USER MANUAL

for RUT750 LTE
Outdoor Router
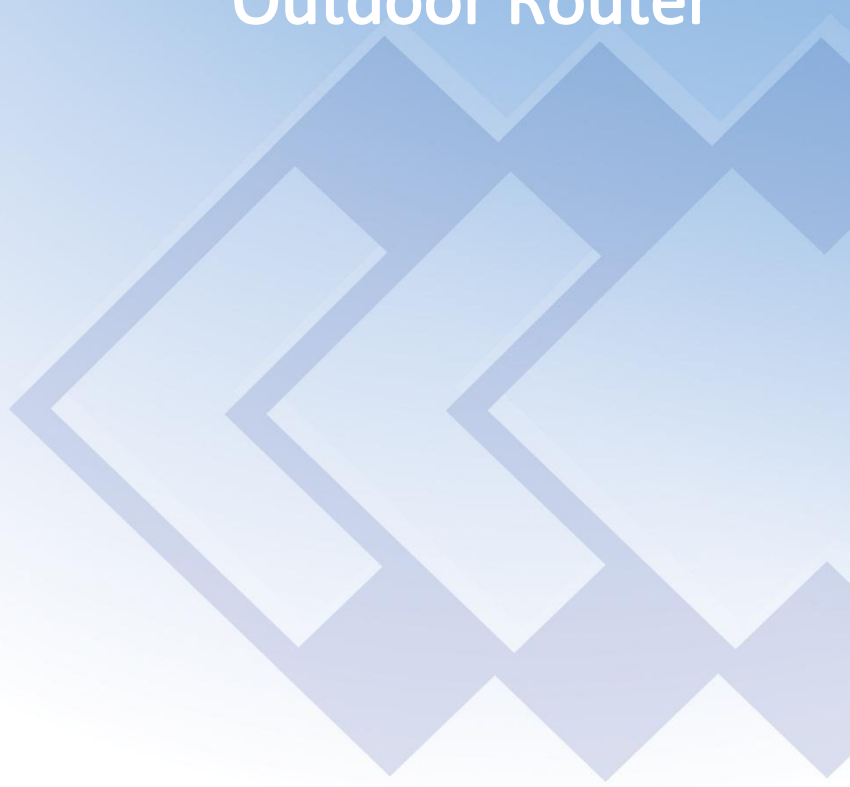
Legal notice

Attention

	Before using the device we strongly recommend reading this manual first.
	Do not rip open the device. Do not touch the device if the device block is broken.
	The device should only be serviced by qualified personel.
	All wireless devices for data transferring may be susceptible to interference, which could affect performance.
	The device is water-resistant (IP65) and can be mounted outdoor, though power adapter must be kept dry.

Table of Contents

SAFETY INFORMATION

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

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

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

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

The highest transient overvoltage in the output (secondary circuit) of used PSU shall not exceed 71V peak.

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

Do not mount or service the device during a thunderstorm.

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

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

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

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

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

Device connection
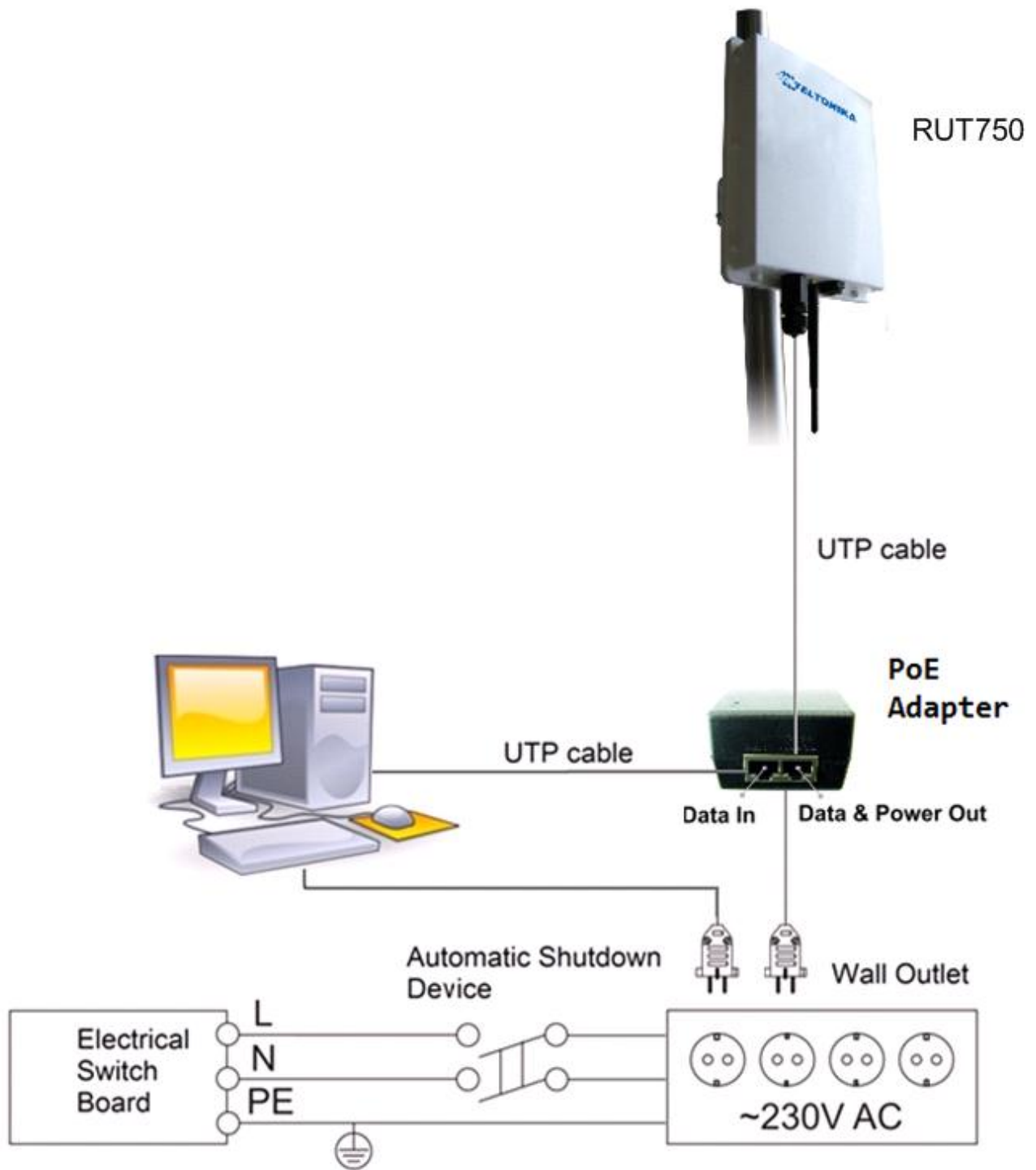
Introduction

Thank you for purchasing a RUT750 LTE router!

Teltonika RUT750 is outdoor LTE router with high speed wireless and Ethernet connections. Internal LTE modem can reach download rate of up to 100Mbps. Router supports the latest IEEE802.11n as well as IEEE802.11b/g standards and provides wireless receiving and transmitting rate of up to 150 Mbps. High gain directional antenna LTE antenna allows the router to be used in low signal locations while external Wi-Fi connector makes it possible to attach desired antenna. IEEE 802.3af-2003 compliant POE uses single Ethernet cable to communicate with the device and to power it making for an easy installation.

Key features

- LTE downlink of up to 100Mbps
- LTE uplink of up to 50Mbps
- DC-HSPA+ downlink of up to 42Mbps
- DC-HSPA+ uplink of up to 5.76Mbps
- Complies with IEEE 802.11n, IEEE 802.11g, IEEE 802.11b wireless standards
- Complies with IEEE 802.3 and IEEE 802.3u standards
- IEEE 802.3af-2003 compliant POE
- One 10/100 Base-T Ethernet port
- Adjustable pole mounting kit
- Waterproof RJ45 socket
- Secure SIM card socket
- Dual-poliarization 6/8 dBi MIMO antenna
- Integrated OpenVPN, IPSec and Dynamic DNS
- SMS reboot function

Specifications

LTE
- FDD 800/850/900/1800/1900/2100/2600 MHz
- Up to 100 Mbps downlink speed
- Up to 50 Mbps uplink speed
- All bands with diversity

UMTS
- 850/900/1900/2100 MHz
- DC-HSPA+ mode: DL up to 43.2 Mbps, UL 5.76 Mbps
- HSPA+ mode: DL up to 21.6 Mbps, UL 5.76 Mbps
- UMTS mode: 384 kbps DL/384 kbps UL
- All bands with diversity

GSM/GPRS/EDGE
- 850/900/1800/1900 MHz
- Power Class 4 (2 W, 33 dBm) GSM/GPRS 850/900 MHz
- Power Class 1 (1 W, 30 dBm) GSM/GPRS 1800/1900 Mhz
- Power Class E2 (0.5 W, 27 dBm) for EDGE 850/900 MHz
- GPRS: 85.6 kbps DL/85.6 kbps UL (class 12)
- EDGE: 236.8 kbps DL/236.8 kbps UL (class 12)

LAN and Wi-Fi

- High performance 320 MHz CPU with 256 Mbits SDRAM
- IEEE 802.11b/g/n, IEEE 802.3, IEEE 802.3u standards
- IEEE 802.3af-2003 compliant POE
- 64/128-bit WEP, WPA, WPA2, WPA&WPA2 encryption methods
- 1x LAN 10/100Mbps Ethernet port
- Supports Auto MDI/MDIX
- Remote/local Web management
- 1x RP-SMA Wi-Fi antenna connector
- SSID stealth mode and access control based over MAC address
- System log to record the status of the Router
- Auto negotiation/manual mode for IEEE 802.11b/g/n
- Dynamic DNS
- LAN access control over Internet connection
- Virtual server
- Auto wireless channel selection
- OpenVPN, IPSec, PPPoE
- SMS and Ping reboot, Status via SMS
- 1 x LAN LED

Electrical, Mechanical & Environmental

- Dimensions (H x W x D)   290mm x 240mm x 45mm
- Weight   1.3kg
- Power supply   36 – 57VDC POE adapter
- Power consumption   < 7W
- Antenna connectors   1 x RP-SMA for Wi-Fi
- Indicators   1 x Power LED, 1 x LAN LED, 1 x Status LED
- Operating temperature   -20º to 50º C
- Storage temperature   -20º to 70º C
- Operating humidity   10% to 90% Non-condensing
- Storage humidity   5% to 95% Non-condensing

Applications

Device can provide internet connection by either Wi-Fi or Ethernet cable. Ethernet switch can be used to provide more Ethernet ports and to be able to connect several devices.
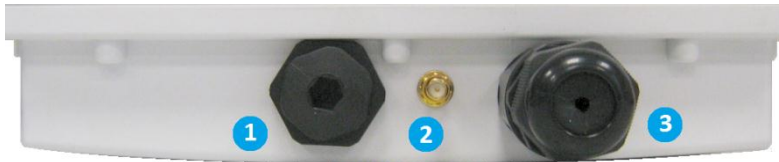
Setting up your router

Installation

After you unpack the box, follow the steps, documented below, in order to properly connect the device.
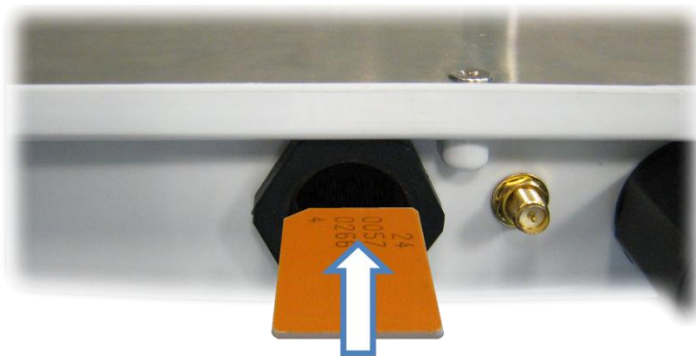
Connectors

1. SIM card
2. Wi-Fi antenna connector
3. Ethernet connector

Inserting the SIM card

- Remove the hex cap which is protecting the SIM holder

- Insert the SIM card. Correct SIM card orientation is shown in the picture

- Screw the protecting hex cap back on

Connecting the device

To set up the router perform these steps:

- Connect your PC, PoE power supply adapter and router using included LAN cables as shown in the picture bellow (make sure that the power LED on the router lights up), attach Wi-F i antenna if required
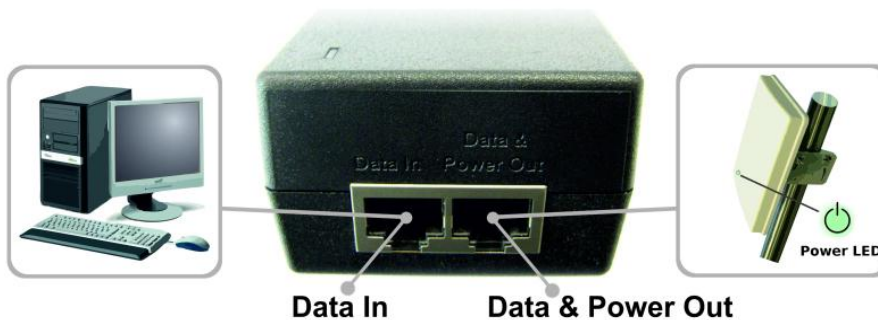
- Plug the PoE power supply adapter into an AC socket

- Connect to the using Ethernet cable or wirelessly (SSID: Teltonika)

- Find the best signal location and secure the router on a pole

Note: Device position and angle has a big impact on the performance. By monitoring the **Status** window in the WebUI try to find a location with the best signal quality.

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)

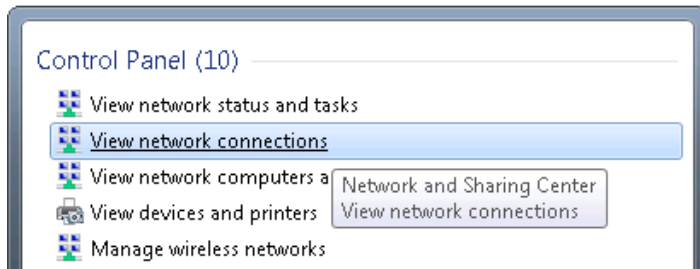We first must set up our network card so that it could properly communicate with the router.
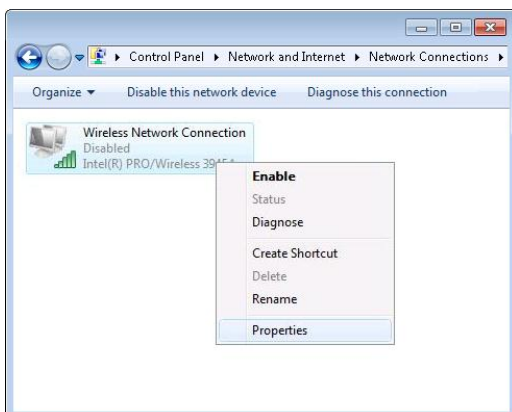
1. Press the start button
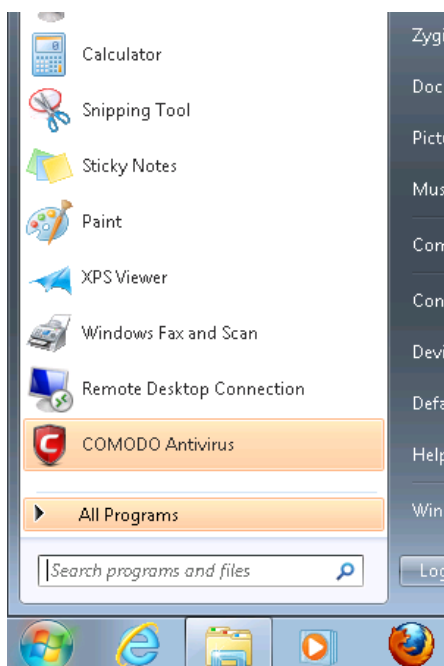
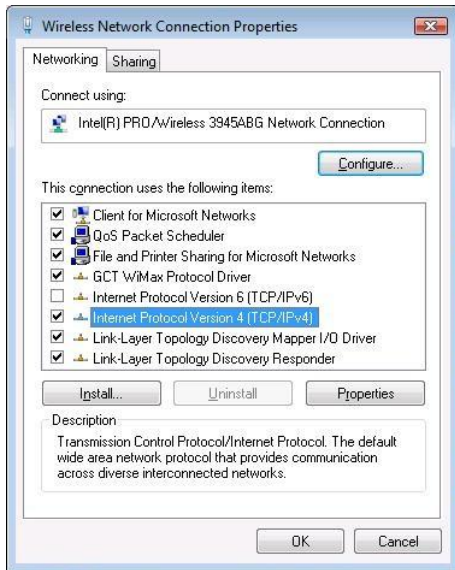2. Type in "network connections", wait for the results to pop up.
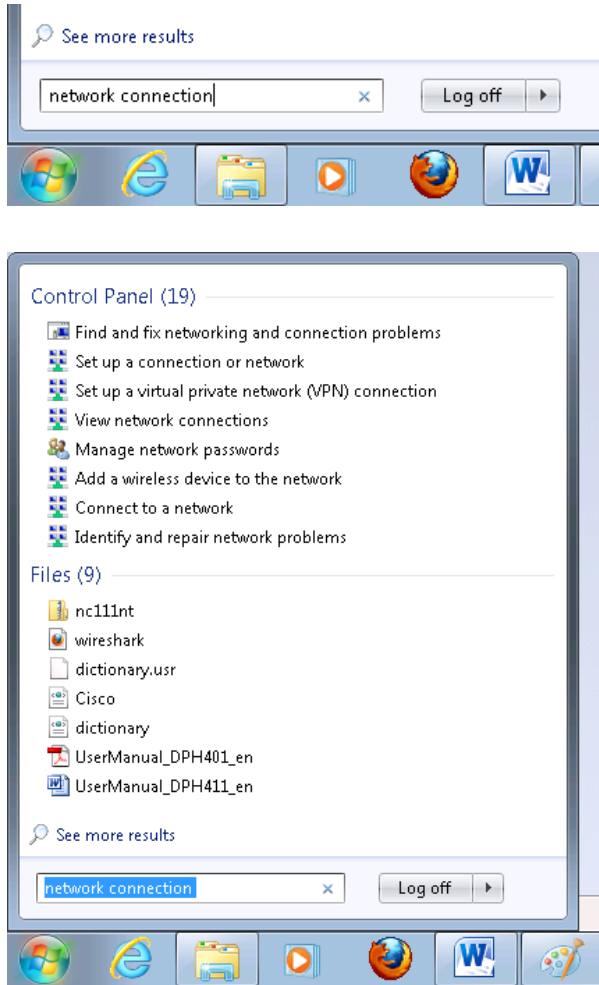

3. Click "View network connections"

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

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

6. By default the router is going to have DHCP enabled, which means that if you select "Obtain an IP address automatically" and "Obtain DNS server address automatically", the router should lease you an IP and you should be ready to login.
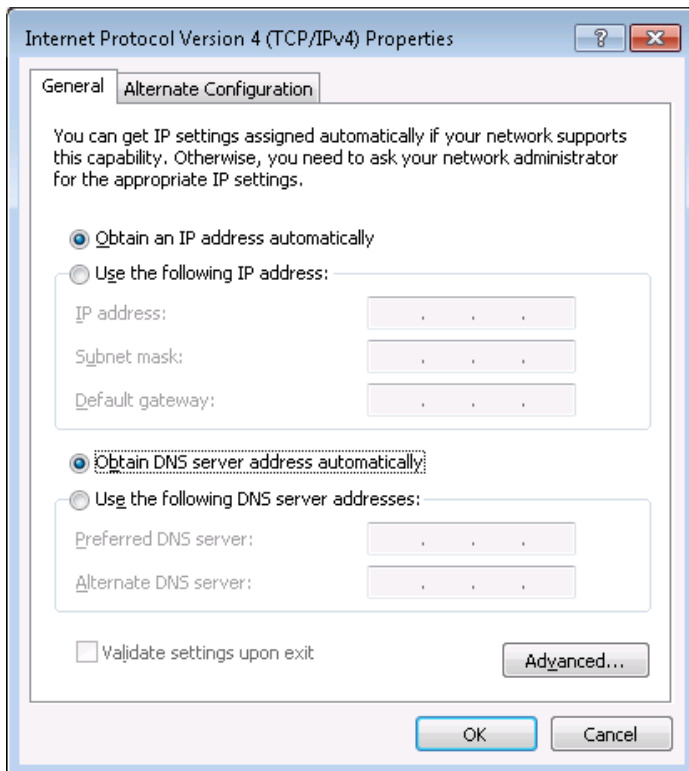
7. If you choose to configure manually here's what you do:
   First select an IP address. Due to the stock settings that your router has arrived in you can only enter an IP in the form of 192.168.1.XXX , where XXX is a number in the range of 2-254 (192.168.1.2 , 192.168.1.254 , 192.168.1.155 and so on… are valid; 192.168.1.0 , 192.168.1.1 , 192.168.1.255 , 192.168.1.699 and so on… are not). Next we enter the subnet mask: this has to be "255.255.255.0". Then we enter the default gateway: this has to be "192.168.1.1". Finally we enter primary and secondary DNS server IPs. One will suffice, though it is good to have a secondary one as well as it will act as a backup if the first should fail. The DNS can be your routers IP (192.168.1.1), but it can also be some external DNS server (like the one Google provides: 8.8.8.8).
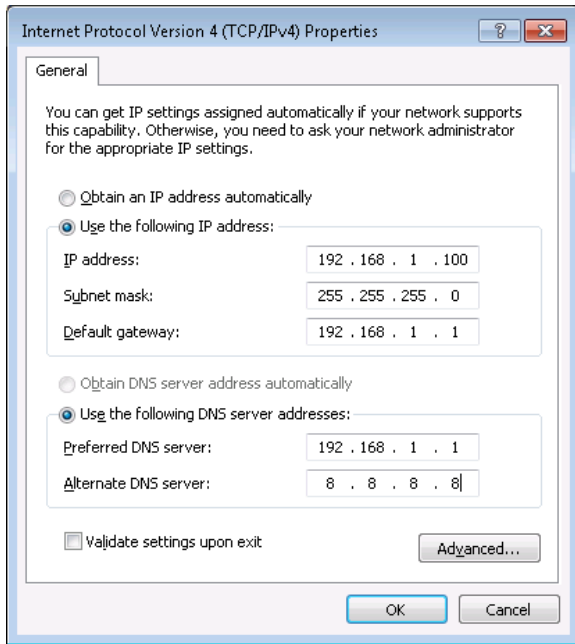
Right click on the Wireless network icon and select **Connect / Disconnect**. A list should pop up with all available wireless networks. Select "Teltonika" and click **connect**.
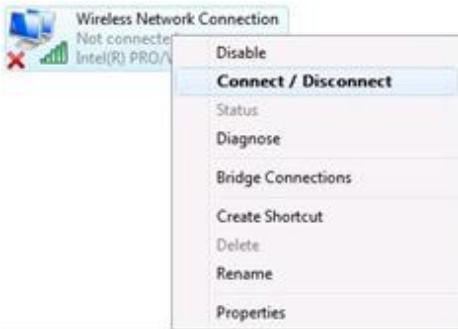
Launch your favorite browser and enter the routers IP into the address field:

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

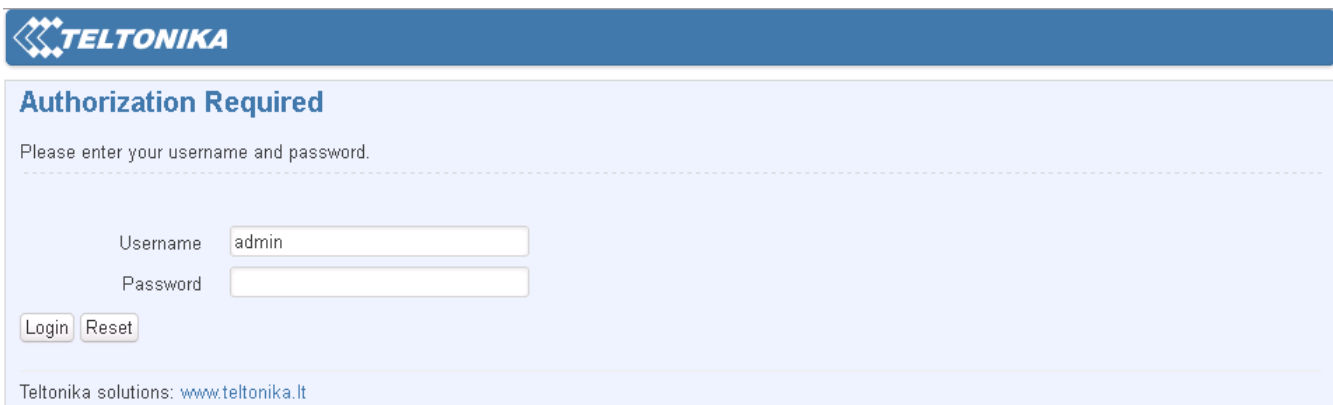Enter the default password, which is "admin01" into the "Password" field and then either click Login with your mouse or press the Enter key. You have now successfully logged into the router and should see the Status page.

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

Operation Modes

The router supports various operation modes. It can be connected to the internet (WAN) via LTE, standard Ethernet cable or via a wireless network. If you connect to the internet via an Ethernet cable of Wi-Fi, you may also backup your connection with LTE for added stability. Selected WAN type determines available LAN interfaces:

WAN	LAN		LTE Backup link
	Ethernet	Wi-Fi	
LTE	√	√	x
Ethernet	x	√	√
Wi-Fi	√	x	√

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

Function explanations

The following sections contain a detailed explanation of every page, tab and sub tab of the configuration interface in the order that they appear on the router.

Status

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

System Information

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

System

	Field Name	Sample value	Explanation
1.	Router Name	Teltonika	Name of the router (hostname of the routers system).
2.	Router Model	Teltonika RUT750	Routers model.
3.	Firmware Version	RUT750_T_00.00.436	Shows the version of the firmware that is currently loaded in the router. Newer versions might become available as new features are added. Use this field to decide whether you need a firmware upgrade or not.
4.	Kernel Version	3.2.15	The version of the Linux kernel that is currently running on the router.
5.	Local Time	Fri Jun 29 16:38:48 2012	Shows the current system time. Might differ from your computer, because the router synchronizes it's time with an NTP server.
6.	Uptime	4h 29m 3s	Indicates how long it has been since the router booted up. Reboots will reset this timer to 0.
7.	Load Average	0.98, 0.57, 0.30	Indicates how busy the router is. Let's examine some sample output: "2.43, 2.96, 3.41". The first number 2.43 means that in the past minute there have been, on average, 2.43 processes running or waiting for a resource. The second number show that in the past 10 minutes, on average, there have been 2.96 processes running or waiting for a resource. The last number indicates the same on the last 15 minutes.

Memory

	Field Name	Sample Value	Explanation
1.	Total Available	14416/29964	Shows how much memory is available to maintain routers functionality.
2.	Free	1476/29964	The amount of memory that is completely free. Should this rapidly decrease or get close to 0, it would indicate that the router is running out of memory, which could cause crashes and unexpected reboots.
3.	Cached	9868/29964	The size of the area of memory that is dedicated to storing frequently accessed data.
4.	Buffered	3072/29964	The size of the area in which data is temporarily stored before moving it to another location.

Network Information

This page is much like the status page, previously described, though dedicated to data associated with networking.

LTE

Statistics for the LTE modem and the connection.

	Field Name	Explanation
1.	State	Shows the state of the connection.
2.	IMEI	Shows the LTE modem's IMEI number.
3.	Sim card state	Indicates whether the SIM card is inserted or not.
6.	Signal strength	Indicates connection strength.
7.	Operator	Indicates the operator of the mobile network.
8.	Connection type	Indicates the connection type.
9.	Bytes received	How many bytes were received via LTE.
10.	Bytes sent	How many bytes were sent via LTE.

WAN

Statistics on the routers WAN connection.

	Field Name	Sample Value	Explanation
1.	Interface	3G	Specifies through what medium the router is connecting to the internet. This can either be Wired, 3G or Wi-Fi.
2.	Type	DHCP	Specifies the type of connection. This can either be static, DHCP, PPPoE or LTE.
3.	IPv4 address	10.12.104.103	The IP address that the routers uses to connect the internet.
4.	Netmask	255.255.255.240	Indicates the networks netmask.
5.	Gateway	10.12.104.97	Indicates the default gateway, an address where traffic destined for the internet is routed to.
6.	DNS#	8.8.8.8	Domain name server(s).
7.	Expires	1h 57m 25s	The amount of time before the routers DHCP lease expires.
8.	Connected	0h 2m 2s	How long the connection has been successfully maintained.

LAN

	Field Name	Sample Value	Explanation
1.	IPv4 address	192.168.1.161	Address that the router uses on the LAN network.
2.	Netmask	255.255.255.0	Indicates the networks netmask.
3.	Connected	0h 6m 14s	How long LAN has been successfully maintained.

18

Wireless

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

Client

	Field Name	Sample Value	Explanation
1.	SSID	teltonika_rnd_division_ap	The SSID that the AP, to which the routers is connected to, uses.
2.	Mode	Client	Connection mode – Client indicates that the router is a client to some local AP.
3.	Channel	6 (2.44 GHz)	The channel that the AP, to which the routers is connected to, uses. Your wireless radio is forced to work in this channel in order to maintain the connection.
4.	BSSID	C8:3A:53:02:FC:B0	The MAC address of the access points radio.
5.	Encryption	WPA2 PSK (CCMP)	The AP, to which the router is connected to, dictates the type of encryption.
6.	Bit rate	65.0 MBit/s	The physical maximum possible throughput that the routers radio can handle. Keep in mind that this value is cumulative - The bitrate will be shared between the router and other possible devices that connect to the local AP.
7.	Country	LT	Country code.

AP

	Field Name	Sample Value	Explanation
1.	Signal Quality	100%	The quality between routers radio and some other device that is connecting to the router. Will show 0% if no devices are trying to connect or are currently maintaining a connection.
2.	SSID	Teltonika_demo	The SSID that is being broadcast. Other devices will see this and will be able to use to connect to your wireless network.
3.	Mode	Master	Connection mode – Master indicates that you router is an access point.
4.	Channel	6 (2.44 GHz)	The channel which is used to broadcast the SSID and to establish new connections to devices.
5.	BSSID	00:0C:43:30:50:38	MAC address of your wireless radio.

6.	Encryption	WPA2 PSK (CCMP)	The type of encryption that the router will use to authenticate, establish and maintain a connection.
7.	Bit rate	1.0 MBit/s	The bitrate will be shared between all devices that connect to the routers wireless network.
8.	Country	LT	Country code.

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

Associated Stations

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

This can either be the information of the Access Point that the router is connecting to in Client Mode OR a list of all devices that are connecting to the router in Access Point mode:

DHCP Leases

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

The picture above shows a DHCP lease for an Android phone that is currently connecting to the routers Access Point.

Backup WAN

When enabled this field will indicate the health of your primary connection:

IN USE	Indicates that the connection is being used for main traffic.
READY	Indicates that the connection is ready to take over network traffic, if the other link should fail.
NOT READY	Indicates that the connection is down.

More on this see the main backup WAN section of this manual.

Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	Interface
192.168.0.30	70:71:bc:0c:f9:f5	br-lan
192.168.99.254	00:00:00:00:00:00	eth0.2

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric
wan	0.0.0.0/0	192.168.99.254	0
lan	192.168.0.0/24	0.0.0.0	0
wan	192.168.99.0/24	0.0.0.0	0

Teltonika solutions: www.teltonika.lt

ARP

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

Active IPv4-Routes

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

Network	Protocol	Source	Destination	Transfer
IPV4	TCP	192.168.0.156:37706	192.168.99.30:3389	613.24 KB (8338 Pkts.)
IPV4	UDP	192.168.0.19:137	192.168.0.255:137	7.24 KB (84 Pkts.)
IPV4	UDP	192.168.0.19:138	192.168.0.255:138	5.20 KB (24 Pkts.)
IPV4	TCP	192.168.0.156:52547	173.194.78.139:80	3.30 KB (11 Pkts.)
IPV4	TCP	192.168.0.156:38821	199.127.194.80:80	1.97 KB (17 Pkts.)
IPV4	UDP	192.168.1.9:67	255.255.255.255:68	1.13 KB (2 Pkts.)
IPV4	TCP	192.168.0.156:42797	209.85.148.148:80	930.00 B (5 Pkts.)
IPV4	TCP	192.168.0.30:55669	192.168.0.161:80	703.00 B (3 Pkts.)
IPV4	UDP	0.0.0.0:68	255.255.255.255:67	688.00 B (2 Pkts.)
IPV4	UDP	192.168.0.5:67	255.255.255.255:68	604.00 B (2 Pkts.)
IPV4	UDP	192.168.0.156:54245	8.8.8.8:53	142.00 B (2 Pkts.)
IPV4	UDP	192.168.0.156:41391	8.8.8.8:53	66.00 B (1 Pkts.)

On the same page you can also analyze a detailed list of all active connections that the router maintains. Each entry consists of a type of network ("IPV4"), protocol (TCP, UDP, ICMP), the source address (an IPv4 address + the source port), the destination address (an IPv4 address + the destination port) and how much traffic has gone through that particular connection: its size in Bytes and the amount of packets.

Network

LTE

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

The configuration is simple and straightforward. Here we will gloss over all the fields:

	Field name	Possible values	Explanation
1.	LTE connection	Use pppd mode Use NDIS mode Use bridge mode	Pppd mode uses dialing number to establish data connection. NDIS mode (default) does not use dialing to establish data connection and is usually faster than pppd mode. Bridge mode bridges LTE data connection with LAN. In this mode the router does not have internet connection as ISP provides IP directly to end device (PC, tablet or smartphone).
2.	APN	"bangapro"	**Access Point Name** (APN) is a configurable network identifier used by a mobile device when connecting to a GSM carrier.
3.	PIN Number	"5555" or any number that falls between 0000 and 9999	A **personal identification number** is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system.
4.	Dialing number	"*99#"	Dialing number is used only in pppd mode to establish data connection.
5.	Authentication method	CHAP, PAP or none	Authentication method, that your carrier uses to authenticate new connections. (This selection is unavailable on the alternate model)
6.	Username	"user"	Your username and password that you would use to connect to your carriers network. These field become available when you select an authentication method (i.e. authentication method is not "none"). These fields are always enabled on the alternate model.
7.	Password	"passwd"	
8.	Service mode	GSM, UMTS, LTE or	Your network preference. If your local mobile network supports GSM

		automatic.	(2G), UMTS (3G) and LTE (4G) you can specify to which network you wish to connect. E.g.: if you choose GSM (2G), the router will connect to a GSM (2G) network, so long as it is available, otherwise it will connect to a LTE (4G) network. If you select auto, then the router will connect to the network that provides better connectivity.

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

WAN

WAN configuration is, arguably, the crux of the routers configuration as it determines how the router will connect to the internet. Here is quick rundown of how the page looks and what each field means.

Operation Mode
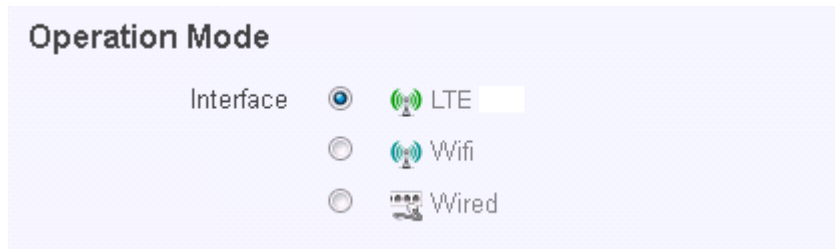
First and foremost a mode of connection has to be defined. Available selections:

	Type	Description
1.	Wired	An Ethernet cable connected to the WAN port of the router.
2.	Wifi	The router will be able to connect to a local wireless access point and reach the internet through it.
3.	LTE	The router will connect to your local mobile network for LTE access.

Common configuration

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

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

General

This area is dedicated for protocol specific options.

Static:

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

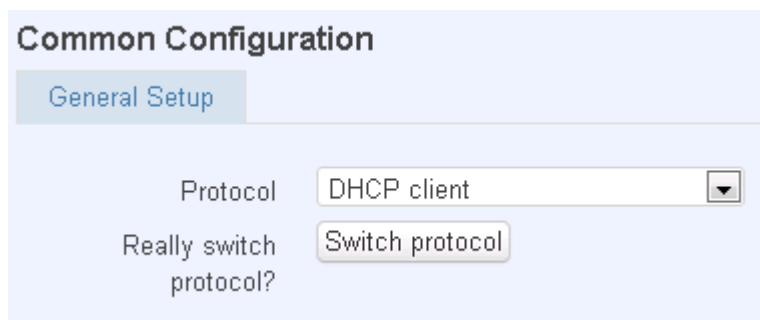|	Filed name	Sample	Explanation
1.	IPv4 address	192.168.99.162	Your routers address on the WAN network
2.	IPv4 netmask	255.255.255.0	A mask used to define how "large" the WAN network is
3.	IPv4 gateway	192.168.99.254	Address where the router will send all the outgoing traffic
4.	IPv4 broadcast	192.168.99.255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

DHCP:

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

PPPoE. This protocol is mainly used by DSL providers:

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

	Filed name	Sample	Explanation
1.	PAP/CHAP username	test	Your username and password that you would use to connect to your carriers network.
2.	PAP/CHAP password	your_password	
3.	Access Concentrator	isp	Specifies the name of access concentrator. Leave empty to autodetect.
4.	Service Name	isp	Specifies the name of the service. Leave empty to autodetect.

Advanced

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

Static:

	Field name	Sample value	Explanation
1.	Bring up on boot	On	Specifies whether the interface will be configured and brought up when the router boots up. Disabling will render your WAN connection non-functional
2	Disable NAT	On/Off	Toggle NAT on and off.
3.	Override MAC address	00:0C:43:30:50:38	Override MAC address of the WAN interface. If your ISP gives you a static IP address it might also bind it to your computers MAC

				address (i.e. that IP will only work with your computer). In this field you can enter your computers MAC address and fool the gateway in thinking that it is communicating with your computer.
4.	Override MTU	1500	**Maximum transmission unit** – specifies the largest possible size of a data packet.
5.	Use gateway metric	0	The WAN configuration by default generates a routing table entry. With this field you can alter the metric of that entry.

DHCP:

PPPoE:

IP Aliases

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

```
IP-Aliases
SUBNET55
  General Setup      Advanced Settings

      IPv4-Address    192.168.55.161
      IPv4-Netmask    255.255.255.0        ▼
      IPv4-Gateway    192.168.55.153
  Delete

                                    Add
```

As you can see, the configuration is very similar to the static protocol; only in the example a 55'th subnet is defined. Now if some device has an IP in the 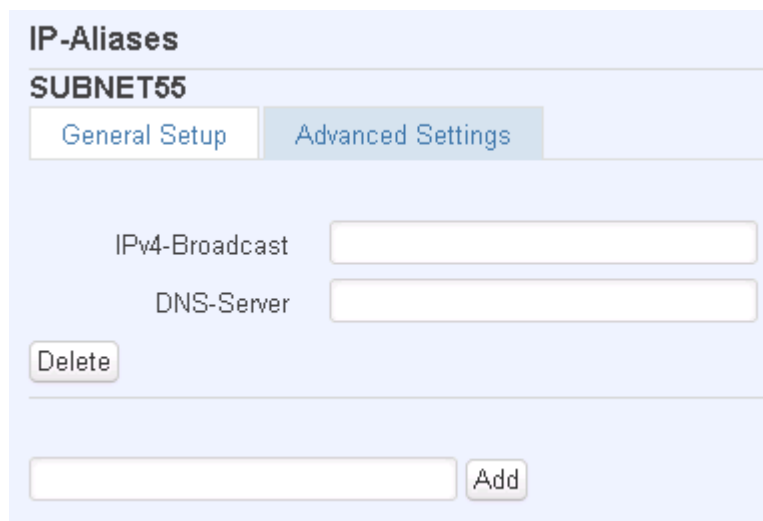55 subnet (192.168.55.xxx) and the subnets gateway metric is "higher" and the device is trying to reach the internet it will reroute it's traffic not to the gateway that is defined in common configurations but through the one that is specified in IP aliases.

```
IP-Aliases
SUBNET55
  General Setup      Advanced Settings

      IPv4-Broadcast
      DNS-Server
  Delete

                                    Add
```

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

How do I setup Wi-Fi WAN?

First we must switch the mode to Wi-Ffi. Do so by selecting Wi-F i from the list and wait for the page to quickly reload.

Now you have a selection of protocols available for you. Depending on whether the Access Point that you intend to connect to runs a DHCP server or not, you will have to choose DHCP or Static (AP runs a DHCP server – DHCP; Does not run - Static). When you've configured your protocol settings press Save and wait until the settings are applied.

Next, goto the Network -> Wireless page and wait until it loads (For the first time an automatic Site Survey will be initiated). You should now see a list of available, local Access Points. Choose one and click Join Network.

Should you be asked enter the secret Encryption Key and click Submit.

Now you should be transported to the Wireless Station page. Click Save and wait until all the settings are applied.

The configuration is complete and you should now be able to access the internet.

LAN

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

The common configuration and IP aliasing sections are identical to the ones found in WAN, so for an explanation on how they work please follow through there.

DHCP Server

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

	Field Name	Sample value	Explanation
1.	Disable	Checked/unchecked	Check to **DISABLE** the DHCP server.
2.	Start	100	The starting address of the range that the DHCP server can use to give out to devices. E.g.: if your LAN IP is 192.168.2.1 and your subnet mask is 255.255.255.0 that means that in your network a valid IP address has to be in the range of [192.168.2.1 – 192.168.2.254](192.168.2.0 and 192.168.2.255 are special unavailable addresses). If the Start value is set to 100 then the DHCP server will only be able to lease out addresses starting from 192.168.2.100
3.	Limit	150	How many addresses the DHCP server gets to lease out. Continuing on the above example: if the start address is 192.168.2.100 then the end address will be 192.168.2.254 (100 + 150 – 1 = 254).
4.	Lease time	12h	How long can a leased IP be considered valid. An IP address after the specified amount of time will expire and the device that leased it out will have to request for a new one.

Advanced settings

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

	Field Name	Sample Value	Explanation
1.	Dynamic DHCP	Checked/Unchecked	Dynamically allocate client addresses, if set to `0` only clients present in the `ethers` files are served
2.	Force	Checked/Unchecked	Forces DHCP serving even if another DHCP server is detected on the same network segment.
3.	IPv4 netmask	255.255.255.0	You can override your LAN netmask here to make the DHCP server think it's serving a larger or a smaller network than it actually is.

| 4. | DHCP-Options | 6,192.168.2.1,192.168.2.2
26,1470
option:mtu, 1470 | Additional options to be added for this DHCP server. For example with '26,1470' or 'option:mtu, 1470' you can assign an MTU per DHCP. Your client must accept MTU by DHCP for this to work. |

Wireless

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

Access Point:

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

Device

General

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

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

Advanced

Here you can configure more advanced parameters:

	Field name	Sample value	Explanation
1.	Mode	Auto, b, g, g+n	Different modes provide different throughput and security options.
2.	Country Code	Any ISO/IEC 3166 alpha2 country code	Selecting this will help the wireless radio configure its internal parameters to meet your countries wireless regulations.
3.	Distance Optimization	100	Distance to farthest network member in meters.
4.	Frag. Threshold	2346	The smallest packet size that can be fragmented and transmitted by multiple frames. In areas were interference is a problem, setting a lower fragment threshold might help reduce the probability of unsuccessful packet transfers, thus increasing speed.
5.	RTS/CTS Threshold	2346	Request to send threshold. It can help resolve problems arising when several access points are in the same area, contending.

Interface

General

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

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

Security

Encryption – There are many modes of encryption, though two distinctive classes have to be pointed out.

WEP

Enter the keys that will be used as passphrase for connecting computers and then specify which key will be preferred above the remaining. It's sufficient to enter one key and then specify it as the preferred one. Length is important as well: 10 or 26 characters in length in hex mode OR 5 or 13 in ASCII mode. A hex key may only contain numbers '0' through '9' and letters 'a' through 'f'.

WPA

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

MAC-Filter

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

Client

Client mode is nearly identical to AP, except for the fact that most for the options are dictated by the wireless access point that the router is connecting to. Changing them can result in an interrupted connection to an AP.

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

Backup WAN

Backup WAN is function that allows you to back up your wired OR wireless connection in case they go down. At the current moment you can only backup wired/Wi-F i connection with LTE.

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 the your primary connection. When the connections state starts to change (READY->NOT READY and vice versa) a necessary

33

amount of failed or passed health checks has to be reached before the state changes completely. This delay is instituted so as to mitigate "spikes" in connection availability, but it also extends the time before the backup link can be brought up or down.

	Field Name	Sample value	
1.	Health Monitor Interval	Dsb/5/10/20/30/60/120 Seconds	The interval at which health checks are performed
2.	Health Monitor ICMP HOST	Dsb/DNS/WAN GW/Custom	Where to PING for a health check. As there is no definitive way to determine when the connection to internet is down for good, you'll have to define a host whose availability that of the internet as a whole.
3.	Health Monitor ICMP Timeout	½/3/4/5/10 Seconds	How long to wait for an ICMP request to come back. Set a higher value if your connection has high latency or high jitter (latency spikes).
4.	Attempts Before WAN Failover	1/3/5/10/15/20	How many checks should fail for your WAN connection to be declared DOWN for good.
5.	Attempts Before WAN Recovery	1/3/5/10/15/20	How many checks should pass for your WAN connection to be declared UP.
6.	DNS Servers	Auto/Custom	Define custom DNS servers. Has meaning when you select DNS as your Health Monitor ICMP HOST.
7.	Backup ICMP host	IPv4 address	This is where the address of an ICMP host, that will be used to check the health of your LTE backup link, goes. This has to be a ping-able host.

How do I set up a backup link?

First we must pick a main link: Wired or Wi-Fi, and ensure that the link is working. Configure your WAN settings to use that link and see whether you have internet access. If the main link is working we can continue configuring our Backup Link.

Now, go to Backup WAN page and configure the settings to your liking. Click Save and wait until the settings are applied.

Now in the Status -> Network Information page there should be a status indication for the backup WAN. If everything is working correctly you should see this:

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

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

Backup WAN Status

WAN: [Wired] IN USE   Backup WAN: [3G] READY

If you witness the above sequence, your backup link is working!

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

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

	Field name	Sample value	Explanation
1.	Enable SYN-flood protection	Checked/Unchecked	When checked the router becomes more resistant against SYN-flood attacks.
2.	Drop Invalid packets	Checked/Unchecked	A "Drop" action is performed on a packet that is determined to be invalid
3.	Input	Reject/Drop/Accept	DEFAULT* action that is to be performed for packets that pass through the Input chain.
4.	Output	Reject/Drop/Accept	DEFAULT* action that is to be performed for packets that pass through the Output chain.
5.	Forward	Reject/Drop/Accept	DEFAULT* action that is to be performed for packets that pass through the Forward chain.

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

Accept – Packet gets to continue down the next chain.

Drop – Packet is stopped and deleted.

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

DMZ

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

Port Forwarding
Here you can define your own port forwarding rules.

You can use port forwarding to set up servers and services on local LAN machines. The above picture shows how you can set up a rule that would allow a website that is being hosted on 192.168.99.156, to be reached from the outside by entering http://routersExternalIp:12345/ .

	Field Name	Sample Value	Explanation
1.	Name	"localWebsite"	Name of the rule. Used purely to make it easier to manage rules.
2.	Protocol	TCP/UDP/TCP+UDP/Other	Type of protocol of incoming packet.
3.	External Port	1- 65535	From what port on the WAN network will the traffic be forwarded.
4.	Internal IP address	IPv4 address of some computer on your LAN	The IP address of the internal machine that hosts some service that we want to access from the outside.
5.	Internal port	1-65535	To what port on the internal machine would the rule redirect the traffic.

Additional note: Notice how the external port is 12345 and not 80. It is perfectly fine to define the external port as 80, but then the routers configuration interface would not reachable (unless you change the web access port from remote management).

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

Traffic Rules

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

	Field name	Sample Value	Explanation
1.	Name	"ruleName"	Used to make rule management easier
2.	Family	IPv4	Only IPv4 is currently supported
3.	Protocol	TCP/UDP/Other…	Protocol of the packet that is being matched against traffic rules.
4.	Source	IPv4 address	The source of the packet.
5.	Destination	IPv4 address	The destination of the packet
6.	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.	Enable	Checked/Unchecked	Self-explanatory. Uncheck to make the rule inactive. The rule will not be deleted, but it also will not be loaded into the firewall.
8.	Sort	Up/Down	When a packet arrives, it gets checked for a matching rule. If there are several rules that match the rule, the first one is applied i.e. the order of the rule list impacts how your firewall operates, therefore you are given the ability to sort your list as you wish.

Custom Rules

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

Static Routes

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

	Field name	Value	Explanation
1.	Interface	Lan/wan	The zone where the 'Target' resides
2.	Target	IPv4 address	The source of the traffic.
3.	IPv4-Netmask	IPv4 mask	Mask that is applied to the Target to determine to what actual IP addresses the routing rule applies
4.	IPv4-Gateway	IPv4 address	To where the router should send all the traffic that applies to the rule
5.	Metric	integer	Used as a sorting measure. If a packet about to be routed fits two rules, the one with the higher metric is applied.

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

192.168.55.161	255.255.255.255	Only applies to 192.168.55.161
192.168.55.0	255.255.255.0	Applies to IPs in range 192.168.55.0-192.168.55.255
192.168.55.240	255.255.255.240	Applies 192.168.55.240 - 192.168.55.255
192.168.55.161	255.255.255.0	192.168.55.0 - 192.168.55.255
192.168.0.0	255.255.0.0	192.168.0.0 - 192.168.255.255

Diagnostics

Contains Network Utilities used for testing network.

Ping – the utility used to test the reachability of a host on an Internet IP network and to measure the round-trip time for messages sent from the originating host to a destination server. Enter server IP address or hostname and click "Ping". Server echo response will be shown after few seconds if server is accessible.

Traceroute – diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet IP network. Enter server IP address or hostname and click "Traceroute". Log containing route information will be shown after few seconds.

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. Enter server hostname and click "Nslookup". Log containing specified server DNS lookup information will be shown after few seconds. Full manual with all available "Nslookup" commands and parameters can be found in Linux manual page nslookup(1).

Important notes:

- Note that DNS server must be configured correctly if you use server hostname instead of server IP address in address field.

Services

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.

Common configuration

	Field name	Description	Notes
1.	Enable PING Reboot	This check box will enable or disable PING reboot feature.	PING Reboot is disabled by default.
2.	Reboot router if no echo received	This check box will disable router rebooting after the defined number of unsuccessful retries.	This check box must be unselected if you want to use PING Reboot feature as "Keep Alive" function.
3.	Interval between PINGs	Time interval in minutes between two PINGs.	Minimum time interval is 5 minutes.
4.	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.
5.	Server to PING	Server IP address or host name, which will receive PING from router	If you use server host name instead of the IP address you must configure DNS server first.

Important notes:

- Always check if your defined server responds to echo commands before using PING Reboot function. Otherwise router keeps rebooting after unsuccessful PING echo receive. You can test PING send at "Network" > "Diagnostics".

SMS Reboot

It is possible to reboot router via SMS text message. This function is useful when router does not respond and it is difficult to manually restart router by hand.

Common configuration

	Field name	Description	Notes
1.	Enable SMS Reboot	This check box will enable and disable SMS reboot function.	SMS reboot is disabled by default.
2.	SMS text	SMS text which will reboot router.	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.
3.	Sender phone number	Phone number of person who can reboot router via SMS message	You can add as many phone numbers as you need. Dropdown list with additional rows will show up if you click on "add" icon at the end of phone number row.
4.	Get status	Check this to receive connection status via SMS after a reboot.	Disabled by default.

Status via SMS

It is possible to get routers connection status via SMS text message.

Common configuration

	Field name	Description	Notes
1.	Enable SMS Status	This check box will enable and disable SMS status function.	SMS status is disabled by default.
2.	SMS text	SMS text which will send routers status.	SMS text can contain letters, numbers, spaces and special symbols. Capital letters also matters.
3.	Sender phone number	Phone number of person who can receive router status via SMS message	You can add as many phone numbers as you need. Dropdown list with additional rows will show up if you click on "add" icon at the end of phone number row.

Important Notes:

- LTE settings must be configured correctly. If SIM card has PIN number you must enter it at "Network" > "LTE" settings. Otherwise SMS reboot function will not work.

- Sender phone number must contain country code. You can check sender phone number format by reading the details of old SMS text massages you receiving usually.

NTP

Hostname, Network Time Protocol (NTP) and time zone configuration settings is needed to periodically update router local time.

"Sync with browser" button will synchronize local router time with computer browser time.

	Field name	Description	Notes
1.	Current system time	Local time of router.	---
2.	Timezone	Time zone of your country.	---
3.	Run NTP client on startup	This check box will turn on automatic time synchronizing with defined NTP servers.	When check box is selected you must enter one or more working NTP servers. Otherwise time sync feature will not work.
4.	Update interval	Interval between time updates in seconds	Use shorter interval for more precise system time. Specify longer interval to save data traffic.
5.	Save time to flash	Turn on saving time to flash memory after every time update	Prevents situation when devices is using wrong time after power failure. Use this if correct system time is critical for your application.
6.	Count of time measurements	Specify the number of time updates to perform	Use this to save data traffic
7.	Offset frequency	Specify frequency offset so fix system clock the is too fast or too slow	---
8.	Time servers	NTP server hostname and port	You can add as many servers as you need by clicking "Add" button.

Dynamic DNS

Dynamic DNS (DDNS) is a domain name service allowing to link dynamic IP addresses to static hostname.

To start using this feature firstly you should register to DDNS service provider.

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

	Field name	Description
1.	Enable	Enables current DDNS configuration.
2.	Status	Timestamp of the last IP check or update.
3.	Service	Your dynamic DNS service provider selected from the list: 1. dydns.org 2. 3322.org 3. no-ip.com 4. easydns.com 5. zoneedit.com In case your DDNS provider is not present from the ones provided, please feel free to use "custom" and add hostname of the update URL.
4.	Hostname	Domain name which will be linked with dynamic IP address.
5.	Username	Name of the user account.
6.	Password	Password of the user account.
7.	IP renew interval	Time interval (in minutes) to check if the IP address of the device have changed.
8.	Force IP renew	Time interval (in minutes) to force IP address renew.

Wireless 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 and so on…).

General Settings

Picture above illustrate a sample configuration of the general section.

	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. "192.168.182.254/24" 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 192.168.182.1 to 192.168.182.253).
3.	Radius server #1	The IP address of the RADIUS server that is to be used for Authenticating your wireless clients.
4.	Radius server #2	The IP address of the second RADIUS server.
5.	Authentication port	RADIUS server authentication port.
6.	Accounting port	RADIUS server accounting port.
7.	Hotspot name	The name of your hotspot. Will appear on the login screen.
8.	Secret Key	The secret key used for authenticating with the RADIUS server.
9.	Allowed hosts	A list of hosts that your clients will be able to reach regardless of whether they were authenticated or not.

Logging and FTP settings

The above picture illustrates a sample configuration of the Logging and FTP settings portion of the page.

	Field name	Explanation
1.	Logging enabled	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.	FTP enabled	Check this box if you want you logs to be periodically uploaded to an FTP server of your choice.
3.	Server address	The IP address of the FTP server to which you want the logs uploaded.
4.	Username	The username of the user on the aforementioned FTP server.
5.	Password	The password of the user.
6.	Port	The TCP/IP Port of the FTP server.
7.	Description	The description of the schedule.
8.	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.
9.	Weekdays	This field specifies on what weekdays the uploading should be done. The entry format is numbers from 1 to 7 separated by only commas. E.g. If you want to upload the logs on Monday, Wednesday and Saturday you should enter "1,3,6".
10.	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.
11.	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.

You can also one than more uploading schedule. Simply click Add at the very bottom of the configuration page and an additional configuration box will appear.

OpenVPN

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

OpenVPN

OpenVPN instances

Below is a list of configured OpenVPN instances and their current state

Tunnel Name	Tun/Tap	Protocol	Port	Status	
This section contains no values yet					

Role: Client ▼ New configuration name: [   ] [Add New]

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

Role: Client ▼ New configuration name: [Demo   ] [Add New]

A new configuration entry has appeared in the list and it is populated with default OpenVPN client settings.

Tunnel Name	Tun/Tap	Protocol	Port	Status	
client_Demo	-	-	1194	Disabled	[Edit] [Delete]

(You could select a server in previous step to create server default configuration).To see at specific configuration settings press **"edit"** button located in newly created configuration entry. A new page with detailed configuration appears, as shown in the picture below.

OpenVPN instance: 'client_Demo'

Main settings

Enable	☐
Tun/Tap	Tun(tunnel) ▼
	❓ Type of used device
Protocol	Udp ▼
Port	1194
	❓ TCP/UDP port for both, local and remote
LZO	☐ ❓ Use fast LZO compression
Authentication	Tls ▼
Remote host IP address	[ ]
Resolve Retry	infinite
No Bind	☐ ❓ Do not bind to local address and port
Keep alive	[ ]
	❓ Helper directive to simplify the expression of --ping and --ping-restart
Client	☐
Certificate authority	[ ] [Browse...]
Client certificate	[ ] [Browse...]
Client key	[ ] [Browse...]

[Save]

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

	Field name	Explanation
1.	Enabled	Switches configuration on and off. This must be selected to make configuration active.
2.	TUN/TAP	Selects virtual VPN interface type. TUN is most often used in typical IP-level VPN connections, however, TAP is required to some Ethernet bridging configurations.
3.	Protocol	Defines a transport protocol used by connection. You can choose here between TCP and UDP.
4.	Port	defines TCP or UDP port number (make sure, that this port allowed by firewall).
5.	LZO	This setting enables LZO compression. With LZO compression, your VPN connection will generate less network traffic; however, this means higher router CPU loads. Use it carefully with high rate traffic or low CPU resources.
6.	Authentication	Sets authentication mode, used to secure data sessions. Two possibilities you have here: "Static" means, that OpenVPN client and server will use the same secret key, which must be uploaded to the router using "Static pre-shared key" option. "Tls" authentication mode uses X.509 type certificates. Depending on your selected OpenVPN mode (client or server) you have to upload these certificates to the router: **For client:** Certificate Authority (CA), Client certificate, Client key. **For server:** Certificate Authority (CA), Server certificate, Server key and Diffie-Hellman (DH) certificate used to key exchange through unsafe data networks. All mention certificates can be generated using OpenVPN or OpenSSL utilities on any type host machine. Certificate generation and theory is out of scope of this user manual.
7.	Remote host IP address	IP address of OpenVPN server (applicable only for client configuration).
8.	Resolve Retry	Sets time in seconds to try to resolve server hostname periodically in case of first resolve failure before generating service exception.
9.	Keep alive	Defines two time intervals: one is used to periodically send ICMP request to OpenVPN server, and another one defines a time window, which is used to restart OpenVPN service, if no ICPM request is received during the window time slice.
10.	Local tunnel endpoint	IP address of virtual local network interface (applicable only for point to point connections).
11.	Remote tunnel endpoint	IP address of virtual remote network interface.
12.	Remote network IP address	IP address of remote virtual network.
13.	Remote network IP netmask	Subnet mask of remote virtual network.

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

IPsec

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

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

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

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

Automatic IPSec Key exchange

	Field name	Description
1.	Enable IPSec	Check box to enable IPSec.
2.	IPSec key exchange mode	Automatic Key exchange.
3.	Enable NAT traversal	Enable this function if client-to-client applications will be used.
4.	Enable initial contact	Enable this to send an INITIAL-CONTACT message.
5.	Peers identifier type	Choose "fqdn" or "user fqdn" accordingly to your IPSec server configuration.
6.	Mode	Select "Main" or "Aggressive" mode accordingly to your IPSec server configuration.
7.	My identifier	Set the device identifier for IPSec tunnel.
8.	Preshare key	Specify the authentication secret [string]. Secret's length depends on selected algorithm, eg. 128 bit long secret is 16 characters in length, 128 bits / 8 bits (one character) = 16.
9.	Remote VPN Endport	Set remote IPSec server IP address.

Phase 1 and **Phase 2** must be configured accordingly to the IPSec server configuration.

Remote Network Secure Group – Set the remote network (Secure Policy Database) information.


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

GRE Tunnel

GRE (Generic Routing Encapsulation RFC2784) is a solution for tunneling RFC1812 private address-space traffic over an intermediate TCP/IP network such as the Internet. GRE tunneling does not use encryption it simply encapsulates data and sends it over the WAN.
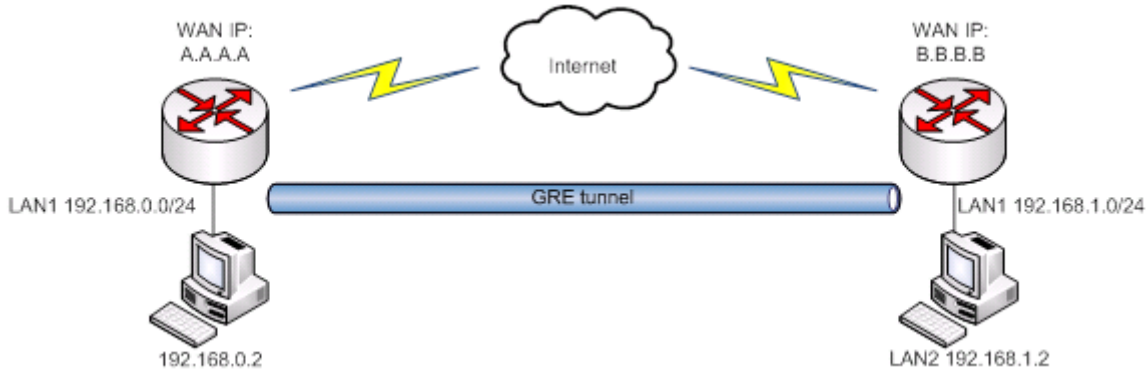
In the example network diagram two distant networks LAN1 and LAN2 are connected.

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

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

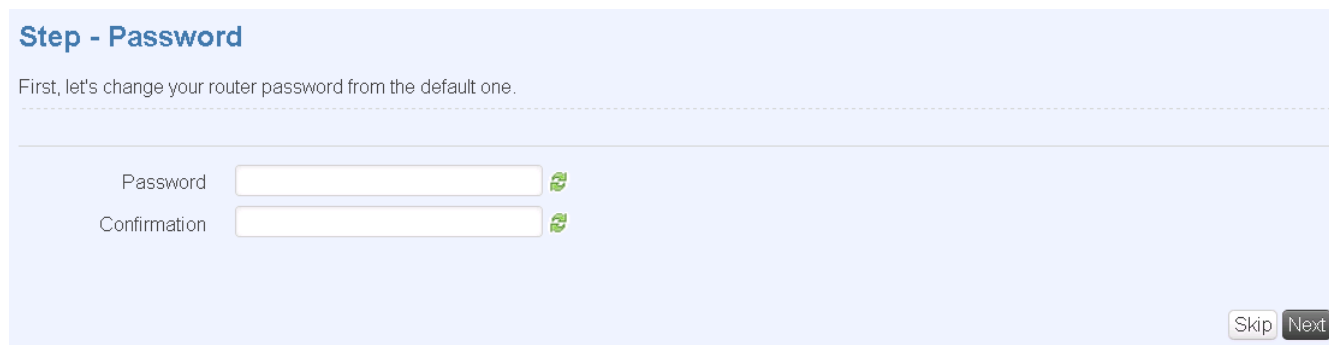|	Field name	Explanation
1.	Enable GRE Tunnel	Check the box to enable the GRE Tunnel function.
2.	TTL	Specify the fixed time-to-live (TTL) value on tunneled packets [0-255]. The 0 is a special value meaning that packets inherit the TTL value.
3.	PMTUD	Check the box to enable the Path Maximum Transmission Unit Discovery (PMTUD) status on this tunnel.
4.	Remote tunnel network address	Specify remote LAN Subnet address.
5.	Remote CIDR	Specify remote LAN Subnet CIDR value.
6.	Remote IP address	Specify remote WAN IP address.
7.	MTU	Specify the maximum transmission unit (MTU) of a communications protocol of a layer in bytes.

System

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:
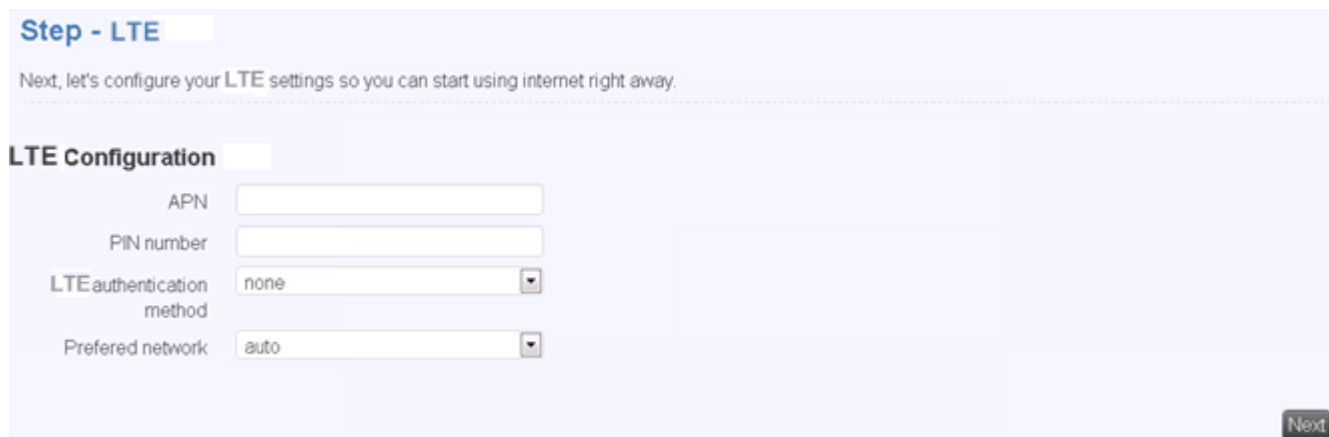
Step 1 (Password change)

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

Note: At this point you can also **Skip** the wizard.

Step 2 (LTE)

Next we have to enter your LTE configuration. On a detailed instruction on how this should be done see the LTE 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-F i)

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 **Finish**.

Administration

Administration properties

Administration password

	Field name	Explanation
	Field name	Explanation
1.	Password	Enter your new administration password.
2.	Confirmation	Re-enter your new administration password.

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**

Logging

	Field name	Explanation
1.	System log level	Select log level to be used for messages in system log (requires restart of the device)
2.	Save log in	Select whether system log is saved to ram or flash memory (requires restart of the device)
3.	Include GSMD information	Include GSMD information in the system log
4.	Include PPPD information	Include PPPD information in the system log (relevant only when pppd mode is selected in LTE configuration)
5.	Include Chat script information	Include Chat script information in the system log (relevant only when pppd mode is selected in LTE configuration)
6.	System log	View system log
7.	Kernel log	View kernel log

SSH Access control

	Field name	Explanation
	Field name	Explanation
1.	SSH Access	SSH can be enabled or disabled by choosing "Enable" or "Disable" from dropdown list.
2.	Port	Specify port for SSH access. Default port is 22.

3.	Remote SSH access	If check box is selected users can access the router via SSH from the outside (WAN). When check box is not selected users can access the router only from LAN.

Note: The router has 2 users: „admin" for webUI and „root" for SSH. When loging in via SSH use „root".

Web Access control

	Field name	Explanation
1.	HTTP Web server port	Specify a port number for routers web management via HTTP protocol. Default port is 80.
2.	Remote HTTP access	If check box is selected users can access the router via the HTTP WEB Interface from the outside (WAN). When check box is not selected users can access the router only from LAN.
3.	HTTPS server port	Specify a port number for routers web management via HTTPS protocol. Default port is 443.
4.	Remote HTTPS access	If check box is selected users can access the router via the HTTPS WEB Interface from the outside (WAN). When check box is not selected users can access the router only from LAN.

Backup and Firmware
Router firmware backup, upgrade and settings reset to their factory defaults.

Backup and reset configuration
Backup archive – download current router settings file to personal computer.
Reset to defaults – reset router settings to their default values.

Troubleshoot package
Logging information and configuration– download troubleshoot package to provide to device support team when facing a problem.

Restore configuration
Restore backup – upload and restore router settings file from personal computer.

Firmware upgrade
Keep settings – when 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.

Image – router firmware upgrade file.

Firmware upgrade – Verify

Compare firmware file checksum to ensure data integrity. If checksum is correct click "Proceed" button below. Wait until upgrade process completes.

Important notes:

- Leaving "Keep settings" check box unselected before upgrade process will change IP address of router to default value 192.168.1.1 and you may need to configure router again (please read chapter "Logging in" at page 9)

Warning: Do not ever remove router power supply and do not press reset button during upgrade process! This will totally damage your router and it won't be accessible. If you have any problems related to firmware upgrade you should always consult with local dealer.

Reboot
Reboot router by pressing button "Reboot".

Logout
Log out from router management WEB interface.

Glossary

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

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

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

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

DNS – Domain Name 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.