Mounting and Operating Manual

Dear Customer!
By selecting this VC product you have chosen a professional device, which guarantees highest possible quality and reliability.

Please read the following instructions carefully before comissioning the product in order to be able to take full advantage of all quality features regarding this product line.

Video transmission via mobile

GSM-/ UMTS router

Art. no. 15601

VC-videocomponents.... aligned for professional videosystems

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

CE COMPLIANCE

This equipment has been tested and found to comply with the limits for a Class B digital device.

ATTENTION

Before using the device we strongly recommend read this user manual.

Do not rip the device. Do not touch the device if the device block is broken or its connecting wires are without isolation.

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

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

The device requires high 230V AC voltage.

IMPORTANT NOTES!

It is mandatory to read the notes and manual carefully before starting to use the device.

Table of Contents

1 SAFETY INFORMATION

In this document you will be introduced how to use 3G Mobile Router safely. We suggest you to adhere to following recommendations to avoid any damage to person or property.

You have to be familiar with the safety requirements before starting to use the device!
3G Mobile Router is used to provide a mobile Internet access using a GSM network. To avoid burning and voltage caused traumas, of the personnel working with device, please follow these safety requirements.

Device requires power supply source that satisfies all safety requirements listed in LST EN 60950-1 standard. Each power supply source should not exceed 15VA.

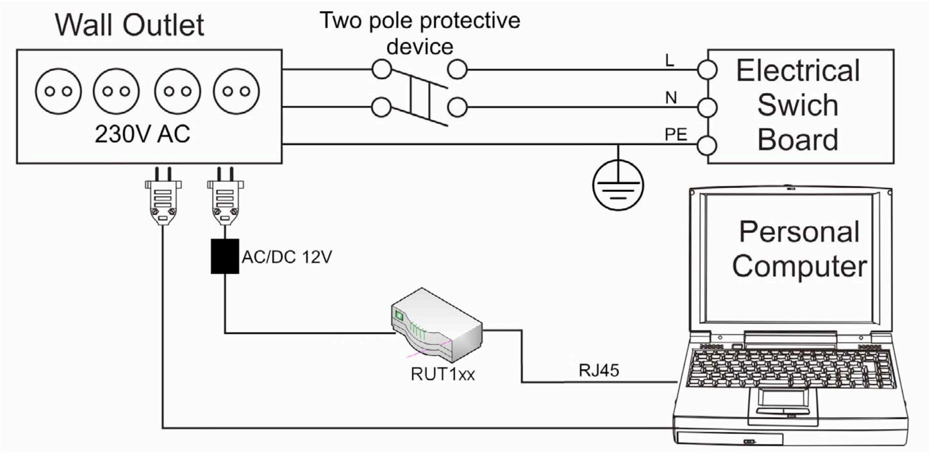
The PC and power supply source, to which the device is connected, should satisfy LST EN 60950-1 standard. The device can be used on first (Personal Computer) or second (Notebook) computer safety class.

Disconnect device from power supply before mounting to avoid voltage effect!

Do not mount or serve device during a thunderbolt.

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

Protection against over currents, short circuits and earth faults should be provided as a part of the building installation. Two pole protective device is required to protect from short-circuit and earth false. The power of connected device should satisfy power of release device. To disconnect the device plug off AC/DC power adapter from the wall outlet or power strip. The interstice between contacts should be no less than 3mm.



Signal level of the device depends on the environment in which it is working. If the device starts working insufficiently only qualified personnel may repair this product. We recommend to forward it to repair centre or to manufacturers. No exchangeable parts inside of the device.

2 PRODUCT OVERVIEW

2.1 Introduction

VC 3G Mobile Router provides WAN connectivity to wired and wireless clients using the 3G cellular data network. It allows multiple users to get IEEE 802.11 compliant connection within your wireless broadband network with a single 3G data access account and SIM card. 3G Mobile Router is extremely useful for mobile work teams or emergency crews that need access to the broadband Internet but have no permanent base. The 3G/IEEE 802.11 router might be an easy solution to provide Internet connection for commuter vehicles, such as trains or company buses. Quickly set up a IEEE 802.11 hotspot Internet connection to check email and browse the web or share files.

2.2 Package contents

- 3G Mobile Router
- 2 external Wireless LAN antennas
- 2 External GSM antennas
- Power adapter
- CAT5 LAN cable
- CD with User Manual
- Leaflet “Quick Start Guide”

Note: The manufacturer does not supply the SIM card, which is mandatory for setting up a connection to the GSM network! The SIM card may be purchased from your GSM (mobile) service provider!

Note: Using a power supply with a different voltage rating than the one included with the RUT100 will cause damage and void the warranty for this product.

Note: If any of the components is missing or damaged, please contact the retailer or reseller from which this product was purchased.

2.3 System requirements

A computer with Windows®, Macintosh®, or Linux-based operating systems with a network connection (wired or wireless).

A web browser Internet Explorer 6.0, Netscape Navigator™ 6.0, Opera 9.0, Mozilla 5.0 or later versions for configuration.

2.4 Hardware, LED's and connections

2.4.1 Back panel

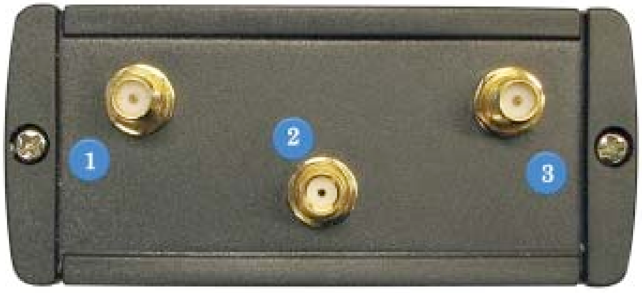


Figure 1. Router back panel view.

1. Wireless LAN antenna connection.
2. GSM antenna connection.
3. Wireless LAN antenna connection.

2.4.2 Front panel

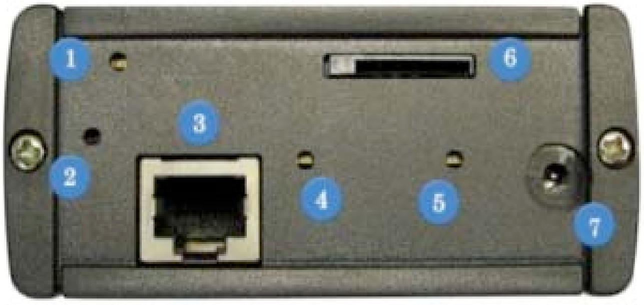


Figure 2. Router front panel view.

1. 3G LED. A solid light indicates proper connection of the 3G.
2. Reset button.
3. Ethernet socket.
4. Ethernet LED. A solid light indicates proper connection of the Ethernet. A blinking light indicates data transfer.
5. Power LED. A solid light indicates a proper connection to the power supply.
6. SIM card socket.
7. Power supply adapter socket.

3 GETTING STARTED

3.1 Initial setup

3G Mobile Router enables to access network using a wireless connection from virtually anywhere within the operating range of wireless network. Some things should be considered before finding place to set up access point:

1. Make sure the power outlet is nearby as the router requires power supply.
2. Keep the access point as central in work area as possible.
3. The number of walls and ceilings between the router and other network devices should be kept to a minimum as each wall or ceiling probably will reduce adapter's range from 1-30 meters. Signal strength and speed fall off with distance.
4. Higher is often better. Set up the router on the top shelf of a bookcase rather than the bottom one, if it is possible. The antenna usually works best if oriented to point straight up.
5. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access point and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, mirrors, file cabinets, bricks, and concrete will degrade wireless signal.
6. Keep router away (at least 1-2 meters) from electrical devices or appliances that generate RF noise.
7. If you are using 2.4GHz cordless phones or other wireless products your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone in not in use.

3.2 Router installation guide

1. Attach Wireless LAN and GSM antennas.
   - Remove the antenna from its plastic wrapper.
   - Screw the antenna in a clockwise direction to the back panel of the unit.
   - Position the antenna upward at its connecting joint. This will ensure optimal reception.
2. Insert the SIM card which was given by your GSM (mobile) service provider.
3. Insert the Ethernet cable into LAN Port if the router will be configured using wired connection.
4. Connect the power adapter to the socket on the front panel of 3G Mobile Router. Then plug the other end of the power adapter into a wall outlet or power strip.

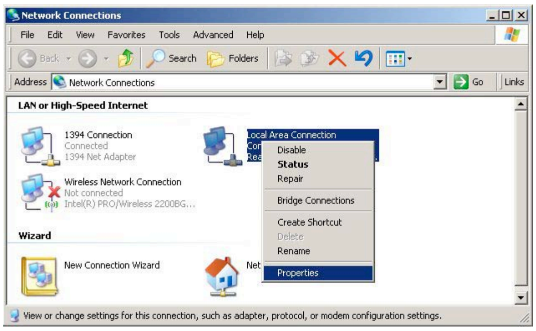
Note: SIM card is mandatory for setting up connection to the GSM network. However, the manufacturer of this equipment does not supply the SIM card. The SIM card can be purchased from your GSM (mobile) service provider! For APN, user name and password please contact your GSM (mobile) service provider. The 3G Mobile Router must be powered off while inserting or taking out the SIM card.

4 ROUTER CONFIGURATION

4.1 Connect to router WEB configuration page using wired connection

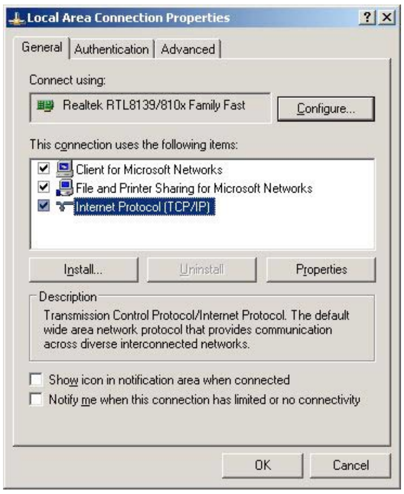
Step 1 Connect 3G Mobile Router to your PC using LAN cable.

Step 2 Setup Local Area Network adapter on your computer (Go to **Start** > **Settings** > **Network Connections** Right click on **Local Network Connection** select **Properties)**



View or change settings for this connection, such as adapter, protocol, or modem configuration settings.

Step 3 Setup the Local Area network adapter's IP address. Choose **Internet Protocol (TCP/IP)** and click **Properties**.



Connect using:

Realtek RTL8139/810x Family Fast

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol (TCP/IP)

Description

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

□ Show icon in notification area when connected

□ Notify me when this connection has limited or no connectivity

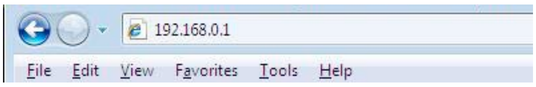
Setup the Local area network adapter to

Obtain an IP address automatically and

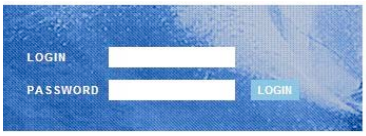
Obtain DNS server address automatically

Note: It is possible to assign manually static IP address within 192.168.0.2 - 192.168.0.254 address range with mask 255.255.255.0, gateway 192.168.0.1 and DNS server 192.168.0.1.

Step 4 Open the Web browser and type the IP address of the router (Default : 192.168.0.1) and enter the 3G Mobile Router administrator login details to access the Web management tool:



192.168.0.1



The default administrator login settings are:

Login: **admin**

Password: **admin01**

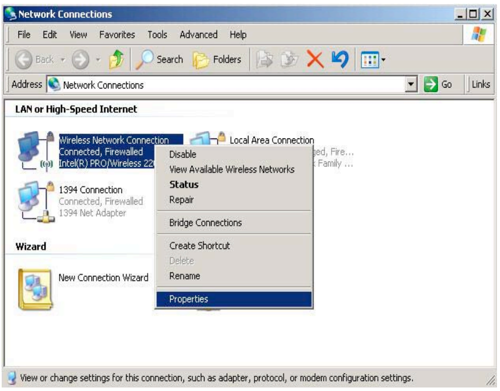
Note: It is strongly recommended to change the password after the first router configuration.

Step 5 After successful administrator log on you will see the main page of the 3G Mobile Router Web configuration interface. The device now is ready for configuration.

4.2 Connect to router WEB configuration page using wireless connection

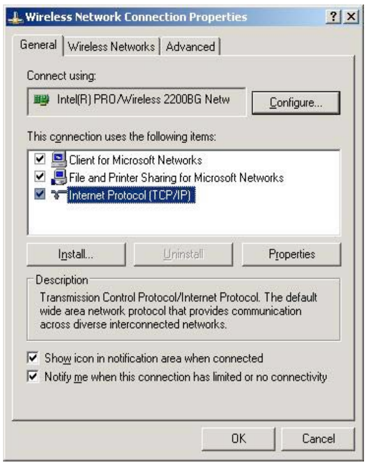
Note: the Wireless network function is shipped disabled by default and the configuration for the first time can be made only by using wired connection.

Step 1 Setup wireless network adapter on your computer (Go to **Start>Settings>Network Connections**>Right click on **Wireless Network Connection** associated with the wireless adapter and select **Properties)**:



View or change settings for this connection, such as adapter, protocol, or modem configuration settings.

Step 2 Setup the wireless network adapter's IP address (choose **Internet Protocol (TCP/IP)** and click **Properties**):


Wireless Network Connection Properties
General Wireless Networks Advanced
Connect using:
Intel(R) PRO/Wireless 2200BG Netw
Configure...
This connection uses the following items:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity
OK Cancel

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

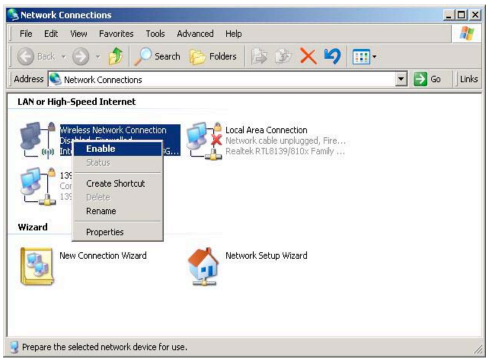
Setup the wireless network adapter to

Obtain an IP address automatically and

Obtain DNS server address automatically

Note: It is possible to assign manually static IP address within 192.168.0.2 - 192.168.0.254 address range with mask 255.255.255.0, gateway 192.168.0.1 and DNS server 192.168.0.1.

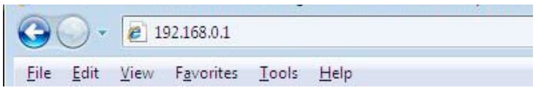
Step 3 Enable the wireless network connection. Right click on **Wireless Network Connection** and chose **Enable**.

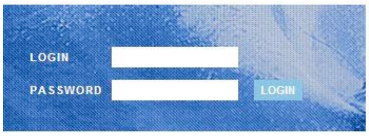

Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections Go Links
LAN or High-Speed Internet
Wireless Network Connection
Local Area Connection
Network cable unplugged, Fire...
Realtek RTL8139/810x Family ...
Enable
Status
Create Shortcut
Delete
Rename
Properties
Wizard
New Connection Wizard
Network Setup Wizard

Prepare the selected network device for use.

Step 4 Choose the wireless network from the list of available wireless networks.

Step 5 Open the Web browser and type the device IP address (default 192.168.0.1) and enter the 3G Mobile Router administrator login details to access the Web management.





The default administrator login settings are:

Login:	**admin**
Password:	**admin01**

Step 6 After successful administrator log on you will see the main page of the 3G Mobile Router Web configuration interface. The device now is ready for configuration.

4.3 WEB configuration page interface structure

The main Web management menu is displayed after successful login into the system (Figure 3). From this menu all essential configuration pages are accessed.

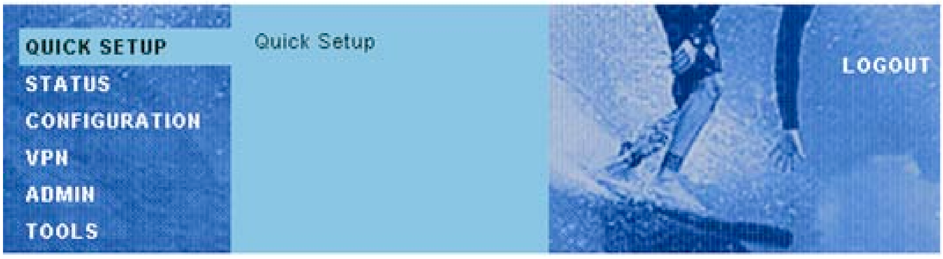


Figure 3. Main Management Menu

By default the **Quick Setup** menu is activated. The web management menu has the following structure:

Quick Setup – quick router configuration wizard.

Status

System Information – displays general information of the device status.

Hardware information – displays device hardware information.

ARP table – displays map of IP addresses assigned to the MAC addresses.

DDNS – displays DDNS status information.

Configuration

Mobile Network Settings

Network Settings

Wireless Settings

Dynamic DNS Settings

Port forwarding

Services – SSH, HTTPS services management.

VPN

OpenVPN – Create site to site tunnel.

GRE Tunnel – Create GRE tunnel.

IPsec – IPsec client settings.

Admin

Account – change administrator's password.

Management – administrative access settings.

Maintenance – firmware upgrade, log troubleshoot file download, reboot or reset to factory defaults the device.

Tools

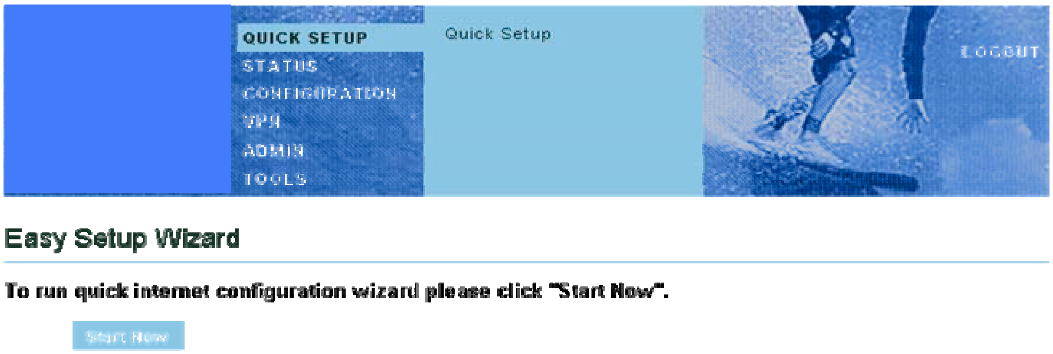
Site Survey – shows information about wireless networks in the local geography.

Ping Reboot – set up continuous ping IP address with possibility to automatically reboot router if no echo received.

4.4 Quick Setup

Use **Quick Setup** to quickly configure basic 3G Mobile Router settings. The configuration is made in four steps (this is the default page when accessing the administration web management interface).

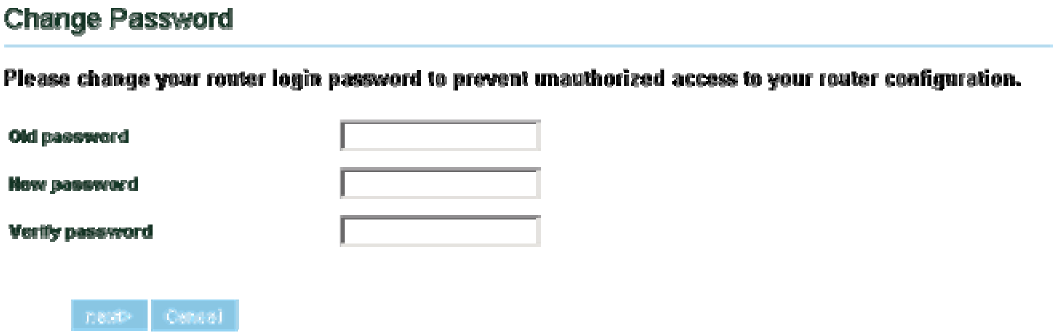
To start quick setup wizard click button **Start Now**.



Easy Setup Wizard

To run quick internet configuration wizard please click "Start Now".

Step 1. Change router login password in order to prevent unauthorized login to the router.



Change Password

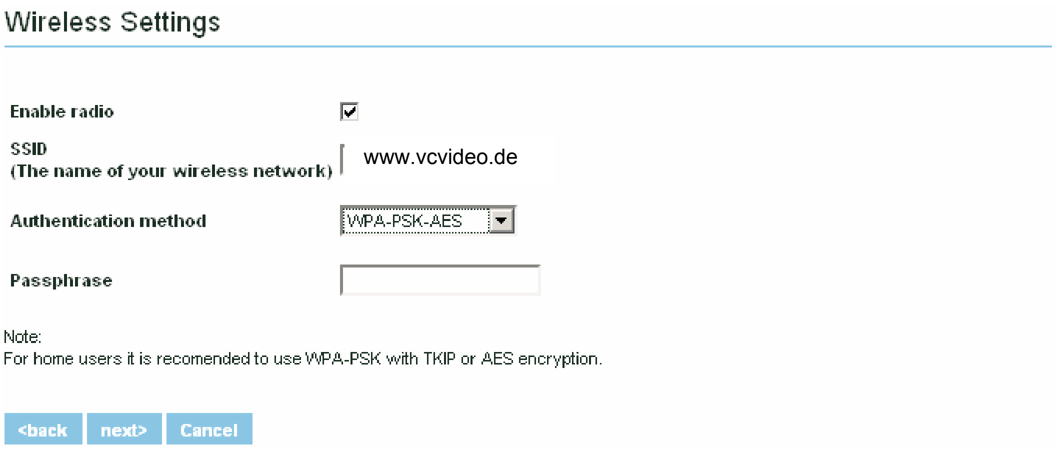
Please change your router login password to prevent unauthorized access to your router configuration.

Old password

New password

Verify password

Step 2. Configure wireless network settings.



Wireless Settings

Enable radio ☑

SSID (The name of your wireless network): www.vcvideo.de

Authentication method: WPA-PSK-AES

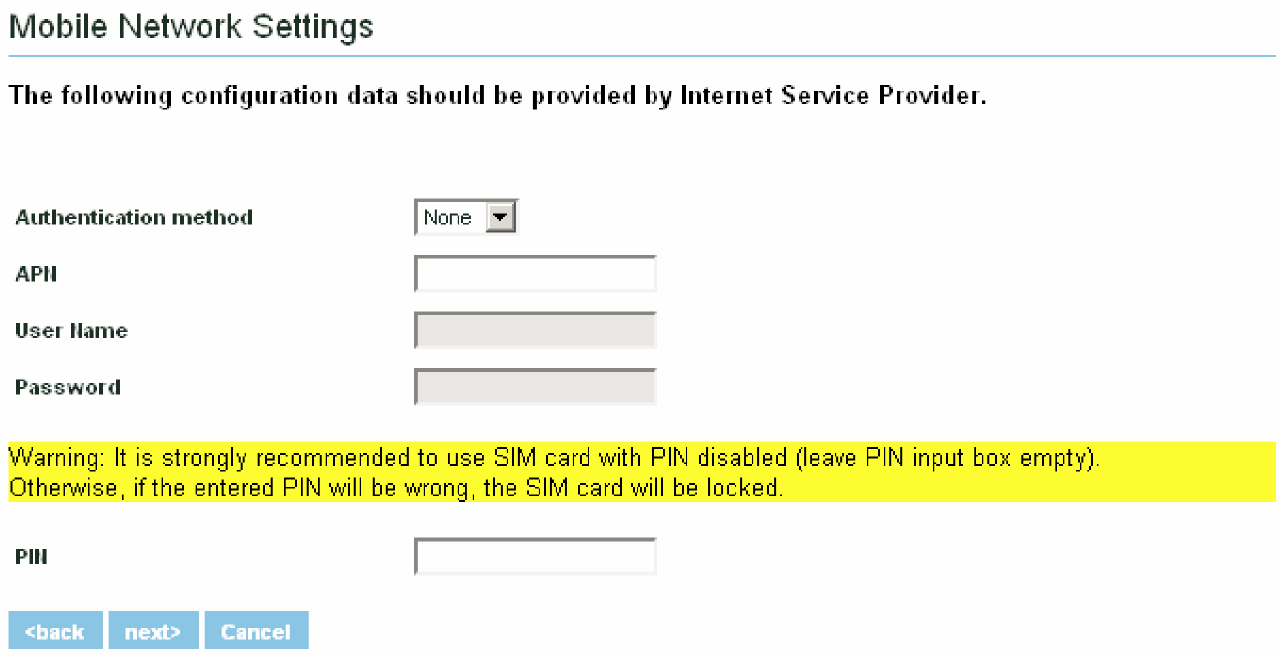
Passphrase

Note:
For home users it is recomended to use WPA-PSK with TKIP or AES encryption.

It is recommended to use **WPA-PSK** with **TKIP** or **AES** data encryption. The passphrase for data encryption may be 8-63 characters long and can include symbols (!?*&_) and spaces. This passphrase must be the same as Network key in the PC wireless network security settings. If encryption is chosen do not forget to configure your PC settings (refer to Appendix A).

Note: If **Open system** will be chosen it will let anyone within the range and with proper equipment to connect to your network.

Step 3. Configure mobile network settings. The configuration data should be provided by your ISP (Internet Service Provider).



Mobile Network Settings

The following configuration data should be provided by Internet Service Provider.

Authentication method: None

APN

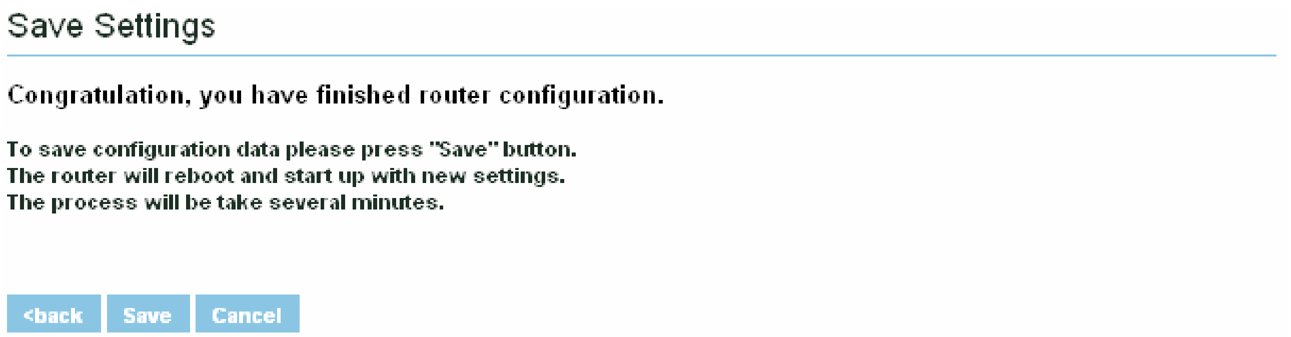
User Name

Password

Warning: It is strongly recommended to use SIM card with PIN disabled (leave PIN input box empty).
Otherwise, if the entered PIN will be wrong, the SIM card will be locked.

PIN

Step 4. After successful configuration please click **Save** button. The router will reboot and start up with new settings. The process will take several minutes.



Save Settings

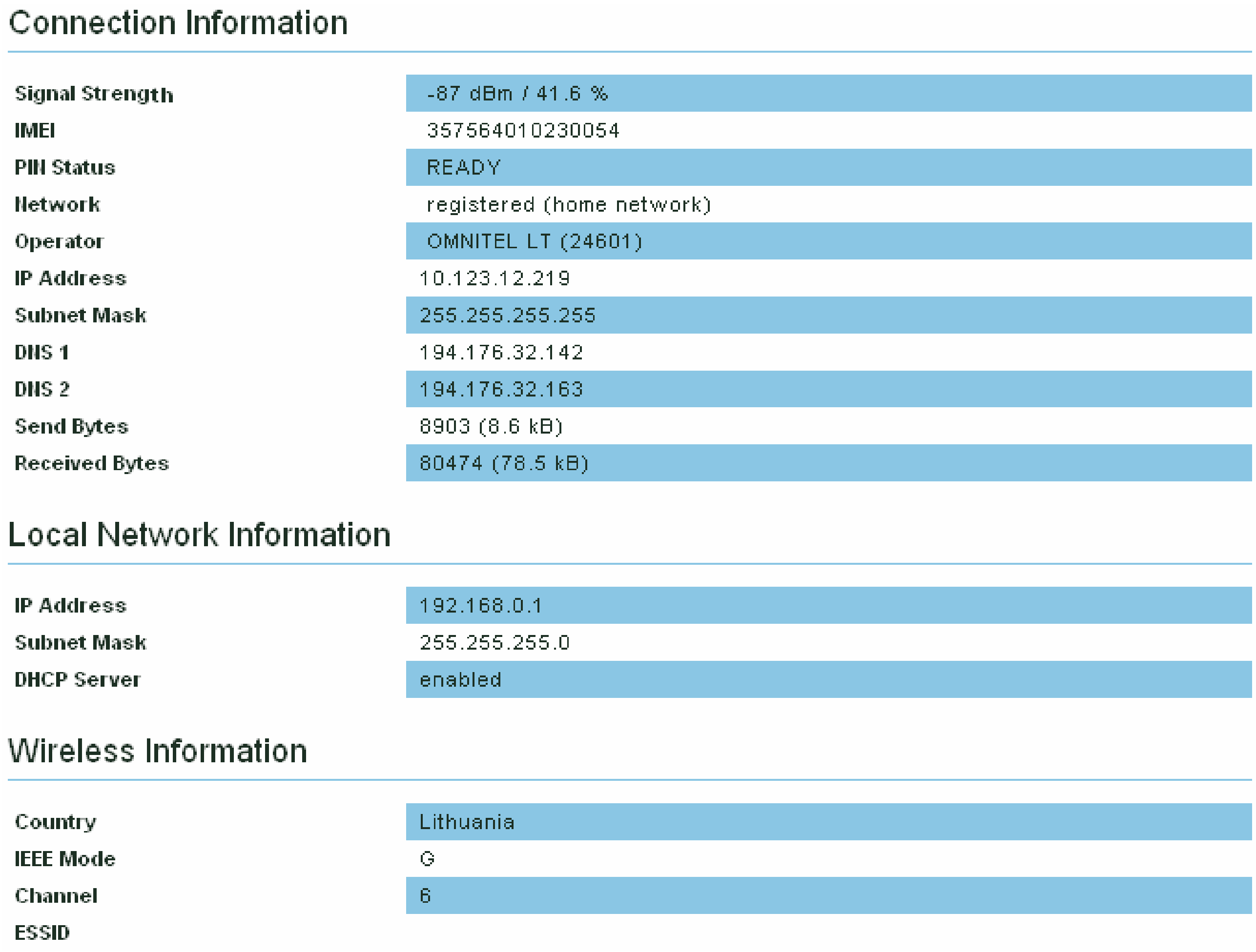
Congratulation, you have finished router configuration.

To save configuration data please press "Save" button.
The router will reboot and start up with new settings.
The process will be take several minutes.

4.5 Status

4.5.1 System Information

System Information menu displays general devices status.



Connection Information

Signal Strength	-87 dBm / 41.6 %
IMEI	357564010230054
PIN Status	READY
Network	registered (home network)
Operator	OMNITEL LT (24601)
IP Address	10.123.12.219
Subnet Mask	255.255.255.255
DNS 1	194.176.32.142
DNS 2	194.176.32.163
Send Bytes	8903 (8.6 kB)
Received Bytes	80474 (78.5 kB)

Local Network Information

IP Address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP Server	enabled

Wireless Information

Country	Lithuania
IEEE Mode	G
Channel	6
ESSID	

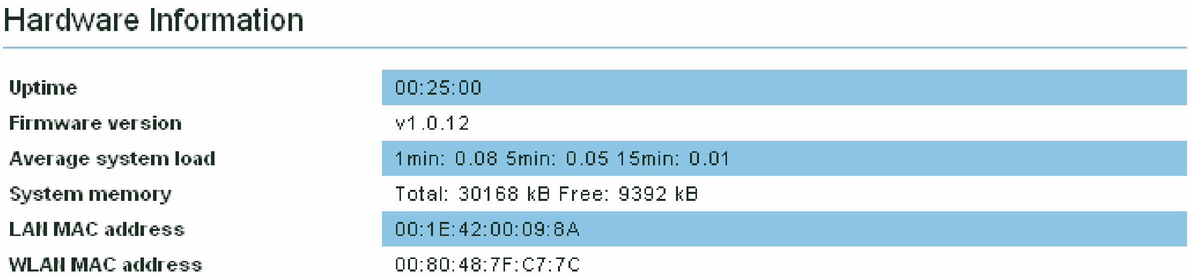
Figure 4. System Information

Connection information – displays the GSM network information

Local Network Information – displays local network configuration.

Wireless Information – displays wireless network information**.**

4.5.2 Hardware information



Hardware Information

Uptime	00:25:00
Firmware version	v1.0.12
Average system load	1min: 0.08 5min: 0.05 15min: 0.01
System memory	Total: 30168 kB Free: 9392 kB
LAN MAC address	00:1E:42:00:09:8A
WLAN MAC address	00:80:48:7F:C7:7C

Figure 5. Interfaces

Uptime – displays the time since the system was last rebooted.

Firmware version – displays current version of the firmware.

Average system load – displays the average load of the device processor in the period of the last 1 minute, 5 minutes and 15 minutes (a larger value means a larger average load on the processor: <1.0 – System is idle; =1.0 – Normal load; >1.0 – Processor is busy).

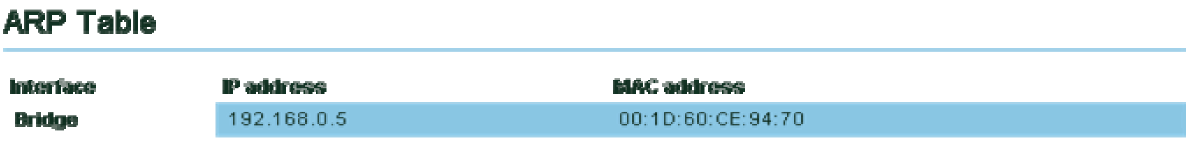
System memory – displays total and free system memory.

LAN MAC address – displays wired LAN MAC address.

LAN MAC address – displays wireless LAN MAC address.

4.5.3 ARP table

The ARP Table shows map of the IP addresses assigned to the MAC addresses.



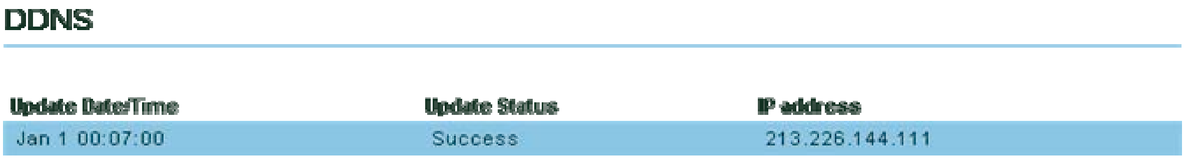
ARP Table

Interface	IP address	MAC address
Bridge	192.168.0.5	00:1D:60:CE:94:70

Figure 6. ARP information

4.5.4 DDNS

Dynamic DNS service status is displayed in the DDNS section.



DDNS

Update Date/Time	Update Status	IP address
Jan 1 00:07:00	Success	213.226.144.111

Figure 7. DDNS status

4.6 Configuration

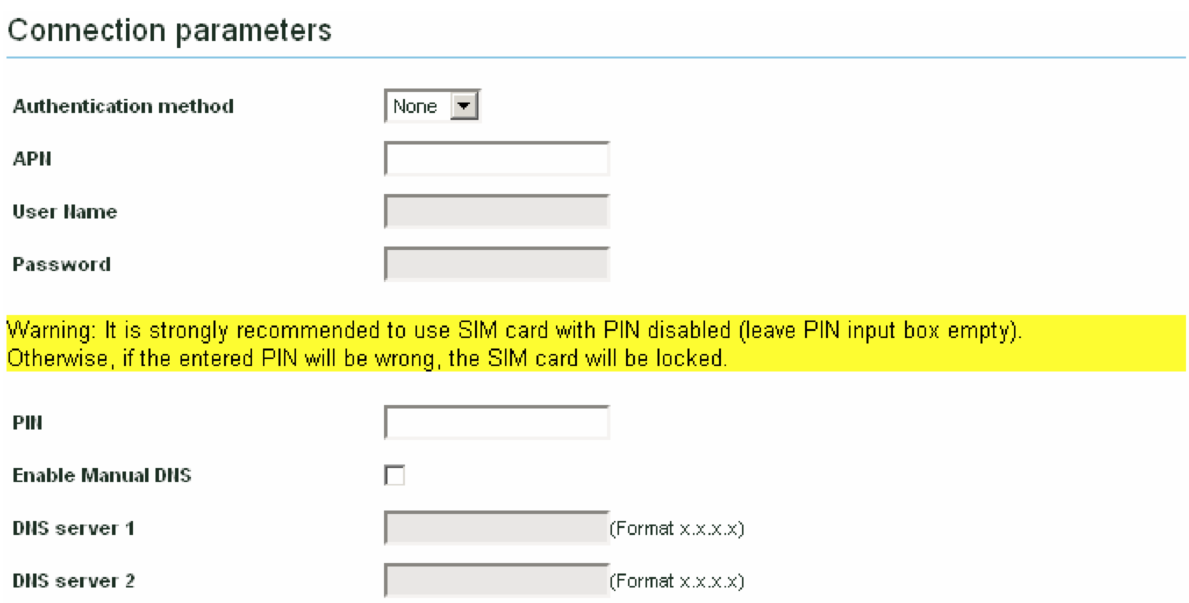
4.6.1 Mobile Network Settings

To set up the GSM connection SIM card is required. SIM card is not supplied with the router. It may be purchased from internet service provider.

The following information to connect to the internet is required:

1. **PPP authentication.** The authentication protocol, which is used by your Internet Service Provider [None, CHAP or PAP].
2. **APN.** Access Point Name (APN).
3. **User Name.** If GSM operator does not require username, leave it blank.
4. **Password.** If GSM operator does not require password, leave it blank.
5. **SIM card PIN number.**
6. **DNS server 1.** If GSM operator does not require DNS server 1, leave it blank.
7. **DNS server 2**. If GSM operator does not require DNS server 2, leave it blank.

Warning: It is strongly recommended to use SIM card with PIN disabled. Otherwise, if the entered PIN will be wrong, the SIM card will be locked.



Connection parameters

Authentication method	None ▾
APN	
User Name	
Password	

Warning: It is strongly recommended to use SIM card with PIN disabled (leave PIN input box empty).
Otherwise, if the entered PIN will be wrong, the SIM card will be locked.

PIN	
Enable Manual DNS	□
DNS server 1	(Format x.x.x.x)
DNS server 2	(Format x.x.x.x)

Figure 8. Mobile network configuration.

Authentication method – Select authentication type PAP, CHAP or None.

APN – Access Point Name (APN)

User Name – Enter your User Name for your mobile connection.

Password – Enter your Password for your mobile connection.

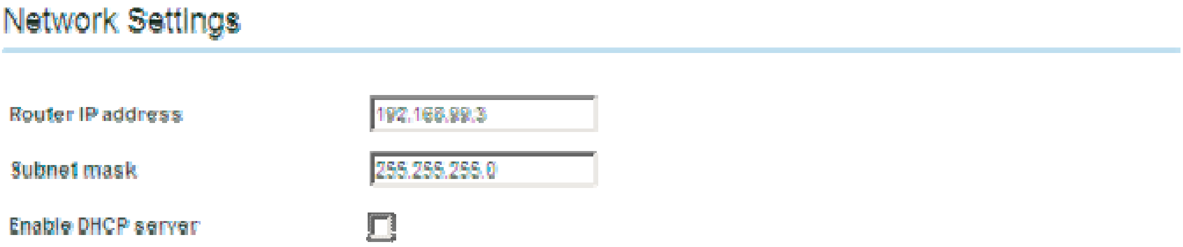
PIN – SIM card pin number.

Enable Manual DNS – check to enter custom DNS server IP addresses

DNS server 1 and **DNS server 2** are ISP domain servers.

4.6.2 Network Settings

This section will allow you to change the local network settings of the router and to configure the DHCP settings



Network Settings

Router IP address	192.168.99.3
Subnet mask	255.255.255.0
Enable DHCP server	□

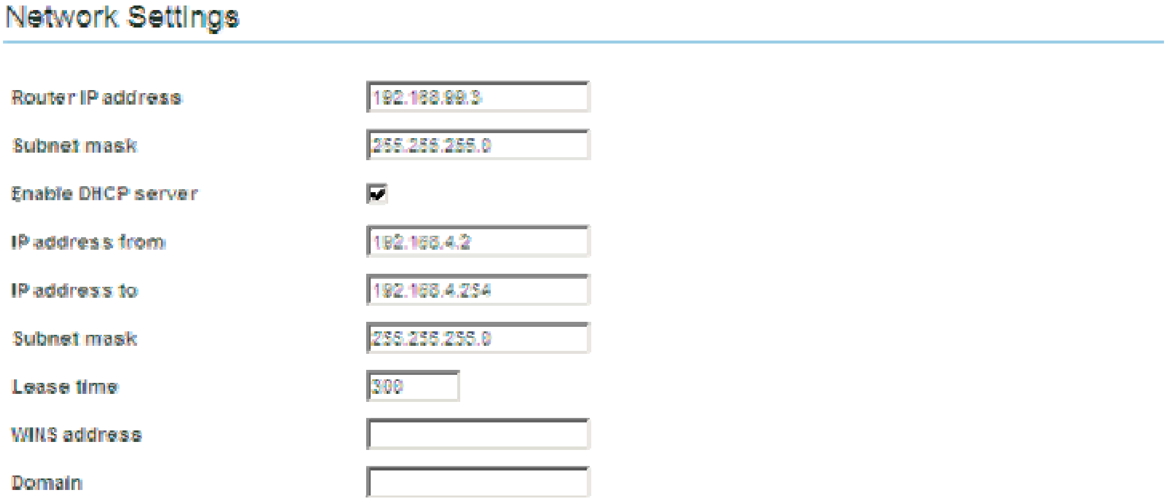
Figure 9. Network settings.

Router IP address. The IP address of the router. The default IP address is 192.168.0.1.

Subnet mask. The Subnet Mask of the router. The default subnet mask is 255.255.255.0.

Enable DHCP server. Check the box to enable the DHCP server on your router. Uncheck to disable this function

Enabled DHCP server allows configuring IP addresses pool that will be assigned by the router.



Network Settings

Router IP address	192.168.99.3
Subnet mask	255.255.255.0
Enable DHCP server	☑
IP address from	192.168.4.2
IP address to	192.168.4.254
Subnet mask	255.255.255.0
Lease time	300
WINS address	
Domain	

Figure 10. Network settings.

IP address from. Starting IP addresses for the DHCP server's IP assignment.

IP address to. Ending IP addresses for the DHCP server's IP assignment.

Subnet mask. The Subnet Mask of the router. The default subnet mask is 255.255.255.0.

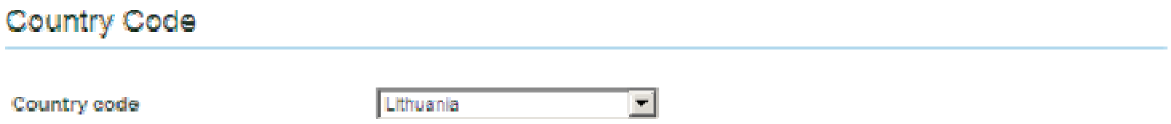
Lease time. Determines how long IP addresses are assigned for you. During the lease time, the DHCP server cannot assign that IP address to any other clients. The purpose of a lease is to limit the length of time that a client may use an IP address. A lease prevents unused clients from taking up IP addresses when there are more clients than addresses. Enter the Lease time in seconds.

WINS address. If WINS (Windows Internet Naming Service) server is specified, the router at system startup, will register its name and IP address with the WINS server. WINS server is used for mapping host names to network addresses. This results in fast and efficient host name resolution. Specify WINS server IP address.

Domain. Enter the domain name for the Router. Some ISP's require it for identification. Check your ISP to see if your broadband Internet service has been configured with a domain name. In most cases, leaving these fields blank will work.

4.6.3 Wireless Settings

4.6.3.1 Country code



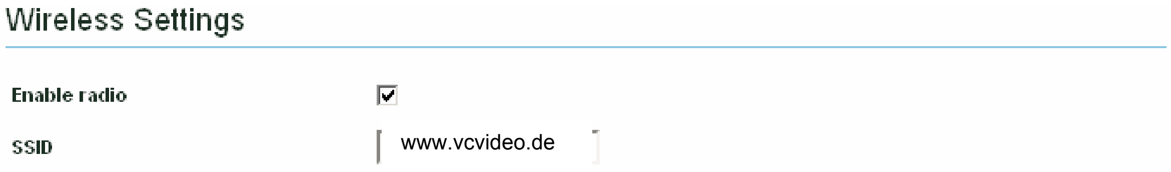
Country Code

Country code: Lithuania

Figure 11. Wireless network settings.

Country code. Select the country where the wireless network will be created.

4.6.3.2 Basic wireless settings



Wireless Settings

Enable radio ☑

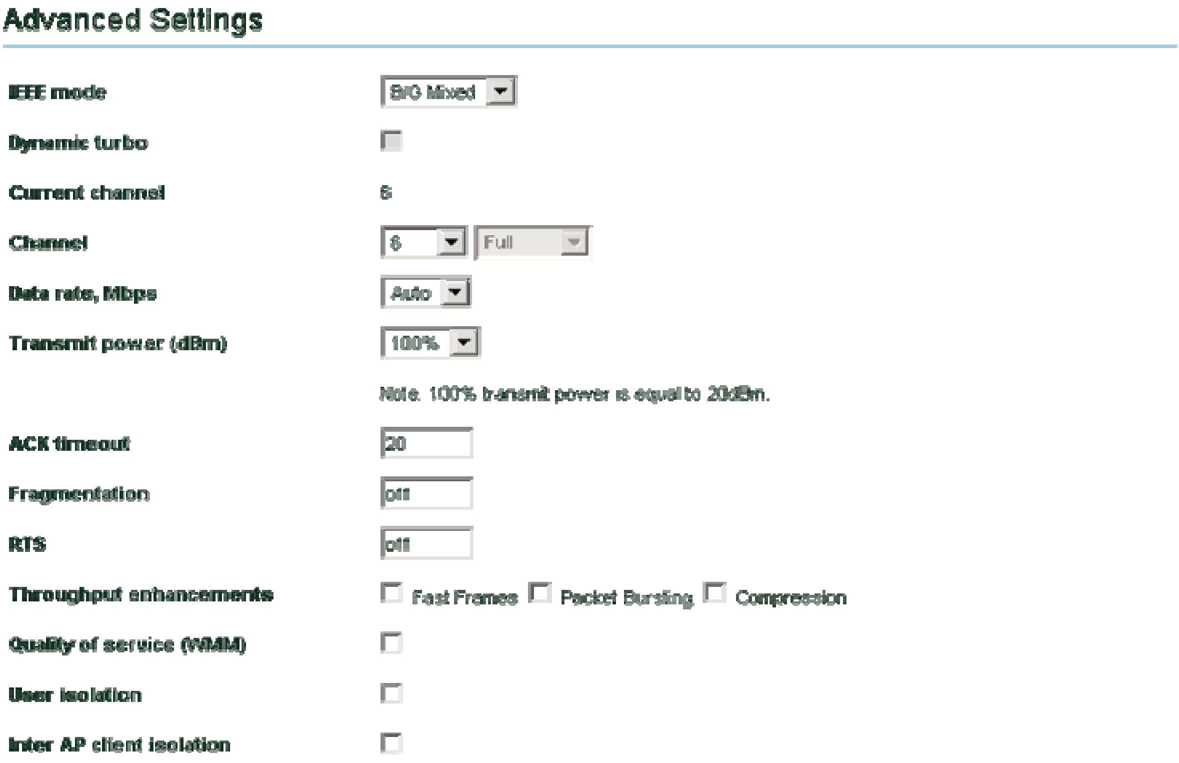
SSID: www.vcvideo.de

Figure 12. Wireless network settings.

Enable radio. Check the box to enable the wireless function. If you do not want to use wireless network, uncheck the box to disable the wireless function.

SSID. Specify a unique name for your wireless network.

4.6.3.3 Advanced wireless settings



Advanced Settings

IEEE mode: B/G Mixed

Dynamic turbo □

Current channel: 6

Channel: 6 Full

Data rate, Mbps: Auto

Transmit power (dBm): 100%

Note. 100% transmit power is equal to 20dBm.

ACK timeout: 20

Fragmentation: off

RTS: off

Throughput enhancements: □ Fast Frames □ Packet Bursting □ Compression

Quality of service (WMM) □

User isolation □

Inter AP client isolation □

Figure 13. Wireless network settings.

IEEE mode. Specify the wireless network mode [B, G, mixed B/G].

Dynamic turbo. The dynamic function allows the router to automatically search for channels with less noise and interference. By default, this feature is disabled. You can enable this feature by selecting the checkbox. (For G mode only.)

Current Channel. Indicates the current channel of the router.

Channel. Select the channel for the wireless network.

Data rate. Set the maximum wireless network data rate.

Transmit power. Set the maximum transmitter radiation power.

ACK timeout. Set ACK timeout in order to adjust the timeout value for long distance operation.

Fragmentation. Specify the fragmentation threshold (in bytes), which determines whether data frames will be fragmented and at what size [256-2346/off/auto]. On the 802.11 wireless LAN, frames exceeding the fragmentation threshold will be fragmented, i.e., split into smaller units suitable for the circuit size. Data frames smaller than the specified fragmentation threshold value are not fragmented. Default: off.

Note: Setting a lower fragmentation threshold value can help improve connection reliability in noisy environments (where radio interference is present). This mechanism does add overhead and therefore reduces effective throughput.

RTS. Specify the maximum packet size beyond which the wireless LAN card invokes it's RTS/CTS mechanism [0-2347/off/auto]. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The card transmits packets smaller than this threshold without using RTS/CTS. Default: off.

Note: Setting a lower RTS threshold value can improve connection reliability and throughput in crowded wireless LAN environments (where many clients are trying to communicate simultaneously). It adds a certain amount of overhead, but can compensate for this by reducing bandwidth lost due to collisions.

Throughput enhancements (available only on G mode).

Fast Frames – packet aggregation and timing modifications.

Packet Bursting – more data frames per given time period.

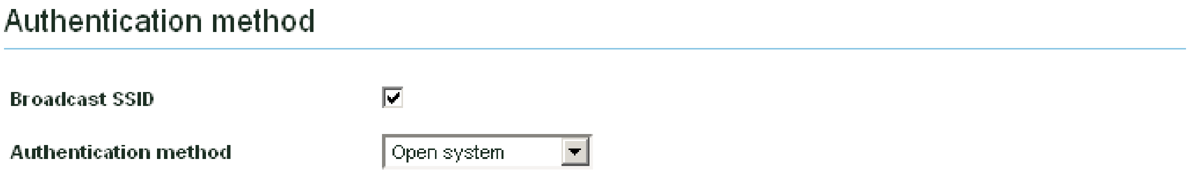
Compression – standards based (Lempel Ziv) real-time hardware compression.

Quality of service (WMM). Check the box to enable applications such as audio, video and voice to have higher priority than less-sensitive data applications.

User isolation. Check the box to isolate the wireless clients from communicating with each other.

Inter AP client isolation. Check the box to enable internal wireless network users isolation.

4.6.3.4 Wireless security



Authentication method

Broadcast SSID ☑

Authentication method Open system ▾

Figure 14. Wireless network authentication settings.

Broadcast SSID. Check the box to enable SSID broadcast.

Authentication Method. Choose the authentication method for wireless network:

Open system – no encryption. It will let anyone within range and with the proper equipment to connect onto your network within the router operating range.

WEP-64-bit – choose the 64 bit WEP security with one of four pre-shared keys.

WEP-128-bit– choose the 128 bit WEP security with one of four pre-shared keys.

WPA-PSK-TKIP – choose the WPA security with pre-shared key, encrypted by the TKIP (Temporal Key Integrity Protocol) algorithm.

WPA-PSK-AES – choose the WPA security with pre-shared key, encrypted by the AES algorithm.

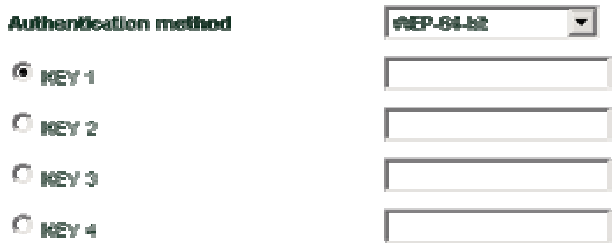
WPA2-PSK-TKIP – choose the WPA2 security with pre-shared key, encrypted by the TKIP (Temporal Key Integrity Protocol) algorithm.

WPA2-PSK-AES – choose the WPA2 security with pre-shared key, encrypted by the AES in Counter mode with CBC-MAC algorithm.

WPA-802.1x-TKIP – choose the WPA security encrypted in TKIP mode with 802.1x authentication (RADIUS infrastructure required).

WPA-802.1x-AES – choose the WPA security encrypted in AES mode with 802.1x authentication (RADIUS infrastructure required).

4.6.3.4.1 Wireless security with WEP 64/128bit



Authentication method: WEP-64-bit

● KEY 1

○ KEY 2

○ KEY 3

○ KEY 4

Figure 15. WEP settings.

Key 1 ~ Key 4: Allows creating up to 4 different WEP keys. By clicking the round button default key is selected. WEP keys should be entered as a series of colon-separated hexadecimal (0-9, A-F, and a-f) pairs:

5 pairs for 64-bit WEP security (eg. 00:AC:01:35:FF)

13 pairs for 128-bit WEP security (eg. 00:11:22:33:44:55:66:77:88:99:AA:BB:CC)

4.6.3.4.2 Wireless security WPA/WPA2 with pre-shared key

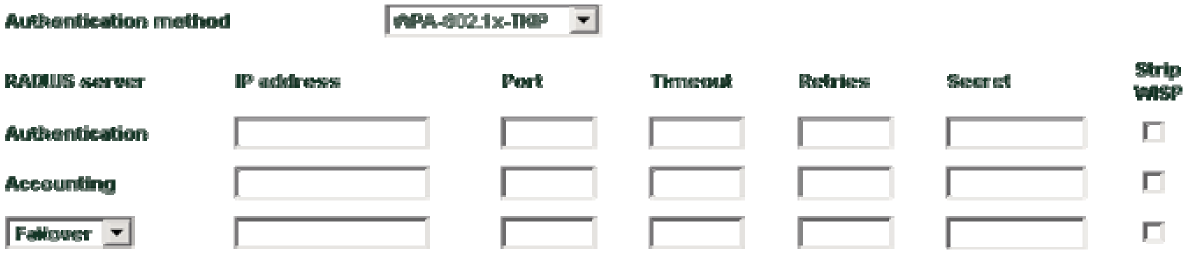
Authentication method: WPA-PSK-TKIP

Passphrase

Figure 16. WPA with Passphrase Encrypted in TKIP Wireless Security

Passphrase – passphrase for data encryption may be 8-63 characters long and can include symbols (!?*&_) and spaces. The passphrase will be converted to pre-shared key format, selected above.

4.6.3.4.3 Wireless security with the RADIUS authentication



Authentication method: WPA-802.1x-TKIP

RADIUS server	IP address	Port	Timeout	Retries	Secret	Strip WISP
Authentication						□
Accounting						□
Failover						□

Figure 17. WPA with RADIUS Authentication Wireless Security

IP address – specify the IP address of the authentication/accounting RADIUS server.

Port – specify the network port used to communicate with the RADIUS authentication/accounting server [1-65535]. Default: 1812 for authentication, 1813 for accounting servers.

Timeout – specify the authentication/accounting request timeout in seconds [1-999]. Default: 2. If RADIUS response is not received during timeout period, request is retransmitted.

Retries – specify the number of times authentication/accounting request is retransmitted [0-99]. Default: 2.

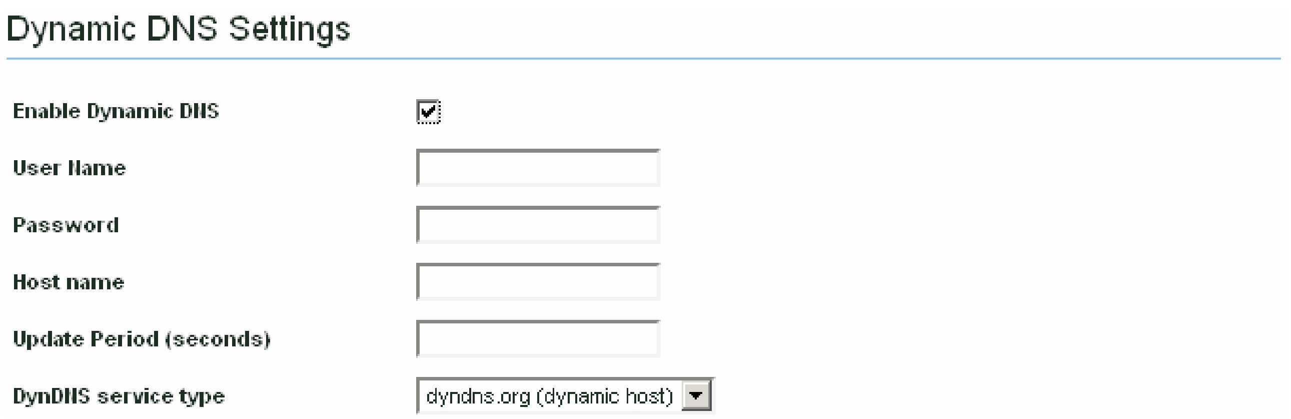
Secret – specify the shared secret of the authentication/accounting server [string]. The shared secret is used to encrypt data packets transmitted between RADIUS server and client.

Note: Shared secrets must be the same on the RADIUS servers and the RADIUS client.

Strip WISP – select this option if you want to remove the WISP domain prefix from the username before sending it to the RADIUS server. Default action is to send the username as is.

4.6.4 Dynamic DNS Settings

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

Enable Dynamic DNS	☑
User Name	
Password	
Host name	
Update Period (seconds)	
DynDNS service type	dyndns.org (dynamic host) ▼

Figure 18. Dynamic DNS Settings.

Enable Dynamic DNS – check the box to enable DDNS.

User name - enter your user name. The router will use it to automatically login to update your IP address in the DDNS server.

Password – enter you login password.

Hostname - enter your hostname which was registered in DDSN server.

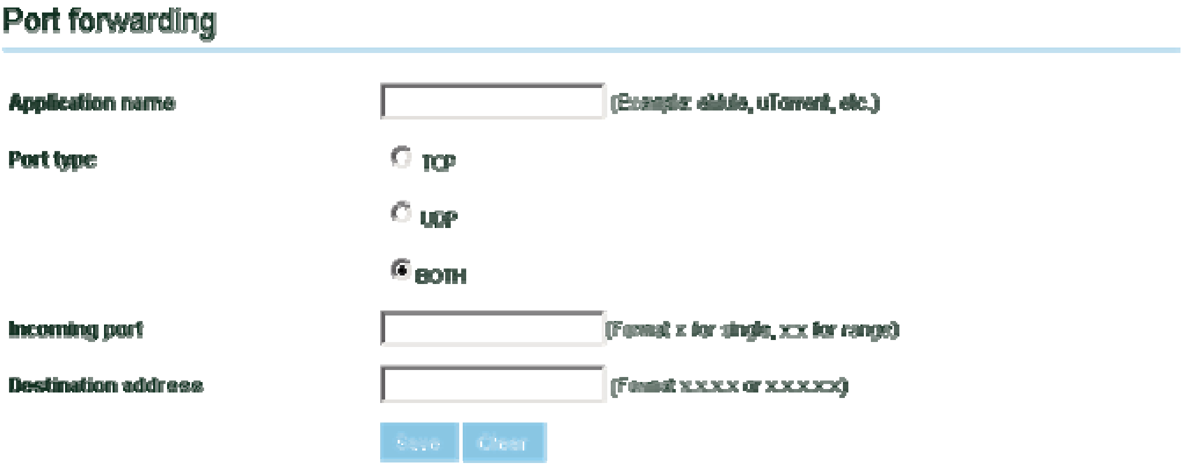
Update period – enter IP address update time in seconds.

DynDNS service type – DYNDNS service type. Allowed service types are:

dyndns.org: dyndns@dyndns.org OR statdns@dyndns.org OR customdns@dyndns.org
freedns.afraid.org: default@freedns.afraid.org
zoneedit.com: default@zoneedit.com
no-ip.com: default@no-ip.com
easydns.com: default@easydns.com
3322.org: dyndns@3322.org

4.6.5 Port forwarding

This section will let to manage port forwarding.



Port forwarding

Application name (Example: aMule, uTorrent, etc.)

Port type ○ TCP ○ UDP ● BOTH

Incoming port (Format x for single, x:x for range)

Destination address (Format x.x.x.x or x.x.x.x:x)

Figure 19. Port forwarding settings.

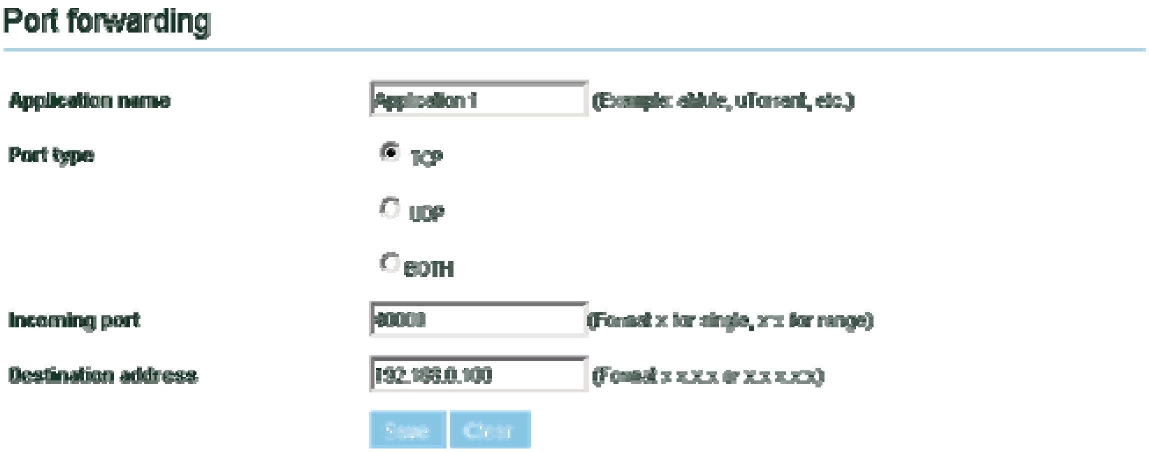
Application name. Set the name of the application.

Port type. Select TCP, UDP, or BOTH

Incoming port. Set incoming port value or range

Destination address Enter the IP address and/or port of the computer on your local network that you want to allow the incoming service to be forwarded.

Example 1: Forward TCP port 40000 to IP address 192.168.0.100



Port forwarding

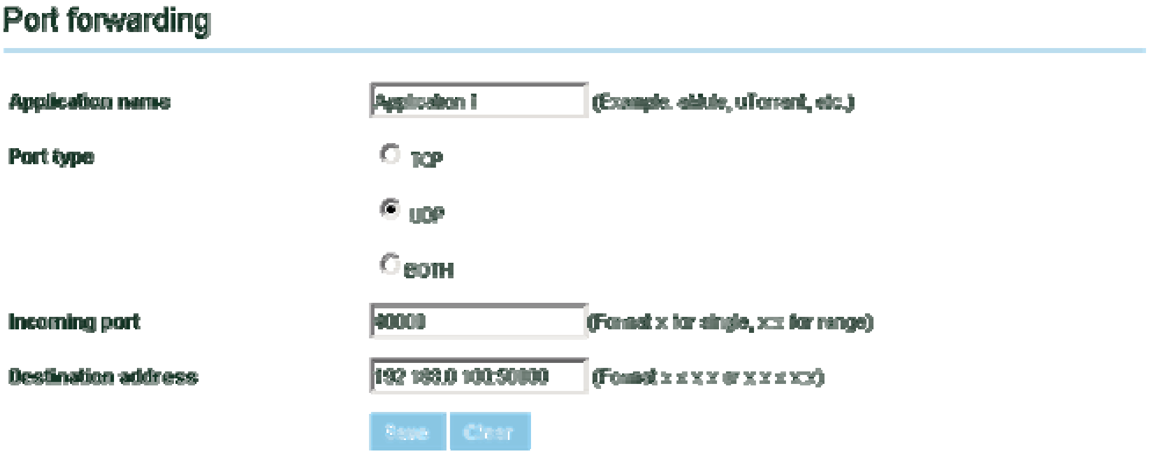
Application name: Application 1 (Example: aMule, uTorrent, etc.)

Port type ● TCP ○ UDP ○ BOTH

Incoming port: 40000 (Format x for single, x:x for range)

Destination address: 192.168.0.100 (Format x.x.x.x or x.x.x.x:x)

Example 2: Forward UDP port 40000 to IP address 192.168.0.100 port 50000.



Port forwarding

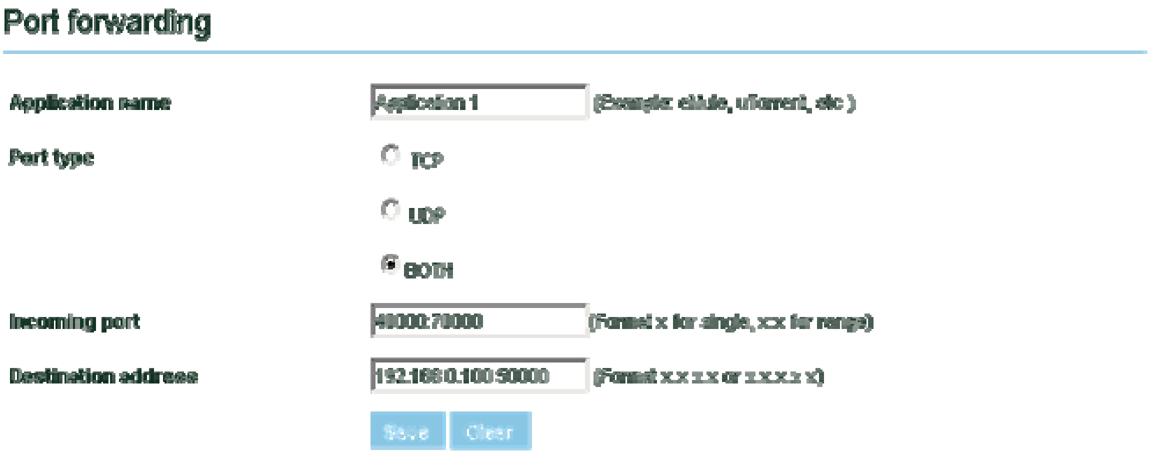
Application name: Application 1 (Example: aMule, uTorrent, etc.)

Port type ○ TCP ● UDP ○ BOTH

Incoming port: 40000 (Format x for single, x:x for range)

Destination address: 192.168.0.100:50000 (Format x.x.x.x or x.x.x.x:x)

Example 3: Forward TCP and UDP ports range 40000 - 70000 to IP address 192.168.0.100 port 50000.

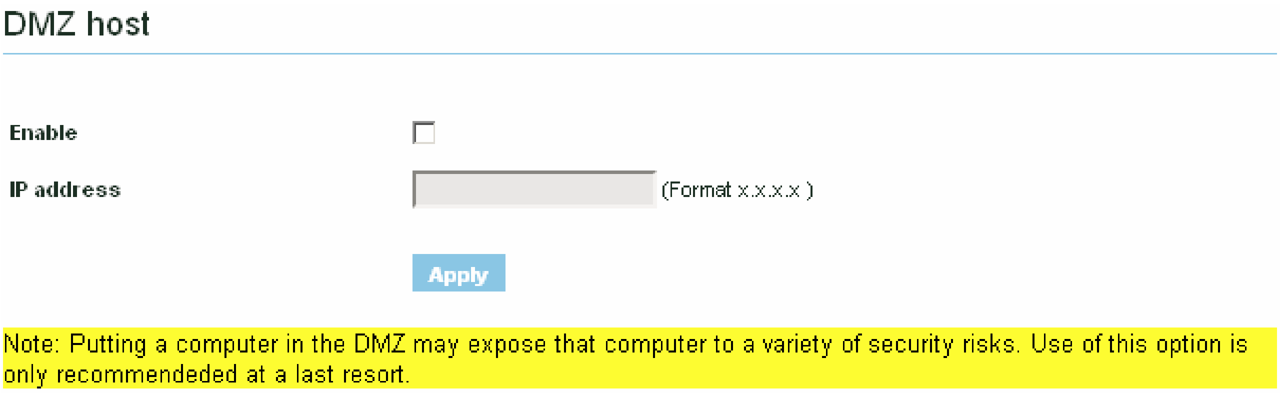


Port forwarding

Application name	Application 1 (Example: eMule, uTorrent, etc)
Port type	○ TCP ○ UDP ● BOTH
Incoming port	40000:70000 (Format x for single, x:x for range)
Destination address	192.168.0.100:50000 (Format x.x.x.x or x.x.x.x:x)

4.6.5.1 DMZ

A DMZ host is not protected by the firewall and may be vulnerable to attack. You should only use this feature when a special application's function fails to make an application work. Designating a DMZ host may also put other computers in the local network at risk. When designating a DMZ host, you must consider the security implications and protect it if necessary.



DMZ host

Enable	□
IP address	(Format x.x.x.x)

Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommendeded at a last resort.

Figure 20. DMZ settings

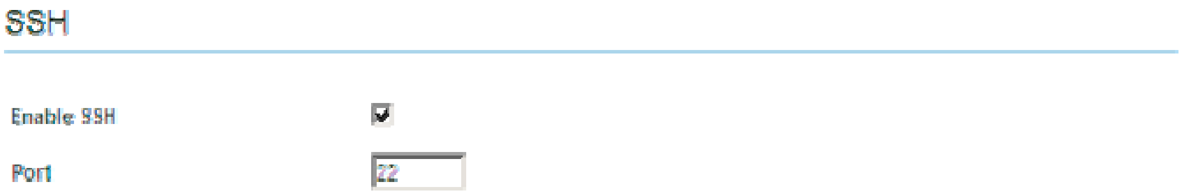
Enable - Click to enable or disable the DMZ.

IP address - Type a host IP address for the DMZ. All remaining incoming packets will be sent to this IP address.

4.6.6 Service

In this section HTTP, SSH services which are important for remote control monitoring and management may be enabled and disabled.

4.6.6.1 SSH



SSH

Enable SSH ☑

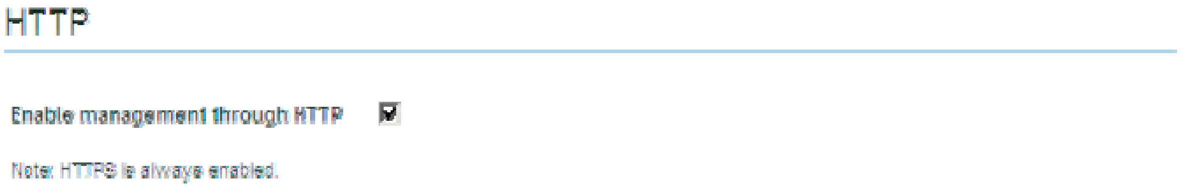
Port 22

Figure 21. SSH service

Enable SSH. Check the box to enable SSH service.

Port. Set port value of the SSH service.

4.6.6.2 HTTP



HTTP

Enable management through HTTP ☑

Note: HTTPS is always enabled.

Figure 22. HTTP service

Enable management trough HTTP. Check the box to enable management though HTTP.

4.7 VPN

4.7.1 OpenVPN (site to site)

OpenVPN site to site graphical user interface (GUI) implementation allows connecting two remote networks via point-to-point encrypted tunnel. OpenVPN implementation offers a cost-effective simply configurable alternative to other VPN technologies. The OpenVPN security model is based on SSL, the industry standard for secure communications via the internet. OpenVPN implementation uses OSI layer 2 secure network extension using the SSL/TLS protocol. The typical VPN site to site implementation using OpenVPN is presented in Figure 23.

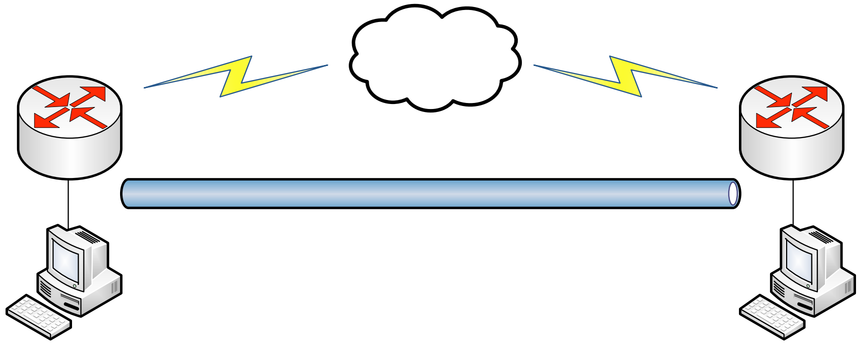
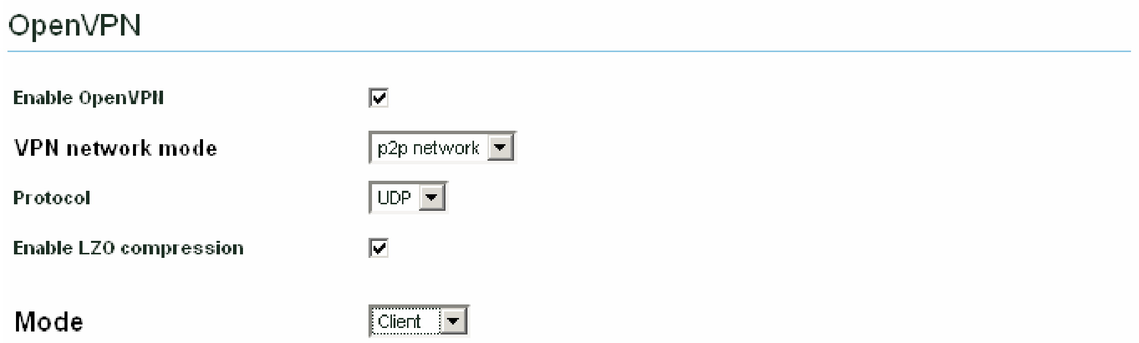


Figure 23. Typical site to site OpenVPN tunnel configuration

Server configuration		Client configuration	
		Remote Endpoint IP	xxx.xxx.xxx.xxx
Local tunnel IP	10.0.0.1	Local tunnel IP	10.0.0.2
Remote tunnel IP	10.0.0.2	Remote tunnel IP	10.0.0.1
Remote network IP	192.168.1.0	Remote network IP	192.168.0.0
Remote network subnet mask	255.255.255.0	Remote network subnet mask	255.255.255.0

The OpenVPN implementation requires server to have public IP or hostname. Also the remote network subnets must be different as in Fig. 23 192.168.0.0/24 and 192.168.1.0/24. If the subnet will be the same tunnel will not be created or may not function correctly due to routing rules.

The server and client have almost the same configuration. The difference in the client configuration is the remote endpoint IP or hostname field. Also the client can set up the keep alive settings. For successful tunnel creation a static key must be generated on one side and the same key must be uploaded on the opposite side.



OpenVPN

Enable OpenVPN ☑

VPN network mode: p2p network

Protocol: UDP

Enable LZO compression ☑

Mode: Client

Figure 24. OpenVPN settings

Enable OpenVPN. Check the box to enable the OpenVPN function.

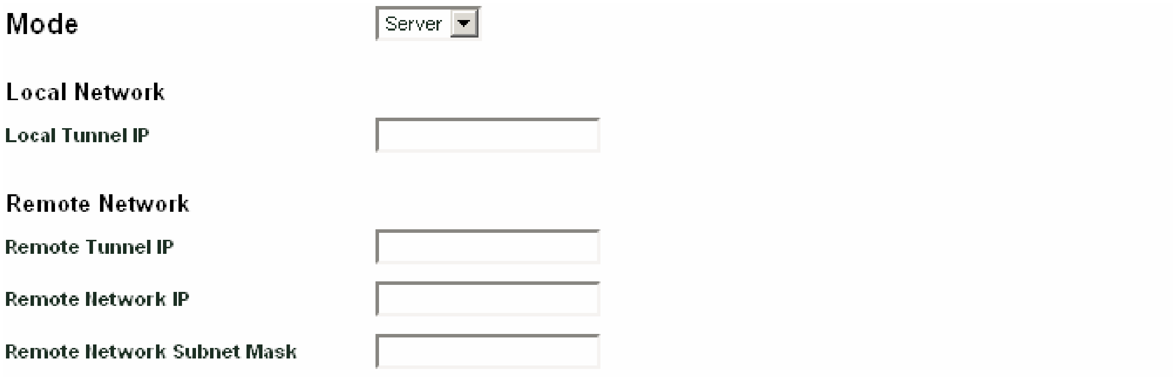
VPN network mode. Select network mode. Currently only p2p configuration is possible.

Protocol - set tunnel protocol (UDP/TCP).

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

Mode – select client or server.

4.7.1.1 Server configuration



Mode Server

Local Network

Local Tunnel IP

Remote Network

Remote Tunnel IP

Remote Network IP

Remote Network Subnet Mask

Figure 25. Server configuration

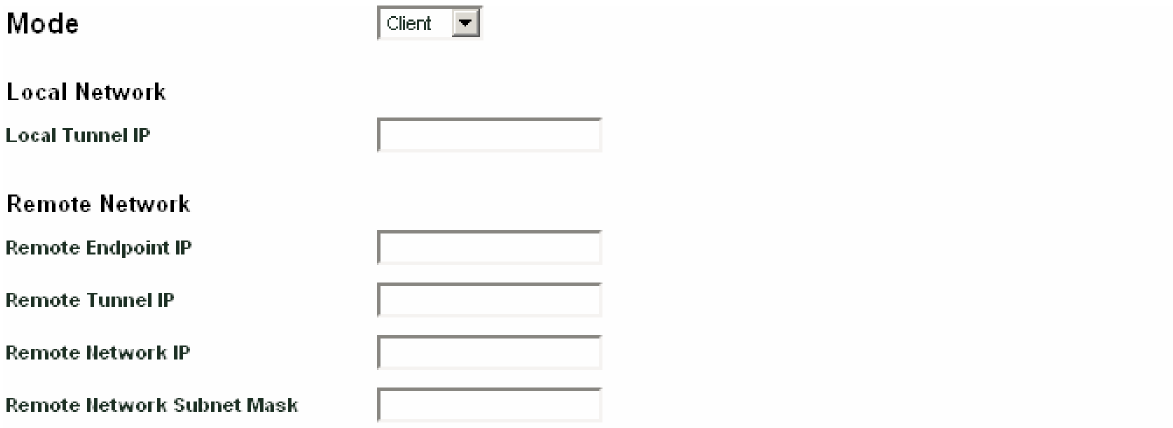
Local network

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

Remote network

Remote tunnel IP – specify the IP address of the remote VPN tunnel endpoint.
Remote network IP – specify the remote network IP.
Remote network subnet mask – specify the remote network subnet mask.

4.7.1.2 Client configuration



Mode Client

Local Network

Local Tunnel IP

Remote Network

Remote Endpoint IP

Remote Tunnel IP

Remote Network IP

Remote Network Subnet Mask

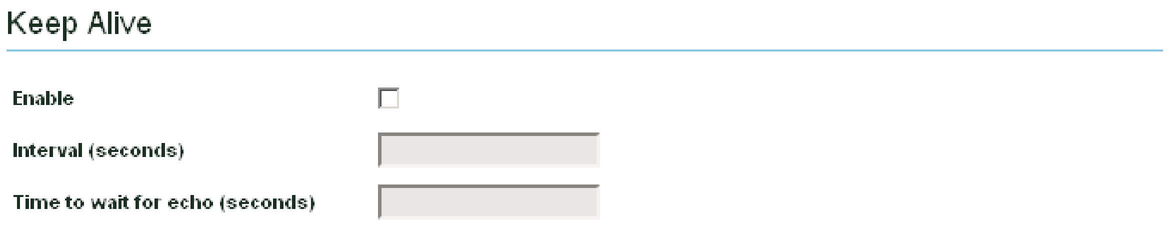
Figure 26. Client configuration

Local network

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

Remote network

Remote Endpoint IP – specify server IP address or hostname.
Remote tunnel IP – specify the IP address of the remote VPN tunnel endpoint.
Remote network IP – specify the remote network IP.
Remote network subnet mask – specify the remote network subnet mask.



Keep Alive

Enable □

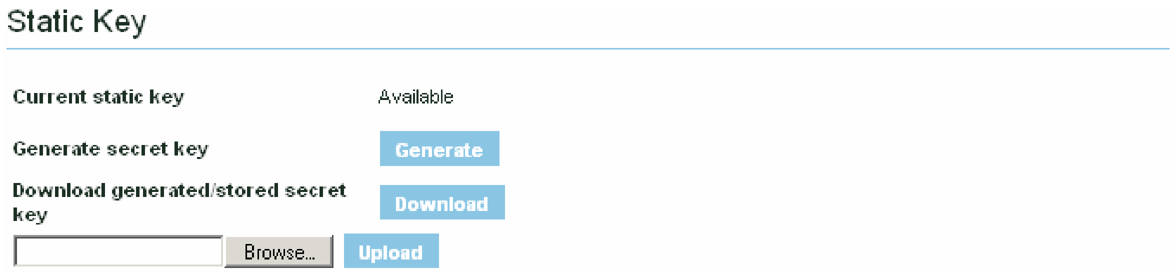
Interval (seconds)

Time to wait for echo (seconds)

Figure 27. Keep alive configuration

Enable Keep request echo messages from the server. If no echo received the tunnel is restarted.

4.7.1.3 Static authentication key



Static Key

Current static key: Available

Generate secret key

Download generated/stored secret key

Figure 28. Client configuration

Static key configurations offer the simplest setup, and are ideal for point-to-point VPNs. The GUI allows to generate, download and upload the static key.

Important! The same key must be uploaded in server and client, e.g. if the key was generated in server, then it must be download by clicking Download , then uploaded in the remote client VPN configuration.

4.7.2 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.

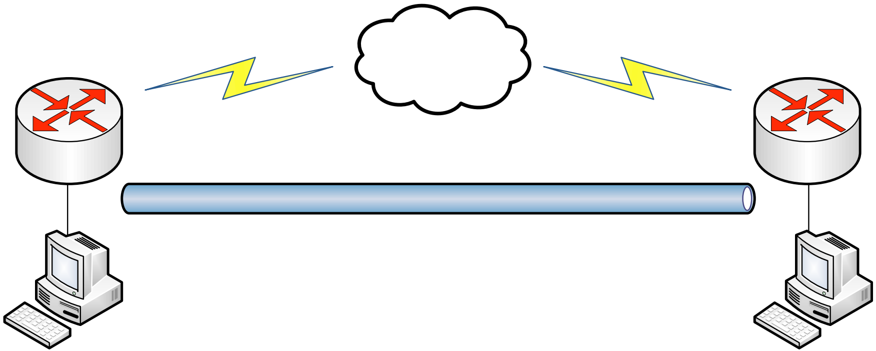
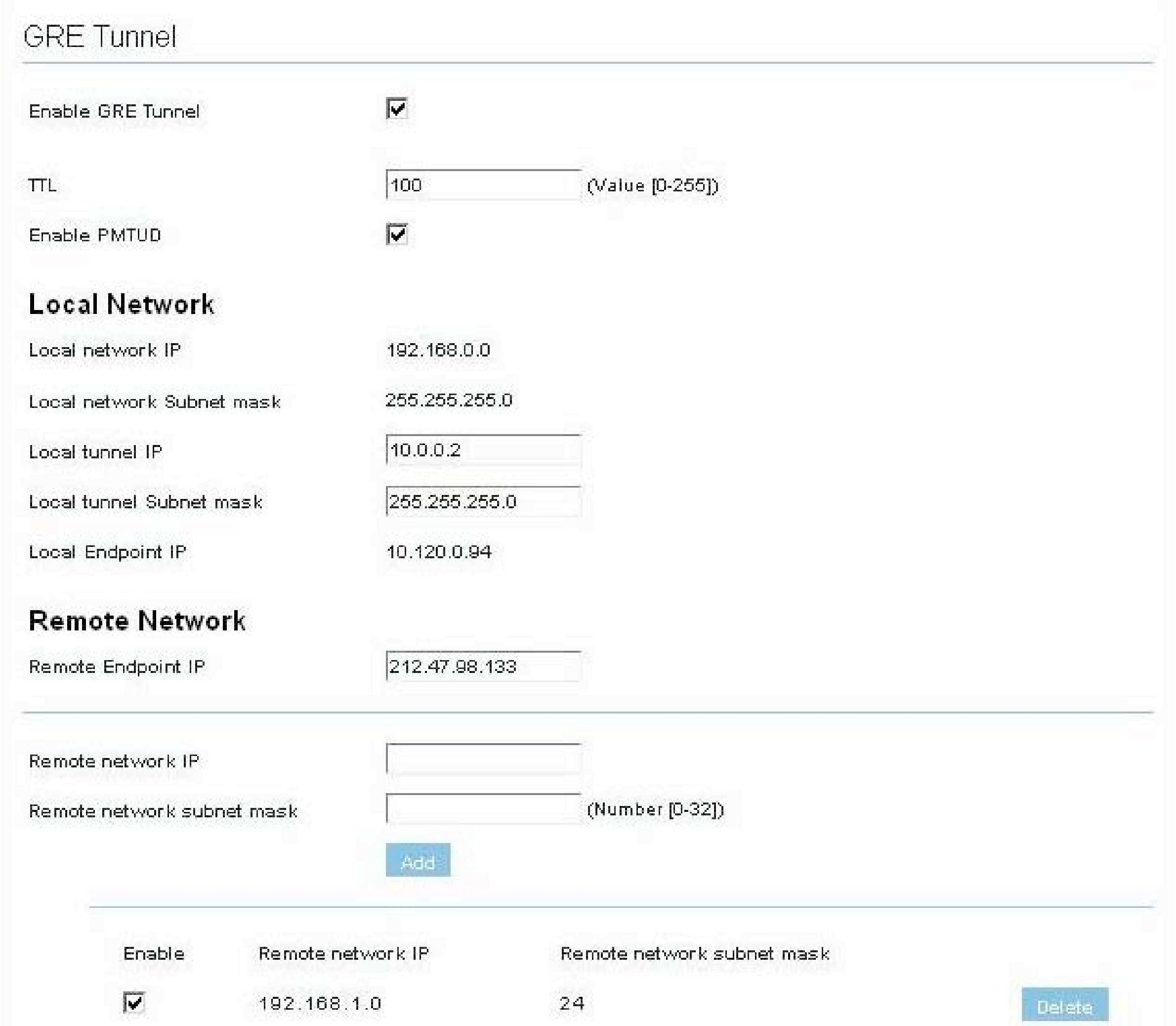


Figure 29. Typical GRE tunnel application connecting two remote networks

In the example network diagram (Fig. 23) 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 (From Fig. 23 A.A.A.A and B.B.B.B).
2. Tunnel local IP address
3. Distant network IP address and Subnet mask



GRE Tunnel

Enable GRE Tunnel ☑

TTL 100 (Value [0-255])

Enable PMTUD ☑

Local Network

Local network IP 192.168.0.0

Local network Subnet mask 255.255.255.0

Local tunnel IP 10.0.0.2

Local tunnel Subnet mask 255.255.255.0

Local Endpoint IP 10.120.0.94

Remote Network

Remote Endpoint IP 212.47.98.133

Remote network IP

Remote network subnet mask (Number [0-32])

Enable	Remote network IP	Remote network subnet mask	
☑	192.168.1.0	24	Delete

Figure 30. GRE tunnel settings

Enable GRE Tunnel. Check the box to enable the GRE Tunnel function.

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. Default: 0.

Enable PMTUD. Check the box to enable the Path Maximum Transmission Unit Discovery (PMTUD) status on this tunnel.

Local Network

Local network IP. Local network IP is taken from network settings. To change it change router IP address mask in the Network settings section (Configuration => Network settings).

Local network Subnet mask. Local network Subnet mask is taken from network settings. To change it change router subnet mask in the Network settings section (Configuration => Network settings).

Local tunnel IP. Specify the fixed local IP address for tunneled packets.

Local tunnel Subnet mask. Specify the subnet mask for the local tunnel.

Local Endpoint IP. Local Endpoint IP is ISP assigned by the ISP provider.

Remote Network

Remote Endpoint IP. Set remote tunnel Endpoint IP.

Remote network IP. Specify remote LAN IP address.

Remote network Subnet mask. Specify remote LAN Subnet mask.

Add – click this button to add configured remote LAN network settings to the router routing table (IP address and subnet mask), so that all packet with destination to the remote LAN would go through the GRE tunnel.

4.7.3 IPsec

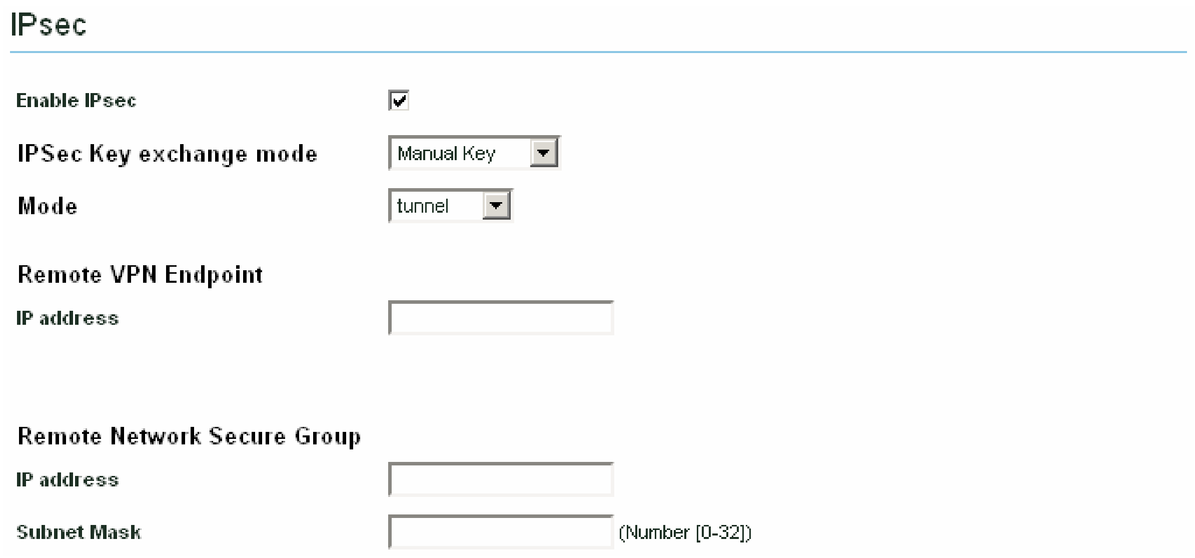
The IPsec protocol client enables the router to establish a secure connection to an IPsec peer via the Internet. IPsec is supported in two modes - transport and tunnel. Transport mode creates secure point to point channel between two hosts. Tunnel mode can be used to build a secure connection between 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 establishes starts establishing tunnel when data from router to remote site over tunnel must be send. For automatic tunnel establishment used tunnel keep alive feature.

4.7.3.1 Manual IPsec Key exchange



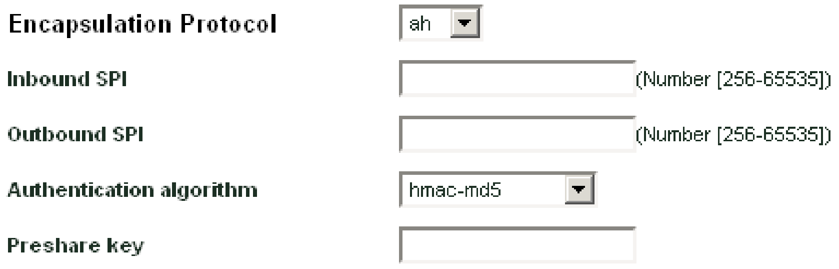
IPsec

Enable IPsec	☑
IPSec Key exchange mode	Manual Key
Mode	tunnel
Remote VPN Endpoint	
IP address	
Remote Network Secure Group	
IP address	
Subnet Mask	(Number [0-32])

Figure 31. Authentication header settings

Mode – select tunnel or transport mode.
Remote VPN Endpoint – set remote IPsec server IP address.
Remote Network Secure Group – Set the remote network (Secure Policy Database) information.

4.7.3.1.1 Authentication header (AH) settings



Encapsulation Protocol	ah
Inbound SPI	(Number [256-65535])
Outbound SPI	(Number [256-65535])
Authentication algorithm	hmac-md5
Preshare key	

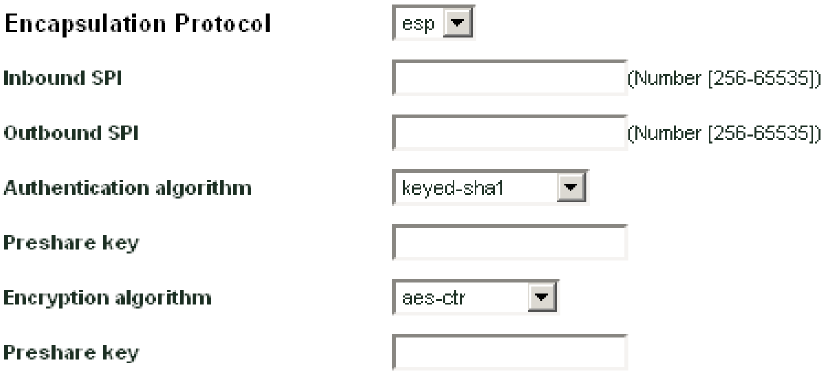
Figure 32. Authentication header settings

Encapsulation Protocol – select encapsulation protocol: Authentication header (AH) or Encapsulating Security Payload (ESP).
Inbound SPI – specify the inbound compression [256-65535].
Outbound SPI – specify the outbound compression [256-65535].
Authentication algorithm – specify the authentication algorithm [Open system/hmac-md5/hmac-sha1/keyed-md5/keyed-sha1/hmac-sha2-256/hmac-sha2-384/hmac-sha2-512/hmac-ripemd160/aes-xcbc-mac].
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. The algorithm key lengths in bits are:

hmac-md5 - 128
hmac-sha1 - 160
keyed-md5 - 128
keyed-sha1 - 160
hmac-sha2-256 - 256
hmac-sha2-384 - 384
hmac-sha2-512 - 512
hmac-ripemd160 - 160
aes-xcbc-mac - 128

4.7.3.1.2 Encapsulating Security Payload (ESP) settings

The ESP protocol provides origin authenticity, integrity, and confidentiality protection of a packet.



Encapsulation Protocol	esp
Inbound SPI	(Number [256-65535])
Outbound SPI	(Number [256-65535])
Authentication algorithm	keyed-sha1
Preshare key	
Encryption algorithm	aes-ctr
Preshare key	

Figure 33. Encapsulating Security Payload (ESP) settings

Encapsulation Protocol – select encapsulation protocol: Authentication header (AH) or Encapsulating Security Payload (ESP).

Inbound SPI – specify the inbound compression [256-65535].

Outbound SPI – specify the outbound compression [256-65535].

Authentication algorithm – specify the authentication algorithm [Open system/hmac-md5/hmac-sha1/keyed-md5/keyed-sha1/hmac-sha2-256/hmac-sha2-384/hmac-sha2-512/hmac-ripemd160/aes-xcbc-mac].

Preshare key – specify the ESP 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. The algorithm key lengths in bits are:

hmac-md5 - 128
hmac-sha1 - 160
keyed-md5 - 128
keyed-sha1 - 160
hmac-sha2-256 - 256
hmac-sha2-384 - 384
hmac-sha2-512 - 512
hmac-ripemd160 - 160
aes-xcbc-mac – 128

Encryption – specify the authentication algorithm [Open system/des-cbc/ blowfish-cbc/ cast128-cbc/des-deriv/3des-deriv/rijndael-cbc/twofish-cbc/aes-ctr].

Preshare key – specify the ESP encryption 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. The algorithm key lengths in bits are:

des-cbc - 64
blowfish-cbc - 40 to 448
cast128-cbc - 40 to 128
des-deriv - 64
3des-deriv - 192
rijndael-cbc -128/192/256
twofish-cbc - 0 to 256
aes-ctr - 160/224/288

4.7.3.2 Auto IKE IPsec Key exchange

Auto IPsec configuration uses the Internet Key Exchange (IKE) for automatically keying IPsec connections.

IKE has two phases:
Phase one - SA for own communication (IKE-SA).
Phase two - IPSec SA establishment.

Note: IKE uses UDP port 500. Make sure that your firewall configuration does not block this port.

During phase one router IKE sends proposals for creating IKE-SA:

1. Hash Algorithm
2. Encryption Algorithm
3. Authentication Methods
4. Diffie-Hellman Group

If proposals do not match IPsec server configuration, then no tunnel will be crated. E.g.

Phase one

Router sent proposals configuration is hardcoded and can not be change. Phase one IKE-SA proposals sent by the router are given below:

Phase one proposal 1

- Pre-shared key authentication
- Aggressive or main mode connection
- AES encryption
- SHA1 hash algorithm
- dh_group 2

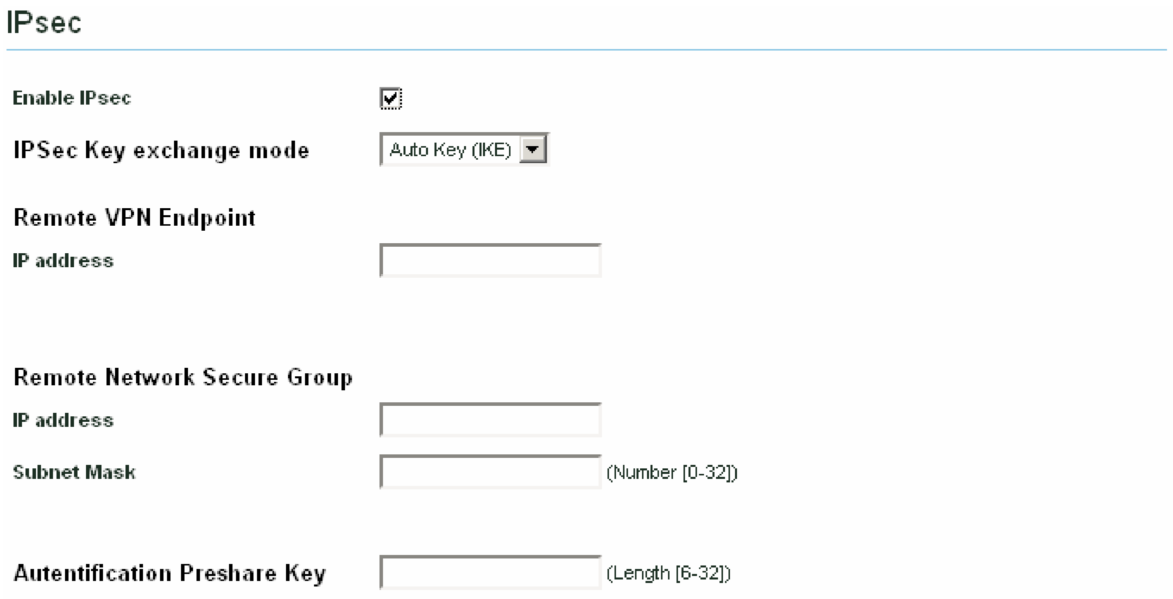
Phase one proposal 2

- Pre-shared key authentication
- Aggressive or main mode connection
- 3DES encryption
- MD5 hash algorithm
- dh_group 2

Phase two

During phase two router supports following configuration:

- PFS group - modp1024 (1024-bit Diffie-Hellman prime modulus group)
- Lifetime time 3600 sec
- Encryption algorithm - aes,3des,des,blowfish
- Authentication algorithm - hmac_sha1,hmac_md5


IPsec

Enable IPsec ☑

IPSec Key exchange mode Auto Key (IKE) ▼

Remote VPN Endpoint

IP address

Remote Network Secure Group

IP address

Subnet Mask (Number [0-32])

Autentification Preshare Key (Length [6-32])

Figure 34. IPsec settings

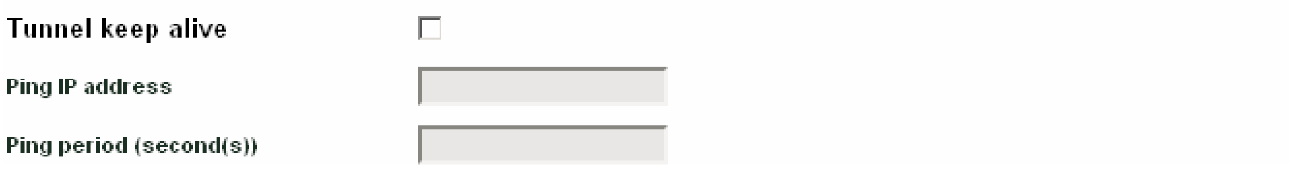
Enable IPsec – Select to enable IPsec feature.
IPsec Key exchange mode – Select Auto Key (IKE)
Remote VPN Endpoint IP address - set remote IPsec server IP address.
Remote Network Secure Group [IP address, Subnet Mask] – Specify the SPD (security policy database) destination IP address and Subnet Mask.
Authentication Preshare Key – Set the IKE preshare key for auto IPsec tunnel negotiation.

Note: The Local VPN Endpoint IP address and Local Network Secure Group are set automatically:

- Local VPN Endpoint IP address – the external IP address assigned by ISP is set
- Local Network Secure Group – router network settings are set (default 192.168.0.0/24)

4.7.3.3 Tunnel keep alive

The tunnel keep alive allows set sending ICMP echo request (ping utility) to the remote tunnel network. This function may be used to automatically start the IPsec tunnel.


Tunnel keep alive □

Ping IP address

Ping period (second(s))

Figure 35. IPsec tunnel keep alive settings

Ping IP address – Enter IP address to which ICMP echo requests will be sent.
Ping period (seconds) – Set sent ICMP request period in seconds.

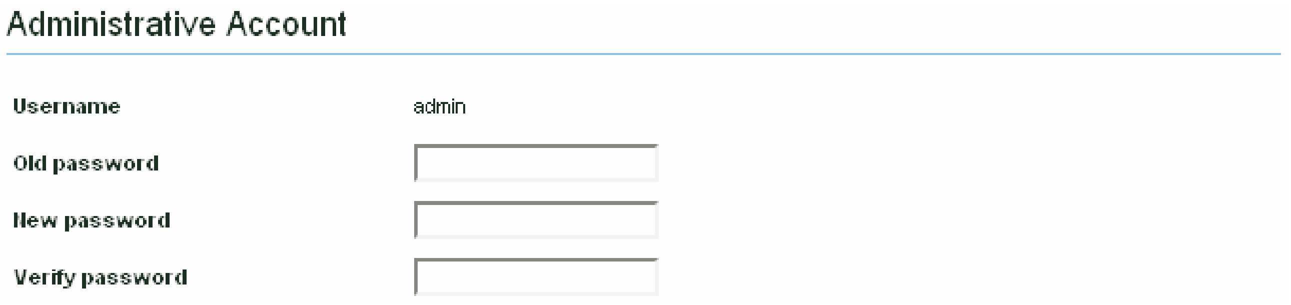
4.8 Admin

Use the **Admin** menu to define access settings to the device, or to use the following system utilities:

- **Account** – change administrator's password.
- **Management** – administrative access settings.
- **Maintenance** – new firmware upgrade, reboot or reset to factory defaults the device.

4.8.1 Account

The Administrative Account menu is used for changing the existing administrators' password.



Administrative Account

Username	admin
Old password	
New password	
Verify password	

Figure 36. Change administrator password

Username – displays the username of the current connected administrator. This parameter is not changeable.

Old password – enter the old administrator password.

New password – enter the new administrator password for user authentication.

Verify password – re-enter the new password to verify its accuracy.

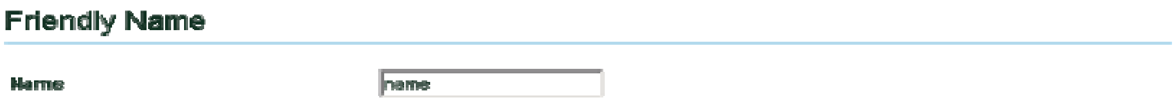
Note: The only way to gain access to the web management if you forget the administrator password is to reset the device factory default settings. Default administrator login settings are:

User Name: **admin**

Password: **admin01**

4.8.2 Management

This section allows configuring device management settings for SNMP and RCMS. Both protocols use same friendly name which is written in the friendly name section.



Friendly Name

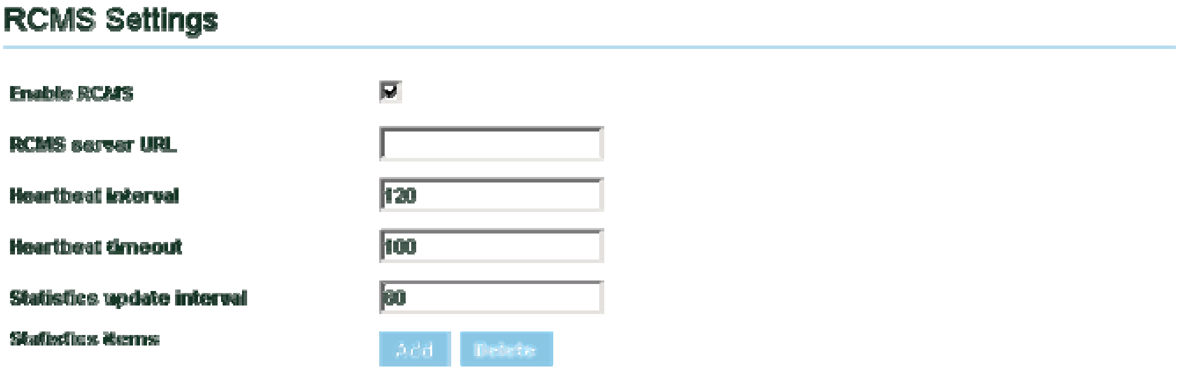
Name	name

Figure 37. Friendly name for SNMP and RCMS

4.8.2.1 RCMS

RCMS is a centralized monitoring and management solution for wireless network equipment. At the heart of RCMS is a powerful and efficient engine that securely gathers, interprets and records information from registered network devices, and makes that information available to network administrators through a convenient, secure, and attractive Web interface to enable RCMS remote control management check the box.

After enabling RCMS setting the following screen should appear.



RCMS Settings

Enable RCMS	☑
RCMS server URL	
Heartbeat interval	120
Heartbeat timeout	100
Statistics update interval	60
Statistics items	Add Delete

Figure 38. RCMS settings

RCMS server URL - specify the URL of the RCMS server to which the heartbeat notifications will be sent.

Heartbeat interval – enter the interval, in seconds, between subsequent heartbeat notifications.

Heartbeat timeout – enter the maximum number of seconds to wait for a response from the RCMS server before considering the connection as having timed out.

Statistics update interval – enter the heartbeat interval, in seconds, between statistics collection.

Statistics items –

Name – specify the name of the statistic.

SNMP OID – specify the local SNMP OID to gather the information from [SNMP OID]. This is used to setup the device to gather a certain statistics of the device and send it to the RCMS server.

Add – click to add a new item of the device statistics.

Delete – click to delete selected statistic items.

4.8.2.2 SNMP

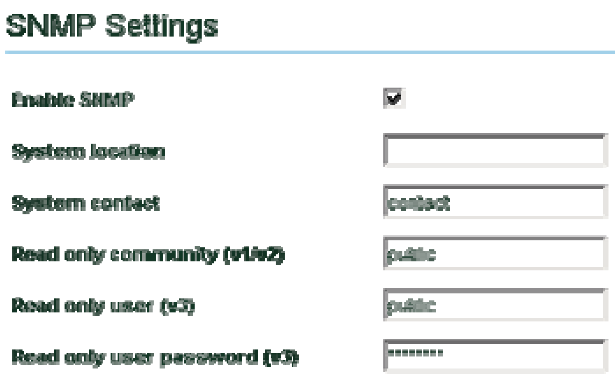
SNMP (Simple Network Management Protocol) allows monitoring the router over a TCP/IP network. SNMP allows network administrators to monitor and manage network performance, find and solve network problems, and plan for network growth.

The router supports the following versions of SNMP:

SNMPv1 – the Simple Network Management Protocol: A Full Internet Standard, defined in RFC1157. (RFC1157 replaces the earlier versions that were published as RFC1067 and RFC1098.) Security is based on community strings.

SNMPv2c – the community-string based Administrative Framework for SNMPv2. SNMPv2c (the "C" stands for "community") is an experimental protocol defined in RFC1901, RFC1905, and RFC1906. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 Classic) and uses the community-based security model of SNMPv1.

SNMPv3 – SNMP v3 is based on version 2 but with added security features. It addresses security requirements through encryption, authentication, and access control rules.



SNMP Settings

Enable SNMP	☑
System location	
System contact	contact
Read only community (v1/v2)	public
Read only user (v3)	public
Read only user password (v3)	********

Figure 39. SNMP settings

Enable SNMP – check the box to enable SNMP service.

System location – specify the physical location of the router [string].

System contact – specify the textual identification of the contact person for the router together with information on how to contact this person [string].

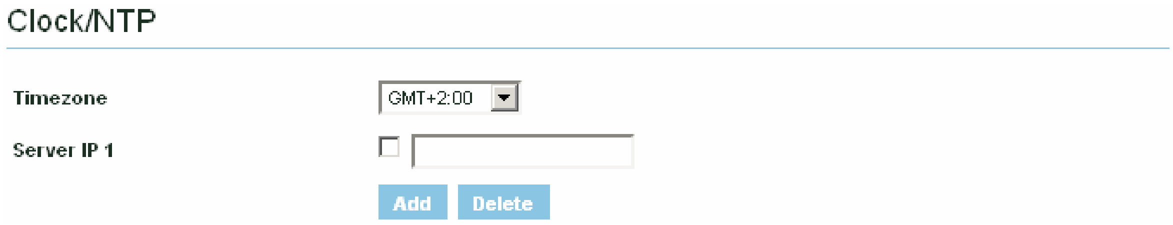
Read only community (v1/v2) – specify the read-only community name for SNMP version 1 and version 2c [string]. The read-only community allows a manager to read values, but denies any attempt to change values.

Read only user (v3) – specify the user name for read-only SNMP version 3 access [string]. The read-only community allows a manager to read values, but denies any attempt to change values.

Read only user password (v3) – specify the password for read-only SNMPv3 access [string].

4.8.2.3 Clock/NTP

Use this section to manage the system time and date on the device automatically, using the Network Time.



Clock/NTP

Timezone	GMT+2:00
Server IP 1	□

Figure 40. Time setting using NTP

To add time server click button **Add**. The new field with server will appear.

Timezone – select the time zone. Time zone should be specified as a difference between local time and GMT time.

Add – click to add NTP server

Delete – click to remove selected NTP servers from the device system.

Server IP – specify the trusted NTP server IP address or hostname for synchronizing time.

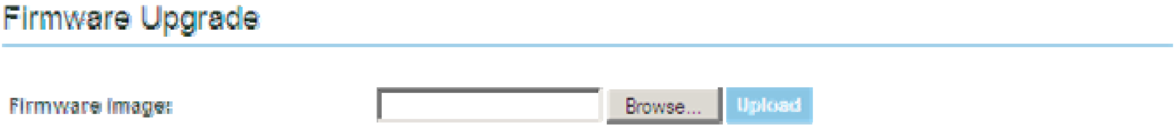
Note: Up to 16 NTP servers can be configured on the router.

4.8.3 Maintenance

Use the **Maintenance** menu to upgrade system firmware, download troubleshoot file, reboot the device or set the device to factory default values.

4.8.3.1 Firmware upgrade

To update your device firmware use the **Firmware** upgrade section, select the firmware file and click the Upload button:


Firmware Upgrade

Firmware image:

Figure 41. Firmware update

Current Firmware Version – displays version of the current firmware.

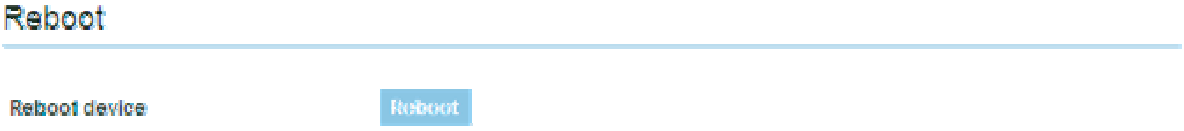
Browse– Click the button to select new image from a folder on the PC.

Upload – Upload the new firmware.

The new firmware image is uploaded to the controller's temporary memory. It is necessary to save the firmware into the controller's permanent memory. Click the **Upgrade** button.

4.8.3.2 Reboot

Use the **Reboot** section to reboot the device:

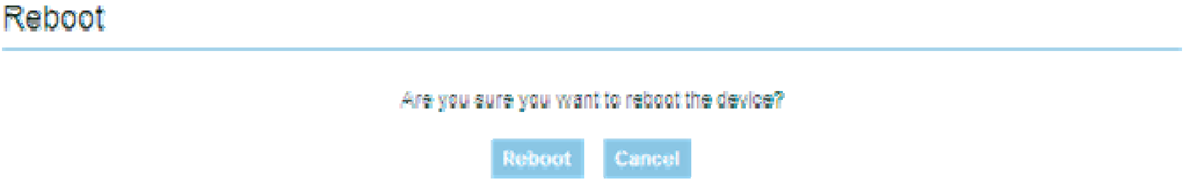

Reboot

Reboot device

Figure 42 . Reboot Device

Reboot. Reboot device with the last saved configuration.

After clicking the **Reboot** button, the confirmation message appears:


Reboot

Are you sure you want to reboot the device?

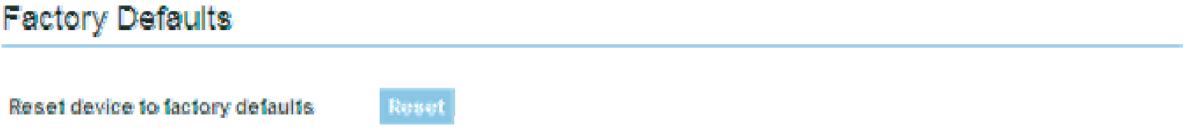
Figure 43. Reboot Confirmation

Reboot. Click to finish the device reboot process.

Cancel. Do not reboot the device.

4.8.3.3 Factory Defaults

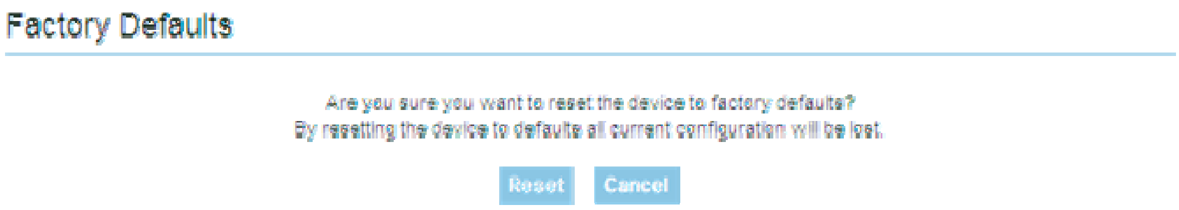
Use the **Factory Defaults** menu to reset device parameters into factory defaults:


Factory Defaults

Reset device to factory defaults

Figure 44. Resetting Device to Factory Defaults

After clicking the **Reset** button, the confirmation message appears:


Factory Defaults

Are you sure you want to reset the device to factory defaults?
By resetting the device to defaults all current configuration will be lost.

Figure 45. Reset to Factory Defaults Confirmation

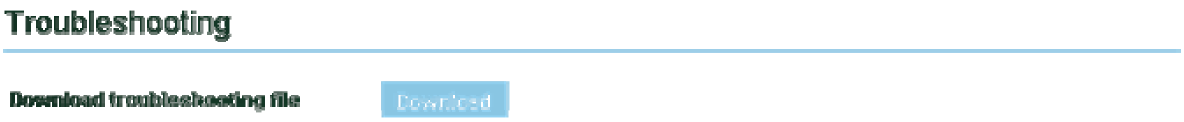
Reset. Click to reset the device to factory default values.

Cancel. Click to cancel reset process.

Note: Resetting the device is an irreversible process. Current configuration and the administrator password will be set back to the factory default.

4.8.3.4 Troubleshooting file download

If there are any problems with router the troubleshoot file may be downloaded. It contains router configuration information, messages and troubleshoot data.


Troubleshooting

Download troubleshooting file

Figure 46. Troubleshoot file download

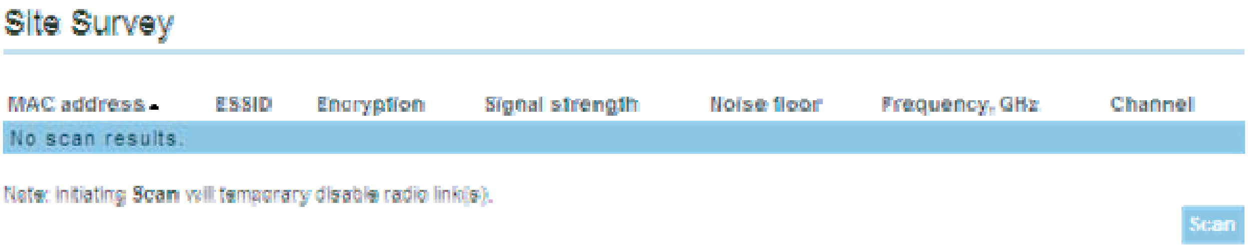
4.9 Tools

4.9.1 Site Survey

The Site Survey test shows overview information for wireless networks in a local geographic area. Using this test, an administrator can scan for working access points, check their operating channels, encryption and see signal/noise levels. An administrator can use this feature to identify a clear channel to set the device.

Note: Note that Site Survey function can take several minutes to perform.

A Site Survey test is performed every time on the startup of the device, therefore the results of the last performed Site Survey test and its time can be found on the page. Thus, to obtain the results, the initiation of the scan is not necessary. To perform the Site Survey test currently, click the **Scan** button:



Site Survey

MAC address ▴	ESSID	Encryption	Signal strength	Noise floor	Frequency, GHz	Channel
No scan results.						

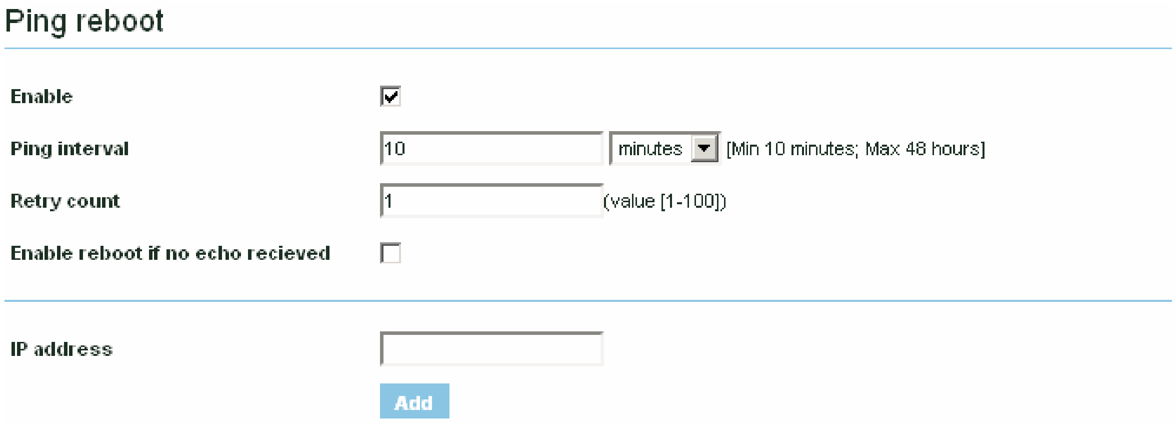
Note: initiating Scan will temporary disable radio link(s).

Figure 47. Site Survey Table

Note: The Site Survey function is impossible if the selected wireless interface is disabled.

4.9.2 Ping Reboot

The Ping Reboot feature allows rebooting the router if the connection to GSM network is lost. This feature checks (using ICMP echo request, like ping utility) if specific hosts are accessible on the network. Function allows adding several host IP addresses. When at least one server does not respond the router is rebooted if the check box "Enable reboot if no echo received".



Ping reboot

Enable	☑
Ping interval	10 minutes ▾ [Min 10 minutes; Max 48 hours]
Retry count	1 (value [1-100])
Enable reboot if no echo recieved	□
IP address	

Figure 48. Site Survey Table

Enable – check the box to enable Ping Reboot feature.

Ping interval – specify the monitoring time period in seconds

Retry count – specify the number of failed reach ability checks

Enable reboot if no echo received– enable reboot the router if no echo to sent ICMP requests is received.

IP address – Set the host IP address to which ICMP requests will be sent.

Add – Click to add host IP.

5 TECHNICAL SPECIFICATION

Wireless IEEE 802.11 network

Standards

IEEE 802.11b: 11Mbps, 5.5Mbps, 2Mbps, 1Mbps

IEEE 802.11g: 54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps, 6Mbps, automatically fall back to 5.5Mbps, 2Mbps, 1Mbps

Transmitter output power at antenna connector

IEEE 802.11b:	1-11Mbps	20dBm
IEEE 802.11g:	6-24Mbps	20dBm
	36Mbps	19dBm
	48Mbps	17dBm
	54Mbps	16dBm

Receiver sensitivity at antenna connector

IEEE 802.11b:	-92 dBm @ 1Mbps
	-87 dBm @ 11Mbps
IEEE 802.11g:	-90 dBm @ 6Mbps
	-70 dBm @ 54Mbps

Security

WPA/WPA2, WEP 64/128 bit, 802.1x authentication

Wireless Frequency Range

2.412GHz to 2.484GHz

External Antenna Type

Detachable reverse SMA

Management

User-friendly Web GUI

Wired and wireless network status.

Site survey test.

Traffic monitoring.

Firmware upgradeable.

SNMP, SSH, RCMS

VPN

IPsec pass through, GRE Tunnel pass through

GRE tunnel, IPsec client

HSUPA/HSDPA/UMTS
850/1900/2100 MHz or 900/2100 MHz or 1900/2100/AWS MHz

HSUPA mode: 2.0: category 5
HSDPA 7.2: Categories 7 and 8
HSDPA 3.6: Categories 5 and 6
HSDPA 1.8: Categories 1-4, 11 and 12
UMTS: 384 Kbps operation in downlink, 384 Kbps in uplink

EDGE 850/900/1800/1900 MHz

GSM Power Class 4 (2W) for 850/900 bands.
GSM Power Class 1 (1W) for 1800/1900 bands.
EDGE class E2 (+27 dBm in 850/900 bands, +26 dBm in 1800/1900 bands).
GPRS/EGPRS Multislot Class 12 (4 slots Rx, 4 slots Tx).
GPRS/EGPRS Class B Type 1 MT.
GPRS CS1-CS4; EGPRS MCS1-MCS9.

Electrical characteristics

Nominal power supply voltage	**9V**	**12V**	**21V**
Current Consumption when idle	⎓ **600mA**	⎓ **350mA**	⎓ **300mA**
Current Consumption when operating	⎓ **980mA**	⎓ **520mA**	⎓ **400mA**

Temperature & Humidity
Operation 0˚ to 55˚ C
Humidity 5% to 95% (non-condensing)
Transit/Storage -40˚ to 85˚ C

LEDS
Power
Mobile Network Activity
LAN Activity

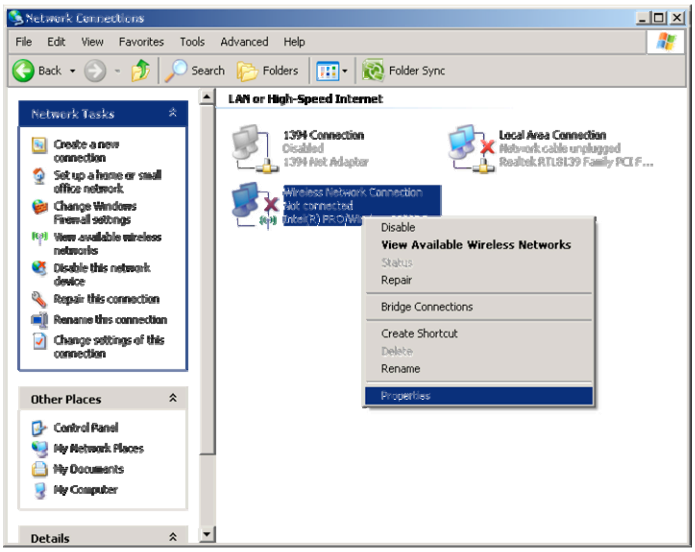
Host Operating System
Microsoft Windows® 98SE/ME/NT4.0/2000/XP, Unix, Linux and MacOS

Dimensions
L = 100mm
W = 85mm
H = 36mm

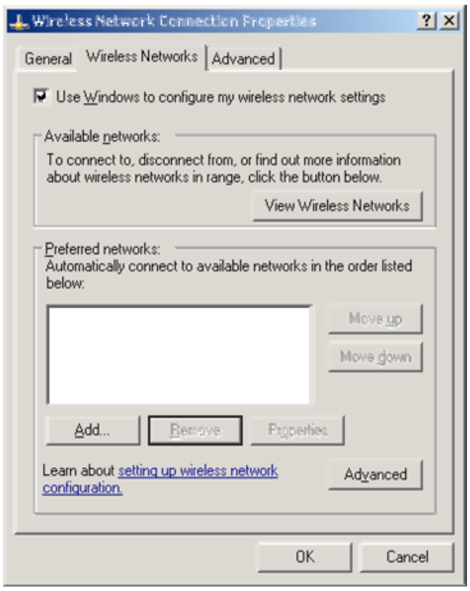
Weight
230g

6 Appendix A Configuring PC wireless security

1. Click **Start** => **Settings** => **Control Panel** (The Control Panel should be in **Classic view**). Double click on the **Network Connections** icon.
2. Right click on the **Local Area Connection** for wired or **Wireless Network Connection** for wireless connection and select **Properties**.



3. In the tab **General** Scroll down to **Internet Protocol (TCP/IP)** and press **Properties.**
4. Select **Obtain IP address automatically** and **Obtain DNS server address automatically** if they are not selected.
5. Click **OK** to close Internet Protocol (TCP/IP) properties.
6. Choose **Wireless Networks** tab. Make sure that box **Use Windows to configure my wireless network settings** is checked and Click **View Wireless Networks**



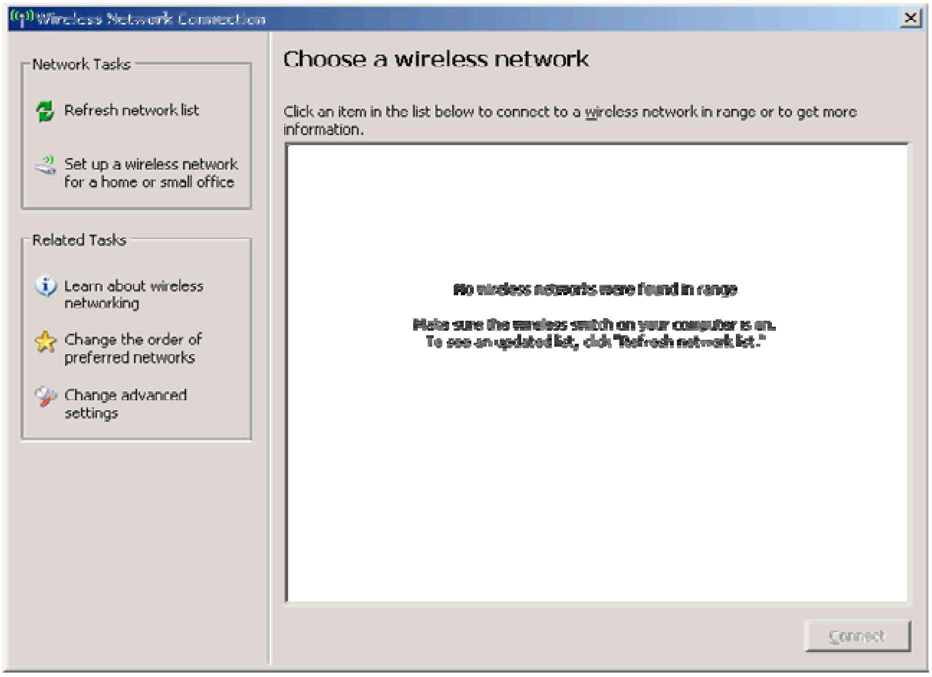
☑ Use Windows to configure my wireless network settings

Available networks:
To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

Preferred networks:
Automatically connect to available networks in the order listed below:

Learn about setting up wireless network configuration.

7. Click **Refresh network list**


Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

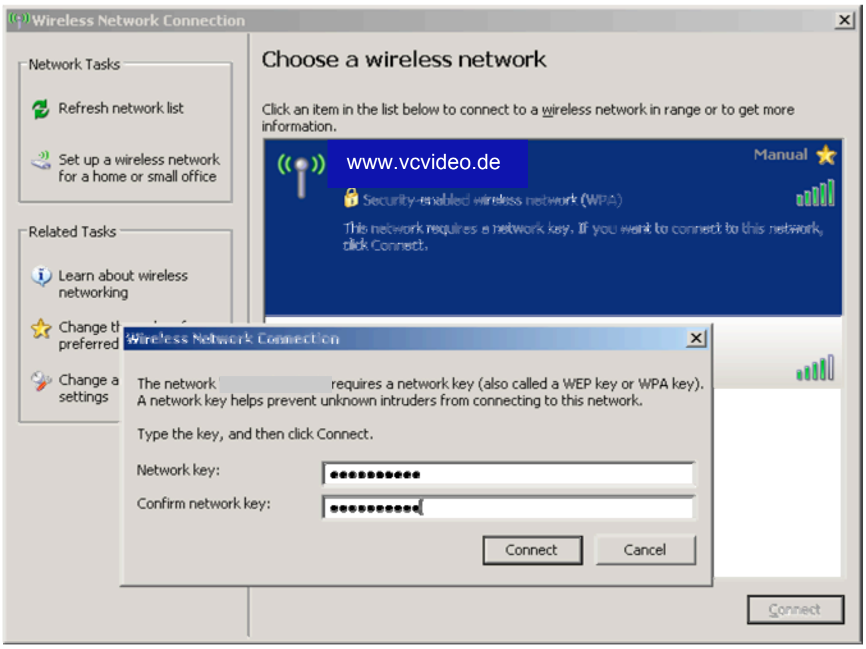
Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

No wireless networks were found in range

Make sure the wireless switch on your computer is on.
To see an updated list, click "Refresh network list."

8. Choose the network with SSID witch was configured on the router (default www.teletonika.lt) and click connect. The window asking for the key should appear. The **Network key** is the **passphrase** which was typed in the router settings.



Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Security-enabled wireless network (WPA)

This network requires a network key. If you want to connect to this network, click Connect.

Wireless Network Connection

The network requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

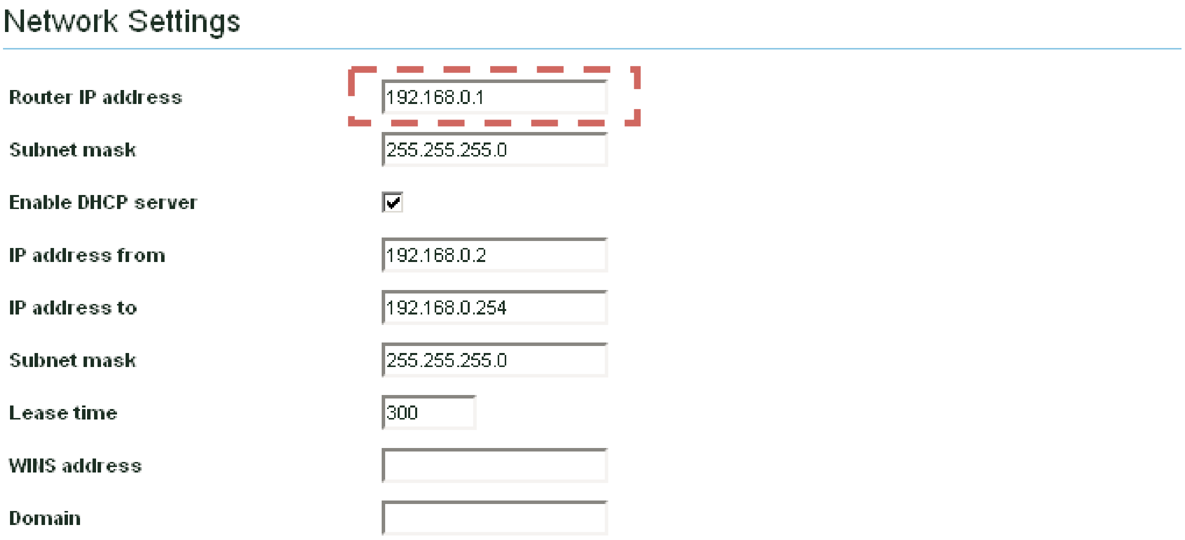
Network key: ●●●●●●●●●●●

Confirm network key: ●●●●●●●●●●●

7 Appendix B Changing router IP address

Step 1 Connect to router WEB configuration page. Then go **CONFIGURATION** then **Maintenance**.

Step 2 Change router IP address:
In the field **Router IP address** write new router address. (eg. 192.168.123.1)

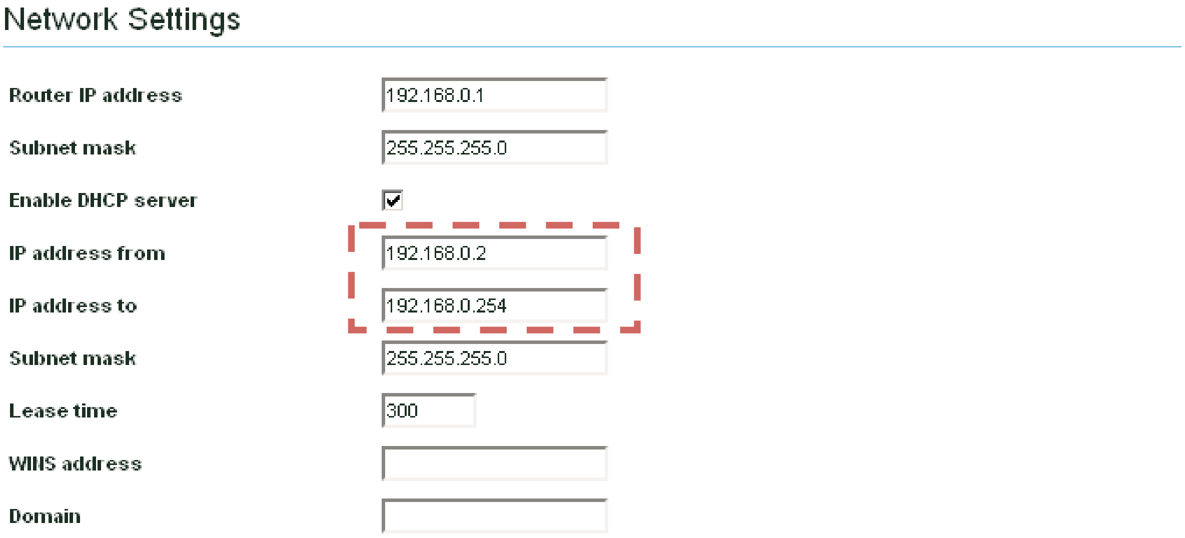


Network Settings

Router IP address	192.168.0.1
Subnet mask	255.255.255.0
Enable DHCP server	☑
IP address from	192.168.0.2
IP address to	192.168.0.254
Subnet mask	255.255.255.0
Lease time	300
WINS address	
Domain	

Step 2 Change router DHCP server assigned IP address range:
Type the fields **IP address from** and **IP address to** type new range
Example:

Router IP address:	192.168.123.1
IP address from:	192.168.123.2
IP address to:	192.168.123.254



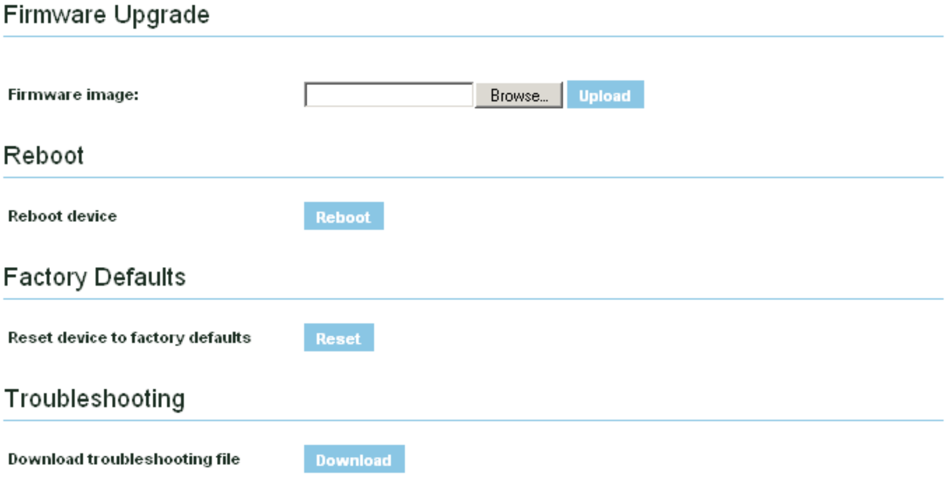
Network Settings

Router IP address	192.168.0.1
Subnet mask	255.255.255.0
Enable DHCP server	☑
IP address from	192.168.0.2
IP address to	192.168.0.254
Subnet mask	255.255.255.0
Lease time	300
WINS address	
Domain	

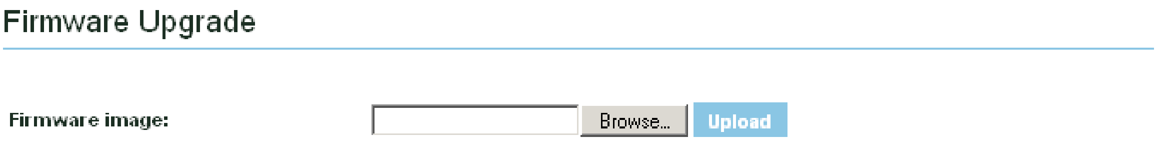
Step 3 Reboot the router.

8 Appendix C Updating router firmware

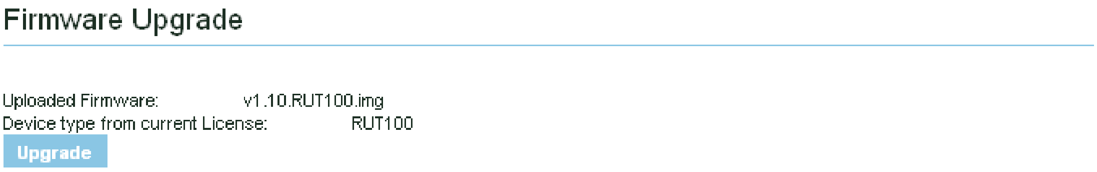
Step 1 Connect to router WEB configuration page. Then go **ADMIN then Maintenance** to upgrade system firmware.



Step 2 To update your device firmware click **Browse** button to select the new image from a folder on the PC and click the **Upload** button:



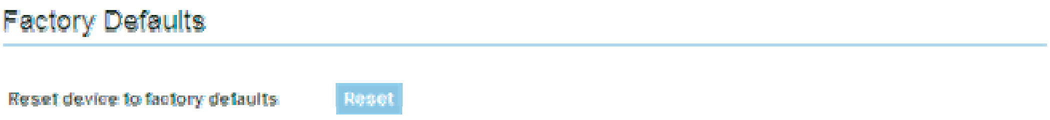
Step 3 When the new firmware image is uploaded to the router's temporary memory it is necessary to save the firmware into the router's permanent memory. Click the **Upgrade** button.



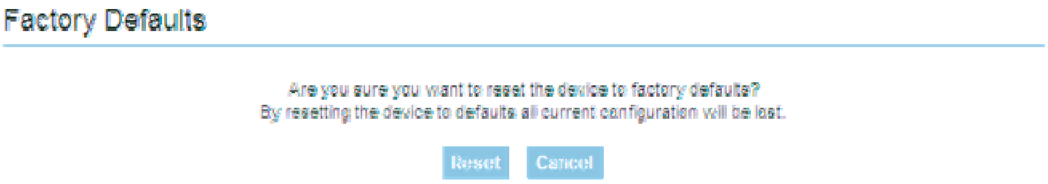
Uploaded Firmware: v1.10.RUT100.img
Device type from current License: RUT100

During the upgrade the router will reboot. Overall process takes several minutes.

Step 4 After the router is rebooted it is required to reset router to defaults. To do that connect to router WEB configuration page. Then go **ADMIN**, **Maintenance** and use the **Factory Defaults** menu to reset device parameters into factory defaults



After clicking the **Reset** button, the confirmation message appears:



Are you sure you want to reset the device to factory defaults?
By resetting the device to defaults all current configuration will be lost.

Click to **Reset** the device to factory default values.

9 Appendix D Accessing from the WEB

There are two ways to connect the router from internet:

1. Using SIM card with public static IP address
2. Using SIM card with public dynamic IP address witch will be linked to static hostname using DDNS service.

Note: If the SIM card is with private IP address then reaching camera from the internet is not possible as connection is routed through a NAT firewall in your provider's network.

SIM card with public static IP address

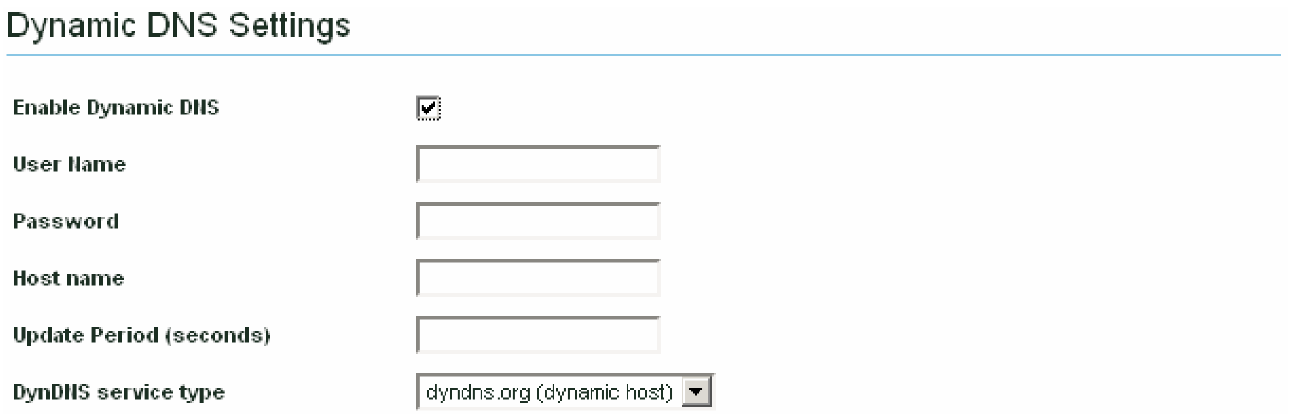
Open your WEB browser and type SIM card IP address, when the camera GSM connection has been set up. After successful connection router's login page must appear.

SIM card with public dynamic IP address

For the SIM card with dynamic public IP address the IP address is given for a limited period of time, which is usually no more than a few hours, then the IP address is changed. As he IP address is continuously changed it becomes a problem to connect to the camera. To solve this problem Dynamic Domain Name Service (DDNS) may be used. DDNS is a domain name service allowing to link dynamic IP addresses to static hostname.

To start using this feature firstly a hostname must be registered on the DDNS server. After creating account you will get: Hostname Username and Password.

To link router's IP address to the static hostname, Dynamic DNS settings must be configured. To configure DDNS connect to the router WEB configuration page, go the **Configuration** => **Dynamic DNS Settings** (Refer to Figure below).



Dynamic DNS Settings

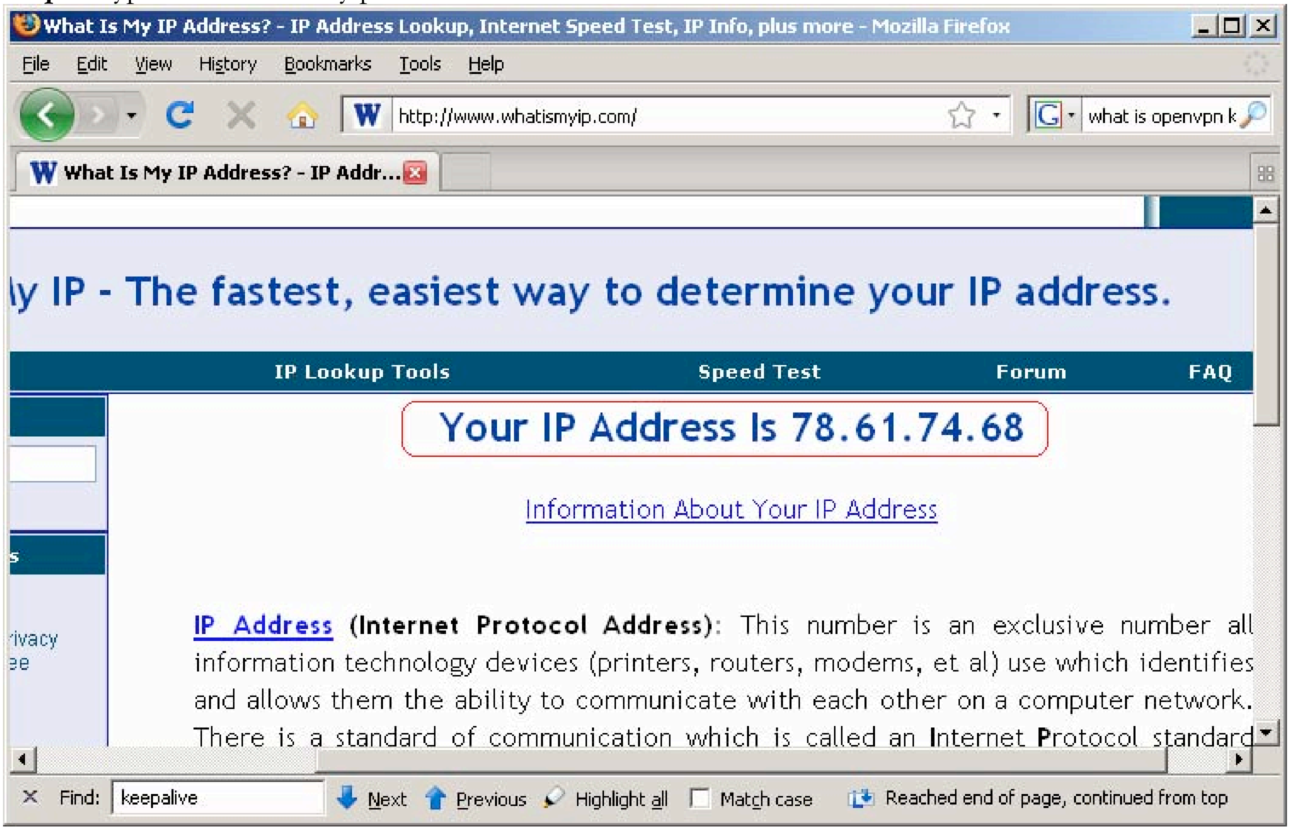
Enable Dynamic DNS	☑
User Name	
Password	
Host name	
Update Period (seconds)	
DynDNS service type	dyndns.org (dynamic host)

Check the **Enable** check box. Enter username, password and hostname which where got from the DDNS server provider. In the Update period field enter the IP address update interval. Select the DDNS service provider from the DynDNS service type list. After setting DDNS settings press **Save** button, then press reboot to start router with new settings.

10 Appendix E SIM card public or private IP address

Step 1 Connect PC to router and check if it is possible to browse Internet.
If you are not able then there is problem with MOBILE NETWORK SETTINGS. If you are able then go to next step.

Step 2 Type www.whatismyip.com in the web browser and write down the red marked IP address.


What Is My IP Address? - IP Address Lookup, Internet Speed Test, IP Info, plus more - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.whatismyip.com/
what is openvpn k
What Is My IP Address? - IP Addr...
IP Lookup Tools
Speed Test
Forum
FAQ
Find: keepalive
Next
Previous
Highlight all
Match case
Reached end of page, continued from top

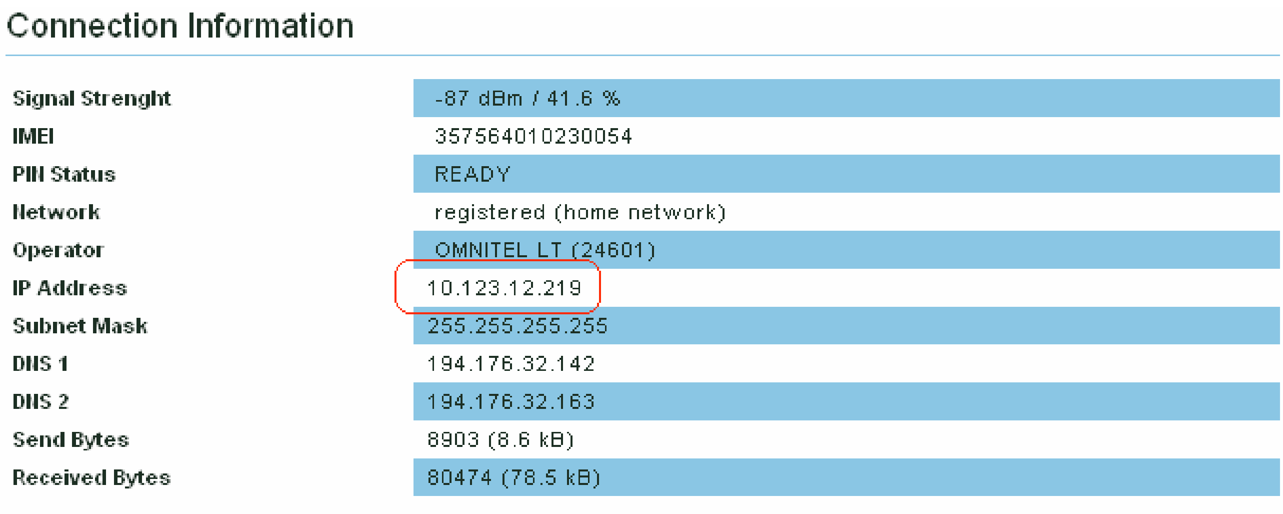
ly IP - The fastest, easiest way to determine your IP address.

Your IP Address Is 78.61.74.68

Information About Your IP Address

IP Address (Internet Protocol Address): This number is an exclusive number all information technology devices (printers, routers, modems, et al) use which identifies and allows them the ability to communicate with each other on a computer network. There is a standard of communication which is called an Internet Protocol standard

Step 3 Connect to router web configuration tool and then go STATUS – System Information and write down the marked IP address.



Connection Information

Signal Strenght	-87 dBm / 41.6 %
IMEI	357564010230054
PIN Status	READY
Network	registered (home network)
Operator	OMNITEL LT (24601)
IP Address	10.123.12.219
Subnet Mask	255.255.255.255
DNS 1	194.176.32.142
DNS 2	194.176.32.163
Send Bytes	8903 (8.6 kB)
Received Bytes	80474 (78.5 kB)

Step 4 Compare the IP addresses in step 2 and 3. If they are the same then SIM card is with public IP address, if they are different SIM card is with private IP address.

VC Videocomponents GmbH
Brachenfelder Str. 45
D-24534 Neumünster
Tel.: ++ 49 (0) 4321 - 39 05 40
Fax: ++ 49 (0) 4321 - 28 04 82
e-mail: mail@vcvideo.de
Internet: www.vcvideo.de

Service
Tel.: ++ 49 (0) 4321 - 3 90 54 33
e-mail: technik@vcvideo.de