МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра космического приборостроения и систем связи

УТВЕРЖДАЮ
Проректор по учебной работе

_____О.Г. Локтионова
«14» 02 2018 г.

Подготовка комплекта типовых документов для предпроектных работ

Методические указания
по выполнению лабораторной работы №5
по курсу «Проектирование систем и сетей радиодоступа»
для студентов направления подготовки 11.04.02

Курск 2018

УДК 621.3.095

Составитель А.Е.Севрюков

Рецензент
Доктор технических наук, профессор *В.Г. Андронов*

Подготовка комплекта типовых документов для предпроектных работ: методические указания по выполнению лабораторной работы по курсу «Проектирование систем и сетей радиодоступа» / Юго-Зап. гос. ун-т; сост. А.Е.Севрюков. Курск, 2017. 18 с.

Содержат методические указания по выполнению лабораторной работы «Планирование сети радиодоступа UMTS и расчёт основных параметров» по курсу «Проектирование систем и сетей радиодоступа».

Методические указания соответствуют требованиям типовой программы, утвержденной УМО по направлению подготовки «Инфокоммуникационные технологии и системы связи», рабочей программы дисциплины «Проектирование систем и сетей радиодоступа».

Предназначены для студентов направления подготовки 11.04.02 очной и заочной форм обучения.

Текст печатается в авторской редакции

Подписано печать 14.02 Формат 60x841/16.
Усл. печ. л. 1,04. Уч.-изд. л.0,95. Тираж 100 экз. Заказ 892 . Бесплатно
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94

Разработка Технического Задания на сеть стандарта WiFi (WLAN или БЛВС).

В данных методических рекомендациях описываются некоторые базовые подходы к формулированию сети стандарта WiFi 802.11. Методические рекомендации направлены на формулирование Технического Задания на Проектирование сети стандарта WiFi IEEE 802.11 (WLAN / БЛВС) Централизованной архитектуры.

Часть 1. Общие требования к Решению на сеть стандарта WiFi.

Вначале необходимо описать общие принципы решения, которое Вы хотели бы видеть у себя. Например:

1. Решение должно основываться на стандартах wifi IEEE 802.11,
2. Решение должно поддерживать частотный диапазон 2.4ghz *(если и 5ghz, то стоит указать 2.4+5ghz)*,
3. Решение должно поддерживать российские регуляторные требования к подобному оборудованию для всех используемых частотных диапазонов wifi *(прежде всего это касается требований к 5ghz, но в 2.4ghz также есть свои местные ограничения)*,
4. Решение должно поддерживать стандарт IEEE 802.11n и быть обратно совместимо со стандартами 802.11g, 802.11b и 802.11a *(если предполагается использовать 5ghz)*,
5. Решение должно строиться на централизованной архитектуре – Точки Доступа управляются Контроллером сети Wi-Fi *(отличие централизованной и автономной архитектур описано на нашем сайте здесь)*.

Сценарии проектирования и развертывания сети стандарта Wi-Fi (WLAN)

Сначала необходимо сказать, что существует три больших направления разработки и использования архитектур Wi-Fi-решений:

1. автономная архитектура,
2. централизованная/управляемая архитектура.
3. конвергентная архитектура (объединение проводного и беспроводного доступа)

Именно на основе данных архитектур создается основное количество проектов сетей стандарта Wi-Fi.

В данном модуле мы остановимся на первом и втором вариантах. Необходимо сразу отметить что абсолютное большинство сетей стандарта WiFI Корпоративного или Операторского классов среднего и большого масштаба сегодня строятся на принципах Централизованной Архитектуры с Контроллером сети WiFi во главе. Все основные производители решений WiFi высокого уровня (Cisco, Aruba, Ruckus, HP, Huawei и тд) имеют такие предложения. Выбор подходящего решения и вендора является ключевым

В случае Автономной архитектуры сети Wi-Fi решение представляет собой набор несвязанных точек доступа, каждая из которых конфигурируется и обслуживается независимо. Поэтому сложность обслуживания сети, построенной подобным образом, растет линейно, а порой и экспоненциально,

с ростом количества устройств. Отсюда сети с автономной архитектурой, как правило, давно не проектируют большими. Обычно это не более 3-5 Точек Доступа WiFi. Здесь существуют некоторые исключения, которые облегчают создание чуть более масштабных сетей, например, технология кластеризации точек доступа. Такое решение предлагает Cisco в линейке Точек Доступа Wi-Fi для малого бизнеса (Cisco WAP 321, WAP 121). Но такая архитектура в любом случае не имеет полноценного управления радиоресурсами и тп, т.к. нет единого центра. Все сводится к упрощению задачи конфигурирования сети WiFi. Также в случае автономной архитектуры возникают огромные проблемы с реализацией системы безопасности беспроводной сети, т.к. почти невозможно выполнять корелляцию атаки с учетом всех Точек Доступа в зоне покрытия при отсутствии единого центра. Точки Доступа Wi-Fi независимы и видят эфир каждая по своему, а для полноценной интерпретации такого события как атаки важен масштаб восприятия, понимания динамики атаки. Эта же явление наблюдается и при возникновении проблем с интерференцией, когда невозможно организовать совместное динамическое управление радиоресурсами (RRM-Radio Resource Management) в виду отсутствия единого центра сбора информации со всех ТД и соответствующего принятия решений. Стоит отметить, что известны случаи автономных сетей, состоящих из десятков ТД. Но гарантией эффективной работы такой инфраструктуры в нашей практике являлось наличие квалифицированных инженеров по Wi-Fi в ИТ-службе, которые сами писали специальные скрипты для массового управления всеми Точками Доступа, контроля по SNMP и сбора статистики и т.п. В любом случае, это весьма нетривиальный подход, который еще и очень опасен в перспективе из-за проблем с обслуживанием подобного решения в случае ухода инженера-разработчика данного самописного программного обеспечения. Автономные точки доступа можно приобрести практически у любого вендора решений стандарта Wi-Fi.

В случае Централизованной архитектуры сети Wi-Fi полное управление инфраструктурой сети радиодоступа выполняется контроллером сети WLAN. Например, у Cisco подобная архитектура называется CUWN (Cisco Unified Wireless Network). Контроллер в централизованном решении сети стандарта WiFi управляет загрузкой/изменением ПО, изменениями конфигурации, RRM (динамическое управление радиоресурсами), управляет связью сети WiFi-стандарта с внешними серверами (AAA, DHCP, LDAP и т.п.), управляет аутентификацией пользователей, управляет профилями качества обслуживания QoS, специальными функциями и т.п. Более того, контроллеры могут объединяться в группы для обеспечения бесшовного роуминга клиентов между различными точками доступа в зоне покрытия. Например, в решениях Cisco Systems можно объединить десятки контроллеров в один мобильный домен и, соответственно, до нескольких десятков тысяч точек доступа. Создание подобных мобильных доменов позволяет обеспечить бесшовные хендоверы (в терминах Wi-Fi - это роуминг) между точками доступа управляемых как одним контроллером, так и разными. Существуют эффек-

тивно работающие сети, количество точек доступа в которых приближается к 100.000. Подобных масштабов можно добиться только в централизованной архитектуре решения. Необходимо отметить, что централизованную архитектуру в своих решениях предлагают все ведущие производители: Cisco, Aruba, Ruckus, HP и тд..

Естественно для Точек Доступа или маршрутизаторов с Wi-Fi необходимо ориентироваться на поддержку стандарта IEEE 802.11n и 802.11ac.

На базе технологии WiFi-стандарта развертываются разнообразные решения, приведем несколько примеров по направлениям:

- Wi-Fi-доступ для дома
(с использованием небольших домашних маршрутизаторов с поддержкой радио стандарта Wi-Fi, например от Belkin/Linksys, D-Link, Netgear и т.п.).
Чаще всего в квартире устанавливается один домашний маршрутизатор с Wi-Fi (обычно с частотным спектром 2.4GHz, но лучше, если 2.4+5GHz), который подключается тем или иным проводным интерфейсом к сети провайдера и предоставляет беспроводный доступ домашним пользователям. Здесь имеет смысл обзавестись хотя бы простейшим программным обеспечением типа Wi-Fi Analizer под Android (доступен для Андроид-устройств через Google Play) и проверить, на каких частотных каналах работают подобные устройства соседей. Часто большинство использует идентичные каналы или, что хуже, смежные и перекрывающиеся. Анализ спектра позволит настроить ваше устройство на не занятые каналы, либо каналы с наименьшим уровнем сигнала. И не забывайте включать WPA2 (обычно дома это WPA2-Personal с PSK).

- SOHO/Small Office Home office - WiFi-доступ для небольшого офиса (используются небольшие роутеры с Wi-Fi, более производительные и многофункциональные, чем домашние роутеры, например, Cisco WAP, WET, AP, Cisco ISR с Wi-Fi модулями и ряд других схожих функционально устройств, а также Точки Доступа в Автономном режиме).
Здесь как раз чаще всего очень оправдано использование одного многофункционального, но производительного устройства. Зона покрытия мала, доступного места мало, но нагрузка уже может быть существенно выше, чем в квартире, и требования к стабильности WiFi-доступа и в целом к сети передачи данных несоизмеримы. Поэтому лучше всего выбрать специализированное устройство, спроектированное для данных задач.

- Небольшие корпоративные сети доступа Wi-Fi
(часть этажа, этаж, небольшое здание и т.п.).
Здесь очень хорошо могут применяться решения с централизованной архитектурой, но рассчитанные на небольшое количество Точек Доступа, редко данный уровень решения имеет более 10-20 ТД. Поэтому стоит подобрать небольшой современный контроллер (например, Cisco 2500, Aruba 3000) на

базе отдельного устройства или как модуль в многофункциональный маршрутизатор (например, модуль SRE в маршутизатор Cisco ISR).

- Большие корпоративные сети доступа Wi-Fi
(университетские кампусы, корпоративные кампусы, офисные кампусы, заводские территории, порты и т.п.).
Для подобных задач централизованная архитектура с мощными и функциональными контроллерами - это единственно правильный подход. Можно использовать современные контроллеры. Например такие контроллеры сети стандарта Wi-Fi, как:
- Cisco 5508,
- Aruba A6000,
- Ruckus ZoneDirector 3000
и тп.
В каждом конкретном случае потребуются Точки Доступа того же производителя, что и контреллер сети WiFi-стандарта. Такие контроллеры обычно развертываются в Датацентре компании.

Если производитель WiFi-систем предлагает решение на модулях для коммутаторов или маршрутизаторов, например:
- модуль Cisco WiSM2 в коммутатор семейства Cisco Catalyst 6500/6800,
- модуль Huawei ACU2 в коммутаторы Huawei S12700, S9700, S7700,
- модуль HP JD442A в коммутатор HP 9500, модуль JD440A в коммутатор HP 7500
и тп,
то можно их использовать и на Границе сети (вспомним трехуровневую модель сети передачи данных: ядро, дистрибьюция, доступ). Централизованная архитектура сети WiFi позволит обеспечить практически любой масштаб сети и эффективно управлять ею из единой точки с минимальной нагрузкой на ИТ-персонал.

- Так называемые «бранчи» (Branches) - WiFi-доступ для маленьких удаленных офисов (объединяет большое количество небольших удаленных офисов под централизованным управлением, например, широко используется в банковской сфере для связи штаб-квартиры с удаленными офисами; здесь чаще всего связь между удаленными офисами и центральной штаб-квартирой организуется по арендованным каналам у операторов связи, а иногда и через спутниковые каналы).

В данном случае ключевой проблемой является то, что в силу обычной практики минимизации затрат в бизнесе, коммуникационные каналы для связи с малыми офисами из штаб-квартиры редко бывают выделенными, широкими и надежными. Чаще всего подключение малых удаленных офисов выполняется путем "подключения к интернету" через ближайшего и дешевого провайдера, а о подписании контракта с SLA (Service Level Agreement) с этим провайдером никто и не задумывается (а провайдер, вероятно, даже

не обеспечивает таких услуг). Доступ к корпоративной сети организуется через VPN. При таком подходе очень нередко возникает ситуация, когда канал в удаленном офисе падает или возникают перегрузки на сети провайдера или на стыке его сети с сетью провайдера, к которому подключена штаб-квартира, и связь со штаб-квартирой временно пропадает или становится очень нестабильной. В любом случае подобные проблемы не отменяют желания иметь беспроводную сеть в удаленном офисе, но если таких офисов много (как почти в каждом банке, страховой компании или ритейловой сети), то обслуживание их становится большой проблемой, так как держать ИТ-персонал в каждом офисе просто не рентабельно, а посылать инженера из центра при малейших проблемах с сетью долго и дорого.

Решение должно обеспечивать:

- централизованное управление всем конгломератом удаленных сетей Wi-Fi стандарта (в удаленных офисах) из центрального сайта. Причем это не должно зависеть от разных характеристик каналов « удаленный офис - штаб-квартира»; при этом должны быть возможности централизованного мониторинга, разрешения проблем и конфигурирования удаленных устройств.
- предоставление услуги Wi-Fi в удаленном офисе и при временном падении связи с центральным сайтом (с обязательной поддержкой аутентификации и возможностью входа/выхода Wi-Fi-клиентов),
- возможность как центральной коммутации пользовательского трафика (вывод трафика из удаленного сайта в центральный), так и локальной коммутации (в удаленном офисе).

Для этого необходимо специальное решение и оно есть, например, это специальные облачные контроллеры Flex от Cisco серии 7500 или любой другой Контроллер с поддержкой функционала Cisco FlexConnect.

- Внешние городские сети доступа Wi-Fi

(точки доступа располагаются на улице и предоставляют сервис круглогодично вне помещений, например, для городских служб, горожан и гостей города).

В данном случае наибольший интерес вызывают полносвязные сети Wi-Fi (Mesh), где услуга конечным пользователям предоставляется через один радиоинтерфейс Точки Доступа (обычно на частотах 2.4GHz), а через другой (обычно на частотах WiFi 5GHz) формируется транспортный радиоканал с соседними Точками Доступа. В Mesh-сетях обычно присутствуют два типа ТД: тип Mesh (MAP у Cisco) и Root (RAP у Cisco), где RAP соединяется с проводной сетью, а на MAP строится беспроводная часть сети. В сети Mesh формируются деревья с корнем в RAP, а деревья строятся посредством специализированных протоколов (IAPP у Cisco). Ветви деревьев, как правило, не должны превышать 8 хопов, но здесь все упирается в профили трафика на сети и услуги, а также в конструкцию ТД (если в частотах 5GHz присутствует один радиомодуль, то на каждом хопе пропускная способность бекхола падает практически в два раза, а если есть два независимых радиомодуля частоты 5GHz, то пропускная способность снижается минимально). Сама инфра-

структура Mesh обычно управляется Контроллером сети WiFi-стандарта. Очень хорошо, если программное обеспечение Контроллера WiFi может одновременно управлять и Точками Доступа WiFi в обычном режиме и ТД в Mesh-режиме, так как это позволяет гибко подходить к проектированию сети и связывать как внешние домены, так и внутренние для обеспечения бесшовной мобильности на сети.
Необходимо отметить, что подобные решения нередко применяются и для таких "уличных/внешних" проектов беспроводного доступа WiFi, как покрытие карьеров, заводских территорий, линий рельсового транспорта и т.п..

- Различные решения сети доступа WiFi для специальных случаев (тем не менее, довольно широко распространено):
/ решения WiFi для ангаров, складов,
/ решения WiFi для заводских цехов и территорий,
/ решения WiFi для железнодорожного транспорта (надземного и подземного - здесь подходы различны),
/ решения WiFi для авиационного транспорта,
/ решения Wi-Fi для больших торговых центров,
/ решения Wi-Fi для стадионов и больших демонстрационных или концертных залов (здесь характерна высокая плотность пользователей),
/ решения WiFi для больниц и госпиталей
и т.п.

Во всех этих случаях централизованная архитектура сети стандарта WiFi 802.11 это наиболее правильный выбор, а решение надо разрабатывать с учетом особенностей задачи. На других страницах нашего сайта можно найти более сфокусированную информацию и примеры, посмотрите здесь.
Мы постоянно пополняем наш ресурс. Регистрируйтесь для получения анонсов о размещении новых материалов на сайте или присоединяйтесь к группе Wi-Life на Фейсбуке.

Необходимо отметить, что для реализации Wi-Fi-решений в различных условиях окружениях разработаны и используются Точки Доступа трех основных типов конструкций:
1. Точки Доступа WiFi для использования внутри помещений / "офисный" вариант (часто такие ТД характеризуются привлекательным внешним видом, интегрированными антеннами и относительно узким температурным диапазоном, например, 0- +40 грС),
2. Точки Доступа Wi-Fi для использования внутри помещений / "ангарно-складской" вариант (часто такие ТД имеют металлический корпус, возможность использования внешних антенн и более широкий температурный диапазон, например, -20 - +55 грС),
3. Точки Доступа WiFi для использования вне помещений, на улице / "уличный" вариант (часто такие ТД WiFi характеризуются усиленным внешним корпусом, внешними, иногда интегрированными антеннами, влагозащищенностью корпуса и соединений, широким температурным диапазоном, напри-

мер, -40 - +55 гр С).
Надо также отметить, что существуют модели со специальными корпусами, предназначенными для очень тяжелых окружений, например, для опасной атмосферы, как на химических или нефтеперерабатывающих предприятиях и т.п. Также важно знать, что существует предложение специальных термочехлов, позволяющих использовать внутренние точки доступа вне помещений, а также взрывобезопасных кожухов для особо опасных зон, но здесь надо очень аккуратно и внимательно исследовать вопрос, прежде чем делать выводы.

Часть 2. Требования к Радиоподсистеме сети стандарта Wi-Fi

Мы рассматриваем двухдиапазонную Точку Доступа WiFi (2,4GHz+5GHz), т.к. ставится цель построить современную, качественную и удобную в эксплуатации WiFi-сеть.

1. Радиоподсистема сети стандарта Wi-Fi (Точка Доступа WiFi) должна быть совместима со стандартом IEEE 802.11n и поддерживать совместную работу со стандартами 802.11g, 11b, 11a.

2. Радиоподсистема сети стандарта Wi-Fi (Точка Доступа WiFi) должна отвечать российским нормам регуляторики в обоих частотных диапазонах 2.4GHz и 5GHz.

Частотные полосы и каналы Wi-Fi

Мировая практика использования нелицензируемого частотного спектра:

ISM– Industrial, Scientific, Medical
1. Industrial/Промышленный: 902 – 928 MHz (ширина 26 MHz),
2. Scientific/Научный: 2400 – 2500 MHz (ширина 100 MHz),
3. Medical/Медицинский: 5725 – 5875 MHz (ширина 150 MHz).

Здесь для сетей стандарта Wi-Fi используется в основном часть диапазона 2400 - 2500 MHz.

UNII – Unlicensed National Information Infrastructure
набор полос в диапазоне частот 5150 – 5825 MHz (частично используется для устройств WiFi).

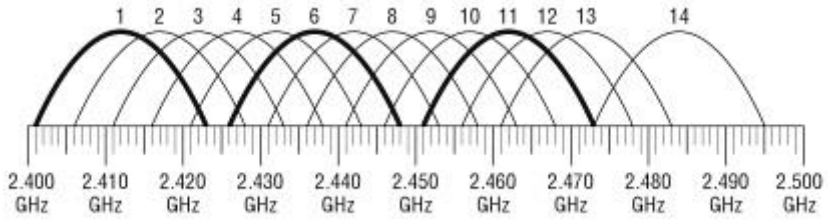
Выбор корректных частотных каналов является одной из ключевых задач для проектирования сети стандарта WiFi 802.11. При этом процесс выбора должен учитывать фундаментальный выбор частотной архитектуры подходящего WiFi-решения: многоканальная или одноканальная архитектура?. Эта ин-

формация также крайне важна при проведении радиообследования (site survey) зоны покрытия будущей сети Wi-Fi.

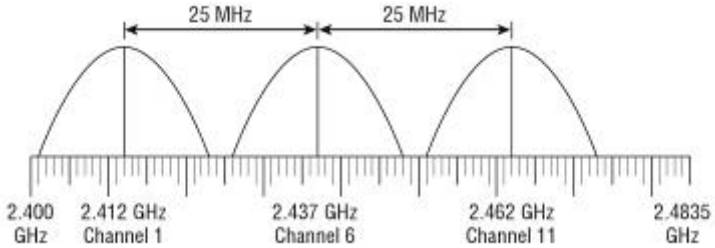
Частотные полосы и каналы WiFi в 2.4 GHz

Канал WiFi	Нижняя частота	**Центральная частота**	Верхняя частота
1	2.401	**2.412**	2.423
2	2.406	**2.417**	2.428
3	2.411	**2.422**	2.433
4	2.416	**2.427**	2.438
5	2.421	**2.432**	2.443
6	2.426	**2.437**	2.448
7	2.431	**2.442**	2.453
8	2.436	**2.447**	2.458
9	2.441	**2.452**	2.463
10	2.446	**2.457**	2.468
11	2.451	**2.462**	2.473
12	2.456	**2.467**	2.478
13	2.461	**2.472**	2.483

Общая диаграмма перекрытия частотных каналов WiFi в 2.4GHz



В полосе частот WiFi 2.4GHz доступны 3 неперекрывающихся канала: 1, 6, 11.
Данное выделение строится на требовании IEEE по обеспечению минимума в 25MHz для разнесения центров неперекрывающихся частотных каналов WiFi. При этом ширина канала составляет 22MHz.



Частотные полосы и каналы WiFi в 5 GHz

Базовая мировая практика, которая может существенно изменяться по странам.

UNII-1: 5150 – 5250 MHz (доступно 4 частотных канала WiFi)
UNII-2: 5250 – 5350 MHz (доступно 4 частотных канала WiFi)
UNII-2 Extended: 5470 – 5725 MHz (доступно 11 частотных каналов WiFi)
UNII-3: 5725 – 5825 MHz (доступно 4 частотных канала WiFi)

Сетка рабочих каналов WiFi и частоты в 5GHz:

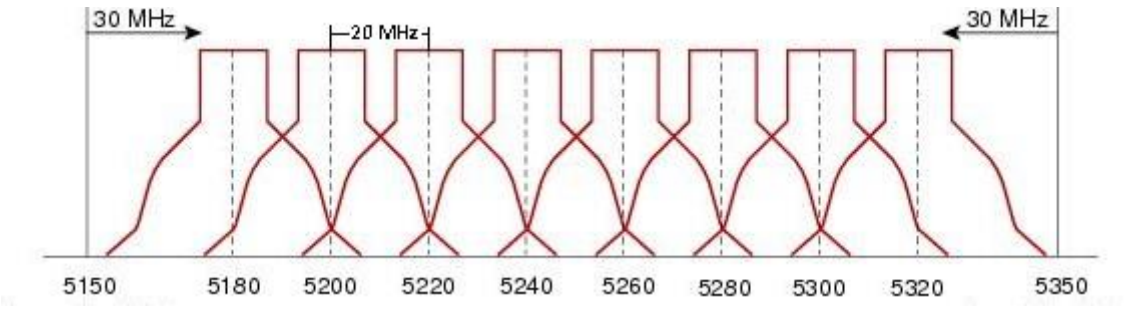
Канал	36	40	44	48
Центральная частота, MHz	5180	5200	5220	5240
Полоса	UNII-1			

Канал	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140
Центральная частота, MHz	5260	5280	5300	5320	5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700
Полоса	UNII-2														

Канал	149	153	157	161
Центральная частота, MHz	5745	5765	5785	5805
Полоса	UNNII-3			

Для вычисления центральной частоты канала WiFi можно использовать следующую формулу:
5000+(5*N) / MHz
/где N это номер канала WiFi, например 36, 40 и т.д./

Формирование каналов WiFi в 5 GHz:



При этом дистанция от граничных диапазонов составляет 30 MHz, а межканальное разнесение составляет 20MHz.

3. Радиоподсистема сети стандарта Wi-Fi (Точка Доступа WiFi) должна поддерживать для IEEE 802.11n частотные каналы шириной как 20MHz, так и 40MHz.

4. Радиоподсистема сети стандарта Wi-Fi (Точка Доступа WiFi) должна поддерживать технологию MIMO (Multiple Input Multiple Output) для 802.11n минимум на уровне 2x2 *(лучше на уровне 2x3 или 3x3, хотя уже вышли решения 4x4, что еще лучше, т.к. здесь уже можно будет эффективно поддерживать 3 пространственных потока)*.

5. Радиоподсистема сети стандарта Wi-Fi (Точка Доступа WiFi) должна поддерживать минимум 2 пространственных потока.

6. Радиоподсистема сети стандарта Wi-Fi (Точка Доступа WiFi) должна иметь необходимые сертификаты РФ, как соответствующее радиоэлектронное средство *(прежде всего Связь)*.

7. В Решении и Предложении должны использоваться Точки Доступа с интегрированными антеннами *(использование ТД с интегрированными/внутренними обычно хороший выбор, если сейчас Ваша задача сделать сеть внутри типовых офисных помещений или просто есть требования по эстетике; если же помещение сложное, например очень высокие потолки или это ангар, заводской цех и т.п., то лучший выбор использование ТД с внешними антеннами, но надо подбирать соответствующие антенны)*.

8. Радиоподсистема сети стандарта Wi-Fi (Точка Доступа WiFi) должна поддерживать функционал интеллектуального контроля спектра на физическом уровне радиосреды в своих частотных диапазонах. Спектральное разрешение здесь должно быть достаточно для определения источников интерференции в зоне покрытия и определения их типа и уровня опасности. *(Подобный функционал является довольно новым в Точках Доступа Wi-Fi и крайне полезен для операционной деятельности ИТ-персонала БЛВС, т.к. позволяет буквально видеть, что влияет на работоспособность беспроводной инфраструктуры. Это удобно как с точки зрения контроля источников интерференции, так и контроля нарушителей безопасности на физическом уровне. Для реализации, как правило, помимо ТД еще необходим соответствующий функционал в Контроллере WLAN, Системе Управления и Платформе Приложений)*.

9. Радиоподсистема сети стандарта Wi-Fi (Точка Доступа WiFi) должна поддерживать динамическое управление диаграммой направленности для усиления уровня сигнала, направленного от ТД к удаленным клиентам.

10. Радиоподсистема сети стандарта Wi-Fi (Точка Доступа WiFi) должна поддерживать MRC (Maximal Ratio Combining) для усиления сигнала приходящего от клиента на ТД.

11. Радиоподсистема сети стандарта Wi-Fi (Точка Доступа WiFi) должна поддерживать репликацию мультикастовых потоков своими средствами. *Это очень важно, если необходимо передвать видеопотоки к большому ко-*

личеству Wi-Fi-клиентов, например с тренингами или речью главы компании и т.п.. Т.к. при отсутствии подобного функционала решение сможет обслуживать видеопотоки только в юникастовом режиме – каждый запросивший поток будет подключен к видеосерверу, даже если тысяча пользователей смотрят один поток! Это означает, что проводная инфраструктура, к которой подключается беспроводная сеть доступа WLAN, должна также поддерживать Весь! объем видеотрафика для, фактически, стресс-режима. Если же мы можем поддерживать мультикастинг на ТД и уже здесь реплицировать мультикаст в юникаст для передачи его только в радиоканале и только тем кто захотел подключиться (послал IGMP join), то мы можем существенно сэкономить на требуемой емкости проводной инфраструктуры в компании.

12. Точка Доступа WiFi должна поддерживать следующие виды питания:

- питание от источника переменного тока 220В, расчитанного на электросети РФ,
- питание через кабель передачи данных Ethernet, в соответствии со стандартом 802.3af или 802.3at

(здесь желательно иметь такие опции как PoE /802.3af или 802.3at/ от коммутатора LAN или наличие инжектора питания в кабель передачи данных).

Часть 3. Требования к Контроллеру сети WiFi-стандарта.

1. Контроллер сети стандарта WiFi должен поддерживать любые допустимые сценарии развертывания и использования Точек Доступа Wi-Fi без дополнительных лицензий.

2. Контроллер сети стандарта WiFi должен поддерживать изменение количества лицензий Точек Доступа Wi-Fi вплоть до максимального для своей модели без замены конструктива.

Имеется ввиду, что расширение количества лицензий должно проводиться только путем докупки лицензий и активации некоего ключа, а не заменой коробки.

3. Контроллер сети стандарта WiFi должен поддерживать не менее X Точек Доступа WiFi.

Здесь X это то количество, которое Вам необходимо на некоем обозримом горизонте планирования. Иначе, если взять небольшой контроллер, а через пару месяцев еще один, потом еще, то скоро возникнет слабоуправляемый и ненадежный огород. Хотя даже в этом случае использование Системы Управления WLAN может существенно упростить работу с такой сетью.

4. Контроллер сети стандарта WiFi должен поддерживать корелляцию возникновения событий изменения интерференционной картины со всех подключенных Точек Доступа WiFi.

Это важно для более точного понимания проблем в радиоэфире, т.к. чем

больше ТД могут предоставить свое видение картины, тем точнее выводы. И, при наличии дополнительного функционала определения местоположения, это позволяет выполнять триангуляцию и предоставлять информацию о том, где расположен источник интерференции или вражеское устройство.

5. Контроллер сети стандарта WiFi должен поддерживать централизованную аутентификацию пользователей с использованием как функциональности второго уровня 802.1x, так и третьего уровня с использованием встроенного Web-сервера. Встроенный функционал 802.1x должен обеспечивать аутентификацию посредством протоколов: EAP-TLS, EAP-TTLS, EAP-FAST, MD5 и т.п.. Встроенный функционал Web-сервера и Web-портала должен обеспечивать ручное конфигурирование и возможность добавления-удаления учетных записей пользователей сети неквалифицированным персоналом.

6. Контроллер сети стандарта WiFi должен поддерживать централизованную аутентификацию пользователей с возможностью интеграции с внешними AAA-серверами по протоколу RADIUS.

7. Контроллер сети стандарта WiFi должен обеспечивать возможность напрямую или через AAA-сервер подключать популярные базы данных: LDAP и Microsoft Active Directory.

8. Контроллер сети стандарта WiFi должен иметь встроенный функционал системы обнаружения вторжений и нарушения безопасности сети Wi-Fi.

9. Контроллер сети стандарта WiFi должен поддерживать простой Web интерфейс для удаленного управления и конфигурирования.

Часть 4. Требования к Системе Управления сети стандарта WiFi.

1. Система Управления сети стандарта WiFi должна поддерживать полный жизненный цикл инфраструктуры Wi-Fi. Необходимы, как минимум, следующие функции:

- инструменты оценочного планирования как для новых развертываний Wi-Fi-сети, так и для расширения/изменения существующей сети WiFi; инструмент должен быть достаточно аккуратным и позволять планировать по картам зоны покрытия, учитывать ожидаемые услуги на сети Wi-Fi, учитывать предполагаемый тип и модель Точек Доступа WiFi и внешних антенн (когда необходимо) и т.п..
- инструменты анализа развернутой инфраструктуры WLAN и рекомендации к необходимым изменениям,
- инструменты мониторинга инфраструктуры WLAN (БЛВС),
- инструменты поиска и устранения неисправностей в WLAN (БЛВС),
- инструменты контроля производительности и т.п..

2. Система Управления сети стандарта WiFi должна поддерживать все основные элементы инфраструктуры WLAN (БЛВС), как минимум:

- Точки Доступа Wi-Fi,
- Контроллеры сети WiFi,
- Интегрированные Платформы Приложений сети WiFi, если присутствуют в решении,
- Клиенты с радио стандарта Wi-Fi - мониторинг и управление устранением неисправностей,

3. Система Управления сети стандарта WiFi должна поддерживать системы обеспечения безопасности WLAN (БЛВС) и предотвращения вторжений. Комплексные политики безопасности должны быть решены в виде обобщенных профилей безопасности для упрощения взаимодействия оператора с системой. Необходимы механизмы оценки текущего уровня безопасности WLAN (БЛВС) и рекомендации к его коррекции. Необходимы механизмы формирования отчетов на соответствие нормам PCI.

Примеры типовых проектов

Проект сети стандарта WiFi для Кампуса

(Университетский городок, Группа офисных зданий, Заводская территория и т.п.)

Тренировочный пример с учетом реальных задач, возникающих на подобных проектах.
Важно: представлен один из возможных подходов к реализации поставленной задачи, конечно решить ее можно многими способами, но здесь приведен один из обоснованных примеров.

Сначала хотелось бы отметить, что сети стандарта Wi-Fi для Кампусов очень популярное направление проектной разработки. А для таких Заказчиков как, например, университеты США, наличие доступа Wi-Fi для судентов уже давно стало особой отличительной чертой, которая долгое время использовалась для увеличения привлекательности Университета в глазах будущих абитуриентов (если ты не входишь в Лигу Плюща, то за студентов приходится бороться). Сейчас в США это стало едва ли не обязательно, и уровень университетских кампусных сетей Wi-Fi очень высок. Жаль, что наши Высшие Учебные Заведения нечасто могут похвастаться чем-то подобным. А ведь сеть WiFi важна не только для созданий привлекательности, но и легко становится очень важным подспорьем в учебном процессе, при построении системы безопасности и поддержке ежедневных вспомогательных операций. Все это возможно только при разумном и комплексном подходе к проектированию сети WiFi-стандарта и услуг через сеть WiFi.

Проанализируем возможные исходные данные проекта кампусной сети стандарта WiFi:

общая концепция

- будут ли присутствовать внутренние сегменты сети стандарта WiFi (внутри помещений);
- будут ли присутствовать внешние сегменты сети WiFi (вне помещений - открытое размещение на улице);
- расположение узла управления и контроля сетью WiFi (центральный сайт);
- сервисная ориентация сети WiFi: для обеспечения внутренних задач, для продажи услуг третьим лицам, смешанный вариант;
- общий подход к предоставлению услуг на сети: какие услуги предполагается оказывать, какие из них будут предоставляться на контролируемой и гарантируемой основе, а какие на принципах «как получится».

география, архитектура и особенности окружения предполагаемой зоны покрытия сетью

- внутренние сегменты сети (внутри помещений) / конструктивные особенности зданий (типовое жилое или офисное помещение, офис с высокими потолками, цех, ангар и т.п.), / источники интерференции и их опасность, / требуемая плотность развертывания радиоподсистемы (зависит от распределения пользователей, концентрации пользователей, предоставляемых услуг и т.п.),
- внешние сегменты сети (уличные сегменты)

/ холмистая местность или плоская, / есть ли деревья или иные препятствия в зонах распространения радиосигнала, (необходимо учитывать сезонные особенности, например, появление листвы в теплое время года или развертывание больших рекламных конструкций, которые ранее были сняты)

/ источники интерференции и их опасность,

количество пользователей Wi-Fi-сети, прежде всего мобильных

- надо четко понимать общее количество пользователей сети,
- зоны их максимальной концентрации и ожидаемые величины концентрации в этих зонах,
- процент активных пользователей из общего количества,
- ожидаемый прирост количества пользователей сети в обозримой перспективе,

используемое пользовательское оборудование на сети и владение/управление этим оборудованием

- какие терминалы у пользователей (лаптопы, смартфоны, планшеты и т.п.);
- какое оборудование используют корпоративные службы (лаптопы, Wi-Fi IP-телефоны, метки RFID, беспроводные сканнеры бар-кодов и т.п.);
- есть ли четкие правила распределения пользователей в различных зонах покрытия сети по типам используемого оборудования;

- кто управляет оборудованием (конфигурирует).

детализация предполагаемых услуг на сети

- детализация услуг на сети;
- требования к каждому виду услуг (полоса пропускания, задержка, джиттер, потери пакетов и т.п.);
- ожидаемые величины потребителей различных услуг;
- очень неплохо вообще попытаться продумать возможные профили трафика на сети по различным группам потребителей;
- надо также оценить возможные проблемы от «опасного» использование услуг, например, неограниченное «висение» пользователей в пиринговых сетях, как например BitTorrent, eDonkey и т.п. Имеет смысл заранее планировать минимизацию подобных проблем через специальные подходы и средства, но это не тема данной статьи.

принципы безопасности на сети WiFi

- группы пользователей и методы аутентификации для разных групп (студенты, преподавательский состав, технический персонал и т.п.);
- необходимость организации гостевого доступа и методы аутентификации в данном случае.

Рассмотрим возможные подходы к дизайну кампусной сети:

1. Основной и проверенный подход настоящего времени - это проектирование архитектуры такой крупной сети, как Решения, управляемого Контроллером WLAN. Преимущества Централизованной Архитектуры с Контроллером WLAN по сравнению с Автономной кратко описаны здесь.
2. Есть опции сделать сеть на автономных уличных и офисных точках доступа или даже на дешевых домашних раутерах с Wi-Fi...-). Заставить работать можно и такую «инфраструктуру», но неизбежным фактом является то, что казалось бы большая экономия на капитальных затратах CapEx будет едва ли не мгновенно съедена ничем не ограниченным OpEx-ом (операционные затраты), так как эта сеть будет совершенно неуправляемой и крайне нестабильной в работе. Так что принимайте обоснованные решения!

Итак остановимся на том, что реально будет работать и то что является гибким, надежным и максимально масштабируется. Очевидно это будет первый подход с использованием Решения Централизованной архитектуры.

Очень полезно написать для себя Техническое Задание на проектирование сети Wi-Fi,
пример формирования которого можно найти на нашем сайте.

Решение WLAN (БЛВС) для Кампусной сети на базе Централизованной Архитектуры

Как показывает практика, делать «ковровое» покрытие в Кампусе с доступом в каждом углу и на каждой площадке погрузки мусора совсем не обязательно. Это подтверждает пример кампуса американского Университета

Юго-Восточной Луизианы (SouthEastern Louisiana University). Пример взят с сайта университета.

На карте покрытия WLAN видно распределение зон покрытия внутри помещений и снаружи (уличное покрытие).

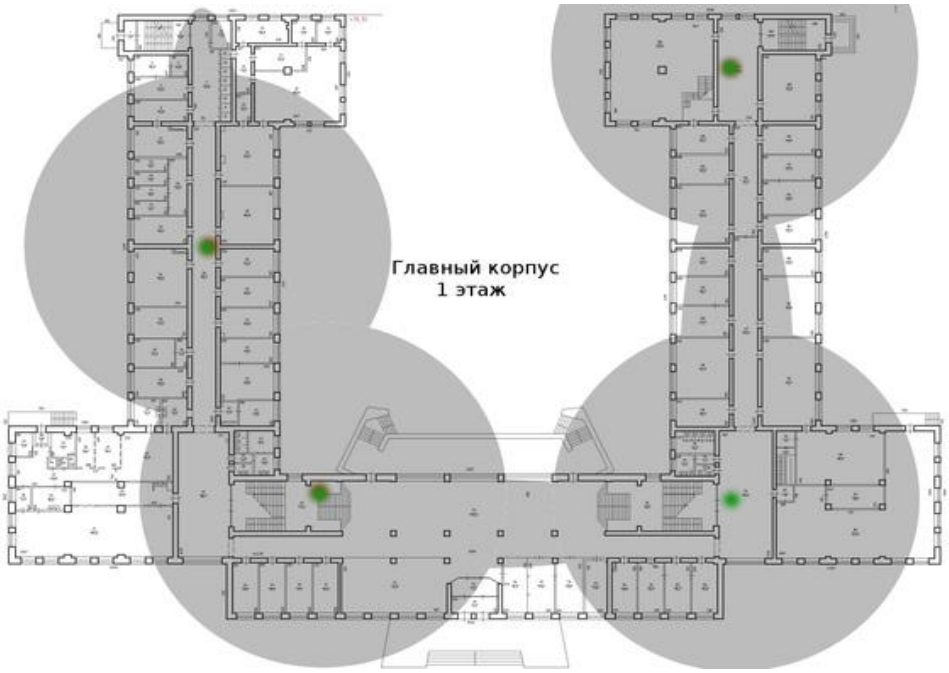
Внутри помещений -Желтый цвет

Снаружи -Зеленый цвет

Видно, что покрытие далеко не повсеместное. Все построено на принципе «горячих зон», в которых уже обеспечивается беспроводный доступ.

Пример Кампусной Wi-Fi сети Университета SouthEastern Louisiana University.

С другой стороны, внутри самих зданий нередко создается достаточно полное покрытие. Следующий пример взят с сайта НГУ. Это покрытие первого этажа сетью Wi-Fi, построенной Университетом для своих студентов:



Необходимо провести собственное исследование и точно определить зоны, где покрытие действительно важно!

После выявления зон, определимся с тем, что внутри помещений будем использовать в основном внутренние Точки Доступа WiFi с Интегрированными антеннами (для специальных задач - внутренние ТД с внешними антеннами), а снаружи специальные Точки Доступа уличного исполнения в защитном корпусе и с широким температурным диапазоном. Все управляется Контроллером сети WiFi (точее, как минимум парой контроллеров, где один является резервным, например по схеме N+1).

В случае проектирования сети стандарта WiFi для студенческого городка зону покрытия на улице для уличных Точек Доступа Wi-Fi надо просчитывать особенно тщательно. С одной стороны, эти Точки Доступа обычно весьма дороги (в сравнении с внутренними - из-за специальных корпусов и т.п.), с другой стороны, в условиях российского климата студенты не много времени реально проводят в парке кампуса, если таковой имеется. Хотя и здесь вполне можно рассмотреть варианты внутренного сквера для студентов, зон погрузки/разгрузки транспорта для персонала, работающего с поставщиками и т.п. Самое тяжелое планирование – внутри помещений, особенно в зонах концентрации пользователей, например, аудитории и большие лекционные залы, актовые залы и обеденные зоны. Здесь основной подход – оценка сети WiFi «по ёмкости». Вероятно, в общих коридорах, где нет сидячих мест, нет смысла предоставлять доступ стандарта Wi-Fi.

В кампус могут входить и весьма сложные для сети стандарта WiFi зоны покрытия, например, спортивные залы, высокие лекционные залы (в кампусе могут быть и офисные помещения с высокими потолками без перекрытий на высоту нескольких этажей, заводские цеха, складские ангары и т.п.). Здесь используются внутренние Точки Доступа WiFi, но с внешними антеннами, часто даже с направленными. Нередко в таких помещениях приходится даже отдалять Точки Доступа WiFi или их антенны от потолка - из-

за наличия на оном силовых или технических конструкций, вызывающих мощное многолучевое распространение сигнала (multipath) в направлениях как от ТД Wi-Fi, так и к ТД Wi-Fi. Выручает использование специальных, закрепляемых на потолке, штанг, на которые уже крепятся сами Точки Доступа WiFi с антеннами или же только Антенны на кабелях, а ТД WiFi в таком случае могут крепиться и на потолке, и за фальшпотолком. И, естественно, применение направленных антенн позволяет снизить многолучевое распространение, так как значительно меньше излучения уходит к потолочным конструкциям по сравнению, например, с всенаправленными омни-антеннами. Важно заметить, что в среднем высота подвеса антенн от уровня, где находятся пользователи, не должна превышать 10 м. Это касается и внутреннего развертывания (например, точки на потолке с направленными антеннами), и внешнего. Снаружи чаще всего Точки подвешивают на фонарных столбах или светофорах. Но важно найти не просто место удобное для подвеса, но и такое, к которому постоянно подведено электрическое питание (24 ч), поэтому с уличными фонарями надо быть осторожнее. Так как наружную сеть часто проектируют с беспроводным транспортным каналом (бэкхолом), чтобы снизить нагрузку от необходимости проектировать и строить активную транспортную сеть на улице, то здесь прежде всего важно наличие электропитания для ТД.

Выполним первичную оценку сети стандарта Wi-Fi Кампуса на следующем примере:

Задача:

1. Необходимо в первом приближении спланировать и оценить сеть университетского городка, в которую входят (см. рисунок):

- 1. 2 х Учебных здания

(оба здания идентичны; каждое имеет 5 этажей, на каждом этаже 10 аудиторий площадью 80 кв.м с местами для 20 студентов; в каждом здании 4 больших лекционных зала на 100 студентов, площадью 300 кв.м с обычнми потолками каждый; в каждом здании 1 столовая площадью 500 кв.м),

- 2. 1 х Общежитие (16 этажей, каждый этаж площадью 600 кв.м, 20 комнат на этаже),
- 3. 1 х Спортивный зал (высота потолков в зале 7 метров, общая площадь 3000 кв.м)
- 4. 1 х Сквер (площадь 100.000 кв.м)

2. Центральный сайт (комната с ИТ-оборудованием и персонал ИТ-службы) находится в Учебном здании-1.

Каждую удаленную зону покрытия (здание) необходимо связать с центральным сайтом беспроводным транспортным каналом, обеспечивающим скорость передачи данных на уровне 1Gbps, так как нет возможности прокладывать оптику под землей, а воздушная прокладка пресекается контролирующими службами. Максимальное расстояние для оценки между зданиями со-

ставляет 1 км.

3. Специальные услуги предоставлять не предполагается. Основная услуга, на которую планируется сеть Wi-Fi, - это смешанный доступ к Интернет и к информационным службам локальной сети Университета. Особенно сложных профилей трафика не предполагается. Минимальная скорость на границе ячейки около 6 Mbps. Примем, около 50% студентов должны получить возможность одновременно выходить в сеть через различные Wi-Fi-устройства (и это довольно жесткое условие).

Исходные данные к заданию на рисунке
(в реальной практике очень важно иметь карту с расположением зданий Кампуса – можно использовать Google Earth, а также поэтажные планы Всех зон покрытия внутри строений)

Выполним оценочное планирование сети WLAN:

Сразу подчеркнем – все оценки по возможному радиусу покрытия, емкости и т.п. представлены из обобщенного опыта и не являются окончательной истиной. В нормальной практике эти оценки надо обязательно проверять в реальных условиях зоны развертывания, с реальным пользовательским оборудованием и моделированием ожидаемых услуг - до заказа оборудования.

Первичный подход к планированию – визуализация на карте покрытия

1. Учебное Здание

- примем подход, при котором полное покрытие выполняться не будет и мы будем покрывать каждую аудиторию, лекционные залы и столовую – формируем «горячие зоны» Wi-Fi.

- Аудитории:

будем планировать 1хТочку Доступа на 1хАудиторию

/если аудитории малы и есть риск того, что частотный канал в одной аудитории будет «виден» в соседней аудитории с таким же каналом, можно просто снизить мощность Точек Доступа на Контроллере, для уменьшения интерференции/.

По покрытию этот подход вполне проходит, см. калькулятор для R=14м и площади 80 кв.м: http://wi-life.ru/uslugi/kalkulyator;

В то же время по емкости мы имеем 50% от 20 потенциальных пользователей в аудитории, то есть 10 (надо заметить, что при обычных профилях трафика мы можем ориентироваться на средний допустимый максимум порядка 20-25 активных пользователей на одну Точку Доступа).

Итак, примем 1 ТД на 1 Аудиторию.

Для оценки будем использовать бюджетную модель Точки Доступа WiFi начального уровня Cisco 1041 (частоты 2,4GHz, интегрированные антенны).

- Лекционный зал:

Если планировать «по покрытию», то, вероятно, нам будет достаточно 1 ТД на весь лекционный зал

(см. калькулятор для оценочного радиуса R=14м и площади 300 кв.м: http://wi-life.ru/uslugi/kalkulyator). Но здесь присутствует емкостное условие: 100 студентов, из них до 50% - активные пользователи (50 человек). Учиты-

вая, что в среднем мы ориентируемся на 20-25 пользователей на 1 ТД, нам потребуется 2 ТД на 1 Лекционный зал.
Итак, примем 2 ТД на 1 Лекционный зал.
Для оценки будем использовать модель ТД среднего уровня Cisco 1142 (2,4+5GHz, интегрированные антенны). Такой выбор обоснован необходимостью запаса по емкости - если в учебных целях потребуется доступ для большинства студентов в зале. Дополнительное радио 5GHz позволит нам иметь потенциал почти удвоения емкости, а поддерживаемая функция BandSelect от Cisco на этой ТД даст возможность вытянуть всех совместимых с 5GHz клиентов в этот диапазон принудительно, распределить нагрузку между интерфейсами 2.4GHz и 5GHz и существенно поднять емкость.

- Столовая:
Учитывая, что в столовой большая часть времени тратится на еду и не поощряется долгое сидение с лаптопами и иными мобильными устройствами, то можно ограничиться оценкой «по покрытию». В данном случае остановимся на 1 ТД на всю столовую (см. калькулятор для R=14м и площади 500 кв.м: http://wi-life.ru/uslugi/kalkulyator) .
Итак, примем 1 ТД на 1 Столовую.
Для оценки будем использовать бюджетную модель начального уровня Cisco 1041 (2,4GHz, интегрированные антенны).

Обобщенная оценка на два Учебных здания:

1. Аудитории:
- 10 Точек Доступа Cisco 1041 на этаж,
(1 ТД на 1 Аудиторию, при 10 Аудиториях на этаж = 10 ТД на этаж для аудиторий)
- 10x5=50 Точек Доступа на Здание,
- 50 x 2 = 100 ТД на 2 Здания

2. Лекционные залы:
- 2 ТД Cisco 1142 на 1 Лекционный зал,
- 8 ТД Cisco 1142 на 4 Лекционных зала / 1 Здание,
- 8 x 2 = 16 ТД на 2 Здания.

3. Столовая:
- 1 ТД Cisco 1041 на 1 Столовую,
- 1 x 2 = 2 ТД на 2 Здания.

4. - на каждый этаж используем 1 Коммутатор LAN. Для примера возьмем распространенный вариант Cisco Catalyst модели WS-C2960S-24PS-L, который имеет 24 GE порта с поддержкой 802.3af/PoE (для присоединения Точек Доступа и подачи к ним питания по кабелю по PoE), и слоты под модули SFP для проброса оптических каналов к аггрегирующему коммутатору. Для ми-

нимизации затрат примем, что один Cat 2960 будет выполнять и функцию аггрегации Здания, собирая на свои SFP-порты оптические кабели с 4-х других этажей. Со следующим уровнем можно состыковаться, используя свободные электрические порты 1GE, с помощью, например, Gigabit Etherchannel.
Итак, на Здание 5x Cisco Catalyst модели WS-C2960S-24PS-L + 4 x (2xSFP GLC-LH-SM (Single Mode)),
на 2 Здания 2 x (5x Cisco Catalyst модели WS-C2960S-24PS-L + 4 x (2xSFP GLC-LH-SM (Single Mode))

5. Для аггрегации всех зданий и формирования LAN центрального сайта используем один Коммутатор LAN Центрального сайта. Для оценки используем модель Cisco Catalyst WS-C3560E-48TD-S (48 портов 10/100/1000 и 2 слота под SFP X2 на 10GE)
Итак, на всю сеть 1 x Cisco Catalyst WS-C3560E-48TD-S

2. Общежитие
Здесь необходимо обеспечить повсеместное покрытие с минимальными затратами.
(По нашей задаче, здание имеет 16 этажей, каждый этаж площадью 600 кв.м, на этаже 20 комнат 5x4м расположенные по 10 комнат с каждой стороны общего коридора, плюс сам общий коридир).
В каждой комнате такой площади можно ожидать 2-3 человека и, вероятно, каждый будет использовать интернет-доступ. Поэтому будем планировать исходя из емкости. На данном этапе разумным выглядит подход с планированием 1 ТД на 4 комнаты. Целевой радиус покрытия, при этом, составит 8-10м, что вполне разумно даже через стену (естественно, это надо проверять на практике).
Итак, примем 5 ТД на 1 Этаж.
Для оценки будем использовать бюджетную модель начального уровня Cisco 1041 (2,4GHz, интегрированные антенны). Добавление 5GHz вряд ли существенно добавит емкости из-за значительного поглощения этих частот стенами, а в коридоре, обычно, не так много пользователей с терминалами.
На каждые два этажа планируем использовать один Коммутатор LAN с PoE модели Cisco Catalyst WS-C2960S-24PS-L, соответственно всего 8 Коммутаторов LAN на Здание. Для аггрегации всех 8-и Коммутаторов здания Общежития перед транспортным пролетом в сторону Центрального сайта используем Коммутатор LAN модели Cisco Catalyst 3750X с оптическими модулями SFP GLC-LH-SM.

<u>Обобщенная оценка на все Общежитие:</u>

- 5 ТД Cisco 1041 на 1 Этаж
- 5 x 16 = 80 ТД на 16 этажей

- 8 Коммутаторов Catalyst WS-C2960S-24PS-L на этажах на все Здание

- 1 Аггрегационный Коммутатор LAN Cisco Catalyst 3750X на все Здание
- 2x8 =16 модулей SFP (GLC-LH-SM) + 1 модуль SFP (GLC-T/электрический) для стыка с оборудованием микроволновой трансмиссии к центральному сайту.

3. Спортивный зал

См. пример на рисунке задания с метражем:
- Зона фойе и служебных помещений: 2 этажа, каждый этаж площадью 600 кв.м (20x30 м)
- Зона игрового поля не покрывается
- Зона сидячих мест в Зале имеет площадь 600 кв.м (10x60м) и расчитана на 500 человек.

Выполним оценку зоны фойе и служебных помещений. Будем оценивать сплошное покрытие по площади, так как нет никаких требований по емкости. Здесь используем калькулятор количества ТД и примем необходимое количество ТД равное 2. Для оценки будем использовать бюджетную модель начального уровня Cisco 1041 (2,4GHz, интегрированные антенны).
Итак, для двух этажей примем 4 ТД модели Cisco 1041.

Выполним оценку зоны сидячих мест в зале.
Здесь дополнительно необходимо учесть два крайне важных фактора:
1. Высота потолков (7м),
2. Высокая плотность посадки потенциальных пользователей (приблизительно 1 человек на 1 кв.м).

Соответственно, будем выполнять оценку как к объекта с высокой плотностью пользователей и увеличенной дистанцией ТД<>Пользовательское устройство. Для этого будем применять следующие приемы:
1. подвес внутренних ТД с внешними антеннами на потолке (или за фальшпотолком);
2. использование панельных направленных антенн для настенного размещения с узкой диаграммой направленности для жесткого «секторирования» зоны покрытия;
3. расположение антенн на стене позади кресел и снижение высоты подвеса антенн от потолка к креслам.

При максимальном заполнении Зала мы можем иметь следующее количество активных пользователей: 50% от 500 человек = 250 человек (обычно процент бывает существенно ниже – до 10-15%, но с ростом количества смартфонов и при наличии бесплатной сети доступа можно ожидать существенного прироста активных пользователей - с этим лучше определиться точнее во время начального ассесмента). При оценочной емкости Точки Доступа в 20-25 пользователей на один радиоинтерфейс мы можем ориентироваться на показатели 40-50 пользователей на два радиоинтерфейса с частотами

2,4GHz+5GHz. Соответственно, в данной задаче будем использовать ТД Cisco 1262, которая поддерживает оба диапазона, с портами под внешние антенны.
Далее нам необходимы Панельные антенны с возможностью настенного монтажа. В этом случае мы можем планировать монтаж Точек на потолке (например, за фальшпотолком), а антенны опускать по стене вниз на несколько метров, соединяя ТД WiFi и антенну подходящим коаксиальным кабелем. Антенны будут размещаться на стене позади кресел (возможен вариант «прострела» через игровое поле, но здесь дальности существенно больше, хотя и с радиотенью будет значительно меньше проблем). Для оценки будем использовать две схожие по геометрии диаграммы направленности панельные антенны от Cisco:
- для частот 2.4GHz: двухэлементную панельную антенну «AIR-ANT2465P-R» (Азимут: 75 гр, Элевация: 57 гр),
- для частот 5GHz: двухэлементную панельную антенну «AIR-ANT5170P-R» (Азимут: 70 гр, Элевация: 50 гр).
При азимуте около 70 гр и удалении от стены до дальней точки – первого ряда кресел - около 15 м можно ожидать зону максимально уверенного покрытия на 1 ряду порядка 12-15 м.
Соответственно, в первом приближении нам необходимо 4-5ТД для покрытия длины первого ряда в 60м. Элевация этих антенн порядка 50гр и, если их дополнительно наклонить вниз при монтаже (зависит от реального расположения кресел) , то можно сформировать уверенное покрытие. Но остается проблема возможной радиотени вблизи стены, на которой расположены антенны в промежутке между антеннами. В принципе, одним из возможных подходов может быть использование антенн 5GHz для решения этой проблемы. Можно попробовать немного доворачивать антенны 5GHz во время монтажа в сторону радиотени от двух соседних ячеек 2.4GHz. Это «немного» определяется в ходе предварительного радиообследоваия и моделирования в реальной зоне покрытия с реальным оборудованием. Либо можно пойти по пути установки антенны чередуя 2.4-5-2.4-5 и т.д. При этом угол наклона, например, антенн 5GHz может быть больше, чем 2.4. Эти показатели надо подбирать только опытным путем в ходе радиообследования!
Для оговоренной целевой емкости в 250 активных пользователей (пример, что они распределены равномерно), необходимо 5 ТД с двумя радиоинтерфейсами. Соответственно, имеет эквивалентность требований покрытия и емкости с текущим уровнем информации.

Итак, примем 5 ТД на зону сидячих мест в Зале.
Для оценки будем использовать модель Cisco 1262 (частоты WiFi 2,4GHz+5GHz, внешние антенны).
На каждую ТД используем внешние антенны (1+1 каждой модели на 1 ТД):
- для частот 2.4GHz: двухэлементную панельную антенну «AIR-ANT2465P-R» (Азимут: 75 гр, Элевация: 57 гр),
- для частот 5GHz: двухэлементную панельную антенну «AIR-ANT5170P-R»

(Азимут: 70 гр, Элевация: 50 гр).

Обобщенная оценка сети стандарта WiFi на все здание Спортивного Зала:

1. Фойе и служебные помещения:
- 2 Точки Доступа Cisco 1041 на этаж,
- 2 + 2 = 4 ТД на всю зону фойе и служебных помещений.

2. Зона сидячих мест спортивного зала:
- 5 ТД Cisco 1262 на данную зону,
- 5 Антенн AIR-ANT2465P-R,
- 5 Антенн AIR-ANT5170P-R.

3. Коммутаторы LAN
- 1 Catalyst WS-C2960S-24PS-L для присоединения ТД в Зале,
- 1 Catalyst WS-C2960S-24PS-L для присоединения ТД в фойе и служебных помещениях, а также аггрегации всего здания перед стыком с микроволновой трансмиссией в сторону центрального сайта.

4. Сквер

Примем, что сквер частично освещен и есть фонарные столбы высотой 5 м. Для оценки будем использовать радиус ячейки порядка 100 м (по неофициальным данным, при высоте подвеса 10 м в уличных условиях на уличных Точек Доступа WiFi от Cisco можно ожидать радиуса ячейки до 180 м). Используем Калькулятор Точек Доступа WiFi для R=100 и площади 100.000 кв.м:
Получим: 4 ТД WiFi. Из них: 3 ТД будут иметь тип Mesh и будут осуществлять основное покрытие для сервиса. Монтироваться они будут в сквере на столбах (важно иметь питание 220В 24 часа в сутки. 1 ТД WiFi будет иметь тип Root с подключением проводным интерфейсом к Коммутатору LAN). Данная Точка Доступа WiFi монтируется на внешней стене Учебного здания-1, там, где находится Центральный сайт сети WiFi.
Итак, примем 4 Точки Доступа WiFi на весь сквер.
Для оценки будем использовать модель Точки Доступа WiFi Cisco 1552 (частоты 2,4GHz+5GHz, внешние антенны).

5. Беспроводные каналы точка-точка

Для соединения удаленных зданий в Кампусе с Центральным сайтом используем радиорелейные пролеты («микроволновки» или микроволновую трансмиссию) - это специальные радиосистемы, которые физически выглядят как два радиобриджа, но используют несколько иную технологию и, чаще всего, работают на значительно более высоких частотах. Некоторые системы здесь могут выходить на уровень скорости передачи порядка 1Gbps на дистанциях 1-2 км и используемых частостах в диапазоне 71-76GHz, например, системы

Siklu. Это недорогие системы *(примем для оценки $8.000 на один пролет точка-точка/два устройства, но для корректного предложения связывайтесь с официальным представителем в РФ)*. Решение Siklu это прозрачный L2-тоннель, моделирующий транспортный канал Gigabit Ethernet. Транспортные каналы такой емкости позволят собрать адекватную инфраструктуру как для соединения высокозагруженных удаленных сетей доступа с центральным сайтом и замкнуть ЛВС (LAN) всего Кампуса, так и обеспечить высокие скорости доступа в Интернет (конечно, если далее каналы связи со встречными ISP достаточны для поддержания высоких скоростей).
Итак, примем 3 пролета Siklu "EtherHaul E-Band Radio" на весь проект. Каждый пролет имеет оценочную стоимость $8.000. Итого: 3 x $8К = $24.000 *(для корректного предложения связывайтесь с официальным представителем в РФ)*

Большим плюсом для использования в РФ является то, что радиоустройства, работающие на столь высоких частотах и с узким лучом не требуют сложного лицензирования. Легализация решения носит уведомительный характер на момент выхода данной статьи.

На данном этапе не будем планировать резервирования транспортной микроволновой инфраструктуры. Пока придерживаемся дизайна Звезда (hub and spoke). Целесообразность этого надо выяснять на первичном ассесменте (обследовании/обсуждении) со всеми заинтересованными лицами.
Но, при необходимости, резервирование этой части можно легко выполнить, например, замкнув транспортные каналы в треугольник (по сути кольцо) и добавив небольшие маршрутизаторы на каждый узел треугольника. Это позволит не только выполнить резервирование по кольцу на третьем уровне, но и локализовать бродкастные домены в каждой удаленной локации, а также ввести дополнительные точки применения политик безопасности. Хотя цена решения, безусловно, возрастет.

6. Центральный сайт
Для начальной оценки мы не будем глубоко детализировать данную часть, так как необходимо больше практической информации о том, что уже используется в коммуникационной инфраструктуре данного Кампуса, что можно переиспользовать, а с чем надо интегрироваться новой сети.

Необходимость планирования Коммутатора LAN для Центрального сайта уже упоминалась, и модель предложена в части Учебных Зданий. Из обязательной программы нам необходимо добавить два Контроллера WLAN и Систему Управления, которая позволит не только эффективнее мониторить сеть, но легче и быстрее решать проблемы требовательных пользователей.
Итак:
1. 2хКонтроллера сети WiFi, для оценки примем модель Cisco 5508-250 (оба контроллера работают как Primary/Secondary (не путать с Active/Standby)),

2. 1xСистема Управления WLAN, для оценки примем модель Cisco NCS-250 как отдельное устройство.

Оценка Решения WLAN для рассмариваемой сети Кампуса

1. Точки Доступа:
- 186 x Cisco 1041,
- 16 x Cisco 1142,
- 5 x Cisco 1262,
- 4 x Cisco 1552.

2. Антенны:
- 5 x 2465,
- 5 x 5170.

3. Контроллеры WLAN:
- 2xCisco 5508-250.

4. Система Управления WLAN:
- Cisco NCS-250.

5. Коммутаторы LAN:
- 20 x Cisco Catalyst 2960S,
- 1 x Cisco Catalyst 3560E-48,
- 1 x Cisco Catalyst 3750X

6. Модули SFP:
- 1 x SFP GLC-T,
- 32 x SFP GLC-LH

Далее используем калькулятор оценки Решения для WLAN на нашем сайте. В результате получаем оценочную стоимость проекта $507.888 (по ценам Cisco GPL из Интернет/Google).
Потенциально возможны существенные скидки от партнеров Cisco, но это функция переговоров.
Представлены затраты только на инфраструктурное оборудование с учетом адекватных сервисных контрактов на один год. Дополнительно будут затраты на развертывание сети и интеграцию с существующей инфраструктурой, после доопределения этой части задачи.

Мы рекомендуем проведение радиообследования зоны покрытия, как обязательную часть программы.

Радиообследование (Site Survey) зоны покрытия сети стандарта Wi-Fi.

Проект беспроводной сети Wi-Fi всегда должен включать в себя радиообследование объекта на стадии проектных работ и до начала инстал-

ляции оборудования. Это единственная действительно реальная возможность, при правильном проведении, получить достаточно оснований для создания работоспособного решения беспроводной сети с предсказуемыми характеристиками.

В беспроводных системах очень сложно предсказать распространение радиоволн и определить наличие интерференции без использования тестового оборудования. Даже если вы используете всенаправленные омни-антенны в действительности радиоволны не распространяются на одинаковое расстояние во всех направлениях. Вместо этого различные препятствия, как например стены, двери, лифтовые шахты, люди и т.п. вводят различный уровень затухания сигнала, что является причиной того, что диаграмма направленности радио становится неоднозначной и непредсказуемой. В результате часто необходимо выполнять радиообследование зоны покрытия к сети стандарта Wi-Fi (Site Survey) для полноценного понимания поведения и распространения радиосигналов до начала развертывания Точек Доступа беспроводной сети WiFi.

Основная цель радиообследования (Site Survey) это получение достаточного объема информации, чтобы определить количество и позиции Точек Доступа WiFi для предоставления требуемого покрытия внутри всей целевой зоны. В большинстве случаев требуемое покрытие определяется обеспечением минимальной скорости передачи данных (data rate). Радиообследование также определяет присутствие интерференции идущей от других источников, которая может снизить производительность сети Wi-Fi.

Требования и сложность радиообследования объекта будут варьироваться в зависимости от самого объекта и его характеристик. Например небольшой офис, состоящий из нескольких комнат открытого типа, может вообще не требовать радиообследования. Хотя интерференцию, тем не менее, проверить стоит (полезные приложения для базового анализа частотного спектра). Этот сценарий, вероятно, может быть реализован путем установки одной Точки Доступа WiFi где-то в офисе и можно ожидать, что покрытие для общих задач будет адекватным. Если же Точка Доступа столкнется с интерференцией от БЛВС соседнего офиса, то, вероятнее всего, переход на соседний неперекрывающийся канал может решить проблему. Но живое Радиообследование никогда не надо замещать кабинетной аналитикой даже в случае проектирования небольших сетей.

Большие помещения, такие крупные офисы, жилые дома, больницы, ангары, цеха и пр. обычно требуют детального радиообследования. Без обследования очень вероятно пользователи столкнутся с недостаточным покрытием и будут испытывать проблемы с производительностью сети (пропускной способностью) в некоторых зонах. Определенно вряд ли захочется заново менять места установки нескольких десятков Точек Доступа, а также все их подключения, если возникшая проблема потребует редизайн радиоподсистемы уже после развертывания.

При проведении Радиообследования объекта (Site Survey) для развертывания будущей сети стандарта Wi-Fi можно рекомендовать следующий план действий:

1. Получить план помещения

До начала радиообследования получите план всей территории и зоны покрытия будущей сети стандарта WiFi, включая поэтажные планы Всех помещений, где предполагается иметь покрытие. Если нет ничего доступного, то нарисуйте свой план с размерами и укажите положение всех стен, переходов, окон, лифтов и т.п.

2. Визуально осмотреть весь объект

До начала любых тестов пройдите по всему объекту и проверьте точность планов помещений. Это также хороший момент для выявления потенциальных препятствий, которые могут влиять на распространение радиосигналов. Например, визуальное обследование поможет выявить такие препятствия для радиосигнала, как металлические шкафы и перегородки и т.п., которых обычно нет на плане помещения.

3. Определить места нахождения будущих пользователей сети Wi-Fi

На плане помещения отметьте зоны нахождения пользователей с проводным и беспроводным соединением. Дополнительно проиллюстрируйте где может потребоваться роуминг для беспроводных/мобильных пользователей , а также куда они не ходят. Возможно удастся обойтись меньшим количеством Точек Доступа, если удастся ограничить зоны роуминга или вообще перейти к модели организации «горячих зон» Wi-Fi, а не сплошного покрытия, как представлено в примере тренингового задания сети Кампуса в Wi-Fi-Решебнике на нашем сайте.

4. Определить тип и модель Точек Доступа в будущей сети WiFi

Исходя из первичного полного обследования объекта и собранной информации необходимо определиться с типами Точек Доступа Wi-Fi, Антеннами и т.п. для будущей беспроводной сети. Это может зависеть от большого количества факторов, например: необходимость использования интегрированных антенн, когда есть требования по эстетике; высокие потолки, соответственно решения с внешними антеннами; зоны высокой плотности пользователей, необходимо увеличение емкости путем формирования узких ячеек, соответственно точки с внешними антеннами с узкой диаграммой направленности и т.д..

5. Определить предварительные места установки Точек Доступа WiFi

Предварительно можно оценить местоположение и количество Точек Доступа WiFi для обеспечения адекватного покрытия требуемой зоны путем анализа мест положения пользователей сети WiFi, ожидаемой зоны покрытия и величины ячеек, сервисов на сети и самих элементов радиоподсистемы. Для обеспечения сплошного покрытия необходимо планировать некоторое пере-

крытие ячеек смежных Точек Доступа, но надо помнить, что при назначении каналов для Точек Доступа WiFi (при ручном конфигурировании или при предварительном планировании) Точка с идентичным частотным каналом должна быть достаточно далеко от данной, чтобы отсутствовала или была минимальной интерференция от доходящего излучения через соседнюю Точку Доступа WiFi. Помните, что в частотном спектре WiFi 2.4GHz у нас доступны всего три неперекрывающихся частотных канала 1, 6 и 11. Также стоит добавить, что достаточным уровнем перекрытия ячеек можно считать:
- перекрытие порядка 10-15% при предоставлении сервиса передачи данных, как основной услуги,
- перекрытие порядка 20%, когда на сети предоставляются голосовые услуги VoIP через Wi-Fi,

Хорошим подспорьем в деле предварительного и обоснованного определения положения Точек Доступа может стать специальный программный модуль для планирования сети Wi-Fi. Подобный программный модуль встроен, например, в известную систему управления сети WiFi-стандарта от ***Cisco: Prime Infrastructure***. Кстати, Prime изначально доступен в полноценной демо-версии. В демо-версии это полнофункциональная система управления сети WiFi от Cisco с ограниченным сроком действия. Cisco Prime можно скачать с сайта Cisco для тестов, а позже купить. Или обращайтесь к партнерам Cisco. Некоторые такие компании (Системные Интеграторы), которые имеют соответствующую экспертизу, представлены на нашем сайте. НО это только облегчает проведение радиообследования Не замещая его. С оценкой расположения ТД на плане помещения необходимо проводить обследование и проверять и корректировать рекомендованные положения ТД.

Необходимо выявить подходящие монтажные позиции для инсталляции Точек Доступа, Антенн, кабелей передачи данных и кабелей питания.Также учитывайте необходимость применения различных типов антенн, когда принимаете решение о позиции Точки Доступа WiFi. Например если предполагается монтировать ТД рядом с внешней стеной здания, то в этом случае возможно лучший подход это использование направленной Панельной антенны с относительно высоким усилением внутрь здания. Если предполагается использовать Точки Доступа с интегрированными антеннами, то они часто имеют диаграмму направленности такую что наиболее правильно их располагать на потолке (не за фальшпотолком, а обязательно выступающими внутрь помещения). Естественно в данном случае высота потолков должна быть обычной для обычных офисов. Для помещения с высокими потолками или в цехах/ангарах используйте ТД с направленными антеннами. Некоторые примеры на эту тему рассмотрены в Примере сети Wi-Fi для Кампуса на нашем сайте в Wi-Fi-Решебнике.

6. Проверка мест положения Точек Доступа WiFi и реального уровня параметров сети

Это происходит при начале реальных тестов. Обычно размещается несколько Точек Доступа WiFi в предварительно спланированные позиции на объекте и

проводятся натурные тесты с использованием специализированных инструментов для проведения радиообследования. Например можно порекомендовать посмотреть и использовать инструменты для радиообследования от таких известных производителей как:
- Ekahau, программа: Ekahau Site Survey,
- Fluk/AirMagnet, программа: AirMagnet Survey PRO и т.п.
Очень важно использовать при обследовании именно те модели Точек Доступа и Антенн WiFi, которые впоследствии будут на реальной сети, а также выполнять тесты с учетом самых худших по радиохарактеристикам пользовательских устройств, которые Вы ожидаете увидеть на своей сети. Также очень важно проводить не просто пассивные тесты снимая характеристики именно радиосети, а надо делать Активные тесты с формированием реальной нагрузки от трафика (обычно есть встроенные механизмы в инструменты с активным функционалом радиообследования), т.к. только это проявит реальную картину будущего поведения сети. Очень полезно также иметь в арсенале анализатор спектра для частотных диапазонов WiFi: 2.4GHz и 5GHz. Это позволит выявить и точно представлять себе интерференционную картину в зоне покрытия.

7. Документирование результатов
С того момента, как получены удовлетворительные результаты тестов и определена правильная позиция Точки Доступа и/или антенн необходимо внести эти данные на план объекта.Это потребуется для будущих работ по инсталляции. Также необходимо сохранить и приложить к отчету логи уровней сигналов, скорости передачи данных и т.п. вплоть до ожидаемой границы ячейки каждой Точки Доступа. Это позволит иметь базовую информацию для будущих работ по редизайну сети.
Описаные здесь шаги направят Вас в верном направлении, но реальный опыт не заменят. Если для Вас это первые шаги в направлении WLAN/БЛВС, то имеет смысл обратиться в компании с соответствующей экспертизой. Например многие Системные Интеграторы имеют в своем штате подготовленных сотрудников и смогут провести данные работы на платной основе.

8. Специальный раздел - для тех кто проектирует внешнюю Wi-Fi сеть, например Outdoor Mesh Wi-Fi
Очень важно иметь ввиду следующее:
- еще до проведения Радиообследования надо найти системного интегратора, который знает территорию развертывания сети и имеет специальных людей, которые умеют договариваться с местными административными органами и владельцами недвижимости; также возможен вариант, при котором нанимается на работу или берется на контракт специальный человек, который хорошо знает эту работу и данную территорию (часто из надзирающего за беспроводными сетями органа).
- при проведении предварительного анализа проекта и обработке входных данных на специализированном ПО по дизайну наружных сетей будут опре-

делены предварительные места установки Точек Доступа WiFi. Эти предварительные позиции должны быть очень внимательно проанализированы на предмет реальности установки там Точек Доступа WiFi. Реальность по технической возможности и реальность по административному ресурсу. Например, техническая возможность существует, если для монтажа есть подходящая позиция по высоте, наличию электропитания 24 ч, отсутствию существенных препятствия для распространения сигналов. Например, административная возможность существует, если при развертывании реальной сети, именно на данную по дизайну позицию можно будет инсталлировать и запустить Точку Доступа WiFi (часто возникают сложности при необходимости использования крыш зданий в чужой собственности, а использование элементов недвижимости в коллективной собственности практически нереально - ТСЖ, кооперативные варианты и т.п. -т.к. люди просто боятся радиотехнологий вблизи и не соглашаются на установку оборудования; часто возникают сложности и с фонарными столбами, т.к. их много, но электропитание в основном подается только в вечерне-ночное время, поэтому здесь более реальны, например, светофоры и т.п.).
На данном этапе имеется реальный практический смысл корректировать предварительный дизайн сети до того момента пока предварительные позиции ВСЕХ ТД WiFi будут признаны хотя бы как потенциально реальными для монтажа. Чем более детально и точно будет выполнена данная фаза, тем меньше затрат возникнет впоследствии в условиях развертывания реальной сети и меньше будет необходимо выполнять коррекций в полевых условиях.
-во время проведения полевого Радиообследования при уточнении предварительных позиций ТД Wi-Fi, если возникает необходимость корректирования этих позиций, то все обновленные позиции также необходимо проводить через подробный анализ на возможность последующего развертывания ТД Wi-Fi. В идеале Site Survey в данном случае должен вестись не только с целью обеспечения требований по покрытию и емкости сети, но и с четким фокусом на возможность последующего развертывания Точек Доступа WiFi в спланированных позициях.

Помните простую вещь - чем подробнее и практичнее проведено предварительное проектирование, тем меньше проблем возникнет позже, при строительстве реальной инфраструктуры.