Программа и методика испытаний оборудования беспроводной точки доступа (БТД) для реализации услуги доступа в Интернет из состава Универсальных Услуг Связи

Москва
2014 г.

Содержание

1 Назначение

Настоящий документ содержит Программу и Методику Испытаний (ПМИ) решения беспроводной точки доступа (БТД) для проверки соответствия качества и доступности предоставления услуги доступа в Интернет характеристикам, заданным в рамках реализации Универсальной Услуги Связи (УУС)

2 Общие положения

2.1 Цель испытаний

Целью испытаний являются:

- Инструментальная проверка технических параметров, характеристик и функционала предлагаемого оборудования БТД на соответствие требованиям по предоставлению УУС согласно Федеральному Закону РФ «О связи» от 07.07.2003 № 126-ФЗ.
- Проверка совместимости решения с ключевыми элементами сети передачи данных ОАО «Ростелеком» и оценка возможности предоставления различных телематических услуг связи а также авторизации и тарификации абонента.

2.2 Условия порядок проведения испытаний

Испытания проводятся совместной рабочей группой, куда входят технические специалисты ОАО «Ростелеком» и представитель(и) производителя (поставщика) оборудования:

- Тестирование Услуги производится на выделенных площадка МРФ в населенных пунктах либо в тестовой лаборатории ООА Ростелеком.

Тестированию в рамках данной ПМИ подлежит следующее оборудование:

1. Оборудование точки доступа Wi-Fi (диапазон 2,4 МГц). Тестирование может проводится как для точек доступа устанавливаемых вне помещений так и для внутренних точек доступа. Для тестирования необходимо минимум 2 идентичных точки доступа.

2. Контроллер точек доступа если он предусмотрен архитектурой решения.

3. Сервер и рабочее место системы управления БТД.

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 и должностей.

Испытания могут быть приостановлены, если какие-либо факторы могут повлечь нарушение правил и мер безопасности для персонала или создать условия, препятствующие нормальной эксплуатации тестируемого оборудования, измерительных приборов, другого оборудования ОАО «Ростелеком».
Перед началом проведения испытаний 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 испытания предоставляются и используются в работе:

- Тестируемое оборудование в правильной комплектации включая версию;
- Техническая документация: спецификация, руководство и пр.;
- Сертификаты и декларации соответствия;
- Настоящая программа и методика испытаний.

Испытания проводятся полностью по одной (каждой) модели оборудования, включая одну версию аппаратного и одну версию программного обеспечения. Если в процессе испытаний выясняется необходимость в замене моделей и/или версий оборудования, то все процедуры проводятся повторно с начальной позиции.

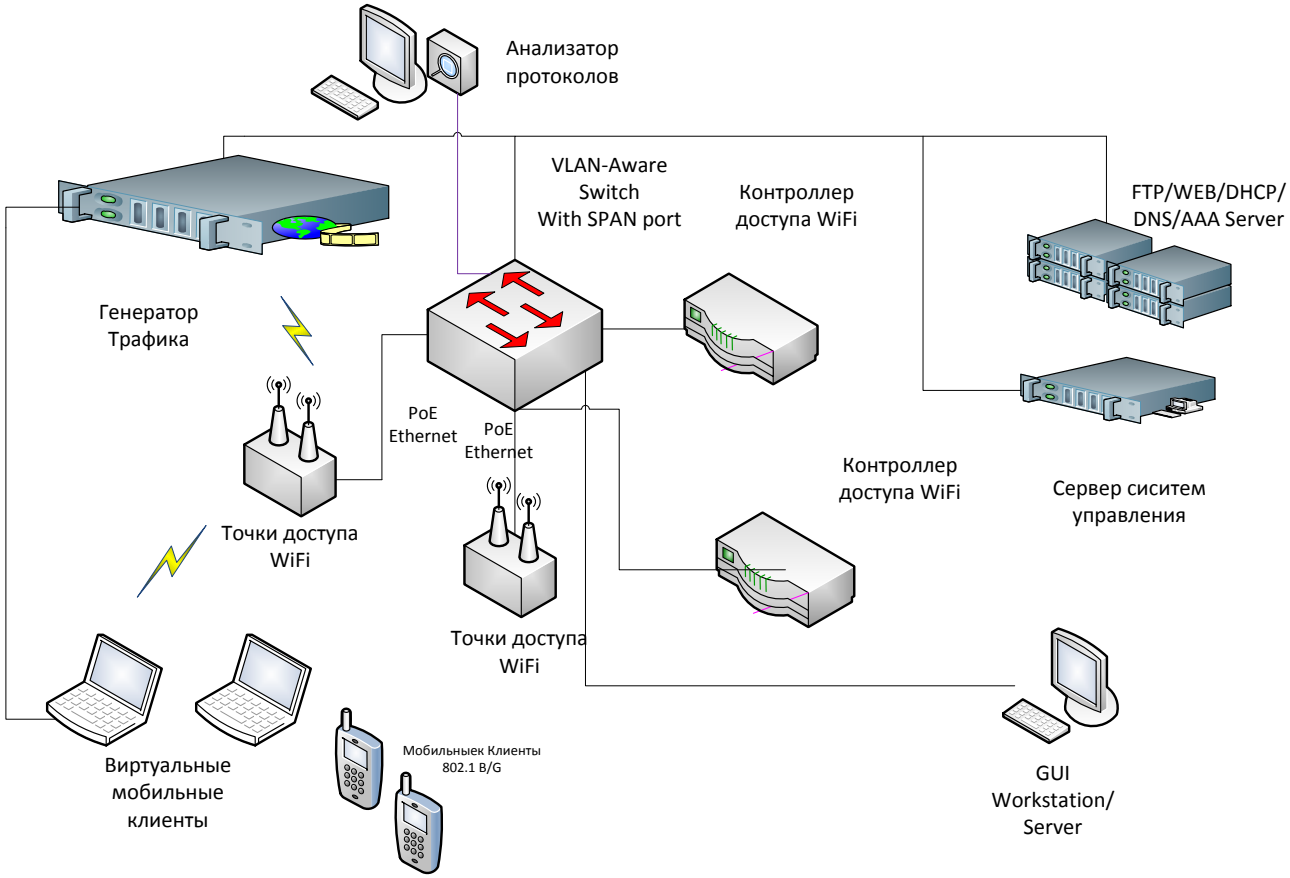
Протокол испытаний подписывается специалистами ОАО “Ростелеком”, проводившими тестирование и заверяется руководителем структурного подразделения ОАО «Ростелеком», проводившего испытания.

2.3 Руководящие документы и оформление отчета

При проведении испытаний используются следующие внутренние нормативные документы:

- Процедура организации тестирования абонентского оборудования для оказания услуг ШПД в ОАО «Ростелеком» (далее – Процедура);
- Технические требования, утвержденные Приказами по ОАО «Ростелеком» (далее – Требования);
- Настоящий документ с Программой и методикой испытаний (далее – Методика);

3 Схема испытательного стенда



Основное тестовое оборудование включает в себя:

1. Анализатор протоколов IP (В качестве инспектора пакетов будет использоваться ноутбук с установленной программой WireShark).

2. Программные пробники Wi-Fi на базе Ноутбуков (2 штуки, используются утилита NetStumbler или ПО WiFi Analyzer установленное на планшетах) – в дальнейшем это оборудование будет обозначаться ка Сканер Wi-Fi.

3. Средство тестирования производительности – в качестве средства тестирования производительности используется програмное обеспечение IxChariot 7.3 – обеспечивает функции генератора трафика и хранилища результатов измерений.

Дополнительное тестовое оборудование состоит из системы управления и мониторинга сети, серверов приложений FTP/DHCP/DNS, сервера FreeRadius, не менее трех мобильных клиентов (смартфонов или планшетов) с поддержкой Wi-Fi

802.1 B/G, не менее 2-х ноутбуков с поддержкой стандарта IEEE 802.11n и не менее 2-х дополнительных точек доступа Wi-Fi 2,4 ГГц работающих в режиме Bridge L2.

4 Методика проверки функциональности оборудования

Методика проверки основывается на рекомендации IEEE 802.11T Task Group:
Подлежат измерению следующие параметры:

a) задержка распространения пакетов;
b) уровень потерь пакетов;
c) максимальная пропускная способность

4.1 Проверка на соответствие требованиям по индустриальному исполнению

№	Процедура	Ожидаемый результат:
4.1.1	По документации и/или визуально проверить соответствие требованиям на индустриальное исполнение.	БТД имеет корпус в промышленном исполнении. Указать класс защиты IP.
4.1.2		БТД предназгначена для эксплуатации в температурном диапазоне -40…+65.

4.2 Проверка интерфейсов точки доступа БТД

№	Процедура	Ожидаемый результат:
4.2.1	По документации и/или визуально проверить наличие интерфейсов и портов.	Порт WAN Ethernet Base-T Ethernet (RJ-45) с поддержкой PoE
4.2.2		ТД 2.4 ГГц IEEE802.11b/g/n
4.2.3		Устройство грозозащиты

4.3 Тестирование базовой функциональности

Проверка производится для следующих макросценариев:

a) при установке абонентского терминала в непосредственной близости от базовой станции БТД;
b) при равноудаленной установке нескольких абонентских устройств относительно БС (проверка на емкость сети радиодоступа).

Проверка проводится только для диапазона 2,4 ГГц при максимально используемом диапазоне 20 Мгц. Для БТД внешнего исполнения используются только встроенные или стандартные антенны поставляющиеся совместно с точкой доступа. В случае если предусмотрена только внешняя антенна, то используются максимум 2 внешние OMNI антенны.

4.3.1 Измерение пропускной способности для одного абонента.

Номер теста	BWA_LAB_01
Название теста	Измерение пропускной способности для одного абонента.
Цель теста	Измерение пропускной способности для одного абонента на уровне TCP и UDP.
Важность теста	Базовый
Тестовая процедура	Измерения проводятся при ограничении при условии ограничения максимальной мощности точки доступа уровнем 100 МВт. В качестве клиента используются ноутбук с поддержкой стандарта IEEE 802.11n. 1. Осуществить передачу потока трафика от виртуального клиента в направлении сети с использованием программного обеспечения тестирования производительности. 2. Повторить п. 1, осуществив передачу потока трафика в обратном направлении. 3. Повторить п. 1 для двунаправленного потока трафика. 4. Измерения выполнить для 3-х положений клиента (в непосредственной близости от антенны, на расстоянии 15м, и на расстоянии 30 м. от антенны) 5. Зафиксировать результаты измерений в таблицу. В таблице указываются максимальные скорости передачи по протоколам TCP и UDP для трех положений мобильного клиента.
Ожидаемый результат	Результаты измерений пропускной способности системы в лабораторных условиях зафиксированы в таблице.

4.3.2 Измерение пропускной способности точки Wi-Fi.

Номер теста	BWA_LAB_02
Название теста	Измерение пропускной способности точки.
Цель теста	Измерение пропускной способности точки доступа на уровне TCP.
Важность теста	Базовый

Тестовая процедура	Измерения проводятся при ограничении при условии ограничения максимальной мощности точки доступа уровнем 100 МВт. Используется единый набор из 5 клиентов для тестирования всех точек доступа: 2 ноутбука с поддержкой стандарта IEEE 802.11n (Клиент 1 и Клиент 2), 2 планшет (смартфона) с поддержкой IEEE 802.11n (Клиент 3 и Клиент 4), 1 ноутбук с поддержкой стандарта IEEE 802.11g (Клиент 5). Клиенты располагаются на одинаковом расположении от антенны БТД. 1. Осуществить одновременную передачу потоков трафика от клиентов в направлении сети с использованием програмного обеспечения тестирования производительности. Передача должна осуществляться непрерывно в течение не менее 1 минуты. 2. Повторить п. 1, осуществив передачу потока трафика в обратном направлении. 3. Повторить п. 1 для двунаправленного потока трафика. 4. Измерения выполнить для 3-х положений клиентов (в непосредственной близости от антенны, на расстоянии 15м, и на расстоянии 30 м. от антенны) 5. Зафиксировать результаты измерений в таблицу. В таблице указываются максимальные скорости передачи по TCP для трех положений мобильных клиентов.
Ожидаемый результат	Результаты измерений пропускной способности системы в лабораторных условиях зафиксированы в таблице.

4.3.3 Поддержка до 5x SSID (SSID в диапазоне 2.4ГГЦ).

Номер теста	BWA_LAB_03
Название теста	Поддержка до 5x SSID (SSID в диапазоне 2.4ГГЦ).
Цель теста	Поддержка до 5x SSID (SSID в диапазоне 2.4ГГЦ).
Важность теста	Базовый
Тестовая	Сконфигурировать на точке доступа с использованием Web GUI интерфейса 5 различных SSID с различными правилами

процедура	аутентификации абонента и шифрования: 1 – Без аутентификации и шифрования 2 – Wep 64 bit 3 – Wep 128 bit 4 – WPA 5 – 802.1x PEAP Сконфигурировать передачу трафика каждой SSID в отдельном VLAN. Установить 5 разных уровней приоритетов (Priority) для каждого из SSiD. Последовательно осуществить передачу трафика по всем SSID между мобильным клиентом и сетью (выкачка тестового файла по ftp). Убедится при помощи анализатора протоколов (ПО Wireshark), что трафик передается в различных VLAN.
Ожидаемый результат	Сконфигурированы 5 различных SSID с различными правилами аутентификации и шифрования. Трафик по ним передается в различных VLAN.

4.3.4 Управление мощностью передаваемого сигнала.

Номер теста	BWA_LAB_04
Название теста	Управление мощностью передаваемого сигнала.
Цель теста	Проверить возможность гибкого регулирования мощности излучаемого сигнала БТД.
Важность теста	Базовый
Тестовая процедура	При помощи GUI БТД изменить не менее трех раз значение максимального уровня передаваемого сигнала. При помощи тестового оборудования (ПО WiFi Analyzer) убедиться в изменении уровня сигнала от точки доступа.
Ожидаемый результат	Возможность плавного изменения максимального уровня сигнала точки доступа.

4.3.5 Ограничение доступа к сети Wi-Fi при минимальном уровня сигнала.

Номер теста	BWA_LAB_05
Название теста	Ограничение доступа к сети Wi-Fi при минимальном уровня сигнала.
Цель теста	Убедится в возможности ограничения доступа к сети Wi-Fi при минимальном уровне сигнала клиента
Важность теста	Опциональный
Тестовая процедура	1.Сконфигурировать точку доступа и осуществить передачу данных с использованием мобильного клиента с расстояния 30м. от точки доступа. 2. При помощи GUI БТД изменить значение минимального уровня сигнала клиента с которым разрешен доступ к сети существенно его увеличив. 3. Убедится в невозможности регистрации клиента с расстояния 30-40м. после существенного увеличения минимального уровня сигнала с которым возможен доступ к сети.
Ожидаемый результат	Возможность ограничения доступа клиентов к точке доступа при слабом уровне сигнала от мобильного клиента.

4.3.6 Управление каналами

Номер теста	BWA_LAB_06
Название теста	Управление каналами.
Цель теста	Возможность ручного задания радиоканала. Возможность автоматического определения канала точкой доступа – выбор канала с наименьшей интерференцией.
Важность теста	Базовый
Тестовая процедура	Измерения проводятся при ограничении при условии ограничения максимальной мощности точки доступа уровнем 100 МВт. В качестве клиента используются ноутбук с поддержкой стандарта IEEE 802.11n. 1. Убедится в возможности ручного задания номера канала Wi-Fi через GUI БТД. Проверить при помощи тестового

	оборудования (Сканера Wi-Fi) что БТД использует выбранный канал. 2. Включить в GUI БТД автоматический выбор радиоканала. при помощи сканера Wi-Fi определить номер используемого точкой канала. При помощи двух ноутбуков создать AdHoc Wi-Fi сеть с отличным от тестируемого SSId. Принудительно задать номер канала соответствующий используемому точкой доступа. Осуществить в этой сети постоянную передачу файла данных при помощи утилиты Iperf без ограничения мощности адаптеров. При помощи тестового оборудования убедиться что при регистрации клиента БТД изменила канал на другой.
Ожидаемый результат	Возможно ручное задание радиоканала БТД. Возможность автоматического определения канала точкой доступа – выбор канала с наименьшей интерференцией.

4.3.7 Ограничение максимального числа клиентов подключаемых к точке доступа.

Номер теста	BWA_LAB_07
Название теста	Ограничение максимального числа клиентов подключаемых к точке доступа.
Цель теста	Убедится в возможности ограничения количества одновременных подключений к точке доступа с целью гарантировать качество сервиса.
Важность теста	Базовый
Тестовая процедура	1. Осуществить одновременное подключение и передачу данных для трех мобильных клиентов на тестовой точке доступа. 2. Через GUI БТД ограничить максимальное число клиентов на точке доступа указав значенеи user limit =2. 3. Убедится что после ограничения максимального числа клиентов невозможно подключение более двух клиентов к БТД.
Ожидаемый результат	Возможно ограничение количества одновременных подключений к точке доступа с целью гарантировать качество сервиса.

4.4 Тестирование аутентификации и безопасности

4.4.1 Поддержка аутентификации 802.1x с использованием внешнего радиус сервера.

Номер теста	AUT_LAB_01
Название теста	Поддержка аутентификации 802.1x с использованием внешнего радиус сервера.
Цель теста	Убедиться в поддержке аутентификации 802.1x с использованием внешнего радиус сервера и протоколов EAP-PEAP.
Важность теста	Базовый
Тестовая процедура	1.Сконфигурировать точку доступа с двумя SSID на одном из (SSID1) которых указать режим шифрования WPA2 (или WPA2 AES); режим аутентификации 802.1x с опцией аутентификации EAP-PEAP. В качестве алгоритма проверки подлинности на втором этапе авторизации указать MSCHAPV2 Настройка должна позволять аутентифицировать пользователя по паре логин/пароль без необходимости использовать сертификаты на клиентском оборудовании. 2.Через GUI БТД сконфигурировать внешний радиус сервер – указать IP адрес, порт и секретный ключ для лабораторного FreeRadius сервера. 3. На лабораторном радиус сервере FreeRadius сконфигурировать двух пользователей TestUser1 и TestUser2. Определить для них разные пароли для доступа. Сконфигурировать серверный сертификат для радиус сервера. Сконфигурировать БТД как NAS клиент для FreeRadius сервера. 4. Установить для SSID1 режим аутентификации через внешний radius сервер (Enterprise) mode. 5. Активировать сессию с использованием клиента Windows 7/8 на ноутбуке с настройками аутентификации 802.1 x и советующим именем пользователя и паролем.
Ожидаемый результат	Убедиться, что клиенты с парой логин/пароль указанной в Radius сервере получают доступ к SSID1. Убедится что клиенты с неправильным паролем не получают доступ к SSID1. Убедится что клиенты с выключенной аутентификацией 802.1 x или не поддерживающие такую аутентификацию не получают доступ к

	802.1 x.

4.4.2 Передача MAC адреса абонента при авторизации абонента на Радиус сервере

Номер теста	AUT_LAB_02
Название теста	Передача MAC адреса абонента при авторизации абонента на Радиус сервере.
Цель теста	Убедится в передаче MAC адреса абонента при авторизации абонента на Радиус сервере
Важность теста	Базовый
Тестовая процедура	1. Для теста AUT_LAB_01 проверить при помощи протокол анализатора наличие MAC Адреса клиента в сообщении Radius
Ожидаемый результат	Mac адрес клиента присутствует в сообщении Radius

4.4.3 Поддержка разрыва сессии по сигналу от Радиус сервера RID (Radius Initiated Disconnect)

Номер теста	AUT_LAB_03
Название теста	Поддержка разрыва сессии по сигналу от Радиус сервера RID (Radius Initiated Disconnect)
Цель теста	Убедится в поддержке разрыва сессии по сигналу от Радиус сервера RID (Radius Initiated Disconnect)
Важность теста	Базовый
Тестовая процедура	1.Сконфигурировать точку доступа с двумя SSID на одном из (SSID1) которых указать режим шифрования WPA2 (или WPA2 AES); режим аутентификации 802.1x с опцией аутентификации EAP-PEAP. В качестве алгоритма проверки подлинности на втором этапе авторизации указать MSCHAPV2 Настройка должна позволять аутентифицировать пользователя по паре логин/пароль без необходимости использовать сертификаты на клиентском оборудовании.

	2.Через GUI БТД сконфигурировать внешний радиус сервер – указать IP адрес, порт и секретный ключ для лабораторного FreeRadius сервера. 3. На лабораторном радиус сервере FreeRadius сконфигурировать двух пользователей TestUser1 и TestUser2. Определить для них разные пароли для доступа. Сконфигурировать серверный сертификат для радиус сервера. Сконфигурировать БТД как NAS клиент для FreeRadius сервера. 4. Установить для SSID1 режим аутентификации через внешний radius сервер (Enterprise mode). 5. Активировать Accounting для SSID1 указать IP адрес лабораторного FreeRadius сервера в качестве Accounting сервера. 6. Активировать сессию с использованием клиента Windows 7/8 на ноутбуке с настройками аутентификации 802.1 x и соответствующим именем пользователя и паролем. 7. Убедится при помощи анализатора протоколов что произведена аутентификация пользователя на радиус сервере и началась accounting сессия (сообщение Accounting Start). Определить Accounting Session ID из этого сообщения. 8. При активной сессии направит с радиус сервера на точку доступа запрос на отключение пользователя при помощи утилиты radclient: # echo "Acct-Session-Id=D91FE8E51802097" > packet.txt # echo "User-Name=TestUser1" >> packet.txt # echo "NAS-IP-Address=y.y.y.y" >> packet.txt # cat packet.txt | radclient -x y.y.y.y:3799 disconnect "secret" Где y.y.y.y – IP адрес точки доступа (или контроллера точек доступа в случае если он выступает radius клиентом) Acct-Session-Id – Идентификатор сессии из пункта 7. 9. При помощи анализатора протоколов убедится что радиус сервер направил Radius сообщение DisconnectRequest(40). 10. Убедится что для пользователя TestUser1 сессия разорвана и при помощи анализатора протоколов убедится в отправке БТД или контроллером точек доступа Radius сообщения DisconnectAck(41) и Radius сообщения Accounting Stop с завершающей сессию статистикой.
Ожидаемый результат	Поддерживается разрыва сессии по сигналу от Радиус сервера RID (Radius Initiated Disconnect)

4.4.4 Периодическая передача информации о сессии в Радиус сервер (Accounting)

Interim update)

Номер теста	AUT_LAB_04
Название теста	Периодическая передача информации о сессии в Радиус сервер (Accounting)
Цель теста	Убедится в наличии периодическая передача информации о сессии в Радиус сервер (Accounting)
Важность теста	Базовый
Тестовая процедура	1.Сконфигурировать точку доступа с двумя SSID на одном из (SSID1) которых указать режим шифрования WPA2 (или WPA2 AES); режим аутентификации 802.1x с опцией аутентификации EAP-PEAP. В качестве алгоритма проверки подлинности на втором этапе авторизации указать MSCHAPV2 Настройка должна позволять аутентифицировать пользователя по паре логин/пароль без необходимости использовать сертификаты на клиентском оборудовании. 2.Через GUI БТД сконфигурировать внешний радиус сервер – указать IP адрес, порт и секретный ключ для лабораторного FreeRadius сервера. 3. На лабораторном радиус сервере FreeRadius сконфигурировать двух пользователей TestUser1 и TestUser2. Определить для них разные пароли для доступа. Сконфигурировать серверный сертификат для радиус сервера. Сконфигурировать БТД как NAS клиент для FreeRadius сервера. 4. Установить для SSID1 режим аутентификации через внешний readius сервер (Enterprise mode). 5. Активировать аккаунтинг для SSID1 указать IP адрес лабораторного FreeRadius сервера в качестве Accounting сервера. 6. Активировать сессию с использованием клиента Windows 7/8 на ноутбуке с настройками аутентификации 802.1 x и советующим именем пользователя и паролем. 7. Убедится при помощи анализатора протоколов что произведена аутентификация пользователя на радиус сервере и началась accounting сессия (сообщение Accounting Start). Определить

	Accounting Session ID из этого сообщения. 8. Начать выкачку файла размером более 200 Мбайт по протоколу FTP с FTP сервера из сети. 2. При помощи протокол анализатора убедится что периодически происходят обновления информации от БТД на Accounting сервер типа Accounting - Interim Update.
Ожидаемый результат	Периодически осуществляется передача информации о сессии в Радиус сервер путем сообщений Interim Update.

4.4.5 Передача информации в Радиус сервер по окончании сессии.

Номер теста	AUT_LAB_05
Название теста	Передача информации в Радиус сервер по окончании сессии.
Цель теста	Убедиться в наличии передачи информации о сессии в Радиус сервер (Accounting)
Важность теста	Базовый
Тестовая процедура	1.Сконфигурировать точку доступа с двумя SSID на одном из (SSID1) которых указать режим шифрования WPA2 (или WPA2 AES); режим аутентификации 802.1x с опцией аутентификации EAP-PEAP. В качестве алгоритма проверки подлинности на втором этапе авторизации указать MSCHAPV2 Настройка должна позволять аутентифицировать пользователя по паре логин/пароль без необходимости использовать сертификаты на клиентском оборудовании. 2.Через GUI БТД сконфигурировать внешний радиус сервер – указать IP адрес, порт и секретный ключ для лабораторного FreeRadius сервера. 3. На лабораторном радиус сервере FreeRadius сконфигурировать двух пользователей TestUser1 и TestUser2. Определить для них разные пароли для доступа. Сконфигурировать серверный сертификат для радиус сервера. Сконфигурировать БТД как NAS клиент для FreeRadius сервера. 4. Установить для SSID1 режим аутентификации через внешний radius сервер (Enterprise mode). 5. Активировать аккаунтинг для SSID1 указать IP адрес лабораторного FreeRadius сервера в качестве Accounting сервера.

	6. Активировать сессию с использованием клиента Windows 7/8 на ноутбуке с настройками аутентификации 802.1 x и советующим именем пользователя и паролем. 7. Убедится при помощи анализатора протоколов что произведена аутентификация пользователя на радиус сервере и началась accounting сессия (сообщение Accounting Start). Определить Accounting Session ID из этого сообщения. 8. Осуществить дерегистрацию клиента в ходе сессии путем отключения мобильного клиента и выключения питания клиента 9. При помощи протокол анализатора убедится что по завершении сессии произошла передача сообщения Accounting Stop от БТД на Radius сервер с информацией об объеме переданного трафика.
Ожидаемый результат	По завершении сессии путем отключения мобильного клиента и выключения питания клиента осуществляется корректная передача информации о сессии в Радиус сервер.

4.4.6 Создание отдельного динамического VLAN на абонента

Номер теста	AUT_LAB_06
Название теста	Создание отдельного динамического VLAN на абонента
Цель теста	Поддержка C-VLAN модели на точке доступа.
Важность теста	Опциональный
Тестовая процедура	1. Сконфигурировать точку доступа с двумя SSID на одном из (SSID1) которых указать режим шифрования WPA2 (или WPA2 AES); режим аутентификации 802.1x с опцией аутентификации EAP-PEAP. В качестве алгоритма проверки подлинности на втором этапе авторизации указать MSCHAPV2 Настройка должна позволять аутентифицировать пользователя по паре логин/пароль без необходимости использовать сертификаты на клиентском оборудовании. 2. Через GUI БТД сконфигурировать внешний радиус сервер – указать IP адрес, порт и секретный ключ для лабораторного FreeRadius сервера. 3. На лабораторном радиус сервере FreeRadius сконфигурировать

	двух пользователей TestUser1 и TestUser2. Определить для них разные пароли для доступа. Сконфигурировать серверный сертификат для радиус сервера. Сконфигурировать БТД как NAS клиент для FreeRadius сервера. 4. Установить для SSID1 режим аутентификации через внешний radius сервер (Enterprise mode). 5. Активировать Accounting для SSID1 указать IP адрес лабораторного FreeRadius сервера в качестве Accounting сервера. 6. На точке доступа в соответчики с документацией сконфигурировать режим динамического назначения уникального VLAN каждому пользователю. 7. Активировать сессию с использованием клиента Windows 7/8 на ноутбуке с настройками аутентификации 802.1 x и советующим именем пользователя и паролем. 8. Убедится что трафик абонентов маршрутизируется по сети по уникальному VLAN VLAN-ID вне зависимости от того какой VLAN указан на точке доступа как соответствующий SSID используемой сети. Подключить к данному SSID не менее трех клиентов. Убедится что трафик каждого из них маршрутизируется по сети с уникальным тегом VLAN.
Ожидаемый результат	Поддерживается модель C-Vlan на точку доступа Указать максимальное количество поддерживаемых VLAN на 1 точке доступа (из документации).

5 Проверка общих требований

5.1 Проверка электропотребления оборудования точки доступа

№	Процедура	Ожидаемый результат
5.1.1	1. Проверить основное электропитание (-48V, потребл. мощн. до 10 Вт). Проверить по документации, что блок питания обладает функцией защиты абонентского устройства от скачков переменного напряжения в электросети с применением сглаживающих	1. Напряжение питания 48 В, потребл. мощн. до 10 Вт 2. Блок питания с функциональностью защиты от скачков переменного напряжения в электросети. 3. Потребляемая мощность оборудования соответствует заявленной производителем.

	фильтров. 2. Проверить при помощи МИП потребляемую мощность БС и коммутатора L2.	

5.2 Проверка требований к хранению и эксплуатации

№	Процедура	Ожидаемый результат
5.2.1	По документации проверить, что условия хранения и эксплуатации соответствуют требуемым.	Рабочая температура: от -40˚ до 65˚С.
		Температура хранения: от -40˚ до 70˚С.
		Рабочая влажность: от 5% до 90%, без образования конденсата.
		Класс защиты не хуже IP55

5.3 Тестирование надежности и стабильности работы

№	Процедура	Ожидаемый результат
5.3.1	Во время проведения испытаний, убедиться в отказоустойчивости ТД БШПД. Во время испытаний не должна происходить самопроизвольная перезагрузка ТД. Проверить возможность сброса настроек на заводские. С помощью МИП выполнять непрерывные тесты производительности на максимальной поддерживаемой скорости в течение 8-24 часов (более длительные тесты являются предпочтительными). Зафиксировать ошибки в ходе выполнения теста (потери кадров).	MTBF операционной системы не меньше 1 года.
5.3.2		Продолжительность жизни устройства не меньше семи лет.
5.3.3		Среднее время наработки на отказ устройства не менее 2 лет.
5.3.4		Возможность возврата пользователем конфигурации к заводской.

6 Проверка функционала управления точкой доступа

6.1 Проверка функций мониторинга и управления

6.1.1 Управление ТД через WebGUI/Telnet

Номер теста	MAN_LAB_01
Название теста	Управление ТД через WebGUI/Telnet
Цель теста	Проверить возможность прямого управления точкой доступа через Web GUI и Telnet.
Важность теста	Базовый
Тестовая процедура	Проверить возможность управления параметрами ТД через WebGUI ПРверить возможность управления базовыми параметрами ТД включая настройку параметров IP через Telnet.
Ожидаемый результат	ТД удаленно управляется через Web GUI ТД удаленно управляется через Telnet Web-интерфейс и CLI должны быть защищены паролем. Пользователь устройства должен иметь возможность изменить пароль. Наличие web-интерфейса на русском языке.

6.1.2 Резервное копирование и восстановление файла конфигурации

Номер теста	MAN_LAB_02
Название теста	Резервное копирование и восстановление файла конфигурации
Цель теста	Проверка возможности резервного копирования текущей конфигурации ТД и её восстановление из резервной копии
Важность теста	Базовый
Тестовая процедура	1. Через WebGUI/CLI сделать backup текущей конфигурации. 2. Сбросить ТД в заводские установки. 3. Восстановить текущую конфигурацию из файла. 4. Проверить корректность настроек.
Ожидаемый	Конфигурация успешно выгружается через CLI и Web GUI и

результат	восстанавливается

6.1.3 Обновление микропрограммы

Номер теста	MAN_LAB_03
Название теста	Обновление микропрограммы
Цель теста	Проверка возможности обновления микропрограммы ТД
Важность теста	Базовый
Тестовая процедура	С помощью WebGUI и CLI выполнить загрузку новой версии микропрограммы с удаленного сервера и обновление микропрограммы ТД с удаленного сервера.
Ожидаемый результат	Конфигурация успешно выгружается через CLI и Web GUI и восстанавливается

6.1.4 Мониторинг по SNMP

Номер теста	MAN_LAB_04
Название теста	Мониторинг по SNMP
Цель теста	Проверка возможности обновления микропрограммы ТД
Важность теста	Базовый
Тестовая процедура	1. Проверить возможность мониторинга и управления ТД с ПК управления через протокол SNMP v1/2c. a. Проверить доставку аварийных сообщений (interface up/down) посредством SNMP. b. Произвести настройку любого параметра ТД c. Считать параметры с веток IF-MIB ifEntry и ifXEntry 2. Проверить возможность получения SNMP Trap.
Ожидаемый	1. Мониторинг параметров и управление по SNMP возможно

результат	(получить от вендора MIB файлы и их описание при наличии). 2. ТД отправляют SNMP Trap (необходимо у вендора получить описание событий, при которых ТД шлёт SNMP Trap).

6.2 Проверка системы управления и мониторинга

6.2.1 Возможность централизованного мониторинга аварий на системе управления.

Номер теста	MAN_LAB_06
Название теста	Возможность централизованного мониторинга аварий на системе управления
Цель теста	Проверка возможности централизованного мониторинга аварий на системе управления
Важность теста	Базовый
Тестовая процедура	1. Настроить 2 точки доступа и подключить их к системе управления для мониторинга аварий по SNMP. a. Проверить отображение в системе аварийных сообщений (например interface up/down) посредством SNMP. b. Проверить отображение аварий различного уровня (severity) c. Проверить возможность обработки аварии (handle) с рабочего места операторoа системы а также генерации on-line окна со всеми активными авариями в системе. 2. Проверить возможность выхода аварии в случае потери связи с точкой доступа (иммитируется физическим отсоединением точки доступа от коммутатора).
Ожидаемый результат	Присутвует возможность централизованного мониторинга и обработки аварий различного уровня (severity) на системе управления.

6.2.2 Возможность генерации пользовательских аварий.

Номер теста	MAN_LAB_07

Название теста	Возможность генерации пользовательских аварий
Цель теста	Возможность генерации пользовательских аварий на основе комбинаций из нескольких аварийных сообщений или на основании превышения порогового значения.
Важность теста	Опциональный
Тестовая процедура	1. При помощи GUI сконфигурировать на ситеме управления пользовательскую аварию как результат двух стандартных аварийных сообщений (например 2 аварии SNMP link down и SNMP link up в течении 1 минуты = новая авария link unstable) a. Убедится в генерировании новой аварии при наличии соответсвующих аварийных сообщений на сети. b. Убедится в возможности настройки Severity новой аварии. 2. Проверить возможность генерации кастмерской аварии в случае превышения опереедельнного уровня параметра УТД (например CPU_load>xx%) – (в целях испытания параметр xx следует сделать максимально низким – например 15% чтобы гарантировать выход аварии даже в случае отсутвия нагрузки на БТД.). Убедится в возможности настройки Severity новой аварии.
Ожидаемый результат	Возможна генерации пользовательских аварий на основе комбинаций из нескольких аварийных сообщений или на основании превышения порогового значения.

6.2.3 Возможность управления конфигурациями точек доступа через графический интерфейс системы управления.

Номер теста	MAN_LAB_08
Название теста	Возможность управления конфигурациями точек доступа через графический интерфейс системы управления.
Цель теста	Проверка возможности управления индивидуальными конфигурациями точек доступа через графический интерфейс системы управления.
Важность теста	Базовый
Тестовая	Открыть окно конфигурации конкретной точки доступа.

процедура	Убедиться что в окне показываются актуальные параметры текущей конфигурации. Настроить индивидуальные параметры БТД при помощи GUI системы управления (параметры IP, параметры сетей Wi-Fi – SSID, авторизации) Убедится что после команды применить (Apply) – параметры заданной точки доступа изменены.
Ожидаемый результат	Возможно управление конфигурациями точек доступа через графический интерфейс системы управления

6.2.4 Возможность централизованного сбора и обработки статистики о пользовательских сессиях и их параметрах на системе управления.

Номер теста	MAN_LAB_09
Название теста	Возможность централизованного сбора и обработки статистики о пользовательских сессиях и их параметрах на системе управления.
Цель теста	Проверка возможности централизованного сбора и обработки статистики о пользовательских сессиях и их параметрах на системе управления.
Важность теста	Базовый
Тестовая процедура	1. Выполнить несколько сессий передачи данных на обеих точках доступа. 2. Убедиться что система управления отображает основные статистические параметры сессий (как минимум количество активных пользователей, переданный объем трафика, скорость передачи данных)
Ожидаемый результат	Система управления имеет возможность собирать основную статистику по точкам доступа и агрегировать ее. Привести список поддерживаемой статистики из системы управления (по документации или из экран системы управления).

6.2.5 Возможность добавления в систему единовременно нескольких ТД путем импорта конфигурационного файла.

Номер теста	MAN_LAB_10

Название теста	Возможность добавления в систему управления единовременно нескольких ТД путем импорта конфигурационного файла.
Цель теста	Проверка возможности добавления в систему единовременно списка точек доступа путем импорта конфигурационного файла.
Важность теста	Базовый
Тестовая процедура	1. Вручную удалить все УТД из системы управления. 2. Подготовить конфигурационный файл в который включить минимум 5 точек доступа включая две точки установленные в лаборатории. 3. Провести импорт конфигурационного файла в систему. Убедится в появлении всех 5 точек доступа в системе после импорта и в том что 2 работающие точки доступа доступны для мониторинга и конфигурирования.
Ожидаемый результат	Возможно добавлять УТД в систему управления путем импорта конфигурационного файла. Приложить формат и пример конфигурационного файла.

6.2.6 Возможность автоматического обнаружения новых ТД .

Номер теста	MAN_LAB_11
Название теста	Возможность автоматического обнаружения новых ТД
Цель теста	Возможность автоматического обнаружения новых ТД как в одной подсети с системой управления так и в заданных подсетях.
Важность теста	Базовый
Тестовая процедура	1. Вручную удалить все БТД из системы управления. 2. Провести процедуру автоматического определения БТД в подсети лаборатории. 3. Убедится что 2 работающие точки доступа доступны для мониторинга и конфигурирования.
Ожидаемый результат	Возможно добавлять БТД в систему управления автоматически путем сканирования указанных фрагментов IP сетей.

	Приложить список протоколов и методов которая система управления может использовать для сканирования фрагментов сетей.

6.2.7 Поддержка массовой конфигурации точек доступа с использованием шаблонов.

Номер теста	MAN_LAB_12
Название теста	Поддержка массовой конфигурации точек доступа с использованием шаблонов
Цель теста	Проверка массовой конфигурации точек доступа с использованием пользовательских шаблонов
Важность теста	Базовый
Тестовая процедура	1. Создать в GUI пользовательский шаблон конфигурации точки доступа. 2. Проверить возможность выполнения конфигурации одновременно нескольких точек доступа с использованием стандартных шаблонов и пользовательских шаблонов.
Ожидаемый результат	Возможно выполнение конфигурации одновременно нескольких точек доступа с использованием стандартных шаблонов и пользовательских шаблонов.

6.2.8 Отображение сводной информации о БТД, включая конфигурацию, аварии и статистику в одном окне.

Номер теста	MAN_LAB_13
Название теста	Отображение сводной информации о БТД включая конфигурацию, аварии и статистику в одном окне.
Цель теста	Проверка возможности наглядного отображения информации о конкретной точки доступа.
Важность теста	Базовый
Тестовая процедура	1. Открыть окно информации о конкретной точки доступа. Убедится что в нем в удобном виде представлена информация о текущем состоянии точки доступа включая ее имя и

	местоположение и основная статистика ее работы.
Ожидаемый результат	Есть возможность наглядного отображения информации о конкретной точки доступа.

6.2.9 Возможность автоматической настройки новых точек доступа по заданному шаблону.

Номер теста	MAN_LAB_14
Название теста	Возможность автоматической настройки новых точек доступа по заданному шаблону
Цель теста	Проверка возможности авто конфигурирования точек доступа по заданному шаблону при включении новой БТД.
Важность теста	Базовый
Тестовая процедура	1. Удалить все точки доступа из системы управления. 2. Создать шаблон конфигурации для группы точек доступа. 3. Создать профайл конфигурации устройства с учетом шаблона конфигурации и версии программного обеспечения. 4. Сымитировать установку точек доступа со складу загрузив в них дефолтную (bootstrap) конфигурацию достаточную для обращения к системе управления. 5. Убедится что точки доступа в состоянии получить из системы управления свою текущую конфигурацию и версию ПО в соответствии с созданным профилем и своим идентификатором (Device ID – например произвольным именем или серийным номером устройства) 6. Убедится что точки доступа видимы в системе управления с актуальной конфигурацией и версией ПО.
Ожидаемый результат	Присутствует возможность автоматической настройки новых точек доступа по заданному шаблону и профилю.

6.2.10 Возможность получения информации о радио-окружении и основных параметрах радио-обстановки каждой точки доступа в текстовой и графической форме.

Номер теста	MAN_LAB_15

Название теста	Возможность получения информации о радио-окружении и основных параметрах радио-обстановки каждой точки доступа в текстовой и графической форме.
Цель теста	Убедится в наличии в системе управления средства позволяющего в текстовой и графической форме показывать состояние эфира и параметры сети для каждой точки доступа.
Важность теста	Опциональный
Тестовая процедура	Средствами GUI системы управления отобразить окно отображающее состояние спектра и радио-окружение конкретной точки доступа (средство типа “Wi-Fi радар”)
Ожидаемый результат	Наличие в системе управления средства позволяющего в текстовой и графической форме показывать состояние эфира и параметры сети для каждой точки доступа.

6.2.11 Возможность управления версиями ПО с использованием системы управления.

Номер теста	MAN_LAB_16
Название теста	Возможность управления версиями ПО с использованием системы управления
Цель теста	Проверка возможности загрузки информации о текущих версиях ПО и массовом обновлении версий ПО с системы управления.
Важность теста	Базовый
Тестовая процедура	1. Осуществить сбор информации о версии ПО с двух точек доступа средствами системы управления. 2. Выполнить массовое обновление ПО на новую версию как минимум на 2-х точках доступа средствами системы управления.
Ожидаемый результат	В системе управления присутствует возможность централизованного управления версиями ПО точек доступа.

6.2.12 Возможность интеграции в систему управления оборудования точек доступа сторонних производителей.

Номер теста	MAN_LAB_17

Название теста	Возможность интеграции в систему управления оборудования точек доступа сторонних производителей
Цель теста	Проверка возможности интеграции стороннего оборудования.
Важность теста	Опциональный
Тестовая процедура	По документации проверить возможность интеграции: 1) аварий по протоколу SNMP или SysLog 2) конфигурирования оборудования (по протоколу SNMP или любому другому протоколу) 3) агрегация статистики со сторонних точек доступа, контроллеров точек доступа или систем управления.
Ожидаемый результат	Присутствует возможность интеграции; Приложить описание поддерживаемых протоколов.

6.2.13 Возможность экспорта из системы информации о списке точек доступа и их конфигурации и статистической информации в виде текстового файла/отчета.

Номер теста	MAN_LAB_18
Название теста	Возможность экспорта из системы информации о списке точек доступа и их конфигурации и статистической информации в виде текстового файла/отчета.
Цель теста	Проверка возможности экспорта информации в открытом текстовом формате.
Важность теста	Базовый
Тестовая процедура	Через GUI системы управления осуществить экспорт информации о точках доступа в текстовой файл. Опционально сгенерировать отчет по статистическим параметрам точек доступа в табличном или графическом виде. В файле должна быть как минимум информация о названии точек доступа, ее IP адресе, основных параметрах ее конфигурации и базовых параметрах статистики ее работы включая как минимум время непрерывной работы, объём пользовательского трафика и количество пользователей.
Ожидаемый результат	Подтверждается возможность экспорта информации о точках доступа в виде текстового файла или отчета. Приложен формат

	файла экспорта.

6.2.14 Наличие в системе управления северных интерфейсов для интеграции с системами управления более высокого уровня.

Номер теста	MAN_LAB_19
Название теста	Наличие в системе управления северных интерфейсов для интеграции с системами управления более высокого уровня.
Цель теста	Проверка возможности интеграции с системами управления более высокого уровня.
Важность теста	Опциональный
Тестовая процедура	1. Проверить наличие и спецификации северных интерфейсов по документации к системе управления и возможность их конфигурации в окне системы управления.
Ожидаемый результат	Описание северных интерфейсов для интеграции аварий, конфигурации и статистики представлено вендором и они являются открытыми.

7 Проверка сертификации оборудования БТД.

№	Процедура	Ожидаемый результат
7.1	Проверить документацию и убедиться, в том, что оборудование имеет действующий сертификат или декларацию.	Действующий сертификат или декларация о соответствии в соответствии с действующим законодательством РФ.