



Комплексные решения для построения сетей

NTP-RG-1402 rev.C

Руководство пользователя, версия 1.0 (5.08.2013)

Абонентские оптические терминалы

IP-адрес: 192.168.1.1
имя пользователя: user
пароль: user

<http://eltex.nsk.ru/support/documentations>
<http://mc240.ru/support/documentations>

Версия документа	Актуальность для ПО	Дата выпуска	Содержание изменений
Версия 1.0	2.8.5656	5.08.2013	Первая публикация

ПРИМЕЧАНИЯ И ПРЕДУПРЕЖДЕНИЯ



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



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

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ	5
2 ОПИСАНИЕ ИЗДЕЛИЯ	6
2.1 Назначение	6
2.2 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	13
2.7 Перегрузка/сброс к заводским настройкам.....	14
2.8 Комплект поставки	14
3 АРХИТЕКТУРА NTP-RG-1402 REV.C.....	15
4 НАСТРОЙКА NTP-RG-1402 REV.C ЧЕРЕЗ WEB-ИНТЕРФЕЙС. ДОСТУП ПОЛЬЗОВАТЕЛЯ.....	18
4.1 Меню Device Info . Информация об устройстве.....	19
4.1.1 Подменю Summary. Общая информация об устройстве	19
4.1.2 Подменю WAN. Информация о состоянии сервисов	19
В данном меню производится мониторинг состояния сетевых сервисов.	19
Для просмотра доступна следующая информация о сервисах:.....	19
4.1.3 Подменю SIP. Мониторинг состояния телефонных портов	20
4.1.4 Подменю LAN. Мониторинг состояния портов LAN. Мониторинг статуса Wi-Fi интерфейса	20
4.1.5 Подменю Authenticated Wireless Station. Подключенные беспроводные устройства	21
4.1.6 Подменю ARP. Просмотр кэша протокола ARP.....	21
4.1.7 Подменю DHCP. Активные аренды DHCP	21
В таблице DHCP можно посмотреть список активных аренд DHCP сервера и срок их истечения.....	21
4.1.8 Подменю Route. Просмотр таблицы маршрутизации	22
4.1.9 Подменю Statistics. Информация о прохождении трафика на портах устройства	22
4.2 Меню «PPP settings». Настройки PPP.....	23
4.3 Меню SIP Settings. Настройки SIP	24
4.4 Меню VoIP.SIP Advanced Setting. Дополнительные настройки SIP	25
4.5 Меню Wi-Fi. Настройка беспроводной сети	26
4.5.1 Подменю Basic. Общая информация	26
4.5.2 Подменю Security. Настройка параметров безопасности	27
4.5.3 Подменю MAC Filter. Настройки фильтрации MAC-адресов.....	31
4.5.4 Подменю Wireless Bridge. Настройки беспроводного соединения в режиме моста.....	32
4.5.4.1 Подменю Advanced. Расширенные настройки	33
4.6 Меню LAN. Настройки локальной сети.....	35
4.6.1 Подменю General Settings. Настройка основных параметров	35
4.6.2 Подменю VLAN Settings. Настройка параметров VLAN	36
4.7 Меню Port Mapping	36
4.8 Меню NAT. Настройки NAT	37
4.8.1 Подменю Virtual Servers. Настройки виртуальных серверов	37
4.8.2 Подменю Port Triggering. Настройки запуска портов.....	38
4.8.3 Подменю DMZ Host. Настройки демилитаризованной зоны.....	40
4.9 Меню Storage Device Info	40
4.10 Меню UPnP.....	41
4.11 Меню «Dynamic DNS». Настройка динамической системы доменных имен	41
4.12 Меню Security. Настройки безопасности	43
4.12.1 Подменю IP Filtering. Настройки фильтрации адресов.....	43
Настройки фильтрации исходящего трафика (Outgoing):.....	43
Настройки фильтрации входящего трафика (Incoming):.....	44
4.12.2 Подменю MAC Filtering. Настройки фильтрации по MAC-адресам	46
4.13 Меню Parental control. «Родительский контроль» – настройки ограничения.....	46

4.13.1 Подменю Time Restriction. Настройки ограничения продолжительности сеансов	47
4.13.2 Подменю Url Filter. Настройки ограничения доступа в интернет	48
4.14 Меню Management . Управление устройством	48
4.14.1 Подменю Restore Default. Возврат к настройкам по умолчанию	48
4.14.2 Подменю System Log. Просмотр и настройка системного журнала	48
4.14.3 Подменю Internet Time. Настройки системного времени	50
4.14.4 Подменю Update Software. Обновление ПО.....	50
4.14.5 Подменю Reboot. Перезагрузка устройства	51
ПРИЛОЖЕНИЕ А ВОЗМОЖНЫЕ ПРОБЛЕМЫ И ВАРИАНТЫ ИХ РЕШЕНИЯ	52
ПРИЛОЖЕНИЕ Б. ИСПОЛЬЗОВАНИЕ ДОПОЛНИТЕЛЬНЫХ УСЛУГ	53
1. Уведомление о поступлении нового вызова – Call Waiting.....	53
2. Передача вызова – Calltransfer	53
3. Конференция – Conference	53
4. Message Waiting Indication (MWI) - индикация о наличии голосовых сообщений в почтовом ящике	54
СВИДЕТЕЛЬСТВО О ПРИЕМКЕ И ГАРАНТИИ ИЗГОТОВИТЕЛЯ	55

1 ВВЕДЕНИЕ

Сеть GPON относится к одной из разновидностей пассивных оптических сетей PON. 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 Gbps в направлении downlink и 1.25 Gbps 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 *NTP-RG-1402 rev.C* 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 *NTP-RG rev.C*.

2 ОПИСАНИЕ ИЗДЕЛИЯ

2.1 Назначение

Устройства серии NTP-RG rev.C GPON ONT (Gigabit Passive Optical Network) обеспечивают с одной стороны соединение по оптическому каналу с устройством GPON класса OLT (оптическое терминальное оборудование), а с другой – соединение до 10/100/1000Мбит/с с конечным оборудованием пользователя.

Главным преимуществом технологии GPON 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 NTP-RG можно подключить до четырех компьютеров, доступ в интернет для которых возможен с помощью встроенных функций роутинга.

2.2 Варианты исполнения

NTP-RG rev.C существует только в одном варианте исполнения. Набор интерфейсов модели представлен в Таблице 1.

Таблица 1 – Наличие интерфейсов

Наименование модели	Интерфейс WAN	Количество/тип портов интерфейса LAN	Количество портов FXS	Наличие Triplexer	Наличие Wi-Fi
NTP-RG-1402G-W rev.C	SFF	4 Gigabit	2	-	+

Устройство имеет 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 стандарты 802.1b/g.

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, 802.11g;
- 2 порта USB2.0 - для подключения внешних накопителей USB или HDD.

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;
 - поддержка 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";
 - определитель номера Caller ID по ETSI FSK;
 - запрет выдачи Caller ID (анонимный звонок) - Anonymous calling;
 - теплая линия - Warmline;
 - гибкий план нумерации;
 - индикация о наличии сообщений на голосовой почте - MWI;
 - блокировка анонимных звонков - Anonymous call blocking;

- запрет на исходящие вызовы - Call Barring;
 - "не беспокоить" – DND.
- обновление ПО через Web-интерфейс, TR-069;
 - удаленный мониторинг, конфигурирование и настройка:
 - TR-069;
 - Web-интерфейс;
 - Telnet.

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

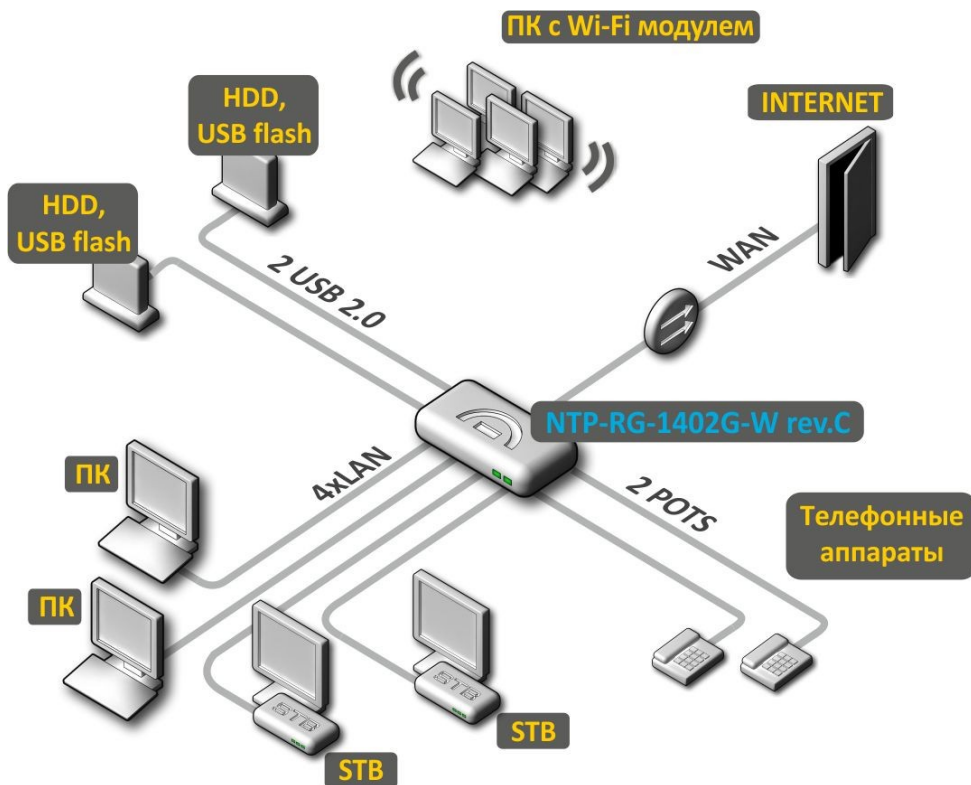


Рисунок 1 – Схема применения NTP-RG-1402G-W rev.C

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
Электрический разъем	RJ-45
Скорость передачи, Мбит/с	Автоопределение, 10/100/1000 Мбит/с, дуплекс/ полудуплекс
Поддержка стандартов	IEEE 802.3i 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3x Flow Control IEEE 802.3 NWay auto-negotiation

Параметры интерфейса PON

Количество интерфейсов PON	1
Поддержка стандартов	ITU-T G.984.x Gigabit-capable passive optical networks (GPON) ITU-T G.988 ONU management and control interface (OMCI) specification 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 1:64
Максимальная дальность действия	до 10 км
Передатчик:	1310Нм
Скорость соединения upstream	1244Mb/s
Мощность передатчика	-2..+3 dBm
Ширина спектра опт. излучения (RMS)	3 nm
Приемник	1490Нм
Скорость соединения downstream	2488Mb/s
Чувствительность приемника	от -3 до -23 dBm

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-Fi

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 +/-1.5dBm 802.11g: 15dBm +/-1.5dBm 802.11n: 14.75dBm +/-1.5dBm
MAC-протокол	CSMA/CA модель ACK 32 MAC
Безопасность	64/128-битное WEP-шифрование данных; WPA, WPA2 802.1x AES & 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 dBi
Рабочий диапазон температур	от 0 до +70°C

Управление

Локальное управление	web-интерфейс
Удаленное управление	по протоколу Telnet, TR-069, OAM
Ограничение доступа	по паролю

Общие параметры

Питание	адаптер питания 12V DC /220 AC
Потребляемая мощность	не более 24 Вт
Рабочий диапазон температур	от +5 до +40°C
Относительная влажность	до 80%
Габариты	218x120x49 мм
Масса устройства	0,3 кг

2.5 Конструктивное исполнение

Абонентский терминал NTP-RG-1402G-W rev.C выполнен в виде настольного изделия в пластиковом корпусе.

Внешний вид задней панели устройства NTP-RG-1402G-W rev.C приведен на Рисунке 3.

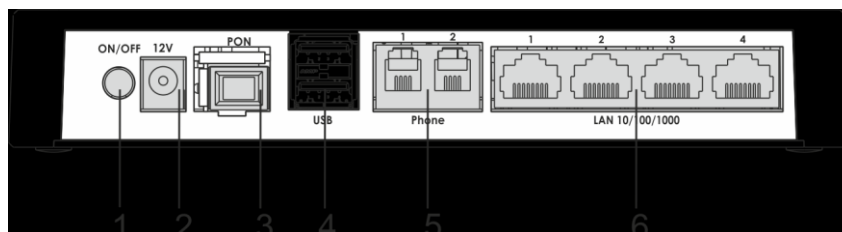


Рисунок 3 – Внешний вид задней панели NTP-RG-1402G-W rev.C

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

Таблица 3 – Описание разъемов, и органов управления задней панели

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

Внешний вид боковой и верхней панелей устройства NTP-RG-1402G-W rev.C приведен на Рисунке 4.

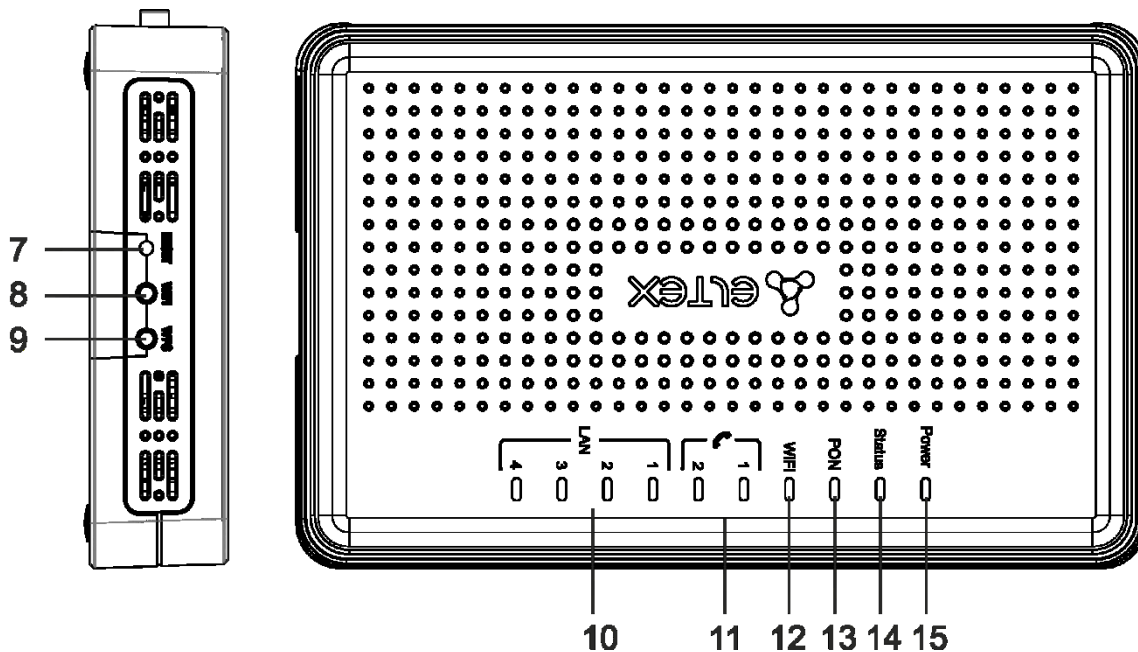


Рисунок 4 – Внешний верхней и боковой панели NTP-RG-1402G-W rev.C

На боковой панели устройства расположены следующие кнопки, таблица 4.

Таблица 4 – Описание кнопок боковой панели

№	Элемент панели	передней	Описание
7	Reset		функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам
8	Wi-Fi		кнопка включения/выключения Wi-Fi
9	WPS		кнопка для автоматического защищенного подключения к сети Wi-Fi на устройстве

На верхней панели устройства расположены следующие световые индикаторы, таблица 5.

Таблица 5 – Описание индикаторов верхней панели

№	Элемент панели	передней	Описание
10	LAN 1..4		индикаторы работы Ethernet-портов
11	Phone 1..2		индикатор активности портов FXS
12	Wi-Fi		индикатор активности Wi-Fi
13	PON		индикатор работы оптического интерфейса
14	Status		индикатор сигнализации прохождения авторизации устройства
15	Power		индикатор питания и статуса работы

2.6 Световая индикация

Текущее состояние устройства отображается при помощи индикаторов **LAN 1..4, Phone 1..2, Wi-Fi, PON, Status, Power**, расположенных на передней панели.

Перечень состояний индикаторов приведен в таблице 5.

Таблица 5 – Световая индикация устройства

Индикатор	Состояние индикатора	Состояние устройства
Индикаторы LAN 10/100/1000		
LAN 1..4	зеленый	установлено соединение 10/100 Мбит/с
	оранжевый	установлено соединение 1000 Мбит/с
	мигает	процесс пакетной передачи данных
Phone 1..2	горит	телефонная трубка снята
	мигает	порт не зарегистрирован или не пройдена авторизация на SIP-сервере
	медленно мигает	прием сигнала вызова
Wi-Fi	зеленый	сеть Wi-Fi активна
	мигает	процесс передачи данных по Wi-Fi
	не горит	сеть Wi-Fi не активна
PON	не горит	процесс загрузки устройства
	зеленый	установлено соединение между стационарным оптическим терминалом и устройством
	красный	нет сигнала от стационарного оптического терминала
Status	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)
Power	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

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 Перезагрузка/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 секунд, пока индикатор POWER не загорится красным светом. При заводских установках IP адрес: LAN - 192.168.1.1, маска подсети – 255.255.255.0. Доступ возможен с портов LAN 1 и LAN 2.

2.8 Комплект поставки

В базовый комплект поставки устройства *NTP-RG-1402G-W rev.C* входят:

- абонентский оптический терминал *NTP-RG-1402G-W rev.C*;
- адаптер питания 220/12;
- руководство по эксплуатации.

3 АРХИТЕКТУРА NTP-RG-1402 REV.C

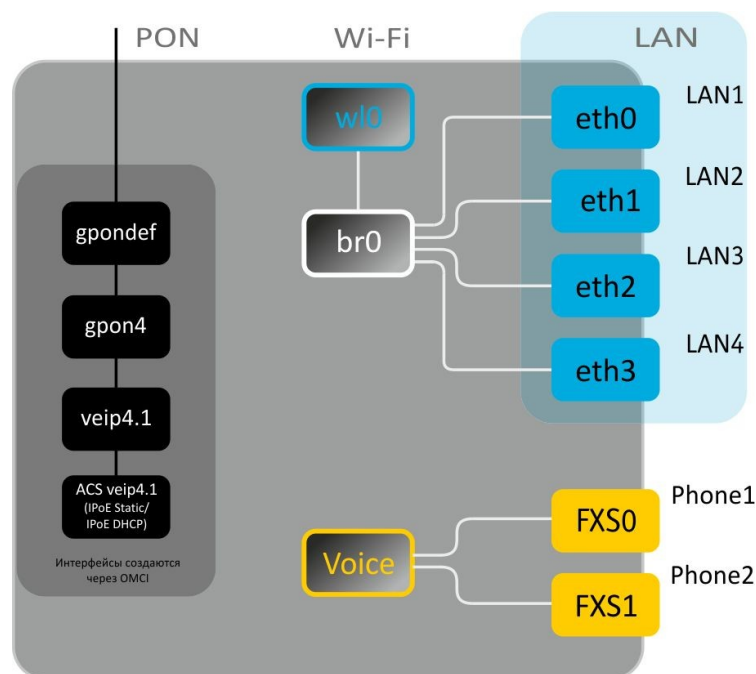


Рисунок 5 – Архитектура устройства с заводской конфигурацией

Основные элементы устройства

- **процессор (PON-чип)** – является конвертером интерфейсов Ethernet и GPON;
- **Wi-Fi модуль** – предназначен для организации беспроводного интерфейса на устройстве.

При заводской (начальной) конфигурации в устройстве присутствуют следующие логические блоки (рисунок 5):

- `br0`;
- VOICE (блок IP телефонии);
- `eth0...3`;
- `FXS0...1`;
- `wl0`.

Блок `br0` предназначен для объединения портов LAN в одну группу.

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

Блоки `FXS0..1` физически являются портами с разъемом RJ-11 для подключения аналоговых телефонных аппаратов. Логически включены в блок VOICE. Управление блоком VOICE может осуществляться через WEB-интерфейс, а также удаленно с помощью сервера ACS по протоколу TR-069. В данном блоке задаются параметры сервиса VoIP (адрес SIP сервера, номера телефонных аппаратов, услуги ДВО и т.д).

Блок `wl0` является интерфейсом для подключения Wi-Fi-модуля.

При подключении к устройству ОВ (установлении успешного соединения со стационарным оптическим устройством OLT) дополнительно создаются блоки `gpondef`, `gpon4`, `veip4`, `veip4.1 (ACS)` при помощи протокола OMCI (ONT Management and Control Interface).

Блок ACS может работать в 2-х режимах: IPoE Static (задание статического адреса для интерфейса veip4.1) и IPoE DHCP (получение адреса автоматически по протоколу DHCP). Блок используется для удаленного управления устройством с помощью сервера ACS (Auto Configuration Server – сервер автоконфигурации абонентских устройств). При помощи данного блока организуется взаимодействие с абонентским оборудованием, осуществляется обработка запросов от устройств NTP и подключаются сервисы.

На рисунке 6 представлена архитектура устройства, сконфигурированного для предоставления услуг Triple Play.

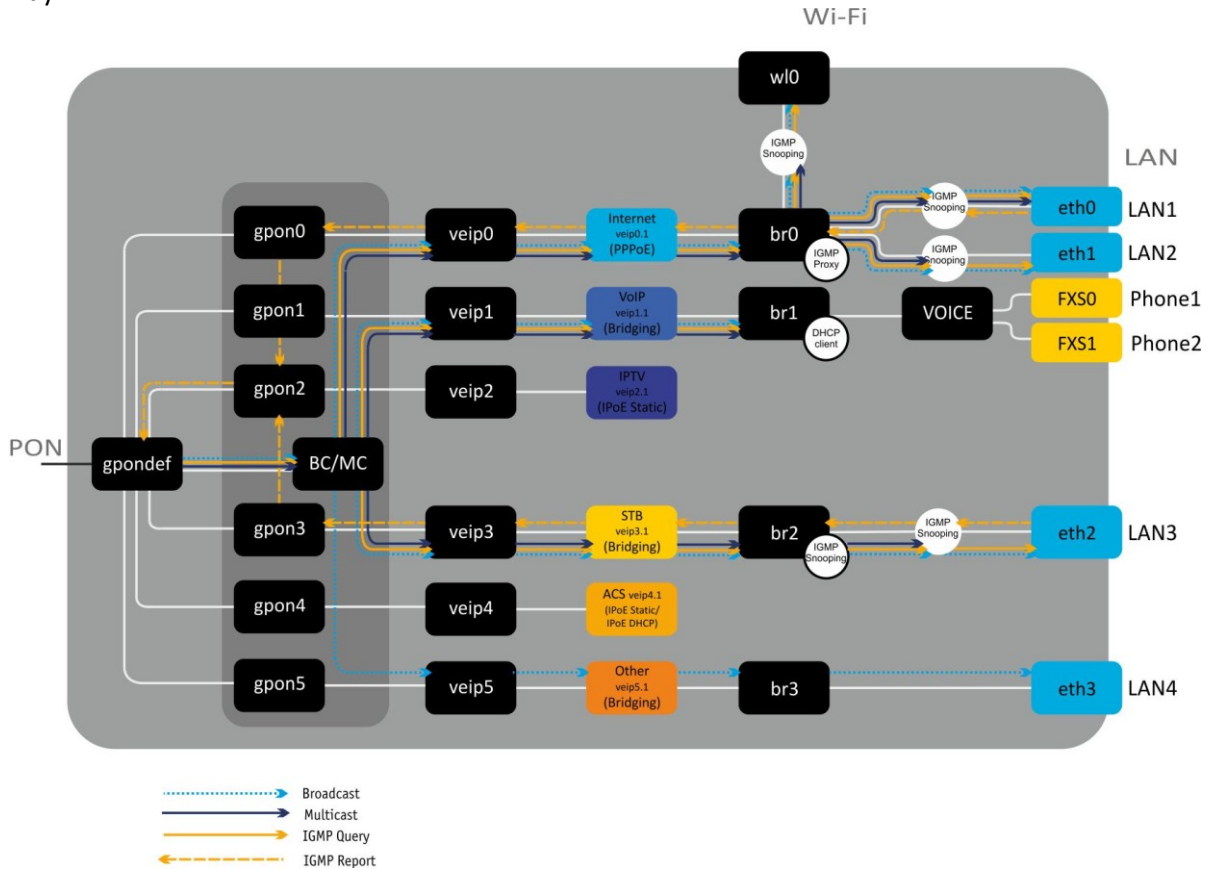


Рисунок 6 – Архитектура устройства, сконфигурированного для предоставления услуг Triple Play

Блоки gpon i (где $i=0..5$) представляют собой логическое окончание gem-портов, по которым передается трафик различных услуг. Весь unicast-трафик, проходящий через блоки *gpon i* (*gpon0 – gpon5*) передается на соответствующие *veip*-интерфейсы.

Блок BC/MC является логическим окончанием GEM-портов широковещательной (broadcast) и групповой (multicast) передачи. Через него передается multicast/broadcast-трафик в нисходящем потоке (downstream).

Veip-интерфейсы обеспечивают стык интерфейсов *gpon* (OMCI часть) и *Linux*-интерфейсов. Через *veip i* интерфейсы (где $i=0..5$) передается тегированный трафик, полученный с соответствующих *veip i.n*-интерфейсов.

Multicast/broadcast-трафик, полученный с блока *MC/BC*, попадает на все *veip*-интерфейсы.

Блоки veip i.n являются WAN-интерфейсами роутера устройства, каждый из которых служит для предоставления определенного вида услуг. В приведенном примере:

- *veip0.1* служит для предоставления услуги Internet;
- *veip1.1* – для предоставления услуги VoIP;

- veip2.1 – для управления multicast-трафиком;
- veip3.1 – для предоставления услуг VoD, IPTV на STB;
- veip4.1 предназначен для удаленного управления и мониторинга по протоколу TR-069;
- veip5.1 – для предоставления других услуг (например, VPN) на отдельном порту.

Любой из WAN-интерфейсов может работать в следующих режимах:

- PPPoE – запускается PPP client;
- IPoE DHCP – запускается DHCP client;
- IPoE Static – используется статический адрес;
- Bridging – работа в режиме моста.

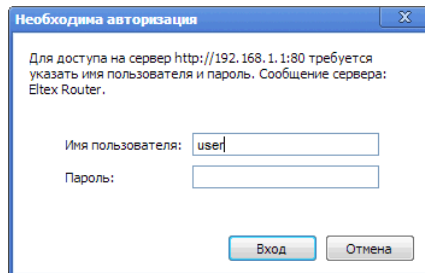
Блоки eth0..3 являются LAN-интерфейсами (LAN1...4) для подключения клиентского оборудования.

Логическими блоками, которые объединяют интерфейсы LAN и WAN, являются **br0..3**. **Br0** подключен к интерфейсу veip0.1, который работает в режиме PPPoE и к портам *eth0*, *eth1*, *wl0*. Блок **br1** работает в режиме bridge + DHCP, что позволяет использовать адрес этого интерфейса для SIP клиента (блок VOICE). Блоки *br2* и *br3* работают в режиме моста, который позволяет прозрачно пропускать трафик на LAN порты маршрутизатора.

4 НАСТРОЙКА NTP-RG-1402 REV.C ЧЕРЕЗ WEB-ИНТЕРФЕЙС. ДОСТУП ПОЛЬЗОВАТЕЛЯ

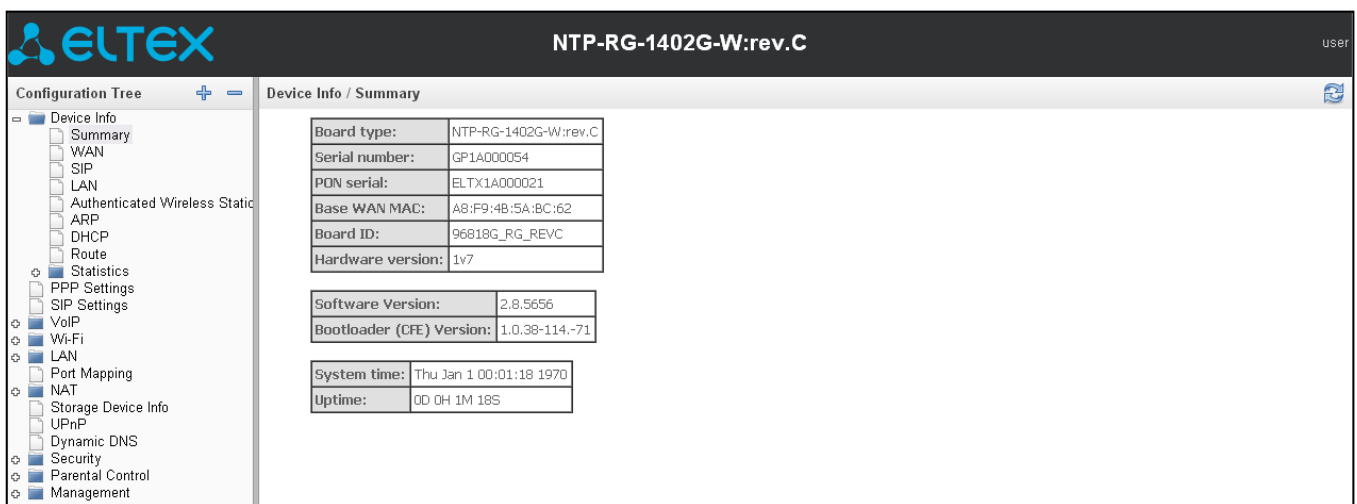
Для того чтобы произвести конфигурирование устройства, необходимо подключиться к нему через web browser (программу для просмотра гипертекстовых документов), например, Firefox, Google Chrome. Для этого необходимо ввести в адресной строке браузера IP-адрес устройства (при заводских установках адрес: - 192.168.1.1, 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.



4.1 Меню *Device Info* . Информация об устройстве

4.1.1 Подменю *Summary*. Общая информация об устройстве

Device Info / Summary	
Board type:	NTP-RG-1402G-W:rev.C
Serial number:	GP1A027048
PON serial:	ELTX1A006993
Base WAN MAC:	A8:F9:4B:5E:82:C6
Board ID:	96818G_RG_REVC
Hardware version:	1V10
Software Version:	2.8.5656
Bootloader (CFE) Version:	1.0.38-114.-71
System time:	Thu Jan 1 00:26:03 1970
Uptime:	0D 0H 26M 3S

- *Board type* – модель устройства;
- *Serial number* – серийный номер устройства;
- *PON serial* – серийный номер устройства в сети PON;
- *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.

4.1.2 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;
- *Default Gateway* – шлюз по умолчанию;
- *Primary DNS Server*¹ – адрес первичного DNS сервера, используемого для работы;
- *Secondary DNS Server* – адрес вторичного DNS сервера, используемого для работы;
- *Bridging to* – список связанных интерфейсов.

WAN service 0: Internet.1100	
Interface	ppp0.1
Type	PPPoE
Status	Connected
IPv4 Address	192.168.100.111
Primary DNS Server	192.168.100.1
Secondary DNS Server	10.10.0.2
Bridging to	eth0.0,eth1.0,wl0
WAN service 1: VoIP.1101	
Interface	veip1.1
Type	Bridge
Status	Connected
IPv4 Address	192.168.101.147
Default Gateway	192.168.101.1
Primary DNS Server	192.168.198.102

¹ Только для сервиса **INTERNET, VoIP**

4.1.3 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	192.168.101.1:5060	
SIP Outbound Proxy	192.168.101.1:5060	
SIP Registrar	192.168.101.1:5060	
	Account 0	Account 1
State	Up	Up
Error	None	None
Response code	200 OK	200 OK
Account enabled	Enabled	Enabled
Extension	4390	4391
Display name	4390	4391
Authentication name	4390	4391

- *Voice daemon status* – состояние работы голосового демона;
- *SIP Proxy* – адрес и порт SIP Proxy;
- *SIP Outbound Proxy* – адрес и порт SIP проху, 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;
- *Error* – ошибка, выдаваемая сервером SIP;
- *Response code* – код ответа сервера SIP;
- *Account enabled* – состояние порта FXS;
- *Extension* – номер телефона;
- *Display name* – отображаемое имя пользователя;
- *Authentication name* – имя пользователя для аутентификации.

4.1.4 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 1	Down
Port 2	Up; 1000M full
Port 3	Down
Port 4	Down
Wi-Fi	Up

4.1.5 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*».

4.1.6 Подменю *ARP*. Просмотр кэша протокола ARP

Эффективность функционирования ARP во многом зависит от ARP-кэша, который присутствует на каждом хосте. В кэше содержатся 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
192.168.1.2	Complete	00:25:22:78:55:1f	br0
192.168.200.1	Complete	a8:f9:4b:80:4f:83	veip4.1

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

4.1.7 Подменю *DHCP*. Активные аренды DHCP

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

Device Info / DHCP			
Hostname	MAC Address	IP Address	Expires In
manager07	bc:ae:c5:b3:95:fe	192.168.1.2	23 hours, 32 minutes, 14 seconds
android-16b54973c7ad4980	18:00:2d:c7:43:8c	192.168.1.3	20 hours, 8 minutes, 17 seconds

- *Hostname* – имя хоста(сетового устройства);
- *MAC Address* – MAC адрес устройства;

- *IP Address* – адрес устройства в локальной сети, выданный маршрутизатором из пула IP-адресов;
- *Expires In* – время, через которое истекает аренда данного адреса.

4.1.8 Подменю **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
192.168.100.1	0.0.0.0	255.255.255.255	UH	0	Internet	ppp0.1
192.168.100.1	0.0.0.0	255.255.255.255	UH	0	Internet	ppp0.1
192.168.15.100	192.168.101.1	255.255.255.255	UGH	0		br1
172.16.0.3	192.168.101.1	255.255.255.255	UGH	0		br1
192.168.115.102	192.168.101.1	255.255.255.255	UGH	0		br1
192.168.111.1	192.168.101.1	255.255.255.255	UGH	0		br1
192.168.101.0	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	MC	veip2.1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
192.168.200.0	0.0.0.0	255.255.252.0	U	0	ipoe_veip4	veip4.1
0.0.0.0	0.0.0.0	0.0.0.0	U	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.

4.1.9 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 1	0	0	0	0	0	0	0	0
Port 2	410101	3967	0	0	1421128	2086	0	0
Port 3	0	0	0	0	0	0	0	0
Port 4	0	0	0	0	0	0	0	0
Wi-Fi	0	0	0	0	0	0	0	0

Reset Statistics

WAN Service:

Device Info / Statistics / WAN Service									
Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
veip1.1	VoIP	92646	1450	0	0	35007	73	0	0
veip2.1	IGMP	0	1319150	0	0	2146	37	0	0
veip3.1	STB	5048	51	0	0	0	0	0	0
veip4.1	ipoe_veip4	2329604	9425	0	0	4207318	8985	0	0
veip5.1	VPN	3438	16	0	0	0	0	0	0
ppp0.1	Internet	10415	38	0	0	34592	564	0	0

[Reset Statistics](#)

Интерфейс Optical:

Для устройств серии NTP-RG-1402GC-(W) rev.C с возможностью приема услуг кабельного телевидения (CaTV) данное меню имеет дополнительную таблицу:

- *Link Status* – статус оптического линка,
- *Optical Signal Level* – уровень принимаемого сигнала (1490нм),
- *Transmit Optical Level* – уровень передаваемого сигнала (1310нм),
- *Optical Video Level* – уровень принимаемого аналогового видео-сигнала (CaTV 1550нм).

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](#)

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

4.2 Меню «*PPP settings*». Настройки PPP¹

PPP Settings

INTERNET (ppp0.1)

Enable Service

IP_Routed

Username:

Password:

[Apply/Save](#)

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.

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

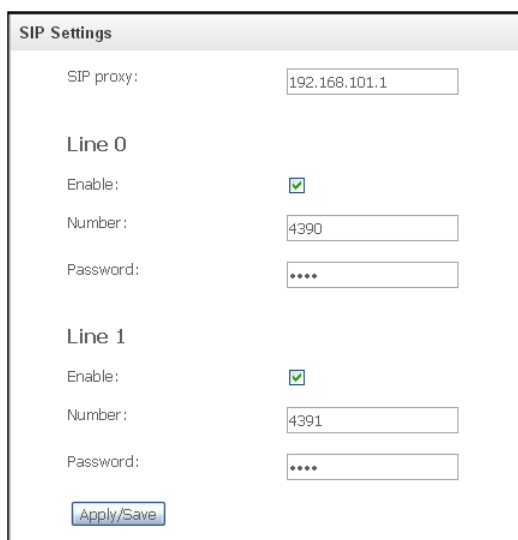
- *Username* – логин пользователя для доступа к сети Интернет;
- *Password* – пароль пользователя для доступа к сети Интернет;



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

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

4.3 Меню *SIP Settings*. Настройки SIP¹



- *SIP proxy* – адрес SIP прокси 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;
- *Password* – пароль для доступа.

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

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

4.4 Меню *VoIP.SIP Advanced Setting*. Дополнительные настройки SIP

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

VoIP / SIP Advanced Setting		
	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 ▾	2 ▾
Call barring digit map	<input type="text"/>	4390
Warm line	<input type="checkbox"/>	<input type="checkbox"/>
Warm line number	<input type="text"/>	<input type="text"/>
Anonymous call blocking	<input type="checkbox"/>	<input type="checkbox"/>
Anonymous calling	<input type="checkbox"/>	<input type="checkbox"/>
DND	<input type="checkbox"/>	<input type="checkbox"/>

- *Account 0, Account 1* – 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 исходящие вызовы;
- *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»;
- *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*».

4.5 Меню *Wi-Fi*. Настройка беспроводной сети

4.5.1 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: A8:F9:4B:5E:82:C7

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

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



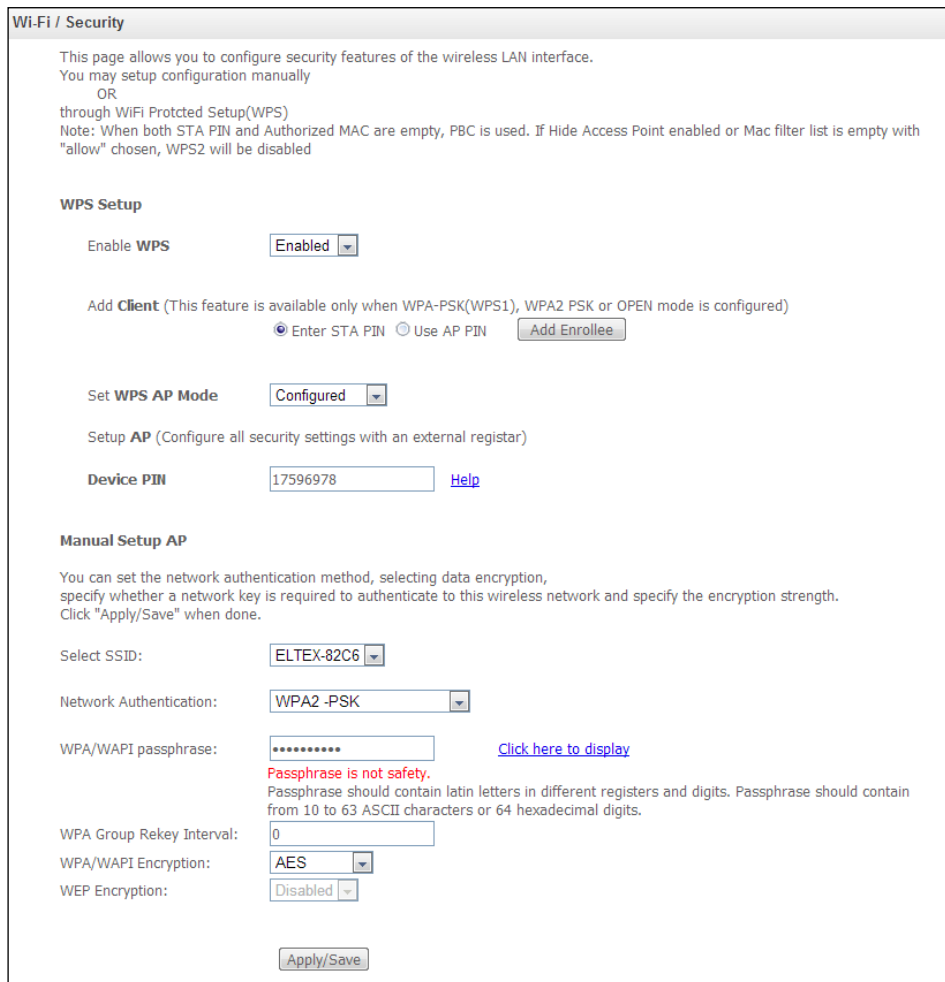
По умолчанию на устройстве установлено имя беспроводной сети (SSID) ELTX-aaaa, где aaaa - это 4 последние цифры WAN MAC. WAN MAC указан в наклейке на корпусе устройства.

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

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

4.5.2 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.



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

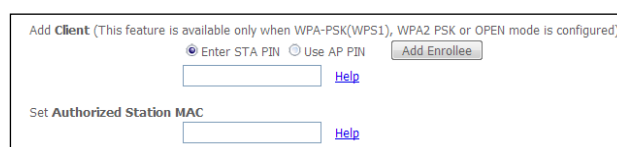
Для того чтобы подключиться, достаточно нажать на кнопку WPS, расположенную на боковой панели устройства, или же ввести PIN-код, используя веб-конфигуратор.

WPS setup:

— *Enable WPS* – для разрешения доступа по WPS в выпадающем списке выберите «*Enable*», если сетевой адаптер Wi-Fi Вашего устройства поддерживает данный режим настройки;

— *Add Client*– выбор метода авторизации клиента (настройки применимы только в режимах *WPA-PSK*, *WPA2-PSK*). Для начала процесса авторизации необходимо нажать кнопку «*Add Enrollee*»:

— *Enter STA PIN* – авторизация с помощью PIN кода, выданного клиентом;



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



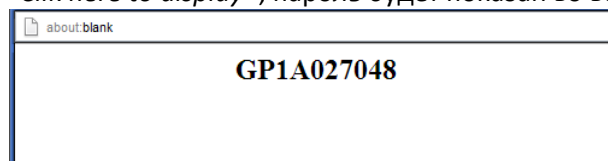
Недостатки метода WPS

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

Manual Setup AP:

- *Select SSID* – выбрать имя беспроводной сети из списка;
- *Network Authentication* – установить режим сетевой аутентификации из перечня в выпадающем списке:

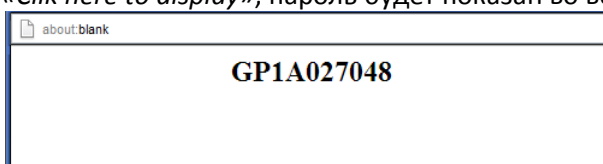
- *open* – открытый – защита беспроводной сети отсутствует (в этом режиме может использоваться только WEP-ключ);
- *Shared* – общий (режим позволяет пользователям получать аутентификацию по их SSID или WEP-ключу);
- *802.1x* – включает стандарт 802.1x (позволяет пользователям аутентифицироваться с использованием сервера аутентификации RADIUS, для шифрования данных используется WEP-ключ);
 - *RADIUS Server IP Address* – IP-адрес RADIUS-сервера;
 - *RADIUS Port* – номер порта RADIUS-сервера. По умолчанию установлен порт 1812;
 - *RADIUS Key* – секретный ключ для доступа к RADIUS-серверу;
- *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 «*Click here to display*», пароль будет показан во всплывающем окне.



По умолчанию ключ сети соответствует серийному номеру устройства. Серийный номер указан в наклейке на корпусе устройства.

- *WPA Group Rekey Interval* – интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности

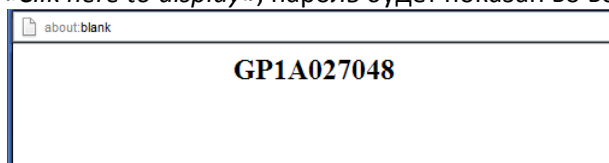
- беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение;
- *WPA/WAPI Encryption* – выбор метода шифрования данных WPA/WAPI: TKIP+AES, AES:
 - TKIP – протокол шифрования, используемый для WPA. Обладает более эффективным механизмом управления ключами по сравнению с WEP;
 - AES – алгоритм 128 битного блочного шифрование с ключом 128/192/256 бит, используется обычно для WPA2);
 - *WPA2* – включает WPA2 (режим использует протокол WPA2 и требует использования сервера аутентификации RADIUS);
 - *WPA2 Preauthentication*;
 - *Network Re-auth Interval*;
 - *WPA Group Rekey Interval* – интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение;
 - *RADIUS Server IP Address* – IP-адрес RADIUS-сервера;
 - *RADIUS Port* – номер порта RADIUS-сервера. По умолчанию установлен порт 1812;
 - *RADIUS Key* – секретный ключ для доступа к RADIUS-серверу;
 - *WPA/WAPI Encryption* – выбор метода шифрования данных WPA/WAPI: TKIP+AES, AES:
 - TKIP – протокол шифрования, используемый для WPA. Обладает более эффективным механизмом управления ключами по сравнению с WEP;
 - AES – алгоритм 128 битного блочного шифрование с ключом 128/192/256 бит, используется обычно для WPA2);
 - *WPA2-PSK* – включает WPA2-PSK (режим использует протокол WPA2, но не требует использования сервера аутентификации RADIUS);
 - *WPA/WAPI passphrase* – секретная фраза. Установка пароля, строка 8-63 символа ASCII. Для просмотра секретной фразы необходимо нажать на ссылку «*Click here to display*», пароль будет показан во всплывающем окне.



По умолчанию ключ сети соответствует серийному номеру устройства. Серийный номер указан в наклейке на корпусе устройства.

- *WPA Group Rekey Interval* – интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение;
- *WPA/WAPI Encryption* – выбор метода шифрования данных WPA/WAPI: TKIP+AES, AES:
 - TKIP – протокол шифрования, используемый для WPA. Обладает более эффективным механизмом управления ключами по сравнению с WEP;
 - AES – алгоритм 128 битного блочного шифрование с ключом 128/192/256 бит, используется обычно для WPA2);
- *Mixed WPA2/WPA* – включает комбинацию WPA2/WPA (данный режим шифрования использует протоколы WPA2 и WPA, требует использования сервера аутентификации RADIUS);

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

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



Убедитесь, что беспроводной адаптер компьютера поддерживает выбранный тип шифрования.

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

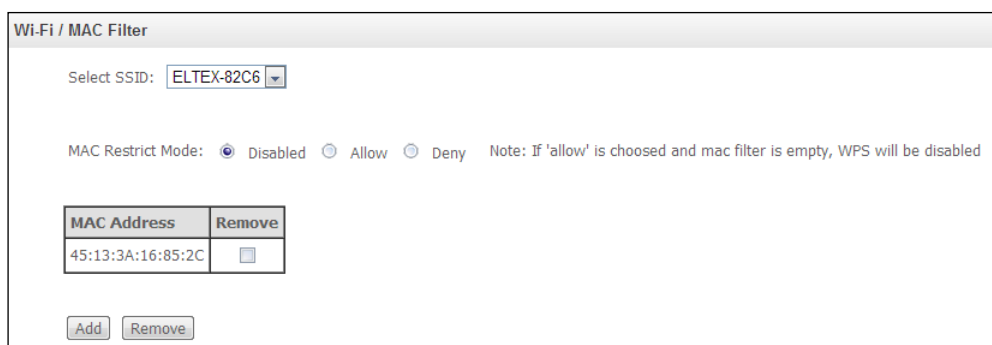
— *WEP Encryption*– для включения шифрования WEP выберите *Enable* в выпадающем списке;

- *Encryption Strength* – 64- или 128-битное шифрование ключа;
- *Current Network Key* – выбор ключа, который будет использоваться для установления соединения;
- *Network Key 1..4* - возможно задать до четырех различных ключей из 10 символов в 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*».

4.5.3 Подменю **MAC Filter**. Настройки фильтрации MAC-адресов

В данном меню производится настройка фильтрации MAC-адресов



Wi-Fi / MAC Filter

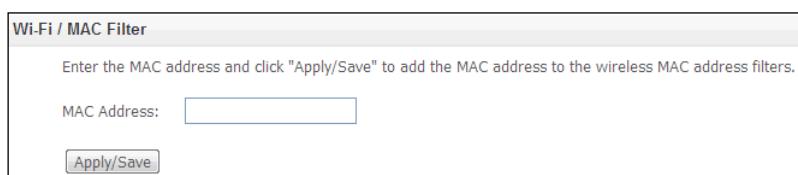
Select SSID:

MAC Restrict Mode: Disabled Allow Deny Note: If 'allow' is choosed and mac filter is empty, WPS will be disabled

MAC Address	Remove
45:13:3A:16:85:2C	<input type="checkbox"/>

- *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:



Wi-Fi / MAC Filter

Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.

MAC Address:

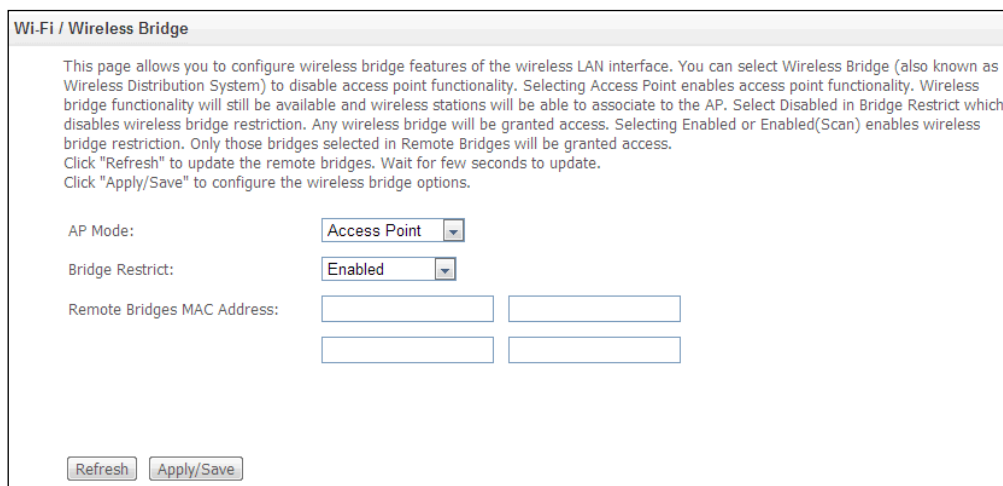
Для принятия изменений необходимо нажать кнопку «*Apply/Save*».

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

4.5.4 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.



Wi-Fi / Wireless Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Apply/Save" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

В режиме «Wireless Bridge» возможно задать следующие на тройки:

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



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

Для обновления доступных удаленных мостов необходимо нажать «*Refresh*».

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

4.5.4.1 Подменю **Advanced**. Расширенные настройки

В данном меню производится 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: 6 (interference: acceptable)

Channel:

Auto Channel Timer(min):

802.11n/EWC:

Bandwidth: Current: 20MHz

Control Sideband: Current: N/A

802.11n Rate:

802.11n Protection:

Support 802.11n Client Only:

RIFS Advertisement:

OBSS Coexistence:

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 20ГГц или 40 ГГц. 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 Advertisemen** – (Reduced Interframe Space) уменьшение интервала между блоками данных (PDUs), повышает эффективность Wi-Fi;

— **OBSS Co-Existance** – 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»;

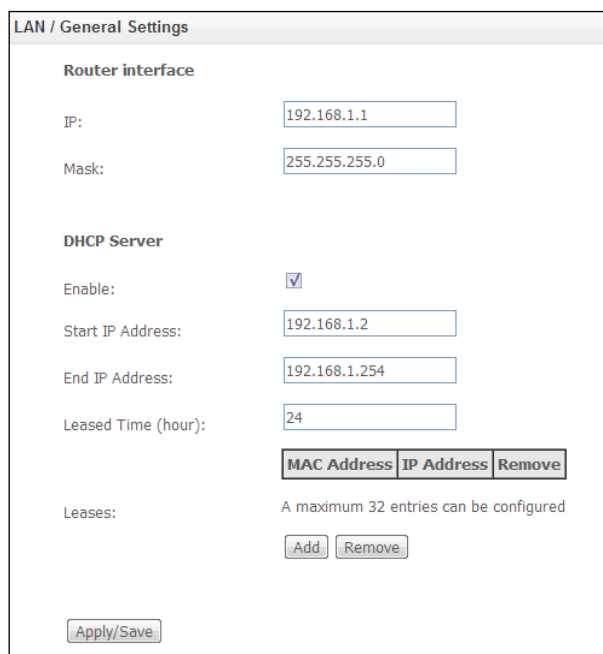
- *RX Chain Power Save* – отключение приема на одной из антенн устройства в целях энергосбережения;
- *RX Chain Power Save Quiet Time* – период времени, в течении которого интенсивность трафика должна быть ниже PPS, для включения режима энергосбережения;
- *RX Chain Power Save PPS* – верхняя граница 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 широковещательные и многоадресные пакеты, помещенные в буфер, будут доставлены беспроводным клиентам;
- *Beacon Interval* – период отправки информационного пакета в беспроводную сеть, сигнализирующего о том что точка доступа активна;
- *Global Max Clients* – максимальное количество беспроводных клиентов;
- *XPress™ Technology* – использование позволяет повысить пропускную способность до 27% в сетях стандарта 802.11g. А в смешанных сетях 802.11g и 802.11b использование XPress™ Technology может повысить пропускную способность до 75%;
- *Transmit Power* – определяется мощность сигнала точки доступа;
- *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*».

4.6 Меню LAN. Настройки локальной сети

4.6.1 Подменю *General Settings*. Настройка основных параметров

В данном меню производится настройка основных параметров для LAN интерфейса.



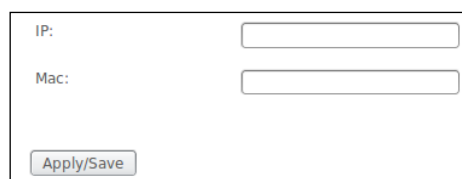
Router interface:

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

DHCP Server:

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

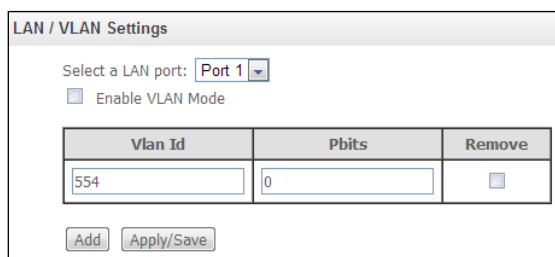
- *Enable* – при установленном флаге использовать DHCP сервер (сетевые устройства будут получать IP-адреса динамически, из нижеприведенного диапазона);
- *Start IP Address* – начальный адрес диапазона;
- *End IP Address* – конечный адрес диапазона;
- *Leased Time (hour)* – время аренды адреса (в часах);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



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

4.6.2 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».

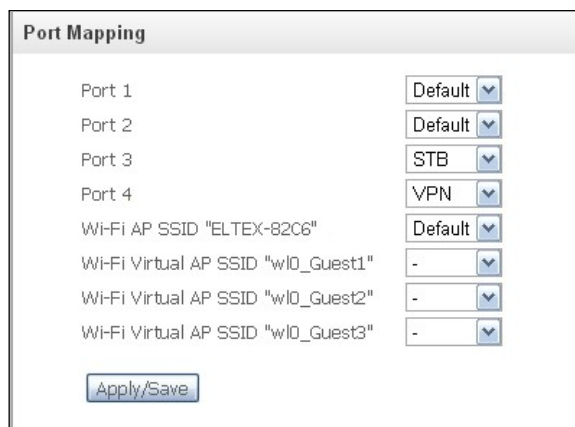
Для удаления необходимо установить флаг «Remove» в выбранной строке и нажать кнопку «Apply/Save».

4.7 Меню *Port Mapping*¹

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».



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

4.8 Меню NAT. Настройки NAT

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

4.8.1 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.

NAT / Virtual Servers

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
Blizzard Battle.net	4000	4000	TCP	4000	4000	192.168.1.123	veip0.1	<input type="checkbox"/>
Blizzard Battle.net	6112	6112	TCP	6112	6112	192.168.1.123	veip0.1	<input type="checkbox"/>
Blizzard Battle.net	6112	6112	UDP	6112	6112	192.168.1.123	veip0.1	<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:

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:32

Use Interface: Internet/ppp0.1
 Service Name:
 Select a Service: Active Worlds
 Custom Service:
 Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
<input style="width: 50px;" type="text" value="3000"/>	<input style="width: 50px;" type="text" value="3000"/>	TCP	<input style="width: 50px;" type="text" value="3000"/>	<input style="width: 50px;" type="text" value="3000"/>
<input style="width: 50px;" type="text" value="5670"/>	<input style="width: 50px;" type="text" value="5670"/>	TCP	<input style="width: 50px;" type="text" value="5670"/>	<input style="width: 50px;" type="text" value="5670"/>
<input style="width: 50px;" type="text" value="7777"/>	<input style="width: 50px;" type="text" value="7777"/>	TCP	<input style="width: 50px;" type="text" value="7777"/>	<input style="width: 50px;" type="text" value="7777"/>
<input style="width: 50px;" type="text" value="7000"/>	<input style="width: 50px;" type="text" value="7000"/>	TCP	<input style="width: 50px;" type="text" value="7000"/>	<input style="width: 50px;" type="text" value="7000"/>
<input style="width: 50px;" type="text"/>	<input style="width: 50px;" type="text"/>	TCP	<input style="width: 50px;" type="text"/>	<input style="width: 50px;" type="text"/>
<input style="width: 50px;" type="text"/>	<input style="width: 50px;" type="text"/>	TCP	<input style="width: 50px;" type="text"/>	<input style="width: 50px;" type="text"/>
<input style="width: 50px;" type="text"/>	<input style="width: 50px;" type="text"/>	TCP	<input style="width: 50px;" type="text"/>	<input style="width: 50px;" type="text"/>
<input style="width: 50px;" type="text"/>	<input style="width: 50px;" type="text"/>	TCP	<input style="width: 50px;" type="text"/>	<input style="width: 50px;" type="text"/>
<input style="width: 50px;" type="text"/>	<input style="width: 50px;" type="text"/>	TCP	<input style="width: 50px;" type="text"/>	<input style="width: 50px;" type="text"/>
<input style="width: 50px;" type="text"/>	<input style="width: 50px;" type="text"/>	TCP	<input style="width: 50px;" type="text"/>	<input style="width: 50px;" type="text"/>
<input style="width: 50px;" type="text"/>	<input style="width: 50px;" type="text"/>	TCP	<input style="width: 50px;" type="text"/>	<input style="width: 50px;" type="text"/>
<input style="width: 50px;" type="text"/>	<input style="width: 50px;" type="text"/>	TCP	<input style="width: 50px;" type="text"/>	<input style="width: 50px;" 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*».

4.8.2 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		Protocol	Port Range			
		Start	End		Start			End
Napster	TCP	6699	6699	TCP	6699	6699	veip0.1	<input type="checkbox"/>
Napster	TCP	6699	6699	TCP	6697	6697	veip0.1	<input type="checkbox"/>
Napster	TCP	6699	6699	TCP	4444	4444	veip0.1	<input type="checkbox"/>
Napster	TCP	6699	6699	TCP	5555	5555	veip0.1	<input type="checkbox"/>
Napster	TCP	6699	6699	TCP	6666	6666	veip0.1	<input type="checkbox"/>
Napster	TCP	6699	6699	TCP	7777	7777	veip0.1	<input type="checkbox"/>
Napster	TCP	6699	6699	TCP	8888	8888	veip0.1	<input type="checkbox"/>

Для добавления правил в таблицу необходимо нажать кнопку «*Add*», удаление происходит нажатием кнопки «*Remove*» 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 "Apply/Save" to add it.

Remaining number of entries that can be configured: 32

Use Interface: Internet/ppp0.1

Application Name:

Select an application:

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP

- *Use Interface* – используемый интерфейс.



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

- *Application Name* – настройки приложения:
 - *Select an application* – выбор преднастроенного правила.
 - *Custom an application* – создать свои, не указанные в списке *Select an application*, правила.

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

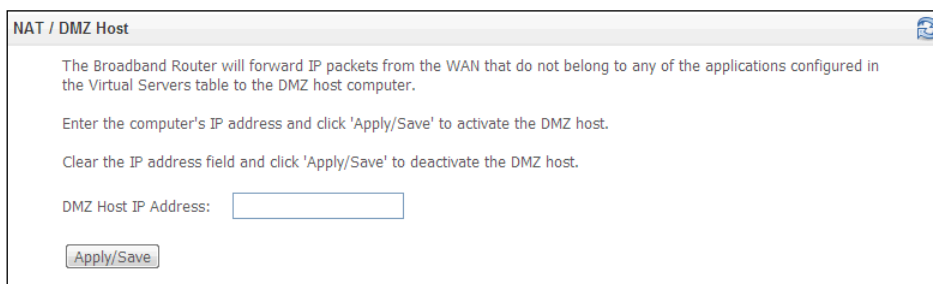
- *Trigger Port Start* – начальный порт диапазона портов, которые осуществляют функцию триггера;
- *Trigger Port End* – конечный порт диапазона портов, которые осуществляют функцию триггера;
- *Trigger Protocol* – протокол, используемый для триггера;
- *Open Port Start* – начальный порт диапазона портов,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

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

4.8.3 Подменю *DMZ Host*. Настройки демилитаризованной зоны

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

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



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

4.9 Меню *Storage Device Info*

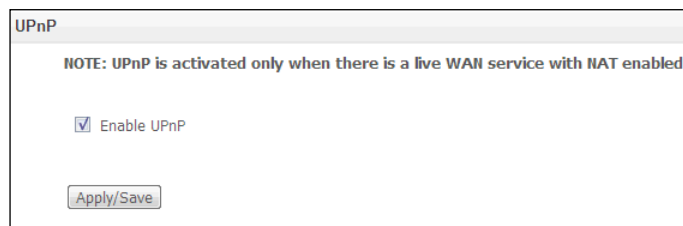
В данном меню доступен список всех подключенных запоминающих устройств. Предоставляется следующая информация:

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	3897	629	Unmount

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

4.10 Меню UPnP

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




Для использования UPnP необходимо настроить NAT на активном WAN интерфейсе.

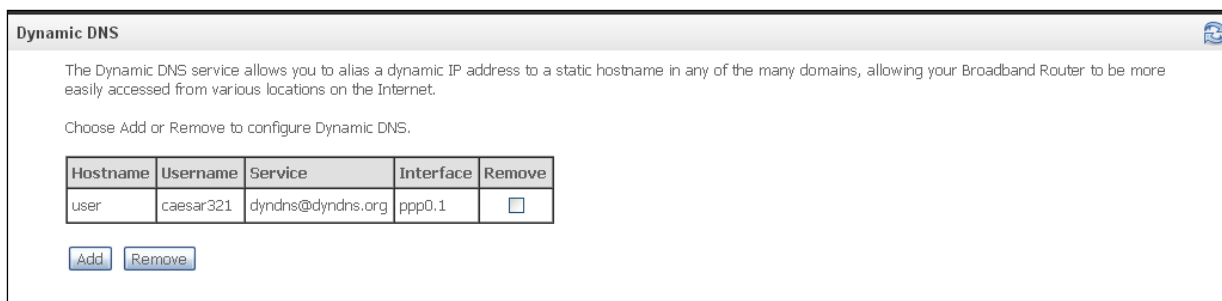
Для включения UPnP необходимо установить флаг «*Enable UPnP*».

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

4.11 Меню «Dynamic DNS». Настройка динамической системы доменных имен

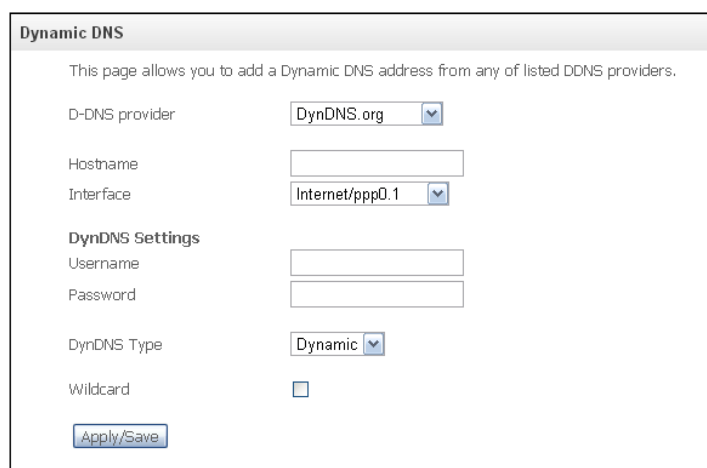
Dynamic DNS (динамическая система доменных имен) позволяет информации на DNS-сервере обновляться в реальном времени и (по желанию) в автоматическом режиме. Применяется для назначения постоянного доменного имени устройству (компьютеру, роутеру, например NTP-RG) с динамическим IP-адресом. Это может быть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

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

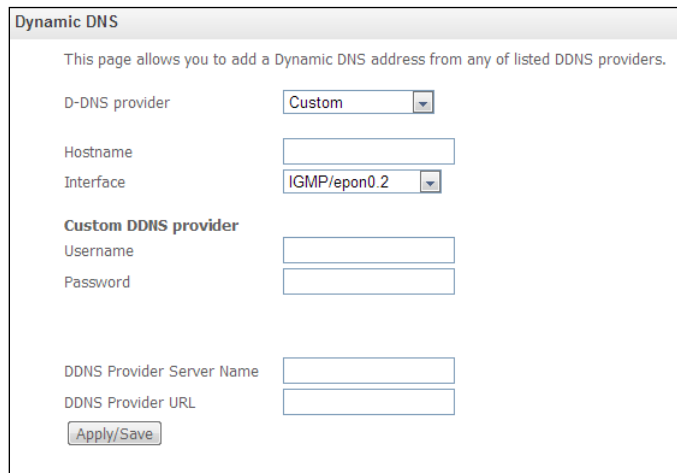


Hostname	Username	Service	Interface	Remove
user	caesar321	dyndns@dyndns.org	ppp0.1	<input type="checkbox"/>

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



- *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: Custom

Hostname:

Interface: IGMP/epon0.2

Custom DDNS provider

Username:

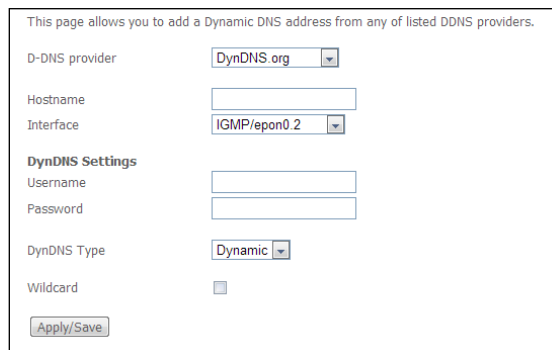
Password:

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

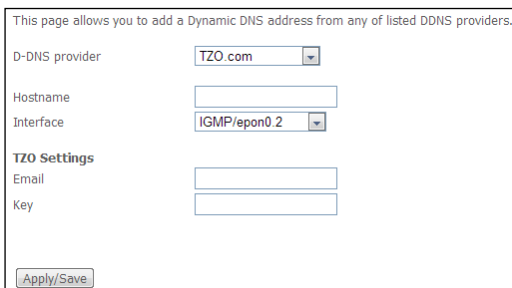
DynDNS Settings

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

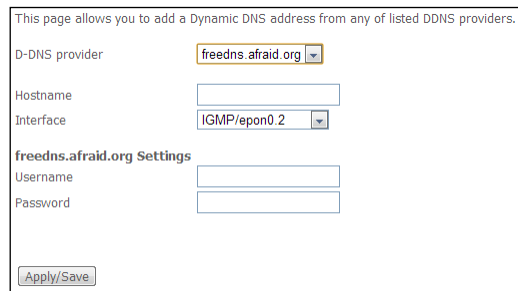
Hostname:

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».

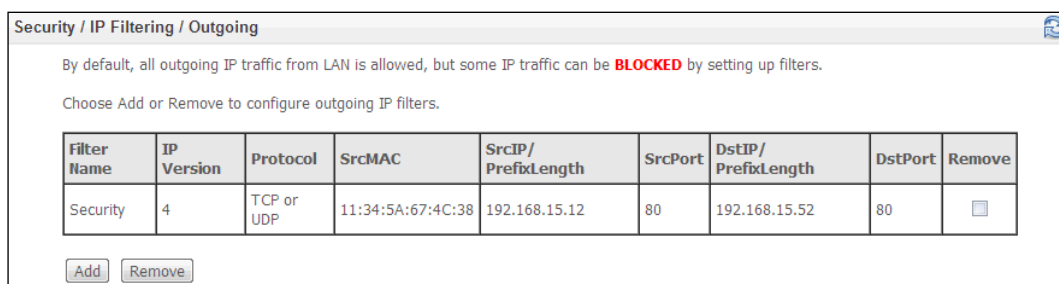
4.12 Меню *Security*. Настройки безопасности

В данном разделе проводится настройка параметров безопасности устройства.

4.12.1 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.

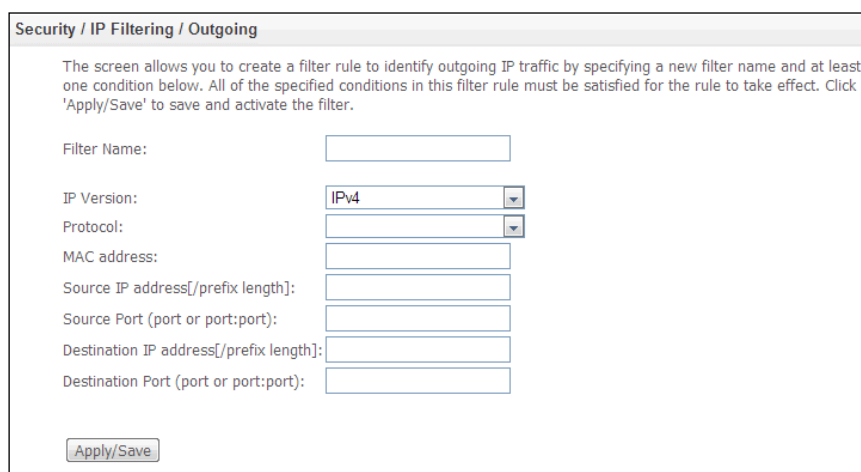
Choose Add or Remove to configure outgoing IP filters.

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



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

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



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]:

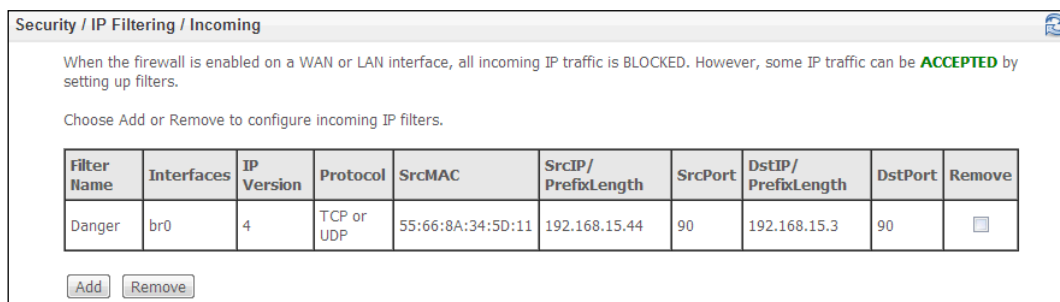
Destination Port (port or port:port):

- *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».

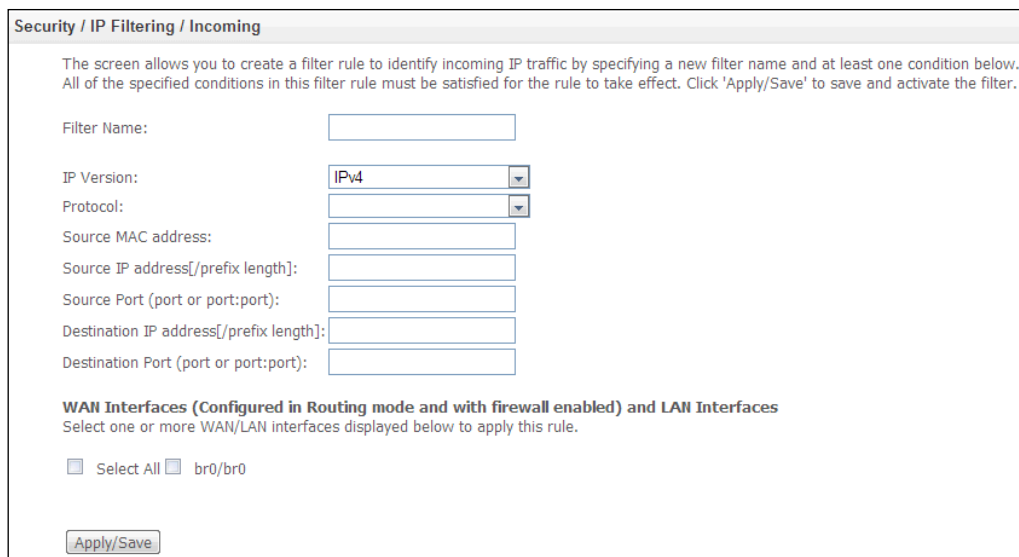
Настройки фильтрации входящего трафика (Incoming):



Filter Name	Interfaces	IP Version	Protocol	SrcMAC	SrcIP/PrefixLength	SrcPort	DstIP/PrefixLength	DstPort	Remove
Danger	br0	4	TCP or UDP	55:66:8A:34:5D:11	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».



- *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;

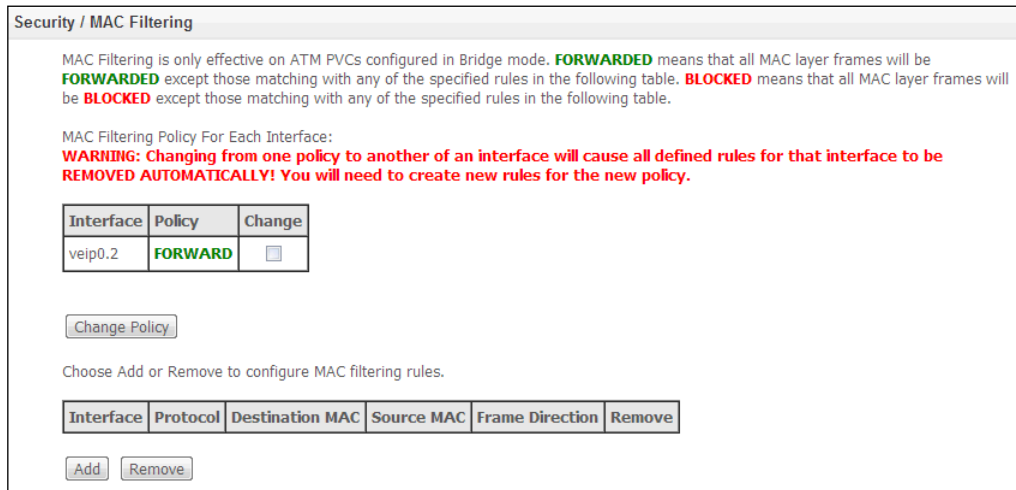
Интерфейсы WAN (сконфигурированные в режиме маршрутизатора и с включенным брандмауэром) и интерфейсы LAN:

- *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*».

4.12.2 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
veip0.2	FORWARD	<input type="checkbox"/>

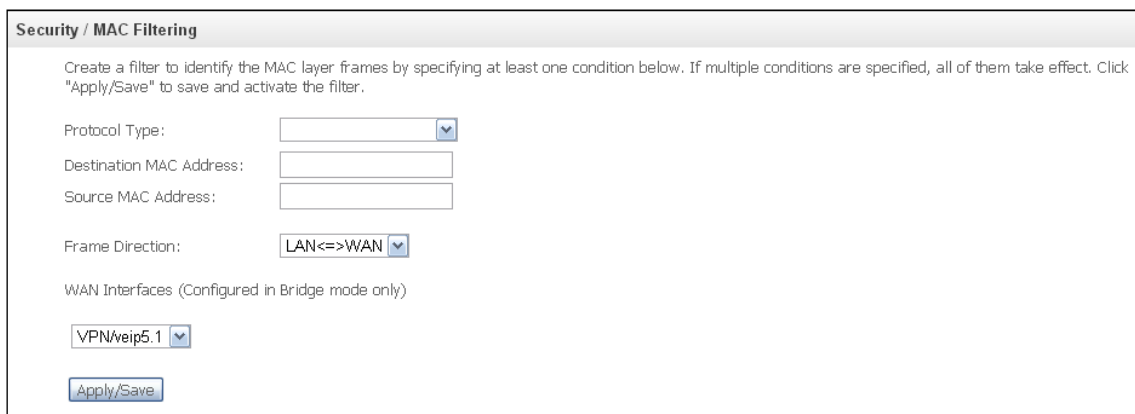
Choose Add or Remove to configure MAC filtering rules.

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.



Security / MAC Filtering

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

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

- *Protocol type* – выбор протокола (PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP);
- *Destination MAC Address* – MAC-адрес получателя;
- *Source MAC 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/Save*».

4.13 Меню *Parental control*. «Родительский контроль» – настройки ограничения

4.13.1 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.

Parental Control / Time Restriction											
A maximum 16 entries can be configured.											
Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
Mummy	bc:ae:c5:b3:95:fe	x	x	x	x	x			16:30	23:59	<input type="checkbox"/>
<input type="button" value="Add"/> <input type="button" value="Remove"/>											

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

Parental Control / Time Restriction							
<p>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".</p>							
User Name	<input type="text" value="Mummy"/>						
<input checked="" type="radio"/> Browser's MAC Address	<input type="text" value="bc:ae:c5:b3:95:fe"/>						
<input type="radio"/> Other MAC Address (xx:xx:xx:xx:xx:xx)	<input type="text"/>						
Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Start Blocking Time (hh:mm)	<input type="text" value="16:30"/>						
End Blocking Time (hh:mm)	<input type="text" value="23:59"/>						
<input type="button" value="Apply/Save"/>							

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

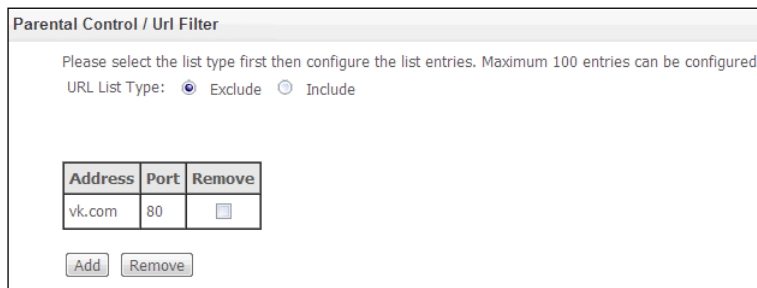


Ограничения будут действовать, если на устройстве установлено корректное системное время.

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

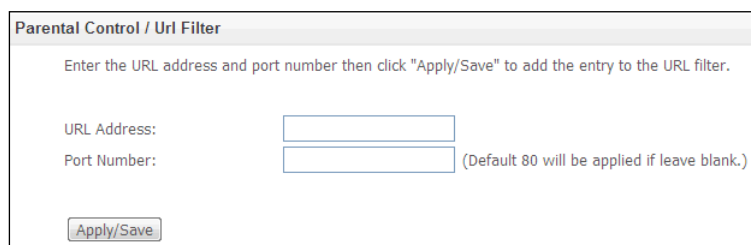
4.13.2 Подменю *Url Filter*. Настройки ограничения доступа в интернет

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



- *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*» .



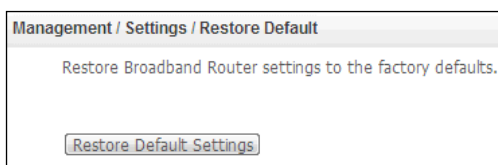
- *URL Address* – URL-адрес;
- *Port Number* – номер порта (если оставить поле пустым, будет использоваться 80 порт).

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

4.14 Меню *Management* . Управление устройством

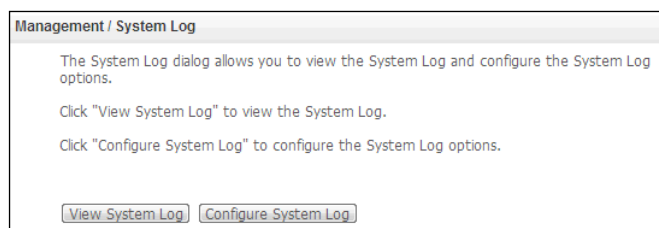
4.14.1 Подменю *Restore Default*. Возврат к настройкам по умолчанию

Меню позволяет вернуться к настройкам устройства, установленным по умолчанию. Устройство при этом будет перезагружено.



4.14.2 Подменю *System Log*. Просмотр и настройка системного журнала

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

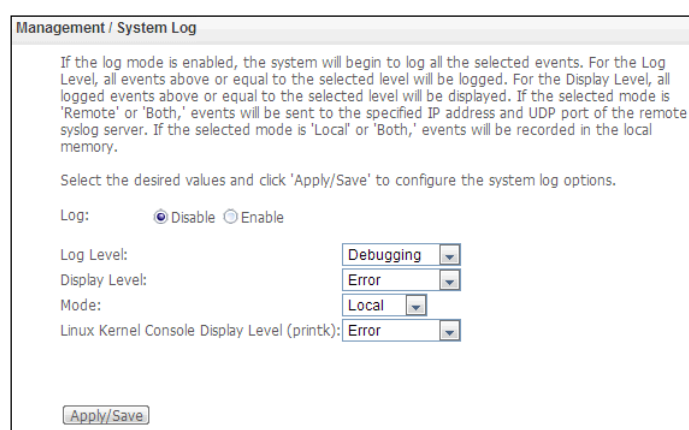


Переход к просмотру системного журнала осуществляется кнопкой «*View System Log*».



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

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



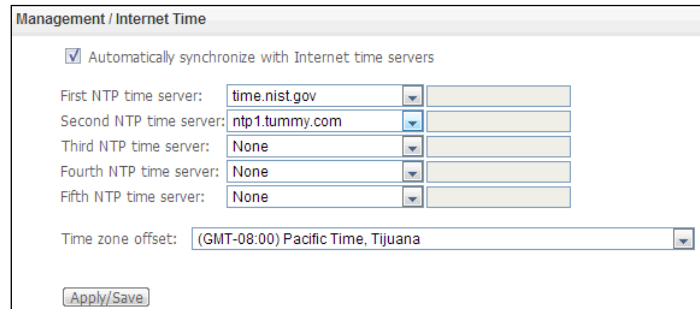
- *Log* – включение/выключение системного журнала(enabled/disabled);
- *Log Level* – установка уровня детализации журнала событий. Классификация уровней важности в порядке снижения значимости:
 - *Emergency* – аварийный случай;
 - *Alert* – тревога;
 - *Critical* – критическое событие;
 - *Error* – ошибка;
 - *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);
 - *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*».

4.14.3 Подменю *Internet Time*. Настройки системного времени



Во вкладке настраивается системное время на устройстве.

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



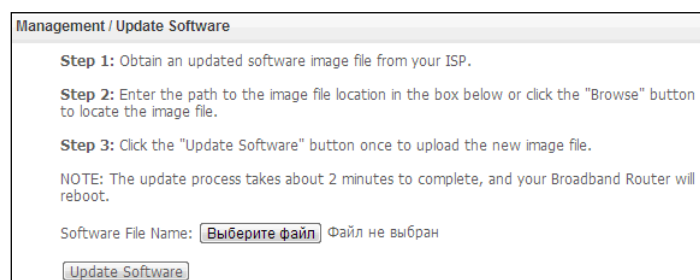
При выборе в выпадающем списке серверов значения *Other* справа станет активным окно для заполнения, куда следует вручную ввести адрес сервера точного времени.

4.14.4 Подменю *Update Software*. Обновление ПО

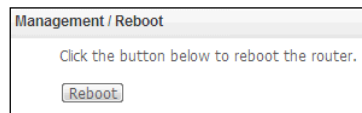
Для обновления ПО необходимо выбрать файл ПО в строке «*Software File name*» (используя кнопку «*Выберите файл*») и нажать «*Update Software*».



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

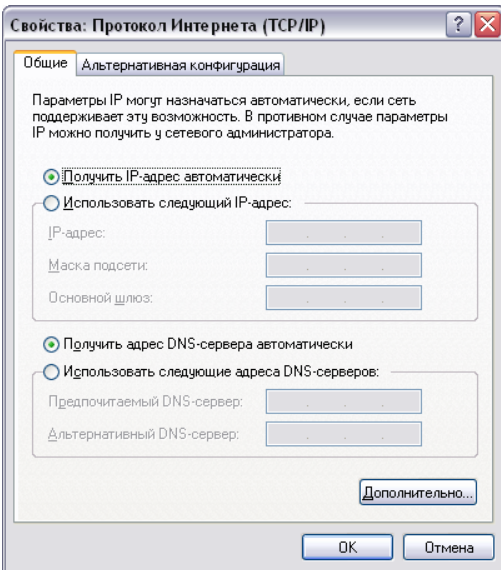


4.14.5 Подменю *Reboot*. Перезагрузка устройства



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
При вводе IP-адреса маршрутизатора (например, 192.168.1.1) не удается получить доступ к Web-интерфейсу	компьютер не принадлежит к данной IP-подсети для подключения к Web-интерфейсу.	В свойствах подключения к интернету на Вашем компьютере установите параметр «Получать IP-адрес автоматически». 
	на компьютере установлен Web-браузер с выключенной опцией Java-script	включите опцию Java-script в Вашем браузере или воспользуйтесь другим Web-браузером
	неисправный кабель	проверьте физическое соединение по статусу индикаторов (они должны гореть). Если индикаторы не горят, попробуйте использовать другой кабель или подключитесь к другому порту устройства, если это возможно. Если компьютер выключен, индикатор может не гореть.
	доступ запрещен программным обеспечением интернет-безопасности Вашего компьютера	отключите программное обеспечение интернет-безопасности на компьютере (брандмауэры)
Воспроизводится сигнал ошибки в телефоне, подключенном к порту FXS	Неверные настройки порта	проверьте корректность настроек в меню «VoIP» (см. 4.4 Меню VoIP.SIP Advanced Setting. Дополнительные настройки SIP)
Утерян/не подходит пароль доступа к WEB-интерфейсу устройства	_____	Необходимо сбросить маршрутизатор к настройкам по умолчанию с помощью кнопки F на задней панели устройства. К сожалению, при этом все выполненные настройки будут утрачены.

ПРИЛОЖЕНИЕ Б. ИСПОЛЬЗОВАНИЕ ДОПОЛНИТЕЛЬНЫХ УСЛУГ

1. Уведомление о поступлении нового вызова – Call Waiting

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

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

Доступ к услуге устанавливается через меню настроек абонентского порта на странице «VoIP/SIP Advanced Setting» (**раздел Ошибка! Источник ссылки не найден. Ошибка! Источник ссылки не найден.**) путем установки флага «Call waiting».

Использование услуги:

Находясь в состоянии разговора и при получении индикации о поступлении нового вызова, нажав R, возможно принять ожидающий вызов с установкой текущего соединения на удержание. Последующие нажатия R обрабатываются в соответствии с алгоритмами, описанными в разделе **2 Передача вызова – Calltransfer** 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 «*VoIP/SIP Advanced Setting*» (**раздел Ошибка! Источник ссылки не найден. Ошибка! Источник ссылки не найден.**) установить флаг в поле «*MWI*» для требуемого порта.

5. Запрет на исходящие вызовы – Call Barring

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

Доступ к услуге осуществляется через меню настроек абонентского порта на странице «*VoIP/SIP Advanced Setting*» (**раздел 4.4 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 mode* = 0, все исходящие звонки разрешены
- *Call barring mode* = 1, все исходящие звонки запрещены
- *Call barring mode* = 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 NTP-RG-1402_____ rev.C зав. № _____ соответствует требованиям технических условий ТУ6650-083-33433783-2012 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.

