Руководство пользователя

R2000

Промышленный VPN маршрутизатор с поддержкой двух SIM карт

robustOS

Компания «Guangzhou Robustel LTD»
www.robustel.com

Об этом документе

В настоящем документе представлена информация об аппаратном и программном обеспечении промышленного маршрутизатора Robustel R2000, включая введение, информацию об установке, конфигурировании и эксплуатации.

Торговые марки и разрешения

, являются торговыми марками компании «Guangzhou Robustel LTD». Все остальные торговые марки и торговые наименования, упомянутые в настоящем документе, являются собственностью соответствующих владельцев.

Заявление об ограничении ответственности

Запрещается воспроизводить какую-либо часть настоящего документа в любой форме без письменного разрешения владельца авторского права.

Содержание настоящего документа может быть изменено без уведомления в связи с постоянным совершенствованием технологий, разработки и производства. Компания «Robustel» не несет ответственности за какие-либо ошибки или ущерб любого рода, возникающие в результате использования настоящего документа.

Важное примечание

Принцип беспроводной связи не позволяет гарантировать передачу и прием данных в любых условиях. Возможна задержка данных, их повреждение (т.е. появление в них ошибок) или полная потеря. При использовании таких беспроводных устройств, как маршрутизатор, если они используются надлежащим образом и в составе правильно построенной сети, значительные задержки и потеря данных происходят редко, однако, не следует использовать маршрутизатор в ситуациях, когда невыполнение передачи или приема данных может привести к причинению пользователю или третьей стороне ущерба какого-либо рода, включая, в частности, травмирование, летальный исход или потерю имущества. Компания «Robustel» не несет ответственности за ущерб любого роба, возникший вследствие задержек или ошибок в данных, переданных или принятых с использованием маршрутизатора, а также за неспособность маршрутизатора передать или принять такие данные.

Меры предосторожности

Общие сведения

- Маршрутизатор вырабатывает радиочастотную (РЧ) энергию. При использовании маршрутизатора необходимо обращать внимание на вопросы безопасности, связанные с РЧ-помехами, а также на нормативные документы, относящиеся к РЧ-оборудованию.
- Запрещается использовать маршрутизатор в самолетах, больницах, на бензозаправочных станциях, а также в местах, где использование сотового оборудования запрещено.
- Убедитесь, что маршрутизатор не создает помех для находящегося поблизости оборудования. Например, для кардиостимуляторов или медицинского оборудования. Запрещается размещать антенны маршрутизатора вблизи компьютеров, офисного оборудования, бытовых электроприборов и т.д.
- Для надлежащей работы маршрутизатора к нему необходимо подключить внешнюю антенну. С маршрутизатором следует использовать только антенны, одобренные для применения. По вопросам выбора одобренной антенны обращайтесь к уполномоченному поставщику.
- Антенна должна располагаться на безопасном расстоянии от тела человека – не менее 20 см. Запрещается размещать антенну внутри металлических коробок, контейнеров и т.д.
- Предупреждения о воздействии РЧ
    1. Для мобильных устройств без совместного размещения (передающая антенна устанавливается или размещается на расстоянии более 20 см от пользователя и других лиц, находящихся поблизости)
- Предупреждения Федеральной комиссии по связи (ФКС) США о воздействии РЧ-излучения
    1. Запрещается размещать или эксплуатировать передатчик совместно с любой другой антенной или передатчиком.
    2. Оборудование соответствует ограничениям ФКС на воздействие РЧ-излучения, установленным для неконтролируемых сред. Оборудование следует устанавливать и эксплуатировать, соблюдая расстояние не менее 20 см между излучателем и телом человека.

Примечание. Некоторые авиакомпании разрешают использование сотовых телефонов, пока самолет находится на земле с открытой дверью. Использование маршрутизатора в этих условиях разрешается.

Использование маршрутизатора в транспортном средстве

- Прежде чем устанавливать маршрутизатор, изучите местные нормативные документы или законы, касающиеся использования устройств сотовой связи в транспортных средствах.
- Водителю или оператору транспортного средства запрещается работать с маршрутизатором во время движения.

- Установка маршрутизатора должна выполняться квалифицированным персоналом. Проконсультируйтесь с поставщиком транспортного средства относительно помех, которые могут создаваться для электронных компонентов маршрутизатором.
- Маршрутизатор следует подключать к системе электропитания транспортного средства через защищенный предохранителем разъем в блоке предохранителей транспортного средства.
- В случае питания маршрутизатора от основного аккумулятора автомобиля необходимо соблюдать осторожность. Через продолжительное время аккумулятор может разрядиться.

Защита маршрутизатора

Чтобы обеспечить бесперебойное использование, при установке и эксплуатации маршрутизатора необходимо соблюдать осторожность. Обратите внимание на следующее:

- Запрещается эксплуатация маршрутизатора в экстремальных условиях: при повышенной влажности или в дождь, при повышенной температуре, на прямом солнечном свету, в присутствии едких или агрессивных химикатов, пыли или воды.
- Запрещается предпринимать попытки разобрать маршрутизатор или внести изменения в его конструкцию. В этом случае гарантия аннулируется, так как внутри маршрутизатора детали, обслуживаемые пользователем, отсутствуют.
- Избегайте падений, ударов и тряски маршрутизатора. Запрещается использовать маршрутизатор в условиях сильной вибрации.
- Запрещается тянуть за антенну или силовой кабель. При подключении и отключении придерживайте кабель за соединительный узел.
- Подключайте маршрутизатор только в соответствии с руководством пользователя. Несоблюдение этих требований приведет к аннулированию гарантии.
- В случае возникновения вопросов обращайтесь к уполномоченному поставщику.

Заявление Федеральной комиссии по связи (ФКС) о помехах

Данное устройство соответствует требованиям Части 15 Правил ФКС. Работа устройства соответствует двум условиям: (1) Данное устройство не может производить вредоносные помехи, а также (2) данное устройство должно принимать любые поступающие помехи, в т.ч. помехи, которые могут вызывать нежелательные процессы.

Данное оборудование прошло испытание, в результате которого установлено его соответствие ограничениям для цифрового устройства класса B согласно Части 15 Правил ФСК. Данные ограничения предназначены для обеспечения необходимой защиты от вредных помех на жилом объекте. Данное оборудование генерирует, использует и может излучать радиочастотную энергию и, без надлежащей установки и при нарушении инструкций, может вызывать вредные помехи в радиосвязи. Однако это не гарантирует отсутствие помех на конкретном объекте. Если данное оборудование вызывает вредные помехи в приеме радио- или телесигнала, что может быть установлено при включении и выключении этого оборудования, пользователю следует произвести коррекцию помех, приняв одну из следующих мер:

- изменить ориентацию или местоположение приемной антенны;
- усилить разделение между оборудованием и приемником;
- подключить оборудование к одному из выходов цепи, кроме того, к которому подключен приемник;
- Для получения поддержки проконсультируйтесь с дилером или с опытным техническим специалистом по радио/ТВ технологиям.

Предостережение ФКС:

- Любые изменения или модификации, прямо не одобренные ответственной стороной на предмет соответствия, могут лишить пользователя права на эксплуатацию данного оборудования.
- Запрещается размещать или эксплуатировать передатчик совместно с любой другой антенной или передатчиком.

Информация о нормативах и сертификатах соответствия

Таблица 1. Директивы

2011/65/EU	Европейская директива RoHS2.0 2011/65/EU была издана Европейским парламентом и Европейским советом 1 июля 2011 г. и предусматривает ограничение использования определенных опасных веществ в производстве электрического и электронного оборудования.
2012/19/EU	Европейская директива WEEE 2012/19/EU была издана Европейским парламентом и Европейским советом 24 июля 2012 г. и содержит положения об обращении с о электрического и электронного оборудования.
2013/56/EU	Европейская Директива 2013/56/EU – директива об аккумуляторах, опубликованная в официальном издании ЕС 10 декабря 2013 г. Аккумулятор таблеточного типа, используемый в данном изделии, соответствует стандарту директивы 2013/56/EU.

Таблица 2. Стандарты электронной промышленности Китайской Народной Республики

SJ/T 11363-2006	Стандарт электронной промышленности Китайской Народной Республики SJ/T 11363-2006 «Требования к предельно допустимым концентрациям некоторых токсичных и опасных веществ в электронных изделиях для обработки информации», изданный Министерством информационной промышленности Китайской Народной Республики 6 ноября 2006 г., устанавливает максимально допустимые концентрации токсичных и опасных веществ в электронных изделиях для обработки информации. В **таблице 3** представлен обзор токсичных и опасных веществ и элементов, которые могут содержаться в деталях изделия в концентрациях, превышающих пределы, установленные стандартом SJ/T 11363-2006.
SJ/T 11364-2014	Стандарт электронной промышленности Китайской Народной Республики SJ/T 11364-2014 «Требования к маркировке ограниченного использования опасных веществ в электронных и электротехнических изделиях», изданный Министерством промышленности и информационных технологий Китайской Народной Республики 9 июля 2014 г., устанавливает требования к маркировке опасных веществ в электронных и электротехнических изделиях, предельно допустимые сроки экологически безопасного использования этих изделий и возможность их переработки. Этот стандарт распространяется на электронные и электротехнические изделия, продаваемые в Китайской Народной Республике, а также может использоваться в качестве справочного материала для логистических операций с электронными и электрот и изделиями. Логотип оранжевого цвета, представленный ниже, используется для изделий ко «Robustel»: Является атрибутом предупреждения, т.е. указывает, что в изделии содержатся некоторые опасные вещества. Цифра «10» в середине набора обозначений указывает срок экологически безопасного использования (СЭБИ)* электронного изделия для обработки информации, составляющий 10 лет. Изделие может использоваться безопасным образом на протяжении этого срока. По истечении срока экологически безопасного использования изделие следует

	направить на переработку. *Термин «экологически безопасное использование» в отношении электронных изделий для обработки информации означает срок, на протяжении которого, при нормальных условиях использования, токсичные и опасные вещества или элементы, содержащиеся в электронном изделии для обработки информации, не будут вытекать из него или видоизменяться и приводить к серьезному загрязнению окружающей среды или к серьезному ущербу для людей и имущества.

Таблица 3. Токсичные и опасные вещества и элементы с заданными предельными концентрациями

Название детали	Опасные вещества									
	(Свинец)	(Ртуть)	(Кадмий)	(Хром (VI))	(Полибромдифенил)	(Полибромистый дифенилэфир)	(Диэтилгексилфталат)	(Бутилбензилфталат)	(Дибутилфталат)	(Диизобутилфталат)
Металлические детали	o	o	o	o	-	-	-	-	-	-
Модули схемы	o	o	o	o	o	o	o	o	o	o
Кабели и кабельные узлы	o	o	o	o	o	o	o	o	o	o
Пластмассовые и полимерные детали	o	o	o	o	o	o	o	o	o	o

o:
Указывает, что содержание данного токсичного или опасного вещества, присутствующего во всех однородных материалах данной детали, ниже предела, установленного в Директиве RoHS2.0.
X:
Указывает, что содержание данного токсичного или опасного вещества, присутствующего, по меньшей мере, в одном из однородных материалов данной детали, *может превышать* предел, установленный в Директиве RoHS2.0.
-:
Указывает, что элемент не содержит токсичного или опасного вещества.

История изменений

Обновления между версиями документа являются суммарными. Поэтому актуальная версия документа содержит все изменения, внесенные в предыдущие версии.

Дата	Версия встроенного микропрограммного обеспечения	Версия документа	Описание изменения
24 августа 2016 г.	1.2.2	V2.0.0	Первый выпуск
31 августа 2016 г.	1.2.2	V2.0.1	• Изменение диапазона частот Дуплекса с частотным разделением каналов и дуплекса связи с временным разделением каналов согласно Стандарту «Долгосрочное развитие сетей связи» • Изменение данных EMC • Изменение номеров телефона и факса
8 октября 2016 г.	1.2.2	V2.0.2	Информация об обновленном диапазоне частот в главе 1.5 Другие незначительные изменения
11 ноября 2016 г.	1.2.2	V2.0.3	Обновленный раздел об электропитании 2.9
18 ноября 2016 г.	1.2.2	v.2.0.4	Обновленная информация о напряжении на входе
29 ноября 2016 г.	1.2.2	v.2.0.5	Обновленный раздел о выборе и запросе данных 1.5
19 января 2017 г.	1.2.2	v.2.0.6	• Измененный номер телефона +86-20-29019902 • Измененная информация о CD в главе 1.2 • Обновленный раздел о выборе и запросе данных 1.5
23 февраля 2017 г.	1.2.2	v.2.0.7	Добавлено примечание о подключении
24 июля 2017 г.	3.0.0	v.3.0.0	Обновление прошивки
21 октября 2017 г.	3.0.0	v.3.0.1	• Добавлена информация «Выходная мощность РЧ» для интерфейса WiFi • Добавлен новый сертификат: EAC • Добавлена новая модель продукта: R2000-NU • Обновлено изображение маршрутизатора • Обновлен сетевой протокол и приложение • Другие незначительные изменения
17 января 2018 г.	3.0.0	v.3.0.2	Обновлены диапазоны частот для модели 3G
28 июня, 2018 г.	3.0.0	v.3.0.3	Изменено название компании
12 декабря 2018 г.	3.0.0	v.3.0.4	Добавлено описание модуля BG96

22 января 2019 г.	3.0.0	v.3.0.5	• Добавлено описание прибора R2000-4M • Изменена информация о сертификации • Изменены полосы частот сети Wifi
14 февраля 2019 г.	3.0.0	v.3.0.6	• Добавлено Заявление Федеральной комиссии по связи (ФКС) о помехах
28 мая 2019 г.	3.0.0	v.3.0.7	• Внесены изменения в сведения о разрешениях • Внесены изменения в информацию о нормативных требованиях и утверждении типа
17 сентября 2019 г.	3.0.0	v.3.0.8	• Внесены изменения в сведения о разрешениях • Внесены изменения в информацию о нормативных требованиях и утверждении типа
25 ноября 2019 г.	3.0.0	v.3.0.9	• Внесены изменения в описание обновления встроенного ПО через tftp
4 марта 2020 г.	3.0.5	v.3.1.0	• Добавлена соответствующая информация об IPv6; • Внесены изменения в скриншот интерфейса ROS • Внесены изменения в описание параметров; • Внесены изменения в информацию о нормативных требованиях и утверждении типа • Внесены изменения в информацию об адресе шлюза IPsec VPN • Изменено максимальное количество операций фильтрации • Удалены некоторые неактуальные описания в спецификациях продукта

Содержание

Глава 1 Обзор изделия

1.1 Основные особенности

Промышленный сотовый VPN-маршрутизатор с поддержкой двух SIM карт Robustel (R2000) является надежным сотовым маршрутизатором, обеспечивающим самую современную мобильную связь для M2M (машина/машина) приложений.

R2000 – это мощный маршрутизатор на основе RobustOS, операционной системы собственной разработки компании «Robustel» на базе Linux и предназначенной для использования в устройствах компании «Robustel». RobustOS включает в себя базовые сетевые функции и протоколы, тем самым обеспечивая клиентам очень удобное взаимодействие с пользователем. Между тем, компания «Robustel» предлагает партнерам и клиентам набор инструментальных средств разработки программного обеспечения (SDK), позволяющий выполнять дополнительную настройку с использованием C, Python или Java. Она также предоставляет многофункциональные приложения для удовлетворения требований фрагментированного рынка Интернета вещей.

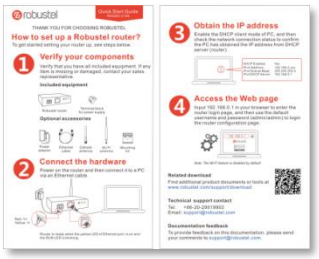
1.2 Содержание упаковки

Перед установкой маршрутизатора R2000 проверьте содержимое комплекта следующим образом.
Примечание. Следующие изображения представлены только в качестве иллюстрации и не отображают реальные размеры.

- 1 x промышленный сотовый VPN маршрутизатор Robustel R2000 с поддержкой двух SIM карт

- 1 x 3-контактная клеммная колодка со штекером 3,5 мм с блокировкой для источника питания

- 1 x *Руководство по быстрому запуску* со ссылкой для скачивания других документов или инструментов



Примечание: если что-либо из вышеперечисленного отсутствует или повреждено, обратитесь к торговому представителю компании «Robustel».

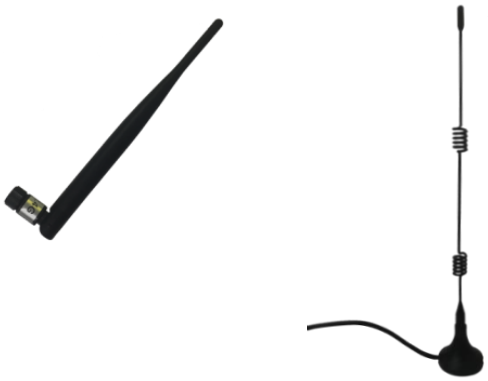
Дополнительные принадлежности (продаются отдельно)**:**

- Сотовая антенна 3G/4G с разъемом SMA (дополнительно короткая/магнитная)

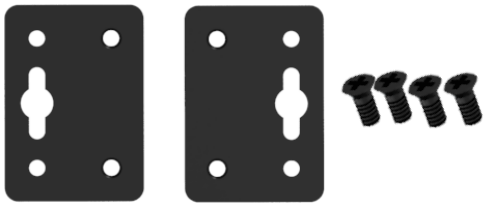
Короткая антенна Магнитная антенна

- WiFi антенна с разъемом RP-SMA (дополнительно короткая/магнитная)

Короткая антенна Магнитная антенна



- Комплект для монтажа к стене



- Комплект для монтажа на рейку 35 мм (DIN)

- Кабель Ethernet

- Адаптер питания перем./пост. тока (12 В пост. тока, 1,5 А; дополнительно вилка для ЕС/США/Соединенного Королевства/Австралии)

1.3 Спецификации

Сотовый интерфейс

- Количество антенн: 2 (ГЛАВНАЯ + ВСПОМОГАТЕЛЬНАЯ)
- Соединитель: SMA-K
- SIM: 2 (3,0 и 1,8 В)
- Стандарты: GSM/GPRS/EDGE/WCDMA/HSDPA/HSUPA/HSPA+/DC-HSPA+/TD-SCDMA/CDMA (CDMA 1X/EVDO)/FDD LTE/TDD LTE

Интерфейс Ethernet

- Количество портов: 2 x 10/100 Мбит/с, 2 x LAN или 1 x LAN + 1 x WAN
- Порт WAN: Поддержка 802.3 при свойстве PD (опционально)
- Магнитная изоляционная защита: 1,5 кВ

Интерфейс WiFi (дополнительно)

- Количество антенн: 2 (WiFi1 + WiFi2)
- Соединитель: RP-SMA-K
- Стандарты: 802.11b/g/n, поддержка режима точки доступа (AP) и клиентского режима
- Диапазоны частот: 2,4 ГГц
- Безопасность: WEP, WPA, WPA2

- Шифрование: 68/124 AES, TKIP
- Скорость передачи данных: 2*2 MIMO, 300 Мб/с

Другое

- 1 x кнопка RST
- Светодиодный индикатор - 1 x RUN, 1 x PPP, 1 x USR, 3 x RSSI
- Встроенная схема безопасности, таймер

Электропитание и потребление

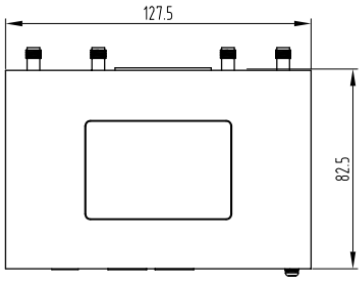
- Соединитель: 3-контактное гнездо 3,5 мм
- Входное напряжение: 9–36 В пост. тока
- Потребляемая мощность: Режим покоя: 100 мА при 12 В
  Канал передачи данных: 500 мА (пик) при 12 В
- Свойство PD* (опционально): порт WAN с поддержкой
  Напряжение на входе: 48~57 В пост. тока

**Не рекомендуется использовать источник питания пост. тока одновременно с источником питания PD.*

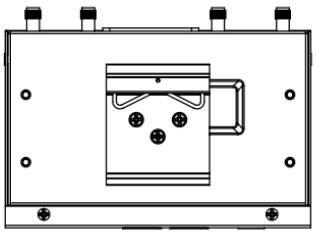
Физические характеристики

- Степень защиты: IP30
- Корпус и масса: металл, 305 г
- Габариты: 127,5 x 82,5 x 29,5 мм
- Места установки: стол, настенный монтаж или монтаж на рейку 35 мм (DIN)

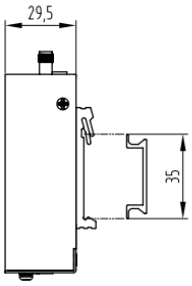
1.4 Размеры



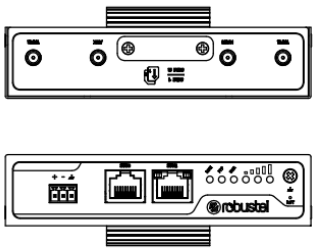
Вид спереди



Вид сзади



Вид сбоку



Вид сверху и снизу

Глава 2 Установка аппаратного обеспечения

2.1 Назначение контактов

PIN	Полярность
1	Положительно
2	Отрицательно
3	GND

2.2 Светодиодные индикаторы

Маршрутизатор R2000 был разработан для размещения на рабочем столе. Ниже показан вид снизу маршрутизатора R2000.

Name	Цвет	Статус	Описание
RUN	Зеленый	Включено, быстрое мигание (время мигания 250 мс)	Маршрутизатор включен (Система инициализируется)
		Включено, мигание (время мигания 500 мс)	Маршрутизатор начинает работать
		Off	Маршрутизатор выключен
PPP	Зеленый	Включено, постоянное мигание	Соединение работает
		Off	Соединение не работает

USR-SIM	Зеленый	Включено, мигание	Используется резервная карта
		Off	Используется основная карта
USR-NET	Зеленый	Включено, постоянное мигание	Сеть успешно подключается и функционирует на оптимальном режиме
		Включено, мигание	Сеть успешно подключается, но функционирует на меньшей мощности, нежели предусмотрено стандартом
		Off	Сеть не подключена или не поддерживает подключение
USR-OpenVPN	Зеленый	Включено, постоянное мигание	Установлено соединение OpenVPN
		Off	Не установлено соединение OpenVPN
USR-IPsec	Зеленый	Включено, постоянное мигание	Установлено соединение IPsec
		Off	Не установлено соединение IPsec
USR-WiFi	Зеленый	Включено, постоянное мигание	Wi-Fi включен и работает должным образом
		Off	Wi-Fi отключен и не работает должным образом
	Зеленый	Вкл. 3 немигающих световых сигнала	Доступен высокий уровень сигнала (21–31)
		Вкл., 2 немигающих световых сигнала	Доступен средний уровень сигнала (11–20)
		Вкл., 1 немигающий световой сигнал	Доступен низкий уровень сигнала (1–10)
		Off	Нет сигнала
		Включено, мигание	При отключении сети указанные три светодиодных индикатора функционируют как бинарный комбинационный код для подачи серии отчетов об ошибках. Мигающий Выкл.: 0 : 1 001 Команда AT не выполнена 010 SIM-карта не обнаружена 011 необходимо ввести PIN-код 100 необходимо ввести PUK-код 101 регистрация не выполнена 110 ошибка модуля 111 модуль не поддерживается

Примечание. Можно выбрать тип отображения светодиода USR. Дополнительные сведения см. в разделе **3.25 Сервис > Дополнительно**.

2.3 Кнопка Reset

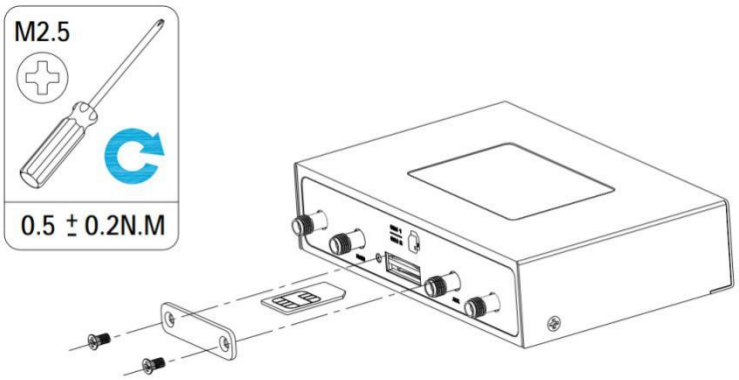
Функция	Работа
Reboot	Зажмите кнопку RST в течение 2–7 секунд в рабочем состоянии.
Восстановите заводские настройки по	Подождите 3 секунд после включения маршрутизатора, зажмите кнопку RST, пока все шесть светодиодов не начнут мигать один за другим, и отпустите кнопку, чтобы вернуть маршрутизатор к заводским настройкам по умолчанию.

2.4 Порт Ethernet

Маршрутизатор R2000 имеет два порта Ethernet, включая ETH0 и ETH1. Каждый порт имеет два светодиодных индикатора. Желтый индикатор является индикатором связи, а зеленый не имеет предусмотренного значения. Дополнительную информацию о статусе см. в таблице ниже.

Индикатор	Статус	Описание
Индикатор соединения	Включено, постоянное мигание	Соединение установлено
	Включено, мигание	Выполняется передача данных
	Off	Соединение не установлено

2.5 Вставьте или извлеките SIM-карту



Вставьте или извлеките SIM-карту, как показано в следующих шагах.

- **Вставьте SIM-карту**

1. Убедитесь, что маршрутизатор выключен.
2. Чтобы снять крышку гнезда, ослабьте винты, на крышке, с помощью отвертки, а затем найдите гнездо для SIM-карты.
3. Чтобы вставить SIM-карту, нажмите на карту пальцем, пока не услышите щелчок, а затем затяните винты на крышке с помощью отвертки.
4. Установить крышку и затянуть винты на крышке с помощью отвертки.

- **Извлечь SIM-карту**

1. Убедитесь, что маршрутизатор выключен.
2. Чтобы снять крышку гнезда, ослабьте винты, на крышке, с помощью отвертки, а затем найдите гнездо для SIM-карты.
3. Чтобы извлечь SIM-карту, нажмите на карту пальцем, пока она не выскочит, а затем извлеките карту.
4. Установить крышку и затянуть винты на крышке с помощью отвертки.

Примечание:

1. Рекомендуемый момент затяжки для вставки составляет 0,5 Н.м, а максимально допустимый – 0,7 Н.м.
2. Используйте специальную карту, когда устройство работает при экстремальных температурах (температура превышает 40 °C), потому что обычная карта для длительной работы в суровых условиях будет часто отключаться.
3. Обратите внимание, что крышку необходимо затянуть достаточно плотно, чтобы ее не смогли украсть.
4. Запрещается прикасаться к металлической поверхности карты, иначе информация на карте будет потеряна или уничтожена.
5. Запрещается сгибать и царапать карту.
6. Запрещается подвергать карту воздействию электричества или магнита.

7. Перед установкой или извлечением карты убедитесь, что маршрутизатор выключен.

2.6 Подключение внешней антенны (тип SMA)

Подключите внешнюю антенну типа SMA к разъему антенны маршрутизатора и плотно закрутите. Убедитесь, что антенна находится в правильном частотном диапазоне, указанном поставщиком услуг Интернета, и имеет сопротивление 50 Ом.

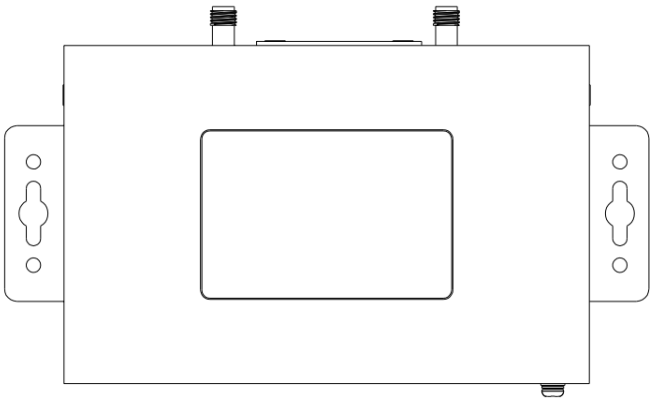
Примечание. Рекомендуемый момент затяжки составляет 0,35 Н.м.

2.7 Монтаж маршрутизатора

Маршрутизатор можно разместить на столе, закрепить на стене или на рейке 35 мм (DIN).

Монтаж маршрутизатора осуществляется двумя способами

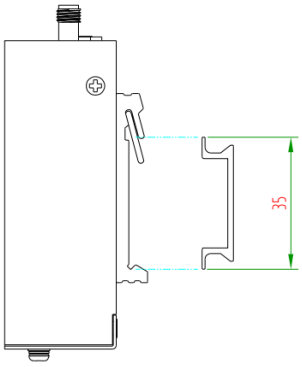
- Монтаж на стене (в мм)



Используйте 4 винта M2.5*4 с плоской головкой с крестообразным шлицем, чтобы прикрепить комплект для настенного монтажа к маршрутизатору, а затем используйте 2 винта M3 для гипсокартона, чтобы закрепить маршрутизатор с комплектом для настенного монтажа на стене.

Примечание: рекомендуемый момент затяжки для монтажа составляет 0,5 Н.м, а максимально допустимый – 0,7 Н.м.

- Монтаж на рейке (в мм)



Используйте 3 винта M3*6 с плоской головкой и крестообразным шлицем, чтобы прикрепить рейку (DIN) к маршрутизатору, а затем повесьте рейку (DIN) на монтажный кронштейн. Необходимо выбрать стандартный кронштейн.

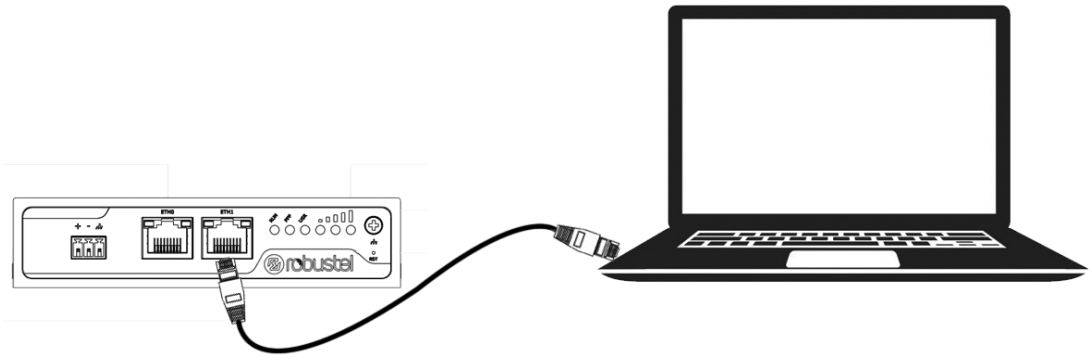
Примечание. Рекомендуемый момент затяжки для монтажа составляет 1,0 Н.м, а максимально допустимый – 1,2 Н.м.

2.8 Заземление маршрутизатора

Заземление маршрутизатора помогает предотвратить эффект шума из-за электромагнитных помех (EMI). Перед включением подключите маршрутизатор к проводу заземления на месте с помощью винта заземления.

Примечание. Это изделие подходит для установки на звукозаземленной поверхности устройства, например на металлической панели.

2.9 Подключите маршрутизатор к компьютеру.

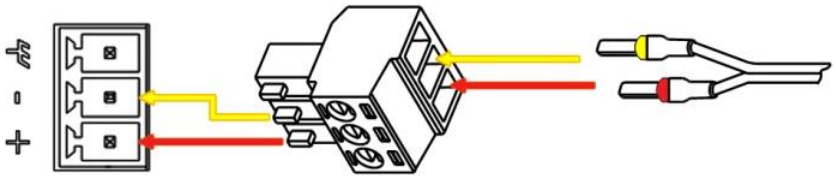


Подключите кабель Ethernet к порту с маркировкой ETH0 или ETH1 на передней панели маршрутизатора, а другой конец кабеля подключите к компьютеру.

2.10 Электропитание

ПОДКЛЮЧЕНИЕ КАБЕЛЯ ПИТАНИЯ

COLOR	POLARITY
RED	+
YELLOW	-



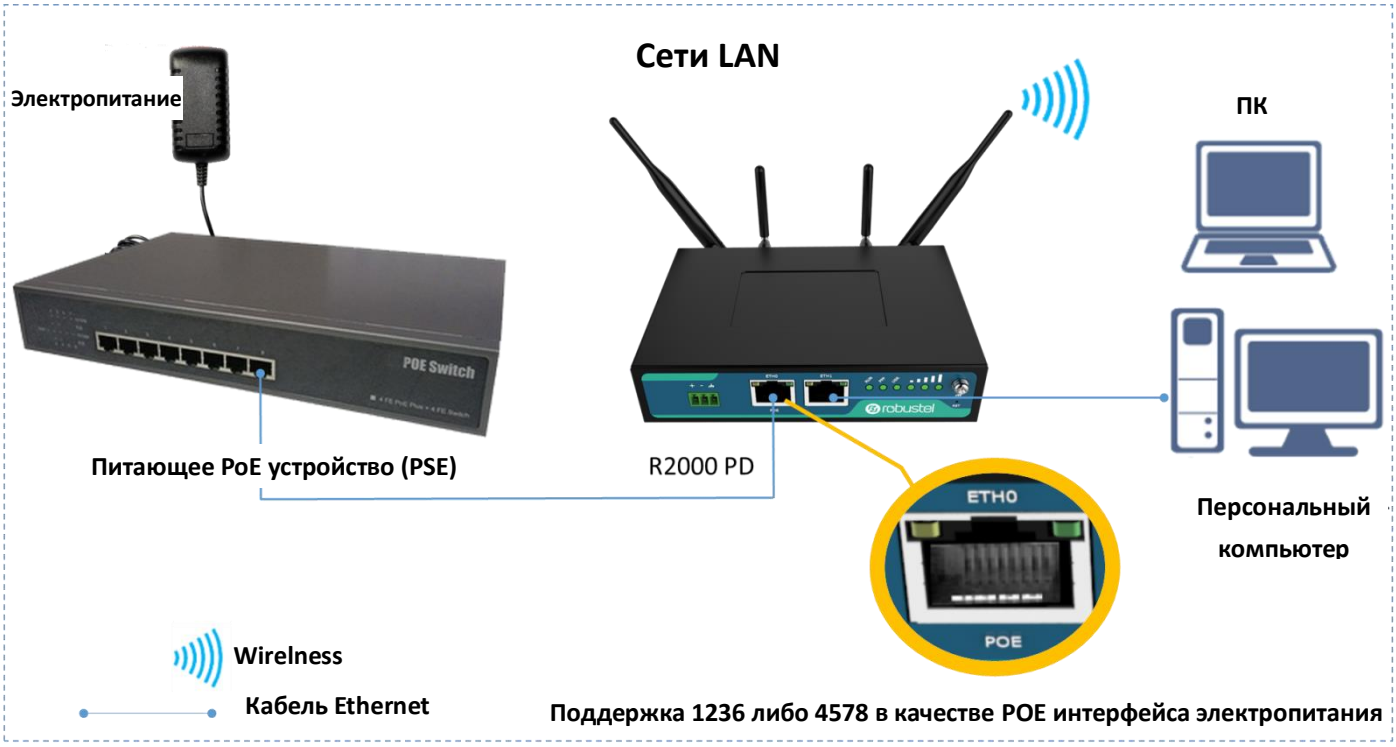
Маршрутизатор R2000 поддерживает защиту от обратной полярности, но всегда обращайтесь к рисунку выше для правильного подключения адаптера питания. К адаптеру питания подключены два кабеля. В соответствии с цветом головки подключите кабель с красной маркировкой к положительному полюсу через клеммную колодку, а желтый – аналогично к отрицательному полюсу.

Примечание: диапазон мощности питания – от 9 до 26 В пост. тока (A014401, A014402, A014403, A014404, A014405, A014406, A014701, A014702, A014703, A014704, A014705, A014706) либо 9-36В пост. тока.

2.11 Подключение PD (опционально)

Если вы желаете подключить к сети питания маршрутизатор R2000 через порт Ethernet, ознакомьтесь со следующей топологией для подключения маршрутизатора R2000 к оборудованию электропитания (PSE). Диапазон напряжения питания PoE порта – 48~57 пост. тока.

Примечание: не рекомендуется использовать источник питания пост. тока одновременно с источником питания PD.


Сети LAN
Электропитание
ПК
POE Switch
Питающее PoE устройство (PSE)
R2000 PD
ETH0
POE
Персональный компьютер
Wirelness
Кабель Ethernet
Поддержка 1236 либо 4578 в качестве POE интерфейса электропитания

Глава 3 Начальная конфигурация

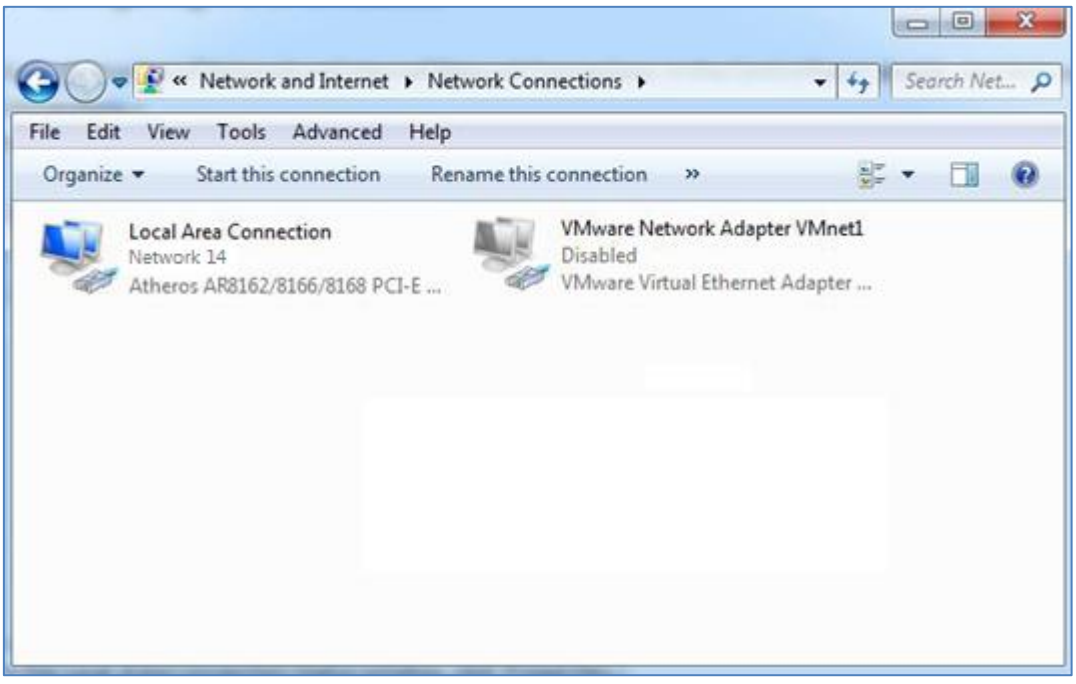
Маршрутизатор можно настроить через веб-браузер, включая IE 8.0 или версию выше, Chrome, Firefox и др. Веб-браузер включен в качестве стандартного приложения в следующие операционные системы: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8 и др. Он обеспечивает простой и удобный интерфейс для настройки. Существует несколько способов подключения маршрутизатора: через внешний ретранслятор/концентратор или напрямую к ПК. Однако перед подключением маршрутизатора убедитесь, что на ПК правильно установлен интерфейс Ethernet. Необходимо настроить используемый ПК для получения IP-адреса через DHCP-сервер или фиксированного IP-адреса, который должен находиться в той же подсети, что и маршрутизатор. При возникновении каких-либо проблем с доступом к веб-интерфейсу маршрутизатора, рекомендуется удалить программу брандмауэра на вашем ПК, поскольку это может вызвать проблемы с доступом к IP-адресу маршрутизатора.

3.1 Конфигурация ПК

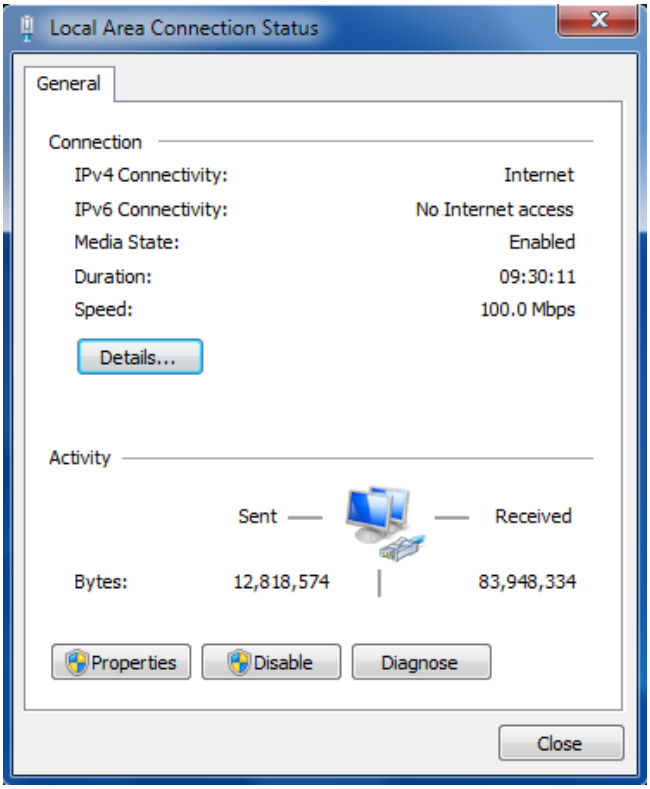
Получить IP-адрес для ПК можно двумя способами. Один из них – автоматическое получение IP-адреса через «Подключение по локальной сети», а другой – настройка статического IP-адреса вручную в той же подсети маршрутизатора. См. шаги ниже.

В качестве примера используется **Windows 7**, конфигурация для системы Windows аналогична.

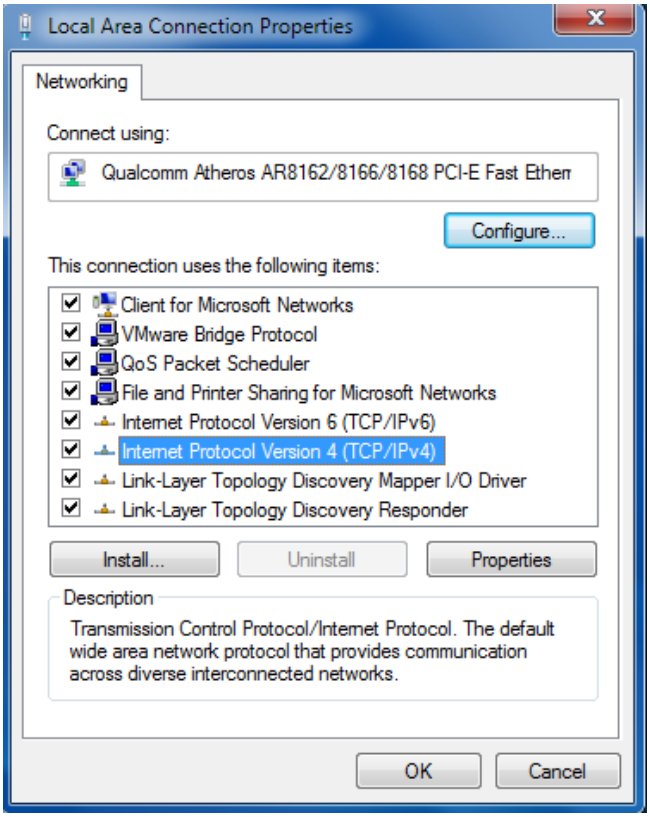
1. Нажмите на **Start > Control panel,** дважды нажмите на **Network and Sharing Center**, а затем дважды нажмите на **Local Area Connection**.



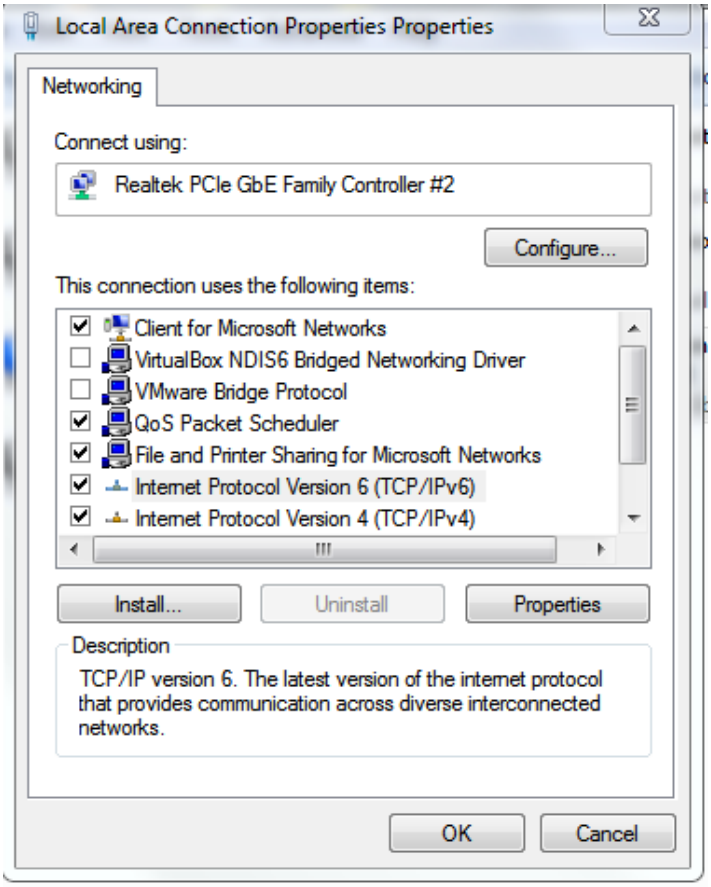
2. Нажмите **на Properties** в окне **Local Area Connection Status**.



3. Выберите **Internet Protocol Version 4 (TCP/IPv4)** и нажмите на **Properties**.

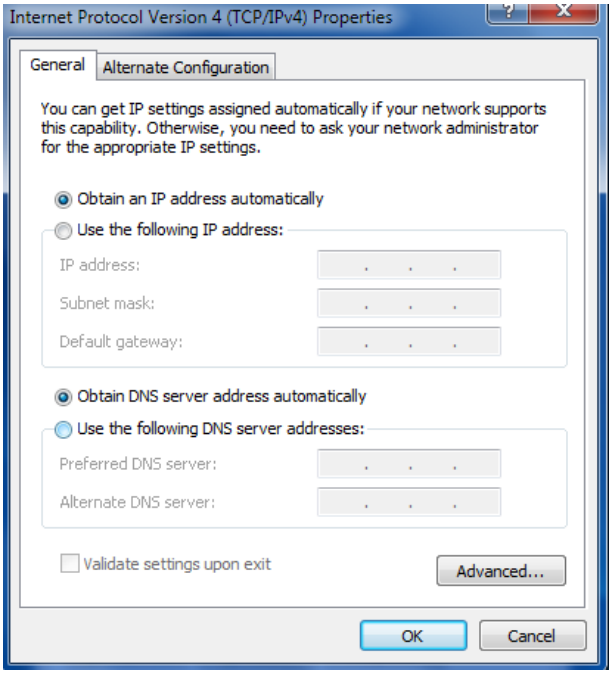


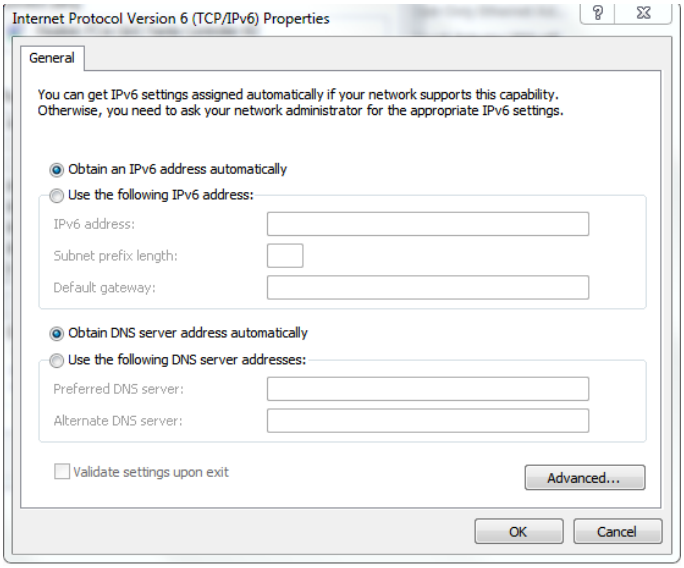
4. Выберите **Internet Protocol Version 6 (TCP/IPv6)** и нажмите на **Properties**.



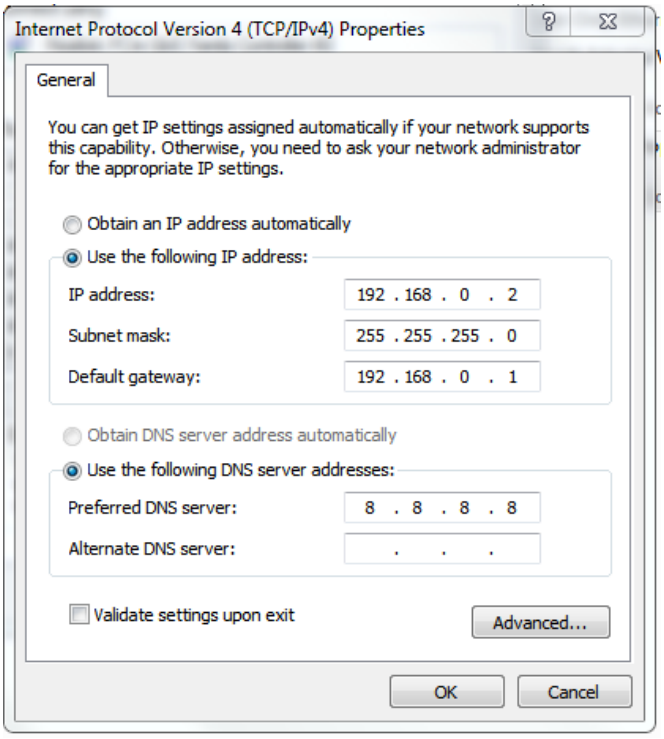
5. Два способа настройки IP-адреса персонального компьютера.

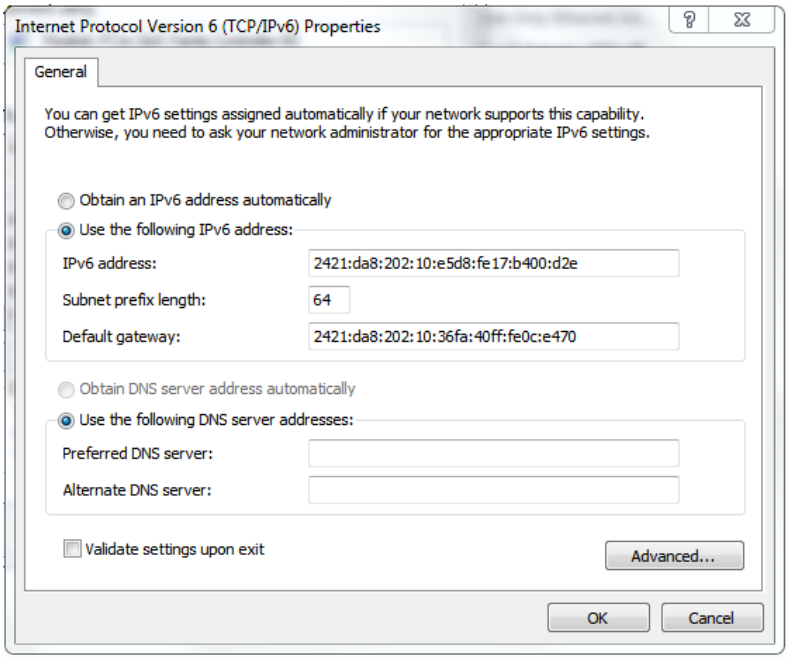
Чтобы получить IP-адрес автоматически от DHCP сервера, нажмите «**Получить IP-адрес автоматически»**;





Для ручной настройки конфигурации ПК со статическим IP-адресом в той же подсети, к которой относится адрес маршрутизатора, нажмите «**Использовать следующий IP-адрес»** и выполните конфигурацию;





6. Нажмите на **OK**, чтобы завершить настройку.

3.2 Заводские настройки по умолчанию

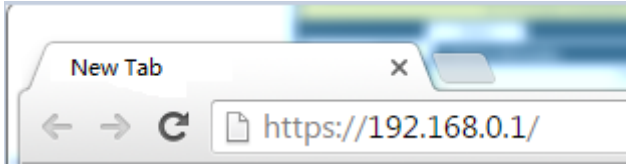
Перед настройкой маршрутизатора необходимо изучить следующие настройки по умолчанию.

Позиция	Описание
Username	admin
Password	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 Вход в систему в маршрутизатора

Чтобы попасть на страницу управления и просмотреть состояние конфигурации маршрутизатора, выполните следующие действия.

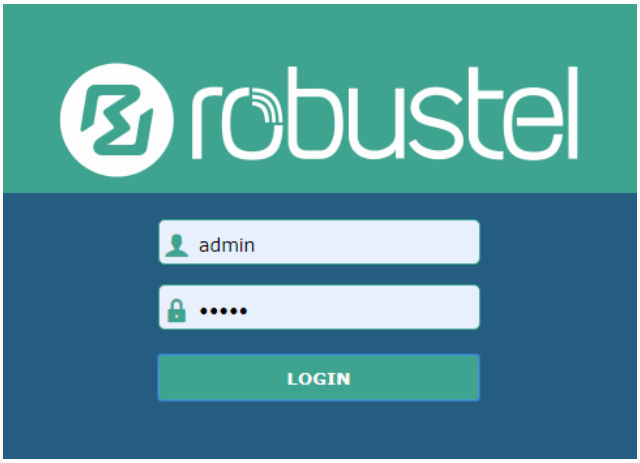
1. Откройте веб-браузер на используемом ПК, например Internet Explorer, Google, Firebox и т. д.
2. В веб-браузере введите IP-адрес маршрутизатора в адресную строку и нажмите на кнопку enter. IP-адрес маршрутизатора по умолчанию – http://192.168.0.1/, однако фактический адрес может отличаться.
   Примечание: при вводе в маршрутизатор SIM-карты с IP-адресом общего пользования введите соответствующий IP-адрес общего пользования в адресную строку браузера для получения беспроводного доступа к маршрутизатору.



3. На странице входа в систему введите имя пользователя и пароль, выберите язык и нажмите на **LOGIN**.

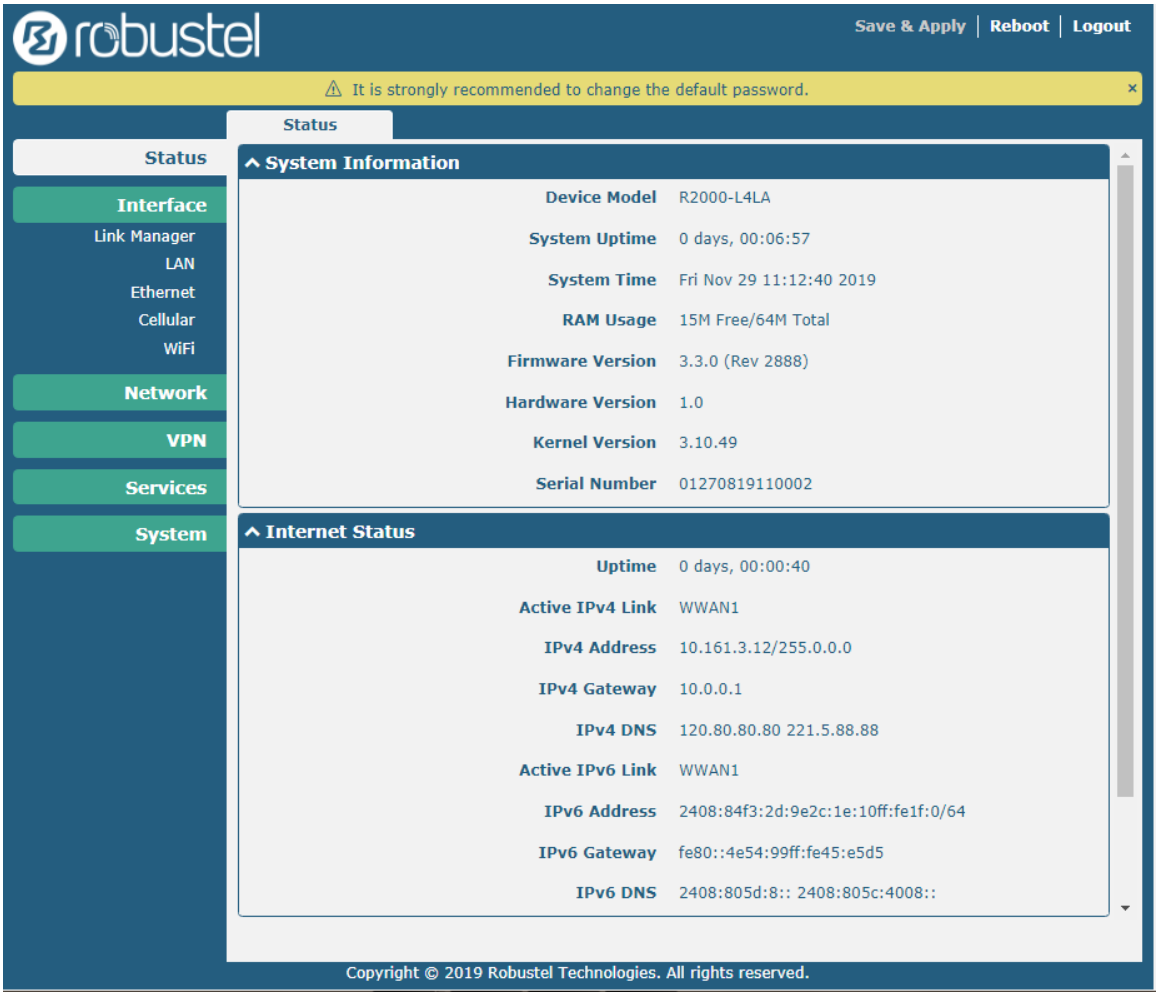
Имя пользователя и пароль по умолчанию – «admin».

Примечание: если ввести неправильное имя пользователя или пароль более 6 раз, веб-страница входа в систему будет заблокирована на 5 минут.



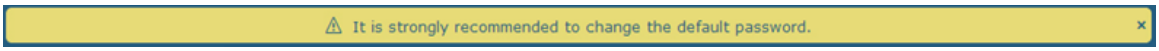
3.4 Панель управления

После входа в систему отображается, например, домашняя страница веб-интерфейса маршрутизатора R2000.



На домашней странице пользователи могут выполнять такие операции, как сохранение конфигурации, перезапуск маршрутизатора и выход из системы.

При использовании исходного пароля для входа в систему маршрутизатора на странице появится следующее всплывающее окно



В целях безопасности настоятельно рекомендуется изменить имя пользователя и/или пароль по умолчанию.

Нажмите на кнопку ×, чтобы закрыть всплывающее окно. Чтобы изменить имя пользователя и/или пароль, см. **3.31 Система > Управление пользователями**.

Панель управления		
Позиция	**Описание**	**Кнопка**
Save & Apply	Нажмите, чтобы сохранить текущую конфигурацию во флэш-памяти маршрутизатора и применить изменение на каждой странице конфигурации, и чтобы изменение вступило в силу.	Save & Apply
Reboot	Нажмите, чтобы перезагрузить маршрутизатор. Если кнопка Reboot желтого цвета, это означает, что некоторые завершенные настройки вступят в силу только после перезагрузки.	Reboot
Logout	Нажмите, чтобы безопасно выйти из системы текущего пользователя. После выхода он переключится на страницу входа в систему. Напрямую закройте веб-страницу, не выходя из системы, следующий пользователь может войти на веб-страницу в этом браузере без пароля до истечения времени ожидания.	Logout
Submit	Нажмите, чтобы сохранить изменение на текущей странице конфигурации.	Submit
Cancel	Нажмите, чтобы отменить изменение на текущей странице конфигурации.	Cancel

Примечание. Шаги по изменению конфигурации представлены ниже:

1. Изменить на одной странице;
2. Нажмите на Submit под этой страницей;
3. Изменить на другой странице;
4. Нажмите на Submit под этой страницей;
5. Завершить все модификации;
6. Нажмите на Save & Apply.

3.5 Статус

Эта страница позволяет просматривать информацию о системе, статус интернет-подключения и статус локальной сети используемого маршрутизатора.

Информация о сети

Информация о сети	
Позиция	**Описание**
Device Model	Отображает название модели используемого устройства.
System Uptime	Отображает текущее количество времени, в течение которого маршрутизатор был подключен.
System Time	Отображает текущее время системы.
RAM Usage	Отображает свободную память и общий объем памяти.
Firmware Version	Отображает версию аппаратно-программного обеспечения, используемого в маршрутизаторе.
Hardware Version	Отображает текущую версию аппаратного обеспечения.
Kernel Version	Отображает текущую версию ядра.
Serial Number	Отображает последовательный номер используемого устройства.

Статус интернет-подключения

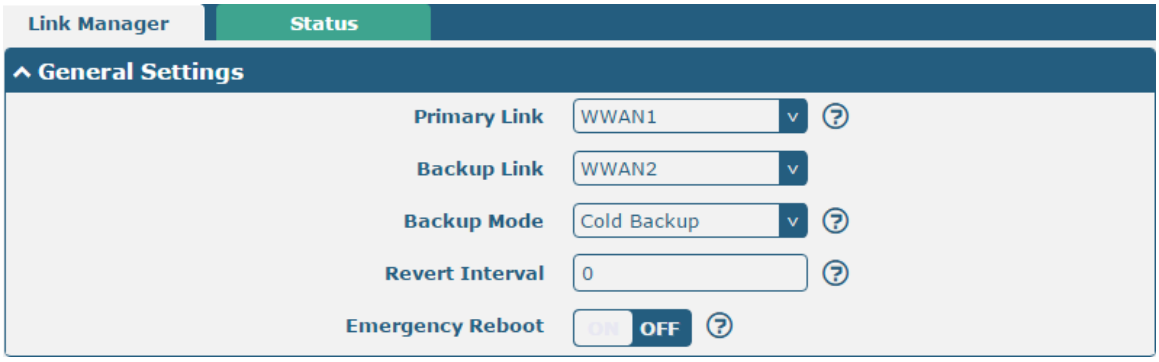
Статус интернет-подключения	
Позиция	**Описание**
Uptime	Отображает текущее количество времени, в течение которого было подключено соединение.
IPv4 Link Description	Отображает текущее онлайн-соединение: WWAN1, WWAN2, WAN или WLAN.
IPv4 Address	Отображает IPv4-адрес текущего соединения.
IPv4 Gateway	Отображает адрес IPv4-шлюза текущего соединения.
IPv4 DNS	Показать текущий первичный IPv4 DNS сервер и вторичный сервер.
IPV6 Link Description	Отображает текущее онлайн-соединение: WWAN1, WWAN2, WAN или WLAN.
IPv6 Address	Отображает IPv6-адрес текущего соединения.
IPv6 Gateway	Отображает адрес IPv6-шлюза текущего соединения.
IPv6 DNS	Показать текущий первичный IPv6 DNS сервер и вторичный сервер.

Статус локальной сети

Статус локальной сети	
Позиция	**Описание**
IP Address	Отображает IP-адрес и сетевую маску маршрутизатора.
IPv6 Address	Отображает IPv6-адрес и длину префикса, полученные маршрутизатором, а также текущее онлайн-соединение.
Inactive IPv6 Address	Отображает IPv6-адрес и длину префикса, полученные маршрутизатором вместе с текущим резервным каналом.
MAC Address	Отображает MAC-адрес маршрутизатора.

3.6 Interface > Link Manager

Этот раздел позволяет настроить подключение соединения.

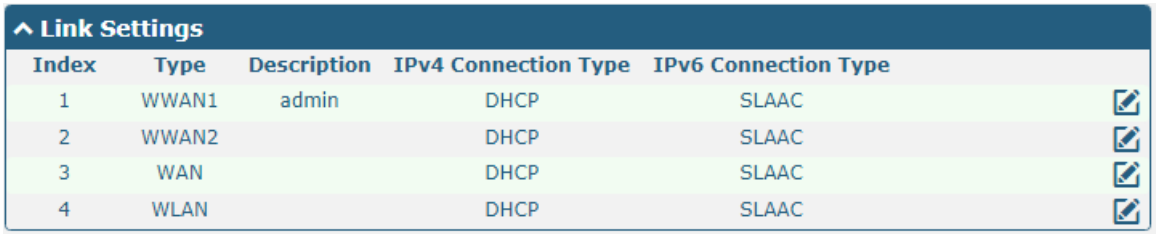


General Settings и Link Manager		
Позиция	**Описание**	**По умолчанию**
Primary Link	Выберите из «WWAN1», «WWAN2», «WAN» или «WLAN». • WWAN1: выберите, чтобы назначить SIM1 основным беспроводным соединением. • WWAN2: выберите, чтобы назначить SIM2 основным беспроводным соединением. • WAN: выберите, чтобы назначить порт WAN Ethernet основным проводным соединением. **Примечание.** Соединение WAN доступно, только если включить eth0 в качестве порта WAN в разделе **Interface > Ethernet > Ports > Port Settings**. • WLAN: выберите, чтобы назначить WLAN основным беспроводным соединением. **Примечание.** Соединение WLAN доступно только в том случае, если режим Wi-Fi включен в качестве режима клиента, см. **3.10 Интерфейс > WiFi**.	WWAN1
Backup Link	Выберите из «WWAN1», «WWAN2», «WAN», «WLAN» или «None». • WWAN1: выберите, чтобы назначить SIM1 резервным беспроводным соединением • WWAN2: выберите, чтобы назначить SIM2 резервным беспроводным соединением. • WAN: выберите, чтобы назначить порт WAN Ethernet основным проводным соединением. **Примечание.** Соединение WAN доступно, только если включить eth0 в качестве порта WAN в разделе **Interface > Ethernet > Ports > Port Settings**. • WLAN: выберите, чтобы назначить WLAN основным беспроводным соединением. **Примечание.** Соединение WLAN доступно только в том случае, если режим Wi-Fi включен в качестве режима клиента, см. **3.10 Интерфейс > WiFi**. • None: не выбирать резервную ссылку	WWAN2

General Settings и Link Manager		
Позиция	**Описание**	**По умолчанию**
Backup Mode	Выберите из «Cold Backup», «Warm Backup» или «Load Balancing». • Cold Backup: неактивное соединение офлайн в режиме ожидания • Warm Backup: неактивное соединение онлайн в режиме ожидания • Load Balancing: использовать два соединения одновременно **Примечание**: маршрутизатор R2000 не поддерживает теплое резервирование и балансирование нагрузки при наличии двух соединений WWAN.	Cold Backup
Revert Interval	Укажите количество минут, которое должно пройти до проверки основного соединения, если резервное соединение используется в режиме Cold backup. «0» означает отключение проверки. **Примечание.** Интервал возврата доступен только в режиме Cold backup.	0
Emergency Reboot	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Включите, чтобы перезагрузить всю систему, если соединения недоступны.	OFF

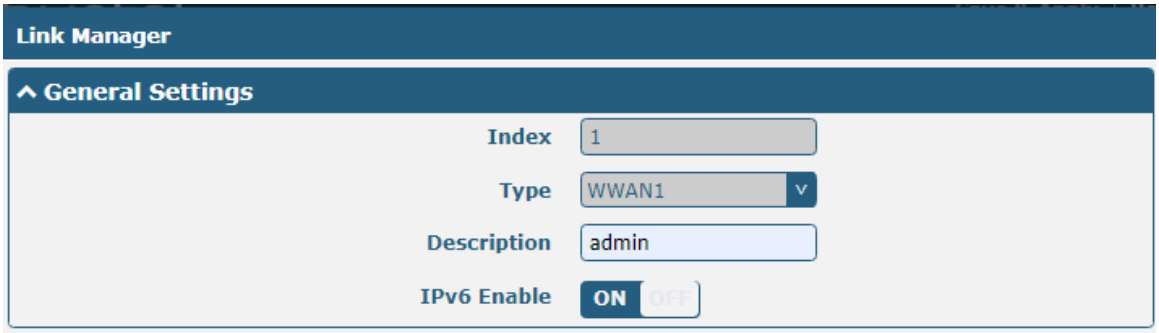
Примечание: Нажмите на для получения помощи.

Раздел **Link Settings** позволяет настроить параметры соединения, включая WWAN1/WWAN2, WAN и WLAN. Рекомендуется включить обнаружение Ping-запроса, чтобы маршрутизатор всегда был онлайн. Обнаружение Ping-запроса повышает надежность, а также снижает трафик данных.

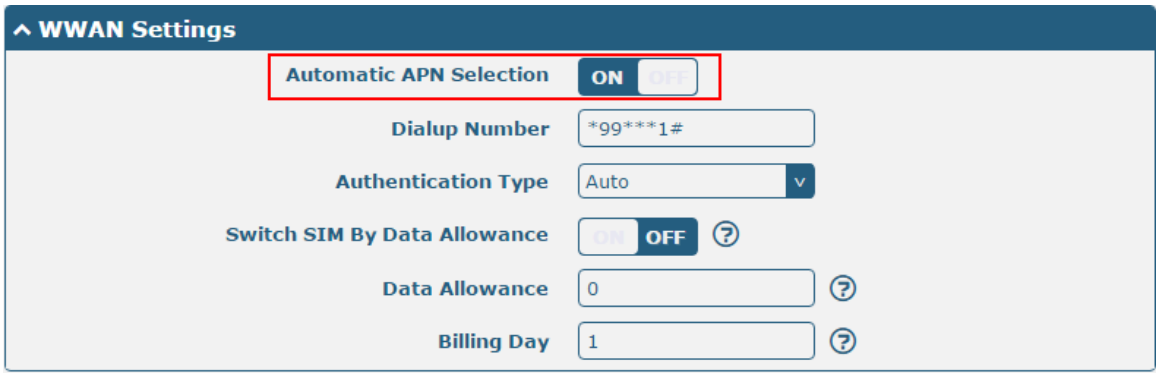


Нажмите на на крайней правой части WWAN1/WWAN2, чтобы открыть окно конфигурации.

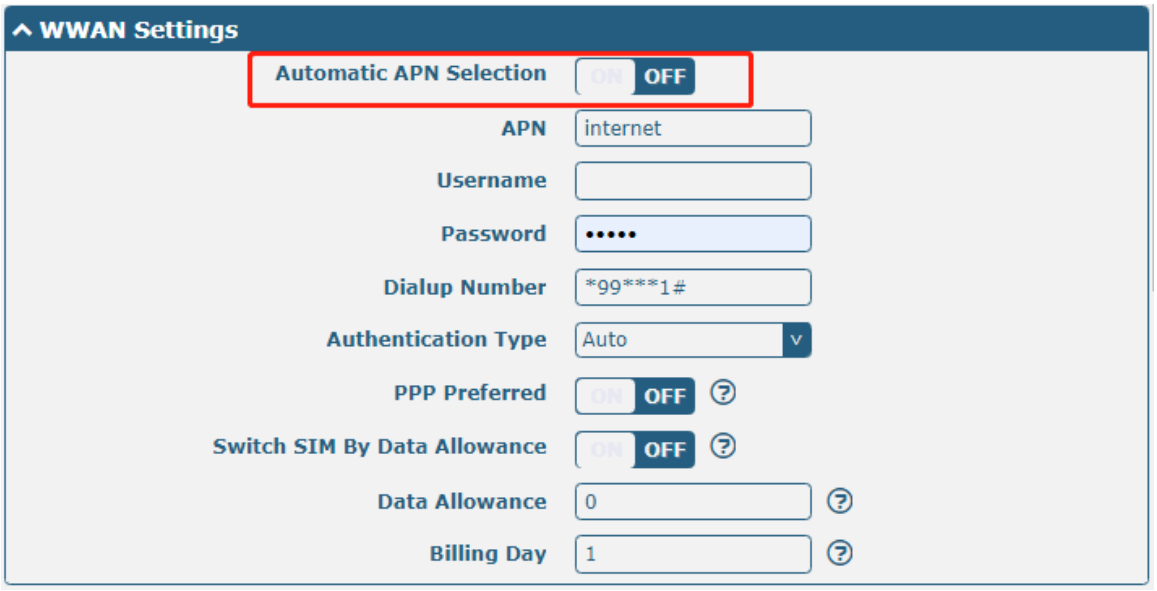
WWAN1/WWAN2

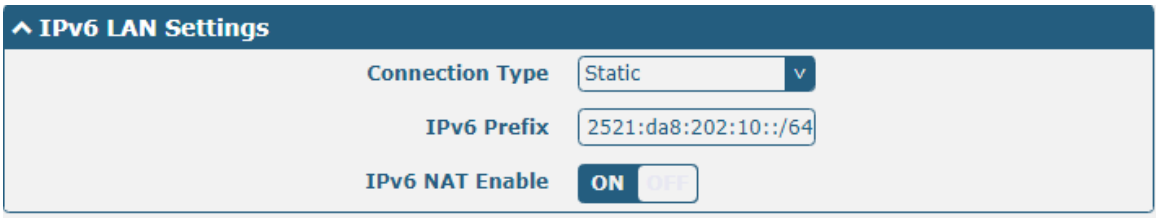


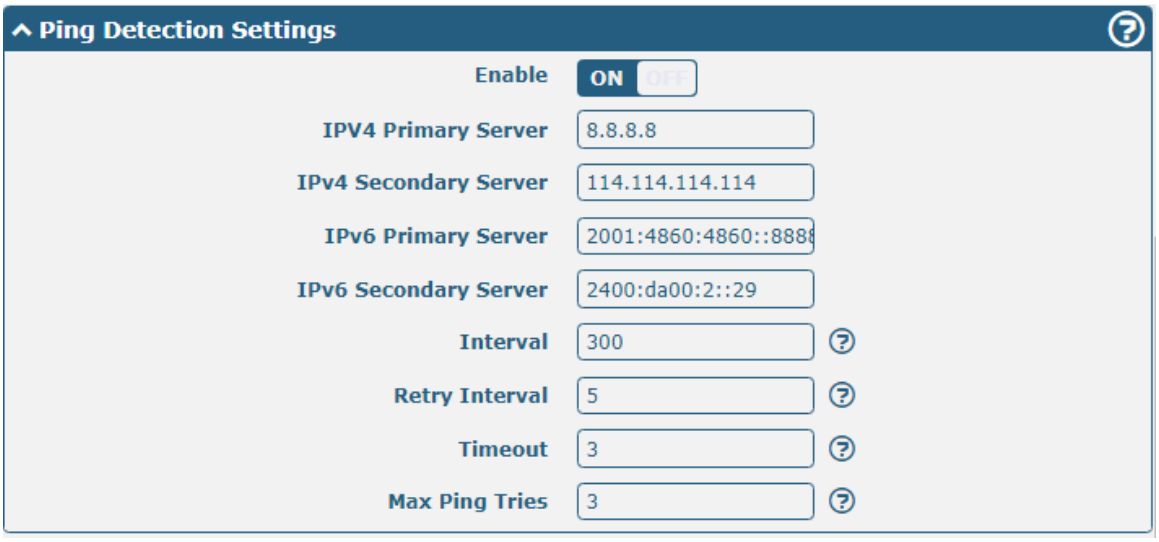
При включении опции **«Automatic APN Selection»** отображается окно в соответствии с рисунком ниже.

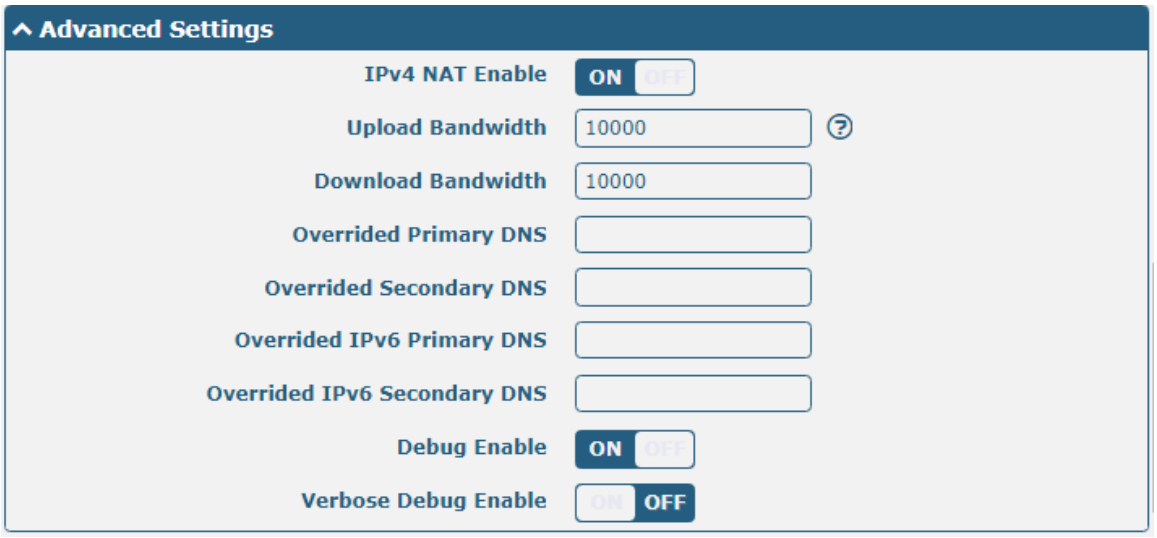


При выключении опции **«Automatic APN Selection»** отображается окно в соответствии с рисунком ниже.









Link Settings (WWAN)		
Позиция	**Описание**	**По умолчанию**
General Settings		
Index	Указывает порядковый номер списка.	--
Type	Отображает тип соединения.	WWAN1
Description	Вводит описание для этого соединения.	Null
IPv6	Нажмите на кнопку-переключатель, чтобы включить/отключить IPv6.	OFF
WWAN Settings		
Automatic APN Selection	Нажмите на кнопку-переключатель, чтобы включить/отключить опцию «Automatic APN Selection». После включения устройство автоматически распознает имя точки доступа. Кроме того, можно отключить эту опцию и вручную добавить имя точки доступа.	ON
APN	Введите имя точки доступа для коммутируемого сотового соединения, предоставленное местным интернет-провайдером.	internet
Username	Введите имя пользователя для коммутируемого сотового соединения, предоставленное местным интернет-провайдером.	Null
Password	Введите пароль для коммутируемого сотового соединения, предоставленное местным интернет-провайдером.	Null
Dialup Number	Введите коммутируемый номер для коммутируемого сотового соединения, предоставленное местным интернет-провайдером.	*99***1#
Authentication Type	Выберите из «Auto», «PAP» или «CHAP» в зависимости от требований местного интернет-провайдера.	Auto
PPP Preferred	Метод коммутируемого доступа PPP является предпочтительным.	OFF
Switch SIM By Data Allowance	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. После включения он переключится на другую SIM-карту при достижении лимита данных. **Примечание**: используется только для резервного копирования с двумя SIM-картами.	OFF

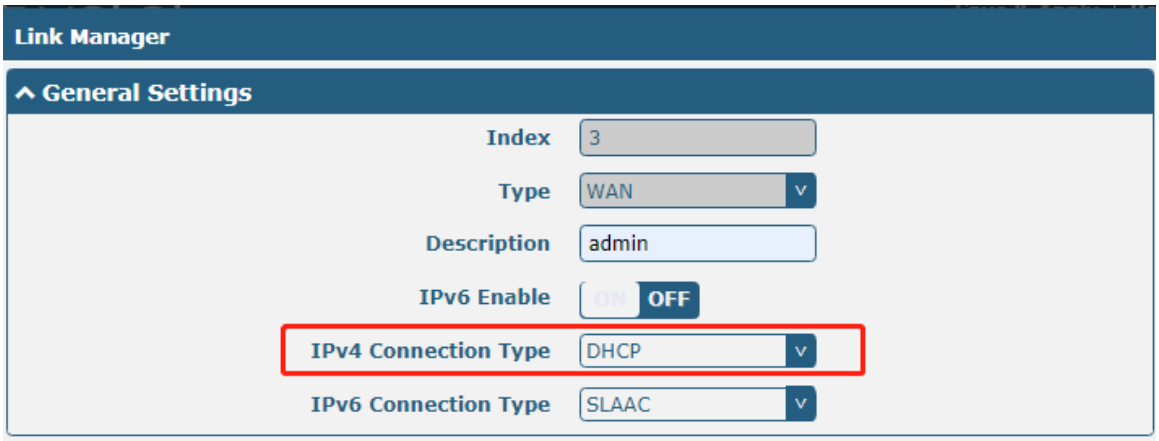
Link Settings (WWAN)		
Позиция	**Описание**	**По умолчанию**
Data Allowance	Устанавливает ежемесячное ограничение трафика данных. Система будет записывать статистику трафика данных, если указано ограничение трафика данных (MiB). Запись трафика будет отображаться в разделе **Interface > Link Manager > Status > WWAN Data Usage Statistics**. «0» означает отключение записи трафика данных.	0
Billing Day	Указывает день ежемесячного выставления счетов. Статистика трафика данных будет пересчитана с этого дня.	1
IPv6 LAN Settings		
Connection Type	Выберите соединение, чтобы назначить префикс IPv6 локальной сети.	Delegated
IPv6 prefix	Установите статический префикс IPv6, назначенный соединением на LAN.	Null
Enable IPv6 NAT	Установите соединение, чтобы включить IPv6 NAT.	OFF
Ping Detection Settings		
Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить механизм обнаружения ping-запросов, политику проверки активности соединения маршрутизатора.	ON
IPv4 Primary Server	Маршрутизатор будет пинговать этот основной адрес/доменное имя, чтобы проверить, активно ли текущее соединение IPv4.	8.8.8.8
IPv4 Secondary Server	Маршрутизатор будет пинговать этот вторичный адрес/доменное имя, чтобы проверить, активно ли текущее соединение IPv4.	114.114.114.114
IPv6 Primary Server	Маршрутизатор будет пинговать этот основной адрес/доменное имя, чтобы проверить, активно ли текущее соединение IPv6.	2001:4860:4860::8888
IPv6 Secondary Server	Маршрутизатор будет пинговать этот вторичный адрес/доменное имя, чтобы проверить, активно ли текущее соединение IPv6.	2400:da00:2::29
Interval	Установка интервала ping-запроса.	300
Retry Interval	Установка интервала повтора ping-запроса. При неудачном ping-запросе маршрутизатор будет повторно направлять ping-запрос через каждый интервал повтора.	5
Время ожидания	Установите время ожидания ping-запроса.	3
Max Ping Tries	Установка макс. количества попыток ping-запроса. Переключитесь на другое соединение или примите экстренные меры, если достигнуто максимальное количество попыток непрерывного ping-запроса.	3
Advanced Settings		
NAT Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить опцию «Network Address Translation».	ON
Upload Bandwidth	Установите полосу пропускания загрузки, используемую для QoS, измеряемую в кбит/с.	10000
Download Bandwidth	Установите полосу пропускания скачивания, используемую для QoS, измеряемую в кбит/с.	10000
Specify Primary DNS	Определяет основной DNS-сервер IPv4, используемый соединением.	Null

Link Settings (WWAN)		
Позиция	**Описание**	**По умолчанию**
Specify Secondary DNS	Определяет вторичный DNS-сервер IPv4, используемый соединением.	Null
Specify IPv6 Primary DNS	Определяет основной DNS-сервер IPv6, используемый соединением.	Null
Specify IPv6 Secondary DNS	Определяет вторичный DNS-сервер IPv6, используемый соединением.	Null
Debug Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Включите вывод отладочной информации.	ON
Verbose Debug Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Включите вывод подробной отладочной информации.	OFF

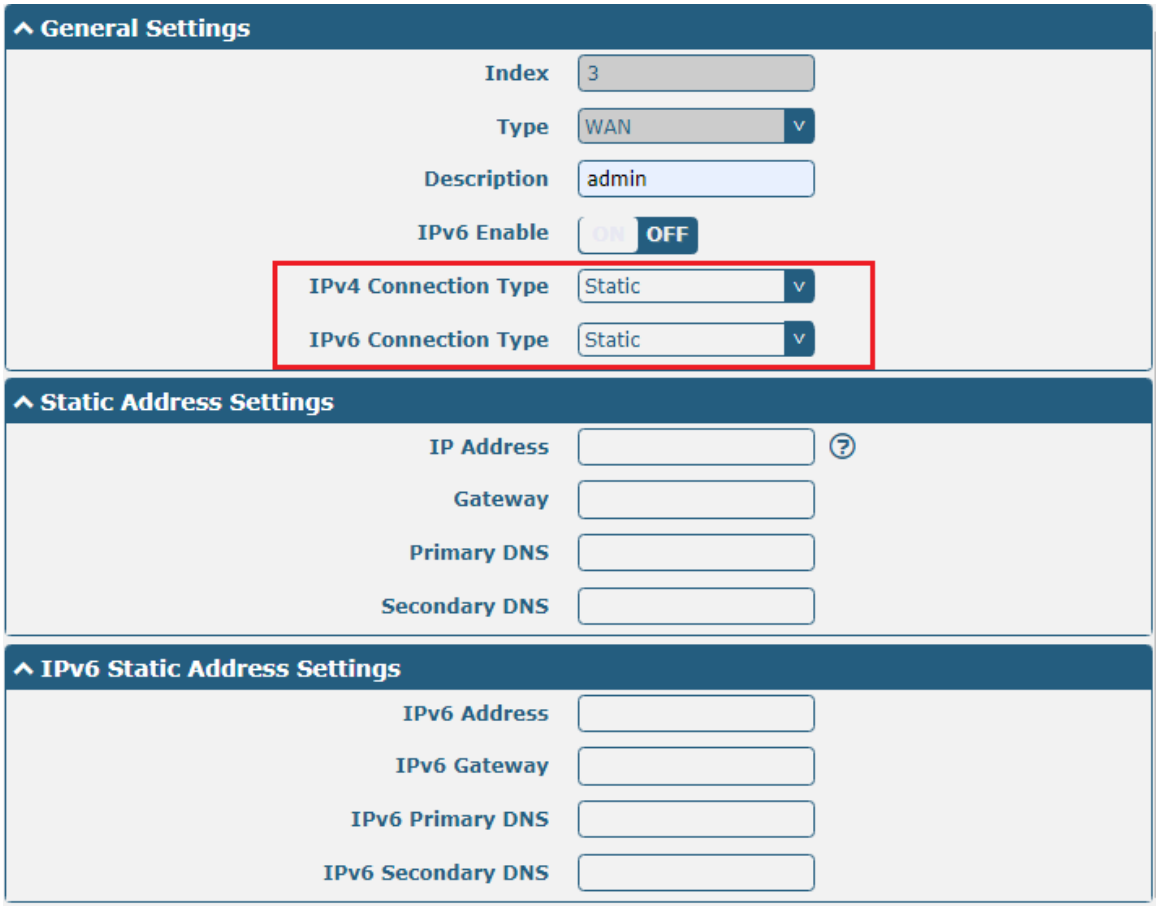
WAN

Маршрутизатор автоматически получит IP-адрес от DHCP-сервера, если в качестве **типа подключения IPv4** выбрано **«DHCP»**. Окно отображается, как показано ниже.

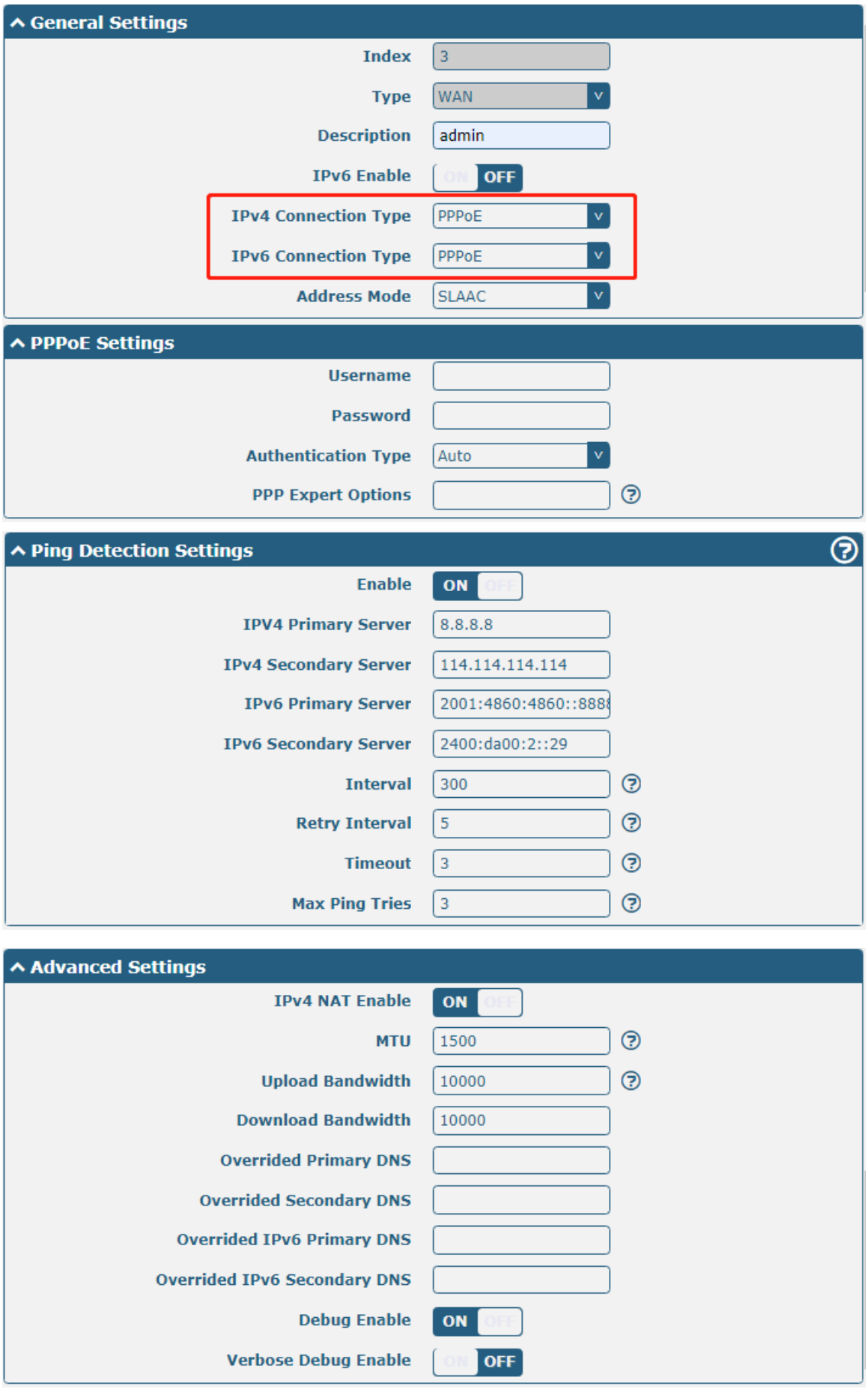
Роутер автоматически получает префикс IPv6 от сервера DHCP при выборе SLAAC для **типа подключения IPv6** .



При выборе **«Static»** в качестве типа **подключения IPv4** и **типа подключения IPv6** окно отображается в соответствии с рисунком ниже.



При выборе **«PPPoE»** в качестве типа подключения **IPv4** и **типа подключения IPv6** окно отображается в соответствии с рисунком ниже.


General Settings
Index
3
Type
WAN
Description
admin
IPv6 Enable
OFF
IPv4 Connection Type
PPPoE
IPv6 Connection Type
PPPoE
Address Mode
SLAAC
PPPoE Settings
Username
Password
Authentication Type
Auto
PPP Expert Options
Ping Detection Settings
Enable
ON
IPV4 Primary Server
8.8.8.8
IPv4 Secondary Server
114.114.114.114
IPv6 Primary Server
2001:4860:4860::8888
IPv6 Secondary Server
2400:da00:2::29
Interval
300
Retry Interval
5
Timeout
3
Max Ping Tries
3
Advanced Settings
IPv4 NAT Enable
ON
MTU
1500
Upload Bandwidth
10000
Download Bandwidth
10000
Overrided Primary DNS
Overrided Secondary DNS
Overrided IPv6 Primary DNS
Overrided IPv6 Secondary DNS
Debug Enable
ON
Verbose Debug Enable
OFF

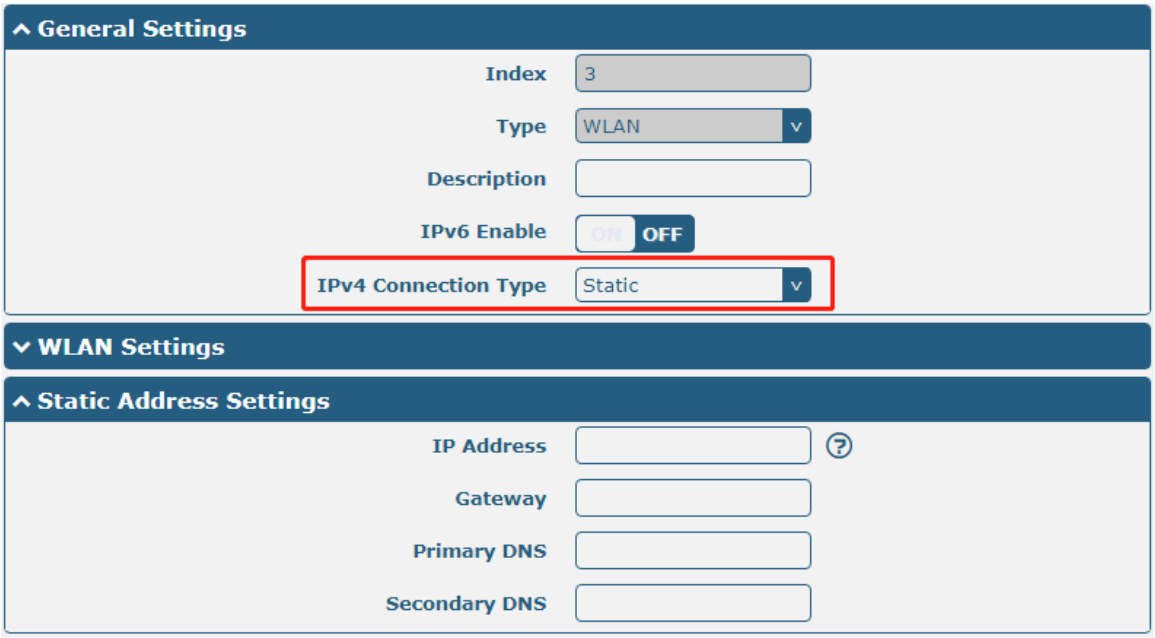
Link Settings (WAN)		
Позиция	**Описание**	**По умолчанию**
General Settings		
Index	Указывает порядковый номер списка.	--
Type	Отображает тип соединения.	WAN
Description	Вводит описание для этого соединения.	Null
Enable IPv6	Нажмите на кнопку-переключатель, чтобы включить/отключить IPv6.	OFF
IPv4 connection type	Выберите из «DHCP», «Static» или «PPPoE».	DHCP
IPv6 Connection Type	Выберите из «SLAAC», «DHCPv6», «Static» или «PPPoE».	SLAAC
Address Type	Выберите из «SLAAC» или «DHCPv6».	SLAAC
IPv4 Static Address Settings		
IP Address	Введите IP-адрес с сетевой маской, который может получить доступ в Интернет. IP-адрес с сетевой маской, например 192.168.1.1/24	Null
Gateway	Установка шлюза IP-адреса в порт WAN.	Null
Primary DNS	Установка основного DNS.	Null
Secondary DNS	Установка вторичного DNS.	Null
IPv6 Static Address Settings		
IPv6 Address	Введите IP-адрес с сетевой маской, который может получить доступ в Интернет. IP-адрес с сетевой маской, например, 2521:da8:202:10::20/64。	Null
Gateway	Установка шлюза IPv6-адреса в порт WAN.	Null
IPv6 Primary DNS	Определяет основной DNS-сервер IPv6, используемый соединением.	Null
IPv6 Secondary DNS	Определяет вторичный DNS-сервер IPv6 для соединения.	Null
Настройки PPPoE		
Username	Введите имя пользователя, предоставленное интернет-провайдером.	Null
Password	Введите пароль, предоставленный интернет-провайдером.	Null
Authentication Type	Выберите из «Auto», «PAP» или «CHAP» в зависимости от требований местного интернет-провайдера.	Auto
PPP Expert Options	Введите параметры PPP Expert, используемые для коммутируемого доступа PPPoE. Можно ввести в это поле другие строки набора PPP. Каждая строка может быть разделена точкой с запятой.	Null
IPv6 LAN Ping Settings		
Connection Type	Выберите соединение, чтобы назначить префикс IPv6 локальной сети.	Delegated
IPv6 prefix	Установите статический префикс IPv6, назначенный соединением на LAN.	Null
Enable IPv6 NAT	Установите соединение, чтобы включить IPv6 NAT.	OFF
Ping Detection Settings		

Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить механизм обнаружения ping-запросов, политику проверки активности соединения маршрутизатора.	ON
Primary Server	Маршрутизатор будет пинговать этот основной адрес/доменное имя, чтобы проверить, активно ли текущее соединение.	8.8.8.8
Secondary Server	Маршрутизатор будет пинговать этот вторичный адрес/доменное имя, чтобы проверить, активно ли текущее соединение.	114.114.114.114
IPv6 Primary Server	Маршрутизатор пингует первичный адрес/доменное имя, чтобы проверить, постоянно ли активно текущее соединение IPv6.	2001:4860:4860::8888
IPv6 Secondary Server	Маршрутизатор пингует альтернативный адрес/доменное имя, чтобы проверить, постоянно ли активно текущее соединение IPv6.	2400:da00:2::29
Interval	Установка интервала ping-запроса.	300
Retry Interval	Установка интервала повтора ping-запроса. При неудачном ping-запросе маршрутизатор будет повторно направлять ping-запрос через каждый интервал повтора.	5
Время ожидания	Установите время ожидания ping-запроса.	3
Max Ping Tries	Установка макс. количества попыток ping-запроса. Переключитесь на другое соединение или примите экстренные меры, если достигнуто максимальное количество попыток непрерывного ping-запроса.	3
Advanced Settings		
NAT Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить опцию «Network Address Translation».	ON
MTU	Ввод максимальной единицы передачи.	1500
Upload Bandwidth	Ввод полосы пропускания загрузки, используемой для QoS, измеряемой в кбит/с.	10000
Download Bandwidth	Ввод полосы пропускания скачивания, используемой для QoS, измеряемой в кбит/с.	10000
Specify Primary DNS	Определяет основной DNS-сервер IPv4, используемый соединением.	Null
Specify Secondary DNS	Определяет вторичный DNS-сервер IPv4 для соединения.	Null
Specify IPV6 Primary DNS server	Определяет основной DNS-сервер IPv6, используемый соединением.	Null
Specify IPv6 secondary DNS server	Определяет вторичный DNS-сервер IPv6 для соединения.	Null
Debug Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Включите вывод отладочной информации.	ON
Verbose Debug Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Включите вывод подробной отладочной информации.	OFF

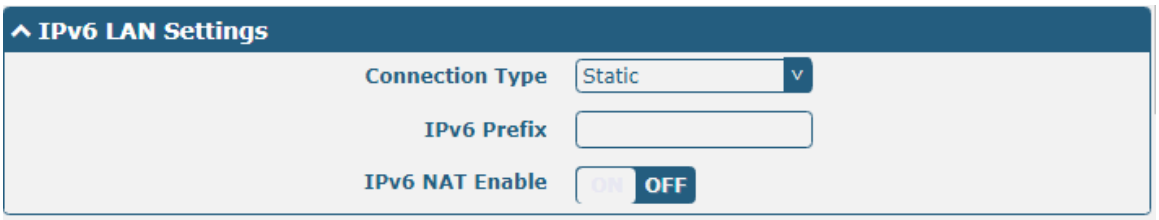
WLAN

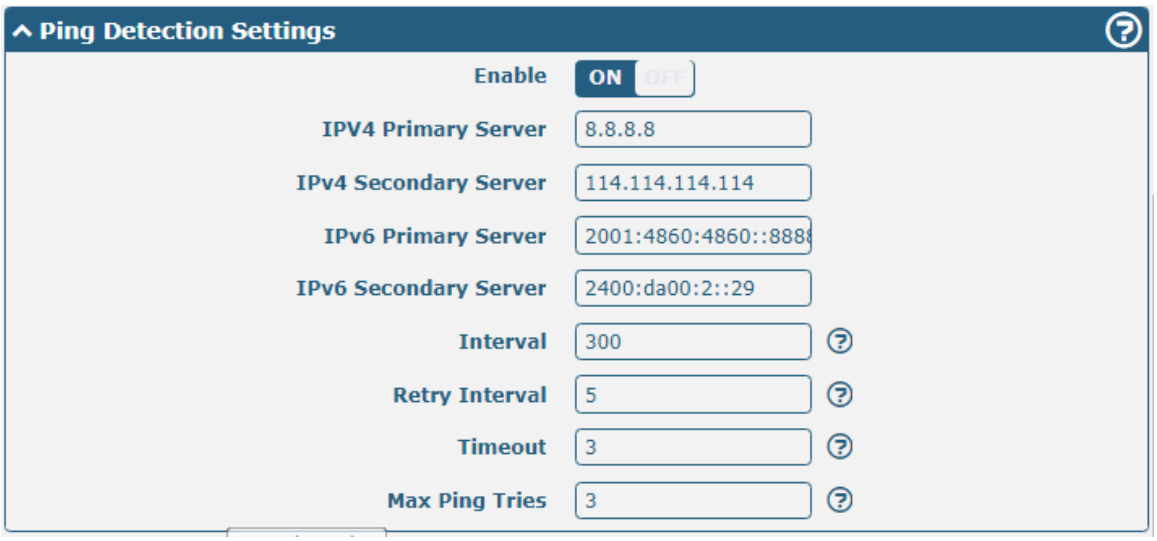
Маршрутизатор автоматически получит IP-адрес от точки доступа WLAN, если в качестве типа подключения выбрано «DHCP». Конкретная конфигурация параметров SSID показана ниже.

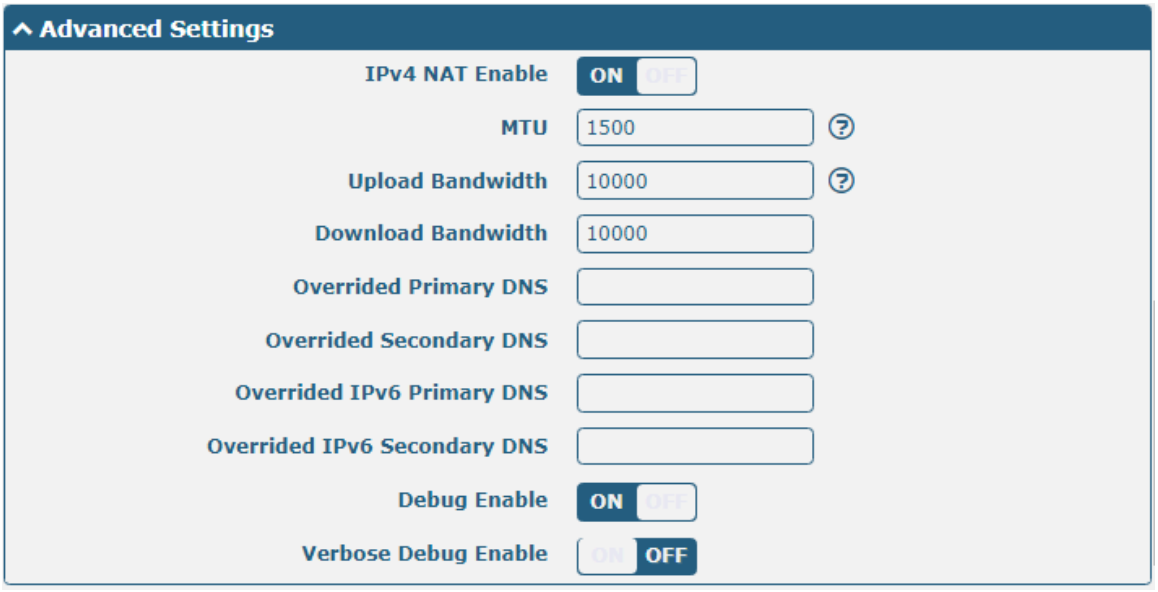
При выборе «Static» в качестве типа подключения окно отображается в соответствии с рисунком ниже.



Маршрутизатор R2000 не поддерживает тип подключения **PPPoE** WLAN.







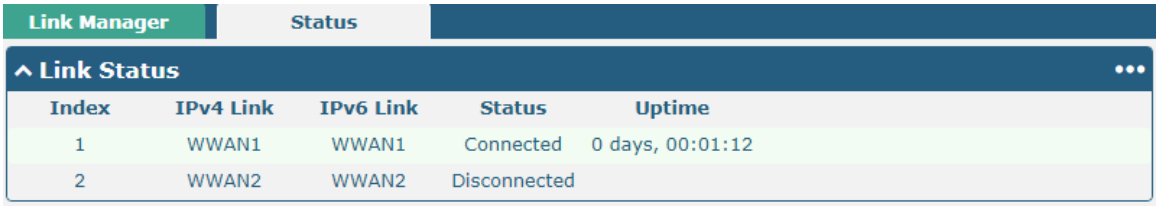
Link Settings (WLAN)		
Позиция	**Описание**	**По умолчанию**
General Settings		
Index	Указывает порядковый номер списка.	--
Type	Отображает тип соединения.	WLAN
Description	Вводит описание для этого соединения.	Null
Enable IPv6	Нажмите на кнопку-переключатель, чтобы включить/отключить IPv6。.	OFF
Connection Type	Выберите из «DHCP» или «Static».	DHCP
Настройки сети WLAN		
SSID	Введите SSID от 1 до 32 символов, к которому необходимо подключить используемый маршрутизатор. SSID (идентификатор набора услуг) – это название используемой беспроводной сети.	маршрутизатор
Connect to Hidden SSID	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Когда маршрутизатор работает в режиме клиента и ему необходимо подключить любую точку доступа со скрытым SSID,	OFF

	необходимо включить эту опцию.	
Password	Введите пароль из 8–63 символов для точки доступа, к которой необходимо подключить используемый маршрутизатор.	Null
Static Address Settings		
IP Address	Введите IPv6-адрес с сетевой маской, который может получить доступ в Интернет. например, 192.168.1.1/24	Null
Gateway	Введите IP-адрес WiFi AP.	Null
Primary DNS	Установка основного DNS.	Null
Secondary DNS	Установка вторичного DNS.	Null
IPv6 LAN Settings		
Connection Type	Выберите соединение, чтобы назначить префиксы IPv6 для локальной сети.	Delegated
IPv6 prefix	Установите статический префикс IPv6, назначенный соединением на LAN.	Null
Enable IPv6 NAT	Установите соединение, чтобы включить IPv6 NAT.	OFF
Ping Detection Settings		
Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить механизм обнаружения ping-запросов, политику проверки активности соединения маршрутизатора.	ON
Primary Server	Маршрутизатор будет пинговать этот основной адрес/доменное имя, чтобы проверить, активно ли текущее соединение.	8.8.8.8
Secondary Server	Маршрутизатор будет пинговать этот вторичный адрес/доменное имя, чтобы проверить, активно ли текущее соединение.	114.114.114.114
IPv6 Primary Server	Маршрутизатор будет пинговать этот основной адрес/доменное имя, чтобы проверить, активно ли текущее соединение IPv6.	2001:4860:4860::8888
IPv6 Secondary Server	Маршрутизатор будет пинговать этот вторичный адрес/доменное имя, чтобы проверить, активно ли текущее соединение IPv6.	2400:da00:2::29
Interval	Установка интервала ping-запроса.	300
Retry Interval	Установка интервала повтора ping-запроса. При неудачном ping-запросе маршрутизатор будет повторно направлять ping-запрос через каждый интервал повтора.	5
Timeout	Установите время ожидания ping-запроса.	3
Max Ping Tries	Установка макс. количества попыток ping-запроса. Переключитесь на другое соединение или примите экстренные меры, если достигнуто максимальное количество попыток непрерывного ping-запроса.	3
Advance Settings		
NAT Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить опцию «Network Address Translation».	ON
MTU	Ввод максимальной единицы передачи.	1500
Upload Bandwidth	Ввод полосы пропускания загрузки, используемой для QoS, измеряемой в кбит/с.	10000
Download Bandwidth	Ввод полосы пропускания скачивания, используемой для QoS, измеряемой в кбит/с.	10000

Specify Primary DNS	Определяет основной DNS-сервер IPv4, используемый соединением.	Null
Specify Secondary DNS	Определяет вторичный DNS-сервер IPv4 для соединения.	Null
Specify IPV6 Primary DNS server	Определяет основной DNS-сервер IPv6, используемый соединением.	Null
Specify IPv6 secondary DNS server	Определяет вторичный DNS-сервер IPv6 для соединения.	Null
Debug Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Включите вывод отладочной информации.	ON
Verbose Debug Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Включите вывод подробной отладочной информации.	OFF

Статус

На этой странице можно посмотреть статус подключения соединения и очистить ежемесячную статистику использования данных.



Нажмите на крайнюю правую кнопку •••, чтобы выбрать статус подключения текущего соединения.

Нажмите на строку соединения, под строкой отобразится подробная информация о текущем подключении соединения.

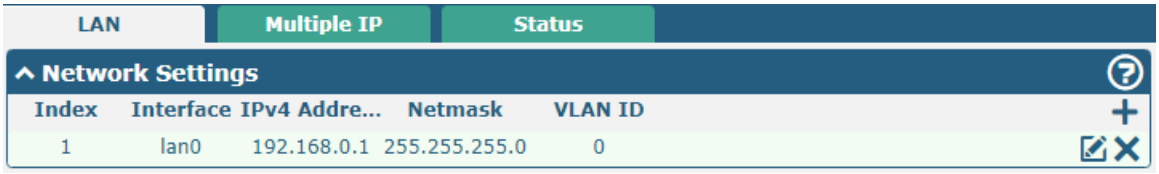
Нажмите на кнопку **Clear**, чтобы очистить ежемесячную статистику использования трафика данных SIM1 или SIM2. Статистика данных будет отображаться только в том случае, если включить функцию «Data Allowance» в разделе **Interface > Link Manager > Link Settings > WWAN Settings > Data Allowance**.

3.7 Interface > LAN

Этот раздел позволяет установить соответствующие параметры для порта LAN. Маршрутизатор R2000 имеет два порта LAN, включая ETH0 и ETH1. Для ETH0 и ETH1 можно свободно выбирать из lan0 и lan1, но по крайней мере один порт LAN должен быть назначен как lan0. Настройки по умолчанию для ETH0 и ETH1 – lan0, а их IP-адреса по умолчанию – 192.168.0.1/255.255.255.0.

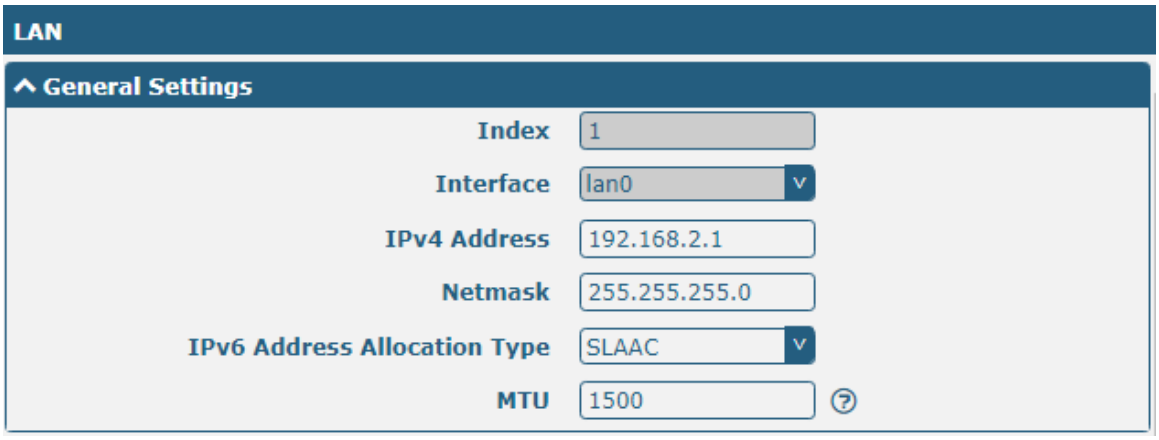
Сети LAN

По умолчанию в списке есть порт LAN (lan0). Чтобы начать добавление нового порта LAN (lan1), сначала настройте ETH0 или ETH1 как lan1 в разделе **Ethernet> Ports> Port Settings**. В противном случае операция будет помечена диалоговым окном с сообщением «List is full».



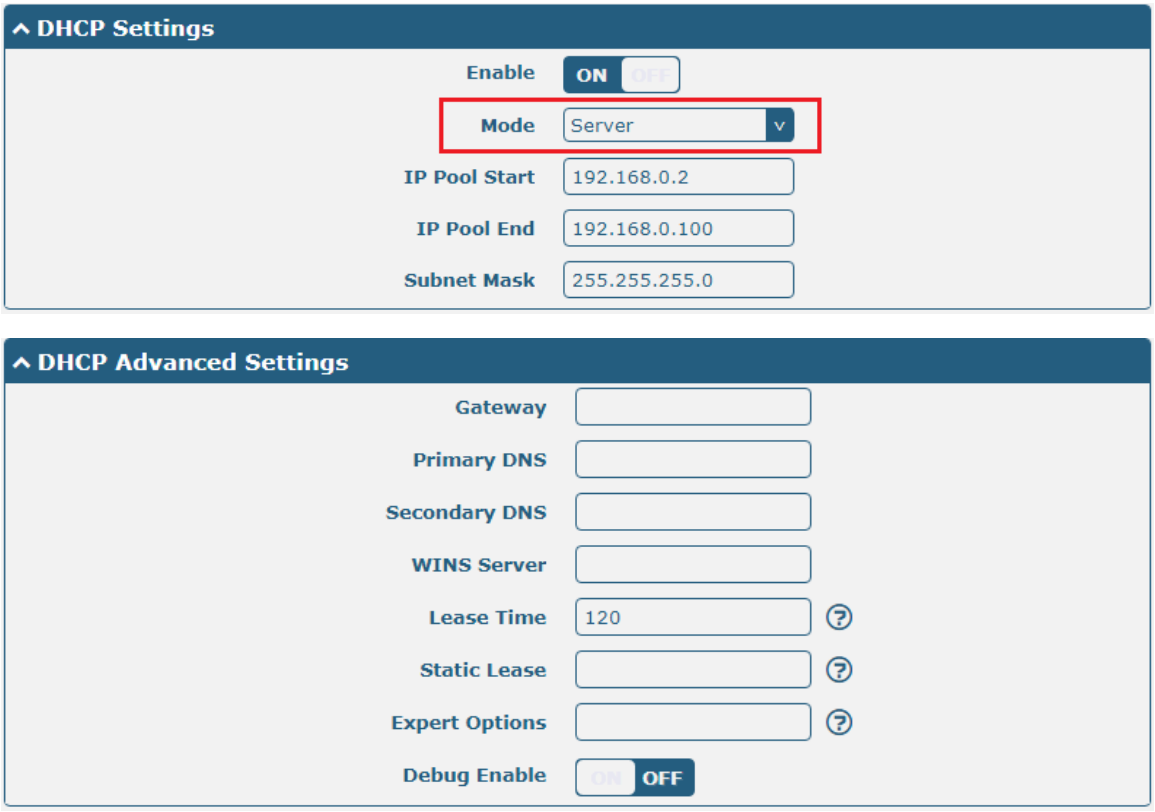
Примечание. Lan0 не может быть удален.

Можно нажать на +, чтобы добавить новый порт LAN, или нажать на ✕, чтобы удалить текущий порт LAN. Теперь нажмите на , чтобы изменить конфигурацию порта LAN.

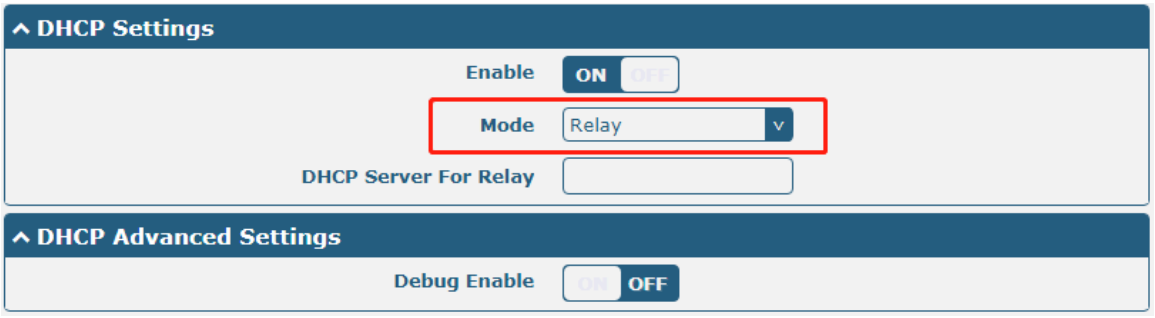


General Settings @ LAN		
Позиция	**Описание**	**По умолчанию**
Index	Указывает порядковый номер списка.	--
Interface	Отображает редактируемый порт. Lan1 доступен только в том случае, если он был выбран для одного из портов ETH0~ETH1 в разделе **Ethernet> Ports> Port Settings**.	--
IP Address	Установка IP-адреса порта LAN.	192.168.0.1
Netmask	Установка сетевой маски порта LAN.	255.255.255.0
IPv6 Address Allocation Type	Установка метода назначения IPv6-адресов на стороне LAN.	SLAAC
MTU	Ввод максимальной единицы передачи.	1500

При выборе «Server» в качестве режима, окно отображается в соответствии с рисунком ниже.



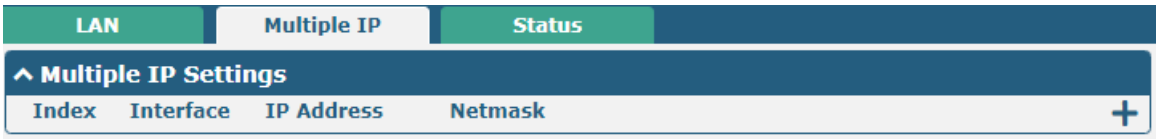
При выборе «Relay» в качестве режима, окно отображается в соответствии с рисунком ниже.



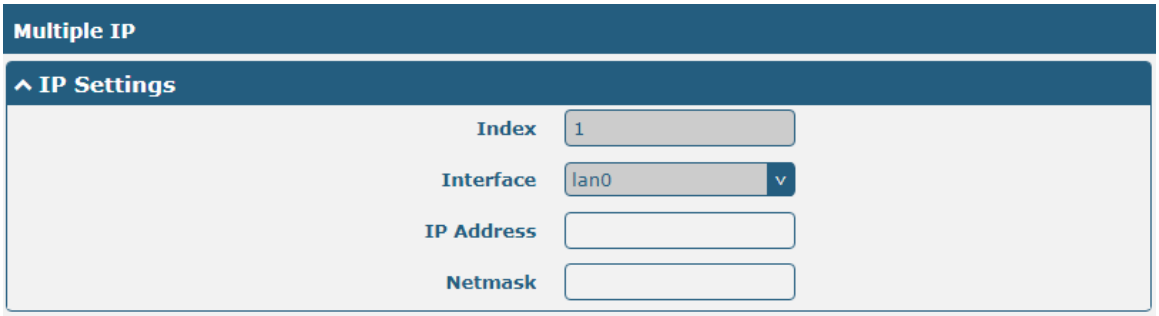
Сети LAN		
Позиция	**Описание**	**По умолчанию**
DHCP Settings		
Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить функцию DHCP.	ON
Mode	Выберите из «Server» или «Relay». • Server: аренда IP-адреса DHCP-клиентам, подключенным к порту LAN. • Relay: маршрутизатор может быть DHCP-ретранслятором, который будет обеспечивать ретрансляционный туннель для решения проблемы, заключающейся в том, что DHCP-клиент и DHCP-сервер не находятся в одной подсети.	Server
IP Pool Start	Определяет начало пула IP-адресов, которые будут сданы в аренду DHCP-клиентам.	192.168.0.2

Сети LAN		
Позиция	**Описание**	**По умолчанию**
IP Pool End	Определяет конец пула IP-адресов, которые будут сданы в аренду DHCP-клиентам.	192.168.0.100
Subnet Mask	Определяет маску подсети IP-адреса, полученного DHCP-клиентами от DHCP-сервера.	255.255.255.0
DHCP Server for Relay	Ввод IP-адреса сервера DHCP-ретрансляции.	Null
DHCP Advanced Settings		
Gateway	Определяет шлюз, назначаемый DHCP-сервером клиентам, который должен находиться в том же сегменте сети, что и пул адресов DHCP.	Null
Primary DNS	Определяет основной DNS-сервер, назначенный DHCP-сервером клиентам.	Null
Secondary DNS	Определяет вторичный DNS-сервер, назначенный DHCP-сервером клиентам.	Null
WINS Server	Определяет Службу имен Интернет для Windows, полученную DHCP-клиентами от DHCP-сервера.	Null
Lease Time	Установка времени аренды, в течение которого клиент может использовать IP-адрес, полученный от DHCP-сервера, в секундах.	120
Static lease	Привязать аренду к соответствию IP-адресу через MAC-адрес. формат: mac,ip;mac,ip;..., например, FF:ED:CB:A0:98:01,192.168.0.200	Null
Expert Options	Введите в это поле некоторые другие опции DHCP-сервера. формат: config-desc;config-desc, например, log-dhcp;quiet-dhcp	Null
Debug Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Включите вывод информации о DHCP.	OFF

Multiple IP



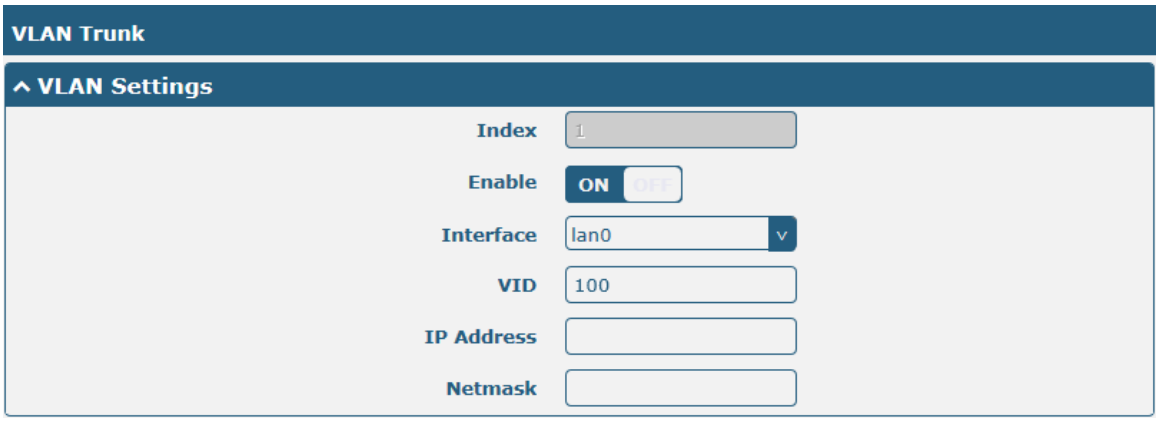
Можно нажать на +, чтобы добавить несколько IP-адресов к порту LAN, или нажмите на ✕, чтобы удалить несколько IP-адресов порта LAN. Теперь нажмите на , чтобы отредактировать несколько IP порта LAN.



IP Settings		
Позиция	**Описание**	**По умолчанию**
Index	Указывает порядковый номер списка.	--
Interface	Отображает редактируемый порт.	--
IP Address	Установка нескольких IP-адресов порта LAN.	Null
Netmask	Установка нескольких сетевых масок порта LAN.	Null

VLAN Trunk

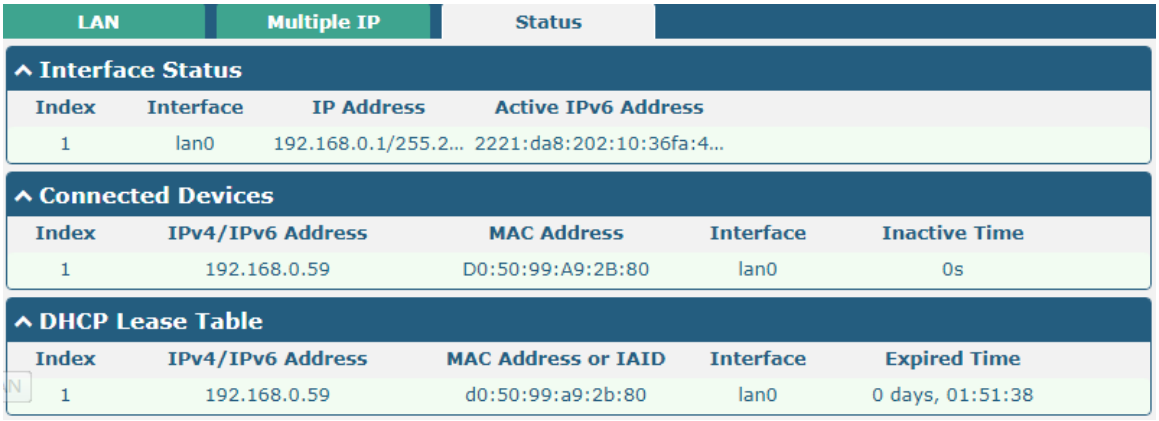
Нажмите на +, чтобы добавить VLAN. Максимальное количество равно 8.



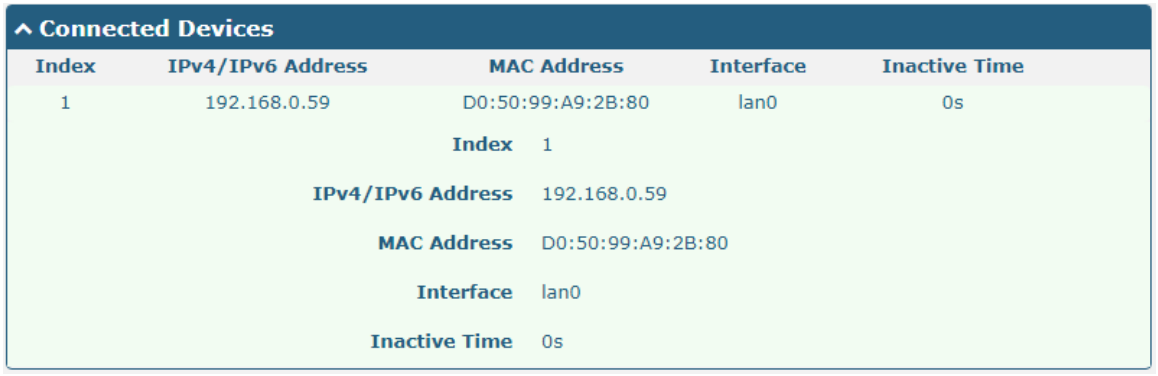
Настройки VLAN		
Позиция	**Описание**	**По умолчанию**
Index	Указывает порядковый номер списка.	--
Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить этот VLAN. Включите, чтобы маршрутизатор мог инкапсулировать и деинкапсулировать тег VLAN.	ON
Interface	Выберите интерфейс, на котором требуется включить функцию магистрали VLAN. Выберите «lan0» или «lan1» в зависимости от вашего ETH0 и соответствующих портов LAN ETH1.	lan0
VID	Установка ID тега VLAN и цифр от 1 до 4094.	100
IP Address	Установка IP-адреса порта VLAN.	Null
Netmask	Установка сетевой маски порта VLAN.	Null

Статус

Этот раздел позволяет просматривать состояние подключения к локальной сети.

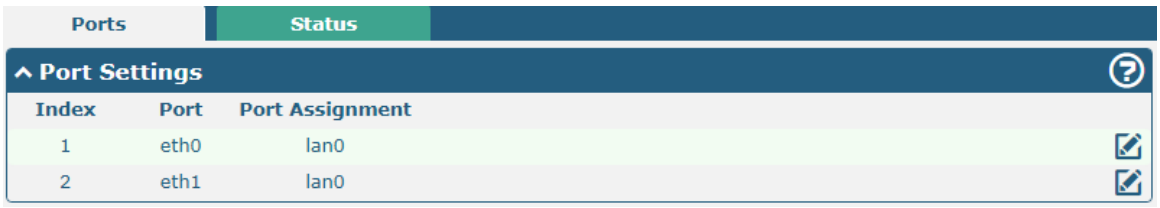


Нажмите на строку состояния, подробная информация о состоянии будет отображаться под строкой. См. скриншоты ниже.

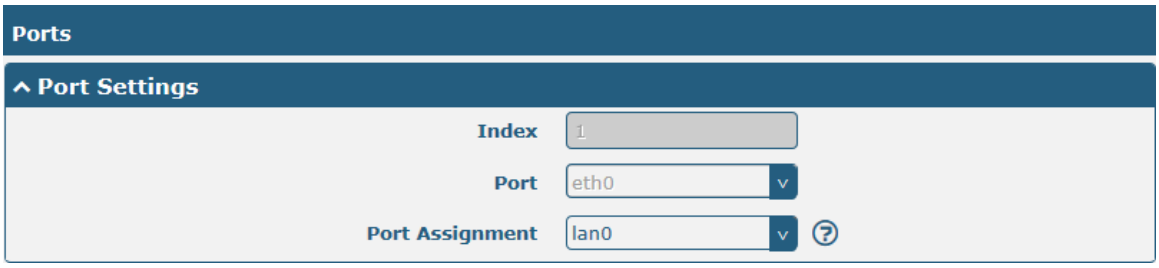


3.8 Interface > Ethernet

Этот раздел позволяет установить соответствующие параметры для Ethernet. Маршрутизатор R2000 имеет два порта Ethernet, включая ETH0 и ETH1. Конфигурация порта ETH0 на маршрутизаторе может выполняться как WAN-порт либо как LAN-порт, также может быть назначение в качестве PoE-порта, тогда как конфигурация порта ETH1 может выполняться в качестве LAN-порта. Настройки по умолчанию для ETH0 и ETH1 – lan0, а их IP-адреса по умолчанию – 192.168.0.1/255.255.255.0.

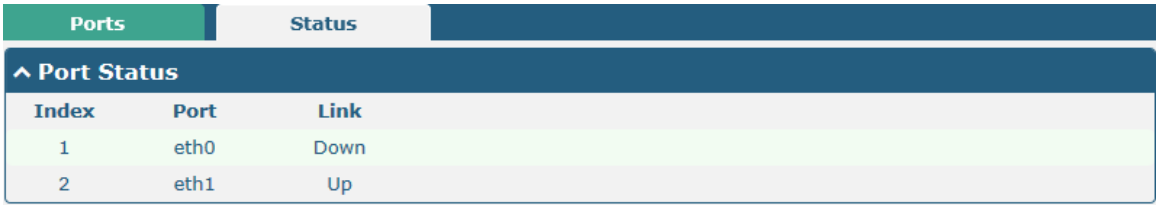


Нажмите на кнопку порта eth0 для конфигурирования его параметров, затем измените параметры назначения порта eth0 во всплывающем окне.



Port Settings		
Позиция	**Описание**	**По умолчанию**
Index	Указывает порядковый номер списка.	--
Port	Отображает редактируемый порт, только для чтения.	--
Port Assignment	Выберите тип порта Ethernet: порт WAN или порт LAN. При настройке порта в качестве порта LAN можно нажать на раскрывающийся список, чтобы выбрать «lan0» или «lan1».	lan0

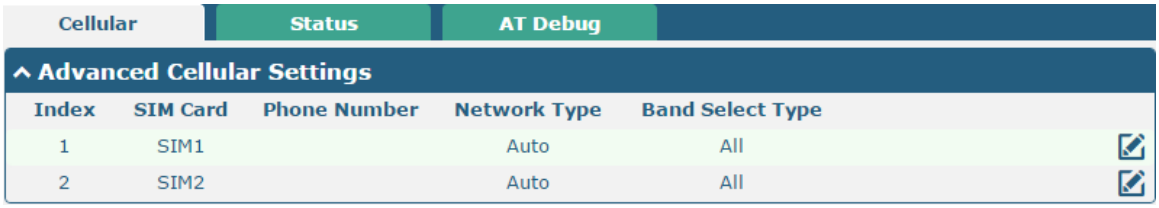
Этот столбец позволяет просматривать состояние порта Ethernet.



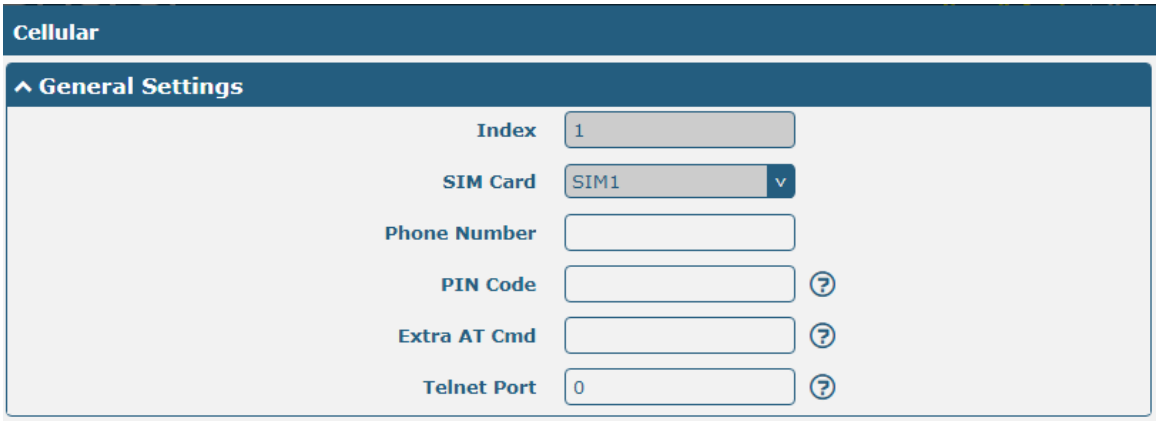
Нажмите на строку состояния, подробная информация о состоянии будет отображаться под строкой. См. скриншоты ниже.

3.9 Interface > Cellular

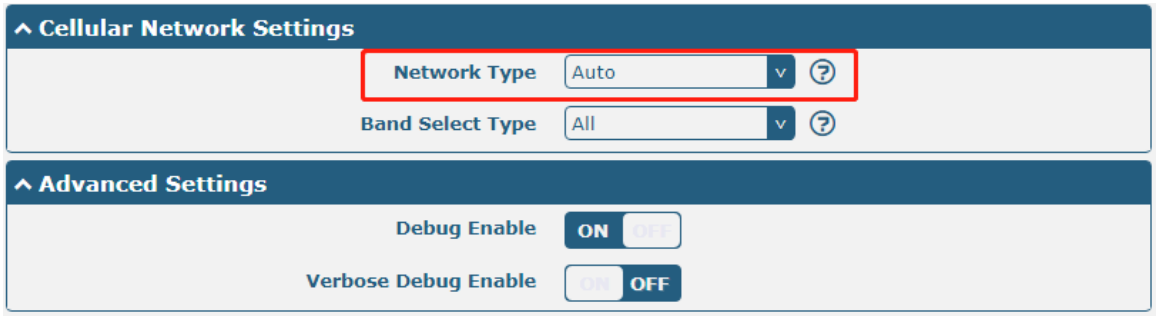
Этот раздел позволяет установить соответствующие параметры сотовой связи. Маршрутизатор R3000 имеет два слота для SIM-карт, но не поддерживает одновременное подключение двух SIM-карт из-за своей одномодульной конструкции. Если вставить одну SIM-карту в первый раз, доступны слоты SIM1 и SIM2.



Нажмите на кнопку в правом углу SIM 1 для редактирования параметров.

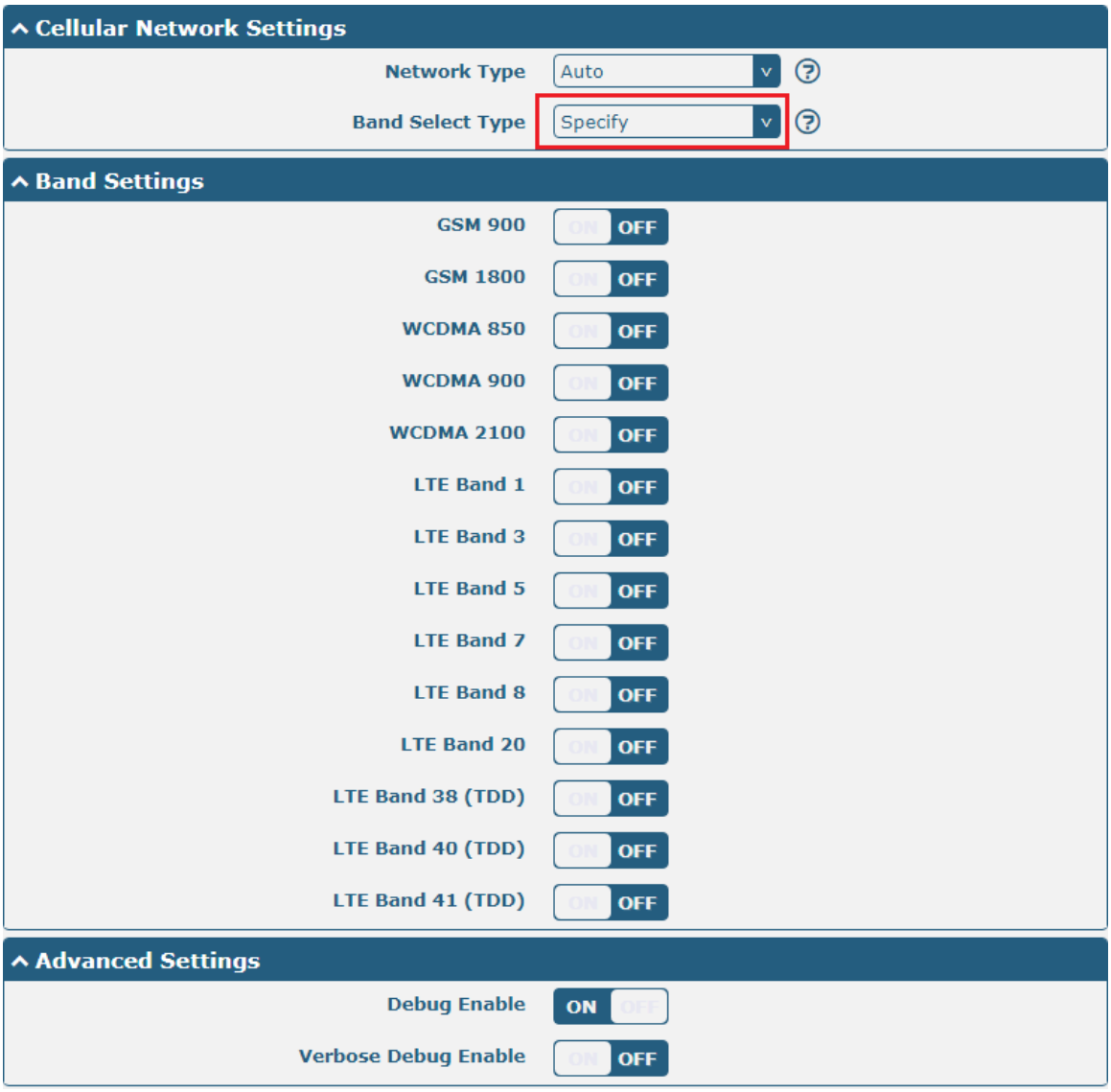


При выборе «Auto» в качестве сети, окно отображается в соответствии с рисунком ниже.

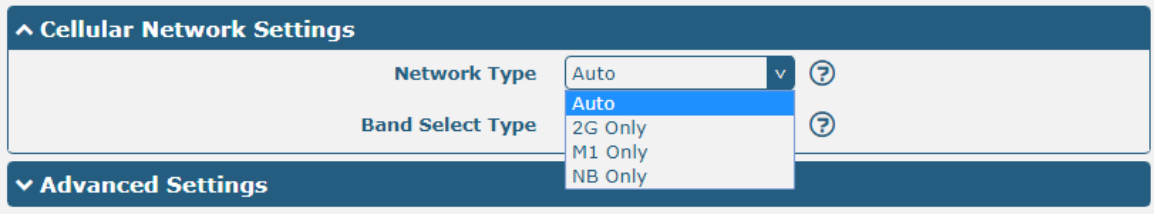


Примечание: При наличии модуля BG96 опции в «Типе сети» следующие:

При выборе «Specify» в качестве типа полосы, окно отображается в соответствии с рисунком ниже.



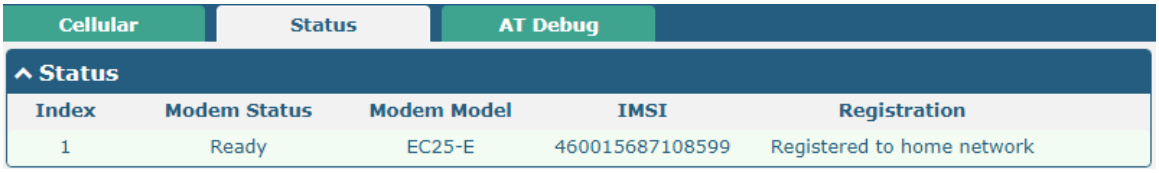
Примечание:Когда модулем при выборе устройства стал BG96, опциями «Network Type» являются:



Сотовый		
Позиция	**Описание**	**По умолчанию**
General Settings		
Index	Указывает порядковый номер списка.	--
SIM Card	Показ текущей редактируемой SIM-карты.	SIM1
Phone Number	Ввод телефонного номера SIM-карты.	Null

Сотовый		
Позиция	**Описание**	**По умолчанию**
PIN Code	Ввод PIN-кода из 4–8 символов, используемого для разблокировки SIM-карты.	Null
Extra AT Cmd	Ввод AT-команд, используемых для инициализации сотовой сети.	Null
Telnet Port	Указание порта прослушивания службы telnet, используемого для AT через Telnet.	0
Cellular Network Settings		
Network Type	Выберите тип сотовой сети, прописанный в запросе на доступ к сети. Выберите из «Auto», «2G Only», «2G First», «3G Only», «3G First», «4G Only», «4G First». • Auto: автоматическое подключение к сети с лучшим сигналом • 2G Only: подключена только сеть 2G • 2G First: предпочтительное подключение к сети 2G • 3G Only: подключена только сеть 3G • 3G First: предпочтительное подключение к сети 3G • 4G Only: подключена только сеть 4G • 4G First: предпочтительное подключение к сети 4G Примечание:Когда модулем при выборе устройства стал BG96, выберите из «Auto», «2G Only», «M1 Only», «NB Only». • Auto: автоматическое подключение к сети с лучшим сигналом • 2G Only: подключена только сеть 2G • M1 Only: подключена только сеть CAT M1 • NB Only: подключена только сеть NB-IOT	Auto
Band Select Type	Выберите из «All» или «Specify». Можно выбрать определенные полосы, выбрав «Specify».	All
Advanced Settings		
Debug Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Включите вывод отладочной информации.	ON
Verbose Debug Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Включите вывод подробной отладочной информации.	OFF

Этот раздел позволяет просматривать состояние подключения к сотовой сети.



Нажмите на строку состояния, подробная информация о состоянии будет отображаться под строкой.

Status

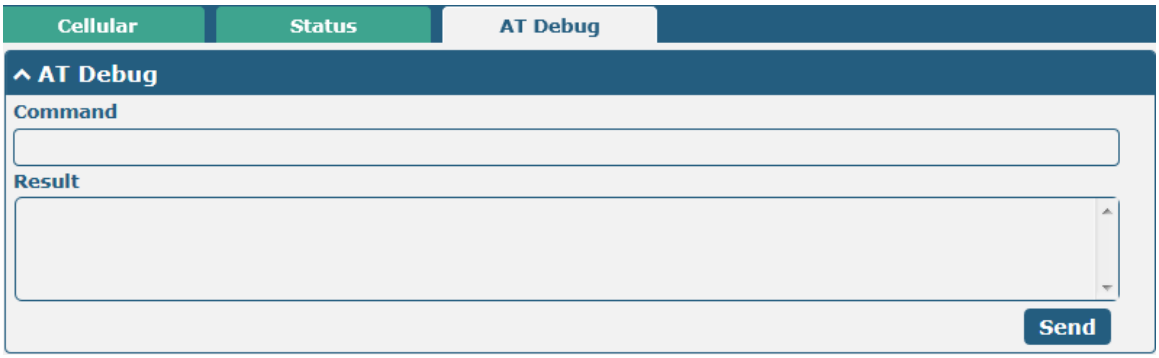
Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	EC25-E	460015687108599	Registered to home network

Index	1
Modem Status	Ready
Modem Model	EC25-E
Current SIM	SIM1
Phone Number	
IMSI	460015687108599
ICCID	89860119801073537094
Registration	Registered to home network
Network Provider	CHN-UNICOM
Network Type	LTE
Signal Strength	27 (-59dBm)
Bit Error Rate	99
PLMN ID	46001
Local Area Code	2507
Cell ID	6074716
IMEI	866758047488842
Firmware Version	EC25EFAR06A03M4G

Статус	
Позиция	**Описание**
Index	Указывает порядковый номер списка.
Modem Status	Отображает статус радиомодуля.
Modem Model	Отображает модель радиомодуля.
Current SIM	Отображает SIM-карту, которую использует маршрутизатор.
Phone Number	Отображает номер телефона текущей SIM-карты. **Примечание.** Эта опция будет отображаться, если ввести вручную в разделе **Cellular > Advanced Cellular Settings > SIM1/SIM2 > General Settings > Phone Number**.
IMSI	Отображает номер IMSI текущей SIM-карты.
ICCID	Отображает номер ICCID текущей SIM-карты.
Registration	Отображает текущий статус сети.
Network Provider	Отображает имя сетевого провайдера.
Network Type	Отображает текущий тип сетевой службы, например, GPRS.
Signal Strength	Отображает уровень сигнала, обнаруженный мобильным устройством.
Bit Error Rate	Отображает текущую частоту ошибок по битам.
PLMN ID	Отображает текущий ID PLMN.
Local Area Code	Отображает текущий код местности, используемый для идентификации другой области.

Статус	
Позиция	**Описание**
Cell ID	Отображает текущий ID соты, используемый для определения местоположения маршрутизатора.
IMEI	Отображает номер международного идентификатора оборудования мобильной связи (IMEI) радиомодуля.
Firmware Version	Отображает текущую версию аппаратно-программного обеспечения радиомодуля.

Эта страница позволяет проверить AT Debug.



AT Debug		
Позиция	**Описание**	**По умолчанию**
Command	Введите в это текстовое поле AT-команду, которую необходимо отправить на сотовый модуль.	Null
Result	Отображает в этом текстовом поле AT-команду, на которую ответил сотовый модуль.	Null
Send	Нажмите на кнопку, чтобы отправить AT-команду.	--

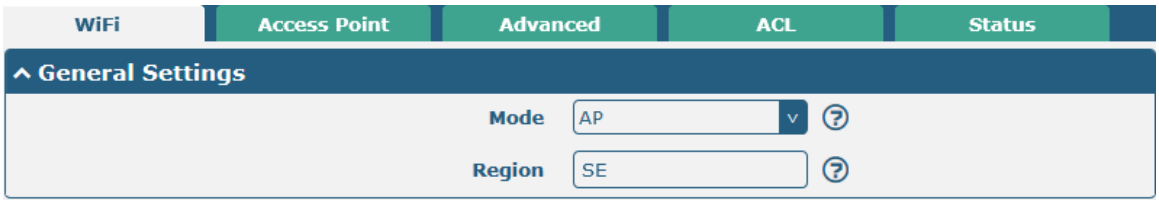
3.10 Interface > WiFi (опционально)

В этом разделе можно настроить параметры двух режимов WiFi. Маршрутизатор поддерживает либо режим точки доступа (AP) Wi-Fi, либо режим клиента и по умолчанию является режимом AP.

WiFi AP

Настройка маршрутизатора в качестве AP WiFi

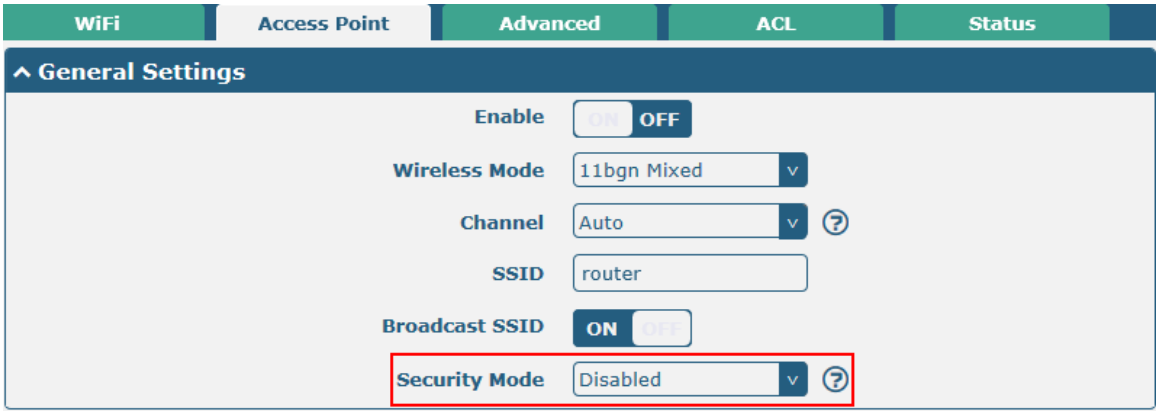
Нажмите на **Interface > WiFi > WiFi**, выберите в качестве режима «AP» и нажмите на «Submit».



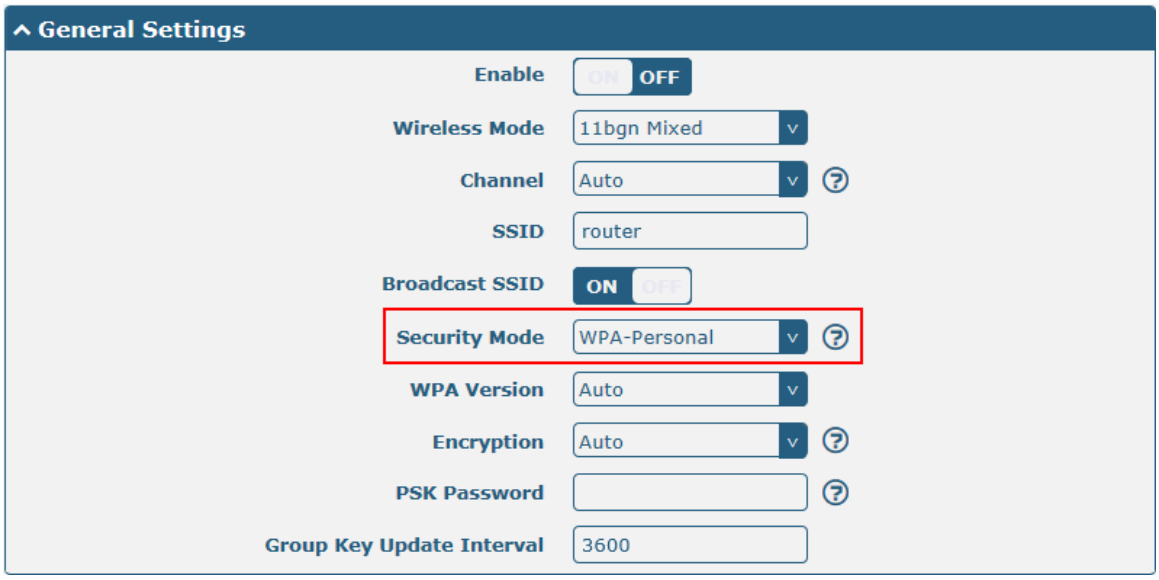
Примечание:. Необходимо обязательно нажать на **Save & Apply > Reboot** после завершения настройки, чтобы

настройки вступили в силу.

Нажмите на столбец **Access Point**, чтобы настроить параметры AP WiFi. По умолчанию режим безопасности установлен как «Disabled».

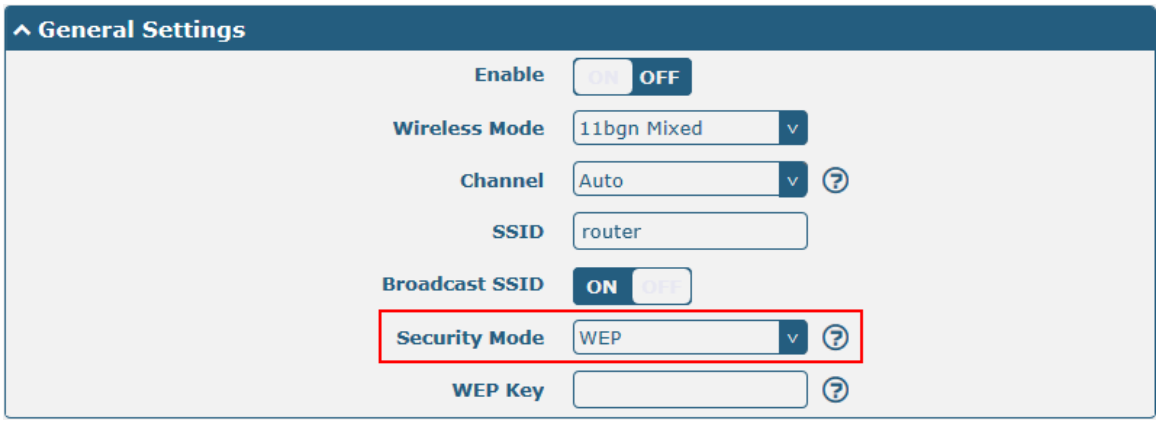


При установке «WPA-Personal» в качестве режима безопасности окно отображается в соответствии с рисунком ниже.



При установке «WPA-Personal» в качестве режима безопасности окно отображается в соответствии с рисунком ниже.

При установке «WEP» в качестве режима безопасности окно отображается в соответствии с рисунком ниже.



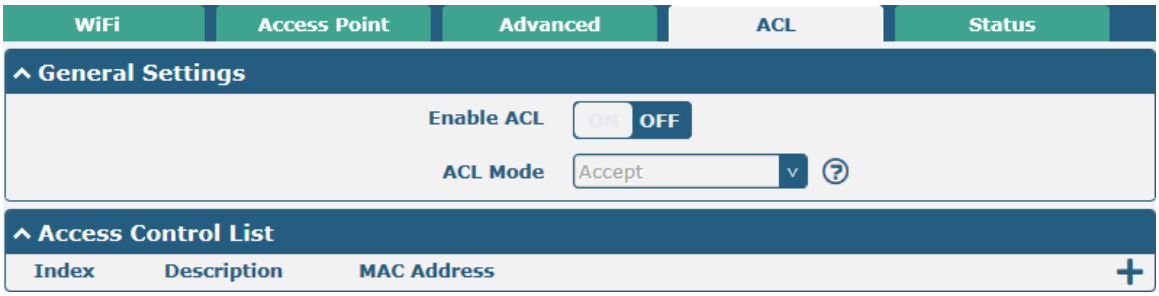
General Settings и Access Point		
Позиция	**Описание**	**По умолчанию**
Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить опцию точки доступа WiFi.	OFF
Wireless Mode	Выберите из «11bgn Mixed», «11b Only», «11g Only» либо «11n Only». • 11bgn Mixed: Сочетание трех договоров для обратной совместимости • 11b only: IEEE 802.11b，11Мбит/с~2.4ГГц • 11g only: IEEE 802.11g，54Мбит/с~2.4ГГц • 11n only: IEEE 802.11n，300Мб/с~600Мб/с	11bgn Mixed

General Settings и Access Point		
Позиция	**Описание**	**По умолчанию**
Channel	Выберите частотный канал, включая «Auto», «1», «2»–«13». • Auto: маршрутизатор будет сканировать все частотные каналы, пока не будет найден лучший. • 1~13: маршрутизатор будет настроен на работу с этим каналом Ниже представлены частоты 1~13 каналов: 1: 2412 МГц 2: 2417 МГц 3: 2422 МГц 4: 2427 МГц 5: 2432 МГц 6: 2437 МГц 7: 2442 МГц 8: 2447 МГц 9: 2452 МГц 10: 2457 МГц 11: 2462 МГц 12: 2467 МГц 13: 2472 МГц	Auto
SSID	Введите идентификатор набора услуг, название используемой беспроводной сети. SSID клиента и SSID AP должны быть идентичны, чтобы клиент и AP могли связываться друг с другом. Введите от 1 до 32 символов.	маршрутизатор
Broadcast SSID	Нажмите на кнопку-переключатель, чтобы включить/отключить передаваемый SSID. Если он включен, клиент может сканировать используемый SSID. Если он отключен, клиент не может сканировать используемый SSID. Если необходимо подключиться к AP маршрутизатора, вручную введите SSID точки доступа маршрутизатора на стороне клиента WiFi.	ON

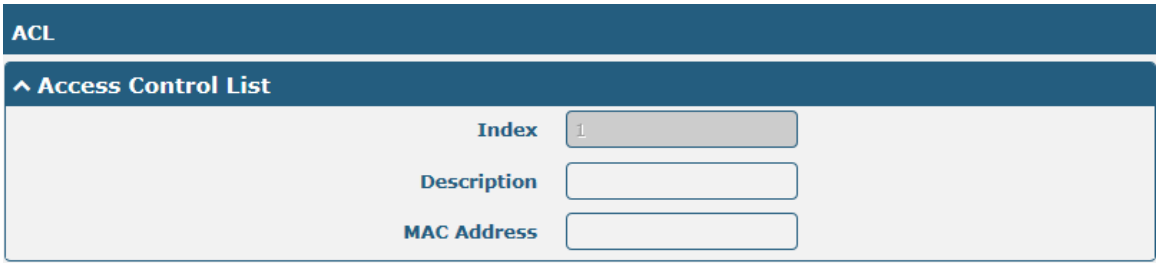
General Settings и Access Point		
Позиция	**Описание**	**По умолчанию**
Security Mode	Выберите из «Disabled», «WPA-Personal», «WEP-Enterprise» или «WEP». • Disabled: Пользователю предоставляется доступ к сети WiFi без пароля **Примечание**. В целях безопасности настоятельно рекомендуется не выбирать этот режим. • WPA-Personal: Доступ с защитой сети WiFi предоставляет один пароль, используемый для аутентификации идентичности • WPA-Enterprise: Предоставляет интерфейс аутентификации для EAP, аутентификация которого возможна через Radius-сервер аутентификации либо по другой расширенной аутентификации. • WEP: протокол эквивалента конфиденциальности проводных сетей (WEP) обеспечивает шифрование для передачи данных беспроводного устройства.	Disabled
WPA Version	Выберите из «Auto», «WPA» или «WPA2». • Auto: маршрутизатор автоматически выберет наиболее подходящую версию WPA. • WPA2 является более надежной функцией безопасности, чем WPA	Auto
Encryption	Выберите из «Auto», «TKIP» или «AES». • Auto: маршрутизатор автоматически выберет наиболее подходящее шифрование. • TKIP: шифрование с использованием временных ключей (TKIP) использует беспроводное соединение. Шифрование TKIP можно использовать для WPA-PSK и WPA с аутентификацией 802.1x. **Примечание**. Не рекомендуется использовать шифрование TKIP в режиме 802.11n. • AES: шифрование AES использует беспроводное соединение. AES можно использовать для CCMP WPA-PSK и WPA с аутентификацией 802.1x. AES является более сильным алгоритмом шифрования, чем TKIP	Auto

General Settings и Access Point		
Позиция	**Описание**	**По умолчанию**
PSK Password	Введите пароль предопределенного ключа. Когда маршрутизатор функционирует в режиме AP, введите главный ключ для генерирования ключей для шифрования. Пароль PSK используется в качестве основы для методов шифрования (либо типов шифров) при соединении WLAN. Пароль PSK должен быть сложным и максимально длинным. В целях безопасности данный пароль PSK подлежит раскрытию исключительно пользователям, которым он нужен при условии его регулярной смены. Введите от 8 до 63 символов.	Null
Radius Authentication Server Address	Введите адрес radius-сервера аутентификации	Null
Radius Authentication Server Port	Введите порт radius-сервера аутентификации	1812
Radius Server Share Secret	Введите совместно используемый секретный ключ radius-сервера аутентификации	Null
Group Key Update Interval	Введите временной период обновления группового ключа	3600
WEP Key	Введите ключ WEP. Длина ключа должна составлять от 10 до 26 шестнадцатеричных цифр, в зависимости от того, какой ключ WEP используется, на 64 или 128 цифр.	Null

Advanced Settings		
Позиция	**Описание**	**По умолчанию**
Max Associated Stations	Установка максимального количества клиентов, которым разрешен доступ к AP маршрутизатора.	64
Beacon Interval	Установите временной интервал, в котором маршрутизатор AP передает сигнал, используемый для аутентификации беспроводной сети.	100
DTIM Period	Установите период для сообщений об индикации трафика доставки, и маршрутизатор AP будет осуществлять многоадресную передачу данных за этот период.	2
RTS Threshold	Установите порог «запрос на рассылку» Когда порог установлен на уровне 2347, маршрутизатор не будет отправлять сигнал детектирования до рассылки данных. А когда порог установлен на 0, маршрутизатор AP отправит сигнал обнаружения до рассылки данных.	2347
Fragmentation Threshold	Установите порог фрагментации WiFi AP. Рекомендуется использовать значение по умолчанию 2346.	2346
Transmit Rate	Установка скорости передачи. Вы можете выбрать Auto или назначить Transmit Rate (скорость передачи данных), в т.ч. 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps, MCS0, MCS1, MCS2, MCS3, MCS4, MCS5, MCS6 и MCS7.	Auto
11N Transmit Rate	Установить скорость передачи данных в режиме IEEE 802.11n либо значение по умолчанию на «Auto».	Auto
Transmit Power	Выбрать из «Max», «High», «Medium» либо «Low».	Max
Channel Width	Выберите из «Auto», «20MHz» либо «40MHz». **Примечание**: диапазон канала 40 МГц предоставляет более высокую доступную скорость передачи данных, в два раза больше диапазона канала 20 МГц.	Auto
Enable WMM	Нажмите на кнопку-переключатель, чтобы включить/отключить опцию WMM.	ON
Enable Short GI	Нажмите на кнопку-переключатель, чтобы включить/отключить опцию Short Guard Interval. Short GI – незаполненное время между двумя символами, обеспечивающее длительное буферное время для задержки сигнала. Использование Short GI повышает скорость передачи данных на 11%, но также приводит к увеличению числа ошибок в пакете.	ON
Enable AP isolation	Нажмите на кнопку-выключатель, чтобы включить/отключить опцию изоляции AP. При включении маршрутизатор будет изолировать все подключенные беспроводные устройства. Беспроводное устройство не может обеспечить доступ к маршрутизатору непосредственно через сеть WLAN.	OFF
Debug Level	Выберите из «verbose», «debug», «info», «notice», «warning» или «none».	none



Нажмите на +, чтобы добавить MAC-адрес в список контроля доступа. Максимальное количество MAC-адресов – 64.



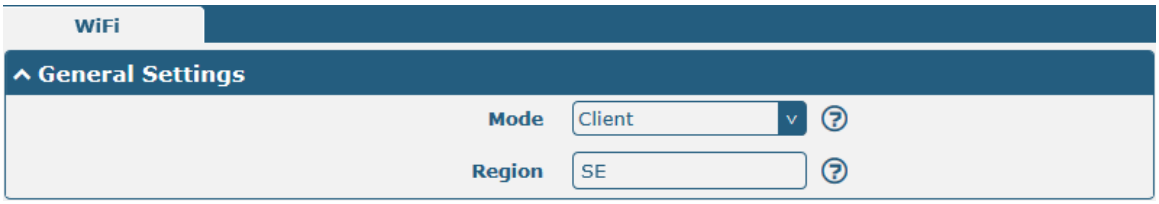
ACL		
Позиция	**Описание**	**По умолчанию**
General Settings		
Enable ACL	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию.	OFF
ACL Mode	Выберите из «Accept» или «Deny». • Accept: могут быть разрешены только пакеты, соответствующие объектам «Списка контроля доступа». • Deny: будут запрещены все пакеты, соответствующие объектам «Списка контроля доступа». **Примечание**. Маршрутизатор может разрешать или запрещать только устройства, которые включены в «Список контроля доступа» одновременно.	Accept
Access Control List		
Index	Указывает порядковый номер списка.	--
Описание	Ввод описания для этого списка контроля доступа.	Null
MAC Address	Здесь добавляется MAC-адрес.	Null

Этот раздел позволяет просматривать состояние точки доступа.

Клиент WiFi

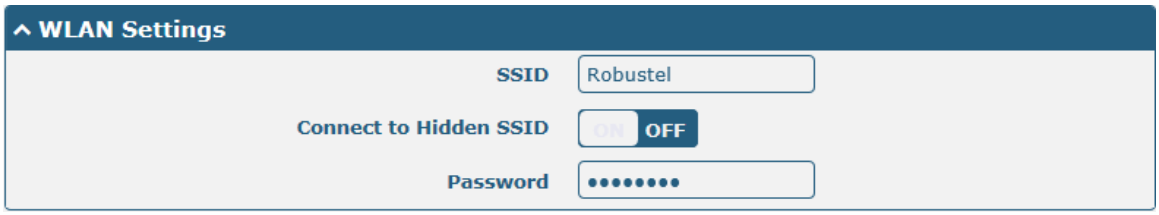
Настройка маршрутизатора в качестве клиента WiFi

Нажмите на **Interface > WiFi > WiFi**, выберите в качестве режима «Client» и нажмите на «Submit».

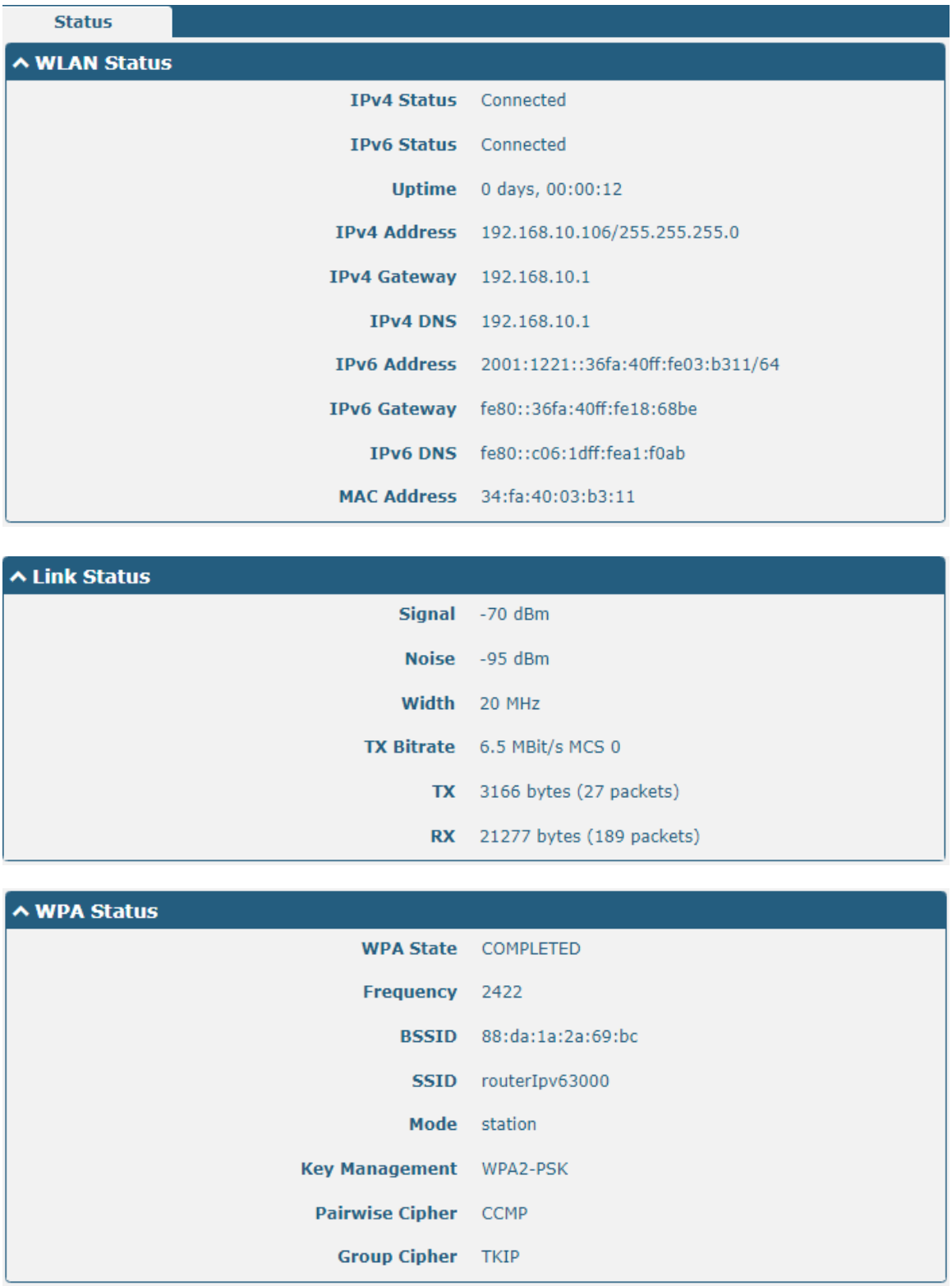


После этого под списком интерфейсов появится столбец «WLAN».

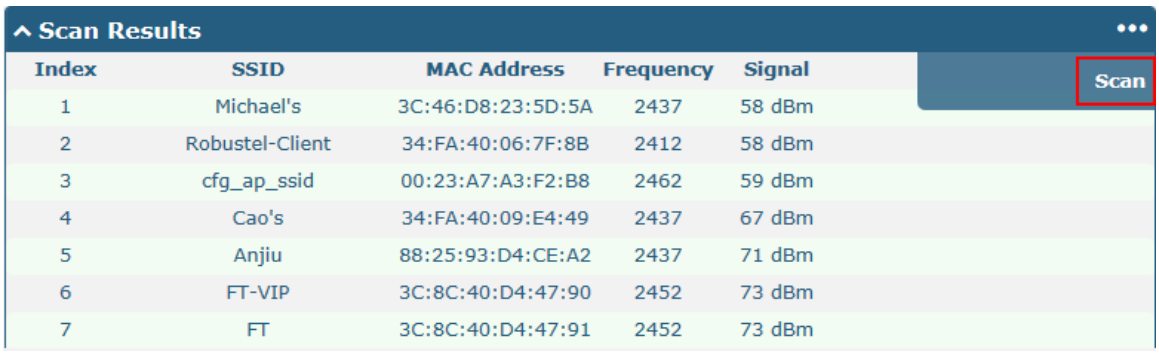
Нажмите на **Interface > Link Manager > Link Settings** и нажмите на кнопку WLAN «Edit», затем настройте соответствующие параметры WLAN.



Нажмите на **Interface > WLAN**, чтобы настроить параметры WiFi-клиента после установки режима «Client». Необходимо обязательно нажать на **Save & Apply > Reboot** после завершения настройки, чтобы настройки вступили в силу.



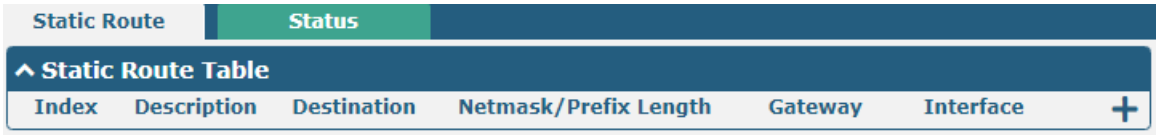
Данное окно позволяет вам отсканировать вашу область на предмет всех доступных SSID. Нажмите на кнопку ..., затем нажмите «Scan» для обновления окружающего SSID.



3.11 Network > Route

Данный раздел позволяет вам установить статический маршрут. Статический маршрут – это форма маршрутизации, которая возникает, когда маршрутизатор использует настроенную вручную запись маршрутизации, а не информацию из трафика динамической маршрутизации. Протокол информации о маршрутах (RIP) широко используется в небольших сетях со стабильной скоростью использования. Протокол маршрутизации по принципу выбора кратчайшего пути (OSPF) – это маршрутизатор в рамках отдельной автономной системы, который используется в большой сети.

Статический маршрут



Нажмите на кнопку +, чтобы добавить статический маршрут. Максимальное количество равно 20.

Статический маршрут		
Позиция	**Описание**	**По умолчанию**
Index	Указывает порядковый номер списка.	--

Статический маршрут		
Позиция	**Описание**	**По умолчанию**
Description	Ввод описание для этого статического маршрута.	Null
Destination	Ввод IP-адреса целевого хоста или целевой сети.	Null
Netmask/IPv6 address Prefix Length	Ввод сетевой маски целевого хоста или целевой сети.	Null
Gateway	Определение шлюза места назначения.	Null
Interface	Выбор соответствующего порта соединения, который вы хотите настроить.	wwan

Статус

Это окно позволяет просматривать статус маршрута.

Static Route | Status

Route Table

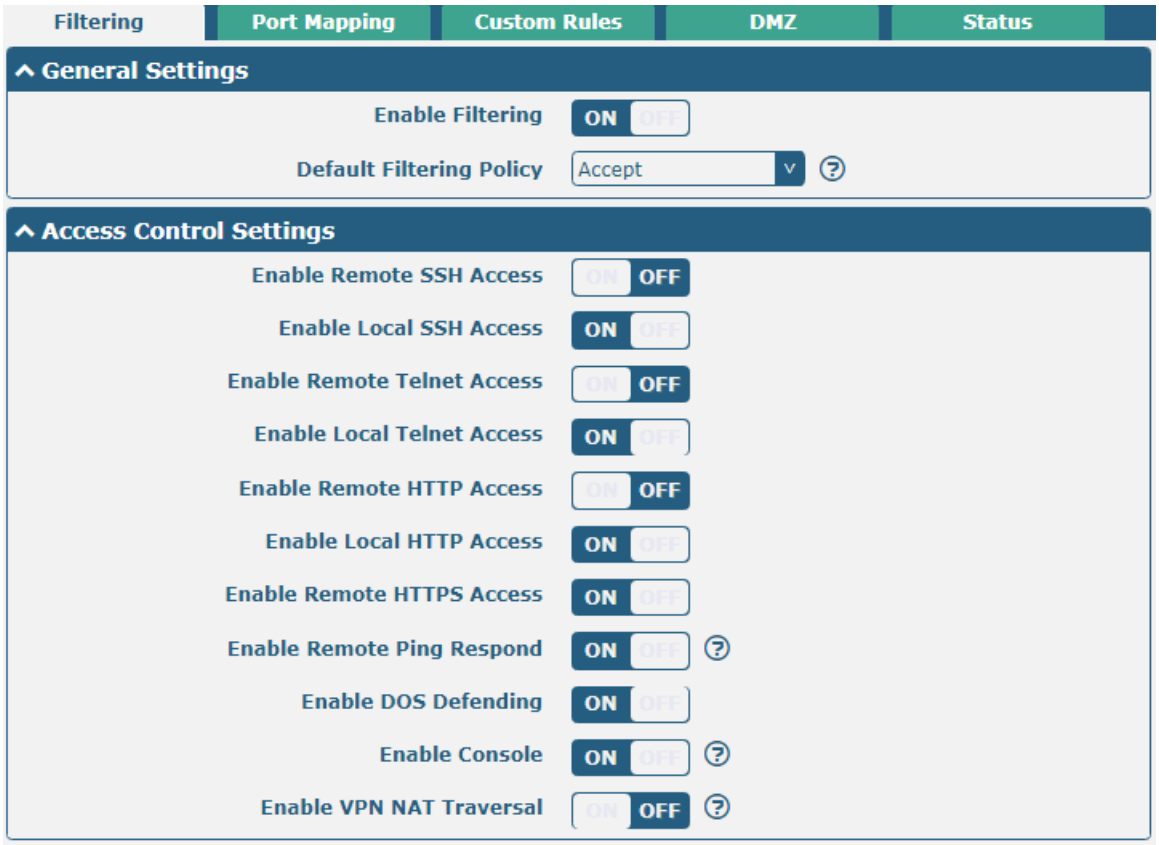
Index	Destination	Netmask/Prefix Length	Gateway	Interface	Metric
1	0.0.0.0	0.0.0.0	192.168.10.1	wlan0	0
2	192.168.0.0	255.255.255.0	0.0.0.0	lan0	0
3	192.168.10.0	255.255.255.0	0.0.0.0	wlan0	0
4	2001:1221::	64	::	wlan0	256
5	2001:4860:4860::...	128	fe80::36fa:40ff:fe...	wlan0	0
6	2400:da00:2::29	128	fe80::36fa:40ff:fe...	wlan0	0
7	2421:da8:202:10::	64	::	lan0	256
8	fe80::	64	::	lan0	256
9	fe80::	64	::	eth1	256
10	fe80::	64	::	wwan	256
11	fe80::	64	::	wlan0	256
12	::	0	fe80::36fa:40ff:fe...	wlan0	1024
13	ff02::1	128	::	lan0	0
14	ff02::1	128	::	wlan0	0
15	ff02::2	128	::	wlan0	0
16	ff02::16	128	::	lan0	0
17	ff02::1:2	128	::	wlan0	0
18	ff02::1:3	128	::	lan0	0
19	ff02::1:ff14:4f32	128	::	lan0	0
20	ff00::	8	::	lan0	256
21	ff00::	8	::	eth1	256
22	ff00::	8	::	wwan	256
23	ff00::	8	::	wlan0	256

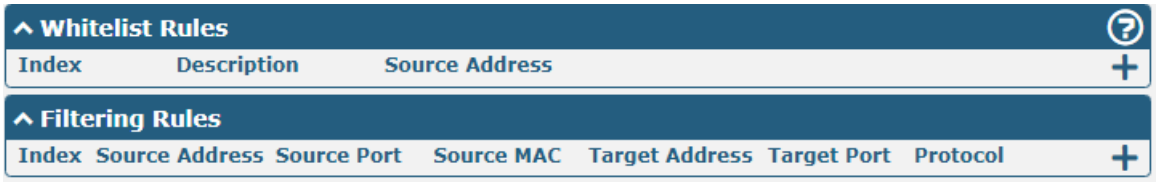
3.12 Network > Firewall

В этом разделе можно настроить межсетевой экран и связанные с ним параметры, включая фильтрацию, сопоставление портов и DMZ.

Фильтрация

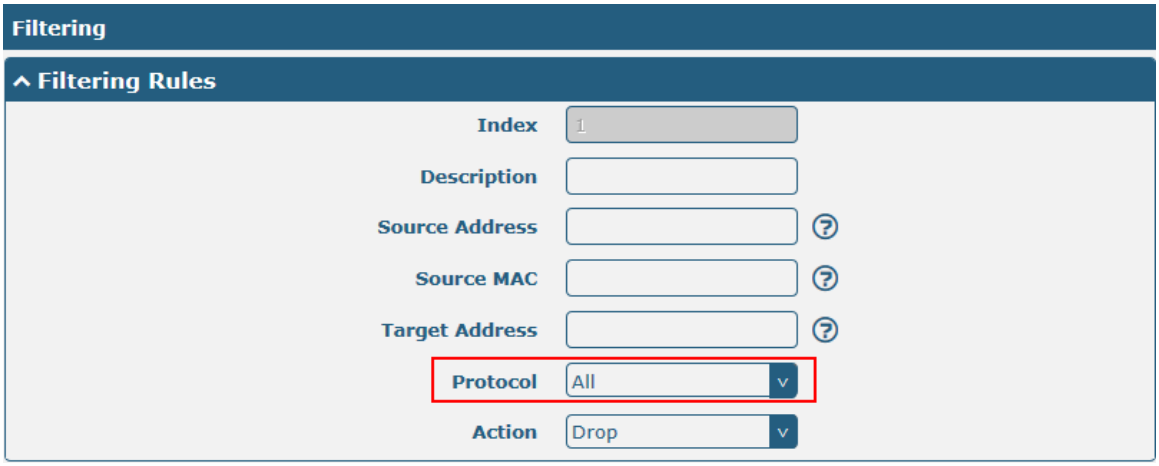
Правила фильтрации могут использоваться для принятия или блокировки доступа определенных пользователей или портов к используемому маршрутизатору. Нажмите Network> Firewall> Filter. Отображается следующая информация:



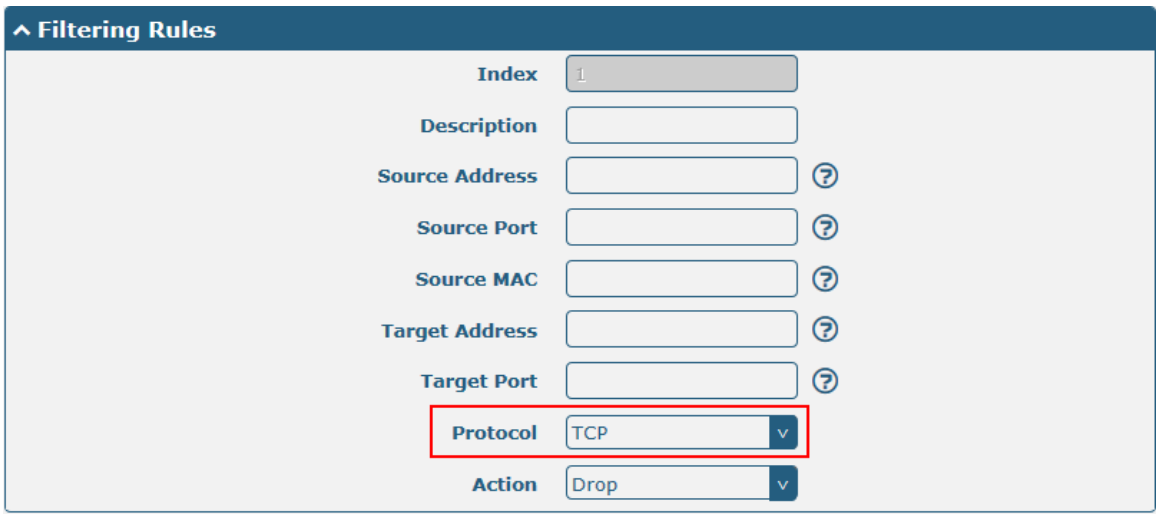


Нажмите на кнопку + для добавления правил списка аккредитованных лиц

Нажмите на кнопку + для добавления правила фильтрации. Максимальное количество равно 50. При установке по умолчанию значения «All» или выборе в качестве протокола «ICMP» или «ICMPv6» окно отображается в соответствии с рисунком ниже. Возьмем, к примеру, значение «All».



При выборе протокола «TCP», «UDP» или «TCP-UDP» окно отображается в соответствии с рисунком ниже. Возьмем, к примеру, значение «TCP».



Фильтрация		
Позиция	**Описание**	**По умолчанию**
General Settings		
Enable Filtering	Нажмите на кнопку-переключатель, чтобы включить/отключить опцию фильтрации.	ON
Default Filtering Policy	Выберите из «Accept» или «Drop». Невозможно изменить, если таблица правил фильтрации не пуста. • Accept: маршрутизатор будет принимать все запросы на подключение, кроме хостов, которые соответствуют списку фильтров отбрасывания. • Drop: маршрутизатор отбрасывает все запросы на подключение, кроме хостов, которые соответствуют списку фильтров приема.	Accept

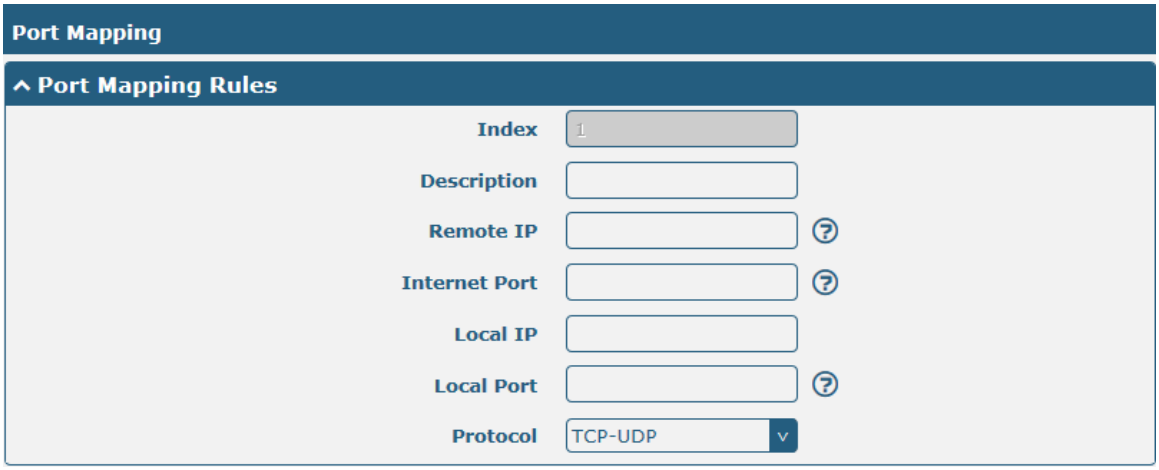
Фильтрация		
Позиция	**Описание**	**По умолчанию**
Access Control Settings		
Enable Remote SSH Access	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Если этот параметр включен, Интернет-пользователь может получить доступ к маршрутизатору удаленно через SSH.	OFF
Enable Local SSH Access	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Если этот параметр включен, LAN-пользователь может получить доступ к маршрутизатору локально через SSH.	ON
Enable Remote Telnet Access	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Если этот параметр включен, Интернет-пользователь может получить доступ к маршрутизатору удаленно через Telnet.	OFF
Enable Local Telnet Access	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Если этот параметр включен, LAN-пользователь может получить доступ к маршрутизатору локально через Telnet.	ON
Enable Remote HTTP Access	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Если этот параметр включен, Интернет-пользователь может получить доступ к маршрутизатору удаленно через HTTP.	OFF
Enable Local HTTP Access	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Если этот параметр включен, LAN-пользователь может получить доступ к маршрутизатору локально через HTTP.	ON
Enable Remote HTTPS Access	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Если этот параметр включен, Интернет-пользователь может получить доступ к маршрутизатору удаленно через HTTPS.	ON
Enable Remote Ping Respond	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Если этот параметр включен, маршрутизатор будет отвечать на Ping-запросы от других хостов в Интернете.	ON
Enable DOS Defending	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Если этот параметр включен, маршрутизатор будет защищать DOS. Dos-атака – это попытка сделать устройство или сетевой ресурс недоступными для предполагаемых пользователей.	ON
Enable debug port	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию.	ON
Enable vpn nat traversal	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Если этот параметр включен, включите прохождение NAT для пакетов GRE/L2TP/PPTP VPN.	OFF
Правила списка аккретитованных лиц		
Index	Указывает порядковый номер списка.	--
Описание	Ввод описания для этого (белого) списка аккредитованных лиц.	Null
Source Address	Указание источника доступа и ввод его порта источника.	Null
Filtering Rules		
Index	Указывает порядковый номер списка.	--

Фильтрация		
Позиция	**Описание**	**По умолчанию**
Описание	Ввод описания для этого правила фильтрации.	Null
Source Address	Указание источника доступа и ввод его порта источника.	Null
Source Port	Указание источника доступа и ввод его порта источника.	Null
Source MAC	Указание источника доступа и ввод его MAC-адреса источника.	Null
Target Address	Ввод целевого адреса, к которому отправитель доступа хочет получить доступ.	Null
Target Port	Ввод целевого порта, к которому отправитель доступа хочет получить доступ.	Null
Protocol	Выберите из «All», «TCP», «UDP», «ICMP», «ICMPv6» и «TCP-UDP». **Примечание**. Рекомендуется выбрать «All», если неизвестно, какой протокол использовать в приложении.	All
Action	Выберите из «Accept» или «Drop». • Accept: при отказе от политики фильтрации по умолчанию маршрутизатор отбрасывает все запросы на подключение, кроме хостов, которые соответствуют этому списку фильтрации принятия. • Accept: при принятии политики фильтрации по умолчанию маршрутизатор принимает все запросы на подключение, кроме хостов, которые соответствуют этому списку фильтрации отбрасывания.	Drop

Перенаправление портов

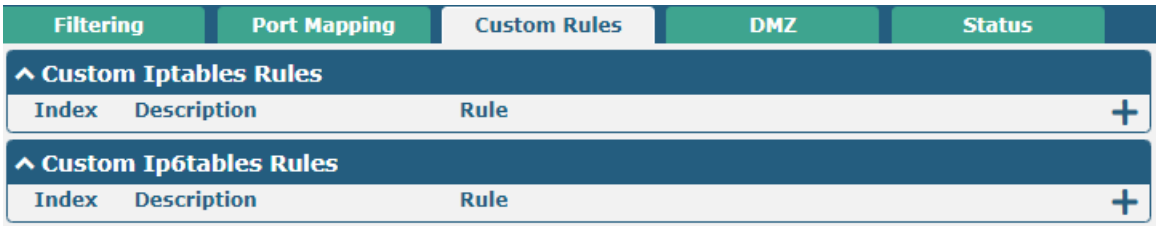
Перенаправление портов устанавливается в маршрутизаторе вручную, и все данные, полученные от определенных портов в общедоступной сети, передаются на определенный порт по определенному IP-адресу во внутренней сети. Нажмите Network> Firewall> Port Mapping для отображения следующих данных:

Нажмите на +, чтобы добавить правила отображения портов. Максимальное количество правил равно 40.

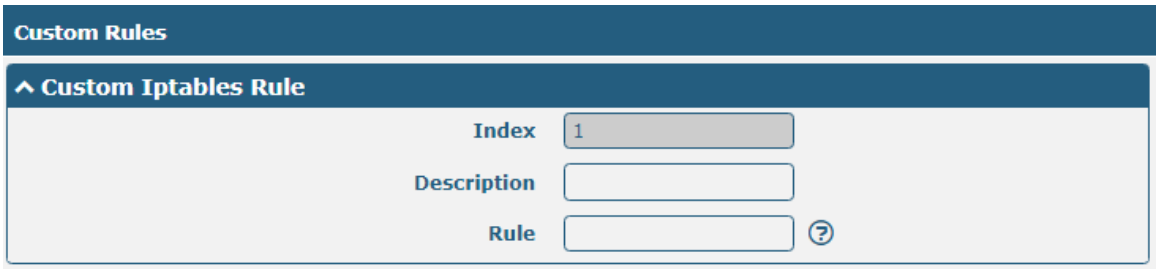


Port Mapping Rules		
Позиция	**Описание**	**По умолчанию**
Index	Указывает порядковый номер списка.	--
Description	Ввод описания для этого отображения портов.	Null
Remote IP	Указание хоста или сети, которая может получить доступ к локальному IP-адресу. Пустое поле означает отсутствие ограничений, например, 10.10.10.10/255.255.255.255 или 192.168.1.0/24	Null
Internet Port	Установка интернет-порта маршрутизатора, к которому другие хосты могут получить доступ из сети Интернет.	Null
Local IP	Ввод IP-адреса LAN маршрутизатора, который будет перенаправлен на интернет-порт маршрутизатора.	Null
Local Port	Ввод порта IP LAN маршрутизатора.	Null
Protocol	Выберите из «TCP», «UDP» или «TCP-UDP» в зависимости от требований вашего приложения.	TCP-UDP

Пользовательские правила, то есть правила, которые определяются пользователем. Нажмите Network> Firewall> Custom Rule для отображения следующих данных:



Нажмите на +, чтобы добавить пользовательское правило IPv4 или IPv6, окно отобразится следующим образом (например, «IPv4»):

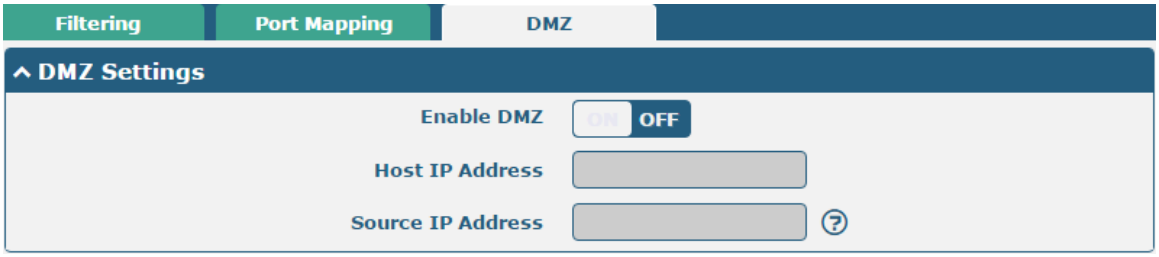


Правила клиентского брандмауера		
Позиция	**Описание**	**По умолчанию**
Index	Указывает порядковый номер списка.	--
Description	Ввод описания для данных правил клиентского брандмауера.	Null
Rule	Ввод специальных правил.	Null

DMZ

DMZ (Demilitarized Zone), также известная как демилитаризованная зона. Устанавливается именно буфер между небезопасной системой и безопасной системой для решения проблемы отсутствия доступа к серверу внутренней сети у пользователей с доступом к внешней сети после установки брандмауэра. Хост DMZ – это хост интрасети, где все порты открыты для указанного адреса, за исключением портов, которые заняты и перенаправляются.

Нажмите Network> Firewall> DMZ. Отображается следующая информация:



DMZ Settings		
Позиция	**Описание**	**По умолчанию**
Enable DMZ	Нажмите на кнопку-переключатель, чтобы включить/отключить DMZ. Хост DMZ – это хост во внутренней сети, у которого открыты все порты, кроме тех, которые в противном случае перенаправляются.	OFF
Host IP Address	Ввод IP-адреса хоста DMZ во внутренней сети.	Null
Source IP Address	Установить адрес, совместимый с хостом DMZ. Null означает совместимость с любым адресом.	Null

Нажмите на строку «Состояние», чтобы просмотреть состояние устройства.

Filtering | Port Mapping | Custom Rules | DMZ | Status

Chain Input

Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	DROP	tcp	wlan0	*	0.0.0.0/0	0.0.0.0/0
2	0	DROP	tcp	wlan0	*	0.0.0.0/0	0.0.0.0/0
3	0	DROP	tcp	wlan0	*	0.0.0.0/0	0.0.0.0/0
4	0	REJECT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
5	6	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
6	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
7	5	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
8	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
9	0	ACCEPT	icmp	*	*	0.0.0.0/0	0.0.0.0/0
10	0	DROP	icmp	*	*	0.0.0.0/0	0.0.0.0/0
11	0	DROP	tcp	wlan0	*	::/0	::/0
12	0	DROP	tcp	wlan0	*	::/0	::/0
13	0	DROP	tcp	wlan0	*	::/0	::/0
14	0	REJECT	tcp	*	*	::/0	::/0
15	0	ACCEPT	tcp	*	*	::/0	::/0
16	0	DROP	tcp	*	*	::/0	::/0
17	0	ACCEPT	tcp	*	*	::/0	::/0
18	0	DROP	tcp	*	*	::/0	::/0
19	0	ACCEPT	icmpv6	*	*	::/0	::/0
20	0	DROP	icmpv6	*	*	::/0	::/0

Chain Forward

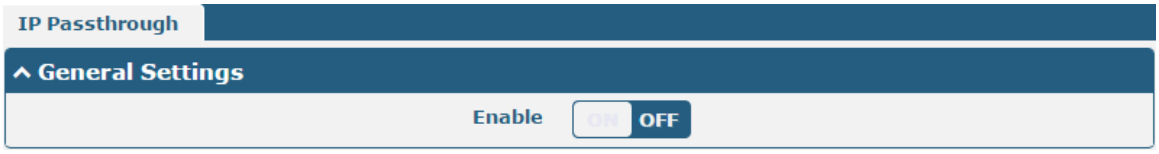
Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	TCPMSS	tcp	*	*	0.0.0.0/0	0.0.0.0/0
2	0	TCPMSS	tcp	*	*	::/0	::/0

Chain Output

Index	Packets	Target	Protocol	In	Out	Source	Destination

3.13 Network > IP Passthrough

Нажмите на **Network > IP Passthrough > IP Passthrough**, чтобы включить или отключить опцию IP Pass-through.



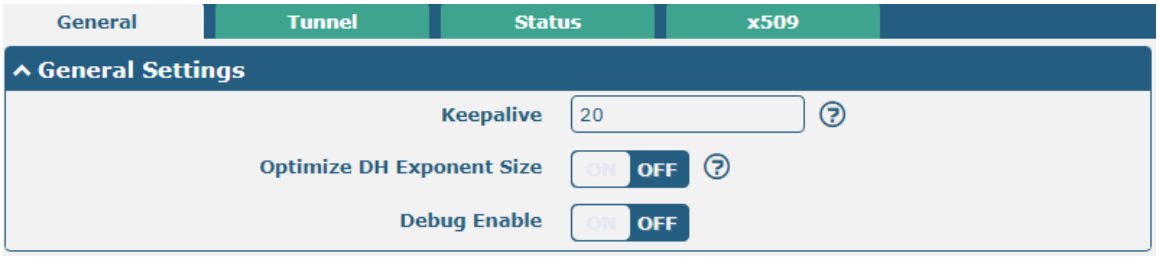
Если маршрутизатор включает сквозной IP-адрес, оконечное устройство (например, ПК) включит режим DHCP-клиента и подключится к порту LAN маршрутизатора; и после успешного подключения маршрутизатора ПК автоматически получит IP-адрес и адрес DNS-сервера, назначенные интернет-провайдером.

3.14 VPN > IPsec

В этом разделе можно установить IPsec и связанные с ним параметры. Безопасность интернет-протокола (IPsec) – комплект протоколов для безопасной передачи данных по интернет-протоколу (IP) ,

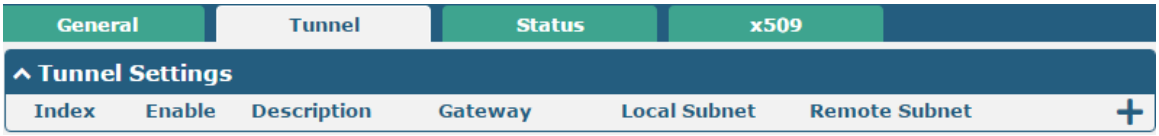
функционирующей путем аутентификации и шифрования каждого IP пакета сеанса передачи данных. Нажмите **на Virtual Private Network> IPsec> General , чтобы установить параметры IPsec.**

Общие сведения

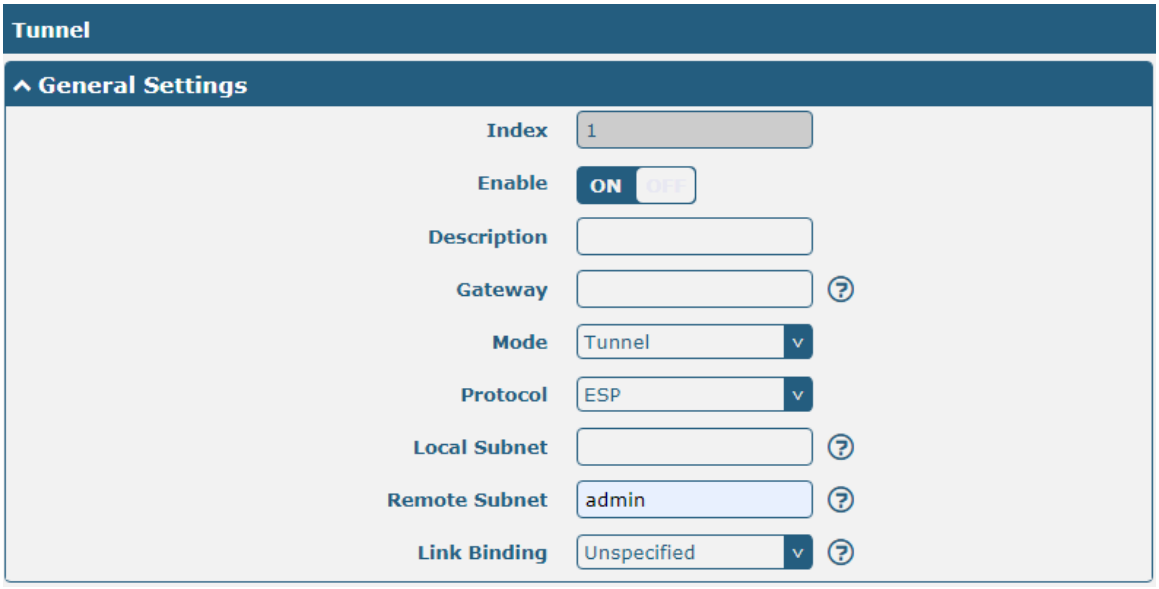


General Settings и General		
Позиция	**Описание**	**По умолчанию**
Enable NAT Traversal	Нажмите на кнопку-переключатель, чтобы включить/отключить опцию NAT Traversal. Эта опция должна быть включена, когда маршрутизатор находится в среде NAT.	ON
Keepalive	Установите время поддержки активности в секундах. Маршрутизатор будет отправлять пакеты на NAT-сервер каждый раз, когда сохраняется активность, чтобы избежать удаления записи из списка NAT.	60
Debug Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Включите вывод информации IPsec VPN на порт отладки.	OFF

Tunnel



Нажмите на +, чтобы добавить настройки туннеля. Максимальное количество равно 3.



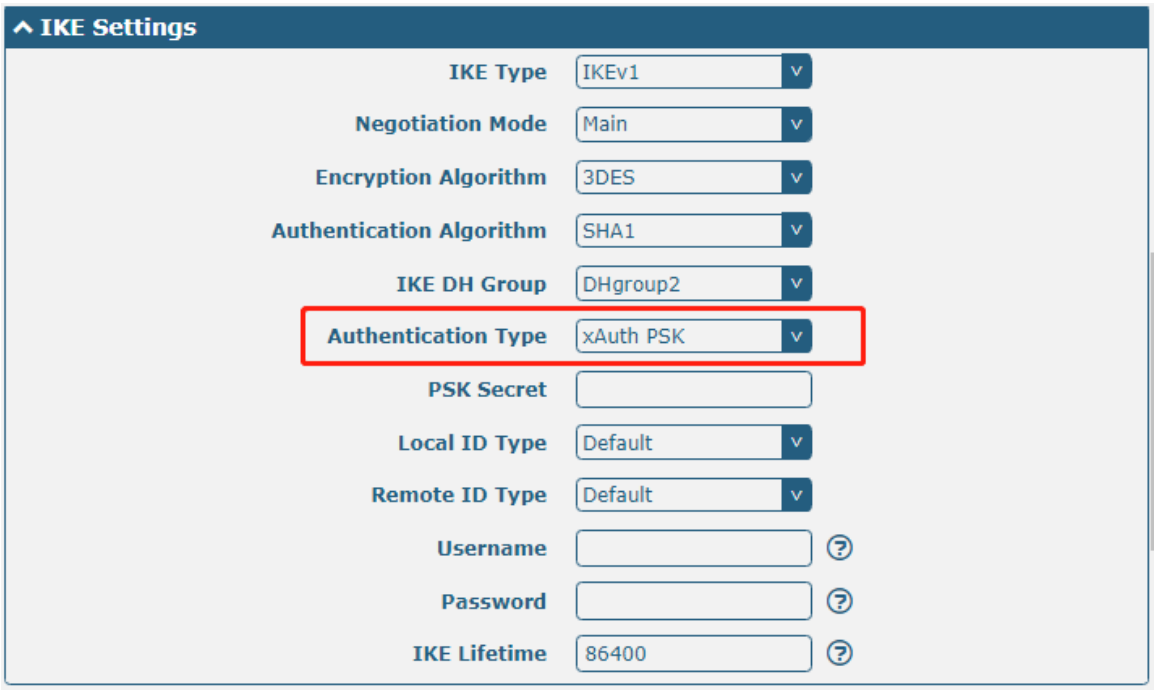
General Settings и Tunnel		
Позиция	**Описание**	**По умолчанию**
Index	Указывает порядковый номер списка.	--
Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить этот туннель IPsec.	ON
Description	Ввод описания для этого туннеля IPsec.	Null
Gateway	Ввод адреса или доменного имени удаленного IPsec VPN-сервера. 1.0.0.0 представляет любой адрес.	Null
Mode	Выберите из «Tunnel» и «Transport». • Tunnel: Обычно используется между шлюзами или на конечной станции к шлюзу, шлюз действует в качестве прокси для хостов, находящихся за ним. • Transport: используется между конечными станциями или между конечной станцией и шлюзом, если шлюз рассматривается в качестве хоста, например, зашифрованный сеанс Telnet от рабочей станции к маршрутизатору, в котором маршрутизатор является фактическим местом назначения.	Tunnel
Protocol	Выбор протокола безопасности из «ESP» и «AH». • ESP: Использование протокола ESP • AH: Использование протокола AH	ESP
Local Subnet	Ввод адреса локальной подсети с маской, защищенной IPsec, например 192.168.1.0/24	Null
Remote Subnet	Ввод адреса удаленной подсети с маской, защищенной IPsec, например 10.8.0.0/24	Null
Link binding	Выберите из «WWAN1», «WWAN2», «WAN» или «WLAN».	Not bound

При выборе «PSK» в качестве типа аутентификации окно отображается в соответствии с рисунком ниже.

При выборе «CA» в качестве типа аутентификации окно отображается в соответствии с рисунком ниже.

При выборе «PKCS#12» в качестве типа аутентификации окно отображается в соответствии с рисунком ниже.

При выборе «xAuth PSK» в качестве типа аутентификации окно отображается в соответствии с рисунком ниже.



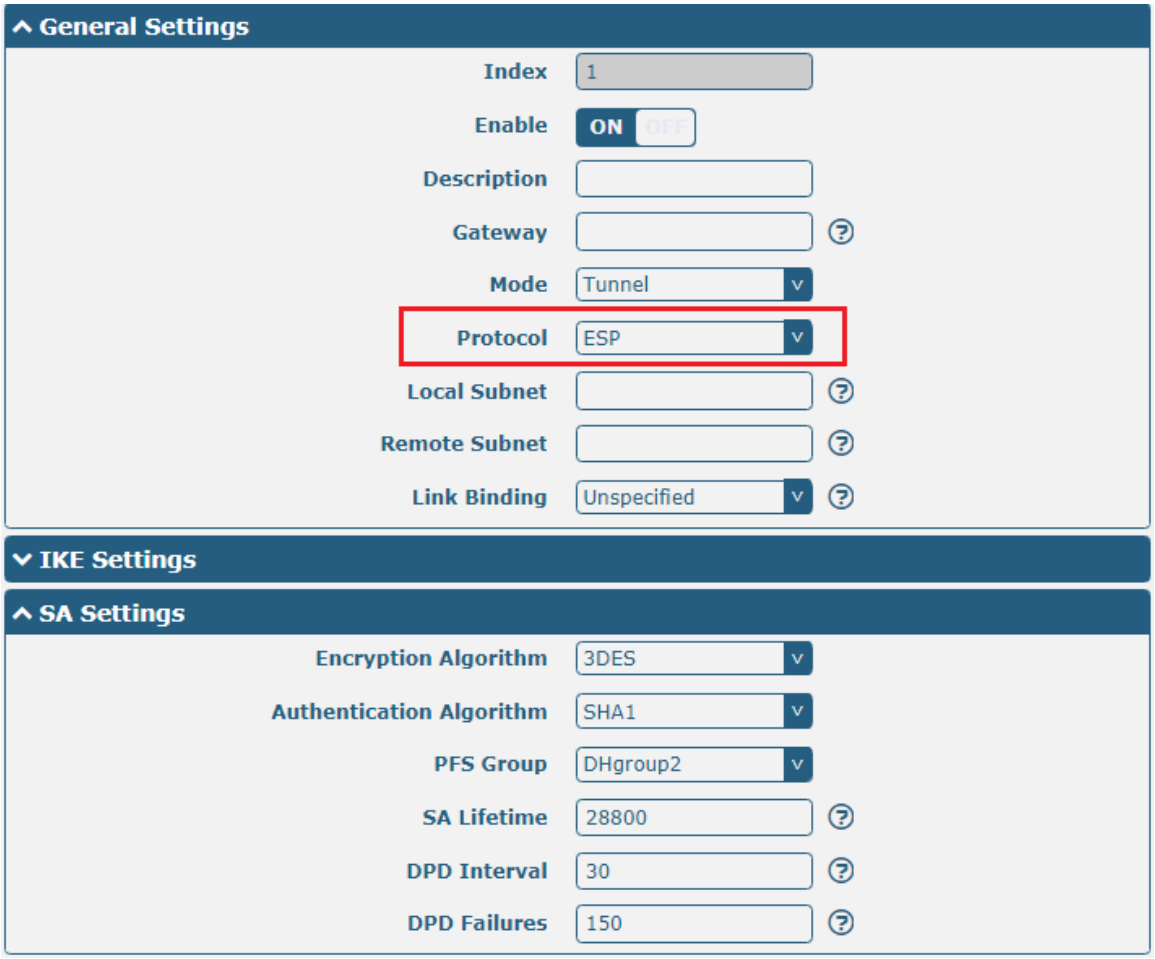
При выборе «xAuth CA» в качестве типа аутентификации окно отображается в соответствии с рисунком ниже.

IKE Settings		
Позиция	**Описание**	**По умолчанию**
IKE Type	Выберите из «IKEv1» and «IKEv2».	IKEv1
Negotiation Mode	Выберите из «Main» или «Aggressive» для режима согласования IKE в фазе 1. Если IP-адрес одного конца туннеля IPsec получается динамически, режим согласования IKE должен быть агрессивным. В этом случае SA могут быть установлены, если имя пользователя и пароль верны.	Main
Authentication	Выберите из «MD5», «SHA1», «SHA2 256» или «SHA2 512» для	SHA1

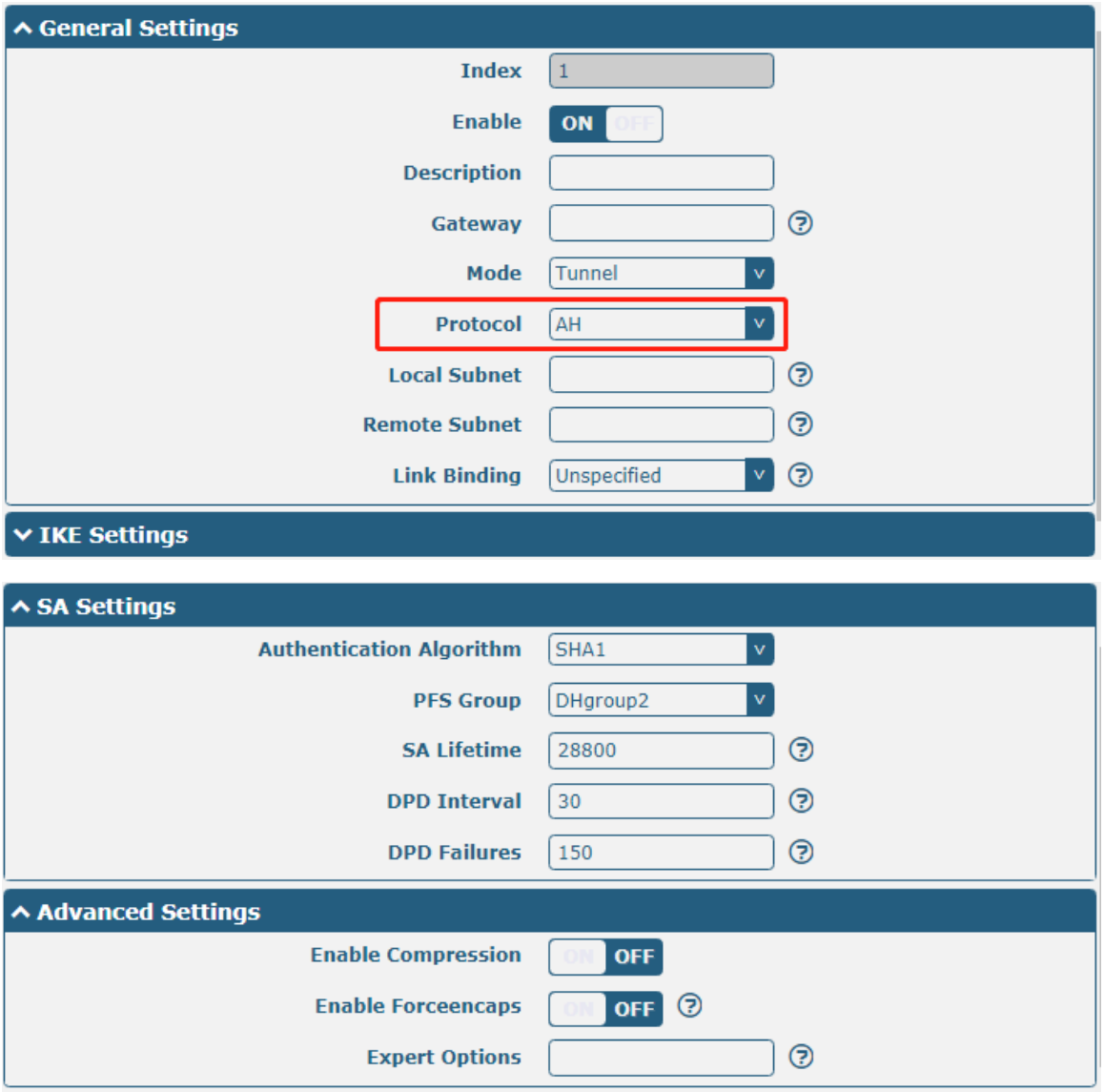
IKE Settings		
Позиция	**Описание**	**По умолчанию**
Algorithm	использования в согласовании IKE.	
Encrypt Algorithm	Выберите из «3DES», «AES128», «AES192» и «AES256» для использования в согласовании IKE. • 3DES: используйте 168-битный алгоритм шифрования 3DES в режиме CBC • AES128: используйте 128-битный алгоритм шифрования AES в режиме CBC • AES256: используйте 256-битный алгоритм шифрования в режиме CBC	3DES
IKE DH Group	Выберите из «DHgroup1», «DHgroup2», «DHgroup5», «DHgroup14», «DHgroup15», «DHgroup16», «DHgroup17» или «DHgroup18» для использования в согласовании ключей на этапе 1.	DHgroup2
Authentication Type	Выберите из «PSK», «CA», «PKCS # 12», «xAuth PSK» и «xAuth CA» для использования в согласовании IKE. • PSK: предварительно определенный ключ • CA: x509 Издатель сертификата • xAuth: расширенная аутентификация на сервере AAA	PSK
PSK Secret	Ввод предварительно определенного ключа.	Null
Local ID Type	Выберите из «Default», «FQDN» или «User FQDN» для согласования IKE. • Default: использует IP-адрес в качестве идентификатора при согласовании IKE • FQDN: использует тип полностью определенного имени домена (FQDN) в качестве идентификатора при согласовании IKE. Если выбрана эта опция, введите имя локального шлюза безопасности без знака «@», например test.robustel.com. • User FQDN: использует тип FQDN пользователя в качестве идентификатора при согласовании IKE. Если выбрана эта опция, введите строку имени для локального шлюза безопасности со знаком «@», например test@robustel.com.	По умолчанию
Remote ID Type	Выберите из «Default», «FQDN» или «User FQDN» для согласования IKE. • Default: использует IP-адрес в качестве идентификатора при согласовании IKE • FQDN: использует тип полностью определенного имени домена (FQDN) в качестве идентификатора при согласовании IKE. Если выбрана эта опция, введите имя локального шлюза безопасности без знака «@», например test.robustel.com. • User FQDN: использует тип FQDN пользователя в качестве идентификатора при согласовании IKE. Если выбрана эта опция, введите строку имени для локального шлюза безопасности со знаком «@», например test@robustel.com.	По умолчанию
IKE Lifetime	Установка срока службы при согласовании IKE. Перед истечением срока	86400

IKE Settings		
Позиция	**Описание**	**По умолчанию**
	действия SA IKE согласовывает новую SA. Как только новая SA настроена, она сразу же вступает в силу, а старая будет автоматически очищена по истечении срока ее службы.	
Private Key Password	Ввод закрытого ключа для типов аутентификации «CA» и «xAuth CA».	Null
Username	Ввод имени пользователя, используемого для типов аутентификации «xAuth PSK» и «xAuth CA».	Null
Password	Ввод пароля, используемого для типов аутентификации «xAuth PSK» и «xAuth CA».	Null

При нажатии на **VPN > IPsec > Tunnel > General Settings** и выборе в качестве протокола **ESP**. Конкретная конфигурация параметров представлена ниже.



Если в качестве протокола выбрать **AH**, отобразится окно настроек SA в соответствии с рисунком ниже..

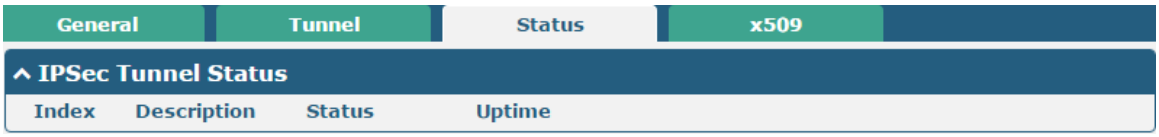


SA Settings		
Позиция	**Описание**	**По умолчанию**
Encrypt Algorithm	Выберите из «3DES», «AES128» или «AES256» при выборе «ESP» в разделе «Protocol». Более высокая безопасность означает более сложную реализацию и более низкую скорость. DES достаточно для удовлетворения общих требований. Используйте 3DES, когда требуется высокая конфиденциальность и безопасность.	3DES
Authentication Algorithm	Выберите из «MD5», «SHA1», «SHA2 256» или «SHA2 512» для использования в согласовании SA.	MD5
PFS Group	Выберите из «DHgroup1», «DHgroup2», «DHgroup5», «DHgroup14», «DHgroup15», «DHgroup16», «DHgroup17» или «DHgroup18» для использования в согласовании SA.	DHgroup2
SA Lifetime	Установка срока службы SA IPsec. При согласовании для установки SA IPsec IKE использует меньшее значение между сроком службы,	28800

SA Settings		
Позиция	**Описание**	**По умолчанию**
	установленным локально, и сроком службы, предложенным одноранговым узлом.	
DPD Interval	Установка интервала, по истечении которого срабатывает DPD, если от одноранговой узла не поступают пакеты, защищенные IPsec. DPD – это обнаружение мертвого одноранговой узла. DPD нерегулярно обнаруживает мертвые одноранговые узлы IKE. Когда локальный конец отправляет пакет IPsec, DPD проверяет время получения последнего пакета IPsec от одноранговой узла. Если время превышает интервал DPD, он отправляет DPD приветствие одноранговуму узлу. Если локальный конец не получает подтверждения DPD в течение интервала повторной передачи пакета DPD, он повторно передает приветствие DPD. Если локальный конец все еще не получает подтверждения DPD после того, как сделал максимальное количество попыток повторной передачи, он считает, что одноранговый узел уже мертв, и очищает SA IKE и SA IPsec на основе SA IKE.	60
DPD Failures	Установка времени ожидания пакетов обнаружения мертвых одноранговых узлов (DPD).	180
Advanced Settings		
Enable Compression	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Включите сжатие внутренних заголовков IP-пакетов.	OFF
Enable Forced Encapsulation	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. После включения, даже если условие NAT не обнаружено, инкапсуляция пакетов ESP в UDP происходит принудительно. Это может помочь преодолеть ограничительные брандмауэры.	OFF
Expert Options	Добавьте сюда дополнительные параметры конфигурации PPP, формат: config-desc; config-desc, например protostack=netkey; plutodebug=none	Null

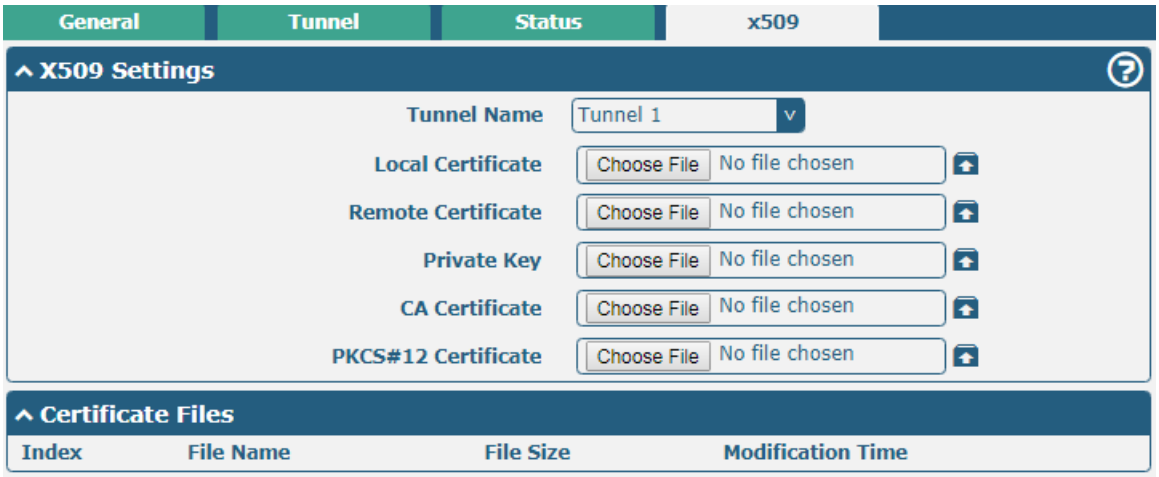
Статус

Этот раздел позволяет просматривать состояние туннеля IPsec.



x509

В этом разделе пользователь может загрузить сертификаты X509 для туннеля IPsec.



x509		
Позиция	**Описание**	**По умолчанию**
X509 Settings		
Tunnel Name	Выбор действующего туннеля.	Tunnel 1
Certificate Files	Нажмите «Choose File», чтобы найти файл сертификата на вашем компьютере, а затем нажмите, чтобы импортировать этот файл в свой маршрутизатор. Правильный формат файла отображается следующим образом: @ca.crt @remote.crt @local.crt @private.key @crl.pem	--
Peer Certificate	Выберите сертификат одноранговой узла для импорта в маршрутизатор.	--
Private Key	Выбор правильного файла закрытого ключа для импорта в маршрутизатор.	--
Root certificate	Выбор файла корневого сертификата для импорта в маршрутизатор.	--
PKCS # 12 certificate	Выбор файла сертификата PKCS # 12 для импорта в маршрутизатор.	--
Certificate Files		
Index	Указывает порядковый номер списка.	--
Filename	Отображает имя импортированного сертификата.	Null
File Size	Отображает размер файла сертификата.	Null
Last Modification	Отображает метку времени последнего изменения файла сертификата.	Null

3.15 VPN > OpenVPN

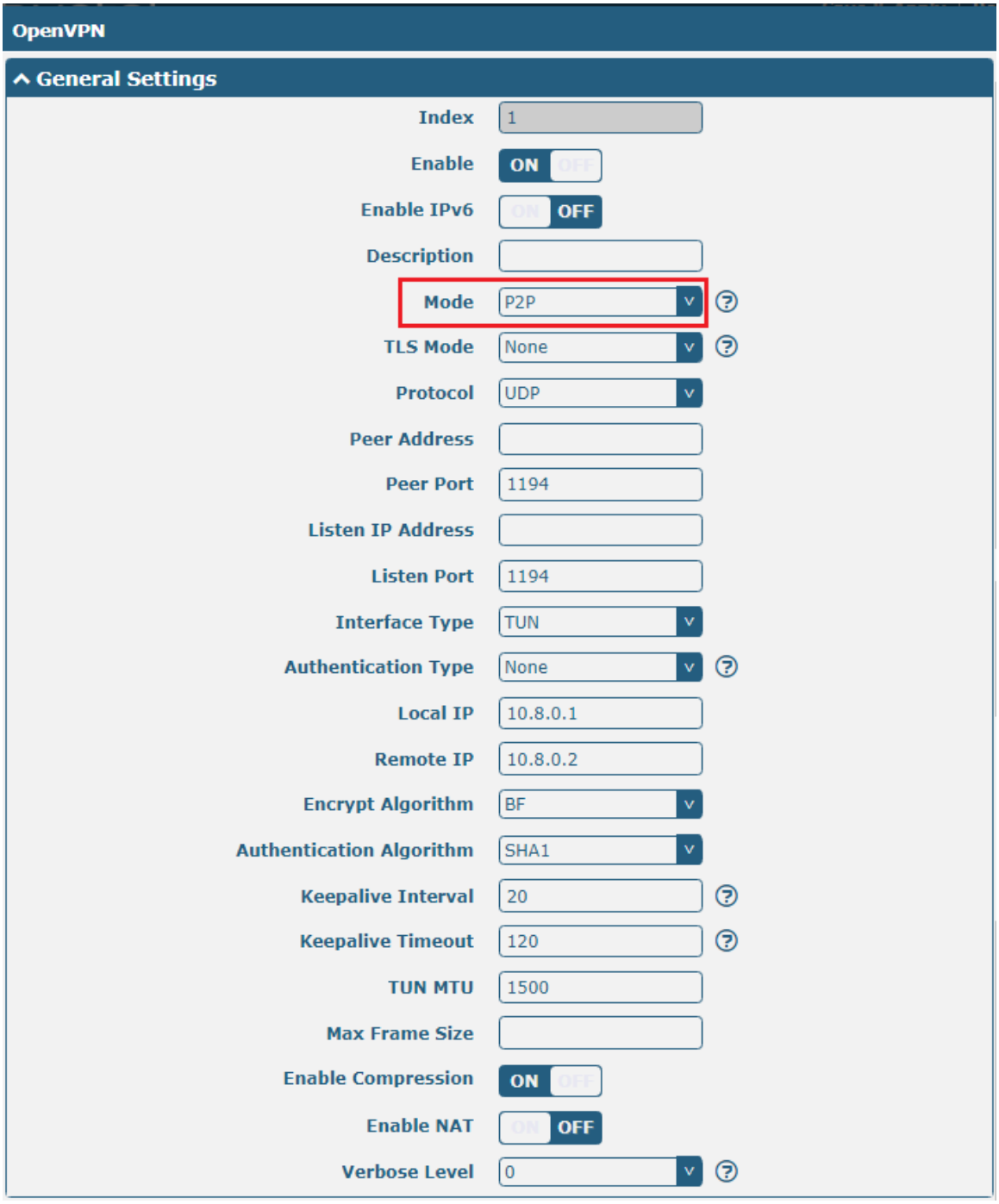
В этом разделе можно установить OpenVPN и связанные с ним параметры. OpenVPN – это программное приложение с открытым исходным кодом, которое реализует методы виртуальной частной сети (VPN) для

создания безопасных соединений типа точка-точка или сайт-сеть в маршрутизируемых или мостовых конфигурациях и средствах удаленного доступа. Маршрутизатор поддерживает соединения типа точка-точка и точка-точки.

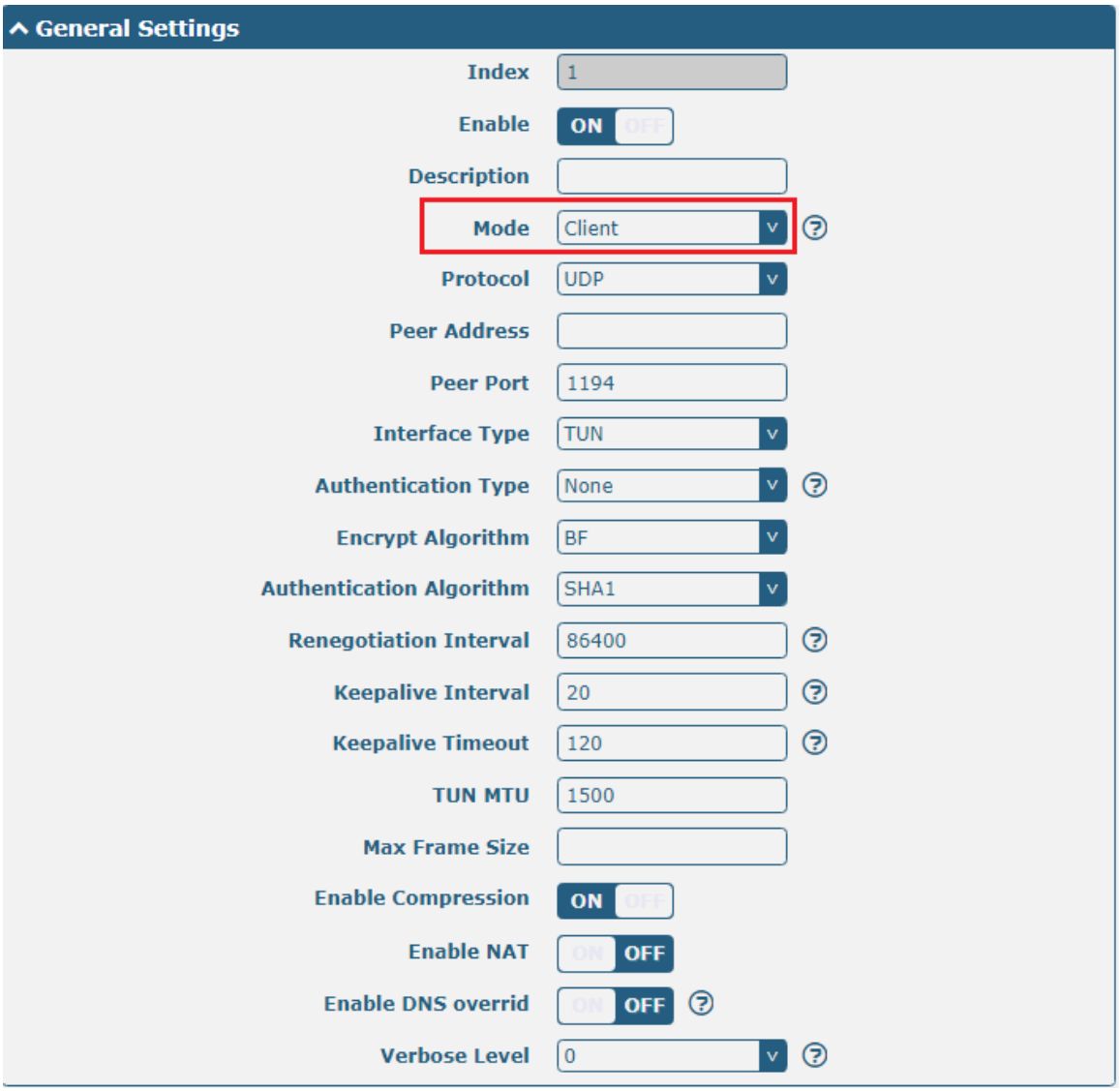
Нажмите **Virtual Private Network> OpenVPN> OpenVPN**. Отображается следующая информация:

OpenVPN

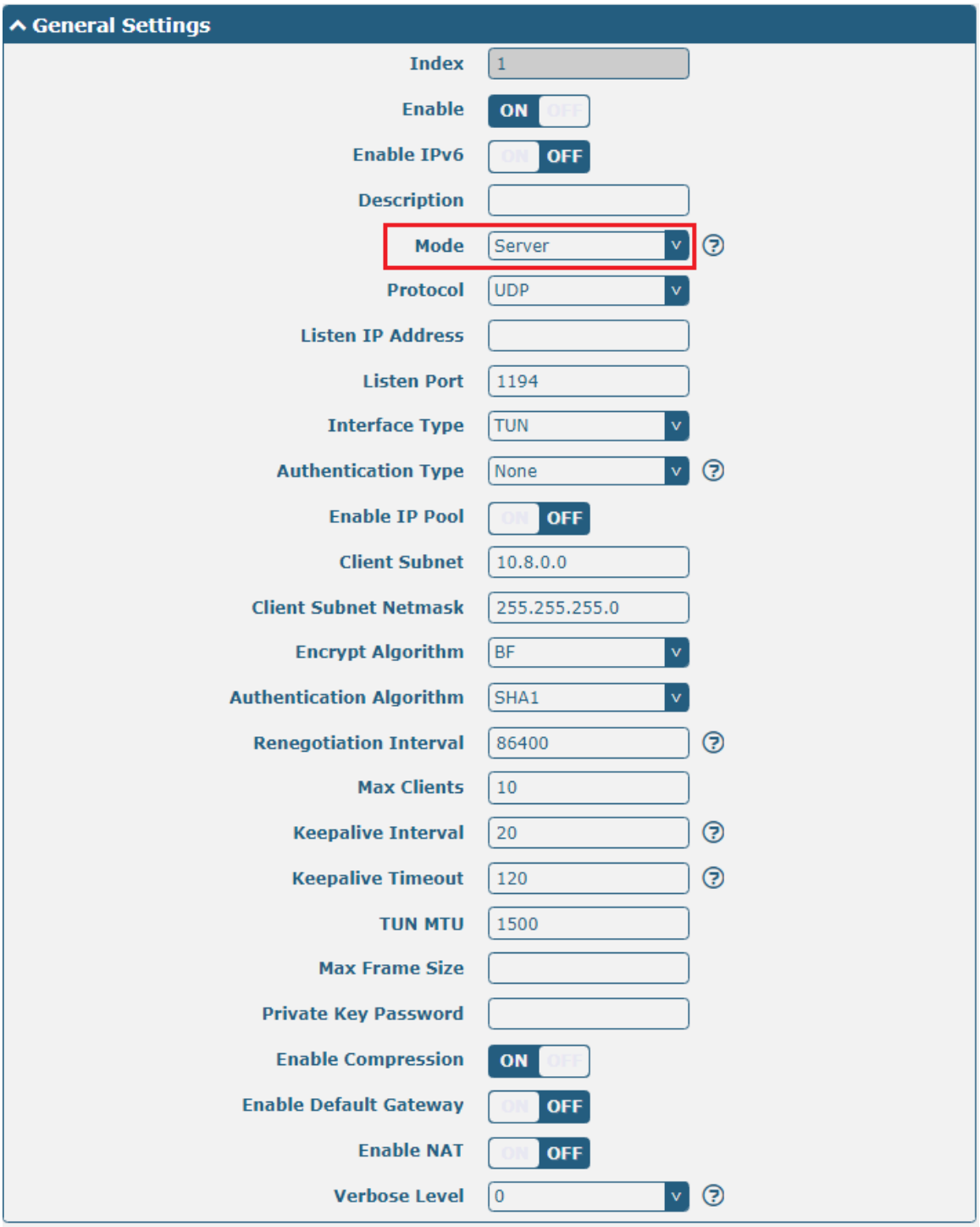
Нажмите на , чтобы добавить настройки туннеля. Максимальное количество равно 3. При выборе «None» в качестве типа аутентификации окно отображается в соответствии с рисунком ниже. По умолчанию режим установлен на «P2P».



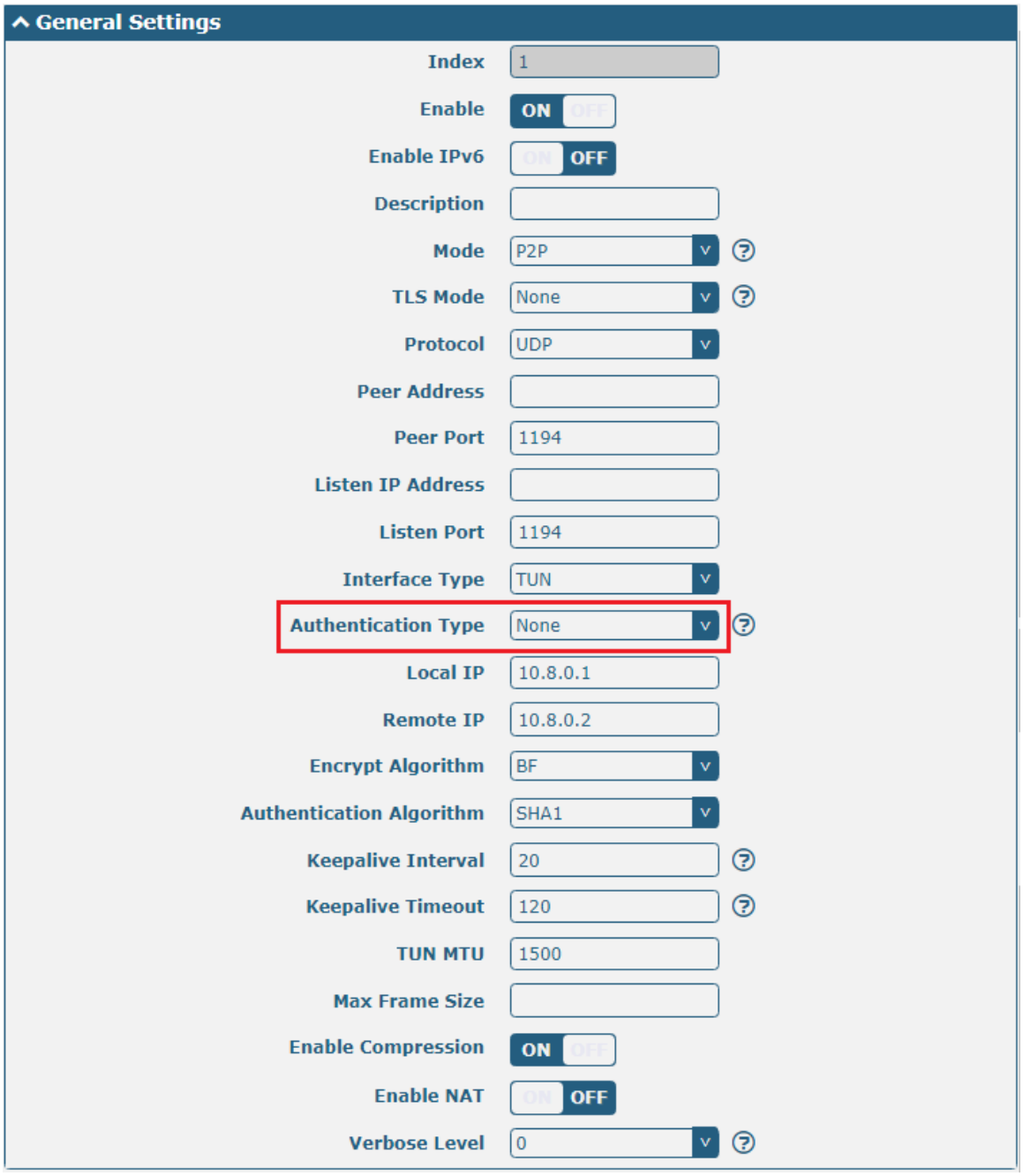
При выборе «Client» в качестве режима окно отображается в соответствии с рисунком ниже.



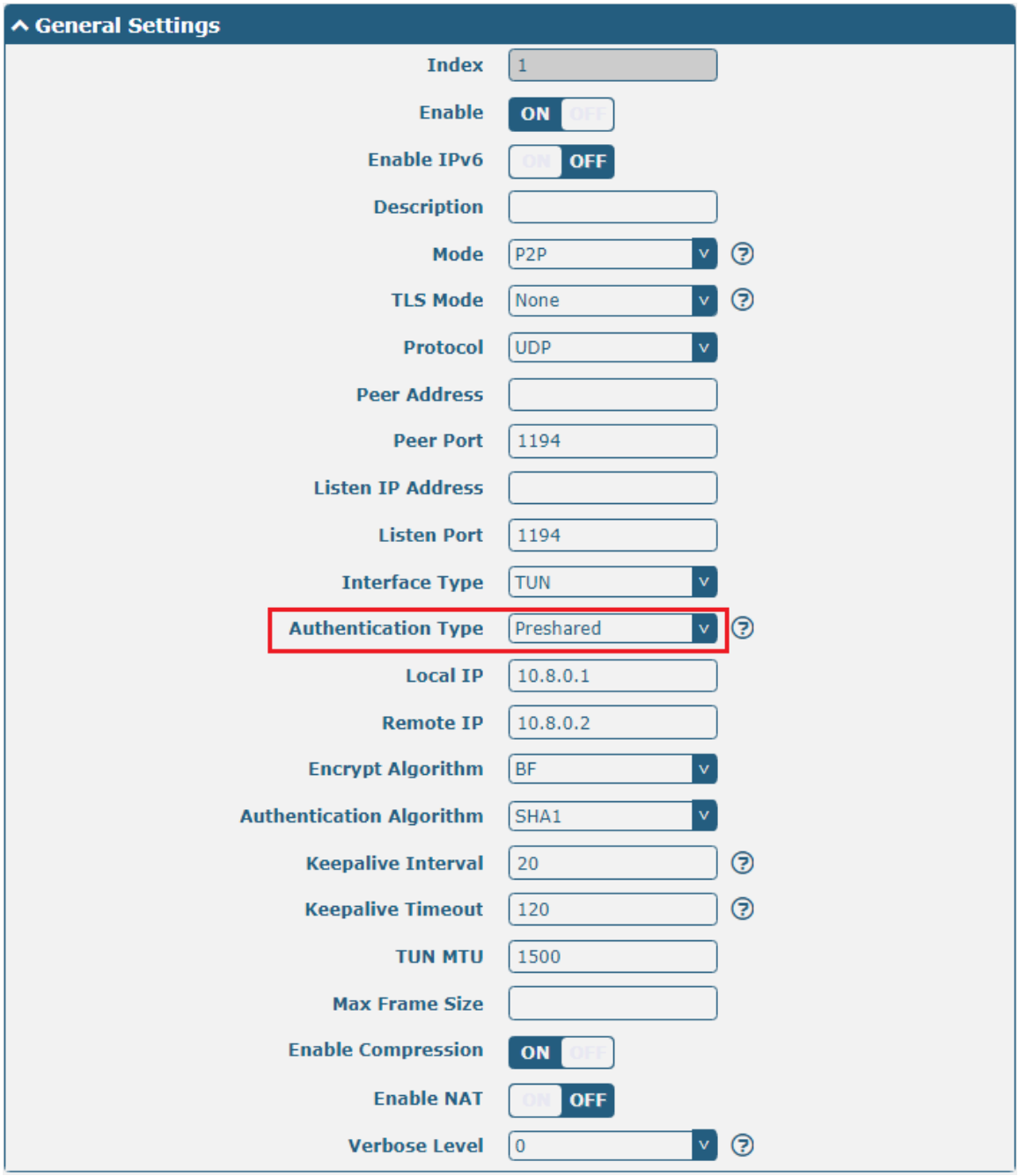
При выборе «Server» в качестве режима, окно отображается в соответствии с рисунком ниже.


General Settings
Index
1
Enable
ON
Enable IPv6
OFF
Description
Mode
Server
Protocol
UDP
Listen IP Address
Listen Port
1194
Interface Type
TUN
Authentication Type
None
Enable IP Pool
OFF
Client Subnet
10.8.0.0
Client Subnet Netmask
255.255.255.0
Encrypt Algorithm
BF
Authentication Algorithm
SHA1
Renegotiation Interval
86400
Max Clients
10
Keepalive Interval
20
Keepalive Timeout
120
TUN MTU
1500
Max Frame Size
Private Key Password
Enable Compression
ON
Enable Default Gateway
OFF
Enable NAT
OFF
Verbose Level
0

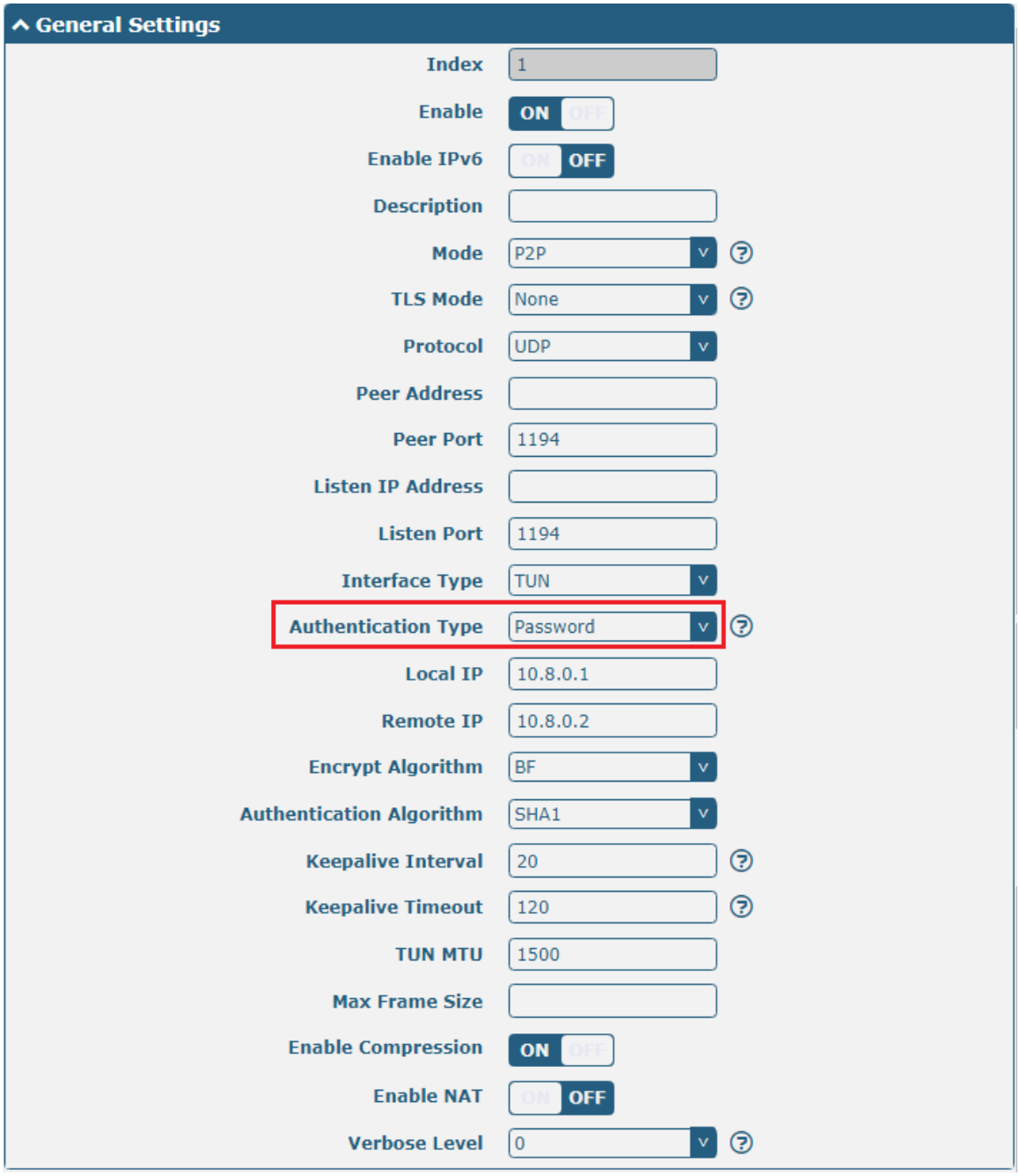
При выборе «None» в качестве типа аутентификации окно отображается в соответствии с рисунком ниже.



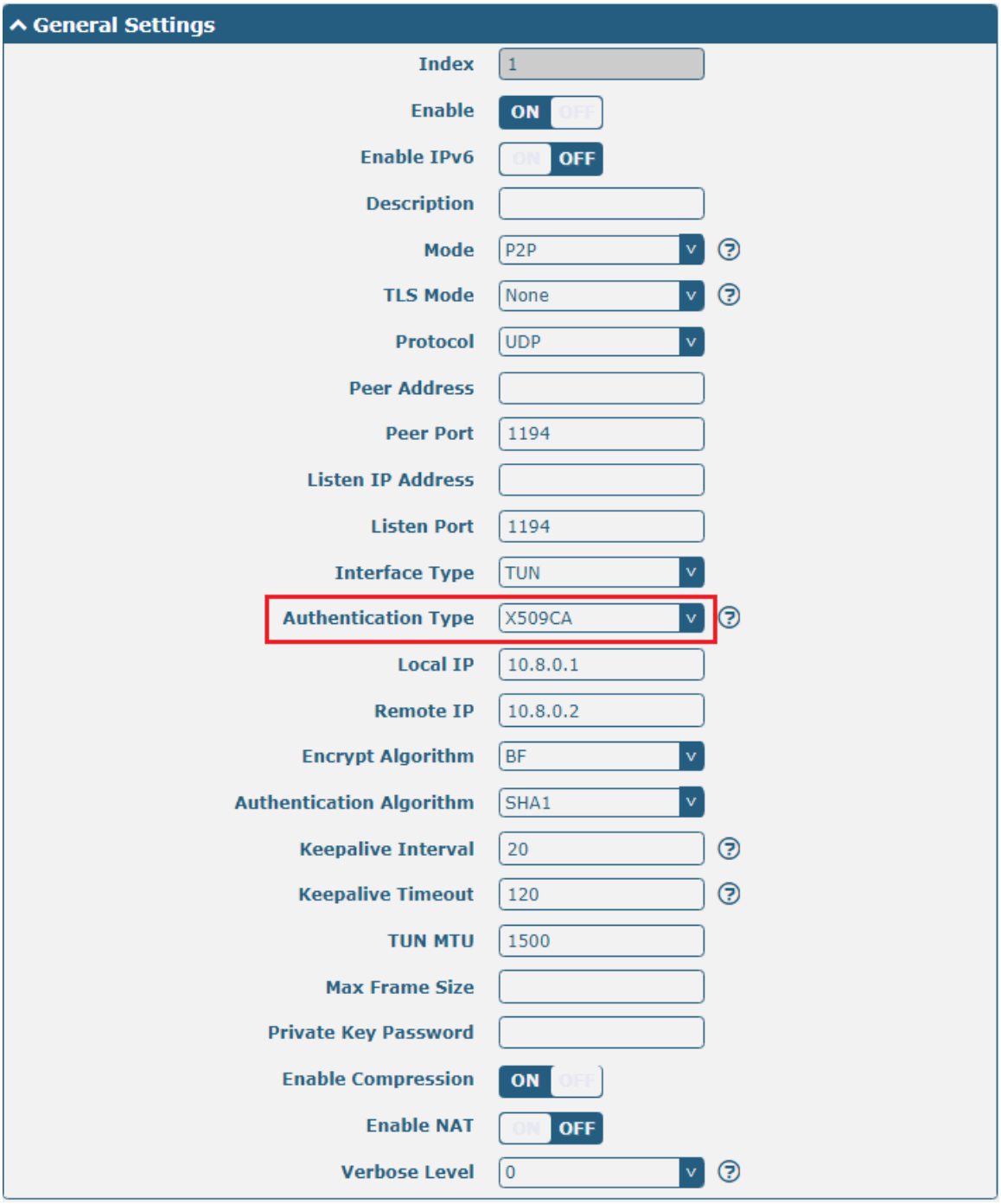
При выборе «Preshared» в качестве типа аутентификации окно отображается в соответствии с рисунком ниже.



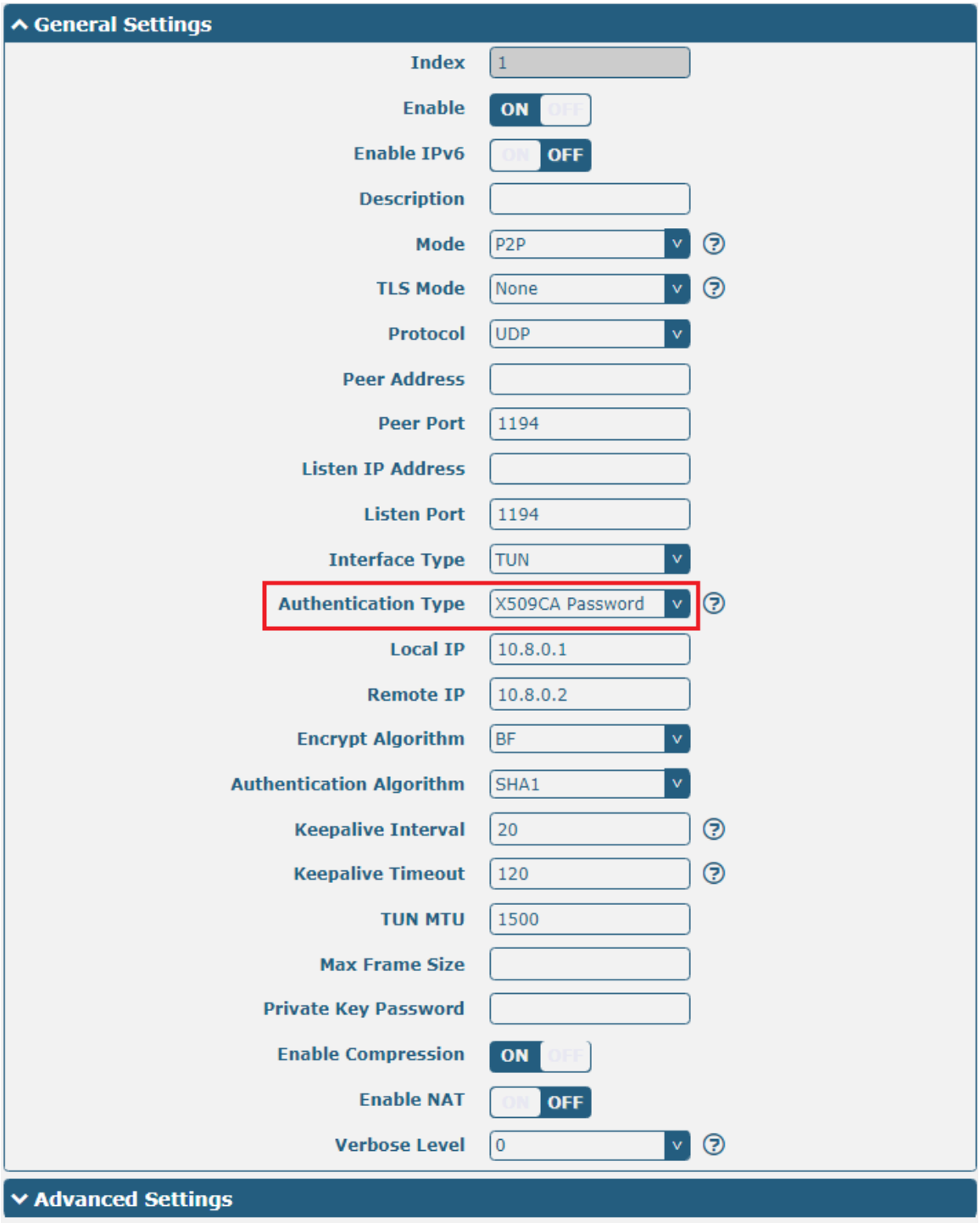
При выборе «Password» в качестве типа аутентификации окно отображается в соответствии с рисунком ниже.



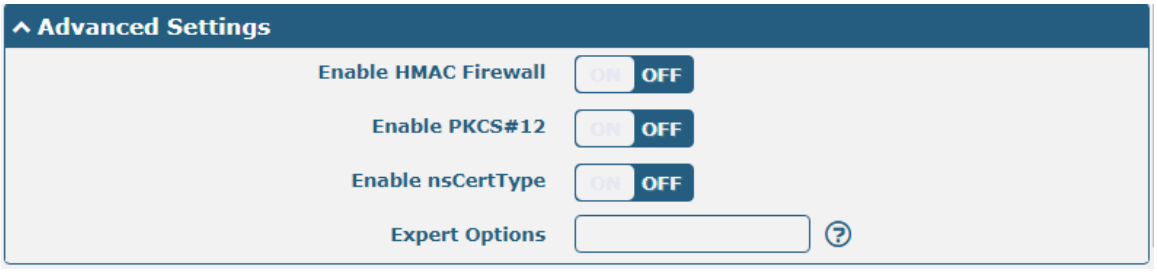
При выборе «X509CA» в качестве типа аутентификации окно отображается в соответствии с рисунком ниже.



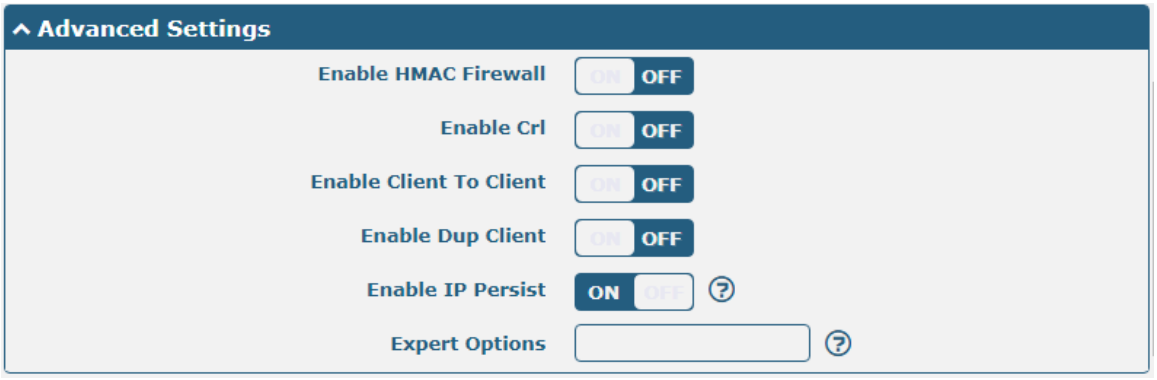
При выборе «X509CA Password» в качестве типа аутентификации окно отображается в соответствии с рисунком ниже.



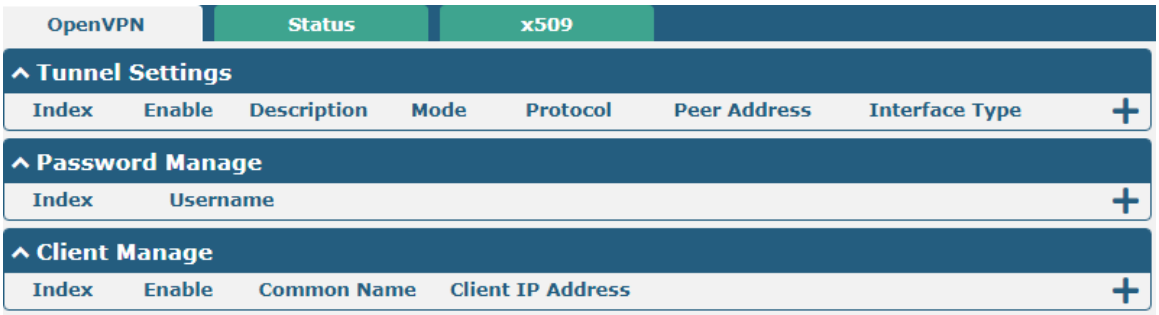
При выборе «Client» в качестве режима окно отображается в соответствии с рисунком ниже.



При выборе «Server» в качестве режима, окно отображается в соответствии с рисунком ниже.



При выборе параметра «Server» в качестве режима и при и выборе «X509CA Password» в качестве типа аутентификации окно «Virtual Private Network> OpenVPN> OpenVPN» отображается в соответствии с рисунком ниже.



Нажмите на User Password Management , чтобы добавить имя пользователя и пароль в соответствии с рисунком ниже:

Нажмите на Client Management чтобы добавить информацию о клиенте в соответствии с рисунком ниже:

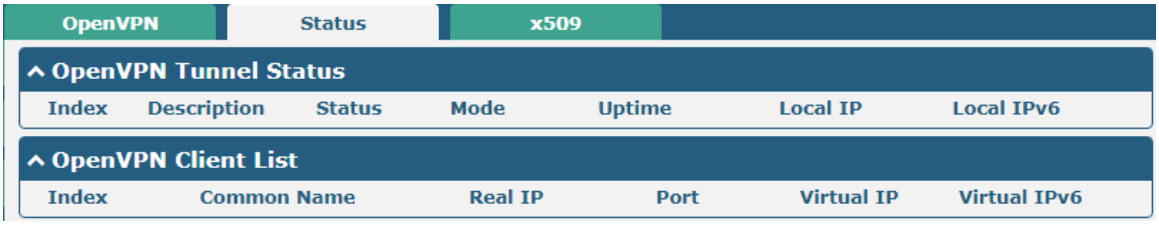
General Settings и OpenVPN		
Позиция	**Описание**	**По умолчанию**
Index	Указывает порядковый номер списка.	--
Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить этот туннель OpenVPN.	ON
Enable IPv6	Нажмите на кнопку-переключатель, чтобы включить/отключить OpenVPN с помощью IPv6.	OFF
Description	Ввод описания для этого туннеля OpenVPN.	Null
Mode	Выберите из «P2P» или «Client».	Client
TLS Mode	Выберите из «None», «Client» или «Server».	None
Protocol	Выберите из «UDP», «TCP-Client» или «TCP-Server».	UDP
Server Address	Ввод сквозного IP-адреса или домена удаленного сервера OpenVPN.	Null
Server port	Ввод порта сквозного прослушивания или порта прослушивания сервера OpenVPN.	1194
Listening address	Адрес локального сервера.	Null
Listening port	Порт локального сервера.	1194
Interface Type	Выберите из «TUN» или «TAP», которые представляют собой два разных типа интерфейса устройства для OpenVPN. Разница между устройством TUN и TAP заключается в том, что устройство TUN представляет собой виртуальное устройство типа точка-точка в сети, а устройство TAP – это виртуальное устройство в сети Ethernet.	TUN
Authentication Type	Выберитеиз «None», «Preshared», «Password», «X509CA» и «X509CA Password». **Примечание**. Типы аутентификации «None» и «Preshared» работают только в режиме P2P.	None
Enable IP Address Pool	Нажмите на кнопку-переключатель, чтобы включить/отключить функцию распределения пула IP-адресов.	OFF
Starting Address	Определяет начало пула IP-адресов, который назначает адреса клиентам OpenVPN.	10.8.0.5
End Address	Определяет конец пула IP-адресов для назначения адресов клиентам OpenVPN.	10.8.0.254
Client Network	Ввод IP-адреса клиентской сети.	10.8.0.0
Client Netmask	Ввод сетевой маски клиента.	255.255.255.0
Username	Ввод имени пользователя, используемого для типа аутентификации «Password» или «X509CA Password».	Null
Password	Ввод пароля, используемого для типа аутентификации «Password» или «X509CA Password».	Null
Local IP	Ввод локального виртуального IP-адреса.	10.8.0.1
Remote IP	Ввод удаленного виртуального IP-адреса.	10.8.0.2

General Settings и OpenVPN		
Позиция	**Описание**	**По умолчанию**
Encrypt Algorithm	Выберите из «BF», «DES», «DES-EDE3», «AES128», «AES192» и «AES256». • BF: используйте 128-битный алгоритм шифрования BF в режиме CBC • DES: используйте 64-битный алгоритм шифрования DES в режиме CBC • DES-EDE3: используйте 192-битный алгоритм шифрования DES-EDE3 в режиме CBC • AES128: используйте 128-битный алгоритм шифрования AES в режиме CBC • AES192: используйте 192-битный алгоритм шифрования в режиме CBC • AES256: используйте 256-битный алгоритм шифрования в режиме CBC	BF
Renegotiation Interval	Установка интервала повторного согласования. Если соединение не удалось, OpenVPN выполнит повторное согласование по достижении интервала повторного согласования.	86400
Maximum Number of Clients	Установка максимального количества клиентов, которым разрешен доступ к серверу OpenVPN.	10
Keepalive Interval	Установите интервал поддержки активности (ping-запрос), чтобы проверить, активен ли туннель.	20
Keepalive Timeout	Установка времени ожидания поддержки активности. Запустить перезапуск OpenVPN по прошествии n секунд без получения ping-запроса или другого пакета от удаленного устройства.	120
MTU	Установка максимальной единицы передачи.	1500
Data Fragmentation	Установка максимальной длины кадра.	Null
Private Key Password	Ввод пароля закрытого ключа под типом аутентификации «X509CA» и «X509CA Password».	Null
Enable Compression	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Включите сжатие потока данных заголовка.	ON
Enable Default Gateway	Автономная кнопка-выключатель для включения/отключения функции шлюза по умолчанию. После включения установите адрес локального туннеля в качестве шлюза по умолчанию для однорангового устройства.	OFF
Receive DNS Push	Автономная кнопка-выключатель для включения/отключения функции приема DNS push. После ее включения, ему разрешено получать информацию DNS, отправленную одноранговым узлом.	OFF
Enable NAT	Нажмите на кнопку-переключатель, чтобы включить/отключить опцию NAT. Если эта опция включена, исходный IP-адрес хоста за маршрутизатором будет замаскирован перед доступом к удаленному клиенту OpenVPN.	OFF

General Settings и OpenVPN		
Позиция	**Описание**	**По умолчанию**
Verbose Level	Выберите уровень выходного журнала и значения от 0 до 11. • 0: нет вывода, кроме фатальных ошибок • 1~4: нормальный диапазон использования • 5: вывод символов R и W на консоль для каждого пакета чтения и записи • 6~11: диапазон информации об отладке	0
Advanced Settings и OpenVPN		
Enable HMAC Firewall	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Добавьте дополнительный уровень аутентификации HMAC поверх канала управления TLS для защиты от DoS-атак.	OFF
Enable PKCS#12	Нажмите на кнопку-переключатель, чтобы включить/отключить сертификат PKCS#12. Это стандарт обмена цифровыми сертификатами, используемый для описания личной информации.	OFF
Enable nsCertType	Нажмите на кнопку-переключатель, чтобы включить/отключить nsCertType. Требуется, чтобы сертификат однорангового узла был подписан с явным обозначением nsCertType «server».	OFF
Enable Crl	Нажмите на кнопку-переключатель, чтобы включить/отключить опцию. Когда опция включена, клиентские сертификаты можно отозвать.	OFF
Enable client to client	Нажмите на кнопку-переключатель, чтобы включить/отключить опцию. Когда опция включена, клиенты могут общаться друг с другом.	OFF
Enable Dup Client	Нажмите на кнопку-переключатель, чтобы включить/отключить опцию. После включения туннельные IP-адреса, полученные несколькими клиентами, различны, а туннельный IP-адрес клиента и туннельный IP-адрес сервера являются совместимыми.	OFF
Enable IP Address Hold	Нажмите на кнопку-переключатель, чтобы включить/отключить опцию. При включении IP-адрес в пуле адресов получается автоматически.	ON
Expert Options	Введите в это поле некоторые другие опции OpenVPN. Каждое выражение может быть разделено точкой с запятой.	Null
Advanced Settings и User Password Management		
Username	Настраиваемое имя пользователя для туннельного подключения.	Null
Password	Настраиваемый пароль для туннельного подключения.	Null
Управление клиентом		
Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Если эта опция включена, можно управлять IP-адресом клиента.	OFF
Common Name	Установка названия сертификата.	Null
Client IP Address	Установка фиксированного виртуального IP-адреса клиента.	Null

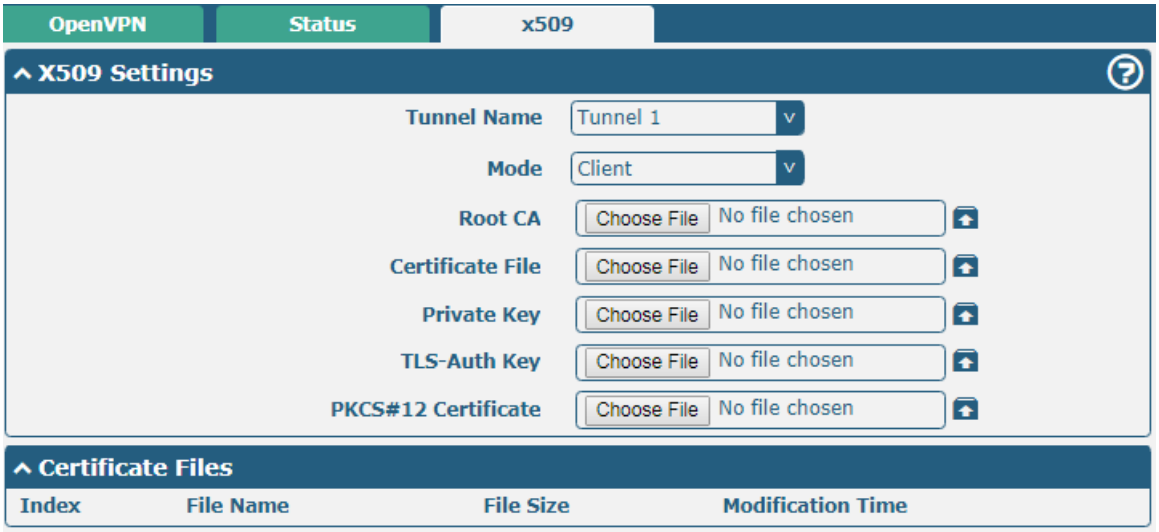
Статус

Этот раздел позволяет просматривать состояние туннеля OpenVPN.



x509

В этом разделе пользователь может загрузить сертификаты X509 для OpenVPN.



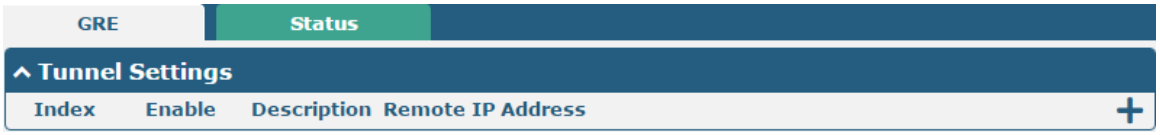
x509		
Позиция	**Описание**	**По умолчанию**
X509 Settings		
Tunnel Name	Выбор действующего туннеля. Выберите из «Tunnel 1», «Tunnel 2», «Tunnel 3», «Tunnel 4», «Tunnel 5» или «Tunnel 6».	Tunnel 1
Tunnel Mode	Выберите из «P2P Mode», «Client Mode» или «Server Mode».	Client mode
Root certificate	Выбор файла корневого сертификата для импорта в маршрутизатор.	--
Certificate Files	Нажмите «Choose File», чтобы найти файл сертификата на вашем компьютере, а затем нажмите, чтобы импортировать этот файл в свой маршрутизатор.	--
Private Key	Выбор файла закрытого ключа для импорта в маршрутизатор.	--
TLS-Auth Key	Выбор файла ключа TLS-Auth для импорта в маршрутизатор.	--

PKCS # 12 certificate	Выбор файла сертификата PKCS # 12 для импорта в маршрутизатор.	--
Certificate Files		
Index	Указывает порядковый номер списка.	--
Filename	Отображает имя импортированного сертификата.	Null
File Size	Отображает размер файла сертификата.	Null
Last Modification	Отображает метку времени последнего изменения файла сертификата.	Null

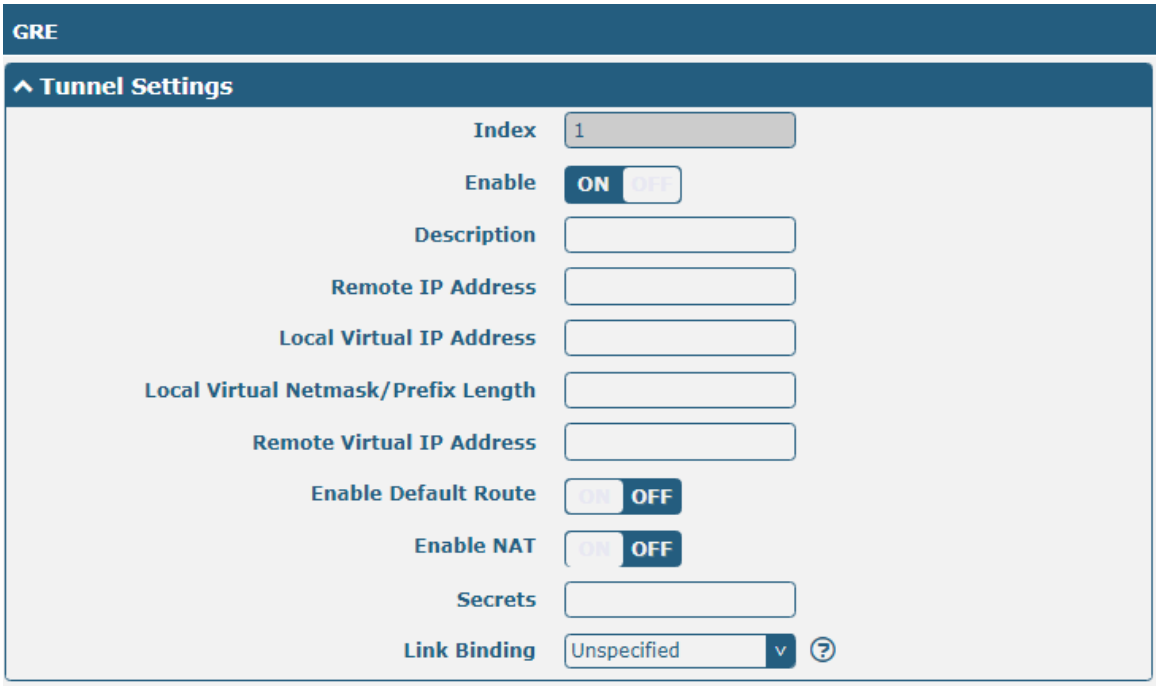
3.16 VPN > GRE

В этом разделе вы можете установить GRE и связанные с ним параметры. Общая инкапсуляция маршрутов (GRE) .– это протокол туннелирования, который может инкапсулировать широкий спектр протоколов сетевого уровня внутри виртуальных соединений типа точка-точка по сети Интернет-протокола. Предусмотрено два целевых назначения протокола GRE: инкапсуляция корпоративного внутреннего протокола и инкапсуляция частных адресов.

GRE



Нажмите на +, чтобы добавить настройки туннеля. Максимальное количество равно 3.

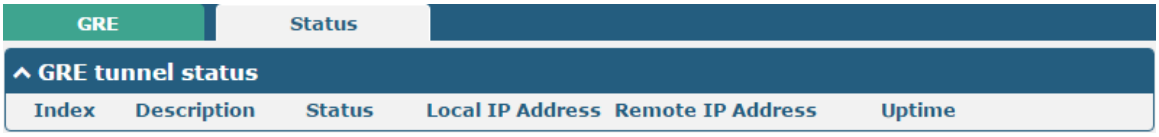


Tunnel Settings и GRE		
Позиция	**Описание**	**По умолчан**

		ию
Index	Указывает порядковый номер списка.	--
Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить этот туннель GRE.	ON
Описание	Ввод описания для этого туннеля GRE.	Null
Remote IP Address	Установка удаленного реального IP-адреса туннеля GRE.	Null
Local Virtual IP Address	Установка локального виртуального IP-адреса туннеля GRE.	Null
Local Virtual Netmask/ IPv6 prefix length	Установка локальной виртуальной маски сети туннеля GRE.	Null
Local Virtual IP Address	Установка удаленного виртуального IP-адреса туннеля GRE.	Null
Enable Default Route	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Если эта опция включена, весь трафик маршрутизатора будет проходить через VPN GRE.	OFF
Enable NAT	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Эта опция должна быть включена, когда маршрутизатор находится в среде NAT.	OFF
Secrets	Установка ключа туннеля GRE.	Null
Link binding	Выберите из «WWAN1», «WWAN2», «WAN» или «WLAN».	Not bound

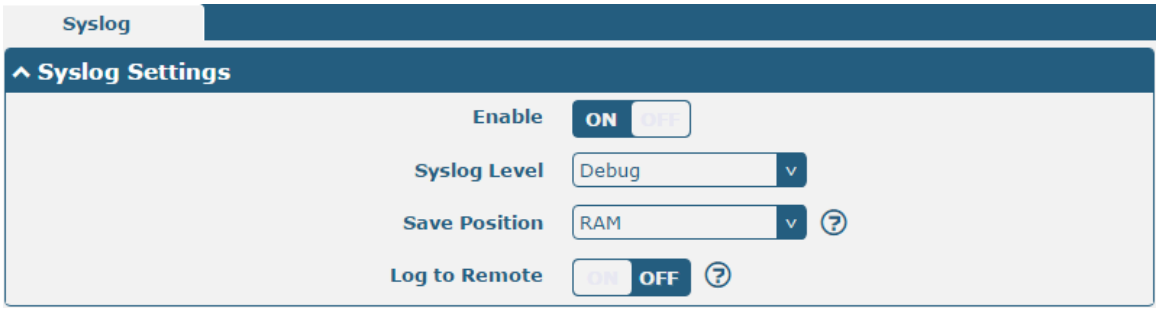
Статус

Этот раздел позволяет просматривать состояние туннеля GRE.

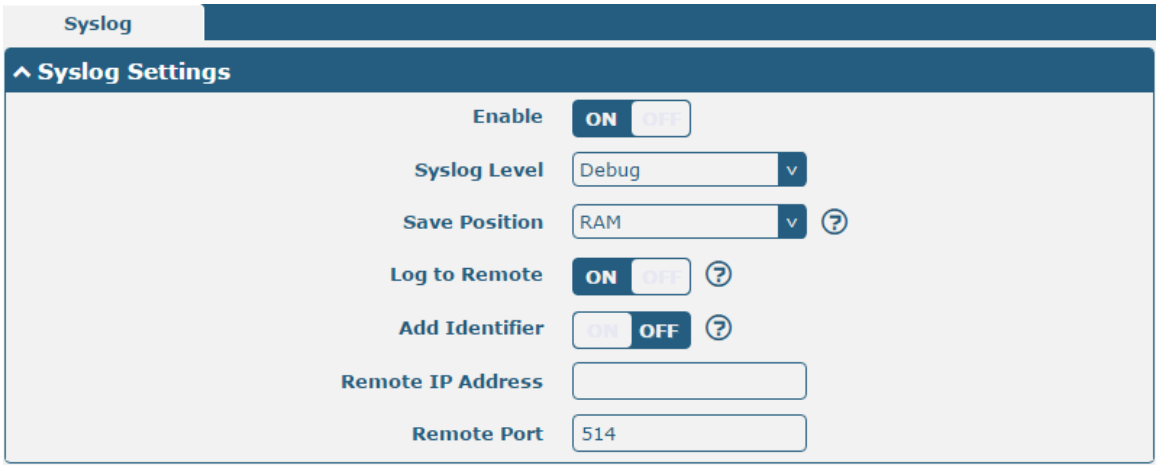


3.17 Services > Syslog

Данный раздел позволяет установить параметры системного журнала. Системный журнал маршрутизатора может быть сохранен на локальном компьютере, а также поддерживает отправку на удаленный сервер журнала и отладку указанного приложения. По умолчанию опция «Log to Remote» отключена.



При включении опции «Log to Remote» окно отображается в соответствии с рисунком ниже.

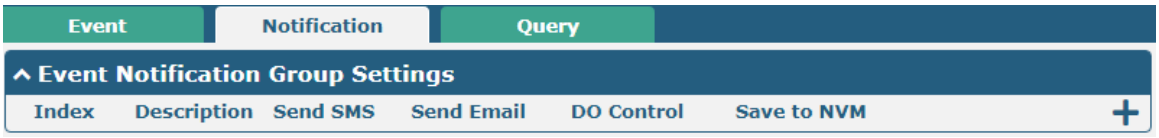


Настройки системного журнала		
Позиция	**Описание**	**По умолчанию**
Enable	Нажмите кнопку-переключатель, чтобы включить/отключить параметр настроек системного журнала.	OFF
Syslog Level	Выберите «Debug», «Info», «Notice», «Warning» или «Error», снизу вверх. На нижнем уровне выводится более подробная информация о системном журнале.	Отладка
Save Position	Выберите позицию сохранения из «RAM», «NVM» или «Console». Очистка данных будет произведена после перезагрузки при выборе фукнции «RAM». **Примечание**: не рекомендуется сохранять системный журнал в энергонезависимую память на длительное время.	RAM
Log to Remote	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Включите, чтобы разрешить маршрутизатору отправлять системный журнал на удаленный сервер системного журнала. Вам необходимо ввести IP-адрес и порт сервера системного журнала.	OFF
Add Identifier	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Если этот параметр включен, можно добавить серийный номер в сообщение системного журнала, которое используется для загрузки системного журнала в RobustLink.	OFF
Remote IP Address	Введите порт сервера системного журнала при включении опции «Log to Remote».	Null
Remote Port	Введите порт сервера системного журнала при включении опции «Log to Remote».	514

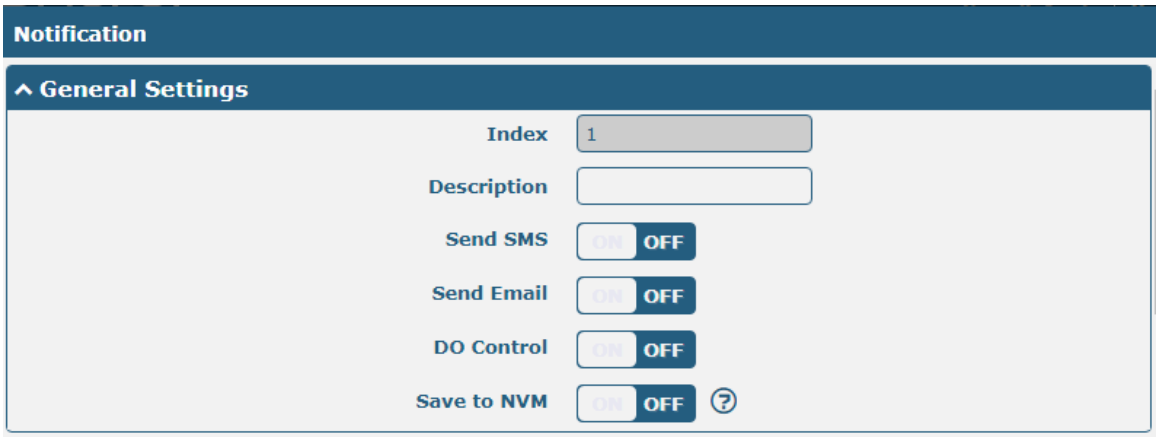
3.18 Services > Event

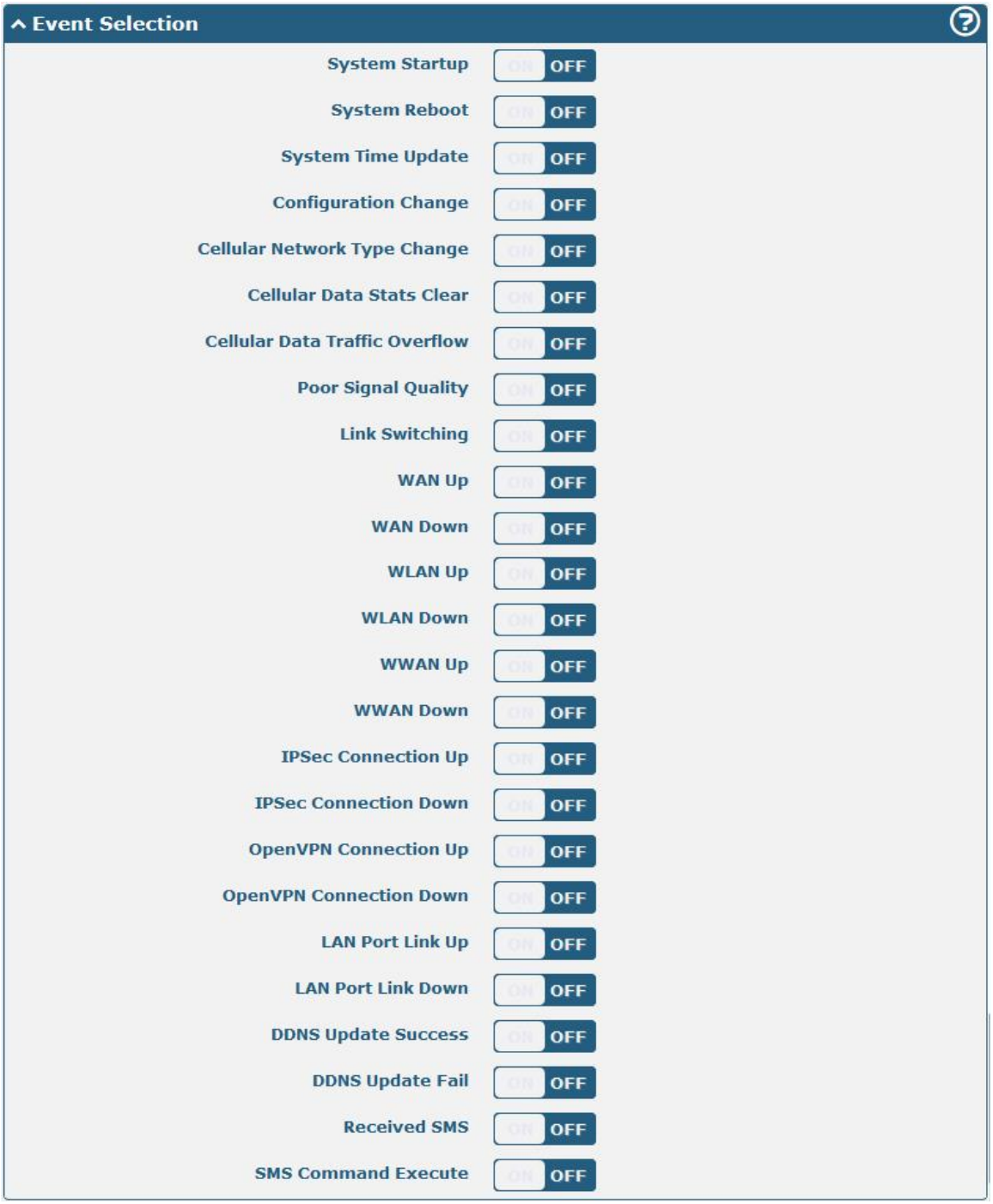
Данный раздел позволяет установить параметры события. Функция событий представляет возможность отправлять оповещения по SMS или электронной почте при возникновении определенных системных событий.

General Settings @ Event		
Позиция	**Описание**	**По умолчанию**
Порог качества сигнала	Установите порог качества сигнала. Маршрутизатор будет генерировать событие журнала, когда фактическое пороговое значение меньше указанного порога. 0 означает отключение этой опции.	0



Нажмите кнопку +, чтобы добавить параметры события.

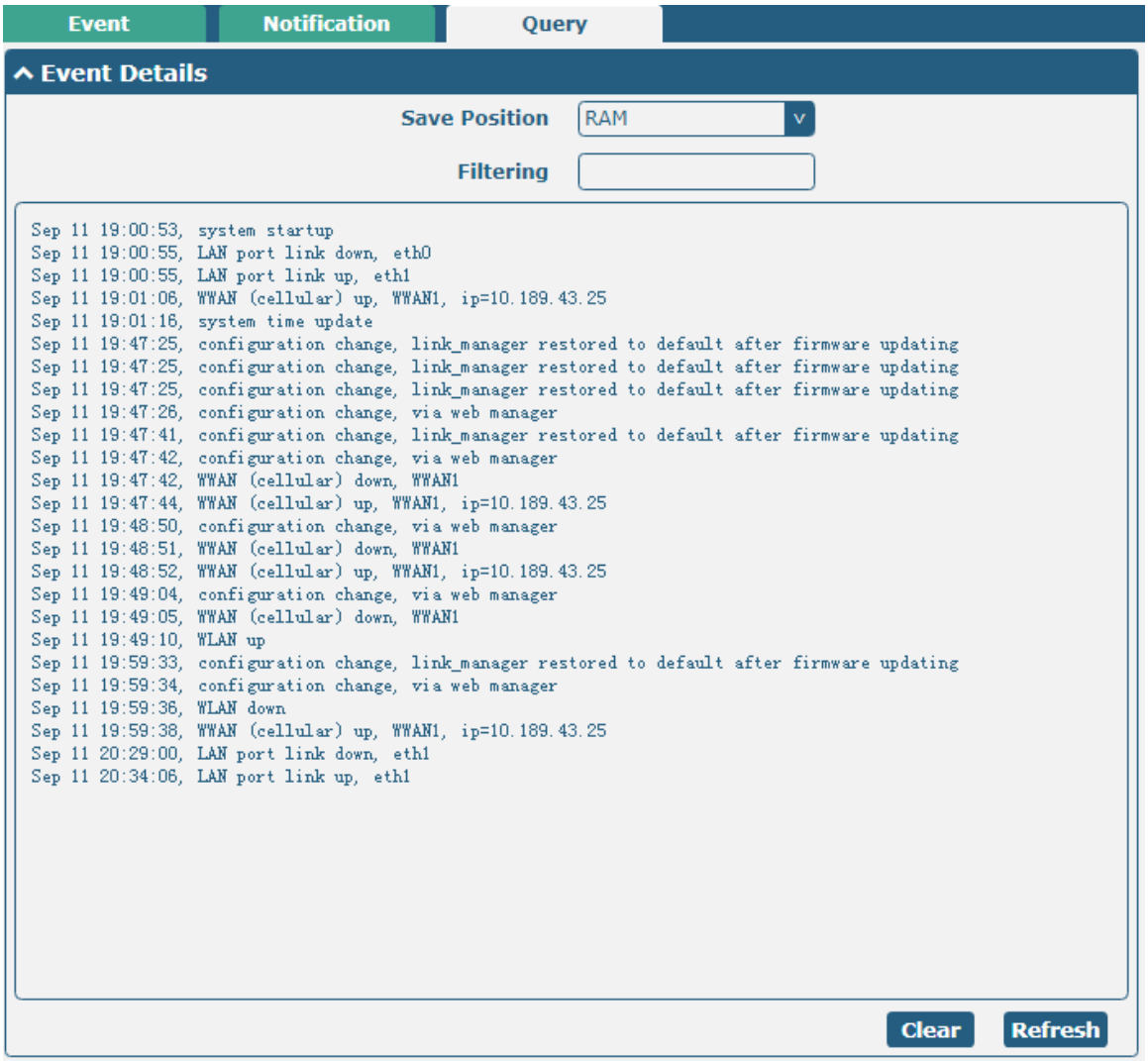




General Settings @ Notification		
Позиция	**Описание**	**По умолчанию**
Index	Указывает порядковый номер списка.	--
Описание	Вводит описание для этой группы.	Null
Отправка SMS	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Если эта функция включена, маршрутизатор отправит уведомление на указанные номера телефонов с помощью SMS в случае возникновения события. Установите соответствующий номер телефона в «3.24 Services > Email» и используйте «;» для разделения каждого номера.	OFF

Отправка эл. почты	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Если этот параметр включен, маршрутизатор будет отправлять уведомление на указанный адрес электронной почты по электронной почте при наступлении события. Установите соответствующий адрес электронной почты в «3.21 Services > Email».	OFF
Контроль цифрового выхода (DO)	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. После включения маршрутизатор событий отправит его соответствующему DO в виде низкого/высокого уровня.	OFF
Сохранить в NVM	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Включите, чтобы сохранить событие в энергонезависимой памяти.	OFF

В следующем окне можно запросить различные типы записей событий. Нажмите на Refresh для запроса отфильтрованных событий, нажмите на Clear, чтобы очистить записи событий в окне.

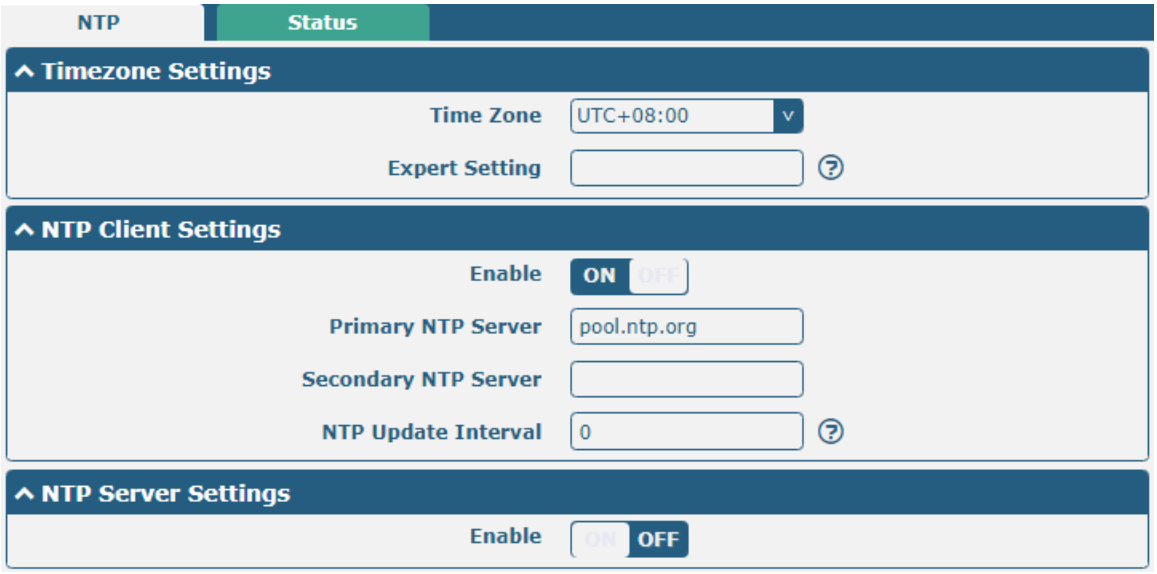


Детали события		
Позиция	**Описание**	**По умолчанию**
Сохраните	Выберите позицию сохранения событий из «RAM» или «NVM».	RAM

позицию	• RAM: оперативная память • NVM: энергонезависимая память	
Фильтр сообщения	Введите сообщение для фильтрации на основе ключевых слов, установленных пользователями. Нажмите на кнопку «Refresh», отфильтрованное событие отобразится в следующем поле. Используйте «&», чтобы разделить более одного сообщения фильтра, например message1 и message2.	Null

3.19 Services > NTP

В этом разделе можно установить соответствующие параметры NTP (Network Time Protocol), включая часовой пояс, NTP-клиент и NTP-сервер.



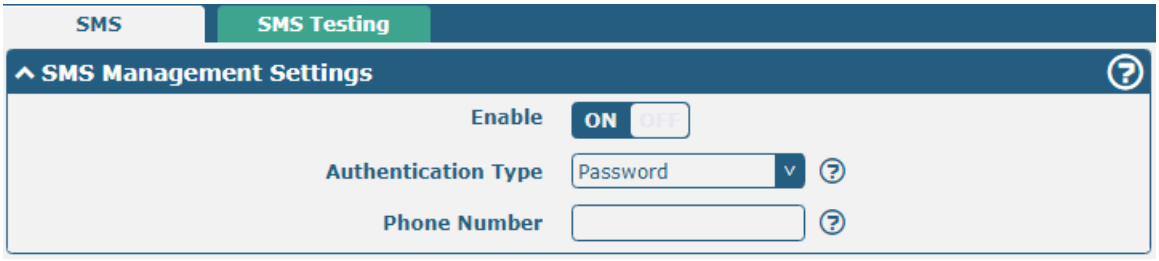
NTP		
Позиция	**Описание**	**По умолчанию**
Настройка Time zone		
Time Zone	Нажмите на раскрывающийся список, чтобы выбрать часовой пояс, в котором находитесь.	Универсальное координированное время (UTC) +08:00
Экспертные настройки	Укажите часовой пояс с переходом на летнее время в формате переменной среды TZ. В этом случае параметр «Time Zone» будет проигнорирован.	Null
NTP Client Settings		
Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Включите для синхронизации времени с сервером NTP.	ON
Первичный сервер	Enter primary NTP Server's IP address or domain name.	pool.ntp.org

NTP		
Вторичный сервер NTP	Введите IP-адрес или доменное имя вторичного NTP-сервера.	Null
Интервал обновления NTP	Введите интервал (в минутах) для синхронизации времени NTP клиента с сервером NTP. Минуты ожидания следующего обновления, а 0 означает лишь одноразовое обновление.	0
Настройки сервера NTP		
Enable	Нажмите кнопку-переключатель, чтобы включить параметр NTP-сервера.	OFF

Это окно позволяет просматривать текущее время маршрутизатора, а также синхронизировать время маршрутизатора. Нажмите кнопку **Sync**, чтобы синхронизировать время маршрутизатора с компьютером.

3.20 Services > SMS

Данный раздел позволяет установить параметры SMS. Маршрутизатор поддерживает управление с помощью SMS, и пользователь может контролировать и настраивать свои маршрутизаторы, отправляя SMS. Дополнительную информацию об управлении с помощью SMS см. в разделе **4.1.2 Удаленное управление с помощью SMS**.



Настройки управления SMS		
Позиция	**Описание**	**По умолчанию**
Enable	Нажмите кнопку-переключатель, чтобы включить/отключить параметр управления SMS. **Примечание**. Если эта опция отключена, конфигурация SMS недействительна.	ON

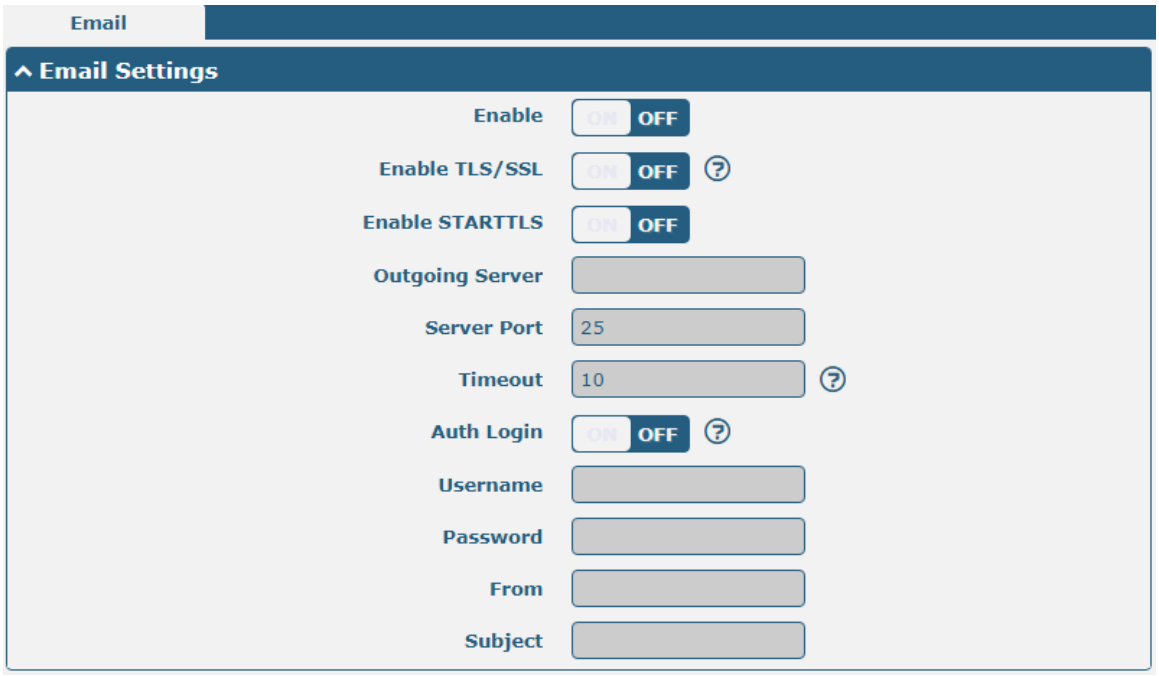
Authentication Type	Выберите тип аутентификации из «Пароль», «Phonenum» или «Оба». • Пароль: используйте то же имя пользователя и пароль, что и WEB-менеджер для аутентификации. Например, формат SMS должен быть «имя пользователя: пароль; cmd1; cmd2; … » **Примечание**. Установите пароль WEB-менеджера в разделе **System > User Management.** • Phonenum: используйте номер телефона для аутентификации, и пользователь должен установить номер телефона, который разрешен для управления SMS. Формат SMS должен быть «cmd1; cmd2; … » • Оба: используйте для аутентификации и «Пароль», и «Phonenum». Пользователь должен установить номер телефона, который разрешен для управления SMS. Формат SMS должен быть «имя пользователя: пароль; cmd1; cmd2; … »	Password
Phone Number	Установите номер телефона, используемый для управления SMS, и используйте ‘; «Отделить каждое число. **Примечание**. Он может быть пустым, если в качестве типа аутентификации выбран «Пароль».	Null

Пользователь может протестировать текущую услугу SMS, доступна ли она в этом разделе.

Тестирование SMS		
Позиция	**Описание**	**По умолчанию**
Phone Number	Введите указанный номер телефона, на который можно получать SMS от маршрутизатора.	Null
Сообщение	Введите сообщение, которое маршрутизатор отправит на указанный номер телефона.	Null
Результат	Результат SMS-теста отобразится в поле результатов.	Null
Send	Нажмите кнопку, чтобы отправить тестовое сообщение.	--

3.21 Services > Email

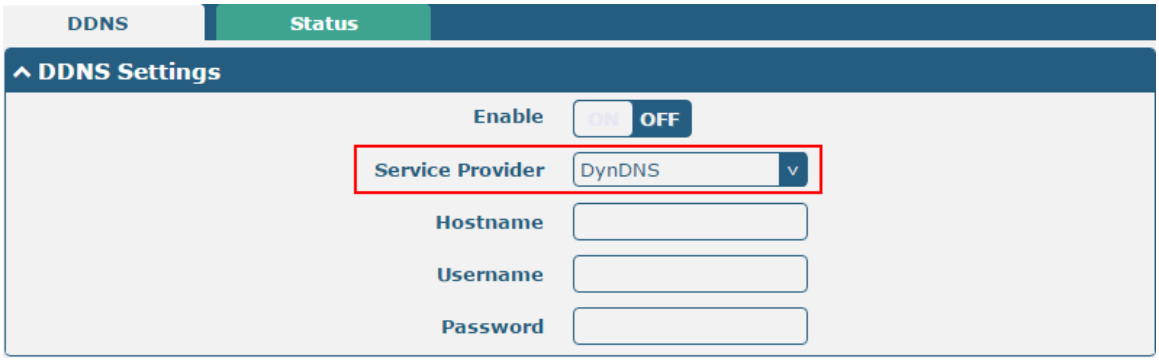
Функция электронной почты поддерживает отправку уведомлений о событиях указанному получателю по электронной почте.



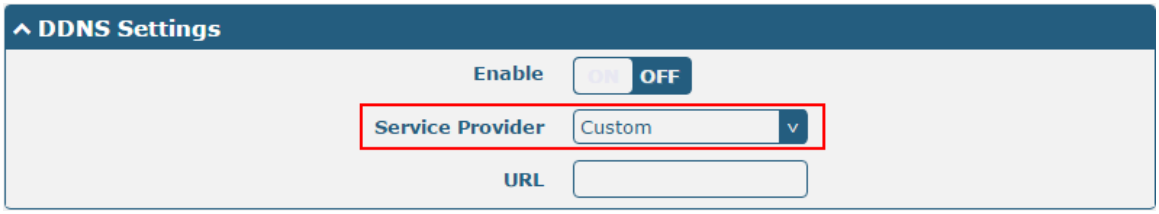
Настройки Email		
Позиция	**Описание**	**По умолчанию**
Enable	Нажмите кнопку-переключатель, чтобы включить/отключить параметр электронной почты.	OFF
Включить TLS/SSL	Нажмите кнопку-переключатель, чтобы включить/отключить параметр TLS/SSL.	OFF
Включить STARTTLS	Нажмите кнопку-переключатель, чтобы включить/отключить шифрование STARTTLS.	OFF
Исходящий сервер	Введите IP-адрес или доменное имя SMTP-сервера.	Null
Server port	Введите порт SMTP-сервера.	25
Время ожидания	Установите максимальное время отправки электронной почты на SMTP-сервер. Если сервер не получит письмо в течение этого времени, он попытается отправить его повторно.	10
Auth Login	Если почтовый сервер поддерживает авторизацию AUTH, необходимо активировать эту кнопку и установить имя пользователя и пароль.	OFF
Username	Введите имя пользователя, зарегистрированное с SMTP-сервера.	Null
Password	Введите пароль от имени пользователя, указанного выше.	Null
Из	Введите исходный адрес электронной почты.	Null
Предмет	Введите тему этого письма.	Null

3.22 Services > DDNS

Данный раздел позволяет установить параметры DDNS. Функция динамического DNS позволяет связать динамический IP-адрес со статическим доменным именем, позволяет вам, чей провайдер не назначает им статический IP-адрес, использовать доменное имя. Это особенно полезно для хостинга серверов через ваше соединение, так что любой желающий подключиться к вам может использовать ваше доменное имя, вместо того, чтобы использовать ваш динамический IP-адрес, который время от времени меняется. Этот динамический IP-адрес является WAN IP-адресом маршрутизатора, который назначается вам вашим интернет-провайдером. Поставщик услуг по умолчанию использует «DynDNS», как показано ниже.



Когда выбран «Пользовательский» поставщик услуг, отображается окно, как показано ниже.



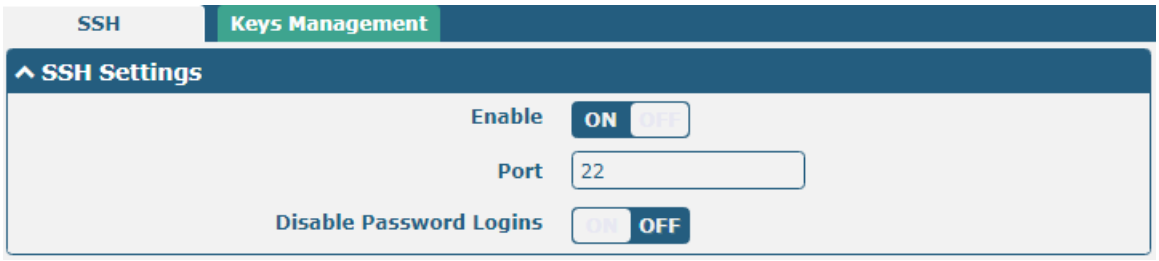
Настройки DDNS		
Позиция	**Описание**	**По умолчанию**
Enable	Нажмите кнопку-переключатель, чтобы включить/отключить опцию DDNS.	OFF
Service Provider	Выберите службу DDNS из «DynDNS», «NO-IP» «3322» или «Custom». **Примечание**: Служба DDNS может использоваться только после регистрации соответствующим поставщиком услуг.	DynDNS
Hostname	Введите имя хоста, предоставленное сервером DDNS.	Null
Username	Введите имя пользователя, предоставленное сервером DDNS.	Null
Password	Введите пароль, предоставленный сервером DDNS.	Null
URL	Введите URL-адрес, настроенный пользователем.	Null

Нажмите на строку «Состояние», чтобы просмотреть состояние DDNS.

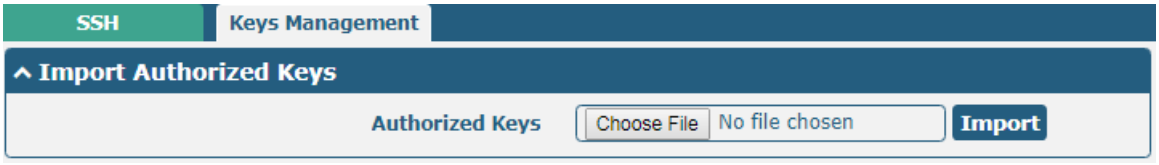
Статус DDNS	
Позиция	**Описание**
Статус	Отобразите текущий статус DDNS.
Время последнего обновления	Отображение даты и времени последнего успешного обновления DDNS.

3.23 Services > SSH

Маршрутизатор поддерживает доступ по паролю SSH и доступ по секретному ключу.



Настройки SSH		
Позиция	**Описание**	**По умолчанию**
Enable	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Когда он включен, можно получить доступ к маршрутизатору через SSH.	ON
Port	Установите порт доступа по SSH.	22
Отключить вход по паролю	Нажмите на кнопку-переключатель, чтобы включить/отключить эту опцию. Если этот параметр включен, невозможно использовать имя пользователя и пароль для доступа к маршрутизатору через SSH. В этом случае для входа можно использовать только ключ.	OFF

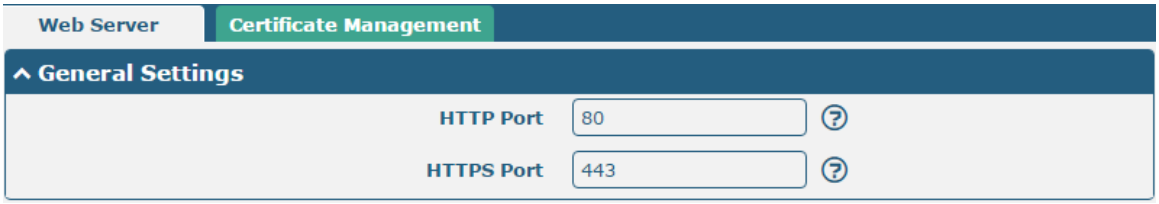


Import Authorized Keys	
Позиция	**Описание**

Authorized_keys	Нажмите «Выбрать файл», чтобы найти авторизованный ключ на вашем компьютере, а затем нажмите «Импорт», чтобы импортировать этот ключ в свой маршрутизатор. **Примечание**: Эта опция действительна при включении опции входа в систему с паролем.

3.24 Services > Web Server

Этот раздел позволяет вам изменять параметры Web Server.



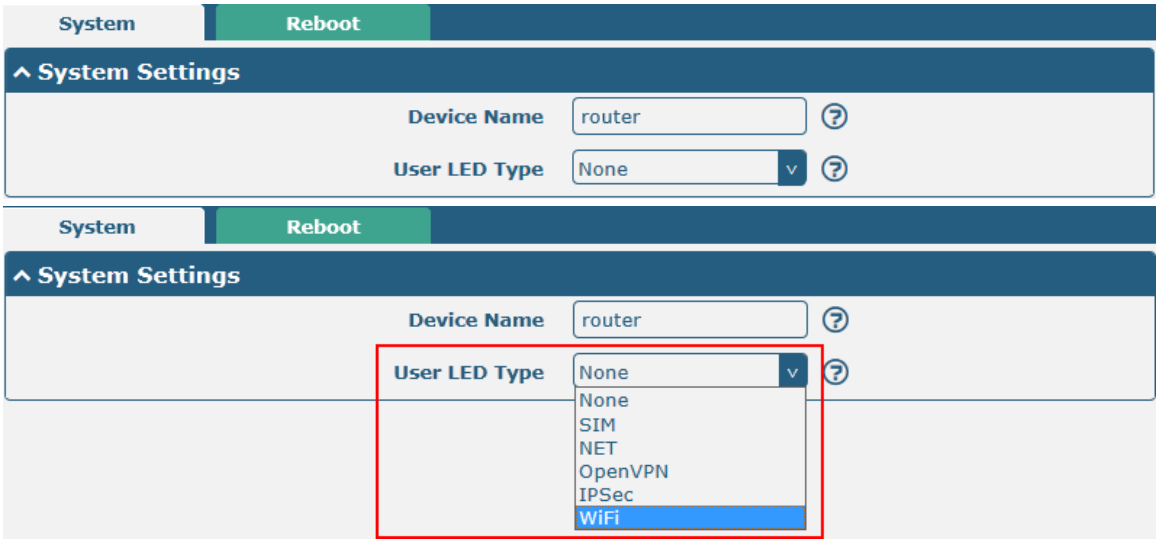
General Settings @ Web Server		
Позиция	**Описание**	**По умолчанию**
HTTP Port	Введите номер порта HTTP, который вы хотите изменить на веб-сервере маршрутизатора. На веб-сервере порт 80 – это порт, который сервер «слушает» или ожидает получить команду от веб-клиента. Если настроить маршрутизатор с другим номером порта HTTP, кроме 80, добавив только этот номер порта, вы сможете войти на веб-сервер маршрутизатора.	80
HTTPS Port	Введите номер порта HTTPS, который необходимо изменить, на веб-сервере маршрутизатора. На веб-сервере порт 443 – это порт, который сервер «слушает» или ожидает получить команду от веб-клиента. Если настроить маршрутизатор с другим номером порта HTTPS, кроме 443, добавив только этот номер порта, можно войти на веб-сервер маршрутизатора. **Примечание**. HTTPS более безопасен, чем HTTP. Во многих случаях клиенты могут обмениваться конфиденциальной информацией с сервером, который необходимо защитить, чтобы предотвратить несанкционированный доступ. По этой причине корпорация «Netscape» разработала протокол HTTP для авторизации и обеспечения безопасности транзакций.	443

Этот раздел позволяет импортировать файл сертификата в маршрутизатор.

Импортировать сертификат		
Позиция	**Описание**	**По умолчанию**
Тип импорта	Выберите «CA» или «Private Key». • CA: цифровой сертификат, выданный центром CA • Закрытый ключ: файл закрытого ключа	CA
HTTPS Certificate	Нажмите «Выбрать файл», чтобы найти файл сертификата на вашем компьютере, а затем нажмите «Импорт», чтобы импортировать этот файл в свой маршрутизатор.	--

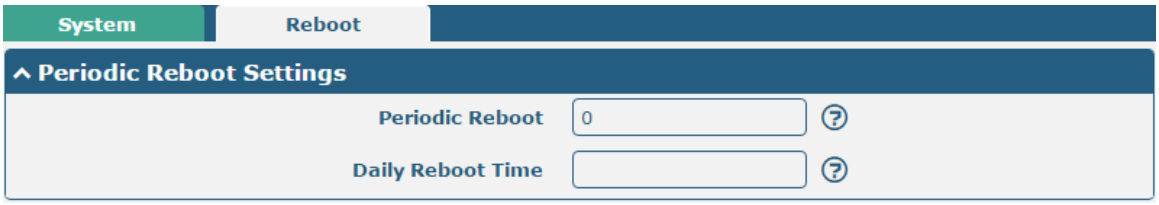
3.25 Services > Advanced

Этот раздел позволяет установить дополнительные параметры.



Системные настройки		
Позиция	**Описание**	**По умолчанию**
Device Name	Задайте имя устройства, чтобы различать разные установленные устройства; допустимые символы: a-z, A-Z, 0-9, @,., -, #, $ и *.	маршрутизатор
Тип светодиода пользователя	Укажите тип отображения вашего светодиода USR. Выберите из «None», «SIM», «NET», «OpenVPN», «IPsec» или «WiFi». • None: индикация бессмысленна, светодиод не горит. • SIM: Индикатор USR, показывающий состояние SIM. • NET: Индикатор USR, показывающий состояние NET • OpenVPN: индикатор USR, показывающий статус OpenVPN • IPsec: индикатор USR, показывающий состояние IPsec. • WiFi: индикатор USR, показывающий статус WiFi	None

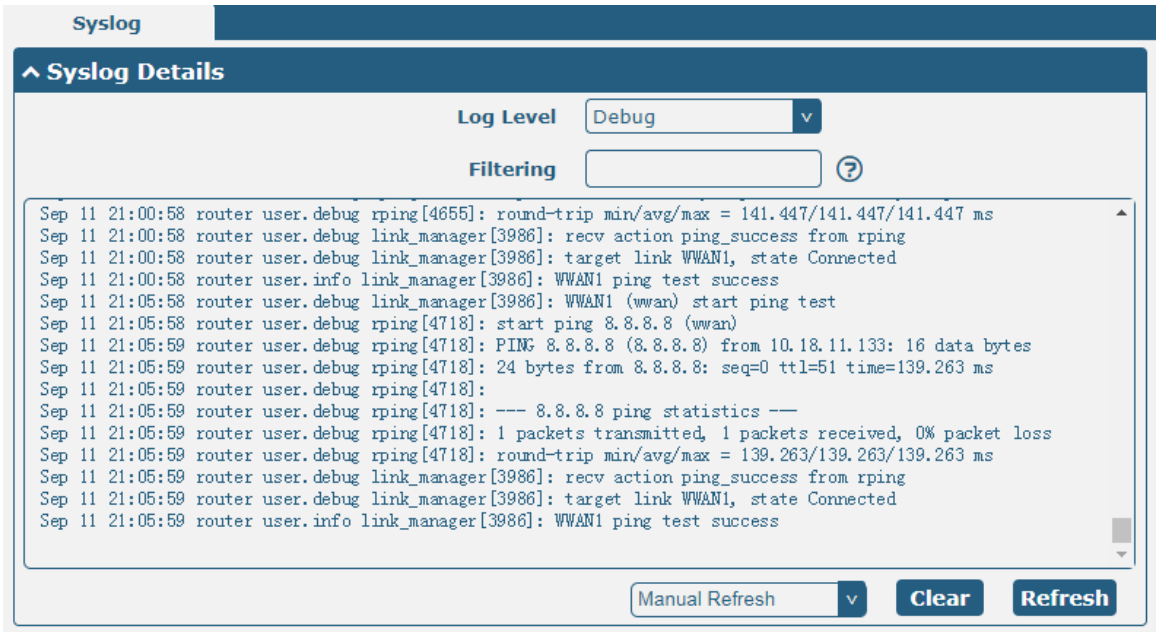
	Примечание. Дополнительные сведения об индикаторе USR см. В разделе «2.2 Светодиодные индикаторы».	

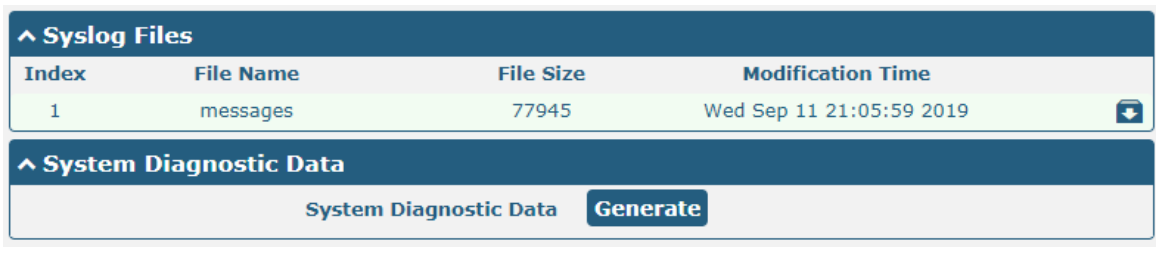


Настройки периодической перезагрузки		
Позиция	**Описание**	**По умолчанию**
Периодическая перезагрузка	Установите период перезагрузки маршрутизатора. 0 означает отключение.	0
Время ежедневной перезагрузки	Установка времени ежедневной перезагрузки роутера. Вам следует соблюдать формат HH: MM, временные рамки 24 ч, в ином случае данные будут недействительны. Оставьте поле пустым,это означает отключение.	Null

3.26 System > Debug

Этот раздел позволяет вам проверить и загрузить подробную информацию о системном журнале.



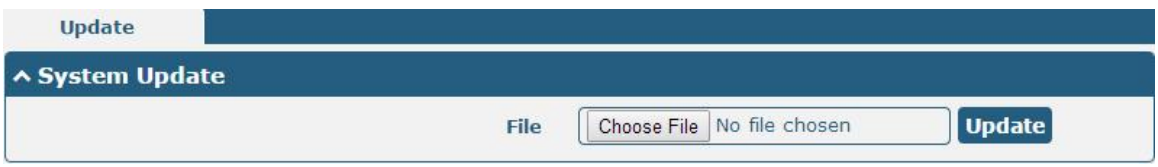


Syslog		
Позиция	**Описание**	**По умолчанию**
Данные Syslog		
Уровень журнала	Выберите из «Debug», «Info», «Notice», «Warn», «Error», снизу вверх. На нижнем уровне выводится более подробная информация о системном журнале.	Отладка
Фильтрация	Введите сообщение для фильтрации на основе ключевых слов. Используйте «&», чтобы разделить более одного сообщения фильтра, например «keyword1&keyword2».	Null
Обновить	Выберите «Manual Refresh», «5 Seconds», «10 Seconds», «20 Seconds» или «30 Seconds». Вы можете выбрать эти интервалы, чтобы обновить информацию журнала, отображаемую в следующем поле. Если выбрано «manual refresh», следует нажать кнопку обновления, чтобы обновить системный журнал.	Обновить вручную
Clear	Нажмите кнопку, чтобы очистить системный журнал.	--
Refresh	Нажмите кнопку, чтобы обновить системный журнал.	--
Файлы системного журнала		
Список файлов системного журнала	Он может отображать не более 5 файлов системного журнала в списке, имена файлов варьируются от message0 до message 4. И самый новый файл системного журнала будет помещен в начало списка.	--
Данные диагностики системы		
Generate	Нажмите, чтобы создать файл диагностики системного журнала.	--
Download	Нажмите, чтобы перезагрузить файл диагностики системы.	--

3.27 System > Update

Данный раздел позволит вам обновить систему маршрутизатора и выполнить обновление системы путем импорта и обновления файлов прошивки. Для импорта файла прошивки из компьютера к маршрутизатору нажмите Update и перезагрузите устройство согласно подсказкам для завершения обновления файлов прошивки.

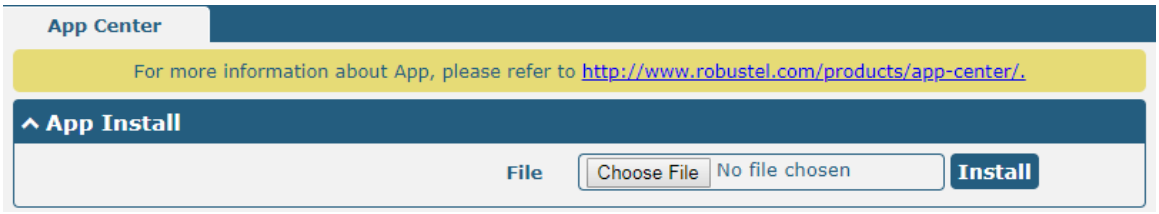
Примечание. Чтобы получить доступ к последней версии прошивки, обратитесь к инженеру службы технической поддержки.



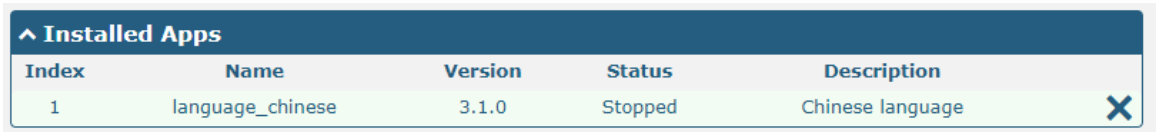
3.28 System > App Center

Этот раздел позволяет добавлять к маршрутизатору некоторые необходимые или настраиваемые приложения. Импортируйте и установите приложения в Центр приложений и перезагрузите устройство в соответствии с подсказками системы. Каждое установленное приложение будет отображаться в меню «Services», а другие приложения, связанные с VPN, будут отображаться в меню «VPN».

Примечание: после импорта приложений в маршрутизатор отображение страницы может иметь небольшую задержку из-за кэша браузера. Рекомендуется сначала очистить кэш браузера и снова войти в маршрутизатор.



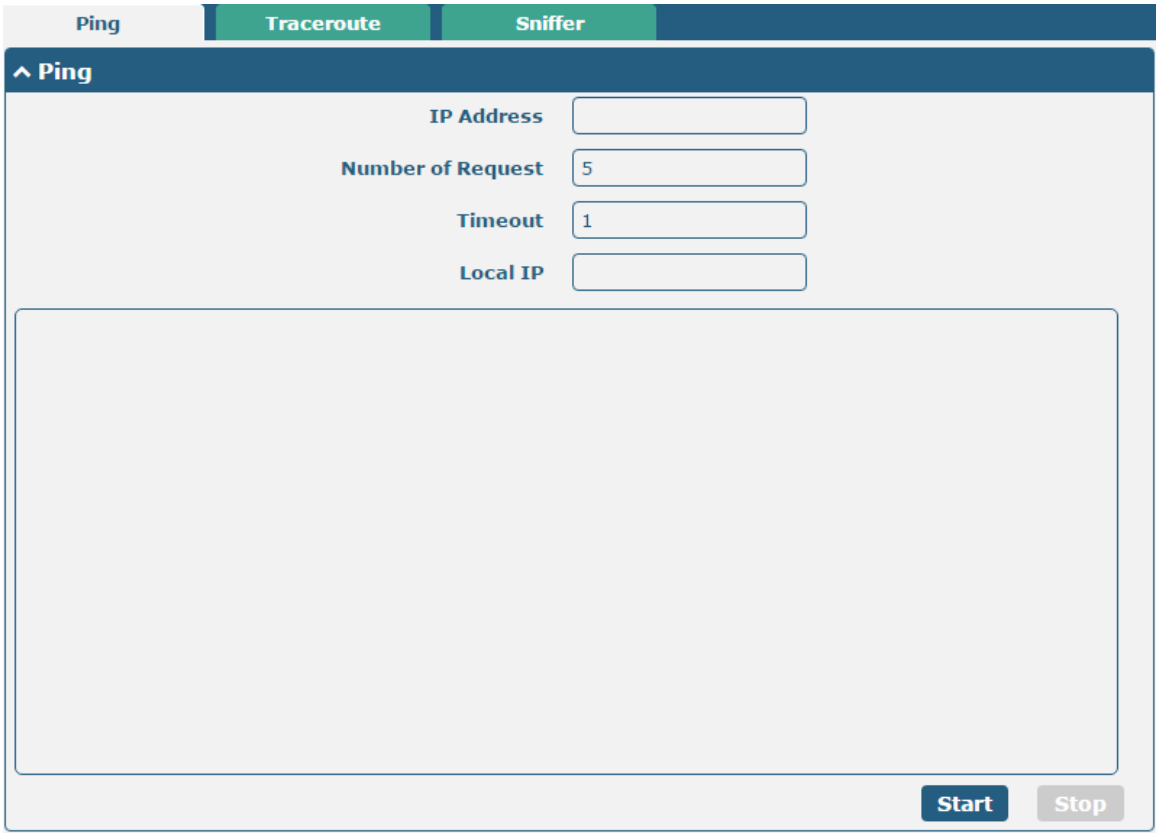
Успешно установленное приложение отобразится в следующем списке. Нажмите на ✕, чтобы удалить приложение.



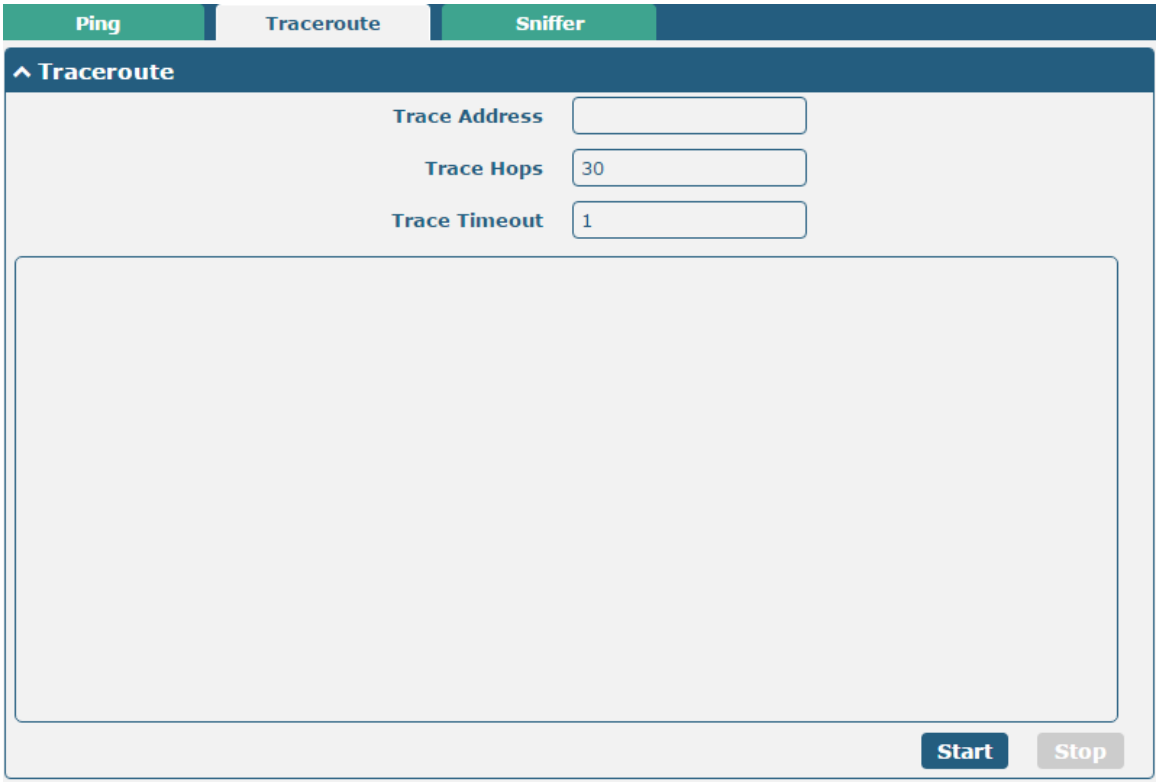
App Center		
Позиция	**Описание**	**По умолчанию**
Установить приложение		
File	Нажмите «Choose File», чтобы найти файл приложения на вашем компьютере, а затем нажмите Install, чтобы импортировать этот файл в свой маршрутизатор. **Примечание**: Формат файла должен быть *xxx.rpk*, например, *R2000-robustlink-1.0.0.rpk*.	--
Установленные приложения		
Index	Указывает порядковый номер списка.	--
Name	Отображает название приложения.	Null
Version	Отображает версию приложения.	Null
Статус	Отображает статус приложения.	Null
Описание	Отображает описание этого приложения.	Null

3.29 System > Tools

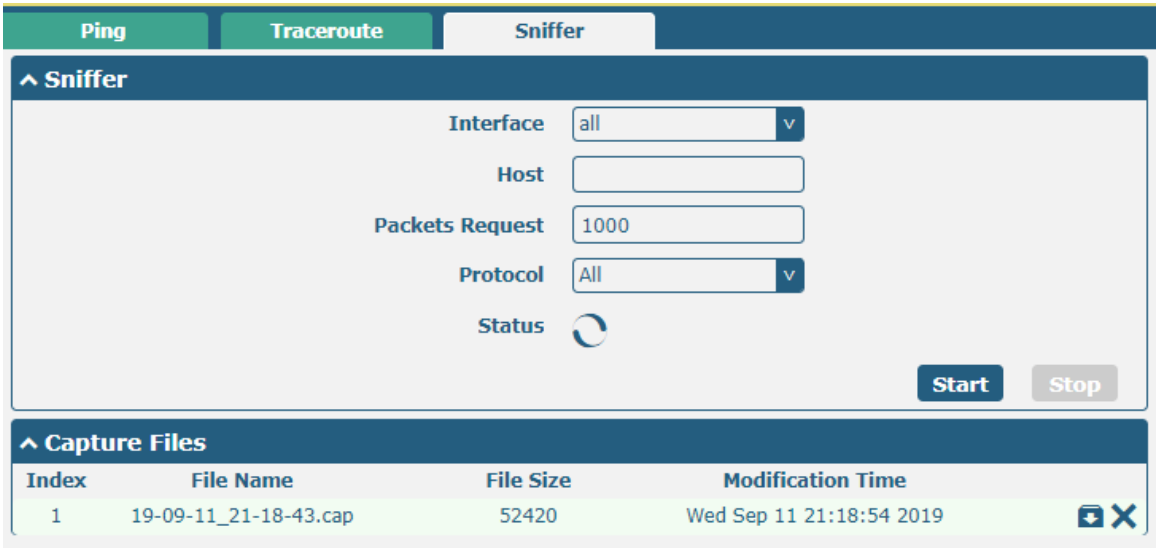
Этот раздел предоставляет пользователям три инструмента: Ping, Traceroute и Sniffer.



Ping		
Позиция	**Описание**	**По умолчанию**
IP Address	Введите IP-адрес пункта назначения ping или домен назначения.	Null
Количество запросов	Укажите количество запросов ping.	5
Время ожидания	Укажите время ожидания запросов ping.	1
Local IP	Укажите локальный IP-адрес из сотовой WAN, Ethernet WAN или Ethernet LAN. Null означает автоматический выбор локального IP-адреса из этих трех.	Null
Start	Нажмите эту кнопку, чтобы запустить запрос ping, и журнал отобразится в следующем поле.	--
Stop	Нажмите эту кнопку, чтобы остановить запрос ping.	--



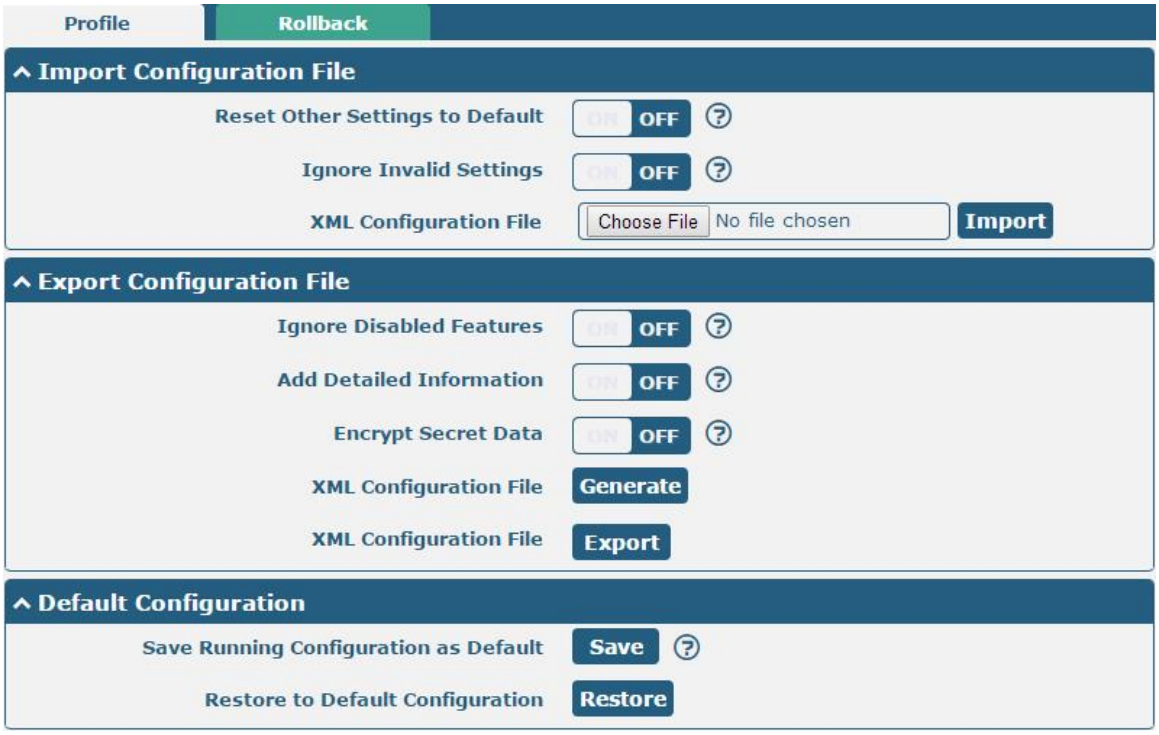
Программа контроля прохождения сигнала по сети		
Позиция	**Описание**	**По умолчанию**
Адрес контроля прохождения сигнала по сети	Введите IP-адрес или домен назначения трассировки.	Null
Следы контроля прохождения сигнала по сети	Укажите максимальное количество скачков трассировки. Маршрутизатор прекратит трассировку, если количество скачков трассировки достигнет максимального значения, независимо от того, достигнут пункт назначения или нет.	30
Время ожидания контроля прохождения сигнала по сети	Укажите время ожидания запроса контроля прохождения сигнала по сети.	1
Start	Нажмите эту кнопку, чтобы запустить запрос контроля прохождения сигнала по сети, и журнал отобразится в следующем поле.	--
Stop	Нажмите эту кнопку, чтобы остановить запрос контроля прохождения сигнала по сети.	--



Sniffer		
Позиция	**Описание**	**По умолчанию**
Interface	Выберите интерфейс в соответствии с вашей конфигурацией Ethernet.	All
Host	Отфильтруйте пакет, содержащий указанный IP-адрес.	Null
Запрос пакетов	Установите номер пакета, который маршрутизатор может перехватывать за раз.	1000
Protocol	Выберите «All», «IP», «TCP», «UDP» и «ARP».	All
Статус	Показать текущий статус сниффера.	--
Start	Нажмите эту кнопку, чтобы запустить сниффер.	--
Stop	Нажмите эту кнопку, чтобы остановить сниффер. При нажатии на эту кнопку новый файл журнала отобразится в следующем списке.	--
Поиск файлов	Каждый раз журнал сниффера автоматически сохраняется как новый файл. Можно найти файл в этом Списке данных трафика сниффера и нажмите на , чтобы загрузить журнал, нажмите на , чтобы удалить файл журнала. Он может кэшировать максимум 5 файлов.	--

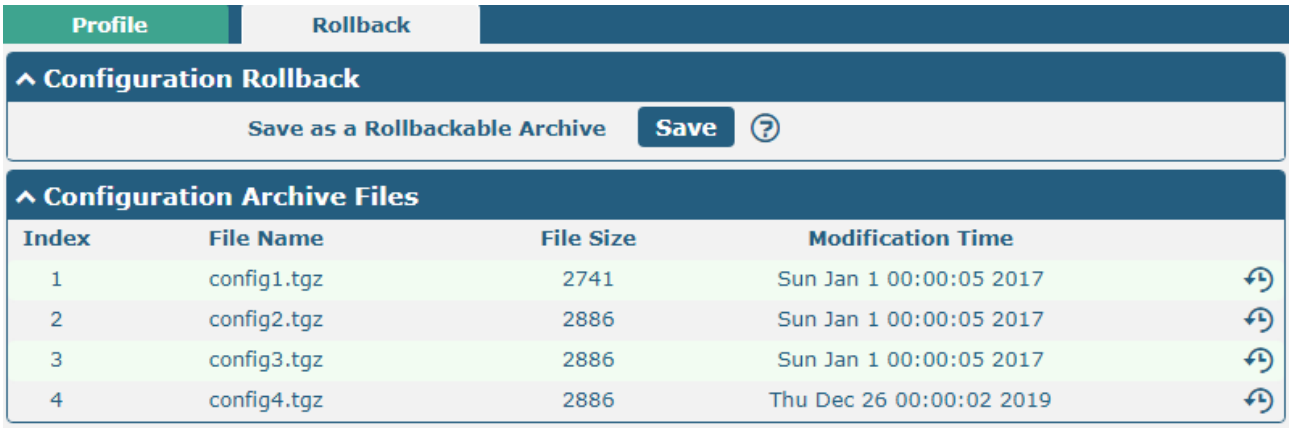
3.30 System > Profile

В этом разделе можно импортировать или экспортировать файл конфигурации и восстановить заводские настройки маршрутизатора по умолчанию.



Profile		
Позиция	**Описание**	**По умолчанию**
Импортировать файл конфигурации		
Сбросить другие настройки по умолчанию	Установите переключатель в положение «ON», чтобы вернуть другие параметры к настройкам по умолчанию.	OFF
Игнорировать неверные настройки	Установите переключатель в положение «OFF», Чтобы игнорировать недопустимые настройки.	OFF
Файл конфигурации XML	Нажмите на Choose File, чтобы найти файл конфигурации XML на своем компьютере, а затем нажмите на Import, чтобы импортировать этот файл в маршрутизатор.	--
Экспорт файла конфигурации		
Игнорировать отключенные функции	Установите переключатель в положение «OFF», Чтобы игнорировать отключенные функции.	OFF
Добавить подробную информацию	Установите переключатель в положение «On», Чтобы добавить подробную информацию.	OFF
Шифровать секретные данные	Установите переключатель в положение «ON», чтобы зашифровать секретные данные.	OFF
Файл конфигурации XML	Нажмите кнопку Generate для генерирования файла конфигурации XML и нажмите Export для экспорта файла конфигурации XML.	--
Конфигурация по умолчанию		
Сохранить текущую конфигурацию по умолчанию	Нажмите на кнопку Save, чтобы сохранить текущие рабочие параметры в качестве конфигурации по умолчанию.	--
Восстановить	Нажмите на кнопку Restore, чтобы восстановить заводские	--

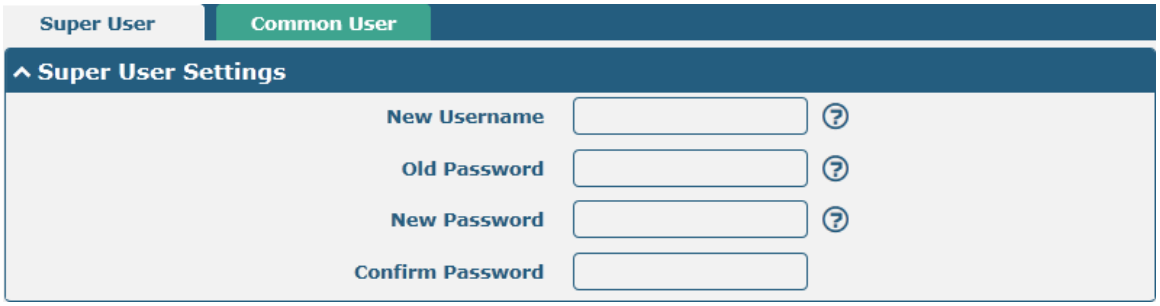
конфигурацию по умолчанию	настройки по умолчанию.	



Возврат в исходное состояние		
Позиция	**Описание**	**По умолчанию**
Конфигурация возврата в исходное состояние		
Сохранить как исходный архив	Создайте точку сохранения вручную. Кроме того, при изменении конфигурации система каждый день будет автоматически создавать точку сохранения.	--
Конфигурация архивных файлов		
Конфигурация архивных файлов	Просмотрите соответствующую информацию о файлах архива конфигурации, включая имя, размер и время изменения.	--

3.31 System > User Management

Данный раздел позволяет вам изменить ваше имя пользователя и пароль, а также создавать аккаунты пользователей и управлять ими. У одного маршрутизатора есть только один суперпользователь, который имеет наивысшие полномочия изменять, добавлять и управлять другими общими пользователями.
Примечание: ваш новый пароль должен состоять более чем из 5 символов и менее чем из 32 символов, может содержать номера, буквы верхнего и нижнего регистра, а также стандартные символы.



Настройки суперпользователя		
Позиция	**Описание**	**По умолчанию**
Новое имя пользователя	Введите новое имя пользователя, которое хотите создать; допустимые символы: a-z, A-Z, 0-9, @,., -, #, $ и *.	Null
Старый пароль	Введите старый пароль используемого маршрутизатора. По умолчанию – «admin».	Null
Новый пароль	Введите новый пароль, который хотите создать; допустимые символы: a-z, A-Z, 0-9, @,., -, #, $ и *.	Null
Подтвердить пароль	Введите новый пароль еще раз для подтверждения.	Null

Нажмите кнопку +, чтобы добавить нового обычного пользователя. Максимальное количество правил – 5.

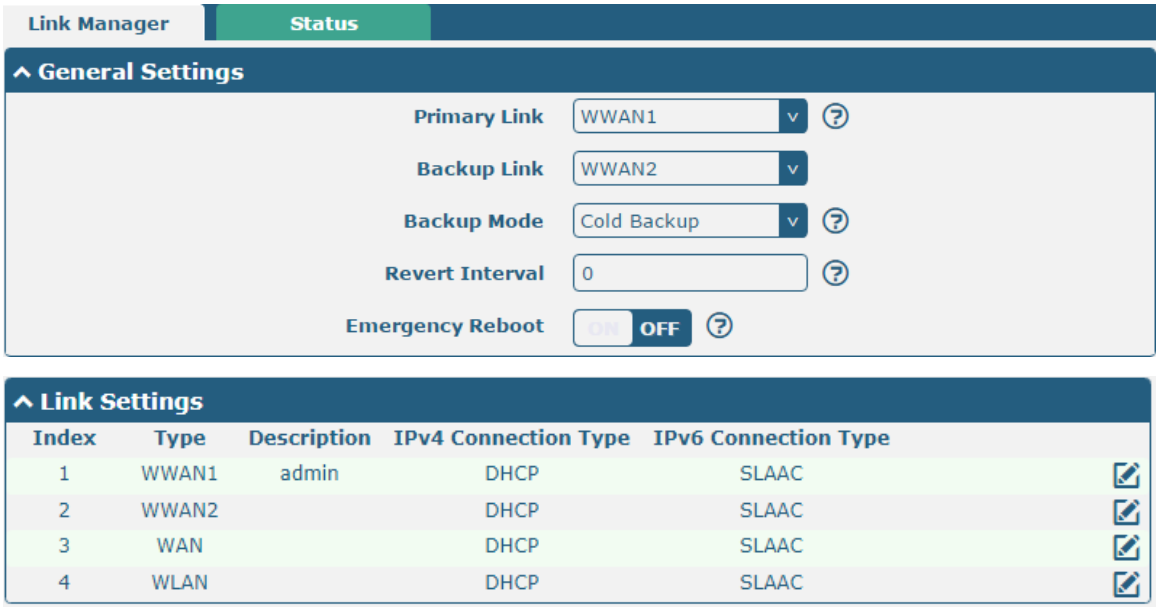
Общие настройки пользователя		
Позиция	**Описание**	**По умолчанию**
Index	Указывает порядковый номер списка.	--
Роль	Выберите «Visitor» или «Editor». • Visitor: только пользователи могут просматривать конфигурацию маршрутизатора на этом уровне. • Editor: пользователи могут просматривать и настраивать конфигурацию маршрутизатора на этом уровне.	Visitor
Username	Установите имя пользователя; допустимые символы: a-z, A-Z, 0-9, @,., -, #, $ и *.	Null
Password	Установите пароль, содержащий не менее 5 символов; допустимые символы: a-z, A-Z, 0-9, @,., -, #, $ и *.	Null

Глава 4 Примеры конфигурации

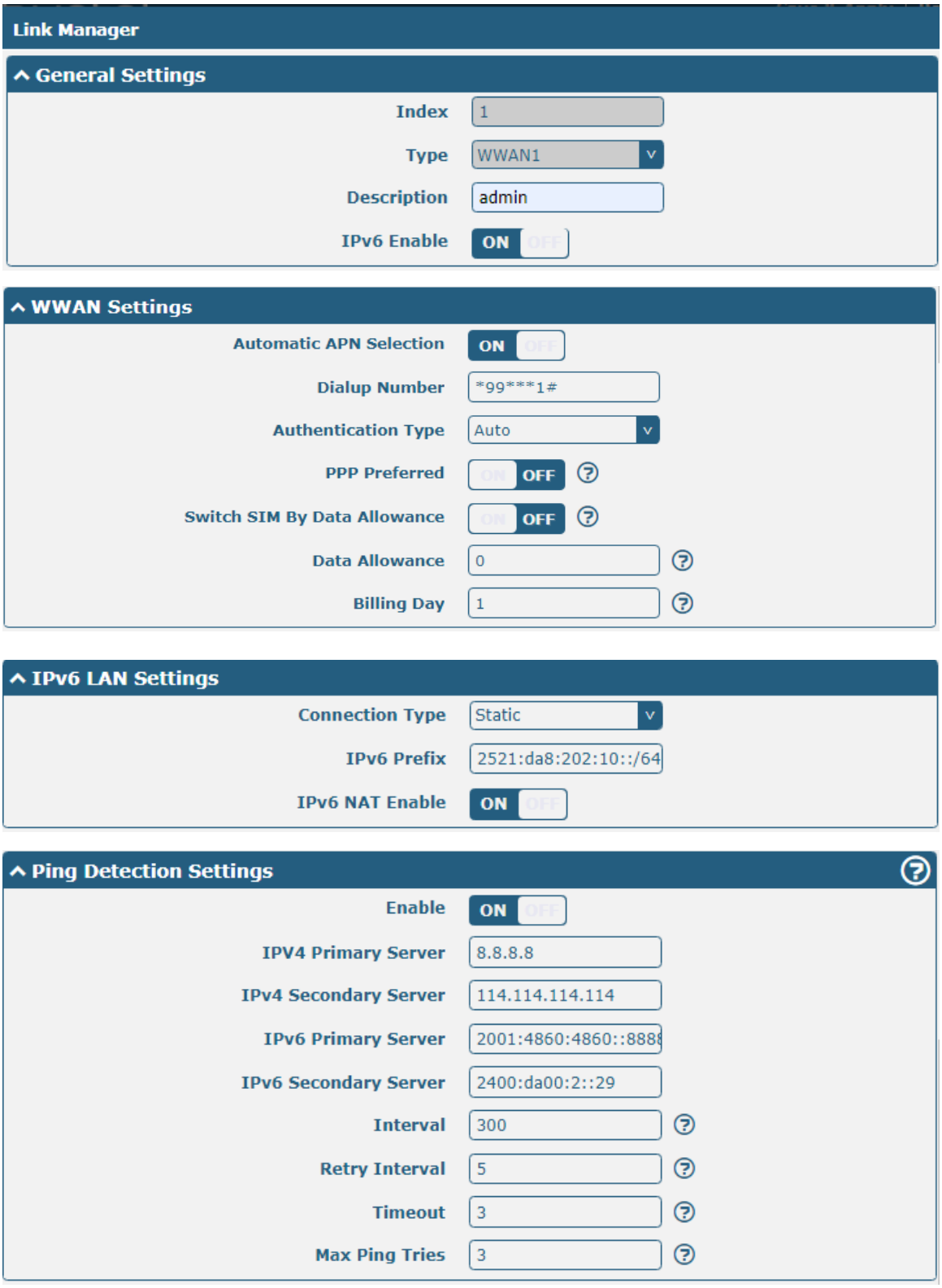
4.1 Сотовый

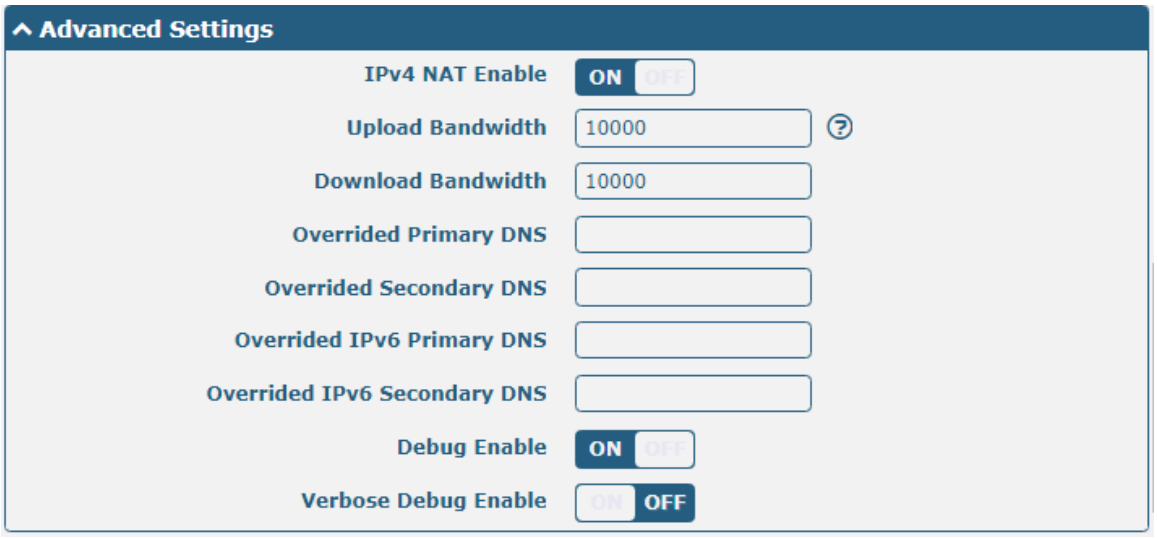
4.1.1 Сотовый коммутируемый доступ

В этом разделе описан способ настройки основной и резервной SIM-карты для подключения к сотовой сети. Подключите маршрутизатор правильно и вставьте две SIM-карты, затем откройте страницу конфигурации. В меню домашней страницы нажмите на **Interface > Link Manager > Link Manager > General Settings**, выберите «WWAN1» в качестве основного канала и «WWAN2» в качестве резервного канала и установите «Холодное резервное копирование» в качестве режима резервного копирования, затем нажмите «Submit».
Примечание. Все данные будут передаваться через WWAN1, если WWAN1 выбрана в качестве основного канала и установлен режим резервного копирования как «холодное». В то же время WWAN2 всегда находится в автономном режиме в качестве резервного канала. Вся передача данных будет переключена на WWAN2 при отключении WWAN1.



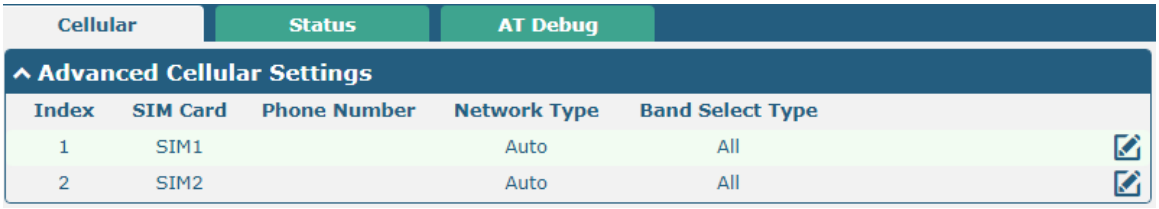
Нажмите на кнопку по самой правой из WWAN1, чтобы установить ее параметры в соответствии с текущим интернет-провайдером.


Link Manager
General Settings
Index
1
Type
WWAN1
Description
admin
IPv6 Enable
ON
WWAN Settings
Automatic APN Selection
ON
Dialup Number
*99***1#
Authentication Type
Auto
PPP Preferred
OFF
Switch SIM By Data Allowance
OFF
Data Allowance
0
Billing Day
1
IPv6 LAN Settings
Connection Type
Static
IPv6 Prefix
2521:da8:202:10::/64
IPv6 NAT Enable
ON
Ping Detection Settings
Enable
ON
IPV4 Primary Server
8.8.8.8
IPv4 Secondary Server
114.114.114.114
IPv6 Primary Server
2001:4860:4860::8888
IPv6 Secondary Server
2400:da00:2::29
Interval
300
Retry Interval
5
Timeout
3
Max Ping Tries
3

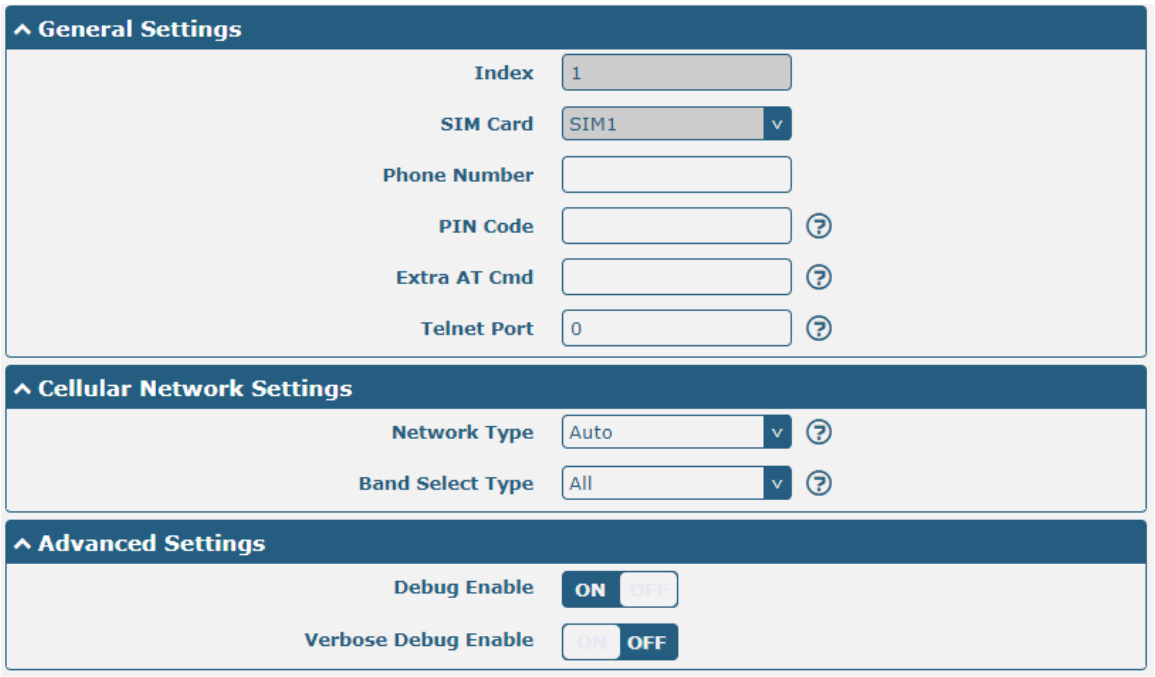


По завершении нажмите **Submit > Save & Apply**, чтобы конфигурация вступила в силу.

Окно отображается ниже, если нажать **Interface > Cellular > Advanced Cellular Settings**.



Нажмите кнопку редактирования SIM1, чтобы настроить ее параметры в соответствии с запросом ипользуемого приложения.



По завершении нажмите **Submit > Save & Apply**, чтобы конфигурация вступила в силу.

4.1.2 Удаленное управление по SMS

Маршрутизатор поддерживает удаленное управление через SMS. Можно использовать следующие команды, чтобы получить статус маршрутизатора и установить все параметры. Для управления по SMS существует три типа аутентификации. Можно выбрать «Password», «Phonenum» или «Both».

SMS-команда имеет следующую структуру:

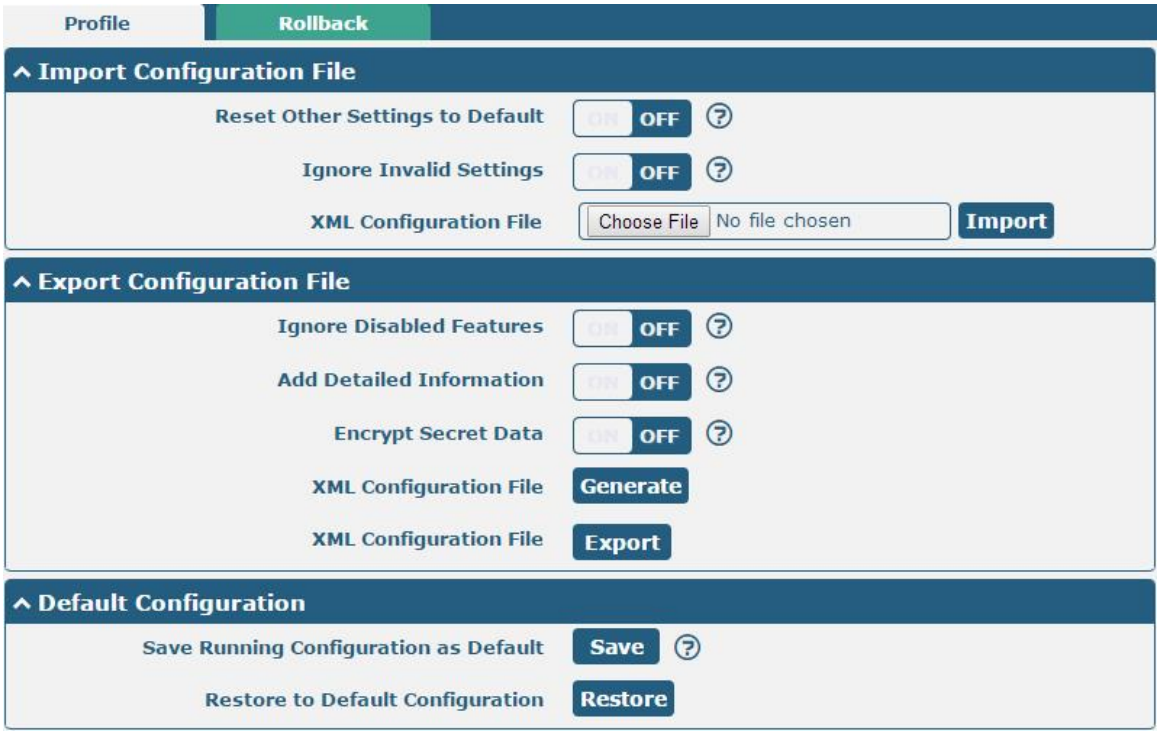
1. Режим пароля – Username: **Password;cmd1;cmd2;cmd3; …cmdn** (доступно для каждого номера телефона).
2. Режим Phonenum; **Password; cmd1; cmd2; cmd3; … cmdn**(доступно, если SMS было отправлено с номера телефона, который был добавлен в группу телефонов маршрутизатора).
3. Оба режима – **Username: Password;cmd1;cmd2;cmd3; …cmdn** (доступно, если SMS было отправлено с номера телефона, который был добавлен в группу телефонов маршрутизатора).

Пояснение к SMS-команде:

1. Username и Password: используйте те же имя пользователя и пароль, что и WEB-менеджер для аутентификации.
2. **cmd1, cmd2, cmd3 на Cmdn**, формат команды такой же, как у команды CLI, более подробную информацию о CLI cmd см. в **главе 5 Введение в CLI**.

   Примечание. Загрузите XML-файл конфигурации из настроенного веб-браузера. Формат управляющей SMS-команды может относиться к данным файла XML.

   Перейдите в **System > Profile > Export Configuration File**, нажмите на Generate, чтобы сгенерировать файл XML, и на Export, чтобы экспортировать файл XML.



Команда XML:

<lan >

<network max_entry_num="2" >
<id > 1</id >
<interface > lan0</interface >
<ip > 172.16.10.67</ip >
<netmask > 255.255.0.0</netmask >
<mtu > 1500</mtu >

SMS cmd:

установить интерфейс локальной сети 1 lan0
установить интерфейс локальной сети 1 ip 172.16.10.67
установить сетевую маску LAN 1 255.255.0.0
установить сеть LAN 1 MTU 1500

3. Символ точки с запятой (';') используется для разделения более чем одной команды, упакованной в одно SMS.
4. Например,

admin:admin;status system

В этой команде имя пользователя «admin», пароль «admin», а функция команды - получить статус системы.

Получено SMS:

hardware_version = 1.0
firmware_version = "3.0.0"
kernel_version = 3.10.49
device_model = R2000
serial_number = 111111111
system_uptime = «0 days, 06:17:32»
system_time = «Thu Jul 6 17:28:51 2017»

admin:admin;reboot

В этой команде имя пользователя – «admin», пароль – «admin», а команда предназначена для перезагрузки маршрутизатора.

Получено SMS:

OK

admin:admin;set firewall remote_ssh_access false;set firewall remote_telnet_access false

В этой команде имя пользователя – «admin», пароль– «admin», команда предназначена для отключения доступа remote_ssh и remote_telnet.

Получено SMS:

OK
OK

admin:admin; set lan network 1 interface lan0;set lan network 1 ip 172.16.99.11;set lan network 1 netmask 255.255.0.0;set lan network 1 mtu 1500

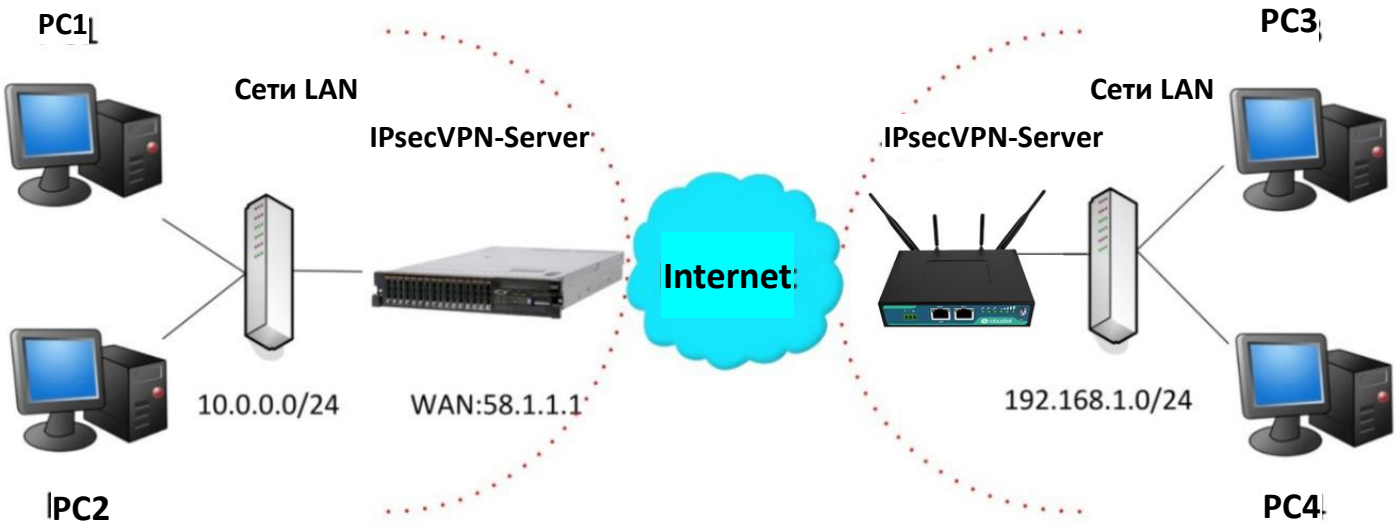
В этой команде имя пользователя – «admin», пароль – «admin», а команды предназначены для настройки параметра LAN.

Получено SMS:

OK
OK
OK
OK

4.2 Network

4.2.1 IPsec VPN



Конфигурация сервера и клиента следующая.

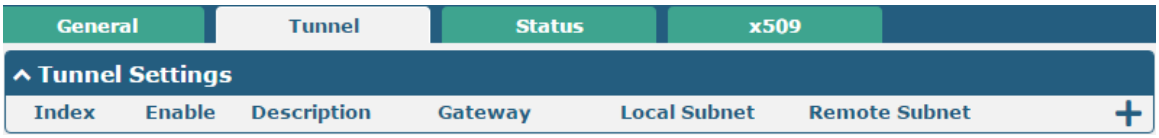
IPsec VPN_Server:

Cisco 2811:

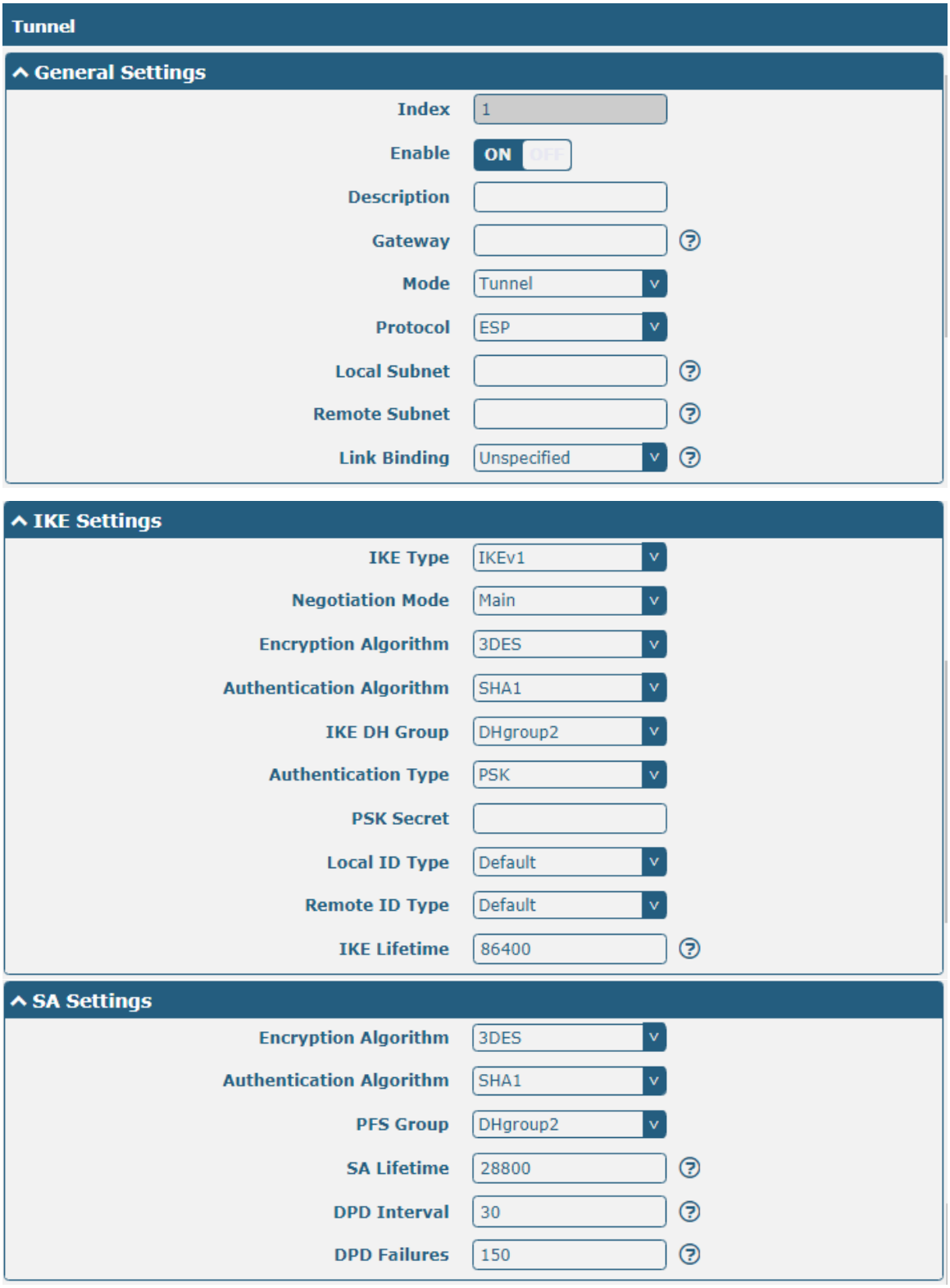
```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp ?
  client  Set client configuration policy
  enable  Enable ISAKMP
  key     Set pre-shared key for remote peer
  policy  Set policy for an ISAKMP protection suite
Router(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0


Router(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
Router(config)#crypto ipsec ?
  security-association  Security association parameters
  transform-set         Define transform and settings
Router(config)#crypto ipsec transform-set Trans ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-sha-hmac  ESP transform using HMAC-SHA auth
Router(config)#crypto ipsec transform-set Trans esp-3des esp-md5-hmac


Router(config)#ip access-list extended vpn
Router(config-ext-nacl)#permit ip 10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config-ext-nacl)#exit

Router(config)#crypto map cry-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#match address vpn
Router(config-crypto-map)#set transform-set Trans
Router(config-crypto-map)#set peer 202.100.1.1
Router(config-crypto-map)#exit


Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 58.1.1.1 255.255.255.0
Router(config-if)#cr
Router(config-if)#crypto map cry-map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

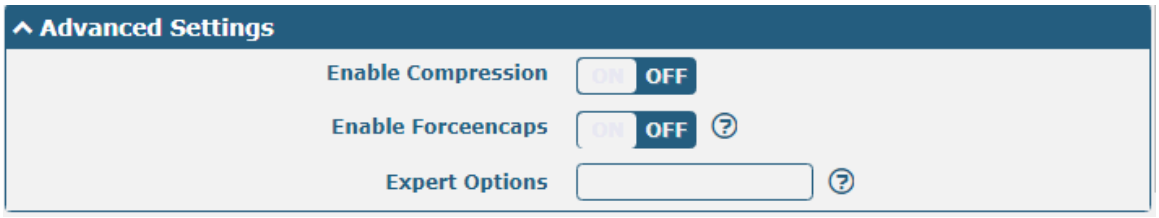
IPsec VPN_Client:

После нажатия **VPN> IPsec> Tunnel** окно отображается в соответствии с рисунком ниже.



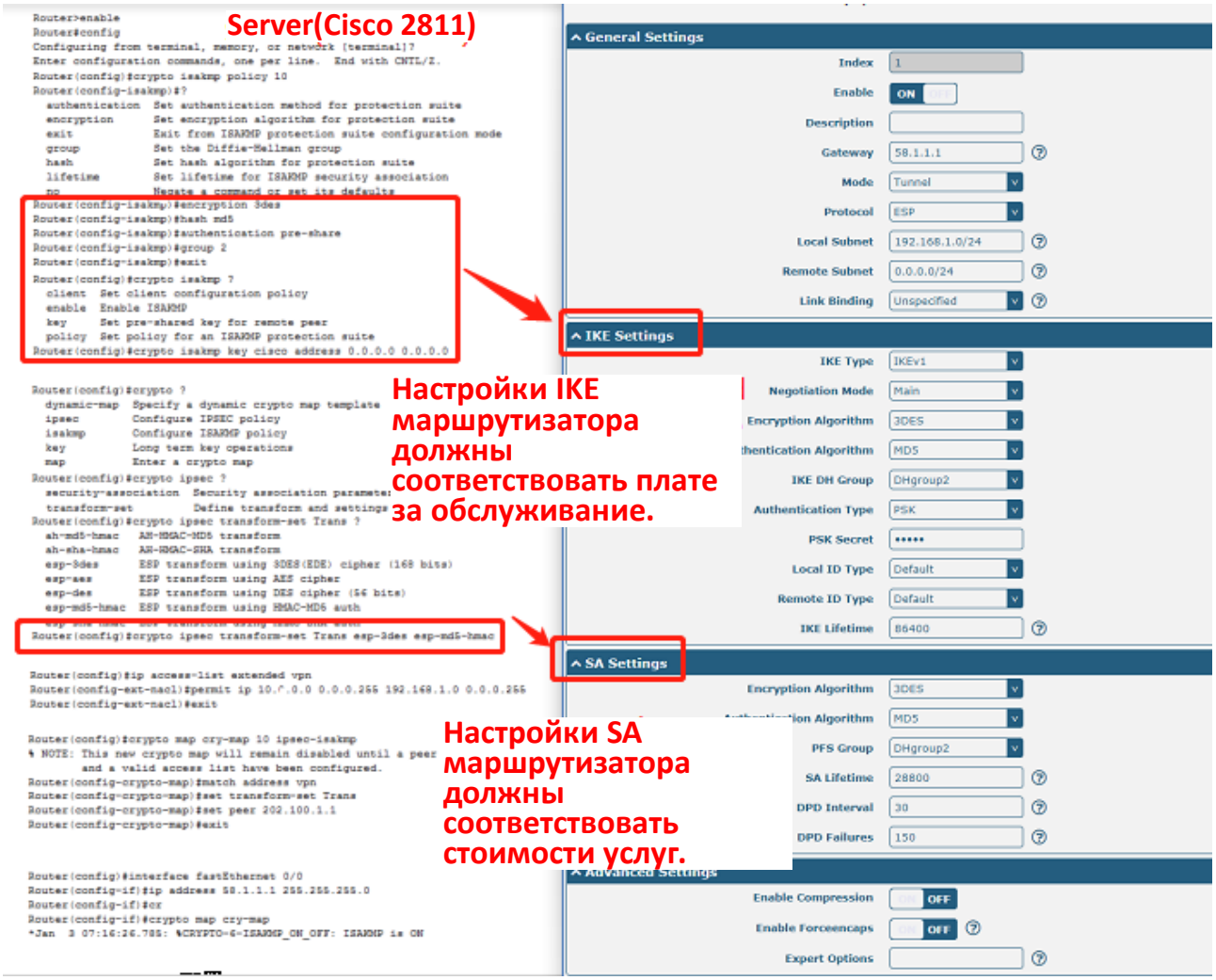
Нажмите кнопку + и установите параметры клиента IPsec в соответствии с рисунком ниже.





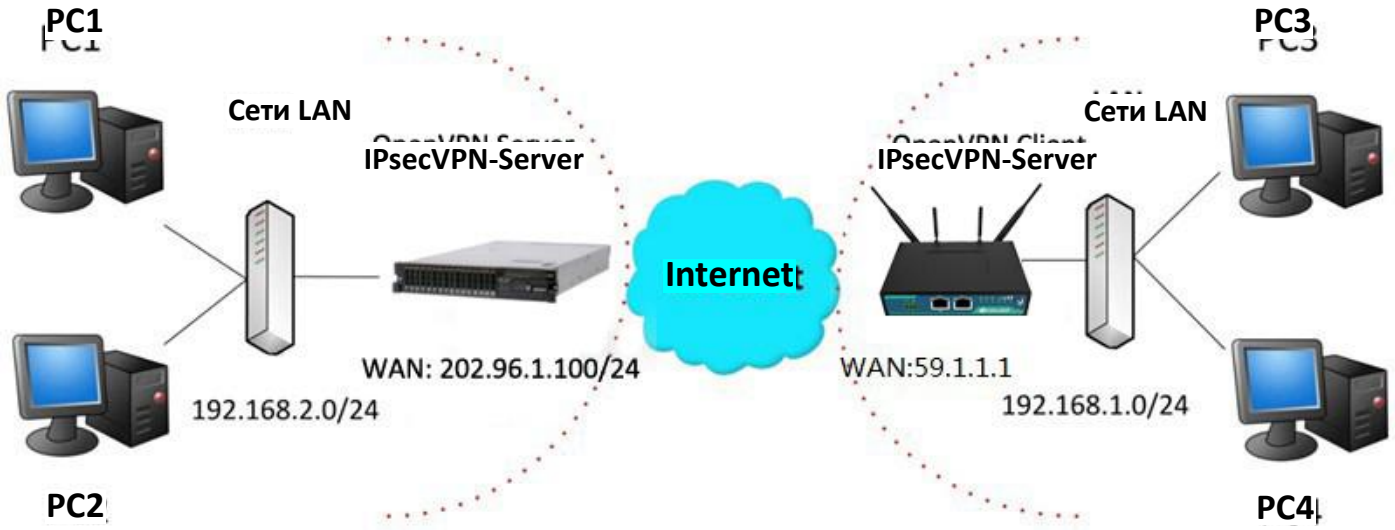
По завершении нажмите **Submit > Save & Apply**, чтобы конфигурация вступила в силу.

Сравнение между сервером и клиентом показано ниже.



4.2.2 OpenVPN

OpenVPN поддерживает два режима, включая клиентский и P2P. Здесь в качестве примера возьмем Client.



OpenVPN_Server:

Сначала сгенерируйте соответствующий сертификат OpenVPN на стороне сервера и воспользуйтесь следующими командами для настройки сервера:

local 202.96.1.100
mode server
port 1194
proto udp
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert Server01.crt
key Server01.key
dh dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.3.0 255.255.255.0"
client-config-dir ccd
route 192.168.1.0 255.255.255.0
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3

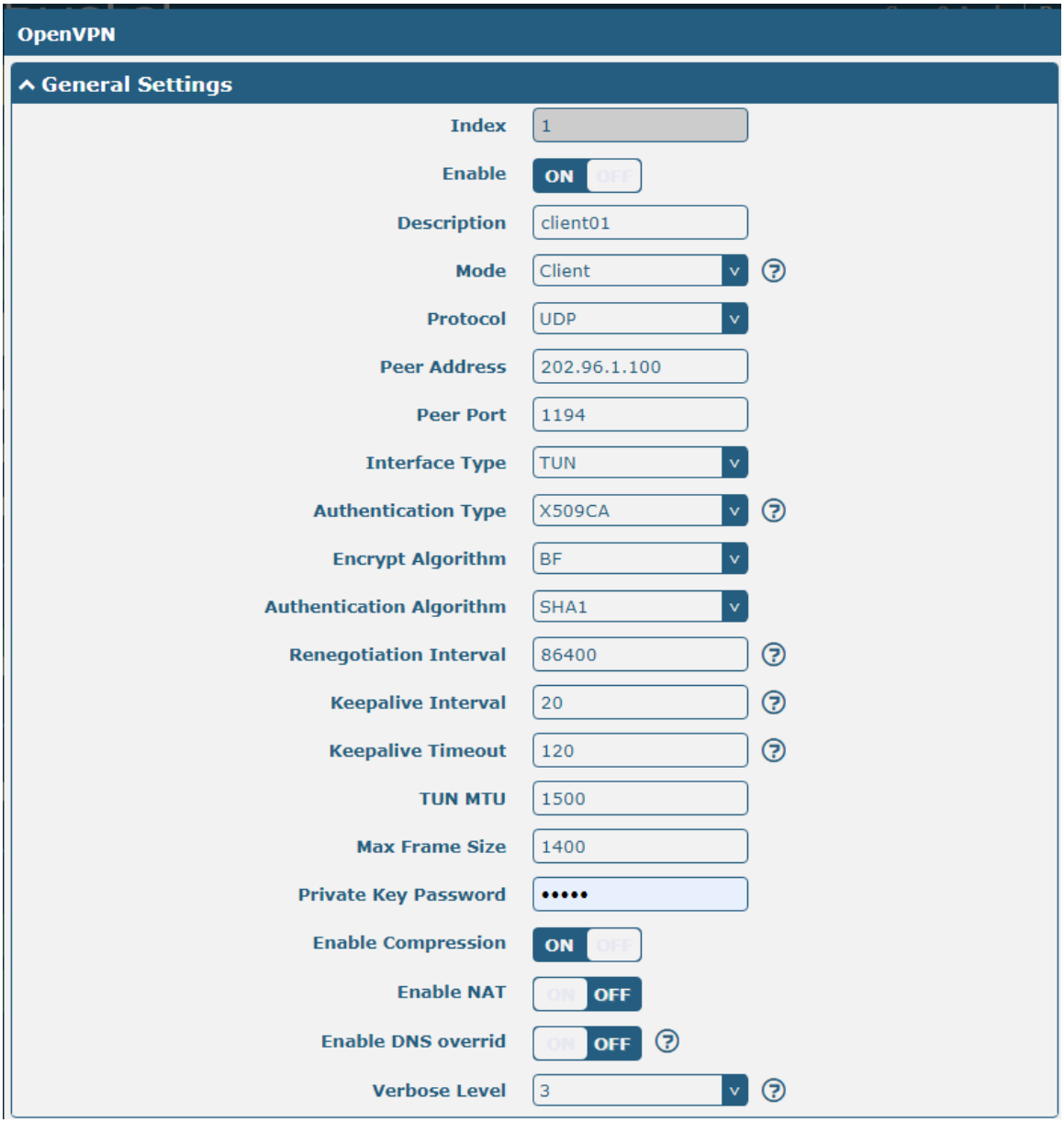
Примечание. Для получения дополнительных сведений о конфигурации обратитесь к инженеру службы

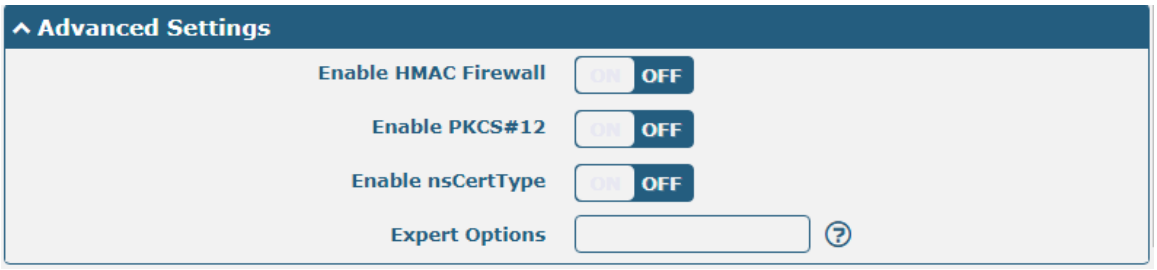
технической поддержки.

OpenVPN_Client:

Нажмите **на VPN> OpenVPN> OpenVPN в соответствии с рисунком** ниже**.**

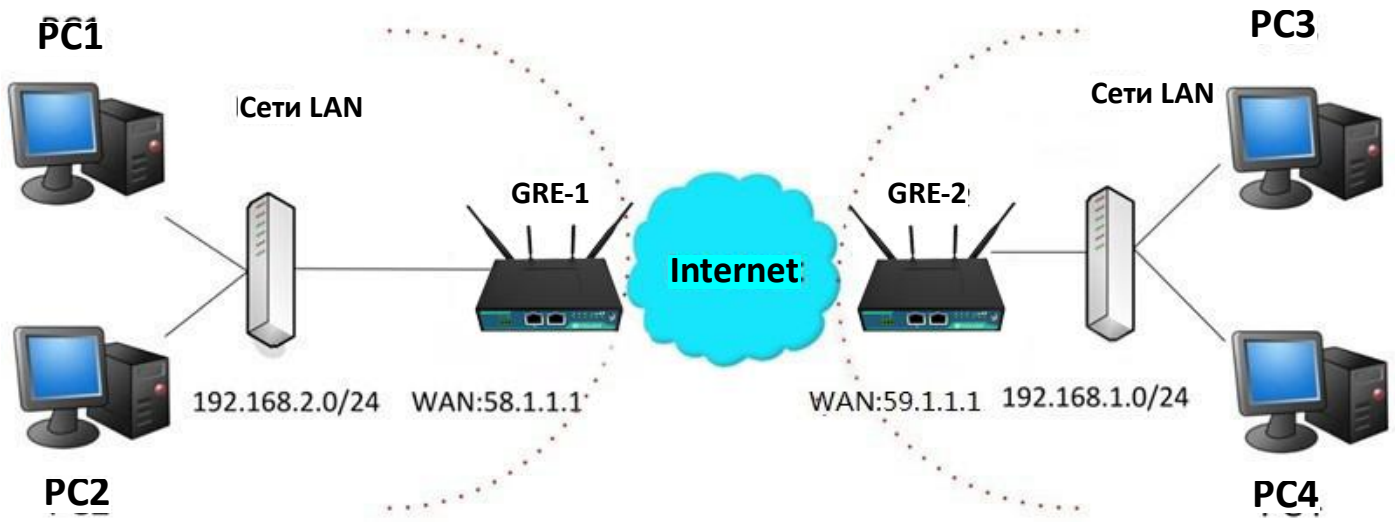
Нажмите на + для настройки клиента 01 в соответствии с рисунком ниже..





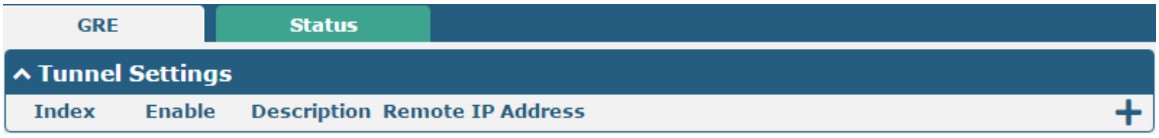
По завершении нажмите **Submit > Save & Apply**, чтобы конфигурация вступила в силу.

4.2.3 GRE VPN



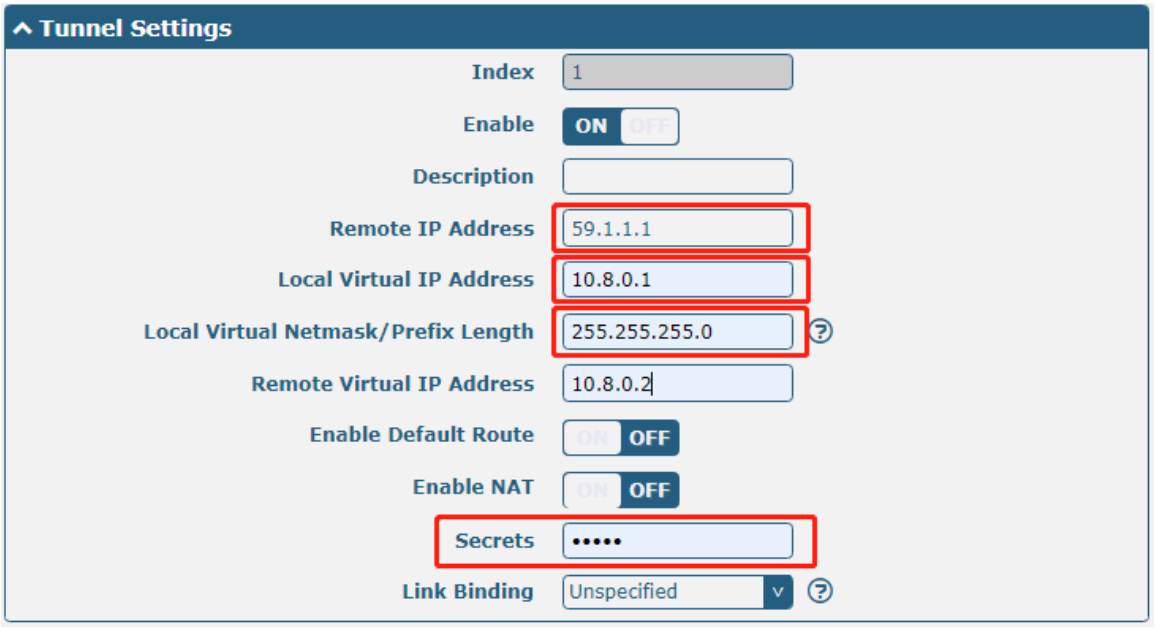
Конфигурация двух точек следующая.

При нажатии **VPN> GRE> GRE** окно отображается в соответствии с рисунком ниже.



GRE-1：

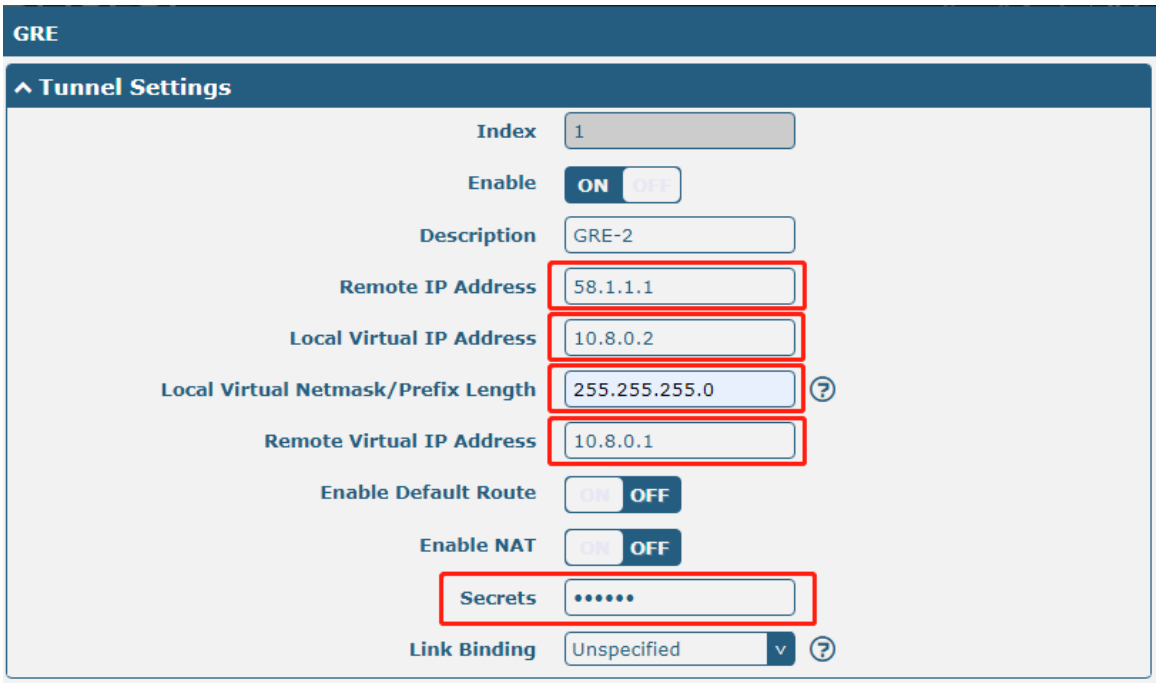
Нажмите кнопку + и установите параметры GRE-1 в соответствии с рисунком ниже.



По завершении нажмите **Submit > Save & Apply**, чтобы конфигурация вступила в силу.

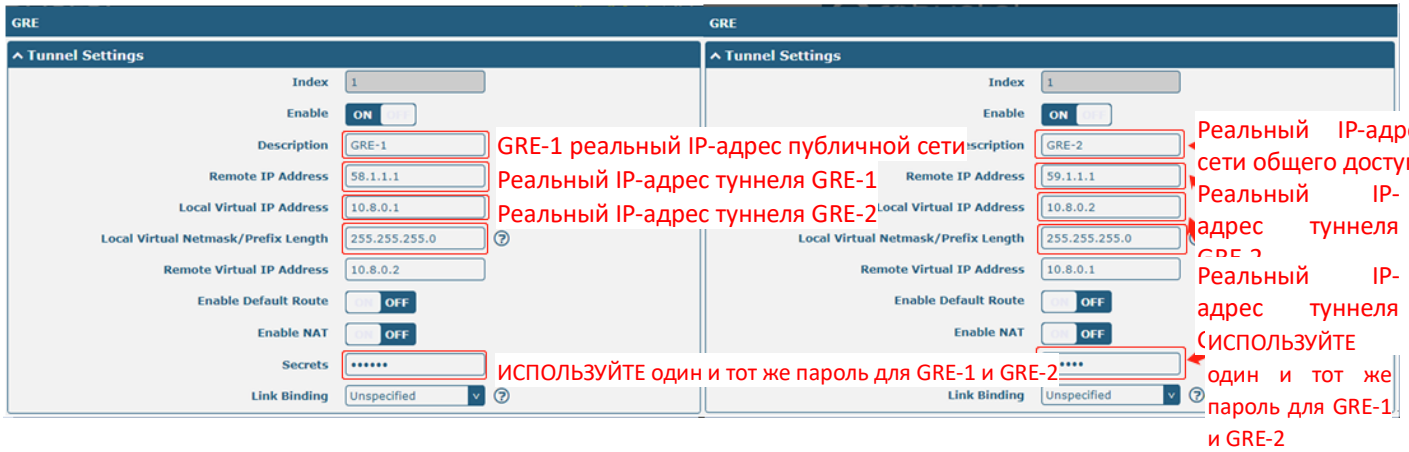
GRE-2:

Нажмите кнопку + и установите параметры GRE-1 в соответствии с рисунком ниже.



По завершении нажмите **Submit > Save & Apply**, чтобы конфигурация вступила в силу.

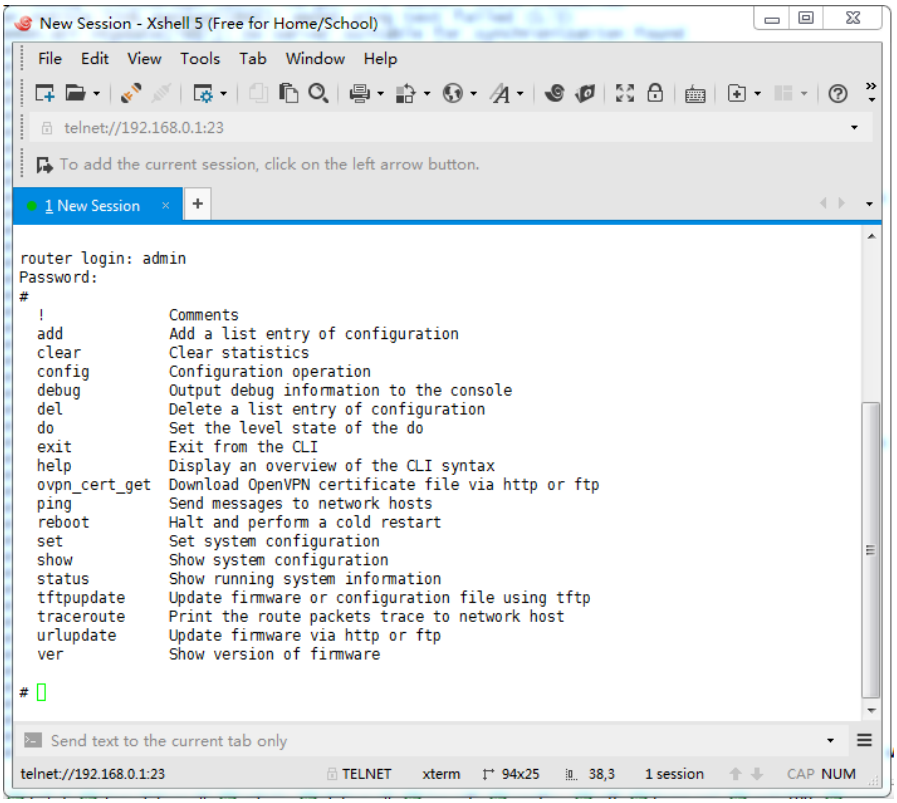
Сравнение GRE-1 и GRE-2 представлено ниже.



Глава 5 Введение в CLI

5.1 Что такое CLI

Интерфейс командной строки (CLI) – это программный интерфейс, обеспечивающий другой способ установки параметров оборудования через SSH или через сетевое соединение telnet.



Вход в систему:

Вход в систему: admin

Пароль: admin

#

Команды CLI:

? (**Примечание**. знак "?" не будет отображаться на странице.)

!	Комментарии
add	Добавить запись в список конфигурации
очистить	Очистить статистику
config	Операция настройки
отладка	Вывод отладочной информации на консоль
del	Удалить запись в списке конфигурации
exit	Выйти из CLI

help	Показать обзор синтаксиса интерфейса командной строки
ovpn_cert_get	Загрузить файл сертификата OpenVPN через http или ftp

ping	Отправить сообщения сетевым узлам
reboot	Остановить и выполнить холодный перезапуск
route	Статический маршрут изменяется динамически, этот параметр не сохраняется.
set	Установить конфигурацию системы
show	Показать конфигурацию системы
статус	Отображает информацию о работающей системе
tftpupdate	Обновить прошивку с помощью tftp
программа контроля прохождения сигнала по сети	Распечатать трассировку пакетов маршрута к сетевому узлу
urlupdate	Обновить прошивку через http или ftp
ver	Отображает версию прошивки

5.2 Как настроить интерфейс CLI

Ниже представлена таблица с описанием справки и ошибок, которые должны возникнуть в программе настройки.

Commands /tips	**Описание**
?	При вводе вопросительного знака «?» отобразится справочная информация. Например, # config（Нажать «?»） config Операция настройки # config（Нажмите пробел + «?»） commit Сохранить изменения конфигурации и применить измененную конфигурацию save_and_apply Сохранить изменения конфигурации и применить измененную конфигурацию Loaddefault Restore Factory Configuration
Ctrl+c	Нажмите эти две кнопки одновременно, за исключением функции «copy», это сочетание также можно использовать для «break» из программы настройки.
Syntax error: Команда не завершена	Команда не завершена.
Нажмите пробел + Tab	Это может помочь вам завершить вашу команду.

	Пример: # config (tick enter key) Syntax error: Команда не завершена # config (tick space key+ Tab key) commit save_and_apply loaddefault
#config commit # config save_and_apply	По завершении настройки необходимо ввести эти команды, чтобы настройки вступили в силу на устройстве. **Примечание:** Commit и save_and_apply играют одинаковую роль.

5.3 Команды

Commands	Syntax	Описание
Отладка	*Параметры* Debug	Включение или отключение функции отладки
Show	Show *parameters*	Отображает текущую конфигурацию каждой функции, если необходимо увидеть все, используйте «show running»
Set	Set *parameters*	Все параметры функции устанавливаются командами set и add, разница в том, что set – для одного параметра, а add – для параметра списка.
Add	Add *parameters*	

Примечание. Загрузите XML-файл конфигурации из настроенного веб-браузера. Формат команды может относиться к формату файла config.XML.

5.4 Быстрый старт с примерами конфигурации

Лучший и самый быстрый способ освоить интерфейс командной строки – сначала просмотреть все функции с веб-страницы, а затем прочитать все команды интерфейса за раз, наконец, научиться настраивать его с помощью некоторых справочных примеров.

Пример 1. Отобразить текущую версию

# status system
hardware_version = 1.0
firmware_version = "3.0.0"
kernel_version = 3.10.49
device_model = R2000
serial_number = 111111111
system_uptime = «0 days, 06:17:32»
system_time = «Thu Jul 6 17:28:51 2017»

Пример 2. Обновление прошивки через tftp

```
# tftpupdate (space+?)
    firmware New firmware
# tftpupdate firmware (space+?)
    String Firmware name
# tftpupdate firmware filename R2000-firmware-sysupgrade-unknown.bin host 192.168.100.99 //введите новое
имя прошивки
Скачивание
R2000-firmware-s 100% |*******************************|    5018k    0:00:00 ETA
Мерцание
Проверка 100 %
Расшифровка 100 %
Мерцание 100 %
Проверка 100 %
Проверка прошла успешно
   успех обновления                          //успех обновления
   # config save_and_apply
   OK                                        // сохранить и применить текущую конфигурацию, после этого ваши
                                             настройки конфигурации будут применены
```

Пример 3. Установить менеджер ссылок

```
# set
# set
 at_over_telnet          AT Over Telnet
 сотовый                 Сотовый
 ddns                    Dynamic DNS
 ethernet                Ethernet
 event                   Управление событием
 firewall                Firewall
 gre                     GRE
 ipsec                   ipsec
 сети lan                локальная сеть
 link_manager            Link Manager
 ntp                     NTP
 openvpn                 OpenVPN
 reboot                  Automatic Reboot
 RobustLink              RobustLink
 route                   Route
 sms                     SMS
 snmp                    Агент SNMP
 ssh                     SSH
 syslog                  Syslog
 system                  System
 user_management         User Management
 vrrp                    VRRP
 web_server              Web Server
```

```
# set link_manager
   primary_link              Primary Link
   backup_link               Backup Link
   backup_mode               Backup Mode
   emergency_reboot          Emergency Reboot
   link                      Link Settings
       # set link_manager primary_link (space+?)
Enum    Primary Link (wwan1/wwan2/wan)
  # set link_manager primary_link wwan1                    // выберете «wwan1» как primary_link
  OK                                                       //установка прошла успешно
# set link_manager link 1
 type                        Type
 desc                        Описание
 connection_type             Connection Type
 wwan                        WWAN Settings
 static_addr                 Static Address Settings
 pppoe                       Настройки PPPoE
 ping                        Настройки Ping
 mtu                         MTU
 dns1_overrided              Overrided Primary DNS
 dns2_overrided              Overrided Secondary DNS
# set link_manager link 1 type wwan1
OK
# set link_manager link 1 wwan
 auto_apn                    Automatic APN Selection
 apn                         APN
 username                    Username
 password                    Password
 dialup_number               Dialup Number
 auth_type                   Authentication Type
 aggressive_reset            Aggressive Reset
 switch_by_data_allowance    Switch SIM By Data Allowance
 data_allowance              Data Allowance
 billing_day                 Billing Day
# set link_manager link 1 wwan switch_by_data_allowance true
OK
#
  # set link_manager link 1 wwan data_allowance 100        // открыть сотовый switch_by_data_traffic
  OK                                                       //установка прошла успешно
  # set link_manager link 1 wwan billing_day 1             // настройка указывает день месяца для
                                                           выставления счета
  OK                                                       //установка прошла успешно
# config save_and_apply
  OK                          // сохранить и применить текущую конфигурацию, после этого ваши
                              настройки конфигурации будут применены
```

Пример 4. Настройка Ethernet

```
# set Ethernet port_setting 2 port_assignmEnt lan0          // Установка таблицы 2 (eth1) до значения lan0
OK
# config save_and_apply                                    //установка прошла успешно
OK
```

Пример 5: Установка IP-адрес LAN

```
# show lan all
network {
    id = 1
    interface = lan0
    ip = 192.168.0.1
    netmask = 255.255.255.0
    mtu = 1500
    dhcp {
        enable = true
        mode = server
        relay_server = ""
        pool_start = 192.168.0.2
        pool_end = 192.168.0.100
        netmask = 255.255.255.0
        gateway = ""
        primary_dns = ""
        secondary_dns = ""
        wins_server = ""
        lease_time = 120
        expert_options = ""
        debug_enable = false
    }
}
multi_ip {
    id = 1
    interface = lan0
    ip = 172.16.10.67
    netmask = 255.255.0.0
}
#
# set lan
 network          Network Settings
 multi_ip         Multiple IP Address Settings
```

```
 vlan                VLAN
# set lan network 1(space+?)
   interface          Interface
   ip                 IP Address
   netmask            Netmask
   mtu                MTU
   dhcp               DHCP Settings
# set lan network 1 interface lan0
OK
  # установить интерфейс локальной сети 1 IP        // установить IP-адрес для локальной сети
  172.16.10.67
  OK                                                //установка прошла успешно
# установить сетевую маску LAN 1 255.255.0.0
OK
#
…
# config save_and_apply
OK                                          // сохранить и применить текущую конфигурацию, после этого ваши настройки конфигурации будут применены
```

Пример 6: CLI для настройки сотовой связи

```
# show cellular all
sim {
    id = 1
    card = sim1
    phone_number = ""
    extra_at_cmd = ""
    network_type = auto
    band_select_type = all
    band_gsm_850 = false
    band_gsm_900 = false
    band_gsm_1800 = false
    band_gsm_1900 = false
    band_wcdma_850 = false
    band_wcdma_900 = false
    band_wcdma_1900 = false
    band_wcdma_2100 = false
    band_lte_800 = false
    band_lte_850 = false
    band_lte_900 = false
    band_lte_1800 = false
    band_lte_1900 = false
    band_lte_2100 = false
    band_lte_2600 = false
    band_lte_1700 = false
```

```
    band_lte_700 = false
    band_tdd_lte_2600 = false
    band_tdd_lte_1900 = false
    band_tdd_lte_2300 = false
    band_tdd_lte_2500 = false
}
sim {
    id = 2
    card = sim2
    phone_number = ""
    extra_at_cmd = ""
    network_type = auto
    band_select_type = all
    band_gsm_850 = false
    band_gsm_900 = false
    band_gsm_1800 = false
    band_gsm_1900 = false
    band_wcdma_850 = false
    band_wcdma_900 = false
    band_wcdma_1900 = false
    band_wcdma_2100 = false
    band_lte_800 = false
    band_lte_850 = false
    band_lte_900 = false
    band_lte_1800 = false
    band_lte_1900 = false
    band_lte_2100 = false
    band_lte_2600 = false
    band_lte_1700 = false
    band_lte_700 = false
    band_tdd_lte_2600 = false
    band_tdd_lte_1900 = false
    band_tdd_lte_2300 = false
    band_tdd_lte_2500 = false
}
# set(space+?)
  at_over_telnet     сотовый          ddns          dhcp          dns
  event              firewall         ipsec         сети lan      link_manager
  ntp                openvpn          reboot        route         serial_port
  sms                snmp             syslog        system        user_management
vrrp
# set cellular(space+?)
    Настройки sim SIM
# set cellular sim(space+?)
    Integer Index (1..2)
```

```
# set cellular sim 1(space+?)
    card                        SIM Card
    phone_number                Phone Number
    extra_at_cmd                Extra AT Cmd
    network_type                Network Type
    band_select_type            Band Select Type
    band_gsm_850                GSM 850
    band_gsm_900                GSM 900
    band_gsm_1800               GSM 1800
    band_gsm_1900               GSM 1900
    band_wcdma_850              WCDMA 850
    band_wcdma_900              WCDMA 900
    band_wcdma_1900             WCDMA 1900
    band_wcdma_2100             WCDMA 2100
    band_lte_800                LTE 800 (band 20)
    band_lte_850                LTE 850 (band 5)
  band_lte_900                  LTE 900 (band 8)
  band_lte_1800                 LTE 1800 (band 3)
  band_lte_1900                 LTE 1900 (band 2)
  band_lte_2100                 LTE 2100 (band 1)
  band_lte_2600                 LTE 2600 (band 7)
  band_lte_1700                 LTE 1700 (band 4)
  band_lte_700                  LTE 700 (band 17)
  band_tdd_lte_2600             TDD LTE 2600 (band 38)
  band_tdd_lte_1900             TDD LTE 1900 (band 39)
  band_tdd_lte_2300             TDD LTE 2300 (band 40)
  band_tdd_lte_2500             TDD LTE 2500 (band 41)
# set cellular sim 1 phone_number 18620435279
OK
…
# config save_and_apply
   OK                           // сохранить и применить текущую конфигурацию, после этого ваши
                                настройки конфигурации будут применены
```

Глоссарий

Сокращение	Описание
Пер. ток	Переменный ток
APN	Имя точки доступа
ASCII	Стандартный американский код обмена информацией
CE	Европейское соответствие
CHAP	Протокол аутентификации по квитированию вызова
CLI	Интерфейс командной строки для выполнения сценариев в пакетном режиме
CSD	Данные, передаваемые по коммутируемому каналу
CTS	Разрешение отправки
дБ	Децибел
дБи	Изотопный децибел
Пост. ток	Постоянный ток
DCD	Сигнал об активности и готовности модема к передаче
DCE	Оборудование передачи данных (обычно модемы)
DCS 1800	Система цифровой сотовой связи, также называемая PCN
DI	Цифровой вход
DO	Цифровой выход
DSR	Сигнал готовности (модема) к передаче данных
ООД	Оконечное оборудование данных
DTMF	Режим цифрового двухтонального многочастотного набора
DTR	Оконечное оборудование данных
EDGE	Повышенная скорость передачи данных для глобального развития стандарта GSM и IS-136
ЭМС	Электромагнитная совместимость
EMI	Электромагнитные помехи
ESD	Электростатический разряд
ETSI	Европейский институт стандартизации в области телекоммуникации
EVDO	Технология усовершенствованной передачи данных с использованием адаптивной модуляции, позволившей увеличить пропускную способность канала, используемая в сетях сотовой связи стандарта CDMA.
FDD LTE	Дуплекс с частотным разделением каналов Стандарт «Долгосрочное развитие сетей связи»
GND	Заземление
GPRS	Система пакетной радиосвязи общего пользования
GRE	Общая инкапсуляция маршрутов
GSM	Глобальная система мобильной связи
HSPA	Технология высокоскоростной пакетной передачи данных
ID	идентификационные данные
IMEI	Международный идентификатор оборудования мобильной связи

Сокращение	Описание
IP	Протокол Интернет
ipsec	Безопасность интернет-протокола
кбит/с	килобит в секунду
L2TP	Протокол туннелирования второго уровня
Сети LAN	локальная сеть
LED	Светодиод
M2M	Межмашинное взаимодействие
MAX	Максимальное значение
Мин.	Минимальное значение
MO	Инициируемый мобильными абонентами
MS	Станция мобильной связи
MT	Мобильный получатель сообщения
OpenVPN	Открытая виртуальная частная сеть
PAP	Протокол аутентификации по паролю
ПК	Персональный компьютер
PCN	Сеть персональной связи, также называемая DCS 1800
PCS	Система персональной связи, также называемая GSM 1900
PDU	Модуль данных протокола
PIN	Персональный идентификационный номер
PLCs	Система управления логикой работы программы
PPP	Двухточечный протокол
PPTP	Протокол установления сквозного соединения «точка-точка»
БП	Блок питания
PUK	Личный код разблокировки
R&TTE	Радио- и телекоммуникационное оконечное оборудование
РЧ	Радиочастота
RTC	Часы реального времени
RTS	Разрешение отправки
RTU	Дистанционный терминал
Rx	Направление приема
SDK	Набор инструментальных средств разработки программного обеспечения
SIM	Модуль идентификации абонента
SMA antenna	Короткая штыревая или магнитная антенна
SMS	Служба коротких сообщений
SNMP	Простой протокол управления сетью
TCP/IP	Протокол управления передачей/межсетевой протокол
ОД	Оконечное оборудование, также называемое ООД
Tx	Направление передачи
UART	Универсальный асинхронный приемопередатчик
UMTS	Универсальная система мобильной связи
USB	Универсальная последовательная шина

Сокращение	Описание
USSD	Неструктурированные дополнительные служебные данные
В пост. тока	Напряжение постоянного тока в вольтах
VLAN	Виртуальная локальная компьютерная сеть
VPN	Виртуальная частная сеть
VSWR	Коэффициент стоячей волны по напряжению
WAN	Глобальная сеть