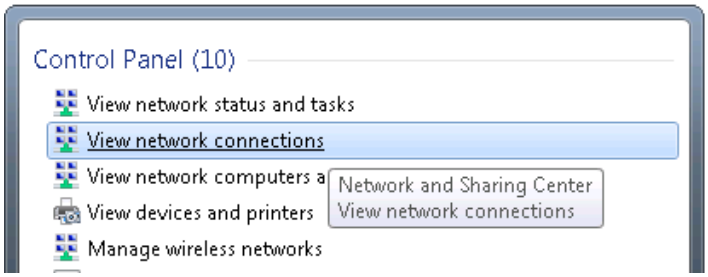
1. Press the start button



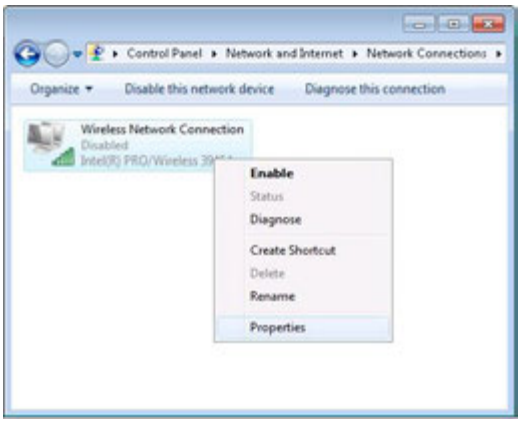
2. Type in "network connections", wait for the results to pop up



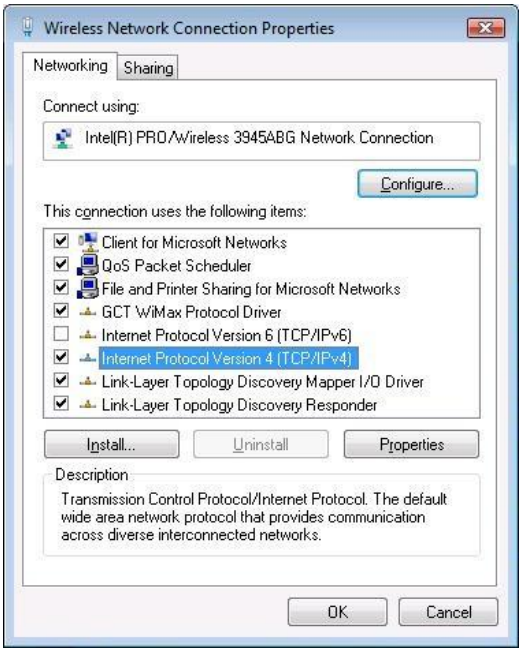
3. Click "View network connections"



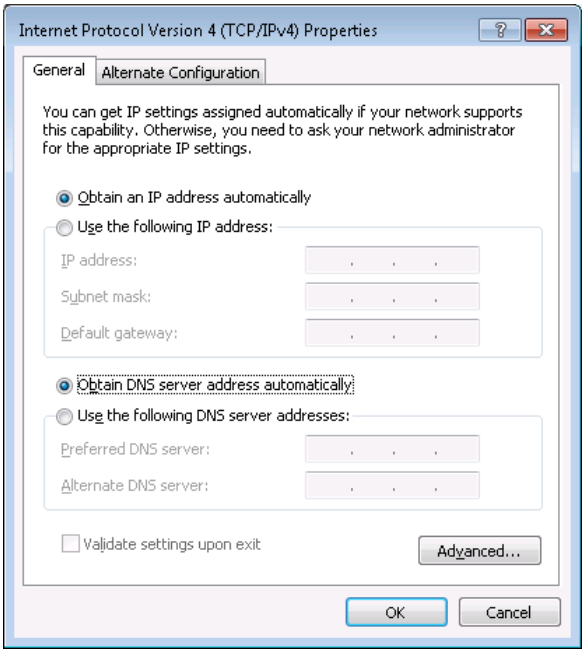
4. Then right click on your wireless device that you use to connect to other access points (it is the one with the name "Wireless Network Connection" and has signal bars on its icon)



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

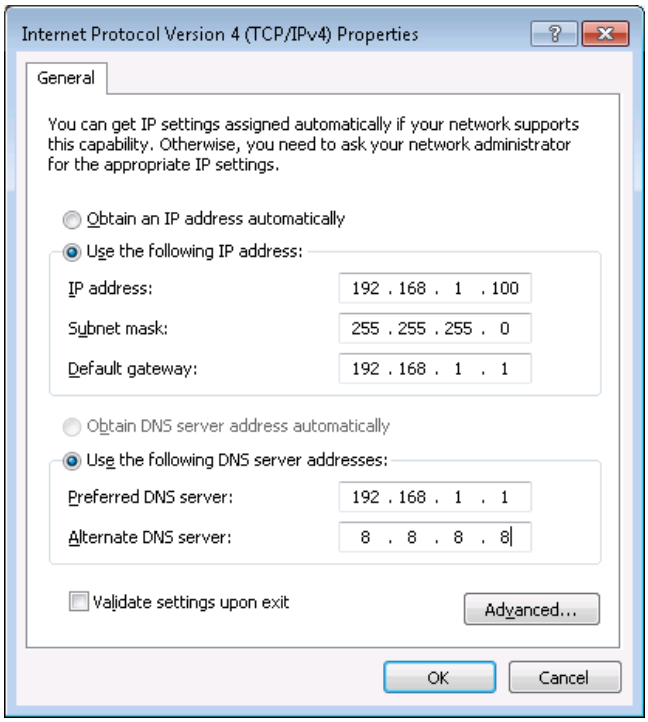


6. By default the router is going to have DHCP enabled, which means that if you select "Obtain an IP address automatically" and "Obtain DNS server address automatically", the router should lease you an IP address and you should be ready to login.



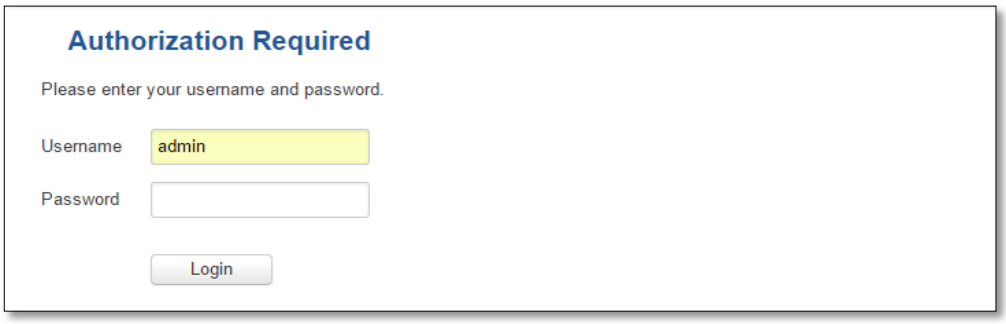
7. If you choose to configure manually here's what you do:

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



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

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



Enter the default password, which is "admin01" into the "Password" field and then either click Login with your mouse or press the Enter key. You have now successfully logged into the RUT955!

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

4 Operation Modes

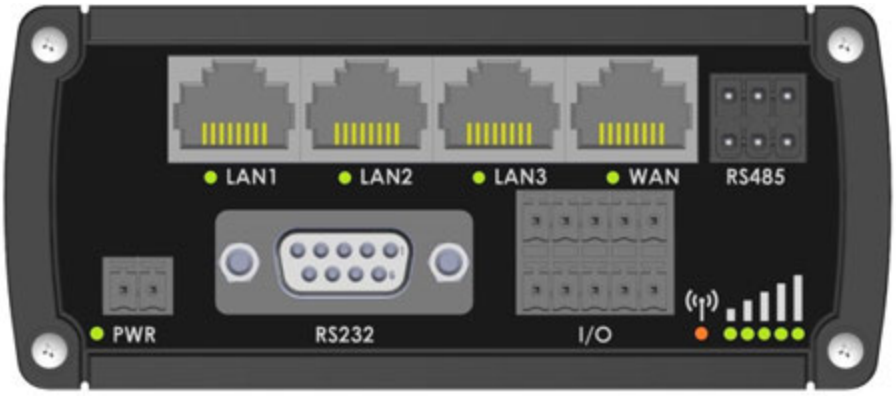
The RUT9xx series router supports various operation modes. It can be connected to the internet (WAN) via mobile, standard Ethernet cable or via a wireless network. When connecting to the internet, you may also backup your main WAN connection with one or two backup connections. Any interface can act like backup if configured so. At first the router uses its main WAN connection, if it is lost then the router tries to connect via backup with higher priority and if that fails too, the router tries the second backup option.

WAN	Main WAN	Backup WAN	LAN
Mobile	√	√	x
Ethernet	√	√	√
Wi-Fi	√	√	√

Operation modes will be explained more thoroughly in this section.

5 Powering Options

The RUT9xx router can be powered from a power socket or over an Ethernet port. Depending on your network architecture you can use the LAN1 port to power the device.



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

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

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

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

5.1 Powering the device from higher voltage

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

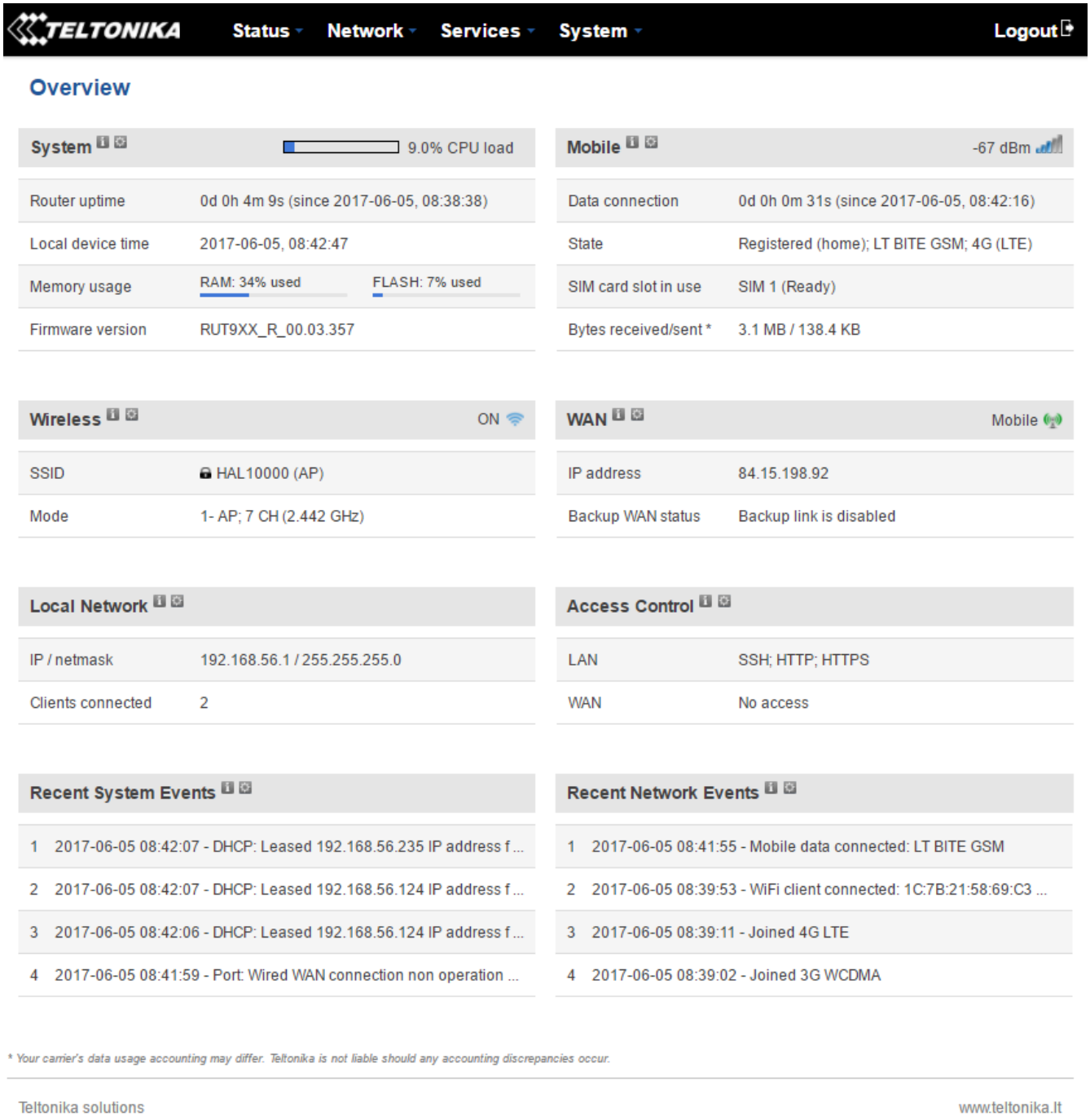
While the device is designed to accept input voltage of up to 30 VDC, peaks from high voltage power supplies can harm the device. If you want to use high voltage power supplies it is recommended to also use additional safety equipment to suppress voltage peaks from the power supply.

6 Status

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

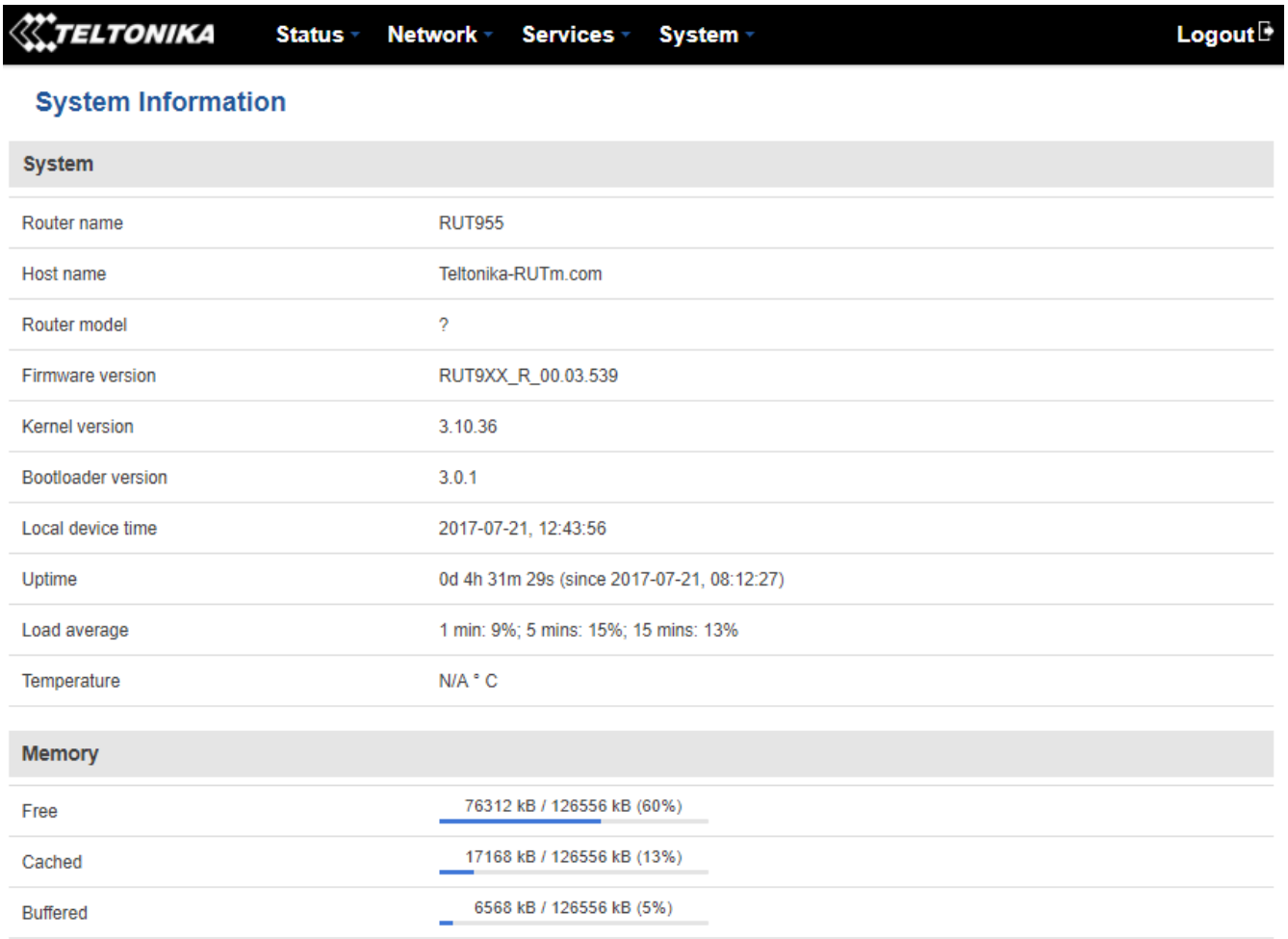
6.1 Overview

The Overview window displays various information summaries.



6.2 System Information

The System Information window displays data about the router's operating system.



System explanation:

	Field Name	Sample value	Explanation
1.	Router Name	RUT955	Name of the router (hostname of the router's system)
2.	Host name	Teltonika-RUT955.com	Indicates how router will be seen by other devices on the network
3.	Router Model	Teltonika RUT955 LTE	Router's model
4.	Firmware Version	RUT9XX_R_00.02.376	The version of the firmware that the router is currently operating on
5.	Kernel Version	3.10.36	The Linux kernel version that is currently running on the router
6.	Local Time	2016-05-24, 11:01:14	Shows the current system time
7.	Uptime	0d 0h 42m 1s (since 2016-05-24, 10:19:03)	Indicates how long it has been since the router booted up. Reboots will reset this timer to 0
8.	Load Average	1 min: 99%; 5 mins: 63%; 15 mins: 35%	Indicates how busy the router is
9.	Temperature	34.9° C	Device's temperature

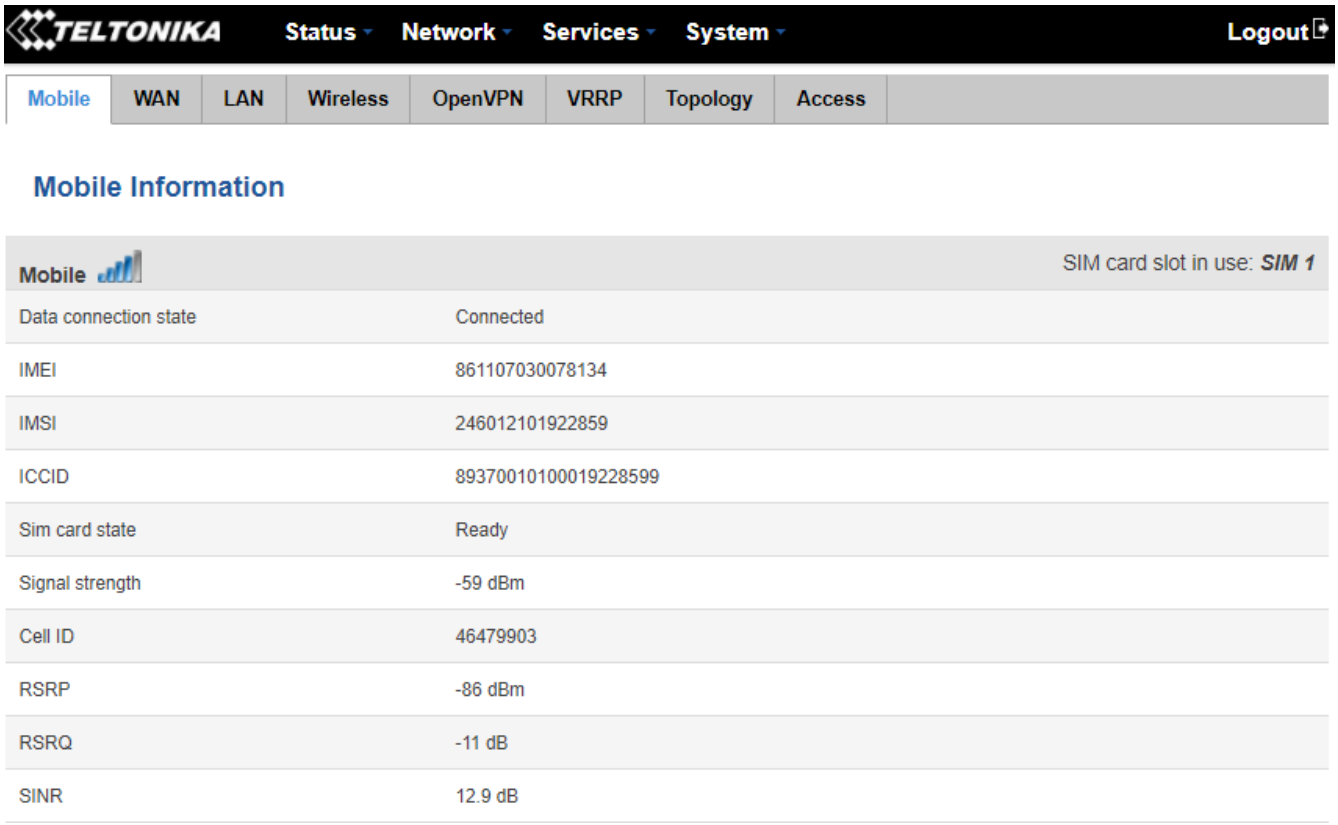
Memory explanation:

	Field Name	Sample Value	Explanation
1.	Free	84868 kB /126556 kB (67%)	The amount of memory that is free.
2.	Cached	14740 kB /126556 kB (11%)	The memory that is dedicated to storing frequently accessed data
3.	Buffered	5476 kB / 126556 kB (4%)	The size of the area in which data is temporarily stored before moving it to another location

6.3 Network Information

6.3.1 Mobile

The Mobile Information window displays information about the mobile connection.



Mobile information:

	Field Name	Sample Value	Explanation
1.	Data connection state	Connected	Mobile data connection status
2.	IMEI	861107030078134	Modem's IMEI (International Mobile Equipment Identity) number
3.	IMSI	246020100944448	IMSI (International Mobile Subscriber Identity) is used to identify the user in a cellular network
4.	SIM card state	Ready	Indicates the SIM card's state, e.g. PIN required, Not inserted, etc.
5.	Signal strength	-67 dBm	Received Signal Strength Indicator (RSSI). Signal strength measured in dBm
6.	Cell ID	1037079	ID of the operator cell that the device is currently connected to
7.	RSRP	-95 dBm	Indicates the Reference Signal Received Power
8.	RSRQ	-8 dBm	Indicates the Reference Signal Received Quality
9.	SINR	16.3 dBm	Indicates the Signal to Interference plus Noise Ratio

Operator	OMNITEL LT
Operator state	Registered (home)
Connection type	4G (LTE)
Bytes received *	2.1 MB (2244660 bytes)
Bytes sent *	632.0 KB (647137 bytes)

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

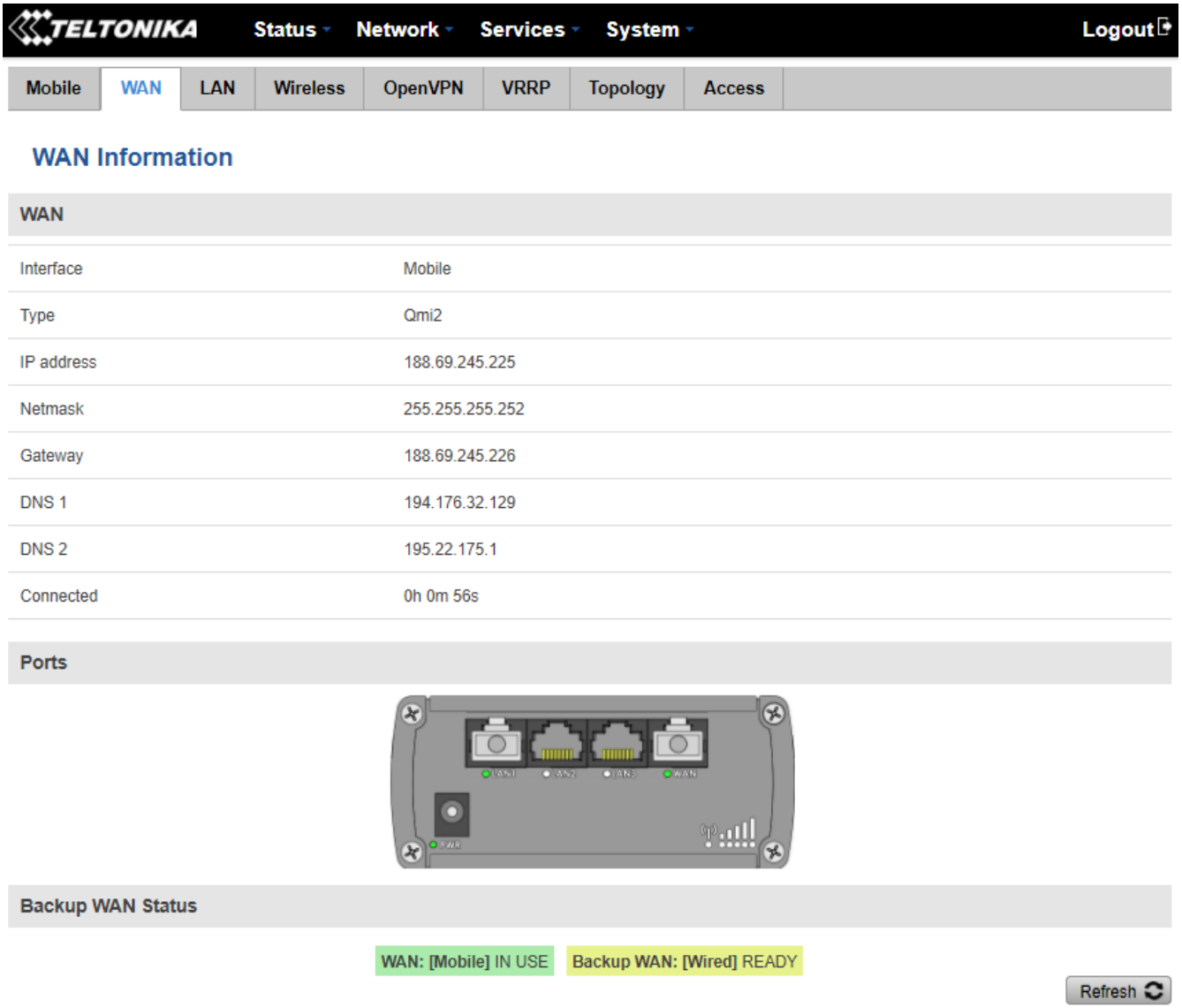
*Your carrier's data usage accounting may differ. Teltonika is not liable should any accounting discrepancies occur.

Teltonika solutions www.teltonika.lt

10.	Operator	LT BITE GSM	Mobile operator's name
11.	Operator state	Registered (home)	GSM network's status
12.	Connection type	4G (LTE)	Indicates the GSM network's access technology
13.	Bytes received	15.7 MB (16453520 bytes)	How many bytes were received via mobile data connection
14.	Bytes sent	624.0 KB (638962 bytes)	How many bytes were sent via mobile data connection
15.	Reboot modem	-	Reboots the modem
16.	Restart connection	-	Restarts the mobile connection
17.	(Re)register	-	Reregisters the SIM card to a network operator
18.	Refresh	-	Refreshes the Mobile Information window

6.3.2 WAN

The WAN Information window displays information about the current WAN connection.



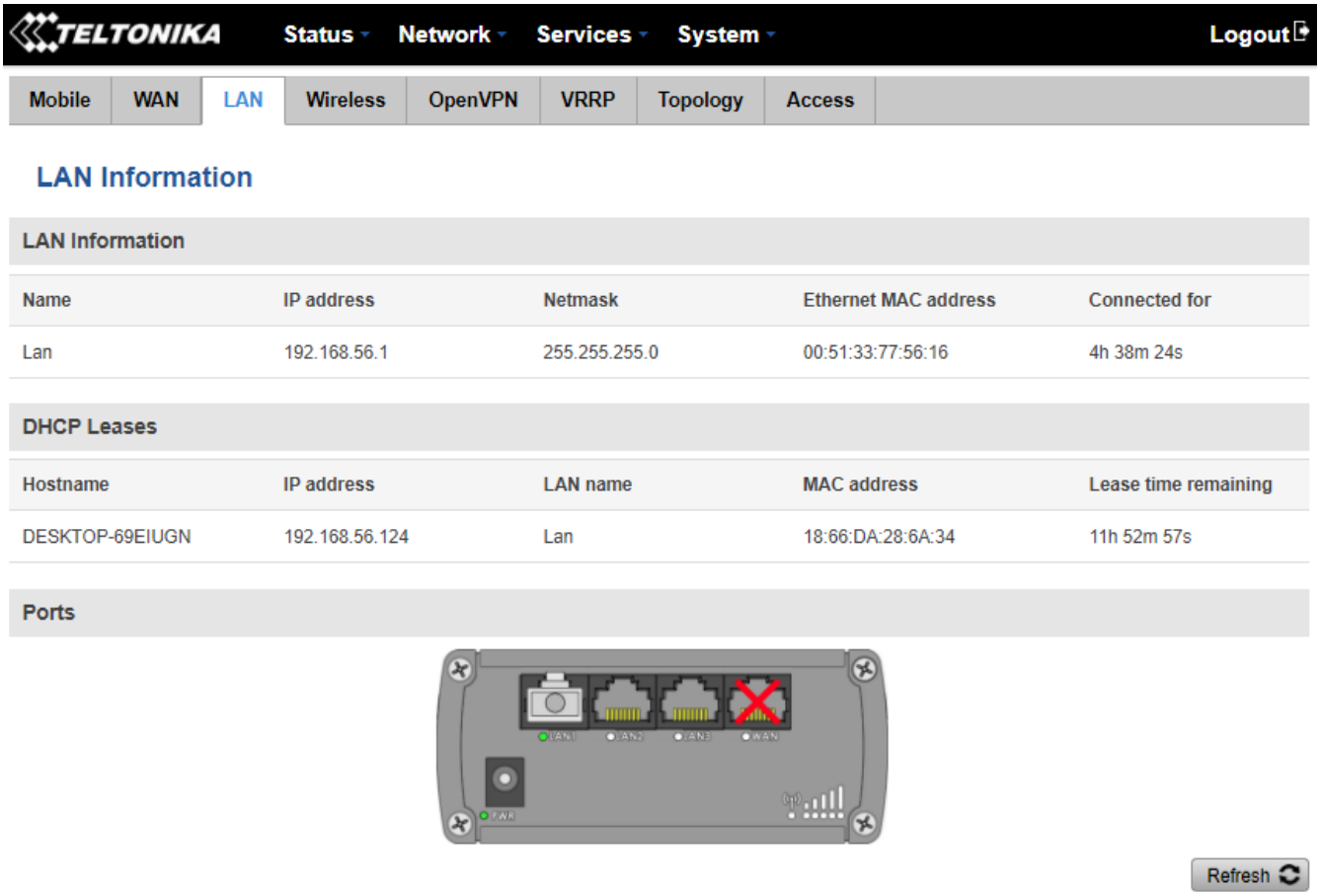
WAN information:

	Field Name	Sample Value	Explanation
1.	Interface	Mobile	Specifies the interface through which the router is connecting to the internet. This can either be Wired, Mobile or Wi-Fi
2.	Type*	Qmi2	Specifies the connection type
3.	IP address	188.69.245.225	The IP address that the router uses to connect the internet
4.	Netmask	255.255.255.252	Specifies a mask used to define how large the WAN network is
5.	Gateway	188.69.245.226	The address where traffic destined for the internet is routed to
6.	DNS 1 DNS 2	194.176.32.129 195.22.175.1	Domain name server(s)
7.	Connected	0h 0m 56s	How long the connection has been successfully maintained
8.	Ports	-	A visual indication of which ports are being used
9.	Backup WAN Status	READY	Indicates the status of backup WAN
10.	Refresh	-	Refreshes the WAN Information window

*** When using a different WAN interface, this field shows the type of protocol being used. It can either be DHCP, Static or PPPoE.**

6.3.3 LAN

The LAN Information window displays information about LAN connections.



LAN information:

	Field Name	Sample Value	Explanation
1.	Name	Lan	Lan instance name
2.	IP address	192.168.56.1	The address that the router uses on the LAN network
3.	Netmask	255.255.255.0	A mask used to define how large the LAN network is
4.	Ethernet MAC address	00:51:33:77:56:16	MAC (Media Access Control) address used for communication in an Ethernet LAN
5.	Connected for	4h 38m 24s	How long LAN has been successfully maintained

DHCP Leases

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

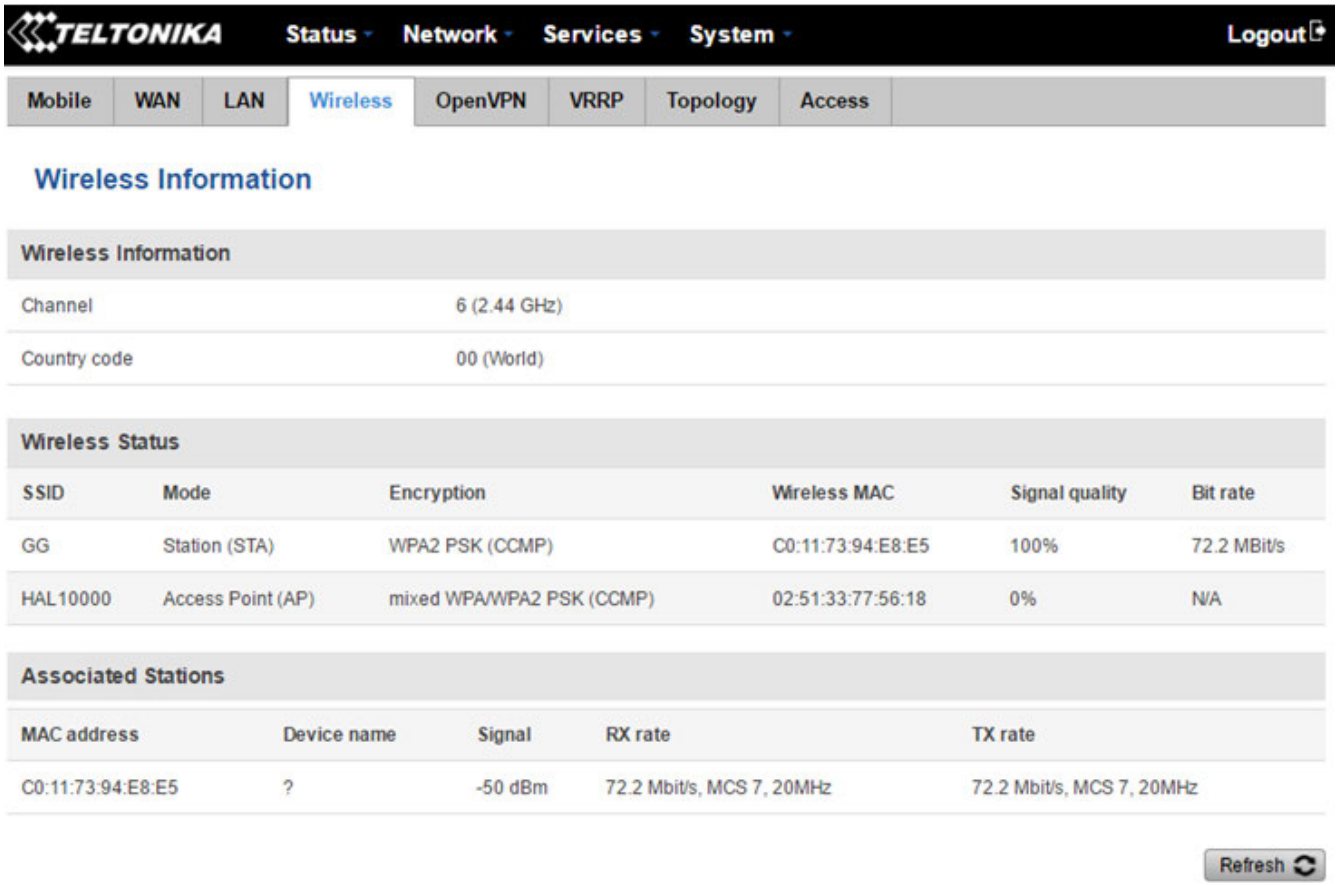
	Field Name	Sample Value	Explanation
1.	Hostname	DESKTOP-69EIUGN	DHCP client's hostname
2.	IP address	192.168.56.124	The IP address of one of the device's connected to the LAN
3.	LAN name	Lan	Lan instance name
4.	MAC address	18:66:DA:28:6A:34	The MAC address of the network interface on which the lease will be used.
5.	Lease time remaining	11h 52m 57s	Remaining lease time for addresses handed out to clients
6.	Ports	-	A visual indication of which ports are being used
7.	Refresh	-	Refreshes the LAN Information window

6.3.4 Wireless

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

6.3.4.1 Station

The Wireless Information window displays information about wireless connections (Station mode.)

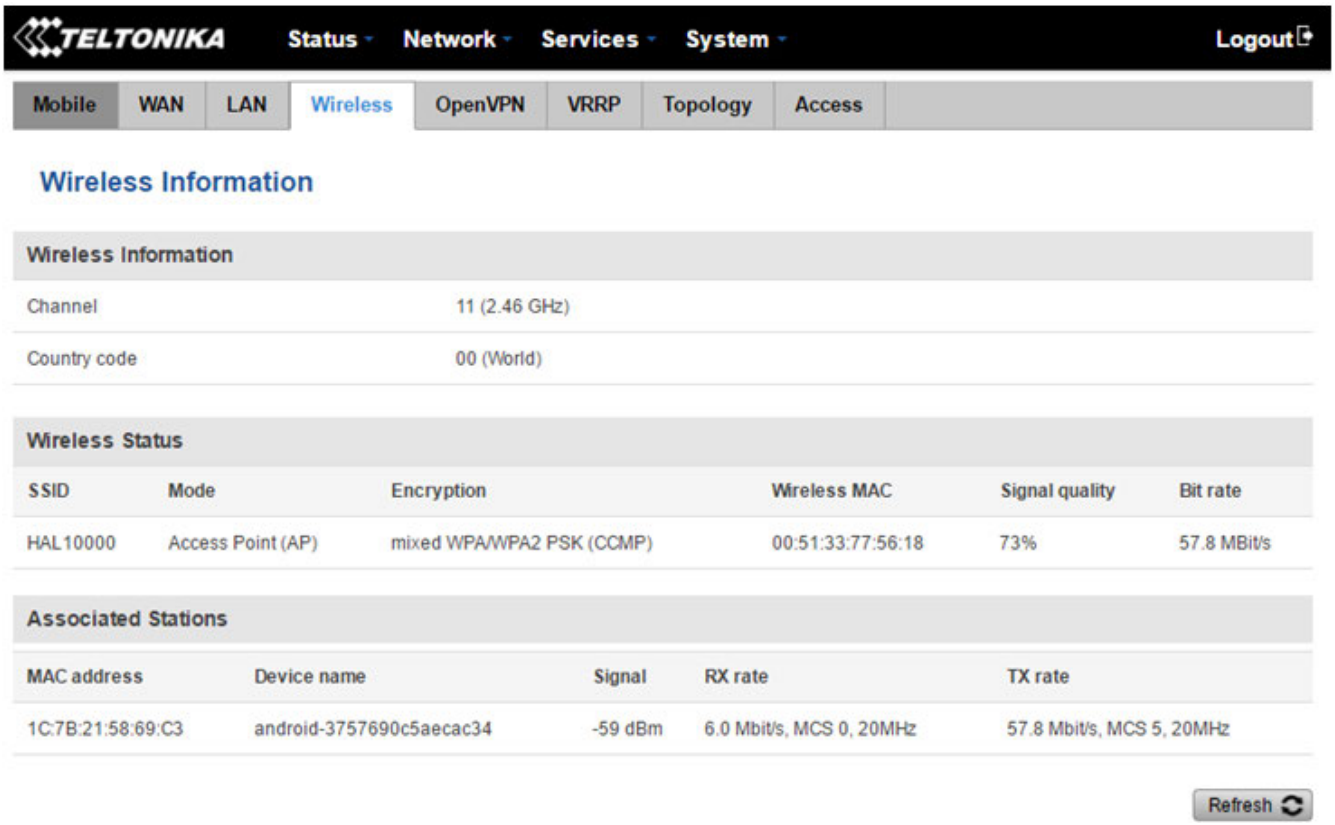


Client mode information

	Field Name	Sample Value	Explanation
1.	Channel	6 (2.44 GHz)	The channel that the AP, to which the router is connected to, uses. Your wireless radio is forced to work on this channel in order to maintain the connection
2.	Country	00 (World)	Country code
3.	SSID	GG	The SSID that the AP, to which the router is connected to, uses
4.	Mode	Station (STA)	Indicates that the router is a client to some local AP
5.	Encryption	WPA2 PSK (CCMP)	The type of encryption that the AP uses
6.	Wireless MAC	C0:11:73:94:E8:E5	The MAC address of the access point's radio
7.	Signal Quality	100%	The quality between the router's 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	72.2 MBit/s	The maximum possible physical throughput that the router's radio can handle. Keep in mind that this value is cumulative - the bitrate will be shared between the router and other possible devices that connect the local AP

6.3.4.2 Access Point

The Wireless Information window displays information about wireless connections (Access Point mode.)



Wireless AP information

	Field Name	Sample Value	Explanation
1.	Channel	11 (2.46 GHz)	The channel that is used to broadcast the SSID and to establish new connections to devices
2.	Country code	00(World)	Country code
3.	SSID	HAL10000	The SSID is a name by which other devices will recognize the router
4.	Mode	Access Point (AP)	Indicates that you router is an access point
5.	Encryption	Mixed WPA/WPA2 PSK (CCMP)	The type of encryption that the router uses to authenticate, establish and maintain connections
6.	Wireless MAC	00:51:33:77:56:18	MAC address of the router's wireless radio
7.	Signal Quality	73%	The signal quality between the router's radio and another device that is connected to the router. Will show 0% if no devices are trying to connect or are currently maintaining a connection
8.	Bit rate	57.8 MBit/s	The bitrate shared between all devices that are connected to the router's wireless network

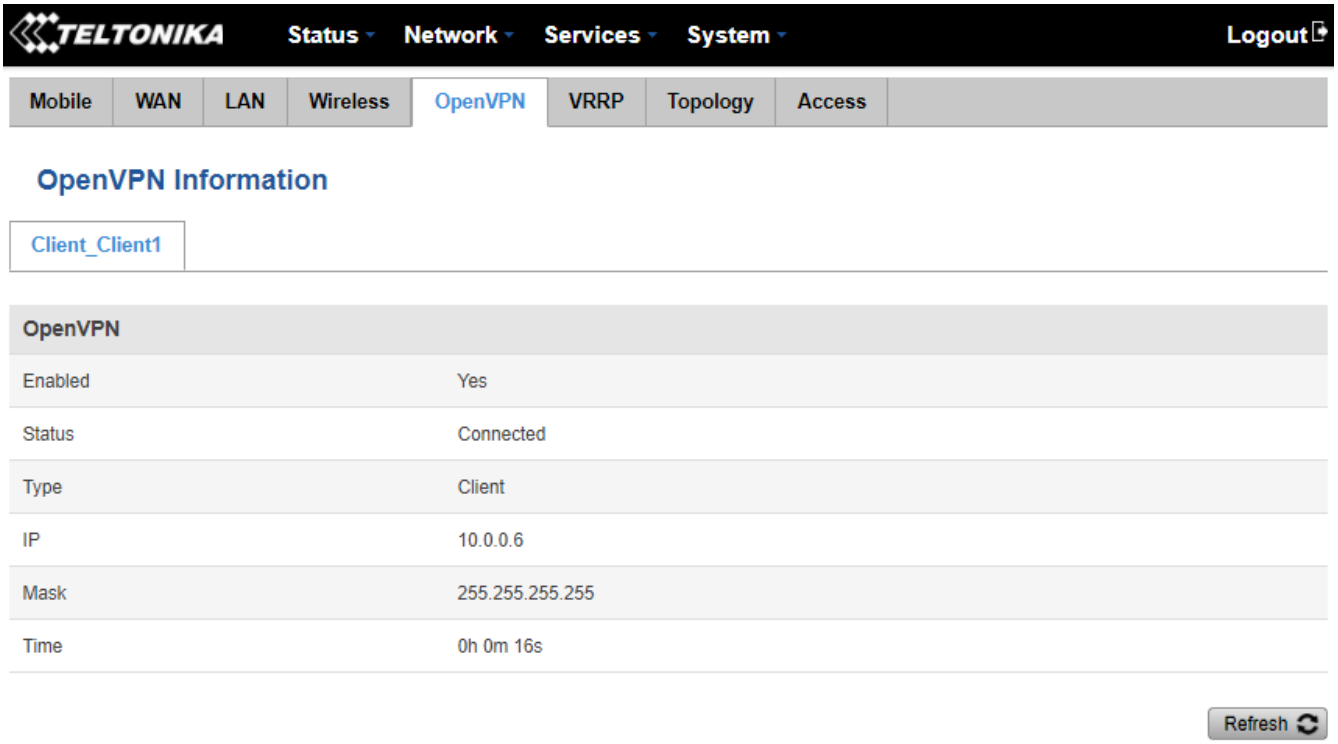
*Associated stations**

	Field Name	Sample Value	Explanation
1.	MAC Address	1C:7B:21:58:69:C3	Associated station's MAC (Media Access Control) address
2.	Device Name	android-3757690c5aecac34	DHCP client's hostname
3.	Signal	-59 dBm	Received Signal Strength Indicator (RSSI)
4.	RX Rate	6.0Mbit/s, MCS 5, 20MHz	The rate at which packets are received from the associated station
5.	TX Rate	57.8Mbit/s, MCS 5, 20MHz	The rate at which packets are sent to the associated station

* **This can either be the information of the Access Point that the router is connected to in STA mode or a list of all devices that are connected to the router's AP.**

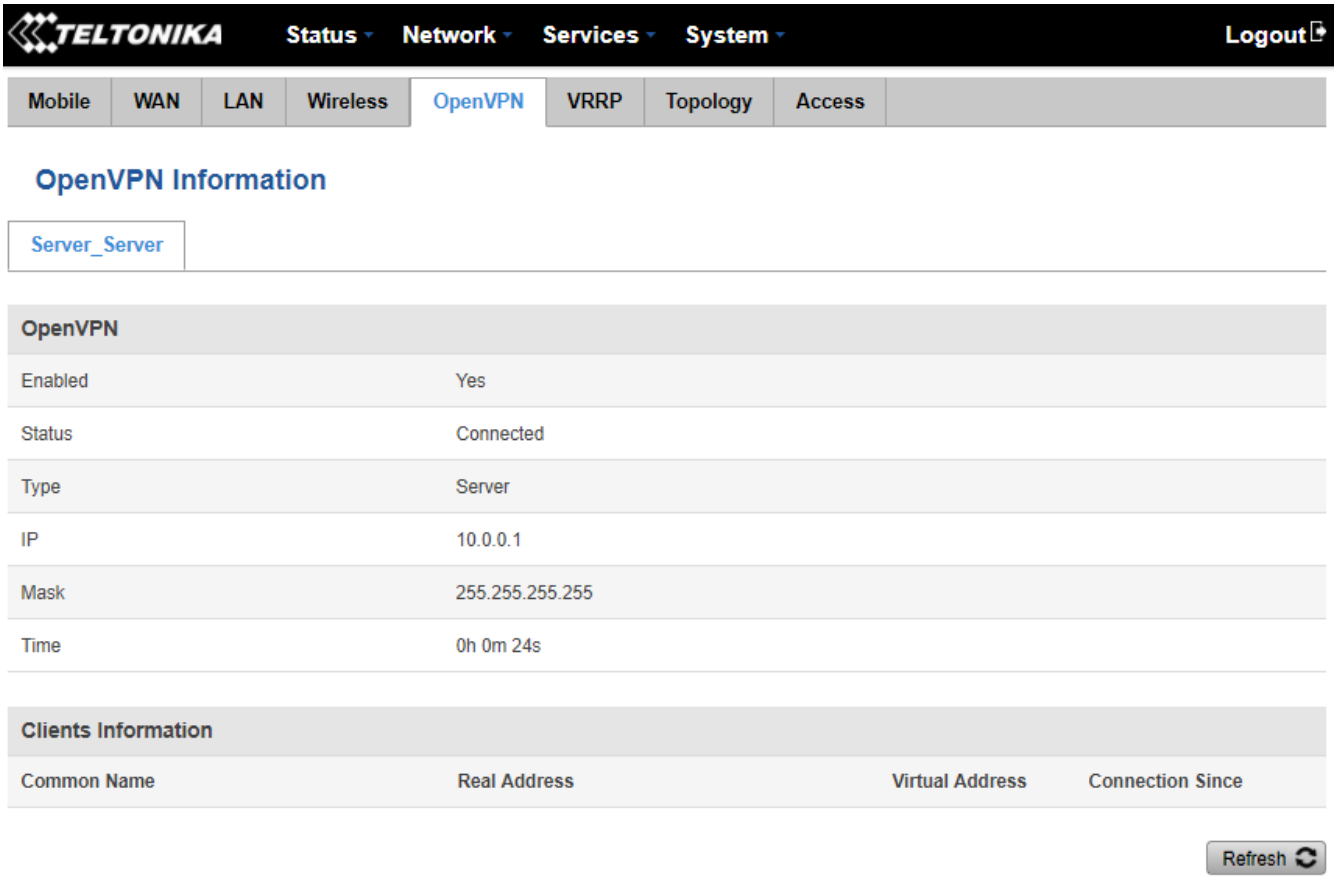
6.3.5 OpenVPN Client

The OpenVPN Information window displays OpenVPN client or server information.



	Field Name	Sample Value	Explanation
1.	Enabled	Yes	OpenVPN status
2.	Status	Connected	Connection status
3.	Type	Client	The type of OpenVPN instance that has been created
4.	IP	10.0.0.6	Remote virtual network's IP address
5.	Mask	255.255.255.255	Remote virtual network's subnet mask
6.	Time	0h 0m 16s	Connection uptime

6.3.6 OpenVPN Server



	Field Name	Sample Value	Explanation
1.	Enabled	Yes	OpenVPN status
2.	Status	Connected	Connection status
2.	Type	Server	The type of OpenVPN instance that has been created
3.	IP	10.0.0.1	Remote virtual network's IP address
4.	Mask	255.255.255.255	Remote virtual network's subnet mask
5.	Time	0h 0m 28s	Connection uptime

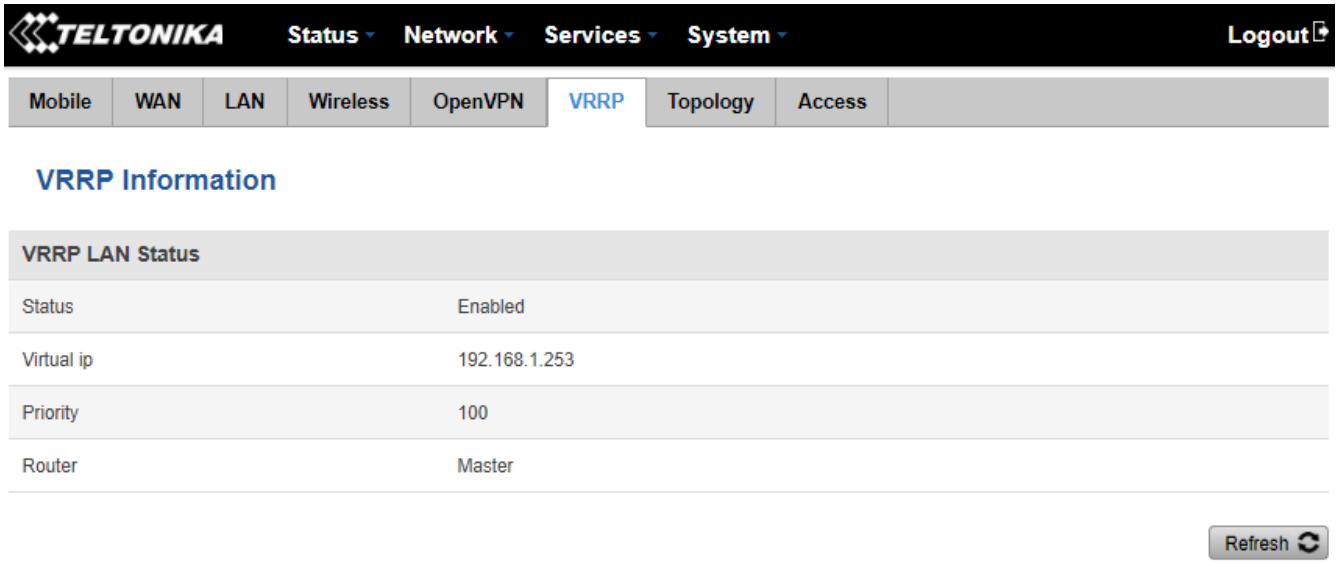
*Clients Information**

	Field Name	Possible Values	Explanation
1.	Common Name	Test001	Client's common name
2.	Real Address	212.59.13.225:52638	Client's IP address and port number
3.	Virtual Address	10.0.0.6	Virtual address which has been given to a client
4.	Connection Since	Thu May 05 2016 07:46:29 GMT + 0300 (FLE Standard Time)	Since when the connection has been established

*** The OpenVPN Information window also shows connected client information when an OpenVPN TLS server instance is online.**

6.3.7 VRRP

The VRRP Information window displays VRRP(Virtual Router Redundancy Protocol) LAN Status.

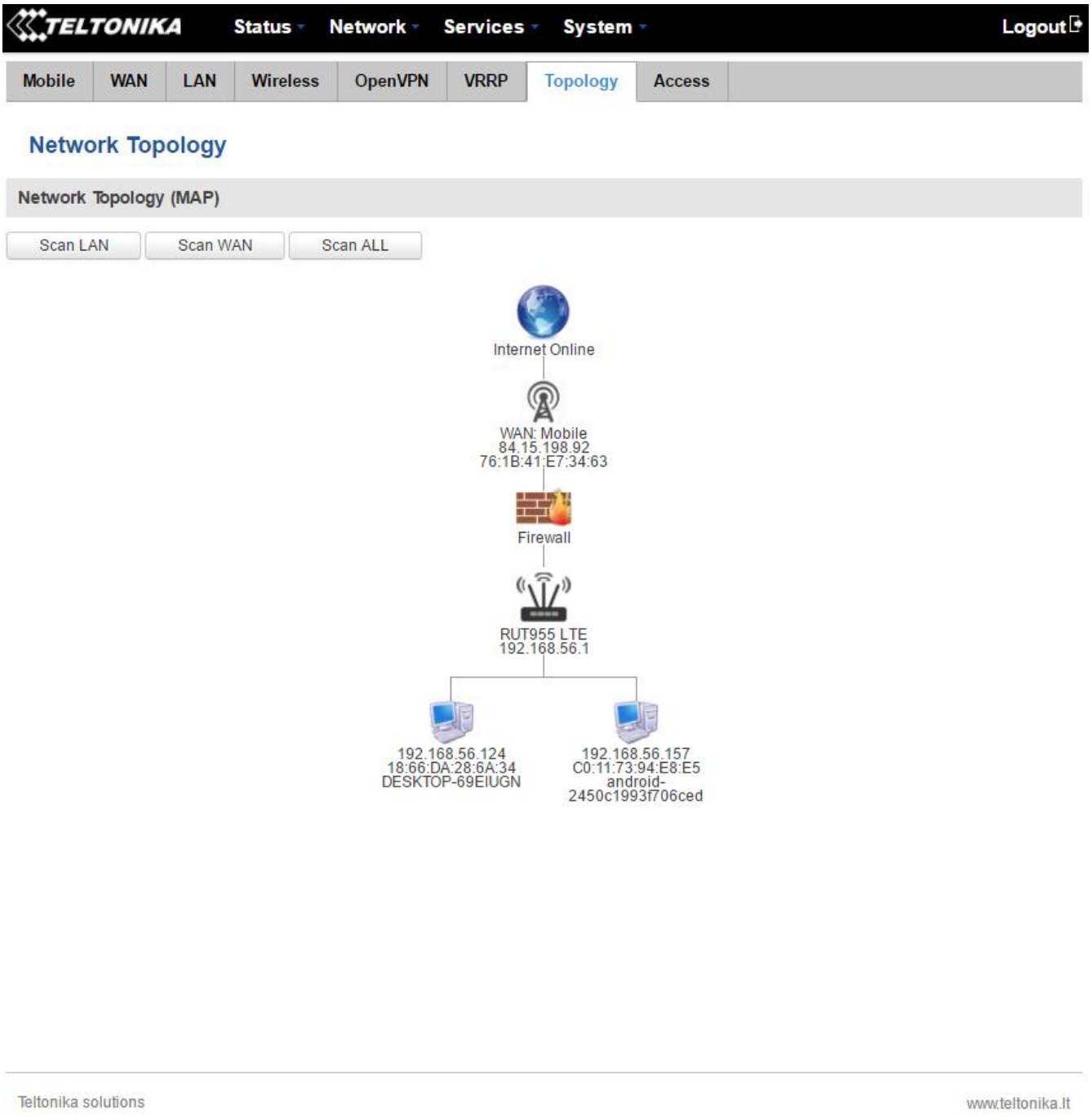


	Field Name	Sample Value	Explanation
1.	Status	Enabled	VRRP status
2.	Virtual IP	192.168.1.253	Virtual IP address (-es) for LAN's VRRP (Virtual Router Redundancy Protocol) cluster
3.	Priority	100	Router with the highest priority value on the same VRRP cluster will act as a master; range [1 - 255]
4.	Router*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

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

6.3.8 Topology

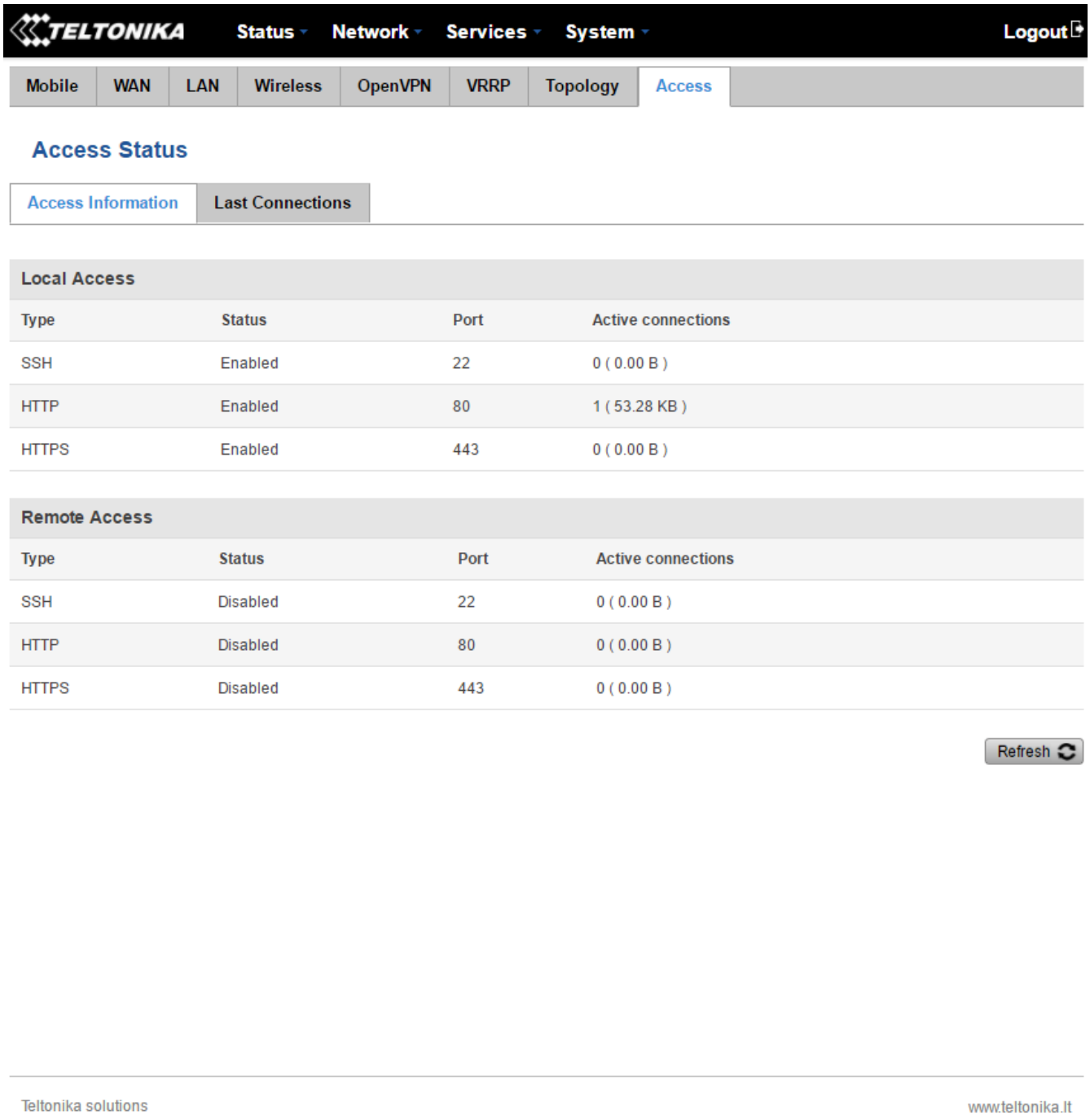
The Network Topology window provides the ability to scan and quickly retrieve information about devices in your network. When the router uses Mobile as WAN and the selected Connection type is „PPP", you can only scan the LAN side.



6.3.9 Access

6.3.9.1 Access Status

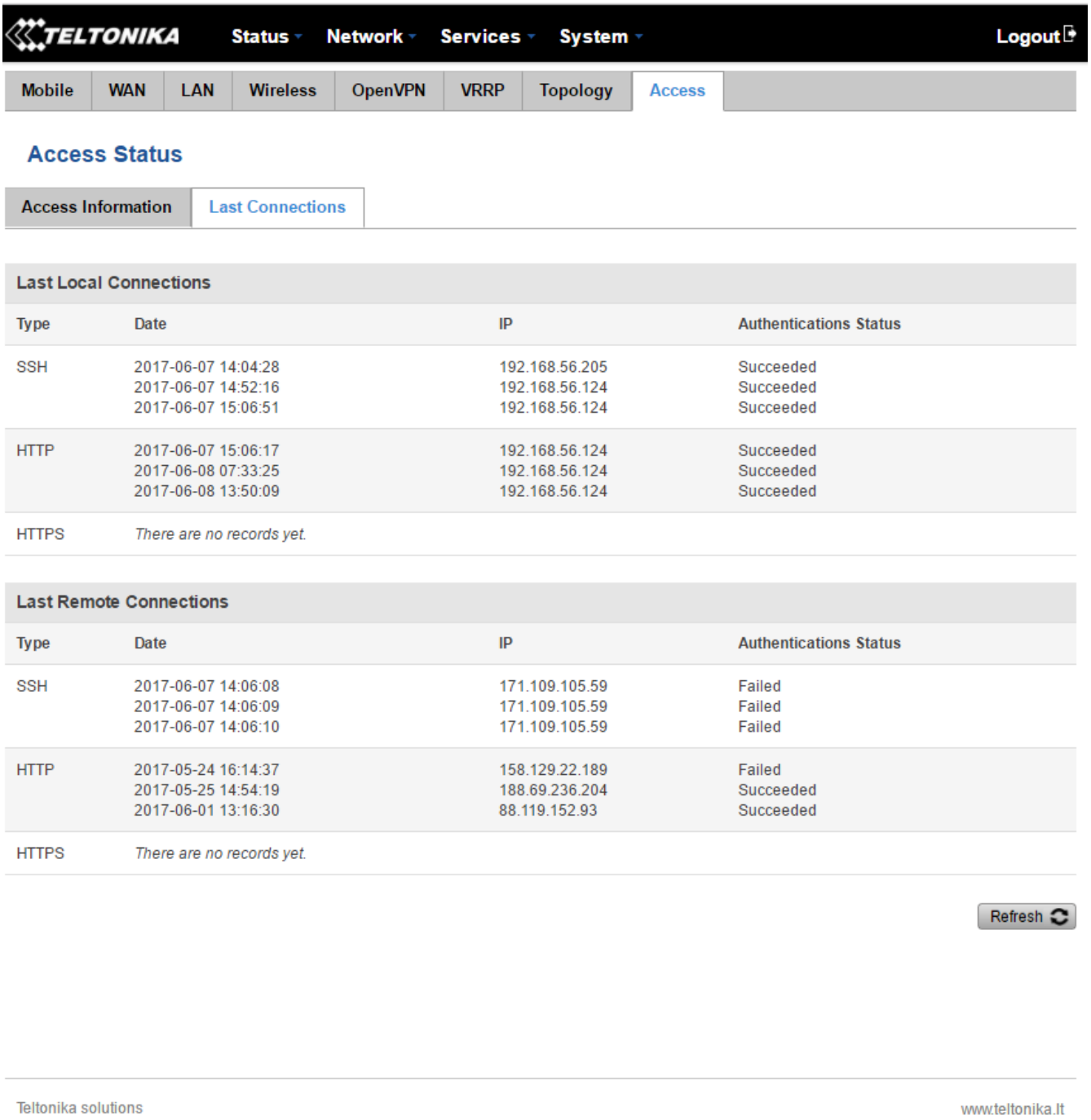
The Access Status window displays information about active local and remote SSH, HTTP and HTTPS connections.



	Field Name	Possible Values	Explanation
1.	Type	SSH; HTTP; HTTPS	Type of connection protocol
2.	Status	Disabled/Enabled	Connection status
3.	Port	22; 80; 443	Port used for the connection
4.	Active connections	0(0.00B);1(53.28 KB); 0(0.00 B)	Count of active connections and amount of data transmitted

6.3.9.2 Last Connections

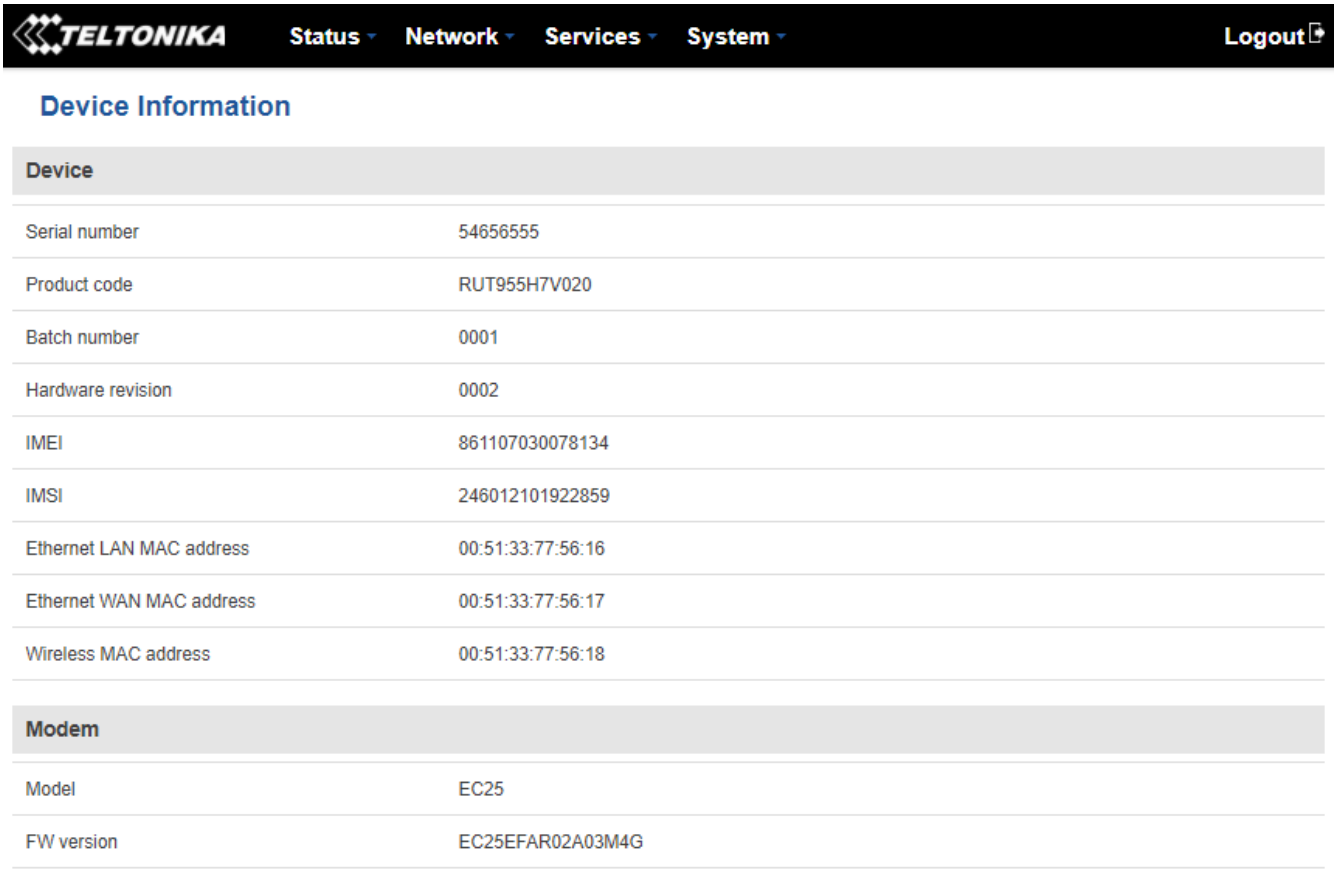
The Last Connections window displays information about the last 3 connections for each of the different connection types.



	Field Name	Possible 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	192.168.56.205	IP address from which the connection was made
4.	Authentications Status	Failed; Succeeded	Result of authentication attempt

6.4 Device information

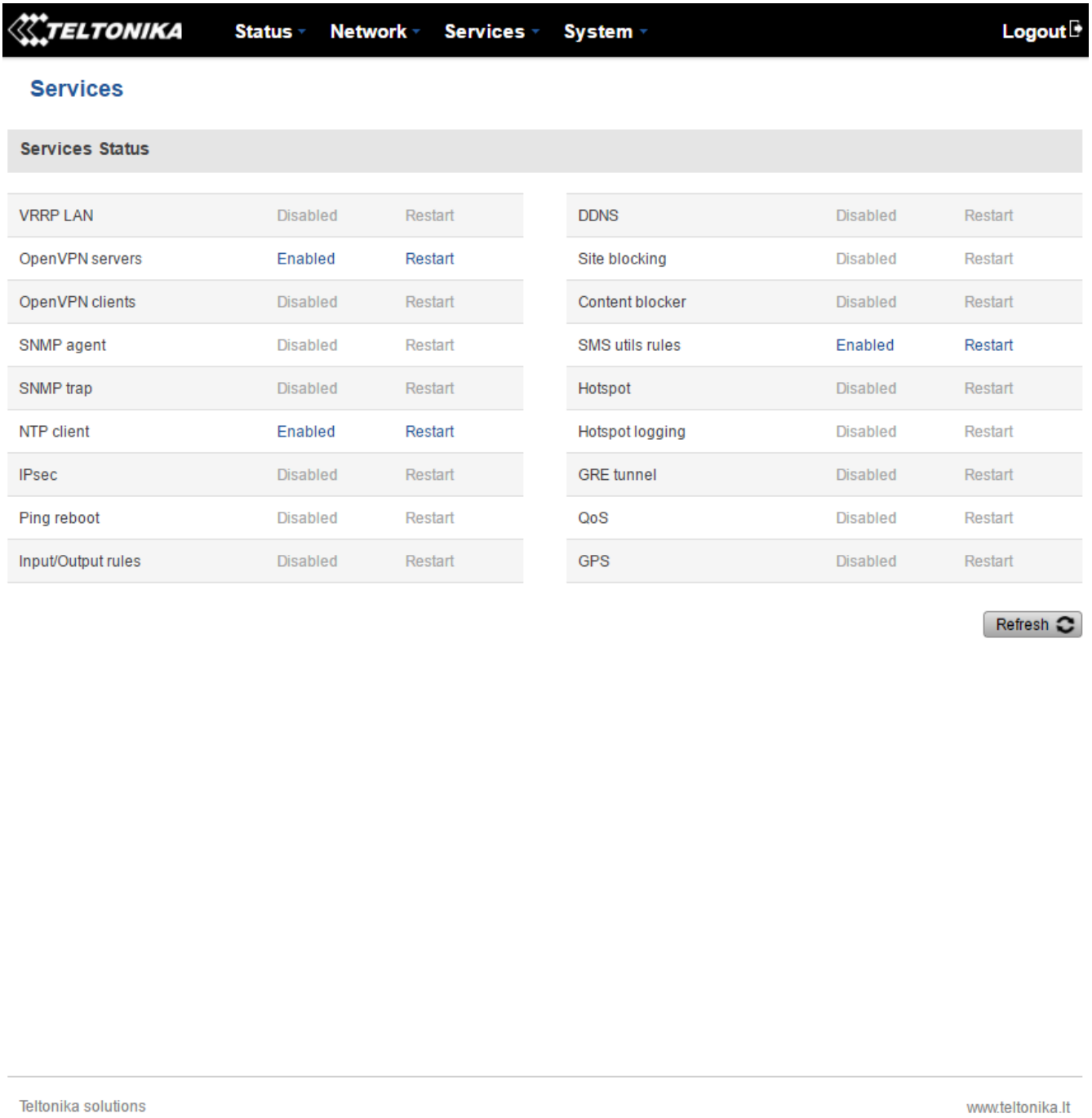
The Device Information page displays factory information that was written into the device during the manufacturing process.



	Field Name	Sample Value	Explanation
1.	Serial number	54656	Serial number of the device
2.	Product code	RUT955H7V020	Product code of the device
3.	Batch number	0001	Batch number used during device's manufacturing process
4.	Hardware revision	0002	Hardware revision of the device
5.	IMEI	861107030078134	Identification number of the internal modem
6.	IMSI	246020100944448	Subscriber identification number of the internal modem
6.	Ethernet LAN MAC	00:51:33:77:56:16	MAC address of the Ethernet LAN ports
7.	Ethernet WAN MAC	00:51:33:77:56:17	MAC address of the Ethernet WAN port
8.	Wireless MAC	00:51:33:77:56:18	MAC address of the Wi-Fi interface
9.	Model	EC25	Router's modem model
10.	FW version	EC25EFAR02A03M4G	Router's modem firmware version

6.5 Services

The Services page displays the status of available services and gives you the ability turn them on/off or restart them.

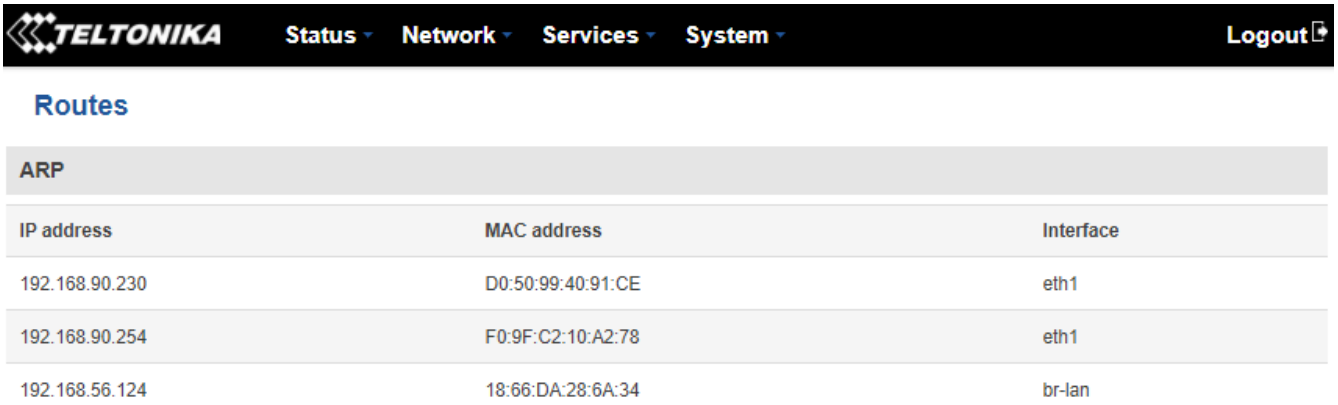


6.6 Routes

The Routes page displays the router's ARP table and active IP and IPv6 routes.

6.6.1 ARP

The ARP table shows the router's recently cached MAC addresses of every immediate device that was communicating with the router.



	Field Name	Sample Value	Explanation
1.	IP address	192.168.56.235	Recently cashed IP addresses of every immediate device that was communicating with the router
2.	MAC address	1C:7B:21:58:69:C3	Recently cached MAC addresses of every immediate device that was communicating with the router
3.	Interface	br-lan	Interface that the device used for connection

6.6.2 Active IP Routes

The Active IP Routes section shows the router's routing table. The routing table indicates where a TCP/IP packet with a specific IP address will be directed to.

Active IP Routes

Network	Target	IP gateway	Metric
wan	0.0.0.0/0	192.168.90.254	0
tun_rms	10.100.96.0	0.0.0.0	0
tun_rms	10.100.96.0/19	10.100.96.0	0
lan	192.168.56.0/24	0.0.0.0	0
wan	192.168.90.0/24	0.0.0.0	0

	Field Name	Sample Value	Explanation
1.	Network	wan	Interface used to transmit TCP/IP packets through
2.	Target	0.0.0.0	Indicates where a TCP/IP packet with a specific IP address will be directed
3.	IP gateway	192.168.90.254	Indicates through which gateway a TCP/IP packet will be directed
4.	Metric	0	Indicates interface's priority of usage

6.6.3 Active IPv6-Routes

The Active IPv6-Routes table shows active IPv6 routes for data packet transition.

Active IPv6-Routes

Network	Target	IPv6 gateway	Metric
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF
loopback	0:0:0:0:0:0:0:1	0:0:0:0:0:0:0:0/0	00000000
wan	FF02:0:0:0:0:0:0:C	0:0:0:0:0:0:0:0/0	00000000
wan	FF02:0:0:0:0:0:0:FB	0:0:0:0:0:0:0:0/0	00000000
wan	FF02:0:0:0:0:0:1:2	0:0:0:0:0:0:0:0/0	00000000
wan	FF02:0:0:0:0:0:1:3	0:0:0:0:0:0:0:0/0	00000000
wan	FF02:0:0:0:0:1:FF9C:DCEF	0:0:0:0:0:0:0:0/0	00000000
wan	FF02:0:0:0:0:1:FFE5:F7AD	0:0:0:0:0:0:0:0/0	00000000
wan	FF00:0:0:0:0:0:0:0/8	0:0:0:0:0:0:0:0/0	00000100
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF

Teltonika solutions www.teltonika.lt

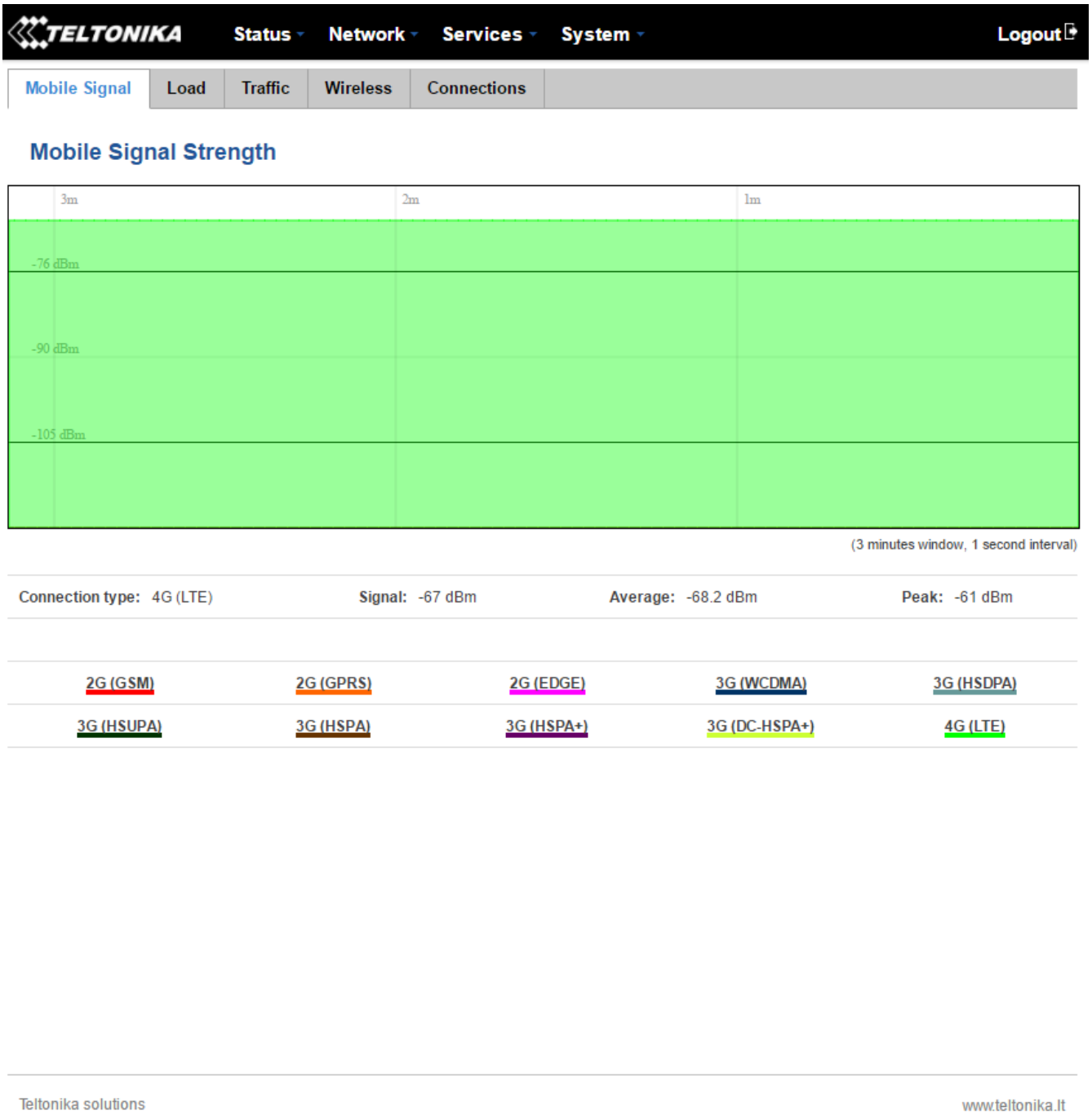
	Field Name	Sample Value	Explanation
1.	Network	loopback	Network interface used
2.	Target	0:0:0:0:0:0:0:0/0	Indicates where a TCP/IP packet with a specific IP address will be directed
3.	IPv6 gateway	0:0:0:0:0:0:0:0/0	Indicates through which gateway a TCP/IP packet will be directed
4.	Metric	FFFFFFFF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

6.7 Graphs

The Real-time graph window displays various statistical data changes over time in the form of graphs.

6.7.1 Mobile Signal Strength

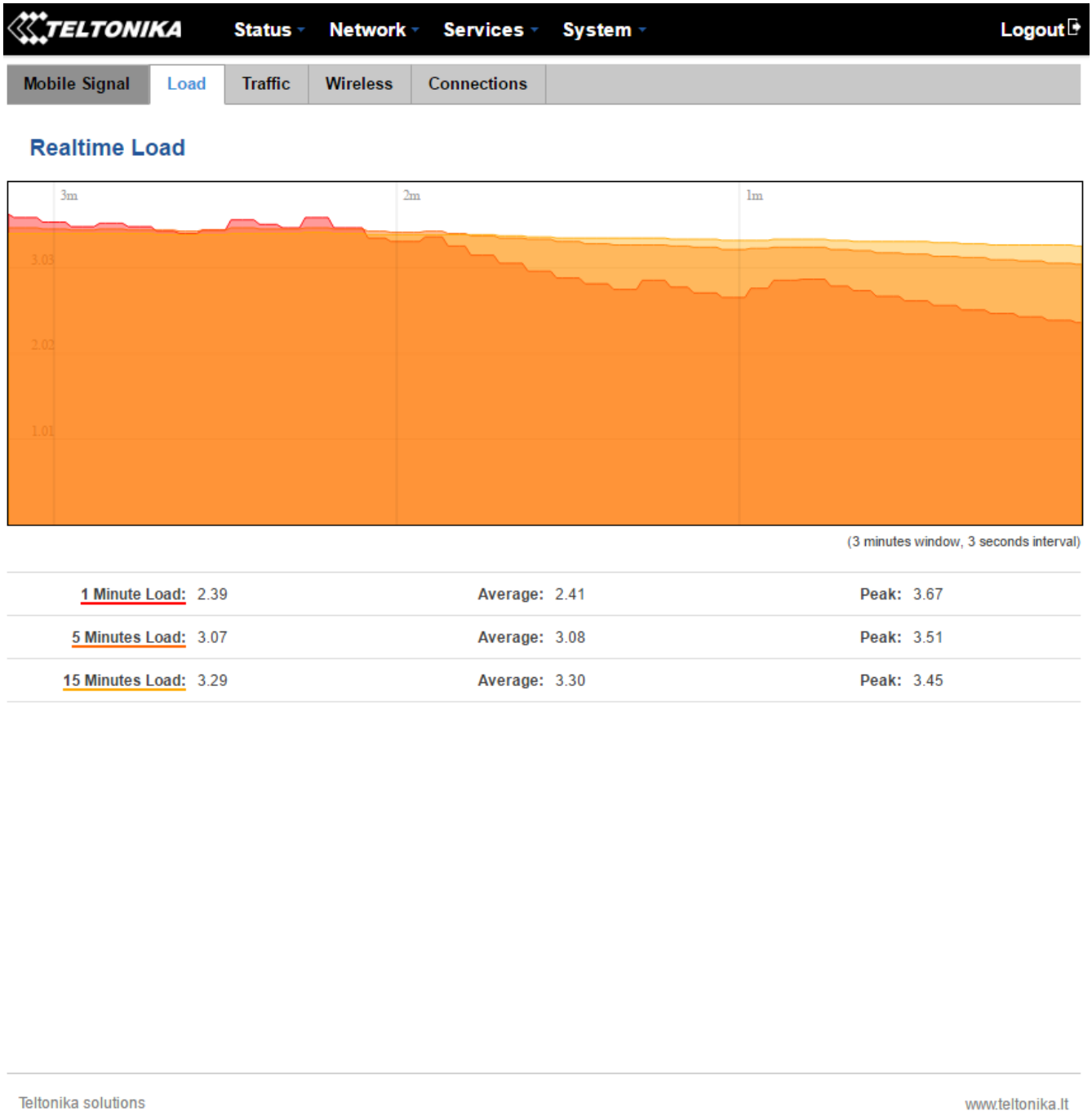
The Mobile Signal strength graph displays mobile signal strength variation in time (measured in dBm).



	Field Name	Sample Value	Explanation
1.	Connection type	4G (LTE)	Type of mobile connection used
2.	Signal	-67 dBm	Current signal strength value
3.	Average	-68.2 dBm	Average signal strength value
4.	Peak	-61 dBm	Peak signal strength value

6.7.2 Realtime Load

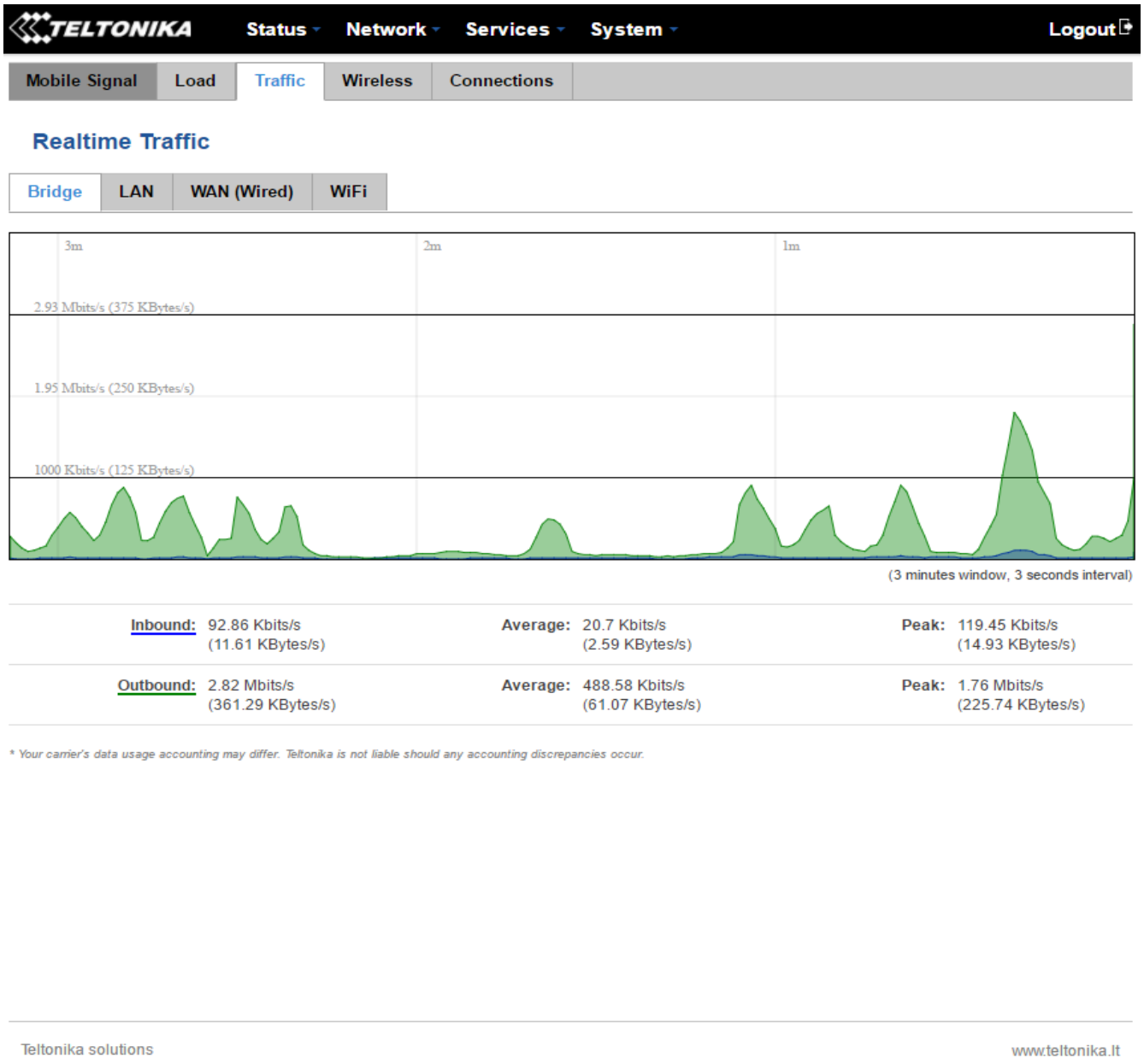
The Realtime Load window displays a tri-graph that illustrates average CPU load values in real time. The graph consists out of three color coded graphs, each one corresponding to the average CPU load over 1 (red), 5 (orange) and 15 (yellow) most recent minutes.



	Field Name	Sample Value	Explanation
1.	1/5/15 Minute Load	2.39	Time interval for load averaging, colour of the diagram
2.	Average	2.41	Average CPU load value over a time interval (1/5/15 Minute)
3.	Peak	3.67	Peak CPU load value of the time interval

6.7.3 Realtime Traffic

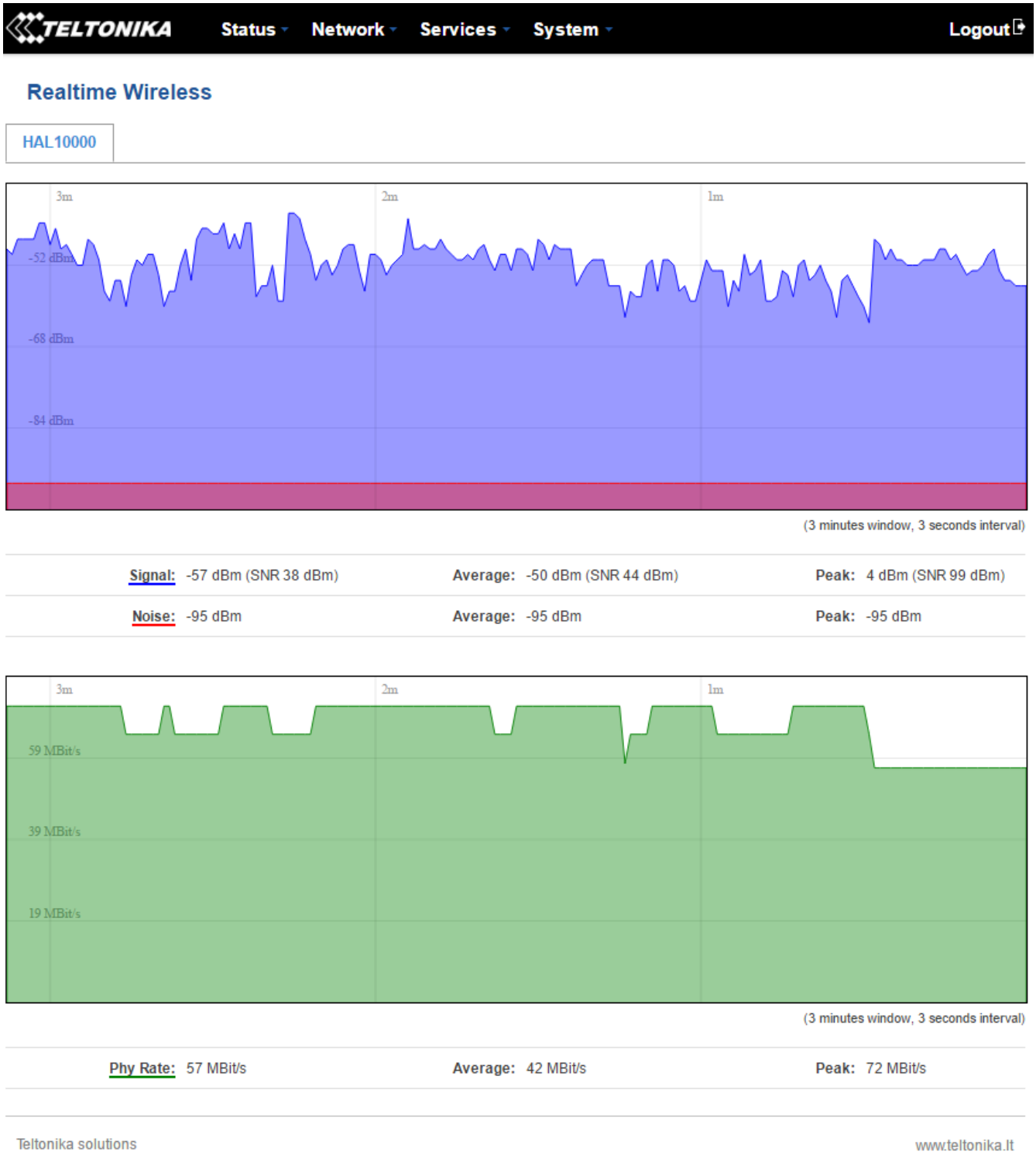
The Realtime Traffic window lets you monitor average inbound and outbound traffic over the course of ~3 minutes; each new measurement is taken every 3 seconds. The graphs consist out of two color coded graphs: the green graph shows the outbound traffic, the blue graph shows the inbound traffic. Although not graphed, the page also displays peak loads and averages of inbound and outbound traffic.



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

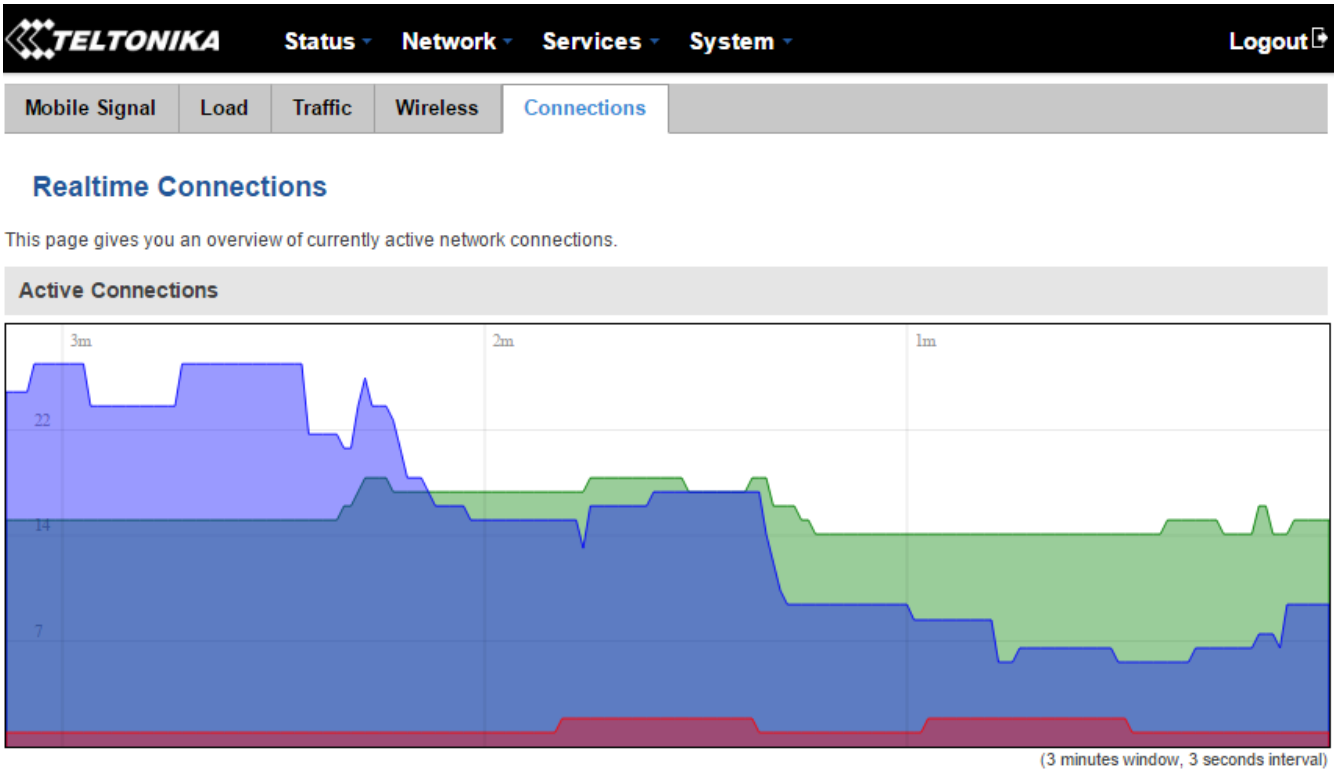
6.7.4 Realtime Wireless

The Realtime Wireless window displays the wireless radio signal strength, signal noise, average and peak signal levels and the theoretical maximum channel permeability.



6.7.5 Realtime Connections

The Realtime Connections window displays currently active network connections with the information about network, protocol, source and destination addresses and transfer speed.

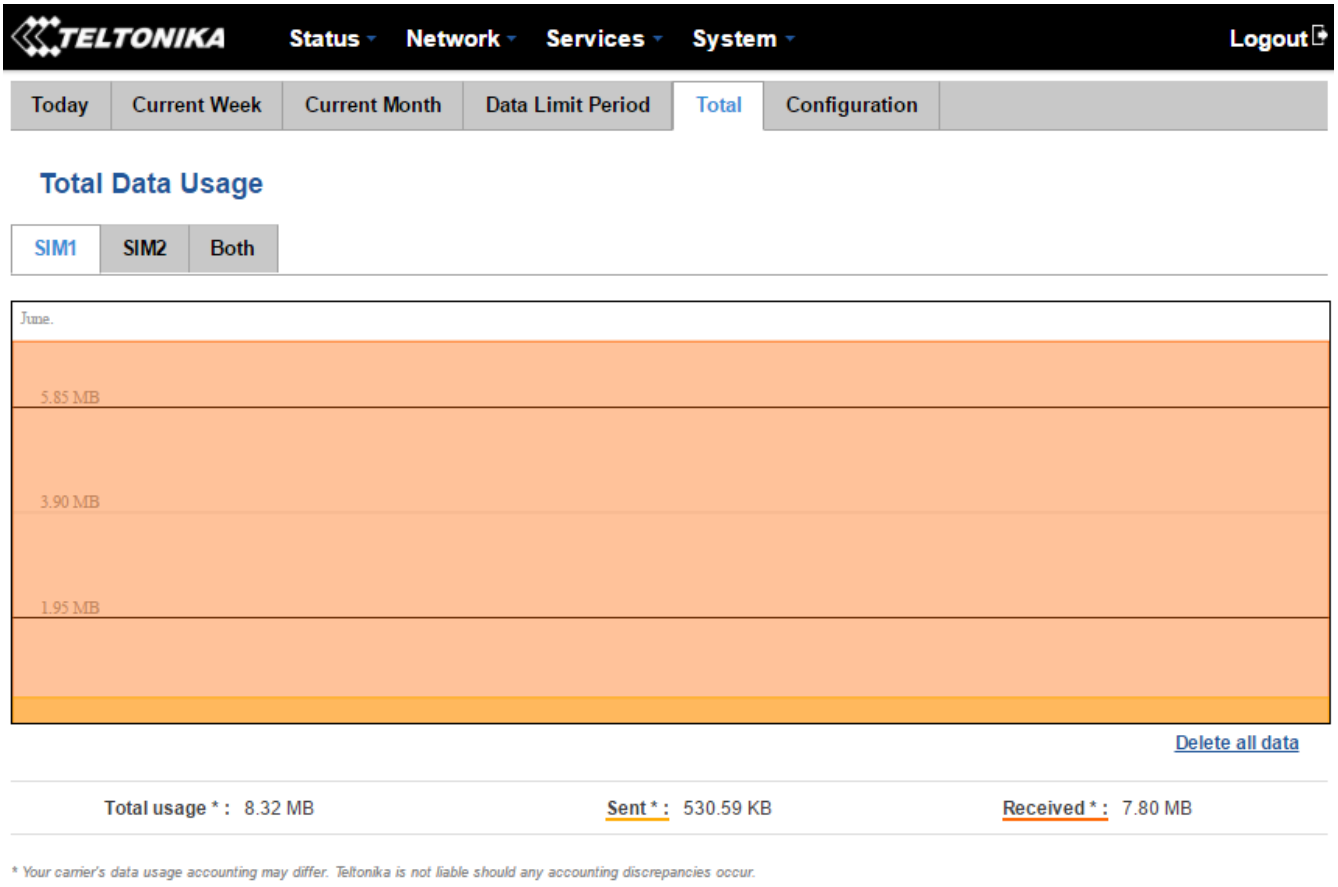


UDP: 10	Average: 9	Peak: 27
TCP: 16	Average: 15	Peak: 19
Other: 1	Average: 1	Peak: 2

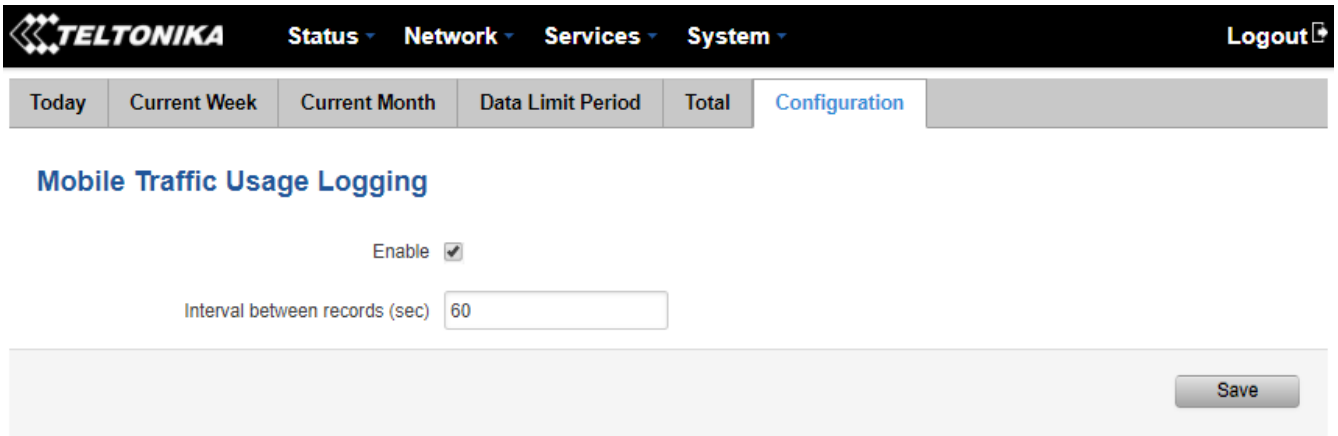
Network	Protocol	Source	Destination	Transfer
IPV4	TCP	DESKTOP-69EIUGN.lan:59208	192.168.90.230:3389	3.58 MB (24759 Pkts.)
IPV4	UDP	DESKTOP-69EIUGN.lan:50810	212.59.13.226:4090	1.02 MB (20641 Pkts.)
IPV4	TCP	DESKTOP-69EIUGN.lan:61216	Teltonika-RUT955.com.lan:80	629.19 KB (6224 Pkts.)
IPV4	TCP	DESKTOP-69EIUGN.lan:61221	Teltonika-RUT955.com.lan:80	612.46 KB (6158 Pkts.)
IPV4	TCP	DESKTOP-69EIUGN.lan:61283	Teltonika-RUT955.com.lan:80	421.54 KB (3986 Pkts.)
IPV4	UDP	DESKTOP-69EIUGN.lan:65170	cache.google.com:443	413.54 KB (5901 Pkts.)
IPV4	TCP	DESKTOP-69EIUGN.lan:61209	db5sch101110527.wns.windows.com:443	278.26 KB (2887 Pkts.)
IPV4	TCP	DESKTOP-69EIUGN.lan:58229	212.59.13.226:4090	182.45 KB (3286 Pkts.)
IPV4	TCP	DESKTOP-69EIUGN.lan:61322	edge-star-shv-01-waw1.facebook.com:443	28.55 KB (158 Pkts.)

6.8 Mobile Traffic

The Mobile Traffic graphs display the mobile connection data that was sent and received this day, week or month for each or both of the SIM cards.



By default the mobile traffic usage logging is disabled. In order to use this function, you will have to enable it in the Configuration tab.



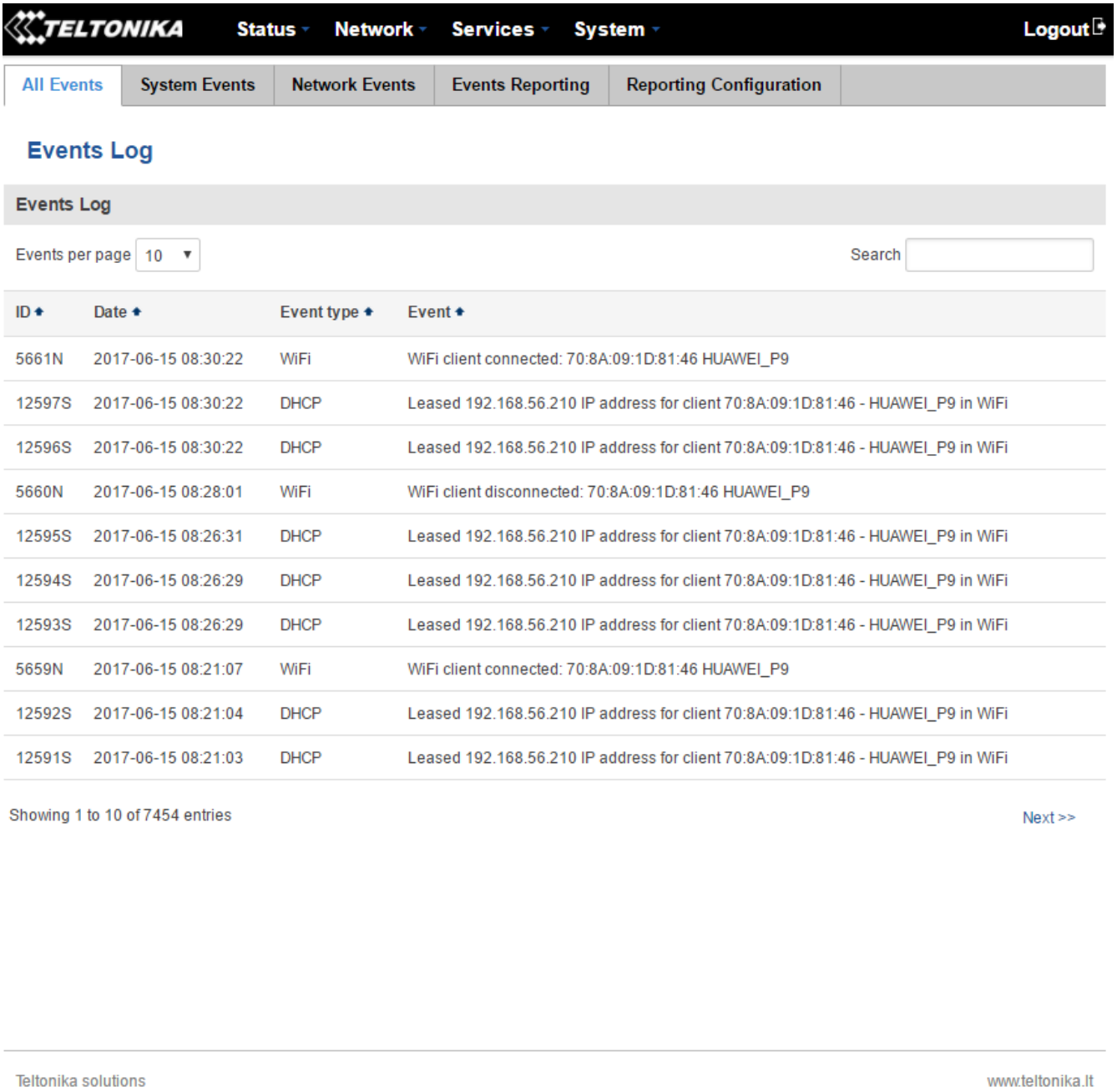
	Field Name	Possible Value	Explanation
1.	Enable	Enable/Disable	Makes the function active or inactive
2.	Interval between records (sec)	(minimum) 60 (sec)	The interval between logging records

6.9 Events Log

The Events Log windows display records of such event as logins, reboots, resets, connections and configuration changes.

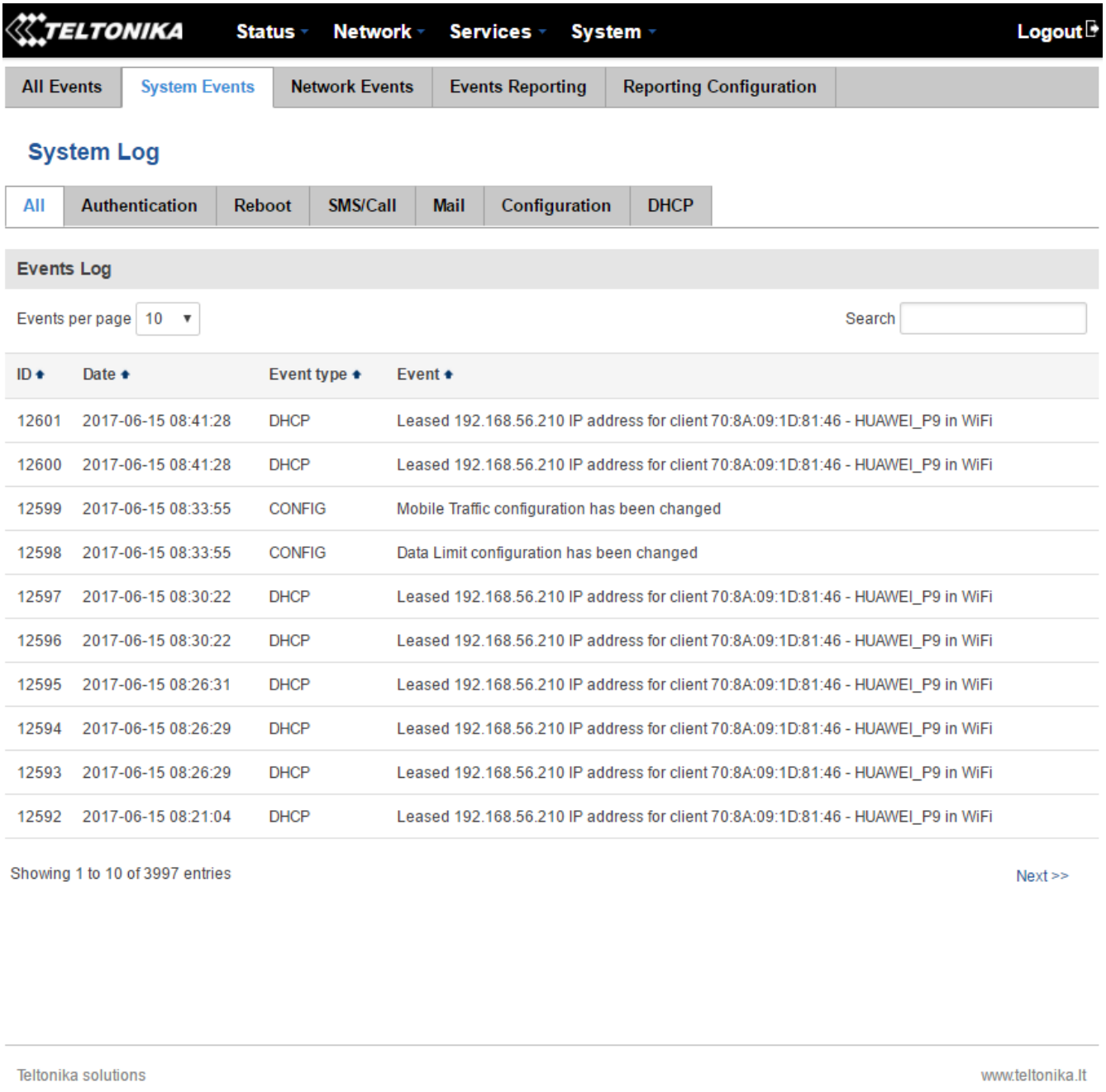
6.9.1 All Events

The All Events window displays all of the router's recorded events, their types and times of occurrence.



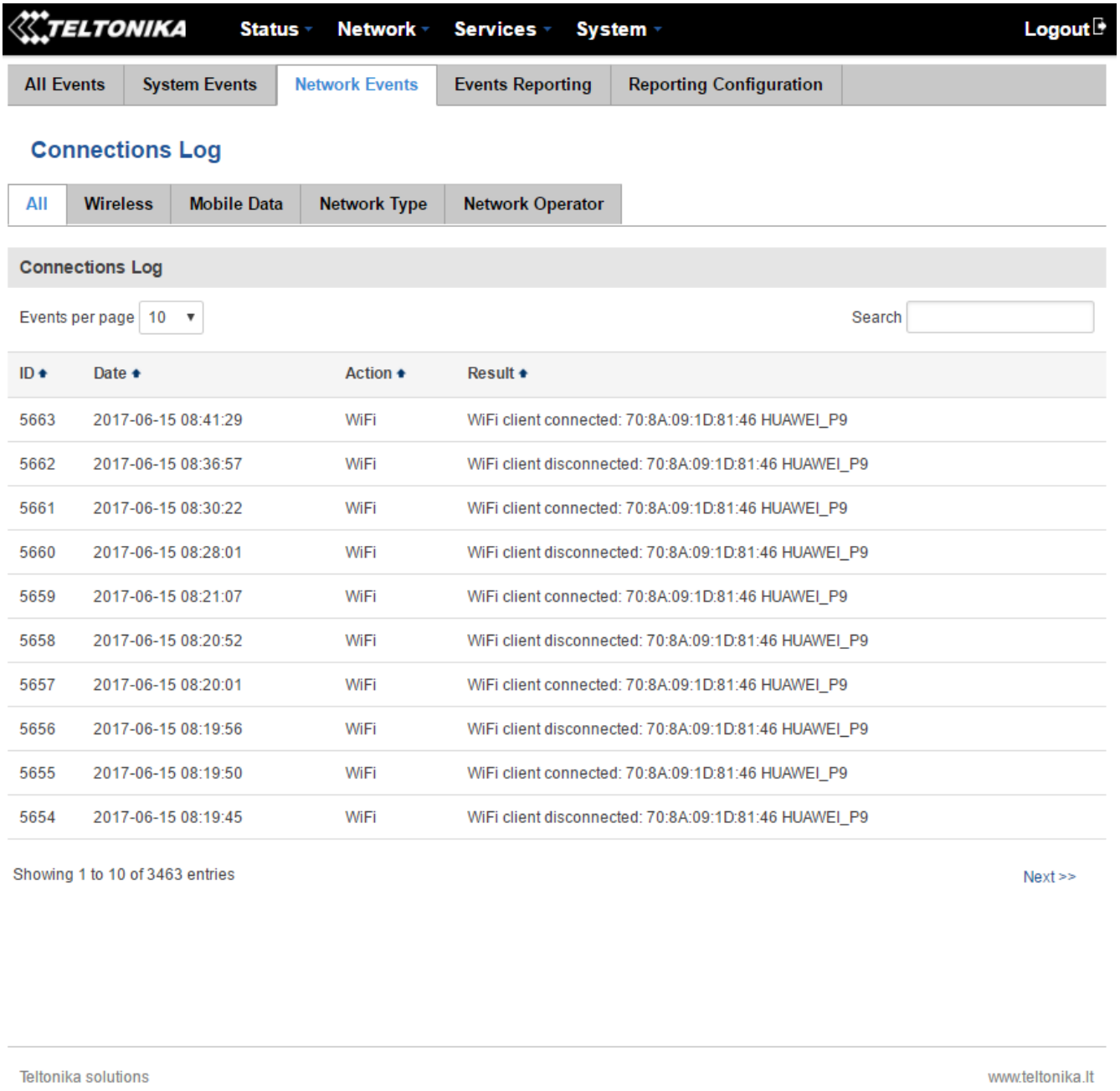
6.9.2 System Events

The System Events window displays all system events, their types and times of occurrence. These events include authentication, reboot requests, incoming and outgoing SMS messages and calls, emails, configuration changes and DHCP events.



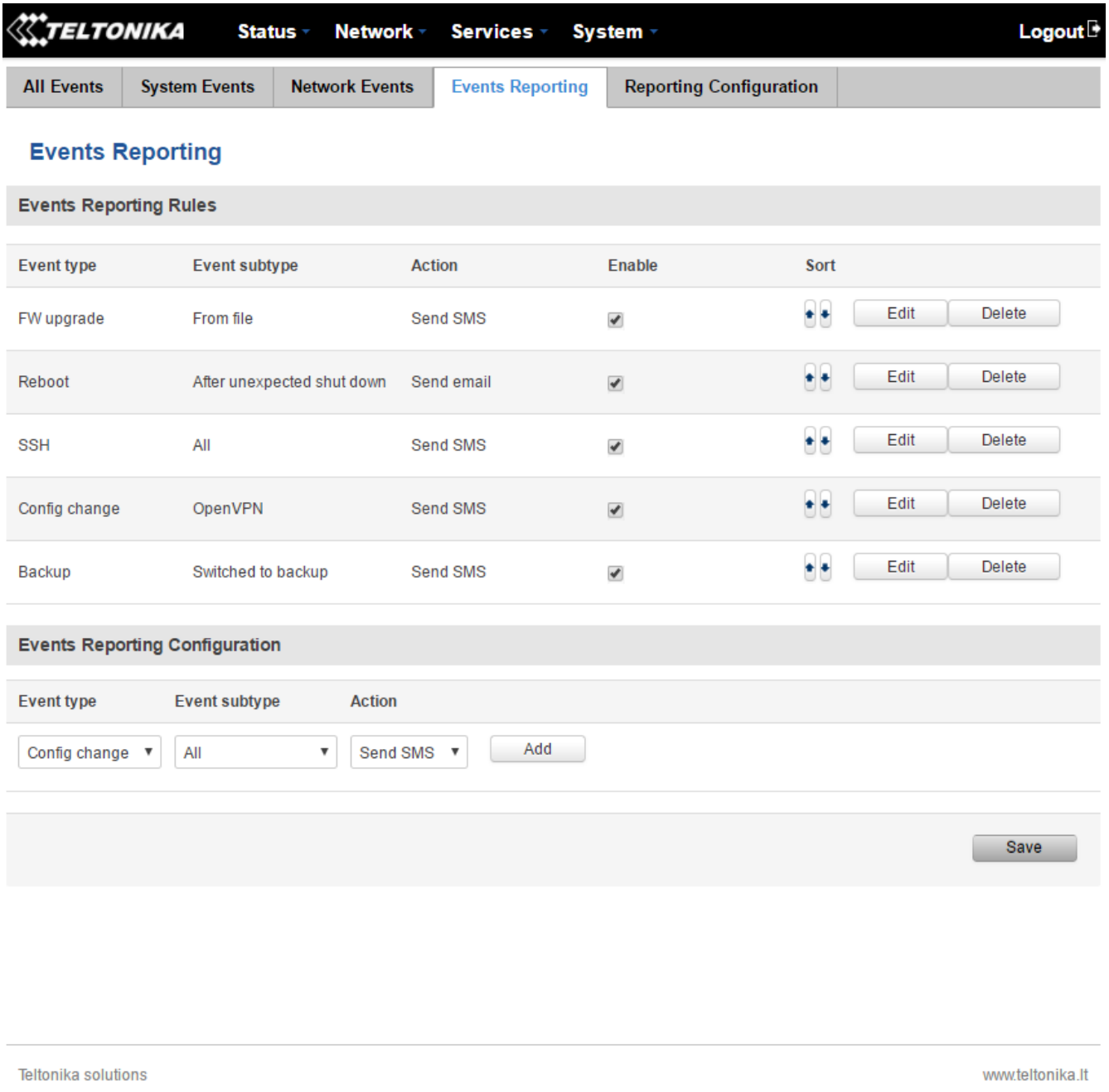
6.9.3 Network Events

The Network Events window displays information about recent network events like new connections, lease status changes, network types or operator changes.



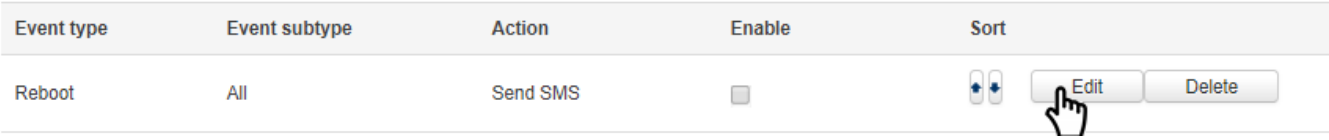
6.9.4 Events Reporting

The Events Reporting page gives you the ability to configure rules that will inform you via SMS or email when certain events occur on your router. These events can be almost anything – configuration changes, new connections, various status updates, SIM switches, etc.

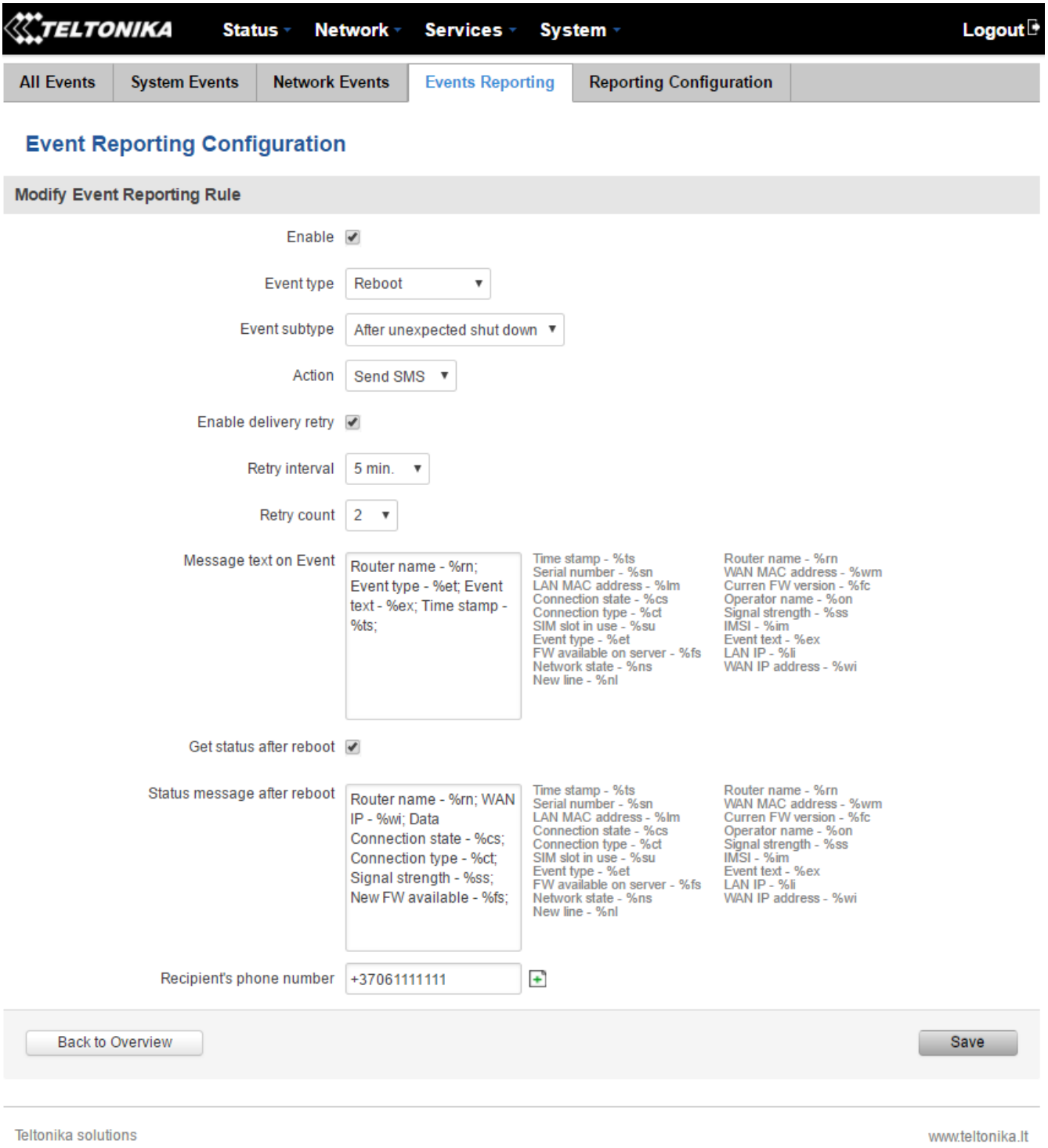


6.9.4.1 Events Reporting Configuration

The Events Reporting Configuration tab is used to customize Events Reporting Rules. Here you can specify any event type and subtype, chose whether you want to be informed by an SMS message or email, modify what kind of information you want receive should an event occur. To open this window, create a rule and press "edit".



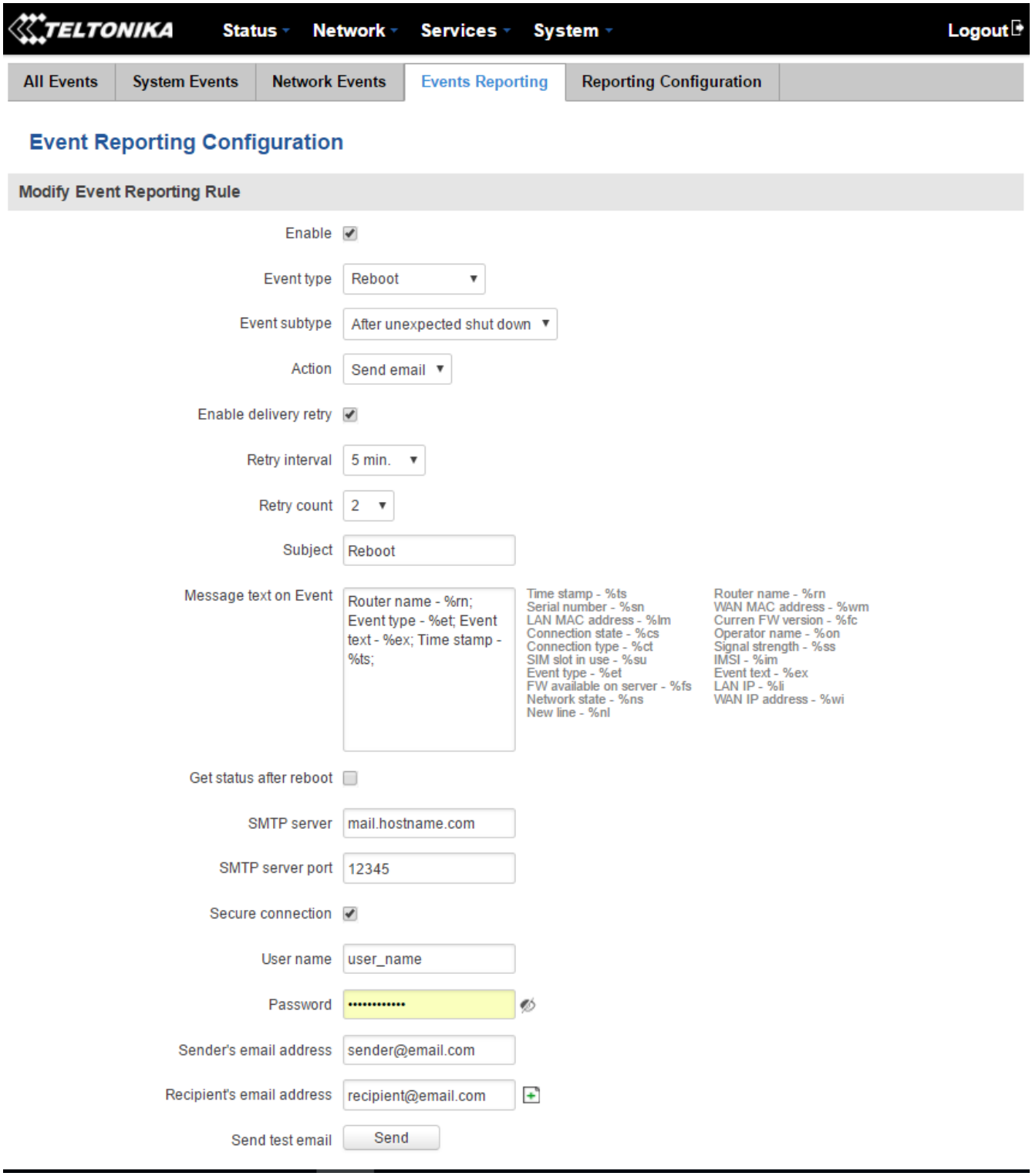
6.9.4.1.1 Send SMS



	Field Name	Sample Value	Explanation
1.	Enable	Enable	Make a rule active/inactive
2.	Event type	Reboot	Select the type of event that you wish to receive information about
3.	Event subtype	After unexpected shut down	Specify the subtype of the event
4.	Action	Send SMS	Action to perform when the specified event occurs
5.	Enable delivery retry	Enable	Enable SMS delivery retry on unsuccessful delivery attempts

6.	Retry interval	5 min.	The amount of time after an unsuccessful attempt before the delivery retry is initiated
7.	Retry count	2	How many attempts of delivery retry will be performed
8.	Message text on Event	Router name - %rn; Event type - %et; Event text - %ex; Time stamp - %ts;	The content of the message
9.	Get status after reboot	Enable	Indicate whether to receive router’s status information after reboot or not
10.	Status message after reboot	Router name - %rn; WAN IP - %wi; Connection state - %cs; Connection type - %ct; Signal strength - %ss; New FW available - %fs;	The content of the status message
11.	Recipient‘s phone number	+37061111111	The phone number that will receive the message after the specified event occurs

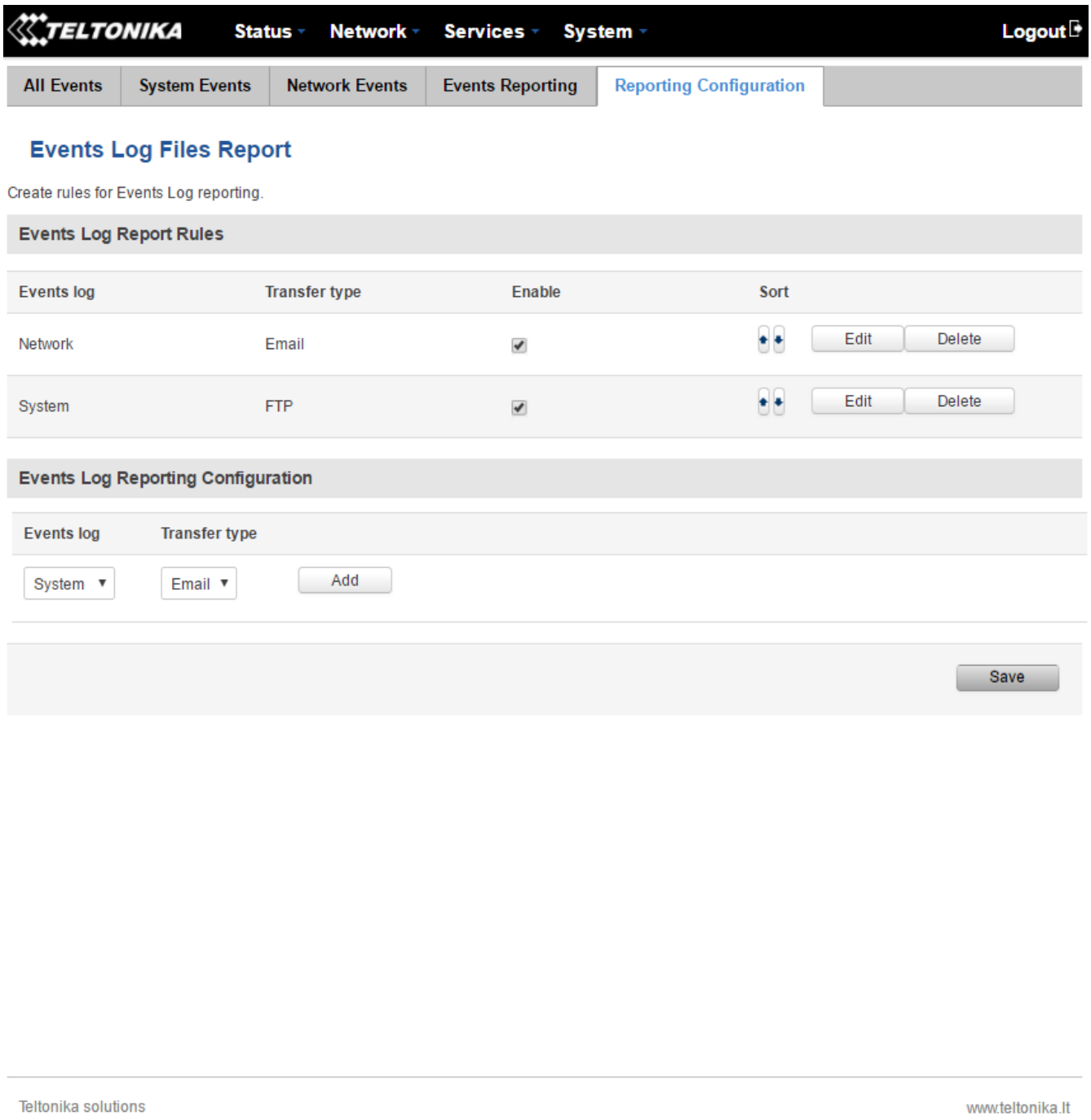
6.9.4.1.2 Send email



	Field Name	Sample Value	Explanation
1.	Enable	Enable	Make the rule active or inactive
2.	Event type	Reboot	Select the type of event that you wish to receive information about
3.	Event subtype	After unexpected shut down	Specify the subtype of the event
4.	Action	Send email	Action to perform when the specified event occurs
5.	Enable delivery retry	Enable	Enable email delivery retry on unsuccessful delivery attempts
6.	Retry interval	5 min.	The amount of time after an unsuccessful attempt before the delivery retry is initiated
7.	Retry count	2	How many attempts of delivery retry will be performed
8.	Subject	Reboot	The subject of the email
9.	Message text on Event	Router name - %rn; Event type - %et; Event text - %ex; Time stamp - %ts;	The content of the message
10.	Get status after reboot	Disable	Indicate whether to receive router’s status information after reboot or not
11.	SMTP server	mail.hostname.com	Sender’s email provider SMTP (Simple Mail Transfer Protocol) server address
12.	SMTP server port	12345	Sender’s email provider SMTP server port number
13.	Secure connection	Enable	Enable or disable secure connection (use only if the server has SSL or TLS)
14.	User name	user_name	Sender’s email account user name
15.	Password	••••••••••••	Sender’s email account password
16.	Sender’s email address	sender@email.com	Sender’s email address
17.	Recipient’s email address	recipient@email.com	Recipient’s email address
18.	Send test email	Send	Sends out a simulated test message according to your given data

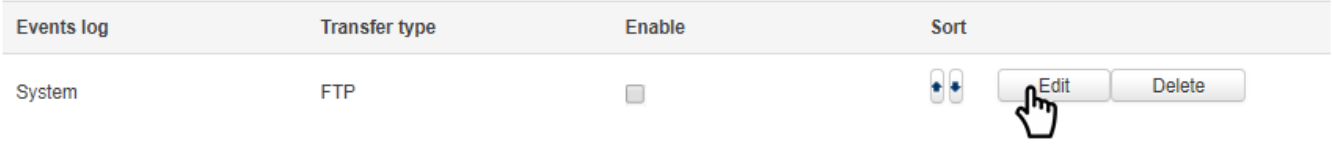
6.9.5 Reporting Configuration

The Reporting Configuration window lets you create rules that transfer logs to email or FTP.

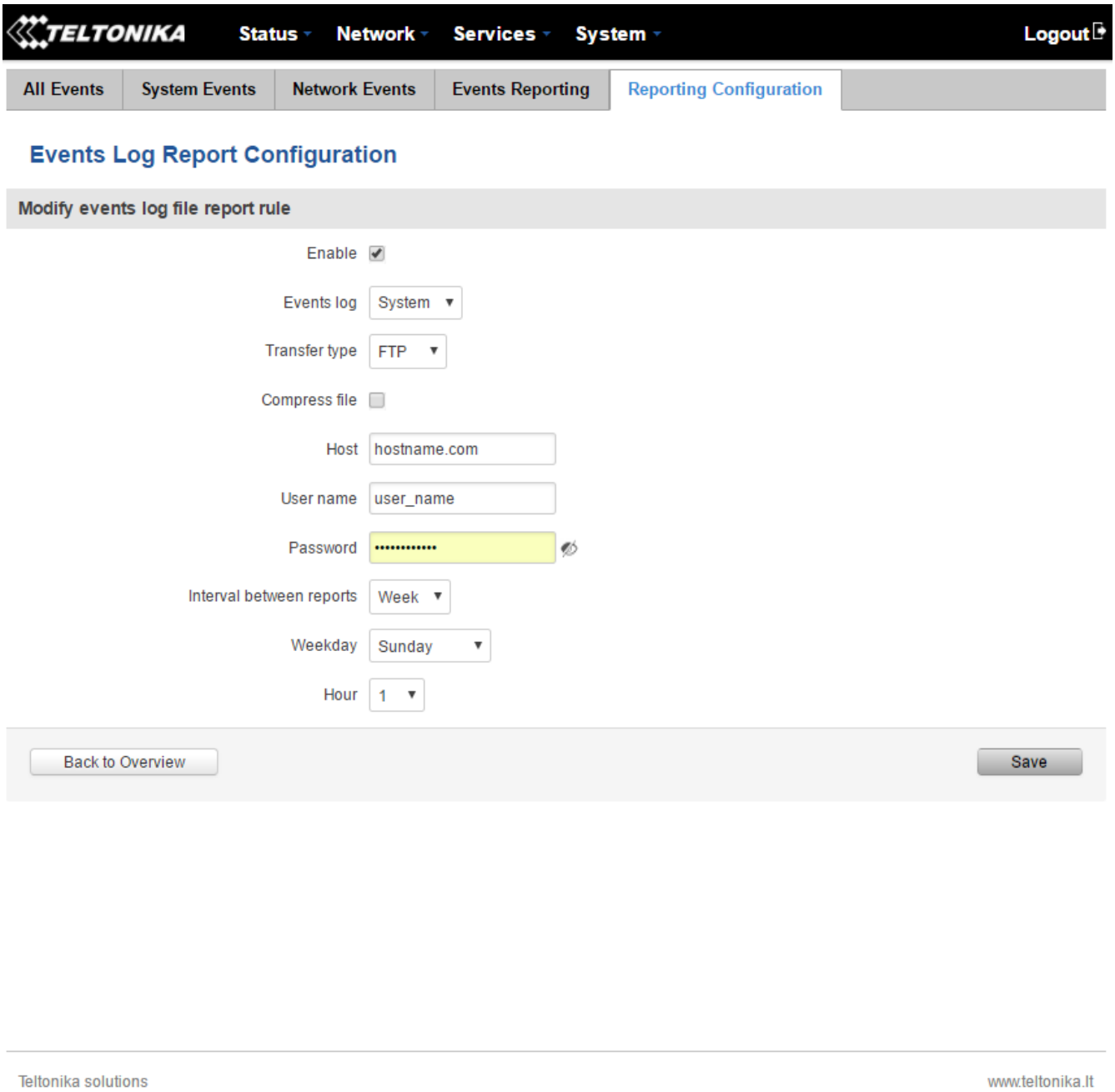


6.9.5.1 Events Log Report Configuration

The Events Log Report Configuration window gives you the ability to change the configuration of periodic events reporting to email or FTP. You can access it by creating a rule and pressing the "edit" button next to it, just like Event Reporting Configuration.

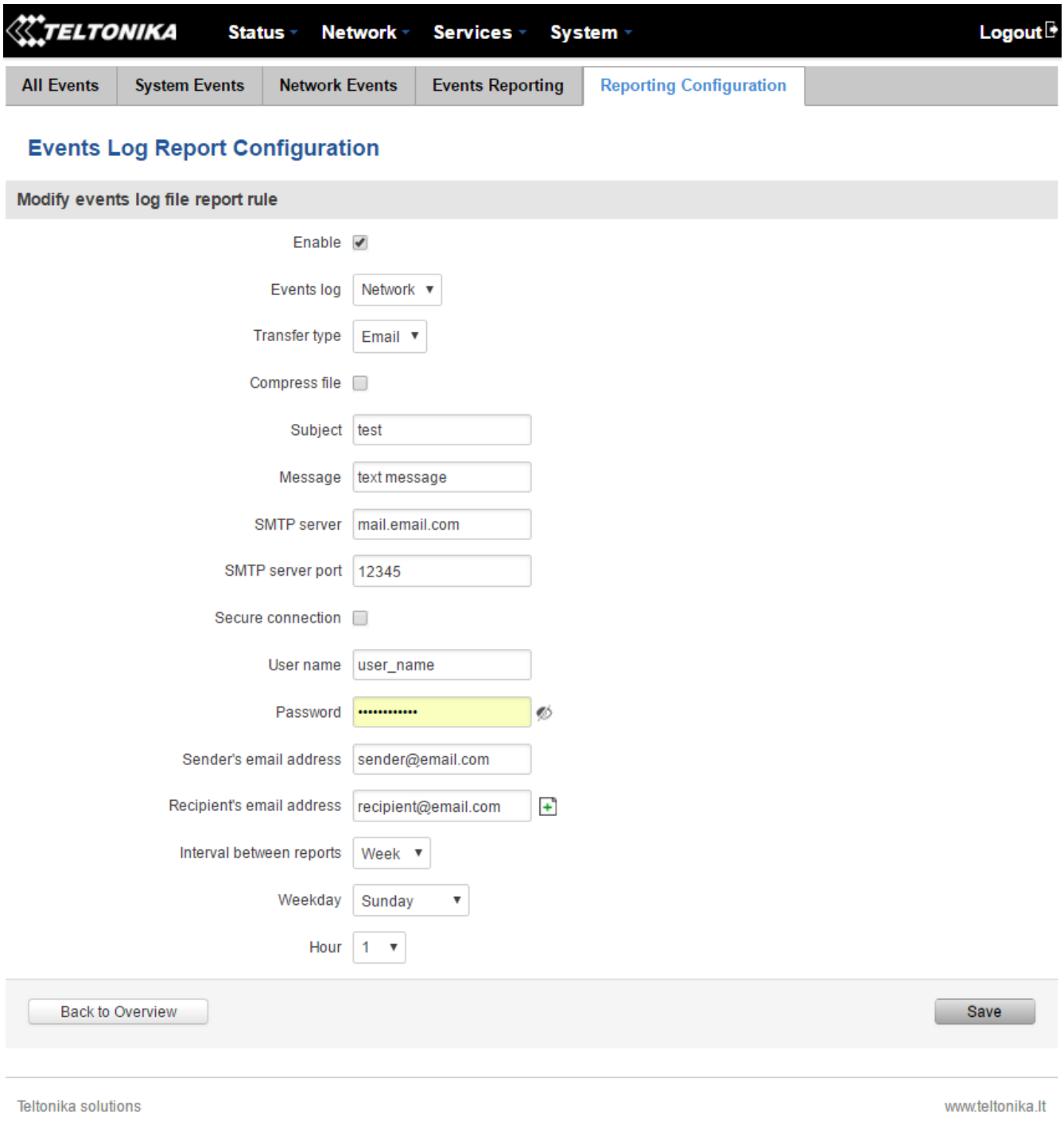


6.9.5.1.1 FTP



	Field Name	Sample Value	Explanation
1.	Enable	Enable	Make the rule active or inactive
2.	Events log	System	Events log to which the rule is applied
3.	Transfer type	FTP	Events log file transfer type: Email or FTP
4.	Compress file	Disable	Enable or disable compress events log file using gzip
5.	Host	hostname.com	FTP (File Transfer Protocol) host name, e.g. ftp.example.com, 192.168.123.123. Allowed characters (a-z-A-Z0-9!@#$%^&*+-/=?_`{|}~.)
6.	User name	user_name	User name for authentication on SMTP (Simple Mail Transfer Protocol) or FTP (File Transfer Protocol) server. Allowed characters (a-z-A-Z0-9!@#$%^&*+-/=?_`{|}~.)
7.	Password	••••••••••••	Password for authentication on SMTP (Simple Mail Transfer Protocol) or FTP (File Transfer Protocol) server. Allowed characters (a-z-A-Z0-9!@#$%^&*+-/=?_`{|}~.)
8.	Interval between reports	Week	The frequency at which Events log reports will be submitted
9.	Weekday	Sunday	Day of the week on which the events log report will be submitted
10.	Hour	1	Hour of the day on which the events log report will be submitted

6.9.5.1.2 Email


TELTONIKA
Status
Network
Services
System
Logout
All Events
System Events
Network Events
Events Reporting
Reporting Configuration
Events Log Report Configuration
Modify events log file report rule
Enable
Events log
Network
Transfer type
Email
Compress file
Subject
test
Message
text message
SMTP server
mail.email.com
SMTP server port
12345
Secure connection
User name
user_name
Password
Sender's email address
sender@email.com
Recipient's email address
recipient@email.com
Interval between reports
Week
Weekday
Sunday
Hour
1
Back to Overview
Save
Teltonika solutions
www.teltonika.lt

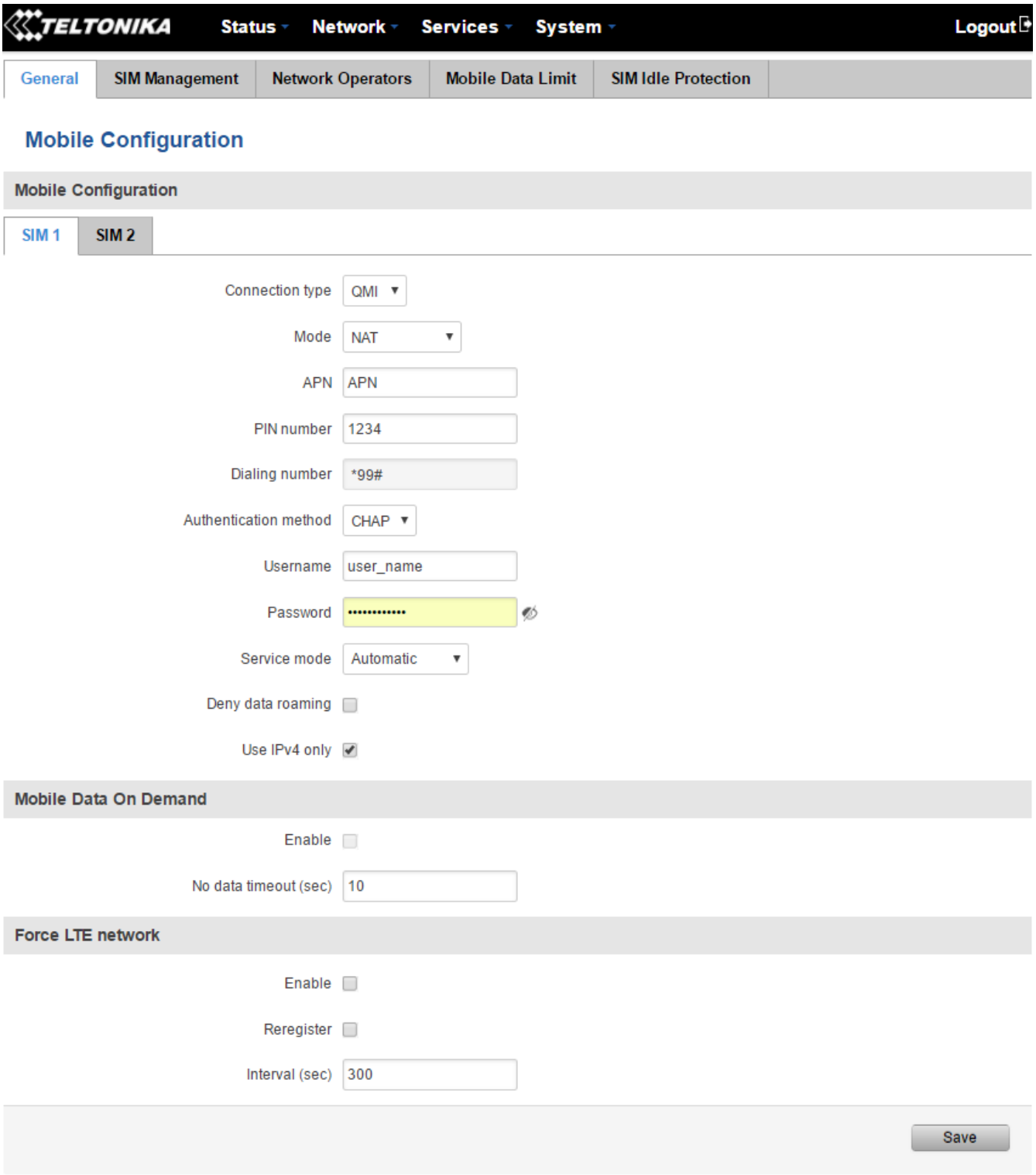
	Field Name	Sample Value	Explanation
1.	Enable	Enable	Make the rule active or inactive
2.	Events log	Network	Events log to which the rule is applied
3.	Transfer type	Email	Events log file transfer type: Email or FTP
4.	Compress file	Disable	Enable or disable compress events log file using gzip
5.	Subject	Test	Subject of the email
6.	Message	text message	The message of the email
7.	SMTP server	mail.email.com	Sender’s email provider SMTP (Simple Mail Transfer Protocol) server address
8.	SMTP server port	12345	Sender’s email provider SMTP server port number
9.	Secure connection	Enable/Disable	Enable or disable secure connection (use only if the server has SSL or TLS)
10.	User name	User	Sender’s email account user name
11.	Password	••••••••••••	Sender’s email account password
12.	Sender‘s email address	sendersemail@example.com	Sender’s email address
13.	Recipient‘s email address	recipientemail@example.com	Recipient’s email address
14.	Interval between reboots	Week	The frequency at which Events log reports will be submitted
15.	Weekday	Sunday	Day of the week on which the events log report will be submitted
16.	Hour	1	Hour of the day on which the events log report will be submitted

7 Network

7.1 Mobile

7.1.1 General

In the Mobile Configuration window you can configure various mobile settings that are used in order to connect to your local 2G/3G/LTE network.

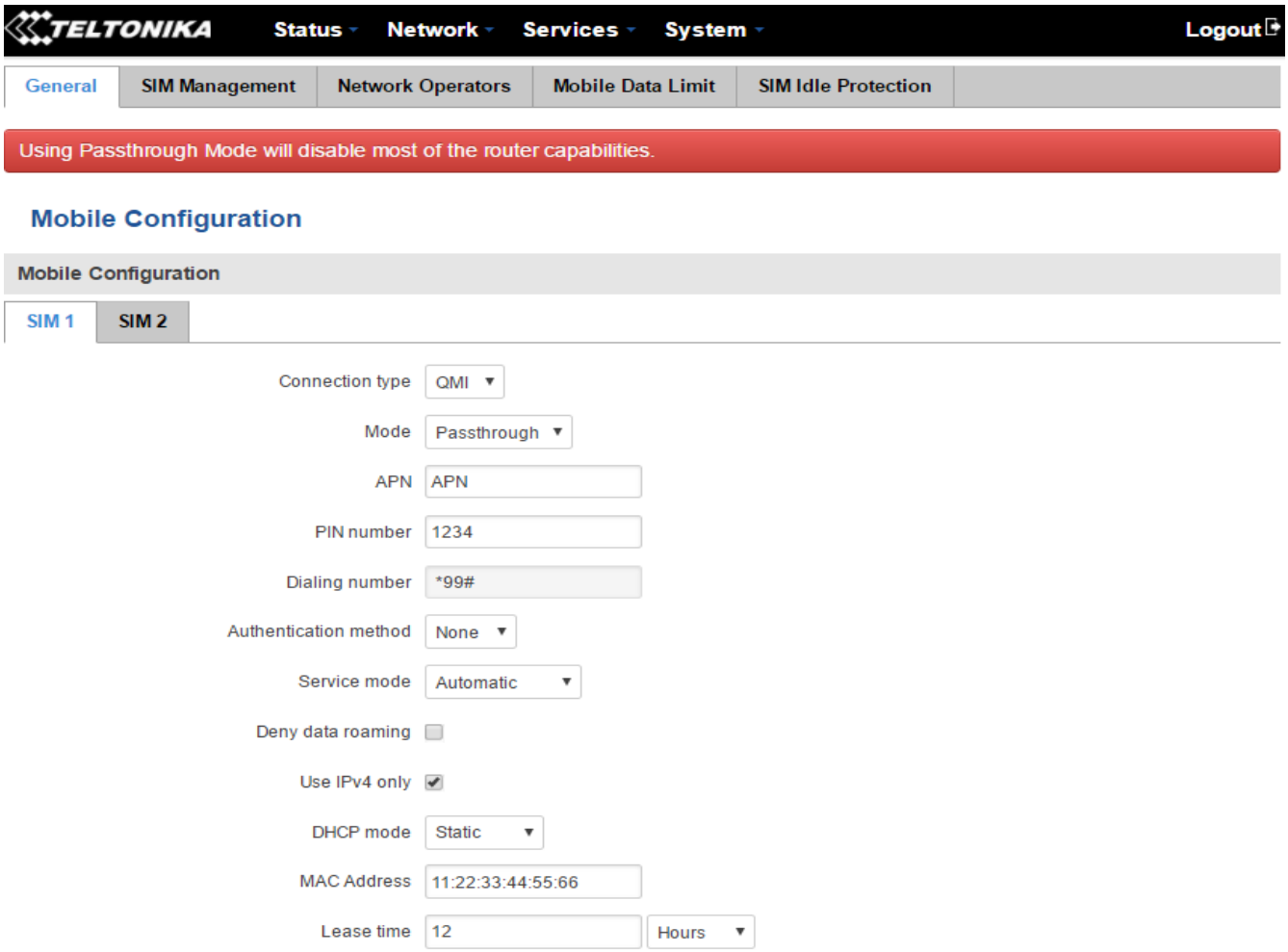


	Field Name	Possible values	Explanation
1.	Connection type	PPP / QMI	Defines how the router's modem will connect to the internet. **PPP** mode uses a dialling number to establish a data connection. **QMI** mode (default) does not use dialling or the PPP protocol to establish a data connection and it is usually faster than PPP mode
2.	Mode	NAT / Passthrough / Bridge	**NAT** mode enables network address translation on the router. **Bridge** mode bridges the LTE data connection with LAN. In this mode the router does not have an internet connection as the ISP provides an IP address directly to the end device. Using Bridge mode will disable most of the router's capabilities and you will only be able to access your router's settings with a static IP address. **Passthrough** mode works in a similar fashion to Bridge mode, except in passthrough mode the router does have an internet connection
3.	APN	"APN"	An **Access Point Name (APN)** is a gateway between a GSM, GPRS, 3G or 4G mobile network and another computer network
4.	PIN number*	Any number that falls between 0000 and 9999	A **personal identification number** is a numeric password used to authenticate a user to a system
5.	Dialing number	*99#	A **Dialling number** is used to establish a mobile PPP connection
6.	Authentication method	CHAP, PAP or none	The **Authentication method** that your GSM carrier uses to authenticate new connections on its network
7.	Username	user_name	The username used to connect to your carrier's network. This field becomes available when you select an authentication method (i.e., the selected authentication method is not "None")
8.	Password	••••••••••••	The password used to connect to your carrier's network
9.	Service mode	2G only, 3G only, 4G (LTE) only or Automatic.	Your service mode preference. If your local mobile network supports 2G, 3G and 4G (LTE) you can specify to which type of network you wish to connect, e.g. if you choose 2G, the router will connect to a 2G network, so long as it is available, otherwise it will connect to a network that provides better connectivity. If you select Automatic, then the router will connect to the network that provides the best connectivity
10.	Deny data roaming	Enable / Disable	When enabled this function prevents the device from establishing mobile data connection while not in your home network
11.	Use IPv4 only	Enable / Disable	When enabled this function makes the device use only IPv4 settings when connecting to an operator
12.	Mobile Data On Demand	Enable / Disable	When Enabled **The Mobile Data On Demand** function keeps the mobile data connection **on** only when it is in use
		No data timeout (sec) – 10 - 99999999	The mobile data connection will be terminated if no data is transferred during the timeout period specified in this field
13.	Force LTE network	Enable/Disable	When enabled this function makes the router connect to an LTE network after every specified amount of seconds
		Enable/Disable	When enabled the modem will reregister before trying to connect to an LTE network
		180 – 3600	Time in seconds between attempts to connect to an LTE network

***Warning: If you enter an invalid PIN number (i.e. if the entered PIN does not match the one that is used in 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.**

7.1.1.1 Passthrough Mode

Passthrough mode is used to redirect all traffic to another device. In the process the router itself becomes "transparent" as all traffic is redirected to another device which will also have the router's public IP address assigned to it.

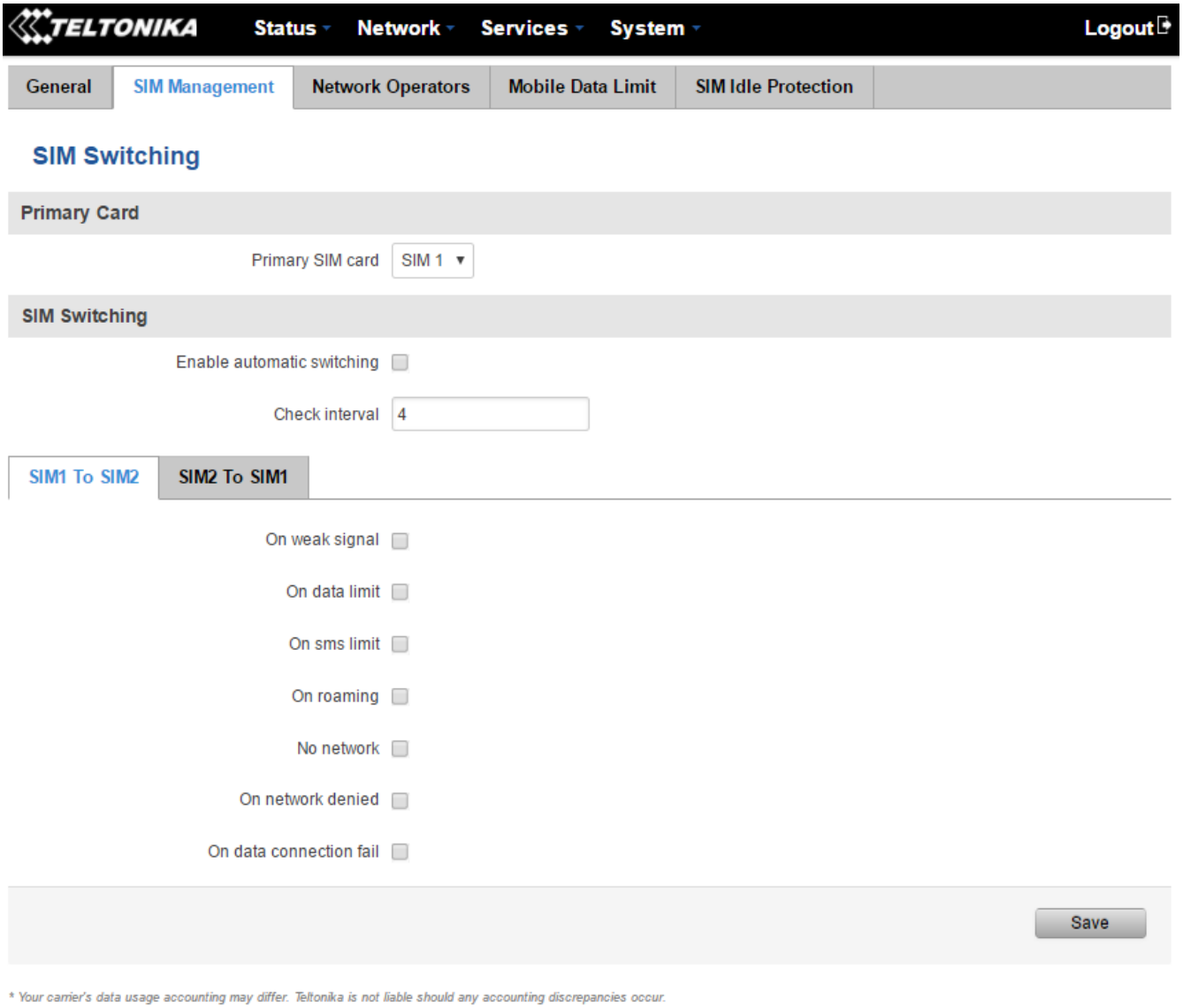


Field name	Possible values	Explanation
DHCP mode*	Static	The **Static** mode requires that you enter your computer's **MAC address** (xx:xx:xx:xx:xx:xx) and select a lease time (expiration time for the leased address.) The device will get an IP address from your GSM operator. Other devices that are connected to the router will get IP addresses from the router's DHCP server, but they will not have internet access
	Dynamic	In **Dynamic** mode the GSM operator will connect to the router first and give out an IP address to your computer. When using Passthrough in Dynamic mode, the router's LAN DHCP server will be disabled, but it will enabled again automatically when you switch to a different mode
	No DHCP	In **No DHCP** mode the IP address, subnet mask, default gateway and DNS from the GSM operator will have to be entered on your computer manually. When using Passthrough in No DHCP mode, the router's LAN DHCP server will be disabled, but it will become enabled automatically when you switch to a different mode

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

7.1.2 SIM Management

The SIM Management window is used for setting your primary SIM card and setting up scenarios after which the router will perform a SIM switch.

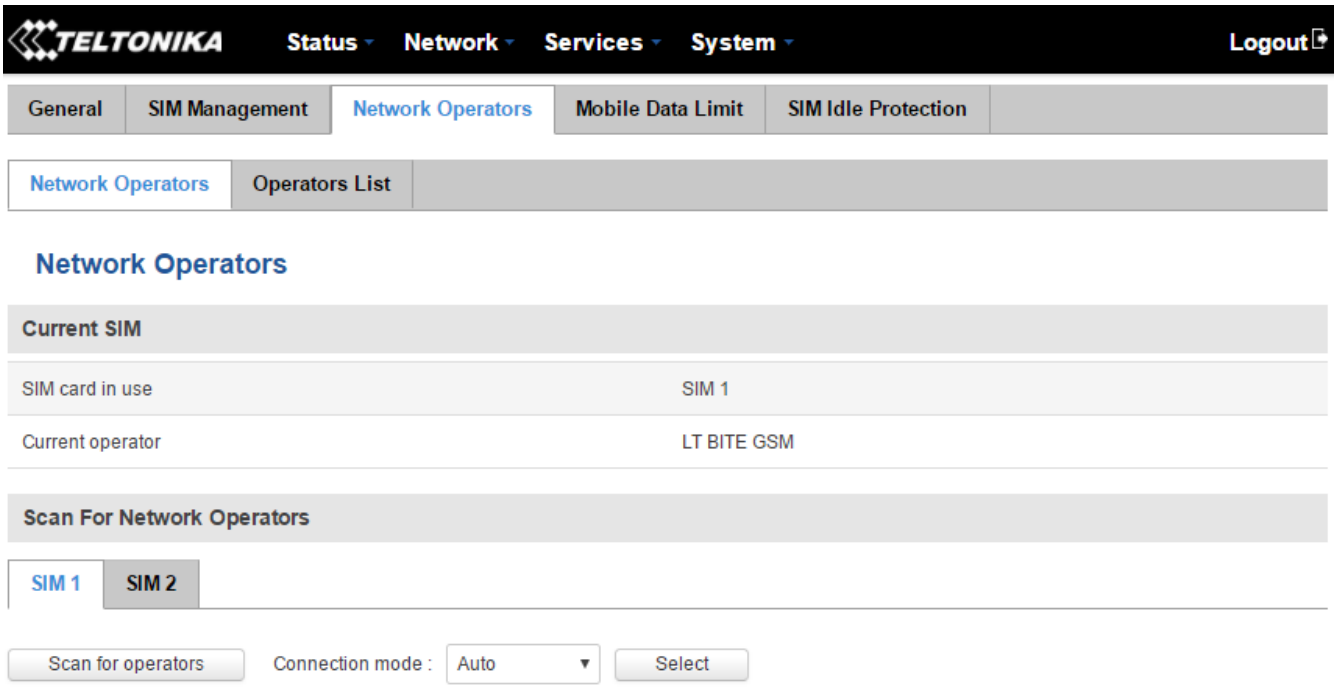


	Field name	Possible values	Explanation
1.	Primary SIM card	SIM 1 / SIM 2	Which SIM card will be used by the system as the primary SIM card
2.	Enable automatic switching	Enable/Disable	Automatically switch between primary and secondary SIM cards based on the various rules and criterions defined below
3.	Check interval	1-3600	Check interval in seconds
4.	On weak signal	Enable/Disable	Performs a SIM card switch when signal strength drops below the specified threshold
5.	On data limit*	Enable/Disable	Performs a SIM card switch when mobile data limit is reached
6.	On SMS limit*	Enable/Disable	Performs a SIM card switch when the SMS limit is reached
7.	On roaming	Enable/Disable	Performs a SIM card switch when roaming is detected
8.	No network	Enable/Disable	Performs a SIM card switch when no operator is detected
9.	On network denied	Enable/Disable	Performs a SIM card switch when access to a network is denied
10.	On data connection fail	Enable/Disable	Performs a SIM card switch when data connection fails

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

7.1.3 Network Operators

The Network Operators window provides you with the ability to scan, select and enter manual Network Operator codes. This function is a great utility when the router is in Roaming conditions. Operator selection is only available for the primary SIM card. In order to specify an operator for the other SIM card it must first be selected as the primary SIM in the "SIM Management" section.

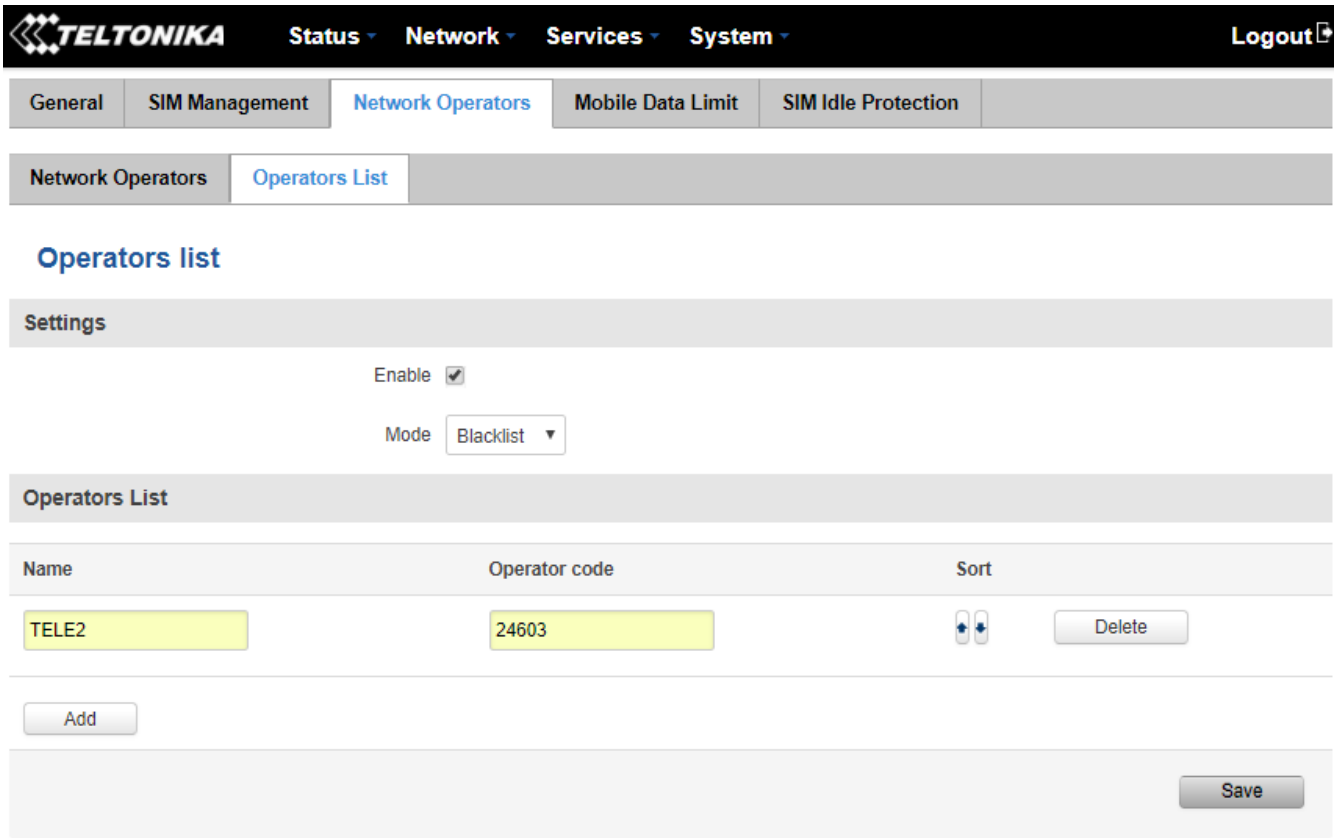


	Field Name	Sample Value	Explanation
1.	SIM card in use	SIM 1	Shows the SIM card in use
2.	Current operator	LT BITE GSM	GSM operator's name
3.	Scan for operators*	-	Initiates a scan for available operators in your area
4.	Connection mode	Auto	Lets you chose whether you want to select your operator manually or automatically

***While scanning for operators, you will lose your current mobile connection!**

7.1.3.1 Operators List

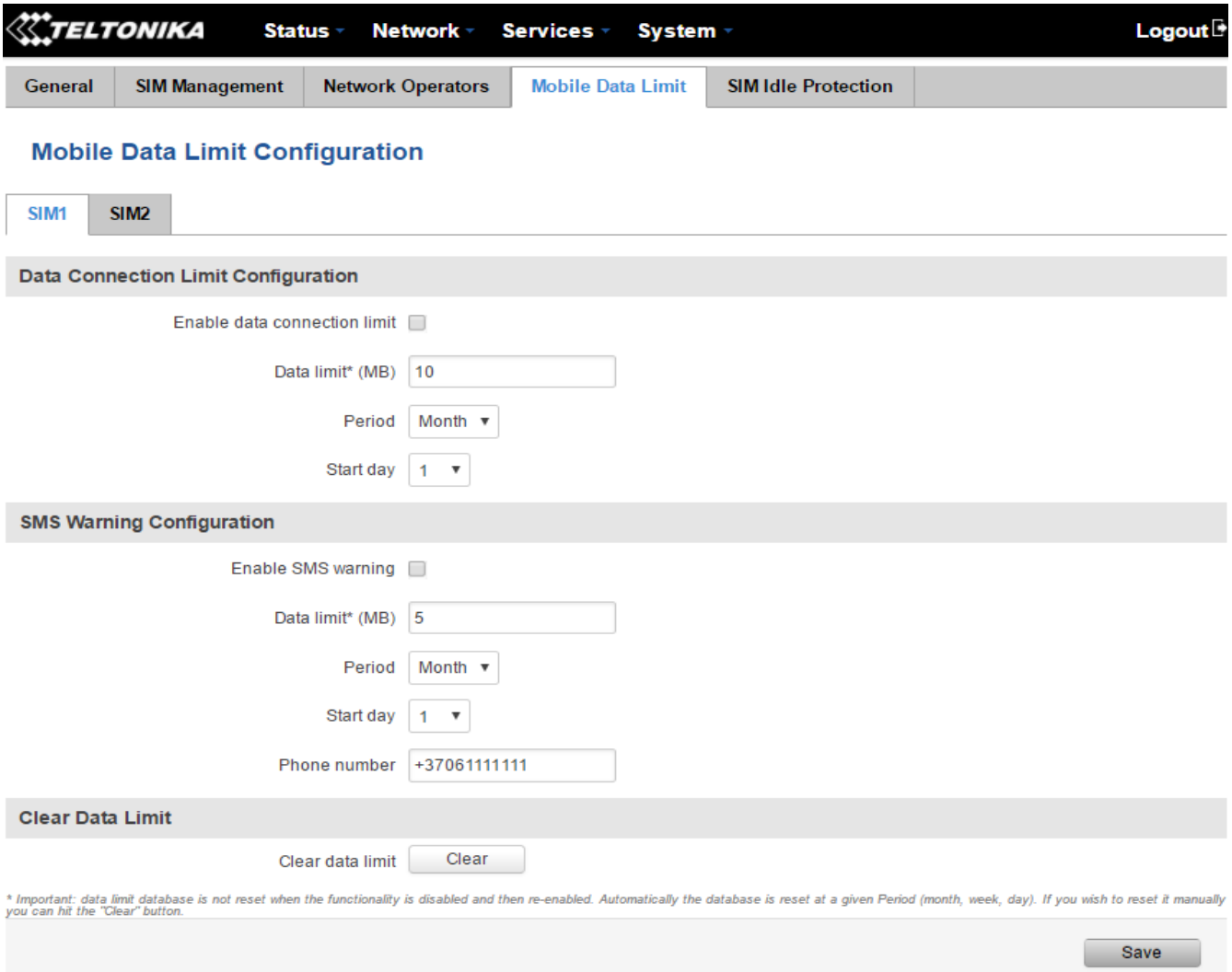
The Operators List window provides you with the opportunity to create either a white list or a black list to help you differentiate preferred operators from unwanted operators. This is especially useful when travelling to different countries because it gives you protection from unwanted data charges by denying the SIM card access to unknown or unwanted operators.



	Field name	Possible values	Explanation
1.	Enable	Enable/Disable	Enable/disable operator blocking
2.	Mode	Whitelist/Blacklist	**Whitelist** - allows every operator on the list, blocks every other operator. **Blacklist** - blocks every operator on the list, allows every other operator
3.	Name	TELE2	Operator's name
4.	Operator code	24603	Operator's code

7.1.4 Mobile Data Limit

The Mobile Data Limit window provides you with the ability to set data limits for your SIM cards in order to protect yourself from unwanted data charges.



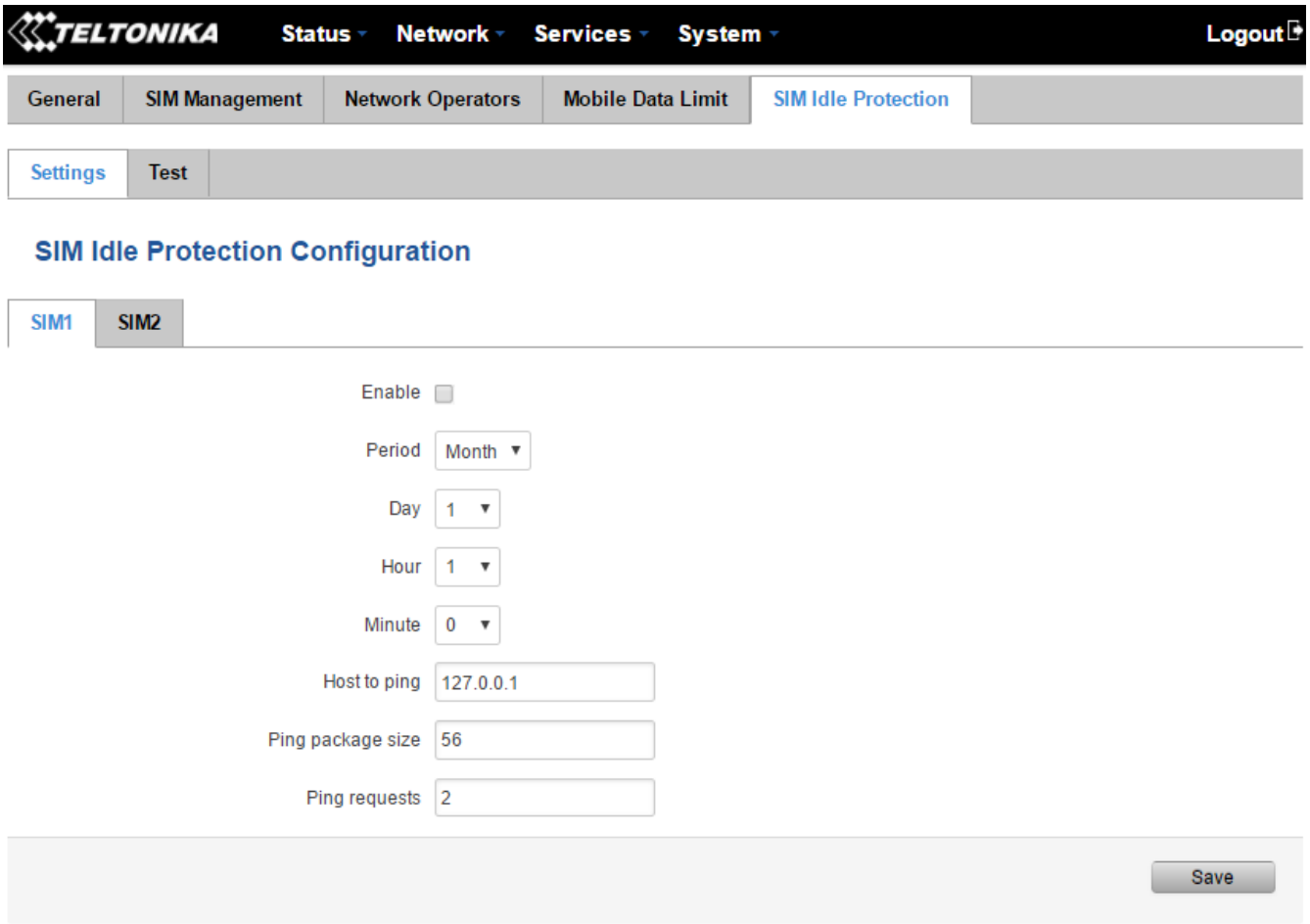
Data Connection Limit Configuration			
	Field Name	**Sample value**	**Explanation**
1.	Enable data connection limit	Enable/Disable	Disables the mobile data connection when the limit for the current period is reached
2.	Data limit* (MB)	10	Data limit that triggers the mobile data disconnection
3.	Period	Month	Period for which the mobile data limiting will be applied
4.	Start day/ Start hour	1	A starting time for the mobile data limiting period
SMS Warning Configuration			
1.	Enable SMS warning	Enable/Disable	Enables the sending of a warning SMS message before or when the mobile data limit for the current period is reached
2.	Data limit* (MB)	5	Data limit which triggers the warning message
3.	Period	Month	Period for which the 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 the warning SMS message to
Clear Data Limit			
1.	Clear data limit	-	Clears all sent and received data for the selected period

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

7.1.5 SIM Idle Protection

Some operators block user SIM cards after a period of inactivity. The SIM Idle Protection window provides you with the possibility to configure the router to periodically switch to the secondary SIM card and establish a data connection with a mobile network in order to prevent the SIM card blocking.

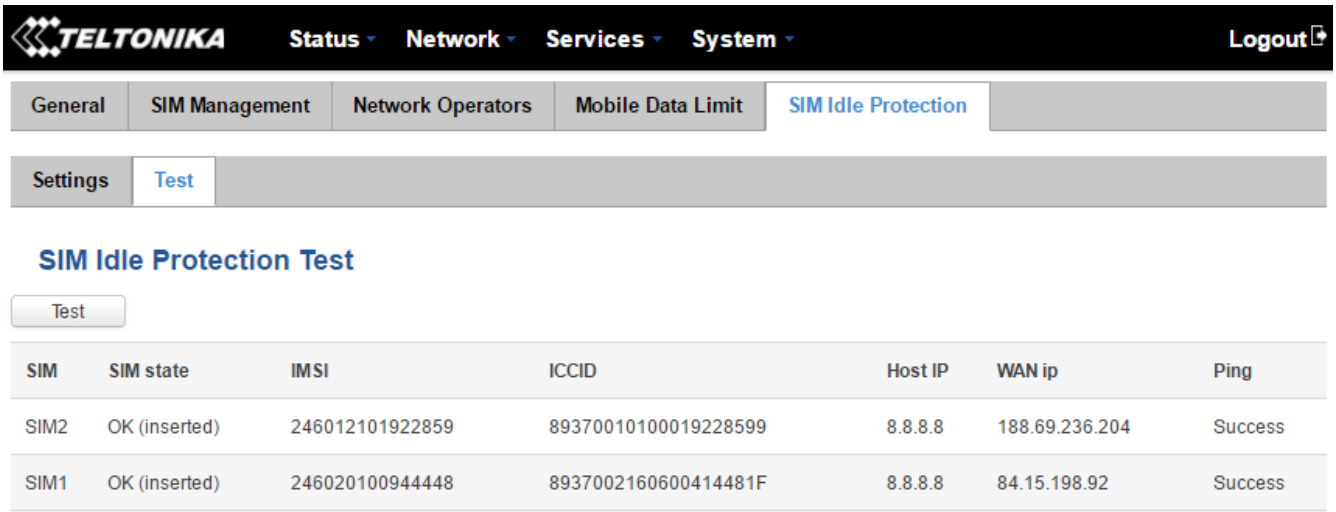
7.1.5.1 Settings



	Field Name	Possible values	Explanation
1.	Enable	Enable/Disable	Enables SIM idle protection
2.	Period	Month / Week	The frequency at which the SIM switch will be initiated
3.	Day	1-31 / Monday - Sunday	Specifies the day of SIM idle protection activation. 1-31 if the period is a month; Monday – Sunday if the period is a week
4.	Hour	1 - 24	Specifies the hour of SIM idle protection activation
5.	Minute	0 - 60	Specifies the minute of SIM idle protection activation
6.	Host to ping	127.0.0.1	Specifies the IP address or domain name to send data packages to
7.	Ping package size	56	Specifies the ping package size in bytes
8.	Ping requests	2	Number of ping requests that will be sent

7.1.5.2 Test

The SIM Idle Protection Test window lets you test the functionality of SIM Idle Protection with the parameters entered at the settings tab. Once you press the 'Test'* button it will simulate a SIM Protection scenario for both of the SIM cards. Once you initiate the test do not commit any actions until the test is finished, as doing otherwise will result in errors that can only be resolved by reseting your device..



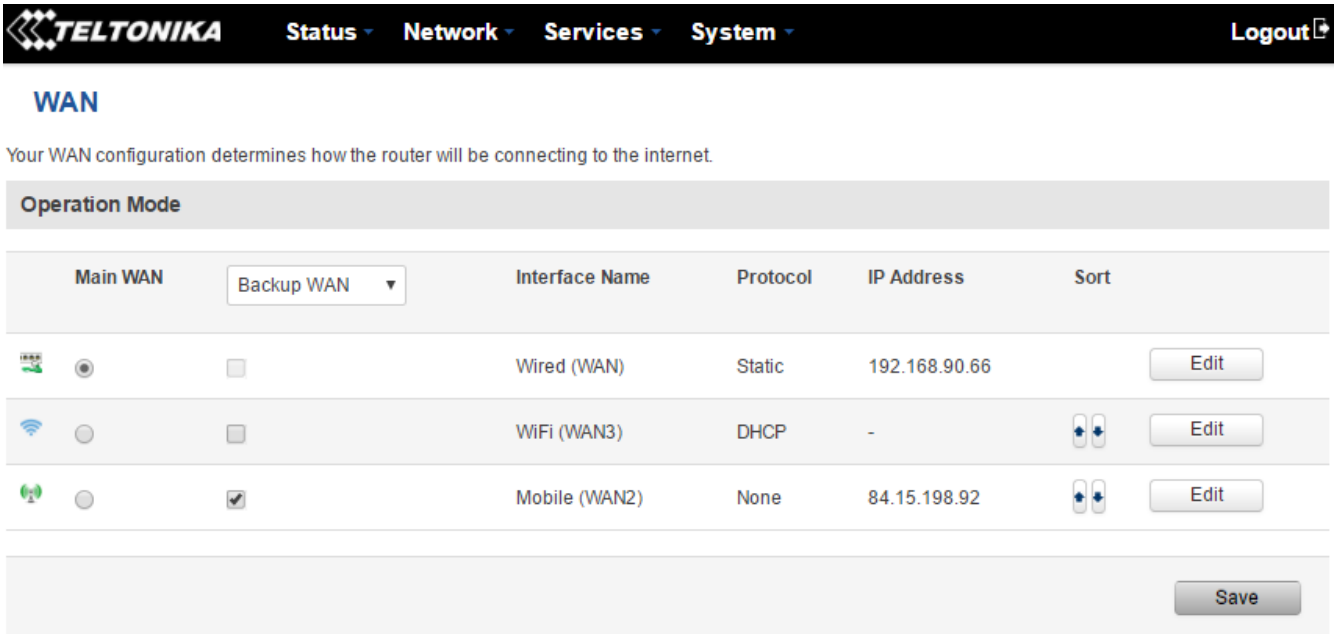
	Field Name	Sample value	Explanation
1.	SIM	SIM1	SIM card number
2.	SIM state	OK (inserted)	Status of the SIM card
3.	IMSI	246020100944448	International Mobile Subscriber Identity used to identify the user in a cellular network
4.	ICCID	8937002160600414481	Integrated circuit card identifier used to identify the SIM card internationally
5.	Host IP	8.8.8.8	IP address of the host
6.	WAN IP	84.15.198.92	SIM card's public IP address
7.	Ping	Success	Status of the ping attempt

***During test phase do not commit any action, wait for the test to finish**

7.2 WAN

7.2.1 Operation Mode

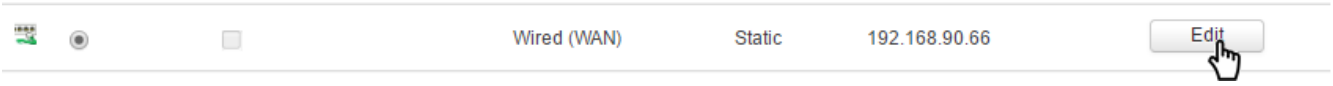
The WAN window lets you determine how the router will be connecting to the internet. You can chose between three types of WAN – Mobile, Wired and Wi-Fi.



	Field Name	Possible values	Explanation
1.	Main WAN	Wired/Mobile/Wi-Fi	Allows you to select the main WAN
2.	Backup WAN / Load Balancing	Enable/Disable	Allows you to select one or two interface to act as your backup WAN
3.	Interface Name	WAN/WAN2/WAN3	Names of the WAN interfaces
4.	Protocol	Static/DHCP/PPPoE	The protocol used by a WAN interface
5.	IP Address	192.168.90.66	WAN IP address
6.	Sort	-	Allows you to sort table rows and change interface priority (i.e., the highest interface has the highest priority)

7.2.2 Common Configuration

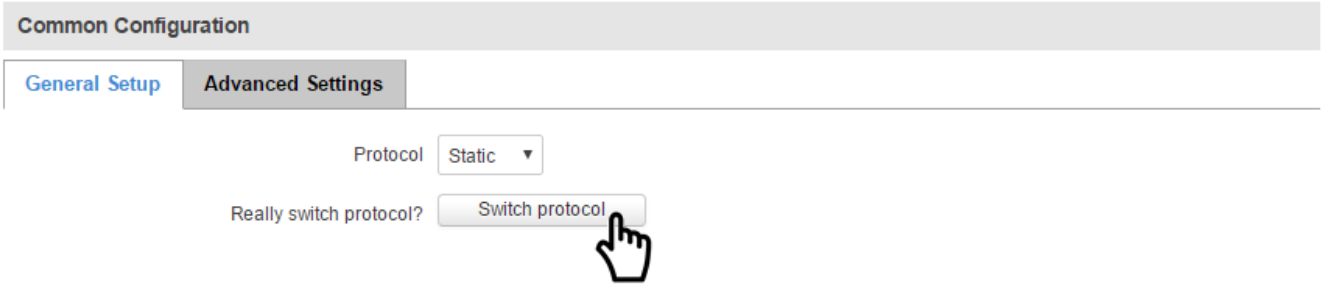
You can further configure each of your WAN interfaces by clicking the 'edit' button found at the far right of the WAN table next to each interface:



It will open the Common Configuration window where you can select the protocol to be used with your by your WAN interface, configure your backup WAN settings, set up IP aliases, custom DNS servers and more.

7.2.2.1 General Setup

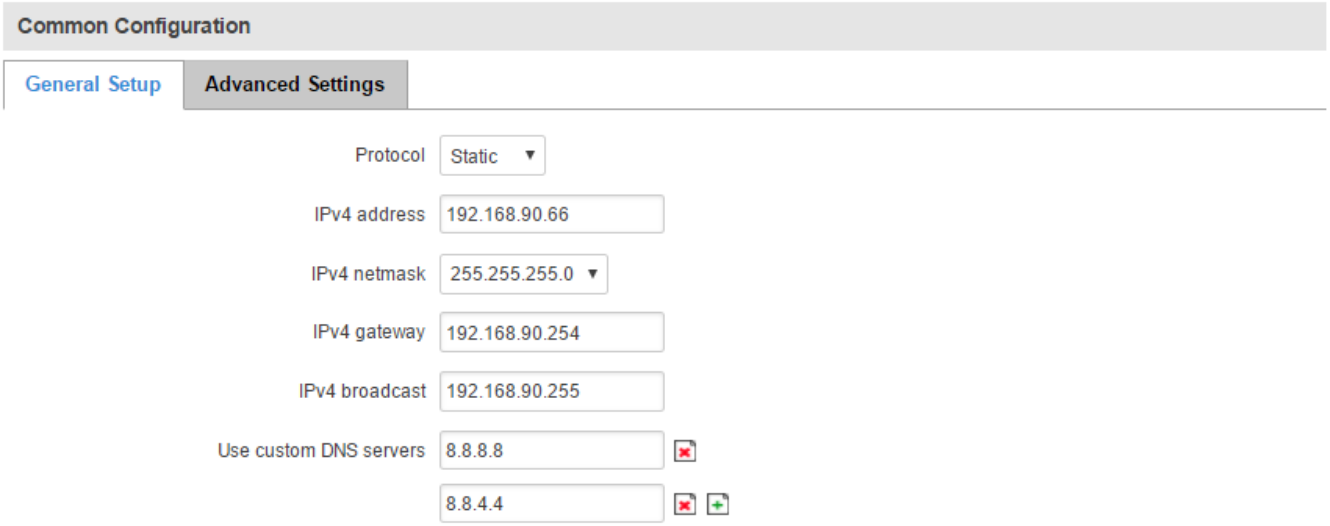
You can switch between Static, DHCP or PPPoE protocols by selecting the one that you want to use and then pressing the 'Switch Protocol'* button.



***The "Switch protocol" button does not apply any changes. In order for the changes to take effect, you must click the "Save" button found at the bottom left corner of the window after you are done making changes.**

7.2.2.1.1 Static:

The Static protocol is used when the source of your internet doesn't have a DHCP server enabled. Therefore, in order to connect to the internet, you have to make configurations in accordance to the source (much like in the **Logging In** section of this user's manual.)



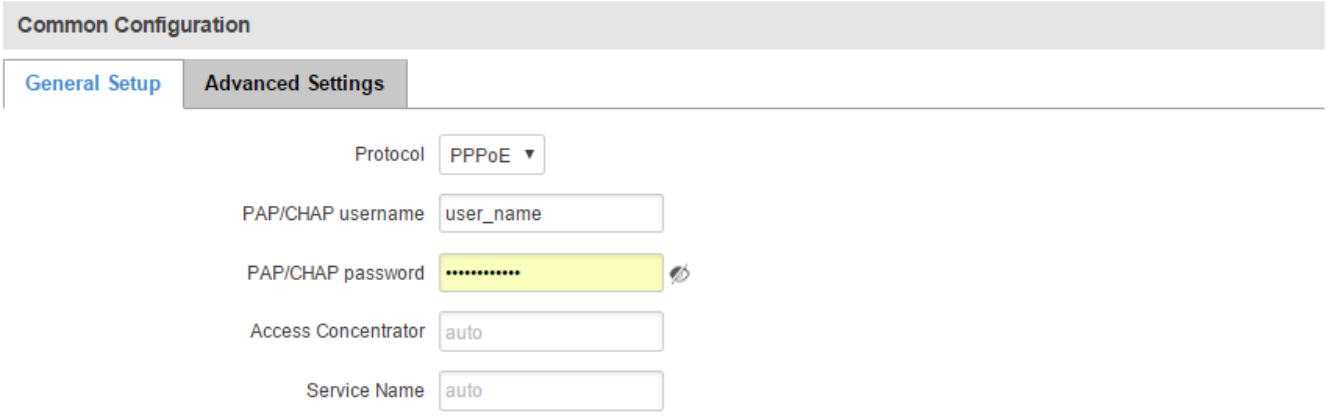
	Filed name	Sample Value	Explanation
1.	Protocol	Static	The protocol used by the WAN interface
2.	IPv4 address	192.168.90.66	Your router's address on the WAN network
3.	IPv4 netmask	255.255.255.0	A mask used to define how "large" the WAN network is
4.	IPv4 gateway	192.168.90.254	The address where the router will send all the outgoing traffic
5.	IPv4 broadcast	192.168.90.255	Broadcast address (auto generated if not set). It is best to leave this blank unless you know what you are doing
6.	Use custom DNS servers	8.8.8.8 8.8.4.4	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 the host name resolution. You can enter multiple DNS servers to provide redundancy in case one of the servers fails

7.2.2.1.2 DHCP:

The DHCP protocol should be used when the source of your internet has a DHCP server enabled. If that is the case, when you select the DHCP protocol you can use it as is, because most networks will not require any additional advanced configuration.

7.2.2.1.3 PPPoE

The PPPoE protocol is mainly used if you have a DSL internet provider.



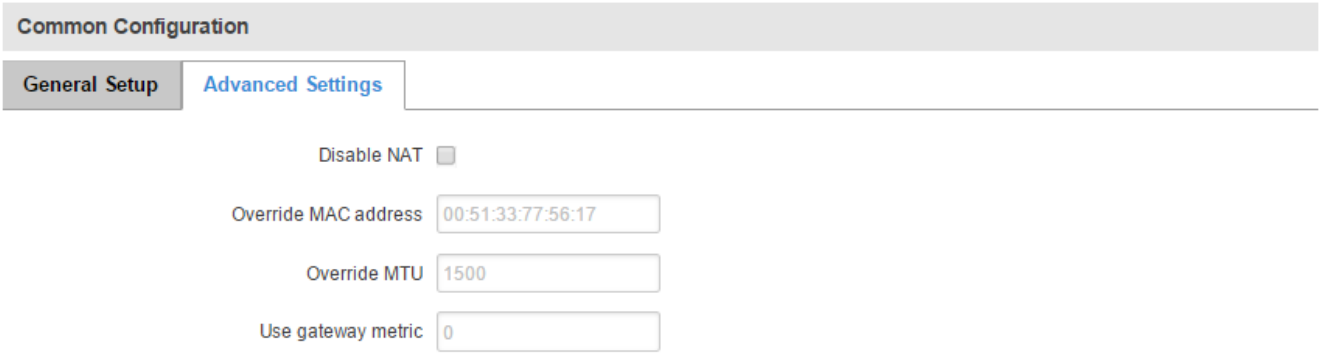
	Filed name	Sample Value	Explanation
1.	Protocol	PPPoE	The protocol used by the WAN interface
2.	PAP/CHAP username	user_name	The username that you would use to connect to your carrier's network
3.	PAP/CHAP password	••••••••••••	The password that you would use to connect to your carrier's network
4.	Access Concentrator	auto	The name of the access concentrator. Leave empty to auto detect
5.	Service Name	auto	The name of the service. Leave empty to auto detect

7.2.2.2 Advanced

The Advanced Setting tab offers you the ability to configure more advanced settings for each of the protocols. If you are unsure of how to alter these settings, it is highly recommended to leave them unchanged or consult a trained professional.

7.2.2.2.1 Static

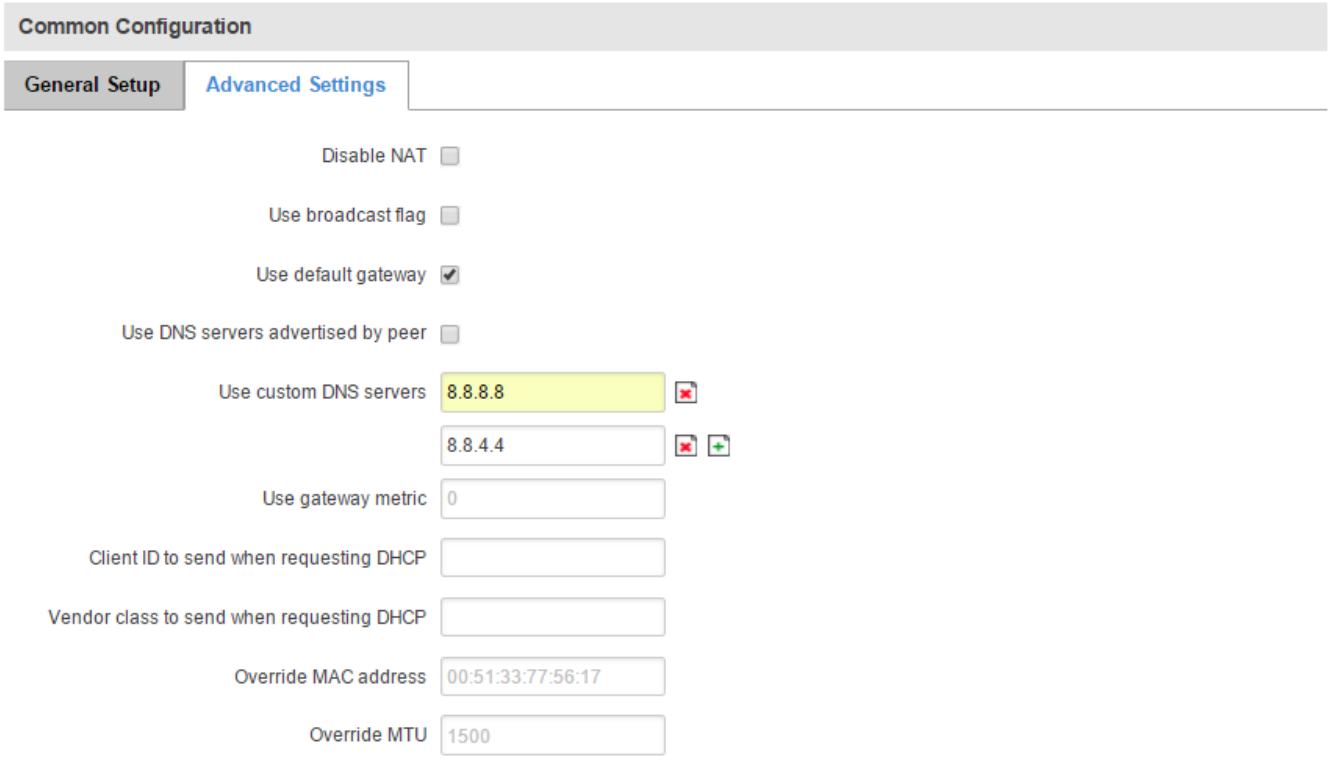
The Advanced Settings tab will change in accordance to which network protocol is selected. For the Static protocol you can turn NAT on or off, override the router's MAC address, MTU and define the gateway metric. You will find additional information on how to define these settings bellow.



	Field name	Sample value	Explanation
1.	Disable NAT	On/Off	Toggle **Network Address Translation (NAT)** on or off for the selected network interface
2	Override MAC address	00:51:33:77:56:17	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 but not with your router). In this field you can enter your computer's MAC address and fool the gateway in to thinking that it is communicating with your computer
3.	Override MTU	1500	**Maximum Transmission Unit (MTU)** – specifies the largest possible size of a data packet
4.	Use gateway metric	0	The WAN configuration by default generates a routing table entry. In this field you can alter the metric of that entry

7.2.2.2.2 DHCP

For the DHCP protocol you can turn NAT on or off, specify custom DNS servers, define the gateway metric, override the router's MAC address, set MTU and more. You will find additional information on how to define these settings bellow.

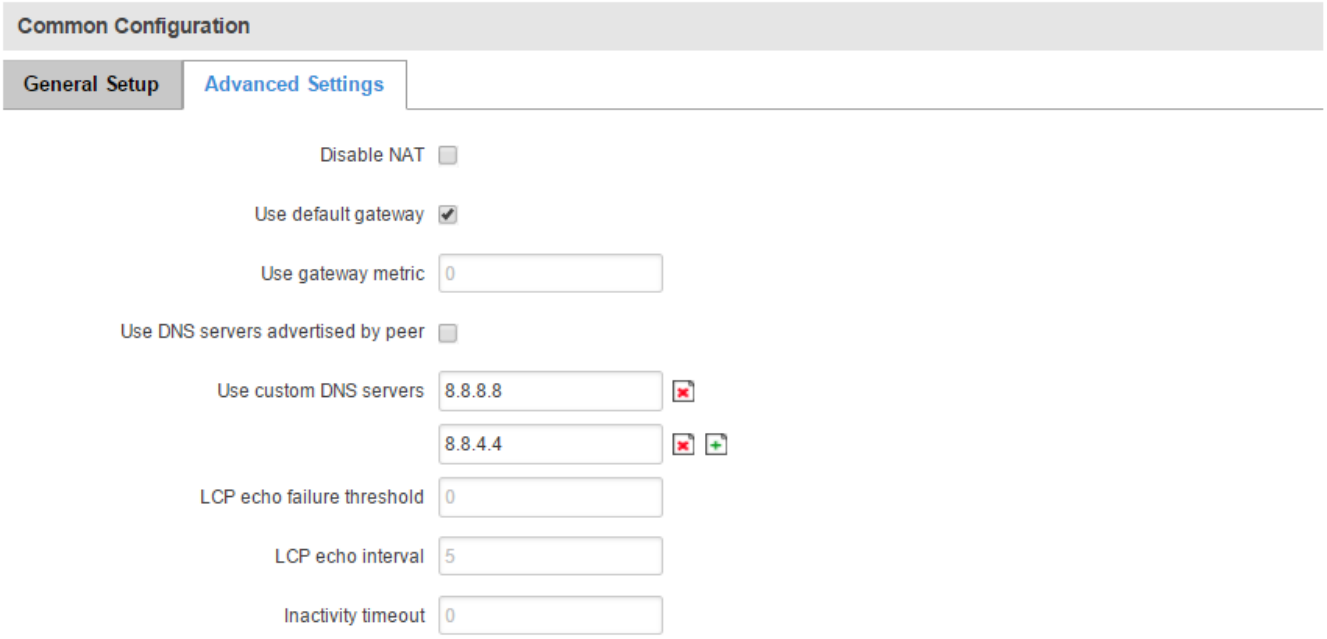


	Field name	Sample value	Explanation
1.	Disable NAT	On/Off	Toggle **Network Address Translation (NAT)** on or off for the selected network interface
2	Use broadcast flag	Enable/Disable	Required for certain ISPs, e.g. Charter with DOCSIS 3
3.	Use default gateway	Enable/Disable	If left unchecked, no default route is configured
4.	Use DNS servers advertised by peer	Enable/Disable	If left unchecked, the advertised DNS server addresses are ignored
5.	Use custom DNS Servers	8.8.8.8 8.8.4.4	Lets you chose your own preferred DNS servers
6.	User gateway metric	0	The WAN configuration by default generates a routing table entry. In this field you can alter the metric of that entry
7.	Client ID to send when requesting DHCP		Client ID which will be sent when requesting a DHCP lease
8.	Vendor Class to send when requesting DHCP		Vendor class which will be sent when requesting a DHCP lease
9.	Override MAC address	00:51:33:77:56:17	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 but not with your router). In this field you can enter your computer's MAC address and fool the gateway in to thinking that it is communicating with your computer

10.	Override MTU	1500	**Maximum Transmission Unit (MTU)** – specifies the largest possible size of a data packet

7.2.2.2.3 PPPoE

For the PPPoE protocol you can turn NAT on or off, specify custom DNS servers, define the gateway metric, configure LCP echo settings and more. You will find additional information on how to define these settings bellow.

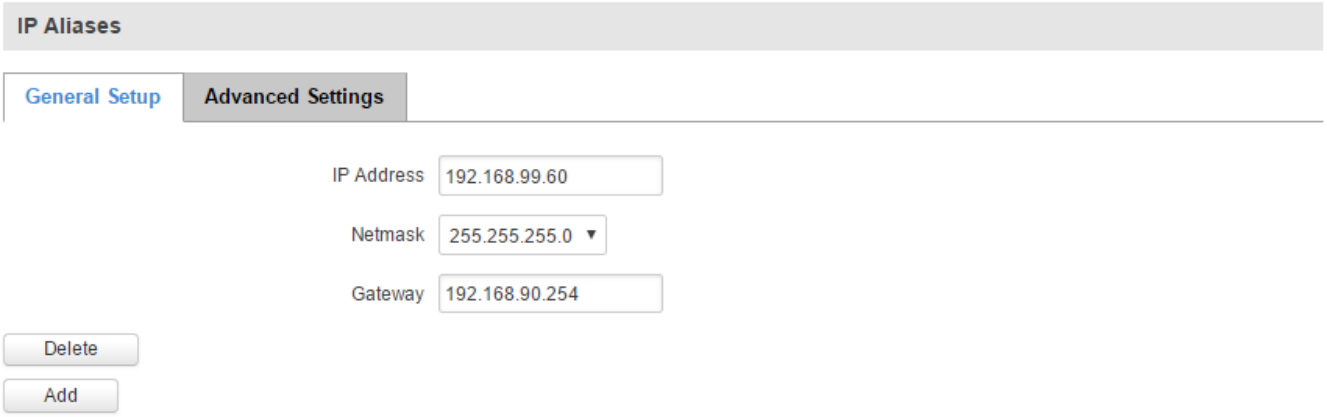


	Field name	Sample value	Explanation
1.	Disable NAT	Enable/Disable	Toggle **Network Address Translation (NAT)** on or off for the selected network interface
2	Use default gateway	Enable/Disable	If left unchecked, no default route is configured
3.	Use gateway metric	0	The WAN configuration by default generates a routing table entry. In this field you can alter the metric of that entry
4.	Use DNS servers advertised by peer	Enable/Disable	If left unchecked, the advertised DNS server addresses are ignored
5.	Use Custom DNS Servers	8.8.8.8 8.8.4.4	Lets you chose you own preferred DNS servers
5.	LCP echo failure threshold	0	Presume peer to be dead after given amount of LCP echo failures. Leave it at 0 to ignore failures
6.	LCP echo interval	5	Send LCP echo requests at the given interval in seconds. This function is only effective in conjunction with failure threshold
7.	Inactivity timeout	0	Close inactive connection after the given amount of seconds. Leave it at 0 to persist connection

7.2.2.3 IP Aliases

7.2.2.3.1 General setup

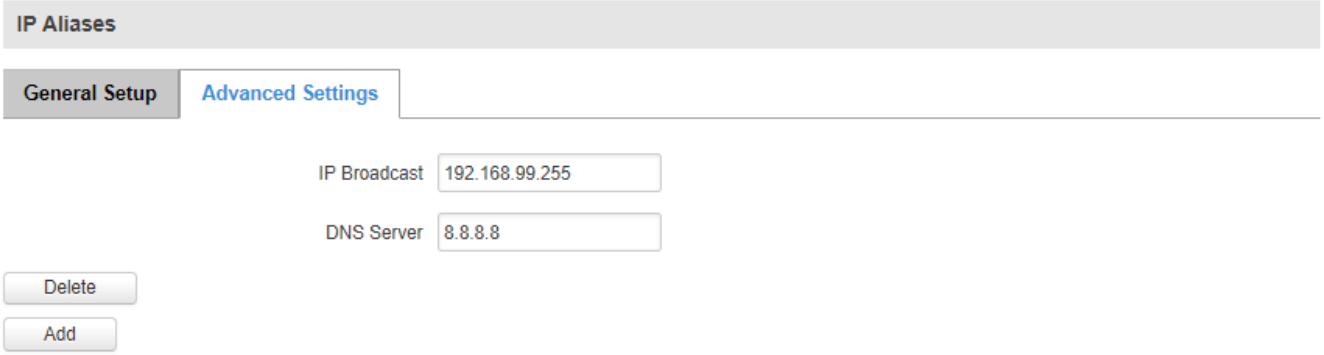
IP Aliases are a way of defining or reaching a subnet that works in the same space as the regular network. This is useful if you need to reach the router in the same network but in a different subnet. If you have a static IP configuration on your computer and don't want to change it every time you need to reach a router in a different subnet, you can configure an IP alias in order to do so.



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

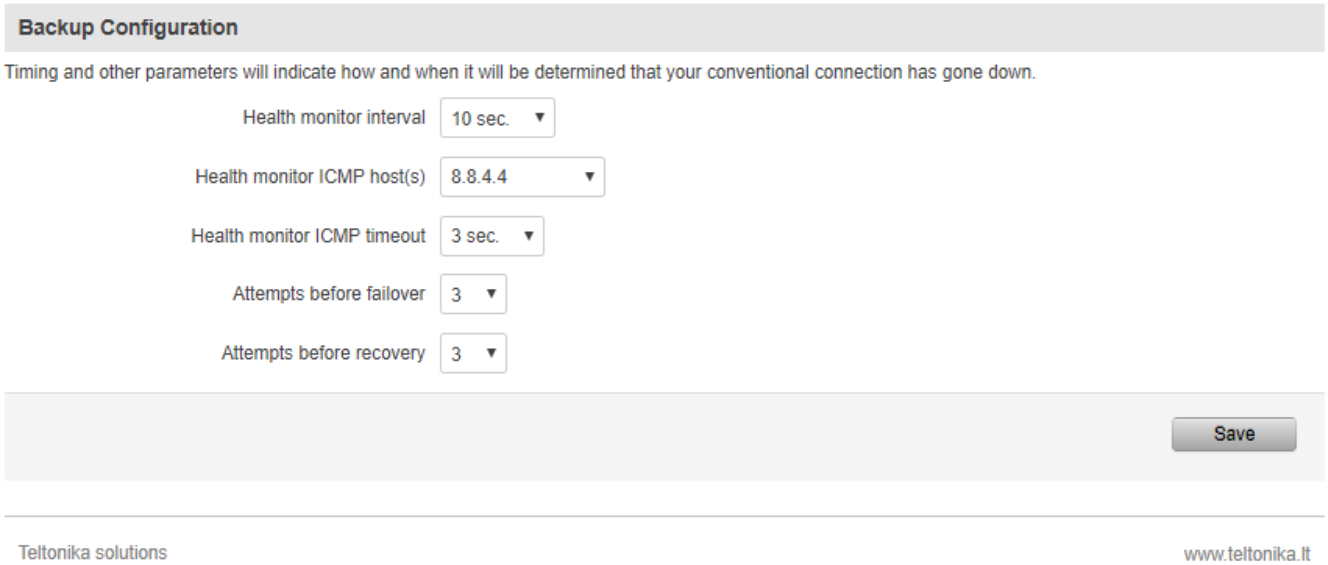
7.2.2.3.2 Advanced Settings

You may also define a broadcast address and a custom DNS server for your IP Aliases in the Advanced Settings tab.



7.2.2.4 Backup WAN configuration

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

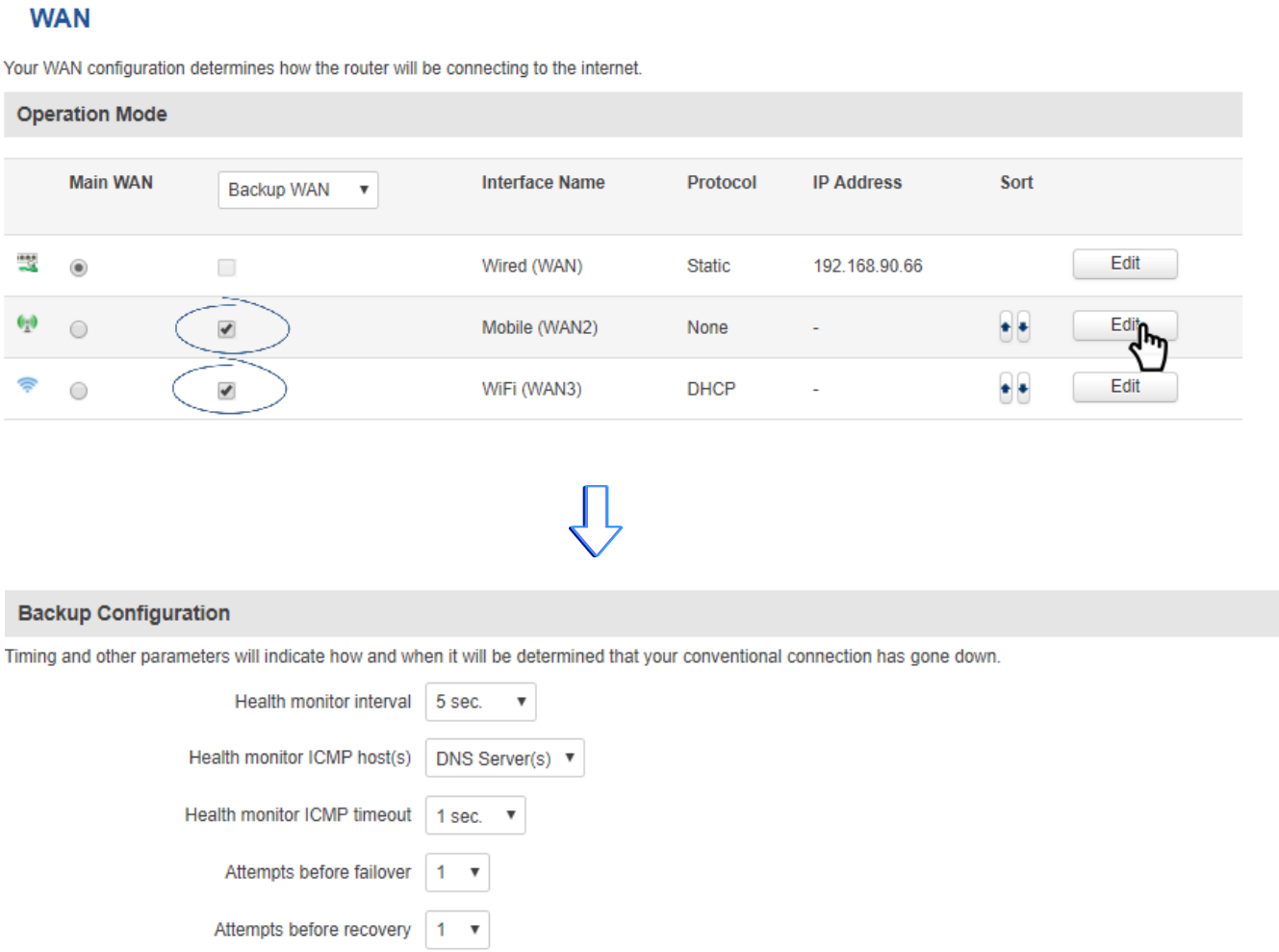


The majority of the options consist of timing and other important parameters that help determine the health of your primary connection. Regular health checks are constantly performed in the form of ICMP packets (Pings) on your primary connection. When the connections state starts to change (READY->NOT 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.

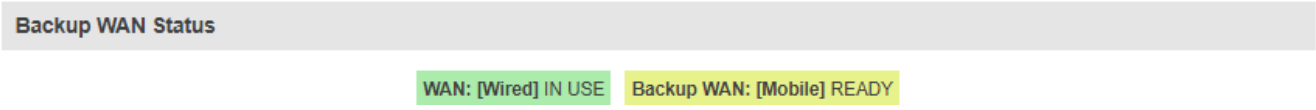
	Field Name	Possible values	Explanation
1.	Health monitor interval	Disable/5/10/20/30/60/120 Seconds	The interval at which health checks are performed
2.	Health monitor ICMP host(s)	8.8.4.4 / Disable / DNS Server(s) / WAN Gateway / custom	Indicate where to send ping requests for a health check. As there is no definitive way to determine when the connection to internet is down for good, it is best to define a host whose availability is that of the internet as a whole (e.g., 8.8.8.8, 8.8.4.4)
3.	Health monitor ICMP timeout	1/2/3/4/5/10 Seconds	The frequency at which ICMP requests are to be sent. It is advised to 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	The number of failed ping attempts after which the connection is to be declared as "down"
5.	Attempts before recovery	1/3/5/10/15/20	The number of successful ping attempts after which the connection is to be declared as "up"

7.2.3 How do I set up a backup link?

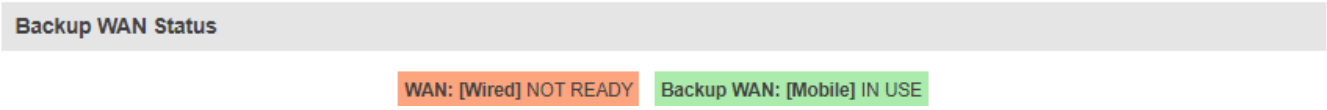
First you must select a main link and choose one or two backup links in the WAN section. Then push the "Edit" button and configure your WAN and Backup Wan settings to your liking.



Click Save after you have made your changes and wait until the settings are applied. You can monitor main/backup WAN status in the Status -> Network Information -> WAN page. If everything is working correctly you should see something like this:



The above picture shows the status for the Mobile 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:



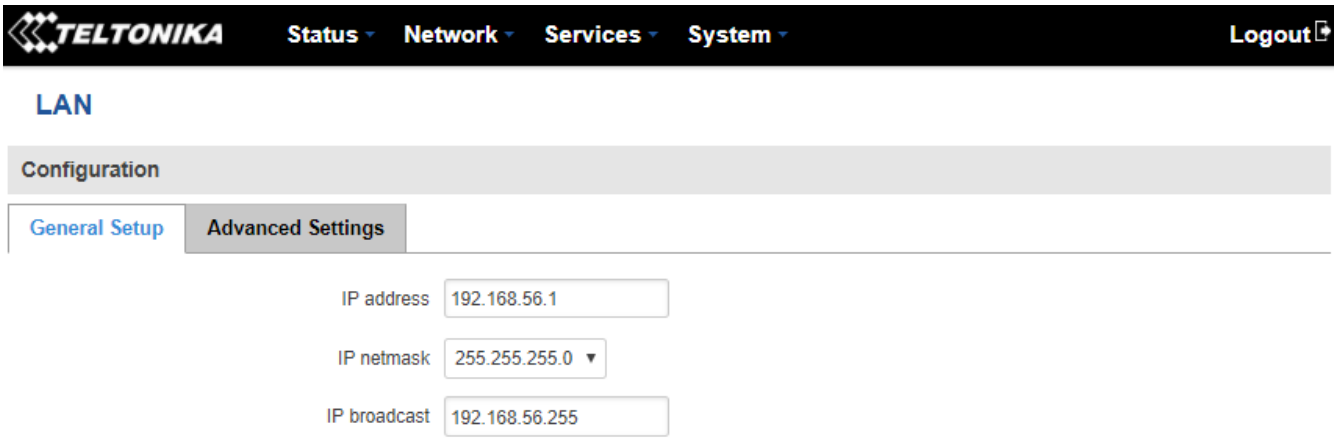
When the main connection is down, all the traffic will go through the backup WAN interface (in this case, mobile.) When you plug the cable back in, the connection will be restored and the traffic will again go through the main WAN interface (in this case, wired.)

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.

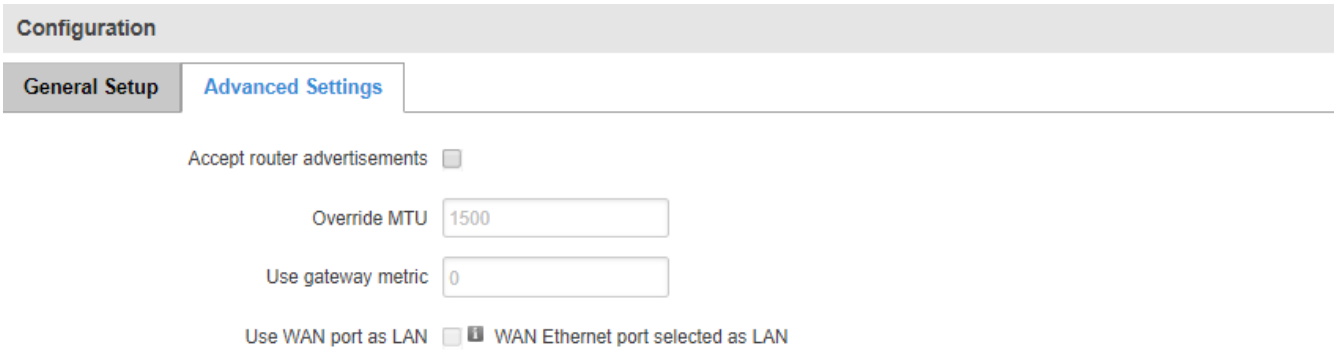
7.3.1 Configuration

7.3.1.1 General Setup



	Field name	Sample value	Explanation
1.	IP address	192.168.56.1	IP 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	192.168.56.255	IP broadcasts are used by BOOTP and DHCP clients to find and send requests to their respective servers

7.3.1.2 Advanced settings

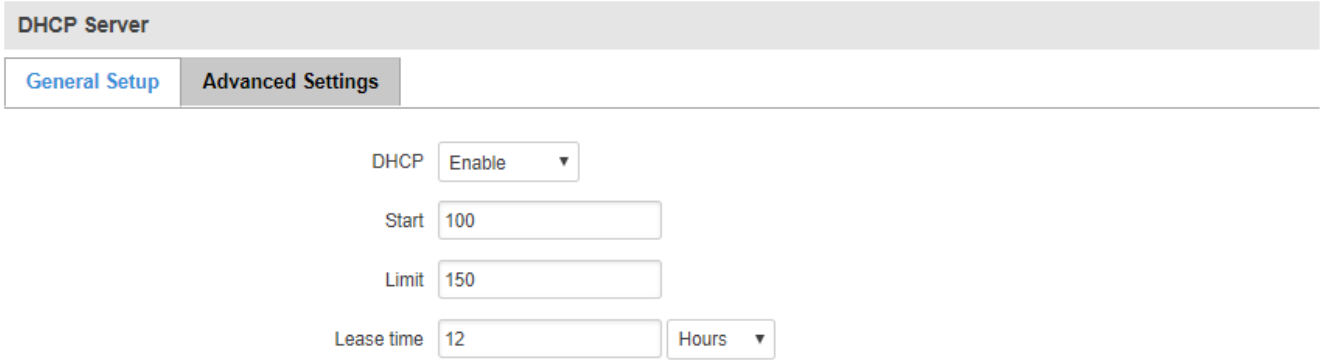


	Field name	Possible values	Explanation
1.	Accept router advertisements	Enable/Disable	When enabled, this function allows accepting router advertisements (disabled by default)
2.	Override MTU	0 - 1500	MTU (Maximum Transmission Unit) specifies the largest possible size of a data packet
3.	Use gateway metric	Any integer number	The LAN configuration generates an entry in the routing table. In this field you can alter the metric of that entry. Higher metric means higher priority
4.	Use WAN port as LAN	Enable/Disable	Lets you use the WAN port as if it were a LAN port

7.3.2 DHCP Server

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 an IP address automatically the DHCP server will lease out an IP address and the device will be able to communicate with the router.

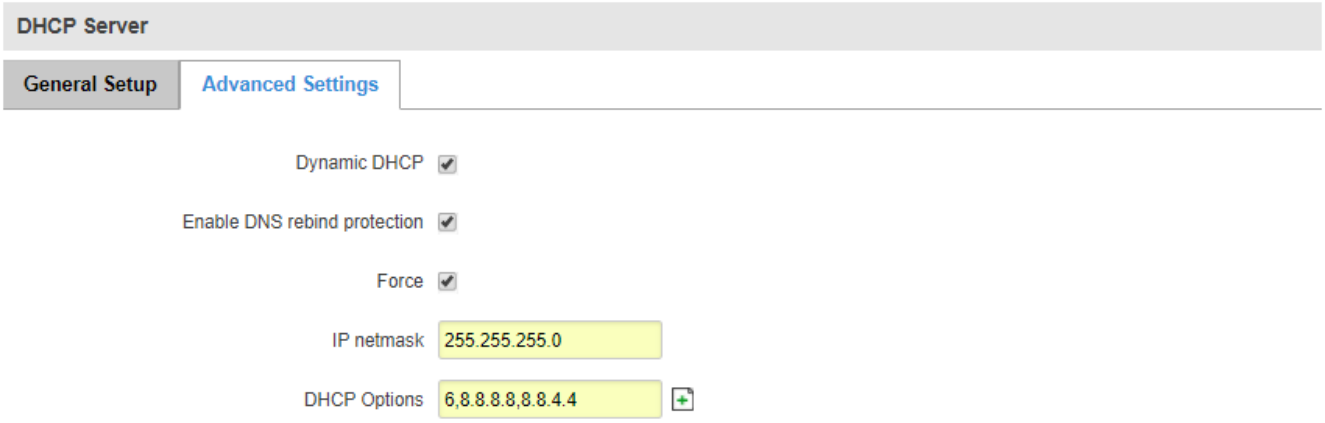
7.3.2.1 General Setup



	Field Name	Sample value	Explanation
1.	DHCP	Enable / Disable/ DHCP Relay	Enables or disables DHCP Server. If DHCP Relay is selected, you will be prompted to enter an IP address of another DHCP server in your LAN. In this case, Whenever a new device connects to the router, the router will redirect any DHCP requests to the specified DHCP Server
2.	Start	100	The starting IP address value. e.g., if your router's 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 lease out addresses starting from 192.168.2.100
3.	Limit	150	How many addresses the DHCP server can lease out. Continuing from the above example: if the start address is 192.168.2.100 and the server can lease out 150 (sample value) addresses starting from 192.168.2.100 and ending in 192.168.2.249 (100 + 150 – 1 = 249; this is because the first address is inclusive)
4.	Lease time	12	The duration of an IP lease. Leased out addresses will expire after the amount of time specified in this field and the device that was using the lease will have to send a new DHCP request to the router's DHCP server. However, if the device stays connected, its lease will be renewed after half of the specified amount of time passes, e.g., if the lease time is 12 hours, then every 6 hours the device will send a request to the router asking to renew its lease. Lease time can be set in hours or minutes. The minimal amount of time that can be specified is 2min

7.3.2.2 Advanced settings

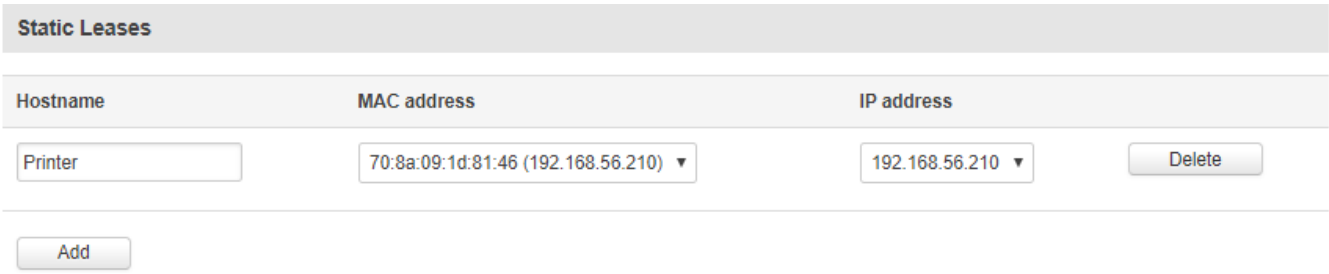
You can also define some advanced options that specify how the DHCP server will operate in your LAN network.



	Field Name	Sample Value	Explanation
1.	Dynamic DHCP	Enabled / Disabled	Enables Dynamic allocation of client addresses. If this is disabled, only clients that have static IP leases will be served
2.	Enable DNS rebind protection	Enabled / Disabled	Enables DNS rebind attack protection by discarding upstream RFC1918 responses (leave default unless necessary otherwise)
3.	Force	Enabled / Disabled	By default the router's DHCP server will not start when it is connected to a network segment that already has a working DHCP server. If enabled, the DHCP force function ensures that the router will always start it's DHCP server, even if there is another DHCP server already running in the router's network
4.	IP netmask	255.255.255.0	Overrides your LAN netmask thus making the DHCP server think that it's serving a larger or smaller network than it actually is
5.	DHCP Options	6,8.8.8.8.,8.8.4.4	Additional options to be added to the DHCP server. For example with '26,1470' or 'option:mtu, 1470' you can assign an MTU per DHCP

7.3.3 Static Leases

Static IP leases are used to reserve specific IP addresses for specific devices by binding them to their MAC address. This is useful when you have a stationary device connected to your network that you need to reach frequently, e.g., printer, fax, etc.

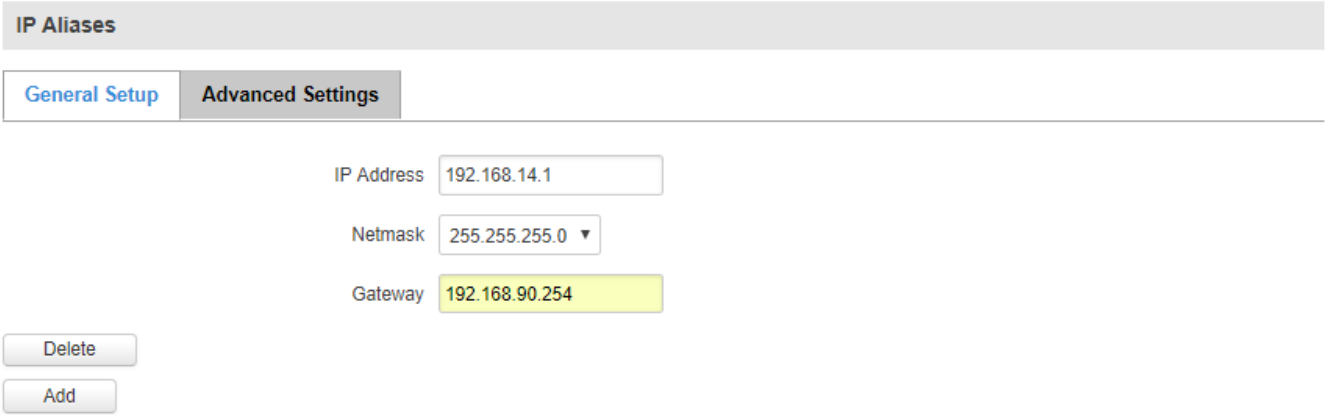


	Field Name	Sample Value	Explanation
1.	Hostname	Printer	A custom name that will be linked with the device
2.	MAC address	10:a5:d0:70:9c:72 (192.168.1.104)	Device's MAC address
3.	IP address	192.168.1.104	The desirable IP address that will be reserved for the specified device

7.3.4 IP Aliases

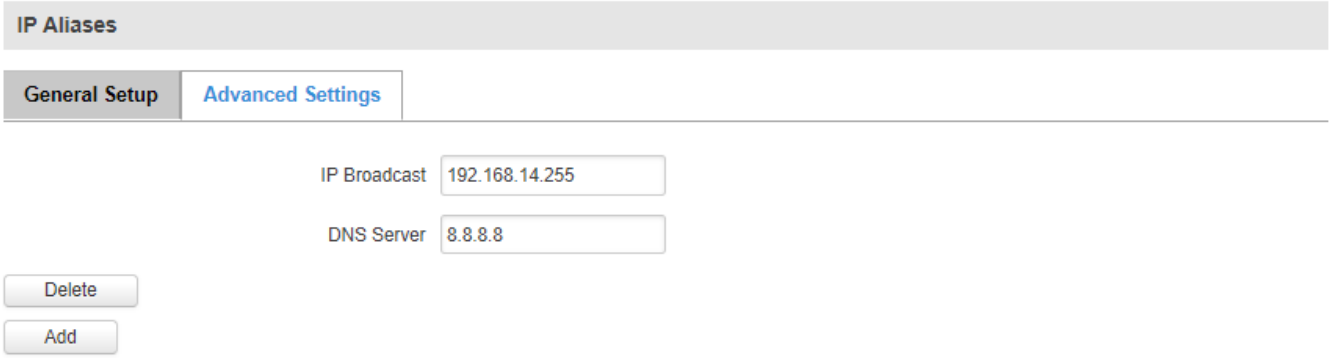
7.3.4.1 General Setup

IP Aliases are a way of defining or reaching a subnet that works in the same space as the regular network. This is useful if you need to reach the router that is located in the same network but in a different subnet. If you have a static IP configuration on your computer and don't want to change it every time you need to reach a router in a different subnet, you can configure an IP alias in order to do so.



7.3.4.1 Advanced Settings

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



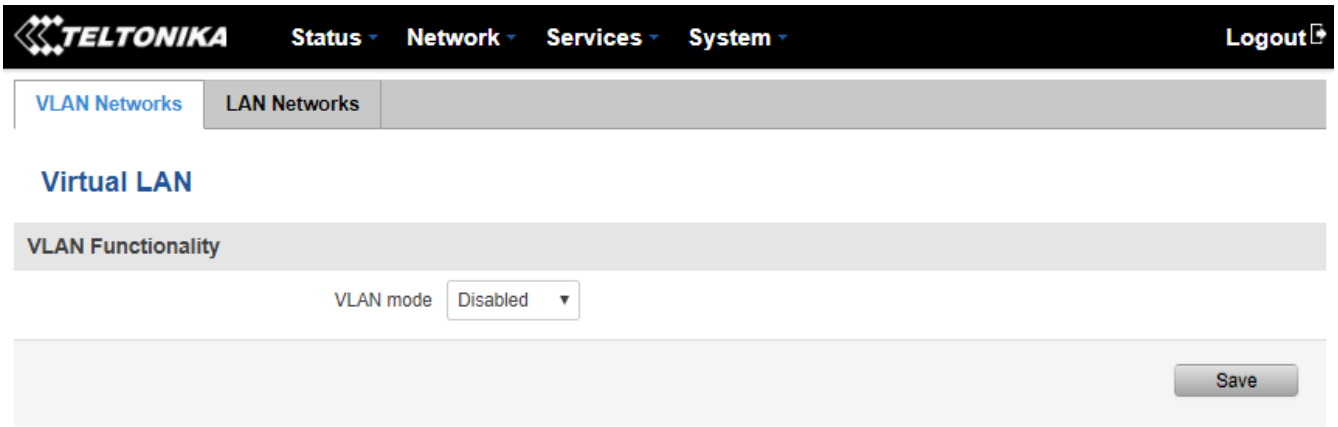
You can find the directions on how to configure IP aliases in the WAN section of this document

7.4 VLAN

The VLAN window provides you with the possibility to create and configure your own Virtual LAN networks, which can either be Port based or Tag based.

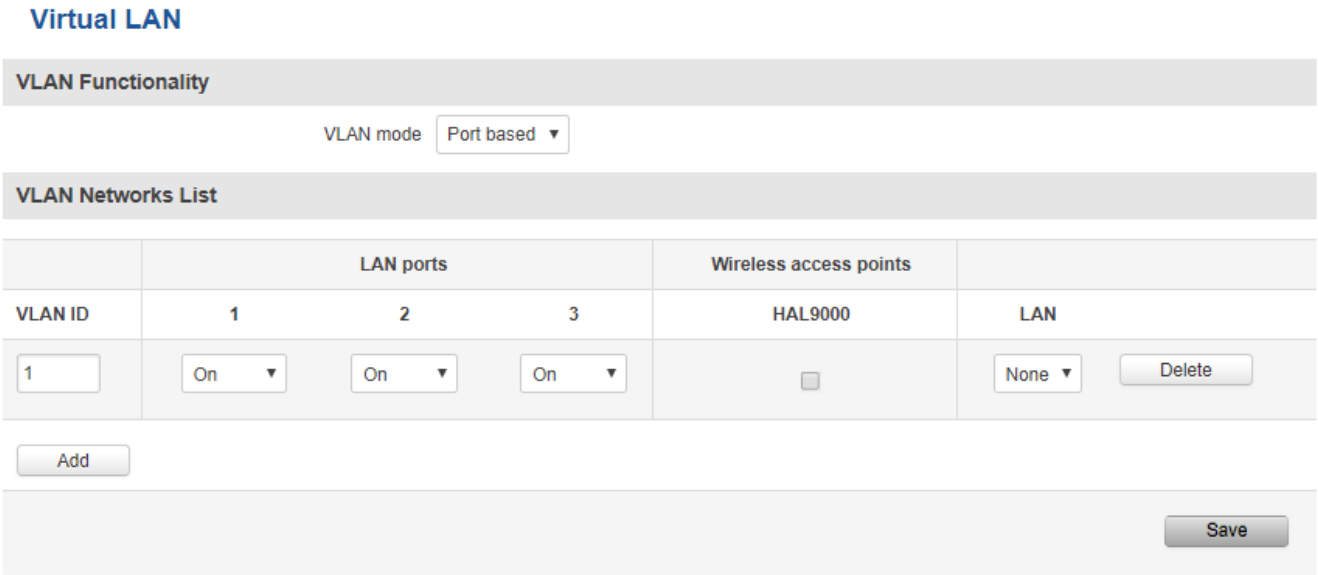
7.4.1 VLAN Networks

7.4.1.1 VLAN Functionality



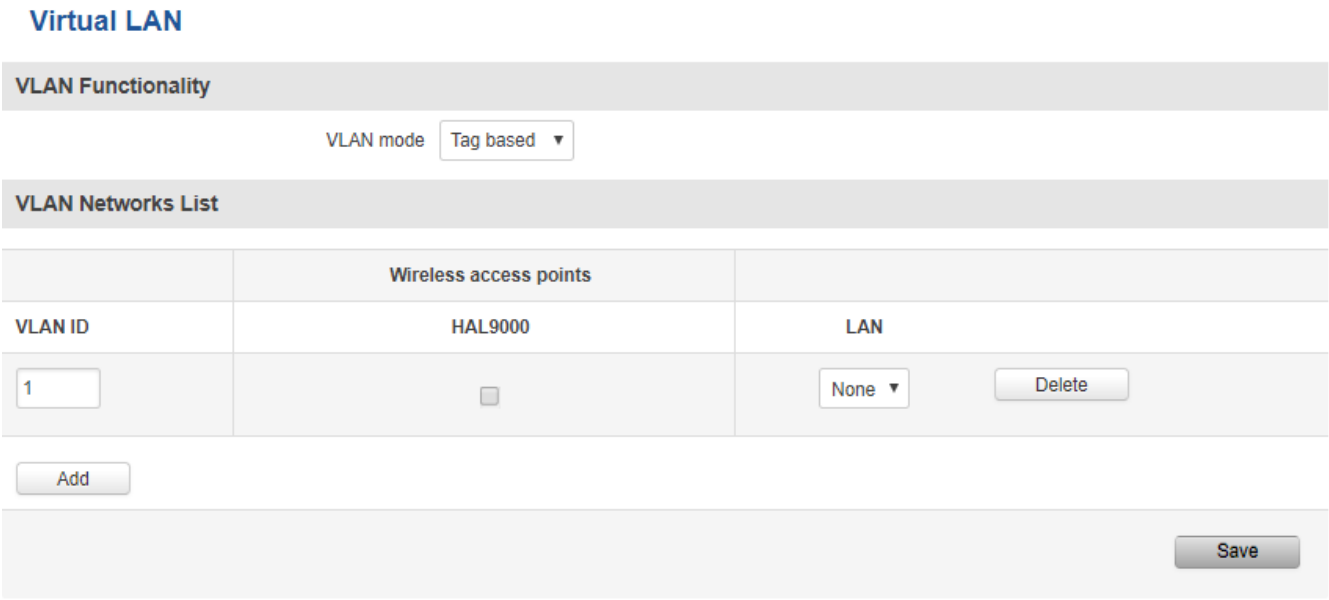
	Field Name	Possible Values	Explanation
1.	VLAN mode	Disabled / Port based / Tag based	Lets you choose the VLAN mode or disable VLAN functionality

7.4.1.2 Port based VLAN



	Field Name	Possible Values	Explanation
1.	VLAN ID	1-4094	VLAN Identification number
2.	LAN ports 1 / 2 / 3	On / Off / Tagged	Switches the LAN port state
3.	Wireless access points	Enabled / Disabled	Assign selected access point(s) to the selected LAN
4.	LAN	None / lan (default LAN name)	Assign selected LAN ports and wireless access point(s) to a LAN network

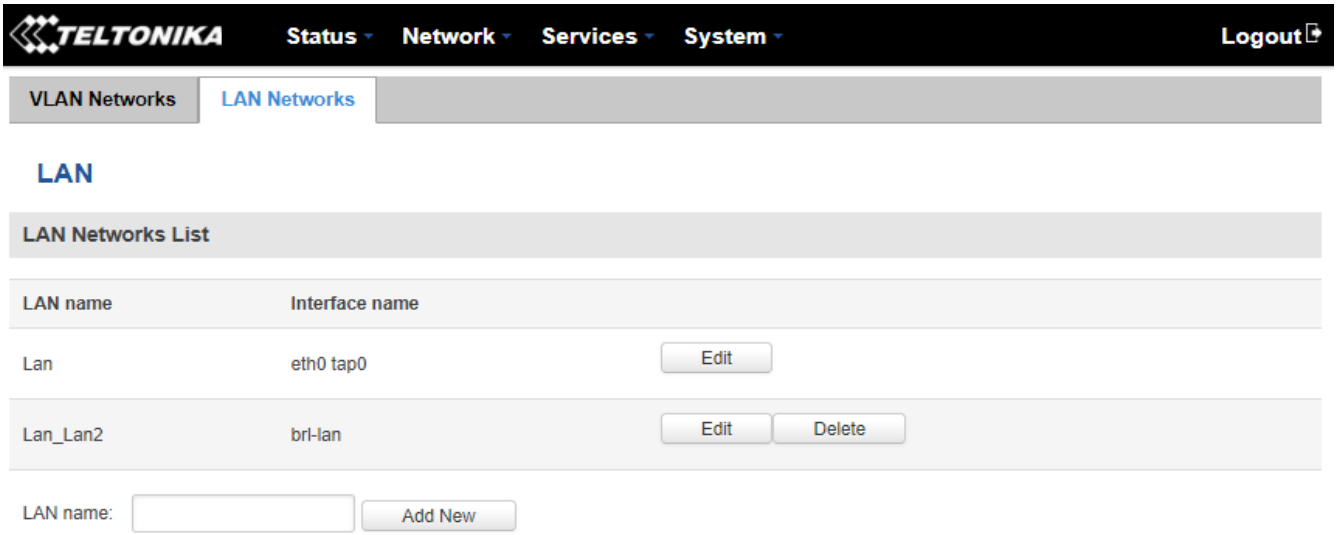
7.4.1.3 Tagged based VLAN



	Field Name	Possible Values	Explanation
1.	VLAN ID	1-4094	VLAN Identification number
2.	Wireless access points	Enabled / Disabled	Assign selected access point(s) to the selected LAN
3.	LAN	None / lan (default LAN name)	Assign selected wireless access point(s) to a LAN network

7.4.2 LAN Networks

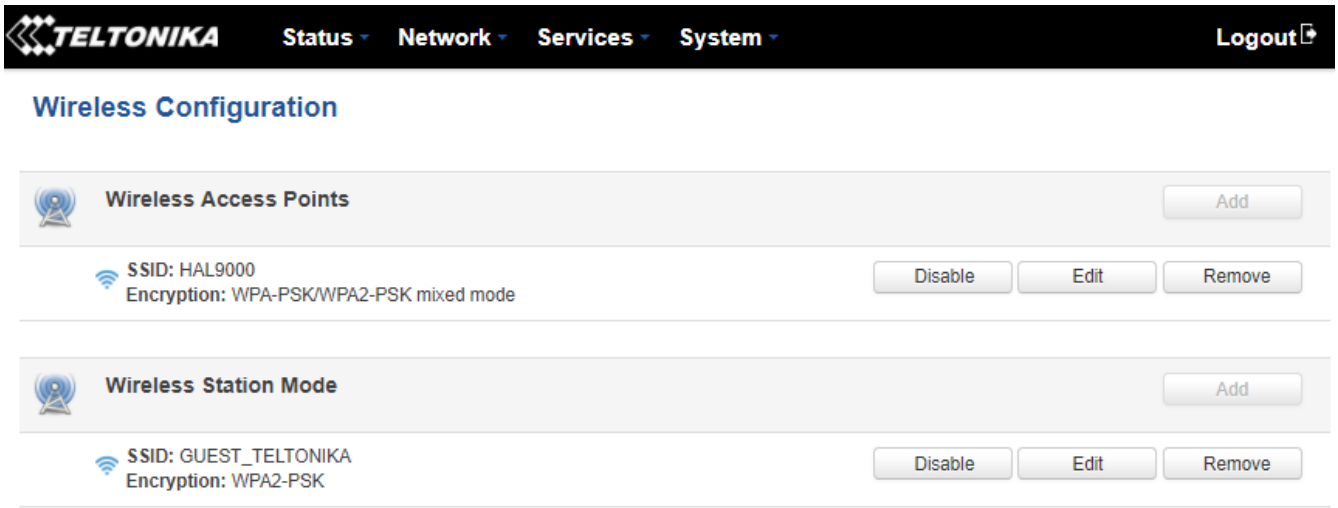
In the LAN Networks page you can create extra LAN networks, and assign them with LAN Ports and wireless access points. You can get extra information on how to configure any of your LAN settings in section 7.3 LAN.



	Field Name	Sample Value	Explanation
1.	LAN name	Lan	Specifies LAN name
2.	Interface name	eth0 tap0	Specifies LAN interface name

7.5 Wireless

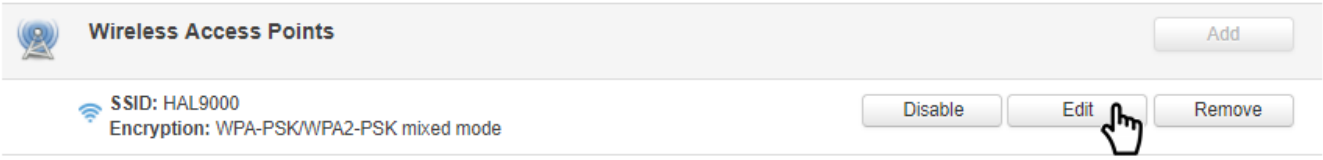
The Wireless configuration window provides you with the possibility to configure your wireless access points and wireless stations. The Wireless Station Mode will become active only when Wi-Fi is configured as an active WAN interface (either main or backup.)



Above is the overview of the Wireless Configuration window. It displays active access points and stations. Here you can disable or enable your Wi-Fi interfaces, remove unwanted access points or stations or enter a configuration window for each Wi-Fi, where you can configure it more thoroughly.

7.5.1 Wireless Access Point

The Wireless Access Point configuration window is used to make changes to different access points. It is divided into two main sections – device and interface. One is dedicated to configuring hardware parameters, the other – software. To access this window, simply click the 'edit' button next to the Wi-Fi interface that you wish to configure:

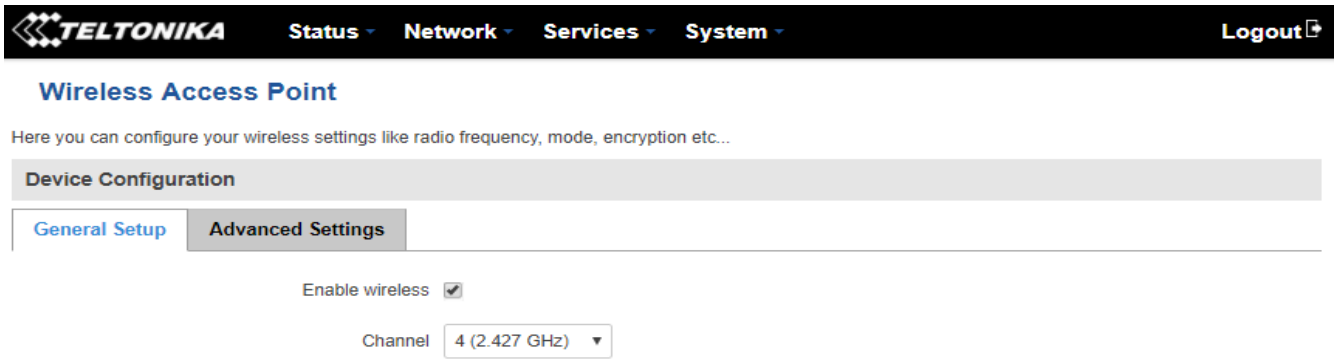


7.5.1.1 Device Configuration

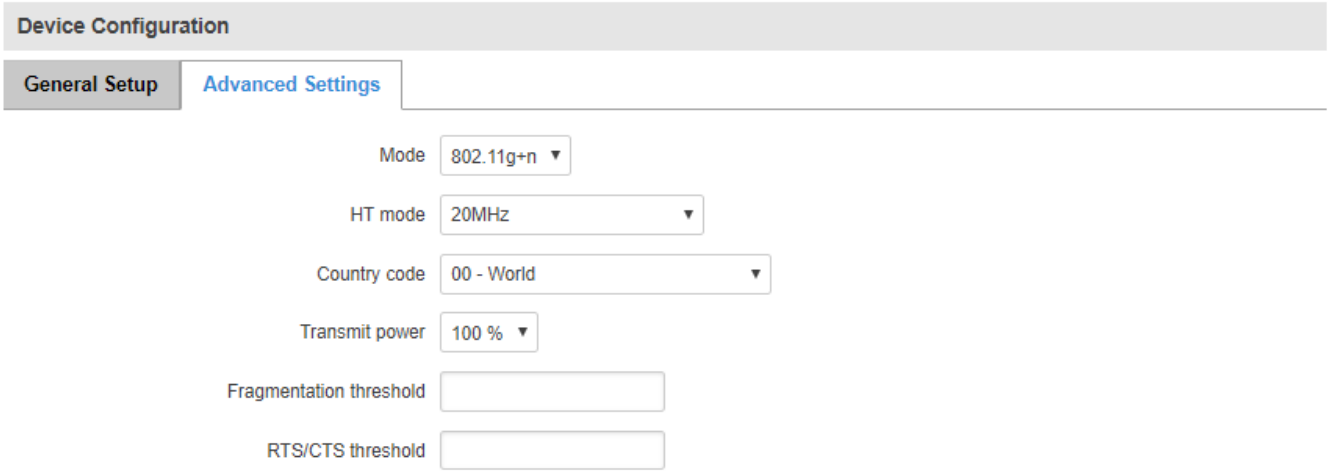
The Device Configuration section is used for configuring Wi-Fi hardware parameters.

7.5.1.1.1 General Setup

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



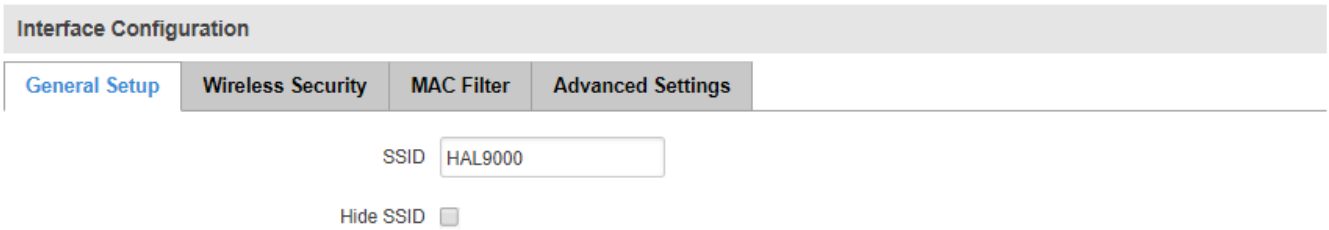
7.5.1.1.2 Advanced Settings



	Field Name	Possible Values	Explanation
1.	Mode	Auto, 802.11b, 802.11g, 802.11g+n	Different modes provide different wireless standard support which directly impacts the radio's throughput performance
2.	HT mode	20MHz / 40MHz 2nd channel above	HT (High Throughput) mode. 40 MHz bandwidth provides better performance
3.	Country code	Any ISO/IEC 3166 alpha2 country code	SO/IEC 3166 alpha2 country codes as defined in ISO 3166-1 standard
4.	Transmit power	20% / 40% / 60% / 80% / 100 %	Wi-Fi signal power
5.	Fragmentation threshold	256-2346	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	0-2347	RTS/CTS (Request to Send/Clear to Send) are mechanisms, used to reduce frame collisions introduced by the hidden node problem. It can help resolve problems arising when several access points are in the same area, contending

7.5.1.2 Interface Configuration

7.5.1.2.1 General Setup

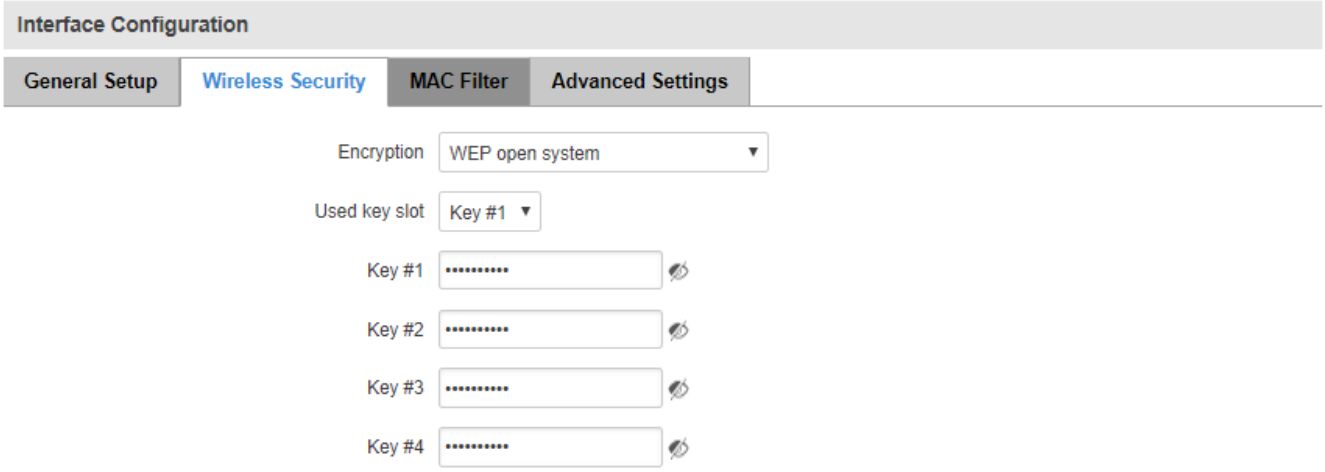


	Field Name	Possible Values	Explanation
1.	SSID	any_name	The name of your Wi-Fi interface. When other Wi-Fi capable computers or devices scan the area for Wi-Fi networks they will see your network with this name
2.	Hide SSID	Enabled/Disabled	Will render your SSID hidden from other devices that try to scan the area

7.5.1.2.2 Wireless Security

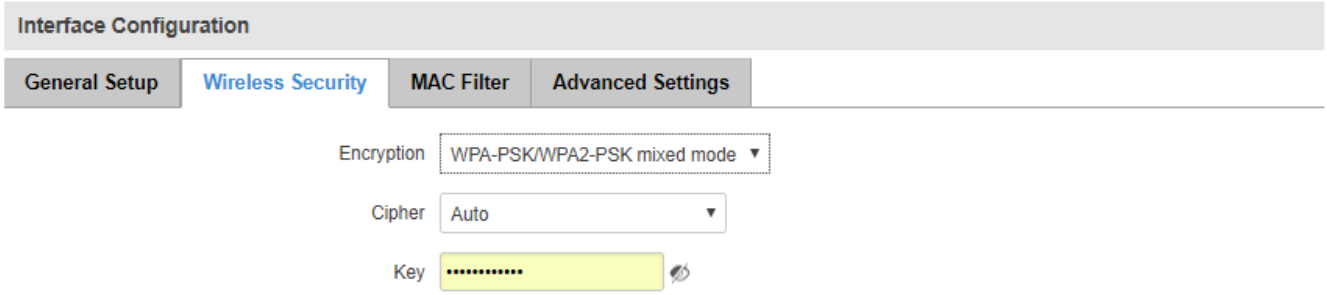
The Wireless Security tab is used to determine what kind of encryption your WLAN will use. You can choose between different types of WEP (Wireless Encryption Protocol) or WPA (Wi-Fi Protected Access.) WPA provides better security because it uses improved data encryption through the temporal key integrity protocol (TKIP) but not all devices support WPA and will work only with WEP type of encryption.

7.5.1.2.2.1 WEP



	Field Name	Sample Value	Explanation
1.	Encryption*	WEP open system	The type of Wi-Fi encryption used
2.	User key slot	Key #1	Which key is used for authentication
3.	Key #1 / Key #2 / Key #3 / Key #4	••••••••••	A 10 symbol custom key used for authentication

7.5.1.2.2.2 WPA

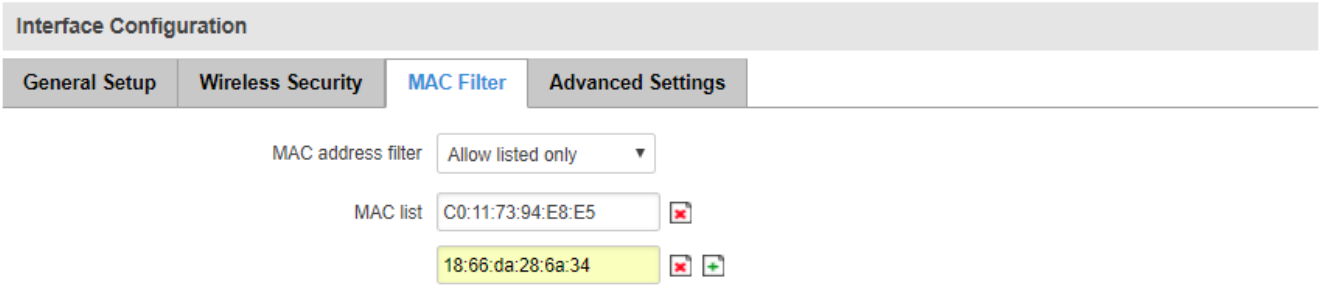


	Field Name	Sample Value	Explanation
1.	Encryption*	WPA-PSK/WPA2-PSK mixed mode	The type of Wi-Fi encryption used
2.	Cipher	Auto	An algorithm for performing encryption or decryption
3.	Key	••••••••••••	A custom passphrase used for authentication (at least 8 characters long)

***Some authentication methods won't support TKIP (and TKIP&CCMP) encryption**

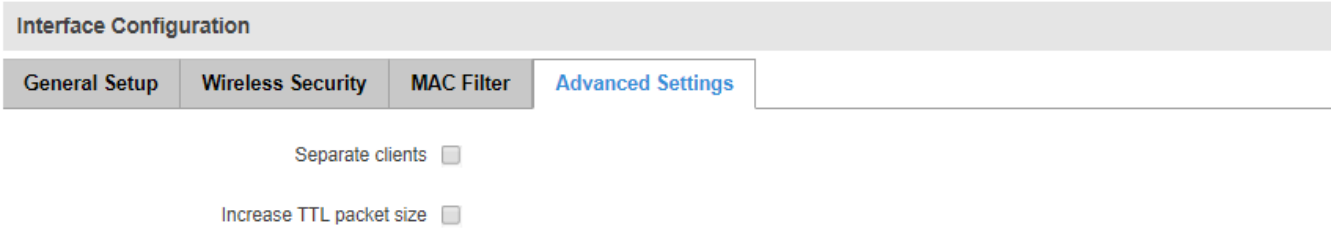
7.5.1.2.3 MAC Filter

The MAC Filter tab is used for setting up rules that allow or exclude devices with specified MAC addresses from connecting to your Wi-Fi network.



	Field Name	Sample Value	Explanation
1.	MAC address filter	Allow listed only / Allow all except listed	**Allow listed only** – only allows devices with MAC addresses specified in the MAC list to connect to your Wi-Fi network **Allow all except listed** - blocks devices with MAC addresses specified in the MAC list to connect to your W-Fi network
2.	Mac list	C0:11:73:94:E8:E5	List of MAC addresses to be included or excluded from connecting to your Wi-Fi network

7.5.1.2.4 Advanced settings

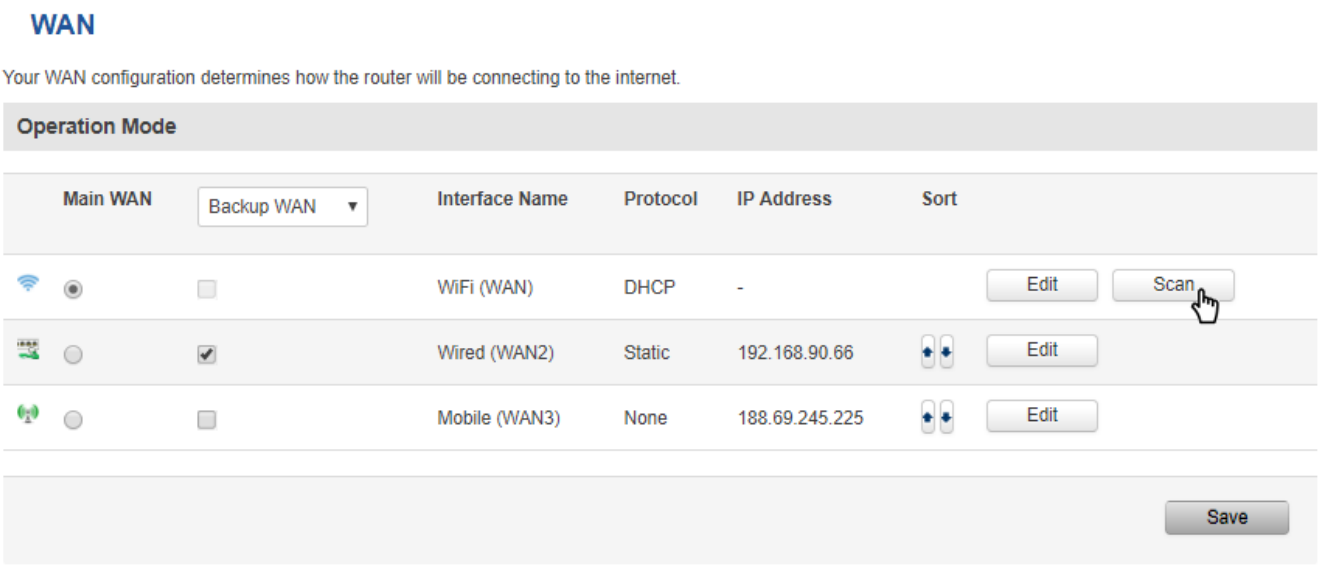


	Field Name	Sample Value	Explanation
1.	Separate clients	Enabled / Disabled	Prevents Wi-Fi clients from communicating with each other on the same subnet
2.	Increase TTL packet size	Enabled / Disabled	Increase TTL packet size for incoming packets

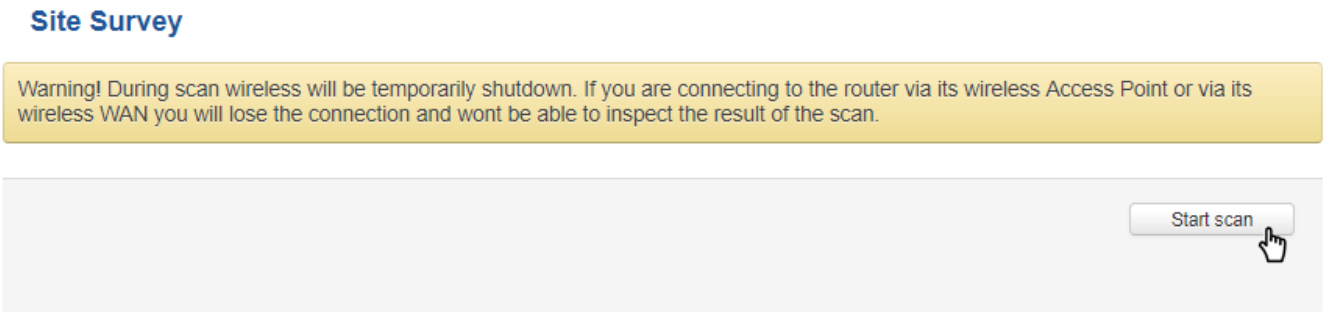
7.5.2 Wireless Station

RUT955 can also work as a Wi-Fi client. Configuring client mode is nearly identical to AP, except for the fact that most of the options are dictated by the wireless access point that the router is connecting to. Changing them can result in an interrupted connection to that 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.



After which you will be redirected to the window shown below.



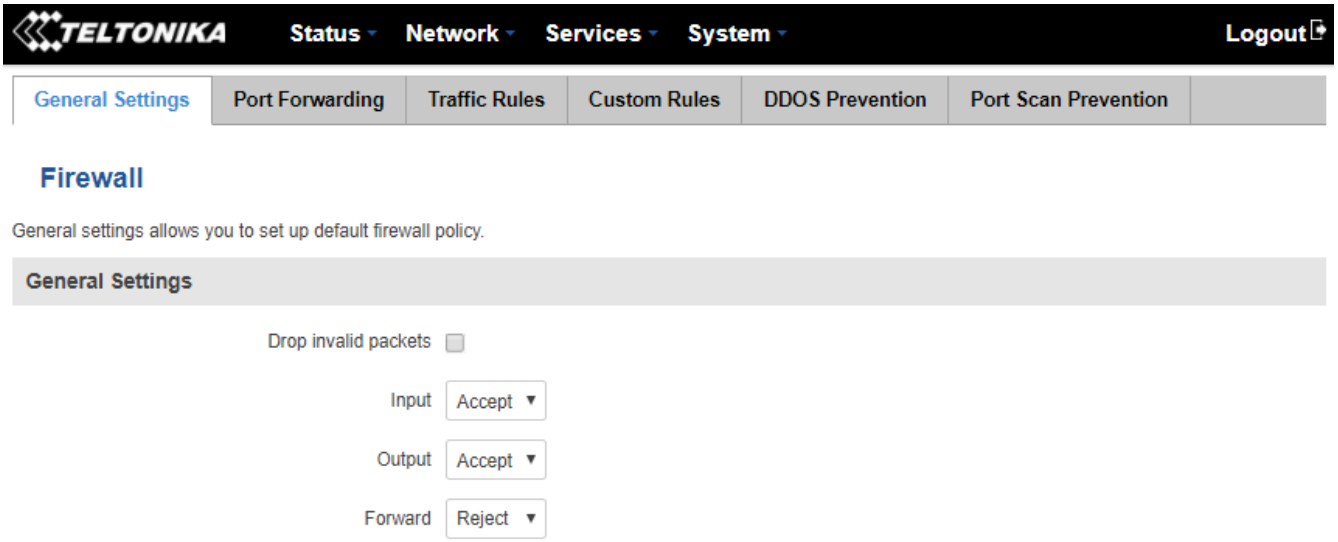
Pressing **Start scan** will initiate a scan for available Wi-Fi Access Points in the area. After the scan finishes, you will see a list of these Access points. Choose one according to your liking and press the **Join Network** button next to it.

7.6 Firewall

In this section we will look over the various firewall features that come with RUT955.

7.6.1 General Settings

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



	Field Name	Possible values	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 of that specific chain. If no rule matches said packet, an according Action (Drop, Reject or Accept) is performed**

Accept – Packet gets to continue down to the next chain;

Drop – Packet is stopped and deleted;

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

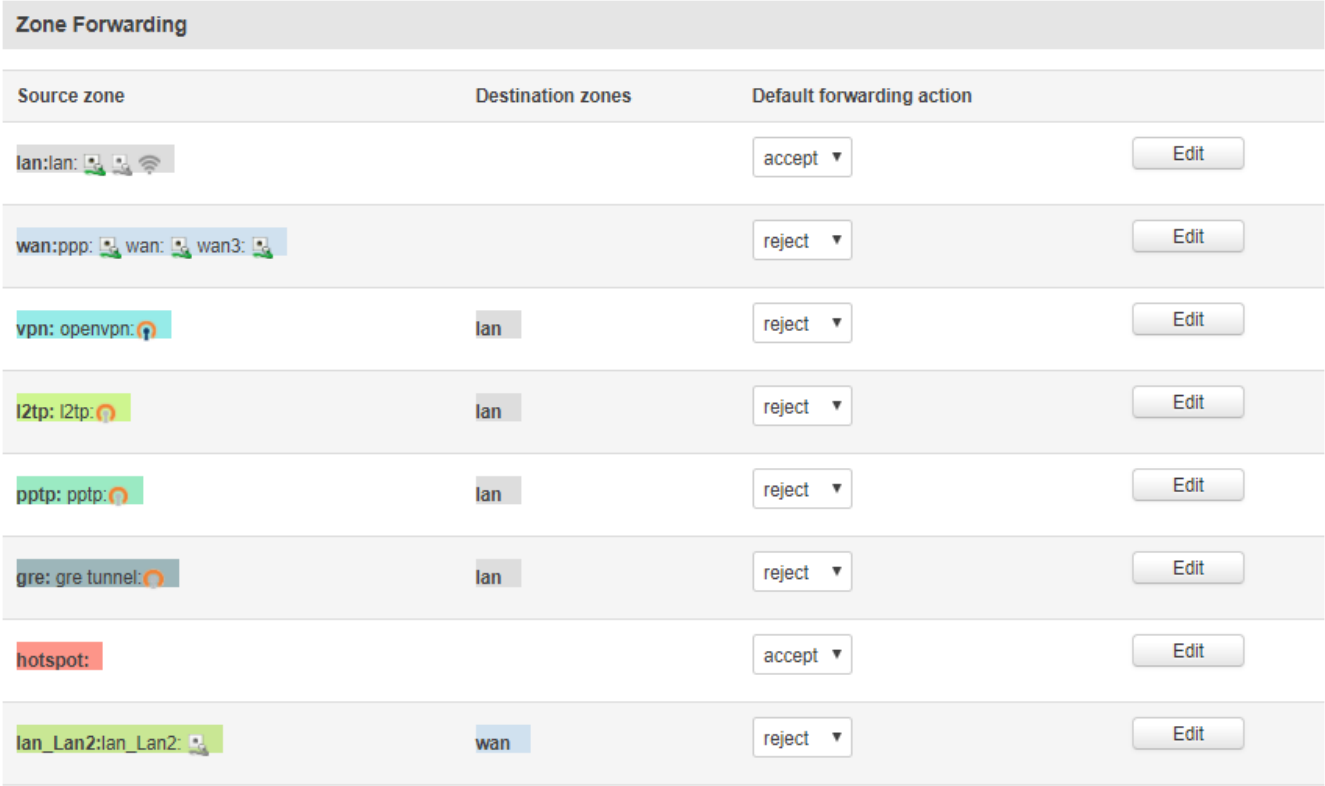
7.6.2 DMZ

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

	Field Name	Possible values	Explanation
1.	Enable	Checked/Unchecked	Enables DMZ
2.	DMZ host IP address	Any IP address from your LAN	Internal host to which the DMZ rule will be applied

7.6.3 Zone Forwarding

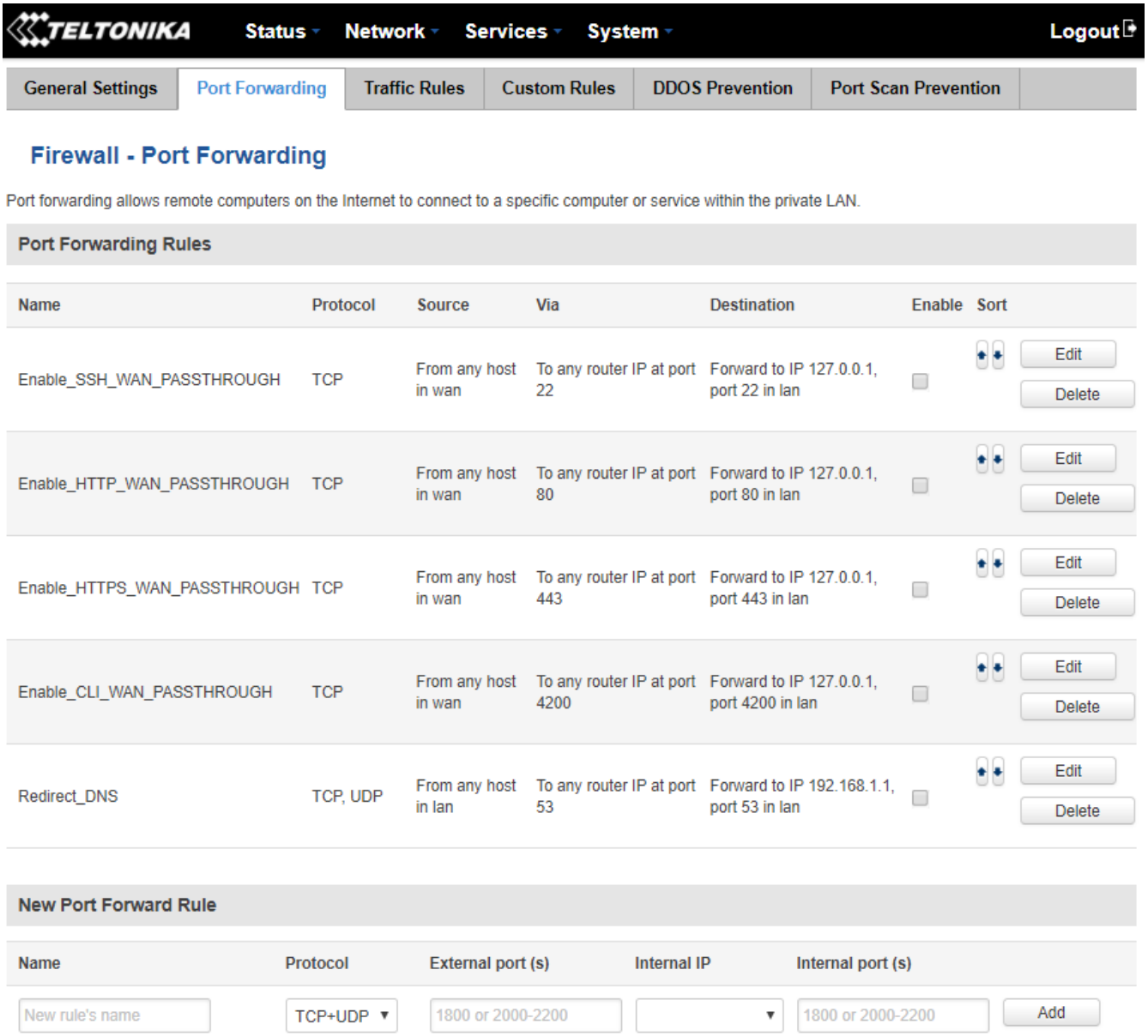
A zone section groups one or more interfaces and serves as a source or destination for forwardings, rules and redirects. The Zone Forwarding window allows you to configure these forwardings.



	Field Name	Sample value	Explanation
1.	Source zone	**vpn:** openvpn	The source zone from which data packets will redirected from
2.	Destination zones	**lan**	The destination zone to which data packets will be redirected to
3.	Default forwarding action	reject	Action to be performed with the redirected packets

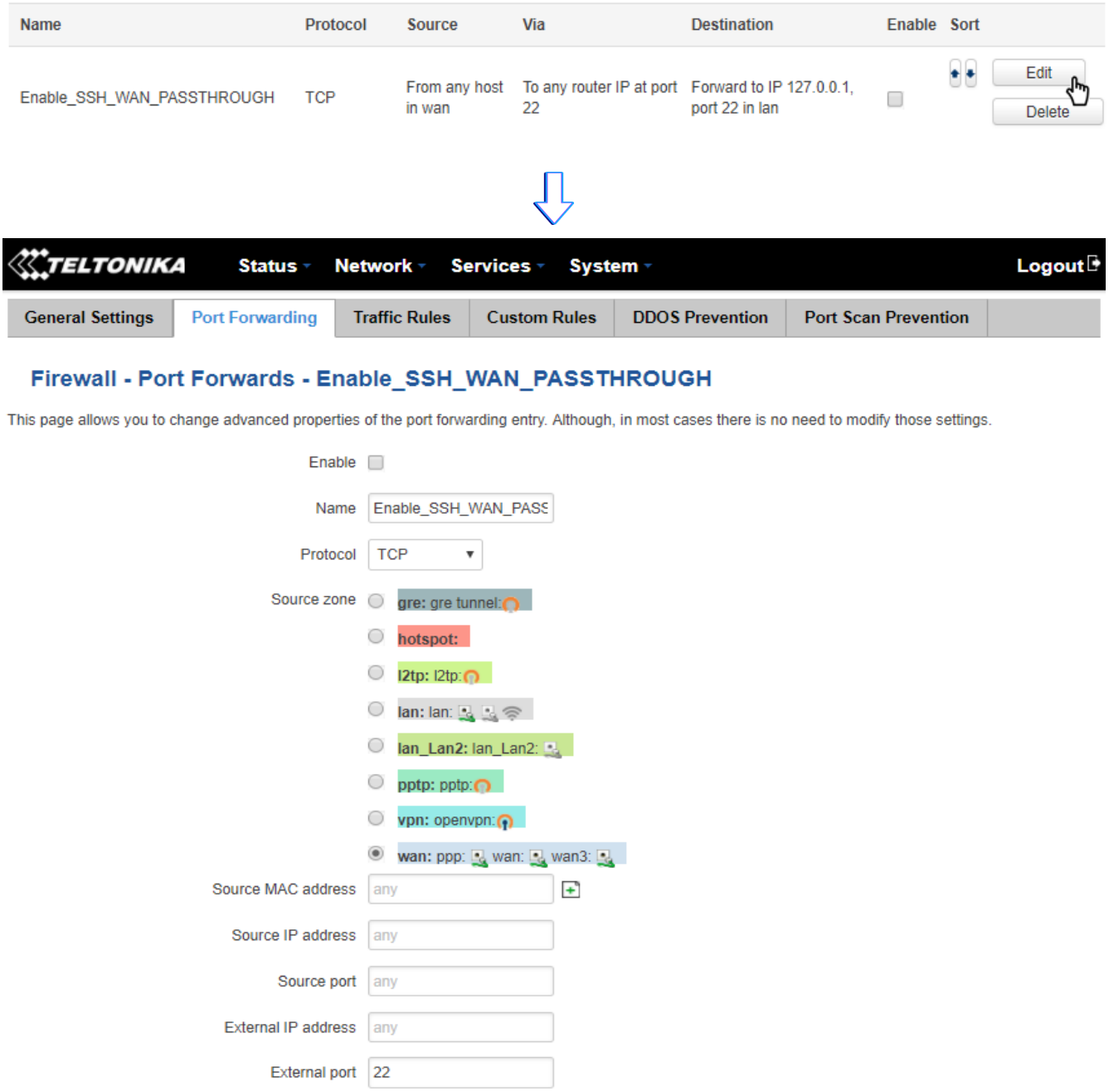
7.6.4 Port Forwarding

The Port Forwarding window is used to set up servers and services on local LAN machines. The picture below 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/

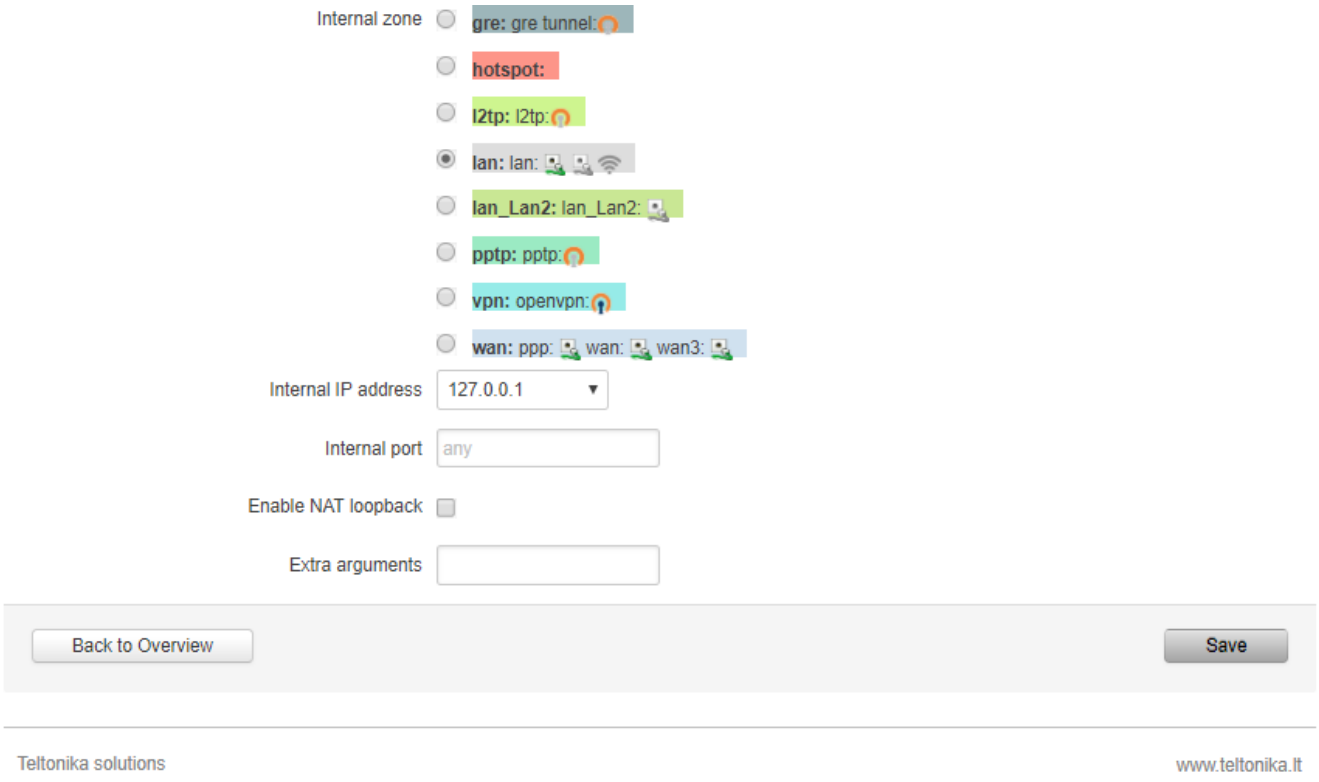


	Field Name	Possible values	Explanation
1.	Name	New rule's name	Name of the rule, used purely to make rule management easier
2.	Protocol	TCP/UDP/TCP+UDP/Other	Type of protocol of incoming packet
3.	External Port	1800 or 2000-2200	From this port on the WAN network the traffic will be forwarded
4.	Internal IP address	IP address of some device 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	1800 or 2000-2200	The rule will redirect the traffic to this port on the internal machine

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



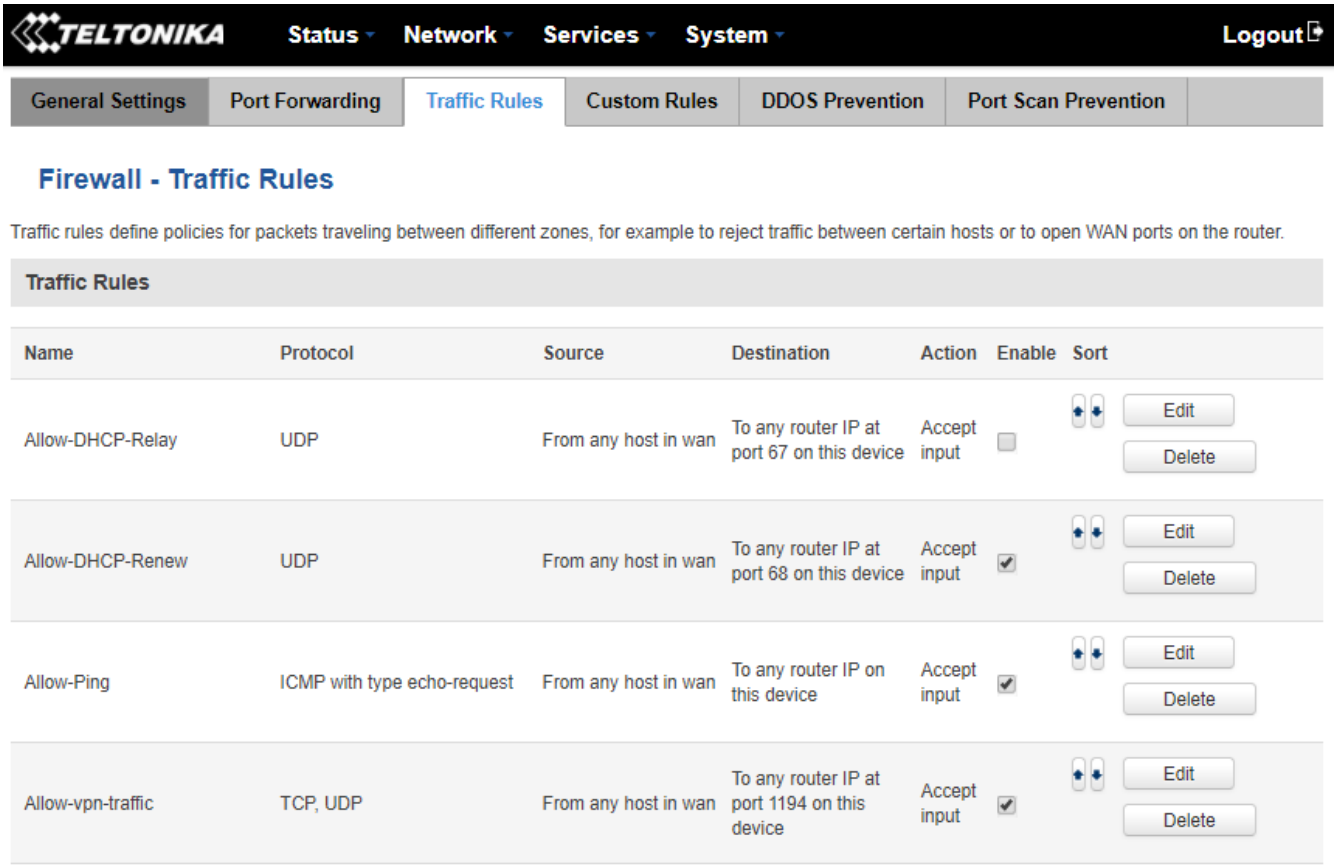
	Field Name	Possible values	Explanation
1.	Name	rule's name	Name of the rule
2.	Protocol	TCP/UDP/TCP+ UDP/ICMP/Custom	You may specify multiple by selecting (custom) and then entering protocols separated by space
3.	Source zone	gre/hotspot/l2tp/lan/pptp/vpn/wan	Match incoming traffic from this zone only
4.	Source MAC address	Any MAC address	Match incoming traffic from these MACs only
5.	Source IP address	Any IP address or range of IPs	Match incoming traffic from this IP or range only
7.	Source port	Any port	Match incoming traffic originating from the given source port or port range on the client host only
8.	External IP address	Any external IP address	Match incoming traffic directed at the given IP address only
9.	External port	Any external port	Match incoming traffic directed at the given destination port or port range on this host only



10.	Internal zone	gre/hotspot/l2tp/lan/pptp/vpn/wan	Redirect matched incoming traffic to the specified internal zone
11.	Internal IP address	Any Internal IP address	Redirect matched incoming traffic to the specified internal host
12.	Internal port	Any port	Redirect matched incoming traffic to the given port on the internal host
13.	Enable NAT loopback	Enable/Disable	NAT loopback enables your local network (i.e. behind your router/modem) to connect to a forward-facing IP address (such as 208.112.93.73) of a machine that it also on your local network
14.	Extra arguments	-	Passes additional arguments to iptables. Use with care!

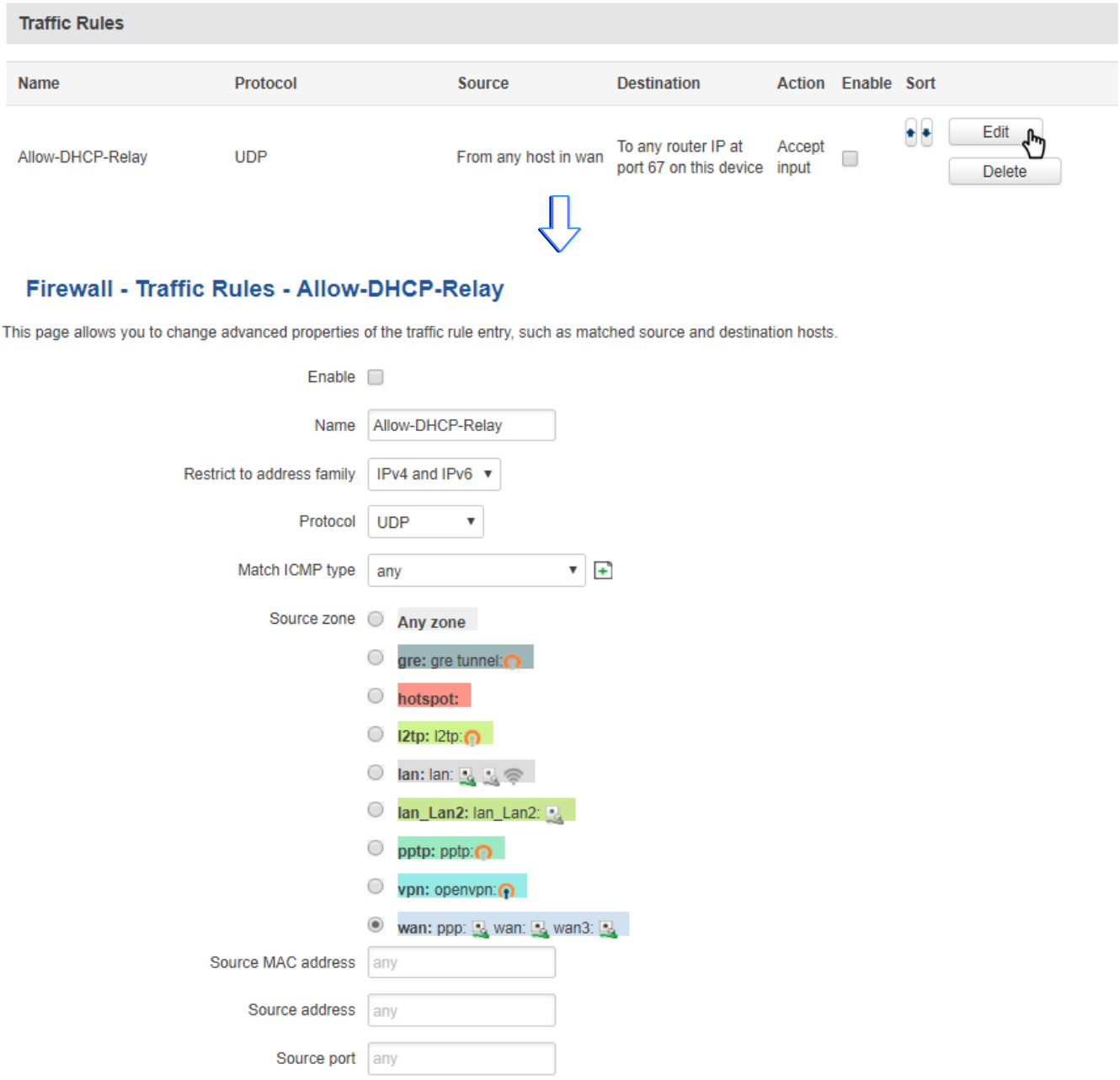
7.6.5 Traffic Rules

The Traffic Rules 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.

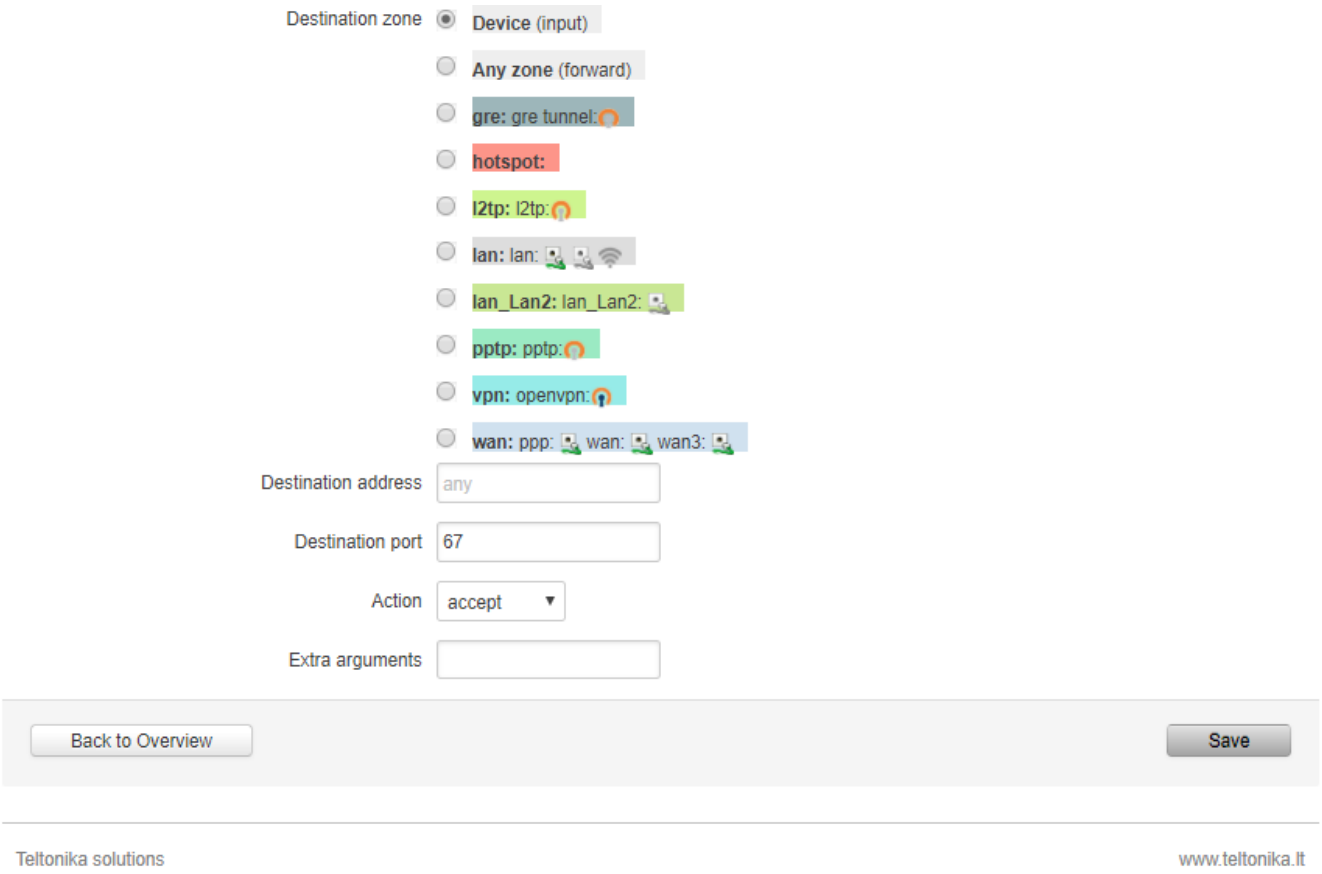


	Field Name	Explanation
1.	Name	Name of the rule. Used for easier rule management purposes
2.	Protocol	Protocol type of incoming or outgoing packet
3.	Source	Match incoming traffic from this IP or range only
4.	Destination	Redirect matched traffic to the given IP address and destination port
5.	Action	Action to be performed with the packet if it matches the rule
6.	Enable	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 however you want

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

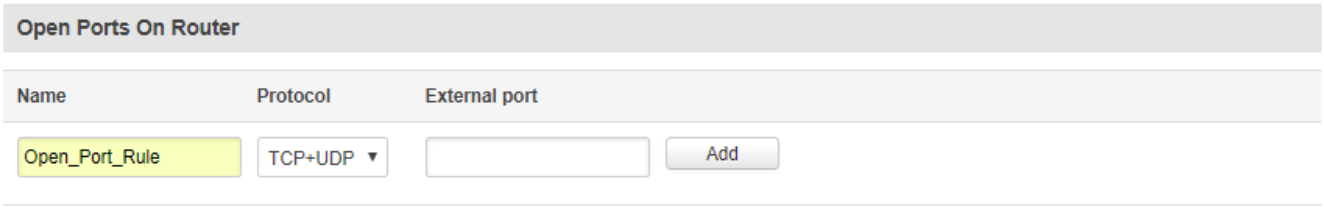


	Field Name	Possible values	Explanation
1.	Name	Rule's name	Used to make rule management easier
2.	Restrict to address family	IPv4 and IPV6 / IPv4 only / IPv6 only	Match traffic from selected address family only
3.	Protocol	TCP / UDP / Any / ICMP / Custom	Protocol of the packet that is being matched against traffic rules
4.	Match ICMP type	Any	Match traffic with selected ICMP type only
5.	Source zone	Any zone / gre / hotspot / l2tp / lan / pptp / vpn / wan	Match incoming traffic from the selected zone only
6.	Source MAC address	Any MAC address	Match incoming traffic from these MACs only
7.	Source address	Any IP address or range	Match incoming traffic from this IP or range only
8.	Source port	Any port	Match incoming traffic originating from the given source port or port range on the client host only



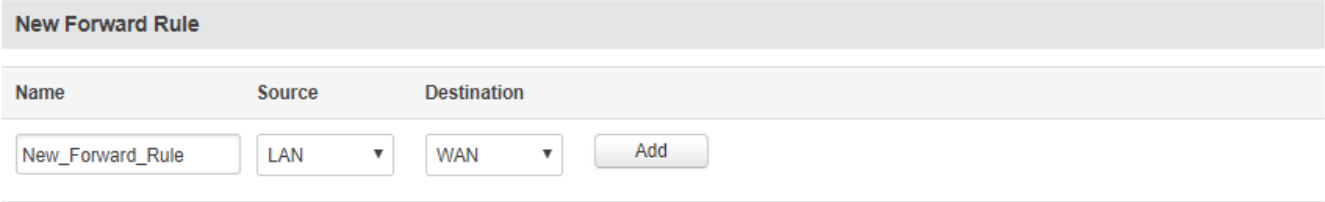
9.	Destination zone	Device/Any zone/LAN/VPN/WAN	Match forwarded traffic to the given destination zone only
10.	Destination address	any	Match forwarded traffic to the given destination IP address or IP range only
11.	Destination port	67	Match forwarded traffic to the given destination port or port range only
12.	Action	Drop/Accept/Reject + chain + additional rules	Action to be taken on the packet if it matches the rule. You can also define additional options like limiting packet volume, and defining to which chain the rule belongs

7.6.5.1 Open Ports On Router



	Field Name	Sample value	Explanation
1.	Name	Open_Port_Rule	Name of the rule, used for easier management
2.	Protocol	TCP/UDP/Any/ICMP/Custom	Protocol of the packet that is being matched against traffic rules
3.	External port	1-65535	Match incoming traffic directed at the given destination port or port range on this host

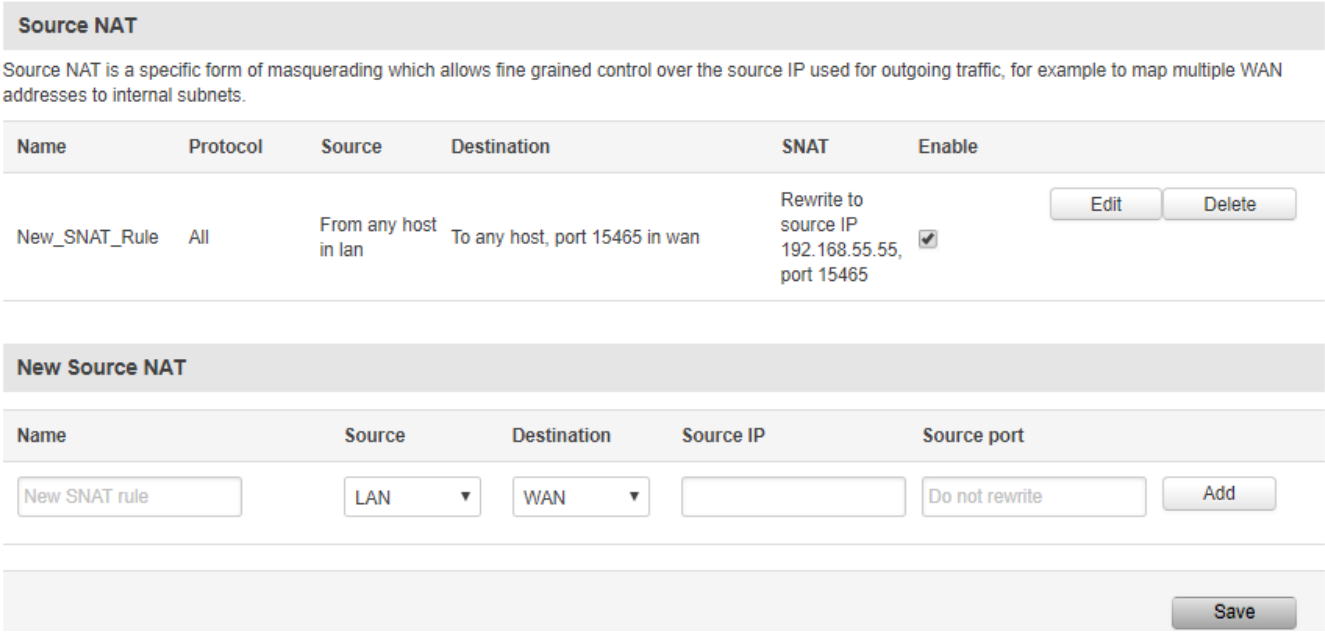
7.6.5.2 New Forward Rule



	Field Name	Possible values	Explanation
1.	Name	Rule's name	Name of the rule, used for easier management
2.	Source	GRE / HOTSPOT / L2TP / LAN / PPTP / VPN / WAN	Match incoming traffic from selected address family only
3.	Destination	GRE / HOTSPOT / L2TP / LAN / PPTP / VPN / WAN	Forward incoming traffic to selected address family only

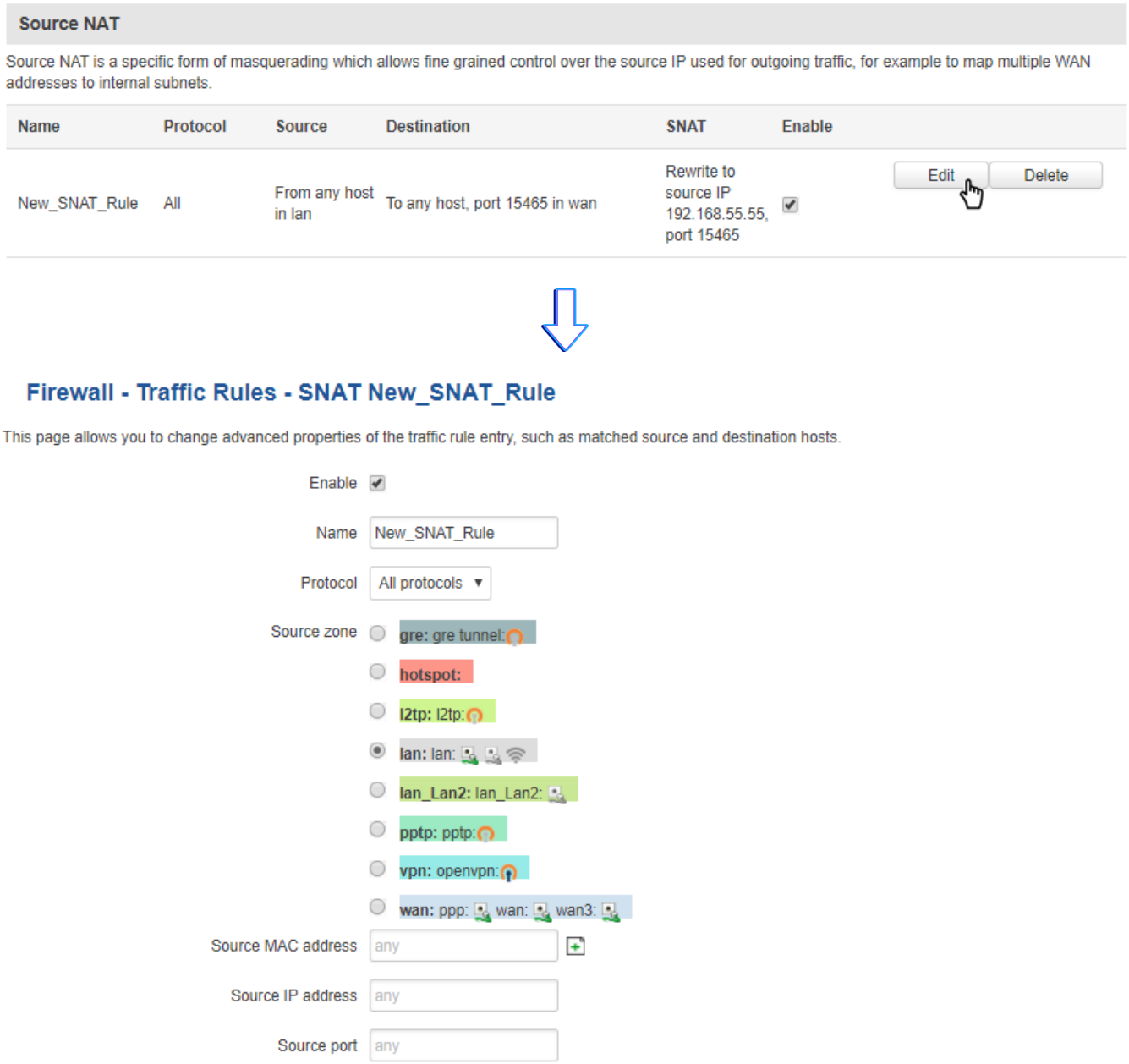
7.6.5.3 Source NAT

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.

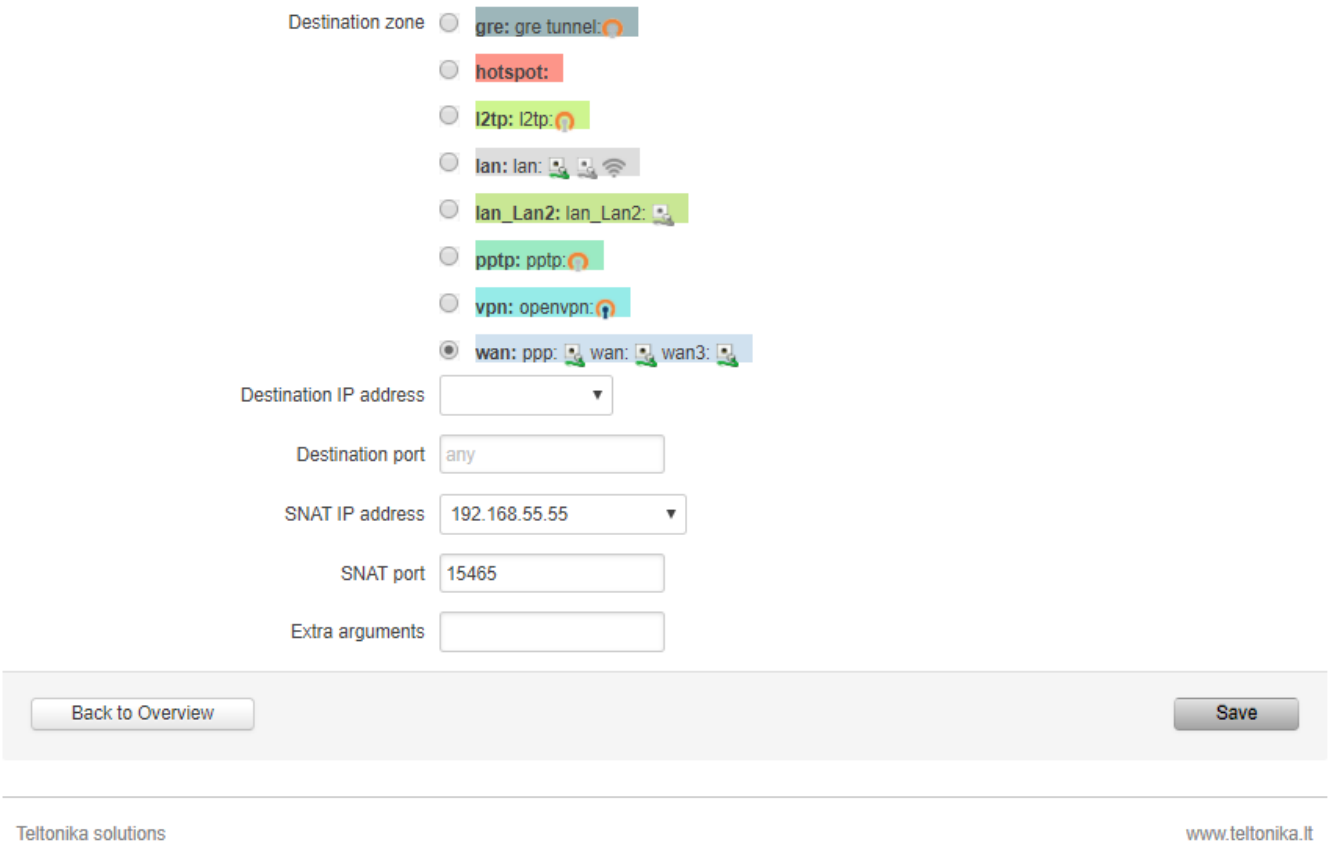


	Field Name	Possible values	Explanation
1.	Name	Rule's name	Name of the rule, used for easier management
2.	Protocol	TCP/UDP/Any/ICMP/Custom	Protocol of the packet that is being matched against traffic rules
3.	Source	GRE / HOTSPOT / L2TP / LAN / PPTP / VPN / WAN	Match incoming traffic from selected address family only
4.	Destination	GRE / HOTSPOT / L2TP / LAN / PPTP / VPN / WAN	Forward incoming traffic to selected address family only
5.	SNAT	Rewrite to source IP 192.168.55.55, port 15465	SNAT (Source Network Address Translation) rewrites packet's source IP address and port
6.	Enable	Enable/Disable	Makes the rule active/inactive

You can configure firewall source NAT rules, by clicking the **edit** button next to them:



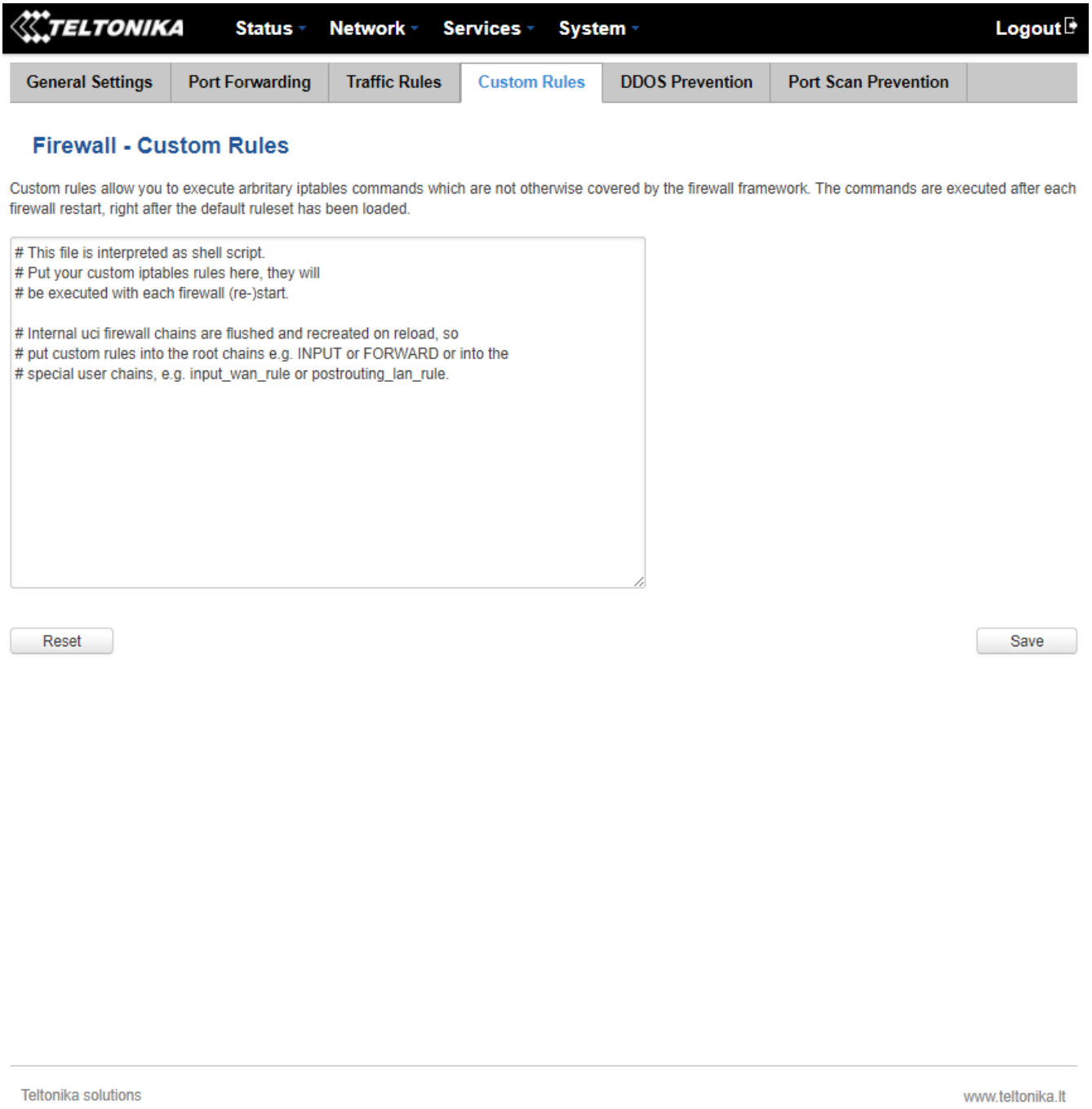
	Field Name	Sample value	Explanation
1.	Name	Rule's name	Name of the rule, used for easier management
2.	Protocol	All protocols / TCP / UDP / TCP+UDP / ICMP / Custom	Protocol of the packet that is being matched against traffic rules
3.	Source zone	Any zone / gre / hotspot / l2tp / lan / pptp / vpn / wan	Match incoming traffic from the selected zone only
4.	Source MAC address	Any MAC address	Match incoming traffic from these MACs only
5.	Source address	Any IP address or range	Match incoming traffic from this IP or range only
6.	Source port	Any port	Match incoming traffic originating from the given source port or port range on the client host only



7.	Destination zone	Device/Any zone/LAN/VPN/WAN	Match forwarded traffic to the given destination zone only
8.	Destination address	Any IP address	Match forwarded traffic to the given destination IP address or IP range only
9.	Destination port	Any port	Match forwarded traffic to the given destination port or port range only
10.	SNAT IP address	Any IP address	Rewrite matched traffic to the given IP address
11.	SNAT port	Any 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!

7.6.6 Custom Rules

The custom rules page provides with 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.

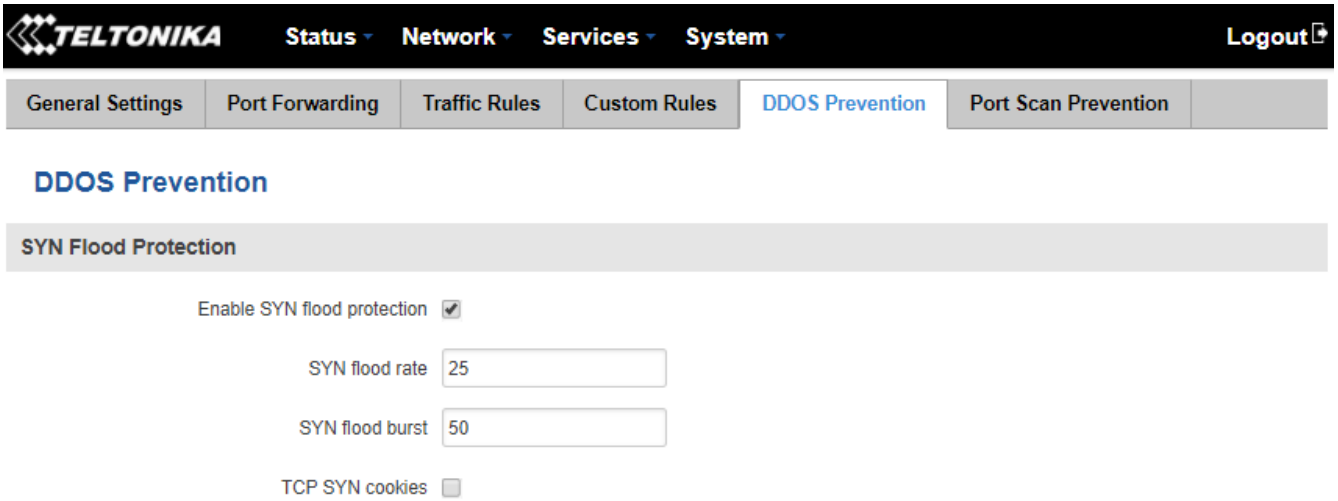


7.6.7 DDOS Prevention

The DDOS prevention page allows you to set up protections from various types of DDOS attacks. You will find information on all of these methods bellow.

7.6.7.1 SYN Flood Protection

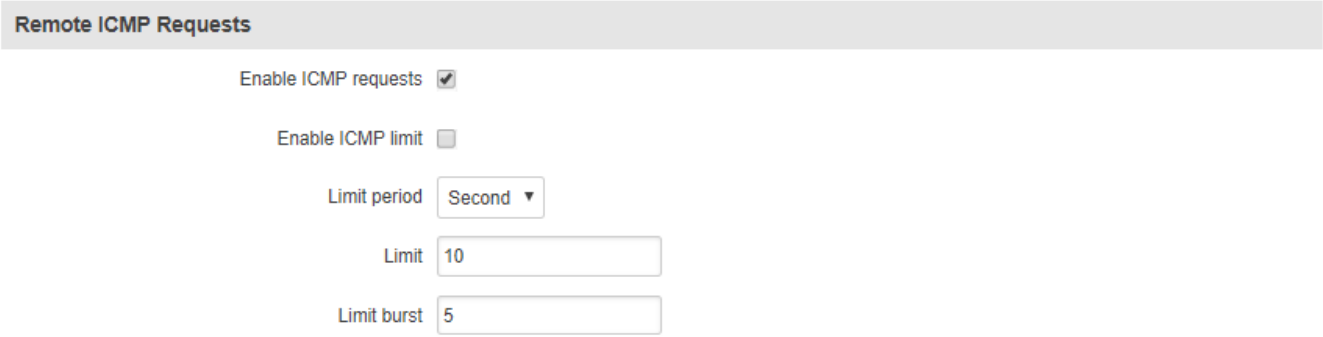
SYN Flood Protection allows you to protect yourself from attacks that exploit part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive. Essentially, with SYN flood DDOS, the offender sends TCP connection requests faster than the targeted machine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



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

7.6.7.2 Remote ICMP requests

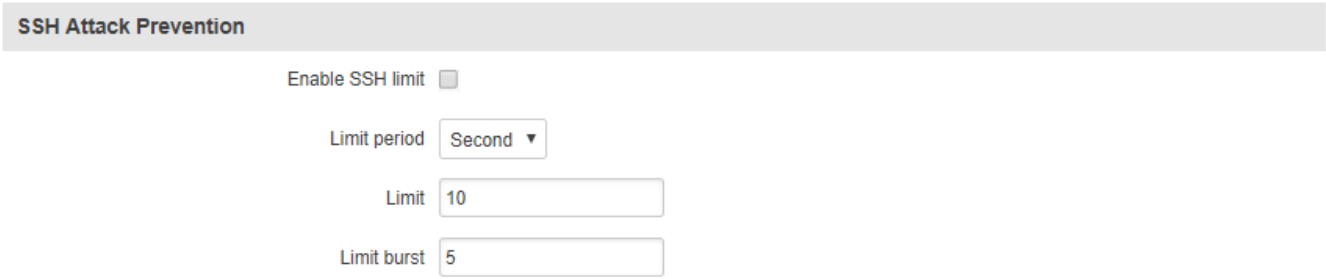
Some attackers use ICMP echo request packets directed to IP broadcast addresses from remote locations to generate denial-of-service attacks.



	Field Name	Possible values	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 ICMP echo-request period limit.
4.	Limit	Integer numbers	Maximum ICMP echo-request number during the period
5.	Limit burst	Integer numbers	Indicate the maximum burst before the above limit kicks in

7.6.7.3 SSH Attack Prevention

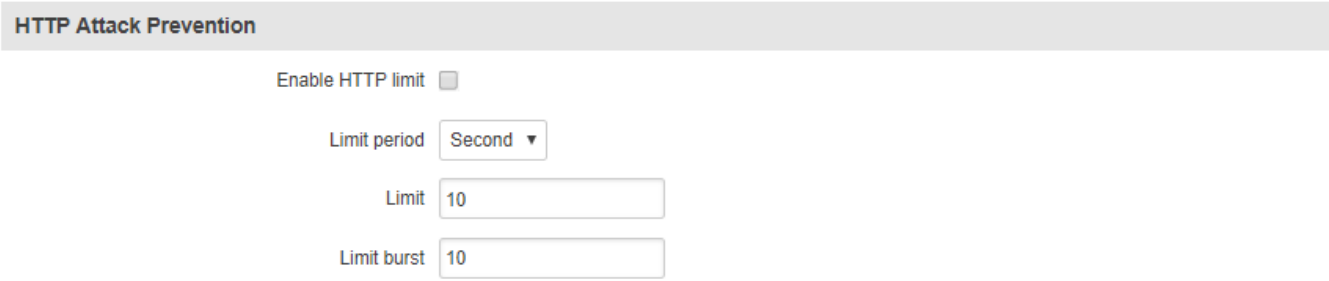
Prevent SSH (allows a user to run commands on a machine's command prompt without them being physically present near the machine) attacks by limiting connections in a defined period.



	Field Name	Possible values	Explanation
1.	Enable SSH limit	Enable/Disable	Enable SSH connection limit in a selected period
2.	Limit period	Second/Minute/Hour/Day	The period in which SSH connections are to be limited
3.	Limit	Integer numbers	Maximum SSH connections during the set period
4.	Limit burst	Integer numbers	Indicate the maximum burst before the above limit kicks in

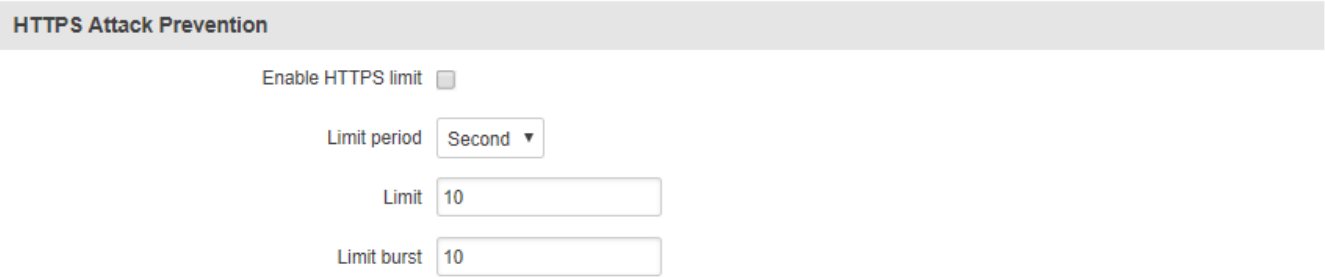
7.6.7.4 HTTP Attack Prevention

An 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.



	Field Name	Possible values	Explanation
1.	Enable HTTP limit	Enable/Disable	Limits HTTP connections per set period of time
2.	Limit period	Second/Minute/Hour/Day	The period in which HTTP connections are to be limited
3.	Limit	Integer number	Maximum HTTP connections during the set period
4.	Limit burst	Integer number	The maximum burst before the above limit kicks in

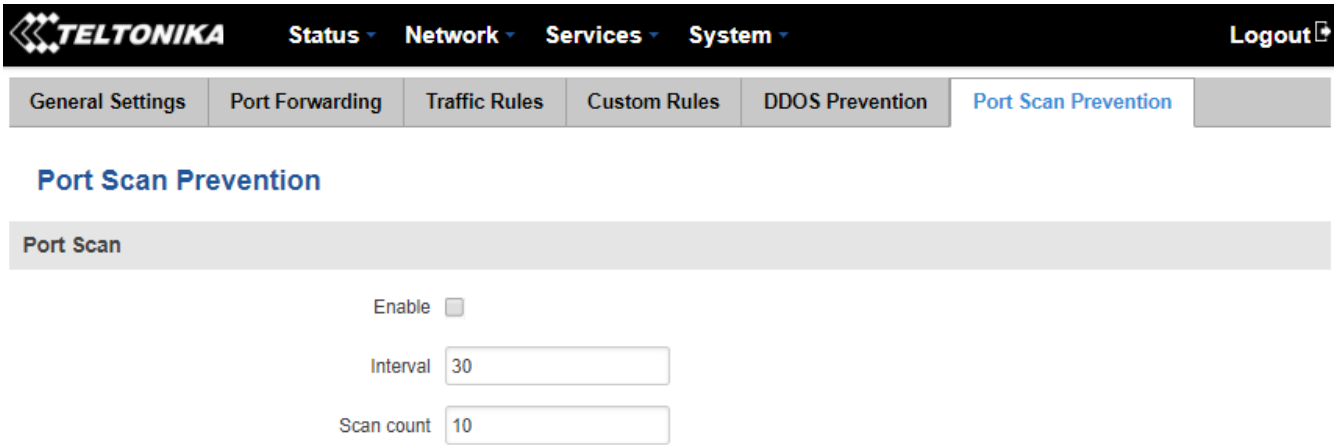
7.6.7.5 HTTPS Attack Prevention



	Field Name	Possible values	Explanation
1.	Enable HTTPS limit	Enable/Disable	Limits HTTPS connections per set period of time
2.	Limit period	Second/Minute/Hour/Day	The period in which HTTPS connections are to be limited
3.	Limit	Integer number	Maximum HTTPS connections during the set period
4.	Limit burst	Integer number	The maximum burst before the above limit kicks in

7.6.8 Port Scan Prevention

7.6.8.1 Port Scan



	Field Name	Possible values	Explanation
1.	Enable	Enable/Disable	Enables port scan prevention
2.	Interval	10-60	Time interval in seconds in which port scans are counted
3.	Scan count	5-65534	How many port scans before blocked

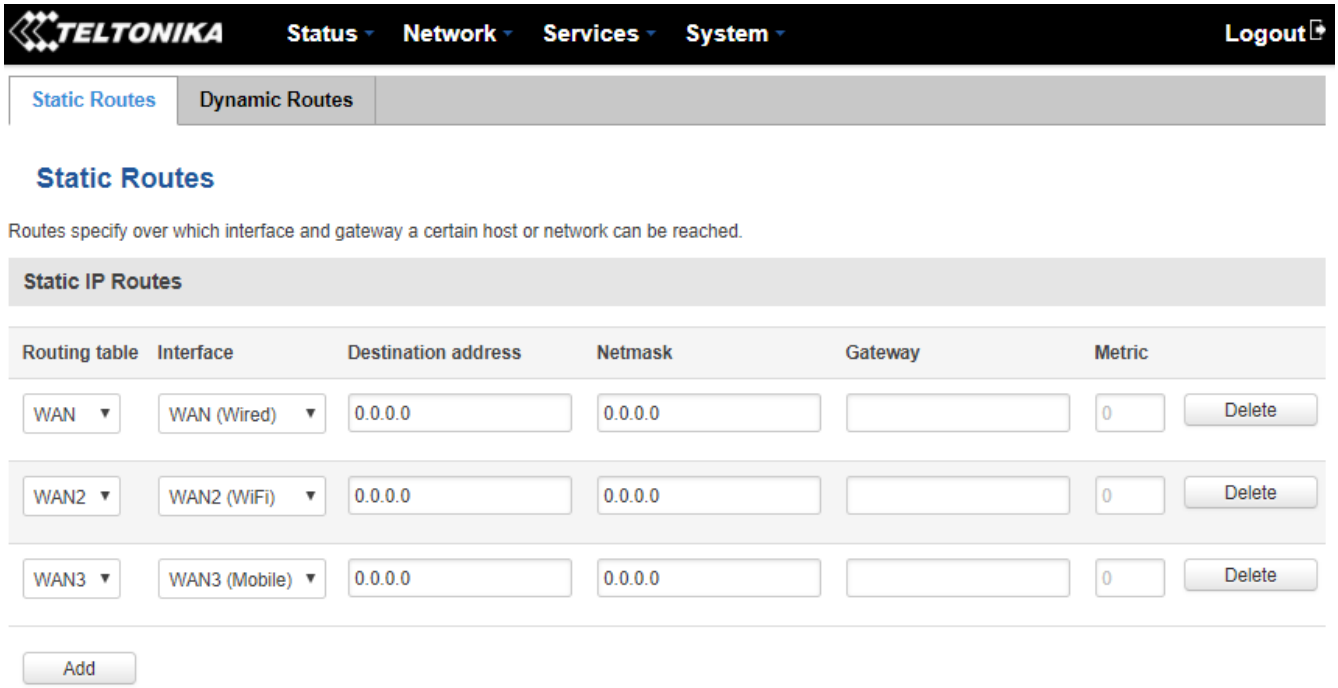
7.6.8.1 Defending type

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

7.7 Routing

7.7.1 Static Routes

Static routes specify over which interface and gateway a certain host or network can be reached. In this page you can configure your own custom routes.



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

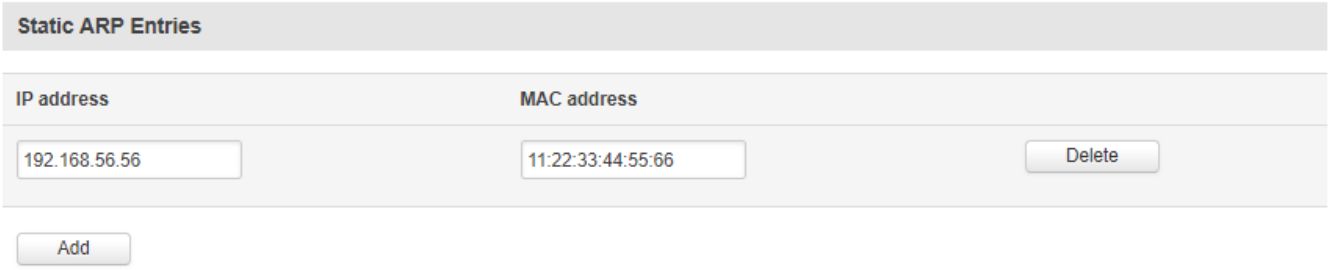
***Additional notes on Destination & Netmask:**

You can define a rule that applies to a single IP like this: Destination - **some IP**; Netmask - **255.255.255.255**. Furthermore, you can define a rule that applies to a segment of IPs like this: Destination – 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 the 192.168.55.0 - 192.168.55.255 range
192.168.55.240	255.255.255.240	192.168.55.240 - 192.168.55.255
192.168.55.161	255.255.255.0	192.168.55.0 - 192.168.55.255
192.168.0.0	255.255.0.0	192.168.0.0 - 192.168.255.255

7.7.1.1 Static ARP entries

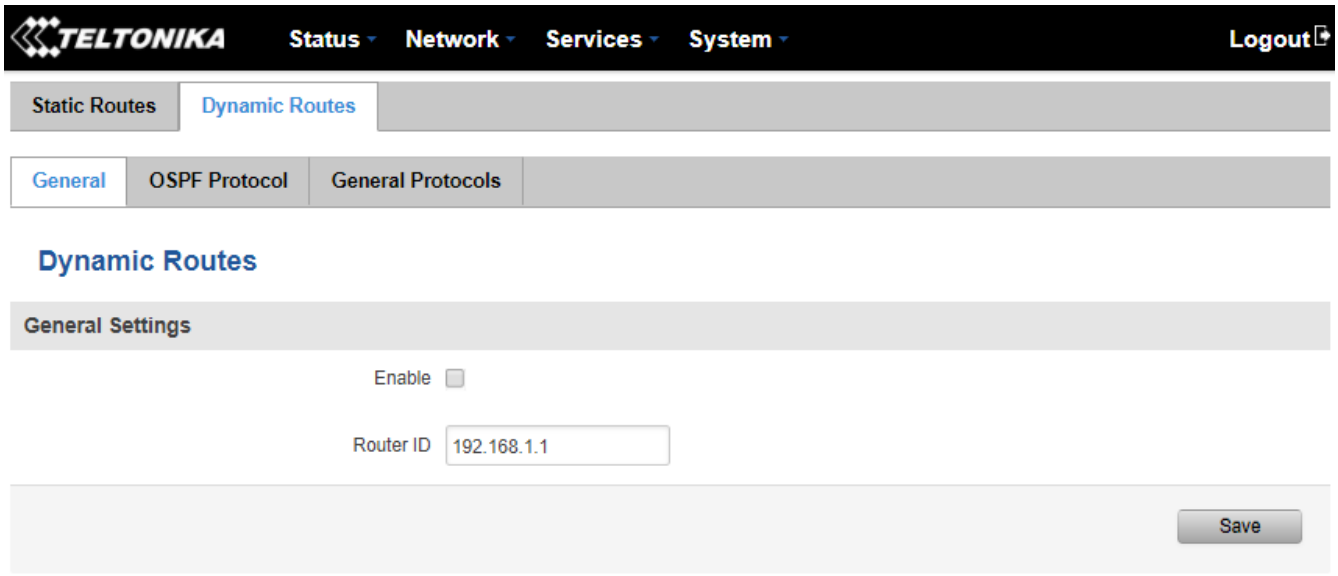
Static ARP entries are used to bind a MAC address to a specific IP address. For example, if you want some device to get the same IP every time it connects to the router, you can create a Static ARP entry by binding that device's MAC address to a desired IP address. The router will then create an entry in the ARP table, which in turn make sure that that device will get the specified IP address every time.



7.7.2 Dynamic Routes

7.7.2.1 General

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



	Field name	Value	Explanation
1.	Enable	Enable/Disable	Enable dynamic routes
2.	Router ID	192.168.1.1	Router's ID

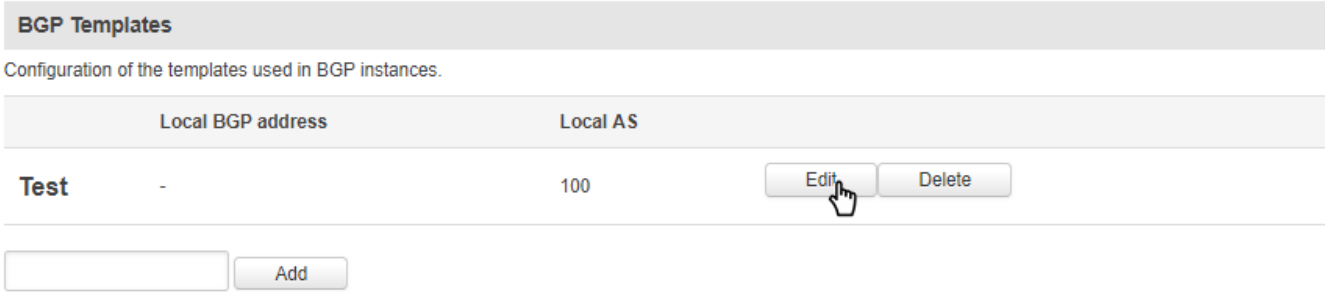
7.7.2.2 BGP Protocol

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet. The protocol is often classified as a path vector protocol but is sometimes also classed as a distance-vector routing protocol. The Border Gateway Protocol makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator and is involved in making core routing decisions.

7.7.2.2.1 BGP Templates

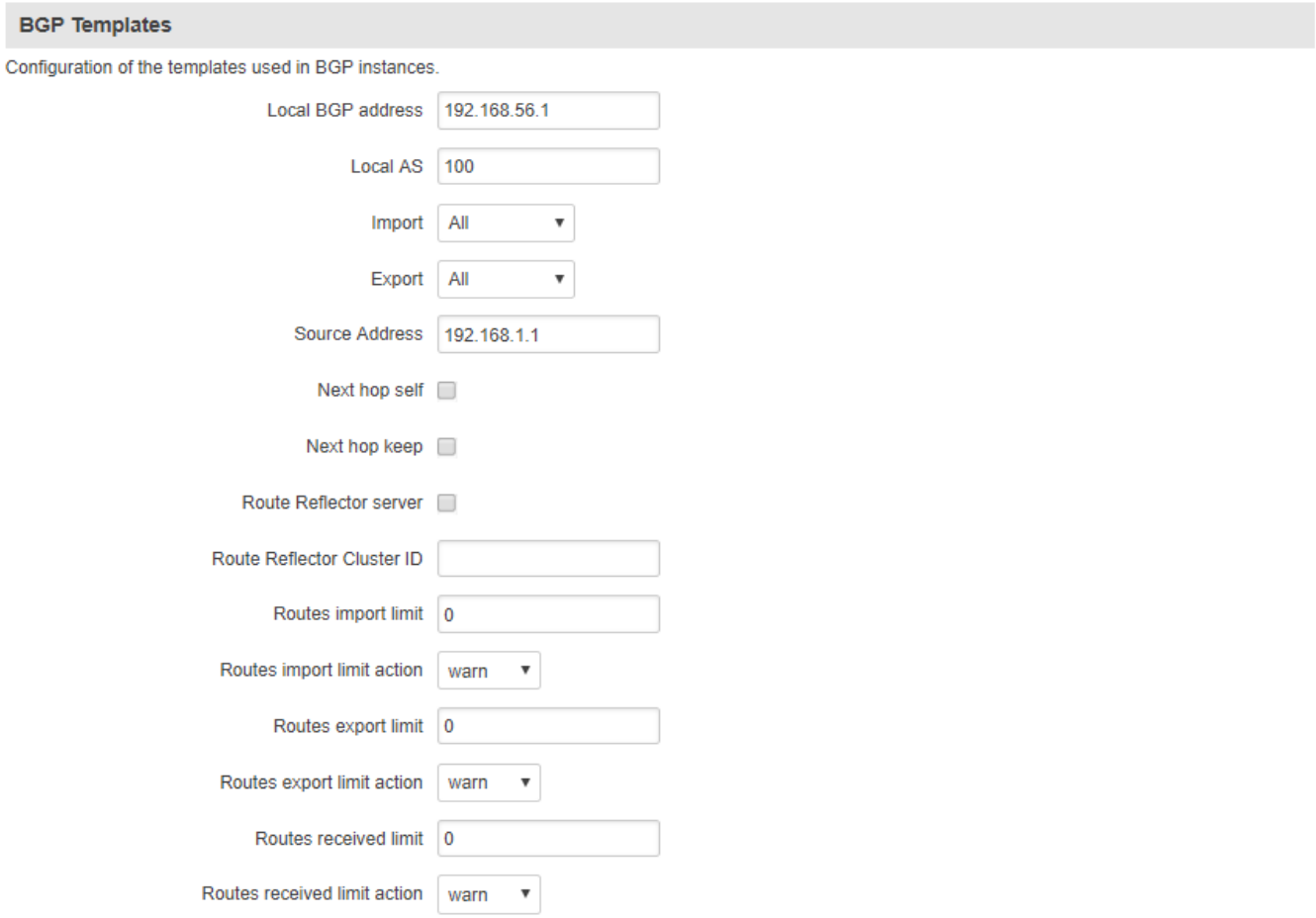
You can create a BGP template by typing in a name (BGP template names can only contain letters) in the text bar and pressing the "Add" button next to it.

This action will create a new template with your given name. You can then start configuring your BGP template by pressing the "Edit" button next to it.



After this you will be redirecting to the BGP protocol's configuration window where you can configure your new BGP protocol in detail.

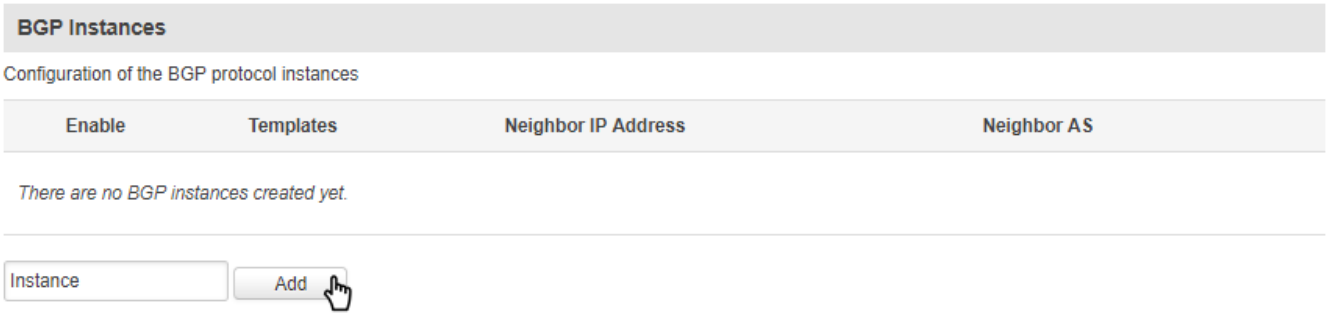
7.7.2.2.2 Bird4 BGP protocol's configuration



	Field Name	Value	Explanation
1.	Local BGP address	192.168.56.1	
2.	Local AS	100	
3.	Import	All	
4.	Export	All	
5.	Source address	192.168.1.1	
6.	Next hop self	Enabled/Disabled	
7.	Next hop keep	Enabled/Disabled	
8.	Route Reflector server	Enabled/Disabled	
9.	Route Reflector Cluster ID		
10.	Routes import limit	0	
11.	Routes import limit action	Warn	
12.	Routes export limit	0	
13.	Routes export limit action	Warn	
14.	Routes received limit	0	
15.	Routes received limit action	warn	

7.7.2.3 BGP Instances

You can create a BGP instance by typing in a name (BGP instance names can only contain letters) in the text bar and pressing the "Add" button next to it.



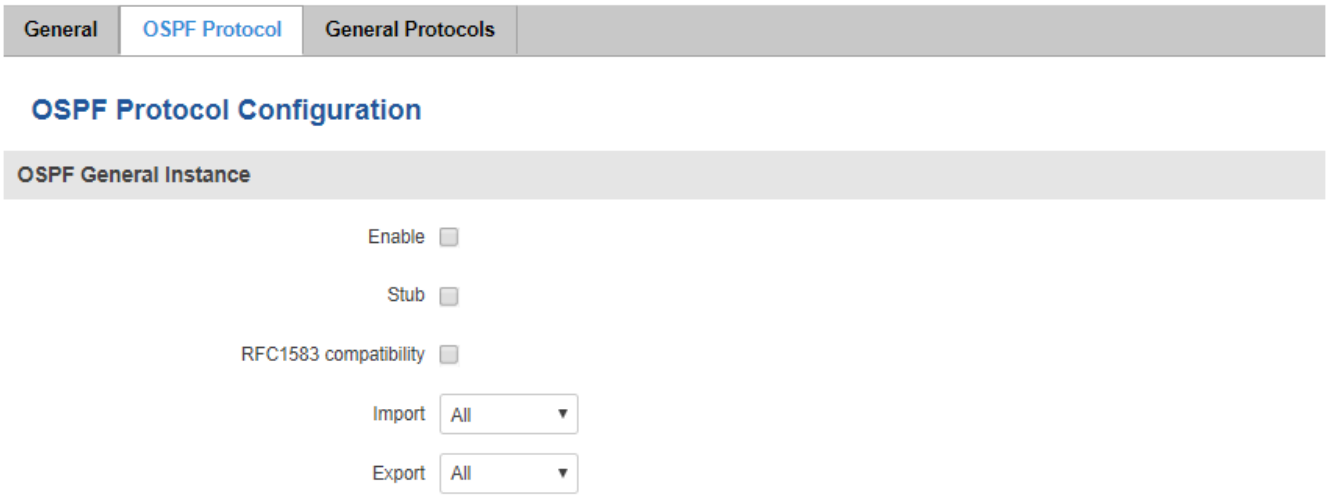
Your instance is now created and should be visible in the BGP Instances tab.

	Field name	Value	Explanation
1.	Enable	Enable/Disable	Enable or disable the BGP instance
2.	Template	Test	Select which BGP template the instance will use
3.	Neighbour IP Address	192.168.90.66	IP address of a neighboring device
4.	Neihgbour AS	100	Neighboring device's autonomous system

7.7.2.4 OSPF Protocol

Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4.

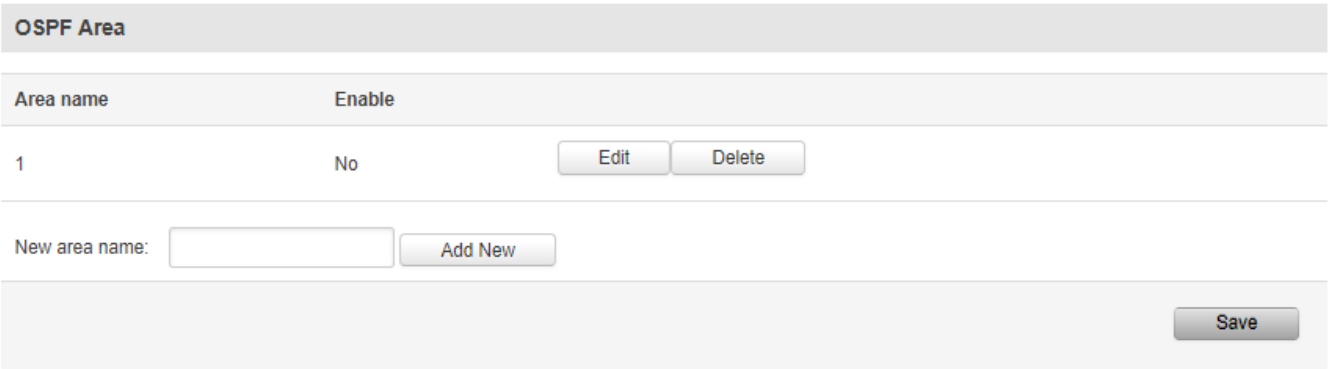
7.7.2.4.1 OSPF General Instance



	Field name	Value	Explanation
1.	Enable	Enable/Disable	Enables OSPF protocol
2.	Stub	Enable/Disable	Changes the area to stub
3.	RFC1583 compatibility	Enable/Disable	Enables OSPF compatibility with RFC1583 specification
4.	Import	All/None/custom	Set if the protocol must import routes
5.	Export	All/None/custom	Set if the protocol must export routes

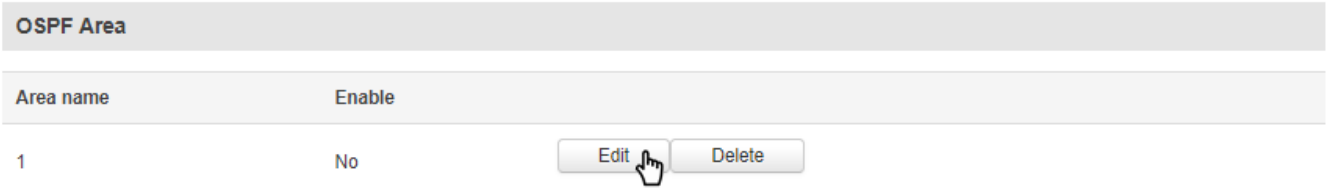
7.7.2.4.2 OSPF Area

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

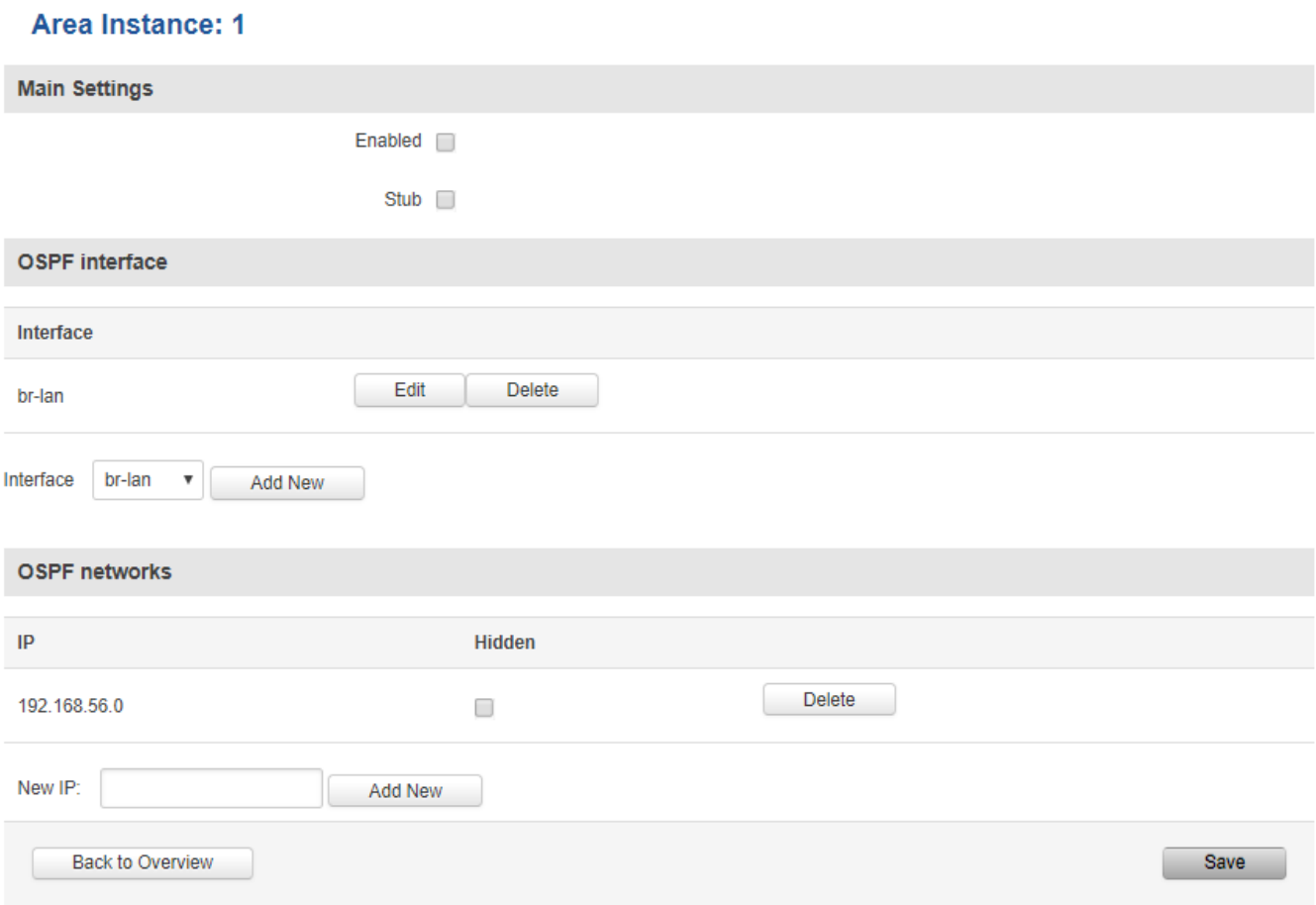


	Field name	Value	Explanation
1.	Area name	1	OSPF area's name. Area instance name must be a number
2.	Enable	Yes/No	Enable/disable OSPF area

To configure the OSPF area, press the "edit" button located next to it.



This action will redirect you to the OSPF are configuration window.



	Field name	Value	Explanation
1.	Enabled	Enable/Disable	Enable or disable the OSPF area
2.	Stub	Enable/Disable	Enable/disable stub
3.	Interface	br-lan	An interface that the area will use
4.	New IP	192.168.56.0	IP addresses of the OSPF networks that are a part of the OSPF area

7.7.2.2.2.1 OSPF Interface

Interface: Brlan_1

Main Settings

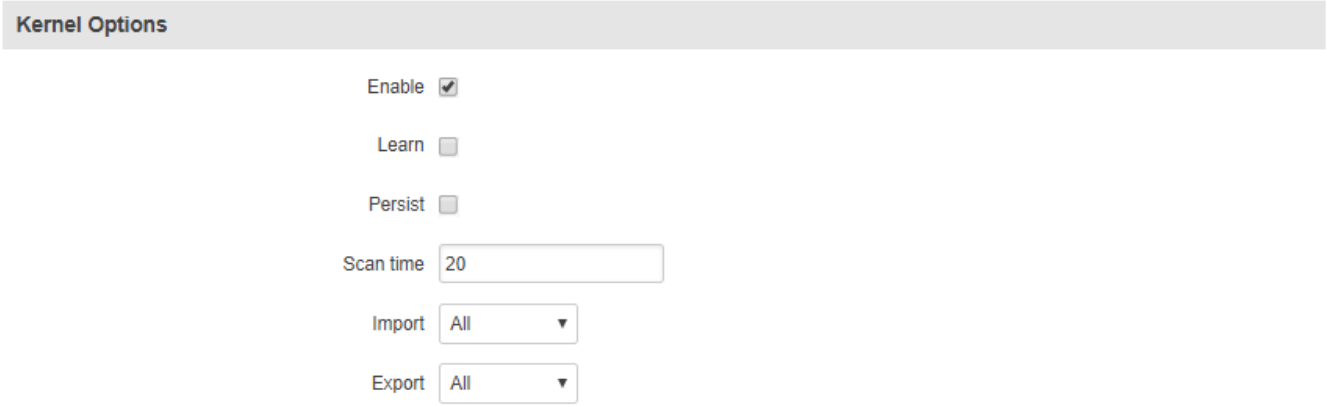
Cost	10
Hello	10
Poll	20
Retransmit	5
Priority	1
Wait	40
Dead count	3
Dead	30
RX buffer	Normal
TX length	100
Type	Broadcast
Authentication	None

	Field Name	Value	Explanation
1.	Cost	10	
2.	Hello	10	
3.	Poll	20	
4.	Retransmit	5	
5.	Priority	1	
6.	Wait	40	
7.	Dead count	3	
8.	Dead	30	
9.	RX buffer	Normal	
10.	TX length	100	
11.	Type	Broadcast	
12.	Authentication	None	

7.7.2.5 General Protocols

The general protocols window lets you configure Kernel Options, Device Options and Static Routes

7.7.2.5.1 Kernel Options

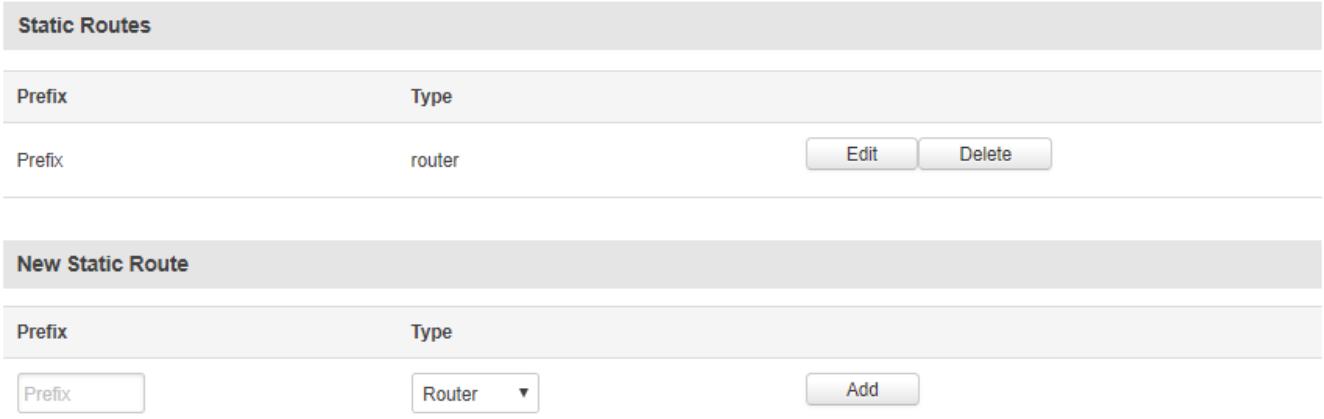


	Field name	Value	Explanation
1.	Enable	Enable/Disable	Enable/Disable settings
2.	Learn	Enable/Disable	Enables route learning
3.	Persist	Enable/Disable	Store routes. After a restart, routes will still be configured
4.	Scan time	20	Time between scans
5.	Import	All	Set if the protocol must import routes
6.	Export	All	Set if the protocol must export routes

7.7.2.5.2 Device Options

	Field name	Value	Explanation
1.	Enable	Enable/Disable	If checked the protocol will not be configured
2.	Scan time	10	Time between scans

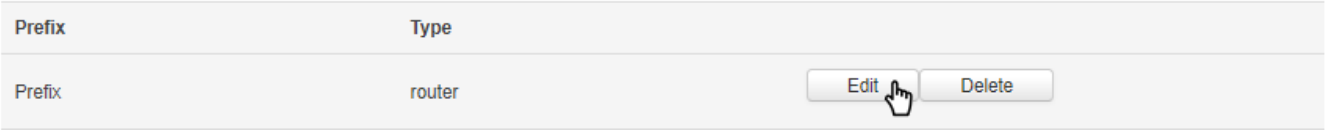
7.7.2.5.3 Static Routes



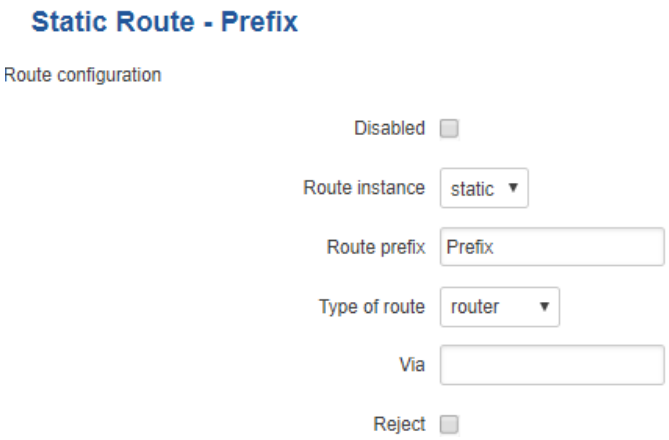
	Field name	Explanation
1.	Prefix	Protocol prefix of incoming or outgoing packet
2.	Type	Protocol type of incoming or outgoing packet
3.	Add	Add a new Static Route

7.7.2.2.2.2 Static Route configuration

You can configure your new static routes in detail by pressing the "Edit" button next to them.



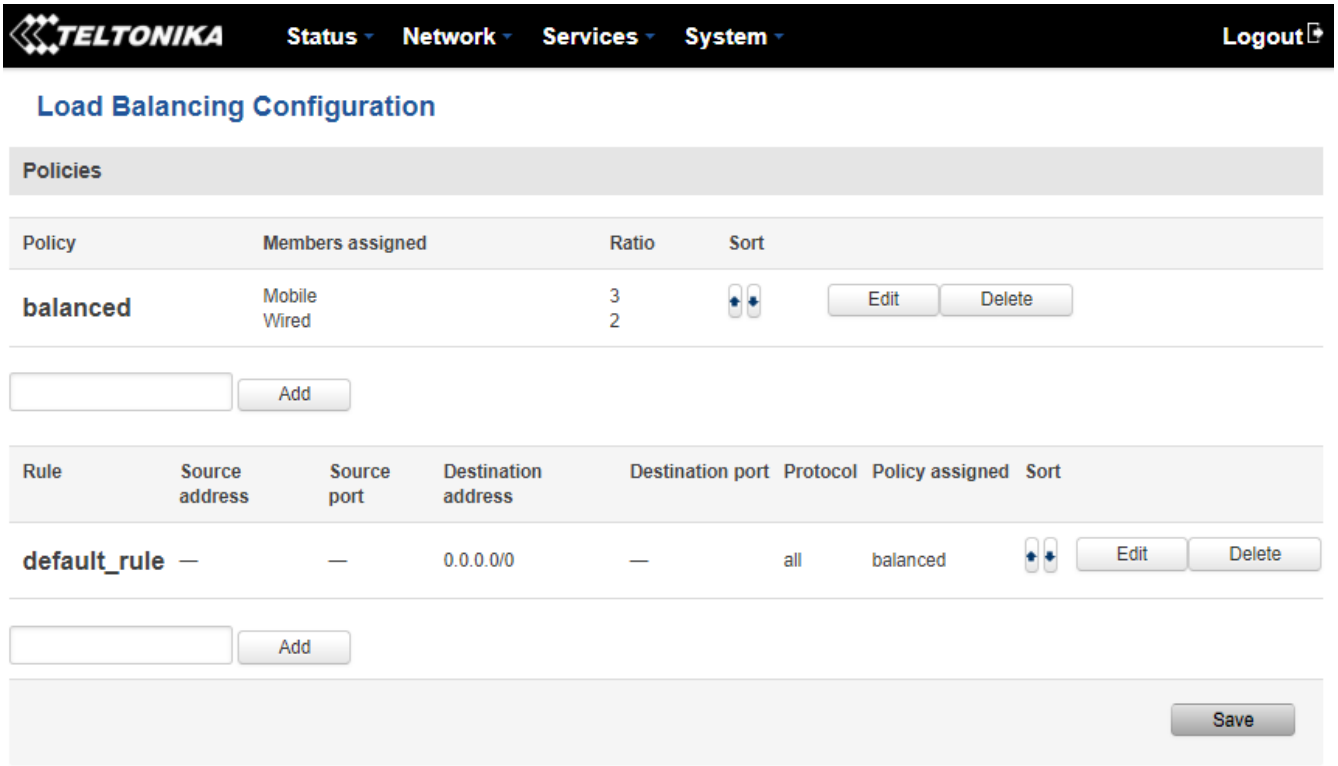
This action will redirect you to the Static Route's configuration window.



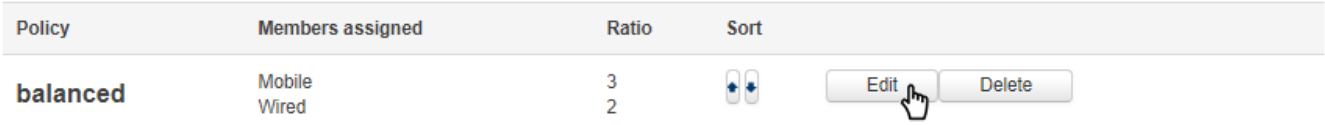
	Field name	Value	Explanation
1.	Disabled	Checked/Unchecked	If this option is true, the protocol will not be configured
2.	Route instance	Static	
3.	Route prefix	Prefix	
4.	Type of route	Router	
5.	Via		
6.	Reject	Checked/Unchecked	

7.8 Load Balancing

Load balancing lets users create rules that divide traffic between different interfaces.



To configure a rule, click the "edit" button located next to it.



This action will redirect you to the rule's configuration window.

Here you can define the ratio of each WAN interface. In the example above we can see that the mobile interface's ratio is 3, and the wired interface's ratio is 2. This means that $\frac{3}{5}$ of all traffic will go through the mobile interface, and $\frac{2}{5}$ will go through the wired interface. After you've finished configuring you Load Balancing rules, go the WAN section and activate Load Balancing for the desired interface.

8 Remote monitoring and administration

RUT955 supports multiple monitoring and administration possibilities. One can get router's information through SMS or using RMS (Remote Management System). Furthermore, some system related parameters can be obtained using MQTT or MODBUSD publisher services. Instruction on how to use them can be found in 9.19 and 9.20 chapters of this document respectively. The main focus is on parameters, which change from time to time, like signal strength, operator's name (it is quite common to change operator's name in countries where inner roaming is used) or module temperature. Although it is also possible to read static values, like MAC address, router's serial number and many others. The access to the mentioned parameters is implemented in both MODBUSD and MQTT publisher applications. Apart from getting parameters, MODBUSD can also be used to set some system related parameters, for example, it can be used to change the value of the digital output.

Some applications, like MQTT publisher or RMS, allow monitoring or administrating several routers at once. It is a very useful functionality when you want to change the same parameters on more than one router at once. RMS shares some similarities with SSH (Secure Shell) and one of RMS features is to allow SSH access to a remote router. There is no separate chapter about RMS in this manual, because the interface of RMS is very intuitive and user friendly. You can access RMS by using your browser with a supplied username and a password at http://rms.teltonika.lt

By sending SMS messages to the router the user can execute various commands like reboot, switch Wi-Fi on or off and many others. With each SMS the user needs to specify the router's administrator password. This is done for authentication purposes. The list of commands that may be executed through SMS is limited. Full list of commands can be found at Services->SMS Utilities of the router's WEB page. More information on how to manage the router using SMS can be found in chapter 9.8 of this document.

Another interesting router monitoring solution is SNMP (Simple Network Management Protocol). By not going into deep detail about this protocol, it is another manner to monitor router parameters. It allows the user to check the current operator, modem model and other router parameters. Compared to other applications and services, only SNMP has ability to inform the user about the occurrence of specific events (called traps) in the system. The main drawback of this protocol is that it does not allow the user to change anything. You can read more about SNMP in chapter 9.9.

Apart from the services mentioned earlier, there is one service, which is used only for communication between the router and an Android type device (phones, etc.). It is called JSON-RPC and it allows the user to set or get various parameters of the system. JSON-RPC provides users with the possibility to execute the same commands as they would through SSH. To sum up, this approach opens up wide possibilities in communication between the router and an Android device. However, there is no separate topic about JSON-RPC in this manual, because this type of communication is generally not for end-user use.

Each approach has its advantages and disadvantages. In some situations MQTT publisher works better than MODBUSD, while in others MODBUSD will be the better choice. The most versatile manner of system monitoring and administration is through SSH. SSH provides complete control of the router. The user can execute commands, write shell scripts and do many other things. In such case, the user only needs an application to connect to the router through SSH. The most popular application used in Windows type operating systems is called Putty. If one is trying to connect to the router from a UNIX type operating system, all that is needed is the hostname, username (in this case – root) and password.

Sometimes the use of SSH is not necessary, so other more conservative services/applications are used. The complete list of applications and services that can be used for router administration and monitoring is given below. It can be seen that all applications, except MQTT publisher and SNMP, support setting/getting of some system related parameters.

	Application	Can obtain parameters	Can set parameters
1.	MQTT publisher	•	o
2.	MODBUS daemon	•	•
3.	SSH	•	•
4.	RMS	•	•
5.	SMS	•	•
6.	SNMP	•	o
7.	JSON-RPC	•	•
8.	TR-069	•	•

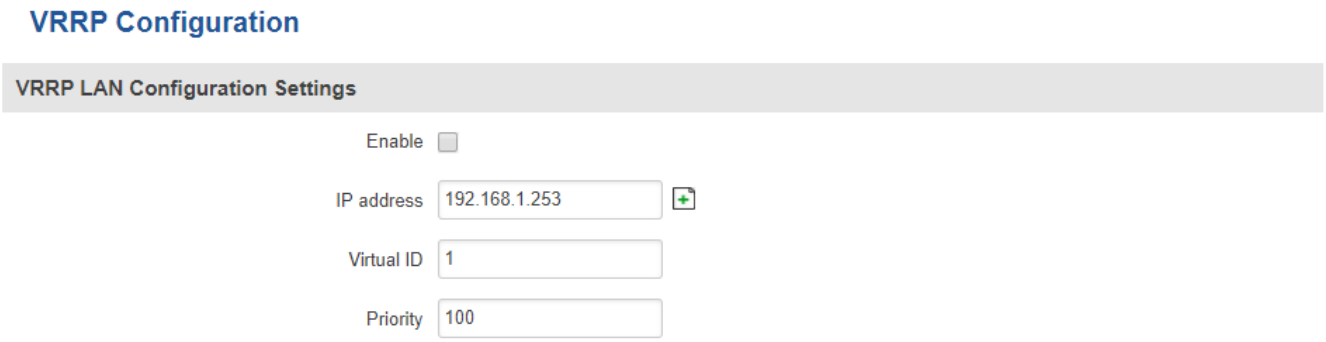
To summarize, RUT955 provides several solutions for router management. Each user can choose what solution to use. If the required functionality is not supported be a particular service, the user can combine several applications, for example, use MQTT publisher along with SNMP. Finally, if a user has special needs, he can write shell scripts and execute them via SSH or use JSON-RPC.

9 Services

9.1 VRRP

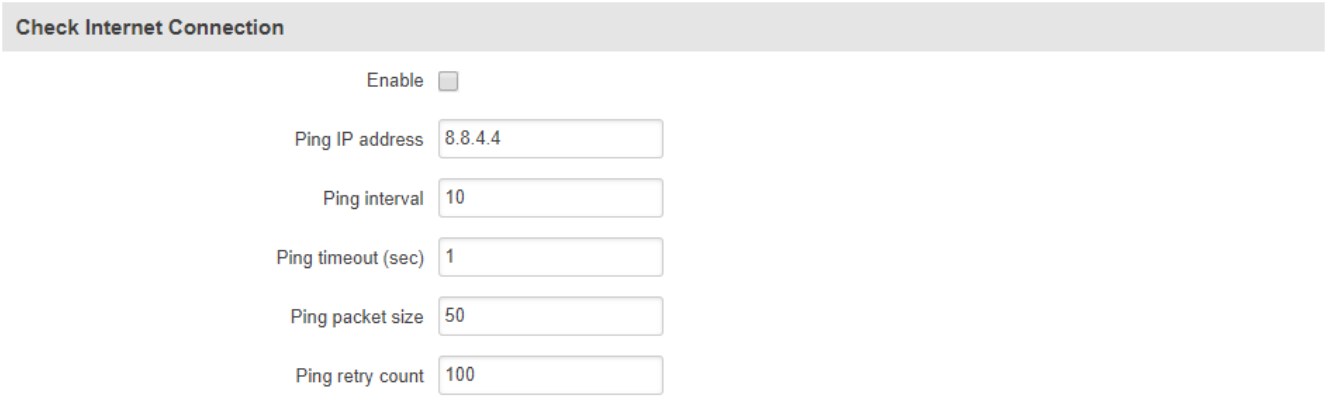
The Virtual Router Redundancy Protocol (VRRP) is a computer networking protocol that provides for automatic assignment of available Internet Protocol (IP) routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork.

9.1.1 VRRP LAN Configuration Settings



	Field name	Sample	Explanation
1.	Enable	Enable/Disable	Enable or disable VRRP for LAN
2.	IP address	192.168.1.253	Virtual IP address for LAN's VRRP cluster
3.	Virtual ID	1	Routers with same IDs will be grouped in the same VRRP cluster, range [1-255]
4.	Priority	100	The router with the highest priority value on the same VRRP cluster will act as a master, range [1-255]

9.1.2 Check Internet connection

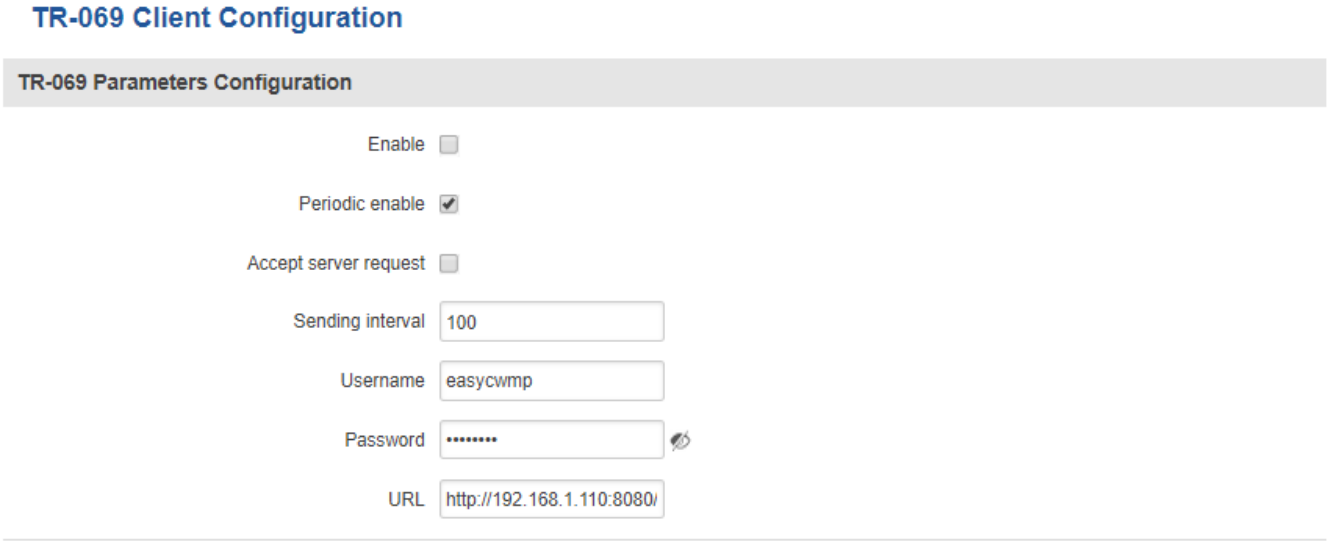


	Field name	Possible values	Explanation
1.	Enable	Enable/Disable	Enable WAN's connection monitoring
2.	Ping IP address	8.8.4.4	A host to send ICMP packets to
3.	Ping interval	Any integer number	Time interval in seconds between two Pings
4.	Ping timeout (sec)	1 – 9999	Response timeout value
5.	Ping packet size	0 – 1000	ICMP packet's size
6.	Ping retry count	1 – 9999	Failed Ping attempt count before determining that the connection is lost

9.2 TR-069

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

9.2.1 TR-069 Parameters Configuration

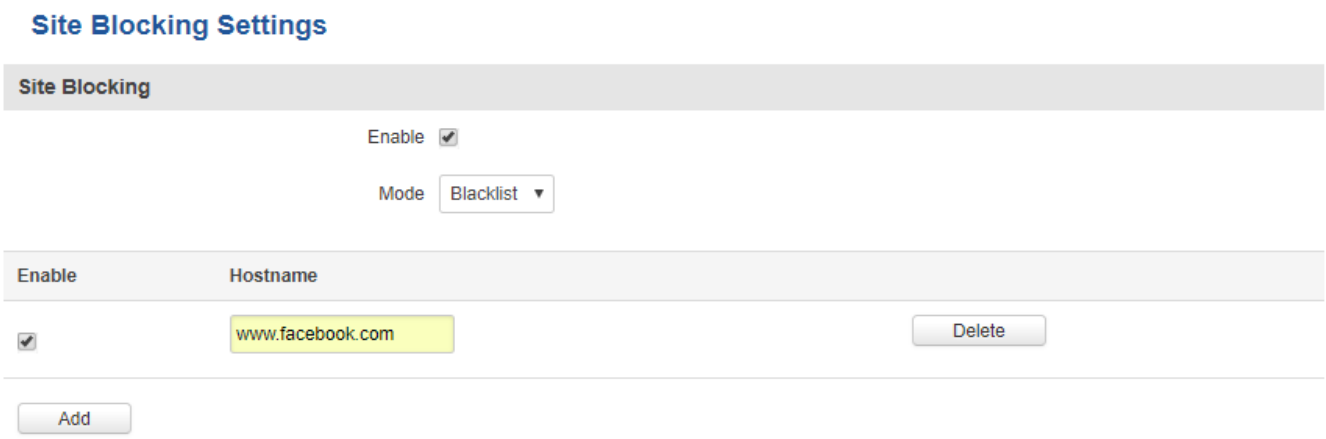


	Field name	Possible values	Explanation
1.	Enable	Enabled/Disabled	Enable TR-069 client
2.	Periodic enable	Enabled/Disabled	Enable periodic transmissions of data to server
3.	Accept server request	Enabled/Disabled	Check to accept connection requests from server
4.	Sending interval	60-9999999	Periodic data transmission interval
5.	User name	admin	User name used for authentication on a TR-069 server
6.	Password	********	Password used for authentication on a TR-069 server
7.	URL	http://192.168.1.110:8080/	TR-069 server's URL address

9.3 Web filter

9.3.1 Site Blocking

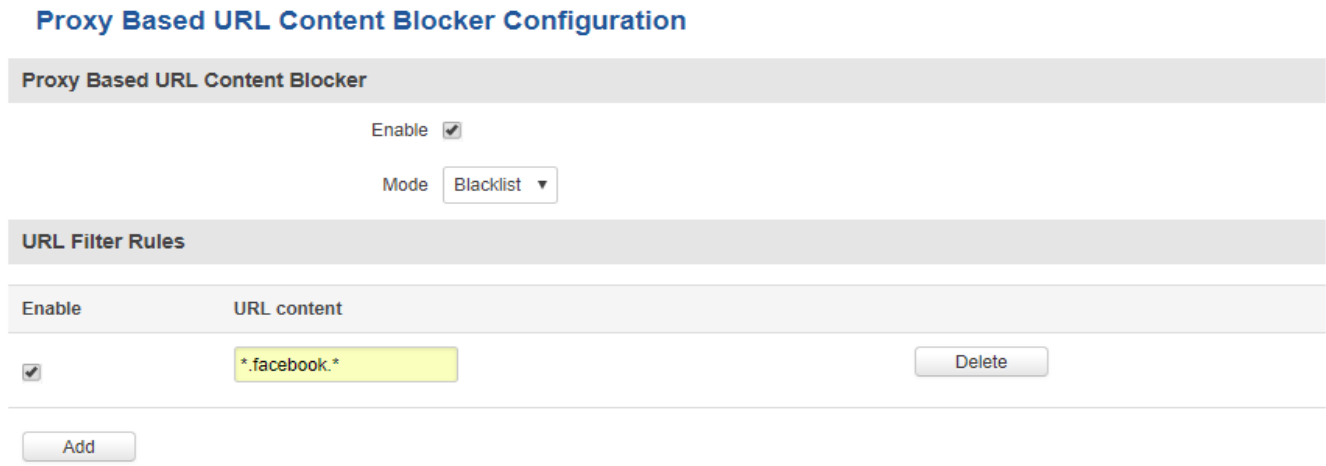
Site Blocking provides you with the possibility to block unwanted websites.



	Field name	Possible values	Explanation
1.	Enable	Enable/Disable	Enable host name based website 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	Enable block/allow for that specific entry
4.	Host name	www.facebook.com	Block/allow site with this hostname

9.3.2 Proxy Based Content Blocker

Proxy Based Content Blocker works in a similar manner to Site Blocking, except with Content Blocker you have the ability to filter out content with more versatility.



	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 a URL on the list and block everything else. Blacklist - block every part of a URL on the list and allow everything else
3.	URL content	*.facebook.*	Block/allow any URL containing this string. The asterisk can stand for anything, e.g., www.facebook.* would block www.facebook.net, www.facebook.com, www.facebook.org, etc.

9.4 MQTT

9.4.1 MQTT Broker

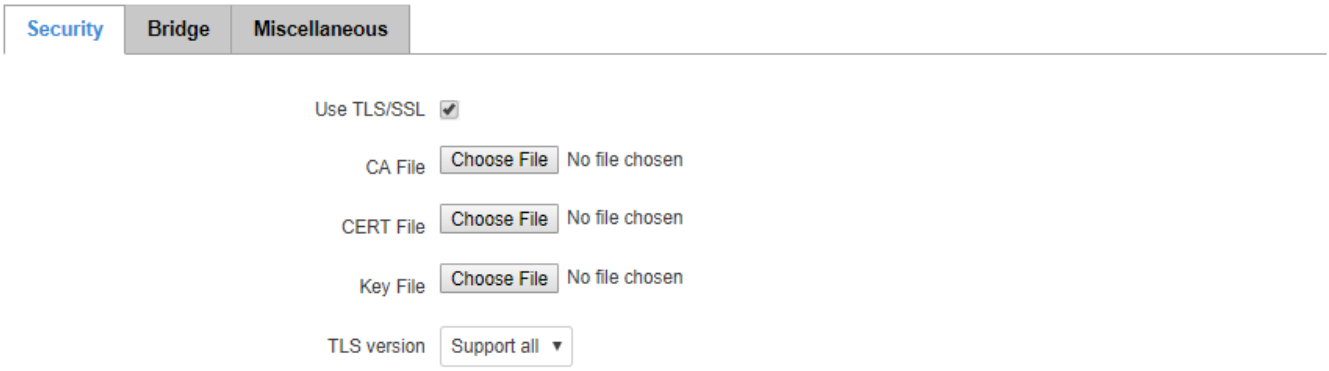
MQTT also known as MQ Telemetry Transport is a publisher-subscriber based messaging protocol for use on top of the TCP/IP protocol. It is designed to send short messages from one client (publisher) to another (subscriber) through brokers, which are responsible for message delivery to the end point. RUT955 routers support this functionality via an open source Mosquitto broker. The messages are sent this way: a client (subscriber) subscribes to a topic(s); a publisher posts a message to that specific topic(s). The broker then checks who is subscribed to that particular topic(s) and transmits data from the publisher to the subscriber.

The MQTT Broker can be enabled by checking ***Enable***. The Broker will then "listen" for connections on the specified ***Local port.*** In order to accept connections from WAN, you also need to check ***Enable Remote Access***.

	Field name	Possible Values	Explanation
1.	Enable	Enabled/Disabled	Enable MQTT Broker
2.	Local port	0 – 65535	Specify the local port that MQTT broker will listen to
3.	Enable remote access	Enabled/Disabled	If enabled, your MQTT broker will be reachable from remote (WAN) clients

9.4.1.1 MQTT Broker Security

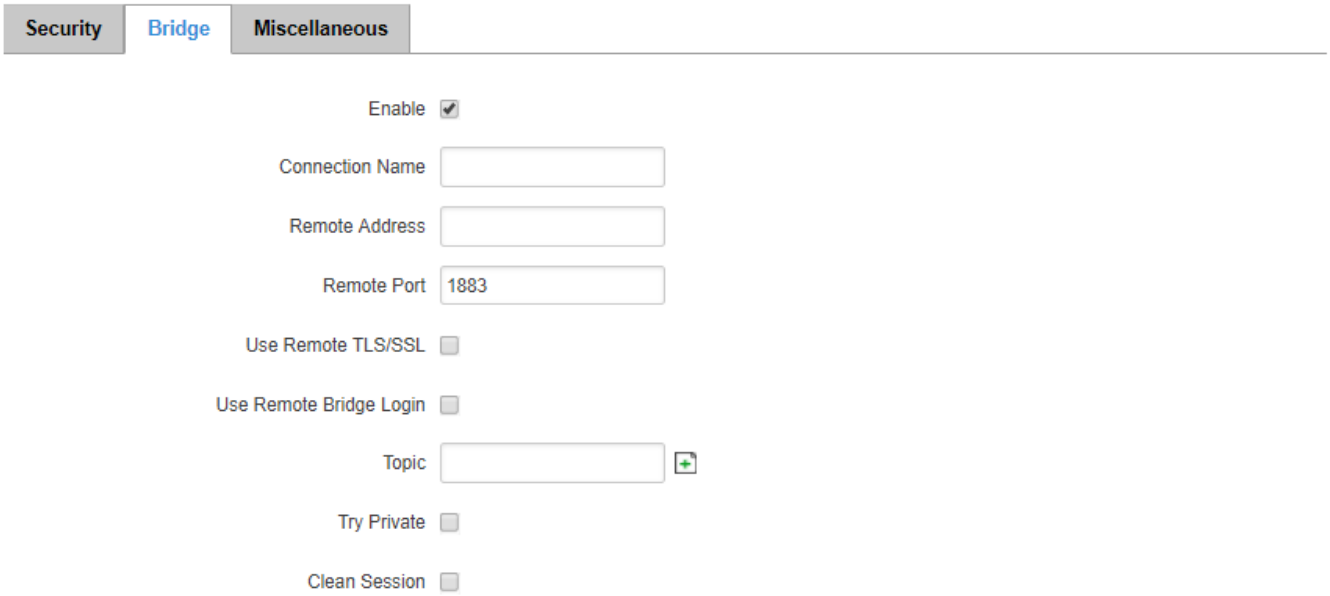
In order to use TLS/SSL authentication for client-broker-client communications, you must check ***Use TLS/SSL***. After that, additional settings will be displayed to the user as shown in the figure below.



	Field name	Sample	Explanation
1.	Use TLS/SSL	Checked/Unchecked	Enable TLS/SSL authentication for the broker
2.	CA File	-	Upload a CA file
3.	CERT File	-	Upload a CERT file
4.	Key File	-	Upload a Key file
5.	TLS version	tlsv1/tlsv1.1/tlsv1.2/Support all	Select which TLS version the broker will use

9.4.1.2 MQTT Bridge

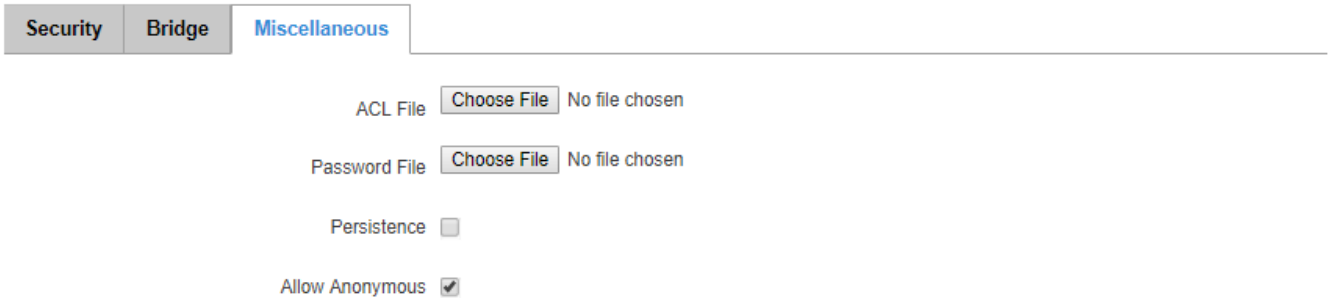
The MQTT Broker also supports a functionality called ***Bridge***. An MQTT Bridge is used for the communication of two MQTT Brokers. The window of Bridge parameters is presented below. Some of these are mandatory as they are needed to create a connection: ***Connection Name***, ***Remote Address*** and ***Remote Port***. For more information on MQTT Bridge parameters you can read the official mosquitto.conf manual page.



	Field name	Possible Values	Explanation
1.	Enable	Checked/Unchecked	Enable MQTT Bridge
2.	Connection Name	Any name	Name of the Bridge connection. Although this is used for easier management purposes, this field is mandatory
3.	Remote Address	Any remote IP address	Remote Broker's address
4.	Remote Port	0 – 65535	Select which port the broker should use to listen for connections
5.	Use Remote TLS/SSL	Checked/Unchecked	Select this to use TSL/SSL certificates of the remote broker
6.	Use Remote Bridge Login	Checked/Unchecked	Select this to use Remote login data. If checked, you will be prompted to enter a remote client ID, username and password
7.	Topic	Any existing Topic name	Enter the names of the Topics that your Broker will subscribe to
8.	Try Private	Checked/Unchecked	Check if the remote Broker is another instance of a daemon
9.	Clean Session	Checked/Unchecked	Check to discard session state after connecting or disconnecting

9.4.1.3 Miscellaneous

The last section of MQTT Broker parameters is called ***Miscellaneous***. It contains parameters that are related to neither Security nor Bridge.



	Field name	Sample	Explanation
1.	ACL File	-	The contents of this file are used to control client access to topics of the broker
2.	Password File*	-	The Password stores user names and corresponding passwords, used for authentication
3.	Persistence*	Checked/Unchecked	If checked, connection, subscription and message data will be written to the disk. Otherwise, the data is stored in the router's memory only
4.	Allow Anonymous	Checked/Unchecked	If checked, the Broker allows anonymous access

*** More on ACL and Password files can be read in the Mosquitto configuration manual.**

9.4.2 MQTT Publisher

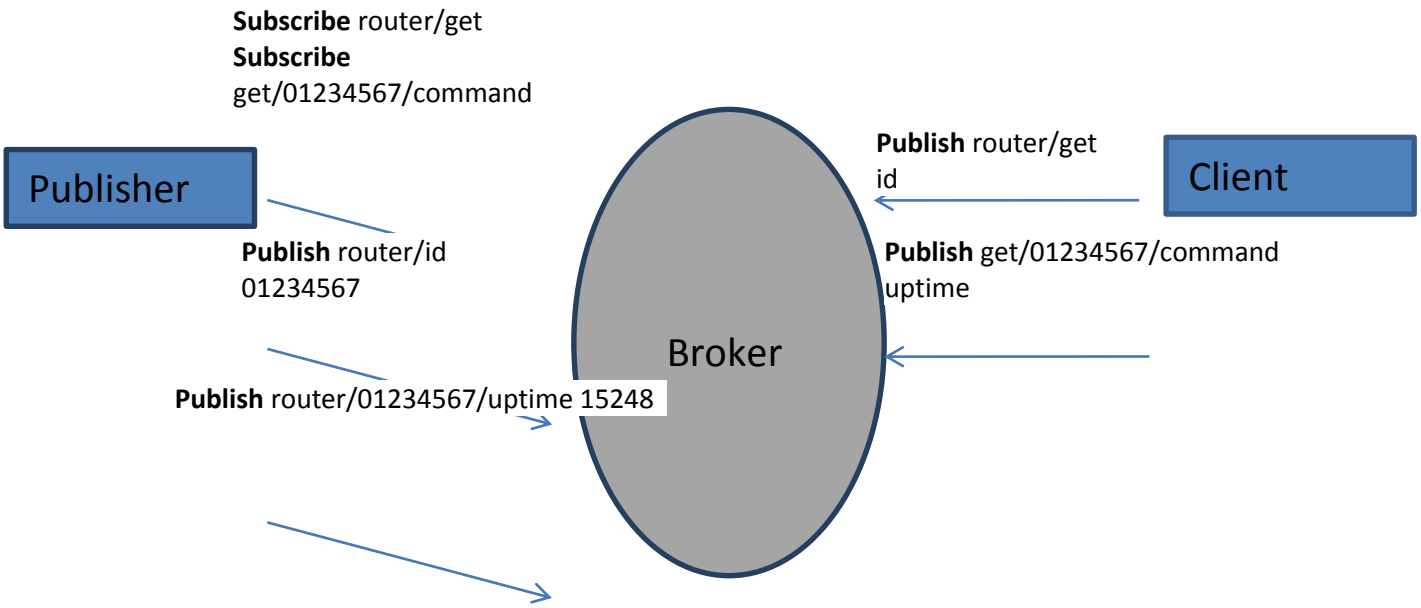
An MQTT Publisher is a client that sends messages to the Broker, who then forwards these messages to the Subscriber.

	Field name	Sample	Explanation
1.	Enable	Checked/Unchecked	Enables the router to act as an MQTT Publisher. The other MQTT Publisher parameters will appear only if this is checked
2.	Hostname	IP address or hostname	Broker's IP address or hostname
3.	Port	0 – 65535	Specify the port used for connecting to the Broker
4.	Username	Your username	Username used for authentication when connecting to the Broker
5.	Password	Your password	Password used for authentication when connecting to the Broker

The MQTT publisher can "publish" system parameters to the broker. The full list of system parameters that can be published is given in the table below.

Parameter name	Parameter description
temperature	Get temperature of the module in 0.1 degrees Celsius
operator	Get current operator's name
signal	Get signal strength in dBm
network	Get current network type (2G, 3G, 4G)
connection	Check if data connection is available
wan	Get WAN IP address
uptime	Get system uptime in seconds
name	Get router's name
digital1	Get value of digital input no. 1
digital2	Get value of digital input no. 2
analog	Get value of analog input

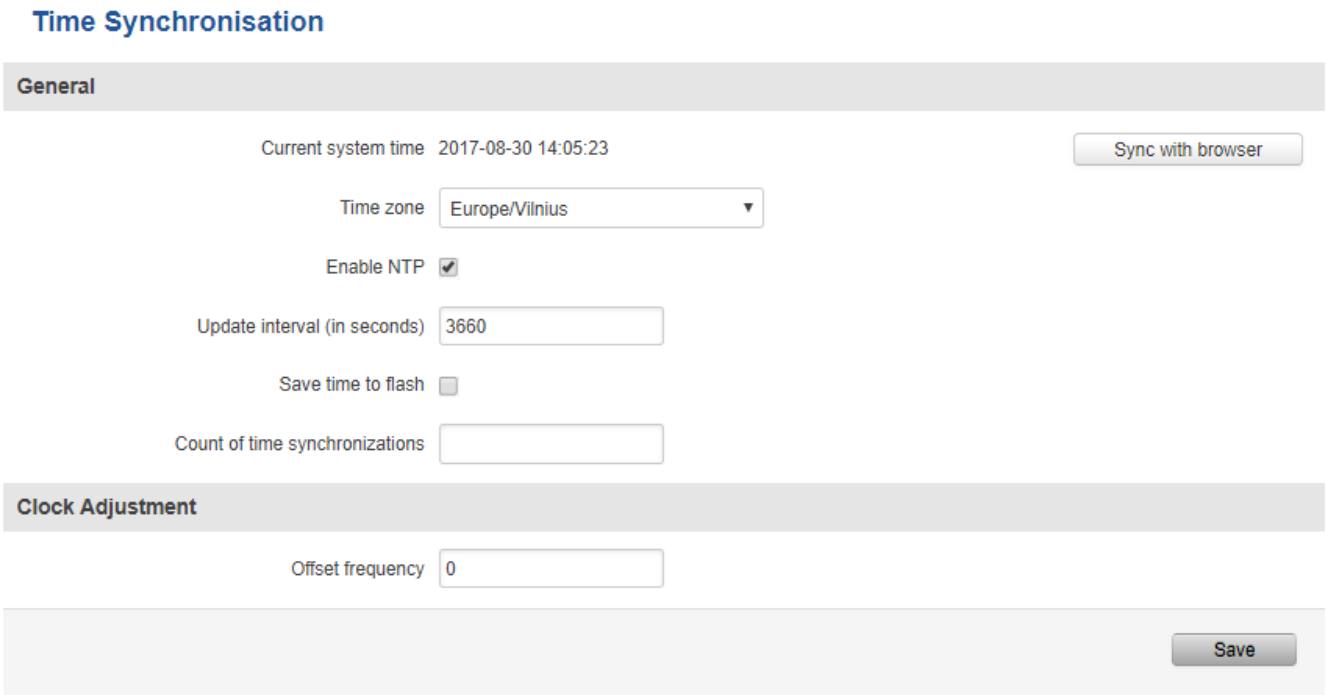
In order for the system to work, the MQTT broker should be configured in advance. You can use the Broker that is installed in the router or another, independent Broker. Shown below is a scheme where the client tries to subscribe for information about the router's uptime. To achieve this, multiple commands between the client and the publisher are being sent.



In general the publisher works in this way: the publisher connects to the broker and subscribes to the topics ***router/get*** and ***get/<SERIAL>/command***. ***<SERIAL>*** denotes the serial number of the client's router. The client then sends a message ***id*** to the topic ***router/get***. The following message is received by the publisher, since it is subscribed to that topic. Then the publisher sends a response with its serial number to the topic ***router/id***. Now the client knows that a publisher with some serial number exist. It means that the client can send a message with the parameter name from the list as a message to the topic ***get/<SERIAL>/command*** to the Broker. The message will be received only by the subscriber, which has the same SERIAL number mentioned in the topic. Now the publisher can send a response back with ***router/<SERIAL>/parameter_name*** topic and a message with the value of the requested parameter. It should be noted that, according to the MQTT protocol, topic names are case-sensitive, for example topic router is not the same as topic RoUtEr.

9.5 NTP

NTP (Network Time Protocol) configuration lets you setup and synchronize your router's time.



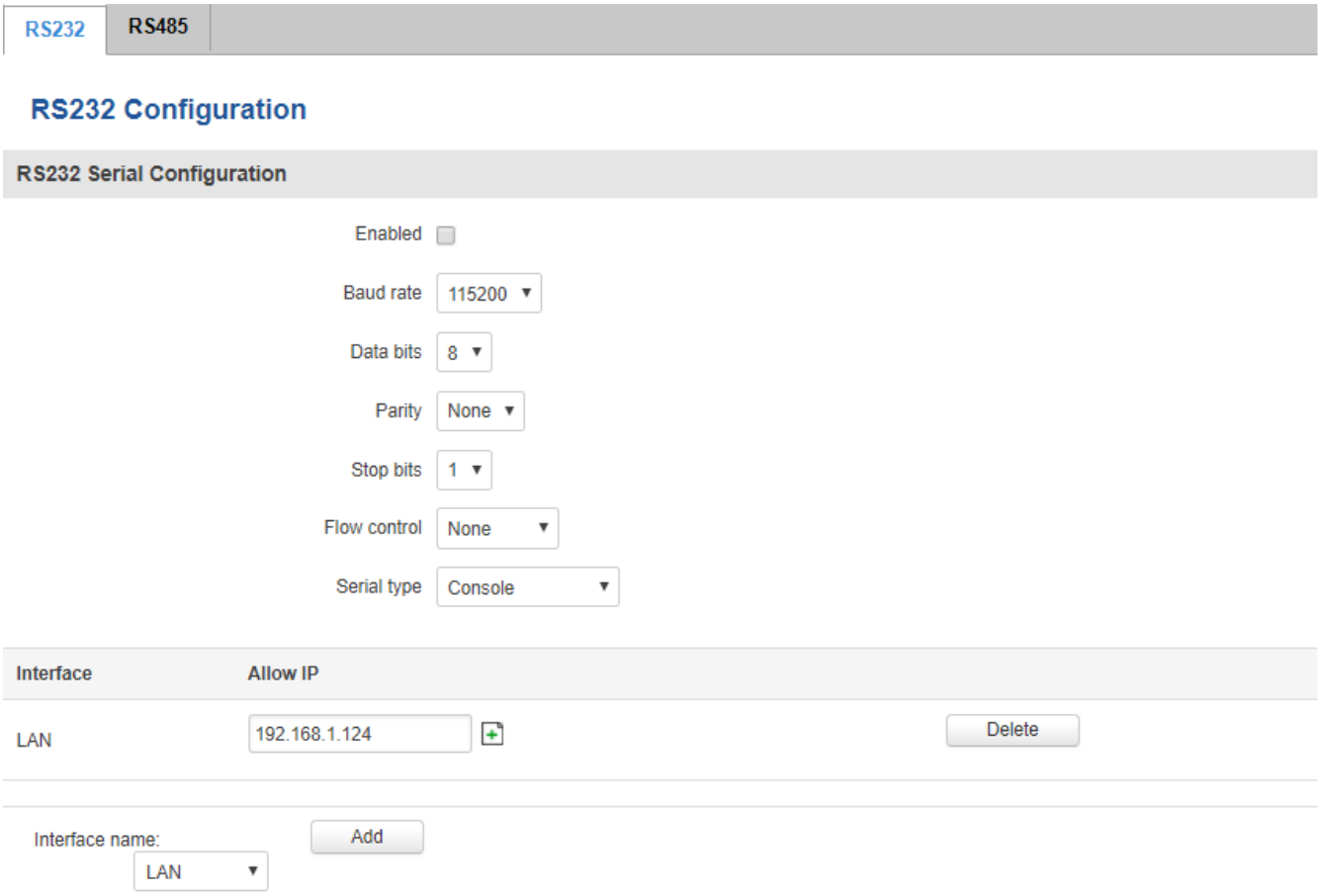
	Field name	Description
1.	Current System time	Local time of the router
2.	Time zone	Time zone of the country where the router is located
3.	Enable NTP	Enable synchronization with the time server using NTP
4.	Update interval	How often the router updates systems time
5.	Save time to flash	Save last synchronized 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	Adjusts the minor drift of the clock so that it will run more accurately

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

9.6 RS232/RS485

RS232 and RS485 functions are designed to utilize available serial interfaces of the router. Serial interfaces provide a possibility for legacy devices to gain access to IP networks.

9.6.1 RS232



	Field name	Possible values	Explanation
1.	Enabled	Checked/Unchecked	Check to enable the serial port function
2.	Baud rate	300/1200/2400/4800/9600/ 19200/38400/57600/115200	Select the communication speed of the serial interface
3.	Data bits	5 – 8	Specifies how many bits will be used for each character
4.	Parity	None/Odd/Even	Select the parity bit setting used for error detection during data transfer
5.	Stop bits	1 / 2	Specifies how many stop bits will be used to detect the end of character
6.	Flow control	None/RTS- CTS/Xon-Xoff	Specifies what kind of characters to use for flow control
7.	Serial type	Console/Over IP/Modem/ Modbus Gateway/NTRIP Client	Specifies the function of the serial interface
8.	Interface	LAN/ WAN/ VPN/L2TP/PPTP/GRE/HOTSPOT	Interface used for connection
9.	Allow IP	Any IP address	Allow IP to connect to server

9.6.1.1 RS232 connector pinout

RS232 connector type on this device is DCE female. DCE stands for Data Communication Equipment.

Pin	Name*	Description*	Direction on this device
1	DCD	Data Carrier Detect	Output
2	RXD	Receive Data	Output
3	TXD	Transmit Data	Input
4	DTR	Data Terminal Ready	Input
5	GND	Signal Ground	-
6	DSR	Data Set Ready	Output
7	RTS	Ready To Send	Input
8	CTS	Clear to send	Output
9	RI	Ring indicator	Output (connected to +5V permanently via a 4.7k resistor)

*The names and descriptions that indicate signal direction (such as TXD, RXD, RTS, CTS, DTR, and DSR) are named from the point of view of the DTE device.

9.6.1.2 Cables

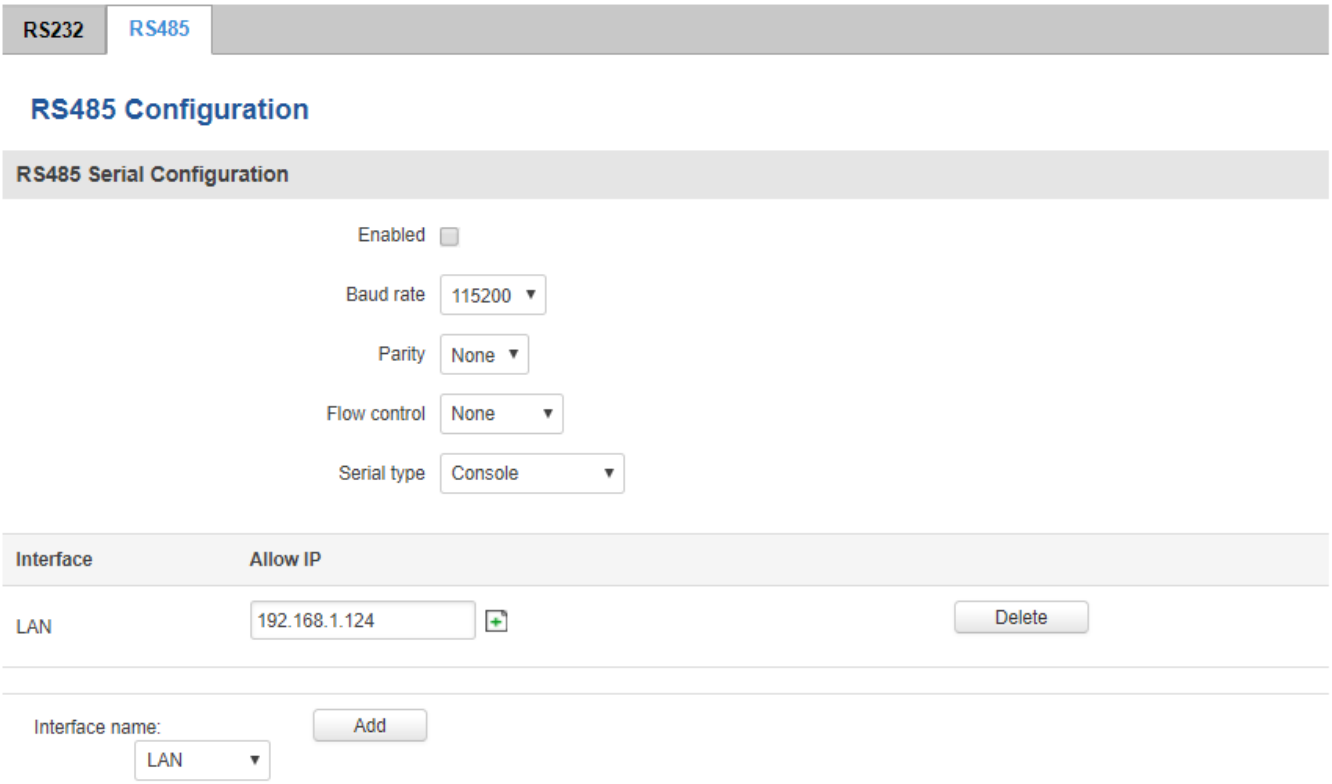
RUT955 has a DCE female connector. To connect a standard DTE device to it, use a straight-through Female/Male RS232 cable:

To connect another DCE device to RUT955, a Null-modem (crossed) Female/Female cable should be used:

Maximum cable length is 15 meters or the cable length equal to a capacitance of 2500 pF (for a 19200 baud rate). Using lower capacitance cables can increase the distance. Reducing communication speed can also increace maximum cable length.

9.6.2 RS485

RS-485 is a different serial data transmission standart for use in long ranges or noisy environments.



	Field name	Possible values	Explanation
1.	Enabled	Enable/Disable	Check the box to enable the serial port function
2.	Baud rate	300/1200/2400/4800/9600/ 19200/38400/57600/115200	Select the communication speed of the serial interface
3.	Parity	None / Odd / Even	Parity bit setting is used for error detection during data transfer
4.	Flow control	None/RTS-CTS/Xon-Xoff	Specifies what kind of characters are to be used for flow control
5.	Serial type	Console/Over IP/Modem/ Modbus Gateway/NTRIP Client	Specifies the function of the serial interface
6.	Interface	LAN/ WAN/ VPN/L2TP/PPTP/GRE/HOTSPOT	Interface used for connection
7.	Allow IP	192.168.1.102	Allow IP connecting to server

9.6.2.1 Maximum data rate vs. transmission line length

RS-485 standart can be used for network lengths up to 1200 meters, but the maximum usable data rate decreases as the transmission length increases. A device operating at the maximum data transfer rate (10Mbps) is limited to a transmission length of about 12 meters, while the 100kbps data rate can achieve a distance up to 1200 meters. A rough relation between maximum transmission length and data rate can be calculated using this approximation:

$$L_{max}(m) = \frac{10^8}{DR(bit/s)}$$

Where Lmax is the maximum transmission length in meters and DR is maximum data rate in bits per second.

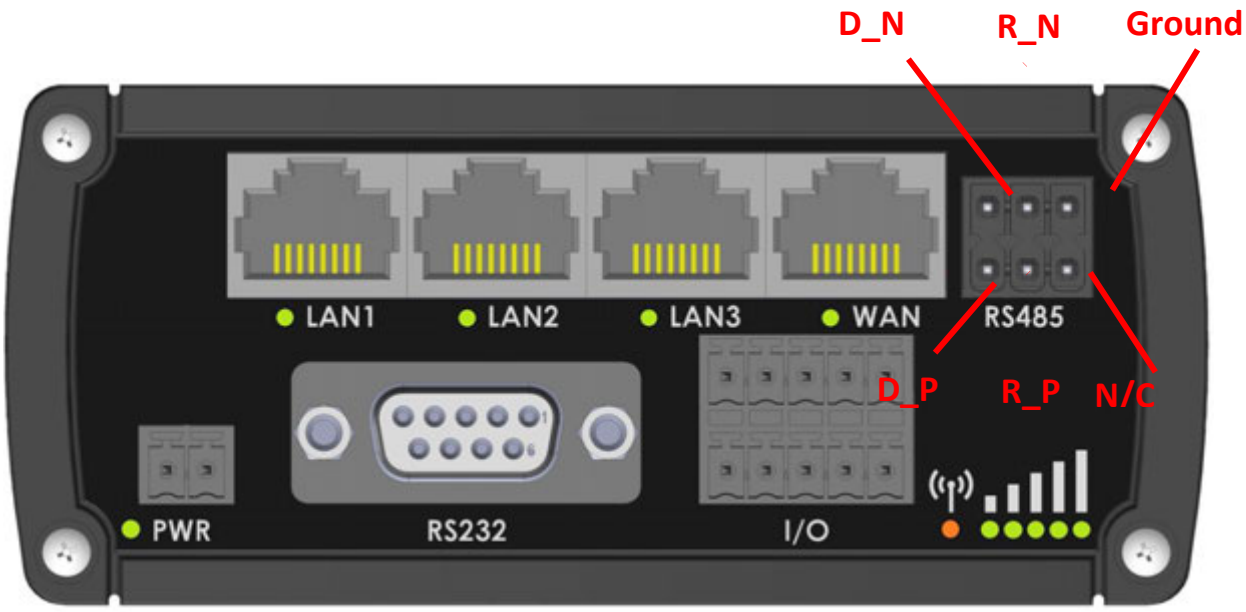
Twisted pair is the prefered cable type for RS-485 networks. Twisted pair cables pick up noise and other electromagnetically induced voltages as common mode signals, which are rejected by the differential receivers.

9.6.2.2 Cable type

Recomended cable parameters:

Parameter	Value
Cable Type	22-24 AWG, 2 – pair (used for full-duplex networks) or 1-pair (used for half duplex networks). One addtitional wire for ground connection is needed
Characteristic cable Impedance	120 Ω @ 1MHz
Capacitance (conductor to conductor)	36 pF/m
Propagation Velocity	78% (1.3 ns/ft)

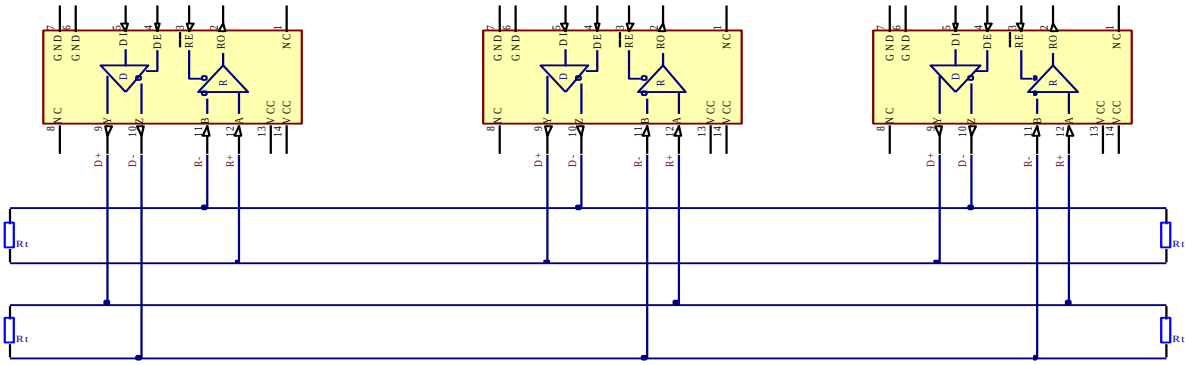
9.6.2.3 RS485 connector pin-out



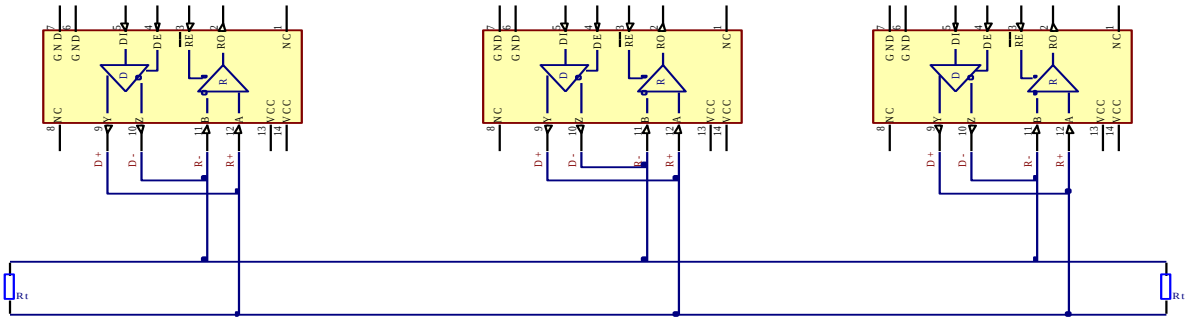
Name	Description	Type
D_P	Driver positive signal	Differential Output
D_N	Driver negative signal	Differential Output
R_P	Receiver positive signal	Differential Input
R_N	Receiver negative signal	Differential Input
Ground	Device ground	Differential Output

9.6.2.4 2-Wire and 4-Wire Networks

Below is an example of a 4-wire network electrical connection. There are 3 devices shown in the example. One of the devices is the "master" and other two are "slaves". Termination resistors are placed at each cable end. Four-wire networks consists of one „master" with its transmitter connected to each of the "slaves"' receivers on one twisted pair. The"slave" transmitters are all connected to the "master" receiver on a second twisted pair.



Example 2-wire network electrical connection: to enable a 2-wire RS-485 configuration on a Teltonika router, you need to connect D_P to R_P and D_N to R_N on the device's RS-485 socket. Termination resistors are placed at each cable end.



9.6.2.5 Termination

When to use (place jumper)

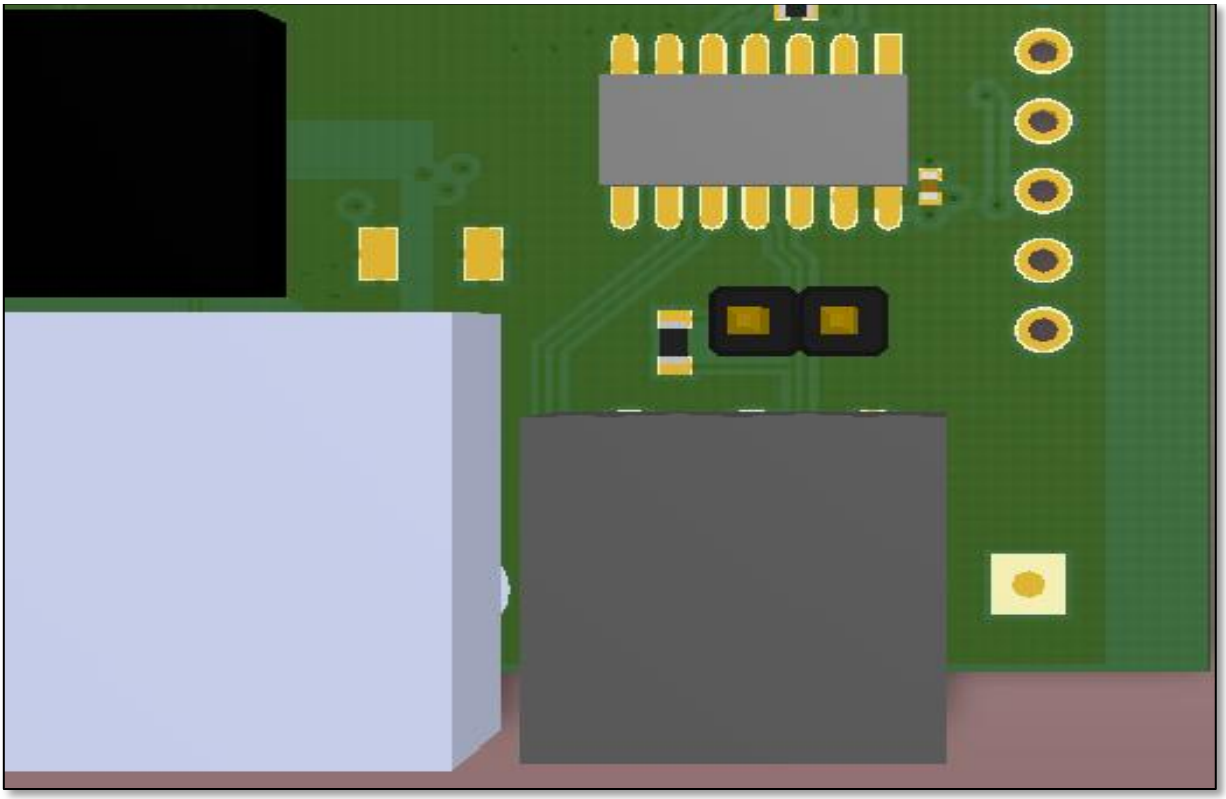
Termination resistor, equal in resistance to cable characteristic impedance, must be connected at each end of the cable to reduce reflection and ringing of the signals when the cable lengths get relatively long. Rise time of the RUT955 RS-485 driver is about 5 ns, so the maximum unterminated cable length is about 12 cm. As transmission line cables will always be longer than 12 cm, termination is mandatory all the time if RUT955 is located at the end of the cable.

When not to use (remove jumper)

If your RS-485 consists of more than two devices and the RUT955 router is located not on the end of the line but, for example, in the middle, RUT955 termination resistor needs to be disabled. In this case, place termination at other devices which are situated at the ends of the line.

How to enable termination

120 Ω termination resistor is included on the RUT955 PCB and can be enabled by shorting contacts (shown in the picture below), placing 2.54mm pitch jumper:



9.6.2.6 Number of devices in an RS-485 Network

One RUT955 RS-485 driver is capable of driving a maximum of 32 receivers, provided that the receiver input impedance is 12 kΩ. If receiver impedances are higher, the maximum number of receivers in the network increases. Any combination of receiver types can be connected together, provided their parallel impedance does not exceed $R_{Load} > 375$ Ω.

9.6.3 Modes of different serial types in RS232 and RS485

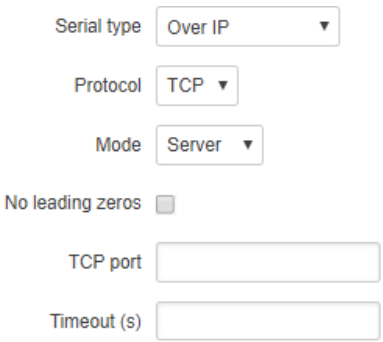
9.6.3.1 Console

In this mode the serial interface set up as a Linux console of the device. It can be used for debugging purposes, to get the status of the device or to control it.

9.6.3.2 Over IP

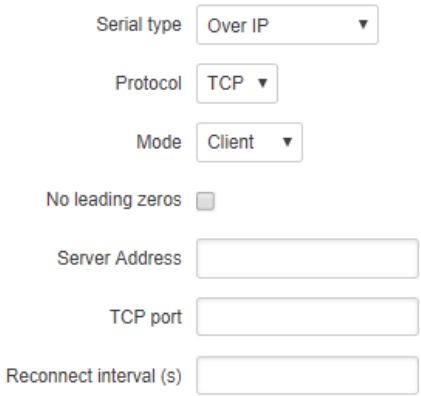
In the Over IP Serial type the router provides a connection to a TPC/IP network for the devices connected via serial interfaces.

Mode: Server



	Field name	Possible values	Explanation
1.	Protocol	TCP	The protocol uses for data transmission
2.	Mode	Server / Client / Bidirect	**Server** - wait for incoming connection **Client** - initiate the connection **Bidirect** – acts as a client by default, but at the same time waits for incoming connections
3.	No leading zeros	Checked / Unchecked	Check to skip first hex zeros
3.	TCP port	0 - 65535	The port number used to listen for incoming connections
4.	Timeout (s)	Any integer number	Disconnects client after the specified timeout of inactivity

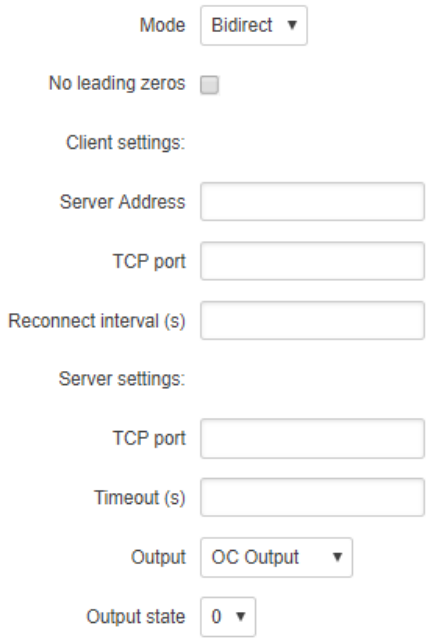
Mode: Client



	Field name	Possible values	Explanation
1.	Server Address	Hostname or IP address	Server's address to which the client will have to connect to
2.	TCP port	0 - 65535	The port number of the remote server
3.	Reconnect intervals (s)	Any integer number	Indicates the time period between reconnection attempts

Mode: Bidirect

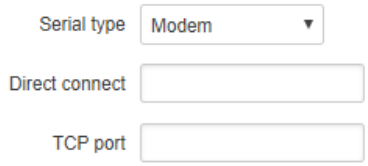
Bidirect mode allows bi-directional communication through the serial interface. In its default state the application acts like a client, but at the same time it listens to any incoming connections on the dedicated port. When there is an incoming connection, the application drops the current connection to the remote server and acts like a server in the new connection. This triggers a configured output change, which can be used to inform any auxiliary devices about connection status changes. When the client connection is terminated, the application returns to its default mode and continues to act as a client to the remote server.



	Field name	Possible values	Explanation
1.	Server Address	Hostname or IP address	Server's address to which the client will have to connect to
2.	TCP port	0 - 65535	The port number of the remote server
3.	Reconnect intervals (s)	Any integer number	Indicates the time period between reconnection attempts
4.	TCP port	0 – 65535	The port number used to listen for incoming connections
5.	Timeout (s)	Any integer number	Disconnects client after the specified timeout of inactivity
6.	Output	OC Output / Relay Output	Output to indicate that application switched from client (default) to server state
7.	Output state	0 or 1	Output state value after the application reverts to server mode

9.6.3.3 Modem

With Modem Serial type, the router imitates a dial-up modem. Connections to TCP/IP networks can be established using AT commands. The connection can be initiated by the device connected via serial interface with an ATD command: ATD <host>:<port>. If **Direct connect** settings are specified, the connection to the server is always active. Data mode can be entered by issuing the ATD command. Incoming connections are indicated by sending a RING to the serial interface.



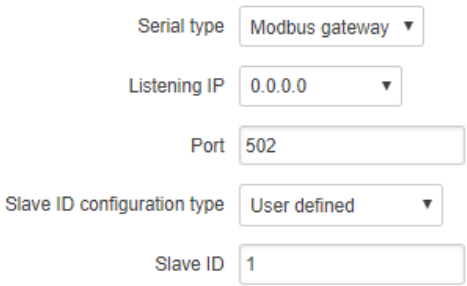
	Field name	Possible values	Explanation
1.	Direct connect	Hostname/IP address:port	Maintain a constant connection to specified host. Leave empty to use an ATD command to initiate the connection.
2.	TCP port	0 – 65535	The port number used to listen for incoming connections. Leave it empty to disable incoming connections

This is the AT command set used in **Modem** mode of the serial interfaces:

Command	Description	Usage
A	Answer incoming call	To answer incoming connection: **ATA**
D	Dial a number	To initiate data connection: **ATD <host>:<port>** To enter data mode with **Direct connect** settings: **ATD**
E	Local echo	Turn local echo on: **ATE1**; Turn local echo off: **ATE0**
H	Hang up current call	To end data connection: **ATH**
O	Return to data mode	To return to data mode from command mode: **ATO**
Z	Reset to default configuration	To reset the modem to default configuration: **ATZ**

9.6.3.4 Modbus gateway

The Modbus gateway Serial type allows redirecting TCP data coming to a specified port to RTU specified by the Slave ID. The Slave ID can be specified by the user or be obtained directly from the Modbus header.



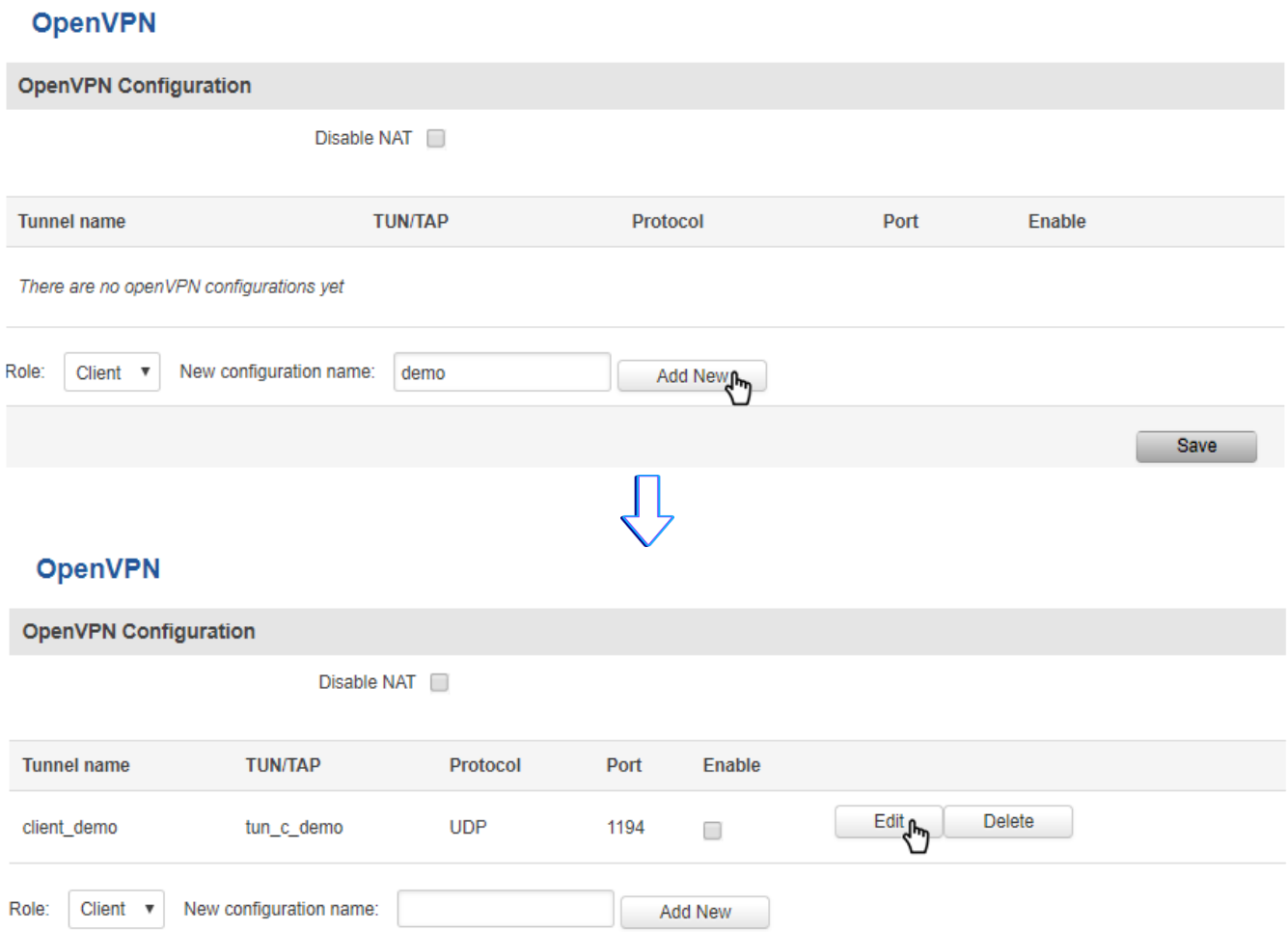
	Field name	Possible values	Explanation
1.	Listening IP	Any IP address	IP address on which the Modbus gateway will wait for incoming connections
2.	Port	0 – 65535	The port number used to listen for incoming connections
3.	Slave ID configuration type	User defined / Obtained from TCP	There are two options available for this parameter: **User defined** - redirects all data to the specified Slave ID **Obtain from TCP -** redirects data to slave IDs from the Modbus TCP
4.	Slave ID / Permitted slave IDs	Any integer number / Any few integer numbers or ranges of numbers	This field's name and possible values change according to the selected Slave ID configuration type: **Slave ID** - ID of the slave device connected to the router **Permitted slave IDs** - allows specifying the list of permitted slave IDs for redirecting of the Modbus TCP data. Individual values can be separated using commas (','), the range can be specified using hyphens ('-'), e.g., 1, 2, 4-6. Slave IDs not listed here are ignored

9.7 VPN

9.7.1 OpenVPN

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

The default OpenVPN Configuration list is empty, so you have to define your own configuration to establish any sort of OpenVPN connection. OpenVPN configurations can have one of two **roles**: client and server. Let's start with an OpenVPN client. To create it, enter the desired instance name in the **"New configuration name"** field, select the instance's role from the **"Role"** drop down list and press the **"Add New"** button.



Once you've added a new OpenVPN instance there is no need to press the "Save" button, since the "Add New" button both creates and saves the new instance. By default the instance will be disabled and unconfigured. I order to establish an OpenVPN connection you must Enable your instance, enter an OpenVPN server address, choose an authentication method and a few other things, all of which can be configured in the Settings window, which can reached by pressing the **"Edit"** button next to your OpenVPN instance (as shown in the figure above).

9.7.1.1 OpenVPN Client

OpenVPN Instance: Client_demo

Main Settings

Enable	☑
TUN/TAP	TUN (tunnel)
Protocol	UDP
Port	1194
LZO	☑
Encryption	BF-CBC 128 (default)
Authentication	TLS/Password
TLS cipher	All
Remote host/IP address	84.15.198.92
Resolve retry	infinite
Keep alive	10 120
Remote network IP address	10.0.0.0
Remote network IP netmask	255.255.255.0
User name	client
Password	••••••••••••
Extra options	
HMAC authentication algorithm	SHA1 (default)
Additional HMAC authentication	☐
Certificate authority	Choose File ca.crt
Client certificate	Choose File client1.crt
Client key	Choose File client1.key

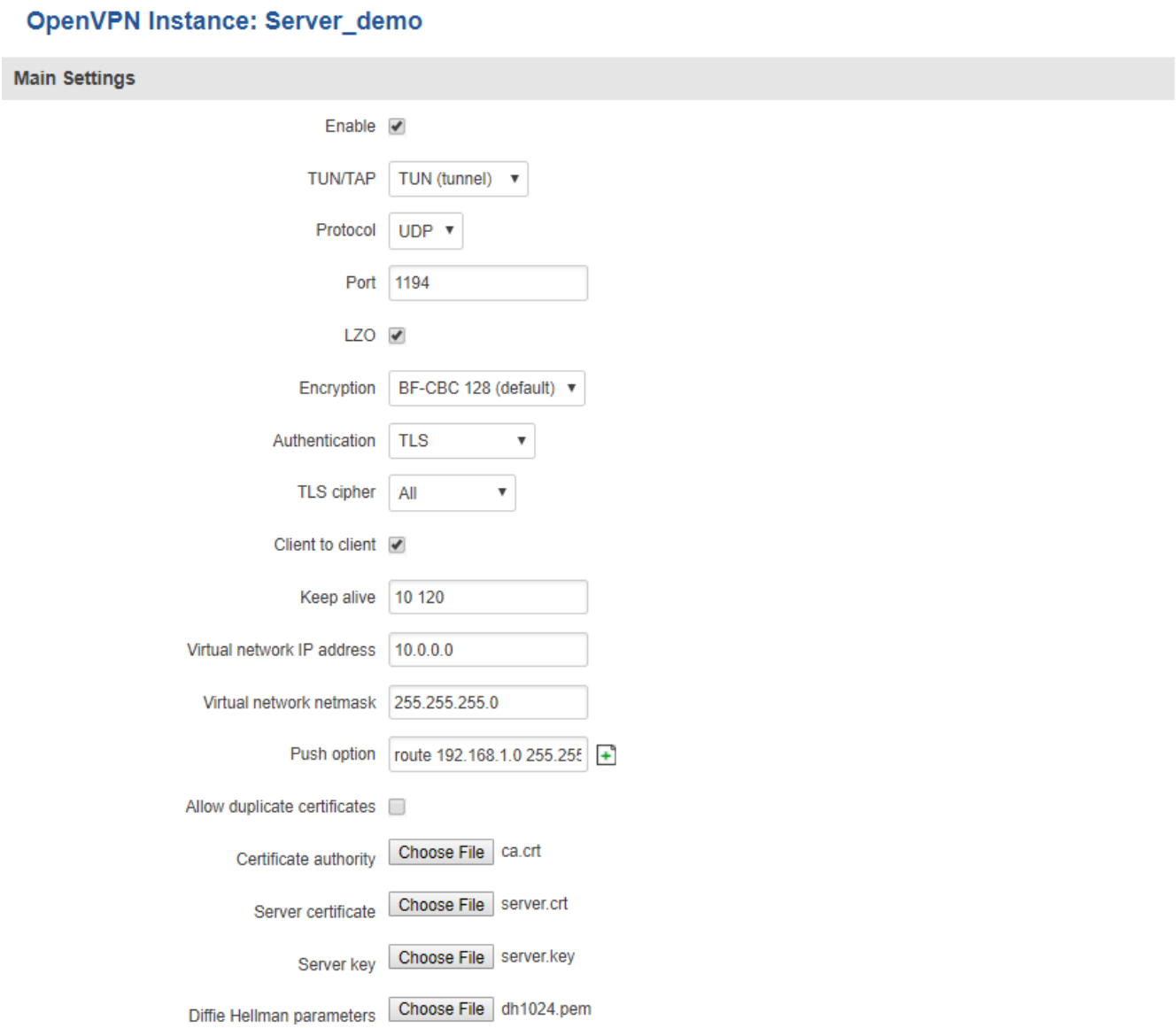
The figure above is a picture of a configured OpenVPN Client instance that uses the UDP protocol and TLS/Password authentication. Comprehensible explanations on how to configure each field are presented in the table below.

	Field name	Possible values	Explanation
1.	Enable	Checked / Unchecked	Turns the OpenVPN instance **on** or **off**
2.	TUN/TAP	TUN (tunnel) / TAP (bridged)	OpenVPN interface type. **TUN** is most often in typical VPN connections, however, **TAP** is required in some Ethernet bridging configurations
3.	Protocol	UDP / TCP	The transfer protocol used by the connection
4.	Port	0 – 65535	Port number (make sure that this port is allowed by firewall)
5.	LZO	Checked / Unchecked	With LZO compression, your VPN connection will generate less network traffic. However, enabling this causes a higher CPU load. Use it carefully with a high traffic rate or low CPU resources
6.	Encryption	BF-CBC 128 (default) / AES-128-CBC 128 / …	Packet encryption algorithm
7.	Authentication	TLS / Static Key / Password / TLS/Password	Authentication mode, used to secure data sessions. **Static key** is a secret key used for server – client authentication**.** **TLS** authentication mode uses X.509 type certificates: **Certificate Authority (CA), Client certificate, Client key**. All mentioned certificates can be generated using OpenVPN or Open SSL utilities on any type of host machine. **Password** is a simple username/password based authentication where the owner of the OpenVPN server provides the login data. **TLS/Password** uses both TLS and Password authentication
8.	TLS cipher	All / DHE + RSA / Custom	Packet encryption algorithm (cipher)
9.	Remote host/IP address	Any hostname or IP address	IP address or hostname of an OpenVPN server
10.	Resolve Retry	Infinite / any integer number	Time in seconds to resolve server hostname periodically in case of first resolve failure before generating service exception
11.	Keep alive	Any integer number *space* any integer number	Defines two time intervals: one is used to periodically send ICMP request to the OpenVPN server, the other defines a time window, which is used to restart the OpenVPN service, if no ICPM response is received during the window time slice. Example: "10 60"
12.	Remote network IP address	Any private IP address	LAN IP address of the remote network
13.	Remote network IP netmask	Any netmask	Subnet mask of the remote LAN network
14.	User name	Client's username	Username used for authentication
15.	Password	Client's password	Password used for authentication
16.	Extra options		Extra options to be used by the OpenVPN instance
17.	HMAC authentication algorithm	none / SHA1(default) / SHA256 / SHA384 / SHA512	The type of HMAC authentication algorithm
18.	Additional HMAC authentication	Checked / Unchecked	An additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks
19.	Certificate authority	.ca file	Certificate authority is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate

20.	Client certificate	.crt file	Client certificate is a type of digital certificate that is used by client systems to make authenticated requests to a remote server. Client certificates play a key role in many mutual authentication designs, providing strong assurances of a requester's identity
21.	Client key	.key file	Authenticates the client to the server and establishes precisely who they are

After setting any of these parameters press the **"Save"** button or else the changes will not be applied. Some of the selected parameters will be shown in the configuration list table. You should also be aware of the fact that the router will launch a separate OpenVPN service for every configuration entry (if it is defined as active at the time, of course) so the router has the ability to act as server and client at the same time.

9.7.1.2 OpenVPN Server



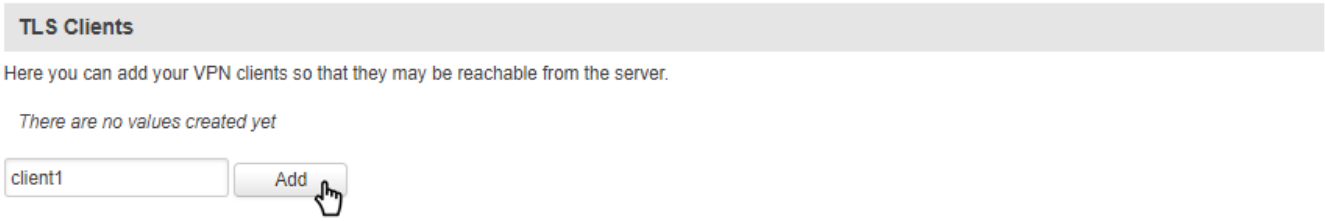
The figure above is a picture of a configured OpenVPN Server instance that uses the UDP protocol and TLS authentication. As you can see, the configuration is similar to OpenVPN Client but with a few key differences. Comprehensible explanations on how to configure each field are presented in the table below.

	Field name	Possible values	Explanation
1.	Enable	Checked / Unchecked	Turns the OpenVPN instance **on** or **off**
2.	TUN/TAP	TUN (tunnel) / TAP (bridged)	OpenVPN interface type. **TUN** is most often in typical VPN connections, however, **TAP** is required in some Ethernet bridging configurations
3.	Protocol	UDP / TCP	The transfer protocol used by the connection
4.	Port	0 – 65535	Port number (make sure that this port is allowed by firewall)
5.	LZO	Checked / Unchecked	With LZO compression, your VPN connection will generate less network traffic. However, enabling this causes a higher CPU load. Use it carefully with a high traffic rate or low CPU resources
6.	Encryption	BF-CBC 128 (default) / AES-128-CBC 128 / …	Packet encryption algorithm
7.	Authentication	TLS / Static Key / Password / TLS/Password	Authentication mode, used to secure data sessions. **Static key** is a secret key used for server – client authentication. **TLS** authentication mode uses X.509 type certificates: **Certificate Authority (CA), Server certificate, Server key, Diffie Hellman parameters (DH)**. All mentioned certificates can be generated using OpenVPN or Open SSL utilities on any type of host machine. **TLS/Password** uses both TLS certificates and a User/Password type of authentication
8.	TLS cipher	All / DHE + RSA / Custom	Packet encryption algorithm (cipher)
9.	Client to client	Checked / Unchecked	Enables client to client communication in the Virtual network. In order for Client to client to work, the TLS Clients section most be utilized
10.	Keep alive	Any integer number *space* any integer number	Defines two time intervals: one is used to periodically send ICMP request to the OpenVPN server, the other defines a time window, which is used to restart the OpenVPN service, if no ICPM response is received during the window time slice. Example: "10 60"
11.	Virtual network IP address	Any private IP address	IP address of the Virtual network
12.	Virtual network IP netmask	Any netmask	Subnet mask of the Virtual network
13.	Push option	i.e., route 192.168.1.0 255.255.255.0	Push options are a way to "push" user defined routes to connecting clients' routing tables. In the given example, the server will push the route of 192.168.1.0 network with the 255.255.255.0 netmask to connecting clients. Therefore, the client will be able to reach devices in the 192.168.1.0 network. This is useful when a client needs to reach devices located in the OpenVPN server's LAN.
14.	Allow duplicate certificates	Checked / Unchecked	If checked, the server allows clients to connect with identical certificates
15.	Certificate authority	.ca file	Certificate authority is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate
16.	Server certificate	.crt file	Server certificate is a type of digital certificate that is used to identify the OpenVPN server
17.	Server key	.key file	Authenticates clients to the server
18.	Diffie Hellman parameters	.pem file	DH parameters define how OpenSSL performs the Diffie-Hellman (DH) key-exchange.

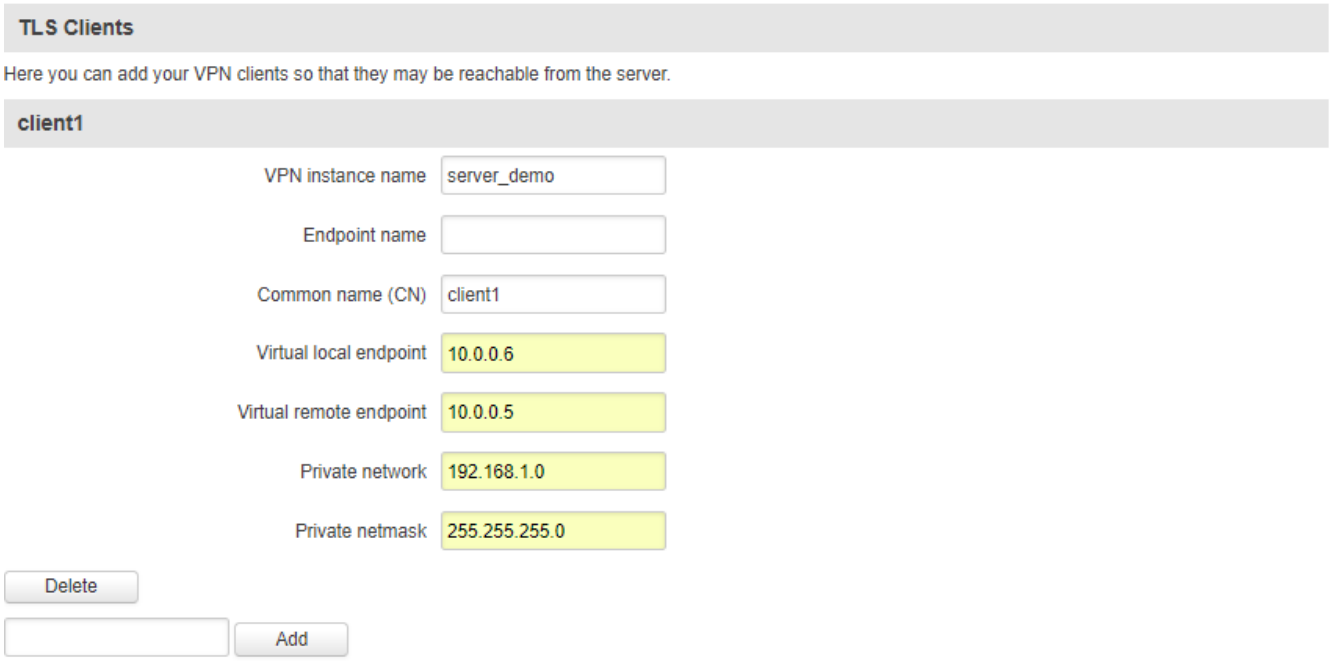
9.7.1.3 TLS Clients

TLS Clients is a way to more specifically differentiate clients by their Common Name (CN) found in the client certificate file. It can be used to assign specific VPN addresses to specific clients and bind them to their LAN addresses so that other device's in the client's LAN can be reached from the server or other clients.

The TLS Clients section can be found in the OpenVPN Server configuration window, provided that the OpenVPN server uses TLS or TLS/Password authentication methods. To create a new TLS client, type in the new client's name in the text field found bellow the TLS Clients tab and press the **„Add"** button next to it as shown in the picture bellow.



This action will create a new, unconfigured TLS Client. The picture below depicts a configured TLS Client.



	Field name	Samle value	Explanation
1.	VPN instance name	server_demo	With what VPN instance should the TLS Client be associated with
2.	Endpoint name		Your endpoint name
3.	Common name (CN)	client1	Client's Common Name (CN) found in the client's certificate file
4.	Virtual local endpoint	10.0.0.6	Client's virtual local address in the virtual network
5.	Virtual remote endpoint	10.0.0.5	Client's virtual remote address in the virtual network
6.	Private network	192.168.1.0	Client's private network address
7.	Private netmask	255.255.255.0	Client's private netmask

9.7.2 IPSec

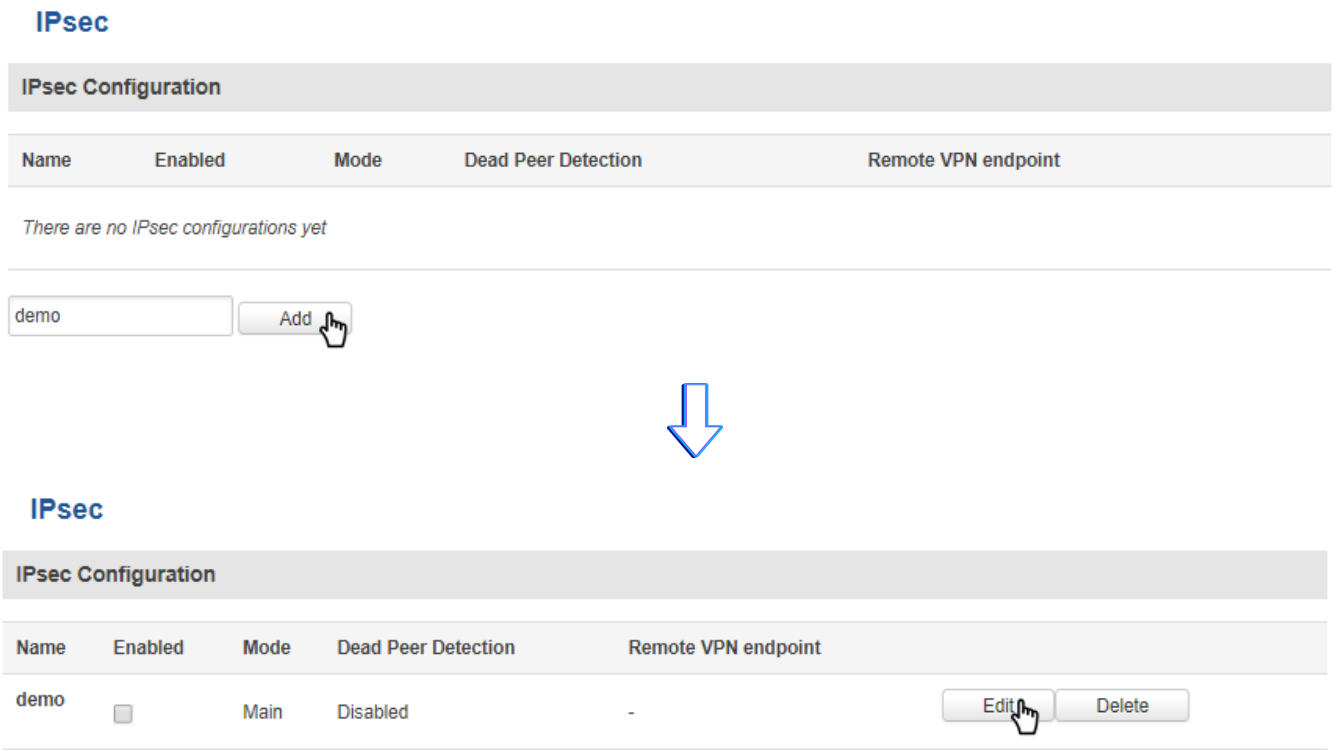
The IPsec protocol client enables the router to establish a secure connection to an IPsec peer via the Internet. IPsec is supported in two modes - transport and tunnel. Transport mode creates a secure point to point channel between two hosts. Tunnel mode can be used to build a secure connection between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

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

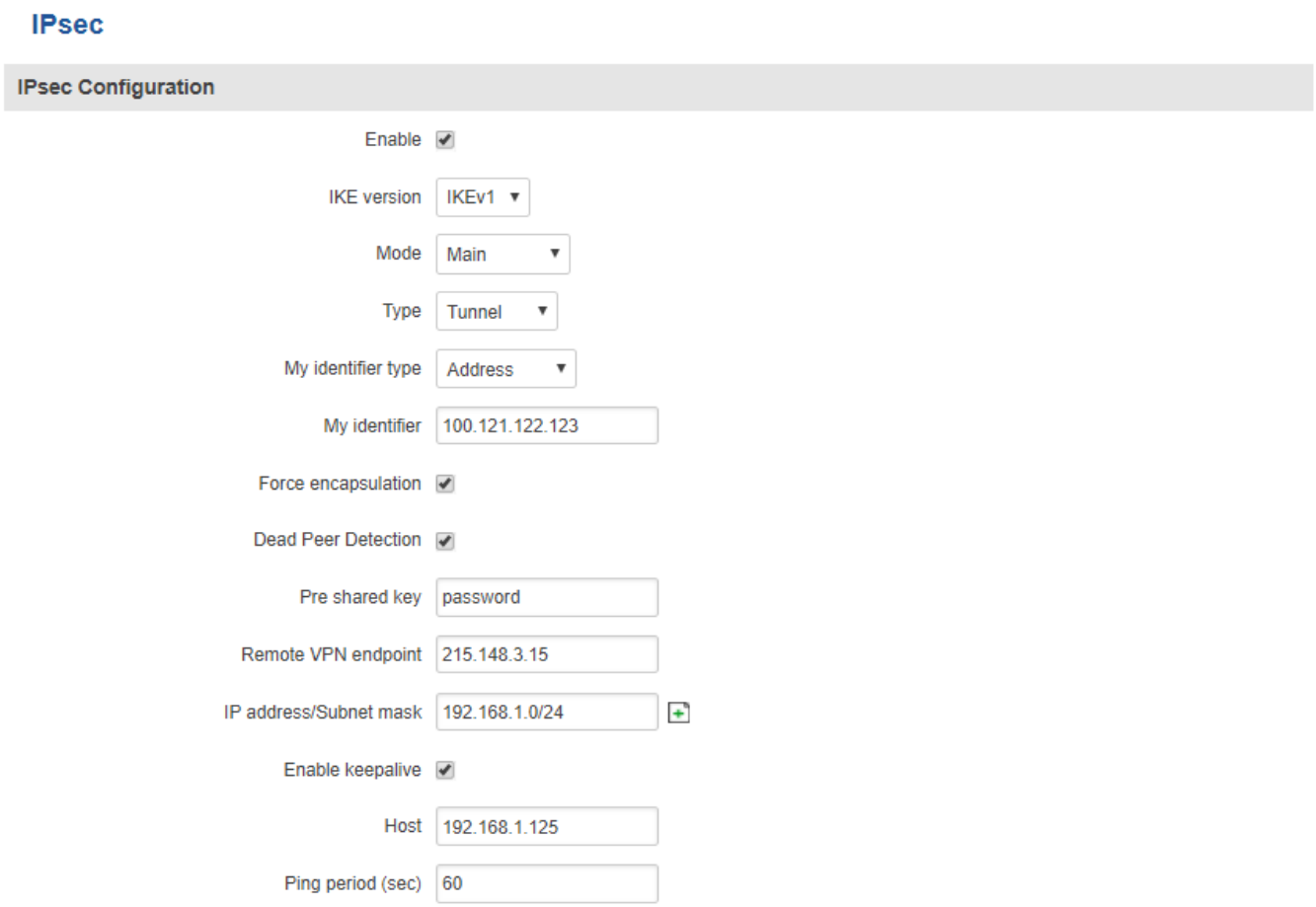
The establishment of the Security Association (IPsec-SA) between two peers is needed for IPsec communication. It can be done by using manual or automated configuration.

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

To create a new IPsec instance, go to the IPsec tab, type in a name for your new instance in the text field below the IPsec tab and press the **"Add"** button next to it.

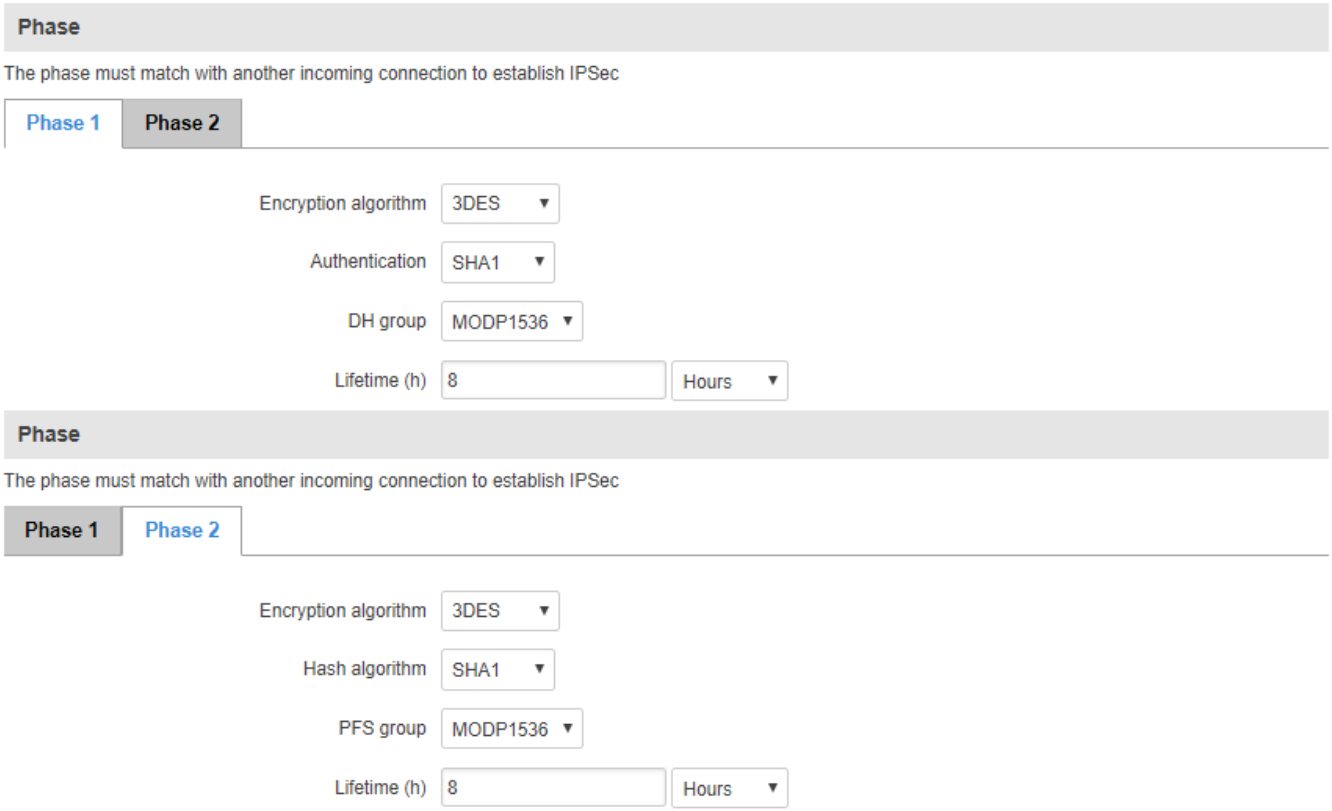


The newly created instance will be disabled and unconfigured. To configure it press the **"Edit"** button located next to it (as seen in the example above). This action will redirect you to the instance's IPsec Configuration window.



	Field name	Possible values	Explanation
1.	Enable	Checked/Unchecked	Turns IPsec on or off
2.	IKE version	IKEv1 or IKEv2	Method of key exchange
3.	Mode	Main / Aggressive	ISAKMP phase 1 exchange mode
4.	Type	Tunnel / Transport	Type of connection
5.	My identifier type	Address / FQDN / User FQDN	The type of identifier used to establish a connection with another IPsec instance
6.	My identifier	Depends on identifier type	In case RUT has a Private IP, its identifier should be its own LAN network address. In this way, the Road Warrior approach is possible
7.	Force encapsulation	Checked / Unchecked	Force UDP encapsulation for ESP packets even if no NAT situation is detected
8.	Dead Peer Detection	Checked / Unchecked	The values clear, hold and restart all activate DPD
9.	Pre shared key	Any string	A shared password to authenticate between the peers
10.	Remote VPN endpoint	Host's address	IP address or hostname of the remote IPsec instance
11.	IP address / Subnet mask	IP address/[0 - 32]	Remote network secure group IP address and mask used to determine to what subnet an IP address belongs to. Should differ from device's LAN IP
12.	Enable keep alive	Checked/Unchecked	Enable tunnel keep alive function
13.	Host	Host's address	A host address to which an ICMP echo requests will be sent
14.	Ping period (sec)	0 - 9999999	Send ICMP echo request every x seconds

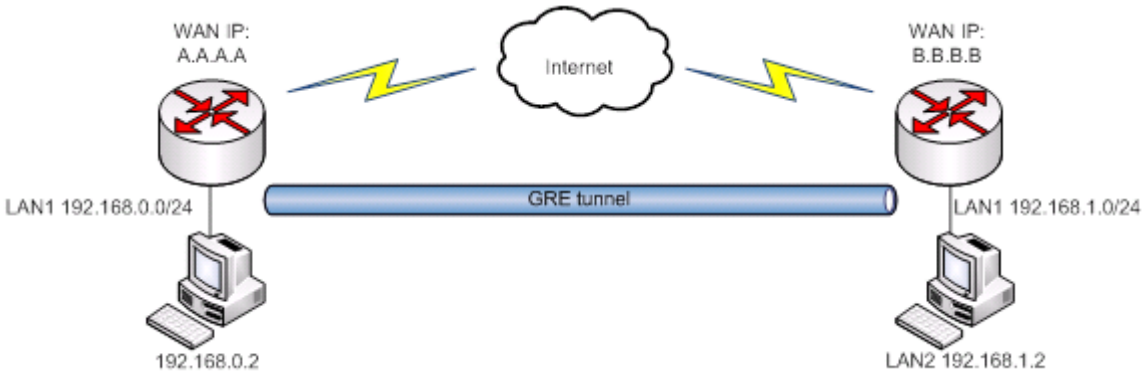
Phase 1 and **Phase 2** must be configured in accordance to the IPSec server configuration, thus algorithms, authentication and lifetimes of each phase must be identical.



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

9.7.3 GRE Tunnel

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

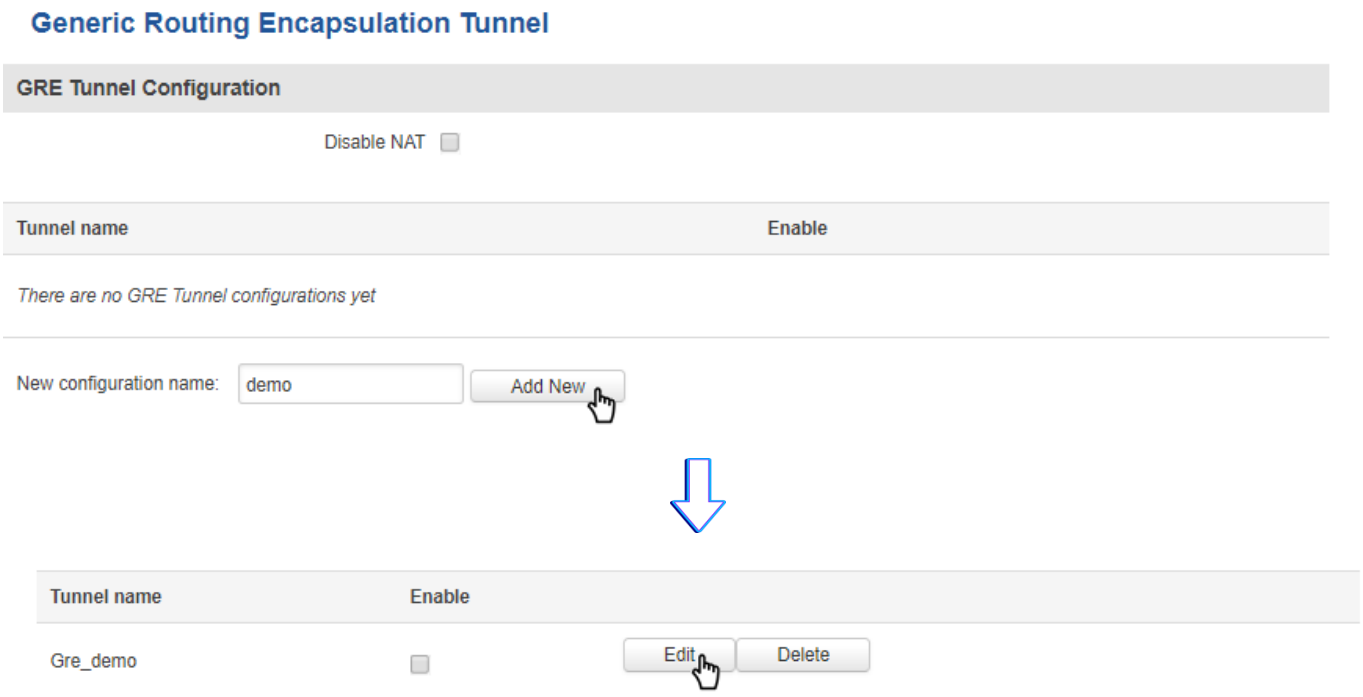


In the example network diagram two distant networks LAN1 and LAN2 are connected.

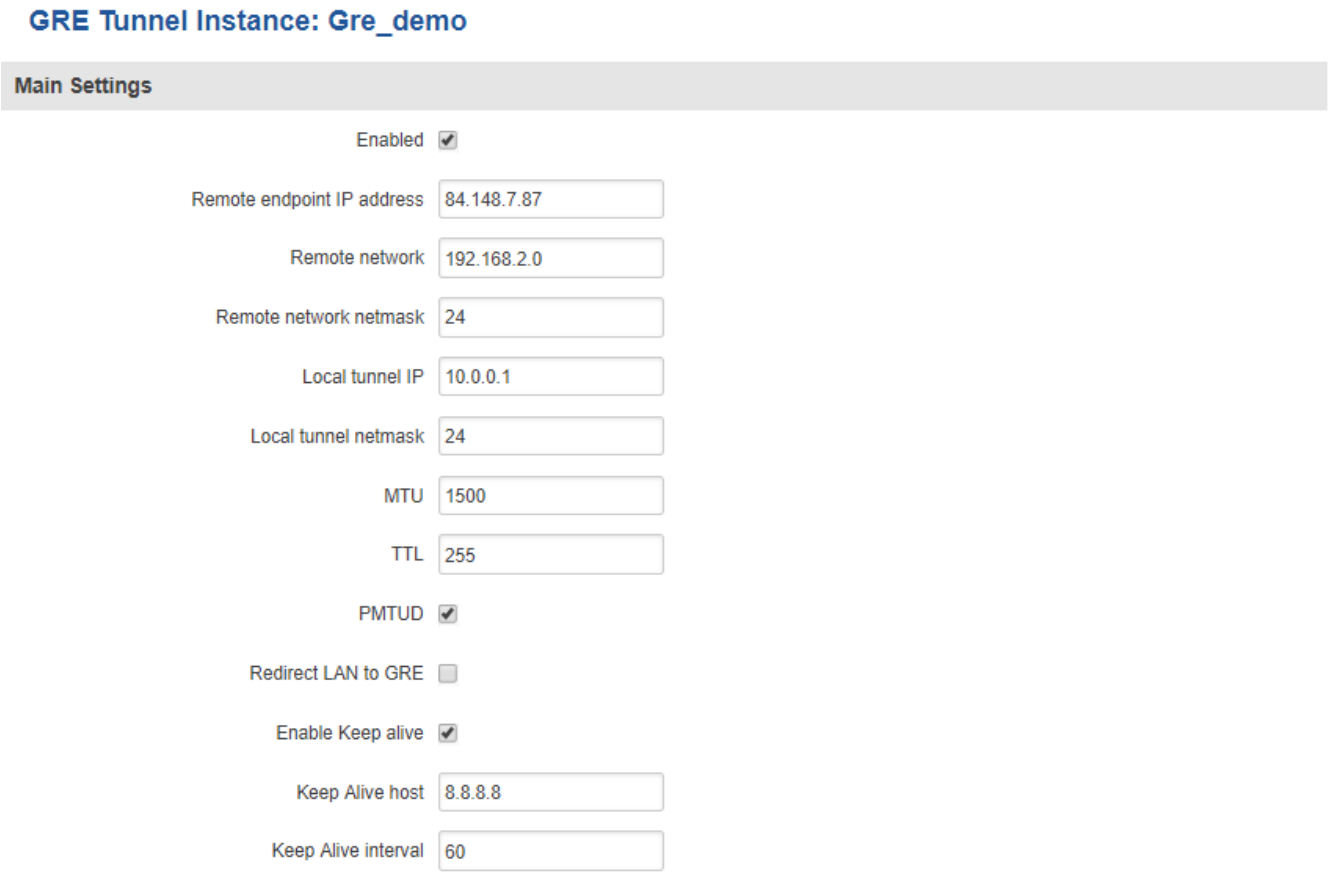
To create GRE tunnel the user must know the following parameters:

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

To create a new GRE instance, go to the GRE Tunnel tab, type in a name for your new instance in the text field below the GRE Tunnel tab and press the **"Add New"** button next to it.



The newly created instance will be disabled and unconfigured. To configure it press the **"Edit"** button located next to it (as seen in the example above). This action will redirect you to the instance's GRE Tunnel Configuration window.



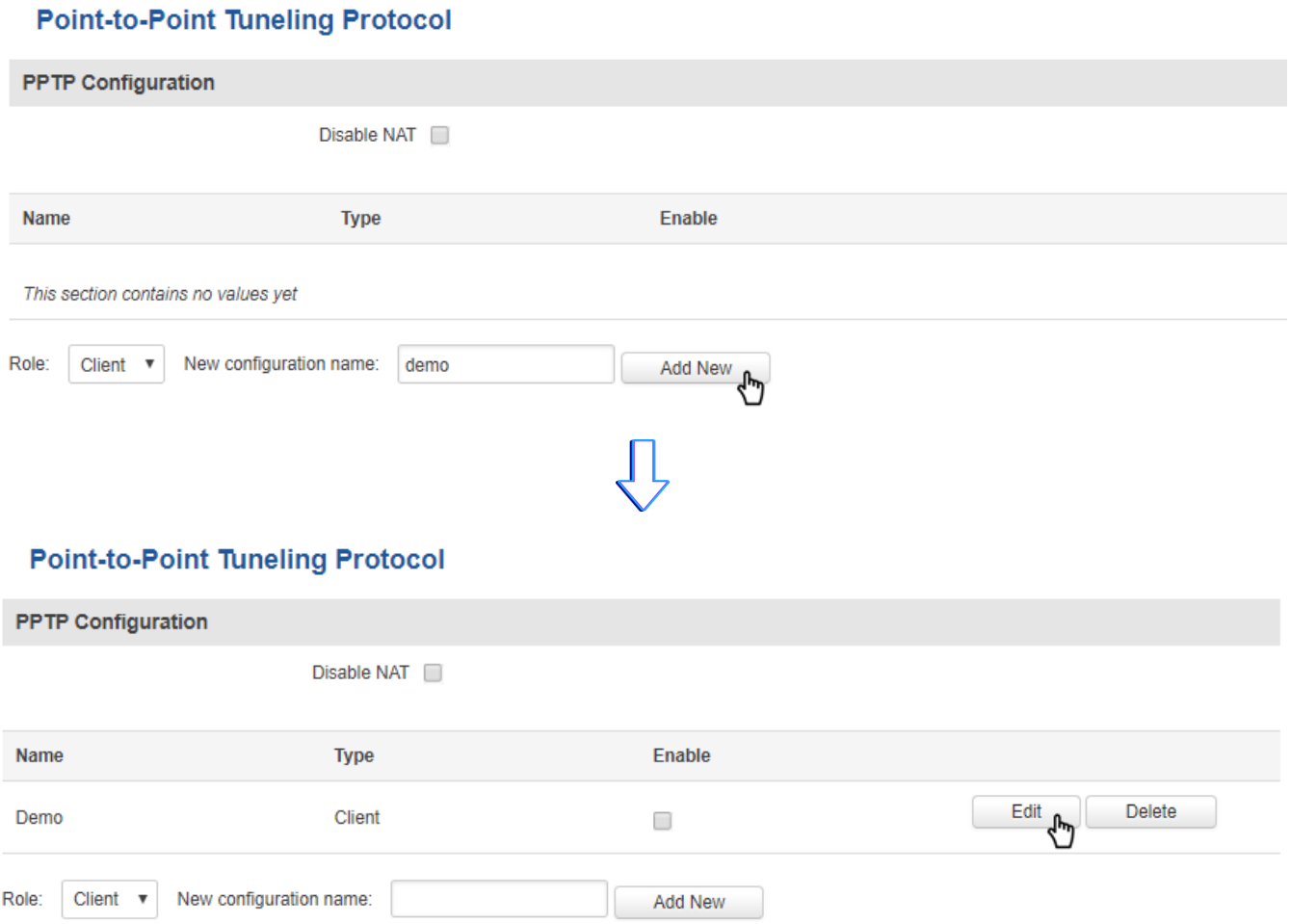
	Field name	Possible values	Explanation
1.	Enabled	Checked / Unchecked	Check to enable the GRE Tunnel function
2.	Remote endpoint IP address	Remote IP address or hostname	Specify remote WAN IP address or hostname
3.	Remote network	A private IP address	LAN IP address of the remote device.
4.	Remote network netmask	0 – 32	LAN network on the remote device
5.	Local tunnel IP	A private IP address	Local virtual IP address. Can't be in the same subnet as LAN network.
6.	Local tunnel netmask	0 – 32	Network of local virtual IP address
7.	MTU	0 – 1500	The maximum transmission unit in bytes
8.	TTL	0 – 255	Specify the fixed time-to-live (TTL) value on tunneled packets. The 0 is a special value meaning that packets inherit the TTL value
9.	PMTUD	Checked / Unchecked	Check to enable the Path Maximum Transmission Unit Discovery (PMTUD) status on this tunnel.
10.	Redirect LAN to GRE	Checked / Unchecked	Check to redirect LAN traffic to the GRE interface
10.	Enable Keep alive	Checked / Unchecked	It gives the ability for one side to originate and receive keep alive packets to and from a remote router
11.	Keep Alive host	IP address	Keep Alive host IP address. Preferably IP address which belongs to the LAN network on the remote device
12.	Keep Alive interval	0 - 255	Time interval for Keep Alive in seconds

9.7.4 PPTP

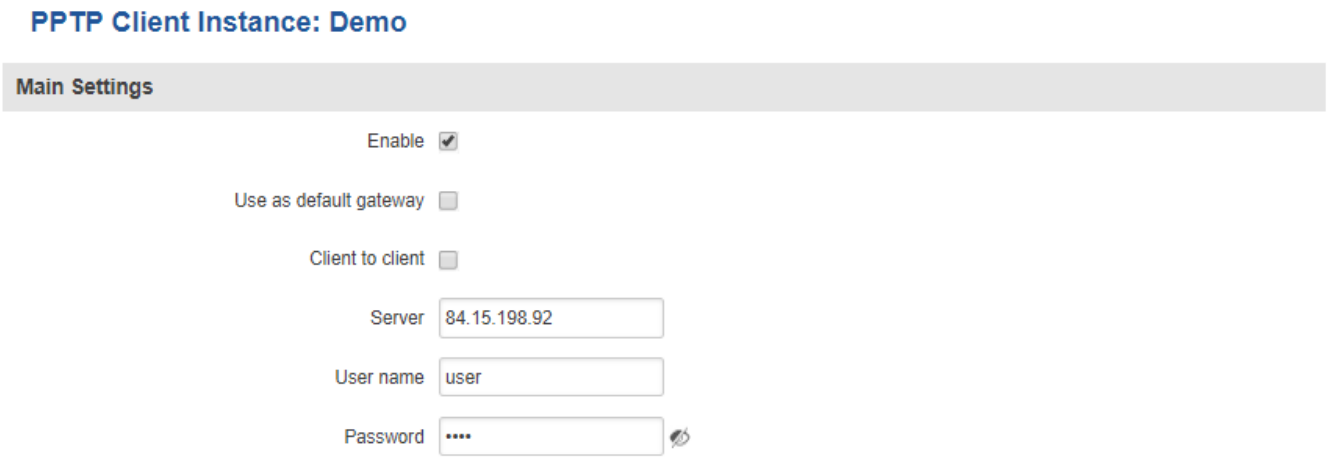
Point-to-Point Tunneling Protocol (PPTP) is a protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network. A company no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

9.7.4.1 PPTP client

To create a new PPTP instance, go to the PPTP tab, select the **Role** (server or client) of your instance, type in a name in the "New configuration name" field and press the **"Add"** button next to it.

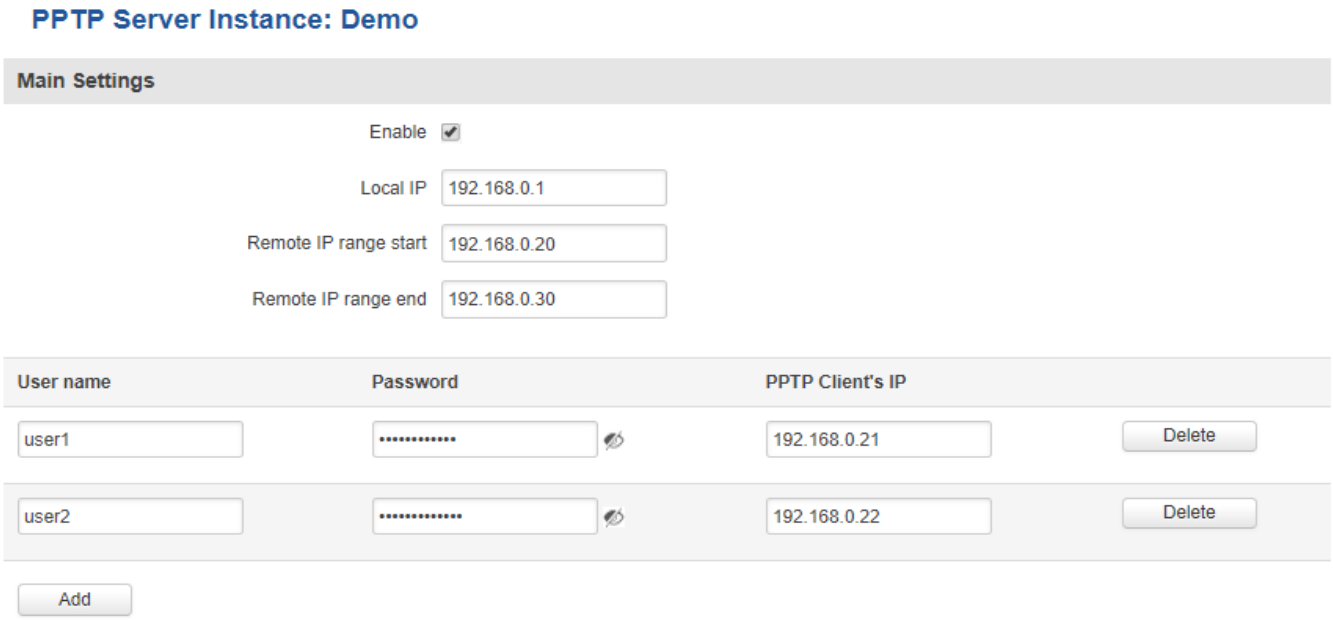


The newly created instance will be disabled and unconfigured. To configure it press the **"Edit"** button located next to it (as seen in the example above). This action will redirect you to the instance's PPTP Configuration window.



	Field name	Possible values	Explanation
1.	Enable	Checked / Unchecked	Check to enable current configuration
2.	Use as default gateway	Checked / Unchecked	Use this PPTP instance as default gateway
3.	Client to client	Checked / Unchecked	Check to enable client to client communication
4.	Server	IP address or hostname	The PPTP server's IP address or hostname
5.	Username	Any name	The user name for authorization with the server
6.	Password	Any password	The password for authorization with the server

9.7.4.2 PPTP server



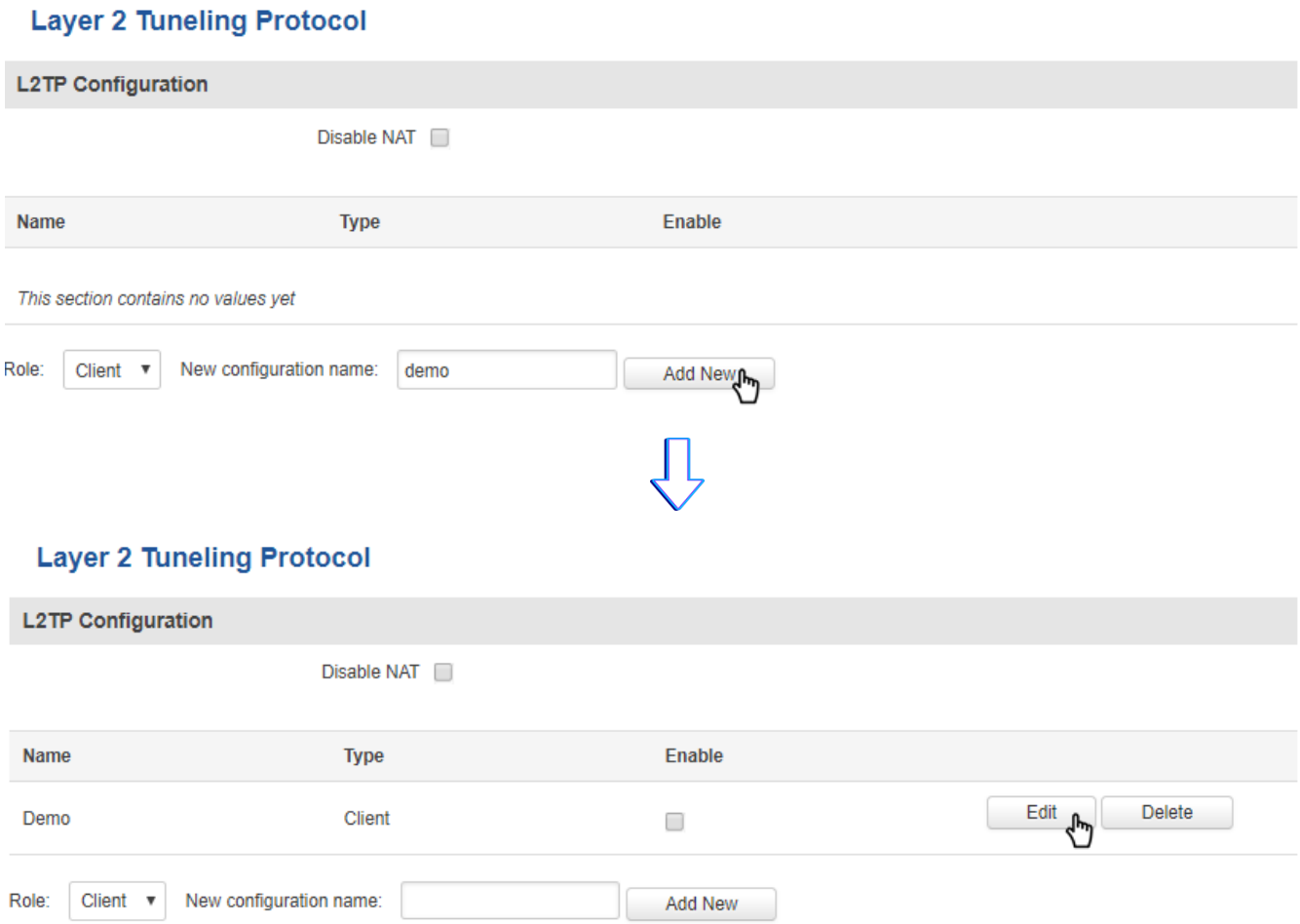
	Field name	Explanation
1.	Enable	Check the box to enable the PPTP function.
2.	Local IP	Virtual IP Address of this device (RUT)
3.	Remote IP range begin	IP address leases beginning
4.	Remote IP range end	IP address leases end
5.	Username	Username to connect to PPTP (this) server
6.	Password	Password to connect to PPTP (this) server
7.	PPTP Client's IP	User's IP address. Leave empty to assign a random IP from the given range above

9.7.5 L2TP

In computer networking, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs).It is more secure than PPTP but, because it encapsulates the transferred date twice, it is slower and uses more CPU power.

9.7.5.1 L2TP client

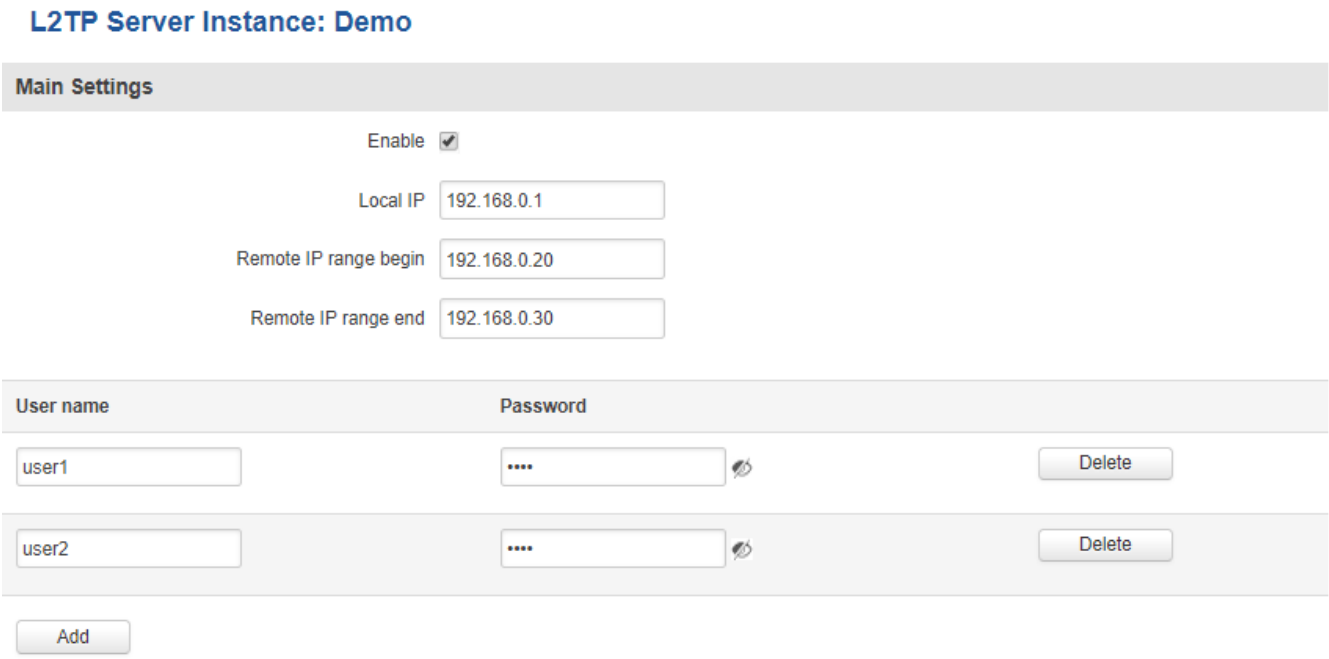
To create a new L2TP instance, go to the L2TP tab, select the **Role** (server or client) of your instance, type in a name in the "New configuration name" field and press the **"Add"** button next to it.



The newly created instance will be disabled and unconfigured. To configure it press the **"Edit"** button located next to it (as seen in the example above). This action will redirect you to the instance's L2TP Configuration window.

	Field name	Explanation
1.	Enable	Check to enable the L2TP Tunnel instance
2.	Server	IP Address or hostname of the L2TP server
3.	Username	Username used to authenticate you to the server
4.	Password	Password used to authenticate you to the server

9.7.5.2 L2TP Server

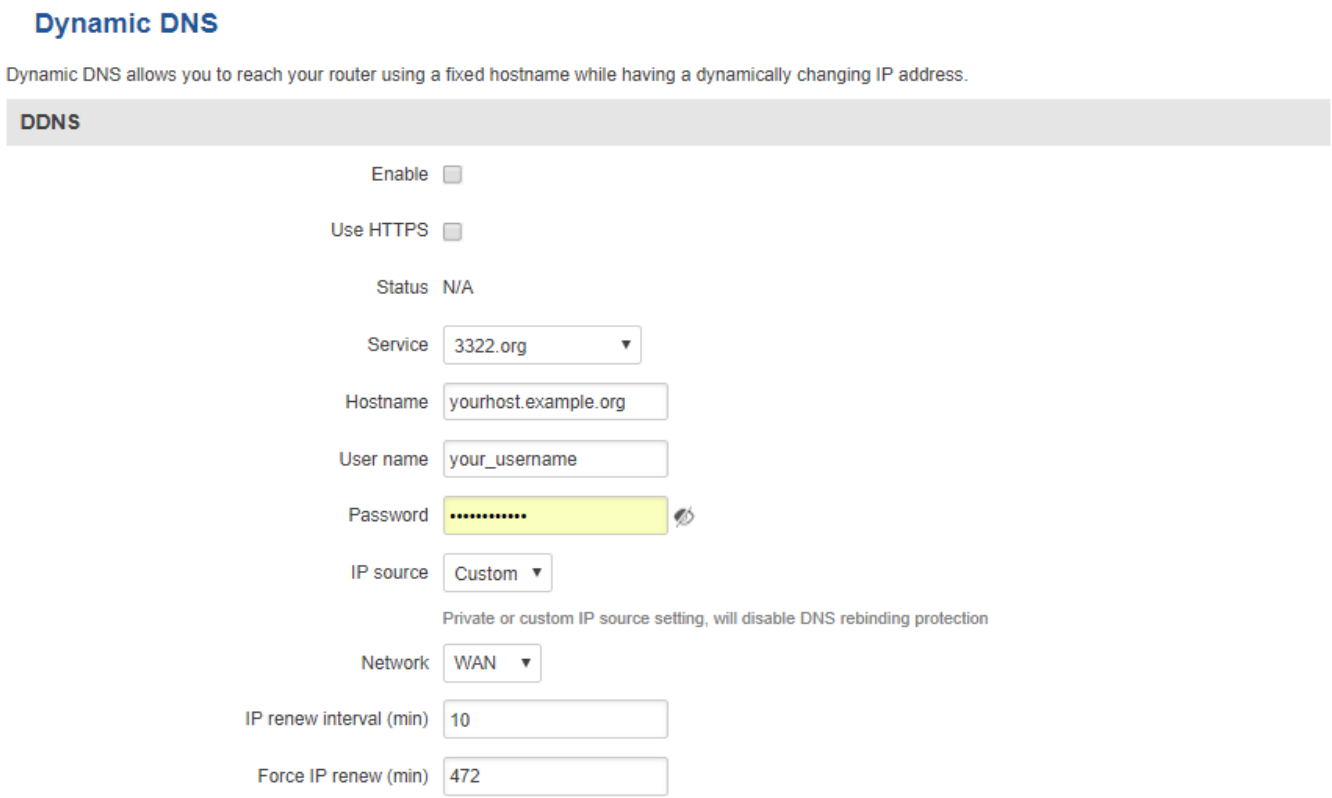


	Field name	Explanation
1.	Enable	Check to enable the L2TP Tunnel instance
2.	Local IP	Local IP Address of your L2TP server
3.	Remote IP range begin	Beginning of the IP pool for connecting clients
4.	Remote IP range end	End of the IP pool for connecting clients
5.	Username	Client's username used for authentication to the L2TP (this) server
6.	Password	Client's password used for authentication to the L2TP (this) server

9.8 Dynamic DNS

Dynamic DNS (DDNS) is a domain name service allowing to link dynamic IP addresses to a static hostname. To start using this feature you must first register to a DDNS service provider (example list is given in description).

By default, an unconfigured DDNS will be present. Below is a picture of this instance. You can create more DDNS instances if you wish to do so.



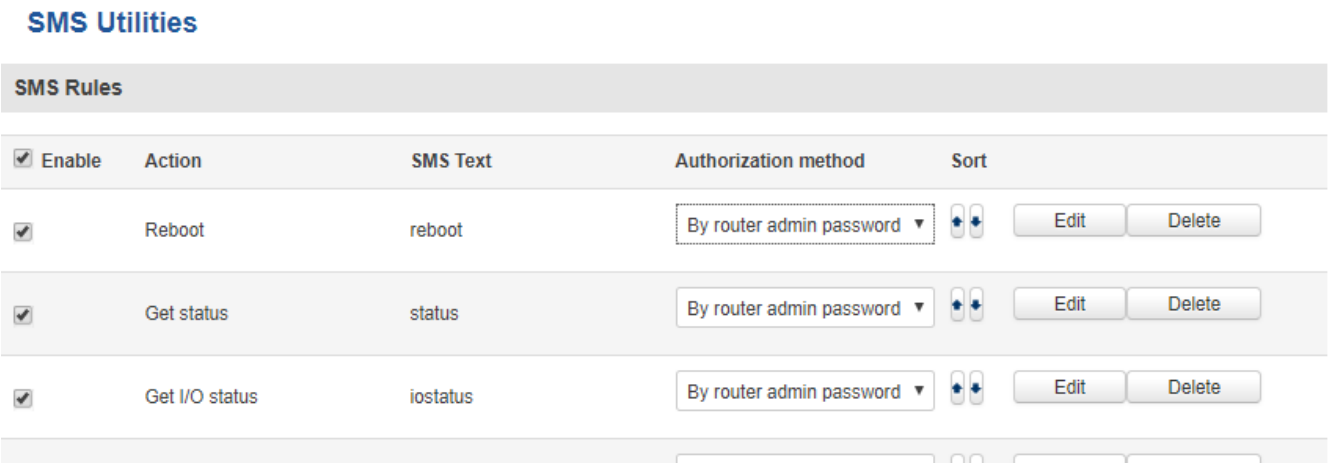
	Field name	Possible values	Explanation
1.	Enable	Checked / Unchecked	Enables current DDNS configuration.
2.	Use HTTPS	Checked / Unchecked	Enables SSL data encryption
3.	Status		Timestamp of the last IP check or update
4.	Service	1. dydns.org 2. no-ip.com 3. …	Your dynamic DNS service provider selected from the list. In case your DDNS provider is not present from the ones provided, please feel free to use "custom"
5.	Hostname	Any hostname	Domain name that will be linked with dynamic IP address
6.	Username	your_username	Name of the user account (from registration)
7.	Password	your_password	Password of the user account (from registration)
8.	IP Source	Public Private Custom	This option allows you to select a specific RUT interface and then send the IP address of that interface to the DDNS server. So if, for example, your RUT has a 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
9.	Network	WAN / WAN2 / WAN3 / LAN / PPP	Source network
10.	IP renew interval (min)	5 – 600000	Time interval to check if the IP address of the device has changed
11.	Force IP renew (min)	5 - 600000	Time interval to force IP address renew

9.9 SMS Utilities

RUT955 has an extensive amount of various SMS Utilities. The SMS Utilities section is subdivided into 6 subsections: SMS Utilities, Call Utilities, User Groups, SMS Management, Remote Configuration and Statistics.

9.9.1 SMS Utilities

The SMS Utilities tab contains a list of rules that perform certain actions when they are activated by SMS messages.



The figure above is an illustration of the SMS Utilities rules list. The entire list contains 26 rules but you are also be provided with the possibility to configure custom ones.

All default configuration options are listed below:

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

How to execute a rule:

To execute a rule, just send an SMS message to the router's SIM card number with the rules' **SMS Text**, e.g., if you send a message with the text **"reboot"**, the router will reboot provided the selected Authorization method is **"No authorization"**. However, if there is an Authorization method present you will need to include the **"Authorization key"** in the text message. This **"Authorization key"** depends on the chosen Authorization method, i.e.., if the method is **"By serial"**, the **"Authorization key"** is the router's serial number, if the method is **"By router admin password"**, the **"Authorization key"** is the router's admin password. The authorization **"key"** must precede the activation text and they must be separated by a **space**. For example, if the chosen Authorization method is **"By router admin password"** and the password is **"admin01"**, the entire message should look like this: **"admin01 reboot"**. The same applies to **"By serial"** authorization.

9.9.1.1 Default SMS Rules

In this section you will be provided with a table containing all of the default rules and explanations for them.

	Field name	Explanation	Notes
1.	**Reboot**		
	Enable	This check box will enable or disable SMS reboot function	Allows router restart via SMS
	Action	The action to be performed when this rule is met	
	SMS text	SMS text that will trigger the rule. In this case, reboot the router	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number
	Get status via SMS after reboot	Check this to receive connection status via SMS after the reboot	If checked, the router will send a status message once it has rebooted and is operational again. This is both a separate SMS Rule and an option under the SMS Reboot rule. After checking this, the „Send status SMS to other number" field will become available
	Send status SMS to other number	Enable this if you want the status message to be sent to another (other than the sender) number (s)	If this is checked, you will be prompted to enter a phone number (s) This field appears only if you have checked „Get status via SMS after reboot"
	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	This check box will enable or disable SMS status function	Allows you to get the router's status via SMS. This is both a separate SMS Rule and an option under the SMS Reboot rule
	Action	The action to be performed when this rule is met	
	SMS text	SMS text that will trigger the rule. In this case, send you the router's status	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password.
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number
	Send status SMS to other number	Enable this if you want the status message to be sent to another (other than the sender) number (s)	If this is checked, you will be prompted to enter a phone number (s)
	Message text	Which status information should be included in the SMS: Data state, Operator, Connection type, Signal Strength, Connection State, IP	You can select which status elements the message will contain

3.	**Get I/O status**		
	Enable	This check box will enable or disable SMS I/O status function	Allows you to get the router‘s I/O status via SMS
	Action	The action to be performed when this rule is met	
	SMS text	SMS text that will trigger the rule. In this case, send you the router‘s I/O status	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password.
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number
	Send status SMS to other number	Enable this if you want the status message to be sent to another (other than the sender) number (s)	If this is checked, you will be prompted to enter a phone number (s)
4.	**Get OpenVPN status**		
	Enable	This check box will enable or disable the OpenVPN status function	Allows to get the router‘s OpenVPN status via SMS
	Action	The action to be performed when this rule is met	
	SMS text	SMS text that will trigger the rule. In this case, send you the router‘s OpenVPN status	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number
	Send status SMS to other number	Enable this if you want the status message to be sent to another (other than the sender) number (s)	If this is checked, you will be prompted to enter a phone number (s)
5.	**Switch WiFi On/Off**		
	Enable	This check box will enable or disable the Switch WiFi function	Allows Wi-Fi control via SMS
	Action	The action to be performed when this rule is met	Turns WiFi On or Off
	SMS text	SMS text that will trigger the rule. In this case, turn Wi-Fi On/Off	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number
	Write to config	Permanently saves Wi-Fi state	With this setting enabled, the router will keep the new Wi-Fi state even after reboot. If it is not selected, the router will revert the Wi-Fi state after reboot

6.	**Switch mobile data on/off**		
	Enable	This check box will enable or disable the Switch mobile data 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 that will trigger the rule. In this case, turn mobile data On/Off	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number
	Write to config	Permanently saves mobile network state	With this setting enabled, the router will keep the new mobile data state even after reboot. If it is not selected, the router will revert the mobile data state after reboot
7.	**Manage OpenVPN**		
	Enable	This check box will enable or disable the Manage OpenVPN function	Allows OpenVPN control via SMS
	Action	The action to be performed when this rule is met	Turn OpenVPN On or Off
	SMS text	SMS text that will trigger the rule. In this case, turn OpenVPN On/Off	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter **After the SMS text you have to write OpenVPN instance's name**
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all numbers, From group or from Single number
8.	**Change mobile data settings**		
	Enable	This check box will enable or disable the Change mobile data settings function	Allows you to change mobile settings via SMS
	Action	The action to be performed when this rule is met	
	SMS text	SMS text that will trigger the rule. In this case, change the specified mobile data settings	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter. **Detailed explanations on how to use this function will be presented in the table below**
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed 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
2.	dialnumber=	e.g., *99***1#	Sets dial number
3.	auth_mode=	none pap chap	Sets authentication mode
4.	service=	Auto 4gonly 3gonly 2gonly	Sets the mobile service mode
5.	username=	e.g., user	Used only if PAP or CHAP authorization is selected
6.	password=	e.g., pass	Used only if PAP or CHAP authorization is selected

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

Example: *cellular apn=internet.gprs dialnumber=*99***1# auth_mode=pap service=3gonly username=user password=user*

	Field name	Explanation	Notes
9.	**Get list of profiles**		
	Enable	This check box will enable or disable the Get list of profiles function	Allows you to get the list of profiles via SMS
	Action	The action to be performed when this rule is met	
	SMS text	SMS text that will trigger the rule. In this case, send you The list of profiles	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number
10.	**Change profile**		
	Enable	This check box will enable or disable the Change profile function	Allows changing profiles via SMS
	Action	The action to be performed when this rule is met	
	SMS text	SMS text that will trigger the rule. In this case, send change profile	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter. **After the SMS text you have to write OpenVPN instance's name**
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number

11.	**SSH access Control**		
	Enable	This check box will enable or disable the SSH access control function	Allows SSH access control via SMS
	Action	The action to be performed when this rule is met	
	SMS text	SMS text that will trigger the rule. In this case, turn SSH access On/Off	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number
	Enable SSH access	Enable this to reach the router via SSH from LAN	If this is checked, SMS will enable SSH access from LAN, if not, SMS will disable SSH access from LAN
	Enable remote SSH access	Enable this to reach the router via SSH from WAN	If this is checked, SMS will enable SSH access from WAN, if not, SMS will disable SSH access from WAN
12.	**Web access Control**		
	Enable	This check box will enable or disable the Web access control function	Allows web access control via SMS
	Action	The action to be performed when this rule is met	
	SMS text	SMS text that will trigger the rule. In this case, turn web access On/Off	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number
	Enable HTTP access	Enable this to reach router via HTTP from LAN	If this is checked, SMS will enable HTTP access from LAN, if not, SMS will disable HTTP access from LAN
	Enable remote HTTP access	Enable this to reach router via HTTP from WAN	If this is checked, SMS will enable HTTP access from WAN, if not, SMS will disable HTTP access from WAN
	Enable remote HTTPS access	Enable this to reach router via HTTPS from WAN	If this is checked, SMS will enable HTTPS access from WAN, if not, SMS will disable HTTPS access from WAN
13.	**Restore to default**		
	Enable	This check box will enable or disable the Restore to default function	Allows you to restore the router to its default settings via SMS
	Action	The action to be performed when this rule is met	Router will reboot after this rule is executed and all configurations will be deleted
	SMS text	SMS text that will trigger the rule. In this case, restore the router to its default settings	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number

14.	**Force SIM switch**		
	Enable	This check box will enable or disable the Force SIM switch function	Allows SIM switch via SMS
	Action	The action to be performed when this rule is met	
	SMS text	SMS text that will trigger the rule. In this case, force a SIM switch	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number
15.	**GPS coordinates**		
	Enable	This check box will enable or disable the GPD coordinates function	Allows you to get GPS coordinates via SMS
	Action	The action to be performed when this rule is met	
	SMS text	SMS text that will trigger the rule. In this case, send GPS coordinates	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number
16.	**GPS**		
	Enable	This check box will enable or disable the GPS On/Off function	Allows you to control GPS via SMS
	Action	The action to be performed when this rule is met	Turn GPS On or Off
	SMS text	SMS text that will trigger the rule. In this case, turn GPS On/Off	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all uers, From group or From single number
17.	**Force FW upgrade from server**		
	Enable	This check box will enable or disable the FW upgrade from server function	Allows you to upgrade the router's FW via SMS
	Action	The action to be performed when this rule is met	Router will reboot after this rule is executed
	SMS text	SMS text that will trigger the rule. In this case, force a FW upgrade from server	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number

18.	**Force Config update from server**		
	Enable	This check box will enable or disable the Config update from server function	Allows you to upgrade the router's configurations via SMS
	Action	The action to be performed when this rule is met	The router will reboot after this rule is executed
	SMS text	SMS text that will trigger the rule. In this case, force a configuration update from server	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number
19.	**Switch monitoring on/off**		
	Enable	This check box will enable or disable the Switch monitoring function	Allows you to control monitoring status via SMS
	Action	The action to be performed when this rule is met	Turn monitoring On or Off
	SMS text	SMS text that will trigger the rule. In this case, switch monitoring On/Off	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number
20.	**Monitoring status**		
	Enable	This check box will enable or disable the Monitoring status function	Allows you to get monitoring status via SMS
	Action	The action to be performed when this rule is met	
	SMS text	SMS text that will trigger the rule. In this case, send monitoring status	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number

21.	**UCI API**		
	Enable	This check box will enable or disable the UCI API function	Allows you to set or get any configurations from the router
	Action	The action to be performed when this rule is met	
	SMS text	SMS text that will trigger the rule. In this case, set/send router parameters	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number
22.	**Switch output on / off**		
	Enable	This check box will enable or disable the Switch output function	Allows output control via SMS
	Action	The action to be performed when this rule is met	Turn output On or Off
	Active timeout	Rule active for a specific time, format - seconds	
	SMS text	SMS text that will trigger the rule. In this case, switch output on/off	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matter
	Authorization method	What kind of authorization to use for SIM management	No authorization, By serial or By router admin password
	Allowed users	Whitelist of allowed users	From all numbers, From group or From single number
	Output type	Which output (Digital OC output or Relay output) will be activated	

UCI via SMS parameters:

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

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

Important Notes:

- Mobile settings must be configured correctly. If SIM card has a PIN number you must enter it at "Network" > "3G" settings. Otherwise SMS reboot function will not work.
- Sender's phone number must contain country code. You can check sender's phone number format by reading the details of old SMS text messages on your phone.

9.9.1.2 Custom SMS Rules

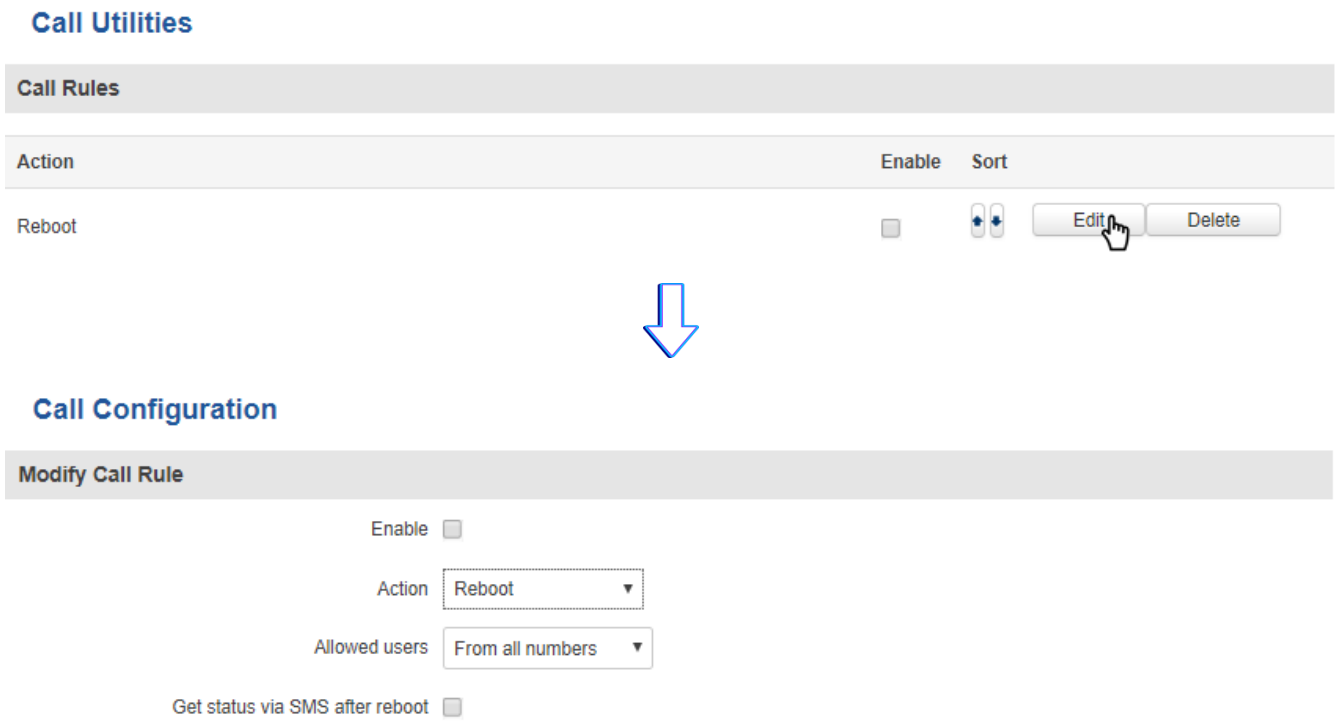
Apart from the default rules, you can also configure custom ones. To do so, go to the bottom of the SMS Utilities page. There you will find the **"New SMS Rule"** tab. Select an **Action** and press the **"Add"** button located next to it.

The configuration of these custom rules is the same as the configuration of default rules. Therefore, the instructions found in the section above apply here as well.

9.9.2 Call Utilities

Just like SMS Utilities, Call Utilities provide you with the possibility to issue certain commands to the router from your mobile phone. The list of possible rules is of course shorter because you can only make one type of call. Keep that in mind when creating Call Utilities rules because one call will trigger all of the enabled rules at once.

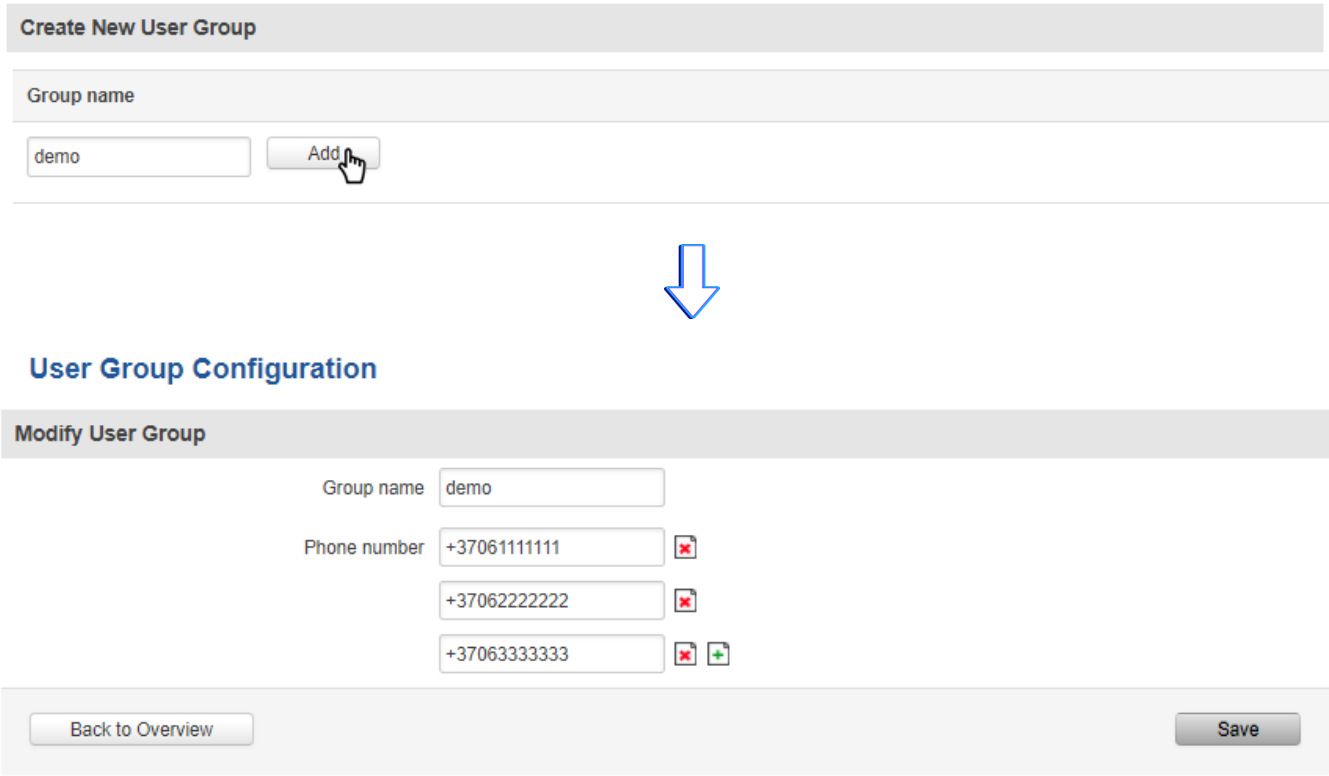
There is only one default rule (Reboot) configured and it is disabled. To make a new rule click the **"Edit"** button located next to the one default rule (as shown in the example below) or make an entirely new entry for you Call Rules list by adding a rule from the **New Call Rule** tab.



	Field name	Possible values	Explanation
1.	Enable	Checked / Unchecked	Enables the rule
2.	Action	Reboot / Get Status / Turn WiFi on/off / Turn mobile data on/off / Turn Output on/off	Action to be taken after receiving a call
3.	Allowed users	From all numbers / From group / From single number	Limits action triggering. If **From group** is checked, you will prompted to select a **User Group** (you will information on how to configure User Groups in the 9.9.3 section of this document). If **From single number** is selected, you will be prompted to enter the sender's number
4.	Get status via SMS after reboot	Checked / Unchecked	Enables automatic message sending with router status information after reboot. If this is checked, you will be prompted to enter recipient's phone number

9.9.3 User Groups

User Groups provides you with the possibility to group phone numbers for SMS management purposes. You can then later use these groups in all related SMS and call functionalities. This option helps if there are several Users who should have same roles when managing the router via SMS or calls. You can create new user group by entering a name in the **Group name** text field and clicking the **"Add"** button located next to it in the **"Create New User Group"** section. After this you will re redirected get to the **"Modify User Group"** section.



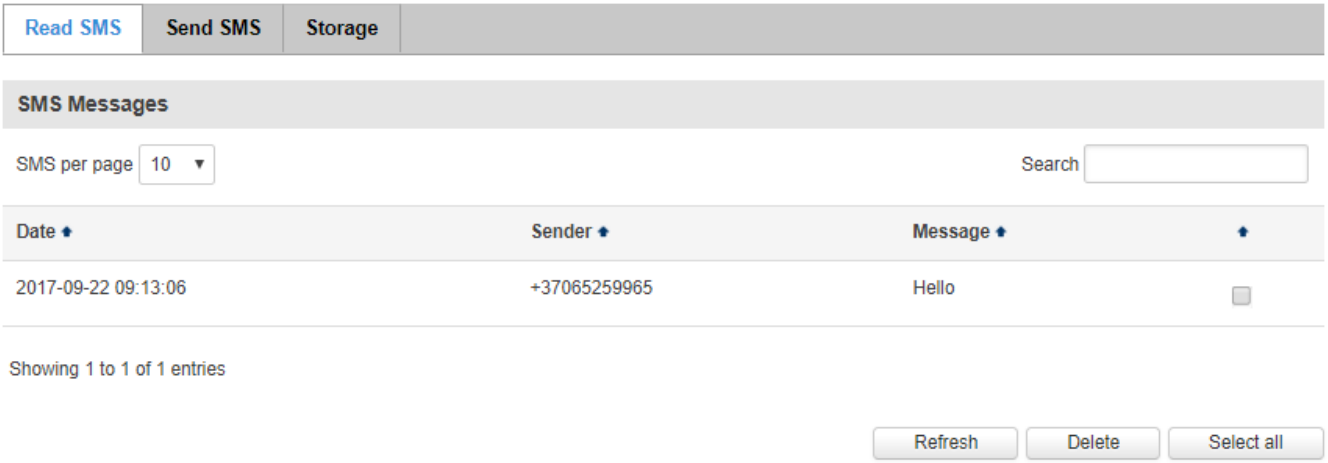
	Field name	Sample	Explanation
1.	Group name	demo	Name of the group of phone numbers. Used for easier management purposes
2.	Phone number	+37061111111, +37062222222, +37063333333	Add numbers to the user group. Must match international format. You can add more phone numbers fields by clicking on the green "+" symbol

9.9.4 SMS Management

With the help of the SMS Management tab you can read and send SMS messages.

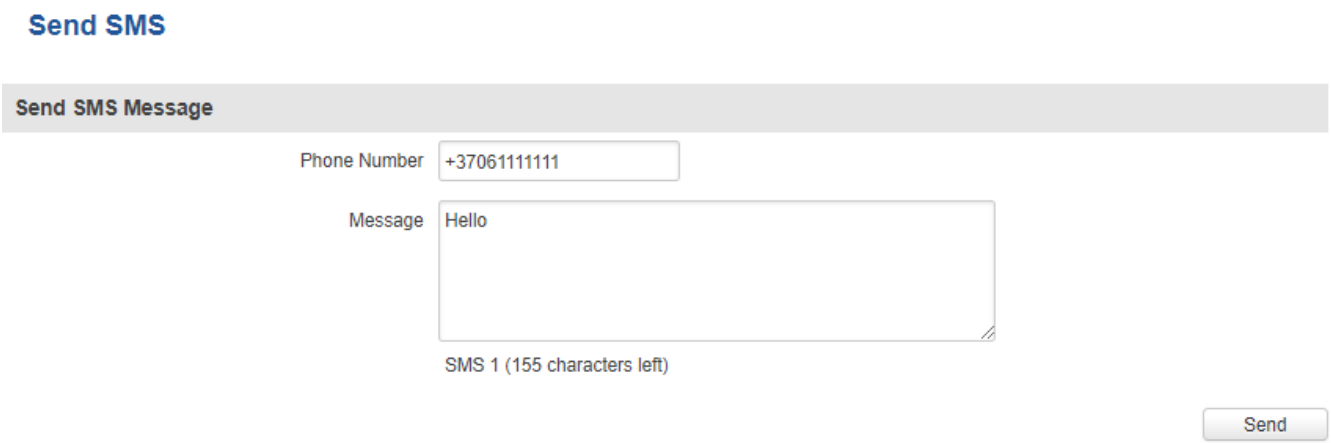
9.9.4.1 Read SMS

In the Read SMS page you can read and delete received/stored SMS messages. The layout is simple, there is a list of received SMS messages and you can choose how many entries of that list should visible at one time with **SMS per page** drop box in the top left corner of the page and there is a **Search** field to help you navigate more efficiently through the list of messages in the top right corner of the page.



9.9.4.2 Send SMS

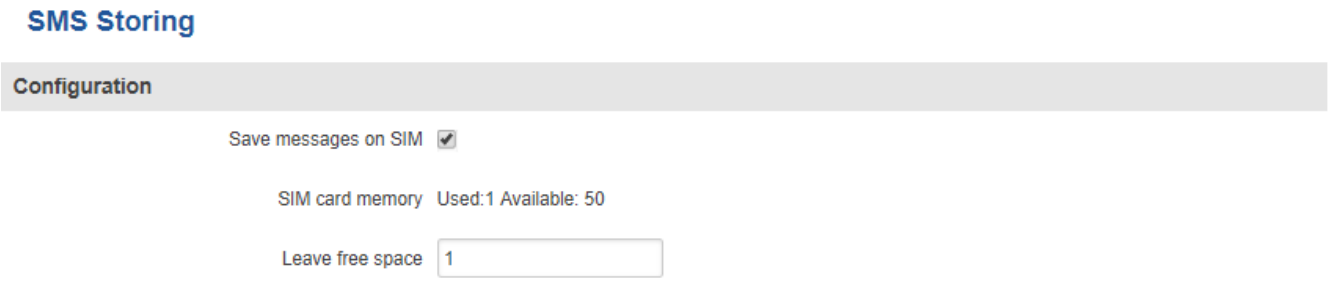
The Send SMS page lets you send SMS messages from the router's SIM card.



All you have to do is enter the recipient's phone number, type in your message and hit the **"Send"** button. If everything went well, a green bar saying "Message sent" should appear.

9.9.4.3 Storage

The Storage tab shows you how much SIM card memory space is used and how much is available. You can also chose the option for the router to not delete messages. If this option is not used, the router will automatically delete all incoming messages after they have been read. Message status "read/unread" is examined every 60 seconds. All "read" messages are deleted.



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

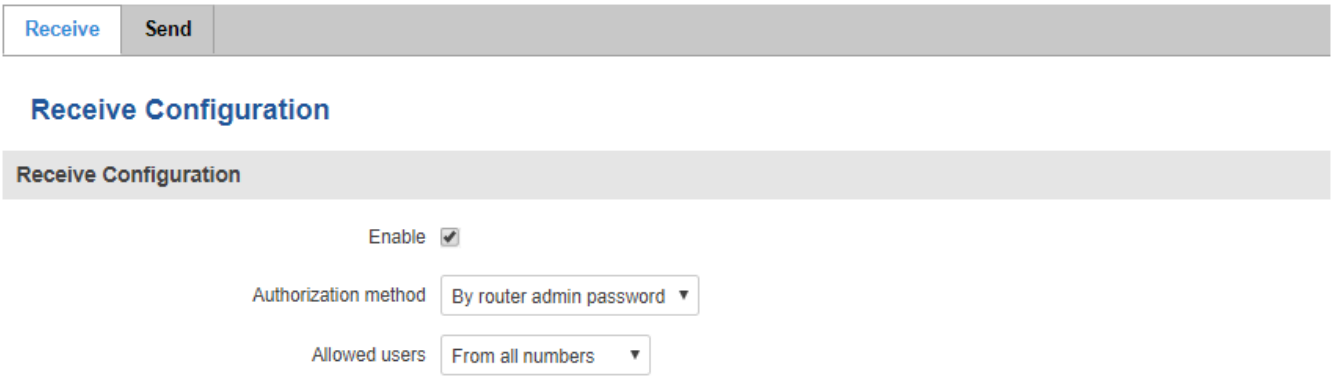
9.9.5 Remote Configuration

RUT955 can be configured via SMS from another RUTxxx router. You only have to select which configuration details have to be sent and type in the phone number of the other router. The router will then generate the SMS Text needed for the configurations to be applied.

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

9.9.5.1 Receive configuration

This section controls how the configuration initiation party should identify itself. In this scenario RUT955 itself is being configured.

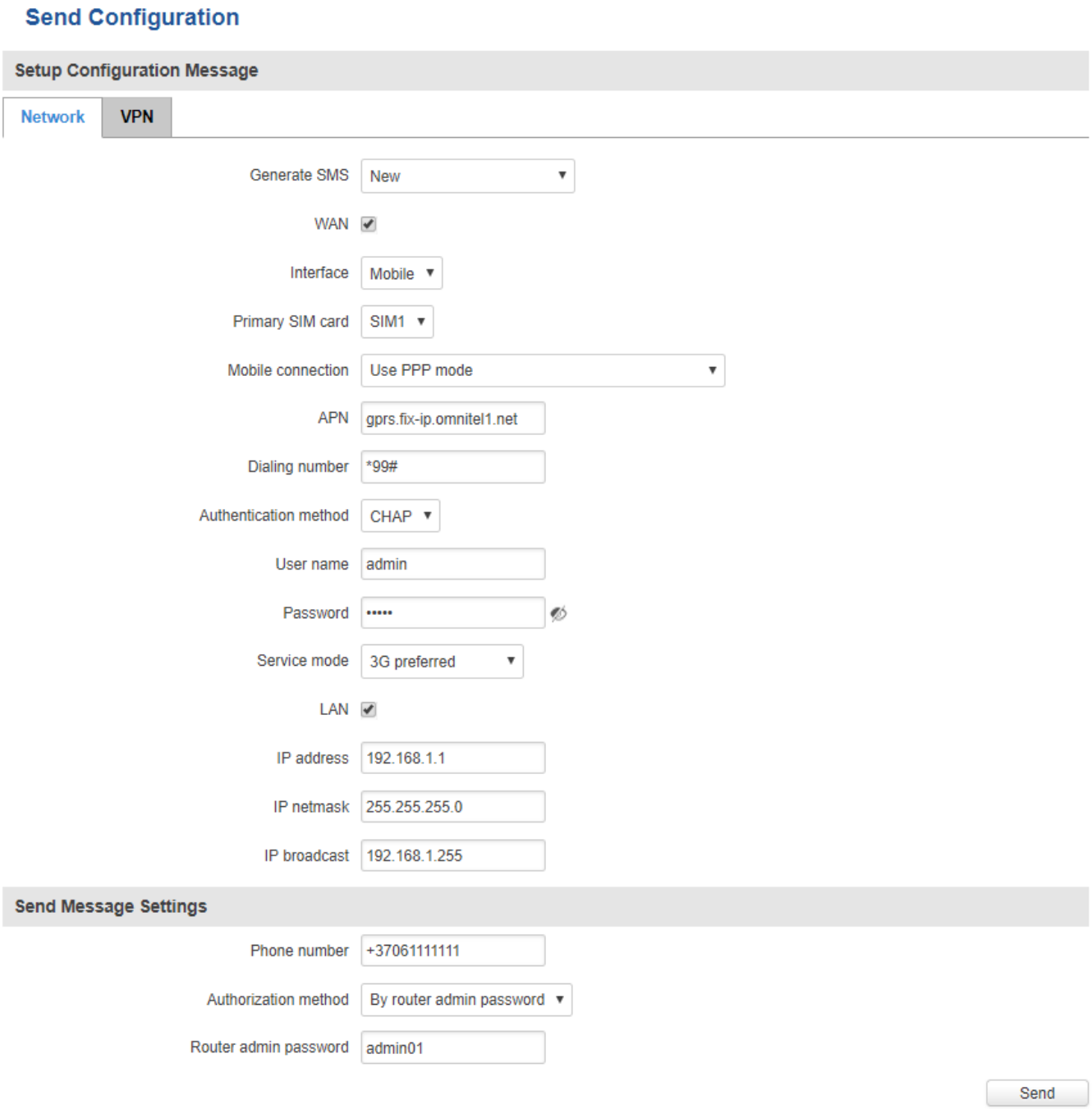


	Field name	Values	Notes
1.	Enable	Checked / Unchecked	Enables the router to receive configuration
1.	Authorization method*	No authorization / By serial / By router admin password	Describes what kind of authorization to use for SMS management. Methods of the Receiving and Sending ends must match
2.	Allowed users	From all numbers From group From single number	What numbers are allowed to send configurations

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

9.9.5.2 Send configuration

This section lets you configure remote RUTxxx devices. The authorization settings must match those that are set on the receiving party. An example of how sending a new network configuration with both WAN and LAN settings looks is presented below.



	Field name	Values	Notes
	Setup configuration message		
1.	Generate SMS	New / From current configuration	Generate new SMS settings or use current device configuration
2.	WAN	Checked / Unchecked	Include configurations for WAN (Wide Area Network)
3.	Interface	Mobile / Wired	Interface type used for WAN (Wide Area Network) connection
4.	Primary SIM card	SIM1 / SIM2	SIM card that will be used as primary
5.	Mobile connection	PPP / NDIS / NCM / QMI	An underlying agent that will be used for mobile data connection creation and management
6.	APN	Operator's APN	(APN) is the name of a gateway between a GPRS or 3G mobile networks and another computer network, frequently the public Internet
7.	Dialing number	*99#	A phone number that will be used to establish a mobile PPP (Point-to-Point Protocol) connection
8.	Authentication method	CHAP / PAP / None	Select an authentication method that will be used to authenticate new connections on your GSM carrier's network
9.	User name	"admin"	User name used for authentication on your GSM carrier's network
10.	Password	"•••••"	Password used for authentication on your GSM carrier's network
11.	Service mode	Auto 4G (LTE) only 3G only 2G only	Your network's preference. If your local mobile network supports GSM (2G), UMTS (3G) or LTE (4G) you can specify to which network you prefer to connect to
12.	LAN	Enable/Disable	Include configurations for LAN (Local Area Network)
13.	IP address	"192.168.1.1"	IP address that the remote router will use on LAN
14.	IP netmask	"255.255.255.0"	A subnet mask that the remote router will use to define how large the LAN network is
15.	IP broadcast	"192.168.1.255"	A logical address at which all devices connected to a multiple-access communications network are enabled to receive datagrams
	Send Message Settings		
16.	Phone number	"+37061111111"	Phone number of the router that will receive the configuration
17.	Authorization method	No authorization By serial By router admin password	What kind of authorization to use for remote configuration

This is an example of only one scenario but you can also send different Network and VPN settings. The settings being sent are the same as they would be configured on your router locally, therefore, you can find information on what different Network and VPN parameters do in 7 and 9.7 sections of this document.

9.9.6 Statistics

The Statistics page represents sent and received SMS numbers.

Statistics

SMS Statistics

SIM Card	Sent SMS	Received SMS	
SIM 1	4	1	Reset
SIM 2	0	0	Reset

9.10 SNMP

Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from, and configuring, network devices.

9.10.1 SNMP Settings

SNMP Configuration

SNMP Service Settings

Enable SNMP service ☐

Enable remote access ☐

Port 161

Community Public

Location Location

Contact email@example.com

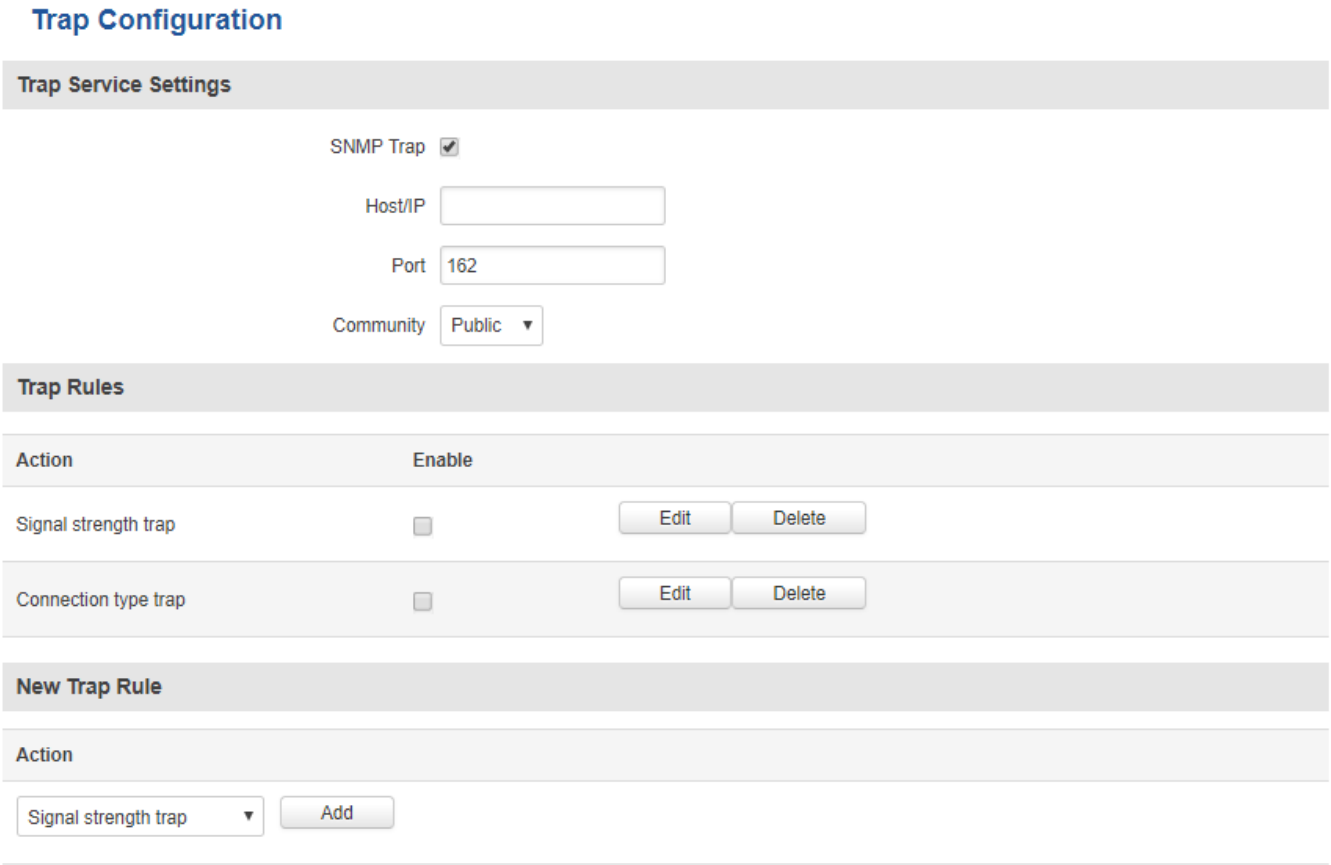
Name Name

	Field name	Possible values	Explanation
1.	Enable SNMP service	Checked / Unchecked	Run SNMP service on system start up
2.	Enable remote access	Checked / Unchecked	Open a port in firewall so that the SNMP service may be reached from WAN
3.	Port	0 - 65535	SNMP service port
4.	Community	Public / Private / Custom	The SNMP Community is an ID that allows access to a router's SNMP data
6.	Location	Location	Trap named sysLocation
7.	Contact	Email address	Trap named sysContact
8.	Name	Any name	Trap named sysName

SNMP Variables/OID

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

9.10.2 TRAP Settings



	Field name	Possible values	Explanation
1.	SNMP Trap	Checked / Unchecked	Enables SNMP trap functionality
2.	Host/IP	IP address or hostname	Host to transfer SNMP traffic to
3.	Port	0 – 65535	Port for trap's host
4.	Community	Public/Private	The SNMP Community is an ID that allows access to a router's SNMP data

9.11 SMS Gateway

9.11.1 Post/Get Configuration

Post/Get Configuration allows you to perform action requests by writing them in the URL after your device's IP address.

	Field name	Possible Values	Notes
1.	Enable	Checked / Unchecked	Enable SMS management functionality through POST/GET
2.	User name	Any username	User name used for authorization
3.	Password	Any password	Password used for authorization (default - user1)

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

9.11.1.1 SMS by HTTP POST/GET

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

9.11.1.2 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 strings are in capital letters inside curly brackets. Curly brackets ("{ }") are not needed when submitting HTTP POST/GET string.

9.11.1.3 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 the SMS message. 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 the router will respond with return status.

9.11.1.4 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

9.11.1.5 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

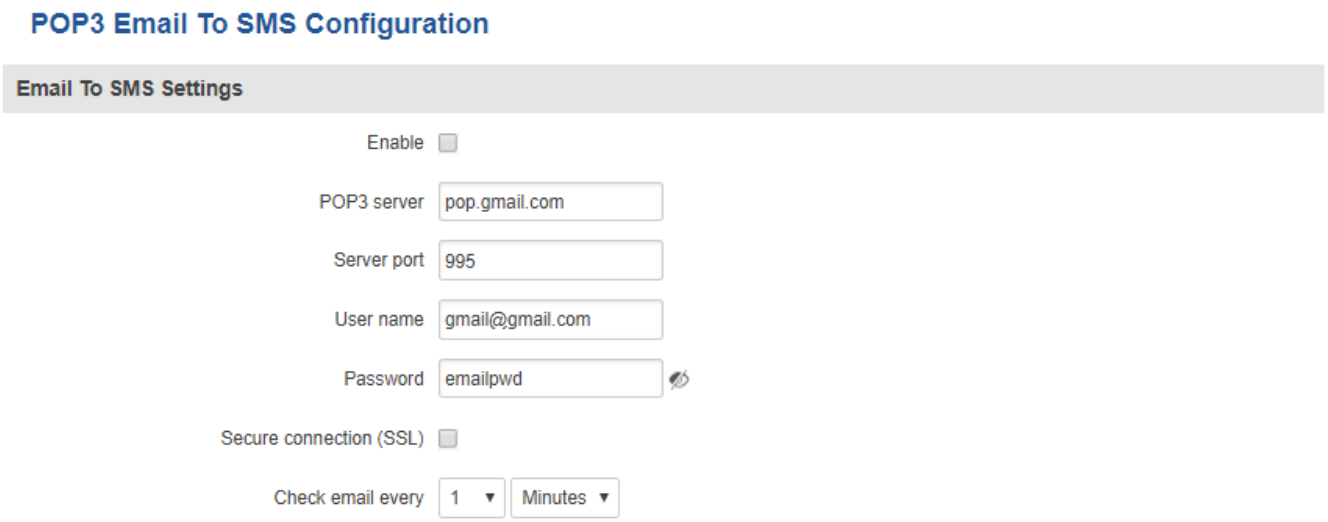
http://192.168.1.1/cgi-bin/sms_delete?username=admin&password=admin01&number=4

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

9.11.2 Email to SMS

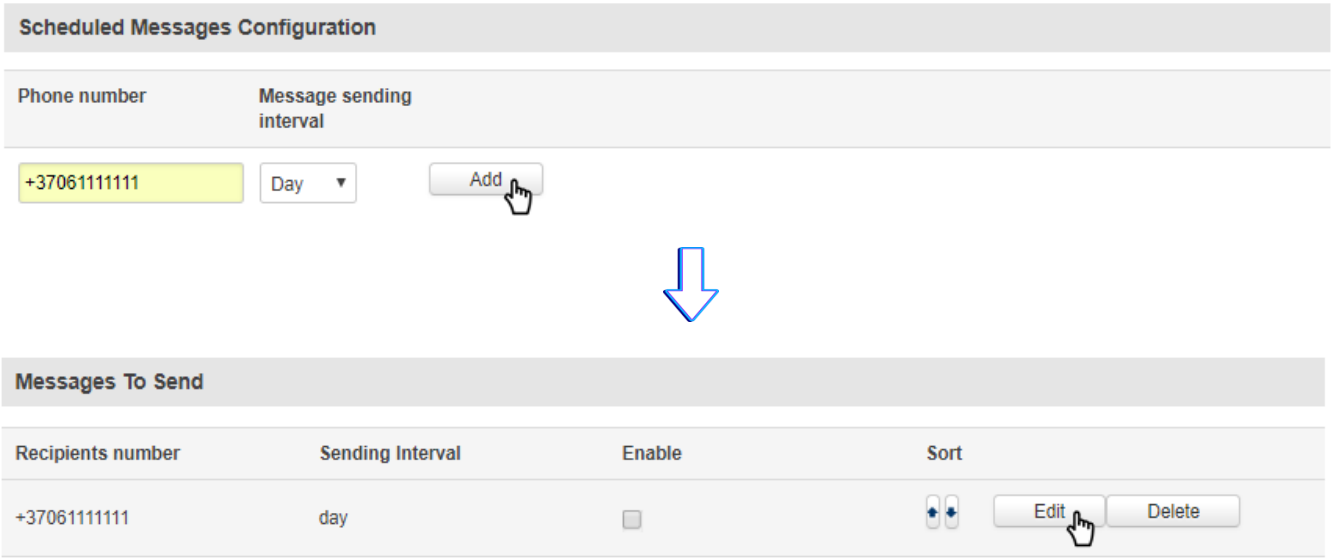
Email to SMS is a function that checks your email's inbox after a specified amount of time and, if it finds any new received emails, it converts them to SMS messages.



	Field name	Values	Notes
1.	Enable	Checked / Unchecked	Allows to convert received Email to SMS
2.	POP3 server	"pop.gmail.com"	POP3 server address
3.	Server port	0 – 65535	Server authentication port
4.	User name	Any username	Your email account's user name
5.	Password	Any password	Your email account's password
6.	Secure connection (SLL)	Checked / Unchecked	(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

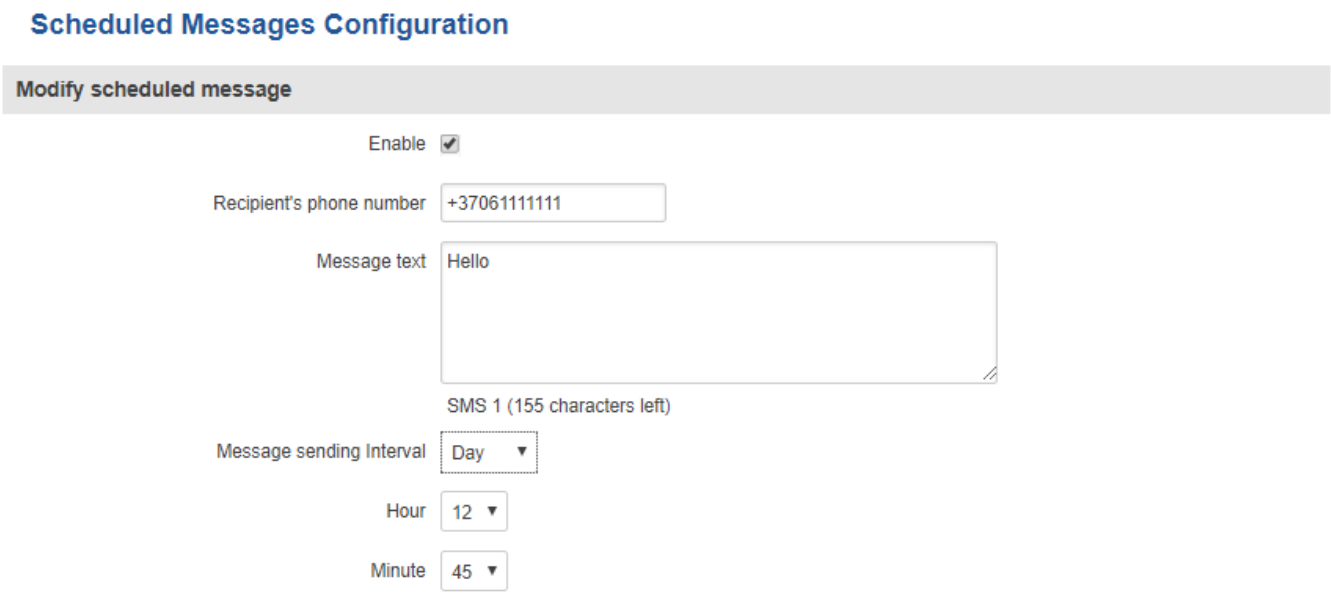
9.11.3 Scheduled Messages

Scheduled messages allow you to periodically send SMS messages to a specified number. Scheduled messages are managed in rule form, i.e., similar to Events Reporting, SMS Utilities, etc. Therefore, to configure a new Scheduled Message, we must first create a rule. To create a new rule, type in a phone number in the **Phone number** field located in the **"Scheduled Messages Configuration"** section and press the **"Add"** button located next to it.



After this your new rule will appear in the **"Messages To Send"** section. Apart from the phone number, the new rule will be disabled and unconfigured. To configure your rule, simply click the **"Edit"** button located next to it, as shown in the example above.

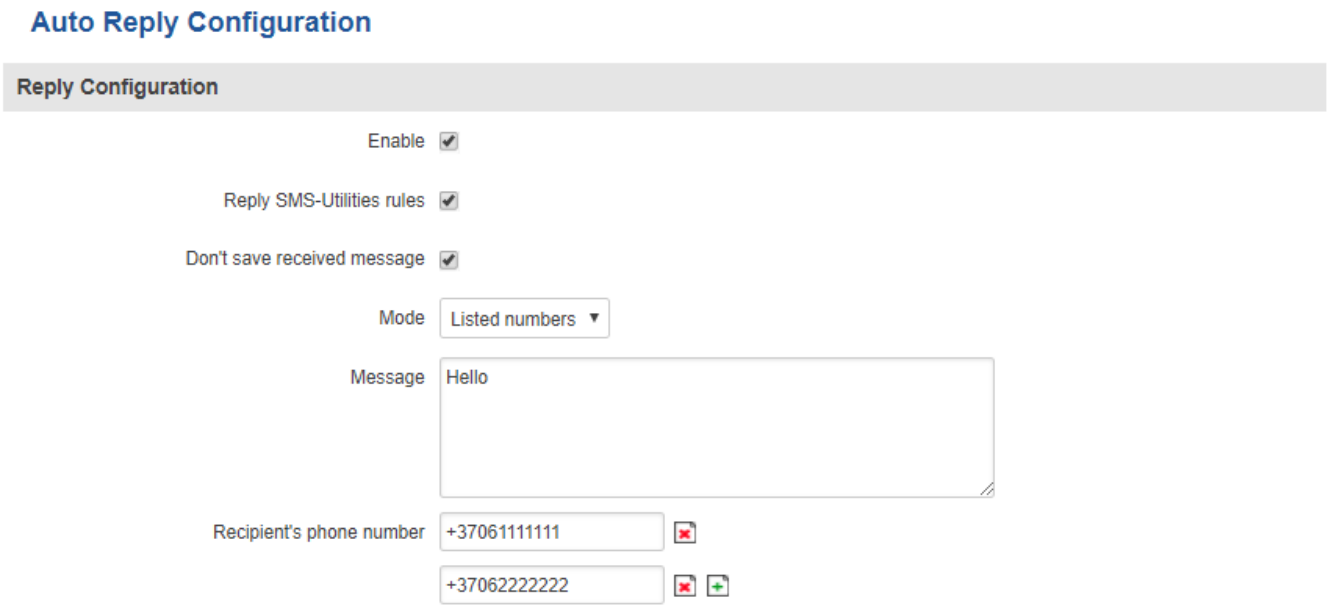
9.11.3.1 Scheduled Messages Configuration



	Field name	Possible values	Notes
1.	Enable	Checked/Unchecked	Activates periodical message sending
2.	Recipient's phone number	Any phone number	Phone number that will receive the scheduled messages
3.	Message text	Any text	Message that will be sent
4.	Message sending interval	Day / Week / Month / Year	Message sending period

9.11.4 Auto Reply

Auto reply allows you to configure automatic replying to SMS messages that the router receives from everyone or from listed numbers only.

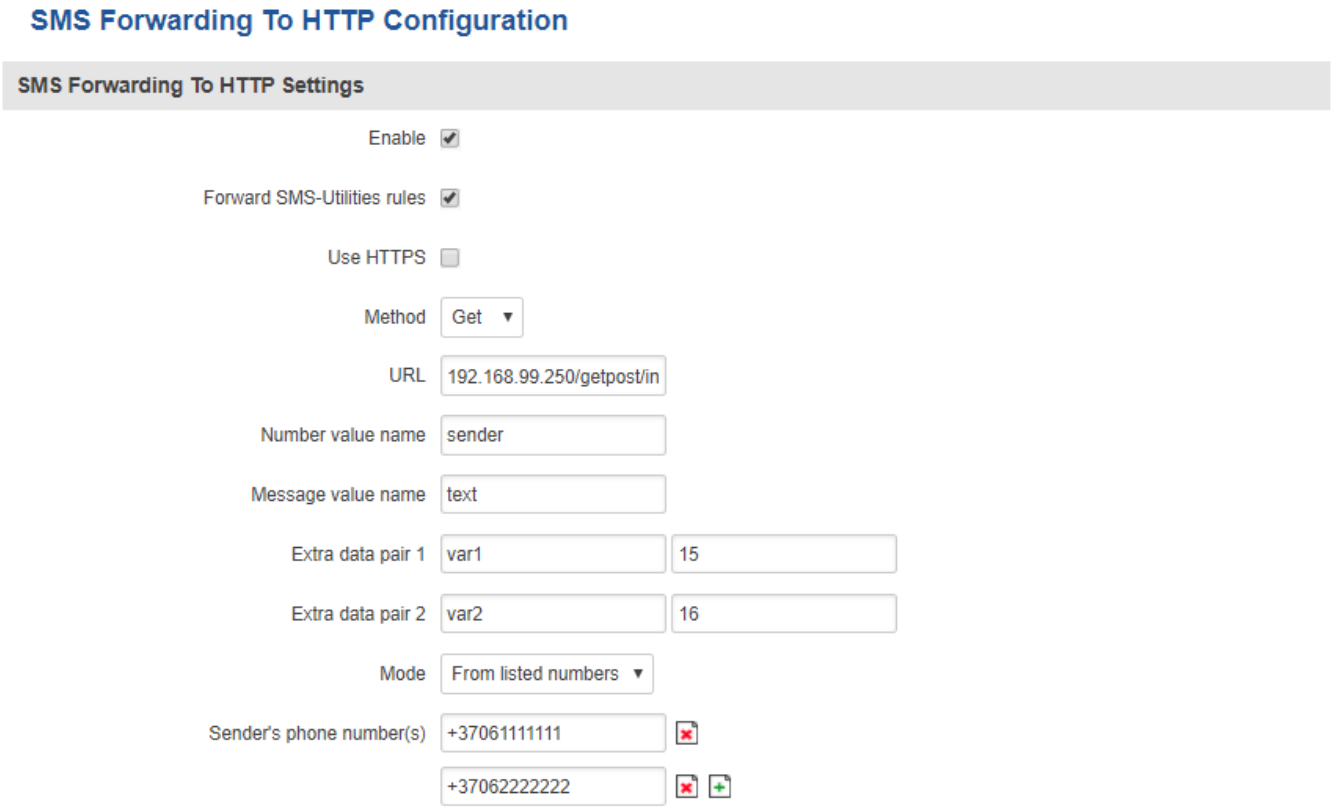


	Field name	Values	Notes
1.	Enable	Checked / Unchecked	Enable auto reply to every received mobile message
2.	Reply SMS-Utilities rules	Checked / Unchecked	If checked, the router will also auto reply to SMS Utilities rules
3.	Don't save received message	Checked / Unchecked	If enabled, received messages will not be saved
4.	Mode	Everyone / Listed numbers	Select which messages are to be auto replied to. Either all messages or ones from specified numbers
5.	Message	Any text message	Message text that will be sent in reply
6.	Recipient's phone number	Any phone number	Phone numbers to which an automatic reply will be sent to

9.11.5 SMS Forwarding

9.11.5.1 SMS Forwarding To HTTP

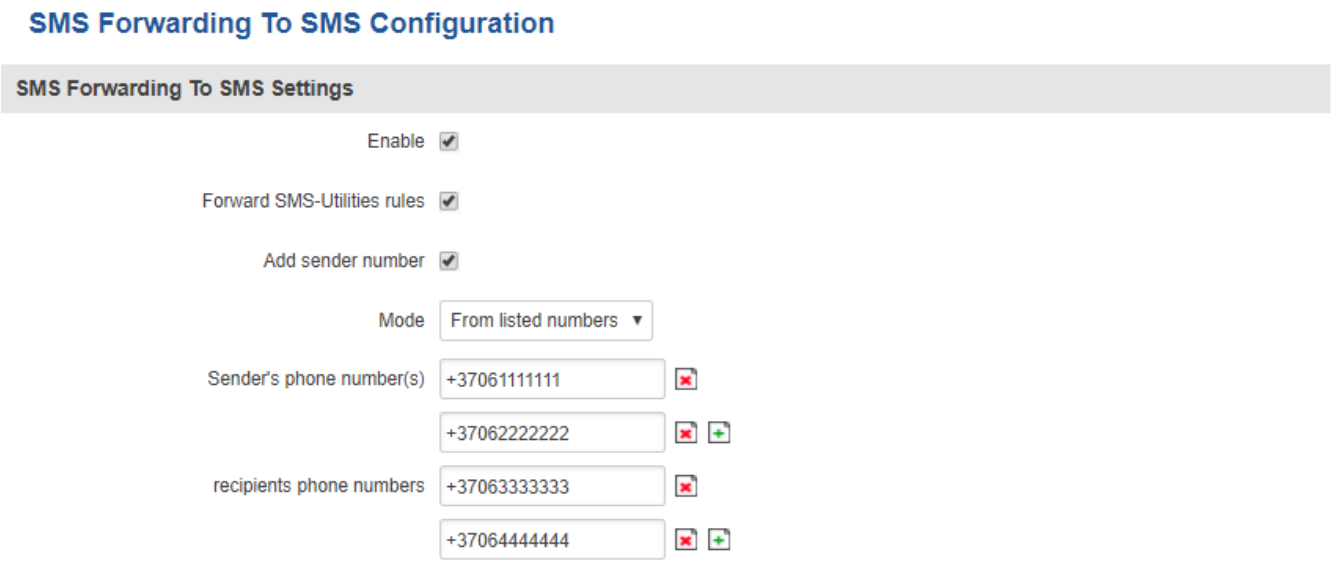
The SMS Forwarding To HTTP functionality forwards SMS messages to HTTP, using either POST or GET methods.



	Field name	Possible values	Notes
1.	Enable	Checked / Unchecked	Enable mobile message forwarding to HTTP
2.	Forward SMS-Utilities rules	Checked / Unchecked	If checked, the router will also forward SMS Utilities to HTTP
3.	Use HTTPS	Checked / Unchecked	Check to use HTTPS
4.	Method	Post / Get	Defines the HTTP transfer method
5.	URL	192.168.99.250/getpost/index.php	URL address to forward messages to
6.	Number value name	Any name	Name to assign for sender's phone number value in query string
7.	Message value name	Any text	Name to assign for message text value in query string
8.	Extra data pair 1	Var1 - 17	If you want to transfer some extra information through the HTTP query, enter variable name on the left field and its value on the right
9.	Extra data pair 2	Var2 – "go"	
10.	Mode	All messages / From listed numbers	Specifies which sender messages to forward
11.	Sender's phone number(s)	Any phone number(s)	Specifies from which phone numbers the SMS messages should be forwarded

9.11.5.2 SMS Forwarding to SMS

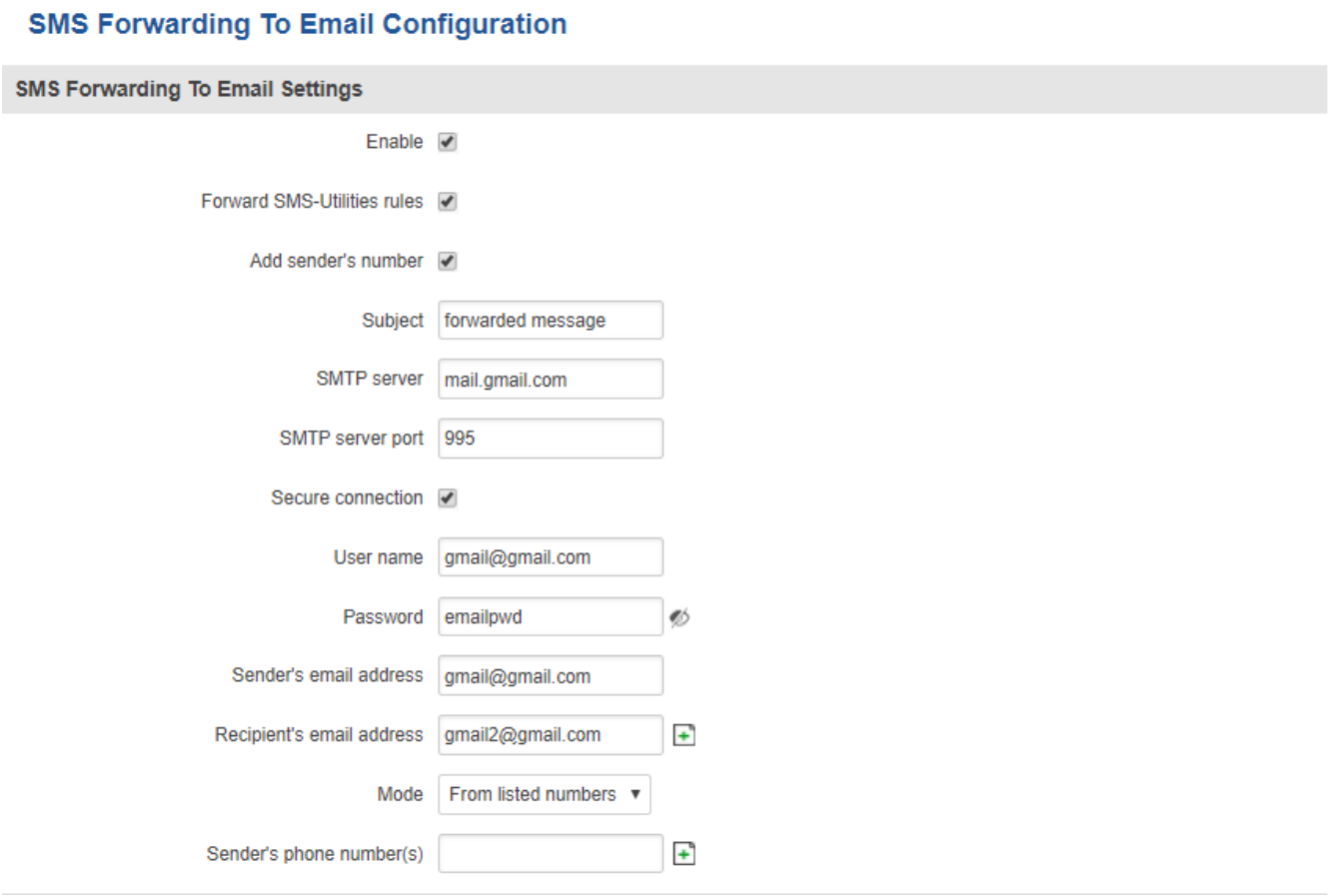
The SMS Forwarding To SMS function forwards SMS messages to one or several recipients.



	Field name	Values	Notes
1.	Enable	Checked / Unchecked	Enable mobile message forwarding
2.	Forward SMS-Utilities rules	Checked / Unchecked	If checked, the router will also forward SMS Utilities to SMS
3.	Add sender number	Checked / Unchecked	If enabled, original sender's number will be added at the end of the forwarded message
4.	Mode	All messages / From listed numbers	Specifies from which senders received messages are going to be forwarded.
5.	Sender's phone numbers(s)	Any phone number(s)	Specifies from which phone numbers SMS messages should be forwarded
6.	Recipient's phone numbers	Any phone number(s)	Phone numbers to which messages are going to be forwarded to

9.11.5.3 SMS Forwarding to Email

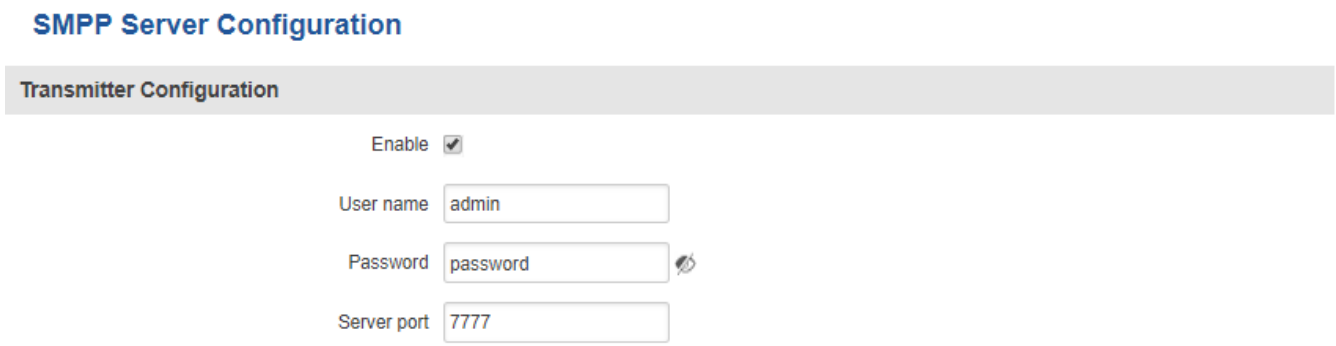
The SMS Forwarding To Email function forwards SMS messages to email.



	Field name	Possible values	Explanation
1.	Enable	Checked / Unchecked	Enable SMS message forwarding to email
2.	Forward SMS-Utilities rules	Checked / Unchecked	If checked, the router will also forward SMS Utilities to email
3.	Add sender number	Checked / Unchecked	If enabled, original sender's number will be added at the end of the forwarded message
4.	Subject	Any text	Text that will be inserted in the email's Subject field
5.	SMTP server	"mail.teltonika.lt"	Your SMTP server's address
6.	SMTP server port	0 – 65535	Your SMTP server's port number
7.	Secure connection	Checked / Unchecked	Enables the use of cryptographic protocols. Enable only if your SMTP server supports SSL or TLS
7.	User name	Any username	Your email account's login name
8.	Password	Any password	Your email account's password
9.	Sender's email address	Any email address	Your address that will be used to send emails from
10.	Recipient's email address	Any email address	Address that you want to forward your messages to
11.	Mode	All messages / From listed numbers	Choose which sender's messages are to be forwarded to email
12.	Sender's phone number(s)	Any phone number(s)	Specifies from which phone numbers SMS messages should be forwarded

9.11.6 SMPP

The Short Message Peer-to-Peer (SMPP) is a protocol used for exchanging SMS messages between Short Message Service Centers (SMSC) and/or External Short Messaging Entities (ESME)

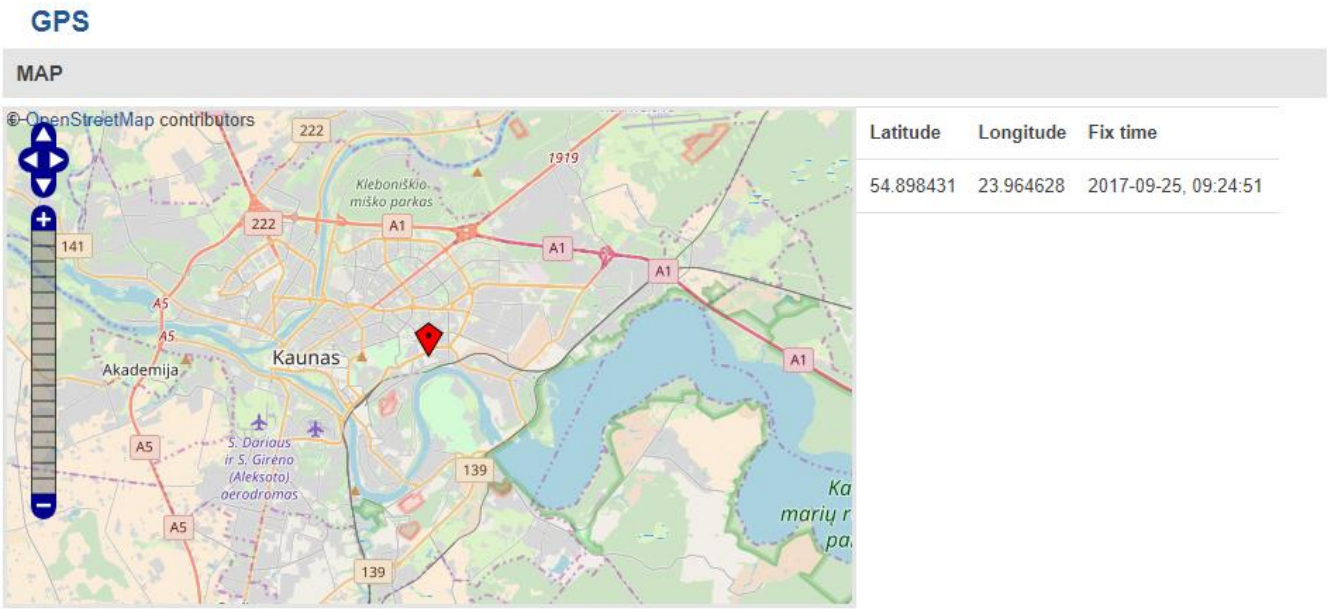


	Field name	Values	Explanation
1.	Enable	Checked / Unchecked	Enables SMPP server
2.	User name	Any username	User name for authentication on SMPP server
3.	Password	Any password	Password for authentication on SMPP server
4.	Server port	0 – 65535	A port that will be used for SMPP server communications

9.12 GPS

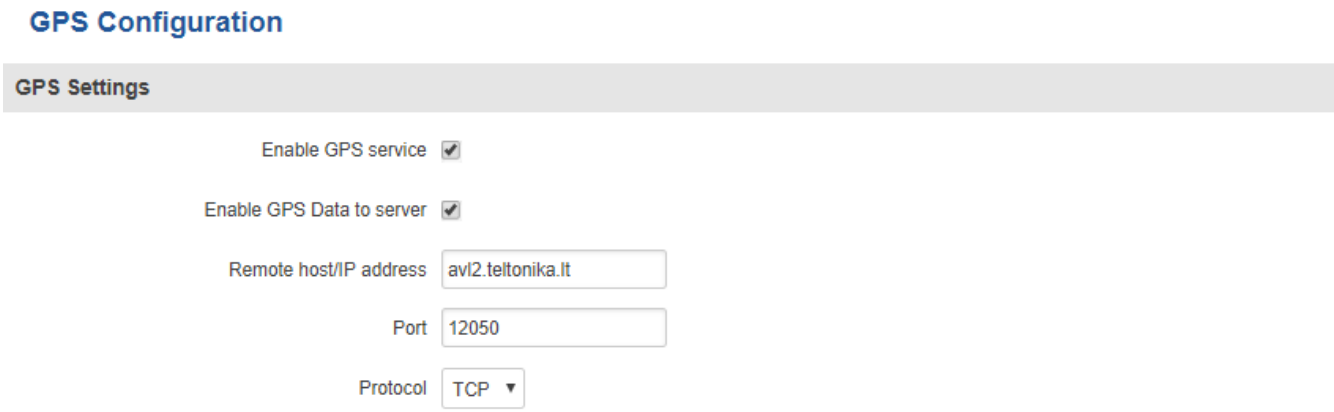
9.12.1 GPS

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



9.12.2 GPS Settings

This is the GPS parameter configuration window.

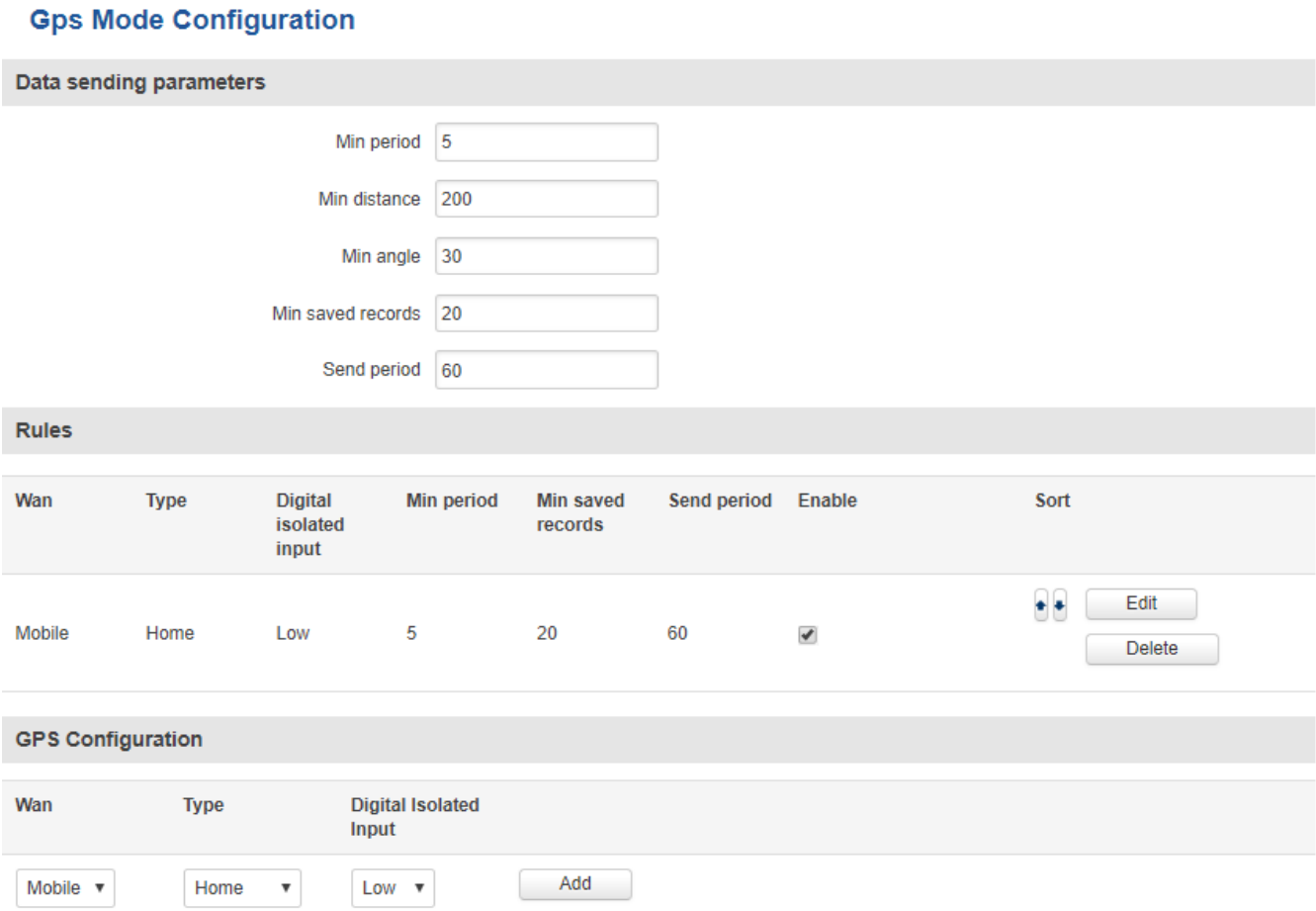


	Field name	Values	Notes
1.	Enable GPS service	Checked / Unchecked	Enables the GPS function
2.	Enable GPS Data to server	Checked / Unchecked	Enables automatic GPS data transferring to a remote server
3.	Remote host / IP address	Any IP address or hostname	Server IP address or domain name to send the coordinates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

9.12.2.1 TAVL Settings

	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
2.	Send analog input	Checked / Unchecked	Check to include analog input state in GPS data package to be sent to server
3.	Send digital input (1)	Checked / Unchecked	Check to include digital input #1 state in GPS data package to be sent to server
4.	Send digital input (1)	Checked / Unchecked	Check to include digital input #2 state in GPS data package to be sent to server

9.12.3 GPS Mode



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.

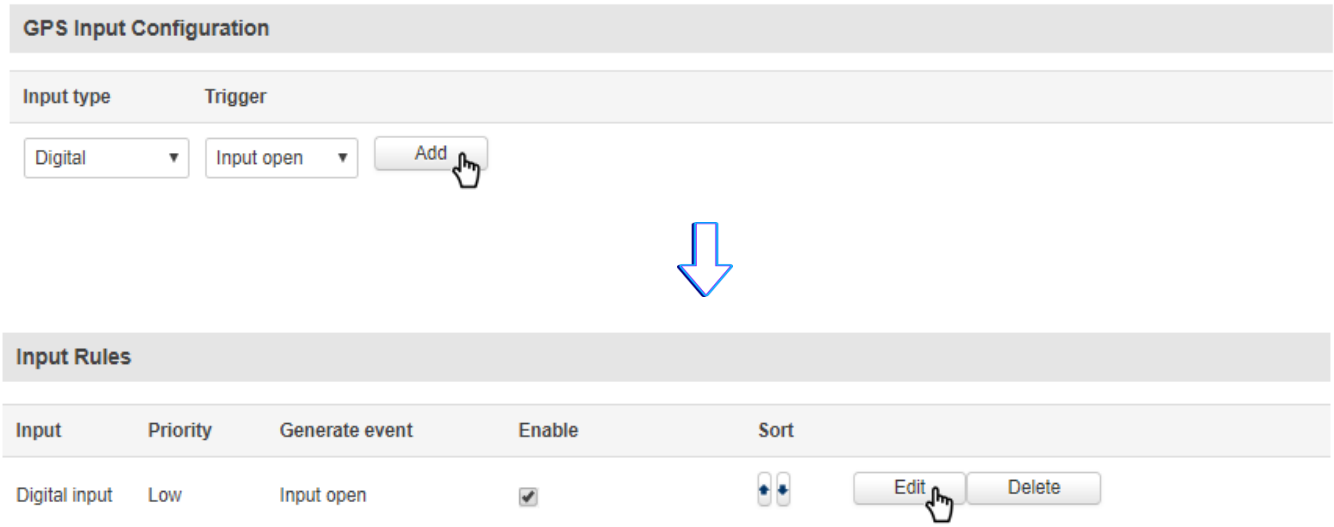
GPS Configuration

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

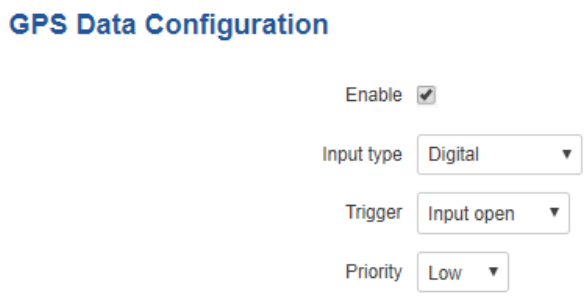
	Field name	Values	Notes
1.	WAN	Mobile / Wired / WiFi	Interface which needs to be used to activate this configuration
2.	Type	Home / Roaming / Both	Mobile connection state needed to activate this configuration
3.	Digital Isolated Input	Low logic level / High logic level / Both	Input state needed to activate this configuration

9.12.4 GPS I/O

The GPS I/O window provides you with the possibility to configure GPS Input rules. To create a new Input rule select **Input type** and **Trigger**, both of which can be found in the **GPS Input Configuration** section, then click the **Add** button.

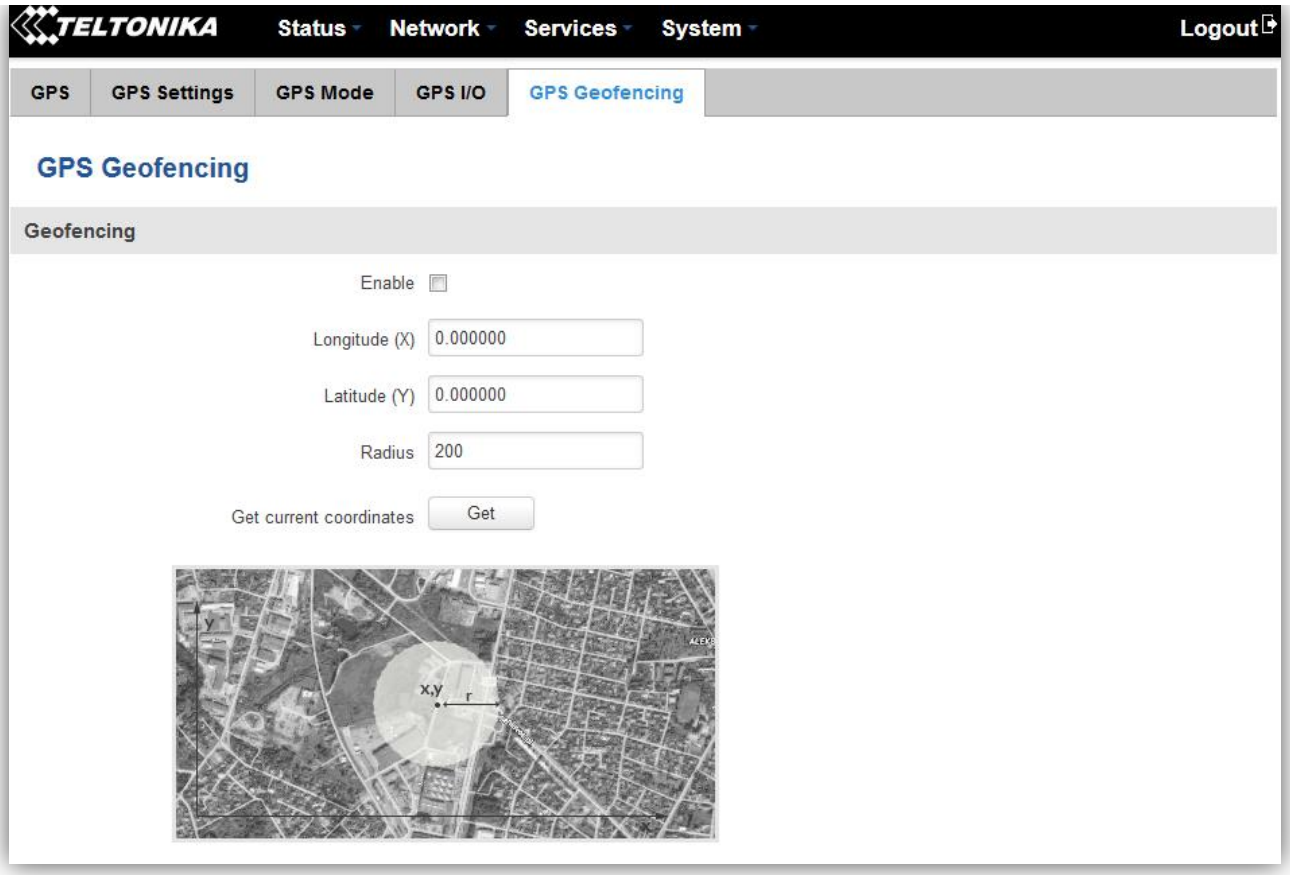


This will create a new unconfigured Input rule. To configure it press the **Edit** button located next to the newly created rule.



	Field name	Values	Notes
1.	Enable	Checked / Unchecked	Enables the rule
2.	Input Type	Digital / Digital isolated / Analog	Which type of the input the rule will apply to
3.	Trigger	Input open / Input shorted / Both	Trigger event for your intended configuration
4.	Priority	Low / High / Panic	Different priority settings add different priority flags to event packets, and they can be displayed differently

9.12.5 GPS Geofencing



Geofencing is a feature which can detect whenever a device enters or leaves customized area.

	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	Get current coordinates	Get current device coordinates from GPS

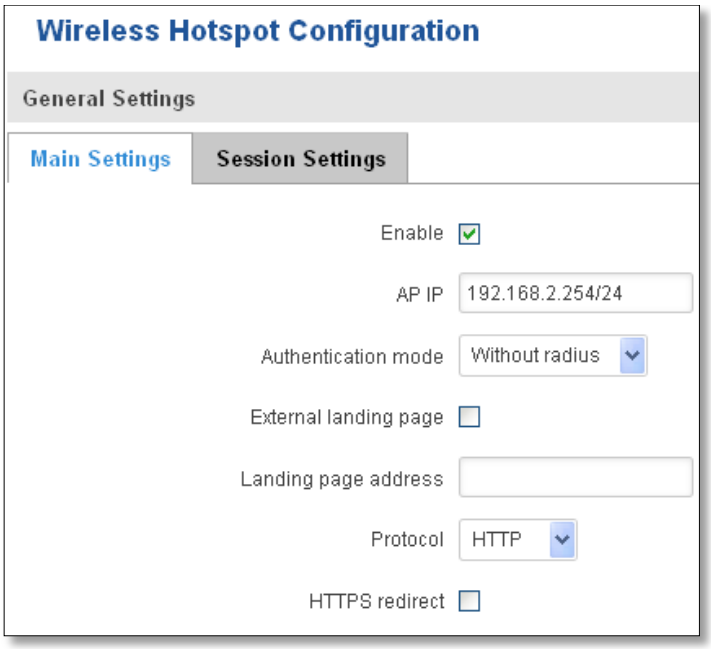
To receive SMS or email when entering or leaving geofence zone, go to Status -> Events Log -> Events reporting page and configure GPS event type!

9.13 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.).

9.13.1 General settings

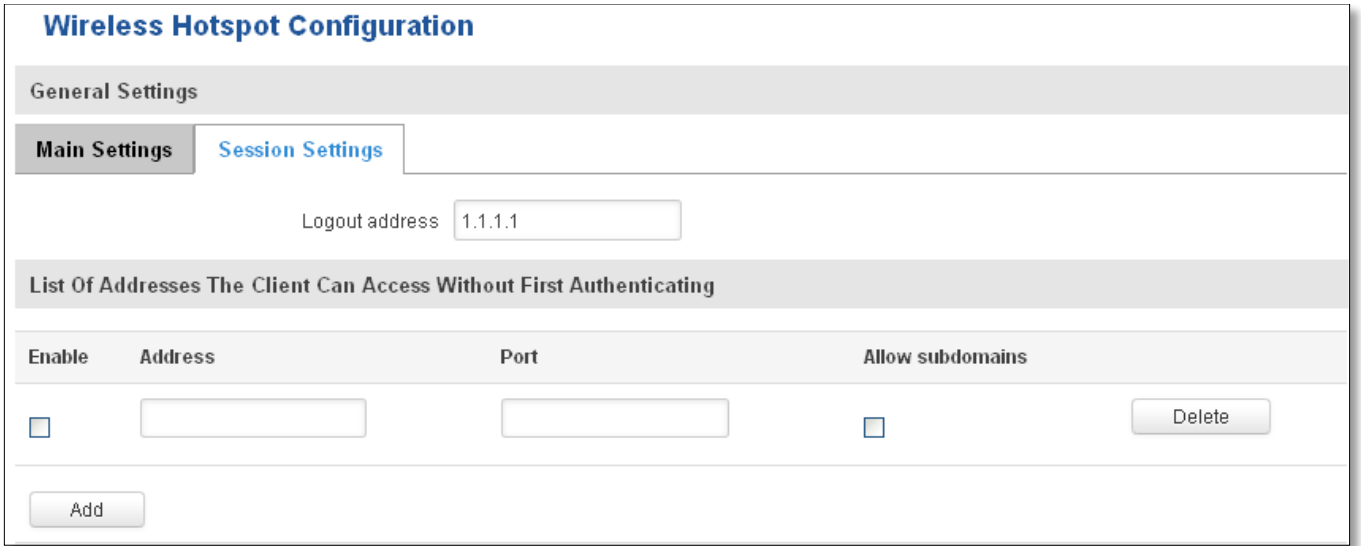
9.13.1.1 Main settings



	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).
		Authentication mode: External radius
1.	Radius server #1	The IP address of the RADIUS server that is to be used for Authenticating your wireless clients.

2.	Radius server #2	The IP address of the second RADIUS server.
3.	Authentication port	RADIUS server authentication port.
4.	Accounting port	RADIUS server accounting port.
5.	Radius secret key	The secret key is used for authentication with the RADIUS server
6.	UAM port	Port to bind for authenticating clients
7.	UAM UI port	UAM UI port
8.	UAM secret	Shared secret between UAM server an hotspot
9.	NAS Identifier	NAS Identifier
10.	Swap octets	Swap the meaning of input octets and output as it related to RADIUS attributes
11.	Location name	The name of location
Authentication mode: Internal radius/Without radius		
1.	External landing page	Enables the use of external landing page.
2.	Landing page address	The address of external landing page
3.	HTTPS redirect	Redirects HTTP pages to landing page.
Authentication mode: SMS OTP		

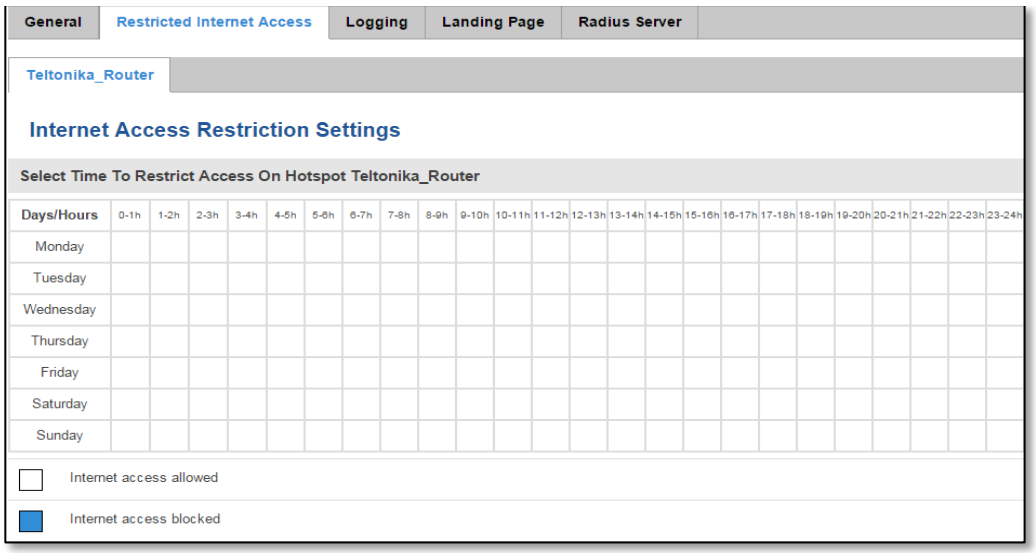
9.13.1.2 Session settings



	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

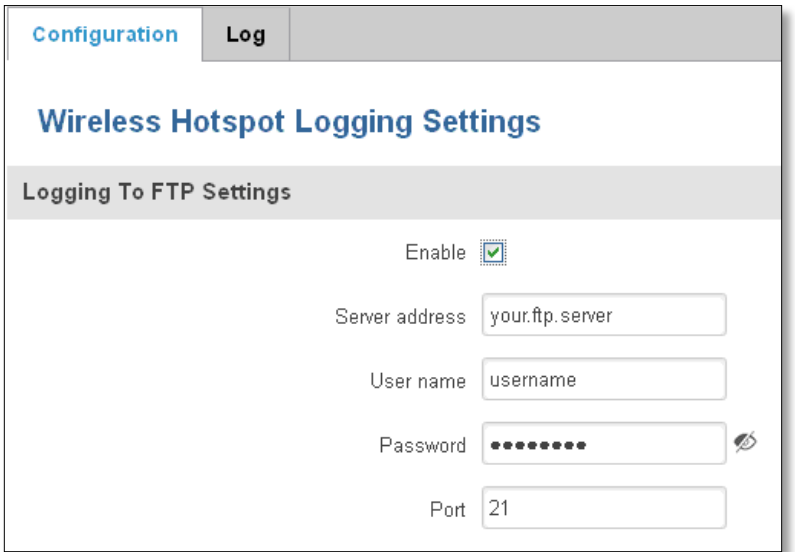
9.13.2 Internet Access Restriction Settings

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

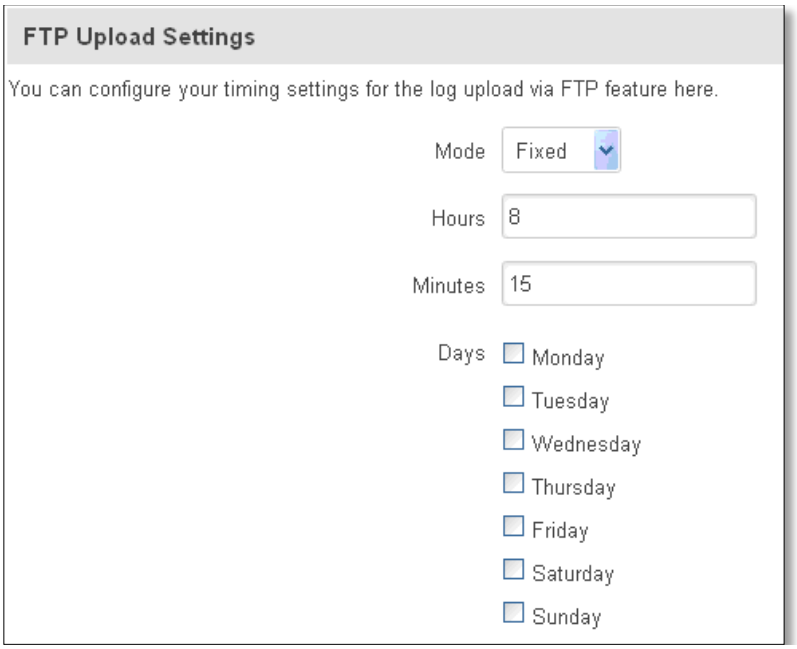


9.13.3 Logging

9.13.3.1 Configuration

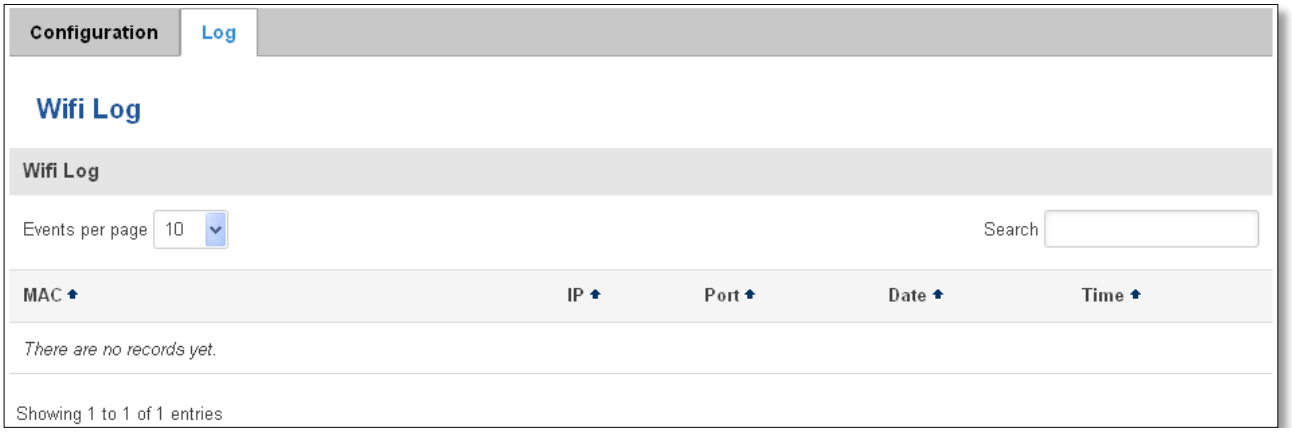


	Field name	Explanation
1.	Enable	Check this box if you want to enable wireless traffic logging. This feature will produce logs which contain data on what websites each client was visiting during the time he was connected to your hotspot.
2.	Server address	The IP address of the FTP server to which you 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.



	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.

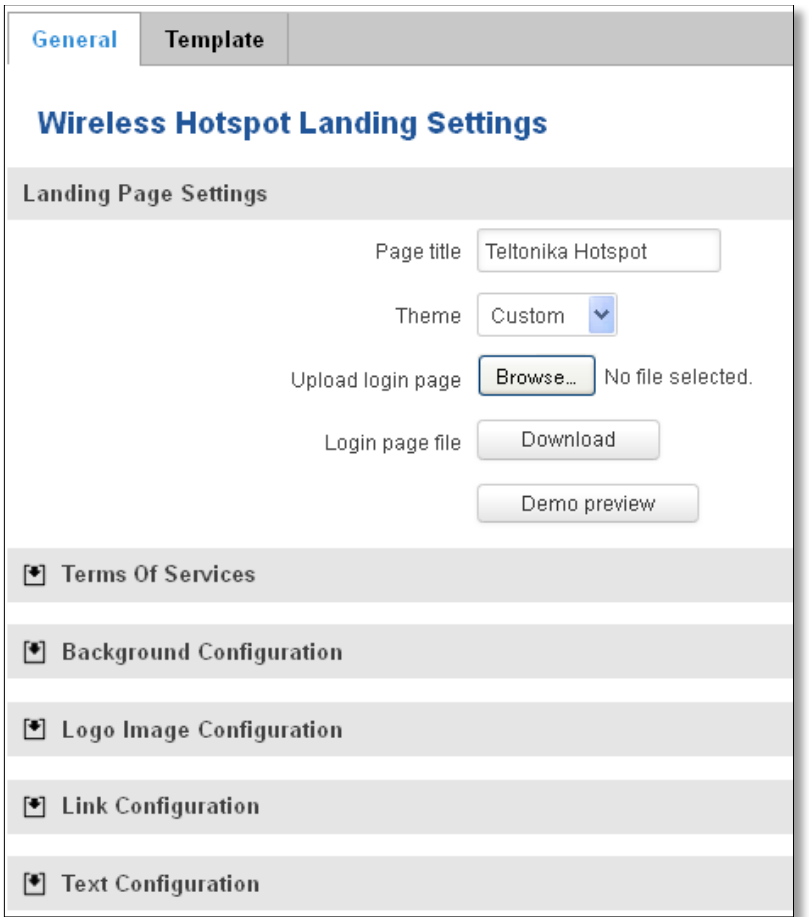
9.13.3.2 Log



9.13.4 Landing Page

9.13.4.1 General Landing Page Settings

With this functionality you can customize your Hotspot Landing page.

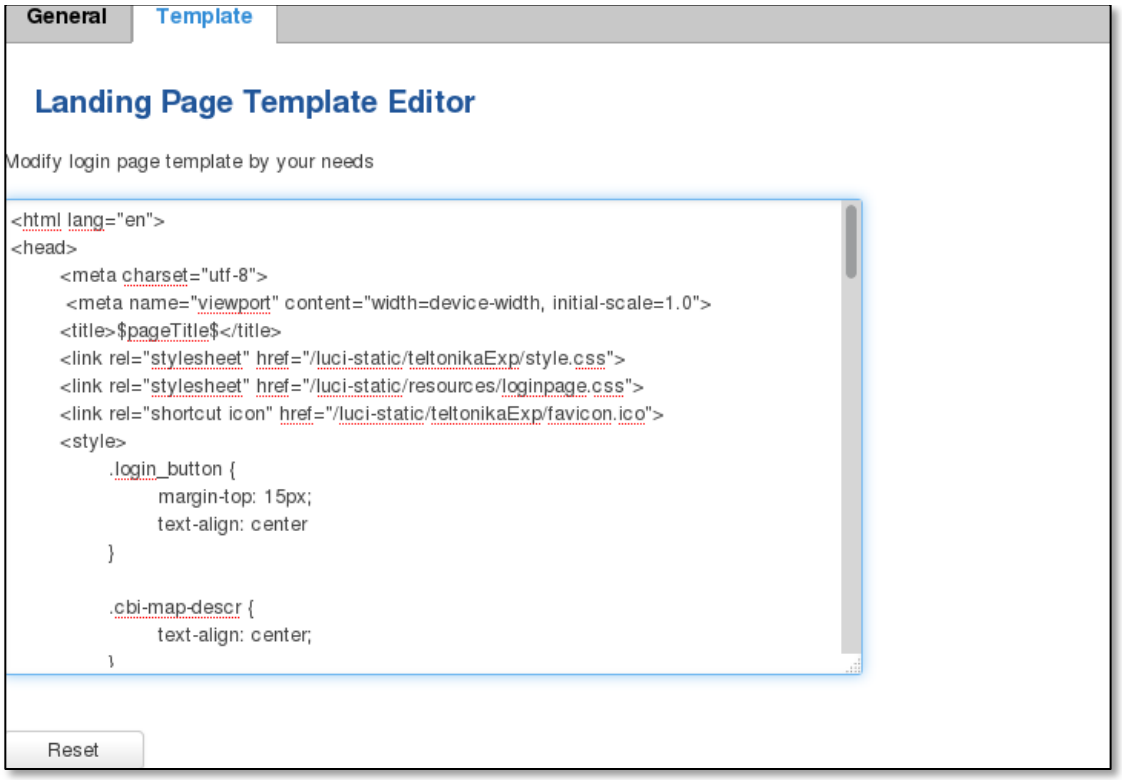


	Field name	Explanation
1.	Page title	Will be seen as landing page title
2.	Theme	Landing page theme selection
3.	Upload login page	Allows to upload custom landing page theme
4.	Login page file	Allows to download and save your landing page file

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

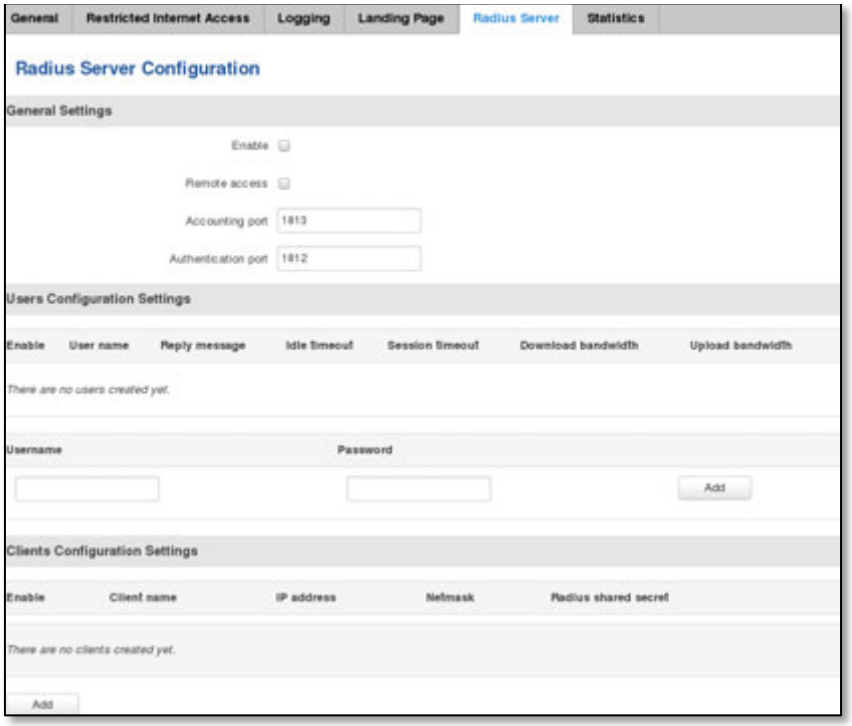
9.13.4.2 Template

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



9.13.5 Radius server configuration

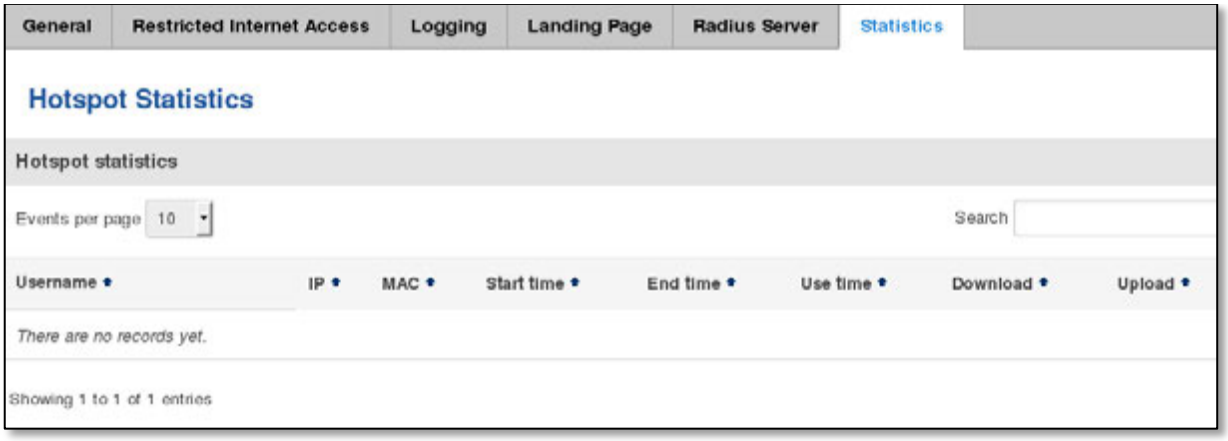
An authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.



	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

9.13.6 Statistics

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



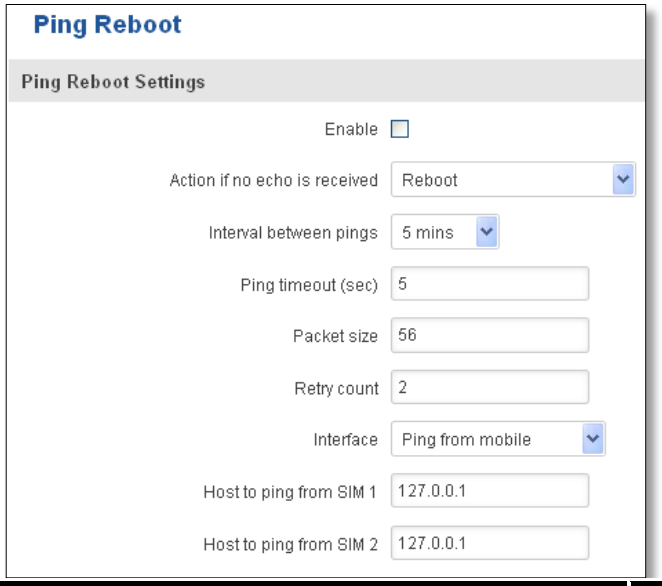
9.14 CLI

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

9.15 Auto Reboot

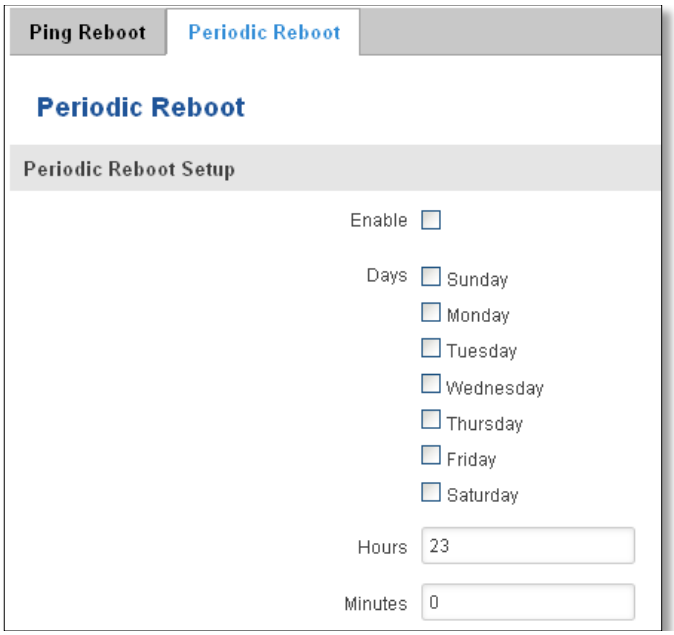
9.15.1 Ping Reboot

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.



	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 from SIM 1	IP address or domain name which will be used to send ping packets to. E.g. 127.0.0.1 (or www.host.com if DNS server is configured correctly)	Ping packets will be sending from SIM1.
8.	Host to ping from SIM 2	IP address or domain name which will be used to send ping packets to. E.g. 127.0.0.1 (or www.host.com if DNS server is configured correctly)	Ping packets will be sending from SIM2.

9.15.2 Periodic Reboot

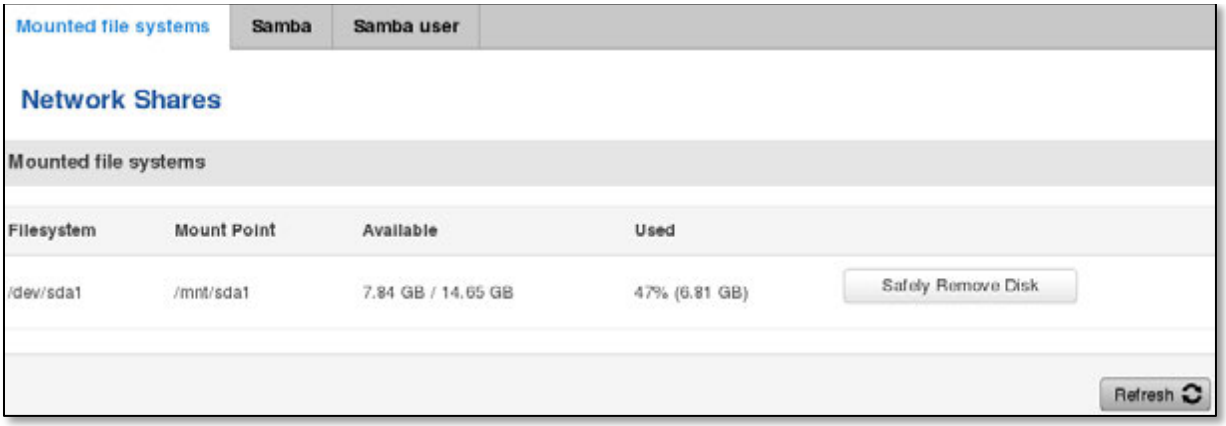


	Field name	Explanation
1.	Enable	This check box will enable or disable Periodic reboot feature.
2.	Days	This check box will enable router rebooting at the defined days.
3.	Hours, Minutes	Uploading will be done on that specific time of the day

9.16 Network Shares

9.16.1 Mounted File Systems

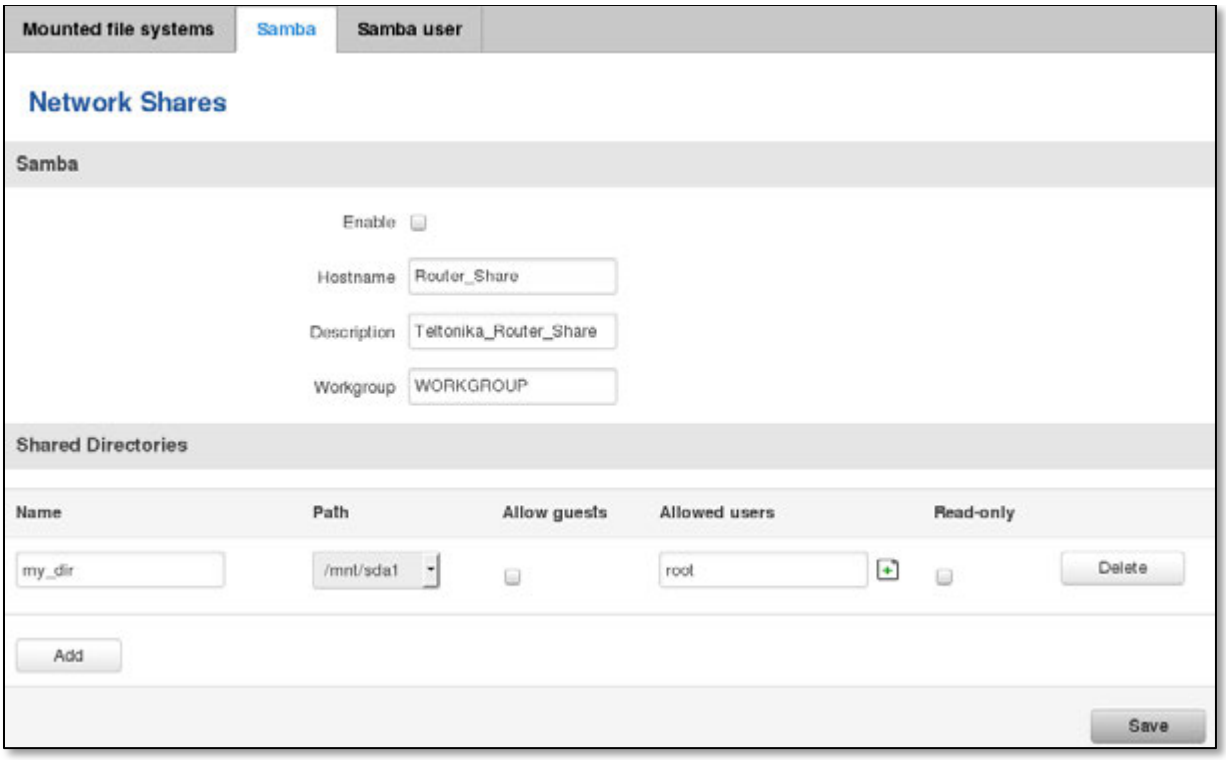
On this page you can review mounted file systems (for example USB flashdrive).



	Field name	Explanation
1.	File System	Filesystem on which additional file system is mounted
2.	Mount Point	Directory available for mounting additional file system
3.	Available	Total memory available in mounted system
4.	Used	Free memory in mounted system

9.16.2 Samba

Samba functionality allows network sharing for specified directories.



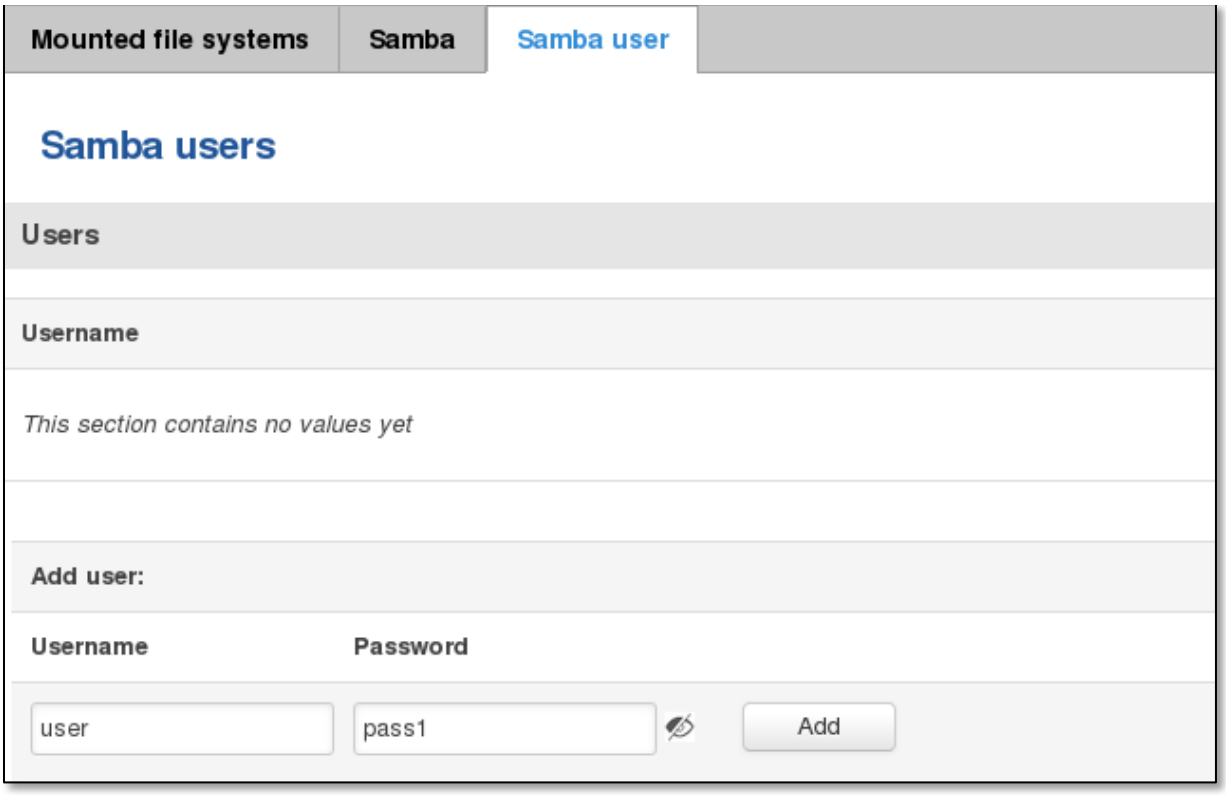
	Field name	Values	Notes
1.	Enable	Enable / Disable	Enables Samba service
2.	Hostname	Router_Share	Name of samba server
3.	Description	Teltonika_Router_Share	Short server description
4.	Workgroup	WORKGROUP	Name of the workgroup

In Shared Directories section you can add directories to be shared and configure some usage parameters:

	Field name	Values	Notes
1.	Name	My_dir	Name of the shared directory
2.	Path	/mnt/sda1	Path to directory to be shared
3.	Allow guests	Enable / Disable	Enable viewing the directory as a guest
4.	Allowed users	root	Specify users to be allowed to share this directory
5.	Read-only	Enable / Disable	Sets user's wrights in the specified directory to read-only

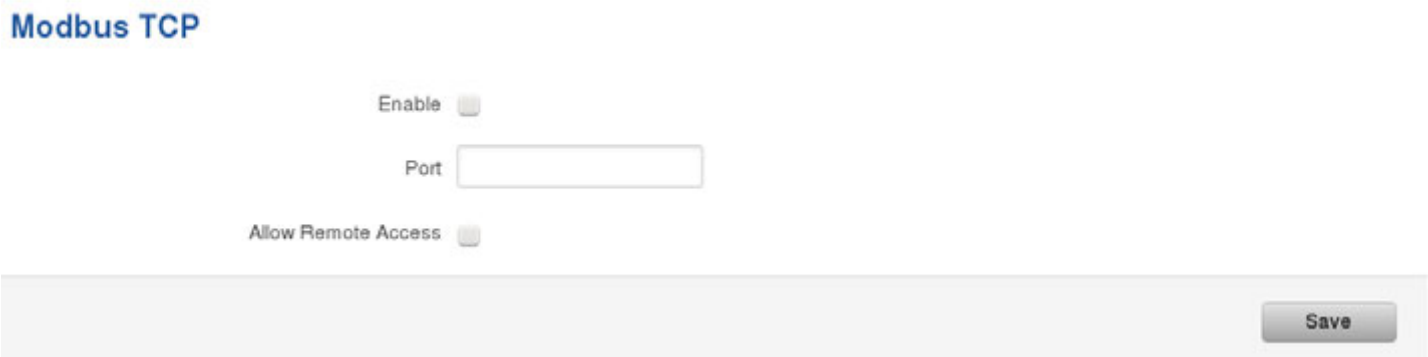
9.16.3 Samba User

In this page you can add new samba users.



	Field name	Values	Notes
1.	Username	user	Name of new user
2.	Password	Pass1	New user's password

9.17 Modbus TCP interface



Modbus TCP interface allows the user to set or get some parameters like module temperature, signal strength, etc. from the router. In other words, Modbus TCP allows to control routers behavior and get its status information. To use Modbus TCP capabilities this feature must be enabled by navigating to Services-Modbus. After "Save" button is pressed, the Modbus daemon will be launched on selected port of the system. Modbus daemon acts as slave device that means, it accepts connection from the master (client) and sends out a response or sets some system related parameter. By the default Modbus will only accept connections through LAN interface. In order to accept connections through WAN interface also, Allow Remote Access must be checked.

To obtain some parameter from the system, the read holding registers command is used. The register number and corresponding system values are described below. Each register contains 2 bytes. For simplification the number of registers for storing numbers is 2, while for storing text information the number of registers is 16.

Required value	Representation	Register number	Number of registers
System uptime	32 bit unsigned integer	1	2
GSM signal strength (dBm)	32 bit integer	3	2
System temperature in 0.1 degrees Celcium	32 bit integer	5	2
System hostname	Text	7	16
GSM operator name	Text	23	16
Router serial number	Text	39	16
Router MAC address	Text	55	16
Router name	Text	71	16
Current SIM card	Text	87	16
Network registration	Text	103	16
Network type	Text	119	16
Digital input 1	32 bit integer	135	2
Digital input 2	32 bit integer	137	2
Current WAN IP address	32 bit unsigned integer	139	2
Analog input	32 bit integer	141	2

The Modbus daemon also supports setting of some system parameters. For this task write holding register command is used. System related parameters and how to use them are described below. The register number refers to the register number where to start write required values. All commands, except "Change APN" accepts only one input parameter. For the APN the number of input registers may vary. The very first byte of APN command denotes a number

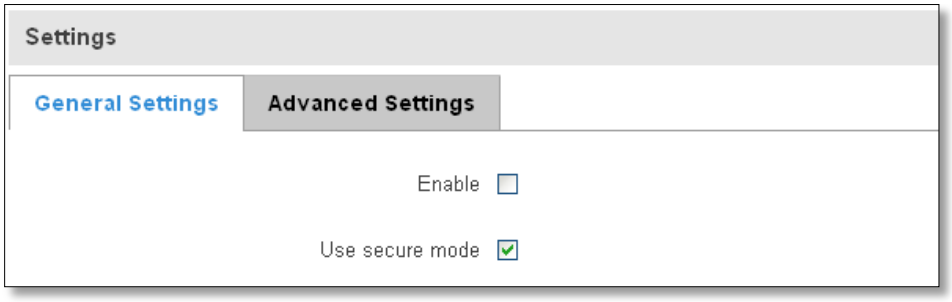
of SIM card for which set the APN. This byte should be set to 1 (in order to change APN for SIM card number 1) or to 2 (in order to change APN for SIM card number 2).

Value to set	Description	Register number	Register value
Digital output 1 (on/off)	Change the state of the digital output number 1	201	1/0
Digital output 2 (on/off)	Change the state of the digital output number 2	202	1/0
Switch WiFi (on/off)	Allows to switch WiFi on or off	210	1/0
Switch mobile data connection (on/off)	Turns on or off mobile data connection	211	1/0
Switch SIM card (SIM1, SIM2, SIM1->SIM2 and SIM2->SIM1)	Allows to change SIM card in use, 3 possible options are supported	212	0/1/2
Change APN	Allows to change APN	213	APN code
Reboot	Reboots a router	220	1

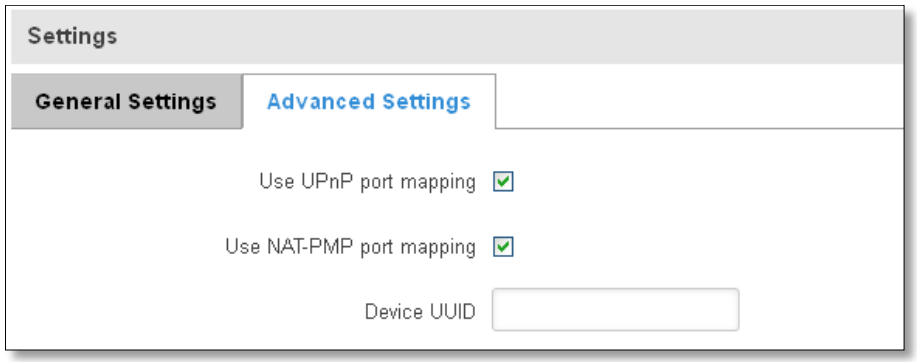
9.18 UPNP

9.18.1 General Settings

UPnP allows clients in the local network to automatically configure the router.



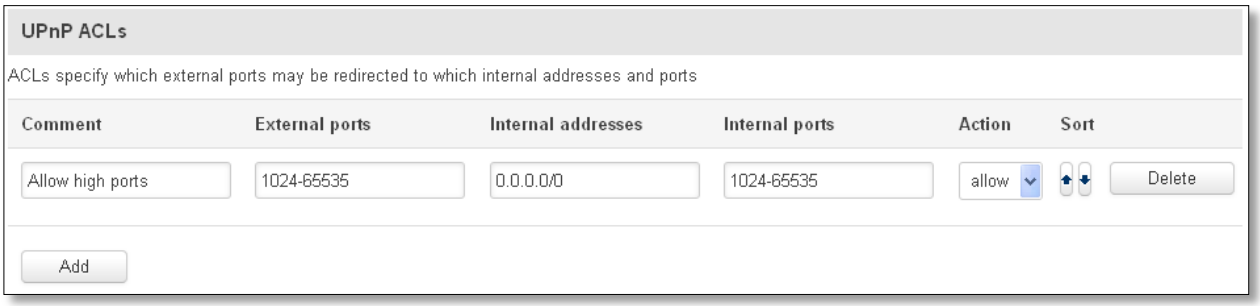
9.18.2 Advanced Settings



	Field name	Explanation
1.	Use UPnP port mapping	Enable UPnP port mapping functionality
2.	Use NAT-PMP port mapping	Enable NAT-PMP mapping functionality
3.	Device UUID	Specify Universal unique ID of the device

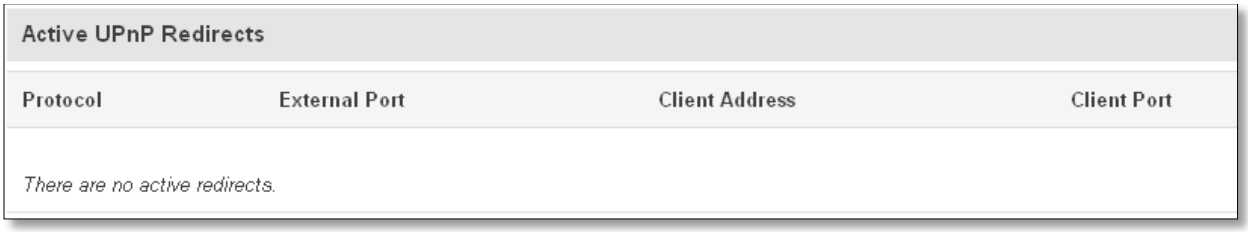
9.18.3 UPnP ACLs

ACLs specify which external ports may be redirected to which internal addresses and ports.



	Field name	Explanation
1.	Comment	Add comment to this rule
2.	External ports	External ports which may be redirected
3.	Internal addresses	Internal address to be redirect to
4.	Internal ports	Internal ports to be redirect to
5.	Action	Allow or forbid UPNP service to open the specified port

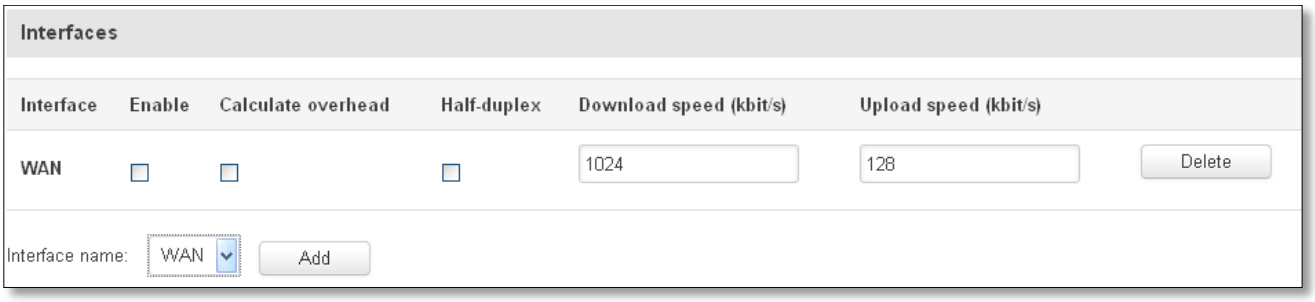
9.18.4 Active UPnP Redirects



9.19 QoS

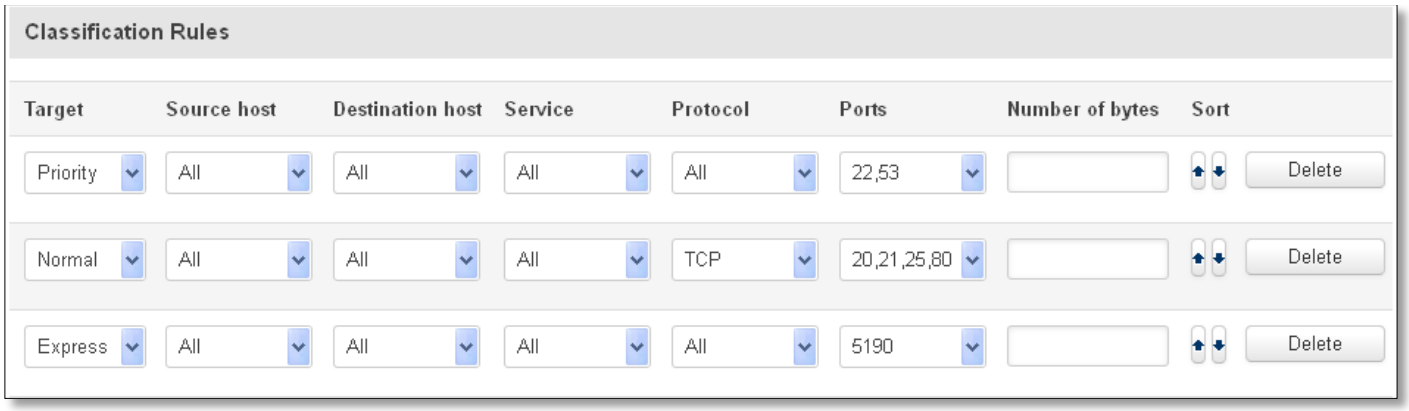
QoS (Quality of Service) is the idea that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. QoS is of particular concern for the continuous transmission of high-bandwidth video and multimedia information.

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



	Field name	Value	Explanation
1.	Interface	WAN/LAN/PPP	
2.	Enable	Enable/Disable	Enable/disable settings

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

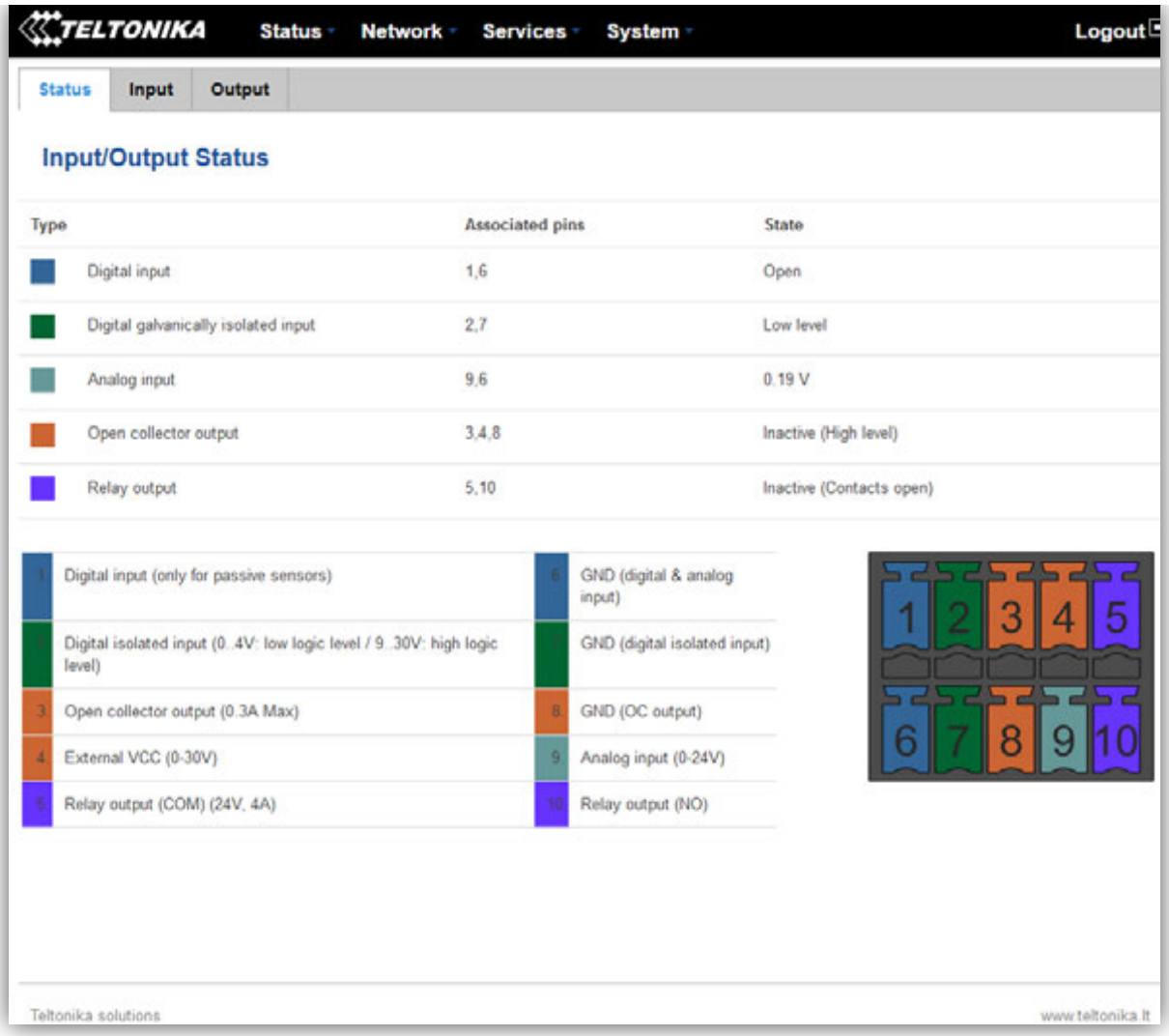


	Field name	Explanation
1.	Target	Select target for which rule will be applied
2.	Source host	Select host from which data will be transmitted
3.	Destination host	Select host to which data will be transmitted
4.	Service	Select service for which rule will be applied
5.	Protocol	Select data transmission protocol
6.	Ports	Select which port will be used for transmission
7.	Number of bytes	Specify the maximal number of bytes for connection

9.20 Input/Output

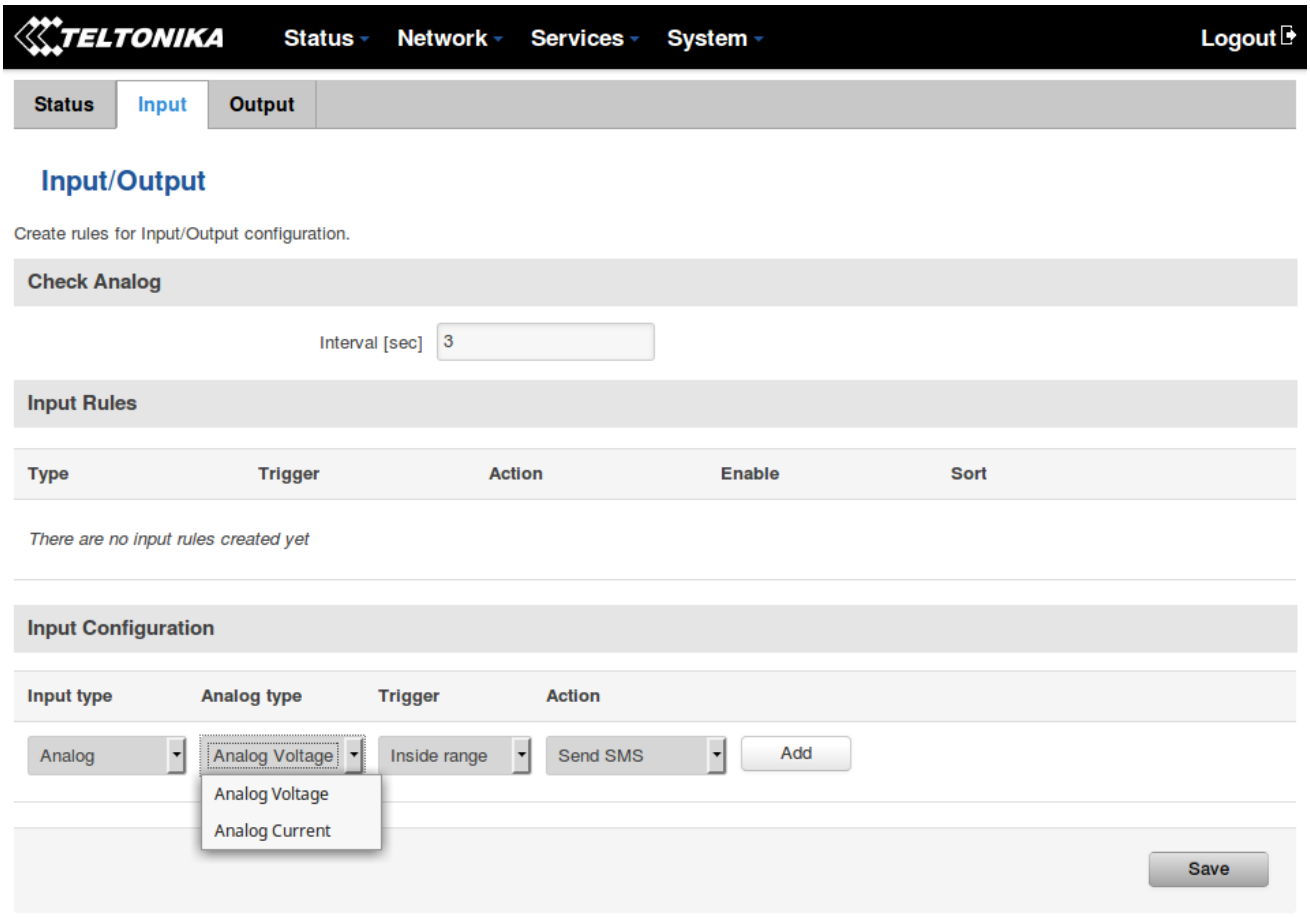
9.20.1 Status

In this page you can review the current state of all router's inputs and outputs.

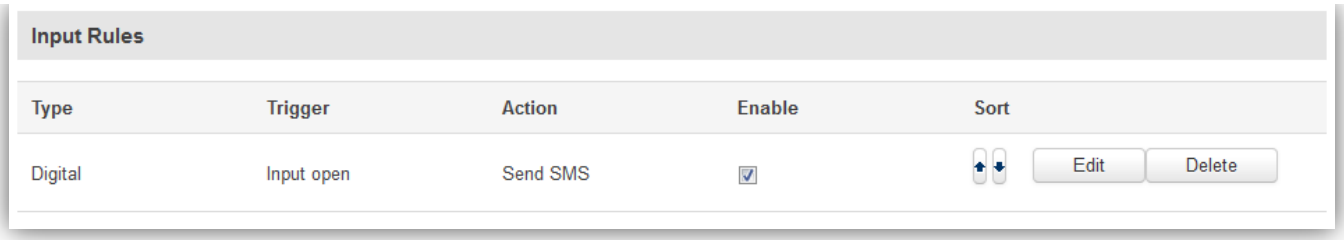


9.20.2 Input

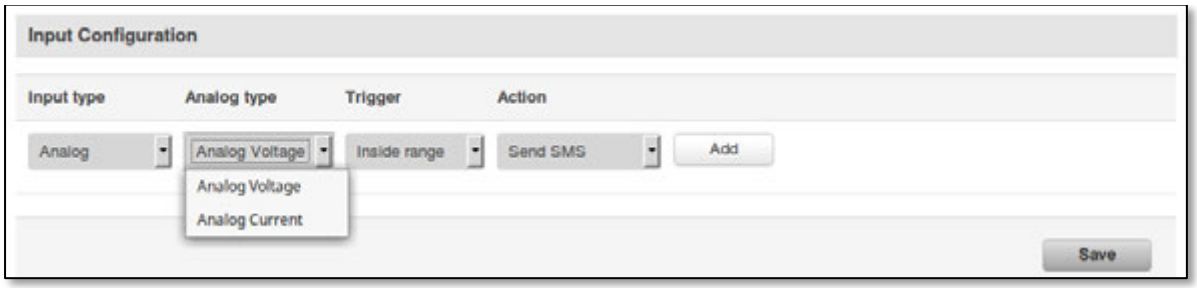
Allows you to set up input parameters and specify what actions should be taken after triggering event of any input. In check analog section you can change the analog input checking interval.



In the input rules section you can create and modify the rules for action after specific input triggering.

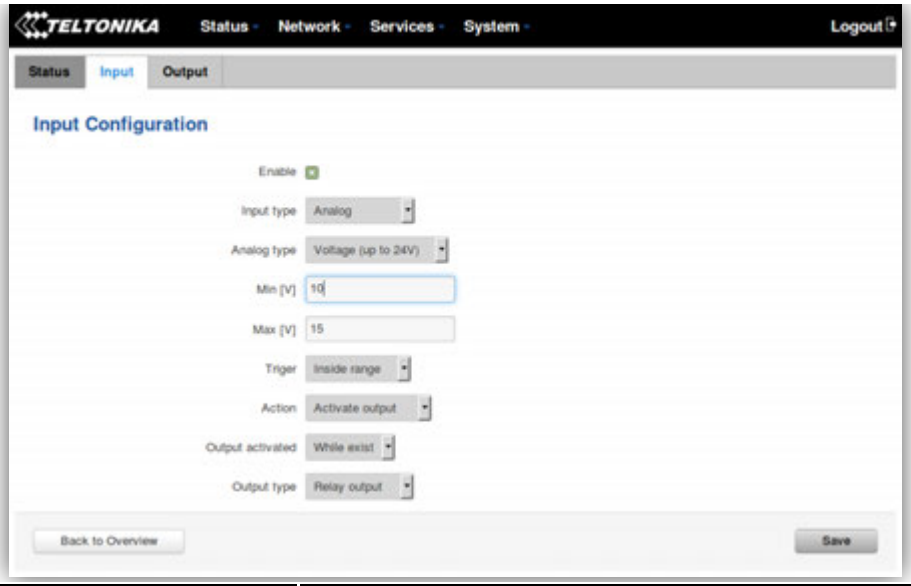


	Field name	Sample	Explanation
1.	Type	Digital/Digital isolated/Analog	Specifies input type
2.	Triger	Input open	Specifies for which trigger rule is applied
3.	Action	Send SMS	Specifies what action is done
4.	Enable	Enable/Disable	Enable input configuration



	Field name	Values	Explanation
1.	Input type	Digital/Digital isolated/Analog	Specify input type
1.a	Analog type	Analog Voltage/Analog Current	Specify voltage or current measurement
2.	Triger	Input open / Input shorted/ both	Specify for which trigger rule will be applied
3.	Action	Send SMS/ Change SIM card/ Send email/ Change profile/ Turn WiFi ON or OFF/Reboot/ Output	Choose what action will be done after input triggering

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

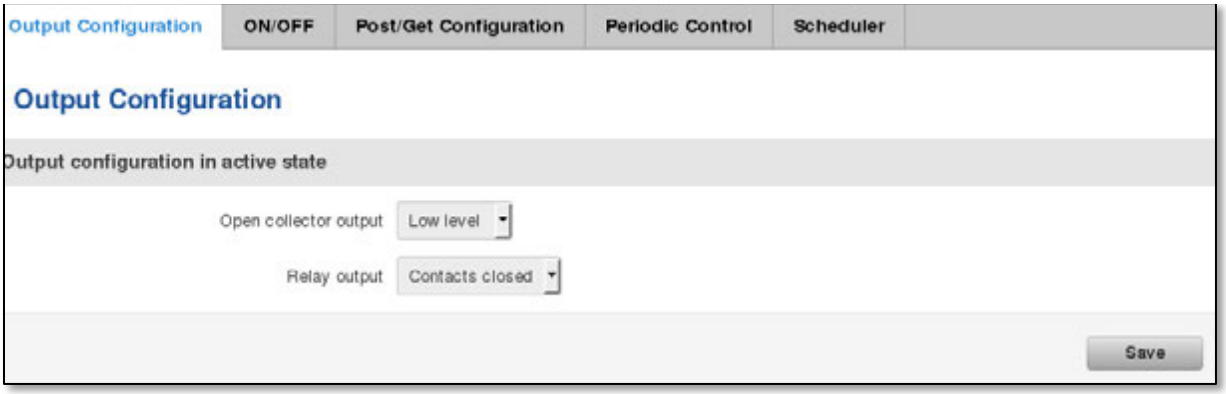


	Field name	Sample	Explanation
1.	Enable	Enable/Disable	Enable this input rule
2.	Input type	Digital/Digital isolated/Analog	Specify the input type
3.	Min V/mA	10	Specify minimum voltage/current. Only shown when Input type is Analog
4.	Max V/mA	20	Specify maximum voltage/current. Only shown when Input type is Analog
5.	Triger	Input open	Specify for which trigger rule will be applied
6.	Action	Send SMS	Specify what action to do
7.	SMS text	Input	Specify message to send in SMS
8.	Recipients phone number	+37012345678	Phone number where you will get SMS. Only shown when Action is Send SMS
9.	Subject	Input	Specify subject of email. Only shown when Action is Send email
10.	Message	Input	Specify message to send in email. Only shown when Action is Send email
11.	SMTP server	mail.example.com	Specify SMTP (Simple Mail Transfer Protocol) server. Only shown when Action is Send email
12.	SMTP server port	123	Specify SNMP server port. Only shown when Action is Send email
13.	Secure connection	Enable/Disable	Specify if server support SSL or TLS. Only shown when Action is Send email
14.	User name	username	Specify user name to connect SNMP server. Only shown when Action is Send email
15.	Password	password	Specify the password of the user. Only shown when Action is Send email

16.	Sender's email address	sender@example.com	Specify your email address. Only shown when Action is Send email
17.	Recipient's email address	recipient@example.com	Specify for whom you want to send email. Only shown when Action is Send email
18.	Sim	Primary/ Secondary	Specify which one SIM card will be changed. Only shown when Action is Change SIM Card
19.	Profile	Admin	Specify which profile will be set and used. Only shown when Action is Change Profile
20.	Reboot after (s)	4	Device will reload after a specified time (in seconds). Only shown when Action is Reboot
21.	Output activated	10	Output will be activated for specified time (in seconds) , or while exists.
22.	Output type	Digital OC output/ Relay output	Specify output type, which will be activated, depending on output time. Only shown when Action is Activate output

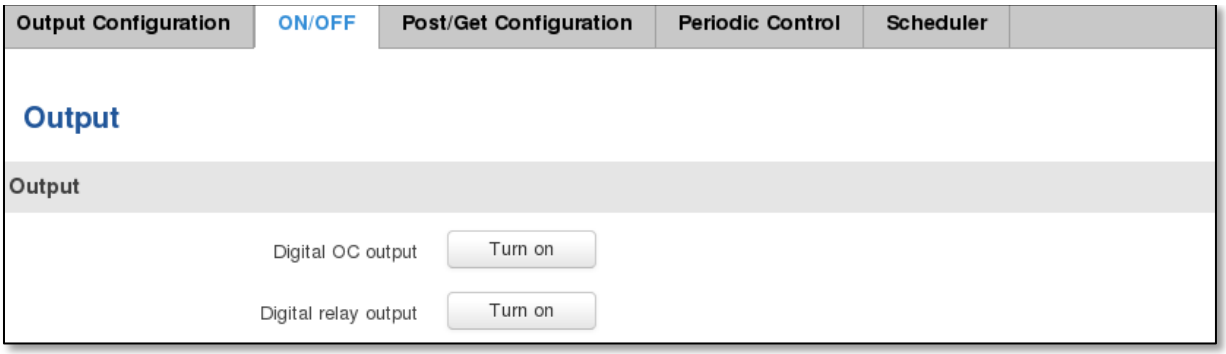
9.20.3 Output

9.20.3.1 Output Configuration



	Field name	Sample	Explanation
1.	Open collector output	Low level / High level	Choose what open collector output will be in active state
2.	Relay output	Contacts closed / Contacts open	Choose what relay output will be in active state

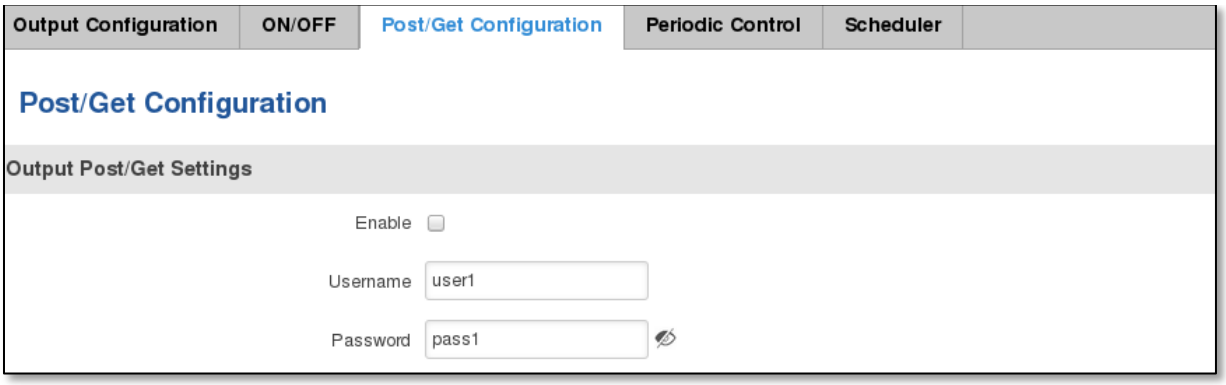
9.20.3.2 ON/OFF



	Field name	Sample	Explanation
1.	Digital OC output	Turn on / Turn Off	Manually toggle Digital OC output

2.	Digital relay output	Turn on / Turn Off	Manually toggle Digital relay output

9.20.3.3 Post/Get Configuration



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

9.20.3.4 Syntax of Output HTTP POST/GET string

With Output post/get you can manage only Outputs (Open collector output and Digital relay output).

	Field name	Example	Explanation
1.	IP_ADDRESS	192.168.1.1	IP address of your router
2.	action	on and off	Specify the action to be taken
3.	pin	oc and relay	Specify the output
4.	delay (sec)	15	Delay in seconds after which action will be started
5.	time (sec)	10	Time in seconds after which the action will be stopped. (if action is on, then it will go back to off after *time*)

Please note:

Delay and time parameters can be used together. Example: delay is 10, time is 5, action is „on". 10 seconds after command execution output will switch to „on" (or stay in „on" state if it's already on), then after 5 more seconds it will switch to off state. Overall command execution time is 15 seconds.

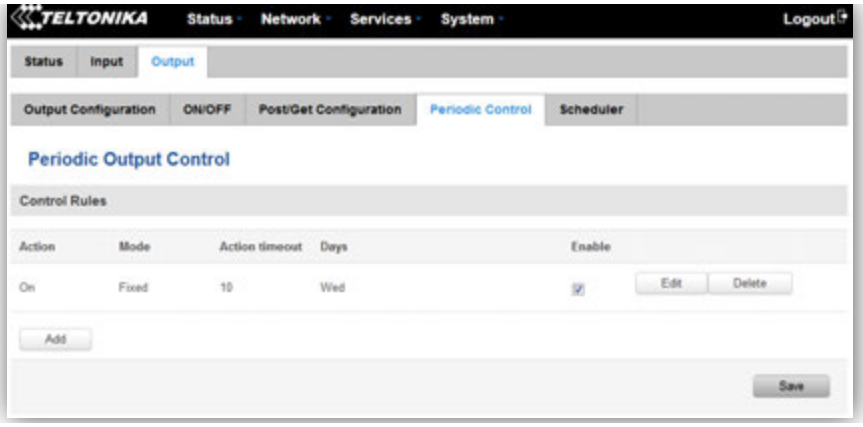
Actions „on" and „off" depend on setting „Output configuration in active state" (on is active state), which can be set via Services > Input/Output > Output

9.20.3.5 Output HTTP POST/GET string examples

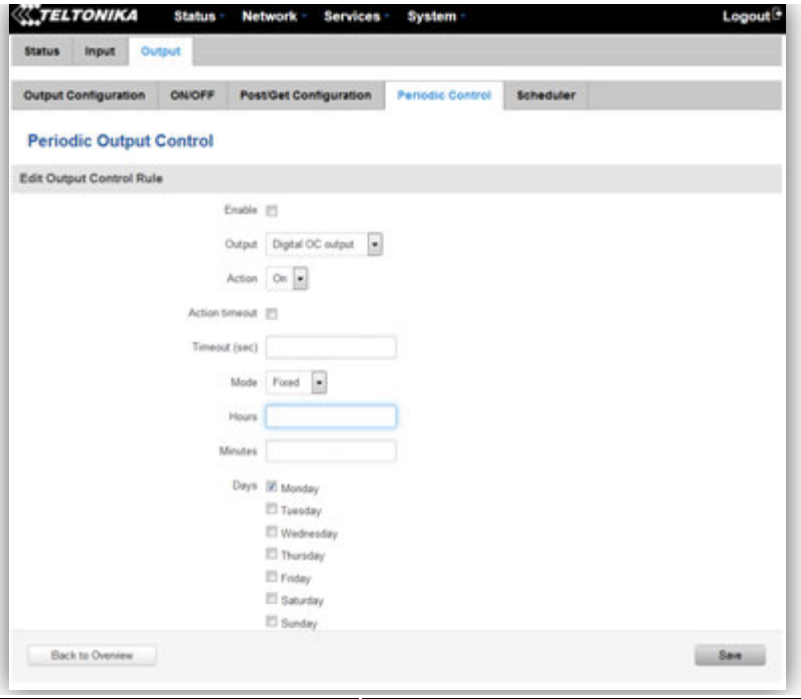
http://192.168.1.1/cgi-bin/output?username=User1&password=Pass1&action=on&pin=relay
http://192.168.1.1/cgi-bin/output?username=User1&password=Pass1&action=on&pin=relay&delay=10
http://192.168.1.1/cgi-bin/output?username=User1&password=Pass1&action=on&pin=relay&time=5
http://192.168.1.1/cgi-bin/output?username=User1&password=Pass1&action=on&pin=relay&delay=15&time=5
http://192.168.1.1/cgi-bin/output?username=User1&password=Pass1&action=off&pin=relay&delay=15&time=5
http://192.168.1.1/cgi-bin/output?username=User1&password=Pass1&action=on&pin=oc
http://192.168.1.1/cgi-bin/output?username=User1&password=Pass1&action=off&pin=oc

9.20.3.6 Periodic Control

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



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

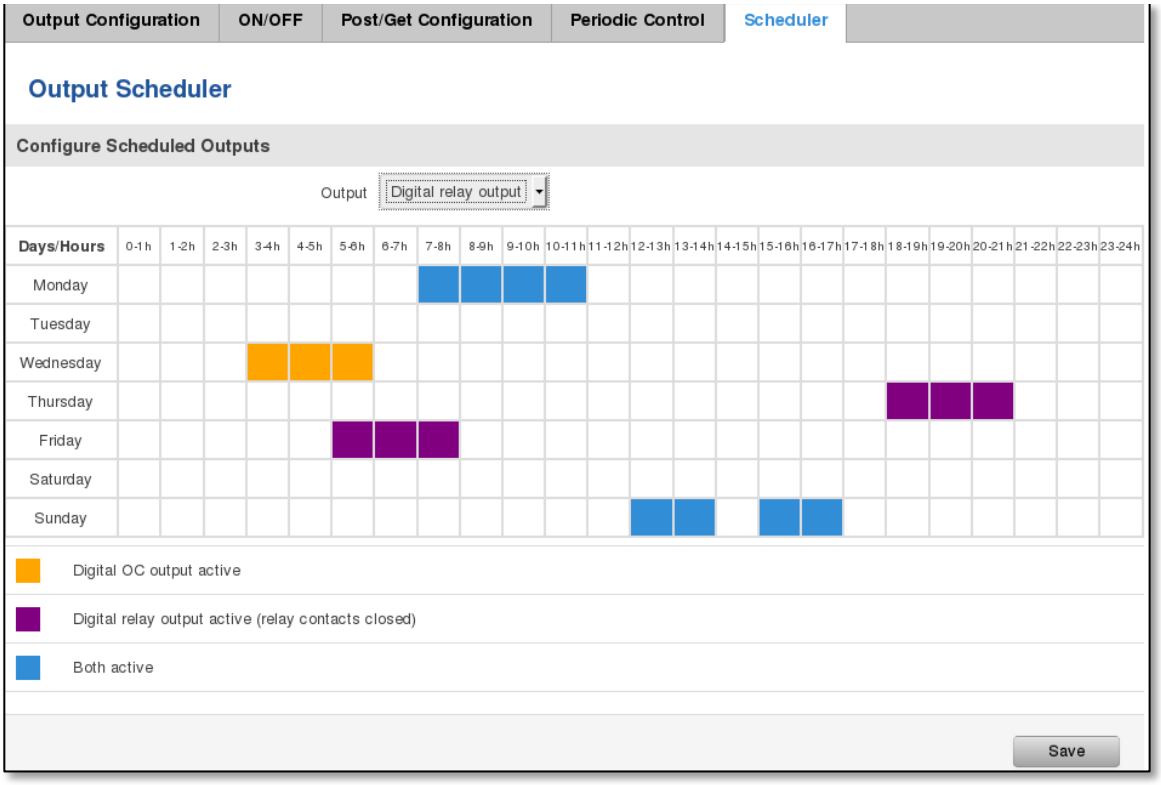


	Field name	Sample	Explanation
1.	Enable	Enable/Disable	Enable this output rule
2.	Output	Digital/Digital isolated/Analog	Specify the output type
3.	Action	On / Off	Specify the action to be taken
4.	Action timeout	Enabled / Disabled	Enable timeout for this rule
5.	Timeout (sec)	10	Specifies after how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

9.20.3.7 Scheduler

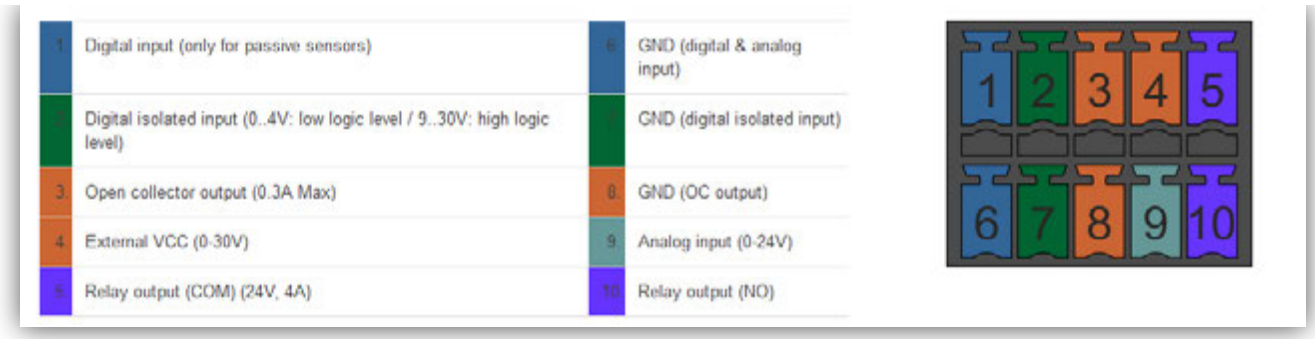
This function allows you to set up the periodical, hourly schedule for the outputs. You can select on which week

days the outputs are going to be on or off.



9.20.4 Input/Output hardware information

The Input/output (I/O) connector is located in the front panel next to LEDs. Pin-out of the I/O connector:

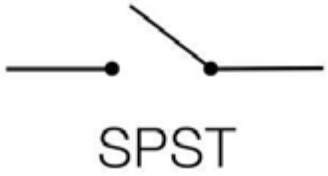


Type	Description	Ratings	QTY
Input (digital)	Digital non-isolated input for passive sensors	3V Max	1
Input(digital)	Digital input with galvanic isolation	0..4V – low level 9..30V – high level	1
Input (analog voltage/current)	Analog input (0-24V/0-20mA)	24V/20mA Max (with 1.2kΩ shunt)	1
Output (Open collector)	Open collector (OC) output	30V, 0.3A	1
Output (relay)	SPST relay output	24V, 4A	1

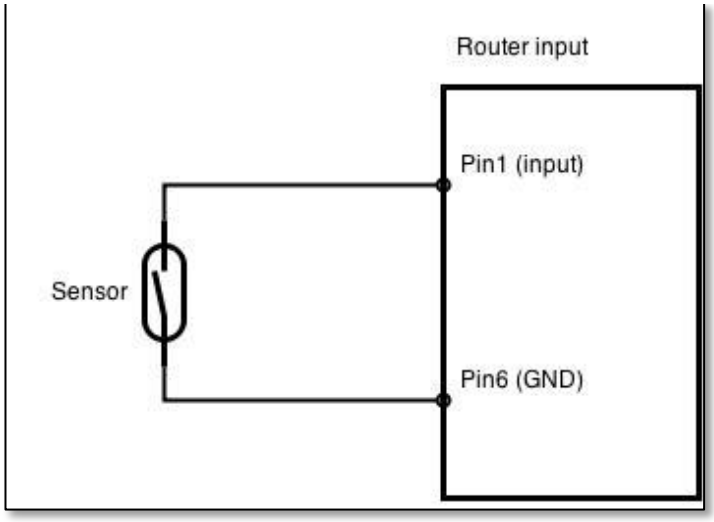
9.20.4.1 Digital input for passive sensors

Absolute maximum ratings:

Maximum voltage on input pin1 with respect to pin6: **3V**
Minimum voltage on input pin1 with respect to pin6: **0V**
The input is protected from short positive or negative ESD transients
This input is designed for connecting sensors with passive output (not outputting voltage) such as:

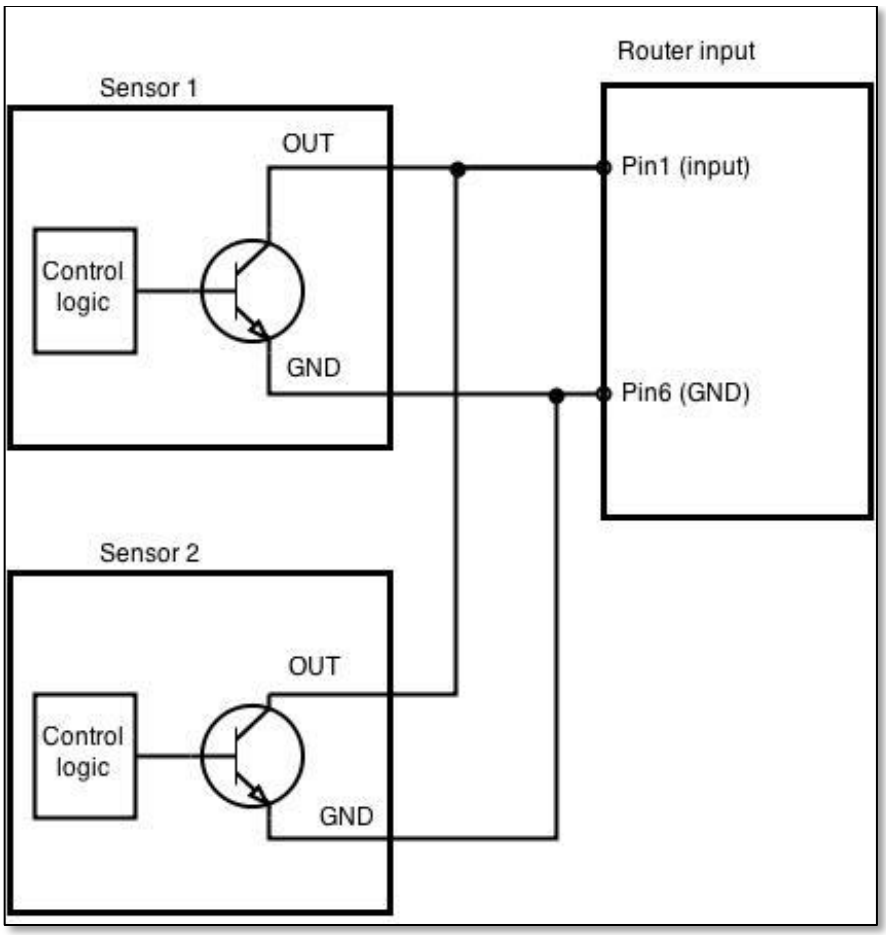
Passive infrared (PIR) sensors for motion detection (sensors with open collector or relay output are suitable type to use)	
Mechanical Switches, pushbuttons	
Reed switches, which opens or closes its contacts when magnetic field is near	
Any sensor with open collector or open drain output (use without pull-up resistor)	

Example schematic of using PIR sensors, mechanical switches, reed switches:



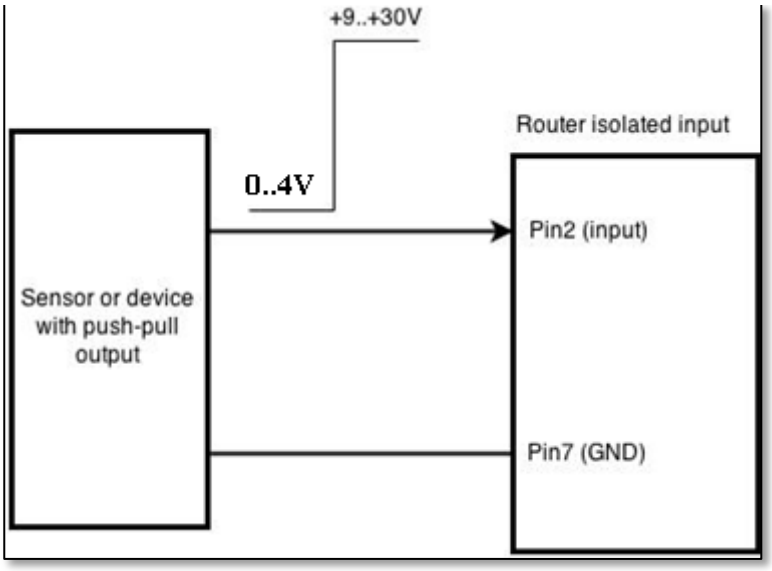
Example schematic of connecting multiple sensors with open collector outputs:

Multiple sensors can be connected in parallel like in the schematic below. In this configuration any sensor will activated the input. The example could be multiple motion sensors located in multiple places. If either of them will sense motion, the configured event (for e.g. alarm) will be activated. This is suitable when you just need to know that alarm is triggered but it is not necessary to know which sensor activated an alarm.



9.20.4.2 Digital galvanically isolated input

Sensors with push-pull output stage can be connected to this input. Example of such circuit is shown in the picture below. The circuit uses optocoupler to isolate the input. In case of the failure at the input, the rest of the circuit remains safe.



The signal source resistance should be less than 100Ω.

Input voltage levels:

- Low level voltage: **0..+4V**
- High level voltage: **+9..30V**

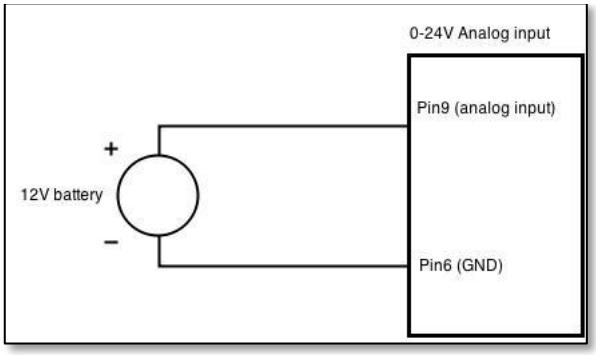
Maximum ratings:

- Maximum voltage that can be connected to pin2 with respect to pin7 is **30V.** Do not exceed this voltage!
- The input is protected from reverse voltage down to -200V.

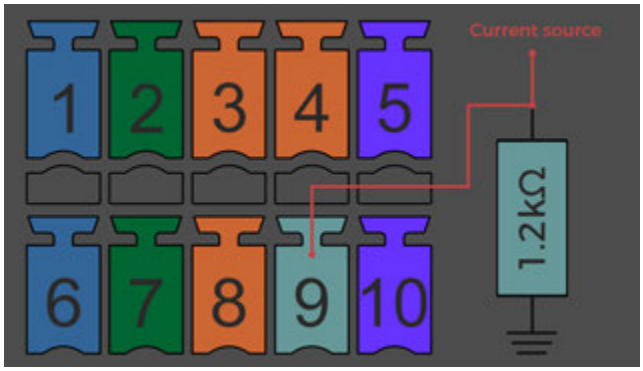
9.20.4.3 Analog input

Analog input is designed to measure analog voltages in the range of 0-24V and convert it to digital domain. This input can also be used to measure current up to 20mA.

Example of monitoring 12V battery voltage:



When Analog input type is „Analog Current“ a 1.2kΩ resistor shunt must be connected as shown below:



Input electrical characteristics:

Parameter	Value
Maximum voltage	24V
Minimum voltage	0V
Resolution	5.859mV
Input low-pass filter cut-off frequency (-3dB)	10Hz
Input resistance (seen between I/O header pins 9 and 6)	131kΩ

Input accuracy:

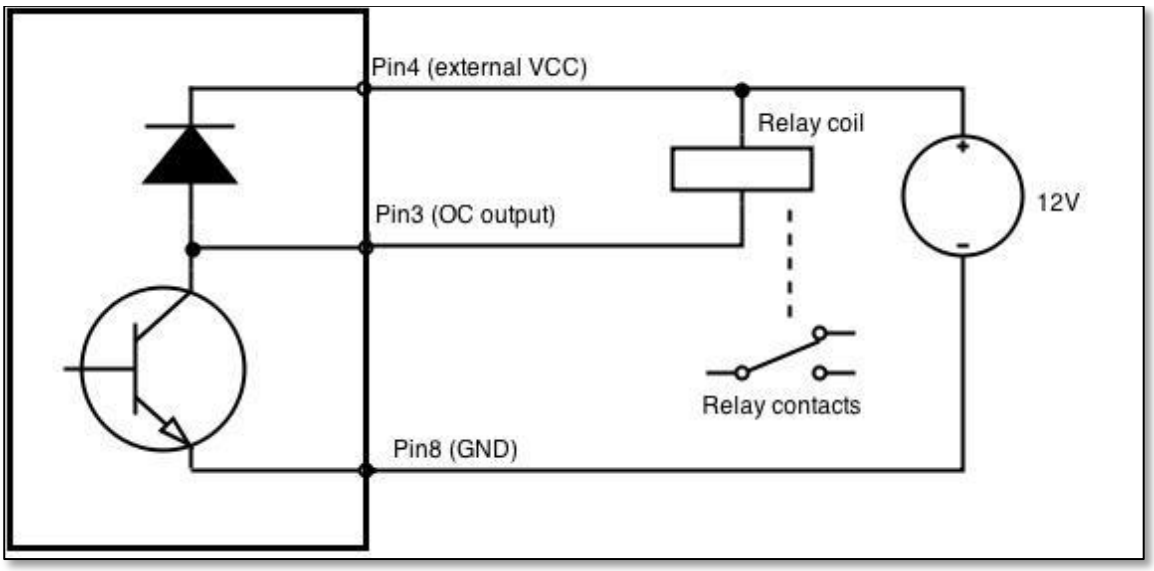
Input voltage range, V	Measurement error, %
0 <Vin≤ 1	<20
1 <Vin≤ 2	<10
2 <Vin≤ 5	<5
5 <Vin≤ 24	<3

9.20.4.4 Open collector output

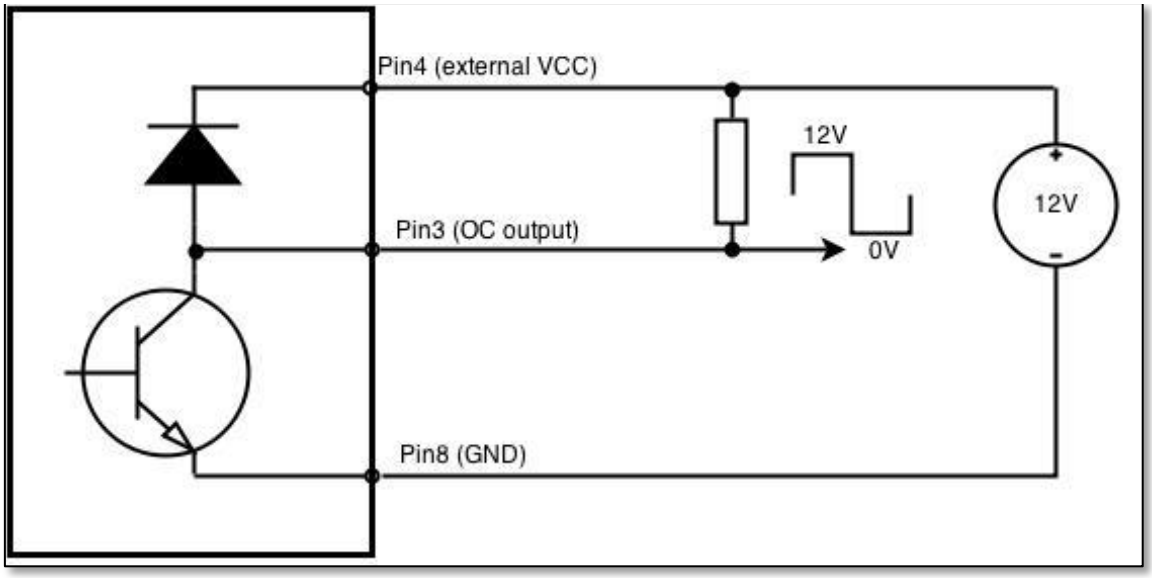
This output can be used to drive external relay. In order for the output to work correctly, external voltage that is connected to a relay also needs to be connected to I/O header pin 4. There is flyback diode located inside the device to protect it from spikes occurring when inductive load (relay coil) is suddenly switched off, so connection of the external diode is not necessary. The output is isolated from the rest of the circuitry using optocoupler. In case of the output failure, the rest of the circuit will remain protected.

Maximum external DC voltage	30V
Maximum output sink current	0.3A

Example of driving a relay:



Output can be also used to generate signals with desired amplitude. Resistor could be for example 4.7kΩ.

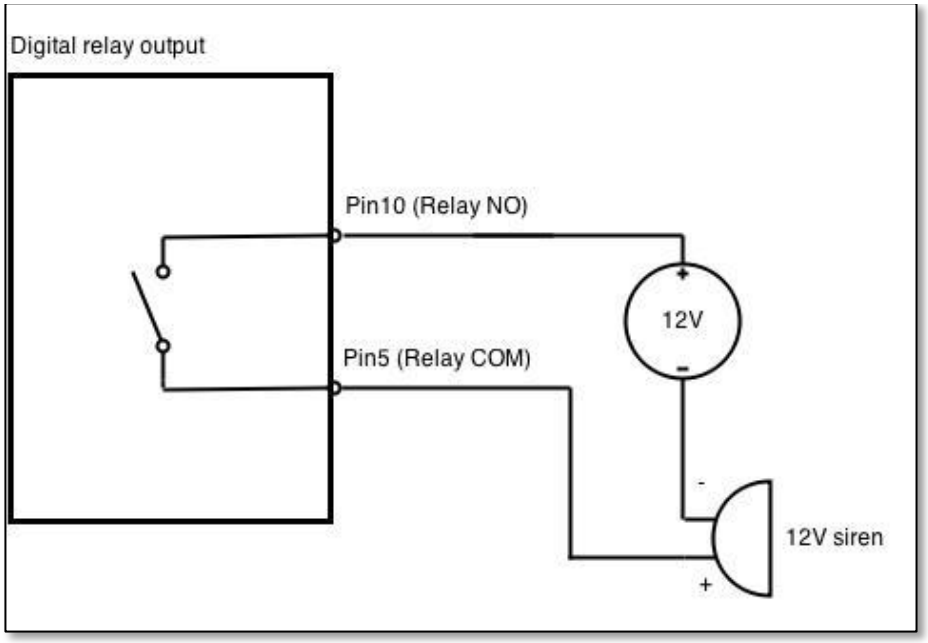


9.20.4.5 Relay output

Relay output has two pins: COM and NO. When the relay is not energized (output not active), these pins are disconnected. One the relay is energized (output active) these pins are become connected together. Relay output is not intended to drive AC voltages.

Maximum DC voltage across relay contacts	24V
Maximum relay DC current	4A

Example of connecting alarm siren to the relay output:



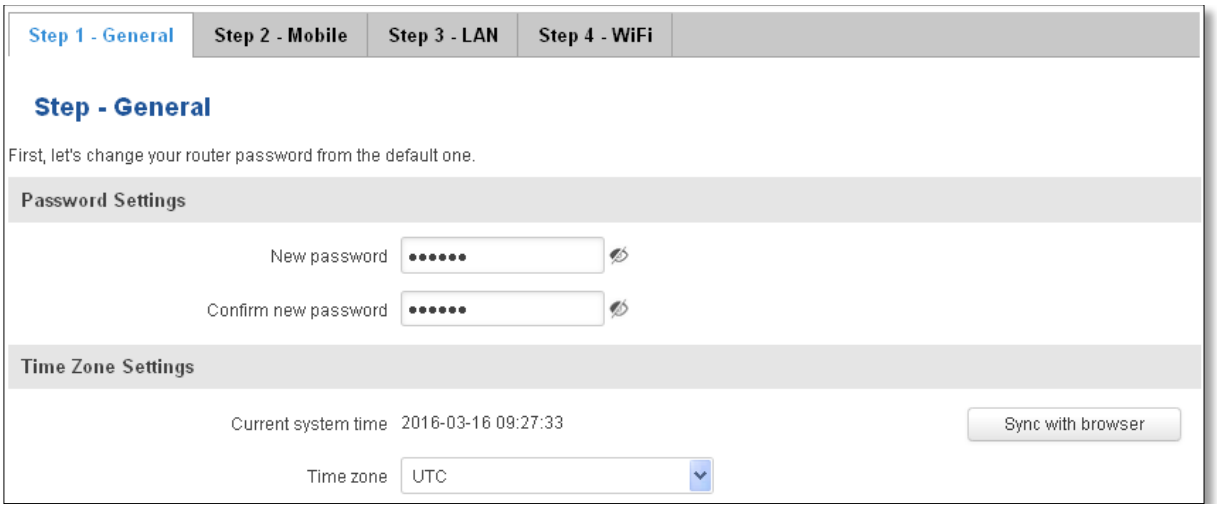
10 System

10.1 Configuration Wizard

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

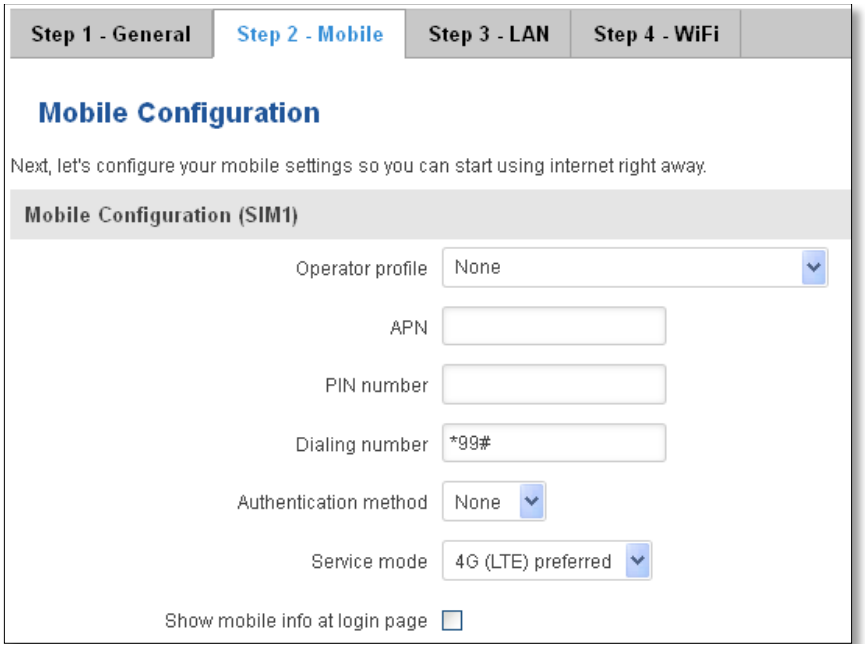
Step 1 (General change)

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



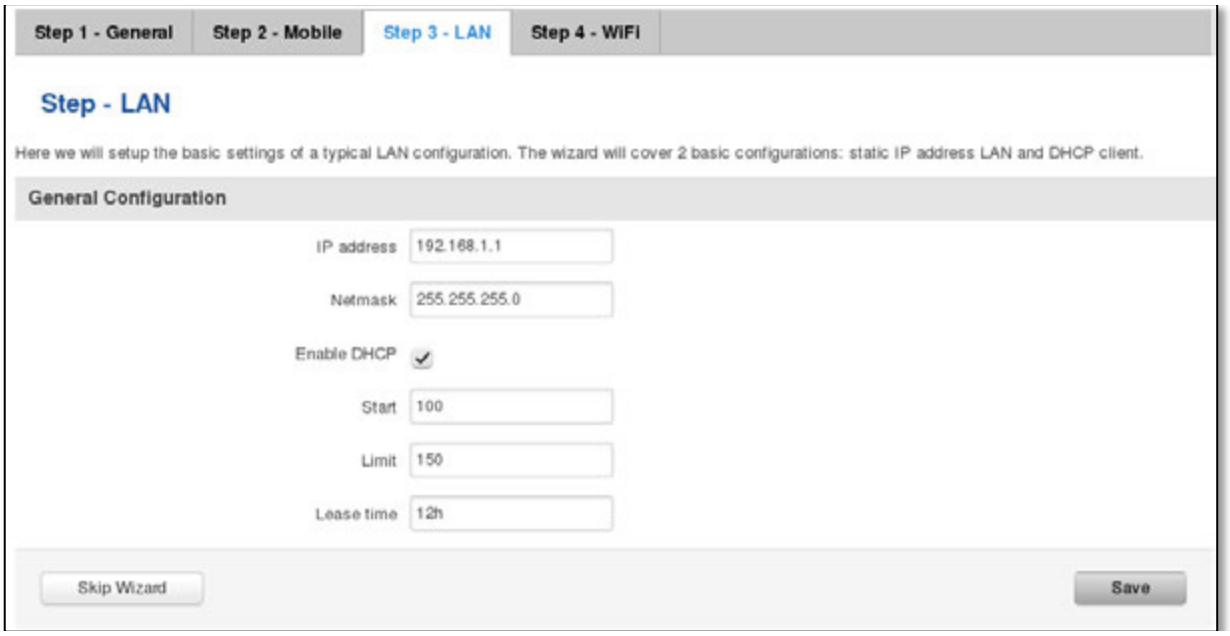
Step 2 (Mobile Configuration)

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



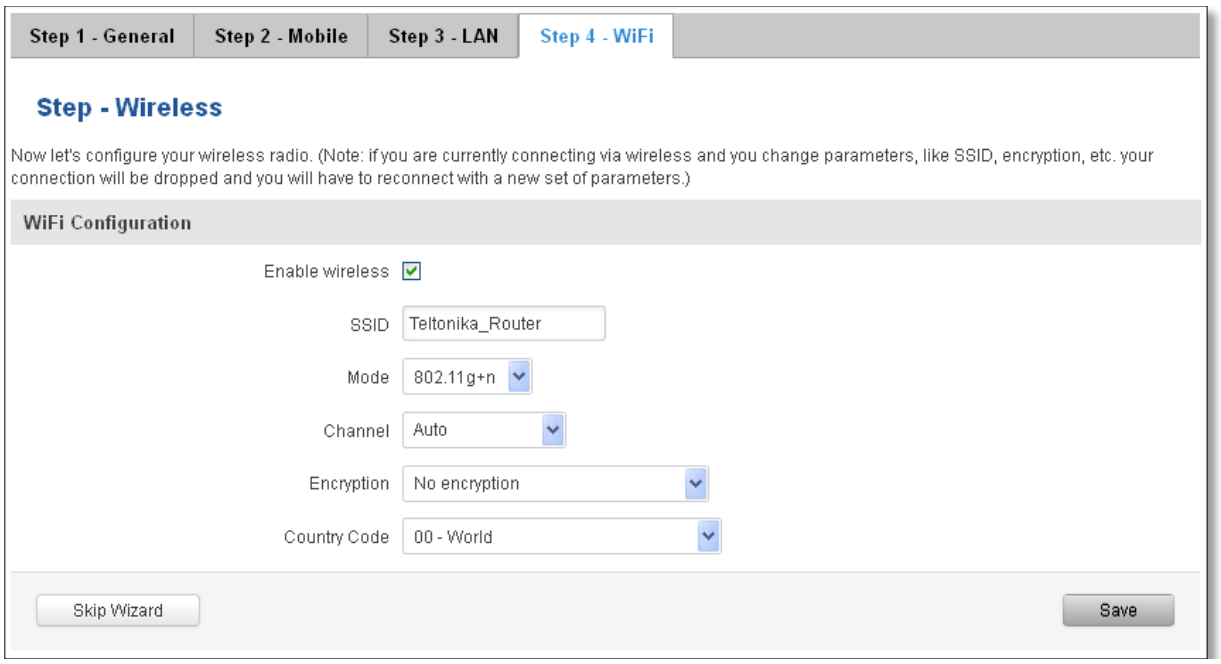
Step 3 (LAN)

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



Step 4 (Wi-Fi)

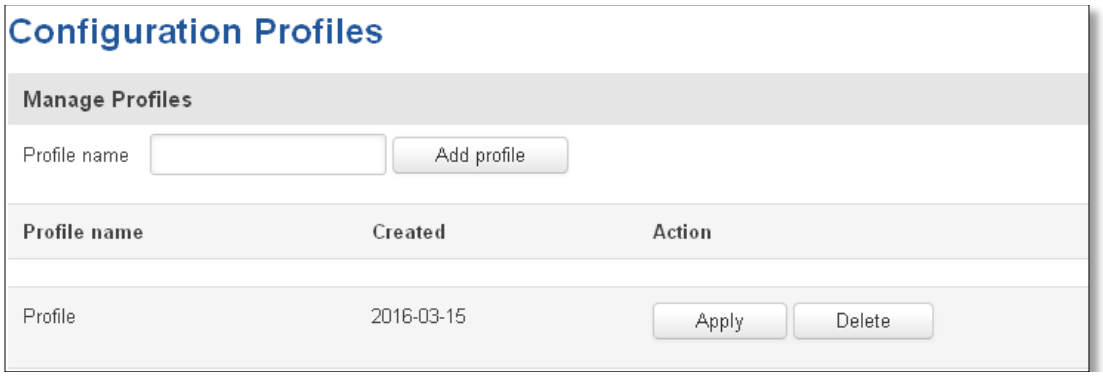
The final step allows you to configure your wireless settings in order to set up a rudimentary Access Point.



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

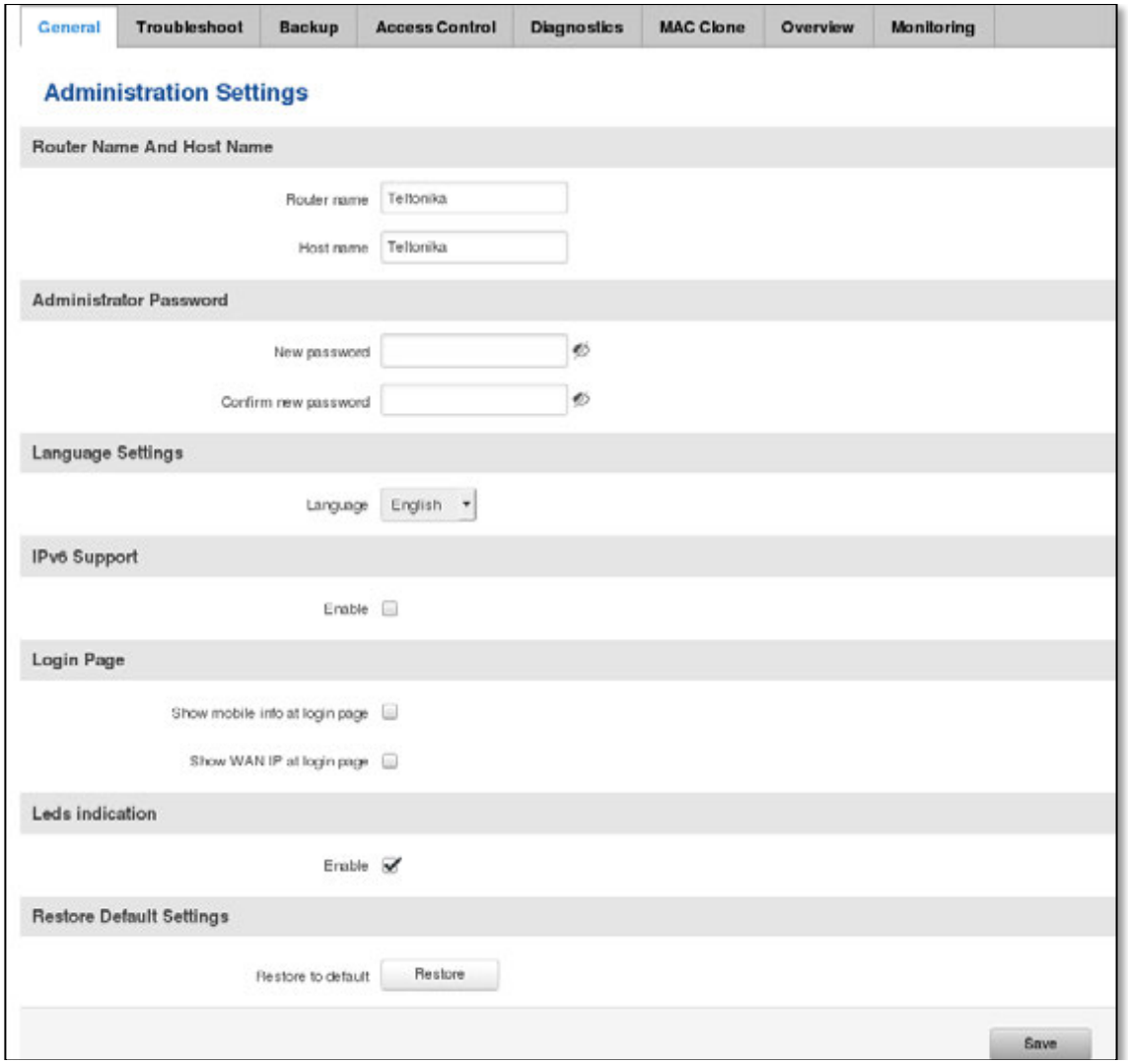
10.2 Profiles

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



10.3 Administration

10.3.1 General



	Field name	Explanation
1.	Router name	Enter your new router name.
2.	Host name	Enter your new host name
3.	New Password	Enter your new administration password. Changing this password will change SSH password as well.

4.	Confirm new password	Re-enter your new administration password.
5.	Language	Website will be translated into selected language.
6.	IPv6 support	Enable IPv6 support on router
7.	Show mobile info at login page	Show operator and signal strength at login page.
8.	Show WAN IP at login page	Show WAN IP at login page.
9	On/Off LEDs	If uncheck, all routers LEDs are off.
10	Restore to default	Router will be set to factory default settings

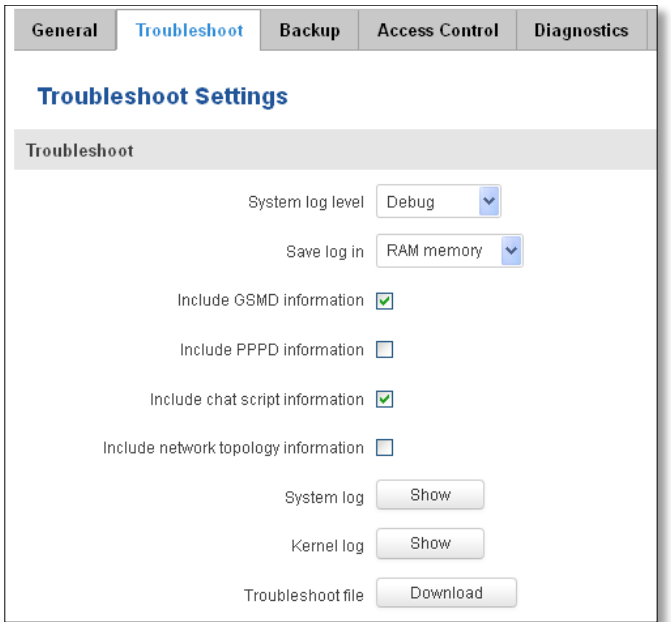
Important notes:

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

User Name: **admin**

Password: **admin01**

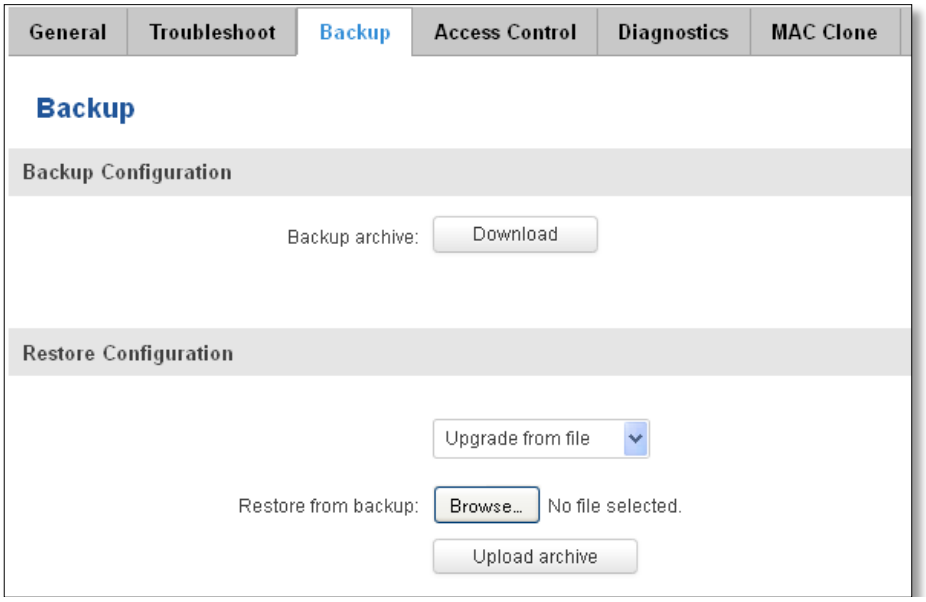
10.3.2 Troubleshoot



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

8.	Kernel Log	Provides on-screen Kernel logging information. It does not, however, substitute troubleshooting file that can be downloaded from System -> Backup and Firmware menu.
9.	Troubleshoot file	Downloadable archive, that contains full router configuration and all System log files.

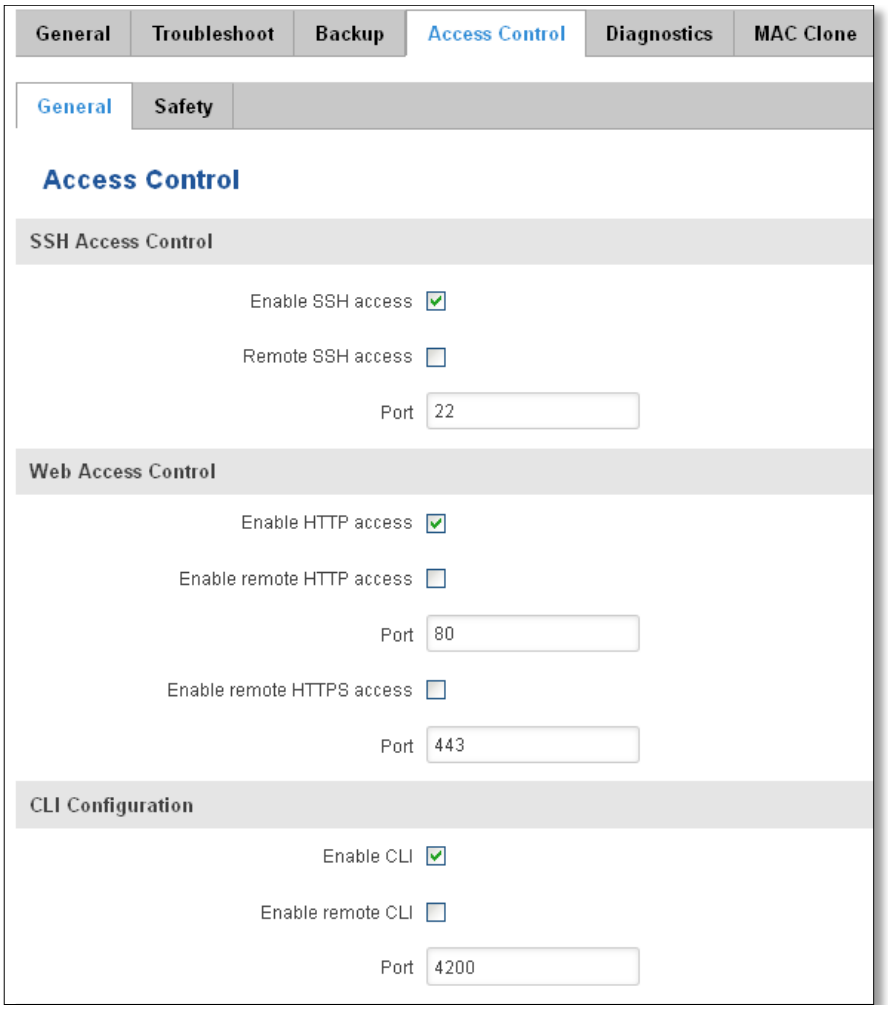
10.3.3 Backup



	Field name	Explanation
1.	Backup archive	Download current router settings file to personal computer. This file can be loaded to other RUT955 with same Firmware version in order to quickly configure it.
2.	Restore from backup	Select, upload and restore router settings file from personal computer.

10.3.3.1 Access control

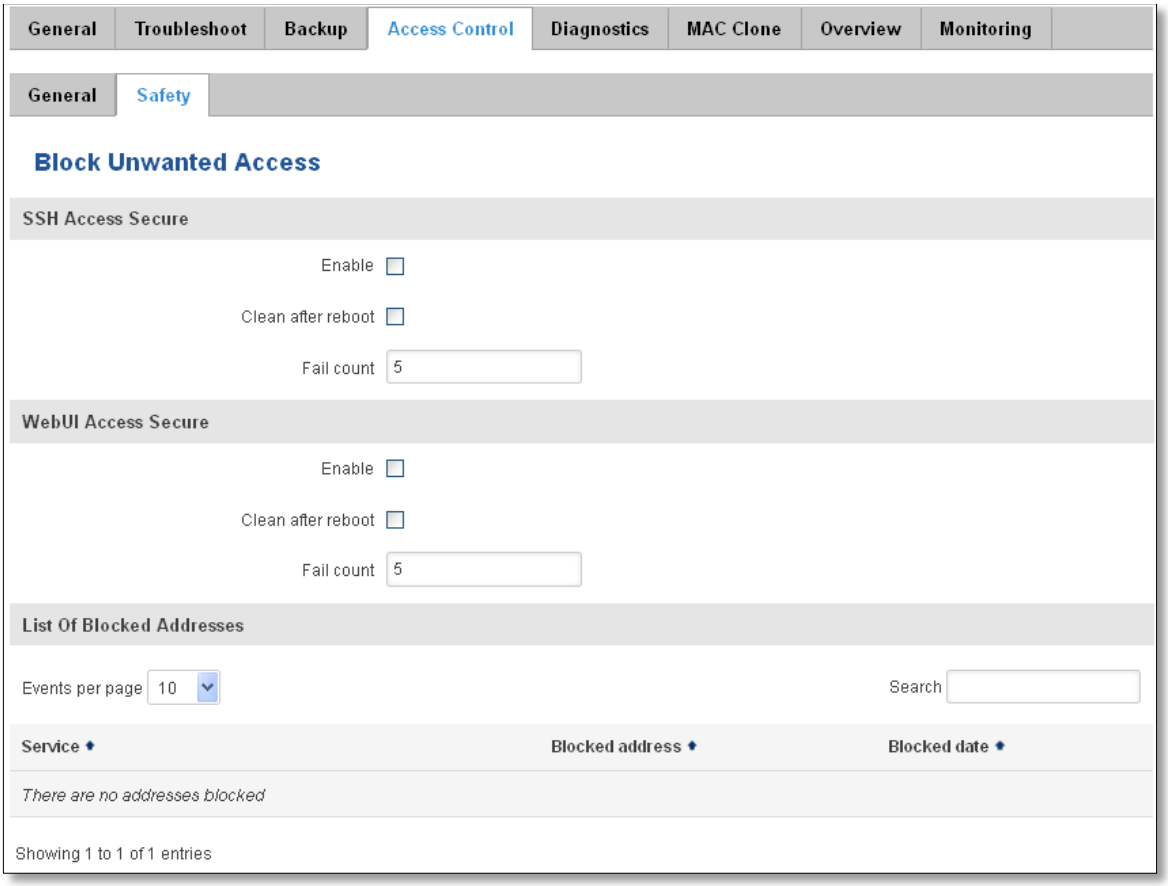
10.3.3.1.1 General



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

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

10.3.3.1.2 Safety



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

10.3.4 Diagnostics

	Field name	Explanation
1.	Host	Enter server IP address or hostname.

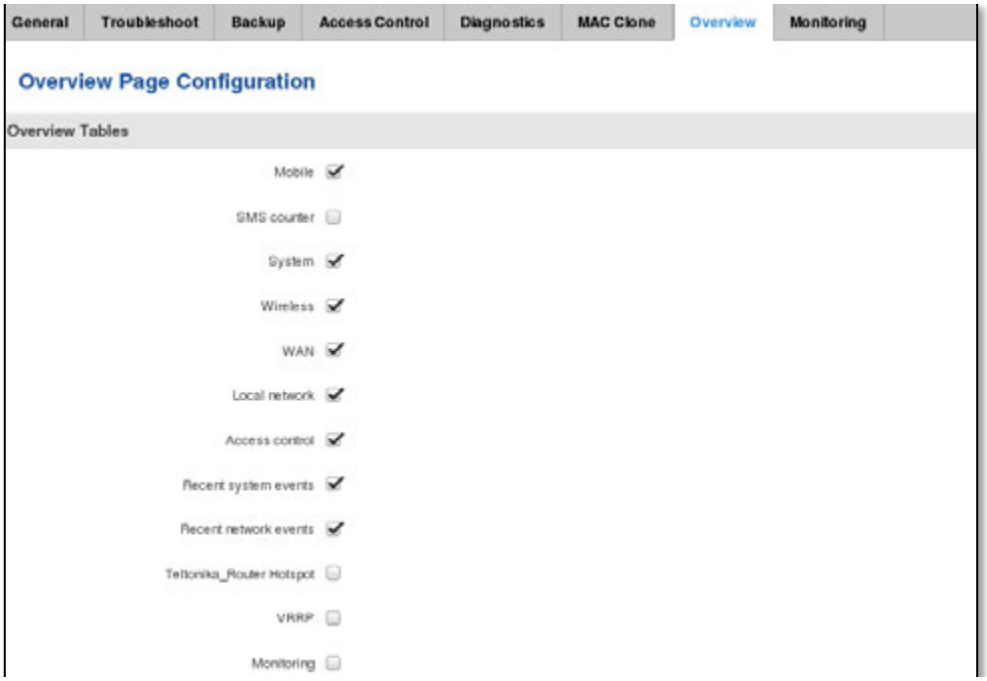
2.	Ping	Utility used to test the reach ability of a host on an Internet IP network and to measure the round-trip time for messages sent from the originating host to a destination server. Server echo response will be shown after few seconds if server is accessible.
3.	Traceroute	Diagnostics tool for displaying 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.

10.3.5 MAC Clone

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

10.3.6 Overview

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

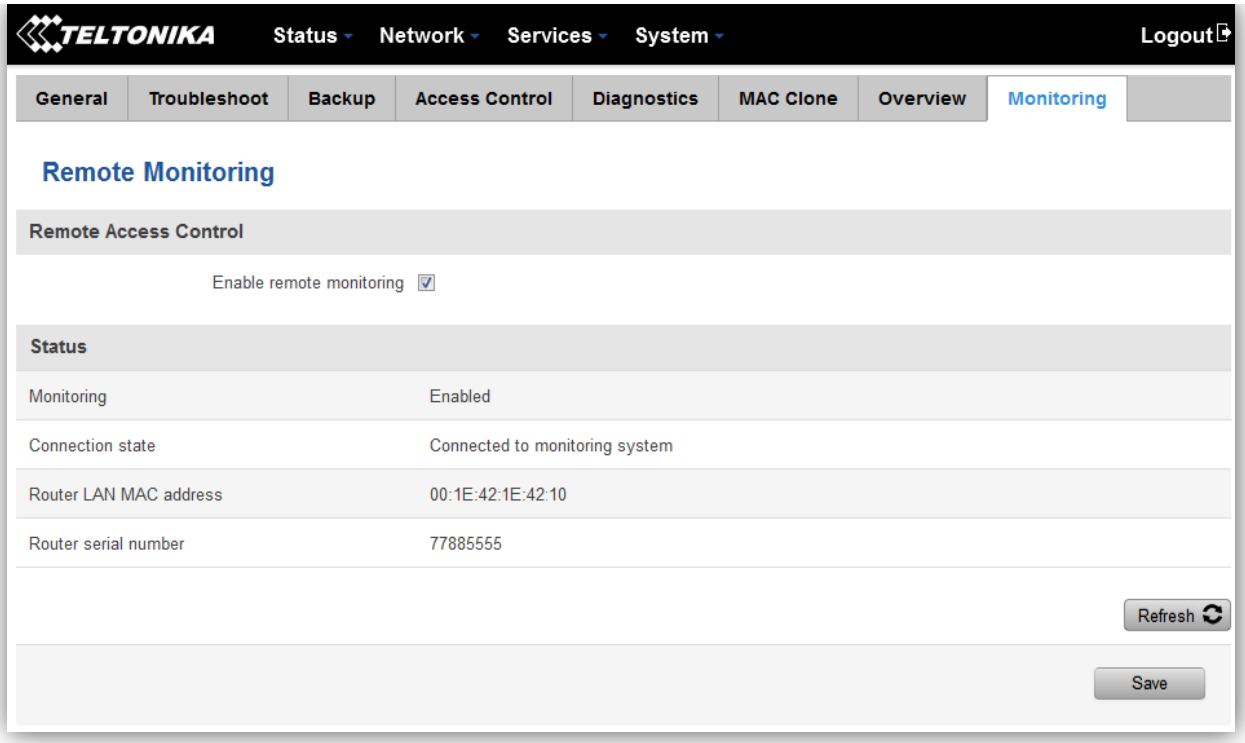


	Field name	Explanation

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

10.3.7 Monitoring

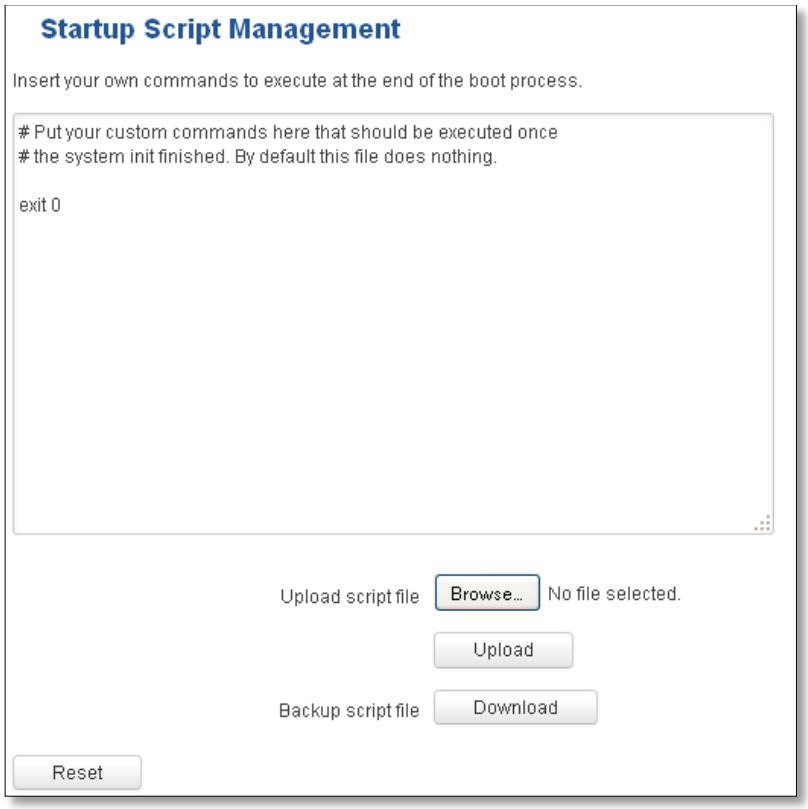
Monitoring functionality allows your router to be connected to Remote Monitoring System. Also MAC address and router serial numbers are displayed for convenience in this page, because they are needed when adding device to monitoring system.



	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

10.4 User scripts

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



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.

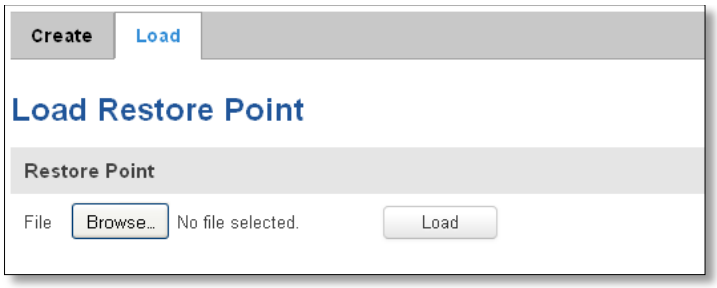
10.5 Restore point

10.5.1 Restore point create

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

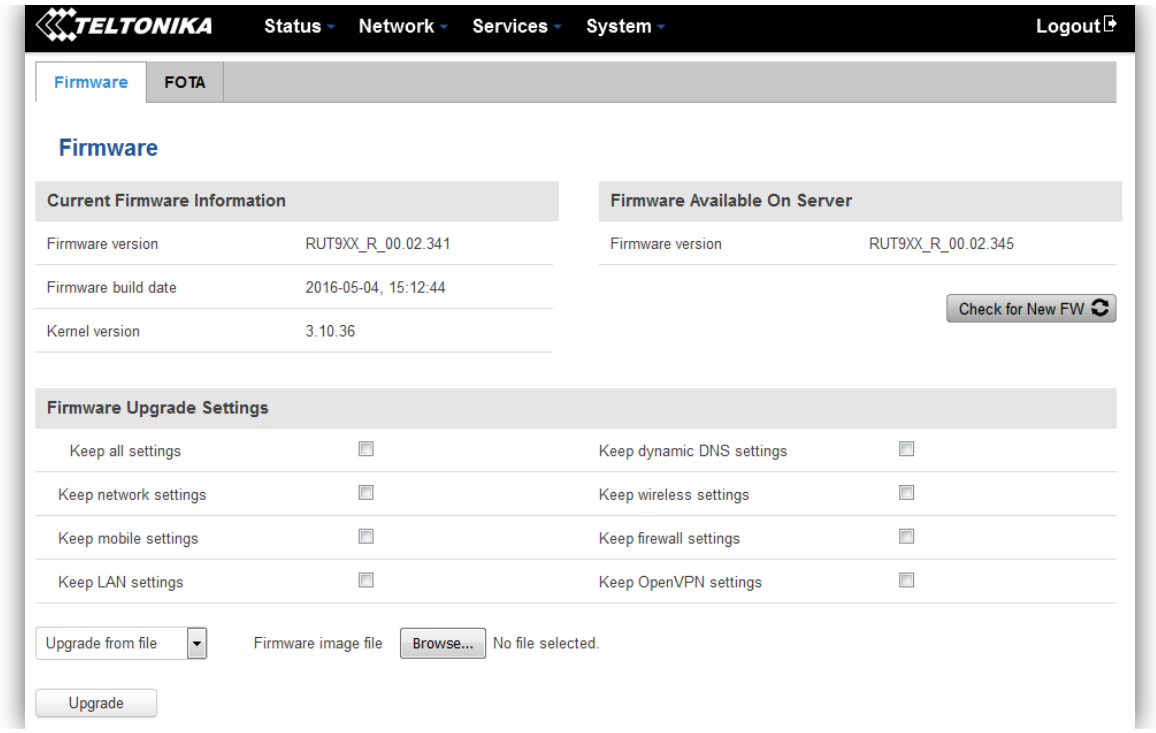
10.5.2 Restore point load

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



10.6 Firmware

10.6.1 Firmware

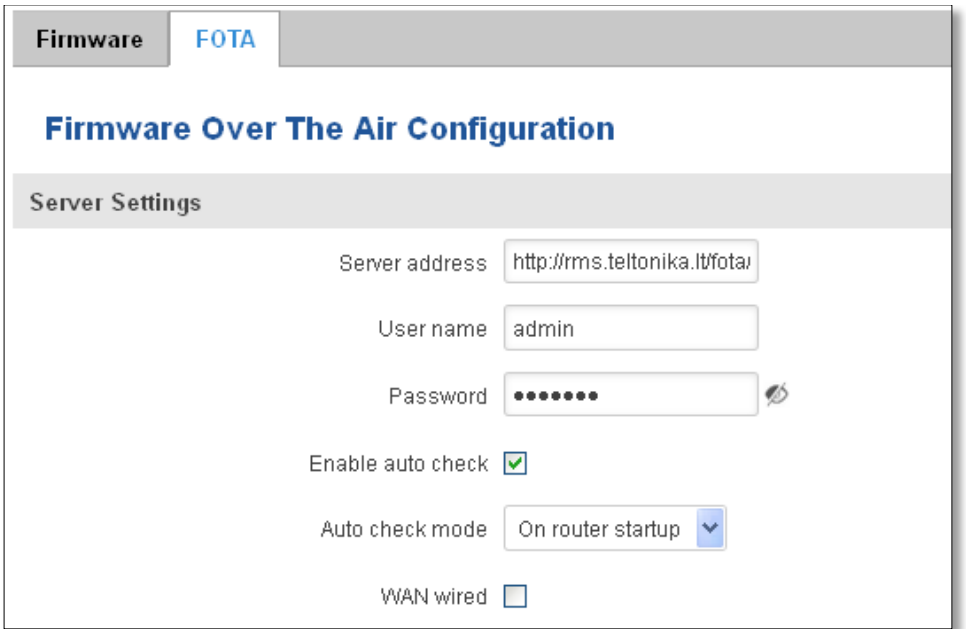


Keep all settings – if the check box is selected router will keep saved user configuration settings after firmware upgrade. When check box is not selected all router settings will be restored to factory defaults after firmware upgrade. When upgrading firmware, you can choose settings that you wish to 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.

10.6.2 FOTA



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

10.7 Reboot

Reboot router by pressing button "Reboot".

11 Device Recovery

The following section describes available options for recovery of malfunctioning device. Usually device can become unreachable due to power failure during firmware upgrade or if its core files were wrongly modified in the file

system. Teltonika's routers offer several options for recovering from these situations.

11.1 Reset button

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

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

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

11.2 Bootloader's WebUI

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

Procedure for starting bootloader's webserver:

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

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

Bootloader's WebUI can be accessed by typing this address in the web browser:

http://192.168.1.1/index.html

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

12 Glossary:

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

LAN – A local area network (LAN) is a computer network that interconnects computers in a limited area such as a

home, school, computer laboratory, or office building.

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

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

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

DNS – Domain Name Resolver.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 layerprotocol used to convert an IP address into a physical address (called a *DLC address*), such as an Ethernet address.

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

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

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

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

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

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

TKIP – Temporal Key Integrity Protocol – scrambles the keys using hashing algorithmand, 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 enchanged data cryptographic encapsulation designed for data confidentiality and

based upon the Counter Mode with CBC-MAC (CCM) of the AES (Advanced Encyprion Standard) standard.

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

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

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

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

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

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

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

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

13 Changelog

Nr.	Date	Version	Comments
1	2017-02-01	1.26	