Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра геометрии и компьютерных наук

ПОСТРОЕНИЕ И НАСТРОЙКА БЕСПРОВОДНЫХ СЕТЕЙ

Методические указания

Рекомендовано к изданию редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» для обучающихся по программам высшего образования по направлению подготовки 02.04.02 Фундаментальная информатика и информационные технологии

Оренбург
2017

УДК 004.732 (076.5)
ББК 32.973.202я7
П63

Рецензент – кандидат технических наук Д. В. Горбачев
Авторы: Ю. А. Ушаков, М. В. Ушакова, П. Н. Полежаев, А. Л. Коннов

П63 Построение и настройка беспроводных сетей : методические указания / Ю. А. Ушаков, М. В. Ушакова, П. Н. Полежаев, А. Л. Коннов; Оренбургский гос. ун-т. – Оренбург : ОГУ, 2017.

Методические указания содержат методику проектирования, развертывания и настройки беспроводных сетей.

Методические указания предназначены для выполнения лабораторных работ по дисциплине «Компьютерные коммуникации и сети» для магистров направления подготовки 02.04.02 Фундаментальная информатика и информационные технологии.

УДК 004.732 (076.5)
ББК 32.973.202я7

Содержание

Введение 5

1 Теоретические сведения по беспроводным сетям 7

1.1 Принципы работы беспроводных сетей 7

1.2 Типы локальных беспроводных сетей 7

1.3 Обеспечение безопасности беспроводных сетей 9

1.4 Методика развертывания корпоративной беспроводной сети 11

2 Лабораторная работа №1 – Проектирование зоны покрытия беспроводной сети .. 13

2.1 Теоретические сведения 13

2.2 Задание на лабораторную работу 16

3 Лабораторная работа №2 – Проектирование обеспечивающей инфраструктуры .. 17

3.1 Теоретические сведения 17

3.1.1 Выбор аппаратного обеспечения 17

3.1.2 Проектирование проводной сети 20

3.1.3 Проектирование электропитания PoE 20

3.1.4 Пассивные элементы сети 22

3.2 Задание на лабораторную работу 23

4 Лабораторная работа №3 – Настройка контроллера точек доступа 24

4.1 Теоретические сведения 24

4.1.1 Базовая настройка контроллера 24

4.1.2 Настройка взаимодействия с точками доступа 34

4.1.3 Настройка контроллера OpenFlow 34

4.1.4 Настройка взаимодействия точек доступа с контроллером OpenFlow 35

4.2 Задание на лабораторную работу 36

5 Лабораторная работа №4 – Тестирование беспроводной сети 37

5.1 Теоретические сведения 37

5.2 Задание на лабораторную работу 39

Список использованных источников 40

Введение

При повсеместном внедрении беспроводных технологий в последние годы изучение работы беспроводных сетей стандарта IEEE 802.11n и IEEE 802.11ac является ключом к пониманию правильной проектирования и настройки радиочастотной и канальной части. Также важны такие исследования при разработке программных методов улучшения работы беспроводных сетей, драйверов, разработки расширений протоколов.

Среднее количество беспроводных устройств на одну точку доступа даже в домашних сетях уже приблизилось к трем, в многоквартирных домах беспроводные сети полностью используют весь диапазон 2.4ГГц при крайне высокой плотности сетей.

Корпоративные беспроводные сети должны поддерживать широкий спектр услуг и функциональных возможностей, такие как: аутентификация, авторизация и учет, управление политикой безопасности, динамическое конфигурирование канала, мобильность, помехоустойчивость и балансировка нагрузки. Решения, направленные на охват всех этих услуг, закрыты для изменения и копирования законодательными актами, с закрытым исходным кодом, что приводит к использованию оборудования конкретного производителя.

Современные корпоративные беспроводные сети стандарта IEEE 802.11 [1] включают в себя от нескольких десятков до тысяч точек доступа, которые должны обслуживать большое число пользователей. Пользователи подключаются к корпоративной беспроводной сети с помощью множества устройств включая смартфоны, коммуникаторы и планшеты. Независимо от размера эти сети должны предоставлять различный набор сервисов с возможностью их масштабирования. Сервисы включают поддержку аутентификации, доступа и учета, управления сетью на основе политик, обнаружения и предотвращения вторжений, управление мобильностью, балансировку нагрузки, а также предоставляют динамическую настройку канала и гарантированное качество обслуживания. Управление такими

сетями обычно централизовано (через контроллер) и является одним из видов программно-управляемой инфраструктуры.

Контролирование сетевого трафика происходит посредством программного обеспечения, так же, как в ПКС (программно-конфигурируемых сетях). Протокол OpenFlow [2-5] считается родоначальником ПКС, он предоставляет собой стандартизированный способ, который может быть использован контроллером для управления таблицами коммутации. Создание средства для программирования беспроводных сетей даст сетевым провайдерам возможность реализовать специфику конкретно взятой сети. Программируемость так же исключает потребность в разработке крупной системы управления и дает возможность использовать в сети оборудование различных производителей.

Особенность беспроводных сетей в том, что в отличие от проводных сетей передачи данных, для них существует ряд специфических проблем. По стандарту IEEE 802.11 клиенты выбирают точки доступа на основе собственного решения (от операционной системы или от драйвера сетевой карты). Стандарт не описывает механизм выбора точки доступа по мощности сигнала, и это существенно усложняет управление клиентами в стандартной инфраструктуре.

Также сочетание промышленного контроллера управления точками доступа с возможностью внешнего управления и программно-конфигурируемой сети позволяет более гибко использовать все возможности оборудования.

В связи со сказанным выше весьма актуальным является детальное изучение технологий беспроводных сетей в рамках дисциплины «Компьютерные коммуникации и сети». Данные методические указания описывают выполнение лабораторных работ, охватывающих все этапы создания беспроводной сети – от проектирования до реализации и тестирования.

1 Теоретические сведения по беспроводным сетям

1.1 Принципы работы беспроводных сетей

Беспроводные сети — это технология, позволяющая создавать сети, соответствующие стандартам для обычных проводных сетей, без использования кабельной проводки. IEEE 802.11 является общепринятым стандартом построения беспроводных сетей, это набор стандартов связи, для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 2.4 ГГц и 5 ГГц.

В основе работы беспроводных сетей лежит принцип разделения канального уровня на два подуровня – верхний и нижний. Нижний уровень управляется аппаратным образом, а верхний уровень осуществляет управление кадрами данных, таких как пробный пакет, пакеты аутентификации и привязки клиента и соответствующие ответные пакеты. Верхний уровень управляется программным образом, драйвером, системной программой или даже удаленным контроллером (как в случае промышленных контроллеров беспроводных сетей)

Клиент или пассивно узнает о точках доступа, которые периодически рассылают широковещательные кадры, или активно, посредством поиска. Когда клиент собирается присоединиться к беспроводной сети, он сканирует пространство в поисках доступных сетей, путем отправки пробного кадра на все каналы. Точки доступа, которые получают этот кадр и готовы принять подключение клиента, отправляют ответ на этот кадр (ACK), таких точек доступа может быть несколько. Далее клиент посылает аутентификационный кадр и ждет ответ, после чего от клиента следует запрос на привязку к точке доступа и ответ точки доступа, потом запускается механизм авторизации.

1.2 Типы локальных беспроводных сетей

Спецификация уровня доступа сети (MAC) IEEE 802.11 имеет 2 режима работы – специальный режим (Ad-hoc) и режим инфраструктуры. В режиме Ad-Hoc две и более беспроводных станции (STA) распознают друг друга и устанавливают

соединение без использования другого оборудования по принципу одноранговой сети. В режиме инфраструктуры имеется точка доступа, которая централизованно управляет передачей данных между ассоциированными с ней клиентами. Точка доступа и ассоциированные с ней клиенты образуют так называемый BSS (basic service set, зону с базовым набором услуг), работающий в не лицензируемом радиочастотном диапазоне.

Несколько точек доступа, подключаемых через распределенные системы (DS, Distribution System) расширяет BSS в ESS (Enhanced Service Set, расширенный набор услуг) в соответствии с рисунком 1.

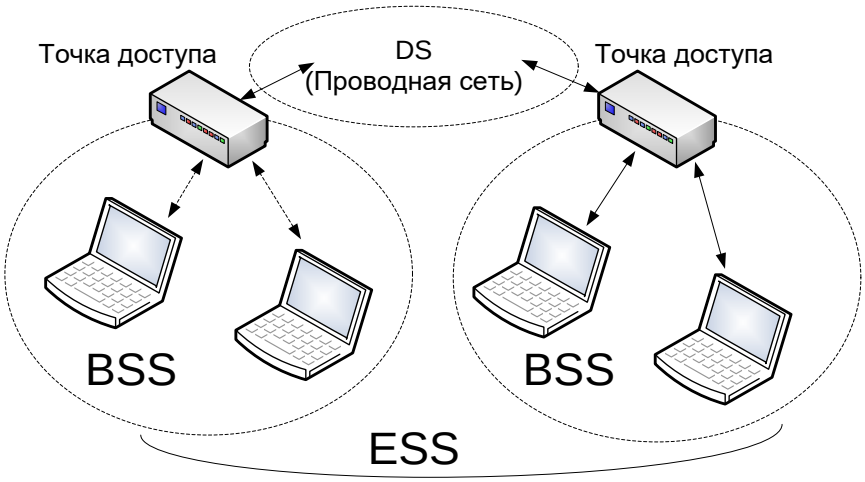

Рисунок 1 – Схема работы ESS

На самом деле, каждое беспроводное устройство, выполненное на аппаратной платформе, поддерживающей BSS, может работать в следующих режимах:

а) AP (Access Point) – режим точки доступа;

б) STA (Station) – клиент беспроводной сети;

в) Ad-Hoc – децентрализованный клиентский режим без точек доступа;

г) Monitor – режим перехвата всех пакетов на беспроводном канале;

в) WDS (Wireless Distribution System) – режим расширения зоны охвата, практически это режим повторителя третьего уровня OSI.

Остальные режимы являются дополнительными и не всегда поддерживаются драйверами и программным обеспечением.

В режиме точки доступа устройство периодически передает специальные пакеты (beacon) для идентификации имени сети (SSID, Service Set Identificator), которые принимают клиенты и отображают имя в списке доступных сетей. Это имя SSID может также и не содержаться в пакетах beacon (отключение широковещания SSID) или содержаться в зашифрованном виде (шифрование SSID).

1.3 Обеспечение безопасности беспроводных сетей

В беспроводных сетях основной проблемой безопасности является общая незащищенная среда доступа. Поэтому все меры по обеспечению безопасности делятся на два типа:

а) шифрование для предотвращения перехвата трафика;

б) аутентификация или авторизация для подтверждения прав доступа к сети.

Как правило, эти методы используются параллельно, после проверки ключа шифрования выполняется авторизация по уже защищенному каналу. Для шифрования в настоящий момент целесообразно использовать только WPA и WPA2 (Wi-Fi Protected Access) методы. При этом в корпоративных средах используют дополнительные надстройки для авторизации IEEE 802.1x EAP (Extensible Authentication Protocol, расширяемый протокол аутентификации), позволяющую проводить авторизацию по множеству параметров, таких как логин, пароль, ключ, сертификат. В случае использования EAP шифрование может использоваться TKIP, AES или CCMP, но не все системы корректно работают с протоколом CCMP. Без аутентификации доступ в сеть будет запрещен. БД пользователей и система проверки в корпоративных сетях расположены на сервере RADIUS.

Большинство версий Windows требуют для корректной аутентификации EAP валидный серверный сертификат SSL, без которого запрещают сам сеанс аутентификации.

Беспроводное сетевое подключение должно быть защищено методом шифрования WPA2-Enterprise.

Чаще всего предусматривают две категории доступа к беспроводной сети:

а) Персональный авторизованный доступ.

1) Подключение компьютеров/ноутбуков организации и других устройств пользователей, прошедших обязательную регистрацию в личном кабинете на сайте, должно осуществляться по команде пользователя. По запросу операционной системы вводится регистрационное имя личной учётной записи. Затем вводится пароль в соответствующее поле запроса системы. После успешного сетевого соединения доступ предоставляется к Web-ресурсам по протоколу HTTP, а также к общим сетевым папкам.

2) Подключение личных компьютеров/ноутбуков сотрудников и других устройств осуществляется аналогично зарегистрированным устройствам. При этом методе подключения общие сетевые папки недоступны.

Пользователям необходимо произвести настройку в своей операционной системе беспроводного сетевого подключения с соответствующим SSID в зависимости от версии операционной системы, используемой на клиентском устройстве.

б) Гостевой авторизованный доступ. Чтобы получить временный доступ к беспроводной сети для гостя организации должна предварительно подаваться заявка. После ее оформления для гостя активируется временная учётная запись, атрибуты которой отправляются ответственному лицу, подавшему заявку, на указанный электронный адрес. Пользователям также необходимо произвести настройку беспроводного сетевого подключения. Доступ предоставляется только к Web-ресурсам по протоколу HTTP.

Пропускная способность гостевого и общего доступа к сети Интернет должна квотироваться.

Для упрощения самостоятельной регистрации пользователей через личный кабинет может быть создана открытая незащищенная сеть с отдельным SSID, предоставляющая доступ только в личный кабинет для регистрации.

1.4 Методика развертывания корпоративной беспроводной сети

В общем случае при установке беспроводной сети в помещениях методика выглядит следующим образом:

а) необходимо на плане помещений отметить необходимые зоны охвата беспроводной сети;

б) разделить зону на части радиусом не более 20 метров и в центре обозначить точку доступа;

в) провести тестовую установку точки доступа в каждую отмеченное место на плане, по факту проверить зону покрытия и отметить уровень сигнала на краях проектируемой зоны каждой точки, а при уменьшении зоны отметить ее на плане;

г) с учетом корректировок рассчитать необходимое количество кабеля, сопутствующих монтажных элементов, портов коммутаторов с поддержкой питания PoE, источников бесперебойного питания;

д) произвести установку кабеля от ближайших мест доступа в сеть до места установки точек доступа;

е) произвести установку шкафов, сетевого оборудования, кабельного и кроссировочного оборудования;

ж) установить контроллер в центральную серверную, обеспечить подключение к требуемым подсетям (корпоративная сеть, Интернет, сеть WiFi);

и) установить сервер и ПО для управления контроллером в центральную серверную, обеспечить связность с контроллером;

к) провести первоначальную настройку контроллера, активировать лицензии на контроллер и ПО;

л) создать пилотную сеть, установив 3 точки в места, где их зоны покрытия пересекаются;

м) создать на контроллере несколько сетей со своими SSID и правилами авторизации;

н) провести тестирование авторизации 802.1x (только WPA2 TKIP), веб-авторизации, open-авторизации;

п) после отладки авторизации необходимо заполнить базу пользователей или создать внешний шлюз авторизации с синхронизацией с внутренними базами пользователей (например, домен Active Directory);

р) провести монтаж оставшихся точек доступа, провести тестирование зон покрытия, задокументировать все изменения в проект;

с) провести обучение технического персонала, обеспечить доступ к документации, техподдержке производителей.

Основные базовые этапы развертывания корпоративной беспроводной сети будут представлены в виде отдельных лабораторных работ.

2 Лабораторная работа №1 – Проектирование зоны покрытия беспроводной сети

2.1 Теоретические сведения

Первоначально, после указания на плане необходимой зоны покрытия нужно проверить радиопроницаемость материала стен, другие факторы, влияющие на распространения радиосигнала. Для этого необходимо на плане помещений разделить зону покрытия на части с радиусом не более 20 метров и не менее 10 метров. Если часть зона находится в большом помещении или коридоре без стен, то в этих местах радиус можно увеличивать до 30-40 метров. В центре зон необходимо отметить предполагаемые места установки точек доступа, например, как показано на рисунке 2.

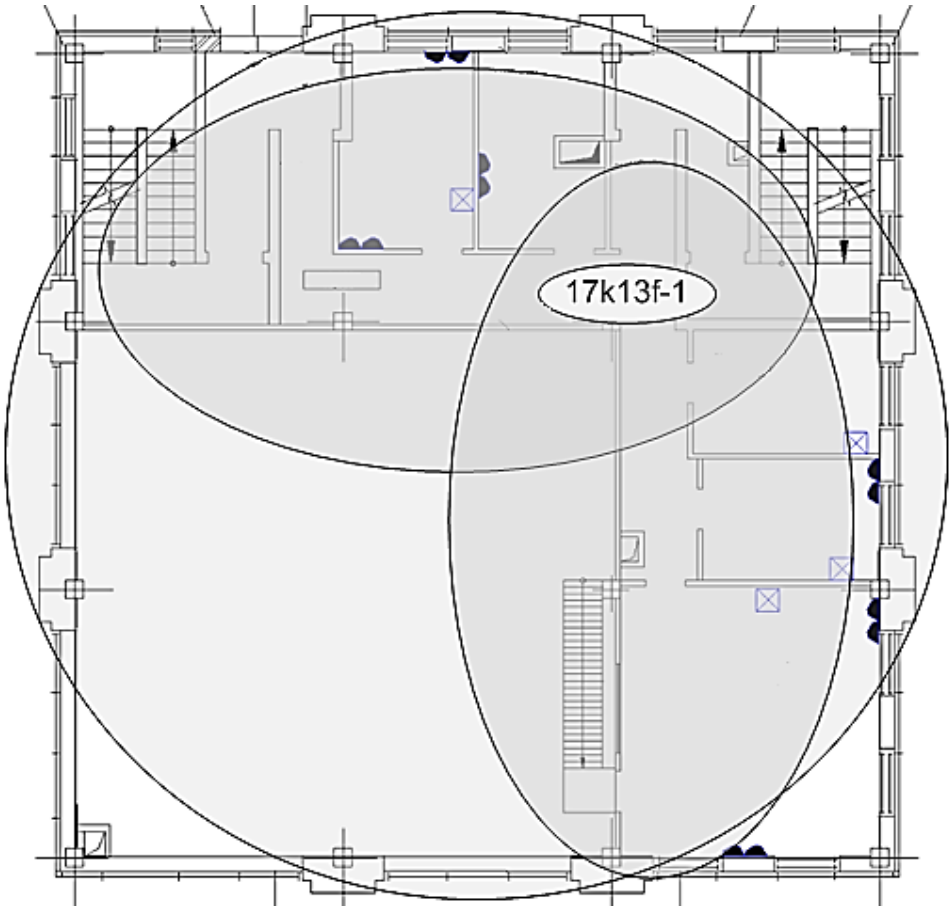

Рисунок 2 – Примерный план покрытия и разделения за зоны

Место примерной установки точки доступа отмечено именем точки, сформированном из номера корпуса, этажа и порядкового номера на этаже. Если предполагается несколько точек, то необходимо, что бы из зоны пересекались для обеспечения непрерывного покрытия, как, например, на рисунке 3.

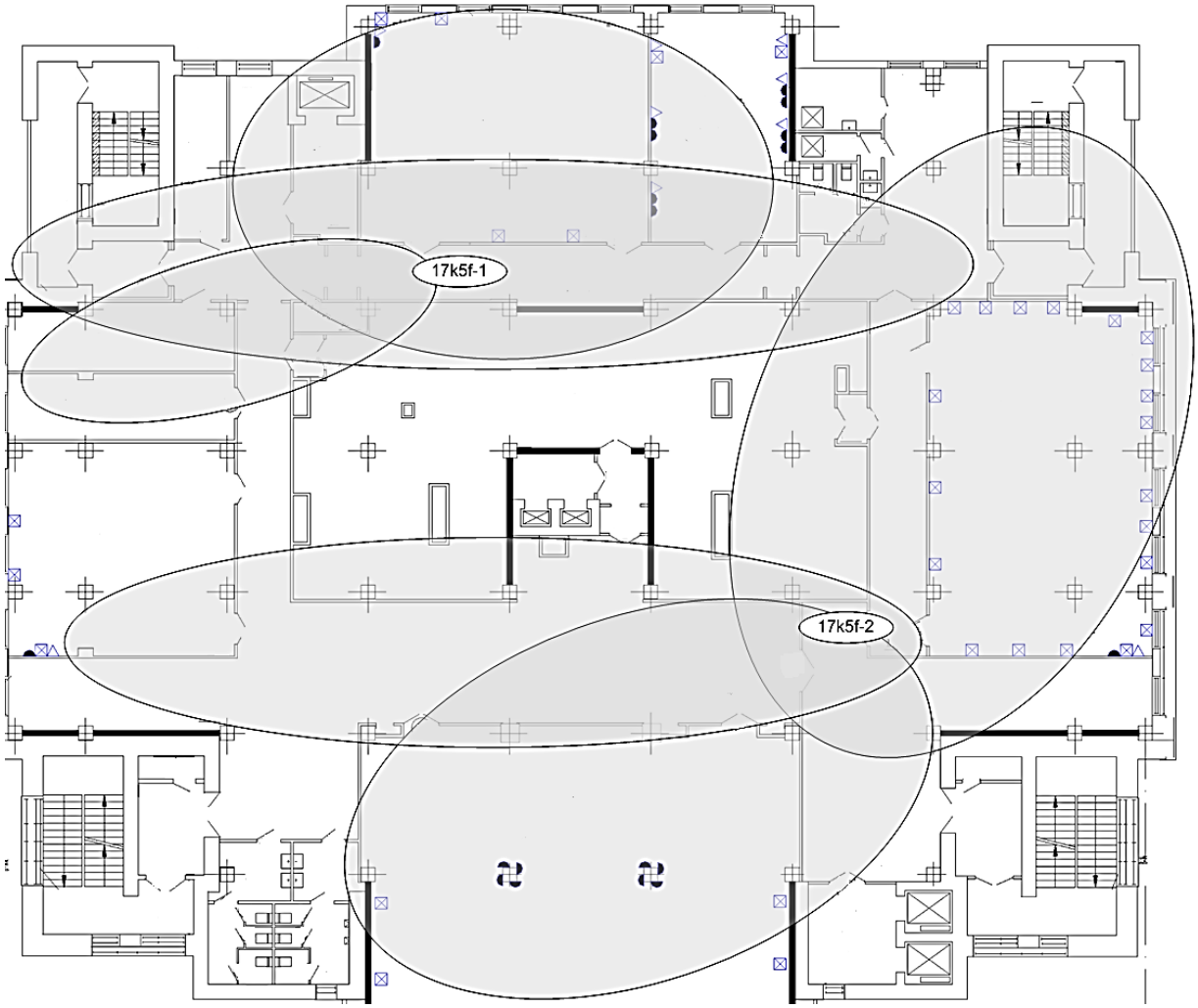

Рисунок 3 – Пересечение зон покрытия

Не всегда требуется стопроцентное покрытие сетью, это можно использовать для экономии точек доступа. Затем необходимо на месте установить точку доступа со схожими характеристиками и антеннами и проверить по факту зоны покрытия, при этом нужно учитывать, что мощность сигнала уменьшается пропорционально квадрату расстояния. Поэтому при составлении карты рисуют линии границы

сигнала с одинаковым уровнем (по принципу топографических карт) в соответствии с рисунком 4.

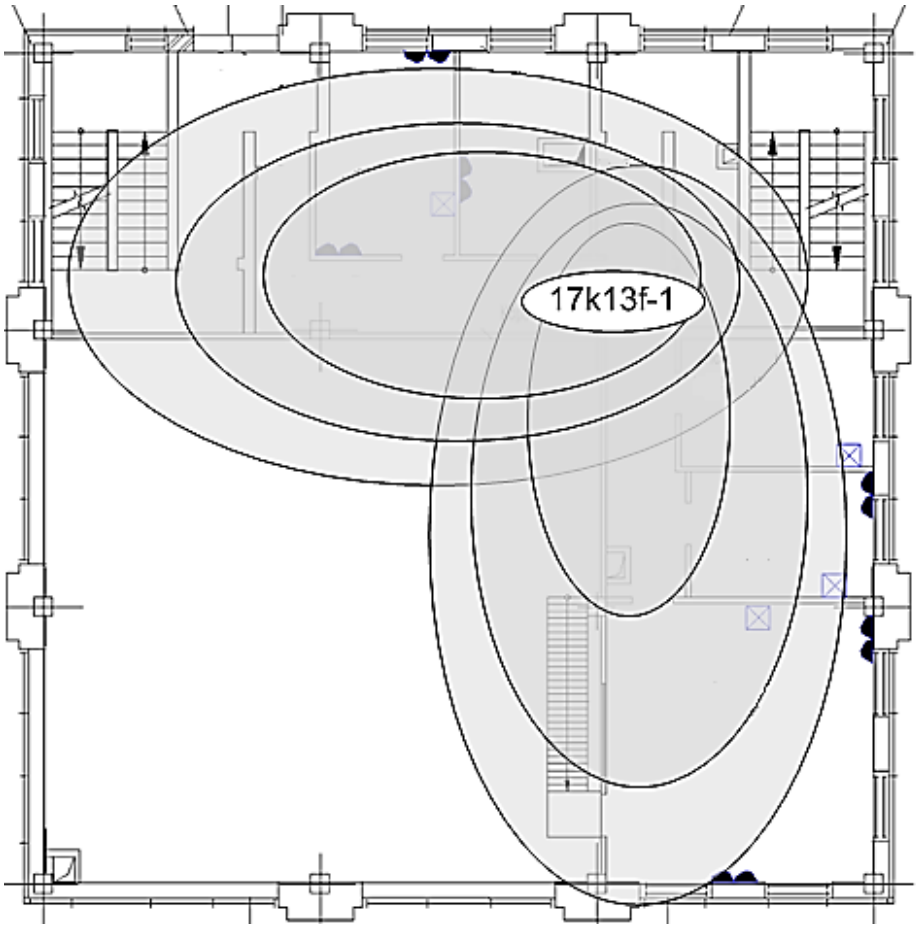

Рисунок 4 – Зоны разных уровней сигнала

При этом необходимо проверить уровень сигнала на этаж выше и ниже, чтобы предотвратить пересечение каналов. Если сигнал проходит на другой этаж, на карте его отображают пунктиром, как показано на рисунке 5.

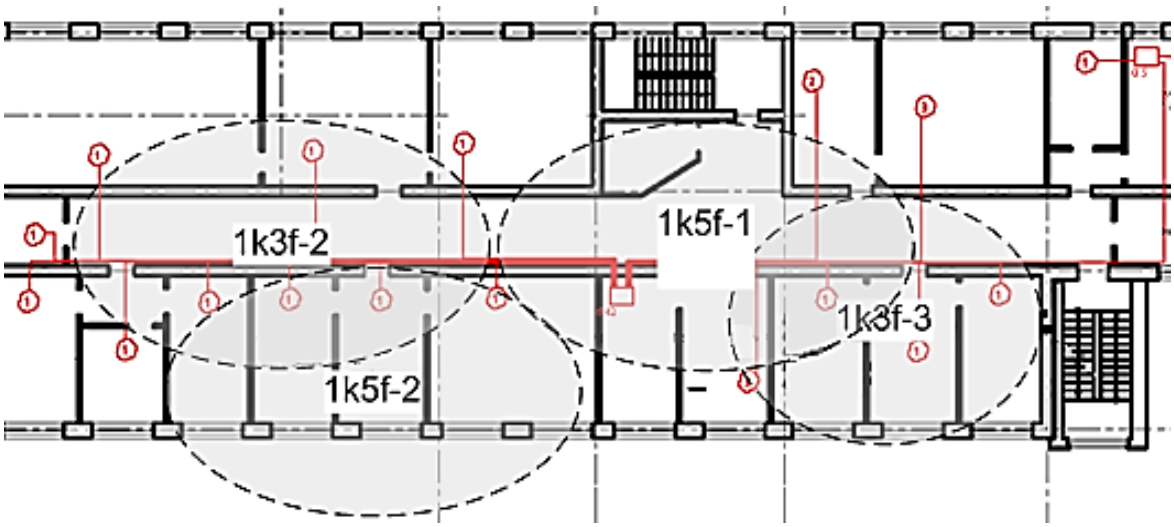

Рисунок 5 – Действие точек доступа на другие этажи

В результате, после проверки всех возможных мест установки точек доступа создается рабочий проект установки оборудования.

2.2 Задание на лабораторную работу

Необходимо спроектировать зоны покрытия беспроводной сети, для этого нужно воспользоваться картой помещений минимум трех этажей одного из учебных корпусов ОГУ или любой другой организации.

3 Лабораторная работа №2 – Проектирование обеспечивающей инфраструктуры

3.1 Теоретические сведения

3.1.1 Выбор аппаратного обеспечения

Рассмотрим оборудование для организации корпоративных беспроводных сетей с центральным управлением. Таблица 1 показывает основные доступные на Российском рынке производители подобных решений.

Таблица 1 – Возможности решений по беспроводному доступу

Характеристика	Juniper WLC800R	D-Link DWC-1000	Cisco 5508	HP MSM720
1	2	3	4	5
Максимальное количество подключаемых точек доступа	128	24	500	200
Протоколы шифрования беспроводных каналов	Определяются точками доступа, WPA/WPA2	WEP, Dynamic WEP, WPA/WPA2	Определяются точками доступа	Определяются точками доступа
Протоколы безопасной аутентификации	IEEE 802.11i, WRAP CCMP	IEEE 802.11i, WRAP, CCMP	IEEE 802.11i, WRAP, CCMP	IEEE 802.11i, WRAP, CCMP
Функционал по анализу радиочастотного спектра	Да, с возможностью управлением количеством точек с таким функционалом с помощью лицензий	Нет	Да	Нет
Функции сбора данных спектрального анализа	Да, в качестве специализированного спектрального датчика или вместе с обеспечением клиентского доступа.	Нет	Да	Нет

Продолжение таблицы 1

1	2	3	4	5
Возможность обнаружения источника помех и его локализации	Да	Нет	Да	Нет
Возможности внешнего управления контроллером	С помощью отдельно приобретаемого программного обеспечения	Нет	С помощью отдельно приобретаемого программного обеспечения	С помощью отдельно приобретаемого программного обеспечения
Возможность автономной работы удаленных точек доступа при потере связи	Да, 10 дней	Нет	Нет	Нет
Обеспечение бесшовного роуминга между точек	Да	Да	Да	Да
Возможность обмена трафиком без участия контроллера	Да	Нет	Да	Нет
Автоматическая настройка мощности точек доступа	Да	Нет	Да	Да
Балансировка нагрузки на точки от беспроводных клиентов	Да	Да	Да	Да
Автоматическая настройка частоты точек доступа	Да	Нет	Да	Да
Поддержка QoS беспроводных сетей	Да	Нет	Да	Да
Поддержка QoS проводных сетей	Да, настройка приоритетов и групп QoS	Да, настройка приоритетов и групп QoS	Да, настройка приоритетов и групп QoS	Да, настройка приоритетов и групп QoS
Принципиальная возможность работы с беспроводной IP телефонией	Да, с поддержкой определения SIP трафика	Да	Да	Да
Возможность разработки собственных приложений для платформы контроллера	Да	Нет	Нет	Нет

Продолжение таблицы 1

1	2	3	4	5
Наличие инструментария разработчика (SDK) для создания приложений под платформу контроллера	Да	Нет	Нет	Нет
Наличие документированных способов программного взаимодействия с контроллером и с программным обеспечением управления контроллером (API)	Да	Нет	Нет	Нет
Возможность организации доступа в Internet с аутентификацией через ПО или браузер (hotspot)	Да	Да	Да	Да
Поддержка протокола управления CAPWAP	Да	Нет	Да	Нет

Как показано в таблице, основные характеристики и функциональность предлагаемых решений практически одинаковы, однако решение Juniper позволяет разрабатывать свое собственное ПО с открытым исходным кодом и предоставляет документацию по программированию интерфейса взаимодействия. В связи с этим дальше будет представлены методические материалы по использованию оборудования Juniper. Схема подключения показана на рисунке 6.

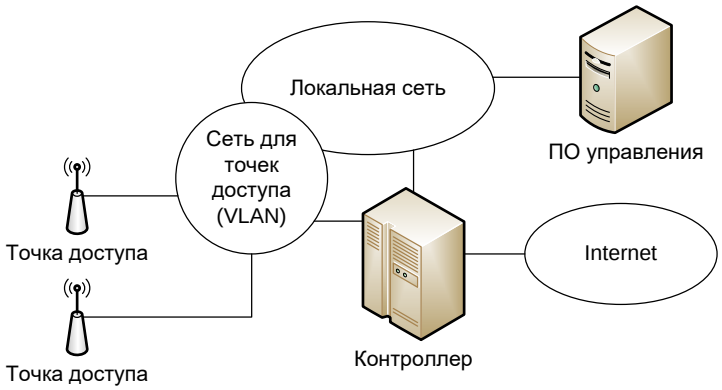

Рисунок 6 – Схема подключения

3.1.2 Проектирование проводной сети

Проводной сегмент сети имеет очень важную роль в проектировании беспроводной сети. Он предоставляет как электропитание, так и доступ к контроллеру. В общем проект проводного сегмента зависит от мест установки точек доступа, существующей кабельной инфраструктуры, коммуникационных шкафов. При недостаточном количестве шкафов или при их значительной удаленности необходимо добавить в проект еще шкафы, запланировать проводку для электропитания шкафа, его вентиляцию и внутреннее оборудование.

Для подключения 1 точки доступа необходим один из двух вариантов:

а) существующий порт в существующем коммутаторе с поддержкой PoE;

б) новый модуль в существующем коммутаторе с поддержкой PoE;

в) новый коммутатор с поддержкой PoE;

г) существующий коммутатор без поддержки PoE и PoE-инжектор с внешним блоком питания;

д) существующий коммутатор без поддержки PoE и PoE патч-панель с внешним блоком питания.

3.1.3 Проектирование электропитания PoE

Технология Power over Ethernet (PoE) – это механизм подачи питания сетевым устройствам по кабелю Ethernet, передающему сетевой трафик. Как правило, точки доступа потребляют до 14 Вт на устройство, однако некоторые точки доступа требуют большего питания и поэтому имеют два порта Ethernet с PoE или один с поддержкой PoE+ (IEEE 802.3at High PoE). Это необходимо учитывать при подсчете необходимого количества портов.

Требование по мощности всего оборудования, которое будет подключено к коммутатору, должно быть рассчитано таким образом, чтобы общая активная мощность была меньше, чем энергетический потенциал PoE коммутатора. Классы потребления показаны в таблице 2.

Таблица 2 – Классы энергопотребления PoE

Класс	Максимальная мощность на выходе коммутатора	Максимальный уровень мощности у питаемого устройства
1	2	3
0	15,4 Вт	0,44 - 12,95 Вт
1	4,0 Вт	0,44 - 3,84 Вт
2	7,0 Вт	3,84 - 6,49 Вт
3	15,4 Вт	6,49 - 12,95 Вт
4	30 Вт	12,95 - 25,5 Вт

Например, коммутатор с 48 портами и поддержкой максимальной PoE мощности 316 Вт может обслужить только 20 точек доступа нулевого класса. Поэтому при подборе оборудования необходимо рассчитывать необходимую мощность коммутатора.

При расчете источника бесперебойного питания (ИБП) надо руководствоваться требованиями по длительности работы на максимальном уровне потребления. ИБП должен быть линейно-интерактивного типа, мощность должна превышать уровень потребления минимум в два раза, ИБП должен быть загружен не более чем на 80%. Емкость аккумулятора должна рассчитываться как суммарная емкость аккумуляторной батареи UPS. Производители ИБП рекомендуют использовать формулу (Б.1) для расчета емкости

$$T\ [час] = C\ [А*час] * V\ [В] * \eta / P\ [Вт],$$

$$C = \frac{T * P}{V * \mu}$$

, (1)

где C – емкость батарей в VA;

T – требуемое время работы, в часах;

P – мощность нагрузки, Вт;

V – напряжение аккумулятора, В;

μ – КПД, примем за 0.85.

Например, при подключении нагрузки в 316 Вт к ИБП 1000 ВА и двумя батареями по 12 Ач время работы будет составлять 46 минут. А для подключения нагрузки в 1000 Вт для ИБП в 2000 ВА и автономной работы не менее 30 минут понадобиться аккумуляторы суммарной емкостью 40 Ач или не менее четырех стандартных 12 Ач батарей. Это надо учитывать при проектирования места в шкафу, так как дополнительные батареи, как правило, помещают в отдельный корпус, который занимает не менее 1U места в стойке.

3.1.4 Пассивные элементы сети

Каждый активный элемент должен находиться в специальном телекоммуникационном шкафу или комнате. При возможности, необходимо для окончания кабеля от точек доступа использовать патч-панель и патч-корды для присоединения к коммутатору. Если коммутатор без поддержки PoE, необходимо предусмотреть крепление PoE инжекторов или использовать PoE патч-панель. Кроме этого, по правилам кабельной разводки необходимо использовать горизонтальный кабель-органайзер в расчете 2 штуки на 1 коммутатор или патч-панель и вертикальные кольца для кабельной организации. Для патч-панели необходимо использовать кабельную полку при количестве портов более 16.

Каждый шкаф должен быть с принудительной вентиляцией, так как PoE оборудование потребляет значительную мощность. Вентиляторы для шкафов обычно имеют крепление для стойки и рассчитываются как 1 вентилятор на 1 коммутатор или 16 PoE инжектором.

При расчете количества портов необходимо заложить запас не менее 20%, как и для кабеля. Длина патч-кордов должна быть достаточна для пользования

кабельными органайзерами. Остальные этапы проектирования проводной ети подробно описаны в многочисленных руководствах и в стандарте EIA/TIA-568B-2.

3.2 Задание на лабораторную работу

Для беспроводной сети из лабораторной работы №1 в соответствии с рекомендациями выбрать аппаратное обеспечение, спроектировать проводную сеть, обеспечить питание по PoE, а также определить пассивные элементы сети.

4 Лабораторная работа №3 – Настройка контроллера точек доступа

4.1 Теоретические сведения

4.1.1 Базовая настройка контроллера

После установки контроллера необходимо на компьютер технического персонала установить программное обеспечение RingMaster для графического управления. После запуска ПО появится главное окно программы, разделенное на функциональные элементы (см. рисунки 7 и 8).

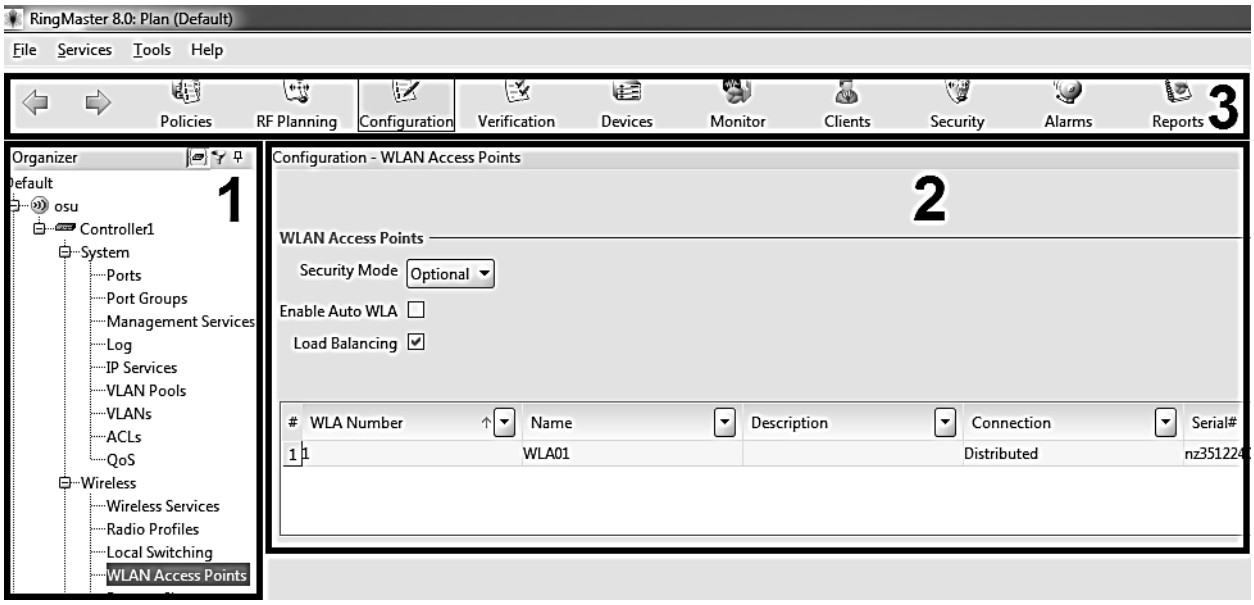

Рисунок 7 – Фрагмент основного окна программы

Поле 1 рисунка 7 – «Панель органайзера» - содержит основные элементы управления, такие как список контроллеров, разделов настройки. Поле 2 рисунка 7 – «Основная панель» - служит для внесения изменений и просмотра информации. Поле 3 рисунка 7 – «Панель навигации» - содержит категории информации, доступной при выборе конкретного элемента панели. Например, вкладка «Configuration» позволяет изменять настройки устройств и ПО.

Поле 4 рисунка 8 – «Панель задач» - содержит полный список задач в соответствии с выбранным пунктом из панели органайзера. Поле 5 рисунка 8 – «Строка состояния» - отображает статус контроллера и журналов.

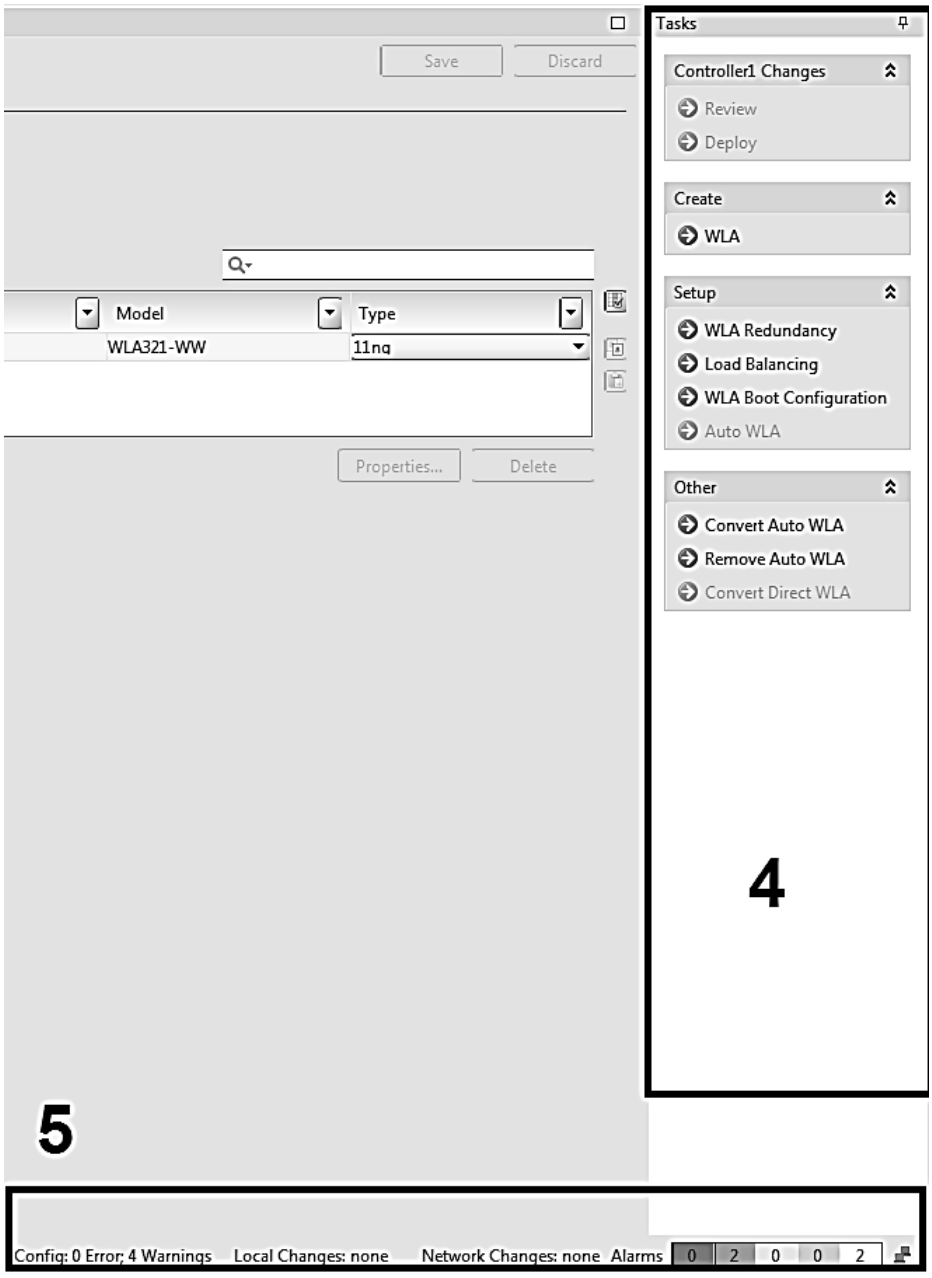

Рисунок 8 – Фрагмент основного окна программы

Основные задачи, решаемые с помощью данного ПО следующие:

а) обмен информацией с контроллером;

б) централизованная настройка точек доступа;

в) настройка разнообразных беспроводных услуг;

г) планирование радиочастотного размещения точек доступа;

д) настройка аутентификации и мониторинга.

Первоначально необходимо настроить соединение с контроллером. Для этого, на вкладке «Configuration» при выборе параметра «Default» в панели органайзера доступна задача «Create WLAN Controller» в соответствии с рисунком 9, запускающая мастер добавления контроллера в программу.

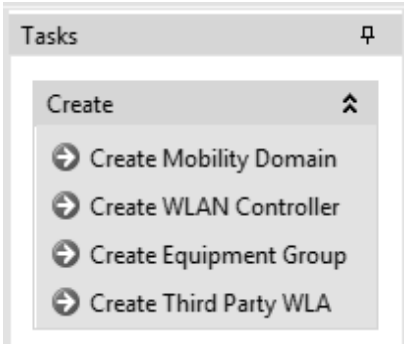

Рисунок 9 – Основные задачи домена

Мастер настройки запросит параметры сети контроллера, пароль, тип контроллера и отображаемое имя (см. рисунки 10 и 11).

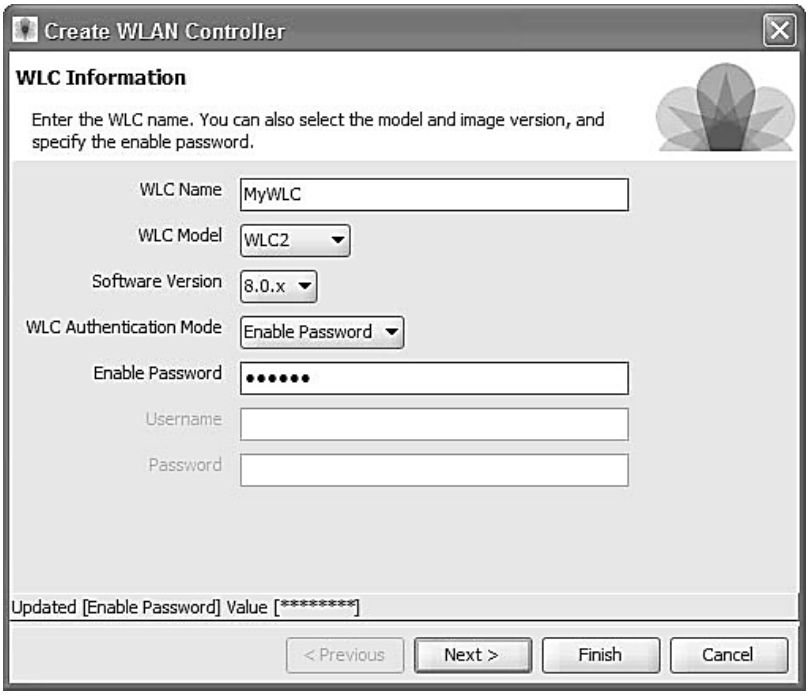

Рисунок 10 – Создание контроллера WLAN

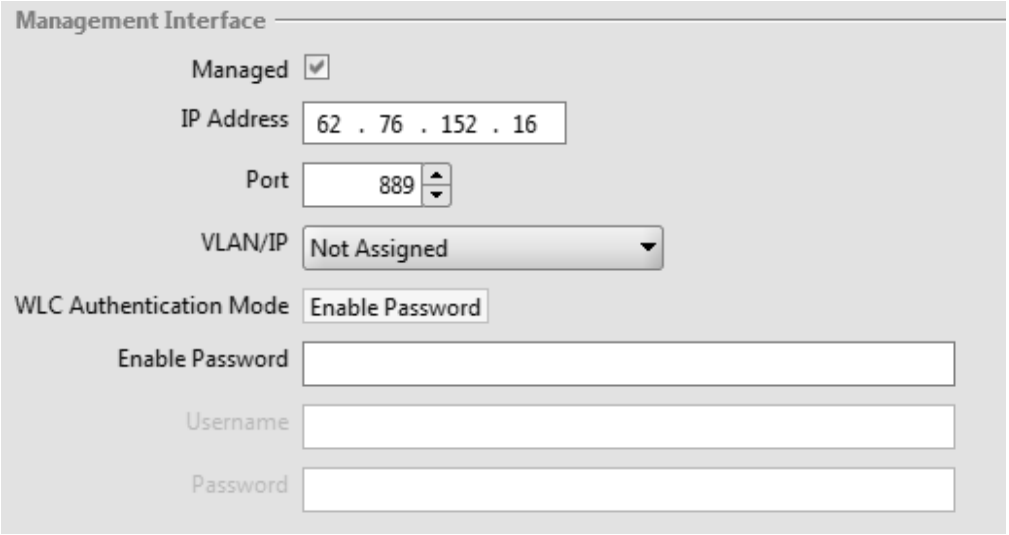

Рисунок 11 – Настройка адреса контроллера

Для массовой настройки точек только в пределах какого-либо набора точек (домена) необходимо создать домен типа «Mobility Domain». Несколько доменов создают для раздельной конфигурации нескольких областей сети. Домен создается в том же порядке, что и контроллер сети. На панели задач необходимо выбрать поле «Create Mobility Domain», в открывшемся мастере необходимо задать имя и контроллеры нового домена.

Для подключения точек доступа проще всего использовать специальный инструмент «Auto WLA», позволяющий всем точкам доступа Juniper автоматически добавляться в контроллер, применяя заранее заданные настройки. Для включения автоматического добавления необходимо выбрать на панели органайзера нужный контроллер, в раскрывшемся списке выбрать «Wireless», далее выбрать «WLA Access Point». На основной панели необходимо активировать переключатель «Enable AutoWLA», как показано на рисунке 12 (поле 1).

На панели задач также располагается область с задачами для этой функции – удалить автоматически добавленные точки или преобразовать в статические, как показано на рисунке 13.

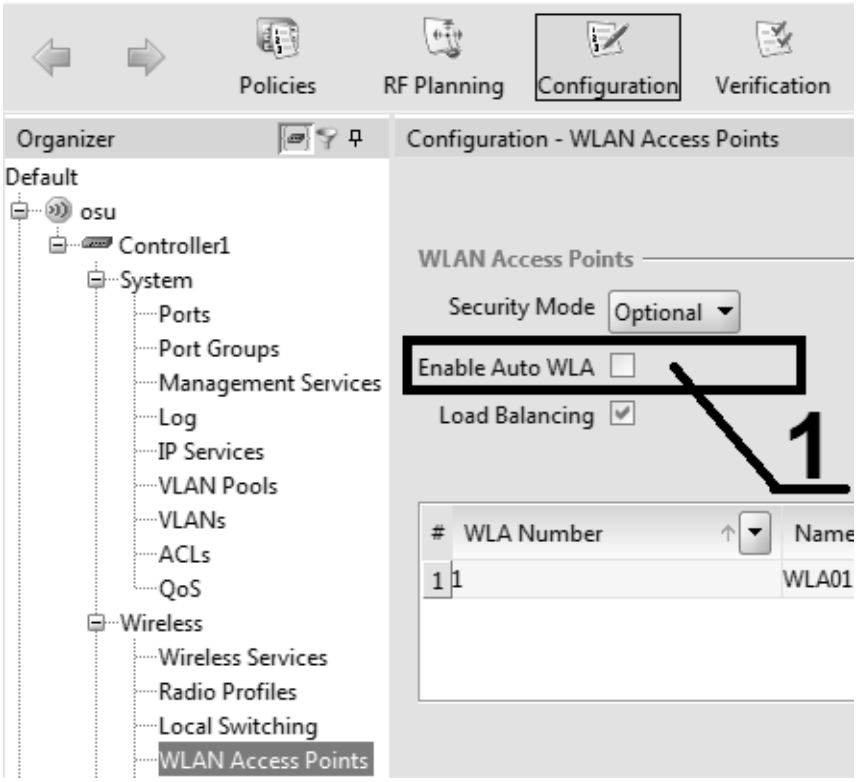

Рисунок 12 – Подключение точек доступа

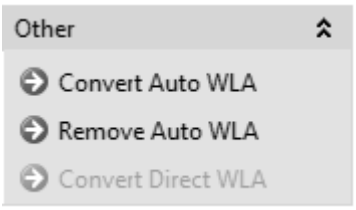

Рисунок 13 – Задачи для функции Auto WLA

Также на этой вкладке можно увидеть список точек доступа, уже добавленных в систему (см. рисунок 14).

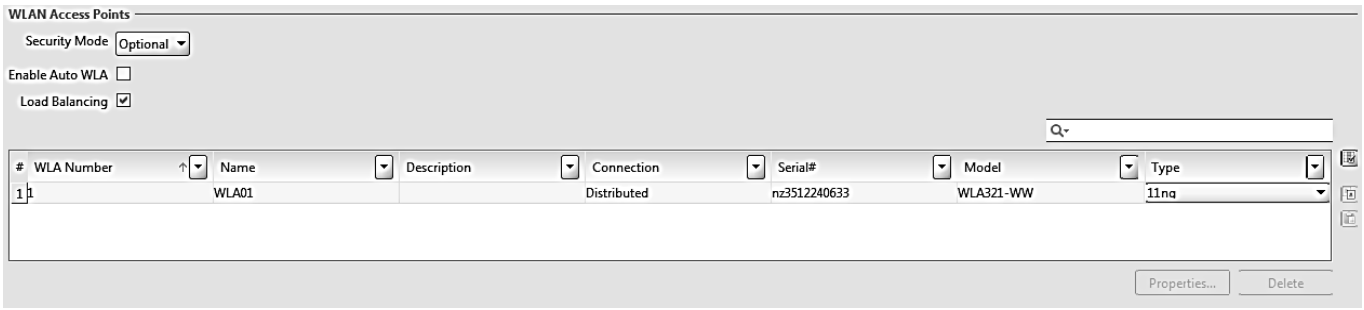

Рисунок 14 – Список добавленных в систему точек доступа

На рисунке 15 показано, как при необходимости можно добавить точку доступа вручную (поле 1), настроить балансировку нагрузки (поле 2), задать вручную сетевые параметры для точки доступа (поле 3) и настроить параметры типового профиля для «Auto WLA» (поле 4).

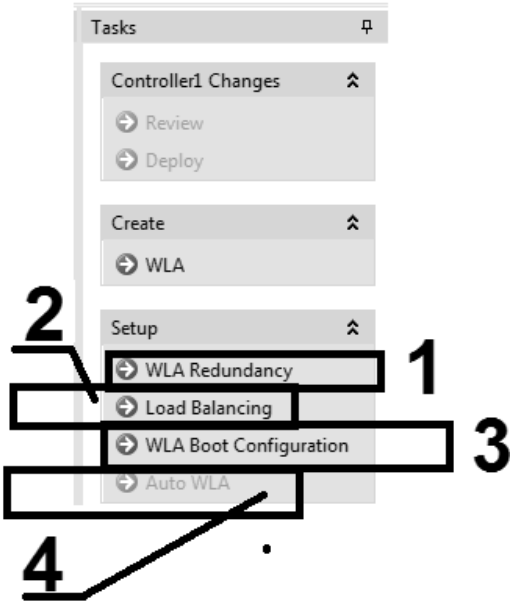

Рисунок 15 – Ручная настройка точек доступа

Настройка балансировки при необходимости заключается в выборе режима и диапазона, как показано на рисунке 16. Режим «Low» означает отсутствие запрета на подключения клиентов к перегруженным точкам, в режиме «Medium» клиенты перенаправляются на ближайшие точки доступа в течение нескольких секунд после попытки подключения. Остальные режимы увеличивают задержку при первоначальном подключении до одной минуты и более для лучшего распределения клиентов.

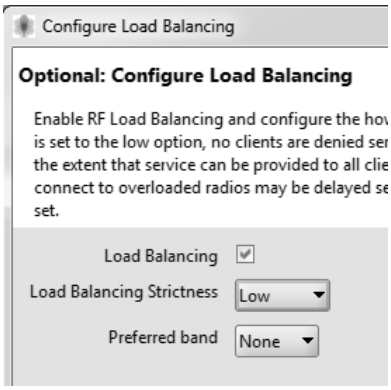

Рисунок 16 – Настройка балансировки

Для каждого SSID балансировка может настраиваться отдельно, как показано на рисунке 17.

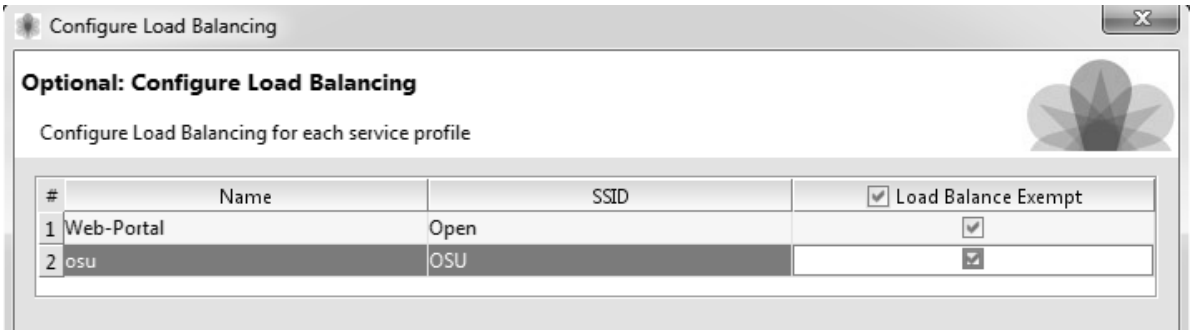

Рисунок 17 – Балансировка для конкретного SSID

После добавления точек доступа каждую точку можно настраивать отдельно или через профиль «Radio Profile», как показано на рисунке 18. Настройки могут быть подвергнуты множество параметров, таких как:

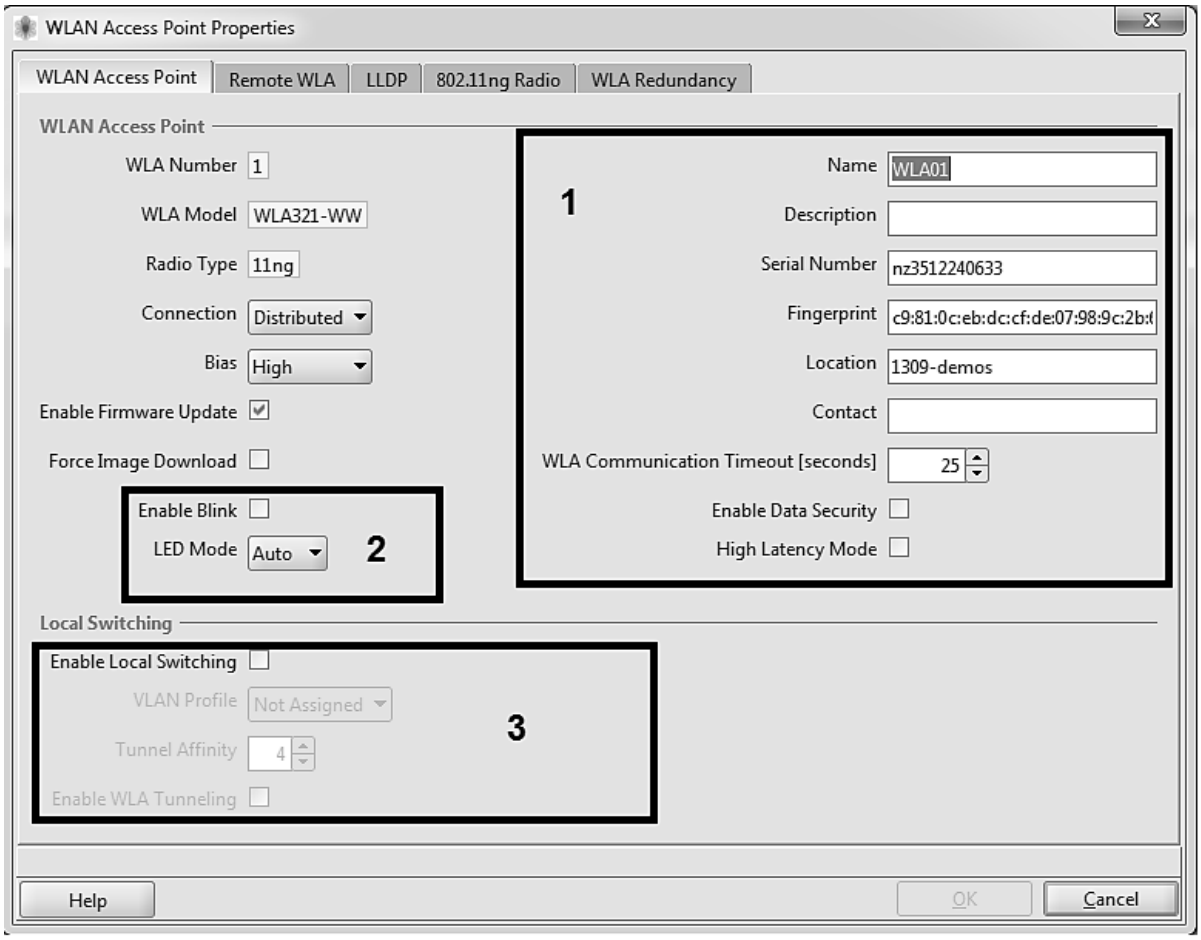

Рисунок 18 – Настройка конкретной точки доступа

а) поле 1 – имя, ключ безопасности, серийный номер, сведения о местоположении;

б) поле 2 – параметры светодиодных индикаторов;

в) поле 3 – коммутация без использования контроллера;

г) ассоциированные профили типовых настроек для радиопередатчиков, настройка сетевых параметров, параметров избыточности.

Основное, что необходимо настроить для беспроводной сети – это сервис ESS. Для настройки необходимо в панели органайзера выбрать нужный контроллер, затем выбрать «Wireless», потом «Wireless Service». На основной панели будет отображен список сетей (см. рисунок 19).

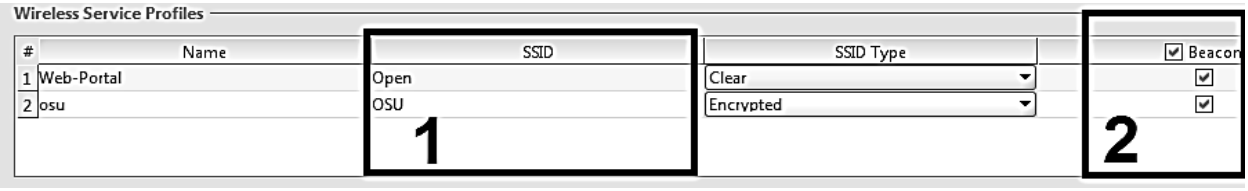

Рисунок 19 – Список сетей на основной панели

В поле 1 показано видимое имя сети, в поле 2 – видимость имени сети. В свойствах сети можно настроить довольно большое количество параметров, начиная с имени сети и видимости для клиентов, заканчивая параметрами безопасности и маршрутизации. Каждый SSID может быть ассоциирован со своей сетью, диапазоном, способом авторизации, профилем QoS, как показано на рисунке 20.

При необходимости создать новую сеть надо воспользоваться соответствующими задачами на панели задач, как показано на рисунке 21 (поле 2). Каждый пункт открывает мастер, адаптированный для конкретного типа сети. Корпоративные сети, как правило, создают с 802.1x авторизацией, публичные сети или гостевые – с «Open» или «Web-portal» авторизацией.

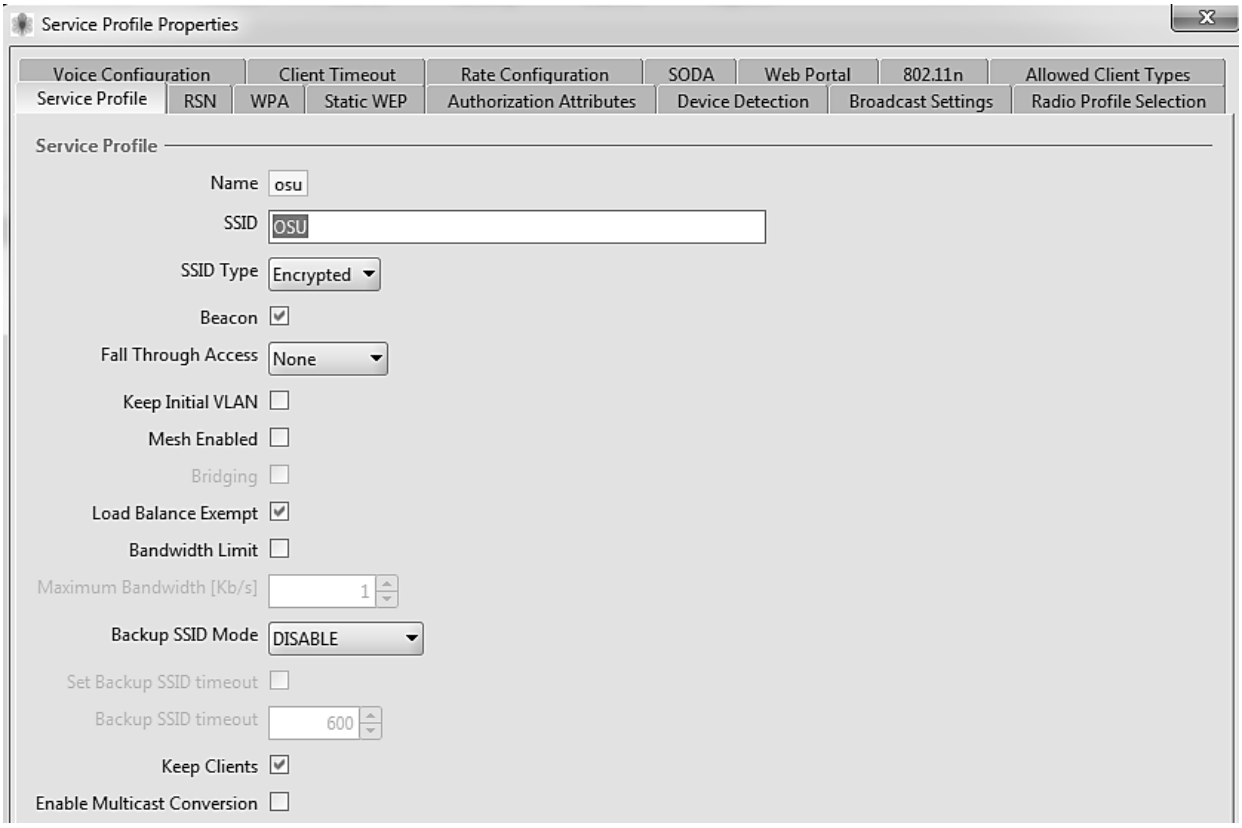

Рисунок 20 – Параметры конкретного SSID

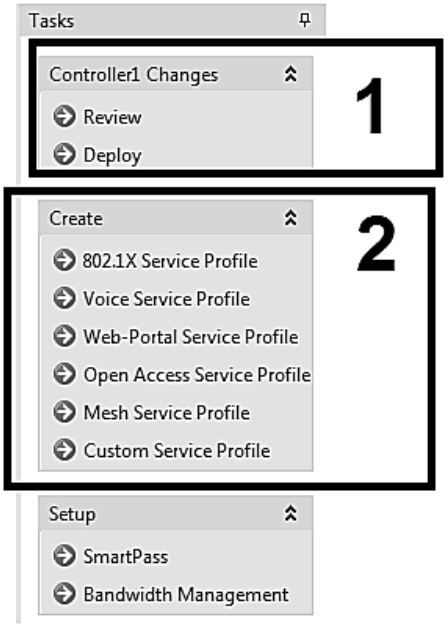

Рисунок 21 – Создание новой сети

После любого изменения параметров необходимо сообщить контроллеру об изменениях при помощи задачи «Deploy» (поле 1).

4.1.2 Настройка взаимодействия с точками доступа

Контроллер Juniper может управлять произвольными точками доступа с поддержкой протокола CAPWAP и SNMP. Для этого в поле органайзера существует раздел «Third-Party WLAs», куда можно добавить точку доступа аналогично другим точкам доступа.

4.1.3 Настройка контроллера OpenFlow

Для настройки взаимодействия агентов OpenFlow необходимо сначала установить и скомпилировать контроллер. Затем необходимо обеспечить связность на уровне IP агентов с контроллером OpenFlow в соответствии с рисунком 22.

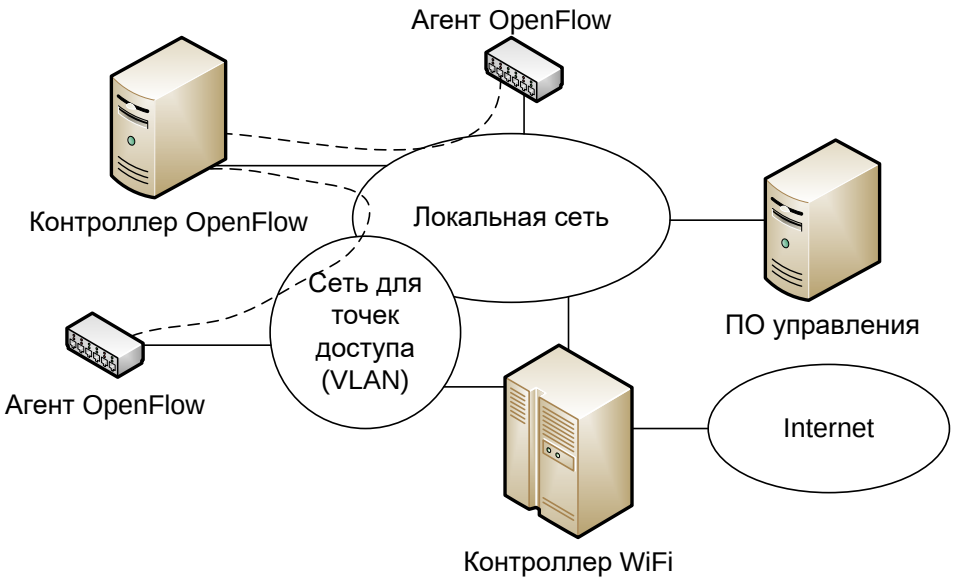

Рисунок 22 – Схема взаимодействия контроллеров

Контроллер OpenFlow должен содержать настройки для взаимодействия с контроллером WiFi. Поскольку контроллер Junier может использовать для управления протокол HTTP, приложения контроллера для управления беспроводной инфраструктурой будут пользоваться Web запросами. Например, для получения списка точек доступа будет использован запрос «https://127.0.0.1/webservice/rm-agent/v1/monitor/devices?scope=all».

4.1.4 Настройка взаимодействия точек доступа с контроллером OpenFlow

«Модуль виртуальной точки доступа» взаимодействует непосредственно с «Модуль расширения сетевой операционной системы». При каждом запуске «модуль виртуальной точки доступа» получает от контроллера сведения о топологии, виртуальных точках и клиентах, ассоциированных с ними.

При получении команды о добавлении новой виртуальной точки доступа контроллер взаимодействует с драйвером беспроводной карты через механизм debugfs, передавая новую маску списка bssid для вещания.

Первоначальная установка заключается в копировании файла в файловую систему точки доступа по адресу /bin. После этого необходимо создать файл с настройками для конкретной точки доступа, записать в файл MAC адреса точки и адрес контроллера по адресу /etc/config/virtap. После этого необходимо создать скрипт для запуска следующего содержания для точки на базе чипсетов Atheros:

```
vi /etc/init.d/virtap.sh
#!/bin/sh
wlanconfig ath1 destroy
wlanconfig  ath1 create wlandev wifi0 wlanmode monitor
/bin/virtap  /etc/config/virtap &
```

Если установлен другой чипсет или другой драйвер и нет утилиты wlanconfig, необходимо использовать следующий скрипт:

```
vi /etc/init.d/virtap.sh
#!/bin/sh
iw dev phy0 del
iw dev phy0 interface add wifi0 type monitor
/bin/virtap  /etc/config/virtap &
```

4.2 Задание на лабораторную работу

Для беспроводной сети из лабораторной работы №2 в соответствии с теоретическими сведениями из раздела 4.1 выполнить настройку беспроводного контроллера, при необходимости дополнительно установите контроллер OpenFlow NOX [6] и выполните настройку точек доступа.

5 Лабораторная работа №4 – Тестирование беспроводной сети

5.1 Теоретические сведения

Для тестирования необходимо использовать пакет aircrack-ng и сниффер Wireshark [7-10] для перехвата пакетов. Также необходимо иметь беспроводные сетевые карты на чипсете Atheros с неразборчивым режимом.

Основной методологией тестирования является использование сниффера (физически в пределах радиочастотного спектра клиентов в любое время), чтобы захватить все связанные с клиентом пакеты для анализа.

Во время передачи управления, точки доступа и мобильная станция обмениваются набором управляющих кадров, таких как Probe, кадры аутентификации и ассоциации, ключи. При сниффинге всех кадров из радиочастотной среды. Перед началом эксперимента необходимо активировать режим монитора сетевых карт. Для этого

а) выполнить команду «iw phy list» для вывода реальных имен физических устройств сетевых карт (имена вида phy0, phy1);

б) выполнить для каждого устройства команду «iw phy phyN interface add wlan type monitor», где N – номер устройства.

в) выполнить команду «iwconfig» для отображения имен созданных интерфейсов (вида wlan0, wlan1);

г) запустить мониторинг каждого устройства командой «airmon-ng start wlanN C», где N – номер интерфейса, C – номер канала для мониторинга (1, 6 или 12). Каждый интерфейс должен быть на своем канале;

д) командой «airomon-ng» вывести имена новых интерфейсов мониторинга (вида mon0,mon1);

е) запустить сбор пакетов командой «tshark -i monN –n –w experiment_monN.dump», где N – номер интерфейса. Необходимо запустить по 1 копии программы на каждую сетевую карту.

ж) на беспроводном клиенте присоединиться к требуемой беспроводной сети

и запустить команду «hping3 -1 --faster 192.168.1.1 > experiment_wifi.dump»

и) начать движение по заранее выбранному маршруту с заданной скоростью;

к) после окончания траектории необходимо остановить сбор пакетов и посылку ICMP сообщений командой Ctrl-C;

л) затем необходимо объединить результаты в один файл командой «mergecap –w result.dump experiment_mon1.dump experiment_mon2.dump experiment_mon3.dump»

В результате получается файл с исходными данными для анализа. Теперь необходимо провести анализ в программе wireshark. Для этого , после запуска программы нужно открыть файл «result.dump» и ввести в поле «filter» строку

«(wlan.addr=адрес1 || wan.addr=адрес2 || wan.addr=адрес3 || wan.addr=адрес4)»,

где «адрес2», «адрес3», «адрес4» – адреса точек доступа (при большем количестве нужно писать все адреса), «адрес1» - адрес беспроводной карты клиента, как например в соответствии с рисунком 23. В поле 1 показан пакет для начала анализа роуминга (Probe request после деаутентификации).

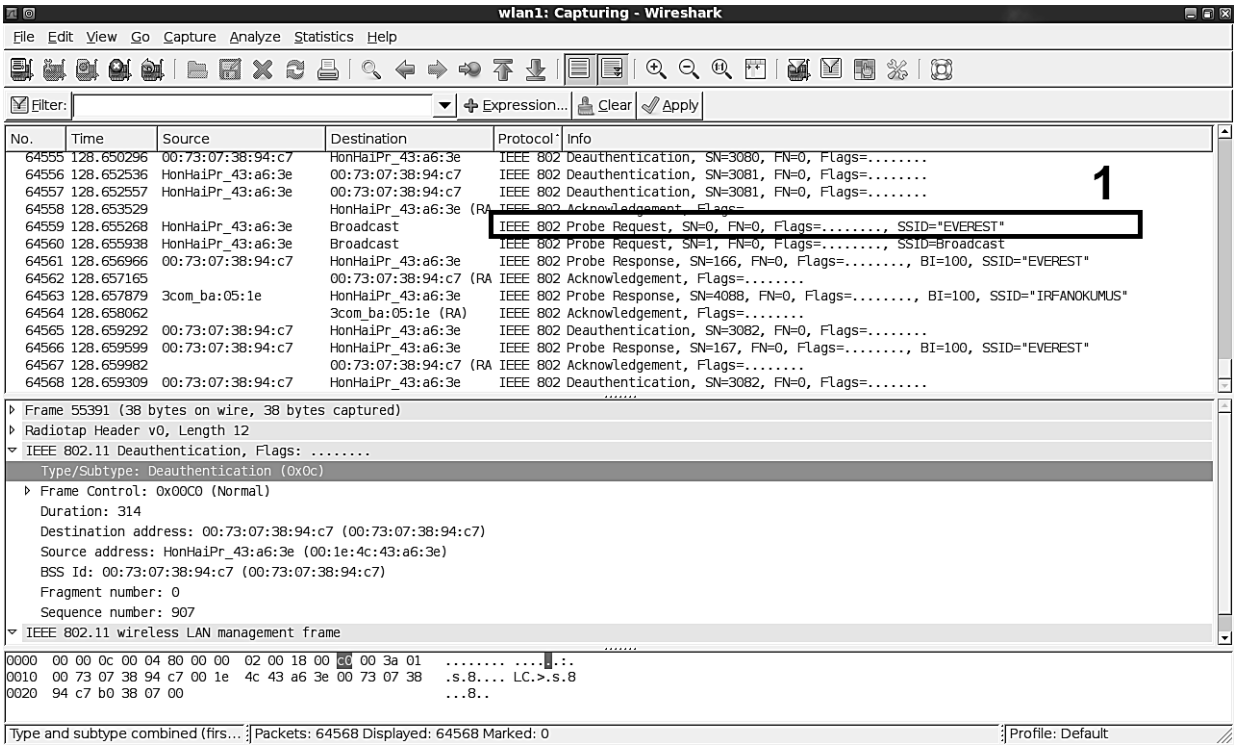

Рисунок 23 – Перехват трафика

При проведении теста на время роуминга мобильная станция должна перемещаться по зданию по фиксированному пути. После захвата трафика и включение фильтра в Wireshark выводится таблица с перехваченными пакетами. Для расчета времени переключения на другую точку доступа необходимо искать в списке пакетов первый из серии «Probe Request», выделить его и нажать Ctrl-T. Затем искать пакет «Reassociation Response», время во второй колонке будет временем переключения. При использовании аутентификации необходимо искать пакет «EAPOL key (msg 4/4)», после которого аутентификация считается успешной, и записывать время этого пакета.

На рисунке 24 показан результат измерения времени переключения на другую точку доступа при установке точки отсчета времени на пакете «Probe request».

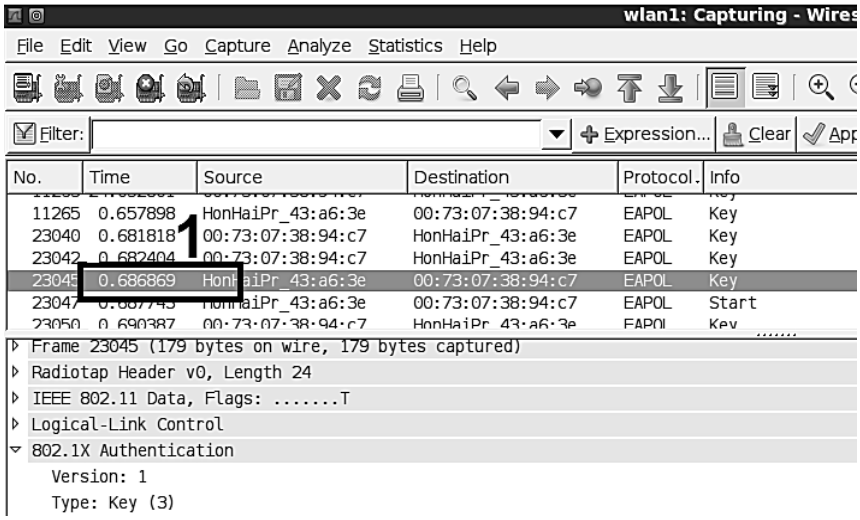

Рисунок 24 – Перехвата трафика

Результат указан в секундах, однако 0,68 означает 68 мс. После этого нужно искать следующую запись «Probe Request» и повторять все заново.

5.2 Задание на лабораторную работу

Для беспроводной сети из лабораторной работы №3 выполнить тестирование в соответствии с описанной в 5.1 методикой.

Список использованных источников

1 Базовые положения стандарта IEEE 802.11n для сетей Wi-Fi [Электронный ресурс] // ZyXEL– Электрон. дан. – 2015. Режим доступа: http://zyxel.ua/kb/2105. – Загл. с экрана. – (Дата обращения: 10.01.2015).

2 OpenFlow 1.0 Released . [Электронный ресурс] // OpenFlow. – Электрон. дан. – 2011. Режим доступа: http://www.openflow.org/wp/2009/12/openflow-1-0-released. – Загл. с экрана. – (Дата обращения: 10.04.2013).

3 OpenFlow in Europe: Linking Infrastructure and Applications [Электронный ресурс] // Ofelia. – Электрон. дан. – 2011. Режим доступа: http://www.fp7-ofelia.eu/about-ofelia. – Загл. с экрана. – (Дата обращения: 20.04.2013)

4 Контроллер NOX, Beacon. Обзорный курс [Электронный ресурс] / Сайт Центра прикладных исследований компьютерных сетей. — Электрон. дан. – 2013. – Режим доступа: http://sdto.arccn.ru/portal/major/index.jf. – Загл. с экрана. – (Дата обращения: 01.04.2013)

5 McKeown, N. OpenFlow: Enabling Innovation in Campus Networks / N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, J. Turner // ACM SIGCOMM Computer Communication Review. — New York, 2008. – т. 38, №2. – с. 69-74.

6 About NOX [Электронный ресурс] // Сайт NoxRepo.org. – Режим доступа: http://www.noxrepo.org/nox/about-nox/. – Загл. с экрана. – (Дата обращения: 22.04.2013)

7 WireShark Docs [Электронный ресурс] // Сайт Wireshark Foundation. – Электрон. дан. – 2015. – Режим доступа: https://www.wireshark.org/docs/. – Загл. с экрана. – (Дата обращения: 01.01.2015)

8 Murty, R. Designing high performance enterprise Wi-Fi networks / R. Murty, J. Padhye, R. Chandra, A. Wolman, B. Zill // In Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation, NSDI'08. – 2008. – C. 73-88.

9 Bahl, P. Enhancing the security of corporate Wi-Fi networks using DAIR / Paramvir Bahl, Ranveer Chandra, Jitendra Padhye, Lenin Ravindranath, Manpreet Singh,

Alec Wolman, and Brian Zill // In Proceedings of the 4th international conference on Mobile systems, applications and services, MobiSys ’06. – 2006. – С. 1-14.

10 Bejerano, Y. Cell breathing techniques for load balancing in wireless LANs [Текст] / Y. Bejerano, S.-J. Han // IEEE Transactions on Mobile Computing. – 2009. – № 8(6). – С. 735-749.