iRZ® automation

GSM router iRZ RCA CDMA 450

USER MANUAL

List of contents

1. Safety requirements

Restrictions on the device use near other electronic devices:

- Turn off the router in hospitals or near medical equipment (such as pacemakers and hearing aids). The interference with medical equipment is possible;
- Turn off the router in planes. Take precautions against accidental activation;
- Turn off the router near gas stations, chemical plants, blasting works. The interference with technical equipment is possible;
- The router may cause interference with TVs and radios at close distance.

Protect your router from dust and moisture.

Improper use deprives you of all warranty claims.

2. General

2.1.Purpose of the device

GSM router iRZ RCA, using the technology of CDMA (data transfer rate up to 2.4 Mbps), provides reliable high-speed Internet access for individual devices or entire network. It can be used for any distributed business, which requires transmission of large amounts of information - Internet access for computers and networks, vending machines and ATMs, industrial equipment, security systems and surveillance, as well as for remote monitoring and control.

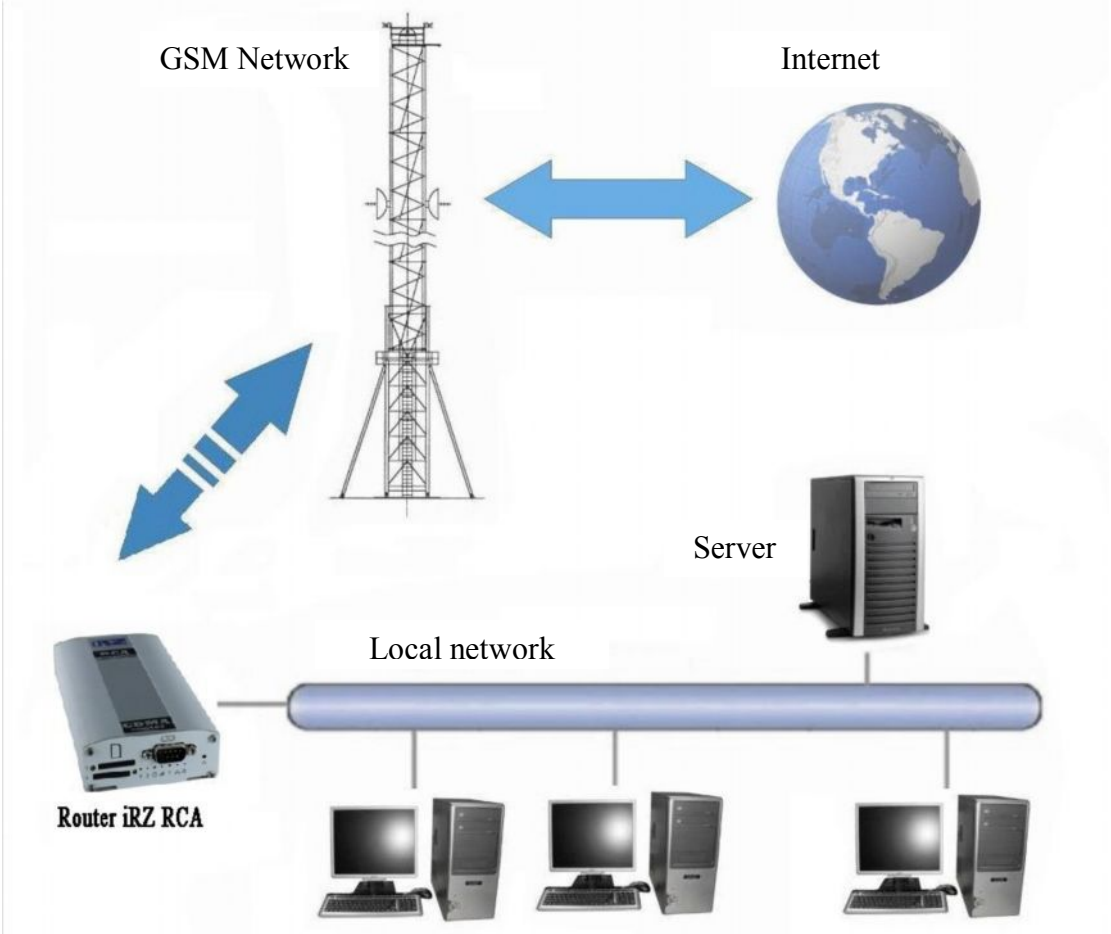
High productivity of the platform and availability of two R-UIM card slots make it possible for the device to solve additional tasks without compromising the quality of the core functions.

The device runs on Linux operational system. LEDs are used to display the router work.

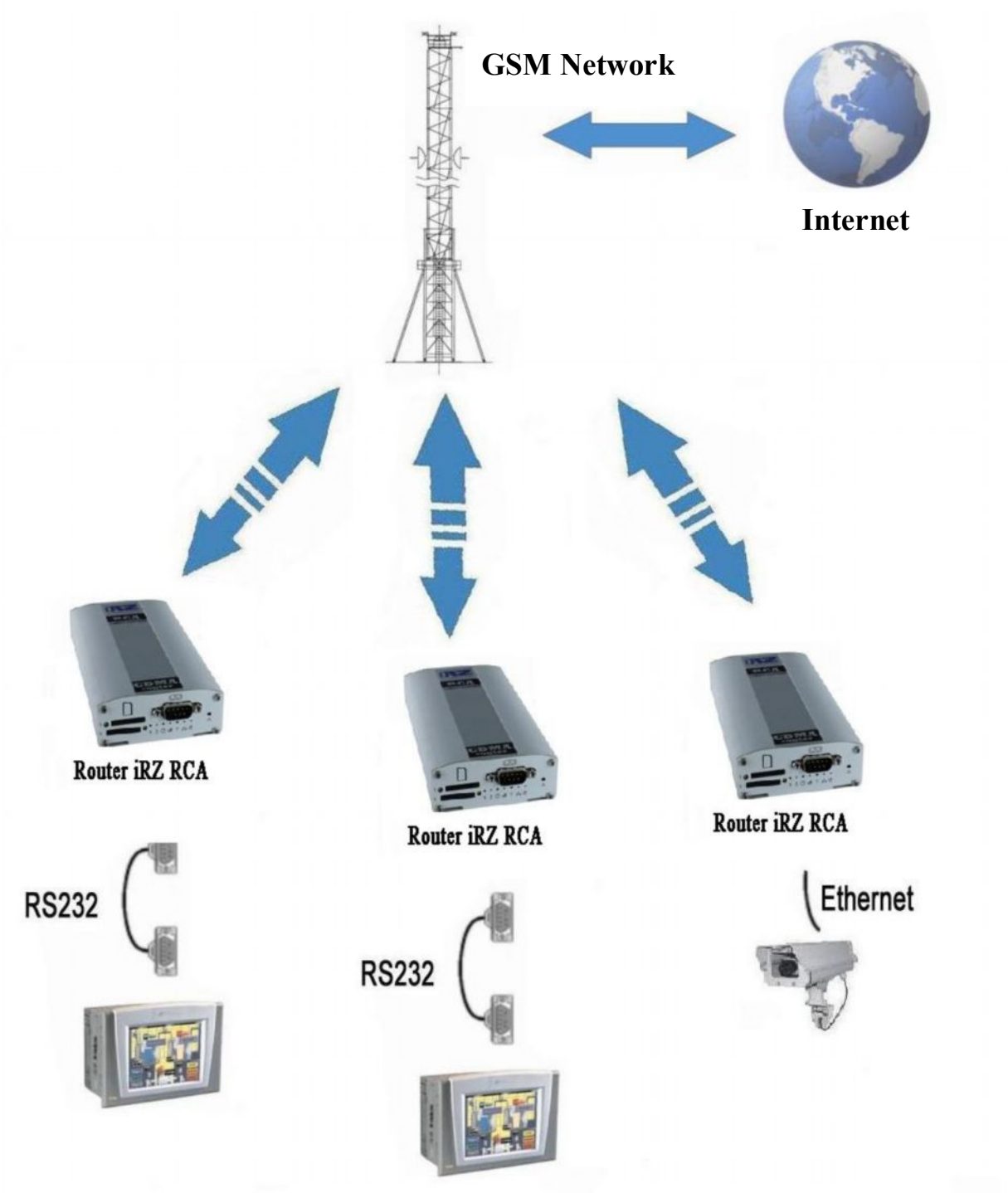
It is designed in a durable aluminum housing.

2.2. Typical Application

- Internet access for a computer or the entire network;



- Connection of vending machines and ATMs, industrial equipment and security systems and surveillance to the Internet, as well as for remote monitoring and control.


GSM Network
Internet
Router iRZ RCA
Router iRZ RCA
Router iRZ RCA
RS232
RS232
Ethernet

2.3. List of parts

Parts of GSM router iRZ RCA:

- Router iRZ RCA;
- Power unit 12V/1000mA;
- GSM antenna;
- 2 supply cables;
- Factory packaging.

2.4. Features

Key features:

- NAT configuration to access internal network resources from outside;
- DynDNS client to update information about a domain name when using dynamic IP address;
- GRE, IPsec and OpenVPN tunnels;
- Internal clock synchronization with external sources;
- Two R-UIM card slots, automatic switching between them or on the command via the web interface. Automatic switching takes place either due to the loss of connection with the operator, or according to the schedule. In the case of switching due to the loss of connection it can be returned to the priority R-UIM card.

Communication standards:

- CDMA,
- 1xRTT,
- 1xEVDO.

Hardware specifications:

- Processor ARM920T;
- Dynamic RAM 64 Mb;
- Flash-memory 8 MB;
- Ethernet 10/100Mbit.

Power supply:

- Supply voltage from 8 to 30 V;
- Current consumption not exceeding:
  - at supply voltage + 12 V – 800 mA;
  - at supply voltage + 24 V – 400 mA;

Physical Characteristics:

- Dimensions not exceeding 170x78x32 mm;
- Weight not exceeding 190 g;
- Operating temperature range from -30° C to 70° C;
- Storage temperature range from -50° C to 85° C.

Interfaces:

- DB9 connector for connecting the data cable, RS-232:
  - Data collection or equipment control by means of additional software;
  - Connection of two remote devices with COM-interface via the Internet.
- Connector Ethernet 10/100 Mbit;
- Connector USB A - USB Host. To connect an external device (flash-drives, USB-COM adapters) - centralized storage of files;
- Power connector;
- SMA connector to connect the GSM antenna.

2.5. Exterior view

Router iRZ RCA is produced in the industrial variant - in durable and lightweight aluminum housing. The exterior view is presented by fig.2.5.1 and fig.2.5.2.

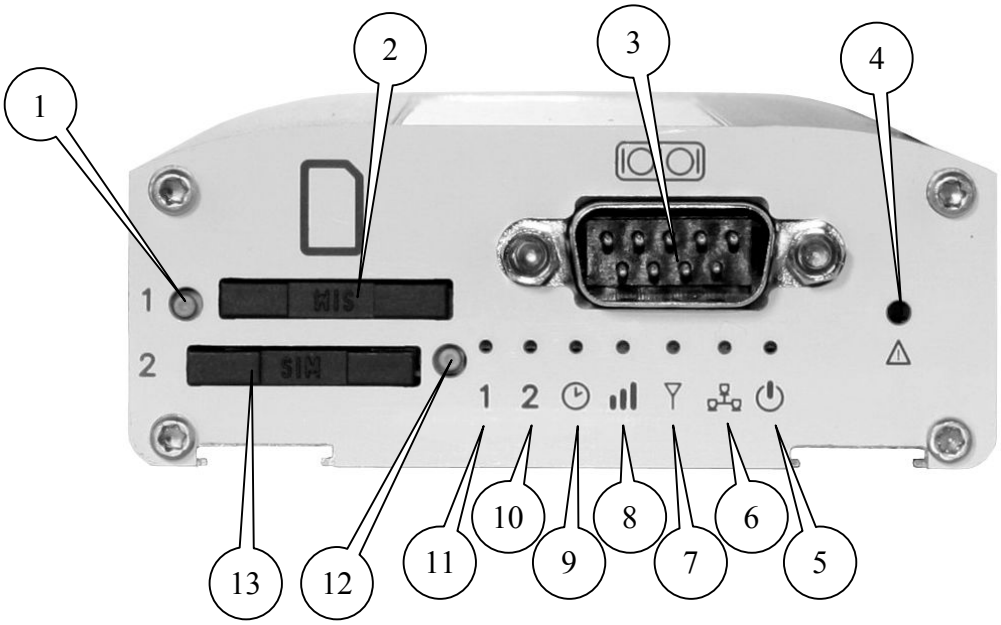


Fig. 2.5.1 Front view

The numbers in Figure 2.5.1 indicate:

1. R-UIM card № 1 tray eject button;
2. R-UIM card № 1 tray;
3. DB9 connector for data cable connection, RS-232;
4. Reset button;
5. Power indicator;
6. LAN indicator;
7. Connection type indicator;
8. GSM signal level indicator;
9. Router load indicator or software update;
10. R-UIM card № 2 activity indicator;
11. R-UIM card № 1 activity indicator;
12. R-UIM card № 2 tray eject button;
13. R-UIM card № 2 tray;

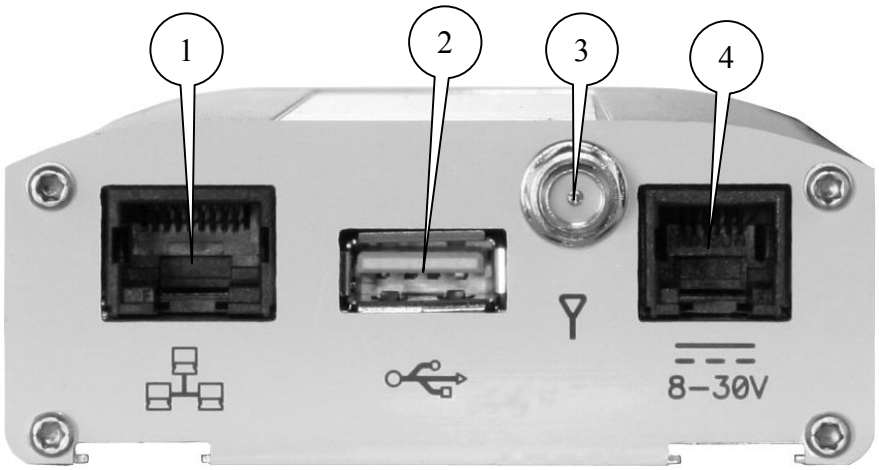


Fig. 2.5.2 Rear view

The numbers in Figure 2.5.2 indicate:

1. Ethernet network connector;
2. USB Host connector;
3. SMA connector to connect the GSM antenna;
4. Power connector.

2.6. Interfaces

2.6.1. Connector DB9 (RS232)

DB9 connector for connecting the data cable, RS-232 interface.

- Data collection or equipment control by means of additional software,
- Connection of two remote devices with COM-interface via the Internet.

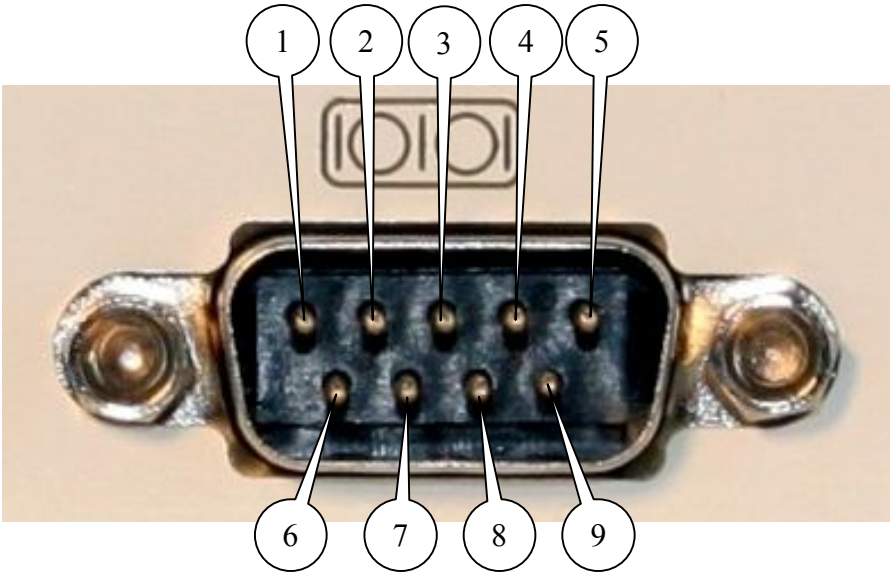


Fig. 2.5.1 Connector DB9

Table 2.6.1 DB9 connector pin functions

Pin	Signal	Direction	Function
1	not used	-	-
2	RXD	Device - Router	Data receiving
3	TXD	Router - Device	Data transmission
4	not used	-	-
5	GND	general	System housing
6	not used	-	-
7	not used	-	-
8	not used	-	-
9	not used	-	-

2.6.2. Power connector RJ11

This connector is used for power supply.

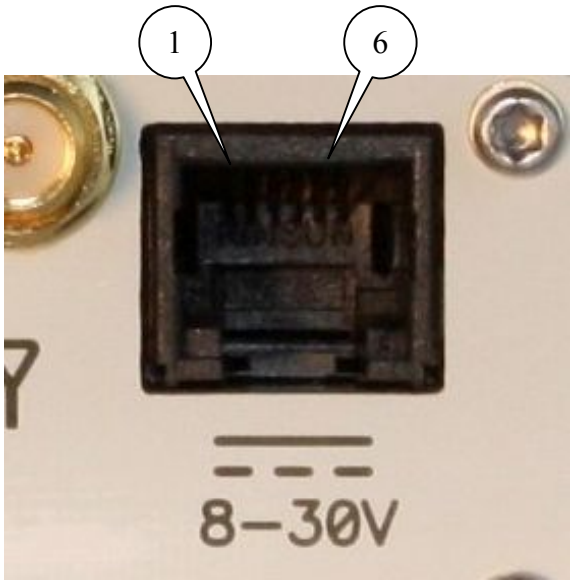


Fig. 2.6.2 Connector RJ11

Table 2.6.2 Power supply connector pin functions

Pin	Signal	Function
1	+ U sup	Positive pole of DC supply voltage Protected by fuse and surge voltage protection scheme (if input voltage above 30 V is supplied), and reverse polarity
2	not used	
3	not used	
4	not used	
5	not used	
6	GND	System housing

2.6.3. USB A connector

USB Host, allowing you to connect external devices such as flash-drives. This enables the user to organize centralized file storage.

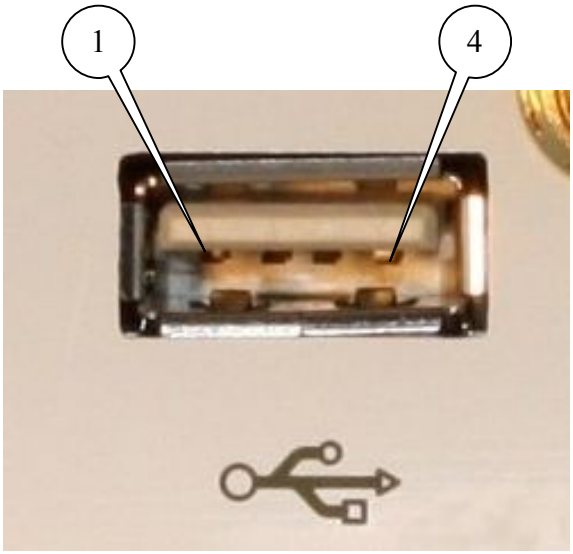


Fig. 2.6.3 Connector USB A

Table 2.6.1 USB connector pin functions

Pin	Signal	Function
1	VBUS	Supply circuit of peripherals, +5 V, 500 mA
2	D-	Data receiving/transmission
3	D+	Data receiving/transmission
4	GND	System housing

2.6.4. Ethernet network connector

Ethernet 10/100 Mbitps. Connection of a single computer or an entire network of devices for data collection and control.

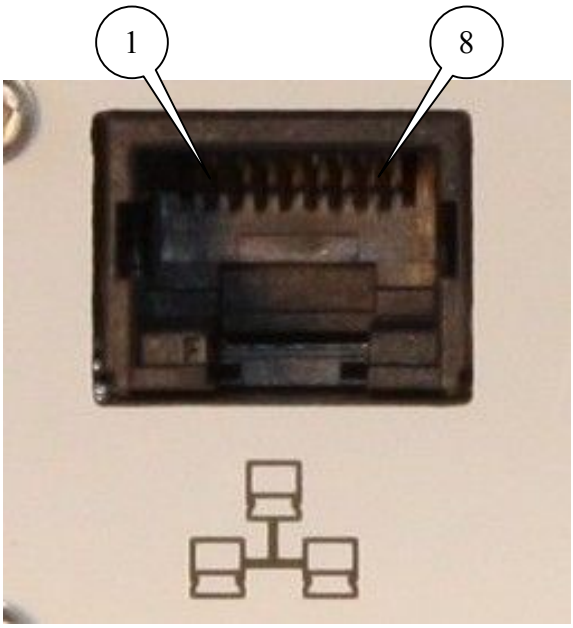


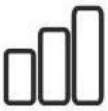
Table 2.6.4 Ethernet connector pin functions

Pin	Signal	Direction	Function
1	ETX P	Router - PC	Transmission, positive pole
2	ETX N	Router - PC	Transmission, negative pole
3	ERX P	PC - Router	Receiving, positive pole
4	not used	-	
5	not used	-	
6	ERX N	PC - Router	Receiving, negative pole
7	not used	-	
8	not used	-	

2.7. State indication

The front panel has 7 LEDs, which inform about the operation mode.

Table 2.7.1 LED indicator function

Symbol	Function, operation mode
1	R-UIM card № 1 selected;
2	R-UIM card № 2 selected;
	The router is busy – router loading, settings saving or inner program updating is under way. Wait until the indicator goes out before starting workю Do not turn off when the indicator is on!
	GSM signal level: • red light - weak signal level, • yellow light – average signal level, • green light - strong signal level.
	GSM connection type: • green light – CDMA, • off - connection not made.
	LAN: • on in case of the network cable connecting, • flashes when transferring data on LAN.
	Power supply - on when power is supplied.

3. Connection and Settings

3.1. Router connection to the computer to set up

Before power supply insert the R-UIM card into the router. To do this you need to:

- Pull out R-UIM tray by pressing the eject button on the R-UIM tray (fig.2.5.1) by long, thin object (straighten paper clip, toothpick, etc.);
- Insert R-UIM card № 1 into the tray;
- Insert R-UIM tray with R-UIM card into the router so that the edges of R-UIM tray got into the holder slots.

Do not apply physical effort when you insert the R-UIM card. If necessary, insert the second R-UIM card.

Connect GSM antenna and power cable. Use straight-through cable for connection to the switching unit or a crossover cable when connecting directly to your computer. Supply the router with power unit.

After power supply the router begins loading and load indicator is on. After load indicator is off, the router is ready for use.

3.2. Basic Configuration

Web-based interface is used to configure the router and monitor its status. Source IP address is 192.168.1.1. Configuration can only be made by a user "root" with the initial password "root".

Web-interface top contains Status and log, Configuration and Administration tabs. Left part has menu items for each tab.

3.2.1. Network Connection Settings

If the router iRZ RCA is used for only one device Internet access, there is no need to reconfigure the router network connection. You need only to configure the device properly: indicate the IP address from the range of 192.168.1.2... 192.168.1.254, netmask 255.255.255.0 and default gateway 192.168.1.1. You can also configure the device as DHCP-client. Then all these settings will be received from the router automatically.

If the Internet connection is provided for the network, select such router settings to avoid conflicts with the already connected devices. Consult your network administrator to obtain the correct settings.

3.2.2. Access to web-interface

To configure the router, connect it directly to your computer using a crossover cable. Set network connection properties "Automatically get IP address" in your computer. Enter 192.168.1.1

in the address line of the browser; click the link "iRZ RCA Router". Enter username "root", password "root" in the open window. Router web-interface will open. Click the tab "Configuration" and select "LAN". You'll be directed to the router network connection configuration page. Available options menu is on the left.

3.2.3. Configuring Network Connection Settings

Specify IP address of the router in the IP Address line.

This address should be free in the local network. If necessary, change the subnet mask (field “Subnet Mask”) and specify the desired DHCP-server settings. Note that if you want the computers in the network to use the Internet connection established by the router, you need to indicate the IP address of the router as the default gateway in the computers network settings. You may also need to specify IP address of the router in the field “DNS server”.

3.2.4. GSM Connection Configuring

Once the router is connected, and the network connection is set up, you can configure GSM connection. To do this choose menu item "Internet" in web-interface tab "Configuration".

To make a connection with the Internet you need to know the access point name (APN), username and password. This information can be obtained from your mobile operator. Indicate R-UIM card number. Enter APN, Username and Password values in the appropriate fields. Click "Apply" to save the settings and make a connection. After a while the connection will be established. Its status can be checked on the tab "Status and log" in the menu item "Internet".

3.2.5. Settings reset

If, due to incorrect settings you cannot access the router interface, or you forgot your password, you can revert to factory settings as follows:

- Switch on router;
- Press and hold the reset button (Figure 2.5.1);
- Reset is confirmed by triple flashing of load indicator;
- Release the reset button.

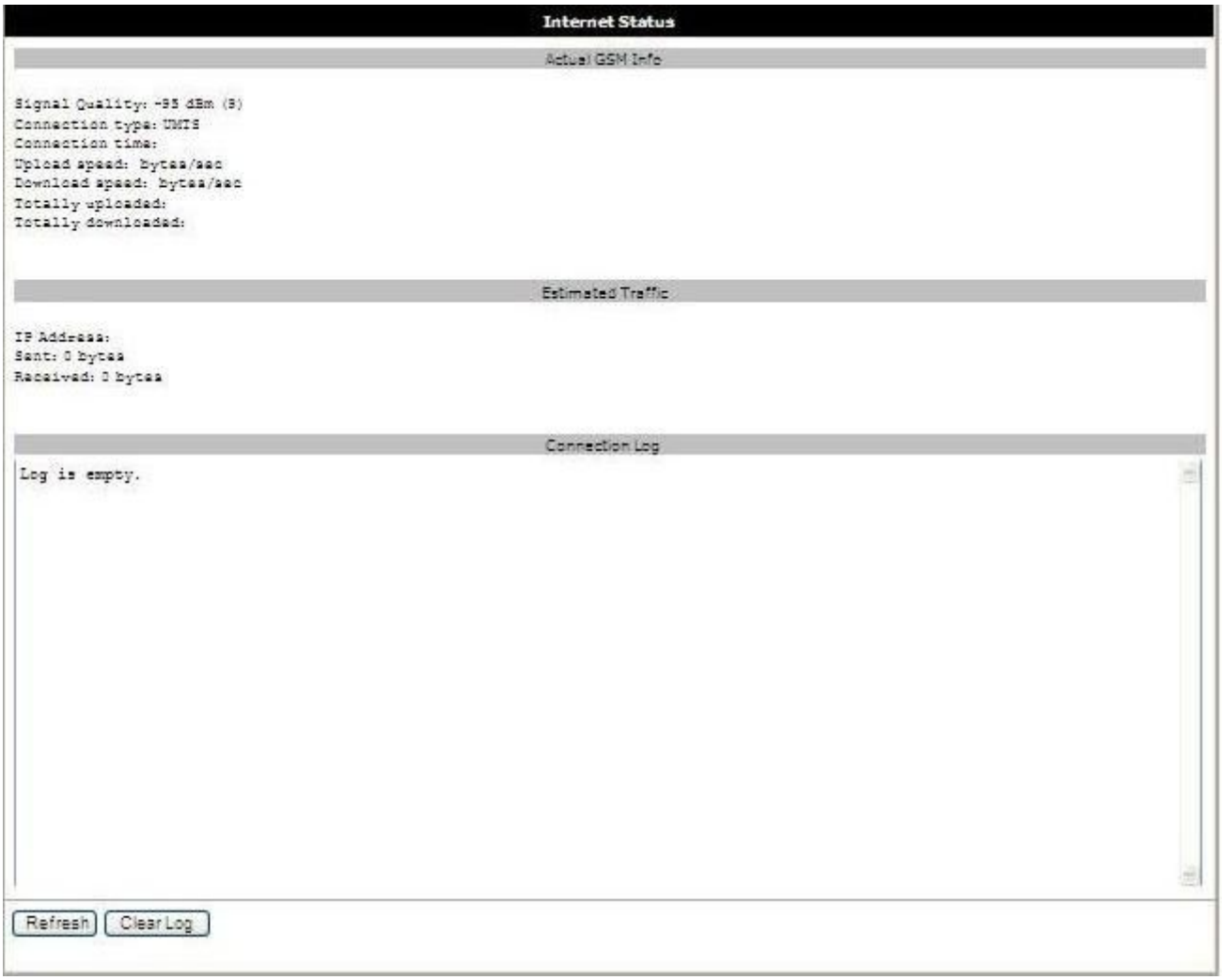
After resetting the device will be available at the address 192.168.1.1 with the username **root** and password **root.**

4. Web-interface Description

4.1. Status and log

4.1.1. Internet

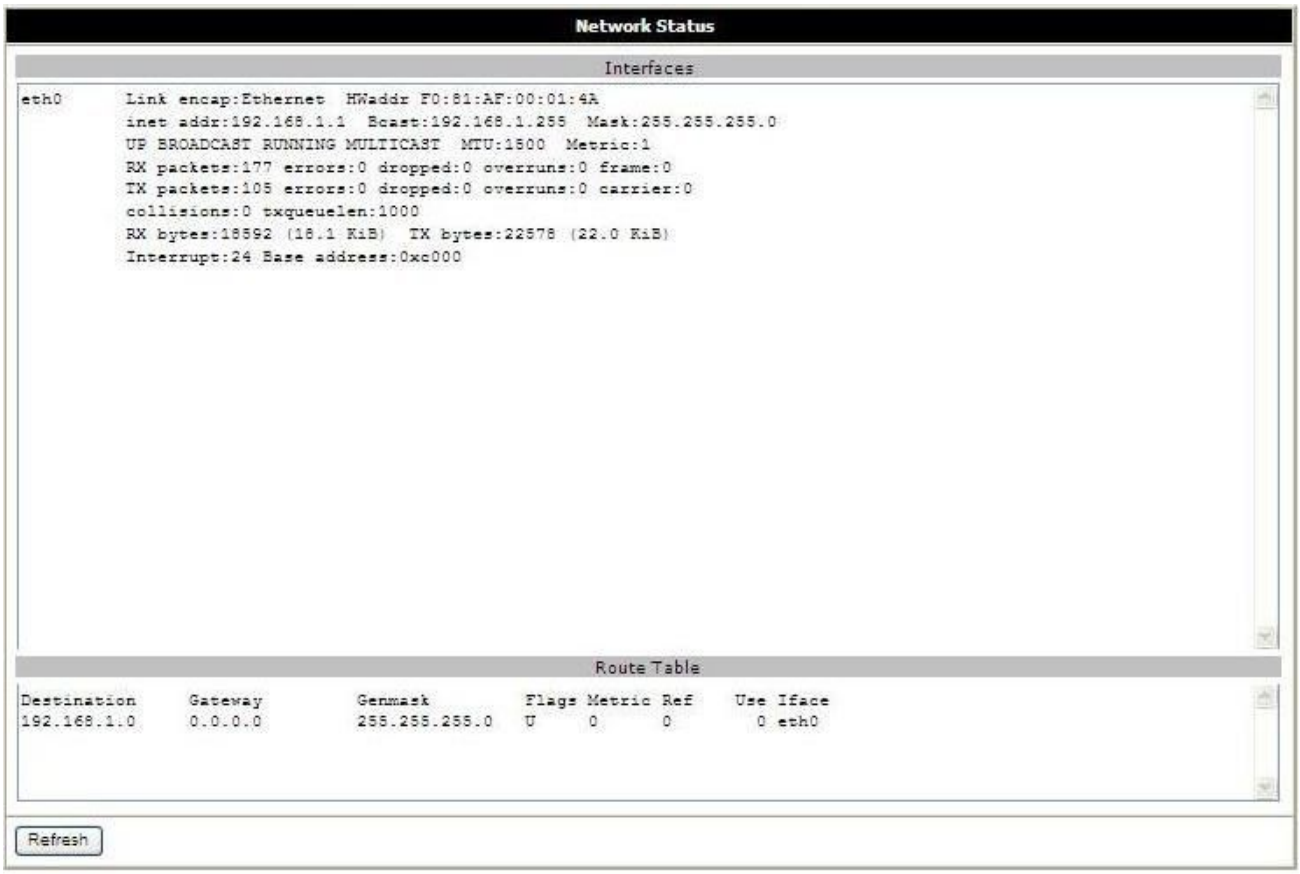
GSM-network and Internet connection status.



Where:
Actual GSM Info - information on GSM network,
Estimated Traffic- approximate traffic for a session,
Connection Log - log of the made connections,
Refresh - refresh page,
Connection Log - clear the log of connections

4.1.2. LAN

Current state of network connections and routing table.

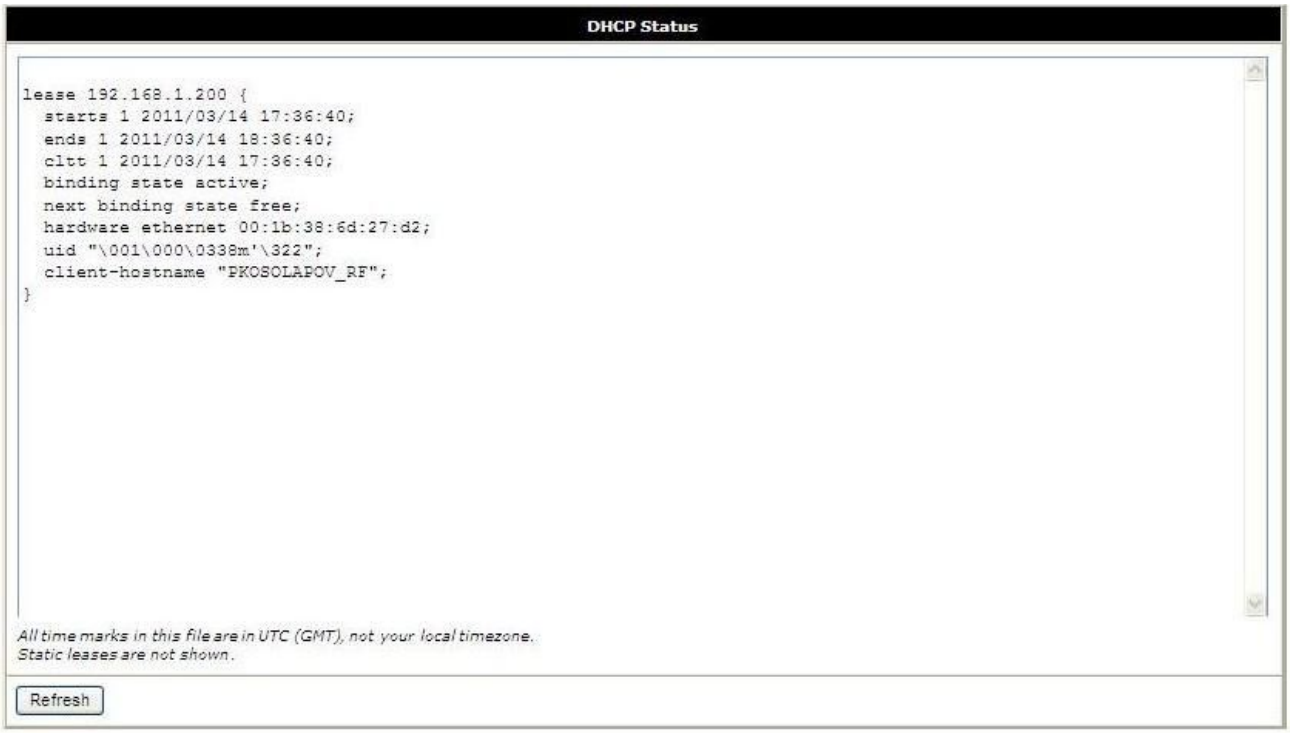


Where:

Interfaces - operating interfaces and their status,
eth0 - LAN connection,
ppp0 - UMTS/ EDGE/GPRS connection,
gre1 - GRE-tunnel,
Route table – routing table.

4.1.3. DHCP

Information about issued IP addresses and their recipients.

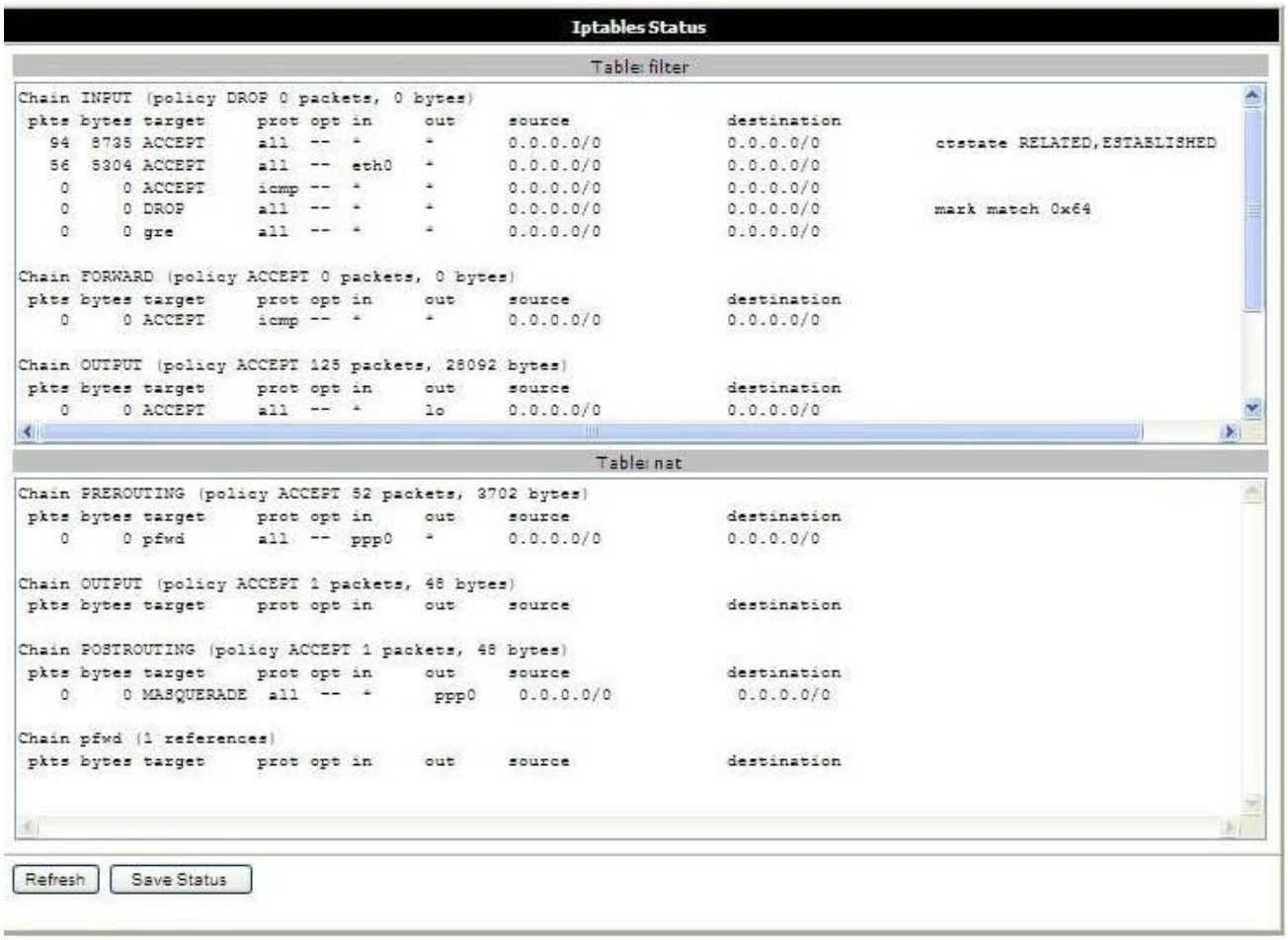


Where:
DHCP Status - current DHCP issues,
lease - leased IP address,
starts - date and time of IP address issuance,
ends - Date and time of IP address expiry,
hardware ethernet - device MAC-address.

Please note that time is indicated in UTC format. That is, not taking into account the shift for the specific time zone. Thus, the local time for Moscow, for example, will be 3 hours more (or 4 if the time of summer). This is due to the DHCP server peculiarities.

4.1.4. Iptables

Iptables rules.



Where:
Table filter - table filter rules,
Table nat - table nat rules.

4.1.5. OpenVPN Tunnel

Initialization Sequence Completed - connection is made

4.1.6. OpenVPN Server

OpenVPN server reports log

4.1.7. IPsec

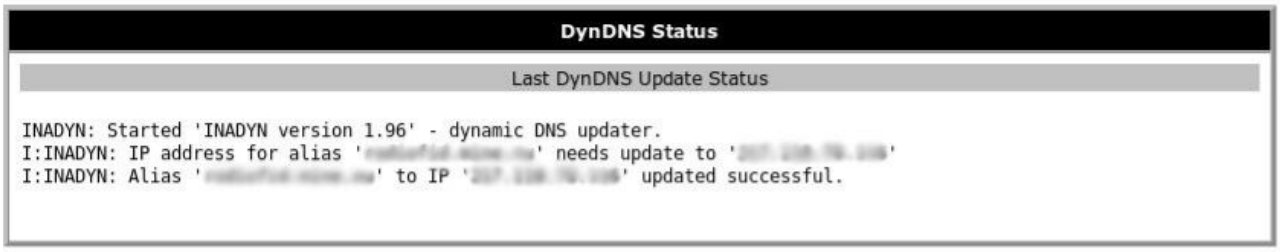
Status of encrypted tunnel IPsec.

```
000 "ipsec1": 192.168.1.0/24===85.26.139.166...217.66.146.11===192.168.2.0/24; erouted; eroute owner: #6
000 "ipsec1":     myip=unset; hisip=unset; myup=/etc/init.d/updown; hisup=/etc/init.d/updown;
000 "ipsec1":   ike_life: 3600s; ipsec_life: 3600s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0
000 "ipsec1":   policy: PSK+ENCRYPT+TUNNEL+UP; prio: 24,24; interface: ppp0;
000 "ipsec1":   newest ISAKMP SA: #1; newest IPsec SA: #6;
000 "ipsec1":   IKE algorithm newest: AES_CBC_128-SHA1-MODP2048
```

The first line shows the tunnel configuration and its state: erouted - determined, unrouted – not determined. The bottom line shows the used encryption algorithm.

4.1.8. DynDNS

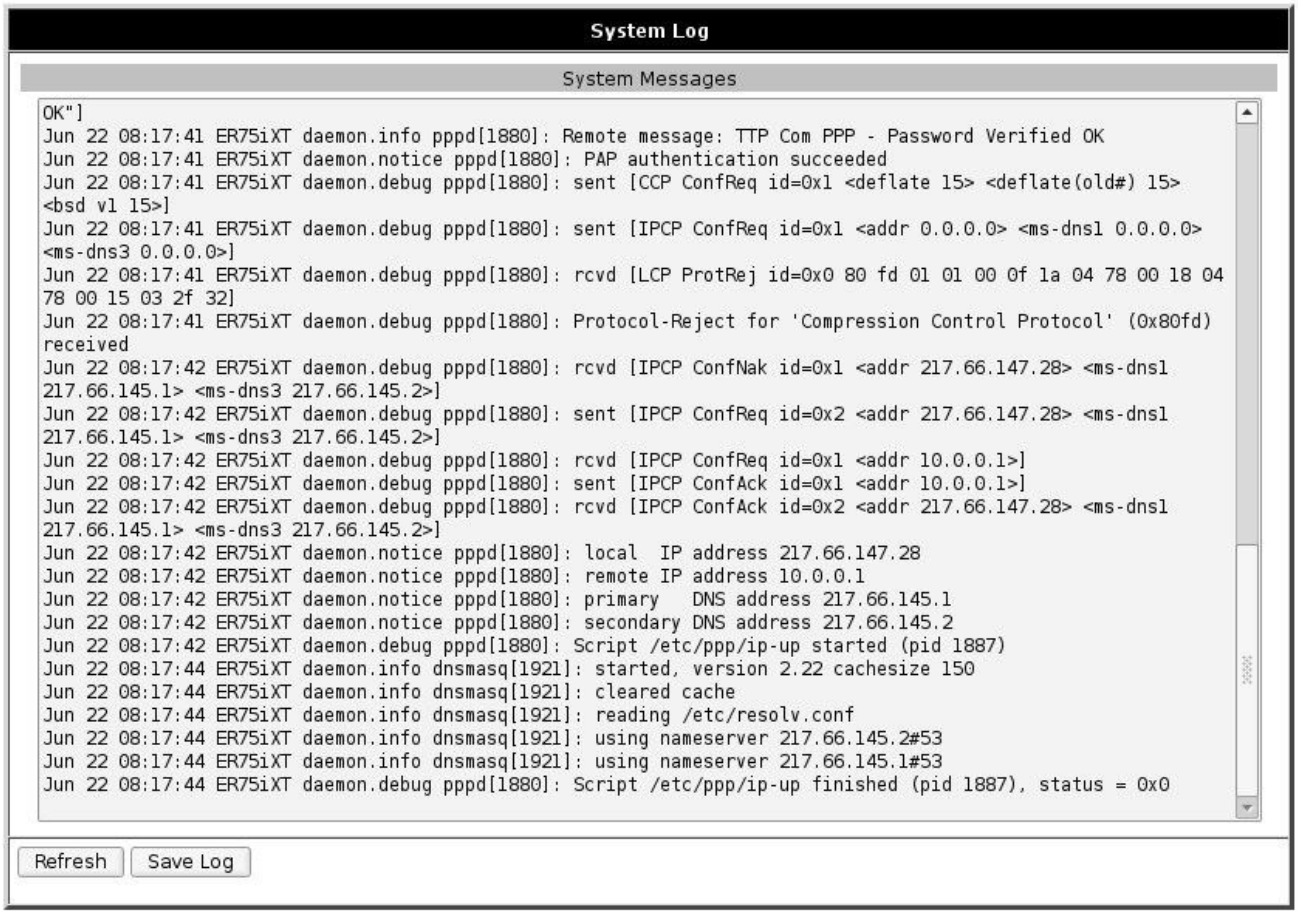
Information on the results of updating IP address in DynDNS system.



Last DynDNS Update Status - log of DynDNS last update

4.1.9. System Log

Log of system messages.

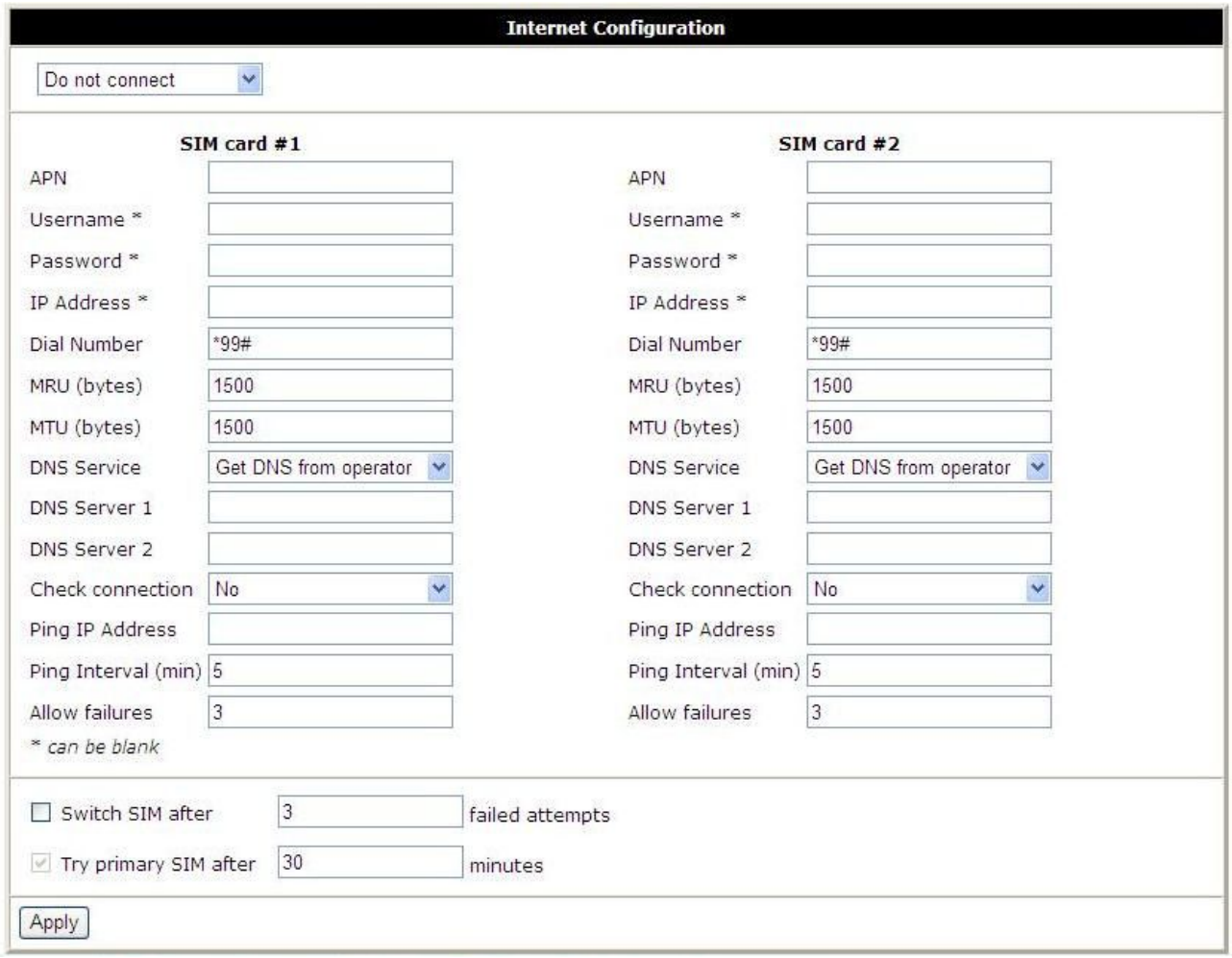


Where:
System Messages - Log of system messages,
Refresh - refresh page,
Save Log - save log on the computer.

4.2. *Configuration*

4.2.1. Internet

GSM Connection Configuring.



Where:
Do not connect/Connect using SIM 1/Connect using SIM 2 – SIM card selection at the start,
SIM card #1 – connection settings for SIM card №1,
SIM card #2 – connection settings for SIM card №2,
APN - access point name,
Username* - name of the user,
Password* - password,
IP Address* - network address (if it is required by the operator),
Dial Number – command to establish Internet connection,
MRU - the maximum size of received package,
MTU - the maximum size of transmitted package,
DNS service - DNS service configuring (do not use/receive DNS server address from the operator/ use indicated DNS server),

Check GPRS connection - do not check/check connection,
Ping IP Address - address, which connection is being checked,
Ping Interval - check interval,
Allow failures - allowed number of failed checks,
Switch SIM cards on failure - switch to another SIM card when the connection fails,
Switch SIM after X failed attempts - switch the SIM card after X failed attempts
Try primary SIM after XX minutes - switch to the primary SIM card after XX minutes of work with the reserve one.
Apply - apply settings.

* - the field can be empty.

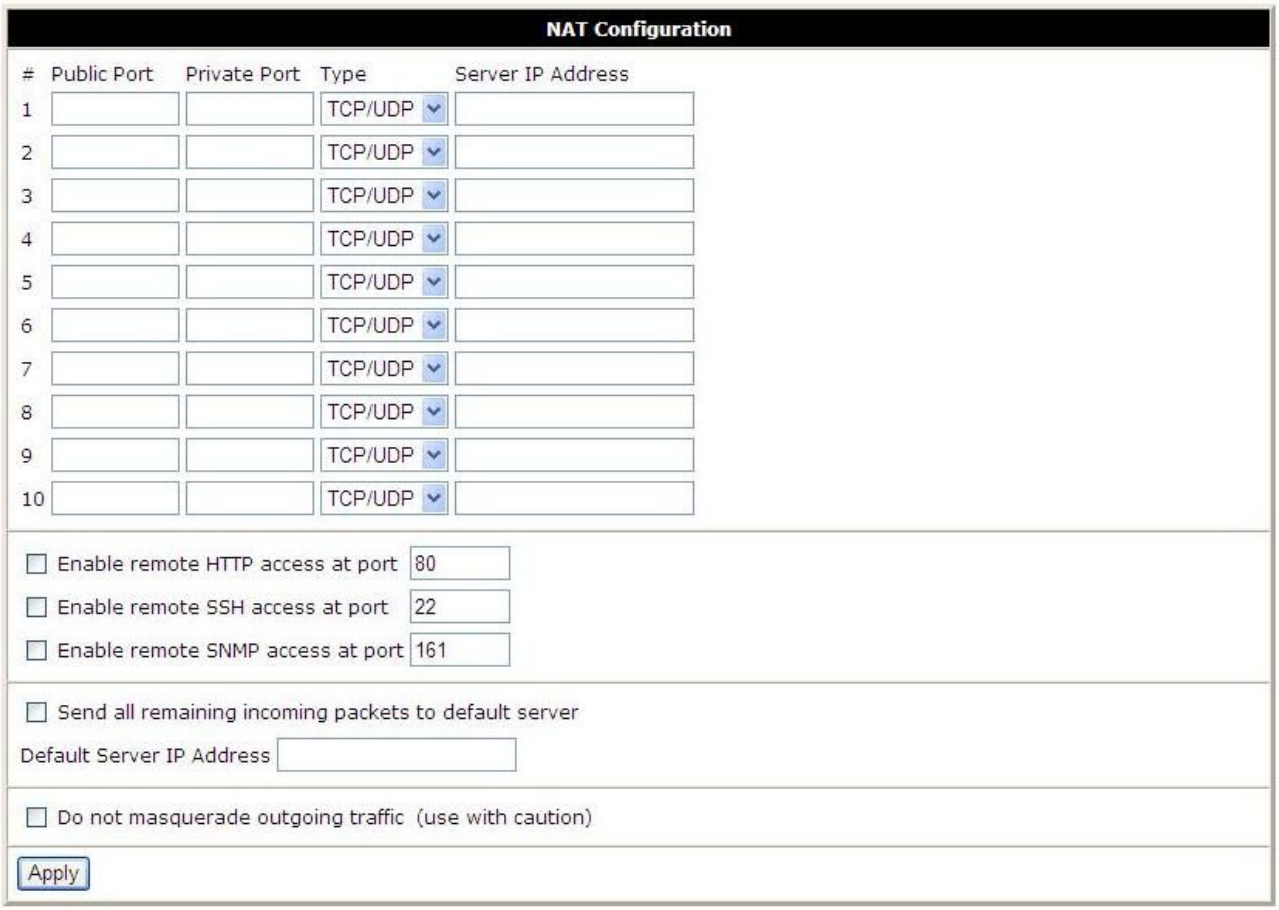
4.2.2. LAN

Configuring LAN connection and DHCP-server.

Where:
IP Address - router IP address,
Subnet Mask - subnet mask,
Enable DHCP server - turn on DHCP server,
IP Pool Start - beginning of the issued addresses range,
IP Pool End - end of the issued addresses range,
Default Lease Time - default term of the address lease,
Maximum Lease Time - maximum term of the address lease,
Apply - apply settings.

4.2.3. Port Forwarding

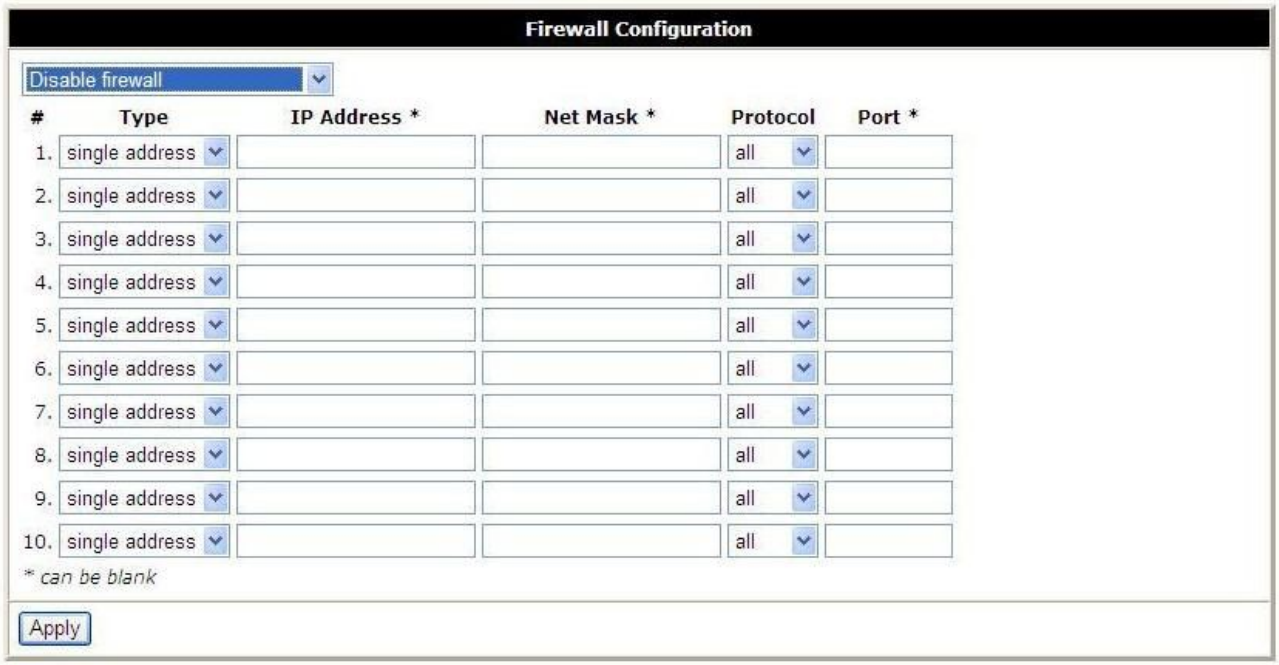
Providing computers from Internet with access to a server in the LAN.



Where:
Public Port - the port, accessible from the Internet,
Private Port - server port on the LAN,
Type - protocol type: TCP or UDP,
Server IP Address - IP address of the server,
Enable remote HTTP access - allow access to the web-interface of the router via the Internet on a specified port,
Send all remaining incoming packets to default server - send all other incoming packets to the default server,
Default Server IP Address - IP address of the default server,
Do not masquerade outgoing traffic – switch off outgoing traffic masquerading,
Apply - apply settings.

4.2.4. Firewall

Firewall restricts access to the specified network resources.

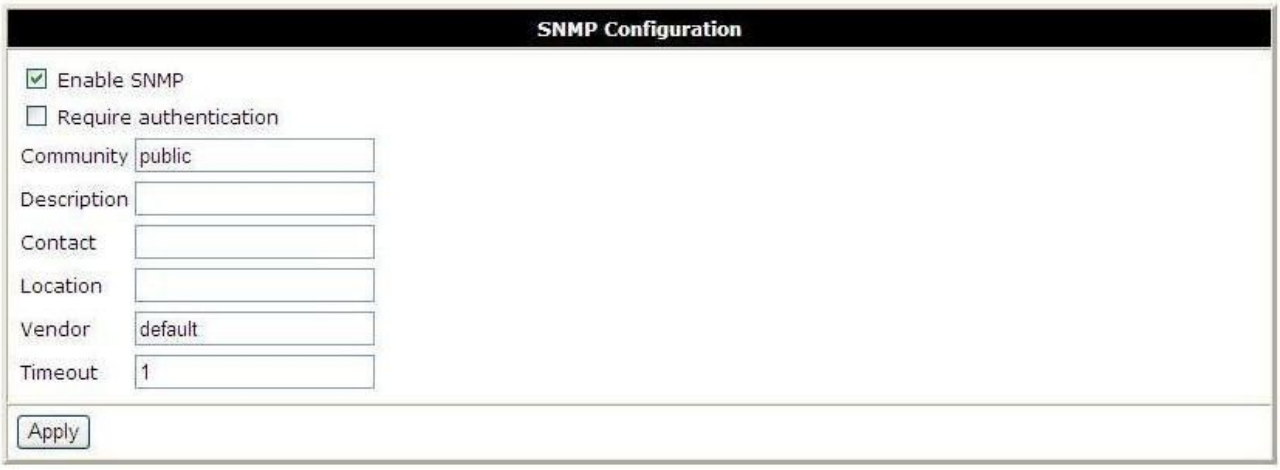


Where:
Disable firewall/Disable specified, allow others - select filter to enable access to the specified hosts,
Type: single address - any specified address,
IP Address - source IP address,
Protocol - protocol (all, tcp, udp, icmp)
Port - target port
Apply - apply settings.

* - the field can be empty.

4.2.5. SNMP

Service for remote monitoring of the device status.



Where:
Enable SNMP server – turn on SNMP service,
Require authentication - require authentication (protocol 2c),
Community - community name,
Description – device description,
Contact - information about the owner,
Location – location,
Vendor – producer,
Timeout - statistics updating period,
Apply - apply settings.

Note: Is not allowed to use spaces in the text boxes due to software specific. All fields are optional: the correct values will be entered automatically.

4.2.6. GRE

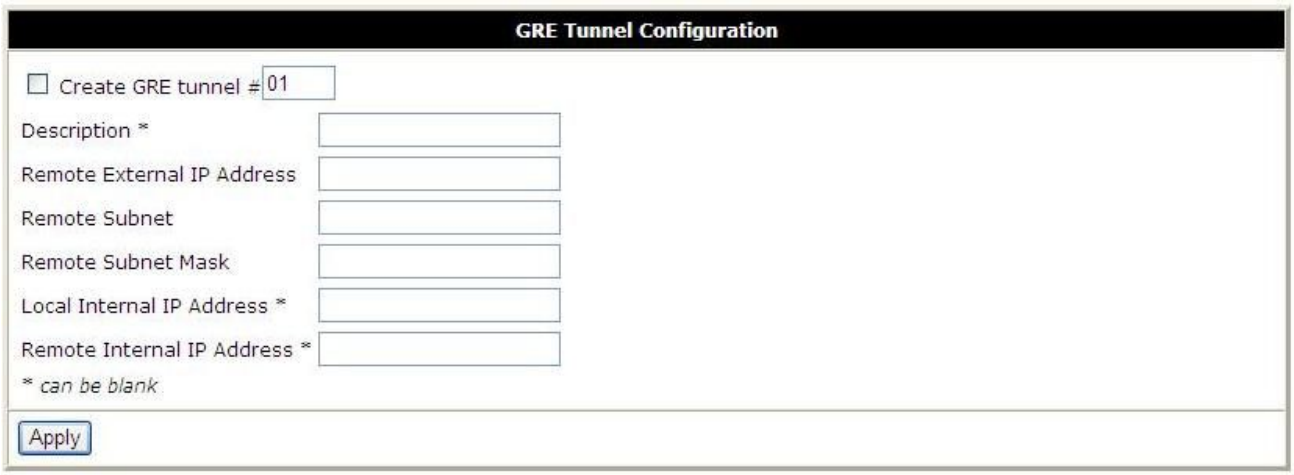
Using GRE tunnel you can combine two physically separated LANs into a single logical net. Attention: data is transmitted openly!

Tunnels summary table:

Where:
- tunnel number,
Create - create tunnel: yes, no,
Description - brief description,
Remote IP Address - remote machine address,
Remote Subnet - remote net,
Edit - edit tunnel settings,
Apply - apply settings.

You can enable or disable individual tunnels or go to the settings page of one of the tunnels in this page.

Tunnel configuration page



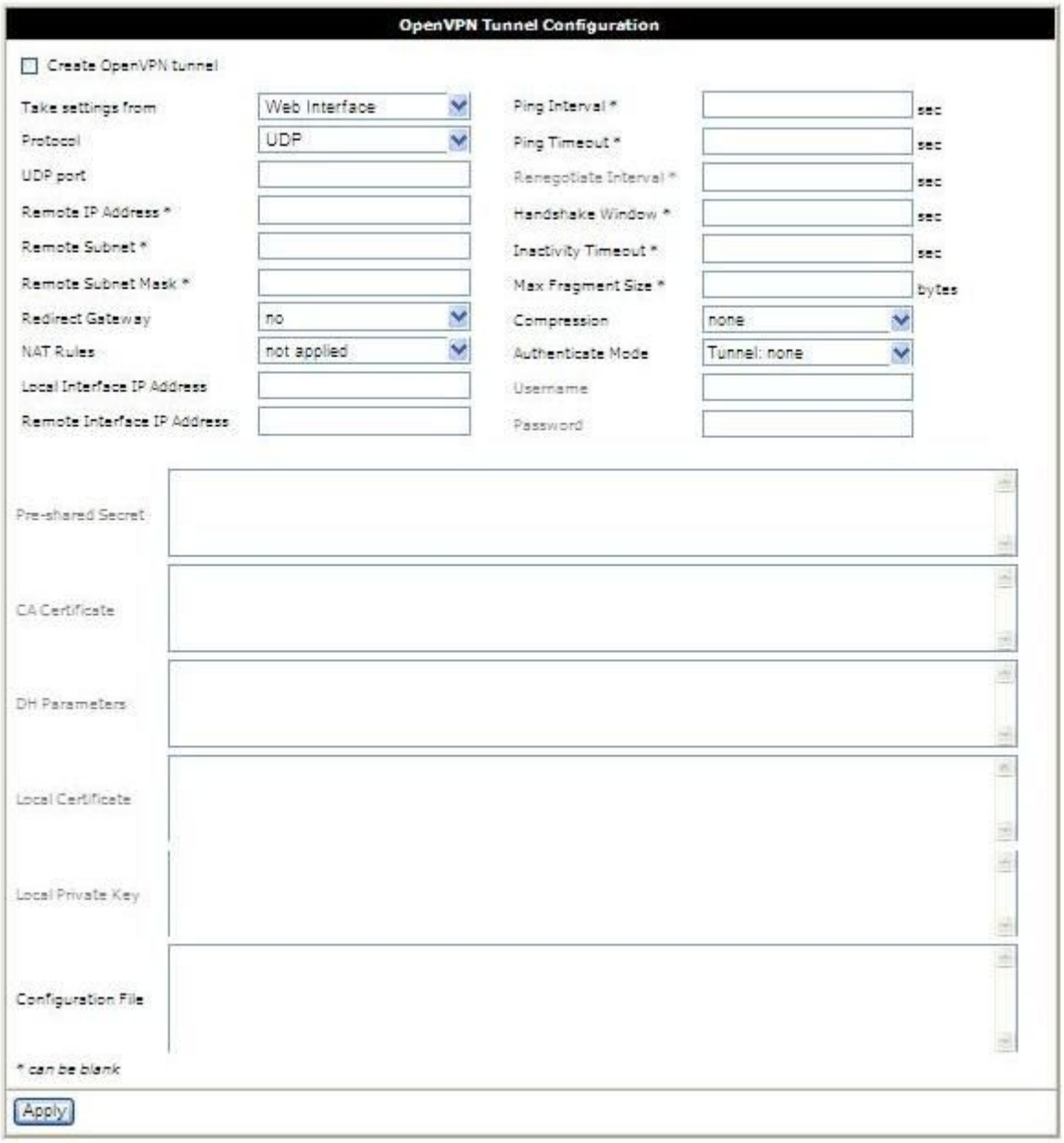
Where:
Create GRE tunnel #01 - create GRE tunnel № 01
Description - brief tunnel description,
Remote External IP Address - external IP address of the remote net
Remote Subnet – remote net,
Subnet Mask - remote net mask,
Local Internal IP Address - local internal IP address,
Remote Internal IP Address - remote internal IP Address,
Apply - apply settings.

* - the field can be empty.

Fields **Local Internal IP Address** and **Remote Internal IP Address** are used when combining two devices only in different networks.

4.2.7. OpenVPN Tunnel

OpenVPN is a secure tunnel between two devices.



Where:
Create OpenVPN tunnel - Create OpenVPN tunnel,
Take settings from:

- Web-interface,
- Configuration file

Protocol:

- UDP - recommended (requires both external IP addresses),
- TCP server - for device with external IP address,

- TCP client - for device without external IP address,

UDP Port - UDP port number,
Remote IP Address - remote IP address,
Remote Subnet - remote network,
Remote Subnet Mask - remote network mask,
Redirect Gateway - change default gateway:

- no;
- yes,

NAT rules:

- no applied - do not apply,
- applied - apply,

Local Interface IP Addresss - local virtual interface address,
Remote Interface IP Address - remote virtual interface address,
Ping Interval - check interval (seconds),
Ping Timeout - waiting interval (seconds),
Renegotiate Interval - reconnection interval (seconds),
Handshake Window - maximum interval of key exchange when connecting,
Inactivity Timeout - завершать соединение при отсутствии активности в течение заданного интервала,
Max Fragment Size - maximum size of a fragment,
Compression:

- none,
- LZO - according LZO algorithm,

Authenticate Mode:

- Tunnel: none,
- Tunnel: pre-shared secret - Tunnel: with key,
- Tunnel: X.509 certificate (client),
- Tunnel: X.509 certificate (server),
- Client: username/password - Client: with username and password,
- Client: X.509 certificate,

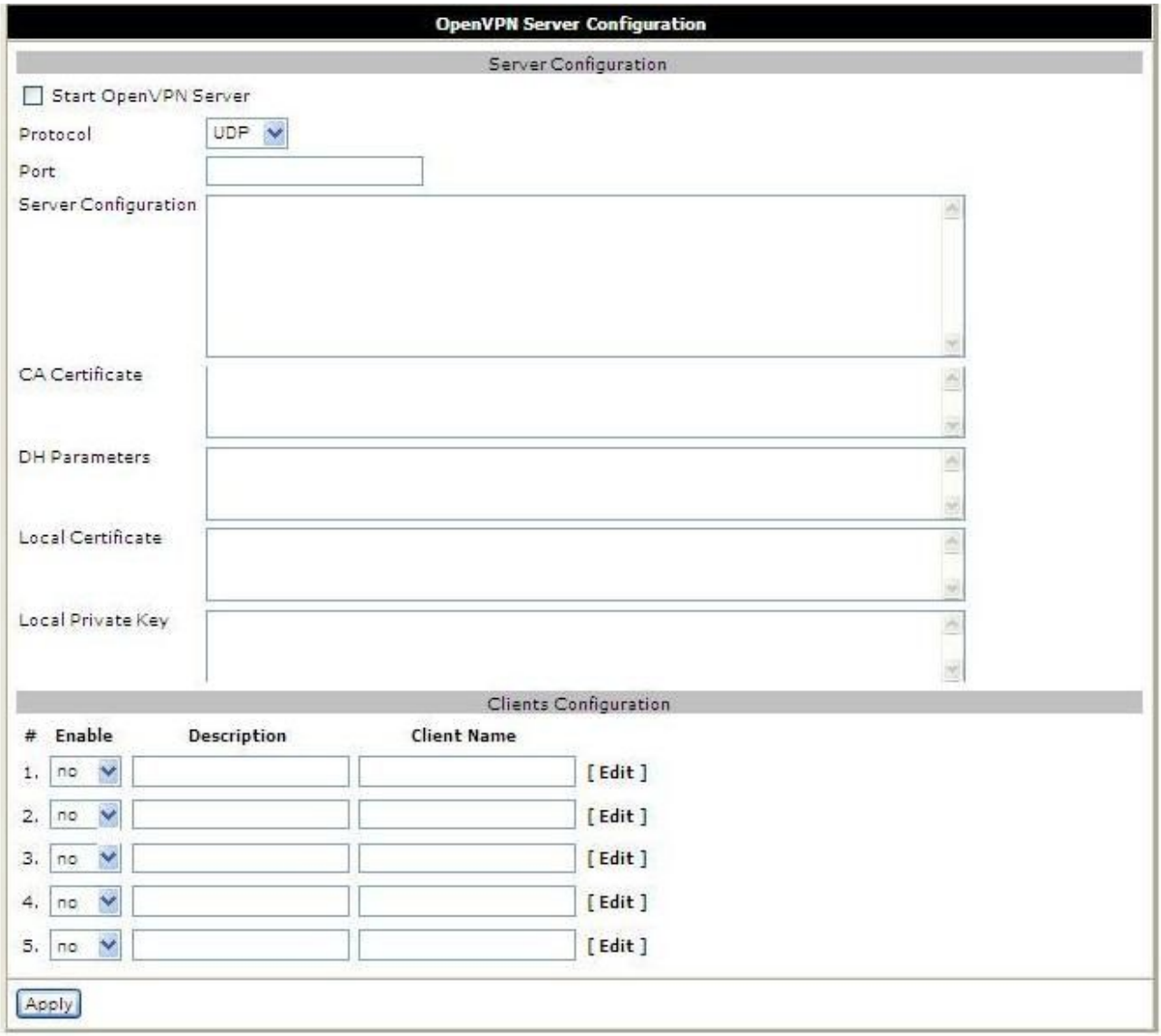
Username - name of the user,
Password - password,
Pre-shared Secret – authentication key,
CA Certificate - root certificate,
DH Parameters - Diffie-Hellman algorithm parameters,
Local Certificate - personal certificate,
Local Private Key - personal secret key,
Configuration File - field to enter configuration file,
Apply - apply settings.

* - the field can be empty.

A detailed guide for OpenVPN tunnel configuration can be found at our website, in "Support" section.

4.2.8. OpenVPN Server

OpenVPN server enables connections with OpenVPN clients.

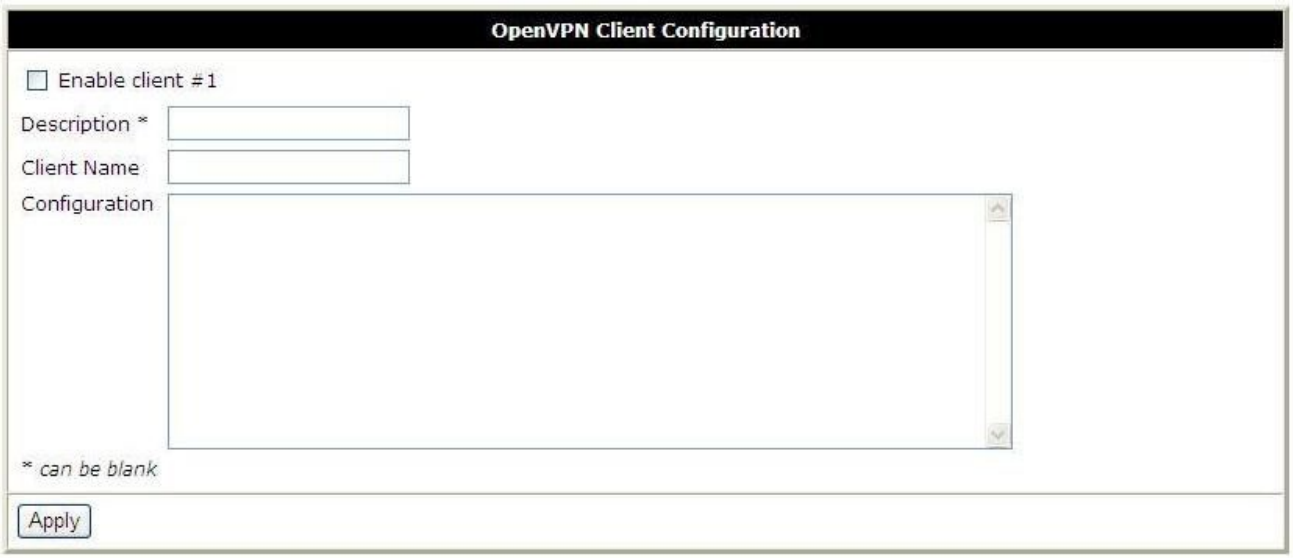


Where:
Server Configuration - server configuration,
Start OpenVPN Server - start OpenVPN server,
Protocol - protocol (TCP or UDP),
Port - port,
Server Configuration - server configuration,
CA Certificate - root certificate,
DH Parameters - Diffie-Hellman algorithm parameters,
Local Certificate - local certificate,
Local Private Key - local key,
Clients Configuration - clients configurations,
- client number,
Enable - Enable /disable connection,

Description - brief description,
Client Name - client name,
Edit - edit client settings,
Apply - apply settings.

Server configuration is similar to OpenVPN server configuration on the computer, except that the parameters of dev, port, and proto are not needed to be indicated.

Client configuration page.

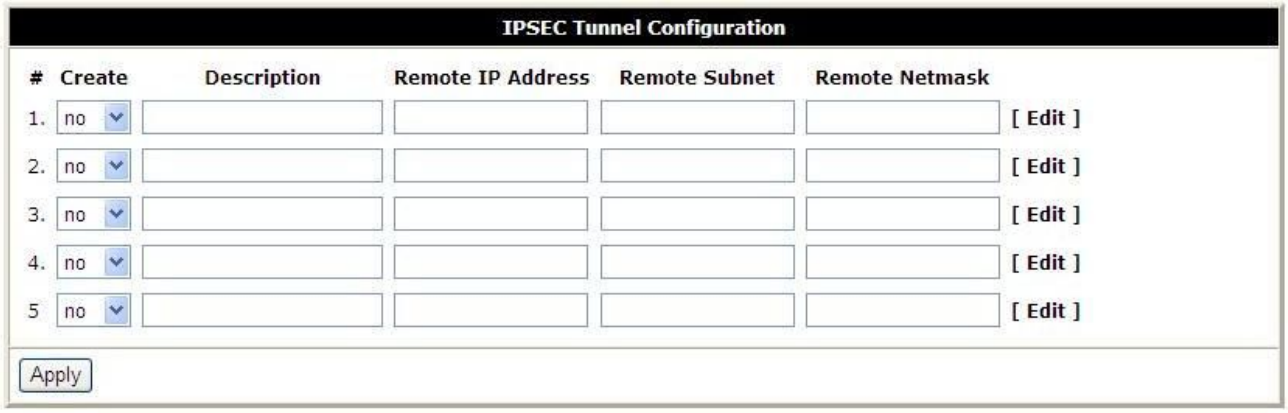


Where:
Enable client #1 - Enable client № 1,
Description - brief description,
Client Name - client name,
Configuration - client configuration,
Apply - apply settings.

* - the field can be empty.

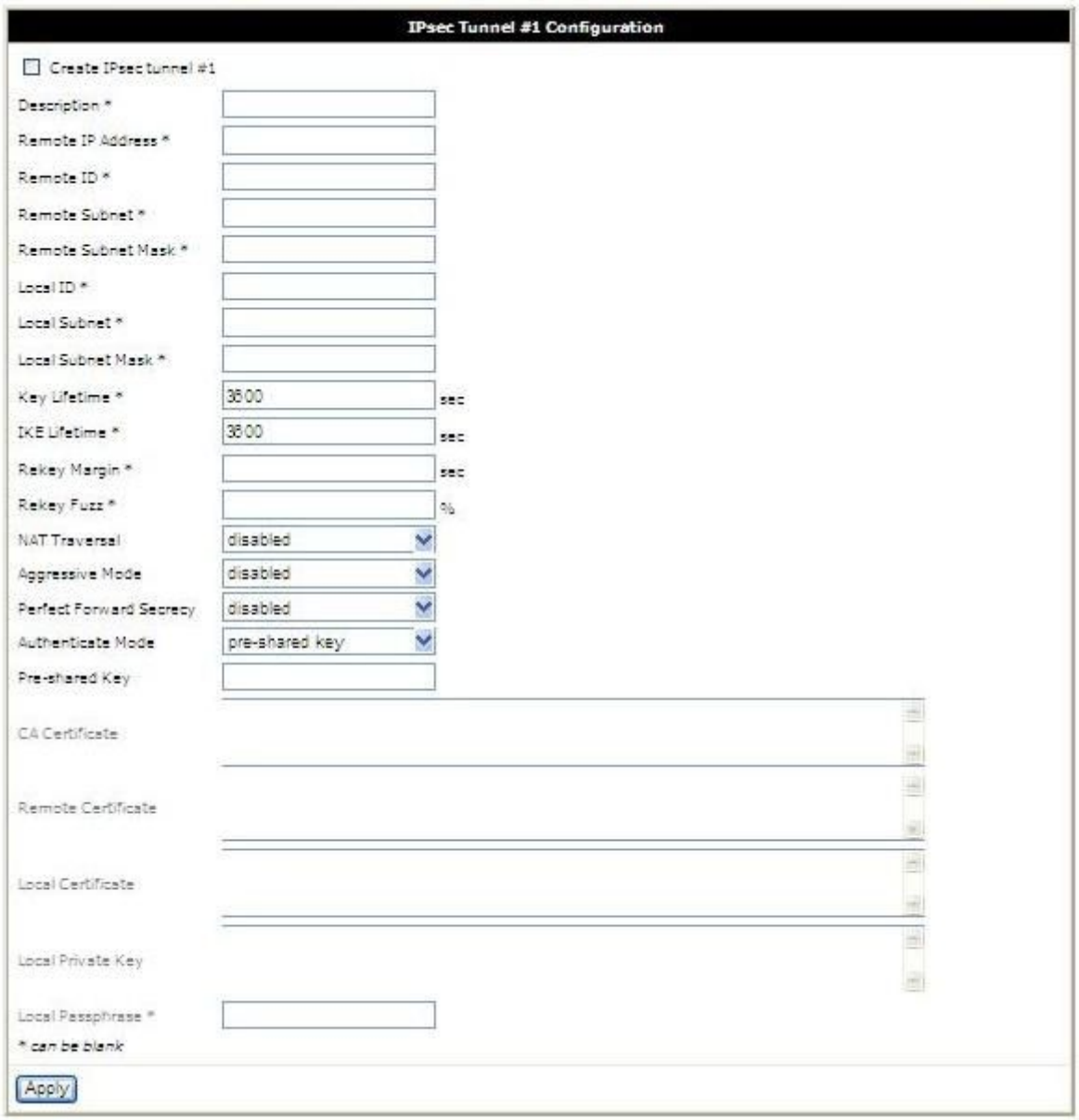
4.2.9. IPsec

IPsec tunnel connects two networks via encrypted channel.



Where:
- tunnel number,
Create - create IPsec tunnel,
Description - brief description,
Remote IP Address - remote IP address,
Remote Subnet - remote network,
Remote Subnet Mask - remote network mask,
Edit - edit client settings,
Apply - apply settings.

Client configuration page.



Where:
Create IPsec Tunnel #1- create tunnel IPsec №1,
Description - brief description,
Remote IP Address - remote IP address,
Remote ID - remote identifier,
Remote Subnet - remote subnet,
Remote Subnet Mask - remote subnet mask,
Local ID - local identifier,
Local Subnet - local subnet,
Local Subnet Mask - local subnet mask,
Key Lifetime - lifetime of the key,
IKE Lifetime - IKE connection lifetime,
Rekey Margin - reinitialization lead,
Rekey Fuzz - lead accidental addition,

NAT Traversal:
- disabled,
- enabled,

Aggressive Mode:
- disabled,
- enabled,

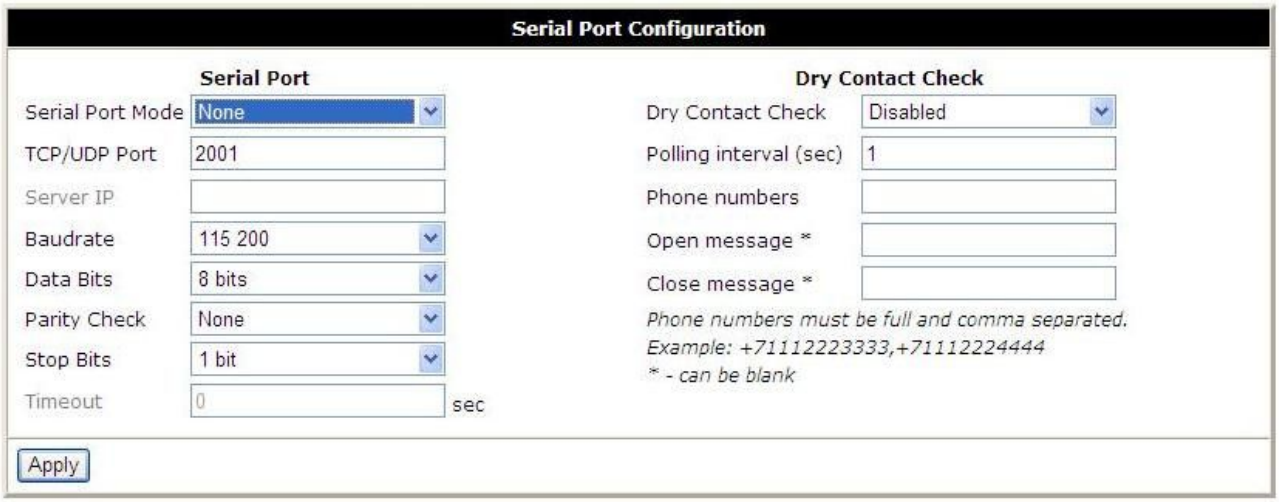
Authenticate Mode:
- pre-shared key - common key,
- X.509 certificate,

Pre-shared key - common key,
CA Certificate - root certificate,
Remote Certificate - remote certificate,
Local Certificate - local certificate,
Local Private Key - local key,
Local Passphrase - local password phrase,
Apply - apply settings.

* - the field can be empty.

4.2.10. Serial Port

External serial port access configuration.



Where:
Serial Port Mode - serial port access mode,

- None - no access,
- Telnet (TCP) - via Telnet (protocol TCP),
- Raw Data (TCP) - binary data (protocol TCP),
- Tunnel Server (UDP) - Tunnel Server (protocol UDP),
- Tunnel Client (UDP) - tunnel client (protocol UDP),

TCP/UDP Port - connection port (TCP or UDP),
Server IP - server IP address (in tunnel client mode only),
Baudrate - data transmission rate,
Data Bits - data bit volume,
Parity Check:

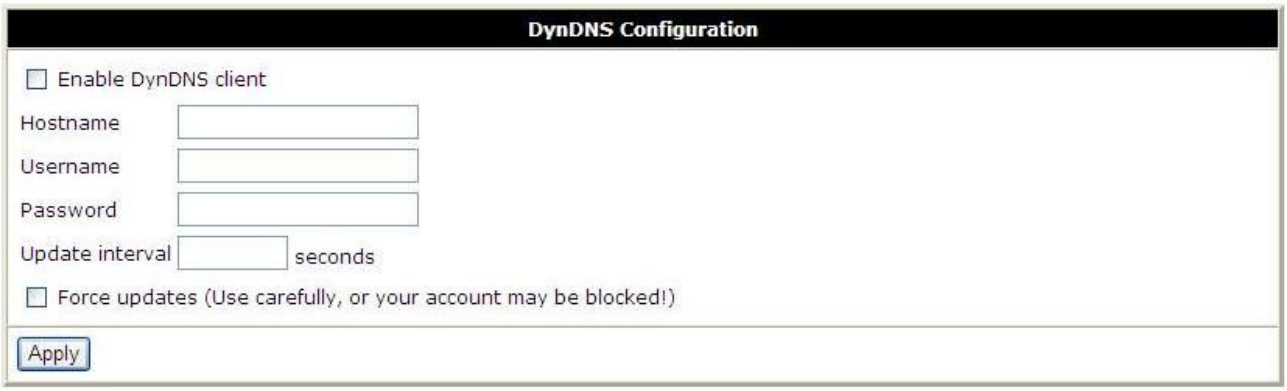
- None,
- Even,
- Odd,

Stop Bits - stop bits volume,
Timeout - Timeout (only in Telnet and Raw Data modes)
Apply - apply settings.

A detailed guide for serial port configuration can be found at our website, in "Support" section.

4.2.11. DynDNS

Allows you to assign a domain name for a computer with an external dynamic IP address.

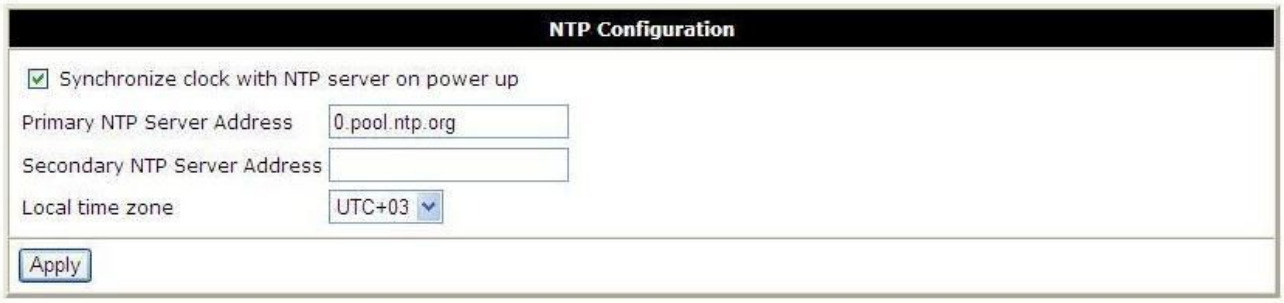


Where:
Enable DynDNS client - enable DynDNS client,
Hostname - domain name,
Username - name of the user,
Password - password,
Apply - apply settings.

Note: To use DynDNS service you should register at the site http://www.dyndns.com.

4.2.12. NTP

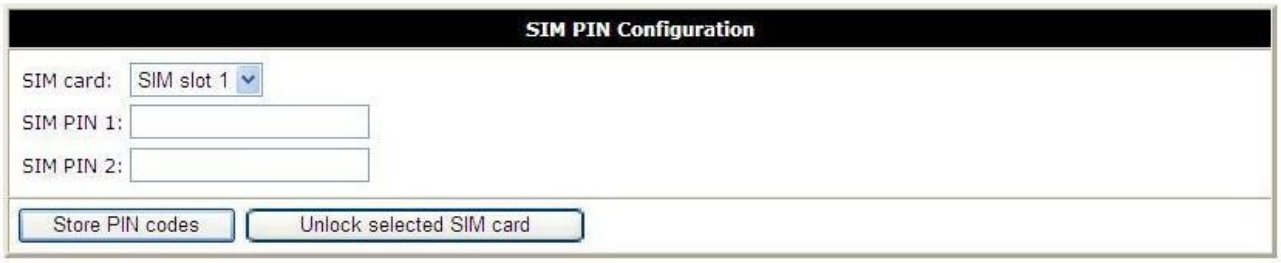
Router clock synchronization with time servers via the Internet.



Where:
Synchronize clock with NTP server on power up - synchronize clock at the start up,
Primary NTP Server Address - first NTP server address,
Secondary NTP Server Address - second NTP server address,
Local time zone - local time zone,
Apply - apply settings.

4.2.13. PIN

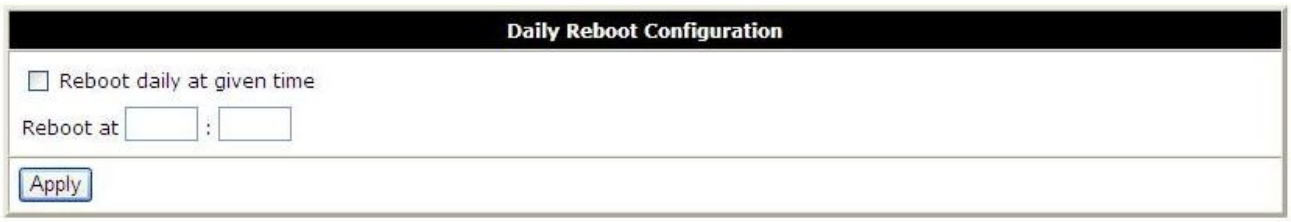
Card secured by PIN code unlocking.



Where:
SIM card - selection of SIM card to disable PIN code,
SIM PIN 1 - PIN code for the 1st SIM card,
SIM PIN 2 - PIN code for the 2nd SIM card,
Store PIN codes - store PIN codes,
Unlock selected SIM card - disable PIN code check for the selected SIM card.

4.2.14. Daily Reboot

Daily Reboot in the specified time.

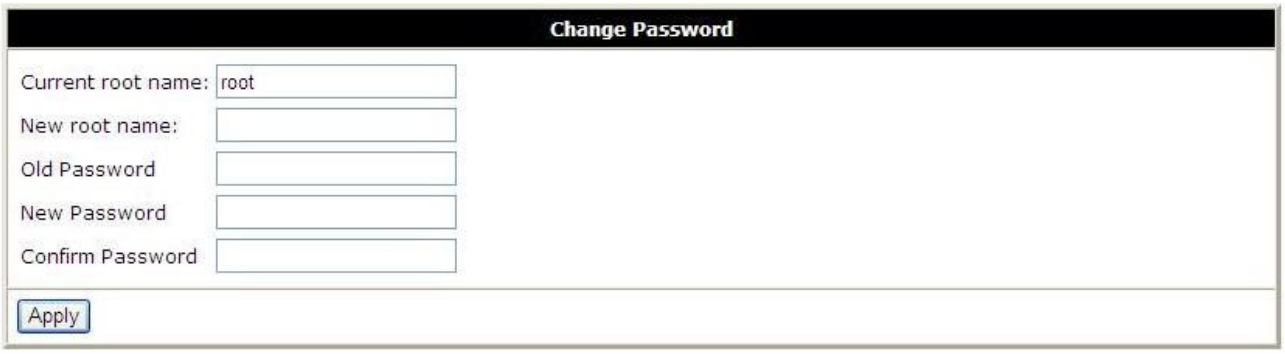


Where:
Reboot daily at given time - reboot every day at specified time,
Reboot at - reboot time (HH:MM),
Apply - apply settings.

4.3. Administration

4.3.1. Change Password

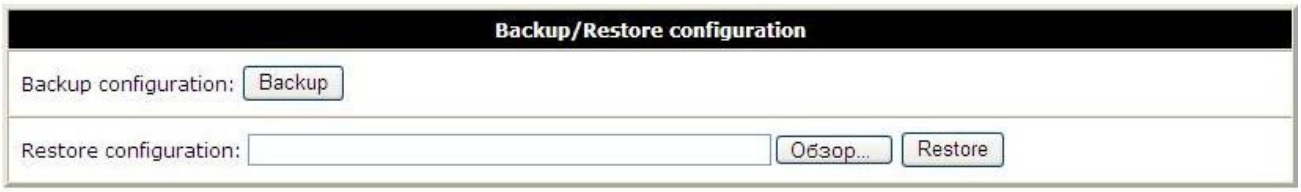
Set a password to access the web-interface and the console, change administrator name.



Where:
Current root name - current administrator name,
New root name - new administrator name,
Old Password - previous password,
New Password - new password,
Confirm Password - repeat new password,
Apply - apply settings.

4.3.2. Backup/Restore

Router settings saving and restoring.



Where:
Backup - save configuration in the computer,
Обзор… - select file of saved configuration,
Restore - restore configuration.

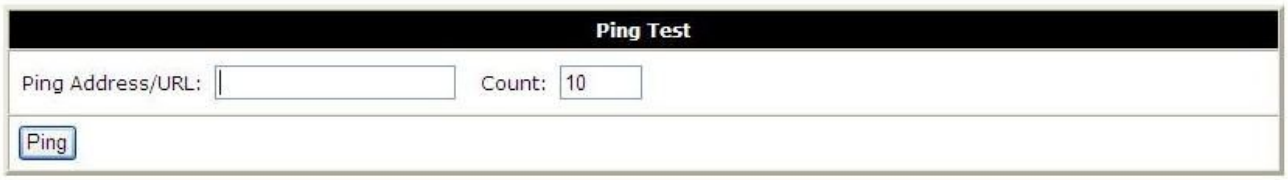
4.3.3. Set Real Time clock

Synchronize the internal clock with time server, or set the time manually.

Where:
Current date and time - actual time and date,
NTP Server Address - server address for clock synchronization,
Enter manually - enter time manually,
Year - Month - Day,
Hours : Minutes : Seconds,
Apply - apply settings.

4.3.4. Ping Test

Checking your Internet connection.



Where:
Ping Address/URL - address,
Count - number of attempts,
Ping - start checking.

4.3.5. Startup Script

Script starts at powering on the device and enables additional settings.

Where:
Run script at startup - run script after startup,
#!/bin/sh - script is to begin with the interpreter indication,
Save Script - save script.

4.3.6. IP-Up Script

Script starts at the device connection to the Internet and enables additional settings.

Where:
Run script when connected - run script after connection to the Internet,
#!/bin/sh - script is to begin with the interpreter indication,
Save Script - save script.

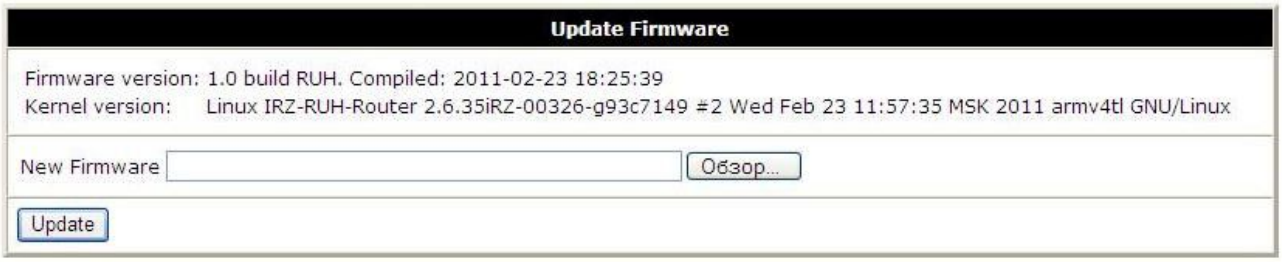
4.3.7. IP-Down Script

Script starts at the device disconnection from the Internet and enables additional settings.

Where:
Run script when disconnected - run script after disconnection from the Internet,
#!/bin/sh - script is to begin with the interpreter indication,
Save Script - save script.

4.3.8. Update Firmware

Internal router software upgrading.



Where:
Firmware Version - internal program current version,
Обзор... - select a file with new program version
Update - execute the update.

4.3.9. Reboot

Router rebooting, reset to factory settings.

Where:
Reset configuration to defaults - at rebooting change to default settings,
The reboot process will take about 60 seconds to complete
Reboot - execute the reboot.

5. Support

New versions of router software and documentation can be found on the company Radiofid site http://radiofid.ru.