

Лабораторная работа 1

Изучение интерфейсов и принципов настройки точек доступа Wi-Fi

Цель работы

Освоить принципы настройки точек доступа Wi-Fi и изучить интерфейсы.

Общие сведения о настройках точек доступа

Настройки точек доступа различных производителей значительно отличаются. Однако основные принципы настройки и параметры настройки одинаковы для всех решений.

В любой точке доступа находятся один или несколько радиочипов (Рис. 1).

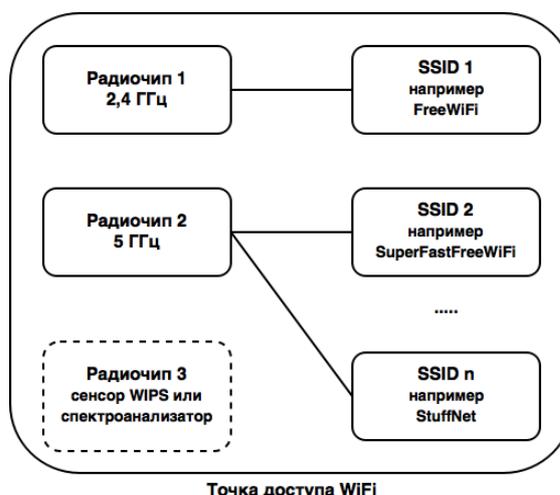


Рис. 1. Пример функциональной схемы настройки точки доступа

Большинство точек доступа класса SOHO содержат только один радиочип. Как правило этот радиочип может работать только в диапазоне 2,4 ГГц. Однако на рынке представлены решения, радиочипы которых можно переключать между диапазонами 2,4 и 5 ГГц. В последнее время появляется все больше устройств, содержащих одновременно 2 радиочипа, один из которых работает в диапазоне 2,4 ГГц, а другой — в диапазоне 5 ГГц.

В профессиональных точках доступа, как правило встроено два и более радиочипа, хотя существуют и «недорогие» решения с одним радиочипом, переключаемым между диапазонами 2,4 и 5 ГГц. Если устройство содержит 2 радиочипа, то один работает в диапазоне 2,4 ГГц, а другой — в диапазоне 5 ГГц. Также встречаются точки доступа с 3 радиочипами. Третий радиочип в них используется как сенсор системы обнаружения вторжений или спектроанализатор. Как правило, такие точки доступа самые дорогие в продуктовых линейках вендоров WiFi-решений.

На каждом из радиочипов можно запустить одну или несколько сетей WiFi, т.е. использовать один или несколько SSID одновременно. В последнем случае одна точка доступа (аппаратная) будет создавать сразу несколько WiFi-сетей, видимых для абонентских станций. Каждый SSID можно использовать для различных целей.

Например, может быть реализована следующая схема настройки (Рис. 1). В диапазоне 2,4 ГГц будет создана одна сеть WiFi (SSID = FreeWiFi). В диапазоне 5 ГГц эта же аппаратная точка доступа создаст 2 сети WiFi: SSID = SuperFastFreeWiFi и SSID = StuffNet. В приведенном примере абонентские станции, умеющие работать сразу в двух диапазонах, вероятно выберут сеть с названием SuperFastFreeWiFi. Абонентские станции диапазона 2,4 ГГц не увидят этой

сети и подключатся в сети FreeWiFi. Такая схема при настройке сети может быть использована в общественных местах, например в кафе или ресторане. Кроме того, для сотрудников кафе или ресторана будет создана сеть StuffNet, работающая в диапазоне 5 ГГц.

Таким образом, главная задача администратора при настройке оборудования заключается в создании SSID и налаживании связей между радиочипами и SSID.

Параметры настройки физического уровня обычно задаются в настройках радиочипа. Это могут быть используемый частотный канал, ширина канала, диапазон частот, мощность передатчика и др. Все остальные параметры задаются в настройках SSID: безопасность, допустимые модуляционно-кодирующие схемы, параметры QoS и др.

Принципы настройки Extreme Networks Altitude AP6521i

Для настройки радиочипа точки доступа Extreme Networks Altitude AP6521i с помощью веб-интерфейса необходимо перейти в меню Configuration -> Devices -> System Profile -> Interface -> Radios (Рис. 2). Далее следует выбрать радиочип из таблицы, кликнув по нему дважды мышью.

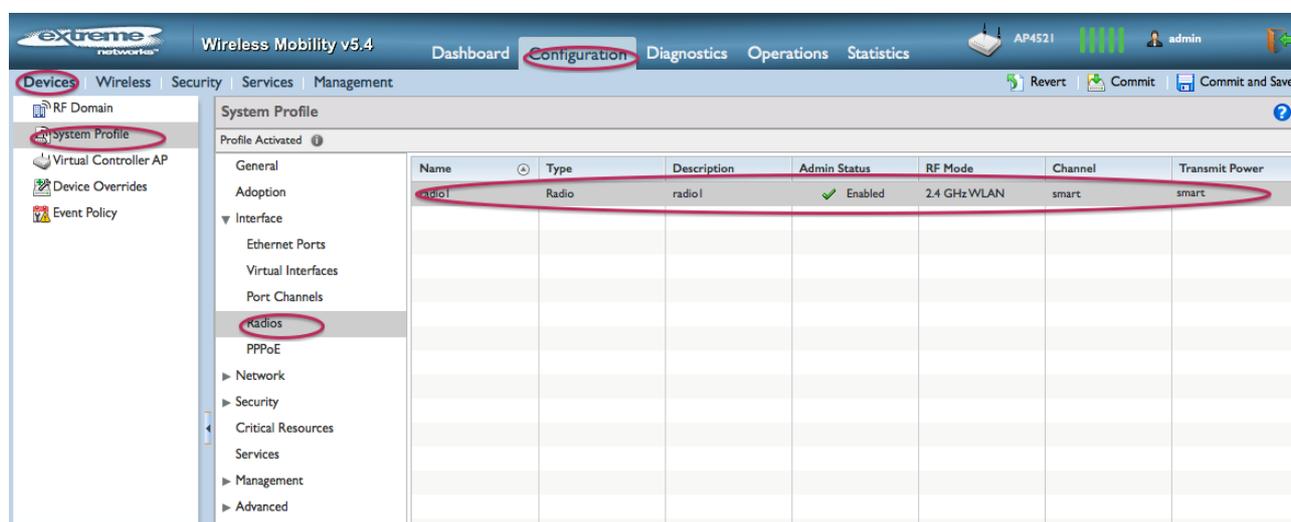


Рис. 2. Доступ к настройкам радиочипа

Раскроется окно настроек радиочипа (Рис. 3).

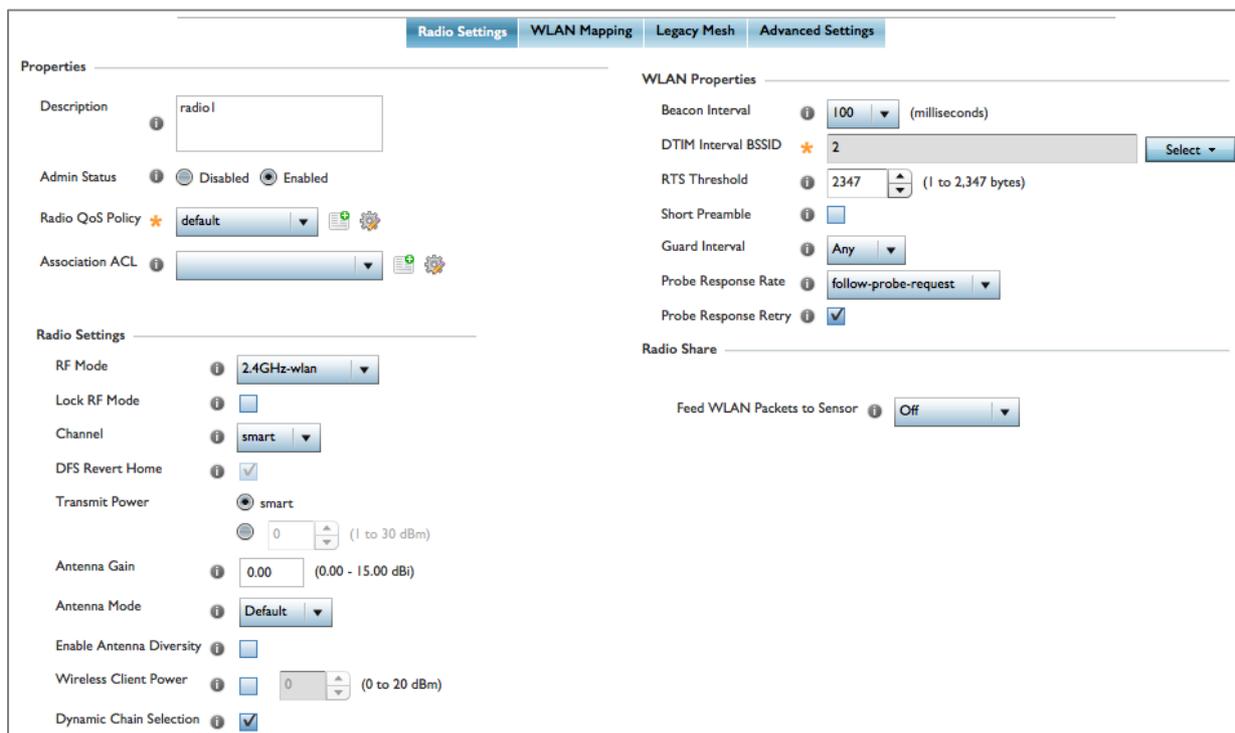


Рис. 3. Настройки радиочипа

Для создания и настроек SSID необходимо перейти в меню Configuration -> Wireless -> Wireless LANs (Рис. 4)

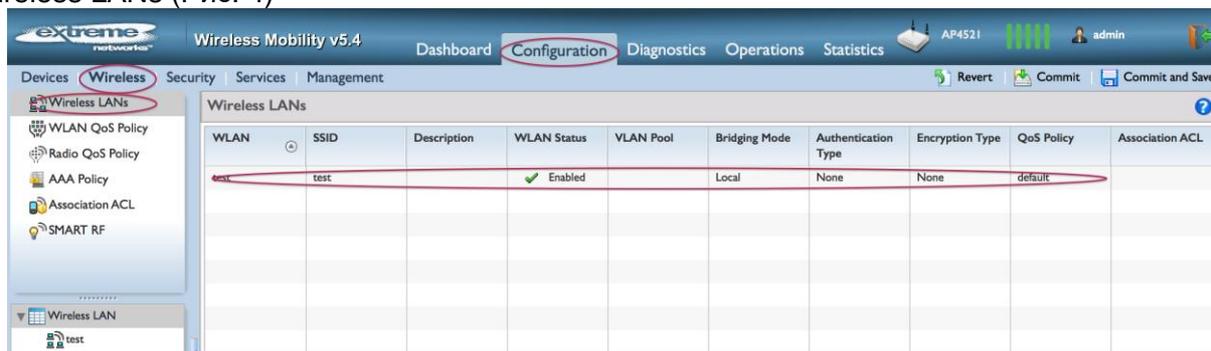


Рис. 4. Настройки сетей WiFi (SSID)

Для создания связи между радиочипом и SSID необходимо вернуться в окно настроек радиочипа (Рис. 2) и перейти во вкладку WLAN Mapping (Рис. 5).

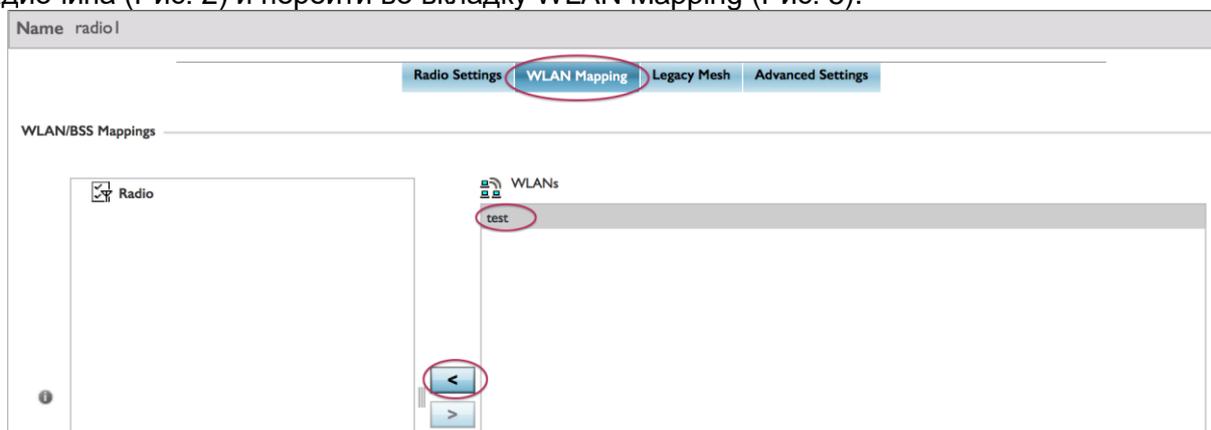


Рис. 5 Настройка связи между радиочипом и SSID

Задания

Найти в Интернете и записать конфигурацию MIMO для всех используемых в лаборатории точек доступа.

	Число радиочипов	Поддерживаемые диапазоны	MIMO-конфигурация	Максимальная скорость передачи на физическом уровне
Extreme Networks Altitude AP6521i				
Ruckus Wireless ZoneFlex 7372				

Табл. 1 Параметры точек доступа

Подключиться к точке доступа Extreme Networks Altitude AP6521i с использованием web-интерфейса. Пользуясь документацией к точкам доступа, ознакомиться с основными параметрами настройки радиочасти и создать тестовую сеть со следующими параметрами:

- SSID — [Test](#)
- защита WPA2-PSK (парольная фраза — [wifi_test_Lab](#))
- Ширина канала — [20](#) МГц
- Номер канала — [36](#)
- Отключить скорости [1, 2, 5,5, 11, 6, 9](#) Мбит/с в данном SSID.

С помощью Putty подключиться к точке доступа Extreme Networks Altitude AP6521i, используя протокол SSH. Пользуясь документацией к точкам доступа, ознакомиться с основными командами интерфейса командной строки (CLI) для управления точкой доступа.

После выполнения всех заданий выполнить сброс настроек точки доступа к заводским установкам. Для этого открыть терминал Putty или любой другой терминал SSH, подключиться к точке доступа и ввести следующие команды:

```
Welcome to CLI
```

```
Cannot handle term 'xterm-256color'. Setting term to dumb.
```

```
ap4521-71651E>enable
```

```
ap4521-71651E#erase startup-config
```

```
Erase startup-config? (y/n): y
```

```
ap4521-71651E#reload
```

```
The system will be rebooted, do you want to continue? (y/n): y
```

```
ap4521-71651E#Connection to 10.10.10.5 closed by remote host.
```

```
Connection to 10.10.10.5 closed.
```

Лабораторная работа 2

Изучение системы безопасности в сетях Wi-Fi

Цель работы

Проанализировать методы реализации безопасности в сетях Wi-Fi.

Предварительные шаги

Для выполнения данной работы необходим анализатор протоколов Wireshark и дампы пакетов, выложенные в материалах курса:

В ходе выполнения данной работы подготовить развернутый отчет о ходе выполнения данной лабораторной работы, описать выбранную методику анализа в Wireshark (с описанием выбранных фильтров).

Задание

Часть 1

- 1) Открыть в Wireshark дамп «*ConnectionOpenSystem.wcap*».
- 2) С помощью фильтров отобразить только фреймы отправленные «к» и «от» устройства с MAC-адресом 14:5a:05:d9:da:5a.
- 3) Найти процесс подключения к сети WiFi. Определить какие фреймы были отправлены на каждом из этапов подключения: сканирование, аутентификация, ассоциация. Изучить содержимое кадров Probe Request и Probe Response, Authentication, Association Request и Association Response.
- 4) Какие параметры абонентской станции и точки доступа можно узнать по указанным кадрам.

Часть 2

- 5) Открыть в Wireshark дамп «*ConnectionPSK.wcap*». С помощью фильтров отобразить только фреймы отправленные «к» и «от» устройства с MAC-адресом 14:5a:05:d9:da:5a. Найти процесс подключения к сети WiFi. Определить какие фреймы были отправлены на каждом из этапов подключения: сканирование, аутентификация, ассоциация. Изучить содержимое кадров Probe Request и Probe Response, Authentication, Association Request и Association Response.
- 6) Какие параметры абонентской станции и точки доступа можно узнать по указанным кадрам. Изучить какие фреймы были отправлены в процессе 4 Way Handshake.
- 7) Можно ли после обмена 4 Way Handshake считать содержимое фреймов с данными. Если нельзя, то почему.
- 8) Расшифруйте фреймы с данными для станции с MAC-адресом 14:5a:05:d9:da:5a, которые передавались после установления режима шифрования в дампе «*ConnectionPSK.wcap*». Для этого воспользуйтесь приведенными источниками:
 - [How to Decrypt 802.11](#)
 - [Decrypt WPA2](#)
 - [Расшифровка WPA2-PSK трафика с использованием wireshark](#)

В качестве парольной фразы для SSID Bonch используйте «FtYpp86z».

Представить развернутый отчет о ходе выполнения данной лабораторной работы, описать выбранную методику анализа в Wireshark (с описанием выбранных фильтров).

Ответить на следующие вопросы:

- Почему Wireshark может расшифровать трафик данных для этого MAC-адреса?
- Можно ли расшифровать трафик с данными других абонентских станций? Если нет, то почему.

Лабораторная работа 3

Ознакомление с принципами функционирования и основными протоколами LTE

Цель работы

Ознакомится с ключевыми аспектами настройки оборудования eUTRAN, EPS, IMS, а также проанализировать сетевой трафик сети LTE.

Применяемое оборудование, ПО и данные

- 1) Персональный компьютер с ОС Windows, ОС Linux или ОС MacOS
- 2) ПО Wireshark, ПО PuTTY (для Windows), любой терминал (для Linux и MacOS)
- 3) Записанные дампы

Порядок выполнения работы

1. Ознакомиться с конфигурационными файлами различных элементов конфигурации LTE-сети и IMS-сети.
2. По очереди открыть различные дампы
3. ok_voice_call.pcapng
Здесь можно прослушать голос
4. 3009 2ue ok.pcapng
Сравнить UE capabilities
5. Открыть файлы ho1.pcapng и ho2.pcapng и проанализировать процедуру хэндовера.

Порядок обработки результатов

Представить результаты работы, в следующем формате.

Вставить соответствующий скриншот

Рис. <Номер рисунка> — Название

Указать инструмент, использованный для получения.

Сделать выводы

Лабораторная работа 4

Исследование аппаратного состава базовых станций (eNodeB) и их характеристик

Цель работы: изучение аппаратного состава базовых станций (eNodeB) и их характеристик на примере создаваемого в программном комплексе шаблона.

Выполнение работы:

1. Создать новый проект;
2. Создать район расчета 4G площадью не менее 20 км² с моделью расчета Klin_2_5_City, шагом расчета = 100 м., эквивалентным числом абонентов = 10 000 чел. и абонентским терминалом LTE_class_4_20МГц
3. Поместить в созданный район расчета шаблон eNodeB, процесс создания которого описан ниже:

Создание шаблона:

- Перейти во вкладку «Справочники»;
- Нажать значок «+» около строки «Шаблоны БС»;
- Нажать значок «+» около папки «LTE»;
- Выделить единичным «щелчком» левой клавиши мыши папку нужного стандарта и нажав правую кнопку мыши создать выбрать «Создать шаблон БС» (рис 4.1).

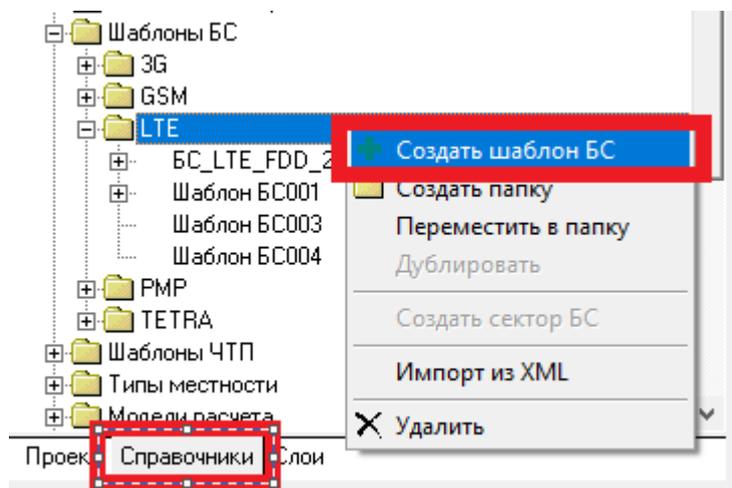


Рис. 4.1. Создание шаблона БС

Редактирование шаблона:

- В колонке «Название» таблицы параметров созданного шаблона БС навести курсор мыши на «Сектора» и затем, нажав правую кнопку мыши, выбрать «Добавить сектор» (рис. 4.2);

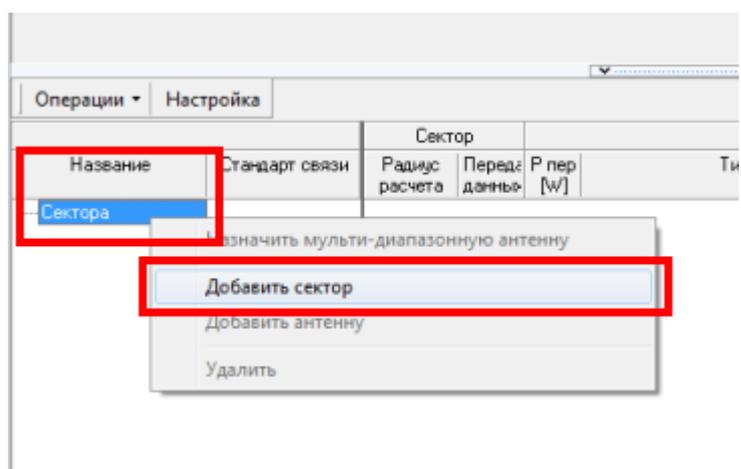


Рис. 4.2. Добавление сектора БС

- В появившемся окне (рис. 4.3) в строке «Стандарт сети» нажать на значок «...»;

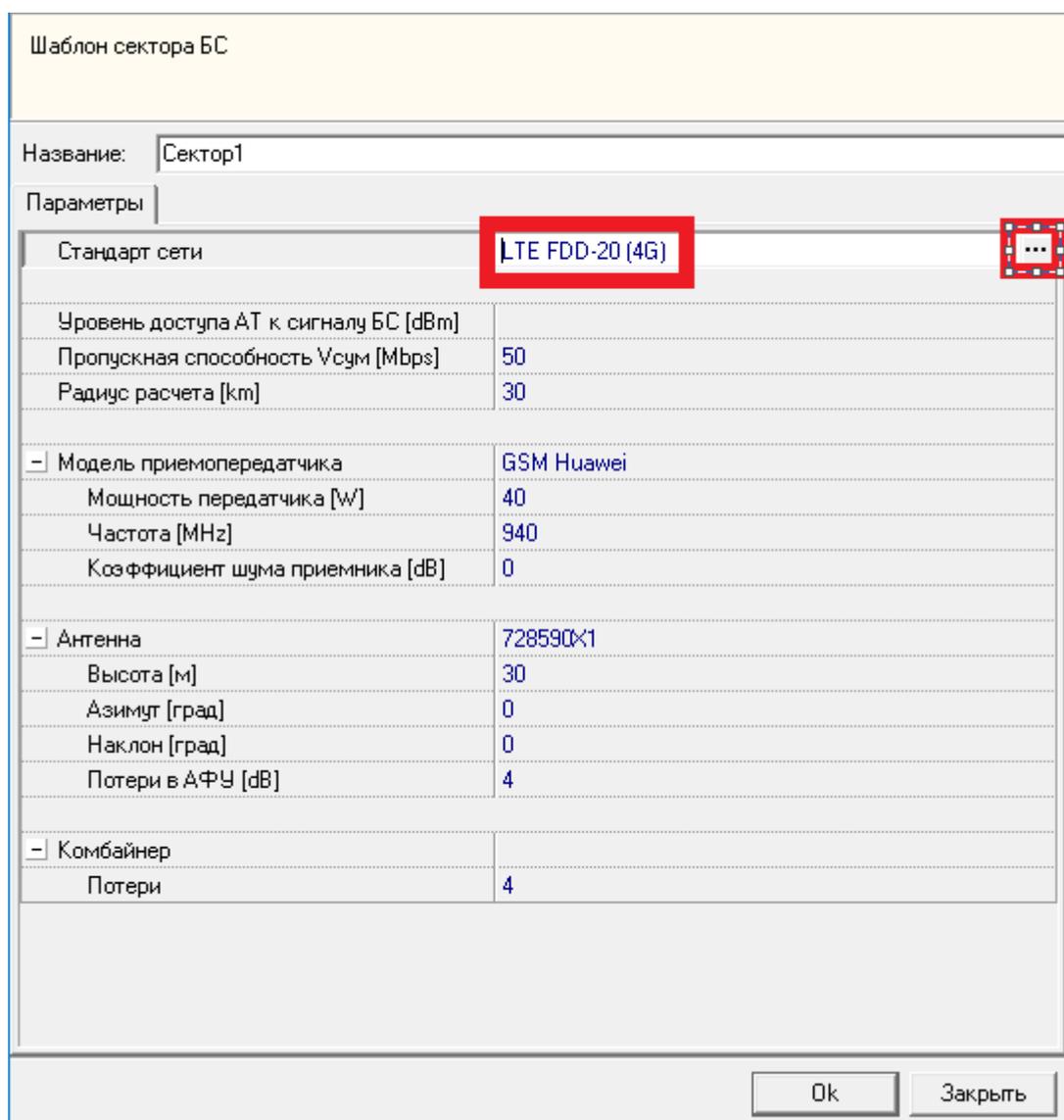


Рис. 4.3. Параметры шаблона сектора БС

- В открывшемся окне выбрать стандарт «LTE FDD-20» и нажать «ОК»;

- В параметрах шаблона сектора (см. рис. 4.3) в строке «Антенна» указать модель антенного оборудования с КУ = 10...18,8 дБи. Следует помнить, что ширина диаграммы направленности в горизонтальной плоскости у выбранной антенны должна находиться в пределах $\theta_H = 60...65^\circ$. На рис. 4.4 показаны примеры отображения ДН антенны в горизонтальной и вертикальной плоскостях.

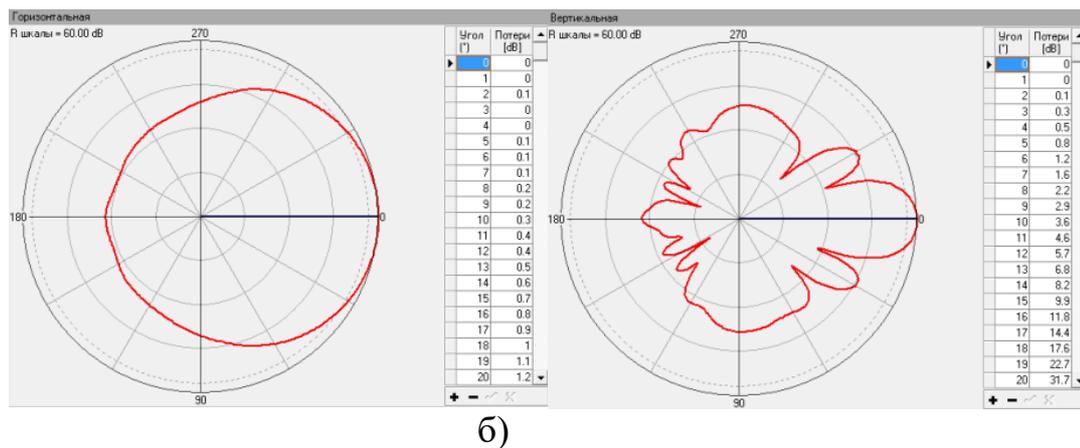


Рис. 4.4. ДН выбранной антенны БС (а – в горизонтальной плоскости; б – в вертикальной плоскости)

- В строке «Радиус расчета [km]» установить значение = 35;
- В строке «Высота [m]» установить значение = 30;
- В строке «Модель приемопередатчика» указать оборудование по указанию преподавателя;
- В строке «Комбайнер» выбрать параметр «Комбайнер» и ниже в поле «Потери» указать значение по указанию преподавателя. Нажать на кнопку «ОК» (рис. 4.5);

Шаблон сектора БС

Название: Сектор1

Параметры

Стандарт сети	LTE FDD-20 (4G)
Уровень доступа АТ к сигналу БС [dBm]	
Пропускная способность Vsum [Mbps]	50
Радиус расчета [km]	30
Модель приемопередатчика	GSM Huawei
Мощность передатчика [W]	40
Частота [MHz]	940
Коэффициент шума приемника [dB]	0
Антенна	728590X1
Высота [м]	30
Азимут [град]	0
Наклон [град]	0
Потери в АФУ [dB]	4
Комбайнер	
Потери	4

Ok Закрыть

Рис. 4.5. Заполнение шаблона параметров сектора БС

- Аналогичным образом добавить еще 2 сектора (сформированная ранее конфигурация оборудования будет сохраняться по умолчанию при создании новых секторов);

- В таблице параметров шаблона БС в графе «Антенна» → «Азимут» установить значения 0°, 120° и 240° для 1, 2 и 3 сектора соответственно (рис. 4.6);

Антенна						Комбайнер	
Частота [MHz]	Электрический наклон [°]	Высота [m]	Азимут [°]	Наклон [°]	Потеря АФУ	Тип	Потеря [dB]
1767.5	0	30	0	0	2	Комбайнер	3
1767.5	0	30	120	0	2	Комбайнер	3
1767.5	0	30	240	0	2	Комбайнер	3

Рис. 4.6. Азимуты секторов.

ПРИМЕЧАНИЕ: выбор фидера осуществляется после установки созданного шаблона БС в район расчета путем перехода во вкладку «Проект» → папка «БС подвижной связи» → двойной «клик» левой клавиши мыши на выбранную БС. В появившемся окне (рис. 4.7.) выбрать графу «Фидер» и в колонке «Название» для каждой антенны указать оборудование, подходящее под планируемый частотный диапазон с выбранными параметрами;

		Фидер			
Название	Cell ID	Название	Здельные потери	Длина [m]	Потери [dB]
GSM900					
Сектор1	5				
Антенна1		...	X		
Сектор2	6				
Антенна1					
Сектор3	7				
Антенна1					

Рис. 4.7. Выбор фидера

4. Посчитать созданный шаблон eNodeB, для чего:

- 4.1 Разместить eNodeB в районе расчета 4G;
- 4.2 Включить eNodeB в состав района расчета;
- 4.3 Сделать район расчета **активным**;
- 4.4 Создать модель трафика 3G/4G и добавить в нее видео (с параметрами по умолчанию);
- 4.5 Создать конфигурацию сети (кликнуть правой кнопкой мыши на название района расчета и выбрать соответствующий пункт);
- 4.6 В созданной конфигурации нажать на «Операции», далее «Расчет»;
- 4.7 Сделать конфигурацию **активной** и выполнить общий расчет поля;
- 4.8 Сделать скриншоты карт скоростей передачи данных для неподвижного и подвижного абонентов на улице, в автомобиле и здании.

Содержание отчета:

- 1) Список оборудования созданного шаблона eNodeB;
- 2) Карты скоростей передачи данных для неподвижного и подвижного абонентов на улице, в автомобиле и здании.

Контрольные вопросы:

- 1) Чем обоснован выбор модели Klin_2_5_City в расчетах уровня поля?
- 2) Из каких элементов состоит шаблон eNodeB?
- 3) На что стоит обратить внимание при выборе места установки eNodeB?
- 4) Чем объясняются различные скорости передачи данных для неподвижного и подвижного абонентов на улице, в автомобиле и здании?
- 5) Как изменится покрытие eNodeB, если изменить высоту подвеса антенны и угол ее наклона?
- 6) Чем объясняется выбор антенн для eNodeB?

Лабораторная работа 5. Планирование сетей LTE с использованием программного комплекса.

Цель работы: освоить принципы планирования сотовой сети мобильной связи стандарта LTE в программном комплексе ONEPLAN.

Выполнение работы:

- 1) Создать в городской местности район расчета 4G площадью 50 км² по модели Klin 2_5 City и числом абонентов = 10000 (рис. 5.1);

Параметры	
Название:	Район расчета (4G)001
Папка	\
Модель расчета	Klin_2_5_City
Шаг расчета [m]	10
Эквивалентное количество абонентов в районе	10000
Тип местности	default
Абонентский терминал (AT)	LTE_class_4_20MГц

Рис. 5.1. Параметры района расчета 4G.

- 2) Разместить в созданный район 1 eNodeB, используя шаблон из лаб. раб. №4. Включить eNodeB в район расчета и сделать его активным (рис. 5.2.).

Базовые станции

Выбрать по критерию 1. БС внутри района

Выбрать из файла

БС, включенные в состав района

БС, не включенные в состав района

Имя	Номер	Статус
БС		

* Нет данных *

Рис. 5.2. Включение eNodeB в состав района.

- 3) Создать модель трафика (рис.5.3) 3G/4G;

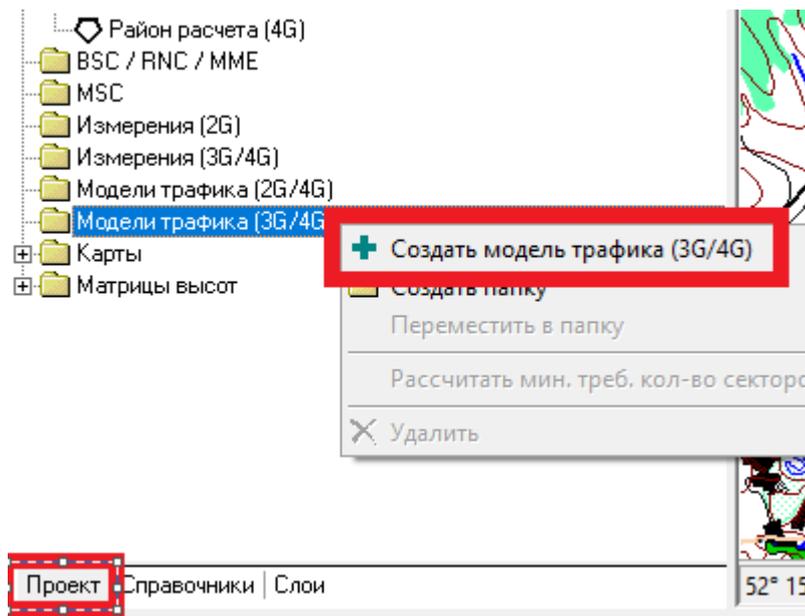


Рис. 5.3. Создание модели трафика.

- 4) Добавить в созданную модель трафика передачу данных со скоростью 60 Мбит/с (рис. 5.4).

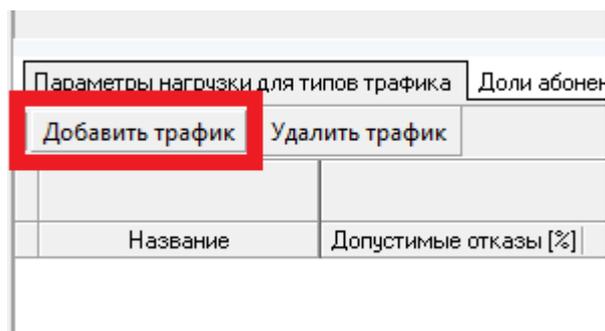


Рис. 5.4. Добавление вида трафика в модель

- 5) Создать конфигурацию сети (кликнуть правой кнопкой мыши на название района расчета и выбрать соответствующий пункт) (рис.5.5.).

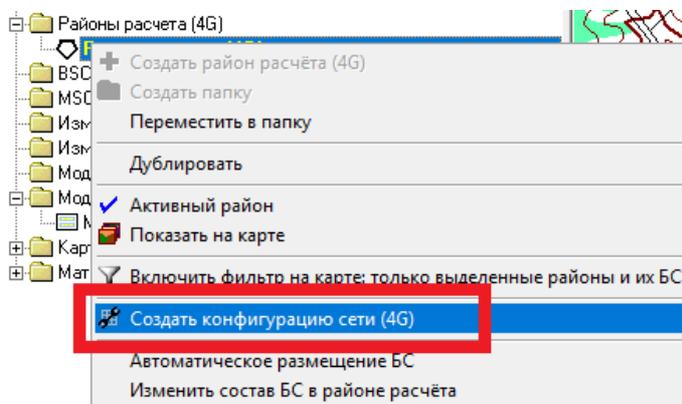


Рис. 5.5. Создание конфигурации сети.

- 6) В созданной конфигурации нажать на «Операции», далее «Расчет» (рис. 5.6).

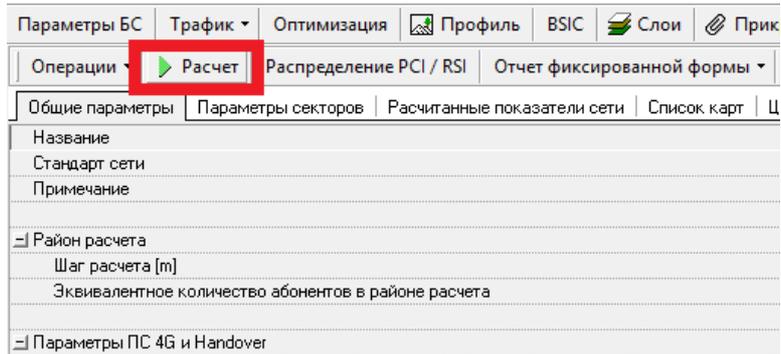


Рис. 5.6. Расчет сетевой конфигурации.

- 7) Далее сделать конфигурацию *активной* и выполнить общий расчет поля;
- 8) Разместить еще некоторое количество eNodeB так, чтобы добиться сплошного покрытия района (отношение SINR между соседними eNodeB не менее -3 dB.).

Пример территориального распределение параметра SINR на входе UE для промоделированного фрагмента представлено на рис. 5.7.

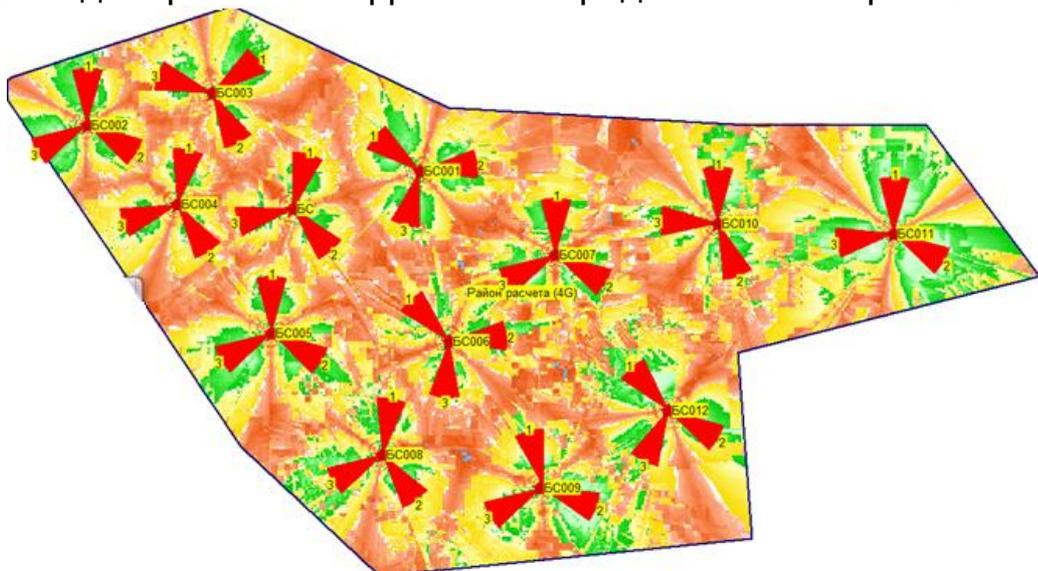


Рис. 5.7. Территориальное распределение параметра SINR на входе UE

- 9) Для оценки радиосети в данной работе следует также использовать показатель RSRP, требуемые значения которого для заданного фрагмента радиосети представлены в таблице 5.1.

Таблица 5.1. Требования к проектируемой сети

Критерий	Результат
RSRP	≥ -100 дБм
Покрытие территории	$\geq 95\%$
SINR	≥ -3 дБ
Средняя скорость на абонента DL Мбит/с	60

Пример территориального распределения параметра RSRP на входе UE для промоделированного фрагмента представлено на рис. 5.8.

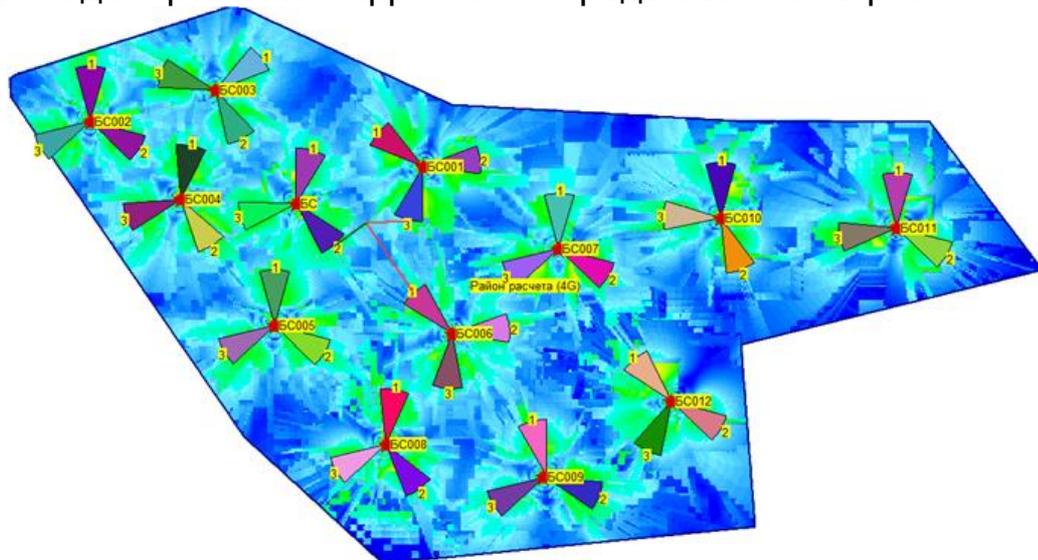


Рис. 5.8. Территориальное распределение параметра RSRP на входе UE

- 10) Поочередно обеспечить требование по средней скорости передачи данных (см. Табл. 5.1) для неподвижного и подвижного абонентов на улице, в автомобиле и здании.

Содержание отчета:

- 3) Карты скоростей передачи данных для неподвижного и подвижного абонентов на улице, в автомобиле и здании;
- 4) Карта SINR;
- 5) Карта RSRP;

Контрольные вопросы:

- 1) Чем обусловлена необходимость использования специализированного программного комплекса при решении задачи планирования сети?
- 2) От чего зависит требуемое количество eNodeB в сети?
- 3) Назовите перечень основных исходных данных, необходимых для планирования сети стандарта LTE.
- 4) В чем заключается сходство и различие в подходах к планированию сетей GSM, UMTS и LTE?
- 5) На основании анализа каких параметров, полученных в программном комплексе, можно сделать предварительный вывод о выполнении/не выполнении задачи планирования сети LTE?

Лабораторная работа 5

Ознакомление с принципами функционирования и основными протоколами 5G

Цель работы

Проанализировать сетевой трафик сети Vo5G.

Применяемое оборудование, ПО и данные

- 1) Персональный компьютер с ОС Windows, ОС Linux или ОС MacOS
- 2) ПО Wireshark, ПО PuTTY (для Windows), любой терминал (для Linux и MacOS)
- 3) Записанные дампы

Порядок выполнения работы

1. Ознакомиться с конфигурационными файлами различных элементов конфигурации 5G-сети и IMS-сети.
2. По очереди открыть различные дампы
3. ok_voice_call.pcapng
Здесь можно прослушать голос
4. 3009 2ue ok.pcapng
Сравнить UE capabilities
5. Открыть файлы ho1.pcapng и ho2.pcapng и проанализировать процедуру хэндовера.

Порядок обработки результатов

Представить результаты работы, в следующем формате.

Вставить соответствующий скриншот

Рис. <Номер рисунка> — Название

Указать инструмент, использованный для получения.

Сделать выводы