

■ Описание средств
управления и мониторинга
**RUH, RUH2, RUH2b,
RUH3, RCA**





Содержание

1. Введение	5
1.1. Описание документа	5
1.2. Обзор пакета инструкций	5
1.3. Предупреждение	6
1.4. Термины и сокращения	6
2. Способы управления роутером iRZ	8
3. Быстрый доступ к устройству	9
4. Возвращение к заводским настройкам	11
5. Web-интерфейс. Раздел «Configuration»	12
5.1. Страница Internet.....	12
5.2. Страница LAN.....	14
5.2.1. Раздел «Local Ethernet Interface»	14
5.2.2. Раздел «USB Ethernet Interface»	14
5.2.3. Раздел «Reserve Link»	15
5.2.4. Раздел «DHCP Server».....	15
5.3. Страница Port Forwarding.....	16
5.4. Страница Static Routes	17
5.5. Страница VRRP	18
5.6. Страница Firewall.....	19
5.7. Страница SNMP	20
5.8. Страница GRE	20
5.9. Страница OpenVPN Tunnel	22
5.10. Страница OpenVPN Server.....	24
5.11. Страница IPSec	25
5.12. Страница L2TP	29
5.13. Страница Serial Port	30
5.14. Страница DynDNS	31
5.15. Страница NTP.....	32
5.16. Страница SMS.....	33
5.17. Страница Daily Reboot.....	34
6. Web-интерфейс. Раздел «Status and log»	35
6.1. Страница Internet.....	35



7. Web-интерфейс. Раздел «Administration»	36
7.1. Страница Change Password	36
7.2. Страница Backup/Restore	36
7.3. Страница Set Real Time Clock	37
7.4. Страница Remote access	37
7.5. Страница Unit name	37
7.6. Страница Ping Test	38
7.7. Страница System Log	38
7.8. Страница Startup Script	39
7.9. Страница IP-Up Script	39
7.10. Страница IP-Down Script	39
7.11. Страница User Crontab	39
7.12. Страница Upload File	40
7.13. Страница Send SMS	40
7.14. Страница Disable PIN	40
7.15. Страница Send Report	41
7.16. Страница Update Firmware	41
7.17. Страница Reboot	42
8. Настройка доступа к устройству	43
8.1. Настройка удаленного доступа	43
8.2. Управление с помощью команд консоли Telnet/SSH	44
8.2.1. Удаленное управление по Telnet	44
8.2.2. Удаленное управление по SSH	44
9. Контакты и поддержка	45
Приложение 1	46
Синтаксис IP-адреса	46
Синтаксис IP-адреса сети	46
Синтаксис маски подсети	46
Синтаксис MAC-адреса	46
Приложение 2	47
Доступные команды управления	47



Перечень таблиц

Таблица 2.1	Сетевые службы, используемые для управления роутером.....	8
Таблица 5.1	Настройка доступа к сети Интернет (для каждой SIM-карты)	12
Таблица 5.2	Настройка интерфейса Ethernet.....	14
Таблица 5.3	Настройка интерфейса USB-Ethernet.....	14
Таблица 5.4	Настройка резервирования интернет-соединения	15
Таблица 5.5	Настройка DHCP-сервера	15
Таблица 5.6	Настройка перенаправления трафика	16
Таблица 5.7	Настройка правил статической маршрутизации трафика	17
Таблица 5.8	Настройка параметров VRRP.....	18
Таблица 5.9	Настройка параметров межсетевого экрана.....	19
Таблица 5.10	Настройка параметров службы SNMP	20
Таблица 5.11	Настройка включения GRE-туннелей.....	21
Таблица 5.12	Настройка параметров GRE-туннеля.....	21
Таблица 5.13	Настройка параметров OpenVPN-туннеля.....	22
Таблица 5.14	Настройка параметров сервера OpenVPN.....	24
Таблица 5.15	Настройка параметров IPSec-туннеля	26
Таблица 5.16	Настройка параметров L2TP-туннеля.....	29
Таблица 5.17	Настройка параметров COM-портов	30
Таблица 5.18	Настройка параметров DynDNS-клиента	31
Таблица 5.19	Настройка параметров NTP-клиента	33
Таблица 6.1	Описание показателей страницы «Internet»	35
Таблица 7.1	Настройка параметров доступа к роутеру	36

Перечень рисунков

Рис. 3.1	Ввод IP-адреса роутера в адресную строку интернет-браузера	9
Рис. 3.2	Ввод логина и пароля для доступа к web-интерфейсу роутера	9
Рис. 4.1	Индикатор загрузки и кнопка «Сброс» на корпусе роутера	11
Рис. 5.1	Создание IPSec-туннеля.....	26
Рис. 6.1	Пример содержания страницы «Internet» в разделе «Status and log»	35
Рис. 8.1	Пример организации доступа. Открыт доступ к сервисам: HTTP (порт 8080), SSH (порт 2222), Telnet (порт 2323), SNMP (порт 9025).....	43



1. Введение

1.1. Описание документа

Данный документ является частью пакета инструкций по обслуживанию роутера iRZ и содержит информацию только по средствам мониторинга и управления устройством. Для получения более подробной информации о работе с устройством см. «Пакет инструкций по обслуживанию роутера iRZ».

Версия документа (Дата публикации)		Изменения	
1.0.1 (26.06.2013)		Основной документ	
1.0.2 (11.09.2015)		Актуализация ссылок на родственные документы	
Выполнил		Проверил	

1.2. Обзор пакета инструкций

Содержание «Пакета инструкций по обслуживанию роутера iRZ»:

- Руководство по эксплуатации роутера iRZ;
- **Описание средств управления и мониторинга роутера iRZ;**
- Диагностика и методы устранения неисправностей роутера iRZ;
- Руководство по настройке роутера iRZ с помощью USB-накопителя;
- Примеры рабочих конфигураций роутера iRZ:
 - Создание виртуальных сетей и туннелей средствами OpenVPN;
 - Удалённый доступ к COM-порту роутера;
 - Защита передаваемых данных средствами IPSec;
 - DynDNS и обход ограничений внешнего динамического IP-адреса;
 - Объединение сетей с помощью GRE-туннелей;
 - Отказоустойчивость уровня сети средствами VRRP;
 - Обеспечение доступа к внутрисетевым службам средствами PortForwarding;
 - Защита локальной сети и сервисов средствами встроенного Firewall;
- Технические условия (ТУ);
- Протокол температурных испытаний;
- Декларация о соответствии.



1.3. Предупреждение

Примечание. Для каждой модели роутера существует своя версия комплекта документации. Обращайтесь, пожалуйста, к документации для Вашего устройства.

Внимание! Нарушение условий эксплуатации роутера лишает Вас права на гарантийное обслуживание устройства.

Предупреждение:

- Рекомендуется уделить особое внимание разделу «Настройка доступа к устройству», посвященному предоставлению доступа к роутеру. При нарушении описанных рекомендаций возможна угроза несанкционированного доступа к роутеру, сетям и другому сетевому оборудованию со стороны третьих лиц.
- Параметры конфигурации следует вводить в полном соответствии с рекомендациями данного документа. Например, для IP-адреса:
Корректно: 123.213.132.001
Некорректно: 123,456.789.000, 123..456.789.000, 12 3.456.789.000
- Все поля настроек роутера необходимо заполнять только на английском языке.

1.4. Термины и сокращения

OpenVPN – открытый бесплатный программный продукт, позволяющий создать защищенную виртуальную среду передачи данных внутри IP-сети. Представляет собой многофункциональный программный пакет, поэтому термин «OpenVPN» может иметь различные значения. Например, наиболее распространены следующие:

- сервер доступа к сети OpenVPN;
- клиент, позволяющий подключиться к сети OpenVPN;
- сеть, сектор, уровень или слой сети, подразумевающие использование программного обеспечения OpenVPN.

Роутер – маршрутизатор iRZ RUH(2)/RCA/RC1 Router.

3G – общее название для набора стандартов, описывающих работу в сетях UMTS и GSM: GPRS, EDGE, HSPA.

Сервер – термин, использующийся для обозначения следующих понятий:

- серверная часть программного пакета, используемого в вычислительном комплексе;
- роль компонента или объекта в структурно-функциональной схеме технического решения, развертываемого с использованием роутера iRZ;
- компьютер, предоставляющий те или иные сервисы (сетевые службы, службы обработки и хранения данных и т.д.).



Техническое решение – идея или документ, которые описывают набор технических мероприятий, направленных на реализацию конкретной задачи. Для выполнения такой задачи используются функциональные возможности компонентов решения, связанных между собой и взаимодействующих друг с другом определенным образом.

Внешний IP-адрес – IP-адрес в сети Интернет, предоставляемый компанией-провайдером услуг связи в пользование клиенту на своем или его оборудовании для обеспечения прямой связи с оборудованием клиента через сеть Интернет.

Фиксированный внешний IP-адрес – внешний IP-адрес, не изменяющийся ни при каких условиях (при смене типа оборудования клиента и т.п.) или событиях (при переподключении к сети компании-провайдера и т.д.). Единственной возможностью изменить фиксированный IP-адрес является обращение в компанию-провайдер.

Аутентификация – процедура проверки подлинности пользователя, клиента или узла, во время которой реквизиты, предоставленные на момент подключения, сравниваются с реквизитами в базе данных.

RXX – обозначение линейки моделей роутеров iRZ, включающей:

- iRZ RC1,
- iRZ RCA,
- iRZ RUH,
- iRZ RUH2,
- iRZ RUH2b,
- iRZ RUH3.

Web-интерфейс роутера – встроенное средство управления, позволяющее настраивать и контролировать работу роутера через любой стандартный интернет-браузер.

HW VSP – сокращенное название программы HW Virtual Serial Port, позволяющей добавить в операционную систему виртуальный COM-порт и перенаправлять данные с этого порта через TCP/IP-сеть на заданный IP-адрес и порт физического интерфейса.

Удаленное устройство (удаленный узел) – устройство, территориально удаленное от рассматриваемого места, объекта или узла.



2. Способы управления роутером iRZ

Внимание! Рекомендуется уделить особое внимание настройкам доступа к устройству по протоколам HTTP, Telnet, SSH. От сложности паролей, разрешения удаленного доступа, используемых портов сетевых служб, настроек межсетевого экрана и других настроек сетевых служб зависит безопасность не только самого роутера, но и устройств и сетей, находящихся за ним.

Таблица 2.1 Сетевые службы, используемые для управления роутером

Название	Описание	Требуемое ПО
HTTP	Web-интерфейс, позволяющий настроить все регламентированные функции роутера. Можно использовать любой стандартный интернет-браузер.	Интернет-браузер - Opera, Firefox, IE, Chrome, Safari и т.д.
Telnet	Командная консоль, предназначенная для более тонкой настройки устройства. Позволяет использовать стандартные команды Linux.	Telnet-клиент - присутствует во всех ОС (в Windows 7 требуется включить).
SSH	Аналог Telnet, в котором шифруется трафик при авторизации и работе с консолью, что снижает угрозу перехвата конфиденциальной информации третьими лицами.	<ul style="list-style-type: none">■ SSH-клиент – native в UNIX■ PuTTY, WinSCP, openssh (win32) в Windows



3. Быстрый доступ к устройству

Для получения доступа к web-интерфейсу роутера можно использовать любой стандартный интернет-браузер, поддерживающий HTTP 1.0. Например, Opera, Firefox, IE или Chrome.

Откройте интернет-браузер и выполните следующие действия.

1. Введите IP-адрес роутера в адресную строку интернет-браузера.



Рис. 3.1 Ввод IP-адреса роутера в адресную строку интернет-браузера

Примечание. IP-адрес для доступа к настройкам роутера, используемый по умолчанию, указан на наклейке на нижней стороне корпуса устройства.

Если роутер включен, то после ввода IP-адреса роутера появится страница приветствия. Страница приветствия содержит краткую информацию о состоянии устройства и сети:

- имя устройства (UNIT NAME);
- время работы устройства после включения (uptime);
- название оператора сотовой связи;
- тип GSM-связи, уровень GSM-сигнала;
- IP-адрес, скорость соединения;
- количество переданной и полученной информации и т.д.

2. Введите логин и пароль для доступа к web-интерфейсу роутера

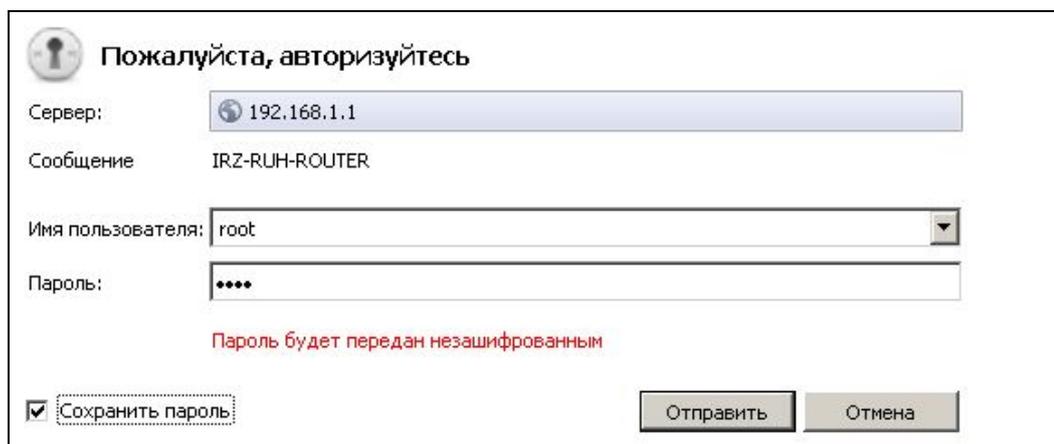


Рис. 3.2 Ввод логина и пароля для доступа к web-интерфейсу роутера



После корректно ввода логина и пароля открывается доступ к основному интерфейсу управления устройством.

Примечание. При утере пароля следует обратиться к главе [«Возвращение к заводским настройкам»](#). Для получения подробной информации о способах доступа и настройки роутера можно обратиться к главе [«Настройка доступа к устройству»](#).



4. Возвращение к заводским настройкам

Внимание! Данная операция необратима. Прежде чем выполнять сброс настроек, убедитесь, что текущие настройки устройства Вам не понадобятся (в том числе ключи и сертификаты OpenVPN, IPSec, GRE, параметры подключения к сети Интернет и т.д.).

Для того чтобы сбросить настройки роутера к заводским установкам, необходимо выполнить следующие действия:

1. Отключите питание роутера.
2. Нажмите и удерживайте кнопку «Сброс» -
3. Не отпуская кнопки «Сброс», подайте питание на роутер.
4. Подождите, пока не загорится индикатор загрузки -
5. Подождите, пока индикатор загрузки трижды не загорится и погаснет -
6. Отпустите кнопку: теперь устройство загрузится с заводскими настройками.

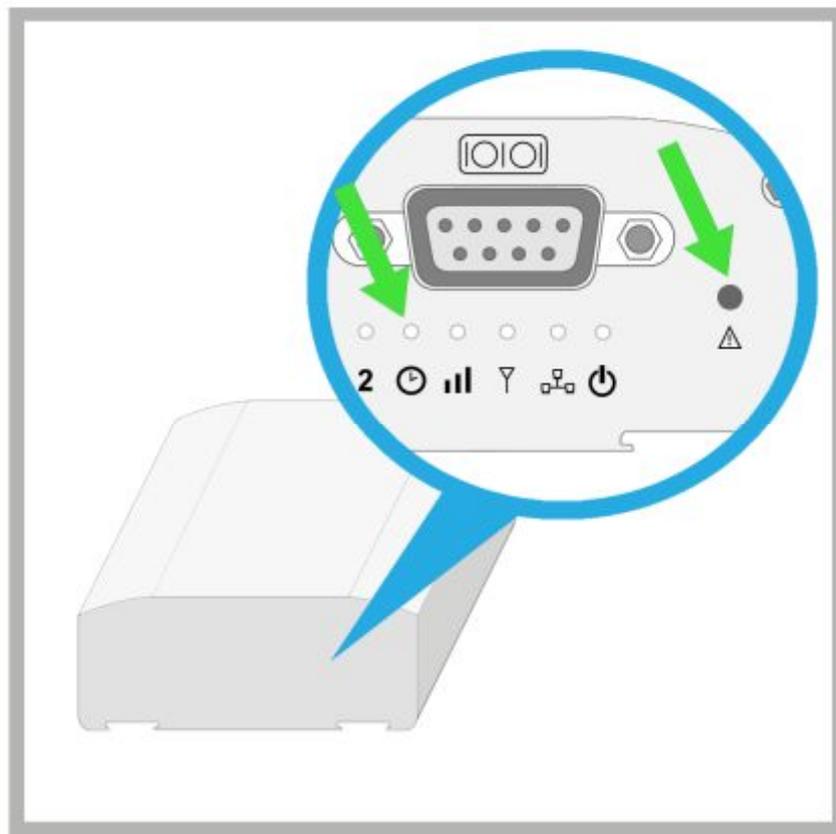


Рис. 4.1 Индикатор загрузки и кнопка «Сброс» на корпусе роутера



5. Web-интерфейс. Раздел «Configuration»

В данной главе рассматриваются возможности web-интерфейса роутера iRZ. Благодаря web-интерфейсу можно настраивать и контролировать работу роутера в любом стандартном интернет-браузере, а также выявлять причины в случае некорректной работы устройства.

5.1. Страница Internet

Как открыть: Configuration → Internet

Страница «Internet» позволяет настроить GPRS/EDGE/3G-соединения. Для подключения к сети Интернет роутер может использовать две SIM-карты, одна из которых, как правило, является основной, а вторая - резервной.

Таблица 5.1 Настройка доступа к сети Интернет (для каждой SIM-карты)

Название	Описание	Допустимое значение
(Поле выбора SIM-карты)	Выбор используемой SIM-карты	<input type="checkbox"/> SIM1 <input type="checkbox"/> SIM2
APN*	Точка доступа GSM-сети	Предоставляется оператором, чаще всего роутер определяет значение автоматически
Username	Логин для GPRS/EDGE/3G-подключения (предоставляется оператором)	(Свободный текст)
Password	Пароль для GPRS/EDGE/3G-подключения (предоставляется оператором)	(Свободный текст)
Authentication	Метод аутентификации	<input type="checkbox"/> Any (Любой) <input type="checkbox"/> PAP <input type="checkbox"/> CHAP
PIN	PIN-код SIM-карты	0000 – 9999
Local IP Address	Фиксированный IP-адрес внутри сотовой сети	см. «Синтаксис IP-адреса»
Remote IP Address	IP-адрес сервера сотовой сети	см. «Синтаксис IP-адреса»
Dial Number	Телефонный номер для подключения	“*99#” – RUH, RUH2, RC1 “#777” – RCA
MRU (bytes)	Maximum Receive Unit, определяется опытным путем	Число (байт)
MTU (bytes)	Maximum Transmission Unit, определяется опытным путем	Число (байт)



Название	Описание	Допустимое значение
Set GSM bands to	Выбор комбинаций допустимых частот для работы GSM-модуля в сотовой сети	900 MHz, 1800 MHz, 1900 MHz, 850 MHz, 900+1900 MHz, 900+1800 MHz, 850+1800 MHz, 850+1900 MHz, 900+1800+2100 MHz
Set modem mode to	Выбор режима работы модема в GSM-сети (EDGE/3G)	<ul style="list-style-type: none"><input type="checkbox"/> Auto (Определять автоматически)<input type="checkbox"/> 2G Only (Только 2G)<input type="checkbox"/> 2G Preferred (Предпочтительно 2G)<input type="checkbox"/> 3G Only (Только 3G)<input type="checkbox"/> 3G Preferred (Предпочтительно 3G)
DNS Service	Выбор источника службы DNS	<ul style="list-style-type: none"><input type="checkbox"/> Set manually (Установить вручную)<input type="checkbox"/> Get DNS from operator (Использовать службу DNS оператора)<input type="checkbox"/> Don't use DNS service (Не использовать службу DNS)
DNS Server 1	IP-адрес DNS-сервера №1	см. «Синтаксис IP-адреса»
DNS Server 2	IP-адрес DNS-сервера №2	см. «Синтаксис IP-адреса»
Check connection	Включение проверки соединения	<ul style="list-style-type: none"><input type="checkbox"/> Yes (Проверять соединение)<input type="checkbox"/> No (Не проверять соединение)
Ping IP Address(es)	IP-адрес для проверки соединения с помощью команды PING	см. «Синтаксис IP-адреса»
Ping Interval (min)	Интервал проверки соединения	1 – 32768 (минут)
Ping Repeat Interval (min)	Интервал запуска проверки соединения после первой неудачи	1 – 32768 (минут)
Allow failures	Количество неудачных попыток проверки соединения	1 – 999
Switch SIM after	Количество неудачных попыток регистрации SIM-карты, после которого будет происходить переключение на другую SIM-карту	1 – 32768
Try primary SIM after	Интервал возвращения к SIM-карте №1	1 – 32768 (минут)
Reboot after	Количество попыток регистрации SIM-карты, после которого роутер будет перезагружаться	1 – 32768
Number of soft retries	Количество попыток дозвона без перезапуска модема	1 – 32768
Apply	Применение и сохранение изменений	–

С информацией о состоянии GSM-соединения, GPRS/EDGE/3G-соединения и журналом подключения к сети Интернет можно ознакомиться на странице **Status and log → Internet**.



5.2. Страница LAN

Как открыть: Configuration → LAN

В данном разделе описана настройка интерфейсов Ethernet и DHCP-сервера.

5.2.1. Раздел «Local Ethernet Interface»

Таблица 5.2 Настройка интерфейса Ethernet

Название	Описание	Допустимое значение
IP Address	IP-адрес основного интерфейса Ethernet	см. «Синтаксис IP-адреса» (по умолчанию 192.168.1.1)
Subnet Mask	Маска подсети	см. «Синтаксис маски подсети» (по умолчанию 255.255.255.0)
Secondary IP address	Назначение дополнительного IP-адреса для основного интерфейса Ethernet	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Secondary IP	Дополнительный IP-адрес	см. «Синтаксис IP-адреса»
Secondary Mask	Маска подсети дополнительного IP-адреса	см. «Синтаксис маски подсети»
Force media type	Ручная установка режима работы адаптера Ethernet	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Media type	Технология передачи данных основного интерфейса Ethernet	100 Base-TX; 10 Base-T
Duplex type	Тип дуплекса	<input checked="" type="checkbox"/> full duplex (полный дуплекс) <input type="checkbox"/> half duplex (полудуплекс)
Apply	Применение и сохранение изменений	–

5.2.2. Раздел «USB Ethernet Interface»

Таблица 5.3 Настройка интерфейса USB-Ethernet

Название	Описание	Допустимое значение
USB-LAN IP address	Использование адаптера USB-LAN	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
USB-LAN IP	IP-адрес адаптера USB-LAN	см. «Синтаксис IP-адреса»
USB-LAN Mask	Маска подсети адаптера USB-LAN	см. «Синтаксис маски подсети»
Apply	Применение и сохранение изменений	–



5.2.3. Раздел «Reserve Link»

Таблица 5.4 Настройка резервирования интернет-соединения

Название	Описание	Допустимое значение
Activate reserve link mode	Включение режима «Reserve Link»	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Main router IP	Шлюз по умолчанию	см. «Синтаксис IP-адреса»
IP address to ping	IP-адрес для проверки основного соединения	см. «Синтаксис IP-адреса»
Main interface	Используемый интерфейс	<input type="checkbox"/> eth0 <input type="checkbox"/> eth0:0 <input type="checkbox"/> eth1
PPP link mode	Правило работы GPRS-интерфейса	<input type="checkbox"/> Disconnect when not used (Отключать, когда не используется) <input type="checkbox"/> Always connected (Всегда включен)
Apply	Применение и сохранение изменений	–

5.2.4. Раздел «DHCP Server»

Таблица 5.5 Настройка DHCP-сервера

Название	Описание	Допустимое значение
Enable DHCP server	Использование DHCP-сервера	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
IP Pool Start	Начальный IP-адрес в диапазоне адресов, раздаваемых DHCP-сервером	см. «Синтаксис IP-адреса»
IP Pool Stop	Конечный IP-адрес в диапазоне адресов, раздаваемых DHCP-сервером	см. «Синтаксис IP-адреса»
Default Lease Time	Стандартное время аренды IP-адреса, выданного DHCP-сервером	0 – 99999999 (секунд)
Maximum Lease Time	Максимальное время аренды IP-адреса, выданного DHCP-сервером	0 – 99999999 (секунд)
Enable static addresses	Использование DHCP-сервером привязки к MAC-адресу	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Host name	Имя или обозначение узла	(Свободный текст)
MAC address	MAC-адрес	см. «Синтаксис MAC-адреса»



Название	Описание	Допустимое значение
IP address	IP-адрес, присваиваемый узлу с указанным до этого MAC-адресом	см. «Синтаксис IP-адреса»
Apply	Применение и сохранение изменений	–

С информацией о состоянии интерфейсов, а также таблицей маршрутизации можно ознакомиться на странице **Status and log** → **LAN**. Информация о текущих арендах IP-адресов, выданных DHCP-сервером, находится на странице **Status and log** → **DHCP**.

5.3. Страница Port Forwarding

Как открыть: Configuration → Port Forwarding

Эта страница позволяет настроить перенаправление трафика из внешней сети на указанные TCP-порты устройств, находящихся за роутером (в его локальной подсети).

Таблица 5.6 Настройка перенаправления трафика

Название	Описание	Допустимое значение
Public Port	Порт, на котором роутер будет принимать подключения из сети Интернет	1 - 65535
Private Port	Порт, который используется для подключения узлом локальной сети	1 - 65535
Type	Тип протокола перенаправляемого трафика	<input type="checkbox"/> TCP <input type="checkbox"/> UDP <input type="checkbox"/> ICMP <input type="checkbox"/> TCP / UDP
Send all remaining incoming packets to default server	Отправка всех пакетов на указанный IP-адрес по умолчанию (DMZ)	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Default Server IP Address	IP-адрес, на который по умолчанию будут перенаправляться все пакеты	см. «Синтаксис IP-адреса»
Do not masquerade outgoing traffic (use with caution)	Отключение функции «MASQUERADE» для исходящего трафика (использовать с осторожностью)	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Apply	Применение и сохранение изменений	–



5.4. Страница Static Routes

Как открыть: Configuration → Static Routes

Эта страница позволяет создать правила статической маршрутизации трафика, проходящего через роутер.

Примечание. При использовании служб IPSec, GRE, OpenVPN, VRRP не требуется добавлять маршруты для тех сетей, к которым будет предоставляться доступ через эти службы (когда не требуется явно). Роутер автоматически создает все необходимые маршруты к таким сетям.

Таблица 5.7 Настройка правил статической маршрутизации трафика

Название	Описание	Допустимое значение
Network	Сеть назначения, к которой будет указан маршрут	см. «Синтаксис IP-адреса»
Netmask	Маска сети назначения	см. «Синтаксис маски подсети»
Gateway	Следующий шлюз / маршрутизатор, обеспечивающий связь с указанной сетью	см. «Синтаксис IP-адреса»
Interface	Интерфейс, к которому будет привязан создаваемый маршрут	<ul style="list-style-type: none">■ eth0■ eth0:0■ ppp0■ eth1■ gre1 ... gre10
Apply	Применение и сохранение изменений	—



5.5. Страница VRRP

Как открыть: Configuration → VRRP

Эта страница позволяет настроить использование VRRP.

VRRP – это технология, обеспечивающая резервирование шлюза в сети или на объекте. При включенном VRRP роутер контролирует присутствие основного роутера сети и, если тот вышел из строя, берет на себя его функции.

Таблица 5.8 Настройка параметров VRRP

Название	Описание	Допустимое значение
VRRP enable	Использование VRRP	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Instance name	Имя узла VRRP	(Свободный текст)
Instance IP	IP-адрес общего экземпляра роутера	см. «Синтаксис IP-адреса»
Instance router ID	VRRP-идентификатор роутера	(Любое число)
Instance priority	Приоритет роутера	1 – 255
Instance authentication	Тип аутентификаций	<input type="checkbox"/> None (Отключить аутентификацию) <input type="checkbox"/> Simple <input type="checkbox"/> AH
Instance password	Пароль аутентификации	(Свободный текст)
SMTP server	Е-mail сервер, используемый для отправки оповещений	<input type="checkbox"/> IP-адрес (см. «Синтаксис IP-адреса») <input type="checkbox"/> Доменное имя сервера
From mail	Поле «Отправитель» в письме е-mail оповещения	(Е-mail адрес)
To mail	Поле «Получатель» в письме е-mail оповещения	(Е-mail адрес)
Apply	Применение и сохранение изменений	–



5.6. Страница Firewall

Как открыть: Configuration → Firewall

Эта страница позволяет настроить межсетевой экран, являющийся важным компонентом роутера.

Внимание! Рекомендуется уделить особое внимание настройкам на этой странице. Указание некорректных настроек может нарушить работу всей сети или сделать ее уязвимой со стороны третьих лиц.

Таблица 5.9 Настройка параметров меж сетевого экрана

Название	Описание	Допустимое значение
(Раскрывающийся список)	Режим работы меж сетевого экрана	<ul style="list-style-type: none">Disable firewall (Отключить меж сетевой экран)Allow specified, disable others (Разрешить соединения, заданные правилами, а остальные запретить)Disable specified, allow others (Запретить соединения, заданные правилами, а остальные разрешить)
Type	Тип источника трафика	<ul style="list-style-type: none">Single address (Один IP-адрес)Any address (Любой адрес)Subnet (Подсеть)
IP Address	IP-адрес узла, принимающего/отправляющего трафик	см. «Синтаксис IP-адреса», см. «Синтаксис IP-адреса сети»
Net Mask	Маска сети, в которой находится принимающий трафик узел	см. «Синтаксис маски подсети»
Protocol	Протокол, используемый для передачи пользовательского трафика	<ul style="list-style-type: none">All (Все протоколы)TCPUDPICMP
Port	Номер TCP или UDP-порта	1 - 65535
Apply	Применение и сохранение изменений	—



5.7. Страница SNMP

Как открыть: Configuration → SNMP

Эта страница позволяет настроить службу SNMP. SNMP используется для мониторинга подключенных к сети устройств, служб и узлов, состояние которых критично для вычислительного комплекса.

Версия службы SNMP, реализованная в роутерах, позволяет получать информацию о следующих показателях:

- System name ("IRZ-RUH-ROUTER");
- Snmpd uptime;
- Contact;
- Location;
- Total interfaces count;
- Interfaces info: names, states, RX/TX/discard/error counter values;
- System uptime.

Таблица 5.10 Настройка параметров службы SNMP

Название	Описание	Допустимое значение
Enable SNMP	Использование SNMP	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Require authentication	Включение аутентификации при подключении SNMP-агента	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Community	Имя snmp-community	public
Description	Описание или название	(свободный текст)
Contact	Контакт ответственного сотрудника	(свободный текст)
Location	Местонахождение узла	(свободный текст)
Timeout	Интервал обновления информации с внутренних сенсоров системы	1 – 86400 (минут)

5.8. Страница GRE

Как открыть: Configuration → GRE

Эта страница позволяет настроить создание GRE-туннелей. Технология GRE обеспечивает виртуальное соединение между собой нескольких узлов или целой сети устройств, независимо от их местоположения.



Таблица 5.11 Настройка включения GRE-туннелей

Название	Описание	Допустимое значение
Create	Включение создания туннеля	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Description	Название (краткое описание) туннеля	[Нераз редактируемое поле]
Remote IP Address	IP-адрес оконечного устройства удаленной стороны туннеля	[Нераз редактируемое поле]
Remote Subnet	IP-адрес удаленной сети	[Нераз редактируемое поле]
Ссылка «[Edit]»	Редактирование свойств туннеля	-
Apply	Применение и сохранение изменений	-

Чтобы перейти к настройке параметров GRE-туннеля, щелкните ссылку «[Edit]» напротив названия редактируемого туннеля.

Таблица 5.12 Настройка параметров GRE-туннеля

Название	Описание	Допустимое значение
Create GRE tunnel #[N]	Включение создания туннеля №	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Description	Краткое описание или название туннеля	(Свободный текст)
Remote External IP Address	IP-адрес оконечного устройства удаленной стороны туннеля	см. «Синтаксис IP-адреса»
Remote Subnet	IP-адрес удаленной сети	см. «Синтаксис IP-адреса сети»
Remote Subnet Mask	Маска удаленной сети	см. «Синтаксис маски подсети»
Local Internal IP Address	Локальный IP-адрес виртуального интерфейса туннеля	см. «Синтаксис IP-адреса»
Remote Internal IP Address	IP-адрес виртуального интерфейса удаленного узла	см. «Синтаксис IP-адреса»
Tunnel Mask	Маска подсети между виртуальными интерфейсами узлов	см. «Синтаксис маски подсети»
Tunnel MTU	Характеристика MTU в среде передачи данных, созданной GRE-туннелем	1 – 1440
Apply	Применение и сохранение изменений	-



5.9. Страница OpenVPN Tunnel

Как открыть: Configuration → OpenVPN Tunnel

Эта страница позволяет настроить создание OpenVPN-туннелей. OpenVPN является одной из основных служб, определяющих функционал роутера iRZ. Служба OpenVPN многогранна, и ее настройка зависит от определенного применения, поэтому перед использованием OpenVPN рекомендуется внимательно ознакомиться с возможностями ее настройки.

Примечание. Для ознакомления с примерами конфигураций OpenVPN-туннелей, а также для получения инструкций по развертыванию решений на базе OpenVPN обратитесь к документу «Создание виртуальных сетей и туннелей средствами роутеров iRZ».

Таблица 5.13 Настройка параметров OpenVPN-туннеля

Название	Описание	Допустимое значение
Create OpenVPN tunnel	Включение создания OpenVPN-туннеля	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Take settings from	Указание источника конфигурации	<input checked="" type="checkbox"/> Web interface (Web-интерфейс) <input type="checkbox"/> Configuration file (Конфигурационный файл)
Protocol	Протокол, используемый службой OpenVPN	<input checked="" type="checkbox"/> UDP <input type="checkbox"/> TCP Server <input type="checkbox"/> TCP Client
UDP Port / TCP Port	Порт для подключения	1 - 65535
Remote IP Address	IP-адрес или доменное имя удаленного узла (сервера или оконечного узла туннеля) OpenVPN	см. «Синтаксис IP-адреса»
Remote Subnet	Адрес удаленной подсети	см. «Синтаксис IP-адреса сети»
Remote Subnet Mask	Маска удаленной подсети	см. «Синтаксис маски подсети»
Redirect Gateway	Направление всего исходящего IP-трафика через OpenVPN-туннель (за исключением служебного трафика самого OpenVPN)	<input type="checkbox"/> No (Отключить перенаправления IP-трафика через OpenVPN-туннель) <input checked="" type="checkbox"/> Yes (Использовать перенаправления IP-трафика через OpenVPN-туннель)
NAT Rules	Применения правил к таблице преобразований сетевых адресов (NAT)	<input type="checkbox"/> Not applied (Не применять) <input checked="" type="checkbox"/> Applied (Применить)
Local Interface IP Address	IP-адрес локального виртуального интерфейса	см. «Синтаксис IP-адреса»



Название	Описание	Допустимое значение
Remote Interface IP Address	IP-адрес удаленного виртуального интерфейса	см. «Синтаксис IP-адреса»
Authenticate Mode	Режим аутентификации	<ul style="list-style-type: none"> ■ Tunnel: none (Туннель – без аутентификации) ■ Tunnel: pre-shared secret (Туннель – предустановленный ключ) ■ Tunnel: X.509 certificate (client) (Туннель – клиентский сертификат X.509) ■ Tunnel: X.509 certificate (server) (Туннель – серверный сертификат X.509) ■ Client: username / password (Клиент – логин и пароль) ■ Client: X.509 certificate (Клиент – сертификат X.509)
Ping Interval	Интервал времени проверки соединения	1 – 86400 (секунд)
Ping Timeout	Максимальное время ответа при проверке соединения	1 – 1000 (секунд)
Renegotiate Interval	Интервал времени повторной авторизации (в секундах). Изменения вступают в силу только в случае совпадения значения опции на обеих сторонах туннеля	0 – ∞ 0 → выключить функцию <i>Максимальное значение не тестировалось</i>
Handshake Window	Время, в течение которого должно быть произведено согласование на уровне протокола TLS (в секундах)	0 – ∞ <i>Максимальное значение не тестировалось</i>
Inactivity Timeout	Период отсутствия активности, после которого OpenVPN завершает работу (в секундах)	0 – ∞ 0 → выключить функцию <i>Максимальное значение не тестировалось</i>
Max Fragment Size	Максимальный размер фрагмента пакета OpenVPN (в байтах)	0 – ∞ <i>Максимальное значение не тестировалось</i>
Compression	Компрессия (сжатие) данных	None (Отключить сжатие данных); LZO
Username	Имя пользователя	
Password	Пароль	
Ping IP Address	Адрес, используемый для проверки соединения	см. «Синтаксис IP-адреса сети»
Ping Interval	Интервал времени проверки соединения	1 – 86400 (минут)
Allow failures	Разрешенное число неудачных попыток при проверке соединения	1 – 1000
Pre-shared Secret	Секретная фраза / слово-ключ	Криптографическая информация в ASCII-представлении (см. документ «Создание



Название	Описание	Допустимое значение
CA Certificate	Корневой сертификат	виртуальных сетей и туннелей средствами OpenVPN» из серии документов «Примеры рабочих конфигураций роутера iRZ»)
DH Parameters	Параметры группы Diffie-Hellman	
Local Certificate	Сертификат клиента OpenVPN	
Local Private Key	Секретный ключ клиента OpenVPN	
Configuration File	Текстовое поле, содержащее тело конфигурационного файла	Конфигурационные директивы OpenVPN
Apply	Применение и сохранение изменений	-

С ходом запуска, подключения и всей отладочной информацией можно ознакомиться на странице **Status and log → OpenVPN Tunnel**.

5.10. Страница OpenVPN Server

Как открыть: Configuration → OpenVPN Server

Роутеры iRZ поддерживают функцию сервера OpenVPN непосредственно на собственной платформе. Эта страница позволяет настроить на роутере сервер OpenVPN.

Примечание. Для ознакомления с примерами конфигураций OpenVPN-туннелей, а также для получения инструкций по развертыванию решений на базе OpenVPN обратитесь к документу «Создание виртуальных сетей и туннелей средствами роутеров iRZ».

Таблица 5.14 Настройка параметров сервера OpenVPN

Название	Описание	Допустимое значение
Server Configuration		
Start OpenVPN Server	Запуск сервера OpenVPN	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Protocol	Протокол, используемый службой OpenVPN	<input checked="" type="checkbox"/> UDP <input type="checkbox"/> TCP
Port	Порт для подключения к серверу	1 – 65535
Server Configuration	Поле, содержащее директивы конфигурации сервера	Криптографическая информация в ASCII-представлении (см. документ «Создание виртуальных сетей и туннелей средствами OpenVPN» из серии
CA Certificate	Корневой сертификат	



Название	Описание	Допустимое значение
DH Parameters	Параметры группы Diffie-Hellman	документов «Примеры рабочих конфигураций роутера iRZ»)
Local Certificate	Сертификат клиента OpenVPN	
Local Private Key	Секретный ключ клиента OpenVPN	
Client Configuration		
Description	Описание / название конфигурации	(Свободный текст)
Client Name	Имя клиента	см. документ «Создание виртуальных сетей и туннелей средствами OpenVPN» из серии документов «Примеры рабочих конфигураций роутера iRZ»
Ссылка «[Edit]»	Открытие страницы редактирования конфигурации, отсылаемой клиенту	-
Apply	Применение и сохранение изменений	-

С ходом запуска, подключения и всей отладочной информацией можно ознакомиться на странице **Status and log → OpenVPN Server**.

5.11. Страница IPsec

Как открыть: Configuration → IPsec

Эта страница содержит параметры для настройки IPsec.

Примечание. В связи со сложностью настройки IPsec рекомендуется уделить этому процессу особое внимание. Даже небольшое несовпадение параметров узлов может привести к ошибке при создании IPsec-туннеля.



Для быстрого включения и выключения IPSec-туннелей можно использовать таблицу управления. Чтобы открыть таблицу управления, щелкните ссылку «IPSec» в панели навигации. Для создания туннеля требуется выполнить следующие действия:

1. выберите «yes» в колонке «Create» напротив названия туннеля;
2. нажмите кнопку «Apply» (при этом настройки будут сохранены).

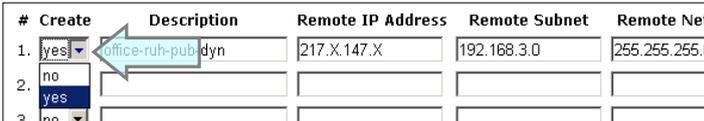


Рис. 5.1 Создание IPSec-туннеля

Для того чтобы задать параметры IPSec-туннеля, необходимо щелкнуть ссылку «[Edit]» напротив требуемого туннеля.

Таблица 5.15 Настройка параметров IPSec-туннеля

Название	Описание	Допустимое значение
Create IPsec tunnel #[N]	Включение создания IPSec-туннеля #[N]	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Description	Описание или название туннеля	(Свободный текст)
Remote IP Address	IP-адрес удаленного оконечного узла	см. «Синтаксис IP-адреса»
Remote ID	Идентификатор удаленного узла	(Свободный текст)
Remote Subnet	IP-адрес удаленной подсети или узла, доступ к которым будет предоставлен туннелем	см. «Синтаксис IP-адреса сети»
Remote Subnet Mask	Маска удаленной сети или узла, доступ к которым будет предоставлен туннелем	см. «Синтаксис маски подсети»
Local ID	Собственный идентификатор	(Свободное слово)
Local Subnet	IP-адрес локальной подсети, доступ к которой будет предоставлен роутером через туннель	см. «Синтаксис IP-адреса сети»
Local Subnet Mask	Маска локальной подсети, доступ к которой будет предоставлен роутером через туннель	см. «Синтаксис маски подсети»
Key Lifetime	Время жизни ключа	1 – 86400 (секунд)
IKE Lifetime	Время жизни IKE	1 – 86400 (секунд)
Rekey Margin	Время между сессиями обмена ключами	1 – 1000 (секунд)
Rekey Fuzz	Энтропия нового ключа по отношению к старому	0 – 100 (процентов)



Название	Описание	Допустимое значение
NAT Traversal	Использование NAT Traversal	<input type="checkbox"/> Disabled (Не использовать NAT Traversal) <input type="checkbox"/> Enabled (Использовать NAT Traversal)
Aggressive Mode	Агрессивный режим синхронизации протокола	<input type="checkbox"/> Disabled (Отключить) <input type="checkbox"/> Enabled (Включить)
Authenticate Mode	Режим аутентификации	<input type="checkbox"/> Pre-shared key (Предустановленный ключ) <input type="checkbox"/> X.509 certificate (Сертификат X.509)
Verify Certificate	Проверка подлинности сертификата	<input type="checkbox"/> Disabled (Отключить) <input type="checkbox"/> Enabled (Включить)
Pre-shared Key	Секретное слово или пароль	(свободный текст)
Phase I		
Encryption Algorhythm	Алгоритм шифрования	<input type="checkbox"/> 3DES <input type="checkbox"/> DES <input type="checkbox"/> BLOWFISH <input type="checkbox"/> AES
Hash Algorhythm	Алгоритм хеширования	<input type="checkbox"/> SHA1 <input type="checkbox"/> SHA256 <input type="checkbox"/> SHA384 <input type="checkbox"/> MD5
DH Group	Группа Diffie-Hellman	<input type="checkbox"/> DH Group 1 (768 bits) <input type="checkbox"/> DH Group 2 (1024 bits) <input type="checkbox"/> DH Group 5 (1536 bits) <input type="checkbox"/> DH Group 14 (2048 bits) <input type="checkbox"/> DH Group 15 (3072 bits) <input type="checkbox"/> DH Group 16 (4096 bits) <input type="checkbox"/> DH Group 17 (6144 bits) <input type="checkbox"/> DH Group 18 (8192 bits)
Phase II		
Encryption Algorhythm	Алгоритм шифрования	<input type="checkbox"/> 3DES <input type="checkbox"/> DES <input type="checkbox"/> BLOWFISH <input type="checkbox"/> RC5 <input type="checkbox"/> AES
Authentication Algorhythm	Алгоритм аутентификации	<input type="checkbox"/> HMAC-SHA1 <input type="checkbox"/> HMAC-SHA256 <input type="checkbox"/> HMAC-SHA384 <input type="checkbox"/> DES <input type="checkbox"/> 3DES <input type="checkbox"/> HMAC-MD5



Название	Описание	Допустимое значение
PFS Group	Группа «Perfect Forward Secrecy»	<ul style="list-style-type: none"> <input type="checkbox"/> None (Не использовать) <input type="checkbox"/> PFS Group 1 (768 bits) <input type="checkbox"/> PFS Group 2 (1024 bits) <input type="checkbox"/> PFS Group 5 (1536 bits) <input type="checkbox"/> PFS Group 14 (2048 bits) <input type="checkbox"/> PFS Group 15 (3072 bits) <input type="checkbox"/> PFS Group 16 (4096 bits) <input type="checkbox"/> PFS Group 17 (6144 bits) <input type="checkbox"/> PFS Group 18 (8192 bits)
Identifier verification		
Verify Identifier	Проверка идентификаторов узлов при создании туннеля	<ul style="list-style-type: none"> <input type="checkbox"/> On (Включить) <input type="checkbox"/> Off (Отключить)
My Identifier Type	Тип идентификатора роутера	<ul style="list-style-type: none"> <input type="checkbox"/> None (Не использовать идентификатор) <input type="checkbox"/> Address <input type="checkbox"/> User FQDN <input type="checkbox"/> ASN1DN <input type="checkbox"/> FQDN
My Identifier	Идентификатор роутера	(Свободный текст)
Peers Identifier Type	Тип идентификатора удаленного узла	<ul style="list-style-type: none"> <input type="checkbox"/> None(Не использовать идентификатор) <input type="checkbox"/> Address <input type="checkbox"/> User FQDN <input type="checkbox"/> ASN1DN <input type="checkbox"/> FQDN
Ping Test IP	IP-адрес для автозапуска туннеля и проверки связи	см. «Синтаксис IP-адреса»
Ping Test Interval	Интервал времени проверки связи	1 – 86400 (минут)
CA Certificate	Корневой сертификат	Криптографическая информация в ASCII-представлении (см. документ «Защита передаваемых данных средствами IPSec» из серии документов «Примеры рабочих конфигураций роутера iRZ»)
Remote Certificate	Сертификат удаленного узла	
Local Certificate	Собственный сертификат	
Local Private Key	Собственный секретный ключ	
Local Passphrase	Собственное секретное слово или пароль	Общее секретное слово или ключ
Apply	Применение и сохранение изменений	-

С ходом запуска, подключения и всей отладочной информацией можно ознакомиться на странице **Status and log → IPSec**.



Внимание! Часть отладочной информации может быть зафиксирована модулем ядра, в таком случае он будет отображаться в системном журнале (**Status and log** → **Systemlog**).

5.12. Страница L2TP

Как открыть: *Configuration* → *L2TP*

Эта страница позволяет настроить режим работы службы L2TP.

Таблица 5.16 Настройка параметров L2TP-туннеля

Название	Описание	Допустимое значение
L2TP enable	Включение сервиса L2TP	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
L2TP mode	Режим работы	<input checked="" type="checkbox"/> Client <input type="checkbox"/> Server
Server IP	Адрес сервера (в режиме клиента)	См Синтаксис IP-адреса
Client Start IP Address	Начало диапазона клиентских адресов (в режиме сервера)	См Синтаксис IP-адреса
Client End IP Address	Конец диапазона клиентских адресов (в режиме сервера)	См Синтаксис IP-адреса
UDP Port	Порт для приёма/передачи данных	1 — 65535
Redial Timeout (sec)	Задержка между подключениями (секунды) (в режиме клиента)	1— 32768
Default route	Использовать как маршрут по умолчанию	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Username	Имя пользователя	(Свободный текст)
Password	Пароль	(Свободный текст)
Local Interface IP Address	Локальный адрес туннеля	См Синтаксис IP-адреса
Remote Interface IP Address	Удалённый адрес туннеля	См Синтаксис IP-адреса
Remote Subnet	Адрес удалённой сети	См Синтаксис IP-адреса
Remote Subnet Mask	Маска удалённой сети	См Синтаксис IP-адреса
Apply	Применение и сохранение изменений	-



5.13. Страница Serial Port

Как открыть: Configuration → Serial Port

Эта страница позволяет настроить последовательные COM-интерфейсы (RS-232).

Таблица 5.17 Настройка параметров COM-портов

Название	Описание	Допустимое значение
Serial Port		
Serial Port Mode	Режим перенаправления данных с последовательного порта	<input type="checkbox"/> None (Не использовать перенаправление) <input type="checkbox"/> Tunnel Server <input type="checkbox"/> Tunnel Client
Interface	Тип интерфейса, используемого последовательным портом	<input type="checkbox"/> RS-232 <input type="checkbox"/> USB-COM
TCP/UDP Port	Порт для подключения программы опроса	1 – 65535
Server IP	IP-адрес сервера TCP (Serial Port mode = Tunnel Client)	см. «Синтаксис IP-адреса»
Baudrate	Скорость передачи данных, бит/с	<input type="checkbox"/> 300 <input type="checkbox"/> 1200 <input type="checkbox"/> 2400 <input type="checkbox"/> 4800 <input type="checkbox"/> 9600 <input type="checkbox"/> 19200 <input type="checkbox"/> 38400 <input type="checkbox"/> 57600 <input type="checkbox"/> 115200
Data Bits	Количество бит данных	<input type="checkbox"/> 7 bits <input type="checkbox"/> 8 bits
Parity Check	Контроль четности	<input type="checkbox"/> None (Отключить контроль четности) <input type="checkbox"/> Even (Четный) <input type="checkbox"/> Odd (Нечетный)
Stop Bits	Количество стоповых битов	<input type="checkbox"/> 1 bit <input type="checkbox"/> 2 bits
Timeout	Закрытие COM-порта после указанного периода времени при отсутствии активности, секунд	0 – 86400
Accumulator interval	Интервал ожидания данных перед отправкой (мс)	0 - 65535
Accumulator attempts	Количество ожиданий перед принудительной отправкой	0 - 65535
Reconnect delay	Задержка перед подключением (секунды)	0 - 65535



Название	Описание	Допустимое значение
Banner	Идентификатор, посылаемый после установки соединения	(Свободный текст)
Dry Contact Check		
Dry Contact Check	Включение проверки «сухого контакта» на указанном интерфейсе	<input type="checkbox"/> Disabled (Отключить) <input type="checkbox"/> USB-COM <input type="checkbox"/> RS-232
Polling interval	Интервал проверки контакта (в секундах)	1 – более 4 млрд.
Phone numbers	Телефонный номер для оповещения по SMS	(Например: +38112223333)
Open message	Текст сообщения, отправляемого при разрыве «сухого контакта»	(Свободный текст)
Close message	Текст сообщения, отправляемого при восстановлении «сухого контакта»	(Свободный текст)
Apply	Применение и сохранение изменений	-

Для поля Banner допускается использовать специальные символы возврата каретки (\r), переноса строки (\n) и шестнадцатеричные значения (\0x20).

5.14. Страница DynDNS

Как открыть: Configuration → DynDNS

Роутер поддерживает сервис DynDNS от различных поставщиков, часть из которых предоставляют свои услуги на платной основе. Кроме того, возможна организация собственного аналогичного сервиса на платформе программного обеспечения BIND.

Таблица 5.18 Настройка параметров DynDNS-клиента

Название	Описание	Допустимое значение
Enable DynDNS client	Использования клиента DynDNS	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Service Provider	Провайдер сервиса DynDNS	<input type="checkbox"/> dyndns.com <input type="checkbox"/> no-ip.com <input type="checkbox"/> freedns.afraid.org <input type="checkbox"/> zoneedit.com <input type="checkbox"/> Custom
Hostname	Арендованное доменное имя	(Свободный текст)



Название	Описание	Допустимое значение
Username	Имя пользователя	(Свободный текст)
Password	Пароль	(Свободный текст)
Custom Server	Адрес собственного сервера	<ul style="list-style-type: none">■ Доменное имя■ IP-адрес (см. «Синтаксис IP-адреса»)
Custom URL	URL-адрес на собственном сервере	(Свободный текст)
Update interval	Период времени обновления информации об IP-адресе	0 – 864000 (секунд)
Apply	Применение и сохранение изменений	-

С ходом запуска клиента DynDNS, подключения и всей отладочной информацией можно ознакомиться на странице **Status and log** → **DynDNS**.

5.15. Страница NTP

Как открыть: Configuration → NTP

Эта страница позволяет настроить синхронизацию внутренних часов роутера iRZ с мировыми серверами времени (NTP-серверами).



Таблица 5.19 Настройка параметров NTP-клиента

Название	Описание	Допустимое значение
Synchronize clock with NTP server on first connect	Синхронизация с NTP-сервером при первом подключении	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Enable clock synchronization with NTP	Синхронизация с NTP-сервером	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Allow to use as NTP server	Использование роутера в качестве NTP-сервера	<input checked="" type="checkbox"/> Check (Включено) <input type="checkbox"/> Uncheck (Выключено)
Primary NTP Server Address	Имя или IP-адрес основного NTP-сервера	<input type="checkbox"/> Доменное имя <input checked="" type="checkbox"/> IP-адрес (см. «Синтаксис IP-адреса»)
Secondary NTP Server Address	Имя или IP-адрес вторичного NTP-сервера	<input type="checkbox"/> Доменное имя <input checked="" type="checkbox"/> IP-адрес (см. «Синтаксис IP-адреса»)
Local time zone	Локальный часовой пояс	GMT -12...GMT +14
Apply	Применение и сохранение изменений	-

5.16. Страница SMS

Как открыть: Configuration → SMS

Эта страница позволяет настроить отправку уведомительных SMS-сообщений. Такие SMS-сообщения могут быть отправлены при следующих событиях:

- Power up (включение питания);
- GPRS-connect (подсоединение к сети Интернет);
- GPRS-disconnect (отсоединение от сети Интернет);
- USB-Ethernet connect (подключение адаптера USB-LAN);
- USB-Ethernet disconnect (отключение адаптера USB-LAN).

Для того чтобы включить отправку SMS-сообщения при определенном событии, необходимо установить флажок напротив интересующего события и указать не более двух номеров телефона, на которые будут приходить уведомления (Phone number 1 и Phone number 2).

Чтобы было легче опознать отправителя SMS-сообщения, можно указать в поле UnitID имя роутера. Тогда в исходящих SMS-сообщениях устройства будет содержаться его имя.



5.17. Страница Daily Reboot

Как открыть: Configuration → Daily Reboot

Эта страница позволяет настроить регулярную перезагрузку роутера iRZ в заданное время.

Для того чтобы включить данную функцию, необходимо установить флажок для опции «Reboot daily at given time» (Перезагружать ежедневно в заданное время). Время перезагрузки задается в формате: **ЧАС : МИНУТА**. Для сохранения внесенные изменения необходимо нажать кнопку «Apply».



6. Web-интерфейс. Раздел «Status and log»

Страницы данного раздела предназначены для мониторинга и анализа работы устройства, а также его служб. Роутер предоставляет такую информацию на страницах Internet, LAN, DHCP, Iptables, OpenVPN Tunnel, OpenVPN Server, IPsec, DynDNS, System Log. Протоколирование отдельных служб представлено в интуитивно понятном виде, поэтому подробно не описывается. В качестве примера рассматривается наиболее сложная страница «Internet».

6.1. Страница Internet

Как открыть: Status and log → Internet

На этой странице отображается следующая информация о статусе интернет-соединения.

Таблица 6.1 Описание показателей страницы «Internet»

Название	Описание
Current SIM card	Номер SIM-карты
Signal Quality	Уровень GSM-сигнала dBm (CSQ)
Connection type	Тип GSM-соединения
Connection state	Состояние подключения к сети Интернет
Connection time	Время (длительность) подключения
Upload speed	Исходящая скорость передачи данных
Download speed	Нисходящая скорость передачи данных
Totally uploaded	Суммарный объем отправленных данных
Totally downloaded	Суммарный объем полученных данных
IP Address	IP-адрес: адрес (тип - внешний/внутренний)

```
Current SIM card: 1
Current operator: Megafon
Signal Quality: -74 dBm (19)
Connection type: HSDPA
Connection state: established
Connection time: 2 minutes, 4 sec
Upload speed: 2,268 KiB/sec
Download speed: 0 bytes/sec
Totally uploaded: 99 KiB 768 bytes
Totally downloaded: 1 KiB 120 bytes

IP Address: 85.26.210.128 (Public)
```

Рис. 6.1 Пример содержания страницы «Internet» в разделе «Status and log»



7. Web-интерфейс. Раздел «Administration»

На страницах данного раздела настраивается администрирование, в том числе логин и пароль доступа к настройкам роутера.

7.1. Страница Change Password

Как открыть: Administration → Change Password

Внимание! В связи с тем, что в данном разделе рассматривается предоставление доступа к устройству, рекомендуется уделить ему особое внимание.

Эта страница позволяет настроить доступ к системе (задать имя пользователя и пароль).

Таблица 7.1 Настройка параметров доступа к роутеру

Название	Описание	Допустимое значение
Current root name	Текущий логин суперпользователя	[неизменяемое поле]
New root name	Новый логин суперпользователя	(Свободный текст)
Old password	Старый пароль суперпользователя	(Свободный текст)
New password	Новый пароль суперпользователя	(Свободный текст)
Confirm password	Подтверждение нового пароля суперпользователя	(Свободный текст)
Apply	Применение и сохранение изменений	-

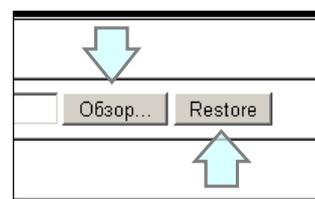
7.2. Страница Backup/Restore

Как открыть: Administration → Backup/Restore

Эта страница позволяет сохранять и восстанавливать текущую конфигурацию роутера. Для того чтобы сохранить текущую конфигурацию устройства, необходимо нажать кнопку «Backup» (Резервная копия), расположенную после текста «Backup configuration» (Настройка резервной копии).

Для восстановления ранее сохраненной конфигурации устройства необходимо выполнить следующие действия:

1. нажмите кнопку «Обзор», расположенную после надписи «Restore configuration» (Восстановление конфигурации из резервной копии);





2. выберите сохраненный ранее файл с расширением «.BIN» и нажмите кнопку «Открыть» в диалоге выбора файла;
3. нажмите кнопку «Restore» (Восстановление) для загрузки резервной копии конфигурации.

После загрузки конфигурации появится сообщение со словами «Settings restored, rebooting...». После сохранения настроек роутер перезагрузится с новыми настройками.

Если необходимо сохранять и восстанавливать конфигурацию при помощи USB-накопителя, то следует обратиться к документу «Руководство по настройке роутера iRZ с помощью USB-накопителя».

7.3. Страница Set Real Time Clock

Как открыть: Administration → Set Real Time Clock

Эта страница позволяет установить системное время. Возможно как получение информации о текущем времени от NTP-сервера, так и настройка времени вручную.

Для того чтобы использовать NTP-сервер, необходимо установить флажок для опции «NTP Server Address» и указать IP-адрес или доменное имя NTP-сервера.

Для установки системного времени вручную следует нажать на переключатель слева от надписи «Enter manually» и ввести дату и время в формате: **ГОД : МЕСЯЦ : ДЕНЬ, ЧАС : МИНУТА : СЕКУНДА**. Для применения и сохранения изменений нажмите кнопку «Apply».

7.4. Страница Remote access

Как открыть: Administration → Remote access

Внимание! В связи с тем, что в данном разделе рассматривается предоставление доступа к устройству, рекомендуется уделить ему особое внимание.

Эта страница позволяет настроить удаленный доступ к устройству. Описание параметров приведено в разделе «[Настройка доступа к устройству](#)».

7.5. Страница Unit name

Как открыть: Administration → Unit name

Данная страница позволяет задать идентификатор устройства и имя узла.



Доступны следующие варианты идентификатора:

- Unit name disabled — идентификатор устройства не используется;
- Take unit name from OpenVPN certificate - брать идентификатор из сертификата OpenVPN;
- Take unit name from SNMP description - брать идентификатор из описания SNMP;
- Enter unit name below — ввести идентификатор вручную в поле ниже.

Доступны следующие варианты имени узла:

- Default host name — заводское имя узла;
- Take host name from OpenVPN certificate - брать имя узла из сертификата OpenVPN;
- Take host name from SNMP description - брать имя узла из описания SNMP;
- Enter host name below — ввести имя узла вручную в поле ниже.

Для применения настроек нажмите кнопку Set unit name.

7.6. Страница Ping Test

Как открыть: Administration → Ping Test

Эта страница позволяет проверить доступность узла, находящегося в сети Интернет, локальной сети роутера или в подсети, доступной за OpenVPN/GRE/IPSec-туннелем. Для того чтобы проверить связь, необходимо ввести IP-адрес или доменное имя проверяемого узла в текстовое поле, находящееся после надписи «Ping Address/URL» и нажать кнопку «Ping».

Дополнительные опции «Count» и «Packet size» позволяют указать количество отправленных пакетов и их размер соответственно.

7.7. Страница System Log

Как открыть: Administration → System Log

Эта страница позволяет установить место сохранения системного журнала. Доступные опции:

- Log locally only (Сохранять локально);
- Log via network only (Сохранять только на сервер Syslog);
- Log locally and via network (Сохранять локально и дублировать сообщения на сервер Syslog).

В режимах «Log via network only» и «Log locally and via network» требуется указать IP-адрес сервера Syslog и порт UDP, куда будут отправлены системные сообщения.



7.8. Страница Startup Script

Как открыть: Administration → Startup Script

Эта страница позволяет указать набор системных команд, которые будут выполняться роутером после каждой загрузки его операционной системы. Startup Script интерпретируется программой sh, встроенной в каждую UNIX-native систему, как если бы это был shell-скрипт. Для получения более подробной информации о вариантах использования функции обратитесь к документам из серии «Примеры конфигурации».

7.9. Страница IP-Up Script

Как открыть: Administration → IP-UP Script

Эта страница позволяет указать набор системных команд, выполняемых после создания 3G/GPRS-соединения. Функция аналогична Startup Script.

7.10. Страница IP-Down Script

Как открыть: Administration → IP-Down Script

Эта страница позволяет указать набор системных команд, выполняемых после разрыва 3G/GPRS-соединения. Функция аналогична Startup Script.

7.11. Страница User Crontab

Как открыть: Administration → User Crontab

Страница предназначена для добавления пользовательских задач в системный планировщик cron. Для включения данной функции установите галочку «Enable user crontab», впишите правило в текстовое поле и нажмите кнопку Save crontab.

Правило выглядит следующим образом:

MM HH DoM DoW Command

где:

MM — минуты (0-59);

HH — часы (0-23);

DoM — день месяца (1-31);

MON — месяц (1-12);



DoW — день недели (0-7, где 0, 7 — воскресенье, 1 — понедельник и т. д.);

Command — команды оболочки или имя скрипта для запуска

Во всех полях, кроме команды, допускается использовать символ звёздочка (*) для обозначения любого значения.

Примеры:

```
0 1 * * 0 reboot
```

Перезагрузка в 01:00 в воскресенье.

```
* * * * * ping 192.168.1.100
```

Пинговать адрес 192.168.1.100 каждую минуту.

7.12. Страница Upload File

Как открыть: Administration → Upload File

Данная страница позволяет загружать файлы на роутер, удалять их и устанавливать атрибут исполняемости для скриптов.

Для загрузки файла нажмите кнопку **Обзор**, выберите файл и нажмите кнопку **Upload**.

Для удаления файла нажмите ссылку **delete** рядом с его именем.

Для установки/снятия атрибута исполняемости нажмите на ссылку **change exec** рядом с именем файла.

7.13. Страница Send SMS

Как открыть: Administration → Send SMS

Эта страница позволяет отправить SMS-сообщение на номер, указанный в текстовом поле после надписи «Phone Number +». Текст сообщения вводится в текстовое поле после надписи «Message Text». Для отправки сообщения необходимо нажать кнопку «Send».

7.14. Страница Disable PIN

Как открыть: Administration → Disable PIN



Эта страница позволяет отключить PIN-код, в случае если на SIM-карте включена его проверка. Для выбора SIM-карты используйте раскрывающийся список, расположенный после надписи «SIM card». PIN-код вводится в текстовое поле после надписи «SIM PIN». Для отмены запроса PIN-кода необходимо нажать кнопку «Disable PIN on selected SIM card» (отключить PIN-код для выбранной SIM-карты).

7.15. Страница Send Report

Как открыть: Administration → Send Report

Эта страница предназначена для передачи отладочной информации в отдел технической поддержки группы компаний «Радиофид».

Нажмите кнопку Generate report чтобы собрать информацию об устройстве. Нажмите кнопку Save report чтобы сохранить отчёт на компьютере. Для удаления собранной информации с роутера нажмите кнопку Remove report.

7.16. Страница Update Firmware

Как открыть: Administration → Update Firmware

Эта страница позволяет:

- узнать тип релиза текущей версии программного обеспечения роутера;
- узнать дату сборки и текущую версию программного обеспечения роутера, версию ядра Linux;
- обновить программное обеспечение роутера.



Внимание!

- Перед обновлением прошивки рекомендуется сохранить резервную копию конфигурации устройства. Создание резервной копии конфигурации роутера описано в разделе «[Страница Backup/Restore](#)».
- Перед прошивкой устройства убедитесь, что файл прошивки предназначен именно для Вашей модели роутера.
- Убедитесь в надежности сети питания, к которой подключен роутер. Рекомендуется использовать источник бесперебойного питания (ИБП) для непрерывной подачи питания на роутер во время обновления его прошивки.
- При прошивке роутера необходимо точно следовать инструкциям.

Описание текущей версии программного обеспечения роутера:

- Router model — модель роутера;
- Firmware version — версия ПО. Состоит из номера версии и модификации. В большинстве случаев модификация будет master;
- Build date — дата и время создания ПО;
- Commit hash — хэш последнего коммита в системе управления версиями;
- Kernel version — имя, версия, дата сборки и архитектура ядра Linux

Внимание! Перед внедрением роутера рекомендуется убедиться, что для прошивки указан тип «master».

7.17. Страница Reboot

Как открыть: Administration → Reboot

Эта страница позволяет:

- вернуться к заводским настройкам;
- выполнить ручную перезагрузку устройства.

Для того чтобы вернуться к заводским настройкам, необходимо установить флажок для опции «Reset configuration to defaults» и затем нажать кнопку «Reboot» (Перезагрузка). Для простой перезагрузки устройства достаточно нажать кнопку «Reboot».



8. Настройка доступа к устройству

Настроить доступ к роутеру можно как через Web-интерфейс, так и через локальную сеть с помощью сервисов SSH и Telnet. Для того чтобы изменить параметры доступа через локальную сеть, необходимо выполнить следующие действия:

1. в web-интерфейсе роутера открыть раздел «Administration» → «Remote access»;
2. разрешить требуемый сервис, установив флажок для опций:
 - Enable SSH on port;
 - Enable Telnet on port.

8.1. Настройка удаленного доступа

По умолчанию доступ к устройству через Интернет запрещен встроенным межсетевым экраном IPTables. Для того чтобы разрешить доступ, требуется выполнить следующие действия:

1. в web-интерфейсе роутера откройте раздел «Administration» → «Remote access»;
2. установите флажок напротив сетевого сервиса, через который требуется получить удаленный доступ:
 - Enable WAN access to HTTP on port;
 - Enable WAN access to SSH on port;
 - Enable WAN access to Telnet on port;
 - Enable WAN access to SNMP on port;
3. в поле после названия сервиса укажите номер сетевого порта, который будет использоваться для удаленного доступа;
4. сохраните настройки, нажав кнопку «Save».

HTTP	
<input checked="" type="checkbox"/> Enable WAN access to HTTP	on port <input type="text" value="8080"/>
SSH	
<input checked="" type="checkbox"/> Enable SSH	on port <input type="text" value="22"/>
<input checked="" type="checkbox"/> Enable WAN access to SSH	on port <input type="text" value="2222"/>
Telnet	
<input checked="" type="checkbox"/> Enable Telnet	on port <input type="text" value="23"/>
<input checked="" type="checkbox"/> Enable WAN access to Telnet	on port <input type="text" value="2323"/>
SNMP	
<input checked="" type="checkbox"/> Enable WAN access to SNMP	on port <input type="text" value="9025"/>
<input type="button" value="Save"/>	

Рис. 8.1 Пример организации доступа. Открыт доступ к сервисам: HTTP (порт 8080), SSH (порт 2222), Telnet (порт 2323), SNMP (порт 9025)



8.2. Управление с помощью команд консоли Telnet/SSH

8.2.1. Удаленное управление по Telnet

Для удаленного управления достаточно установить соединение с IP-адресом устройства на порт службы Telnet. В роутере можно использовать стандартные команды операционной системы Linux. Список доступных команд приведен в [Приложение 2](#).

8.2.2. Удаленное управление по SSH

Управление по SSH аналогично управлению по Telnet, однако управляющий трафик, передаваемый между компьютером и роутером, шифруется для обеспечения безопасности передаваемой информации.



Приложение 1

Синтаксис IP-адреса

IP-адрес описывает адрес узла в IP-сети и состоит из 4х частей (октетов). Октет не может быть больше числа 254. Последний октет не может быть нулем.

Пример: 80.70.224.2

Синтаксис IP-адреса сети

IP-адрес сети описывает все адресное пространство IP-сети. Состоит из 4х частей (октетов) и маски подсети. Октет не может быть больше числа 254, маска подсети не больше числа 32.

Пример: 90.30.173.60/28

Пример 2: 125.24.55.219 255.255.255.0

Синтаксис маски подсети

Маска подсети состоит из 4х октетов, каждый из которых не может быть больше числа 255.

Пример: 255.255.255.0

Синтаксис MAC-адреса

MAC-адрес состоит из 6 частей, каждая из которых не может иметь значение более FF (шестнадцатеричная система счисления).

Пример: 00:FF:BD:69:07:4A



Приложение 2

Доступные команды управления

Ниже приведен список команд, которые могут быть использованы для работы с роутером. Перед вызовом команды рекомендуется ознакомиться с ее описанием.

A	dbclient	ftpget	hwclock
arp	decode	ftpput	hwinfo
ash	depmod	fw_printenv	
awk	df	fw_setenv	I
	dhcpcd	fwload	id
B	dmesg		ifconfig
base64	dnsdomainname	G	ifdown
bash	dnsmasq	gdbserver	ifup
blockdev	dropbear	genhash	inadyn
brctl	dropbearconvert	genreport	inetd
busybox	dropbearkey	getimei	init
byteconv	du	getopt	ip
		getpid	ip6tables
C	E	getty	ip6tables-restore
cat	echo	getusbcom	ip6tables-save
chat	egrep	gpin	ipaddr
chmod	encode	gpio	ipaddress
chown	env	gpiod	ipcalc
chpasswd	expr	grep	iplink
clear		gsminfo	iproute
cont_check	F	gsminfod	iprule
cp	false	gunzip	ipsec_ping
crond	fgrep	gzip	iptables
crontab	firmware_update		iptables-restore
cryptpw	flash_erase	H	iptables-save
cut	flash_lock	halt	iptables-xml
D	flash_unlock	head	iptunnel
date	flashcp	hostname	
	flex	httpd	



K

keepalived
kill
killall
klogd

L

led
less
ln
loaddefaults
loadset
lockfile-check
lockfile-create
lockfile-remove
lockfile-touch
logger
login
logrotate
ls
lsuf

M

mail-lock
mail-touchlock
mail-unlock
makedevs
md5sum
mdev
mesg
migrate_set
mii-diag
mini_snmpd

mkdir
mkfs.jffs2
mknod
mkpasswd
modem
modinfo
modprobe
mount
mv

N

net services
netstat
nohup
nslookup
ntpd
ntpdate

O

openssl
openvpn
opinfo
ovpn_ping

P

passwd
pcgrep
pcretest
picocom
pidof
pin_enter
pin_lock
pin_unlock

ping
pinger
plainrsa-gen
post_decode
poweroff
ppp_ping
ppp_watch
pppd
pppdump
pppinfo
pppstats
printf
ps
pwd
python

R

racoon
racoonctl
reboot
reserved
rm
rmmod
route
run-parts

S

scp
sed
seq
set_gsm_param
setkey
setsim

sh
sim
sim_check
sim_check_pres
sim_check_reg
sim_switch
sleep
sms
sort
ssh
start-stop-daemon
stat
stty
sync
syslogd

T

tail
talk
tar
tcpdump
telnet
telnetd
test
tftp
tftp_reflash
timeconv
top
touch
tr
traceroute
tty-lock
tty-unlock



ttyS1-lock	xtables-multi
ttyS1-unlock	xz
ttyS2-lock	xzcat
ttyS2-unlock	

U

umount
uname
uniq
unxz
update_index
uptime
usb
usleep
ussd
uudecode
uuencode

Y

yes

Z

zcat

V

vconfig
vi

W

watchdog
wc
wget
wget_reflash
which

X

xl2tpd
xl2tpd-control