Абонентский терминал GPON RV6688

Руководство по эксплуатации

GPON ONT RV6688

1. Обзор

Содержание комплекта

В комплект поставки абонентского терминала GPON RV6688 входят следующие компоненты:

– Терминал GPON RV6688;
– Адаптер питания AC\DC;
– Руководство по эксплуатации;
– Кабельный органайзер.

Индикация устройства

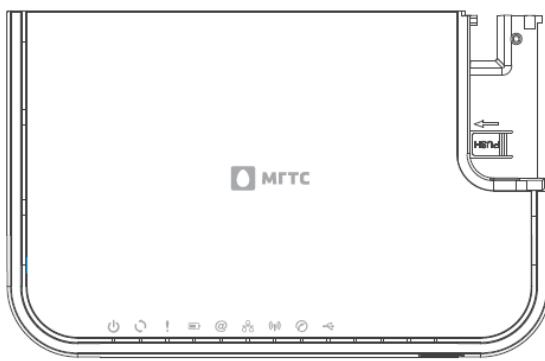


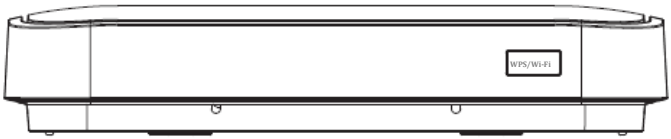
Рис.1: Индикация RV6688.

Значения LED индикаторов устройства:

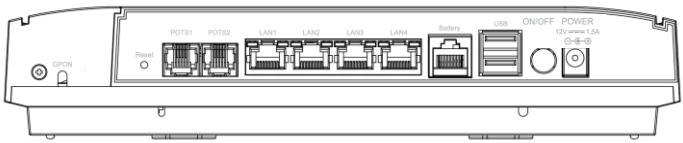
 **Power\Питание (Зеленый)**	**On** – питание Вкл. **Off** – питание Выкл.
 **GPON (Зеленый)**	**On –** ONT (Optical Network Terminal) успешная регистрация. **Off –** регистрация отсутствует. **Flashing** (мигает один раз в секунду) - ONT процесс регистрации. **Fast Flashing** (быстрое мигание 4 раза в секунду) **–** обновление ПО.
 LOS **(Красный)**	**Off –** оптический кабель подключен. **On –** оптический кабель отключен либо поврежден.
 **Battery (Красный)**	**On –** источник бесперебойного питания (ИБП) в нормальном состоянии. **Off –** ИБП отключен. **Slow Flashing –** низкий заряд ИБП.
 **Internet (Зеленый)**	**On –** соединение устройства с сетью Интернет установлено. **Off –** соединение с сетью Интернет отсутствует. **Flashing –** индикатор передачи данных.
 **LAN (Зеленый)**	**On** –активность LAN портов. **Off** – отсутствие активности на LAN портах. **Flashing** (мигает**)** – прием\передача трафика на LAN портах.

 **WiFi/WPS (Зеленый/ Голубой)**	**ON** (зелёный) - Wi-Fi-сеть включена. **Flashing** (зелёный) - передача данных по Wi-Fi-сети. **Flashing** (голубой) - функция WPS активирована для подключения устройств. **Fast Flashing** (голубой) - при регистрации устройства по WPS возникла ошибка. **Off** – Wi-Fi-сеть отключена.
 **Phone (Зеленый)**	**On –** подключение к Soft Switch выполнено успешно. **Off –** подключение к Soft Switch не выполнено. **Flashing** (мигает один раз в секунду) – телефонная линия используется. **Fast Flashing** (быстрое мигание 4 раза в секунду) – осуществляется телефонный разговор.
 **USB (Зеленый)**	**On –** USB порт используется. **Off –** USB порт не используется. **Flashing –** осуществляется передача данных с использованием USB порта.

Лицевая панель устройства



Задняя панель устройства



Назначение разъемов на задней панели RV6688

GPON	Порт для подключения оптоволоконного кабеля.
Порты LAN1…LAN4	Используйте стандартные Ethernet кабели (с разъемами RJ45) для подключения ПК к этим портам
Порты POTS1…POTS2	Используйте телефонный кабель (с разъемами RJ11) для подключения аналогового телефона к этим портам.

Порт мониторинга статуса источника бесперебойного питания «Battery»	Разъем для подключения кабеля мониторинга резервного источника питания (тип разъема RJ-45). ✓ Не следует использовать данный разъем для подключения стационарного ПК.
Разъем POWER	Разъем для подключения адаптера питания
Переключатель «ON/OFF»	Нажмите для включения или выключения устройства
RESET	Перезагрузка устройства (кратковременное нажатие). Сброс конфигурации к заводским настройкам (держать нажатой 5 секунд).

2. Установка

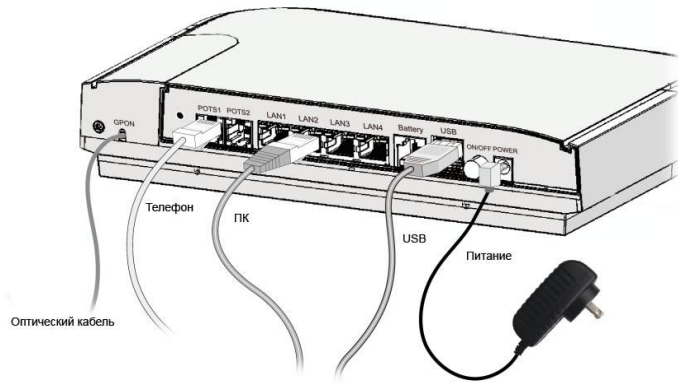


Рис.2: Установка RV6688.

Выберите подходящее место для установки RV6688;
Подключите порт GPON к оптоволоконной широкополосной сети;
Подключите Ethernet кабели к разъему сетевого интерфейса компьютера или маршрутизатора;
Подключите адаптер питания, поставляемый в комплекте с устройством RV6688 к розетке питания, затем нажмите переключатель Power;

Проверьте индикацию устройства Индикатор **POWER** должен быть **включен** Индикатор **GPON** должен быть **включен** Индикатор **LAN** должен быть **включен.**

Настенный монтаж

На Рис.3 показаны крепления для монтажа устройства на стену (с использованием кабельного органайзера). Крепление осуществляется с использованием специальных отверстий на нижней части корпуса устройства.

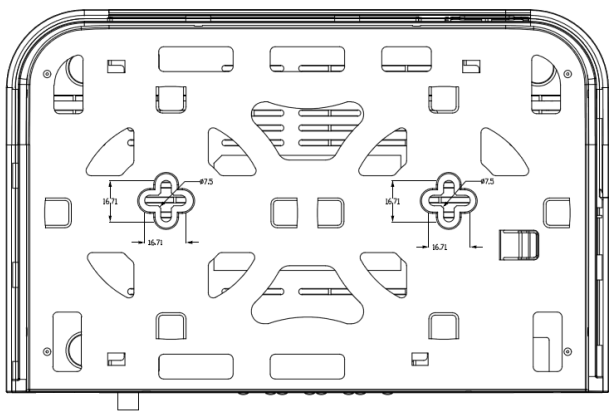


Рис.3: Настенный монтаж RV6688.

3. Настройка

1. Запустите Web-браузер. В адресной строке браузера введите **http://192.168.1.254**
2. В появившемся диалоговом окне введите имя пользователя:

Username: **admin**
Password: **admin**

3. После аутентификации вы перейдете на заглавную страницу конфигурации и статуса - «Информация». Теперь Вы можете приступить к настройке ONT RV6688 с помощью WEB браузера.

Рис.4: Настройка RV6688.

Для настройки устройства абоненту доступны следующие вкладки:
-Локальная сеть (LAN);
-Беспроводная сеть;
-Функции маршрутизации (NAT);
-Динамическое обновление доменного имени DDNS;
- Настройка USB порта.

Конфигурация LAN

Воспользуйтесь вкладкой LAN в главном меню, чтобы перейти на страницу конфигурации LAN, пример экрана показан ниже.
В выпадающем списке вы можете выбрать любую из четырех подсетей, в разделе TCP\IP показывается ее IP адрес и маска подсети. Если сеть отключена вы увидите SubnetX.

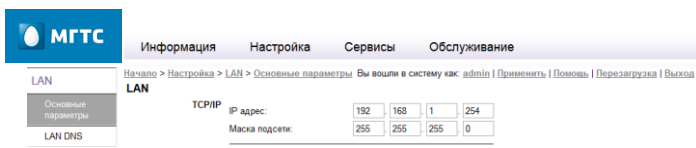


Рис.5: Конфигурация LAN.

В некоторых версиях ПО локальный доступ на WEB интерфейс устройства может быть ограничен, для изменения настроек оборудования вы можете обратиться в контактный центр по телефону 8 495 636-0-636.

TCP/IP	
Настройки	Для включения сети LAN: • Выберите LAN сеть: Выберите новую подсеть или Enabled Network; • Включите эту сеть «LAN сеть Включить» если это необходимо; • IP-адрес: введите IP-адрес маршрутизатора или шлюза по умолчанию, например: 192.168.1.254; • Маска подсети: Маска подсети определяет сетевую часть IP-адреса. Ваш маршрутизатор автоматически вычисляет маску подсети на основе IP-адрес, который вы назначаете. Рекомендуется использовать 255.255.255.0 в качестве маски подсети.

DHCP	
Настройки	Локальный сервер Dynamic Host Configuration Protocol (DHCP) автоматически выделяет и контролирует распределение IP адресов для всех хостов в сети. • **DHCP начальн.IP адрес**: это значение начального IP адреса из пула выделенных. • **DHCP начальн.IP адрес**: это значение конечного IP адреса из пула выделенных. • **Время аренды адреса DHCP:** Время аренды DHCP это промежуток времени, в течении которого сетевые устройства будут иметь возможность подключиться к шлюзу с текущим динамическим IP-адресом. Введите желаемое кол-во (минут) для указания значения «аренды». После того, как время истекло, устройство будет автоматически присвоен новый динамический IP-адрес. Значение по умолчанию составляет 1 день.

Резервирование адресов (Address Reservation)	
Резервирование адресов	С помощью резервирования вы можете указать IP-адрес и зарезервировать его для ПК в локальной сети, тогда компьютер будет получать один и тот же IP адрес от DHCP сервера. •Нажмите кнопку « Добавить». •Установите курсор на компьютер\хост, для которого вы хотите сделать резервацию и добавьте его в таблицу резервирования: «Таблица зарезервированных адресов». •Если компьютер не находится в таблице зарезервированных адресов, введите IP адрес, MAC адрес или имя для устройства, которое вы хотите добавить. •Нажмите кнопку «Сохранить», когда закончите.
Изменить	• Установите курсор рядом с зарезервированным адресом, который вы хотите изменить. Нажмите кнопку «Изменить». • Измените параметры: IP адрес, MAC адрес или Устройство. • Нажмите кнопку «Сохранить».
Удалить	• Установите курсор рядом с зарезервированным адресом, который вы хотите удалить. • Нажмите кнопку «Удалить «.

Конфигурация беспроводной сети

Используйте вкладку «Беспроводная сеть» в основном меню конфигуратора чтобы произвести настройку функции. Пример меню конфигурации беспроводной сети приведен ниже.

Вкладка настроек беспроводной сети позволяет произвести настройку параметров беспроводной сети. RV6688 поддерживает работу до четырех беспроводных сетей одновременно (4xSSID). Основная функциональность беспроводной сети по умолчанию включена на устройстве.

Для настройки беспроводной сети доступны следующие меню:

-Основные параметры;

-Безопасность;

-Настройка автоматического защищенного соединения - WPS (Wi-Fi Protected Setup);

-Ограничения доступа к беспроводной сети (Фильтрация по MAC).

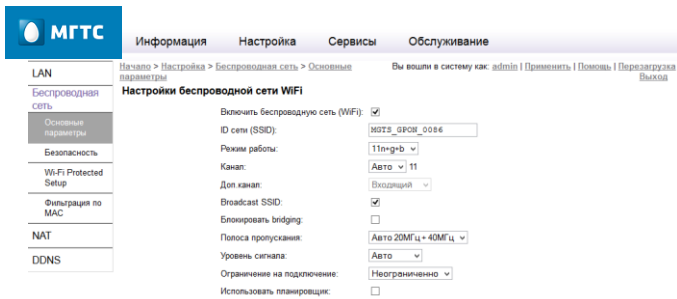


Рис. 6: Меню конфигурации Беспроводная сеть.

Основная конфигурация (Basic Setup)

802.11 Wireless Settings	
Включить беспроводную сеть (WiFi)	Если снять этот флажок для основной и гостевых беспроводных сетей функциональность беспроводной сети будет отключена (устройство не будет предоставлять или распространять любые услуги беспроводной локальной сети).
ID сети (SSID)	SSID является эквивалентом имени беспроводной сети. Вы можете оставить значение SSID по умолчанию или изменить его имя в свободной форме (до 32 символов). Примечание: Значение SSID вводится с использованием латинских букв и цифр.
Режим работы	Выпадающее меню позволяет выбрать и задать значение шлюза в режиме беспроводной передачи. Для совместимости с клиентами, использующими 802.11b (до 11 Мбит передачи), 802.11b + g (до 20 + Mbps) и 802.11n (до 300 Mbps), 11b + g + n используется по умолчанию.
Канал	Выберите канал который вы будете использовать. Если установлено значение «Auto», система будет сканировать и устанавливать наилучший канал. Примечание: Настройка беспроводного канала является глобальной для основной и гостевых Wi-Fi-сетей.

Доп. канал:	В режиме 802.11n при установке автовыбора канала (используется канал 20 МГц + 40 МГц) можно произвести автоматический выбор расширения канала, чтобы получить более «чистый» канал. • Если используются каналы 1 ~ 4, расширение каналов допускается в сторону увеличения. • Если используются каналы 5 ~ 9, расширение каналов допускается как в сторону увеличения так и уменьшения. • Если используются каналы 10 ~ 13, расширение каналов допускается в сторону уменьшения.
Broadcast SSID	Эта опция может сделать беспроводную сеть практически невидимой. Отключив трансляцию SSID, сеть не будет видна при «сканировании».
Блокировать Bridging	Установите флажок, чтобы блокировать возможность общения «беспроводных клиентов» между собой.
Полоса пропускания	Вы можете выбрать канал пропускной способности вручную для соединения 802.11n. • Если произведена настройка и установлено значение в 20 МГц, используется только канал 20 МГц. • Если произведена настройка и установлено значение в 20 МГц, 40 МГц + авто, при подключениях 802.11n будут использовать 40 МГц канала, но 802.11b и 802.11g будут по-прежнему использовать канал в 20 МГц .
Уровень сигнала	Выберите предпочитаемый уровень сигнала.

Ограничение на подключение	Вы можете настроить разрешение на использование беспроводной сети для определенного кол-ва пользователей. Если выбрать от 1 до 6, то только 1 ~ 6 беспроводных клиентов могут подключаться к SSID одновременно. Есть возможность выбрать безлимитное кол-во пользователей.
Использовать планировщик	Если вы включите эту опцию можно настроить гибкое расписание использования беспроводной сети.
Гостевая (виртуальная) точка доступа	
Настройки	• Установите флажок «Включено», чтобы включить гостевую SSID. • Гостевая SSID должна отличаться от основного SSID и остальных гостевых SSID. • Установите флажок «Скрыть», чтобы ваша гостевая беспроводная сеть стала невидимой.

Меню конфигурации Безопасность

Это меню конфигуратора позволяет управлять настройками security/encryption для обеспечения максимальной степени безопасности.

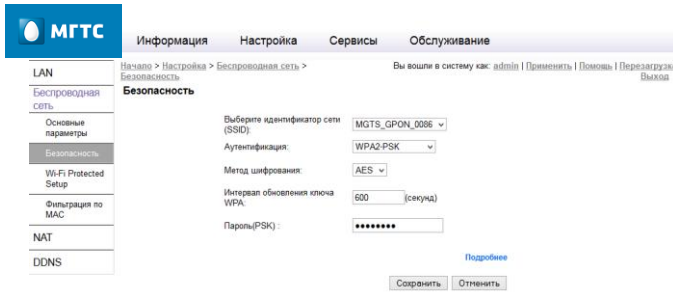


Рис. 7: Меню конфигурации Безопасность для беспроводной сети.

Выберите идентификатор SSID для настройки уровня и параметров сетевой безопасности беспроводной сети. Поддерживаются следующие режимы беспроводной сети:

Disabled: в этом режиме шифрование отключено.

WEP-64: Этот режим безопасности в соответствии с рекомендацией IEEE 802.11 и имеет более слабую степень защиты по сравнению с другими типами защиты (например WEP), например WPA2-PSK.

WEP-128: Это аналогичный WEP-64 алгоритм шифрования, однако имеет более длинный ключ.

Безопасность	
Настройки	• Passphrase: Если вы хотите создать несколько WEP ключей, используйте контрольную фразу (пароль сети) и введите их в соответствующие поля, затем нажмите кнопку «Создать ключ\Generate Key». • Keys 1-4: Вы можете ввести WEP ключи вручную. Каждый WEP ключ может состоять из букв от «A» до «F» и цифры «0» до «9». Длина ключа должна быть не менее 10 символов для 64-битных WEP или до 26 символов длиной при использовании 128 бит WEP. WPA-PSK: Wireless Protected Access обеспечивает беспроводной защищенный доступ с использованием шифрования TKIP. WPA2-PSK: Wireless Protected Access 2 обеспечивает беспроводной защищенный доступ с использованием шифрования AES. WPA/WPA2-PSK: рекомендуется как самый безопасный вариант защиты беспроводного подключения. •Password (PSK): Все клиенты должны использовать один и тот же PSK. Ключ может иметь длину от 8 до 63 символов или 64 Hex символа (0-F), ключ сети чувствителен к регистру вводимых символов. • WPA Group Rekey Interval: указывает устройству, как часто необходимо менять ключи шифрования.

Авто настройка безопасности: Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) это функция, которая позволяет с легкостью настроить беспроводную сеть. Если у вас есть устройства, поддерживающие Wi-Fi Protected Setup, следуйте приведенным ниже инструкциям. Если у вас есть клиентские устройства, такие как беспроводной адаптер с функцией WPS, то вы можете выполнить настройки беспроводной безопасности автоматически. Для включения функции WPS* необходимо нажать и удерживать кнопку «WPS/Wi-Fi» в течении 3 секунд. Для отключения Wi-Fi-сети необходимо нажать и удерживать кнопку «WPS/Wi-Fi» 7 секунд. Повторное включение Wi-Fi-сети осуществляется нажатием и удержанием кнопки «WPS/Wi-Fi» в течении 7 секунд. Также, управление функционалом WPS и Wi-Fi-сети доступно через WEB-интерфейс пользователя.

***Wi-Fi Protected Setup настраивает одного клиента устройств в один момент времени.**

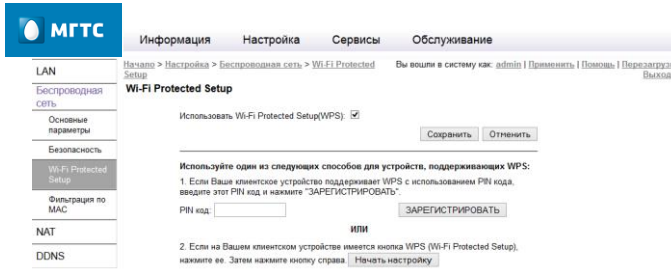


Рис. 8: Конфигурация Wi-Fi Protected Setup.

Конфигурация Wi-Fi Protected Setup

802.11 Wireless Settings	
Настройки	• PIN-метод: 1. Введите PIN-код клиентского устройства и нажмите кнопку «Зарегистрировать». 2. Затем запустите WPS на клиентском устройстве (с помощью утилиты настройки или в режиме конфигурации устройства), в течение 2 минут произойдет регистрация устройствами и между ними будет установлено соединение. • PBC метод: Используйте этот метод, если ваше клиентское устройство имеет кнопку Wi-Fi Protected Setup. 1. Нажмите кнопку «Пуск PBC **\Start PBC»** кнопку на экране. 2. Нажмите кнопку Wi-Fi Protected Setup на клиентском устройстве.

Фильтрация по MAC

Это окно позволяет вам указать, какие клиентские компьютеры могут иметь доступ к беспроводной локальной сети по конкретным MAC-адресам или быть заблокированными.

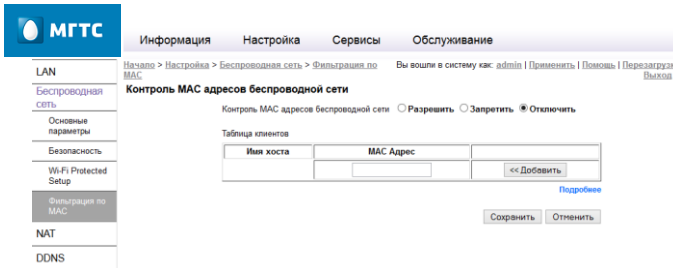


Рис. 9: Конфигурация MAC Filter.

Конфигурация фильтрации по MAC	
Настройка	• Есть три режима для управления доступом к ресурсам беспроводной сети на основе MAC-адресов: 1. Выберите «Разрешить» режим, чтобы перечисленные компьютеры, получили доступ к беспроводной сети. 2. Выберите «Запретить», чтобы заблокировать компьютерам из списка доступ к беспроводной сети. 3. Выберите «Отключить», чтобы отключить функцию управления доступом к Wireless на основе MAC. • Настройка беспроводного доступа клиента: 1. Выберите режим контроля беспроводного доступа на основе контроля MAC-адресов, установите: разрешить или запретить. 2. Введите MAC-адрес компьютера, доступ которого вы хотите разрешить или запретить. 3. Нажмите кнопку «Применить». Примечание: Вы можете добавить не более 32 записей MAC адресов.

Настройка маршрутизации NAT

Для доступа к настройкам ***NAT*** используйте ссылку в левом меню.

NAT позволяет настроить внешние сервисы в вашей сети, такие как веб-серверы, FTP-серверы, почтовые серверы или другие специализированные Интернет-приложения.

Note!

Перед использованием перенаправления рекомендуется назначить статический IP-адрес на выбранном ПК.

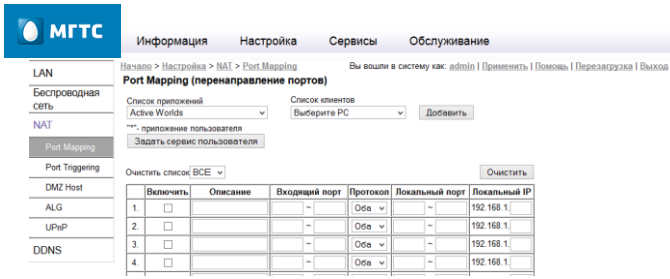


Рис. 10: Конфигурация Application Support.

Конфигурация Port Mapping

Port Maping	
Настройки	Настройка виртуального сервера для выбранного приложения : 1. Выберите приложение в предопределенном списке «Список приложений», если Вашего приложения нет в списке, Вы можете настроить его сами, нажав на кнопку «Задать сервис пользователя». 2. Выберите LAN хост из списка «Список клиентов», если Вы еще не включили Ваш сервер в LAN сеть, Вы можете вручную ввести последний октет IP адреса, которой вы хотите зарезервировать для этого сервера. 3. Нажмите кнопку «Добавить», после этого Вы сможете увидеть

	добавленную группу записей в таблице. 4. Нажмите «Сохранить» чтобы сохранить изменения. **5.** Нажмите «Применить» чтобы применить изменения.
Очистить	Для удаления записи: 1. Выберите «Очистить список» и отметьте номер записи. 2. Нажмите кнопку «Очистить». 3. Нажмите «Сохранить» чтобы сохранить изменения. 4. Нажмите «Применить» чтобы применить изменения.

Настройки - Port Triggering

Для доступа к настройкам ***Port Triggering*** используйте ссылку в левом меню.
Эта функция предназначена для интернет-приложений, которые обычно не могут работать через встроенный брандмауэр. Если интернет-приложение не работает, вы можете попробовать использовать Port Triggering. Вам нужна подробная информация о программе от поставщика услуг или приложений. Обратите внимание, что термины «Входящие порты» и «Порты триггеры» , относятся к трафику от клиента (ПК).
Работает это следующим образом:

1. Когда исходящий трафик с компьютера используется порт, который определен как порт перенаправления, маршрутизатор запоминает компьютер и порт приложения.

2. Когда входящее соединение, которое использует полученный входящий порт для этого приложения, то трафик направляется к компьютеру. (Без этой записи, входящий трафик будет отброшен.)

Ограничения:

- Только 1 ПК может использовать Port Triggering в одно и то же время. После каждого использования, имеется тайм-аут перед тем как этот порт сможет использовать другое приложение.
- Каждая запись для порта должна использовать уникальный номер порта. Вы не можете включить два приложения используя один и тот же порт.
- Функция Port Triggering работает с исходящим трафиком. Поэтому она не будет работать с любым из входящих соединений. (Виртуальный сервер и DMZ должны использоваться, чтобы определить входящие соединения).

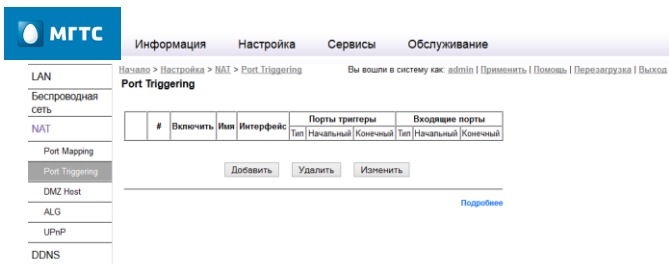


Рис.11: Конфигурация Port Triggering.

Конфигурация Port Triggering

Application Support	
Включить	Отметьте, чтобы включить или отключить запуск портов приложений по мере необходимости.
Имя	Наименование для этого порта запуска приложений.
Интерфейс	Выберите нужный интерфейс.
Порты триггеры	• Тип - Выберите протокол (TCP или UDP), используемый при получении данных из специального приложения или службы. (Примечание: Некоторые приложения используют различные протоколы для входящих и исходящих данных). • Начальный - Введите начало диапазона портов, используемых сервером приложений, для принимаемых данных. Если приложение использует один порт, введите его в оба поля « Начальный» и « Конечный». • Конечный - Введите конечный порт диапазона, используемых сервером приложений, для принимаемых данных.
Входящие порты	• Тип - Выберите протокол (TCP или UDP), используемый при передаче данных на удаленной системе или услуге. • Начальный - Введите начало диапазона портов, используемых сервером приложений, для отправляемых Вами данных. Если приложение использует один порт, введите его в оба поля « Начальный» и « Конечный».

	• Конечный - Введите конечный порт диапазона, используемых сервером приложений, для отправляемых Вами данных. Если приложение использует один порт, введите его в оба поля «Начальный» и « Конечный».

Настройка DMZ Host

DMZ (demilitarized zone) демилитаризованная зона - технология обеспечения защиты информационного периметра, при которой серверы, отвечающие на запросы из внешней сети, находятся в особом сегменте сети (который и называется ДМЗ) и ограничены в доступе к основным сегментам сети с помощью межсетевого экрана, соответственно DMZ Host – ПК, находящийся внутри DMZ или имеющий к ней подключение.

Для доступа к настройкам ***DMZ*** используйте ссылку в левом меню.

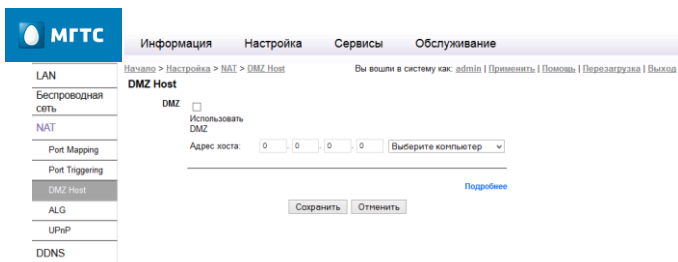


Рис.12: Меню конфигурации DMZ Host.

Настройка DMZ

Эта функция, если она включена, позволяет всем пользователям сети Интернет получить доступ к компьютеру DMZ в вашей локальной сети.

- Это позволяет практически использовать любое приложение, которые будут работать на «DMZ ПК».
- «DMZ ПК» получает все данные и устанавливает соединения как «Неизвестные».
- Если функция DMZ включена, вы должны ввести IP-адрес компьютера или выберите нужный компьютер в списке, который будет использоваться как «DMZ ПК».

Если «DMZ ПК» находится фактически за пределами межсетевого экрана, это делает его более уязвимым для атак. По этой причине, вы должны включать функцию DMZ только в случае необходимости.

Настройка ALG

ALG (Application-level gateway) - *шлюз прикладного уровня* - компонент NAT-технологии, который понимает трафик прикладного приложения пользователя (или протокол), и при прохождении через него пакетов этого приложения модифицирует их таким образом, что бы находящиеся за NAT пользователи могли пользоваться трафиком приложения.

Для доступа к настройкам ***ALG*** используйте ссылку в левом меню.

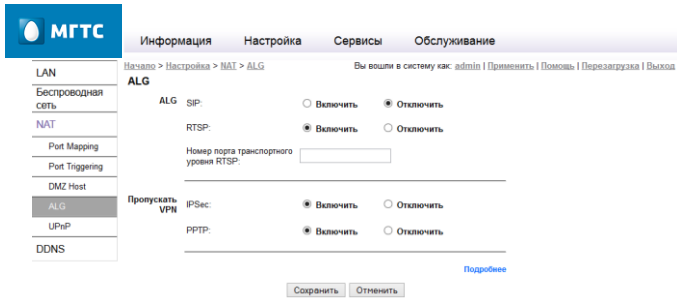


Рис. 13: Конфигурация ALG Host.

Конфигурация ALG

ALG	
SIP	SIP ALG отключен по умолчанию.
RTSP	Протокол потока в реальном времени (RTSP) – это сетевой управляемый протокол разработанный для использования в сфере развлечений и коммуникаций для контроля потоковых медиа-серверов. Он включен по умолчанию.
Номер порта транспортного уровня RTSP	Для некоторых провайдеров необходимо изменить порт видео сервера, по умолчанию порт 554, можно указать дополнительные 7 портов через запятую, как порт RTSP по умолчанию.
Пропускать VPN	
IPSec	Internet Protocol Security (IPSec) представляет собой набор протоколов, используемых для осуществления безопасного обмена пакетами на IP уровне. IPSec Pass-Through включен по умолчанию.
PPTP	Point-Point Tunneling Protocol (PPTP)

	позволяет использовать Point-Point Protocol (PPP) для туннелирования через IP-сеть. PPTP Pass-Through включен по умолчанию.

Настройки UPnP

UPnP (Universal Plug and Play) - набор сетевых протоколов, публикуемых форумом UPnP. Технология UPnP позволяет автоматически настраивать сетевые и периферийные устройства в домашней и корпоративной сети.

Для доступа к настройкам ***UPnP*** используйте ссылку в левом меню.

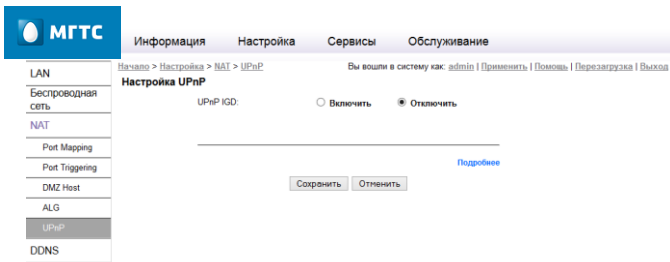


Рис. 14: Конфигурация UPnP.

Конфигурация UPnP

UPnP Настройки	
UPnP IGD	Функция UPnP позволяет Вашему ПК автоматически настроить маршруты для различных интернет приложений, таких как онлайн игры и видеоконференции. Данная функция по умолчанию отключена.
Настраиваемый	Выберите Disable, если Вы не хотите,

	иметь возможность запрещать любые интернет-соединений.
NAT Traversal	Выберите Disable, если Вы не хотите, иметь возможность вносить изменения вручную в маршруты, используя UPnP.
Таблица NAT Traversal	Нажмите эту кнопку если Вы хотите увидеть детальную информацию по таблице маршрутов.

Настройка DDNS

Для доступа к настройкам ***DDNS*** используйте ссылку в левом меню.

Многие интернет соединения используют «Dynamic IP address», где интернет IP адрес выделяется, когда интернет-соединение устанавливается.

Это означает, что другие пользователи интернета не знают этот IP-адрес, поэтому не могут установить соединение.

DDNS решает эту проблему следующим образом:

- Необходимо оформить подписку на услугу DDNS у поставщика услуг DDNS. Поставщик службы DDNS выделит доменное имя Вам по запросу.
- DDNS настройки, должны быть правильными.
- RV6688 свяжется с сервером DDNS, когда он определит, что интернет IP адрес изменился, и проинформирует сервер DDNS о новом IP адресе.

Эта система позволяет другим пользователям сети Интернет к вам подключиться, используя доменное имя, выделенное поставщиком услуг DDNS.

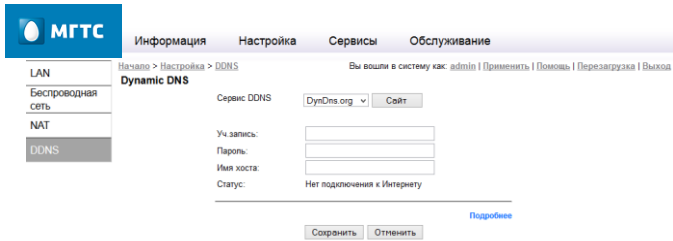


Рис.15: Конфигурация DDNS.

Конфигурация DDNS

Dynamic DNS	
Сервис DDNS	Выберите поставщика услуг из списка. • None • DynDns • Уч.запись: Введите имя пользователя для учетной записи DDNS. • Пароль: Введите пароль для учетной записи DDNS. • Имя хоста: Введите имя хоста для учетной записи DDNS. • TZO • Адрес Email: Введите адрес электронной почты для учетной записи. • Пароль TZO: Введите пароль для учетной записи TZO. • Доменное имя: Введите доменное имя для учетной записи. • Dynip • Ключ регистрации: Введите ключ для регистрации. • Доменное имя: Введите доменное имя для учетной записи.

Настройка порта USB

Для доступа к настройкам порта USB перейдите в меню «Сервис» и затем используйте ссылку в левом меню.

Для настройки беспроводной сети доступны следующие меню:

-Обзор;
-Сетевой файловый сервер (Samba);
-Сервер FTP;
-Сервер печати;
-Медиасервер;
-Дополнительно.

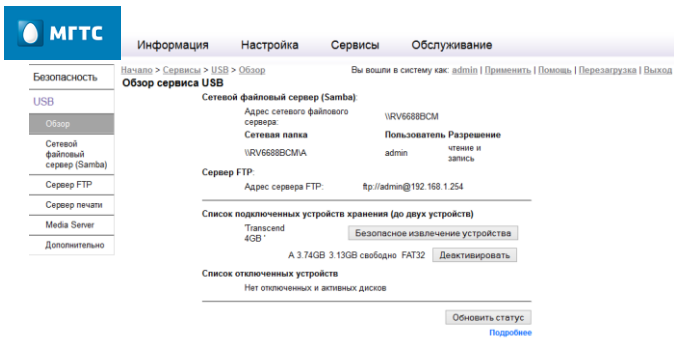


Рис.16: Обзор подключенных устройств USB.

Обзор

Обзор	
Сетевой фаловый сервер (Samba)	Страница сетевого файлового сервера показывает доступную папку, права на изменения файлов и учетную запись пользователя, имеющего доступ к общей

	папке. 1. «**Адрес сетевого файлового сервера**» показывает сетевой адрес устройства. 2. «**Сетевая папка**» показывает список доступных папок. 3. «**Пользователь**» показывает имя пользователя, имеющего доступ к папке. 4. «**Разрешение**» показывает разрешенные права на запись и чтение файлов из общей папки.
Сервер FTP	Сервер FTP показывает список адресов серверов FTP.
Список подключенных устройств хранения	Список подключенных и активных дисков. Диски будут активированы автоматически, если количество дисков не превышает максимально разрешенного. 1.Таблица показывает имя диска, общий размер, размер свободного пространства и файловую систему. 2.Кнопка «**Безопасное извлечение устройства**» используется для безопасного извлечения диска. 3.Кнопка **«Деактивировать»** используется для деактивации дисков и удаления сведений о них из конфигурации.
Список отключенных устройств	Приводится список отключенных и активных дисков.
Обновить статус	Кнопка «**Обновить статус**» используется для обновления списка активных дисков. Подключенные диски будут активными если их количество не превышает максимально допустимого (В настоящее время максимальное количество дисков 2).

Сетевой файловый сервер (Samba)

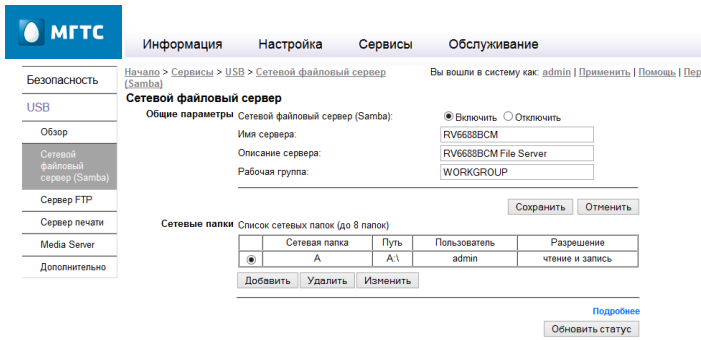


Рис.17: Сетевой файловый сервер Samba.

Сетевой файловый сервер (Samba)

Сетевой файловый сервер	
Общие параметры	Эта часть описывает конфигурацию Samba. 1. Сетевой файловый сервер (Samba): выберите Включить/Выключить для разрешения/запрещения доступа к сетевым ресурсам. 2. Имя сервера: показывает имя устройства. 3. Описание сервера: содержит описание устройства. 4. Рабочая группа: показывает имя рабочей группы.
Сетевые папки	Доступ на текущие подключенные диски\папки. 1. «Сетевая папка»: указывает имя доступной папки. 2. «Путь»: указывает путь к папке. 3. «Пользователь»: указывает пользователя этой папки. 4. «Разрешение»: указывает права пользователя для доступа к папке.

	5. Нажатие программной кнопки «Добавить» приведет к созданию новой папки. 6. Для удаления выбранной папки нажмите кнопку «Удалить». 7. Для редактирования данных выбранной папки нажмите кнопку «Изменить».
Обновить статус	Программная кнопка «обновить статус» предназначена для обновления списка активных дисков.

Сетевой файловый сервер FTP

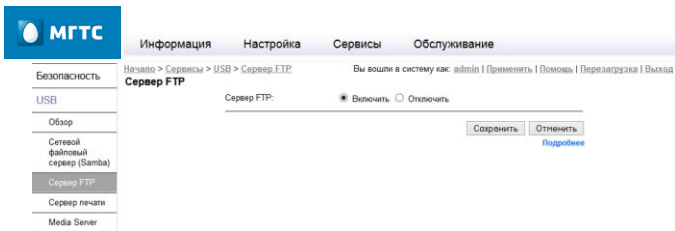


Рис.18: Сетевой файловый сервер FTP.

Сетевой файловый сервер FTP

Сервер FTP	
Сервер FTP	1. Выберите одно из двух: Enable или Disable для FTP сервера. 2. Нажмите Save для сохранения установок.

Характеристики устройства*

Устройство ONT RV6688 - терминал оптической сети GPON, реализующий функции оконечного абонентского оборудования широкополосного доступа FTTH, выполненный в соответствии с рекомендацией ITU-T G.984.

Описание устройства

PON	SFF, одномодовый разъем SC/APC
Gigabit Ethernet	4*10/100/1000Base-T Gigabit Ethernet порта с RJ-45 разъемами
POTS	2*FXS порта с RJ-11 разъема
Wireless	Беспроводная точка доступа 802.11n в диапазоне 2,4 Ггц
USB	Два порта USB 2.0
Мониторинг ИБП	Порт мониторинга состояния ИБП, RJ-45

Физические характеристики

Размеры, мм (ШхГхВ)	240 x150 x 33
Вес, грамм	516

Характеристики оптического интерфейса

Тип SFF трансивера		RV6688 - GPON optical diplexer
Стандарт		Class B+ ITU-T G.984.2
Лазер		Class 1
Диапазон		До 20 км, в зависимости от расслоения и с учетом стандартных потерь
Разъем		Одномодовый SC/APC
Тип оптического волокна		G.652
Уровень	**мин**	+0.5 dBm[a]

выходного сигнала, Дб	**макс**	+5.0 dBm[a]
Минимальная чувствительность приемника		-28.0 dBm[a]
Overload level (receiver)		-8.0 dBm

Электрические характеристики

Разъемы	Для подключения к адаптеру: 2.1 mm круглый разъем постоянного тока для подключения адаптера переменного тока, поставляемого вместе с прибором
Адаптер	AC 110~240V / 50~60 Hz
Входное напряжение	12 V DC
Входной ток	1.5 A
Номинальное энергопотребление	Менее 15Вт

Условия эксплуатации и хранения

Температура	эксплуатация: от 0°C до +40°C складирование: от -20°C до +70°C
Влажность	эксплуатация: от 10% до 85% относительной влажности воздуха (RH), без конденсации хранение: от 5% до 90% относительной влажности воздуха (RH), без конденсации

По всем вопросам связанным с эксплуатацией устройства просьба обращаться в контактный центр по телефону 8 495 636 0 636.

*Производитель сохраняет за собой право изменять любую информацию, технические характеристики и комплектацию без предварительного уведомления и обязательств.

Для заметок.