WiMAX camera

User Manual

Version 1.02

Suitable for:

MVC323, MVC325, MVC335, MVC338

1. Legal notice

Copyright © 2012 TELTONIKA Ltd. All rights reserved. Reproduction, transfer, distribution or storage of part or all of the contents in this document in any form without 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.

2. 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.

Device is powered by a low voltage +12V DC power adaptor.

3. Table of Contents

4. SAFETY INFORMATION

In this document you will be introduced on how to use a MVC300 camera 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 be supplied from a Limited Power Source (LPS) whose 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 damage 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 in 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 centre or the manufacturer. There are no exchangeable parts inside the device.

5. Introduction

Thank you for purchasing a Teltonika WiMAX Camera!

Teltonika WiMAX Camera encompasses a large number of environmental monitoring applications. WiMAX technology provides wide coverage in remote areas allowing transmitting high resolution video wirelessly.

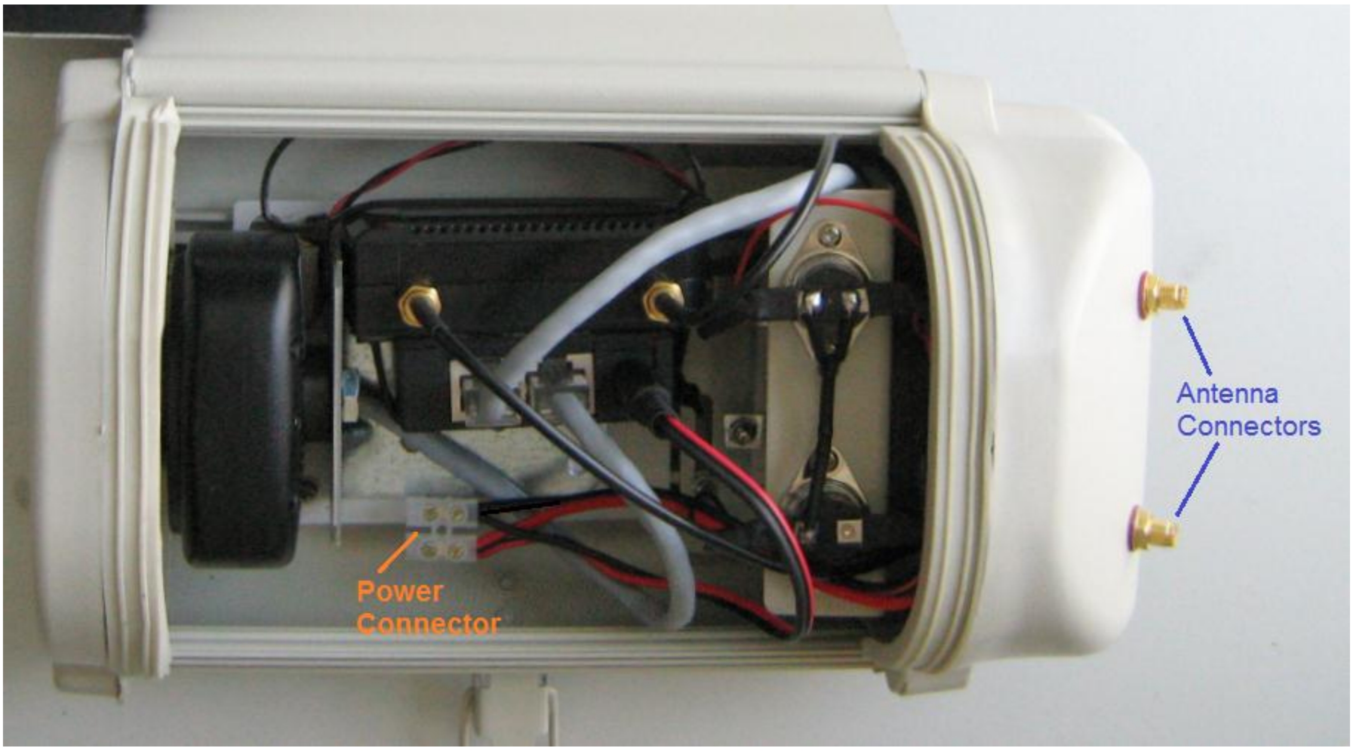
Simple installation and remote management allows user deploying the device easily. Wireless Teltonika camera saves installation time as no wired cable installation is required on the clients' premises. 'Live' video stream can be accessed from any location via Web Users Interface or through any video player. Camera has a huge amount of control settings and operational modes that can satisfy even the most demanding user's needs.

The camera also features DVR (Digital Video Recorder) function.

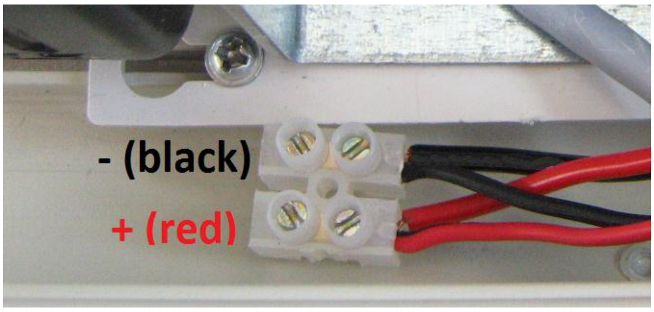
Teltonika WiMAX Camera provides wireless connectivity using WiMAX technology. It supports IEEE 802.16e standard, therefore it is flexible and can be used in a set of different environments.

6. Camera installation

The camera needs 12 VDC (11VDC to 14 VDC) power supply and antennas for operation:



Power consumption of the camera is less than 10 watts (see "Technical specifications"), so 12V, 1A power supply (12V x 1 A = 12 W) will be enough for the camera.
Connect "+" contact of the DC power supply to red wires, "-" contact to black wires :

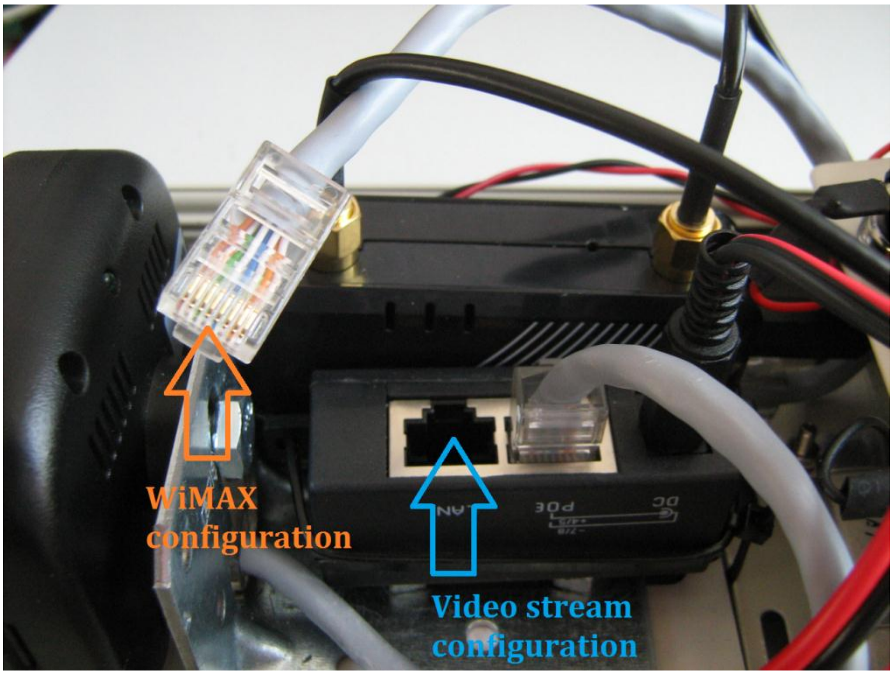


Attach the antennas to the camera.

7. Camera and PC setup for configuration

7.1. Camera connection for configuration

Open the camera's cover, connect the DC power supply as shown in "Camera installation" chapter.
Cable, connected to socket (port) named "LAN" can be connected to PC and used for WiMAX configuration.
If you connect "LAN" port with your PC via Ethernet cable, you will be able to reach camera's interface for its configuration.



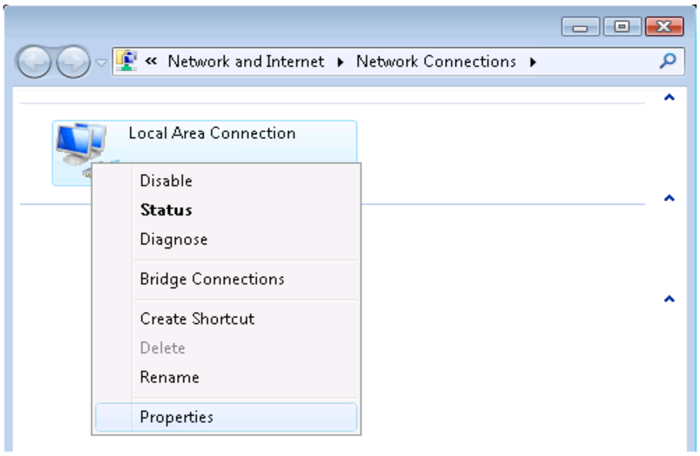
The video stream and WiMAX can be configured separately in this setup. You will need an Ethernet switch to configure the video stream and WiMAX simultaneously.

7.2. PC setup for configuration

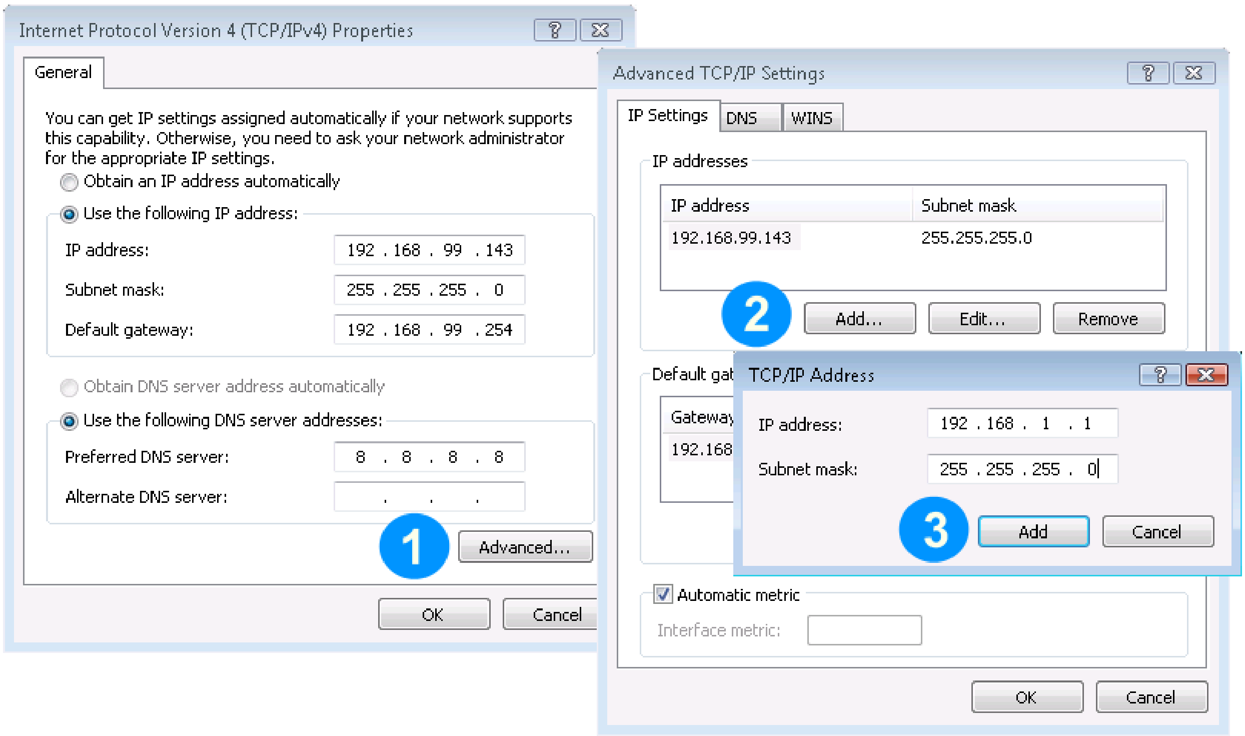
7.2.1. Network setup

The camera can be connected to your computer via an ethernet cable. IP address for camera configuration is **192.168.1.10** and IP address for WiMAX configuration is **192.168.0.1.** Your PC has to be in these subnets.

1. Go to **Start > Control Panel > Network and Internet > Network and Sharing Center**. In the left pane click **Manage network connections** link. Right click on **Local Area Connection** and select **Properties**.



2. Choose **Internet Protocol Version 4 (TCP/IP)** and click **Properties**.
3. Check if your PC's IP adress starts 192.168.1.x. If not, click **Advanced...** to bring up advanced setting. Click **Add...**, specify IP adress and Subnet mask (e.g. 192.168.1.1 and 255.255.255.0), click **Add** to save changes.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 99 . 143

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 99 . 254

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

Alternate DNS server: . . .

Advanced TCP/IP Settings

IP Settings | DNS | WINS

IP addresses

IP address	Subnet mask
192.168.99.143	255.255.255.0

Default gat

Gateway
192.168

☑ Automatic metric

Interface metric:

TCP/IP Address

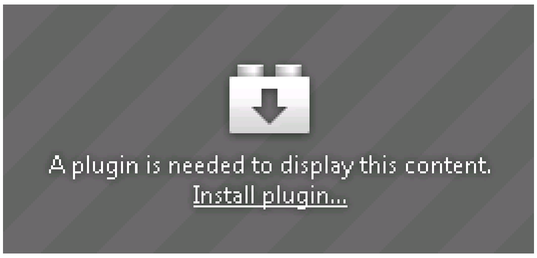
IP address: 192 . 168 . 1 . 1

Subnet mask: 255 . 255 . 255 . 0

4. Add IP address in the 192.168.0.xx subnet (e.g. 192.168.0.5 and and 255.255.255.0), click **Add.**
5. Click **OK** to apply new network settings.

7.2.2. Installing VLAN player

VLAN player is necessary in order to be able to see video in the **Live view** window. If the player's plugin is missing camera's WebUI won't show live video and may display a warning message:

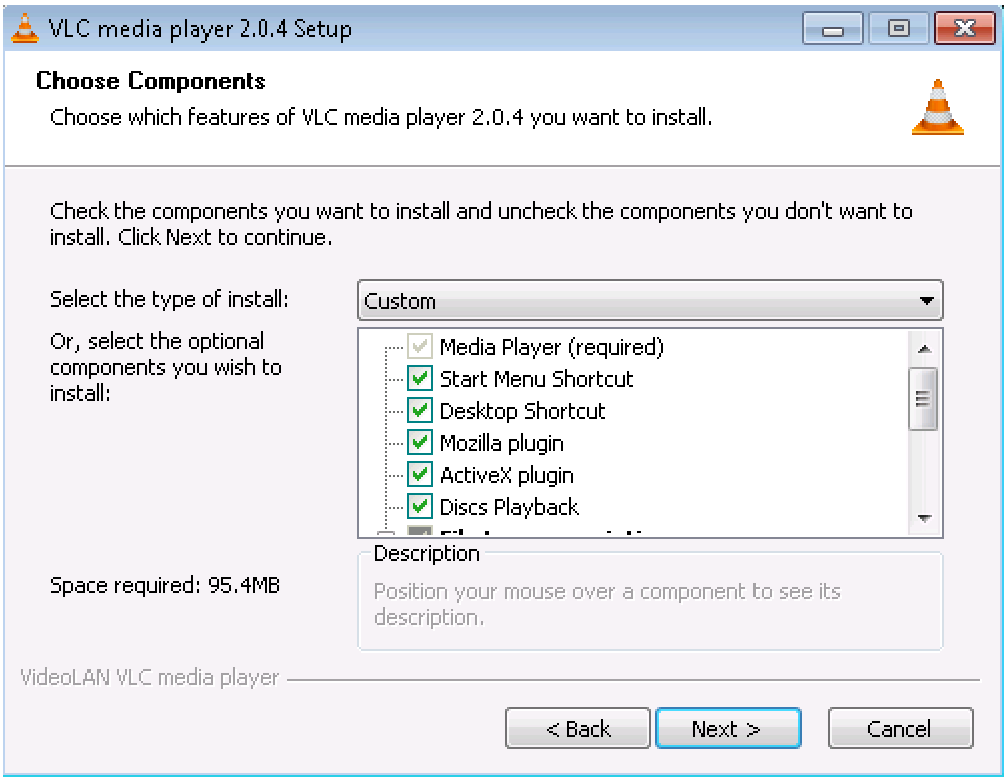


A plugin is needed to display this content.
Install plugin...

VLAN player installation steps:

1. Acquire VideoLAN player installer from www.videolan.org.
2. Launch downloaded installer.

3. Make sure both **Mozilla plugin** and **ActiveX plugin** are selected when choosing components. This will ensure that the plugin is installed on all browsers.



VLC media player 2.0.4 Setup

Choose Components

Choose which features of VLC media player 2.0.4 you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select the type of install: Custom

Or, select the optional components you wish to install:

- ☑ Media Player (required)
- ☑ Start Menu Shortcut
- ☑ Desktop Shortcut
- ☑ Mozilla plugin
- ☑ ActiveX plugin
- ☑ Discs Playback

Space required: 95.4MB

Description

Position your mouse over a component to see its description.

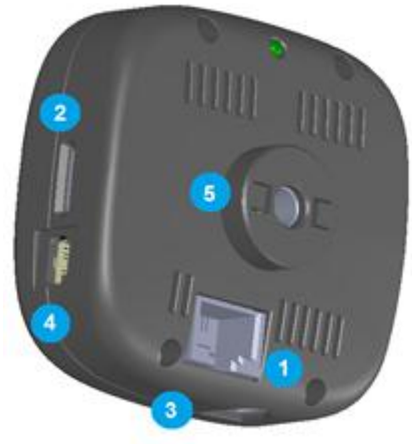
VideoLAN VLC media player

4. Complete VLAN player installation process.

8. Configuring the video streams

8.1. Camera connectors

IP camera is used to create H.264 video stream:

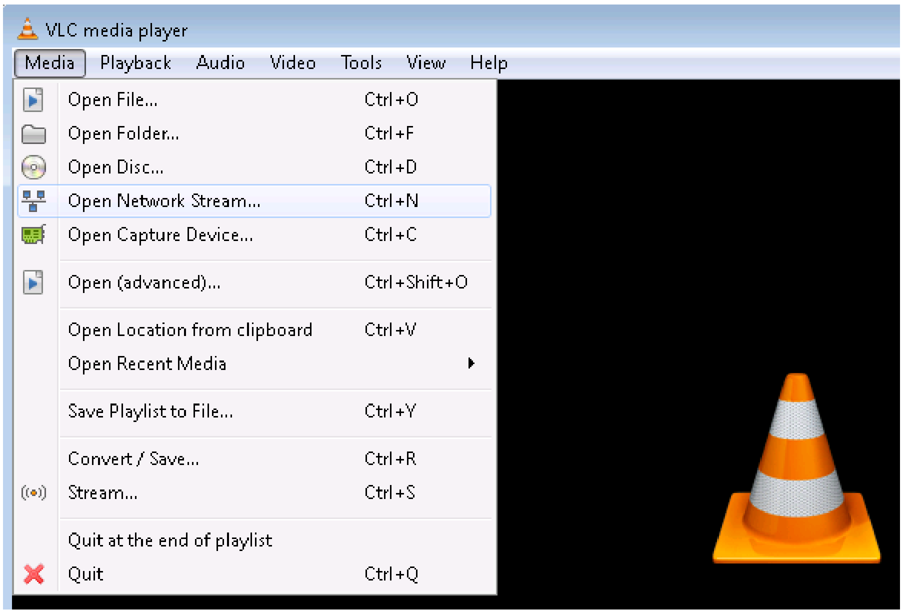


1	Ethernet connector
2	microSD card slot
3	DC power connector
4	USB connector
5	Mounting connector

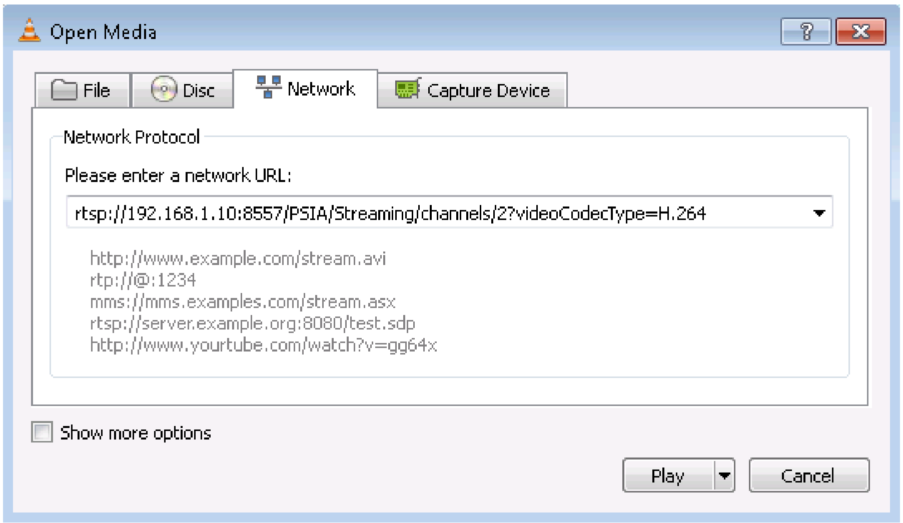
8.2. Using RTSP

Camera is capable of streaming video by RTSP protocol. After the camera is connected to the PC (or network) any RTSP capable media player can be used to see the video stream. To start an RTSP stream in VideoLAN player:

1. Go to **Media** and select **Open Network Stream** (alternatively Ctrl +N combination can be used).


VLC media player
Media
Playback
Audio
Video
Tools
View
Help
Open File... Ctrl+O
Open Folder... Ctrl+F
Open Disc... Ctrl+D
Open Network Stream... Ctrl+N
Open Capture Device... Ctrl+C
Open (advanced)... Ctrl+Shift+O
Open Location from clipboard Ctrl+V
Open Recent Media
Save Playlist to File... Ctrl+Y
Convert / Save... Ctrl+R
Stream... Ctrl+S
Quit at the end of playlist
Quit Ctrl+Q

2. Enter URL **rtsp://192.168.1.10:8557/PSIA/Streaming/channels/2?videoCodecType=H.264** and press **Play** to see stream video.



Network Protocol

Please enter a network URL:

rtsp://192.168.1.10:8557/PSIA/Streaming/channels/2?videoCodecType=H.264

http://www.example.com/stream.avi
rtp://@:1234
mms://mms.examples.com/stream.asx
rtsp://server.example.org:8080/test.sdp
http://www.yourtube.com/watch?v=gg64x

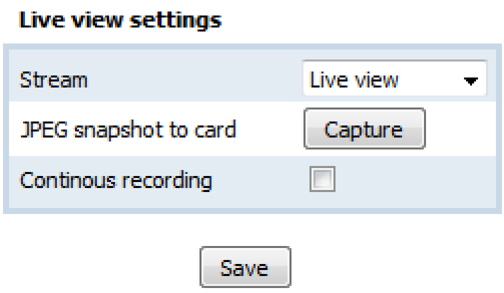
□ Show more options

9. User interface for video stream

Camera’s WebUI can be accessed when camera is connected to your PC. Type http://192.168.1.10 into your internet browser’s address field in order to reach the camera’s WebUI.

9.1. Live view

Live view tab displays video from the camera and is used to configure basic video settings.



Live view settings

Stream	Live view ▾
JPEG snapshot to card	Capture
Continous recording	□

Save

Stream Select stream to view in live view window. You can choose between Live view stream and Video storage stream. The streams can be specified in “Video settings” tab.

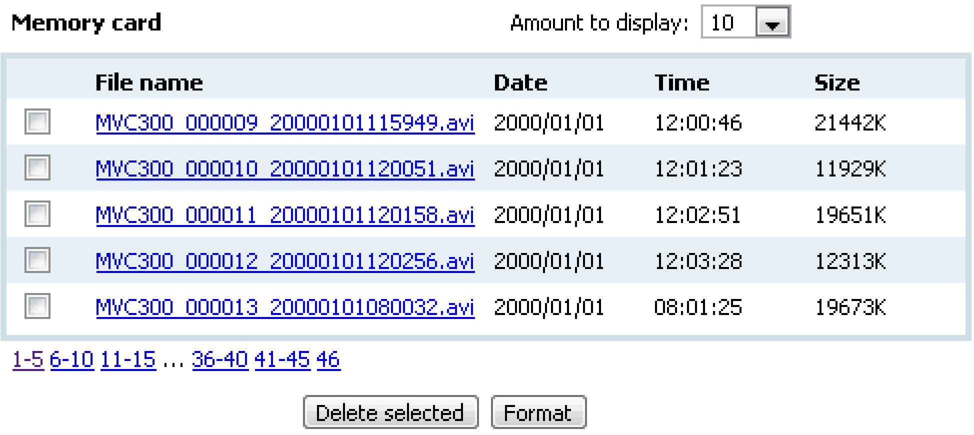
JPEG snapshot to card Press “Capture” button to record one snapshot to memory card.

Continous recording Check to continuously record to memory card.

Save Press **Save** to apply new settings.

9.2. Playback

In the **Playback** tab on the WebUI you can browse, download and delete recorded video files.



Memory card

Amount to display: 10

	File name	Date	Time	Size
□	MVC300_000009_20000101115949.avi	2000/01/01	12:00:46	21442K
□	MVC300_000010_20000101120051.avi	2000/01/01	12:01:23	11929K
□	MVC300_000011_20000101120158.avi	2000/01/01	12:02:51	19651K
□	MVC300_000012_20000101120256.avi	2000/01/01	12:03:28	12313K
□	MVC300_000013_20000101080032.avi	2000/01/01	08:01:25	19673K

1-5 6-10 11-15 ... 36-40 41-45 46

Format To be able to use memory card it should be formatted as FAT32. The card can be formatted when inserted in your PC or by pressing **Format** when inserted in the camera.

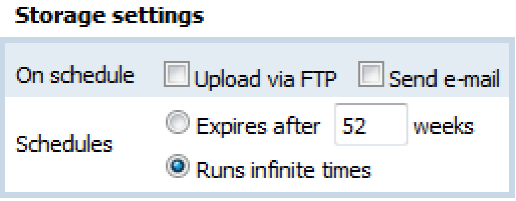
Amount to display Select number of files per page to display

Delete selected Press to permanently delete selected files from camera's SD card.

9.3. Alarm & schedules

Alarms & schedules tab provides possibility to configure recording schedules and alarm settings of the camera.

9.3.1. Schedule recording



Storage settings

On schedule	□ Upload via FTP □ Send e-mail
Schedules	○ Expires after 52 weeks ● Runs infinite times

On shedule

Upload via FTP Check to upload video via FTP on schedule.

Send e-mail Send e-mails on schedule.

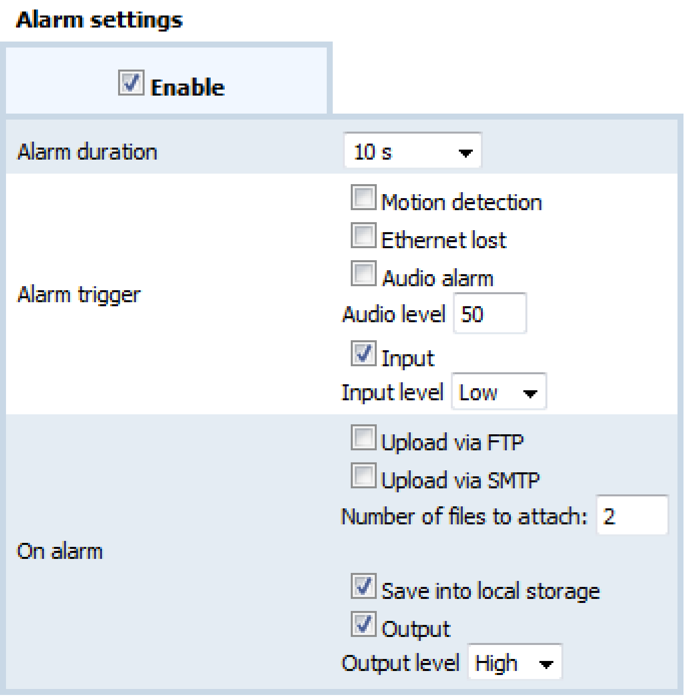
Schedules Set expiry limit to scheduler or let run it infinitely

Schedule time table Press to enable storage, and press once more to inhibit storage:

■ Storage enabled

□ Storage inhibited

9.3.2. Alarm settings



Alarm settings

☑ Enable

Alarm duration: 10 s

Alarm trigger:
□ Motion detection
□ Ethernet lost
□ Audio alarm
Audio level 50
☑ Input
Input level Low

On alarm:
□ Upload via FTP
□ Upload via SMTP
Number of files to attach: 2
☑ Save into local storage
☑ Output
Output level High

Alarm duration Specify recording to local storage on alarm/alarm output duration.

Alarm trigger

Motion detection Select to activate recording on motion detection.

Ethernet lost Select to activate alarm recording on Ethernet lost.

Audio alarm Select to trigger alarm recording/alarm when audio level exceeds a specified level.

Audio level Specify audio level of alarm triggering. Allowed range is from 0 to 100.

Input N/A to this camera.

Input level N/A to this camera.

On alarm

Upload via FTP Select to upload video clip via FTP.

Upload via SMTP Select to send specified number of snapshots via SMTP (e-mail).

Number of files to attach Specify number of snapshots attached to e-mail.

Save into local storage Select to save alarm recording into local microSD card.

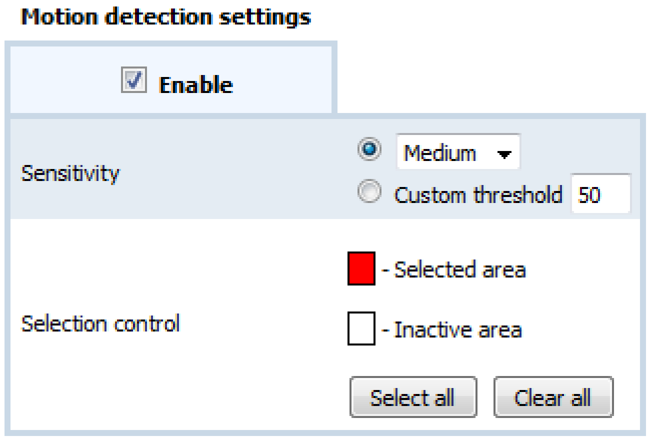
Output N/A to this camera.

Output level N/A to this camera.

Save Press **Save** to apply new settings.

9.4. Motion

Motion tab allows configuration of **Motion detection settings.**



Motion detection settings

☑ **Enable**

Sensitivity	● Medium ▾ ○ Custom threshold 50
Selection control	🟥 - Selected area □ - Inactive area Select all · Clear all

Sensivity Specify motion detection sensitivity. Possible options are:

Low	1280 x 720
Medium	720 x 480
High	1280 x 960

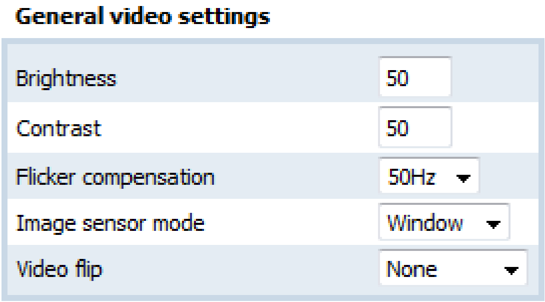
Custom threshold Specify custom motion detection sensitivity. Allowed range is from 0 to 100

Selection control Press area on the video to select it. Press once more to deselect it.

9.5. Video settings

Video settings tab allows configurations of **Video settings** and **Stream settings**.

9.5.1. Video settings



General video settings

Brightness	50
Contrast	50
Flicker compensation	50Hz ▾
Image sensor mode	Window ▾
Video flip	None ▾

Brightness Specify brightness of the video. Allowed range is from 0 to 100.

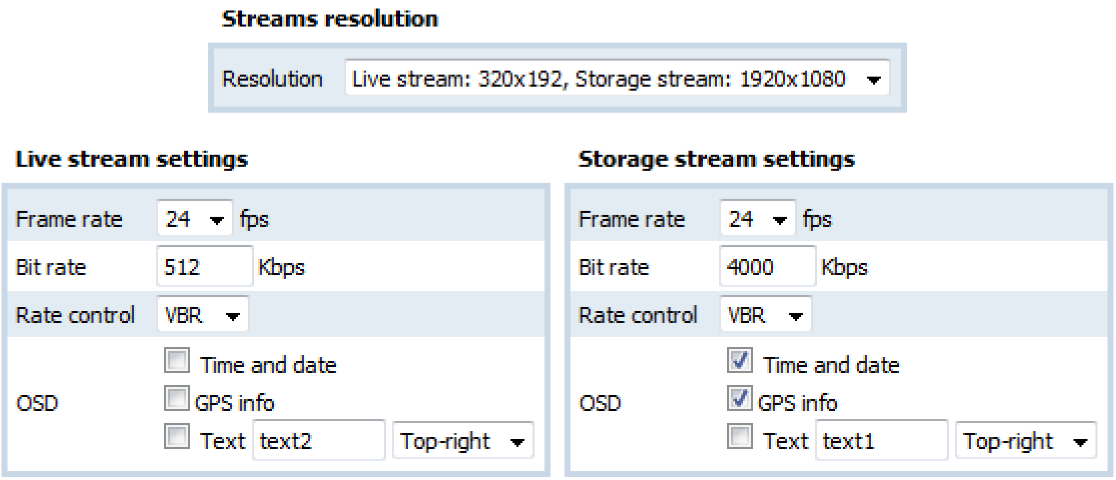
Contrast Specify contrast of the video. Allowed range is from 0 to 100.

Flicker compensation When using the camera indoors, select correct flicker frequency to get a clean video.

Image sensor mode Select image sensor mode.

Video flip You can flip image vertically, horizontally or in both directions

9.5.2. Streams settings



Streams resolution

Resolution: Live stream: 320x192, Storage stream: 1920x1080

Live stream settings

Frame rate	24 fps
Bit rate	512 Kbps
Rate control	VBR
OSD	□ Time and date □ GPS info □ Text text2 Top-right

Storage stream settings

Frame rate	24 fps
Bit rate	4000 Kbps
Rate control	VBR
OSD	☑ Time and date ☑ GPS info □ Text text1 Top-right

Stream resolution Increased resolution results in better video quality while decreasing it allows for a smaller recorded file size.

Frame rate Specify frame rate.

Bit rate Increased bit rate results in better video quality while decreasing it allows for a smaller recorded file size.

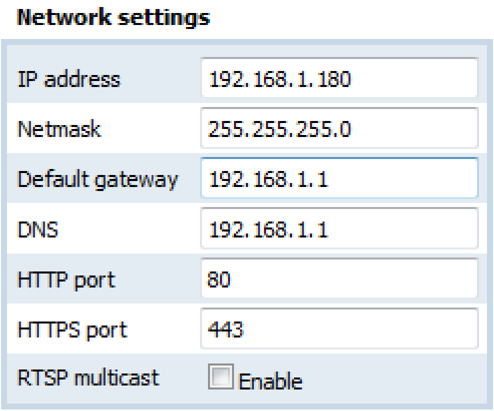
Rate control Rate control mode can to be constant (CBR), variable (VBR) or can be turned off.

OSD Specify additional text to be displayed in the video and select its position.

9.6. Network

Network tab provides possibility to configure **Network, Mail & FTP** and **Firewall s**ettings.

9.6.1. Network



Network settings

IP address	192.168.1.180
Netmask	255.255.255.0
Default gateway	192.168.1.1
DNS	192.168.1.1
HTTP port	80
HTTPS port	443
RTSP multicast	□ Enable

IP address Specify camera's IP address.

Netmask Specify netmask.

Default gateway Specify default gateway.

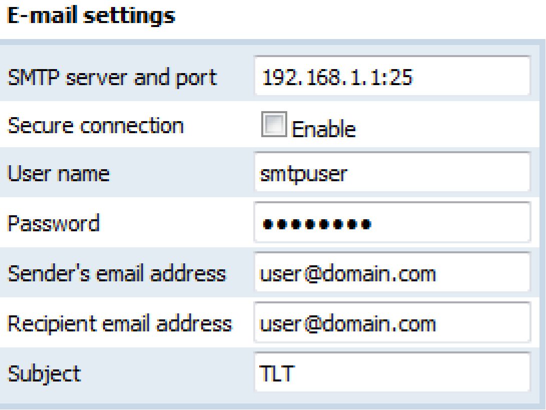
DNS Specify DNS.

HTTP port Specify HTTP port of the camera.

HTTPS Specify HTTPS port of the camera.

RTSP multicast Check to enable RTSP multicast.

9.6.2. Mail & FTP



E-mail settings

SMTP server and port	192.168.1.1:25
Secure connection	□ Enable
User name	smtpuser
Password	●●●●●●●●
Sender's email address	user@domain.com
Recipient email address	user@domain.com
Subject	TLT

SMTP server and port Specify SMTP server and port.

Secure connection Check to enable secure (SSL) connection.

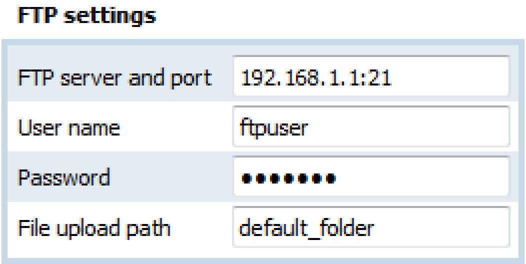
User name Type user name of email account.

Password Type password to be used when authorizing.

Sender’s email address Specify sender’s email address.

Recipient email address Specify recipients.

Subject Press to synchronize camera’s date and time with your computer.



FTP settings

FTP server and port	192.168.1.1:21
User name	ftpuser
Password	●●●●●●●
File upload path	default_folder

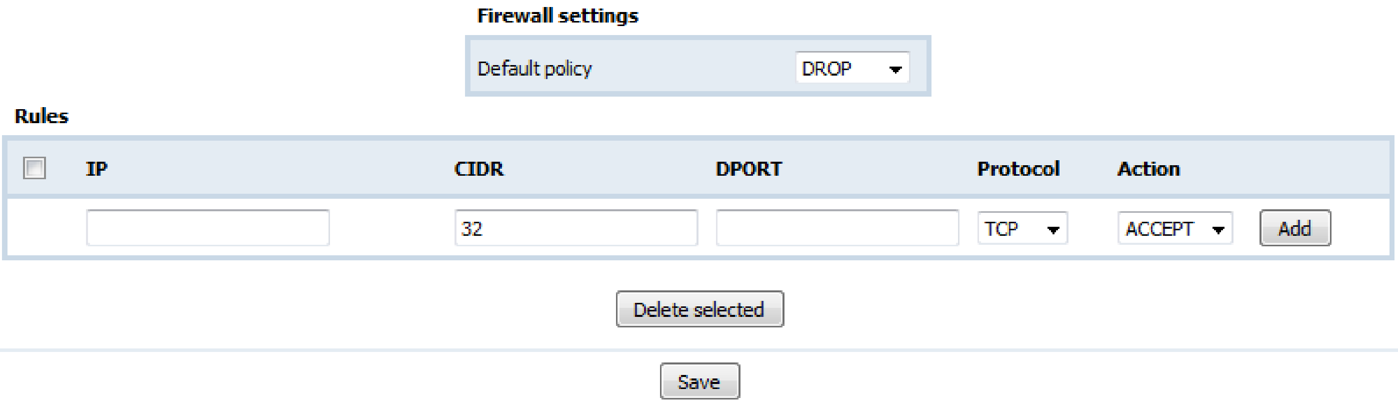
FTP server and port Specify FTP server and port.

User name Type user name on FTP server.

Password Type password to be used when authorizing.

File upload path Specify file upload path.

9.6.3. Firewall



Firewall settings

Default policy: DROP

Rules

☐	IP	CIDR	DPORT	Protocol	Action	
		32		TCP	ACCEPT	Add

Default Policy The default state of the firewall.

IP The IP address of incoming connection

CIDR The CIDR number

DPORT The incoming port of the connection

Entry format:

- Leave blank if you don't wish to specify the a port number
- Single port: enter one number within range 1 to 65535, e.g. 2345
- Port range: enter two port number separated by a clash, e.g. 2435-4562

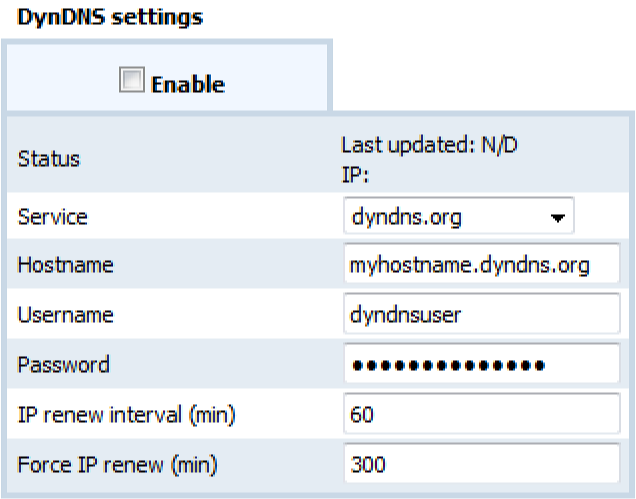
Protocol The protocol of the connection

Action What action will be taken on the connection.

9.7. Services

Services tab provides possibility to configure **dynamic DNS, and OpenVPN** settings.

9.7.1. DynDNS



DynDNS settings

☐ Enable

Status	Last updated: N/D IP:
Service	dyndns.org
Hostname	myhostname.dyndns.org
Username	dyndnsuser
Password	••••••••••••••
IP renew interval (min)	60
Force IP renew (min)	300

Status

Last updated The last time when a dynamic DNS domain was updated with a new IP.

IP: The IP address that will be resolved from the hostname.

Service Select dynamic DNS service.

Hostname The URL name that can be used to access the camera

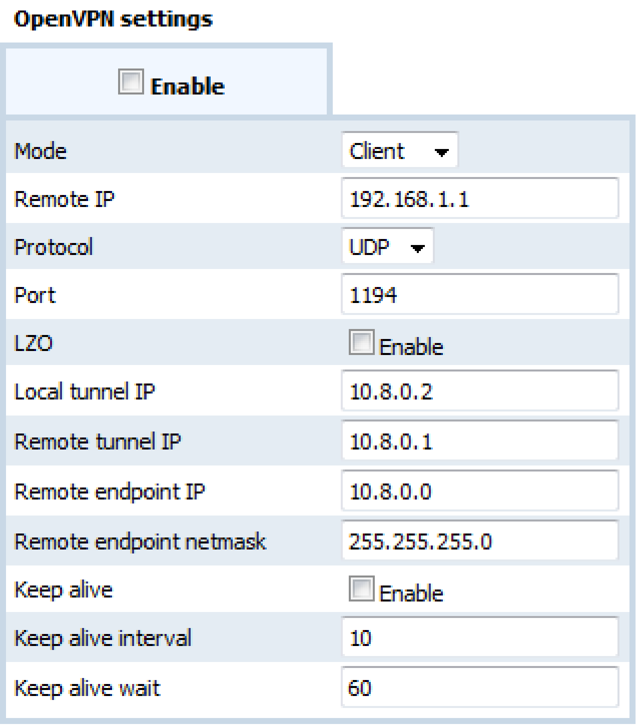
Username Type dynamic DNS service user’s name.

Password Type password to be used when authorizing.

IP renew interval (min) Specify IP renew interval in minutes.

Force IP renew (min) Specify forced IP renew interval in minutes.

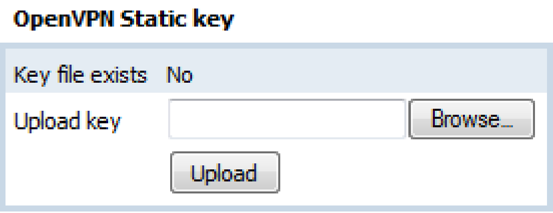
9.7.2. OpenVPN



OpenVPN settings

□ Enable

Mode	Client
Remote IP	192.168.1.1
Protocol	UDP
Port	1194
LZO	□ Enable
Local tunnel IP	10.8.0.2
Remote tunnel IP	10.8.0.1
Remote endpoint IP	10.8.0.0
Remote endpoint netmask	255.255.255.0
Keep alive	□ Enable
Keep alive interval	10
Keep alive wait	60



OpenVPN Static key

Key file exists	No
Upload key	

Mode Select VPN mode (Client / Server)

Remote IP IP address of OpenVPN server (applicable only for client configuration)

Protocol Defines a transport protocol used by connection. You can choose here between TCP and UDP.

Port Defines TCP or UDP port number (make sure, that this port allowed by firewall).

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.

Local tunel IP IP address of virtual local network interface.

Remote tunel IP IP address of virtual remote network interface.

Remote endpoint IP IP address of remote virtual network.

Remote endpoint netmask Subnet mask of remote virtual network.

Keep alive Check to enable.

Keep alive interval Specifies the interval the client waits before sending a keep-alive request.

Keep alive wait Specifies the interval the client waits for a keep-alive response.

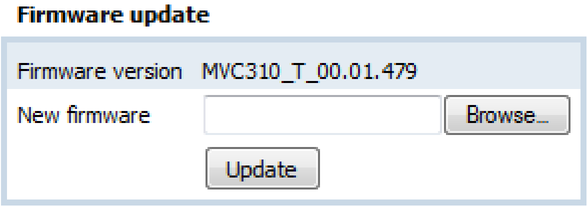
Key file exists Key file name if uploaded otherwise No.

Upload key Browse, then upload key file.

9.8. Maintenance

Maintenance tab provides possibility to configure such settings as update device’s firmware, camera’s name, time, and authorization.

9.8.1. Firmware



Firmware update

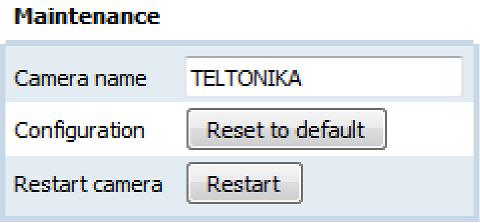
Firmware version	MVC310_T_00.01.479	
New firmware		Browse...
	Update	

Firmware version Displays current camera‘s firmware version

Browse Press **Browse** and select new firmware file.

Update To upgrade camera‘s firmware press **Update** buton.

9.8.2. Maintenance and time settings



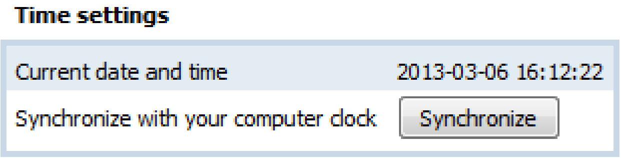
Maintenance

Camera name	TELTONIKA
Configuration	Reset to default
Restart camera	Restart

Camera name Specify the name of the camera. Name will be used in the file name of the recorded videos.

Reset to defaults Press to reset camera’s configuration to default values.

Restart Press to restart the camera.



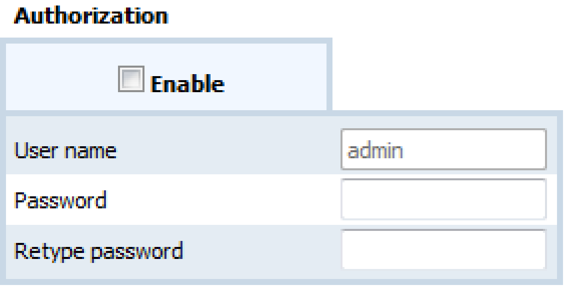
Time settings

Current date and time	2013-03-06 16:12:22
Synchronize with your computer clock	Synchronize

Current date and time Displays current camera’s date and time.

Synchronize Press to synchronize camera’s date and time with your computer.

9.8.3. User authorisation



Authorization

□ Enable

User name	admin
Password	
Retype password	

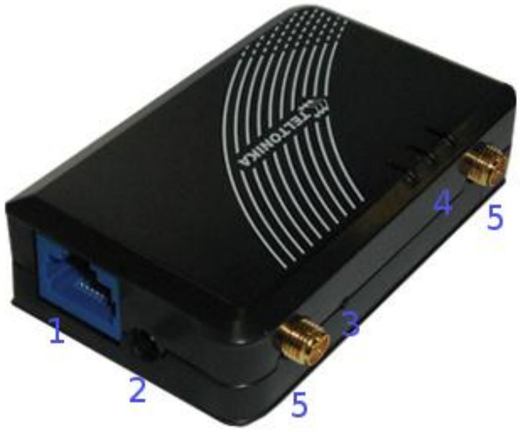
Authorization Check **Enable** if you want to use authorization when accessing camera’s WebUI.

Password Type password to be used when authorizing. Username is always **admin**.

Retype password Confirm previously typed password.

10. WiMAX hardware, LED's and connections

RUT4xx device is used for tranmitting data through WiMAX network:



1. Ethernet port.
2. Power connection.
3. Reset (Reset to factory defaults – optional).
4. Indication LED (from left to right)
    - Activity.
    - Power plugged in.
    - LAN cable plugged-in.
5. Antenna connectors.

11. WiMAX WebUI OVERVIEW

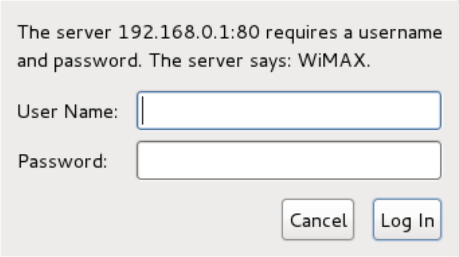
In this section you will be briefly introduced to our user interface.

Note: we use an intuitive tool tip system in our web user interface which displays additional data for the user. To see this data hover your mouse cursor above the field. Also, if the frame of the field becomes red, it usually means that the data in the field is incorrect, in this case look into red tool tip for more information.

11.1. Connecting to the WebUI

To connect to the configuration web page do the following steps:

1. Type **192.168.0.1** to your favorite internet browser. Skip the step 2 if the password is disabled.
2. Window asking for authentication will pop up. Enter your username and password (default: username: user, password: user) and press enter.

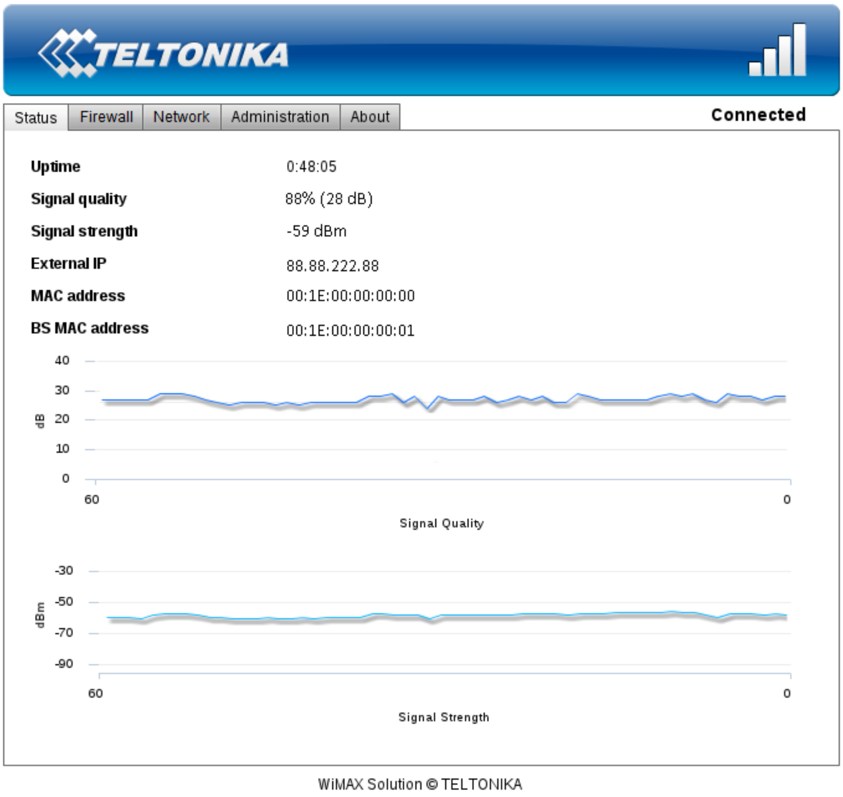


The server 192.168.0.1:80 requires a username and password. The server says: WiMAX.

User Name:

Password:

3. Status window will appear in a few seconds:



Uptime 0:48:05

Signal quality 88% (28 dB)

Signal strength -59 dBm

External IP 88.88.222.88

MAC address 00:1E:00:00:00:00

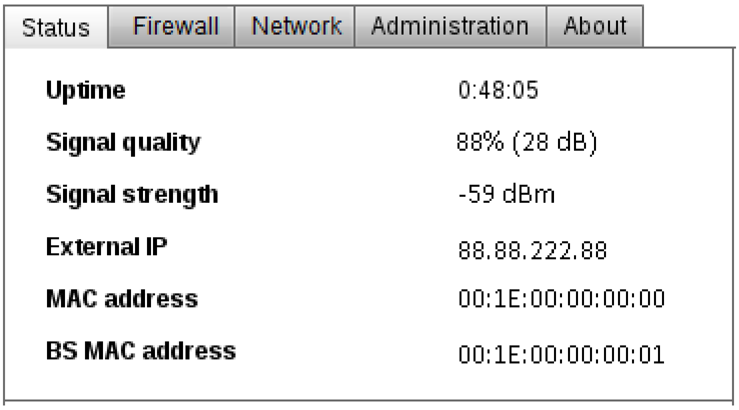
BS MAC address 00:1E:00:00:00:01

First page of WebUI

11.2. WebUI structure

Our modern web user interface provides you with all the tools needed within the five main pages: **Status**, **Network**, **Firewall**, **Administration**, **About**.

11.3. Status



Uptime	0:48:05
Signal quality	88% (28 dB)
Signal strength	-59 dBm
External IP	88.88.222.88
MAC address	00:1E:00:00:00:00
BS MAC address	00:1E:00:00:00:01

Status page

The status page consists of 6 properties that define the current state of the router:

1. **Uptime** – amount of time since the last reboot (or plug in).
2. **Signal quality** – the quality of a signal in percents (and decibels).

   <30% poor

   >30% <50% decent

   >50% <90% good

   >90% very good

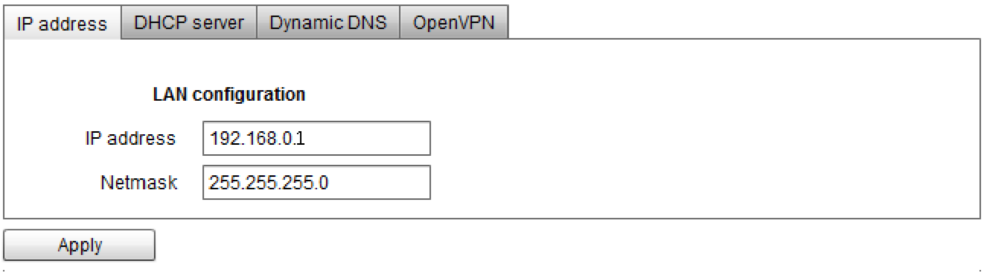
   Note: signal quality depends on the distance between the device and the base station, plus other factors: interference with other devices, etc.

3. **Signal strength** – the strength of the signal in dBm.
4. **External IP** – IP which was assigned by the base station to your device.
5. **MAC address** – physical address of the WiMAX connection module.
6. **BS MAC address** - physical address of the base station.

11.4. Network

Network settings page allows the user to change the IP address, net mask and DHCP server settings.

11.4.1. IP address



LAN configuration

IP address	192.168.0.1
Netmask	255.255.255.0

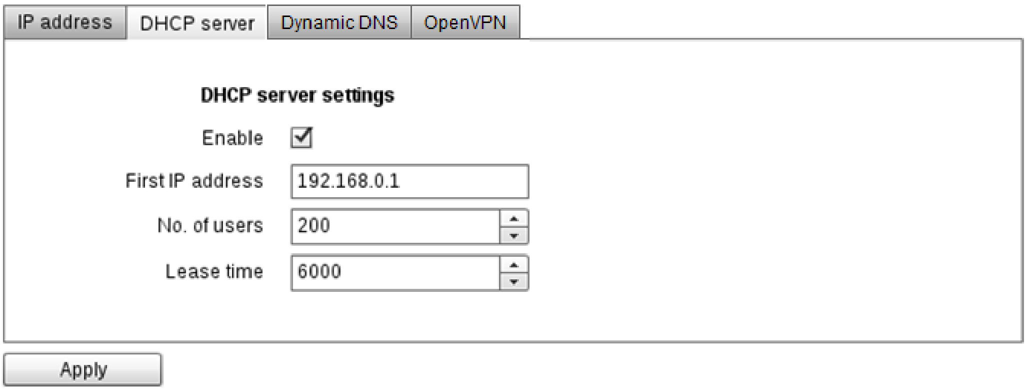
IP address settings page

IP address – IP address of the router.

Netmask – mask used to divide IP address into subnets.

11.4.2. DHCP server

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers configured for a given network.



DHCP server settings

Enable	☑
First IP address	192.168.0.1
No. of users	200
Lease time	6000

DHCP server form

Enable – check to enable the DHCP server.

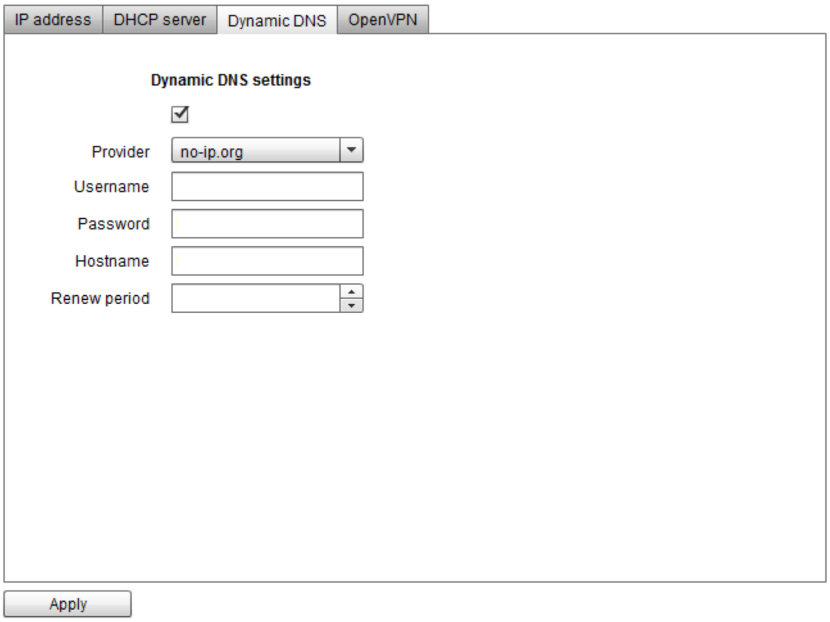
First IP address – First IP from the range to be leased.

No. of users – number of IP addresses to be leased.

Lease time – time after the leased IP expires.

11.4.3. Dynamic DNS

Dynamic DNS (DDNS) is a domain name service allowing to link dynamic IP addresses to static hostname. To start using this feature firstly you should register to DDNS service provider.



Dynamic DNS settings

☑

Provider: no-ip.org

Username:

Password:

Hostname:

Renew period:

DDNS form

Provider – your dynamic DNS service provider selected from the list.

Username – name of the user account.

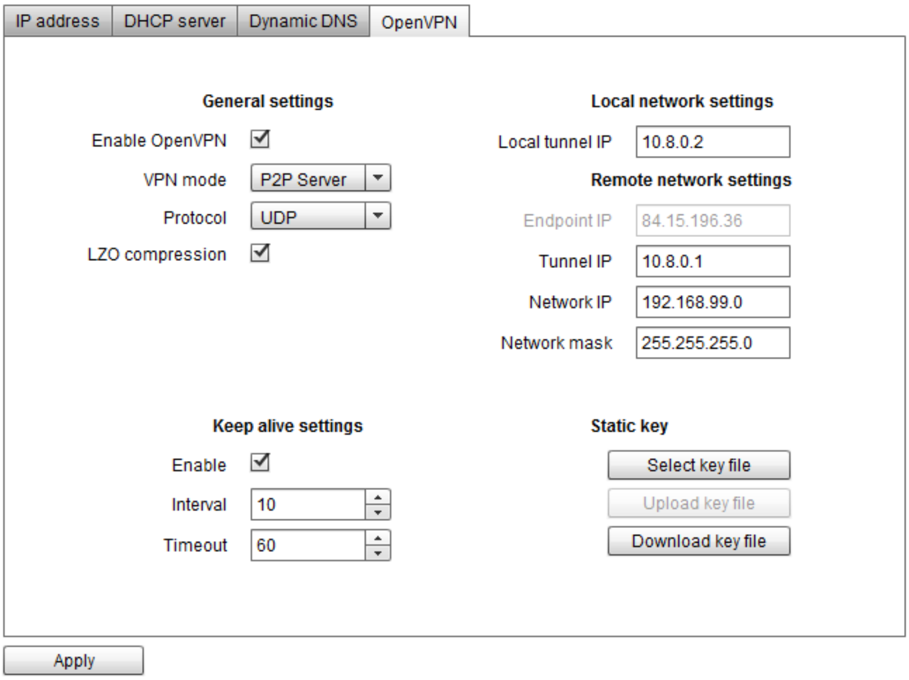
Password – password of the user account.

Hostname – domain name that you will be able to use instead of your IP address.

Renew period – time interval to check if IP address of the device have changed.

11.4.4. OpenVPN

VPN (virtual private network) is a secure network that provides remote offices or traveling users an access to a central organizational network.



General settings

Enable OpenVPN ☑

VPN mode: P2P Server

Protocol: UDP

LZO compression ☑

Local network settings

Local tunnel IP: 10.8.0.2

Remote network settings

Endpoint IP: 84.15.196.36

Tunnel IP: 10.8.0.1

Network IP: 192.168.99.0

Network mask: 255.255.255.0

Keep alive settings

Enable ☑

Interval: 10

Timeout: 60

Static key

OpenVPN form

General:

Enable OpenVPN – enables VPN functionality.

VPN mode – changes VPN mode **Client**/**Server.**

Protocol – use **TCP** or **UDP** for transmitting packets.

LZO compression – check the box to enable fast adaptive LZO compression.

Network:

Local tunnel IP – specifies the IP address of the local VPN tunnel endpoint.

Endpoint IP – specifies server IP address.

Tunnel IP – specifies the IP address of the remote VPN tunnel endpoint.

Network IP – specifies the remote network IP.

Network mask – specifies the remote network subnet mask.

Keep alive:

Enable – turns on “Keep alive” feature.

Interval – specifies time interval to check if VPN connection is still alive.

Timeout – specifies time span for the network to respond.

11.5. Firewall

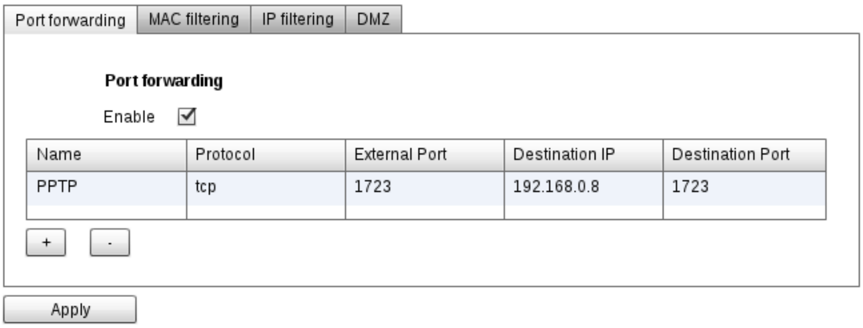
Firewall page lets you configure firewall settings to meet your requirements. It includes port-forwarding, MAC filtering and IP filtering

11.5.1. Port forwarding

Port forwarding is the process of translating the address and port number of a packet to a new destination.

Follow these steps to add a port-forwarding rule:

1. **Enable** – check to enable the Port forwarding.
2. Press the **+** button.



Port forwarding

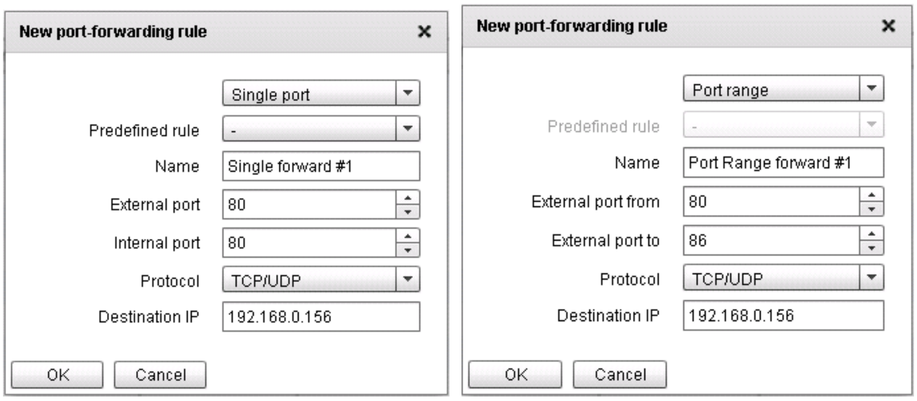
Enable ☑

Name	Protocol	External Port	Destination IP	Destination Port
PPTP	tcp	1723	192.168.0.8	1723

Port forwarding form

The following port-forwarding rule creation window will pop-up. Choose a rule type (single port or port range) and fill the fields in a window to define your rule:

- **Predefined rule** – select from a list of most common rules.
- **Name** – the name of the rule that will be visible in the list of your defined rules.
- **External port from/to** – external port range to be redirected to an identical internal port range.
- **External port** – external port to be redirected to **Internal port.**
- **Internal port** – port used by the destination device to receive data.
- **Protocol** – protocol in which rule operates.
- **Destination IP** – the address of the device to which all the data coming to the selected external ports is forwarded to.



	Single port
Predefined rule	-
Name	Single forward #1
External port	80
Internal port	80
Protocol	TCP/UDP
Destination IP	192.168.0.156

	Port range
Predefined rule	-
Name	Port Range forward #1
External port from	80
External port to	86
Protocol	TCP/UDP
Destination IP	192.168.0.156

New port-forwarding rule windows

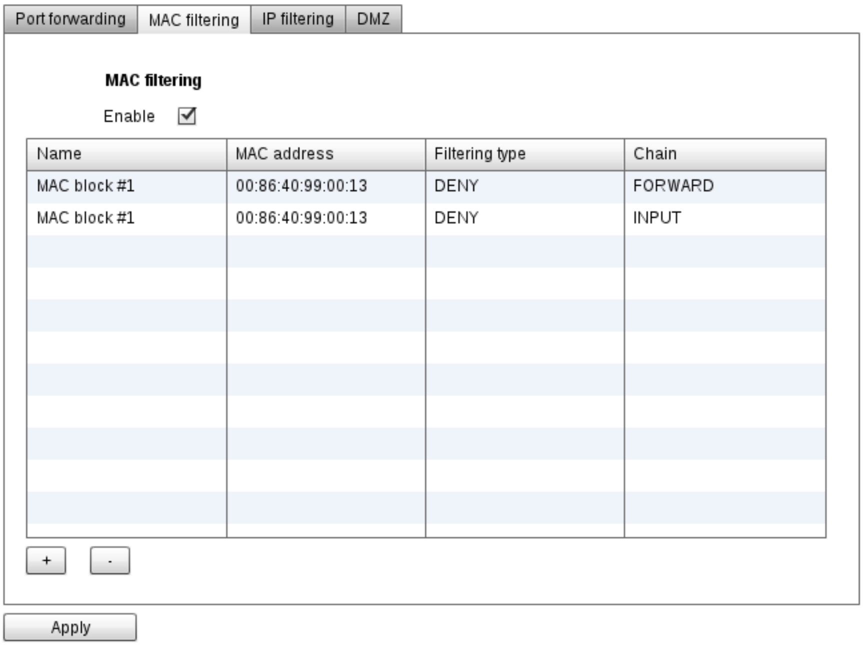
3. Press **OK** button to accept the rule.
4. Press **Apply** to save the rules to the configuration.

11.5.2. Mac filtering

MAC filtering is a security access control method used to determine access to the network by physical address.

Follow these steps to add a MAC filtering rule:

1. **Enable** – check to enable the MAC filtering.
2. Press the **+** button.



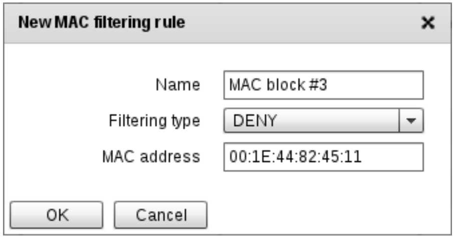
MAC filtering

Enable ☑

Name	MAC address	Filtering type	Chain
MAC block #1	00:86:40:99:00:13	DENY	FORWARD
MAC block #1	00:86:40:99:00:13	DENY	INPUT

Mac filtering form

3. The following MAC filtering rule creation window will pop-up.



New MAC filtering rule

Name	MAC block #3
Filtering type	DENY
MAC address	00:1E:44:82:45:11

New MAC filtering rule window

- **Name** – MAC filtering rule name.
- **MAC address** – physical address that you want to block from connecting to and/or through the router.

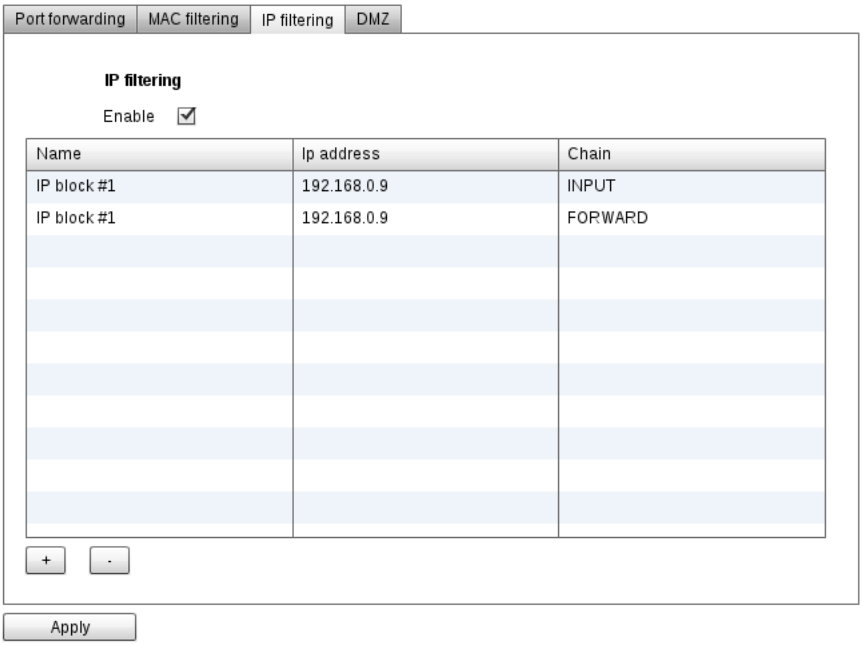
4. Press **OK** to add the rule.
5. After adding all the rules that you needed, press **Apply** to save the rules to the configuration.

11.5.3. IP filtering

IP filtering is a security access control method used to determine access to the network by IP address.

Follow these steps to add an IP filtering rule:

1. **Enable** – check to enable the IP filtering.
2. Press the **+** button.



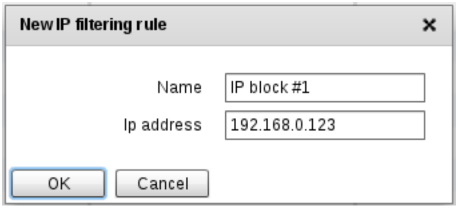
IP filtering

Enable ☑

Name	Ip address	Chain
IP block #1	192.168.0.9	INPUT
IP block #1	192.168.0.9	FORWARD

IP filtering form

3. The following IP filtering rule creation window will pop-up.



New IP filtering rule

Name: IP block #1

Ip address: 192.168.0.123

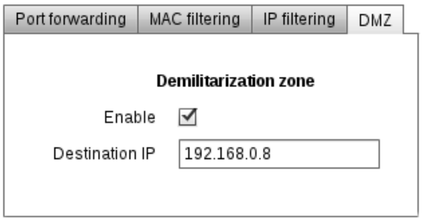
New IP filtering rule window

- **Name** – IP filtering rule name.
- **IP address** – remote IP address that you want to block from connecting to and/or through the router.

4. Press **OK** to add the rule.
5. After adding all the rules that you needed, press **Apply** to save the rules to the configuration.

11.5.4. DMZ

In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a private network and the outside public network.



Demilitarization zone

Enable ☑

Destination IP: 192.168.0.8

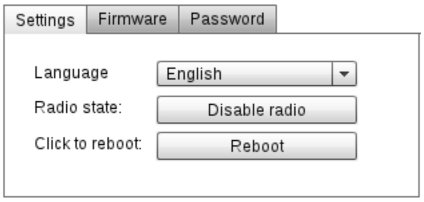
DMZ page

To set up DMZ, click the **Enable** checkbox and put in IP address of your destination in the **Destination IP** text field.

11.6. Administration

Administration page allows you to change the language of the WebUI, disable radio connection, reboot the router, save firmware to your computer (in a binary file format) or update it with the newer version. In addition, you can set up a new password for WebUI connection.

11.6.1. Settings



Language: English

Radio state: Disable radio

Click to reboot: Reboot

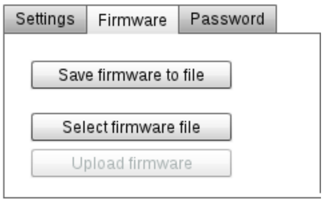
Settings page

Language – select a language from the drop down list.

Radio state – disables or enables radio (WiMAX) connection.

Reboot button – click to reboot this device. You will have to wait for a few seconds until it boots up again.

11.6.2. Firmware



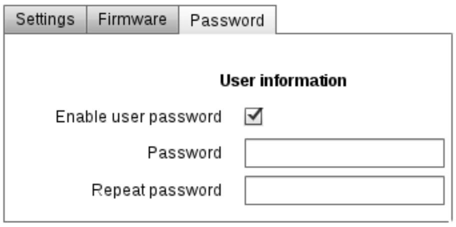
Firmware page

To save firmware: click **Save firmware to file** and at the following dialog browse to the directory you want to place binary file.

To update firmware: click **Select firmware file** and at the following dialog window select firmware file (note: file must be named firmware.bin). To start updating click: **Update firmware**. This process usually takes 5 to 10 minutes.

Note: A firmware backup is only suitable for the device from which it was downloaded. If a firmware backup is uploaded to another router, that device will malfunction.

11.6.3. Password



User information

Enable user password ☑

Password

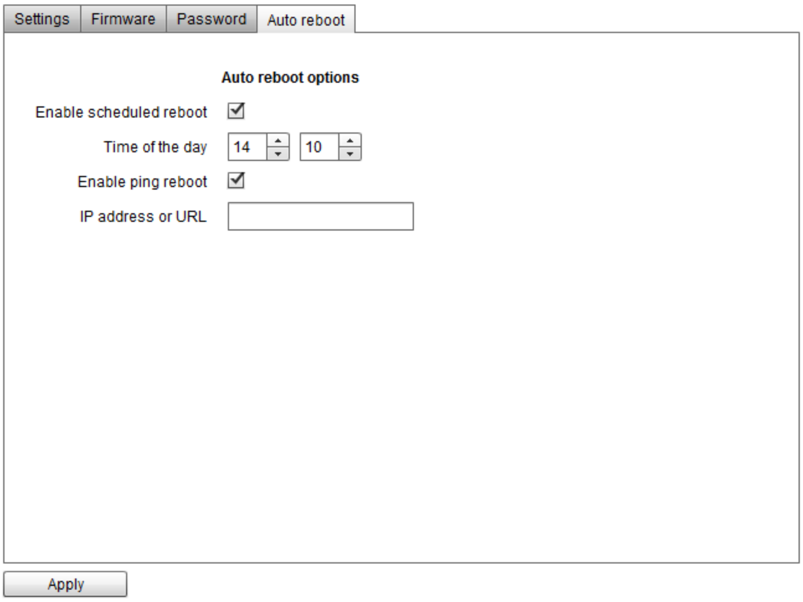
Repeat password

To set up or change a password check **Enable user password** and write a new one into two fields bellow. To disable user password simply uncheck **Enable user password** checkbox. You must click **Apply** if you want to save any of these to configuration.

Note: it is strongly not recommended to disable user password if a router is reachable from Local area network.

11.6.4. Auto Reboot

Auto reboot tab lets you set up scheduled reboot or ping reboot to the URL of your choice.



Auto reboot options

Enable scheduled reboot ☑

Time of the day 14 10

Enable ping reboot ☑

IP address or URL

Auto Reboot form

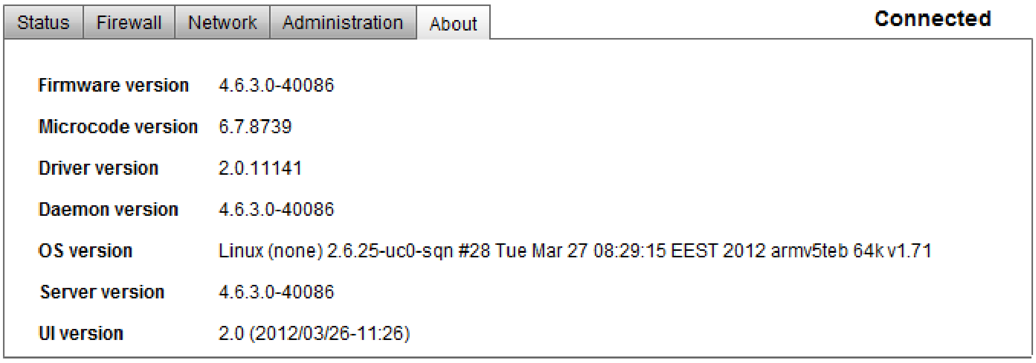
Enable scheduled reboot – tick to enable scheduled reboot

Time of the day – set the time of the day reboot will begin

Enable ping reboot – tick to enable ping reboot

IP address or URL – ping destination to decide whether to reboot or not

11.7. About



Firmware version	4.6.3.0-40086
Microcode version	6.7.8739
Driver version	2.0.11141
Daemon version	4.6.3.0-40086
OS version	Linux (none) 2.6.25-uc0-sqn #28 Tue Mar 27 08:29:15 EEST 2012 armv5teb 64k v1.71
Server version	4.6.3.0-40086
UI version	2.0 (2012/03/26-11:26)

About page

The About page displays the versions of your firmware and software that are currently running on your device. This helps you decide whether or not you need to update your firmware.

Note: The last part in the OS version string refers to the sector size (64 kilobytes in this case) of the flash memory. It is important that the firmware you update is made for the same flash sector size as the flash memory in the device.

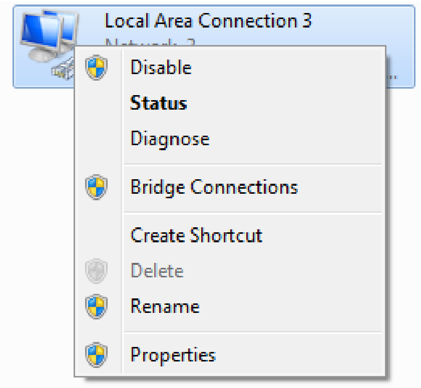
12. Troubleshooter:

Q: I think my router is not working: can not acquire connection and WebUI is not reachable.

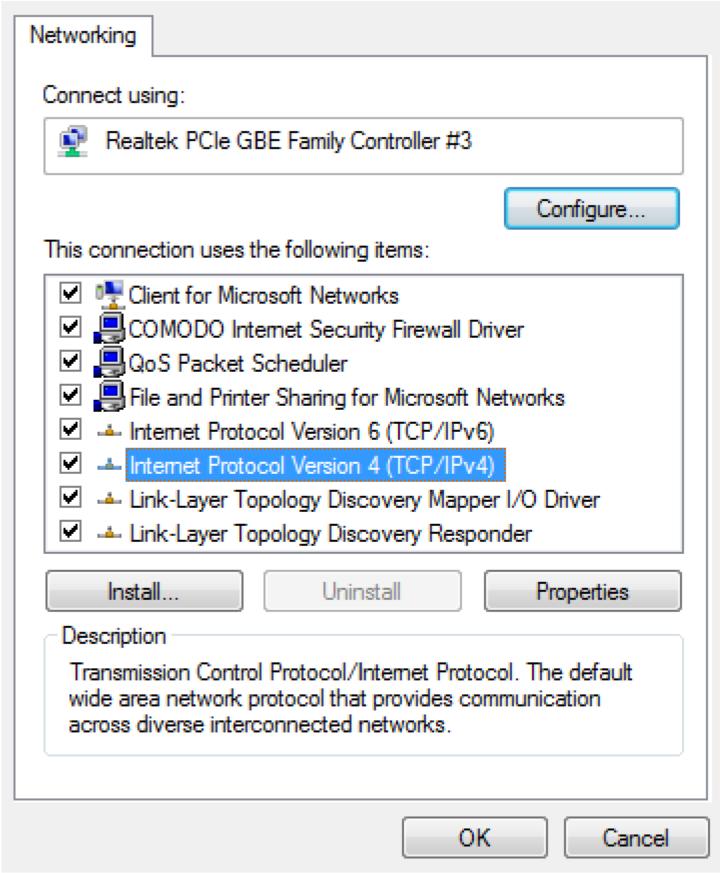
A: Check if IP address is set to obtain automatically via DHCP. Follow these steps:

Windows 7:

- Go to **Control panel -> Network and internet -> Network sharing center -> change adapter settings**.
- Right click on a Local Area Connection which uses RUT4xx for connecting to the internet and click **Properties**.



- Check **Internet Protocol IPv4 (TCP/IP)** and click **Properties**.



Connect using:

Realtek PCIe GBE Family Controller #3

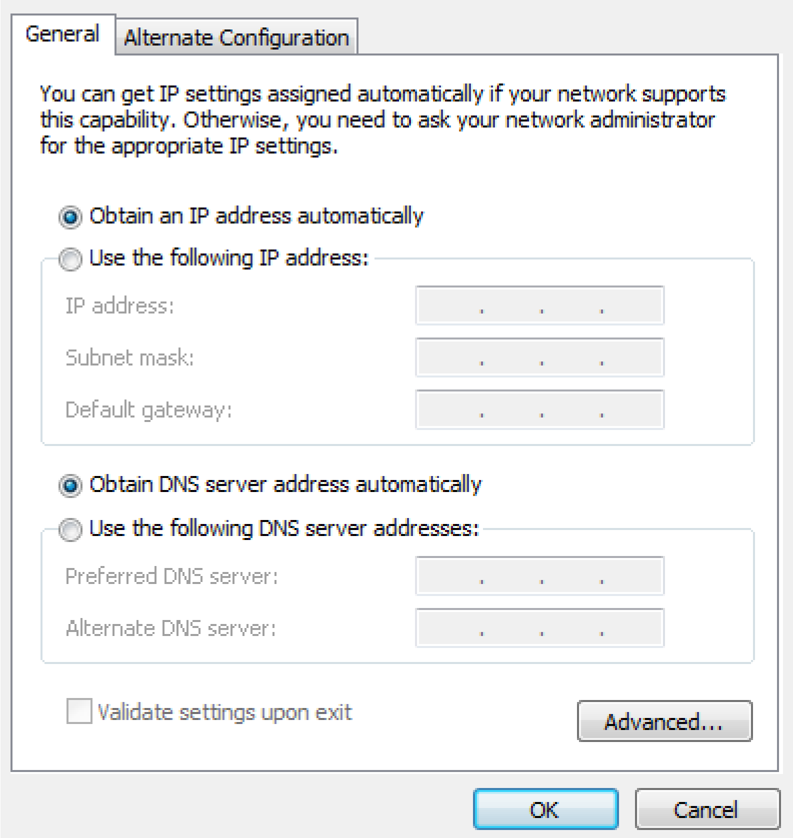
This connection uses the following items:

☑ Client for Microsoft Networks
☑ COMODO Internet Security Firewall Driver
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

- Make sure that **Obtain IP address automatically** is checked in the **General** settings.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

- Click **OK**.

13. Technical specifications

Video

Sensor	5Mpix CMOS
Sensor size	1/2.5 inch
Compression	H.264
Resolution	Full HD 1080p @ 23 fps SXVGA (1280 x 960) @ 30 fps
Supported microSD card capacity	up to 32GB

WiMAX

Standard Compliant	IEEE 802.16e-2005
Air Interface	S-OFDMA
Frequency Band	2.3 – 2.4 GHz (RUT423), 2.5 – 2.7 GHz (RUT425), 3.3 – 3.6 GHz (RUT435) or 3.3 – 3.8 GHz (RUT438)
Channel Bandwidth	3 MHz, 3.5 MHz, 5 MHz, 6 MHz, 7 MHz, 8.75 MHz and 10 MHz
Modulation Adaptive	QPSK, 16QAM, 64QAM
MIMO	MRC, Matrix A + MRC, Matrix B
Beamforming	All I/O Beamforming Items
RF Output Power	2x25 dBm @ 2.3 – 2.7GHz; 2x23dBm @ 3.3 – 3.8GHz
RX Sensitivity	RUT435: QPSK1/2: -99 @ 3.5 GHz and 10 MHz BW 16QAM1/2: -93.8 @ 3.5 GHz and 10 MHz BW RUT425: QPSK1/2: -99.5 @ 2.5 GHz and 10 MHz BW 16QAM1/2: -94.29 @ 2.5 GHz and 10 MHz BW
Antenna Gain	Several option available. 2 dBi with standart antenna
Antenna Type	External (2 x RP-SMA connectors)
Handover	Hard / Optimized Handover
QoS Mechanism	UGS, Real-Time-VR, Non Real-Time-VR, Best Effort, ERT-VR
Authentication	EAP-TLS, EAP-TTLS-MSCHAPv2
Encryption	3 CCM-Mode 128-bit AES
Error Handling	HARQ UL and DL, up to Category 7
Throughput	40 Mbps Total DL + UL

Electrical, Mechanical & Environmental

Dimensions (H x W x D)	280mm x 140mm x 94mm
Weight	920g
Power Supply Voltage	11VDC...14VDC
Power Consumption	< 10W
Operating Temperature	-20º to 50º C
Storage Temperature	-20º to 60º C
Storage Humidity	10% to 90% Non-condensing

14. Abbreviations

CBR	Constant Bit Rate
CMOS	Complementary Metal–Oxide–Semiconductor
FPS	Frames Per Second
HD	High Definition
Hz	Hertz
IP	Internet Protocol
IR	Infrared
Kbps	Kilobits Per Second
LED	Light-Emitting Diode
LPS	Limited Power Source
Mbps	Megabits Per Second
Mpix	Mega pixel
OSD	On-Screen Display
PC	Personal Computer
PSU	Power Supply Unit
RTSP	Real Time Streaming Protocol
SD	Secure Digital
SXVGA	Super Extended Video Graphics Array
USB	Universal Serial Bus
V	Volts
VBR	Variable Bit Rate
VDC	Volts of Direct Current