МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Кафедра компьютерных технологий

«Допущен к защите»
Заведующий кафедрой
Куралбаев З.К. профессор
_____ «_____»_____**20__ г.**
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: «Исследование и анализ методов создания и администрирования беспроводной ЛВС ТОО Регион-А»

Специальность «Вычислительная техника и программное обеспечение»

Выполнил Дараев К.А группа ВТу-11-1

Научный руководитель Байжанова Д.О ст.преп.каф.КТ

Консультанты:
по экономической части:
Еркешева З.Д ст. преп.
_____ «20» мая 20 14 г.
(подпись)
по безопасности жизнедеятельности:
Бегимбетова А.С ст.преп.
_____ «28» мая 20 14 г.
(подпись)
по применению вычислительной техники:
_____
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____20___г.
(подпись)

Нормоконтролер: Тусупов Д.М. ассистент
_____ «06» июня 20 14 г.
(подпись)
Рецензент: Байтуленов Жаныбек Бачытович
_____ «_____»_____20___г.
(подпись)

Алматы 2014 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Факультет Информационных технологий

Специальность Вычислительная техника и программное обеспечение

Кафедра компьютерных технологий

ЗАДАНИЕ

на выполнение дипломного проекта

Студент Дараев Калбидин Абдумелитович
(фамилия, имя, отчество)

Тема проекта „Исследование и анализ методов создания и администрирования беспроводной ЛВС Ретон-А"

утверждена приказом ректора № 115 от «24» сентября 2013 г.

Срок сдачи законченной работы «___» _____ 20___ г.

Исходные данные к проекту требуемые параметры результатов проектирования (исследования) и исходные данные объекта

Исследование технологий беспроводных сетей по технологии Wi-Fi

Перечень подлежащих разработке дипломного проекта вопросов или краткое содержание дипломного проекта:

Целью данной работы является разработка проекта сети ТОО „Ретон-А", предоставляющей пользователям мобильный беспроводной доступ к разделяемым ресурсам и возможность выход в Internet.

Перечень графического материала (с точным указанием обязательных чертежей)

1. Зона покрытия ТД
2. Структурная схема ТОО "Регион-Т"

Рекомендуемая основная литература

Консультанты по проекту с указанием относящихся к ним разделов

Раздел	Консультант	Сроки	Подпись
Экономика	Ерешева З.Д.	26.04-30.05.14	Ерешева
БЖД	Балгимбекова А.С.	20.04-20.05.14	
Нормоконтроль	Тусупов Д.М.	06.06.14г.	

Г Р А Ф И К

подготовки дипломного проекта

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления руководителю	Примечание
1	Сбор и анализ данных	3.03 -27.03.14	
2.	Исследование технологии беспроводных сетей.	1.04 -13.04.14	
3.	Анализ существующих сетей и тенденции новых стандартов	19.04 -23.04.14	
4.	Описание сети.	26.04-06.05.14	
5	Экономическое обоснование	28.04.-20.05.14	
6	Безопасность жизнедеятельности	20.03-28.05.14	

Дата выдачи задания «03» марта 2014 г.

Заведующий кафедрой _____ _____
(подпись) (Фамилия и инициалы)

Руководитель Д. Бакен _____
(подпись) (Фамилия и инициалы)

Задание принял к исполнению
студент _____ _____
(подпись) (Фамилия и инициалы)

Аңдатпа

Ұсынылған бітірушіні жұмысы ТОО «Регион-А» WI-FI технологиясын қолданып, жергілікті желіні жобалауға арналған.

Сымсыз байланыс желісі үшін қолданылатын технологияларға шолу жасалып, жергілікті желі құру қарастырылған.

Бітіру жұмысын дайындау барысында радиотрассаның, тура көріністің және Френель зоналарының есептеулері жүргізілген.

Өміртіршілік қауіпсіздігі бөлімінде қауіпті және зиянды өнеркәсіп факторларына және қорғану шараларына талдау жүргізілген.

Бітіру жұмысында экономикалық бөлім қарастырылған.

Аннотация

Данная выпускная работа посвящена разработке проектирования локальной сети с использованием технологии Wi-Fi в ТОО «Регион-А».

Рассмотрен обзор технологий применяемых для беспроводных сетей связи и выполнена разработка структуры локальной сети.

При разработке выпускной работы были выполнены следующие расчеты: расчет радиотрассы, расчет прямой видимости, расчет зоны Френеля.

Были рассмотрены вопросы анализа условий труда работников на предприятии, оценка освещенности, пожарной безопасности, электробезопасности.

В выпускной работе была разработана экономическая часть.

Abstract

This outlet is devoted to develop the design of the local network using Wi-Fi technology in LLP "Region- A".

Considered review of technologies used for wireless communication networks and the development of the structure for local network is made.

In developing the final work were made the following calculations: radio path calculation, calculation of line of sight, the calculation of the Fresnel zone.

Also the questions of analysis of working conditions at the plant, evaluation of the illumination, fire safety, electrical, safety were considered.

In the final work was developed economic part.

Содержание

Введение

В настоящее время, локальные сети (LAN) стали одним из основных общего инструмента или инфраструктура еще можно назвать для проведения бизнес-процессы предприятий, организаций и корпораций. Компьютерные сети, также известный как компьютерных сетей или сетей передачи данных являются логическим результатом соединения двух крупных научно-технических отраслей современной цивилизации - компьютерных и телекоммуникационных технологий. Но все виды сетей, созданная на базе проводных линий связи.

Последние время в большое распространение получил беспроводные сети (Wireless Local Area Network, WLAN), использующие для передачи информации всепроникающие радиоволны.

Wi-Fi - это аббревиатура от Wireless Fidelity, так моделируемой Hi-Fi, называют одним из форматов передачи цифровых данных по радио, или, скорее, стандартный IEEE 802.11, 802.11, или просто. Вообще говоря, ряд 802,11 скрывает целое семейство стандартов, связанных логотип Wi-Fi: 802.11a, 802.11b, 802.11.g и 802.11.n.

Понятно, что для бизнеса или для корпораций vyborp технологии LAN сделать, исходя из целей и задач, потому что цели, компания - не здание самой сети, а также улучшение бизнес. Отсюда стремление минимизировать время и затраты на развертывание сети. Согласитесь, когда на эффективности кола компании в целом, сбережения и платежа стать естественным и снижение затрат - это необходимость. Поэтому, если мы рассмотрим ситуацию, в которой организация является по существу невозможно LAN кабелей, где стоимость прокладки кабельной сети является очень высоким, где скорость является развертывание сети, или нужна полная мобильность, в этой области беспроводных сетей Wi Текстовая нет конкуренции.

В нашей стране, в отличие от западных стран, где локальную сеть, как правило, используются в качестве корпоративных сетей в зданиях, хотя эти сети изначально разработана здания, предоставляя пользователям услуги скорость передачи данных, разбросанных на значительные расстояния. Сегмент WLAN в системе передачи корпоративного трафика мы слаборазвитых, но с каждым годом растет. Из всего вышесказанного, можно утверждать, что эта тема рассматривается в этом проекте на сегодняшний день является актуальным.

Целью данной работы является разработка проекта сети ТОО «Регион-А», предоставляющей пользователям мобильный беспроводной доступ к разделяемым ресурсам и возможность выхода в Internet.

WLAN рассматривается как дополнение к проводным сетям, а не конкурентоспособное решение, поэтому проверьте технология Wi-Fi необходимо в системе координат с учетом уровня Программы по борьбе с Ethernet доступа и функций, которые он выполняет. А если учесть, что сегодня

беспроводные сети активно взаимодействуют с проводной, расширяя их, ТЭО сходимость двух коммуникационных технологий актуальны.

Беспроводные сети имеют, по сравнению с традиционными проводными сетями, большие преимущества, большинство из которых, конечно же, является:

- Простота развертывания.

- Гибкая архитектура сети, когда можно динамически изменять топологию сети при подключении или отключении движение мобильных пользователей без значительной потери времени.

- Быстрая разработка и внедрение, что очень важно при жестких требованиях по времени сети.

- Кроме того, беспроводная сеть не требует кабелей часто требующий сокрушительные стены.

В то же время, беспроводные сети на современном этапе их развития не лишены серьезных недостатков. Прежде всего, это зависимость от скорости соединения и диапазон от того, препятствия и расстояние между передатчиком и приемником. Одним из способов увеличения диапазона беспроводной сети представляет собой распределенную сеть через несколько точек доступа, подключенных друг с другом. Создание таких сетей есть возможность превратить здание в единый покрытия беспроводной сети и увеличить скорость соединения вне зависимости от количества стен и других препятствий. Точно так же, решена проблема масштабируемости сети, а использование внешних направленных антенн позволяет эффективно решать проблему препятствий, ограничивающих сигнал.

1 Беспроводные Локальные Сети

1.1 Технологии локальных сетей

Сети WLAN, так же известный "беспроводные Ethernet", или Wi-Fi (от WirelessFidelity - высокая точность воспроизведения с использованием беспроводной технологии), с каждым годом становятся очень популярными потому, что они могут работать параллельно вмести проводными сетями Ethernet. Поэтому, мы прежде чем внимательно расмотрим беспроводную сеть Ethernet, имеет смысл сделать обзор , идля проводной технологии Ethernet. Чтобы лучше понять, где мы сейчас находимя и куда нужно идти.

Можно сказать, что в иерархии сетей выдиляется три логических уровня.

Уровень доступа (accesslayer), на котором происходит соединение конечной станции со сетью.

Уровень распределения (distributionlayer) - сегменты сетей определенного широковещательного домена уровня 2, которая ограниченно маршрутизаторами, или уровня 2, ограниченного коммутаторами. Службы сети, такие как списки контроля доступа, фильтрация маршрута (routefiltering) и трансляция сетевых адресов, которая работает именно на уровне распределения.

Базовый уровень (corelayer) работать для максимально быстрой пересылки фреймов между уровнями распределения. Не стоит искать на этом уровне какие-либо службы, потому что для большинства сетевых сервисов нужны уже обработанные фреймы или пакеты, которые вступают в коллизии на всем "протяжении" уровня. Базовый уровень может быть являться или уровнем 2 (несегментированный уровень), или уровнем 3.

Хотя технологии Ethernet применимы на любом из перечисленых уровней, мы посмотрим в основном их работу на уровне доступа и особенно специфику данного семейства Ethernet 802.3. Любой сетевой стандарт хорош когда работает в изолированной однородной среде. Как правило, вомногих сетей работаются разные топологии. Сети стандарта Ethernet 802.3 используюся с помощью мостов или маршрутизаторов в сети стандарта TokenRing 802.5, сети стандарта ANSIX3T9 FDDI работается с помощью мостов или маршрутизаторов в сети FastEthernet 802.3 и т.д.

Кадр Ethernet имеет формат, показанный на рисунке 1.1 (цифры в верхней части рисунка показывают размер поля в байтах).

Рисунок 1.1 - Формат кадра сетей Ethernet.

Поле преамбула служит для стабилизации и синхронизации (последовательность байтов вида 10101010), далее следует поле SFD, которое предназначено для выявления начала кадра (последовательность 10101011). Любому пользователю доступны поля, начиная с адреса получателя и кончая полем информация, включительно. EFD поле задает конец кадра. CRC поле контрольной суммы, также как и преамбула, SFD и EFD, формируются и контролируются на аппаратном уровне. В некоторых измодификаций протокол EFD поле не используется.

Ethernet адреса представляют собой 48-разрядные значения, который однозначно идентифицируют Ethernet-станции локальной сети (MAC-адресация). MAC-адреса вомногих случаев представляются в шестнадцатеричной форме, причем каждый байт отделяется дефисом или двоеточием, либо каждые два байта отделяются точкой.

Ethernet стандарт, регламентирующий его работу, основанной архитектуре Carrier Sense Multiple Access with Collision Detection (CSMA/CD). Это полудуплексная архитектура, что передает информацию в тот или иной момент времени только для одной станции. Ответственный за контроль несущей части CSMA/CD опирается на возможность станций определять, в данный момент работается ли среда Ethernet. На самом деле никакого сигнала несущей нет, поэтому в действительности станции выявляют отсутствие сигнала, это означает , что среда передачи свободна. Часть CSMA/CD, относящаяся к множественному доступу, опирается на возможность среды быть доступной одновременно для многих пользователей. Все станции одинаково имеют возможность доступа к среде, но им нужно ждать, пока среда передачи не освободится. Поскольку число станций, использующих Ethernet, возрастает, повышается и вероятность возникновения коллизий фреймов. Когда две станции пытаются одновременно передавать информацию через одну и ту же среду возможно возникновение коллизия. Данные, который переданный как одной, так и другой станцией, нельзя работать, поэтому станция повторно передает информацию. И наконец, обнаружение коллизий является доказательством возможности станций выявлять возникновение коллизий. Технология Ethernet предоставляет эффективный механизм повторной передачи для станций, переданные фреймы которых подверглись коллизии [1].

Диаметр сети определяется расстоянием между Ethernet-станциями, расположенных на максимально удаленных (противоположных) сторонах широковещательного домена. Эти устройства могут быть соединены с использованием хабов, повторителей, коммутаторов или мостов. Правила, установленные для сетей Ethernet стандарта 802.3, требуют, чтобы коллизия была обнаружена в течение времени, которое необходимо для передачи наименьшего по длительности фрейма, допустимого в сети Ethernet. Размер наименьшего допустимого фрейма является 64 байт, или 512 бит. С учетом скорости передачи электрического сигнала по проводам и скорости передачи данных (10 Мбит/с) получаем, что максимально допустимая длина провода в сетях Ethernet составляет 2800м. Интервалом Ethernet (slottimeEthernet)

называется время, необходимое фрейму Ethernet для преодоления диаметра сети.

Станция может адресовать передаваемые фреймы 3 способами.

- Широковещательная адресация. Станция направляет фрейм для всем станциям широковещательного домена.
- Много адресатная или групповая рассылка. Станция адресует свои фреймы части (подмножеству) станций широковещательного домена, входящих в предварительно определенную группу.
- Одно адресатная рассылка. Станция адресует свои фреймы одному определенной станции.

Ethernet предлагает все 3 метода адресации, благодаря чему приложения могут использовать наиболее удобный для них метод, и тем самым снижать нагрузку на сеть.

В качестве разделяемой среды Ethernet использует кабельные линии стандартов 10Base2, 10Base5, 10Base-T и 10Base-FL. Каждый из вариантов Ethernet имеет преимущества и недостатки по сравнению с другими типами.

1.1.1 Технология FastEthernet

Тем больше Ethernet становился все более востребованным стандартом передачи данных в сетях, пользователи начинали требовать расширения полосы пропускания. Чтобы успокоить массы, в 1995 году IEEE анонсировала стандарт 802.3u, которая была необходима для продвижения Ethernet со скоростью 100 Мбит/с. Хотя уже существовала несколько решений для передачи данных со скоростью 100 Мбит/с, наибольшее распространение получили два из них: 100Base-TX (две неэкранированные витые пары) и 100Base-FX (оба называются стандартом 100Base-X). Технология 100Base-X создалось на разработанном не организацией IEEE стандарте FDDI, ставшим стандартом де-факто еще до появления FastEthernet и имевшим ряд преимуществ перед обычным Ethernet [3].

Диаметр сети и интервал FastEthernet отличаются от таковых для Ethernet 10 Мбит/с. Интервал Ethernet ограничивается максимальным диаметром сети с условием, что диаметр не должен превышать расстояние, которое преодолеет 512-битовый фрейм, прежде чем станция передающаюся закончит его передачу. Система FastEthernet поддерживает 512-битовый размер фрейма, так же обеспечевает обратное совместимость с предыдущим поколением систем Ethernet .

Для Ethernet сетей максимальное значение диаметра составляет 2800 м. В случае 100Base-TX операция передачи заканчивается в 10 раз быстрее, чем требуется для ее проведения станциями Ethernet. Естественно, для того чтобы передающая станция успела обнаружить коллизию в ходе передачи 512-битового фрейма, он не должен пройти более чем одну десятую пути, характерного для Ethernet. Этот предел является тем фактором, что снижает диаметр сети приблизительно до 200м. Такое сокращение допустимого

расстояния не создает большую проблему, поскольку в большинстве систем FastEthernet используется технология 100Base-TX, для которой максимальное расстояние составляет лишь 100 м.

Технология 100Base-FX является разновидностью технологии 100Base-TX, в котором использует для передачи данных многомодовое оптическое волокно. Сетевая карта преобразует электрические сигналы в световые импульсы, которые передаются по волокной сетевой карте для приемной станции. Принемающая сетевая карта осуществляет обратное преобразование световых импульсов в электрические сигналы, которые и обрабатывает станция-приемник.

В полудуплексном режиме работы диаметр сети для технологии 100Base-FX составляет примерно 400м. Так же в сетях на основе 100Base-FX можно работать полнодуплексный режим. Такой режим работы дает возможность принимать и передавать сигналы одновременно, благодаря чему более полно используются возможности среды передачи. Пример работы в полнодуплексном режиме изображен на рисунке 1.2. Коллизия не возникает при работе в полнодулексном режиме, поэтому максимальное расстояние может довольно сильно превышать 400м.

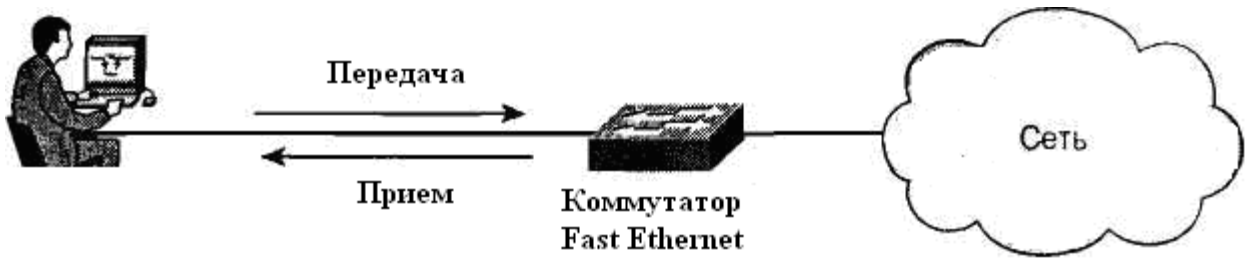


Рисунок 1.2 - Работа в полнодуплексном режиме.

1.1.2 Технология GigabitEthernet

В результате перехода от Ethernet к FastEthernet пользователи получили более широкую полосу передачи сигналов, как минимум в десятки раз. GigabitEthernet, со скоростью 1000 Мбит/с, предлагает столь же резкий переход для пользователей. GigabitEthernet имеет две основные разновидности:

- 1000Base-T. Как и технологии 10Base-T и 100Base-TX, основном работает кабели с неэкранированными витыми парами длиной не более100м.

1000Base-Химеет три варианта:

- 1000Base-SX. Волоконно-оптическая среда передачи на основе стандартны многомодовых волокон, предназначенная для работаты на небольшие расстояния (до 200м).
- 1000Base-LX. Волоконно-оптическая среда передачи на основе

одномодовых волокон, предназначенная для работаты на расстояниях до 10км, а в некоторых исключениях допускается использование многомодовых волокон.

- 1000Base-CX. Экранированная медная среда, работаться в случаях для небольших расстояний между устройствами. 1000Base-CX применяется при расстояниях не более 25м.

С диаметром сети в GigabitEthernet появляются проблемы, которая была у Ethernet. При работе в полудуплексном режиме действует правило Ethernet относительно 512-битового фрейма. Если следовать этой методологии, то максимальная длина кабелей в системах 1000Base-T и 1000Base-X была бы ограничена значением 20м. Кабелей длиной 20м совершенно недостаточно для большинстве ситуаций, поэтому, для того чтобы увеличить названный предел, IEEE потребовал для GigabitEthernet увеличения минимального размера фрейма в 8 раз - до 4096 бит (512 байт). Вместо того чтобы "набивать" полезную часть фрейма бесполезной информацией, этот стандарт вел новую характеристику, получившуюся название расширение несущей (carrierextension).

Предположим, например, что GigabitEthernet-станция выявляет, что среда передачи свободна и пытается передать 512-битовый фрейм. И сетевая плата добавляет к концу фрейма расширение, состоящее из 3584 бит. Для остальным станциям GigabitEthernet известно, что эти биты не несут какой-либо информации, однако считаются частью фрейма. Когда станция-приемник получает такой фрейм, она отбрасывает расширение несущей.

Метод расширения несущей конечно решает проблему диаметра сети, однако он так же создает новую проблему. Для каждого переданного фрейма размером 512 бит передаются также в 7 раз более многочисленные биты расширения несущей. И потому для снижения "накладных расходов" стандарт предписывает в качестве дополнительного работать пакетный режим (burstmode), который решает эту маленькую проблему диаметра сети и неэффективного работы полосы пропускания. Расширение несущей и метод пакетирования нужно применять только при работе в полудуплексном режиме. При работе в полнодуплексном режиме станциям не приходится конкурировать за контроль над средой передачи, поэтому не приходится волноваться об интервале Ethernet и о связанном с ним минимальном размере фрейма.

Поскольку при работате Ethernet есть вероятность многочисленные комбинации скоростей передачи и дуплексных режимов, для оценки совместимости используемых устройств был предложен способ автоматического согласования. Если честно, способ согласования скоростей и дуплексных режимов был разработан для среды передачи "витая пара", поскольку устройства, ориентированные на работу волоконной оптики, не поддерживают автоматическое согласование; это относится ко всем типам волоконно-оптической среды передачи.

Ethernet все время развивается, стараясь удовлетворить новые требования, предъявляемым к ней пользователями и администраторами сетей. Она продолжает развиваться и после появления GigabitEthernet.

Самая интересная особенность проекта 10 GigabitEthernet - это то, что это первая технология для Ethernet, которая специально было создана сдля того, чтобы выйти за рамки локальных вычислительных сетей.

Первое время продукты на базе 10 GigabitEthernet стоило крайне дорого. У некоторых производителей (сейчас в число крупнейших поставщиков оборудования 10 GbEthernet входят Cisco Systems, Enterasys Networks, Extreme Networks, Foundry Networks, Nortel Networks и Force10 Networks), к примеру, цена за порт составляла около $100 тыс. На сегодняшний день цена изделий значительно уменьшилось, но при этом все равно осталось довольно высокой по сравнению со стоимостью оборудования FastEthernet и GigabitEthernet.

Каждая топология находит свое место при проектирование сетей, должна удовлетворять таким параметрами, как стоимость, высокую скорость передачи данных, протяженность и уже имеющаяся кабельная проводка. Для проводного Ethernet, как обычно характерна обратная совместимость, благодаря чему новые топологии появляются, улучшаются и получают статус стандарта. В таблице 1.1 приведены основные характеристики сетей семейства Ethernet.

Т а б л и ц а 1.1 - Основные параметры семейства Ethernet

Параметры	Ethernet	FastEthernet	GigabitEthernet	10 GigabitEthernet
Скорость передачи, Мб/с	10	100	1 000	10 000
Метод доступа к среде	CSMA/CD	CSMA/CD	CSMA/CD	-
Физическая среда	коаксиал / медь / оптика	медь / оптика	медь / оптика	оптика
Режим передачи	полудуплексный	полудуплексный / полнодуплексный	полудуплексный / полнодуплексный	полнодуплексный
Мин. размер кадра, бит	512	512	4096	4096
Макс.диаметр сети	2800	200 (полудупл.)	200 (полудупл.)	-
Макс. протяженность среды, м: - коаксиал - медь - оптика	 185 / 485 100 2000	 - 100 400 / 2 000 (полнодупл.)	 - 100 до 10 000 (полнодупл.)	 - - до 10 000

1.2 Общие сведения о WLAN

WLAN- это беспроводная сеть которая исключает колизии. На данный момент технология WLAN получило большое распростроннение, по причине того что почти у каждого жителя планеты имеется смартфон. Так же к плюсам системы WLAN можно отнести:

- Полная мобильность (доступ к нужной информации независимо от местоположения).
- Гибкость конфигурации (поддержка разных режимов организации сети).
- Подключение к сетям Ethernet/FastEthernet (возможность взаимодействия беспроводных рабочих станций с уже существующей сетью Ethernet).
- Простота расширения сети (добавление беспроводных рабочих станций без ухудшения производительности сети).
- Поддержка роуминга.
- Беспроводный доступ в Интернет.
- Соответствие стандартам.

Несмотря на все достоинства, WLAN-сети обладают рядом недостатков, главный из которых - безопасность, которая остается желать лучшего, даже когда данные передаются не по проводам.

WLAN- является качественной радиосвязью обеспечивающее скоростной передачи данных до 100mb\s. В качестве узла сети может выступать как отдельный компьютер, ноутбук или PDA, так специальный устройство "точка доступа" или "AccessPoint" - обеспечивающее доступ к кабельному сегменту сети Ethernet, к Интернету или другому компьютеру.

Все специальные стандарты для WLAN-сетей разрабатываются институтом инженеров по электротехнике и электронике (Instituteof Electricaland Electronics Engineers), которые более известного под аббревиатурой IEEE. Их ний первый стандарт IEEE 802.11 для беспроводных локальных сетей был принят в 1997 году. Он подразумевал работу оборудования на частоте 2.4ГГц, их скорости составляла 1 и 2 Мб/с. Стандарт разрабатывался около 7 лет и поэтому ко времени его принятия уже не мог соответствовать выросшим потребностям. Независимая международная организация Wi-FiAlliance (Wi-Fi- сокращение от WirelessFidelity), была создана в 1999 году и занимается сертификацией на совместимость WLAN-устройств от различных производителей. Эта организация объединяет практически всех ведущих производителей Intel, IBM, Cisco, HP, Dell, D-Link и многих других. В сейчас в нее входят более 200 компаний, и уже более 1500 устройств получили сертификат Wi-Fi с момента начала сертификации в марте 2000 года. На рисунке 1.3 представлена эволюция стандарта Wi-Fi (802.11).

Рисунок 1.3 – Эволюция стандарта Wi-Fi (802.11)

1.2Беспроводные (радио) каналы и системы

В настоящее время существует следующая классификация беспроводных систем который связано по скорости передачи информации в канале, которая показана на рисунке 1.3.

Применение электромагнитных волн для телекоммуникаций имеет более столетнию историю. Спектр работаты волн делится на ряд диапазонов, показаных в таблице 1.2.

Так же следуют диапазоны видимого света, ультрафиолета, рентгеновских и гамма-лучей. Диапазоны часто, работает разными каналами связи показаны на рисунке 1.4 .

Т а б л и ц а 1.2- Основные диапазоны используемых в радиоканалах волн

Номер	Название диапазона	Частота	Длина волны
1	Высокочастотный	3 – 30 МГц	100 – 10 м
2	VHF	50 - 100 МГц	6 - 3 м
3	УВЧ (UHF)	400-1000 МГц	75-30 см
4	Микроволновый	$3\ 10^{9} – 10^{11}$ Гц	10 см – 3 мм
5	Миллиметровый	$10^{11} – 10^{13}$ Гц	3 мм – 0,3 мм
6	Инфракрасный	$10^{12} – 6\ 10^{14}$ Гц	0,3 мм – 0,5 мкм

Рисунок 1.4- Классы беспроводных систем передачи данных

Например, наша местная радиостанция АМ-диапазона (средние и длинные волны) может вести вещание на частоте 1290 кГц, поскольку интервал частот для широковещания с амплитудной модуляцией составляет 535-1605 кГц. И интервал частот для FM-вещания (УКВ) имеет значение 88-108 МГц. А инфракрасные системы передачи данных основаны на известном принципе передачи информации с помощью света с длиной волны инфракрасного диапазона (около 1000 нм). Воздушное пространство работет как среда для передачи данных. Связь на основе инфракрасного излучения не стандартизована, и каждый производитель самостоятельно разрабатывает способы передачи данных. Показан диапазон сигналов на рисунке 1.5.

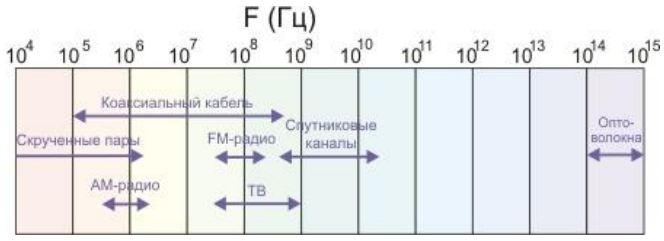


Рисунок 1.5- Диапазоны частот различных телекоммуникационных каналов

Направленные лазерные системы были разработаны на основе инфракрасных лазеров первого или второго класса предназначены для передачи данных. Эти системы обычно работают только при условиях прямой видимости и средне континентальном климате. Средняя дальность между станциями связи 500-1000 метров. Отдельные образцы оборудования могут работать на более больших расстоянии до 4 км. Дальнейшее развитие по увеличению расстояния практически невозможно из-за непредсказуемого преломления света воздухом по причине температурного градиента воздушной среды (глазом это можно наблюдать как мерцание огней ночью).

Такую проблему возможно частично решить, с помощью продублированного канала передачи данных, так как вероятность

одновременного преломления света в двух достаточно разнесённых точках мала. Подобную иллюстрирует показана рисунок 1.6. Ограничивающим фактор является климата, так как при дожде, снеге или тумане самое максимальное расстояние для связи обычно не превышает 500 метров. Еще своё влияние так же оказывают и птицы, вносящие около 0,1% искажений. У такого метод связи есть свое примущество: поддержка скоростей доступных оптоволоконным линиям связи, возможность размещения любого количества устройств без пагубного взаимовлияния.

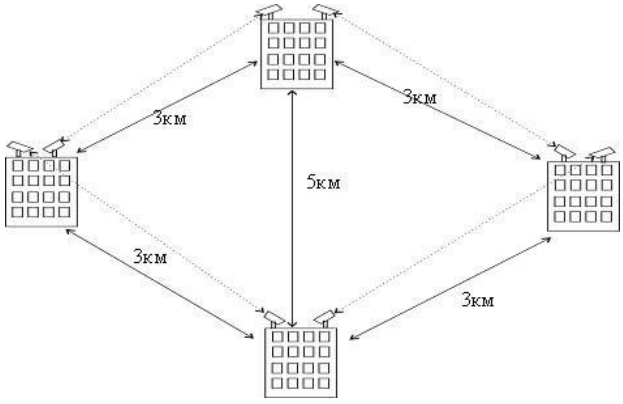


Рисунок 1.6- Пример дублирования канала в целях улучшения качества

В наше время большинство оборудование разработано для сетей Ethernet 10 Мб/с, но есть и устройства, работающие на скорости до 100 Мб/с. С точки зрения медицины инфракрасные лазеры применяемых длин волн и мощности (до 0.1 Вт) является безопасны для человека. Из-за того что всё излучение поглощается роговицей глаза и не достигает сетчатки. По защите канала от нелегального подключения воздушный канал превосходит оптоволоконную линию, но из-за необходимости прямой видимости оборудование размещаются на крышах зданий или мачтах, а подключение устройств к компьютерам производится по коаксиальному кабелю либо витой паре, что ухудшает показатели защиты передачи данных. Такой вид связи может поддерживать только соединение типа точка-точка, и для реализации полноценных сетей необходимо дополнительное оборудование либо объединение с другими способами передачи данных.

Диффузионные светодиодные системы может работает аналогично пультам дистанционного управления бытовой техникой. Эти системы передачи данных работется в одной комнате в пределах до 20 метров, излучение в диапазоне длин волн 850 - 950 нм. Скорость передачи в этой системе не превышает 4 Мб/с. Такая малая скорость обусловлена быстродействием светодиодов. Причём 4 Мб/с это скорость, которая должна делится между всеми абонентами сети. Эти сети очень требовательны к параметрам комнаты: цвет стен пола и потолка, количество объектов в комнате, тип и количество светильников. Такие ограничения очень сужают область применения диффузионных беспроводных систем передачи данных.

Так как инфракрасный свет всегда должен иметь или прямой или отраженный путь между передатчиком и приемником, инфракрасные сигналы не могут проходить через преграду типа стены или двери. Чтобы достигнуть всех приемников в комнате инфракрасному сигналу нужно разработать различные методы. Один из метод состоит в том, чтобы разместить все передатчики и приемники выше, чем приблизительно 2.5 метра, чтобы избежать интерференции от большинства мебели в офисе. Все передатчики должны быть направлены к приемникам, чтобы улучшить прием, но прямая видимость не является необходимой. Но этот - метод основной который работает для построение связи. Второй метод состоит в том, чтобы направить все сигналы непосредственно на потолок, как показано на рисунке 1.7.

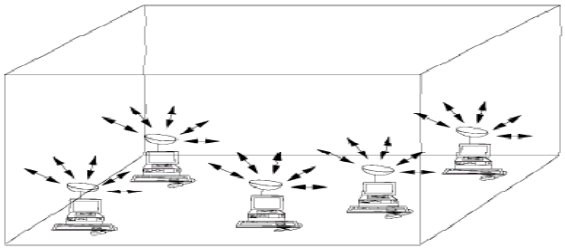


Рисунок 1.7- Диффузионная сеть

Передатчик посылает сигнал и после этого происходит отражений от стен и потолка, сигнал достигает приемника с различных направлений под различными углами. Но такое построение приводит к ограничению на скорость передачи из-за многократного отражения и наложения сигнала, что вызывает сильное искажения сигнала. Третий метод заключается в размещении в центре потолка ретранслятора, который может быть активным или пассивным. Таким образом, на передатчики направляются достаточно узкий луч на ретранслятор, который отражает его в нужном направлении либо обрабатывает его, подобную схему иллюстрирует рисунок 1.8.

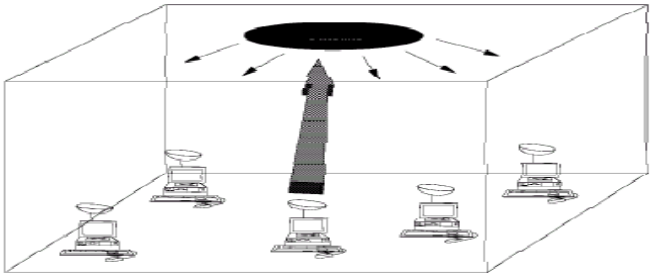


Рисунок 1.8- Инфракрасная сеть с ретранслятором

.

Для охвата большой территории нужно разработать несколько ретрансляторов, в том числе и связанных. Много путевая дисперсия - не вызывает проблемы для пассивных или активных ретрансляторов, так как

сигнал принимается только непосредственно от ретранслятора, а не от стен или потолка.

Радиосистемы передачи данных можно разделять по способу модуляции на узкополосные и широкополосные. Узкополосные способы модуляции нужно использовать минимальное необходимой ширины полосы радио спектра. Вся мощность передатчика должна быть направлена на превышение уровня шума. Такие системы позволяют нам чётко планировать радиочастотный спектр, и позволяют в определённой мере компенсировать многолучевое распространение радиовол, что очень важно особенно в городских условиях, работает длины волн не критичных к большинству препятствий и не требующих прямой видимости, и которая поддерживают работу при достаточно высокой дальности. К недостаткам можно отнести низкую помехозащищённость, очень низкую степень защиты от нелегального подключения, довольно таки низкую скорость передачи данных. Можно повысить скорости передачи данных за счёт перехода в диапазон выше 10 ГГц, это позволит оперировать скоростями от 2 Мб/с.

Широкополосные системы передачи данных - это новая в коммерческой связи очень бурно развивающаяся технология передачи информации на основе работает шум подобных сигналов (ШПС). Системы с ШПС известны очень давно, однако, ранее они использовались и работается сейчас почти исключительно для военных и научных целей.

ШПС спроектированы с целью минимизации средней мощности для любой данной частоты, а также для повышения его надёжности, передачи данных за счёт увеличения избыточности. Полезная информация как бы "размазывается" по частотному диапазону, существенно более широкому, чем при традиционных способах модуляции сигнала (в 10-1000 раз). Возможно осуществить это за счет перемножения последовательности полезных битов информации на псевдослучайную последовательность более коротких импульсов. В результате можно получить сигнал, который занимает больший частотный диапазон и имеет значительно меньшую интенсивность, чем получаемый при узкополосной модуляции. Узкополосная помеха иммет возможность «испортить» широкополосный сигнал только в каком-то относительно узком частотном диапазоне, но полезная информация может быть восстановлена по неповрежденным участкам несущего диапазона. Конечно, такой сигнал несколько ухудшается, однако это несопоставимо с потерями качества связи при работе с обычными методоми модуляции.

Ясно, что в этом случае можно принять информацию, только зная последовательность, на которую должен быть перемножен полезный сигнал при передаче, - в противном случае он будет выглядеть как шум (отсюда и название). Данный метод используется обычно в военных приложениях в первую очередь для защиты от помех (широкополосный сигнал очень устойчив к узкополосным помехам) и подслушивания. Для нас же сейчас более важно следующее: два абонента, находящиеся в одной зоне действия и работающие на общей частоте, но с разными кодирующими последовательностями,

практически не будут создавать помех друг для друга.

Широкополосные системы передачи данных (ШСПД) подчиняются в части протоколов единому стандарту IEEE 802.11 и CDMAIS-95, а в радиочастотной части - единым правилам FCC (Федеральной комиссии США по связи). Однако при этом они сильно отличаются друг от друга способом и скоростью передачи данных, типом модуляции, дальностью передачи, сервисными возможностями и так далее. Все эти характеристики играют огромное значение при выборе ШСПД, и элементной базы (разработчиком, производителем систем связи).

ШПС делятся на две технологий DSSS (расширение спектра путём прямой последовательности) и HSS (расширение спектра путём частотного перемежения). Данные технологии передачи сигнала на физическом уровне будут изложены при рассмотрении базового стандарта IEEE 802.11.

Если не работается направленная антенна и на пути нет препятствий, радиоволны распространяются по всем направлениям равномерно и сигнал падает пропорционально квадрату расстояния между передатчиком и приемником (удвоение расстояния приводит к потерям 6дБ). Радио каналы для таких целей передачи информации работает в частотным диапазоне 902-928 МГц (расстояния до 10 км, пропускная способность до 64кбит/с), 2,4 ГГц и 12 ГГц (до 50 км, до 8 Мбит/с). Они работаются обычно там, где не существует кабельных или оптоволоконных каналов, или их создание по каким-то причинам невозможно или слишком дорого. Более низкие частоты (например, 300 МГц) менее привлекательны из-за ограничений пропускной способности, а большие частоты (>30 ГГц) работоспособны для расстояний не более или порядка 5 км из-за поглощения радиоволн в атмосфере. При работе диапазонов 4, 5 и 6 следует знать, что любые препятствия на пути волн приведут к их практически полному поглощению. Для этих диапазонов большое влияние оказывает и поглощение в атмосфере, где значительную роль в поглощении радиоволн играет вода атмосфере. И по этому сильный дождь, град или снег могут привести к прерыванию связи.

Мощность этого передатчика обычно лежит в диапазоне 50 мВт - 2 Вт. Модемы, как правило, обычно работается шум подобный метод передачи SST (spreadspectrumtransmission). Для устройств на частоты 2.4 ГГц и выше, как правило, обычно работается направленные антенны и необходима прямая видимость между приемником и передатчиком. Такие каналы чаще работают по схеме точка-точка, но можно реализовать и многоточечного соединения. На аппаратном уровне здесь можно разработать радиорелейное оборудование радиомодемы или радио-бриджи. Схема этих устройств имеет много общего, пример такой схемы показан на рисунке 1.9. Отличаются они только сетевым интерфейсом. Антенна служит как для приема, так и для передачи. Трансивер (приемопередатчик) обыно может соединяться с антенной через специальные усилители. Между трансивером и модемом может включаться преобразователь частот. Модемы подключаются к локальной сети через последовательные интерфейсы, для многих модемов такие интерфейсы являются встроенными.

Отечественное радиорелейное оборудование имеет в качестве выходного интерфейс типа G.703 и по этой причине нуждается в адаптере. Радио-бриджи есть встроенный Ethernet-интерфейс. Длина кабеля от модема до трансивера обычно лежит в пределах 30-70м, а соединительный кабель между модемом и ЭВМ может иметь длину около 100-150м. Трансивер располагается обычно рядом с антенной.

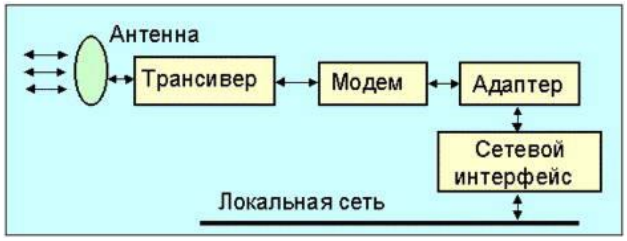


Рисунок 1.9- Схема оборудования радиоканала передачи данных

Подключение всех объектов к центральному узлу осуществляется по звездообразной схеме. Значительное влияние на конфигурацию сети оказывает ожидаемое распределение потоков информации. Если все объекты, подключенные к узлу, примерно эквивалентны, а ожидаемые информационные потоки не очень велики, можно в центральном узле обойтись простым маршрутизатором, имеющим достаточное число последовательных интерфейсов. Применение радио-бриджей особенно выгодны для организаций, имеющих здания, отстоящие друг от друга на несколько километров.

Микроволновые (СВЧ) технологии может применяться для связи на больших расстояниях и могут обеспечить сетевые коммуникации между континентами через спутники. Сети на базе низкоорбитальных спутников являются еще одной из разновидностью беспроводных сетей, на основе которых в определенный момента может быть создана "всемирная сеть", доступная во всех точках планеты. Эти каналы работаются диапазоны перечисленные в таблице 1.3.

Т а б л и ц а 1.3- Частотные диапазоны, используемые для спутниковых телекоммуникаций

Диапазон	Канал снижения (downlink), ГГц	Канал подъема (uplink), ГГц	Источники помех
C	3,7-4,2	5,925-6,425	Наземные помехи
ku	11,7-12,2	14,0-14,5	Дождь
ka	17,7-21,7	27,5-30,5	Дождь

1.3 Беспроводные локальные сети стандарта IEEE 802.11

1.3.1 Базовый стандарт IEEE 802.11

Стандарт IEEE 802.11 является базовым стандартом и обычно определяет протоколы, необходимые для организации и создание беспроводных локальных сетей. Основные из них является протокол управления доступом для среды MAC (Medium Accsess Control- нижний подуровень канального уровня) и протокол PHY, которая работет для передачи сигналов в физической среде. В качестве последнего из этих методов допускается работа радиоволн, а так же инфракрасное излучения. На рисунке 1.10 показана алгоритмическая структура радиосети стандарта 802.11.

Стандарт 802.11 работает по методу прямой последовательности (Direct Sequence Spread Spectrum, DSSS), а так же по метод частотных скачков (Frequency Hopping Spread Spectrum, FHSS). Эти методы кардинально отличаются, и несовместимы друг с другом.

Рисунок 1.10- Алгоритмическая структура беспроводной сети стандарта 802.11

При работе этим методом частотно скачковых полоса 2,4 ГГц будет делится на 79 каналов по 1 МГц. Отправитель и получатель согласовывают между мобой схему переключения каналов (на выбор имеется 22 таких схемы), и эти данные будут посылаются последовательно по разным каналам с работающийся по этой схеме. Каждая передача этих данных в сети 802.11 работае по разным схемам переключения, а сами схемы были разработаны таким образом, чтобы минимизировать шансы того, что эти два отправителя будут работать один и тот же канал одновременно.

Метод FHSS может позволяет работать эту простую схему приёмопередатчика, однако он имеет ограничен максимальной скоростью 2 Мбит/с. Это ограничение было вызвоно тем, что канал связи выделил 1 МГц, что заставило FHSS системы использовать весь диапазон 2,4 ГГц. Это означает, что должно происходить частое переключение каналов (например, в США установлена минимальная скорость 2,5 переключения в секунду), что, в свою очередь, приводит к увеличению этих накладных расходов. Данный метод

иллюстрирует рисунок 1.11.

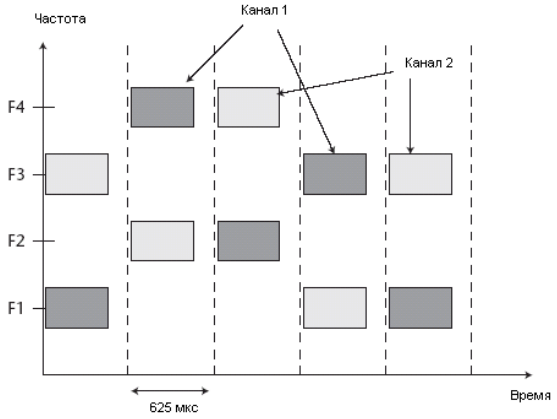


Рисунок 1.11- Расширение спектра методом частотных скачков

Метод DSSS делит полосу частот 2,4 ГГц на 14 перекрывающихся каналов . Для того чтобы более каналов могут работать одновременно в одном месте , необходимо, чтобы они разнесены на 25 МГц , и она должна predatvrascheniya помех. Таким образом, в одном месте может одновременно обрабатывать максимум трех каналов . Данные , использующие этот один из этих каналов без переключения на другие каналы . Чтобы компенсировать нежелательные фоновые шумы , работет 11 - немного последовательность Bracker , и каждый бит пользовательских данных должны быть преобразованы в 11 -разрядные данные, передаваемые . Такое большое резервирование для каждого бита дает нам возможность значительно повысить надежность его данным, в то время как довольно снижения мощности передаваемого сигнала . Даже если часть этого сигнала , будут потеряны при передаче в большинстве случаев все равно будет восстановлен . Это сведет к минимуму количество его повторных передач данных.

В основном поддерживается передачи двухскоростной данных - 1 и 2 Мбит / с. В потоке 1 Мбит / сек данных мы разделим квартетов , и каждый из них затем кодируется в один из 16 импульсов , и будет работать фазовый сдвиг двоичного манипуляции diffentsialnaya Дифференциальный двоичная фазовая манипуляция (DBPSK). 2 Мбит / с немного способ модуляции отличается тем, что - поток данных делится на битовых пар, каждая из которых является то, что мы модулировать один из четырех импульсов представляет собой так называемый дифференциальный квадратурной фазовой манипуляции Дифференциальный квадратурная фазовая манипуляция (DQPSK) . Самая большая мощность передаваемого сигнала будет 2 Вт .

802.11 Канальный уровень состоит из двух подуровней : управление логическим каналом (LogicalLinkControl , ООО) и контроля доступа к средствам массовой информации (MediaAccessControl , MAC) . В работе того же 802,11 ООО и 48 - битной адресации , как другие сети 802 , что позволит нам легко интегрировать беспроводные и проводные сети , но слой MAC имеет

китайско различия. Как правило, слой MAC знает, алгоритмы и структуру кадра доступа к каналу , передаваемые на этом уровне. Уровень MAC 802.11 кадров обычно работает три категории :

- Кадры управления (controlframes) . Способствует передавать кадры данных при нормальном обмене информацией станций 802,11 .

- Утилиты кадры (managementframes). Мы предоставляем подключение к беспроводной ЛВС , аутентификацию , и показывают состояние.

- Кадры Данных (dataframes) . Отправка данных от передатчика к приемной станции .

Все кадры 802,11 давольно очень похожие на основной раме стандарта . Вызывается все виды трения и расширить рамки работы конкретных областей основной рамы MAC для своих собственных целей . На рисунке 1.12 показаны основные кадры и поля MAC .

Контроль фрейма	Продолжительность/ID	Адрес 1	Адрес 2	Адрес 3	Управление очередностью	Адрес 4	Тело фрейма	FCS
2 байта	2 байта	6 байт	6 байт	6 байт	2 байта	6 байт	0-2312 байт	4 байт

Рисунок 1.12- Основной фрейм MAC по стандарту 802.11

VCB рама (framecontrol) обычно содержит версию MAC, тип кадра , ее цели . Продолжительность / ID (Продолжительность / ID) Режим станция . Адреса 1, 2, 3 и 4 обычно варьируется в зависимости от типа кадра и подтипа . Управление очередью , как правило (sequencecontrol) включает в себя серийный номер и номер трека кадра. Контрольная сумма ФТС кадра.

802.11 MAC слой очень похож на реализованный в 802,3 , где он будет, естественно, поддержки нескольких пользователей на общей несущей , когда пользователь проверяет носитель перед доступом к нему , с использованием протокола CSMA / CD . 802.11 , как правило, применяется модифицированный протокол , известный всем как перевозчик Sense Multiple Accesswith предотвращения столкновений (CSMA / CA) , или распределенных функция координации (DCF). CSMA / CA , что бы предотвратить столкновения она пошла через ACK пакета (ACK) , то это означает , что пакет ACK будет отправлен для подтверждения , что пакет был получен без изменений.

Работает CSMA / CA следующим образом. Станция , Катори peredavet , тестирование канала и если канал отвечает за , станция ждет случайный период времени, а затем передает , если среда передачи данных все еще свободна . Если пакет отправляется приходит целое, принимающая станция посылает пакет ACK , по получении которого отправитель завершает процесс передачи . Если датчик еще не получила пакетов ACK , что означает, что данные не были

получены , или поврежден прибыли ACK , то делается вывод, что произошло столкновение , и пакет данных передается снова и снова после произвольного интервала.

Связь , чтобы определить, является ли канал бесплатно или нет , работает алгоритм оценки чистый канал (просвет канала алгоритм , CCA) . Суть его состоит в определении мощности принимаемого сигнала (RSSI). Если мощность принимаемого сигнала ниже порога , необходимого для нас , то канал будет объявлен вакантным , и уровень УДС получает статус CTS. Если питание над нами желаемые ценности, данных , сохраняемых в соответствии с правилами протокола . Стандартный дает нам еще один setod RSSI - этот метод называется нагрузку. И это селективный , так как он может быть использован для проверки того же типа , что и в несущую 802,11 .

Стандарт определяет , что процесс естественного SSA должны применяться по крайней мере один из следующих способов .

Таким образом, CSMA / CA предоставляет нам путь к разделению радиодоступа . Механизм явное подтверждение прекрасно решает проблему помех. Тем не менее, он добавляет некоторую дополнительную нагрузку , которая не присутствует в 802,3 , 802,11 поэтому всегда будет медленнее , чем эквивалентные локальных сетей Ethernet .

Еще одна интересная проблема MAC - уровень - это проблема «скрытых точек" , когда две станции находятся "слышать" точку доступа , но не могут "слышать" друг с другом , из-за расстояния или различные препятствия. Для решения этой проблемы в УДС 802.11 был добавлен к факультативному протоколу Requestto Отправить / CleartoSend (RTS / CTS) . Когда работет этот протокол , посылающая станция передает RTS и ждет ответа от точки доступа CTS. Так как все станции в сети может "слышать" точку доступа , сигнал CTS заставляет их отложить передачу , что означает, что передающая станция может послать пакет ACK. C RTS / CTS добавляет дополнительные накладные расходы в сети, временно оставляя за собой носитель. Он , как правило, работает только тогда, когда пакет передается с большими данными obmom , для которых повторная бы слишком дорого.

Наконец, уровень ПДК 802,11 можете позволяют вычислить CRC и фрагментации пакетов. Каждый пакет должен иметь контрольной суммы CRC , который мы будет рассчитана и прикрепленный к упаковке. Здесь мы можем увидеть сильный контраст с Ethernet сетей , в которых ошибки ретушировать участие протоколов более высокого уровня (TCP) . Фрагментация пакетов позволяет разбивать большие пакеты на более мелкие передачи по радиоканалу , что полезно в очень " поселились " средах или в случаях . Когда есть сильные помехи , так как более мелкие пакеты меньше шансов быть повреждены. Способ во многих случаях исключает необходимость повторной передачи , и , таким образом, повысить его производительность. Уровень MAC должны stonovitsya Болле ответственность за сборочных полученных фрагментов , что делает процесс более "прозрачным" для протоколов высокого уровня.

802.11 MAC слой должен нести ответственность за то, как клиент

нормально текущего доступа . Когда клиент 802,11 обычно покрыта одним или несколькими точками доступа , он выбирает мощность сигнала и количество ошибок в стояке использует одну из них. После того, как клиент получает уведомление деревянные подключения пульта будут созданы . Будет иногда происходило проверки , чтобы определить более высокий качественный сигнал . Если есть такая точка доступа , станция perenastraevaetsya и соединяется с ним .

Пере соединение обычно происходит, когда станция была Перн или удалены на значительное расстояние , в результате чего затухание . В других случаях , обратное переключение соединение за счет изменения частотных характеристик здания , или просто из-за тяжелого сетевого трафика через prohodyaschigosya оригинальной точки доступа. В этом случае функция протокол, называемый " балансировка нагрузки " в качестве основного значения является распределение общей нагрузки в беспроводной сети более эффективно на всех доступных сетевой инфраструктуры.

Динамическое соединение связи и передачи позволяет всем нам администраторами для установки беспроводных сетей с очень большой поверхностью . Создание перекрытия "ячейку ". Идеальный вариант мы можем рассматривать такую каторый перекрытия точек доступа будет работать различные DSSS каналы , чтобы избежать помех в работе друг друга.

Такие, как потоковое видео голосовые данные , как правило, поддерживается на 802.11 MAC слоя через Координационного Точка Function (PCF) . В отличие это Распределенная координация Функция (DCF) , где управление всегда делится между станциями в режиме PCF , точка доступа только контролирует доступ к каналу . В этом случае, если он установлен BSS включен PCF , время, чтобы быть равномерно разнесены на режим и режим PCF CSMA / CA разделить . Когда система находится в ждущем режиме, ФКП , точка доступа опрашивает все станции для получения этих данных. Для каждой станции vydelin определенный период времени . В это время , ни одна из станций не может передовать данные . Так как PCF позволяет каждому станции передавать в определенный момент времени , это гарантирует максимальную задержку . Основным недостатком этой схемы включают точки доступа , которые должны опрашивать станции все, что будет snezheniyu его эффективность.

Кроме того, в связи с управлением доступа к средствам массовой информации , уровень ПДК 802,11 имеет режима энергосбережения для увеличения срока службы батареи на мобильных устройствах. Этот стандарт поддерживает два режима энергопотребления называемые "непрерывный режим работы " и " Idle " . В первом случае , радио будет в включенном состоянии , а второй только в случае необходимости . Эти сигналы включают в себя информацию о том, какие станция должна принимать данные. Таким образом , клиент может взять мигающий сигнал , получать данные , а затем еще раз, чтобы переключиться обратно в режим "сна" .

Подключение к беспроводным сетям в значительной степени зависят от

погодных условий, солнечные блики , другой беспроводной связи , естественные препятствия , а также других источников помех. Все эти нарушения могут нарушить успешный прием данных. 802.11 была предоставлена автоматического запроса повторной (automaticrepeat - запрос , АЗП) , что позволяет нам рассмотреть возможность ошибок при передаче может быть решена каторый запросы запросы .

Если вы используете запросы АЗП - станция , отправить пакет не получил от него подтверждение (ACK), то он должен автоматически повторной передачи пакета . Количество повторений зависит от его obma . Каждая станция будет всегда содержать два значения: максимальный размер короткого размера пакета и длины пакета . Кроме того, существуют два дополнительных параметра : количество повторов для отправки короткого пакет и количество повторов в течение длительного пакета. Анализ всех этих значений позволит станции принять решение о прекращении ретрансляции пакетов, которые этого не делают.

В качестве примера мы можем рассмотреть запросы по обработке операционной ошибках рассмотреть ARQ - станцию . За что короткий пакет имеет максимальную длину 776 байт , и число повторений для этого короткого пакета будет 10 . Или считают, что станция передает длина пакета 608 байт , но не получает подтверждения от принимающей станции . Затем передающая станция будет передавать 10 раз этот пакет снова в отсутствие подтверждения. После 10 неудачных попыток остановить передаточной станции этот пакет .

1.3.2 Стандарты беспроводной связи IEEE 802.11

Ethernet 802.3 много лет развивается, прежде чем он включает в себя стандарты, такие как GigabitEthernet и FastEthernet стандартов 802.3u 802.3z/802.3ab. Точно таким разработаны и беспроводной Ethernet 802.11, теперь она включает в себя различные семейства стандартов целое передача данных в первую очередь отличительной чертой этих стандартов является физический уровень.

Есть несколько типов WLAN-сетей, которые отличаются друг от друга организации схемы ставок сигнальных данных, радиуса охвата сотовой сети, а также от характеристик радиопередатчиков и приемников. Наиболее широко используется беспроводная сеть стандарта IEEE 802.11b/802.11g/802.11a/802.11as. Сравнение показано в таблице 1.4.

Т а б л и ц а 1.4- Сравнительная таблица основных характеристик Wi-Fi-сетей

Описание	802.11a	802.11b	802.11g	802.11n
Дата принятия стандарта	Июль 1999	Июль 1999	Июнь 2003	Сентябрь 2009
Пропускная способность передачи, Мбит/с	54	11	54	600
Пропускная способность данных,Мбит/с	23	6	20	30-150
Радиус покрытия внутри помещения, м.	35	38	38	70
Тип модуляции	OFDM	CCK	CCK или OFDM	Пространственный OFDM
Диапазон частот	5 ГГц	2,4 ГГц	2,4 ГГц	2,4 ГГц или 5 ГГц
Пространственные потоки мультиплексирования	1	1	1	2, 3, 4 (не предназначено для Wi-Fi)
Ширина частотной полосы, МГц	20	20	20	20 или 40

Первый из 802.11a утвержденных стандартов спецификации и 802.11b , в 1999 году , но наиболее широко используемых устройства, изготовленные в соответствии со стандартом 802.11b.

В стандарте 802.11b был применен метод Высокая широкополосный модуляции с прямым расширением HR- DSSS .

Стандарт IEEE 802.11b обеспечивает нам хорошую максимальной теоретической скоростью передачи 11 Мбит / с, что можно сравнить с обычной кабельной сети 10 BaseTEthernet . Но это достигается skororost mazhno будет работать, если одно устройство WLAN - каторый будет передавать данные . В способе последовательности CCK состоит из 64 8 - Кодирование чип словами , что позволяет ему кодировать слово 6 битов. Это добавляет к характеру два бита . Символы передаются со скоростью 1,375 Мбит / с, и что результаты в полосе пропускания 11 Мбит / с.

Поскольку оборудование , что работает на максимальной скорости 11 Мбит / с , имеет меньший диапазон, чем на более низких скоростях . Это был

стандартный 802.11b predumano автоматическое снижение скорости при ухудшении качества сигнала . Как и в случае основного 802,11 четких механизмов на роуминг спецификации 802.11b не определены .

Преемник IEEE 802.11b IEEE 802.11 сделаны B + , между ними удвоение максимальную скорость передачи данных и более типов модуляции в IEEE 802.11 B + .

Несмотря на то, что 802.11a ratifikatsirovan был в 1999 году, он действительно начал применяться только с 2001 года. Данный стандарт широко используется в основном в таких странах, как США и Япония . Оборудование стандарта 802.11a, в Казахстане этот стандарт применяется только к общественной adminestrativnyh доставлено.

802.11a стандарт работает в ортогональным частотным разделением нескольких plexing сигнала схема модуляции - мультиплексирования по ортогональным частотным разделением (OFDM) , pokazonaya на рисунке 1.13. OFDM делит сигнал на несколько nesuzhih делает параллельный сигнал в полосу частот разделение фильтры могут работать или разделени частотного диапазона на носителях с помощью преобразования Фурье. Устраняет interferensnye явления в течение одного приемопередатчика тракта. Самая большая разница между этим методом и радио технологий DSSS и FHSS в том, что OFDM сигнал preredaet параллельно и одновременно в нескольких диапазоне частот , в то время как технология расширения спектра последовательно передавать сигнал . И его результат увеличивается пропускная способность и качество сигнала.

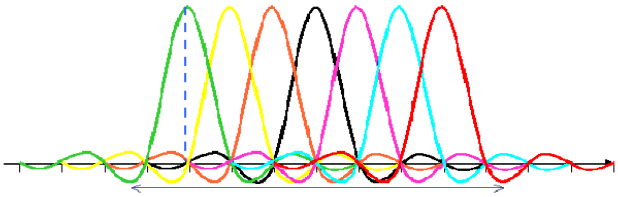


Рисунок 1.13-OFDM мультиплексирование

К недостаткам 802.11a можно отнести к большим радио энергопотребления до 5 ГГц , а также ряд Маленко . Основной поток данных разделен на несколько параллельных потоков , имеющих относительно низкую скорость передачи , а далее работает , чтобы модулировать их желаемого носителя. В этом стандарте есть три обязательные скорости передачи данных (6 , 12 и 24 Мбит / с) и еще пять (9 , 18, 24 , 48 и 54 Мбит / с) . Таким образом, можно работать два канала передачи данных , которые увеличили бы свою скорость .

Наиболее важным аспектом можно отнести , что беспроводные сетевые стандарты IEEE 802.11a и 802.11b (B +) невидимы друг с другом и должны быть в состоянии сосуществовать параллельно, не мешая друг другу . Другими словами, эти два стандарта беспроводных сетей не совместимы .

Поэтому , учитывая низкий уровень 802.11b оборудования и отсутствие оборудования стандарта 802.11a , хорошее и верное решение теста становится стандартом IEEE 802.11g . Она сочетает в себе скорость 802.11a (54 Мбит / с) и совместимость с существующей 802.11b (B +) . Конечно, максимальная скорость 54 Мбит / с может развить скорость устройства - 802.11g . Но если bespravodnaya сети смешивается , то есть , она включает в себя устройство, совместимое стандарты , что его максимальная скорость передачи данных ограничивается его пиковой скорости обмена старых устройств .

Стандарт 802.11g был принят в июне 2003 года. И это еще спецификация развитие IEEE 802.11b, и Катори позволяет передавать данные в том же диапазоне частот , как 802.11b. Основное различие между этим стандартом является его увеличенная емкость - Катори составляет 54 Мбит / с по сравнению с 11 Мбит / с в 802.11b. Как IEEE 802.11b , новая спецификация включает в себя работу на частоте 2,4 ГГц , но и увеличить его скорость применяя тот же схему модуляции сигнала - как и в 802.11a - мультиплексирование с ортогональным частотным разделением каналов (OFDM) .

Некоторые производители предлагают нам оборудование стандарта 802.11g + (SuperG) , и на коробках своих изделий (точки доступа и беспроводные адаптеры) в дополнение к надписи '802 .11 g+ ' они также указать скорость 100 , 108 или даже 125 Мбит / с .

Никакой протокол 802.11g + не существует , и все, что лежит в основе этой загадочной протокола - это просто расширение основного стандарта 802.11g . На самом деле, все эти производители чипсетов для беспроводных решений (Intersil , TexasInstruments , Atheros , Broadcom и Agere) в том или ином виде реализовали эту передовую режим 802.11g +. Важнейшей проблемой можно считать, что все производители по-разному создать этот режим , и нет никакой гарантии, что решения различных производителей будут работать вместе . Поэтому, когда вы покупаете этот точки доступа стандарта 802.11g + следует Убида что ваши беспроводные адаптеры также поддерживают тот же стандарт .

Как уже было сказано , что по количеству 802,11 скрывает целое семейство различных стандартов , ниже мы кратко рассмотрим каждый из них .

Рабочая группа 802.11c (точка доступа моста) обычно протоколы и процедуры , необходимые для согласования точек доступа каторый внутри сети 802.11 в не большом расстоянии .

В целях расширения распространения сетей, стандарт 802.11 , IEEE вел довольно общие требования к физическому уровню 802.11 , но странно совместимый 802.11d (Интернационализация) .

Стандартная спецификация 802.11e (QoSExtensions) может создать мультисервисную беспроводную локальную сеть , каторый будет orintirovatsya на другого пользователя. При сохранении все были совместимы с 802.11a и Ь, она может продлить их функциональность за счет поддержки потокового мультимедиа данных.

Технические характеристики 802.11f (Inter- поставщиков точка доступа передачи обслуживания) имеет протокол служебную информацию между точками доступа (Inter- AccessPointProtocol , IAPP) , что нам нужно для создания беспроводной сети передачи данных .

Рабочая группа IEEE 802.11h (мощность Controlfor 5 - ГГц область) будет рассматриваться как возможность дополнить существующие спецификации 802.11 MAC и алгоритмы 802.11a PHY лучше выбора частоты для офиса и наружных беспроводных сетей , а также спектр управления , мониторинга и мощность излучения генерировать соответствующие отчеты.

Предполагается, что эти цели будут основаны на работе протоколов Dynamic Frequency Selection (DFS) и управления мощностью передачи (TPC) , каторые были предложения по Европейским институтом телекоммуникационных стандартов (ETSI) . Эти протоколы смогут динамично реагировать на беспроводных клиентов , интерференции радиосигналов , переключившись на другой канал , что насытить для снижения мощности или обоих.

До мая 2001 года, стандартизация информационной безопасности для 802.11 беспроводных сетей в пределах компетенции рабочей группы IEEE 802.11e , но то для решения этой проблемы не было выделены самостоятельная единица . Разработанный стандарт 802.1x был вызван на возможности протокола rasshirireniya 802.11 MAC , была предоставлена для шифрования передаваемых данных , а также централизованную проверку подлинности пользователей и рабочих станций. Теперь , в результате шкале беспроводные локальные сети может быть увеличена до сотен или тысяч рабочих станций. В центре 802.1x протокола аутентификации лежал расширяемый протокол аутентификации (EAP) , который был основан на ППС . Процедура идентификации сама по себе предполагает , что он участвует три стороны - Вызывающий абонент (клиент) вызова (точка доступа) и сервер аутентификации . В то же время , новый стандарт оставляет на усмотрение производителей , реализующих основные алгоритмы управления .

Все данные , разработанные средства могут быть применены не только в беспроводных, но и другие - ЛВС Ethernet и TokenRing . Здесь, на этой будущей стандартном номере получил IEEE 802.1x , и его группа разработки 802.11i (EnhancedSecurity) приводит вместе с комитетом IEEE 802.1 .

Спецификация 802.11j - что проект поправок к стандарту , необходимых для локальных сетей / столичной области (парень), который регулирует работу в соответствии с правилами 802.11a 4,9 ГГц , выделенных в Японии и США для общественного пользования , а также в соответствии с правилами техники безопасности и диапазоне 5,03-5,091 в Японии. В схеме нумерации каналов (канал) numberingscheme эти каналы пронумерованы от 240 до 255 , ширина каждой составляет 5 МГц . Предполагается, что стандарт будет указать существование целого ряда сетевых стандартов 802.11a и HiperLAN2 .

Спецификация 802.11r будет устанавливает универсальную и совместимой системы для возможности роуминга пользователь переходит с одного покрытия сети в диапазоне от другой.

Также создан новый стандарт WLAN - IEEE 802.11n . Каторый работает вдвое быстрее, чем 802.11a и 802.11g , со скоростью 100 Мбит / с до максимум 540 Мбит / с. Этот стандарт уравнять проводной и беспроводной систему, которая позволит корпоративным клиентам использовать беспроводные сети, где не было возможности из-за ограниченной скорости .

Стандарт IEEE 802.11n

Этот стандарт был утвержден 11 сентября 2009 . 802.11n и ее скорость передачи сравнима с проводными стандартов. Его максимальная скорость передачи данных 802.11n сравнительно 5 раз производительность классической Wi-Fi.

Можно отметить, следующие основные преимущества стандарта 802.11n :

- Высокоскоростная передача данных (около 600 Мбит / с) .
- Униформа , стабильная, надежная и качественная зона покрытия станции , не имеющие покрытия области .
- Совместимость с предыдущими версиями стандарта Wi-Fi.

недостатки:

- Высокое энергопотребление .
- Два рабочий диапазон (возможно замена оборудования) .
- Сложная и более общий аппарат .
- Увеличение скорости в стандартной IEEE 802.11n достигается , во-первых, за счет удвоения его ширину канала от 20 до 40 МГц , а во-вторых, за счет реализации технологии MIMO (рис. 1.14) .

Технология MIMO (Multiple Input Multiple Output) обычно включает в себя использование множества передающих и приемных антенн. По аналогии , традиционная система , то есть системы с одной передающей и одной приемной антенны , называется SISO (один вход один выход) .

Стандартный технологии IEEE 802.11n был основан на OFDM -MIMO . Большое количество realizovannych это tehnicheskich элементы были взяты из стандартного 802.11a , однако , стандарт IEEE 802.11n также предусматривает использование в качестве частотного диапазона , принятого для стандартной IEEE 802.11a, и диапазон частот , принятого для стандартов IEEE 802.11b / г . То есть, устройство поддерживает стандарт IEEE 802.11n,также может работать в диапазоне частот 5 ГГц или 2,4 ГГц.

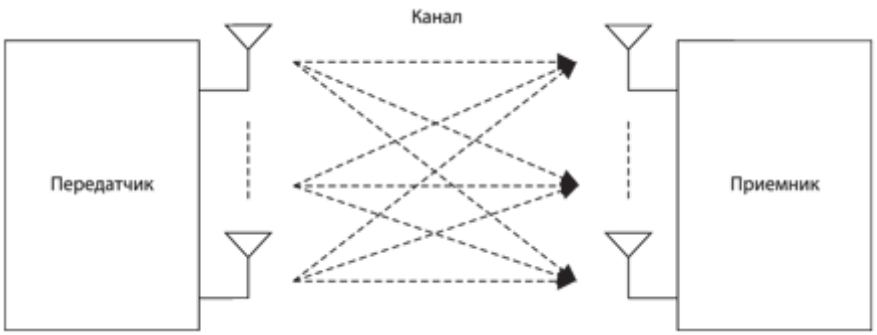


Рисунок 1.14- Принцип реализации технологии MIMO

Передаваемый сигнал разделен на последовательность параллельных потоков из которых на приемном конце она сводится в качестве исходного сигнала. Там могут быть некоторые трудности - каждая антенна получает наложение сигналов , которые должны быть отделены друг от друга . Для этого на приемном конце , как правило, используется специально разработанный алгоритм пространственного сигнала обнаружения . Это распределение основано на algoritmbyl поднесущей и тем труднее , чем больше их число . Единственный недостаток использования MIMO включают сложность и громоздкость системы и, как следствие , более высокое потребление энергии .

Для каждого режима работы имеет свой преамбулы структуру - пакет услуг поле , что указывает на начало его передачи и служит для синхронизации передатчика и приемника . В преамбуле , как правило, содержит информацию о длине пакета и типа , в том числе типа модуляции , способ кодирования , выбранный , а также все его параметров кодирования . Чтобы избежать конфликтов в рабочих станций MIMO и обычных (с одной антенной) во время обмена между станциями MIMO пакетов преамбулы и сопровождается специальным заголовком . Обычно получил такой информации станции, которая работает в стандартном режиме , не задерживая передачу до конца сессии между станциями MIMO. Кроме того, структура преамбулы может обнаружить определенную основную задачу приемника , например, его оценки мощности принимаемого сигнала для системы автоматического управления усилением , обнаружения пакета начальное смещение по времени и частоте .

MIMO режимов работы станций

Наследие режима . Этот режим обычно предоставляется в целях содействия обмену между двумя станциями с одной антенной . Передача информации обычно осуществляется по протоколам 802.11a . Если передатчик станции MIMO , и приемник - стандарт станция ,передающая система может работать только одна антенна , и процесс передачи так же, как и в предыдущих вариантах стандартной Wi-Fi. Если передача идет в противоположном направлении - от обычного станции в многоантенным , станция может ispolzuvatsya много MIMO приемные антенны , но в этом случае скорость передачи не самая высокая . Структура преамбулы в этом режиме так же, как в версии стандарта 802.11a .

Смешанный режим . В этом режиме обмен пойдет между системами MIMO , и между регулярными станций . В связи с этим , система MIMO будет генерировать два типа пакетов , в зависимости от типа приемника . С обычными станции работают идет медленно , поскольку они не поддерживают работу на высоких скоростях , а также между MIMO - гораздо быстрее, но скорость передачи данных ниже, чем при зеленом поле. Преамбула пакета в обычной установке так же, как в стандарте 802.11a и пакет MIMO , она будет слегка изменен. Если система MIMO передатчик выполняет , то каждая антенна не будет передавать всю преамбулу , ициклически сдвинуты . В связи с этим пониженным энергопотреблением всей станции и канала является более эффективным. Однако, не все в наследство станция может работать в этом режиме . Дело в том, что если алгоритм устройство синхронизации была основана на кросс-корреляции , будетпотеря синхронизации .

Режим Зеленые поля . В этом режиме вы можете систем полностью ispolzuvat преимущества MIMO . Передача возможна только между множеством антенн станций в присутствии традиционных приемников. Когда есть передача MIMO -системы , когда станция дожидаясь выхода обычного канала , чтобы избежать конфликтов. В зеленом поле принимает сигнал от систем, работающих в первых двух схемах , насколько это возможно , и передача им - нет. Это было сделано для того, чтобы исключить из обмена станции с одной антенной и тем самым увеличить его скорость. Пакеты будут сопровождаться преамбуле , которая поддерживается только станции MIMO . Все эти меры позволят максимально использовать возможности системы MIMO - OFDM. Во всех режимах должен быть обеспечен защитой от влияния его работы от соседней станции , чтобы предотвратить искажение сигнала . На физическом уровне модели OSI , как правило, разработаны для этой специальной области преамбулы структуры, которая может уведомить станцию, которая передает и принимает определенное время ожидания. Некоторые методы защиты будут доступны только на канальном уровне . В зависимости от его режима пропускной rabotoemoy классифицируются следующим образом :

1 унаследованные режим . Этот режим необходим для согласования с предыдущими версиями Wi-Fi. Это очень похоже на 802.11a / г, как на оборудование и пропускной способности , что на 20 МГц .

2 Дважды унаследовал режим . Устройства , которые используют полосу 40 МГц , в то время как та же данные передаются по верхним и нижним каналами (по 20 МГц), но с фазовым сдвигом на 90 °. Обыно Структура пакета будет направлена на то, что приемник регулярно станция . Дублирование имеет жизненно важное значение сигнала уменьшения искажения , тем самым увеличивая скорость передачи .

Режим 3 с высокой пропускной способностью . Устройство, которое может поддерживать как базовой полосы -20 и 40 МГц . В этом режиме , станции общаться только пакеты MIMO . Скорость такой сети максимальна.

Режим 4 из верхнего канала . Этот режим будет работать только верхнюю половину диапазона 40 МГц. Станции могут обмениваться любыми пакеты.

5 Режим нижний канал . Этот режим будет действовать только нижнюю половину полосы частот 40 МГц . Станции также можете поделиться любые пакеты.

1.4Топологии беспроводных сетей Wi-Fiстандартов 802.11

802.11 может основываться на любом из этих топологий:

- Независимый площадь основная услуга (Независимый Basic Service устанавливает, IBSSs).

- Основная зона обслуживания (базисные множества Обслуживание, ПБС).

- Расширенная зона обслуживания (расширенные наборы Обслуживание, ESS,).

Независимый основная зона обслуживания (IBSS)

IBSS, как правило, обычный группа действует в соответствии с 802,11 станций, которые взаимодействуют непосредственно друг с другом. Рисунок 1.15 показывает, как vzaimodestvuyut станция и связаны друг с другом, оборудован беспроводной NIC (сетевая карта, NIC) 802.11 IBSS могут образовывать Содин и непосредственно друг с другом.

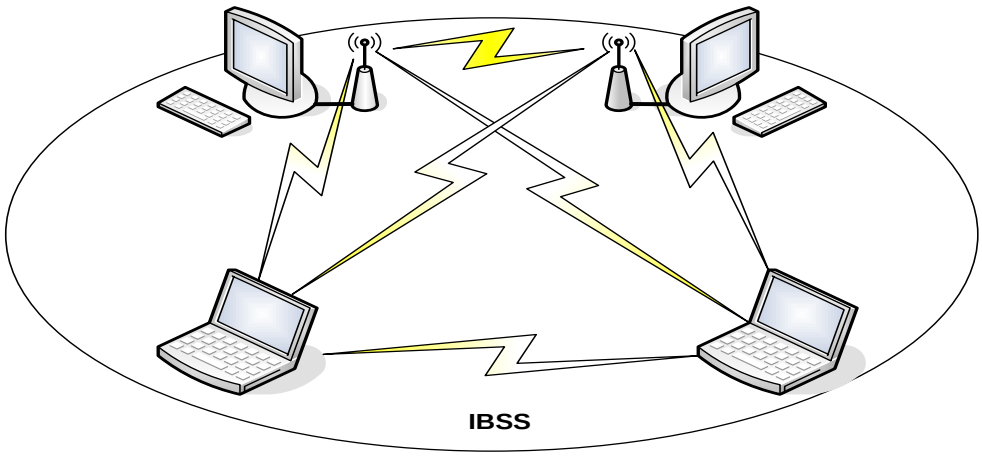


Рисунок 1.15- Ad-Hoc сеть (IBSS)

Специальная сеть , или как его еще называют независимым основная зона обслуживания (IBSS) , как правило, происходит, когда человек клиентские устройства образуют самоподдерживающейся сети без использования одной точки доступа (AP - AccessPoint) . Обычно при создании таких сетей , как правило, не развивается никаких карты места для их размещения и предварительным планам , поэтому они , как правило, небольшие и имеют

ограниченную степень , достаточную для передачи общих данных , когда это необходимо .

Поскольку IBSS нет точки доступа , распределение времени (временной) осуществляется в децентрализованной . По клиентов, которые начинает передачу в IBSS , устанавливает сигнал (мигающий) интервала (beaconinterval) , чтобы создать набор времени передачи мигающий сигнал (setoftargetbeacontransmissiontime , TBTT) . После завершения TBTT каждому клиенту IBSS будет:

Базовая зона обслуживания (BSS)

BSS - группа работает на 802,11 станций , как правило, соединяющий друг с другом. Технология BSS обычно подразумевает наличие какой-либо конкретной станции , которая называется точкой доступа AP (AccessPoint) . Точка доступа - это центральный пункт связи для всех станций BSS . Клиентские станции обычно не взаимодействовать непосредственно друг с другом. Вместо этого, они будут общаться с точкой доступа , и уже он будет передавать кадры до станции назначения . Точка доступа может быть порт восходящая линия связи (uplinkport) , через которую BSS могут быть подключены к проводной сети (например, по восходящей линии связи Ethernet). Поэтому , как правило, называется BSS инфраструктуры BSS . На рисунке 1.16 показана типичная инфраструктура BSS.

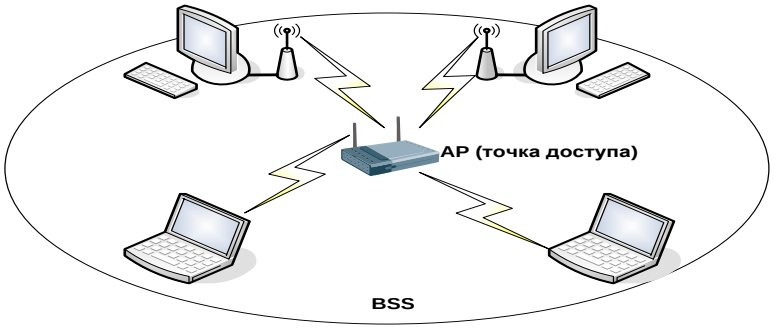
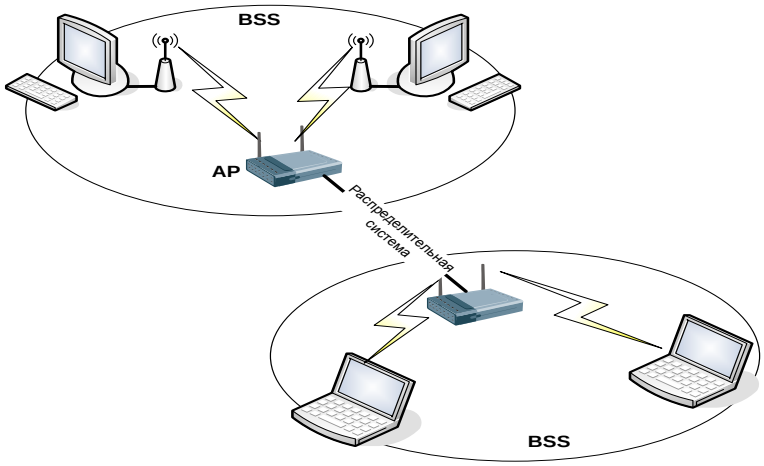


Рисунок 1.16- Инфраструктура локальной беспроводной сети BSS

Расширенный зона обслуживания (ESS)

Несколько инфраструктуры BSS, как правило, подключаются через их интерфейсы восходящей. В ситуациях, когда стандартный интерфейс восходящей 802.11 соединяется с системой распределения BBS (система распределения, DS). Несколько BBS, которые взаимосвязаны через систему распределения образуют расширенную зону обслуживания (ESS). Uplink к системе распределения не должны работать как проводной связи. На рисунке 1.17 приведен пример практической реализации ESS. 802.11 Спецификация обычно оставляет открытой возможность для этого канала в виде беспроводной сети. Но чаще всего они эти каналы проводной *технологии Ethernet.*



.

Рисунок 1.17- Расширенная зона обслуживания ESS беспроводной сети

1.5 Беспроводное оборудование используется в Wi-Fi сетях

Сегодня беспроводные сети могут позволить пользователям для обеспечения связи , где трудно кабель или нужно полную мобильность . В то же беспроводной сети можно подключить без проблем и взаимодействовать с проводными сетями .

1.5.1 Точки доступа Wi-Fi

Просто точка доступа Wi-Fi работает через радио. Я хочу сказать , что подключение к точкам доступа через RJ45 дает большую скорость и более низкие потери передачи в отличие от Wi-Fi , который очень chustvitelen вмешательству ли стена или алюминия на крыше. Для того, чтобы создать беспроводную сеть , как правило, используется в закрытом помещении в помещении вариант этого устройства. Он имеет значительно более низкую стоимость и , как правило , большие эстетику , но и менее мощный . Может работать такие точек доступа внутри одной или более комнат . На открытых участках может работать до 300 метров с рабочих стандартных всенаправленные антенны . Точка доступа для любых погодных обычных версий предназначены для создания сети радиосвязи между зданиями . В зависимости от типов антенн были такие устройства способны создать каналы связи на расстоянии 3-5 км . Максимальная дальность беспроводной связи , как правило, заметно возросла с использованием усилителей. В этом случае длина радиолинии достигает 10,8 км. Такие устройства, как точки доступа показаны на рисунке 1.18.

Комбинированные устройства

Большой интерес у пользователей вызывает беспроводных точек доступа, которые сочетают в себе функции других устройств, таких как высокоскоростной беспроводной широкополосный маршрутизатор со встроенным переключателем FastEthernet . Маршрутизатор обычно позволяет

нам быстро и легко настроить общий доступ к Интернету , как проводной или беспроводной сети , а также организовать широкополосный линию обмена и кабельное / DSL модем дома или в офисе.

а б в г

Рисунок 1.18- Виды точек доступа: а, б – внутренние; в, г – внешние

1.5.2 Wi-Fi адаптеры

Для подключения к беспроводной сети Wi-Fi в присутствии достаточно иметь ноутбук или персональный цифровой помощник (PDA) с подключенной Wi-Fi адаптера.

Любая беспроводная Wi-Fi адаптер необходим для отвечать ряду требований :

- Нужно сделать его совместимым со стандартами .
- Работа у него есть частотный диапазон 2,4 ГГц - 2,435 ГГц (или 5 ГГц) .
- Просто держать протоколы WEP и предпочтительно WPA.
- Кроме того, поддержка двух типов " точка- - точки " и "компьютерный сервер . "
- Просто имейте функцию роуминга .

Пока существует три основных типа Wi-Fi адаптеров , дифференцированные по видам связи :

- Первая из них связана с портом USB на вашем компьютере. Такие адаптеры , как правило, компактный , простой в настройке , а интерфейс USB обеспечивает" горячей замены " .
- Второй подключен через PCMCIA слот (CardBus) ПК . Такие устройства , как правило, находится внутри компьютера (ноутбук) и поддерживать любые стандарты для передачи данных на скорости до 108 Мбит / с .
- Это же устройство интегрирован непосредственно в материнскую плату компьютера. Это наиболее перспективный вариант . Такие адаптеры обычно устанавливаются ноутбуки серии IntelCentrino . И , в настоящее время используется на подавляющем большинстве мобильных компьютеров. Все виды беспроводных адаптеров показаны на рисунке 1.19.

а б в

Рисунок 1.19- Беспроводные адаптеры:

где а - С USB портом.

б- Формата PCMCIA.

в -Встроенный в материнскую плату.

2 Организация беспроводной сети

2.1 Развитие сети

Каждый системный администратор или кортировшик знаем, что место работы - количество , расположение и конфигурация требуется в зданиях TD. Для получения этой информации , как уже говорилось , необходимо сначала определить, какие бы развертыванию namiset - которая должна быть ориентирована на максимальную зону покрытия , высокую пропускную способность , или гибрид, перехода , то вы должны немедленно рассмотреть два аспекта. Физический аспект создания отображения администратором пространства должны дать представление о том, что область может охватить все TD , и сколько точек доступа необходимо , чтобы служить все указанную область , какие каналы и вещателей , и как власть должна быть использована и какой тип или как должны получить быть антенной .

Пусть те, рассмотреть этот вариант в nachalinuzhno с требуемой производительностью и перенаправления скорости каждого пользователя, и нужно выяснить, плотность всех пользователей , чтобы определить свое отношение ", количество пользователей / количество TD ". В конце концов, надо поставить и настроить точку доступа , чтобы максимизировать их производительность в главной области сервиса .

В нашем случае это необходимо покрыть локальной сети несколько этажей здания, поэтому при планировании нужно помнить, что сеть первом этаже может вмешиваться в сети dlyav второй этаж , и наоборот , etozavisit от конструкции здания. Потенциально это может привести к задержкам в процессе отображения по месту работы , потому что это необходимо для измерения интенсивности сигнала не только " его" полу , но и на этажах одного сверху и один снизу .

В дополнение к рассмотрению все эти аспекты , необходимо обратить внимание на характеристики всех клиентских устройств , конечных пользователей , с учетом типов клиентских устройств , типов приложений , эксплуатируемых персоналом с использованием WLAN. В sluchaekogda офисе , используемой настольных ПК , объем роуминге будет мало, так что в центре внимания должно быть уделено уменьшить перекрытие между каналами. Если вы используете ноутбук , вы не обязательно должны предоставить высокую скорость передачи данных от рабочих станций и конференц-залов. После изучения этих вопросов станет основой для определения требований к пропускной способности и перенаправить пакеты в сети - и, в общем , и в некоторых своих местах с конкретными требованиями.

Следующим шагом является на самом деле проводить работу отображения . При развертывании нашей сети подход был выбран ори ¬ strated высокую эффективность , поэтому каналы распределения делается таким образом, чтобы избежать дублирования ; каждое исследование должно

проводиться именно в канале , который будет использоваться . Пример этого метода непересекающихся каналов различных точек доступа показана на рисунке 2.1. Там также должны быть ряд исследований при скорости передачи данных минимального требуемого . Поскольку мы говорим о высотном здании , не забывайте о своих маргинальных зон - этажом выше и этажом ниже будет рассматриваться ; мы должны сделать все измерения. Eslioni будет ниже, чем ожидалось , вы должны попытаться изменить каналы , потому что проблема может быть вызвана помехами.

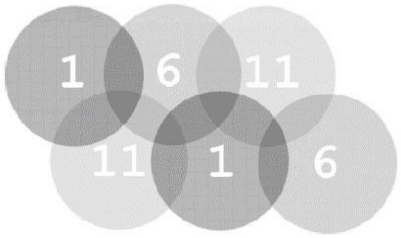


Рисунок 2.1 - Пример использования неперекрывающихся каналов

Когда мы выбрали быть поход, а также для определения количества пользователей, которые будут подключаться к каждой точке доступа , и плотность их размещения .

В начале выберите один из краев плоских , положить туда TD ; то искал предел ее охвата ,А.П. находится там и исследовать его зону обслуживания . Затем у нас есть два варианта: " снаружи внутрь ", а затем заполнение "дыры" или " от одной точки доступа к другой. " В любом из подходов, описанных здесь , мы должны определить края клеток и предоставить нам нужный уровень перекрытия , поэтому необходимо , чтобы настроить свой потенциал до тех пор не достичь желаемых размеров клеток. Так как пользователи размещаются в некоторой степени от некоторых отдельных групп , подход будет применяться " от краев к середине. " Такой подход показан на рисунке 2.2.

В настоящее время существует огромное количество оборудования и программного обеспечения , вы можете выбрать местоположение точек доступа namvybratoptimalnoe учитывая ее экономически жизнеспособной выбор дополнительного оборудования для них , такая схема может настроить оптимальные границы сети в режим радио.

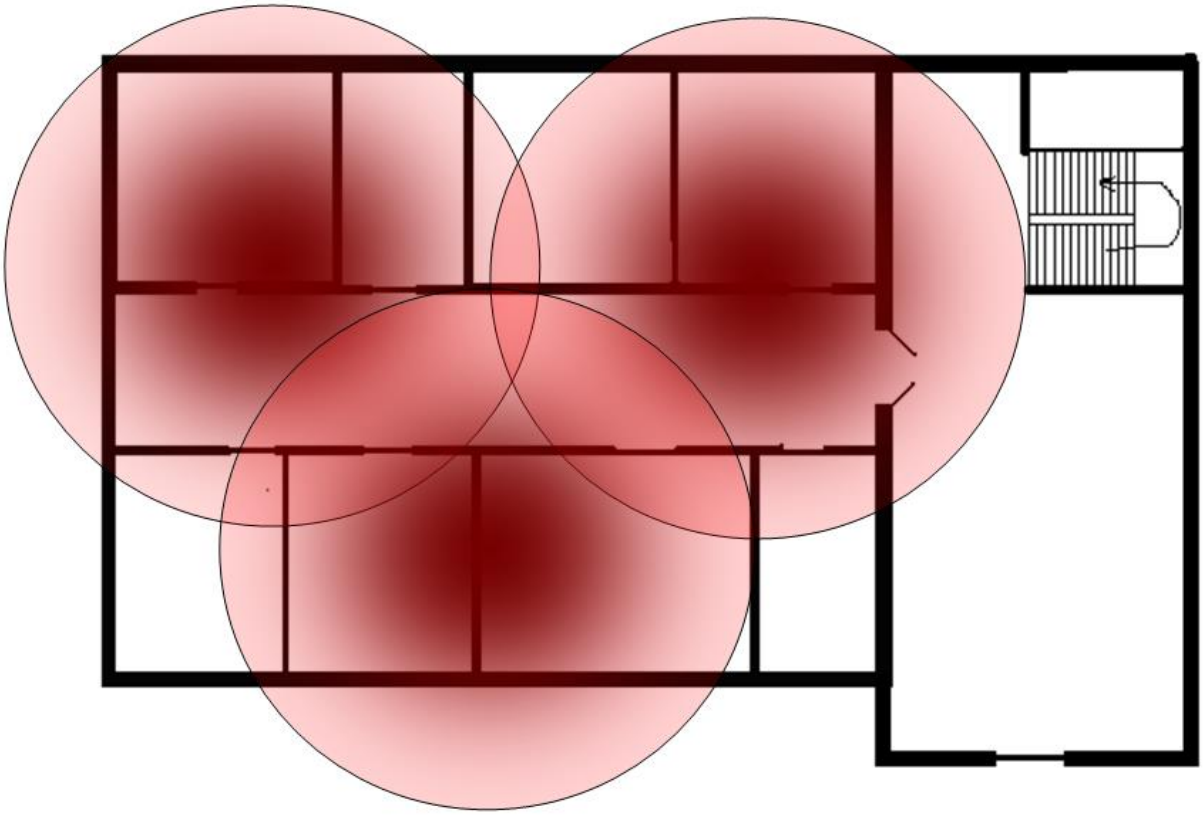


Рисунок 2.2 - Покрытие сети этажа точками доступа

Примером такого программного обеспечения может служить произведение Ekahau - SiteSurvey (ESS) 2.1 для сетей 802.11a/b/g . Особенность этого программного обеспечения является то, что часть аппаратных средств , нам нужен ноутбук с Wi-Fi адаптером , и предпочтительно , внешняя антенна , что позволяет нам повысить точность измерений . Пакет этого программного SiteSurveysostoit базовой программы и заказчиком аудита в сетевой вместе с набором драйверов для карт от разных производителей . В результате EkahauClientstanovitsyanash обычного ноутбука с Wi-Fi- адаптера в качестве инструмента для мониторинга беспроводной сети , и в большинстве случаев позволяет избежатьстоимость приобретения и размещения дополнительных приборов .

Схема этой программы довольно прост. Сначала мы сделали с помощью планирования SiteSurvey сети , которая в окне редактора состоит из сети охватывает пространство . Далее идет выбор расположения точек доступа и использования EkahauClient и ноутбук - проверка и отладка выбранные положения точек доступа . Тогда есть этап выбора оптимального режима радио и повторного управления радио. Вообще , работая с этой программой напоминает подходит как podnashe результате , условия в численных методов . Корреляция требуемое положение беспроводной сети радио продолжается, пока не будет найден достаточные условия для данного режима .

По мере увеличения числа Wi-Fi и появлением инструментов, которые позволяют автоматизировать некоторые из этих процессов , то разумно ожидать, что Wi-Fi будет иметь такую же производительность и надежность, как проводной сети .

2.2 оборудование

Для построения нашей беспроводной сети использует Wi-Fi - адаптеры и точки доступа .

Pokazanyadaptery рис. 2.3 , который представляет собой устройство , которое соединяет через слот расширения PCI, CardBus , CompactFlash . Также есть адаптеры для подключения непосредственно через порт USB 2.0. Wi - Fi - адаптер выполняет ту же задачу, что и сетевой карты в проводной сети. Необходимо подключить компьютер к беспроводной сети . Сейчас многие современные компьютеры имеют встроенный Wi-Fi- адаптера. Wi-Fi - adapteramisnabzheny КПК, который также позволяет им подключаться своих беспроводных сетей.

Рисунок 2.3 - Адаптеры

Чтобы получить доступ к адаптера беспроводной сети можно подключить непосредственно с другими адаптерами. Такая сеть обычно называется специальная (для данного случая) , или внеплановой сети . Адаптер также можете общаться через специальное устройство - точку доступа . Этот режим связи называется инфраструктура .

Чтобы определить, как подключить адаптер , как правило, быть настроен на использование AdHoc или режим инфраструктуры .

Точка доступа представляет собой что-то вроде автономное устройство со встроенным микрокомпьютером и приемно- передающего устройства. Через точку доступа , вы можете взаимодействовать и обмениваться информацией между беспроводными адаптерами , а также связь с проводным сегментом сети . ТД можно считать чем-то вроде ступицы.

Точка доступа должна иметь свой сетевой интерфейс (uplinkport) , который помогает нам подключиться к проводной сети. Через тот же интерфейс может быть все настройки точки .

Просто точка доступа может быть использован для подключения к ее различных клиентов (основной режим - точки доступа в режиме) , и работать с

другими точками доступа , чтобы построить распределенную сеть (Wirelessdistributedsystem - WDS) . Эта беспроводная режимы мост " точка-точка " и " точка -многоточка " , беспроводной клиент и повторитель .

Доступ к сети обеспечивается путем пропускания его через эфир сигналов вещания . Приемная станция может естественно получает сигнал в диапазоне от нескольких передающих станций . Станция приемник использует идентификатор зоны обслуживания (servicesetindentifier , SSID) для фильтрации сигналов , которые мы получаем и выбрать тот, который нам нужен.

Зона обслуживания (serviceset , CC) называется логическое группирование устройств , которая обеспечивает подключение к беспроводной сети.

Основная зона обслуживания (basicserviceset , BSS) - он работает gruppakotoraya 802,11 станций , которые общаются друг с другом по беспроводной сети. Технология BSS предполагает использование специальной станции , которая называется точкой доступа (AccessPoint) . Сетевой интерфейс точки доступа , как правило, используется для подключения область база службы к проводной сети (например, Ethernet) , так называемый, потому BSS , которая также называется инфраструктуры BSS .

Для выполнения задач dannoyvypusknoy работу я выбрал беспроводные адаптеры D-Link DWL- G520 и точку доступа D- linkDWL - 3200AP , так как они являются наиболее полезными сочетают в себе качество и цену, необходимую для реализации dannoyraboty .

Плюсы решения :

- Поддержка всех современных стандартов - точка доступа может подключаться как клиенты и 802.11g 802.11b , и клиенты сети 802.11n .

- Режим работы: точка доступа , мост точка -точка мост точка - многоточка , беспроводной клиент , повторитель . LAN порт (10/100 Base-T) для подключения к проводной части сети .

- Поддержка WDS (беспроводная система распределения). Сегментация беспроводных клиентов , проводной и беспроводной части сети.

Необходимо подключиться к серверу номера в разных концах здания , на 3-м этаже . Для этого мы используем 3 TD бренд DWL- 3200AP на рисунке 2.4 .

Особенности:

- Скорость nashegosoedineniya до 54 Мбит / с .

- Рабочий диапазон частот от 2400 до 2483,5 МГц.

- Тип антенны - две съемные 5dBi дипольных антенн разнообразие с обратным SMA -коннектором .

- Защита данных : Тип WEP- шифрование 64 - , 128 - , 152-бит .

- Сервер аутентификации пользователя RADIUSIEEE 802.1x . WPA- Wi-FiProtectedAccess (64 - , 128-бит с TKIP) .

- PodderzhkatehnologiiAES (Advanced Encryption Standard) .

- Веб - управление , Telnet

Рисунок 2.4 - Точка доступа DWL-7100AP

AirPlusXtremeGrabotayut на скорости до 54 Мбит / с, что достаточно для этого seriibolshinstva современных бизнес-приложений. Улучшение на 20 дБ чувствительность нашего приемника. Это обеспечивает хорошую устойчивость и повышает производительность клиентов в беспроводной сети.

Расстояние, которое является нашим антенны 10 метров. Одна точка доступа будет подключен непосредственно к серверу, и двумя другими офисами в рисунке 2.4.

2.3 Расчет влияния

2.3.1 Расчет диапазона беспроводной связи. график платежей

Этот метод позволяет определить теоретическую спектр беспроводного канала связи, построенный на нашем оборудовании D-Link стандартов 802.11 б и г (2,4) и 802,11 (5 ГГц). Следует отметить, что расстояние между антеннами, в результате формула - теоретически достижимой максимум, а также влияет на беспроводную связь слишком много факторов, чтобы получить спектр производительности, особенно в городе, практически невозможно.

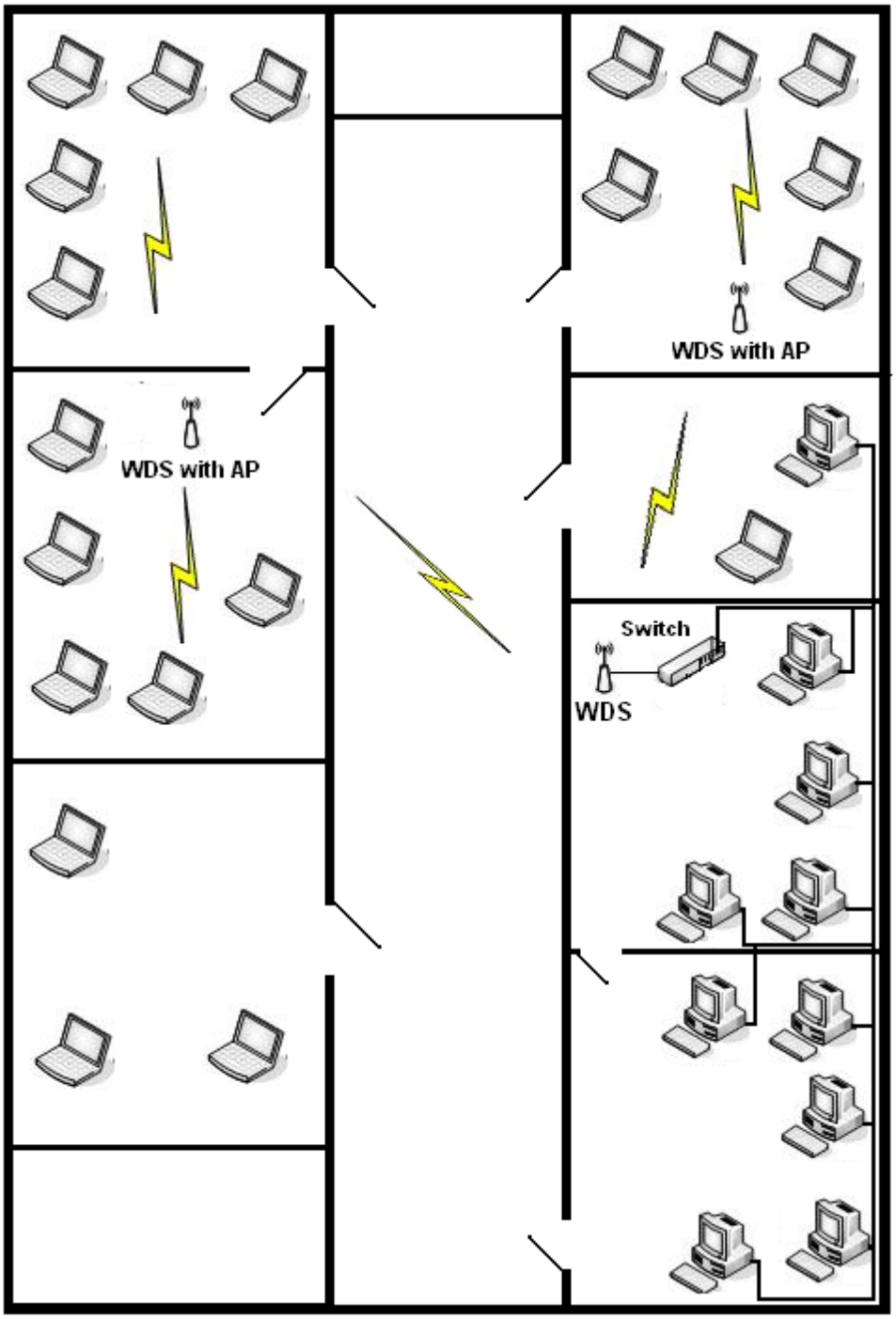


Рисунок 2.5 - Структура сети

Для определения дальности связи нам необходимо рассчитать суммарное усиление тракта и по графику определить соответствующую этому значению дальность. Усиление тракта в дБ определяется нами по формуле

$$Y_{\partial Б} = P_{t,\partial Б} + G_{t,\partial Б} + G_{r,\partial Б} - P_{\min,\partial Б} - L_{t,\partial Б} - L_{r,\partial Б} \qquad (2.1)$$

где $P_{t,\partial Б}$ -Мощность передатчика.

$G_{t,дБ}$ -Коэффициентусиления, передающийся антенны.

$G_{r,дБ}$ - Коэффициент усиления, принимающийся антенны.

$P_{\min,дБ}$-Реальная чувствительность приемника.

$L_{t,дБ}$ -Потери сигнала в коаксиальном кабеле и разъемах передающего тракта.

$L_{r,дБ}$ -Потери сигнала в коаксиальном кабеле и разъемах приемного тракта.

По графику, приведённому нами на рисунке 2.6, мы находим необходимую дальность работы беспроводного канала связи.

Разберем каждый параметр на примере:

- $P_{t,дБ}$ - мощность передатчика - мощность беспроводной точки доступа или адаптера в дБмВт. Эта информация берем из спецификации на оборудование. Для нашего оборудования D-LINK это значение от 15 дБм для обычных точек доступа и карт. (В нашем случае 20 дБм).

- $G_{t,дБ}$ - коэффициент усиления передающей антенны (дБи). D-LINK предлагает нам антенны для внешнего и внутреннего использования от 4 до 21 дБи. (В нашем случае он равен 5 Дби).

- $G_{r,дБ}$ - коэффициент усиления приемной антенны. Тоже что и $G_{t,дБ}$ но "на другой стороне" радиолинка.

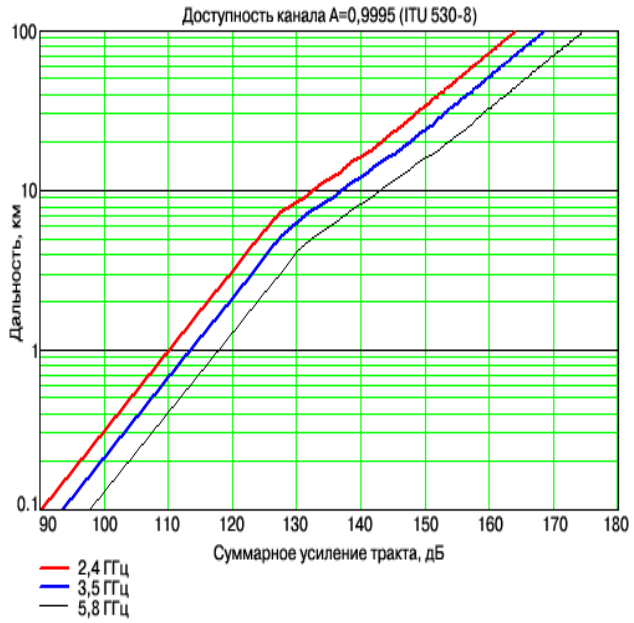


Рисунок 2.6 - Доступность канала

- $P_{\min,дБ}$ - чувствительность приемника, которую также можно найти в спецификации на оборудование. Чувствительность приемника всегда зависит от скорости, на котором работает оборудование и она задается со знаком "минус".

- $L_{t,дБ}$, $L_{r,дБ}$ - потери в коаксиальном кабеле и разъемах приемного или передающего тракта. Рассчитать потери можно следующим образом: предлагаемый кабель BELDEN 9880 имеет затухание 0,24 дБ/м т.е. при 5-метровой длине кабеля затухание в нем составит 1,2 дБ. Также следует прибавить к потерям по ~ 0,5 - 1,5 дБ на каждый разъем. Итого 10-метровый кабель между антенной и точкой доступа имеет потери $1.2 + 2 * 1{,}5 = 4.2$ дБ.

Поскольку расстояние между точками доступа одинаково, рассчитаем потери между двумя точками. Мы имеем три точки доступа DWL-3200AP. Оконечные точки находятся на одинаковом расстоянии от центральной, поэтому расчёт для каждой пары точек доступа будет одинаковым.

$P_{t,dB}$= 20 дБмВт.
$G_{t,dB}$= 5 дБи.
$G_{r,dB}$= 5 дБи.
$P_{\min,dB}$= -72 дБмВт.
$L_{t,dB}$= 4,2 дБ.
$L_{r,dB}$= 4,2 дБ.

Отсюда

$Y_{дБ}$ = 20+5+5-(-72)-4,2-4,2=93,6 дБ.

По графику (красная кривая для 2.4 ГГц) определяем соответствующую этому значению дальность. Получаем дальность равную ~110 метрам.

Мы проводили расчет для скорости 54 1 Мбит/с.

При скорости 1 Мбит/с:

$P_{\min,дБ}$= -94 дБмВт.

тогда

$Y_{дБ}$ = 20+5+5-(-94)-4,2-4,2=115,6 дБ.

По графику (верхняя кривая для 2.4 ГГц) определяем соответствующую этому значению дальность. Получаем дальность равную ~1100 метрам.

Рассчитаем суммарное усиление тракта для компьютеров находящихся в кабинетах. Кабинеты расположены симметрично относительно точки доступа подключаемой к серверу. Затухание вносимое железной дверью примем равным 7 дБ, тогда потери в каждом направлении:

$P_{t,dB}$= 20 дБмВт.

$G_{t,dB}$= 5 дБи.

$G_{r,dB}$= 2 дБи.

$P_{\min,dB}$= -71 дБмВт.

$L_{t,dB}$= 4,2 дБ.

$L_{r,dB}$= 7 дБ.

Отсюда

$Y_{дБ}$ =20+5+2-(-71)-4,2-7=86,8 дБ.

По графику (красная кривая для 2.4 ГГц) определяем соответствующую этому значению дальность. Получаем дальность равную ~80 метрам. Расчет для скорости 54 1 Мбит/с.

При скорости 1 Мбит/с:

$P_{\min,дБ}$= -92 дБмВт.

тогда

$Y_{дБ}$ = = 20+5+2-(-92)-4,2-7=107,8 дБ.

По графику (верхняя кривая для 2.4 ГГц) определяем соответствующую этому значению дальность. Получаем дальность равную ~600 метрам.

Этот расчёт также был произведён на языке программирования TurboPascal, листинг программы которого приведён в Приложении А.

2.3.2 Расчет по формуле.

Без вывода приведём формулу для расчёта дальности. Она берётся из инженерной формулы (2.2) расчёта потерь в свободном пространстве

$$FSL = 33 + 20(\lg F + \lg D) \qquad (2.2)$$

где FSL (freespaceloss) - потери в свободном пространстве (дБ).

F-центральная частота канала на котором работает система связи (МГц).

D-расстояние между двумя точками (км).

FSL определяется суммарным усилением системы. Оно считается следующим образом:

Общий прирост = Мощность передатчика (дБм) + | Чувствительность приемника (дБм) (по модулю) | + Коэффициенты . Uisleniya антенны

передатчик + приемник Коэффициент усиления антенны Коэффициенты - затухание в передатчике антенно-фидерных трактов - затухание в антенно-фидерных трактов приемника - SOM

Для каждой скорости , приемник имеет определенную чувствительность. Для малых скоростях (например, 1-2 мегабит) высшей чувствительности: -90 дБм до -94 дБм. Для более высоких скоростях , чувствительность намного меньше.

В зависимости от марки радиомодулей максимальная чувствительность могут незначительно отличаться. Ясно, что для различных скоростей максимального диапазона будет отличаться .

SOM (SystemOperatingMargin) - поставка энергии в радио (дБ) . Принимает во внимание возможные факторы , неблагоприятно воздействующих на дальность связи , таких как:

- Температурный коэффициент чувствительности приемника и выходная мощность передатчика .

- Все виды погодных аномалий : туман, снег, дождь .

- Несоответствие антенна, приемник, передатчик с антенно-фидерных трактов .

Параметр SOM берется 15 дБ . Считается, что 15 - децибел высота достаточна для инженерных расчетах .

Центральный канал частота F берется из таблицы 2.1.

Т а б л и ц а 2.1 - Вычисление центральной частоты

Канал	Центральная частота (МГц)
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472
14	2484

В итоге получим формулу дальности связи

$$D = 10^{\left(\frac{FSL}{20} - \frac{33}{20} - \lg F\right)} \qquad (2.3)$$

D=0.079 км =79 м.

2.4 Расчет зоны Френеля

Радиоволна в процессе распространения в пространстве занимает объем в виде эллипсоида вращения с максимальным радиусом в середине пролета, который называют зоной Френеля рисунок 2.7. Естественные (земля, холмы, деревья) и искусственные (здания, столбы) преграды, попадающие в это пространство, ослабляют сигнал.

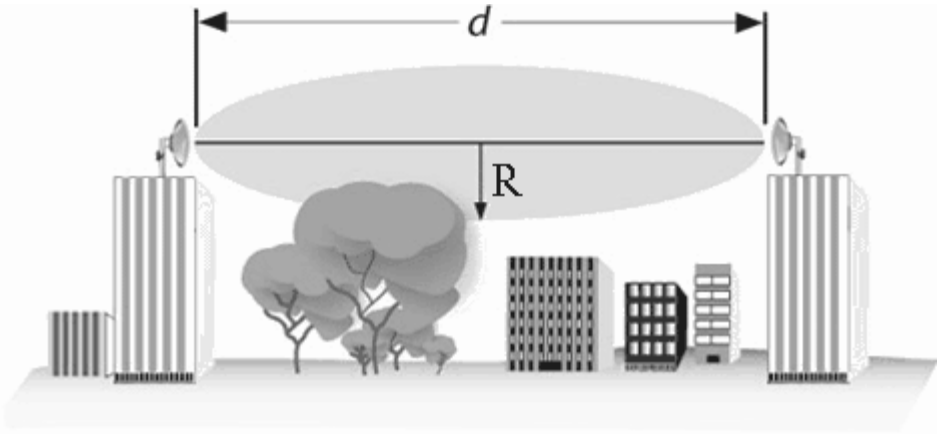


Рисунок 2.7- Зона Френеля

Радиус первой зоны Френеля в самой широкой части может быть рассчитан с помощью формулы

$$R = \sqrt{\frac{cSD}{f(S+D)}} \qquad (2.4)$$

где R-Радиус зоны Френеля (м).

S и D - Расстояние от антенн до замеряемой области (м).

f -Частота (Гц).

c - Скорость света (м/с).

$$R = \sqrt{\frac{3\cdot 10^8 \cdot 2\cdot 8}{2{,}4\cdot 10^9 (2+8)}} = 0{,}44\text{м} = 44\text{ см}.$$

Как правило, блокирующий 20% зоны Френеля вводит небольшое ослабление в канале. Более 40% ослабления сигнала уже значительное, избежать столкновения препятствий на пути распространения.

Этот расчет сделан на предположении, что Земля плоская. Это не учитывает кривизну земной поверхности. Для расширенным пакетом каналов должно быть всеобъемлющее урегулирование, с учетом местности и

естественные преграды на пути распространения. Когда расстояние между антеннами должен попытаться увеличить высоту подвески антенн с учетом кривизны земной поверхности.

2.5 Анализ потерь сигнала в свободном пространстве

Одной из проблема сигнала является физическое повреждение контактов либо же физическое воздействие на них из вне к примеру если поставить возле кабеля радиочастотный передатчик, то возможно в канале начнутся потери данных, которые приведут к ухудшению качеству связи либо приведут к периодическим прерываниям сигнала сети Данный тип затухания называют потерями в свободном пространстве и вычисляют через отношение мощности излучённого сигнала P_t к мощности полученного сигнала P_r. Для вычисления того же значения децибелах следует взять десятичный логарифм от указанного отношения, после чего умножить полученный результат на 10.

Для идеальной изотропной антенны потери в свободном пространстве составляют

$$\frac{P_t}{P_r} = \frac{(4\pi d)^2}{\lambda^2} = \frac{(4\pi f^2 d)^2}{c^2} \tag{2.5}$$

где P_t-Мощность сигнала передающей антенны.

P_r-Мощность сигнала, поступающего на антенну приемника.

λ-Длина волны несущей;

d-Расстояние, пройденное сигналом между двумя антеннами.

c-Скорость света ($\approx 3 \cdot 10^8$ м/с).

Приведённое выражение можно записать в следующем виде

$$L_{дБ} = 10\lg\frac{P_t}{P_r} = 20\lg\left(\frac{4\pi d}{\lambda}\right) = 20\lg\left(\frac{4\pi f d}{c}\right) \tag{2.6}$$

Рисунок 2.6 показывает зависимость потери сигнала в свободном пространстве расстояния.

Используется в этой работе являются антенны на расстоянии 10 м друг от друга. На графике, показанном на рисунке 2.6 показывает зависимость затухания от расстояний между антеннами от 1 км. На основе этого исследования дро изменения затухания на расстояниях менее 1 км от несущей частоты 2,4 ГГц.

Зависимость затухания зависимости от расстояния между антеннами примет форму

$$L_{дБ} = 20\lg\left(\frac{4\pi \cdot 24d}{3}\right) = 20\lg(32\pi d) \qquad (2.7)$$

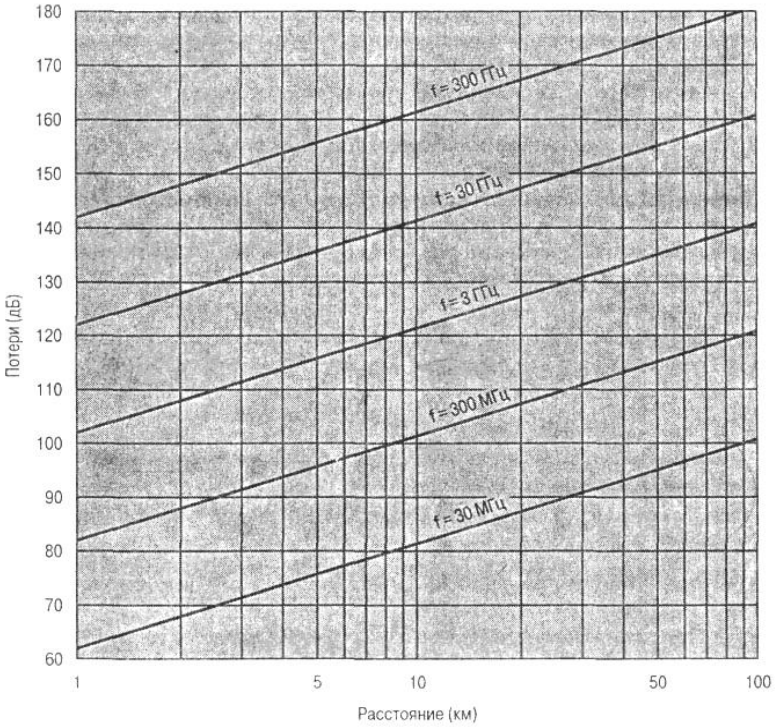


Рисунок 2.8- Потери мощности сигнала

Полученные параметры расчётов занесём в таблицу 2.2.

Таблица 2.2- Полученные параметры расчётов

Расстояние d, км	Потери L, дБ
10	60,04
110	80,87
210	86,49
310	89,87
410	92,30
510	94,19
610	95,75
710	97,07
810	98,21
910	99,22
1010	100,13

Изходя из полученных данных построим график зависимости представленный на рисунке 2.9.

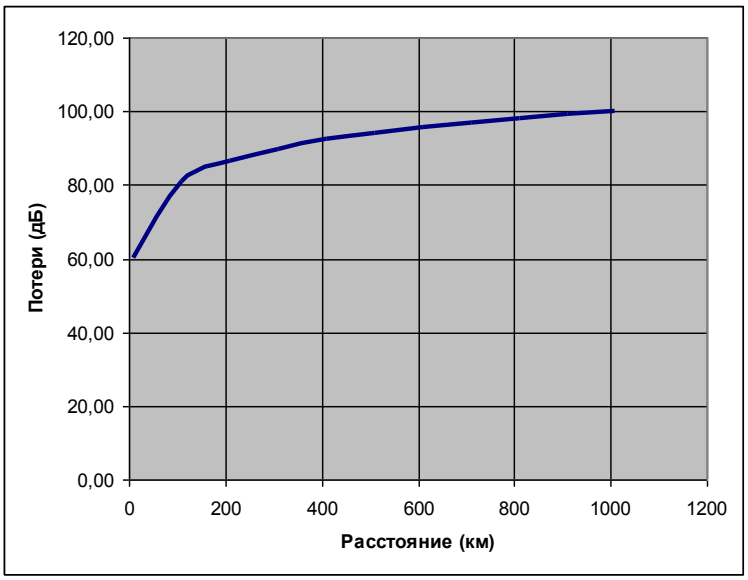


Рисунок 2.9- График зависимости потерь от расстояния

Этот расчёт также был произведён на языке программирования TurboPascal, листинг программы которого приведён в Приложении А.

2.6 Расчёт шумов

Для любого утверждения передачи данных , что принимаемый сигнал состоит из переданного сигнала , модифицированного различными искажений, вносимых системы,передачи , а также дополнительные нежелательные сигналы , которые взаимодействуют с исходной волны при распространении от точки передачи в точку приема . Эти нежелательные сигналы называются шум . Шум является основным фактором, ограничивающим производительность систем связи.

Шум можно разделить на четыре категории :

- Тепловой шум .
- Интермодуляция шума .
- Перекрестные помехи .
- Импульсный шум .

Тепловой шум является результатом теплового движения электронов . Этот тип вмешательства влияет на все электрические устройства , а на среду передачи электромагнитных сигналов . Тепловой шум является функцией температуры и равномерно распределены по частотному спектру , так что этот тип шума также называют белым шумом. Тепловой шум не могут быть устранены , так что он определяет верхний предел производительности систем связи. Тепловой шум оказывает значительное воздействие на системы спутниковой связи , так как сигнал, полученный от спутниковой наземной станции , является слабым.

Тепловой шум присутствует в полосе 1 Гц , для любого устройства или

проводника

$$N_0 = kT \tag{2.8}$$

где N_0 - плотность мощности шумов в ваттах на 1 Гц полосы.

k -постоянная Больцмана, $k = 1{,}3803 \times 10^{-23}$ $Дж/К$.

T - температура в Кельвинах (абсолютная температура).

Считается, что шум не зависит от частоты. Следовательно, тепловой шум, присутствовавший в полосе диапазона В Гц, можно выразить следующим образом:

$$N = kTB. \tag{2.9}$$

Запишем данное выражение, используя децибел-ватты

$$N = 10\lg k + 10\lg T + 10\lg B \tag{2.10}$$

Ширину канала Wi -Fiпримем равной 5 МГц, остда по формуле (2.10)

$$N = 10\lg 1.38 \cdot 10^{-23} + 10\lg 293 + 10\lg 5 \cdot 10^{6} = -137 \text{ (Вт/Гц)}.$$

Если сигналы разной частоты передаются в одной среде, может иметь место интермодуляционный шум. Интермодуляционным шумом являются помеха, возникающие на частотах, которые представляют собой сумму, разность или произведение частот двух исходных сигналов. Например, смешивание двух сигналов, передаваемых на частотах f_1 и f_2 соответственно, может привести к передаче энергии на частоте $f_1 + f_2$. При этом данный паразитный сигнал может интерферировать с сигналом связи, передаваемым на частоте $f_1 + f_2$.

Интермодуляция шум вызван нелинейности приемника, передатчика, или промежуточную систему передачи. Как правило, все эти компоненты ведут себя как линейной системы, то есть их выходную мощность, равную входного сигнала, умноженной на константу. Для вывода нелинейных систем является более сложной функцией входной мощности. Нелинейность может быть вызвано неисправностью одного из частей сигнала с использованием чрезмерной силы или просто природу усилителя. Для этих случаев интерференция происходит на частотах, суммы и разности частот исходных сигналов.

С перекрестных помех встречается каждый, кто использовать телефон во время переменно услышал разговор незнакомых людей. Этот тип помех возникает от нежелательных путей передачи объединение. Это объединение может быть вызвано муфты близко расположенных витых пар, которые несут несколько сигналов. Перекрестные помехи могут возникнуть при приеме

посторонние сигналы микроволновых антенн. Хотя этот тип соединения с помощью направленного точность антенны, потери мощности во время распространения сигнала по-прежнему невозможно избежать. Как правило, перекрестные помехи мощность порядка (или ниже) мощности теплового шума. Все вышеперечисленные виды вмешательства характеризуются относительно предсказуемой и постоянной мощности. Таким образом, можно спроектировать систему для передачи сигнала, который был бы устойчивы к этим помехам.

Однако, помимо указанных выше типов помех, есть так называемые переходные, которые по своей природе являются прерывистыми и состоят из нерегулярный пульс или краткосрочного шума пакетов относительно высокой амплитудой. Причины импульсных помех может быть установлен, в том числе внешних электромагнитных воздействий (например, молния) или дефектов (повреждений), большинство из системы связи.

3Защита беспроводных сетей

3.1 Защита данных

По мере увеличения числа поставщиков и производителей, которые предпочитают беспроводную технологию, последняя чаще изображается как инструмент, способный спасти мир от современного компьютера Гнев его провода.

Разработчики беспроводной заметил рифы в своих водах, в результате первых робких попыток завоевать мир беспроводных технологий не удалось. Препятствие к широкому распространению беспроводных технологий, то есть, таким образом, "Риф", стал достаточно высокий уровень безопасности.

3.2 Методы сети защиты стандартные IEEE 802.11 (рекомендации)

Конечно, вопрос о безопасности далеко нетривиальная, и подойти к решению этой проблемы, необходимо определить возможные меры и средства, чтобы сделать беспроводную сеть как можно более безопасным. Таким образом, мы должны:

- Уменьшить зону покрытия (конечно, до самого низкого приемлемо). В идеале, зона покрытия сети не должна выходить за контролируемой зоне.
- Измените пароль администратора по умолчанию.
- Включить фильтрацию по MAC-адресам.
- Запретить вещания идентификатор сети (SSID).
- Измените идентификатор сети (SSID), по умолчанию.
- Периодически меняйте идентификатор сети (SSID).
- Активировать функцию WEP.
- Периодически менять WEP-ключ.
- Установка и настройка персональных брандмауэров и антивирусного программного обеспечения для абонентов беспроводной сети.
- Заполните соответствующие параметры для фильтрации трафика на телекоммуникационного оборудования и сетевых экранов.
- Обеспечить резервное оборудование входящее в состав беспроводной сети
- Обеспечение резервного копирования и аппаратных конфигураций.
- Выполните периодический контроль состояния безопасности беспроводной сети с использованием специализированных инструментов для анализа безопасности.

Все эти методы защиты могут быть реализованы сегодня практически на любой аппаратной производителя представлены в беспроводной 802,11 и имеющие логотип Wi-Fi. Мы называем вышеуказанных комплексных мер защиты "начальная" уровня, ниже которого абсолютно не может быть опущена

при проектировании сети беспроводного предприятия.

Даже если весь комплекс мер реализована, учитывая известные технические и технологические проблемы протокола WER, и, как следствие, низкий уровень сложности взлома такой сети, беспроводной сети с «начальной» уровня безопасности лучше всего видно, насколько незащищенной сети. Как следствие, точка сети (даже при использовании WEP) доступ не соединяются с внутренней проводной сети, - они должны быть на внешней стороне брандмауэра. Таким образом, обработка конфиденциальной информации в сети, описанной выше исходного уровня безопасности невозможно.

Чтобы исправить эту ситуацию, некоторые производители (например, AgereSystems, D-Link, США робототехника,), с целью улучшения базовый уровень безопасности, предлагают использовать более длинные ключи шифрования протокола WEP - 128, 152 или даже 256 бит. Но это часто приводит к недостаточной совместимости с другими производителями 802.11 оборудования.

Многие эксперты считают, что необходимо заменить WEP шифрования инструменты более прочными.

Таким образом, осведомленность о проблемах WEP не пришел вчера, поэтому сегодня на рынке есть решения, чтобы сделать использование WEP безопаснее. Например:

- Использование некоторых стандартных протоколов 802.1x, решает проблему динамического изменения ключи шифрования для беспроводных устройств.

- Протокол MIC для защиты WEP-пакеты на их изменения и подделки в процессе передачи.

- Протокол TKIP, также разработаны для улучшения протокола безопасности WEP, предполагает использование уникальной комбинации клавиш для каждого устройства, а также обеспечивает динамическую клавишу схеме каждые 10000 пакетов. Тем не менее, как и WEP, TKIP использует протокол шифрования криптографический алгоритм RC4.

Обратимся теперь к вопросу о безопасности обмена информацией пользователей беспроводной сети с корпоративным сетевым ресурсам. Чтобы решить эту проблему, нам необходимо реализовать беспроводную аутентификации пользователя в сети, и использовать более сильные методы безопасности, которые могут обеспечить необходимый уровень конфиденциальности и целостности информации. Один из таких способов является установка сервера управления доступом с помощью стандартных протоколов с целью EAP/802.1h беспроводные абоненты усиленной аутентификации. Следует четко понимать, что в нашей сети могут представлять различные категории пользователей (заказчиков), которым необходимо предоставить различные права на доступ к определенным ресурсам. Самый простой пример показан на рисунке 3.1.

Очевидно, что после аутентификации абонента беспроводной сети,

необходимо будет назначать соответствующую категорию своей политики безопасности. Одна из возможных реализаций этого подхода является использование технологии, и определенный стандарт 802.1q позволяет авторизованным пользователям размещать беспроводную сеть в различных VirtualLAN (VLAN) с ранее определенной политики безопасности для каждой из VLAN (в зависимости от типа человек).

Абоненты беспроводной сети	Доступ к конфиденциальной информации	Доступ к публичной информации (в т.ч. Internet)
Сотрудник	+	+
Гость	-	-
Злоумышленник	-	-

Рисунок 3.1- Права доступа различных категорий пользователей

Так, в дополнение к использованию методы базового уровня защиты означает строгую аутентификацию через 802.1x и средства повышения протокол безопасности WEP, сегодня мы можем достичь приемлемого уровня защиты информации, циркулирующей в беспроводной сети. К сожалению, эти решения могут предложить довольно узкий круг компаний. В первую очередь - это лидер на рынке беспроводных сетей оборудования. И бесспорным законодателем мод на рынке решений для обеспечения безопасности беспроводных сетей является CiscoSustems компании.

Отметим также, что реализация средств защиты в популярных операционных систем может существенно "подтянуть" уровень безопасности для беспроводных сетей, в частности путем удаления этого "головную боль" с производителями оборудования. Но вопрос о совместимости конкретных реализаций протокола различных производителей остается открытым.

При условии, что использование современного оборудования и программного обеспечения в настоящее время можно построить на основе стандартов серии безопасности 802.11x и сопротивление, чтобы напасть на беспроводную сеть, которая необходима для реализации его в течение нескольких разумных постулатов.

Мы должны помнить, что почти всегда связано с беспроводной сетью и проводной его, помимо необходимости защиты беспроводных каналов является стимулом для внедрения новых методов для защиты беспроводных сетей. В противном случае сеть будет иметь фрагментарный защиту, что, по сути, представляет собой угрозу безопасности. Желательно использовать оборудование с сертифицированной Wi-FiCertified, т.е. подтверждение того, что WPA.

Протокол WPA хотя уязвимы, но это намного сложнее взломать. Тот факт, что успех взлома секретного WPA-ключ зависит от ее наличие или нет в

словаре. Стандартный словарь, который описан, имеет размер чуть более 40 МБ, что, в общем, не так много. В результате, после нескольких попыток, вы можете забрать ключ, который отсутствует в словаре, и ключ будет невозможно взломать. Для исчерпывающего ключа потребовалось два с половиной часа. Количество слов в словаре - только 6475760, что, конечно, очень мало. Конечно, можно использовать словари и большую емкость. Но даже эти словари содержат не все возможные пароли. Если примерно подсчитать количество паролей между 8 до 63 символов, которые могут быть получены с использованием 26 букв английского алфавита (с учетом регистра), десять цифр и 32 буквы русского алфавита, мы находим, что каждый персонаж может выбрать 126 способов . Соответственно, если мы будем рассматривать только пароли длиной до 8 символов, число возможных комбинаций составляет 12 · 68 = 6,3 · 1016. Если учесть, что размер каждого разрядности 8 составляет 8 байт, то получим, что размер из словаря -4500000 терабайт. Но это только комбинация из восьми символов. А если попробовать все возможные комбинации между 8 до 63 символов, размер словаря будет примерно 1,2 · 10119 терабайт. Конечно, это пространство не существует. Но даже если мы гипотетически предположить, что такой словарь создан, то перебора всех ключей на нашем компьютере потребует не менее 1,8 · 10 120 лет. На самом деле, такая задача не по зубам любой самого мощного суперкомпьютера. Но следует отметить, одну особенность, связанную с использованием WPA: в конце 2003 года, мы выпустили исследование, в котором фраза короче 20 символов и состоящий исключительно из слов в словаре, которые могут быть расшифрованы. Вывод прост: использовать длинные ключевые фразы, включить их в номера, и пунктуация. Лучше всего, это был беспорядок символов.

Рисунок 3.2 показывает пример комплексного применения средств правовой защиты в беспроводных сетях (от начального до специализированных средств).

Тем не менее, считался только один возможный пример нарушая ключ со словарем, но, как отмечалось выше, существуют и другие виды атак.

Многие администраторы, установив сетевое устройство, оставить заводские установки по умолчанию, это категорически недопустимо в серьезных беспроводных сетей.

Должен быть объединены в качестве протокола и методов защиты программного обеспечения и административной. Это имеет смысл подумать о реализации технологии IntrusionDetectionSystems (IDS) или специальных пакетов программ для выявления возможных вторжений.

Для создания надежной системы безопасности беспроводной сети разработали множество методов. Например, самый надежный способ заключается в использовании виртуальной частной сети VPN (VirtualPrivateNetwork). Создание беспроводной виртуальной частной сети шлюз предусматривает установку непосредственно перед установкой точки доступа и VPN-клиентов сети рабочие станции пользователей. Администрация по виртуальной частной

сети настроен виртуальной частной соединение (VPN-туннель) между шлюзом и каждым VPN-клиента сети.

Рисунок 3.2 - Пример применения средств защиты в беспроводных сетях.

Как всегда, вопрос обеспечения необходимого уровня безопасности и для удобства и простоты использования отличаются масштабы. "Плато" в случае технологии VPN является снижение общей пропускной способности сети, сложности агентов VPN-поиска и криптографической ядро при использовании карманных компьютеров (КПК) и / или беспроводные IP-телефоны, увеличивая общую стоимость решения.

Тем не менее, VPN-сети редко используются в небольших офисных сетей, и не используются в домашних условиях. Как протокола 802.1x, VPN-сети-прерогативой корпоративных сетей.

Теперь, когда все основные вопросы, обсуждавшиеся на последний раз видели, как архитектура может выглядеть защищенной сети передачи данных, принимая во внимание все выше; Пример показан на рисунке 3.3.

Взятые вместе, все выше, ответ очевиден - с помощью беспроводных сетей безопасно и удобно, если это использовать все доступные средства для обеспечения безопасности. Конечно, вероятность разрыва сети есть всегда, и главным критерием интерес для злоумышленника в сети является ее стоимость. Чтобы «открыть» даже WEP-шифрование требует, по крайней мере, Wi-Fi-ноутбук и знания. Во всех остальных случаях возможность получения несанкционированного доступа к сети зависит от ценности информации, содержащейся в нем (в конце концов, он должен окупить стоимость взлома). Что касается WPA, а затем использовать этот протокол в сочетании с другими средствами защиты (фильтрация по MAC-адресам, запрет вещания SSID, используйте 802.1x протокола аутентификации, EAP) для небольших сетей вполне достаточно. В случае смешанной сети, чтобы использовать виртуальные локальные сети; с внешним антенная технология используется для виртуальных частных сетей VPN.

Мораль: прежде чем принимать определенные меры безопасности, возможно, взвесить все последствия. При планировании защищенной

беспроводной сети, вы должны помнить, что любой шифрования или другой обработки данных неизбежно приведет к дальнейшим задержкам, увеличить количество трафика маршрутизации и процессора накладных расходов сетевых устройств. Безопасность - безусловно, важный фактор в современных сетях, но это теряет всякий смысл, если трафик пользователя не было быть пропускная способность. Сети, в конечном счете не для администраторов и пользователей.

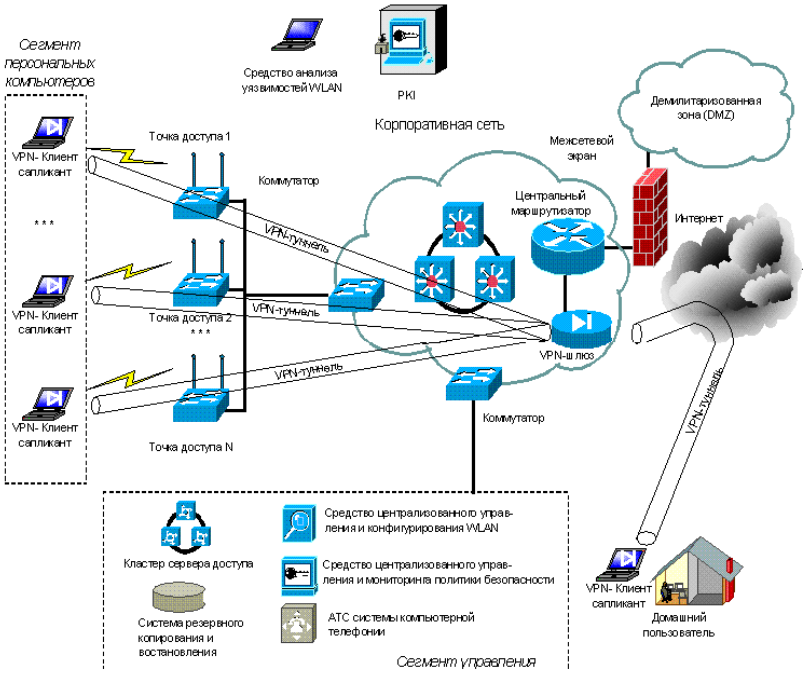


Рисунок 3.3 – Пример схемы защищенного беспроводного сегмента корпоративной сети.

3.3 Программное обеспечение

Решения, предлагаемые различными производителями для защиты беспроводных сетей. Программное обеспечение позволяет достичь трех целей:

- Найти другим, то есть провести инвентаризацию беспроводной сети для обнаружения несанкционированных точек доступа и беспроводных клиентов, которые могут прослушивать трафик и вклинивается в помолвки.

- Проверьте, что является контроль параметров качества, и рекомендовать пути для устранения дыры в уставном набор беспроводных устройств.

- Защитите свой, то есть для предотвращения несанкционированного доступа и атак на беспроводном сегменте сети узлов (Рисунок 3.4).

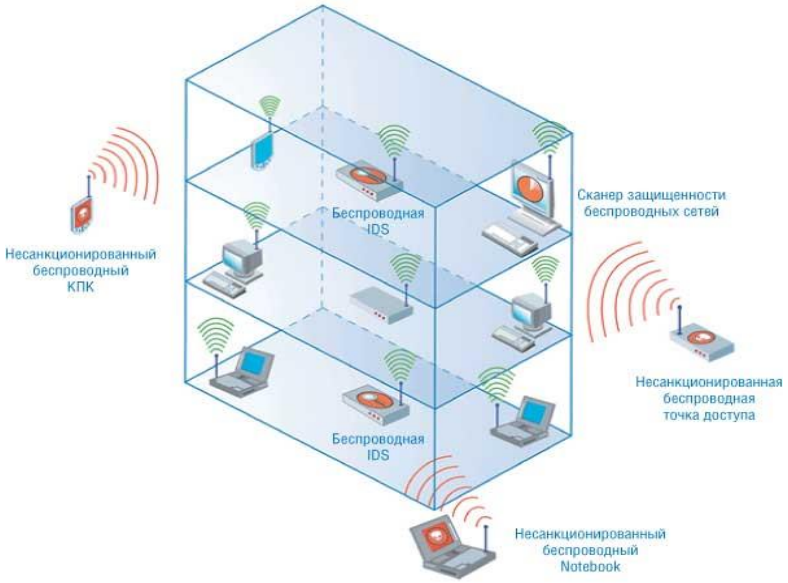


Рисунок 3.4 - Беспроводная сеть

3.4 Инвентаризация беспроводной сети

Первый , и наиболее распространенная , проблема может быть решена с помощью большого количества инструментов - NetStumbler , Wellenreiter , WifiScanner и другие , а также через сканеры безопасности беспроводных сетей , а также ряд систем обнаружения вторжений .

Пионер инвентаризации беспроводного оборудования NetStumbler , который работает под управлением ОС Windows 9x/2000/XP и позволяет не только очень быстро найти все незащищенные беспроводные точки доступа , но и проникнуть в сеть, предположительно , защищенное с WEP. Подобные проблемы решаются WifiScanner , PrismStumbler и многие другие продукты с открытым исходным кодом . В связи с этим , интересная система Wellenreiter , который также ищет беспроводных клиентов и точек доступа . Однако, если вы подключите его к GPS- приемнику , система приобретает безграничные возможности , вы можете не только определить все несанкционированные беспроводные устройства, установленные , но и знать их местонахождение с точностью до метра . Еще одной отличительной особенностью этой системы является ее способность работать на Pocket PC.

В наглядной форме представляет свои заключения красных Видение система от компании красно- М , которая не только обнаруживает точку доступа , но и визуально организовать их в шаблон вашего помещения компании . В брошюрах красно- М пользователи обещают : " Мы откроем вам глаза на беспроводной технологии ! "

3.5 Анализ защищенности беспроводных устройств

Поиск дыр в беспроводных устройствах осуществляют многие утилиты и инструменты, но, как правило, поиск дыр ограничивается попыткой взлома

ключей шифрования WEP, и не более того. По такому принципу, например, действуют AirSnort и WEPCrack.

Более интересен специализированный инструментарий, обеспечивающий всесторонний аудит беспроводных устройств. Таких продуктов сегодня немного. Если быть точным, то только один -WirelessScanner от компании InternetSecuritySystems, вид интерфейса системы WirelessScanner представлен на рисунке 3.5

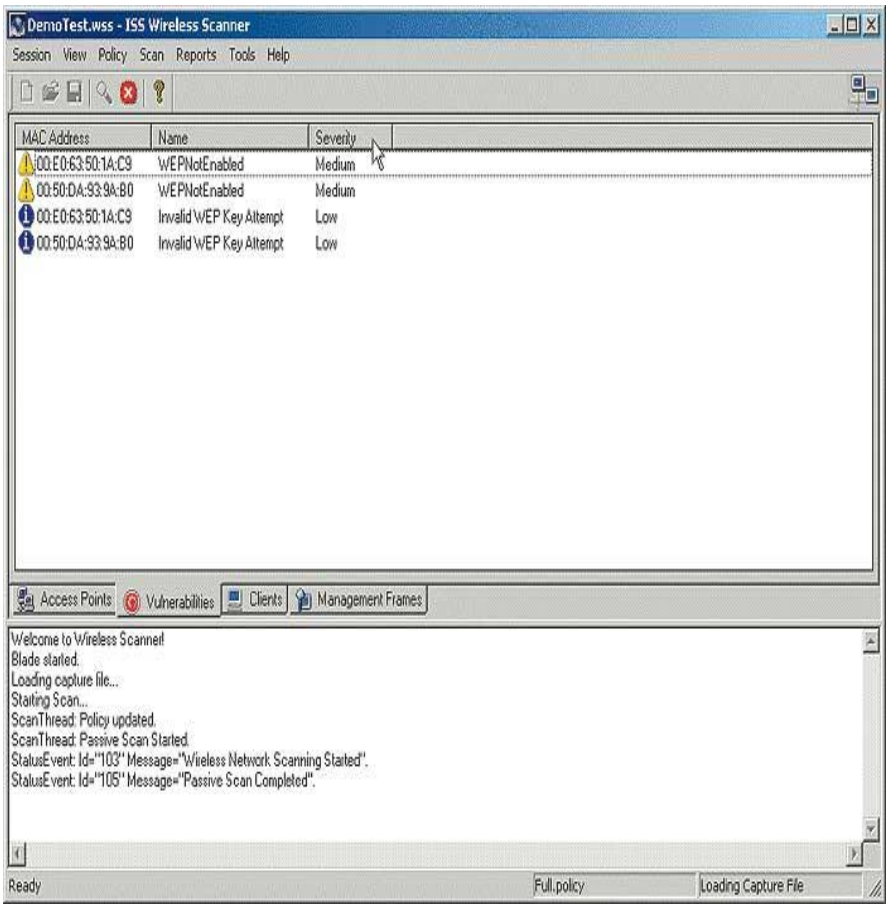


Рисунок 3.5 - Интерфейс системы WirelessScanner

Эта система, базирующаяся на широко известном и самом первом в мире сетевом сканере безопасности InternetScanner, проводит инвентаризацию сети и обнаруживает все санкционировано и несанкционированно установленные беспроводные точки доступа и клиенты. После этого проводится всесторонний анализ каждого устройства с целью определения любых слабых мест в системе защиты - недостатков в настройке или ошибок программирования. В базу сигнатур уязвимостей WirelessScannerвходит большое число записей о дырах в решениях ведущих игроков этого рынка -Cisco, Avaya, 3Com, Lucent, Cabletron и т.д. В гораздо меньшем объеме проверку проводит WirelessSecurityAuditor(WSA) - программный продукт от компании IBM. Пока это только прототип, и трудно сказать, каков будет окончательный результат усилий разработчиков. Как и вышеназванные системы, WSA проводит

инвентаризацию сети и анализирует конфигурацию обнаруженных устройств в плане безопасности.

3.6 Обнаружение атак на беспроводные сети

После обнаружения иностранных устройств и устранения их отверстия для пользователей сталкиваются с задачей, чтобы обеспечить непрерывное беспроводной безопасности и своевременное обнаружение атак на его узлов. Эта проблема решается с помощью системы обнаружения вторжений, из которых есть также достаточно, чтобы задуматься над выбором .. Что касается беспроводных сетей очень трудно провести различие между сканера, сети инвентаризация и системы обнаружения вторжений, а под большинство производителей понимают обнаружение выявление изгоев точек доступа. Различие между ними состоит лишь в том, что сканеры выполнить эту задачу по команде или с заданными временными интервалами и системы обнаружения непрерывно контролировать сеть.

Airsnare система от компании DigitalMatrix. Он отслеживает MAC-адресов всех пакетов, передаваемых в беспроводном сегменте, а в случае иностранной адрес указывает на это, а также для определения IP-адрес несанкционированного соединительному узлу. Включает интересный модуль Airhorn, которая позволяет злоумышленнику послать сообщение, что он вторгся в чужие владения и стоит их быстро, если он не нуждается в дополнительных проблем.

Лидер рынка системы беспроводной безопасности можно назвать AirDefense же компания, которая позволяет:

- Автоматическое определение всех подключенных беспроводных устройств к сети.
- Построить карту сети, указывающую расположение точек беспроводных устройств.
- Изменения (инвалиды, украденные, инвалиды и т.д.) в рамках беспроводных устройств Track.
- Монитор сетевого трафика передается в беспроводном сегменте, и обнаружить ее различные аномалии.
- Сбор информации для исследований, связанных с несанкционированной активности.
- Обнаружение разнообразные атак и попытки сканирования.
- Отслеживание отклонения в параметрах политики безопасности и беспроводных устройств.

4 Технико-Экономическое Обоснование

4.1 Преимущества беспроводной сети

В данном проекте рассматривается проектирование беспроводной сети на базе технологии Wi-Fi.

Беспроводные локальные сети все больше становятся популярными среди современных пользователей. В каждый несколько лет они проводит процесс стандартизации, повышалась скорость передачи данных, цена с каждым годом становилось доступней.

Сегодня беспроводные сети позволяют предоставить подключение пользователей там, где затруднено кабельное подключение или необходима полная мобильность. При этом беспроводные сети взаимодействуют с проводными сетями. В настоящее время необходимо принимать во внимание беспроводные решения при проектировании любых сетей - от малого офиса до предприятия. Это, возможно, сэкономит и средства и трудозатраты и время.

Постоянно расширяющийся спектр оборудования, усовершенствование стандартов и улучшение защиты делает возможным применение Wi-Fi практически в любом месте. Новейшее оборудование соответствует высоким требованиям безопасности, стабильности и высокой скорости.

Беспроводные сети позволяют предоставить подключение пользователей там, где затруднено кабельное подключение или необходима полная мобильность. При этом беспроводные сети могут взаимодействовать с проводными сетями. В настоящее время необходимо принимать во внимание беспроводные решения при проектировании любых сетей - от малого офиса до предприятия. Это, возможно, сэкономит и средства и трудозатраты и время.

Преимущества Wi-Fi:

- Отсутствие проводов. Передача данных в сети осуществляется по воздуху на очень высокой частоте, которая не воздействует на человека и не создает помехи для электронной техники.
- Мобильность. Так как беспроводная сеть не привязана к проводам, Вы можете свободно изменять местоположение Ваших компьютеров в зоне покрытия точки доступа, не беспокоясь о нарушениях связи. Сеть легко монтируется и демонтируется, при переезде в другое помещение Вы можете даже забрать свою сеть с собой.
- Уникальность технологии. Возможна установка в местах, где прокладка проводной сети по тем или иным причинам невозможна или нецелесообразна, например, на выставках, залах для совещаний.

4.2 Исследование мировых достижений в области беспроводных сетей

Есть немало причин восхищаться тем, как быстро развивается индустрия беспроводных сетей. По данным компании SynergyResearchGroup, объем

мирового рынка этих сетей вырос с 600 млн. долларов в 2000 году до 2,8 млрд. долларов в 2012 году. Рост продаж, выражающийся числом беспроводных устройств, выглядит еще более впечатляющим. Этому способствует быстрое снижение цен на них. Набирает силу тенденция к встраиванию интерфейсов Wi-Fi в мобильные компьютерные и коммуникационные устройства, включая ноутбуки, карманные ПК и смартфоны. Проведенная корпорацией Intel маркетинговая компания по продвижению на рынок средств для беспроводных сетей оказалось успешной, и многие потребители обратили внимание на технологию Wi-Fi. Почти все сетевые специалисты уверены в том, что рынок услуг беспроводной передачи данных будет развиваться и дальше и технологии Wi-Fi суждено сыграть в этом весьма важную роль.

По данным консалтингового агентства Pyramid Research, которое исследовало пользователей беспроводных сетей в США, в настоящее время их насчитывается 14,2 млн., а к 2007 году это число возрастет до 31 млн. Что же касается мирового распространения данной технологии PyramidResearch прогнозирует, что к концу 2006 года число абонентов услуг Wi-Fi во всем мире достигнет 707 млн. человек и превысит число абонентов услуг других видов доступа, а также число абонентов услуг доступа в Интернет операторов сотовой связи.

4.3 Организация беспроводной сети в ТОО «Регион-А»

Организационный план является неотъемлемой частью бизнес-плана.

В данном проекте будет произведен расчет затрат на покупку, доставку, установку и запуск оборудования беспроводной сети на базе технологии Wi-Fi, производства компании D-Link. Оборудование этой компании очень хорошо зарекомендовали себя на рынке информационных технологий своей надежностью, функциональностью и гибкостью систем. Так же будет проведен сравнение с технологией от компаний Cisco.

Сегодня компании могут предложить оборудование для построения сети Wi-Fi стандарта IEEE 802.11a/g/n:

1) Программноеобеспечение (OperationsSupportSystem (OSS)). Программное обеспечение сервера заведует всеми функциям: конфигурацией, авторизацией. Сервер OSS удаленно управляет всеми сессиями пользователей для публичного доступа в пределах сети рекламного агентства.

2) Коммутатор. Для агрегирования трафика в проекте используется коммутатор 2-го уровня. В качестве такого устройства выбрано оборудование DES-3526-24-SMI-PoE.

3) Точка доступа (AccessPoint). В качестве точки доступа используется оборудование D-Link DWL-3200 AP WirelessAccessPoint 802.11b/g, работающее в диапазоне 2,4 до 2,4835 ГГц соответствующее рекомендациям IEEE 802.11b и g (Wi-Fi). Радиус покрытия одной точки доступа составляет до 400 метров вне помещения и может масштабироваться за счет установки дополнительных точек доступа.

4) Беспроводные Wi-Fi адаптеры. В качестве беспроводных Wi-Fi адаптеров будут использоваться устройство D-Link DWL-G520 WirelessAdapter 802.11g, а также встроенные беспроводные адаптеры в ноутбуках сотрудниках фирмы.

Для осуществления данного проекта необходимо будет установить 3 точки доступа в здании. Наименование и стоимость оборудования для построения сети по 1 варианту приведен в таблице 4.1.

Таблица 4.1 - Наименование и стоимость оборудования для построения сети по 1 варианту

Наименование оборудования	Количество	Цена, тенге	Стоимость, тенге
Программноеобеспечение Operations Support System	1	29832	29832
Точка доступа D-Link DWL-3200 AP	3	20570	61710
Беспроводной адаптер D-Link DWL-G520	16	6100	97600
Коммутатор DES-3526-24-ports	2	47740	95480
Кабель UTPCat.5E катушка 305 м	1	13071	13071
Розетка RJ-45 DIN двойная UTPCat.5E	16	745	11920
Итого	309613		

Общая стоимость оборудования составляет 309613 тенге.

Компания Cisco является безусловным лидером в классе оборудования для построения надежных, высокопроизводительных и защищенных беспроводных сетей в помещениях.

Основными критериями выбора оборудования для построения корпоративной Wi-Fi сети являются безопасность, управляемость и функциональность. Серия CiscoAironet отвечает этим критериям в полной мере.

1)Программноеобеспечение (OperationsSupportSystem (OSS)). Программное обеспечение сервера заведует всеми функциям: конфигурацией, авторизацией. Сервер OSS удаленно управляет всеми сессиями пользователей для публичного доступа в пределах сети рекламного агентства.

2) Коммутатор. Catalyst 3750G с поддержкой удаленного питания 24 или 48 точек доступа и интегрированным контроллером.

3)Точка доступа (Access Point). AIR-AP1131AG.Два радиоинтерфейса - 802.11a и 802.11b/g с возможностью одновременной работы Интегрированная мультидиапазонная всенаправленная антенна 3 dB Остальные характеристики - аналогично AIR-AP1131G.

4)Беспроводные Wi-Fi адаптеры. Cisco Aironet 802.11a/b/g CardBus Wireless LAN Client Adapter. Беспроводной адаптер CiscoAironet формата

CardBus, работающий в сетях стандарта 802.11a/b/g, обеспечивает высокоскоростную связь 54 Мбит/с в диапазоне 2.4 и 5 ГГц.

Наименование и стоимость оборудования для построения сети по 2 варианту приведен в таблице 4.2.

Таблица 4.2 - Наименование и стоимость оборудования для построения сети по 2 варианту

Наименование оборудования	Количество	Цена, тенге	Стоимость, тенге
Программноеобеспечение Operations Support System	1	29832	29832
Точка доступа AIR-AP1131AG	3	60725	182175
Беспроводной адаптер Cisco Aironet 802.11a/b/g	16	4365	69840
Коммутатор Catalyst 3750G – 24 port	2	1 463 000	2926000
Кабель UTPCat.5E катушка 305 м	1	13071	13071
Розетка RJ-45 DIN двойная UTPCat.5E	16	745	11920
Итого	3232838		

Общая стоимость оборудования составляет 3232838 тенге.

Если сравнивать построение сети с помощью компаний Cisco и D-Link любой блеснет тем, что знает случай, когда существует то или иное решение, которое проще, дешевле, лучше, ,быстрее, чем решение от Cisco. Вот только шаг влево, шаг вправо от этого решения, и становится гораздо труднее подыскать замену.

Охват. У решений Cisco нет конкурентов по этому параметру. Наиболее широкая линейка по всем сетевым решениям, от рынка SOHO до провайдерских решений, от небольших, но функциональных маршрутизаторов, до систем управления сетями крупных предприятий.

Основные направления:

1) Многофункциональные маршрутизаторы.
2) Мощные, умные коммутаторы.
3) Устройства активной защиты - ASA, ACE.
4) Системы предотвращения вторжений - IPS.
5) Системы централизованного беспроводного доступа.
6) Унифицированные коммуникации (VoIP, видеоконференции, telepresence, системы управления звонками).
7) Системы централизованной защиты хостов (CSA).
8) Система контроля доступа (NAC).

9) И все, что вы можете придумать ещё :).

Главное -Cisco не останавливается на достигнутом и «держит нос по ветру», придумывая новые проекты и вкладывая в них денги, например, покупая перспективные разработки и встраивая их в свои решения. Таки образом, получив поддержку такого гиганта, у интересных решений есть шанс пробиться «в люди».

Надёжность. Ломается всё, вопрос только когда. Надёжность cisco проверена годами успешной эксплуатации. Врать не буду - и у Cisco бывали неудачные серии, неудачные релизы операционных систем, однако в целом отказоустойчивость сомнений не вызывает.

Гибкость. Одно и то же железо, в зависимости от операционной системы и набивки модулями, может выполнять совершенно различные функции: защитные, шлюза унифицированных коммуникаций, сервисные… А это значит, что если захочется чего то нового, есть большой шанс ничего не покупать, а просто набрать несколько команд.

Взаимозависимость. Кривое слово, но оно отражает суть. Разные железки, выполняющие разные функции, могут зависеть друг от друга и управлять друг другом. Это позволяет сделать сеть живым организмом, а не набором разрозненных устройств.

Отладка. Очень важно для настройки и настройщиков: широчайшие возможности по поиску неисправностей, встроенные практически во все устройства Cisco.

Интеллектуальность. Трудно продать просто дорогое железо. Надо продавать идею и возможности. Все устройства Cisco содержат широкий спектр технологий, протоколов, идеологий, как стандартных, так и своих собственных, позволяющих расширить возможности сети.

Производительность. Компания Cisco является лидером во многих сегментах рынка и должна соответствовать этому высокому званию. Поэтому появляются уникальные решения, типа CRS (одной такой железки достаточно, чтобы обеспечить связью, скажем, всю Великобританию!). Сейчас топовые решения с 10 гигабитными интерфейсами есть и в сегменте межсетевых экранов, и в сегменте маршрутизаторов, и в сегменте систем предотвращения вторжений.

Централизация. Устройствами Cisco можно управлять не по одиночке, а использую мощные комплексы, например, ciscosecuritymanager. Также централизованно можно собирать всевозможнейшую статистику и анализировать её - MARS. Подобного решения по централизации учёта пока никто ещё не предложил.

Но даже имя такие достоинства есть существенный недостаток – это стоимость обородувание. Из-за свой дороговизны не каждая компония может позволить установку Cisco , и его обслуживание.

У D-link Во-первых, плюсы:

- Оборудование из класса эконом, его цена варьирует от 3000 до 10000 тенге, в разных магазинах. Доступность. Его легко можно найти в любом городе, так как фирма и модель очень распространена.
- Стабильность стандарт Wi-Fi. Работает в наиболее распространенном стандарте- 802.11n. Присутствие DHCP-сервера тоже радует. Web-интерфейс.
- Во-вторых, минусы:
- Температура. При длительной работе сам роутер не греется, а вот его блок питания греется.

4.4 Капитальные затраты

Капитальные затраты определим по формуле (4.1)

$$K = K_{вб} + Кус + K_{у} \quad (4.1)$$

где$К_{вб}$-Кап вложение на оборудование.

$К_{ус}$-Кап вложение установки сети.

$К_{У}$ -Стоимость монтажа и установки оборудования (5% от стоимости оборудования).

Вариант 1:

кап вложения на сети в соответствие с данными таблицы 4.1 составляют 309613 тенге.

Кап вложения на оборудование составляют 583690 тенге. Общий перечень оборудования, необходимого для организации работы сети на местах представлена в таблице 4.3.

Т а б л и ц а 4.3 – Кап вложения на оборудования

Наименование	Цена, тенге	Количество	Стоимость, тенге
Компьютер (системный блок, монитор)	43 909	10	439090
Компьютерный стол	9 500	10	95000
Стул	2 500	10	25000
Шкаф	12 300	2	24600
Итого:			583690

Капитальные вложения на монтаж рассчитывается по формуле

$$К_{у}= К_{у}*0,05 \quad (4.2)$$

и составляют

$К_{у}$=309613*0,05=15480тенге.

Таким образом, общая сумма капитальных вложений по первому варианту реализации проекта составят

К = 309613 + 583690 + 15480 = 908783 тенге.

Капитальные затраты по 1 варианту составили 908783 тенге и приведена в таблице 4.4.

Т а б л и ц а 4.4 - Капитальные затраты

Наименование затрат	Стоимость, тенге	Удельный вес, %
Стоимость капитальное вложение обо	309 613	34,07
Стоимость рабочих мест, (Км)	583 690	64,23
Установка и монтаж оборудования, (Ку)	15 4806,5	1,70
Итого	908783	100,00

Вариант 2:

кап вложения на сети в соответствие с данными таблицы 4.2 составляют 3232838 тенге.

Кап вложения на оборудование составляют 583690 тенге. Общий перечень оборудования, необходимого для организации работы сети на местах представлина в таблице 4.3

Капитальные вложения на монтаж согласно по формуле 4.2 составят:

$К_у$=3232838*0.05=161641 тенге.

Таким образом, общая сумма капитальных вложений по второму варианту реализации проекта составят:

К = 3232838 + 583690 + 161641 = 3978169тенге.

Капитальные затраты по 1 варианту составили 3978169 тенге и приведена в таблице 4.5.

Т а б л и ц а 4.5 - Капитальные затраты

Наименование затрат	Стоимость, тенге	Удельный вес, %
Стоимость оборудования, (Ц)	3232838	81,2
Стоимость рабочих мест, ($К_м$)	583 690	14,6
Установка и монтаж оборудования, ($К_у$)	161641	4,2
Итого	3978169	100,00

4.5 Расчет годовых эксплуатационных расходов

Эксплуатационные расходы определим по формуле

$$Э = ЗП + А + М + С_{ЭЛ} + С_{АДМ}, \quad (4.3)$$

где ЗП - основная и дополнительная заработная плата персонала с отчислением на социальное налог.

А - Амортизационные отчисления.

М - Затраты на материалы и запасные части.

$С_{ЭЛ}$ - Электроэнергия со стороны производственных нужд.

$С_{АДМ}$ - Прочие административные управленческие и эксплуатационные расходы.

Для вычисления заработной платы в таблице 4.6 приведем среднемесячные оклады обслуживающего персонала.

В годовой фонд заработной платы включается дополнительная заработная плата (работа в праздничные дни, сверхурочные и т.д.) в размере 30% от основной заработной платы.

Т а б л и ц а 4.6 – Среднемесячные оклады обслуживающего персонала

Список персонала	Количество	Ежемесячная зарплата, тенге	Зарплата в год, тенге	Всего, тенге
Сетевой администратор	1	80 000	960000	960000
Инженер	2	60 000	1440000	1440000
Итого	2400000			

Дополнительная заработная плата составляет 10% от основной заработной платы и рассчитывается по формуле

$$ЗП_{ДОП} = ЗП_{ОСН} * 0,1 \quad (4.4)$$

где $ЗП_{ОСН}$ - годовой фонд основной заработной платы.

Подставив значения в (4.4) найдем годовой фонд дополнительной заработной платы

$ЗП_{ДОП}$ = 2400000*0,1 = 240000тенге.

Фонд оплаты труда складывается из основной и дополнительной заработной платы

$$ФОТ = ЗП_{ОСН} + ЗП_{ДОП} \quad (4.5)$$

Определим фонд оплаты труда по формуле (4.5)

ФОТ = 2400000+ 240000= 2640000 тенге.

4.5.1 Расчет затрат по социальному налогу

Социальный налог составляет 11% (ст. 358 п. 1 НК РК) от дохода работника, и расчитывается по формуле

$$С_Н=(ФОТ-ПО)*0,1 \qquad (4.6)$$

где ПО- пенсионные отчисления, которые составляют 10% от ФОТ о социалным налогом не облагаются ирасчитывается по формуле

$$ПО=ФОТ*10\% \qquad (4.7)$$

ПО=2640000*0,1=264000 тенге.

Таким образом в целом сумма отчислений на социальные нужды составит:

$С_Н$=(2640000-264000)*0,1=237600 тенге.

Суммарная заработная плата с учетом отчислений на социальный налог:

ЗП = ФОТ + $С_Н$=2640000+264000=2904000 тенге.

4.5.2 Расчет амортизационных отчислений

Сумма амортизационных отчислений начисляется по единым нормам, которые устанавливаются в процентах от стоимости основных фондов формула (4.7)

$$A_0 = \frac{ф \cdot H_A}{100\%} \qquad (4.8)$$

где Ф -Балансовая стоимость основных фондов, тенге.

$Н_А$ -Норма амортизационных отчислений.

Найдем амортизационные отчисления для оборудования, компьютеров и офисной мебели из (4.8).

Для оборудования для построения сети амортизация составляет 25% от цены оборудования:

По варианту 1:
$A_{1D\text{-}link}$ = 309 613*0,25= 77 403 тенге.

По варианту 2:
A_{1Cisco}=3232838*0,25=808209 тенге.

Амортизация компьютеров составляет 40% от цены:

A_2 = 439 090*0,4 = 175 636 тенге.

Амортизация офисной мебели составляет 15% от цены:

A_3 = 144 600*0,15 = 21 690 тенге.

По варианту 1:

$A_{D\text{-}link} = A_1 + A_2 + A_3$ = 77 403+ 175 636+ 21 690 = 274 729 тенге.

По варианту 2:

$A_{Cisco} = A_1 + A_2 + A_3$ = 808209+ 175 636+ 21 690 = 1005535 тенге.

4.5.3 Расчет затрат на электроэнергию

Затраты на электроэнергию рассчитаем по следующей формуле

$$C_{ЭЛ.} = W*T*S \quad (4.9)$$

где W- Потребляемая мощность W = 1210 Вт.
T - Количество часов работы T = 8760 ч/год.
S - Стоимость киловатт-часа электроэнергии S = 15 тенге / кВт-час.

Рассчитаем затраты на электроэнергию по формуле (4.9)

$C_{ЭЛ}$ = 1,210*8760*15 = 162936 тенге.

Мощность, потребляемая на прочие нужды, берется в размере 5% от мощности, потребляемой основным оборудованием.
Стоимость электроэнергии, потребляемой на прочие нужды:

$C_{ЭЛ.пр}$= $C_{эл}$*0,05 = 8146 тенге.

Общие затраты на электроэнергию:

$С_{эл.общ} = С_{эл} + С_{ЭЛ.пр}$= 162936 + 8146 = 171082 тенге.

4.5.4 Расчет затрат на материалы и запасные части

Затраты на материалы и запасные части принимают в размере 5% от стоимости системы:

По варианту 1:

$М_{D\text{-}link}$ = 309 613*0,05 = 15481 тенге.

По варианту 2:

$М_{Cisco}$ = 3232838*0,05 = 161641 тенге.

4.5.5 Расчет стоимость административных расходов

Стоимость административных расходов составляет 10% от ФОТ:

$С_{АДМ}$ = ФОТ*10% = 2640000*0,10 = 264000 тенге.

Таким образом, эксплуатационные расходы исходя из (4.7,4.8) составят:

По варианту 1:

$Э_{D\text{-}link}$ = 2904000+ 274 729 + 171082+ 15 481+ 264000 = 3629292 тенге.

По варианту 2:

$Э_{Cisco}$ = 2904000+ 1005535+ 171082+ 161641+ 264000 = 4506258 тенге.

Расчеты эксплуатационных работпо вариантам 1 и 2в таблицах 4.7-4.8 и определим удельный вес каждой статьи расходов.

Т а б л и ц а 4.7 – Эксплуатационные расходы D-link (вариант 1)

Статьи эксплуатационных затрат	Стоимость, тенге	Удельный вес, %
Заработная плата персонала	2904000	80
Амортизационные отчисления	274729	9,4
Затраты на материалы и запасные части	15481	0,4
Затраты на электроэнергию	171082	4,7
Административные расходы	264000	5,5
Итого:	3629292	100,00

Т а б л и ц а 4.8 – Эксплуатационные расходы Cisco (вариант 2)

Статьи эксплуатационных затрат	Стоимость, тенге	Удельный вес, %
Заработная плата персонала	2904000	64,4
Амортизационные отчисления	1005535	22,3
Затраты на материалы и запасные части	161641	3,5
Затраты на электроэнергию	171082	3,7
Административные расходы	264000	7,1
Итого:	4506258	100,00

4.5.6 Расчетоценки эффективности реализаций проекта

Оценка эффективности проекта осуществляется на основе на минимума приведённых затрат рассчитывается по формуле (4.9).

Приведённые затраты по каждому i-му варианту представляют собой сумму себестоимости Ci и удельных капитальных вложений Куді, приведённых к годовой размерности в соответствии с нормативным коэффициентом сравнительной эффективности Ен.

$$Зi = Ci + ЕнКуд_i \rightarrow \text{минимум} \quad (4.10)$$

где Ci -Приведённые затраты по каждому i-му варианту представляют собой сумму себестоимости.

$Куд_i$-Удельные капитальные вложение.

Ен-Коэффициентом сравнительной эффективности(20%).

По варианту 1 приведенные затраты составят:

$З_1 = С_1 + ЕнКуд_1$ =3629292+0.2*309613=3691214 тенге.

По варианту 2приведенные затраты составят:

$З_2 = С_2 + ЕнКуд_2$ =4506258+0.2*3232838=5152825тенге.

Т а б л и ц а 4.9- Сравнение 2-х вариантов

Варианты	Кап.затраты тг.	Эксп-ные расходы тг.	Приведенные затраты, тг.
Вариант 1 D-link	908783	3629292	3691214
Вариант 2 Cisco	3978169	4506258	5152825

Как видите на таблице 4.9 приведенные затраты по 1-му варианту реализаций проекта меньше 2-го на 1461611 тенге, и поэтому рекомендуется для внедрения, как наиболее оптимальный.

5 Безопасность жизнедеятельности

5.1 Анализ условий труда

Оборудование сервера проектируемой локальной сети размещается на третьем этаже пятиэтажного здания в помещении ЦРБ. Высота этажей 3.2 м. Стены кабинета покрашены в белый цвет, и имеются большие окна и верхние люминесцентные лампы. Поэтому помещение производит светлое, легкое впечатление, не смотря на тот факт что окна выходят на северную сторону. Верхнее освещение работает даже днем, и чтобы снизить вредное влияния на зрение двух разнотипных источника света, в кабинете имеются плотные жалюзи. План помещения и размещения оборудования показан на рисунке 5.1.

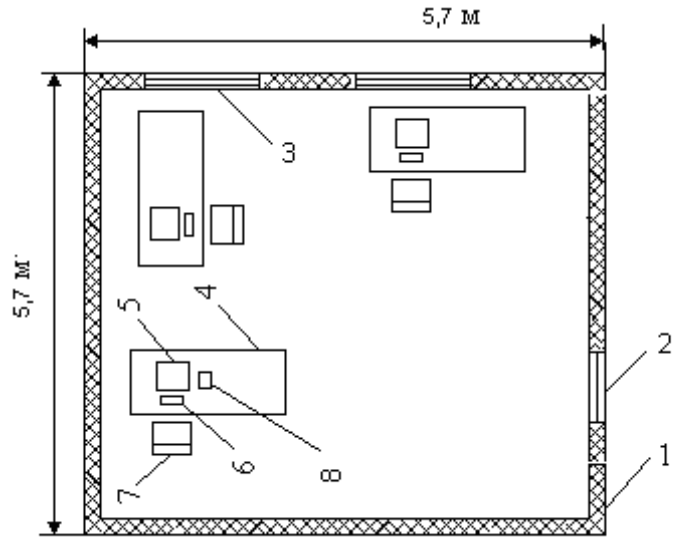


Рисунок 5.1 - План помещения и размещения оборудования

где 1 -Стена.
2 - Дверной проем.
3 -Окно деревянное двойное раздельное.
4 -Компьютерный стол.
5 - Компьютер.
6 - Клавиатура.
7 - Стул.
8 -Точка доступа Wi-Fi.

В помещении «серверной» помимо места системного администратора находится 5 рабочих мест, и поэтому максимальное число находящихся в «серверной» человек равно 6.

Площадь комнаты контроля $S_{контр}$=5.7·5.7=32.49 м^2, объем - $V_{контр}$=32.49·3.2=103.97 м^3. На одного человека приходится площадь 32,49/6= 5,42 м^2 и объем 17,33 м^3. Это больше минимальных площади и объема

приходящихся на одного работающего, установленных нормами (объем - не менее 15 $м^3$, площадь - не менее 4.5 $м^2$).

Согласно, ГОСТ 12.1.005-88 работы, производимые системным администратором, относятся к категории I б лёгкой физической (Таблица 5.1).

Аппаратура, установленная в «серверной» выделяет большое количество тепла. В результате в летнее время года помещение нуждается в выводе избыточного тепла. Для создания нормального микроклимата в помещениях установлены настенные кондиционеры, характеристики которых показана в таблице 5.2. Они охлаждают воздух, автоматически поддерживать заданную температуру, изменять скорость движения воздушного потока и направлять его, обеспечивая воздухообмен с наружной средой.

Т а б л и ц а 5.1 - Категории работ по энергозатратам организма

Работа	Категория	Энергозатраты организма, Дж/с	Характеристика работы
Легкая физическая	I б	138 – 172	Производится сидя, стоя или связана с ходьбой и сопровождается некоторым физическим напряжением

Т а б л и ц а 5.2 - Характеристики установленных кондиционеров

Модель	Мощность охлаждения, кВт	Мощность нагрева, кВт	Мощность потребляемая, кВт	Расход воздуха, куб.м/час
SANYO SAP-K181GJHA	5	5.75	2.25/1.96	760

Оптимальные нормы параметров микроклимата в холодный и тёплый периоды года с учётом категории работы приведены в таблице 5.3. Регулирование параметров микроклимата производится автоматически по регулируемым характеристикам. Изменение контролируемых характеристик производится оператором.

Т а б л и ц а 5.3 - Оптимальные нормы параметров микроклимата

Период работы	Температура, ^0C	Скорость движения воздуха, м/с, не более
Холодный	21-23	0.1
Теплый	22-24	0.2

В качестве нагревательных приборов в обоих помещениях установлены регистры из гладких труб. Имеющаяся система кондиционирования

поддерживает температуру в пределах оптимальных норм параметром микроклимата. В помещения подается объем наружного воздуха до 100 куб.м на одного рабочего. Скорость движения воздуха в помещениях в любой период года не превышает 0.1 м/с.

Поэтому микроклиматические условия обслуживания оборудования согласно ГОСТ 12.0.003-74 охарактеризованы как оптимальные.

5.1.1 Оценка освещенности

Работа системного администратора в основном заключается в управлении и наблюдении за аппаратурой и при необходимости устранении мелких неполадок в работе оборудования. Таким образом, выполняемую работу операторов относим к работе со средней точностью, т.е. к IV разряду зрительной работы.

Естественное освещение создается благодаря двум окнам размерами 170×240 см, окна начинаются с высоты один метр. В качестве свет пропускающего материала имеем стекло оконное листовое двойное. В качестве солнцезащитного устройства используются убирающиеся регулируемые жалюзи.

Так как окна выходят на теневую сторону и из-за климатических условий, в помещениях принята система общего освещения четырьмя светильниками по четыре люминесцентные лампы II группы ЛД, мощностью 40 Вт и световым потоком $Ф_л$=2340 лм, уровень освещенности которых 150 лк.

Оптимальные параметры освещенности помещений приведены в таблице 5.4.

Для достижения уровня нормируемой освещенности - 300 лк, соответствующей IV разряду зрительной работы увеличивается количество источников света.

Т а б л и ц а 5.4 - Оптимальные параметры освещенности помещений

характеристика зрительной работы	Разряд	Контраст объекта с фоном	Характеристике фона	При комбинированном освещении, лк	При общем освещении, лк
Средней точности 0.5-1.0	IV	большой	светлый	300	304

5.1.2Оценка пожарной безопасности

В помещении существует вероятность возникновения пожара, причина которых:

- Неисправности электропроводки, розеток и выключателей которые приводят к короткому замыканию или пробою изоляции.
- Использование неисправных (поврежденных) электроприборов.
- Возникновение пожара вследствие попадания молнии в здание.
- Возгорание здания вследствие внешних воздействий.

В помещении имеется огнетушитель ОП-10, предназначенный для тушения пожаров и загораний нефтепродуктов, ЛВЖ и ГЖ, растворителей, твердых веществ, а также электроустановок под напряжением до 1000 В.

Исходя из приведенного анализа, для помещения проводится реконструкция системы освещения и разрабатывается меры по профилактике пожара и план эвакуации людей.

Для исключения возникновения пожара по приведенным выше причинам:

- Вовремя выявляются повреждения в электропроводке, проводится плановый осмотр, и своевременно устраняются все неисправности.
- Своевременно проводится качественный ремонт электроприборов, и не используются неисправные электроприборы.
- На станции проводится противопожарный инструктаж, на котором работников знакомят с правилами противопожарной безопасности, а также обучают использованию первичных средств пожаротушения.

На третьем этаже здания одновременно находятся более 20 человек, поэтому разработаны и на видных местах вывешены планы (схемы) эвакуации людей в случае пожара, а также предусмотрена система (установка) оповещения людей о пожаре. План эвакуации приведен на рисунке 5.2.

Необходимое время эвакуации людей из производственных зданий (мин) приведено в таблице 5.5. Наше предприятие относится к категории В.

Таблица 5.5 - Необходимое время эвакуации людей из производственных зданий (мин)

Категория производства	Объем помещений, тыс.м^3				
	до 15	30	40	50	60 и более
А, Б, Е	0,50	0,75	1	1,5	1,75
В	1,25	2	2	2,5	3
Г,Д	не ограничивается				

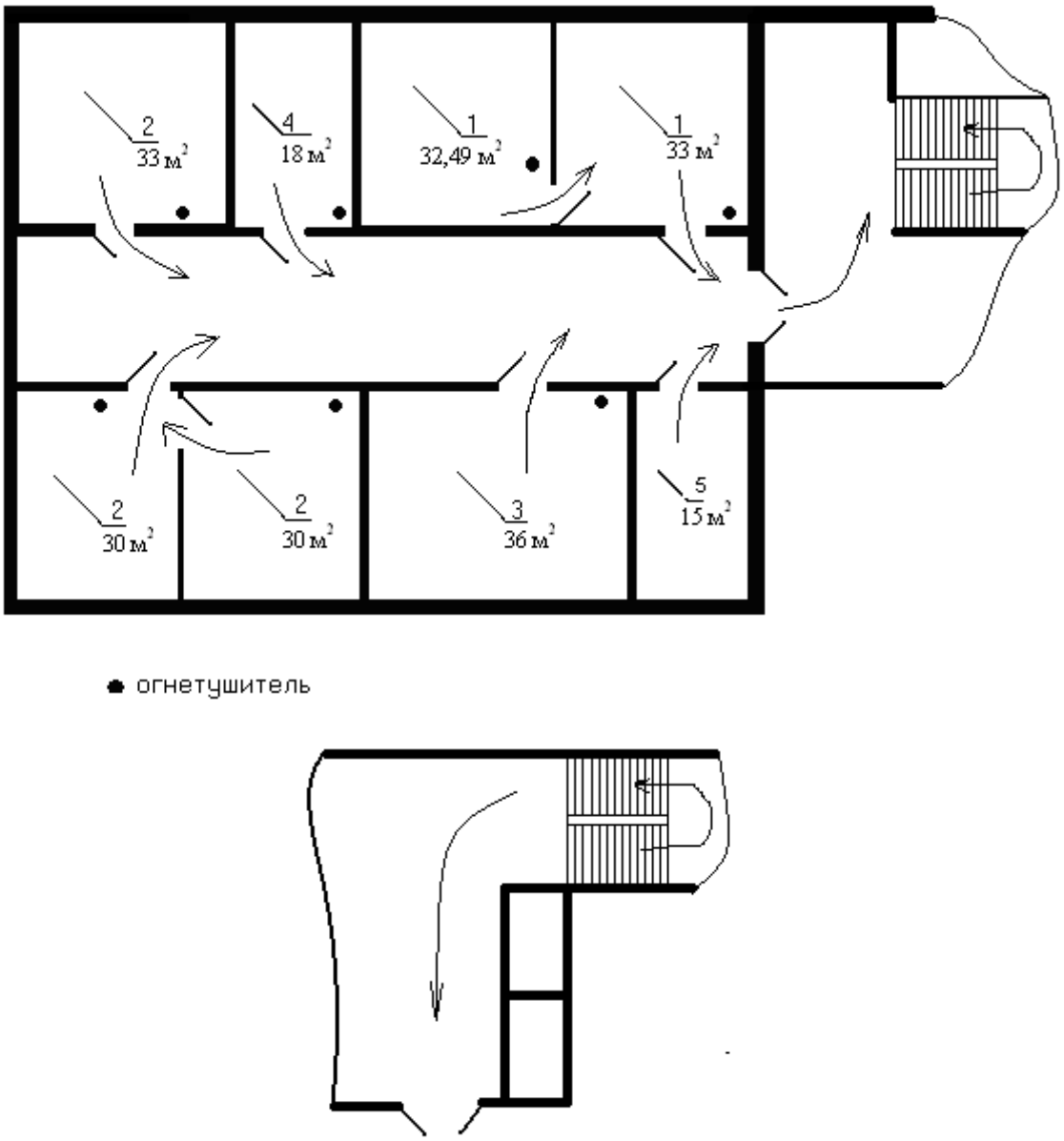


Рисунок 5.2 - Действующий план эвакуации из помещения ЦРБ

5.2 Обеспечение общих условий электробезопасности

Существуют следующие способы защиты, применяемые отдельно или в сочетании друг с другом: защитное заземление, зануление, защитное отключение, электрическое разделение сетей разного напряжения, применение малого напряжения, изоляция токоведущих частей, выравнивание потенциалов.

В электроустановках (ЭУ) напряжением до 1000 В с изолированной нейтрально и в ЭУ постоянного тока с изолированной средней точкой применяют защитное заземление в сочетании с контролем изоляции или защитное отключение.

В этих электроустановках сеть напряжением до 1000В, связанную с сетью напряжением выше 1000 В через трансформатор, защищают от появления в

этой сети высокого напряжения при повреждении изоляции между обмотками низшего и высшего напряжения пробивным предохранителем, который может быть установлен в каждой фазе на стороне низшего напряжения трансформатора.

В электроустановках напряжением до 1000 В с глухо заземлённой нейтрально или заземленной средней точкой в ЭУ постоянного тока применяется зануление или защитное отключение. В этих ЭУ заземление корпусов электроприемников без их заземления запрещается.

Защитное отключение применяется в качестве основного или дополнительного способа защиты в случае, если не может быть обеспечена безопасность применением защитного заземления или зануления или их применение вызывает трудности.

Защитное заземление. Заземлением (Рисунок 5.3) называется соединение с землей нетоковедущих металлических частей электрооборудования через металлические детали, закладываемые в землю и называемые заземлителями, и детали, прокладываемые между заземлителями и корпусами электрооборудования, называемые заземляющими проводниками.

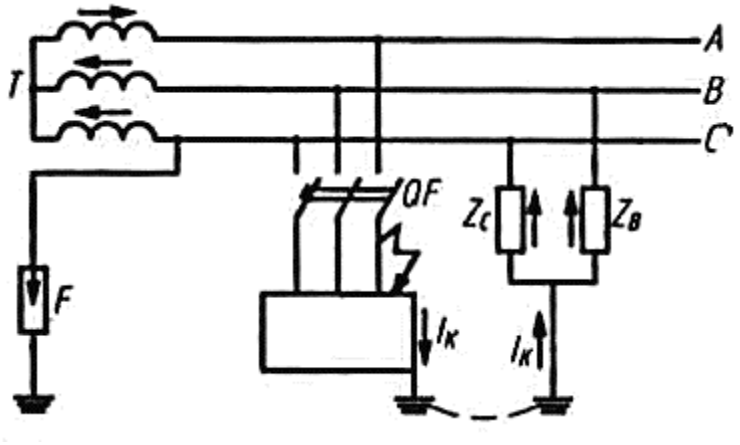


Рисунок 5.3 - Схема заземления в сети с изолированной нейтралью при наличии короткого замыкания

где Z_c, $Z_в$ - Полные сопротивления проводов относительно земли.

Iк -Ток короткого замыкания.

F-Разрядник.

Проводники и заземлители обычно делаются из низкоуглеродистой стали, называемой в просторечии железом.

Заземлители в виде штырей, вбиваемых в землю, называются электродами, и могут быть одиночными или групповыми. К характеристикам заземлителя относятся:

- Напряжение на заземлителе.

- Изменение потенциалов точек в земле вокруг заземлителя в зависимости от их расстояния от заземлителя в зоне растекания тока - вид потенциальной кривой.

- Вид линий равного потенциала - эквипотенциальных линий на поверхности земли.

- Сопротивление заземляющего устройства.

- Напряжения прикосновения и шага.

Принцип расчета защитного заземления сводится к определению общего сопротивления заземления устройства Rз. Rз нормируют при Uс<1кВ Rз≤10Ом при Ри.п<100кВА; Rз≤4Ом при Ри.п>100кВА; при Uс>1кВ Rз≤0,5Ом.

Необходимо рассчитать сопротивление защитного заземления электропитающего устройства предприятия связи, распределяющего электроэнергию напряжением 380/220 Заземляющее устройство должно использовать естественные заземлители (части металлических конструкций, находящиеся в земле), сопротивление растеканию которых R_e=20 Ом.

Требуемое сопротивление защитного заземляющего устройства для этого случая (ГОСТ 464-79) должно быть не более 4 Ом, т.е. Rз≤4 Ома. Следовательно, дополнительно к естественному заземлителю монтируется искусственный из вертикальных стальных стержней длиной L=2,5 м, диаметром d=12 мм, верхние концы которых соединяются стальной полосой сечением 20х4 мм^2, уложенной в грунт с удельным сопротивлением ρ =140 Ом*м на глубине t_0=0,5 м.

Контурный заземлитель размещается по периметру здания предприятия связи, длина которого $L_г$=70 м.

При расстоянии между заземлителями, а=5 необходимое количество вертикальных электродов n=70/5=14.

Требуемое сопротивление искусственного заземляющего устройства

$$R_{И.ТР.} = \frac{R_e R_з}{R_e - R_з} \quad (5.1)$$

$R_{И.ТР.}$=20*4/(20-4)=5 Ом

Сопротивление растеканию вертикальных (R) и горизонтальных (R_n) электродов

$$R = \frac{\rho}{2\pi L}(\ln\frac{2L}{d} + \frac{1}{2}\ln\frac{4t+L}{4t-L}) \quad (5.2)$$

$$R = \frac{140}{2*3{,}14*2{,}5}(\ln\frac{2*2{,}5}{0{,}012} + \frac{1}{2}\ln\frac{4*1{,}75+2.5}{4*1{,}75-2{,}5}) = 55\,\text{Ом}$$

$$R_n = \frac{\rho}{2\pi L_Г} \ln \frac{L_Г^2}{0{,}5b * t_0} \qquad (5.3)$$

$$R_n = \frac{140}{2*3{,}14*70} \ln \frac{2*70^2}{0{,}5*0{,}0004*0{,}5} = 6\ Ом.$$

Сопротивление растеканию группового искусственного заземлителя

$$R_{è} = \frac{RR_n}{(R\eta_{å} + R_n\eta_{ç}n)} \qquad (5.4)$$

$$R_{и} = \frac{55*6}{(55*0{,}36 + 6*0{,}66*14)} = 4{,}4 \text{ Ом}$$

Это сопротивление несколько меньше заданного (5 Ом), что повышает безопасность.

Общее сопротивление (действительное) заземляющего устройства

$$R_{З.Д} = \frac{R_e R_и}{(R_e + R_и)} \quad (5.5)$$

$$R_{З.Д.} = \frac{20*4{,}4}{20 + 4{,}4} = 3{,}66 \text{ Ом}$$

Что меньше требуемого по ГОСТ 464-79.

Заключение

В данном проекте были рассмотрены вопросы организации и создание локальной сети в здании ТОО «Регион-А» по технологии Wi-Fi.

Данная технология была выбрана как альтернатива проводной сети. Преимущества Wi-Fi в его высокой мобильности, простоте развертывания и установки оборудования, гибкости архитектуры сети, быстроте проектирования и реализации.

В частности были рассмотрены такие важные вопросы, как организация доступа к сети, подключение локальных сетей к глобальным сетям типа Internet, доступ к электронным библиотекам и базам данных, организация виртуальных локальных сетей и защита сетей от несанкционированного использования информации.

В проекте применен принцип одноточечного административного управления локальной вычислительной сетью.

Рассмотренные вопросы представляют большой практический интерес. На сегодняшний день разработка и внедрение локальных вычислительных сетей является одной из самых интересных и важных задач в области информационных технологий и потому количество растет с каждым годом. Все больше возрастает стоимость информации и зависимость предприятий от оперативной и достоверной информации. В связи с этим появляется потребность в использовании новейших технологий передачи информации, и появление новых стандартов. Сетевые технологии очень быстро развиваются, в связи с чем, они начинают выделяться в отдельную информационную отрасль.

СПИСОК ЛИТЕРАТУРЫ

1 Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник. - Санкт-Петербург: Питер, 2001.

2 Щербо В.К. Стандарты вычислительных сетей. - М.: Кудиц - Образ, 2000.

3 Педжман Рошан, Джонатан Лиэри. Основы построения беспроводных локальных сетей стандарта 802.11.: Практическое руководство по изучению, разработке и использованию беспроводных ЛВС стандарта 802.11. / Cisco Press Перевод с английского: - М.: Издательский дом «Вильямс»,2004.

4 Шахнович И. Современные технологии беспроводной связи - М.: Техносфера, 2004.

5 Григорьев В.А., Лагутенко О.И., Распаев Ю.А. Сети и системы радиодоступа. - М.: Эко-Трендз, 2005.

6 Сергей Пахомов. Анатомия беспроводных сетей. - Компьютер-Пресс, 2002. - №7.

7 Томас Мауфер. WLAN: практическое руководство для администраторов и профессиональных пользователей. - М.: КУДИЦ-Образ, 2005.

8 Джим Гейер. Беспроводные сети. Первый шаг. - М.: Издательский дом «Вильямс», 2005.

9 Джек Маккалоу. Секреты беспроводных технологий. - М.: НТ-Пресс, 2005.

10 Кузнецов М.А., Рыжков А.Е. Современные технологии и стандарты подвижной связи. - Санкт-Петербург: Линк, 2006.

11 В.Г. Олифер, Н.А. Олифер. Базовые технологии локальных сетей. - Санкт-Петербург: Питер, 1999.

12 Сайт: http://www.Aperto Networks..com

13 Шахнович С. Современные беспроводные технологии. - Санкт-Петербург: Питер, 2004.

14 Голубицкая Е.А., Жигуляская Г.М. Экономика связи. - М.: Радио и связь, 1999.

15 Баклашов Н.И., Китаева Н.Ж., Терехов Б.Д. Охрана труда на предприятиях связи и охрана окружающей среды: Учебник. - М.: Радио и связь, 1989.

16 Верховский Е.И. Пожарная безопасность на предприятиях радиоэлектроники. - М.: Высшая школа, 1987.

17 Долин П.А. Основы техники безопасности в электроустановках. - М.: Энергоатомиздат, 1984.

18 Сайт: www.telecom.kz

19 Базылов К.Б., Алибаева С.А., Бабич А.А. Методические указания для студентов всех форм обучения специальности 050719 - Радиотехника электроника и телекоммуникации. - Алматы: АИЭС, 2008. - 20 с.

Приложение А

Листинг программы расчёта

```
program Raschet;
uses crt;
const
SOM=15;
Lv=0.125;
varPt,Gt,Gr,Pmin,Lt,Lr,Y,R,Sl,Dl,d,L :real;
begin
clrscr;
Writeln ('  Pt=');
Readln (Pt);
Writeln ('  Gt=');
Readln (Gt);
Writeln ('  Gr=');
Readln (Gr);
Writeln ('  Pmin=');
Readln (Pmin);
Writeln ('  Lt=');
Readln (Lt);
Writeln ('  Lr=');
Readln (Lr);
Writeln ('  Sl=');
```

```
Readln (Sl);
Writeln ('  Dl=');
Readln (Dl);
begin
clrscr;
Y:=Pt+Gt+Gr+Pmin-Lt-Lr;
writeln('Y:=',Y);
R:=sqrt((Lv*Sl*Dl)/(Sl+Dl));
d:=10;
while d<1100 do
begin
L:=20*((ln(32*3.14*d)/ln(10)));
d:=d+100;
writeln ('L=', L);
end;
end;
end.
```

Окончание приложения А

На рисунке А.1 показан вывод приведенных нами расчетов консольном приложений.

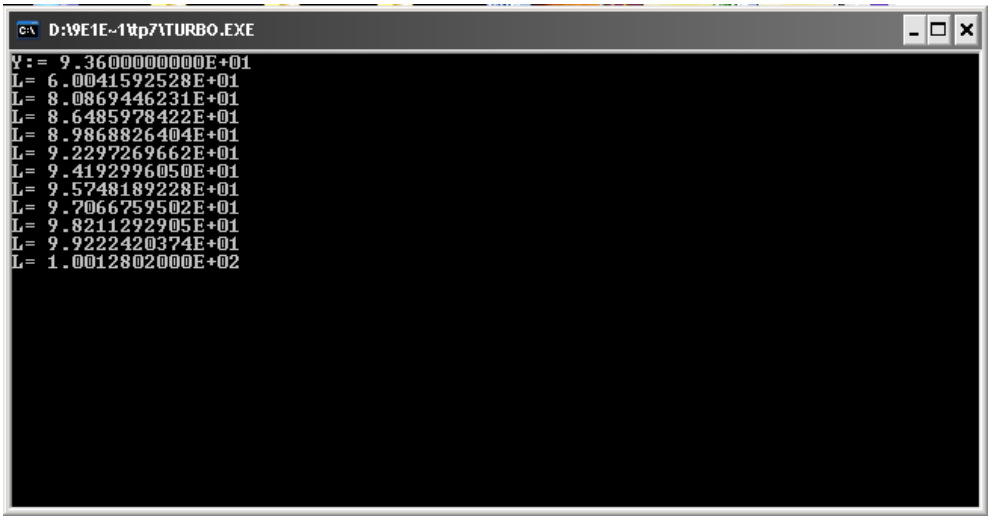


Рисунок А.1 – Вывод на консольном приложений

Приложение Б

На рисунке Б.1 показано структурная схема сети собранное на Cisco.

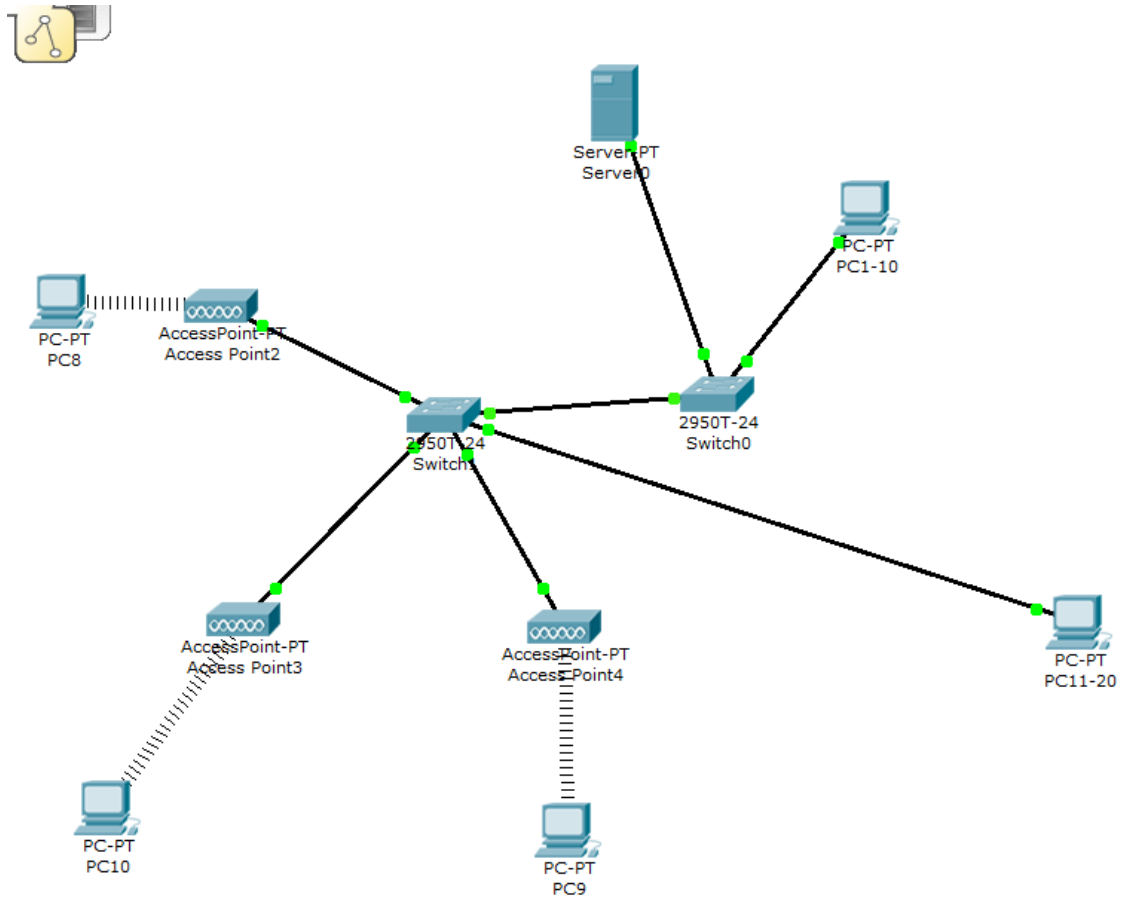


Рисунок Б.1 – Структурная схема сети