

 **Описание средств
управления и мониторинга
RU10w, RU11w,
RL11w, RL12w**





Содержание

1. Введение	3
1.1. Описание документа	3
2. Средства доступа	4
2.1. Доступ к роутеру	4
2.2. Доступ к Web-интерфейсу	4
2.3. Доступ к устройству через Telnet/SSH.....	5
3. Описание web-интерфейса	6
3.1. Web-интерфейс: Status	6
3.2. Web-интерфейс: Networking → Wired Internet	6
3.3. Web-интерфейс: Networking → Mobile Internet	7
3.4. Web-интерфейс: Networking → Local Network	7
3.5. Web-интерфейс: Networking → PPTP Client	8
3.6. Web-интерфейс: Networking → OpenVPN Tunnel.....	8
3.7. Web-интерфейс: Services → DHCP	10
3.8. Web-интерфейс: Services → MAC Filter.....	10
3.9. Web-интерфейс: Services → Time	10
3.10. Web-интерфейс: Services → Port Forwarding	11
3.11. Web-интерфейс: Tools → Change Password.....	12
3.12. Web-интерфейс: Tools → Ping.....	14
3.13. Web-интерфейс: Tools → System log.....	14
3.14. Web-интерфейс: Tools → Reboot.....	14
3.15. Web-интерфейс: Tools → Management.....	14
4. Контакты и поддержка	15



1. Введение

1.1. Описание документа

Данный документ описывает средства диагностики и управления роутеров iRZ серии R-mini (RU10w, RU11w, RL11w, RL21w). Данный документ не содержит всей информации по работе с роутером.

Версия документа		Дата публикации	
1.0.1		13.11.2014	
Подготовлено:	Коробань Д.С., Головин В.Н.	Проверено:	Коробань Д.С., Щукин С.Л.



2. Средства доступа

2.1. Доступ к роутеру

Данные, необходимые для доступа к роутеру напечатаны на наклейке на нижней части корпуса.

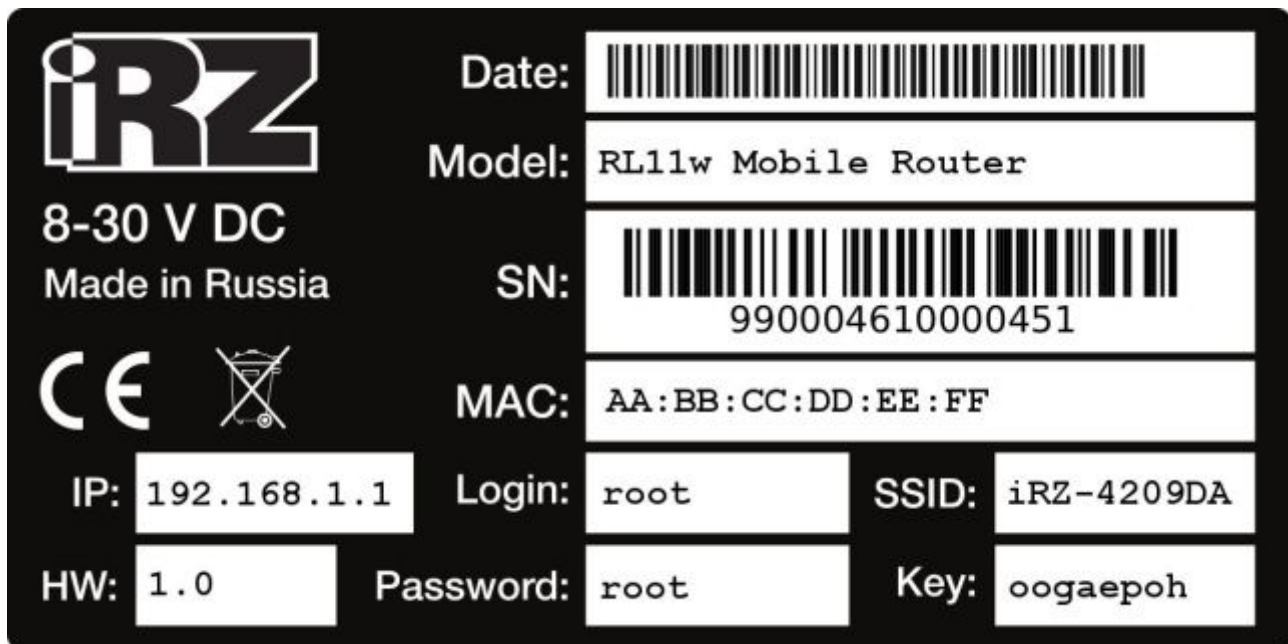


Рис. 1. Образец наклейки (RL11w)

IP (192.168.1.1) — адрес, по которому доступен web-интерфейс роутера

Login (root) — имя пользователя для доступа к роутеру

Password (root) — пароль для доступа к роутеру

SSID (iRZ-<6 символов MAC-адреса>) — имя точки доступа для WiFi-подключения

Key (<8 случайных символов>) — WPA2-PSK ключ для WiFi-подключения

Важно! Для предотвращения несанкционированного доступа к оборудованию обязательно смените пароль. Помимо доступа через web-интерфейс по умолчанию имеется открытый доступ к устройству по протоколу **Telnet**. После смены пароля **Telnet** отключается и включается доступ по **SSH**.

2.2. Доступ к Web-интерфейсу

Для управления роутером через web-интерфейс впишите в адресной строке браузера IP-адрес роутера (**192.168.1.1**) и нажмите **<Enter>**. Роутер запросит логин и пароль (**root/root**). После авторизации вы попадёте на страницу статуса устройства.



2.3. Доступ к устройству через Telnet/SSH

На новом устройстве или после сброса настроек к заводским открыт доступ по протоколу **Telnet** (порт 23) без пароля. После смены пароля доступ через **Telnet** отключается, и включается защищённый паролем доступ по **SSH** (порт 22). Настоятельно рекомендуем сменить пароль через web-интерфейс при первой же настройке устройства. Для Windows рекомендуется использовать Telnet/SSH клиент **Putty** (<http://www.putty.org/>).

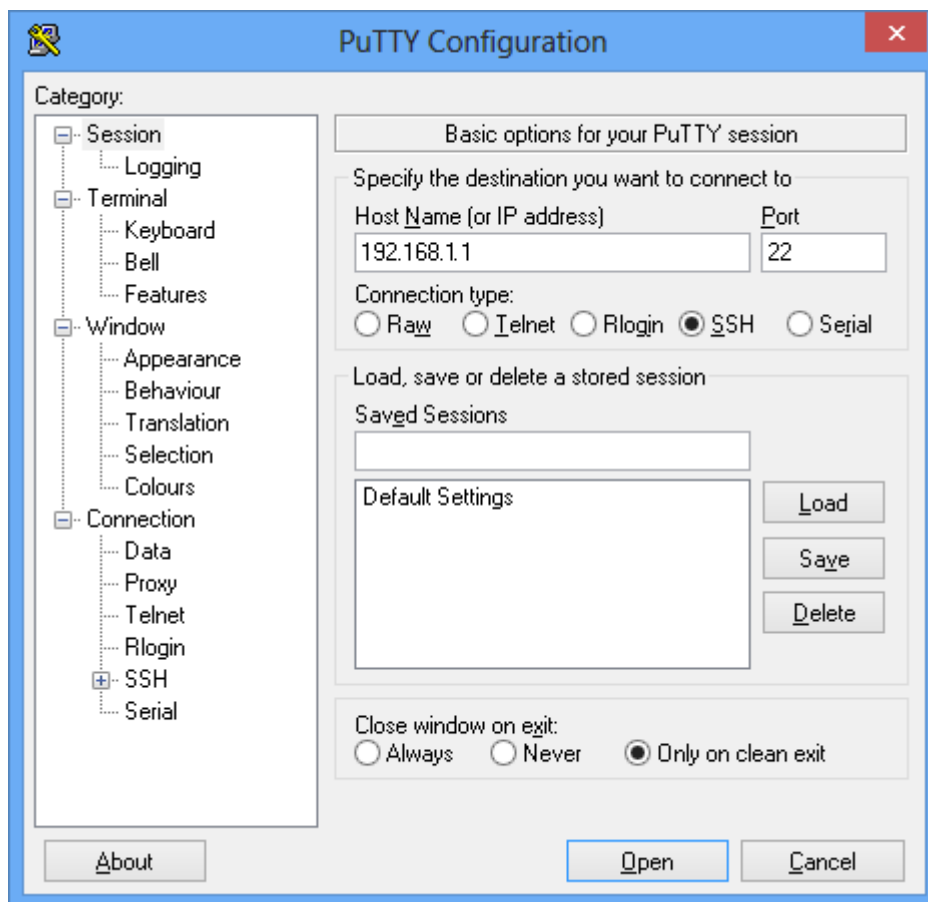


Рис. 2. Окно настройки программы PuTTY

В поле **Host Name (or IP address)** введите IP-адрес роутера (**192.168.1.1**), выберите тип подключения (Telnet или SSH) в строке **Connection type** и нажмите кнопку **Open**. Для Ssh-подключения потребуется указать логин и пароль (**root/root**). После входа в систему вы увидите приглашение командной строки вида **root@iRZ-Router:/#**



3. Описание web-интерфейса

3.1. Web-интерфейс: Status

На странице статуса отображаются основные данные об интерфейсах роутера: LAN, WAN и Mobile.

LAN — интерфейс локальной сети. Отображается состояние (Status: Up/Down) и адрес (Address: 192.168.1.1). Настроить интерфейс можно на странице **Networking** → **Local Network**.

WAN — интерфейс внешней сети (Internet). Отображается состояние (Status: Up/Down) и адрес (Address: 172.16.84.4/30). Настроить интерфейс можно на странице **Networking** → **Wired Internet**.

Mobile Internet — интерфейс беспроводной мобильной сети. Отображается состояние (Status: Up/Down), код или название оператора (Operator: 25001), адрес (Address: 10.154.208.137/32), режим соединения (Mode: WCDMA) и уровень сигнала по шкале от 0 до 31 (CSQ: 27). Настроить интерфейс можно на странице **Networking** → **Mobile Internet**.

Если одновременно включены WAN и Mobile Internet, то роутер будет автоматически переключаться на беспроводной канал в случае отказа проводного соединения. Используемый в данный момент интерфейс помечен строкой **(Active)**.

3.2. Web-интерфейс: Networking → Wired Internet

Conection Type — тип соединения. Возможные варианты:

DHCP — автоматически получить настройки по протоколу DHCP. дополнительных настроек не требуется.

PPPoE — установить соединение через PPPoE. Могут потребоваться логин и пароль.

Static — вручную настроить интерфейс. Необходимо задать IP-адрес, маску сети, адреса шлюза и DNS-сервера.

Disabled — порт WAN используется как второй порт LAN.

MAC — установить MAC-адрес интерфейса. Оставьте пустым чтобы использовать стандартное значение.

Show failover settings — отобразить настройки автоматического переключения на беспроводное соединение. Если одновременно включены WAN и Mobile Internet, то роутер будет автоматически переключаться на беспроводной канал в случае отказа проводного соединения. Проверочный адрес и интервал проверки можно настроить.



Ping address — адрес, который будет проверяться командой ping.

Ping interval — интервал между проверками в секундах.

3.3. Web-интерфейс: Networking → Mobile Internet

Enable Mobile Internet — включить мобильный интернет.

PIN — Укажите здесь PIN-код, если карта защищена.

Show advanced settings — показать дополнительные настройки.

APN — точка доступа. Определяется автоматически, если поле пустое.

Username — имя пользователя.

Password — пароль.

Additional pppd options — дополнительные параметры демона pppd.

3.4. Web-интерфейс: Networking → Local Network

Local Address — настройки интерфейса локальной сети.

IP — адрес роутера в локальной сети (192.168.1.1).

Mask — маска сети (255.255.255.0).

WiFi — настройки беспроводной сети.

Enable WiFi — включить беспроводную сеть.

SSID — имя беспроводной сети.

Channel — номер канала для сети.

Hide wireless network — не передавать название сети в эфир.



Access mode — тип защиты сети:

- Open — открытая сеть без защиты;
- WPA — шифрование WPA;
- WPA2-PSK — шифрование WPA2-PSK (рекомендуется).

Password — ключ доступа к сети.

3.5. Web-интерфейс: Networking → PPTP Client

Enable PPTP Client — включить клиент PPTP.

Server — IP-адрес сервера, к которому нужно подключиться.

Username — имя пользователя.

Password — пароль.

Authentication Protocol — методы авторизации.

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

Additional Options — дополнительные параметры сервиса rppd.

3.6. Web-интерфейс: Networking → OpenVPN Tunnel

Enable OpenVpn Tunnel — включить туннель OpenVPN.

Device - тип устройства:

- TAP (L2) — Канальный уровень;
- TUN (L3) — Сетевой уровень.

Transport protocol — тип протокола соединения:

- UDP — протокол UDP;
- TCP Server - протокол TCP, роутер ждёт входящих соединений;
- TCP Client — протокол TCP, роутер устанавливает исходящее соединение.

Remote — IP-адрес удалённого устройства.



Port — номер порта.

Local VPN endpoint IP address — адрес локального конца туннеля (10.8.0.1);

VPN subnet mask — маска виртуальной сети (255.255.255.0) (только для канального уровня L2, устройство TAP).

Remote VPN endpoint IP address - адрес удалённого конца туннеля (10.8.0.2) (только для сетевого уровня L3, устройство TUN).

Authentication method — метод авторизации:

None — без авторизации;

Shared secret — общий ключ;

TLS Server — сертификат, сервер;

TLS Client — сертификат, клиент.

Shared secret — поле для ввода общего ключа.

Ca Certificate — поле для ввода корневого сертификата.

DH Parameter — поле для ввода параметров Diffie-Hellman.

Local Certificate — поле для ввода сертификата устройства.

Local private key — поле для ввода ключа устройства.

Show advanced settings — показать дополнительные настройки.

Remote Subnet — адрес удалённой сети.

Remote Subnet Mask — маска удалённой сети.

Ping interval — интервал проверки туннеля в секундах.

Ping timeout — интервал, по истечении которого туннель переустанавливается.

LZO Compression — режим LZO-сжатия:

Adaptive — адаптивный;

Always — всегда включено;



No — всегда выключено.

Additional config — дополнительные параметры демона openvpn.

3.7. Web-интерфейс: Services → DHCP

Enable DHCP server — включить сервис DHCP для автоматической раздачи IP-адресов устройствам в локальной сети.

Pool start — первый адрес пула DHCP.

Pool size — размер пула DHCP.

Static Leases — фиксированные адреса (необходимо заполнить все три поля!):

- **Hostname** — имя клиента.
- **MAC** — MAC-адрес клиента.
- **IP** — назначенный клиенту IP.

По умолчанию роутер имеет адрес **192.168.1.1** и маску **255.255.255.0**. Если **Pool Start** задан **100**, то первый адрес пула будет **192.168.1.100**. Если **Pool Size** задан **150**, то последний адрес пула будет **192.168.1.250**.

3.8. Web-интерфейс: Services → MAC Filter

Enable MAC Filter — включить фильтрацию беспроводных клиентов по MAC-адресу.

Filter Mode — режим фильтрации:

Black list — запретить указанные, разрешить остальные;

White list — разрешить указанные, запретить остальные.

Comment — комментарий.

MAC — MAC-адрес клиента.

3.9. Web-интерфейс: Services → Time



Current Time — текущее время.

Time Source — источник времени:

NTP — серверы точного времени (необходим доступ в интернет);

Manual — ручная настройка.

Primary NTP server — основной NTP-сервер

Secondary NTP server — дополнительный NTP-сервер.

Time zone — местная временная зона.

3.10. Web-интерфейс: Services → Port Forwarding

По умолчанию роутер не принимает никакие входящие соединения из внешней сети (интернет). Чтобы получить доступ к роутеру или устройствам в локальной сети за ним необходимо настроить проброс портов.

Важно! Для того, чтобы проброс портов работал, роутер должен иметь внешний статический IP-адрес.

Protocol — протокол соединения:

tcp — только TCP;

udp — только UDP;

tcpudp — TCP и UDP.

Source Port — порт на роутере, к которому устанавливается соединение.

Dest Port — порт на роутере или в сети за ним, к которому будет проброшено соединение.

Dest IP — IP-адрес, к которому будет проброшено соединение.

Comment — комментарий.

Пример 1.



Роутер имеет внешний статический IP **1.2.3.4** и внутренний IP **192.168.1.1**. Необходимо, чтобы при подключении к внешнему адресу на порт **8181** открывался web-интерфейс. Настройки будут такие:

Protocol = TCP
Source Port = 8181
Dest Port = 80
Dest IP = 192.168.1.1
Comment = Remote web access

Адрес для удалённого доступа будет <http://1.2.3.4:8181/>

Пример 2.

Роутер имеет внешний статический IP **1.2.3.4** и внутренний IP **192.168.1.1**. Необходимо, пробросить туннель OpenVPN с порта **9191** на устройство с адресом **192.168.1.110**. Считаем, что OpenVPN использует протокол UDP, входящее соединение ожидается на порт **1194**. Настройки будут такие:

Protocol = UDP
Source Port = 9191
Dest Port = 1194
Dest IP = 192.168.1.110
Comment = OpenVPN tunnel

Параметры для клиента OpenVPN:

Сервер = 1.2.3.4
Порт = 9191

3.11. Web-интерфейс: Tools → Change Password

Old password — старый пароль для проверки полномочий

New password — новый пароль

Confirm password — повтор нового пароля для исключения опечаток

Важно! Для предотвращения несанкционированного доступа к оборудованию обязательно смените пароль. Помимо доступа через web-интерфейс по умолчанию имеется открытый доступ к устройству по протоколу **Telnet**. После смены пароля **Telnet** отключается и включается доступ по **SSH**.

Если вы забыли пароль, необходимо сбросить настройки роутера. Для этого удерживайте кнопку RST на задней панели устройства нажатой примерно 10 секунд.





3.12. Web-интерфейс: Tools → Ping

Проверка доступности удалённого устройства с помощью утилиты ping.

Host — IP-адрес удалённого устройства.

Count — количество запросов.

Datagram size — размер пакета.

3.13. Web-интерфейс: Tools → System log

Журнал работы устройства. Обращаясь в службу технической поддержки используйте кнопку **System report** для генерации отчёта и приложите полученный файл к письму.

3.14. Web-интерфейс: Tools → Reboot

Используйте кнопку **Reboot** для перезагрузки роутера.

Perform factory reset — сбросить настройки к заводским перед перезагрузкой.

3.15. Web-интерфейс: Tools → Management

Backup settings — сохранить текущие настройки роутера в файл.

Restore settings — восстановить сохранённые ранее настройки. Выберите файл с настройками и нажмите кнопку **Restore**.

Update firmware — обновление программного обеспечения роутера. Нажмите «Обзор...» и выберите заранее скачанный файл обновления и нажмите кнопку **Update**. Для возврата в основное меню нажмите на ссылку «Return to main menu» вверху страницы.



4. Контакты и поддержка

Новые версии прошивок, документации и сопутствующего программного обеспечения можно получить, обратившись по следующим контактам:

сайт компании в Интернете:	www.radiofid.ru
тел. в Санкт-Петербурге:	+7 (812) 318 18 19
e-mail:	support@radiofid.ru

Наши специалисты всегда готовы ответить на все Ваши вопросы, помочь в установке, настройке и устранении проблемных ситуаций при эксплуатации оборудования.

В случае возникновения проблемной ситуации, при обращении в техническую поддержку, следует указывать версию программного обеспечения, используемого в роутере. Так же рекомендуется к письму прикрепить журналы запуска проблемных сервисов, снимки экранов настроек и любую другую полезную информацию. Чем больше информации будет предоставлено сотруднику технической поддержки, тем быстрее он сможет разобраться в сложившейся ситуации.

Примечание: Перед обращением в техническую поддержку настоятельно рекомендуется обновить программное обеспечение роутера до актуальной версии.