Wireless solutions
for M2M world

USER GUIDE

Control and Diagnostic Tools

for the iRZ R-mini Routers:

RU10w, RU11w, RL11w, RL21w

Table of contents

1. Introduction

1.1. About the Document

The document provides information on the diagnostic and control tools for the iRZ routers of R-mini series (RU10w, RU11w, RL11w, RL21w). This document does not contain complete information on the routers operation.

Document version		**Issue date**	
1.0		24.08.2015	
Prepared by:	D. Koroban, V. Golovin	**Checked by:**	D. Koroban, S. Schukin

2. Access Tools

2.1. Router Access

The data required to access the router, is printed on the label at the case bottom.

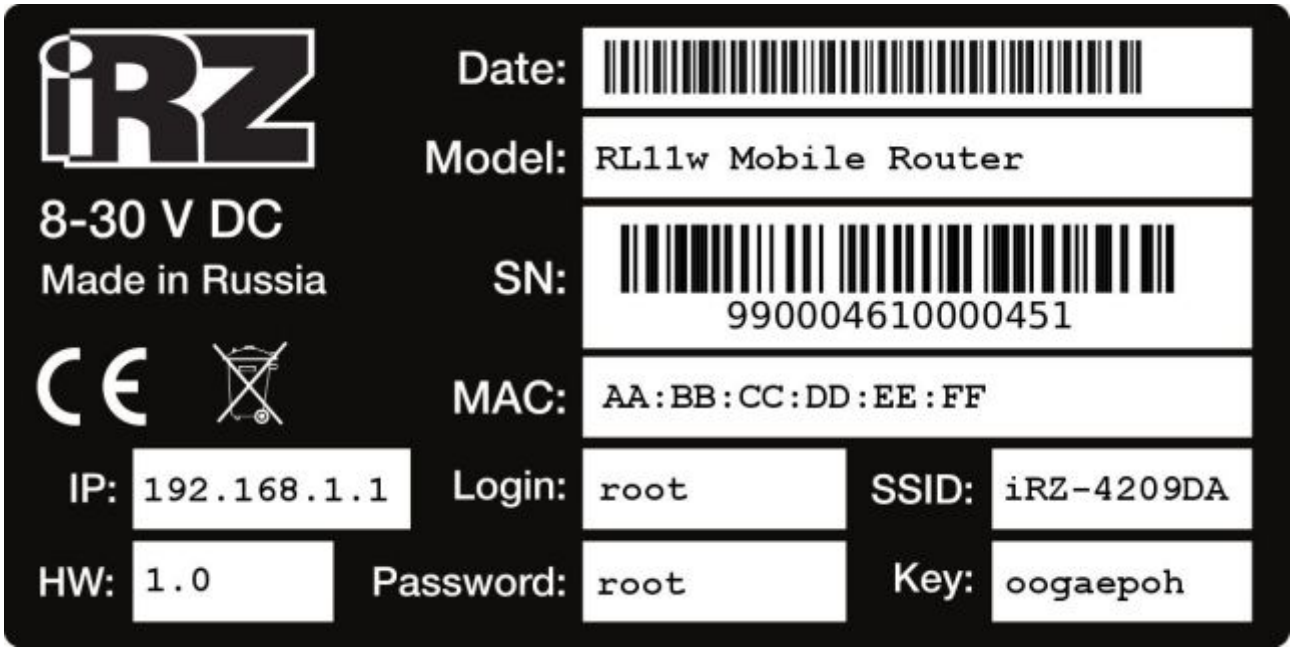

Fig. 1. The label sample (RL11w)

IP (192.168.1.1) — The address to access the router web interface

Login (root) — The user name to access the router

Password (root) — The password to access the router

SSID (iRZ-<6 символов MAC-адреса>) — The access point name for Wi-Fi connection

Key (<8 случайных символов>) — The WPA2-PSK key for Wi-Fi connection

Important! To prevent unauthorized access to the equipment, it is required to change the password. In addition to the web interface-based access, open access to the router via **Telnet** is provided by default. After the password change, **Telnet** is disabled and access via **SSH** is enabled.

2.2. Web Interface Access

To control the routers via web interface, input the router IP address (**192.168.1.1**) in a browser address bar and press **<Enter>**. The router will request a login and a password (**root/root**). After authentication you will get into the device status page.

2.3. Device Access via Telnet/SSH

With a new device or after resetting to factory defaults, the password-free access via **Telnet** (port 23) is provided. After the password change, access via **Telnet** is disabled and the password-based access via **SSH** (port 22) is enabled. It is strongly recommended to change the password via web interface at the first configuration of the device. For Windows it is recommended to use the **Putty Telnet/SSH** client (http://www.putty.org/).

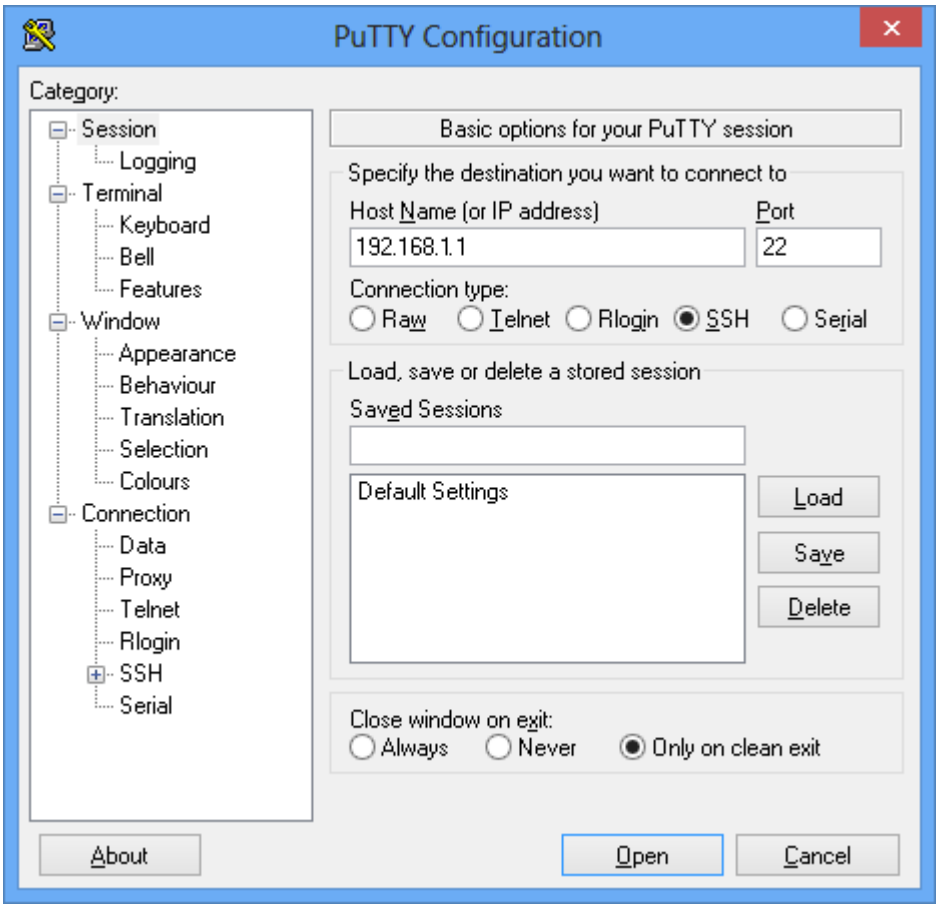

Fig. 2. PuTTY configuration window

In the **Host Name (or IP address)** field enter the router IP address **(192.168.1.1)**, select the type of connection (Telnet or SSH) in **Connection type** and click **Open**. For Ssh-connection you need to specify the login and password (**root**/**root**). After logging in, you will see the command prompt of the **root@iRZ-Router:/#** form

3. Web Interface Overview

3.1. Web interface: Status

The status page displays basic data on the router interfaces: LAN, WAN и Mobile.

LAN — local network interface. Status (Status: Up/Down) and address (Address: 192.168.1.1) are displayed. The interface can be configured on the **Networking** → **Local Network** page.

WAN — external network interface (Internet). Status (Status: Up/Down) and address (Address: 172.16.84.4/30) are displayed. The interface can be configured on the **Networking** → **Wired Internet** page.

Mobile Internet — The interface of wireless mobile network. Status (Status: Up/Down), operator code or name (Operator: 25001), address (Address: 10.154.208.137/32), connection mode (Mode: WCDMA) and signal strength on the scale from 0 to 31 (CSQ: 27) are displayed. The interface can be configured on the **Networking** → **Mobile Internet** page.

If both WAN and Mobile Internet interfaces are enabled at the same time, the router will automatically switch to the wireless link in the event of wired connection failure. The interface used at a given moment is specified as **Active**.

3.2. Web interface: Networking → Wired Internet

Conection Type — The type of connection. Possible options:

DHCP — Automatically receives settings via DHCP. Additional configuration is not required.

PPPoE — Establishes connection via PPPoE. A login and a password may be required.

Static — Configures interface manually. IP address, network mask, gateway and DNS server addresses need to be specified.

Disabled — WAN port is used as the second LAN port.

MAC — Specify the interface MAC address. Leave it blank to use the standard value.

Show Failover Settings — oDisplays settings of automatic switching to the wireless connection. If both WAN and Mobile Internet interfaces are enabled at the same time, the router will automatically switch to the wireless link in the event of wired connection failure. A verification address and a verification interval can be configured.

Ping address — The address to be verified by the ping command.

Ping interval — The interval between the verifications in seconds.

3.3. Web interface: Networking → Mobile Internet

Enable Mobile Internet — Enables the mobile Internet.

PIN — Specify a PIN code if a card is protected.

Show advanced settings — Shows advanced settings.

APN — The access point. Identified automatically if the field is blank.
Username — The user name.

Password — The password.

Additional pppd options — Additional pppd daemon options.

3.4. Web interface: Networking → Local Network

Local Address — The local network interface settings.

IP — The router address in the local network (192.168.1.1).

Mask — The network mask (255.255.255.0).

WiFi — The wireless network settings.

Enable WiFi — Enables wireless network.

SSID — The wireless network name.

Channel — The number of a network channel.

Hide wireless network — Stops broadcasts from the access point of the SSID (Wireless Network Name).

Access mode — The type of network protection:

Open — Insecure open network;

WPA — wireless network is secured with WPA encryption;
WPA2-PSK — Wireless network is secured with WPA2-PSK encryption (recommended).

Password — The key to access wireless network.

3.5. Web interface: Networking → PPTP Client

Enable PPTP Client — Enables the VPN Client.

Server — The address of the server you need to connect.

Username — The user name.

Password — The password.

Authentication Protocol — Authentication methods:
MPPE — Microsoft Point-to-Point Encryption;
PAP — Password Authentication Protocol;
CHAP — Challenge Handshake Authentication Protocol.

Additional Options — Additional pppd daemon options.

3.6. Web interface: Networking → OpenVPN Tunnel

Enable OpenVpn Tunnel — Enables OpenVpn Tunnel.

Device — The device type:
TAP (L2) — Datalink layer;
TUN (L3) — Network layer.

Transport protocol — Connection protocol type:
UDP — UDP protocol;
TCP Server — TCP protocol, the router is waiting for incoming connections;
TCP Client — TCP protocol, the router is establishing outgoing connection.

Remote — IP address of a remote device.

Port — Port number.

Local VPN endpoint IP address — The address of a tunnel local endpoint (10.8.0.1);

VPN subnet mask — The mask of virtual network (255.255.255.0) (only for L2 datalink layer, TAP device).

Remote VPN endpoint IP address — The address of a tunnel remote endpoint (10.8.0.1) (only for L3 network layer, TUN device).

Authentication method — Authentication methods:
None — Without authentication;
Shared secret — The public key;
TLS Server — Certificate, server;
TLS Client — Certificate, client.

Shared secret — The field to enter the public key.

Ca Certificate — The field to enter the root certificate.

DH Parameter — The field to enter the Diffie-Hellman parameters.

Local Certificate — The field to enter the device certificate.

Local private key — The field to enter the device key.

Show advanced settings — Shows advanced settings.

Remote Subnet — The address of a remote network.

Remote Subnet Mask — The subnet mask of the remote IP address.

Ping interval — The interval to verify tunnel in seconds.

Ping timeout — The tunnel reset interval.

LZO Compression — The LZO compression mode:
Adaptive;
Always — Always enabled;
No — Always disabled.

Additional config — Additional openvpn daemon options.

3.7. Web interface: Services → DHCP

Enable DHCP server — Enables the DHCP service for automatic distribution of IP addresses to the devices in a local network.

Pool start — The first address of the DHCP pool.

Pool size — The DHCP pool size.

Static Leases — The static addresses (all three fields need to be filled!):

- **Hostname** — The client name.
- **MAC** — The client MAC address.
- **IP** — The IP address assigned to the client.

By default, the router has **192.168.1.1** address and **255.255.255.0** mask. If **Pool Start** is set to **100**, the first pool address is **192.168.1.100**. If **Pool Start** is set to **150**, the last pool address is **192.168.1.250**.

3.8. Web interface: Services → MAC Filter

Enable MAC Filter — Enables filtering of wireless clients by MAC address.

Filter Mode — The filtering mode:
Black list — Disables specified IP addresses, enables others;
White list — Enables specified IP addresses, enables others.

Comment.

MAC — The client MAC address.

3.9. Web interface: Services → Time

Current Time.

Time Source — The time source:
NTP — The accurate time servers (the Internet access is required);

Manual — The manual time setting.

Primary NTP server — The primary NTP server

Secondary NTP server — The secondary NTP server.

Time zone — The local time zone.

3.10. Web interface: Services → Port Forwarding

By default, the router does not receive any incoming connections from the external network (Internet). To gain access to the router or devices behind it in the local network, port forwarding needs to be configured.

Important! To activate port forwarding, the router must have an external static IP address.

Protocol — Connection protocol:
tcp — only TCP ;
udp — only UDP;
tcpudp — TCP and UDP.

Source Port — The router port to which connection is established.

Dest Port — The port on the router or in the network behind it to which connection is forwarded.

Dest IP — The IP address to which connection is forwarded.

Comment.

Example 1.

The router has an external static IP **1.2.3.4** and an internal IP **192.168.1.1.** When connecting to the external address on port **8181**, web interface needs to be open. The settings will be as follows:
Protocol = TCP
Source Port = 8181
Dest Port = 80
Dest IP = 192.168.1.1
Comment = Remote web access

The remote access address is http://1.2.3.4:8181/

Example 2.

The router has an external static IP **1.2.3.4** and an internal IP **192.168.1.1**. It is required to forward the OpenVPN tunnel from port **9191** to the device with the **192.168.1.110** address. Let us say that OpenVPN uses the UDP protocol, the incoming connection is expected on port **1194**. The settings will be as follows:

Protocol = UDP Source Port = 9191

Dest Port = 1194

Dest IP = 192.168.1.110

Comment = OpenVPN tunnel

OpenVPN client parameters:

Server = 1.2.3.4

Port = 9191

3.11. Web interface: Tools → Change Password

Old password — старый пароль для проверки полномочий

New password — новый пароль

Confirm password — повтор нового пароля для исключения опечаток

Important! To prevent unauthorized access to the equipment, it is required to change the password. In addition to the web interface-based access, open access to the router via **Telnet** is provided by default. After the password change, Telnet is disabled and access via SSH is enabled.

If you have forgotten the password, you need to reset the router. For this purpose press and hold down the **RST** button for about 10 seconds.

3.12. Web interface: Tools → Ping

Verification of the device remote access via the ping utility.

Host — The IP address of a remote device.

Count — The number of requests.

Datagram size — The packet size.

3.13. Web interface: Tools → System log

The log of device operation. When you contact the technical support service, use the **System Report** button to generate report and attach the resulting file to a letter.

3.14. Web interface: Tools → Reboot

Use the **Reboot** button to restart the router.

Perform Factory Reset — Resets the router to the factory defaults before rebooting.

3.15. Web interface: Tools → Management

Backup Settings — Saves the router current settings into a file.

Restore Settings — Restores previously saved settings. Select the settings file and press the **Restore** button.

Update Firmware — Updates the router software. Click "**Browse...**" and select previously downloaded update file and click **Update**. Click **Return to Main Menu** at the top of the page to get back to the main menu.

4. Contacts and Support

To get a new firmware, documentation and companion software versions, please apply at the following contacts:

The company's website:	www.irz.net
Phone number in St. Petersburg:	+7 (812) 318 18 19
e-mail:	support@radiofid.ru

Our specialists are always ready to answer your questions, assist in installation or configuration, and solve problems regarding the equipment operation.

In case of a problem with the router, specify the software version to the support service. Besides, we recommend you to attach a log of problem services, screenshots of settings, and any other useful information to a letter. The more information you will provide to a specialist, the more immediate solution to your problem you will get.

Note: Before applying to the technical support it is required to update your router firmware up to a current version.