

Абонентские оптические терминалы

NTE-RG-1421G-Wac

NTE-RG-1421G-WZ

Руководство по эксплуатации

Версия ПО 3.16.6

IP-адрес: <http://192.168.0.1>

имя пользователя: user

пароль: user

Текущая версия ПО: 3.16.6

Версия документа	Актуальность для ПО	Дата выпуска	Содержание изменений
Версия 4.0	3.16.6	21.20.2021	Синхронизация с версией ПО 3.16.6
Версия 3.0	3.16.2	05.12.2018	Добавлено описание устройства NTE-RG-1421G-WZ
Версия 2.0	3.16.1.624	20.04.2018	Вторая публикация
Версия 1.0	3.16.0.2124	30.03.2017	Первая публикация

ПРИМЕЧАНИЯ И ПРЕДУПРЕЖДЕНИЯ

Примечания содержат важную информацию, советы или рекомендации по использованию и настройке устройства.



Предупреждения информируют пользователя о ситуациях, которые могут нанести вред устройству или человеку, привести к некорректной работе устройства или потере данных.

СОДЕРЖАНИЕ

1	ВВЕДЕНИЕ	5
2	ОПИСАНИЕ ИЗДЕЛИЯ.....	6
2.1	Назначение	6
2.2	Характеристики устройств	7
2.3	Основные технические параметры.....	9
2.4	Конструктивное исполнение	12
2.5	Перезагрузка/сброс к заводским настройкам.....	14
2.6	Комплект поставки	14
3	АРХИТЕКТУРА УСТРОЙСТВ.....	15
3.1	Архитектура NTE-RG-1421G-Wac и NTE-RG-1421G-WZ	15
4	НАСТРОЙКА NTE-RG-1421G-WAC И NTE-RG-1421G-WZ ЧЕРЕЗ WEB-ИНТЕРФЕЙС. ДОСТУП ПОЛЬЗОВАТЕЛЯ.....	17
4.1	Меню « <i>Device Info</i> ». Информация об устройстве.....	18
4.1.1	Подменю « <i>Summary</i> ». Общая информация об устройстве	18
4.1.2	Подменю « <i>WAN</i> ». Информация о состоянии сервисов.....	18
4.1.2.1	Подменю « <i>General</i> ». Общая информация.....	18
4.1.2.2	Вкладка « <i>Detail</i> ». Подробная информация	19
4.1.3	Подменю « <i>LAN</i> ». Мониторинг состояния портов LAN. Мониторинг статуса Wi-Fi интерфейса.....	19
4.1.4	Подменю « <i>Statistics</i> ». Информация о прохождении трафика на портах устройства.....	20
4.1.5	Подменю « <i>Route</i> ». Просмотр таблицы маршрутизации	20
4.1.6	Подменю « <i>ARP</i> ». Просмотр кэша протокола ARP	21
4.1.7	Подменю « <i>DHCP</i> ». Активные аренды DHCP	21
4.1.8	Подменю « <i>Wireless Stations</i> ». Подключенные беспроводные устройства.....	22
4.1.9	Подменю « <i>Wireless Monitor</i> ». Обнаруженные беспроводные сети	22
4.1.10	Подменю « <i>Voice</i> ». Мониторинг состояния телефонных портов	23
4.2	Меню « <i>Advanced Setup</i> ». Расширенные настройки конфигурации	24
4.2.1	Подменю « <i>LAN</i> ». Настройка основных параметров	24
4.2.2	Подменю « <i>VLAN Settings</i> ». Настройка параметров VLAN.....	25
4.2.2.1	Подменю « <i>Port Mapping</i> ». Настройки распределения портов и услуг	25
4.2.3	Подменю « <i>PPPoE</i> ». Настройки PPP.....	26
4.2.4	Подменю « <i>NAT</i> ». Настройки NAT	26
4.2.4.1	Подменю « <i>Virtual Servers</i> ». Настройки виртуальных серверов.....	26
4.2.4.2	Подменю « <i>Port Triggering</i> ». Настройки запуска портов	28
4.2.4.3	Подменю « <i>DMZ Host</i> ». Настройки демилитаризованной зоны	29
4.2.5	Подменю « <i>Security</i> ». Настройки безопасности.....	29
4.2.5.1	Подменю « <i>IP Filtering</i> ». Настройки фильтрации адресов	29
4.2.5.2	Подменю « <i>MAC Filtering</i> ». Настройки фильтрации по MAC-адресам.....	32
4.2.6	Подменю « <i>Parental control</i> ». «Родительский контроль» – настройки ограничения	33
4.2.6.1	Подменю « <i>Time Restriction</i> ». Настройки ограничения продолжительности сеансов	33
4.2.6.2	Подменю « <i>URL Filter</i> ». Настройки ограничения доступа в интернет	34
4.2.7	Подменю « <i>Dynamic DNS</i> ». Настройки динамической системы доменных имен.....	34
4.2.8	Меню « <i>Print Server</i> ». Настройки сервера печати	36
4.2.9	Подменю « <i>Z-WAVE</i> ».....	37
4.2.10	Подменю « <i>UPnP</i> ». Автоматическая настройка сетевых устройств	37
4.3	Меню « <i>Voice</i> ». Настройки телефонии SIP	38
4.3.1	Подменю « <i>SIP Basic Settings</i> ». Общие настройки SIP.....	38
4.3.2	Подменю « <i>SIP Advanced Settings</i> ». Дополнительные настройки SIP.....	39
4.4	Меню « <i>Wireless</i> ». Настройка беспроводной сети	41
4.4.1	Подменю « <i>Basic</i> ». Общая информация	41
4.4.2	Подменю « <i>Security</i> ». Настройка параметров безопасности.....	42
4.4.3	Подменю « <i>MAC Filter</i> ». Настройки фильтрации MAC-адресов.....	45
4.4.4	Подменю « <i>Bridge</i> ». Настройки беспроводного соединения в режиме моста	46

4.4.5	Подменю «Advanced». Расширенные настройки	47
4.5	Меню «Storage Service». Службы файловых хранилищ	49
4.5.1	Подменю «Storage Device Info». Информация о подключенных USB-устройствах	49
4.5.2	Подменю «User Accounts». Настройка пользователей Samba	49
4.6	Меню «Management». Управление устройством	50
4.6.1	Подменю «Settings». Настройки	50
4.6.1.1	Подменю «Backup». Резервное копирование	50
4.6.1.2	Подменю Update. Обновление конфигурации.....	50
4.6.1.3	Подменю «Restore Default». Возврат к настройкам по умолчанию	50
4.6.2	Подменю «Internet Time». Настройки системного времени	51
4.6.3	Подменю «Ping». Проверка доступности сетевых устройств	51
4.6.4	Подменю «Passwords». Настройка контроля доступа (установка паролей).....	52
4.6.5	Подменю «System Log». Просмотр и настройка системного журнала	52
4.6.5.1	Подменю «Configuration». Настройка системного журнала	52
4.6.5.2	Подменю «View». Просмотр системного журнала	53
4.6.6	Подменю «Update Software». Обновление ПО.....	53
4.6.7	Подменю «Reboot». Перезагрузка устройства	54
ПРИЛОЖЕНИЕ А. ВОЗМОЖНЫЕ ПРОБЛЕМЫ И ВАРИАНТЫ ИХ РЕШЕНИЯ		55
ПРИЛОЖЕНИЕ Б. ИСПОЛЬЗОВАНИЕ ДОПОЛНИТЕЛЬНЫХ УСЛУГ.....		56
ТЕХНИЧЕСКАЯ ПОДДЕРЖКА		58

1 ВВЕДЕНИЕ

Сеть Turbo GPON относится к одной из разновидностей пассивных оптических сетей PON, базирующихся на технологиях Ethernet. Это одно из самых современных и эффективных решений задач «последней мили», позволяющее существенно экономить на кабельной инфраструктуре и обеспечивающее скорость передачи информации до 2,5 Гбит/с в направлении downlink и 1,25 Гбит/с в направлении uplink. Использование в сетях доступа решений на базе технологии GPON дает возможность предоставлять конечному пользователю доступ к новым услугам на базе протокола IP совместно с традиционными сервисами.

Основным преимуществом GPON является использование одного станционного терминала (OLT) для нескольких абонентских устройств (ONT). OLT является конвертором интерфейсов Gigabit Ethernet и GPON, служащим для связи сети PON с сетями передачи данных более высокого уровня. ONT предназначено для подключения к услугам широкополосного доступа оконечного оборудования клиентов. Может применяться в жилых комплексах и бизнес-центрах.

ONT *NTE-RG-1421G-Wac* и *NTE-RG-1421G-WZ* рассчитаны на **четыре UNI-интерфейса 10/100/1000BASE-T** и поддержку интерфейсов FXS, Wi-Fi, USB.

В настоящем руководстве по эксплуатации изложены назначение, основные технические характеристики, правила конфигурирования, мониторинга и смены программного обеспечения оптических терминалов *NTE-RG-1421G-Wac* и *NTE-RG-1421G-WZ*.

2 ОПИСАНИЕ ИЗДЕЛИЯ

2.1 Назначение

Устройства *NTE-RG-1421G-Wac* и *NTE-RG-1421G-WZ* GEPON ONT (Gigabit Ethernet Passive Optical Network) обеспечивают соединение по оптическому каналу с устройством GEPON класса OLT (оптическое терминальное оборудование) и соединение до 10/100/1000 Мбит/с с конечным пользователем LAN. Главным преимуществом технологии Turbo GEPON является оптимальное использование полосы пропускания. Эта технология является следующим шагом для обеспечения новых высокоскоростных интернет-приложений дома и в офисе. Разработанные для развертывания сети внутри дома или здания, данные устройства ONT обеспечивают надежное соединение с высокой пропускной способностью на дальние расстояния для пользователей, живущих и работающих в удаленных многоквартирных зданиях и бизнес-центрах.

Благодаря встроенному маршрутизатору устройства обеспечивают возможность подключения оборудования локальной сети к сети широкополосного доступа. Терминалы обеспечивают защиту межсетевым экраном для компьютеров в сети от атак DoS и вирусных атак, осуществляют фильтрацию пакетов для осуществления управления доступом на основе портов и MAC/IP-адресов источника/назначения. Пользователи могут настроить домашний или офисный web-сайт, добавив один из LAN-портов в зону DMZ. Функция «Родительский контроль» обеспечивает фильтрацию web-сайтов с нежелательным содержанием, блокировку доменов и позволяет задавать расписание использования интернета. Виртуальная частная сеть (VPN) предоставляет мобильным пользователям и филиалам защищенный канал связи для подключения к корпоративной сети.

Порт FXS позволяет пользоваться услугами IP-телефонии, предоставляя множество полезных функций, таких как отображение идентификатора звонящего, трехстороннюю конференцию, телефонную книгу, ускоренный набор. Все это обеспечивает удобство пользователя при наборе номера и приеме телефонных звонков.

Порты USB могут использоваться для подключения USB-устройств (USB flash-накопитель, внешний HDD).

Абонентские маршрутизаторы *NTE-RG-1421G-Wac* и *NTE-RG-1421G-WZ* позволяют подключать клиентов Wi-Fi по стандарту IEEE 802.11b/g/n, поддерживают стандарт 802.11ac, что обеспечивает рекордную скорость передачи данных до 1 Гбит/с и позволяют доставлять современные высокоскоростные сервисы клиентскому оборудованию по беспроводной сети.

Устройства позволяют подключать клиентов Wi-Fi по стандартам IEEE 802.11a/b/g/n/ac. Поддержка стандарта 802.11ac обеспечивает скорость передачи данных до 1,3 Гбит/с и позволяет доставлять современные высокоскоростные сервисы клиентскому оборудованию по беспроводной сети. Два встроенных контроллера Wi-Fi сети позволяют обеспечить работу устройства одновременно в двух частотных диапазонах — 2,4 ГГц и 5 ГГц.

2.2 Характеристики устройств

Устройства NTE-RG-1421G-Wac и NTE-RG-1421G-WZ имеют следующие интерфейсы:

- 1 порт RJ-11 для подключения аналоговых телефонных аппаратов;
- 1 порт PON SC/APC для подключения к сети оператора;
- 4 порта Ethernet RJ-45 LAN для подключения сетевых устройств 10/100/1000BASE-T;
- Приемопередатчик Wi-Fi 802.11a/b/g/n/ac;
- 2 порта USB 2.0 — для подключения внешних накопителей USB или HDD;
- Интерфейс системы управления "Умный дом"¹.

Питание терминалов осуществляется через внешний адаптер от сети 220 В/12 В.

Устройства поддерживают следующие функции:

- *сетевые функции:*
 - работа в режиме «моста» или «маршрутизатора»;
 - поддержка PPPoE (PAP-, CHAP-, MSCHAP-авторизация);
 - поддержка статического адреса и DHCP (DHCP-клиент на стороне WAN, DHCP-сервер на стороне LAN);
 - поддержка UPnP;
 - поддержка IPSec;
 - поддержка NAT;
 - поддержка Firewall;
 - поддержка NTP;
 - поддержка механизмов качества обслуживания QoS;
 - поддержка IGMP snooping;
 - поддержка IGMP proxy;
 - поддержка функции Parental Control;
 - поддержка функции Storage service.
- *Wi-Fi:*
 - поддержка стандартов 802.11a/b/g/n/ac;
 - одновременная работа в двух диапазонах: 2,4 ГГц и 5 ГГц;
- *IP-телефония:*
 - поддержка протокола SIP;
 - аудиокодеки: G.729 (A), G.711 (A/U), G.723.1;
 - ToS для пакетов RTP;
 - ToS для пакетов SIP;
 - эхокомпенсация (рекомендации G.164, G.165);
 - детектор тишины (VAD);
 - генератор комфортного шума;
 - обнаружение и генерирование сигналов DTMF;
 - передача DTMF (INBAND, RFC2833, SIP INFO);
 - передача факса: upspeed/pass-through. G.711, T.38;
- *функции ДВО:*
 - удержание вызова — Call Hold;
 - передача вызова — Call Transfer;
 - уведомление о поступлении нового вызова — Call Waiting;

¹Функция реализована только в NTE-RG-1421G-WZ

- безусловная переадресация — Forward unconditionally;
 - переадресация по неответу — Forward on «no answer»;
 - переадресация по занятости — Forward on «busy»;
 - определитель номера Caller ID по ETSI FSK;
 - запрет выдачи Caller ID (анонимный звонок) — Anonymous calling;
 - теплая линия — Warmline;
 - гибкий план нумерации;
 - индикация о наличии сообщений на голосовой почте — MWI;
 - блокировка анонимных звонков — Anonymous call blocking;
 - запрет на исходящие вызовы — Call Barring;
 - "не беспокоить" — DND.
- обновление ПО через web-интерфейс, TR-069;
 - удаленный мониторинг, конфигурирование и настройка:
 - TR-069;
 - Web-интерфейс;
 - Telnet.

На рисунках 1, 2 приведены схемы применения оборудования NTE-RG-1421G-Wac и NTE-RG-1421G-WZ.

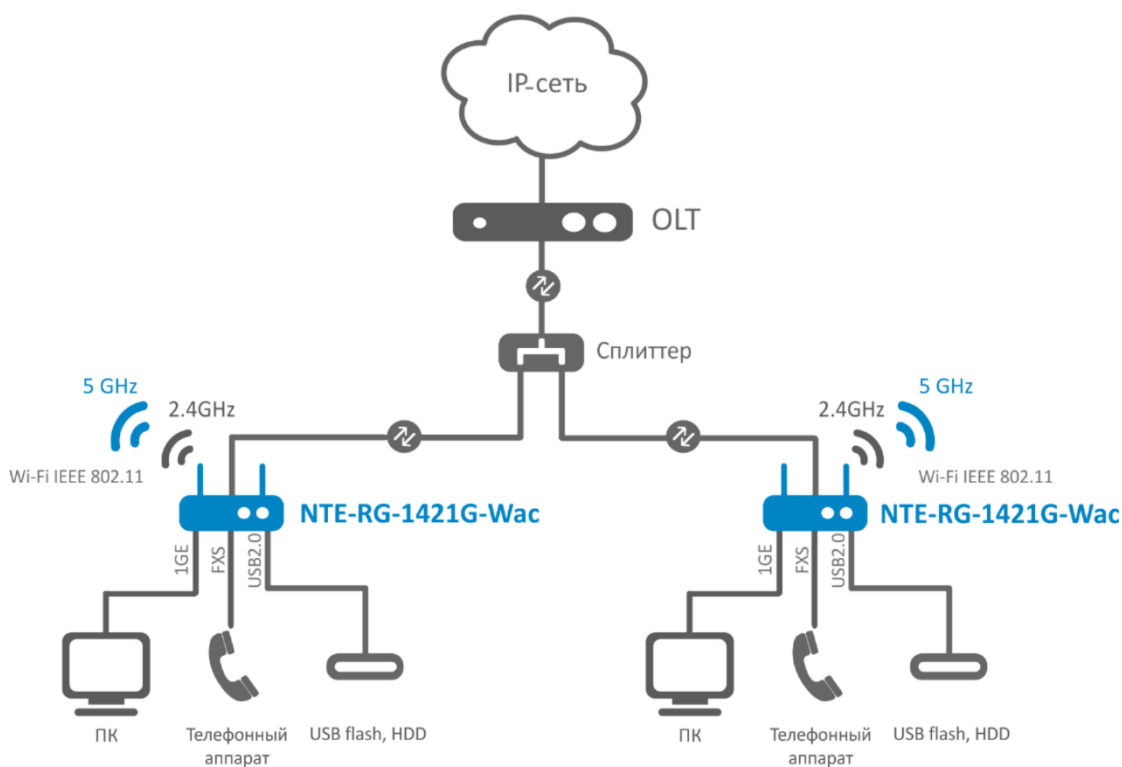


Рисунок 1 — Схема применения NTE-RG-1421G-Wac

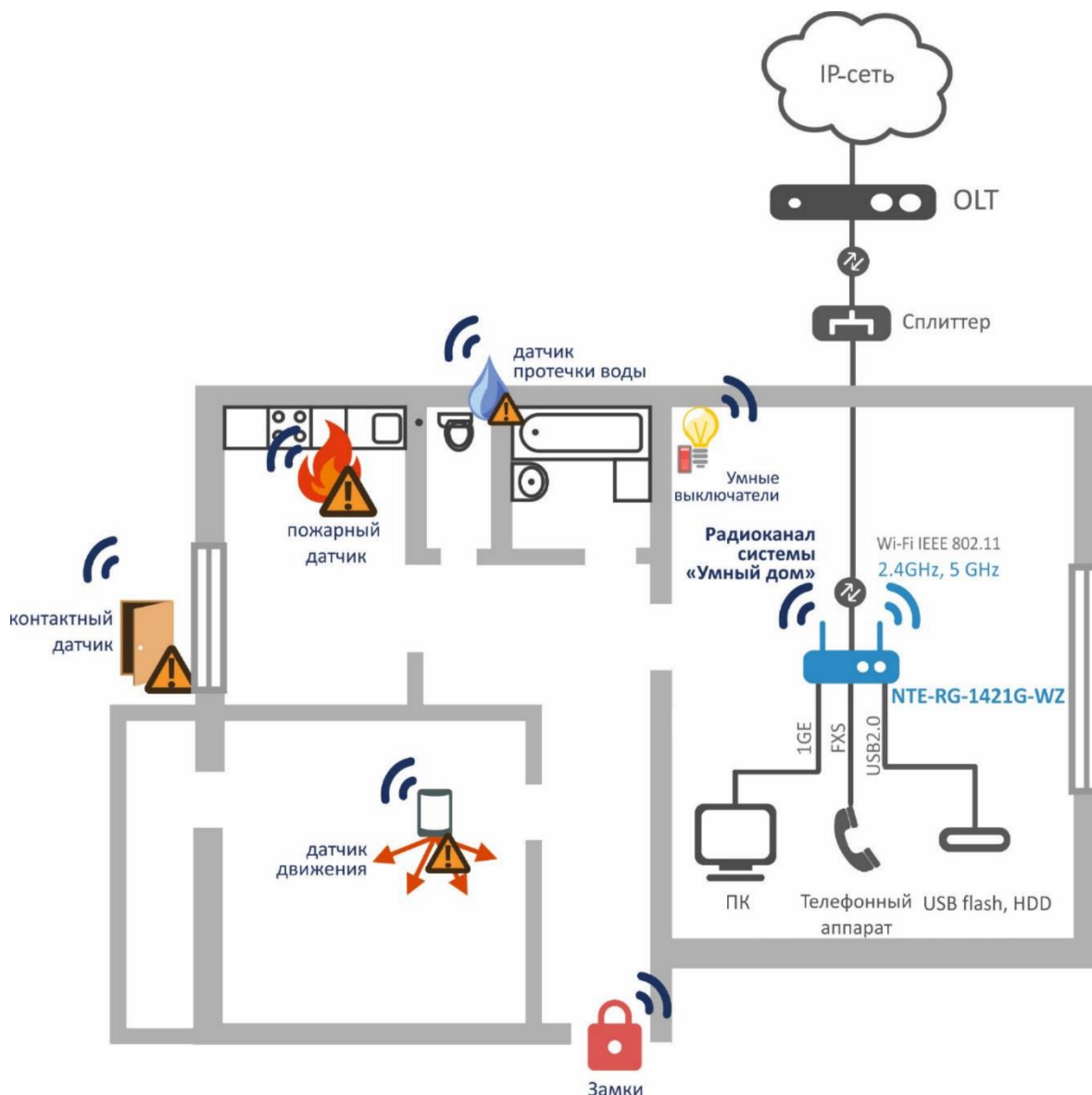


Рисунок 2 — Схема применения NTE-RG-1421G-WZ

2.3 Основные технические параметры

Основные технические параметры терминалов приведены в таблице 1.

Таблица 1 — Основные технические параметры

Протоколы VoIP

Поддерживаемые протоколы	SIP
--------------------------	-----

Аудиокодеки

Кодеки	G.729, annex A G.711(A/μ) G.723.1 (5,3 кбит/с) Передача факса: G.711, T.38
--------	---

Параметры интерфейсов Ethernet LAN

Количество интерфейсов	4
Электрический разъем	RJ-45

Скорость передачи	Автоопределение, 10/100/1000 Мбит/с, дуплекс/ полудуплекс
Поддержка стандартов	IEEE 802.3i 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3x Flow Control IEEE 802.3 NWay auto-negotiation

Параметры интерфейса PON

Количество интерфейсов PON	1
Поддержка стандартов	IEEE 802.3ah EPON IEEE 802.3z Gigabit Ethernet IEEE 802.1Q Tagged VLAN IEEE 802.1p Priority Queues IEEE 802.1D Spanning Tree Protocol
Тип разъема	SC/APC соответствует ITU-T G.984.2
Среда передачи	Оптоволоконный кабель SMF — 9/125, G.652
Коэффициент разветвления	До 1:128
Максимальная дальность действия	20 км
Передатчик:	1310 нм
Скорость соединения upstream	1244 Мбит/с
Мощность передатчика	От +0,5 до +5 дБм
Ширина спектра опт. излучения (RMS)	1 нм
Приемник	1490 нм
Скорость соединения downstream	2488 Мбит/с
Чувствительность приемника	От -8 до -28 дБм

Параметры аналогового абонентского порта

Количество портов	1
Сопrotивление шлейфа	До 2 кОм
Прием набора	Импульсный/частотный (DTMF)
Выдача Caller ID	Есть

Параметры беспроводного интерфейса Wi-Fi

Стандарт	802.11a/b/g/n/ac
Частотный диапазон	2400 ~ 2483,5 МГц, 5150 ~ 5350 МГц, 5650 ~ 5850 МГц Одновременная работа в двух частотных диапазонах (Simultaneous Dual Band)
Модуляция	CCK, BPSK, QPSK, 16 QAM, 64 QAM, 256 QAM
Скорость передачи данных	802.11b: 1; 2; 5,5 и 11 Мбит/с 802.11g: 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с 802.11n: 150 Мбит/с (канал 20 МГц), 300 Мбит/с (канал 40 МГц) 802.11ac: 1300 Мбит/с (80 МГц)
Максимальная выходная мощность передатчика	802.11b: 17 дБм +/-1.5 дБм 802.11g: 15 дБм +/-1.5 дБм 802.11n: 14.75 дБм +/-1.5 дБм 802.11ac: (5 ГГц): 19 дБм
MAC-протокол	CSMA/CA модель AСK 32 MAC
Безопасность	64/128-битное WEP-шифрование данных; WPA, WPA2 802.1xAES+TKIP
Поддержка операционной системы	Windows XP 32/64, Windows Vista 32/64, Windows 2000, Windows 7 32/64 Linux, VxWorks

Количество антенн	2,4 ГГц	2
	5 ГГц	3
Коэффициент усиления антенны	5 дБи	
Рабочий диапазон температур	От 0 до +70 °С	

Управление

Локальное управление	Web-интерфейс
Удаленное управление	Telnet, TR-069
Обновление программного обеспечения	TR-069, HTTP, TFTP
Ограничение доступа	По паролю

Общие параметры

Питание	Адаптер питания 12 В DC /220 В AC
Потребляемая мощность	Не более 15 Вт
Рабочий диапазон температур	От +5 до +40 °С
Относительная влажность	До 80%
Габариты (ШхВхГ)	187х32х120 мм
Масса	0,3 кг

2.4 Конструктивное исполнение

Абонентские терминалы *NTE-RG-1421G-Wac*, *NTE-RG-1421G-WZ* выполнены в виде настольного изделия в пластиковом корпусе.

Внешний вид задней панели устройств приведен на рисунке 3.

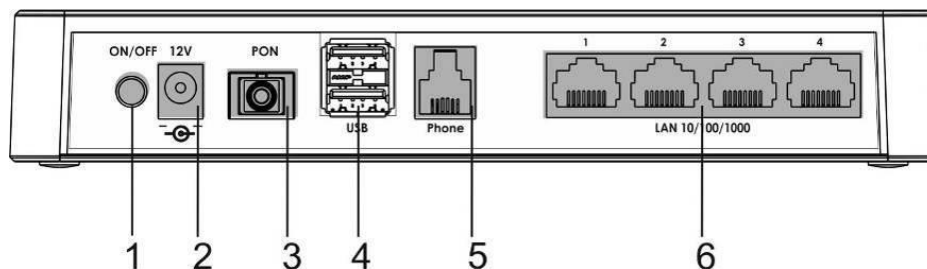


Рисунок 3 — Внешний вид задней панели *NTE-RG-1421G-Wac* и *NTE-RG-1421G-WZ*

На задней панели устройства расположены следующие разъемы и органы управления, таблица 2.

Таблица 2 — Описание разъемов, и органов управления задней панели

№	Элемент задней панели	Описание
1	<i>On/Off</i>	Кнопка питания
2	<i>12V</i>	Разъем подключения адаптера питания
3	<i>PON</i>	Разъем SC (розетка) PON оптического интерфейса GEPON
4	<i>USB</i>	2 разъема для подключения внешних накопителей и других USB-устройств
5	<i>Phone</i>	Разъем RJ-11 для подключения аналоговых телефонных аппаратов
6	<i>LAN 10/100/1000 [1..4]</i>	4 разъема RJ-45 для подключения сетевых устройств

Внешний вид боковой и верхней панелей устройств приведен на рисунке 4.

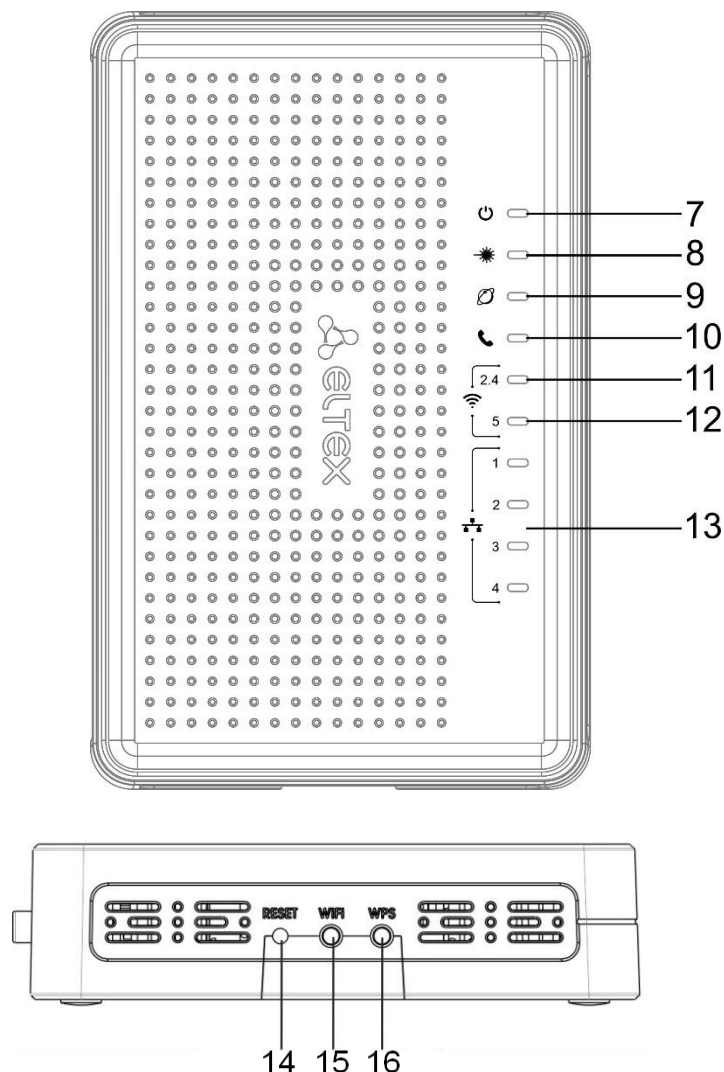







Рисунок 4 — Внешний вид боковой и верхней панелей NTE-RG-1421G-Wac и NTE-RG-1421G-WZ

На верхней панели устройства расположены следующие индикаторы, таблица 3.

Таблица 3 — Описание индикаторов верхней панели

№	Элемент верхней панели		Состояние	Описание
7		Индикатор питания и статуса работы	Не горит	Устройство отключено от сети питания или неисправно
			Красный	Возникли проблемы при загрузке устройства
			Зеленый	Процесс загрузки завершен, на устройстве установлена конфигурация, отличная от конфигурации по умолчанию
			Оранжевый	Процесс загрузки завершен, на устройстве установлена конфигурация по умолчанию
8		Индикатор работы оптического интерфейса	Не горит	Процесс загрузки устройства
			Зеленый	Установлено соединение между стационарным оптическим терминалом и устройством
			Мигает красным	Нет сигнала от стационарного оптического терминала

9		Индикатор состояния сервиса «Интернет»	Не горит	Интерфейс с признаком «Интернет» не сконфигурирован
			Зеленый	Интерфейс с признаком «Интернет» сконфигурирован, на нем получен IP-адрес
			Оранжевый	Интерфейс с признаком «Интернет» сконфигурирован, но IP-адрес на нем не получен
			Мигает зеленым	Процесс обновления ПО на устройстве
10		Индикатор активности порта FXS	Горит	Телефонная трубка снята
			Мигает	Порт не зарегистрирован или не пройдена авторизация на SIP-сервере
			Медленно мигает	Прием сигнала вызова
11		Индикатор активности Wi-Fi в диапазоне 2,4 ГГц	Зеленый	Сеть Wi-Fi активна
			Мигает	Процесс передачи данных по Wi-Fi
			Не горит	Сеть Wi-Fi не активна
12		Индикатор активности Wi-Fi в диапазоне 5 ГГц	Зеленый	Сеть Wi-Fi активна
			Мигает	Процесс передачи данных по Wi-Fi
			Не горит	Сеть Wi-Fi не активна
13		Индикаторы работы Ethernet-портов	Зеленый	Установлено соединение 10/100 Мбит/с
			Оранжевый	Установлено соединение 1000 Мбит/с
			Мигает	Процесс пакетной передачи данных

На боковой панели устройства расположены следующие кнопки, таблица 4.

Таблица 4 — Описание кнопок боковой панели

№	Элемент боковой панели	Описание
14	Reset	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам
15	Wi-Fi	Кнопка включения/выключения Wi-Fi
16	WPS	Кнопка для автоматического защищенного подключения к сети Wi-Fi на устройстве

2.5 Перезагрузка/сброс к заводским настройкам

Для перезагрузки устройства нужно однократно нажать кнопку «Reset» на боковой панели изделия. Для загрузки устройства с заводскими настройками необходимо нажать и удерживать кнопку «Reset» 7-10 секунд, пока индикатор *POWER* не загорится красным светом. При заводских установках IP-адрес: LAN — 192.168.0.1, маска подсети — 255.255.255.0. Доступ возможен с портов LAN 1 и LAN 2.

2.6 Комплект поставки

В базовый комплект поставки устройства *NTE-RG-1421G-Wac* и *NTE-RG-1421G-WZ* входят:

- Абонентский оптический терминал;
- Адаптер питания 220 В/12 В;
- Руководство по установке и первичной настройке.
- Памятка о документации.

3 АРХИТЕКТУРА УСТРОЙСТВ

3.1 Архитектура NTE-RG-1421G-Wac и NTE-RG-1421G-WZ

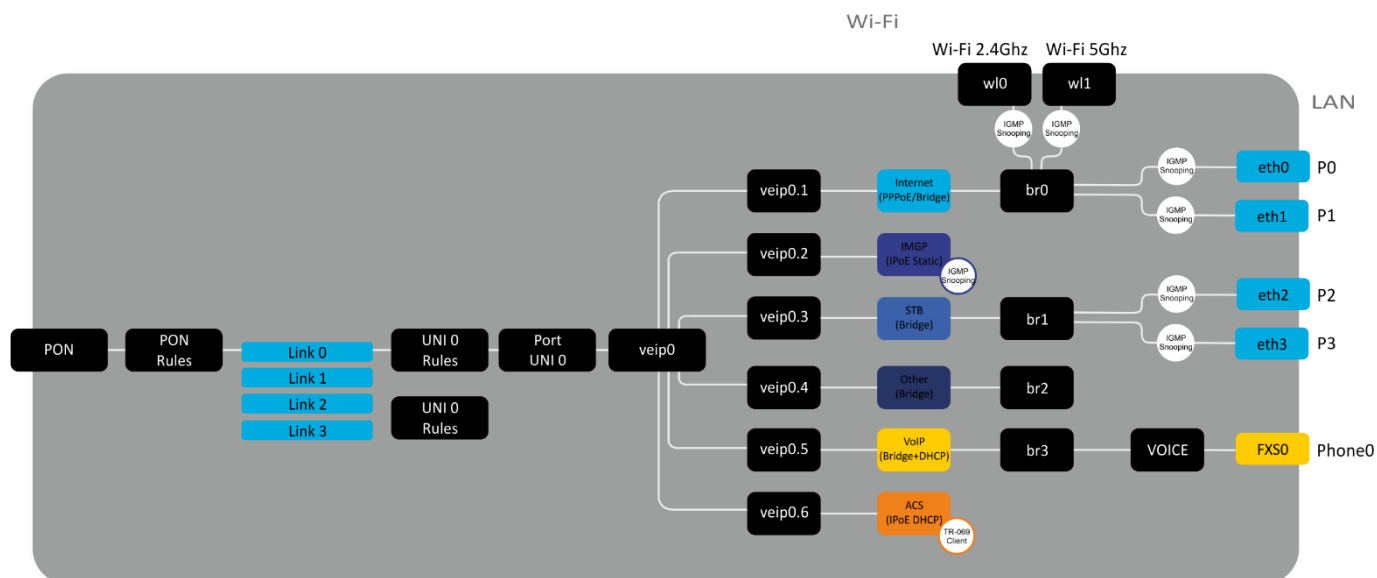


Рисунок 5 — Логическая архитектура устройства с заводской конфигурацией

Процессор логически состоит из следующих блоков: **Internet**, **IGMP**, **STB**, **Other**, **VoIP**, **ACS**. Для каждого блока назначена своя VLAN, в которой передаются пакеты установленной услуги.

Блоки процессора

- **Блок ACS** работает в режиме IPoE DHCP (получение адреса автоматически по протоколу DHCP). Блок используется для удаленного управления устройством с помощью сервера ACS (Auto Configuration Server — сервер автоконфигурации абонентских устройств). Из Option 43, полученной от DHCP-сервера, могут быть получены параметры ACS-сервера.
- **Блок VoIP** работает в режиме bridge+DHCP. На данный интерфейс подключается VOICE-приложение, через которое осуществляется предоставление услуг телефонии.
- **Блок Other** работает в режиме bridge и служит для подключения дополнительных видов услуг для пользователя. Через данный блок пакеты проходят без модификации.
- **Блок STB** работает в режиме bridge и служит для подключения телевизионных приставок STB пользователя. Через данный блок проходит трафик VoD и загрузка STB. Пакеты проходят без модификации.
- **Блок IGMP** используется для работы IGMP проху.
- **Блок Internet** работает в режиме PPP-клиента и служит для предоставления пользователю доступа в сеть Интернет.

Блок br0 предназначен для объединения портов LAN в одну группу для предоставления доступа в блок **Internet**.

Блоки eth0..3 физически являются Ethernet-портами с разъемом RJ-45 для подключения ПК, STB или других сетевых устройств. Логически включены в блок **br0** и **br1**.

Блок FXS0 физически является портом с разъемом RJ-11 для подключения аналоговых телефонных аппаратов. Логически включен в блок **VOICE**. Управление блоком **VOICE** может осуществляться через web-интерфейс, а также удаленно с помощью сервера ACS по протоколу TR-069. В данном блоке задаются параметры сервиса VoIP (адрес SIP-сервера, номера телефонных аппаратов, услуги ДВО и т.д).

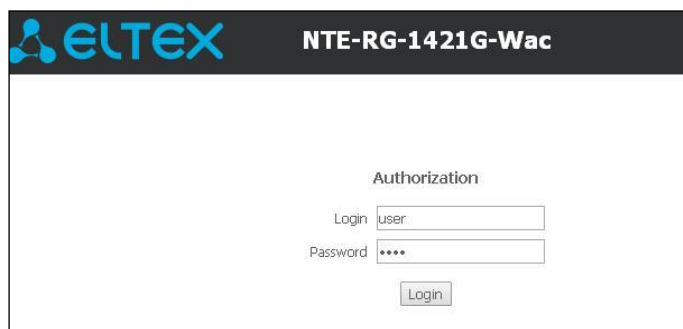
Блоки wl0 и wl1 являются интерфейсами для подключения Wi-Fi модуля 2,4 и 5 ГГц соответственно.

Управление блоками с **PON** до **Port UNI0** осуществляется по протоколу OAM со стороны OLT.

4 НАСТРОЙКА NTE-RG-1421G-WAC И NTE-RG-1421G-WZ ЧЕРЕЗ WEB-ИНТЕРФЕЙС. ДОСТУП ПОЛЬЗОВАТЕЛЯ

Для того чтобы произвести конфигурирование устройства, необходимо подключиться к нему через web-браузер (программу для просмотра гипертекстовых документов), например, Firefox, Google Chrome. Для этого необходимо ввести в адресной строке браузера IP-адрес устройства (при заводских установках IP-адрес: LAN — 192.168.0.1, маска подсети — 255.255.255.0).

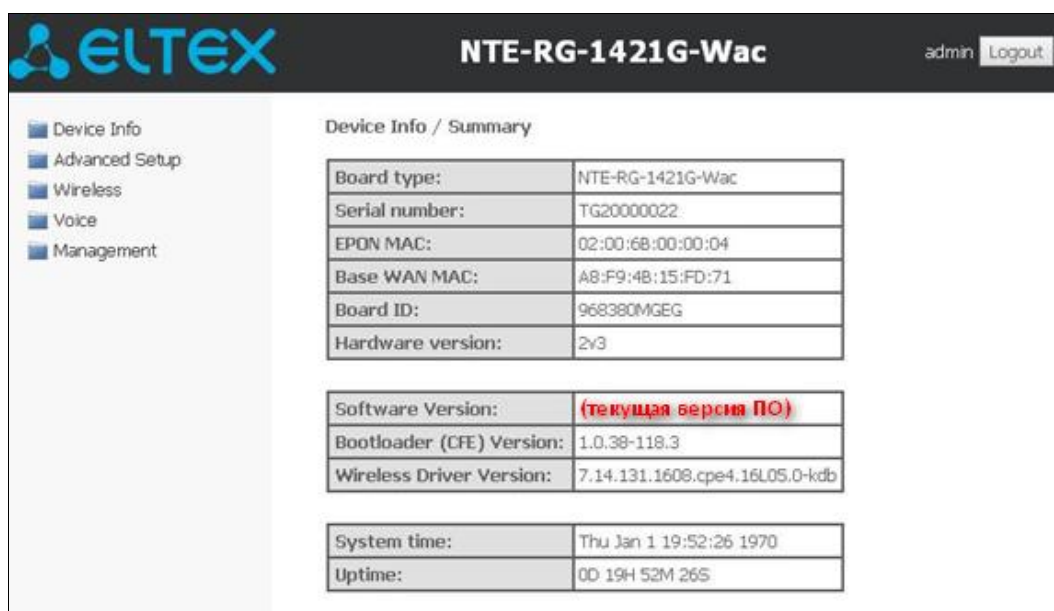
После введения IP-адреса устройство запросит имя пользователя и пароль.



Имя пользователя *user*, пароль *user*.

Во избежание несанкционированного доступа при дальнейшей работе с устройством рекомендуется изменить пароль (раздел 4.6.4 Подменю «Passwords». Настройка контроля доступа (установление паролей)).

Ниже представлен общий вид окна конфигурирования устройства. Слева расположено дерево навигации по меню настроек объектов, справа — область редактирования параметров.



Device Info / Summary	
Board type:	NTE-RG-1421G-Wac
Serial number:	TG20000022
EPON MAC:	02:00:68:00:00:04
Base WAN MAC:	A8:F9:4B:15:FD:71
Board ID:	968380MGEG
Hardware version:	2v3
Software Version:	(текущая версия ПО)
Bootloader (CFE) Version:	1.0.38-118.3
Wireless Driver Version:	7.14.131.1608.cpe4.16L05.0-kdb
System time:	Thu Jan 1 19:52:26 1970
Uptime:	00:19H 52M 26S

4.1 Меню «Device Info». Информация об устройстве

4.1.1 Подменю «Summary». Общая информация об устройстве

Device Info / Summary	
Board type:	NTE-RG-1421G-Wac
Serial number:	TG20000022
EPON MAC:	02:00:68:00:00:04
Base WAN MAC:	A8:F9:4B:15:FD:71
Board ID:	968380MGEg
Hardware version:	2v3
Software Version:	(текущая версия ПО)
Bootloader (CFE) Version:	1.0.38-118.3
Wireless Driver Version:	7.14.131.1608.cpe4.16L05.0-kdb
System time:	Thu Jan 1 19:52:26 1970
Uptime:	00 19H 52M 26S

- *Board type* — модель устройства;
- *Serial number* — серийный номер устройства;
- *EPON MAC* — EPON MAC-адрес устройства;
- *Base WAN MAC* — WAN MAC-адрес устройства;
- *Board ID* — идентификатор платы;
- *Hardware Version* — версия аппаратного обеспечения;

- *Software Version* — версия ПО;
- *Bootloader (CFE) Version* — версия начального загрузчика;
- *Wireless Driver Version* — версия адаптера Wi-Fi;

- *System time* — текущее время на устройстве;
- *Uptime* — время работы устройства с момента последней перезагрузки.

4.1.2 Подменю «WAN». Информация о состоянии сервисов

4.1.2.1 Подменю «General». Общая информация

Device Info / WAN / General									
Interface	Description	Type	VlanMuxId	Igmp Pxy	Igmp Src Enbl	NAT	Firewall	Status	IPv4 Address
veip0.2	IGMP	IPoE	2	Enabled	Enabled	Disabled	Disabled	Connected	192.168.21.21
veip0.3	STB	Bridge	3	Disabled	Disabled	Disabled	Disabled	Connected	1.2.3.4
veip0.4	OTHER	Bridge	4	Disabled	Disabled	Disabled	Disabled	Connected	0.0.0.0
veip0.5	VOIP	Bridge	5	Disabled	Disabled	Disabled	Disabled	Connected	192.168.101.92
veip0.6	Tr069	IPoE	4094	Disabled	Disabled	Disabled	Disabled	Connected	192.168.211.89
ppp0.1	INTERNET	PPPoE	1	Disabled	Disabled	Enabled	Enabled	Connected	192.168.100.102

В данном подменю выводится общая информация о существующих конфигурациях интерфейса WAN.

4.1.2.2 Вкладка «Detail». Подробная информация

В данном подменю выводится подробная информация о существующих конфигурациях интерфейса WAN.

Для просмотра доступна следующая информация о сервисах:

- *Interface* — имя интерфейса;
- *Type* — режим работы интерфейса;
- *Connection type* — тип подключения;
- *NAT* — статус NAT;
- *Firewall* — статус Firewall;
- *Status* — статус соединения;
- *IPv4 Address* — адрес для доступа;
- *Primary DNS Server*¹ — адрес первичного DNS-сервера, используемого для работы;
- *Secondary DNS Server*¹ — адрес вторичного DNS-сервера, используемого для работы;
- *Bridging to* — список связанных LAN-интерфейсов;
- *Default Gateway* — шлюз по умолчанию.

Device Info / WAN / Detail

WAN service 0: INTERNET

Interface: ppp0.1
 Type: PPPoE
 Connection type: IP_Routed
 NAT: Enabled
 Firewall: Enabled
 Status: Connected
 IPv4 Address: 192.168.100.102
 Primary DNS Server: 192.168.100.1
 Secondary DNS Server: 10.10.0.2
 Bridging to: eth0.0,eth1.0,wl0,wl1

WAN service 1: IGMP

Interface: veip0.2
 Type: IPoE
 Connection type: IP_Routed
 Status: Connected
 IPv4 Address: 192.168.21.21
 Default Gateway: 192.168.21.1

4.1.3 Подменю «LAN». Мониторинг состояния портов LAN. Мониторинг статуса Wi-Fi интерфейса

В данном подменю доступен просмотр статусов и характеристик проводных и беспроводных интерфейсов LAN. Для проводных соединений указан статус, скорость соединения, режим работы (дуплекс/полудуплекс).

Device Info / LAN	
Port 1	Up; 100M full
Port 2	Down
Port 3	Down
Port 4	Down
Wi-Fi 2.4	Down
Wi-Fi 5	Up

¹Только для сервисов **Internet, VoIP**

4.1.4 Подменю «Statistics». Информация о прохождении трафика на портах устройства

В подменю осуществляется просмотр статистики принятых и переданных пакетов для WAN Service, LAN и оптического интерфейса.

Интерфейс LAN:

Device Info / Statistics / LAN

Interface	Received							Transmitted						
	Total				Multicast	Unicast	Broadcast	Total				Multicast	Unicast	Broadcast
	Bytes	Pkts	Errs	Drops	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Pkts	Pkts	Pkts
Port 1	2672349	40111	0	2	39325	786	208	2675159124	20912050	0	0	20911378	672	0
Port 2	0	0	0	0	0	0	0	0	0	0	0	0	0	208
Port 3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Port 4	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Wi-Fi	0	0	0	74	0	0	0	0	0	0	0	0	0	0
Wi-Fi (wl1)	0	0	0	259	0	0	0	58064	229	0	0	0	0	0

Reset Statistics

WAN Service:

Device Info / Statistics / WAN Service

Interface	Description	Received								Transmitted							
		Total				Multicast	Unicast	Broadcast	Total				Multicast	Unicast	Broadcast		
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
veip0.2	VoIP.1101	24402	283	0	0	0	0	122	161	16995	171	0	0	0	0	171	0
veip0.3	IGMP.30	0	0	0	0	0	0	0	0	492	6	0	0	0	0	6	0
veip0.4	STB.1102	11633	139	0	0	0	0	113	26	168230	677	0	0	4848	71	577	29
veip0.5	VPN.1103	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
veip0.6	OS.1105	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
veip0.7	Wi-Fi Guest.100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ppp0.1	Internet.1100	4141	62	0	0	0	0	62	0	3811	67	0	0	0	0	67	0

Reset Statistics

4.1.5 Подменю «Route». Просмотр таблицы маршрутизации

В подменю осуществляется просмотр таблицы маршрутизации.

Device Info / Route

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
0.0.0.0	0.0.0.0	0.0.0.0	U	0	INTERNET	ppp0.1
1.2.3.0	0.0.0.0	255.255.255.0	U	0		br1
10.10.10.10	192.168.101.249	255.255.255.255	UGH	0		br3
192.168.0.0	0.0.0.0	255.255.255.0	U	0		br0
192.168.5.0	0.0.0.0	255.255.255.0	U	0		br4
192.168.6.0	0.0.0.0	255.255.255.0	U	0		br5
192.168.21.0	0.0.0.0	255.255.255.0	U	0	IGMP	veip0.2
192.168.21.0	192.168.21.1	255.255.255.0	UG	1	IGMP	veip0.2
192.168.100.1	0.0.0.0	255.255.255.255	UH	0	INTERNET	ppp0.1
192.168.101.0	0.0.0.0	255.255.255.0	U	0		br3
192.168.211.0	0.0.0.0	255.255.255.0	U	0	Tr069	veip0.6

Flags:
 U - up,
 G - gateway,
 H - host,
 R - reinstate,
 D - dynamic (redirect),
 M - modified (redirect),
 ! - reject

- *Destination* — IP-адрес назначения;
- *Gateway* — IP-адрес шлюза;
- *Subnet mask* — маска подсети (Genmask);
- *Flag* — флаг маршрута:
 - *U* — маршрут активен;
 - *!* — нерабочий маршрут, пакеты будут отброшены;
 - *G* — маршрут использует шлюз (gateway);
 - *H* — адресом назначения является отдельный хост;
 - *R* — восстановленный маршрут;
 - *D* — устанавливается, если маршрут был создан по приходу перенаправляемого сообщения ICMP;
 - *M* — устанавливается, если маршрут был модифицирован перенаправляемым сообщением ICMP.
- *Metric* — приоритет маршрута;
- *Service* — сервис, к которому относится маршрут;
- *Interface* — сетевой интерфейс, к которому относится маршрут.

4.1.6 Подменю «ARP». Просмотр кэша протокола ARP

Эффективность функционирования ARP во многом зависит от ARP-кэша, который присутствует на каждом хосте. В кэше содержатся IP-адреса и соответствующие им аппаратные адреса. Время жизни каждой записи в кэше 5 минут с момента создания записи.

Device Info / ARP			
IP address	Flags	HW Address	Device
192.168.101.2	Complete	1c:bd:b9:d8:08:e5	br3
192.168.0.100	Complete	bc:ae:c5:b3:96:09	br0
192.168.211.2	Complete	00:15:17:e4:27:ca	veip0.6

- *IP address* — IP-адрес клиента;
- *Flags* — флаги состояния:
 - *Complete* — клиент активен;
 - *Incomplete* — клиент не отвечает на ARP-запросы.
- *HW Address* — MAC-адрес клиента;
- *Device* — интерфейс, на котором находится клиент.

4.1.7 Подменю «DHCP». Активные аренды DHCP

В таблице DHCP можно посмотреть список активных аренд DHCP-сервера и срок их истечения.

Device Info / DHCP			
Hostname	MAC Address	IP Address	Expires In
tester	08:2e:5f:86:86:d9	192.168.0.2	19 hours, 19 minutes, 1 seconds
tester	74:de:2b:fd:59:d9	192.168.0.3	21 hours, 48 minutes, 41 seconds
RedmiNote3-Redmi	ac:c1:ee:44:a3:ef	192.168.0.4	21 hours, 51 minutes, 6 seconds

- *Hostname* — имя хоста (сетового устройства);
- *MAC Address* — MAC-адрес устройства;
- *IP Address* — адрес устройства в локальной сети, выданный маршрутизатором из пула IP-адресов;
- *Expires In* — время, через которое истекает аренда данного адреса.

4.1.8 Подменю «Wireless Stations». Подключенные беспроводные устройства

В данном подменю доступен просмотр перечня аутентифицированных беспроводных устройств и их статус.

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface
74:DE:2B:FD:59:D9			test_24_K	wl0
AC:C1:EE:44:A3:EF	Yes	Yes	test_5_K	wl1

Данные об устройствах выводятся в таблице, содержащей следующие параметры:

- *MAC* — MAC-адрес устройства;
- *Associated* — статус связи с SSID;
- *Authorized* — статус авторизации;
- *SSID* — идентификатор сети, с которой связан клиент;
- *Interface* — интерфейс доступа.

Для обновления данных необходимо нажать кнопку «Refresh».

4.1.9 Подменю «Wireless Monitor». Обнаруженные беспроводные сети

В данном подменю доступен просмотр списка обнаруженных беспроводных сетей в радиоэфире.

Device Info / Wireless Monitor

This page shows known wireless networks.

5GHz ▾

SSID	BSSID	Channel	RSSI
000111_test01	A8:F9:4B:B4:AF:C0	36	-59 dBm
Eltex VAP	A8:F9:4B:B7:95:60	36	-76 dBm
000111_scenarii	A8:F9:4B:B4:AF:C1	36	-59 dBm
000111_test_enterprise	A8:F9:4B:B4:AF:C2	36	-59 dBm
_test_802.11r	A8:F9:4B:B6:01:21	40	-80 dBm
Eltex-Guest	A8:F9:4B:B6:01:22	40	-80 dBm
Eltex-Local	A8:F9:4B:B6:01:24	40	-80 dBm
__1204_e.sh_test_portal_181_5	A8:F9:4B:B0:26:30	44	-66 dBm

Данные об устройствах выводятся в таблице, содержащей следующие параметры:

- *SSID* — идентификатор беспроводной сети;
- *BSSID* — MAC-адрес точки доступа;
- *Channel* — канал, на котором работает точка доступа;
- *RSSI* — уровень сигнала от точки доступа, принимаемый ОНТ.

Для обновления данных необходимо нажать кнопку «Refresh».

4.1.10 Подменю «Voice». Мониторинг состояния телефонных портов

В данном подменю доступен просмотр статуса FXS-портов и параметры SIP-аккаунтов.

Device Info / Voice	
Voice daemon status	RUNNING
SIP Proxy	192.168.101.2:5060
SIP Outbound Proxy	192.168.101.2:5060
SIP Registrar	192.168.101.2:5060
Account enabled	Enabled
State	Up
Error	None
Response code	200 OK
Extension	4004
Display name	4004
Authentication name	4004

- *Voice daemon status* — состояние работы голосового демона;
- *SIP Proxy* — адрес и порт SIP Proxy;
- *SIP Outbound Proxy* — адрес и порт SIP проxy, через который будет осуществляться передача всех запросов (запросы на SIP Proxy и SIP Registrar будут маршрутизироваться через этот сервер);
- *SIP Registrar* — адрес и порт SIP-сервера;
- *Account enabled* — состояние порта FXS в конфигурации;
- *State* — статус аутентификации;
- *Error* — ошибка, выдаваемая сервером SIP;
- *Response code* — код ответа сервера SIP;
- *Extension* — номер телефона;
- *Display name* — отображаемое имя пользователя;
- *Authentication name* — имя пользователя для аутентификации.

4.2 Меню «Advanced Setup». Расширенные настройки конфигурации

4.2.1 Подменю «LAN». Настройка основных параметров

В данном подменю производится настройка основных параметров для LAN-интерфейса.



- *IP address* — адрес устройства в локальной сети;
- *Subnet Mask* — маска подсети.

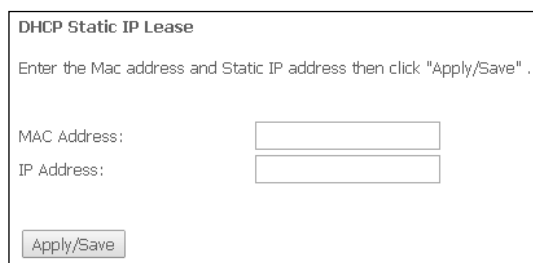
DHCP Server:

DHCP-сервер (Dynamic Host Configuration Protocol — протокол динамической настройки хостов) позволяет провести автоматическую настройку локальных компьютеров для работы в сети. Он назначает IP каждому компьютеру внутри сети. Эта дополнительная функция позволяет уйти от необходимости назначать IP-адреса вручную.

- *Enable* — при установленном флаге использовать DHCP-сервер (сетевые устройства будут получать IP-адреса динамически, из нижеприведенного диапазона);
- *Start IP Address* — начальный адрес диапазона;
- *End IP Address* — конечный адрес диапазона;
- *Leased Time (hour)* — время аренды адреса (в часах).

Static IP Lease List:

В данной таблице производится привязка выдаваемых IP-адресов MAC-адресам устройств. Для добавления записи в таблицу необходимо нажать «Add». Может быть установлено до 32 соответствий.

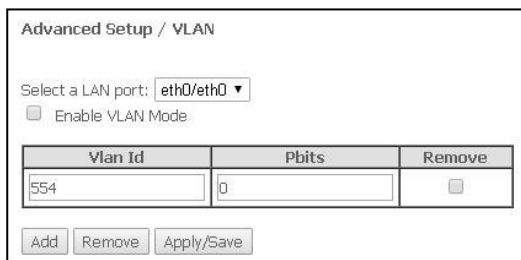


- *MAC Address* — MAC-адрес устройства;
- *IP Address* — IP-адрес устройства.

Для принятия и сохранения изменений необходимо нажать кнопку «Apply/Save».

4.2.2 Подменю «VLAN Settings». Настройка параметров VLAN

В данном подменю производится настройка параметров виртуальных локальных сетей.



Vlan Id	Pbits	Remove
554	0	<input type="checkbox"/>

- *Select a LAN port* — выбор Ethernet-порта;
- *Enable VLAN Mode* — при установленном флаге разрешено использование VLAN.

Для добавления новой VLAN необходимо нажать кнопку «Add» и заполнить следующие поля:

- *Vlan Id* — номер VLAN из диапазона от 1 до 4094;
- *Pbits* — номер приоритета VLAN из диапазона от 0 до 7 (0 — максимальный приоритет, 7 — минимальный).

Для удаления необходимо установить флаг «Remove» в выбранной строке и нажать кнопку «Remove».

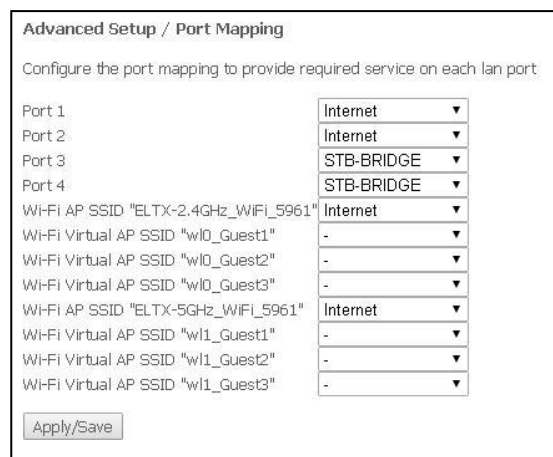
Для принятия и сохранения изменений необходимо нажать кнопку «Apply/Save».

4.2.2.1 Подменю «Port Mapping». Настройки распределения портов и услуг

Подменю предназначено для настройки Ethernet-портов на предоставление конкретной услуги оператора, что позволяет разграничить различные типы трафика. Данная функция используется преимущественно в сетях Triple Play.

В подменю возможно изменить текущие раскладки портов по услугам, например, настроить 4 порта для пользования Internet или 3 порта для STB, в отличие от конфигурации по умолчанию, приведенной на рисунке выше.

Для принятия изменений и сохранения необходимо нажать кнопку «Apply/Save».



Port	Service
Port 1	Internet
Port 2	Internet
Port 3	STB-BRIDGE
Port 4	STB-BRIDGE

4.2.3 Подменю «PPPoE». Настройки PPP

Для включения услуги установите флаг в поле «Enable Service».



Для сервиса Internet доступны 2 режима работы:

1. IP_Routed — режим, в котором сессия PPPoE поднимается на абонентском устройстве;
2. PPPoE_Bridged — режим, в котором сессия PPPoE поднимается на ПК пользователя.

- Username — логин пользователя для доступа к сети Интернет;
- Password — пароль пользователя для доступа к сети Интернет.



При выборе режима работы PPPoE_Bridged поля Username и Password недоступны, логин и пароль вводятся на ПК пользователя.

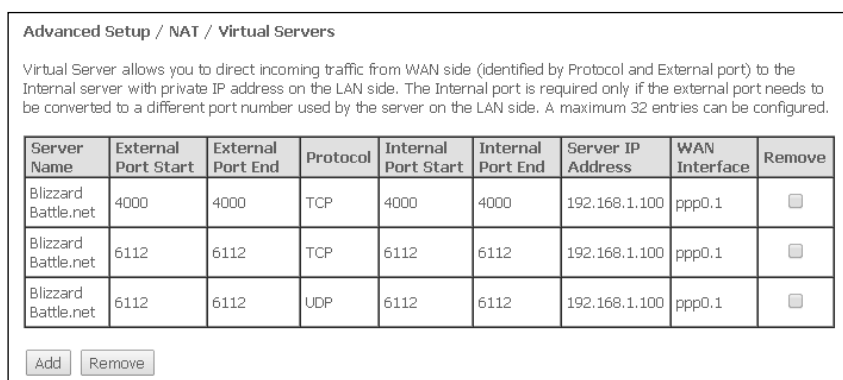
Для принятия и сохранения изменений необходимо нажать кнопку «Apply/Save».

4.2.4 Подменю «NAT». Настройки NAT

Настройки NAT могут быть эффективны при работе устройства в режиме маршрутизатора.

4.2.4.1 Подменю «Virtual Servers». Настройки виртуальных серверов

Virtual Server — это функция маршрутизаторов, предназначенная для предоставления доступа пользователям через сеть Интернет к серверам, находящимся в вашей локальной сети, например к почтовым серверам, WWW, FTP. На устройстве может быть создано до 32 записей.



Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
Blizzard Battle.net	4000	4000	TCP	4000	4000	192.168.1.100	ppp0.1	<input type="checkbox"/>
Blizzard Battle.net	6112	6112	TCP	6112	6112	192.168.1.100	ppp0.1	<input type="checkbox"/>
Blizzard Battle.net	6112	6112	UDP	6112	6112	192.168.1.100	ppp0.1	<input type="checkbox"/>



Правило Virtual Server не будет работать в том случае, если запрос на IP-адрес WAN-интерфейса устройства пришел из локальной сети, так как устройство не поддерживает функцию NAT Loopback. Тестирование созданных правил Virtual Server должно осуществляться только через сеть Интернет.

Для добавления записи в таблицу фильтрации необходимо нажать «Add» и заполнить поля в открывшемся меню:

Advanced Setup / NAT / Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server.
 NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End".
 Remaining number of entries that can be configured:29

Use Interface:

Service Name:
 Select a Service:
 Custom Service:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
<input type="text" value="4000"/>	<input type="text" value="4000"/>	TCP ▾	<input type="text" value="4000"/>	<input type="text" value="4000"/>
<input type="text" value="6112"/>	<input type="text" value="6112"/>	TCP ▾	<input type="text" value="6112"/>	<input type="text" value="6112"/>
<input type="text" value="6112"/>	<input type="text" value="6112"/>	UDP ▾	<input type="text" value="6112"/>	<input type="text" value="6112"/>
<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>

– *Use Interface* — используемый интерфейс;



Для использования доступны только интерфейсы, настроенные на работу в режиме маршрутизатора с разрешенной трансляцией сетевых адресов.

- *Service Name* — настройки сервиса:
 - *Select a Service* — выбор преднастроенного правила;
 - *Custom Service* — создать свои, не указанные в списке *Select a Service*, правила;
- *Server IP Address* — IP-адрес сервера, находящегося в локальной сети;
- *External Port Start* — начальный внешний порт диапазона портов, на которые осуществляется обращение из сети Интернет;
- *External Port End* — конечный внешний порт диапазона портов, на которые осуществляется обращение из сети Интернет;
- *Protocol* — выбор сетевого протокола;
- *Internal Port Start* — начальный внутренний порт диапазона портов, на который будет переадресовываться трафик с внешнего порта маршрутизатора;
- *Internal Port End* — конечный внутренний порт диапазона портов, на который будет переадресовываться трафик с внешнего порта маршрутизатора.

Для принятия и сохранения изменений необходимо нажать кнопку «Apply/Save».

4.2.4.2 Подменю «Port Triggering». Настройки запуска портов

Маршрутизатор по умолчанию блокирует все входящие запросы на установку соединения. Механизм работы функции *Port Triggering* заключается в том, чтобы при появлении определенного события динамически открывать порты на своем внешнем интерфейсе и привязывать их к соответствующим портам компьютера в локальной сети.

Advanced Setup / NAT / Port Triggering

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application Name	Trigger		Open		WAN Interface	Remove		
	Protocol	Port Range	Protocol	Port Range				
		Start	End	Start	End			
ICQ	UDP	4000	4000	TCP	20000	20059	ppp0.1	<input type="checkbox"/>

Для добавления правил в таблицу необходимо нажать кнопку «Add», удаление происходит нажатием кнопки «Remove» напротив выбранного правила.

Advanced Setup / NAT / Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Apply/Save" to add it. Remaining number of entries that can be configured: 32

Use Interface:

Application Name:

Select an application:

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
4000	4000	UDP	20000	20059	TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

– *Use Interface* — используемый интерфейс.



Для использования доступны только интерфейсы, настроенные на работу в режиме маршрутизатора с разрешенной трансляцией сетевых адресов.

– *Application Name* – настройки приложения:

- *Select an application* — выбор преднастроенного правила.
- *Custom an application* — создать свои, не указанные в списке *Select an application*, правила.

В отличие от функции *Virtual Server*, здесь нет необходимости фиксировано задавать IP-адрес компьютера в LAN.

- *Trigger Port Start* — начальный порт диапазона портов, которые осуществляют функцию триггера;
- *Trigger Port End* — конечный порт диапазона портов, которые осуществляют функцию триггера;
- *Trigger Protocol* — протокол, используемый для триггера;

- *Open Port Start* — начальный порт диапазона портов, которые маршрутизатор будет открывать;
- *Open Port End* — конечный порт диапазона портов, которые маршрутизатор будет открывать;
- *Open Protocol* — используемый протокол для открываемых портов.

Для принятия и сохранения изменений необходимо нажать кнопку «Apply/Save».

4.2.4.3 Подменю «DMZ Host». Настройки демилитаризованной зоны

При установке IP-адреса в поле «DMZ Host IP Address» все запросы из внешней сети, не попадающие под правила **Virtual Servers**, будут направляться на DMZ-хост (доверительный хост с указанным адресом, расположенный в локальной сети);

Для отключения данной настройки необходимо стереть IP-адрес из поля ввода.

Advanced Setup / NAT / DMZ Host

The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click 'Apply/Save' to activate the DMZ host.

Clear the IP address field and click 'Apply/Save' to deactivate the DMZ host.

DMZ Host IP Address:

Для принятия и сохранения изменений необходимо нажать кнопку «Apply/Save».

4.2.5 Подменю «Security». Настройки безопасности

В данном подменю проводится настройка параметров безопасности устройства.

4.2.5.1 Подменю «IP Filtering». Настройки фильтрации адресов

Функция *IP Filtering* позволяет фильтровать проходящий через маршрутизатор трафик по IP-адресам и портам.

Настройки фильтрации исходящего трафика (Outgoing):

Advanced Setup / Security / IP Filtering / Outgoing

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcMAC	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
Security	4	TCP or UDP	11:34:5A:67:4C:38	192.168.15.12	80	192.168.15.52	80	<input type="checkbox"/>



По умолчанию весь исходящий трафик будет пропускаться. Правила, созданные в этом меню, позволят блокировать нежелательный трафик.

Для добавления нового правила фильтрации необходимо нажать кнопку «Add».

Advanced Setup / Security / IP Filter / Outgoing / Add

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

MAC address:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

- *Filter Name* — текстовое описание фильтра;
- *IP Version* — выбор версии протокола IP;
- *Protocol* — выбор протокола (TCP/UDP, TCP, UDP, ICMP);
- *MAC address* — MAC-адрес источника;
- *Source IP address[/prefix length]* — IP-адрес источника (через слеш возможно указать длину префикса);
- *Source Port (port or port:port)* — порт источника или диапазон портов через двоеточие;
- *Destination IP address[/prefix length]* — IP-адрес места назначения (через слеш возможно указать длину префикса);
- *Destination Port (port or port:port)* — порт места назначения или диапазон портов через двоеточие.

Для принятия и сохранения настроек необходимо нажать кнопку «Apply/Save».

Настройки фильтрации входящего трафика (Incoming):

Advanced Setup / Security / IP Filtering / Incoming

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	SrcMAC	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
Security1	ppp0.1	4	TCP or UDP	11:25:34:a6:57:5c		80			<input type="checkbox"/>



При включении брандмауэра на интерфейсе WAN или LAN весь входящий трафик, не попадающий под установленные правила, будет заблокирован.

Для добавления нового правила фильтрации необходимо нажать кнопку «Add».

Advanced Setup / Security / IP Filter / Incoming / Add

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source MAC address:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
 Select one or more WAN/LAN interfaces displayed below to apply this rule.

Select All Internet/ppp0.1 br0/br0 br1/br1 br2/br2 br3/br3

- *Filter Name* — текстовое описание фильтра;
- *IP Version* — выбор версии протокола IP;
- *Protocol* — выбор сетевого протокола;
- *Source MAC address* — MAC-адрес источника;
- *Source IP address[/prefix length]* — IP-адрес источника (через слеш возможно указать длину префикса);
- *Source Port (port or port:port)* — порт/порты источника;
- *Destination IP address[/prefix length]* — IP-адрес места назначения (через слеш возможно указать длину префикса);
- *Destination Port (port or port:port)* — порт/порты места назначения;

Интерфейсы WAN (сконфигурированные в режиме маршрутизатора и с включенным брандмауэром) и интерфейсы LAN:

- *Select All* — при установленном флаге выбрать все возможные интерфейсы.

Можно выбрать интерфейс из приведенного списка, установив флаг напротив.

Для принятия и сохранения настроек необходимо нажать кнопку «Apply/Save».

4.2.5.2 Подменю «MAC Filtering». Настройки фильтрации по MAC-адресам

Фильтрация на основе MAC-адресов позволяет пересылать или блокировать трафик с учетом MAC-адреса источника и получателя.

MAC Filtering Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
veip0.3	FORWARDED	<input type="checkbox"/>
veip0.4	FORWARDED	<input type="checkbox"/>
veip0.5	FORWARDED	<input type="checkbox"/>

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
veip0.5	PPPoE	1C:AF:B9:D8:1C:17		WAN_TO_LAN	<input type="checkbox"/>



Фильтрация на основе MAC-адресов работает только для интерфейсов, находящихся в режиме моста (Bridge).

Для изменения глобальной политики установите флаг напротив необходимого интерфейса и нажмите кнопку «Change Policy» (изменить политику). Доступно два варианта: FORWARDED и BLOCKED.

В режиме FORWARDED созданные правила будут запрещать прохождение трафика с указанными MAC-адресами источника/получателя, в режиме BLOCKED — разрешать.

Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply/Save" to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

- *Protocol type* – выбор протокола (PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP);
- *Destination MAC Address* — MAC-адрес получателя;
- *Source MAC Address* — MAC-адрес отправителя;
- *Frame Direction* — направление передачи (LAN<=>WAN, LAN=>WAN, WAN=>LAN);
- *WAN Interfaces (Configured in Bridge mode only)* — выбор WAN-интерфейса из выпадающего списка (доступны только интерфейсы, работающие в режиме моста).

Для принятия и сохранения настроек необходимо нажать кнопку «Apply/Save».

4.2.6 Подменю «Parental control». «Родительский контроль» – настройки ограничения

4.2.6.1 Подменю «Time Restriction». Настройки ограничения продолжительности сеансов

В данном подменю производится конфигурирование расписания работы компьютеров с использованием дней недели и часов, по которым определенному компьютеру в локальной сети будет запрещен доступ в интернет.

Advanced Setup / Parental Control / Time Restriction

A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
Mummy	08:60:6e:d7:73:30	x	x	x	x	x			16:30	23:59	<input type="checkbox"/>

Для создания нового расписания необходимо нажать кнопку «Add», всего может быть добавлено не более 16 записей.

Advanced Setup / Parental Control / Time Restriction / Add

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name

Browser's MAC Address

Other MAC Address

(xx:xx:xx:xx:xx:xx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

- *User Name* — имя пользователя;
- *Browser's MAC Address* — автоматически определенный MAC-адрес компьютера, для которого задается расписание;
- *Other MAC Address (xx:xx:xx:xx:xx:xx)* — заданный вручную MAC-адрес компьютера, для которого определяется расписание;
- *Days of the week* — дни недели, запрещенные для доступа в интернет;
- *Start Blocking Time (hh:mm)* — время начала блокировки в формате ЧЧ:ММ;
- *End Blocking Time (hh:mm)* — время окончания блокировки в формате ЧЧ:ММ;

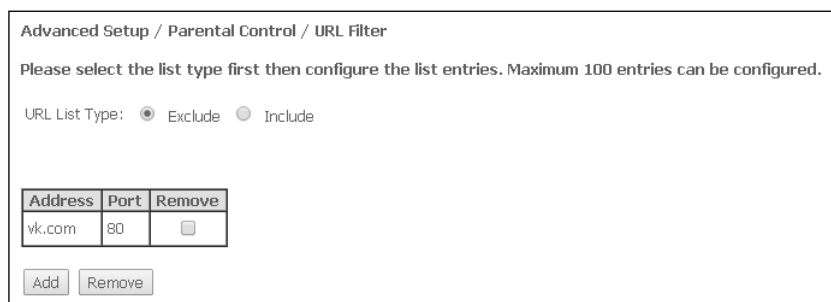


Ограничения будут действовать, если на устройстве установлено корректное системное время.

Для добавления настроек в таблицу необходимо нажать кнопку «Apply/Save».

4.2.6.2 Подменю «URL Filter». Настройки ограничения доступа в интернет

URL Filter — функция полноценного анализа и контроля доступа к определённым ресурсам сети Интернет. В данном разделе задается список запрещенных/разрешенных *URL*-адресов для посещения.



Advanced Setup / Parental Control / URL Filter

Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: Exclude Include

Address	Port	Remove
vk.com	80	<input type="checkbox"/>

- *URL List Type* — тип списка:
 - *Exclude* — запрещенные адреса;
 - *Include* — разрешенные адреса.

Для добавления нового адреса в список необходимо установить флаг напротив требуемого типа списка (*URL List Type*) и нажать кнопку «Add».



Advanced Setup / Parental Control / URL Filter / Add

Enter the URL address and port number then click "Apply/Save" to add the entry to the URL filter.

URL Address:

Port Number: (Default 80 will be applied if leave blank.)

- *URL Address* — URL-адрес;
- *Port Number* — номер порта (если оставить поле пустым, будет использоваться порт 80).

Для добавления настроек в таблицу необходимо нажать кнопку «Apply/Save».

4.2.7 Подменю «Dynamic DNS». Настройки динамической системы доменных имен

Dynamic DNS (динамическая система доменных имен) позволяет информации на DNS-сервере обновляться в реальном времени и (по желанию) в автоматическом режиме. Применяется для назначения постоянного доменного имени устройству (компьютеру, роутеру, например NTP-RG) с динамическим IP-адресом. Это может быть IP-адрес, полученный по IPCP в PPP-соединениях или по DHCP.

Динамическая DNS часто применяется в локальных сетях, где клиенты получают IP-адрес по DHCP, а потом регистрируют свои имена в локальном DNS-сервере.

Advanced Setup / Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove
user	caesar321	dyndns@dyndns.org	ppp0.1	<input type="checkbox"/>

Для добавления записи необходимо нажать кнопку «Add», удаление происходит нажатием кнопки «Remove» напротив выбранной записи.

Advanced Setup / DNS / Dynamic DNS / Add

This page allows you to add a Dynamic DNS address from any of listed DDNS providers.

D-DNS provider:

Hostname:

Interface:

DynDNS Settings

Username:

Password:

DynDNS Type:

Wildcard:

- *D-DNS provider* – выбор типа службы D-DNS (провайдера): *DynDNS.org*, *TZO.com*, *ZoneEdit.com*, *freedns.afraid.org*, *easyDNS.com*, *3322.org*, *DynSIP.org*, *No-IP.com*, *dnsomatic.com*, *sitelutions.com*;
- *Custom* – иной провайдер, выбранный пользователем. В данном случае необходимо самостоятельно указать имя и адрес провайдера:

Advanced Setup / DNS / Dynamic DNS / Add

This page allows you to add a Dynamic DNS address from any of listed DDNS providers.

D-DNS provider:

Hostname:

Interface:

Custom DDNS provider

Username:

Password:

DDNS Provider Server Name:

DDNS Provider URL:

- *Username* — имя пользователя для учетной записи DDNS;
- *Password* — установка пароля для учетной записи DDNS;
- *DDNS Provider Server Name* — имя провайдера услуг DDNS;
- *DDNS Provider URL* — адрес провайдера услуг DDNS;
- *Hostname* — имя хоста, зарегистрированное у провайдера DDNS;
- *Interface* — интерфейс доступа;

В зависимости от выбранного провайдера возможны следующие поля для заполнения:

Advanced Setup / DNS / Dynamic DNS / Add

This page allows you to add a Dynamic DNS address from any of listed DDNS providers.

D-DNS provider: DynDNS.org

Hostname:

Interface: INTERNET/ppp0.1

DynDNS Settings

Username:

Password:

DynDNS Type: Dynamic

Wildcard:

Apply/Save

Advanced Setup / DNS / Dynamic DNS / Add

This page allows you to add a Dynamic DNS address from any of listed DDNS providers.

D-DNS provider: TZO.com

Hostname:

Interface: INTERNET/ppp0.1

TZO Settings

Email:

Key:

Apply/Save

Advanced Setup / DNS / Dynamic DNS / Add

This page allows you to add a Dynamic DNS address from any of listed DDNS providers.

D-DNS provider: freedns.afraid.org

Hostname:

Interface: INTERNET/ppp0.1

freedns.afraid.org Settings

Username:

Password:

Apply/Save

- *Username* — имя пользователя для учетной записи DDNS;
- *Password* — установка пароля для учетной записи DDNS;
- *DynDNS Type* — выбор типа услуги, зарегистрированной Вами у провайдера:
 - *Dynamic* — зарегистрирована услуга Динамический DNS (Dynamic DNS);
 - *Static* — зарегистрирована услуга Статический DNS (Static DNS);
 - *Custom* — зарегистрирована услуга Пользовательский DNS (Custom DNS).
- *Wildcard* — при установленном флаге использовать специальную запись DNS, отвечающую за все поддомены, которая будет соответствовать любому запросу к несуществующему поддомену. Она указывается в виде * в качестве поддомена, например *.domain.tld.
- *Email* — электронный адрес для аутентификации;
- *Key* — ключ для учетной записи DDNS.

Для принятия и сохранения изменений необходимо нажать кнопку «Apply/Save».

4.2.8 Меню «Print Server». Настройка сервера печати

Принт-сервер (сервер печати) — программное обеспечение или устройство, позволяющее группе пользователей проводных и беспроводных сетей совместно использовать принтер дома или в офисе. Он не зависит ни от одного компьютера в сети, что дает возможность не перегружать рабочую среду пользователя. Кроме того, принт-сервер обеспечивает бесперебойную связь с принтером, МФУ, сканером или другой оргтехникой, находящейся в локальной сети.

Advanced Setup / Print Server

This page allows you to enable / disable printer support.

Enable on-board print server.

Printer name:

Make and model:

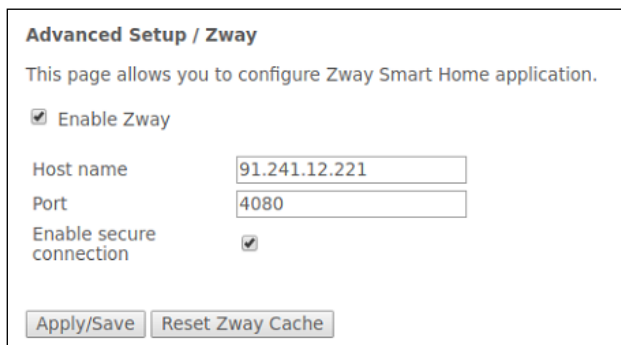
Apply/Save

- *Enable on-board print server* — при установленном флаге принт-сервер активен, иначе — нет;
- *Printer name* — имя принтера;
- *Make and model* — производитель и модель принтера.

Для принятия и сохранения настроек необходимо нажать кнопку «*Apply/Save*».

4.2.9 Подменю «Z-WAVE»¹

В данном подменю настраиваются параметры взаимодействия с сетью «Умного дома».



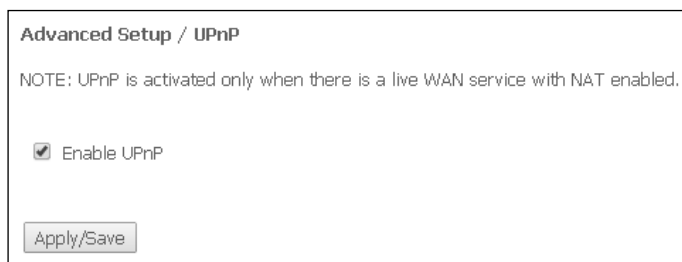
- *Enable Zway* — включить\выключить контроллер «Умного дома»;
- *Host name* — указать адрес удалённой платформы «Умного дома»;
- *Port* — указать порт платформы, к которому подключается контроллер «Умного дома»;
- *Enable secure connection* — установите флаг, если для обмена с платформой используется защищенный канал.

Для принятия и сохранения настроек нажмите кнопку «*Apply/Save*».

При нажатии на кнопку «*Reset Zway Cache*» контроллер отключается, с него удаляется вся информация о подключении к платформе, о привязанных датчиках и сценарии.

4.2.10 Подменю «UPnP». Автоматическая настройка сетевых устройств

В данном подменю производится настройка функции Universal Plug and Play (UPnP™). UPnP обеспечивает совместимость с сетевым оборудованием, программным обеспечением и периферийными устройствами.




Для использования UPnP необходимо настроить NAT на активном WAN интерфейсе..

Для включения UPnP необходимо установить флаг «*Enable UPnP*».

Для принятия и сохранения настроек необходимо нажать кнопку «*Apply/Save*».

¹Меню доступно только для NTE-RG-1421G-WZ

4.3 Меню «Voice». Настройки телефонии SIP

4.3.1 Подменю «SIP Basic Settings». Общие настройки SIP

Voice / SIP Basic Settings

Service Provider 0

Locale selection*: RUS - RUSSIA (Note: Requires vodsl restart to take affect)

SIP domain name*:

Voip Dialplan Setting:

Use SIP Proxy.

SIP Proxy:

SIP Proxy port:

Use SIP Outbound Proxy.

SIP Outbound Proxy:

SIP Outbound Proxy port:

Use SIP Registrar.

SIP Registrar:

SIP Registrar port:

Enable	<input checked="" type="checkbox"/>
Number	<input style="width: 100px;" type="text" value="1001"/>
Display name	<input style="width: 100px;" type="text" value="1001"/>
Authentication name	<input style="width: 100px;" type="text" value="1001"/>
Password	<input style="width: 100px;" type="password" value="...."/>
Preferred ptime	<input style="width: 100px;" type="text" value="20"/> ▾
Preferred codec 1	G.711ALaw ▾
Preferred codec 2	G.729a ▾
Preferred codec 3	G.723.1 ▾
Preferred codec 4	- ▾
Preferred codec 5	- ▾
Preferred codec 6	- ▾

- *Local selection* — выбор места расположения;
- *SIP domain name* — имя домена SIP;
- *VoIP Dialplan Setting* — настройка плана нумерации (рекомендуется указать «x.t»)
- *Use SIP Proxy* — при установленном флаге использовать SIP Proxy;
 - *SIP Proxy* — адрес SIP Proxy;
 - *SIP Proxy port* — порт для SIP Proxy.
- *Use SIP Outbound Proxy* — при установленном флаге использовать SIP Outbound Proxy для передачи всех запросов, иначе — не использовать;
 - *SIP Outbound Proxy* — адрес SIP Proxy, через который будет осуществляться передача всех запросов (запросы на SIP Proxy и SIP Registrar будут маршрутизироваться через этот сервер);
 - *SIP Outbound Proxy port* — порт для SIP Proxy, через который будет осуществляться передача всех запросов;
- *Use SIP Registrar* — при установленном флаге использовать сервер регистрации SIP;
- *SIP Registrar* — адрес сервера;
- *SIP Registrar port* — порт сервера;

В таблице приведены общие параметры SIP для порта FXS.

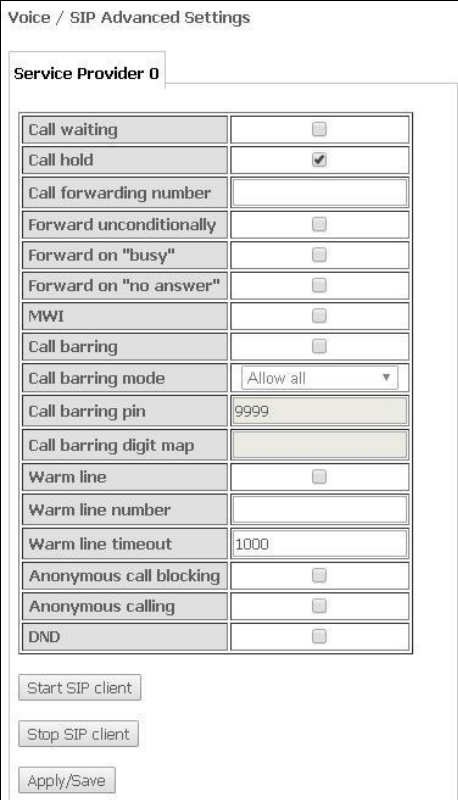
- *Enable* — при установленном флаге данный порт включен в работу;
- *Number* — номер телефона;
- *Display name* — отображаемое имя пользователя;
- *Authentication name* — имя пользователя для аутентификации;
- *Password* — пароль для аутентификации;
- *Preferred ptime* — количество миллисекунд речи, передаваемых в одном речевом пакете протокола RTP;
- *Preferred codec* — выбор кодека в порядке предпочтения (1 — наиболее приоритетный);

Для принятия изменений необходимо нажать кнопку «Apply/Save».

Для принятия и сохранения изменений необходимо нажать кнопку «Apply/Save».

4.3.2 Подменю «SIP Advanced Settings». Дополнительные настройки SIP

В данном подменю производится настройка услуг ДВО (подробное описание доступно в ПРИЛОЖЕНИЕ Б. ИСПОЛЬЗОВАНИЕ ДОПОЛНИТЕЛЬНЫХ УСЛУГ).



Voice / SIP Advanced Settings	
Service Provider 0	
Call waiting	<input type="checkbox"/>
Call hold	<input checked="" type="checkbox"/>
Call forwarding number	<input type="text"/>
Forward unconditionally	<input type="checkbox"/>
Forward on "busy"	<input type="checkbox"/>
Forward on "no answer"	<input type="checkbox"/>
MWI	<input type="checkbox"/>
Call barring	<input type="checkbox"/>
Call barring mode	Allow all
Call barring pin	9999
Call barring digit map	<input type="text"/>
Warm line	<input type="checkbox"/>
Warm line number	<input type="text"/>
Warm line timeout	1000
Anonymous call blocking	<input type="checkbox"/>
Anonymous calling	<input type="checkbox"/>
DND	<input type="checkbox"/>
Start SIP client	
Stop SIP client	
Apply/Save	

- *Call waiting* — при установленном флаге разрешено уведомление о поступлении нового вызова;
- *Call hold* — при установленном флаге разрешено удержание вызова;
- *Call forwarding number* — номер для переадресации вызова;
- *Forward unconditionally* — при установленном флаге разрешена безусловная переадресация;
- *Forward on "busy"* — при установленном флаге разрешена переадресация вызова по занятости;
- *Forward on "no answer"* — при установленном флаге разрешена переадресация вызова по неответу абонента;
- *MWI* — при установленном флаге поддерживается индикация о наличии сообщений на голосовой почте;
- *Call barring* — при установленном флаге абонент может установить запрет на исходящие вызовы;

- *Call barring mode* — режим ограничения вызовов;
- *Call barring pin* — пароль, по которому разрешено совершать вызовы;
- *Call barring digit map* — план нумерации, по которому разрешено/запрещено совершать вызовы;
- *Warm line* — при установленном флаге разрешена услуга «теплая линия», иначе — не разрешена. Услуга позволяет автоматически установить исходящее соединение без набора номера сразу после подъема трубки — «горячая линия», либо с задержкой — «теплая линия»;
- *Warm line number* — номер «теплой линии»;
- *Warm line timeout* — таймаут до начала набора номера «теплой линии»;
- *Anonymous call blocking* — при установленном флаге разрешена блокировка вызовов от абонентов, номер которых не определен;
- *Anonymous calling* — при установленном флаге вызовы с порта совершаются анонимно (услуга Анти-АОН);
- *DND* — при установленном флаге включена услуга «Не беспокоить».

Для принятия и сохранения изменений необходимо нажать кнопку «*Apply/Save*».

Для применения новых настроек необходимо остановить клиента SIP нажатием кнопки «*Stop SIP client*», далее запустить его кнопкой «*Start SIP client*».

4.4 Меню «Wireless». Настройка беспроводной сети

Настройки в данном меню производятся отдельно для рабочих диапазонов 2,4 ГГц и 5 ГГц.

4.4.1 Подменю «Basic». Общая информация

В данном подменю производятся основные настройки беспроводного интерфейса LAN. Также возможно задать до трех виртуальных точек беспроводного доступа.

Wireless / Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

Enable Wireless
 Hide Access Point
 Clients Isolation
 Disable WMM Advertise
 Enable Wireless Multicast Forwarding (WMF)

SSID:
 BSSID:
 Country:
 Country RegRev:
 Max Clients:

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
<input type="checkbox"/>	wl0_Guest1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	16	N/A
<input type="checkbox"/>	wl0_Guest2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	16	N/A
<input type="checkbox"/>	wl0_Guest3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	16	N/A

- *Enable Wireless* — включить Wi-Fi на устройстве;
- *Hide Access Point* — скрытый режим работы точки доступа (в данном режиме SSID беспроводной сети не будет широкоэвещательно распространяться маршрутизатором);
- *Clients Isolation* — при установленном флаге беспроводные клиенты не смогут взаимодействовать друг с другом;
- *Disable WMM Advertise* — отключить WMM (Wi-Fi Multimedia — QoS для беспроводных сетей);
- *Enable Wireless Multicast Forwarding (WMF)* — включить WMF;
- *SSID* — *Service Set Identifier* — назначить имя беспроводной сети (ввод с учетом регистра клавиатуры);



По умолчанию на устройстве установлено имя беспроводной сети (SSID) ELTX-2.4/5GHz_WiFi_aaaa, где aaaa — это 4 последние цифры WAN MAC. WAN MAC указан в наклейке на корпусе устройства.

- *BSSID* — MAC-адрес точки доступа;
- *Country* — установить местоположение (страну);
- *Country RegRev* — установить идентификатор региона (для России: 0-34);
- *Max Clients* — установить максимально возможное количество одновременных беспроводных подключений.

Для принятия изменений необходимо нажать кнопку «Apply/Save».

4.4.2 Подменю «Security». Настройка параметров безопасности

В данном подменю производятся основные настройки шифрования данных в беспроводной сети. Возможно настроить клиентское оборудование беспроводного доступа вручную или автоматически, используя WPS.

Wireless / Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)
Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

WPS Setup

Enable WPS:

Add Client (This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)
 Use STA PIN Use AP PIN [Help](#)

Set Authorized Station MAC: [Help](#)

Set WPS AP Mode:

Setup AP (Configure all security settings with an external registrar)

Device PIN: [Help](#)

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:

Network Authentication:

Protected Management Frames:

WPA/WPA1 passphrase: [Click here to display](#)

WPA Group Rekey Interval:

WPA/WPA1 Encryption:

WEP Encryption:

WPS (Wi-Fi Protected Setup) — стандарт, разработанный альянсом производителей беспроводного оборудования Wi-Fi с целью упрощения процесса настройки беспроводной сети. Данная технология позволяет пользователю быстро, просто и безопасно настроить беспроводную сеть, не вникая в тонкости работы Wi-Fi и протоколов шифрования. WPS автоматически задает имя сети и шифрование для защиты от несанкционированного доступа, что в иных случаях приходилось делать вручную.

Для того чтобы подключиться, достаточно нажать на кнопку WPS, расположенную на боковой панели устройства, или же ввести PIN-код, используя web-конфигуратор.

WPS Setup:

- *Enable WPS* — для разрешения доступа по WPS в выпадающем списке выберите «Enable», если сетевой адаптер Wi-Fi вашего устройства поддерживает данный режим настройки;
- *Add Client* — выбор метода авторизации клиента (настройки применимы только в режимах WPA-PSK, WPA2-PSK). Для начала процесса авторизации необходимо нажать кнопку «Add Enrollee»:
 - *Use STA PIN* — авторизация с помощью PIN-кода, выданного клиентом;
 - *Use AP PIN* — авторизация с использованием собственного PIN-кода.

Add Client (This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)

Use STA PIN
 Use AP PIN

[Help](#)

Set Authorized Station MAC

[Help](#)

- *Set Authorized Station MAC* — установить MAC-адрес клиентского устройства, запись в формате XX: XX: XX: XX: XX;
- *Set WPS AP Mode* — установить режим точки доступа WPS;
- *Device PIN* — собственный PIN-код (восьмизначный цифровой код, генерируемый устройством).



Недостатки метода WPS

В Wi-Fi роутерах с поддержкой технологии WPS существует уязвимость относительно безопасности сети. Она заключается в том, что методом подбора возможно узнать используемый восьмизначный ключ сети (PIN-код) к протоколам шифрования WPA и WPA2.

Manual Setup AP:

- *Select SSID* — выбрать имя беспроводной сети из списка;
- *Network Authentication* — установить режим сетевой аутентификации из перечня в выпадающем списке:
 - *Open* — открытый — защита беспроводной сети отсутствует (в этом режиме может использоваться только WEP-ключ);
 - *Shared* — общий (режим позволяет пользователям получать аутентификацию по их SSID или WEP-ключу);
 - *802.1x* — включает стандарт 802.1x (позволяет пользователям аутентифицироваться с использованием сервера аутентификации RADIUS, для шифрования данных используется WEP-ключ):
 - *RADIUS Server IP Address* — IP-адрес RADIUS-сервера;
 - *RADIUS Port* — номер порта RADIUS-сервера. По умолчанию установлен порт 1812;
 - *RADIUS Key* — секретный ключ для доступа к RADIUS-серверу;
 - *WPA2* — включает WPA2 (режим использует протокол WPA2 и требует использования сервера аутентификации RADIUS):
 - WPA2 Preauthentication;
 - Network Re-auth Interval;
 - *WPA Group Rekey Interval* — интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение;
 - *RADIUS Server IP Address* – IP-адрес RADIUS-сервера;
 - *RADIUS Port* — номер порта RADIUS-сервера. По умолчанию установлен порт 1812;
 - *RADIUS Key* – секретный ключ для доступа к RADIUS-серверу;
 - *WPA/WAPI Encryption* – выбор метода шифрования данных WPA/WAPI: TKIP+AES, AES:
 - TKIP — протокол шифрования, используемый для WPA. Обладает более эффективным механизмом управления ключами по сравнению с WEP;
 - AES — алгоритм 128-битного блочного шифрования с ключом 128/192/256 бит, используется обычно для WPA2);
 - *WPA2-PSK* — включает WPA2-PSK (режим использует протокол WPA2, но не требует использования сервера аутентификации RADIUS);

- *WPA/WAPI passphrase* — секретная фраза. Установка пароля, строка 8-63 символа ASCII¹. Для просмотра секретной фразы необходимо нажать на ссылку «*Click here to display*», пароль будет показан во всплывающем окне.



По умолчанию ключ сети соответствует серийному номеру устройства. Серийный номер указан на наклейке на корпусе устройства. При изменении пароля необходимо задать комбинацию из 10 символов. Пароль должен содержать цифры и латинские буквы в верхнем и нижнем регистрах.

- *WPA Group Rekey Interval* — интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение;
- *WPA/WAPI Encryption* — выбор метода шифрования данных WPA/WAPI: TKIP+AES, AES:
 - TKIP — протокол шифрования, используемый для WPA. Обладает более эффективным механизмом управления ключами по сравнению с WEP;
 - AES — алгоритм 128-битного блочного шифрования с ключом 128/192/256 бит, используется обычно для WPA2);
- *Mixed WPA2/WPA* — включает комбинацию WPA2/WPA (данный режим шифрования использует протоколы WPA2 и WPA, требует использования сервера аутентификации RADIUS);
 - *WPA2 Preauthentication* — предварительная проверка подлинности беспроводного клиента на других беспроводных точках доступа в используемом диапазоне. В течение проверки связь осуществляется через текущую беспроводную точку доступа;
 - *Network Re-auth Interval* — период повторной проверки подлинности. Определяет, как часто точка доступа посылает сообщение и требует от клиентов ответа, содержащего правильные данные безопасности;
 - *WPA Group Rekey Interval* — интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение;
 - *RADIUS Server IP Address* — IP-адрес RADIUS-сервера;
 - *RADIUS Port* — номер порта RADIUS-сервера. По умолчанию установлен порт 1812;
 - *RADIUS Key* — секретный ключ для доступа к RADIUS-серверу;
 - *WPA/WAPI Encryption* — выбор метода шифрования данных WPA/WAPI: TKIP+AES, AES:
 - TKIP — протокол шифрования, используемый для WPA. Обладает более эффективным механизмом управления ключами по сравнению с WEP;
 - AES — алгоритм 128-битного блочного шифрования с ключом 128/192/256 бит, используется обычно для WPA2);
- *Mixed WPA2/WPA-PSK* — включает комбинацию WPA2/WPA-PSK (этот режим шифрования использует протоколы WPA2-PSK и WPA-PSK, не требует использования сервера аутентификации RADIUS).

¹ ASCII — набор из 128 символов для машинного представления прописных и строчных букв латинского алфавита, чисел, знаков препинания и специальных символов.

- *WPA/WAPI passphrase* — секретная фраза. Установка пароля, строка 8-63 символа ASCII. Для просмотра секретной фразы необходимо нажать на ссылку «*Click here to display*», пароль будет показан во всплывающем окне.



По умолчанию ключ сети соответствует серийному номеру устройства. Серийный номер указан в наклейке на корпусе устройства. При изменении пароля необходимо задать комбинацию из 10 символов. Пароль должен содержать цифры и латинские буквы в верхнем и нижнем регистрах.

- *WPA Group Rekey Interval* — интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение;
- *WPA/WAPI Encryption* — выбор метода шифрования данных WPA/WAPI: TKIP+AES, AES:
 - TKIP — протокол шифрования, используемый для WPA. Обладает более эффективным механизмом управления ключами по сравнению с WEP;
 - AES — алгоритм 128-битного блочного шифрования с ключом 128/192/256 бит, используется обычно для WPA2);



Убедитесь, что беспроводной адаптер компьютера поддерживает выбранный тип шифрования. Наиболее стойкую защиту беспроводного канала даёт совместная работа точки доступа и RADIUS-сервера (для аутентификации беспроводных клиентов).

- *WEP Encryption* — для включения шифрования WEP выберите *Enable* в выпадающем списке;
- *Encryption Strength* — 64- или 128-битное шифрование ключа;
- *Current Network Key* — выбор ключа, который будет использоваться для установления соединения;
- *Network Key 1..4* — возможно задать до четырех различных ключей из 10 символов в шестнадцатеричной системе счисления либо 5 символов ASCII для 64-битного шифрования. Или 26 символов в 16-ричной системе счисления либо 13 символов ASCII для 128-х битного шифрования.

Для принятия изменений необходимо нажать кнопку «*Apply/Save*».

4.4.3 Подменю «MAC Filter». Настройки фильтрации MAC-адресов

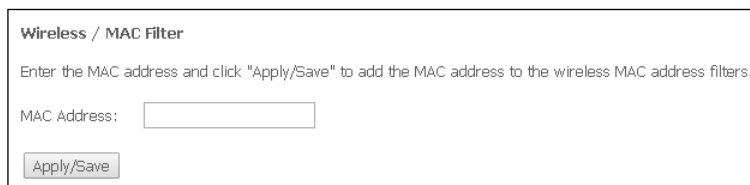
В данном подменю производится настройка фильтрации MAC-адресов.



- *Select SSID* — выбрать идентификатор беспроводной сети, для которой будет создано правило;

- *MAC Restrict Mode* — выбор режима фильтрации по MAC-адресам:
 - *Disabled* — не использовать фильтр;
 - *Allow* — фильтр по разрешенным адресам;
 - *Deny* — фильтр по запрещенным адресам.

Для добавления MAC-адреса в таблицу фильтрации необходимо нажать «Add» и ввести его значение в поле «MAC address» в открывшемся меню:

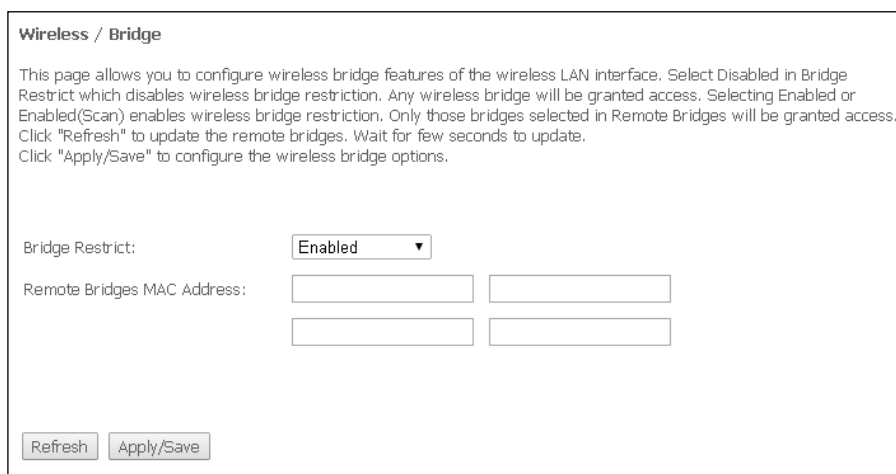


Для принятия изменений необходимо нажать кнопку «Apply/Save».

4.4.4 Подменю «Bridge». Настройки беспроводного соединения в режиме моста

В данном подменю задается режим работы точки доступа: в качестве точки доступа или беспроводного моста.

При использовании режима моста необходимо ввести MAC-адреса удаленных мостов. Данный режим используется для установки беспроводного соединения между двумя отдельными сетями.



В режиме «Wireless Bridge» возможно задать следующие настройки:

- *Bridge Restrict* — выбор режима работы моста:
 - *Enabled* — включить фильтр по MAC-адресам (разрешены только заданные адреса);
 - *Enable (Scan)* — поиск удаленных мостов;
 - *Disable* — ограничения по MAC-адресам отсутствуют;
- *Remote Bridges MAC Address* – адреса удаленных мостов.



В режиме моста маршрутизатор не поддерживает функцию Wi-Fi Multimedia (WMM).

Для обновления доступных удаленных мостов необходимо нажать «Refresh».

Для принятия и сохранения изменений необходимо нажать кнопку «Apply/Save».

4.4.5 Подменю «Advanced». Расширенные настройки

В данном подменю производятся расширенные настройки беспроводной сети.

Wireless / Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.
Click "Apply/Save" to configure the advanced wireless options.

Band: Current: 1 (interference: acceptable)

Channel:

Auto Channel Timer(min):

Auto Channel Set:

Allowed Channels:

1	2	3	4	5	6	7	8	9	10	11	12	13
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

802.11n/EWC:

Bandwidth: Current: 20MHz

Control Sideband: Current: N/A

802.11n Rate:

802.11n Protection:

Support 802.11n Client Only:

RIFS Advertisement:

RX Chain Power Save: Power Save status: Full Power

RX Chain Power Save Quiet Time:

RX Chain Power Save PPS:

54g™ Rate:

Multicast Rate:

Basic Rate:

Fragmentation Threshold:

RTS Threshold:

DTIM Interval:

Beacon Interval:

Global Max Clients:

XPress™ Technology:

Transmit Power:

Transmit Power Boost:

WMM(Wi-Fi Multimedia):

WMM No Acknowledgement:

WMM APSD:

Enable Traffic Scheduler:

Airtime Fairness:

- *Band* — установка частотного диапазона;
- *Channel* — устанавливает рабочий канал для маршрутизатора. При наличии помех или проблем в работе беспроводной сети изменение канала может способствовать их устранению. Рекомендуется установить значение "Auto" во избежание помех, вызываемых работой смежных сетей;
- *Auto Channel Timer (min)* — время в минутах, через которое маршрутизатор будет искать более оптимальный беспроводный канал. Параметр доступен, если установлен автовыбор канала (0 — выключить);
- *Auto Channel Set* — определяет режим работы автовыбора каналов:
 - *Full* — автовыбор производит сканирование и выбор канала из всех доступных;
 - *Legacy* — автовыбор производит сканирование и выбор канала из набора каналов, поддерживаемых старыми устройствами (только для диапазона 2,4 ГГц);

- *Custom* — автовыбор производит сканирование и выбор канала из списка, заданного пользователем в настройках «*Allowed Channels*».
- *802.11n/EWC* — режим совместимости с оборудованием 802.11n Draft2.0 и EWC (Enhanced Wireless Consortium);
- *Bandwidth* — установка полосы пропускания 20 МГц или 40 МГц. В режиме 40 МГц используются две смежные полосы по 20 МГц для увеличения пропускной способности канала;
- *Control Sideband* — выбор второго канала (Lower или Upper) в режиме 40 МГц;
- *802.11n Rate* — установка скорости соединения;
- *802.11n Protection* — при включении увеличится безопасность, но уменьшится пропускная способность;
- *Support 802.11n Client Only* — при включении клиентам 802.11b/g будет запрещен доступ к устройству;
- *RIFS Advertisement* — (Reduced Interframe Space) уменьшение интервала между блоками данных (PDUs), повышает эффективность Wi-Fi;
- *OBSS Co-Existence* — настройка толерантности при выборе режима работы (20 МГц или 40 МГц). Если параметр в состоянии «*Enable*» — будет выбран оптимальный режим работы устройства, учитывая «*Bandwidth*», иначе режим работы будет зависеть только от параметра «*Bandwidth*»;
- *RX Chain Power Save* — отключение приема на одной из антенн устройства в целях энергосбережения;
- *RX Chain Power Save Quiet Time* — период времени, в течении которого интенсивность трафика должна быть ниже PPS (packet per second), для включения режима энергосбережения;
- *RX Chain Power Save PPS* — верхняя граница параметра PPS. Если в течение времени, определенного параметром «*RX Chain Power Save Quiet Time*», интенсивность пакетов на интерфейсе WLAN не превышает данную величину, включается режим энергосбережения;
- *54g™ Rate* — установка скорости в режиме совместимости с устройствами 54g™;
- *Multicast Rate* — установка скорости трафика при многоадресной передаче;
- *Basic Rate* — базовая скорость передачи;
- *Fragmentation Threshold* — установка порога фрагментации в байтах. Если размер пакета будет превышать заданное значение, он будет фрагментирован на части подходящего размера;
- *RTS Threshold* — если сетевой пакет меньше, чем установленное пороговое значение RTS, механизм RTS/CTS (механизм соединения по каналу с использованием сигналов готовности к передаче/готовности к приему) задействован не будет;
- *DTIM Interval* — временной интервал, по истечении которого широковещательные и многоадресные пакеты, помещенные в буфер, будут доставлены беспроводным клиентам;
- *Beacon Interval* — период отправки информационного пакета в беспроводную сеть, сигнализирующего о том что точка доступа активна;
- *Global Max Clients* — максимальное количество беспроводных клиентов;
- *XPress™ Technology* — использование позволяет повысить пропускную способность до 27% в сетях стандарта 802.11g. А в смешанных сетях 802.11g и 802.11b использование XPress™ Technology может повысить пропускную способность до 75%;
- *Transmit Power* — определяется мощность сигнала точки доступа;
- *Transmit Power Boost* — повышенная мощность сигнала точки доступа;
- *WMM (Wi-Fi Multimedia)* — установка режима Wi-Fi Multimedia (WMM). Данный режим позволяет быстро и качественно передавать аудио- и видеоконтент одновременно с передачей данных;
- *WMM No Acknowledgement* — при использовании данного режима приемная сторона не подтверждает принятые пакеты. В среде с малым количеством помех это позволит увеличить эффективность передачи, в среде с большим количеством помех эффективность передачи снизится;
- *WMM APSD* — установить автоматический переход в режим экономии энергии (enabled — автоматический переход разрешен);
- *Enable Traffic Scheduler* — включение планировщика трафика;
- *Airtime Fairness* — эфирная равнодоступность.

Для принятия и сохранения изменений необходимо нажать кнопку «*Apply/Save*».

4.5 Меню «Storage Service». Службы файловых хранилищ

4.5.1 Подменю «Storage Device Info». Информация о подключенных USB-устройствах

В данном подменю доступен список всех подключенных запоминающих устройств. Предоставляется следующая информация:

Storage Service / Storage Device Info				
The Storage service allows you to use Storage devices with modem to be more easily accessed				
Volumename	FileSystem	Total Space	Used Space	Action
usb1_1	fat	3854	163	Unmount

- *Volumename* — имя устройства;
- *FileSystem* — тип файловой системы;
- *Total Space* — общий объем;
- *Used Space* — используемый объем;
- *Unmount* — для безопасного извлечения устройства необходимо предварительно нажать данную кнопку.

4.5.2 Подменю «User Accounts». Настройка пользователей Samba

В данном подменю происходит настройка учетных записей пользователей Samba.

Storage Service / User Accounts		
Choose Add, or Remove to configure User Accounts.		
UserName	HomeDir	Remove
test	usb1_1/test	<input type="checkbox"/>

Add Remove

Для добавления записи необходимо нажать кнопку «Add». Для удаления — установить флаг напротив требуемой записи в колонке Remove и нажать кнопку «Remove».

Advanced Setup / Storage Service / User Accounts / Add	
In the boxes below, enter the user name, password and volume name on which the home directory is to be created.	
Username:	<input type="text"/>
Password:	<input type="password"/>
Confirm Password:	<input type="password"/>
volumeName:	<input type="text"/>
Apply/Save	

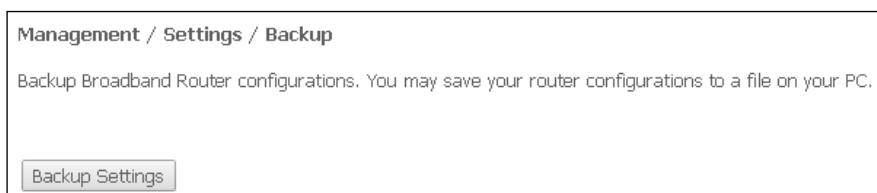
- *UserName* — логин для доступа к сетевому ресурсу;
- *Password* — пароль для доступа к сетевому ресурсу;
- *Confirm Password* — подтверждение пароля для доступа;
- *volumeName* — путь к сетевому ресурсу (имя подключенного запоминающего устройства отображается на странице «Storage Device Info»).

4.6 Меню «Management». Управление устройством

4.6.1 Подменю «Settings». Настройки

4.6.1.1 Подменю «Backup». Резервное копирование

Подменю позволяет по нажатию кнопки «Backup Settings» выгрузить конфигурацию на ПК.

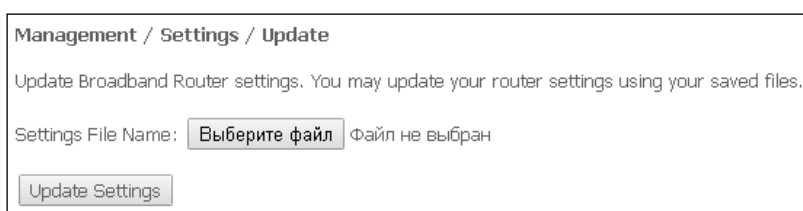


4.6.1.2 Подменю Update. Обновление конфигурации

Для обновления конфигурации необходимо выбрать файл конфигурации в поле «Settings File name» (используя кнопку «Выберите файл» или «Обзор..») и нажать кнопку «Update Settings».



В процессе обновления не допускается отключение питания устройства либо его перезагрузка. Процесс обновления может занимать несколько минут, после чего устройство автоматически перезагружается.



4.6.1.3 Подменю «Restore Default». Возврат к настройкам по умолчанию

По нажатию кнопки «Restore Default Settings» происходит сброс настроек к заводским. Устройство при этом будет перезагружено.



При выполнении данной операции все выполненные вами настройки будут утрачены.

4.6.2 Подменю «Internet Time». Настройки системного времени

Management / Internet Time

This page allows you to the modem's time configuration.

Automatically synchronize with Internet time servers

First NTP time server:

Second NTP time server:

Third NTP time server:

Fourth NTP time server:

Fifth NTP time server:

Time zone offset:

Во вкладке настраивается системное время на устройстве.

- *Automatically synchronize with Internet time servers* — при установленном флаге производить автоматическую синхронизацию с интернет-серверами точного времени;
- *First NTP time server* — выбор основного сервера точного времени;
- *Second NTP time server* — выбор второго сервера точного времени, none — не использовать дополнительные сервера;
- *Third NTP time server* — выбор третьего сервера точного времени, none — не использовать дополнительные сервера;
- *Fourth NTP time server* — выбор четвертого сервера точного времени, none — не использовать дополнительные сервера;
- *Fifth NTP time server* — выбор пятого сервера точного времени, none — не использовать дополнительные сервера;
- *Time zone offset* — установка часового пояса в соответствии с всемирным координационным временем (UTC).



При выборе в выпадающем списке серверов значения *Other*, справа станет активным окно для заполнения, куда следует вручную ввести адрес сервера точного времени.

Для принятия изменений и сохранения необходимо нажать кнопку «Apply/Save».

4.6.3 Подменю «Ping». Проверка доступности сетевых устройств

Данное подменю предназначено для проверки доступности подключенных к маршрутизатору сетевых устройств при помощи утилиты Ping.

Для проверки доступности подключенного устройства необходимо ввести его IP-адрес в поле и нажать кнопку «Ping». Для просмотра трассировки маршрута нажмите кнопку «TraceRoute». Вывод будет осуществлен на данной странице web-конфигуратора.

Management / Ping

Traceroute started

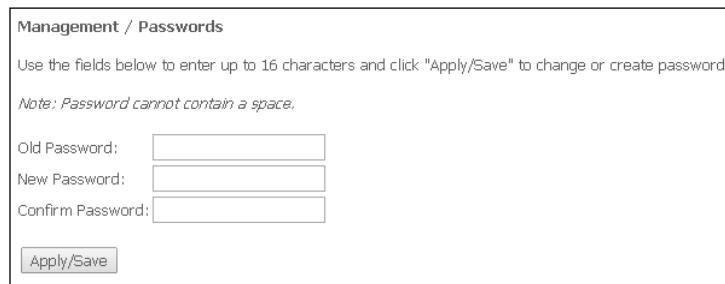
```

traceroute to 192.168.0.2 (192.168.0.2), 30 hops max, 38 byte packets
 1 192.168.0.2 (192.168.0.2) 0.632 ms 0.593 ms 0.538 ms
    
```

Traceroute finished

4.6.4 Подменю «Passwords». Настройка контроля доступа (установка паролей)

В данном подменю осуществляется смена пароля для доступа к устройству.



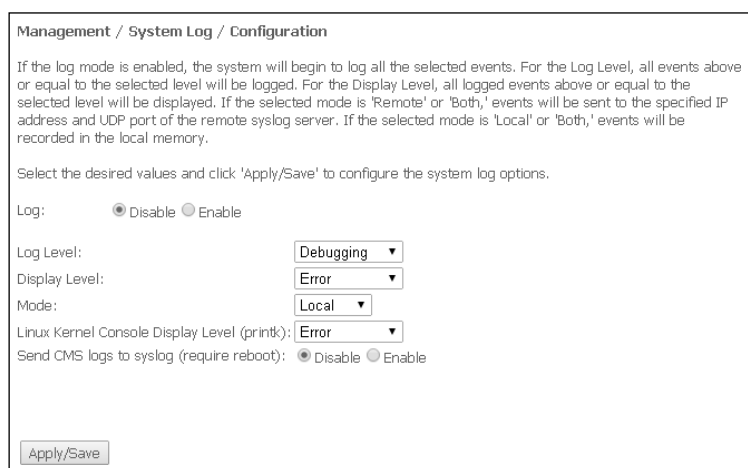
Для смены пароля необходимо ввести существующий пароль, затем новый пароль и подтвердить его.

Для принятия изменений и сохранения необходимо нажать кнопку «Apply/Save».

4.6.5 Подменю «System Log». Просмотр и настройка системного журнала

4.6.5.1 Подменю «Configuration». Настройка системного журнала

Подменю используется для настройки событий, происходящих на маршрутизаторе.



- *Log* — включение/выключение системного журнала (enable/disable);
- *Log Level* — установка уровня детализации журнала событий. Классификация уровней важности в порядке снижения значимости:
 - *Emergency* — аварийный случай;
 - *Alert* — тревога;
 - *Critical* — критическое событие;
 - *Error* — ошибка;
 - *Warning* — предупреждение;
 - *Notice* — уведомление;
 - *Informational* — информация;
 - *Debugging* — устранение неполадок;
- *Display Level* — установка уровня отображения выводимых сообщений журнала событий;
- *Mode* — режим работы журнала:
 - *Local* — местный (все события возвращаются на маршрутизатор через буферную память);
 - *Remote* — удаленный (все события возвращаются на сервер Syslog);
 - *Both* — работают оба режима;

- *Flash* — отправка на USB-накопитель;
- *Linux Level Console Display Level (printk)* — установка уровня сообщений, выводимых в консоль Linux;
- *Send CMS logs to syslog (require reboot)* — включение/выключение отправки сообщений от CMS в системный журнал.

При выборе удаленного режима (Remote) доступны следующие настройки:

- *Server IP address* — IP-адрес сервера Syslog, на котором сохраняются все события;
- *Server IP Port* — номер порта сервера Syslog.

Для принятия изменений и сохранения необходимо нажать кнопку «Apply/Save».

4.6.5.2 Подменю «View». Просмотр системного журнала

Подменю служит для просмотра событий, происходящих на маршрутизаторе.

Management / System Log / View			
Date/Time	Facility	Severity	Message
Jan 1 00:01:00	syslog	emerg	#####
Jan 1 00:01:00	syslog	emerg	## syslogd started: BusyBox v1.17.2 ##
Jan 1 00:01:00	syslog	emerg	#####
Jan 1 00:01:00	kern	err	kernel: i2c i2c-0: Failed to register i2c client gpon_i2c at 0x50 (-16)
Jan 1 00:01:00	kern	err	kernel: i2c i2c-0: Failed to register i2c client gpon_i2c at 0x50 (-16)
Jan 1 00:01:00	kern	err	kernel: i2c i2c-0: Failed to register i2c client gpon_i2c at 0x51 (-16)
Jan 1 00:01:00	kern	err	kernel: i2c i2c-0: Failed to register i2c client gpon_i2c at 0x51 (-16)
Jan 1 00:01:00	kern	err	kernel: sd 0:0:0:0: [sda] No Caching mode page present
Jan 1 00:01:00	kern	err	kernel: sd 0:0:0:0: [sda] Assuming drive cache: write through
Jan 1 00:01:00	kern	err	kernel: sd 0:0:0:0: [sda] No Caching mode page present
Jan 1 00:01:00	kern	err	kernel: sd 0:0:0:0: [sda] Assuming drive cache: write through
Jan 1 00:01:00	kern	err	kernel: sd 0:0:0:0: [sda] No Caching mode page present
Jan 1 00:01:00	kern	err	kernel: sd 0:0:0:0: [sda] Assuming drive cache: write through
Jan 1 00:01:00	kern	crit	kernel: eth0 Link UP 1000 mbps full duplex
Jan 1 00:01:02	kern	crit	kernel: eth0 Link DOWN.
Jan 1 00:01:06	kern	crit	kernel: eth0 Link UP 1000 mbps full duplex

Refresh

Чтобы закрыть окно просмотра журнала, нажмите «Close». Обновить информацию можно кнопкой «Refresh».

4.6.6 Подменю «Update Software». Обновление ПО

Для обновления ПО необходимо выбрать файл ПО в строке «Software File name» (используя кнопку «Выберите файл» или «Обзор») и нажать «Update Software».



В процессе обновления не допускается отключение питания устройства либо его перезагрузка. Процесс обновления может занимать несколько минут, после чего устройство автоматически перезагружается.

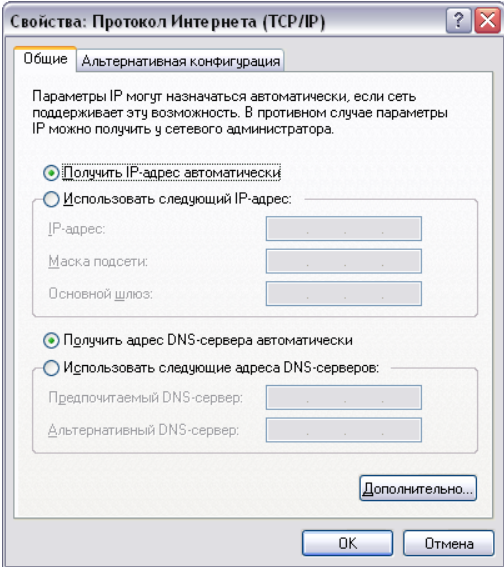
Management / Update Software	
Step 1:	Obtain an updated software image file from your ISP.
Step 2:	Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
Step 3:	Click the "Update Software" button once to upload the new image file.
NOTE:	The update process takes about 2 minutes to complete, and your Broadband Router will reboot.
Software File Name:	<input type="button" value="Выберите файл"/> Файл не выбран
<input type="button" value="Update Software"/>	

4.6.7 Подменю «Reboot». Перегрузка устройства



Для перезагрузки устройства необходимо нажать на кнопку «Reboot». Перегрузка устройства может занять несколько минут.

ПРИЛОЖЕНИЕ А. ВОЗМОЖНЫЕ ПРОБЛЕМЫ И ВАРИАНТЫ ИХ РЕШЕНИЯ

Проблема	Возможная причина	Решение
При вводе IP-адреса маршрутизатора (например, 192.168.0.1) не удается получить доступ к web-интерфейсу.	Компьютер не принадлежит к данной IP-подсети для подключения к web-интерфейсу.	В свойствах подключения к интернету на вашем компьютере установите параметр «Получать IP-адрес автоматически». 
	На компьютере установлен web-браузер с выключенной опцией Java-script.	Включите опцию Java-script в вашем браузере или воспользуйтесь другим web-браузером.
	Неисправный кабель.	Проверьте физическое соединение по статусу индикаторов (они должны гореть). Если индикаторы не горят, попробуйте использовать другой кабель или подключитесь к другому порту устройства, если это возможно. Если компьютер выключен, индикатор может не гореть.
	Доступ запрещен программным обеспечением интернет-безопасности вашего компьютера.	Отключите программное обеспечение интернет-безопасности на компьютере (брандмауэры).
Воспроизводится сигнал ошибки в телефоне, подключенном к порту FXS.	Неверные настройки порта.	Проверьте корректность настроек в меню «VoIP» (см. раздел 4.3.2 Подменю «SIP Advanced Settings»). Дополнительные настройки SIP).
Утерян/не подходит пароль доступа к web-интерфейсу устройства.	_____	Необходимо сбросить маршрутизатор к настройкам по умолчанию с помощью кнопки «Reset» на задней панели устройства. К сожалению, при этом все выполненные настройки будут утрачены.

ПРИЛОЖЕНИЕ Б. ИСПОЛЬЗОВАНИЕ ДОПОЛНИТЕЛЬНЫХ УСЛУГ

1. Уведомление о поступлении нового вызова — «Call Waiting»

Услуга позволяет пользователю при занятости его телефонным разговором с помощью определенного сигнала получить оповещение о новом входящем вызове.

Пользователь при получении оповещения о новом вызове может принять ожидающий вызов.

Доступ к услуге устанавливается через меню настроек абонентского порта на странице «*VoIP/SIP Advanced Settings*» (раздел 4.3.2 Подменю «**SIP Advanced Settings**». **Дополнительные настройки SIP**) путем установки флага «*Call waiting*».

Использование услуги:

Находясь в состоянии разговора и при получении индикации о поступлении нового вызова, нажав R, возможно принять ожидающий вызов с установкой текущего соединения на удержание. Последующие нажатия R обрабатываются в соответствии с алгоритмами, описанными в разделе **2. Передача вызова** и **3. Конференция**.

- R — короткий отбой (flash).

2. Передача вызова — «Calltransfer»

Услуга «**Calltransfer**» позволяет временно разорвать соединение с абонентом, находящимся на связи (абонент А), установить соединение с другим абонентом (абонент С) и передать вызов с отключением абонента В (абонента, выполняющего услугу).

Использование услуги:

Находясь в состоянии разговора с абонентом А, установить его на удержание с помощью короткого отбоя flash (R), дождаться сигнала «ответ станции» и набрать номер абонента С. После ответа абонента С положить трубку.

3. Конференция — «Conference»

Конференция — услуга, обеспечивающая возможность одновременного телефонного общения трех и более абонентов.

Доступ к услуге устанавливается через меню настроек абонентского порта на странице «*VoIP/SIP Advanced Settings*» (раздел 4.3.2 Подменю «**SIP Advanced Settings**». **Дополнительные настройки SIP**) путем установки флага «*Call hold*».

Использование услуги:

Находясь в состоянии разговора с абонентом А, установить его на удержание с помощью короткого отбоя flash (R), дождаться сигнала «ответ станции» и набрать номер абонента С. После ответа абонента С, нажав R, перейти в режим конференц-связи.

Абонент, собравший конференцию, является ее инициатором, другие два абонента — ее участниками. В режиме конференции нажатие короткого отбоя flash инициатором приводит к отключению абонента, вызов которому был совершен последним. Участник конференции имеет возможность поставить на удержание остальных членов конференции.

Конференция завершается, если ее покидает инициатор, другим участникам при этом будет передано сообщение отбоя. Если конференцию покидает любой из участников, то ее инициатор и второй участник переключатся в состояние обычного двустороннего разговора.

4. Message Waiting Indication (MWI) — индикация о наличии голосовых сообщений в почтовом ящике

Если абоненту оставлено на сервере голосовое сообщение, то включение данной услуги предоставит возможность своевременно узнать об этом. При включенной услуге MWI, если на сервере имеется новое сообщение, абонент при поднятии трубки услышит прерывистый зуммер.

Для включения услуги MWI необходимо на странице «*VoIP/SIP Advanced Settings*» (**раздел 4.3.2 Подменю «SIP Advanced Settings». Дополнительные настройки SIP**) установить флаг в поле «*MWI*» для требуемого порта.

5. Запрет на исходящие вызовы — «Call Barring»

Услуга позволяет установить ограничение на доступ с телефонного аппарата абонента к определенным видам исходящей связи.

Доступ к услуге осуществляется через меню настроек абонентского порта на странице «*VoIP/SIP Advanced Settings*» (**раздел 4.3.2 Подменю «SIP Advanced Settings». Дополнительные настройки SIP**) путем установки флага «*Call barring*» и задания необходимых параметров в полях «*Call barring mode*» и «*Call barring digit map*».

Возможно 3 варианта ограничения вызовов в зависимости от параметра, указанного в поле «*Call barring mode*»:

- *Allow all* — все исходящие звонки разрешены;
- *Deny all* — все исходящие звонки запрещены;
- *Deny by digit map* — исходящие звонки запрещены только на номер, указанный в поле «*Call barring digit map*».

Использование услуги:

Значение «*Call barring digit map*» — 1150. Для ограничения всех исходящих вызовов в поле «*Call barring mode*» необходимо выбрать значение «*Deny all*». Для того чтобы разрешить все исходящие вызовы, требуется выбрать «*Allow all*». Для запрета исходящих звонков на номер 1150 необходимо задать «*Deny by digit map*» в поле «*Call barring mode*».

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «ЭЛТЕКС» Вы можете обратиться в Сервисный центр компании:

Форма обратной связи на сайте: [**https://eltex-co.ru/support/**](https://eltex-co.ru/support/)
Servicedesk: [**https://servicedesk.eltex-co.ru**](https://servicedesk.eltex-co.ru)

На официальном сайте компании Вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к базе знаний, оставить интерактивную заявку или проконсультироваться у инженеров Сервисного центра на техническом форуме.

Официальный сайт компании: [**https://eltex-co.ru/**](https://eltex-co.ru/)
Технический форум: [**https://eltex-co.ru/forum**](https://eltex-co.ru/forum)
База знаний: [**https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base**](https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base)
Центр загрузок: [**https://eltex-co.ru/support/downloads**](https://eltex-co.ru/support/downloads)