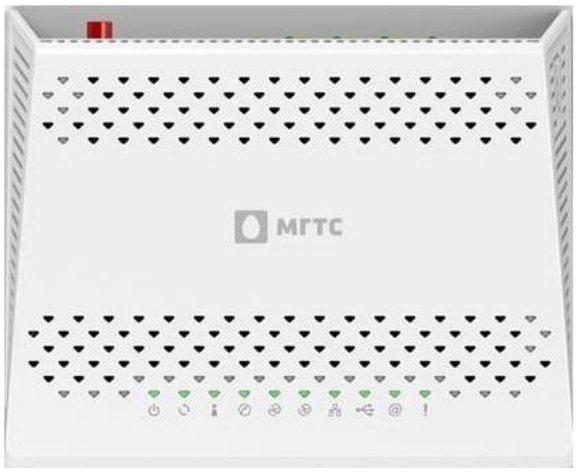
Абонентский терминал GPON RV6699 ver.2 ver.3 3
Руководство по эксплуатации 3
1.Обзор 3
1.2 Содержание комплекта 3
1.3 Индикация устройства 4
1.4 Разъёмы – назначение 5
1.5 Назначение кнопки на боковой панели терминала 6
2. Установка 7
3. Настройка 8
3.1 Настройка LAN 8
3.2 TCP/IP 9
3.3 DHCP 9
3.4 Резервирование адресов (Address Reservation) 9
3.5 Изменение используемых DNS серверов 11
3.6 Конфигурация беспроводной сети 12
3.7 Основная конфигурация (Basic Setup) 13
3.8 Гостевая (виртуальная) точка доступа 15
3.9 Настройки безопасности 15
3.10 Автоматическая настройка безопасности (WPS) 16
3.11 Конфигурация WPS 17
3.12 Фильтрация по MAC 17
3.13 Конфигурация фильтрации по MAC 18
3.14 Настройка беспроводного доступа клиента (отдельно для диапазонов двух диапазонов частот): 18
3.15 Блокирование доступа в интернет устройств по времени 18
3.16 Настройка NAT 19
3.17 Конфигурация Port Mapping 19
3.18 Port Mapping 19
3.19 Настройки Port Triggering 20
3.20 Конфигурация Port Triggering 21
3.21 Настройка DMZ Host 21
3.22 Настройка DMZ 22
3.23 Настройка ALG 22
3.24 Конфигурация ALG 23
3.25 Пропускать VPN 23

3.26 Настройки UPnP 23
3.27 Конфигурация UPnP 24
3.28 Настройка DDNS 24
3.29 Конфигурация DDNS 25
3.30 Настройка порта USB 25
3.31 Обзор сервиса USB 25
3.32 Сетевой файловый сервер (Samba) 27
3.33 Отключение IPv6 28
3.34 Для работы сторонней SIP телефонии 28
4. Характеристики устройства 29
Описание устройства 29
Характеристики оптического интерфейса 29
Электрические характеристики 29
Условия эксплуатации и хранения 30

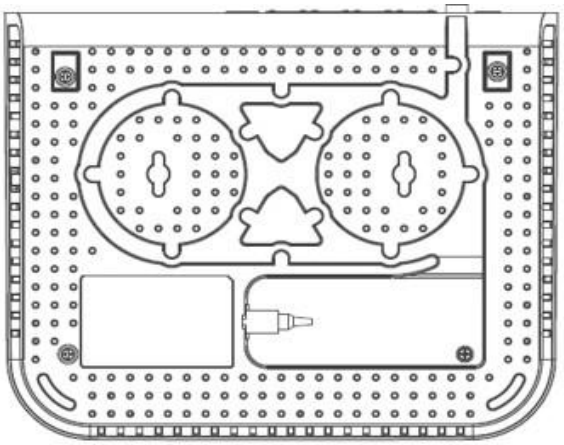
Абонентский терминал GPON RV6699 ver.2 ver.3

Руководство по эксплуатации

1.Обзор



Вид сверху:



Вид снизу:



Вид сзади:



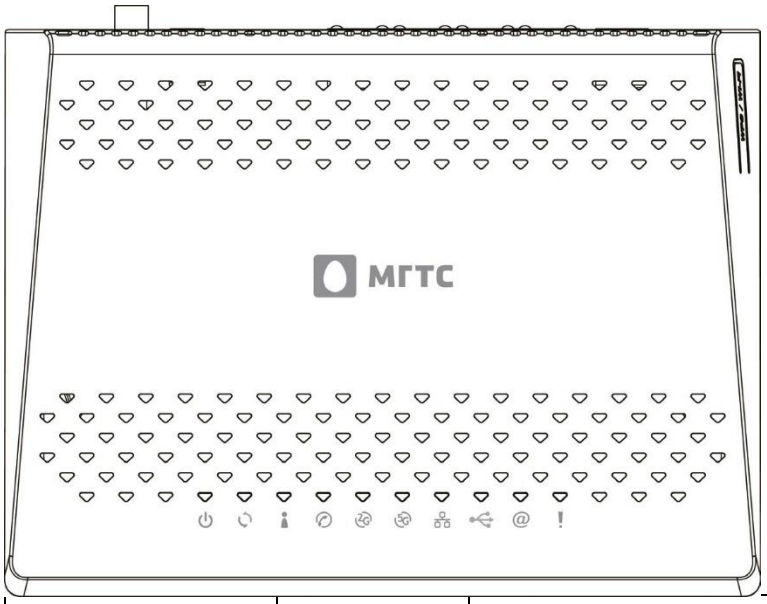
Вид сбоку:

1.2 Содержание комплекта

В комплект поставки абонентского терминала GPON RV6699 входят:

- ③ терминал GPONx RV6699;
- ③ адаптер электропитания AC/DC;
- ③ руководство по эксплуатации.

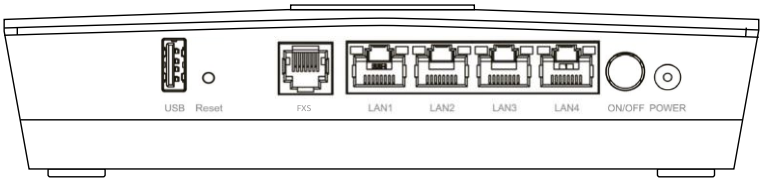
1.3 Индикация устройства



Индикатор	Состояние	Описание
Электропитание	Зелёный	Электропитание включено
	Мигающий зелёный (1 раз в секунду)	Выполняется обновление ПО
	Мигающий зелёный (5 раз в секунду)	Устройство загружается (установка соединения)
	Не горит	Электропитание отлючено
GPON	Зелёный	Регистрация и настройка выполнены
	Мигающий зелёный	Выполняется регистрация GPON и настройка устройст
	Не горит	Нет подключения к GPON
LOS	Не горит	Оптический кабель подключён, приёмопередатчик работает
	Красный	Оптический кабель не подключён либо приё мопередатчик отключён
Интернет	Не горит	Отсутствует подключение к сети интернет
	Зелёный	IP-адрес получен, есть подключение к сети интернет
	Мигающий зелёный	Идёт передача/приём данных
LAN	Зелёный	Есть подключение к LAN
	Не горит	Нет подключений к LAN

	Мигающий зелёный	Идёт передача трафика на LAN-портах
USB	Зелёный	Есть подключение к USB-порту
	Не горит	Нет подключения к USB-порту
	Мигающий зелёный	Идёт обмен данными с USB-устройством
Телефон	Зелёный	Номер зарегистрирован в сети
	Мигающий зелёный	Снята трубка телефона, телефонная линия используется
	Не горит	Номер не зарегистрирован
WiFi 2.4 ГГц	Зелёный	Wi-Fi-сеть доступна
	Мигающий зелёный	Идёт передача данных
	Не горит	Wi-Fi-сеть недоступна/выключена
WiFi 5 ГГц	Зелёный	Wi-Fi-сеть доступна
	Мигающий зелёный	Идёт передача данных
	Не горит	Wi-Fi-сеть недоступна/выключена
WPS	Зелёный	Выполнено подключение устройства по WPS
	Мигающий зелёный (1 раз в секунду)	Режим подключения WPS активирован
	Мигающий зелёный (5 раз в секунду)	Ошибка функции WPS

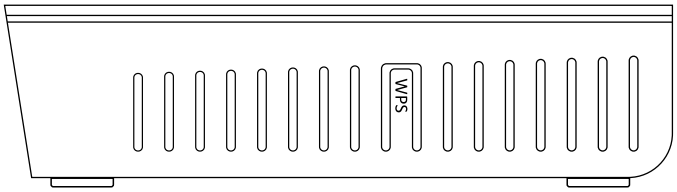
1.4 Разъёмы – назначение



Название	Назначение
USB	При подключении услуг, использующих встроенный USB-порт терминала, соедините его с соответствующим оборудованием
Reset	Нажатие на кнопку в течение 10 с вернёт терминал к заводским настройкам

Порт FXS	Порт с разъёмами RJ11 для подключения телефона с помощью телефонного кабеля
Порты LAN1–LAN4	Порты с разъёмами RJ45 для подключения устройств домашней сети с помощью стандартных Ethernet-кабелей
ON/OFF	Кнопка включения/отключения электропитания
POWER	Разъём для подключения адаптера электропитания
Разъём GPON (не подписан)	Порт для подключения оптоволоконного кабеля

1.5 Назначение кнопки на боковой панели терминала



Название	**Назначение**
WPS / Wi-Fi	Кнопка для активации WPS (удерживайте нажатой 3–7 с) Кнопка для включения/выключения сети Wi-Fi (удерживайте нажатой более 7 с)

2. Установка

1. Выберите подходящее место для установки RV6699.
2. Подключите порт GPON к оптоволоконной широкополосной сети.
3. Подключите Ethernet-кабели к разъёму сетевого интерфейса компьютера или маршрутизатора.
4. Подключите адаптер электропитания, входящий в состав комплекта, к разъёму питания и электросети, затем нажмите кнопку включения электропитания на задней панели.
5. Подождите 2 минуты, пока устройство войдёт в рабочий режим. Проверьте состояния индикаторов:

- индикаторы «Электропитание»,
- «GPON» ,
- «Телефон» ,
- «Интернет»
- «Статус» должны светиться **зелёным** цветом

3. Настройка

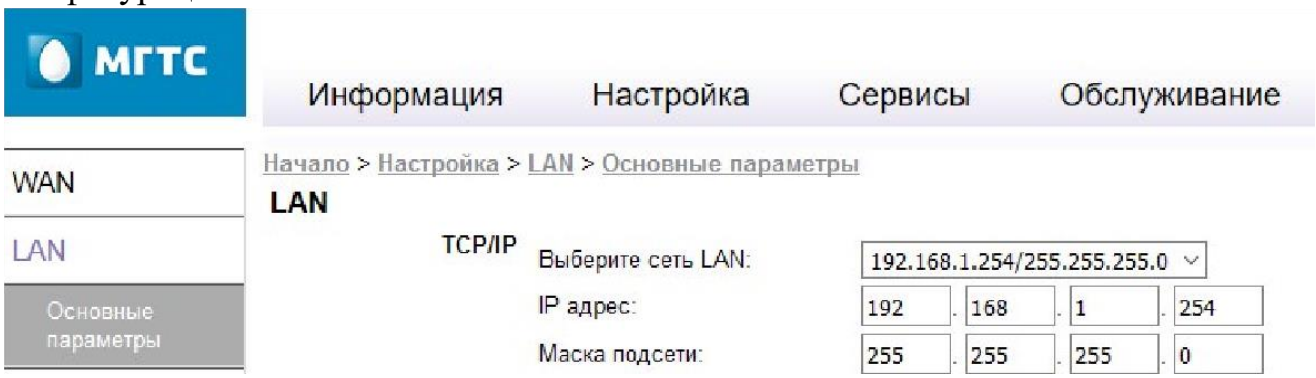
1. Запустите интернет-браузер. (Internet Explorer, Mozilla Firefox, Google Chrome, Opera)
2. В адресной строке браузера введите **http://192.168.1.254**.
3. В появившемся диалоговом окне введите
   имя пользователя: **admin**
   пароль: **admin**
4. После аутентификации вы перейдёте на главную страницу конфигурации и статуса — «Информация». Теперь вы можете приступить к настройке ONT RV6699 с помощью браузера.

Для настройки устройства абоненту доступны следующие вкладки:

- «LAN»;
- «Беспроводная сеть»;
- «NAT»;
- «DDNS»;
- «USB».

3.1 Настройка LAN

Воспользуйтесь вкладкой «LAN» в главном меню, чтобы перейти на страницу конфигурации локальной сети.



В выпадающем списке вы можете выбрать любую из четырёх подсетей. В разделе TCP/IP показывается её IP-адрес и маска подсети.

3.2 TCP/IP

Введите параметры для включения сети LAN:

Выберите LAN сеть	Выберите новую подсеть. Включите опцию «Использовать сеть LAN», если это необходимо.
IP-адрес	Введите IP-адрес маршрутизатора и 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-адреса, который вы назначаете. Рекомендуется использовать 255.255.255.0 в качестве маски подсети.

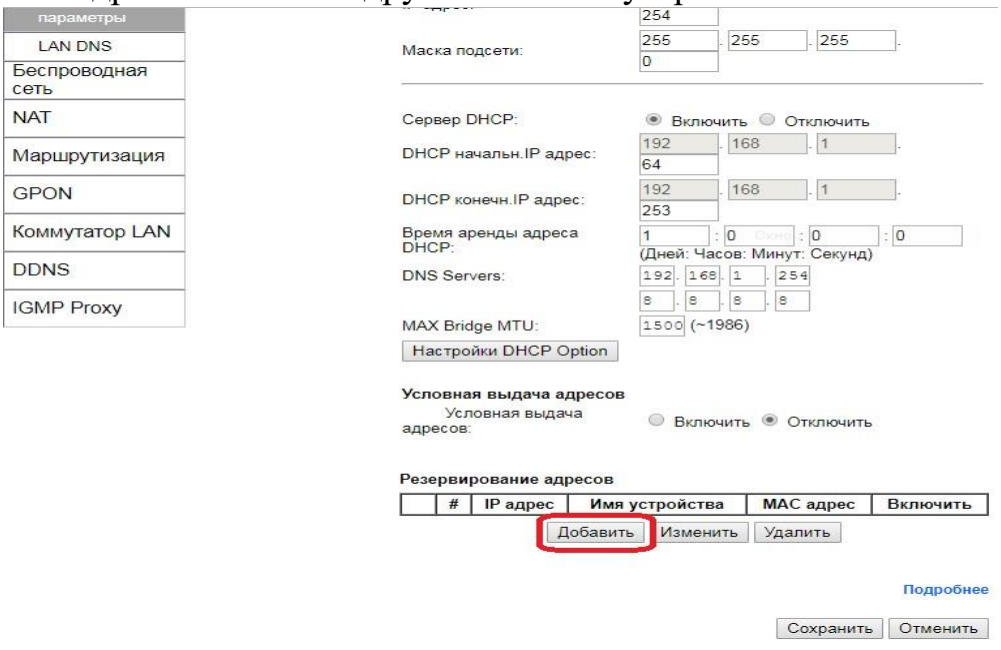
3.3 DHCP

Локальный сервер DHCP автоматически выделяет и контролирует распределение IP-адресов для всех хостов в сети.

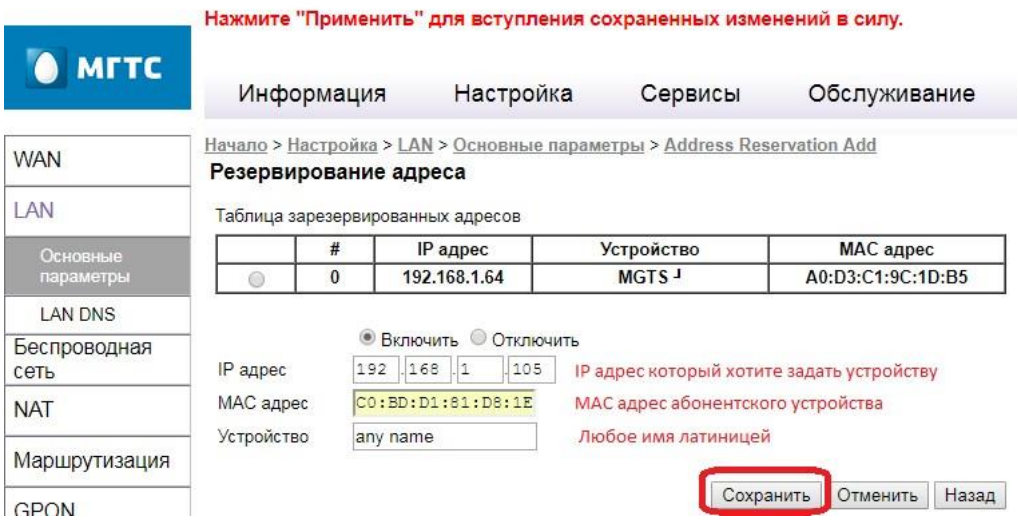
DHCP начальн. IP адрес	Значение начального IP-адреса диапазона адресов для динамического назначения.
Время аренды адреса DHCP	Время аренды DHCP — это промежуток времени, в течение которого сетевые устройства будут иметь возможность подключиться к шлюзу с текущим динамическим IP-адресом. После того, как время истекло, устройству будет автоматически присвоен свободный IP-адрес. Значение по умолчанию составляет 1 день.

3.4 Резервирование адресов (Address Reservation)

Используется в случае необходимости получения фиксированного локального сетевого IP – адреса на ПК или другом сетевом устройстве.



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 DHCP. ③ Нажмите кнопку «Добавить». ③ Выберите устройство, для которого вы хотите сделать резервирование и добавьте его в таблицу резервирования: «Таблица зарезервированных адресов». ③ Если устройство не подключено и его нет в списке, введите IP-адрес, MAC-адрес и имя для устройства, которое вы хотите добавить, вручную. ③ Нажмите кнопку «Сохранить», когда закончите.
Изменить	③ Установите курсор рядом с зарезервированным адресом, который вы хотите изменить. Нажмите кнопку «Изменить». ③ Измените параметры: IP-адрес, MAC-адрес или «Устрой ство». ③ Нажмите кнопку «Сохранить».
Удалить	③ Установите курсор рядом с зарезервированным адресом, который вы хотите удалить. ③ Нажмите кнопку «Удалить».

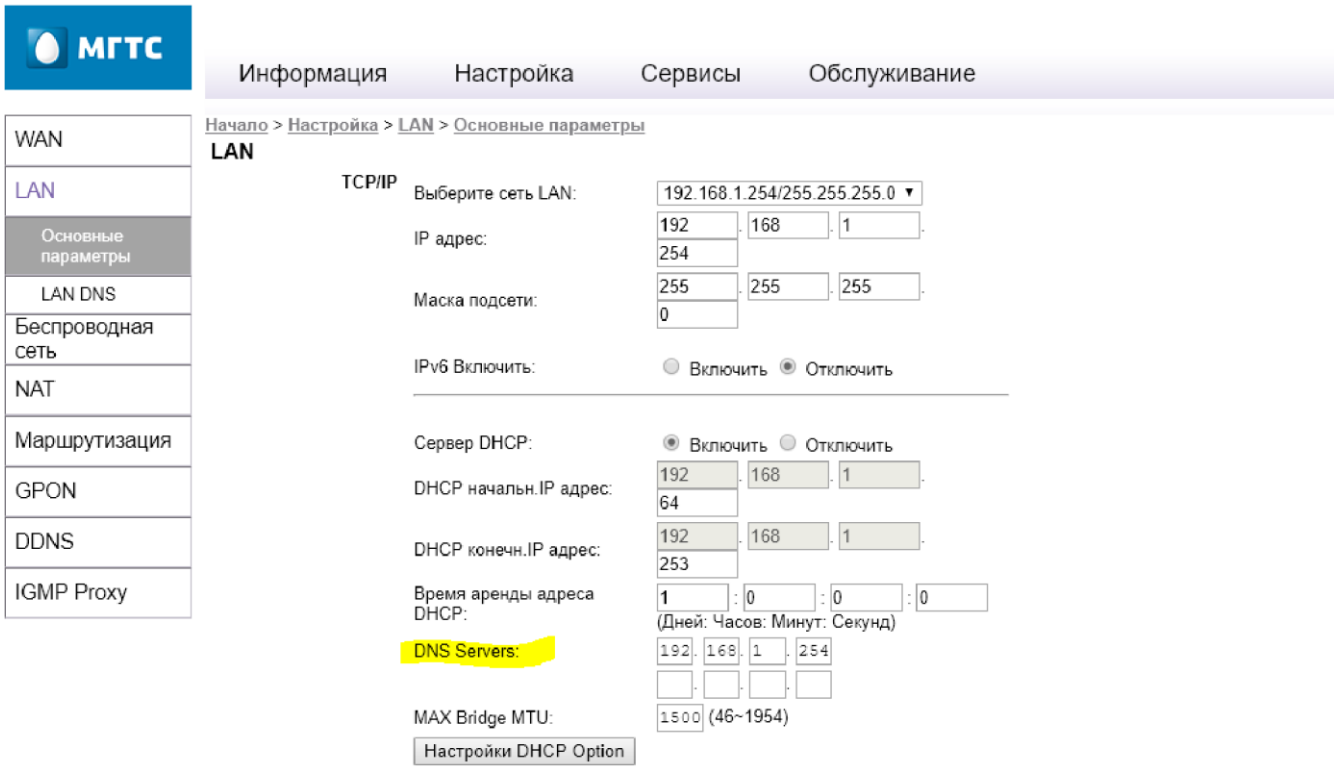


В следующем окне нажимаем ссылку «Применить» сверху справа для сохранения настроек.

Теперь DHCP сервер будет выдавать указанному устройству (MAC-адрес), заданный локальный сетевой IP адрес.

3.5 Изменение используемых DNS серверов

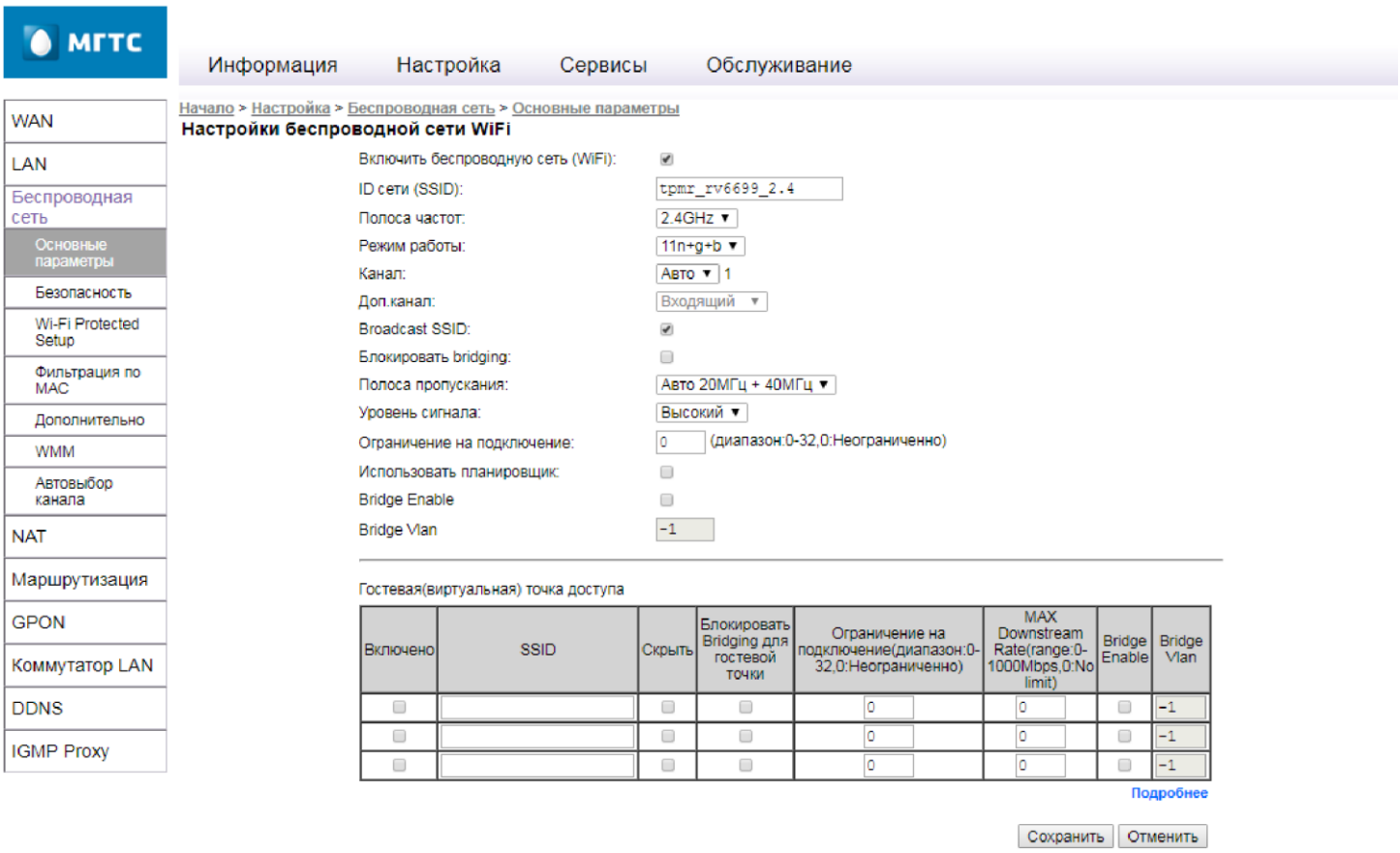
1. Вкладка Настройка – LAN – Основные параметры



2. В поле DNS Servers указываем необходимый IP DNS сервера
3. Нажимаем кнопку «Сохранить»
4. Нажимаем кнопку «Применить»

3.6 Конфигурация беспроводной сети

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



RV6699 поддерживает работу одновременно в двух диапазонах: 2,4GHz и 5GHz.

В терминале RV6699 можно использовать до четырех беспроводных сетей одновременно (4 SSID) в каждом диапазоне. Беспроводная сеть по умолчанию включена на устройстве.

Для настройки беспроводной сети доступны следующие меню:

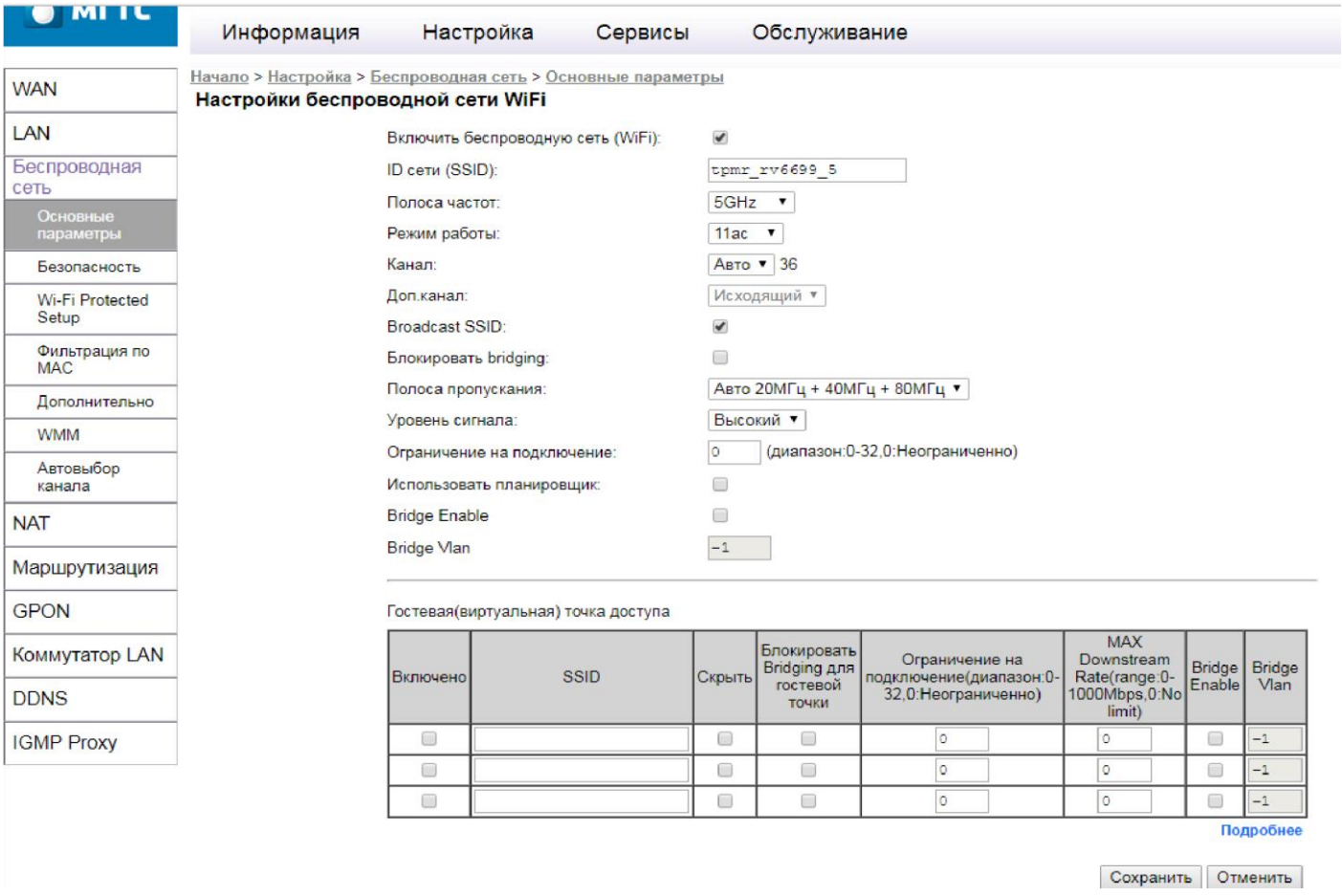
- «Основные параметры»;
- «Безопасность»;
- «WPS» (Wi-Fi Protected Setup) — настройка автоматического защищённого соединения;
- «Фильтрация по MAC» — ограничения доступа к беспроводной сети.

3.7 Основная конфигурация (Basic Setup)

Включить беспроводную сеть (WiFi)	Если снять этот флажок для основной и гостевых беспроводных сетей, 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 дать ему другое имя в свободной форме (до 32 символов). Примечание: значение SSID вводится с использованием латинских букв и цифр.
Полоса частот	Выпадающее меню позволяет выбрать диапазон частот: 2.4 ГГц или 5 ГГц. Все остальные параметры на данной странице (включая ID-сети) настраиваются отдельно для каждого из этих диапазонов.
Режим работы	Выпадающее меню позволяет выбрать и задать значение шлюза в режиме беспроводной передачи. В диапазоне 2.4 ГГц 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. В диапазоне 5 ГГц по умолчанию используется режим 802.11ac.
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 менее зашумлённый канал. ③ Если используются каналы 1 ~ 4, расширение каналов допускается в сторону увеличения. ③ Если используются каналы 5 ~ 9, расширение каналов допускается в сторону как увеличения, так и уменьшения. ③ Если используются каналы 10 ~ 13, расширение каналов допускается в сторону уменьшения.
Broadcast SSID	Эта опция позволяет скрыть беспроводную сеть. В случае отключения трансляции SSID сеть не будет видна при поиске.
Блокировать Bridging	Установите флажок, чтобы блокировать возможность общения подключённых клиентских устройств между собой.

Полоса пропускания	Вы можете выбрать ширину канала вручную для соединения 802.11n. ③ Если произведена настройка и установлено значение в 20 МГц, используется только канал 20 МГц. ③ 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. Для диапазона 5 ГГц можно выбрать ширину канала до 80 МГц.
Уровень сигнала	Установите предпочитаемый уровень сигнала беспроводной сети.
Ограничение на подключение	Вы можете настроить разрешение на использование беспроводной сети для определенного количества пользователей. Если выбрать от 1 до 31, то только 1 ~ 31 беспроводных клиентов могут подключаться к SSID одновременно. Есть возможность выбрать безлимитное количество пользователей, установив значение 0.
Использовать планировщик	Эта опция позволяет настроить время для отключения и включения беспроводной сети.

После выбора настроек, необходимо нажать внизу страницы кнопку **"Сохранить"**, потом сверху справа ссылку **"Применить"** для сохранения настроек.



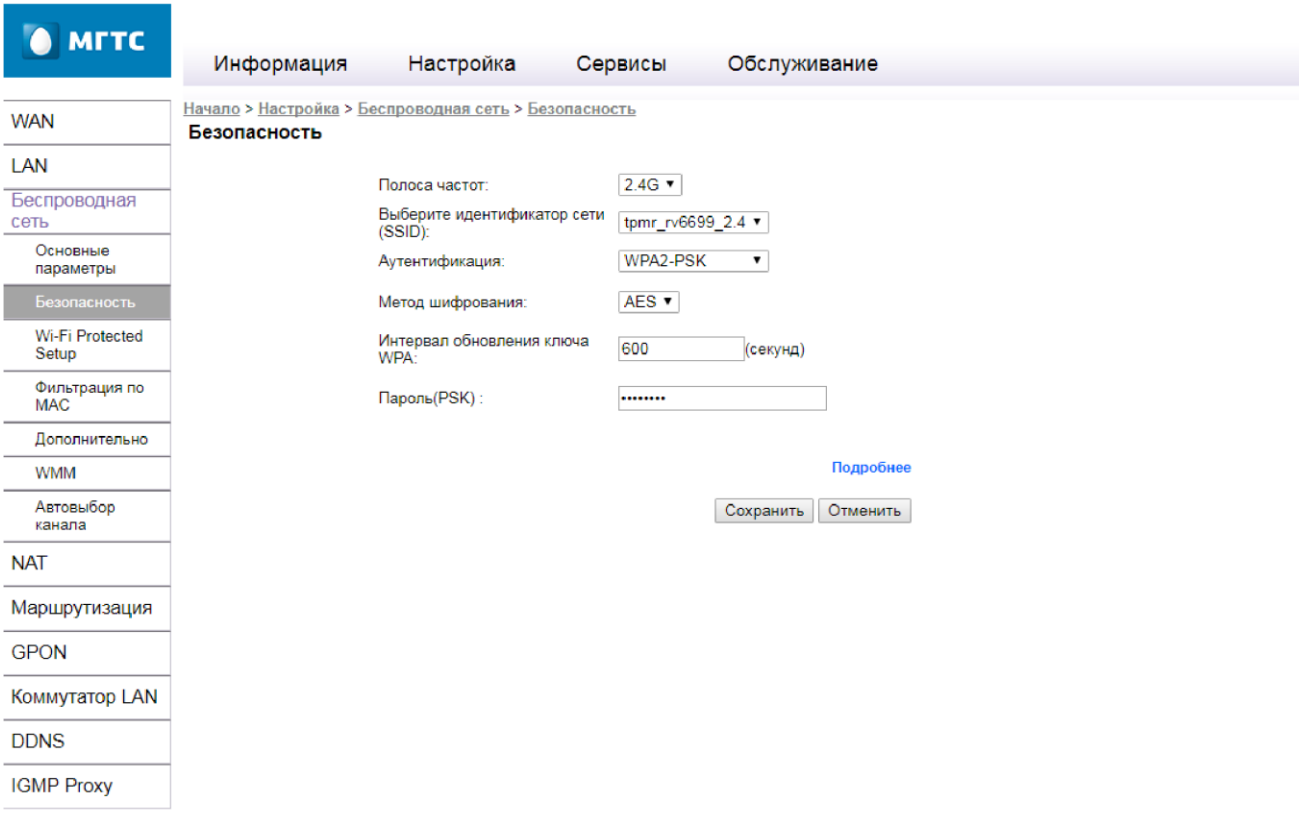
3.8 Гостевая (виртуальная) точка доступа

Настройки	③ Установите флажок «Включено», чтобы включить гостевую SSID. ③ Гостевая SSID должна отличаться от основного SSID и остальных гостевых SSID. ③ Установите флажок «Скрыть», чтобы ваша гостевая беспроводная сеть стала невидимой. ③ Параметры безопасности гостевой сети (тип аутентификации, шифрования, пароль) можно задать в меню «Безопасность», выбрав соответствующий идентификатор SSID.

3.9 Настройки безопасности

Конфигурация безопасности позволяет управлять настройками аутентификации/шифрования для обеспечения максимальной степени безопасности.

Установка ключа шифрования используется для каждой полосы частот (2,4 / 5 GHz) отдельно.



Выберите диапазон частот (5 ГГц или 2.4 ГГц) и 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 соответствует рекомендации IEEE 802.11 и имеет более слабую степень защиты по сравнению с другими типами защиты, например WPA2-PSK.
WEP-128	Это аналогичный WEP-64 алгоритм шифрования, однако имеет более длинный ключ.
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 от «0» до «9». Длина ключа должна быть не менее 10 символов для 64-битных WEP или до 26 символов при использовании 128-битных WEP.
WPA-PSK	Wireless Protected Access обеспечивает беспроводной защищённый доступ с использованием шифрования TKIP.
WPA2-PSK	Wireless Protected Access 2 обеспечивает беспроводной защищённый доступ с использованием шифрования AES.
WPA/WPA2PSK	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.

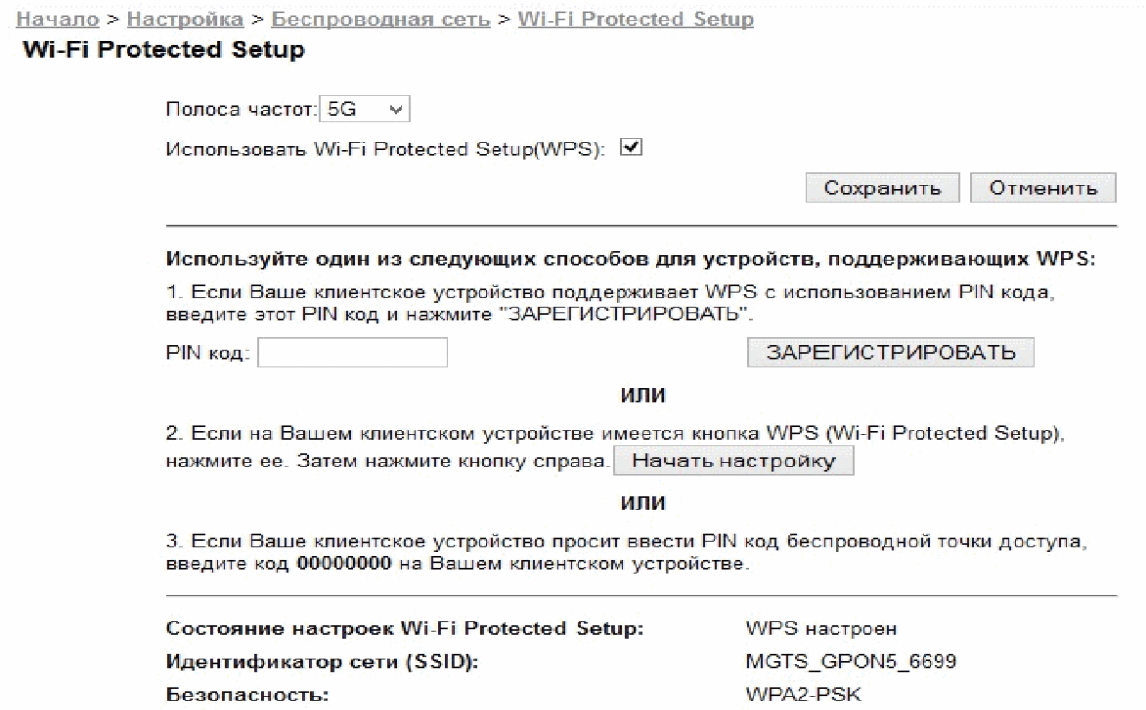
После выбора настроек, необходимо нажать внизу страницы кнопку **"Сохранить"**, потом сверху справа ссылку **"Применить"** для сохранения настроек.

3.10 Автоматическая настройка безопасности (WPS)

Wi-Fi Protected Setup (WPS) — это функция, которая позволяет автоматически настроить защищённое беспроводное соединение. Если у вас есть клиентские устройства с функцией WPS, следуйте приведённым ниже инструкциям.

Для включения функции WPS необходимо нажать и удерживать кнопку **«WPS/Wi-Fi»** в течение 3–7 секунд. Если удерживать кнопку «WPS/Wi-Fi» более 5 секунд, произойдёт включение/отключение сети Wi-Fi. Управление функционалом WPS и Wi-Fi-сети доступно также через веб-интерфейс устройства. Процедура WPS производится для каждого подключаемого устройства отдельно.

Вы можете настроить WPS отдельно для диапазонов 5 ГГц и 2,4 ГГц.



3.11 Конфигурация WPS

③ PIN-метод

1. Введите PIN-код клиентского устройства и нажмите кнопку «Зарегистрировать».
2. Запустите WPS на клиентском устройстве (с помощью утилиты настройки или в режиме конфигурации устройства). В течение 2 минут произойдёт регистрация устройствами и между ними будет установлено соединение.

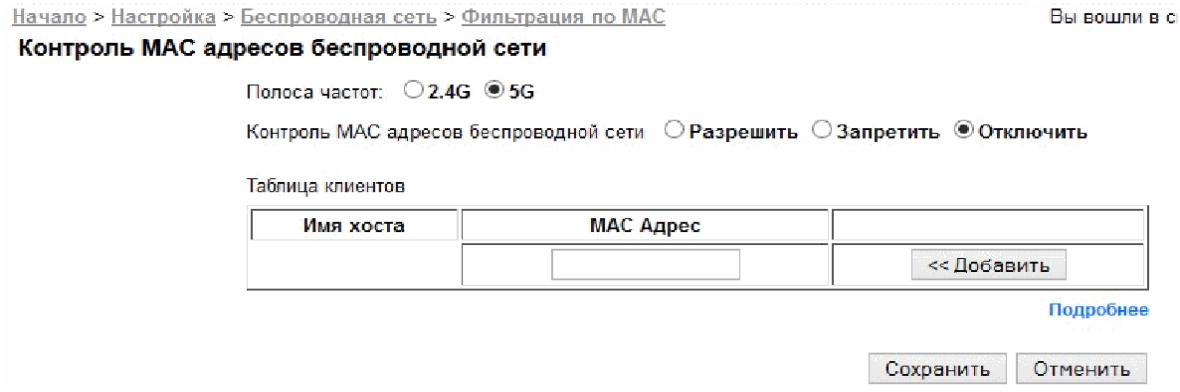
③ PBC метод

Используйте этот метод, если ваше клиентское устройство имеет кнопку WPS.

1. Нажмите кнопку «Начать настройку / Start PBC» кнопку на экране.
2. Нажмите кнопку WPS на клиентском устройстве.

3.12 Фильтрация по MAC

Это окно позволяет вам указать, компьютеры с какими MAC-адресами получат доступ к беспроводной локальной сети, а какие будут заблокированы.



3.13 Конфигурация фильтрации по MAC

Существует три режима для управления доступом к ресурсам беспроводной сети на основе MAC-адресов:

1. Выберите режим «Разрешить», 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 беспроводной сети на основе MAC.

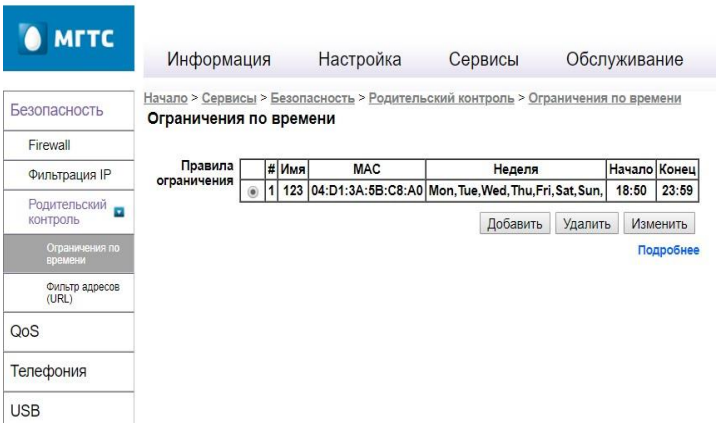
3.14 Настройка беспроводного доступа клиента (отдельно для диапазонов двух диапазонов частот):

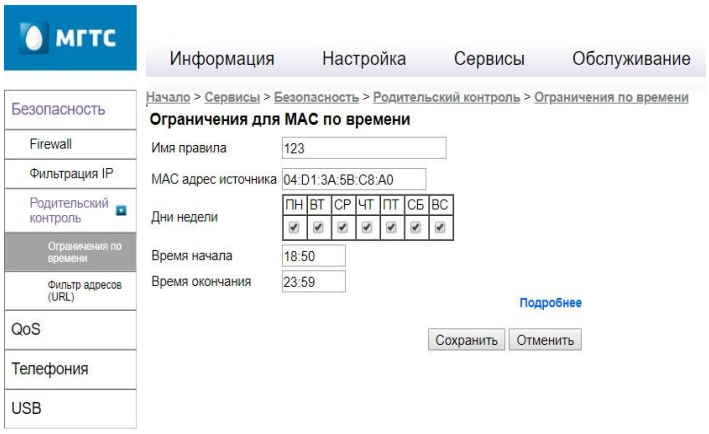
1. Выберите режим контроля беспроводного доступа на основе контроля MAC-адресов, установите: разрешить или запретить.
2. Введите MAC-адрес компьютера, доступ которого вы хотите разрешить или запретить.
3. Нажмите кнопку «Применить».

Примечание: вы можете добавить не более 32 записей MAC-адресов.

3.15 Блокирование доступа в интернет устройств по времени

1. Переходим на страницу Сервисы - Безопасность - Родительский контроль - Ограничение по времени





3. Нажимаем кнопку «Добавить»
4. Пишем Имя правила - любое имя латиницей и цифрами, **ни в коем случае не пишите русскими буквами!!!**.
5. MAC адрес источника - мак устройства в формате 00:00:00:FF:FF:FF
6. Выбираем дни недели и временной интервал блокировки. Если необходимо несколько интервалов, создавайте новое правило
7. Жмём «Сохранить», «Применить».
8. Если функционал не работает, удостоверьтесь, верное ли время на ONT. Также блокировка происходит не сразу, а в течение 1-2 минут.

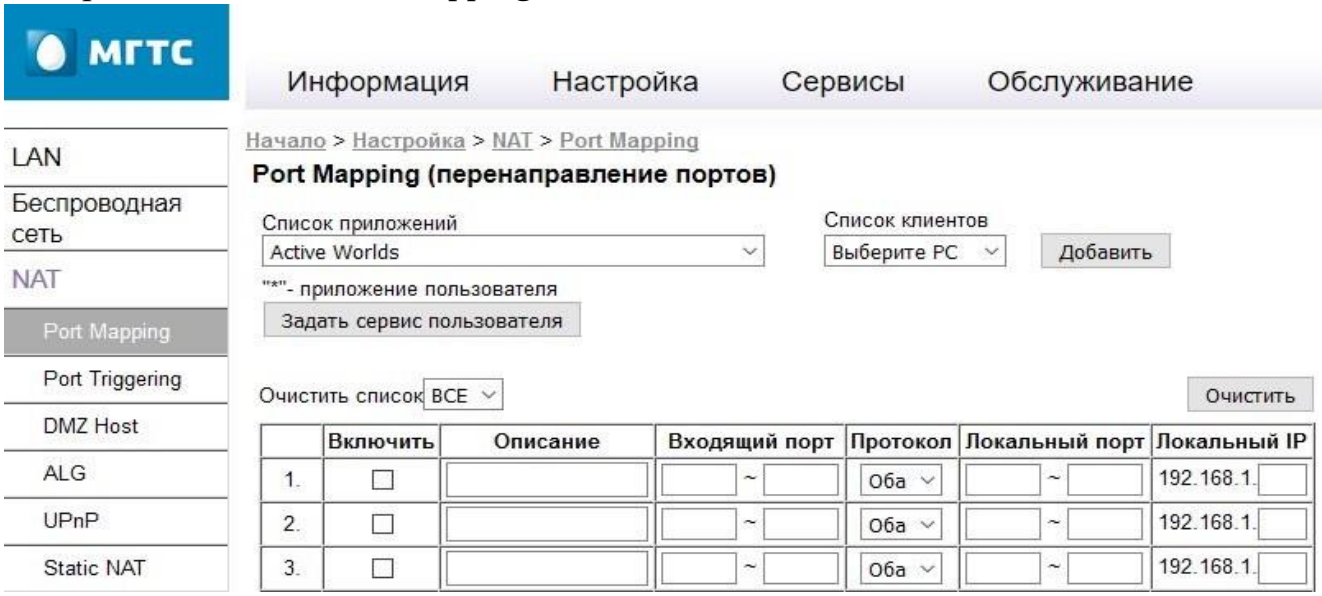
3.16 Настройка NAT

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.

Перед использованием перенаправления портов рекомендуется назначить резервирование IP-адреса для сетевого устройства по MAC-адресу. Пункт 3.4 данной инструкции.

3.17 Конфигурация Port Mapping

Настройка – NAT – Port Mapping



3.18 Port Mapping

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. Если вы еще не включили ваш сервер в LAN сеть, вы можете вручную ввести последний октет IP-адреса, который 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.

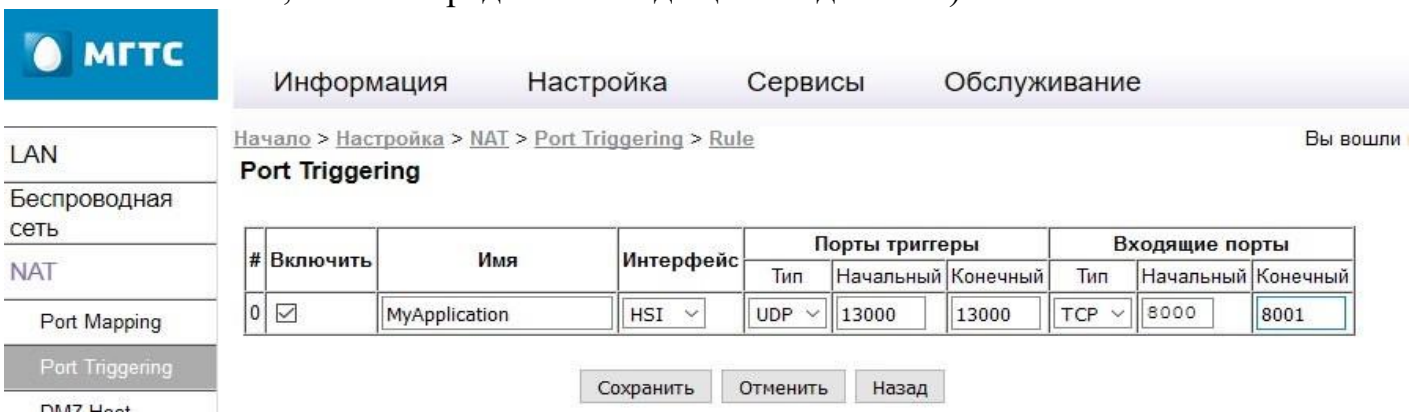
3.19 Настройки Port Triggering

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 идёт с компьютера, используется порт, который определен как порт перенаправления; маршрутизатор запоминает компьютер и порт приложения.
2. Для входящего трафика нужно использовать полученный входящий порт , определённый для этого приложения, тогда 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).



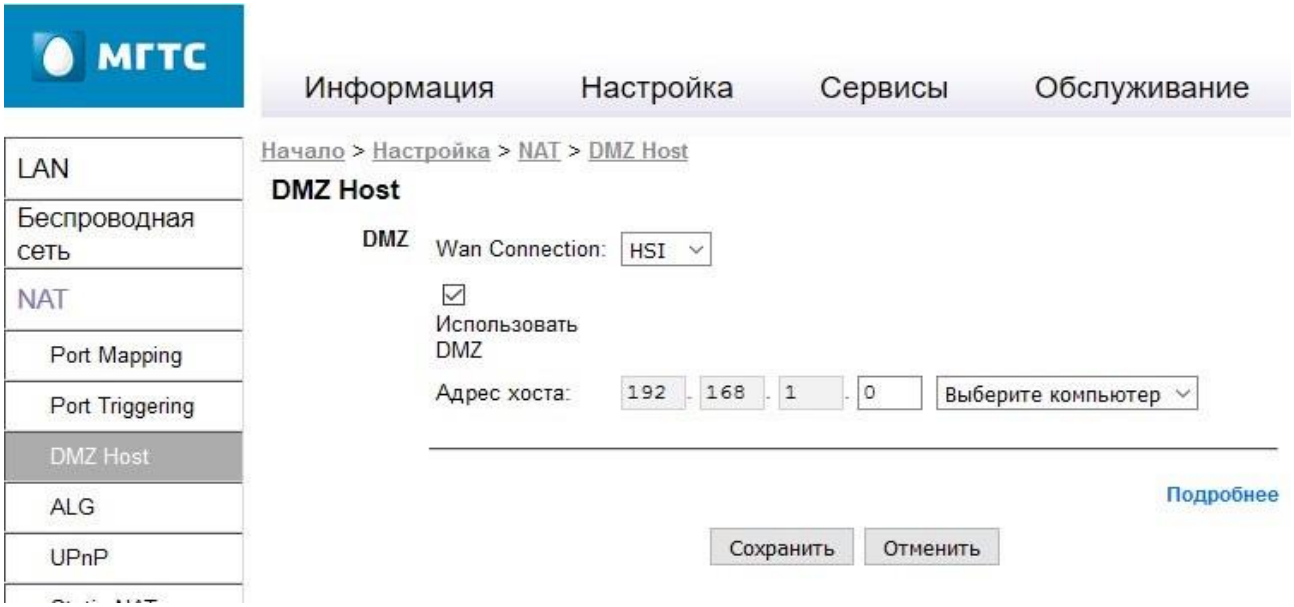
3.20 Конфигурация Port Triggering

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

3.21 Настройка DMZ Host

Demilitarized zone (DMZ) — демилитаризованная зона — это особая технология защиты информационного периметра. Серверы, отвечающие на запросы из внешней сети, находятся в особом сегменте сети, который называется DMZ. Эти серверы ограничены в доступе к основным сегментам сети с помощью межсетевого экрана. DMZ Host — это ПК, находящийся внутри DMZ или имеющий к ней подключение.

Для доступа к настройкам DMZ используйте ссылку в левом меню.



3.22 Настройка DMZ

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

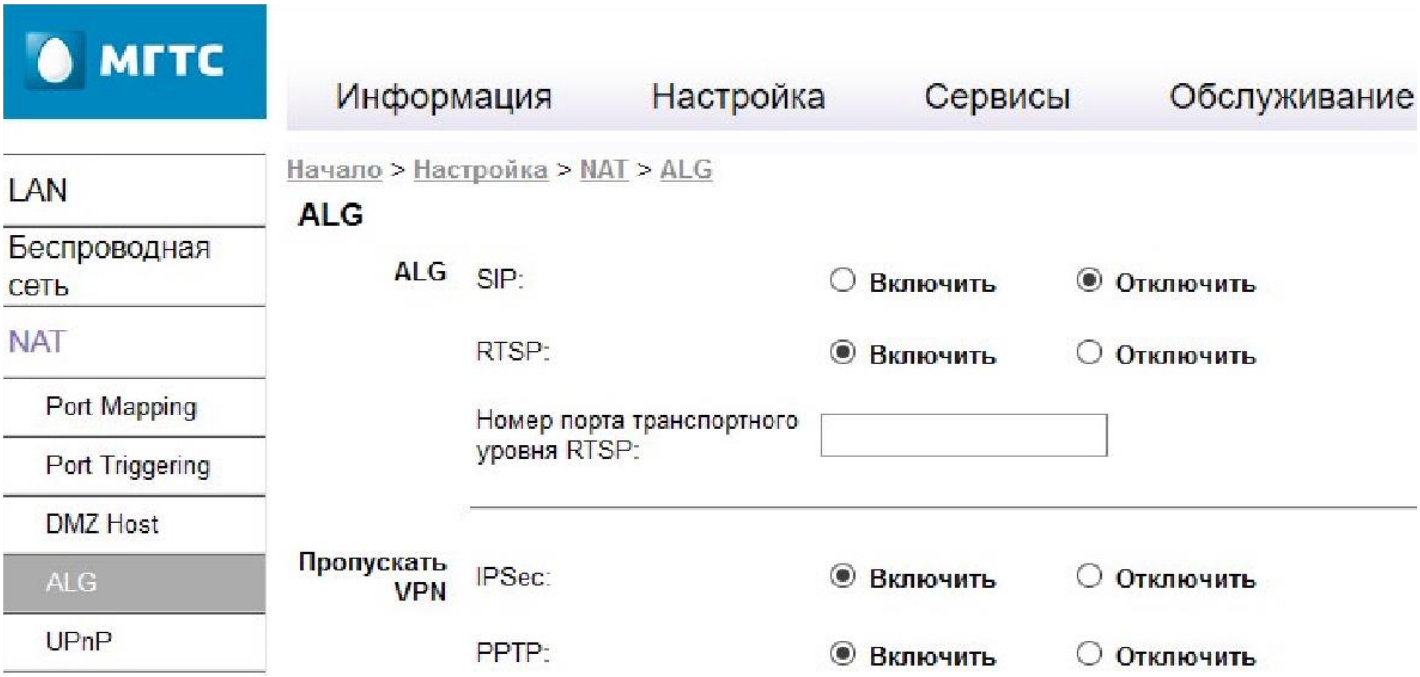
- Это позволяет использовать практически любое приложение, которое будет работать на «DMZ ПК».
- «DMZ ПК» получает все данные и устанавливает соединения как «Неизвестные».
- Если функция DMZ включена, вы должны ввести IP-адрес компьютера или выбирать нужный компьютер в списке, который будет использоваться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

«DMZ ПК» находится фактически за пределами межсетевого экрана, это делает его более уязвимым для атак. Поэтому включайте функцию DMZ только в случае необходимости.

3.23 Настройка ALG

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

Для доступа к настройкам ALG используйте ссылку в левом меню.



3.24 Конфигурация ALG

SIP	SIP ALG по умолчанию отключён.
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 включён по умолчанию.
Номер порта транспортного уровня RTSP	Для некоторых провайдеров необходимо изменить порт видеосервера, по умолчанию — порт 554. Можно указать дополнительные 7 портов через запятую, как порт RTSP по умолчанию.

3.25 Пропускать VPN

IPSec	Internet Protocol Security *(IPSec)* представляет собой набор протоколов, используемых для безопасного обмена пакетами на IP-уровне. IPSec Pass-Through включён по умолчанию.
PPTP	Point-Point Tunneling Protocol *(PPTP)* позволяет использовать Point-Point Protocol *(PPP)* для туннелирования через IP-сеть. PPTP Pass-Through включён по умолчанию.

3.26 Настройки UPnP

Universal Plug and Play (UPnP) — 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.



3.27 Конфигурация UPnP

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 не намерены запрещать какие-либо интернет-соединения.
NAT Traversal	Выберите Disable, если не намерены вносить изменения вручную в маршруты, используя UPnP.
Таблица NAT Traversal	Нажмите эту кнопку, если хотите увидеть детальную информацию по таблице маршрутов.

3.28 Настройка DDNS

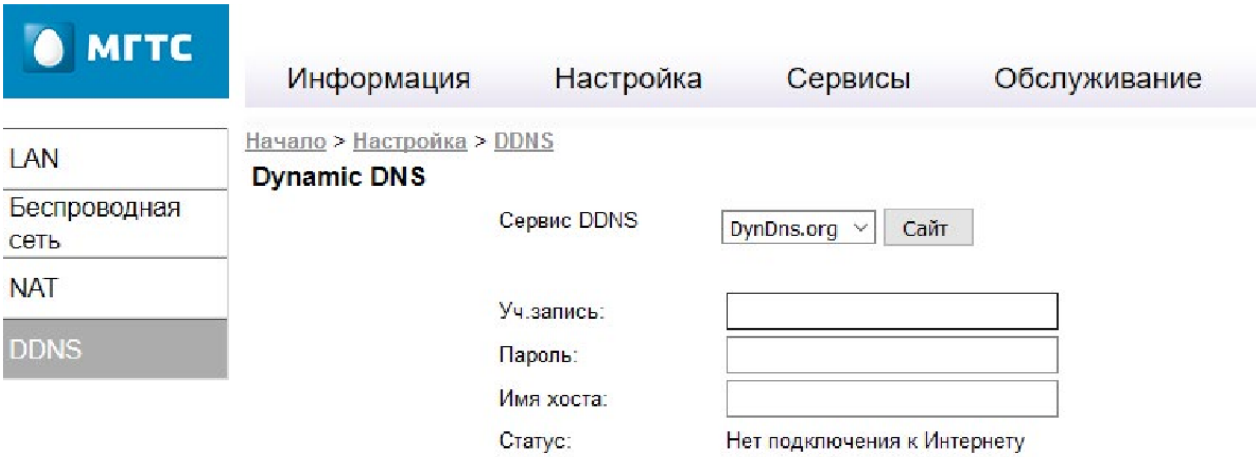
Для доступа к настройкам DDNS используйте ссылку в левом меню.
Провайдеры интернет-услуг обычно предоставляют подключение с динамическим IP-адресом: новый адрес выделяется каждый раз, когда устанавливается интернет-соединение.

Это означает, что другие пользователи интернета не знают ваш IP-адрес и 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 вам доменное имя по запросу.
- RV6699 свяжется с сервером DDNS, когда он определит, что 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.



3.29 Конфигурация DDNS

Выберите поставщика услуг DDNS из списка и введите параметры, соответствующие требованиям сервиса:

Сервис DDNS	Выберите DDNS-провайдера из раскрывающегося списка
Имя хоста	Введите доменное имя узла, зарегистрированное у DDNS-провайдера.
Доменное имя	Введите имя пользователя для авторизации у DDNS-провайдера.
Пароль	Введите пароль для авторизации у DDNS-провайдера.
Адрес E-mail	Введите адрес электронной почты для авторизации у DDNS-провайдера.
Ключ регистрации	Введите ключ регистрации у DDNS-провайдера

3.30 Настройка порта USB

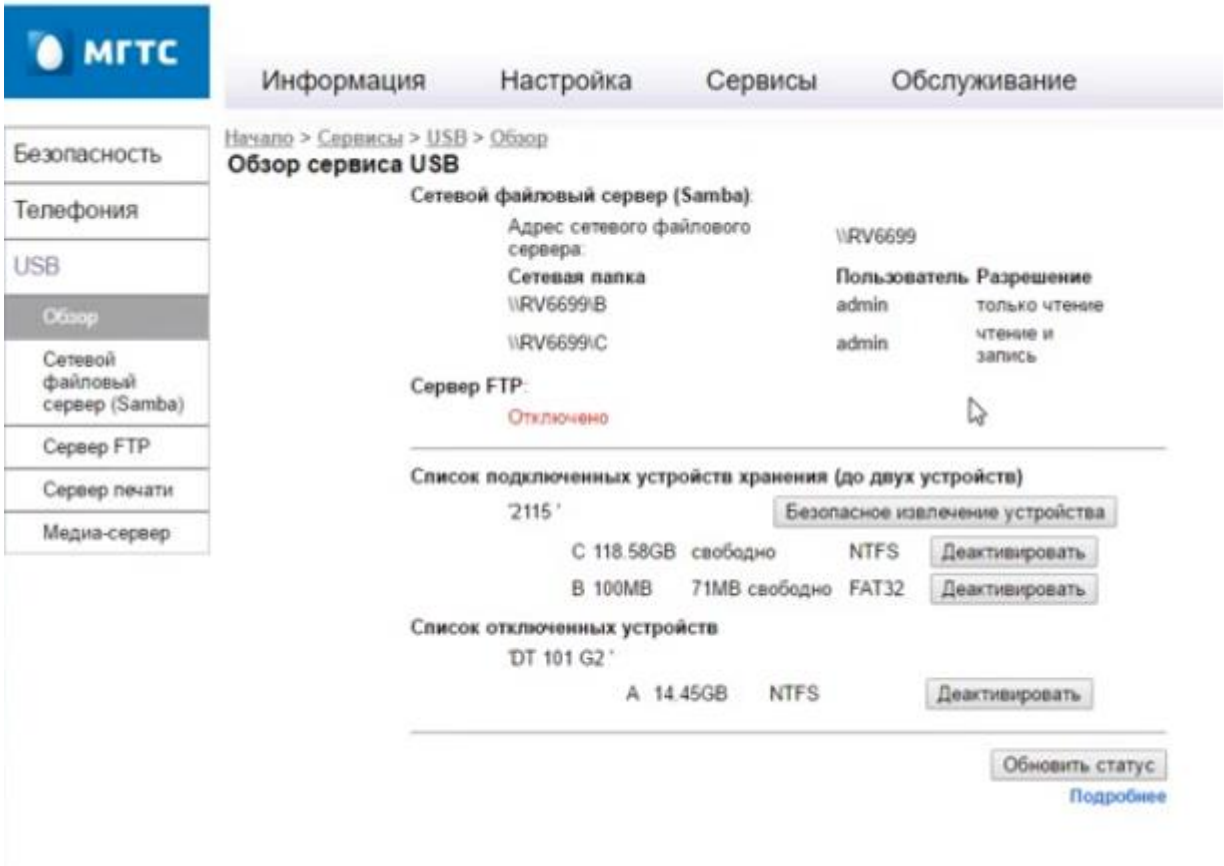
Для доступа к настройкам порта USB перейдите в меню «Сервис» и затем используйте ссылку в левом меню.

Для настройки сервисов USB доступны следующие меню:

- «Обзор»
- «Сервер печати»
- «Медиасервер»

3.31 Обзор сервиса USB

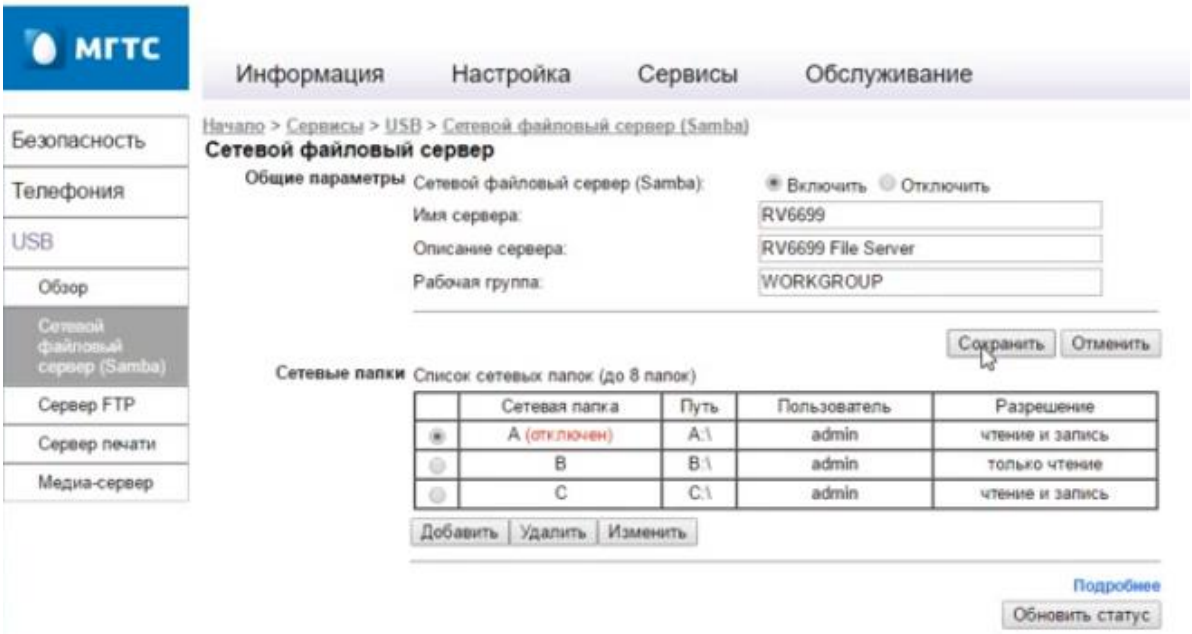
Подключите к USB переносной HDD или Flash накопитель. Вкладка Сервисы – USB - Обзор, позволит перейти к просмотру общей информации о подключенном запоминающем устройстве и настроить дополнительные серверы в домашней локальной сети.



Список подключенных устройств хранения	Список подключённых 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 отключённых дисков.
Обновить статус	Кнопка «Обновить статус» используется для обновления списка активных дисков. Подключённые диски будут активными, если их количество не превышает максимально допустимого (сейчас — 2).

3.32 Сетевой файловый сервер (Samba)

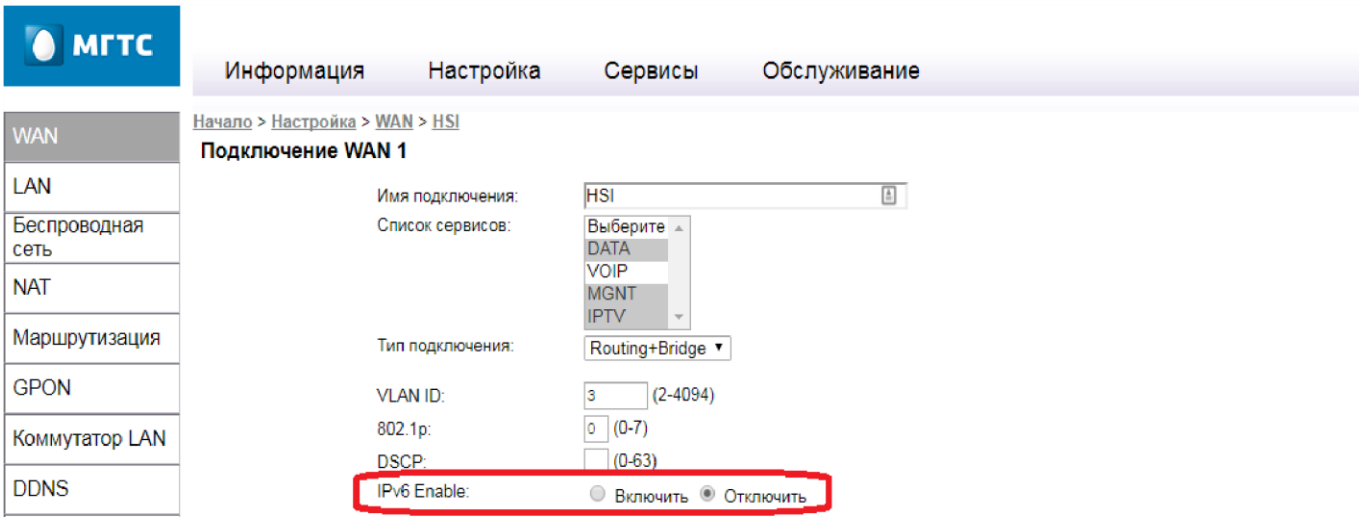
Используется для доступа по локальной сети к файлам находящимся на подключенном к USB, Flash / HDD накопителе



Сетевой файловый сервер (Samba)	• Включить • Отключить
Имя сервера	Имя сервера которое будет отображаться в локальной сети, можно задать произвольное
Описание сервера	Описание которое будет отображаться рядом с именем
Рабочая группа	Локальная рабочая группа сети
Сетевые папки	К папкам на Flash / HDD накопителе можно выделить отдельные пути, а можно использовать корневой каталог для доступа ко всем папкам и файлам на накопителе. Сетевой папке так же можно назначать права на чтение / запись

3.33 Отключение IPv6

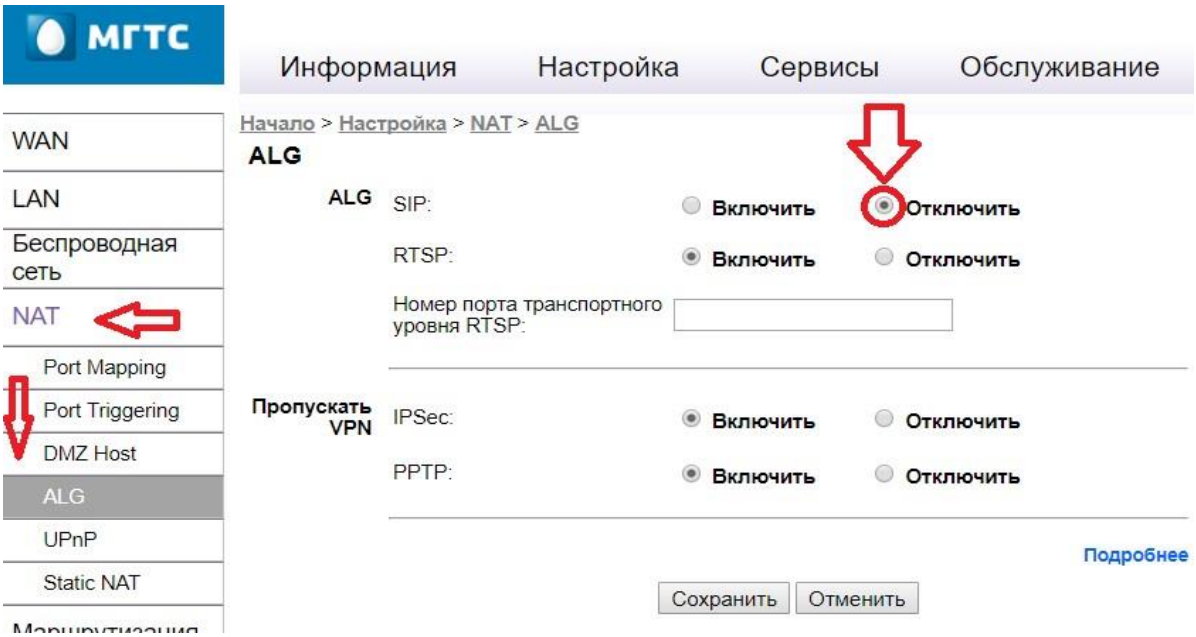
Перейдем Настройка – WAN - выбрать HSI, нажать изменить, включить/отключить IPv6.



После завершения конфигурации, кнопка «Сохранить», кнопка «Применить».

3.34 Для работы сторонней SIP телефонии

1. Необходимо в Настройка – NAT – ALG, отключить SIP ALG.
   Схема переходов ниже:



4. Характеристики устройства

Устройство ONT RV6699 — терминал оптической сети GPON. Терминал реализует функции оконечного абонентского оборудования широкополосного доступа FTTH, выполненный в соответствии с рекомендацией ITU-T G.984.

Описание устройства

PON	SFF, одномодовый разъём SC/APC
Gigabit Ethernet	4*10/100/1000Base-T Gigabit Ethernet порта с разъёмами RJ-45
POTS	FXS порт с разъёмом RJ-11
Wireless	Беспроводная точка доступа: 802.11n в диапазоне 2,4Ггц 802.11ac в диапазоне 5Ггц
USB	Порт USB 2.0
Размеры, мм (Ш×Г×В)	205 × 165 × 44

Характеристики оптического интерфейса

Стандарт	Class B+ ITU-T G.984.2
Диапазон	До 20 км, в зависимости от расслоения и с учётом стандартных потерь
Разъём	Одномодовый SC/APC
Тип оптического волокна	G.652
Уровень выходного сигнала, Дб	Мин: +0,5 dBm Макс: +5,0 dBm
Минимальная чувствительность приемника	–28,0 dBm
Макс уровень (приемник)	–8,0 dBm

Электрические характеристики

Разъёмы	Для подключения к адаптеру постоянного тока: круглый разъём 2,1 мм. Адаптер поставляется вместе с устройством.
Адаптер	Вх. AC 110~240V / 50~60 Hz Вых. 12 V DC, 2 A
Номинальное энергопотребление	Менее 20 Вт

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, обращайтесь в Единый контактный центр МГТС по телефону **8 495 636-0-636**.

Примечание: производитель сохраняет за собой право изменять любую информацию, технические характеристики и комплектацию без предварительного уведомления и обязательств.