МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

ФАКУЛЬТЕТ «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

Допущен к защите:

зав. кафедрой «Компьютерные технологии»

д. ф.-м. н., профессор _____ Куралбаев З.К.

«___»_____20 __г.

Магистерская диссертация

на тему

«Проектирование беспроводной сети Wi-Fi на основе стандарта 802.11n на примере офисного здания»

специальность: 6М070400 - Вычислительная техника и программное обеспечение

Магистрант Сагинаев Тимур Саткенович

_____ Сагинаев Т.С.

Научный руководитель,

к. п. н., доцент _____ Кожамбердиева М.И.

АЛМАТЫ, 2014

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

RF- Radio Frequency
IEEE – Institute of Electrical and Electronics Engineers
QAM - Quadrature Amplitude Modulation
BPSK - Binary Phase-Shift Keying
WEP – Wired Equivalent Privacy
TKIP – Temporal Key Integrity Protocol
WPA – Wi-Fi Protected Access
CCMP – Counter Mode with CBC-MAC Protocol
CBC-MAC – Cipher Block Chaining Message Authentication Code
PSK – Pre-shared Key
MIC – Message Integrity Code
QoS – Quality of Service
AES – Advanced Encryption Standard
SSID – Service Set Identifier
PMK – Pairwise Master Key
PTK – Pairwise Transient Key
EAPoL – EAP over Lan
KCK – Key Confirmation Key
KEK – Key Encryption Key
GTK – Group Transient Key
TK – Temporal Keys
CTR – Counter Mode
IV – Initialization Vector
ICV – Integrity Check Value

АННОТАЦИЯ

В данной магистерской диссертации проводится исследование технических возможностей нового стандарта беспроводной сети 802.11ac и проводится сравнительный анализ преимуществ данного стандарта перед популярным на данный момент стандартом 802.11n. Цель данной работы – провести анализ работы популярного на данный момент стандарта 802.11n и нового стандарта 802.11ac и на основе собранных данных составить сравнительный анализ.

На основе данной диссертации реализован проект беспроводной сети Wi-Fi на основе стандарта 802.11ac

АНДАТПА

Бұл магистрлік диссертацияда жаңа стандарттағы 802.11 ас сымсыз желісінің техникалық мүмкіндігін зерттейді және осы стандарттың қазіргі уақытта кең тараған 802.11n стандартпен артық жеріне салыстырмалы талдау жүргізілуді. Бұл жұмыстың мақсаты – қазіргі уақытта кең тараған 802.11n стандартпен жаңа 802.11ac стандарттың жұмыс істеу мүмкіндігін талдау және жинаған көрсеткіштер арқылы салыстырмалы талдау құрастыру. Осы диссертация арқылы Wi-Fi сымсыз желісінің жобасы 802.11ac стандарт арқылы іске асырылған.

ABSTRACT

In this master dissertation we study the technical capabilities of the new 802.11ac wireless networking standard and a comparative analysis of the benefits of this standard before the currently popular standard 802.11n. The purpose of this study - an analysis of popular at the moment 802.11n standard and the new 802.11ac standard and based on the collected data to make a comparative analysis.

On the basis of this dissertations implemented the project of wireless Wi-Fi network based on the standard 802.11ac

ВВЕДЕНИЕ

Общая характеристика работы. Развитие рынка мобильных устройств идет очень высокими темпами. По прогнозам исследовательской компании Gartner, мировые продажи планшетов за 2013 год выросли на 42,7% и составили около 184 млн. единиц. Продажи смартфонов так же растут и за 2013 год составили 1,8 млрд. единиц, за 2014 год ожидается продажа около 1.9 млрд. единиц [1].

Подавляющая часть ноутбуков и других мобильных устройств, которые доступны на рынке, оснащаются Wi-Fi-адаптерами для доступа к беспроводным сетям Wi-Fi. Это могут быть домашние сети, сети в общественных местах, корпоративные и многие другие сети.

Актуальность темы. Современную информационную среду сложно представить без использования Wi-Fi технологии. Беспроводные Wi-Fi сети стали неотъемлемой частью нашей жизни в цифровой эпохе. Количества беспроводных сетей в общественных местах исчисляются десятками сетей. Почти к каждой квартире есть локальная беспроводная сеть.

На производстве большой проблемой при развертке беспроводных Wi-Fi сетей является большое количество помех и необходимость высокоскоростных беспроводных сетей. Особенно актуально проблема помехоустойчивости на предприятиях где большое количество вещательного оборудования (например, ДРТ «Кок-Тобе»). Любое оборудование, создающее излучение, начиная от микроволновой печи и заканчивая цифровым передатчиком, создает помехи для работы беспроводной сети Wi-Fi, что сказывается на радиусе работы и скорости передачи данных. На данном этапе проблему с помехоустойчивостью решают за счет увеличение мощности и количества антенн на точках доступа, что увеличивает потребление электроэнергии.

Целью настоящей работы является анализ нового стандарта беспроводной сети Wi-Fi 802.11ac. Проведение анализа с целью выяснение всех преимуществ нового стандарта 802.11ac над популярным на данный момент стандартом 802.11n.

Научная новизна. В данной работе проанализированы технические возможности нового цифрового стандарта 802.11ac. Новый стандарт 802.11ac является первым шагом гигабитным беспроводным сетям и благодаря новому режиму модуляций показывает хорошие результаты в плане помехоустойчивости и радиусу работы. Для частных беспроводных сетей новый стандарт расширяет возможности использования облачных хранилищ данных, таких как Dropbox,SkyDrive и Google Drive.

Апробация. Основные результаты диссертационной работы отражены в научных трудах. Основное содержание диссертации отражено в следующих публикациях:

Сагинаев Т.С. Анализ безопасности доступа к защищаемой информации через сети WI-FI // Сборник научных трудов магистрантов «Энергетика,

радиотехника, электроника и связь», «Вычислительная техника и программное обеспечение» и «Информационные системы». –Алматы: АУЭС, 2013. - С. 69-74

1. Обзор технологии беспроводной сети Wi-Fi

1.1 Основные понятия

Термин Wi-Fi изначально был придуман как игра слов в качестве рекламы для привлечения потребителей с «намеком» на Hi-Fi (англ. High Fidelity – высокая точность. По началу в некоторых релизах WECA проскальзывало словосочетание Wireless Fidelity (беспроводная точность). На данный момент от этой формулировки отказались и оставили термин Wi-Fi, который никак не переводится. На данный момент Wi-Fi является брендом продвигаемый организацией Wi-Fi Alliance.

Стандарт Wi-Fi был создан в 1991м году компанией «NCR Corporation» и изначально был предназначен для обслуживания систем кассового оборудования. Продукт использовался под маркой WaveLan, скорость передачи составляла 1-2 Мбит/с. Отцом Wi-Fi по праву можно назвать Вика Хейза, учувствовавшего в последующем в разработке стандартов IEEE 80211a, IEEE 80211b и IEEE 80211g [2].

В 1997 году Институт инженеров электротехники и электроники (IEEE) сертифицировал первый стандарт беспроводной сети 802.11.

1.2 Принципы работы

Беспроводная Wi-Fi сеть состоит из одной или нескольких точек доступа и не менее одного клиента. Точка доступа передает свой идентификатор сети (SSID) с помощью сигнальных пакетов, которые передаются каждый 100мс на скорости 0,1 Мбит/с. Соответственно наименьшая скорость беспроводной сети Wi-Fi 0,1 Мбит/с. Для подключения к беспроводной сети клиенту необходимо знать SSID нужной ему сети. При попаданий приемника в зону действия двух точек доступа с одинаковыми SSID приемник выбирает между точками доступа основываясь на уровне сигнала. Одно из преимуществ технологи Wi-Fi заключается в том, что клиенту дается полная свобода выбора критериев соединения и роуминга.

Беспроводных сетей делятся на три вида (рисунок 1.1):

- WLAN (Wireless Local Area Network) – в основном используется для домашних Wi-Fi сетей;
- WPAN (Wireless Personal Area Network) – используется для персональных беспроводных сетей. Использует стандарт 802.15;
- WWAN (Wireless Wide Area Network) – беспроводные сети городского масштаба.

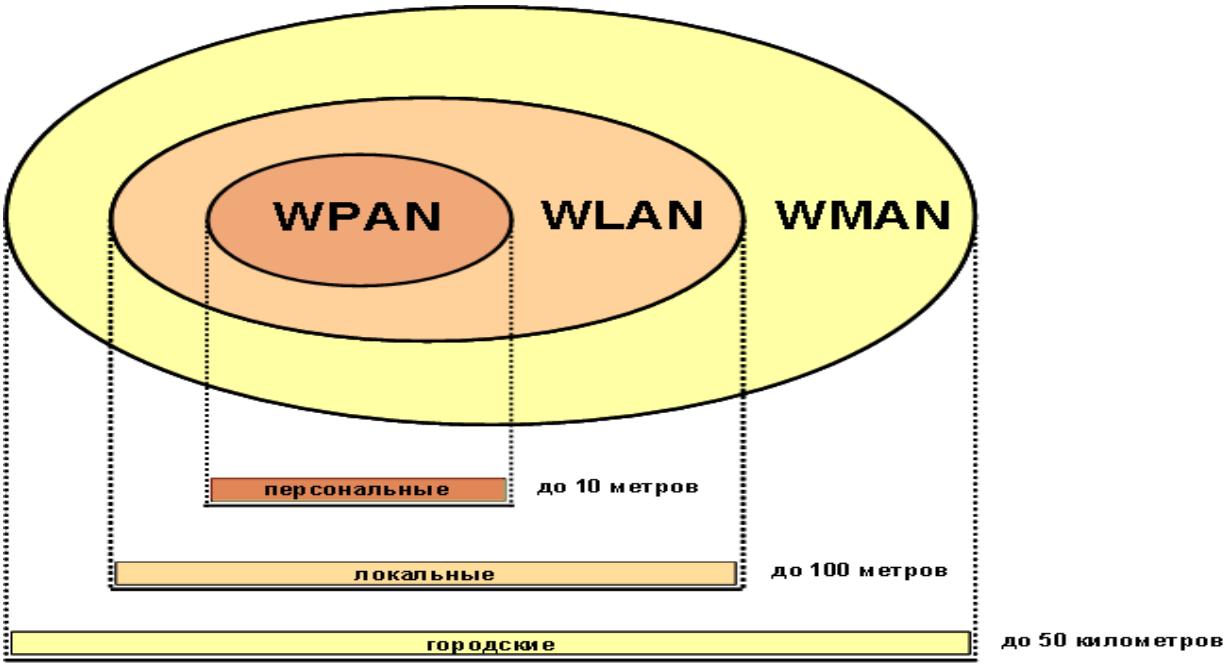


Рисунок 1.1 - Радиус действия беспроводных сетей

Основным различием беспроводных сетей WLAN и WPAN, перед WMAN является диапазон рабочих частот (рисунок 1.2). Локальные (WLAN) и персональный (WPAN) сети не требуют частотного планирования и координацию с другими радиосетями, так как работают в нелицензионных диапазонах частот 2,4 и 5 ГГц. Сети BWA (Broadband Wireless Access) используют как лицензионные, так и нелицензионные диапазоны (от 2 до 66 ГГц).

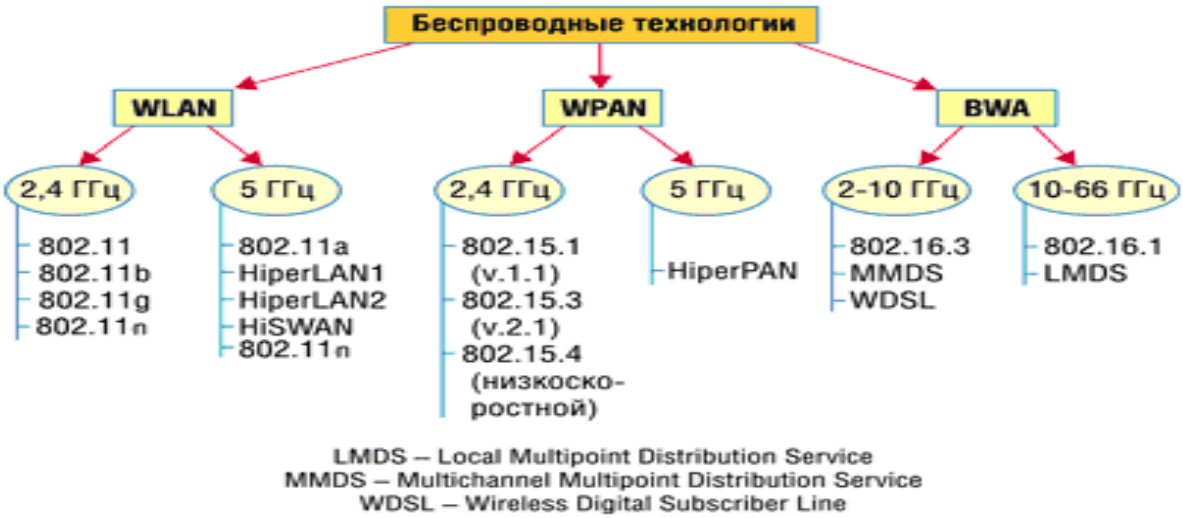


Рисунок 1.2 - Виды беспроводных технологий

1.3.Преимущества и недостатки Wi-Fi

Преимущества. К преимуществам беспроводной технологий Wi-Fi можно отнести отсутствие необходимости прокладки кабелей при развёртывании сети. Это очень удобно в тех местах, где прокладка кабелей является проблемой (напр. исторические объекты). Вместе с удобством при развертывании сетей, беспроводные технологии удобны и при свертывании сетей Отсутствие проводов дает мобильность рабочих мест при необходимости. Данная функция удобна на складах, производстве и т.д.

Недостатки. Главным недостатком беспроводных сетей перед проводными сетями является плохая защита от взлома. Несмотря на постоянное улучшение методов шифрования, полностью проблемы с безопасностью не решены.

При развертывании необходимо учитывать особенности помещения. Железобетонные стены, колонны, являются серьёзным препятствием для Wi-Fi. В большинстве случаев проблему с преградами решают за счет установки точек доступа с более мощными антеннами. Радиопомехи могут влиять на дальность работы и скорость передачи в сети Wi-Fi.

1.4 Вредоносность Wi-Fi

«Убийца-невидимка» - так прозвали Wi-Fi некоторые российские и мировые ученые. Главный тезис против беспроводного интернета – постоянное излучение, в котором находятся жители крупных городов. В некоторых городах США родители даже в судебном порядке обязывают администрацию школ убирать Wi-Fi. Действительно ли Wi-Fi настолько опасен? [17]

Чтобы осознать весь масштаб вопроса, достаточно вбить в поисковой системе на Wi-Fi-фобов. В США существует целое поселение Грин Бэнк, где на площади в 33 тысячи квадратных километров запрещено использование не то что беспроводных сетей, а любой электроники. Со всех штатов сюда переезжают Wi-FI-фобы. Отдельные паникеры сооружают себе шапочки, плащи, стены из фольги защищая себя таким образом от излучения. Некоторые самые расторопные предприниматели начали выпускать обои, которые блокируют излучение по цене 800 долларов за рулон. Работают они якобы с помощью нанесенных на поверхность кристаллов серебра. Традиционная формула: что для одних – страх и ужас, для других – неплохая прибыль [4].

В 2011 году Международное Агентство по Исследованиям в области Рака классифицировало радиоизлучение как “возможно канцерогенное для людей”. Классификация IARC радиоизлучения отражает факт, что некоторые ограниченные доказательства существуют, что излучение радиоволн гипотетически может быть фактором риска для рака. Основной страх у людей вызывают три возможных фактора:

- Влияние на мужскую потенцию и высокая вероятность бесплодия;

- Влияние на мозговую деятельность человека;
- Влияние на детей, так как их черепная коробка еще недостаточно прочна.

Однако достоверного подтверждения этим гипотезам до настоящего времени нет. Так же не было выявлено связи между воздействием радио и раковыми заболеваниями.

При этом нельзя утверждать, что Wi-Fi абсолютно безвреден для человека. В настоящее время данный вопрос требует более глубоких исследований. Всемирная организация здравоохранения и IARC намерены гарантированно провести дополнительные исследования в этой области.

Приведем несколько цифр доступных всем: пиковая мощность сотового сигнала достигает 8 Вт, сигнала обычного бытового Wi-Fi передатчика – 100 мВт. Допустимая плотность потока энергии (по СаНПиН 2.1.8/2.2.4) – 0,1 Вт/м2. А плотность потока энергии – физическая величина, численно равная потоку энергии через единичную площадку, перпендикулярную направлению.

Из чего следует что, излучение беспроводного интернета никак не превышает установленные нормы. Лучшая защита от нежелательного облучения – это расстояние. Причем достаточно 1м, но ученые перестраховываются и рекомендуют 3м. Большую опасность представляют 3G-модемы, так как работают по сигналам сотовой связи.

Дополнительную безопасность от Wi-Fi излучений можно получить, придерживаясь этих правил:

- Точки доступа должны быть расположены подальше от мест сна и постоянных рабочих мест;
- По возможности отключать Wi-Fi роутер, если интернет не используется;
- Держать устройства, принимающие Wi-Fi подальше от себя, например на столе;
- Максимально оградить маленьких детей от Wi-Fi роутеров, с целью избежание перенапряжение растущего организма дополнительным излучением [20].

Последние фактические данные Всемирной организации здравоохранения (WHO):

- Полученные результаты исследований не принесли доказательств того, что RF, исходящие от базовых станций и беспроводных сетей вызывают неблагоприятные медицинские эффекты;
- Университет Пенсильвании провел 356 измерений в 55 местах где присутствует сеть Wi-Fi в четырех странах в условиях, превышающих обычную степень воздействия сигнала. Это исследование пришло к выводу, что радиочастотные поля от WLAN, в обычных сценариях, работают на уровнях значительно более низких, чем предельные значения. Во всех случаях замеренные уровни сигнала Wi-Fi были намного ниже международных норм (IEEE C95.1-2005 и ICNIRP) и почти во всех случаях намного ниже других радиосигналов в той же окружающей среде;
- Health Protection Agency (HPA) Великобритании констатирует факт того, что Wi-Fi сигналы имеют очень низкий уровень воздействия и не

представляют угрозы для здоровья: нет никаких последовательных доказательств воздействий на здоровье от RF, не превышающих установленную норму, и поэтому нет никаких причин, почему школы и другие заведения не могут использовать оборудование Wi-Fi;

- Фактически, обзор HPA показал, что эмиссия WLAN значительно ниже норм инструкций по технике безопасности: агентство измерило плотность воздействия радиоволн вообще, а также в офисах, где развернуты сети WLAN. Полученные показатели намного ниже установленных норм;
- В августе 2010, Health Canada опубликовал положение, в котором отмечено, что;
- Wi-Fi - вторая самая распространенная форма беспроводной технологии, после сотовой связи. Она широко используется в Канаде в школах, офисах, кафе, жилых домах и т.д. Health Canada заверяет, что воздействие радиоволн по технологии Wi-Fi чрезвычайно низко и никак не влияет на состояние здоровья.

Научные исследования демонстрируют, что сигналы Wi-Fi намного ниже допустимых международных норм и не требуют ограничений в использовании и дополнительных мер безопасности. Так что нет никаких видимых причин для отказа от тех огромных преимуществ, которые обеспечивает технология Wi-Fi.

Излучение радиочастоты от оборудования Wi-Fi во всех местах, доступных для широкой публики, должно быть не выше уровня, установленного официальными медицинскими инструкциями по технике безопасности. Пределы, определенные в нормативных инструкциях, намного ниже «порога вредности» и основаны на данных тысяч изданных научных исследований по воздействию излучения радиоволн. Единые нормы определены для взрослых и детей. При этом допускается продолжительное воздействие в режиме 24 часа, 7 дней в неделю.

1.5 Основные стандарты Wi-Fi

Стандарт IEEE 802.11 – это набор стандартов связи для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 2,4 – 66ГГц. В настоящее время широко используется преимущественно три стандарта группы IEEE 802.11:

- IEEE 802.11a;
- IEEE 802.11g;
- IEEE 802.11n.

Стандарт IEEE 802.11ac только набирает популярность (таблица 1.1).

Таблица 2.1 - Основные характеристики стандартов группы IEEE 802.11

Стандарт	802.11a	802.11g	802.11n	802.11ac
Дата сертификации стандарта	1999г	2003г	2009г	2013г
Полоса пропускания, МГц	300	83.5	40	80
Частотный диапазон, ГГц	5	2.4 – 2.483	2.4-2.5 или 5	5-6
Типы модуляции	BPSK, QPSK, OFDM	BPSK, QPSK, OFDM	BPSK, 64-QAM	256-QAM
Скорость передачи данных Мбит/с	6 – 54	1 – 54	6 – 300	300-1000
Совместимость	802.11n	802.11 b/n	802.11 a/b/g	802.11 a/b/g/n
Радиус, м	150	250	500	100 000

Начиная со стандарта 802.11n, беспроводные сети Wi-Fi переходят на квадратурную модуляцию. Это сразу же отражается на скорости передачи данных и радиусе работы беспроводной сети. Стандарт 802.11ac переходит на модуляцию 256-QAM, который используется в цифровых эфирных передатчиках, для которых важно большой радиус вещания и хорошая помехоустойчивость.

Если на канальном уровне все беспроводные сети семейства 802.11 имеют одну и ту же архитектуру, то физический уровень для сетей разных стандартов различен. Именно на физическом уровне определяются возможные скорости соединения и методы модуляции и физического кодирования при передаче данных.

1.5.1 Стандарт IEEE 802.11a

Является наиболее "широкополосным" из семейства стандартов 802.11, предусматривая скорость передачи данных до 54 Мбит/с (редакцией стандарта, утвержденной в 1999 г., определены три обязательных скорости - 6, 12 и 24 Мбит/с и пять необязательных - 9, 18, 36, 48 и 54 Мбит/с).

В отличие от базового стандарта, ориентированного на область частот 2,4 ГГц, спецификациями 802.11a предусмотрена работа в диапазоне 5 ГГц. В качестве метода модуляции сигнала выбрано ортогональное частотное мультиплексирование (OFDM). Наиболее существенное различие между этим методом и радиотехнологиями DSSS и FHSS заключается в том, что OFDM предполагает параллельную передачу полезного сигнала одновременно по нескольким частотам диапазона, в то время как технологии расширения спектра передают сигналы последовательно. В результате повышается пропускная способность канала и качество сигнала.

К недостаткам 802.11a относятся более высокая потребляемая мощность радиопередатчиков для частот 5 ГГц, а так же меньший радиус действия (оборудование для 2,4 ГГц может работать на расстоянии до 300м, а для 5ГГц - около 100м).

1.5.2 Стандарт IEEE 802.11g

Стандарт IEEE 802.11g предусматривает различные скорости соединения: 1; 2; 5,5; 6; 9; 11; 12; 18; 22; 24; 33; 36; 48 и 54 Мбит/с. Одни из них являются обязательными для стандарта, а другие — опциональными. Кроме того, для различных скоростей соединения применяются разные методы модуляции сигнала.

При разработке стандарта 802.11g рассматривались две несколько конкурирующие технологии: метод ортогонального частотного разделения OFDM, заимствованный из стандарта 802.11a и предложенный к рассмотрению компанией Intersil, и метод двоичного пакетного свёрточного кодирования PBCC, опционально реализованный в стандарте 802.11b и предложенный компанией Texas Instruments. В результате стандарт 802.11g содержит компромиссное решение: в качестве базовых применяются технологии OFDM и CCK, а опционально предусмотрено использование технологии PBCC.

Прежде чем переходить к рассмотрению методов модуляции, используемых в 802.11g, отметим, что данным стандартом, как и стандартами 802.11b/b+, предусмотрено применение частотного диапазона от 2,4 до 2,4835 ГГц, который предназначен для безлицензионного использования в промышленности, науке и медицине (Industry, Science and Medicine, ISM). Однако, несмотря на возможность безлицензионного применения данного частотного диапазона, существует жесткое ограничение максимальной мощности передатчика. Поэтому при выборе способов кодирования и модуляции сигнала необходимо решить две основные проблемы.

С одной стороны, скорость передачи в беспроводной сети должна быть как можно более высокой, чтобы конкурировать с проводными сетями и удовлетворять современным потребностям пользователей. Рост скорости передачи приводит к увеличению ширины спектра, что крайне нежелательно, поскольку частотный диапазон передачи ограничен.

С другой стороны, уровень полезного сигнала должен быть достаточно низким, чтобы не создавать помех другим устройствам в ISM-диапазоне. Таким образом, передаваемый сигнал должен быть едва различим на уровне шума, но в этом случае необходимо разработать алгоритм безошибочного выделения сигнала на уровне шума. Уменьшение мощности передаваемого сигнала достигается за счет использования технологии уширения спектра и «размазывания» сигнала по всему спектру.

Еще одна проблема — это обеспечение должного уровня помехоустойчивости протокола.

К сожалению, одновременное выполнение всех перечисленных условий невозможно, поскольку они противоречат друг другу. Таким образом, выбор конкретного метода кодирования и модуляции сигнала — это поиск золотой середины между требованиями высокой скорости, помехоустойчивости и ограничения по мощности передачи.

1.5.3 Стандарт IEEE 802.11n

Новый стандарт лицензированный в 2009м году, призван повысить пропускную способность локальных беспроводных сетей до номинальных скоростей свыше 100 Мбит/с. Стандарт IEEE 802.11n работает в диапазоне 5 ГГц, обеспечивая совместимость с оборудованием IEEE 802.11a. Однако он отличается от предшественников как на физическом, так и на MAC-уровне.

Ключевым нововведением на физическом уровне является применение технологии антенных систем MIMO и возможность удвоить ширину канала. На MAC-уровне появилась возможность объединить несколько пакетов в один.
Технология MIMO – одно из наиболее перспективных направлений развития беспроводных систем передачи данных. Она предполагает наличие в приемнике и передатчике нескольких антенных каналов. Задействовать эти каналы можно по-разному: они могут функционировать как абсолютно независимые (например, поляризационные или частотно-разнесенные) и как коррелированные. Цель применения MIMO-техники в стандарте IEEE 802.11n, где все антенные каналы действуют в едином частотном диапазоне, – увеличение скорости передачи, расширение частотного диапазона и повышение спектральной эффективности по сравнению с “традиционными” системами. Здесь важно напомнить, что в стандарте IEEE 802.11n, равно как и в IEEE 802.11a/g, используется OFDM-модуляция. В стандарте IEEE802.11n каждый информационный символ объединяет 56 модулированных поднесущих частот, где 4 – пилотные и 52 – информационные. Для сравнения: в стандартах 802a/g поднесущих всего 52, из них 4 – пилотные. Таким образом, MIMO – это фактически дополнительное кодирование информации, так называемое пространственно-временное кодирование STC. Именно такое сочетание кодирования в частотной и пространственной области и обеспечивает множественность путей распространения сигнала. Это делает систему связи более надежной, в частности, благодаря устойчивости к межсимвольной интерференции. Последнее крайне актуально при создании систем передачи информации в помещениях или в условиях городской застройки, где уровень переотражений сигнала велик. В упрощенном виде технологию MIMO, применяемую в IEEE 802.11n, можно представить как разделение высокоскоростного потока OFDM символов на N потоков, где N – число передающих антенн. По сравнению с традиционными системами с одной антенной SISO, если в каждом канале сохранять номинальную скорость, общая пропускная способность системы теоретически возрастет в N раз. Если же суммарная пропускная способность MIMO-системы не отличается от SISO-системы, то скорость в каждом антенном канале можно снизить в N раз. Это позволит, например, увеличить дальность передачи – ведь чем медленнее канал, тем ниже предельно допустимое соотношение сигнал/шум. Приемник восстанавливает исходный поток данных, полученный по различным антенным каналам. При этом число приемных антенн может отличаться от числа передающих.

С ростом числа приемных антенн увеличивается и надежность работы MIMO-системы. Это связано с пропорциональным увеличением числа пространственных каналов. Чем их больше, тем более вариативна принимаемая информация и тем ниже вероятность полного замирания сигнала сразу во всех каналах. Добавление одной приемной антенны увеличивает соотношение сигнал/шум примерно на 3 дБ. Однако увеличение числа антенных каналов в приемнике существенно усложняет обработку сигналов. Соответственно, растет и стоимость устройства.

1.5.4 Стандарт IEEE 802.11ac – Стандарт нового поколения

802.11ac — разрабатываемый стандарт беспроводных локальных сетей, работающий на частотах 5—6 ГГц. Стандарт позволяет существенно расширить пропускную способность сети, начиная от 300 Мбит/с и до 1 Гбит/с при 8x MU-MIMO-антеннах. Это наиболее существенное нововведение относительно IEEE 802.11n. Кроме того, ожидается снижение энергопотребления, что, в свою очередь, продлит время автономной работы мобильных устройств.

Новый Wi-Fi предлагает втрое большую скорость (в теории, 1,3 гигабит против 450 мегабит в секунду), что положительно скажется на потоковой медиа (в частности, HD-видео), мобильных играх и передаче данных. Современный 802.11n дает максимальную скорость 150 Мбит/с от одной антенны, 300 от двух и 450 от трех. У 802.11ac эти показатели на порядок выше: 450/900/1,3 Гбит/с соответственно. А скорость у 802.11ac-совместимых аппаратов, имеющих сразу 8 антенн, сможет достигать целых 7 Гбит/с.

Другая полезность гигабитного Wi-Fi — более широкой диапазон покрытия и более стабильный сигнал. Улучшения достигаются за счет технологии формирования луча ("бимформинг"), которая распознает местоположение устройства и направляет сигнал Wi-Fi прямо на него. Такая методика поможет повысить качество приема сигнала.

Электроника со "старым" Wi-Fi работает на переполненной частоте 2,4 ГГц, разделяя ее с планшетником, соседним монитором или даже микроволновкой и другими приборами. Поэтому еще одно достоинство 802.11ac — устранение помех за счет перехода на более эффективный для передачи данных диапазон 5 ГГц (в полосах частот от 80 до 160 мегагерц).

Процесс перехода к 802.11ac растянется на несколько лет, поэтому в устройствах с новым Wi-Fi будет предусмотрена обратная совместимость с устаревающими стандартами. Роутеры при необходимости смогут автоматически переключаться с 5 ГГц на 2,4.

Увеличение скорости в стандарте 802.11ac достигается следующими способами:

- Переход на каналы шириной 80Mhz и 160Mhz позволяющие удвоить и учетверить показатели по сравнению с 802.11n;

- Максимальное число пространственных потоков увеличено до 8, что позволяет удвоить скорость;
- Оптимизация модуляций и методов передачи пакетов, что позволяет добиться большой скорости не только рядом с точкой доступа [11].

Помимо скорости, у 802.11ac есть два ключевых улучшения:

Beamforming — возможность динамически менять диаграмму направленности антенн. Данная функция позволяет зоне покрытия точки доступа оптимально подстраивать зону покрытия под текущее расположение клиентов. Beamforming является частью стандарта 802.11n. Но частью опциональной! В 802.11ac данная функция является обязательной;

MU-MIMO. Большинство Wi-Fi сетей – полудуплексные. Пакеты передаются последовательно — в один момент времени передается один пакет. Если в канале 120Mbps идет поток в 1Mbps — используется 1/120 полосы пропускания. Если при этом прибывают данные для другого клиента — использовать незадействованную полосу пропускания не удастся. В итоге толку от сверхвысоких скоростей 802.11n в сетях с большим количеством небыстрых клиентов (т.е. корпоративных) очень мало. MU-MIMO позволяет разбить канал на несколько более мелких каналов и передавать данные по ним параллельно.

На данный момент известно о двух вариантах реализации MU-MIMO в 802.11ac:

- SDMA (Space Division Multiple Access) позволяет передавать данные разным клиентам по разным пространственным потокам (для этого нужен Beamforming);
- Downlink MIMO позволяет разбить поднесущие OFDM на группы, и динамически выделять каждому клиенту нужное число поднесущих. Таким образом, даже если на точке доступа будут сидеть клиенты 2x2:2 MIMO — все равно можно будет использовать весь потенциал канала.

Даже если ограничить максимальную скорость сети одним Gbps, стандарт 802.11ac дает существенные выгоды как для домашних (высокие скорости), так и для корпоративных сетей (эффективная утилизация этих самых высоких скоростей в сетях с большим числом клиентов) [16].

1.6 Промышленный Wi-Fi

1.6.1 Общая информация о промышленных Wi-Fi сетях

Промышленная Wi-Fi сеть – это мощный бизнес инструмент, позволяющий добиться оптимального качества роуминга, максимальной безопасности сетевых коммуникаций и внедрения современного мобильного функционала.

В современных условиях ведения бизнеса, провода, которые по праву считаются наиболее надежными для создания корпоративной информационной инфраструктуры, все же, в отдельных случаях, не выдерживают конкуренцию

перед промышленными беспроводными сетями. В случае грамотного внедрения Wi-Fi сетей, они не только не уступают традиционным кабельным решениям, но и обеспечивают определенные преимущества, наиболее очевидным из которых является мобильность рабочих мест.

Надо сказать, что словосочетание «промышленная Wi-Fi сеть» по-прежнему ассоциируется у многих с установкой банальной точки доступа, подобно тому, как это делается в сетевых кафе и ресторанах, фойе отелей и салонов красоты, зонах ресепшн в различных организациях и т.д. Соответственно, существует мнение, что промышленный Wi-Fi не требует детальной проработки и качественной установки, ведь он не слишком отличается от домашней беспроводной сети, настроить которую сегодня может едва ли не каждый школьник. Согласно такому мнению, данная технология не может быть достаточно мощной и защищенной, а значит, совершенно не подходит для внедрения серьезных бизнес-проектов. Это представление в корне неверно, ведь промышленная беспроводная сеть на то и является крупномасштабной информационной системой промышленного назначения, что при ее организации используется далеко не примитивное «домашнее» оборудование.

Вот почему построение промышленной сети Wi-Fi не терпит спешки и дилетантского отношения, ведь именно в результате неправильного подхода к её организации и рождаются подобные точки зрения, компрометирующие промышленную беспроводную сеть. Так, к примеру, качество соединения будет зависеть не только от мастерства подрядчика и «брендовости» оборудования, но и от ряда таких специфических факторов, как:

- Материалы, из которых сделаны стены и перегородки в здании;
- Особенности расположения рабочих мест;
- Влияние на беспроводную сеть дополнительных излучающих источников и др.

Ввиду последнего фактора, задолго перед началом организации беспроводной системы, специалисты проводят радио обследование, в ходе которого выясняют возможные преграды на пути прохождения сигнала (например, металлоконструкции, приборы СВЧ-излучения и т. д.). Уровень сигнала измеряется на специальном оборудовании, затем выводится отчет и формируются рекомендации, на основании которых обеспечивается ровное покрытие беспроводной связью всей площади объекта.

1.6.2 Стоимость утечки информации

В настоящее время утечки информации на предприятиях любых отраслей стали обыденным явлением. Неограниченный доступ к конфиденциальным данным, широкий инструментарий быстрой передачи данных, нерадивость и нелояльность отдельных групп сотрудников – всё это ведет к тому, что случайно или злонамеренно люди используют информацию компании в личных целях.

Это подтверждается данными портала информационной безопасности Content Security, озвучивающего степень опасности внутренних и внешних угроз:

- разглашение (излишняя болтливость сотрудников) — **32%**;
- несанкционированный доступ путем подкупа и склонения к сотрудничеству со стороны конкурентов и преступных группировок — **24%**;
- отсутствие в фирме надлежащего контроля и жестких условий обеспечения информационной безопасности — **14%**;
- традиционный обмен производственным опытом — **12%**;
- бесконтрольное использование информационных систем — **10%**;
- наличие предпосылок возникновения среди сотрудников конфликтных ситуаций, связанных с отсутствием высокой трудовой дисциплины, психологической несовместимостью, случайным подбором кадров, слабой работой кадров по сплочению коллектива — **8%**.

По словам профессиональных безопасников, крупные утечки не происходят без подготовки: сотрудники ведут между собой и внешними покупателями информации переговоры, накапливают чужую информацию, уносят свои наработки домой. Минимальные контрмеры – оградить явных инсайдеров от важной информации, провести беседы с колеблющимися и ведомыми сотрудниками.

Пример дорогой для предприятия утечки – проектный институт, где трудится несколько сотен работников. А теперь представьте, что в один день уходит треть из них и не в какую-то другую сферу, а к прямому конкуренту. Так и случилось пару лет назад на одном из крупных институтов России по проектированию предприятий ключевой отрасли промышленности. Сотрудники унесли с собой не только свои разработки (их они на 100% считали личными), но и достижения своих товарищей, которые не сочли возможным покинуть свое предприятие. Как итог: предприятие безвозвратно потеряло около 50% своих собственных разработок за последние пару лет, потеряла ключевых сотрудников [5].

2. Экспериментальная часть

Для анализа работы стандарта 802.11ac было проведен эксперимент для сравнения работы Wi-Fi приемников работающих в стандарте 802.11ac и 80211n:

Для проведения эксперимента была собрана тестовая схема в одной точкой доступа и двумя Wi-Fi приёмниками:

- Wi-Fi адаптер Asus (802.11ac, 3x3:3 MIMO, 80 MHz);
- Wi-Fi адаптер Buffalo (802.11n, 3x3:3 MIMO, 40 MHz).

В Качестве источника сигнала была выбрана точка доступа D-Link DAP 2695. Данная точка доступа поддерживает оба стандарта.

Эксперимент проводился путем по очередного тестирования каждого приемника. Для каждого приемника точка доступа настраивалась на необходимый стандарт (рисунок 2.1).

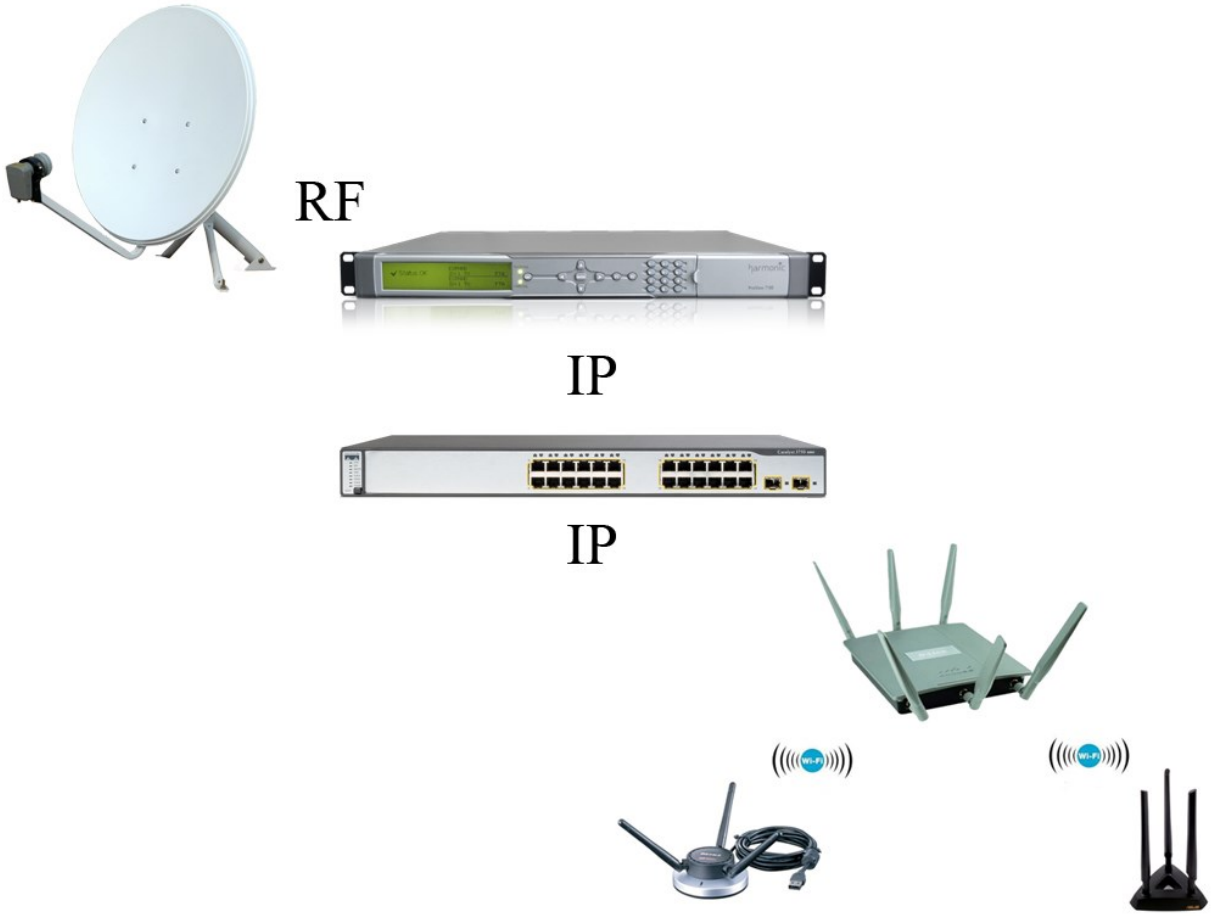


Рисунок 2.1 – Схема тестовой площадки

Результаты исследования работы Wi-Fi адаптеров при нескольких потоках данных приведены в таблице 2.1.

Таблица 2.1 – Сравнительная таблица производительности 802.11ac и 802.11n

Роутер\Кол-во потоков	1	2	3	4	5	6	7	8
802.11.ac	169.937	295.007	352.229	386.338	416.477	427.836	438.516	440.311
802.11n	111.039	145.571	164.583	165.517	160.824			

При передаче одного потока данных реализация 802.11ac особенного преимущество 802.11ac не наблюдется: 802.11n достигает 110Mbps на 40Mhz, 802.11ac — 170Mbps на 80Mhz.

Однако при увеличении количества потоков Wi-Fi адаптер 802.11n перестает увеличивать скорость приема уже на трех потоках, упираясь в потолок 165Mbps). В то время как 802.11ac продолжает увеличивать скорость вплоть до семи потоков. Понятно, что показатель удельной скорости на поток падает, но все равно остается в разумных пределах: 438/7 = ~62Mbps эффективной пропускной способности даже выше чем 165/3 = 55Mbps, у 802.11n. Здесь наглядно виден потенциал новой технологии, показавшей почти в три раза большую скорость, и обеспечивающей большую емкость и масштабируемость потока (рисунок 2.2).

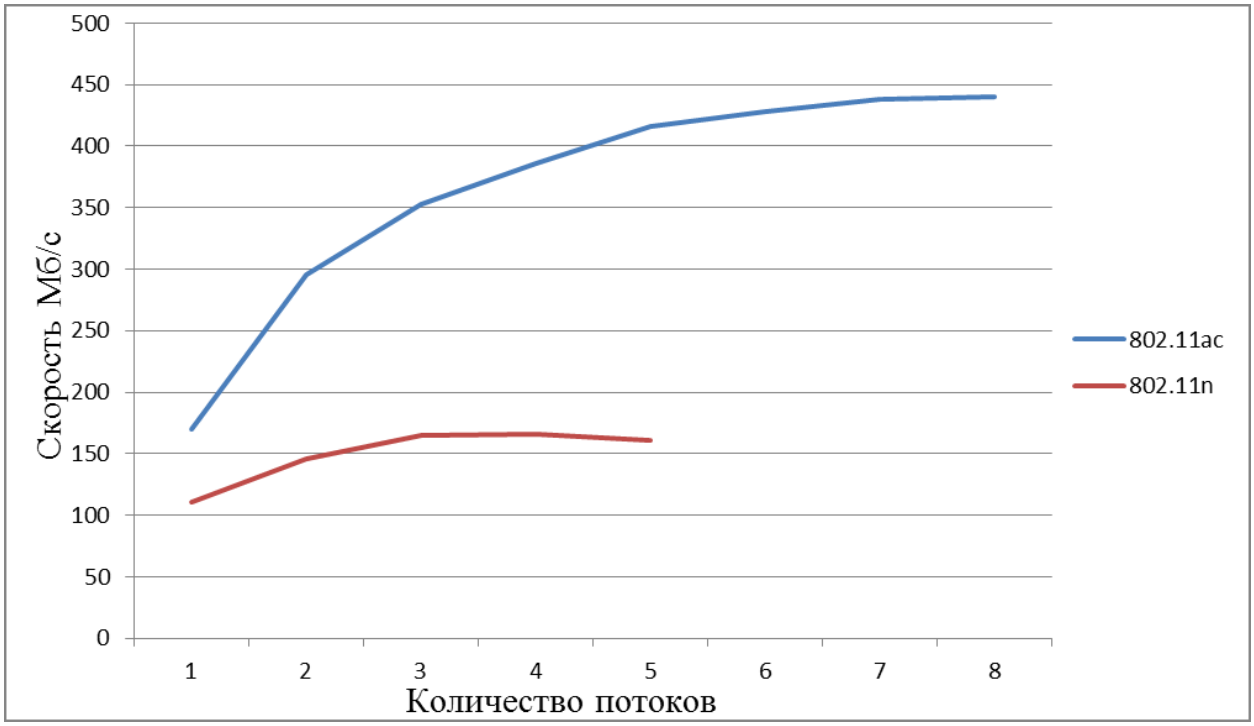


Рисунок 2.2 – Сравнение производительности 802.11ac и 802.11n

3. Методы защиты беспроводных сетей Wi-Fi

3.1 Защита информации

В современном цифровом мире широкое распространение получила технология беспроводного соединения, называемое Wi-Fi. Если включить ноутбук и посмотреть на количество Wi-Fi сетей в каком-нибудь городе, то их там будет даже не две и не три, а гораздо больше. К сожалению, такое распространение приводит к тому, что многие люди, ставят у себя беспроводное оборудование, толком даже не разобравшись в настройках. А следствием неграмотной настройки может стать возможность получения несанкционированного доступа к беспроводной сети.

3.2 История развития безопасности технологий Wi-Fi

Семейство стандартов IEEE 802.11 благодаря своим удобствам быстро обрело широкую популярность. Обратной стороной популярности тут же стал и повышенный интерес к несанкционированному доступу в беспроводные сети Wi-Fi, хищению информации из подобных сетей и прочим злоупотреблениям.

Входящий в спецификации 802.11 базовый механизм для защиты данных в таких сетях получил название WEP, то есть «Приватность, эквивалентная проводной связи». Уже из названия предполагалось, что речь идет не то чтобы о реально серьезной защите, а примерно о таком же уровне безопасности, что предоставляет обычная проводная Ethernet. Где все данные в общем случае передаются в открытом виде, но для доступа к ним посторонних лиц необходимы определенные манипуляции с техникой и протоколами.

И подобно тому, как умельцы без труда подключаются к Ethernet-сетям для перехвата и шпионажа, так и специалисты быстро преодолели защиту WEP. Слабости конструкции WEP уже в 2001 году позволили группе исследователей из университетов и индустрии взломать эту систему защиты. Криптоаналитики продемонстрировали, что атакующая сторона, располагающая всего лишь средненьким ноутбуком, может восстановить секретный криптоключ в сети всего за один-два часа. В последующие годы было разработано и опубликовано несколько усовершенствованных методик взлома, так что теперь нападающим хватало и 60 секунд (в публичной демонстрации на одной из конференций по безопасности в 2007 году все было сделано за 3 секунды).

Иначе говоря, защита WEP отпугивала лишь случайно подключавшихся к Wi-Fi-сети посторонних, а серьезным злоумышленникам стало уже без разницы, включено в настройках шифрование или нет.

Дабы изменить столь печальную ситуацию, IEEE сформировала рабочую группу 802.11i и поставила перед ней задачу: заменить WEP на что-то более сильное и в то же время совместимое с уже эксплуатирующимся

оборудованием. В итоге эта группа выдала два отдельных решения: одно, так сказать, с оглядкой назад, а второе — устремленное в будущее.

Принимая во внимание проданное оборудование, члены 802.11i сделали так, чтобы все уже вышедшие с фабрик Wi-Fi-устройства (начиная с 1999 года) можно было оснастить новой системой защиты TKIP. Конструкция TKIP позволяла обеспечить совместимость со старыми Wi-Fi картами — через обновление драйверов и прошивок. По понятным причинам это сделали в самую первую очередь, и к началу 2003 года TKIP был включен в новый стандарт Wi-Fi-защиты, получивший название WPA.

Помимо этого группа 802.11i разработала WPA2 — более сильное решение для будущих версий Wi-Fi, — добавив в комплект криптосистему на основе надежного алгоритма AES с длинным ключом и особым режимом работы, обеспечивающим дополнительную защиту целостности передаваемых данных. Этот режим носит сокращенное название CCMP. Разбирать в подробностях тонкости функционирования этого режима здесь вряд ли к месту, но можно отметить, что в таком варианте AES обеспечивает как шифрование пакетов данных, так и их целостность (то есть защищает канал от внедрения поддельных пакетов).

Когда эта разработка была завершена, Wi-Fi Alliance выпустил обновленную версию стандарта — WPA2. И если первый WPA подразумевал лишь шифрование TKIP, то в WPA2 требуется поддержка обоих алгоритмов, TKIP и AES. Практически все Wi-Fi-устройства, выпущенные с начала 2003 года, предусматривают модификацию до работы с AES. Начиная же с марта 2006 года Wi-Fi Alliance сделал поддержку WPA2 обязательной для всех сертифицированных Wi-Fi-устройств.

Вся эти телодвижения, казалось бы, должны обещать быстрый и безболезненный переход к гораздо более стойкой защите беспроводных коммуникаций. Тем не менее, несколько потенциальных слабостей, общих у WPA и WPA2, оставляют лазейки для взломщиков.

Одна из таких слабостей носит название PSK. Упрощенный режим использования ключей PSK, также именуемый «Персональным режимом», предназначен для домашних сетей и сетей небольших организаций, где неудобно и не принято управлять множеством ключей с помощью мудреных серверов аутентификации 802.1x.

При использовании PSK каждое Wi-Fi-устройство шифрует сетевой трафик с помощью 256-битного ключа. Этот ключ можно вводить либо как последовательность из 64 шестнадцатеричных цифр, либо — что удобнее для человека — как парольную фразу из «клавиатурных» символов кода ASCII длиной от 8 до 63 знаков. Если используется код ASCII, то 256 бит ключа вычисляются из парольной фразы с помощью стандартной криптографической функции PBKDF2, добавляющей к паролю идентификатор сети SSID и проводящей 4096 битовых «замесов» с помощью хеш-преобразования.

Увы, даже при таких мерах усложнения режим PSK, общеупотребимый в WPA, нередко оказывается уязвимым для словарных атак перебором паролей

— если, конечно, пользователь применяет слабую парольную фразу. Слабость ключа на основе фиксированного пароля, в общем-то, самоочевидна для любой криптосистемы и лечится с помощью общеизвестных в компьютерной безопасности средств, типа выбора более длинных и менее предсказуемых парольных фраз. Как показывает опыт, для противостояния подобным атакам в условиях PSK обычно бывает достаточно выбирать для пароля случайный набор знаков с длиной начиная от тринадцати произвольных символов, разрешенных клавиатурой.

Менее заметной и потому потенциально более опасной выглядит другая врожденная слабость WPA2, встроенная в систему как возможность для обратной криптосовместимости с ранее выпущенными Wi-Fi-устройствами. А именно: сделав криптоалгоритм TKIP в составе WPA и WPA2 совместимым с адаптерами, поддерживающими давно взломанный WEP, Альянс Wi-Fi этим шагом оставил, по сути, прореху, которую постепенно удается расширять для организации достаточно серьезных атак.

В частности, осенью 2008 года на PacSec, проходившей в Токио конференции Тихоокеанского региона по компьютерной безопасности, выступил немецкий аспирант Эрик Тьюз из Технического университета Дармштадта, который представил аудитории первую в своем роде практическую атаку против WPA.

Эту атаку Тьюз разработал в тесном сотрудничестве с другим немецким хакером, Мартином Беком, студентом Дрезденского университета и членом известной исследовательской команды aircrack-ng, занимающейся проблемами взлома Wi-Fi.

В работе Бека и Тьюза был показан метод для усиления уже известной прежде атаки против WEP, а на этой основе им удалось ослабить и защиту WPA — вбив своего рода клин в узкую щель криптосхемы TKIP, после «расширения» которой оказалось возможным встраивать в зашифрованный сетевой трафик поддельные пакеты. Такие пакеты, если их умело сформировать, могут вызвать в атакованной сети нешуточные проблемы.

Обнаруженная в TKIP дыра связана с контрольными суммами, которые используются для обеспечения целостности и правильности передаваемых данных. Общий механизм работы контрольных сумм выглядит примерно так: берут последовательность битов, которые надлежит передать, применяют к ним некое известное преобразование для получения короткого проверочного результата и добавляют этот результат в конец передаваемой последовательности. Проверочное преобразование устроено таким образом, что позволяет выявлять ошибочные биты или места пропусков в пакете данных.

В сетях Wi-Fi, где при беспроводной передаче относительно велики шансы потерять бит или получить его искаженным, контрольные суммы постоянно используются как для выявления ошибок при приеме, так и для обеспечения целостности пакетов. Если содержимое пакета изменилось, а контрольная сумма осталась прежней, получатель может установить, что пакет на пути своего следования был подделан.

В исходном алгоритме защиты WEP подобные идеи хоть и были заложены, но совершенно не срабатывали. Поскольку контрольная сумма там была выбрана откровенно слабой, хакеры-криптоаналитики вскоре разработали инструментарий, позволяющий менять данные в пакетах и вычислять для них новую контрольную сумму, выдавая фальшивый пакет за подлинный.

Тьюз и Бек в своей работе привлекли один из подобных инструментов, именуемый Chopchop и позволяющий «быстрым-быстрым» подбором расшифровывать отдельные пакеты вообще без восстановления WEP-ключа. Именно эта программа и послужила своего рода плацдармом для расширения атаки на WPA.

Суть метода Chopchop заключается в следующем. Алгоритм расшифровывает пакет побайтно, отсекая по одному байту с конца и корректируя контрольную сумму так, как будто этот байт был 0, потом 1… и так до 256 (алгоритм формирования контрольной суммы известен, и она не шифруется). Затем Chopchop отсылает каждый модифицированный пакет точке доступа, а та, в свою очередь, отвергает пакеты, для которых контрольная сумма не подходит. Таким образом, за 256 попыток передачи один байт дешифруемого пакета гарантированно подбирается. После этого Chopchop переходит к подбору следующего байта. Принципиально важно то, что протокол WEP не запрещает бесконечное тестирование вариантов в таком режиме — здесь нет никаких мер защиты от подобных злоупотреблений.

Эта очевидная проблема WEP в протоколе TKIP решается путем добавления второго уровня проверки целостности — через так называемый MIC, в данном случае именуемый Michael. Этот «Майкл» реализует куда лучше сконструированную контрольную сумму, которая, как и поле данных, шифруется. Теперь, дабы предотвратить тривиальную атаку Chopchop, клиент реагирует сразу же, как только получает две неверные контрольные суммы MIC в интервале 60 секунд. В ответ на это подозрительное событие клиент отключается на одну минуту, а затем требует нового обмена ключами с точкой доступа. Точка доступа при обнаружении аналогичной ситуации тоже отключается на 60 секунд, а затем обновляет ключи для каждого из своих клиентов. (В стандарте 802.11i допускается, чтобы новые мастер-ключи создавались по запросу без изменения начальной парольной фразы или сетевого ключа.)

Именно в этом нюансе Мартин Бек углядел слабое место и придумал хитрую уловку для обмана протокола. А именно: поскольку механизмы защиты WEP и TKIP используются один после другого, причем код Michael содержится внутри пакета, который проверяется контрольной суммой более слабого метода WEP, то можно попытаться взламывать пакет таким образом, чтобы быстро использовать Chopchop и при этом не запускать контрмеры со стороны MIC.

Коллега Бека, Эрик Тьюз, заметил, что в очень коротких пакетах, вроде рассылки ARP (то есть информации, которая ассоциирует IP-адрес с MAC-адресом локальной сети Ethernet), остается очень мало места для гадания и опробования догадок. В случае пакета ARP, поясняет Тьюз, заранее известно

почти все содержимое — за исключением всего двух байтов IP-адреса в собственно информационной части и еще 12 байтов в проверочной части: 8 байтов для кода MIC и 4 байтов для контрольной суммы WEP.

В такой ситуации, перебирая контрольные суммы WEP и Michael через Chopchop, разные значения двух оставшихся байтов оказалось возможным тестировать каждые 60 секунд, не вызывая остановки сеанса связи и смены ключей. В среднем, установили исследователи, на получение нужных значений требуется от 12 до 15 минут. На этом Бек и Тьюз, однако, не остановились. Описанная выше техника, позволяющая восстановить точное содержимое исходного пакета, одновременно предоставляет фрагмент использованной шифрующей последовательности. А значит, накладывая эту шифрпоследовательность на собственные данные, злоумышленники могут подделывать пакеты. В принципе, TKIP имеет механизмы для предотвращения повторного использования шифра. Но Мартин Бек обнаружил, что благодаря еще одному стандарту, а именно 802.11e, имеется-таки способ для повторного использования шифрпоследовательности, что позволяет многократно — от семи до пятнадцати раз — ретранслировать фальшивые пакеты с данными, сфабрикованными злоумышленниками.

Такую возможность в стандарте 802.11e предоставляет сервис QoS, обычно используемый для задания приоритетов сетевым пакетам. Эта сервисная возможность была встроена в Wi-Fi таким образом, чтобы пакеты, требующие максимально быстрой доставки — в частности, речевые пакеты, — могли проходить через сеть в первую очередь. Однако это удобство аукнулось тем, что с работой очередей оказалась связана и возможность многократного использования одной и той же шифрпоследовательности. То есть, аккуратно отправляя поддельные пакеты из разных очередей, удается избегать запуска счетчика для защиты от повторов шифра. Используя разные тонкости в работе QoS по стандарту 802.11e, Тьюз и Бек показали, что в принципе имеется возможность отправить от 8 до16 поддельных пакетов, защищенных одной и той же шифрпоследовательностью.

На практике это означает, что можно реализовать несколько типов атак против Wi-Fi, защищенной средствами WPA. Например, становится тривиальной задача по «отравлению ARP», то есть внесению хаоса в работу сети, ассоциируя IP-адрес с совсем другими Ethernet или Wi-Fi-адаптерами. Или, скажем, становится возможным обман межсетевых экранов, которые блокируют лишь входящие (из Интернета в локальную сеть) соединения, поскольку поддельный ARP-пакет создает впечатление, будто запрос исходит от одной из машин локальной сети.

Еще один возможный сценарий: «отравление ARP» позволяет сканировать весь трафик внутренней сети компании и вылавливать любую информацию, в том числе логины-пароли (правда здесь потребуется инсайдер с монитором трафика).

Демонстрируя все эти результаты на PacSec-2008, Эрик Тьюз подчеркнул, что чересчур волноваться по данному поводу вряд ли имеет смысл, поскольку

информация в сети, защищенной WPA, в целом остается в безопасности. Ибо алгоритм TKIP как таковой по-прежнему остался невскрытым, а что реально удалось получить — так это лишь короткий фрагмент шифрпоследовательности без восстановления криптоключа,

Не прошло и года после откровений Тьюза-Бека, как Тосихиро Охигаси из Хиросимского университета и Масакату Мори из Университета Кобе заметно превзошли достижение немцев. Те же самые действия, к тому же без опоры на сервис QoS, занимают теперь около минуты.

Понятно, что подделка отдельных коротких пакетов в сети, защищенной системой TKIP, не тянет на полный взлом защиты WPA (как кричали о том газетные заголовки). Новый метод японцев по-прежнему не позволяет вскрывать собственно ключ шифрования WPA и читать зашифрованные им потоки данных.

Главная особенность атаки, разработанной японцами, — это творческое развитие метода Бека-Тьюза применительно к ситуациям типа «человек посередине». В своей статье2 Охигаси и Мори описывают схему, в которой компьютер-клиент и точка доступа Wi-Fi разнесены так далеко, что общаются не напрямую, а через компьютер-посредник, имеющий более мощный сигнал и принадлежащий атакующей стороне. Посредник действует как ретранслятор, передающий пакеты трафика в обоих направлениях. Когда надлежит послать поддельные пакеты, противник выполняет стандартную атаку типа Chopchop применительно к подходящему короткому пакету, вскрывает его 64-битный MIC, а затем может смастерить пакет такого вида, который требуется злоумышленнику. Новый пакет кодируется с надлежащими проверочными суммами и передается в точку доступа, принимающую его за подлинный.

Как и атака Бека-Тьюза, атака японцев наглядно демонстрирует небезупречность защиты, однако в целом не угрожает шифрованию потока данных в сетях Wi-Fi. Понятно, что оба метода подчеркивают слабости криптографии, основанной на алгоритме TKIP, который был разработан для срочного латания самых вопиющих дыр в защите WEP. Однако красить эту новость только в черный цвет все равно нет оснований, поскольку уже имеющиеся в Wi-Fi-устройствах средства шифрования давно готовы к подобному повороту событий.

Протокол WPA2 с шифрованием на основе криптоалгоритма AES является обязательным стандартом во всех Wi-Fi-продуктах начиная с 2006 года и на сегодняшний день не продемонстрировал абсолютно ничего похожего на подобные слабости. Так что для надежной защиты остается лишь выбрать нужные опции в настройках беспроводной сети.

В случае домашней сети или сети небольшого офиса можно рекомендовать:

- в качестве «имени сети», SSID, выбрать нечто уникальное и характерное только для вас, дабы защититься от взлома сетевого ключа (куда подмешивается SSID) лобовыми методами словарного перебора;
- в поле «режим безопасности» выбрать WPA2;

- в поле «управление ключами» (PSK/EAP) выбрать PSK (про выбор длинной и случайной парольной фразы в PSK уже говорилось);
- в поле «тип шифра» (Cipher Type) выбрать AES.

При таких настройках безопасности (если маршрутизатор и сетевые адаптеры достаточно новые, то есть совместимые) защита должна быть максимально прочной.

3.3 Протокол WPA2

WPA и WPA2 (Wi-Fi Protected Access) — представляет собой обновлённую программу сертификации устройств беспроводной связи. Технология WPA пришла на замену технологии защиты беспроводной Wi-Fi сети WEP. Плюсами WPA являются усиленная безопасность данных и ужесточённый контроль доступа к беспроводным сетям. Немаловажной характеристикой является совместимость между множеством беспроводных устройств, как на аппаратном уровне, так и на программном. На данный момент WPA и WPA2 разрабатываются и продвигаются организацией Wi-Fi Alliance [14].

Низкий уровень безопасности, несомненно, долго оставался одним из главных недостатков сетей W-Fi. Будучи основанными на технологии VPN, первые БЛВС обеспечивали безопасность данных на уровне 3, что сохраняло уязвимость сети IP для атак. Реализованный на уровне 2 протокол WPA2 защищает беспроводную сеть значительно лучше. Однако лишь он один не способен обеспечить должную безопасность корпоративной сети. Управление же доступом по этому протоколу в сочетании с основанным на портах протоколом аутентификации IEEE 802.1X позволяет исключить возникновение большинства проблем безопасности. Применение этой пары протоколов не защитит вас от “нелегальных” устройств, атак типа “отказ в обслуживании” или какого-либо другого вмешательства извне, но обеспечит безопасность беспроводных коммуникаций.

Протокол WPA2 является значительным усовершенствованием механизма безопасности WEP исходного стандарта 802.11. Протокол WEP был уязвимым для атак и плохо реализовывался производителями. В связи с этим он так и не нашел большого применения в корпоративных сетях. Слабые места WEP и то, что их весьма просто использовать в вероломных целях, стимулировали разработку стандарта 802.11i, который был утвержден и опубликован в 2004 г. В рамках проекта стандарта 802.11i организация Wi-Fi Alliance разработала протокол WPA, а позднее — WPA2, обеспечивающий более высокий уровень безопасности, чем первая версия WPA.

WPA поддерживает использующий метод шифрования RC4 протокол TKIP и может быть программно реализован путем обновления драйвера или встроенного ПО. Наличие счетчика пакетов и частых ротаций ключей предотвращают атаки с воспроизведением пакетов или их повторным вводом. Протокол WPA обеспечивает контроль целостности данных, используя метод

контрольной суммы MIC. Данный метод подвержен атакам «Brute-Force», но при этом передача сетевого трафика на минуту автоматически приостанавливается и, если основанная на WPA точка доступа детектирует в течение 60 с более одной ошибки MIC протокола TKIP, сеансовые ключи переустанавливаются, снижая, таким образом, риск атак до минимума.

Между тем протокол WPA2 задействует новый метод шифрования, основанный на более мощном, чем RC4, алгоритме шифрования AES.

WPA и WPA2 работают в двух режимах аутентификации: персональном (Personal) и корпоративном (Enterprise). В режиме WPA2-Personal из введенной открытым текстом парольной фразы генерируется 256-разрядный ключ, иногда именуемый предварительно распределяемым ключом PSK. Ключ PSK, а также идентификатор SSID и длина последнего вместе образуют математический базис для формирования главного парного ключа PMK, который используется для инициализации четырехстороннего квитирования связи и генерации временного парного или сеансового ключа PTK, для взаимодействия беспроводного пользовательского устройства с точкой доступа. Как и статическому протоколу WEP, протоколу WPA2-Personal присуще наличие проблем распределения и поддержки ключей, что делает его более подходящим для применения в небольших офисах, нежели на предприятиях. Все возможные параметры безопасности приведены в таблице 3.1 [15].

Таблица 3.1 Возможные параметры безопасности

Свойство	Статический WEP	Динамический WEP	WPA	WPA 2 (Enterprise)
Идентификация	Пользователь, компьютер, карта WLAN	Пользователь, компьютер	Пользователь, компьютер	Пользователь, компьютер
Авторизация	Общий ключ	EAP	EAP или общий ключ	EAP или общий ключ
Целостность	32-bit ICV	32-bit ICV	64-bit MIC	CRT/CBC-MAC Part of AES
Шифрование	Статический ключ	Сессионный ключ	Попакетный ключ через TKIP	CCMP (AES)
Распределение ключей	Однократное, вручную	PMK	Производное от PMK	Производное от PMK
Вектор инициализации	Текст, 24 бита	Текст, 24 бита	Расширенный вектор, 65 бит	48-бит номер пакета (PN)
Алгоритм	RC4	RC4	RC4	AES
Длина ключа, бит	64/128	64/128	128	До 256
Инфраструктура	Нет	Radius	Radius	Radius

Протокол WPA2-Enterprise успешно решает проблемы с распределением статических ключей и управления этими ключами. Интеграция данного протокола с большинством корпоративных сервисов аутентификации обеспечивает контроль доступа на основе учетных записей. Для работы в данном режиме необходимы следующие данные:

- Имя;
- Пароль;
- Сертификат безопасности или одноразовый пароль.

Аутентификация осуществляется между центральным сервером аутентификации и рабочей станцией. Точка доступа или беспроводной контроллер проводят мониторинг соединения и направляют аутентификационные пакеты на соответствующий сервер аутентификации (как правило, это сервер RADIUS). Базой для режима WPA2-Enterprise служит стандарт 802.1X, поддерживающий основанную на контроле портов аутентификацию пользователей и машин, пригодную как для проводных коммутаторов, так и для беспроводных точек доступа.

К основным компонентам аутентификации 802.1X относятся клиентский “запросчик”, аутентификатор и сервер аутентификации.

Согласно спецификации 802.1X, клиентский запросчиком считается устройство, запрашивающее доступ к сети. Обычно под запросчиком подразумевается ноутбук или какое-либо другое мобильное устройство. На поверку клиентским запросчиком в конечном счете оказывается установленное на этом устройстве ПО, инициализирующее и отвечающее на команды 802.1X (рисунок 3.1)

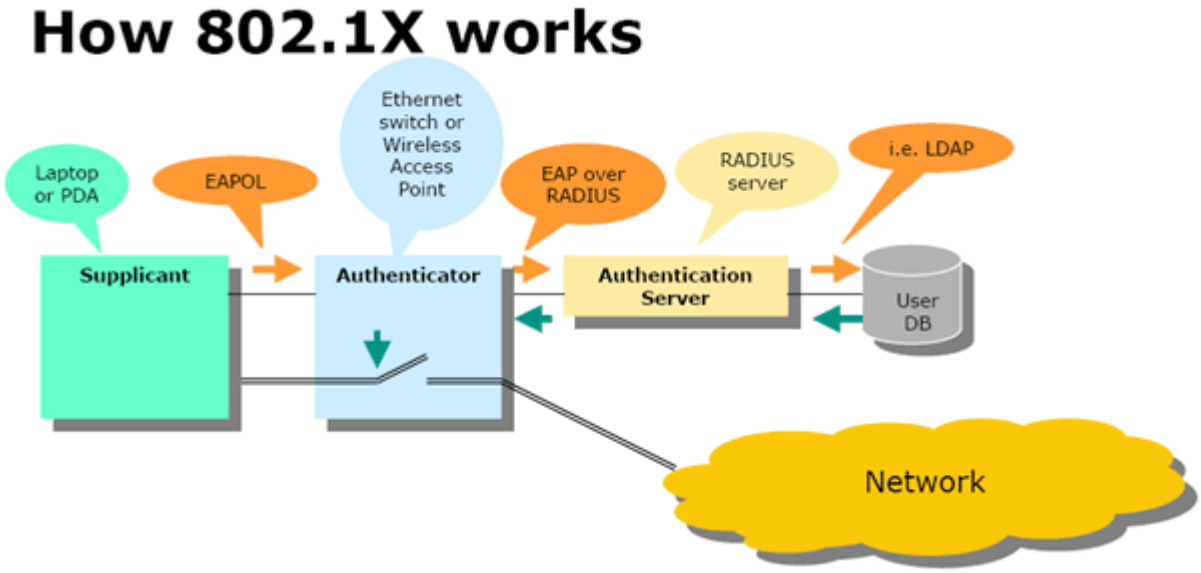


Рисунок 3.1 – 802.1x в действии

Аутентификатор (обычно это точка доступа, хотя в централизованной архитектуре доступа он может размещаться на коммутаторе/контроллере) аутентифицирует клиент для доступа к сети. Это устройство обрабатывает запросы от клиентского запросчика, сохраняя сетевой интерфейс

заблокированным до тех пор, пока не получит от сервера аутентификации указание на его разблокирование. В свою очередь, последний принимает и обрабатывает запрос на аутентификацию. Хотя обычно в качестве сервера аутентификации используется сервер RADIUS, в данной ситуации можно использовать не всякий такой сервер, а лишь тот, что совместим с методами аутентификации [13].

Клиент (клиентский запросчик) и точка доступа (аутентификатор) обмениваются трафиком EAP по протоколу уровня 2 EAPoL. Клиентский запросчик не способен взаимодействовать с сервером RADIUS посредством протокола уровня 3: когда точка доступа получает трафик EAP от клиента, она преобразует его в соответствующий запрос RADIUS и передает серверу RADIUS на обработку (рисунок 3.2).

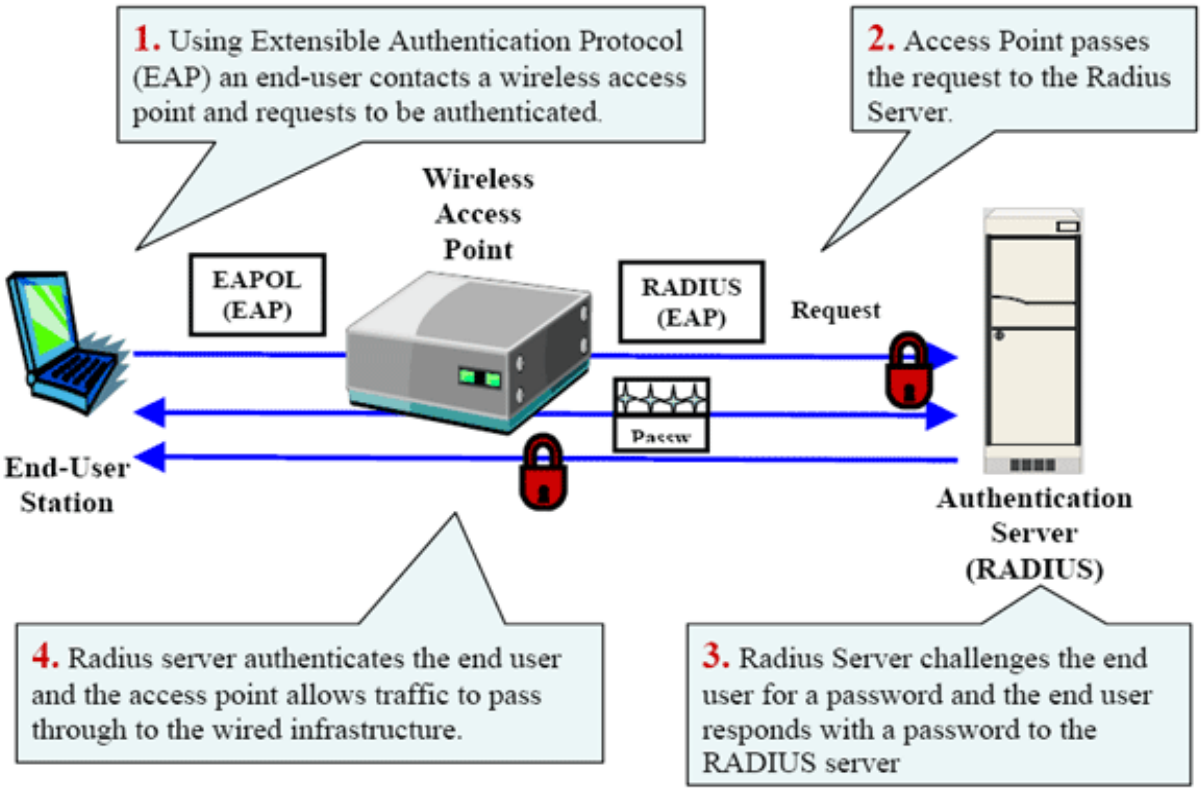


Рисунок 3.2 – Процесс аутентификации

Сам протокол EAP является контейнерным, то есть фактический механизм авторизации дается на откуп внутренних протоколов. На настоящий момент сколько-нибудь значимое распространение получили следующие:

- **EAP-FAST** (Flexible Authentication via Secure Tunneling) — разработан фирмой Cisco; позволяет проводить авторизацию по логину-паролю, передаваемому внутри TLS туннеля между суппликантом и RADIUS-сервером;
- **EAP-FAST EAP-TLS** (Transport Layer Security). Использует инфраструктуру открытых ключей (PKI) для авторизации клиента и сервера (суппликанта и RADIUS-сервера) через сертификаты, выписанные доверенным удостоверяющим центром (CA). Требует выписывания и

установки клиентских сертификатов на каждое беспроводное устройство, поэтому подходит только для управляемой корпоративной среды. Сервер сертификатов Windows имеет средства, позволяющие клиенту самостоятельно генерировать себе сертификат, если клиент — член домена. Блокирование клиента легко производится отзывом его сертификата (либо через учетные записи);

- **EAP-TTLS** (Tunneled Transport Layer Security) аналогичен EAP-TLS, но при создании туннеля не требуется клиентский сертификат. В таком туннеле, аналогичном SSL-соединению браузера, производится дополнительная авторизация (по паролю или как-то ещё);
- **PEAP-MSCHAPv2** (Protected EAP) — схож с EAP-TTLS в плане изначального установления шифрованного TLS туннеля между клиентом и сервером, требующего серверного сертификата. В дальнейшем в таком туннеле происходит авторизация по известному протоколу MSCHAPv2;
- **PEAP-GTC** (Generic Token Card) — аналогично предыдущему, но требует карт одноразовых паролей (и соответствующей инфраструктуры).

Структуру EAP-кадра можно увидеть на рисунке 3.3

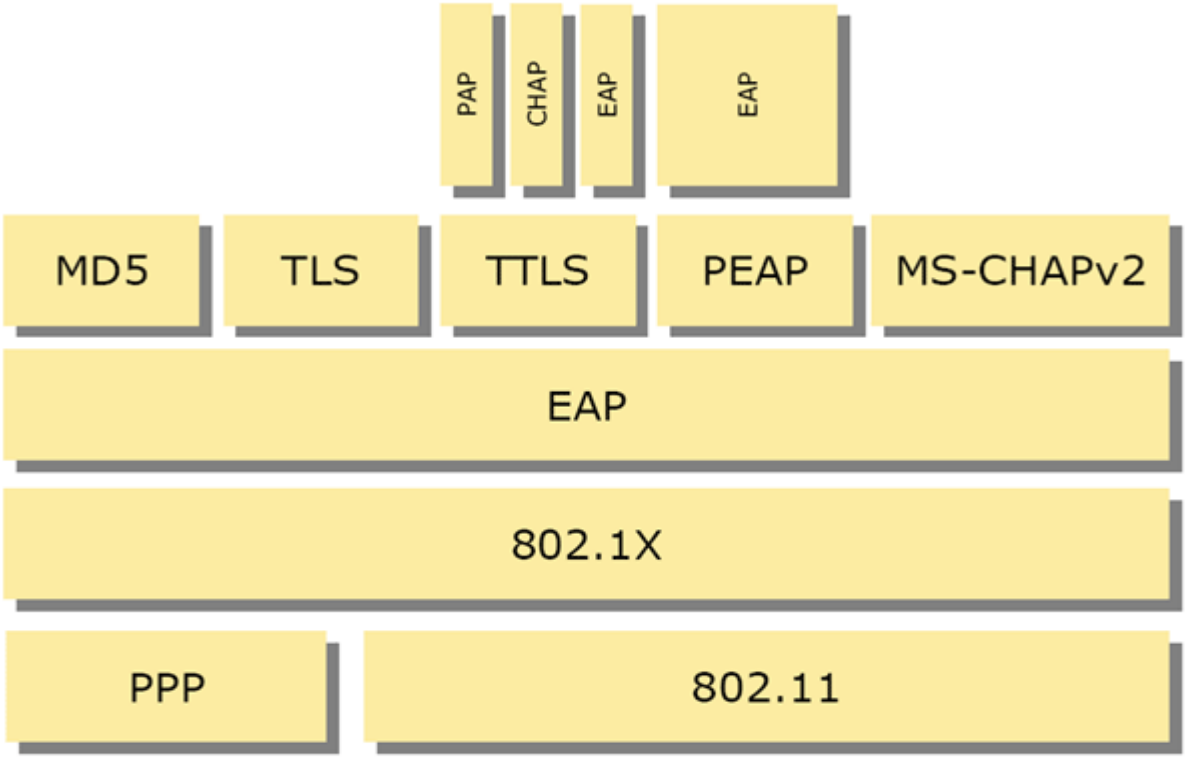


Рисунок 3.3 – Структура EAP-кадра

Выполнив процедуру аутентификации 802.1X, клиент получает от сервера аутентификации главный ключ, который “привязывается” к данному сеансу аутентификации. На основе этого ключа на клиенте и на сервере аутентификации генерируется один и тот же парный главный ключ PMK. Аутентификатор (в данном случае точка доступа) получает ключ PMK от сервера аутентификации посредством предварительно определенного атрибута

RADIUS. Обладая ключом PMK, клиент и точка доступа генерируют парный временный ключ PTK, фактически не обмениваясь им. Такая процедура генерации ключей становится возможной благодаря использованию четырехстороннего квитирования связи, предотвращающего развертывание атак типа «man in the middle», нацеленных на перехват служебной информации.

В WPA2 имеется три типа ключей PTK: ключ подтверждения ключа KCK, применяющийся для проверки целостности кадра EAPOL-Key; ключ шифрования ключа KEK, используемый для шифрования группового временного ключа GTK и временные ключи TK — для шифрования трафика.
Все “привязанные” к точке доступа беспроводные устройства должны “уметь” расшифровывать широковещательный и многоадресный трафик. Они выполняют это посредством одного и того же временного группового ключа GTK. Если точка доступа изменяет ключ GTK — например, по причине его компрометации, то она генерирует новый ключ, используя простое двухстороннее квитирование связи и ключ KEK для шифрования ключа GTK.

При осуществлении клиентским устройством роуминга между двумя точками доступа полный процесс его аутентификации сервером RADIUS может занимать сотни миллисекунд (а то и несколько секунд), что является неприемлемым для телефонов Wi-Fi или потоковых видеоприложений ноутбуков. Поэтому большинство корпоративных беспроводных устройств оснащаются такими предусмотренными спецификацией 802.11i возможностями, как предварительная аутентификация и кэширование ключа PMK, позволяющими минимизировать связанную с роумингом задержку.

Предварительная аутентификация позволяет мобильному клиенту аутентифицироваться на другой, расположенной поблизости точке доступа, оставаясь “привязанным” к своей первичной точке доступа. При применении кэширования PMK клиенту, вернувшемуся с обслуживаемой роумингом территории “домой”, не нужно выполнять полную процедуру повторной аутентификации 802.1X.

3.4 Шифрование WPA2

Протокол WPA2 основывается на методе шифрования AES, сменивший стандарты DES и 3DES. Требующий огромного объема вычислений, стандарт AES нуждается в аппаратной поддержке, которая не всегда имеется в старом оборудовании.

Для аутентификации и обеспечения целостности данных WPA2 использует протокол CBC-MAC, а для шифрования данных и контрольной суммы MIC — режим счетчика CTR. Код целостности сообщения (MIC) протокола WPA2 представляет собой не что иное, как контрольную сумму и в отличие от WEP и WPA обеспечивает целостность данных для неизменных полей заголовка 802.11. Это предотвращает атаки типа «Packet replay» с целью расшифровки пакетов или компрометации криптографической информации.

Для расчета MIC используется 128-разрядный вектор инициализации IV, для шифрования IV — метод AES и временный ключ, а в итоге получается 128-разрядный результат. Далее над этим результатом и следующими 128 бит данных выполняется операция “исключающее ИЛИ”. Результат ее шифруется посредством AES и TK, а затем над последним результатом и следующими 128 бит данных снова выполняется операция “исключающее ИЛИ”. Процедура повторяется до тех пор, пока не будет исчерпана вся полезная нагрузка. Первые 64 разряда полученного на самом последнем шаге результата используются для вычисления значения MIC.

Для шифрования данных и MIC используется основанный на режиме счетчика алгоритм. Как и при шифровании вектора инициализации MIC, выполнение этого алгоритма начинается с предварительной загрузки 128-разрядного счетчика, где в поле счетчика вместо значения, соответствующего длине данных, берется значение счетчика, установленное на единицу. Таким образом, для шифрования каждого пакета используется свой счетчик.

С применением AES и TK шифруются первые 128 бит данных, а затем над 128-бит результатом этого шифрования выполняется операция “исключающее ИЛИ”. Первые 128 бит данных дают первый 128-разрядный зашифрованный блок. Предварительно загруженное значение счетчика инкрементально увеличивается и шифруется посредством AES и ключа шифрования данных. Затем над результатом этого шифрования и следующими 128 бит данных снова выполняется операция “исключающее ИЛИ”.

Процедура повторяется до тех пор, пока не зашифруются все 128-разрядные блоки данных. После этого окончательное значение в поле счетчика сбрасывается в ноль, счетчик шифруется с использованием алгоритма AES, а затем над результатом шифрования и MIC выполняется операция “исключающее ИЛИ”. Результат последней операции пристыковывается к зашифрованному кадру.

После подсчета MIC с использованием протокола CBC-MAC производится шифрование данных и MIC. Затем к этой информации спереди добавляется заголовок 802.11 и поле номера пакета CCMP, пристыковывается концевик 802.11 и все это вместе отправляется по адресу назначения.

Расшифровка данных выполняется в обратном шифрованию порядке. Для извлечения счетчика задействуется тот же алгоритм, что и при его шифровании. Для дешифрации счетчика и зашифрованной части полезной нагрузки применяются основанный на режиме счетчика алгоритм расшифровки и ключ TK. Результатом этого процесса являются расшифрованные данные и контрольная сумма MIC. После этого, посредством алгоритма CBC-MAC, осуществляется перерасчет MIC для расшифрованных данных. Если значения MIC не совпадают, то пакет сбрасывается. При совпадении указанных значений расшифрованные данные отправляются в сетевой стек, а затем клиенту

3.5 Вардайвинг

Вардрайвинг – это процесс поиска и взлома уязвимых точек доступа беспроводных сетей Wi-Fi человеком либо группой лиц, оснащенных переносным компьютером с Wi-Fi-адаптером и определенных программным обеспечением. Цель вардрайвинга – проникнуть в беспроводную сеть с различными целями, начиная от бесплатного использования интернет соединения – до промышленного шпионажа. Важным моментом является то – что такой взлом может производиться на очень большом расстоянии и человек, совершающий данный взлом – может скрыться [7].

Поиск точек доступа осуществляется следующим образом: злоумышленник устанавливает на свой ноутбук любой сетевой анализатор – например, InSSIDer – садится в какой либо транспорт и перемещается по городу, в свою очередь InSSIDer связан с GPS модулем. Итог – хакер получает точки доступа с их примерным расположением, дальше – уже руководствуясь личностными интересами, выбирает нужную точку доступа для атаки. Для перехвата пакетов существует специальный режим мониторинга (Monitor Mode).

В некоторых случаях, для перевода устройства в такой режим, необходимо установить в систему специальные драйверы, которые пишутся под чип конкретного производителя.

Что же касается других программных продуктов, подобных NetStumber они также оставляют нежелательный для взломщика, след – по которому он может быть вычислен. Режим пассивного сканирования также не является панацеей, так например программа Wellenreiter позволяющая проводить пассивное сканирование после опознавания беспроводной карточки ESSID заменяет следующим: «Thisisusedforwellenreiter», а MAC-адрес конфигурирует на произвольный [10].

На этом этапе, хакеру необходимо заполучить определенное количество пакетов, передаваемых в этой сети, а когда это будет выполнено – уже в спокойной обстановке – с помощью программы-взломщика получить нужный ключ. Для этих целей чаще всего используется Aircrack-ng.

Aircrack-ng — набор программ, предназначенных для обнаружения беспроводных сетей, перехвата передаваемого через беспроводные сети трафика, аудита WEP и WPA/WPA2-PSK ключей шифрования проверки их стойкости. Список программ входящих программный пакет aircrack-ng входят указан таблице 3.2.

Таблица 3.2 – Пакет программ Airchack-ng

Aircrack-ng	Взламывает ключи WEP и WP
Airdecap-ng	Расшифровывает перехваченный трафик при известном ключе.
Airmon-ng	Выставления различных карт в режим мониторинга.
Aireplay-ng	Пакетный инжектор (Linux и Windows).
Airodump-ng	Анализатор трафика: Помещает трафик в файлы PCAP или IVS и показывает информацию о сетях.
Airtun-ng	Создаёт виртуальный интерфейс туннелирования.
Airolib-ng	Хранит и управляет списками ESSID и паролей; понижает KPS атак WPA.
Packetforge-ng	Создаёт шифрованные пакеты для инъекции.

Таким образом, для сбора пакетов используется программа airodumpng. Она собирает все пакеты и пишет дамп в файл. Следующим шагом является, работа с данным файлом самой программы взломщика aircrack-ng. По некоторым данным необходимо 500 тыс. пакетов для взлома 128-битного ключа. Что касается более продвинутого шифрования, такого как WPA2-PSK– то и такие ключи возможно найти данной программой. Например, поиск по словарям или же с помощью брутфорса – данный способ гарантирует нахождение ключа, но сам процесс может быть очень длительным [8].

3.6 Сетевые анализаторы

Сетевые анализаторы или сниффер — это программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов.

Первые анализаторы считывали заголовки сообщений в пакетах данных, пересылаемых по сети, предоставляя таким образом администраторам информацию об адресах отправителей и получателей, размере файлов и другие сведения низкого уровня. Причем все это — в дополнение к проверке корректности передачи пакетов. С помощью графов и текстовых описаний анализаторы помогали сетевым администраторам провести диагностику серверов, сетевых каналов, концентраторов и коммутаторов, а также приложений. Сейчас выпускается множество анализаторов, которые подразделяются на два вида. К первому относятся автономные продукты, устанавливаемые на мобильном компьютере. Консультант может брать его с собой при посещении офиса клиента и подключать к сети, чтобы собрать данные диагностики. Второй вид анализаторов является частью более широкой категории аппаратного и программного обеспечения, предназначенного для мониторинга сети и позволяющего организациям контролировать свои

локальные и глобальные сетевые службы, в том числе Web. Эти программы дают администраторам целостное представление о состоянии сети. Например, с помощью таких продуктов можно определить, какие из приложений выполняются в данный момент, какие пользователи зарегистрировались в сети и кто из них генерирует основной объем трафика.

Вместо того чтобы выявлять низкоуровневые характеристики сети, скажем источник пакетов и пункт их назначения, современные анализаторы декодируют полученные сведения на всех семи уровнях сетевого стека Open System Interconnection (OSI) и зачастую выдают рекомендации по устранению проблем. Если же анализ на уровне приложения не позволяет дать адекватную рекомендацию, анализаторы производят исследование на более низком, сетевом уровне.

3.6.1 Wireshark

Wireshark (ранее программа была известна под названием Ethereal) - бесплатный сниффер поддерживающий работу с разными интерфейсами от Ethernet до Bluetooth и USB. По каждому из пакетов предоставляется подробная информация, которую вы можете просматривать в текстовом виде, или в виде HEX-кодов.

Кроссплатформенный, работает в таких ОС как Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Mac OS X, и, естественно, Windows. Распространяется бесплатно под лицензией GNU GPL v2.

Основная задача программы Wireshark состоит в том, чтобы перехватывать сетевой трафик и отображать его в детальном виде. Анализатор сетевого трафика можно сравнить с измерительным устройством, которое используется для просмотра того, что происходит внутри сетевого кабеля, как например вольтметр используется электриками для того чтобы узнать что происходит внутри электропроводки (но, конечно, на более высоком уровне). В прошлом такие инструменты были очень дорогостоящими и проприетарными. Однако, с момента появления такого инструмента как Wireshark ситуация изменилась. Wireshark – это один из лучших анализаторов сетевого трафика, доступных на сегодняшний момент. Wireshark работает на основе библиотеки Pcap. Библиотека Pcap позволяет создавать программы анализа сетевых данных, поступающих на сетевую карту компьютера. Разнообразные программы мониторинга и тестирования сети, сниферы используют эту библиотеку. Она написана для использования языка C/C++ так что другие языки, такие как Java, .NET и скриптовые языки использовать не рационально. Для Unix-подобных систем используют libpcap библиотеку, а для Microsoft Windows NT используют WinPcap библиотеку. Программное обеспечение сетевого мониторинга может использовать libpcap или WinPcap, чтобы захватить пакеты, путешествующие по сети и в более новых версиях для передачи пакетов в сети. Libpcap и WinPcap также поддерживают сохранение захваченных пакетов в файл и чтение файлов содержащих сохранённые пакеты. Программы написанные на основе libpcap или WinPcap могут захватить сетевой трафик,

анализировать его. Файл захваченного траффика сохраняется в формате, понятном для приложений, использующих Pcap.

Программа Wireshark стала стандартом де-факто при исследовании сетей и анализе протоколов среди приложений с открытым исходным кодом. Она предоставляет возможность проводить низкоуровневую фильтрацию пакетов и их анализ. Файлы с захваченными данными из сети (trace files) могут быть открыты в Wireshark и рассмотрены вплоть до каждого пакета [9].

Некоторые примеры использования программы Wireshark:

- Администраторы сетей используют ее для выявления причин неполадок в сетях.
- Специалисты по безопасности сетей используют ее для поиска проблем с безопасностью.
- Разработчики используют ее для отладки реализаций протоколов.
- Пользователи используют ее для изучения принципов работы сетевых протоколов.

Рабочее окно программы Wireshark показано на рисунке 3.4

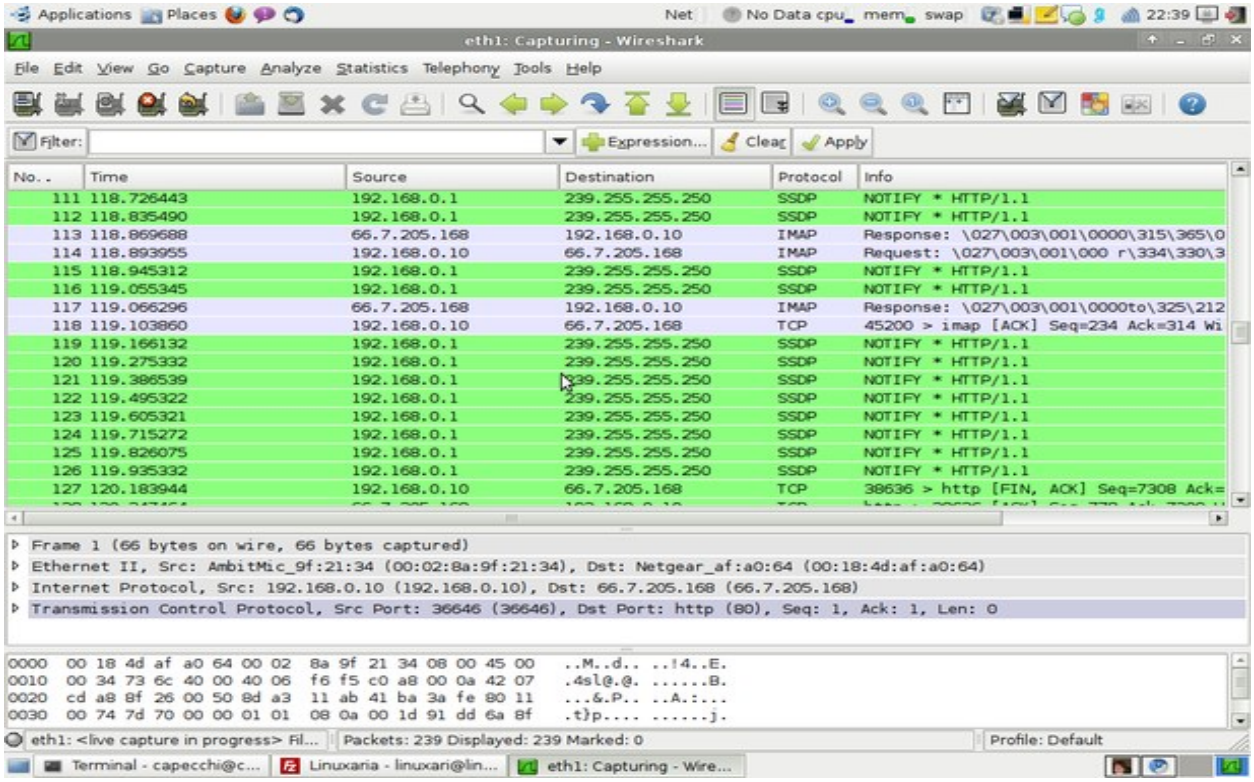


Рисунок 3.4 – Окно Wireshark

Очень частой проблемой при работе со стандартными настройками является то обстоятельство, что пользователю предоставляется огромный объем информации, а интересующую информацию становится очень сложно найти.

Большой объем информации уводит из поля зрения нужную информацию.

По этой причине фильтры так важны, ведь они могут помочь нам с поиском необходимой информации в обширном журнале данных:

- Фильтры захвата: используются для указания на то, какие данные должны записываться в журнал данных. Эти фильтры задаются до начала захвата данных;
- Фильтры отображения: используются для поиска внутри журнала данных. Эти фильтры могут быть изменены в процессе захвата данных.

Так же в установочный пакет входят следующие утилиты:

- Tshark – консольный анализатор сетевого трафика;
- Rawshark – фильтр «сырых» пакетов;
- Editcap – утилита, позволяющая открывать сохраненные пакетные дампы и изменять их;
- Text2Pcap – утилита для конвертации HEX-дампов (побайтовое представление) пакетов в формат Pcap;
- Mergecap – утилита для соединения нескольких дампов в один файл;
- Capinfos – утилита для предоставления информации о сохраненных дампах.

3.6.2 InSSIDer

InSSIDer - бесплатная утилита, которая может быть использована для диагностики Wi-Fi-сетей и загруженности беспроводных каналов. С помощью InSSIDer можно посмотреть список всех обнаруженных беспроводных сетей и узнать мощность сигнала, MAC-адрес точки доступа, производителя устройства, используемые каналы, идентификатор SSID (имя сети), силу сигнала (RSSI), степень защищенности (тип безопасности), скорость и загруженность сети и многое другое. Мощность сигнала можно отслеживать с помощью наглядных графиков в режиме реального времени.

При помощи утилиты InSSIDer вы сможете замерить уровень сигнала в различных помещениях у себя дома или в офисе. После этого можно выбрать наиболее свободный канал с максимальной скоростью и минимальными помехами. В утилите хорошо реализованы возможности по сортировке результатов сканирования сетей [19].

Рабочее окно программы Wireshark показано на рисунке 3.4

Рисунок 3.5 – Окно InSSIDer

4. Реализация проекта

4.1 Место реализации беспроводной сети

На данный момент вопрос о наличии высокоскоростной беспроводной сети Wi-Fi на производстве беспокоит многих работодателей, чьим подчиненным необходимы мобильные рабочие места. Рассмотрим несколько причин для наличия беспроводной сети на производстве.

С современный цифровой век почти у каждого сотрудника есть ноутбук и смартфона с функцией Wi-Fi. Так же беспроводные сети необходимы для компании, которые работают с иностранными поставщиками. Все эти причины побудили руководство АО «Казтелерадио» развернуть беспроводную сеть Wi-Fi на ДРТ «Кок-Тобе».

Изначально на ДРТ «Кок-Тобе» была развернута беспроводная сеть на стандарте 802.11b, с помощью точек доступа Cisco Aironet AIR-AP1242AG-R-K9 (рис. 6.1). Помехоустойчивость данного стандарта относительно слаба. А на территории ДРТ «Кок-Тобе» очень большие помехи из-за большого количества телевизионных передатчиков и спутниковых антенн. В результате для полноценной развертки беспроводной сети понадобилась установка 6й точек доступа вокруг ствола башни (Приложение А). Скорость передачи данных терялся уже в 20-30м от точки доступа. Через год было принято решение модернизаций беспроводной сети на ДРТ «Кок-Тобе».

Высокоскоростная беспроводная сеть на ДРТ «Кок-Тобе» необходима по следующим причинам:

- Необходимость наличие мобильных рабочих мест;
- Предоставление иностранным поставщикам оборудования высокоскоростного доступа в интернет;
- Наличие высокоскоростного интернета для презентаций в Центре Мониторинга и Управления качеством сети.

4.2 Выбор оборудования

На сегодняшний день рынок оборудования беспроводного доступа представлен большим разнообразием производителей. Особой популярностью пользуется продукция компании «Cisco System». Несмотря на огромную популярность данной фирмы, выбор был сделан в пользу оборудование компаний D-Link. Одним из факторов выбора продукций компаний D-Link было высокая стоимость оборудование компаний Cisco. Компаний D-Link предоставляет оборудование того уровня но по умеренным ценам. При сравнении различных систем радио доступа большое преимущество имеет продукция фирмы D-Link. D-Link - в своём классе предлагает лучшие решения для беспроводных ЛВС:

1. Безопасность;
2. Расширяемость;
3. Управление;
4. Продвинутые возможности;
5. Высочайшая скорость;
6. Масштабируемость.

Решение D-Link создает отдельные полностью беспроводные сети, обеспечивая мобильность пользователей и увеличивая их продуктивность быстро и экономически эффективно. Решение основано на беспроводных продуктах стандартов IEEE 802.11ac, предназначенных для организации связи в пределах здания. Эти продукты включают в себя точки радиодоступа, антенны и аксессуары, а также средства управления сетью.

4.2.1 Точка доступа

D-Link DAP-2695. Данное устройство относительно недавно на рынке. Отличительной чертой данного устройства является поддержка нового стандарта 802.11ac. Устройство рассчитано на работу в двух частотных диапазонах и характеризуется суммарной пропускной способностью 1750 Мбит/с (450 Мбит/с - в полосе 2,4 ГГц, 1300 Мбит/с - в полосе 5 ГГц).

Точка доступа оснащена шестью съемными антеннами. Помимо основной роли, она может выступать в качестве системы беспроводной дистрибуции контента (WDS), совмещенной с точкой доступа, моста WDS или клиента с поддержкой WDS. Управление устройством осуществляется удаленно с помощью ПО D-Link AP Manager II или модуля SNMP-управления D-View. Используя Wireless AC1750 Simultaneous Dial-Band PoE Access Point, можно связать две сети, например, находящиеся в двух расположенных рядом зданиях. К достоинствам DAP-2695 относится поддержка технологии PoE - точку доступа можно запитать от порта Ethernet (рисунок 4.1).

Таблица 4.1 – общие характеристики оборудования DAP-2695

Стандарты	• IEEE 802.11a • IEEE 802.11ac • IEEE 802.11b • IEEE 802.11g • IEEE 802.11n • IEEE 802.3 • IEEE 802.3ab • IEEE 802.3af • IEEE 802.3at • IEEE 802.3u
Сетевое управление	• HTTP • Telnet • SNMP • MIB
Алгоритмы	• 64/128-битное WEP-шифрование • Управление доступом на основе MAC-адреса

шифрования данных	• Внутренний сервер RADIUS • Протокол 802.1x • Протокол HTTPS • Протокол SSH • WPA™-Personal • WPA2™-Personal • WPA™-Enterprise • WPA2™-Enterprise
Диапазоны частот беспроводных сетей	• 2,4ГГц • 5ГГц
Модуляция	• DSSS • OFDM
Сертификаты	• FCC • IC • CE • UL • Wi-Fi
Электропитание	• PoE • Входное напряжение 48В
Прием/Передача	• 6 Антенн x 6 dBi • Мощность передатчика 26.5 dBM

Рисунок 4.1 – беспроводная точка доступа DAP-2695

4.2.2. Беспроводной коммутатор

Гигабитный коммутатор D-Link DWS-3024 для управления беспроводными точками доступа уровня 2+ предназначен для развертывания беспроводной сети для бизнеса. Благодаря этому устройству можно создавать

унифицированные масштабируемые, высокопроизводительные, безопасные и управляемые проводные/беспроводные коммутируемые локальные сети. Располагая портами Gigabit Ethernet, поддержкой технологии Power over Ethernet и возможностью подключения резервных источников питания, коммутаторы обеспечивают предприятиям простой переход к беспроводным сетям стандарта 802.11n, быстрое подключение беспроводных устройств вне зависимости от их физического расположения и централизованное управление политиками безопасности. Вид DWS-3024 представлен на рисунке 6.2.

Рисунок 6.2 – беспроводной коммутатор DWS-3024

Гигабитный коммутатор DWS-3024 является корневым устройством, позволяющим управлять безопасностью, полосой пропускания и поддерживать функционирование всей беспроводной сети. Помимо этого, выполняя мониторинг пользователей и управляя их аутентификацией во время роуминга, коммутатор может задавать и управлять всеми параметрами беспроводных точек доступа, включая радиочастотные каналы, управление питанием, сегментацией беспроводного трафика, роумингом, балансировкой нагрузки, обнаружением несанкционированных точек доступа и параметрами безопасности. Разработанный для легкого развертывания сети, коммутатор поддерживает от 24 до 48 беспроводных точек доступа, которые могут быть подключены к его портам непосредственно или опосредованно через коммутатор локальной сети. Каждый порт коммутатора снабжен поддержкой технологии 802.3af PoE, что позволяет осуществлять подключение точек доступа, находящихся в местах, где розетки питания недоступны. Гигабитные порты являются оправданным вложением средств, с целью последующего перехода к беспроводной сети стандарта 802.11ac.

Коммутатор оборудован 24 портами 10/100/1000BASE-T и 4 комбо-портами SFP. К каждому порту 10/100/1000BASE-T можно подключить беспроводную точку доступа или проводное сетевое устройство, например сервер, сетевое устройство хранения информации или другой коммутатор. Комбо-порты SFP обеспечивают гибкое подключение по оптике.

В сетях малого и среднего бизнеса (SMB) для управления несколькими точками доступа или для использования в смешанной проводной/беспроводной локальной сети потребуется только один коммутатор, поддерживающий

управление беспроводными точками доступа. При увеличении количества точек доступа в систему централизованного управления можно объединить до 4 коммутаторов. Благодаря простоте расширения, поддержке гигабитных скоростей для подключения высокоскоростных точек доступа и маршрутизации уровня 3 для организации межсетевого роуминга, DWS-3024 обеспечивает архитектуру, которая унифицирует и упрощает сложную конфигурацию беспроводной сети, подготавливая простой переход к будущим технологиям.

Для облегчения труда IT-персонала коммутатор обеспечивает выбор свободных или наименее используемых радиочастотных каналов для каждой беспроводной точки доступа, чтобы избежать интерференции с другими точками доступа или радиочастотными устройствами. Для каждой точки доступа коммутатор устанавливает выходную мощность передатчика, которая обеспечит устойчивый прием радиосигналов беспроводными клиентами и в то же время сведет к минимуму интерференцию с радиочастотными сигналами других устройств. При каждом добавлении новой точки доступа или удалении ее из сети коммутатор автоматически настраивает радиочастотные каналы и выходную мощность передатчика всех беспроводных точек доступа. Можно задать время или временной интервал выполнения автоматической настройки, что позволяет минимизировать необходимость выполнения настроек вручную.

Коммутатор обладает двумя функциями для повышения отказоустойчивости беспроводной сети, а именно - так называемый процесс "самовосстановления" и функция балансировки нагрузки между точками доступа. Чтобы восполнить недостаточную зону покрытия в результате выхода из строя точки доступа (например, из-за сбоя питания), коммутатор автоматически увеличивает выходную мощность передатчика соседних точек доступа, чтобы увеличить их зону покрытия. Для обеспечения непрерывного подключения существующих клиентов, коммутатор выполняет балансировку нагрузки между точками доступа, когда сетевой трафик достигает определенного порогового значения. В то же время коммутатор отклоняет подключение новых клиентов к точке доступа для того, чтобы избежать перегрузки полосы пропускания.

Через платформу централизованного управления, процесс обслуживания и настройки сети становится более эффективным. При запуске Интернет-браузера на любом персональном компьютере, подключенном к сети, и наборе IP-адреса управляемого коммутатора, пользователи могут рассмотреть карту топологии и точно определить местоположение точек доступа и непосредственно коммутатора. На карте используются иконки точек доступа, на которые можно нажать для выбора точки доступа, и показываются цвета, чтобы дифференцировать различные радиочастотные каналы, используемые точками доступа. В случае отказа точки доступа пользователи могут легко определите ее местонахождение на карте и заменить на другую с аналогичными параметрами.

Благодаря централизованным радиочастотным политикам, автоматическому выбору наименее используемого канала и балансировке

нагрузки точек доступа, коммутатор DWS-3024 может эффективно управлять беспроводной полосой пропускания для оптимизации трафика WLAN. Коммутатор поддерживает централизованную базу данных с информацией по доступу беспроводных пользователей к информации, например, MAC-адреса и ключи аутентификации. В сети с несколькими коммутаторами эта информация обеспечивается обмен информацией между ними. По мере перемещения пользователей по офису с использованием беспроводного оборудования, может меняться используемая для подключения точка доступа. С помощью непрерывного постоянного мониторинга точки доступа коммутатор может установить роуминг между точками доступа для этих пользователей, не требуя переустановки ключей аутентификации. Быстрый роуминг осуществляется без разрыва соединения, обеспечивая надежную работу соединения для таких мобильных приложений, как беспроводная IP-телефония и беспроводное подключение КПК.

Большинство из существующих контроллеров сети LAN осуществляет централизованную обработку трафика, что иногда вызывает его неоправданную задержку. Коммутатор DWS-3024 обеспечивает пользователям дополнительные функции.

В зависимости от беспроводного приложения, беспроводной трафик может направляться обратно к коммутатору в целях обеспечения большей безопасности или локально перенаправляться к точке доступа для оптимальной производительности.

Каждый клиент, подключаемый к беспроводной сети, проходит через процесс строгой аутентификации, что гарантирует максимальную безопасность. Является ли клиент постоянным пользователем, гостем или просто имеет доступ к сети отдела, коммутатор DWS-3024 защищает сетевую инфраструктуру с помощью большого набора функций безопасности, включая: WEP-шифрование данных, WPA/WPA2, аутентификацию пользователей 802.1x и стандарт безопасности 802.11i, адаптивный портал и аутентификацию MAC-адресов.

Коммутатор обеспечивает определение и обнаружение несанкционированных точек доступа, для предотвращения нелегального вторжения во внутреннюю сеть. Коммутатор DWS-3024 предоставляет такие сервисы, как членство в виртуальной частной группе (SSID), шифрование, аутентификацию, определение местонахождения и выдачу статистики о сетях. Во время роуминга пользователь сохраняет авторизацию, т.к. коммутатор DWS-3024 имеют общую базу данных, гарантируя безопасный доступ к соответствующим ресурсам сети. Наряду с проверкой учетных данных подключаемых пользователей в локальной базе данных, также может быть осуществлена аутентификация пользователей на внешнем сервере RADIUS. Эта дополнительная возможность гарантирует, что коммутатор не будет перегружен при одновременном подключении пользователей.

Помимо функционирования в качестве управляющего устройства в беспроводной коммутации DWS-3024 может также использоваться как

стандартный проводной коммутатор уровня 2+ с расширенным функционалом, включая поддержку маршрутизации пакетов, функции безопасности ACL, многоуровневого качества обслуживания (QoS), сегментации трафика 802.1q VLAN, IGMP Snooping для многоадресных IP-потоков, резервные гигабитные каналы с распределением нагрузки. Помимо этого, коммутаторы поддерживают оптические порты 10-Gigabit. Всё это позволяет предприятию объединять беспроводную сеть с проводной сетевой инфраструктурой. При замене существующей инфраструктуры 10/100 Мбит/с для подключения настольных компьютеров на гигабитное подключение можно использовать коммутатор DWS-3024 в качестве устройства управления беспроводной сетью, коммутатора LAN или универсального устройства, выполняющего функции проводного коммутатора и контроллера беспроводной сети [12]. Общие характеристики представлены в таблице 4.2.

Таблица 4.2 – общие характеристики оборудования DWS-3024

Интерфейсы устройства	• 24 порта 10/100/1000BASE-T с поддержкой PoE 802.3af • 4 комбо-порта SFP • Консольный порт RS-232
Резервный источник питания	Коннектор для подключения источника питания DPS-600
Power over Ethernet	• Стандарт: 802.3af • Выходная мощность на каждом порту: 15,4Вт • Общая выходная мощность: 370 Вт • Автоотключение порта при значении тока выше 350мА
Производительность	• Коммутационная матрица: 48 Гбит/с • Макс. скорость передачи пакетов: 35,71 Mbps • Метод коммутации: Store and Forward • Размер буфера пакетов: 750 КБ
Управление потоком	• Управление потоком 802.3x в режиме полного дуплекса • Метод «обратного давления» в полудуплексном режиме
Дополнительные трансиверы SFP	• DEM-310GT Трансивер SFP 1000BASE-LX, SMF, макс. расстояние до 10 км,3.3В • DEM-311GT Трансивер SFP 1000BASE-SX, MMF, макс. расстояние до 550 м, 3.3В • DEM-312GT2 Трансивер SFP 1000BASE-SX, MMF, макс. расстояние до 2 км, 3.3В • DEM-314GT Трансивер SFP 1000BASE-LH, SMF, макс. расстояние до 50 км, 3.3В • DEM-315GT Трансивер SFP 1000BASE-ZX, SMF, макс. расстояние до 80 км, 3.3В • DEM-330T Трансивер SFP 1000BASE-LX, SMF, макс. расстояние до 10 км, 3.3В, WDM (Tx: 1550 nm, Rx: 1310 nm) • DEM-330R Трансивер SFP 1000BASE-LX, SMF, макс. расстояние до 10 км, 3.3В, WDM (Tx: 1310 nm, Rx:1550 nm) • DEM-331T Трансивер SFP 1000BASE-LX, SMF, макс. расстояние до 40 км, 3.3В, WDM (Tx: 1550 nm, Rx: 1310 nm) • DEM-331R Трансивер SFP 1000BASE-LX, SMF, макс. расстояние до 40 км, 3.3В, WDM (Tx: 1310 nm, Rx:1550 nm)
Функции управления WLAN	• До 48 точек доступа (Непосредственное подключение или через коммутатор LAN) • До 2048 беспроводных пользователей (1024 пользователей при использовании туннелирования, 2048 пользователей, если туннелирование не используется)

Роуминг	• Быстрый роуминг • Роуминг между коммутаторами и точками доступа, подключенными к одному коммутатору • Внутри – и межсетевой роуминг
Управление доступом и полосой пропускания	• До 16 SSID на точку доступа (8 SSID на радиочастотный диапазон) • Балансировка нагрузки между точками доступа на основе количества пользователей или использования точки доступа
Управление точками доступа	• Автоматическое обнаружение точек доступа • Удаленная перезагрузка точек доступа • Мониторинг точек доступа: список управляемых точек доступа, несанкционированных и не прошедших аутентификацию точек доступа • Мониторинг клиентов: список клиентов ассоциированных с каждой управляемой точкой доступа • Мониторинг клиентов Ad-hoc • Аутентификация точек доступа с помощью локальной базы данных или внешнего сервера RADIUS • Централизованное управление каналами/политиками безопасности • Автоматическая настройка каналов точек доступа • Автоматическая настройка выходной мощности передачи точек доступа
Функции безопасности WLAN	• WPA Personal/Enterprise • WPA2 Personal/Enterprise • 64/128/152-битное WEP-шифрование • Классификация беспроводных станций и точек доступа на основе канала, MAC-адреса, SSID, времени • Классификация несанкционированных и действительных точек доступа на основе MAC-адреса • Типы шифрования: WEP, WPA, Dynamic WEP, TKIP, AES-CCMP, EAP-TLS, EAP-TTLS, EAP-MD5, PEAP-GTG, PEAP-MS-CHAPv2, PEAP-TLS • Адаптивный портал • Аутентификация на основе MAC-адресов • Изоляция станции

Функции 2 уровня	• Размер таблицы MAC-адресов: 8K записей
	• IGMP Snooping: 1K многоадресных групп
	• Spanning Tree:
	  ▪ 8021.D Spanning Tree
	  ▪ 802.1w Rapid Spanning Tree
	  ▪ 802.1s Multiple Spanning Tree
	• Агрегирование каналов 802.3ad:
	  ▪ до 32 групп
	  ▪ до 8 портов в группе
	• 802.1ab LLDP
	• Зеркалирование портов:
	  ▪ One-to-One
	  ▪ Many to One
	• Размер Jumbo-фреймов: до 9Кб

VLAN	• 802.1Q VLAN Tagging • 802.1V • VLAN на основе MAC-адресов • Doublee VLAN • Группы VLAN Groups: до 3965 • VLAN на основе подсетей • GVRP
Функции 3 уровня	• Статическая маршрутизация IPv4 • Плавающие статические маршруты • Proxy ARP • Размер таблицы маршрутизации: до 128 статических маршрутов • VRRP
QoS (Качество обслуживания)	• Очереди приоритетов 802.1p (до 8 очередей на порт) • CoS на основе: порта коммутатора, VLAN, DSCP, номера порта TCP/UDP,

	TOS, MAC-адреса источника/приемника, IP - адреса источника/приемника • Минимальная гарантия по полосе пропускания на очередь • Формирование трафика на порт
Списки управления доступом (ACL)	ACL на основе: порта коммутатора, MAC-адреса, очередей приоритетов 802.1p, VLAN, Ethertype, DSCP, IP-адреса, типа протокола, номера порта TCP/UDP
Функции безопасности LAN	• Аутентификация RADIUS • Аутентификация TACACS+ • SSH v1, v2 • SSL v3 • Функция Port Security: ▪ 20 MAC-адресов на порт ▪ Уведомления в случае срабатывания функции • Фильтрация MAC-адресов • Управление доступом 802.1x на основе портов и Guest VLAN • Защита от атак DoS • Управление широковещательным штормом в диапазоне от 0 до 255Kpps • Защищенный порт • DHCP-фильтрация
Методы управления	• Web-интерфейс • Сервер Telnet: до 5 сессий • Клиент TFTP • Несколько файлов конфигурации • Клиент BOOTP/DHCP SNTP • Поддержка двух копий ПО (Dual Images) • CLI • Клиент Telnet • SNMP v1, v2c, v3 • RMON v1: 4 группы (Statistics, History, Alarms, Events) • Сервер DHCP • SYSLOG
Индикаторы	• На устройство: Power, Console, RPS • Для порта 10/100/1000BASE-T: Link/Activity/Speed, PoE • Для слота SFP: Link/Activity

4.3 Разработка структурной схемы организации сети

Беспроводная сеть управляться беспроводным коммутатором D-Link DWS-3024. Беспроводной коммутатор установлен с середине башни а две точки доступа установлены на территории башни для охвата всей территорий ДРТ «Кок-Тобе».

Схема беспроводной сети представлена в Приложений Б

5 Расчетная часть

5.1 Взаимные помехи

Согласно спецификации 802.11a минимальная допустимая чувствительность любой радиостанции Wi-Fi работающей на данном стандарте не должна превышать –65 dBm, (для примера Wi-Fi беспроводный адаптер PCI модель HW-2454 имеет чувствительность -70dBm) , подавление перекрестных помех 15 дБ и -1 дБ подавление помехи от соседнего канала работающего на той-же частоте, при скорости передачи данных 54 Мбит/сек. Заметим что, оборудование Wi-Fi проектируется таким образом чтобы его спектральная маска соответствовала соответствующим требованиям по уровню перекрестных помех.

При рассмотрение источников помех для приборов, работающих в диапазоне 2,4 ГГц, необходимо учитывать устройства Bluetooth, другие Wi-Fi устройства, работающие на тех-же каналах. На данной волне создаются помехи радиотелефонами и микроволновками.

5.2 Зона покрытия Wi-Fi сетей

Фирма производитель Wi-Fi оборудования, как правило, указывает зону устойчивой работы Wi-Fi радиостанции. Так для оборудования Wi-Fi при мощности передатчика 16-18 dBm зона устойчивой работы составляет 200 м (HW-2454), исходя из этого и учитывая то что, мощность сигнала падает пропорционально квадрату расстояния можно рассчитать необходимую дополнительную мощность сигнала для передачи на любое расстояние.

$$\Delta P=20(\mathrm{Log}_{10}L - 2{,}3) \qquad (5.1)$$

Где, ΔP – дополнительная мощность [dBm] необходимая системе;
L – расстояние [м]

Необходимую дополнительную мощность ΔP можно получить, используя антенную технику. Так как маркировка продаваемых антенн идет как правило в dBi (коэффициент усиления по отношению к изотропной антенне), то его необходимо перевести в dBd (коэффициент усиления по отношению к дипольной антенне)

$$dBd=dBi - 2{,}2 \qquad (5.2)$$

В целом при использовании антенн на коэффициент усиления системы будет влиять:

- Потери в фидерах;
- Коэффициент усиления антенны передатчика;
- Коэффициент усиления антенны приемника;

Потери в фидерах (кабельных сборках) можно расчитать исходя из следующих характеристик:

- Потери в пиктейлах - 2 dBm/m;

- Потери в кабеле RJ-8U - 0,3 dBm/m;
- Потери в конекторах- 1-2 dBm/m;

Активное оборудование Wi-Fi стандартизируется тремя основными органами стандартизации Wi-Fi Alliance, IEEE, ETSI.

Согласно Code of Federal Regulation 47 (USA), нелицензионное использование Wi-Fi допускается при уровнях мощности меньших чем разрешены для первичного пользователя (есть лицензия). Что вполне разумно, учитывая , что на данной частоте работает ряд медицинских приборов и ввод Wi-Fi сети не должен приводить к сбоям.

Радиостанции стандарта Wi-Fi 802.11 имеют мощность передатчикам от 30- 100 мВт, поэтому могут быть использованы без лицензии.

Кроме того CFR оговаривает и сами уровни мощности передачи. Допустима пиковая мощность 1 Вт (30 dBm) с антенной имеющей коэффициент усиления 6 dBi. Другими словами если радиостанция не участвует в формирование моста, то ее EIRP (эквивалентная изотропно излучаемая мощность) не должен превышать 36 dBi.

Для мостов действует правило, согласно которому мощность передатчика должна снижаться на 1 дБ при каждом увеличение усиления антенны на 3 dB свыше уровня 6 dBi.

Используя выше сказанное можно оценить максимально допустимый радиус охвата точки доступа для случая когда она не работает в качестве моста:

$$L_{max} \simeq 1230 \text{ м.}$$

На радиус действия Wi-Fi связи так-же существенное влияние оказывают предмет находящиеся в зоне действия Wi-Fi передачи.

Данные предметы могут отражать микроволны и приводить к многолучевому замиранию или поглощать их (ткани, бумага).

5.3 Расчет зоны действия сигнала

Расчет дальности работы беспроводного канала связи. Без вывода приведем формулу расчета дальности. Она берется из инженерной формулы расчета потерь в свободном пространстве:

$$FSL = 33+20\ (1gF+1gD) \qquad (5.3)$$

FSL (Free Space Loss) - 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:

$$\text{Yдб} - P_t, \text{дБмВт} + G_t, \text{дБи} + G_T, \text{дБи} - P_{min}, \text{дБмВт} - L_t, \text{дБ} - L_T, \text{дБ} \qquad (5,4)$$

где $P_t, \text{дБмВт}$ - мощность передатчика, $G_t, \text{дБи}$ - коэффициент усиления передающей антенны, $G_T, \text{дБи}$ - коэффициент усиления приемной антенны, $P_{min}, \text{дБмВт}$ - чувствительность приемника на данной скорости, $L_t, \text{дБ}$ - потери сигнала в коаксиальном кабеле и разъемах

передающего тракта, L_T,дБ - потери сигнала в коаксиальном кабеле и разъемах приемного тракта.

Зависимость чувствительности от скорости передачи Фирма Майкрософт включила в свои продукты некоторое подобие криптозащиты. Но это весьма законопослушная фирма, которая чётко соблюдает все экспортные ограничения США, да ещё и перестраховывается. Это не позволяет надеяться на стойкость такой защиты. К тому же, алгоритм шифровки не описан, что, как было показано выше, является показателем ненадёжности.

Таблица 5.4 – Параметры данных

Скорость	Чувствительность
54 Мбит/с	-66 дБмВт
48 Мбит/с	-71 дБмВт
36 Мбит/с	-76 дБмВт
24 Мбит/с	-80 дБмВт
18 Мбит/с	-83 дБмВт
12 Мбит/с	-85 дБмВт
9 Мбит/с	-86 дБмВт
6 Мбит/с	-87 дБмВт

Для каждой скорости приемник имеет определенную чувствительность. Для небольших скоростей (например, 1-2 Мегабита) чувствительность наименьшая: от -90 дБмВт до -94 дБмВт. Для высоких скоростей чувствительность намного выше. В качестве примера в таблице приведены несколько характеристик обычных точек доступа 802.11a,b,g.

В зависимости от марки радио модулей максимальная чувствительность может немного варьироваться. Ясно, что для разных скоростей максимальная дальность будет разной. FSL вычисляется по формуле

$$\mathrm{FSN} = Y_{\text{дБ}} - \mathrm{SOM} \tag{5.5}$$

где SOM(System Operating Margin) - запас в энергетике радиосвязи (дБ). Учитывает возможные факторы, отрицательно влияющие на дальность связи, такие как:

- температурный дрейф чувствительности приемника и выходной мощности передатчика;
- всевозможные атмосферные явления: туман, снег, дождь;
- рассогласование антенны, приемника, передатчика с антенно-фидерным трактом.

Параметр SOM обычно берется равным 10 дБ. Считается, что 10-децибельный запас по усилению достаточен для инженерного расчета.

Центральная частота канала F берется из таблицы 5.5:

Таблица 5.5 – Вычисление центральной частоты

Канал	Центральная частота
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 дальность связи:

$$D = 10(\frac{FSL}{20} - \frac{33}{20} - \lg F) \tag{5.6}$$

Пример. Найти расстояние, на котором будет стабильно работать связь на скоростях 56 Мбит/с и 6 Мбит/с для точки доступа DWL-2100AP и беспроводного адаптера DWL-G132. Их паспортные характеристики:

- Мощность передатчиков DWL-2100AP и DWL-G132: 16 дБмВт;
- Чувствительность DWL-2100AP на скорости 54 Мбит/с: -66 дБмВт;
- Чувствительность DWL-2100AP на скорости 6 Мбит/с: -88 дБмВт;
- Чувствительность DWL-G132 на скорости 54 Мбит/с: -66 дБмВт;
- Чувствительность DWL-G132 на скорости 6 Мбит/с: -87 дБмВт;
- Коэффициент усиления штатной антенны DWL-2100AP: 2 дБи.
- Коэффициент усиления штатной антенны DWL-G132: 0 дБи.

Потерь в антенно-фидерном тракте, т.е. между беспроводными точками и их антеннами, нет.

Решение:

Найдем расстояние на скорости 54 Мбит/с. Параметр FSL равен

$$FSL = 16+2-(-66) - 10 + 74дБ \quad (5.7)$$

Находим дальность работы беспроводного оборудования на данной скорости (в качестве примера возьмем шестой канал):

$$D_{54} = 10\left(\frac{74}{20} - \frac{33}{20} - \lg 2437\right) = 0{,}046км \approx 50м \quad (5.8)$$

Найдем расстояние на скорости 6 Мбит/с. FSL равен

$$FSL = 16+2-(-88) - 10 = 96дБ \quad (5.9)$$

Определим дальность работы беспроводного оборудования на данной скорости:

$$D_6 = 10\left(\frac{96}{20} - \frac{33}{20} - \lg 2437\right) = 0{,}579км \approx 580м \quad (5.10)$$

5.4 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 5.1). Естественные (земля, холмы, деревья) и искусственные (здания, столбы) преграды, попадающие в это пространство, ослабляют сигнал.

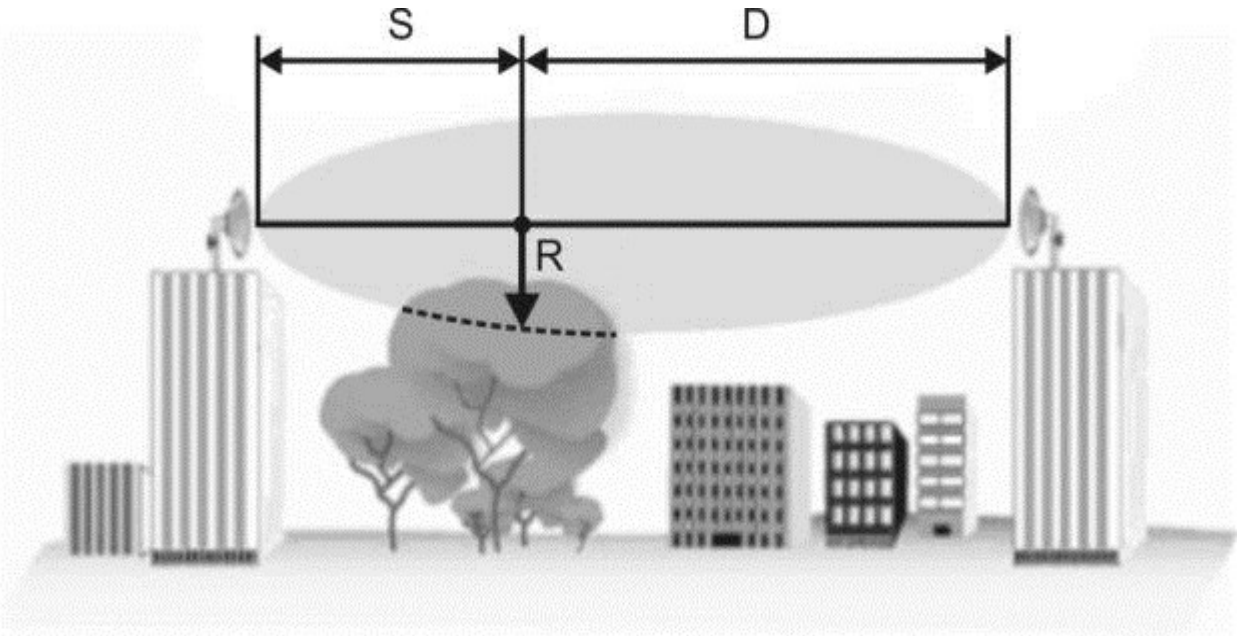


Рисунок 5.1 – Зона Френеля

Радиус первой зоны Френеля над предполагаемой преградой может быть рассчитан с помощью формулы

$$R = 17{,}3\sqrt{\frac{1}{f}\frac{SD}{S+D}}, \qquad (5.11)$$

где R - радиус зоны Френеля (м); S, D - расстояние от антенн до самой высшей точки предполагаемого препятствия (км); f - частота (ГГц).

Обычно блокирование 20% зоны Френеля вносит незначительное затухание в канал. При блокировании свыше 40% затухание сигнала будет уже значительным, следует избегать попадания препятствий на пути распространения.

Этот расчет сделан в предположении, что земля плоская. Он не учитывает кривизну земной поверхности. Для протяженных каналов следует проводить совокупный расчет, учитывающий рельеф местности и естественные преграды на пути распространения. В случае больших расстояний между антеннами следует стараться увеличивать высоту подвеса антенн, принимая во внимание кривизну земной поверхности. Вычисление центральной частоты указанно в таблице 5.6

Таблица 5.6 – Вычисление центральной частоты

Дистанция между антеннами (м)	Требуемый радиус первый зоны Френеля на частоте 2,4 GHz (м)	Требуемый радиус первый зоны Френеля на частоте 5GHz (м)
300	3,06	2,12
1600	7	4,9
8000	15,81	10,95
10000	17,68	12,25
15000	21,65	15

ЗАКЛЮЧЕНИЕ

В данной диссертационной работе был проведен анализ работы беспроводной сети Wi-Fi на основе нового стандарта 802.11ac. Проведен обзор основных стандартов беспроводной сети 802.11. Так же рассмотрена гипотеза об опасности здоровью человека излучения от использования технологий Wi-Fi. Исследование показало что, несмотря на все опасения, уровень излучения от Wi-Fi хоть и присутствует, но он ниже уровня излучения от сотовой связи и соответственно 3G модемов.

Новый стандарт IEEE 802.11ac имеет много преимуществ. Новая рабочая частота дает возможность на полную использовать данную частоту. Новый режим модуляции увеличивает радиус работы и помехоустойчивость.

В экспериментальной части диссертационной магистерской работы был проведен сравнительный анализ работы нового стандарта по сравнению с предыдущим стандартом 802.11n. Для этого была собрана тестовая площадка. Исследования показали что при многоканальной работе новый стандарт IEEE 802.11ac показывает большое увеличение скорости передачи данных по сравнению со стандартом IEEE 802.11n.

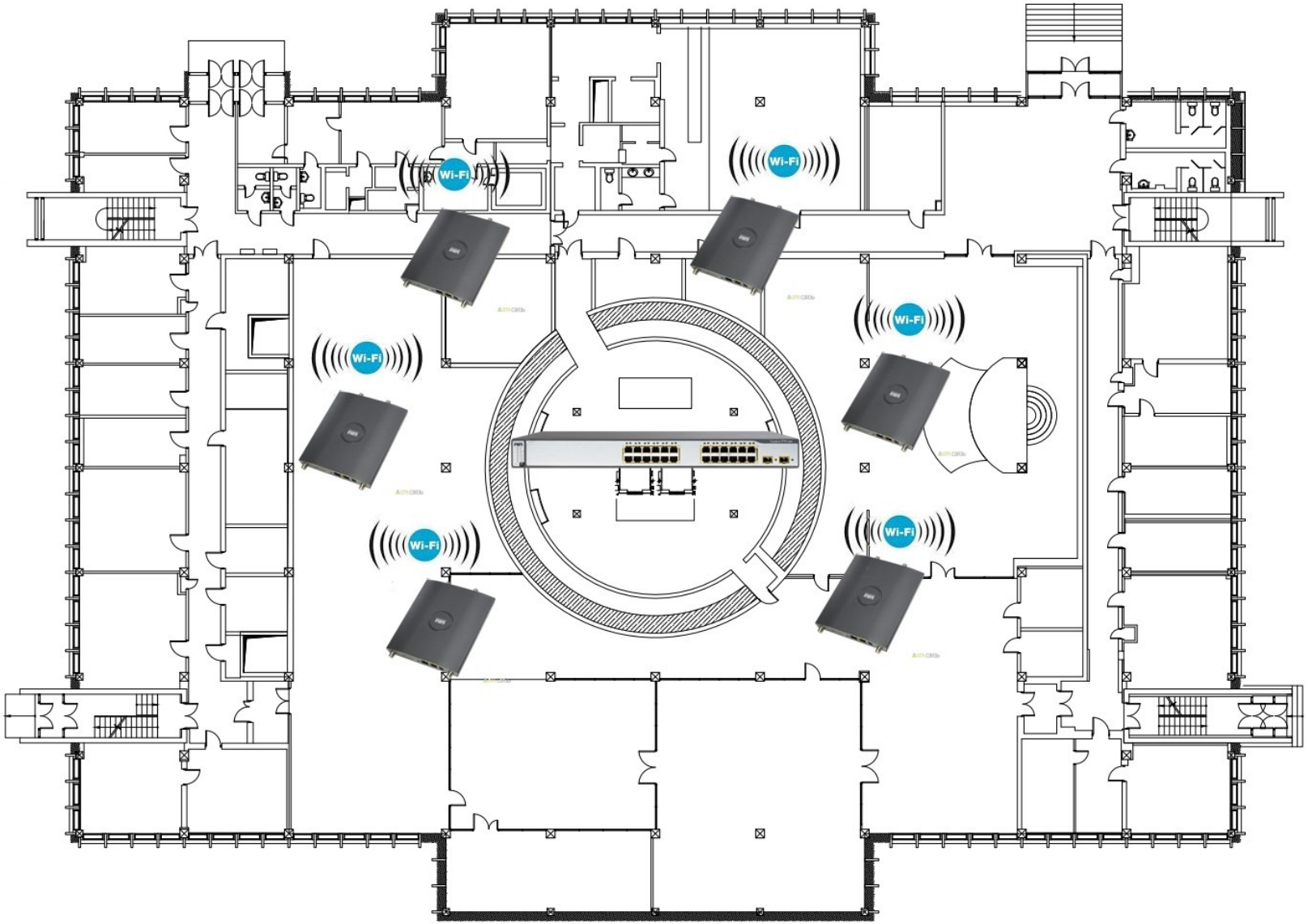
Так как основной проблемой беспроводных сетей является защита информаций, в данной работе рассмотрены протоколы шифрования беспроводных сетей и методы защиты беспроводных сетей.

На основе собранных данных был реализован проект беспроводной сети с использованием стандарта IEEE 802.11ac.

Список литературы

1. Мировые продажи планшетов - http://gfaclaims.com/science/121631-eksperty-mirovye-prodazhi-planshetov-v-2013-godu-uvelichatsya-na-427.html
2. Wi-Fi - http://ru.wikipedia.org/wiki/Wi-Fi.
3. Создание Wi-Fi сетей - http://www.flylink.ru/info/articles/489/1810- Загл. с экрана.
4. Медицинская безопасность сетей Wi-Fi - http://wi-life.ru/stati/wi-fi/marketingovye-stati-2/medicinskaya-bezopasnost-setej-wi-fi.
5. Какова стоимость утечки информации - http://axxtel.ru/press/articles/kakova-stoimost-utechki-informacii/.
6. Стандарты Wi-Fi - http://viconnect.ru/standarty-wi-fi/- Загл. с экрана.
7. Война на колесах - http://www.xakep.ru//magazine/xs/059/008/1.asp - Загл. с экрана.
8. Aircrack-ng — набор программ, предназначенных для обнаружения беспроводных сетей - http://ru.wikipedia.org/wiki/Aircrack-ng — Загл. с экрана.
9. Wireshark приручение акулы – www.habrahabr.ru/company/pentestit/blog-/204274.
10. В поисках Wi-Fi - http://www.xakep.ru//magazine/xs/059/012/1.asp - Загл. с экрана.
11. Следующее поколение Wi-Fi – колесах - http://habrahabr.ru/post/136728/- Загл. с экрана.
12. Официальный сайт компаний D-Link - www.dlink.ru.
13. Защита беспроводных сетей - http://www.ixbt.com/comm/prac-wpa-eap.shtml.
14. WPA - http://ru.wikipedia.org/wiki/WPA.
15. WPA2-Enterprise, или правильный подход к безопасности Wi-Fi сети - http://habrahabr.ru/post/150179.
16. MU-MIMO - http://habrahabr.ru/post/132247.
17. Страхи и ужасы Wi-Fi - http://shkolazhizni.ru/archive/0/n-61311/
18. Вредит ли Wi-Fi нашему здоровью? - http://old.computerra.ru/networks/298522/.
19. InSSIDer - http://zyxel.kz/kb/2696.
20. Вреден ли Wi-Fi - http://inet-boom.ru/vreden-li-wi-fi.

ПРИЛОЖЕНИЕ А – Размещение точек доступа до перехода на стандарт 802.11ac.



ПРИЛОЖЕНИЕ Б – Размещение точек доступа после перехода на стандарт 802.11ac.