**Программа и методика испытаний абонентского оборудования для подтверждения соответствия универсальным техническим требованиям FTTB Medium без FXS (v5.11)**

**Москва**

2021

**Содержание**

[1 Назначение 6](#_Toc88743085)

[2 Общие положения 7](#_Toc88743086)

[3 Программа испытаний 9](#_Toc88743087)

[4 Методика испытаний 10](#_Toc88743088)

[5 Проверка требований к производительности в смешанном режиме 12](#_Toc88743089)

[5.1 Проверка доступных для конфигурации параметров 12](#_Toc88743090)

[5.2 Проверка производительности. 13](#_Toc88743091)

[5.3 Проверка производительности устройства в режиме маршрутизации без использования NAT 15](#_Toc88743092)

[5.4 Проверка производительности устройства в режиме маршрутизатора NAT с IPoE при просмотре ТВ с HD качеством 17](#_Toc88743093)

[5.5 Проверка согласования режимов PPPoE. 18](#_Toc88743094)

[5.6 Проверка загрузки устройства (рабочий режим). 19](#_Toc88743095)

[6 Проверка требований к производительности при функцонально-нагрузочном тестировании. 22](#_Toc88743096)

[6.1 Проверка производительности устройства в режиме маршрутизатора NAT c IPoE, при просмотре ТВ канала с HD качеством и одновременной работой Torrent клиента. 22](#_Toc88743097)

[6.2 Проверка производительности устройства в режиме маршрутизатора NAT c PPPoE, при просмотре ТВ канала с HD качеством и одновременной работой Torrent клиента. 22](#_Toc88743098)

[6.3 Проверка производительности устройства в режиме маршрутизатора NAT c PPPoE, при просмотре ТВ канала с HD качеством и одновременной работой Torrent клиента по беспроводному соединению. 23](#_Toc88743099)

[6.4 Проверка производительности устройства в режиме маршрутизатора NAT c PPPoE, при просмотре ТВ канала с HD качеством через соединение мост с тегами VLAN и одновременной работой Torrent клиента. Проверка изоляции групп. 24](#_Toc88743100)

[7 Проверка требований к производительности беспроводного модуля 26](#_Toc88743101)

[7.1 Проверка доступных для конфигурации параметров 26](#_Toc88743102)

[7.2 Проверка производительности беспроводного соединения между интерфейсами WLAN и LAN в диапазоне 2.4 ГГц 26](#_Toc88743103)

[7.3 Проверка производительности беспроводного соединения между интерфейсами WLAN и LAN в диапазоне 5 ГГц 27](#_Toc88743104)

[7.4 Проверка производительности беспроводного соединения при работе в двух диапазонах. 28](#_Toc88743105)

[7.5 Проверка физических параметров беспроводной сети 29](#_Toc88743106)

[7.6 Проверка работоспособности режимов (2.4 ГГц). 30](#_Toc88743107)

[7.7 Проверка работоспособности режимов (5 ГГц). 31](#_Toc88743108)

[7.8 Проверка работоспособности Multicast по WiFi (2.4 ГГц) при соединении PPPoE 32](#_Toc88743109)

[7.9 Проверка работоспособности Multicast по WiFi (5 ГГц) c максимальной утилизацией частоты 2.4 ГГц. 32](#_Toc88743110)

[7.10 Проверка количества клиентов на SSID 33](#_Toc88743111)

[7.11 Проверка ограничения количества клиентов на SSID 34](#_Toc88743112)

[7.12 Проверка управления передатчиком 34](#_Toc88743113)

[7.13 Проверка Wi-Fi радара 35](#_Toc88743114)

[7.14 Проверка изоляции пользователей в одном SSID 36](#_Toc88743115)

[7.15 Проверка работоспособности SSID3 и SSID4 36](#_Toc88743116)

[7.16 Оценка производительности с разными типами устройств. 37](#_Toc88743117)

[7.17 Тестирование WPS 38](#_Toc88743118)

[8 Проверка качества обслуживания (QoS) и аппаратных очередей 40](#_Toc88743119)

[8.1 Проверка очередей Upstream 40](#_Toc88743120)

[8.2 Управление полосой пропускания. 41](#_Toc88743121)

[9 Управление устройством 43](#_Toc88743122)

[9.1 Проверка установки соединения с ACS при наличии только PPPoE 43](#_Toc88743123)

[9.2 Проверка установки соединения с ACS PPPoE и IPoE с 43 опцией 43](#_Toc88743124)

[9.3 Проверка установки соединения с ACS PPPoE и IPoE с 43 опцией и DGW 44](#_Toc88743125)

[9.4 Проверка установки соединения с ACS PPPoE и IPoE 45](#_Toc88743126)

[9.5 Проверка установки соединения с ACS IPoE с 43 опцией и DGW 46](#_Toc88743127)

[9.6 Проверка установки соединения с ACS IPoE 47](#_Toc88743128)

[9.7 Проверка установки соединения с ACS IPoE с 43 опцией 47](#_Toc88743129)

[9.8 Проверка установки соединения с ACS при наличии только PPPoE в ЦСМ 48](#_Toc88743130)

[9.9 Проверка установки соединения с ACS PPPoE и IPoE в ЦСМ 49](#_Toc88743131)

[9.10 Проверка установки соединения с ACS IPoE в ЦСМ 50](#_Toc88743132)

[9.11 Выполнение тест плана ATP-069 51](#_Toc88743133)

[9.12 Проверка поддержки дерева параметров CPE 54](#_Toc88743134)

[9.13 Обновление ПО устройства 55](#_Toc88743135)

[9.14 Сохранение/обновление конфигурации. 56](#_Toc88743136)

[9.15 Настройка параметров PPPoE соединения 57](#_Toc88743137)

[9.16 Управление беспроводными соединениями 58](#_Toc88743138)

[9.17 Управление учётными записями 59](#_Toc88743139)

[9.18 Диагностика устройства 59](#_Toc88743140)

[9.19 Download тест 60](#_Toc88743141)

[9.20 Upload тест 61](#_Toc88743142)

[9.21 DeviceLog тест 62](#_Toc88743143)

[9.22 Диагностика WiFi Radar 63](#_Toc88743144)

[9.23 Настройка удаленного доступа 63](#_Toc88743145)

[10 Проверка функционала 65](#_Toc88743146)

[10.1 Проверки функционала ALG 65](#_Toc88743147)

[10.2 Проверки функционала UPnP 65](#_Toc88743148)

[10.3 UDP\_to\_HTTP\_proxy 66](#_Toc88743149)

[10.4 Проверка функций PPTP/L2TP/IPSec pass-through 67](#_Toc88743150)

[10.5 Проверка Port Mapping / NatLoopback 67](#_Toc88743151)

[10.6 Проверки функционала шифрования пароля 68](#_Toc88743152)

[10.7 Проверки алгоритма установления PPPoE сессии 69](#_Toc88743153)

[10.8 Проверка резервного хранения образа программного обеспечения и параметров конфигурации в энергонезависимой памяти 70](#_Toc88743154)

[10.9 Проверка работоспособности Wizard 71](#_Toc88743155)

[10.10 Проверка работоспособности Trouble wizard 72](#_Toc88743156)

[10.11 Проверка доступа к устройству 73](#_Toc88743157)

[10.12 Доступность управления со стороны WAN 73](#_Toc88743158)

[10.13 Привилегии пользователей 74](#_Toc88743159)

[10.14 Проверка firewall 75](#_Toc88743160)

[10.15 Проверка журналирования. 77](#_Toc88743161)

[10.16 Проверка фильтрации на основе «белого списка» 78](#_Toc88743162)

[10.17 Проверка фильтрации на основе «черного списка» 79](#_Toc88743163)

[11 Проверка требования к USB-порту и дополнительным приложениям 80](#_Toc88743164)

[11.1 Проверка доступа SMB 80](#_Toc88743165)

[11.2 Проверка DLNA 81](#_Toc88743166)

[12 Проверка IPv4/IPv6 dualstack 82](#_Toc88743167)

[12.1 Проверка работоспособности устройства в режиме DHCPv6/v4 клиента (statefull) и выделением адресов LAN через PD. 82](#_Toc88743168)

[12.2 Проверка работоспособности устройства в режиме SLAAC, получение адресов на LAN через DHCPv6PD 83](#_Toc88743169)

[13 Проверка электропитания 85](#_Toc88743170)

[13.1 Проверка параметров БП 85](#_Toc88743171)

[13.2 Проверка температурных рамок 85](#_Toc88743172)

[Схемы 87](#_Toc88743173)

[Схема беспроводного подключения FTTB 87](#_Toc88743174)

[Схема беспроводного подключения FTTB mesh 88](#_Toc88743175)

[Проверка функционала 89](#_Toc88743176)

[Управление устройством 90](#_Toc88743177)

[Проверка требований к производительности в смешанном режиме FTTB 91](#_Toc88743178)

[Проверка требований к производительности при функцонально-нагрузочном тестировании FTTB 93](#_Toc88743179)

[Проверка качества обслуживания (QoS) и аппаратных очередей 95](#_Toc88743180)

[Проверка требования к USB-порту и дополнительным приложениям 97](#_Toc88743181)

# 1 Назначение

Данная программа и методика испытаний абонентского оборудования FTTB Medium no FXS для подтверждения соответствия универсальным техническим требованиям разработана с целью унификации процессов тестирования абонентского оборудования, предназначенного для оказания услуг связи на сети широкополосного доступа ПАО «Ростелеком» (Далее – Общество).

Настоящая Методика описывает алгоритмы и определяет способы, применяемые при тестировании абонентского оборудования FTTB Medium no FXS, в соответствии с Процедурой организации тестирования абонентского оборудования для оказания услуг ШПД на сети ПАО «Ростелеком» (далее – Процедура) с учетом региональной специфики.

Методика вводится в действие впервые с даты её утверждения.

# 2 Общие положения

*Термины, определения и сокращения*

Для целей Методики в ней используются термины и сокращения, определенные в Глоссарии терминов и определений Общества, а также следующие:

Лаборатория - Лаборатория Корпоративного центра (Московская область, г. Реутов, Юбилейный пр-кт, д. 29, АТС-791, 3 этаж);

Образцы оборудования - Образцы оборудования, переданные для проведения тестирования. Аппаратная и программная версияобразцов оборудования должны полностью совпадать с версией, поставляемой в дальнейшем на сеть связи Общества;

Поставщик - Поставщик оборудования (производитель или системный интегратор);

Тестирование - Процесс испытаний абонентского оборудования;

Тестирование после доработки - Испытания оборудования, ранее прошедшего тестирование с результатом «Рекомендовано с замечаниями»;

Технические требования - Детализированные требования к поддерживаемому функционалу, соответствию стандартам и параметрам производительности абонентского оборудования;

Услуги ШПД - Услуги связи, оказываемые на сети широкополосного доступа, включая доступ в сеть Интернет и цифровое телевидение IPTV, предоставляемые массовому и корпоративному сегментам рынка;

ПМИ - Программа и методика испытаний абонентского оборудования на соответствие утвержденному техническому заданию Общества, является рабочей инструкцией для технического персонала (нижний уровень в структуре ВНД);

ШПД - Широкополосный доступ;

CPE - Customer Premises Equipment. Оконечное сетевое оборудование, располагаемое в помещении абонента. В контексте настоящей Методики - абонентское оборудование, подвергаемое испытаниям.

STB(ТВ приставка) - Устройство позволяющее получить доступ к цифровому телевидению и цифровым телевизионным услугам;

*Область применения*

Положения Методики распространяются на технические подразделения Общества, которые проводят тестирования абонентского оборудования для массового и корпоративного сегментов рынка на сетях связи Общества.

Применение Методики в макрорегиональных и региональных филиалах Общества – «Для информации».

*Нормативные ссылки*

• В данной Методике использованы ссылки на следующие нормативные документы:

• *Процедура управления внутренней нормативной документацией ПАО «Ростелеком»;*

• *Методика по оформлению внутренних нормативных документов ПАО «Ростелеком»;*

• *Инструкция по делопроизводству в ПАО «Роcтeлeкoм»;*

• *Глоссарий терминов и определений ПАО «Ростелеком»;*

• *Процедура управления записями в ПАО «Ростелеком»;*

• *Универсальные технические требования для проведения закупочных процедур абонентского оборудования при оказании услуг ШПД в ПАО Ростелеком;*

• *Процедура организации тестирования абонентского оборудования для оказания услуг ШПД на сети ПАО «Ростелеком».*

# 3 Программа испытаний

Испытания образцов оборудования проводятся после выполнения настройки согласно схеме испытаний. Схемы испытаний образцов оборудования составлены с учетом специфики различных сервисных моделей сетей Общества.

Испытания оборудования состоят из следующих проверок (групп тестов):

• *производительность;*

• *производительность беспроводного модуля;*

• *качество обслуживания и аппаратные очереди;*

• *встроенный агент VoIP если применимо;*

• *управление устройством;*

• *функционал устройства;*

• *протоколы IPv4 и IPv6.*

# 4 Методика испытаний

*Цель тестирования*

Целью тестирования является проверка соответствия абонентского оборудования утверждённым универсальным техническим требованиям для проведения закупочных процедур абонентского оборудования при оказании услуг ШПД в ПАО «Ростелеком». Приказ 01/01/130-15 от 19.02.2015

Методика испытаний предназначена для следующих типов устройств:

1xGE WAN, 4xGE LAN, 1xUSB, 2x2 b/g/n 2.4 GHz, 2x2 WiFi n/ac 5 GHz .

*Руководящие документы и запись результатов тестирования*

Согласно Процедуре при проведении тестирований используются следующие внутренние нормативные документы:

• *Вышестоящая Процедура;*

• *Техническое задание.*

В процессе выполнения тестовых процедур ПМИ, участники тестирования заносят полученные данные в пункт “Ожидаемый результат”, выставляя отметку “Тест не пройден”, “Тест пройден” или комментарий.

В исходном состоянии все заполняемые позиции в пункте “Ожидаемый результат” должны быть пустыми.

Если какой-то тест не был произведен, то напротив него заполняется поле «Комментарии» с пояснением причины, а поля “Тест не пройден” и “Тест пройден” остается пустым.

*Условия и порядок проведения тестирования*

Тестирование проводится совместной рабочей группой, куда входят технические специалисты Общества и представитель(и) поставщика (производителя) оборудования. По результатам составляется протокол тестирования, содержащий:

• *Модель тестируемого оборудования, его аппаратная и программная версия;*

• *Период проведения испытаний;*

• *Краткое заключение с рекомендацией по использованию;*

• *Перечень проводимых тестов с полученными результатами;*

• *Состав рабочей группы с указанием ФИО, должностей, и их подписи.*

Тестирование может быть приостановлено, если какие-либо факторы могут повлечь нарушение правил и мер безопасности для персонала или создать условия, препятствующие нормальной эксплуатации тестируемого оборудования, измерительных приборов и другого оборудования Общества.

Перед началом тестирования производятся подготовительные работы, которые включают в себя:

• *Подготовку стенда в соответствии со схемой проведения испытаний;*

• *Настройку измерительных приборов и вспомогательного оборудования;*

• *Монтаж и настройку тестируемого оборудования.*

На тестирование предоставляются и используются в работе:

• *Тестируемое оборудование в заявленной комплектации, включая версии программной и аппаратной части;*

• *Техническая документация: спецификация, руководство и пр.;*

• *Сертификаты и декларации соответствия.*

Тестирование проводится полностью по одной (каждой) модели оборудования, включая одну версию аппаратного и одну версию программного обеспечения. Если в процессе тестирования выясняется необходимость в замене моделей и/или версий оборудования, то все процедуры полностью повторяются.

Протокол тестирования подписывается членами рабочей группы и заверяется руководителем структурного подразделения Общества, проводившего тестирование. При отсутствии подписи представителя производителя, в протокол заносится соответствующая запись с пояснением причины.

Оборудование, используемое для испытаний, включая генератор трафика, телевизионные приставки, коммутаторы, концентраторы цифровых абонентских линий, ноутбуки, персональные компьютеры, другое вспомогательное оборудование и программное обеспечение является эталонным и применяется для всех испытуемых устройств.

Настройкой оборудования, используемого для испытаний, занимаются специалисты Лаборатории. Представители производителя не допускаются к настройке оборудования, используемого для испытаний. Несанкционированный доступ представителей производителя к настройкам оборудования Лаборатории может стать основанием для прекращения испытаний.

В случае выхода из строя или некорректной работы в процессе проверок оборудования, используемого для испытаний, оно может быть заменено на аналогичное. В таком случае специалисты Лаборатории могут принять решение о повторной проверке устройств предоставленных для испытаний.

Поставщик или представитель производителя, предоставляя устройство на испытания, соглашается с использованием эталонного оборудования Лаборатории. По согласованию со специалистами Лаборатории поставщик или представитель производителя может предоставлять результаты других испытаний или предоставлять другое оборудование для проведения испытаний. Результаты испытаний на не эталонном оборудованием могут приниматься специалистами Лаборатории для информации, но не отражаются в протоколе испытаний.

# 5 Проверка требований к производительности в смешанном режиме

## 5.1 Проверка доступных для конфигурации параметров

|  |  |  |
| --- | --- | --- |
| Цель теста | Предварительная проверка возможности конфигурации. Проверка осуществляется в Web интерфейсе и по технической документации | |
| Конфигурация | Проверка требований к производительности в смешанном режиме FTTB | |
| Процедура | Наличие индикаторов:  ☐ Питание устройства;  ☐ Статус;  ☐ Порт WAN;  ☐ Четыре порта LAN;  ☐ Состояние беспроводного интерфейса 2.4 ГГц;  ☐ Состояние беспроводного интерфейса 5 ГГц.  Наличие на корпусе:  ☐ Корпус по требованиям Ростелеком, согласно требованиям Приложения 1  ☐ Утопленной кнопки возврата к заводским установкам (Reset);  ☐ Кнопки WPS;  ☐ Кнопки включение/отключение Wi-Fi (опция);  ☐ Кнопки включение/отключение устройства (опция);  ☐ Настольное исполнение корпуса с возможностью крепления на стене;  ☐ Прорезиненные ножки.  Проверка в Web интерфейсе устройства:  ☐ Настройки по умолчанию;  ☐ Есть возможность выйти из webUi, при бездействии автовыход через 5-15 минут;  ☐ Есть защита от перебора пароля для web и telnet (блокировка входа на 1 минуту после трех неудачных попыток);  ☐ Web интерфейс на русском языке;  ☐ Кнопка вызова Wizard для настройки подключения к Интернет;  ☐ Присутствуют настройки Firewall и SPI;  ☐ Устройство позволяет создавать до 8 WAN соединений;  ☐ Устройство позволяет резервировать адреса DHCP для локальных клиентов;  ☐ В Web-интерфейсе есть возможность просмотра всех выданных по DHCP адресов с указанием интерфейса (LAN/Wi-Fi);  ☐ Адаптивная верстка (для мобильных устройств с разными операционными системами Android, IOS, Windows phone).  На каждом IP-Host имеется возможность:  ☐ Отключать трансляцию адресов NAT;  ☐ Отключать маршрут по умолчанию;  ☐ Настроить IGMP Proxy.  После настройки соединений:  ☐ Группировка портов была выполнена корректно;  ☐ Интерфейсы IP-Host получили IP адреса;  ☐ Каждое соединение имеет уникальный MAC адрес;  ☐ Таблица маршрутизации содержит маршруты, полученные через DHCP опции: 33, 121, 249 на интерфейсе IP-Host2.  ☐ Устройство передает DHCP option 12 c интерфейса IP-Host2 и получает соответствующий IP.  ☐ Поддержка HTTPS Web-сервера (опционально) | |
| Ожидаемый результат | Выполнение всех пунктов | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 5.2 Проверка производительности.

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка производительности | |
| Конфигурация | Проверка требований к производительности в смешанном режиме FTTB | |
| Процедура | 1. Подключить порт генератора трафика (TG2) к LAN1;  2. Подключить 2 STB к портам LAN2 и LAN3;  3. Подключить SIP Phone к порту LAN4;  4. Убедиться в установке соединения с TR069 через PPPoE;  5. Загрузить конфигурацию в программном обеспечении Spirent Test Center;  6. Запустить потоки Stream 1 и Stream 2 (двунаправленный трафик с скоростью 1000 Мбит/с) в течении 5 минут;  7. Переключать каналы на STB, совершить вызов, осуществить запрос с сервера CWMP;  8. Зафиксировать результат производительности по соотношению значений Rx L1 Rate (bps) и Tx L1 Rate (bps) в программном обеспечении Spirent Test Center;  9. Изменить размер передаваемого пакета с Spirent на 1522;  10. Повторить процедуру измерения скорости.  11. Переключить TG2 из порта LAN1 в LAN2;  12. Переключить STB из LAN2 в LAN1;  13. Запустить потоки Stream 1 и Stream 2 (двунаправленный трафик с скоростью 1000 Мбит/с 1500 потоков) в течении 5 минут;  14. Переключать каналы на STB, совершить вызов, осуществить запрос с сервера CWMP;  15. Зафиксировать результат производительности по соотношению значений Rx L1 Rate (bps) и Tx L1 Rate (bps) в программном обеспечении Spirent Test Center;  16. Подключить в LAN3 другой порт трафик генератора;  17. Запустить потоки Stream 1 и Stream 2 (двунаправленный трафик с скоростью 1000 Мбит/с) в течении 5 минут;  18. Зафиксировать результат производительности по соотношению значений Rx L1 Rate (bps) и Tx L1 Rate (bps) в программном обеспечении Spirent Test Center;  19. Отключить TG от LAN3;  20. Изменить номер vlan для соединения bridge связанного с LAN4 на 271 и добавить в группировку LAN3, отключить STB от LAN1, подключить STB к LAN3 и LAN4;  21. Изменить bridge связанный с LAN1 на тегированный vlan tag 2000;  22. Запустить потоки Stream 1 и Stream 2 (двунаправленный трафик с скоростью 1000 Мбит/с 1500 потоков) в течении 5 минут;  23. Установить на двух STB просмотр одинаковых каналов, переключить канал на одной STB, убедиться, что на WAN CPE отсутствует leave пакет, так как данный канал продолжает «смотреть» вторая STB.  24. Переключать каналы на STB;  25. Переключить TG2 из порта LAN2 в LAN1;  26. Запустить потоки Stream 1 и Stream 2 (двунаправленный трафик с скоростью 1000 Мбит/с) в течении 5 минут;  27. Переключать каналы на STB;  28. Изменить соединение PPPoE на тегированное (vlan 808), выключить IGMP proxy;  29. Изменить номер vlan для соединения bridge связанного с LAN1 на 270;  30. Подключить SIP Phone к порту LAN1;  31. Переключить TG2 из порта LAN1 в LAN2;  32. Настроить тегированное IPoE соединение (с тегом 271) с IGMP Proxy и объединить его в одной группу с PPPoE;  33. Запустить потоки Stream 1 и Stream 2 (двунаправленный трафик с скоростью 1000 Мбит/с 1500 потоков) в течении 5 минут;  34. Переключать каналы на STB;  35. Подключить STB к LAN2, убедиться что STB работает. | |
| Ожидаемый результат | Скорость передачи трафика не менее 800 Мбит/с при работе одного IPTV канала и не менее 800 Mбит/c при работе двух IPTV каналов. Пакеты размером 1522 байта пропускаются. При переключении на одной из STB не проиcходит замираний на другой STB. Скорость передачи трафика между LAN на скорости интерфейса. Весь исходящий «служебный» трафик (PPP, LCP, IPCP, DHCP, IGMP, трафик от встроенного клиента TR069 и/или FXS при его наличии) имеет приоритет перед остальным трафиком. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 5.3 Проверка производительности устройства в режиме маршрутизации без использования NAT

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка динамической маршрутизации (опция) и статической маршрутизации. | |
| Конфигурация | без схемы | |
| Процедура | В качестве маршрутизатора RIP и DHCP сервера с options 33, 121, 249 используется трафик генератор Spirent.  1. Настроить IP-Host1 в режиме PPPoE;  2. Отключить NAT;  3. Включить RIPv2 в настройках CPE;  4. Подключить порт генератора трафика (TG2) к порту LAN2;  5. Загрузить конфигурацию Wan-LAN\_routed\_PPPoE.tcc в программном обеспечении Spirent Test Center;  6. Запустить потоки Stream 1 и Stream 2 в течение 5 минут (двунаправленный трафик с скоростью 1000 Мбит/с);  7. Зафиксировать результат производительности по соотношению значений Rx L1 Rate(bps) и Tx L1 Rate(bps) в программном обеспечении Spirent Test Center;  8. Запустить RIP в Spirent Test Center;  9. Проверить в таблице маршрутизации наличие анонсированного маршрута;  10. Поменять IP адрес LAN на произвольный через TR069;  11. Убедиться через WebUI что IP адрес LAN изменен;  12. Проверить в таблице маршрутизации Spirent наличие анонсированного маршрута;  13. Настроить IP-Host1 в режиме IPoE;  14. Повторить пункты 2-9.  15. Проверить таблицу маршрутизации на наличие маршрутов, полученных по опциям 121, 33, 249;  16. С помощью команды PING убедиться, в получении доступа к IP адресу, полученному через опции.  17. Добавить произвольный маршрут вручную через webUI.  18. С помощью команды PING убедиться, в получении доступа к IP адресу, добавленному вручную. | |
| Ожидаемый результат | Скорость передачи трафика не менее 800 Мбит/с. В таблице маршрутизации есть анонсированные маршруты. После смены IP адреса LAN Spirent получил анонс с новой подсетью. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 5.4 Проверка производительности устройства в режиме маршрутизатора NAT с IPoE при просмотре ТВ с HD качеством

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка производительности | |
| Конфигурация | без схемы | |
| Процедура |  IP-Host 1 связан с Ethernet WAN интерфейсом в режиме Access;   IP-Host 2 связан c Ethernet WAN интерфейсом в режиме VLAN 802.1q (VID=xxx) 802.1p=0;   LAN1, LAN2, LAN3, LAN4, FXS (если используется), SSID1 и SSID5 связаны с IP-Host1 и IP-Host2 в режиме маршрутизации с функцией NAT и локальным DHCP сервером;   SSID2 и SSID6 связан с WAN интерфейсом (VLAN=xxx p=0) в режиме моста.  1. Настроить IP-Host1 в режиме DHCP;  2. Подключить STB к LAN1, LAN3 и LAN4 и запустить просмотр;  3. Подключить порт генератора трафика (TG2) к LAN2;  4. Загрузить конфигурацию в программном обеспечении Spirent Test Center;  5. Запустить потоки Stream 1 и Stream 2 в течение 5 минут (двунаправленный трафик с скоростью 1000 Мбит/с 1500 потоков);  6. Переключать различные каналы на STB;  7. Зафиксировать результат производительности по соотношению значений Rx L1 Rate(bps) и Tx L1 Rate(bps) в программном обеспечении Spirent Test Center.  8. Отключить STB из LAN1 и LAN3 и подключить SIP телефон к LAN1;  9. Настроить правило QoS по SRC MAC STB которая подключена к LAN4.  10. Настроить правило QoS по LAN1.  11. Запустить потоки Stream 1 и Stream 2 в течение 5 минут (двунаправленный трафик с скоростью 1000 Мбит/с);  12. Просматривать VOD, совершить звонок по телефону;  13. Скачивать Torrent файлы с ноутбука подключенного к SSID1 (2.4ГГц);  14. Просматривать VOD, совершить звонок по телефону;  15. Проверить, что работает IGMP Snooping и трафик не копируется на остальные интерфейсы;  16. Скачивать Torrent файлы с ноутбука подключенного к SSID5 (5 ГГц); | |
| Ожидаемый результат | Скорость передачи трафика не менее 800 Мбит/с. ТВ работает без замираний и искажений. При переключении каналов на одной STB не происходит замираний на других STB. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 5.5 Проверка согласования режимов PPPoE.

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка согласования режимов PPPoE | |
| Конфигурация | без схемы | |
| Процедура | 1 Настроить PPPoE сервер (авторизация PAP only) размер MTU=1400;  2 Настроить IP-Host1 в режиме PPPoE (авторизация auto) MTU=1492;  3 Зафиксировать результат;  4 Настроить PPPoE сервер (авторизация CHAP only) размер MTU=1492;  5 Настроить IP-Host1 в режиме PPPoE (авторизация auto) MTU=1492. | |
| Ожидаемый результат | Соединение PPPoE было установлено в режиме авторизации PAP и CHAP. Размер MTU был согласован. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 5.6 Проверка загрузки устройства (рабочий режим).

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка времени загрузки устройства | |
| Конфигурация | без схемы | |
| Процедура | 1. Подключить устройство двупарным кабелем;  2. Выключить, а затем снова включить электропитание устройства;  3. Захватить поток с WAN интерфейса;  4. Проверить, что загрузка устройства и переход в рабочий режим происходит менее чем за 120 с. Под рабочим режимом понимается возможность передавать данные, принимать и исполнять команды управления;  5. Запустить обновление ПО через web-интерфейс, убедиться, что индикация соответствует алгоритму;  6. Активировать функцию arp ping через TR069;  7. Визуально убедиться, что процесс загрузки и установки соединения сопровождается световой индикацией;  8. Убедиться, что CPE отправляет lcp и unicast arp ping в сторону сервера;  9. Сделать недоступными PPPoE и IPoE серверы, убедиться что при отсутствии ответа на 3 lcp (arp) устройство инициализирует новую PPPoE и IPoE сессии;  10. При установленном PPPoE и IPoE соединении перезагрузить устройство через webUI;  11. Перезагрузить устройство, отключив питание;  12. Сбросить устройство к заводским установкам при помощи кнопки reset держа ее от 10 до 14 секунд;  13. Подключить устройство GE кабелем длиной 100 м;  14. Убедиться в установлении PPPoE и IPoE соединения;  15. Подключить STB к LAN2 убедиться что IPTV работает;  16. Проанализировать поток с WAN интерфейса и убедиться что CPE отвечает на General Query с случайной задержкой, ограниченной Max Resp Time (на сервере выставлено 10 сек).  17. IGMP report не копируются во все LAN.  18. Изменить Max Resp Time на 2 сек. Повторить пункт 16.  19. Включить DMZ на IP адрес PC;  20. Запланировать вызов RPC-Метода GetRPCMethods на ACS;  21. Настроить проброс портов в диапазоне включающем порт TR069.  22. Запланировать вызов RPC-Метода GetRPCMethods на ACS;  Примечание:  Для индикации состояния устройства определён алгоритм работы светодиода «Статус»:  • Светодиод быстро мигает (примерно 5 Гц) – идет процесс загрузки CPE и установки соединения с сетью Ростелеком;  • Светодиод горит постоянно – CPE полностью загружено и готово к работе (установлено соединение);  • Светодиод медленно мигает (примерно 1 Гц) – идет процесс обновления ПО;  • Светодиод не горит – ошибка загрузки.  Для индикации состояния встроенного SIP клиента (если он есть на устройстве) определён алгоритм работы светодиода «FXS»:  • Светодиод горит постоянно – SIP агент успешно зарегистрирован;  • Светодиод медленно мигает – при разговоре или снятой трубке;  • Не горит – SIP агент не зарегистрирован или выключен. | |
| Ожидаемый результат | Время загрузки устройства до момента установки соединения не более 120 сек.  В потоке WAN интерфейса нет пакетов с локальными адресами.  Если устройство ранее устанавливало PPPoE сессию, при перезагрузке перед установлением PPPoE сессии устройство посылает сообщение Termination Request и PADT с используемым ранее идентификатором сессии, сервер корректно отвечает.  Устройство посылает DHCP release перед перезагрузкой.  Устройство отправляет lcp (arp ping) и инициализирует новую сессия при не доступности BRAS. CPE отвечает на GENERAL QUERY в пределах заданного интервала с распределение белого шума.  IGMP report не копируются в все LAN интерфейсы.  Индикация соответствует алгоритму.  После успешного сброса к заводским настройкам MAC адрес LAN соответствует информационной наклейке.  После настройки DMZ и/или проброса портов устройство отвечает на запросы TR069.  Соединение устанавливается с кабелем длиной 100 м и двупарным кабелем. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

# 6 Проверка требований к производительности при функцонально-нагрузочном тестировании.

## 6.1 Проверка производительности устройства в режиме маршрутизатора NAT c IPoE, при просмотре ТВ канала с HD качеством и одновременной работой Torrent клиента.

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка производительности услугами Общества | |
| Конфигурация | Проверка требований к производительности при функцонально-нагрузочном тестировании FTTB | |
| Процедура | 1. Настроить IP-Host1 в режиме DHCP;  2. Скачивать Torrent файлы с ноутбука подключенного к порту LAN1;  3. Захватить трафик с WAN интерфейса, убедится, что IGMP запросы отправляются с IP адреса интерфейса;  4. Запустить просмотр ТВ канала в HD качестве на приставке, подключенной к порту LAN2;  5. Во время работы приложения проверить работоспособность сервисов интерактивного телевидения:   переключение каналов;   работа VoD;   функции VoD: “перемотка”, паузы более 5 мин.  6. Запустить игру World of Tanks. | |
| Ожидаемый результат | Во время нагрузочного тестирования скорость Torrent клиента достигала не менее 300 Мбит/с, при этом трансляция телевидения происходила без искажений. Все сервисы интерактивного телевидения: IPTV, VoD работают корректно. Приложение World of Tanks работает корректно | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 6.2 Проверка производительности устройства в режиме маршрутизатора NAT c PPPoE, при просмотре ТВ канала с HD качеством и одновременной работой Torrent клиента.

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка производительности услугами Общества | |
| Конфигурация | Проверка требований к производительности при функцонально-нагрузочном тестировании FTTB | |
| Процедура | 1. Настроить IP-Host1 в режиме PPPoE (с поддержкой TR-101);  2. Скачивать Torrent файлы с ноутбука подключенного к порту LAN1;  3. Запустить просмотр ТВ канала в HD качестве на телевизоре, подключенном к порту LAN2;  4. Зафиксировать скорость передачи Torrent файлов;  5. Захватить трафик с WAN интерфейса, убедится, что IGMP запросы отправляются с адреса 0.0.0.0 (рекомендации TR-101);  6. Во время работы приложения проверить работоспособность сервисов интерактивного телевидения:   переключение каналов;   работа VoD;   функции VoD: “перемотка”, паузы более 5 мин. | |
| Ожидаемый результат | Во время нагрузочного тестирования скорость Torrent клиента достигала не менее 300 Мбит/с, при этом трансляция телевидения происходила без искажений. Все сервисы интерактивного телевидения: IPTV, VoD работают корректно. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 6.3 Проверка производительности устройства в режиме маршрутизатора NAT c PPPoE, при просмотре ТВ канала с HD качеством и одновременной работой Torrent клиента по беспроводному соединению.

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка производительности услугами Общества | |
| Конфигурация | Проверка требований к производительности при функцонально-нагрузочном тестировании FTTB | |
| Процедура | 1. Подключить ноутбук по беспроводному соединению к SSID1 (2.4 ГГц);  2. Скачивать Torrent файлы с ноутбука подключенного по Wi-Fi;  3. Запустить просмотр ТВ канала в HD качестве на приставке, подключенной к порту LAN2;  4. Зафиксировать скорость передачи Torrent файлов;  5. Во время работы приложения проверить работоспособность сервисов интерактивного телевидения   переключение каналов;   работа VoD;   функции VoD: “перемотка”, паузы более 5 мин.  6. Переподкключить ноутбук | |
| Ожидаемый результат | Во время нагрузочного тестирования скорость Torrent клиента достигала не менее 300 Мбит/с, при этом трансляция телевидения происходила без искажений. Все сервисы интерактивного телевидения: IPTV, VoD работают корректно. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 6.4 Проверка производительности устройства в режиме маршрутизатора NAT c PPPoE, при просмотре ТВ канала с HD качеством через соединение мост с тегами VLAN и одновременной работой Torrent клиента. Проверка изоляции групп.

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка производительности услугами Общества | |
| Конфигурация | Проверка требований к производительности при функцонально-нагрузочном тестировании FTTB | |
| Процедура | 1. Скачивать Torrent файлы с ноутбука подключенного к порту LAN1;  2. Запустить просмотр ТВ канала в HD качестве на приставке, подключенной к порту LAN4;  3. Зафиксировать скорость передачи Torrent файлов;  4. Во время работы приложения проверить работоспособность сервисов интерактивного телевидения   переключение каналов;   работа VoD;   функции VoD: “перемотка”, паузы более 5 мин.  5. Захватить пакеты на WAN интерфейсе, убедиться в соответствии пакетов бридж группе. | |
| Ожидаемый результат | Во время нагрузочного тестирования скорость Torrent клиента достигала не менее 300 Мбит/с, при этом трансляция телевидения происходила без искажений. Все сервисы интерактивного телевидения: IPTV, VoD работают корректно. В захваченном трафике отсутствуют пакеты из другой бридж группы. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

# 7 Проверка требований к производительности беспроводного модуля

## 7.1 Проверка доступных для конфигурации параметров

|  |  |  |
| --- | --- | --- |
| Цель теста | Предварительная проверка возможности конфигурации и проверка конфигурации по умолчанию. | |
| Конфигурация | без схемы | |
| Процедура | Multi-SSID выключен;  Возможность включения/отключения интерфейса Wi-Fi через web интерфейс (отдельно для каждого диапазона);  Основной SSID настроен на автоматический выбор канала;  Любой SSID можно включить/отключить не зависимо друг от друга;  Каждый SSID имеет уникальный MAC;  Мощность передатчика выставлена на максимальное значение;  Режим работы 802.11b/g/n (для 2.4 МГц) и 802.11a/n/ac (для 5ГГц);  Ширина канала: Auto (доступно для выбора 20, 40, 20/40 для 2.4МГц и 20, 40, 80, 20/40/80 для 5ГГц);  Функция WMM включена;  Присутствуют функции точной настройки Wi-Fi (Beacon, Preamble) | |
| Ожидаемый результат | Выполнение всех пунктов. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 7.2 Проверка производительности беспроводного соединения между интерфейсами WLAN и LAN в диапазоне 2.4 ГГц

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка производительности беспроводного модуля | |
| Конфигурация | Схема беспроводного подключения FTTB | |
| Процедура | 1. Подключить компьютер к беспроводной сети SSID1 (2.4 ГГц) с помощью функции WPS;  2. Настроить передачу трафика между зондами, подключенными к интерфейсам LAN и к беспроводной сети;  3. Загрузить конфигурацию Unidirect\_UDP-50Mbps\_TCP-Unlim.tst в консоли Ixia IxChariot;  4. Запустить потоки Pair 1-3 в течении 5 минут;  5. Зафиксировать среднее значение производительности во вкладке Throughput, параметр Average (Mbps);  6. Изменить направление трафика в конфигурации, поменяв местами параметры Endpoint 1 address и Endpoint 2 address конфигурацию Unidirect\_UDP-50Mbps\_TCP-Unlim.tst в консоли Ixia IxChariot;  7. Запустить потоки Pair 1-3 в течении 5 минут;  8. Зафиксировать среднее значение производительности во вкладке Throughput, параметр Average (Mbps);  9. Загрузить конфигурацию Bidirect\_UDP-30Mbps\_TCP-Unlim.tst в программном обеспечении Ixia Console;  10. Запустить потоки Pair 1-4 в течении 5 минут;  11. Зафиксировать среднее значение производительности во вкладке Throughput, параметр Average (Mbps). | |
| Ожидаемый результат | Скорость передачи трафика во всех направлениях не менее 90 Мбит/с. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 7.3 Проверка производительности беспроводного соединения между интерфейсами WLAN и LAN в диапазоне 5 ГГц

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка производительности беспроводного модуля | |
| Конфигурация | Схема беспроводного подключения FTTB | |
| Процедура | 1. Подключить компьютер к беспроводной сети SSID5 (5.0 ГГц) с помощью функции WPS;  2. Настроить передачу трафика между зондами, подключенными к интерфейсам LAN и к беспроводной сети;  3. Загрузить конфигурацию Unidirect\_UDP-100Mbps\_TCP-Unlim.tst в консоли Ixia IxChariot;  4. Запустить потоки Pair 1-3 в течении 5 минут;  5. Зафиксировать среднее значение производительности во вкладке Throughput, параметр Average (Mbps);  6. Изменить направление трафика в конфигурации, поменяв местами параметры Endpoint 1 address и Endpoint 2 address конфигурацию Unidirect\_UDP-50Mbps\_TCP-Unlim.tst в консоли Ixia IxChariot;  7. Запустить потоки Pair 1-3 в течении 5 минут;  8. Зафиксировать среднее значение производительности во вкладке Throughput, параметр Average (Mbps);  9. Загрузить конфигурацию Bidirect\_UDP-50Mbps\_TCP-Unlim.tst в программном обеспечении Ixia Console;  10. Запустить потоки Pair 1-4 в течении 5 минут;  11. Зафиксировать среднее значение производительности во вкладке Throughput, параметр Average (Mbps). | |
| Ожидаемый результат | Скорость передачи трафика в downstream не менее 250 Мбит/с для диапазона 5 ГГц. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 7.4 Проверка производительности беспроводного соединения при работе в двух диапазонах.

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка производительности беспроводного модуля | |
| Конфигурация | Схема беспроводного подключения FTTB | |
| Процедура | 1. Подключить ПК1 к беспроводной сети SSID1 (2.4 ГГц);  2. Подключить ПК2 к беспроводной сети SSID1 (5 ГГц);  3. Настроить передачу трафика между зондами, подключенными к интерфейсам LAN и к беспроводной сети;  4. Загрузить конфигурацию Unidirect\_UDP-50Mbps\_TCP-Unlim.tst в консоли Ixia IxChariot;  5. Загрузить конфигурацию Unidirect\_UDP-100Mbps\_TCP-Unlim.tst в консоли Ixia IxChariot.  6. Запустить потоки Pair 1-4 в течении 5 минут;  7. Зафиксировать среднее значение производительности во вкладке Throughput, параметр Average (Mbps);  8. Изменить направление трафика в конфигурации, поменяв местами параметры Endpoint 1 address и Endpoint 2 address конфигурацию Unidirect\_UDP-50Mbps\_TCP-Unlim.tst в консоли Ixia IxChariot;  9. Запустить потоки Pair 1-4 в течении 5 минут;  10. Зафиксировать среднее значение производительности во вкладке Throughput, параметр Average (Mbps);  11. Загрузить конфигурацию Bidirect\_UDP-30Mbps\_TCP-Unlim.tst в программном обеспечении Ixia Console;  12. Загрузить конфигурацию Bidirect\_UDP-50Mbps\_TCP-Unlim.tst в программном обеспечении Ixia Console;  13. Запустить потоки Pair 1-8 в течении 5 минут;  14. Зафиксировать среднее значение производительности во вкладке Throughput, параметр Average (Mbps). | |
| Ожидаемый результат | Скорость передачи трафика во всех направлениях не менее 90 Мбит/с (250 Мбит/с для диапазона 5 ГГц). | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 7.5 Проверка физических параметров беспроводной сети

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка физических характеристик точки доступа | |
| Конфигурация | Схема беспроводного подключения FTTB | |
| Процедура | 1. Захватить пакеты радиоэфира ПО Acrilyc или аналогичным в диапазоне 2.4 ГГц и 5.0 ГГц ;  2. Проанализировать пакеты Beacon Frames от точки доступа | |
| Ожидаемый результат | В заголовках 802.11 содержится информация:  1. Интервал Beacon соответствует настроенному значению (около 100 мс по умолчанию);  2. Режим Powersave отключён;  3. Возможность приёма LongPreamble;  4. Поддержка Short GI для ширины канала 20/40 МГц для 2.4 ГГц и 80 МГц для 5 ГГц (Если есть 5 ГГц);  5. Количество Spatial Stream для 2.4 ГГц и 5.0 ГГц – не менее 2x Spatial Stream;  6. Поддержка Beamforming (SU-MIMO) для 5.0 ГГц. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 7.6 Проверка работоспособности режимов (2.4 ГГц).

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка работоспособности автоматического выбора беспроводного стандарта  Максимально возможной скорости подключения.  Управление шириной канала | |
| Конфигурация | Схема беспроводного подключения FTTB | |
| Процедура | 1. Настроить IP-Host1 в режиме PPPoE;  2. Настроить беспроводную точку доступа Test\_1 в режиме 802.11n only;  3. Настроить ширину канала 40 Mhz;  4. Убедиться при помощи программы InSSIDer что вещание идет в нужном режиме;  5. Подключиться к Test\_1;  6. Проверить доступ к ресурсам;  7. Настроить беспроводную точку доступа Test\_1 в режиме Mixed;  8. Подключить клиента в режиме 802.11n;  9. Подключить клиента в режиме 802.11g only;  10. Подключиться к Test\_1.  11. Запустить игру World of Tanks | |
| Ожидаемый результат | В режиме 802.11n only клиент подключается на максимальной скорости 300 Мбит/с, в режиме Mixed клиент 802.11n подключаются на максимальной скорости, клиент 802.11g на скорости 54 Мбит/с. Приложение World of Tanks работает корректно. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 7.7 Проверка работоспособности режимов (5 ГГц).

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка работоспособности автоматического выбора беспроводного стандарта  Максимально возможной скорости подключения.  Управление шириной канала | |
| Конфигурация | Схема беспроводного подключения FTTB | |
| Процедура | 1. Настроить IP-Host1 в режиме PPPoE;  2. Настроить беспроводную точку доступа Test\_1\_5 (5 ГГц) в режиме 802.11ac only;  3. Настроить ширину канала 80 Mhz;  4. Убедиться при помощи программы InSSIDer что вещание идет в нужном режиме;  5. Подключиться к Test\_1\_5 (5 ГГц);  6. Проверить доступ к ресурсам;  7. Настроить беспроводную точку доступа Test\_1\_5 в режиме Mixed;  8. Подключить клиента в режиме 802.11n;  9. Подключить клиента в режиме 802.11ac;  10. Подключиться к Test\_1\_5. | |
| Ожидаемый результат | В режиме 802.11ac only клиент подключается на максимальной скорости 866 Мбит/с, в режиме Mixed клиенты 802.11ac подключаются на скорости 866 Мбит/с, клиенты 802.11n подключаются на скорости 300 Мбит/с. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 7.8 Проверка работоспособности Multicast по WiFi (2.4 ГГц) при соединении PPPoE

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка передачи Multicast трафика по беспроводному соединению. | |
| Конфигурация | Схема беспроводного подключения FTTB | |
| Процедура | 1. Настроить IP-Host1 в режиме PPPoE с IGMP Proxy;  2. Подключиться к беспроводной сети Test\_1;  3. Запустить просмотр ТВ канала в HD качестве на ноутбуке, подключенном к Test\_1 (2.4 ГГц) и телевизоре, подключенном к LAN3. | |
| Ожидаемый результат | Телевизионная трансляция по беспроводному соединению и через LAN идёт без искажений. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 7.9 Проверка работоспособности Multicast по WiFi (5 ГГц) c максимальной утилизацией частоты 2.4 ГГц.

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка передачи Multicast трафика по беспроводному соединению | |
| Конфигурация | Схема беспроводного подключения FTTB | |
| Процедура | 1. Настроить IP-Host1 в режиме PPPoE с IGMP Proxy;  2. Подключиться ПК к беспроводной сети Test\_1 (2.4 ГГц);  3. Подключиться ПК к беспроводной сети Test\_1\_5 (5 ГГц);  4. Запустить просмотр ТВ канала в HD качестве на ноутбуке, подключенном к Test\_1\_5 (5 ГГц) и телевизоре, подключенном к LAN3;  5. Запустить проверку скорости на сайте speedtest.net на компьютере, подключенном к Test\_1 (2.4 ГГц);  6. Запустить проверку скорости на сайте speedtest.net на компьютере, подключенном к Test\_1\_5 (5 ГГц);  7. Запустить закачку Торрент файла на компьютере, подключенном к Test\_1 (2.4 ГГц);  8. Во время работы Torrent проверять переключение каналов;  9. Зафиксировать скорость торрента. | |
| Ожидаемый результат | Телевизионная трансляция по беспроводному соединению и через LAN идёт без искажений. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 7.10 Проверка количества клиентов на SSID

|  |  |  |
| --- | --- | --- |
| Цель теста | Максимальное количество клиентов на SSID | |
| Конфигурация | Схема беспроводного подключения FTTB | |
| Процедура | 1. Подключиться к беспроводной сети Test\_1 при помощи 15 разных клиентов;  2. Проверить доступность интернет;  3. Повторить для диапазона 5ГГц.  Примечание:  Подключиться к беспроводной сети Test\_1 и Test\_1\_5 с ПК и мобильных устройств с разными операционными системами (Android, IOS, Windows phone) | |
| Ожидаемый результат | Все 15 клиентов получили доступ в интернет. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 7.11 Проверка ограничения количества клиентов на SSID

|  |  |  |
| --- | --- | --- |
| Цель теста | Ограничение клиентов на SSID | |
| Конфигурация | Схема беспроводного подключения FTTB | |
| Процедура | 1. Выставить ограничение подключения к беспроводной сети Test\_2 до 1 клиента;  2. Подключиться к беспроводной сети Test\_2;  3. Подключиться вторым клиентом к беспроводной сети Test\_2;  4. Повторить для диапазона 5ГГц. | |
| Ожидаемый результат | Срабатывает ограничение, второй клиент не может подключиться беспроводной сети SSID2. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 7.12 Проверка управления передатчиком

|  |  |  |
| --- | --- | --- |
| Цель теста | Управление мощностью беспроводного модуля и каналами вещания. | |
| Конфигурация | Схема беспроводного подключения FTTB | |
| Процедура | 1. Запустить анализатор радио эфира (программное обеспечение insider или аналог);  2. Изменить мощность беспроводного модуля;  3. Проверить изменения на анализаторе;  4. Проверить что в списке каналов для диапазона 2.4 доступно 13 каналов. Выбрать канал №13;  5. Проверить что в списке каналов для диапазона 5 ГГц доступны каналы с 36 по 64 (допустимый диапазон частот 5150-5350 МГц) и с 132 по 165 (5650~5850 МГц). Выбрать канал №64, установить ширину канала 80 МГц;  6. Проверить изменения на анализаторе.  7. Установить автоматический выбор каналов на обоих диапазонах  Пункт 5 выполняется при наличии на устройстве 5 ГГц. | |
| Ожидаемый результат | После применения изменений мощности беспроводного передатчика происходит соответствующее изменение уровня сигнала на анализаторе эфира. Шаг уменьшения мощности передатчика равен 20%. Все каналы, разрешенные в РФ, доступны. Выбрать канал, не разрешенный в РФ – нельзя. При выборе крайнего канала из диапазона вещание происходит в заданных рамках (для 2.4 ГГц – 2400:2483 (МГц), для 5 ГГц – 5150:5350 и 5650:5850 МГц).  При автоматическом выборе участвуют только каналы 1-11 в 2,4 ГГц и 36-64 в 5 ГГц. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 7.13 Проверка Wi-Fi радара

|  |  |  |
| --- | --- | --- |
| Цель теста | Отображение в радиусе действия всех активных беспроводных сетей.  Автоматический выбор менее загруженного канала | |
| Конфигурация | Схема беспроводного подключения FTTB | |
| Процедура | 1. Запустить Wi-Fi радар на устройстве и просмотреть все доступные точки доступа;  2 Перейти на вкладку настроек Wi-Fi, выбрать автоматический выбор канала Wi-Fi;  3 Убедиться, что устройство для испытания автоматически выбрало наименее зашумленный канал работы;  4 Убедиться в возможности просмотра всех доступных Wi-Fi сетей в рабочем диапазоне;  5 Повторить для диапазона 5ГГц. | |
| Ожидаемый результат | Выбран наименее зашумленный канал. Через web-интерфейс можно просматривать все доступные WiFi сети. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 7.14 Проверка изоляции пользователей в одном SSID

|  |  |  |
| --- | --- | --- |
| Цель теста | Изоляция клиентов в пределах одного SSID, для предотвращения доступности клиентов в гостевом Wi-Fi | |
| Конфигурация | Схема беспроводного подключения FTTB | |
| Процедура | 1 Настроить изоляцию пользователей на Test\_2;  2 Подключиться к Test\_2 двумя пользователями, используя в качестве профиля безопасности «Домашняя сеть»;  3 Проверить связность с помощью команды ping.  4 Повторить для диапазона 5ГГц | |
| Ожидаемый результат | При включении функции изоляции пользователей, доступ между беспроводными клиентами не возможен | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 7.15 Проверка работоспособности SSID3 и SSID4

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка работоспособности Multi-SSID | |
| Конфигурация | Схема беспроводного подключения FTTB | |
| Процедура | 1. Настроить на SSID3 открытую сеть через TR069. Убедится через webUI что сеть стала без шифрования  2. Подключится с ПК к Test\_3 (2.4 ГГц), убедится что получен IPv4 адрес  3. Подключится с ПК к Test\_4 или Test\_4\_5, убедится что получен IPv4 и IPv6 адрес.  4. Запустить измерение скорости на сервисе speedtest.net | |
| Ожидаемый результат | При подключении к SSID3 и SSID4 получены корректные IP адреса. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 7.16 Оценка производительности с разными типами устройств.

|  |  |  |
| --- | --- | --- |
| Цель теста | Оценка производительности с разными типами устройств. | |
| Конфигурация | без схемы | |
| Процедура | 1. Расположить испытуемые устройства на расстоянии 1 метр от CPE;  2. Подключить по очереди каждое из устройств из списка ниже к SSID работающему в 2,4 Ггц;  3. Произвести на каждом устройстве измерение speedtest.net не менее 10 раз с сервером Rostelecom Moscow и занести полученный результат в таблицу.  4. Подключить по очереди каждое из устройств из списка ниже к SSID работающему в 5 Ггц;  5. Произвести на каждом устройстве измерение speedtest.net не менее 10 раз с сервером Rostelecom Moscow и занести полученный результат в таблицу;  6. Перенести CPE на удаление 10 метров от испытуемых устройств;  7. Повторить пункты 2-5 | |
| Ожидаемый результат | Данную таблицу перенести в протокол, если данный пункт выполняется.  Название устройства 2,4 ГГц 5 ГГц  Downstream Upstream Downstream Upstream  IPAD 8  Iphone 11  Samsung Galaxy Tab  Samsung S20  Honor 30  Honor 30 Pro  Samsung A51  Samsung A11  Xiaomi Mi Note 10 Lite  Xiaomi Redmi 9a | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 7.17 Тестирование WPS

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка работы WPS на устройстве FTTB Expert | |
| Конфигурация | Схема беспроводного подключения FTTB mesh | |
| Процедура | Когда устройство является обычным CPE роутером:  1. Подключиться к SSID "Test\_1" через короткое зажатие кнопки WPS  2. Подключиться к SSID "Test\_5\_1" через короткое зажатие кнопки WPS  Когда из устройств собрана MESH-сеть:  3. Подключиться к SSID "Test\_1" через короткое зажатие кнопки WPS  4. Подключиться к SSID "Test\_5\_1" через короткое зажатие кнопки WPS  5. Запустить перебор WPS PIN | |
| Ожидаемый результат | Пункты 1-4 клиент подключается к WiFi  Пункт 5 - не удалось подобрать PIN | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

# 8 Проверка качества обслуживания (QoS) и аппаратных очередей

## 8.1 Проверка очередей Upstream

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка аппаратных очередей в исходящем направлении | |
| Конфигурация | Проверка качества обслуживания (QoS) и аппаратных очередей | |
| Процедура | 1. Настроить IP-Host1 в режиме PPPoE;  2. Настроить QoS на устройстве для испытания следующим образом через TR069.  3. На основе MAC адреса (высший приоритет), назначение маркировки DSCP (40);  4. На основе Dest IP (высокий приоритет);  5. На основе входящей DSCP (28) метки (средний приоритет) маркировка DSCP – 12, 802.p – 2;  6. На основе порта LAN3 (низший приоритет), маркировка DSCP – 0.  Параметр, по которому производится приоритезация может быть изменен (проверить наличие выбора в Web-интерфейс):  ☐ Connection Type;  ☐ Network Interface;  ☐ MAC;  ☐ IP;  ☐ Hostname;  ☐ DSCP/ToS Value;  ☐ Port Number;  7. Подключить порт трафик генератора (TG-1) к порту WAN через коммутатор;  8. Подключить порты трафик генератора к портам: Lan1-4;  9. Загрузить на трафик генераторе профиль QoS\_Upstream.tcc;  10. Подключить SIP Phone к порту LAN4;  11. Запустить трафик в течении 5 минут  Поток 1 на Lan1 с фиксированным MAC адресом источника, скорость 1 Мбит/с, DSCP метка 20;  Поток 2 на Lan2 скорость 0,2 от 1000 Мбит/с, DSCP метка 20;  Поток 3 на Lan3 скорость 1000 Мбит/с, DSCP метка 20  Поток 4 на Lan4 скорость 0,5 от 1000 Мбит/с, DSCP метка 28, pbit=0.  12. Захватить трафик на WAN интерфейсе.  13. Убедиться, что трафик от SIP клиента на WAN имеет необходимую маркировку и приоритезируется.  14. Повторить пп. 7-13, настроив IP-Host1 в режиме PPPoE для трафика Internet и IP-Host2 в режиме IPoE для трафика VoIP. IP-Host1 и IP-Host2 находятся в одной группе и настроены в режиме Access (без VLAN тэга). | |
| Ожидаемый результат | Настройки в webUi соответствуют переданным по TR069  При разговоре отсутствуют искажения голоса при использовании FXS.  Приоритетный трафик проходит без потерь.  Трафик, поданный с меткой DSCP 28, допускаются незначительные потери.  Трафик, поданный на Lan3 - допускаются большие потери.  На захваченном трафике видно, что происходит маркировка исходящего трафика в соответствии с установленными правилами. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 8.2 Управление полосой пропускания.

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка ограничения скорости Upstream | |
| Конфигурация | Проверка качества обслуживания (QoS) и аппаратных очередей | |
| Процедура | 1. Настроить тип подключения к Интернет в режиме PPPoE;  2. Подключить порты трафик генератора (TG-2, TG-4) к портам: Lan1, Lan3;  3. Подключить STB и убедится, что IPTV работает корректно;  4. Установить общее ограничение скорости upstream 0,2 от 1000 Мбит/с;  5. Загрузить на трафик генераторе профиль QoS\_DSCP.tcc;  6. Запустить трафик;  7. Убедиться, что суммарная скорость прохождения равна заданному значению скорости;  8. Убрать общее ограничение скорости;  9. Установить ограничение скорости на основе Dest IP в размере 0,2 от 1000 Мбит/с;  10. Запустить трафик;  11. Убедиться, что в потоке, на который было установлено ограничение проходит только заданное значение скорости. | |
| Ожидаемый результат | Скорость Upstream соответствует установленным ограничениям. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

# 9 Управление устройством

## 9.1 Проверка установки соединения с ACS при наличии только PPPoE

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка алгоритма загрузки устройства при первом включении  Проверка работоспособности агента TR-069 | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Сбросить устройство к заводским установкам;  2. Подключить устройство к виртуальной сети с активным PPPoE сервером;  3. Убедится в установке соединения PPPoE;  4. Настроить через TR069 UntagPPP+UntagBr+TagBr+UntagVOIP(если применимо);  5. Открыть в браузере произвольный адрес;  6. Запланировать вызов RPC-Метода GetRPCMethods на ACS; | |
| Ожидаемый результат | Устройство установило соединение с PPPoE сервером, успешно зарегистрировалось на ACS сервере по адресу http://acs.rt.ru с отправкой Bootsrap сообщения. Для входящих и исходящих сообщений используется интерфейс PPPoE. Все сервисы созданы.  Все запросы от CPE маркированы DSCP = 56.  Для входящих запросов используется порт tcp 7547.  X\_RTK\_ServiceType для PPPoE равен 1 | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.2 Проверка установки соединения с ACS PPPoE и IPoE с 43 опцией

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка алгоритма загрузки устройства при первом включении  Проверка работоспособности агента TR-069 | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Сбросить устройство к заводским установкам;  2. Подключить устройство к виртуальной сети с активным PPPoE и DHCP сервером на котором настроена выдача option 43 (без option 3);  3. Убедится в установке соединения PPPoE и IPoE;  4. Убедиться что устройство содержит одну bridge группу с индексом 0 и именем default  5. Осуществить попытку connection request с PPPoE соединения.  6. Настроить через TR069 UntagPPP+UntagBr+TagBr+TagVOIP(если применимо);  7. Открыть в браузере произвольный адрес;  8. Запланировать попытку обновления ПО.  9. Осуществить попытку Connection request с IP адреса, отличного от переданного в option 43 | |
| Ожидаемый результат | Устройство установило соединение с PPPoE и IPoE сервером, успешно зарегистрировалось на ACS сервере по адресу, переданному в DHCP option 43, с отправкой Bootsrap сообщения. Для входящих и исходящих сообщений используется интерфейс IPoE. Все сервисы созданы.  X\_RTK\_ServiceType для PPPoE равен 1, для IPoE - 2  Для обновления ПО используется интерфейс для TR069.  CPE отвечает на Connection request с IP адреса, отличного от переданного в option 43 | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.3 Проверка установки соединения с ACS PPPoE и IPoE с 43 опцией и DGW

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка алгоритма загрузки устройства при первом включении  Проверка работоспособности агента TR-069 | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Сбросить устройство к заводским установкам;  2. Подключить устройство к виртуальной сети с активным PPPoE и DHCP сервером на котором настроена выдача option 43, 3, 42;  3. Убедится в установке соединения PPPoE и IPoE;  4. Осуществить попытку connection request с PPPoE соединения.  5. Убедиться в синхронизации времени с сервером, полученном в option 42 через IPoE.  6. Настроить через TR069 UntagPPP+UntagBr+TagBr+UntagVOIP(если применимо);  7. Открыть в браузере произвольный адрес;  8. Осуществить попытку Connection request с IP адреса, отличного от переданного в option 43 | |
| Ожидаемый результат | Устройство установило соединение с PPPoE и IPoE сервером, успешно зарегистрировалось на ACS сервере по адресу, переданному в DHCP option 43, с отправкой Bootsrap сообщения. Для входящих и исходящих сообщений используется интерфейс IPoE. Все сервисы созданы.  X\_RTK\_ServiceType для PPPoE равен 1, для IPoE - 2  Время синхронизируется через IPoE соединение  CPE отвечает на Connection request с IP адреса, отличного от переданного в option 43 | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.4 Проверка установки соединения с ACS PPPoE и IPoE

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка алгоритма загрузки устройства при первом включении  Проверка работоспособности агента TR-069 | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Сбросить устройство к заводским установкам;  2. Подключить устройство к виртуальной сети с активным PPPoE и DHCP сервером на котором настроена выдача option 3;  3. Убедится в установке соединения PPPoE и IPoE;  4. Осуществить попытку connection request с IPoE соединения.  5. Убедиться в синхронизации времени с сервером, заданным по умолчанию, через PPPoE.  6. Настроить через TR069 UntagPPP+UntagBr+TagBr+UntagVOIP(если применимо);  7. Открыть в браузере произвольный адрес;  8. Перенести признак TR069 на IPoE;  9. Убедиться в синхронизации времени с сервером, заданным по умолчанию, через PPPoE.  10. Настроить NTP через TR069;  11. Запланировать попытку обновления ПО. | |
| Ожидаемый результат | Устройство установило соединение с PPPoE и IPoE сервером, успешно зарегистрировалось на ACS сервере по адресу http://acs.rt.ru с отправкой Bootsrap сообщения. Для входящих и исходящих сообщений используется интерфейс PPPoE. Все сервисы созданы.  X\_RTK\_ServiceType для PPPoE равен 1, для IPoE - 1  Время синхронизируется сначала через PPPoE соединение  После переноса интерфейса TR069 на IPoE, TR069 работает только через IPoE, время синхронизируется через PPPoE.  После конфигурации NTP - через интерфейс TR069  Для обновления ПО используется интерфейс для TR069. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.5 Проверка установки соединения с ACS IPoE с 43 опцией и DGW

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка алгоритма загрузки устройства при первом включении  Проверка работоспособности агента TR-069 | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Сбросить устройство к заводским установкам;  2. Подключить устройство к виртуальной сети с активным DHCP сервером на котором настроена выдача option 43, 3;  3. Убедится в установке соединения IPoE;  4. Настроить через TR069 UntagBr+TagBr+UntagVOIP(если применимо);  5. Открыть в браузере произвольный адрес; | |
| Ожидаемый результат | Устройство установило соединение с IPoE сервером, успешно зарегистрировалось на ACS сервере по адресу, переданному в DHCP option 43, с отправкой Bootsrap сообщения. Для входящих и исходящих сообщений используется интерфейс IPoE. Все сервисы созданы.  X\_RTK\_ServiceType для IPoE - 3 | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.6 Проверка установки соединения с ACS IPoE

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка алгоритма загрузки устройства при первом включении  Проверка работоспособности агента TR-069 | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Сбросить устройство к заводским установкам;  2. Подключить устройство к виртуальной сети с активным DHCP сервером на котором настроена выдача option 3;  3. Убедится в установке соединения IPoE;  4. Настроить через TR069 UntagBr+TagBr+UntagVOIP(если применимо);  5. Открыть в браузере произвольный адрес; | |
| Ожидаемый результат | Устройство установило соединение с IPoE сервером, успешно зарегистрировалось на ACS сервере по адресу http://acs.rt.ru с отправкой Bootsrap сообщения. Для входящих и исходящих сообщений используется интерфейс IPoE. Все сервисы созданы.  X\_RTK\_ServiceType для IPoE - 1 | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.7 Проверка установки соединения с ACS IPoE с 43 опцией

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка алгоритма загрузки устройства при первом включении  Проверка работоспособности агента TR-069 | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Сбросить устройство к заводским установкам;  2. Подключить устройство к виртуальной сети с активным DHCP сервером на котором настроена выдача option 43;  3. Убедится в установке соединения IPoE;  4. Настроить через TR069 TagPPP+UntagBr+TagBr+TagVOIP(если применимо);  5. Открыть в браузере произвольный адрес;  6. Запланировать попытку обновления ПО.  7. Осуществить попытку Connection request с IP адреса, отличного от переданного в option 43 | |
| Ожидаемый результат | Устройство установило соединение с IPoE сервером, успешно зарегистрировалось на ACS сервере по адресу, переданному в DHCP option 43, с отправкой Bootsrap сообщения. Для входящих и исходящих сообщений используется интерфейс IPoE. Все сервисы созданы.  X\_RTK\_ServiceType для IPoE - 2  Для обновления ПО используется интерфейс для TR069.  CPE отвечает на Connection request с IP адреса, отличного от переданного в option 43 | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.8 Проверка установки соединения с ACS при наличии только PPPoE в ЦСМ

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка алгоритма загрузки устройства при первом включении  Проверка работоспособности агента TR-069 | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Сбросить устройство к заводским установкам;  2. Подключить устройство к виртуальной сети с активным PPPoE сервером;  3. Убедится в установке соединения PPPoE;  4. Настроить через TR069 Сервис ЦСМ (в режиме PPPoE) и Сервис ЦСМ FXS для всех голосовых портов (если применимо);  5. Открыть в браузере произвольный адрес;  6. Убедиться в успешной регистрации всех настроенных голосовых портов (если применимо);  7. Произвести модификацию сервисов;  8. Открыть в браузере произвольный адрес;  9. Убедиться в успешной регистрации всех настроенных голосовых портов (если применимо).  10. Сбросить устройство к заводским установкам;  11. Убедиться в успешном восстановлении всех сервисов. | |
| Ожидаемый результат | Устройство установило соединение с PPPoE сервером, успешно зарегистрировалось на ACS сервере по адресу http://acs.rt.ru с отправкой Bootsrap сообщения. Для входящих и исходящих сообщений используется интерфейс PPPoE. Все сервисы созданы. Все лишние соединения удалены. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.9 Проверка установки соединения с ACS PPPoE и IPoE в ЦСМ

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка алгоритма загрузки устройства при первом включении  Проверка работоспособности агента TR-069 | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Сбросить устройство к заводским установкам;  2. Подключить устройство к виртуальной сети с активным PPPoE и IPoE сервером;  3. Убедится в установке соединений IPoE и PPPoE;  4. Настроить через TR069 Сервис ЦСМ (в режиме PPPoE) и Сервис ЦСМ FXS для всех голосовых портов (если применимо);  5. Открыть в браузере произвольный адрес;  6. Убедиться в успешной регистрации всех настроенных голосовых портов (если применимо);  7. Произвести модификацию сервисов;  8. Открыть в браузере произвольный адрес;  9. Убедиться в успешной регистрации всех настроенных голосовых портов (если применимо).  10. Сбросить устройство к заводским установкам;  11. Убедиться в успешном восстановлении всех сервисов. | |
| Ожидаемый результат | Устройство установило соединение с PPPoE и IPoE сервером, успешно зарегистрировалось на ACS сервере по адресу http://acs.rt.ru с отправкой Bootsrap сообщения. Для входящих и исходящих сообщений используется интерфейс PPPoE. Все сервисы созданы. Все лишние соединения удалены. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.10 Проверка установки соединения с ACS IPoE в ЦСМ

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка алгоритма загрузки устройства при первом включении  Проверка работоспособности агента TR-069 | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Сбросить устройство к заводским установкам;  2. Подключить устройство к виртуальной сети с активным IPoE сервером;  3. Убедится в установке соединения IPoE;  4. Настроить через TR069 Сервис ЦСМ (в режиме IPoE) и Сервис ЦСМ FXS для всех голосовых портов (если применимо);  5. Открыть в браузере произвольный адрес;  6. Убедиться в успешной регистрации всех настроенных голосовых портов (если применимо);  7. Произвести модификацию сервисов;  8. Открыть в браузере произвольный адрес;  9. Убедиться в успешной регистрации всех настроенных голосовых портов (если применимо).  10. Сбросить устройство к заводским установкам;  11. Убедиться в успешном восстановлении всех сервисов. | |
| Ожидаемый результат | Устройство установило соединение с IPoE сервером, успешно зарегистрировалось на ACS сервере по адресу http://acs.rt.ru с отправкой Bootsrap сообщения. Для входящих и исходящих сообщений используется интерфейс IPoE. Все сервисы созданы. Все лишние соединения удалены. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.11 Выполнение тест плана ATP-069

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка соответствия TR агента рекомендациям BBF | |
| Конфигурация | Управление устройством | |
| Процедура | Оборудование  ACS Сервер Axiros  Подробное описание тест плана находится по ссылке: http://www.broadband-forum.org/technical/download/ATP-069.pdf  Процедура  1. Настроить любой тип подключения к Интернет;  2. Запустить на ACS сервере выполнение тест плана ATP-069. | |
| Ожидаемый результат | Все процедуры выполнены без ошибок:  Тест 1 (BBF 5.7). Начало и завершение сессии  Тест 2 (BBF 5.8). Session\_Initiation\_and\_Termination\_With\_no\_RPC  Тест 3 (BBF 5.15). ACS изменяет URL  Тест 4 (BBF 5.17). Параметры, изменяемые ACS, не создают Inform-событие "4 VALUE CHANGE" в ACS  Тест 5 (BBF 5.19). Соединение после запроса соединения  Тест 6 (BBF 5.20). Connection\_Request\_while\_session\_exists  Тест 7 (BBF 5.21). Соединение после PeriodicInformInterval  Тест 8 (BBF 5.22). Connection\_Establishment\_using\_SSL\_30  Тест 9 (BBF 5.23). Сonnection\_Establishment\_using\_TLS\_10  Тест 10 (BBF 5.24). Connection\_Establishment\_using\_TLS\_12  Тест 11 (BBF 5.25). Common\_Name\_certificate\_validation  Тест 12 (BBF 5.27). Использование множественных cookie между транзакциями в сессии  Тест 13 (BBF 5.28). Восстановление сессии  Тест 14 (BBF 5.29). SOAP\_Response\_HTTP\_Request  Тест 15 (BBF 5.30). HTTP\_Redirection\_Test\_302\_Redirect  Тест 16 (BBF 5.31). HTTP\_Redirection\_Test\_307\_Redirect  Тест 17 (BBF 5.32). HTTP\_Redirection\_Multiple\_Redirections  Тест 18 (BBF 5.33). HTTPS\_with\_URL\_Matching\_Certificate  Тест 19 (BBF 5.34). HTTPS\_with\_URL\_Certificate\_Mismatch  Тест 20 (BBF 5.35). Redirection\_at\_any\_Point\_in\_a\_Session  Тест 21 (BBF 5.36). HTTP\_Redirection\_Use\_of\_session\_cookies  Тест 22 (BBF 5.37). Redirect\_HTTP\_Response\_Contains\_Data  Тест 23 (BBF 5.38). HTTP-аутентификация - Базовая аутентификация  Тест 24 (BBF 5.39). Qop\_Authentication\_setting  Тест 25 (BBF 5.40). HTTP-аутентификация - Дайджест аутентификация  Тест 26 (BBF 5.41). Maximum\_SOAP\_Message\_Size  Тест 27 (BBF 5.42). Формат сообщения о сбое SOAP в методе SetParameterValues  Тест 28 (BBF 5.43). Метод GetRPCMethods и обязательные RPC-методы  Тест 29 (BBF 5.44). Метод GetParameterNames – Полный путь  Тест 30 (BBF 5.45). Метод GetParameterNames – Полный путь, NextLevel=true  Тест 31 (BBF 5.46). Метод GetParameterNames – Неполный путь, NextLevel=true  Тест 32 (BBF 5.47). Метод GetParameterNames – Неполный путь, NextLevel=false  Тест 33 (BBF 5.48). Метод GetParameterNames – Недопустимый путь  Тест 34 (BBF 5.49). Метод GetParameterNames – Вся объектная модель  Тест 35 (BBF 5.50). Метод GetParameterValues – Простой полный путь  Тест 36 (BBF 5.51). Метод GetParameterValues – Несколько полных путей  Тест 37 (BBF 5.52). Метод GetParameterValues – Неполный путь  Тест 38 (BBF 5.53). Метод GetParameterValues – Полные и неполные пути  Тест 39 (BBF 5.54). Метод GetParameterValues – Вся объектная модель  Тест 40 (BBF 5.55). Метод GetParameterValues – Условие ошибки  Тест 41 (BBF 5.56). Метод SetParameterValues – Одиночный параметр  Тест 42 (BBF 5.57). Метод SetParameterValues – Несколько параметров  Тест 43 (BBF 5.58). Метод SetParameterValues – Использование одного параметра несколько раз  Тест 44 (BBF 5.59). Метод SetParameterValues – Тестирование атомарности  Тест 45 (BBF 5.60). GetParameterAttributes\_Complete\_Path  Тест 46 (BBF 5.61). GetParameterAttributes\_Multiple\_Complete\_Paths  Тест 47 (BBF 5.62). GetParameterAttributes\_Partial\_Path  Тест 48 (BBF 5.63). GetParameterAttributes\_Complete\_and\_Partial\_Path  Тест 49 (BBF 5.64). GetParameterAttributes\_Invalid\_Parameter\_Name  Тест 50 (BBF 5.65). GetParameterAttributes\_Partial\_Path\_empty  Тест 51 (BBF 5.66). SetParameterAttributes\_Active\_Notifications  Тест 52 (BBF 5.67). SetParameterAttributes Active Notifications Persistence  Тест 53 (BBF 5.68). SetParameterAttributes\_Atomic  Тест 54 (BBF 5.69). SetParameterAttributes\_Passive\_Notification Complete Path  Тест 55 (BBF 5.70). SetParameterAttributes\_Passive\_Notification Partial Path  Тест 56 (BBF 5.71). SetParameterAttributes\_Passive\_Notification Complete and Partial Path  Тест 57 (BBF 5.72). SetParameterAttributes\_Disable\_Notification  Тест 58 (BBF 5.73). SetParameterAttributes\_Incorrect\_Parameter\_Name  Тест 59 (BBF 5.75). Метод AddObject – Условия ошибки  Тест 60 (BBF 5.77). Метод DeleteObject – Условия ошибки  Тест 61 (BBF 5.78). Метод Reboot  Тест 62 (BBF 5.79). Перезагрузка вручную  Тест 63 (BBF 5.80). Download\_Test\_Basic\_Version\_Upgrade  Тест 64 (BBF 5.81). Download\_Test\_Queuing  Тест 65 (BBF 5.82). Download\_Test\_Delay  Тест 66 (BBF 5.83). Download\_Test\_Retry  Тест 67 (BBF 5.84). CancelTransfer  Тест 68 (BBF 5.85). Upload  Тест 69 (BBF 5.86). Upload\_Queuing  Тест 70 (BBF 5.87). Upload\_Delay  Тест 71 (BBF 5.88). Тест метода ScheduleInform  Тест 72 (BBF 5.89). FactoryReset  Тест 73 (BBF 5.90). Ошибки CWMP – Ошибки базовых RPC-методов  Тест 74 (BBF 5.91). CWMP\_Faults\_Download\_Failure  Тест 75 (BBF 5.92). CWMP\_Faults\_Upload\_Failure  Тест 76 (BBF 5.93). Запуск диагностики  Тест 77 (BBF 5.94). GetAllQueuedTranfers  Тест 78 (BBF 5.95). Проверка префиксов пространств имен XML  Тест 79 (BBF 5.97). DUT\_properly\_encodes\_and\_decodes\_XML\_entities  Тест 80 (BBF 5.100). EnableCWMP\_set\_to\_false  Тест 81 (BBF 5.101). Изменение имени пользователя и пароля ACS  Тест 82 (BBF 5.102). PeriodInformEnable включает периодические Inform-сообщения  Тест 83 (BBF 5.103). PeriodicInformTime\_in\_The\_Past\_Controls Periodic Inform  Тест 84 (BBF 5.104). PeriodicInformTime\_in\_the\_future\_controls periodic Inform  Тест 85 (BBF 5.106). Параметры Inform-сообщения должны соответствовать DeviceInfo  Тест 86 (BBF 5.107). Периодичность отправки Inform-сообщений при сетевой недоступности ACS-сервера | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.12 Проверка поддержки дерева параметров CPE

|  |  |  |
| --- | --- | --- |
| Цель теста | Получение дерева всех параметров доступных для чтения или записи по TR-069 | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Настроить любой тип подключения к интернет;  2. Запланировать вызов RPC-Метода GetParameterValues “InternetGatewayDevice.” | |
| Ожидаемый результат | Устройство успешно зарегистрировалось на ACS сервере, при Connection Request получено все дерево параметров «InternetGatewayDevice.» с устройства. Минимальный перечень приведен в Приложении №1.  Полученная информация соответствует информации на шильде устройстве и обязательно содержит  • логотип Ростелеком и адрес www.rt.ru;  • Модель;  • H/W версия;  • Серийный номер (Длина не менее 16 символов, должен состоять из букв и цифр, не может начинаться с "0");  • MAC адрес LAN;  • Логин/пароль пользовательской учетной записи;  • Адрес для доступа к web (http://rt/ и http://192.168.0.1);  • Данные для подключения WiFi;  • Параметры блока питания;  Полученная информация соответствует информации в webUI устройстве и обязательно содержит  • S/N устройства  • Версия оборудования  • Производитель оборудования  • MAC адрес устройства  • Модель устройства также равна полю ProductClass  • Версия ПО устройства  • Текущее значение датчика температуры.  • Загрузка ЦПУ, ОЗУ, ПЗУ (%) на текущий момент.  • IMEI (если применимо) | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.13 Обновление ПО устройства

|  |  |  |
| --- | --- | --- |
| Цель теста | Обновление программного обеспечения посредством CWMP | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Настроить любой тип подключения к интернет  2. Загрузить на HTTP сервер новую версию ПО, отличную от установленной на устройстве;  3. Запланировать метод Download с аргументами:  "URL": "<путь к файлу прошивки>",  "TargetFileName":<имя файла>"",  "FileType": "1 Firmware Upgrade Image",  "FileSize": <размер файла в байтах>,  "DelaySeconds": 0,  "CommandKey": <уникальное значение>""  В случае если тестируется очередная версия ПО, то проверить обновление с последней рекомендованной версии ПО. | |
| Ожидаемый результат | • Для загрузки файла был использован интерфейс назначенный основным для работы TR агента;  • На RPC метод Download устройство отвечает Download Response с кодом 1;  • Устройство выполняет загрузку и обновление ПО;  • Во время обновления устройство изменило светодиодную индикацию согласно требованиям;  • После обновления ПО в INFORM сообщение включаются параметры "7 TRANSFER COMPLETE" и "M Download" информация о версии из того же сообщения содержит значение НОВОЙ версии прошивки;  • ACS получил RPC-метод TransferComplete, который означает, что загрузка прошла успешно;  • Значение аргумента CommandKey в методе TransferComplete такое же, как в вызываемом RPC методе Download для события "M Download" и не для события "7 TRANSFER COMPLETE". | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.14 Сохранение/обновление конфигурации.

|  |  |  |
| --- | --- | --- |
| Цель теста | Сохранение/обновление конфигурационного файла посредством CWMP | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Подключить устройство к сети;  2. Внести какие либо изменения в конфигурацию устройства;  3. Запланировать метод Upload с аргументами:  "Username": "<Имя пользователя>",  "URL": "<Путь к файлу>",  "CommandKey": "AXESS CONFIG UPLOAD",  "DelaySeconds": 0,  "Password": "<Пароль>",  "FileType": "1 Vendor Configuration File"  4. Выполнить сброс до заводских настроек посредством CWMP  5. Запланировать метод Download с аргументами  "Username": "<Имя пользователя>",  "TargetFileName": "<Имя файла>",  "FailureURL": "",  "URL": "<Адрес сервера>",  "CommandKey": "AXESS CONFIG DOWNLOAD",  "FileSize": 0,  "SuccessURL": "",  "DelaySeconds": 5,  "Password": "<Пароль>",  "FileType": "3 Vendor Configuration File" | |
| Ожидаемый результат | • На метод Upload получен ответ UploadResponse;  • Выполнена передача файла по указанному адресу;  • Если отправка файла выполнена после завершении сессии, следующий INFORM содержит “7 TRANSFER COMPLETE” и “M Upload”;  • На ACS отправлен метод TransferComplete cо значением CommandKey, указанным в RPC-метод Upload;  • Ответ устройства FactoryResetResponse;  • Устройство обнулилось до заводской конфигурации;  • При следующем INFORM устройство шлёт “0 BOOTSTRAP”.  • На RPC метод Download устройство отвечает Download Response с кодом 1;  • Устройство выполняет загрузку и обновление конфигурации;  • Во время обновления устройство изменило светодиодную индикацию согласно требованиям;  • После обновления конфигурации INFORM сообщение включаются параметры «7 TRANSFER COMPLETE” и “M Download”  • ACS получил RPC-метод TransferComplete, который означает, что загрузка прошла успешно;  • Значение аргумента CommandKey в методе TransferComplete такое же, как в вызываемом RPC методе Download для события «M Download» и не для события «7 TRANSFER COMPLETE». | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.15 Настройка параметров PPPoE соединения

|  |  |  |
| --- | --- | --- |
| Цель теста | Изменение параметров настройки PPPoE соединения | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Сбросить устройство к заводским настройкам;  2. Подключить устройство к сети с PPPoE c доступом к ACS серверу;  3. Запланировать вызов RPC-метода GetParameters.InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.  4. Запланировать вызов RPC-метода SetParameter, где указать необходимые параметры для изменения | |
| Ожидаемый результат | • Устройство успешно установило соединение с ACS сервером.  • После конфигурации устройство приняло параметры и установило соединение с BRAS;  • Параметры WANPPPConnection имеют обязательные для конфигурации поля:  Enable (enable/disable)  Username (login) - возможно задать пустой  Password (password) - возможно задать пустой  PPPLCPEchoRetry  PPPLCPEcho  IdleDisconnectTime (0, 120)  ConnectionTrigger (AlwaysOn, OnDemand)  ConnectionType (IP\_Routed)  X\_RTK\_IGMPProxy | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.16 Управление беспроводными соединениями

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка возможности управлять беспроводными соединениями. | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Настроить любой тип подключения к Интернет;  2. Используя функцию connection request запросить с устройство значения ноды InternetGatewayDevice.LANDevice.1.WLANConfiguration;  3. Посредством CWMP выключить беспроводной WiFi модуль;  4. Посредством CWMP выключить одно SSID;  5. Посредством CWMP изменить название сети (SSID), пароль, тип шифрования (WPA, WPA2, WPA/WPA2), тип ключа (TKIP, AES, TKIP/AES), ширина, мощность передатчика и канал;  6. Посредством CWMP включить беспроводной WiFi модуль. | |
| Ожидаемый результат | Имеется возможность выключать беспроводной модуль и менять его параметры/ Все измененные параметры корректно отображаются в webUI | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.17 Управление учётными записями

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка возможности смены пароля администратора | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Настроить любой тип подключения к Интернет;  2. Посредством CWMP изменить пароль администратора используя «InternetGatewayDevice.LANConfigSecurity.ConfigPassword.»  3. Проверить, что пароль изменился, для этого осуществить подключение к устройству через webUI и Telnet с новым паролем. | |
| Ожидаемый результат | Пароль успешно изменен | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.18 Диагностика устройства

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка возможности снятия статистики устройства и обнаружения неисправностей | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Настроить тип подключения PPPoE;  2. Убедиться в регистрации устройства на ACS сервере;  3. Запросить устройство информацию о подключенных клиентах;  3. Запросить устройство информацию о подключенных клиентах на wifi;  4. Запросить статистики переданных пакетах с WAN/LAN/WLAN;  5. Запросить состояние и конфигурацию встроенного DHCP сервера;  6. Выполнить тест IPPingDiagnostics;  7. Выполнить тест TraceRoute;  8. Выполнить тест IPPingUDPDiagnostics;  9. Выполнить тест IPPingUDP+Diagnostics.  10. Запросить дерево InternetGatewayDevice.Layer3Forwarding.  11. Добавить произвольный маршрут через TR069  12. Запросить информацию о физическом WAN интерфейсе. | |
| Ожидаемый результат | Получены MAC адреса подключенных клиентах (включая клиентов со статическим IP и работающие в bridge);  Получена статистика с интерфейсов WAN/LAN/WLAN;  Получена информация о настройках LAN и DHCP сервера.  Получена информация о задержке.  Получена текущая таблица маршрутизации  Получен доступ через добавленный маршрут  Получена информация о физическом WAN интерфейсе | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.19 Download тест

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка возможности проведения диагностики загрузки DownloadDiagnostics. | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Настроить тип подключения к Интернет - PPPoE. Интерфейс для TR069 - IPoE.  2. Посредством процедуры SetParameterValues выставить значение параметра InternetGatewayDevice.DownloadDiagnostics.DiagnosticsState 'Requested', параметра InternetGatewayDevice.DownloadDiagnostics.DownloadURL – ссылку на скачиваемый файл.  3. Дождаться выполнения теста устройством и события DIAGNOSTICS COMPLETE.  4. Запросить ноду InternetGatewayDevice.DownloadDiagnostics. с результатами теста. | |
| Ожидаемый результат | Тест успешно выполнен, устройство вернуло правильные данные. Скачивание производилось через PPPoE. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.20 Upload тест

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка возможности проведения диагностики выгрузки UploadDiagnostics. | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Настроить тип подключения к Интернет - PPPoE. Интерфейс для TR069 - IPoE.  2. Посредством процедуры SetParameterValues выставить значение параметра InternetGatewayDevice.UploadDiagnostics.DiagnosticsState 'Requested', параметра InternetGatewayDevice.DownloadDiagnostics.UploadURL – путь для выгрузки, параметра InternetGatewayDevice.UploadDiagnostics.TestFileLength – длину выгружаемого файла.  3. Дождаться выполнения теста устройством и события DIAGNOSTICS COMPLETE.  4. Запросить ноду InternetGatewayDevice.UploadDiagnostics. с результатами теста. | |
| Ожидаемый результат | Тест успешно выполненен, устройство вернуло правильные данные. Отдача производилось через PPPoE | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.21 DeviceLog тест

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка возможности получения лога устройства. | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Настроить любой тип подключения к Интернет.  2. Посредством процедуры GetParameterValues получить значение параметра InternetGatewayDevice.DeviceInfo.DeviceLog | |
| Ожидаемый результат | Содержимое лог файла успешно получено. Полученный лог имеет структуру  yyyy-mm-dd hh:mm:ss [type] message yyyy-.........  yyyy-mm-dd дата события в таком формате  hh:mm:ss время события в таком формате  [type] тип события, который может принимать следующие значения  emerg  alert  crit  error  warning  notice  info  debug  message само событие, которое произошло | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.22 Диагностика WiFi Radar

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка возможности получения информации о точках доступа в радиоэфире 2.4 ГГц и 5.0 ГГц | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Настроить любой тип подключения к Интернет.  2. Запустить сбор информации о точках доступа в радиоэфире;  3. Убедится что получена информация о всех точках доступа (канал, BSSID, SSID, тип шифрования, мощность, ширина) | |
| Ожидаемый результат | Отображены все точки с указанием необходимой информации (Приложение №1) | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 9.23 Настройка удаленного доступа

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка настройки удаленного доступа через CWMP | |
| Конфигурация | Управление устройством | |
| Процедура | 1. Настроить любой тип подключения к Интернет;  2. Выполнить процедуру настройки удаленного доступа;  3. Проверить работу.  4. Выполнить процедуру настройки ICMP на одном из WAN соединений;  5. Проверить работу, убедиться что на соединении где ICMP не разрешено устройство не отвечает на PING. | |
| Ожидаемый результат | Устройство применило полученную конфигурацию (Пример в Приложении №1).  Доступ со стороны WAN к telnet(ssh), webUI получен. Устройство отвечает со стороны WAN на Ping на выбранном интерфейсе | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

# 10 Проверка функционала

## 10.1 Проверки функционала ALG

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверки функционала ALG | |
| Конфигурация | Проверка функционала | |
| Процедура | 1. Проверить прием файла размером 1 Гбайт по протоколу FTP (активный режим передачи);  2. Подключить к порту LAN2 SIP-телефон с настроенной учетной записью SIP;  3. Выполнить входящий и исходящий вызов. Проверить прохождение пакетов SIP, RTP и RTCP при помощи анализатора сетевого трафика; | |
| Ожидаемый результат | Скорость передачи трафика по FTP не менее 800 Мбит/с. Тестовый вызов выполнен успешно. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 10.2 Проверки функционала UPnP

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверки функционала UPnP | |
| Конфигурация | Проверка функционала | |
| Процедура | 1. Сконфигурировать устройство в любом режиме доступа к Интернет;  2. На компьютере подключенном к LAN1 запустить любой сервис, требующий входящего соединения. Например Telnet сервер;  3. С помощью ПО miniupnpc создать UPnP правило проброса портов на порт 23 upnpc -a <IP адрес компьютера> 23 9022 tcp;  4. Установить соединение с другого компьютера, подключенного к интернет на порт 9022;  5. Удалить правило upnpc -d 9022 tcp.  6. Запустить miniupnpc со стороны WAN, убедиться что правила не создаются. | |
| Ожидаемый результат | Правила успешно создаются и удаляются. Со стороны WAN UPnP не работает. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 10.3 UDP\_to\_HTTP\_proxy

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверки функционала UDP to HTTP proxy | |
| Конфигурация | Проверка функционала | |
| Процедура | 1. Сконфигурировать устройство в любом режиме доступа к Интернет;  2. Сконфигурировать на устройстве через TR069 параметры proxy (буфер 64512 кБ/с);  3. Подключить STB с поддержкой UDP proxy к устройству;  4. Убедиться в работе TV не менее 10 мин.  5. Вынуть WAN Кабель из роутера и оценить время работы ТВ  6. Восстановить WAN подключение и убедиться что ТВ работает  7. Сконфигурировать на устройстве через TR069 параметры proxy (буфер 32256 кБ/с)  8. Убедиться в работе TV не менее 10 мин.  9. Вынуть WAN Кабель из роутера и оценить время работы ТВ | |
| Ожидаемый результат | Устройство успешно сконфигурировано, присутствуют все поля для конфигурации. Конфигурация в webUi соответствует переданной по TR069. Время работы ТВ в п.9 уменьшилось примерно в 2 раза | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 10.4 Проверка функций PPTP/L2TP/IPSec pass-through

|  |  |  |
| --- | --- | --- |
| Цель теста | Трансляция протоколов семейства IP через NAT | |
| Конфигурация | Проверка функционала | |
| Процедура | 1. Настроить любой из типов подключения;  2. Подключить компьютер с IPSec, L2TP и PPTP клиентом;  3. Установить соединение с PPTP сервером;  4. Проверить работоспособность тоннеля и завершить соединение;  5. Установить соединение IPSec;  6. Проверить работоспособность  7. Установить соединение с L2TP сервером;  8. Проверить работоспособность тоннеля и завершить соединение; | |
| Ожидаемый результат | Туннельные сессии устанавливаются, трансляция протоколов ESP и GRE возможна. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 10.5 Проверка Port Mapping / NatLoopback

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка Port Mapping/NatLoopback(Reverse NAT) | |
| Конфигурация | Проверка функционала | |
| Процедура | 1. Настроить любой тип подключения к интернету;  2. В локальной сети настроить FTP сервер в пассивном режиме c адресом 192.168.0.50 и порт TCP 21;  3. Создать правило Port Forwarding средствами TR069, при срабатывании которого, пакеты, приходящие на WAN интерфейс и порт 7700, направляются на FTP сервер. С компьютера в локальной сети с адресом 192.168.0.70 получить доступ к FTP серверу по адресу WAN:7700 и скачать тестовый файл;  4. С компьютера во внешней сети с адресом WAN получить доступ к FTP серверу по адресу WAN:7700 и скачать тестовый файл;  5. Убедиться, что созданное правило корректно отражено в webUI;  6. Сделать ограничение по входящему IP;  7. Попытаться с компьютера во внешней сети получить доступ к FTP серверу по адресу WAN:7700. | |
| Ожидаемый результат | Пакеты IP успешно передаются в рамках сессии, установленной с компьютеров в сети WAN и LAN на FTP сервер. При установленном ограничении по входящему IP получить доступ к FTP возможно только с разрешенного IP. При задании диапазона внешних портов проброс осуществляется 1:1 на внутренние. Т.е. если задан внешний диапазон 5000-6000 а внутренний 10000 то ожидаем что проброс будет 10000-11000 | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 10.6 Проверки функционала шифрования пароля

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверки функционала шифрования пароля | |
| Конфигурация | Проверка функционала | |
| Процедура | 1. Получить доступ к web интерфейсу при помощи любого браузера (например, Internet Explorer, Mozilla Firefox, Google Chrome или Safari);  2. Перейти на вкладку с настройкой WAN соединений и открыть соединение PPPoE;  3. Открыть просмотр исходного кода страницы, убедиться, что значение поля «пароль» находится в зашифрованном виде;  4. Сохранить текущую конфигурацию устройства в файл;  5. Открыть файл конфигурации при помощи текстового редактора (Например, Notepad). Если конфигурационный файл имет текстовую структуру plain/text, значения полей «имя пользователя» и «пароль» PPPoE, а также «имя пользователя» и «пароль» для доступа к CPE находятся в зашифрованном виде. Настроек сервера TR-069, SIP (в случае наличия Phone портов) и QoS нет в конфигурационном файле.  6. Изменить адрес acs сервера.  7. Загрузить сохраненный конфиг. | |
| Ожидаемый результат | Пароли для доступа PPPoE и web интерфейс хранятся в зашифрованном виде. Если конфигурационный файл имеет текстовую структуру plain/text в нем нет Настроек QoS/ACS и Phone. Если файл имеет зашифрованную структуру он не должен иметь настроек TR069. После обновления старого конфига, устройство управляется с ACS. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 10.7 Проверки алгоритма установления PPPoE сессии

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверки алгоритма установления PPPoE сессии | |
| Конфигурация | Проверка функционала | |
| Процедура | 1. Устройство настроено для работы в интернет - PPPoE, для TR069 - IPoE  2. На коммутаторе настраивается режим зеркалирования WAN интерфейса устройства для испытания;  3. На устройстве для испытания настроить соединение PPPoE connect on-demand с заданным интервалом (проверить возможность установки таймера до 600 секунд);;  4. Анализатором сетевого трафика зафиксировать процесс установления соединения и убедиться что устройство отвечает на LCP запросы сервера;  5. Убедиться что при отсутствии активности через заданный интервал времени (Time-out) устройство закрывает PPPoE сессию;  6. Возобновить сетевую активность и убедиться, что устройство восстановило PPPoE соединение с другим BRAS;  7. Отключить PPPoE сервер;  8. Убедиться, что устройство отправляет LCP запросы раз в 30 секунд, не позже чем через 5 минут завершает PPPoE сессию и начинает установку новой.  9. Сравнить с целевой блок схемой процесс установки | |
| Ожидаемый результат | При выборе Connect on Demand устройство корректно завершает сессию при отсутствии сетевой активности через заданный интервал времени и при возобновлении активности восстанавливает соединение с интернетом.  Процесс установления соединения соответствует схеме | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 10.8 Проверка резервного хранения образа программного обеспечения и параметров конфигурации в энергонезависимой памяти

|  |  |  |
| --- | --- | --- |
| Цель теста | Устройство не принимает к обновлению прошивки с некорректной CRC суммой и выводит соответствующее сообщение.  После возобновления питания CPE не должно потерять работоспособность и конфигурацию. | |
| Конфигурация | Проверка функционала | |
| Процедура | 1. Подключить консольный кабель;  2. С помощью Hex-редактора внести изменения в прошивку.  3. Запустить обновление модифицированного ПО;  4. Перезагрузить устройство;  5. Запустить обновление рабочего ПО  6. Во время записи ПО в flash кратковременно отключить питание CPE;  7. Включить питание CPE, убедится, что CPE восстанавливает ПО из резервной области;  8. Запустить обновление ПО, убедится, что после успешного обновления ПО в основной области, ПО перезаписано в резервную область. | |
| Ожидаемый результат | Проверка резервного хранения образа программного обеспечения и параметров конфигурации в энергонезависимой памяти | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 10.9 Проверка работоспособности Wizard

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка работоспособности Wizard | |
| Конфигурация | Проверка функционала | |
| Процедура | 1. Сбросить устройство к заводским установкам;  2. Подключить устройство к сегменту сети с PPPoE или DHCP сервером без доступа к ACS серверу http://acs.rt.ru;  3. Подключить ПК по Wi-Fi с помощью технологии WPS или кабелем;  4. Открыть браузер и отрыть произвольную страницу, например, rt.ru; | |
| Ожидаемый результат | Пользователь переадресован на страницу конфигурации, где были выполнены следующие действия:  - Произведена проверка срабатывания перехвата сообщений о неисправностях  - Произведён выбор профиля согласно региону;  - При необходимости введены учётные данные от пользователя, При запросе учетных данных, старые не отображаются, если пользователь ничего не ввел – выводится ошибка;  - Произведена настройка WiFi;  - Выведено сообщение об успешной конфигурации устройства.  Тест считается завершенным, если после завершения работы Wizard устройство получило доступ к настроенным услугам и конфигурация сохранилась. Из каждого окна Wizard`а есть возможность перейти в ручные настройки.  Профили всех регионов в приложении №4 | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 10.10 Проверка работоспособности Trouble wizard

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка работоспособности Trouble wizard  (Вывод сообщений о неподключенном кабеле) | |
| Конфигурация | Проверка функционала | |
| Процедура | 1. Настроить подключение к Интернет вручную или через мастера установки соединения;  2. Открыть любой сайт;  3. Отключить провод Ethernet от WAN порта устройства;  4. Открыть любой другой сайт или перейти по внешней ссылке на странице;  5. Проверить работу алгоритма;  6. Проверить возможность выхода в настройки устройства (при переходе устройство должно запросить пароль); | |
| Ожидаемый результат | Обращение пользователя перехвачено и выведено информационное сообщение о неподключенном кабеле. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 10.11 Проверка доступа к устройству

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка доступа к устройству | |
| Конфигурация | Проверка функционала | |
| Процедура | 1. Убедиться, что PC получил IPv4/IPv6 адреса;  2. Открыть в браузере адрес http://RT;  3. Открыть в браузере адрес http://192.168.0.1 (где 192.168.0.1 – LAN IP адрес CPE);  4. Открыть в браузере адрес http://[IPv6 LAN адрес CPE]  5. Открыть webUI и скопировать прямую ссылку на мастер настройки и выйти из webUI.  6. Открыть данную ссылку в браузере, убедиться что доступ не возможен без авторизации. | |
| Ожидаемый результат | Браузер отрывает страницу управления устройством во всех пунктах. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 10.12 Доступность управления со стороны WAN

|  |  |  |
| --- | --- | --- |
| Цель теста | Доступность управления со стороны WAN | |
| Конфигурация | Проверка функционала | |
| Процедура | 1. Проверить, что управление устройством со стороны WAN по умолчанию запрещено;  2. Просканировать сканнером nmap IP адрес устройства;  3. Попытаться получить доступ к любому локальному клиенту и webUI CPE по IPv6 адресу (GUA);  4. Убедиться, что в настройках присутствует возможность ограничения доступа со стороны WAN по диапазону IP адресов, портам. Включить управление Telnet/Web со стороны WAN с определенного диапазона IP по определенному порту;  5. Запустить анализатор трафика.  6. Убедиться, что в настройках есть возможность включать/выключать ICMP на любом WAN соединении. Проверить работоспособность.  7. Зайти на Telnet (с парой login/password инженера)/Web по внешнему адресу и назначенному порту. Попытаться зайти по другому порту, убедиться, что доступ не возможен. Попытаться зайти с IP адреса не из указанного диапазона, убедиться, что доступ не возможен. Убедиться, что требование к сложности пароля «инженера» соблюдены;  8. Зайти на telnet с парой login/password пользователя, убедиться, что доступ не возможен. | |
| Ожидаемый результат | При запрещенном управлении со стороны WAN сканнер должен сообщить, что все порты закрыты. После разрешения управления с интерфейса доступ к управлению получен. При Web авторизации пароль передается в зашифрованном виде. Доступ к локальным клиентам и webUI по локальным IPv6 адресам не возможен. Пароль инженера является уникальным для каждой CPE. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 10.13 Привилегии пользователей

|  |  |  |
| --- | --- | --- |
| Цель теста | Привилегии пользователей | |
| Конфигурация | Проверка функционала | |
| Процедура | Устройство должно обладать наличием разных уровней конфигурации. Точное дерево конфигурации для разных пользователей определяется в профиле. Минимальный набор, который должен быть не доступен под уровнем доступа admin: TR-069, QoS, VoIP (за исключением статуса регистрации SIP), возможность изменять WAN соединения с признаками VOIP/TR в любой комбинации.  1. Авторизироваться под пользователем superadmin;  2. Проверить доступность всех пунктов меню, заявленных производителем;  3. Авторизироваться на устройстве под пользователем admin.  4. Проверить отсутствие пунктов меню, в соответствии с Приложение №3.  5. Изменить пароль пользователя superadmin через webUI;  6. Проверить пункты 1-2 с новым и старым паролем;  7. Изменить пароль пользователя admin через webUI на 123, убедиться в выдаче сообщения о недопустимости пароля;  8. Изменить пароль пользователя admin через webUI на надежный;  9. Проверить пункты 3-4 с новым и старым паролем; | |
| Ожидаемый результат | При использования уровня доступа superadmin возможно просматривать и изменять все параметры устройства, при использовании уровня доступа admin доступ к ресурсам и конфигурации ограничен (не доступны для настройки меню TR-069,QoS и VoIP). Нет возможности изменять WAN соединения с признаками VOIP/TR в любой комбинации. Нет возможности включить telnet. Подробнее в Приложении. Пароли успешно заменены, при использовании не безопасного пароля выдается предупреждение.  Пароль admin: минимум 8 символов, одна маленькая буква, одна заглавная и одна цифра  Пароль superadmin: минимум 16 символов, одна маленькая буква, одна заглавная, одна цифра и спецсимвол | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 10.14 Проверка firewall

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка работы firewall по протоколам IPv4/v6 | |
| Конфигурация | Проверка функционала | |
| Процедура | 1. Сконфигурировать устройство для работы в интернет любым способом в режиме dual stack;  2. Проверить отсутствие поддержки протокола HNAP;  3. Проверить возможность создания списков доступа (ACL) c фильтрацией пакетов на основе:  • Номера протокола/поля «Next Header» в заголовке IPv4/6 пакета  • Номера порта  • IP-адреса источника/назначения  • MAC-адреса  4. Подключить со стороны LAN ПК с настроенным статическим адресом Ipv6 (префикс отличный от полученного на WAN) и Трафик генератор;  5. Осуществить ping на любой внешний сервер;  6. Настроить на ПК автоматическое получение адреса;  7. Обратиться из внешней сети к любому клиенту за CPE;  8. Сформировать на Трафик генераторе со стороны WAN последовательность Ipv6 пакетов с multicast адресом в поле source address;  9. Сформировать на Трафик генераторе со стороны LAN последовательность Ipv6 пакетов с multicast адресом в поле destination address;  10. Сформировать на Трафик генераторе со стороны WAN последовательность Ipv6 пакетов с Extension Header Routing Header Type 0 и 1. | |
| Ожидаемый результат | В CPE есть возможность cоздания списков ACL;  CPE не пропускает IPv6 пакеты пересылаемые из LAN в сторону WAN если в поле source address установлен IPv6 адрес отличный от префикса выданного по DHCPv6-PD;  Пакеты, поступающие с WAN, должны быть отброшены, кроме случая, когда они относятся к сессии, инициированной со стороны локальной сети (LAN/WLAN);  CPE должна обрасывать IPv6 пакеты с multicast адресом в поле source address;  CPE должна отбрасывать IPv6 пакеты с multicast адресом в поле destination address пересылаемые из LAN в направлении WAN;  CPE должна отбрасывать IPv6 пакеты с Extension Header Routing Header Type 0 и 1; | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 10.15 Проверка журналирования.

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка функционала журналирования на устройстве. | |
| Конфигурация | Проверка функционала | |
| Процедура | 1. Убедиться что режим журналирования включен по умолчанию, есть уровень debug и information;  2. Настроить через webUI возможность удаленного управления через web и telnet и осуществить вход;  3. Открыть журнал через webUI и убедиться что в наличии записей, содержащих:  • Дату и время  • Имя пользователя, под которым был осуществлен вход  • Протокол доступа (webUi, Telnet)  • интерфейс подключения (WAN/LAN/WLAN).  4. Изменить пароль для пользователя admin от admin, затем для обоих пользователей от superadmin;  5. Изменить пароль superamin через TR069;  6. Открыть журнал через webUI и убедиться что в наличии записей, содержащих:  • Дату и время  • Имя пользователя, пароль которой изменен  • Имя пользователя, кто изменил пароль  • Протокол доступа (webUi, Telnet, TR-069)  7. Изменить настройки NAT и/или ACL и обновить ПО;  8. Открыть журнал через webUI и убедиться что в наличии записей, содержащих:  • Дату и время  • Тип изменяемого объекта (NAT, FW, ACL)  • Имя пользователя, кто изменил  • Полный синтаксис правила после изменения  9. Журналированию подлежат только записи сделанные через webUI/Telnet;  10. Перезагрузить CPE;  11. Журнал должен быть доступен через Web и TR069. | |
| Ожидаемый результат | В журнале устройства присутствуют все необходимые записи, все записи перечисленные в данном пункте сохраняются в энергонезависимой памяти (по каждому типу не менее 100 событий). | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 10.16 Проверка фильтрации на основе «белого списка»

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка фильтрации на основе «белого списка» | |
| Конфигурация | Проверка функционала | |
| Процедура | 1. Включить режим фильтрации клиентов по MAC адресам (LAN клиентам) через веб интерфейс;  Примечание: также может быть настроена фильтрация на основе.  протокола, порта, IP-адреса источника/назначения, MAC-адреса.  2. Выбрать режим работы «белый список» т.е. доступ возможен только для клиентов из списка;  3. Внести тестовый ПК в данный список и авторизоваться на CPE;  4. Проверить доступность CPE (открыть web-интерфейс);  5. Попытаться подключиться с другого ПК (которого нет в белом списке) и убедиться что подключение не возможно. | |
| Ожидаемый результат | Выход в интернет возможен для устройств, внесенных в «белый список». Выход в интернет невозможен для устройств, не внесенных в «белый список». | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 10.17 Проверка фильтрации на основе «черного списка»

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка фильтрации на основе «черного списка» | |
| Конфигурация | Проверка функционала | |
| Процедура | 1. Включить режим фильтрации клиентов по MAC адресам (WiFi клиентам) через веб интерфейс;  Примечание: также может быть настроена фильтрация на основе.  протокола, порта, IP-адреса источника/назначения, MAC-адреса.  2. Выбрать режим работы «черный список» т.е. доступ для клиентов из списка запрещен. Внести тестовый ПК в данный список и попытаться авторизоваться на CPE, убедиться, что подключение не возможно. Подключиться с другого ПК (которого нет в черном списке) и проверить доступность CPE (открыть web-интерфейс);  3. Выполнить подключение с другого ПК (не из списка), убедиться что ПК подключился. | |
| Ожидаемый результат | Выход в интернет (авторизация клиента) невозможен для устройств, внесенных в «черный список». Выход в интернет возможен для устройств, не внесенных в «черный список». | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

# 11 Проверка требования к USB-порту и дополнительным приложениям

## 11.1 Проверка доступа SMB

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка доступа SMB | |
| Конфигурация | Проверка требования к USB-порту и дополнительным приложениям | |
| Процедура | Собрать стенд согласно схеме. Получить доступ к web-интерфейсу CPE. Далее все операции по настройке CPE выполняются через web-интерфейс.  1. Запустить просмотр HD канала на ТВ приставке;  2. Включить SMB для USB Flash Drive;  3. Проверить доступность файлов на USB Flash Drive с подключенного ПК; Проверить доступность необходимых файловых систем (FAT, FAT32, exFAT, NTFS) последовательным подключением USB Flash Drive с различными файловыми системами;  4. Проверить разграничение прав доступа по учетным записям (login, password);  5. По умолчанию должен быть открыт доступ anonymous (без авторизации);  6. Проверить доступность сервисов SMB/AFP на соответствующих операционных системах (Windows/Mac OS X);  7. Запустить передачу файлов (не менее 100Mb) по SMB c USB Flash Drive на ПК;  8. Запустить передачу файлов (не менее 100Mb) по SMB c ПК на USB Flash Drive. | |
| Ожидаемый результат | USB Flash Drive доступно по протоколу Samba. Скорость передачи/записи данных не менее 3 МБ/с  При включенном разграничении прав доступа, доступ к содержимому возможен только с соответствующем логином/паролем.  При передаче файлов с USB Flash Drive на ПК на изображении не наблюдается артефактов. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 11.2 Проверка DLNA

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка DLNA | |
| Конфигурация | Проверка требования к USB-порту и дополнительным приложениям | |
| Процедура | 1. Подключить USB накопитель;  2. Включить DLNA сервер для USB Flash Drive;  3. Создать группы мультимедиа-сервисов и разбить их по каталогам;  4. Проверить работоспособность сервиса с помощью TV. | |
| Ожидаемый результат | Индексация файлов занимает не более 5 минут  Контент USB Flash Drive доступен на TV. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

# 12 Проверка IPv4/IPv6 dualstack

## 12.1 Проверка работоспособности устройства в режиме DHCPv6/v4 клиента (statefull) и выделением адресов LAN через PD.

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка работоспособности устройства в режиме IPoE Dual Stack (stateful) | |
| Конфигурация | без схемы | |
| Процедура | 1. Настроить IPoE-интерфейс устройства в режиме v4 only;  2. Убедится в получении Ipv4 адреса;  3. Изменить значение ноды X\_RTK\_IP\_Version для данного соединения на 3;  4. Убедиться что IPoE-интерфейс устройства находится в режиме DualStack IPv6/v4;  5. Убедиться, что по умолчанию включен режим DHCPv6 PD;  6. Убедиться, что по умолчанию включен режим auto на DHCPv6;  7. Убедиться, что настроена выдача адресов на LAN в автоматическом режиме;  8. Подключить устройство к сети с настроенными сервисами:  a. DHCPv4/v6 сервер с выдачей адресов IANA и префикса IAPD;  b. ICMPv6 RA с установленными флагами M и O;  9. Проверить статус настройки через интерфейс управления устройства;  10. Проверить полученную конфигурацию на ПК и убедиться при помощи wireshark что выдача адресов происходит по SLAAC + DHCPv6;  11. Проверить связность по IPv6/v4 до внешнего сервера;  12. Проверить связность по IPv6/v4 до внешнего сервера с подключенного клиента пол WiFi;  13. Запустить передачу трафика с трафик генератора;  11. Переподключить WAN CPE и добиться получения нового префикса для PD.  12. Проверить полученную конфигурацию на ПК и убедиться при помощи wireshark что в RA старый префикс был передан с life time 0 и, следом, был выдан новый префикс в RA. Также по DHCPv6 клиент переполучил DNS; | |
| Ожидаемый результат | На странице статуса WebUI выведен назначенный адрес, DNS и делегированный префикс с маской /56 от DHCPv6 сервера, а также IPv6-адрес шлюза по умолчанию.  Аренда IANA и IAPD периодически обновляется (DHCPv6 Renew).  Локальный DHCPv6 сервер сконфигурирован согласно полученному префиксу PD и DNS.  LAN GUA назначен из пула PD с маской /64, ПК получает адрес и DNS от локального DHCPv6 в режиме stateless (DNS передаются через DHCPv6)  Трафик от ПК до внешних IPv4/v6 адресов успешно проходит во всех случаях.  Скорость при передаче Ipv6 трафика не менее 800 Мбит/с. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 12.2 Проверка работоспособности устройства в режиме SLAAC, получение адресов на LAN через DHCPv6PD

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка работоспособности устройства в режиме PPPoE Dual Stack (stateless) | |
| Конфигурация | без схемы | |
| Процедура | 1. Настроить PPPoE-интерфейс устройства в режиме v4 only;  2. Убедится в получении Ipv4 адреса;  3. Изменить значение ноды X\_RTK\_IP\_Version для данного соединения на 3;  4. Убедиться что PPPoE-интерфейс устройства находится в режиме DualStack IPv6/v4;  2. Убедиться, что по умолчанию включен режим DHCPv6 PD;  3. Убедиться, что по умолчанию включен режим auto на DHCPv6;  4. Убедиться, что настроена выдача адресов на LAN в автоматическом режиме;  5. Подключить устройство к сети с настроенными сервисами:  a. DHCPv4/v6 сервер с выдачей адресов IANA и префикса IAPD /56;  b. ICMPv6 RA с установленным флагом O;  6. Проверить статус настройки через интерфейс управления устройства;  7. Проверить полученную конфигурацию на ПК и убедиться при помощи wireshark что выдача адресов происходит по SLAAC + DHCPv6;  8. Проверить связность по IPv6/v4 до внешнего сервера;  9. Проверить связность по IPv6/v4 до внешнего сервера с подключенного клиента пол WiFi;  10. Запустить передачу трафика с трафик генератора;  11. Переподключить WAN CPE и добиться получения нового префикса для PD.  12. Проверить полученную конфигурацию на ПК и убедиться при помощи wireshark что в RA старый префикс был передан с life time 0 и, следом, был выдан новый префикс в RA. Также по DHCPv6 клиент переполучил DNS.  13. Повторить пункты 5-12 для IAPD /64. | |
| Ожидаемый результат | На странице статуса WebUI выведен назначенный адрес с маской /64 и делегированный префикс.  Аренда IAPD периодически обновляется (DHCPv6 Renew).  Локальный RADVD сервер сконфигурирован согласно полученному префиксу PD и DNS.  LAN GUA назначен из пула PD с маской /64, ПК получает IPv6 адрес.  Получен доступ от ПК до внешних IPv4/v6 адресов.  Скорость при передаче Ipv6 трафика не менее 800 Мбит/с | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

# 13 Проверка электропитания

## 13.1 Проверка параметров БП

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка параметров БП. | |
| Конфигурация | без схемы | |
| Процедура | 1. Измерить физические размеры посадочного места БП;  2. Измерить длину кабеля БП;  3. Проверить падение БП на пол;  4. Измерить выходное напряжение БП на самом блоке и на CPE при полной нагрузке, сравнить с номинальным;  5. Замкнуть выходные контакты БП между собой на 1 минуту, после размыкания измерить выходное напряжение;  6. Снять осциллограмму выходного напряжения БП. | |
| Ожидаемый результат | Размеры БП соответствуют указанным на схеме  Длина кабеля не мене 1.5 м;  Блок питания после падения нормально функционирует, корпус не имеет механических повреждений;  После снятия КЗ на выходе БП устройство функционирует;  Пульсации на выходе БП не более 200 мВ;  Падение на кабеле не более 0,1 В от напряжения на выходе БП  Выходное напряжение БП соответствует заявленному. | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

## 13.2 Проверка температурных рамок

|  |  |  |
| --- | --- | --- |
| Цель теста | Проверка температурных режимов. | |
| Конфигурация | без схемы | |
| Процедура | 1. Поместить испытуемую CPE в климатическую установку (допускается установка CPE на столе, если есть возможность контролировать температуру CPE и температуру воздуха).  2. Подключить CPE к сети с активным PPPoE сервером;  3. Убедиться в установке соединения с TR069 через PPPoE;  4. Подключить ПК по WiFi 5 ГГц (или 2,4 ГГц при отсутствии 5 ГГц)  5. Запустить передачу трафмка от/с ПК;  6. Установить внутри камеры +25 градусов, не менее чем на 8 часов;  7. Убедиться в нормальной работе CPE и непрерывной передачи трафика. | |
| Ожидаемый результат | В течении всего времени устройство нормально функционирует.  Температура на верхней крышке CPE не превышает 48 градусов (разница между температурой корпуса CPE и температурой воздуха не более 23 градусов). | |
| Tест пройден | | Тест не пройден |
| Комментарии |  | |

Схемы

## Схема беспроводного подключения FTTB

|  |  |
| --- | --- |
| Описание | Предварительная настройка оборудования для проведения испытаний беспроводного модуля |
| Схема |  |
| Используемое оборудование | 1. Консоль Ixia IxChariot;  2. Устройство для испытания;  3. Телевизионная приставка Ростелеком х 3 шт;  4. Коммутатор с поддержкой VLAN и доступом к СПД Общества;  5. ПК с интерфейсом 1000Base-TX;  6. ПК с двумя интерфейсами 802.11 a/b/g/n/ac (4x4). |
| Описание стенда | 1. Консоль Ixia IxChariot;  2. Устройство для испытания;  3. Телевизионная приставка Ростелеком х 3 шт;  4. Коммутатор с поддержкой VLAN и доступом к СПД Общества;  5. ПК с интерфейсом 1000Base-TX;  6. ПК с двумя интерфейсами 802.11 a/b/g/n/ac (4x4). |
| Настройка | 1. Сетевые интерфейсы CPE настроены и сгруппированы в соответствии с таблицей;  Интерфейс WAN Интерфейсы LAN Параметры Wi-Fi  N Тип VLAN Имя SSID Шифрование  IP\_Routed untagged LAN1-4 - -  SSID1 Test\_1 WPA2-PSK/AES  SSID5 Test\_1\_5 WPA2-PSK/AES  Bridge 251 SSID2 Test\_2 WPA2-PSK/AES  SSID6 Test\_2\_5 WPA2-PSK/AES  Bridge 1313 SSID3 Test\_3 WPA-PSK/AES  SSID7 Test\_3\_5 WPA-PSK/AES  Bridge 20 SSID4 Test\_4 Выкл.  SSID8 Test\_4\_5 Выкл.  2. LAN1-4 и SSID1 (в двух диапазонах) связаны с WAN в режиме маршрутизации с функцией NAT и локальным DHCP сервером;  3. Секретный ключ (PSK) для SSID1-3,5-7: 1234567890;  4. Для SSID2 и SSID6 включить режим изоляции клиентов;  5. Для SSID4 и SSID8 настроить ограничение скорости передачи в 2 Мбит/с. |
| Цель |  |

## Схема беспроводного подключения FTTB mesh

|  |  |
| --- | --- |
| Описание | Предварительная настройка оборудования для проведения испытаний беспроводного модуля |
| Схема | None |
| Используемое оборудование | 1. Консоль Ixia IxChariot;  2. Устройство для испытания;  3. 2 дополнительные точки доступа  4. Коммутатор с поддержкой VLAN и доступом к СПД Общества;  5. Ноутбук c беспроводным интерфейсом 802.11n (3x3);  6. 2 ПК с беспроводной картой 802.11 a/b/g/n/ac (3x3 или 4x4)  7. Телефон с поддержкой 802.11k, 802.11v, 802.11r. |
| Описание стенда | 1. Консоль Ixia IxChariot;  2. Устройство для испытания;  3. 2 дополнительные точки доступа  4. Коммутатор с поддержкой VLAN и доступом к СПД Общества;  5. Ноутбук c беспроводным интерфейсом 802.11n (3x3);  6. 2 ПК с беспроводной картой 802.11 a/b/g/n/ac (3x3 или 4x4)  7. Телефон с поддержкой 802.11k, 802.11v, 802.11r. |
| Настройка | 1. Сетевые интерфейсы CPE настроены и сгруппированы в соответствии с таблицей;  Интерфейс WAN Интерфейсы LAN Параметры Wi-Fi  N Тип VLAN Имя SSID Шифрование  IP\_Routed untagged LAN1-4 - -  SSID1 Test\_1 WPA2-PSK/AES  SSID5 Test\_5\_1 WPA2-PSK/AES    2. LAN1-4 и SSID1 (в двух диапазонах) связаны с WAN в режиме маршрутизации с функцией NAT и локальным DHCP сервером;  3. Секретный ключ (PSK) для SSID1-3,5-7: 1234567890; |
| Цель |  |

## Проверка функционала

|  |  |
| --- | --- |
| Описание | Проверка общей функциональности маршрутизатора |
| Схема |  |
| Используемое оборудование | 1. Коммутатор с поддержкой VLAN и доступом к СПД Общества;  2. SIP телефон, настроенный на работу в сети Общества;  3. Телевизионная приставка;  4. Телевизор;  5. Ноутбук и/или ПК с беспроводной картой 802.11n (2x2) 2шт. |
| Описание стенда | 1. Коммутатор с поддержкой VLAN и доступом к СПД Общества;  2. SIP телефон, настроенный на работу в сети Общества;  3. Телевизионная приставка;  4. Телевизор;  5. Ноутбук и/или ПК с беспроводной картой 802.11n (2x2) 2шт. |
| Настройка | Настройка интерфейсов  IP-Host 1 связан c Ethernet WAN в режиме PPPoE.  Настройка группировки  Lan1-4 связан с WAN интерфейсом в режиме маршрутизатора с функцией NAT и локальным DHCP сервером; |
| Цель |  |

## Управление устройством

|  |  |
| --- | --- |
| Описание | Предварительная настройка оборудования для проверки возможности конфигурации устройства по протоколу CWMP |
| Схема |  |
| Используемое оборудование | 1. ACS сервер Axiros;  2. Устройство для испытания;  3. Коммутатор с поддержкой VLAN и доступом к СПД Общества;  4. Ноутбук c беспроводным интерфейсом 802.11n (2x2); |
| Описание стенда | 1. ACS сервер Axiros;  2. Устройство для испытания;  3. Коммутатор с поддержкой VLAN и доступом к СПД Общества;  4. Ноутбук c беспроводным интерфейсом 802.11n (2x2); |
| Настройка | Настройка интерфейсов  1. Конфигурация устройства «по-умолчанию»  Настройка группировки  2. Конфигурация устройства «по-умолчанию» |
| Цель |  |

## Проверка требований к производительности в смешанном режиме FTTB

|  |  |
| --- | --- |
| Описание | Предварительная настройка оборудования для проведения испытаний |
| Схема |  |
| Используемое оборудование | 1. Генератор трафика Spirent;  2. Устройство для испытания;  3. Телевизионная приставка Ростелеком х 3 шт;  4. Коммутатор с поддержкой VLAN и доступом к СПД Общества;  5. Ноутбук или ПК с беспроводной картой 802.11n/ac (4x4).  6. Аналоговый телефон  7. SIP телефон, настроенный на работу с SSW общества. |
| Описание стенда | 1. Генератор трафика Spirent;  2. Устройство для испытания;  3. Телевизионная приставка Ростелеком х 3 шт;  4. Коммутатор с поддержкой VLAN и доступом к СПД Общества;  5. Ноутбук или ПК с беспроводной картой 802.11n/ac (4x4).  6. Аналоговый телефон  7. SIP телефон, настроенный на работу с SSW общества. |
| Настройка |  IP-Host 1 связан с Ethernet WAN интерфейсом в режиме Access, после конфигурации IGMP Proxy на PPPoE интерфейсе IGMP пакеты отправляются без PPP инкапсуляции с IP адресом отправителя 0.0.0.0 При настройке IGMP Proxy на соединении IPoE IGMP пакеты должны отправляться с адреса интерфейса;   IP-Host 2 связан c Ethernet WAN интерфейсом в режиме VLAN 802.1q (VID=xxx) 802.1p=0;   SSID1 (2.4 ГГц) Test\_1, шифрование WPA2-PSK, пароль 1234567890;   SSID2 (2.4 ГГц) Test\_2, шифрование WPA2-PSK, пароль 1234567890;   SSID5 (5 ГГц) Test\_1\_5, шифрование WPA2-PSK, пароль 2345678901;   SSID6 (5 ГГц) Test\_2\_5, шифрование WPA2-PSK, пароль 2345678901.   LAN1 связан с WAN интерфейсом в режиме моста;   LAN2, LAN3, SSID1 и SSID5 FXS (если используется) связаны с IP-Host1 и IP-Host2 в режиме маршрутизации с функцией NAT и локальным DHCP сервером;   LAN4 связан с WAN интерфейсом (VLAN=xxx p=5) в режиме моста;   SSID2 и SSID6 связан с WAN интерфейсом (VLAN=xxx p=0) в режиме моста.   Адреса IP-Host 1 настраиваются в зависимости от теста. Локальный DHCP сервер соответствует адресации на информационной наклейке;   Адрес IP-Host 2 настроен в режиме DHCP. |
| Цель |  |

## Проверка требований к производительности при функцонально-нагрузочном тестировании FTTB

|  |  |
| --- | --- |
| Описание | Предварительная настройка оборудования для проведения испытаний |
| Схема |  |
| Используемое оборудование | 1. Ноутбук или ПК с установленным Torrent клиентом;  2. Устройство для испытания;  3. Телевизионная приставка Ростелеком х 3шт;  4. Коммутатор с поддержкой VLAN и доступом к СПД Общества;  5. Ноутбук или ПК с беспроводной картой 802.11n/ac (4x4) и установленным Torrent клиентом;  6. IP-телефон.  7. Аналоговый телефон |
| Описание стенда | 1. Ноутбук или ПК с установленным Torrent клиентом;  2. Устройство для испытания;  3. Телевизионная приставка Ростелеком х 3шт;  4. Коммутатор с поддержкой VLAN и доступом к СПД Общества;  5. Ноутбук или ПК с беспроводной картой 802.11n/ac (4x4) и установленным Torrent клиентом;  6. IP-телефон.  7. Аналоговый телефон |
| Настройка | На CPE должен быть настроен IP-Host (для работоспособности IPTV при соединении PPPoE IGMP Proxy должен включаться на туннельном интерфейсе, в соответствии с рекомендациями TR-101), два SSID и два 802.1q VLAN:   IP-Host 1 связан с Ethernet WAN, после конфигурации IGMP Proxy на PPPoE интерфейсе IGMP пакеты отправляются без PPP инкапсуляции с IP адресом отправителя 0.0.0.0 При настройке IGMP Proxy на соединении IPoE IGMP пакеты должны отправляться с адреса интерфейса;   IP-Host 2 может быть связан с Ethernet WAN как в режиме access та и в режиме trunk.   SSID1 (2.4 ГГц) Test\_1, шифрование WPA2-PSK, пароль 1234567890;   SSID2 (2.4 ГГц) Test\_2, шифрование WPA2-PSK, пароль 2345678901;   SSID5 (5 ГГц) Test\_1\_5, шифрование WPA2-PSK, пароль 1234567890;   SSID6 (5 ГГц) Test\_2\_5, шифрование WPA2-PSK, пароль 2345678901;   VLAN ID=xxx, 802.1p=4 в режиме моста;   VLAN ID=xxx, 802.1.p=0 в режиме моста.   LAN 1-3, SSID1 и SSID5 связаны с IP-Host 1 и IP-Host 2 в режиме маршрутизации с функцией NAT и локальным DHCP сервером;   LAN 4 связан с WAN интерфейсом (VLAN=xxx) в режиме моста;   SSID2 и SSID6 связан с WAN интерфейсом (VLAN=xxx) в режиме моста. На SSID установлено ограничение полосы пропускания 2 Мбит/с. |
| Цель |  |

## Проверка качества обслуживания (QoS) и аппаратных очередей

|  |  |
| --- | --- |
| Описание | Предварительная настройка оборудования для проведения испытаний аппаратных очередей |
| Схема |  |
| Используемое оборудование | 1. Генератор трафика Spirent;  2. Устройство для испытания;  3. Коммутатор с поддержкой VLAN и доступом к СПД Общества;  4. SIP телефон, настроенный на работу в сети Общества;  5. Аналоговый телефонный аппарат;  6. Телевизионная приставка Ростелеком;  7. Телевизор;  8. Ноутбук или ПК с беспроводной картой 802.11n (2x2). |
| Описание стенда | 1. Генератор трафика Spirent;  2. Устройство для испытания;  3. Коммутатор с поддержкой VLAN и доступом к СПД Общества;  4. SIP телефон, настроенный на работу в сети Общества;  5. Аналоговый телефонный аппарат;  6. Телевизионная приставка Ростелеком;  7. Телевизор;  8. Ноутбук или ПК с беспроводной картой 802.11n (2x2). |
| Настройка | Настройка интерфейсов  IP-Host 1 связан c Ethernet WAN;  Настройка группировки  • Lan1-3 связан с WAN интерфейсом в режиме маршрутизатора с функцией NAT и локальным DHCP сервером;  • LAN4 связан с WAN интерфейсом (VLAN=101) в режиме моста. |
| Цель |  |

## Проверка требования к USB-порту и дополнительным приложениям

|  |  |
| --- | --- |
| Описание | Проверка функций USB порта |
| Схема |  |
| Используемое оборудование | 1. Устройство для испытания;  2. Телевизионная приставка или ТВ с поддержкой DLNA/SMB;  3. Ноутбук и/или ПК с беспроводной картой 802.11n (2x2) 2 шт;  4. USB flash диск с разным контентом |
| Описание стенда | 1. Устройство для испытания;  2. Телевизионная приставка или ТВ с поддержкой DLNA/SMB;  3. Ноутбук и/или ПК с беспроводной картой 802.11n (2x2) 2 шт;  4. USB flash диск с разным контентом |
| Настройка | IP-Host 1 связан c Ethernet WAN с включенным IGMP proxy.  Lan1-3 и SSID1 связан с WAN интерфейсом в режиме маршрутизатора с функцией NAT и локальным DHCP сервером;  Lan4 связан с WAN интерфейсом (VLAN=270) в режиме моста. |
| Цель |  |