



Абонентские оптические терминалы

NTU-RG-5402G-W

NTU-RG-5421G-Wac

NTU-RG-5421G-WZ

Руководство по эксплуатации
Версия ПО 1.0.1

IP-адрес: 192.168.1.1

Username: user

Password: user

Содержание

1	Введение	4
2	Описание изделия	5
2.1	Назначение.....	5
2.2	Варианты исполнения	6
2.3	Характеристика устройства	6
2.4	Основные технические параметры.....	9
2.5	Конструктивное исполнение.....	12
2.6	Световая индикация.....	14
2.7	Индикация интерфейсов LAN	16
2.8	Перезагрузка/сброс к заводским настройкам	16
2.9	Комплект поставки	16
3	Архитектура устройства NTU-RG	17
4	Настройка устройств через Web-интерфейс. Доступ пользователя.....	18
4.1	Меню «Status». Информация об устройстве	19
4.1.1	Подменю «Device status». Общая информация об устройстве	19
4.1.2	Подменю «IPv6 Status». Информация о системе IPv6.....	20
4.1.3	Подменю «PON». Информация о статусе оптического модуля	20
4.1.4	Подменю «LAN». Настройка интерфейса LAN.	21
4.2	Меню «Wireless». Настройка беспроводной сети	21
4.2.1	Подменю «Basic settings». Основные настройки.....	21
4.2.2	Подменю «Advanced settings». Расширенные настройки.....	22
4.2.3	Подменю «Security». Настройка параметров безопасности.....	23
4.2.4	Подменю «Access control». Настройка доступа.....	24
4.2.5	Подменю «WiFi radar». Сканирование беспроводной сети	25
4.2.6	Подменю «WPS». Автоматическая настройка беспроводной сети	25
4.3	Меню «Service». Настройка сервисов.....	26
4.3.1	Подменю «DHCP Setting». Настройка DHCP	26
4.3.2	Подменю «Dynamic DNS». Настройки динамической системы доменных имен.....	27
4.3.3	Подменю «Firewall». Настройка брандмауэра.....	28
4.3.4	Подменю «UPnP». Автоматическая настройка сетевых устройств	32
4.3.5	Подменю «RIP». Настройка RIP	33
4.3.6	Подменю «Samba». Настройка пользователей Samba	33
4.4	Меню «Advance»	34

4.4.1	Подменю «ARP Table». Просмотр кэша протокола ARP	34
4.4.2	Подменю «Bridging». Настройка параметров Bridging	34
4.4.3	Подменю «Routing». Настройка маршрутизации	35
4.4.4	Подменю «Bridging grouping». Объединение интерфейсов в группы	35
4.4.5	Подменю «Link mode». Настройка LAN-портов	36
4.4.6	Подменю «IPv6». Настройка протокола IPv6	37
4.5	Подменю «Diagnostics»	39
4.5.1	Подменю «Ping». Проверка доступности сетевых устройств.....	39
4.6	Подменю «Admin»	40
4.6.1	Подменю «Commit/Reboot». Сохранение изменений и перезагрузка устройства	40
4.6.2	Подменю «Backup/Restore». Восстановление и сброс настроек.....	40
4.6.3	Подменю «Password». Настройка контроля доступа (установление паролей)	41
4.6.4	Подменю «Firmware upgrade». Обновление ПО	41
4.6.5	Подменю «Time zone». Настройки системного времени	42
4.7	Меню «Statistics». Информация о прохождении трафика на портах устройства.....	43
4.7.1	Подменю «Interface»	43
4.7.2	Подменю «PON»	43
4.8	Меню «Z-Wave». Для устройства NTU-RG-5421G-WZ.....	44
5	Список изменений	45

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 Гбит/с в направлении downlink и 1.25 Гбит/с в направлении uplink. Использование в сетях доступа решений на базе технологии GPON дает возможность предоставлять конечному пользователю доступ к новым услугам на базе протокола IP совместно с традиционными сервисами.

Основным преимуществом GPON является использование одного стационарного 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. Устройство ONT предназначено для подключения к услугам широкополосного доступа оконечного оборудования клиентов. Может применяться в жилых комплексах и бизнес-центрах.

Линейка оборудования ONT NTU производства «ЭЛТЕКС» представлена терминалами, которые рассчитаны на четыре UNI интерфейса 10/100/1000Base-T и поддержку интерфейсов FXS, Wi-Fi, USB, Z-Wave¹:

- NTU-RG-5402G-W, NTU-RG-5421G-Wac, NTU-RG-5421G-WZ

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

¹ Для устройства NTU-RG-5421G-WZ.

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, принести к некорректной работе устройства или потере данных.

2 Описание изделия

2.1 Назначение

Устройства NTU-RG GPON ONT (Gigabit Ethernet Passive Optical Network) – высокопроизводительные абонентские терминалы, предназначенные для связи с вышестоящим оборудованием пассивных оптических сетей и предоставления услуг широкополосного доступа конечному пользователю. Связь с сетями GPON реализуется посредством PON-интерфейса, для подключения оконечного оборудования клиентов служат интерфейсы Ethernet.

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

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

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

Абонентский маршрутизатор NTU-RG-5402G-W, поддерживает подключение по Wi-Fi стандарта b/g/n и позволяет обеспечить работу устройства в частотном диапазоне – 2,4 ГГц. В свою очередь абонентские маршрутизаторы NTU-RG-5421G-Wac, NTU-RG-5421G-WZ позволяют подключать клиентов Wi-Fi по стандарту IEEE 802.11a/b/g/n/ac. Поддержка стандарта 802.11ac обеспечивает скорость передачи данных до 1,3 Гбит/с и позволяет доставлять современные высокоскоростные сервисы клиентскому оборудованию по беспроводной сети. Два встроенных контроллера Wi-Fi сети позволяют обеспечить работу устройства одновременно в двух частотных диапазонах – 2,4 ГГц и 5 ГГц.

Устройство NTU-RG-5421G-WZ в своей комплектации имеет контроллер "Умный дом".

Контроллер "Умный дом" позволяет организовать беспроводной радиоканал с низким энергопотреблением специально для дистанционного управления. В отличие от Wi-Fi и других IEEE 802.11 стандартов передачи данных, предназначенных в основном для больших потоков информации, технология "Умный дом" работает в диапазоне частот до 1 ГГц и оптимизирована для передачи простых управляющих команд с малыми задержками (например, включить/выключить, изменить громкость, яркость и т.д.). Выбор низкого радиочастотного диапазона

обусловлен малым количеством потенциальных источников помех (в отличие от загруженного диапазона 2,4 ГГц, в котором приходится прибегать к мероприятиям, уменьшающим возможные помехи от работающих различных бытовых беспроводных устройств – Wi-Fi, ZigBee, Bluetooth).

Контроллер "Умный дом" предназначен для создания недорогой и энергоэффективной потребительской электроники, в том числе устройств на батарейках, таких как пульты дистанционного управления, датчики дыма, температуры, влажности, движения и других датчиков безопасности.

2.2 Варианты исполнения

Устройства серий NTU-RG отличаются набором интерфейсов и функциональными возможностями, таблица 1.

Таблица 1 – Варианты исполнения

Наименование модели	WAN	LAN	FXS	Z-Wave	RF	Wi-Fi	USB
NTU-RG-5402G-W	1xGPON	4x1Gigabit	2	-	-	802.11n, 2*2 - 300 Мбит/с – 2,4 ГГц	1
NTU-RG-5421G-Wac	1xGPON	4x1Gigabit	1	-	-	802.11n, 2*2 - 300 Мбит/с – 2,4 ГГц 802.11ac 2*2 - 866 Мбит/с – 5 ГГц	1
NTU-RG-5421G-WZ	1xGPON	4x1Gigabit	1	1	-	802.11n, 2*2 - 300 Мбит/с – 2,4 ГГц 802.11ac 2*2 - 866 Мбит/с – 5 ГГц	1

2.3 Характеристика устройства

Устройство имеет следующие интерфейсы:

- Порты RJ-11 для подключения аналоговых телефонных аппаратов (FXS):
 - 2 порта в NTU-RG-5402G-W;
 - 1 порт в NTU-RG-5421G-Wac, NTU-RG-5421G-WZ.
- 1 порт PON SC/APC для подключения к сети оператора (WAN);
- Порты Ethernet RJ-45 LAN для подключения сетевых устройств (LAN):
 - 4 порта RJ-45 10/100/1000Base-T;
- Приемопередатчик Wi-Fi:
 - 802.11b/g/n в NTU-RG-5402G-W;
 - 802.11a/b/g/n/ac в NTU-RG-5421G-Wac, NTU-RG-5421G-WZ.
- 1 порт USB2.0 для подключения внешних накопителей USB или HDD;
- Контроллер "Умный дом", входит в состав NTU-RG-5421G-WZ.

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

Устройство поддерживает следующие функции:

- *Сетевые функции:*
 - работа в режиме «моста» или «маршрутизатора»;
 - поддержка PPPoE (auto, PAP, CHAP, MSCHAP-авторизация);
 - поддержка IPoE (DHCP-client и static);
 - поддержка статического адреса и DHCP (DHCP-клиент на стороне WAN, DHCP-сервер на стороне LAN);
 - передача Multicast трафика по Wi-Fi;
 - поддержка DNS (Domain Name System)
 - поддержка DynDNS (Dynamic DNS)
 - поддержка UPnP (Universal Plug and Play);
 - поддержка IPsec (IP Security);
 - поддержка NAT (Network Address Translation);
 - поддержка Firewall;
 - поддержка NTP (Network Time Protocol);
 - поддержка механизмов качества обслуживания QoS;
 - поддержка IGMP-snooping;
 - поддержка IGMP-proxy;
 - поддержка функции Parental Control;
 - поддержка функции Storage service;
 - поддержка SMB, FTP, Print Server;
 - VLAN в соответствии с IEEE 802.1Q.
- *Wi-Fi:*
 - поддержка стандартов 802.11a/b/g/n/ac;
 - одновременная работа в двух диапазонах: 2.4ГГц и 5ГГц.
- *IP-телефония:*
 - поддержка протокола SIP;
 - аудиокодеки: G.729 (A), G.711(A/U), G.723.1;
 - ToS для пакетов RTP;
 - ToS для пакетов SIP;
 - эхо компенсация (рекомендации G.164, G.165);
 - обнаружение голосовой активности (VAD);
 - генератор комфортного шума (CNG);
 - обнаружение и генерирование сигналов DTMF;
 - передача DTMF (INBAND, RFC2833, SIP INFO);
 - передача факса: G.711, T.38;
 - Выдача Caller ID
- *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, OMCI;
- удаленный мониторинг, конфигурирование и настройка:
 - TR-069;
 - Web-интерфейс;
 - OMCI;
 - Telnet.

На рисунках ниже приведены схемы применения оборудования NTU-RG.

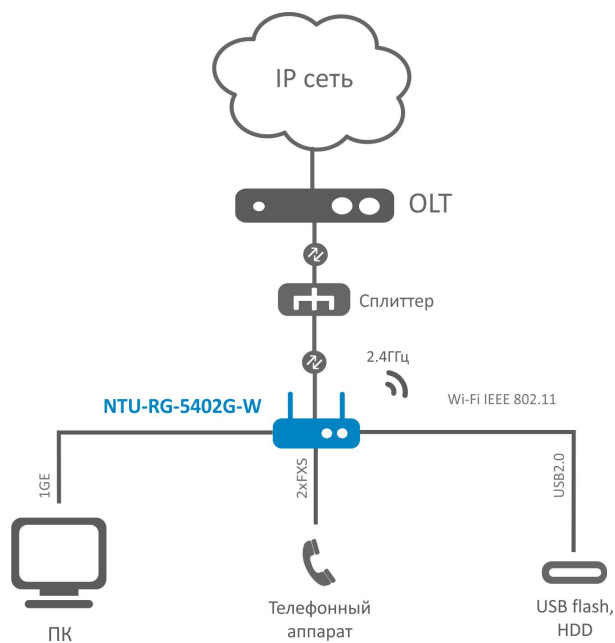


Рисунок 1 – Схема применения NTU-RG-5402G-W

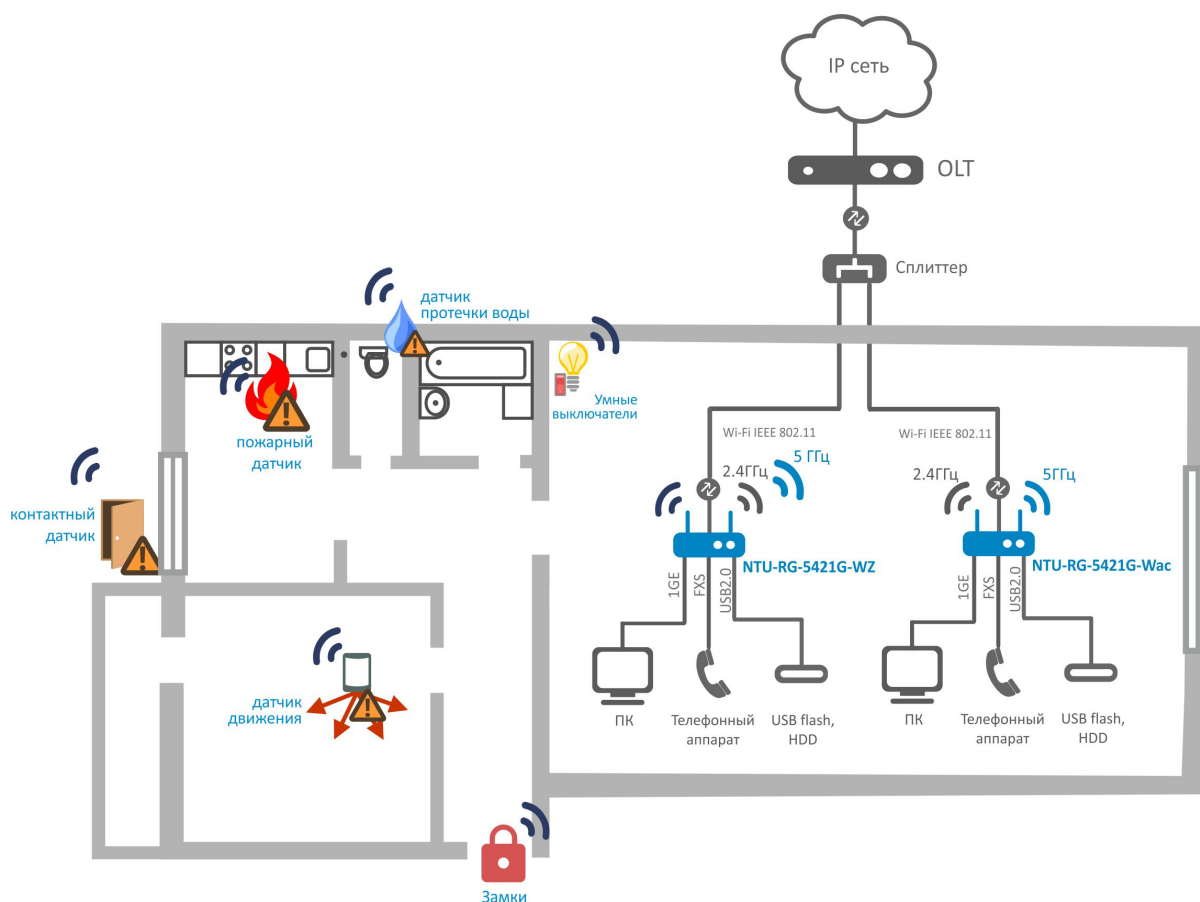


Рисунок 2 – Схема применения NTU-RG-5421G-Wac и NTU-RG-5421G-WZ

2.4 Основные технические параметры

Основные технические параметры терминалов 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	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, ITU-T G.984.5 Filter, FSAN Class B+, SFF-8472
Среда передачи	Оптоволоконный кабель SMF - 9/125, G.652
Коэффициент разветвления	До 1:128
Максимальная дальность действия	20 км
Передатчик:	1310 Нм
• Скорость соединения upstream	1244 Мбит/с
• Мощность передатчика	+0,5 до +5 дБм
• Ширина спектра оптического излучения (RMS)	1 Нм
Приемник:	1490 Нм
• Скорость соединения downstream	2488 Мбит/с
• Чувствительность приемника	от -8 до -28, BER \leq 1.0x10 ⁻¹⁰
Оптическая перегрузка приемника	-4 дБм

Параметры аналоговых абонентских портов

Количество портов	NTU-RG-5402G-W	NTU-RG-5421G-Wac NTU-RG-5421G-WZ
	2	1
Сопротивление шлейфа	До 2 кОм	
Прием выбора	Импульсный/частотный (DTMF)	
Выдача Caller ID	Есть	

Параметры беспроводного интерфейса Wi-Fi

Модель	NTU-RG-5402G-W	NTU-RG-5421G-Wac NTU-RG-5421G-WZ
Стандарт	802.11 b/g/n	802.11 a/b/g/n/ac
Частотный диапазон	2400 ~ 2483,5 МГц	2400 ~ 2483,5 МГц, 5150 ~ 5350 МГц, 5650 ~ 5850 МГц Одновременная работа в двух частотных диапазонах (Simultaneous Dual Band)
Модуляция	ССК, BPSK, QPSK, 16 QAM, 64 QAM, 256 QAM	ССК, BPSK, QPSK, 16 QAM, 64 QAM, 256 QAM
Скорость передачи данных, Мбит/с	– 802.11b/g/n: 1-13 – 802.11b: 1; 2; 5,5 и 11 Мбит/с – 802.11g: 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с – 802.11n: от 6,5 до 300 Мбит/с (от MCS0 до MCS15)	– 802.11b/g/n: 1-13 – 802.11b: 1; 2; 5,5 и 11 Мбит/с – 802.11g: 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с – 802.11ac: 866 Мбит/с (80 МГц)
Максимальная выходная мощность передатчика	– 802.11b (11 Mbps): 17дБм – 802.11g (54 Mbps): 15дБм – 802.11n (MCS7): 15 дБм	– 802.11b (11 Mbps): 17 дБм – 802.11g (54 Mbps): 15 дБм – 802.11n (MCS7): 15 дБм – 802.11ac (MCS0): 19 дБм
MAC-протокол	CSMA/CA модель ACK 32 MAC	
Безопасность	64/128-битное WEP-шифрование данных; WPA, WPA2 802.1x AES & TKIP	
MIMO	2,4 ГГц- 2x2	2,4 ГГц- 2x2, 5 ГГц - 3x3
Коэффициент усиления антенны	5 дБи	

Рабочий диапазон температур	от +5 до +40°C
-----------------------------	----------------

Управление

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

Общие параметры

Питание	Адаптер питания 12В DC /220 AC
Потребляемая мощность	Не более 15 Вт
Рабочий диапазон температур	От +5 до +40°C
Относительная влажность	До 80%
Габариты	187x120x32 мм
Масса	0,3 кг

2.5 Конструктивное исполнение

Абонентский терминал выполнен в виде настольного изделия в пластиковом корпусе.

Внешний вид задней панели устройств приведены на рисунках 3, 4.

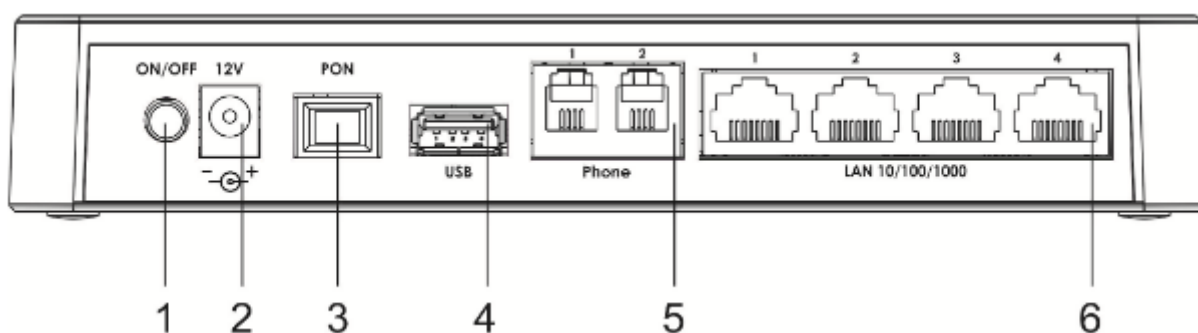


Рисунок 3 – Внешний вид задней панели NTU-RG-5402G-W

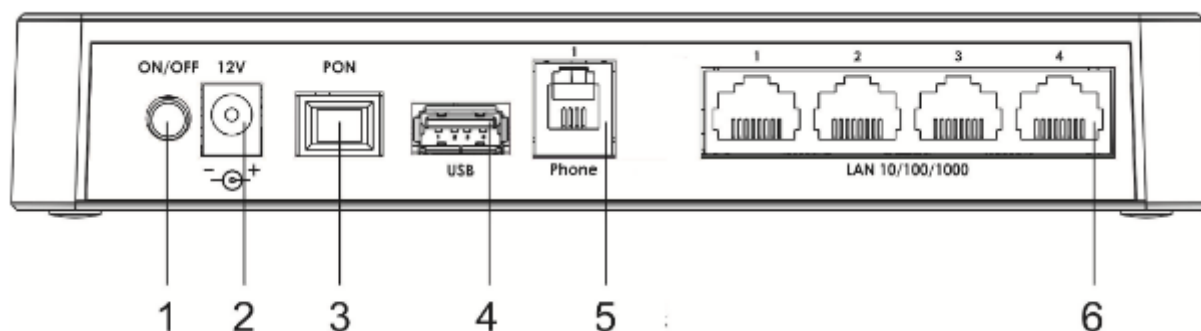


Рисунок 4 – Внешний вид задней панели NTU-RG-5421G-Wac и NTU-RG-5421G-WZ

На задней панели устройства расположены следующие разъемы и органы управления, таблица 3.

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	Разъем для подключения внешних накопителей и других USB-устройств
5	Phone	Разъем RJ-11 для подключения аналогового телефонного аппарата: <ul style="list-style-type: none"> • 2 разъема в NTU-RG-5402G-W • 1 разъем в NTU-RG-5421G-Wac и NTU-RG-5421G-WZ
6	LAN 10/100/1000 1..4	4 разъема RJ-45 для подключения сетевых устройств

Внешний вид боковой панели NTU-RG приведен на рисунке ниже.

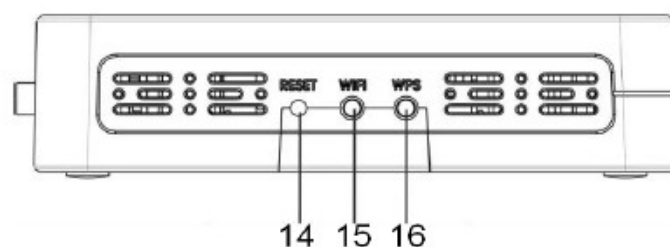


Рисунок 5 – Внешний вид боковой панелей NTU-RG

На боковой панели устройства расположены следующие кнопки, таблица 4.

Таблица 4 – Описание кнопок боковой панели

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

2.6 Световая индикация

Внешний вид верхних панелей NTU-RG-5402G-W, NTU-RG-5421G-Wac, NTU-RG-5421G-WZ приведены на рисунке 6.

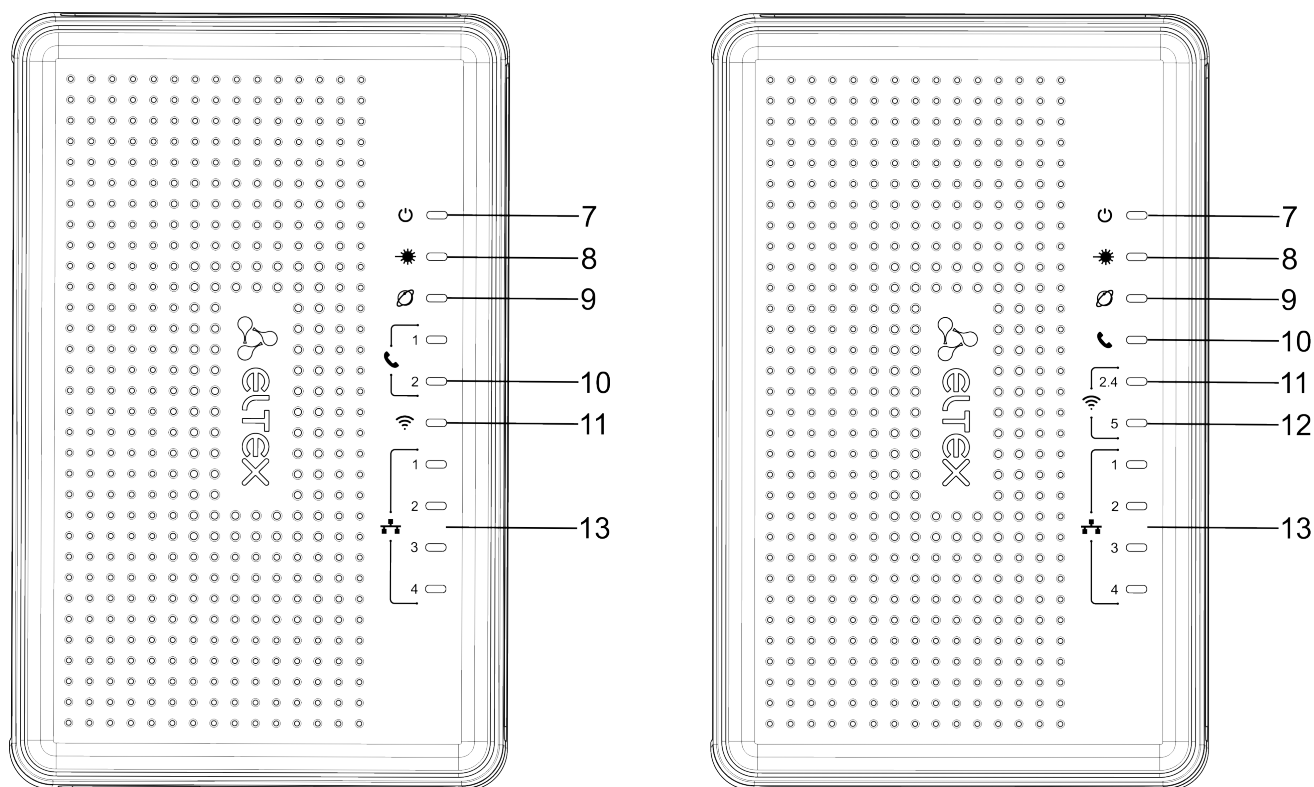








Рисунок 6 – Внешний вид верхних панелей NTU-RG-5402G-W (слева) и NTU-RG-5421G-Wac, NTU-RG-5421G-WZ (справа)

Текущее состояние устройства отображается при помощи индикаторов, расположенных на верхней панели. Перечень состояний индикаторов приведен в таблице 5.

Таблица 5 – Описание индикаторов верхней панели

№	Элемент верхней панели	Состояние индикатора	Описание
7	 – индикатор питания и статуса работы	не горит	устройство отключено от сети питания или неисправно
		красный	в процессе загрузки
		зелёный	процесс загрузки завершен, на устройстве установлена конфигурация, отличная от конфигурации по-умолчанию
		оранжевый	процесс загрузки завершен, на устройстве установлена конфигурация по-умолчанию
8	 – индикатор работы оптического интерфейса	не горит	процесс загрузки устройства
		зелёный	установлено соединение между стационарным оптическим терминалом и устройством
		мигает зелёным	установлено соединение между стационарным оптическим терминалом и устройством, устройство не активировано
		мигает красным	нет сигнала от стационарного оптического терминала
9	 – индикатор статус	не горит	интерфейс с признаком Интернет не сконфигурирован / отсутствует связь с OLT
		зелёный	устройство готово к работе, установлено соединение с интернетом
		мигает зелёным	идет процесс обновления ПО на устройстве
10	 – индикатор активности порта FXS	не горит	SIP агент не настроен / не зарегистрирован / выключен
		горит	SIP агент успешно зарегистрирован
		мигает	при снятой трубке/разговоре
11	 – индикатор активности Wi-Fi в диапазоне 2.4 ГГц	зелёный	сеть Wi-Fi активна
		мигает	процесс передачи данных по Wi-Fi
		не горит	сеть Wi-Fi не активна
12	 – индикатор активности Wi-Fi в диапазоне 5 ГГц	зелёный	сеть Wi-Fi активна
		мигает	процесс передачи данных по Wi-Fi
		не горит	сеть Wi-Fi не активна

№	Элемент верхней панели	Состояние индикатора	Описание
13	✚ 1..4 – индикаторы работы Ethernet-портов	зелёный	установлено соединение 10/100 Мбит/с
		оранжевый	установлено соединение 1000 Мбит/с
		мигает	процесс пакетной передачи данных


2.7 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	не горит
Порт работает в режиме 1000Base-T, есть передача данных	мигает	не горит
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

2.8 Перегрузка/сброс к заводским настройкам

Для перезагрузки устройства нужно однократно нажать кнопку «Reset» на боковой панели изделия. Для загрузки устройства с заводскими настройками необходимо нажать и удерживать кнопку «Reset» 7-10 секунд, пока индикатор  не загорится красным светом и не погаснут все индикаторы. При заводских установках IP-адрес: LAN - 192.168.1.1, маска подсети – 255.255.255.0. Доступ возможен с портов LAN 1, LAN 2, LAN 3 и LAN 4.

2.9 Комплект поставки

В базовый комплект поставки устройства NTU-RG входят:

- Абонентский оптический терминал NTU-RG;
- Адаптер питания 220/12;
- Руководство по эксплуатации.

3 Архитектура устройства NTU-RG

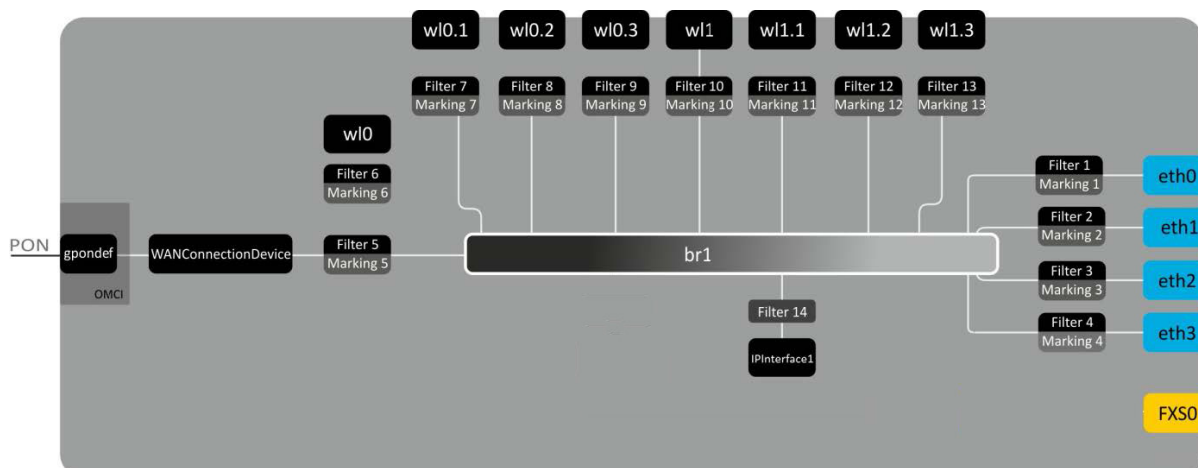


Рисунок 7 – Логическая архитектура устройства с заводской конфигурацией

Основные элементы устройства:

- **Оптический приемо-передатчик (SFF-модуль)** – предназначен для преобразования оптического сигнала в электрический;
- **Процессор (PON-чип)** – является конвертором интерфейсов Ethernet и GPON;
- **Wi-Fi модули** – предназначены для организации беспроводных интерфейсов на устройстве.

При заводской (начальной) конфигурации в устройстве присутствуют следующие логические блоки (рисунок 7):

- Br0;
- Voice (блок IP телефонии);
- eth0...3;
- FXS0;
- wI0, wI0.1..wI0.3, wI1, wI1.1..wI1.3;
- IPInterface.

Блок br0 в данном случае 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**.

Блок FXS0 физически является портом с разъемом RJ-11 для подключения аналогового телефонного аппарата. Логически включен в блок Voice. Управление блоком Voice может осуществляться через Web-интерфейс, а также удаленно с помощью сервера ACS по стандарту TR-069. В данном блоке задаются параметры сервиса VoIP (адрес SIP-сервера, номер телефонного аппарата, услуги ДВО и т. д.).

Блоки wI0, wI0.1...wI1.3 являются интерфейсами для подключения Wi-Fi-модулей. Блоки wI0 являются интерфейсами для работы в диапазоне 2.4ГГц, блоки wI1 – в диапазоне 5ГГц.

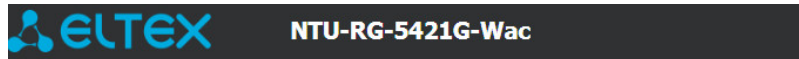
Блоки Filter и Marking предназначены для включения локальных интерфейсов в одну группу (в блок **br0**). Отвечают за правила прохождения трафика, блоки **Filter** отвечают за входящий трафик на интерфейсе, блоки **Marking** – за исходящий.

Блок IPInterface представляет собой некий логический объект, на котором располагается IP-адрес для доступа в локальной сети, а также сервер DHCP, раздающий адреса клиентам.

4 Настройка устройств через Web-интерфейс. Доступ пользователя.

Для того чтобы произвести конфигурирование устройства, необходимо подключиться к нему через Web-браузер (программу для просмотра гипертекстовых документов), например, Firefox, Google Chrome и т.д. 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.



Authorization

User name

Password

Имя пользователя **user**, пароль **user**.

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

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

The screenshot shows the web interface for the ELTEX NTU-RG-5421G-Wac device. The top header includes the ELTEX logo, the device model, and a user profile for 'user' with a 'Logout' button. A navigation menu on the left lists various system settings. The main content area displays the 'Device Status' page, which includes a 'System' table with details like Board Type, Serial Number, and Uptime. Below this are 'LAN Configuration' and 'WAN Configuration' tables. A 'Refresh' button is located at the bottom of the WAN configuration section.

System	
Board Type	NTU-RG-5421G-Wac
Serial Number	GP3A000093
PON Serial	454C545873000120
Base WAN MAC	E0D9E385A498
Hardware Version	1v1
Uptime	18 min
Date/Time	Thu Jan 1 00:17:59 1970
Image 1 Firmware Version (Active)	1.0.1.24
Image 2 Firmware Version	1.0.1.24
CPU Usage	0%
Memory Usage	12%
Name Servers	
IPv4 Default Gateway	
IPv6 Default Gateway	

LAN Configuration	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	e0d9e385a498

WAN Configuration							
Interface	VLAN ID	MAC	Connection Type	Protocol	IP Address	Gateway	Status

4.1 Меню «Status». Информация об устройстве

4.1.1 Подменю «Device status». Общая информация об устройстве

Status → *Device status*

Device Status

This page shows the current status and some basic settings of the device.

System

Board Type	NTU-RG-5421G-Wac
Serial Number	GP3A000093
PON Serial	454C545873000120
Base WAN MAC	E0D9E385A498
Hardware Version	1v1
Uptime	24 min
Date/Time	Thu Jan 1 00:24:32 1970
Image 1 Firmware Version (Active)	1.0.1.24
Image 2 Firmware Version	1.0.1.24
CPU Usage	0%
Memory Usage	12%
Name Servers	
IPv4 Default Gateway	
IPv6 Default Gateway	

LAN Configuration

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	e0d9e385a498

WANConfiguration

Interface	VLAN ID	MAC	Connection Type	Protocol	IP Address	Gateway	Status

Refresh

4.1.2 Подменю «IPv6 Status». Информация о системе IPv6

Во вкладке отображается текущий статус системы IPv6.

Status → IPv6

IPv6 Status

This page shows the current system status of IPv6.

LANConfiguration	
IPv6 Address	
IPv6 Link-Local Address	fe80::1/64

Prefix Delegation	
Prefix	

WANConfiguration					
Interface	VLAN ID	Connection Type	Protocol	IP Address	Status

Refresh

4.1.3 Подменю «PON». Информация о статусе оптического модуля

В данной вкладке показано текущее состояние системы PON-интерфейса.

Status → PON

PON Status

This page shows the current system status of PON.

PON Status	
Vendor Name	Ligent Photonics
Part Number	LTB3468-BC1
Temperature	38.417969 C
Voltage	3.257400 V
Tx Power	2.490033 dBm
Rx Power	-inf dBm
Bias Current	13.572000 mA

GPON Status	
ONU State	O1
ONU ID	255
LOID Status	Initial Status

Refresh

4.1.4 Подменю «LAN». Настройка интерфейса LAN.

В данном подменю доступен просмотр и настройка основных характеристик проводных и беспроводных интерфейсов LAN.

Status → *LAN*

LAN Interface Settings

This page is used to configure the LAN interface of your Device. Here you may change the setting for IP addresses, subnet mask, etc..

InterfaceName:	br0
IP Address:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
IPv6 Address Mode:	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
IPv6 Address:	<input type="text" value="::"/>
IPv6 Prefix Length:	<input type="text" value="0"/>
IP Version:	IPv4/IPv6 ▾
Firewall:	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
IGMP Snooping:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Ethernet to Wireless Blocking:	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Mac Based Tag Decision:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled

4.2 Меню «Wireless». Настройка беспроводной сети

Настройки в данном меню производятся отдельно для рабочих диапазонов 2.4 ГГц и 5 ГГц.

4.2.1 Подменю «Basic settings». Основные настройки

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

Wireless → *wlan0 (2.4GHz)* / *wlan1 (5GHz)* → *Basic settings*

WLAN Basic Settings

This page is used to configure the parameters for WLAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

<input type="checkbox"/> Disable WLAN Interface	
Band:	2.4 GHz (B+G+N) ▾
Mode:	AP ▾ <input type="button" value="Multiple AP"/>
SSID:	<input type="text" value="ELTX-2.4GHz_WIFI_A498"/>
Channel Width:	40MHz ▾
Control Sideband:	Upper ▾
Channel Number:	Auto ▾
Radio Power (%):	100% ▾
Limit Associated Client Number:	Disabled ▾ <input type="text"/>
Associated Clients:	<input type="button" value="Show Active WLAN Clients"/>
<input type="checkbox"/> Enable Universal Repeater Mode (Acting as AP and client simultaneously)	
Regdomain:	RUSSIAN(12) ▾

- *Disable WLAN Interface* – отключает радиointерфейс;

- *Band* – меняет стандарт работы Wi-Fi;
- *Mode* – переключения режим работы "точка доступа" / "клиент";
- *SSID (Service Set Identifier)* – назначить имя беспроводной сети (ввод с учетом регистра клавиатуры);

✓ По умолчанию на устройстве установлено имя беспроводной сети (SSID) **ELTX-2.4GHz_WiFi-aaaa/ELTX-5GHz_WiFi-aaaa**, где **aaaa** - это 4 последние цифры **WAN MAC**. **WAN MAC** указан в наклейке на корпусе устройства. В имени сети фигурирует частотный диапазон (2.4/5ГГц).

- *Channel Width* – ширина полосы 20/40 MHz;
- *Control Sideband* – боковая полоса управления – выбор второго канала (Lower или Upper) в режиме 40 МГц;
- *Channel Number* – Используемый канал;
- *Radio Power* – мощность передатчика;
- *Limit Associated Client Number* – ограничить максимальное количество подключенных клиентов;
- *Associated Clients* – максимальное число подключенных клиентов;
- *Enable Universal Repeater Mode (Acting as AP and client simultaneouly)* – включает режим повторителя;
- *Regdomain* –

Для принятия изменений необходимо нажать кнопку «Apply Changes».

4.2.2 Подменю «Advanced settings». Расширенные настройки

В данном подменю производится расширенные настройки беспроводной сети.

Wireless → wlan0 (2.4GHz) / wlan1 (5GHz) → Advanced settings

WLAN Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about WLAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Fragment Threshold:	2346	(256-2346)
RTS Threshold:	2347	(0-2347)
Beacon Interval:	100	(20-1024 ms)
Data Rate:	Auto	
Preamble Type:	<input checked="" type="radio"/> Long Preamble	<input type="radio"/> Short Preamble
Broadcast SSID:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Relay Blocking:	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled
Protection:	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled
Aggregation:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Short GI:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
TX beamforming:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
MU MIMO:	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled
Multicast to Unicast:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
WMM Support:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled

Apply Changes

- *Fragment 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;
- *Beacon Interval*– период отправки информационного пакета в беспроводную сеть, сигнализирующего о том, что точка доступа активна;
- *Data rate* – скорость передачи;
- *Preamble Type* – выбор преамбулы - длинная / короткая;
- *Broadcast SSID* – вещание SSID;
- *Relay Blocking* – включает изоляцию клиентов;
- *Protection* – включает 802.11n protection;
- *Aggregation* – включить агрегацию кадров для повышения пропускной способности;
- *Short GI* – включение короткого защитного интервала;
- *TX beamforming* – адаптивное формирование диаграммы направленности;
- *Multicast to Unicast* – при включении переключает весь multicast трафик в unicast;
- *WMM Support* – поддержка Wi-Fi Multimedia.

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

4.2.3 Подменю «Security». Настройка параметров безопасности

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

Wireless → wlan0 (2.4GHz) / wlan1 (5GHz) → Security

WLAN Security Settings

This page allows you setup the WLAN security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID Type: Root AP - ELTX-5GHz_WiFi_A498 ▼

Encryption: WPA2 ▼

Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)

IEEE 802.11w: None Capable Required

SHA256: Disable Enable

WPA2 Cipher Suite: TKIP AES

Group Key Update Timer: 86400

Pre-Shared Key Format: Passphrase ▼

Pre-Shared Key: Show

Apply Changes

- *Encryption* – установить режим шифрования:
 - *NONE (открытый)* – защита беспроводной сети отсутствует;
 - *WEP* – для включения шифрования WEP выберите его в выпадающем списке;
- *802.1x Authentication* – включает стандарт 802.1x (позволяет пользователям аутентифицироваться с использованием сервера аутентификации RADIUS, для шифрования данных используется WEP-ключ);
- *Authentication* – аутентификация;
- *Key Length (степень шифрования)* – использование ключей длиной 64 или 128 бит;
- *Key Format (формат ключа)* – использовать формат ASCII или HEX;

- *Encryption Key (сетевой ключ)* – ключ из 10 символов в 16-ричной системе счисления, либо 5 символов ASCII1 для 64-х битного шифрования. Либо 26 символов в 16-ричной системе счисления, либо 13 символов ASCII для 128-х битного шифрования.
 - *RADIUS Server IP Address* – IP-адрес RADIUS-сервера;
 - *RADIUS Server Port* – номер порта RADIUS-сервера. По умолчанию установлен порт 1812;
 - *RADIUS Server Password* – секретный ключ для доступа к RADIUS-серверу;
 - *WPA / WPA2 / WPA2 Mixed*:
- *Authentication Mode* – режим аутентификации RADIUS или Personal (Pre-Shared Key):
- *WPA Cipher Suite* – набор шифров WPA;
- *Group Key Update Timer* – интервал обновления ключа;
- *Pre-Shared Key Format* – формат ключа ASCII или HEX;
- *Pre-Shared Key* – ключ доступа;
- *IEEE 802.11w* – включить шифрование служебных кадров;
- *SHA256* – включить использование SHA256.

4.2.4 Подменю «Access control». Настройка доступа

В данном подменю производится настройка фильтрации MAC-адресов.

Wireless → wlan0 (2.4GHz) / wlan1 (5GHz) → Access control

WLAN Access Control

If you choose 'Allowed Listed', only those WLAN clients whose MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these WLAN clients on the list will not be able to connect the Access Point.

Mode:

MAC Address: (ex. 00E086710502)

Current Access Control List:

MAC Address	Select

- *Mode* – выбор режима фильтрации по MAC-адресам:
 - *Disabled* – фильтр не используется;
 - *Allowed Listed* – фильтр по разрешенным адресам (белый список);
 - *Deny Listed* – фильтр по запрещенным адресам (черный список).
- *MAC-address* – поле для добавления MAC-адреса в таблицу фильтрации. Чтобы внести значение необходимо нажать «Add», для сброса значения кнопка «Reset».

Все добавленные MAC-адреса будут отображаться в *Current Access Control List* – текущий список контроля доступа. Для удаления выделенных позиций в списке нажмите «Delete Selected», чтобы удалить весь список нажмите «Delete All» .

4.2.5 Подменю «WiFi radar». Сканирование беспроводной сети

В данном подменю осуществляется сканирование беспроводной сети, тем самым происходит обнаружение ближайших точек доступа или IBSS.

Wireless → *wlan0 (2.4GHz)* / *wlan1 (5GHz)* → *WiFi radar*

WiFi Radar

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

SSID	BSSID	Channel	Type	Encryption	Signal(%)
ELTX-2.4GHz_WiFi_ODDB	a8:f9:4b:bd:0d:dd	13 (B+G+N)	AP	WPA2-PSK	64
ELTX-2.4GHz_WiFi_6A93	e0:d9:e3:88:6a:93	4 (B+G+N)	AP	WPA2-PSK	60
ELTX-2.4GHz_WiFi_6C3B	e0:d9:e3:88:6c:3b	3 (B+G+N)	AP	WPA2-PSK	52

Refresh

В таблице отображается следующая информация:

- *Channel* – канал;
- *Type* – тип (AP, Client - точка доступа, клиент);
- *Encryption* – шифрование;
- *Signal* – уровень сигнала.

Для сканирования эфира нажмите кнопку «Refresh».

4.2.6 Подменю «WPS». Автоматическая настройка беспроводной сети

В данном подменю производится настройка «WPS».

Wireless → *wlan0 (2.4GHz)* / *wlan1 (5GHz)* → *WPS*

Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your WLAN client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

Disable WPS

WPS Status: Configured UnConfigured

Auto-lock-down state: Unlocked

Self-PIN Number:

Push Button Configuration:

Current Key Info:

Authentication	Encryption	Key
WPA2 PSK	AES	GP3A000093

Client PIN Number:

Для сохранения изменений нажмите кнопку «Apply Changes», для сброса «Reset».

4.3 Меню «Service». Настройка сервисов

4.3.1 Подменю «DHCP Setting». Настройка DHCP

В данном подменю происходит настройка DHCP сервера и DHCP ретранслятора.

Services → *DHCP*

DHCP Settings

This page is used to configure DHCP Server and DHCP Relay.

DHCP Mode: NONE DHCP Relay DHCP Server

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

LAN IP Address: 192.168.1.1 **Subnet Mask:** 255.255.255.0

IP Pool Range: -

Subnet Mask:

Max Lease Time: seconds (-1 indicates an infinite lease)

DomainName:

Gateway Address:

DNS option: Use DNS Relay Set Manually

DHCP сервер на маршрутизаторе может работать в режиме сервера или ретранслятора

- *DHCP Mode* – выбор режима работы;
- *IP Pool Range* – диапазон адресов, выдаваемых клиентам;
- *Show Client* – кнопка для просмотра клиентов арендовавших адреса;
- *Subnet mask* – маска посети;
- *Max leas time* – максимальное время аренды, -1 для бесконечной аренды;
- *DomainName* – домен;
- *Gateway address* – адрес шлюза;
- *DNS option* – определяет работу DNS:
 - *Use DNS relay* – в качестве DNS будет выдан адрес ONT и все запросы будут ретранслироваться через ONT;
 - *Set manually* – установить DNS вручную.

Для сохранения изменений нажмите кнопку «*Apply Changes*». Кнопки «*Port-Based Filter*» и «*MAC-Based Assignment*» позволяют настроить фильтрацию по портам и MAC, соответственно.

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

Динамическая 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, маршрутизатору, например NTU-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.

Services → DNS → Dynamic DNS

Dynamic DNS Configuration

This page is used to configure the Dynamic DNS address from DynDNS.org or TZO or No-IP. Here you can Add/Remove to configure Dynamic DNS.

Enable:

DDNS Provider:

Hostname:

Interface:

DynDns/No-IP Settings:

UserName:

Password:

TZO Settings:

Email:

Key:

Dynamic DNS Table:

Select	State	Hostname	UserName	Service	Status
--------	-------	----------	----------	---------	--------

- *Enable* – при установленном флаге использовать DHCP-сервер (сетевые устройства будут получать IP-адреса динамически, из нижеприведенного диапазона);
- *D-DNS Provider* – выбор типа службы D-DNS (провайдера): DynDNS.org, TZO.com, No-IP.com
- *Custom* – иной провайдер, выбранный пользователем. В данном случае необходимо самостоятельно указать имя (*Hostname*) и адрес (*Interface*) провайдера.
- *DyDDns/No-IP Settings*:
 - *UserName* – имя пользователя;
 - *Password* – пароль авторизации на сервисе, выбранном для работы с D-DNS.

Во вкладке отображается таблица со списком имеющихся DNS. Для добавления записи необходимо нажать кнопку «Add», удаление происходит нажатием кнопки «Remove» напротив выбранной записи, изменение нажатием кнопки «Modify».

4.3.3 Подменю «Firewall». Настройка брандмауэра

4.3.3.1 Подменю «IP/Port Filtering». Настройки фильтрации адресов

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

Записи в этой таблице используются для ограничения определенных типов пакетов данных через шлюз. Использование таких фильтров может быть полезно для защиты или ограничения вашей локальной сети.

Services → Firewall → IP/Port Filtering

IP/Port Filtering

Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Default Action

Incoming Default Action
 Deny Allow

Outgoing Default Action
 Deny Allow

Protocol: <input type="text" value="TCP"/>	Rule Action <input checked="" type="radio"/> Deny <input type="radio"/> Allow	
Source IP Address: <input type="text"/>	Subnet Mask: <input type="text"/>	Port: <input type="text"/> - <input type="text"/>
Destination IP Address: <input type="text"/>	Subnet Mask: <input type="text"/>	Port: <input type="text"/> - <input type="text"/>
Ingress Interface: <input type="text" value="br0"/>		
<input type="button" value="Add"/>		

Current Filter Table:

Select	Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Ingress Interface	Rule Action
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>							

- *Incoming Default action* – действие по-умолчанию для входящих из-вне пакетов;
- *Outgoing Default action* – действие по-умолчанию для исходящих пакетов.

Для сохранения изменений нажмите кнопку «Apply Changes».

4.3.3.2 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.

Services → Firewall → MAC Filtering

MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Mode Whitelist BlackList

MAC Address:

Current Filter Table:

Select	MAC Address
<input type="checkbox"/>	

- *Mode* – выбор типа ограничения *Whitelist* (список разрешённых MAC-адресов) или *Blacklist* (список запрещённых MAC-адресов);
- *MAC Address* – MAC-адрес для которого вводится ограничение/доступ.

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

Во вкладке отображается таблица с ограничениями по MAC-адресам. Для удаления определённого ограничения, выделите позицию и нажмите кнопку «Delete Selected», для удаления всех ограничений кнопку «Delete All».

4.3.3.3 Подменю «Port Forwarding». Настройка проброса портов

Записи в этой таблице позволяют автоматически перенаправлять общие сетевые службы на конкретный компьютер за брандмауэром NAT. Эти настройки необходимы только в том случае, если вы хотите разместить какой-либо хост, например веб-сервер или почтовый сервер, в частной локальной сети за брандмауэром NAT вашего маршрутизатора.

Services → Firewall → Port Forwarding

Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Port Forwarding: Disable Enable

Enable Application: Active Worlds

Comment	Local IP	Local Port from	Local Port to	Protocol	Remote Port from	Remote Port to	Interface	NAT loopback
				Both			Any	<input type="checkbox"/>
				Both			Any	<input type="checkbox"/>
				Both			Any	<input type="checkbox"/>
				Both			Any	<input type="checkbox"/>
				Both			Any	<input type="checkbox"/>
				Both			Any	<input type="checkbox"/>
				Both			Any	<input type="checkbox"/>
				Both			Any	<input type="checkbox"/>
				Both			Any	<input type="checkbox"/>
				Both			Any	<input type="checkbox"/>
				Both			Any	<input type="checkbox"/>
				Both			Any	<input type="checkbox"/>
				Both			Any	<input type="checkbox"/>
				Both			Any	<input type="checkbox"/>
				Both			Any	<input type="checkbox"/>
				Both			Any	<input type="checkbox"/>

Current Port Forwarding Table:

Select	Comment	Local	IP Address	Protocol	Local Port	Enable	Remote Host	Public Port	Interface	NAT loopback
<input type="checkbox"/>										

- *Application* – в меню имеются предустановки для проброса портов различных приложений;
- *Comment* – комментарий;
- *Local IP* – локальный IP-адрес, на который производится проброс;
- *Local port from / to* – укажите диапазон портов локального устройства для проброса;
- *Protocol* – выбор протокола;
- *Remote port from / to* – укажите начальный порт входящего соединения. Поле *Remote port to* заполнится автоматически;
- *Interface* – выбор интерфейса;
- *NAT-loopback* – петля NAT позволяет "заворачивать" запросы из локальной сети на маршрутизатор, таким образом, например, можно проверить работу созданных правил.

Ниже расположена текущая таблица переадресации портов. Для удаления выделенной позиции нажмите кнопку «Delete Selected», для удаления всей таблицы кнопку «Delete All».

4.3.3.4 Подменю «URL Blocking». Настройки ограничения доступа в интернет

Фильтр URL – функция полноценного анализа и контроля доступа к определённым ресурсам сети интернет. В данном разделе задается список запрещенных/разрешенных URL-адресов для посещения. Здесь вы можете добавлять / удалять FQDN и фильтровать по ключевым словам.

Services → Firewall → URL Blocking

URLBlocking

This page is used to configure the Blocked FQDN(Such as tw.yahoo.com) and filtered keyword. Here you can add/delete FQDN and filtered keyword.

URL Blocking: Disable Enable

FQDN:

URL Blocking Table:

Select	FQDN
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>	

Keyword:

Keyword Filtering Table:

Select	Filtered Keyword
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>	

- *URL Blocking Enable / Disable* – включает / выключает работу URL-Blocking;
- *FQDN (Fully Qualified Domain Name)* – полное доменное имя;
- *Keyword* – ключевое слово.

4.3.3.5 Подменю «Domain Blocking». Настройка блокировки доменов

Это страница используется для задания блокировки доменов.

Services → Firewall → Domain blocking

Domain BlockingConfiguration

This page is used to configure the Blocked domain. Here you can add/delete the blocked domain.

Domain Blocking: Disable Enable

Domain:

Domain BlockingConfiguration:

Select	Domain
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>	

- *Domain Blocking Enable / Disable* – включает / выключает блокировку;

Для сохранения изменений используйте кнопку «Apply Changes». Чтобы заблокировать домен заполните поле *Domain* и нажмите кнопку «Add». Все заблокированные домены приведены в таблице ниже во вкладке, для удаления всей таблицы используйте кнопку «Delete All», для удаления одной позиции выделите её и нажмите кнопку «Delete Selected».

4.3.3.6 Подменю «DMZ». Настройки демилитаризованной зоны

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

Services → *Firewall* → *DMZ*

DMZ Configuration

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DMZ Host: Disable Enable

DMZ Host IP Address:

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

4.3.4 Подменю «UPnP». Автоматическая настройка сетевых устройств

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

Services → *UPnP*

UPnP Configuration

This page is used to configure UPnP. The system acts as a daemon when you enable it and select WAN interface (upstream) that will use UPnP.

UPnP: Disable Enable

WAN Interface:

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

Для включения UPnP необходимо установить флаг «Enable».

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

4.3.5 Подменю «RIP». Настройка RIP

Включите RIP, если вы используете это устройство в качестве устройства с поддержкой RIP для связи с другими пользователями с использованием протокола динамической маршрутизации RIP. Эта страница используется для выбора интерфейсов на вашем устройстве, которые используют RIP и версию используемого протокола.

Services → *RIP*

RIP Configuration

Enable the RIP if you are using this device as a RIP-enabled Device to communicate with others using the Routing Information Protocol. This page is used to select the interfaces on your device that use RIP, and the version of the protocol used.

RIP: Disable Enable

Interface:

Receive Mode:

Send Mode:

RIP Config Table:

Select	Interface	Receive Mode	Send Mode
<input type="checkbox"/>			

Для использования протокола динамической маршрутизации RIP установить флаг «*Enable*».

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

- *Interface* – интерфейс, на котором будет запускаться RIP;
- *Receive Mode* – режим обработки входящих пакетов (NONE, RIP1, RIP2, both);
- *Send Mode* – режим отправки (NONE, RIP1, RIP2, RIP1 compat).

4.3.6 Подменю «Samba». Настройка пользователей Samba

В данном подменю происходит настройка Samba, для включения настройки установите флаг «*Enable*».

Services → *Samba*

SambaConfiguration

This page let user to config Samba.

Samba : Disable Enable

Server String :

4.4 Меню «Advance»

4.4.1 Подменю «ARP Table». 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.

Advance → *ARP table*

User List

This table shows a list of learned MAC addresses.

IP Address	MAC Address
192.168.1.15	ec-08-6b-05-c5-33

Refresh

- *IP Address* – IP-адрес клиента;
- *MAC Address* – MAC-адрес клиента.

Для обновления информации нажмите кнопку «Refresh».

4.4.2 Подменю «Bridging». Настройка параметров Bridging

На данной странице можно настроить время жизни адресов в MAC-таблице а также включить 802.1d Spanning Tree.

Advance → *Bridging*

BridgingConfiguration

This page is used to configure the bridge parameters. Here you can change the settings or view some information on the bridge and its attached ports.

Ageing Time: (seconds)

802.1d Spanning Tree: Disabled Enabled

Apply Changes

Show MACs

- *Ageing Time* – время жизни адресов (сек);
- *802.1d Spanning Tree* – включить / выключить 802.1d Spanning Tree.

4.4.3 Подменю «Routing». Настройка маршрутизации

На данной странице можно добавить статические маршруты.

Advance → *Routing*

RoutingConfiguration

This page is used to configure the routing information. Here you can add/delete IP routes.

Enable:	<input checked="" type="checkbox"/>
Destination:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Next Hop:	<input type="text"/>
Metric:	<input type="text"/>
Interface:	Any ▼

Static Route Table:

Select	State	Destination	Subnet Mask	Next Hop	Metric	Interface
--------	-------	-------------	-------------	----------	--------	-----------

- *Enable* – флаг для добавления маршрута;
- *Destination* – адрес назначения;
- *Subnet Mask* – маска подсети;
- *Next Hop* – следующий узел;
- *Metric* – метрика;
- *Interface* – интерфейс.

4.4.4 Подменю «Bridging grouping». Объединение интерфейсов в группы

На данной странице можно объединять интерфейсы в разные группы. По-умолчанию все интерфейсы находятся в одной группе. Для переноса интерфейса в новую группы необходимо:

1. Выбрать новую группу из списка ниже
2. Выбрать интерфейсы в списке доступных интерфейсов (Available Interface)
3. Нажать стрелку ← для переноса интерфейсов в группу
4. Применить действия нажав кнопку «*Apply Changes*»

Advance → *Bridge grouping***Configuration**

To manipulate a mapping group:

1. Select a group from the table.
2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.
3. Click 'Apply Changes' button to save the changes.

Note that the selected interfaces will be removed from their existing groups and added to the new group.

Grouped Interfaces | **Available Interfaces**

-> | <-

Select Interfaces
 Default LAN1, LAN2, LAN3, LAN4, LocalIP, wlan0, wlan1

Apply Changes

4.4.5 Подменю «Link mode». Настройка LAN-портов

На данной странице можно задать режим работы LAN-портов. Доступны режимы 10/100 Full/Half Duplex, 1000 Full Duplex и режим автоопределения. Чтобы сохранить изменения нажмите «*Apply Changes*».

Advance → *Link mode***Ethernet Link Speed/Duplex Mode**

Set the Ethernet link speed/duplex mode.

LAN1: Auto Mode ▼
 LAN2: Auto Mode ▼
 LAN3: Auto Mode ▼
 LAN4: Auto Mode ▼

Apply Changes

4.4.6 Подменю «IPv6». Настройка протокола IPv6

На данной странице можно включить работу IPv6 протокола, для этого необходимо установить флаг «Enable».

Advance → *IPv6*

IPv6Configuration

This page be used to configure IPv6 enable/disable

IPv6: Disable Enable

4.4.6.1 Подменю «RADVD»

На данной странице можно настроить Router Advertisement Daemon.

Advance → *IPv6* → *RADVD*

RADVD Configuration

This page is used to setup the RADVD's configuration of your Device.

MaxRtrAdvInterval:	<input type="text" value="600"/>
MinRtrAdvInterval:	<input type="text" value="198"/>
AdvManagedFlag:	<input checked="" type="radio"/> off <input type="radio"/> on
AdvOtherConfigFlag:	<input type="radio"/> off <input checked="" type="radio"/> on

- *MaxRtrAdvInterval* – максимальный интервал отправки RA (Router Advertisement);
- *MinRtrAdvInterval* – минимальный интервал отправки RA;
- *AdvManagedFlag* – включить/выключить отpravку флага Managed в RA;
- *AdvOtherFlag* – включить/выключить отpravку флага Other RA.

4.4.6.2 Подменю «DHCPv6 setting»

Настройки DHCPv6 сервера. По умолчанию работает в режиме автоконфигурации (*DHCPv6Server(Auto)*) через делегацию префикса.

Advance → *IPv6* → *DHCPv6*

DHCPv6 Settings

This page is used to configure DHCPv6 Server and DHCPv6 Relay.

DHCPv6 Mode: NONE DHCPRelay DHCPv6Server(Manual) DHCPv6Server(Auto)

Auto Config by Prefix Delegation for DHCPv6 Server.

- *DHCPv6 Mode* – выбор режима:
 - *NONE* – работа без DHCP сервера;
 - *DHCPv6Relay* – работа в режиме DHCP-ретранслятора;
 - *DHCPv6Server (Manual)* – ручная настройка DHCP-сервера;
 - *DHCPv6Server(Auto)* – автоконфигурация DHCP-сервера.

4.4.6.3 Подменю «MLD proxy»

На странице можно включить работу MLD-proxy установив флаг, для этого необходимо установить флаг «Enable».

Advance → IPv6 → MLD proxy

MLD ProxyConfiguration

This page be used to configure MLD Proxy.

MLD Proxy: Disable Enable

WAN Interface:

Apply Changes

4.4.6.4 Подменю «MLD snooping»

На странице можно включить работу MLD-snooping, установив флаг «Enable».

Advance → IPv6 → MLD snooping

MLD SnoopingConfiguration

This page be used to configure MLD Snooping.

MLD Snooping: Disable Enable

Apply Changes

4.4.6.5 Подменю «IPv6 routing»

На странице можно добавить статические IPv6 маршруты.

Advance → IPv6 → IPv6 routing

IPv6 Static RoutingConfiguration

This page is used to configure the IPv6 static routing information. Here you can add/delete static IP routes.

Enable:	<input checked="" type="checkbox"/>
Destination:	<input type="text"/>
Next Hop:	<input type="text"/>
Metric:	<input type="text"/>
Interface:	Any ▾
<input type="button" value="Add Route"/> <input type="button" value="Update"/> <input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Show Routes"/>	

Static IPv6 Route Table:

Select	State	Destination	Next Hop	Metric	Interface
--------	-------	-------------	----------	--------	-----------

- *Enable* – флаг для добавления маршрута;
- *Destination* – адрес назначения;
- *Next Hop* – следующий узел;
- *Metric* – метрика;
- *Interface* – интерфейс.

4.4.6.6 Подменю «IPv6 IP/ Port filtering»

На странице осуществляется настройка фильтрации пакетов данных передаваемых через шлюз.

Advance → *IPv6* → *IP/Port filtering*

IPv6 IP/Port Filtering

Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Default Action Deny Allow

Protocol: TCP **Rule Action** Deny Allow

Source Interface ID:

Destination Interface ID:

Source Port: -

Destination Port: -

Current Filter Table:

Select	Protocol	Source Interface ID	Source Port	Destination Interface ID	Destination Port	Rule Action
<input type="button" value="Delete Selected"/>	<input type="button" value="Delete All"/>					

- *Default Action* – действие по умолчанию;
- *Protocol* – протокол;
- *Source Interface ID* – интерфейс источника;
- *Destination Interface ID* – интерфейс назначения;
- *Source Port* – порт источника;
- *Destination Port* – порт назначения.

4.5 Подменю «Diagnostics»

4.5.1 Подменю «Ping». Проверка доступности сетевых устройств

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

Diagnostics → *Ping*

Ping Diagnostics

This page is used to send ICMP ECHO_REQUEST packets to network host. The diagnostic result will then be displayed.

Host Address:

Для проверки доступности подключенного устройства необходимо ввести его IP-адрес в поле и нажать кнопку «Go».

4.6 Подменю «Admin»

4.6.1 Подменю «Commit/Reboot». Сохранение изменений и перезагрузка устройства

Нажмите кнопку «*Commit and Reboot*» для перезагрузки устройства или для сохранения изменений в системной памяти. Перезагрузка устройства может занять несколько минут.

Admin → *Commit/Reboot*

Commit and Reboot

This page is used to commit changes to system memory and reboot your system.

Commit and Reboot

4.6.2 Подменю «Backup/Restore». Восстановление и сброс настроек

В данном подменю возможно скопировать текущие настройки в файл (*Backup Settings to File*) или восстанавливать настройки из файла, который был сохранен ранее (*Restore Settings from File*). Кроме того, вы можете сбросить текущие настройки до заводских настроек по умолчанию (*Reset Settings to Default*).

Admin → *Backup/Restore*

Backup and Restore Settings

This page allows you to backup current settings to a file or restore the settings from the file which was saved previously. Besides, you could reset the current settings to factory default.

Backup

Settings to
File:

Backup...

Restore
Settings from
File:

Выберите файл

Файл не выбран

Restore

Reset Settings
to Default:

Reset

4.6.3 Подменю «Password». Настройка контроля доступа (установка паролей)

В данном меню осуществляется смена пароля для доступа к устройству.

Admin → *Password*

Password

This page is used to set the account to access the web server of router.
Empty user name and password will disable the protection.

Login User: user

Old Password:

New Password:

Confirmed Password:

Для смены пароля необходимо ввести существующий пароль в поле *Old Password*, затем новый пароль в *New Password* и подтвердить его *Confirmed Password*.

Для принятия изменений и сохранения необходимо нажать кнопку «*Apply changes*», для сброса значения использовать кнопку «*Reset*».

4.6.4 Подменю «Firmware upgrade». Обновление ПО

Для обновления ПО необходимо выбрать файл ПО используя кнопку «*Выберите файл*» и нажать «*Upgrade*», для сброса значения использовать кнопку «*Reset*».

Admin → *Firmware upgrade*

Firmware Upgrade

This page allows you upgrade the firmware to the newer version.
Please note that do not power off the device during the upload because this make the system unbootable.

Файл не выбран

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

4.6.5 Подменю «Time zone». Настройки системного времени

Во вкладке настраивается системное время на устройстве, возможна синхронизация с интернет-серверами точного времени.

Admin → *Time zone*

Time Zone Configuration

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Year Mon Day
 Hour Min Sec

Time Zone Select : ▼

Enable Daylight Saving Time

Enable SNTP Client Update

WAN Interface: ▼

SNTP Server : ▼
 (Manual Setting)

- *Current time* – текущее время;
- *Time Zone Select* – временная зона;
- *Enable Daylight Saving Time* – переход на летнее время;
- *Enable SNTP Client Update* – включить синхронизацию времени по SNTP;
- *WAN Interface* – интерфейс, через который производится обновление времени;
- *SNTP Server* – предпочитаемый сервер времени.

Для сохранения изменений нажмите кнопку «*Apply Changes*», для обновления информации кнопку «*Refresh*».

4.7 Меню «Statistics». Информация о прохождении трафика на портах устройства

4.7.1 Подменю «Interface»

В данном подменю отображается следующая информация:

Admin → *Interface*

Interface Statistics

This page shows the packet statistics for transmission and reception regarding to network interface.

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
eth0.2	1059	0	0	217	0	0
eth0.3	0	0	0	0	0	0
eth0.4	0	0	0	0	0	0
eth0.5	0	0	0	0	0	0
wlan0	2769	0	0	0	0	0
wlan1	0	0	0	0	0	0

- *Interface* – интерфейс;
- *Rx pkt* – получено пакетов;
- *RX err* – ошибки на приеме;
- *Rx drop* – отброшено на приеме;
- *Tx pkt* – отправлено пакетов;
- *Tx err* – ошибка отправки;
- *Tx drop* – отброшено при передаче.

4.7.2 Подменю «PON»

В данном подменю отображается следующая информация:

Admin → *PON*

PON Statistics

Bytes Sent	0
Bytes Received	0
Packets Sent	0
Packets Received	0
Unicast Packets Sent	0
Unicast Packets Received	0
Multicast Packets Sent	0
Multicast Packets Received	0
Broadcast Packets Sent	0
Broadcast Packets Received	0
FEC Errors	0
HEC Errors	0
Packets Dropped	0
Pause Packets Sent	0
Pause Packets Received	0

- *Bytes Sent* – отправлено байт;
- *Bytes Received* – байт получено;
- *Packets Sent* – пакетов отправлено;
- *Packets Received* – пакетов получено;
- *Unicast Packet Sent* – Unicast пакетов отправлено;
- *Unicast Packet Received* – Unicast пакетов получено;
- *Multicast Packets Sent* – Multicast пакетов отправлено;
- *Multicast Packets Received* – Multicast пакетов получено;
- *Broadcast Packet Sent* – широковещательных пакетов отправлено;
- *Broadcast Packet Received* – широковещательных пакетов получено;
- FEC Errors – ошибки FEC
- Packets Dropped – пакетов отброшено.

4.8 Меню «Z-Wave». Для устройства NTU-RG-5421G-WZ

Zwave Configuration

This page let user to config Zwave settings

Zway : Disable Enable

Hostname :

Destination Port :

Secure connection : Disable Enable

В данном меню настраиваются параметры «Умного дома».

- *Zway* – включить / выключить контроллер «Умного дома»;
- *Hostname* – указать адрес удалённой платформы «Умного дома»;
- *Destination port* – указать порт платформы, к которому подключается контроллер «Умного дома»;
- *Secure connection* – установить в Enable, если для обмена с платформе используется защищенный канал;
- *Reset controller (очистить кэш Zway)* – при нажатии кнопки, контроллер отключается, с него удаляется вся информация о подключении к платформе, о привязанных датчиках и сценарии.

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

5 Список изменений

Версия документа	Актуальность для ПО	Дата выпуска	Содержание изменений
Версия 1.0	1.0.1	11.2018	Первая публикация