

Абонентские оптические терминалы

NTE-RG-1402 rev.B

Руководство по эксплуатации, версия 1.4 (26.04.2018)
Версия ПО 3.14.5

IP-адрес: **192.168.0.1**
имя пользователя: **user**
пароль: **user**

Текущая версия ПО: 3.14.5			
Версия документа	Актуальность для ПО	Дата выпуска	Содержание изменений
Версия 1.4	3.14.5.924	26.04.2018	Пятая публикация
Версия 1.3	3.14.3.43	05.08.2015	Четвертая публикация
Версия 1.2	3.14.2.22	11.03.2014	Третья публикация
Версия 1.1	3.12.2.22	04.01.2014	Вторая публикация
Версия 1.0	3.6.122	12.11.2012	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

ПРИМЕЧАНИЯ И ПРЕДУПРЕЖДЕНИЯ	2
1 ВВЕДЕНИЕ	5
2 ОПИСАНИЕ ИЗДЕЛИЯ.....	6
2.1 Назначение	6
2.2 Варианты исполнения.....	6
2.3 Характеристика устройства.....	7
2.4 Основные технические параметры.....	9
2.5 Конструктивное исполнение	11
2.6 Световая индикация.....	13
2.6.1 Индикация интерфейсов LAN.....	14
2.7 Перегрузка/сброс к заводским настройкам.....	14
2.8 Комплект поставки	14
3 НАСТРОЙКА NTE-RG-14XX REV.В ЧЕРЕЗ WEB-ИНТЕРФЕЙС. ДОСТУП ПОЛЬЗОВАТЕЛЯ	15
3.1 Меню «Device Info». Информация об устройстве	16
3.1.1 Подменю «Summary». Общая информация об устройстве.....	16
3.1.2 Подменю «WAN». Информация о состоянии сервисов.....	16
В данном меню производится мониторинг состояния сетевых сервисов.	16
Для просмотра доступна следующая информация о сервисах:.....	16
3.1.3 Подменю «SIP». Мониторинг состояния телефонных портов.....	17
В данном меню доступен просмотр статуса FXS портов и параметры SIP-аккаунтов.....	17
3.1.4 Подменю «LAN». Мониторинг состояния портов LAN. Мониторинг статуса Wi-Fi интерфейса	17
3.1.5 Подменю «Authenticated Wireless Station». Подключенные беспроводные устройства	18
3.1.6 Подменю «ARP». Просмотр кэша протокола ARP	18
3.1.7 Подменю «DHCP». Активные аренды DHCP	18
В таблице DHCP можно посмотреть список активных аренд DHCP-сервера и срок их истечения.	18
3.1.8 Подменю «Route». Просмотр таблицы маршрутизации.....	19
3.1.9 Подменю «Statistics». Информация о прохождении трафика на портах устройства.....	19
3.2 Меню «PPP settings». Настройки PPP.....	21
3.3 Меню «VPN». Настройки клиента L2TP	21
3.4 Меню «SIP Settings». Настройки SIP.....	24
3.5 Меню «VoIP. SIP Advanced Setting». Дополнительные настройки SIP	24
3.6 Меню «Wi-Fi» . Настройка беспроводной сети	25
3.6.1 Подменю «Basic». Общая информация	25
3.6.2 Подменю «Security». Настройка параметров безопасности	26
3.6.3 Подменю «MAC Filter». Настройки фильтрации MAC-адресов.....	29
3.6.4 Подменю «Wireless Bridge». Настройки беспроводного соединения в режиме моста	30
3.6.5 Подменю «Advanced». Расширенные настройки.....	31
3.7 Меню «LAN». Настройки локальной сети.....	33
3.7.1 Подменю «General Settings». Настройка основных параметров	33
3.7.2 Подменю «VLAN Settings». Настройка параметров VLAN.....	34
3.8 Меню «Port Mapping»	35
3.9 Меню «NAT». Настройки NAT.....	35
3.9.1 Подменю «Virtual Servers». Настройки виртуальных серверов	35
3.9.2 Подменю «Port Triggering». Настройки запуска портов	37
3.9.3 Подменю «DMZ Host». Настройки демилитаризованной зоны	38
3.10 Меню «IPSec». Настройка защиты данных по протоколу IP.....	38
3.11 Меню «Storage Device Info». Службы файловых хранилищ	41
3.12 Меню «UPnP». Автоматическая настройка сетевых устройств	41
3.13 Меню «Dynamic DNS». Настройка динамической системы доменных имен	41
3.14 Меню «Security». Настройки безопасности	43
3.14.1 Подменю «IP Filtering». Настройки фильтрации адресов	43

3.14.2	Подменю «MAC Filtering». Настройки фильтрации по MAC- адресам	45
3.15	Меню «Parental control» . «Родительский контроль» – настройки ограничения.....	47
3.15.1	Подменю «Time Restriction». Настройки ограничения продолжительности сеансов	47
3.15.2	Подменю «Url Filter». Настройки ограничения доступа к адресам в интернет	48
3.16	Меню «Management». Настройки управления	48
3.16.1	Подменю «Restore Default». Сброс к настройкам по умолчанию	48
3.16.2	Подменю «System Log». Настройки системного журнала.....	49
3.16.3	Подменю «Internet Time». Настройки системного времени устройства	50
3.16.4	Подменю «Ping». Проверка доступности сетевых устройств.....	51
3.16.5	Подменю «Passwords». Настройка контроля доступа (установление паролей)	51
3.16.6	Подменю «Update Software». Обновление ПО	51
3.16.7	Подменю «Access Control». Управление доступом.....	52
3.16.8	Подменю «Reboot». Перезагрузка устройства	52
ПРИЛОЖЕНИЕ А ВОЗМОЖНЫЕ ПРОБЛЕМЫ И ВАРИАНТЫ ИХ РЕШЕНИЯ		53
ПРИЛОЖЕНИЕ Б ИСПОЛЬЗОВАНИЕ ДОПОЛНИТЕЛЬНЫХ УСЛУГ		54
СВИДЕТЕЛЬСТВО О ПРИЕМКЕ И ГАРАНТИИ ИЗГОТОВИТЕЛЯ		56

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 серии *NTE-RG-1402 rev.B* обеспечивают подключение аналоговых телефонных аппаратов к сетям пакетной передачи данных.

В настоящем руководстве по эксплуатации изложены назначение, основные технические характеристики, правила конфигурирования, мониторинга и смены программного обеспечения оптических терминалов серии *NTE-RG rev.B*.

2 ОПИСАНИЕ ИЗДЕЛИЯ

2.1 Назначение

Устройства серии *NTE-RG rev.B* GEAPON ONT (Gigabit Ethernet Passive Optical Network) обеспечивают соединение по оптическому каналу с устройством GEAPON класса OLT (оптическое терминальное оборудование) и соединение до 10/100/1000Мбит/с с конечным пользователем LAN. Главным преимуществом технологии Turbo GEAPON 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. К каждому устройству серии *NTE-RG rev.B* можно подключить до четырех компьютеров, доступ в интернет для которых возможен с помощью встроенных функций роутинга.

2.2 Варианты исполнения

Существует четыре варианта исполнения устройств серии *NTE-RG rev.B*, отличающихся набором интерфейсов и функциональными возможностями, Таблица 1.

Таблица 1 – Варианты исполнения

Наименование модели	Наличие интерфейса WAN	Количество портов интерфейса LAN	Количество портов FXS	Наличие Triplexer	Наличие Wi-Fi
Серия <i>NTE-RG-1402 rev.B</i>					
<i>NTE-RG-1402G rev.B</i>	SFF	4 Gigabit	2	-	-
<i>NTE-RG-1402G-W rev.B</i>	SFF	4 Gigabit	2	-	+
<i>NTE-RG-1402GC rev.B</i>	SFF	4 Gigabit	2	+	-
<i>NTE-RG-1402GC-W rev.B</i>	SFF	4 Gigabit	2	+	+

Устройства моделей *NTE-RG-1402G-W rev.B*, *NTE-RG-1402GC-W rev.B* имеют встроенный адаптер Wi-Fi с возможностью подключения до двух внешних антенн. Встроенный адаптер Wi-Fi поддерживает стандарты 802.11n, 802.11b, 802.11g, что позволяет предоставлять услуги передачи данных беспроводной сети с более высоким качеством сервиса по сравнению с устройствами, поддерживающими стандарт 802.11n, оставаясь при этом обратно совместимым с устройствами с поддержкой 802.11g и 802.11b.

Устройства моделей *NTE-RG-1402GC rev.B*, *NTE-RG-1402GC-W rev.B* имеют встроенный приемопередатчик Triplexer, посредством которого реализуется функция совместной передачи данных и предоставление услуг кабельного телевидения (CaTV).

2.3 Характеристика устройства

Устройство имеет следующие интерфейсы:

- 2 порта 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 оконечного оборудования: 10/100/1000BASE-T;
- Приемопередатчик Wi-Fi 802.11n, 802.11b, 802.11g¹;
- Порт USB2.0 - для подключения внешних накопителей USB или HDD;
- Порт SMB для подключения телевизионного кабеля².

Питание терминала осуществляется через внешний адаптер 12 В постоянного тока от сети 220 В.

Устройство поддерживает 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;
 - Firewall;
 - поддержка NTP;
 - поддержка механизмов качества обслуживания QoS;
 - поддержка IGMP-snooping;
 - поддержка IGMP-proxy;
 - поддержка функции Parental Control;
 - поддержка функции Storage service.
- *IP-телефония:*
 - поддержка протокола SIP;
 - ToS для пакетов RTP;
 - ToS для пакетов SIP;
 - эхо компенсация (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;
 - безусловная переадресация - Forward unconditionally;
 - переадресация по неответу - Forward on "no answer";
 - переадресация по занятости – Forward on Busy;
 - переадресация по неответу – Call FWD – No Reply;
 - определитель номера Caller ID по ETSI FSK;

¹ Только для моделей NTE-RG-1402G-W Rev.B, NTE-RG-1402GC-W Rev.B.

² Только для моделей NTE-RG-1402GC Rev.B, NTE-RG-1402GC-W Rev.B.

- 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;
- "не беспокоить" – DND.

- обновление ПО через Web-интерфейс;
- удаленный мониторинг, конфигурирование и настройка:
 - TR-069,
 - Web-интерфейс,
 - Telnet.

На рисунке 1 приведена схема применения оборудования NTE-RG-1402 rev.B на примере NTE-RG-1402GC-W rev.B.

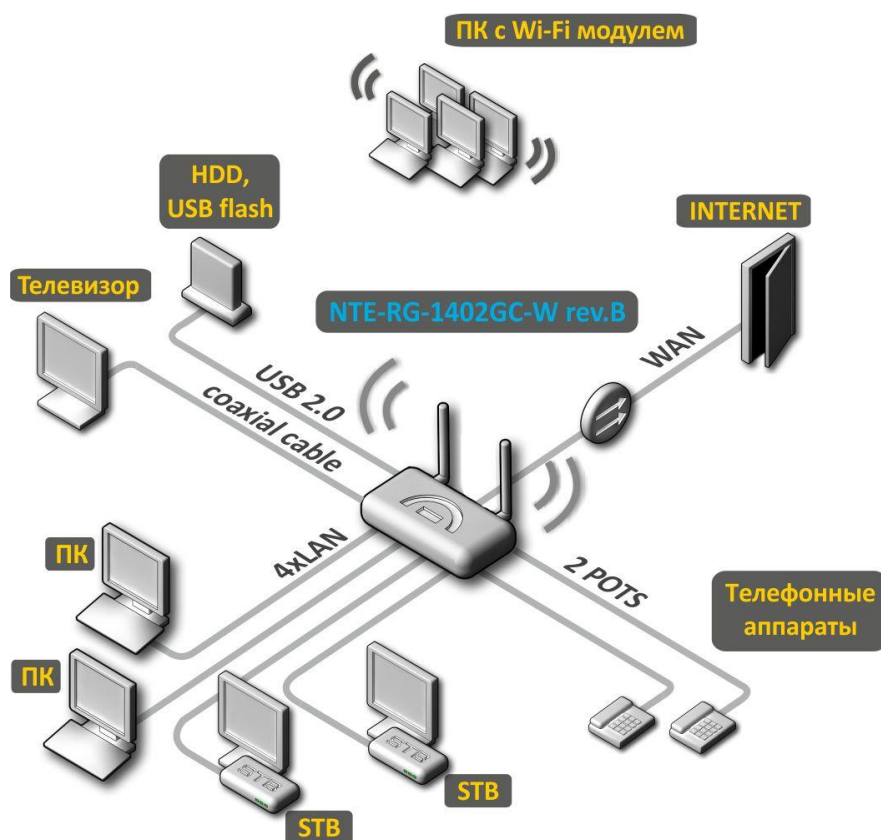


Рисунок 1 – Схема применения NTE-RG-1402GC-W rev.B

2.4 Основные технические параметры

Основные технические параметры терминала приведены в таблице 2:

Таблица 2 – Основные технические параметры
Протоколы VoIP

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

Аудиокодеки

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

Параметры интерфейсов Ethernet LAN

Количество интерфейсов	4
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
Электрический разъем	RJ-45
Скорость передачи, Мбит/с	Автоопределение, 10/100/1000 Мбит/с, дуплекс/ полудуплекс
Поддержка стандартов	Ethernet 10/100/1000 Base-T

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	До 10 км
Передатчик:	1310 Нм
Скорость соединения upstream	1244 Мбит/с
Мощность передатчика	-2..+3 дБм
Ширина спектра опт. излучения (RMS)	3 Нм
Приемник	1490Нм
Скорость соединения downstream	2488 Мбит/с
Чувствительность приемника	от -3 до -23дБм

Параметры аналоговых абонентских портов

количество портов	2
сопротивление шлейфа	До 2 кОм
прием набора	Импульсный/частотный (DTMF)
выдача Caller ID	Есть

Параметры беспроводного интерфейса Wi-Fi¹

Стандарт	IEEE 802.11b/g/n
Частотный диапазон	2.400 ~ 2.497 ГГц
Модуляция	PSK/CCK, DQPSK, DBPSK, OFDM
Скорость передачи данных, Мбит/с	802.11b: 11, 5.5, 2, 1 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 802.11n 20MHz BW: 130, 117, 104, 78, 52, 39, 26, 13 802.11n 40MHz BW: 270, 243, 216, 162, 108, 81, 54, 27
Максимальная выходная мощность передатчика	802.11b: 17dBm +/-1.5 дБм 802.11g: 15dBm +/-1.5 дБм 802.11n: 14.75dBm +/-1.5 дБм
MAC-протокол	CSMA/CA модель ACK 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 7 32/64, Linux, VxWorks
Количество антенн	2 антенны
Коэффициентом усиления антенны	3 дБи
Рабочий диапазон температур	От 0 до +70°C

Характеристика SaTV²

Разъем для RF-выхода	Тип SMB
Поддержка стандартов	ITU-T G.984.2, IEC 60825-1 EEC Directive 2002/95/EC (RoHS)
Рабочая длина волны SaTV ³	1550 Нм
Оптическая мощность на входе	-8÷2 дБм
Порог повреждения	+5 дБм
Диапазон частот выходного сигнала	47÷870 МГц
Уровень выходного сигнала RF	17 дБмВ/Ch.

Управление

Локальное управление	Web-интерфейс
Удаленное управление	По протоколу Telnet, TR-069, OAM
Ограничение доступа	По паролю

Общие параметры

Питание	Адаптер питания 12В DC /220 AC	
Потребляемая мощность	NTE-RG-1402G rev.B	Не более 14 Вт
	NTE-RG-1402G-W rev.B	Не более 14 Вт
Рабочий диапазон температур	От +5 до +40°C	
Относительная влажность	До 80%	
Габариты	218x120x49 мм	
Масса устройства	0,3 кг	

¹ Только для моделей NTE-RG-1402G(C)-W Rev.B

² Только для моделей NTE-RG-1402GC-(W) Rev.B

³ Данные приведены для Ligent LTY9775A

2.5 Конструктивное исполнение

Абонентские терминалы серии *NTE-RG-1402 rev.B* выполнены в виде настольных изделий в пластиковом корпусе.

Внешний вид передних панелей устройств серии *NTE-RG-1402 rev.B* приведен на рисунке 2.

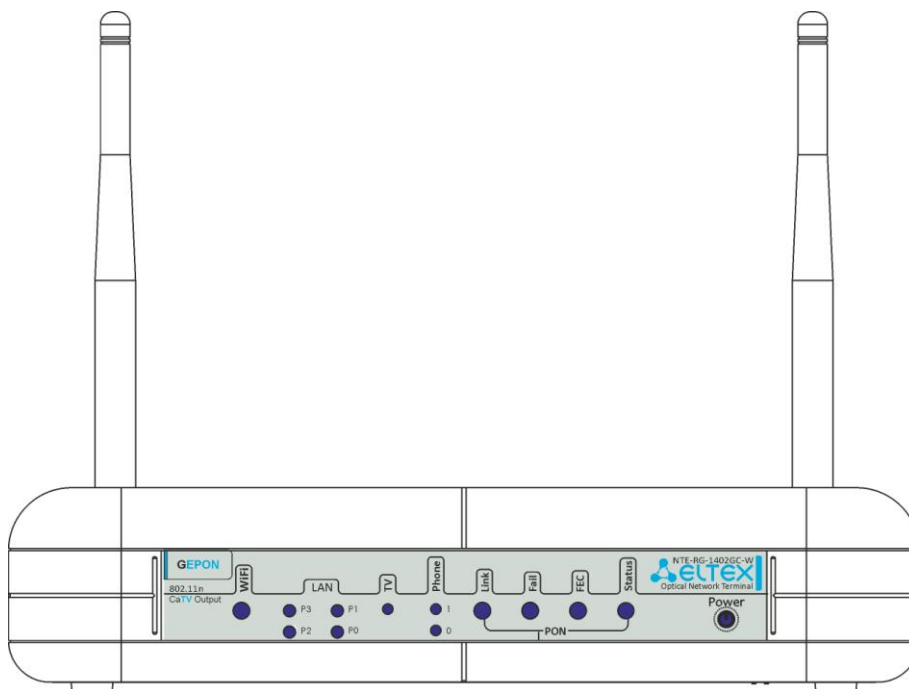


Рисунок 2 – Внешний вид передней панели NTE- RG-1402G-W rev.B

На передней панели устройств серии *NTE-RG* расположены следующие световые индикаторы, таблица 3.

Таблица 3 – Описание индикаторов передней панели

Элемент передней панели		Описание
Wi-Fi¹		Индикатор активности Wi-Fi
TV²		Индикатор работы CaTV
LAN	P0	Индикаторы работы Ethernet-портов
	P1	
	P2	
	P3	
Phone		Индикатор активности портов FXS
Status		Индикатор сигнализации прохождения авторизации устройства
PON		Индикатор работы оптического интерфейса
Power		Индикатор питания и статуса работы

¹ Только для моделей NTE-RG-1402G(C)-W rev.B

² Только для моделей NTE-RG-1402GC-(W) rev.B

Внешний вид задних панелей устройств серии *NTE-RG-1402 rev.B* приведен на рисунке 3.

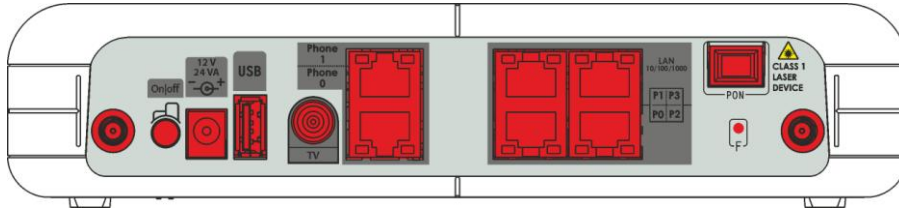


Рисунок 3 – Внешний вид задней панели NTE-RG-1402G-W rev.B

На задней панели устройства расположены следующие разъемы и органы управления, таблица 4.

Таблица 4 – Описание разъемов, и органов управления задней панели

Элемент задней панели		Описание
On/Off		Тумблер питания
12V		Разъем подключения электропитания адаптера питания
USB		Разъем для подключения внешних накопителей и других USB-устройств
TV		Разъем для подключения телевизионного кабеля
Phone0, Phone 1		Разъемы RJ-11 для подключения аналоговых телефонных аппаратов
LAN	P0	Разъем RJ-45 для подключения сетевых устройств
	P1	Разъем RJ-45 для подключения сетевых устройств
	P2	Разъем RJ-45 для подключения сетевых устройств
	P3	Разъем RJ-45 для подключения сетевых устройств
PON		Разъем SC (розетка) <i>PON</i> оптического интерфейса GEPON
F		Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам
Разъемы для антенны		Разъемы предназначены для присоединения антенн Wi-Fi

2.6 Световая индикация

Текущее состояние устройства отображается при помощи индикаторов *Wi-Fi*, *P0..P3*, *Phone 0*, *Phone 1*, *TV*, *PON*, *Status*, *Power* – расположенных на передней панели.

Перечень состояний индикаторов приведен в таблице 5.

Таблица 5 – Световая индикация устройства

Индикатор	Состояние индикатора	Состояние устройства
<i>Wi-Fi</i> ¹	зеленый	сеть Wi-Fi активна
	мигает	процесс передачи данных по Wi-Fi
	не горит	сеть Wi-Fi не активна
Индикаторы LAN 10/100/1000		
<i>P0, P1, P2, P3</i>	зеленый	установлено соединение 10/100 Мбит/с
	оранжевый	установлено соединение 1000 Мбит/с
	мигает	процесс пакетной передачи данных
<i>TV</i> ²	не горит	RF порт отключен
	красный	отсутствие телевизионного сигнала
	оранжевый	уровень сигнала не соответствует нормальному (выше +2 дБм или ниже -8 дБм)
	зеленый	уровень сигнала в норме
<i>Phone 0, Phone 1</i>	зеленый	телефонная трубка снята
	мигает	порт не зарегистрирован или не пройдена авторизация на SIP-сервере
	медленно мигает	прием сигнала вызова
<i>PON</i>	не горит	процесс загрузки устройства
	зеленый	установлено соединение между стационарным оптическим терминалом и устройством
	красный	нет сигнала от стационарного оптического терминала
<i>Status</i>	не горит	установлен режим работы static или bridge для интерфейса wan, PPP-клиент не запущен
	зеленый	устройство успешно прошло авторизацию на стационарном терминале (поднята PPP сессия на интерфейсе wan)
	оранжевый	устройство не прошло авторизацию (PPP сессия не поднята на интерфейсе wan)
<i>Power</i>	не горит	Устройство отключено от сети питания или неисправно
	зеленый	Текущая конфигурация устройства отличается от конфигурации по умолчанию
	оранжевый	установлена конфигурация по умолчанию
	красный	Устройство находится в процессе загрузки

¹ Только для моделей NTE-RG-1402G(C)-W rev.B

² Только для NTE-RG-1402GC-(W) rev.B

2.6.1 Индикация интерфейсов LAN

Режимы работы, отображаемые индикаторами на портах LAN на задней панели устройства, приведены в таблице 6.

Таблица 6 – Световая индикация интерфейсов LAN

Режимы работы	Желтый индикатор	Зеленый индикатор
Порт работает в режиме 1000Base-T, нет передачи данных	Горит постоянно	Горит постоянно
Порт работает в режиме 1000Base-T, есть передача данных	Горит постоянно	Мигает
Порт работает в режиме 10/100Base-TX, нет передачи данных	Не горит	Горит постоянно
Порт работает в режиме 10/100Base-TX, есть передача данных	Не горит	Мигает

2.7 Перегрузка/сброс к заводским настройкам

Для перезагрузки устройства нужно однократно нажать кнопку «F» на задней панели изделия. Для загрузки устройства с заводскими настройками необходимо нажать и удерживать кнопку «F» 7-10 сек, 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 P0 и P1.

2.8 Комплект поставки

В базовый комплект поставки устройства серии NTE-RG входят:

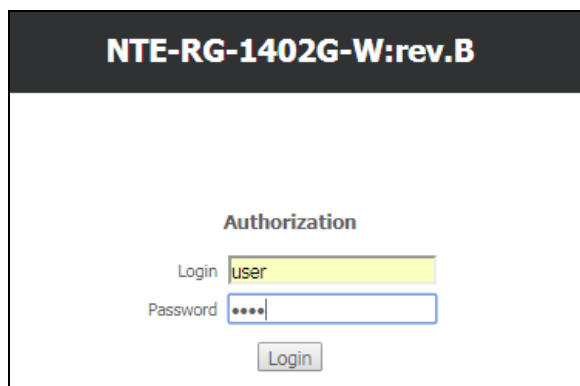
- абонентский оптический терминал серии NTE-RG;
- адаптер питания 220 В/12 В;
- руководство по эксплуатации;
- антенны Wi-Fi¹ - 2 шт.

¹ Только для моделей NTE-RG-1402G(C)-W rev.B

3 НАСТРОЙКА NTE-RG-14XX REV.B ЧЕРЕЗ WEB-ИНТЕРФЕЙС. ДОСТУП ПОЛЬЗОВАТЕЛЯ

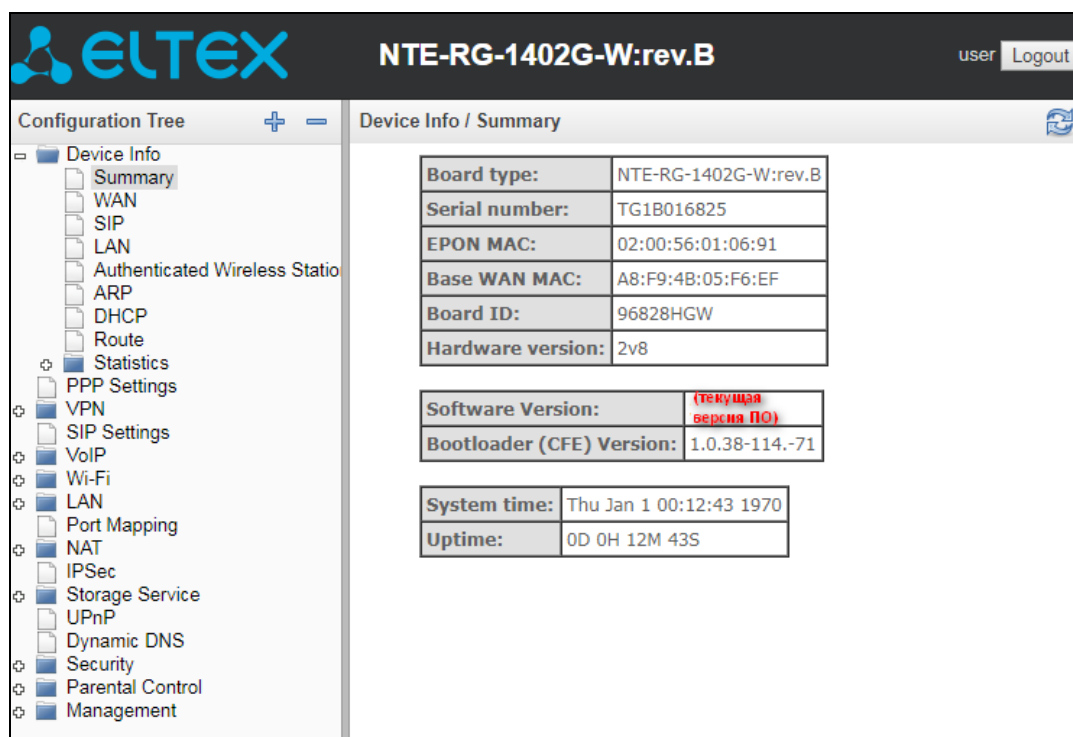
Для того чтобы произвести конфигурирование устройства, необходимо подключиться к нему через Web-браузер (программу для просмотра гипертекстовых документов), например, Firefox, Internet Explorer. Для этого необходимо ввести в адресной строке браузера IP-адрес устройства (при заводских установках адрес: - 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**.

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



Board type:	NTE-RG-1402G-W:rev.B
Serial number:	TG1B016825
EPON MAC:	02:00:56:01:06:91
Base WAN MAC:	A8:F9:4B:05:F6:EF
Board ID:	96828HGW
Hardware version:	2v8

Software Version:	(текущая версия ПО)
Bootloader (CFE) Version:	1.0.38-114.-71

System time:	Thu Jan 1 00:12:43 1970
Uptime:	0D 0H 12M 43S

3.1 Меню «Device Info». Информация об устройстве

3.1.1 Подменю «Summary». Общая информация об устройстве

Device Info / Summary	
Board type:	NTE-RG-1402G-W:rev.B
Serial number:	TG1B016825
EPON MAC:	02:00:56:01:06:91
Base WAN MAC:	A8:F9:4B:05:F6:EF
Board ID:	96828HGW
Hardware version:	2v8
Software Version:	(текущая версия ПО)
Bootloader (CFE) Version:	1.0.38-114.-71
System time:	Thu Jan 1 00:16:51 1970
Uptime:	0D 0H 16M 51S

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

3.1.2 Подменю «WAN». Информация о состоянии сервисов

В данном меню производится мониторинг состояния сетевых сервисов.

Для просмотра доступна следующая информация о сервисах:

- *Interface* – имя интерфейса;
- *Type* – режим работы интерфейса;
- *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 интерфейсов.

Device Info / WAN	
WAN service 0: INTERNET.1	
Interface	ppp0.1
Type	PPPoE
Status	Connected
IPv4 Address	192.168.100.112
Primary DNS Server	192.168.100.1
Secondary DNS Server	10.10.0.2
Bridging to	eth0.0,eth1.0,wl0
WAN service 1: IGMP.2	
Interface	epon0.2
Type	IPoE
Status	Connected
IPv4 Address	192.168.21.21
Default Gateway	192.168.21.1
Bridging to	eth0.0,eth1.0,wl0

¹ Только для сервиса **INTERNET**

3.1.3 Подменю «SIP». Мониторинг состояния телефонных портов

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

Device Info / SIP		
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 0	Account 1
State	Up	Up
Error	None	None
Response code	200 OK	200 OK
Account enabled	Enabled	Enabled
Extension	4000	4001
Display name	4000	4001
Authentication name	4000	4001

- *Voice daemon status* – состояние работы голосового демона;
- *SIP Proxy* – адрес и порт SIP Proxy;
- *SIP Outbound Proxy* – адрес и порт SIP proxy, 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 0, Account 1* – номер аккаунта SIP;
- *State* – статус аутентификации;
- *Error¹* – ошибка, выдаваемая сервером SIP;
- *Response code* – код ответа сервера SIP;
- *Account enabled* – состояние аккаунта SIP;
- *Extension* – номер телефона;
- *Display name* – отображаемое имя пользователя;
- *Authentication name* – имя пользователя для аутентификации.

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

В данном меню 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 0	Up; 100M full
Port 1	Down
Port 2	Down
Port 3	Down
Wi-Fi	Down

¹ В текущей версии ПО не поддерживается

3.1.5 Подменю «Authenticated Wireless Station». Подключенные беспроводные устройства

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

Device Info / Authenticated Wireless Stations				
This page shows authenticated wireless stations and their status.				
MAC	Associated	Authorized	SSID	Interface
74:DE:2B:FD:59:D9	Yes	Yes	ELTEX-89F8	wl0
Refresh				

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».

3.1.6 Подменю «ARP». Просмотр кэша протокола ARP

Эффективность функционирования ARP во многом зависит от ARP-кэша, который присутствует на каждом хосте. В кэше содержатся Internet-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
60.0.0.102	Complete	bc:5f:f4:04:a3:e7	br3
151.0.0.1	Complete	00:1b:21:c4:0d:58	epon0.6
192.168.0.33	Complete	00:1b:21:c4:0a:cd	br0

- *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.

3.1.7 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
vladimir303	00:1b:21:c4:0a:cd	192.168.0.2	23 hours, 50 minutes, 15 seconds

- *Hostname* – имя хоста (сетевого 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.

3.1.8 Подменю «Route». Просмотр таблицы маршрутизации

В меню осуществляется просмотр таблицы маршрутизации.

Device Info / Route						
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect).						
Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
50.0.0.102	0.0.0.0	255.255.255.255	UH	0	INTERNET	ppp0.1
1.2.3.0	0.0.0.0	255.255.255.0	U	0		br1
192.168.21.0	0.0.0.0	255.255.255.0	U	0	IGMP	epon0.2
192.168.0.0	0.0.0.0	255.255.255.0	U	0		br0
151.0.0.0	0.0.0.0	255.255.0.0	U	0	ACS	epon0.6
60.0.0.0	0.0.0.0	255.0.0.0	U	0		br3
0.0.0.0	50.0.0.102	0.0.0.0	UG	0	INTERNET	ppp0.1

- *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.

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

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

Интерфейс LAN:

Device Info / Statistics / LAN								
Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Port 0	572083	5227	0	0	3649744	7114	0	0
Port 1	0	0	0	0	0	0	0	0
Port 2	0	0	0	0	0	0	0	0
Port 3	0	0	0	0	0	0	0	0
Wi-Fi	13655	177	0	0	34204	114	0	0

WAN Service:

Device Info / Statistics / WAN Service

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
epon0.2	IGMP	8128	174	0	0	0	0	0	0
epon0.3	STB	0	0	0	0	0	0	0	0
epon0.4	OTHER	0	0	0	0	0	0	0	0
epon0.5	VOIP	1512768	32367	0	0	44025	647	0	0
epon0.6	Tr069	1658182	21640	0	0	3312141	3619	0	0
ppp0.1	INTERNET	26438	340	0	0	30042	492	0	0

Reset Statistics

Интерфейс Optical:

Для устройств серии NTE-RG-1402GC-(W) rev.B с возможностью приема услуг кабельного телевидения (CaTV) данное меню имеет дополнительную таблицу, в которой доступны следующие данные:

- статус оптического линка,
- уровень принимаемого сигнала (1490нм),
- уровень передаваемого сигнала (1310нм),
- уровень принимаемого аналогового видео-сигнала (CaTV 1550нм).

Вид меню для устройств
серии NTE-RG-1402G-(W) rev.B

Device Info / Statistics / Optical

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Optical	115427971	87889	0	0	5134219	5254	0	0

Reset Statistics

Вид меню для устройств
серии NTE-RG-1402GC-(W) rev.B

Device Info / Statistics / Optical

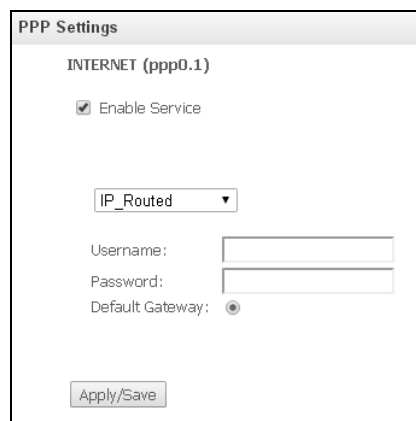
Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Optical	8639	134	0	0	40100	185	0	0

Reset Statistics

Link Status	Optical Signal Level	Transmit Optical Level	Optical Video Level
Down	No signal	No signal	No signal

Для обнуления данных и возобновления накопления статистики необходимо нажать «Reset Statistic».

3.2 Меню «PPP settings». Настройки PPP¹



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;
- *Default Gateway* – данный интерфейс используется в качестве шлюза по умолчанию.

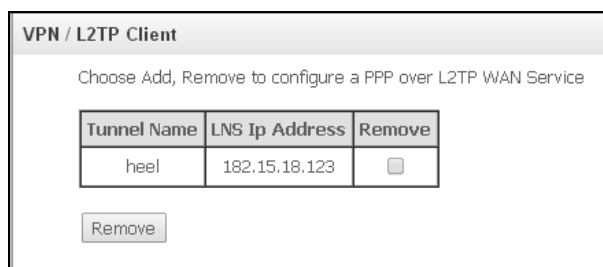


При выборе режима работы PPPoE_Bridged поля *Username* и *Password* недоступны = логин и пароль вводятся на ПК пользователя.

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

3.3 Меню «VPN». Настройки клиента L2TP

L2TP (*Layer 2 Tunneling Protocol* – протокол туннелирования второго уровня) – в компьютерных сетях туннельный протокол, использующийся для поддержки виртуальных частных сетей. Данный протокол позволяет создавать туннель не только в сетях IP, но и в таких, как ATM, X.25 и Frame Relay. L2TP является протоколом Сеансового уровня и использует зарегистрированный UDP-порт 1701.



Tunnel Name	LNS Ip Address	Remove
heel	182.15.18.123	<input type="checkbox"/>

Для добавления туннеля необходимо нажать кнопку «Add», для удаления – установить флаг в колонке «Remove» и нажать одноименную кнопку.

¹ При отсутствии меню в конфигураторе данные настройки уже выполнены Вашим оператором связи.

VPN / L2TP Client

Add a L2TP Client Side PPP Connection (PPPoL2TP WAN Service)

Tunnel Name

L2TP Server Ip Address

- *Tunnel name* – имя туннеля;
- *L2TP Server IP Address* – IP-адрес L2TP-сервера.

Переход к дальнейшим настройкам осуществляется кнопкой «Next».

VPN / L2TP Client

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

Enable NAT

Enable Firewall

Enable Fullcone NAT

Establish the connection:

Disconnect on idle

Inactivity Timeout (minutes) [1-4320]:

Use Static IPv4 Address

IPv4 Address:

Enable PPP Debug Mode

Multicast Proxy

Enable IGMP Multicast Proxy

- *PPP Username* – имя пользователя для авторизации;
- *PPP Password* – пароль для авторизации;
- *PPPoE Service Name* – имя сервиса авторизации;
- *Authentication Method* – метод авторизации (AUTO, PAP, CHAP, MSCHAP);
- *Enable NAT* – при установленном флаге разрешено преобразование сетевых адресов, иначе – запрещено;
- *Enable Firewall* – при установленном флаге активен межсетевой экран, иначе - не активен;
- *Enable Fullcone NAT* – при установленном флаге включен тип трансляции NAT «Полный конус»;
- *Establish the connection* – режим установки соединения:
 - *Always on* – постоянное подключение;
 - *On demand* – установка соединения по запросу – при появлении трафика, направленного в интернет, устройство установит соединение, а при отсутствии активности более времени, указанного в поле «*Inactivity Timeout*», соединение будет разорвано;
 - *Manual* – управление соединением вручную;

- *Disconnect on idle* – установка соединения по требованию. При выборе данного параметра для редактирования станут доступны следующие настройки:
 - *Inactivity Timeout (minutes) [1-4320]* - задает интервал времени, в течение которого служба остается неактивной, перед тем как будет закрыта (1- 4320 минут).
- *Use Static IPv4 Address* – при установленном флаге разрешено использовать статический адрес IPv4. При выборе данного параметра для редактирования доступно поле ввода статического адреса;
- *Enable PPP Debug Mode* – при установленном флаге включен режим отладки PPP.

Multicast Proxy

- *Enable IGMP Multicast Proxy* – при установленном флаге осуществляется управление групповой рассылкой в сетях IPv4, включен IGMP Multicast Proxy.

Для перехода к следующему этапу настройки необходимо нажать «Next», для возврата к предыдущему – «Back».

Проверка и сохранение настроек

VPN / L2TP Client

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

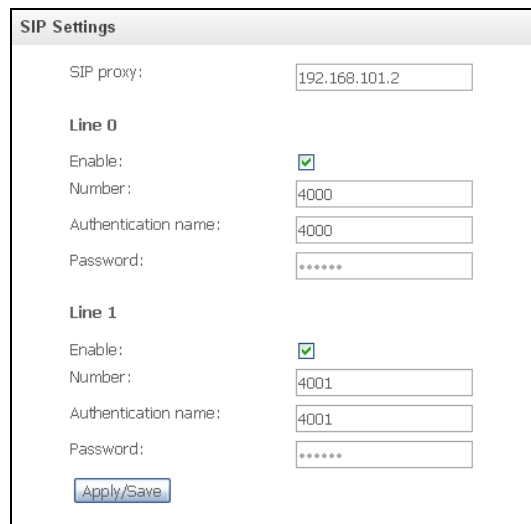
В данном окне отображены все выполненные настройки. Необходимо проверить их правильность, некорректные данные возможно изменить, вернувшись в нужное меню с помощью кнопки «Back».

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

В таблицу сервисов WAN будет добавлена новая запись для сервиса PPPoL2tpAc.

WAN service 6: PPPoL2tpAc	
Interface	ppp1
Type	PPPoE
Connection type	IP_Routed
Status	Unconfigured
IPv4 Address	
Bridging to	eth0.0,eth1.0,wl0

3.4 Меню «SIP Settings». Настройки SIP



- *SIP proxy* – адрес SIP проху сервера для регистрации абонентов;

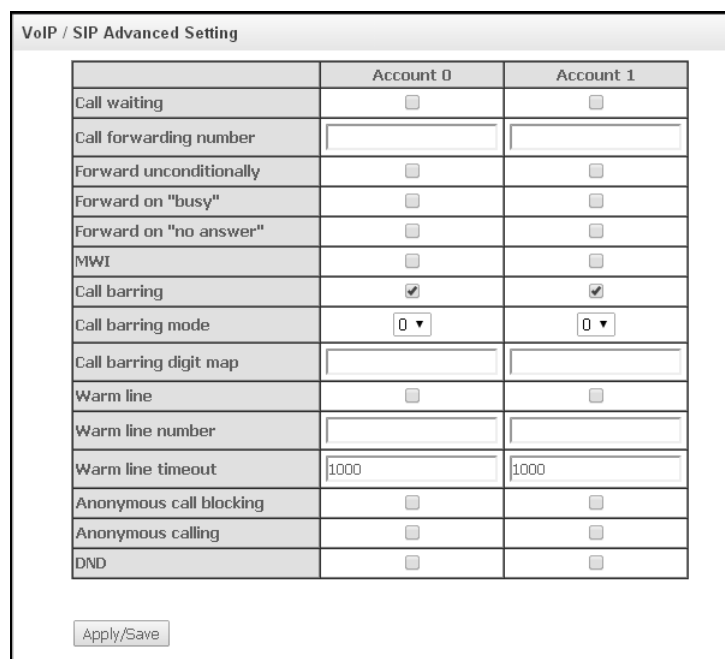
Line 0, Line 1– настройки телефонных портов:

- *Enable* – при установленном флаге данный порт включен в работу, иначе – отключен;
- *Number* – номер телефона;
- *Authentication name* – имя пользователя для аутентификации;
- *Password* – пароль для доступа.

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

3.5 Меню «VoIP. SIP Advanced Setting». Дополнительные настройки SIP

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



	Account 0	Account 1
Call waiting	<input type="checkbox"/>	<input type="checkbox"/>
Call forwarding number	<input type="text"/>	<input type="text"/>
Forward unconditionally	<input type="checkbox"/>	<input type="checkbox"/>
Forward on "busy"	<input type="checkbox"/>	<input type="checkbox"/>
Forward on "no answer"	<input type="checkbox"/>	<input type="checkbox"/>
MWI	<input type="checkbox"/>	<input type="checkbox"/>
Call barring	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Call barring mode	0 ▾	0 ▾
Call barring digit map	<input type="text"/>	<input type="text"/>
Warm line	<input type="checkbox"/>	<input type="checkbox"/>
Warm line number	<input type="text"/>	<input type="text"/>
Warm line timeout	1000	1000
Anonymous call blocking	<input type="checkbox"/>	<input type="checkbox"/>
Anonymous calling	<input type="checkbox"/>	<input type="checkbox"/>
DND	<input type="checkbox"/>	<input type="checkbox"/>

- *SIP Account* – номер аккаунта SIP;
- *Call waiting* – при установленном флаге разрешено уведомление о поступлении нового 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 определенные типы вызовов;
- *Call barring mode* – режим ограничения вызовов;
- *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».

3.6 Меню «Wi-Fi»¹. Настройка беспроводной сети

3.6.1 Подменю «Basic». Общая информация

В данном меню производятся основные настройки беспроводного интерфейса LAN, а также возможно задать до трех виртуальных точек беспроводного доступа.

Wi-Fi / 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: 20:10:7A:4F:ED:5C
 Country:
 Max Clients:

Wireless - Guest/Virtual Access Points:

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

¹ Только для моделей NTE-RG-1402G(C)-W Rev.B

- *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);



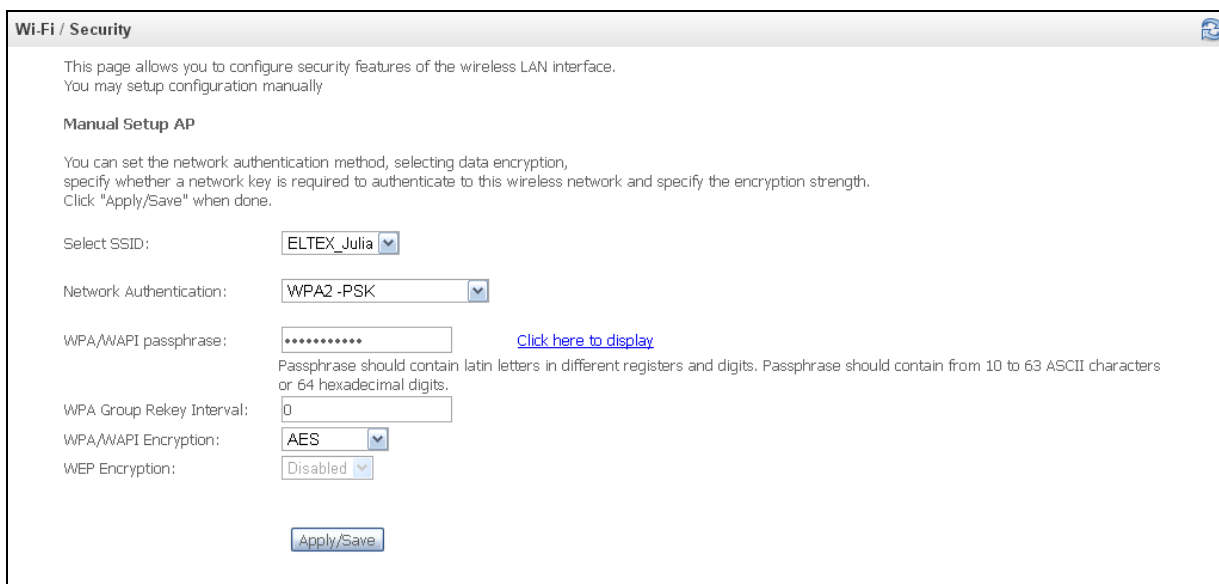
По умолчанию на устройстве установлено имя беспроводной сети (SSID) ELTEX-aaaa, где aaaa - это 4 последние цифры WAN MAC. WAN MAC указан в наклейке на корпусе устройства.

- *BSSID* – MAC-адрес точки доступа;
- *Country* – задать местоположение (страну);
- *Max Clients* – установить максимально возможное количество одновременных беспроводных подключений;

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

3.6.2 Подменю «Security». Настройка параметров безопасности

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



Wi-Fi / Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually

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:

WPA/WAPI passphrase: [Click here to display](#)
Passphrase should contain latin letters in different registers and digits. Passphrase should contain from 10 to 63 ASCII characters or 64 hexadecimal digits.

WPA Group Rekey Interval:

WPA/WAPI Encryption:

WEP Encryption:

Manual Setup AP:

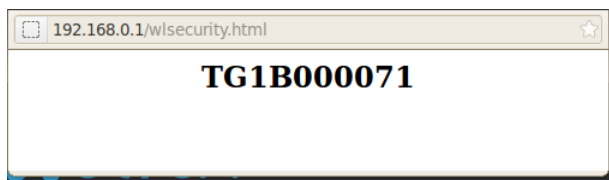
- *Select SSID* – выбрать имя беспроводной сети из списка;
- *Network Authentication* – установить сетевой аутентификации из перечня в выпадающем списке:
 - *Open* – открытый – защита беспроводной сети отсутствует (в этом режиме может использоваться только WEP-ключ);
 - *Shared* – общий (режим позволяет 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;
- *WPA* – включает стандарт WPA (режим использует протокол WPA и требует использования сервера аутентификации RADIUS);
 - *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-PSK* – включает стандарт WPA-PSK (режим использует протокол WPA, но не требует использования сервера аутентификации RADIUS);
 - *WPA/WAPI passphrase* – секретная фраза. Установка пароля, строка 8-63 символа ASCII. Для просмотра секретной фразы необходимо нажать на ссылку «*Clik here to display*», пароль будет показан во всплывающем окне.



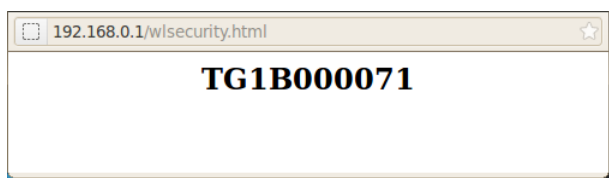
По умолчанию ключ сети соответствует серийному номеру (S/N) устройства. Серийный номер указан в наклейке на корпусе устройства. При изменении пароля необходимо задать комбинацию из 10-ти символов. Пароль должен содержать цифры и латинские буквы в верхнем и нижнем регистрах.

- *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;
- *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;
- *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 ASCII. Для просмотра секретной фразы необходимо нажать на ссылку «*Clik here to display*», пароль будет показан во всплывающем окне.



По умолчанию ключ сети соответствует серийному номеру (S/N) устройства. Серийный номер указан в наклейке на корпусе устройства. При изменении пароля необходимо задать комбинацию из 10-ти 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;
- *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.
- *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).
 - *WPA/WAPI passphrase* – секретная фраза. Установка пароля, строка 8-63 символа ASCII. Для просмотра секретной фразы необходимо нажать на ссылку «*Clik here to display*», пароль будет показан во всплывающем окне.



По умолчанию ключ сети соответствует серийному номеру (S/N) устройства. Серийный номер указан в наклейке на корпусе устройства. При изменении пароля необходимо задать комбинацию из 10-ти 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;



Убедитесь, что беспроводной адаптер компьютера поддерживает выбранный тип шифрования.

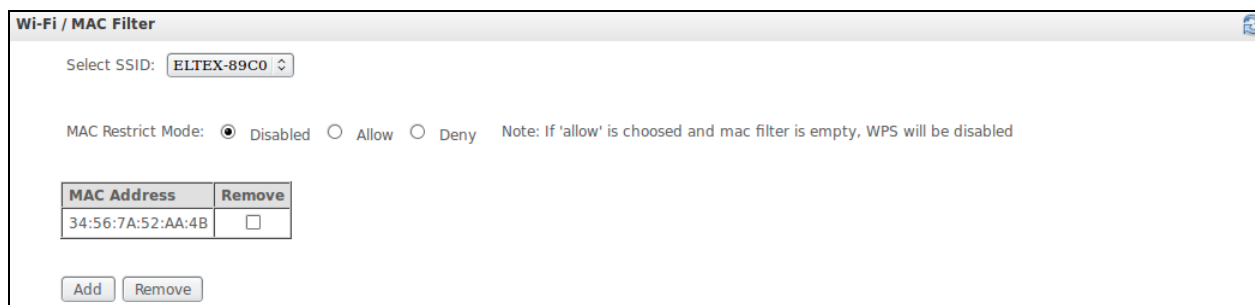
Наиболее стойкую защиту беспроводного канала даёт совместная работа точки доступа и RADIUS сервера (для аутентификации беспроводных клиентов).

- *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 16-ричной системе счисления либо 5 символов ASCII¹ для 64-х 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*».

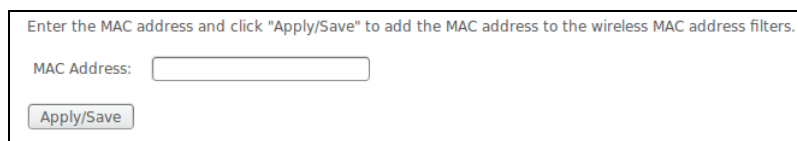
3.6.3 Подменю «*MAC Filter*». *Настройки фильтрации MAC-адресов*

Функция *MAC Filter* позволяет разрешить или запретить доступ беспроводных клиентов к беспроводной сети на базе их 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:



Возможно добавление неограниченного количества MAC-адресов в таблицу фильтрации (список является динамическим).

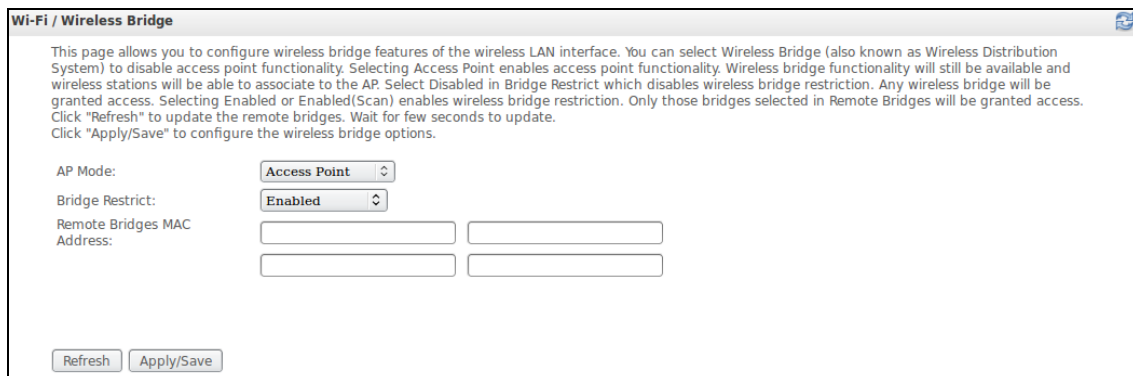
Для принятия изменений необходимо нажать кнопку «*Apply*».

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

3.6.4 Подменю «Wireless Bridge». Настройки беспроводного соединения в режиме моста

В данном меню 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:

- AP Mode – выбор режима работы точки доступа:
 - Access Point – точка доступа;
 - Wireless Bridge – беспроводной мост.
- 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 списка доступных удаленных мостов необходимо нажать «Refresh».

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

3.6.5 Подменю «Advanced». Расширенные настройки

В данном меню производятся расширенные настройки беспроводной сети:

Wi-Fi / 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: severe)

Channel:

Auto Channel Timer(min):

802.11n/EWC:

Bandwidth: Current: 20MHz

Control Sideband: Current: None

802.11n Rate:

802.11n Protection:

Support 802.11n Client Only:

RIFS Advertisement:

OBSS Co-Existence:

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:

WMM(Wi-Fi Multimedia):

WMM No Acknowledgement:

WMM APSD:

Wireless Mode:

URE:

URE Mode:

STA Retry Time(sec):

- *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 Auto выбор канала (0 – выключить);
- *802.11n/EWC* – режим совместимости с оборудованием 802.11n Draft2.0 и EWC(Enhanced Wireless Consortium);
- *Bandwidth* – установка полосы пропускания 20МГц 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 ;

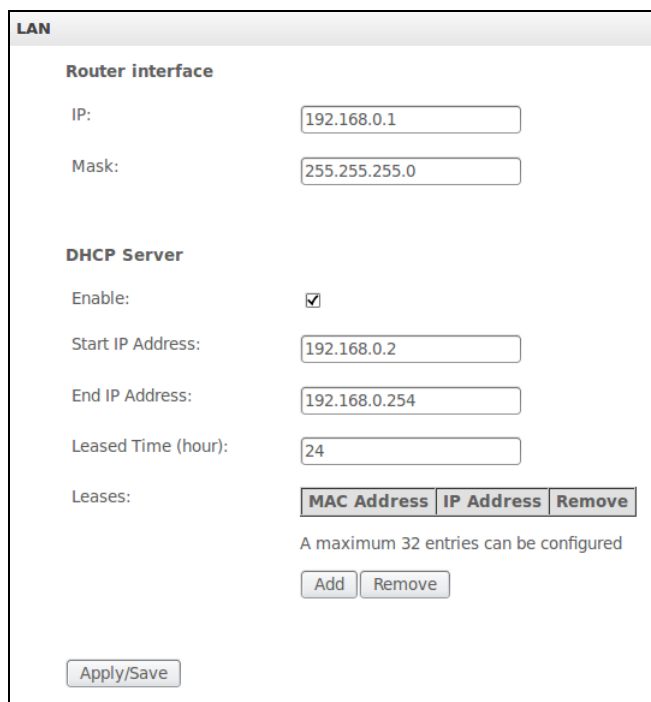
- *OBSS Co-Existence* – настройка толерантности при выборе режима работы (20Мгц или 40Мгц). Если параметр в состоянии “Enable” – будет выбран оптимальный режим работы устройства, учитывая “Bandwidth”, иначе режим работы будет зависеть только от параметра “Bandwidth”;
- *RX Chain Power Save* – отключение 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, для включения режима энергосбережения;
- *RX Chain Power Save PPS* – верхняя граница параметра PPS (packet per second). 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 ширококвещательные и многоадресные пакеты, помещенные в буфер, будут доставлены беспроводным клиентам;
- *Beacon Interval* – период отправки в беспроводную сеть информационного пакета, 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;
- *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 приёмная 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);
- *Wireless Mode* – установка режима работы:
 - *Access Point* – работа в режиме беспроводной точки доступа;
 - *Wireless Ethernet* – работа в режиме поддержки беспроводных сетей Wireless Ethernet для объединения сегментов сети.
- *URE* – использовать точку доступа/маршрутизатор в качестве повторителя. Данный режим необходим для связи двух беспроводных точек доступа в случаях, когда установление прямой связи между ними не представляется возможным;
- *URE Mode* – выбор режима работы повторителя (bridge (Range Extender), Routed (Travel Router))
- *STA Retry Time (sec)* - время, в течение которого точка доступа пытается установить связь с клиентом Wi-Fi.

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

3.7 Меню «LAN». Настройки локальной сети

3.7.1 Подменю «General Settings». Настройка основных параметров

В данном меню производится настройка локальной сети.



The screenshot shows the LAN configuration interface. It is divided into two main sections: "Router interface" and "DHCP Server".

Router interface:

- IP: 192.168.0.1
- Mask: 255.255.255.0

DHCP Server:

- Enable:
- Start IP Address: 192.168.0.2
- End IP Address: 192.168.0.254
- Leased Time (hour): 24
- Leases: A table with columns for MAC Address, IP Address, and Remove. Below the table, it states "A maximum 32 entries can be configured". There are "Add" and "Remove" buttons below the table.

At the bottom of the interface is an "Apply/Save" button.

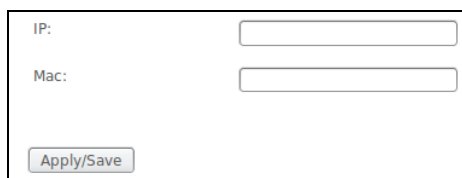
Router interface:

- *IP* – адрес устройства в локальной сети;
- *Mask* – маска подсети;

DHCP Server:

DHCP-сервер (Dynamic Host Configuration Protocol) 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);
- *Leases* – установка соответствия выдаваемых IP-адресов MAC-адресам устройств(привязка). Для добавления записи в таблицу необходимо нажать «Add». Может быть установлено до 32 соответствий.
 - *IP* – IP-адрес устройства;
 - *Mac*– MAC-адрес устройства.

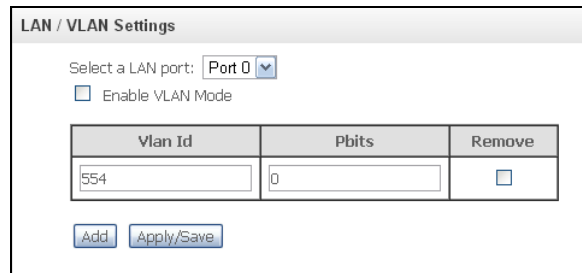


The screenshot shows a small configuration window with two input fields: "IP:" and "Mac:". Below the fields is an "Apply/Save" button.

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

3.7.2 Подменю «VLAN Settings». Настройка параметров VLAN

В данном меню 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).

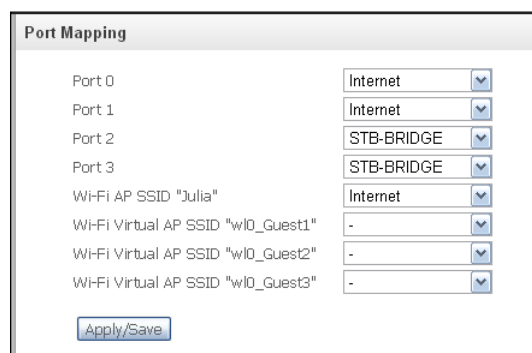
Для принятия и сохранения изменений необходимо нажать кнопку «Apply/Save».

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

3.8 Меню «Port Mapping¹»

Меню 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 меню 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.



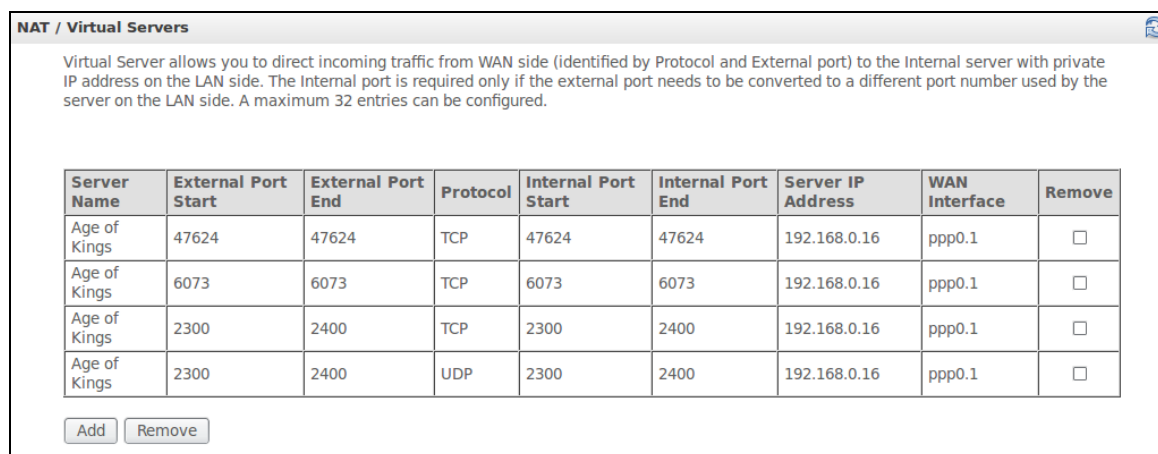
Для принятия изменений и сохранения необходимо нажать кнопку «Apply/Save».

3.9 Меню «NAT». Настройки NAT

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

3.9.1 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
Age of Kings	47624	47624	TCP	47624	47624	192.168.0.16	ppp0.1	<input type="checkbox"/>
Age of Kings	6073	6073	TCP	6073	6073	192.168.0.16	ppp0.1	<input type="checkbox"/>
Age of Kings	2300	2400	TCP	2300	2400	192.168.0.16	ppp0.1	<input type="checkbox"/>
Age of Kings	2300	2400	UDP	2300	2400	192.168.0.16	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 из интернета.

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

¹ При отсутствии меню в конфигураторе данные настройки уже выполнены Вашим оператором связи

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". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".**
 Remaining number of entries that can be configured: 28

Use Interface: INTERNET/ppp0.1
 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="47624"/>	<input type="text" value="47624"/>	TCP	<input type="text" value="47624"/>	<input type="text" value="47624"/>
<input type="text" value="6073"/>	<input type="text" value="6073"/>	TCP	<input type="text" value="6073"/>	<input type="text" value="6073"/>
<input type="text" value="2300"/>	<input type="text" value="2400"/>	TCP	<input type="text" value="2300"/>	<input type="text" value="2400"/>
<input type="text" value="2300"/>	<input type="text" value="2400"/>	UDP	<input type="text" value="2300"/>	<input type="text" value="2400"/>
<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 Интернета;
- *External Port End* – конечный внешний порт диапазона портов, на которые осуществляется обращение из Интернета;
- *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».

3.9.2 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.

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 Start End	Protocol	Port Range Start End			
Napster	TCP	6699 6699	TCP	6699 6699	ppp0.1	<input type="checkbox"/>	
Napster	TCP	6699 6699	TCP	6697 6697	ppp0.1	<input type="checkbox"/>	
Napster	TCP	6699 6699	TCP	4444 4444	ppp0.1	<input type="checkbox"/>	
Napster	TCP	6699 6699	TCP	5555 5555	ppp0.1	<input type="checkbox"/>	
Napster	TCP	6699 6699	TCP	6666 6666	ppp0.1	<input type="checkbox"/>	
Napster	TCP	6699 6699	TCP	7777 7777	ppp0.1	<input type="checkbox"/>	
Napster	TCP	6699 6699	TCP	8888 8888	ppp0.1	<input type="checkbox"/>	

Add Remove

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

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 "Save/Apply" to add it.

Remaining number of entries that can be configured: 32

Use Interface: INTERNET/ppp0.1

Application Name:

Select an application: **Napster**

Custom application:

Apply/Save

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
6699	6699	TCP	6699	6699	TCP
6699	6699	TCP	6697	6697	TCP
6699	6699	TCP	4444	4444	TCP
6699	6699	TCP	5555	5555	TCP
6699	6699	TCP	6666	6666	TCP
6699	6699	TCP	7777	7777	TCP
6699	6699	TCP	8888	8888	TCP
		TCP			TCP

Apply/Save

– 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;

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

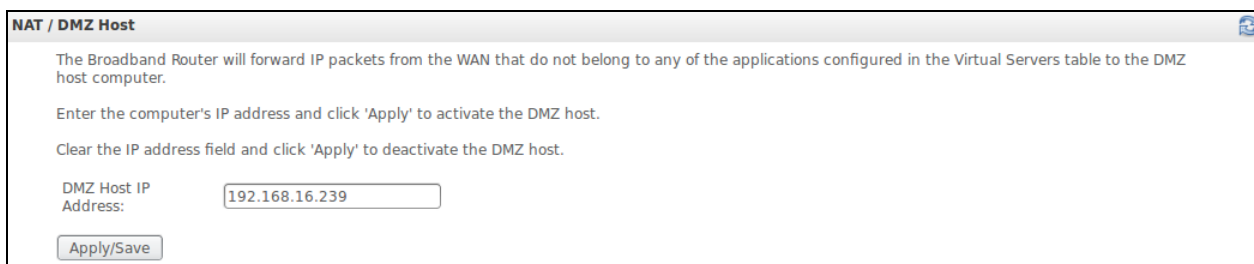
- *Trigger Port Start* – начальный порт диапазона портов, которые осуществляют функцию триггера;
- *Trigger Port End* – конечный порт диапазона портов, которые осуществляют функцию триггера;
- *Trigger Protocol* – протокол, используемый для триггера;
- *Open Port Start* – начальный порт диапазона портов,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

3.9.3 Подменю «DMZ Host». Настройка 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.




The screenshot shows the 'NAT / DMZ Host' configuration window. It contains the following text: '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' to activate the DMZ host. Clear the IP address field and click 'Apply' to deactivate the DMZ host.' Below this text is a text input field labeled 'DMZ Host IP Address:' containing the value '192.168.16.239'. At the bottom left of the window is an 'Apply/Save' button.

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

3.10 Меню «IPSec». Настройка защиты данных по протоколу IP

IP Security – набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяет осуществлять подтверждение подлинности и/или шифрование IP-пакетов. IPSec также включает в себя протоколы для защищённого обмена ключами в сети Интернет.



The screenshot shows the 'IPSec' configuration window. It contains the text: 'Add, remove or enable/disable IPSec tunnel connections from this page.' Below this text is a table with the following columns: 'Connection Name', 'Remote Gateway', 'Local Addresses', 'Remote Addresses', and 'Remove'. The table contains one row with the following data: 'new connection', '192.168.27.6', '192.168.27.18', '192.168.19.2', and an unchecked checkbox. Below the table are two buttons: 'Add New Connection' and 'Remove'.

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove
new connection	192.168.27.6	192.168.27.18	192.168.19.2	<input type="checkbox"/>

Для добавления записи необходимо нажать кнопку «*Add new connection*». Для удаления - установить флаг напротив требуемой записи в колонке *Remove* и нажать кнопку «*Remove*».

IPSec

IPSec Connection Name

IP Version:

Tunnel Mode

IPSec Connection Mode

Local Gateway Interface:

Remote IPSec Gateway Address

Tunnel access from local IP addresses

IP Address for VPN

Mask or Prefix Length

Tunnel access from remote IP addresses

IP Address for VPN

Mask or Prefix Length

Key Exchange Method

Authentication Method

Pre-Shared Key

Perfect Forward Secrecy

Advanced IKE Settings

- *IPSec Connection Name* – имя подключения;
- *IP Version* – версия протокола IP;
- *Tunnel Mode* – режим туннелирования (ESP/AH);
- *IPSec Connection Mode* – выбор режима работы IPsec:
 - *Transport* – транспортный режим;
 - *Tunnel* – туннельный режим.
- *Local Gateway Interface* – выбор интерфейса, используемого в качестве локального шлюза IPsec;
- *Remote IPSec Gateway Address (IPv4 address in dotted decimal)* – установка адреса удаленного шлюза IPsec;
- *Tunnel access from local IP addresses* – режим туннельного доступа с локального адреса(подсеть/одиночный адрес (Subnet/Single Address));
 - *IP Address for VPN* – адрес для VPN;
 - *Mask or Prefix Length* – маска подсети.
- *Tunnel access from remote IP addresses* – режим туннельного доступа с удаленного адреса(подсеть/одиночный адрес (Subnet/Single Address));
 - *IP Address for VPN* – адрес для VPN;
 - *Mask or Prefix Length* – маска подсети.
- *Key Exchange Method* – режим смены ключа (авто/вручную (AUTO(IKE)/Manual));
- *Authentication Method* – выбор метода аутентификации:
 - *Pre-Shared Key* – установка пароля WPA-PSK (один пароль для каждого отдельного узла беспроводной сети);
 - *Certificate (X.509)* – выбор сертификата открытых ключей;
- *Perfect Forward Secrecy* – установка режима секретности. Данный режим добавит ещё один уровень безопасности на уровне шифрования данных, однако приведёт к увеличению нагрузки на CPU (enable – режим включен);
- *Advanced IKE Settings* – при нажатии на кнопку «*Show Advanced Settings*» станут доступны расширенные настройки туннеля IKE:

Hide Advanced Settings

Advanced IKE Settings

Phase 1

Mode: Main

Encryption Algorithm: 3DES

Integrity Algorithm: MD5

Select Diffie-Hellman Group for Key Exchange: 1024bit

Key Life Time: 3600 Seconds

Phase 2

Encryption Algorithm: 3DES

Integrity Algorithm: MD5

Select Diffie-Hellman Group for Key Exchange: 1024bit

Key Life Time: 3600 Seconds

Apply/Save

Концепция управления и обмена ключами, управления и установления SA:

- *Phase 1 – фаза 1*, создание IKE SA для защиты фазы 2:
- *Mode* – выбор режима проведения фазы:
 - *Main* – конфигурация стандартных параметров определения 1 фазы IKE VPN-туннеля (основной режим);
 - *Aggressive* – конфигурация параметров определения 1 фазы IKE VPN-туннеля за минимальное время (превосходит по скорости основной, но не обеспечивает защиту подлинности);
- *Encryption Algorithm* – выбор алгоритма шифрования:
 - *DES* – симметричный алгоритм шифрования, имеет блоки по 64 бита и 16 цикловую структуру сети Фейстеля, для шифрования использует ключ с длиной 56 бит;
 - *3DES* – симметричный блочный шифр с увеличенной длиной ключа, созданный на основе алгоритма DES. При намного более высокой криптостойкости, скорость работы 3DES в 3 раза ниже, чем у DES;
- *Integrity Algorithm* – выбор алгоритма вычисления поля *Integrity Check Value* в заголовке пакета аутентификации (MD5, SHA1);
- *Select Diffie-Hellman Group for Key Exchange* – выбор размерности группы MODP для разделяемого (двойного) ключа в небезопасной среде;
- *Key Life Time* – установка времени жизни ключа, в секундах;

- *Phase 2 – фаза 2*, создание SA для IPsec:
- *Encryption Algorithm* – выбор алгоритма шифрования:
 - *DES* – симметричный алгоритм шифрования, имеет блоки по 64 бита и 16 цикловую структуру сети Фейстеля, для шифрования использует ключ с длиной 56 бит;
 - *3DES* – симметричный блочный шифр с увеличенной длиной ключа, созданный на основе алгоритма DES. При намного более высокой криптостойкости, скорость работы 3DES всего в 3 раза ниже, чем у DES;
- *Integrity Algorithm* – выбор алгоритма вычисления поля Integrity Check Value в заголовке пакета аутентификации (MD5, SHA1);
- *Select Diffie-Hellman Group for Key Exchange* – выбор длины группы MODP для разделяемого (двойного) ключа в небезопасной среде;
- *Key Life Time* – установка времени жизни ключа, в секундах.

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

3.11 Меню «Storage Device Info». Службы файловых хранилищ

В данном меню 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	2543	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.

3.12 Меню «UPnP». Автоматическая настройка сетевых устройств

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

UPnP

NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

Enable UPnP

[Apply/Save](#)



Для использования UPnP необходимо настроить NAT на активном WAN интерфейсе.

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

3.13 Меню «Dynamic DNS». Настройка 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 NTE-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 / DNS / 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
192.168.13.15	test1	dyndns	epon0.2	<input type="checkbox"/>

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

Dynamic DNS

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:

Dynamic DNS

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:

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

D-DNS provider: DynDNS.org

Hostname:

Interface: IGMP/epon0.2

DynDNS Settings

Username:

Password:

DynDNS Type: Dynamic

Wildcard:

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

D-DNS provider: TZO.com

Hostname:

Interface: IGMP/epon0.2

TZO Settings

Email:

Key:

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

D-DNS provider: freedns.afraid.org

Hostname:

Interface: IGMP/epon0.2

freedns.afraid.org Settings

Username:

Password:

- *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».

3.14 Меню «Security». Настройки безопасности

В данном разделе проводится настройка параметров безопасности устройства.

3.14.1 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):

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:3B	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».

Security / IP Filtering / Outgoing

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 слэш 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 слэш 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):

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
Danger	ppp0.1	4	TCP or UDP	3A:80:15:5D:D3:77	192.168.15.44	90	192.168.15.3	90	<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».

Security / IP Filtering / Incoming

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 слэш возможно указать длину префикса);
- *Source Port (port or port:port)* – порт/порты источника;
- *Destination IP address[/prefix length]* – IP-адрес места назначения (через слэш возможно указать длину префикса);
- *Destination Port (port or port:port)* – порт/порты места назначения;

WAN Interfaces (Сконфигурированные в режиме маршрутизатора и с включенным брандмауэром) and LAN Interfaces:

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

Либо выбрать интерфейс из приведенного списка, установив флаг напротив.

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

3.14.2 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.

Security / MAC Filtering

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
epon0.3	FORWARD	<input type="checkbox"/>
epon0.4	FORWARD	<input type="checkbox"/>
epon0.5	FORWARD	<input type="checkbox"/>

Choose Add or Remove to configure MAC filtering rules.

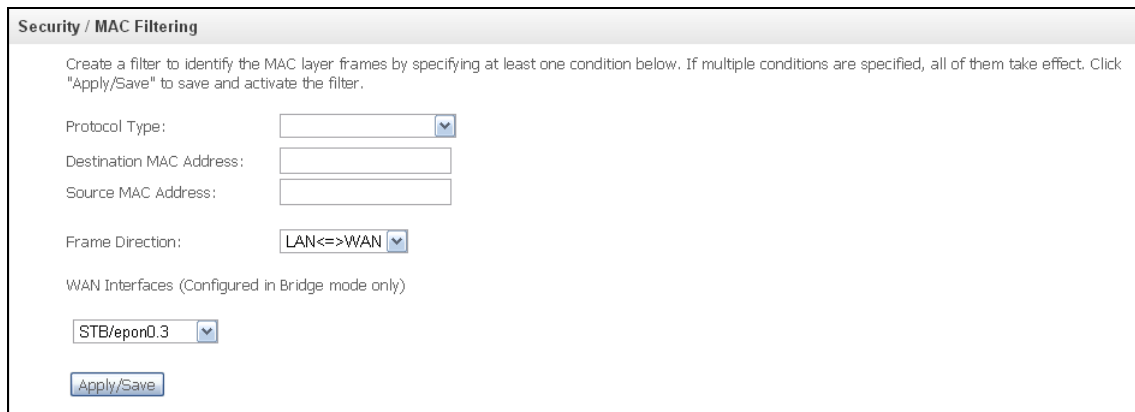
Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
<input type="button" value="Add"/>	<input type="button" value="Remove"/>				



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.



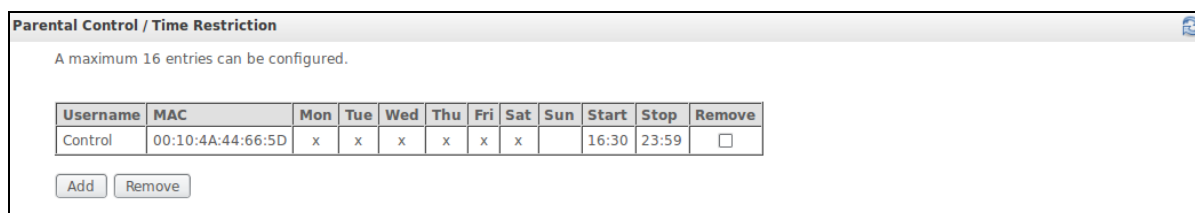
- *Protocol type* – выбор протокола (PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP);
- *Destination MAC Address* – MAC-адрес получателя;
- *Source MAC Add* – MAC-адрес отправителя;
- *Frame Direction* – направление передачи (LAN<=>WAN, LAN=>WAN, WAN=>LAN);
- *WAN Interfaces (Configured in Bridge mode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

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

3.15 Меню «Parental control» . «Родительский контроль» – настройки ограничения

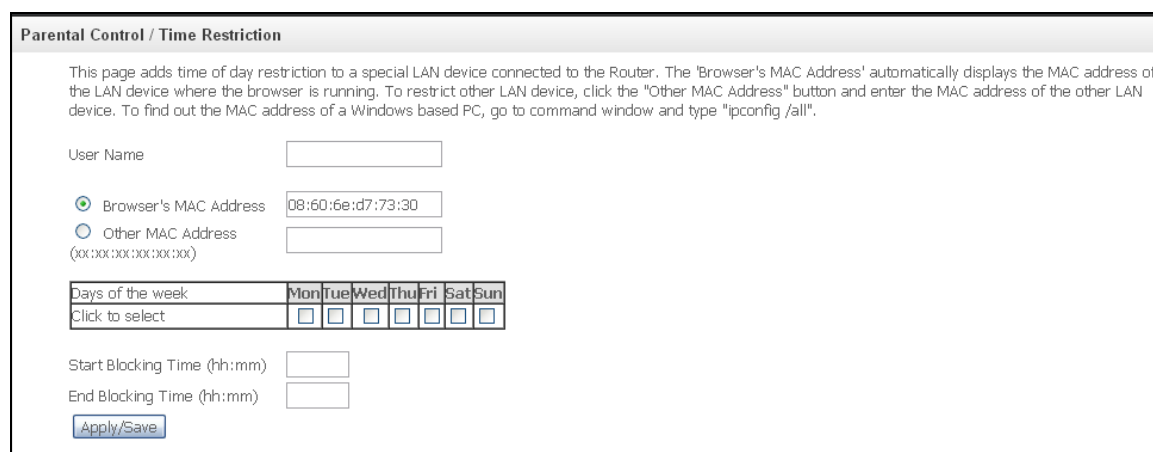
3.15.1 Подменю «Time Restriction». Настройки ограничения продолжительности сеансов

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



Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
Control	00:10:4A:44:66:5D	x	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.



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:

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

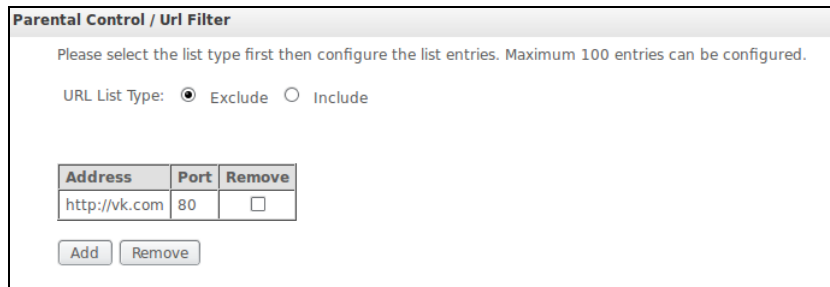


Ограничения будут действовать, если на устройстве установлено корректное системное время.

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

3.15.2 Подменю «Url Filter». Настройки ограничения доступа к адресам 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.



Parental Control / Url Filter

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

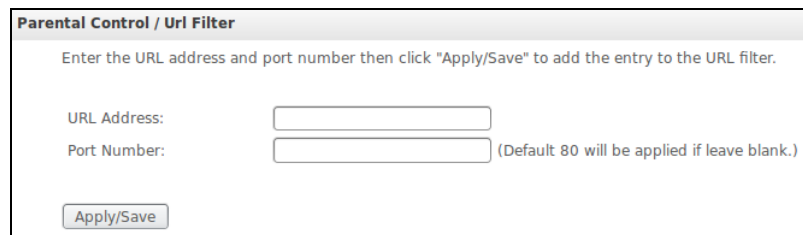
URL List Type: Exclude Include

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

Add Remove

- *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».



Parental Control / Url Filter

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.)

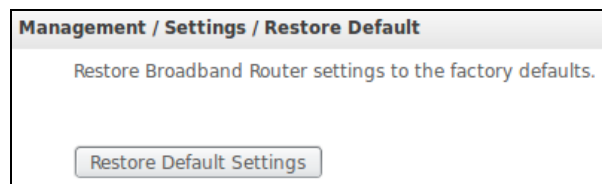
Apply/Save

- *URL Address* – URL адрес;
- *Port Number* – номер порта;

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

3.16 Меню «Management». Настройки управления

3.16.1 Подменю «Restore Default». Сброс к настройкам по умолчанию



Management / Settings / Restore Default

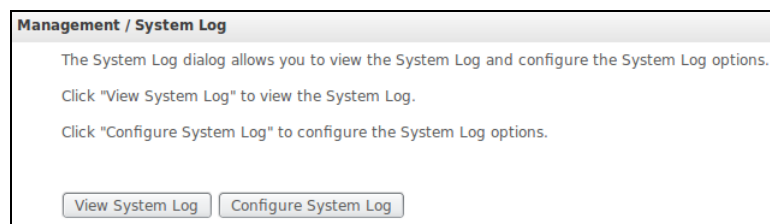
Restore Broadband Router settings to the factory defaults.

Restore Default Settings

По нажатию на кнопку «Restore Default Settings» происходит сброс устройства к заводским настройкам.

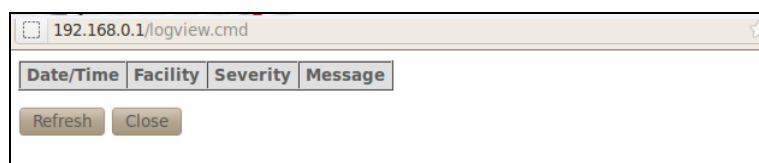
3.16.2 Подменю «System Log». Настройки системного журнала

Меню предназначено для просмотра и/или настройки событий, происходящих на маршрутизаторе.



Просмотр журнала

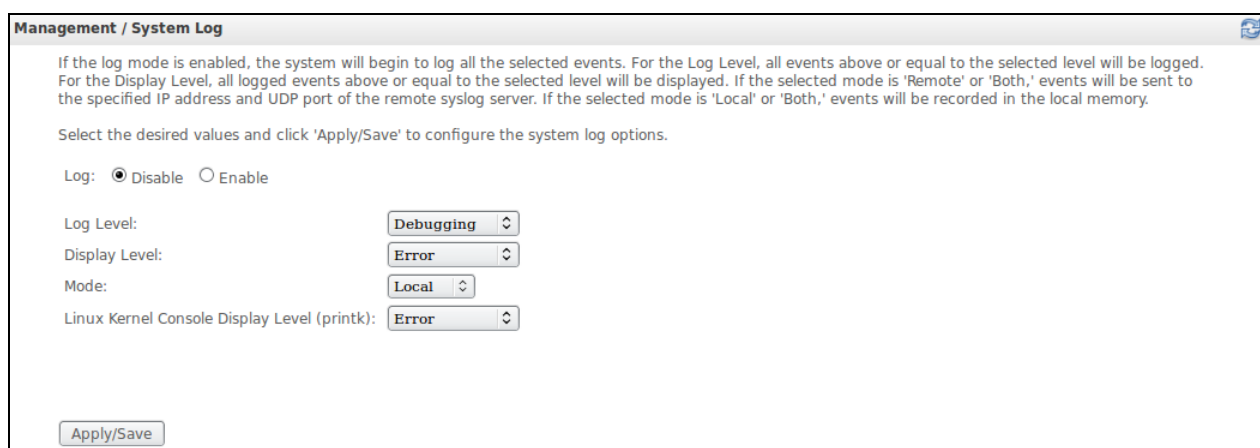
Переход к просмотру системного журнала осуществляется кнопкой «View System Log».



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

Конфигурирование журнала

Переход к конфигурированию системного журнала осуществляется кнопкой «Configure System Log».



- *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;
 - *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);

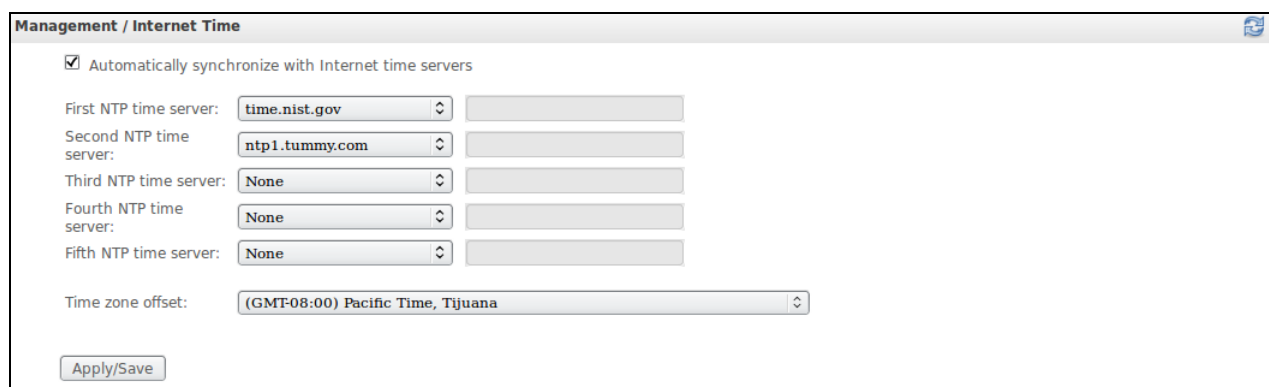
- *Remote* – удаленный (все события возвращаются на сервер Syslog). При выборе удаленного режима (*Remote*) доступны следующие настройки:
 - *Server IP address* – IP-адрес сервера Syslog, на котором сохраняются все события;
 - *Server IP Port* – номер порта сервера Syslog;
 - *Both* – работают оба режима.
- *Linux Level Console Display Level (printk)* – установка уровня сообщений, выводимых в консоль Linux;

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*».

3.16.3 Подменю «*Internet Time*». Настройки системного времени устройства



Во вкладке настраивается системное время на устройстве.

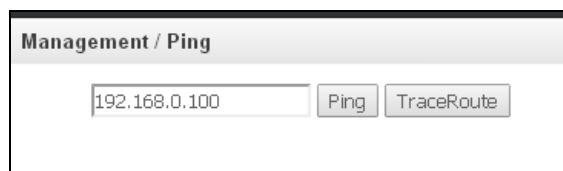
- *Automatically synchronize with Internet time servers* – при установленном флаге производить автоматическую синхронизацию с интернет-серверами точного времени;
- *First NTE time server* – выбор основного сервера точного времени;
- *Second NTE time server* – выбор вторичного сервера точного времени,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

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

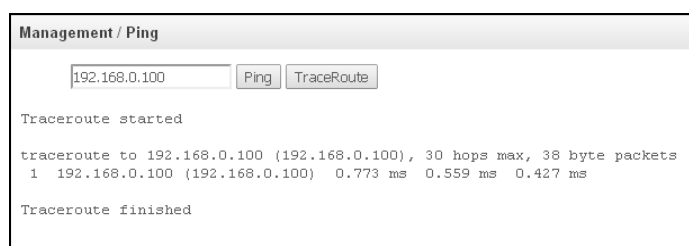
Для принятия изменений и сохранения необходимо нажать кнопку «*Apply/Save*».

3.16.4 Подменю «Ping». Проверка доступности сетевых устройств

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

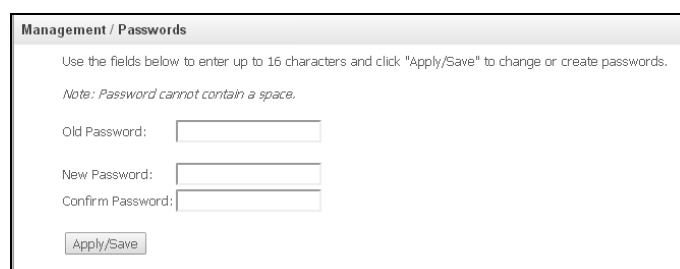


Для проверки доступности подключенного устройства необходимо ввести его IP-адрес в поле и нажать кнопку «Ping». Для просмотра трассировки маршрута нажмите кнопку «TraceRoute». Вывод будет осуществлен на данной странице Web-конфигуратора.



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

В данном меню осуществляется смена пароля для доступа к устройству.



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

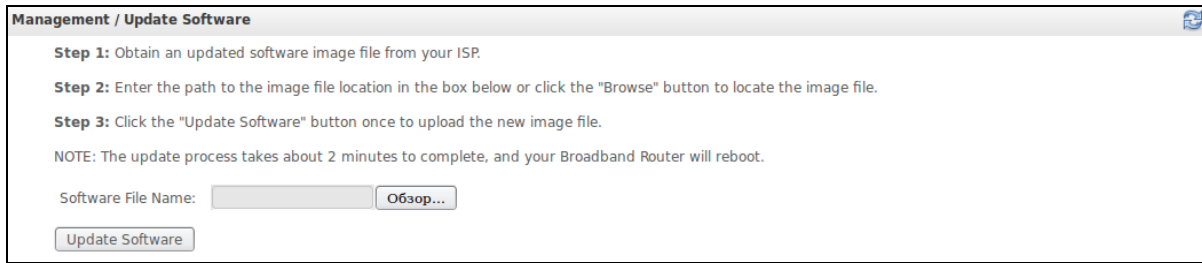
Для принятия изменений и сохранения необходимо нажать кнопку «Apply/Save».

3.16.6 Подменю «Update Software». Обновление ПО

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

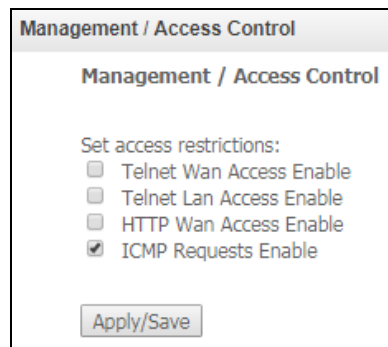


В процессе обновления не допускается отключение питания устройства, либо его перезагрузка. Процесс обновления может занимать несколько минут, после чего устройство автоматически перезагружается.



3.16.7 Подменю «Access Control». Управление доступом

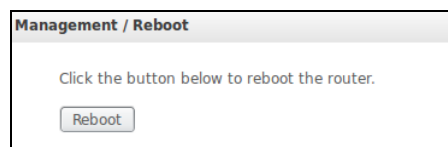
Меню служит для настройки доступа к маршрутизатору из внешней сети. Можно настроить доступ по протоколам Telnet и HTTP.



- *Telnet Wan Access Enable* – включить доступ по протоколу Telnet со стороны WAN-интерфейса;
- *Telnet Lan Access Enable* – включить доступ по протоколу Telnet со стороны LAN-интерфейса;
- *HTTP Wan Access Enable* – включить доступ по протоколу HTTP со стороны WAN-интерфейса;
- *ICMP Requests Enable* – при установленном флаге разрешены эхо-запросы.

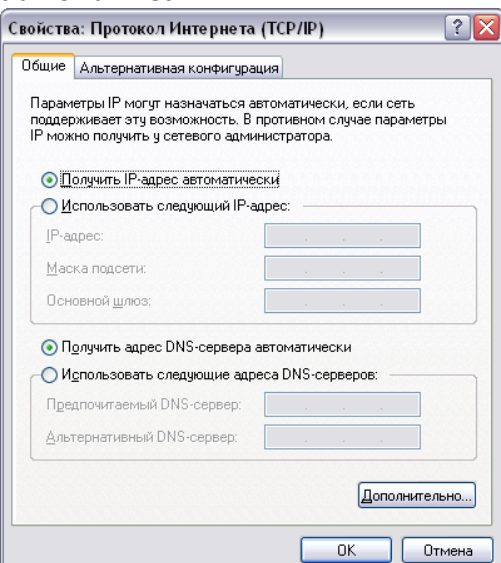
Для принятия изменений и сохранения необходимо нажать кнопку «Apply/Save».

3.16.8 Подменю «Reboot». Перезагрузка устройства



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

ПРИЛОЖЕНИЕ А ВОЗМОЖНЫЕ ПРОБЛЕМЫ И ВАРИАНТЫ ИХ РЕШЕНИЯ

Проблема	Возможная причина	Решение
<p>При вводе IP-адреса маршрутизатора (например, 192.168.0.1) не удается получить доступ к Web-интерфейсу</p>	<p>Компьютер не принадлежит к данной IP-подсети для подключения к Web-интерфейсу.</p>	<p>В свойствах подключения к интернету на Вашем компьютере установите параметр «Получать IP-адрес автоматически».</p> 
	<p>На компьютере установлен Web-браузер с выключенной опцией JavaScript</p>	<p>Включите опцию JavaScript в вашем браузере или воспользуйтесь другим Web-браузером</p>
	<p>Неисправный кабель</p>	<p>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.</p>
	<p>Доступ запрещен программным обеспечением интернет-безопасности Вашего компьютера</p>	<p>Отключите программное обеспечение интернет-безопасности на компьютере (брандмауэры)</p>
<p>Воспроизводится сигнал ошибки в телефоне, подключенном к порту FXS</p>	<p>Неверные настройки порта</p>	<p>Проверьте корректность настроек в меню «VoIP» (см. Раздел 3.4 Меню «SIP Settings». Настройки SIP).</p>
<p>Утерян/не подходит пароль доступа к WEB-интерфейсу устройства</p>	<p style="text-align: center;">_____</p>	<p>Необходимо сбросить маршрутизатор к настройкам по умолчанию с помощью кнопки F на задней панели устройства. К сожалению, при этом все выполненные настройки будут утрачены.</p>

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 «SIP Setting» (раздел 3.5 Меню «VoIP. SIP Advanced Setting». 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 и 3 Конференция – «**Conference**».

- 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.

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 конференцсвязи.

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 разрушается, если ее покидает инициатор, обоим 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 «SIP Setting» (*раздел 3.4*

Меню «SIP Settings». Настройка 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 «SIP Setting» (раздел 3.5 Меню «VoIP. SIP Advanced Setting». 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»:

- Call barring pin = 0, все исходящие звонки разрешены
- Call barring pin = 1, все исходящие звонки запрещены
- Call barring pin = 2, 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 1. Для того чтобы разрешить все исходящие вызовы, требуется выбрать 0. Для запрета исходящих звонков на номер 1150 необходимо задать 2 в поле «Call barring mode».

СВИДЕТЕЛЬСТВО О ПРИЕМКЕ И ГАРАНТИИ ИЗГОТОВИТЕЛЯ

Абонентский оптический терминал NTE-RG-1402_____ rev.В зав. № _____ соответствует требованиям технических условий ТУ6650-081-33433783-2012 и признан годным для эксплуатации.

Предприятие-изготовитель ООО «Предприятие «ЭЛТЕКС» гарантирует соответствие абонентского шлюза требованиям технических условий ТУ6650-083-33433783-2012 при соблюдении потребителем условий эксплуатации, установленных в настоящем руководстве.

Гарантийный срок 1 год.

Изделие не содержит драгоценных материалов.

Директор предприятия _____

подпись

Черников А. Н.

Ф.И.О.

Начальник ОТК предприятия _____

подпись

Игонин С.И.

Ф.И.О.

Изготовитель:

ООО «Предприятие «ЭЛТЕКС»

630020 г. Новосибирск,

ул. Окружная, 29В

E-mail: eltex@eltex-co.ru

Сделано в России

EAC



ОСТОРОЖНО!
ИЗЛУЧЕНИЕ ЛАЗЕРА