Robustel GoRugged R3000

Промышленный VPN маршрутизатор с поддержкой двух SIM карт для GPRS/EDGE/UMTS/HSPA/LTE сетей

Руководство пользователя

Название документа:	**Руководство пользователя**
Встроенное микропрограммное обеспечение:	**1.01.00**
Дата:	**17-01-2014**
ID документа:	**RT_UG_R3000_v.2.0.0**

Robustel

Об этом документе

В настоящем документе описано аппаратное и программное обеспечение промышленного маршрутизатора Robustel R3000, поддерживающего две SIM-карты и работу в сетях 2G/3G/4G.

Перевод ООО «ЕвроМобайл».

Торговые марки и разрешения

Robustel - торговая марка компании Guangzhou Robustel Technologies Co. Limited.

Все другие торговые марки и торговые марки, упомянутые в этом документе, являются собственностью соответствующих правообладателей.

Заявление об ограничении ответственности

Никакая часть этого документа не может быть воспроизведена, ни в какой форме без письменного разрешения владельца авторских прав. Содержание этого документа изменяется без уведомления в соответствии с постоянным совершенствованием технологий, разработки и производства. Robustel не несет ответственности за какие-либо ошибки или повреждения любого вида, проистекающие из использования настоящего документа.

Важное замечание

Принцип беспроводной связи не позволяет гарантировать передачу и прием данных в любых условиях. Данные могут задерживаться, повреждаться (т. е. иметь ошибки) или даже полностью теряться. Хотя существенные задержки или потеря данных редки, при нормальном функционировании беспроводных устройств, например, маршрутизаторов, в сети надлежащего качества, маршрутизатор не должен использоваться в ситуациях, где отказ в передаче или получении данных может привести к любого рода повреждениям для пользователя или любой другой стороны, включая, но, не ограничиваясь телесными повреждениями, смертью или материальным ущербом. Robustel не принимает ответственности за какие-либо убытки, вытекающие из задержек или ошибок в передаче или приеме данных с помощью маршрутизатора, или отказов маршрутизатора в передаче или приеме указанных данных.

Меры безопасности

Общие положения

- Маршрутизатор генерирует радиочастотное излучение. При эксплуатации маршрутизатора необходимо учитывать проблемы, связанные с радиочастотными помехами и нормативные положения относительно радиочастотного оборудования.
- Недопустимо пользоваться маршрутизатором в самолете, больницах, на бензозаправочных станциях или в местах, где использование сотовых устройств запрещено.
- Необходимо убедиться, что маршрутизатор не будет создавать помех расположенному неподалеку оборудованию. Например, кардиостимулятору или иному медицинскому оборудованию. Антенна маршрутизатора должна располагаться в стороне от компьютеров, оргтехники, бытовой техники и т.д.
- Для надлежащего функционирования к маршрутизатору необходимо подключить внешнюю антенну. Допускается использование только одобренных антенн. Приобрести одобренную антенну можно у авторизованного дистрибьютора.
- Для безопасности антенна должна располагаться на расстоянии не менее 26,6 см от человеческого тела. Не следует помещать антенну в металлическую оболочку, контейнер и т.п.
- Заявления о воздействии РЧ (RF)

  1. Для мобильных устройств, не располагающихся совместно (передающая антенна установлена или расположена на расстоянии более 20 см от тела пользователя и др. людей),
- Воздействия излучения РЧ в соответствии с требованиями Федеральной комиссии по связи США
  1. Данный передатчик не должен быть расположен вблизи и не должен работать совместно, ни с какой другой антенной или передатчиком.
  2. Это оборудование соответствует предельным нормам Федеральной комиссии по связи США, касающимся предельному воздействию РЧ излучения для неконтролируемой среды.
     Это оборудование должно устанавливаться и эксплуатироваться на расстоянии не менее 20 сантиметров между его радиатором и телом человека.

***Примечание**: на некоторых авиалиниях может разрешаться использование сотовых телефонов пока самолет находится на земле с открытой дверью.*

В это время допускается пользоваться маршрутизатором.

Пользование маршрутизатором в автомобиле

- Перед установкой маршрутизатора в автомобиле следует ознакомиться с местным законодательством и нормативами, касающихся использования устройств сотовой связи на транспорте.
- Водитель или оператор любого транспортного средства не должны работать с маршрутизатором во время движения.

- Установка маршрутизатора должна выполняться квалифицированным персоналом. Следует проконсультироваться с дистрибьютором машины относительно возможности помех электронным компонентам со стороны маршрутизатора.
- Маршрутизатор должен подключаться к бортовой сети электропитания через защищенный предохранителем разъем в блоке предохранителей машины.
- В случае питания маршрутизатора от основного аккумулятора автомобиля необходимо соблюдать осторожность. Через продолжительное время аккумулятор может быть разряжен.

Защита маршрутизатора

Для гарантии надлежащего функционирования необходимо соблюдать аккуратность при эксплуатации. Ниже перечислены основные правила эксплуатации.

- Не допускается подвергать маршрутизатор воздействию экстремальных условий: высокой влажности/дождя, высоким температурам, прямому солнечному свету, контактам с едкими химикатами, пылью или водой.
- Запрещается разбирать или изменять маршрутизатор. Внутри маршрутизатора отсутствуют части, требующие обслуживания пользователем, а гарантия утратит силу.
- Не бросать. Не подвергать ударам и тряске. Запрещается эксплуатация модема в условиях значительных вибраций.
- Не выдергивать кабель электропитания или антенну. Присоединение/отсоединение производить за коннектор.
- Подключения маршрутизатора следует призводить исключительно в соответствии с руководством по эксплуатации. Несоблюдение влечет прекращение действия гарантии.
- В случае возникновения проблем следует обращаться к авторизованному дистрибьютору.

Информация о нормативах и сертификатах соответствия

Таблица 1: Директивы

2002/95/EC	Директива Европарламента и Европейского Совета от 27 января 2003 по ограничению использования определенных опасных веществ в электро- и электронном оборудовании (RoHS)	
2002/96/EC	Директива Европарламента и Европейского Совета от по отходам электро- и электронного оборудования (WEEE)	
2003/108/E C	Директива Европарламента и Европейского Совета от 8 декабря 2003, вносящая поправки вдирективу 2002/96/ec по отходам электро- и электронного оборудования (WEEE)	

Таблица 2: Стандарты

SJ/T 11363-2006	«Требования по предельной концентрации для определенных опасных веществ в электронной информационной продукции» (2006-06).
SJ/T 11364-2006	«Маркировка для контроля загрязнений, вызываемых электронной информационной продукцией» (2006-06). Согласно «Китайскому управлению по контролю загрязнений, вызываемых электронной информационной продукцией» (ACPEIP) EPUP, т. е. период использования в целях защиты окружающей среды, данного продукта составляет 20 лет согласно приведенному здесь символу, если не указано иное. EPUP применим только, пока продукт используется в пределах ограничений на условия эксплуатации, описанных в Описании аппаратного интерфейса. См. Таблицу 3 с обзором токсичных или опасных веществ или элементов, которые могут содержаться в частях продукта в концентрациях выше пределов, определенных SJ/T 11363-2006. 

Таблица 3: Токсичные или опасные вещества или элементы с определенными пределами концентрации

Название компонента	Опасные вещества					
	(Pb)	(Hg)	(Cd)	(Cr(VI))	(PBB)	(PBDE)
Металлические компоненты	o	o	o	o	o	o
Модули схемы	x	o	o	o	o	o
Кабели и кабельные сборки	o	o	o	o	o	o
Пластмассовые и полимерные компоненты	o	o	o	o	o	o

o:
Указывает, что данное токсичное или опасное вещество, содержится во всех гомогенных материалах данного компонента в концентрации ниже предельной по требованиям в SJ/T11363-2006.
X:
Указывает, что данное токсичное или опасное вещество, содержится во всех гомогенных материалах данного компонента в концентрации, которая *может превышать* предельную по требованиям в SJ/T11363-2006.

История изменений

Обновления между версиями документа являются суммарными. Поэтому, последняя версия документа содержит все обновления предыдущих версий.

Дата версии	Версия встроенного микропрограммного обеспечения	Версия документа	Описание
24-01-2013	1.00	v.1.0.0	Первый выпуск
17-01-2014	1.01	v.2.0.0	Второй выпуск

Содержание

Глава 1 Общие сведения

1.1 Обзор

Robustel GoRugged R3000 является компактным сотовым маршрутизатором, обеспечивающим самую современную мобильную связь для M2M (машина/машина) приложений.

- Избыточность за счет поддержки двух SIM-карт для непрерывных сотовых соединений, поддержка 2G/3G/4G.
- Управление каналами связи через глобальные сети: резервное копирование с беспроводным доступом WAN/Ethernet, WAN WAN/WLAN.
- VPN туннель: IPSec/OpenVPN/PPTP/L2TP/GRE.
- Поддержка шлюза Modbus (RTU/ASCII Modbus — TCP Modbus).
- Поддержка (дополнительно) GPS, обеспечивает получение местоположения в реальном времени и трекинг.
- Поддержка Wi-Fi 802.11 b/g/n (дополнительно), режим точка доступа и клиентский.
- Поддержка SDK, наличие пользовательского интерфейса программирования.
- Автоматическая перезагрузка по SMS/Caller ID/по расписанию.
- Поддержка централизованной платформы M2M управления RobustLink.
- Гибкие методы управления: Web/CLI/SNMP/RobustLink.
- Обновление ПО через Web/CLI/USB/SMS/RobustLink.
- Различные интерфейсы: RS232/RS485/Console/DI/DO/USB/Ethernet.
- Широкий диапазон входных напряжений от 9 до 60 В постоянного тока, рабочие температуры вплоть до экстремальных.
- Металлический корпус допускает монтаж на Din-рейку или на стену, оснащен винтом заземления.

1.2 Комплектность

Необходимо проверить упаковку, чтобы удостовериться в наличии перечисленных ниже компонентов.

- Маршрутизатор Robustel GoRugged R3000, 1 шт.

- 3-контактная сменная клеммная колодка с блокировкой для электропитания, 1 шт.

- 7-контактная сменная клеммная колодка с блокировкой для последовательного порта, входа-выхода и порта консоли, 1 шт.

- Компакт-диск с руководством пользователя, 1 шт.

Примечание*: если какой-либо из вышеупомянутых элементов отсутствует или поврежден, обратитесь к местному торговому представителю.*

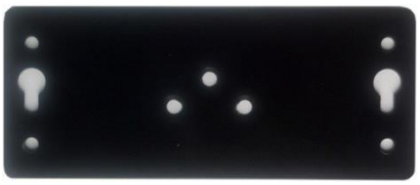
Дополнительные аксессуары (могут быть приобретены отдельно):

- Антенна SMA (короткая штыревая или магнитная антенна, дополнительная), 1 шт.

Штыревая антенна *Антенна на магнитном основании*

- Кабель Ethernet, 1 шт.

- Набор для настенного монтажа



- Набор для монтажа на 35-мм Din-рейку.

- Адаптер электропитания AC/DC (12 В постоянного тока, 1,5 А), 1 шт. (дополнительно разъемы для ЕС, США, Великобритании)

1.3 Технические характеристики

Сотовый интерфейс

- Стандарты: GSM/GPRS/EDGE/UMTS/HSPA/EVDO/FDD LTE
- GPRS/EDGE: 850/900/1800/1900 МГц
- HSUPA: 900/2100 или 850/1900 МГц дополнительно, DL/UL 7,2/5,76 Мбит/с, переход на аварийный режим 2G
- HSPA +: 850/900/1900/2100, DL/UL 21/5,76 Мбит/с, переход на аварийный режим 2G
- FDD LTE: 800/900/1800/2100/2600 МГц, DL/UL 100/50 МГц 800/900/1800/2100/2600, DL/UL 100/50 Мбит/с, переход на аварийный режим 3G/2G
- EVDO: 450 или 800/1900 МГц, v.A/B
- SIM-карта: 2 x (3 В и 1,8 В)
- Антенный интерфейс: SMA (розетка)

Интерфейс Ethernet

- Количество портов: 2 x 10/100 Мбит/с, 2 LAN или 1 LAN и 1 WAN
- Защитная изоляция: 1,5 кВ

WLAN (дополнительно, Wi-Fi)

- Стандарты: 802.11b/g/n до 65 Мбит/с, режим точка доступа/клиент
- Полоса частот: 2400 - 2500 ГГц (ISM 2,4 ГГц)
- Безопасность: открытый ключ (Open) ,WPA, WPA2
- Шифрование: AES, TKIP
- Антенный интерфейс: SMA (розетка)
- Мощность передатчика: 802.11b: 17 дБм, 802.11g/n: 15 дБм
- Чувствительность приемника: 1M: -97 дБм, 2M: -93 дБм, 6M: -91 дБм, 11M: -89 дБм, 54M: -75 дБм, 65M: -72 дБм

GPS (дополнительно)

- Антенный интерфейс: SMA (розетка), импеданс 50 Ом

- Чувствительность трекинга: лучше чем -158 дБм
- Протокол: NMEA-0183 V2.3

Последовательный интерфейс

- Количество портов: 1 x RS-232, 1 x RS-485 или 2 x RS-232 или 2 x RS-485
- Защита от электростатического разряда : ±15 кВ
- Параметры: 8E1, 8O1, 8N1, 8N2, 7E2, 7O2, 7N2, 7E1
- Скорость в бодах: 300 бит/с ... 230400 бит/с
- RS-232: TxD, RxD, RTS, CTS, GND
- RS-485: Data+ (A), Data- (B), GND
- Интерфейс: 3,5-мм клеммная колодка с блокировкой

Цифровой вход

- Тип: 2 x DI, Сухой Контакт
- Сухой Контакт: On: разомкнут, Off: закорочен на GND
- Изоляция: 3 кВ постоянного тока или 2 кВ rms
- Временной интервал цифровой фильтрации: выбирается программно
- Интерфейс: 3,5-мм клеммная колодка с блокировкой

Цифровой выход

- Тип: 2 x DO
- Изоляция: 3 кВ постоянного тока или 2 кВ rms
- Абсолютное максимальное напряжение постоянного тока: 36 В
- Абсолютный максимальный постоянный ток: 50 мА
- Интерфейс: 3,5-мм клеммная колодка с блокировкой

Система

- Светодиодные индикаторы: RUN, PPP/WLAN, USR, RSSI, NET, SIM
- Встроенные RTC, сторожевой таймер, таймер
- Расширение: 1 x USB host 2.0 до 480 Мбит/с
- Хранение данных: 1 x microSD

Программное обеспечение

- Сетевые протоколы: PPP, PPPoE, TCP, UDP, DHCP, ICMP, NAT, DMZ, RIP v1/v2, OSPF, DDNS, VRRP, HTTP, HTTPs, DNS, ARP, QoS, SNTP, Telnet и др.
- VPN туннель: IPSec/OpenVPN/PPTP/L2TP/GRE
- Брандмауэр: SPI, anti-DoS, Фильтр, Контроль доступа
- Управление: Web, CLI, SNMP v1/v2/v3, SMS, RobustLink
- Последовательный порт: TCP client/server, UDP, Modbus RTU/ASCII ↔ Modbus TCP, Virtual COM (COM port redirector)
- RobustLink: централизованная M2M платформа управления

Электропитание и потребление

- Интерфейс электропитания: 5-миллиметровая клеммная колодка с блокировкой
- Входное напряжение: 9 - 60 В постоянного тока
- Энергопотребление: в дежурном режиме: 100 мА при 12 В
- при передаче данных: 400 мА (пик) при 12 В

Физические характеристики

- Корпус и масса: металл, 500 г

- Размеры (Д x Ш x В): 125 x 108 x 45 мм
- Способ монтажа: 35-мм Din-рейка, настенное или настольное крепление

Информация о нормативах и сертификатах соответствия

- Аттестация и директивы: CE, R&TTE, FCC, RCM, RoHS, WEEE
- Электромагнитная совместимость EN 61000-4-2 уровень 4 (ESD), EN 61000-4-3 (PTC) уровень 4
  EN 61000-4-4 (EFT) уровень 4, EN 61000-4-5 (импульс) уровень 3
  EN 61000-4-6 (CS) уровень 4, EN 61000-4-8, EN 61000-4-12

Условия эксплуатации

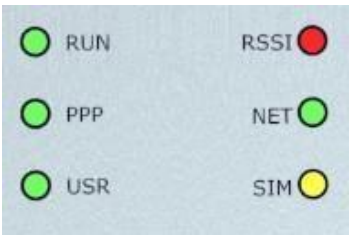
Модель №	Описание	Условия эксплуатации
R3000-2G	GPRS маршрутизатор	- 40 — 85°C / 5 — 95% отн. влажности
R3000-2E	EDGE маршрутизатор	- 40 — 75°C/5 — 95% отн. влажности
R3000-3H	HSUPA маршрутизатор	- 40 — 85°C / 5 — 95% отн. влажности
R3000-3P	HSPA + маршрутизатор	- 40 — 85°C / 5 — 95% отн. влажности
R3000-3E	EVDO версия A/B маршрутизатор	- 20 — 60°C / 5 — 95% отн. влажности
R3000-4L	FDD LTE маршрутизатор	- 25 — 60°C / 5 — 95% отн. влажности
R3000-NU	маршрутизатор без GSM модуля	- 40 — 85°C / 5 — 95% отн. влажности

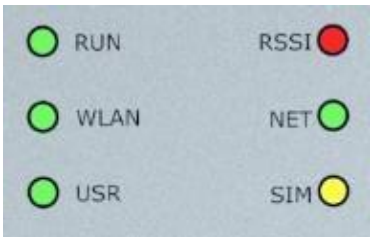
1.4 Данные для выбора и заказа

См. таблицу данных соответствующего R3000.

Глава 2 Установка

2.1 Светодиодные индикаторы

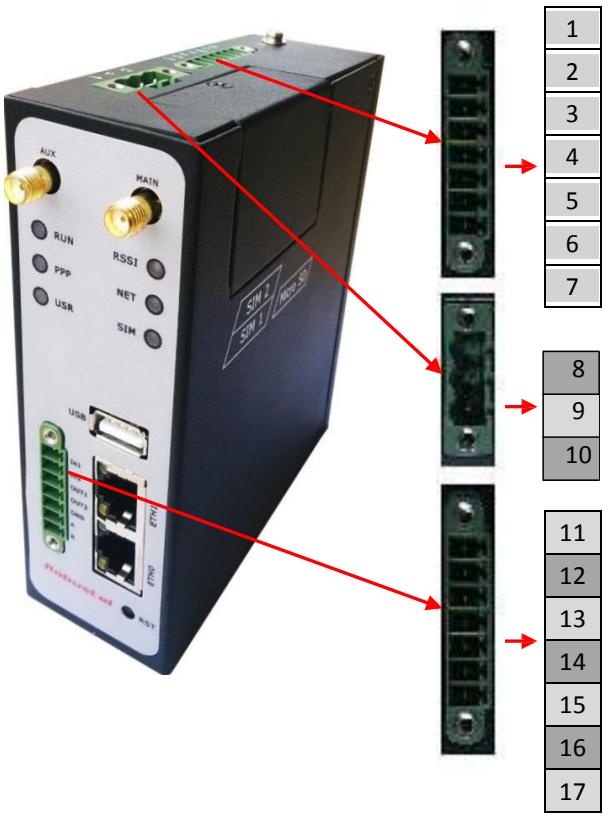




Название	Цвет	Состояние	Функция
RUN	Зеленый	Мигание	Маршрутизатор готов
		Вкл.	Запуск маршрутизатора
		Выкл.	Питание маршрутизатора отключено
WLAN/ PPP	Зеленый	Мигание	**Индикатор WLAN:** передача данных **Индикатор PPP:** нуль
		Вкл.	**Индикатор WLAN:** Wi-Fi точка доступа/клиент активировано. **Индикатор PPP:** установлено соединение PPP
		Выкл.	**Индикатор WLAN:** Wi-Fi точка доступа/клиент выключено **Индикатор PPP:** соединение PPP не активно.
USR	Зеленый	Вкл./мигает	Активно VPN туннель/PPPoE/DynDNS/GPS
		Выкл.	VPN туннель/PPPoE/DynDNS/GPS не активн.
RSSI	Зеленый	Вкл.	Уровень сигнала: 21-31 (наилучший уровень сигнала)
	Желтый	Вкл.	Уровень сигнала: 11-20 (средний уровень сигнала)
	Красный	Вкл.	Уровень сигнала: 1-10 (исключительный уровень сигнала)
NET	Зеленый	мигает	Установлено 4G подключение, отказ соединения PPP
		Вкл.	Установлено 4G подключение, активно соединение PPP
	Желтый	мигает	Установлено 3G подключение, отказ соединения PPP
		Вкл.	Установлено 3G подключение, активно соединение PPP
	Красный	мигает	Установлено 2G подключение, отказ соединения PPP
		Вкл.	Установлено 2G подключение, активно соединение PPP
	/	Выкл.	Невозможно зарегистрироваться в какой-либо сети.
SIM	Зеленый	мигает	Обнаружена только SIM 1, ошибочный PIN-код
		Вкл.	Работа с SIM 1 в обычном режиме
	Желтый	мигает	Обнаружена только SIM 2, ошибочный PIN-код
		Вкл.	Работа с SIM 2 в обычном режиме
	Зеленый и Желтый	Вспышки со сменой цвета	Обнаружены две SIM-карты, оба PIN-кода ошибочны
	/	Выкл.	SIM-карта не обнаружена

***Примечание**: пользователь может выбрать состояние светодиода USR. См. 23.38*

2.2 Назначение контактов



Конт.	Отладка	RS232	Электропитание	Цифровой вход/выход	RS485
1	RXD				
2	TXD				
3	GND	GND			
4		TXD			
5		RXD			
6		RTS			
7		CTS			
8			Положительный		
9			Отрицательный		
10			GND		
11				вход 1	
12				вход 2	
13				выход 1	
14				выход 2	
15				GND	
16					Data+(A)
17					Data- (B)

2.3 USB интерфейс

USB интерфейс используется для обновления встроенного ПО в пакетном режиме и не предназначен для передачи данных от ведомых устройств с USB.

В этот разъем можно вставить USB накопитель, например, флеш- или жесткий диск, если на подключенном накопителе будет файл конфигурации или встроенное микропрограммное обеспечение R3000, устройство автоматически обновит конфигурацию или встроенное ПО.

2.4 Кнопка Reset (сброс)

Функция	Действия
Перезагрузка	В рабочем режиме нажать и удерживать кнопку в течение 5 секунд.
Восстановление заводских установок	Нажать и удерживать кнопку в течение 60 секунд, одновременно включив питание маршрутизатора, все три светодиода слева (RUN, PPP, USR) должны одновременно вспыхнуть 5 раз.

2.5 Порты Ethernet

Каждый порт Ethernet имеет два светодиодных индикатора (см. рис.) Желтый —**скорость**, зеленый — **соединение**. Каждый индикатор имеет три состояния. См. таблицу ниже.

Индикатор	Состояние	Описание
Индикатор скорости	Выкл.	Режим 10 Мбит/с.
	Вкл.	Режим 100 Мбит/с.
Индикатор соединения	Выкл.	Соединение разорвано.
	Вкл.	Соединение установлено.
	Мигает	Идет передача данных.

2.6 Монтаж маршрутизатора

Для настенного крепления маршрутизатора следует использовать 2 винта M3.

Или закрепить маршрутизатор на DIN-рейке 3 винтами M3.

2.7 Установка SIM и microSD карт

- **Установка SIM-карты или микро SD карты**

1. Удостовериться в отключении электропитания.
2. С помощью отвертки отвинтить винт крышки, удалить ее, ниже расположены слоты для SIM и Микро SD карт.
3. Вставить SIM- или микро SD-карту и нажать на нее до щелчка. Установить крышку и закрепить винтом с помощью отвертки.

■ **Удаление SIM- или микро SD-карты**

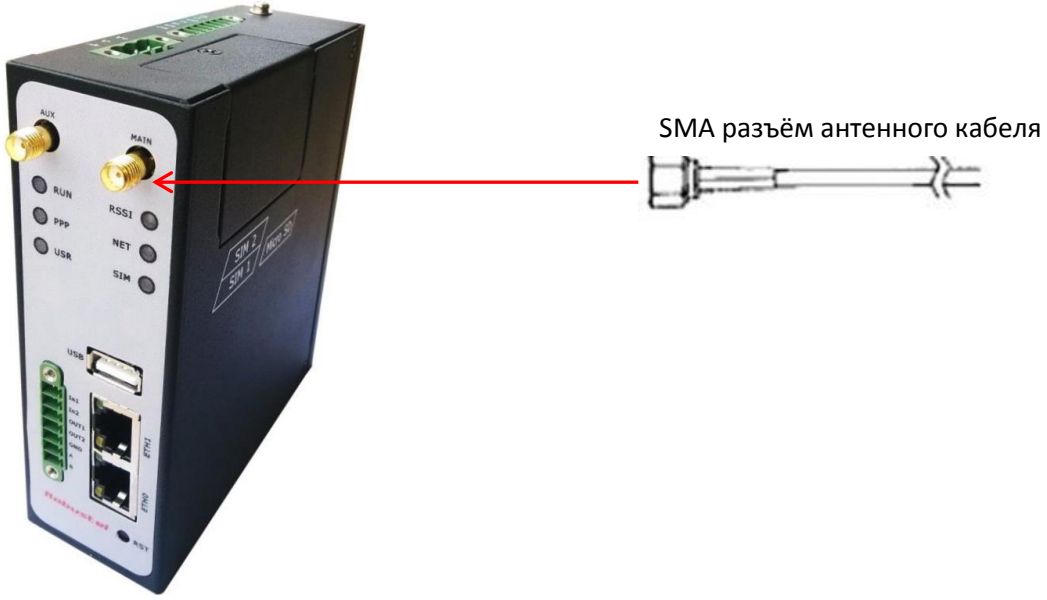
1. Удостовериться в отключении питания маршрутизатора.
2. Нажать на карту до щелчка, карта выдвинется, после чего может быть извлечена.

Примечание:

1. *Следует крепить крышку винтом, это предохранит ее от хищения.*
2. *Не следует касаться металлических поверхностей на SIM-карте, это может привести к повреждению и утрате информации на карте.*
3. *Не изгибать и не царапать SIM-карту. Не подвергать карту воздействию электричества и магнетизма.*
4. *Перед установкой или удалением SIM- или микро SD-карты удостовериться в отключении питания маршрутизатора.*

2.8 Подключение внешней антенны (SMA)

Внешняя антенна подключается штекером к SMA разъему. Необходимо удостовериться, что используемая антенна предназначена для требуемой вашим GSM/3G/4G оператором частоты и имеет импеданс 50 Ом, соединение должно быть плотно затянуто.



2.9 Заземление маршрутизатора

Заземление и должная прокладка кабеля ограничивают влияние электромагнитных помех (EMI). Перед подключением устройств следует выполнить заземление, соединив проводом винт с заземленной поверхностью.

Примечание*: Данный продукт предназначен для монтажа на тщательно заземленную поверхность, например, металлическую панель.*

Глава 3 Настройка через веб

Маршрутизатор может быть сконфигурирован через веб-браузер. Веб-браузер включается в качестве стандартного приложения в следующие операционные системы: Linux, Mac OS, Windows 98/NT/2000/XP/ME/Vista/7/8 и т.д. Продукт снабжен легким и удобным интерфейсом конфигурирования.

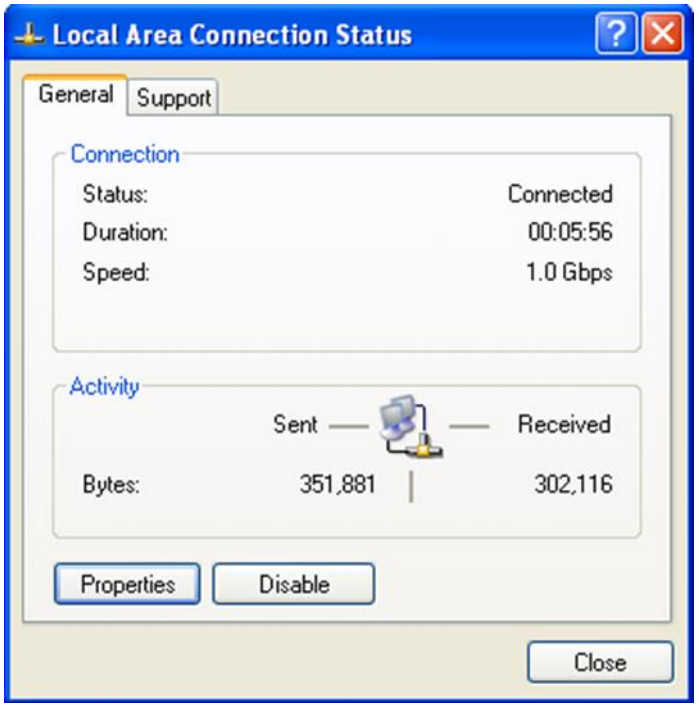
Подключение маршрутизатора можно выполнить различными способами: через внешний репитер/концентратор или непосредственно подключить к ПК. Однако предварительно на ПК должен быть настроен интерфейс Ethernet.

На ПК необходимо задать получение IP-адреса через DHCP сервер или — фиксированный IP-адрес, принадлежащий той же подсети, в которой работает маршрутизатор. Лучший и наиболее легкий путь — настроить ПК на автоматическое получение IP-адреса от маршрутизатора через DHCP. В случае каких-либо проблем с доступом к веб-интерфейсу маршрутизатора, желательно удалить программу брандмауэр на используемом ПК, поскольку она может препятствовать доступу к IP-адресу маршрутизатора.

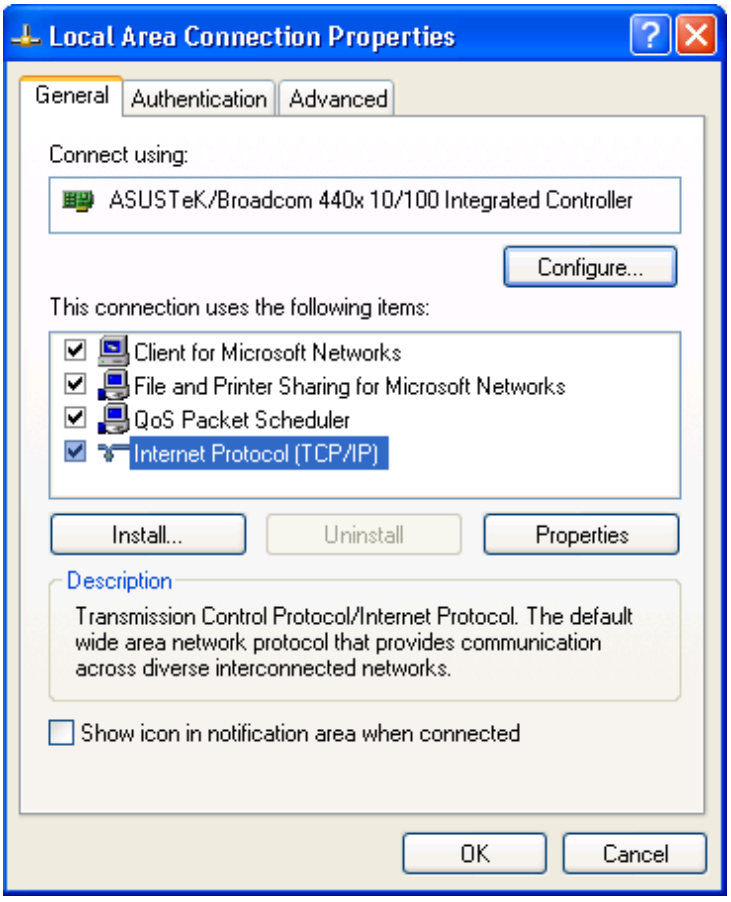
3.1 Конфигурирование ПК в Windows

1. Перейти *Start / Control Panel* (Пуск/Панель управления) в случае классического интерфейса. Выполнить двойной щелчок на пункте *Control Panel — Network Connections* (Панель управления / Сетевые подключения).
2. Дважды щелкнуть *Local Area Connection* (Подключение к локальной сети).

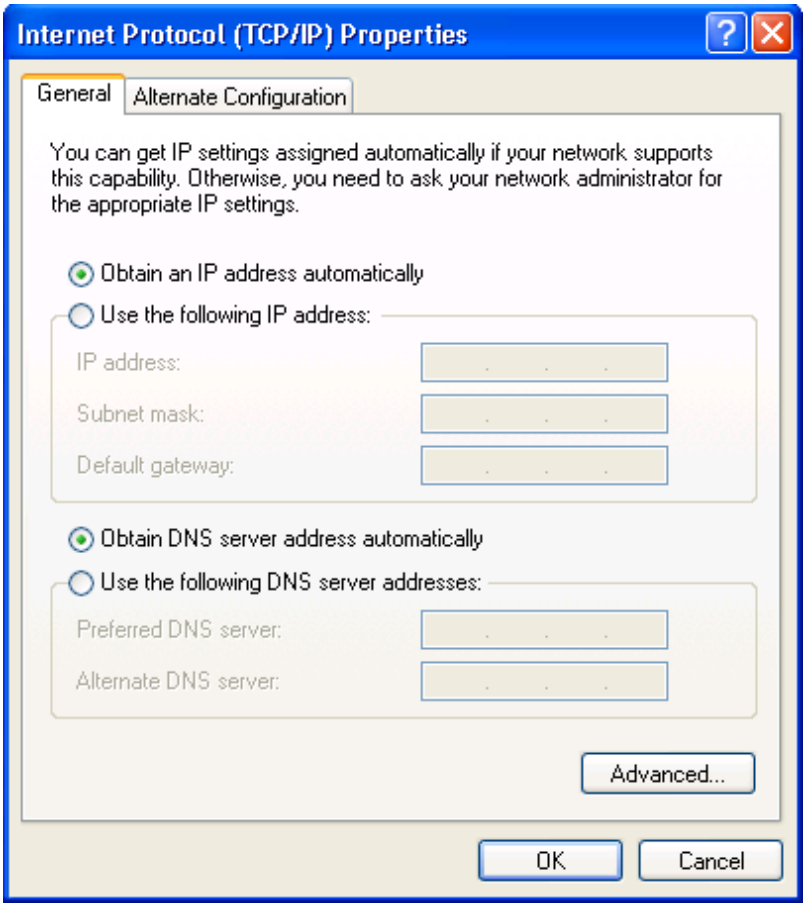
3. В окне *Local Area Connection — Status* (Подключение по локальной сети - состояние) щелкнуть *Properties* (Свойства).



4. Выбрать Internet Protocol (TCP/IP) (Протокол Интернет (TCP/IP)) и щелкнуть *Properties* (Свойства).



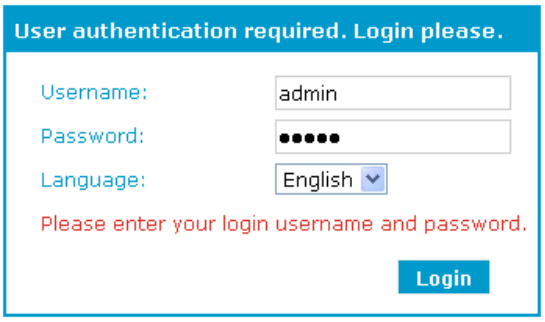
5. Поставить отметки в переключателях *Obtain an IP address automatically* и *Obtain DNS server address automatically* (Получать IP-адрес автоматически и Автоматически получать адрес сервера DNS).



6. Нажать *OK* для выхода из настроек.

3.2 Заводские настройки

Прежде, чем конфигурировать маршрутизатор, необходимо знать следующие настройки по умолчанию.

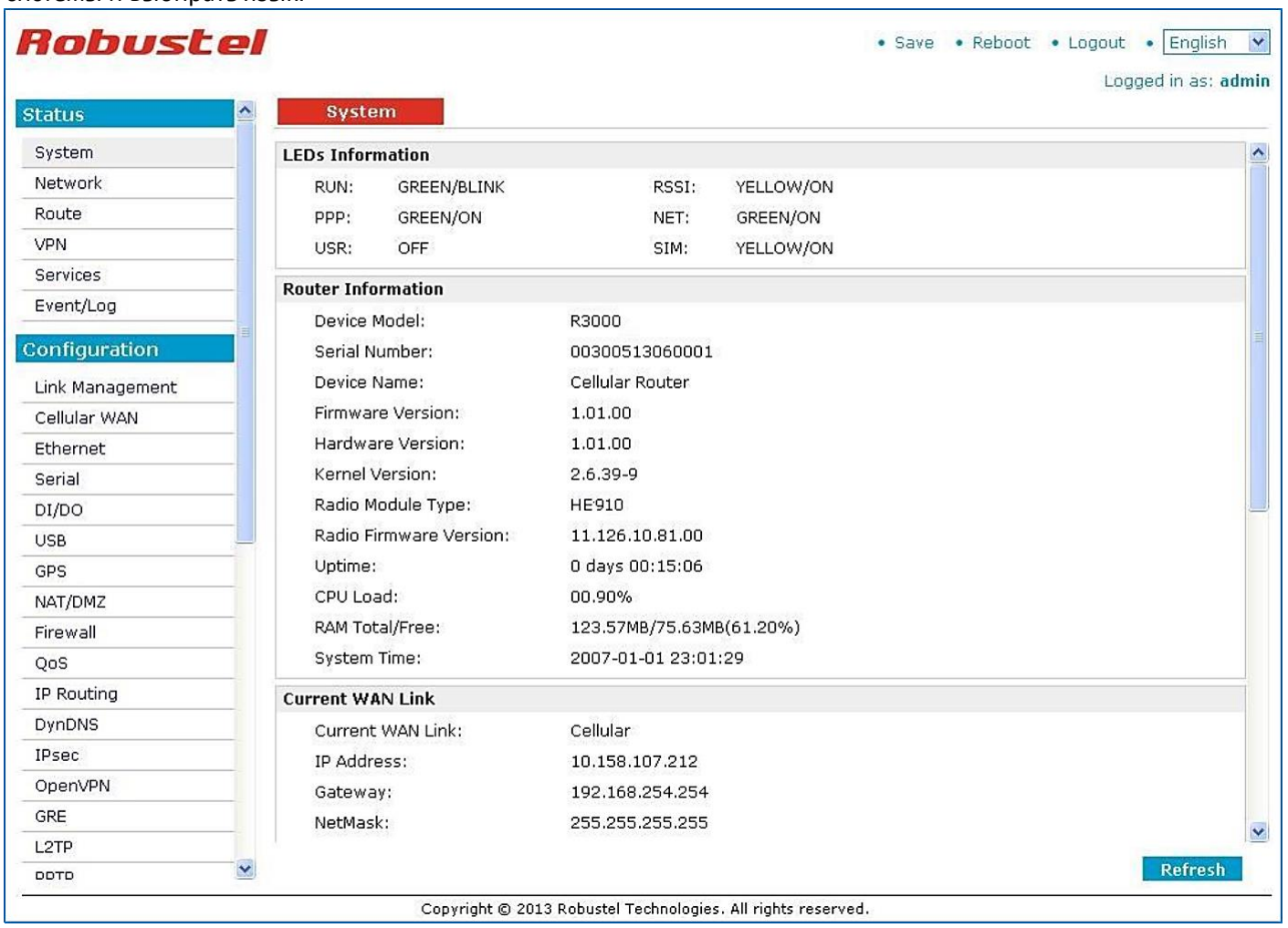


Элемент	Описание
Username (Имя пользователя)	admin
Password (Пароль)	admin
Eth0	192.168.0.1/255.255.255.0, режим LAN
Eth1	192.168.0.1/255.255.255.0, режим LAN

Сервер DHCP включен.

3.3 Панель управления

Этот раздел позволяет пользователю сохранять конфигурацию, перезагружать маршрутизатор, выходить из системы и выбирать язык.



Панель		
Элемент	Описание	Кнопка
Save (Сохранить)	Щелкнуть, чтобы сохранить текущую конфигурацию во флэш-память маршрутизатора.	• Save
Reboot (Перезагрузка)	После сохранения текущей конфигурации, маршрутизатор необходимо перезагрузить, чтобы изменения вступили в силу.	• Reboot
Logout (Выход из системы)	Щелкнуть для возврата к странице авторизации.	• Logout
Language (Язык)	Доступен выбор из китайского, английского, немецкого, французского и испанского языков.	• English
Refresh (Обновить)	Щелкнуть для обновления состояния.	Refresh
Apply (Применить)	Щелкнуть, чтобы применить изменения на каждой странице конфигурации.	Apply
Cancel (Отмена)	Щелкнуть, чтобы отменить изменения на каждой странице конфигурации.	Cancel

Примечание: *шаги, необходимые для редактирования конфигурации.*

1. *Внести изменения на одной странице;*
2. *Щелкнуть* Apply *внизу этой страницы;*
3. *Внести изменения на другой странице;*
4. *Щелкнуть* Apply *внизу этой страницы;*
5. *Завершить все изменения;*
6. *Щелкнуть* • Save *;*
7. *Щелкнуть* • Reboot *;*

3.4 Status -> System (Состояние -> Система)

Этот раздел выводит информацию о состоянии маршрутизатора: индикация светодиодов, сведения о маршрутизаторе, текущий WAN канал, сотовое подключение.

Состояние светодиодных индикаторов

Подробное описание см.2.1 Светодиодные индикаторы.

System

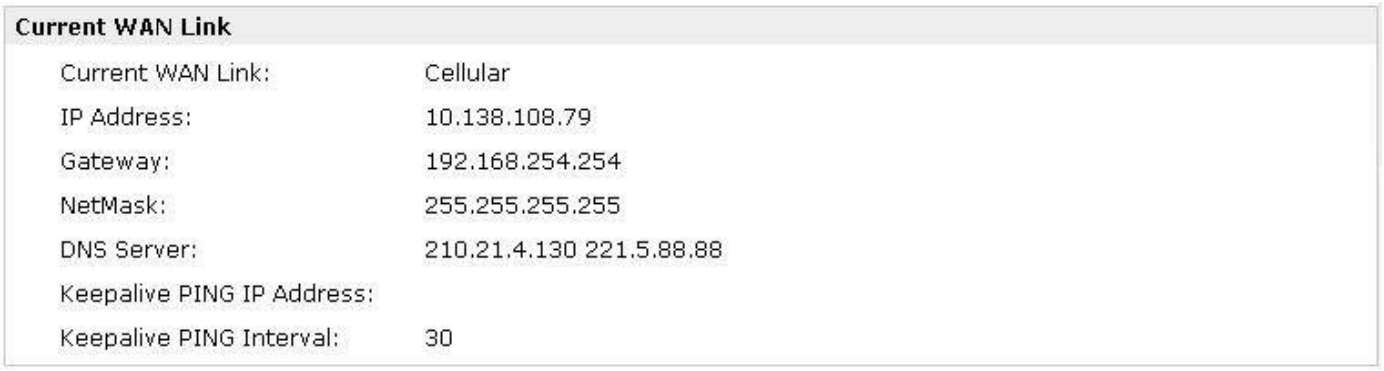
LEDs Information

RUN:	GREEN/BLINK	RSSI:	RED/ON
PPP:	GREEN/ON	NET:	YELLOW/ON
USR:	OFF	SIM:	YELLOW/ON

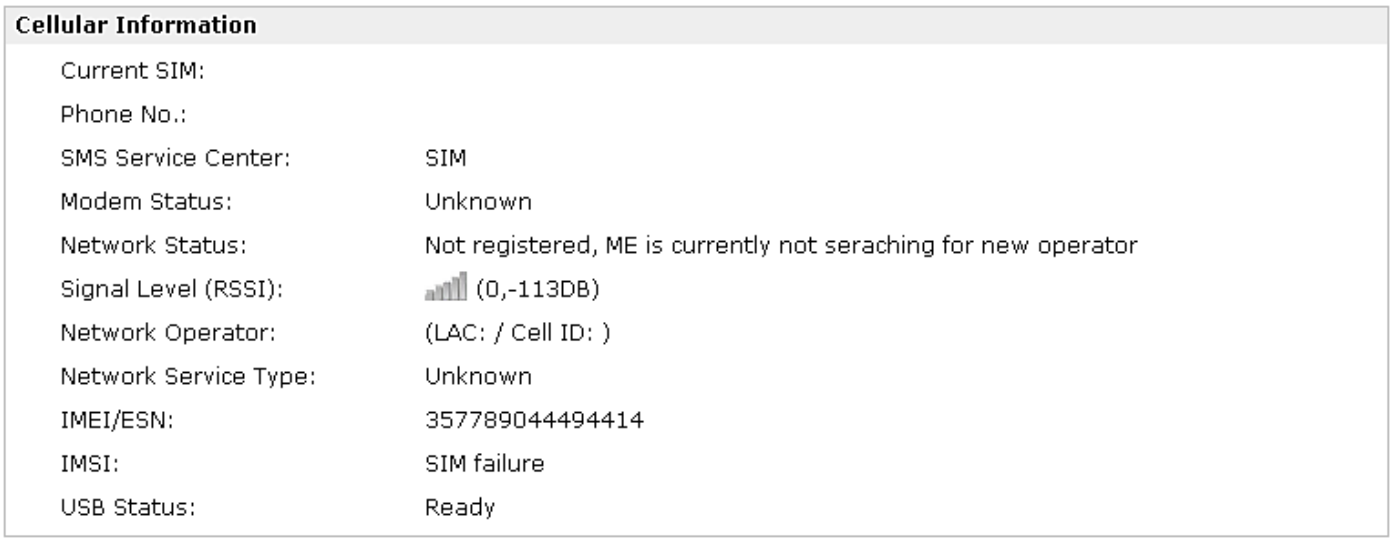
Router Information

Device Model:	R3000
Serial Number:	robustel sn
Device Name:	Cellular Router
Firmware Version:	1.01.00
Hardware Version:	1.01.00
Kernel Version:	2.6.39-3
Radio Module Type:	EM770W
Radio Firmware Version:	11.126.10.87.809
Uptime:	0 days 06:37:42
CPU Load:	00.00%
RAM Total/Free:	123.11MB/72.60MB(58.97%)
System Time:	2013-03-13 14:56:16

Информация о маршрутизаторе	
Элемент	Описание
Device Model (Модель устройства)	Название модели текущего устройства
Serial Number (Серийный номер)	Серийный номер текущего устройства
Device Name (Название устройства)	Название устройства (позволяет различать установленные устройства).
Firmware Version (Версия встроенного ПО)	Версия используемого встроенного микропрограммного обеспечения
Hardware Version (Аппаратная версия)	Версия используемого аппаратного обеспечения
Kernel Version (Версия ядра)	Используемая версия ядра
Radio Module Type (тип радиомодуля)	Тип используемого радиомодуля
Radio Firmware Version (версия встроенного ПО радиомодуля)	Текущая версия встроенного микропрограммного обеспечения радиомодуля
Uptime (Время работы)	Время работы маршрутизатора с момента включения
CPU Load (Загрузка ЦП)	Текущая загрузка ЦП
RAM Total/Free (всего/свободно)	Объем полной и свободной памяти RAM
System Time (Системное время)	Текущее системное время



Текущий канал WAN	
Текущий канал WAN	Сотовое подключение WAN или Ethernet WAN.
IP Address (IP-адрес)	Текущий IP-адрес WAN
Gateway (шлюз)	Текущий шлюз
NetMask (маска подсети)	Текущая маска подсети
DNS Server (сервер DNS)	Текущие первичный и вторичный DNS серверы
Keeping PING IP Address (эхо-тестирование IP-адреса)	Текущий сервер, для которого осуществляется эхо-тестирование ICMP, (задается в *Configuration->LinkConfiguration->Link Management*).
Keeping PING Interval (интервал эхо-тестирования)	Интервал (ы) эхо-тестирования ICMP, (задается в *Configuration->Link-> Management).*

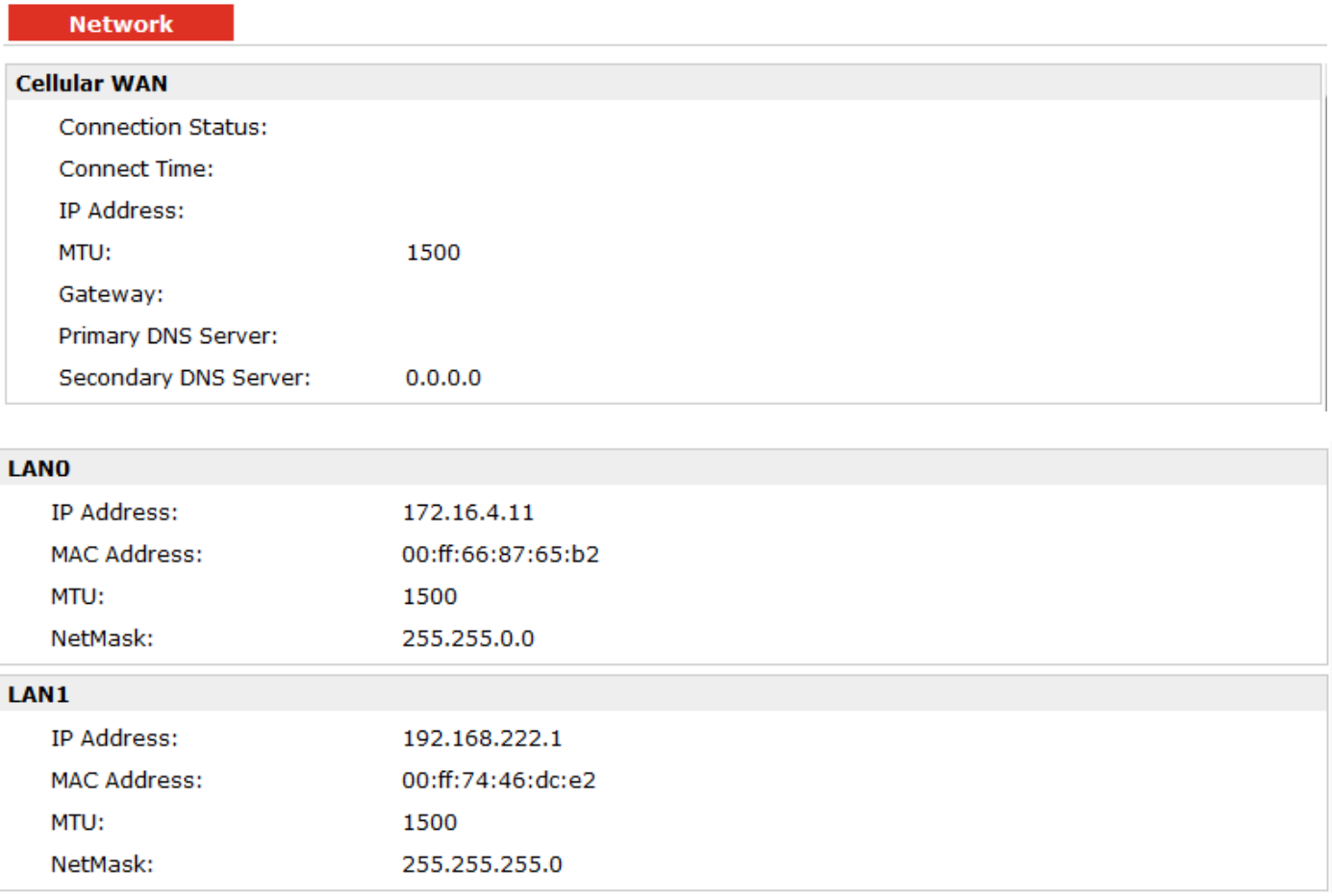


Cellular Information (Информация о сотовой сети)	
Элемент	Описание
Current SIM (текущая SIM-карта)	Отображает SIM-карту, с которой в настоящий момент работает маршрутизатор: SIM1 или SIM2
Phone No. (Номер телефона)	Отображает телефонный номер текущей SIM-карты.
SMS Service Center (Сервис-центр SMS)	Отображает текущий сервис-центр SMS.
Modem Status (Статус модема)	Отображает состояние модема. Возможны 8 состояний: 1. Неизвестно 2. Готов 3. Проверка AT 4. Требуется PIN 5. Требуется PUK 6. Низкий уровень сигнала 7. Не зарегистрирован 8. Отказ инициализации APN (имя точки доступа).
Network Status (Сетевой статус)	Отображает текущее состояние в сети. Возможны 6 состояний: 1. Не зарегистрирован, мобильное устройство в настоящий момент не производит поиск нового оператора! 2. Зарегистрирован в домашней сети. 3. Не зарегистрирован, мобильное устройство в настоящий момент производит поиск нового оператора. 4. Регистрация отклонена. 5. Зарегистрирован, роуминг. 6. Неизвестно
Signal Level (RSSI) (Уровень сигнала)	Отображает текущий уровень сигнала.
Network Operator (Оператор сети)	Отображает код страны в сети мобильной связи (MCC) и код сети мобильной связи (MNC), например, 46001. Здесь также отображается идентификатор соты и код местной зоны (Cell ID и LAC).

Cellular Information (Информация о сотовой сети)	
Network Service Type (Тип сетевых услуг)	Отображает текущий тип сетевых услуг, например, GPRS.
IMEI/ESN	Отображает номер IMEI/ESN радиомодуля.
IMSI	Отображает номер IMSI текущей SIM-карты.
USB Status (Статус USB)	Отображает текущий статус USB-хоста.

3.5 Status -> Network (Состояние-> Сеть)

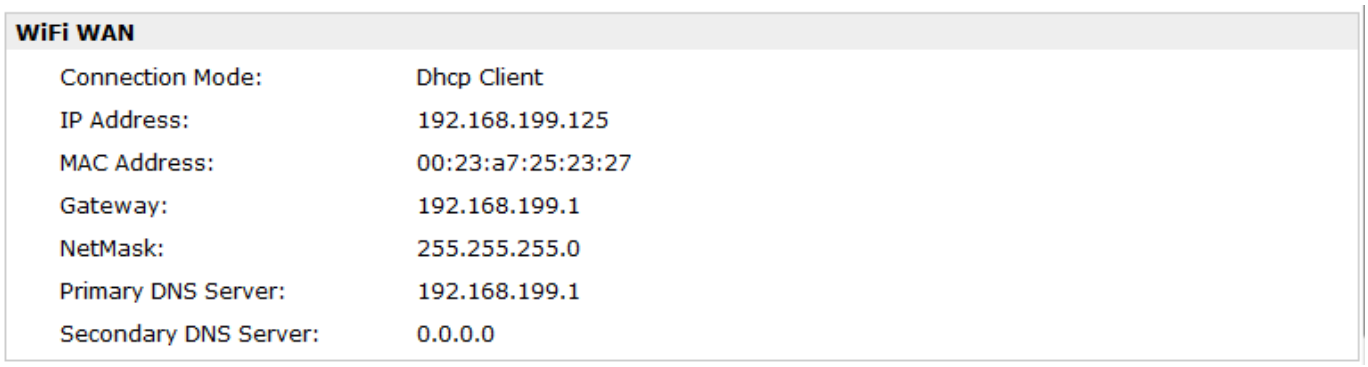
Этот раздел выводит информацию о сетевом статусе маршрутизатора: состояние сотовой WAN, ETH0, ETH11, режим точки доступа/клиента WLAN.



***Примечание**: информация о WAN ETH0 не отображается, если в Configuration -> Link Management -> WAN Link выбрано Cellular Only.*

***Примечание**: данная информация выводится, если для R3000 активирована функция WiFi и выбран режим*

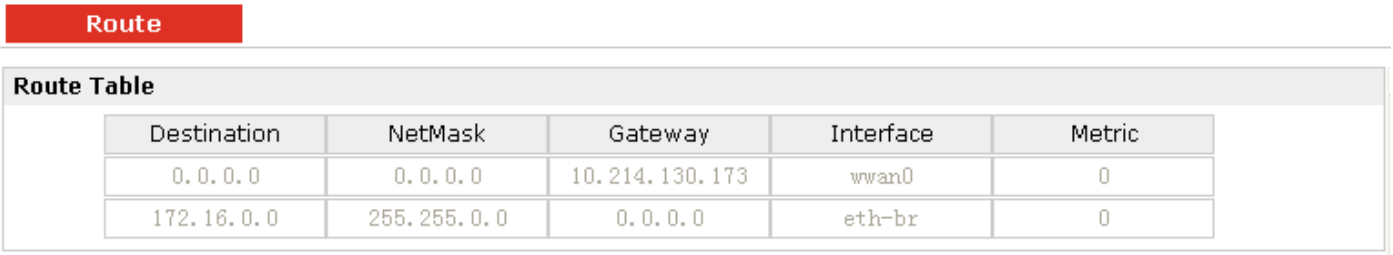
работы точка доступа.



***Примечание**: данная информация выводится, если для R3000 активирована функция WiFi и выбран режим «клиент».*

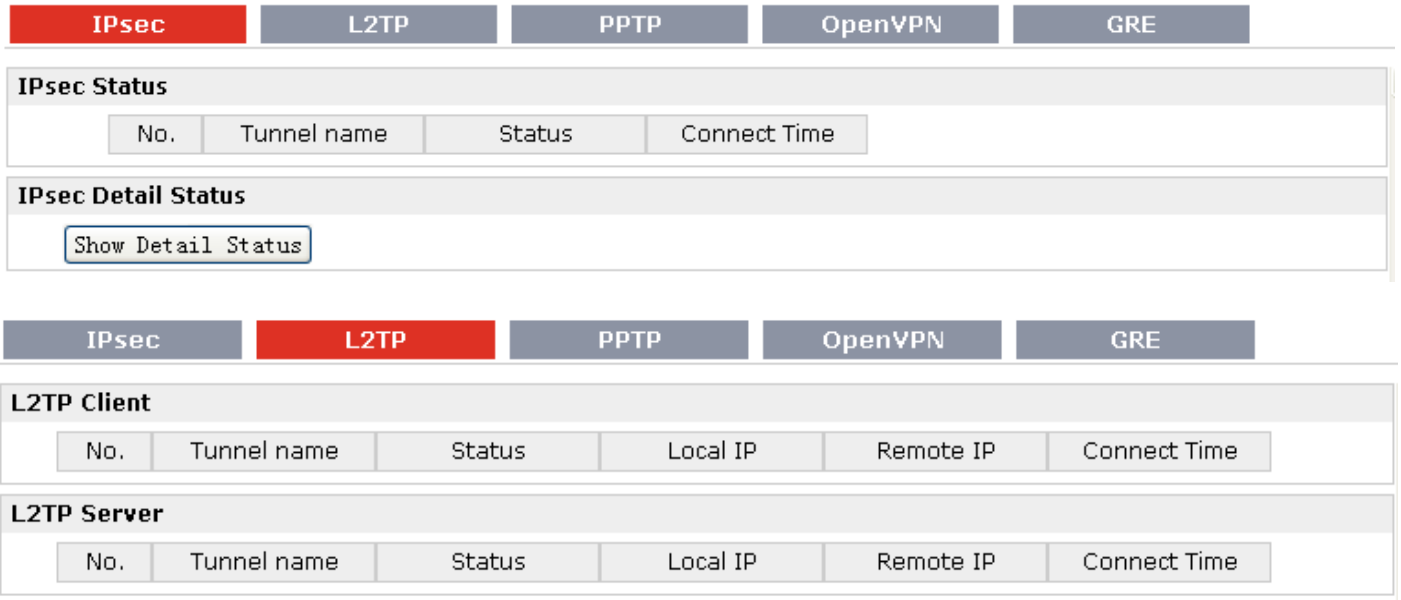
3.6 Status -> Route (Состояние-> Маршрут)

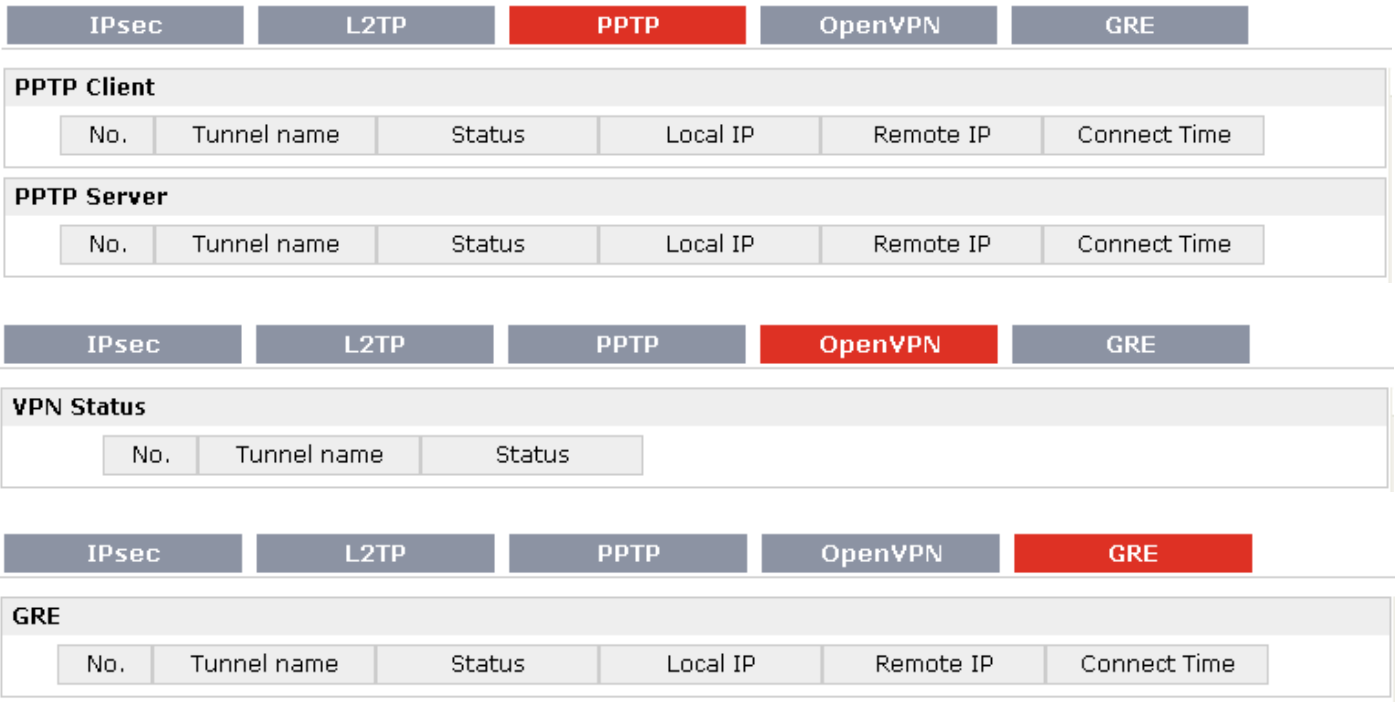
В данном разделе отображается таблица маршрутов маршрутизатора.



3.7 Status -> VPN (Состояние-> VPN)

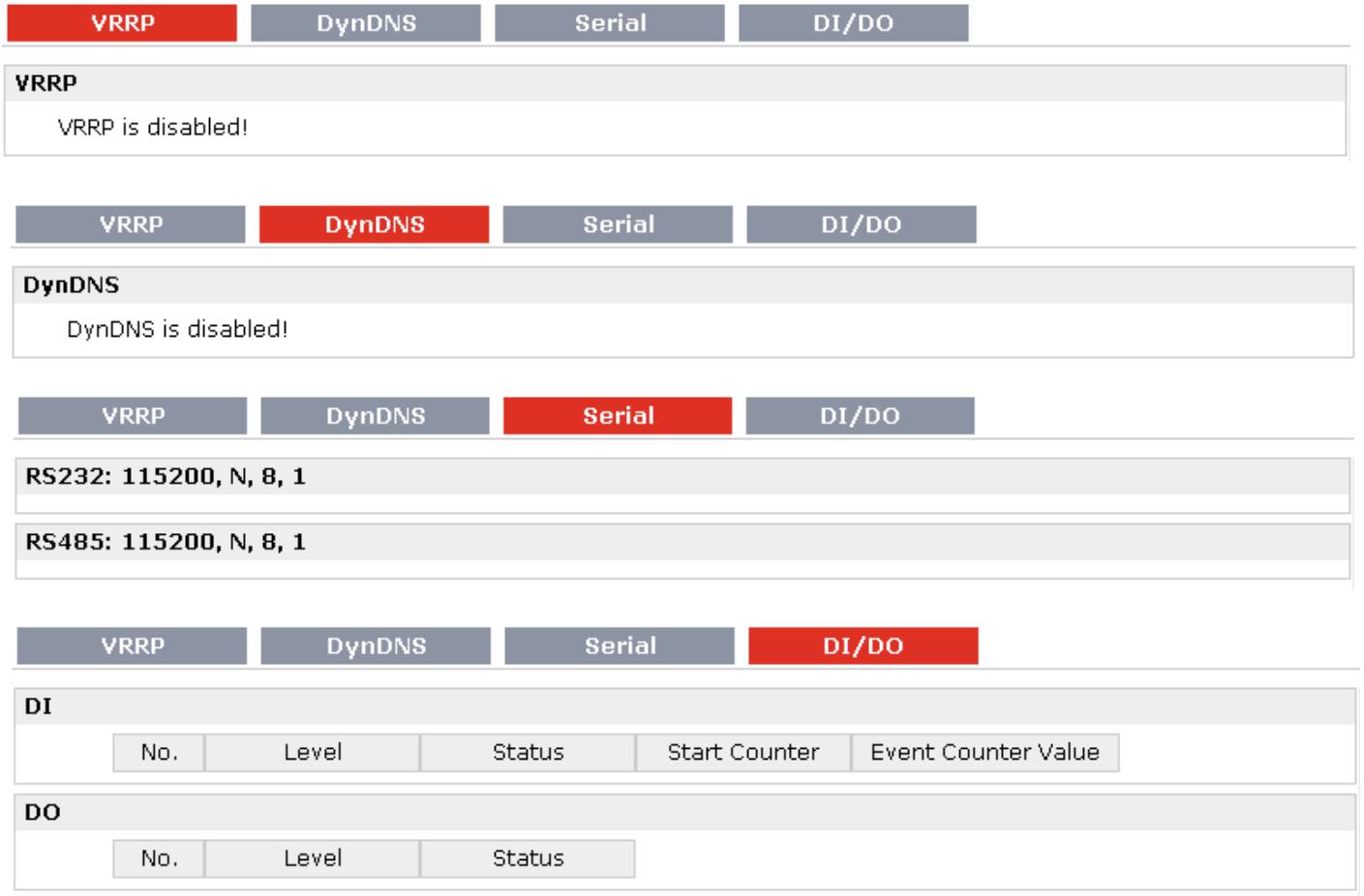
Этот раздел выводит на экран состояние VPN маршрутизатора, включая IPSec, L2TP, PPTP, OpenVPN и GRE.





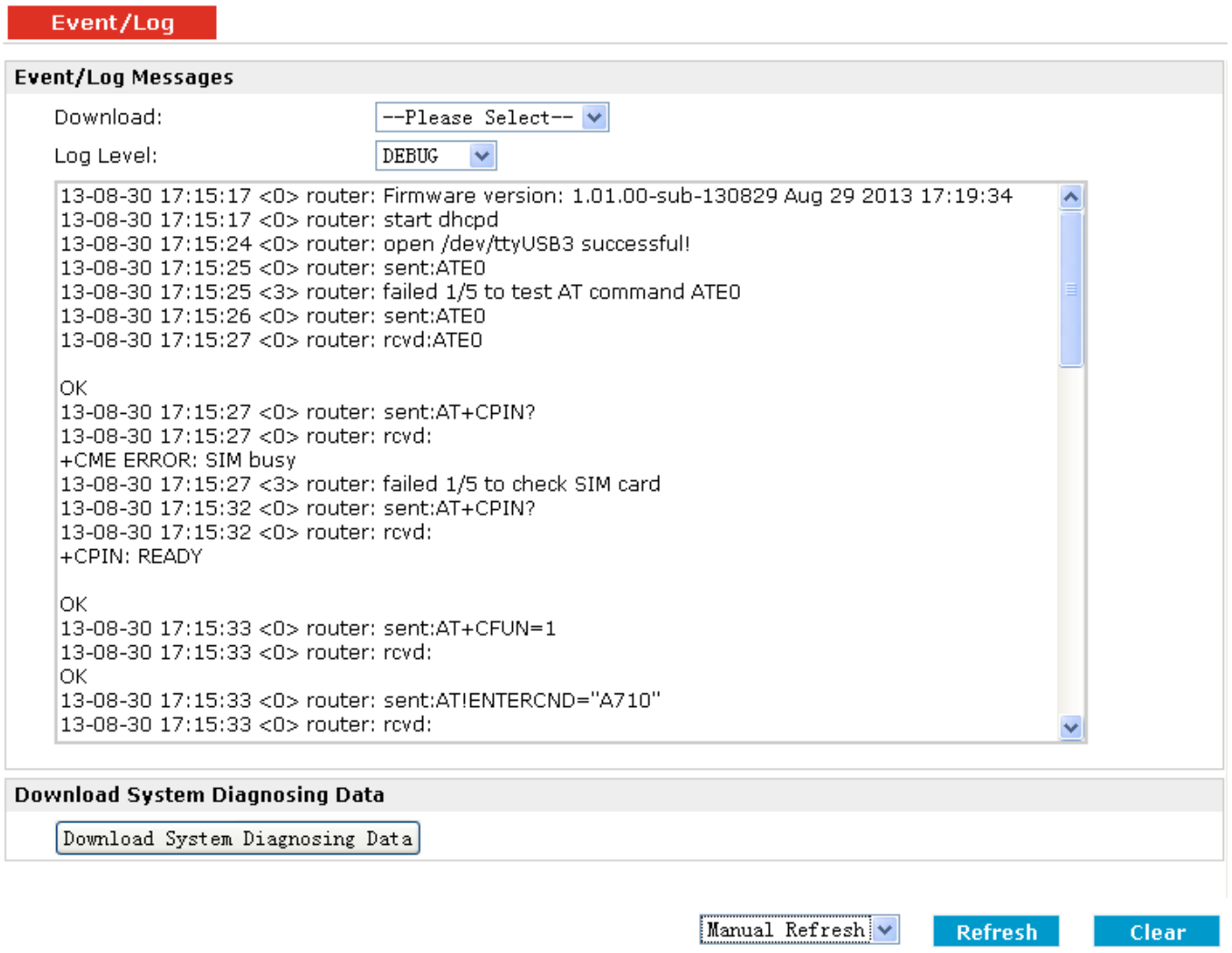
3.8 Status -> Services (Состояние-> Службы)

Этот раздел выводит на экран статус служб маршрутизатора, включая VRRP, DynDNS, последовательный интерфейс и DI/DO.



3.9 Status -> Event/Log (Состояние-> События/ Журнал)

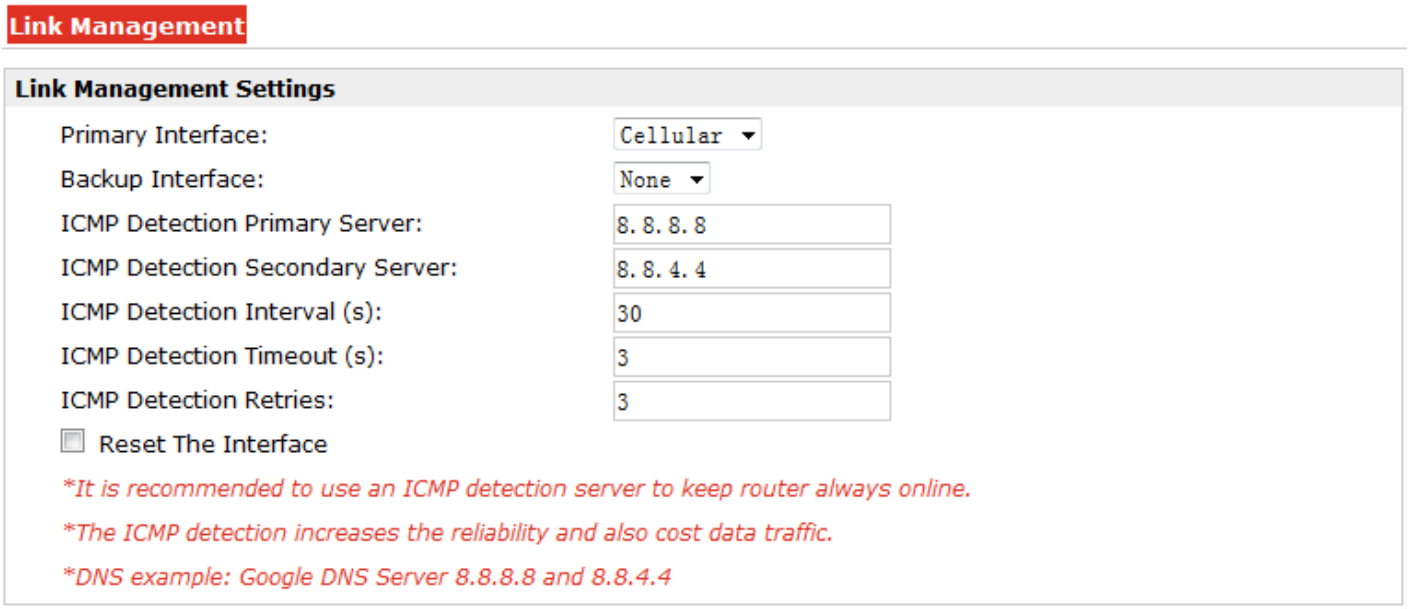
В этом разделе на экране отображается информация о событиях/журналах маршрутизатора. Сначала необходимо подать маршрутизатору команду на вывод журнала и выбрать его тип, после этого здесь можно просмотреть информацию в журнале. Также можно щелкнуть на *Download System Diagnosing Data* (загрузить диагностические данные системы), чтобы загрузить диагностические данные.



Event/Log (События/Журнал)	
Элемент	Описание
Download (Загрузить)	Выбор сообщений журнала для загрузки.
Log Level (Тип журнала)	Выбор типа журнала из выпадающего меню: DEBUG, INFO, NOTICE, WARNING, ERR, CRIT, ALERT, EMERG.
Download Sytem Diagnosing Data (Загрузить данные диагностики ситемы)	Щелкнуть *Download System Diagnosing Data* для загрузки файла диагностики.
Manual Refresh (Обновление)	Возможность обновления журнала вручную или выбора частоты для автоматического обновления информации: 5, 10, 15, 30 секунд и 1 минута.

3.10 Configuration -> Link Management (Конфигурация -> Управление соединением)

Этот раздел позволяет настроить соединение WAN и связанные параметры.



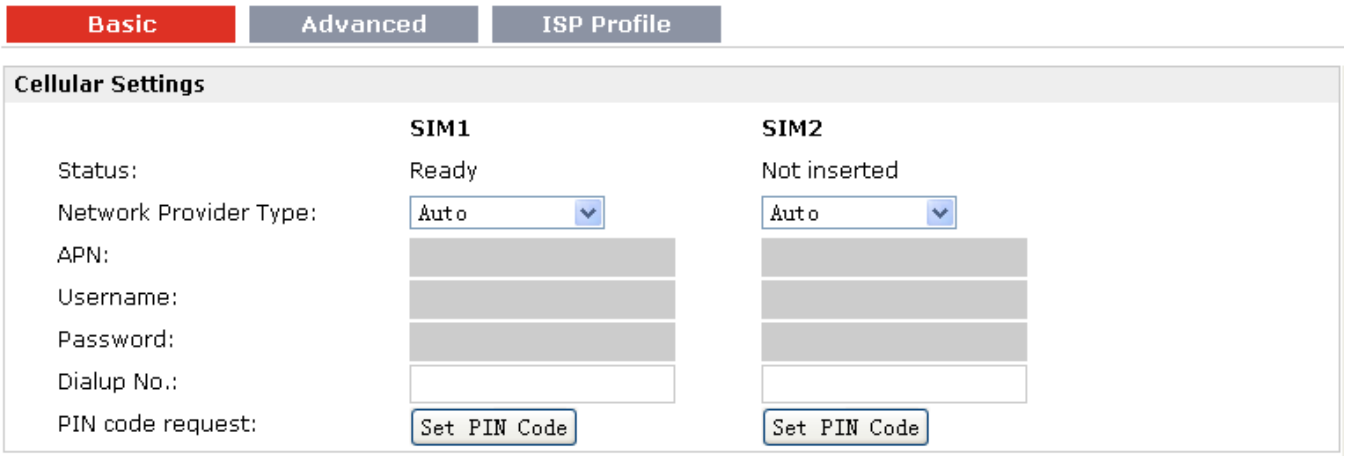
Link Management (Управление соединением)		
Элемент	Описание	По умолчанию
Primary Interface (Основной интерфейс)	Выбор из Cellular, Eth0, WiFi 1. Cellular (сотовый): использовать сотовую связь в качестве основного канала WAN. 2. Eth0: использовать Eth0 в качестве основного канала WAN. 3. WiFi: использовать WiFi в качестве основного канала WAN.	Cellular
Backup Interface (Резервный интерфейс)	Выбор из None (нет), Eth0, WiFi. 1. None: резервный интерфейс не используется. 2. Cellular (сотовый): выбор сотового подключения в качестве резервного канала WAN. 3. Eth0: Выбор Eth0 в качестве резервного канала WAN. 4. WiFi: Выбор WiFi в качестве резервного канала WAN.	None (Нет)
ICMP Detection Primary Server (Основной сервер для проверки ICMP)	Маршрутизатор будет осуществлять эхо-тестирование этого основного адреса/доменного имени для проверки активности текущего соединения.	Null
ICMP Detection Secondary Server (резервный сервер для ICMP проверки)	Маршрутизатор будет осуществлять эхо-тестирование этого резервного адреса/доменного имени для проверки активности текущего соединения.	Null
ICMP Detection Interval (интервал ICMP проверки подключения)	Настройка интервала эхо-тестирования	Null

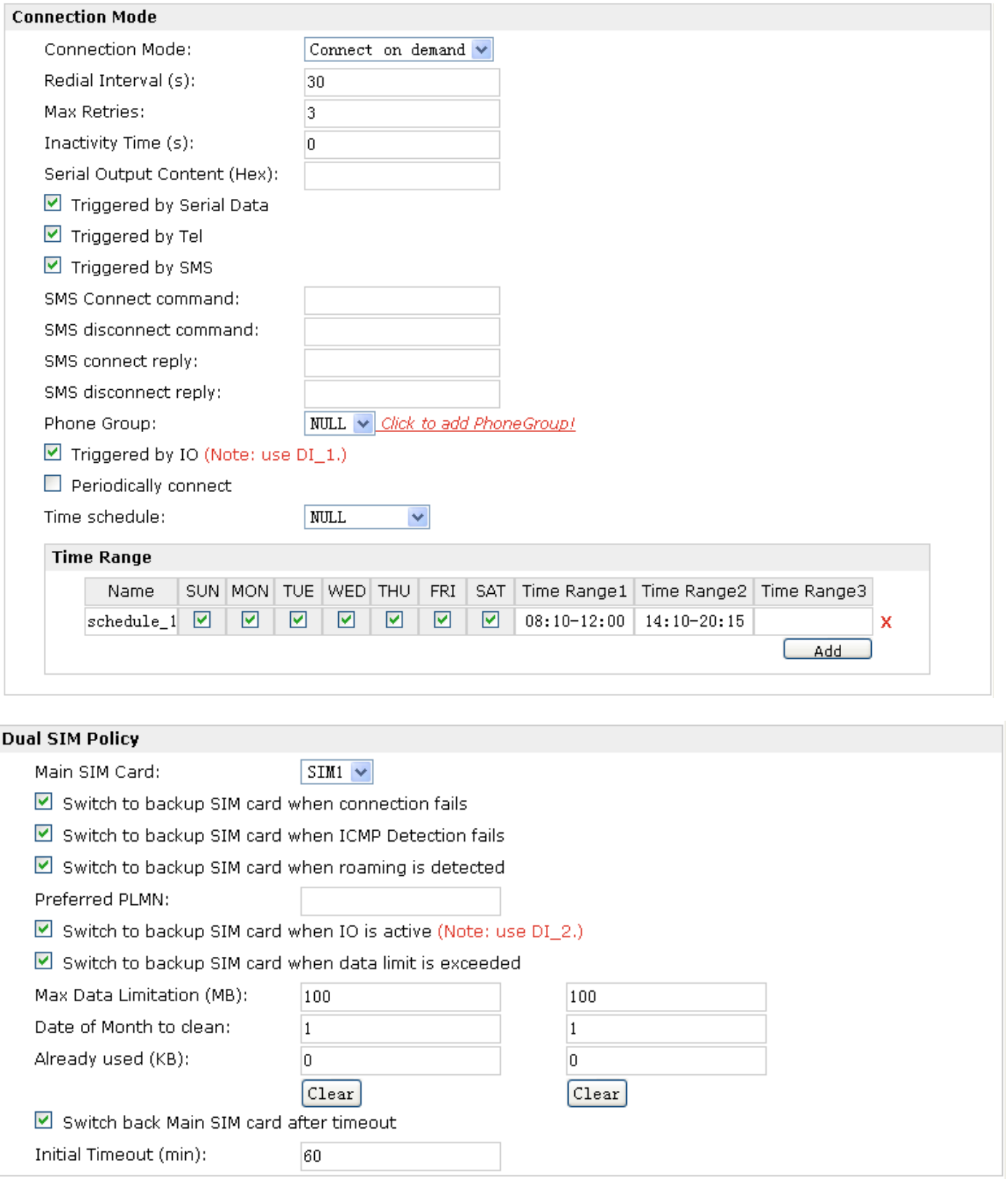
Link Management (Управление соединением)		
ICMP Detection Timeout (Время ожидания ICMP проверки подключения)	Настройка времени ожидания эхо-тестирования.	30
ICMP Detection Retries (Повтор ICMP проверки)	Если последовательная проверка соединения эхо-тестированием заданного адреса/доменного имени маршрутизатором заданное здесь число раз неудачна, соединение будет считаться потерянным.	3
Reset The Interface (Перезагрузка интерфейса)	Включить для сброса сотового/eth0 интерфейса после максимального количества повторов проверки подключения ICMP пакетами.	3

3.11 Configuration -> Cellular WAN (Конфигурация-> Сотовое подключение WAN)

Этот раздел позволяет настроить сотовое WAN подключение и связанные параметры.

Примечание: этот раздел не выводится на экран, если в *Configuration -> Link Management -> WAN Link* выбрано Eth0 Only (только Eth0)





Basic @Cellular WAN (Основные настройки @сотовое подключение WAN)		
Настройки сотового интерфейса		
Элемент	Описание	По умолчанию
Network Provider Type	Выбор из Auto, Custom или ISP name автоматически/пользовательские	Auto

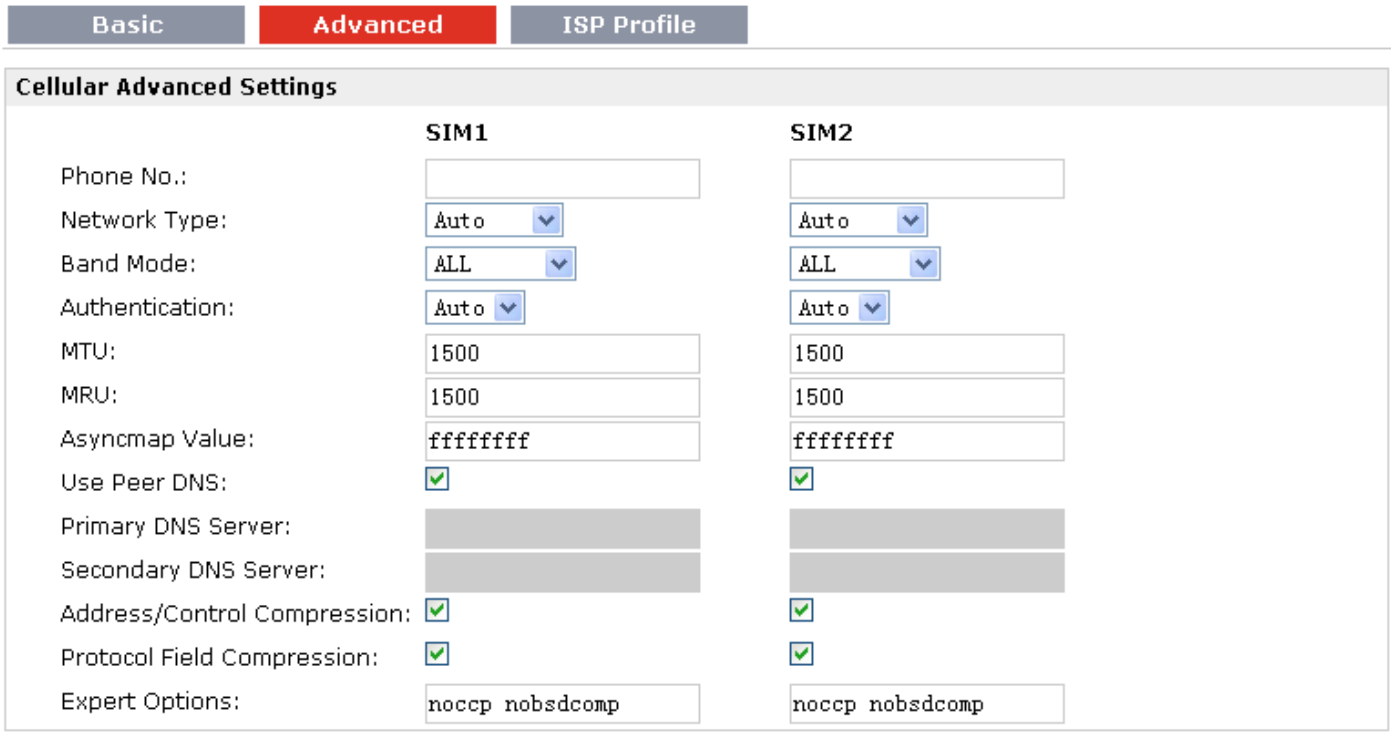
Basic @Cellular WAN (Основные настройки @сотовое подключение WAN)		
(тип поставщика доступа к сети)	настройки или имя провайдера сетевых услуг, указанного в *Configuration -> Cellular WAN -> ISP Profile*. Auto (автоматически): маршрутизатор получает информацию о провайдере с SIM-карты и автоматически устанавливает APN, имя пользователя и пароль. Эта функция доступна только для SIM-карт от известных провайдеров. Custom (пользовательские настройки): пользователю необходимо вручную задать APN, имя пользователя и пароль.	
APN (имя точки доступа)	Имя точки доступа для коммутируемого сотового соединения, предоставляемого локальным интернет провайдером.	Null
Username (Имя пользователя)	Имя пользователя для коммутируемого сотового соединения, предоставляемого локальным интернет провайдером.	Null
Password (Пароль)	Пароль для коммутируемого сотового соединения, предоставляемого локальным интернет провайдером.	Null
Dialup No. (Номер для подключения)	Номер для коммутируемого сотового соединения, предоставляемого локальным интернет провайдером.	*99***1#
PIN Type (Тип)	Выбор из None, Input, Lock, Unlock (нет/ввод/блокировать/разблокировать). None: блокирование PIN или PUK кодом для SIM-карты не предусмотрено. Input: для SIM-карты активировано блокирование PIN или PUK кодом. Потребуется ввод корректного PIN/PUK кода. Lock: выбрать, если пользователю необходимо заблокировать SIM-карту PIN или PUK кодом. Unlock: выбрать, если пользователю необходимо разблокировать SIM-карту PIN или PUK кодом. ***Примечание**: следует уточнить у местного GSM интернет провайдера требуется ли PIN для текущей SIM-карты.* *При необходимости изменить PIN-код, новый вариант следует ввести в New PIN Code и подтвердить в Confirm New PIN Code.* *Текущий статус SIM-карты можно проверить, перейдя на вкладку Status -> Event/Log и введя AT+CPIN?.*	None
Connection Mode (Режим подключения)		
Connection Mode (Режим соединения)	Выбор из Always Online и Connect On Demand (всегда в сети/по запросу). Always Online: после подачи питания PPP активируется и поддерживается автоматически. Connect On Demand: в этом варианте пользователь может выбрать один из способов инициализации Serial Data, Periodically Connect и Time Schedule (данными последовательного порта/ периодически/по расписанию). ***Примечание**: если выбрать несколько политик подключения по требованию, для активации маршрутизатора необходимо будет наличие одной из них.*	Connect On Demand
Redial Interval (Интервал повторного набора)	Время, после которого маршрутизатор автоматически осуществит повторный набор при сбое связи по TCP или UDP.	30
Max Retries	Максимальное количество повторов автоматических попыток	3

Basic @Cellular WAN (Основные настройки @сотовое подключение WAN)		
(Макс. повторов)	подключения при невозможности установить связь. После указанного количества неудачных повторных попыток маршрутизатор перезагрузит беспроводный модуль. Если и после этого установить связь невозможно, маршрутизатор попытается переключиться на другую SIM-карту. Затем он повторит заданное число попыток соединения, используя другую SIM-карту. После успешного соединения отсчет Max Retries будет установлен в 0.	
Inactivity Time (Время отсутствия активности)	Конфигурируется в случае выбора Connect On Demand (Подключение по требованию). Данное поле определяет время простоя, для авторазъединения GPRS/3G и попытки возврата к предпочтительной SIM-карте. 0 означает, что функция будет неактивна.	0
Serial Output Content (Контент последовательного выхода)	Контент, который выводится на последовательное устройство, подключенное к маршрутизатору, для сообщения ему, что маршрутизатор готов получить последовательные данные.	Null
Triggered by Serial Data (подключение по поступлению данных последовательного порта)	Отметить для автоматического подключения маршрутизатора к сотовой сети (из режима ожидания) в случае поступления данных через последовательный порт.	включено
Triggered by Tel (Инициализация по телефону)	Отметить этот флажок для автоматического подключения маршрутизатора к сотовой сети (из режима ожидания) в случае поступления голосового вызова.	отключено
Triggered by SMS (Инициализация по SMS)	Отметить этот флажок для автоматического подключения маршрутизатора к сотовой сети (из режима ожидания) в случае поступления специального SMS.	отключено
SMS Connect Command (SMS команда на подключение)	SMS данного содержания должно быть отправлено на маршрутизатор для инициализации соединения с сотовой сетью.	Null
SMS Disconnect Command (SMS команда на отключение)	SMS данного содержания должно быть отправлено на маршрутизатор для разрыва соединения с сотовой сетью.	Null
SMS Connect Reply (SMS сообщение о подключении)	После подключения маршрутизатора к сотовой сети, он автоматически отошлет SMS указанным пользователям (настраивается в Phone Group).	Null
SMS Disconnect Reply (SMS сообщение об отключении)	После отключения маршрутизатора от сотовой сети, он автоматически отошлет это SMS указанным пользователям (настраивается в Phone Group).	Null
Phone Group (Телефонная группа)	Щелкнуть для добавления в телефонную книгу группы пользователей.	Null
Triggered by IO (Инициализация по IO)	Установить эту отметку для разрешения автоматического подключения маршрутизатора к сотовой сети (из режима ожидания) в случае поступления данных DI (DI_1) alarm (оповещение на цифровом входе).	отключено
Periodically Connect	Отметить этот флажок для автоматического подключения	включено

Basic @Cellular WAN (Основные настройки @сотовое подключение WAN)		
(Периодическое подключение)	маршрутизатора к сотовой сети через интервалы, заданные в *Periodically Connect Interval.*	
Periodically Connect Interval (Интервал периодического подключения)	Интервал периодического подключения.	300
Time Schedule (По расписанию)	Выбор временного диапазона для автоматического подключения маршрутизатора к сотовой сети.	Null
Time Range (Временной диапазон)	Добавление временного диапазона для Time Schedule. Допускается выбор дней в пределах одной недели и не более трех временных диапазонов в течение одного дня.	Null
Dual SIM Policy (политика переключения двух SIM-карт)		
Main SIM Card (Основная SIM-карта)	Выбрать предпочтительную SIM-карту из SIM 1, SIM 2 или Auto (автоматически).	SIM1
Switch to backup SIM card when connection fails (Переключаться на резервную SIM-карту при разрыве соединения)	В случае сбоя подключения к сети на основной SIM-карте, маршрутизатор переключится на другую SIM-карту.	отключено
Switch to backup SIM card when roaming is detected (Переключаться на резервную SIM-карту при обнаружении роуминга)	Маршрутизатор переключится на резервную SIM-карту в случае, если предпочтительная SIM-карта окажется в роуминге.	отключено
Preferred PLMN (Предпочтительная наземная сеть мобильной связи)	Идентификатор для маршрутизатора: контроль нахождения в домашней области или в области роуминга, с последующим решением, требуется ли переключение обратно на привилегированную SIM-карту.	Null
Switch to backup SIM card when IO is active (Переключаться на резервную SIM-карту при активности IO)	Маршрутизатор переключится на другую SIM-карту если обнаружится активность входа сигнала оповещения DI (DI_2).	отключено
Switch to backup SIM card when data limit is exceeded (Переключаться на резервную SIM-карту при превышении предела данных.)	Если для SIM-карты, с которой в текущее время работает маршрутизатор, достигнуто предварительно заданное ограничение трафика передачи данных, будет выполнено переключение на другую SIM-карту.	отключено
Max Data limitation(MB)	Установить максимальный объем данных на месяц.	100

Basic @Cellular WAN (Основные настройки @сотовое подключение WAN)		
(Макс. объем данных (Мбайт)		
Date of Month to Clean (День месяца для очистки)	Установить день месяца для сброса сведений о данных на 0.	1
Already used (Использовано)	На этой вкладке отображается использованный объем трафика.	0
Switch back Main SIM card after timeout(min) (Временная задержка для переключения на основную SIM-карту (мин)	Отметить для переключения на основную SIM-карту после Initial timeout.	отключено
Initial Timeout (min) (задержка инициализации (мин)	Установка задержки инициализации.	60

***Примечание**:* Этот раздел не выводится на экран, если в *Configuration -> Link Management -> WAN Link* выбрано Eth0 Only (только Eth0).

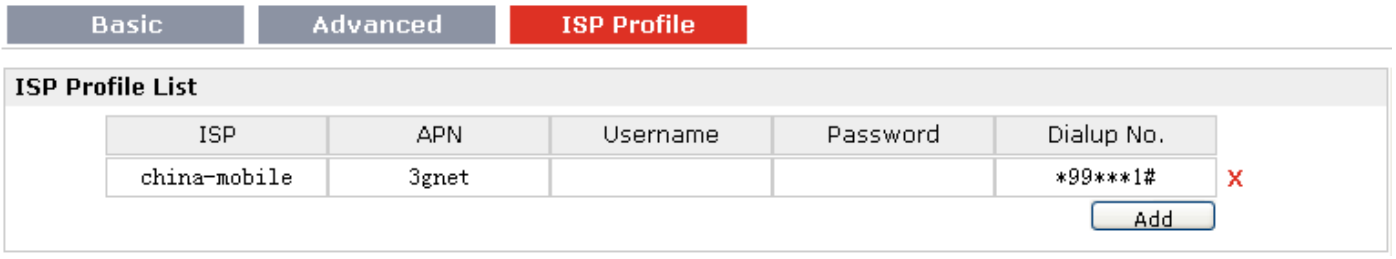


Advanced @Cellular WAN (Сотовое подключение WAN, дополнительные настройки)		
Элемент	Описание	По умолчанию
Phone No. (Номер телефона)	Уазать номер телефона SIM-карты, который будет выводиться в *Status -> System -> System -> Cellular WAN Information -> SIM Phone Number*. Чаще всего, ввод этого номера не требуется, поскольку маршрутизатор считывает его с SIM-карты автоматически.	Null
Authentication	Выбор из Auto, PAP и CHAP, в соответствии с требованиями локального	Auto

Advanced @Cellular WAN (Сотовое подключение WAN, дополнительные настройки)		
(Аутентификация)	поставщика сетевых услуг.	
MTU (Максимальный размер пакета)	Максимальный размер пакета. Это указатель максимального размера передаваемого блока данных, который возможно передать в данных условиях.	1500
MRU (Максимальный размер принимаемого блока данных)	Максимальный размер принимаемого блока данных. Это указатель максимального размера блока данных, который возможно принять в данных условиях.	1500
Asyncmap Value (Значение Asyncmap)	Одна из строк инициализации PPP. Чаще всего изменять это значение не требуется.	1
Use Peer DNS (Использовать DNS оператора)	Включить, если требуется получать адрес DNS-сервера оператора.	включено
Primary DNS Server (Основной DNS-сервер)	Ввод адреса основного DNS-сервера. Этот элемент будет недоступен, если выбрано Use Peer DNS.	Null
Secondary DNS Server (Резервный DNS-сервер)	Ввод адреса резервного DNS-сервера. Этот элемент будет недоступен, если выбрано Use Peer DNS.	Null
Address/Control Compression (Сжатие адресной или управляющей информации)	Используется для инициализации PPP. В большинстве случаев необходимо выбирать enable (включено), как и установлено по умолчанию.	включено
Protocol Field Compression (Сжатие поля протокола)	Используется для инициализации PPP. В большинстве случаев необходимо выбирать enable (включено), как и установлено по умолчанию.	включено
Expert Options (Профессиональные настройки)	В это поле можно ввести некоторые дополнительные строки инициализации PPP. Каждая строка может быть отделена пробелом.	noccp

ISP Profile (Профиль поставщика сетевых услуг)

Этот раздел позволяет задать разные профили поставщиков сетевых услуг, которые будут отображаться в списке выбора *Configuration -> Cellular WAN -> Network Provider Type*.

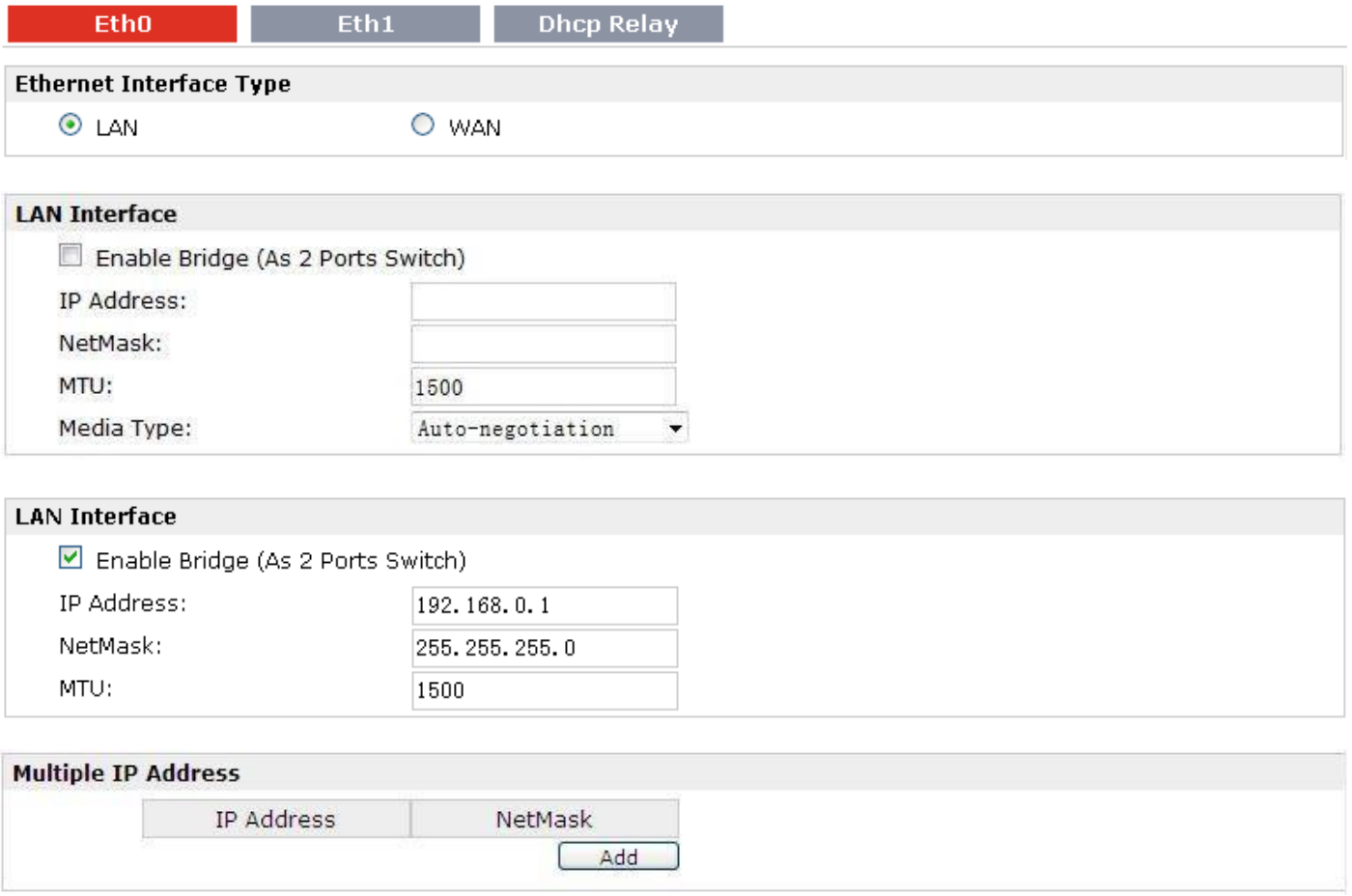


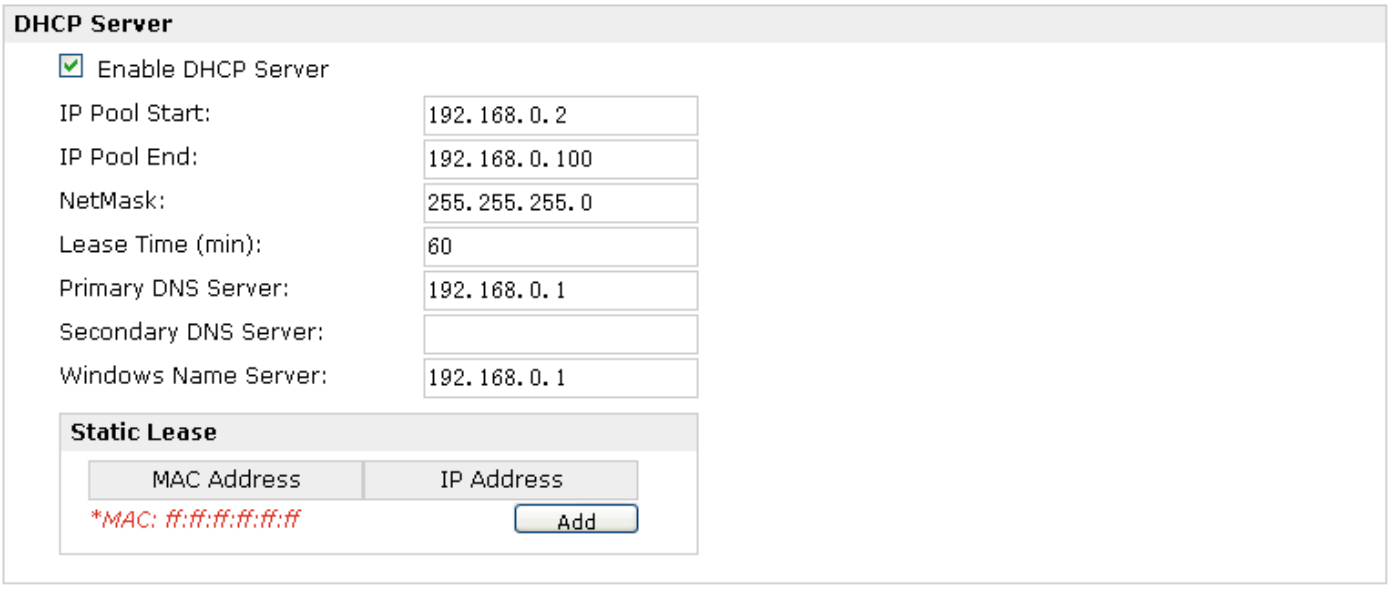
ISP Profile @Cellular WAN (Профиль поставщика услуг сотовой сети)		
Элемент	Описание	По умолчанию
ISP (Поставщик сетевых услуг)	Ввести имя провайдера, которое будет отображаться в списке выбора *Configuration -> Cellular WAN -> Network Provider Type*.	Null

APN, Username, Password, Dialup No (Имя точки доступа/ имя пользователя/пароль/ телефонный номер).	Все эти указанные параметры предоставляются поставщиком сетевых услуг.	Null

3.12 Configuration -> Ethernet (Конфигурация-> Ethernet)

Этот раздел позволяет настроить сетевые параметры Eth0 для глобальной и локальной сети.

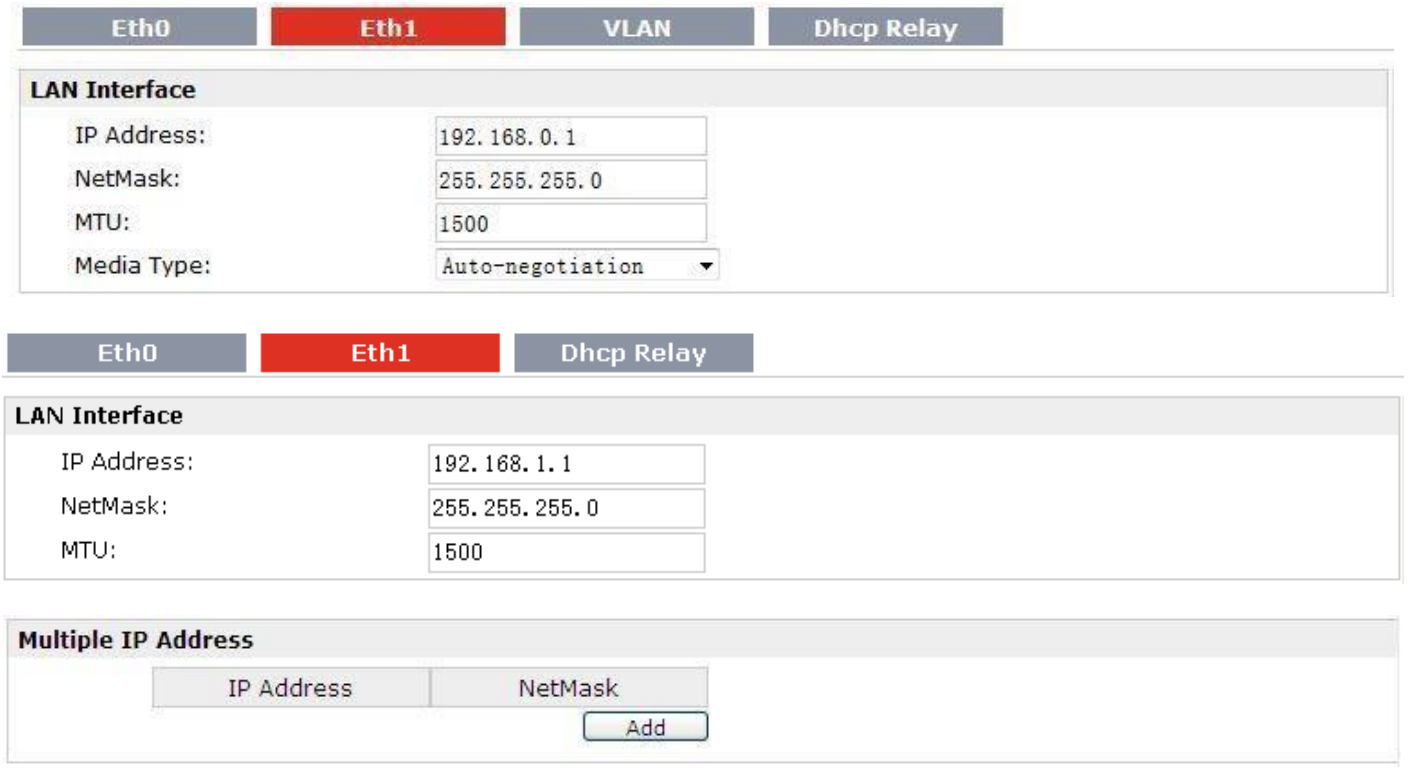


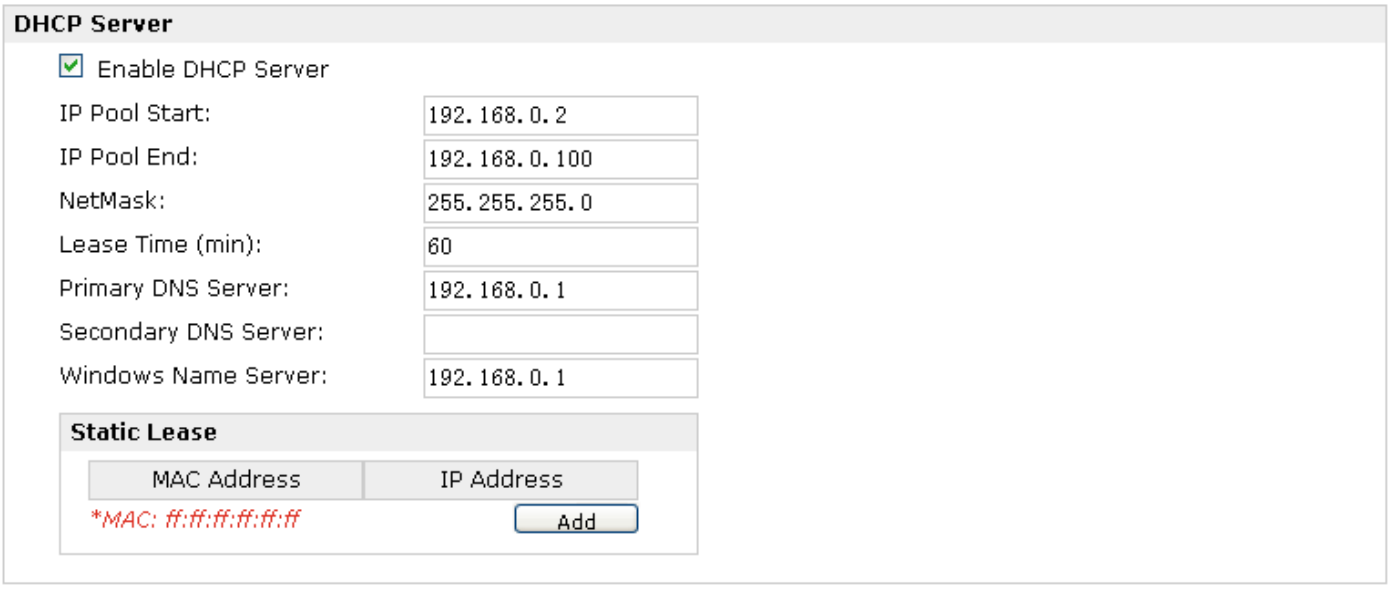


Eth0@Ethernet		
Элемент	Описание	По умолчанию
Ethernet Interface Type (Тип Ethernet интерфейса)	Eth0 может работать в двух различных режимах: LAN (локальная) и WAN (глобальная) сеть.	LAN
Enable Bridge @ LAN Interface (Режим моста для LAN интерфейса)	Включить, чтобы Eth0 работал в режиме моста с Eth1. В таком режиме Eth0 и Eth1 будут иметь единый IP-адрес.	включено
IP Address, Netmask, MTU, Media Type@ LAN Interface (IP адрес/маска подсети/максимальный размер пакета/скорость и режим)	Задать IP-адрес, маску подсети, MTU и скорость/режим (авто, 10 Мбит/с Half Duplex, 100 Мбит/с Full Duplex, 100 Мбит/с Half Duplex, 100 Мбит/с Full Duplex) для Eth0. Настройка этих параметров недоступна, если включен режим моста.	Null
Multiple IP Address @ LAN Interface (Разные IP-адреса для LAN интерфейса)	Назначить разные IP-адреса для Eth0.	Null
Enable DHCP Server @ DHCP Server (Включить DHCP-сервер)	Включить, чтобы маршрутизатор предоставлял аренду IP-адресов клиентам DHCP, подключающимся к Eth0.	отключено
IP Pool Start, IP Pool End @ DHCP Server (Начало и конец пула IP адресов DHCP-сервера)	Указать начало (IP Pool Start), и конец (IP Pool End) пула IP-адресов для выдачи клиентам DHCP.	Null
Netmask @ DHCP Server (Маска подсети DHCP-сервера)	Указать маску подсети, которую клиенты DHCP будут получать с DHCP-сервера.	Null
Lease Time @ DHCP Server (min) (Время аренды для DHCP-сервера, мин)	Указать время аренды клиентом IP-адреса, выданного DHCP-сервером.	60

Eth0@Ethernet		
Primary/Secondary DNS Server @ DHCP Server (основной/резервный DNS-серверы DHCP-сервера)	Указать основной/резервный DNS-сервер, который будут получать клиенты от DHCP-сервера.	Null
Windows Name Server @ DHCP Сервер службы имен Windows для DHCP-сервера)	Указать сервер службы имен Windows, который клиенты будут получать от DHCP-сервера).	Null
Static Lease @ DHCP Server (Раздавать клиентам с DHCP-сервера постоянные IP адреса)	Указать, чтобы выдавать постоянные IP адреса, в соответствии с MAC адресами подключаемого оборудования.	Null

Этот раздел позволяет настроить сетевые параметры Eth1 для глобальной и локальной сети.





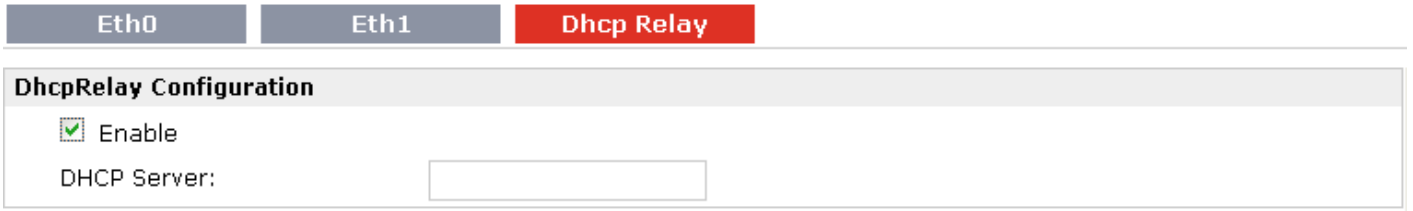
Eth1@Ethernet		
Элемент	Описание	По умолчанию
IP Address, Netmask, MTU, Media Type @ LAN Interface (IP адрес/маска подсети/ макс. размер пакета/способ подключения LAN интерфейса)	Указать IP-адрес, маску подсети, MTU и способ подключения Eth1. Настройка этих параметров будет недоступна, если включен режим мост.	Null
Multiple IP Address @ LAN Interface (Разные IP-адреса для интерфейса LAN)	Назначить разные IP-адреса для Eth1.	Null
Enable DHCP Server @ DHCP Server (Включить DHCP-сервер)	Включить, чтобы маршрутизатор мог предоставлять аренду IP-адресов клиентам DHCP, подключающимся к Eth1.	включено
IP Pool Start, IP Pool End @ DHCP Server (Начало и конец пула IP адресов DHCP-сервера)	Указать начало (IP Pool Start), и конец (IP Pool End) пула IP-адресов для выдачи клиентам DHCP.	192.168.0.2/ 192.168.0.100
Netmask @ DHCP Server (Маска подсети DHCP-сервера)	Уазать маску подсети, которую клиенты DHCP будут получать с DHCP-сервера.	255.255.255.0
Lease Time @ DHCP Server(min) (Время аренды для DHCP-сервера, мин.)	Указать время аренды клиентом IP-адреса, выданного DHCP-сервером.	60
Primary/Secondary DNS Server @ DHCP Server (основной/резервный DNS-серверы DHCP-сервера)	Указать основной/резервный DNS-сервер, который будут получать клиенты от DHCP-сервера.	192.168.0.1/ 0.0.0.0
Windows Name Server @ DHCP Сервер службы имен Windows для DHCP-сервера)	Указать сервер службы имен Windows, который клиенты будут получать от DHCP-сервера.	192.168.0.1
Static Lease @ DHCP Server (Раздавать клиентам с DHCP-сервера постоянные IP адреса)	Указать, чтобы выдавать постоянные IP адреса, в соответствии с MAC адресами подключаемого оборудования.	Null

Маршрутизатор может осуществлять ретрансляцию DHCP, что обеспечивает ретрансляцию туннеля в случае, когда клиент и DHCP-сервер не находятся в единой подсети. Этот раздел позволяет сконфигурировать настройки ретрансляции DHCP.

VLAN

Возможно создание до 2х тегированных виртуальных LAN: eth0 и eth1. Для включения соответсвующей VLAN следует отметить «Enable Eth0/1 VLAN», задать идентификатор VLAN ID (по умолчанию 0), IP-адрес и маску подсети.

DHCP

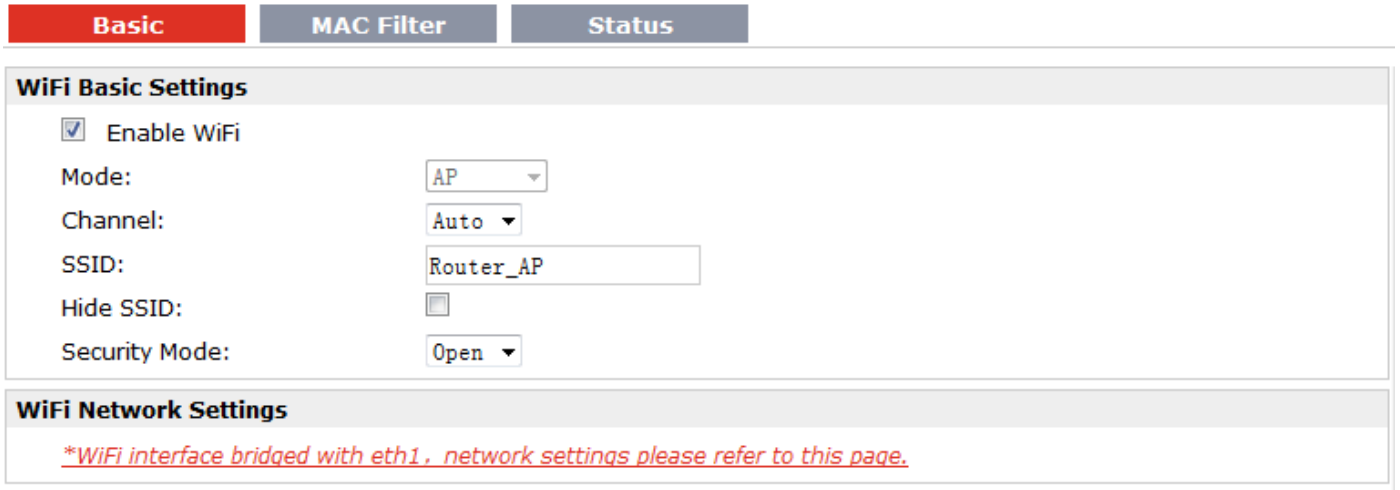


DHCP Relay @ Ethernet		
Элемент	Описание	По умолчанию
Enable Eth0/1 (Разрешить Eth0/1) VLAN@Eth0/1 VLAN Settings (Настрйки VLAN)	Включить, чтобы разрешить маршрутизатору инкапсулировать и «разворачивать» VLAN-тег	Disable (отключено)
VLAN ID@Eth0/1 VLAN Settings (Настройки VLAN)	Задать Tag ID (метку тега) VLAN	10/11
IP Address, NetMask @Eth0/1 VLAN Settings (Настройки IP адреса, маски подсети для Eth0/1 в VLAN)	Указать IP-адрес, маску подсети интерфейса Eth0/1 VLAN	IP Address, маска подсети Eth0/1

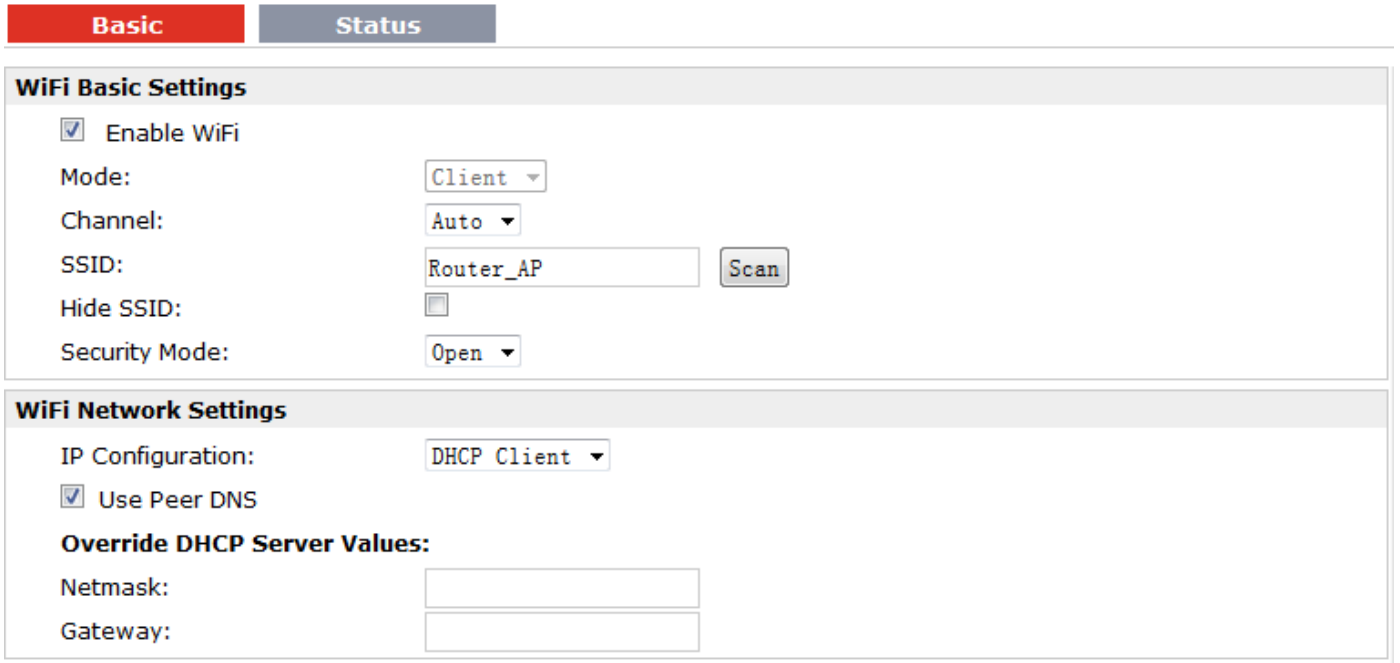
Примечание: IP-адрес и маска подсети будут скрыты, если пользователь соединит мостом два порта Ethernet.

3.13 Configuration -> WiFi (Конфигурация-> WiFi)

Этот раздел позволяет настроить Wi-Fi параметры.



Примечание: для R3000 активирован WiFi и работа в режиме AP (точки доступа).

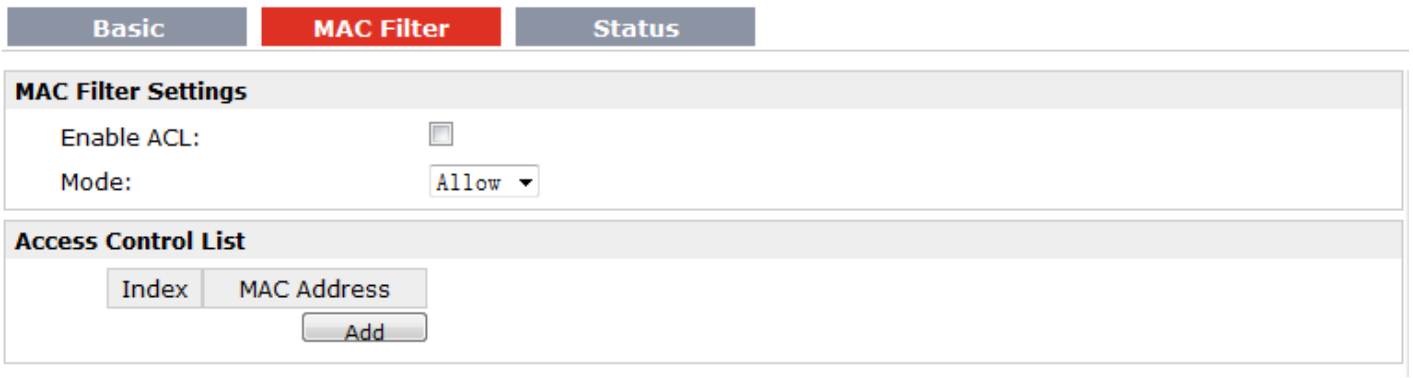


Примечание: для R3000 активирован WiFi и работа в клиентском режиме.

Basic @ WiFi (Основные настройки WiFi)		
Элемент	Описание	По умолчанию
Enable WiFi (Активировать WiFi)	Щелкнуть, чтобы активировать WiFi.	Null

Basic @ WiFi (Основные настройки WiFi)		
Mode (Режим)	Этот элемент отображает AP или Client (точка доступа/ клиент) и не может быть изменен. AP: В беспроводной локальной сети (WLAN) точка доступа является станцией, которая передает и получает данные. Если требуется работа R3000 в режиме точки доступа, необходимо перейти на вкладку Configuration -> Link Management -> Primary Interface и выбрать Cellular или Eth0 для подключения WAN. Client: Когда R3000 работает в клиентском режиме, он может использоваться в качестве сетевого адаптера Ethernet—беспроводная сеть (или LAN—WLAN). Например, ноутбук, оборудованный Ethernet-адаптером, но не имеющий беспроводного модуля, может быть соединен с маршрутизатором Ethernet кабелем, чтобы обеспечить беспроводную связь для другой точки доступа. Если требуется работа R3000 в клиентском режиме, необходимо перейти на вкладку *Configuration -> Link Management -> Primary Interface* и выбрать WiFi для подключения WAN.	Null
Channel (Канал)	Выбрать частотный канал из Auto, 1, 2 … … 13. Auto (автоматически): R3000 сканирует все частоты, пока не найдет доступную точку доступа или беспроводную сеть, к которой возможно подключение. 1~13: R3000 будет работать с указанным каналом.	Auto
SSID	SSID (идентификатор) является сетевым именем WLAN. Для возможности связи SSID клиента и SSID AP должны быть идентичны друг другу. Если R3000 работает в клиентском режиме, необходимо задать SSID точки доступа, к которой подключается R3000. Количество символов для ввода от 1 до 31.	Router_AP
Hide SSID (Скрыть SSID)	Если R3000 работает в режиме AP, и выбран данный переключатель, широковещательная передача SSID не производится. Другие беспроводные устройства не смогут автоматически обнаружить эту точку доступа. Чтобы беспроводные устройства смогли подключиться к такой точке доступа, пользователю необходимо ввести SSID вручную. Если при работе R3000 в клиентском режиме требуется подключение к точке доступа со скрытым SSID, его необходимо ввести вручную на вкладке SSID и щелкнуть на Hide SSID.	Disable (отключено)
Security mode (Тип шифрования)	Выбор из Open, WPA и WPA2. Open (без шифрования): без аутентификации. Из соображений безопасности недопустимо устанавливать режим Open System, поскольку при этом не выполняется аутентификация и шифрование данных. WPA/WPA2: Персональные версии WPA/WPA2 (защищенный доступ WiFi), также известны как WPA/WPA-PSK (предварительный ключ), обеспечивают простой способ шифрования беспроводных соединений с высокой степенью секретности. WPA2 обеспечивает	Open (открытый)

Basic @ WiFi (Основные настройки WiFi)		
	большую защиту, чем WPA. ***Примечание**: R3000 поддерживает персональную версию WPA/WPA2, не корпоративную.*	
Encryption (Шифрование)	Выбор из TKIP и CCMP (AES). TKIP: шифрование с использованием временных ключей (TKIP) используется в беспроводных каналах. Шифрование TKIP может использоваться с аутентификацией WPA-PSK и WPA с 802.1x. CCMP (AES): CCMP (AES) шифрование используется для беспроводного канала. CCMP может использоваться WPA-PSK и WPA с аутентификацией 802.1x. ***Примечание**: CCMP (AES) является более надежным алгоритмом шифрования, чем TKIP.*	CCMP (AES)
Passphrase (парольная фраза)	Если R3000 работает в режиме точки доступа, следует ввести первичный ключ, на основе которого будут генерироваться ключи шифрования. Пароль используется в качестве основы для методов шифрования (или типов шифров) для WLAN соединения. Парольные фразы должны быть сложными и максимально длинными. Из соображений безопасности этот пароль должен быть известен только тем пользователям, которым это необходимо, и его следует регулярно сменять. Если R3000 работает в режиме клиента, следует ввести пароль точки доступа, к которой требется подключение. Ввод от 8 до 63 символов.	Null
Key Renewal Interval(s) (интервал (ы) обновления ключа)	Ввести временной период группового обновления ключа. ***Примечание**: только для режима AP.*	3600
WiFi Network Settings (настройки WiFi сети)	При работе R3000 в режиме AP, щелкнуть для перехода на страницу Eth1, проверки сетевых настроек и интерфейса WiFi с текущим подключением мостом к eth1. Когда R3000 работает в клиентском режиме, этот элемент используется для конфигурирования IP точки доступа.	Null



***Примечание**: доступно, когда для R3000 активирована функция WiFi и режим работы AP.*

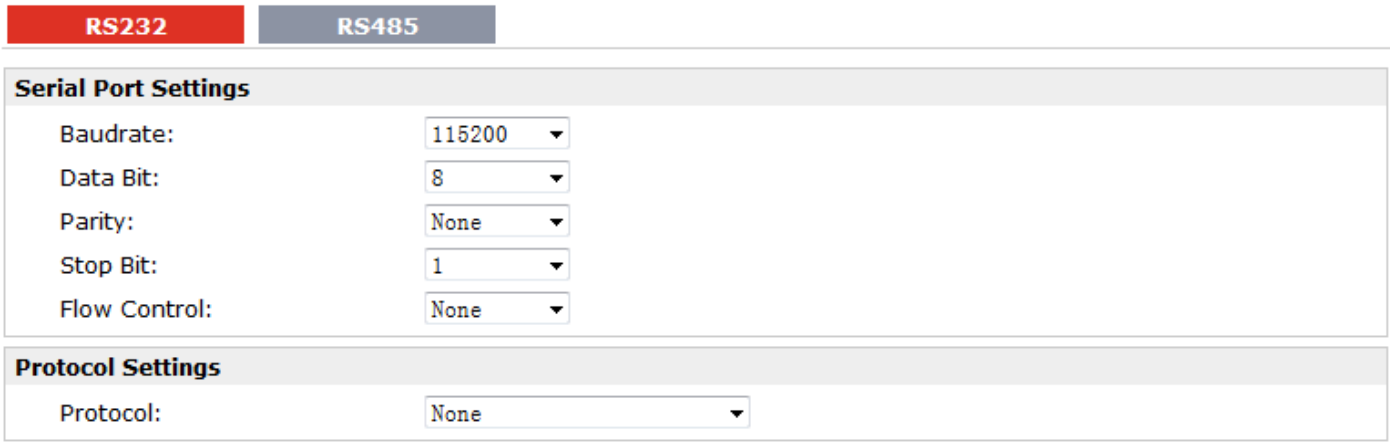
Mac Filter @ WiFi (Only for AP mode) (Фильтрация Mac WiFi — только для режима AP)		
Enable ACL (Включить список)	Щелкнуть для включения ACL (Access Control List - список доступа).	Disable (отключено)
Mode (Режим)	Выбор из: Allow и Deny (разрешить/запретить). Allow: разрешены только пакеты, соответствующие объектам списка доступа. Deny: все пакеты, соответствующие объектам списка доступа, будут отклоняться. ***Примечание**: R3000 может разрешать или отклонять только те устройства, которые одновременно включены в Access Control List.*	Allow (разрешено)
Access Control List (список доступа)	Щелкнуть на *Add* для добавления MAC-адресов.	Null

Status @ WiFi (Состояние WiFi)		
BSSID (физический адрес точки доступа)	Отображается MAC-адрес WiFi интерфейса R3000 или точки доступа, к которой он подключен.	Null
SSID (идентификатор)	Отображается SSID (имя) WiFi интерфейса R3000 или точки доступа, к которой он подключен.	Null
Mode (Режим)	Отображается текущий режим R3000: AP (точка доступа) или клиент.	Null
Key Management (управление ключами)	Отображается текущий режим безопасности R3000 или точки доступа, к которой он подключен.	Null
Cipher Pairwise (Двухключевой шифр) Cipher Group (шифруемая группа знаков)	Отображается текущий алгоритм шифрования, используемый R3000 или точкой доступа, к которой он подключен.	Null
WPA State (статус WPA)	Отображается текущее состояние WPA. Возможны 5 основных состояний: Disconnected, Scanning, Initializing, Associated, 4way_handshark, Completed. Disconnected (отключен): нет соединения ни с какой точкой доступа,	Null

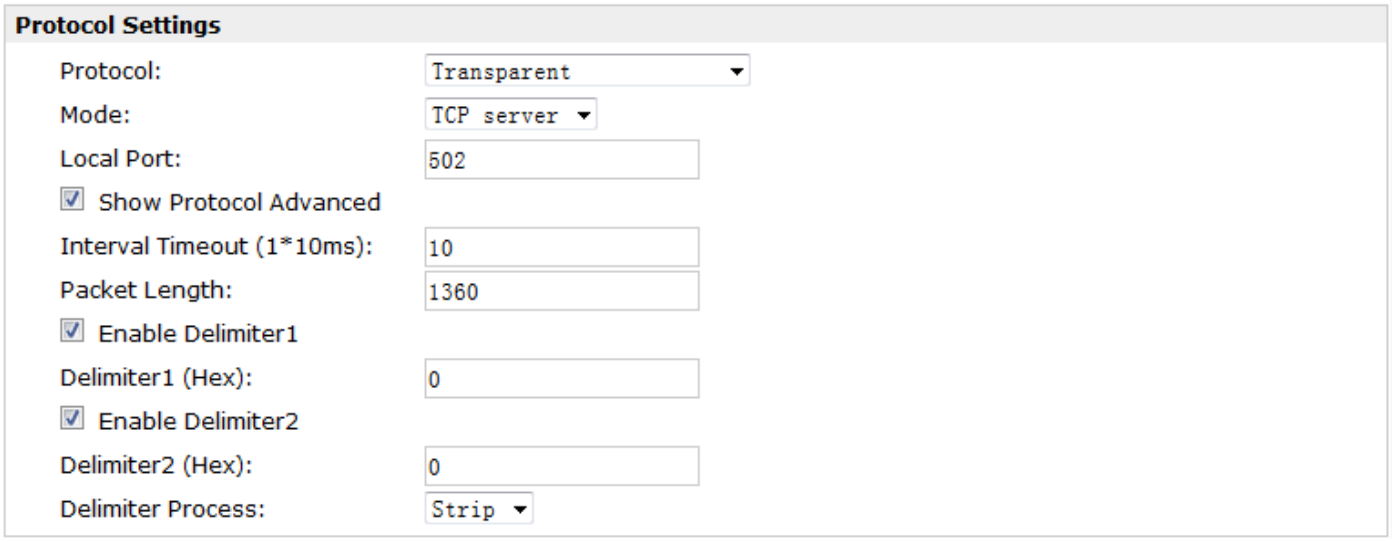
Status @ WiFi (Состояние WiFi)		
	возможная причина в неполной инициализации беспроводного устройства или оно расположено вне зоны действия. Беспроводной интерфейс может быть отключен потому, что включен Ethernet интерфейс. Scanning (сканирование): Поиск беспроводной сети (точки доступа) для подключения. Initializing (инициализация): R3000 инициализирует беспроводную среду. Associated (подключен): состояние, когда драйвер сообщает об успешном установлении связи с AP, но ожидается аутентификация. 4way_handshark: состояние, когда запущено четырехстороннее квитирование WPA/WPA2. Это состояние возникает, при несовпадении пароля. Completed (завершено): беспроводное соединение R3000 с другими беспроводными устройствами установлено.	
Address (адрес)	Отображается MAC-адрес WiFi интерфейса R3000.	Null
Associated Clients @ AP mode (Подключенные клиенты в режиме AP)	Отображается BSSID и IP-адреса подключенных беспроводных устройств-клиентов.	Null
Scan Results @ Client mode (Результат сканирования в клиентском режиме)	Отображаются результаты сканирования доступных беспроводных сетей (точек доступа), такие как: SSID, канал, уровень сигнала, флаги (режим безопасности и флаги алгоритма шифрования точки доступа).	Null

3.14 Configuration -> Serial (Конфигурация-> Последовательный интерфейс)

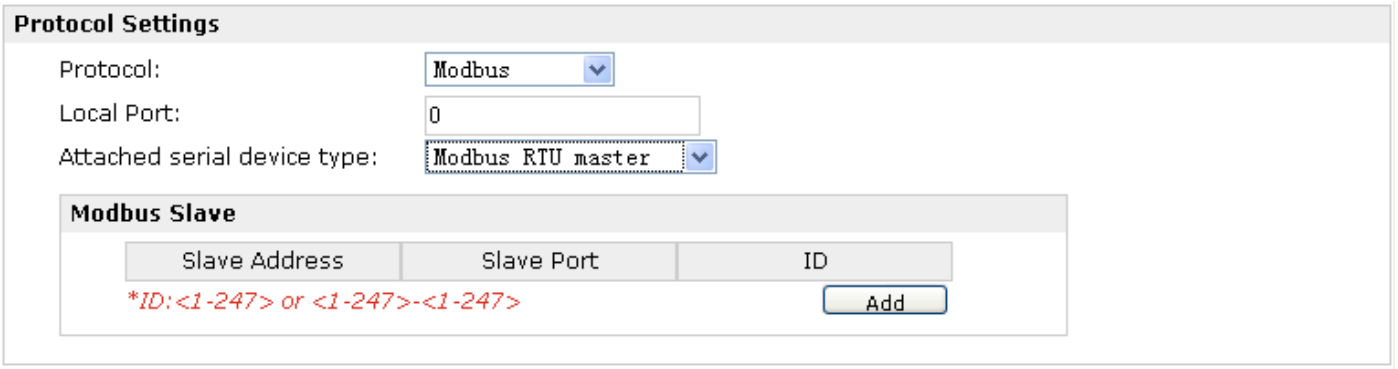
Этот раздел позволяет настроить параметры последовательного интерфейса (RS-232/RS-485).



- Если выбран протокол Transparent:



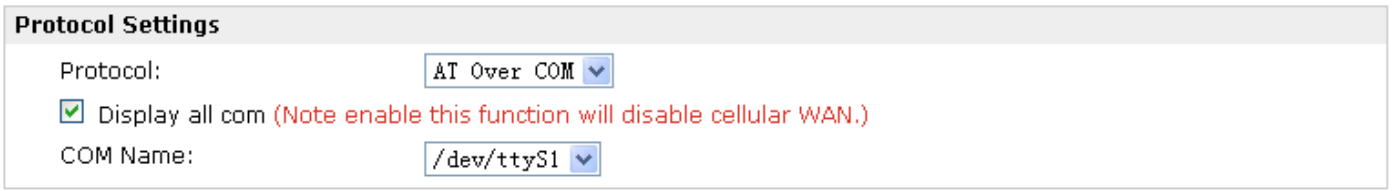
- Если выбран протокол Modbus:



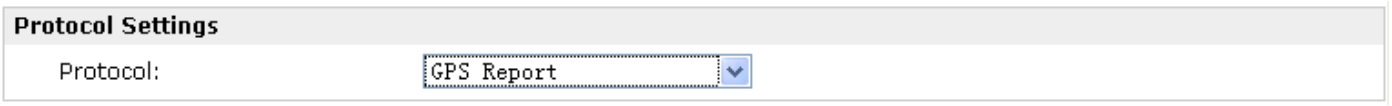
- Если выбран протокол Transparent Over Rlink:

- Если выбран протокол Modbus Over Rlink:

- Если выбран протокол AT Over COM:



- Если выбран протокол GPS Report:

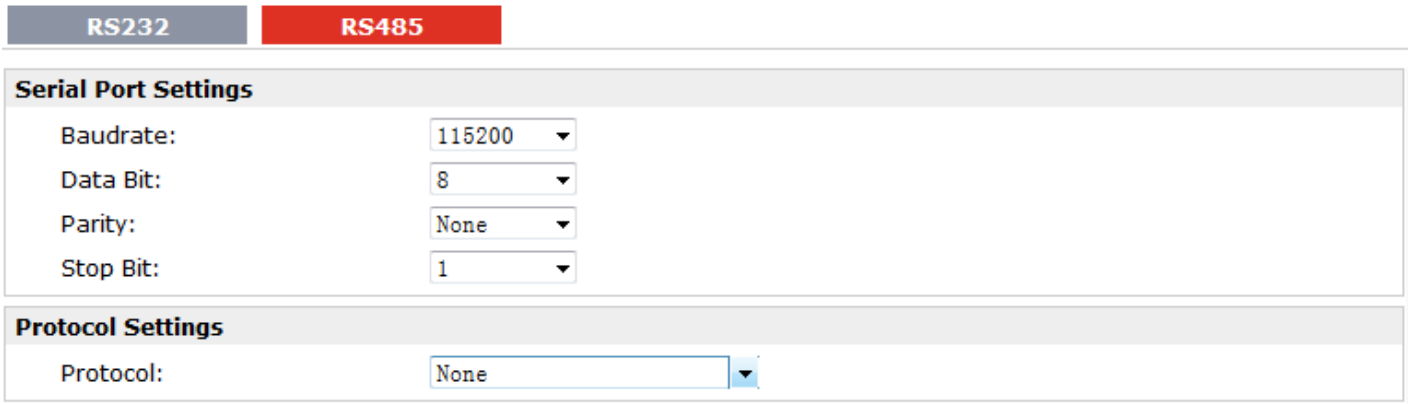


RS232 @ Serial (последовательный интерфейс RS232)		
Элемент	Описание	По умолчанию
Baud-rate (Скорость, в бодах)	Выбор из 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 и 230400.	115200
Data bit (Бит данных)	Выбор из 7 и 8.	8
Parity (Четность)	Выбор из None, Odd и Even.	None
Stop bit (Стоповый бит)	Выбор из 1 и 2.	1
Flow control (Управление потоком)	Выбор из None (нет), Software (программное) и Hardware (аппаратное).	None
Protocol (Протокол)	Выбор из: None, Transparent, Modbus, Transparent Over Rlink, Modbus Over Rlink, AT Over COM и GPS Report. 1. None: Маршрутизатор не работает с портом RS-232. 2. Transparent: маршрутизатор осуществляет прозрачную передачу последовательных данных, не используя какие-либо протоколы. 3. Modbus: маршрутизатор преобразует данные RTU Modbus в данные TCP Modbus и наоборот. 4. Transparent Over Rlink: маршрутизатор передает все данные с последовательного порта RS-232 на Robustlink, который передает их дальше. 5. Modbus Over Rlink: Маршрутизатор преобразует данные с последовательного порта RS-232 в данные протокола Modbus TCP и передает их Robustlink, который передает их дальше. 6. AT Over COM: выбрать, если требуется управлять маршрутизатором через COM порт. Например, передавать AT команды маршрутизатору через COM-порт (RS-232). 7. GPS Report: выбрать, чтобы активировать вывод статусной информации GPS через порт RS-232.	None
Mode @Transparent (режим при Transparent)	Выбор из TCP Server, TCP Client и UDP. TCP Client (Клиент TCP): маршрутизатор работает в качестве TCP клиента, инициализируя TCP соединение с TCP сервером. Адрес сервера поддерживает как IP, так и доменное имя. TCP Server (Сервер TCP): маршрутизатор работает в качестве TCP сервера, прослушивая запросы на соединение от TCP клиента. UDP: маршрутизатор работает в качестве UDP клиента.	TCP Client
Local Port @Transparent (локальный порт для режима Transparent)	Ввести локальный порт для TCP или UDP.	0
Multiple Server @Transparent (мультисервер для	Нажать кнопку *Add*, чтобы добавить мультисервер. Необходимо ввести IP и порт сервера, а также включить или отключить Send data to serial.	None

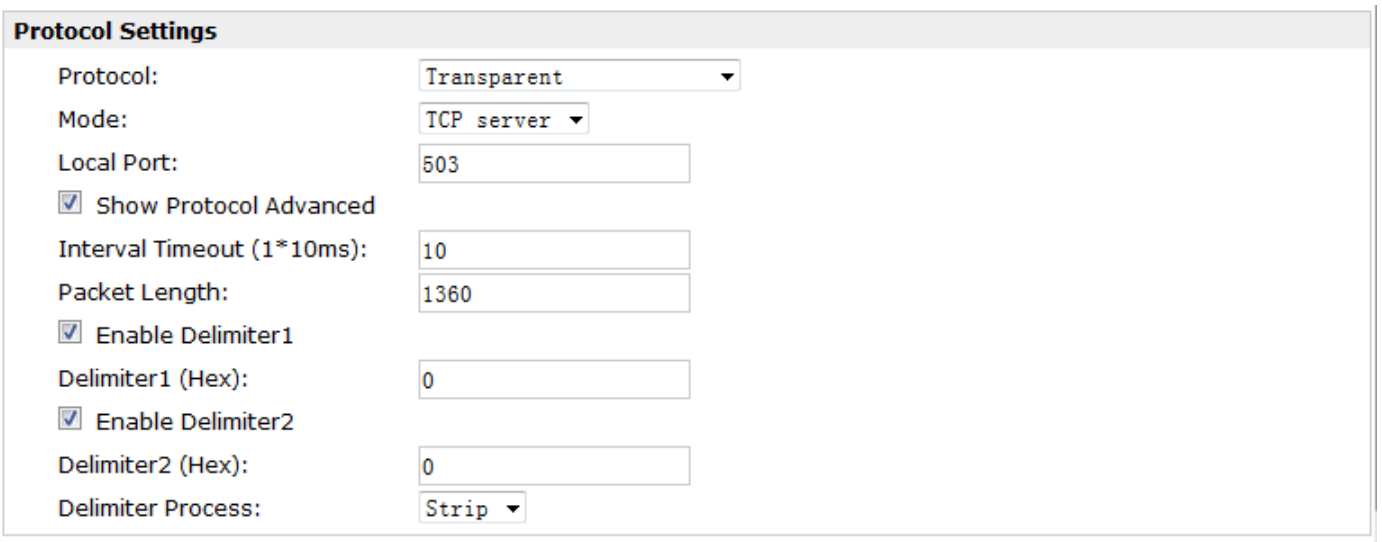
RS232 @ Serial (последовательный интерфейс RS232)		
режима Transparent)	Если отключить Send data to serial, маршрутизатор не будет передавать данные с этого сервера на последовательный порт. ***Примечание:*** *этот раздел недоступен, если Mode выбран TCP server.*	
Show Protocol Advanced @ Transparent (отобразить расширенные настройки)	Установить отметку, чтобы включить расширенные настройки протокола.	Disable (отключено)
Local IP @ Transparent (Локальный IP для Transparent)	Данный элемент отображается, если включен один из VPN туннелей R3000, это означает, что последовательные данные могут быть поставлены в соответствие локальному IP-адресу и переданы или получены через VPN туннель. *Примечание: если не включен ни один туннель, этот элемент не отображается.*	Null
Interval Timeout @Transparent (время ожидания для режима Transparent)	Последовательный порт ставит данные в очередь в буфере и отправляет их в сотовую WAN/Ethernet WAN, по истечении времени, указанного в этом поле. ***Примечание****: передача данных ативируется также согласно настройкам длины пакета или разделителя, даже если указанный в данном поле тайм-аут не истёк.*	10
Packet Length @Transparent (Длина пакета для режима Transparent)	Настройка длины пакета определяет максимальный объем данных, который может накапливаться в буфере последовательного порта перед отправкой. Значение 0 в этом поле, означает, что максимальное количество не задано, и данные в буфере будут отправлены, как определено Interval Timeout, настройками разделителя или — по заполнению буфера. Если для длины пакета определено значение между 1 и 1024 байтами, данные в буфере будут отправлены, как только будет достигнута указанная длина. ***Примечание****: передача данных ативируется также согласно настройкам interval timeout или разделителя, даже если не достигнута указанная в данном поле длина пакета.*	1360
Enable Delimiter1/2 (Включить разделитель 1/2)	Если включен разделитель 1, последовательный порт ставит данные в очередь в буфере и отправляет их в сотовую WAN/Ethernet WAN, когда получает определенный символ, введенный здесь в шестнадцатиричном формате. Второй символ-разделитель может быть включен и задан в поле Delimiter 2, в этом случае оба символа действуют в качестве разделителей для управления отправкой данных.	Disable (отключено)
Delimiter1/2 @Transparent (Разделитель (Hex) для режима Transparent)	Ввести разделитель в шестнадцатеричном формате.	0
Delimiter Process	Это поле определяет способ обработки данных после получения	Strip

RS232 @ Serial (последовательный интерфейс RS232)		
@Transparent (Обработка разделителя для режима Transparent)	разделителя. None: данные из буфера будут переданы при получении разделителя; символы разделителя также включаются в данные. Strip: перед передачей из данных в буфере удаляется разделитель.	
Local IP @ Modbus (Локальный IP для Modbus)	Данный элемент отображается, если включен один из VPN туннелей R3000, это означает, что последовательные данные могут быть поставлены в соответствие локальному IP-адресу и переданы или получены через VPN туннель.	0
Local Port @ Modbus (Локальный порт для Modbus)	Ввести локальный порт для Modbus.	0
Attached serial device type @Modbus (Тип подключенного устройства для Modbus)	Выбор из: Modbus RTU slave, Modbus ASCII slave, Modbus RTU master и Modbus ASCII master. Modbus RTU slave: маршрутизатор соединяется с ведомым устройством Modbus, которое работает по протоколу Modbus RTU. Modbus ASCII slave: маршрутизатор соединяется с устройством Modbus slave, работающим по протоколу Modbus ASCII. ***Примечание**: если выбрано Modbus RTU slave и протокол Modbus* ASCII *slave маршрутизатор служит TCP сервером, пользователю необходимо ввести номер локального порта в Local Port @Modbus и дождаться подключения.* Modbus RTU master: маршрутизатор соединяется с ведущим устройством, работающим по протоколу RTU Modbus. Modbus ASCII master: маршрутизатор соединяется с ведущим устройством, работающим по протоколу Modbus ASCII. *Примечание: если выбраны протоколы Modbus RTU master и Modbus ASCII master, маршрутизатор служит TCP клиентом, и пользователю необходимо указать адрес и номер порта для ведомого устройства в* Slave Address @ Modbus Slave *и* Slave Port @ Modbus Slave*, после чего, подключиться к серверу.*	Modbus RTU slave
Modbus Slave @Modbus	Добавить ведомые Modbus устройства, которые будут опрашиваться ведущим Modbus устройством (маршрутизатором). Этот раздел выводится на экран только при выборе Modbus RTU master или Modbus ASCII master в Attached serial device type.	Null
Slave Address @ Modbus Slave (Адрес ведомого для Modbus)	Это соединение обычно используется для подключения к ведомым устройствам Modbus, например, TCP сервера. Ввести IP-адрес TCP сервера.	Null
Slave Port @ Modbus (Порт ведомого для Modbus)	Ввести номер порта TCP сервера.	Null
ID @ Modbus Slave (ID ведомого устройства Modbus)	Ввести идентификационный номер TCP сервера.	Null
Interval Timeout @	Последовательный порт ставит данные в очередь в буфере и	10

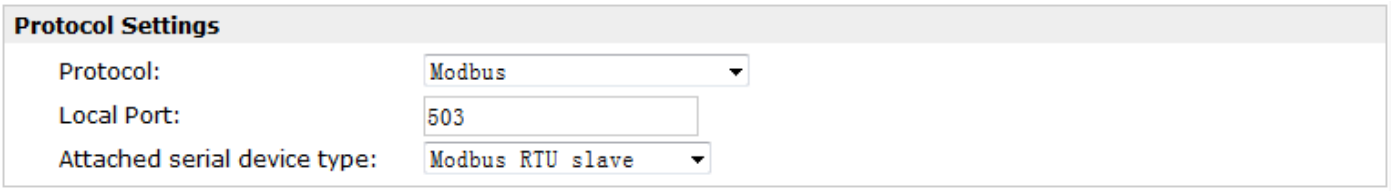
RS232 @ Serial (последовательный интерфейс RS232)		
Transparent Over Rlink (Задержка для Transparent Over Rlink)	отправляет их в сотовую WAN/Ethernet WAN (глобальную сеть), по истечении времени, указанного в этом поле.	
Attached serial device type @Modbus (Тип подключенного устройства для Modbus Over Rlink)	Выбор из Modbus RTU slave, Modbus ASCII slave. Modbus RTU slave: маршрутизатор соединяется с ведомым устройством Modbus, которое работает по протоколу RTU Modbus. Modbus ASCII slave: маршрутизатор соединяется с ведомым устройством, которое работает по протоколу Modbus ASCII.	Null
Display all com @ AT Over COM (Отображение всех com для AT Over COM)	Включить, чтобы выводить на экран все виртуальные com модули маршрутизатора. Обычно для вызовов GPRS маршрутизатор использует /dev/ttyUSB0 и/dev/ttyUSB2. ***Примечание**: включение этой функция вызовет отключение функции Cellular WAN.*	Disable (отключено)
COM Name (Имя COM)	Вывод имени внутреннего виртуального com модуля.	/dev/ttyUSB1



- Если протокол выбран, как Transparent:



- Если выбран протокол Modbus:



- Если выбран протокол Transparent Over Rlink:

- Если выбран протокол Modbus Over Rlink:

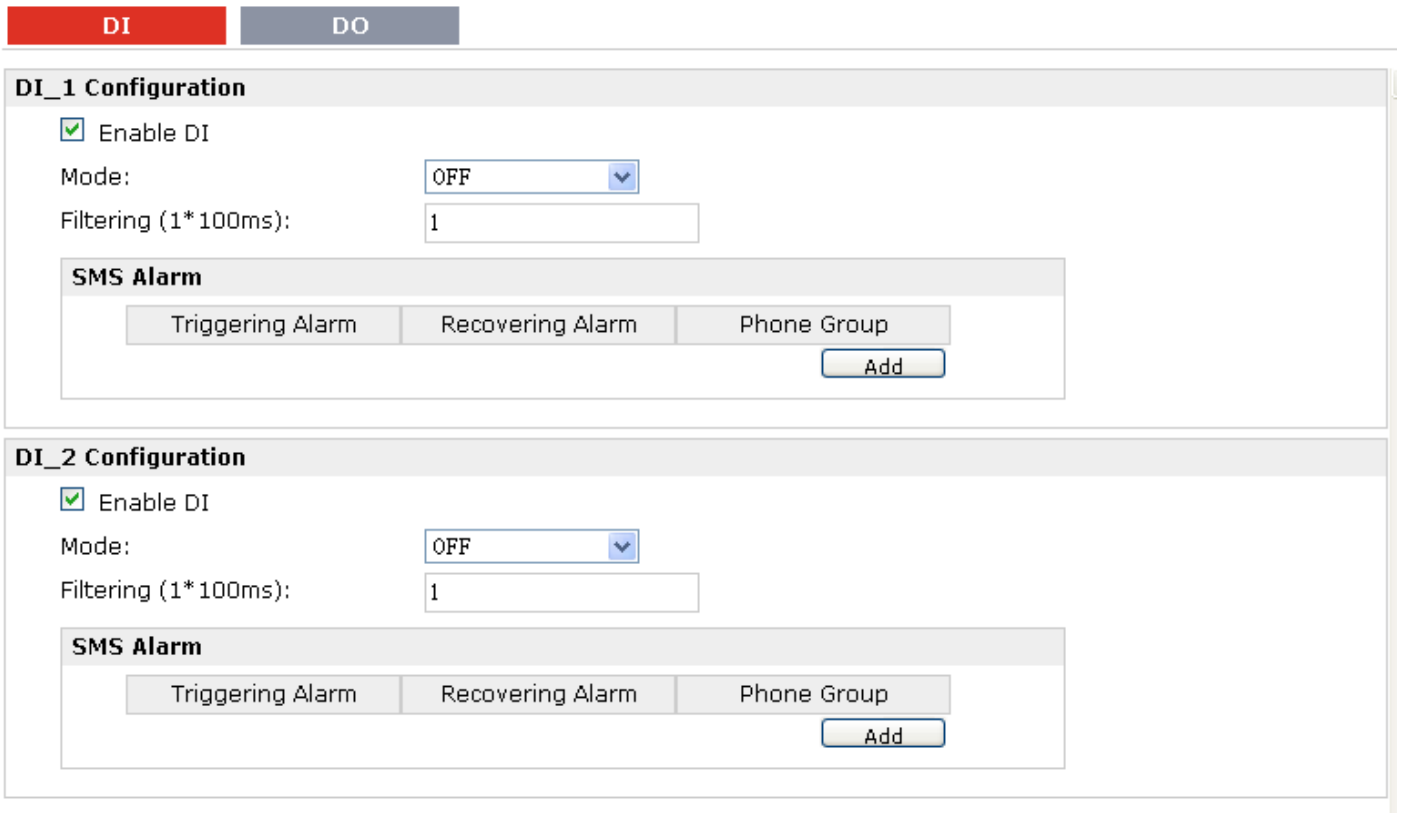
RS485 @ Serial (последовательный интерфейс RS-485)		
Элемент	Описание	По умолчанию
Baud-rate (Скорость в бодах)	Выбор из 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 и 230400.	115200
Data bit (Бит данных)	Выбор из 7 и 8.	8
Parity (Четность)	Выбор из None, Odd и Even.	None (нет)
Stop bit (Стоповый бит)	Выбор из 1 и 2.	1
Protocol (Протокол)	Выбор из None, Transparent и Modbus. Transparent: маршрутизатор осуществляет прозрачную передачу последовательных данных, не используя какие-либо протоколы. Modbus: маршрутизатор осуществляет передачу последовательных данных по протоколу Modbus.	Transparent
Mode @Transparent (Режим при Transparent)	Выбор из TCP Server, TCP Client и UDP.	TCP Client
Local Port @Transparent (Обработка разделителя для режима Transparent)	Ввести локальный порт для TCP или UDP.	0
Multiple Server @Transparent (Обработка разделителя для режима Transparent)	Нажать кнопку *Add*, чтобы добавить мультисервер. Необходимо ввести IP и порт сервера, а также включить или отключить *Send data to serial*. Если отключить *Send data to serial*, маршрутизатор не будет передавать данные с этого сервера на последовательный порт. ***Примечание:*** *этот раздел недоступен, если в Mode выбрано TCP*	Null

RS485 @ Serial (последовательный интерфейс RS-485)		
	server.	
Enable Protocol @Transparent (Обработка разделителя для режима Transparent)	Установить отметку, чтобы включить расширенные настройки протокола.	Disable (отключено)
Local IP @ Transparent (Локальный IP для Transparent)	Данный элемент отображается, если включен один из VPN туннелей R3000, это означает, что последовательные данные могут быть поставлены в соответствие локальному IP-адресу и переданы или получены через VPN туннель. *Примечание: если не включен ни один туннель, этот элемент не отображается.*	0
Interval Timeout @Transparent (Обработка разделителя для режима Transparent)	Последовательный порт ставит данные в очередь в буфере и отправляет их в сотовую WAN/Ethernet WAN по истечении времени, указанного в этом поле. ***Примечание**: передача данных ативируется также согласно настройкам длины пакета или разделителя даже, если указанный в данном поле тайм-аут не достигнут.*	10
Packet Length @Transparent (Длина пакета для Transparent)	Настройка длины пакета определеяет максимальный объем данных, который может накапливаться в буфере последовательного порта перед отправкой. Значение 0 в этом поле, означает, что максимальное количество не задано, и данные в буфере будут отправлены, как определено Interval Timeout, настройками разделителя или — по заполнению буфера. Если для длины пакета определено значение в интервале между 1 и 1024 байтами, данные в буфере будут переданы немедленно по достижении этого значения. ***Примечание**: передача данных ативируется также согласно настройкам interval timeout или разделителя, даже если не достигнута указанная в данном поле длина пакета.*	1360
Enable Delimiter1 (Включить Delimiter1)	Если включен разделитель 1, последовательный порт ставит данные в очередь в буфере и отправляет их в сотовою WAN/Ethernet WAN, когда получает определенный символ введенный здесь в шестнадцатиричном формате. Второй символ-разделитель может быть включен и задан в поле Delimiter 2, в этом случае оба символа действуют в качестве разделителей для управления отправкой данных.	Disable (отключено)
Delimiter1 (Hex) @ Transparent	Ввести разделитель в шестнадцатеричном формате.	0
Delimiter Process @ Transparent (Обработка разделителя для Transparent)	Это поле определяет способ обработки данных после получения разделителя. None: данные из буфера будут переданы при получении разделителя; символы разделителя также включаются в данные. Strip: перед передачей из данных в буфере удаляется разделитель.	Strip
Local IP @ Modbus (Локальный IP для Modbus)	Данный элемент отображается, если включен один из VPN туннелей R3000, это означает, что последовательные данные могут быть	0

RS485 @ Serial (последовательный интерфейс RS-485)		
	поставлены в соответствие локальному IP-адресу и переданы или получены через VPN туннель. *Примечание: если не включен ни один туннель, этот элемент не отображается.*	
Local Port @ Modbus (Локальный порт для Modbus)	Ввести локальный порт для Modbus.	0
Attached serial device type @ Modbus (Тип подключенного устройства для Modbus)	Выбор из Modbus RTU slave, Modbus ASCII slave, Modbus RTU master и Modbus ASCII master. Modbus RTU slave: маршрутизатор соединяется с ведомым устройством Modbus, которое работает по протоколу RTU Modbus. Modbus ASCII slave: маршрутизатор соединяется с устройством Modbus slave, работающим по протоколу Modbus ASCII. Modbus RTU master: маршрутизатор соединяется с ведущим устройством, работающим по протоколу RTU Modbus. Modbus ASCII master: маршрутизатор соединяется с ведущим устройством, работающим по протоколу Modbus ASCI .	Modbus RTU slave
Modbus Slave@ Modbus (Ведомое устройство Modbus)	Добавить ведомые устройства Modbus, которые будут опрашиваться ведущим устройством Modbus (маршрутизатором). Этот раздел выводится на экран только при выборе *Modbus RTU master* или *Modbus ASCII master* в *Attached serial device type*.	Null
Slave Address @ Modbus Slave (Адрес ведомого для Modbus)	Это соединение обычно используется для подключения к ведомым устройствам Modbus, например, TCP сервер. Ввести IP-адрес TCP сервера.	Null
Slave Port @ Modbus (Порт ведомого для Modbus)	Ввести номер порта TCP сервера.	Null
ID @ Modbus Slave (ID ведомого устройства Modbus)	Ввести идентификационный номер TCP сервера.	Null
Interval Timeout @ Transparent Over Rlink (Задержка для Transparent Over Rlink)	Последовательный порт ставит данные в очередь в буфере и отправляет их в сотовую WAN/Ethernet WAN глобальную сеть, по истечении времени, указанного в этом поле.	10
Attached serial device type @Modbus (Тип подключенного устройства для Modbus Over Rlink)	Выбор из: Modbus RTU slave или Modbus ASCII slave. Modbus RTU slave: маршрутизатор соединяется с ведомым устройством Modbus, которое работает по протоколу RTU Modbus. Modbus ASCII slave: маршрутизатор соединяется с устройством Modbus slave, работающим по протоколу Modbus ASCII.	Modbus RTU slave

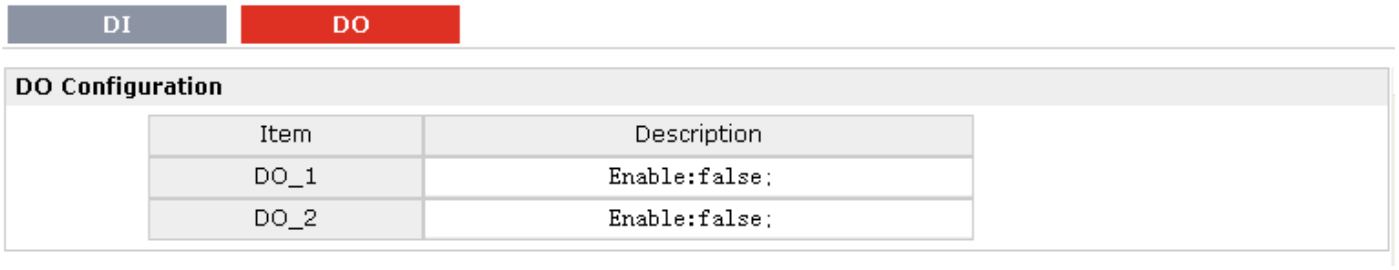
3.15 Configuration -> DI/DO (Конфигурация-> цифровой вход/выход)

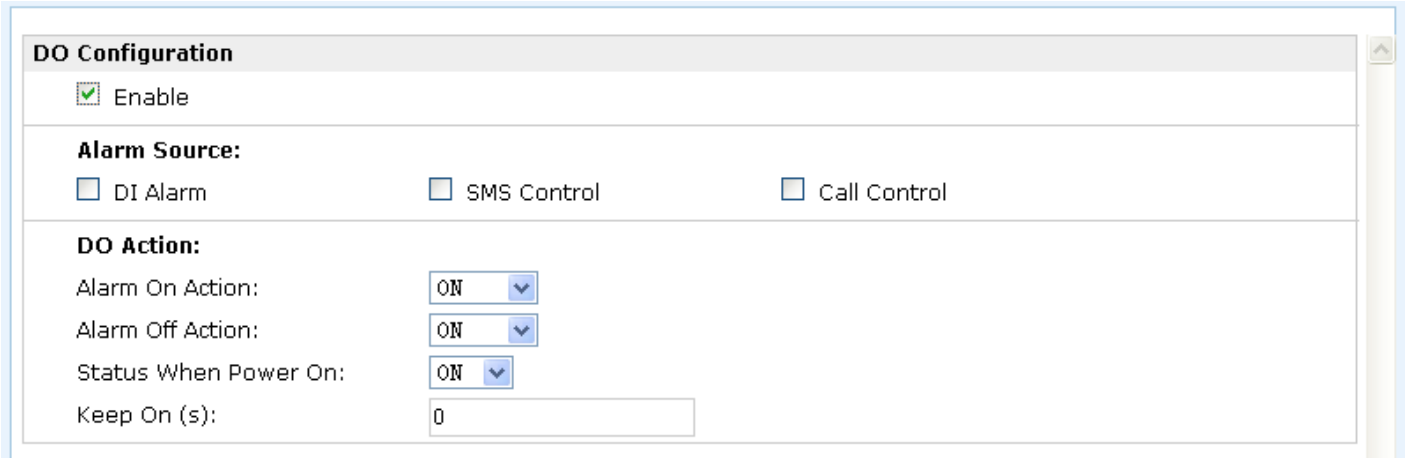
Этот раздел позволяет настроить параметры цифрового входа/выхода DI/DO.



DI (Цифровой вход)		
Элемент	Описание	По умолчанию
Enable DI (Включить цифровой вход)	Щелкнуть для включения DI.	Disable (отключено)
Mode (Режим)	Выбор из OFF, ON, EVENT_COUNTER. OFF: соединен с GND (логический 0). Если контакт DI подключается к GND, R3000 регистрирует сигнал оповещения DI. ON: Изолирован от GND (логическая 1). Если контакт DI отключен от GND, R3000 регистрирует сигнал оповещения DI. EVENT_COUNTER: режим счетчика событий.	OFF
Filtering (Фильтрация)	Программная фильтрация служит для управления переключениями. Ввод от 0 до 10000 мс.	1
Count Trigger (Запуск по счетчику)	Доступно, если для DI выбран режим Event Counter. Ввод от 0 до 100 (0= сигнал оповещения не инициализируется). Сигнал оповещения инициализируется по достижении счетчиком указанного отсчета. После инициирования сигнала оповещения DI продолжает отсчет, но повторная инициализация сигнала оповещения не производится.	0

DI (Цифровой вход)		
Counter Active (Активация отсчета)	Доступно, если для DI выбран режим Event Counter. Выбор из Hi to Lo, Lo to Hi (выс.->низк., низк.->выс). В режиме Event Counter канал допускает работу с концевыми или бесконтактными переключателями и отсчитывает события по состоянию ВКЛ\ВЫКЛ. Если выбрано Lo to Hi, увеличение значения отсчета происходит при нажатии подключенного переключателя. Если выбрано Hi to Lo, увеличение значения отсчета происходит при возврате из нажатого положения подключенного переключателя.	Lo to Hi
Counter Start When Power On (Запуск отсчета при подаче питания)	Доступно, если для DI выбран режим Event Counter. Если включена эта функция, начало отсчета запускается в максимально короткий для модема срок. Если необходима работа R3000 в режиме счетчика событий, пользователь должен активировать Counter Start When Power On. Если Counter Start When Power On отключено, отсчет запускается также по получении SMS команды. Подробнее см. документ *SMS command of R3000 (SMS команды R3000)*.	Disable (отключено)
Triggering Alarm (Запуск оповещения)	SMS, отправляемое после запуска сигнала оповещения (максимум 70 символов ASIC II)	Null
Recovering Alarm (Отключение сигнала оповещения)	SMS, отправляемое после отключения сигнала оповещения (максимум 70 символов ASIC II)	Null
Phone Group (Телефонная группа)	SMS сигнала оповещения передается абонентам указанной телефонной группы. Каждая телефонная группа включает до 10 телефонных номеров.	Null





DO (Цифровой выход)		
Элемент	Описание	По умолчанию
Enable (Разрешить)	Щелкнуть для включения цифрового выхода (DO).	Disable (отключено)
Alarm Source (Источник аварийного сигнала)	Цифровой выход инициализируется различными источниками сигнала оповещения. Выбор из DI Alarm, SMS Control, Call Control, доступен выбор более одного источника. DI Alarm: цифровой выход инициализирует связанное действие при получении сигнала оповещения с цифрового входа. SMS Control: Цифровой выход инициализирует связанное действие при получении SMS с номера из телефонной книги. Call Control: Цифровой выход инициализирует связанное действие при получении телефонного вызова с номера из телефонной книги.	Null
Alarm On Action (Действие при получении оповещения)	Цифровой выход инициируется при получении сигнала оповещения. Выбор из OFF, ON, Pulse. OFF: отключение от GND при инициализации. ON: замыкание на GND при инициализации. Pulse: при активации генерируется последовательность прямоугольных импульсов, как определено в параметрах pulse mode (импульсного режима).	ON
Alarm Off Action (Действие при отключении оповещения)	Цифровой выход инициируется при отключении сигнала оповещения. Выбор из: OFF, ON, Pulse. OFF: отключение от GND при инициализации. ON: замыкание на GND при инициализации. Pulse: при активации генерируется последовательность прямоугольных импульсов, как определено в параметрах pulse mode (импульсного режима).	ON
Status When Power On (Статус при подаче питания)	Задать состояние цифрового выхода, при подаче питания. Выбор из OFF, ON. OFF: отключен от GND. ON: замкнут на GND.	ON
Keep On (s) (время поддержания активности, с)	Доступно, когда для действия цифрового выхода Alarm On Action/Alarm Off Action выбран статус ON, ввести время поддержания активности Digital Output. Ввод от 0 до 255 секунд (0=поддержание активности до следующего действия).	0
Delay (Задержка)	Доступно, когда активирован Pulse в Alarm On Action/Alarm Off Action. Первый импульс генерируется после задержки — Delay. Ввод от 0 - 30000 мс (0=импульс генерируется без задержки)	0
Low (Низкий)	Доступно, когда активирован Pulse в Alarm On Action/Alarm Off Action. В режиме Pulse Output выбранный канал цифрового выхода генерирует последовательность прямоугольных импульсов, как определено в параметрах импульсного режима. Здесь задается ширина импульса	10

DO (Цифровой выход)		
	низкого уровня. Ввод от 1 до 30000 мс.	
High (Высокий)	Доступно, когда активирован Pulse в Alarm On Action/Alarm Off Action. В режиме Pulse Output выбранный канал цифрового выхода генерирует последовательность прямоугольных импульсов, как определено в параметрах импульсного режима. Здесь задается ширина импульса высокого уровня. Ввод от 1 до 30000 мс.	10
Output (Вывод)	Доступно, когда активирован Pulse в Alarm On Action/Alarm Off Action. Количество импульсов, ввод от 0 до 30000. (0 — вывод непрерывной импульсной последовательности)	0
SMS Content On (Текст SMS для On)	Доступно, когда активирован SMS Control в Alarm Source. Ввести текст SMS, для события Alarm On Action — SMS (макс. 70 символов ASIC II).	Null
SMS Content Off (Текст SMS для Off)	Доступно, когда активирован SMS Control в Alarm Source. Ввести текст SMS, для события Alarm Off Action — SMS (макс. 70 символов ASIC II) (максимум 70 символов ASICII)	Null
SMS Content On Reply (Текст ответного SMS для On)	Ввести текст SMS для отправки после инициализации DO (максимум 70 символов ASIC II).	Null
SMS Content Off Reply (Текст ответного SMS для Off)	Ввести текст SMS для отправки после отмены инициализации DO (максимум 70 символов ASIC II).	Null
Phone Group (Телефонная группа)	Щелкнуть для добавления телефонных групп.	Null

Примечание: *R3000-4L не поддерживает функцию SMS/ВЫЗОВ, поэтому на его веб-странице разделы Call и SMS не отображаются.*

3.16 Configuration -> USB (Конфигурация-> USB)

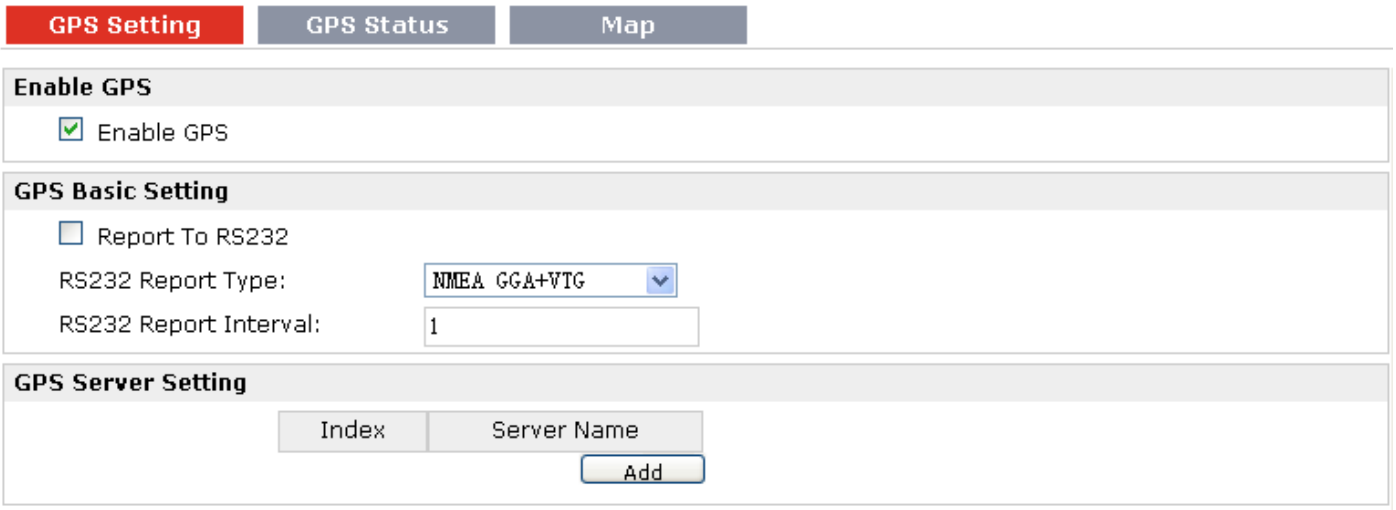
Этот раздел позволяет настроить параметры USB.

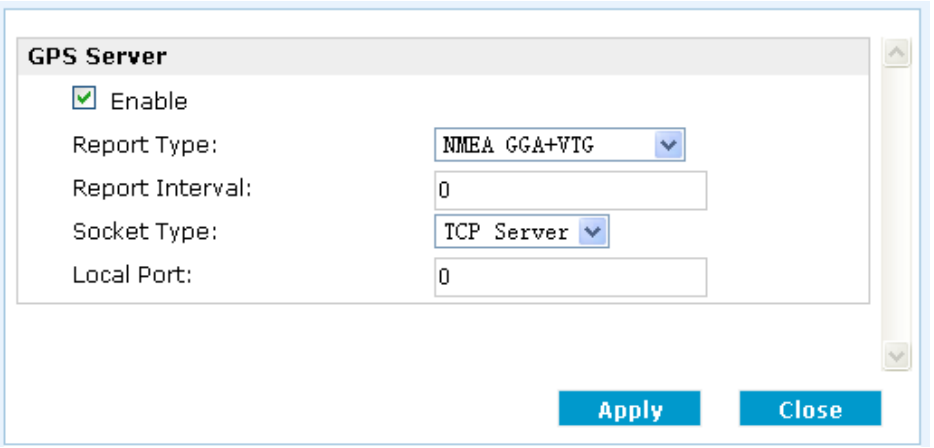
Примечание*: В этот разъем можно вставить USB накопитель, например, флеш-диск или жесткий диск. Если на подключенном накопителе будет файл конфигурации или встроенное микропрограммное обеспечение R3000, устройство автоматически обновит конфигурацию или встроенное ПО. Мы предлагаем отдельный документ с инструкциями по автоматическому обновлению с USB.*

USB		
Элемент	Описание	По умолчанию
Enable automatic update of configuration (Разрешить автоматическое обновление конфигурации)	Отметить, чтобы автоматически обновлять файл ***конфигурации*** R3000, при подключении USB накопителя, с таким файлом.	отключено
Enable automatic update of firmware (Разрешить автоматическое обновление встроенного микропрограммного обеспечения)	Отметить, чтобы автоматически обновлять ***встроенное микропрограммное обеспечение*** R3000, при подключении USB накопителя с ПО.	отключено

3.17 Configuration -> GPS (Конфигурация-> GPS)

Этот раздел позволяет настроить GPS параметры, такие как включение/отключение встроенного навигационного GPS-приемника и выдачу информации (поддерживается не во всех моделях R3000).



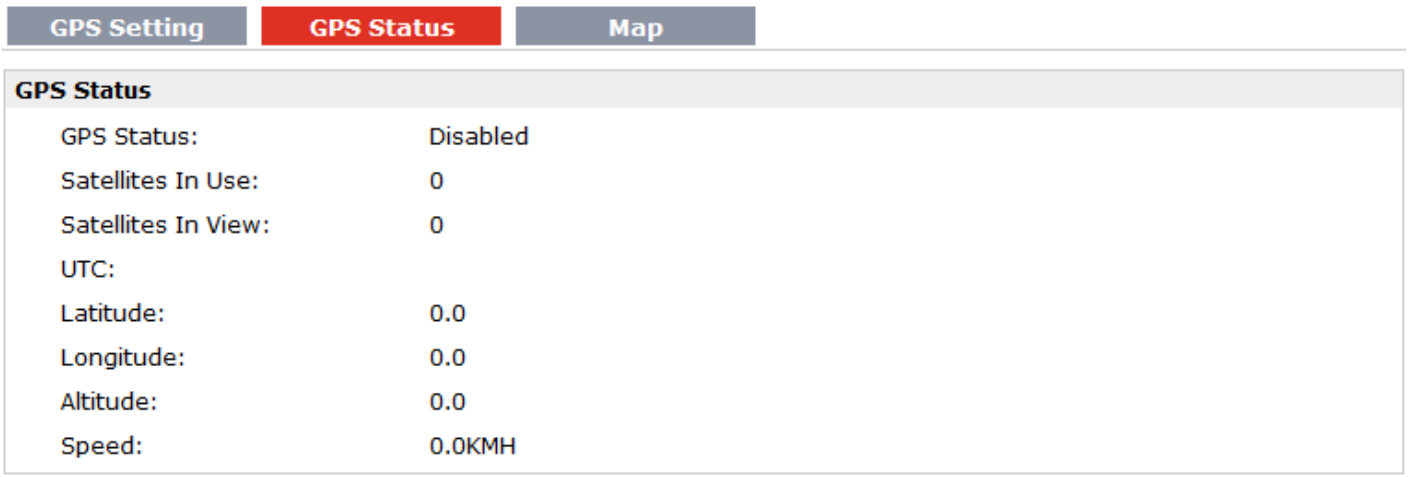


GPS Setting (GPS настройки)		
Элемент	Описание	По умолчанию
Enable GPS (Включить GPS-приёмник)	Щелкнуть для включения GPS-приемника.	Disable (отключено)

GPS Setting (GPS настройки)		
Report To RS232 (Отчет на RS-232)	Щелкнуть для включения вывода GPS отчета на последовательный порт RS-232 маршрутизатора.	Disable (отключено)
RS232 Report Type (Тип отчета RS232)	Выбор из NMEA GGA+VTG, NMEA GGA+VTG+RMC и NMEA RMC". NMEA GGA+VTG: данные о координатах места по GPS(GGA) + фактический трек, путевой угол и скорость относительно грунта (VTG). NMEA GGA+VTG+RMC: данные о координатах места по GPS(GGA) + фактический трек + путевой угол и скорость относительно грунта (VTG) + рекомендуемый минимальный перечень данных по GPS и ГЛОНАСС (RMC). NMEA RMC: рекомендуемый минимальный перечень данных по GPS и ГЛОНАСС (RMC).	NMEA GGA+VTG
RS232 Report Interval (Интервал между отчетами RS232)	Установить интервал между сообщениями о GPS статусе последовательному порту RS-232.	1
Index @ GPS Server Setting (Индекс сервера GPS)	Отображение индекса GPS сервера.	Null
Server Name @ GPS Server Setting (Имя GPS сервера)	Отображение типа GPS сервера.	Null
Add (Добавить)	Щелкнуть на *Add* для добавления GPS сервера.	
Report Type (Тип отчета)	Выбор из NMEA GGA+VTG, NMEA GGA+VTG+RMC и NMEA RMC. NMEA GGA+VTG: данные о координатах места по GPS(GGA) + фактический трек, путевой угол и скорость относительно земли (VTG). NMEA GGA+VTG+RMC: данные о координатах места по GPS (GGA) + фактический трек, путевой угол и скорость относительно земли (VTG) + рекомендуемый минимальный перечень данных по GPS и ГЛОНАСС (RMC). NMEA RMC: рекомендуемый минимальный перечень данных по GPS и ГЛОНАСС (RMC).	NMEA GGA+VTG
Report Interval (Интервал между отчетами)	Установить интервал отправки отчётов на сервер.	0
Socket Type (Тип сокета)	Выбор из TCP Server, TCP Client и UDP. TCP Client (TCP клиент): маршрутизатор работает в качестве TCP клиента, инициирует TCP соединения с TCP сервером (GPS сервером); адрес сервера поддерживает, как IP, так и доменное имя. TCP Server (TCP сервер): маршрутизатор работает в качестве TCP сервера (GPS сервер), прослушивая запросы на подключения от TCP клиентов. UDP: маршрутизатор работает в качестве UDP клиента.	TCP Server
Local Port @ TCP Server (Локальный порт)	Указать номер локального порта TCP сервера.	0
Server Address @ TCP Client (Адрес сервера)	Указать адрес TCP сервера.	Null
Server Port @ TCP Client	Указать номер удаленного порта TCP сервера.	0

GPS Setting (GPS настройки)		
(Порт сервера для TCP клиента)	*Маршрутизатор поддерживает до 3х GPS серверов мониторинга и переподключается при разрыве TCP соединения.*	

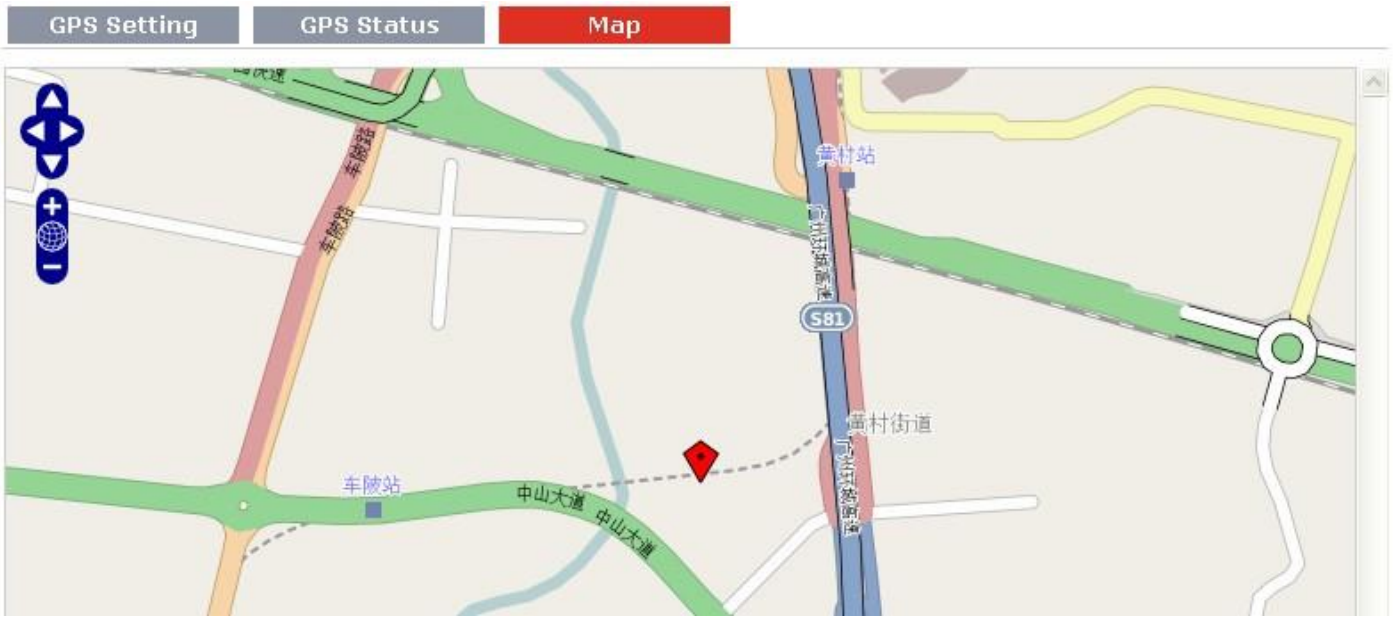
Этот раздел позволяет контролировать видимость GPS-спутников и определение координат местоположения, высоты, скорости.



GPS		
Элемент	Описание	По умолчанию
GPS Status (Состояние GPS навигации)	Включает: Not Installed, Disabled, No Fix/Invalid, Standalone GPS Fix, Differential GPS Fix. Not Installed (не установлено): GPS-модуль отсутствует. Disabled (Отключено): GPS-приемник не активирован (не выполнен щелчок на Enable GPS в GPS Setting). No Fix/Invalid (нет привязки/ошибка): GPS-приемник активен, но GPS сигнал отсутствует (следует поместить маршрутизатор вне помещения, чтобы получить более мощный сигнал GPS). Standalone GPS Fix (автономная навигация): является универсальным режимом GPS позиционирования. Differential GPS Fix (дифференциальный способ): дифференциальные GPS методы используются для повышения качества определения местоположения. Они могут применяться в режиме реального времени непосредственно в поле или — при последующей обработке данных в офисе.	Not Installed
Satellites In Use (используемые спутники)	Отображение количества используемых спутников.	0
Satellites In View (Видимые спутники)	Отображение количества видимых спутников.	0
UTC (универсальное координированное время)	Отображение UTC спутников, предствляющее собой не местное, а универсальное координированное время.	Null
Latitude (Широта)	Отображение широты местоположения маршрутизатора.	0.0
Longitude (Долгота)	Отображение долготы местоположения маршрутизатора.	0.0

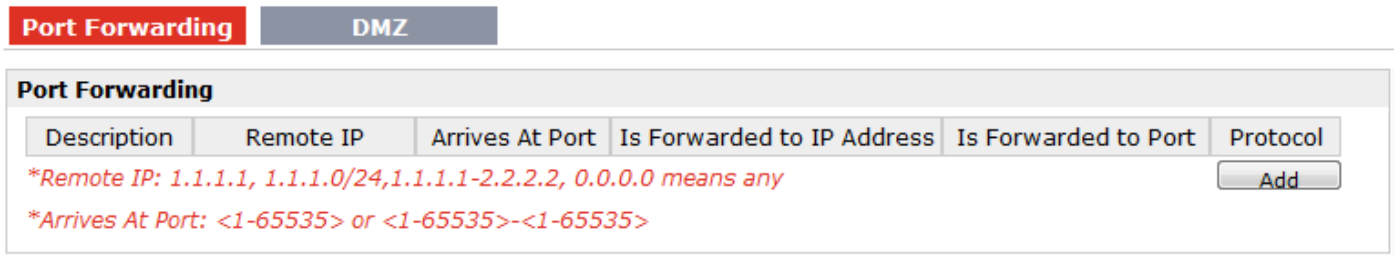
Altitude (Высота)	Отображение высотного положения маршрутизатора.	0.0
Speed (Скорость)	Отображение скорости перемещения маршрутизатора.	0.0 км/ч

Этот раздел позволяет пользователю проверять состояние GPS маршрутизатора в реальном времени на карте.



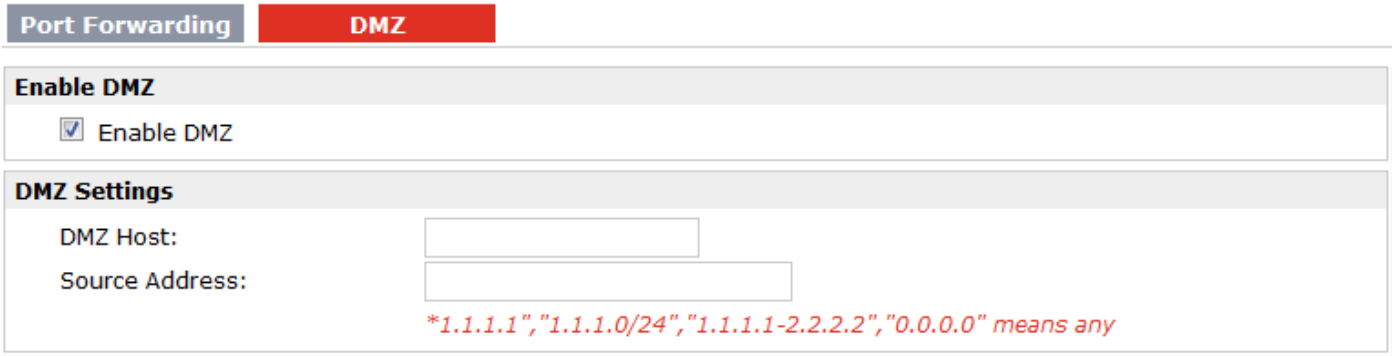
3.18 Configuration -> NAT/DMZ (Конфигурация-> NAT/DMZ)

Этот раздел позволяет настроить параметры NAT/DMZ (транслятор сетевых адресов/демилитаризованная зона).



Port Forwarding @ NAT/DMZ (переадресация портов для NAT/DMZ)		
Элемент	Описание	По умолчанию
Port Forwarding (Переадресация портов)	Вручную задать правило, по которому маршрутизатор будет перенаправлять данные, поступающие с некоторого диапазона портов на стороне Интернет, на порт и IP-адрес на стороне LAN.	Null
Remote IP (Удаленный IP-адрес)	Задать удаленный IP-адрес.	Null
Arrives At Port (Исходный порт)	Порт на стороне Интернет, который требуется ретранслировать в LAN.	Null

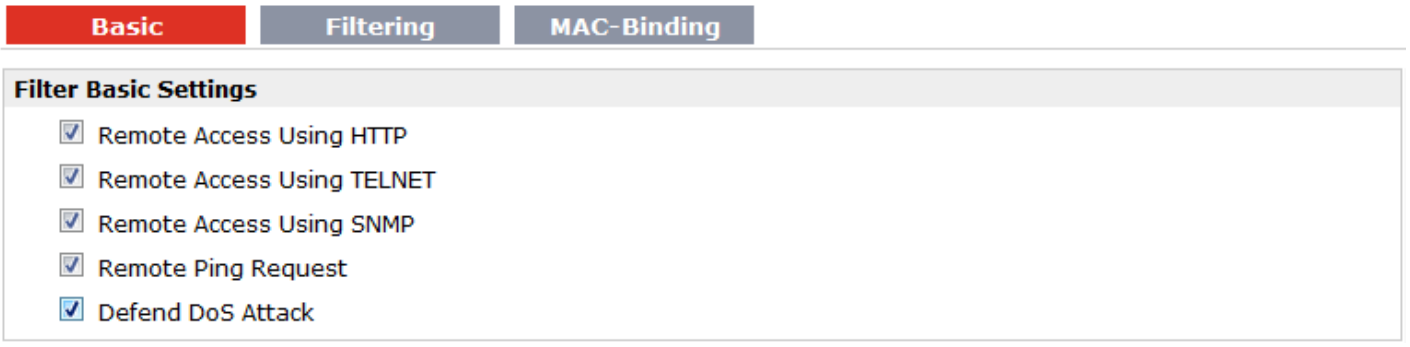
Port Forwarding @ NAT/DMZ (переадресация портов для NAT/DMZ)		
Is Forwarded to IP Address (ретранслировать на IP-адрес)	IP-адрес устройства на стороне LAN, на который требуется передавать данные.	Null
Is Forwarded to Port (Ретранслируется на порт)	Порт устройства на стороне LAN, на который требуется передавать данные.	Null
Protocol (Протокол)	Выбор из TCP, UDP или TCP&UDP, зависит от приложения.	TCP



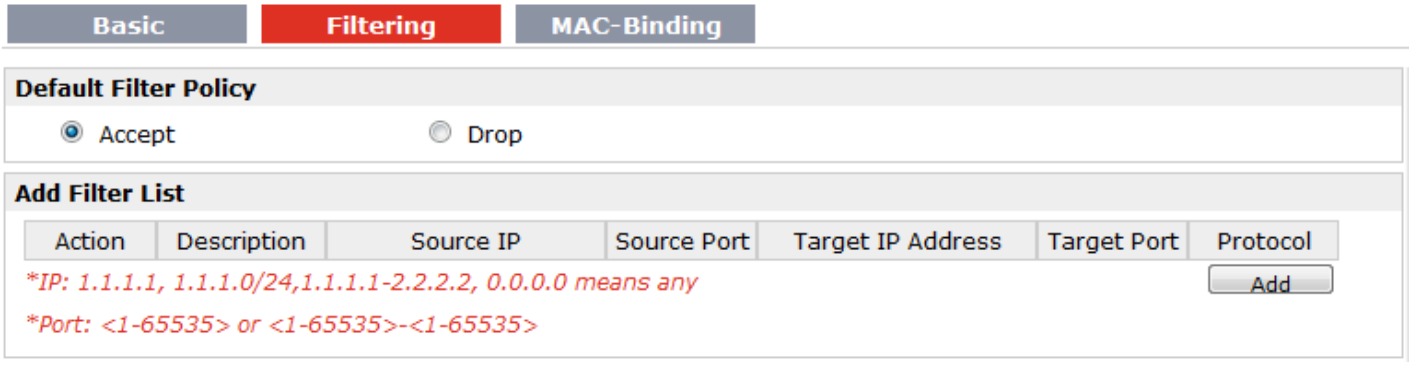
DMZ NAT/DMZ		
Элемент	Описание	По умолчанию
DMZ	DMZ-хост является узлом внутренней сети с открытыми портами, кроме тех, для которых установлена ретрансляция.	Null
Enable DMZ (Разрешить DMZ)	Выбрать для активации функции DMZ.	Enable (включено)
DMZ Host (DMZ-хост)	Ввести IP-адрес DMZ-хост внутренней сети.	0.0.0.0
Source Address (Исходный адрес)	Задать адрес, которому разрешено соединение с DMZ-хост. Нуль означает любой адрес.	0.0.0.0

3.19 Configuration -> Firewall (Конфигурация-> Брандмауэр)

Этот раздел позволяет настроить параметры брандмауэра.



Basic @ Firewall (Основные настройки брандмауэра)		
Элемент	Описание	По умолчанию
Remote Access Using HTTP (Удаленный доступ по HTTP)	Активировать, чтобы разрешить удаленный доступ к маршрутизатору по HTTP.	включено
Remote Access Using TELNET (Удаленный доступ по TELNET)	Активировать, чтобы разрешить удаленный доступ к маршрутизатору со стороны Интернет по Telnet.	включено
Remote Access Using SNMP (Удаленный доступ по SNMP)	Активировать, чтобы разрешить удаленный доступ к маршрутизатору со стороны Интернет по SNMP (упрощённый протокол управления сетью).	включено
Remote Ping Request (Отклик на Ping-запрос)	Активировать, чтобы разрешить маршрутизатору отвечать на запросы эхо-тестирования со стороны Интернет.	включено
Defend Dos Attack (Защита от Dos-атак)	Активировать для защиты от DOS-атак. DOS-атака это попытка сделать устройство или сетевой ресурс недоступным его целевым пользователям.	включено

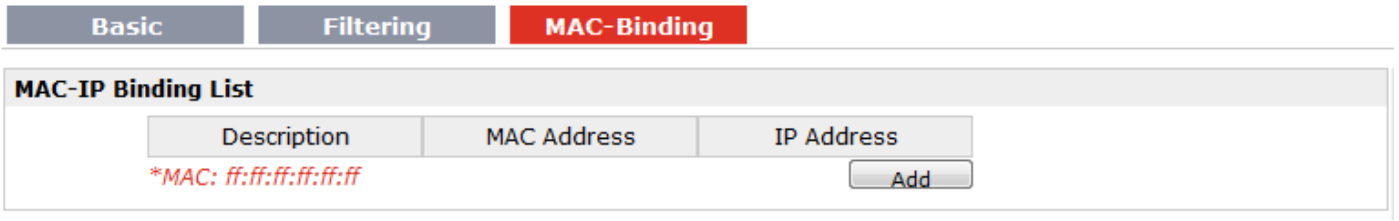


Filtering @ Firewall (Фильтрация. Брандмауэр)		
Элемент	Описание	По умолчанию
Default Filter Policy (Политика фильтрации по умолчанию)	Выбор из: Accept и Drop. Accept (принимать): маршрутизатор отклоняет все запросы на соединения кроме поступающих от узлов, которые соответствуют списку фильтрации. Drop (отклонять): маршрутизатор принимает запросы на соединение только от узлов, которые соответствуют списку фильтрации.	Accept (принимать)
Add Filter List (Добавить список фильтрации)	Щелкнуть на Add для добавления списка фильтрации.	Null
Action (Действие)	Выбор из Accept и Drop. Accept (принимать): Маршрутизатор отклоняет все запросы на соединения кроме поступающих от узлов, которые соответствуют данному правилу фильтрации. Drop (отклонять): Маршрутизатор принимает запросы на соединение только от узлов, которые соответствуют данному правилу фильтрации.	Accept (принимать)
Source IP	Определяет доступность одного или диапазона IP-адресов, которые	Null

Filtering @ Firewall (Фильтрация. Брандмауэр)		
(Исходный IP)	заданы исходным или отдельными IP-адресами.	
Source Port (Исходный порт)	Определяет доступность одного или диапазона портов, которые заданы исходным портом.	Null
Target IP Address (Целевой IP-адрес)	Определяет доступность одного или диапазона IP-адресов, которые заданы целевым или отдельными IP-адресами.	Null
Target Port (Целевой порт)	Определяет доступность одного или диапазона портов, которые заданы целевым портом.	Null
Protocol (Протокол)	Выбор из TCP, UDP, TCP&UDP, ICMP или ALL. Если пользователь не знает протокол своего приложения, рекомендуется выбирать ALL (ВСЕ).	TCP

***Примечание**: для указания диапазона IP-адресов или портов можно использовать «-», например, 1.1.1.1-2.2.2.2, 10000-12000.*

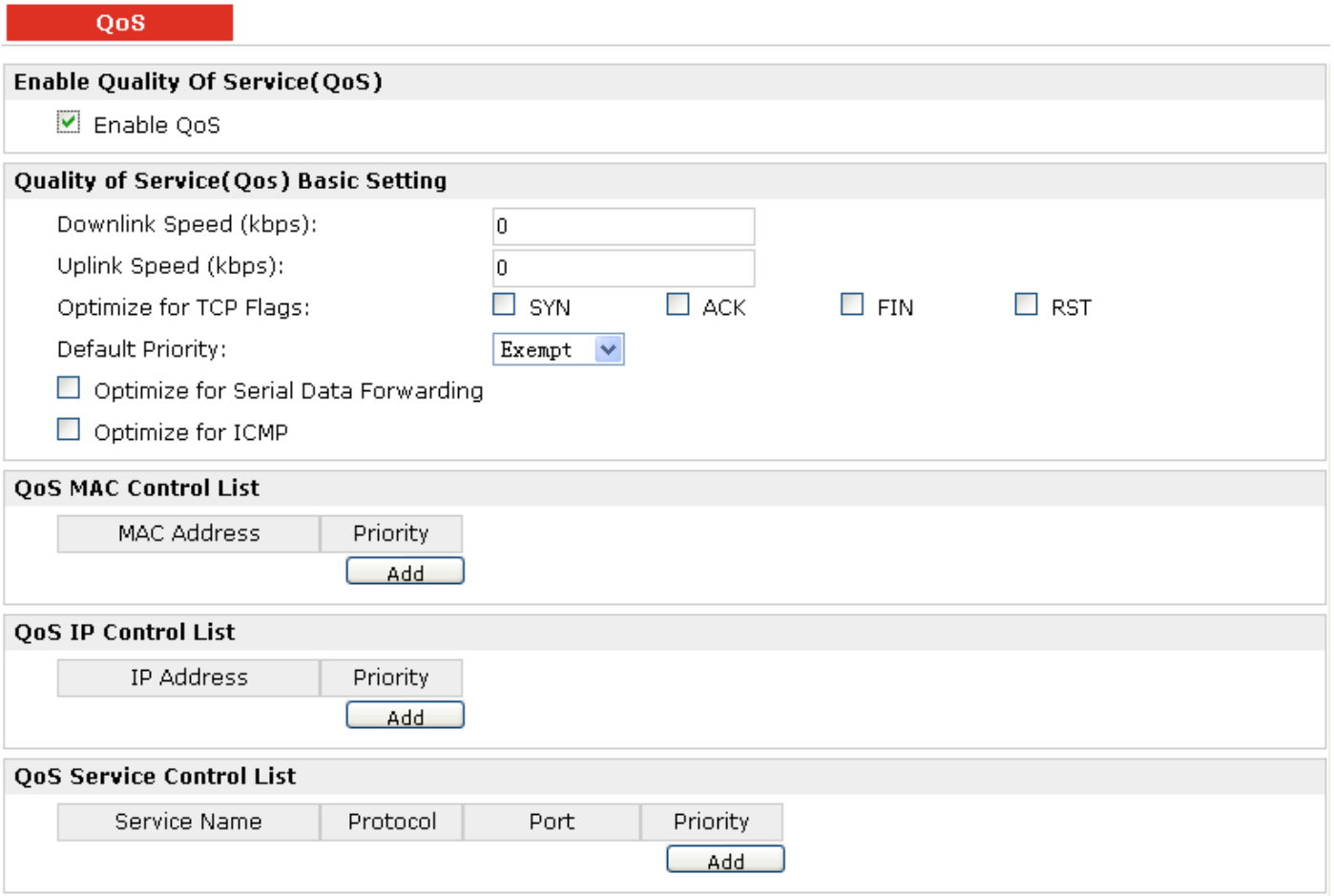
***Примечание**: настройки фильтрации должны быть разделены на две части. Часть 1 является точным списком фильтрации, а Часть 2 — политикой фильтрации по умолчанию. Приоритет Точного списка фильтрации выше политики фильтрации по умолчанию. Это означает, что, во время получения IP пакетов со стороны WAN, маршрутизатор сначала проверяет точный список фильтрации, если IP пакеты не соответствуют точному списку фильтрации, маршрутизатор выполняет политику фильтрации по умолчанию.*



Mac-Binding @ Firewall (Привязка MAC для брандмауэра)		
Элемент	Описание	По умолчанию
Mac-IP Bounding (Привязка IP-Mac)	Определенный узел (MAC) на стороне LAN для связи с маршрутизатором может использовать только определенный IP-адрес, или его запрос будет отклонен.	Null
Mac Address (MAC-адрес)	Ввести MAC-адрес требуемого узла.	Null
IP Address (IP-адрес)	Ввести IP-адрес требуемого узла.	Null

3.20 Configuration -> QoS (Конфигурация-> QoS — качество обслуживания)

Этот раздел позволяет настроить параметры QoS.



QoS		
Элемент	Описание	По умолчанию
Enable QoS (Включить QoS)	Щелкнуть для включения QoS.	Disable (отключено)
Downlink Speed (kbps) (Скорость нисходящего канала, в кбит/с)	Назначить скорость нисходящего канала маршрутизатора. ***Примечание**: настройка по умолчанию «0» означает отсутствие ограничения.*	0
Uplink Speed (kbps) (Скорость восходящего канала, в кбит/с)	Назначить скорость восходящего канала маршрутизатора. ***Примечание**: Настройка по умолчанию «0» означает отсутствие ограничения.*	0
Optimize for TCP Flags (Оптимизация флагов TCP)	Пользователь может включить TCP флаги: SYN, ACK, FIN, RST, в результате данные с вышеупомянутыми флагами получат высший приоритет. После включения данной функции, маршрутизатор оптимизирует тайм-аут управления TCP, в случае частой повторной передачи данных.	Disable (отключено)
Default Priority (Приоритет по умолчанию)	Выбор из Exempt, Premium, Express, Normal и Bulk. Пользователи (службы) без указания какого-либо приорита по умолчанию получают этот приоритет. Exempt (привилегированный): — самый высокий приоритет, который гарантирует минимум 50% и максимум 100% Downlink Speed	Normal (обычный)

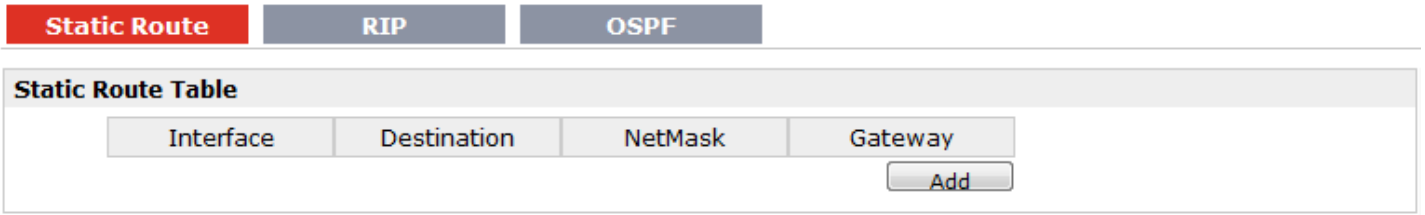
QoS		
	маршрутизатора. Premium (первоочередной): гарантирует минимум 25% и максимум 100% Downlink Speed. Express (срочный): гарантирует минимум 15% и максимум 100% Downlink Speed. Normal (обычный): гарантирует минимум 10% и максимум 100% Downlink Speed. Bulk (массовый): гарантирует минимум 1% и максимум 100% Downlink Speed.	
Optimize for Serial Data Forwarding (оптимизация последовательной переадресации данных)	Включить, чтобы оптимизировать последовательную переадресацию данных, что означает присвоение высшего приоритета последовательной переадресации данных при выделении полосы. Активация последовательной переадресации данных требует указания номера локального порта для управления. Поэтому необходимо определить номер локального порта маршрутизатора, даже если он работает в качестве TCP клиента.	Disable (отключено)
Optimize for ICMP (Оптимизировать для ICMP)	Активировать, чтобы оптимизировать для ICMP, что означает наибольший приоритет для ICMP при выделении полосы. После включения интервал ответа управления эхо-тестированием будет короче. *Если пользователь включает щелчком Optimize for TCP Flags, Optimize for Serial Data Forwarding и Optimize for ICMP одновременно (эти три службы находятся на одном уровне приоритета), маршрутизатор автоматически запустит алгоритм SFQ (Stochastic Fairness Queueing) для удовлетворительного выделения полосы пропускания, если она полностью занята одной службой.*	Disable (отключено)
MAC Address @ QoS MAC Control List (Управляющий список MAC для QoS)	Ввести MAC-адрес пользователя (например, ПК), для которого требуется назначить управление QoS. Маршрутизатор поддерживает до 20 наборов пользователей с управлением QoS по MAC. Приоритет управления QoS по MAC выше, чем по IP.	Null
Priority @ QoS MAC Control List (Приоритет для управляющего списка MAC для QoS)	Выбрать приоритет пользователя (например, ПК), для которого требуется назначить управление QoS. Exempt (привилегированный): — самый высокий приоритет, который гарантирует минимум 50% и максимум 100% скорости загрузки (Downlink Speed) маршрутизатора. Premium (первоочередной): гарантирует минимум 25% и максимум 100% Downlink Speed. Express (срочный): гарантирует минимум 15% и максимум 100% Downlink Speed. Normal (обычный): гарантирует минимум 10% и максимум 100% Downlink Speed. Bulk (массовый): гарантирует минимум 1% и максимум 100% Downlink Speed.	Exempt

QoS		
IP Address @ QoS IP Control List (IP-адрес управляющего списка IP QoS)	Ввести IP-адрес пользователя (например, ПК), для которого требуется назначить управление QoS. Маршрутизатор поддерживает до 20 пользовательских наборов с управлением QoS по IP. Если необходимо управлять одним сегментом сети, IP Address (IP-адрес) можно установить в формате x.x.x.x/24 или x.x.x.x/255.255.255.0. Например, для контроля сегмента 172.16. x.x в поле IP Address можно установить 172.16.0.0/16 или 172.16.0.0/255.255.0.0.	Null
Priority @ QoS IP Control List (Приоритет в управляющем списке IP QoS)	Выбрать приоритет пользователя (например, ПК), для которого требуется назначить управление QoS. Exempt (привилегированный) — самый высокий приоритет, который гарантирует минимум 50% и максимум 100% Downlink Speed маршрутизатора. Premium (первоочередной): гарантирует минимум 25% и максимум 100% Downlink Speed. Express (срочный): гарантирует минимум 15% и максимум 100% Downlink Speed. Normal (обычный): гарантирует минимум 10% и максимум 100% Downlink Speed. Bulk (массовый): гарантирует минимум 1% и максимум 100% Downlink Speed.	Exempt (привилегиро-ванный)
Service Name @ QoS Service Control List (Имя службы для управляющего списка службы QoS)	Задать имя сервера службы, для которой требуется установить управление QoS. Маршрутизатор поддерживает до 20 пользовательских наборов служб с управлением QoS. Приоритет службы управления QoS выше, чем управление по IP и MAC.	Null
Protocol @ QoS Service Control List (Протокол для управляющего списка службы QoS)	Выбор из TCP, UDP и TCP&UDP.	TCP
Port @ Service Control List (Порт для управляющего списка службы)	Ввести номер порта службы, для которой требуется управление QoS.	Null

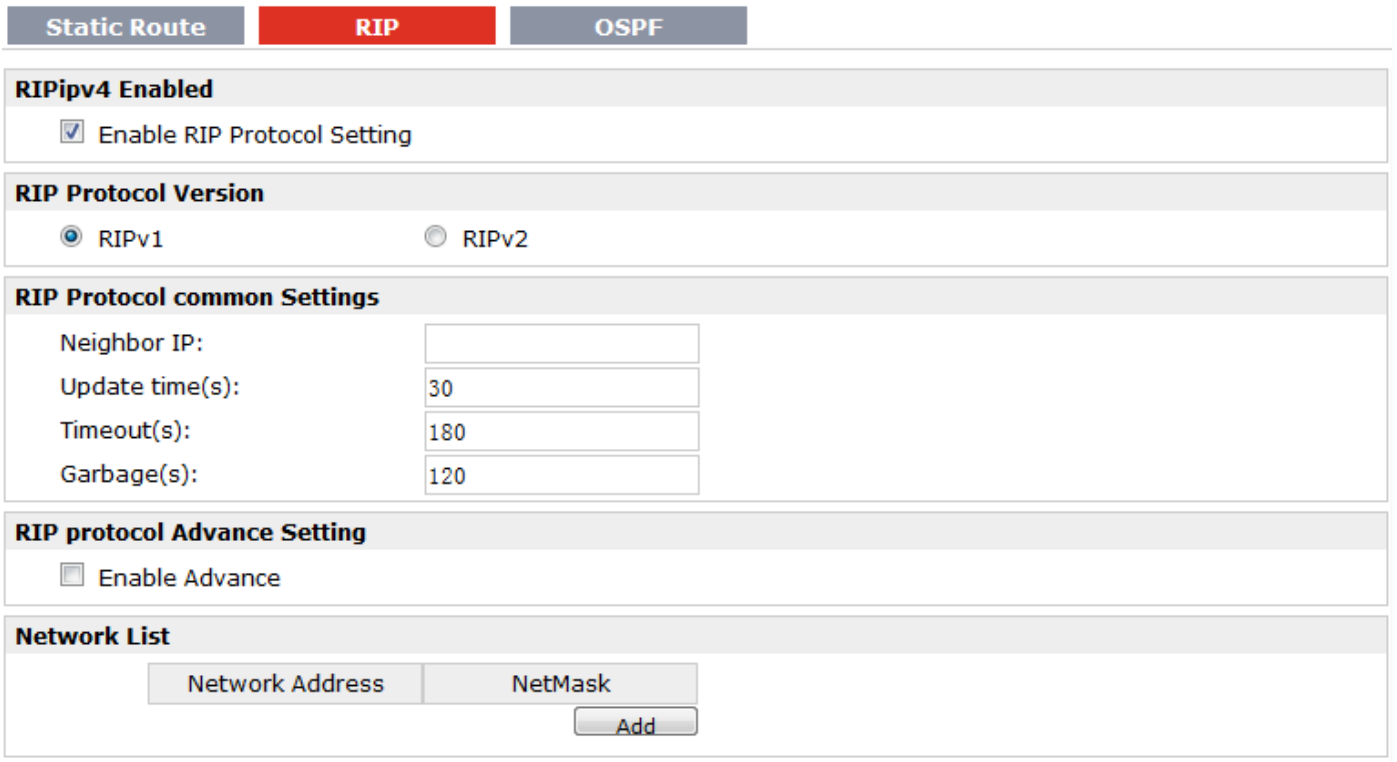
QoS		
Priority @ QoS Service Control List (Приоритет для управляющего списка службы QoS)	Выбор из Exempt, Premium, Express, Normal и Bulk. Выбрать приоритет службы, для которой требуется задать управление QoS. Exempt (привилегированный): — самый высокий приоритет, который гарантирует минимум 50% и максимум 100% скорость загрузки (Downlink Speed) маршрутизатора. Premium (первоочередной): гарантирует минимум 25% и максимум 100% Downlink Speed. Express (срочный): гарантирует минимум 15% и максимум 100% Downlink Speed. Normal (обычный): гарантирует минимум 10% и максимум 100% Downlink Speed. Bulk (массовый): гарантирует минимум 1% и максимум 100% Downlink Speed.	Exempt (привилеги-рованный)
***Примечание**: если службы получают одинаковый уровень приоритета, маршрутизатор автоматически запустит стратегию SFQ (простая реализация семейства алгоритмов справедливой очередизации) для удовлетворительного выделения полосы пропускания.*		

3.21 Configuration -> IP Routing (Конфигурация-> IP маршрутизация)

Этот раздел позволяет настроить параметры IP маршрутизации.



Static Route @ IP Routing (Статическая маршрутизация для IP маршрутизации)		
Элемент	Описание	По умолчанию
Static Route Table (Таблица статических маршрутов)	Позволяет вручную добавлять, удалять или изменять правила статических маршрутов.	Null
Interface (Интерфейс)	Выбор из WAN, LAN_0 или LAN_1.	WAN
Destination (Целевой адрес)	Ввести IP-адрес целевого хоста или целевой сети.	Null
NetMask (Маска подсети)	Ввести маску подсети целевого узла или сети.	Null
Gateway (Шлюз)	Ввести IP-адрес шлюза данного правила статического маршрута. Маршрутизатор будет ретранслировать все данные, соответствующие по месту назначения и маске подсети на этот шлюз.	Null



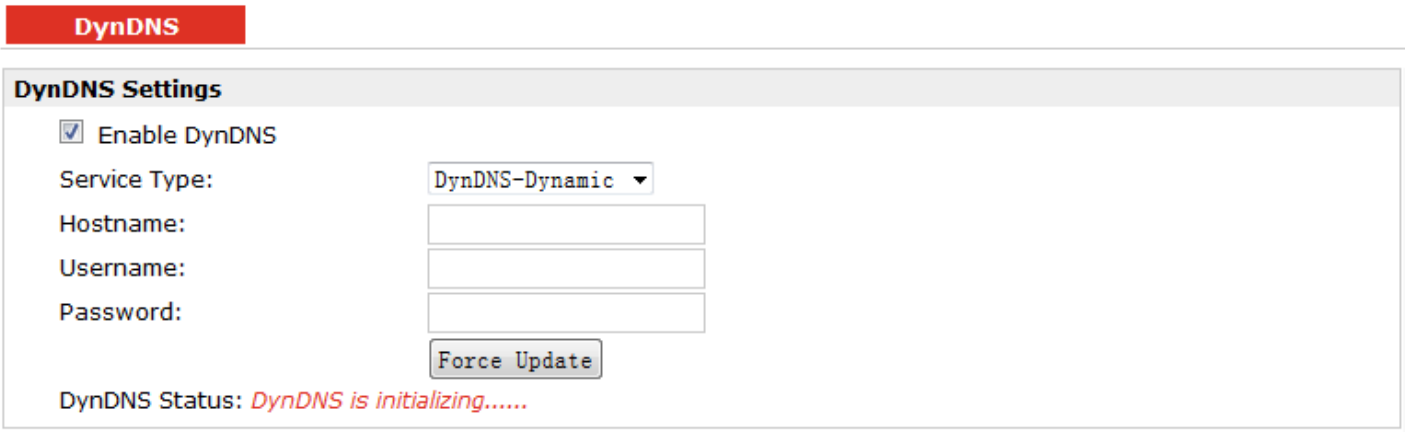
RIP @ IP Routing (Динамическая RIP маршрутизация)		
Элемент	Описание	По умолчанию
RIP (Протокол маршрутизации)	RIP (Протокол маршрутизации) является дистанционно-векторным протоколом маршрутизации, оперирующим HYPERLINK "http://en.wikipedia.org/wiki/Hopcount" \h хопами в качестве метрики маршрутизации. RIP предотвращает возникновение маршрутных петель, вводя максимальное количество переходов, разрешенных на маршруте от отправителя до места назначения.	Null
Enable RIP Protocol Setting (Разрешить протокол RIP)	Установить отметку, чтобы включить функцию RIP.	Disable (отключено)
RIP Protocol Version (Версия RIP протокола)	Выбор из RIPv1 и RIPv2.	RIPv1
Neighbor IP (IP соседнего узла)	Если ввести IP соседнего узла, маршрутизатор будет направлять сообщения-запросы RIP только на этот IP. Этот элемент необходимо задавать только в некоторых одноадресных сетях.	0.0.0.0
Update times (Время обновления)	Определяет интервал обновления маршрутов	30
Timeout (Тайм-аут)	Определяет время существования маршрута. Если не получено обновление для маршрута по истечении времени жизни, метрика маршрута в таблице маршрутизации устанавливается в 16.	180
Garbage (Мусор)	Определяет интервал от установления метрики маршрута 16 до удаления его из таблицы маршрутизации. В течение срока отсчета таймера сборки мусора RIP объявляет маршрут с метрикой, установленной на 16. Если отсутствует извещение об обновлении для этого маршрута после истечения срока отсчета таймера сборки	120

RIP @ IP Routing (Динамическая RIP маршрутизация)		
	мусора, маршрут будет удален из таблицы маршрутизации.	
Enable Advance (Разрешить расширенные настройки)	Установить отметку, чтобы разрешить расширенные настройки протокола RIP.	Disable (отключено)
Default Metric (Метрика по умолчанию)	Это значение используется для перераспределенных маршрутов.	1
Distance (Расстояние)	Это первый критерий, используемый маршрутизатором для определения, какой протокол маршрутизации использовать, когда 2 протокола предоставляют информацию о маршруте для одного места назначения.	120
Passive (Пассивный)	Выбор из: None, Eth0, Eth1 и Default. Эти наборы команд переводят указанный интерфейс в пассивный режим. В интерфейсе пассивного режима все полученные пакеты обрабатываются, как обычные, и информация RIP не отправляется ни в виде многоадресной передачи, ни в качестве одноадресных пакетов, за исключением соседних узлов RIP, определенных соседней командой. Значение по умолчанию должно быть passive для всех интерфейсов.	None
Enable Default Origination (Разрешить исходящую связь по умолчанию)	Разрешить, чтобы маршрутизатор отправлял маршрут по умолчанию другим маршрутизаторам в том же самой AS IGP.	Disable (отключено)
Enable Redistribute Connect (Разрешить перераспределенное подключение)	Перераспределять соединенные маршруты в таблице RIP.	Disable (отключено)
Enable Redistribute Static (Разрешить перераспределение статических)	Перераспределять в RIP таблицах маршрутную информацию о записях статических маршрутов.	Disable (отключено)
Enable Redistribute OSPF (Разрешить перераспределение OSPF)	Перераспределять маршрутную информацию записей OSPF маршрутов в таблицы RIP.	Disable (отключено)
Network List (Список сетей)	Маршрутизатор будет сообщать RIP информацию в этом списке только соседнему.	Null
Network Address (Сетевой адрес)	Ввести сетевой адрес, к которому Eth0 или Eth 1 будут подключаться непосредственно.	Null
NetMask (Маска подсети)	Ввести маску подсети для сети, к которой Eth0 или Eth 1 будут подключаться непосредственно.	Null

OSPF @ IP Routing (Открытый протокол для динамической IP маршрутизации)		
Элемент	Описание	По умолчанию
OSPF	OSPF (первым выбирается кратчайший путь) является протоколом маршрутизации с выявлением маршрутов по состоянию связи для IP сетей. Он использует алгоритм link state routing (маршрутизация с учётом состояния каналов) и попадает в группу внутренних протоколов, работающих в пределах единой автономной системы (AS).	Null
Enable OSPFv2 (Разрешить OSPFv2)	Установить отметку, чтобы включить функции OSPF.	Disable (отключено)

3.22 Configuration -> DynDNS (Конфигурация-> DynDNS)

Этот раздел позволяет настроить параметры DynDNS.



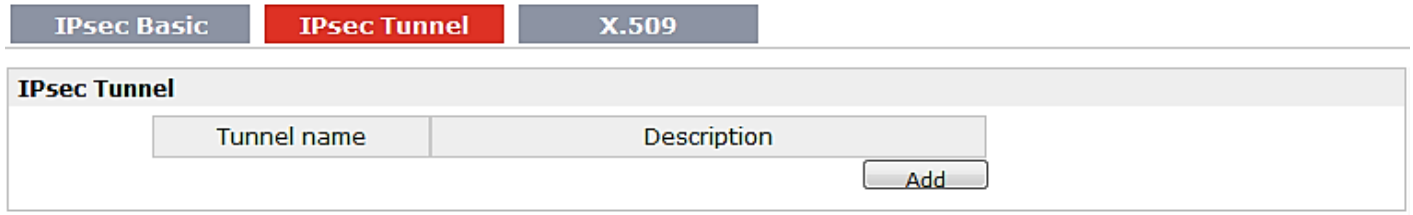
DynDNS		
Элемент	Описание	По умолчанию
DynDNS	Позволяет назначать постоянное доменное имя динамическому IP-адресу, позволяя пользователям, провайдер которых не присваивает им статический IP-адрес, использовать доменное имя. Это особенно полезно для хостинга серверов через пользовательское соединение, так, чтобы любой желающий соединиться с этим пользователем мог использовать его доменное имя вместо необходимости использовать время от времени меняющийся динамический IP-адрес. Этот динамический IP-адрес является IP-адресом WAN маршрутизатора, который присвоен пользователю его сетевым провайдером.	Null
Enable DynDNS	Установить отметку, чтобы включить функцию DynDNS.	Disable

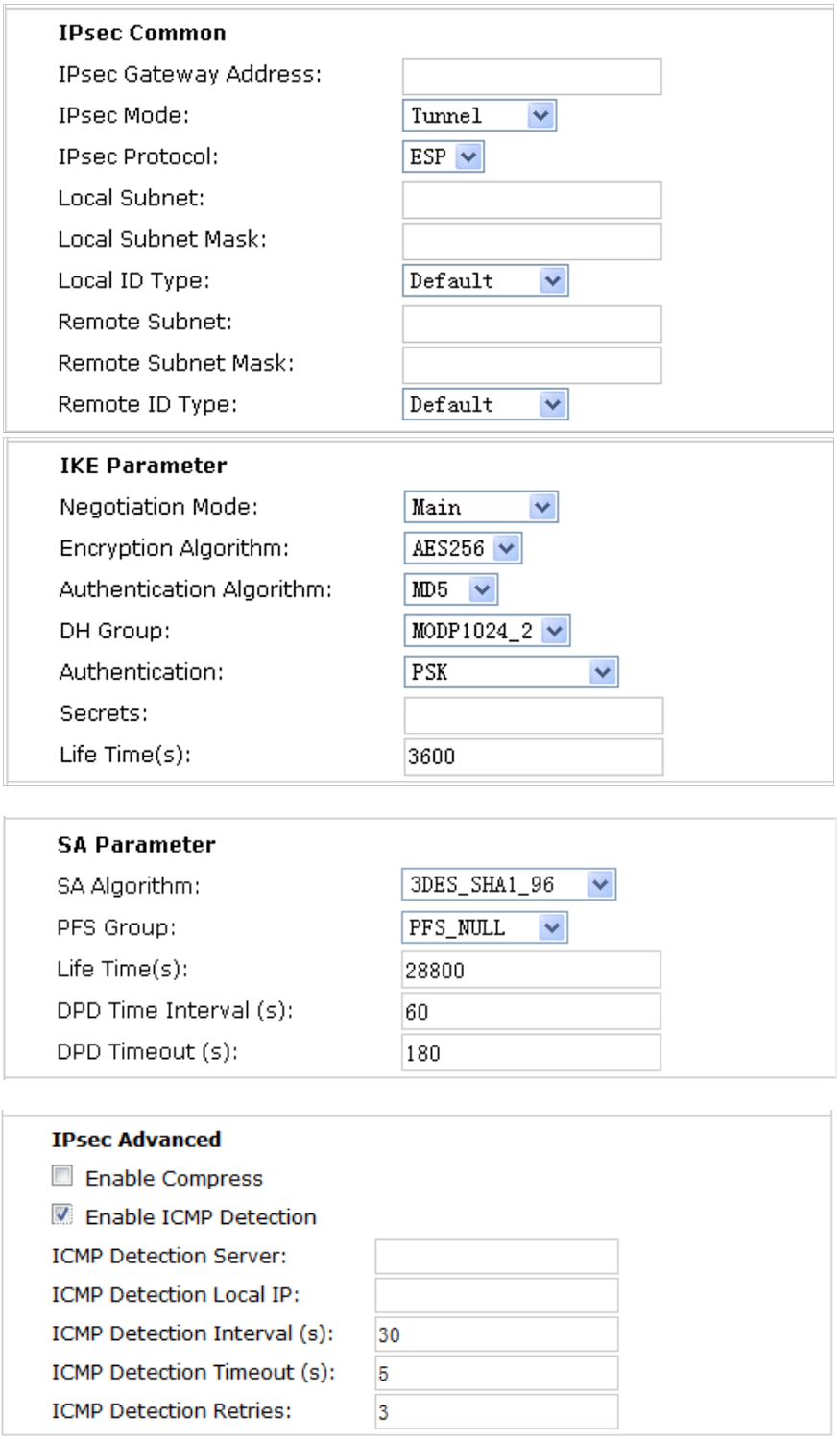
DynDNS		
(Разрешить DynDNS)		(отключено)
Service Type (Тип службы)	Выбрать службу DDNS из DynDNS–Dynamic, QDNS (3322) и NOIP для учетной записи Custom (Пользовательская) может использоваться для соединений пользовательского DDNS сервера.	DynDNS–Dynamic
Hostname (Имя хоста)	Ввести имя хоста имеющегося сервера DDNS.	Null
Username (Имя пользователя)	Ввести имя пользователя имеющегося сервера DDNS.	Null
Password (Пароль)	Ввести пароль имеющегося сервера DDNS.	Null
URL	Ввести адрес для подключения пользовательского сервера DDNS.	Null
Force Update (Обновить)	Щелкнуть для обновления и применения настроек DynDNS.	Null
DynDNS Status (Статус DynDNS)	Отображается текущий статус DynDNS.	Null

3.23 Configuration -> IPSec (Конфигурация-> IPSec)

Этот раздел позволяет настроить параметры IPSec.

IPSec Basic @ IPSec (Основные настройки IPSec)		
Элемент	Описание	По умолчанию
Enable NAT Traversal (Разрешить прохождение NAT)	Установить отметку, чтобы включить прохождение NAT для IPSec. Этот элемент должен быть включен, когда маршрутизатор работает в среде NAT.	Enable (включено)
Keepalive Interval (Интервал проверки активности)	Интервал, через который маршрутизатор отправляет пакеты проверки работоспособности устройству NAT, чтобы предотвратить удаление преобразования (портов) NAT.	30





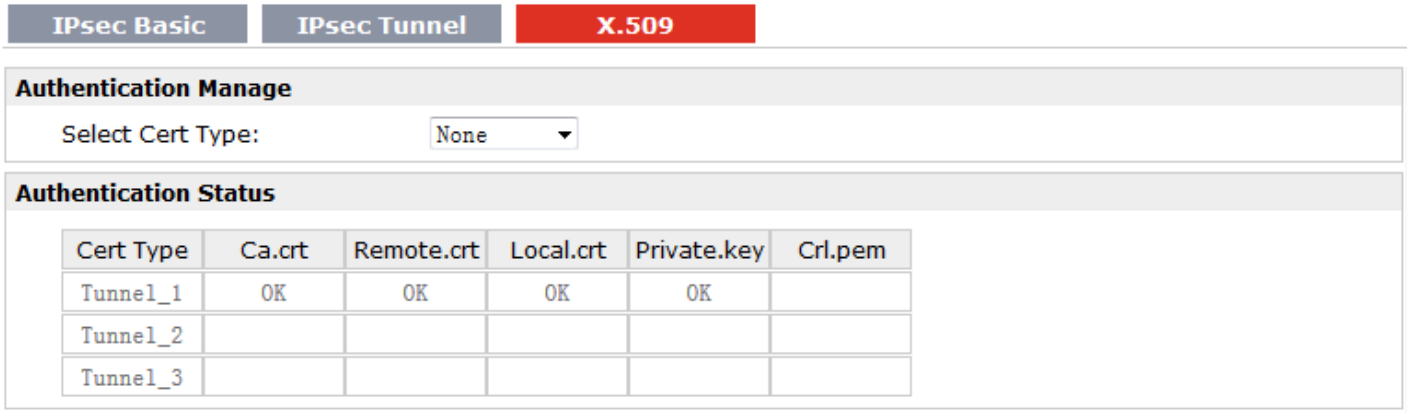
IPSec Tunnel @ IPSec (IPSec Туннель)		
Элемент	Описание	По умолчанию
Add (Добавить)	Щелкнуть Add для добавления нового IPSec туннеля.	Null
Enable (Включить)	Включить туннель. Максимально возможное количество туннелей - 3.	Null
IPSec Gateway Address (Адрес шлюза)	Ввести адрес удаленного сервера VPN IPSec.	Null

IPSec Tunnel @ IPSec (IPSec Туннель)		
IPSec Mode (Режим IPSec)	Выбрать режим из: Tunnel и Transport. Tunnel (Туннель): обычно используется между шлюзами, или между оконечной станцией и шлюзом, шлюз выступает в качестве прокси для узлов позади него. Transport (транспортный): используется между оконечными узлами или между конечным узлом и шлюзом, если шлюз обрабатывается как узел, например, зашифрованный сеанс Telnet от рабочей станции до маршрутизатора, в котором маршрутизатор является фактическим местом назначения.	Tunnel
IPSec Protocol (Протокол IPSec)	Выбрать протоколы системы защиты из ESP и AH. ESP: использовать протокол ESP. AH: использовать протокол AH.	ESP
Local Subnet (Локальная подсеть)	Введите адрес защищенной IPSec локальной подсети.	0.0.0.0
Local Subnet Mask (Маска локальной подсети)	Ввести маску защищенной IPSec локальной подсети.	0.0.0.0
Local ID Type (Тип локального ID)	Выбрать из IP Address, FQDN и User FQDN (для согласования IKE). По умолчанию — IP Address. IP Address (IP-адрес): использовать IP-адрес в качестве ID для согласования IKE. FQDN: Использовать тип FQDN в качестве ID для согласования IKE. Если выбрана эта опция, ввести имя шлюза локальной защиты без знаков в кружке (@), например, test.robustel.com. User FQDN: использовать пользовательский тип FQDN в качестве ID для согласования IKE. Если выбрана эта опция, ввести именную последовательность для локального шлюза защиты со знаком в кружке (@), например, test@robustel.com.	Default (По умолчанию)
Remote Subnet (Удаленная подсеть)	Ввести адрес удаленной защищенной IPSec подсети.	0.0.0.0
Remote Subnet Mask (Маска удаленной подсети)	Ввести маску удаленной защищенной IPSec подсети.	0.0.0.0
Remote ID Type (Тип удаленного ID)	Выбрать из IP Address, FQDN и User FQDN (для согласования IKE). IP Address (IP-адрес): использовать IP-адрес в качестве ID для согласования IKE. FQDN: Использовать тип FQDN в качестве ID для согласования IKE. Если выбрана данная опция, следует ввести имя без символов (@) для шлюза локальной защиты, например, test.robustel.com. User FQDN: использовать пользовательский тип FQDN в качестве ID для согласования IKE. Если выбрана эта опция, ввести именную последовательность для локального шлюза защиты со знаком в кружке (@), например, test@robustel.com.	Default (По умолчанию)
Negotiation Mode (Режим согласования)	Выбрать из Main и Aggressive (для режима согласования IKE в фазе 1). Если IP-адрес одного конца туннеля IPSec получен динамически,	Main

IPSec Tunnel @ IPSec (IPSec Туннель)		
	режим согласования IKE должен быть Aggressive (агрессивный). В этом случае SA могут быть установлены, пока корректны имя пользователя и пароль.	
Encryption Algorithm (Алгоритм шифрования)	Выбрать из DES, 3DES, AES128, AES192 и AES256, для использования при согласовании IKE. DES: использовать алгоритм DES в режиме CBC и 56-разрядный ключ. 3DES: использовать алгоритм 3DES в режиме CBC и 168-разрядный ключ. AES128: Использовать алгоритм AES в режиме CBC и 128-разрядный ключ. AES192: Использовать алгоритм AES в режиме CBC и 192-разрядный ключ. AES256: Использовать алгоритм AES в режиме CBC и 256-разрядный ключ.	3DES
Authentication Algorithm (Алгоритм аутентификации)	Выбор из MD5 и SHA1 для использования при согласовании IKE. MD5: использовать HMAC-SHA1. SHA1: использовать HMAC-MD5.	MD5
DH Group (Группа DH)	Выбрать из MODP768_1, MODP1024_2 и MODP1536_5 для использования в фазе 1 согласования ключей. MODP768_1: использовать 768-разрядную группу Diffie-Hellman. MODP1024_2: использовать 1024-разрядную группу Diffie-Hellman. MODP1536_5: Использовать 1536-разрядную группу Diffie-Hellman.	MODP1024_2
Authentication (Аутентификация)	Выбор из PSK, CA, XAUTH Init PSK и XAUTH Init CA, используемых при согласовании IKE. PSK: предварительный ключ. CA: центр сертификации. XAuth: расширенная аутентификация на AAA сервере.	PSK
Secrets (Ключ)	Ввести предварительный ключ.	Null
Life Time @ IKE Parameter (Время жизни параметра IKE)	Установить время жизни для согласования IKE. Прежде, чем SA истекает, IKE согласовывает новую SA. Как только установлена новая SA, она сразу вступает в силу, а старая будет очищена автоматически, когда потеряет силу.	86400
SA Algorithm (Алгоритм SA)	Если в Protocol выбрано ESP, следует выбрать из DES_MD5_96, DES_SHA1_96, 3DES_MD5_96, 3DES_ SHA1_96, AES128_MD5_96, AES128_ SHA1_96, AES192_MD5_96, AES192_ SHA1_96, AES256_MD5_96 и AES256_ SHA1_96. Если в Protocol выбрано AH, следует выбрать из AH_MD5_96 и AH_ SHA1_96. ***Примечание**: более высокая степень безопасности означает более сложную реализацию и меньшую скорость. Чтобы удовлетворить общим требованиям достаточно DES. 3DES следует использовать, когда имеется необходимость высокой конфиденциальности и безопасности.*	3DES_MD5_96

IPSec Tunnel @ IPSec (IPSec Туннель)		
PFS Group (Группа PFS)	Выбор из PFS_NULL, MODP768_1, MODP1024_2 и MODP1536_5. PFS_NULL: отключить группу PFS MODP768_1: использовать 768-разрядную группу Diffie-Hellman. MODP1024_2: использовать 1024-разрядную группу Diffie-Hellman. MODP1536_5: использовать 1536-разрядную группу Diffie-Hellman.	PFS_NULL
Life Time @ SA Parameter (время жизни параметра SA)	Установить время жизни IPSec SA. ***Примечание**: при согласовании установки IPSec SA, IKE использует меньшее между времени жизни, установленным локально и временем жизни, предложенным удаленным узлом.*	28800
DPD Time Interval (Временной интервал DPD)	Задать интервал, после которого инициируется DPD, если от удаленного узла не получены защищенные пакеты IPSec. DPD: обнаружение зависших туннелей. DPD обнаруживает мертвые одноранговые IKE узлы на нерегулярной основе. При отправке пакета IPSec с локального конца, DPD проверяет время, потребовавшееся для получения последнего пакета IPSec от однорангового узла. Если время превышает интервал DPD, узлу отправляется пакет DPD hello. Если локальный конец не получает подтверждения DPD в пределах интервала повторной передачи пакетов DPD, он ретранслирует DPD hello. Если локальный конец все еще не получает подтверждения DPD, после максимального количества попыток повторной передачи, одноранговый узел считается нерабочим, а IKE SA и IPSec SA очищаются на основе IKE SA.	180
DPD Timeout (Тайм-аут DPD)	Установить тайм-аут пакетов DPD.	60
Enable Compress (Разрешить сжатие)	Установить отметку, чтобы разрешить сжатие внутренних заголовков IP пакетов.	отключено
Enable ICMP Detection (Разрешить ICMP)	Щелкнуть, чтобы включить ICMP.	отключено
ICMP Detection Server (Сервер обнаружения ICMP)	Ввести IP-адрес или доменное имя удаленного сервера. Маршрутизатор будет проверять заданный адрес/доменное имя с помощью ping-запросов для подтверждения активности текущей связи.	Null
ICMP Detection Local IP (локальный IP для обнаружения ICMP)	Задать локальный IP-адрес.	Null
ICMP Detection Interval (интервал обнаружения ICMP)	Задать время интервала эхо-тестирования.	30
ICMP Detection Timeout (Время ожидания ICMP проверки подключения)	Настройка времени ожидания эхо-тестирования.	5

IPSec Tunnel @ IPSec (IPSec Туннель)		
ICMP Detection Retries (Повтор ICMP проверки)	Если маршрутизатор непрерывно проверяет эхо-тестированием заданный адрес/доменное имя в течение предварительно установленного времени Max Retries time, он будет пытаться восстановить VPN туннель.	3

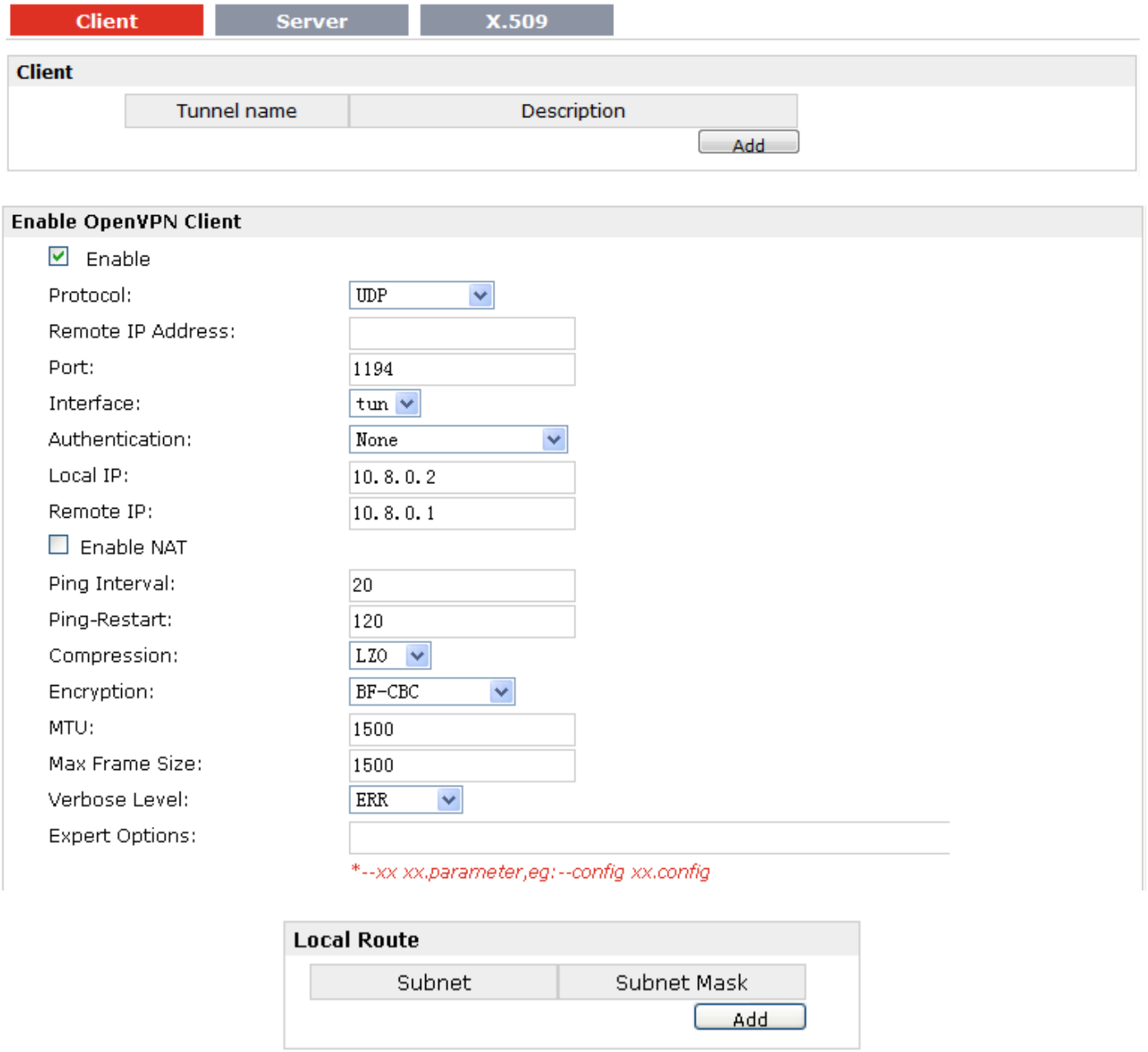


X.509 IPSec		
Элемент	Описание	По умолчанию
Select Cert Type (Выбор типа сертификата)	Выбрать IPSec туннель, для которого будет использован сертификат.	Null
CA	Щелкнуть *Browse*, чтобы выбрать файл CA на локальном ПК, затем щелкнуть *Import*, чтобы импортировать его в маршрутизатор. Для экспорта файла сертификата с маршрутизатора на ПК необходимо щелкнуть *Export*.	Null
Remote Public Key (Удаленный открытый ключ)	Щелкнуть *Browse*, чтобы выбрать корректный файл удаленного открытого ключа на локальном ПК, затем щелкнуть *Import*, для импорта его в маршрутизатор. Для экспорта файла удаленного открытого ключа с маршрутизатора на ПК необходимо щелкнуть *Export*.	Null
Local Public Key (Локальный открытый ключ)	Щелкнуть *Browse*, чтобы выбрать корректный файл локального открытого ключа на локальном ПК, затем *Import*, для импорта его в маршрутизатор. Для экспорта файла локального открытого ключа с маршрутизатора на ПК необходимо щелкнуть *Export*.	Null
Local Private Key (Локальный закрытый ключ)	Щелкнуть *Browse*, чтобы выбрать корректный файл локального закрытого ключа на локальном ПК, затем щелкнуть на *Import*, для импорта его в маршрутизатор. Для экспорта файла локального закрытого ключа с маршрутизатора на ПК необходимо щелкнуть *Export*.	Null
CRL	Щелкнуть *Browse*, чтобы выбрать корректный файл CRL на локальном ПК, затем щелкнуть *Import*, чтобы импортировать его в	Null

X.509 IPSec		
	маршрутизатор. Для экспорта файла CRL с маршрутизатора на ПК необходимо щелкнуть *Export*.	
Authentication Status (Статус аутентификации)	Отображение текущих параметров статуса IPSec.	Null

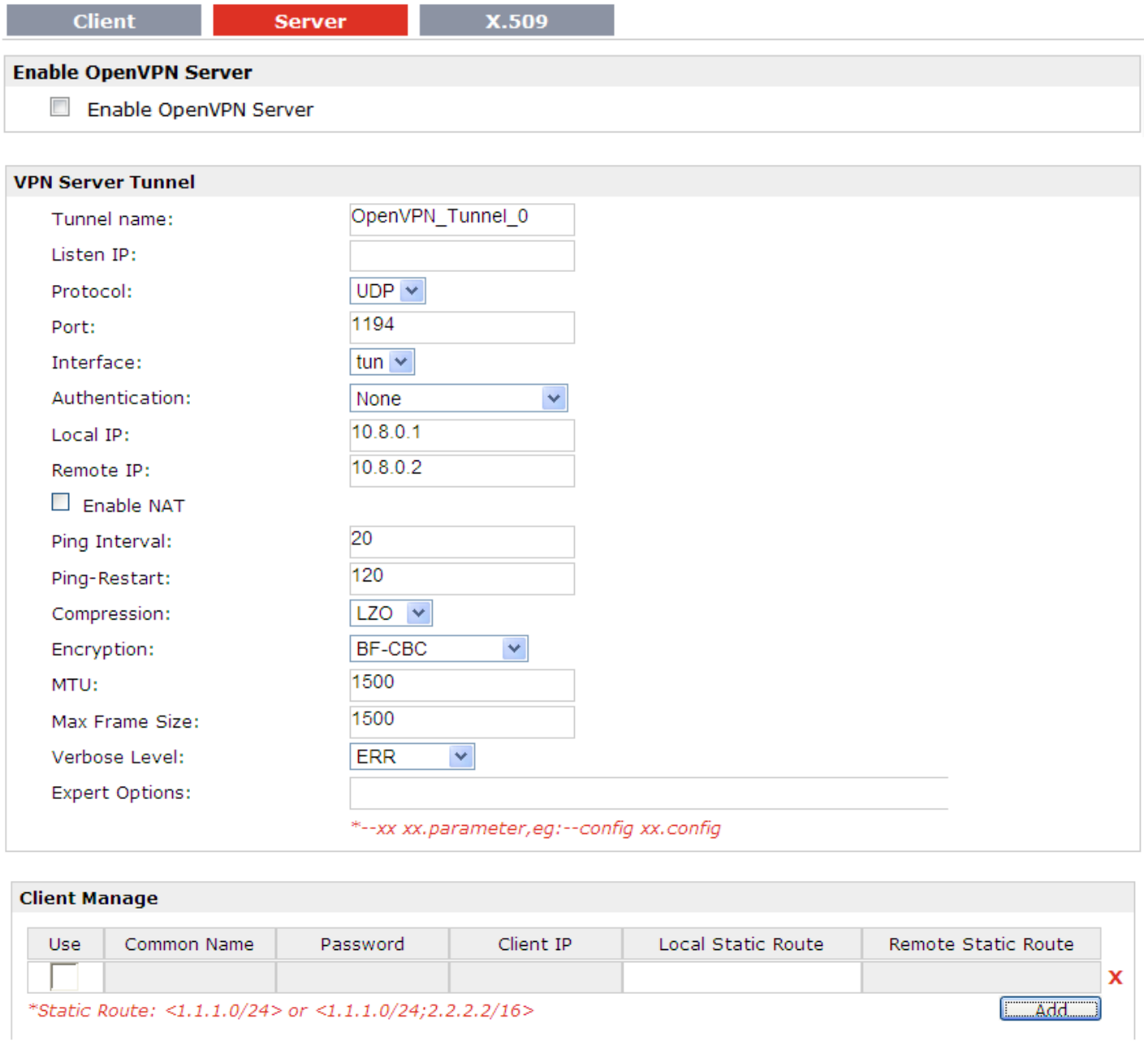
3.24 Configuration -> Open VPN (Конфигурация-> OpenVPN)

Этот раздел позволяет настроить параметры OpenVPN.



Client @ Open VPN (Клиент)		
Элемент	Описание	По умолчанию
Enable (Разрешить)	Разрешить клиент OpenVPN, максимальное количество туннелей - 3.	Null
Protocol (Протокол)	Выбрать из UDP и TCP Client (в зависимости от приложения).	UDP
Remote IP Address (Удаленный IP-адрес)	Ввести удаленный IP-адрес или доменное имя удаленного сервера OpenVPN.	Null
Port (Порт)	Ввести открытый порт удаленного сервера OpenVPN.	1194
Interface (Интерфейс)	Выбрать из tun и tap, которые являются двумя различными типами интерфейса устройств для OpenVPN. Различие этих устройств заключается в том, что tun device является виртуальным двухточечным IP устройством, а tap device является виртуальным Ethernet устройством.	tun
Authentication (Аутентификация)	Выбрать из четырех видов аутентификации: Pre-shared, Username/ Password, X.509 cert и X.509 cert+user.	None
Local IP (Локальный IP-адрес)	Задать локальный IP-адрес туннеля OpenVPN.	10.8.0.2
Remote IP (Удаленный IP-адрес)	Задать удаленный IP-адрес туннеля OpenVPN.	10.8.0.1
Enable NAT (Разрешить NAT)	Установить отметку, чтобы включить SNAT для OpenVPN. Исходный IP-адрес узла позади R3000 будет замаскирован до получения доступа к удаленному серверу OpenVPN.	отключено)
Ping Interval (Интервал эхо-тестирования)	Задать интервал эхо-тестирования для контроля активности туннеля.	20
Ping -Restart (Перезагрузка по ping)	Перезагрузка для установления OpenVPN туннеля если эхо-тестирование постоянно показывает тайм-аут.	120
Compression (Сжатие)	Выбрать LZO, чтобы использовать библиотеку сжатия LZO для сжатия потока данных.	LZO
Encryption (Шифрование)	Выбрать из BF-CBC, DES-CBC, DES-EDE3-CBC, AES128-CBC, AES192-CBC и AES256-CBC. BF-CBC: использует алгоритм BF в режиме CBC и 128-разрядный ключ. DES-CBC: использует алгоритм DES в режиме CBC и 64-разрядный ключ. DES-EDE3-CBC: Использует 3DES алгоритм в режиме CBC и 192-разрядный ключ. AES128-CBC: Использует алгоритм AES в режиме CBC и 128-разрядный ключ. AES192-CBC: Использует алгоритм AES в режиме CBC и 192-разрядный ключ. AES256-CBC: Использует алгоритм AES в режиме CBC и 256-разрядный ключ.	BF-CBC
MTU (Максимальный размер пакета)	Максимальный размер пакета. Это указатель максимального размера передаваемого блока данных, который возможно передать в данных условиях.	1500
Max Frame Size (Максимальный размер кадра)	Задать максимальный размер кадра для передачи.	1500

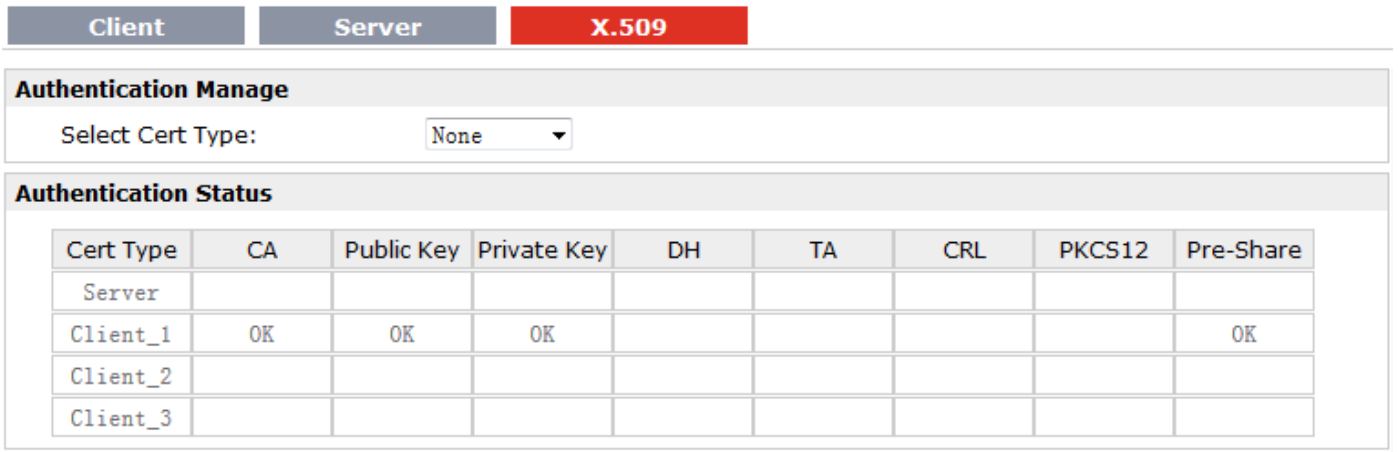
Client @ Open VPN (Клиент)		
Verbose Level (Verbose-уровень)	Выбрать уровень вывода журнала (от меньшего к большему): ERR, WARNING, NOTICE и DEBUG. Более высокий уровень выводит в журнал больше информации.	ERR
Expert Options (Профессиональные настройки)	В это поле можно ввести некоторые дополнительные строки инициализации PPP. Каждая строка может быть отделена пробелом.	Null
Subnet&Subnet Mask@Local Route	Задать подсеть и маску подсети локальной маршрутизации.	Null



Server @ Open VPN (Сервер OpenVPN)		
Элемент	Описание	По умолчанию
Enable OpenVPN Server	Установить отметку, чтобы включить туннель сервера	отключено

Server @ Open VPN (Сервер OpenVPN)		
(Включить туннель OpenVPN сервер)	OpenVPN.	
Tunnel name (Имя туннеля)	Ввести имя туннеля сервера OpenVPN.	Tunnel_OpenVPN_ 0
Listen IP (Прослушивать IP)	Можно ввести IP-адрес сотовой WAN, Ethernet WAN или Ethernet LAN. Нуль или 0.0.0.0 означает использование текущего активного канала WAN, сотовой WAN или Ethernet WAN.	0.0.0.0
Protocol (Протокол)	Выбрать из UDP и TCP Client (в зависимости от приложения).	UDP
Port (Порт)	Задать локальный открытый порт.	1194
Interface (Интерфейс)	Выбрать из tun и tap, которые служат двумя различными типами интерфейса устройств для OpenVPN. Различие этих устройств заключается в том, что tun device является виртуальным двухточечным IP устройством, а tap device является виртуальным Ethernet устройством.	tun
Authentication (Аутентификация)	Выбрать из четырех видов аутентификации: Pre-shared, Username/Password, X.509 cert и X.509 cert+user.	None
Local IP (Локальный IP)	Задать локальный IP-адрес туннеля OpenVPN.	10.8.0.1
Remote IP (Удаленный IP)	Задать удаленный IP-адрес туннеля OpenVPN.	10.8.0.2
Enable NAT (Разрешить NAT)	Установить отметку, чтобы включить SNAT для OpenVPN. Исходный IP-адрес узла позади R3000 будет замаскирован до получения доступа к удаленному клиенту OpenVPN.	Disable (отключено)
Ping Interval (Интервал эхо-тестирования)	Задать интервал эхо-тестирования для контроля активности туннеля.	20
Ping -Restart (Перезагрузка по ping)	Перезагрузка для установления OpenVPN туннеля, если эхо-тестирование постоянно показывает тайм-аут.	120
Compression (Сжатие)	Выбор из None и LZO. Выбрать LZO, чтобы использовать библиотеку сжатия LZO для сжатия потока данных.	LZO
Encryption (Шифрование)	Выбрать из BF-CBC, DES-CBC, DES-EDE3-CBC, AES128-CBC, AES192-CBC и AES256-CBC. BF-CBC: использует алгоритм BF в режиме CBC и 128-разрядный ключ. DES-CBC: использует алгоритм DES в режиме CBC и 64-разрядный ключ. DES-EDE3-CBC: Использует 3DES алгоритм в режиме CBC и 192-разрядный ключ. AES128-CBC: Использует алгоритм AES в режиме CBC и 128-разрядный ключ. AES192-CBC: Использует алгоритм AES в режиме CBC и 192-разрядный ключ. AES256-CBC: Использует алгоритм AES в режиме CBC и 256-разрядный ключ.	BF-CBC
MTU (Максимальный	Максимальный размер пакета. Это указатель максимального	1500

Server @ Open VPN (Сервер OpenVPN)		
размер пакета)	размера передаваемого блока данных, который возможно передать в данных условиях.	
Max Frame Size (Макс. размер кадра)	Задать максимальный размер кадра для передачи.	1500
Verbose Level (Verbose-уровень)	Выбрать уровень вывода журнала (от меньшего к большему): ERR, WARNING, NOTICE и DEBUG. Более высокий уровень выводит в журнал больше информации.	ERR
Expert Options (Профессиональные настройки)	В это поле можно ввести некоторые дополнительные строки инициализации PPP. Каждая строка может быть отделена пробелом.	Null
Client Manage (Управление клиентом)	Щелкнуть *Add* для добавления информации о клиенте OpenVPN, включая Common Name, Password, Client IP, Local Static Route и Remote Static Route. Это поле можно настраивать только после выбора Username/Password в Authentication.	Null



X.509 @ Open VPN		
Элемент	Описание	По умолчанию
Select Cert Type (Выбор типа сертификата)	Выбрать клиента или сервер OpenVPN, для которого будет использован сертификат.	Null
CA	Щелкнуть *Browse*, чтобы выбрать корректный файл CA на локальном ПК, затем щелкнуть *Import*, чтобы импортировать его в маршрутизатор. Для экспорта файла сертификата с маршрутизатора на ПК необходимо щелкнуть *Export*.	Null
Public Key (Открытый ключ)	Щелкнуть *Browse*, чтобы выбрать корректный файл открытого ключа на локальном ПК, затем щелкнуть *Import* для импорта его в маршрутизатор. Для экспорта файла открытого ключа с R3000 на ПК необходимо щелкнуть *Export*.	Null
Private Key (Закрытый ключ)	Щелкнуть *Browse*, чтобы выбрать корректный файл закрытого ключа на локальном ПК, затем щелкнуть на *Import*, для импорта его в маршрутизатор. Для экспорта файла локального закрытого ключа с маршрутизатора на ПК необходимо щелкнуть *Export*.	Null

DH	Щелкнуть *Browse*, чтобы выбрать DH файл на локальном ПК, затем щелкнуть на *Import* для загрузки его в маршрутизатор. Для экспорта DH файла с маршрутизатора на ПК необходимо щелкнуть *Export*.	Null
TA	Щелкнуть *Browse*, чтобы выбрать корректный TA файл на локальном ПК, затем щелкнуть *Import*, чтобы импортировать его в маршрутизатор. Для экспорта TA файла с маршрутизатора на ПК необходимо щелкнуть *Export*.	Null
CRL	Щелкнуть *Browse*, чтобы выбрать корректный файл CRL на локальном ПК, затем щелкнуть *Import*, чтобы импортировать его в маршрутизатор. Для экспорта файла CRL с маршрутизатора на ПК необходимо щелкнуть *Export*.	Null
Pre-Share Static Key (Общий статический ключ)	Щелкнуть *Browse* для выбора общего статического ключа на локальном ПК, затем — щелкнуть *Import* для импорта его в маршрутизатор. Для экспорта файла общего статического ключа с маршрутизатора на ПК необходимо щелкнуть *Export*.	Null

3.25 Configuration -> GRE (Конфигурация-> GRE)

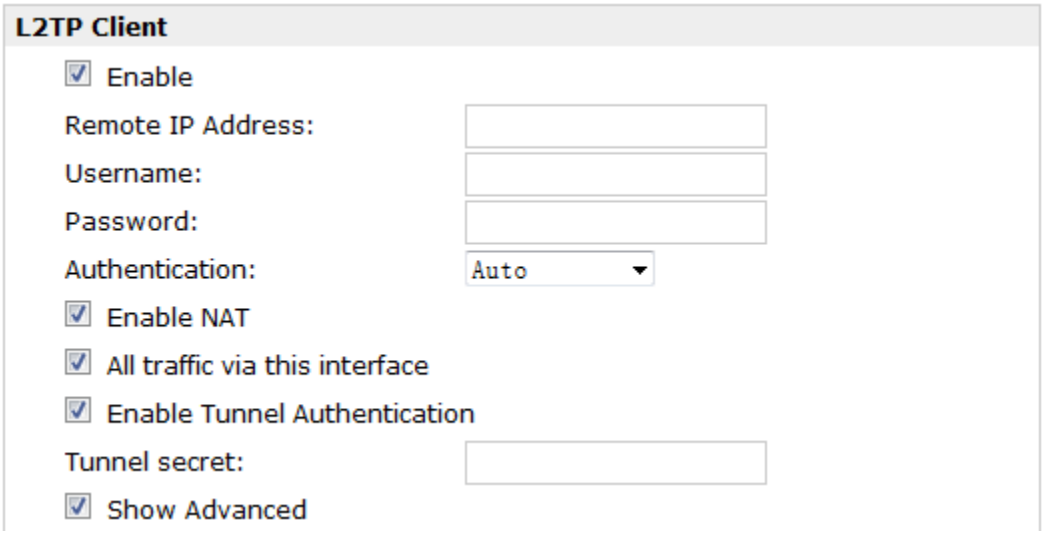
Этот раздел позволяет настроить параметры GRE туннеля (общая инкапсуляция маршрутов).

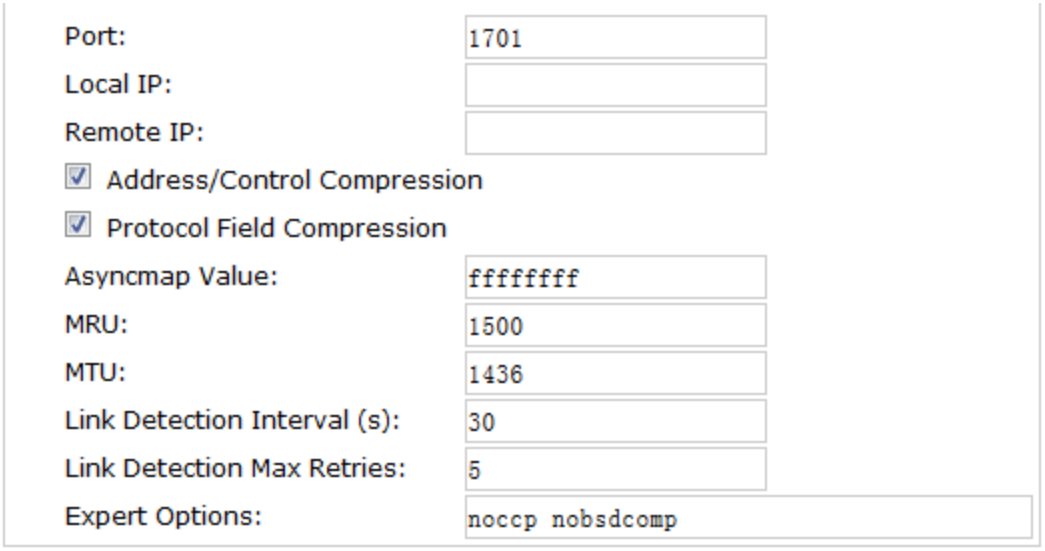
GRE		
Элемент	Описание	По умолчанию
Add (Добавить)	Щелкнуть на Add для добавления GRE туннеля.	
Enable (Разрешить)	Щелкнуть, чтобы разрешить GRE. GRE - это протокол инкапсуляции пакетов с целью передачи иных протоколов в IP сетях.	отключено

GRE		
Remote IP Address (Удаленный IP-адрес)	Задать удаленный IP-адрес виртуального туннеля GRE.	Null
Local Virtual IP (Локальный виртуальный IP)	Задать локальный IP-адрес виртуального туннеля GRE.	Null
Remote virtual IP (Удаленный виртуальный IP)	Задать удаленный IP-адрес виртуального туннеля GRE.	Null
Remote Subnet (Удаленная подсеть)	Добавить статический маршрут к удаленной подсети, чтобы открыть ее для локальной сети.	Null
Remote Subnet Mask (Маска удаленной подсети)	Задать маску удаленной подсети.	Null
All traffic via this interface (Весь трафик через этот интерфейс)	После щелчка, активирующего данную опцию, весь поток данных будет направлен через туннель.	отключено
Enable NAT (Разрешить NAT)	Установить отметку, чтобы включить SNAT для GRE. Исходный IP-адрес узла позади R3000 будет замаскирован до получения доступа к удаленному серверу.	отключено
Secrets (ключи)	Задать ключ GRE туннеля.	Null

3.26 Configuration -> L2TP (Конфигурация-> L2TP)

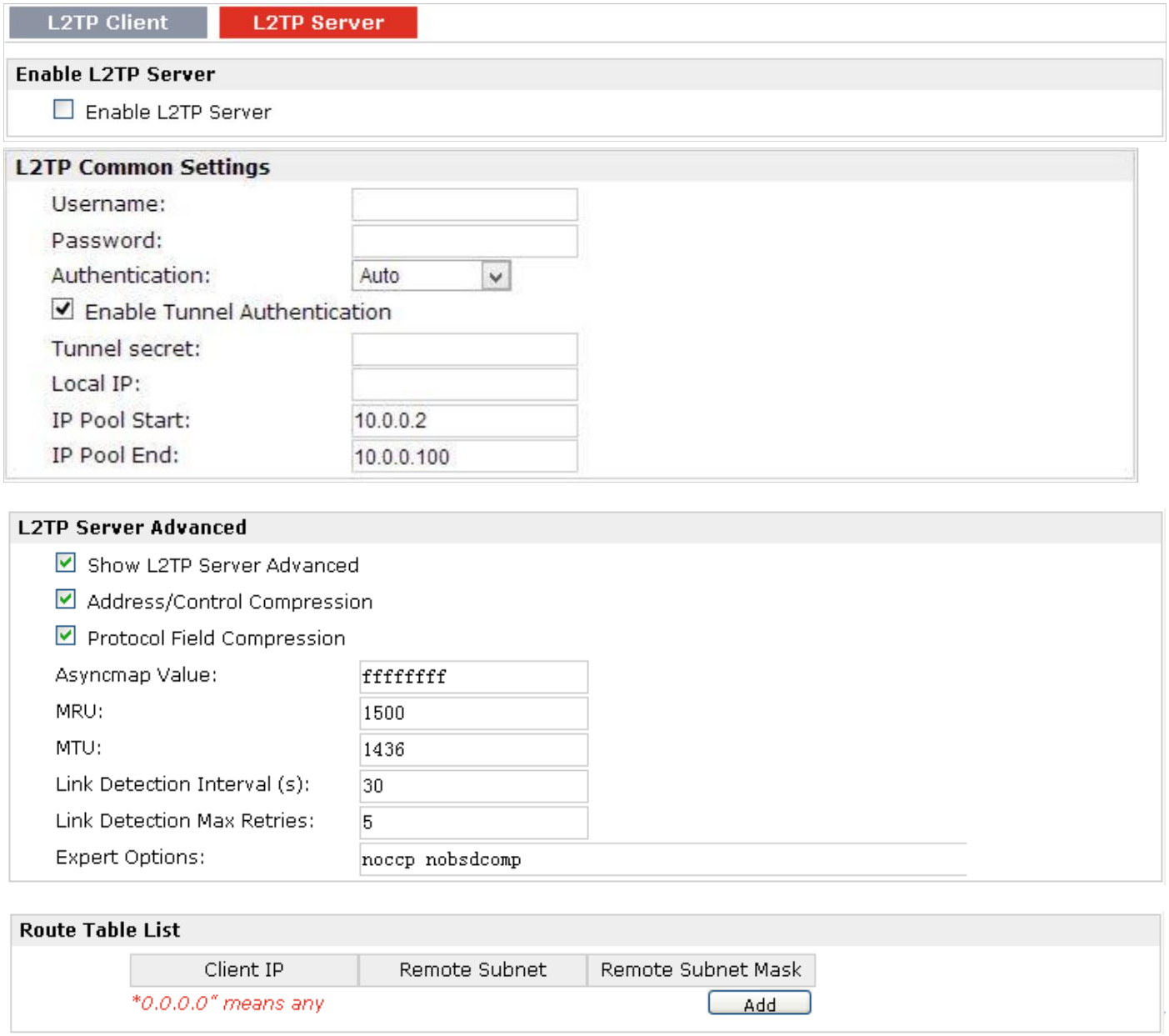
Этот раздел позволяет настроить параметры L2TP.





L2TP Client @ L2TP (L2TP Клиент)		
Элемент	Описание	По умолчанию
Add (Добавить)	Щелкнуть *Add*, чтобы добавить клиента L2TP. Можно добавить до 3 клиентов L2TP.	Null
Remote IP Address (Удаленный IP-адрес)	Ввести общедоступный IP-адрес или доменное имя пользовательского L2TP сервера.	Null
Username (Имя пользователя)	Ввести имя пользователя, предоставленное используемым сервером L2TP.	Null
Password (Пароль)	Ввести пароль, предоставленный используемым сервером L2TP.	Null
Authentication (Аутентификация)	Выбрать из: Auto, PAP, CHAP, MS-CHAP v1 и MS-CHAP v2. Необходимо выбрать соответствующий метод аутентификации, основанный на методе аутентификации сервера. В случае выбора Auto, маршрутизатор будет автоматически выбирать корректный метод в зависимости от сервера.	Disable (отключено)
Remote Subnet (Удаленная подсеть)	Ввести адрес удаленной защищенной L2TP подсети.	Null
Remote Subnet Mask (Маска удаленной подсети)	Ввести маску удаленной защищенной L2TP подсети.	Null
Enable NAT (Разрешить NAT)	Щелкнуть, чтобы активировать функцию NAT L2TP. Исходный IP-адрес узла позади R3000 будет замаскирован до получения доступа к удаленному серверу L2TP.	Disable (отключено)
All traffic via this interface (Весь трафик через этот интерфейс)	После щелчка, активирующего данную опцию, весь поток данных будет направлен через туннель L2TP.	Disable (отключено)
Enable Tunnel Authentication (Включить аутентификацию)	Установить отметку, чтобы включить аутентификацию и ввести секретный ключ для туннеля, предоставляемый L2TP сервером.	Disable (отключено)

L2TP Client @ L2TP (L2TP Клиент)		
Tunnel Secret (ключ туннеля)	В этот элемент следует ввести «секретный» ключ L2TP туннеля.	Null
Show Advanced (Отобразить расширенные настройки)	Установить отметку, чтобы включить расширенные настройки L2TP.	Disable (отключено)
Port (Порт)	Задать номер порта клиента L2TP.	Null
Local IP (Локальный IP-адрес)	Задать IP-адрес клиента L2TP. Можно ввести IP-адрес, присвоенный сервером L2TP. Нуль означает, что клиент L2TP получит IP-адрес автоматически из пула IP сервера L2TP.	Null
Remote IP (Удаленный IP-адрес)	Ввести внутренний IP-адрес удаленного одноранговового узла или адрес шлюза удаленной подсети.	Null
Address/Control Compression (Сжатие адресной/управля-ющей информации)	Используется для инициализации PPP. В большинстве случаев необходимо выбирать enable (включено), как и установлено по умолчанию.	Enable (Разрешить)
Protocol Field Compression (Сжатие поля протокола)	Используется для инициализации PPP. В большинстве случаев необходимо выбирать enable (включено), как и установлено по умолчанию.	Enable (Разрешить)
Asyncmap Value (Значение Asyncmap)	Одна из строк инициализации L2TP. Чаще всего изменять это значение не требуется.	ffffffff
MRU (Максимальный размер принимаемого блока данных)	Максимальный размер принимаемого блока данных. Это указатель максимального размера блока данных, который возможно принять в данных условиях.	1500
MTU (Максимальный размер пакета)	Максимальный размер пакета. Это указатель максимального размера передаваемого блока данных, который возможно передать в данных условиях.	1436
Link Detection Interval (Интервал определения соединения)	Определяет интервал обнаружения соединения между клиентом и сервером L2TP. Чтобы проверить связь в туннеле, клиент и сервер регулярно отправляют друг другу эхо-запрос PPP. Если клиент или сервер не получает ответа от другой стороны в пределах установленного времени, он повторяет запрос. Если ответ не получен после максимального количества повторов передачи эхо-запроса PPP, считается, что туннель L2TP нерабочий, и предпринимается попытка восстановить туннель.	30
Link Detection Max Retries (Максимальное количество повторов определения соединения)	Определяет максимальное количество повторов определения L2TP соединения.	5
Expert Options (Профессиональные настройки)	В это поле можно ввести некоторые дополнительные строки инициализации PPP. Каждая строка может быть отделена пробелом.	noccp nobsdcomp



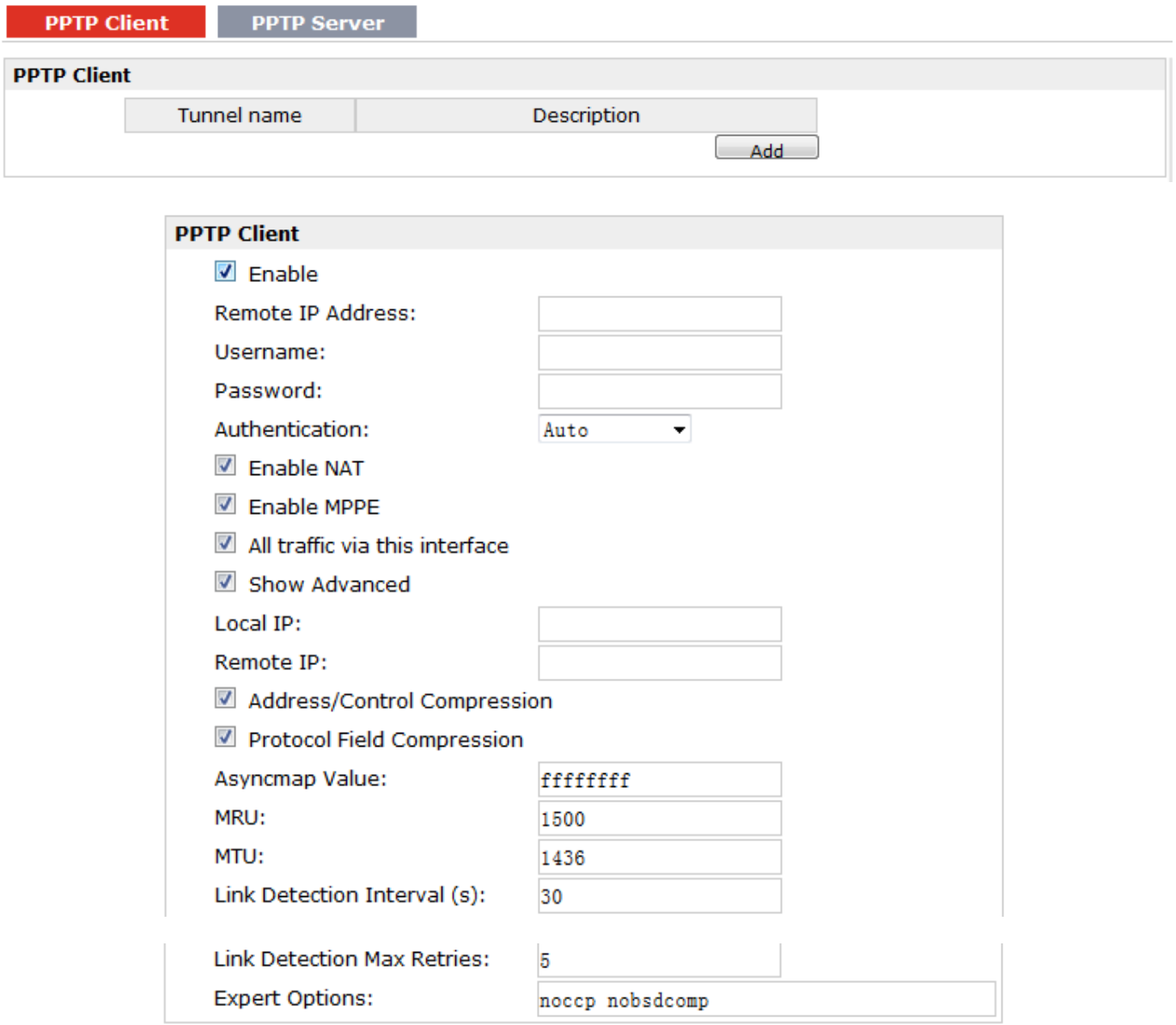
L2TP сервер		
Элемент	Описание	По умолчанию
Enable L2TP Server (Включить L2TP сервер)	Установить отметку, чтобы включить L2TP сервер.	Disable (отключено)
Username (Имя пользователя)	Задать имя пользователя, которое будет присвоено клиенту L2TP.	Null
Password (Пароль)	Задать пароль, который будет присвоен клиенту L2TP.	Null
Authentication (Аутентификация)	Выбор из PAP, CHAP, MS-CHAP v1 и MS-CHAP v2. Клиент L2TP должен выбирать тот же метод аутентификации, что и сервер.	CHAP
Enable Tunnel Authentication (Разрешить аутентификацию	Установить отметку, чтобы включить аутентификацию для туннеля и ввести секретный ключ для туннеля, который будет предоставлен клиенту L2TP.	Disable (отключено)

L2TP сервер		
туннеля)		
Local IP (Локальный IP-адрес)	Задать IP-адрес L2TP сервера.	10.0.0.1
IP Pool Start (Начальный IP пула)	Задать начальный IP-адрес пула для присвоения клиентам L2TP.	10.0.0.2
IP Pool End (Конечный IP адрес пула)	Задать конечный IP-адрес пула для присвоения клиентам L2TP.	10.0.0.100
Show L2TP Server Advanced (Показать дополнительные настройки сервера L2TP)	Установить отметку, чтобы показать дополнительные настройки сервера L2TP	Disable (отключено)
Address/Control Compression (Сжатие адресной или управляющей информации)	Используется для инициализации PPP. В большинстве случаев необходимо выбирать enable (включено), как и установлено по умолчанию.	Enable (Разрешить)
Protocol Field Compression (Сжатие поля протокола)	Используется для инициализации PPP. В большинстве случаев необходимо выбирать enable (включено), как и установлено по умолчанию.	Enable (Разрешить)
Asyncmap Value (Значение Asyncmap)	Одна из строк инициализации L2TP. Чаще всего изменять это значение не требуется.	ffffffff
MRU (Максимальный размер принимаемого блока данных)	Максимальный размер принимаемого блока данных - это указатель максимального размера блока данных, который возможно принять в данных условиях.	1500
MTU (Максимальный размер пакета)	Максимальный размер пакета. Это указатель максимального размера передаваемого блока данных, который возможно передать в данных условиях.	1436
Link Detection Interval (Интервал обнаружения соединения)	Определяет интервал обнаружения соединения между клиентом и сервером L2TP. Чтобы проверить связь в туннеле, клиент и сервер регулярно отправляют друг другу эхо-запрос PPP. Если клиент или сервер не получает ответа от другой стороны в пределах установленного времени, он повторяет запрос. Если ответ не получен после максимального количества повторов передачи эхо-запроса PPP, считается, что туннель L2TP нерабочий, и предпринимается попытка восстановить туннель.	30
Link Detection Max Retries (Макс. количество повторов обнаружения соединения)	Определяет максимальное количество повторов обнаружения L2TP соединения.	5

L2TP сервер		
Expert Options (Профессиональные настройки)	В это поле можно ввести некоторые дополнительные строки инициализации PPP. Каждая строка может быть отделена пробелом.	noccp nobsdcomp
Route Table List (Список таблица маршрутов)	Щелкнуть *Add*, чтобы добавить правило маршрутизации между L2TP сервером и клиентом L2TP.	Null

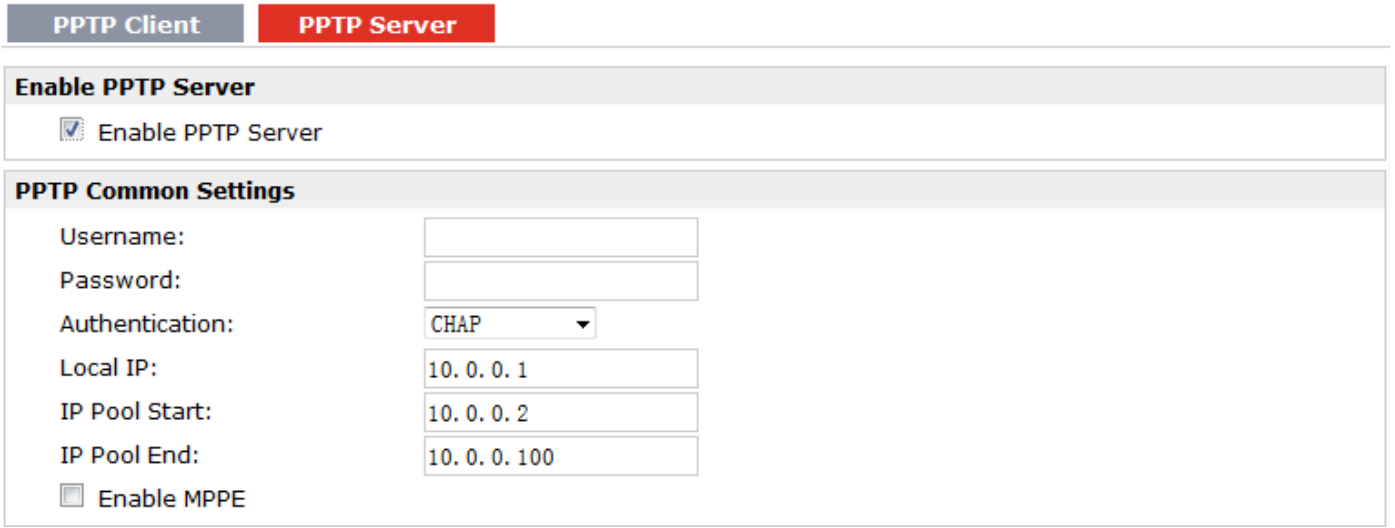
3.27 Configuration -> PPTP (Конфигурация-> PPTP)

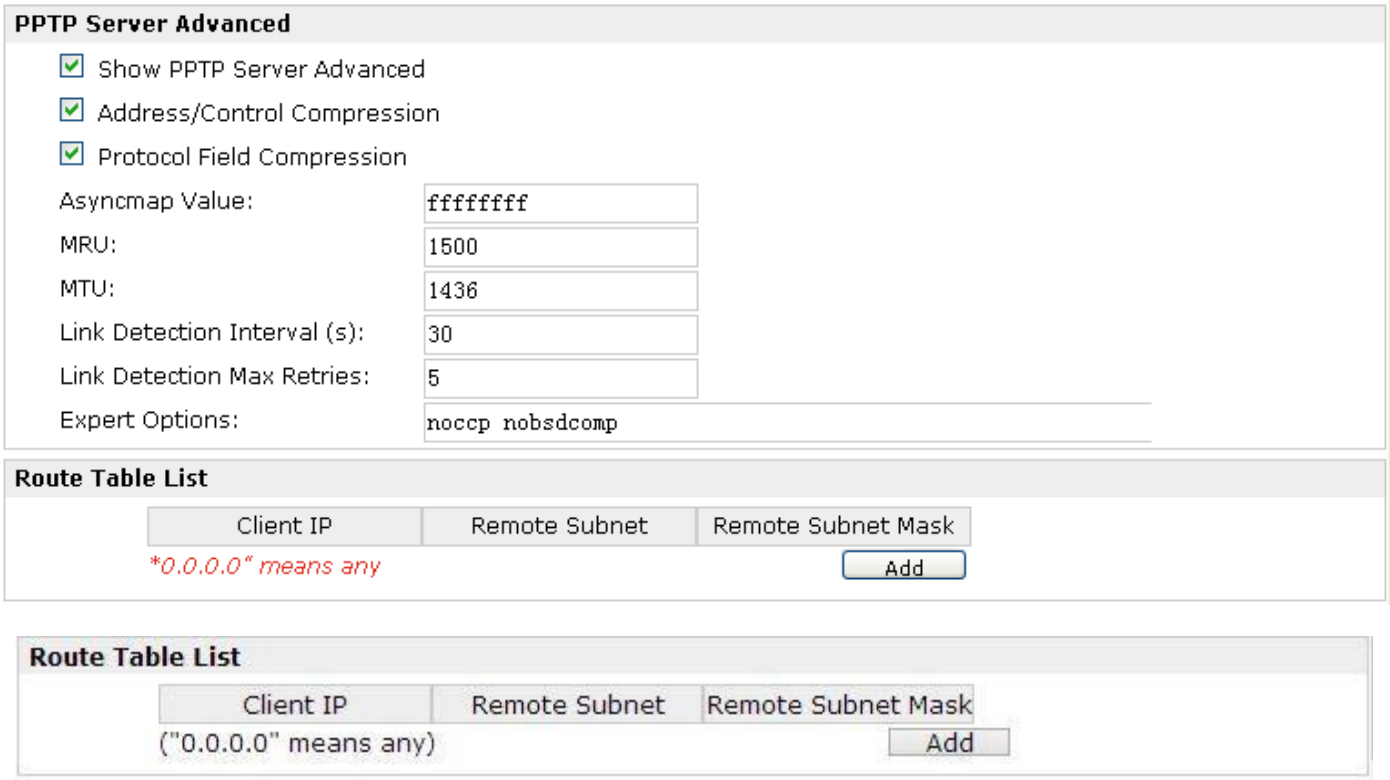
Этот раздел позволяет настроить параметры PPTP.



PPTP Client (PPTP клиент)		
Элемент	Описание	По умолчанию
Add (Добавить)	Щелкнуть на *Add* для добавления клиента PPTP.	
Enable (Включить)	Включить PPTP клиент. Максимальное количество туннелей - 3.	Null
Disable (Отключить)	Отключить PPTP клиент.	Null
Remote IP Address (Удаленный IP-адрес)	Ввести общедоступный IP-адрес или доменное имя используемого PPTP сервера.	Null
Username (Имя пользователя)	Ввести имя пользователя, предоставленное используемым сервером PPTP.	Null
Password (Пароль)	Ввести пароль, предоставленный используемым PPTP сервером.	Null
Authentication (Аутентификация)	выбор из Auto, PAP, CHAP, MS-CHAP v1 и MS-CHAP v2. Необходимо выбрать соответствующий метод аутентификации, основанный на методе аутентификации сервера. В случае выбора Auto, маршрутизатор будет автоматически выбирать корректный метод в зависимости от сервера.	Auto
Enable NAT (Включить NAT)	Щелкнуть, чтобы активировать функцию NAT PPTP. Исходный IP-адрес узла позади R3000 будет замаскирован до получения доступа к удаленному серверу PPTP.	Disable (отключено)
Enable MPPE (Включить MPPE)	Установить отметку, чтобы разрешить MPPE шифрования (Microsoft Point-to-Point Encryption). Это протокол шифрования данных в VPN и PPP соединениях.	Disable (отключено)
All traffic via this interface (Весь трафик через этот интерфейс)	После щелчка, активирующего данную опцию, весь поток данных будет направлен через туннель PPTP.	Disable (отключено)
Show Advanced (Отобразить расширенные настройки)	Установить отметку, чтобы включить расширенные настройки PPTP.	Disable (отключено)
Local IP (Локальный IP-адрес)	Задать IP-адрес клиента PPTP. Можно ввести IP, присвоенный сервером PPTP. Нуль означает, что клиент PPTP получит IP-адрес автоматически из пула IP-адресов сервера PPTP.	Null
Remote IP (Удаленный IP-адрес)	Ввести внутренний IP-адрес удаленного однорангового узла или адрес шлюза удаленной подсети.	Null
Address/Control Compression (Сжатие адресной или управляющей информации)	Используется для инициализации PPP. В большинстве случаев необходимо выбирать enable (включено), как и установлено по умолчанию.	Enable (Разрешить)
Protocol Field Compression (Сжатие поля протокола)	Используется для инициализации PPP. В большинстве случаев необходимо выбирать enable (включено), как и установлено по умолчанию.	Enable (Разрешить)
Asyncmap Value (Значение Asyncmap)	Одна из строк инициализации PPTP. Чаще всего изменять это значение не требуется.	ffffffff

PPTP Client (PPTP клиент)		
MRU (Максимальный размер принимаемого блока данных)	Максимальный размер принимаемого блока данных - это указатель максимального размера блока данных, который возможно принять в данных условиях.	1500
MTU (Максимальный размер пакета)	Максимальный размер пакета - это указатель максимального размера передаваемого блока данных, который возможно передать в данных условиях.	1436
Link Detection Interval (Интервал обнаружения соединения)	Задать интервал обнаружения соединения между клиентом и сервером PPTP. Чтобы проверить связь в туннеле, клиент и сервер регулярно отправляют друг другу эхо-запрос PPP. Если клиент или сервер не получает ответа от другой стороны в пределах установленного времени, он повторяет запрос. Если ответ не получен после максимального количества повторов передачи эхо-запроса PPP, считается, что туннель PPTP нерабочий, и предпринимается попытка восстановить туннель.	30
Link Detection Max Retries (Макс. количество повторов обнаружения соединения)	Определяет максимальное количество повторов обнаружения PPTP соединения.	5
Expert Options (Профессиональные настройки)	В это поле можно ввести некоторые дополнительные строки инициализации PPP. Каждая строка может быть отделена пробелом.	noccp nobsdcomp



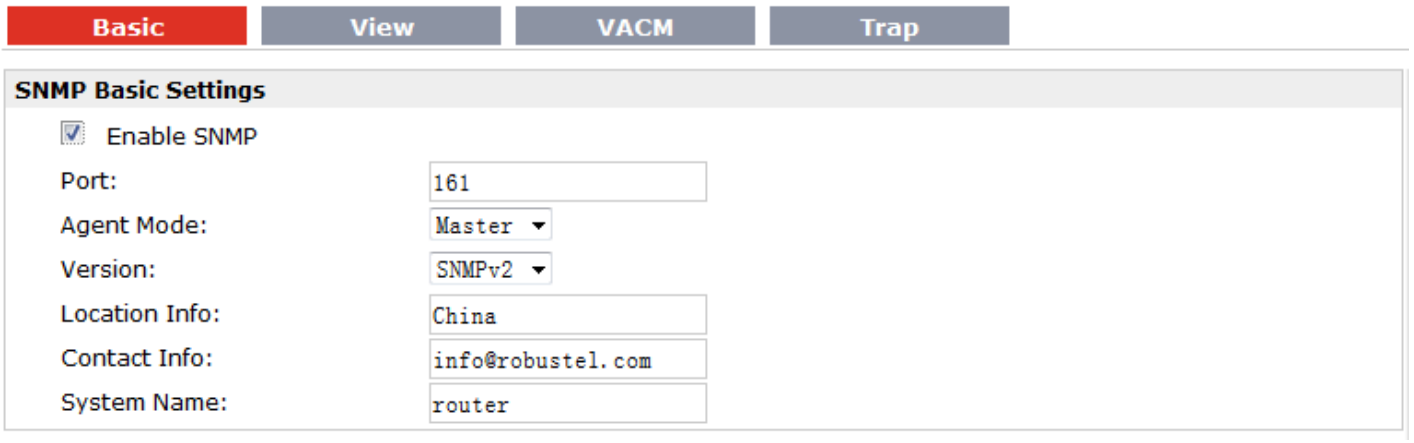


PPTP сервер		
Элемент	Описание	По умолчанию
Enable PPTP Server (Включить сервер PPTP)	Установить отметку, чтобы разрешить PPTP сервер.	Disable (отключено)
Username (Имя пользователя)	Задать имя пользователя, которое будет присвоено клиенту PPTP.	Null
Password (Пароль)	Задать пароль, который будет присвоен клиенту PPTP.	Null
Authentication (Аутентификация)	Выбор из PAP, CHAP, MS-CHAP v1 и MS-CHAP v2. Клиент PPTP должен выбирать тот же метод аутентификации, что и сервер.	CHAP
Local IP (Локальный IP-адрес)	Задать IP-адрес PPTP сервера.	10.0.0.1
IP Pool Start (Начальный IP пул)	Задать начальный IP адрес пула для присвоения клиентам PPTP.	10.0.0.2
IP Pool End (Конечный IP адрес пула)	Задать конечный IP адрес пула для присвоения клиентам PPTP.	10.0.0.100
Enable MPPE (Разрешить MPPE)	Установить отметку, чтобы разрешить MPPE (Microsoft Point-to-Point Encryption). Это - протокол шифрования данных в VPN и PPP соединениях.	Disable (отключено)
Show PPTP Server Advanced (Показать дополнительные настройки сервера PPTP)	Установить отметку, чтобы показать дополнительные настройки сервера PPTP.	Disable (отключено)
Address/Control	Используется для инициализации PPP. В большинстве случаев необходимо выбирать enable (включено), как и установлено по	Enable (включено)

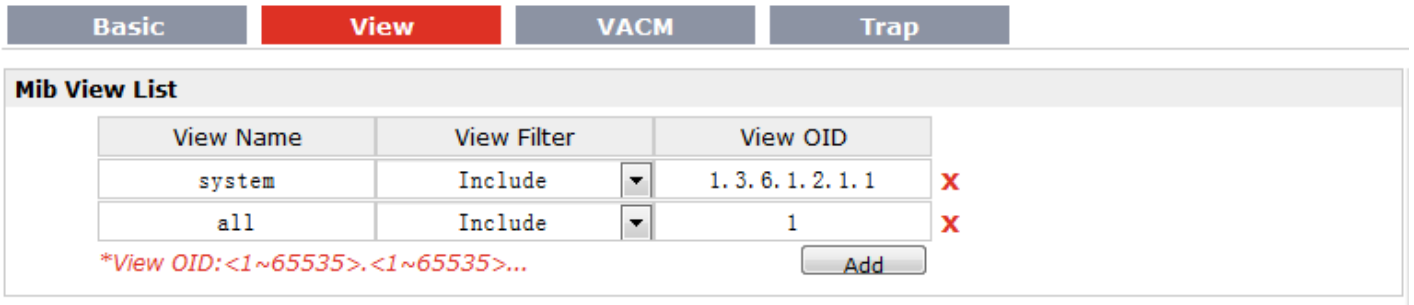
PPTP сервер		
Compression (Сжатие адресной или управляющей информации)	умолчанию.	
Protocol Field Compression (Сжатие поля протокола)	Используется для инициализации PPP. В большинстве случаев необходимо выбирать enable (включено), как и установлено по умолчанию.	Enable (включено)
Asyncmap Value (Значение Asyncmap)	Одна из строк инициализации PPTP. Чаще всего изменять это значение не требуется.	ffffffff
MRU (Максимальный размер принимаемого блока данных)	Максимальный размер принимаемого блока данных - это указатель максимального размера блока данных, который возможно принять в данных условиях.	1500
MTU (Максимальный размер пакета)	Максимальный размер пакета - это указатель максимального размера передаваемого блока данных, который возможно передать в данных условиях.	1436
Link Detection Interval (Интервал обнаружения соединения)	Задать интервал обнаружения соединения между клиентом и сервером PPTP. Чтобы проверить связь в туннеле, клиент и сервер регулярно отправляют друг другу эхо-запрос PPP. Если клиент или сервер не получает ответа от другой стороны в пределах установленного времени, он повторяет запрос. Если ответ не получен после максимального количества повторов передачи эхо-запроса PPP, считается, что туннель PPTP нерабочий, и предпринимается попытка восстановить туннель.	30
Link Detection Max Retries (Максимальное количество повторов обнаружения соединения)	Определяет максимальное количество повторов обнаружения PPTP соединения.	5
Expert Options (Профессиональные настройки)	В это поле можно ввести некоторые дополнительные строки инициализации PPP. Каждая строка может быть отделена пробелом.	noccp nobsdcomp
Route Table List (Список таблица маршрутов)	Щелкнуть *Add*, чтобы добавить правило маршрутизации между PPTP сервером и клиентом PPTP.	Null

3.28 Configuration -> SNMP (Конфигурация-> SNMP)

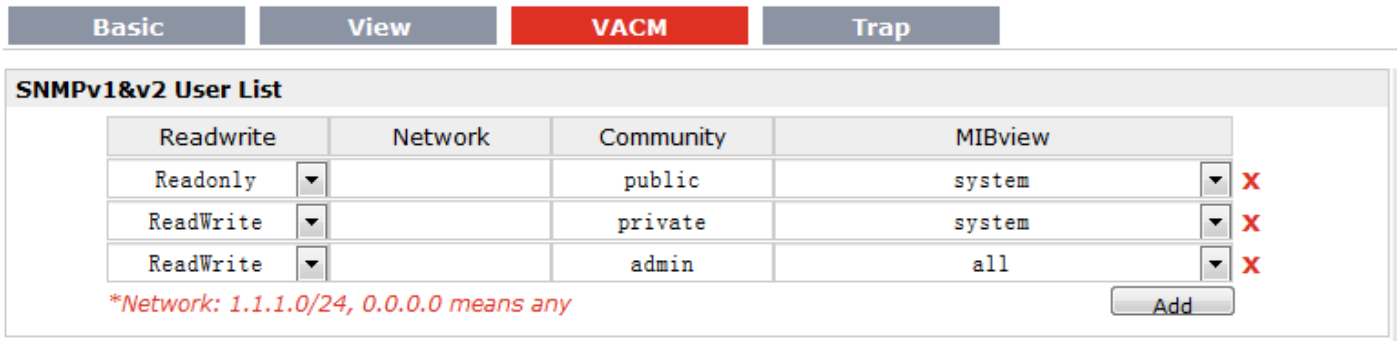
Этот раздел позволяет настроить параметры SNMP.



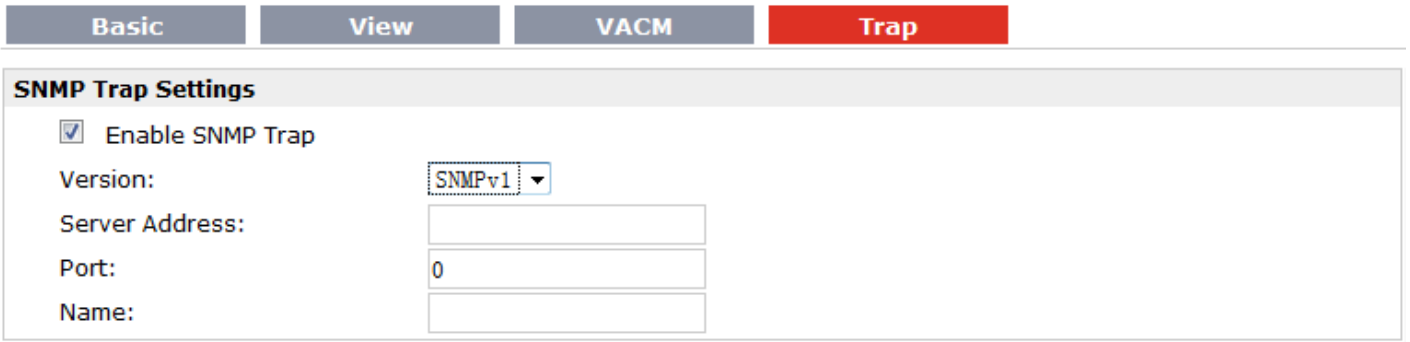
Basic (Основные настройки SNMP)		
Элемент	Описание	По умолчанию
Port (Порт)	Порт UDP для отправки и получения запросов SNMP.	161
Agent Mode (Режим агента)	Выбрать корректный режим агента.	Master
Version (Версия)	Выбор из SNMPv1, SNMPv2 и SNMPv3.	SNMPv2
Location Info (Информация о расположении)	Ввести информацию о местоположении маршрутизатора, которая передается клиенту SNMP.	China (Китай)
Contact Info (Контактная информация)	Ввести контактную информацию, которая передается клиенту SNMP.	info@robustel.com
System name (Системное имя)	Ввести системное имя маршрутизатора, которое передается клиенту SNMP.	router (маршрутизатор)



View @ SNMP (Просмотр SNMP)		
Элемент	Описание	По умолчанию
View Name (Имя)	Ввести имя View.	Null
View Filter (Фильтр)	Выбрать из Include и Exclude (включая/ исключая).	Include
View OID	Ввести идентификаторы объектов	Null



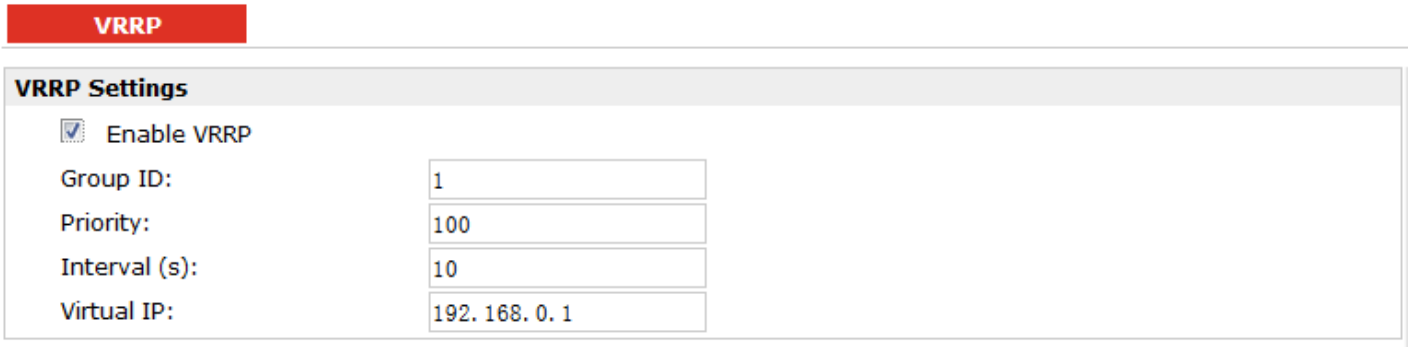
VACM @ SNMP		
Элемент	Описание	По умолчанию
Readwrite (Запись/чтение)	Выбрать права доступа из Readonly и ReadWrite (Только чтение /Чтение-запись).	Readonly
Network (Сеть)	Задать сеть, с которой разрешен доступ. Например, 172.16.0.0.	Null
Community (Сообщество)	Ввести имя сообщества.	Null
MIBview	Выбрать из none, system и all (нет/система/все)	none



Trap @ SNMP		
Элемент	Описание	По умолчанию
Enable SNMP Trap (Разрешить прерывание SNMP)	Щелкнуть, чтобы активировать опцию прерывания SNMP.	Disable (отключено)
Version (Версия)	Выбор из SNMPv1, SNMPv2 и SNMPv3.	SNMPv1
Server Address (адрес сервера)	Ввести IP-адрес сервера SNMP.	Null
Port (Порт)	Ввести номер порта сервера SNMP.	0
Name (Имя)	Ввести имя сервера SNMP.	Null

3.29 Configuration -> VRRP (Конфигурация-> VRRP)

Этот раздел позволяет настроить параметры VRRP.

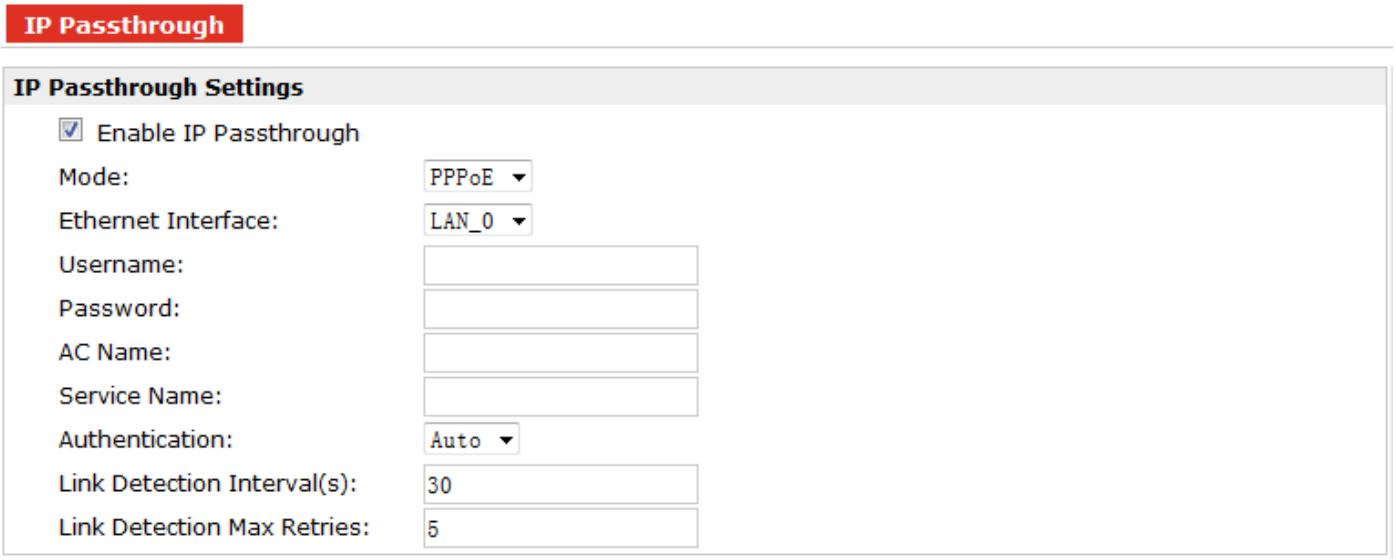


VRRP		
Элемент	Описание	По умолчанию
Enable VRRP (Включить VRRP)	Установить отметку, чтобы включить протокол VRRP.VRRP (Virtual Router Redundancy Protocol) является Интернет протоколом, позволяющим использовать один и более резервный backup-маршрутизатор, в качестве маршрутизатора с постоянной конфигурацией в локальной сети (LAN). VRRP позволяет вручную задать виртуальный IP-адрес.	Disable (отключено)
Group ID (ID группы)	Определяет, к какой VRRP группе принадлежит отдельный маршрутизатор.	1
Priority (Приоритет)	Ввести значение приоритета от 1 до 255. Большее значение означает более высокий приоритет.	100
Interval (Интервал)	Интервал, передачи пакетов проверки работоспособности master-маршрутизатором на backup-маршрутизаторы.	10
Virtual IP (Виртуальный IP)	Виртуальный IP-адрес совместно используется маршрутизаторами, причем один из них определяется как master-маршрутизатор, а другие — как backup-маршрутизаторы. В случае сбоя master, виртуальный IP-адрес передается backup-маршрутизатору вместо его IP-адреса (этот backup-маршрутизатор становится master-маршрутизатором).	192.168.0.1

3.30 Configuration -> IP Passthrough (Конфигурация-> передача IP)

В режиме IP Passthrough R3000 действует как сервер PPPoE, непосредственно передавая свой WAN IP-адрес клиенту PPPoE. Пакеты, полученные с WAN интерфейса, направляются непосредственно на LAN интерфейс. Точно так же пакеты, полученные с LAN интерфейса (все кроме широковещательных/многоадресных), отправляются на WAN интерфейс.

Этот раздел позволяет настроить параметры IP Passthrough.

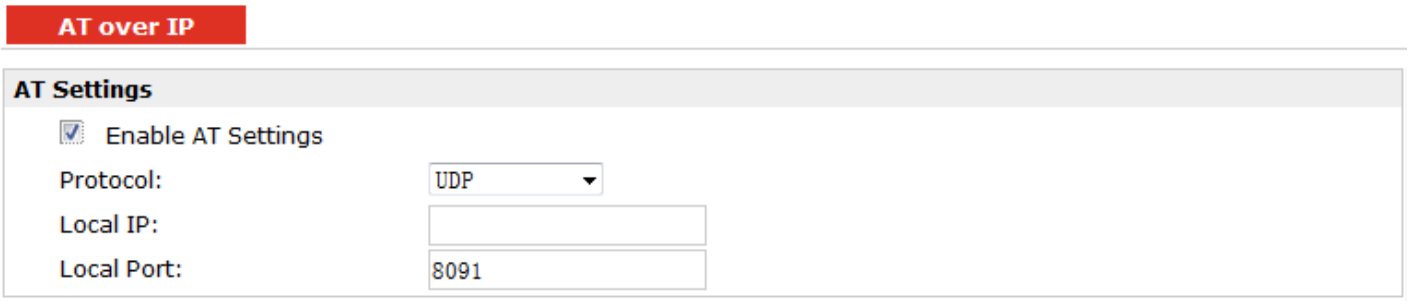


IP Passthrough		
Элемент	Описание	По умолчанию
Enable IP Passthrough (Включить IP Passthrough)	Установить отметку, чтобы активировать опцию IP Passthrough. ***Примечание**: предварительно необходимо выбрать Cellular (сотовый) в качестве Primary Interface (основной интерфейс) на вкладке Configuration -> Link Management (конфигурация/управление подключением).*	Disable (отключено)
Mode (Режим)	В настоящее время доступен выбор только режима PPPoE.	PPPoE
Ethernet Interface (Интерфейс Ethernet)	Выбрать интерфейс LAN из LAN_0, LAN_1. Клиенты PPPoE вызывают R3000 (сервер PPPoE) в соответствии с различными LAN интерфейсами. Например, если выбрать LAN_0 и произвести подключение клиента PPPoE (например, ПК) к LAN 0 по кабелю Ethernet, ПК соединится с R3000 (сервером PPPoE) через LAN 0. ***Примечание**: если активировано Enable Bridge на вкладке Configuration -> Ethernet -> LAN Interface, выбор LAN_0 или LAN_1 не будет иметь значения.*	LAN_0
Username (Имя пользователя)	Задать имя пользователя сервера PPPoE.	Null
Password (Пароль)	Задать пароль сервера PPPoE.	Null
AC Name (имя AC)	Задать имя AC (концентратор доступа) для сервера PPPoE.	Null
Service Name (Имя службы)	Задать имя службы сервера PPPoE. ***Примечание**: клиент PPPoE должен установить то же имя пользователя, пароль, имя AC и имя службы сервера PPPoE, иначе он не сможет успешно подключиться к серверу PPPoE.*	Null
Authentication (Аутентификация)	Задать аутентификацию PPP, выбрав из Auto, PAP, CHAP. Auto (автоматически): автоматическое определение. PAP: протокол аутентификации по паролю. CHAP: запросно-ответный протокол.	Auto
Link Detection Interval	Когда клиент PPPoE вызывает R3000 (сервер PPPoE), R3000 направляет	30

IP Passthrough		
(Интервал обнаружения соединения)	этому клиенту LCP Echo Request (эхо-запрос LCP) после этого интервала. Интервал обнаружения соединения задаётся в пределах от 3 до 30.	
Link Detection Max Retries (Максимальное количество повторов обнаружения соединения)	Если R3000 предпринимает повторные посылки эхо-запроса LCP Link указанное в Detection Max Retries количество раз и не получает корректных ответных пакетов от клиента PPPoE, он отправляет пакет LCP Terminal Request для разъединения соединения между сервером и клиентом PPPoE. Max Retries задаётся в пределах от 3 до 5 попыток.	5

3.31 Configuration -> AT over IP (Конфигурация-> AT по IP)

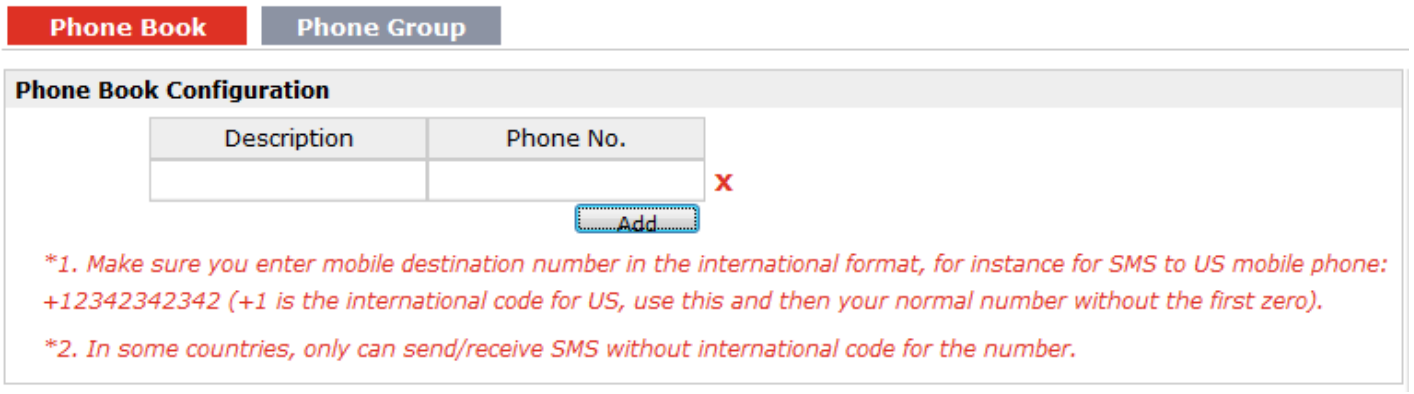
Этот раздел позволяет настроить параметры AT по IP.



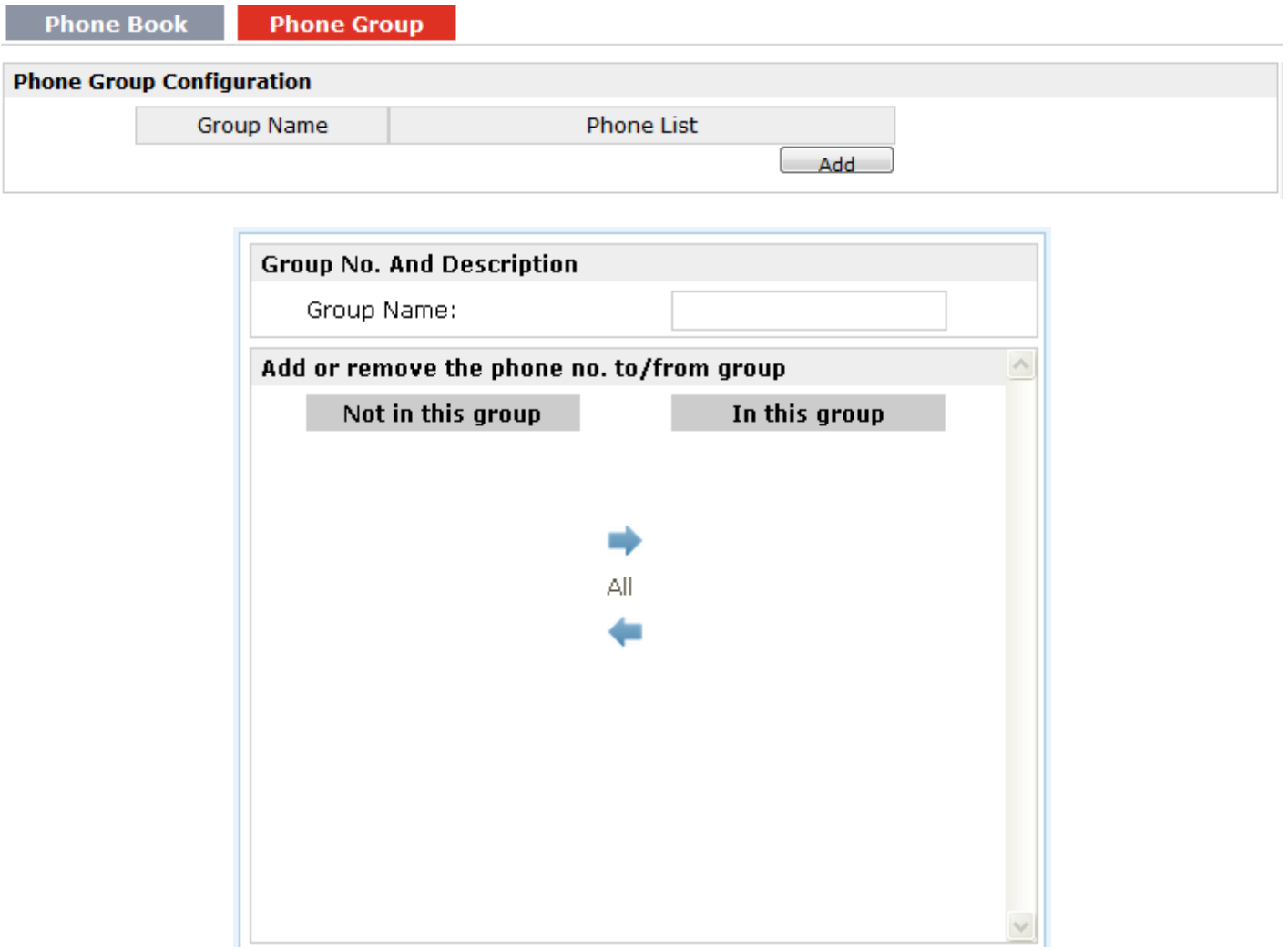
AT over IP (AT по IP)		
Элемент	Описание	По умолчанию
Enable AT Settings (Включить AT настройки)	Установить отметку, чтобы разрешить AT по IP для управления сотовым модулем AT командами удаленно.	Disable (отключено)
Protocol (Протокол)	Выбрать: TCP server или UDP.	UDP
Local IP (Локальный IP)	Можно ввести IP-адрес сотовой WAN, Ethernet WAN или Ethernet LAN. Нуль означает разрешение всех трех указанных IP-адресов.	0.0.0.0
Local Port (Локальный порт)	Ввести локальный открытый TCP или UDP порт.	8091

3.32 Configuration -> Phone Book (Конфигурация-> Телефонная книга)

Этот раздел позволяет настроить параметры телефонной книги.



Phone Book (Телефонная книга)		
Описание элемента	Описание	По умолчанию
Phone No. (Номер телефона)	Ввести имя, соответствующее номеру телефона.	Null
	Ввести свой номер телефона. ***Примечание:*** *в некоторых странах номер телефона требуется вводить в международном формате, начиная с символа «+» с последующим кодом страны.*	Null

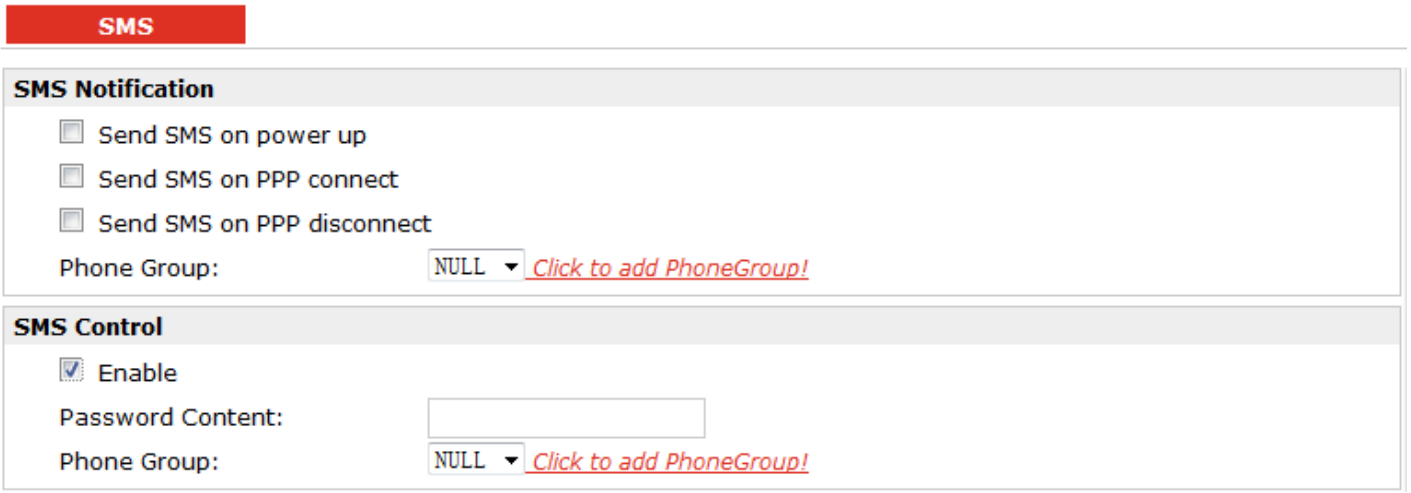


Phone Group (Телефонная группа)		
Group Name (Название группы)	Задать название группы.	Null
Phone List (список телефонов)	Показывать список телефонов в группе.	Null
Add or remove the phone no.to/from group (Добавить/удалить телефон в/из группы)	Щелкнуть на стрелке вправо, чтобы добавить номер телефона в текущую группу; щелкнуть на стрелке влево, чтобы удалить номер телефона из группы.	Null

Примечание: *R3000-4L не поддерживает функцию SMS/Call (SMS/Голосовой вызов), поэтому для него раздел PhoneBook на веб-странице недоступен.*

3.33 Configuration -> SMS (Конфигурация-> SMS)

Этот раздел позволяет настроить уведомление по SMS-сообщениям и параметры управления SMS.



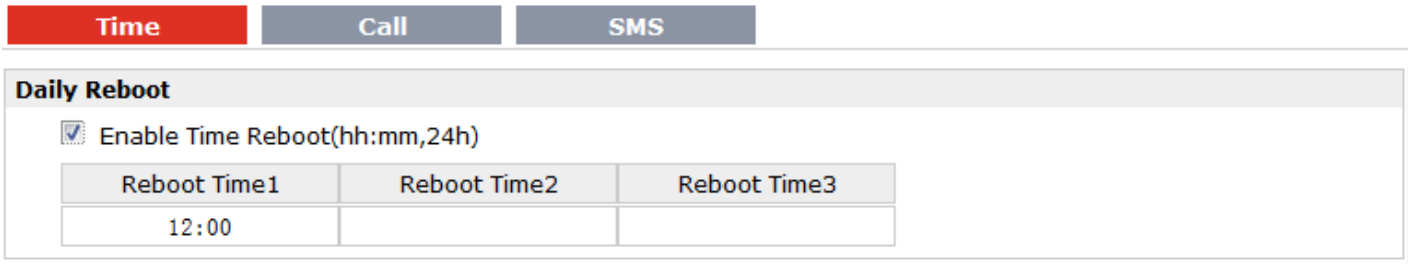
SMS		
Элемент	Описание	По умолчанию
Send SMS on power up (Передать SMS при включении)	Отметить, чтобы отправлять SMS определенному пользователю после включения маршрутизатора.	Disable (отключено)
Send SMS on PPP connect (Отправлять SMS при PPP подключении)	Отметить, чтобы отправлять SMS определенному пользователю после PPP подключения маршрутизатора.	Disable (отключено)
Send SMS on PPP disconnect (Отправлять SMS при отключении PPP)	Отметить, чтобы отправлять SMS определенному пользователю после отключения PPP маршрутизатора.	Disable (отключено)
Phone Group (Телефонная группа)	Выбрать телефонную группу, которая задана в *3.2.27 Configuration -> Phone Book*	Null

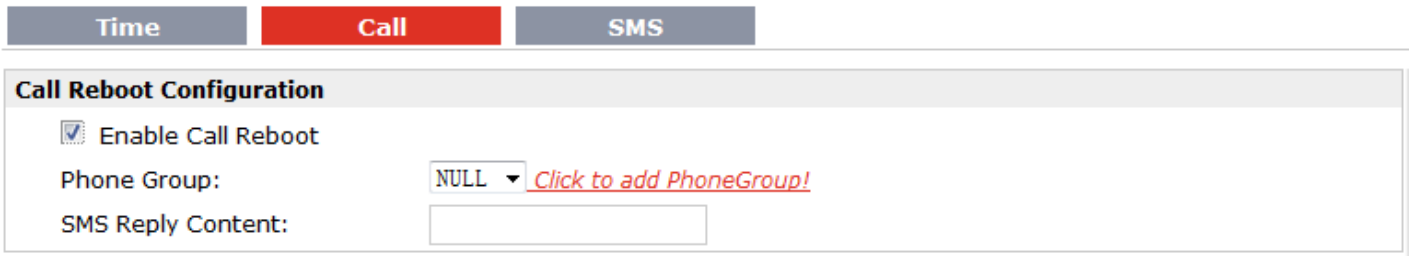
Enable @ SMS Control (Разрешить управление по SMS)	Щелкнуть, чтобы включить дистанционное управление по SMS.	Disable (отключено)
Password Content (Пароль)	Ввести символы, составляющие пароль. ***Примечание**: поддерживается только текстовый формат. Например, 123 или ABC123.*	Null
Phone Group (Телефонная группа)	Выбрать телефонную группу, которая задана в 3.2.27 Configuration -> Phone Book	Null

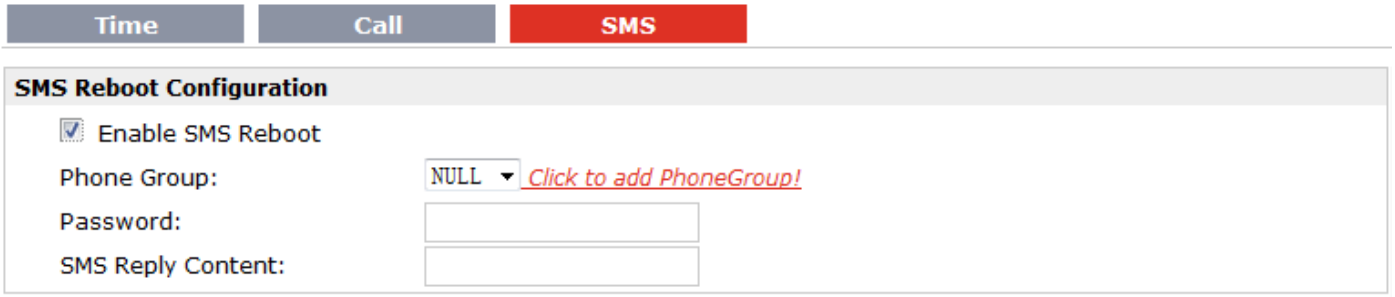
Примечание: см. раздел 4.7 SMS Commands for Remote Control (4.7 Команды SMS для дистанционного управления). R3000-4L не поддерживает функцию SMS/ВЫЗОВ, поэтому на его веб-странице раздел SMS не отображается.

3.34 Configuration -> Reboot (Конфигурация-> Перезагрузка)

Этот раздел позволяет настроить политики перезагрузки.







Time @ Reboot (Время перезагрузки)		
Элемент	Описание	По умолчанию
Enable(ahh:mm,24h) (Разрешить — чч:мм, 24 ч)	Разрешить ежедневную перезагрузку, для корректности данных время вводить в 24-часовом формате, чч:мм.	Disable (отключено)

Reboot Time1 (Время перезагрузки_1)	Задать time1 — время, когда необходимо перезагрузить маршрутизатор.	Null
Reboot Time2 (Время перезагрузки_2)	Задать time2 — время, когда необходимо перезагрузить маршрутизатор.	Null
Reboot Time3 (Время перезагрузки_3)	Задать time3 — время, когда необходимо перезагрузить маршрутизатор.	Null
Call @ Reboot (Перезагрузка по вызову)		
Enable Call Reboot (Разрешить перезагрузку по вызову)	Щелкнуть, чтобы включить функцию перезагрузки по вызову.	Disable (отключено)
Phone Group (Телефонная группа)	Задать телефонную группу, которой разрешено перезагружать маршрутизатор по вызову.	Null
SMS Reply Content (Текст ответного SMS)	Отправка ответного короткого сообщенияпосле автоматической перезагрузки по вызову от указанного абонента — Caller ID (например. Reboot ok! — Перезагружен, ОК). ***Примечание**: поддерживается только текстовый формат SMS.*	Null
SMS @ Reboot (Перезагрузка по SMS)		
Enable SMS Reboot (Разрешить перезагрузку по SMS)	Щелкнуть, чтобы включить функцию перезагрузки по SMS.	Disable (отключено)
Phone Group (Телефонная группа)	Задать телефонную группу, которой разрешено перезагружать маршрутизатор по SMS.	Null
Password (Пароль)	**Пароль для инициализации механизма перезагрузки.**	**Null**
SMS Reply Content (Текст ответного SMS)	Отправка ответного короткого сообщения после автоматической перезагрузки по SMS от указанного абонента — Caller ID (например. Reboot ok! — Перезагружен, ОК). ***Примечание**: поддерживается только текстовый формат SMS.*	Null

***Примечание:** R3000-4L не поддерживает функцию SMS/ВЫЗОВ, поэтому на его веб-странице разделы Call и SMS не отображаются.*

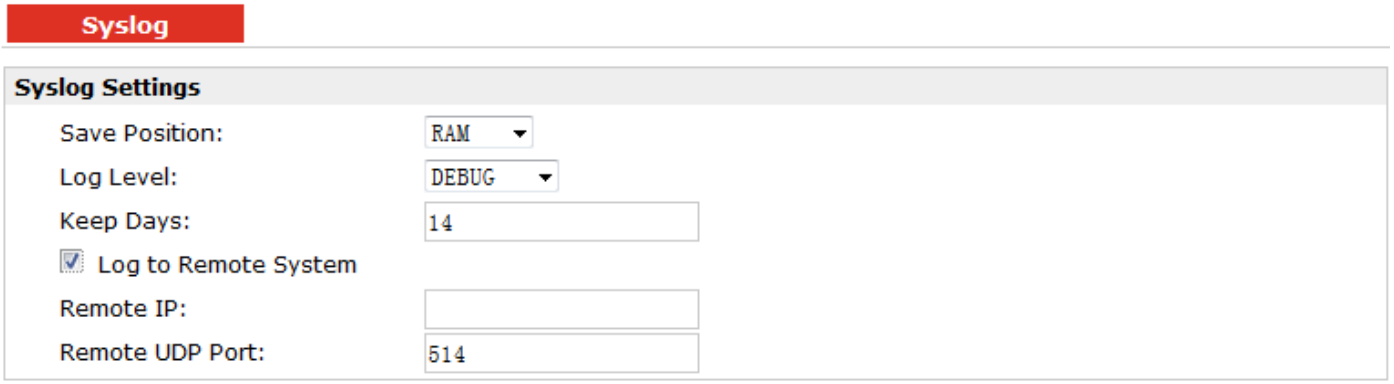
3.35 Configuration -> RobustLink (Конфигурация-> RobustLink)

Этот раздел позволяет конфигурировать параметры RobustLink, централизованной промышленного уровня системы управления и администрирования для R3000. RobustLink позволяет контролировать, конфигурировать и управлять большим количеством удаленных устройств в частной сети через Интернет.

RobustLink		
Элемент	Описание	По умолчанию
Enable RobustLink (Включить)	Щелкнуть, чтобы активировать RobustLink.	Disable (отключено)
Server Address (адрес сервера)	Ввести IP-адрес сервера RobustLink.	Null
Port (Порт)	Ввести номер порта RobustLink.	1883
Password (Пароль)	Ввести пароль, предварительно заданный в RobustLink. *Примечание: в R3000 и RobustLink должен быть идентичный набор паролей.*	Null

3.36 Configuration -> Syslog (Конфигурация-> Syslog — системный журнал)

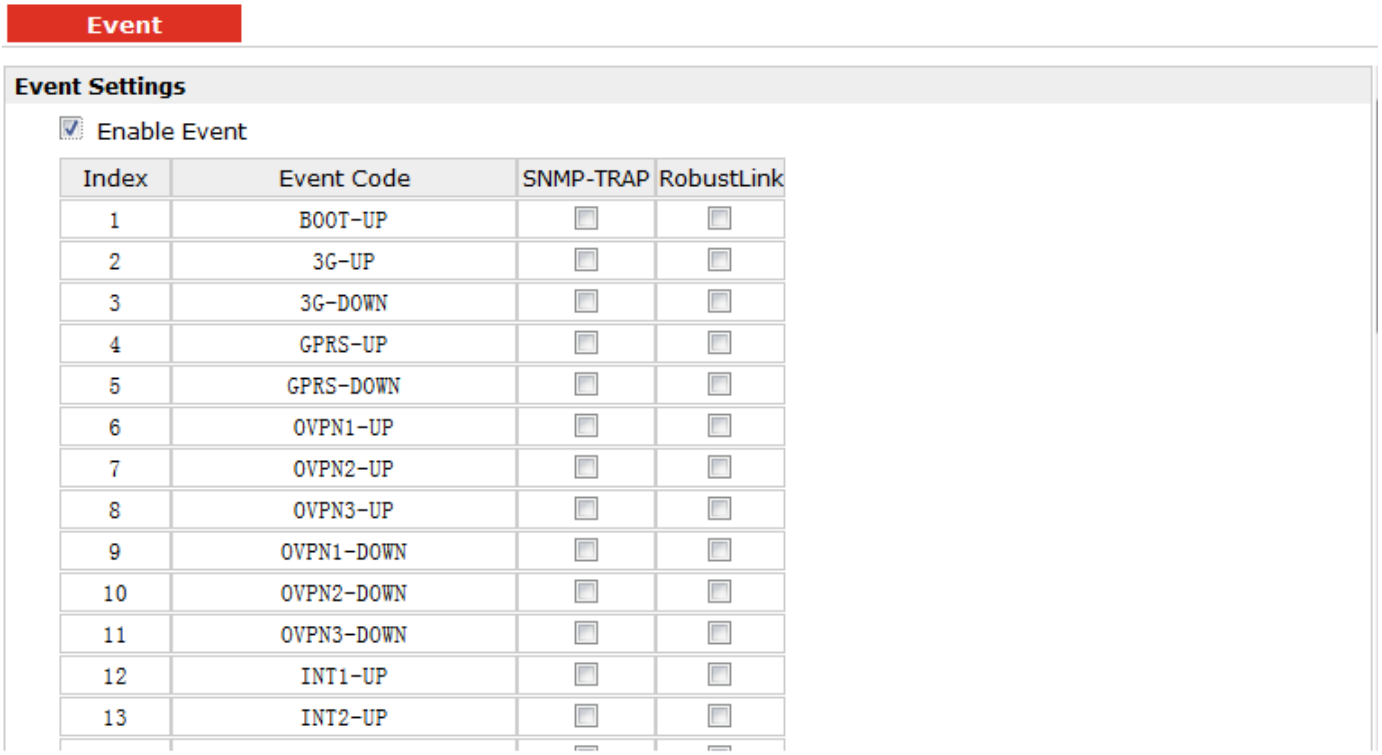
Этот раздел позволяет настроить параметры системного журнала.



Syslog (системный журнал)		
Элемент	Описание	По умолчанию
Save Position (Сохранить местоположение)	Выбрать расположение из None, Flash и SD. None означает, что системный журнал сохраняется только в RAM и будет очищен после перезагрузки.	NONE
Log Level (Тип журнала)	Выбрать из DEBUG, INFO, NOTICE, WARNING, ERR, CRIT, ALERT и EMERG (от низшего уровня до высшего). Более низкий уровень выводит более подробный системный журнал.	DEBUG (ОТЛАДКА)
Keep Days (Сохранять дни)	Выбрать Keep days, чтобы маршрутизатор, очистил старый системный журнал.	14
Log to Remote System (Журнал на удаленной системе)	Активировать, чтобы разрешить маршрутизатору передавать системный журнал на удаленный сервер syslog. Необходимо ввести IP и порт syslog сервера.	Disable (отключено)

3.37 Configuration -> Event (Конфигурация-> События)

Этот раздел позволяет настроить параметры событий.



Event (Событие)		
Элемент	Описание	По умолчанию
Enable Event (Разрешить события)	Щелкнуть для включения Event. Эта функция используется для передачи отчетов об основных событиях в работе R3000 основное рабочее событие на SNMP-TRAP или RobustLink. Имеется ряд кодов событий, доступных для выбора, например BOOT-UP, 3G-UP, 3G-DOWN, и т. д. Например, если щелкнуть 3G-UP и выбрать RobustLink в качестве сервера, после подключения R3000 к сети 3G, он отправит код события-event code 3G-UP с соответствующей информацией на RobustLink.	Disable (отключено)

3.38 Configuration -> USR LED (Конфигурация-> Светодиод USR)

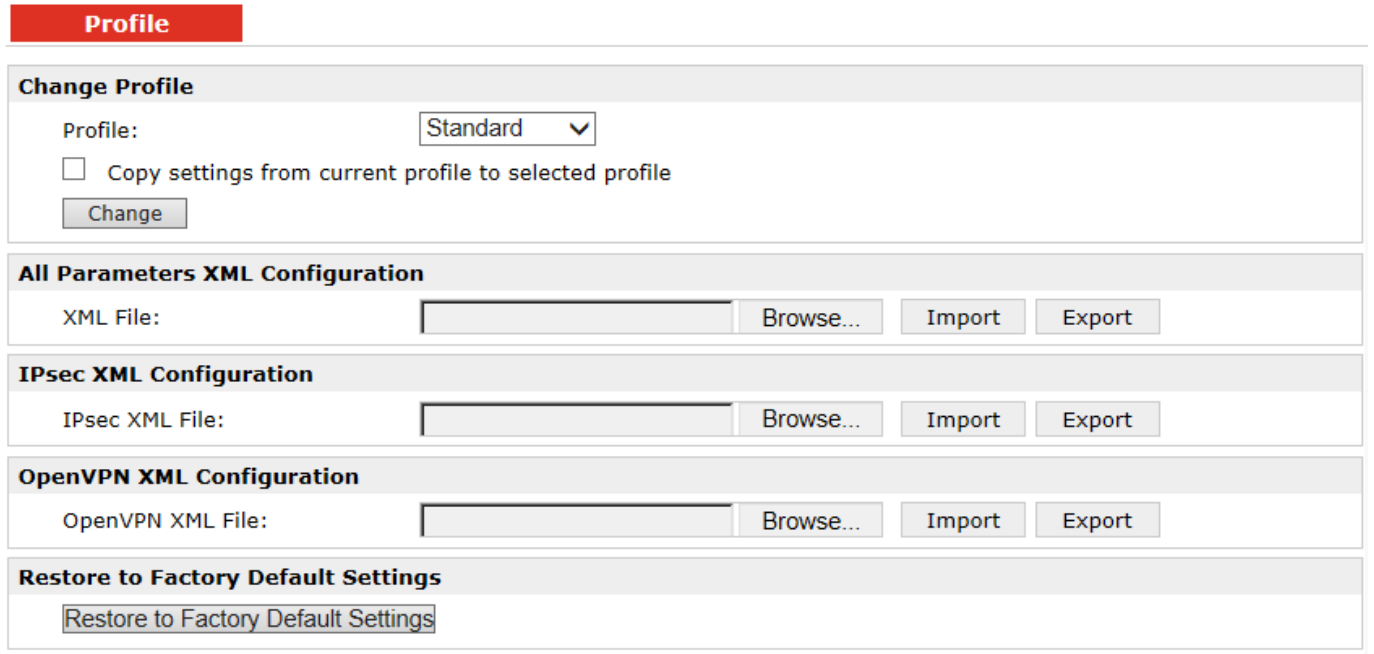
Этот раздел позволяет изменять состояние светодиодной индикации USR.

***Примечание**: См. Status -> System -> LEDs Information -> USR.*

LED USR (Светодиод USR)		
Элемент	Описание	По умолчанию
USR LED Type (Тип USR индикации)	Выбрать из VPN, PPPoE, DynDNS и GPS.	VPN
Indication (Индикация)	Выбрать из ON, Blink (Вкл./мигание). Например, если USR LED Type будет установлен как VPN, и для Indication выбрано Blink, при открытии любого VPN туннеля, светодиод USR будет мигать.	ON

3.39 Administration -> Profile (Администрирование-> Профиль)

Этот раздел позволяет импортировать или экспортировать файл конфигурации и восстанавливать заводские настройки маршрутизатора.



Profile (Профиль)		
Элемент	Описание	По умолчанию
Profile (Профиль)	Этот элемент позволяет пользователю сохранить различные профили конфигурации в разных местах или сохранить один профиль конфигурации в разных местах только для резервного копирования данных коннфигурации. Выбрать из Standard, Alternative 1, Alternative 2, Alternative 3 (Стандартный, альтернативный1 ...3).	Standard (Стандартный)
XML Configuration (XML конфигурация)	Импорт: Щелкнуть на Browse, чтобы выбрать XML-файл на локальном компьютере, затем щелкнуть на Import, чтобы импортировать этот файл в маршрутизатор. Export (Экспорт): Щелкнуть на Export, и конфигурация будет показана в новом открывшемся окне браузера, после этого ее можно сохранить как файл XML.	Null
Restore to Factory Default Settings (Восстановление заводских настроек)	Щелкнуть на кнопке Restore to Factory Default Settings для восстановления заводских настроек маршрутизатора.	Null

3.40 Administration -> Tools (Администрирование-> Инструменты)

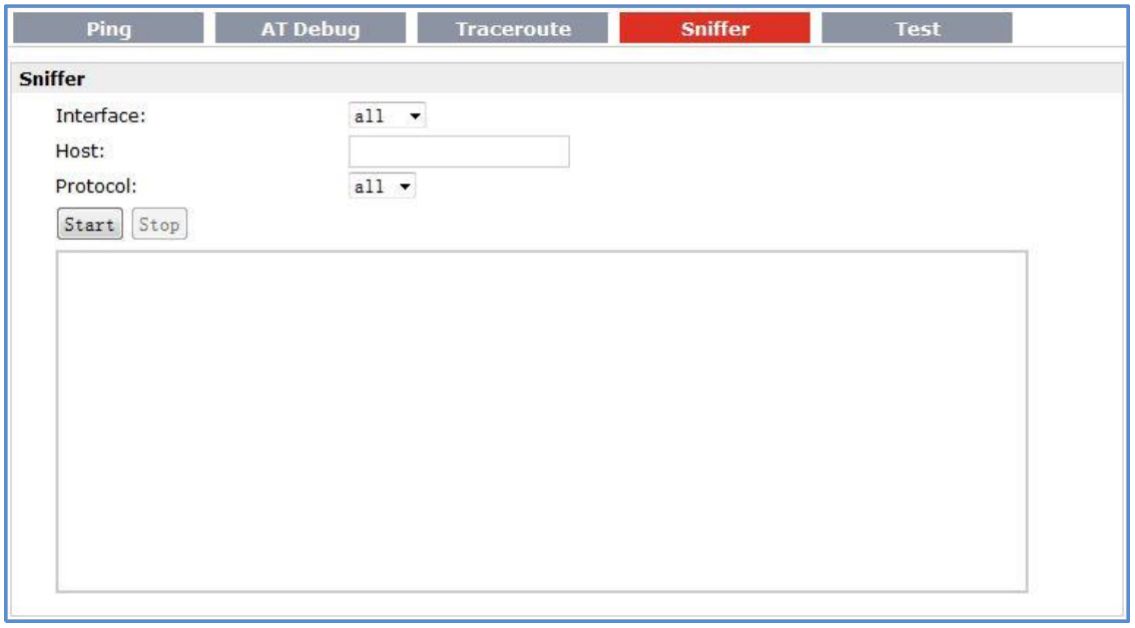
В этом разделе доступны четыре инструмента: Ping, AT Debug, Traceroute и Test.

Ping @ Tools (Инструменты — Ping)		
Элемент	Описание	По умолчанию
Ping IP address (IP-адрес для эхо-	Ввести целевой IP-адрес или доменное имя для эхо-тестирования.	Null

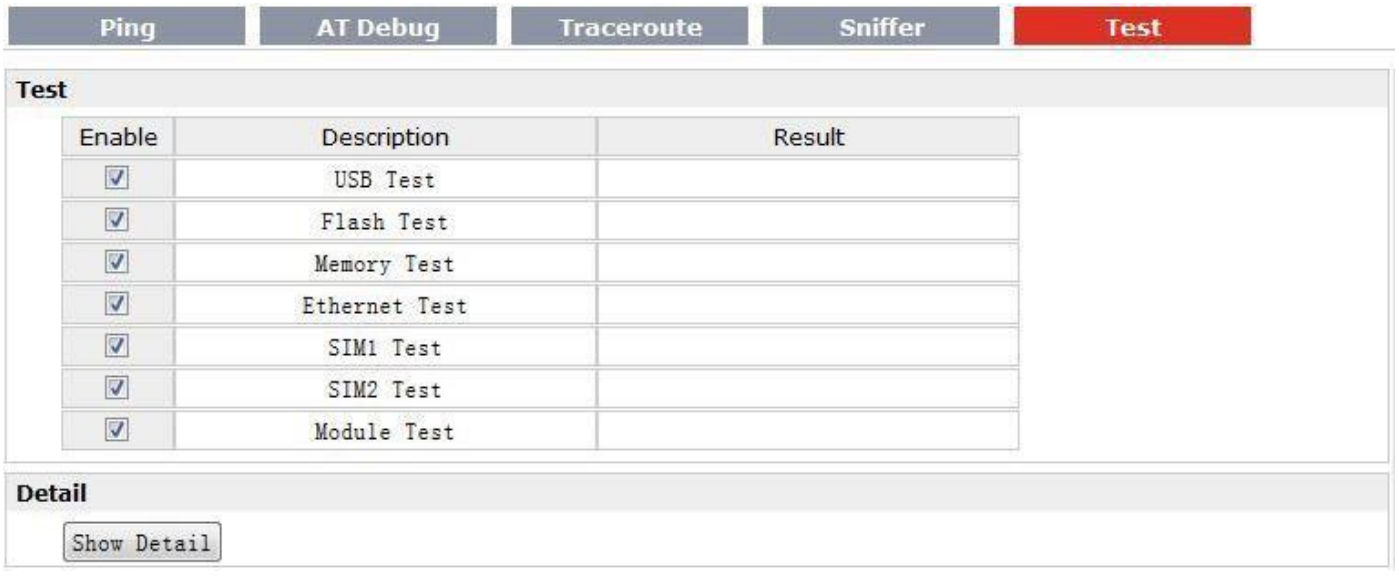
Ping @ Tools (Инструменты — Ping)		
тестирования)		
Number of requests (Число запросов)	Задать количество запросов эхо-тестирования.	5
Timeout (Тайм-аут)	Задать тайм-аут запросов эхо-тестирования.	1
Local IP (Локальный IP)	Выбрать локальный IP из сотовой WAN, Ethernet WAN или Ethernet LAN. Нуль означает автоматический выбор IP-адреса из трех указанных.	Null
Start (Запустить)	Нажать эту кнопку, чтобы запустить запрос эхо-тестирования, в показанном ниже окне будет выведен журнал.	Null

AT Debug @ Tools (Инструменты — AT отладка)		
Элемент	Описание	По умолчанию
Send AT Commands (Отправить AT команды)	Ввести в это поле AT команды для отправки на сотовый модуль.	Null
Send (Передать)	Нажать эту кнопку, чтобы отправить AT команды.	Null
Receive AT Commands (Получить AT команды)	Маршрутизатор выведет в этом поле AT команды, полученные в ответ от сотового модуля.	Null

Traceroute @ Tools (Инструменты — Traceroute)		
Элемент	Описание	По умолчанию
Trace Address (Адрес трассировки)	Ввести целевой IP-адрес или доменное имя для трассировки.	Null
Trace Hops (Транзитные участки трассировки)	Задать максимальное количество транзитных участков трассировки. Маршрутизатор остановит трассировку, если обнаружит достижение максимального количества транзитных участков, вне зависимости от достижения/недостижения места назначения.	30
Timeout (Тайм-аут)	Задатьтайм-аут запросов Traceroute.	1
Send (Передать)	Нажать эту кнопку, чтобы запустить запрос Traceroute, в показанном ниже поле будет выведен журнал.	Null



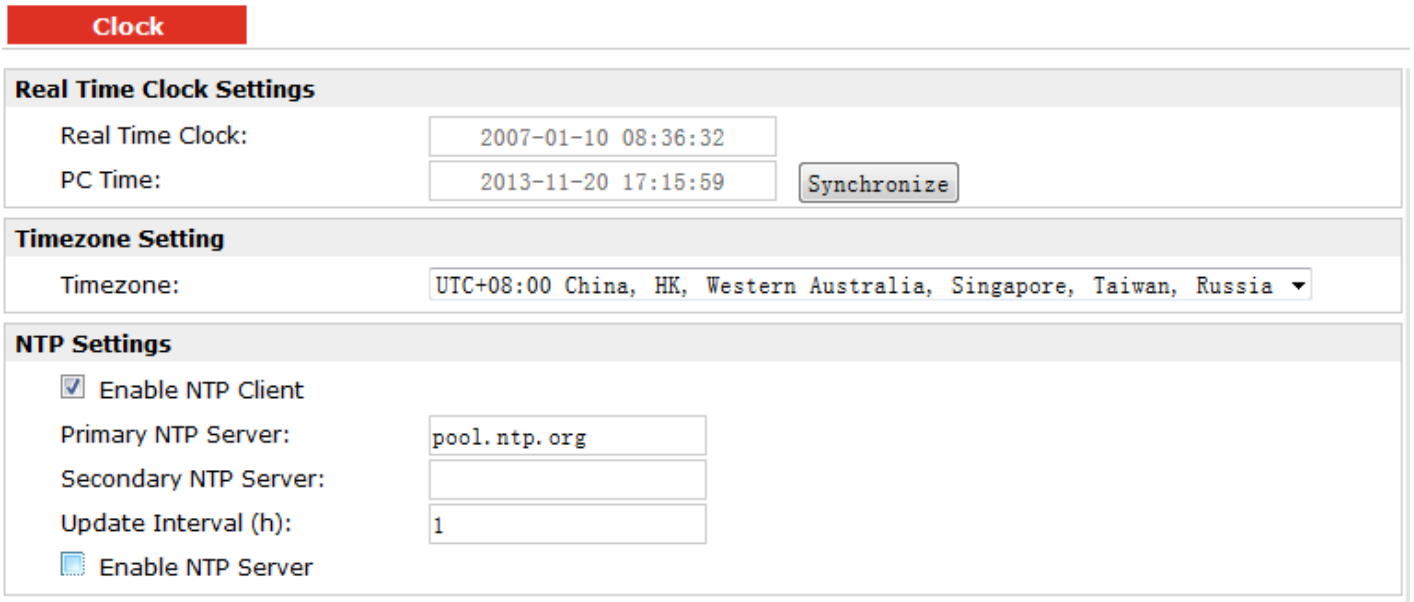
Sniffer @ Tools (Инструменты — Сниффер)		
Элемент	Описание	По умолчанию
Interface (Интерфейс)	Выбрать из all, lo, imq0, imq1, eth0, gre0 и ppp0. all: включить все интерфейсы; lo: локальный петлевой интерфейс; imq0/1: виртуальный интерфейс для QoS, который используется для ограничения скорости загрузки и отправки; eth0: интерфейс Ethernet; gre0: интерфейс GRE туннеля; ppp0: сотовый интерфейс PPP;	All (Все)
Host (Узел)	Фильтровать пакеты, которые содержат определенный IP-адрес.	Null
Protocol (Протокол)	Выбрать из all, ip, arp, tcp и udp.	All (Все)
Start (Запустить)	Нажать эту кнопку, чтобы запустить сниффер, в следующем окне будет выведен журнал.	Null



Test @ Tools (Инструменты — Тестирование)		
Элемент	Описание	По умолчанию
Enable (Разрешить)	Щелкнуть Enable, чтобы выбрать аппаратный компонент, состояние которого требуется проверить.	Enable (Разрешить)
Description (Описание)	Выбрать из SD Test, USB Test, Flash Test, Memory Test, Ethernet Test, SIM1 Test, SIM2 Test и Module Test.	N/A
Result (Результат)	Отображение текущего статуса выбранного аппаратного компонента. Имеется 3 состояния: Testing, Success и Failure (Тестирование, Успешно и Отказ). Testing (Тестирование): маршрутизатор тестирует выбранный аппаратный компонент. Success (Успешно): соответствующий аппаратный компонент подключен должным образом и обнаружен. Failure (Отказ): соответствующий аппаратный компонент не подключен должным образом или не обнаружен маршрутизатором.	Null
Show Detail (Показать подробно)	Подробное отображение тестирования текущего аппаратного компонента.	Null
Щелкнуть Apply, чтобы начать тестирование.		

3.41 Administration -> Clock (Администрирование-> Часы)

Этот раздел позволяет настроить часы маршрутизатора и сервер NTP.

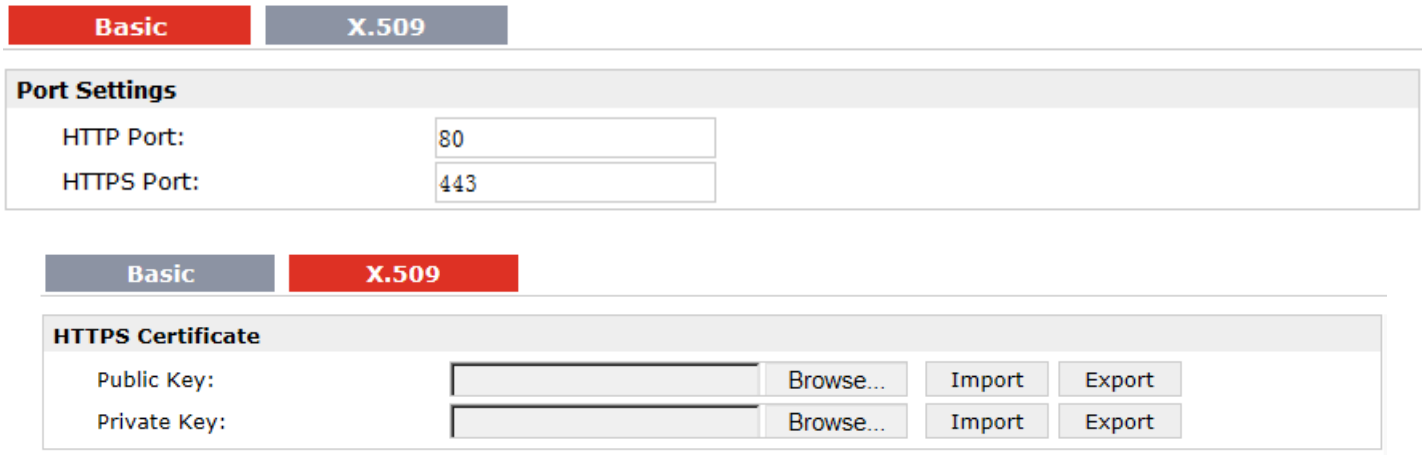


Clock (Часы)		
Элемент	Описание	По умолчанию
Real Time Clock (Часы реального времени)	В этом поле могут быть показаны и настроены часы реального времени маршрутизатора.	Null

PC Time (Время ПК)	Здесь может быть выведено время локального ПК.	Null
Synchronize (Синхронизировать)	Синхронизировать часы реального времени маршрутизатора с ПК.	Null
Enable NTP Client (Разрешить клиент NTP)	Разрешить, синхронизировать время с сервером NTP.	Disable (отключено)
Timezone @ Client (Часовой пояс клиента)	Выберать свой часовой пояс местного времени.	UTC +08:00
Primary NTP Server (Основной сервер NTP)	Ввести IP-адрес или доменное имя основного сервера NTP.	pool.nt p.org
Secondary NTP Server (Дополнительный сервер NTP)	Ввести IP-адрес или доменное имя дополнительного сервера NTP.	Null
Update interval (h) (Интервал обновления (ч)	Ввести временной интервал для синхронизации времени между клиентом и сервером NTP.	1
Enable NTP Server (Разрешить NTP сервер)	Щелкнуть, чтобы включить функцию NTP сервер маршрутизатора.	Disable (отключено)
Timezone @ Server (Местное время сервера)	Выбрать часовой пояс местного времени.	UTC +08:00

3.42 Administration -> Web Server (Администрирование-> веб-сервер)

Этот раздел позволяет изменить параметры веб-сервера.



Basic @ Web Server (Основные настройки веб-сервера)		
Элемент	Описание	По умолчанию
HTTP Port (Порт HTTP)	Ввести номер порта HTTP, который требуется изменить для веб-сервера R3000. Порт 80 веб-сервера является портом прослушивания, на него сервер ожидает получать данные от Веб-клиента. Если в конфигурирации	80

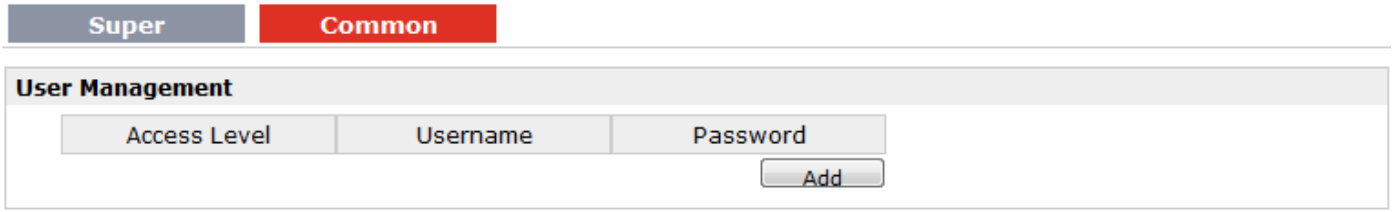
	маршрутизатора задан другой номер порта вместо 80, войти в систему веб-сервера R3000 можно будет только добавив этот номер порта.	
HTTPS Port (Порт HTTPS)	Ввести номер порта HTTPS, который требуется изменить для веб-сервера R3000. Порт 443 веб-сервера является портом прослушивания, на него сервер ожидает получать данные от Веб-клиента. Если в конфигурирации маршрутизатора задан другой номер порта вместо 443, войти в систему веб-сервера R3000 можно будет, только добавив этот номер порта. ***Примечание**: HTTPS обеспечивает большую безопасность, чем HTTP. Во многих случаях клиенты могут обмениваться с сервером конфиденциальной информацией, сервер при этом должен быть защищен, чтобы предотвратить несанкционированный доступ. Поэтому корпорацией Netscape был разработан HTTP, что позволяет авторизацию и защищенные транзакции.*	443
X.509 @ Web Server (Веб-сервер — X.509)		
HTTPS Certificate (Сертификат HTTPS)	На этой вкладке пользователь может импортировать или экспортировать открытый и закрытый ключ для сертификации HTTPS.	Null

3.43 Administration -> User Management (Администрирование-> Управление пользователями)

Этот раздел позволяет изменять или добавлять учетные записи пользователей.

Super @ User Management (Управление пользователями — Администратор системы)		
Элемент	Описание	По умолчанию
Super	Один маршрутизатор может иметь только одну учетную запись администратора системы. Эта учетная запись предоставляет пользователю наибольшие права, включая изменение и добавление учетных записей пользователей.	Admin (Администратор)
User Management (Управление учетной записью администратора)	Задать имя пользователя и пароль.	Null
Login Timeout (Тайм-аут	Задать значение тайм-аута входа в систему. Если в течение	1800

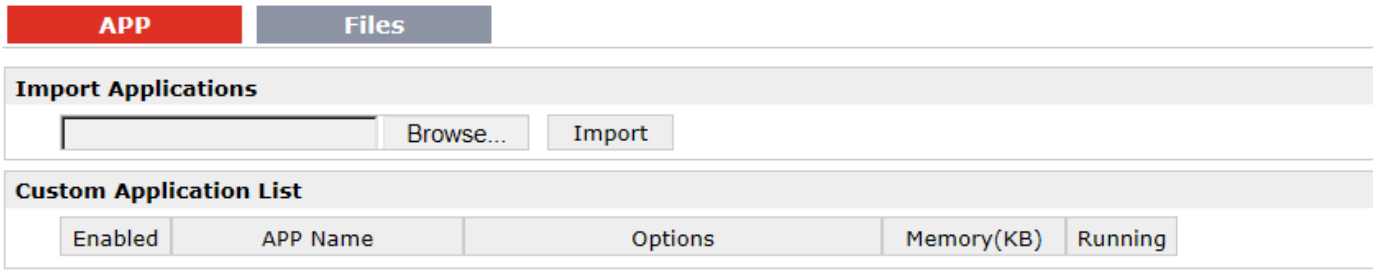
Super @ User Management (Управление пользователями — Администратор системы)		
входа в систему)	этого тайм-аута пользователи неактивны, необходимо повторно войти в систему.	



Common @ User Management		
Элемент	Описание	По
Common (Общий)	У одного маршрутизатора может быть до 9 общих учетных записей пользователя. Общая учетная запись пользователя предоставляет два уровня	Null
Access Level (Уровень доступа)	Выбрать из: ReadWrite и ReadOnly. ReadWrite (чтение/запись): этот уровень предоставляет пользователю возможность просматривать и настраивать конфигурацию	Null
Username/ Password	Задать имя пользователя и пароль.	Null
Add (Добавить)	Щелкнуть эту кнопку для добавления новой учетной записи.	Null

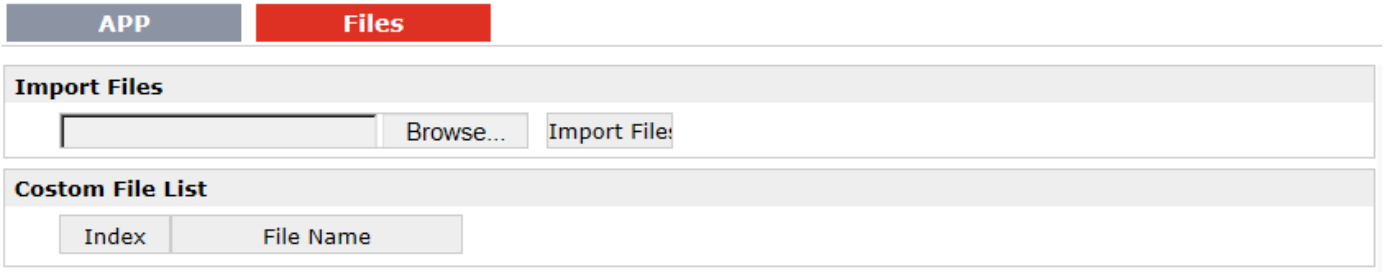
3.44 Administration -> SDK Management (Администрирование-> Работа с SDK)

Этот раздел позволяет настроить параметры работы с SDK маршрутизатора – комплектом средств разработки для создания и работы с собственными приложениями.



APP @ SDK Management (Приложения и работа с SDK)		
Элемент	Описание	По умолчанию
Firmware Version (Версия встроенного микропрограммного обеспечения)	Версия используемого встроенного микропрограммного обеспечения.	Null
Import Files (Импорт файлов)	Щелкнуть, чтобы импортировать файлы APP.	Null
Custom Application List	Этот список показывает, какие файлы APP импортированы	Null

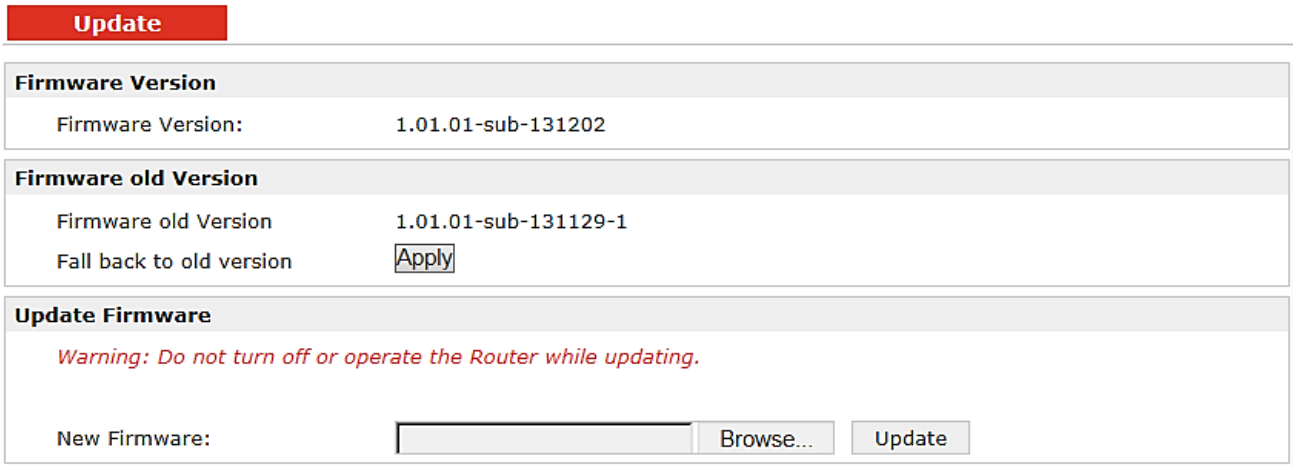
APP @ SDK Management (Приложения и работа с SDK)		
(Список пользовательских приложений)	пользователем в маршрутизатор, какой файл APP требуется запустить, а также — информацию о выполнении. Enable (Разрешить): щелкнуть, чтобы разрешить APP файл. APP Name (Имя APP): показывает имена файлов APP. Options (Опции): это дополнительные элементы, пользователю может потребоваться сконфигурировать здесь параметры запуска. Memory (KB) (Память (кбайт): показывает ресурсы памяти, занятые файлами APP. Running (Выполнение): Показывает, выполняются ли файлы APP.	



Files @ SDK Management (Файлы)		
Элемент	Описание	По умолчанию
Import Files (Импорт файлов)	Щелкнуть здесь для импорта файлов конфигурации.	Null
Custom File List (Список пользовательских файлов)	Этот список показывает файлы конфигурации, импортированные пользователем в маршрутизатор.	Null

3.45 Administration -> Update Firmware (Администрирование-> Обновление встроенного микропрограммного обеспечения)

Этот раздел позволяет обновлять встроенное микропрограммное обеспечение маршрутизатора.



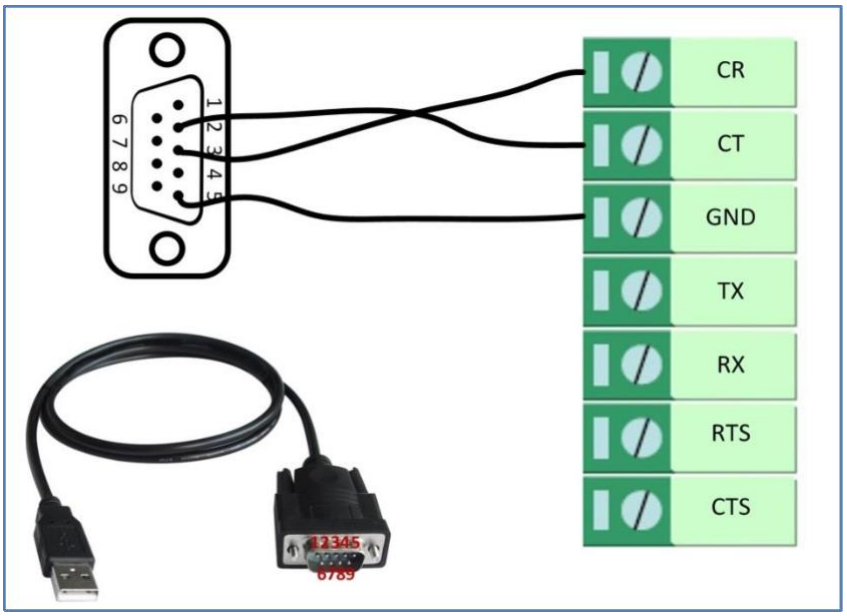
Update (Обновление)		
Элемент	Описание	По умолчанию
Firmware Version (Версия встроенного микропрограммного обеспечения)	Версия используемого встроенного микропрограммного обеспечения	Null
Update firmware (Обновление встроенного микропрограммного обеспечения)	Нажать кнопку *Browse*, чтобы выбрать корректное встроенное микропрограммное обеспечение на локальном ПК, затем — нажать кнопку *Update* для обновления. После успешного обновления необходимо перезагрузить маршрутизатор, чтобы изменения вступили в силу.	Null

Глава 4 Примеры конфигурации

4.1 Интерфейсы

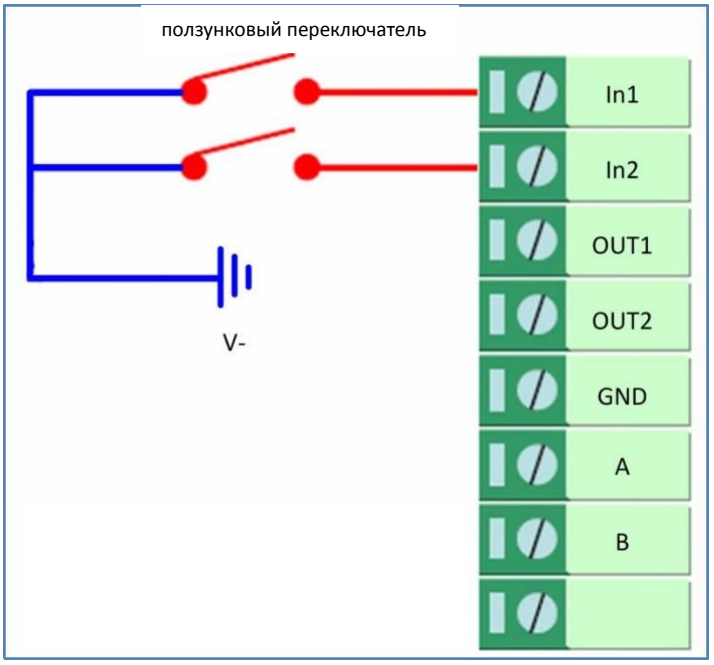
4.1.1 Порт консоли

Пользователь может использовать порт консоли для управления маршрутизатором посредством CLI команд, о CLI см. Введение в CLI.



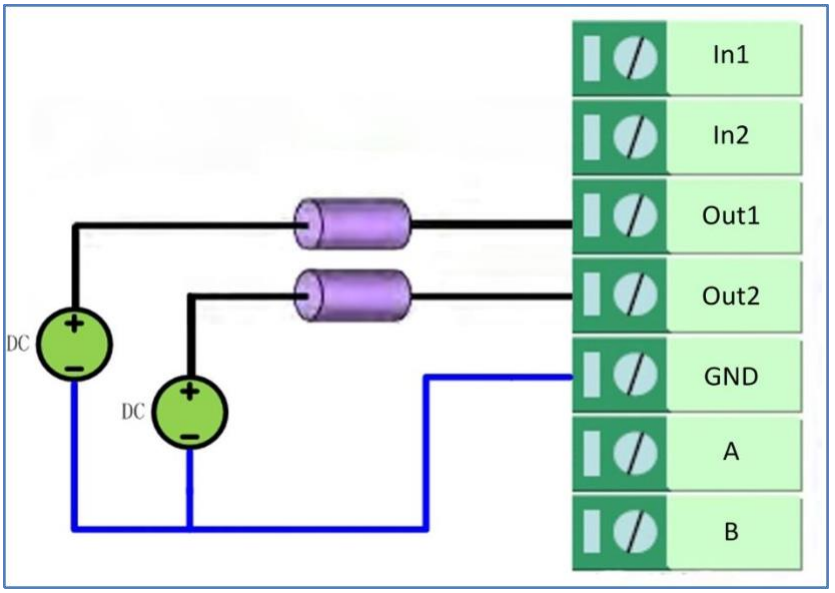
4.1.2 Цифровой вход

R3000 имеет два цифровых входа, он поддерживает только сухой контакт (не поддерживает магнитоуправляемый контакт — wet contact).
Следует ознакомиться с интерфейсным разъемом R3000, V- легко обнаружить на одном из контактов разъема питания.



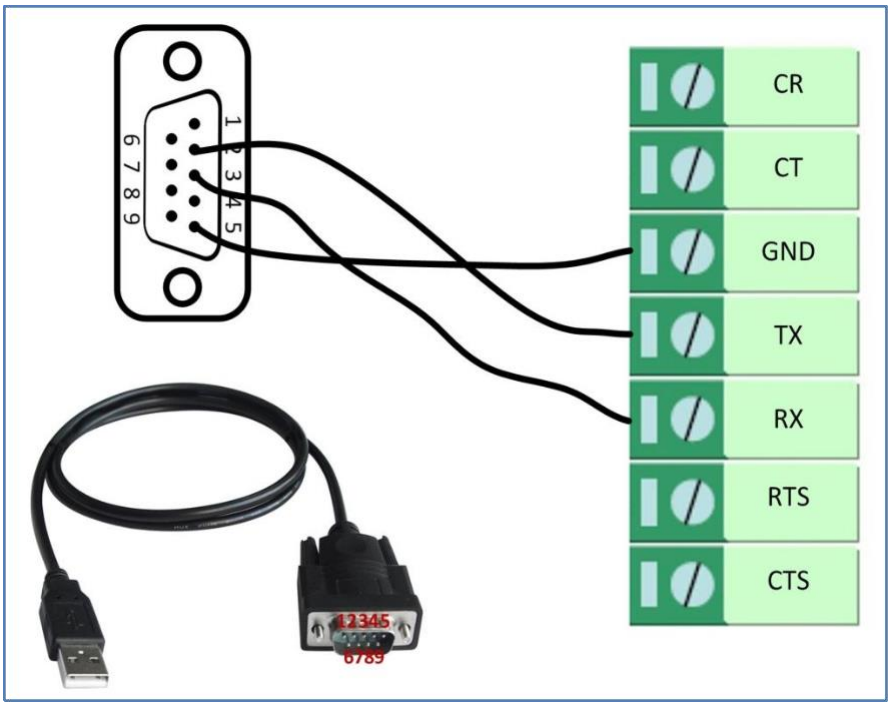
4.1.3 Цифровой выход

R3000 имеет два цифровых выхода. Отрицательный вывод питания постоянного тока необходимо подключать к GND.
См. схему соединений справа.
Максимальное напряжение/ток/выходная мощность DO 36 В постоянного тока/0,05A/ 0,3 Вт. Это означает, что разность потенциалов между Out1/Out2 и GND не может превышать 36 В постоянного тока; сила тока через Out1/Out2 не может превышать 50 мА. Выходная мощность, рассеиваемая Out1/Out2, не может превышать 0,3 Вт.



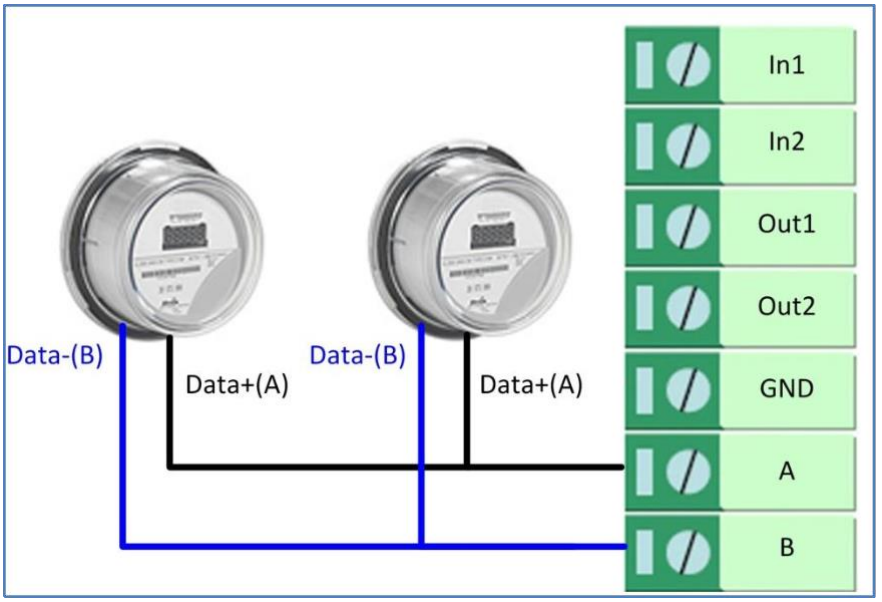
4.1.4 RS-232

R3000 поддерживает один порт RS-232 для последовательной передачи данных. См. схему соединений справа.



4.1.5 RS-485

R3000 поддерживает один порт RS-485 для последовательной передачи данных.
См. схему соединений справа.



4.2 Сотовый интерфейс

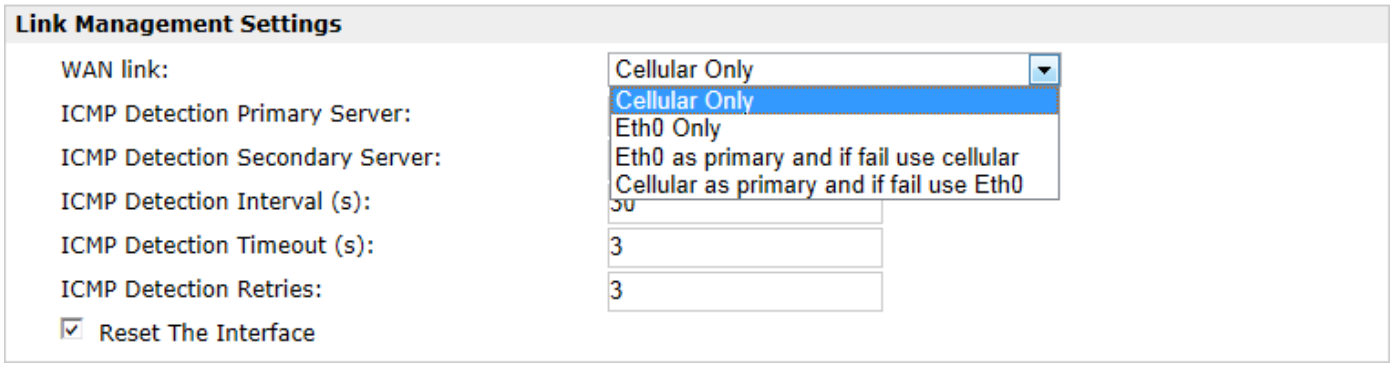
4.2.1 Cellular Dial-Up (Сотовый коммутируемый доступ)

В этом разделе показано, как конфигурировать параметры сотового коммутируемого доступа, которые определяются двумя различными политиками: Always Online и Connect on Demand (подключен постоянно и подключение по требованию).

***Примечание**: этот раздел будет скрыт, если пользователь выберет Eth0 Only в Configuration -> Link Management.*

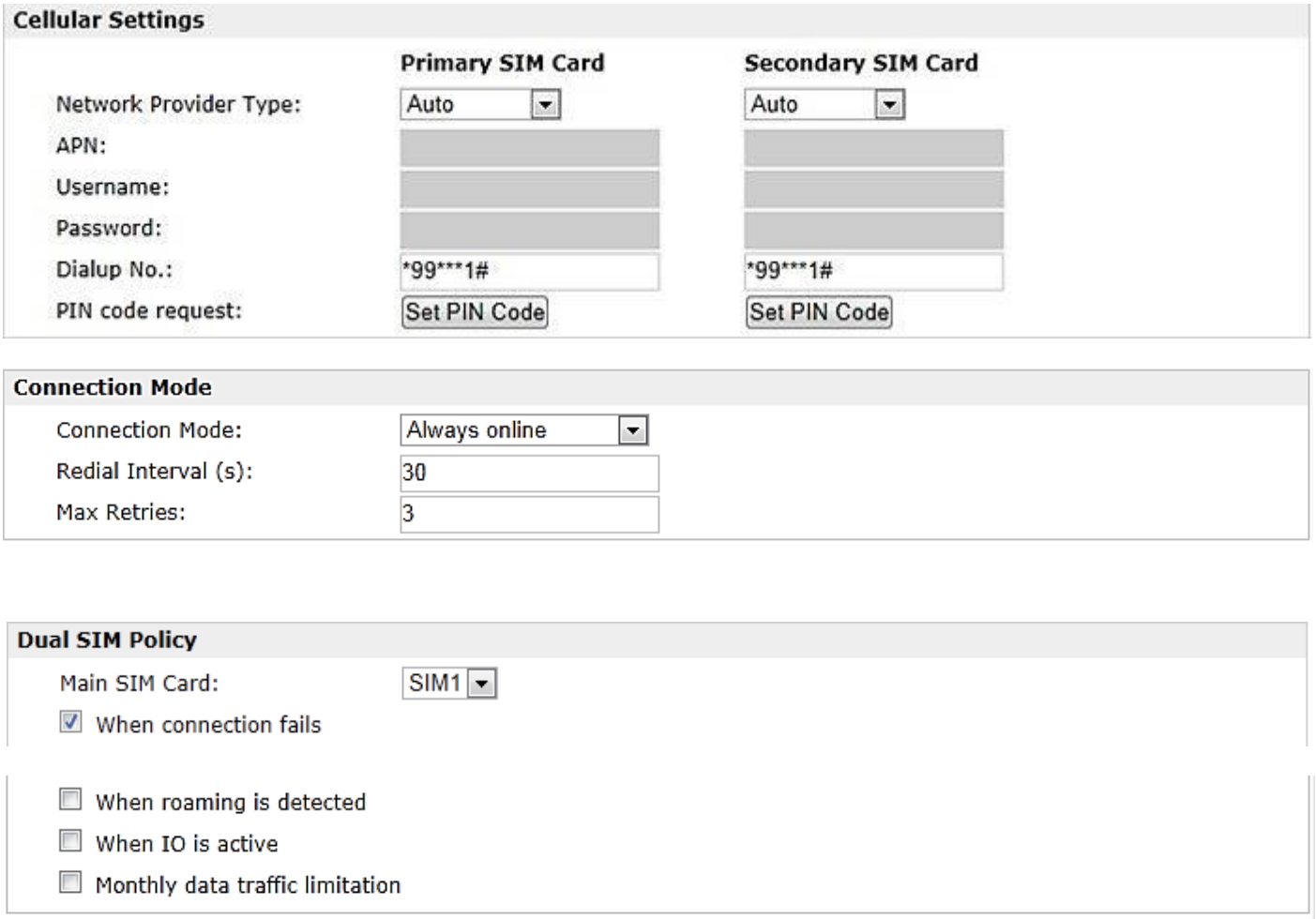
1. **Always Online (Подключен постоянно)**

Configuration-->Link Management-->Cellular Only



Изменения вступают в силу после нажатия кнопки *Apply*.

Configuration-->Cellular WAN -->Basic

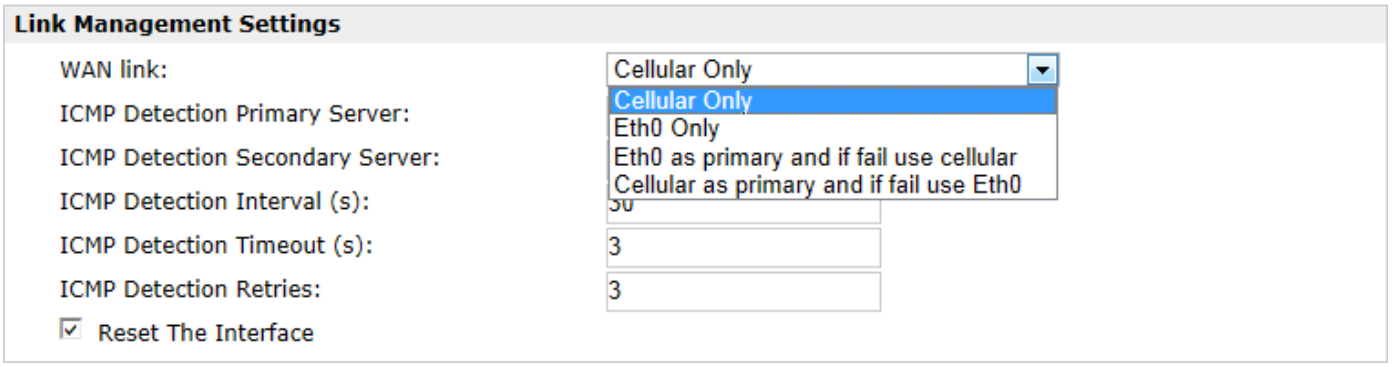


Изменения вступают в силу после нажатия кнопки *Apply*.

Если используется нестандартная SIM-карта, следует выбрать Custom вместо Auto в Network Provider Type, и настроить вручную ряд связанных настроек.

2. Connect on Demand (Подключение по требованию)

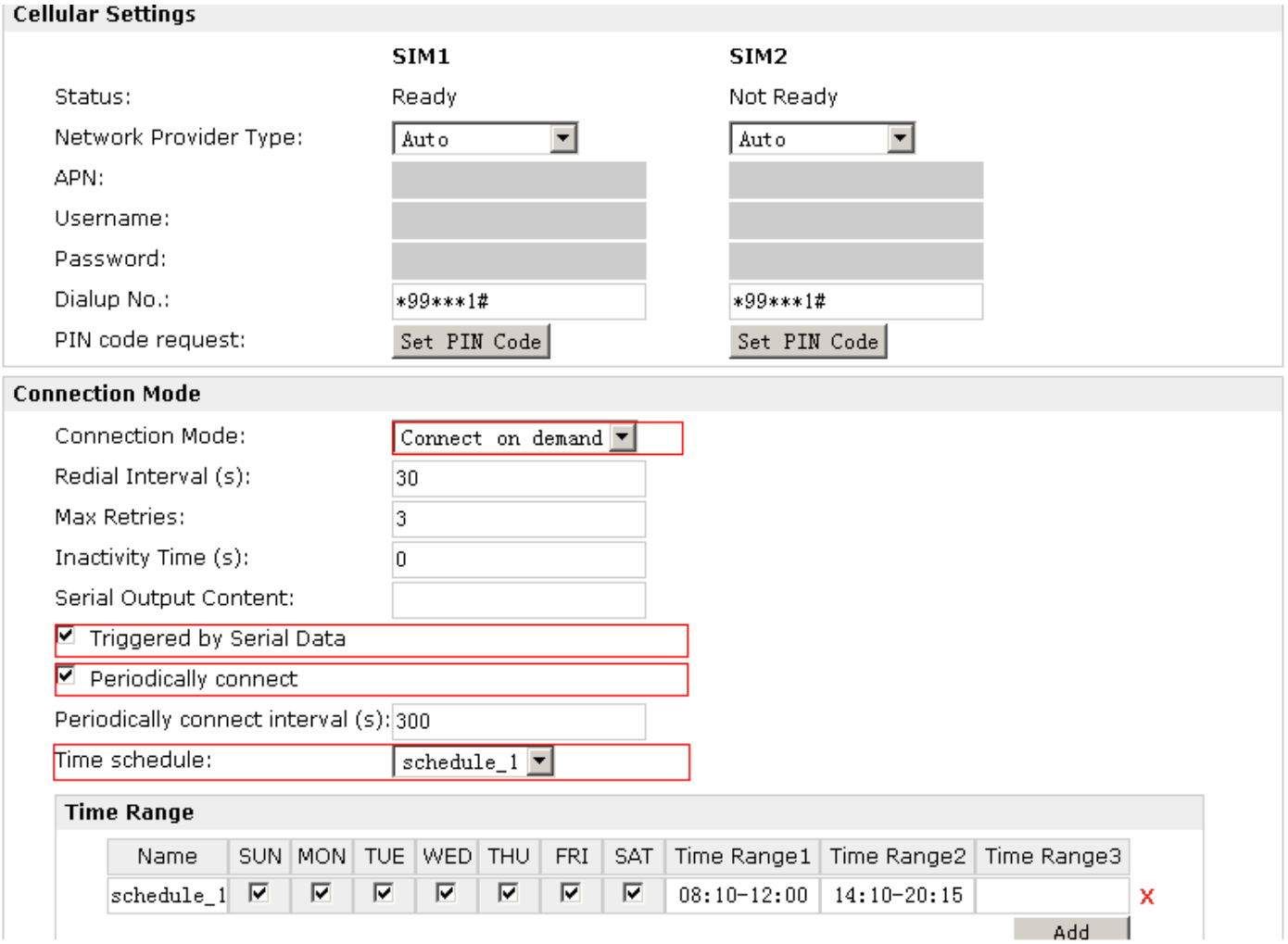
Configuration-->Link Management-->Cellular Only



Изменения вступают в силу после нажатия кнопки *Apply*.

Примечание: *этот раздел будет скрыт, если пользователь выберет Cellular в качестве основного и при сбое использования Eth0 в Configuration ->Link Management.*

Configuration-->Cellular WAN -->Basic



Выбрать требуемую политику активации.

Примечание: *если выбрать несколько политик активирования, маршрутизатор будет инициирован любой из них.*

4.2.2 Удаленное управление по SMS

R3000 поддерживает дистанционный контроль по SMS. В настоящее время пользователю недоступна настройка новых параметров R3000, ниже приведены команды для контроля статуса R3000. Команды SMS имеют следующую структуру: **Password:cmd1,a,b,c;cmd2,d,e,f;cmd3,g,h,i;...;cmdn,j,k,n**

Описание SMS команд:

1. Password: пароль для управления по SMS настраивается в *Basic > SMS Control > Password***,** является дополнительным параметром.
   a) Если пароль не задан, команда SMS имеет следующую структуру: **cmd1;cmd2;cmd3;…;cmdn**
2. При наличии пароля, SMS команда имеет следующую структуру: **Password:cmd1;cmd2;cmd3;…;cmdn** cmd1, cmd2, cmd3 to Cmdn, что служит номером, идентификации команды 0001 – 0010.
3. a, b, c к n являются параметрами команды.
4. Символ точки с запятой («;»), используется для разделения более чем одной команды в одном SMS-сообщении.
5. Например, 1234:0001

В этой команде паролем является 1234, а 0001 команда на сброс R3000.

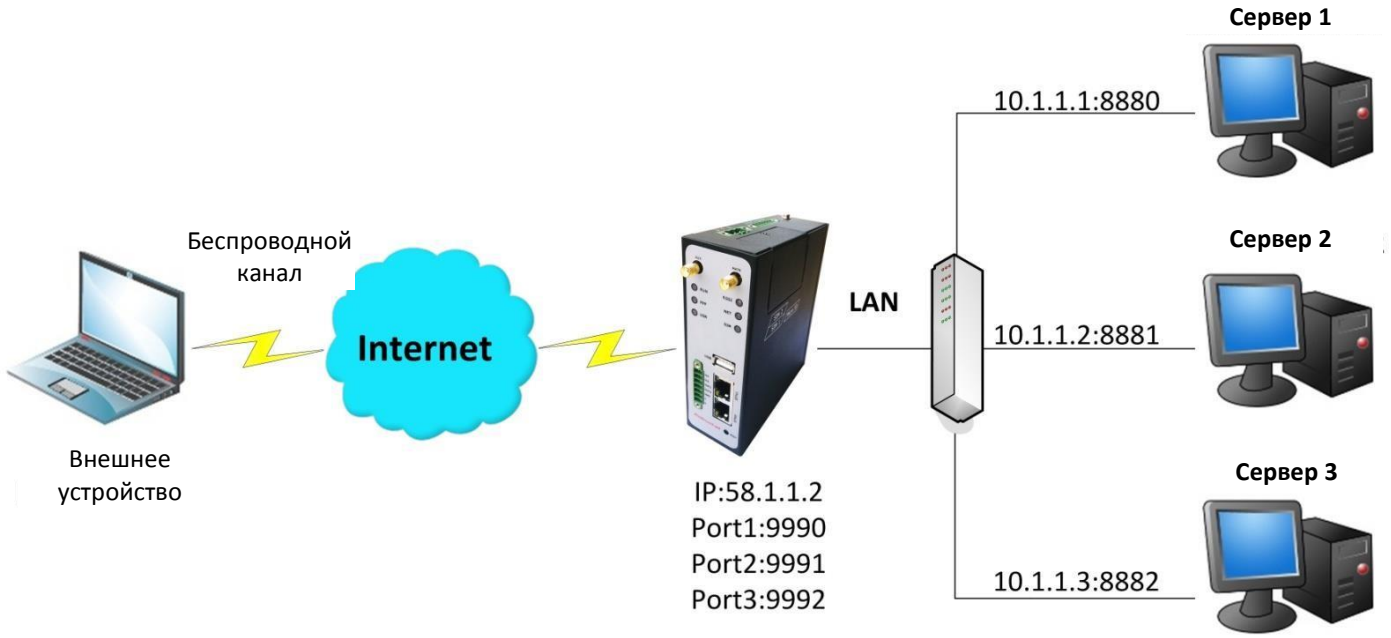
Cmd	Описание	Синтаксис	Комментарии
Команды управления			
0001	Сброс устройства	cmd	если пароль отсутствует, следует использовать команду cmd или — при использовании пароля: password: cmd cmd1 + cmd2: cmd1;cmd2 * - значение может быть нулевым
0002	Сохранить параметры	cmd	
0003	Сохранить параметры и перезагрузить устройство	cmd	
0004	Запустить соединение PPP	cmd	
0005	Остановить PPP	cmd	
0006	Переключить SIM-карту	cmd	
0007	Разрешить/Запретить счетчик событий	cmd,channel,flag	channel (канал): 1 - DI_1 2 - DI_2 flag (флаг): 0 - отключено 1 - включено
0008	Получить значение счетчика событий	cmd,channel	channel (канал): 1 - DI_1 2 - DI_2
0009	Очистить счетчик событий	cmd,channel	channel (канал): 1 - DI_1 2 - DI_2
0010	Очистить ограничение данных SIM-карты	cmd, simNumber	simNumber: 1 - SIM_1 2 - SIM_2

4.3 Сеть

4.3.1 NAT

В этом разделе показано, как настроить конфигурацию NAT маршрутизатора.

Параметр Remote IP (удаленный IP) определяет, разрешен ли доступ к маршрутизации к переадресованному IP порту по WAN IP и Arrives At Port.



Configuration--->NAT/DMZ--->Port Forwarding

Port Forwarding

Remote IP	Arrives At Port	Is Forwarded to IP Address	Is Forwarded to Port	Protocol	
58.1.1.1	9990	10.1.1.1	8880	TCP	X
58.1.1.1	9991	10.1.1.2	8881	UDP	X
58.1.1.1	9992	10.1.1.3	8882	TCP&UDP	X

**Remote IP: 1.1.1.1, 1.1.1.0/24,1.1.1.1-2.2.2.2, 0.0.0.0 means any*

Add

**Arrives At Port: <1-65536> or <1-65536>-<1-65536>*

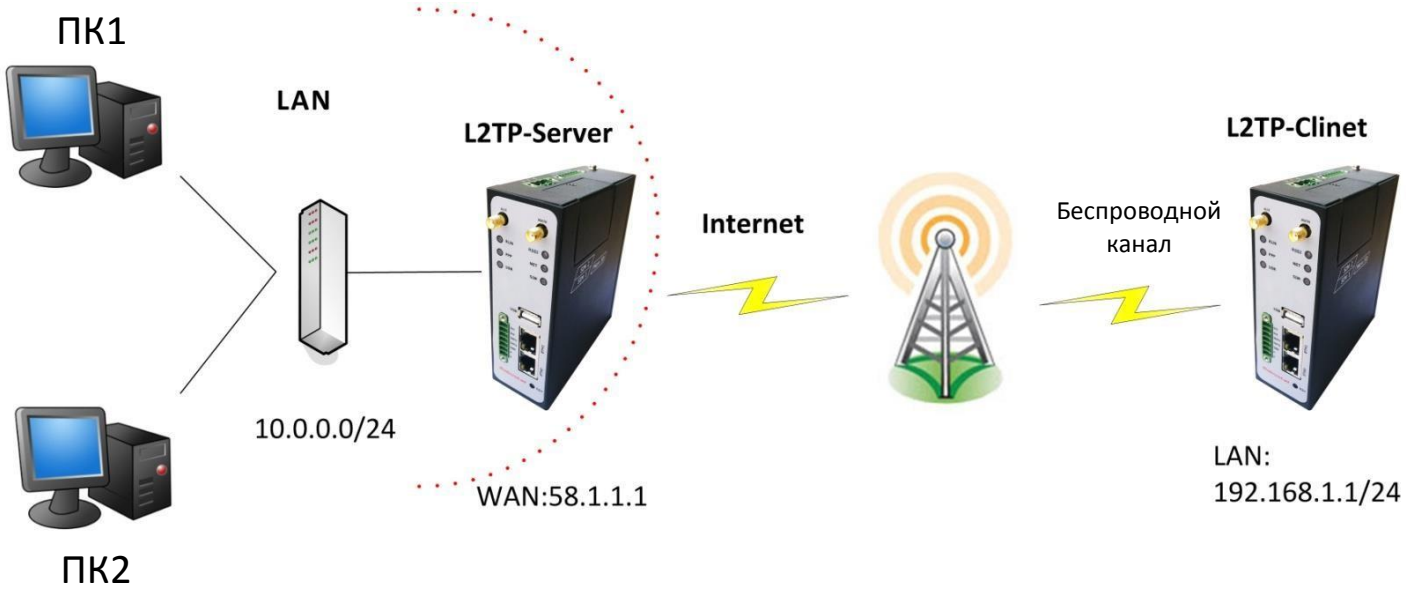
Примечание: *Этот раздел будет скрыт, если пользователь выберет Cellular в качестве основного и при сбое использования Eth0 в Configuration ->Link Management.*

Пояснения к вышеприведенной схеме:

Если для внешних устройств имеются два IP-адреса 58.1.1.1 и 59.1.1.1, результат будет отличаться от теста, когда NAT работает на R3000.

58.1.1.1----------access to--------->58.1.1.2:9990----------be forwarded to------->10.1.1.1:8000 TCP
58.1.1.1----------access to--------->58.1.1.2:9991----------be forwarded to------->10.1.1.2:8001 UDP
58.1.1.1----------access to--------->58.1.1.2:9992----------be forwarded to------->10.1.1.3:8002 TCP&UDP

4.3.2 L2TP



L2TP_SERVER:

Configuration-->L2TP-->L2TP Server (Конфигурация--> L2TP--> Сервер L2TP)

Enable L2TP Server

Enable L2TP Server

Установить отметку Enable L2TP Server (разрешить сервер L2TP) и заполнить пустые текстовые поля.

L2TP Common Settings

Username:	l2tp	1
Password:	••••	2
Authentication:	PAP	3
Enable Tunnel Authentication		
Local IP:	10.1.2.1	
IP Pool Start:	10.1.2.2	
IP Pool End:	10.1.2.254	

L2TP Server Advanced

Show L2TP Server Advanced

Route Table List

Client IP	Remote Subnet	Remote Subnet Mask	
0.0.0.0	192.168.1.0	255.255.255.0	X

"0.0.0.0" means any

Add

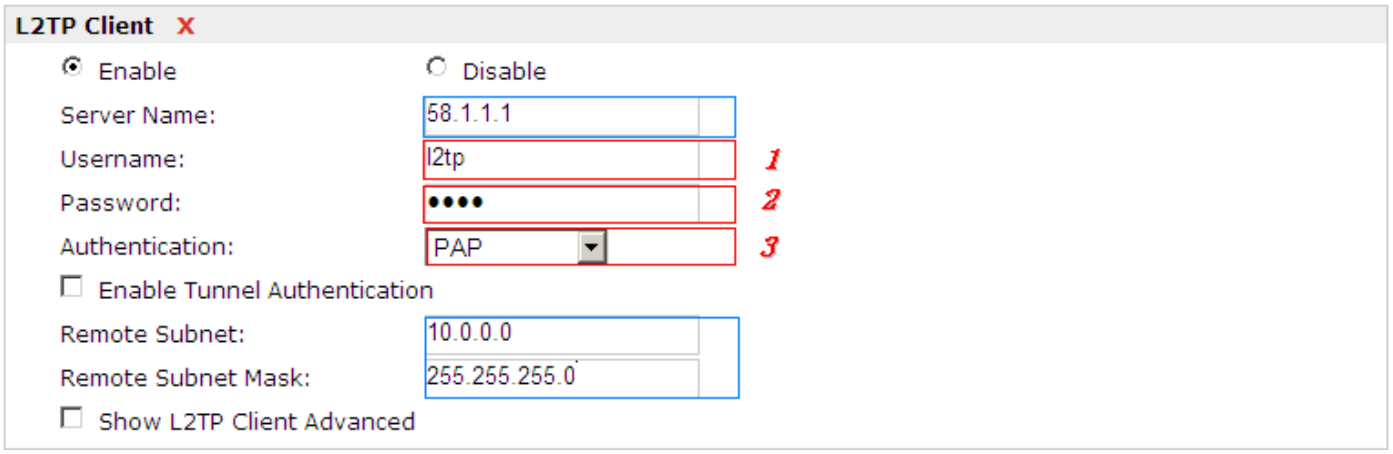
Изменения вступят в силу после *Apply --> Save --> Reboot*.

Примечание: *на следующих примерах номера красного цвета означают необходимость соответствия между сервером и клиентом, а синие номера подразумевают локальные установки для туннеля.*

L2TP_CLIENT:

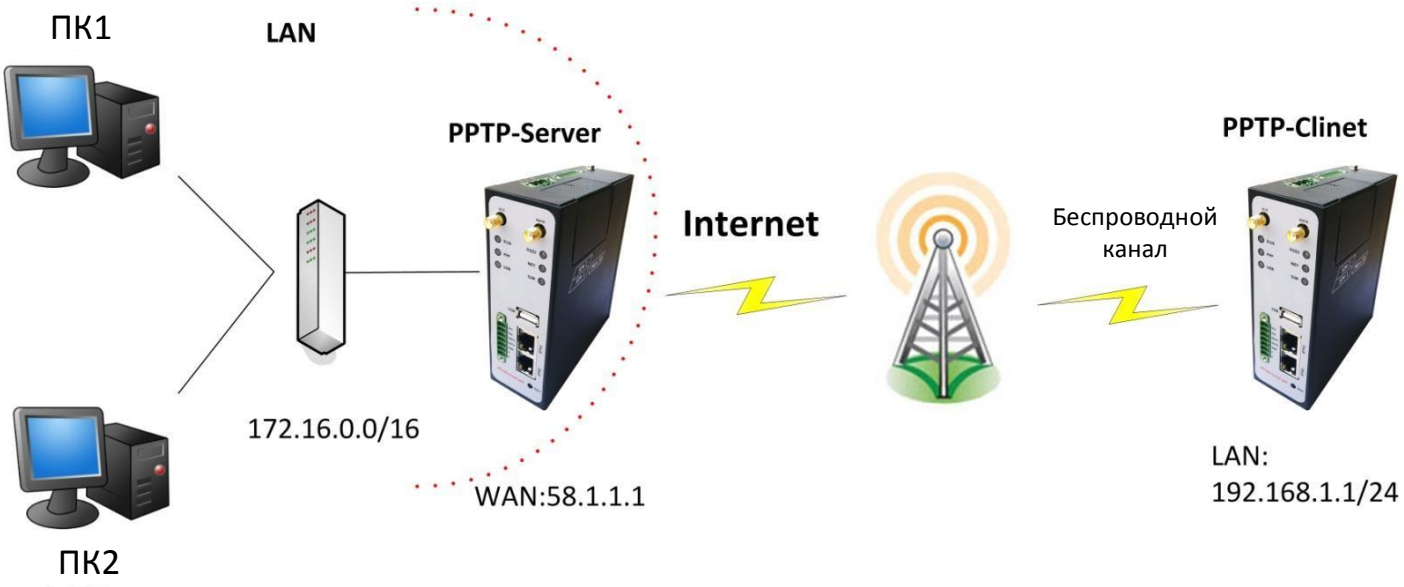
Configuration--->L2TP--->L2TP Client

Нажать кнопку Add (Добавить) и заполнить пустое текстовое поле



Изменения вступят в силу после *Apply --> Save --> Reboot*.

4.3.3 PPTP

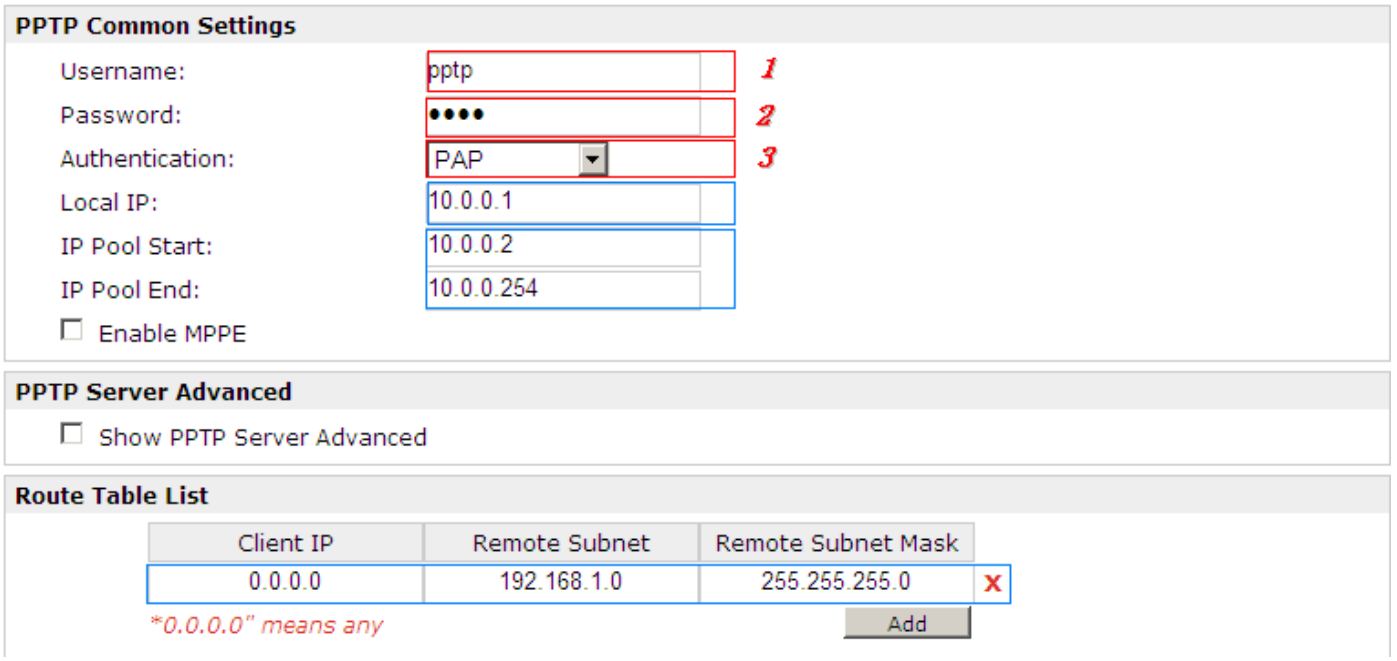


Примечание: *на следующих примерах номера красного цвета означают необходимость соответствия между сервером и клиентом, а синие номера подразумевает локальные установки для туннеля.*

PPTP_SERVER:

Configuration--->PPTP--->PPTP Server

Установить отметку Enable PPTP Server и заполнить пустые текстовые поля.

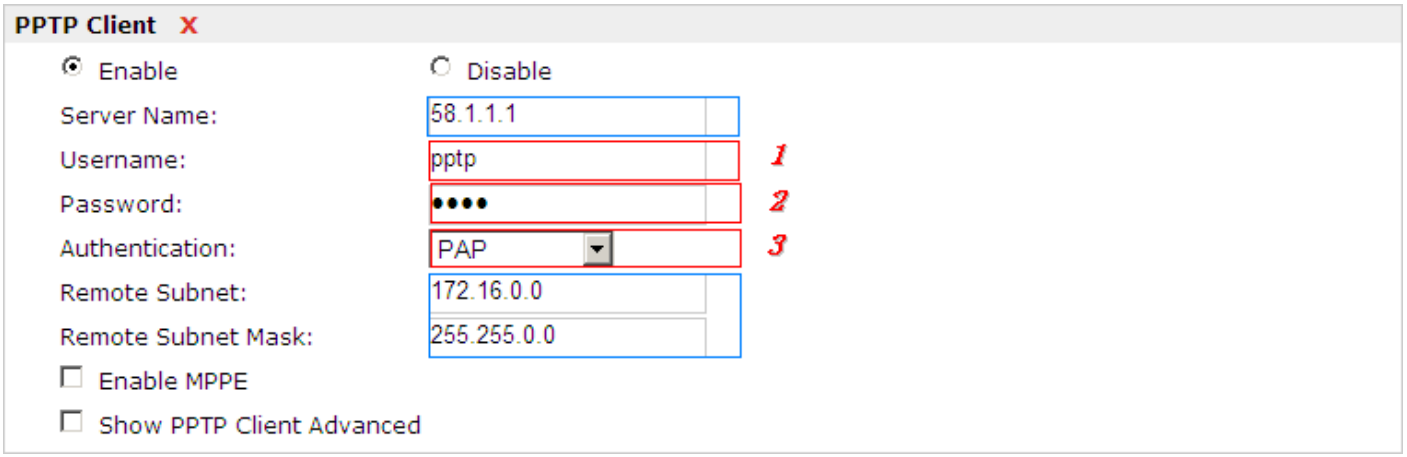


Изменения вступят в силу после *Apply --> Save --> Reboot*.

PPTP_CLIENT:

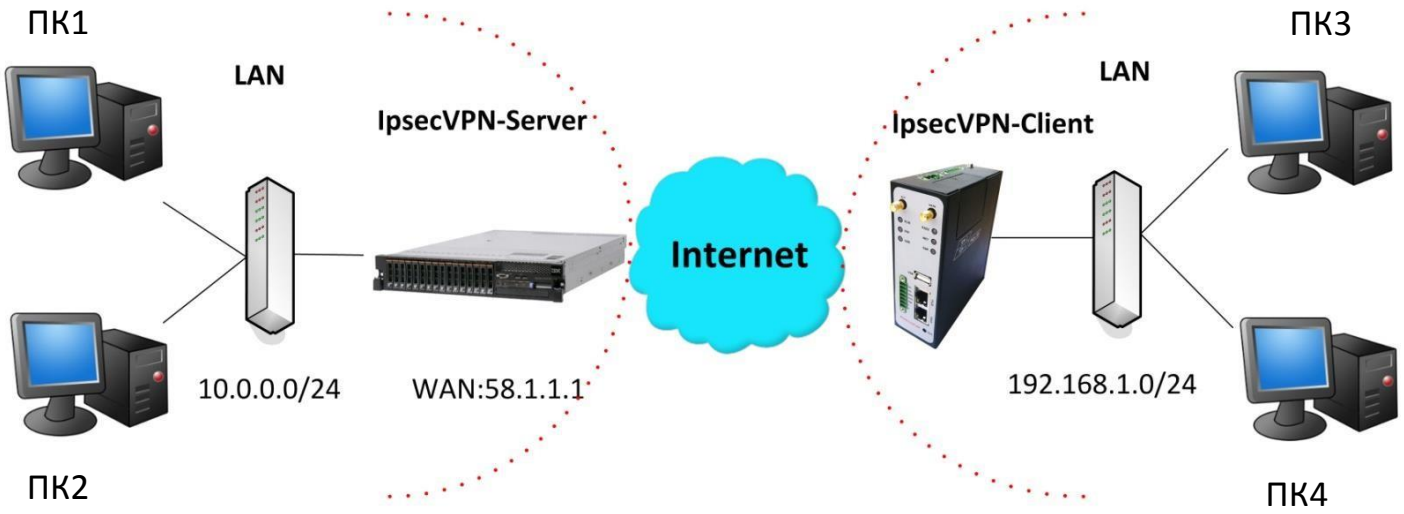
Configuration--->PPTP--->PPTP Client

Нажать кнопку *Add* и заполнить пустое текстовое поле



Изменения вступят в силу после *Apply --> Save --> Reboot*.

4.3.4 IPSEC VPN



Примечание: *на следующих примерах номера красного цвета означают необходимость соответствия между сервером и клиентом, а синие номера подразумевает локальные установки для туннеля.*

IPsecVPN_SERVER:

Cisco 2811:

```
crypto isakmp policy 10
 encr aes 256                                   8
 hash md5                                       9
 authentication pre-share                       11
 group 2                                        10
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
                                12
!
crypto ipsec transform-set trans esp-3des esp-md5-hmac   2, 13
!
crypto dynamic-map dyn 10
  set transform-set trans
  match address 101
!
crypto map map1 10 ipsec-isakmp dynamic dyn
!
interface FastEthernet0/0
  crypto map map1
!
access-list 101 permit ip 10.0.0.0 0.0.0.255 any   3, 5
!
```

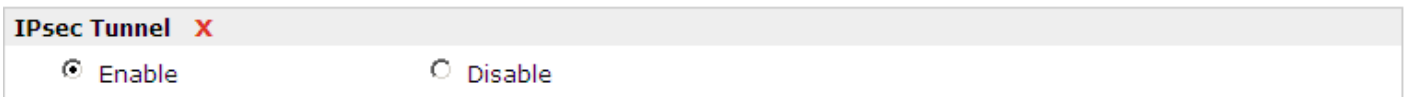
Примечание: *политики 1,4,6,7 приняты по умолчанию для маршрутизатора Cisco и не отображаются в CMD.*

IPsecVPN_CLIENT:

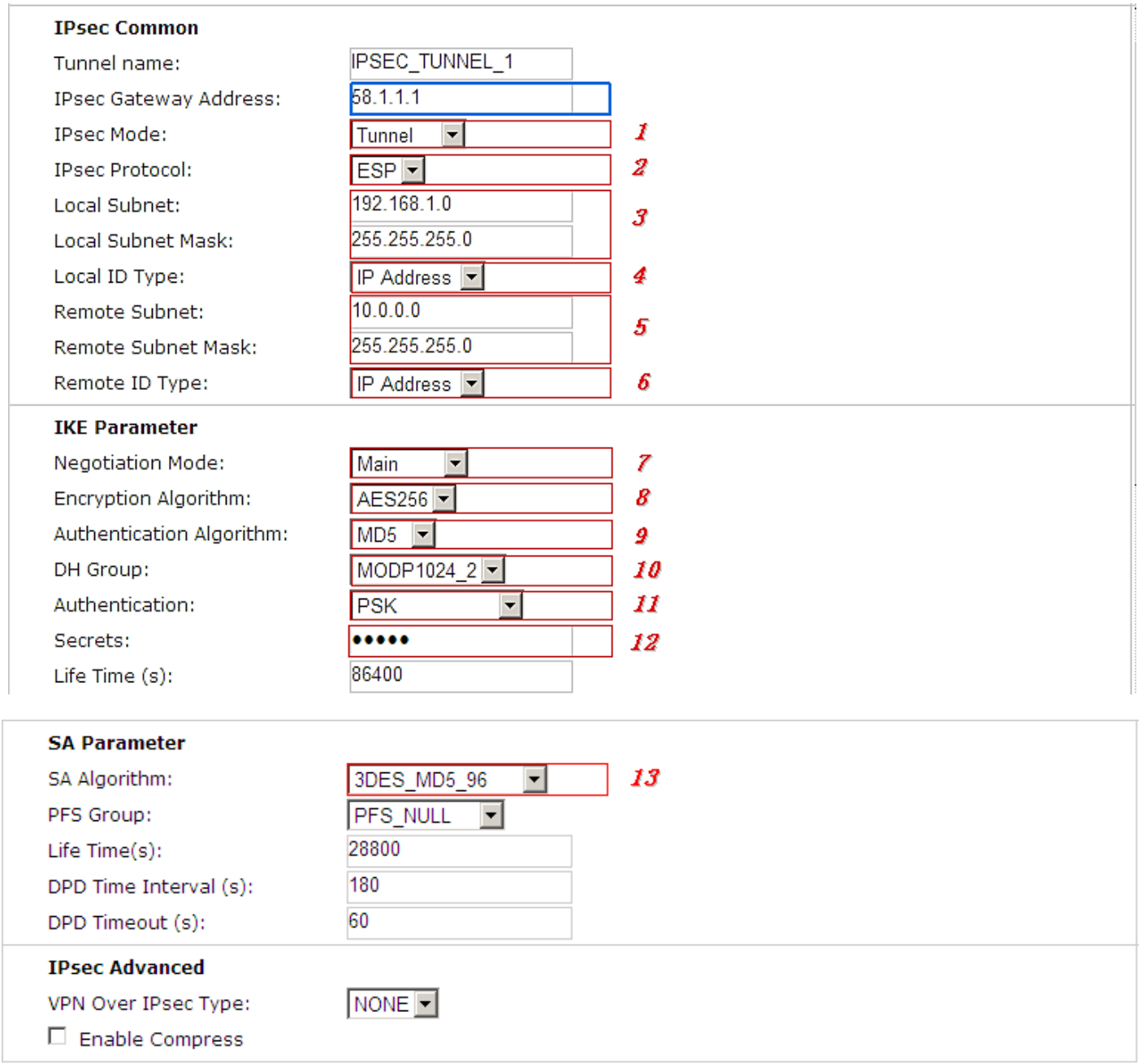
Configuration--->IPSec--->IPSec Basic

Затем щелкнуть *Apply*.

Configuration--->IPSec--->IPSec Tunnel

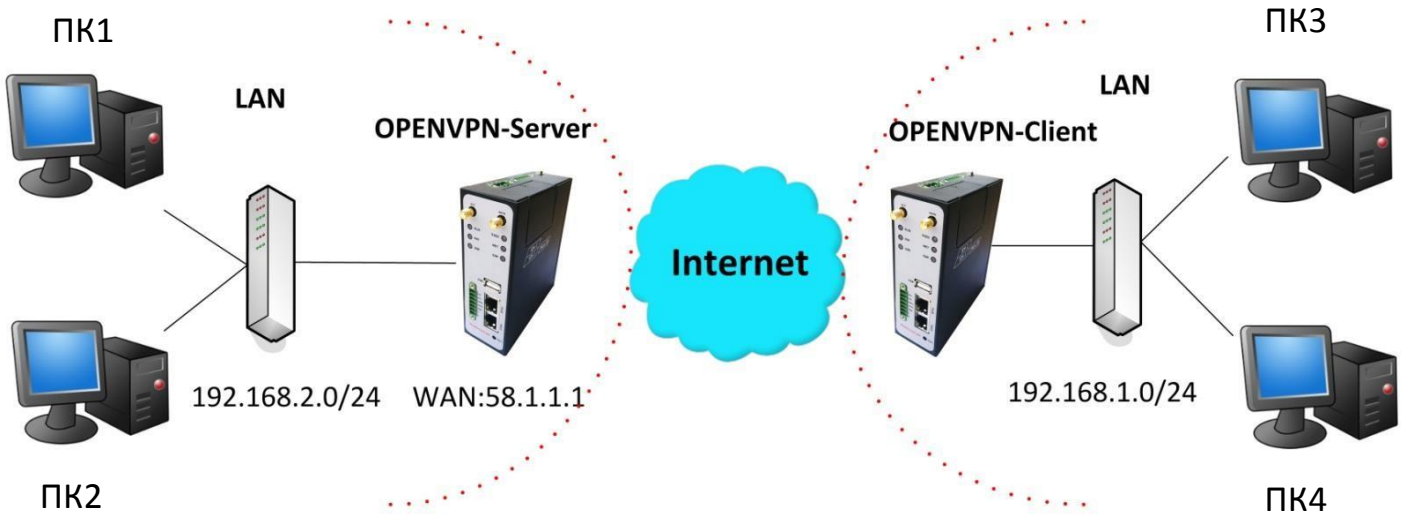


Установить отметку Enable IPSec Tunnel1



Изменения вступят в силу после *Apply --> Save --> Reboot*.

4.3.5 OPENVPN

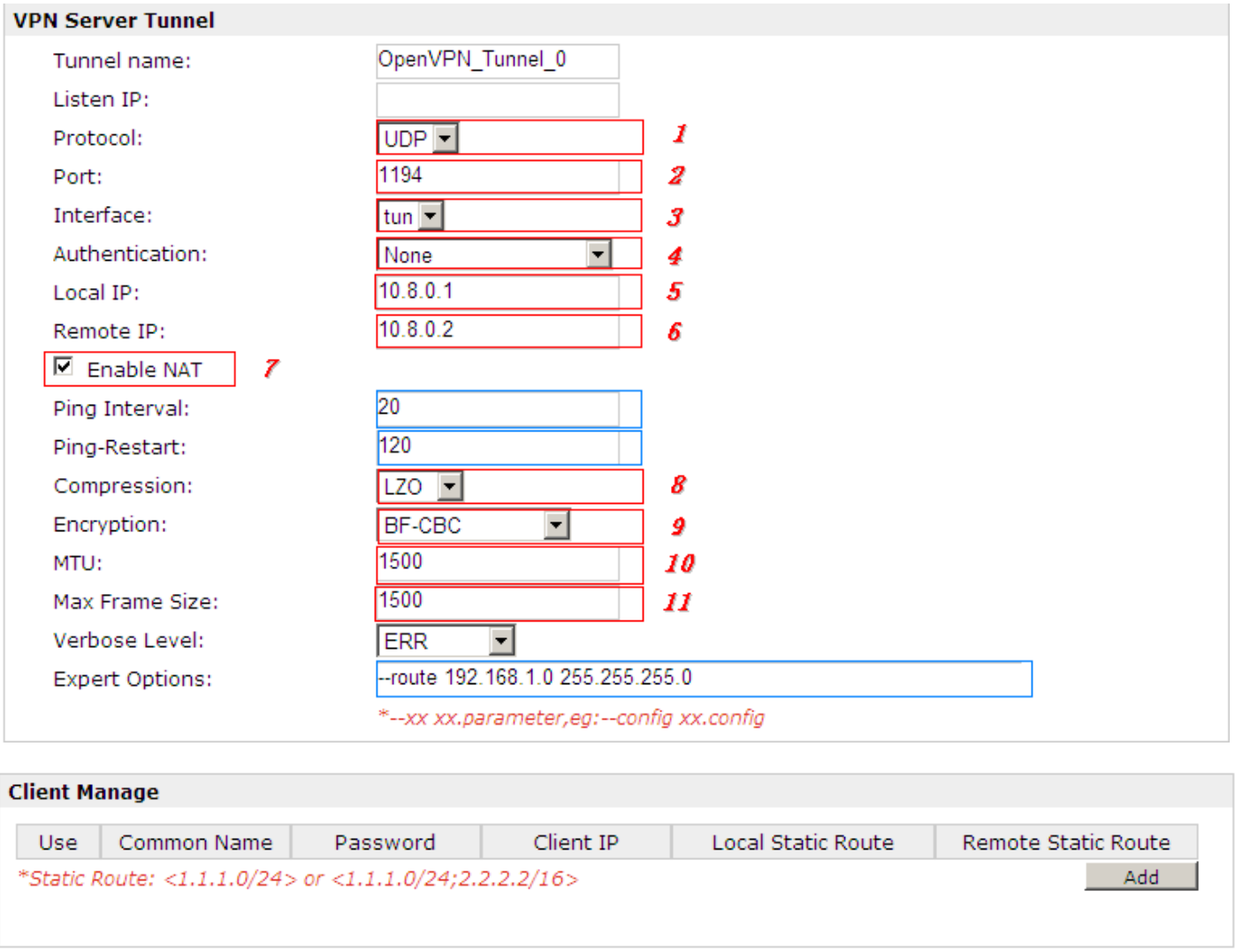


Примечание: *на следующих примерах номера красного цвета означают необходимость соответствия между сервером и клиентом, а синие номера подразумевает локальные установки для туннеля.*

OPENVPN_SERVER:

Configuration--->OpenVPN--->Server

Отметить Enable OpenVPN Server.

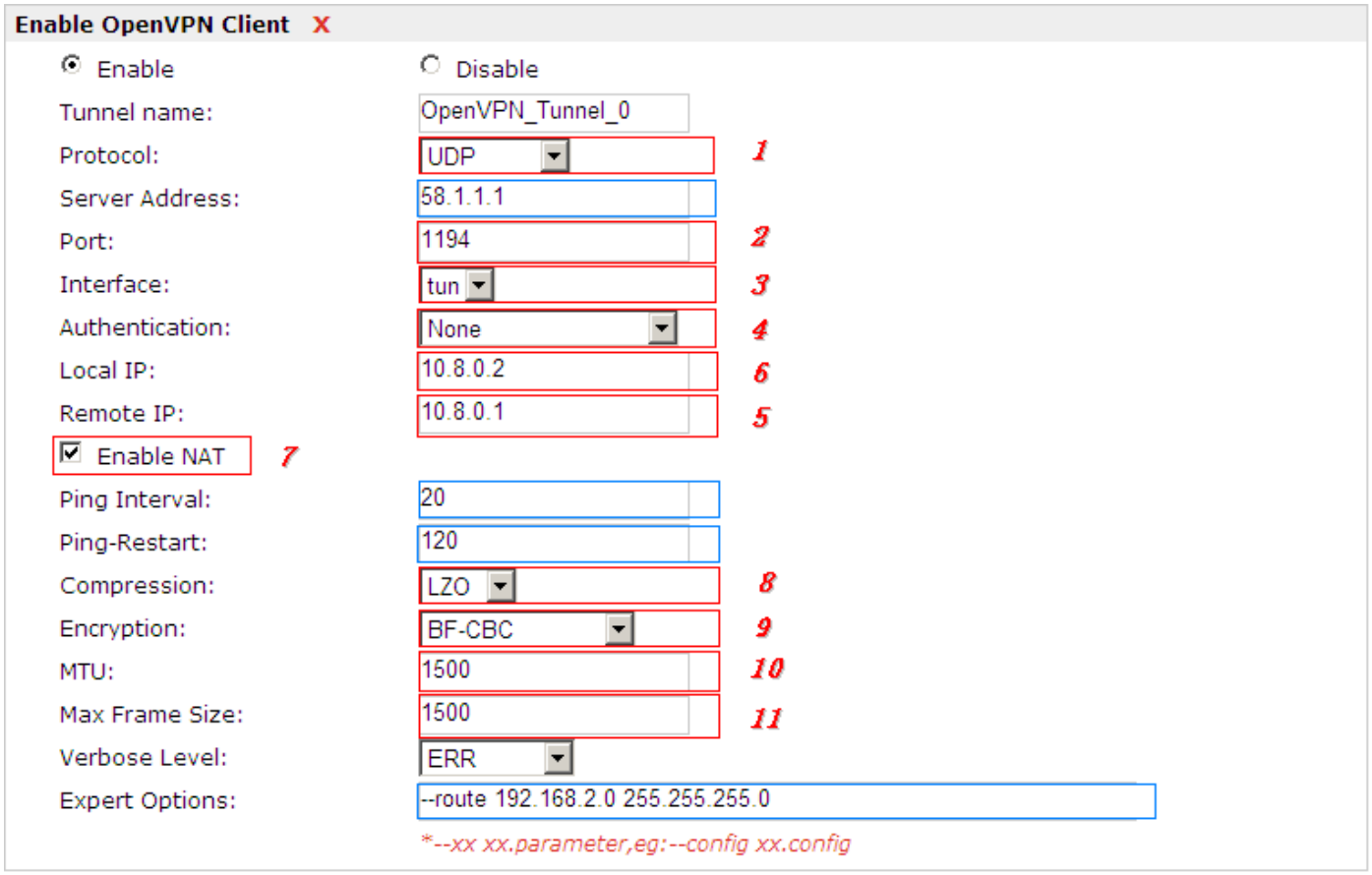


Изменения вступят в силу, после щелчка на Apply-> Save-> Reboot (Перезагрузка).

OPENVPN_CLIENT:

Configuration--->OpenVPN--->Client

Установить отметку Enable OpenVPN Client1 и заполнить пустое текстовое поле.



Изменения вступят в силу после *Apply --> Save --> Reboot (Перезагрузка)*.

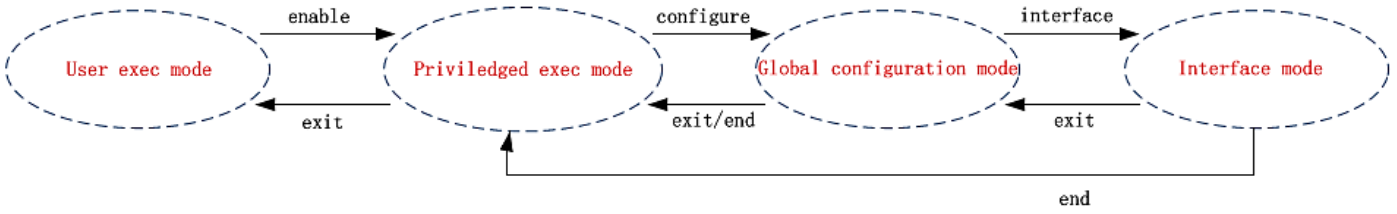
Глава 5 Введение в CLI

5.1 Что такое CLI и иерархические уровни режимов

Интерфейс командной строки — command-line interface (CLI) R3000 является программным интерфейсом, предоставляющим особый способ настройки параметров оборудования из консоли или по сетевому соединению telnet. Перед использованием, желательно рассмотреть некоторые подробности, которые будут представлены на четырех разных иерархических уровнях режима CLI, имеющих разные права доступа:

- User exec mode — приглашение на ввод команды «>» указывает на пользовательский режим (user mode). В этом режиме пользователю доступно использование только некоторых простых команд для просмотра текущей конфигурации и статуса устройства или ввода команды ping для поиска неисправностей сетевых соединений.
- Режим Privileged exec mode — приглашение командной строки изменяется на «#». Теперь, помимо вышеуказанного, пользователю разрешен импорт и экспорт файлов, системный журнал, отладка и т.п.
- Режим Global configuration — приглашение меняется на «<config>#», пользователю разрешено добавлять, настраивать и удалять текущую конфигурацию.
- Режим Interface mode — приглашение «<config-xx>» позволяет настроить IP-адрес и mtu для текущего интерфейса.

Ниже на схеме показано, как соотносятся описанные режимы и как получить доступ/выйти из каждого из них:



USER EXEC MODE:

R3000 Configure Environment

Username: admin

Password: *****

R3000> ?	//проверка: какие команды можно использовать в режиме **user exec mode**
enable	Включить привилегированные операторы
exit	Выход из текущего режима
ping	Эхо-тестирование
reload	Останов и выполнение «холодного» перезапуска
tracert	Тест Tracert
show	Показать информацию о работе системы

PRIVILEDGED EXEC MODE:

R3000> enable

Password: *****

R3000#?	//проверка: какие команды можно использовать в режиме Privileged exec mode
debug	Отладочная информация о конфигурации
enable	Включить привилегированные операторы
exit	Выход из текущего режима
export	Экспортировать файл через tftp
syslog	Экспортировать системный журнал
import	Импортировать файл с tftp
load	Загрузить информацию о конфигурации
ping	Эхо-тестирование
reload	Останов и выполнение «холодного» перезапуска
tracert	Тест Tracert
write	Записать исполняемую конфигурацию
tftp	Копировать с tftp: в файловую систему
show	Показать информацию о работе системы
configure	Войти в режим конфигурирования
end	Выйти в обычный режим

РЕЖИМ КОНФИГУРИРОВАНИЯ:

R3000# configure

R3000(config)# ? //проверить: какие команды доступны в global configuration

mode exit	выйти из текущего режима
end	выйти и перейти в Normal mode
interface	конфигурировать интерфейс
set	настроить параметры системы
add	добавить список параметров системы
modify	редактировать список параметров системы
delete	удалить список параметров системы

INTERFACE MODE:

R3000(config)# interface Ethernet 0

R3000(config-e0)# ? //проверить: какие команды доступны в interface mode

exit	Выйти из текущего режима
end	Выйти и перейти в Normal mode
ip	Задать IP-адрес интерфейса
mtu	Задать IP-адрес интерфейса

5.2 Как конфигурировать CLI

Ниже приводится описание справки, и возможные ошибки, которые могут встретиться в программе конфигурирования.

Команды/советы	Описание
?	Ввод вопросительного знака «?» вызовет справочную информацию.
Ctrl+c	Одновременное нажатие этих двух клавиш, помимо функции копирования, также может служить для выхода из программы настройки.
Invalid command “xxx”	Параметры «xxx» не поддерживаются системой, в этом случае ввод символа «?» вместо «xxx» поможет отыскать корректные в данном контексте параметры.
Incomplete command	Команда не завершена.
% Invalid input detected at '^' marker	«^» маркер указывает на местоположение ошибки.

***Примечание**: Большая часть настройки параметров производится в **Global configuration mode**. Для этого режима особое значение имеют команды **set** и **add**. Если какие-то параметры не удается найти в Global configuration mode, следует вернуться в режим **Privileged exec mode** или — в **Interface mode**.*
Предварительное понимание иерархических режимов CLI необходимо для конфигурирования CLI. При необходимости следует вернуться и ознакомиться с главой 5.

5.2.1 Быстрое начало работы с примерами конфигурации

Лучший и наиболее быстрый способ освоить CLI состоит в просмотре всех функций на веб-странице, затем — чтении обо всех командах CLI, и, наконец, следует освоить конфигурирование на примерах.

Пример 1: Показать текущую версию

```
R3000> show version
software version : 1.01.00
kernel version : v2.6.39
hardware version : 1.01.00
```

Пример 2: Обновление встроенного микропрограммное обеспечения через tftp

```
R3000> enable
Password: *****
R3000#
R3000# tftp 172.16.3.3 get rootfs R3k.1.01.00.02_130325

Tftp transfering tftp succeeded!downloaded
R3000# write            //сохранить текущую конфигурацию
Building configuration...
OK
R3000#reload
!Reboot the system?'yes'or 'no':yes    //перезагрузить для вступления в силу изменений
```

Пример 3: Set link-management (Задать управление соединением)

```
R3000> enable
Password: *****
```

```
R3000#
R3000# configure
R3000(config)# set link-management
wan link :
1.Cellular Only
2.Eth0 Only
3.Eth0 as primary and if fail use Cellular
4.Cellular as primary and if fail user Eth0
->please select mode(1-4)*1+:2          //Выбрать в качестве wan подключения Eth0 Only
->ICMP detection primary server[]:8.8.8.8
->ICMP detection second server[]:8.8.8.4
->ICMP detection interval(3-1800)[30]:
->ICMP detection timeout(1-10)[3]:
->ICMP detection retries(1-20)[3]:
->reset the interface?'yes'or'no'[no]:
 this parameter will be take effect when reboot!
really want to modify[yes]:
R3000# write  //Сохранить текущую конфигурацию Building configuration...
OK
R3000# reload
!Reboot the system ?'yes'or 'no':yes    //перезагрузить, чтобы изменения вступили в силу
```

Пример 4: Задать IP-адрес, шлюз и DNS для Eth0

```
R3000> enable
Password: *****
R3000#
R3000# show link-management          //Показать текущее администрирование связей
   ******************************************
   wan link : Eth0 Only            // теперь в качестве соединения WAN используется Eth0
   ICMP primary server : 8.8.8.8
   ICMP second server : 8.8.8.4
   ICMP detection interval : 30 seconds
   ICMP detection timeout : 3 seconds
   ICMP detection retries : 3
   reset the interface : no
******************************************

R3000 # configure
R3000 (config) # set eth0
ethernet interface type: WAN
type select:
  1. Static IP
  2. DHCP
  3. PPP0E
```

```
->please select mode (1-3) [1]:
->IP address [192.168.0.1]:58.1.1.1                //Задать IP адрес для eth0
->Netmask [255.255.255.0]:255.0.0.0
->gateway [192.168.0.254]:58.1.1.254               //Задать шлюз для eth0
->mtu value (1024-1500)[1500]:
->input primary DNS [192.168.0.254]:58.1.1.254          //Задать DNS для eth0
->input secondary DNS [0.0.0.0]:
 this parameter will be take effect when reboot!
really want to modify[yes]:
R3000 (config) # end
R3000# write   //Сохранение текущей конфигурации
Building configuration...
OK
R3000 # reload
! Reboot the system? 'yes' or 'no': yes //Перезагрузить для вступления в силу изменений
```

Пример 5: CLI для коммутируемого сотового доступа

```
R3000> enable
Password: *****
R3000#
R3000# show link-management

*******************************************
     wan link : Cellular Only       // здесь Cellular Only в качестве подключения WAN
    ICMP primary server : 8.8.8.8
    ICMP second server : 8.8.8.4
    ICMP detection interval : 30 seconds

    ICMP detection timeout : 3 seconds
    ICMP detection retries : 3
    reset the interface : no
  *******************************************
  R3000 (config) # set cellular
  1. set SIM_1 parameters
  2.  set SIM_2 parameters
->please select mode (1-2)[1]:
SIM 1 parameters:
network provider
  1. Auto
  2. Custom
  3.  china-mobile
->please select mode(1-3)[1]:
->dial out using numbers[*99***1#]:
->pin code[]:
```

connection Mode:

1. Always online
2. Connect on demand

->please select mode(1-2)[1]:

->redial interval(1-120)[30]:

->max connect try(1-60)[3]:

R3000(config)# end

R3000# write //сохранение текущей конфигурации

Building configuration...

OK

R3000# show cellular

****

Cellular enable : yes

1. show SIM_1 parameters
2. show SIM_2 parameters

->please select mode(1-2)[1]:

SIM 1 parameters:

network provider : Auto

dial numbers : *99***1#

pin code : NULL

connection Mode : Always online

redial interval : 30 seconds

max connect try : 3

main SIM select : SIM_1

when connect fail : yes

when roaming is detected : no

month date limitation : no

SIM phone number :

network select Type : Auto

authentication type : AUTO

mtu value : 1500

mru value : 1500

asyncmap value : 0xffffffff

use peer DNS : yes

primary DNS : 0.0.0.0

secondary DNS : 0.0.0.0

address/control compression: yes

protocol field compression: yes

expert options : noccp nobsdcomp

****

R3000# reload

!Reboot the system ?'yes'or 'no':yes //перезагрузить, чтобы изменения вступили в силу

5.3 Справка по командам

Команда	Синтаксис	Описание
Debug	Debug *parameters*	Включить или выключить функцию отладки
Export	Export *parameters*	Экспорт сертификатов vpn ca
Import	Import *parameters*	Импорт сертификатов vpn ca
Syslog	syslog	Экспорт информации журнала на tftp сервер
Load	Load default	Восстановление значений по умолчанию
Write	Write	Сохранение текущих параметров конфигурации
tftp	Tftp *IP-address* get {cfg|rootfs} *file-name*	Импорт файла конфигурации или обновление встроенного микропрограммного обеспечения через tftp
Show	Show *parameters*	Показать текущую конфигурацию каждой функции, если необходимо отобразить все, следует использовать show running
Set Add	Set *parameters* Add *parameters*	Добавление параметров. Все параметры функций задаются командами set, и добавляются командами add, их различие в том, что set служит для единичного параметра, а add — для списка параметров.